A MITEL PRODUCT GUIDE

Mitel Administration

Mitel Administration User Guide

July 2025

Powering connections

Contents

Overview 1

This chapter contains the following sections:

Welcome to **Mitel Administration**! Before you onboard your first customer, refer to the following topics :

1.1 What is Mitel Administration

Mitel Administration is a web-based application that enables Mitel Partners to create and manage customer accounts; and allows Account Administrator of a customer account to manage the customer account and the users in that customer account. The users in a customer account can use the various Mitel applications and 3rd party CloudLink applications after CloudLink integration is enabled on these applications. Additionally, with a MiVoice Business solution integration, it now allows Mitel Partners and Customers alike to manage users on the MiVoice Business solution.

1.2 Log in to the Mitel Administration

Note:
The Mitel Administration supports the following browsers:

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Log in as a Mitel Partner

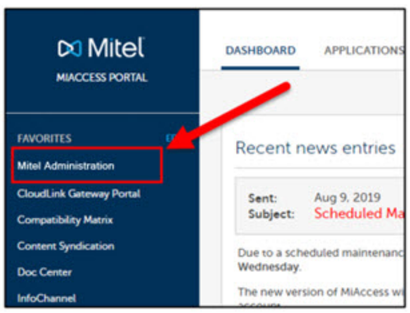
As a Mitel Partner, you can log in to Mitel Administration either via Mitel MiAccess Portal or through the URL https://accounts.mitel.io.

Note:

If you are logging in through **Mitel MiAccess Portal**, use the **Mitel Administration** portal for managing customers and users.

Refer to the *CloudLink Gateway User Guide* for gateway deployment details.

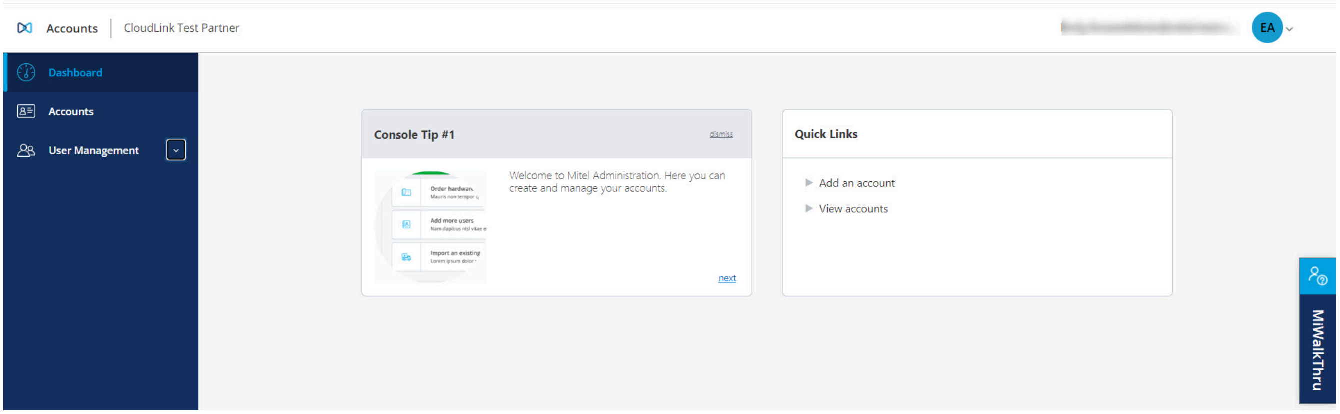
To log in to the Mitel Administration directly via the MiAccess portal, you must first log in to the Mitel MiAccess Portal using your MiAccess credentials. In the MiAccess portal home page, **Mitel Administration** will be listed on the left side of the site, provided that the CloudLink policy has been assigned you. Click **Mitel Administration**. The Mitel Administration opens, and the **Dashboard** is displayed.



To log in through the URL, click the **MiAccess** button on the **Accounts** login screen.

In the Mitel **MiAccess** login page, enter your MiAccess credentials and click **LOGIN** to log in to the Mitel Administration. On successful login, Mitel Administration opens and the **Dashboard** is displayed.

The following image shows an example of the **Dashboard** when a Mitel Partner logs in to the Mitel Administration for the first time.



When you log in to Mitel Administration for the first time, a default Partner Account is created and assigned to you in Mitel Administration and a new user (Partner) is created for you using your Mitel MiAccess User credentials. The Partner Account maintains the login details of all the Partners. The Partner Account and the Partner in an account cannot be deleted.

After logging in, Mitel Partners can Add an Account on page 11, edit, deactivate, or delete their customer accounts; and add, edit, or delete users; and enable or disable administrative rights for users. They can also assign support contacts for an account, enable or disable Integrations, and assign Orders for a customer account.

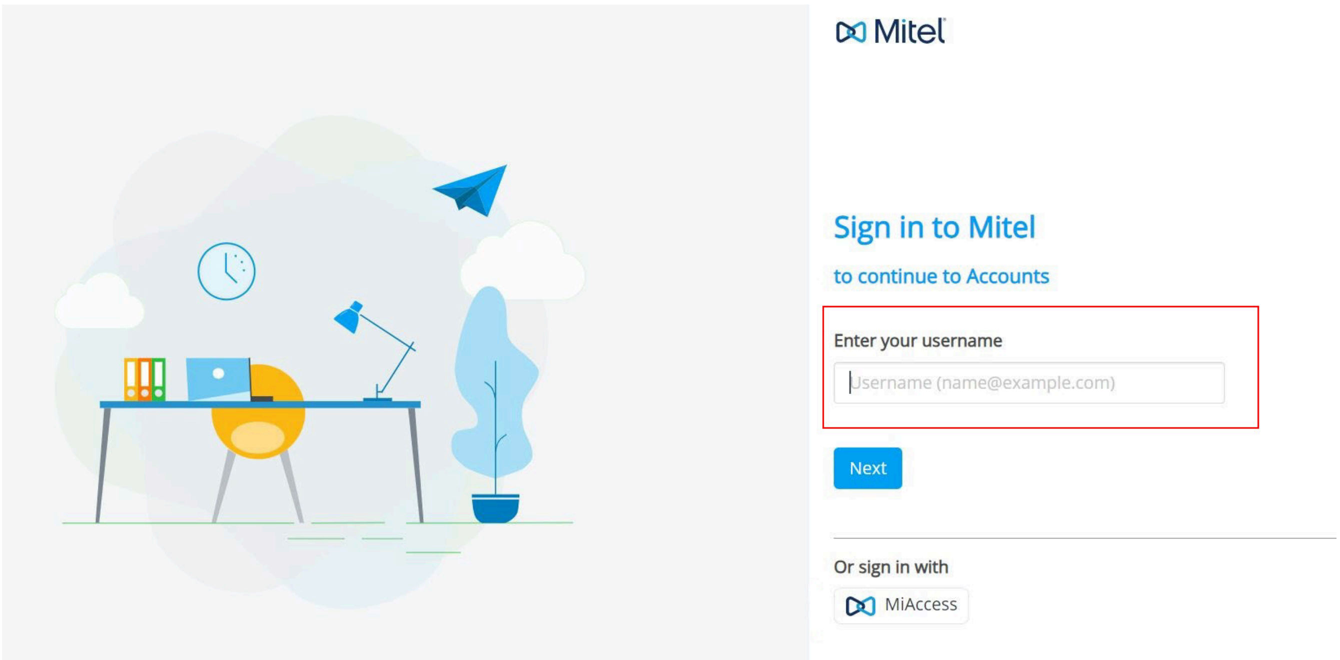
Note:
As a Mitel Partner, you can restrict access to specific end-customer accounts for the technicians and service administrators within that partner account.

Note:
The login details of a Partner remains in Mitel Administration even after the MiAccess user credentials of that Partner are disabled or removed. To remove a Partner from the Partner Account, contact Mitel Partner Technical Support by logging in to https://www.mitel.com/en-ca/login

Log in as an Account Admin or a User

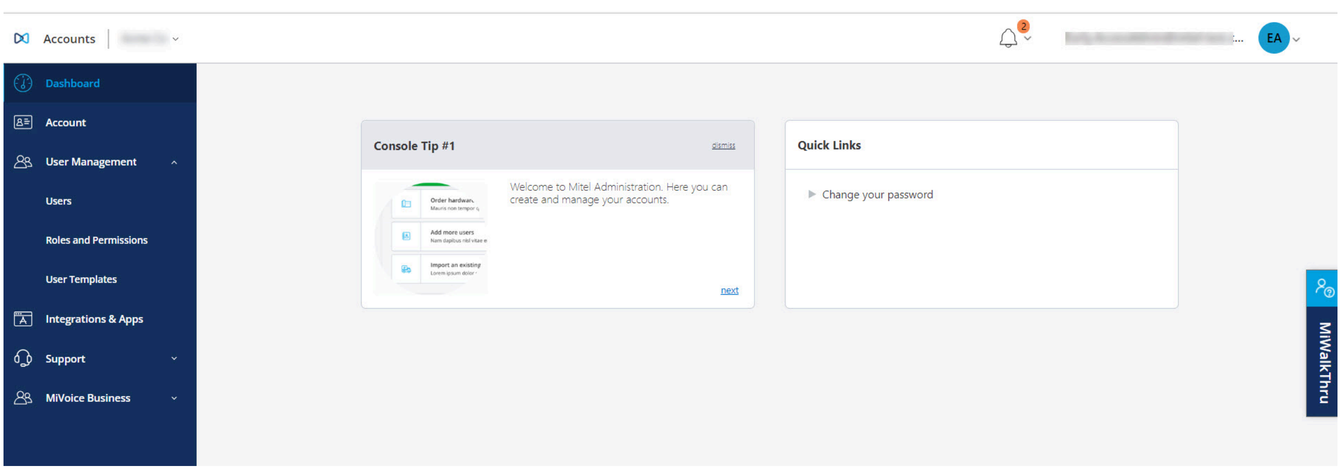
As an Account Admin of a customer account, or as a user, you can log in to Mitel Administration directly through the URL https://accounts.mitel.io after you have registered your account.

For information about how to register an account, see Welcome E-Mail on page 9. To log in, you must enter the email address (specified in the account for you) as the username and the password (selected by you while registering the account) as the password. And click **Next**.



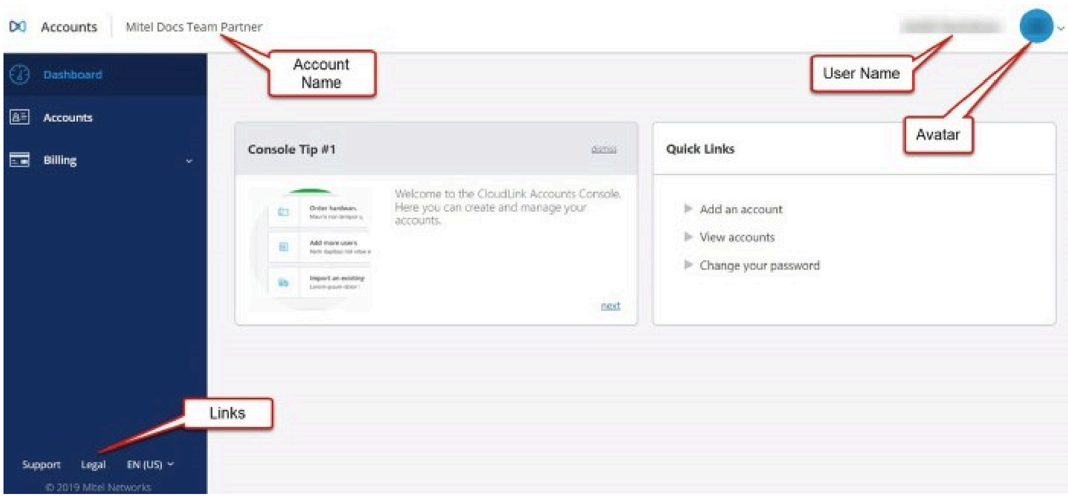
After logging in, an Account Admin of a customer account can add, edit, or delete users (including other Account Admins) in that account; and enable or disable administrative rights for these users.

The following image shows an example of the Dashboard when a Customer Admin or Account Admin logs in to Mitel Administration for the first time.

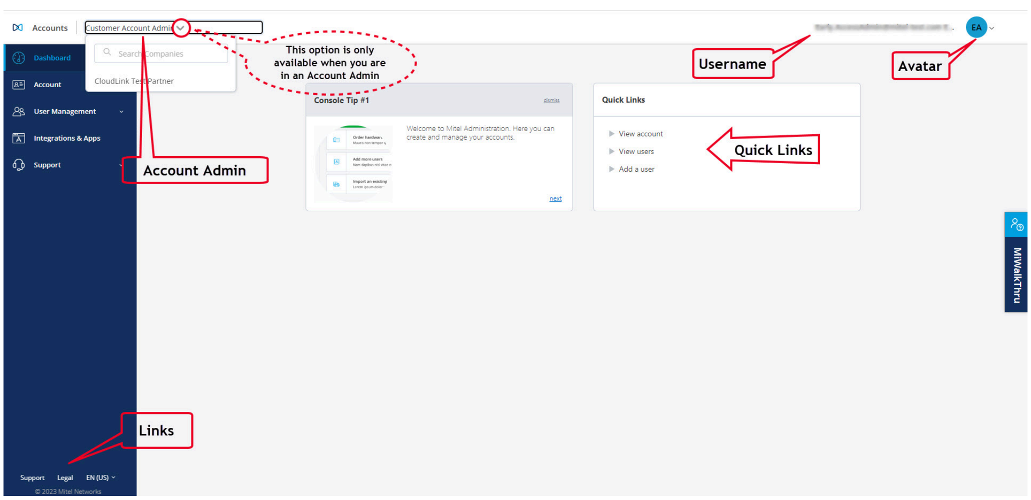


1.3 Mitel Administration Dashboard

The following image shows the Mitel Administration Dashboard when a Mitel Partner logs in.



The following image shows the Mitel Administration Dashboard when an administrative user logs in.



Note:

- The option is *only* available to a Partner Admin and Partner Admin assuming the role of an Account Admin. The admin can use this option to search for other customer accounts under this Partner account.
- As a Mitel Partner, you can restrict access to particular end-customer accounts for technicians and service administrators associated with that partner account. This guarantees that not all technicians or service administrators has the ability to view or handle all end customers within the partner account.

The following table describes the user interface elements on these two dashboards.

Dashboard Element	Function
User Name	This is the name of the Mitel Partner or the Account Admin as in Mitel Administration. To change this name, click the user in the Users page, edit the name, and click Save.
Avatar	You can click your avatar, and click Logout to log out of the application.
Account Name	This is the customer account name added by the Mitel Partner.
Links	At the bottom of Mitel Administration are the following links: • **Support** – Access to the online CloudLink help. • **Legal** – Access to the CloudLink applications end user license agreement. • **Supported Languages** – Click the down-arrow to select the supported languages from the list.
Accounts / View Accounts	This option is available only to a Mitel Partner. Use th is option to view and manage customer accounts. For more information, see Managing Accounts.
Billing	This option is available only to a Mitel Partner. Use this option to access the Orders section.
Orders	This option is available only to a Mitel Partner. Use this option to view a list of, and to manage all orders the pa rtner has purchased.
Account / View account	This option is available on the Mitel Administration Das hboard to a Partner Admin and an Account Admin. Use this option to view and manage a customer account. T his option is available to a Mitel Partner only after they s elect a customer account.

Dashboard Element	Function
Users / View users	This option is available on the Mitel Administration Dashboard only to an Account Admin. Use this option to view and manage the users in a customer account. For more information, see Managing Users. This option is available to a Mitel Partner only after they select a customer account.
Add a user	This option is available on the Mitel Administration Dashboard only to an Account Admin. Use this option to add a new user to a customer account. This option is available to a Mitel Partner only after they select a customer account.
Change your password	Use this option to change your password used to access Mitel Administration. This option will not be visible to a Mitel Partner logging in to the Accounts Console via MiAccess.

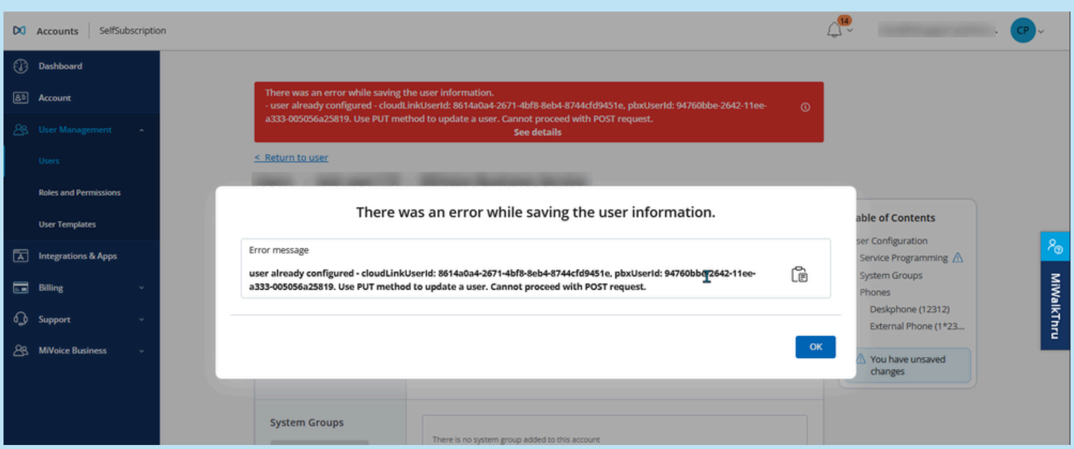
Notifications

The notification bell icon is displayed alerting the Partner and Account Admin of new activities, updates, or relevant tasks performed by them.

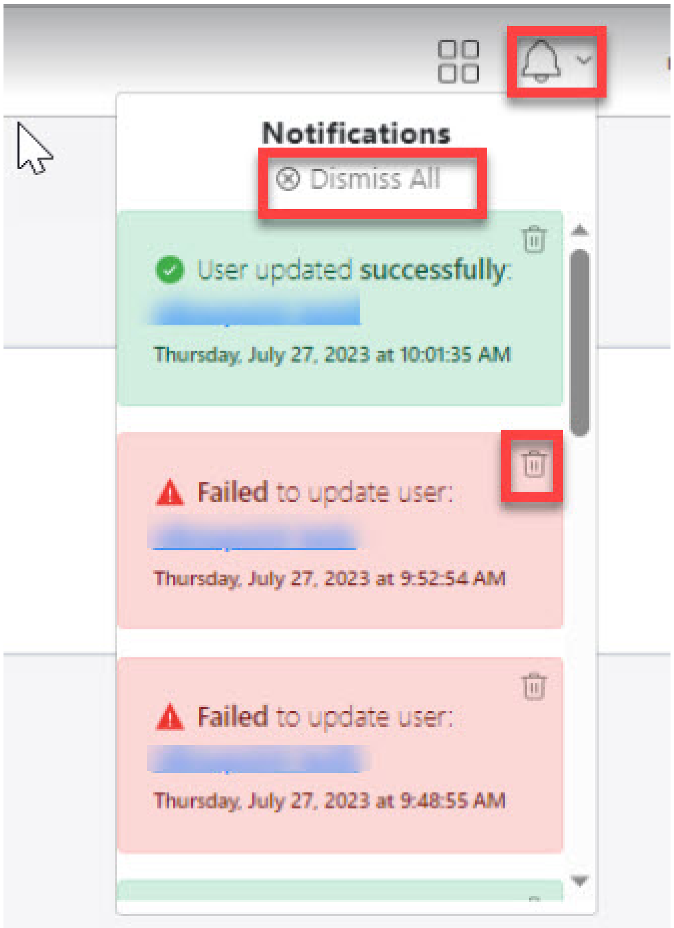
The bell icon displays a small numbered badge in contrasting color to indicate the number of pending notifications 

. By clicking the icon, users can quickly access a notification drop-down that lists the latest activities, and it's completion status on Mitel Administration.

Note:
To view complete details about an error, access the notification drop-down list, and click the **See details** hyperlink.



Partners or Account Admins have the ability to hide all notifications at once using the **Dismiss All** option or permanently delete the individual notifications using icon.



Note:
The **Dismiss All** option will remove the notifications from the current view, however, a page refresh, or a new notification will reload all notifications. Use the icon to permanently delete individual notifications.

Managing Customer Accounts 2

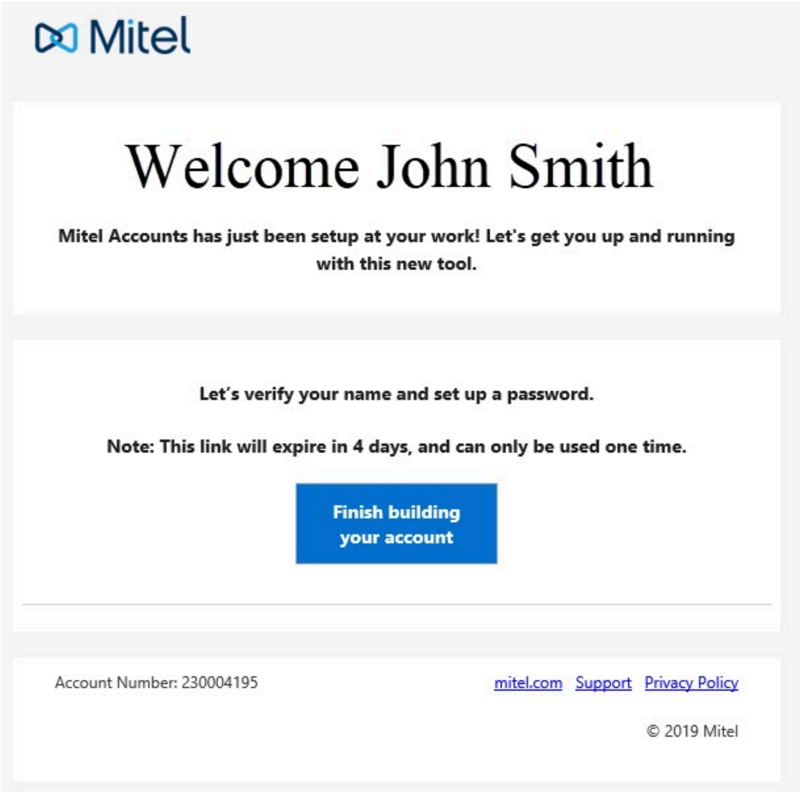
This chapter contains the following sections:

The topics provide instructions for managing customer accounts and users, assigning support contacts, adding users to a customer account in bulk, and to view and assign the MiTeam Meetings subscription purchased by a Partner to a customer account and users in the account.

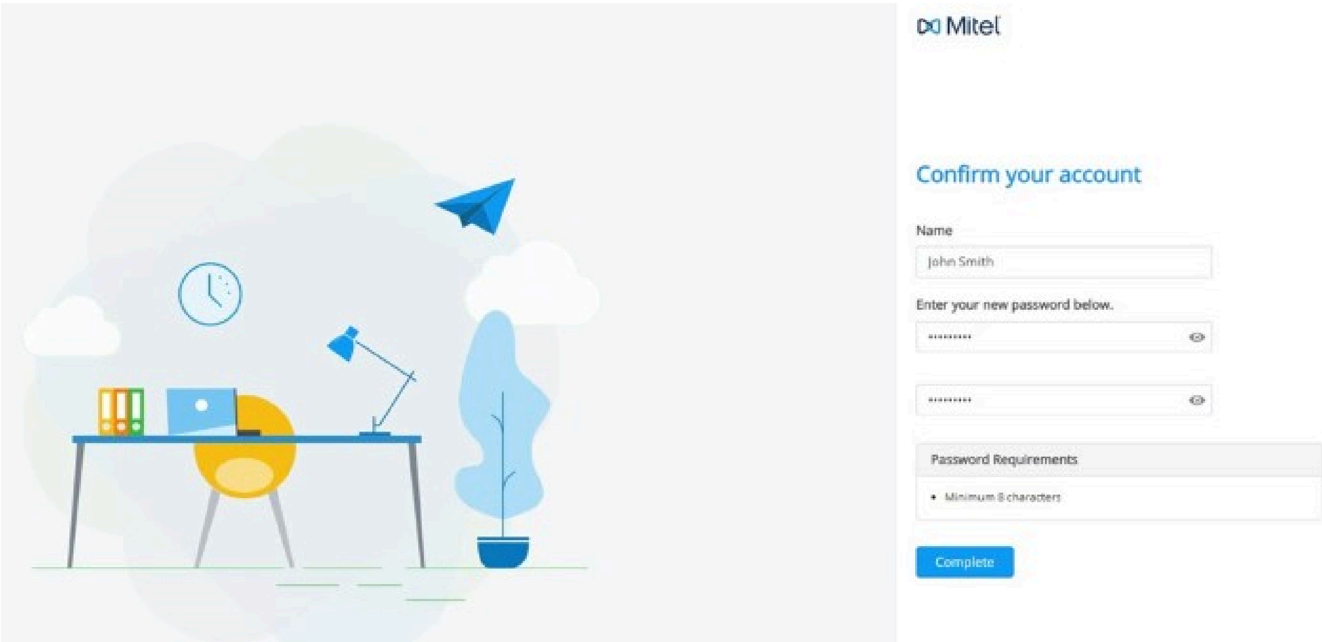
2.1 Welcome E-Mail

After logging in, Mitel Partners must Welcome E-Mail on page 9 to these accounts. They can confer administrative rights to the users they add to a customer account. Administrative users or Account Admins of a customer account can also add users to the account.

After a Mitel Partner or an Account Admin adds a user to a customer account, the Mitel Administration sends a verification email to the user. Users must complete the registration.



This verification email includes a **Finish building your account** hyperlink. Clicking this link takes users to the **Mitel Accounts** sign up page.



Here, users must create a new password for the Mitel Accounts and click **Complete** to complete the registration process.

> **Note**:
> The password must contain at least 8 characters.

After the registration is complete, an Account Admin or a regular user can log in to Mitel Administration. For more information about how to log in to Mitel Administration, see Log in as an Account Admin or a User on page 4.

> **Note**:
> A Mitel Partner has administrative rights for all the customer accounts that Partner created in the same Partner Account. An Account Admin has administrative rights only for the customer account to which they belong. For more information about the types of user roles and their privileges, see User Roles and Privileges.

2.2 Managing Accounts

The Accounts page enables a Mitel Partner to view, search for, add, edit, delete, and deactivate all the customer accounts created by that Partner. To access this page, the Partner must click the **Accounts** option from the navigation menu in the left side of the Mitel Administration Dashboard.

> **Note**:
> Mitel Partners can view the customer accounts created by other Partners within the same Partner account.

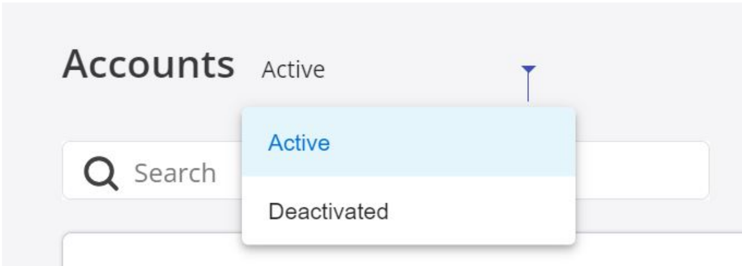
Add an Account

To add a new account, click the **Add Account** button. Enter the **Customer Name**, **Country**, **Address**, **City/Town**, and **Postal/Zip Code** of the customer. Choose the **Default Language** for the account, and assign **Support Contacts**. Click **Save**.

> **Note**:
> Every customer account in Mitel Administration is assigned a unique identifier known as the 'Account ID'. To view the Account ID of an account, go to the Account Information page of that account.

View Accounts

Click the down-arrow above the **Search** bar in the **Accounts** page, and from the drop-down list, select to view a list of active accounts or deactivated accounts by clicking, **Active**, or **Deactivated** respectively.



Search for Accounts

In the **Search** bar, type the name of the account you are searching for. The search field displays a list of matching account names as you type the letters.

Edit an Account

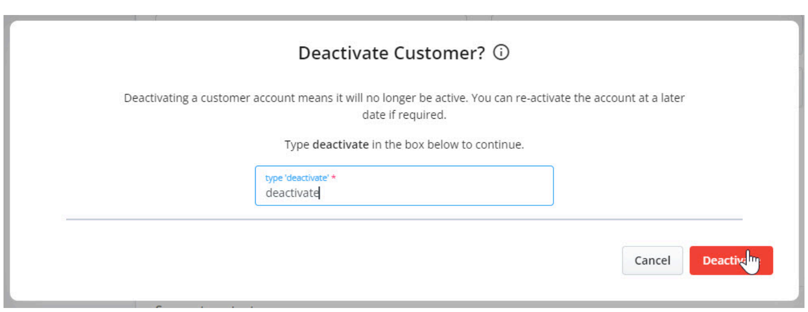
To edit the details of an account, click the account and edit the account details in the **Account Information** page that appears.

Click the  icon at the bottom right to save the changes.

Note:
This option is also available to an Account Admin of an account.

Deactivate an Account

The Mitel Partner can deactivate an account. Click the **Account** option from the left navigation menu, select the account from the **Accounts** page. Click the **Deactivate** button from the **Account Information** page that opens. A pop-up screen appears. To continue to deactivate the account, type the word “deactivate” in the text box and click **Deactivate**.



When you deactivate an account, the users in that account will no longer be able to sign in to Mitel Administration or use any CloudLink applications.

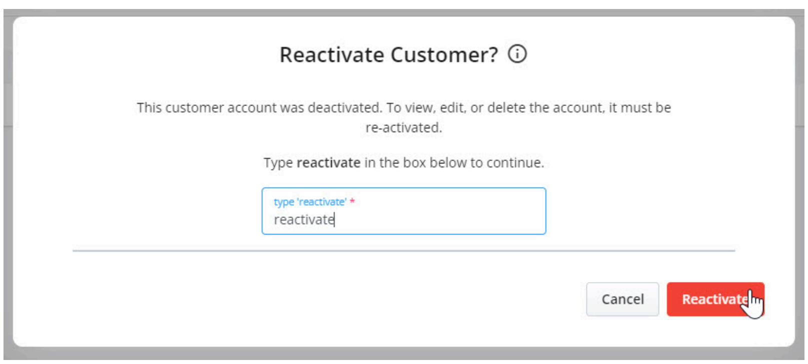
Delete an Account

Note:
When you delete an account, the CloudLink Gateway appliance associated with the account will be factory reset. For more information on factory reset, see **System Options** in Configure Advanced Settings and Options.

To delete an account, select the account from the list and click the **Delete** button. A pop-up screen opens. To continue to delete the account, type the word "delete" in the text box that appears and click **Delete**.

Reactivate an Account

The Mitel Partner can reactivate a previously deactivated account. To do so, in the **Accounts** page, select **Deactivated** using the down arrow, see View Accounts on page 12. Select the deactivated account from list of deactivated accounts in the **Accounts** page. A pop-up screen opens. To continue to reactivate the account, type the word "reactivate" in the text box that appears and click **Reactivate**.



When you reactivate an account, the users in the account will be able to sign in and access all the CloudLink applications and services. Also, the account will be listed in the CloudLink Gateway portal.

2.3 Customer Admin Account Information

The **Account Information** page of a customer admin account enables the Mitel Partner and the Account Admin to view and edit account information, view the Account ID and Cloud location, assign Support contacts, and enable or disable integrations for an account. The Mitel Partner can also delete or deactivate the customer account and view the Subscriptions details for the account.

To access the **Account Information** page of a customer account:

- A Mitel Partner must click that account from the **Accounts** page.

- A Customer Account Admin of that customer account must click the **Account** option from the left navigation menu of the Mitel Administration Dashboard.

For more information, refer Mitel Administration Dashboard.

Customer Information

Customer information panel allows you to view and edit the details of the customer to whom the account belongs to. You can edit the **Customer Name**, **Country**, **Province / State**, **Address**, **City**, and the **Postal / ZIP code** of the customer. You can also view and copy **Account ID** of the customer account, and choose the **Default Language** and the **Business Type** of the customer. The customer information panel also displays the SAP Customer Number on page 15, the Cloud location, and the **PBX Type** of the customer account.

> **Note**:
> The PBX type is available only after the CloudLink Gateway onboarding is completed successfully.

Support Contacts

You must assign Support contacts for a customer account to which all issue reports pertaining to that account are sent. For more information, see Support Contacts.

Integrations

You can integrate customer accounts with other Mitel applications - **CloudLink Gateway**, **MiCC**, **MiCollab** , **Mitel One**, **MiTeam Meetings**, **Mitel Voice Assist**, and **MiVoice Business** by sliding the toggle associated with each of these applications. For more information, see Integrating Mitel Applications with CloudLink. You can also integrate customer accounts with 3rd Party applications - **Single Sign-On**, **Azure AD Sync**, **Microsoft Office 365**, and **Microsoft Teams**.

Privileges

When you integrate a customer account with a Mitel application, the specific Privileges (Delegated Authentication and Allow Guest Access) associated with that application are also enabled for that account. A user can also enable or disable the Privileges separately for an account by using the toggle buttons associated with each of these privileges. For more information, see Integrating Mitel Applications with CloudLink.

Call Services

Bandwidth Optimization

To enable bandwidth optimization for a customer account, slide the **Bandwidth Optimization** toggle button to the right in the **Call Services** section. To learn more about bandwidth optimization, see *Bandwidth Optimization* section in the *System Requirements* topic of the CloudLink Platform documentation.

CloudLink Platform documentation.

Cloud Location

Cloud Location refers to the physical geographic region where the customer's data is stored and managed within cloud data centers.

SAP Customer Number

SAP Customer Number is a read-only field that displays the SAP ID of customers who have a subscription for a CloudLink service or application, as ordered by their Reseller or Distributor. For a MiCloud Connect account, the name of this field will be **Billing Customer Number**.

Subscriptions

The **Subscriptions** panel displays the list of all the licenses assigned to the customer account. For more information, see Subscriptions on page 35.

Note:
If your account has an active subscription but the integration is not enabled, the following error message appears:

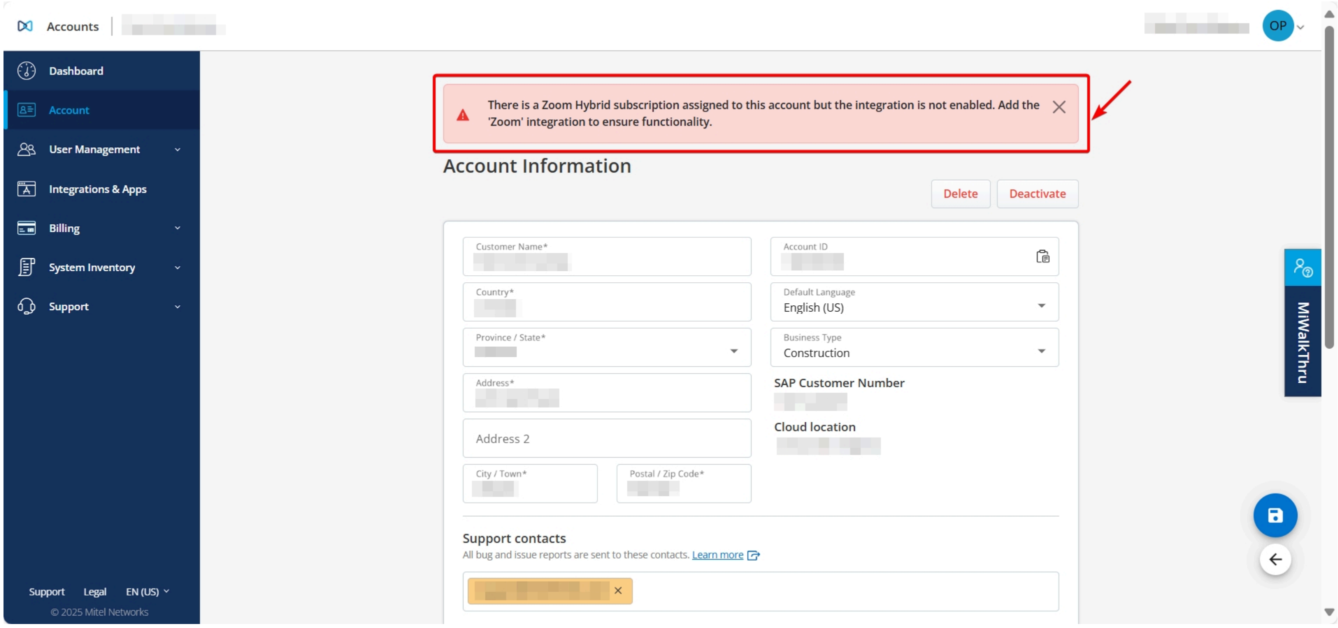
- **"There is a xxxxx subscription assigned to this account but the integration is not enabled. Add the 'xxxxx' integration to ensure functionality."**

Example: Zoom Hybrid Subscription Without Integration

Scenario: You have a **Zoom Hybrid** subscription assigned to your account, but you have not added the **Zoom** integration.

Result: When you attempt to use the subscription features, the following error message appears:

"There is a Zoom Hybrid subscription assigned to this account but the integration is not enabled. Add the 'Zoom' integration to ensure functionality."



Resolution:

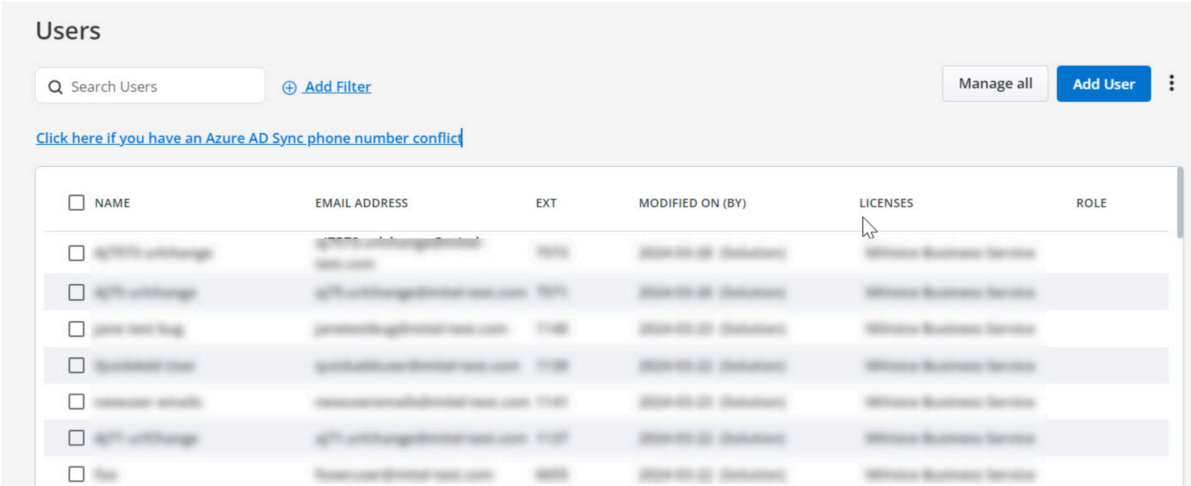
1. Go to the **Integrations** section.
2. Select **+ Add new**.
3. Under the **3rd Party** tab, select **Add** next to **Zoom**.
4. Select **Done**.
5. Complete the integration setup.

   Once the Zoom integration is enabled, the subscription features will be available.

2.4 Managing Users

The **Users** page of a partner or customer admin account contains a list of all the users in that account. All users in a customer account may interact with each other using various Mitel applications after CloudLink integration is enabled on these applications.

To integrate, enable, and manage MiVoice Business features from the Mitel Administration see MiVoice Business Integration on page 106 in this guide. You could also refer to *Mitel Administration for MiVoice Business Solution Guide* on Mitel Document Center for detailed information.



The **Users** page displays the list of users, user's email address, the extension numbers, modified on and by, configured licenses, and the role assigned to the user.

> **Note**:
> When a user's details are modified, CloudLink Gateway sends the update notification to Admin as a direct result of the user being modified by **Mitel Administration**.

The Users page enables Mitel Partners and Account Admins of a customer account to add, edit, view, and search for a user; enable or disable administrative rights for a user; reset a user's password; resend welcome email to a user; assign products and licenses to a user; and delete a user from that account.

To access the **Users** page of an account, do the following:

If you are logged in as a **Mitel Partner**:

1. Click **Accounts** from the left navigation menu. The list of users is displayed.
2. Click the **User** to access the account.

If you are logged in as a customer **Account Admin**:

1. Click and expand **User Management** from the left navigation menu, click **Users**. The list of users for this account is displayed.
2. Click the **User** to access the account.

Add User

The customer Account Admin can add users to that account. To add a new user, do the following:

1. Log into the **Mitel Administration** as an **Account Admin**.
2. Click and expand **User Management** from the left navigation menu.

3. Click **Users**. The Users page opens.
4. Click the **Add User** button. The New User form is displayed.
5. Enter the **First Name**, **Last Name**, and **Email** address. These fields are mandatory.

   Enter a valid email address for the user in the **Email** field. Ensure that you do not enter an email address already assigned to an existing user in the customer account

> **Note**:
> If an error **One or more of the attribute values are already in use** is displayed while adding a user see, the Knowledge Based article (HO4817 CloudLink - Active Directory Managing disabled active directory accounts).

6. Enter a **Mobile Number** for the user. Click the country code field to select the country code from the drop down menu.
7. Select an **SMS Number** for the user from the drop down menu. You can click on the search icon to search for a number.

   You have to enable the **Twilio** integration and **User Numbers** option to be able to assign SMS numbers to users. To do this, navigate to **Integrations and Apps > Twilio**.
8. Set the **Account Admin** toggle to on to enable administrative rights for the user. This field is optional.

   You can also enable administrative rights for the user from the User's edit page, select **Account Admin** in the **Role** drop-down list. To disable the administrative rights for a user, select **User** in the **Role** drop-down list.
9. Click **Create**. A welcome email is sent to the user's email address. Meanwhile, the Account Admin can assign licenses to the user in the User Edit page.

> **Note**:
> You can choose to resend the CloudLink account welcome email to the user, by clicking the **Resend the welcome email** hyperlink in the User Edit page.

You cannot order users by SMS Number.

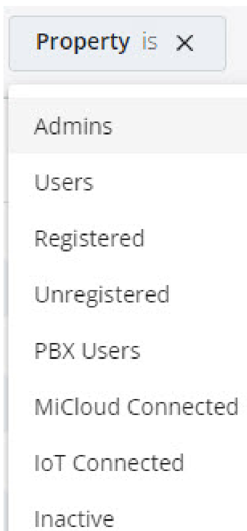
You can add users in bulk to a customer account in Mitel Administration by using the bulk import feature. For more information, see Bulk Import of Users on page 38.

Filter Users

The **+ Add Filter** 

button in the **Users** page enables the Account Administrator or Mitel Partner to filter the list of users in an account by user type and the products for which they have licenses to. To filter, click the **+Add Filter** button. A drop-down list is displayed.

To filter the list of users by user type, select **Property**. From the list of properties that are displayed, choose any type of property. To view a list of administrative users, all users, registered or unregistered users, PBX users, MiCloud or IoT connected users, click the respective options from the **Property** list: **Admins**, **Users**, **Registered**, **Unregistered**, **PBX Users**, **MiCloud Connected**, **IoT Connected**, or **Inactive**.



To filter the list of users based on the products for which they have license to, select **Product**. The products for which a user is licensed are displayed under the **Product** list.

To filter the list of users based on the SMS numbers they have been assign to, select **SMS Number**, enter the SMS number in the **Filter for SMS Number** field and click .

If you search by SMS Number, you cannot use the Search Users option. If you have used the Search Users option and you apply the SMS filter, the Search Users is disabled.

You cannot use the SMS Number filter and the Property filter at the same time. If the SMS Number filter is applied, the Property filter is not available. If the Property filter is applied, the SMS Number filter is not available.

Search for Users

In the **Search** bar, type the name, the email address, or the EXT numbers of the user you are searching for. The **Users** page displays a list of matching users as you type the letters.

Import Users

To add users in bulk to a customer account, select the customer account > click **User Management** > **Users**. Click ⋮ and click **Import Users**. For more information about adding users in bulk to a customer account, see Bulk Import of Users on page 38.

> **Note**:
> A Mitel Partner can add users in bulk to all customer accounts. An Account Admin of a customer account can add users in bulk to that account.

Edit User

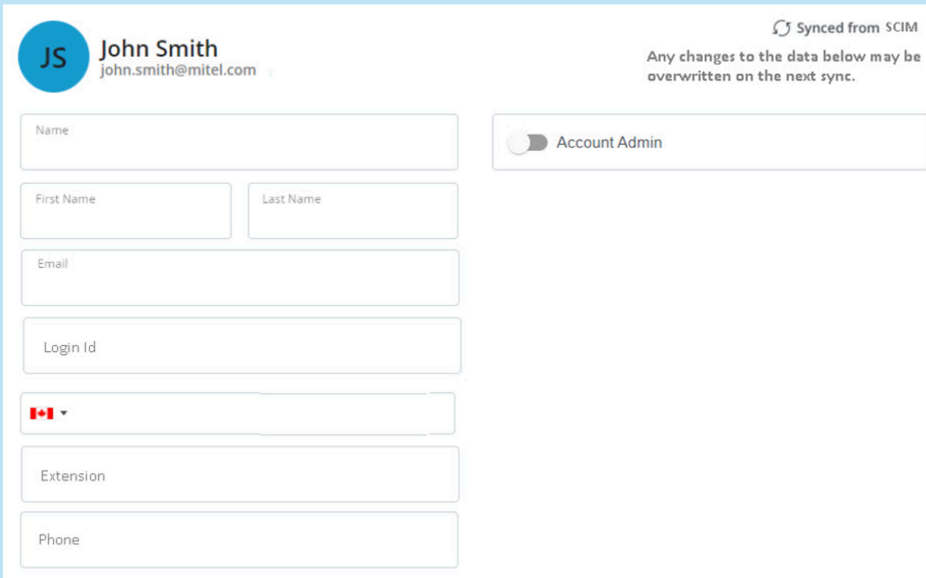
To edit the details of a user, click the user and edit the user details in the form that opens.

You can edit the **Name**, **First Name**, **Last Name**, **Email** address, and mobile number of a user; assign MiTeam Meetings license to a user (if applicable); enable or disable the **Account Admin** toggle; resend the welcome email to a user; reset the password of an Account Admin; or **Delete** a user.

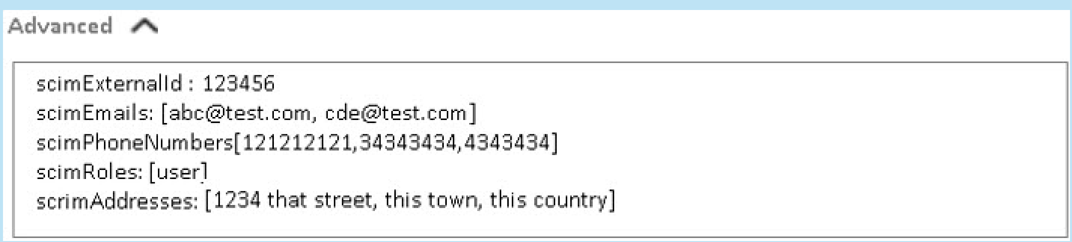
Click **Save** to save the changes or click **Cancel** to discard the changes.

Note:

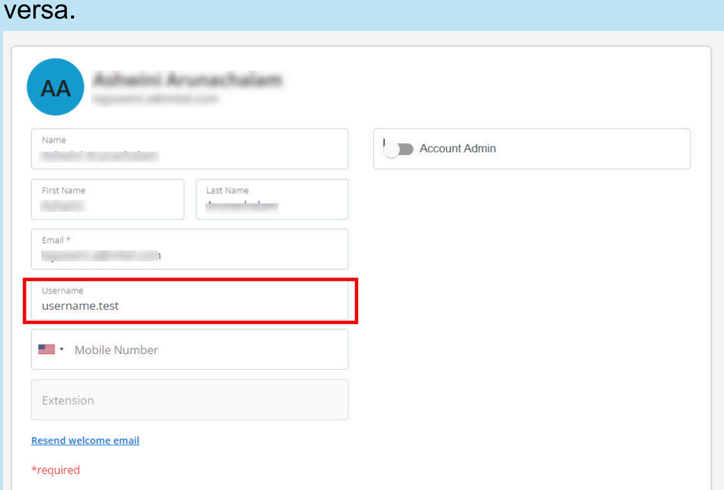
- If a user is created from an external source (such as from SCIM, PBX, or any other source except the Accounts app), some of the fields may be disabled for edit in the Accounts app. If any change is made in the source, the data may be overwritten on the next sync.



- If a user is imported from SCIM, the **User Edit** page displays an **Advance** section, which contains the SCIM data for users.



- When you add the MiVoice Business service to the user, the username field is enabled, and can be updated. If the username for the user is updated in the CloudLink account at this initial configuration of MiVoice Business service, the username entered in the Username field is synced to MiCollab and the MiVoice Business PBX. However, if the username is edited later in the CloudLink account, the updated username is not synced to MiCollab and MiVoice Business, or vice versa.



Assign a User as Account Admin

To enable administrative rights for a new user, slide the **Account Admin** toggle button to the right in the user details form when you create the user. The toggle button turns blue when a user is set as an Account Admin. To enable or disable administrative rights for a user, click the user from the **Users** page and in the user details form that opens, slide the **Account Admin** toggle button respectively to the right or to the left.

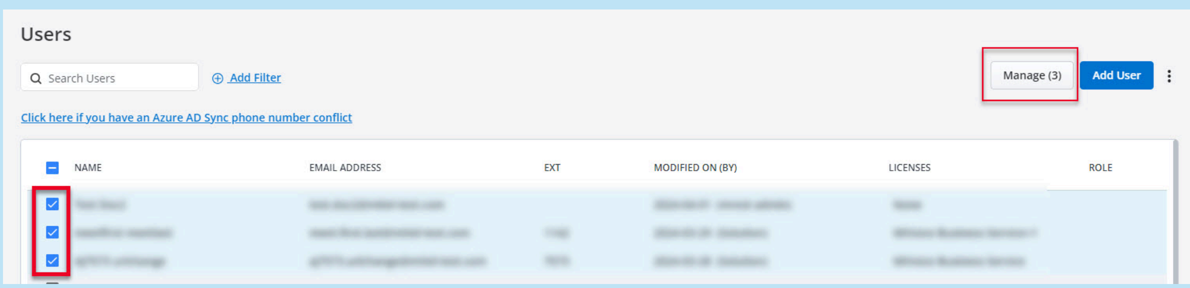
Reset Passwords

To reset the password of all users in a customer account at once, click the **Manage all** option and from the panel that opens, click **Reset passwords for all**. To reset the password of selected users, select the users from the **Users** page and do either of the following.

- Click the  icon. From the panel that opens, click **Reset CloudLink passwords**.
- Click the **Manage (x)** option and from the panel that opens, click **Reset CloudLink passwords**.

Note:

If you are selecting specific users, the **Manage (x)** option will reflect the number of users chosen.



An email containing the **Reset Password** link is sent to the user's registered email address.

Note:

- The Reset Password email is sent only to users who have registered their details with Mitel and created an account.
- If SSO integration is applied to an account, the **Reset Password** function is deferred to the IDP of the customer.

Send Welcome Email

To send a welcome email to all the users in the customer account at once, do either of the following:

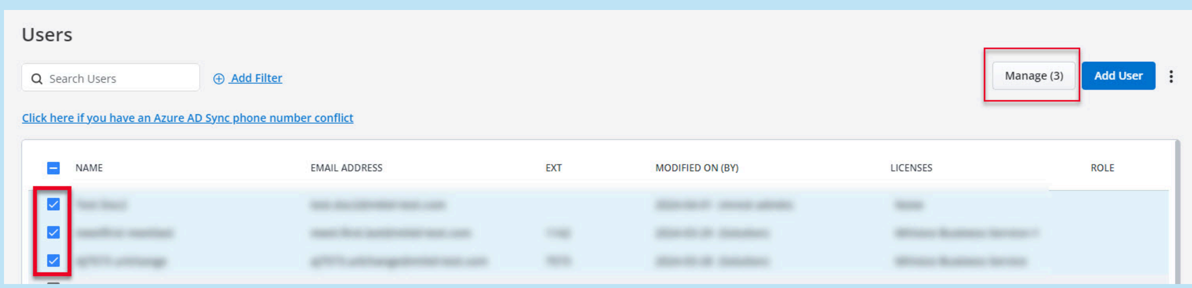
- Click the ⋮ icon from the **Users** page and from the panel that opens, click **Send CloudLink welcome emails to all** or,
- Click the **Manage all** option from the **Users** page, and from the panel that opens, click **Send CloudLink welcome emails to all**.

To send a welcome email to selected users, select the users from the **Users** page and do either of the following:

- Click the ⋮ icon from the **Users** page and from the panel that opens, click **Send CloudLink welcome emails** or,
- Click the **Manage (x)** option from the **Users** page, and from the panel that opens, click **Send CloudLink welcome emails**.

Note:

If you are selecting specific users, the **Manage (x)** option will reflect the number of users chosen.



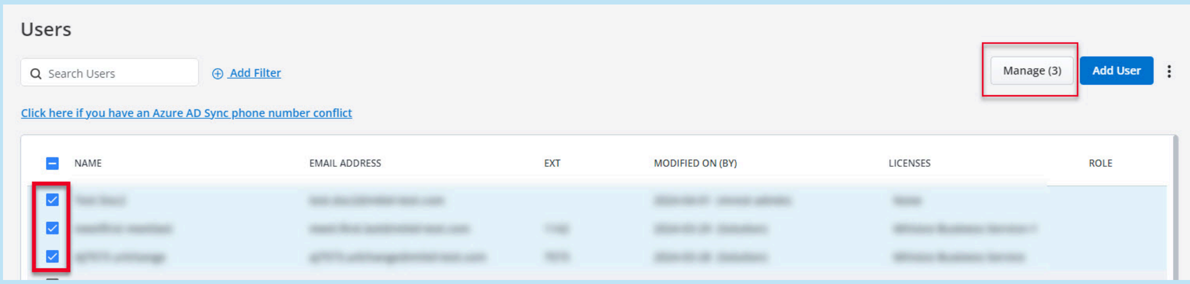
Send MiVoice Business deployment emails

When MiVoice Business Services is applied to a user account (either automatically to existing users or when new users are created), Users for the Customer Account are sent two " **Welcome to MiVB**" emails. These are called MiVoice Business Service **Deployment Emails**. The Administrator determines when the emails are sent by selecting user(s) or sending emails to all users with MiVoice Business Service enabled.

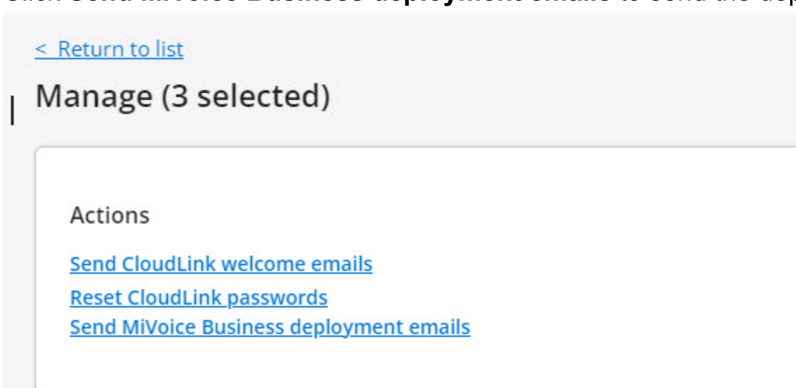
As a Account admin you can send MiVoice Business deployment emails to one or more users, do the following:

1. Log into the **Mitel Administration** as an **Account Admin**.
2. Click and expand **User Management** from the left navigation menu.

3. Click **Users**. The Users page opens.
4. Select the user(s) from the **Users** list. Click **Manage (x)**.

> **Note**:
>
> If you are selecting specific users, the **Manage (x)** option will reflect the number of users chosen.
>
> 
>

5. Click **Send MiVoice Business deployment emails** to send the deployment email the selected users.



6. Click **Close**. The selected end user(s) are sent two "**Welcome to MiVB**" emails with deployment and password details.

> **Note**:
> The first email contains User Portal details, Phone details and MiCollab Client details (if applicable). The second email contains passwords/phone pin.

Note:

MiVoice Business deployment emails will not be sent to users with voicemail enabled when the Open Integration Gateway (OIG) is a Network Element in the customer deployment along with MiCollab for Mitel Administration.

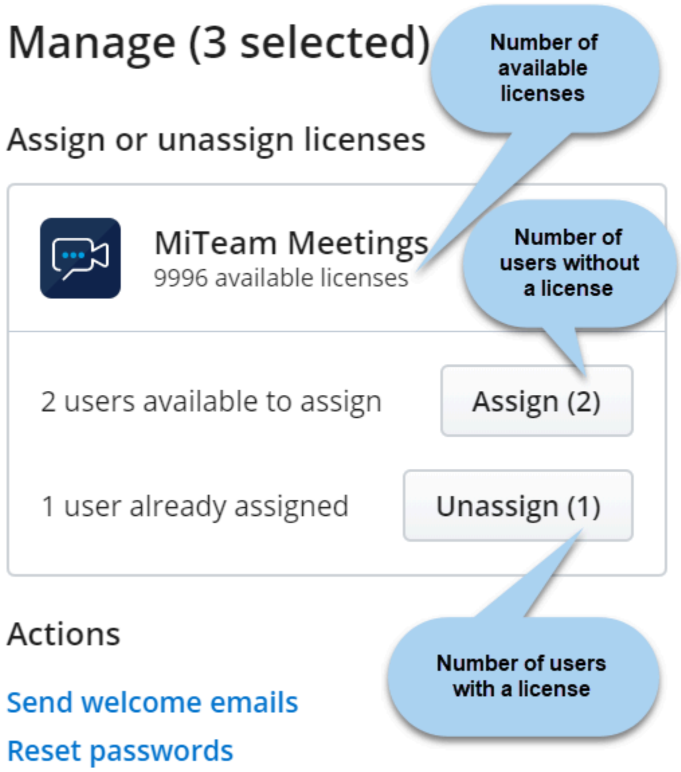
To prevent this issue, ensure that the OIG is not included in the deployment cluster for customers who use Mitel Administration for user provisioning of MiVoice Business Solutions.

Manage MiTeam Meetings License

Clicking the **Manage** option in the **Users** page of a customer account opens a panel that displays the number of MiTeam Meetings licenses available for that account and options, to assign MiTeam Meetings license to users, to unassign MiTeam Meetings license of existing users, to send welcome emails to all users, and reset the password of users.

Note:
MiTeam Meetings licenses details will be displayed only if:

- the account has MiTeam Meetings integration turned on and MiCollab integration turned off.
- the account has at least one MiTeam Meetings subscription/order assigned to it.
- the account is not a Partner Account.



- To assign MiTeam Meetings license to all the users in the customer account at once, click the **Manage** option, and click **Assign all** from the panel that opens.
- To unassign MiTeam Meetings license of all the users in the customer account at once, click the **Manage** option, and click **Unassign all** from the panel that opens.
- To assign MiTeam Meetings license to selected users, select the users from the **Users** page, click the **Manage** option, and click **Assign** from the panel that opens.
- To unassign MiTeam Meetings license to selected users, select the users from the **Users** page, click the **Manage** option, and click **Unassign** from the panel that opens.

Note:
If licenses are not available for assigning to users, the message **X (number of licenses required) more license(s) are needed to apply to the selected users. Please purchase more or unassign existing licenses and try again** is displayed.

Bulk User Settings

To assign SMS Numbers to a selected number of users in bulk do the following:

1. From the **Users** page, select the check boxes associated with the users you want to assign SMS Numbers.
2. Click **Manage (x)**. The Manage page is displayed.

3. In the **Bulk User Settings** panel, click next to Twilio SMS Numbers. The Assign SMS Numbers pop-up window is displayed.
4. Click the **Overwrite SMS numbers for selected users** drop down menu and select **Assign all.**

   If you want to unassign all SMS numbers to the selected users, click **Unassign all.**
5. Click **Save**.

   If the number of users is more than the available SMS numbers, then an error message is displayed and the Assign all option is not available.

Delete User

To delete an active or inactive user(s), do either of the following:

- From the **Users** list page:
  - Select the check box associated with the user(s) whom you want to delete, and click the icon.
  - From the panel that opens, click **Delete users**. **Delete Selected User(s)?** dialog box is displayed.
  - Type the word **delete**, and click **Delete**.
- From the User details page:
  - Select the user from the **Users** page and scroll down to the bottom of the page.
  - Click **Delete**. **Delete User** dialog box is displayed.
  - Type the word **delete**, and click **Delete**.

The user will be deleted.

Note:

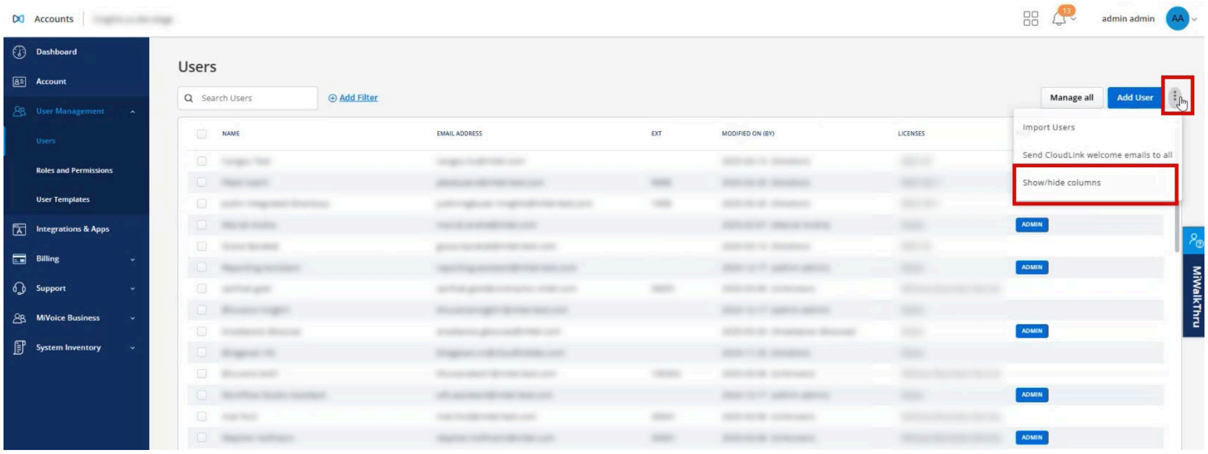
- You cannot delete a Mitel Partner, or a user synced from MiCloud Connect.
- Deleting a user synced from a PBX will only remove the CloudLink account of the user and will not delete the user from the PBX. After deletion, the user will continue to be listed in the **Users** page of Mitel Administration. To add a CloudLink account to the user again, the Account Admin must send a welcome email to the user.
- Deleting the SCIM users synced from Azure Active Directory will only remove the CloudLink account of the user and will not delete the user from Azure Active Directory.

Show/hide Contact Center Column

The **Show/hide Contact Center Column** option allows authorized users to toggle the visibility of the Contact Center column. This column displays the Contact Center modalities each user is configured for in Mitel CX.

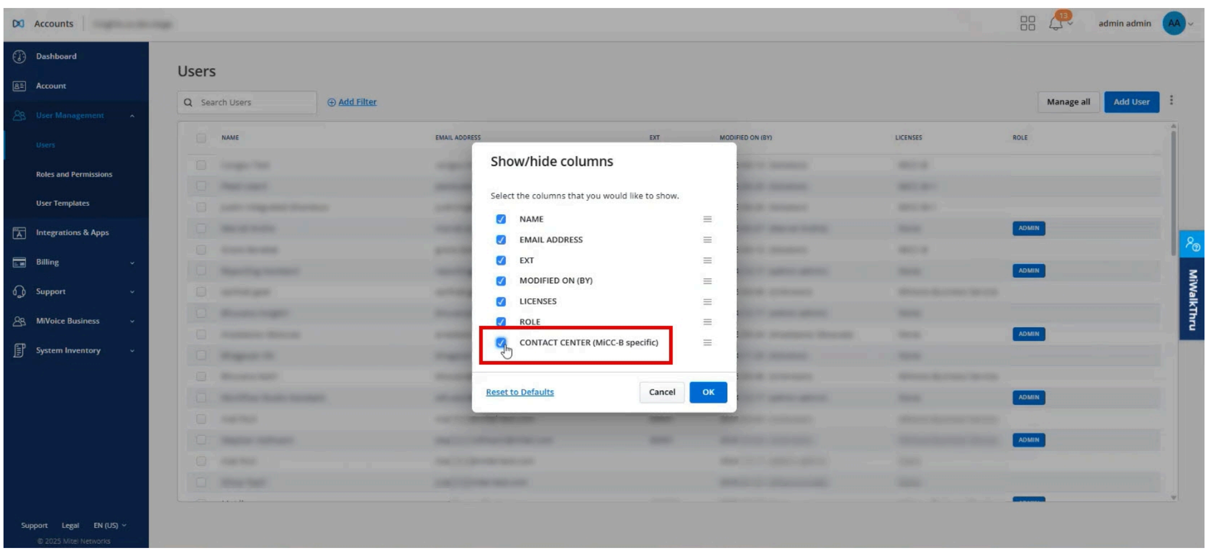
Note:
The Partner Admin, Customer Admin, or user with their email address listed in the Mitel CX can show or hide the Contact Center column.

1. Click the three vertical dots in the top right corner.



2. Select **Show/hide columns** from the options menu.

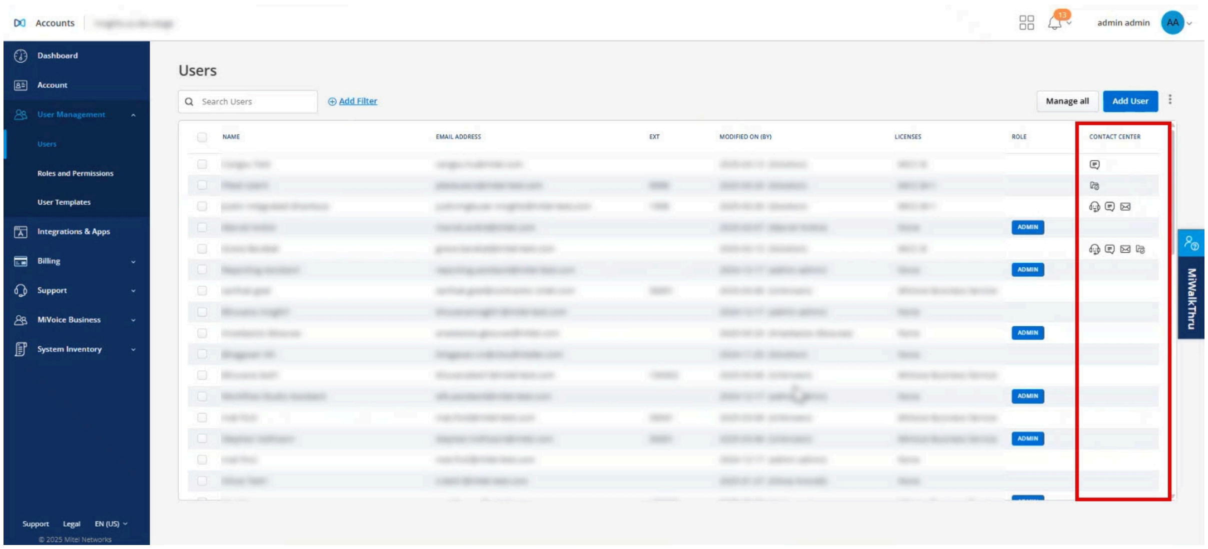
   The **Show/hide columns** pop-up displays.



3. Enable the **Contact Center (Mitel CX specific)** checkbox to show the Contact Center column, or disable it to hide the column.

4. Click **OK**.

The **Contact Center** column is displayed to view the contact center modalities each user is configured for in Mitel CX.



2.5 User Roles and Privileges

Mitel Administration assigns a role to each user when they are added to Mitel Administration. The user's role determines the privileges that are granted to the user. See Roles and Permissions on page 54 for details on how to create Partner, Admin, and User roles; and modifying permissions.

The following user roles and permissions are supported:

Partner

This role is assigned to the Mitel Partner who logs in to Mitel Administration using Mitel MiAccess. After logging in, a Mitel Partner can create, edit, deactivate, or delete customer accounts; add, edit, and delete users; and enable or disable administrative rights for users.

Account Admin

This role is assigned to a user by a Mitel Partner or by an Account Admin. After logging in to a customer account, a user having this role can add, edit, or delete users (including other Account Admins); and enable or disable administrative rights for users in that account.

User

This is the basic user role in Mitel Administration. User privileges for this role are restricted to resetting their login passwords.

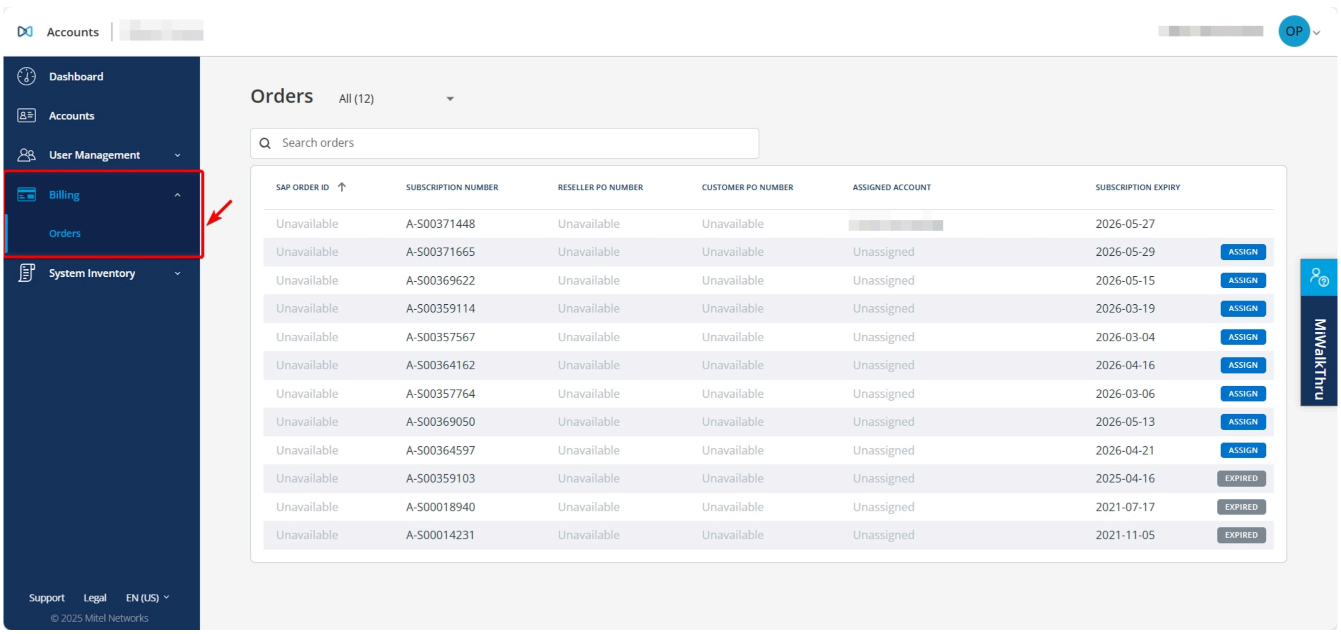
Custom

These roles (Partner and Account Admin) are created and assigned by the Partner. Once a custom role is assigned to an account, it can be assigned to any user within that account. For more information, see Roles and Permissions.

2.6 Orders

The **Orders** page displays the subscriptions purchased by a Mitel Partner. When a Partner purchases a subscription it is automatically listed in this page as an Order. Partners can use the Orders page to view, search, and assign orders to customer accounts. They can also view the details such as the tracking number, the assigned account, the purchase date, and the expiration date.

Navigating to Orders

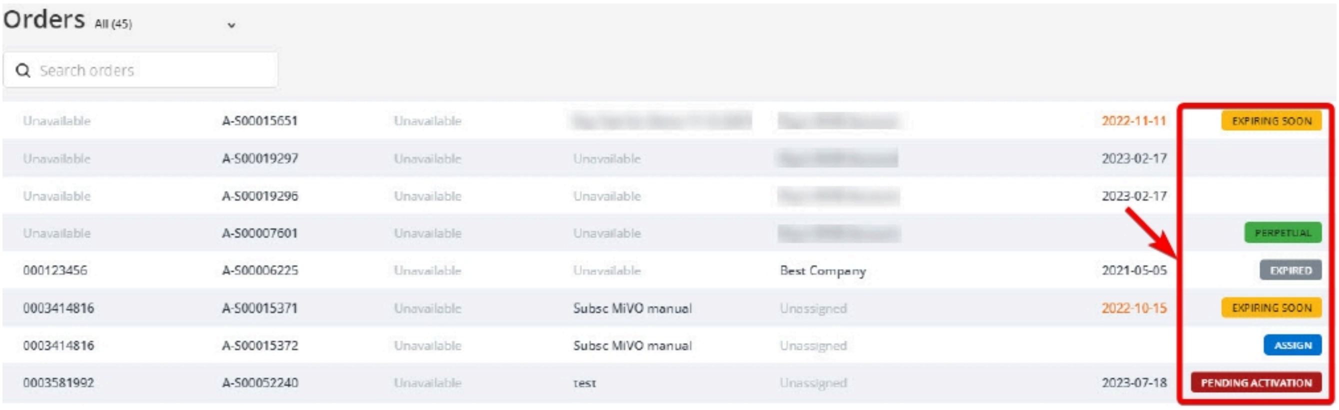


To access the Orders page:

1. Select **Billing** from the navigation menu on the left side of the **Accounts Console Dashboard**.
2. Then select **Orders**.

Understanding Order Statuses

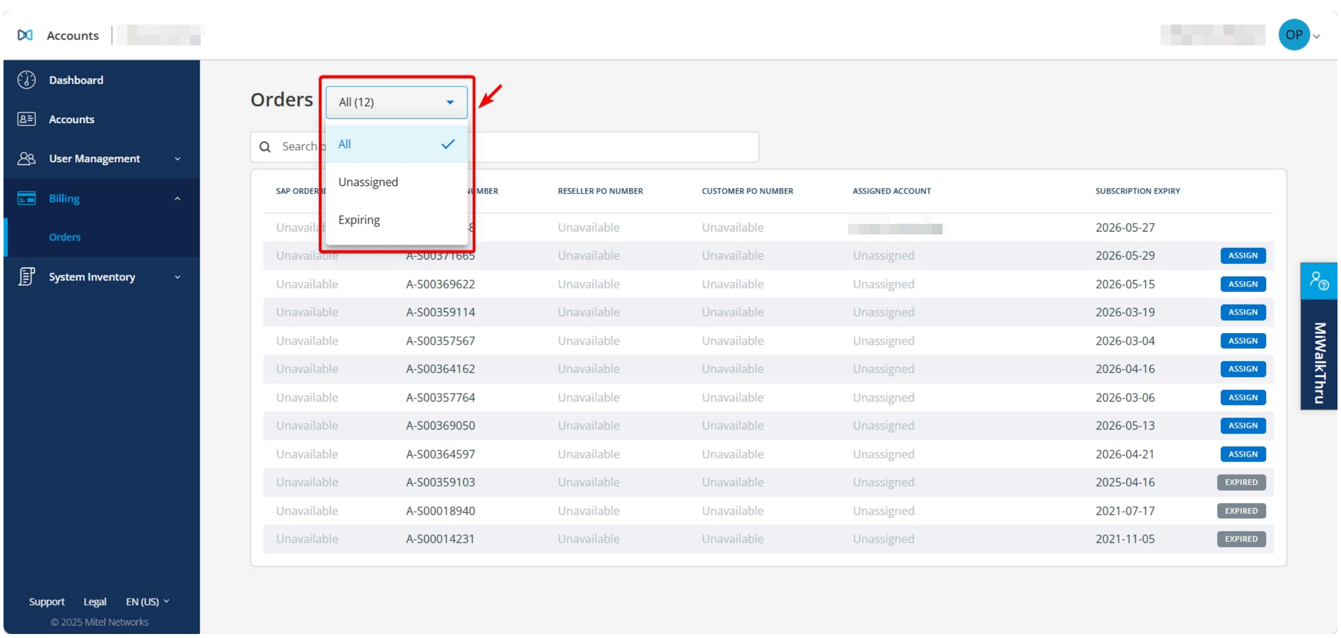
The **order status** shows the current state of an order. You can view the status of each order on the **Orders** page.



The following are the available order statuses:

- **ASSIGN** – Indicates that the order must be assigned to a customer account.
- **EXPIRING SOON** – Indicates that the order will expire soon and should be assigned to an account promptly.
- **EXPIRED** – Indicates that the order has expired and can no longer be assigned to an account.
- **PERPETUAL** – Indicates that the order is perpetual and does not expire.
- **PENDING ACTIVATION** – Indicates that the order is in a pending state and has not yet been activated.

Filtering Orders by Status



To filter the list of orders based on their status:

1. Select the drop-down available next to **Orders**.

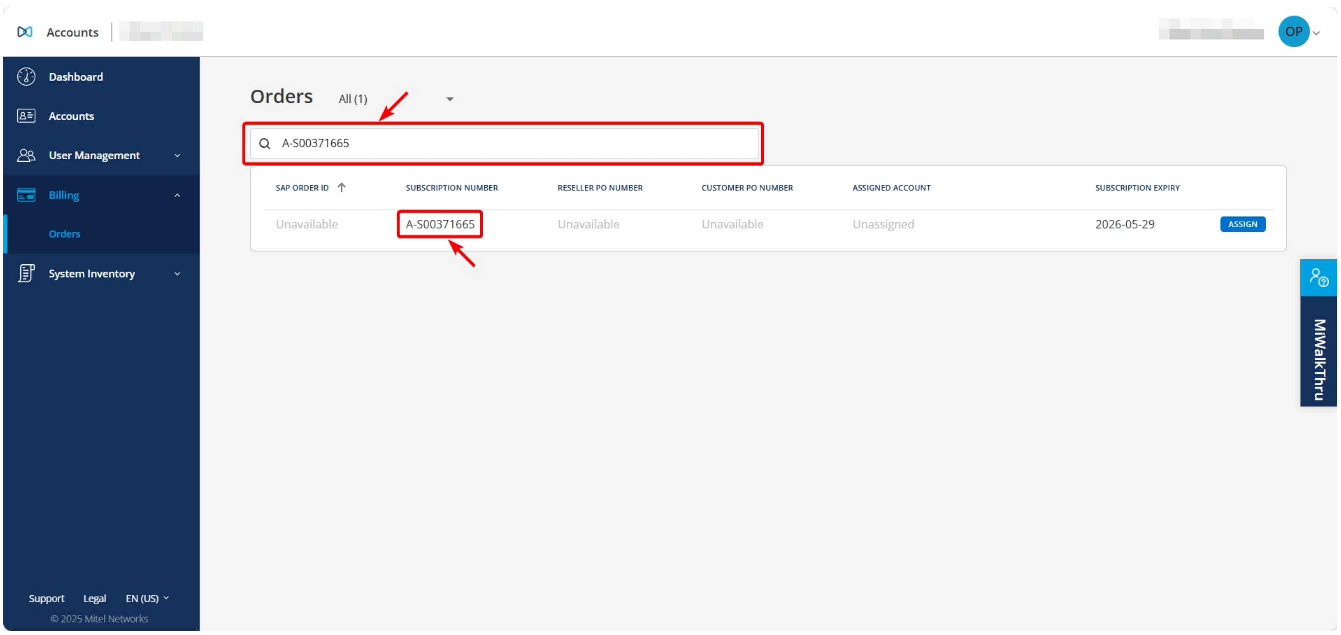
2. In the drop-down list, choose one of the following:
   - **All** – to view all orders.
   - **Unassigned** – to view only unassigned orders.
   - **Expiring** – to view orders that are nearing expiration.

The **Orders** page updates to display only the orders that match the selected status.

Search for Orders

Use the **Search orders** bar to find an order by entering one of the following:

- SAP order ID
- Reseller PO number
- Customer PO number
- Assigned account
- Tracking number
- Expiry date of the order (Subscription Expiry)

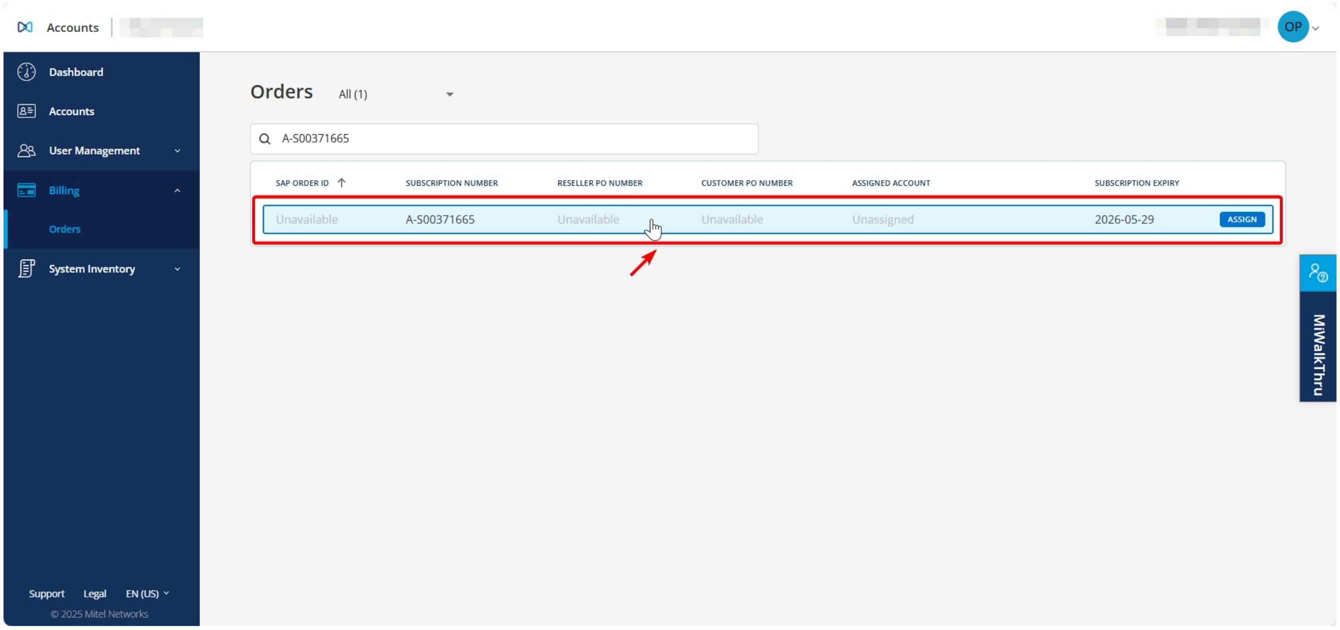


As you type, the **Orders** page displays a list of matching results.

Assigning an Unassigned Order

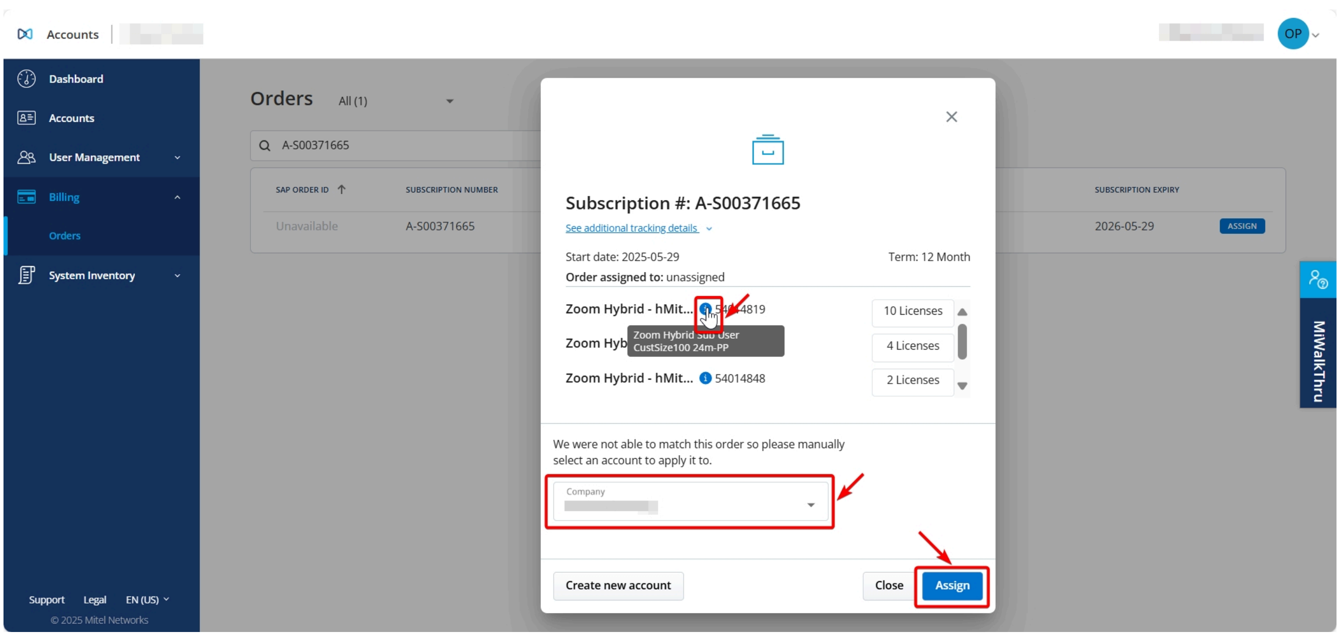
To assign an order to an account:

1. On the **Orders** page, find the order you want to assign.



2. Click the respective subscription.

   A pop-up appears with the subscription details.

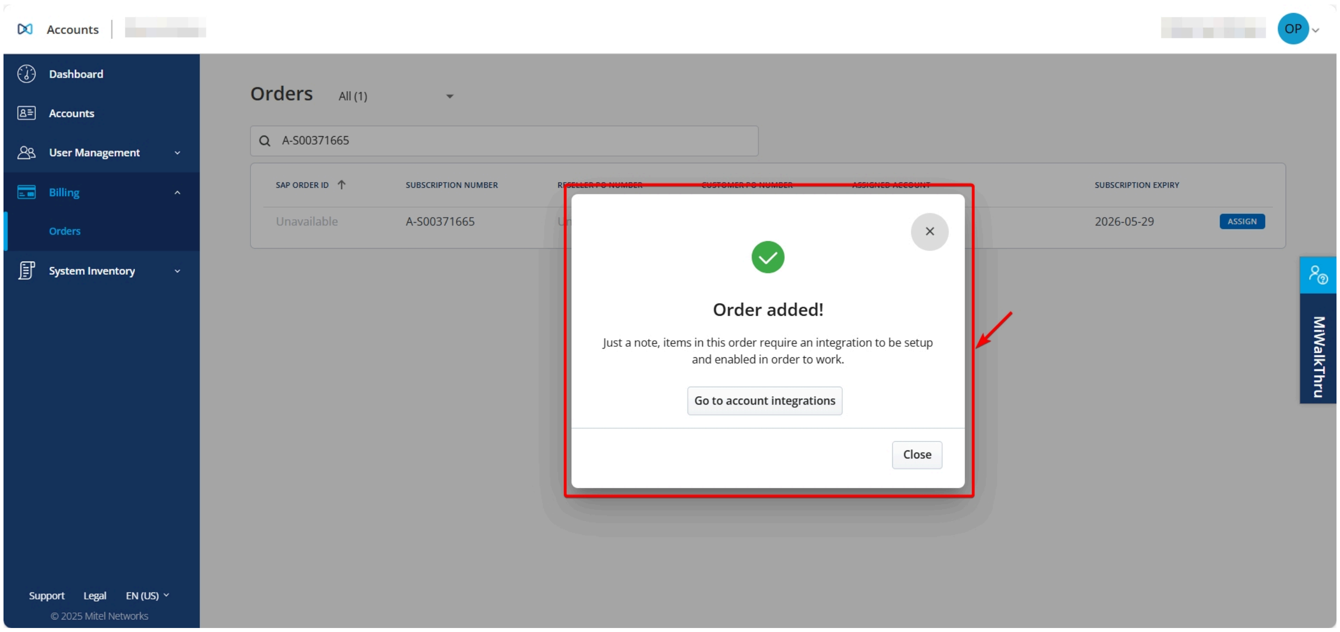


Note:
Hover over the **info** icon to view plan details.

3. Click **Company**.

4. In the drop-down list, use the **Search** field to enter the name of the account.
5. As you type, matching account names appear in the list.
6. Select the correct account.
7. Click **Assign** to complete the process.

   A dialog box appears with a success message.



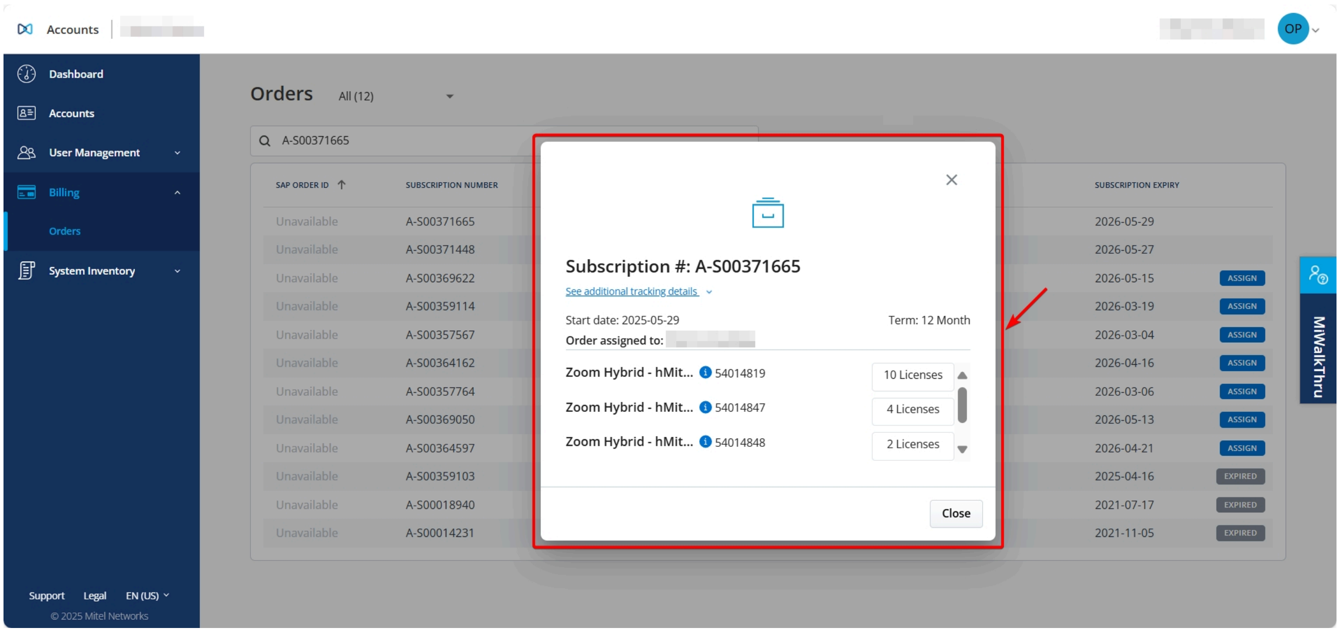
8. Click **Go to account integrations** to navigate to the **Account Information** section in the **Accounts** module.

Viewing Order Details

To view the details of an order:

1. Click the respective order.

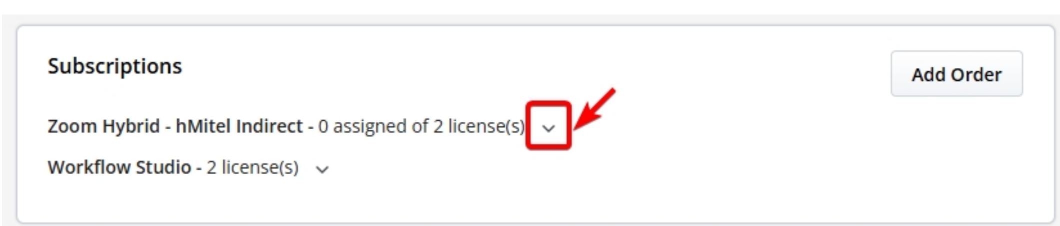
   A dialog box appears with the order details.



2. Review the following information in the panel:
   - Subscription number
   - Start date
   - Assigned account
   - Term
   - Subscription details
   - Number of licenses
3. Click **See additional tracking details** to view more tracking information, if needed.
4. Click **Close** to exit the dialog box.

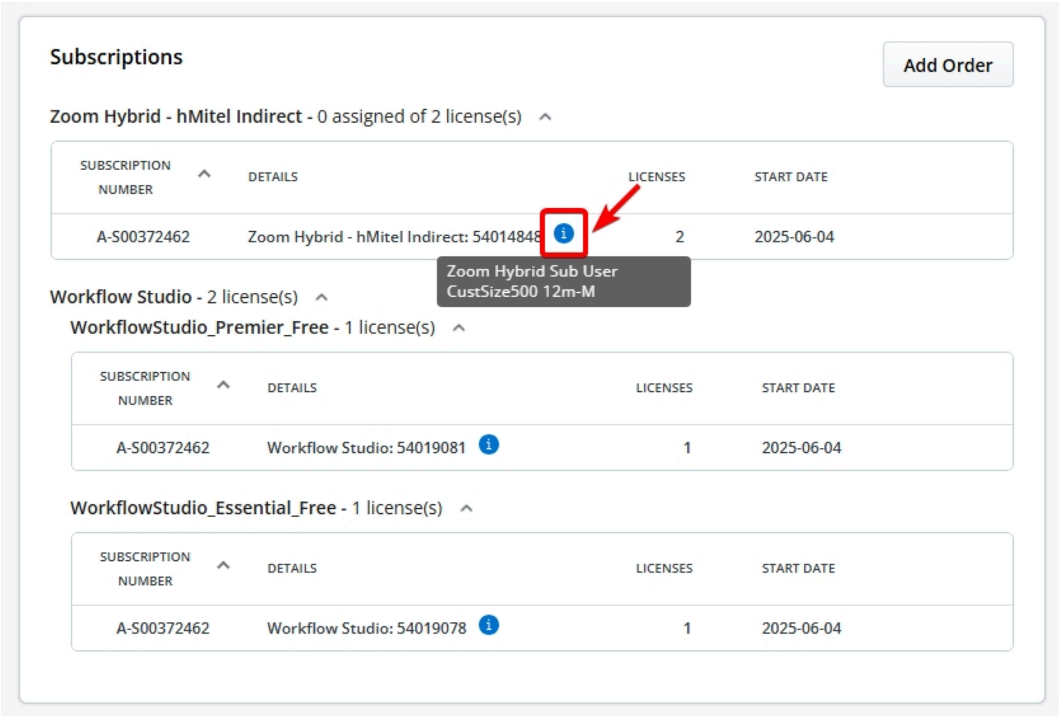
2.7 Subscriptions

The **Subscriptions** panel displays a list of all **CloudLink** application licenses assigned to a customer account.



In the **Subscription** panel, click ⌄ to view the subscription number, subscription details, remaining number of licenses available for the account, and the start date of the subscription.

Note:
Hover over the **info** icon to view plan details.

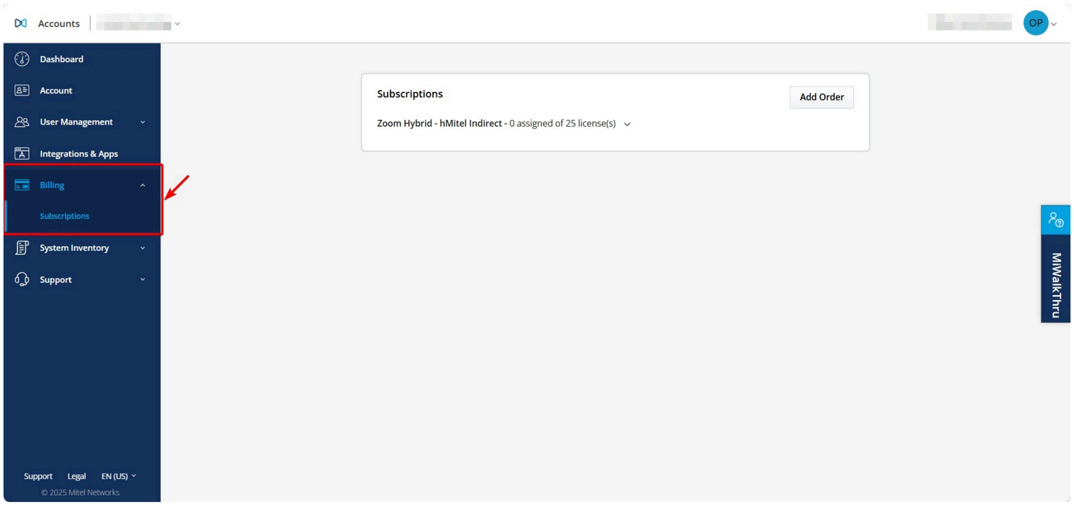


Note:

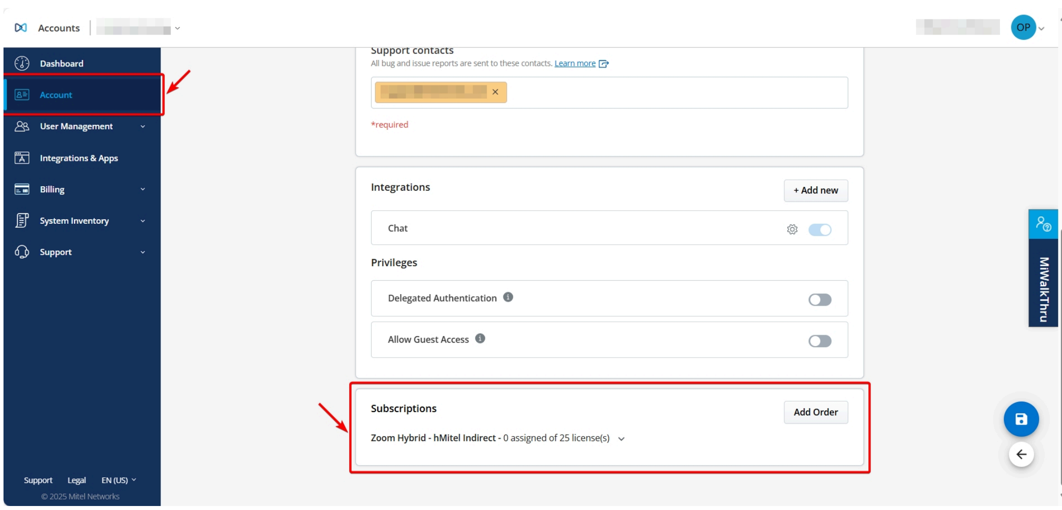
- The **Subscriptions** panel is not available for Prime Partner accounts.
- The **Subscriptions** panel is not available for a Partner who does not have a billing account.

A Mitel Partner or a Customer Account Admin can access the **Subscriptions** panel by doing either of the following ways:

- In the Mitel Administration portal, select**Billing** from the left navigation menu, then select**Subscriptions** to open the Subscriptions panel.



- In the Mitel Administration portal, select**Account** from the left navigation menu. Scroll to the bottom of the page to view the **Subscriptions** section..



Add Order

Note:
This option is available only to Mitel Partners with a billing account.

The **Add Order** option in the **Subscriptions** panel of a customer account allows a Mitel Partner to add an order directly from the panel.

To add an order to the current customer account:

1. In the **Subscriptions** panel, select **Add Order**

   The **Orders** page opens, showing a list of all unassigned orders.
2. Find the order you want to assign and select **Assign** next to it.

   A dialog box appears with the **Company** field pre-filled with the customer account name.
3. Select **Assign**.

   The order is assigned to the customer account, and you're redirected to the **Subscriptions** panel.

To add an order to a different customer account:

1. On the **Orders** page, select **Company**.

   A drop-down list appears with account names and a **Search** field.
2. In the **Search** field, enter the name of the customer account.

   Matching account names appear as you type.
3. Select the desired account and choose **Assign**.

   The order is assigned to the selected customer account.

> **Note**:
> You remain on the **Orders** page and are not redirected to the **Subscriptions** panel.

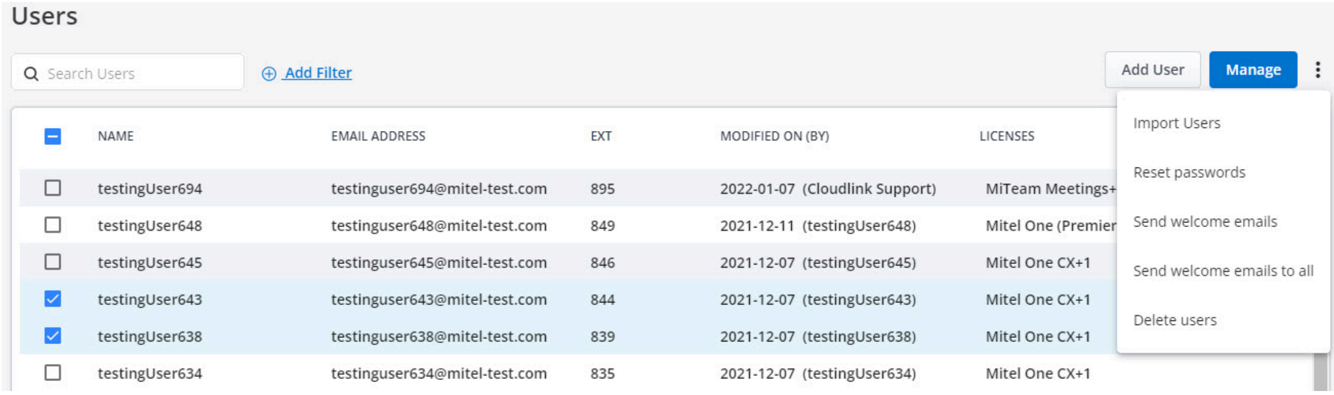
2.8 Bulk Import of Users

A Mitel Partner or a Account Admin can add users in bulk to a customer account in the Mitel Administration by using the bulk import feature. This removes the need for a Partner or Account Admin to add users into the portal one at a time. They only need to enter the details of each user in the spreadsheet template provided, and with the click of a button these users will be added to the customer account.

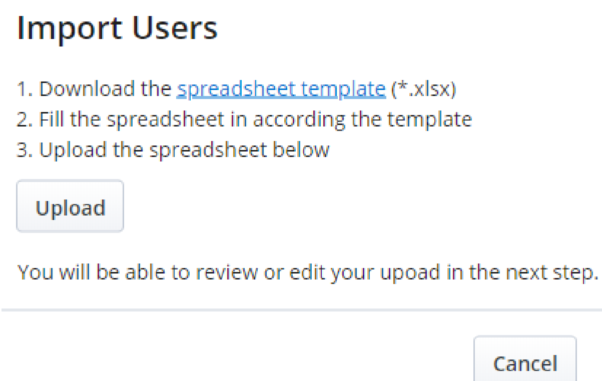
To add users in bulk to a customer admin account, do the following:

1. Expand User Management from the left navigation menu, click **Users**.

2. Click ⋮ icon. And click **Import Users**, the **Import Users** panel opens.



3. Click the **spreadsheet template** hyperlink. See Spreadsheet Template for details to fill the spreadsheet.



4. Save the spreadsheet after updating and return to the Mitel Administration.
5. If the **Import Users** pop-up is still open, click **Upload**. Else,
6. Return to the **Users** page of the customer account, click **Upload** from the **Import Users** panel.

Spreadsheet Template

A spreadsheet containing the fields in which user details must be entered is downloaded to the default download location of your system. Using Microsoft Excel, enter the user details in the relevant fields of the spreadsheet.

A spreadsheet containing the fields in which user details must be entered is downloaded to the default download location of your system. Using Microsoft Excel, enter the user details in the relevant fields of the spreadsheet.

The spreadsheet contains the fields **FIRST NAME**, **LAST NAME**, **NAME**, **EMAIL**, and **ROLE**.

- You must enter the details in at least one of the fields among **FIRST NAME**, **LAST NAME**, and **NAME**.
- You must enter a valid email address for the user in the **EMAIL** field. Ensure to not enter:
  - an email address already assigned to an existing user in the customer account
  - the same email address for different users in the spreadsheet
- You must enter a user role for the user in the **ROLE** field. The available user roles are **User** and **Account Admin**. If you do not enter a user role, the default role **User** is assigned to that user.
- Save the spreadsheet.

Return to the **Users** page of the customer account, and click **Upload** from the **Import Users** panel. A window opens. Navigate to the location where the spreadsheet is saved, select the spreadsheet, and click Open. A Preview window opens.

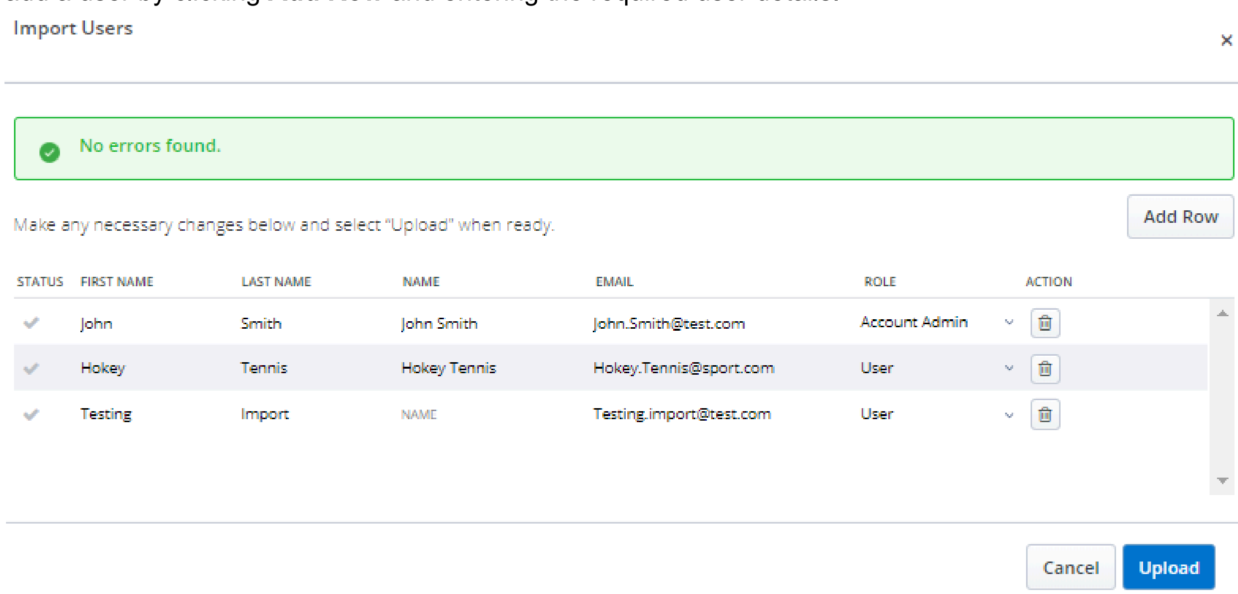
The Preview window summarizes the user details you entered. The **STATUS** column for a user will show an error icon ( ) if there is an error in the details you entered. You can proceed to add users to the customer account by clicking the **Upload** button. However, if you proceed to add users when the STATUS shows the error icon:

- The users without errors in the user details are added to the customer account and will be removed from the Preview window.
- The users with errors in the user details will not be added to the customer account. They will continue to remain in the Preview window until you make the required corrections and add them to the customer account or delete them.

Click the fields that have errors and make the required corrections. If there are no errors in the user details, a label at the top of the Preview window displays **No errors found**.

In the Preview window, you can also:

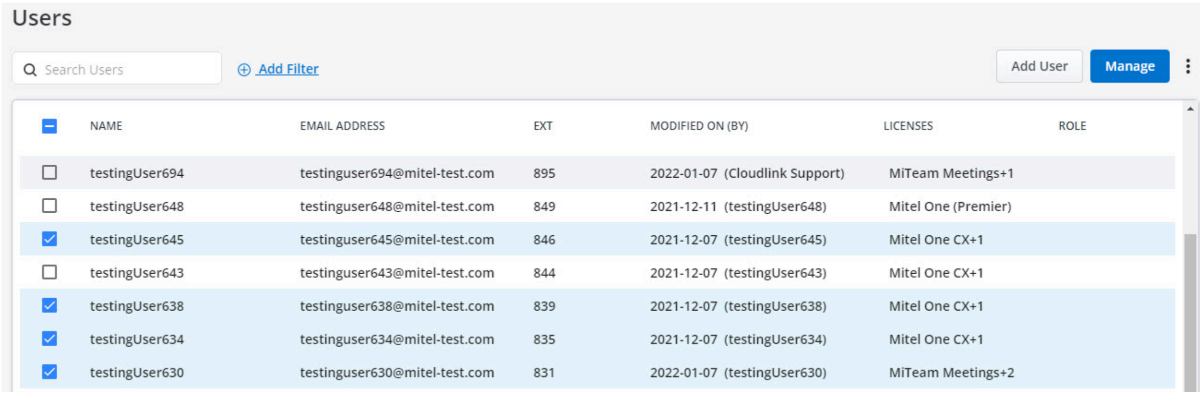
- change the user role by clicking the down-arrow beside the user role and selecting a user-role from the from the drop-down
- delete a user by clicking the icon
- add a user by clicking **Add Row** and entering the required user details.



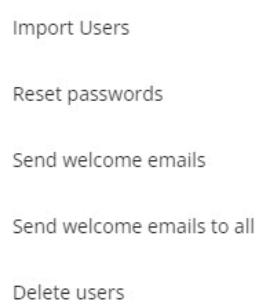
After making all the necessary corrections and modifications, click **Upload** to add the users to the Accounts Console. The users will now be listed in the **Users** page of the Accounts Console. If you click **Cancel** the bulk import operation is canceled.

After you add users in bulk to a customer account, you must send Welcome emails to these users to register and log in to the various CloudLink applications. To send the Welcome email, do the following:

1. In the **Users** page, select the check box associated with the user(s) to whom you want to send the Welcome email.



2. Click the ⋮ icon and from the panel that opens, click **Send welcome emails**.



A Welcome email is sent to the selected users.

2.9 Support Contacts

The **Support Contacts** field of a customer account lists all the contacts added by a Partner user or an Administrative user of that account to which all issue reports pertaining to that account are sent. These contacts can be an existing Partner or any other e-mail address assigned to be a Support Contact for that account.

When a customer reports an issue with a CloudLink application, an email is sent to the Support Contacts. The **Support Contacts** are responsible for addressing the issues reported by their customers and when needed, contact Mitel Partner Technical Support via appropriate channels. Mitel will not reach out to the partner or the customer in regards to these reports. For more information, see CloudLink Applications Partner Support Process.

Adding or Editing a Support Contact (Partner User)

A Partner must add Support Contacts while creating an account. The contacts added can include Partner users and explicit email addresses.

Note:
It is mandatory to add at least one Support Contact while creating a new customer account.

To add Support Contacts to the account as a Partner user, use the following procedure:

- To add Partners as Support Contacts:

  1. Navigate to the **Account Information** page of the customer account.
  2. In the **Support Contacts** search field, type the name of the Partner you are searching for. The search field displays a list of Partners whose names or email addresses match the letters that you type.
  3. Click the name to add that Partner as a Support Contact. The name of the Partner is displayed in the **Support Contacts** list.
  4. Click **Save**. The selected Partners are set as Support Contacts for the account.

- To add explicit email addresses as Support Contacts:

  1. Navigate to the **Account Information** page of the customer account.
  2. In the **Support Contacts** search field, type the email address you want to assign as a Support Contact and press ENTER. If the email address you entered is valid, it is displayed as **Support Contacts**. If the email address you entered is not valid, the portal displays the message **Contains an invalid email**.
  3. Click **Save**. The selected email addresses are set as Support Contacts for the account.

A Partner user can also edit the Support Contacts for an existing account by using the following procedure:

1. Click **View Accounts** from the console dashboard. The **Accounts** page opens. Click the account you want to edit. The **Account Information** page for that account opens.
2. In the **Support contacts** field,
   - Click **X** against a Support Contact name or email address to delete that Support Contact.
   - Follow the same procedure as that for adding Support Contacts for a new account to add Support Contacts to the account.
3. Click **Save** to save the changes.

Editing a Support Contact (Administrator User)

An Administrator user can delete or add Support Contacts only for existing accounts, which are created by a Partner.

To edit the Support Contacts for an account as an administrative user, use the following procedure:

1. Click **View Account** from the console dashboard. The Account Information page opens.

2. The **Support contacts** field displays either the names or email addresses of all existing Support Contacts for that the account.
3. Click **X** against an email address to delete that Support Contact.
4. To add more Support Contacts for the account, enter a valid email address in the search bar. The search field displays a list of valid email addresses that match the letters you type.
5. Click the **Add** button beside an email address to add that email address as that of a Support Contact. The email address is displayed in the **Support Contacts**.
6. Click the  icon to save the changes.

2.10 Support Logs

The **Support Logs** page of a customer account enables the Mitel Partner or an Account Admin to view or edit the support logs in the customer account. Support logs are created when a user in the customer account reports an issue with a CloudLink application. The Mitel Partner or an Account Admin can click a support log to view or edit the details of that log.

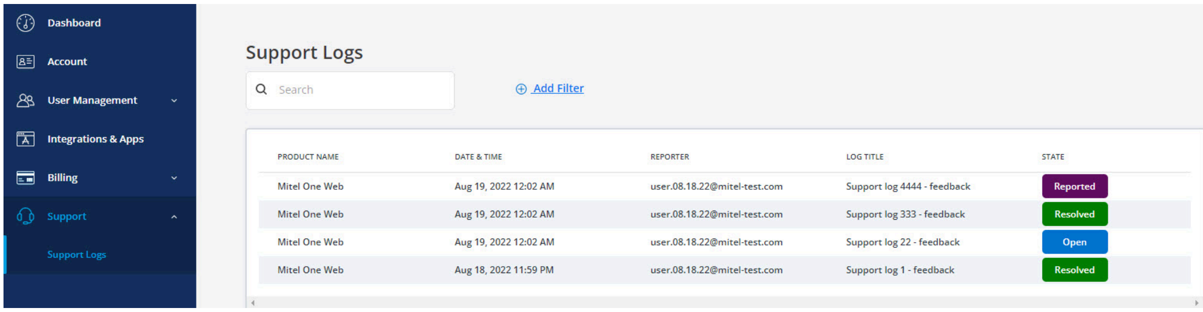
To view the **Support Logs** page, use the following procedure:

1. Log in to the Mitel Administration on page 1.
2. Access the **Support Logs** panel by doing either of the following:
   - If you have logged in as a Mitel Partner:

     On the left panel, click **Accounts** and select the account for which you want to view the logs. The **Account Information** page is displayed. From the left panel click **Support** and then click **Support Logs**.
   - If you have logged in as an Account Admin:

     On the left panel, click **Support** and then click **Support Logs**.

The **Support Logs** page for the selected account opens displaying a list of logs.



Click the log that you want view from the list of logs.

Search for Logs

You can search for logs based on log titles. In the **Search** bar, type the **LOG TITLE** as the search criteria. A list of matching logs will be displayed.

> **Note**:
> You cannot search for logs based on a **PRODUCT NAME**, **DATE & TIME** or **REPORTER**.

Add Filter

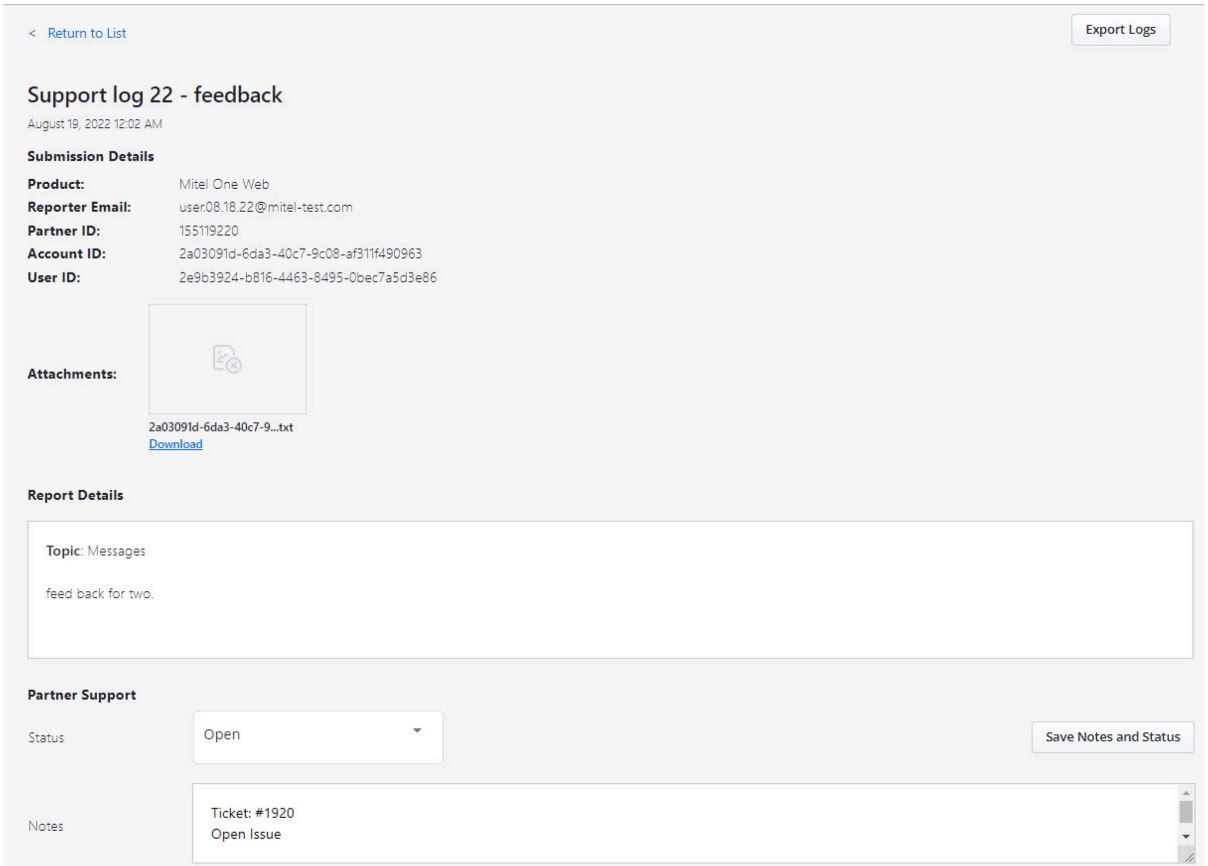
By default, the **Support Logs** page displays all logs for all applications. You can filter the list of logs by application and by state of logs. To do this, click **Add Filter** and select **Product** or **State** to add the corresponding filter.

The list of products displayed after selecting the **Product** filter, shows all the application issues created in the past 60 days.

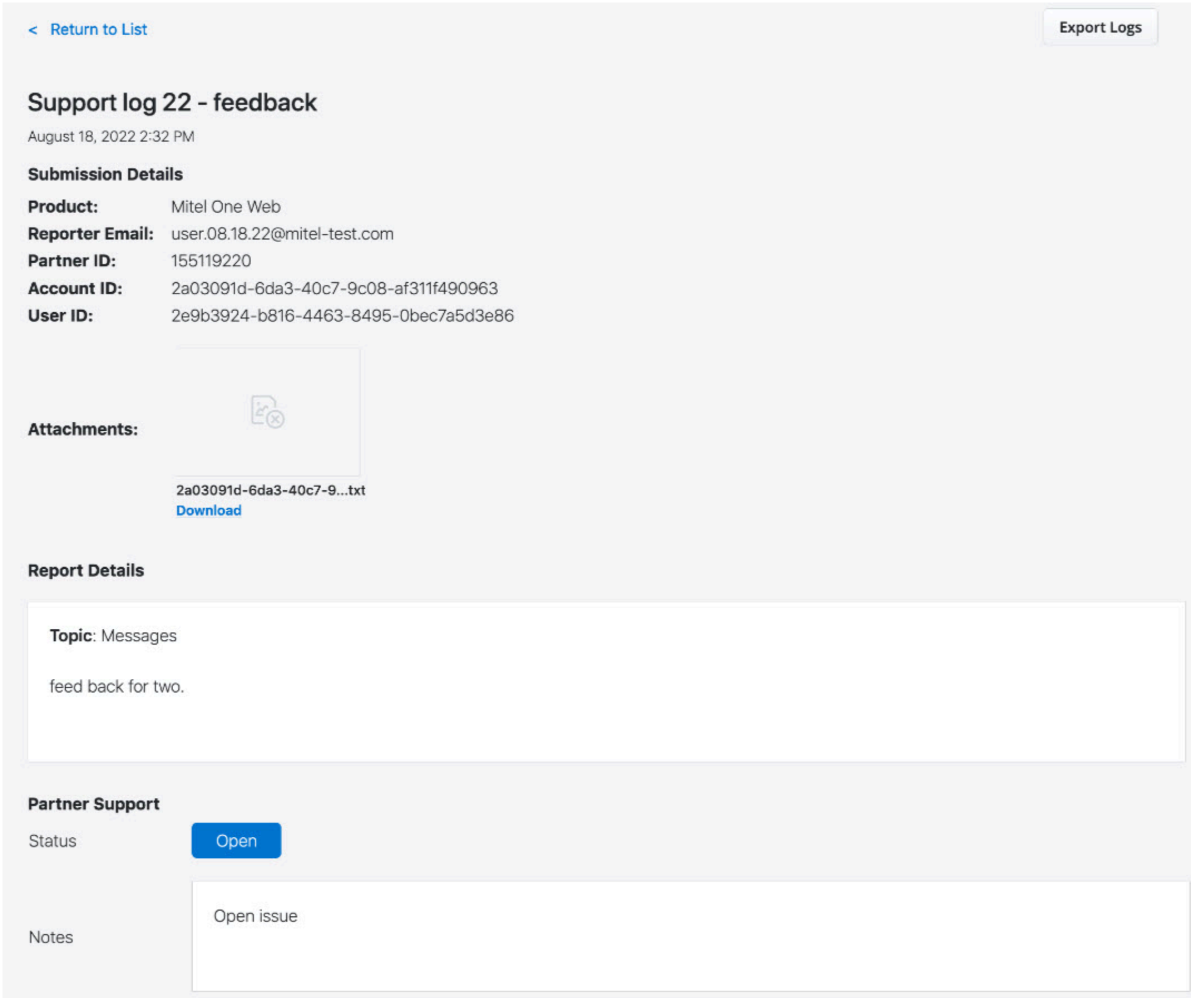
View a Log

Click the log that you want to view from the list of logs displayed in the **Support Logs** page. The log details page opens, displaying details of the log. If the customer has attached an image along with the description, the image will be displayed under **Attachment Details**. The following images show examples of the log details page:

- If you have logged in as Mitel Partner



- If you have logged in as Account Admin



To download a log file and its attachments, click **Export Logs** at the top of the page. The log and the attachments are downloaded as a zip file. Unzip the file to view the text file.

Note:

- For Mitel One Mobile logs, if you click **Export Logs** two zip files are downloaded. The zip file with the suffix logs-XXXXX contains one text file and the report.zip file contains the report in HTML format.
- If the **Log Level** is set to debug, the report.zip file will contain a SIP logs folder and a .txt file.

The **Report Details** box contains a description of the issue written by the customer. For Mitel One Mobile logs, the **Report Details** section displays the following tabs:

- **Report Details**
- **User Details**
- **Device and Apps**
- **Filtered Signal Strength Logs**

> **Note**:
> **Filtered Signal Strength Logs** tab is displayed only for android devices.

- **Error Information**

For Mitel One Web logs, the **Report Details** section displays the following tabs:

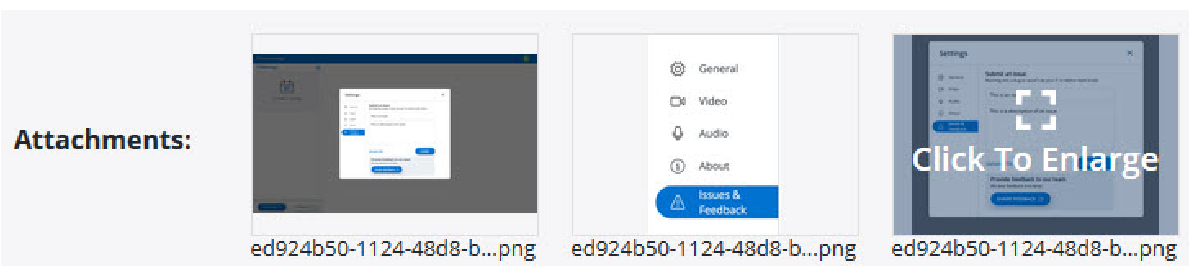
- **Report Details**
- **User Details**
- **Error Information**

Click each tab to view details about the logs of each category.

View Attachment

If the customer has attached an image along with the description, the image will be displayed under

Attachments. To enlarge the image hover over the image and click **Click To Enlarge**. Click the X icon to close the image.



To download an attachment, click **Download**. The attachment will be saved in your system.

Log Status

The log status is helpful for a Mitel Partner in identifying the metrics of logs based on their status. The **Partner Support** section in the Support Logs page displays the status of the logs along with notes.

Following are the three states of logs:

- **Open**: A new issue is created by a CloudLink Application user through the customer account. When the issue is in the open state, a periodic reminder email is sent to the support contact of the partner by CloudLink. The reminder email is to alert that the customer may still be experiencing the issue.
- **Reported**: The issue is reported and is being worked on.

- **Resolved**: The issue is resolved.

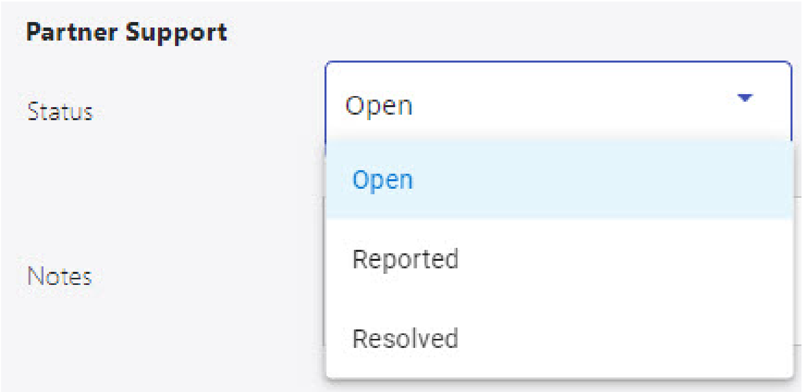
Note:
After the Mitel Partner resolves an issue, the status of the issue must be updated from Open to Resolved. It is only when the Mitel Partner is not able to resolve the issue and has escalated the issue to Mitel that the Reported status is used. Once the issue is resolved by Mitel, the Mitel Partner must update the status from Reported to Resolved.

If you have logged in as a Mitel Partner, you can:

- View the log status.
- Change the status of the log.

Perform the following steps to change the status of the log:

1. From the **Status** drop-down list, select the status as **Open**, **Reported**, or **Resolved**.



2. You can add a note about the log such as ticket ID or the status of the log.
3. Click **Save Notes and Status** to save the changes.

If you have logged in as an Account Admin, you can view the log status along with the notes but cannot change the status of the logs.

Zoom (Support)

The Zoom sub-module within the Support module enables users to support Zoom integrations. It provides the following functionalities:

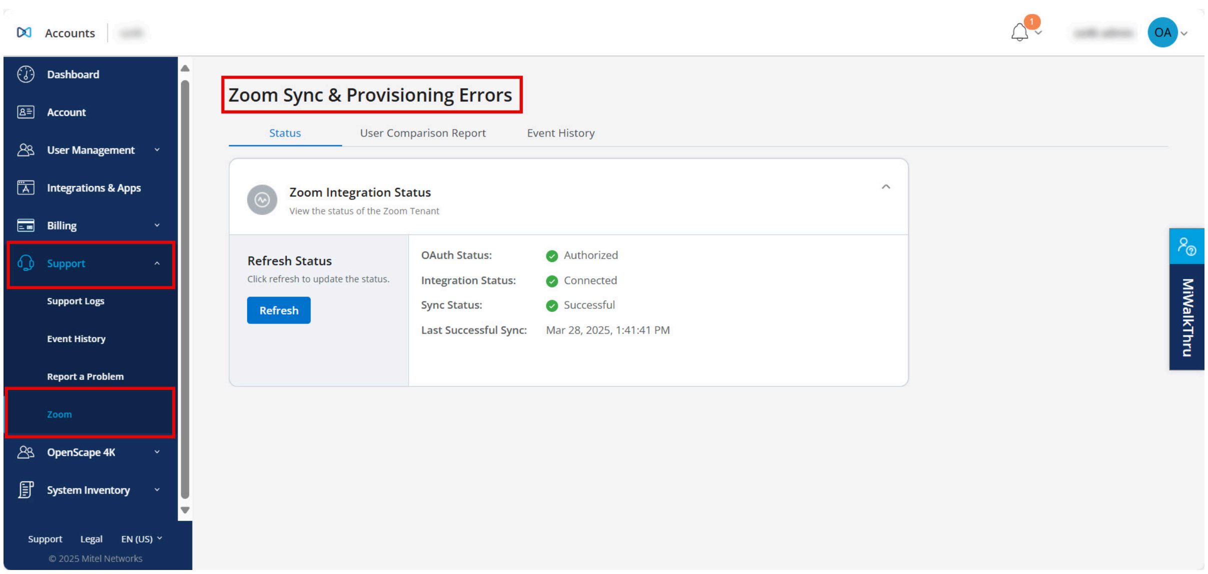
- View the status of the Zoom Integration, including OAuth Status, Integration Status, Sync Status, and Last Successful Sync.
- Refresh the status of the Zoom Integration.
- Generate and download the User Comparison Report.
- View event history.

This sub-module ensures efficient supporting and troubleshooting of Zoom services and integrations.

> **Note**:
>
> The Zoom sub-module is displayed only if the account's Zoom Integration has been properly configured with CloudLink.

Navigating to the Zoom sub-module

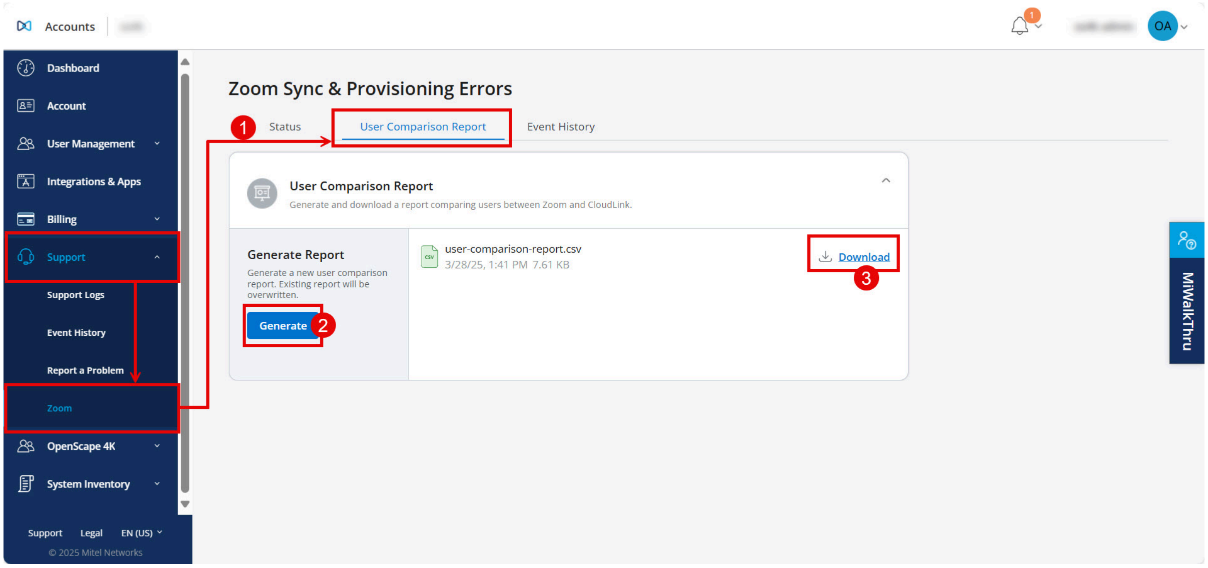
1. On the left panel, click **Support**, then click **Zoom**.
2. The **Zoom** related information's for the selected account will open, displaying the **Zoom Sync & Provisioning Errors** screen.



Generate and Download the User Comparison Report

The User Comparison Report for Zoom allows the generation and download of a comparison between Zoom and CloudLink users. This helps identify discrepancies, evaluate engagement, and manage user data across both platforms.

1. Go to **Support** > **Zoom** > **User Comparison Report** tab.



2. Click the **Generate** button.

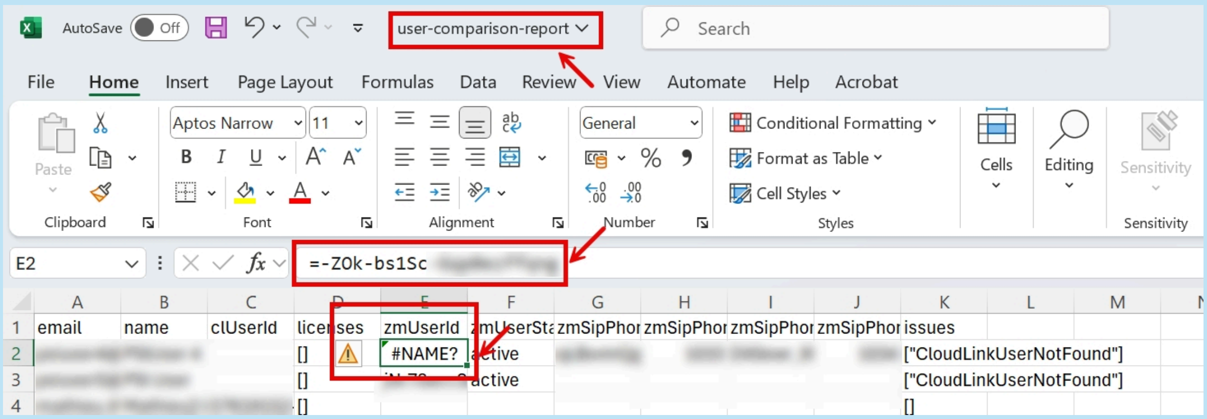
Note:
Generating a new **User Comparison Report** will overwrite the existing report. A success message will appear once the report is generated successfully.

3. Click the **Download** button.

A **user-comparison-report.csv** file will be downloaded to your local device.

Note:

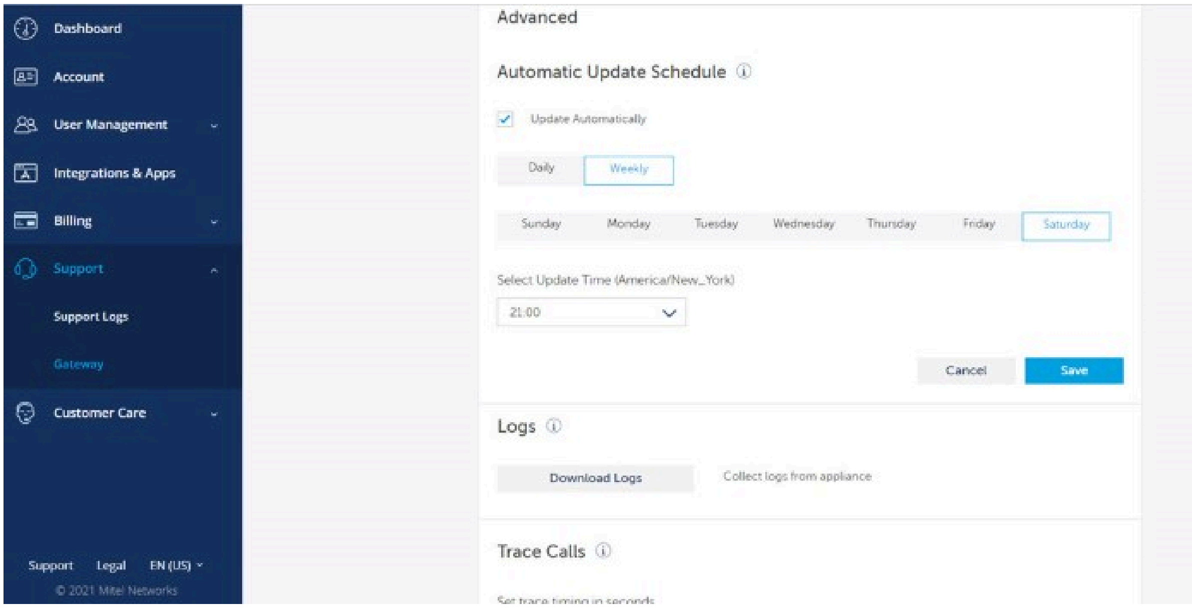
If the **user-comparison-report.csv** file contains Zoom User IDs starting with a dash (**e.g., -Abcd1234**), Microsoft Excel may display the User IDs incorrectly as **"#NAME?"** due to an invalid name error. To view the correct Zoom User ID, open the file in Excel and click on the formula bar.



2.11 Gateway

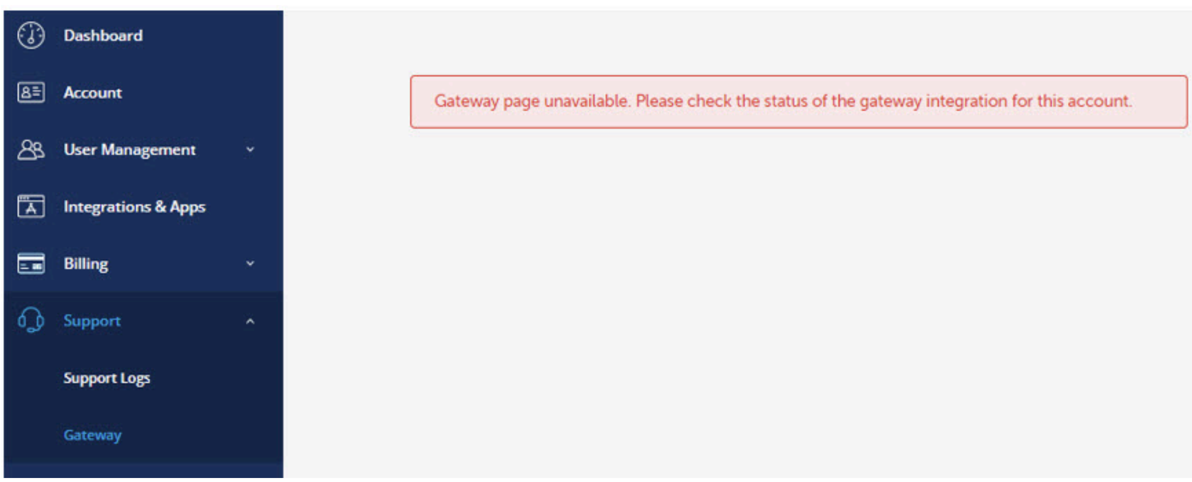
The **Gateway** support page is available for the Mitel Partner and for Account Administrators of customer accounts for which CloudLink Gateway is enabled. The **Gateway** support page provides quick access for the Mitel Partner or the Account Administrator to schedule gateway updates, review specific logs, trace calls, reboot the gateway, and update the system version.

If the CloudLink Gateway is down or not reachable, the **Gateway** support page is not accessible.



To access the **Gateway** support page, click the icon in the **Support** panel and then click **Gateway**. The partial **Advanced** page is displayed. This page enables selecting advanced settings and options that are useful for troubleshooting issues, especially when working with Mitel Support. For more information about configuring advanced settings and options, see Configuring Advanced Settings and Options.

In some cases, when trying to access this page, the following error message is displayed.



The error message is displayed if:

- the customer account has the CloudLink Gateway Integration added, but onboarding has not progressed beyond the **Gateway** step to connect a gateway to the account.
- there is a connection issue with the gateway of the customer account.

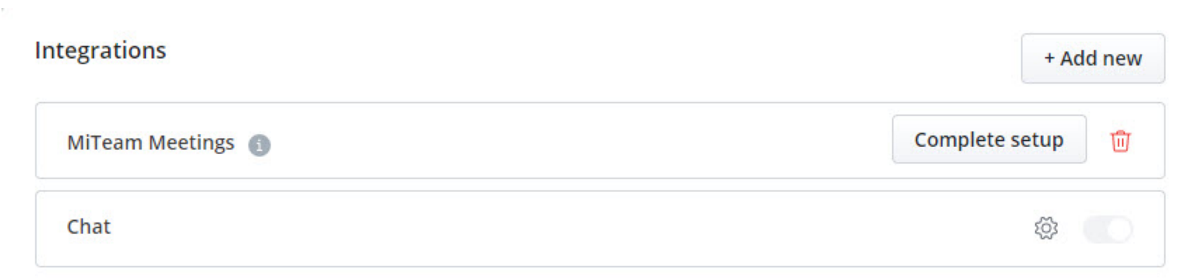
To resolve the status of the CloudLink Gateway Integration, navigate to **Integration & Apps** on the left navigation panel and investigate the issue.

For more information about troubleshooting errors see, Troubleshoot Errors.

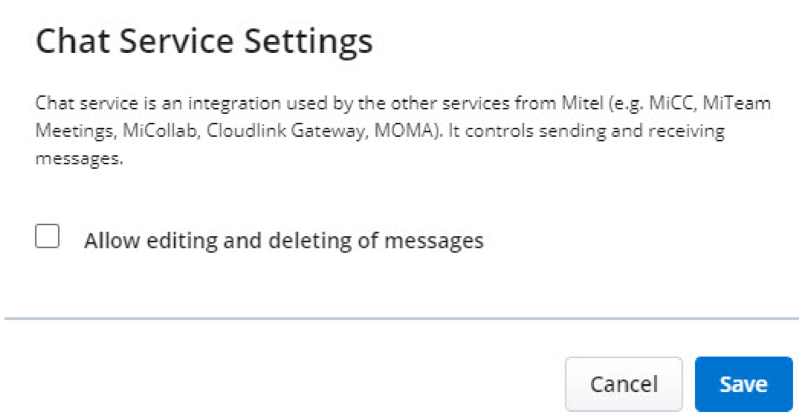
2.12 Allow Users to Edit or Delete Chat Messages in CloudLink Applications

The Mitel Partner or the Account Admin of a customer account can enable or disable the functionality for the users in that customer account to edit or delete the chat messages shared in CloudLink applications. To do this a Mitel Partner or the Admin need to perform the following steps:

1. Log in to the Mitel Administration.
2. Click the **Accounts** option from the navigation menu on the left side of the Accounts Console Dashboard.
3. From the list of accounts that is displayed, click the account for which you want to edit or delete the chat messages. An **Account Information** page is displayed when you click the account.
4. From the **Integrations** panel, click the icon associated with **Chat** integration.



   The **Chat Service Settings** dialog box is opens.
5. By default, the **Allow editing and deleting of messages** is enabled for an account. To prevent the users in an account from deleting or editing their chat messages, clear the **Allow editing and deleting of messages** check box and click **Save**.



2.13 Support

The following section describes how restricting permissions impacts the Support feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can access the **Support** logs page and the **Gateway** logs page if the account has gateway integrations and a PBX onboarded. If the check box associated with **View** is cleared, the Partner or Account Admin is restricted from accessing the **Support** logs and the **Gateway** logs page.
- **Add**: For the Partner and Admin role, the **Add** permission is not applicable.
- **Edit**: For the Partner and Admin role, the **Edit** permission is not applicable.
- **Assign**: For the Partner and Admin role, the **Assign** permission is not applicable.
- **Delete**: For the Partner and Admin role, the **Delete** permission is not applicable.

2.14 Roles and Permissions

As a Mitel Partner you can create a custom role based on the existing Partner or Administrator role and assign these roles to one or more accounts. Once assigned to an account, these roles can be assigned to users in that account.

A role (Partner or Administrator) restricts permissions that exist on the base Partner or Administrator role to view, add, edit, assign, and delete for Mitel Administration application features such as Integrations & Apps, Accounts, and Orders. You can specify permissions that a role allows by selecting or clearing the check boxes corresponding to the respective feature category while creating a role. After creating the custom role, you can assign it to multiple accounts.

Create a Role

To create a role, perform the following steps:

1. Log in to the Mitel Administration on page 1 as a Mitel Partner.
2. Navigate to **User Management** > **Roles and Permissions** option from the navigation menu on the left of the Accounts Console Dashboard. The **Roles** page is displayed.
3. Click **New Role**.
4. Enter a name and a description (optional) for the role in the **Role name** and the **Description** fields respectively. Then select the role type under **Choose the base role** section. By default, **Partner** is selected as the role.
5. Expand the **Permissions** sections and select the permissions you want to provide for the role by selecting the check boxes corresponding to the permissions.
6. Click **Save**. A new role is created.

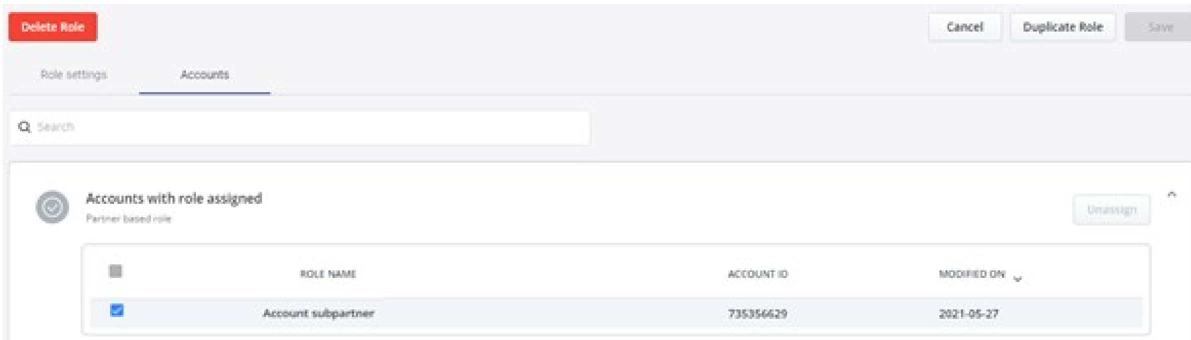
Assign a Role to Account(s)

After creating a role, the Mitel Partner must assign the role to one or more accounts. To assign the role to accounts, perform the following steps:

1. Navigate to the **Accounts** tab that is displayed after creating a new role in the **Roles** edit page.
2. Select the accounts to whom you want to assign the role.

Note:
Only Account Admin role can be assigned to a customer account.

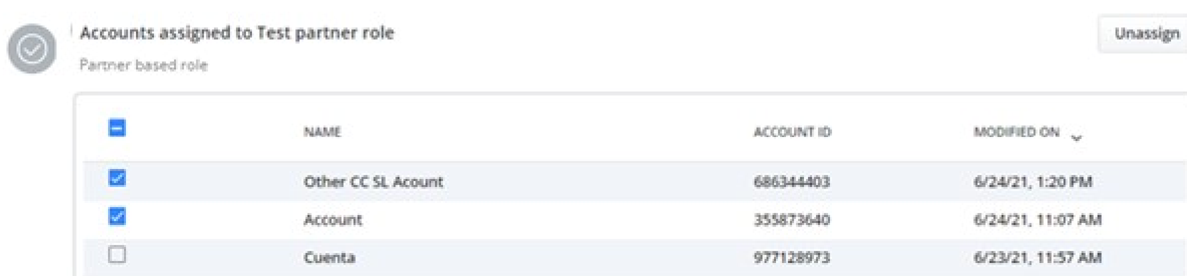
3. Click **Assign**. The role is assigned to the selected accounts.



Unassign a Role from Account(s)

The Mitel Partner can unassign a role that has been assigned to one or more accounts. To unassign a role from accounts, perform the following steps:

1. Navigate to the **User Management** > **Roles and Permissions** option from the navigation menu on the left side of the Accounts Console Dashboard. The **Roles** page is displayed.
2. From the list of roles, click the role that you want to unassign from accounts.
3. Navigate to the **Accounts** tab.
4. Select the accounts from which you want to unassign the role.
5. Click **Unassign**. The role is unassigned from the selected accounts.

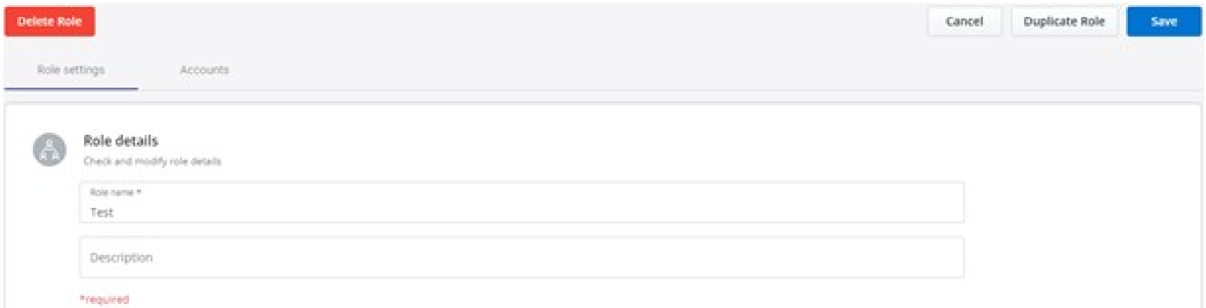


Delete a Role

The Mitel Partner can delete a role by performing the following steps:

1. Navigate to the **User Management** > **Roles and Permissions** option from the navigation menu on the left side of the Accounts Console Dashboard. The **Roles** page is displayed.

2. Select the role that you want to delete.
3. Click **Delete Role** button.



4. A confirmation dialog box is displayed. Type the word "delete" in the **type 'delete'** field and click **Delete**. The selected role is deleted. Clicking **Cancel** cancels the operation.

Duplicate a Role

The Mitel Partner can duplicate a role. Duplicating a role uses the previously used role template, that is, it creates a role that has all the permissions selected as for the original role. The Mitel Partner does not get the option to choose the role type (Partner or Administrator). The duplicate role will be of the same type as the original role. To duplicate a role, perform the following steps:

1. Navigate to the **User Management** > **Roles and Permissions** option from the navigation menu on the left side of the Accounts Console Dashboard. The **Roles** page is displayed.
2. Click the role that you want to duplicate.
3. Click **Duplicate Role**. A new role is created using the previous role template. This role will have all the permissions selected as with the original role.
4. Edit the name and permissions as required and click **Save**.

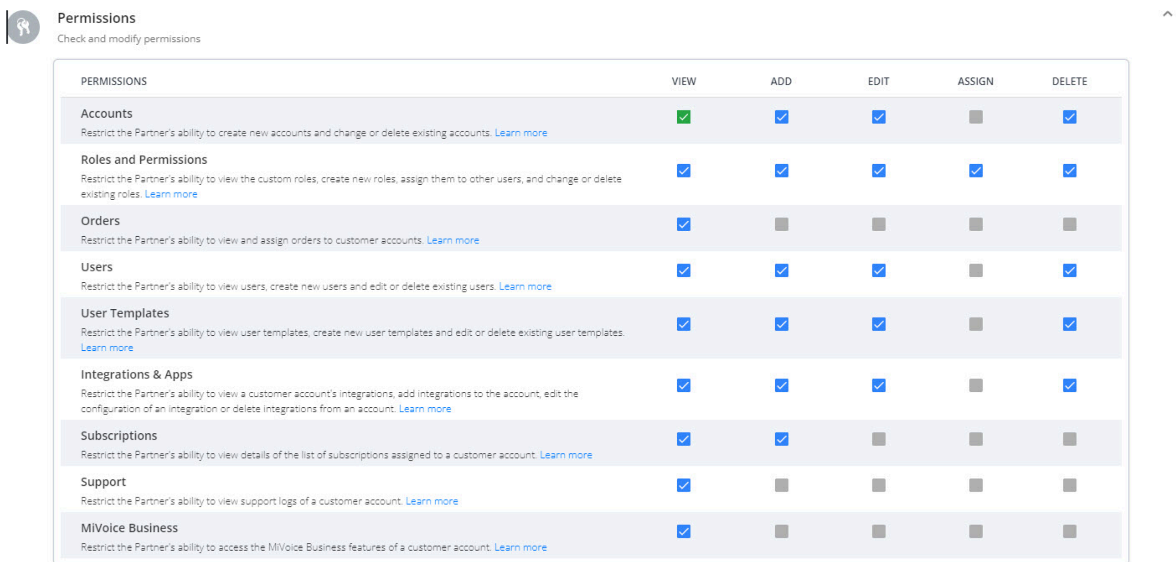
Assigning Permissions

As a Mitel Partner, when you create a new role (Partner or Administrator), you can restrict or grant permissions to view, add, edit, assign, and delete for features such as Integrations & Apps, Accounts, and Orders.

By default, all the permission check boxes are selected, indicating that the role is granted with the standard permissions for the base role. To remove a permission from a role, clear the check box associated with the permission.

Depending on the type of role that you are creating, the following list of features is displayed.

- If you are creating a Partner role, the following table is displayed.

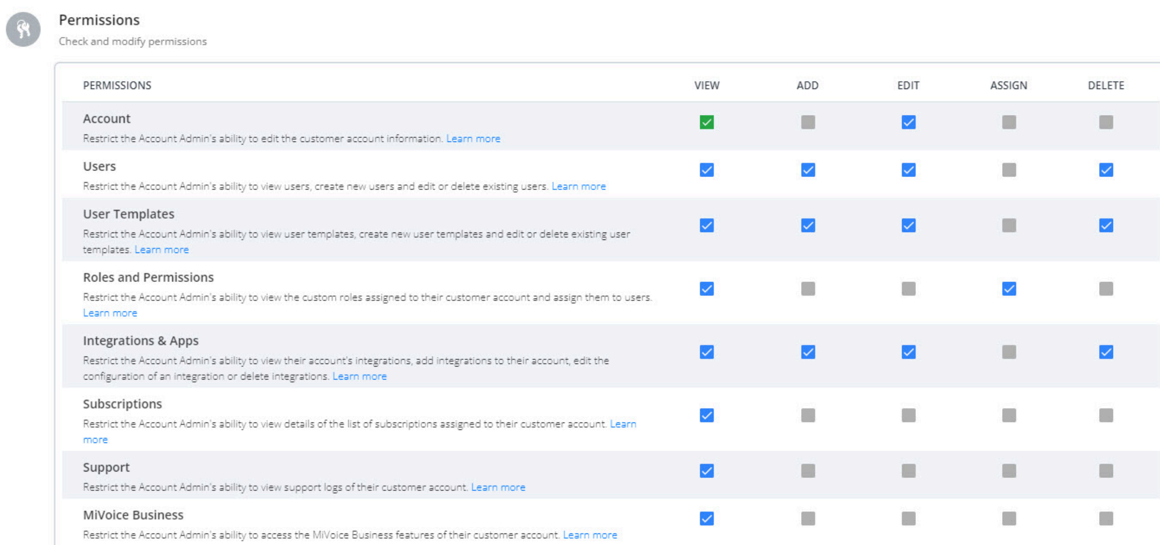


Permissions

Check and modify permissions

PERMISSIONS	VIEW	ADD	EDIT	ASSIGN	DELETE
Accounts Restrict the Partner's ability to create new accounts and change or delete existing accounts. Learn more	☑	☑	☑	☐	☑
Roles and Permissions Restrict the Partner's ability to view the custom roles, create new roles, assign them to other users, and change or delete existing roles. Learn more	☑	☑	☑	☑	☑
Orders Restrict the Partner's ability to view and assign orders to customer accounts. Learn more	☑	☐	☐	☐	☐
Users Restrict the Partner's ability to view users, create new users and edit or delete existing users. Learn more	☑	☑	☑	☐	☑
User Templates Restrict the Partner's ability to view user templates, create new user templates and edit or delete existing user templates. Learn more	☑	☑	☑	☐	☑
Integrations & Apps Restrict the Partner's ability to view a customer account's integrations, add integrations to the account, edit the configuration of an integration or delete integrations from an account. Learn more	☑	☑	☑	☐	☑
Subscriptions Restrict the Partner's ability to view details of the list of subscriptions assigned to a customer account. Learn more	☑	☑	☐	☐	☐
Support Restrict the Partner's ability to view support logs of a customer account. Learn more	☑	☐	☐	☐	☐
MiVoice Business Restrict the Partner's ability to access the MiVoice Business features of a customer account. Learn more	☑	☐	☐	☐	☐

- If you are creating an Administrator (Account Admin) role, the following table is displayed.



Permissions

Check and modify permissions

PERMISSIONS	VIEW	ADD	EDIT	ASSIGN	DELETE
Account Restrict the Account Admin's ability to edit the customer account information. Learn more	☑	☐	☑	☐	☐
Users Restrict the Account Admin's ability to view users, create new users and edit or delete existing users. Learn more	☑	☑	☑	☐	☑
User Templates Restrict the Account Admin's ability to view user templates, create new user templates and edit or delete existing user templates. Learn more	☑	☑	☑	☐	☑
Roles and Permissions Restrict the Account Admin's ability to view the custom roles assigned to their customer account and assign them to users. Learn more	☑	☐	☐	☑	☐
Integrations & Apps Restrict the Account Admin's ability to view their account's integrations, add integrations to their account, edit the configuration of an integration or delete integrations. Learn more	☑	☑	☑	☐	☑
Subscriptions Restrict the Account Admin's ability to view details of the list of subscriptions assigned to their customer account. Learn more	☑	☐	☐	☐	☐
Support Restrict the Account Admin's ability to view support logs of their customer account. Learn more	☑	☐	☐	☐	☐
MiVoice Business Restrict the Account Admin's ability to access the MiVoice Business features of their customer account. Learn more	☑	☐	☐	☐	☐

For more information about each permission see:

2.14.1 Account (for Admin)

The following section describes how restricting permissions impacts the Account feature for an Admin.

- **View**: The **View** permission is in read-only mode for the Account Admin role. The account admin will always have access to view the information on the Account page.
- **Add**: The **Add** permission is not applicable for the Account Admin role.

- **Edit**: If the check box associated with **Edit** permission is selected for an Account Admin role, the Admins can edit their account. If the check box associated with **Edit** permission is cleared, Admins are restricted from editing any accounts.
- **Assign**: The **Assign** permission is not applicable for the Account Admin role.
- **Delete**: The **Delete** permission is not applicable for the Account Admin role.

Note:
The Account Admin must refresh or log out and log back in to see ay change(s) that is made by the Mitel Partner.

2.14.2 Account (for Partner)

The following section describes how restricting permissions impacts the Account feature for the Partner.

- **View**: The **View** permission is in read-only mode for Partner role. Partners can always view an account.
- **Add**: If the check box associated with **Add** is selected, the Partner can add a new account. If you clear the check box associated with **Add**, the Partner is restricted from adding a new account.
- **Edit**: If the check box associated with **Edit** permission is selected for a Partner role, the Partner can edit any existing account. If the check box associated with **Edit** permission is cleared, Partners are restricted from editing any accounts.
- **Assign**: The **Assign** permission is not applicable for Partner role.
- **Delete**: If the check box associated with **Delete** is selected, a Partner can delete an existing account. If you clear the check box associated with **Delete**, a Partner is restricted from deleting an account.

2.14.3 Users

The following section describes how restricting permissions impacts the Users feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can view the users in a customer account and details of the users in an account. However, they will not be able to add, edit, or delete a user account. A role must have the **View** permission in order to add, edit or delete any user. If you clear the check box associated with **View**, for a Partner or an Account Admin role, the Partner or Account Admin is restricted from viewing the users for a customer account and will not have access to the users landing list.
- **Add**: If the check box associated with **Add** is selected, the Partner or Account Admin can add new users individually or in bulk, send welcome emails, and have access to the **Manage** button in the Users list page. If you clear the check box associated with **Add**, for a Partner or an Account Admin role, the Partner or Account Admin is restricted from adding new users, and sending welcome emails, and will not have access to the **Manage** button in the Users list page.

Note:
The role must have **Add** or **Edit** permission to be able to send welcome emails and have access to the **Manage** button in the Users list page.

- **Edit**: If the check box associated with **Edit** permission is selected, the Partner or Account Admin can edit any existing user account, reset passwords, change the existing license, and send welcome emails. If the check box associated with **Edit** permission is cleared for a Partner or an Account Admin role, the Partner or Account Admin is restricted from editing any existing user account, resetting passwords, making changes to the existing licenses, and from sending welcome emails.

> **Note**:
> The role must have **Add** or **Edit** permission to be able to send welcome emails and have access to the **Manage** button in the Users list page.

- **Assign**: The **Assign** permission is not applicable for the Partner or Account Admin role.
- **Delete**: If the check box associated with **Delete** is selected, the Partner or Account Admin can delete an existing user. If you clear the check box associated with **Delete**, the Partner or Account Admin is restricted from deleting a user.

2.14.4 User Templates

The following section describes how restricting permissions impacts the User Templates feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can view the **User Templates** page. If you clear the checkbox associated with **View**, the Partner or Account Admin is restricted from viewing **User Templates** page and accessing the User Templates feature. To add, edit, or delete user templates, the role must have the **View** permission.
- **Add**: If the check box associated with **Add** is selected, the Partner or Account Admin can create new template. If you clear the check box associated with **Add**, the Partner or Account Admin is restricted from adding a new user template.
- **Edit**: If the check box associated with **Edit** permission is selected, the Partner or Account Admin can edit any existing user template. If the check box associated with **Edit** permission is cleared the Partners and Account Admins is restricted from editing any existing user template.
- **Assign**: For the Partner role and the Account Admin role, the **Assign** permission is not applicable.
- **Delete**: If the check box associated with **Delete** is selected the Partner or Account Admin can delete existing user templates. If you clear the check box associated with **Delete**, the Partner or Account Admin is restricted from deleting existing user templates.

2.14.5 Roles and Permissions

The following section describes how restricting permissions impacts the Roles and Permissions feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can view the Roles and Permissions feature. User with a role that has **View** permission only, can view the list of roles and permissions that make each role, but cannot perform actions such as add, delete, or assign. If you clear the check box associated with **View**, the Partner or an Account Admin is restricted from having access to the Roles and Permissions feature. A role must have the **View** permission in order to use the functionalities of **Add**, **Edit**, **Assign**, or **Delete** permissions.
- **Add**: For the Partner role, if the check box associated with **Add** is selected, the Partner can add a new role and duplicate an existing role. If the check box associated with **Add** is cleared, the Partner is restricted from creating a new role and from duplicating an existing role. The **Add** permission is not applicable for the Account Admin role.

- **Edit**: If the check box associated with **Edit** is selected, the Partner can edit an existing role and assign or unassign the role from an account. If the check box associated with **Edit**, is cleared the Partner is restricted from editing an existing role and assigning the role to or unassigning the role from an account. The **Edit** permission is not applicable for the Account Admin role.
- **Assign**: If the check box associated with **Assign** is selected, the Partner or Account Admin can assign or change a user's role. If the check box associated with **Assign** is cleared a Partner or an Account Admin is restricted from assigning and changing a user's role.
- **Delete**: For the Partner role, if the check box associated with **Delete** is selected, the Partner can delete an existing role. If the check box associated with **Delete** is cleared, the Partner is restricted from deleting an existing role. The **Delete** permissio is not applicable for an Account Admin role.

2.14.6 Integrations & Apps

The following section describes how restricting permissions impacts the Integrations and Apps feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can access the details of integrations for an account. If you clear the checkbox associated with **View**, the Partner or Account Admin is restricted from accessing the details of integrations for an account. Without the **View** permission, the **Integrations** panel will not be displayed in the Accounts edit page or under the **Integrations and Apps** menu. A role must have the **View** permission in order to add, edit, or delete an integration in an account.
- **Add**: If the check box associated with **Add** is selected, the Partner or Account Admin can add a new integration to an account and configure the integration setup. The **Privileges** toggle button and the **Add New** buttons are also enabled if the check box associated with **Add** is selected. If you clear the check box associated with **Add**, the Partner or Account Admin is restricted from adding and configuring new or existing integrations for an account. The **Privileges** toggle button and the **Add New** buttons are disabled if the check box associated with **Add** is cleared.

> **Note**:
> Without **Add** or **Edit** permission users with this role cannot configure any existing integrations or access the integration privileges.

- **Edit**: If the check box associated with **Edit** permission is selected, the Partner or Account Admin can change the integration configuration. If the check box associated with **Edit** permission is cleared, the Partner or Account Admins is restricted from changing integration configuration and editing the configuration in an account.

> **Note**:
> Without **Add** or **Edit** permission users with this role cannot configure any existing integrations or access the integration privileges.

- **Assign**: The **Assign** permission is not applicable for the Partner and Account Admin role.
- **Delete**: If the check box associated with **Delete** is selected, the Partner or Account Admin can delete integrations from a customer account. If the Partner and Account Admin has both **Add** and **Delete** permissions, the Partner and Account Admin can add and delete integrations from the integrations catalogue.If you clear the check box associated with **Delete**, the Partner and Account Admin are restricted from deleting an integration from a customer account.

2.14.7 Subscriptions

The following section describes how restricting permissions impacts the Subscription feature.

- **View**: If the check box associated with **View** is selected, the Partner or the Account Admin can view the subscriptions assigned to a customer account in Accounts edit page and in the Subscriptions page. If the check box associated with **View** is cleared, the Partner or Account Admin is restricted from viewing the subscriptions assigned to a customer account.
- **Add**: For the Partner role, if the check box associated with **Add** is selected, the Partner can add subscriptions and **Add Order** button is displayed in the **Subscriptions** section which allows the Partner to add orders in an account. If you clear the check box associated with **Add**, a Partner is restricted from adding subscription and the **Add Order** button is not displayed in the **Subscriptions** section.

> **Note**:
> The Partner role must have the **View** permission selected in order to access the functionalities of **Add** permission.

The **Add** permission is not applicable for the Account Admin role.

- **Edit**: The **Edit** permission is not applicable for the Account Admin role.
- **Assign**: The **Edit** permission is not applicable for the Account Admin role.
- **Delete**: The **Edit** permission is not applicable for the Account Admin role.

2.14.8 Support

The following section describes how restricting permissions impacts the Support feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can access the **Support** logs page and the **Gateway** logs page if the account has gateway integrations and a PBX onboarded. If the check box associated with **View** is cleared, the Partner or Account Admin is restricted from accessing the **Support** logs and the **Gateway** logs page.
- **Add**: For the Partner and Admin role, the **Add** permission is not applicable.
- **Edit**: For the Partner and Admin role, the **Edit** permission is not applicable.
- **Assign**: For the Partner and Admin role, the **Assign** permission is not applicable.
- **Delete**: For the Partner and Admin role, the **Delete** permission is not applicable.

2.14.9 MiVoice Business

The following section describes how restricting permissions impacts the MiVoice Business feature.

> **Note**:
> The MiVoice Business permission is applicable **only** when MiVoice Business is integrated.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can access MiVoice Business features of their customer account. If the check box associated with **View** is cleared, the Partner or Account Admin is restricted from accessing **MiVoice Business features** of their customer account.
- **Add**: The **Add** permission is not applicable.
- **Edit**: The **Edit** permission is not applicable.
- **Assign**: The **Assign** permission is not applicable.
- **Delete**: The **Delete** permission is not applicable.

2.14.10 Customer Care

The following section describes how restricting permissions impacts the Customer Care feature.

- **View**: If the check box associated with **View** is selected, the Partner or Account Admin can access the Customer Care feature. If the check box associated with **View** is cleared, the Partner or Account Admin is restricted from accessing the Customer Care feature.
- **Add**: The **Add** permission is not applicable for Partner and Account Admin role.
- **Edit**: The **Edit** permission is not applicable for Partner and Account Admin role.
- **Assign**: The **Assign** permission is not applicable for Partner and Account Admin role.
- **Delete**: The **Delete** permission is not applicable for Partner and Account Admin role.

2.14.11 Developer

The following section describes how restricting permissions impacts the Developer feature.

> **Note**:
> The **Developer** permission is applicable only for the Partner role.

- **View**: If the check box associated with **View** is selected, the Partner can access the **Developer** page, register new applications, and assign them to customer accounts. If the check box associated with **View** is cleared, the Partner is restricted from accessing the **Developer** page, registering new applications, and assigning them to customer accounts.
- **Add**: The **Add** permission is not applicable.
- **Edit**: The **Edit** permission is not applicable.
- **Assign**: The **Assign** permission is not applicable.
- **Delete**: The **Delete** permission is not applicable.

2.14.12 Orders

The following section describes how restricting permissions impacts the Orders feature.

> **Note**:
> The Order permission is applicable only for the Partner role.

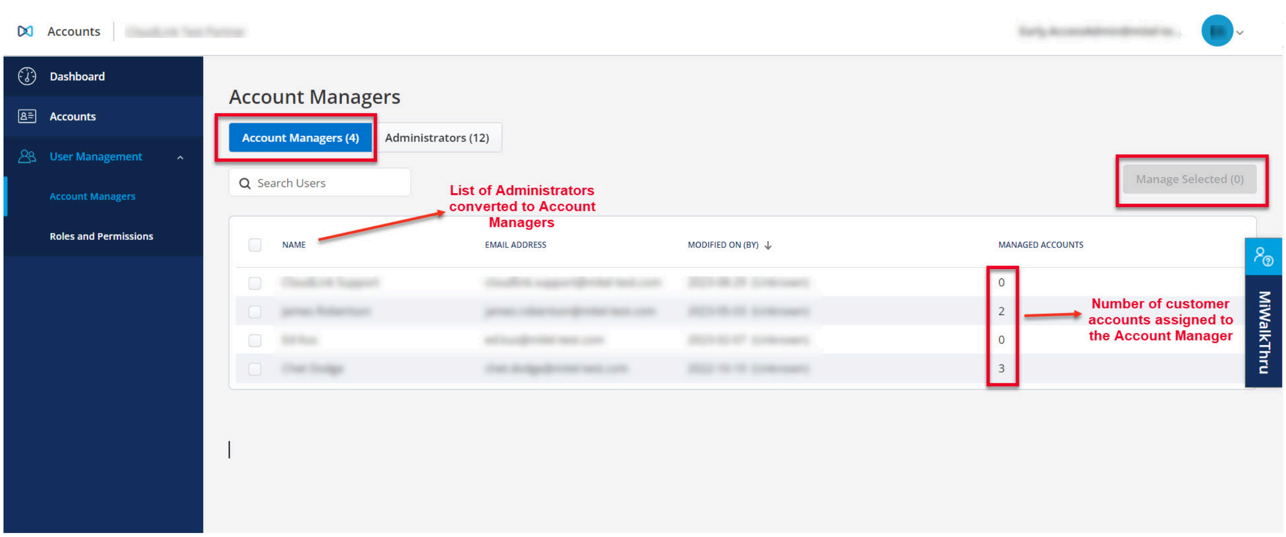
- **View**: If the check box associated with **View** is selected, the Partner can access the **Order** page and assign orders to accounts. If the check box associated with **View** is cleared, the Partner is restricted from accessing the **Orders** page and assigning orders to accounts.
- **Add**: The **Add** permission is not applicable.
- **Edit**: The **Edit** permission is not applicable.
- **Assign**: The **Assign** permission is not applicable.
- **Delete**: The **Delete** permission is not applicable.

2.15 Account Managers

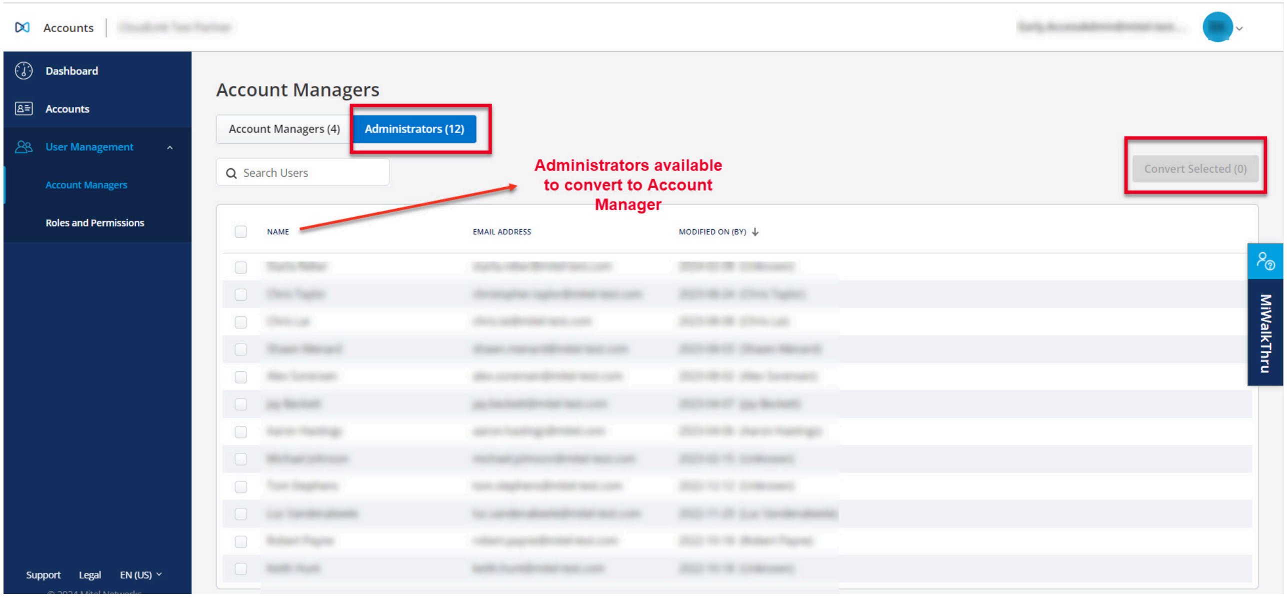
The Account Managers page displays a comprehensive list of the **Account Managers** and **Administrators** within the Partner account.

> **Note**:
> This feature is *not* available to Partners assuming the role of an Account Admin.

Account Managers



Administrators



The Mitel Administration portal now allows unrestricted Partner Administrators to assign Customer Accounts to one or more Administrators within their Partner Account. These administrators are called **Account Managers**.

As a Partner, you can do the following:

- Convert an Administrator to Account Manager
  - Assign Account(s) to an Account Manager
  - Unassign Account(s) from an Account Manager
- Upgrade an Account Manager to an Administrator

2.15.1 Delegating Partner Account Management

The Mitel Administration portal is enhanced to restrict access to specific Customer Accounts. Previously, the configuration listed all customer accounts managed by the partner admin, which were visible to all account admins within that account.

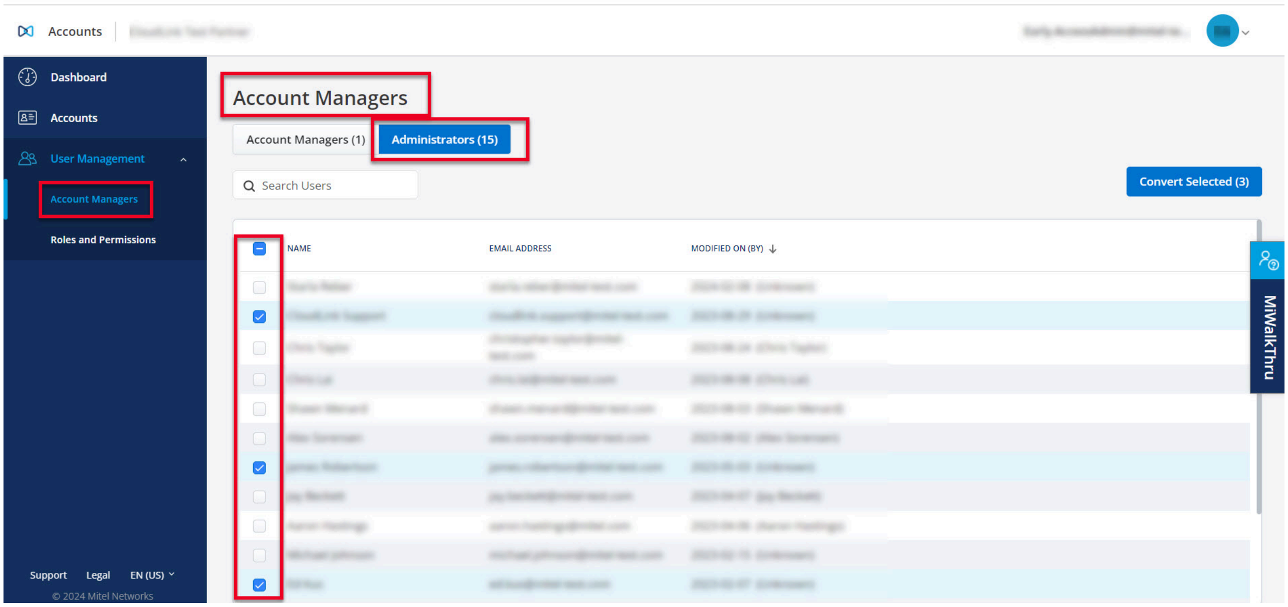
Note:
The Partner Admin who is already logged in cannot manage their own account within the **Account Managers** or the **Administrator** tab.

Converting an Administrator to Account Manager

You need to convert an administrator to an **Account Manager** to restrict access to specific Customer Accounts.

Complete the following steps to convert the admin to an Account Manager from a Partner account:

1. Click **User Management** > **Account Manager** from the left menu. The **Account Managers** page opens.
2. Click and open the **Administrators** tab. The complete list of Partner Admins in the Partner account are displayed.
3. Choose the Admin(s) to be converted to Account Manager(s) by selecting the checkbox next to their name(s).



4. Click **Convert Selected**. The confirmation dialog is displayed.
5. Confirm that the information is correct, and click **OK** to proceed. The progress bar **Convert to Account Managers** is visible, showing the progress. Click **Close** when the conversion is completed.

   Click **Cancel** to cancel the operation.

The newly converted **Account Managers** are displayed are now displayed in the Account Managers tab.

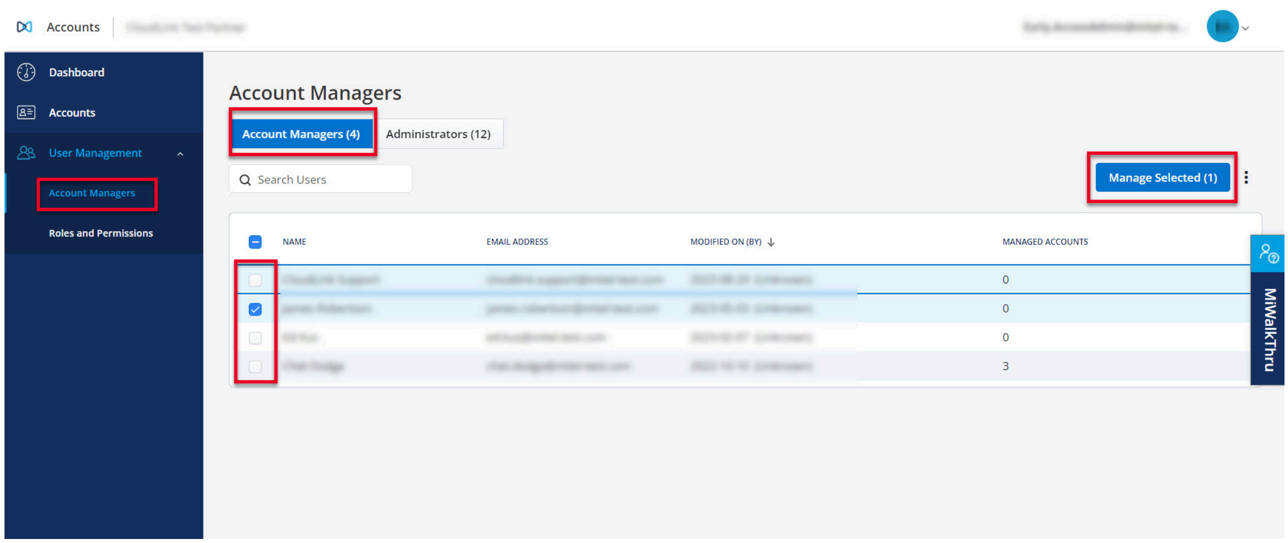
Assigning Account(s) to an Account Manager

As a Partner Administrator, you can assign specific customer accounts to an Account Manager individually, or to multiple Account Managers simultaneously.

Complete the following steps to assign specific customer accounts to ***an Account Manager individually***:

1. Click **User Management** > **Account Managers**.
2. Select the **Account Manager** from the list under the **Account Managers** tab by selecting the checkbox next to their name.

Note:
You can also manage an individual Account Manager by clicking their name in the list.



3. Click **Manage Selected**. The following tabs are displayed.
   - **Accounts assigned** - This tab displays the accounts already assigned to the Account Manager.
   - **Accounts not assigned** - This tab displays accounts that are available to be assigned to the Account Manager.
4. Click the **Accounts not assigned** tab, then select the accounts you want to assign to the selected **Account Manager** using the checkbox.
5. Click **Assign**. The confirmation dialog is displayed.
6. Confirm that the information is correct, and click **Assign** to proceed. The progress bar **Assign Account(s)** is visible, showing the progress. Click **Close** when the task is completed successfully.

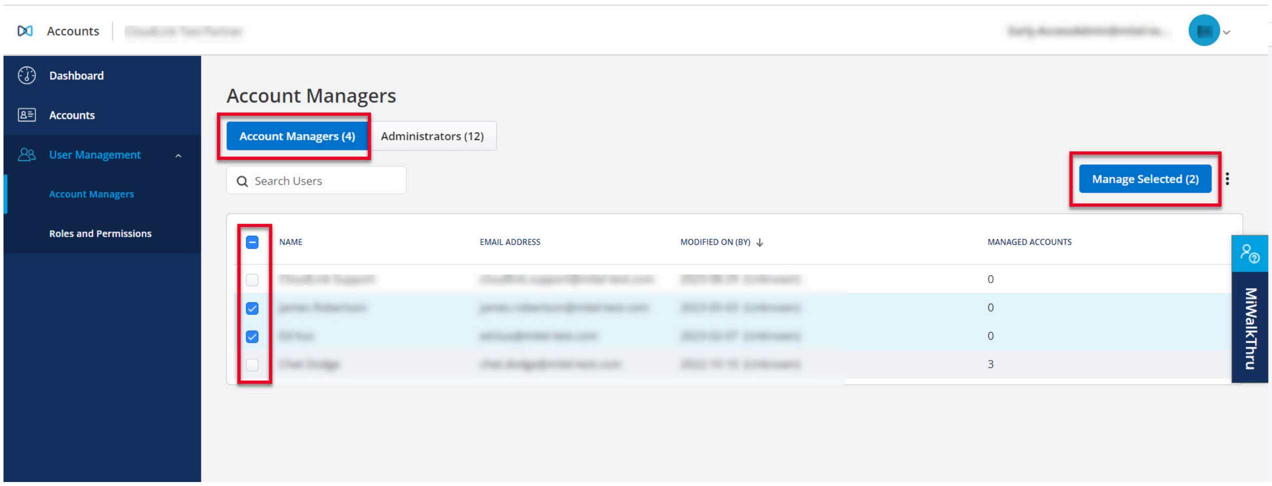
   Click **Cancel** to cancel the operation.

The **Accounts assigned** tab will now display the newly assigned accounts to the selected Account Manager.

Complete the following steps to assign specific customer accounts to ***multiple Account Managers simultaneously***:

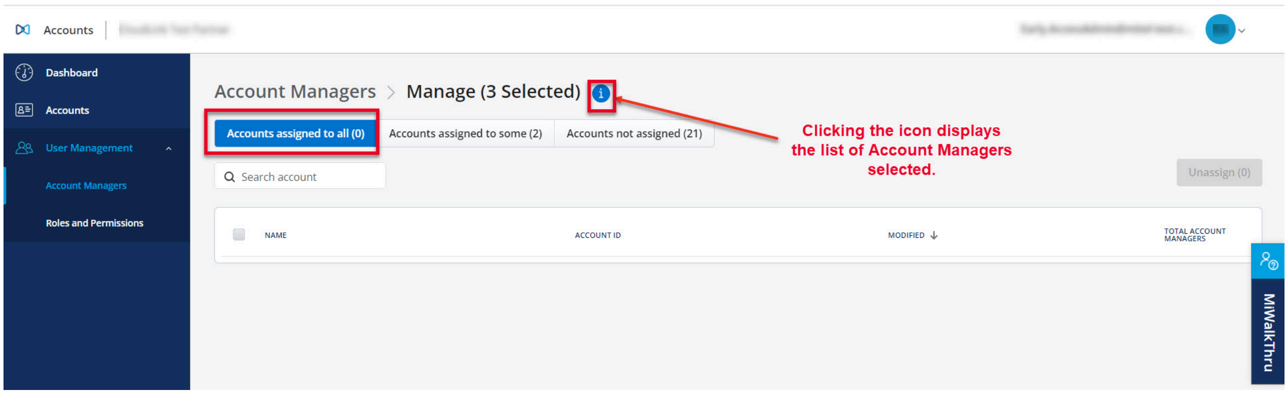
1. Click **User Management** > **Account Managers**.

2. Select the **Account Managers** from the list under the **Account Managers** tab by selecting the checkbox next to their names.



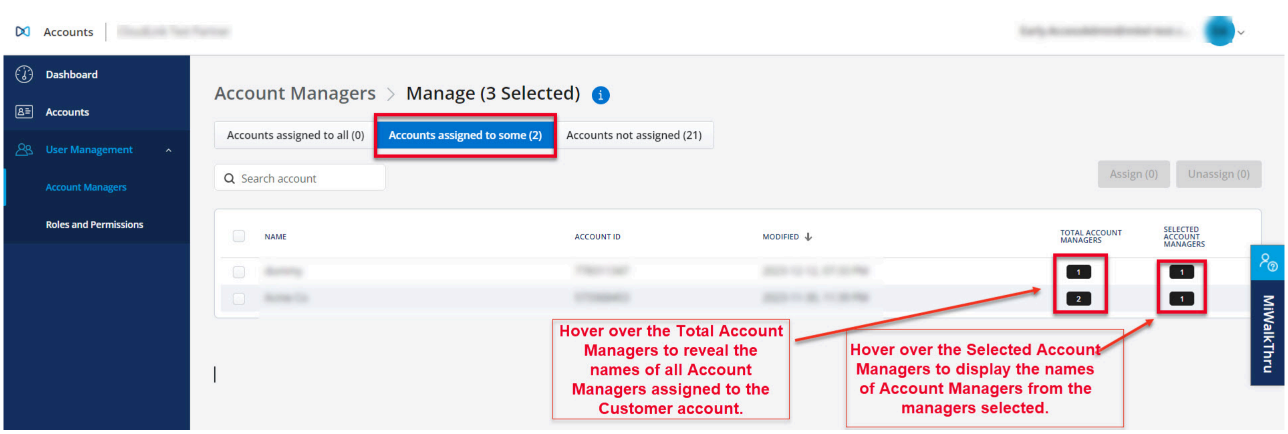
3. Click **Manage Selected**. The following tabs are displayed.

   a. **Accounts assigned to all** - This list displays accounts that are assigned to all the selected account managers.



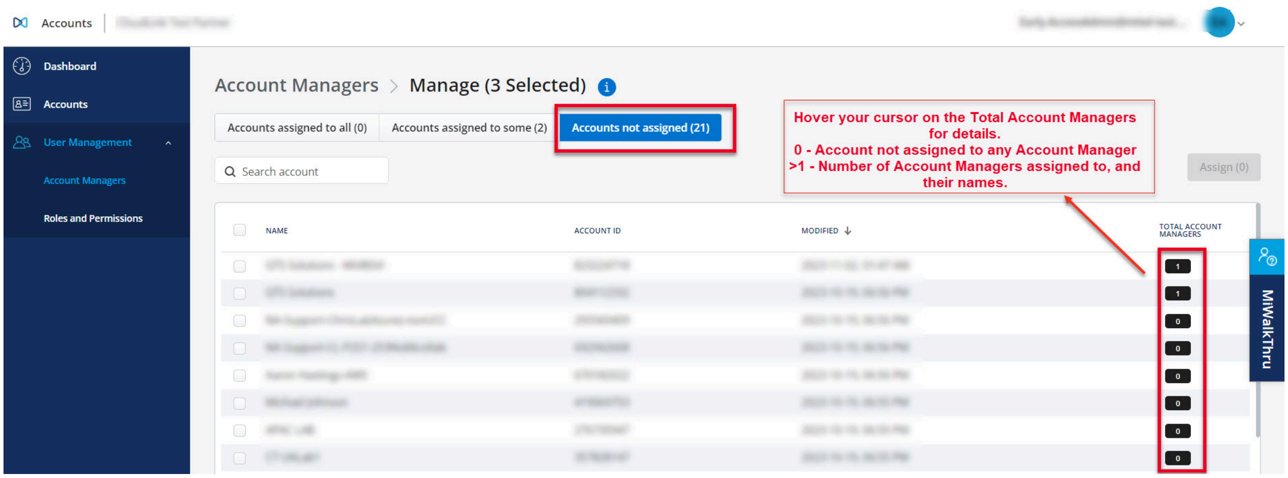
   You have the option to select the checkbox and unassign the account from the selected managers.

   b. **Accounts assigned to some** - This list displays accounts that are assigned to one or more of the selected account managers.



   You have the option to select the checkbox and either assign the account to the selected managers or unassign it from the selected managers.

   c. **Accounts not assigned** - This list displays accounts that are not assigned to any of the selected account managers.



You have the option to select the checkbox and assign the account to the selected managers.

The **Accounts assigned** tab will now display the newly assigned accounts to the selected Account Managers.

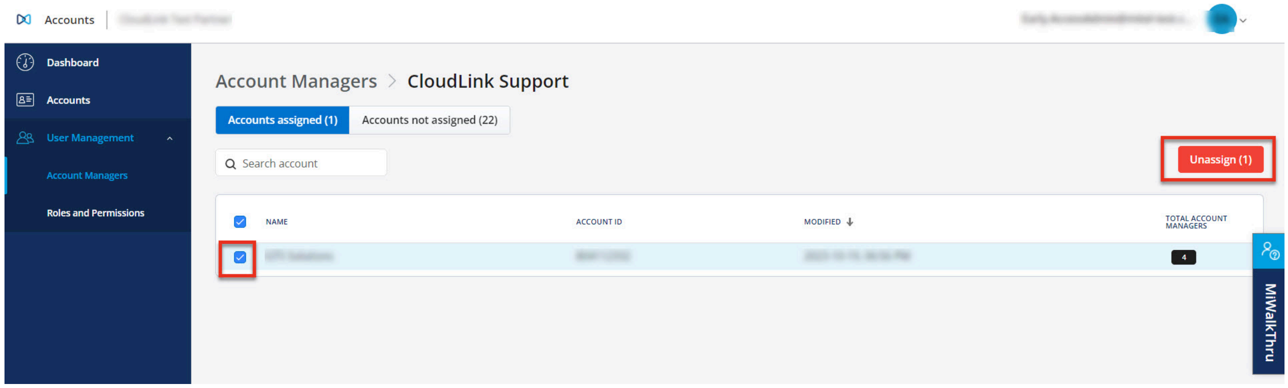
Unassigning Account(s) from an Account Manager

As a Partner Administrator, you can unassign specific customer accounts from an Account Manager individually, or from multiple Account Managers simultaneously.

Unassign Individual Account Manager

1. Go to **User Management** > **Account Managers**.
2. From the list of **Account Managers**, choose the manager whose account(s) you wish to unassign by selecting the checkbox next to their name.
3. Click **Manage Selected**. The following tabs are displayed.
4. From the **Account assigned** list, choose the account you want to unassign by selecting the checkbox next to it.

5. Click **Unassign**.



Confirm by clicking **Unassign** again in the confirmation dialog that opens. The progress bar for unassigning account is visible, showing the progress. Click **Close** when the account is unassigned successfully.

Click **Cancel** to cancel the operation.

The **Accounts assigned** tab will now have removed the unassigned accounts from the selected Account Manager.

Unassign multiple Account Managers

1. Go to **User Management** > **Account Managers**.
2. From the list of **Account Managers**, choose the managers whose accounts you wish to unassign by selecting the checkbox next to their names.
3. Click **Manage Selected**. The following tabs are displayed.
   - *Accounts assigned to all* - Select the account(s) checkbox next to it and click **Unassign** to remove the account from the selected managers.
   - *Accounts assigned to some* - Select the account(s) checkbox next to it and click **Unassign** to remove the account from the selected managers.
4. Confirm by clicking **Unassign** again in the Confirmation dialog. The progress bar for unassigning accounts is visible, showing the progress. Click **Close** when the account is unassigned successfully.

   Click **Cancel** to cancel the operation.

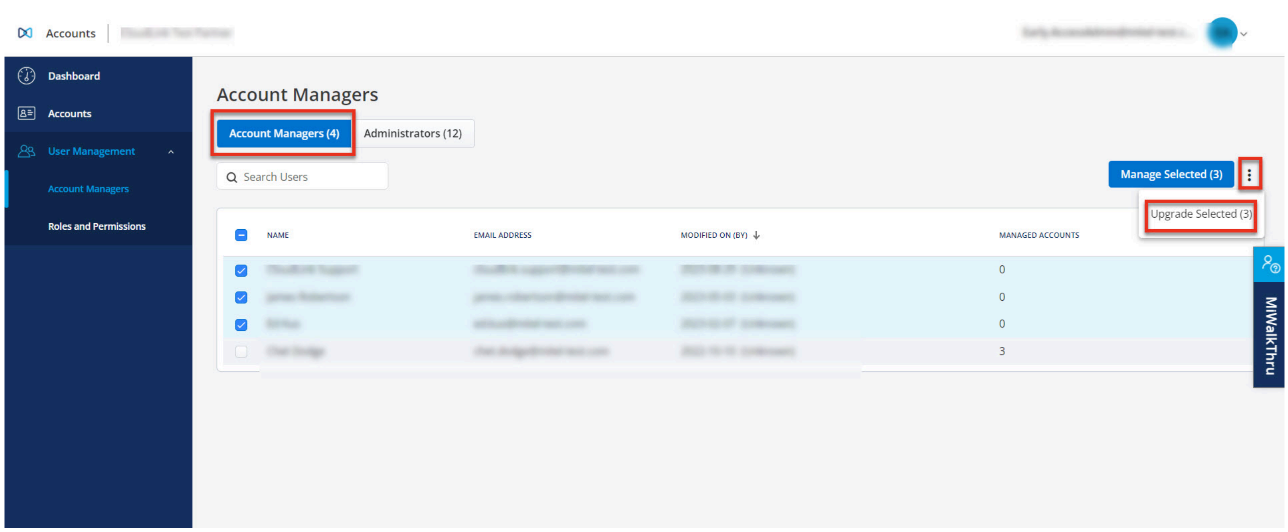
The **Accounts assigned** tab will now have removed the unassigned accounts from the selected Account Managers.

Note:
If the account manager is **upgraded** to an administrator, there are no restrictions, and all accounts can be managed as an administrator.

Upgrading an Account Manager to an Administrator

An Administrator has unrestricted access to the customer accounts, an Account Manager can be upgraded to an Administrator. Complete the following steps to do so:

1. Click **User Management** > **Account Manager** from the left menu. The **Account Managers** page opens.
2. In the **Account Managers** tab select the manager(s) you wish to upgrade to an **Administrator**.
3. Click ⋮, and click **Upgrade Selected**.



The **Confirm Upgrade To Administrator(s)?** confirmation dialog is displayed.

4. Click **Confirm** to upgrade the selected Account Managers to Administrators. The progress bar for upgrade is visible, showing the progress. Click **Close** after the selected managers are upgraded to Administrators successfully.

   Click **Cancel** to cancel the operation.

The list of **Administrators** in the Administrators tab will now include the upgraded Account Managers.

2.16 Event History

The Event History provides insight to Mitel Partners and Account Admins regarding events that occurred within an account. With filtering and exporting capabilities, this feature allows for targeted analysis of events to help with troubleshooting and change management.

The feature is available for the following accounts:

- Accounts with the MiVoice Business integration enabled and the **Administration** feature toggled ON.
- Accounts with the Zoom integration enabled.

Accessing Event History

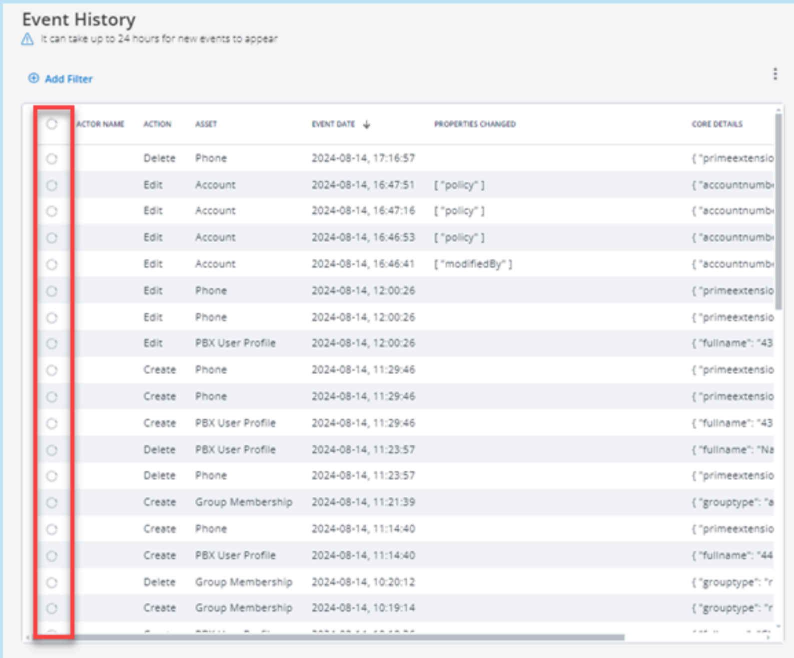
To access Event History and view changes, do the following:

1. Log in to the Mitel Administration on page 1 as a Mitel Partner or Account Administrator.
2. This step is applicable to Mitel Partners only, if you are an Account Administrator, proceed to Step 3. Navigate to **Accounts** and select the desired account.
3. Navigate to **Support** > **Event History**.

   It might take around 15 seconds to load the Event History page.

Note:

- Spinners are displayed while retrieving data.
- It can take up to 24 hours for new events to appear.



ACTOR NAME	ACTION	ASSET	EVENT DATE	PROPERTIES CHANGED	CORE DETAILS
	Delete	Phone	2024-08-14, 17:16:57		{ "primeextensio
	Edit	Account	2024-08-14, 16:47:51	["policy"]	{ "accountnumb
	Edit	Account	2024-08-14, 16:47:16	["policy"]	{ "accountnumb
	Edit	Account	2024-08-14, 16:46:53	["policy"]	{ "accountnumb
	Edit	Account	2024-08-14, 16:46:41	["modifiedBy"]	{ "accountnumb
	Edit	Phone	2024-08-14, 12:00:26		{ "primeextensio
	Edit	Phone	2024-08-14, 12:00:26		{ "primeextensio
	Edit	PBX User Profile	2024-08-14, 12:00:26		{ "fullname": "43
	Create	Phone	2024-08-14, 11:29:46		{ "primeextensio
	Create	Phone	2024-08-14, 11:29:46		{ "primeextensio
	Create	PBX User Profile	2024-08-14, 11:29:46		{ "fullname": "43
	Delete	PBX User Profile	2024-08-14, 11:23:57		{ "fullname": "Na
	Delete	Phone	2024-08-14, 11:23:57		{ "primeextensio
	Create	Group Membership	2024-08-14, 11:21:39		{ "grouptype": "a
	Create	Phone	2024-08-14, 11:14:40		{ "primeextensio
	Create	PBX User Profile	2024-08-14, 11:14:40		{ "fullname": "44
	Delete	Group Membership	2024-08-14, 10:20:12		{ "grouptype": "r
	Create	Group Membership	2024-08-14, 10:19:14		{ "grouptype": "r

Note:

If an error occurs while retrieving data, the following banner will be displayed. Refresh the page to attempt to reload the data.

Note:

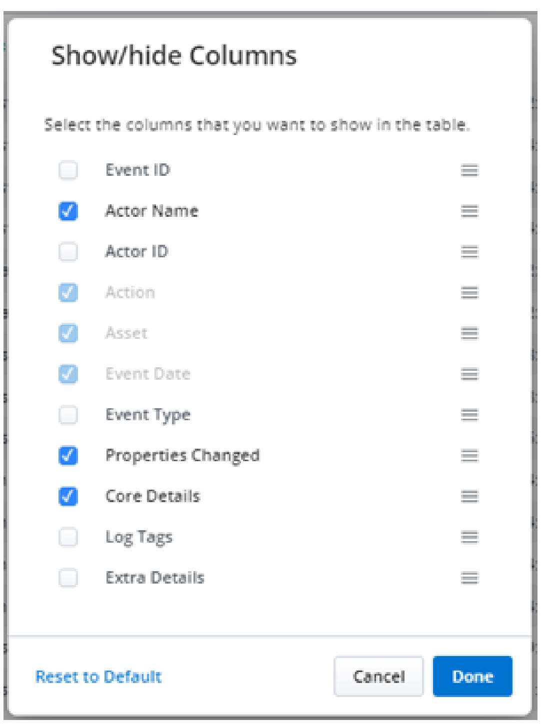
By scrolling down in the table, more events will be retrieved until all available events are displayed. At that point, the following banner will be displayed

Event History table

The Event History table has the following features:

1. The data can be sorted by Event Date by clicking the column header.
2. The columns displayed can be customized:

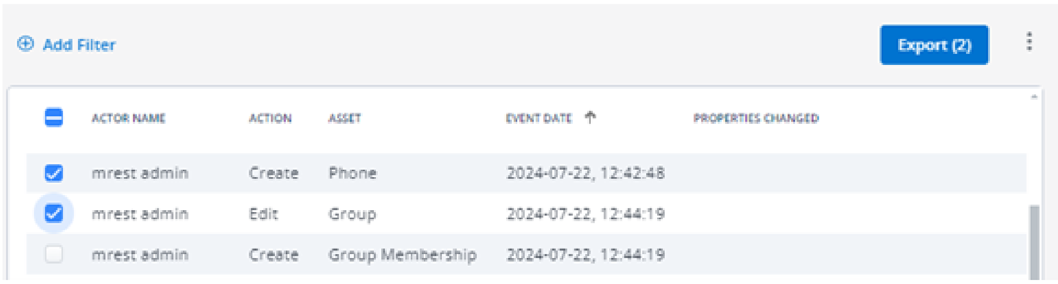
- Click the icon, select **Show/hide columns**.
- In the pop-up, select the checkbox(es) of interest.
- Rearrange the columns by dragging the icon up or down as desired.



Batch Exporting

1. In the event table, select the checkbox(es) of the desired events.

   The Export button appears showing the number of events selected.



2. Click **Export** to export the data of the selected events to a .csv file.

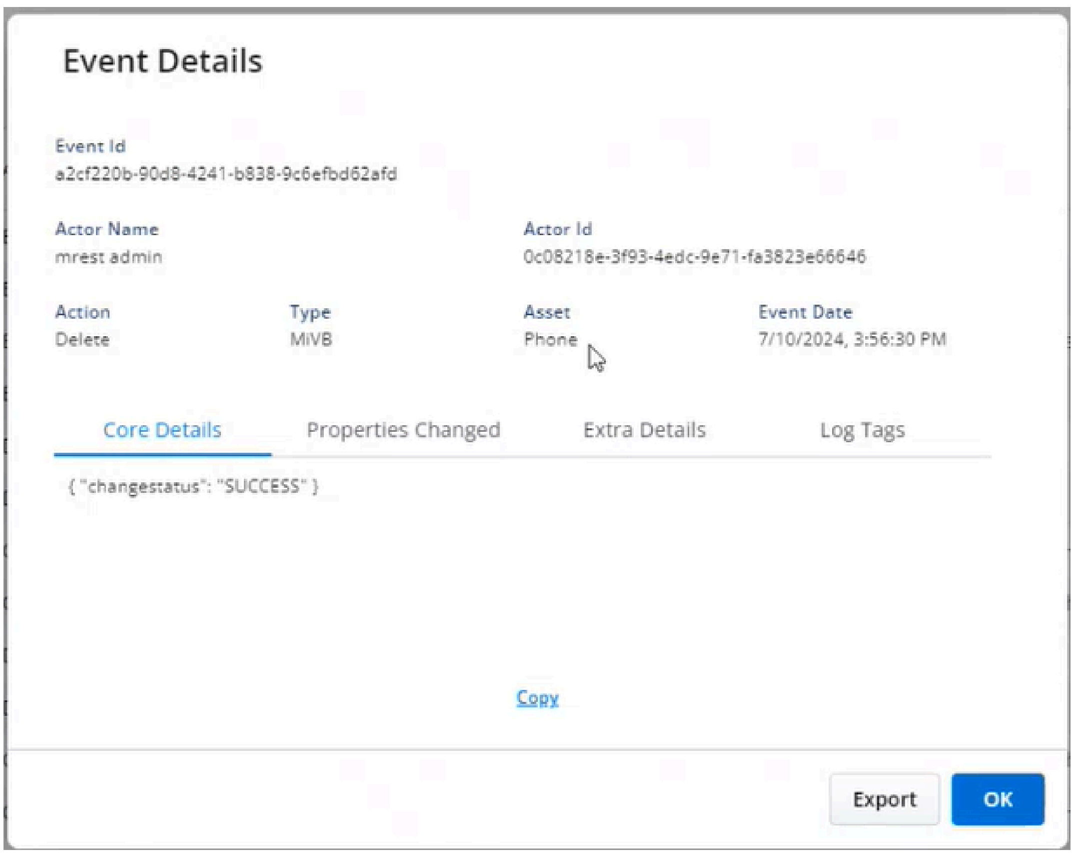
Event Details

The Event History table has the following fields:

Name	Description
EVENT ID	The ID of the event.
ACTOR NAME	The name of the user or entity that triggered the action (for example, User ABC, System, Solution, SCIM, Unknown) 'Unknown' will appear if a name can no longer be found (for example, the user who triggered the event has been deleted)
ACTOR ID	The CloudLink ID or System ID of the entity that triggered the event.
ACTION	The event action (for example, Create, Edit, Delete).
EVENT TYPE	The event type or category (for example, Admin, MiVoice Business, Service Delivery).
ASSET	The object that was acted upon (for example, Phone, Account, User License).

Name	Description
EVENT DATE	The date and time the event occurred.
PROPERTIES CHANGED	A list of properties that changed for the asset during the event. For example, if a phone's macAddress is edited -> ["macAddress"]
CORE DETAILS	Detailed information about the event.
EXTRA DETAILS	Extra details about the event, if available.
LOG TAGS	Special tags are appended to each event to facilitate search functionality.

After clicking on an event in the Event History table, the Event Details window will be displayed.



The Event Details window has the following features:

- **Copy**: to place the selected tab's data on your clipboard.
- **Export**: to export all data from all tabs for that event to a .csv file.

Filtering Event Data

To search for particular events, you can add filters to the table by clicking the **Add Filter** 

button. Multiple filters can be applied to significantly narrow down event data.

The available filter options may vary depending on the integrations enabled for a Cloudlink account. For example, accounts with the MiVoice Business integration enabled and the Administration feature toggled ON will have a unique set of filter options compared to accounts with the Zoom integration enabled. While some filter options may overlap, others will be specific to each integration. Accounts with both integrations enabled will have access to a combined set of filter options, providing a superset of both.

Table 1: Filter options

Filter name	Options	Description	Available with the MiVB integration	Available with the Zoom integration
Asset	Account	The customer account for this CloudLink integration.	X	X
	DID	Direct Inward Dialing numbers.	X	
	DN Range	Directory Numbers, or extensions, that are reserved for user assignment.	X	
	Group	A MiVoice Business system group is based on the following types: • ACD Skills • Pickup • Ring • Page • Hunt groups (voice and emergency)	X	
	Group Membership	User's Directory Numbers added to the MiVoice Business system groups.	X	

Filter name	Options	Description	Available with the MiVB integration	Available with the Zoom integration
	PBX User Profile	The base description of a user in the PBX, contains information like first name, last name, etc.	X	
	Phone	A device that is associated with a user.	X	
	Templated Services	UCC applications deployed for the user based on the definitions in the User Templates learned from the solution.	X	
	User License	The license assigned to a user on Zoom.		X
	Tenant	The Account ID associated with the customer's Zoom account.		X
Action	Create	Events where the asset was created.	X	X
	Delete	Events where the asset was deleted.	X	X
	Edit	Events where the asset was edited.	X	X
	License Assignment	Events where the asset (such as User License) was assigned.		X
	License Configuration Update	Events where the asset (such as User License) was updated.		X
	License Removal	Events where the asset (such as User License) was removed.		X
Event Type	Admin	Events of type Admin are related to the CloudLink configuration.	X	

Filter name	Options	Description	Available with the MiVB integration	Available with the Zoom integration
	MiVB	Events of type MiVB are related to Mitel Administration actions for MiVoice Business solutions.	X	
	Service Delivery	Events of type Service Delivery are related to Mitel Administration actions specific to the Zoom integration.		X
Actor ID	Enter the desired Actor ID	The CloudLink ID or System ID of the entity that triggered the event.	X	X
Event Date	Use the calendar to select a date and time range. You can select: • just a start date • just an end date • both a start date and an end date Custom start and end times can also be specified.	The date and time range within which the events must have occurred.	X	X

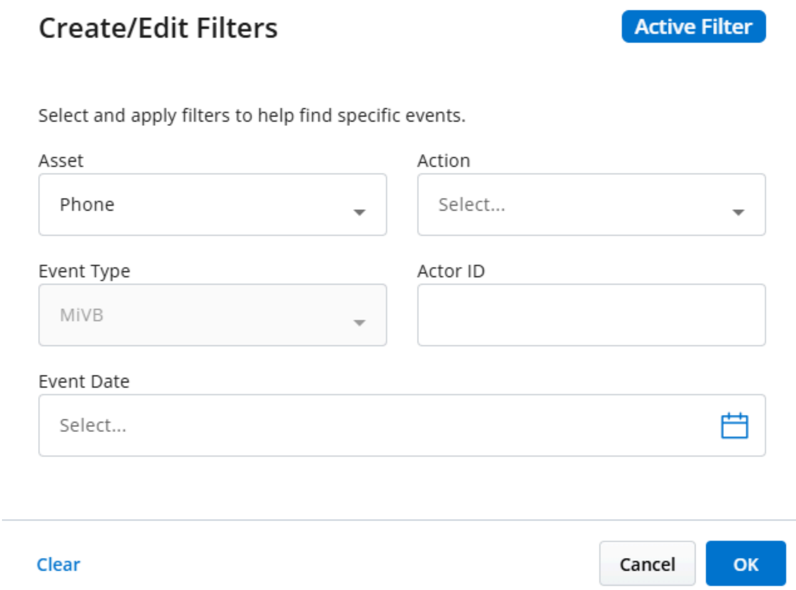
When both integrations are enabled for an account, you can search for events related to a specific integration by selecting filter options that are only available for that integration.

For example, to filter events related to the Zoom integration, you can do one or more of the following:

- From the **Event Type** drop-down list, select **Service Delivery**
- From the **Asset** drop-down list, select **User License** or **Tenant**
- From the **Action** drop-down list, select **License Assignment**, **License Configuration Update** or **License Removal**.

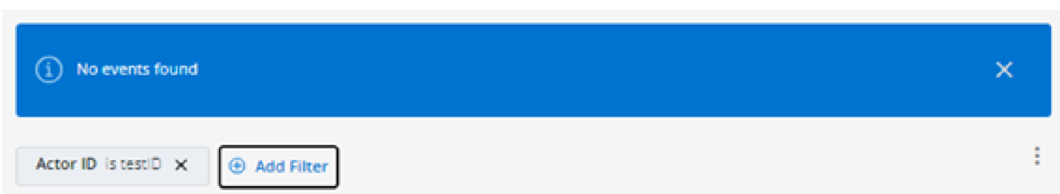
The filter feature is a smart filter, therefore the options will change depending on the filters that have already been applied/selected.

For example, if you select **Phone** as the **Asset**, the only available **Event Type** option will be **MiVB**, as all phone-related events are categorized under **MiVB** (for example, the **Admin** Event Type will not be applicable).



After selecting all the desired filter options, click **OK**. The Event History table will update to show events that match the selected filters.

If no events are found, the following banner is displayed:



.

Editing the active filter

To edit the active filter, do the following:

1. Click in the **Active Filter Details** section.

   The **Create/Edit Filters** page opens.
2. Update the desired information.
3. Click **OK** or **Apply**.

The filter details are updated, and the Event History table refreshes to show events that match the updated filters.

Deleting the active filter

To delete the active filter, click in the **Active Filter Details** section.

The Event History table refreshes and shows all available events for the account.

2.17 System Inventory

System inventory tracks on-premise software and hardware assets, providing Partner and Customer Administrators with a comprehensive view of their deployments.

Accessing System Inventory

1. Log in to the Mitel Administration on page 1 as a Mitel Partner or Account Administrator.
2. Navigate to **Accounts** and select the account of interest.
3. Navigate to **System Inventory**.

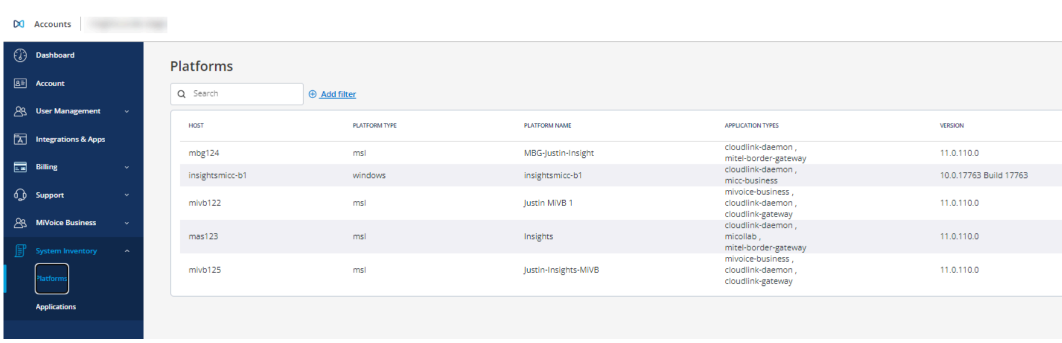
> **Note**:
> System Inventory is dependent on CloudLink Daemon (which is available to configure in MSL11.0.110 and 12.1 or higher). For more information on CloudLink Daemon, refer CloudLink Daemon Solution Guide.

4. Select Platforms or Applications to view the inventory details.

System Inventory has two views, **Partner** view and **Customer** view. Both the views are available for **Platforms** and **Applications.**

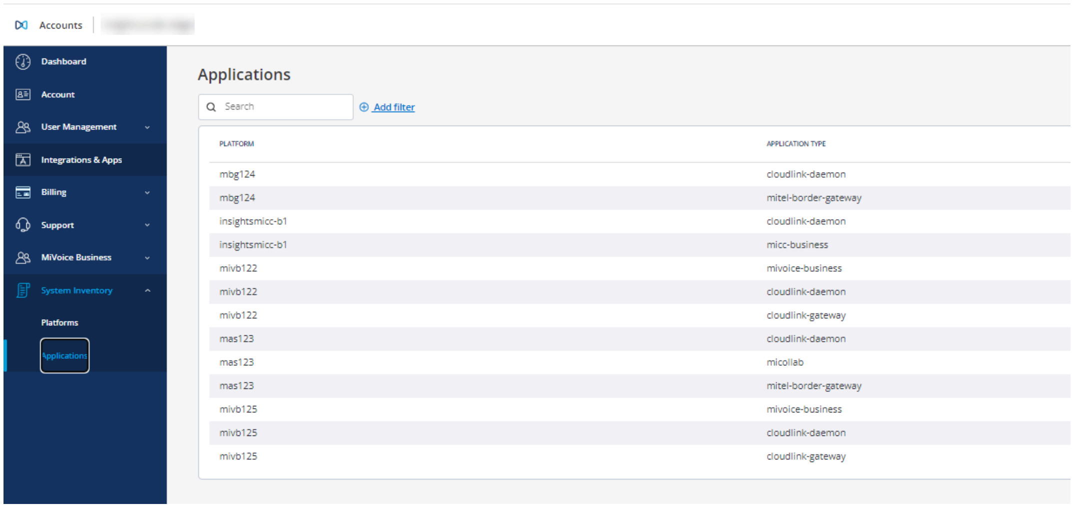
Partner view

The Partner view displays inventory for all customers associated with the partner. It includes an Accounts drop-down list for filtering the displayed accounts.



Customer View

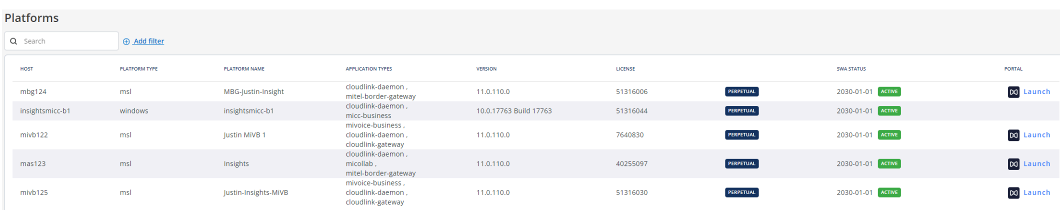
The Customer view presents the inventory specific to the selected customer without the necessity to filter by accounts. This view can be accessed by logging in with either Customer Admin or Partner Admin credentials.



2.17.1 Platforms

The Platforms component displays inventory across all of the Partner's customers.

When **Platforms** component is selected, it might take around 10 seconds to load Platforms page.



Platforms Details

Platforms table has the following features:

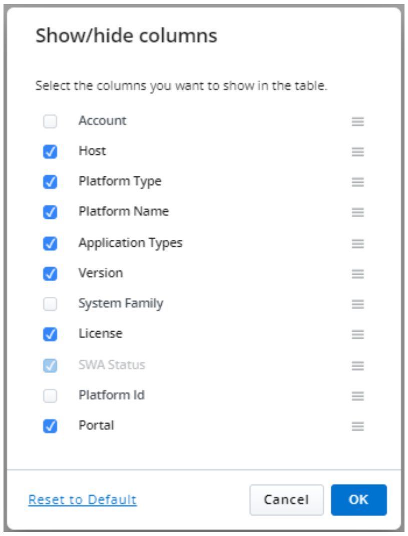
Name	Description
ACCOUNT	Name of the account.
HOST	Hostname of the platform
PLATFORM TYPE	The platform type or category (for example, MSL, MiVoice Business).
PLATFORM NAME	Name of the platform.

Name	Description
APPLICATION TYPES	Type of application (for example: mivoice-business, cloudlink-daemon, cloudlink gateway, mitel-border-gateway).
SYSTEM FAMILY	Operating system type (for example: linux and windows).
LICENCE	License number of the platform.
VERSION	Version of the platform.
SWA STATUS	SWA status of a platform.
PLATFORM ID	ID of a platform.
PORTAL	The Launch  button is displayed to connect to the platform.

Platform Table

1. The columns displayed can be customized:

- Click the ⋮ icon, select **Show/hide columns**.
- In the pop-up, select the checkbox(es) of interest. **SWA Status** is grayed out as it's a fixed column.



- Rearrange the columns by dragging the ≡ icon as desired.

2. **Filtering Data**

To search for particular platform, add filters to the table by using the **Add Filter** Add Filter button.

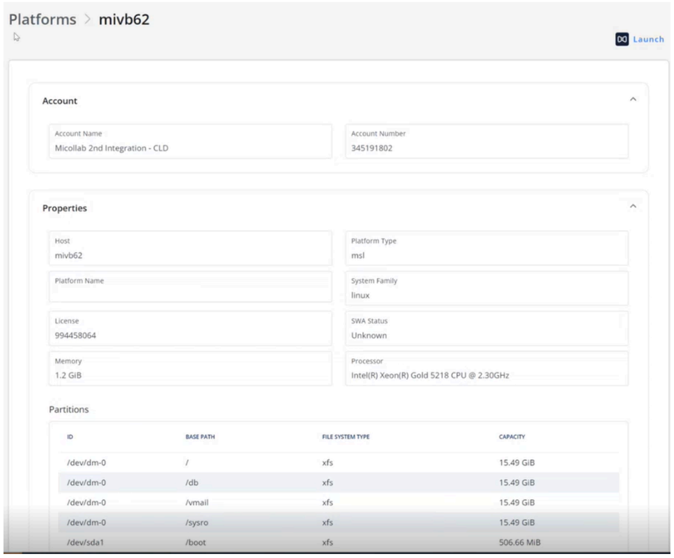
Filter name	Options	Description
Platform Type	msl	Mitel Standard Linux platform type
	windows	Windows platform type
System Family	Linux	Linux (Operating System)
	Windows	Windows (Operating System)
Application Types	mivoice-business	MiVoice Business application
	cloudlink-gateway	CloudLink Gateway Portal application
	mitel-border-gateway	Mitel Border Gateway application

Filter name	Options	Description
	micollab	MiCollab application
License Type	Unlicensed	If the license ID is not found.
	Subscription	Monthly subscription license
	Perpetual	CapEx license
SWA Status	Not Indicated	License without expiration date
	Active	Active subscription or perpetual license with more than 90 days until expiration
	Inactive	Subscription license that has exceeded its expiration date
	Expiring soon	Perpetual license with an expiration date within 90 days
	Expired	Perpetual license that has expired

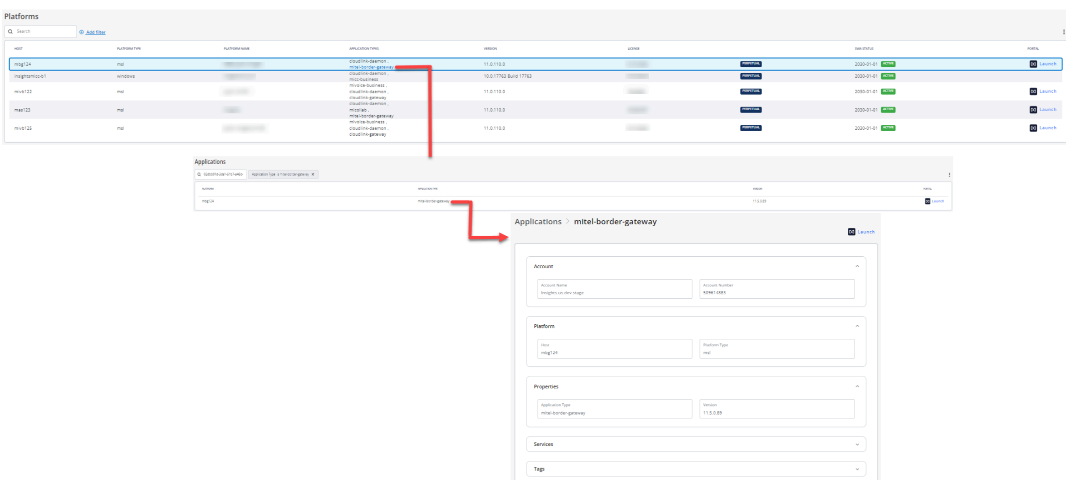
Individual platform details

Click a row on the Platforms table, the details of the selected platform is displayed. The **Launch** button is displayed based on the selected platform.

The Launch button seamlessly presents the administration console of the Platform (example: MSL Server Manager). Clicking the Launch button generates a URL with a unique, secure connection to either platform or application for each use.



When multiple application types are associated with an account, select one to view its details. The selected application type details are displayed in a table format. To access further information, click on the application type once more, and a detailed view is displayed. An example screenshot is shown below:



2.17.2 Applications

The Applications component offers a customer view of inventory, similar to the Platforms component. However, it presents a more streamlined set of information, focusing on customer-specific details and omitting broader data that is available in the Platforms view.

Applications

Search | Add filter

PLATFORM	APPLICATION TYPE	VERSION	PORTAL
mbg124	cloudlink-daemon	1.7.8+52	
mbg124	mitel-border-gateway	11.5.0.89	Launch
insightsmicc-b1	cloudlink-daemon	1.7.8-develop+870	
insightsmicc-b1	micc-business	10.2.09104.1	
mivb122	mivoice-business	10.0.1.18	Launch
mivb122	cloudlink-daemon	1.7.8+52	
mivb122	cloudlink-gateway	2.4.6-05	
mas123	cloudlink-daemon	1.7.8+52	
mas123	micollab	9.8.2.6-01	Launch
mas123	mitel-border-gateway	11.5.2.35	Launch
mivb125	mivoice-business	9.4.1.17	Launch
mivb125	cloudlink-daemon	1.7.8+52	
mivb125	cloudlink-gateway	2.4.6-05	

The Launch button seamlessly presents the administration console of the Application (example: MiVoice Business System Administration portal). Clicking the Launch button generates a URL with a unique, secure connection to either platform or application for each use.

Within the Applications component, the **Add filter** feature includes the *Application Type* option, allowing users to refine their search based on the types of applications available.

Mitel Administration Integrations 3

This chapter contains the following sections:

CloudLink supports integration with other Mitel and third-party applications to enable provisioning of users into the CloudLink database and to enable communication between on-premises solutions and feature-rich cloud-based applications.

Note:

- By default, **Chat** integration is always enabled for a customer account.
- If an account has a subscription assigned for an application and the application is not integrated with CloudLink, a warning message is displayed.

Adding an integration to a customer account

To add integrations to a customer account:

1. Access the **Integrations** page by doing either of the following:

   - From the **Account Information** page:

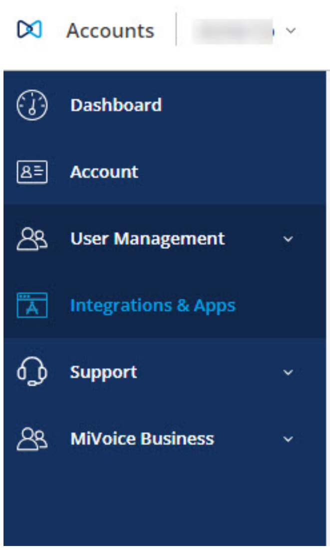
     Access the **Account Information** page of the customer account by doing the following.

     a. A Mitel Partner must click the account from the **Accounts** page.
     b. An Account Admin of the account must click the **Account** option from the navigation menu on the left side of the Accounts Console **Dashboard**.

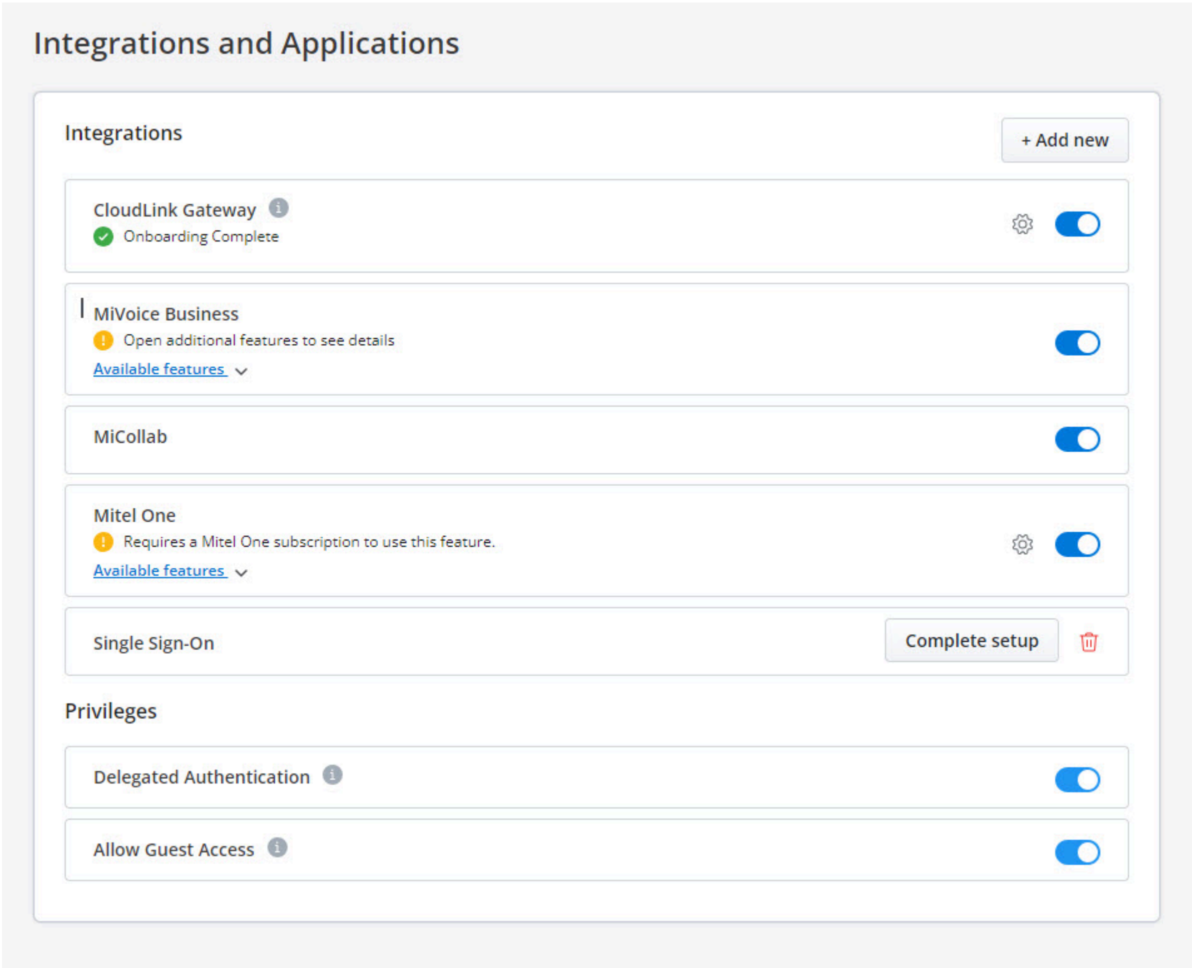
     The **Account Information** page opens, and the **Integrations** panel is displayed in the bottom half of the page.

   - From the **Integration & Apps** option:

     Click the **Integration & Apps** option from the navigation menu on the left side of the Accounts Console Dashboard.



2. In the **Integrations** panel, click **+ Add new**. A pop-up screen displays the available integrations.



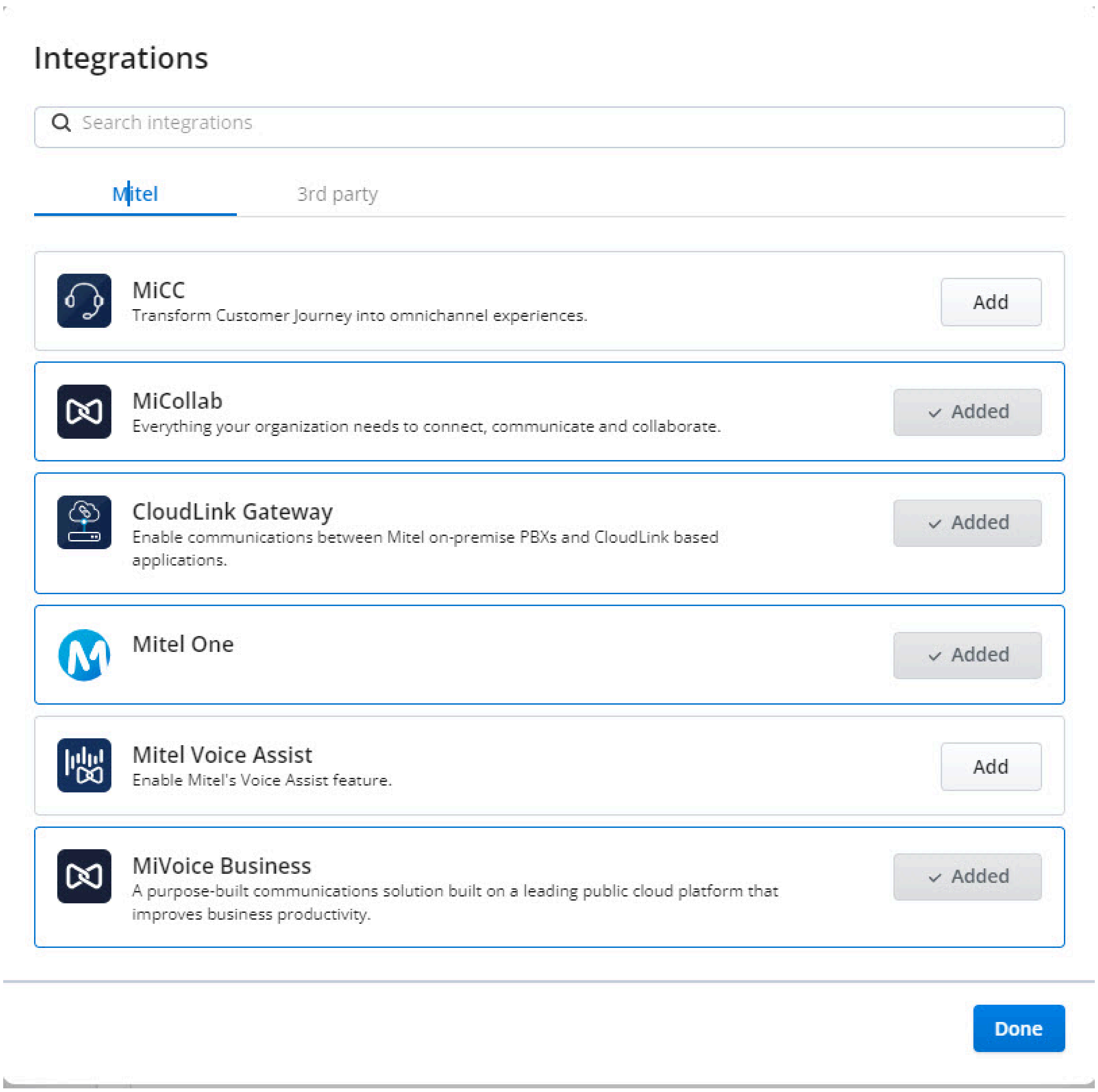
Note:

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

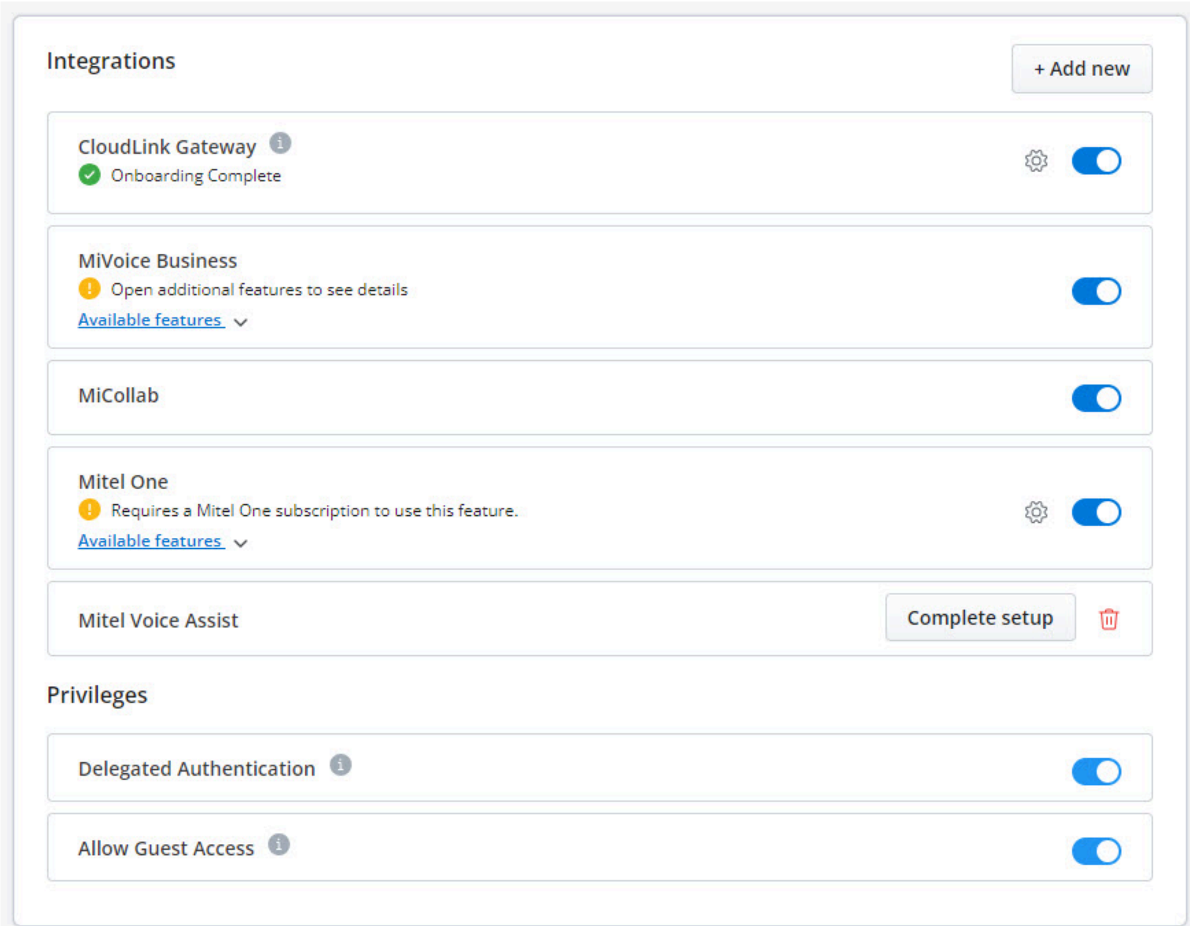
3. Choose the type of integration you want to add by clicking the corresponding tab, **Mitel** or **3rd party**:

- The **Mitel** tab displays all the supported Mitel integrations.
- The **3rd party** tab displays a list of supported third-party integrations.

4. Click the **Add** button associated with the integration and click **Done**.



The integration is added to the customer account and is added to the **Integrations** panel.



Removing an integration from a customer account

To remove an existing integration from a customer account:

1. Access the **Integrations** page by following the instructions mentioned in Step 1 of Adding an integration to a customer account on page 88.
2. From the **Integrations** panel that opens, remove the integration using one of the following methods:
    - Disable the toggle button associated with the integration in the **Integrations** panel.
    - In the Integrations panel, hover over the **Added** button associated with the integration and click **Remove**.

The following topics provide information on how to integrate a CloudLink account with the various Mitel applications, and third-party applications.

3.1 Integrating Mitel Applications with Mitel Administration

CloudLink supports integration with Mitel applications such as Mitel One, CloudLink Gateway, MiTeam Meetings, MiCollab, and Mitel CX to enable communication between on-premises solutions and feature-rich cloud-based applications.

Mitel One Integration

Adding Mitel One integration to a customer account allows the users in the account to access the Mitel One application. The Mitel Partner or the Account Admin can manage the Mitel One features for each user in the account. For more information, see Mitel One Integration.

Mitel One Workgroups Integration

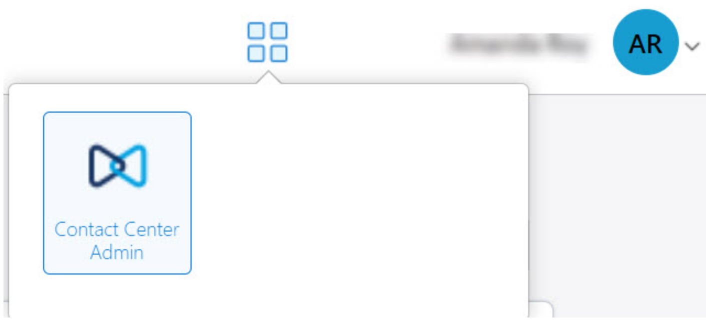
Adding Mitel One Workgroups integration to a customer account allows the Mitel Partner or an Account Admin to access Workgroups portal. After the integration is added, the **Customer Care** option is displayed on left navigation menu of Account console. For more information see, Mitel One Workgroups Integration.

CloudLink Gateway Integration

Adding CloudLink Gateway integration to a customer account allows the Mitel Partner or Account Admin to associate the gateway with the customer account, configure and connect a PBX, and to deploy a CloudLink application for all the users in the account. For more information, see Integrating CloudLink Gateway with Mitel Administration on page 95.

MiCC Integration

Adding MiCC integration to a customer account allows the Mitel Partner or the Account Admin to access the Contact Center Admin Portal. After the integration is added, the Contact Center Admin icon appears at the top right of the Accounts Information page. Click the icon and from the dialogue box that opens, click **Contact Center Admin**. The **Chat Overlays** page opens. You can create new chats from this page. For more information about creating chats, see the section ***Chat Overlays*** in Integration Guide for MiContact Center with Google Contact Center AI.



MiTeam Meetings Integration

Adding MiTeam Meetings integration to a customer account allows all the users in the account having a valid MiTeam Meetings subscription to access the MiTeam Meetings application. For more information, see MiTeam Meetings Integration on page 144.

MiCollab Integration

Adding MiCollab integration to a customer account enables CloudLink Chat in the MiCollab application of all the users in the account if the MiCollab Administrator has enabled CloudLink Chat on the MiCollab Server. For more information about enabling CloudLink Chat on MiCollab Server, see MiCollab CloudLink Solution Document.

Unify Phone Integration

Adding Unify Phone Integration to a customer account supports two primary use cases:

- When **Unify Phone** is already configured to work with an **OpenScape PBX**, it enables CloudLink Chat within the Unify Phone application.
- When a **MiVoice PBX** is linked to the CloudLink customer account, it allows users who exist in both the PBX and the CloudLink account to access the Unify Phone application and use both telephony and CloudLink Chat features offered through the application.

For more information, see Unify Phone Integration on page 159.

Privileges Associated with Integration

When an integration is added to a customer account, the specific privileges associated with that integration are also enabled for that account. A Mitel Partner or Account Admin can also enable or disable these privileges for the users in an account without adding integrations separately by using the toggle buttons associated with each of these privileges in the **Privileges** section. When an integration is removed for an account, the corresponding privileges will also be disabled if there is no other integration that shares those privileges.

The following table describes the privileges that are enabled when a Partner or Account Admin enables the integration toggle button for each integration for an account.

Integration	Function
Mitel One	Mitel One has Allow Guest Access as the privilege as sociated with it by default. Therefore, when the Mitel O ne toggle button is enabled, this privilege is automatic ally enabled and added to the account.
MiCC	MiCC has Delegated Authentication and Allow Guest Ac cess as the privileges associated with it by default. Th erefore, when the MiCC toggle button is enabled, these two privileges are automatically enabled and added to the account.
MiTeam Meetings	MiTeam Meetings has Allow Guest Access as the privil ege associated with it by default. Therefore, when the M iTeam Meetings toggle button is enabled, this privilege is automatically enabled and added to the account.
MiCollab	MiCollab has Delegated Authentication as the privilege associated with it by default. Therefore, when the MiColl ab toggle button is enabled, this privilege is automatic ally enabled and added to the account.

Privileges

Delegated Authentication

Delegated Authentication allows authorized clients in the account to request user tokens on behalf of the users in the account. This allows any server managing the account, such as the MiCollab or MiContact Center server, to use CloudLink features such as Chat service.

Allow Guest Access

When the Allow Guest Access privilege is enabled on an account, it will allow guest-level access to the account for anonymous users who do not actually exist in the account. This allows features such as Guest chat to function; that is anonymous external users can chat with verified users in the account.

Note:
For an integration associated with an account, even if all the privileges for the account are disabled, the integration continues to be associated with that account. However, the integration might not work correctly.

The following topics provide information on how to integrate a CloudLink account with the various Mitel applications.

3.1.1 Integrating CloudLink Gateway with Mitel Administration

After you create a customer account in the Accounts console, you can begin the deployment of the CloudLink Gateway to associate the Gateway with the customer account, configure and connect a PBX, and to deploy a CloudLink application for all the users.

Onboarding the Gateway

To onboard a gateway, that is, 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 for the first time as indicated below:

- For **standalone** platforms, which have an external gateway, access Mitel Administration:
  - by entering the IP address of the gateway appliance in a supported browser.
  - by connecting a supported browser to the gateway at http://cloudlink.local/.

  Note:
  mDNS must be supported in your system in order to access the gateway using http://cloudlink.local/. For Windows, this support can be downloaded and installed with Bonjour Print Services.

  You must do this from a computing device located on the same LAN subnet as the CloudLink Gateway. For more information, see Access the CloudLink Gateway. After successful login, the gateway will redirect you to Mitel Administration.
- For **SMBC** platforms, which have an embedded gateway, access the Mitel Administration from the SMB Controller Manager. Log into MSL Server on the SMBC. Select **Blades** > **Install** > follow the steps. For

more information, see Access the CloudLink Gateway. After successful login, the gateway will redirect you to the Mitel Administration.

The gateway (on a standalone platform or SMBC platform) will be properly associated with the customer account when you complete Step 2 in Configuring the CloudLink Gateway.

Accessing the Mitel Administration

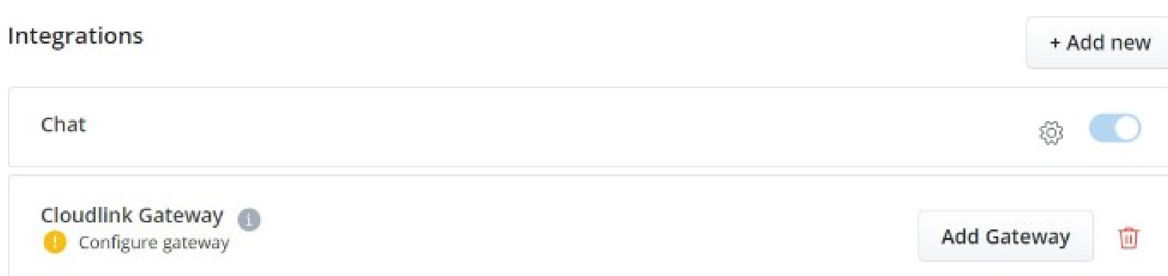
After you have associated an account with a gateway, you can access the Mitel Administration to manage customers in the following different ways:

- By connecting to the gateway at http://cloudlink.local/ from a computing device located on the same LAN subnet as the CloudLink Gateway. (for standalone platforms only)
- By entering the IP address of the gateway appliance in a supported browser from a computing device located on the same LAN subnet as the CloudLink Gateway. (for standalone platforms only)
- By accessing the Application configuration link in the SMB Controller Manager (for SMBC platforms only)
- By accessing Mitel MiAccess at https://connect.mitel.com/, and then clicking **Mitel Administration** from the left navigation panel.
- By accessing the Mitel Administration directly at https://accounts.mitel.io/.

Adding CloudLink Gateway Integration

After logging in to the Mitel Administration, add the CloudLink Gateway integration to a customer account by performing the steps mentioned in Adding an integration to a customer account on page 88.

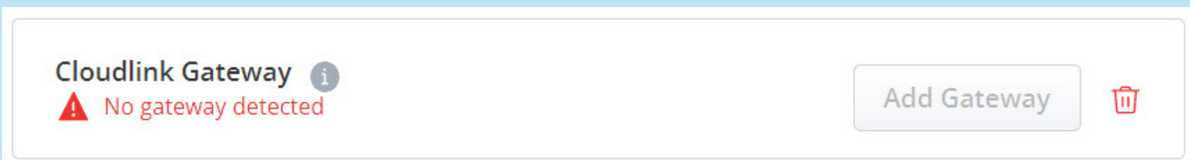
After you have added CloudLink Gateway integration to the customer account, **CloudLink Gateway** will be listed in the **Integrations** panel and a status message **Configure Gateway** will appear indicating that you need to configure the gateway to continue with the integration process.



Note:
The status message that appears beneath CloudLink Gateway might indicate the following:

- the subsequent step that needs to be done to configure the gateway.
- an error message, warning that there is an issue with the gateway.
- an alert message, notifying that there is a software update available.

Note:
If the status message No gateway detected is displayed, you must first access the Mitel Administration portal by following the steps described in Onboarding Gateway.



Status Messages

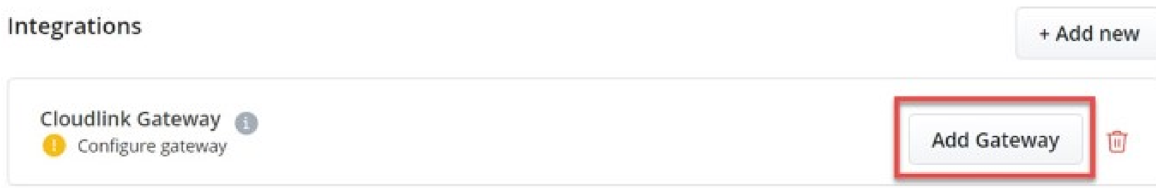
The following are the common status messages that indicate the next step to be completed for configuring the CloudLink Gateway.

- No gateway detected
- Configure gateway
- Add PBX (for standalone platforms) or Sync PBX (for SMBC platforms)
- Connect the PBX
- Deployment

Onboarding the CloudLink Gateway

After enabling the CloudLink Gateway integration in Mitel Administration, you must add a gateway to the customer account, configure that gateway, and sync a PBX to the account to deploy CloudLink applications to the users in the account. To do this, complete the following steps:

1. From the **Integrations** section of the **Account Information** page, click **Add Gateway**.



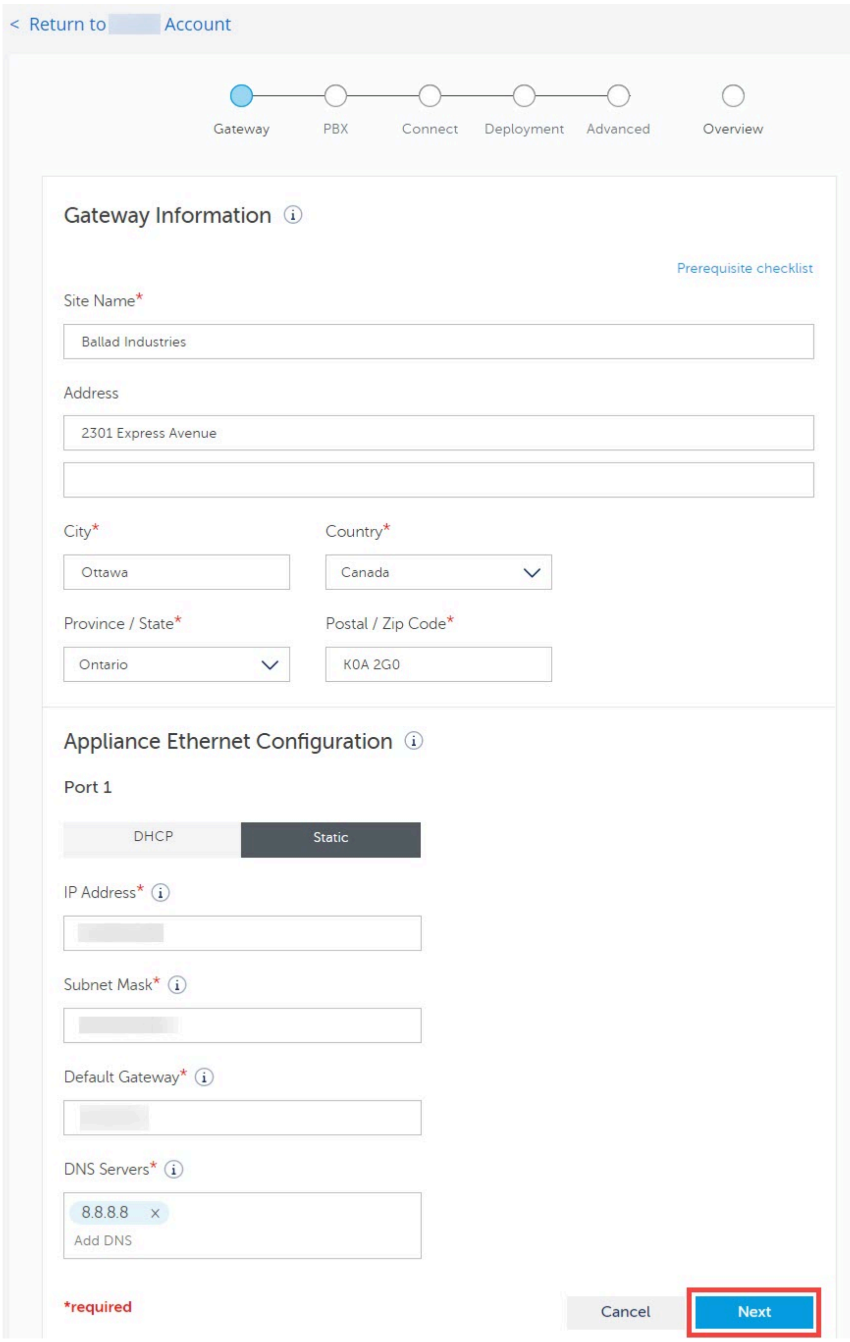
The **Gateway** page opens.

> **Note**:
> Any time during the configuration process, click the **Return to XXXX** (Account Name) option to return to the previous page (**Integrations & Applications** page or **Account Information** page).

2. In the **Gateway** page, within the **Gateway Information** dialog, enter the site name, the complete address for the physical location of the PBX if it is different from your business address (populated by

default), and configure the Ethernet ports on the external Gateway appliance or on the virtual machine. For more information about entering these details, see Configure the Customer Site.

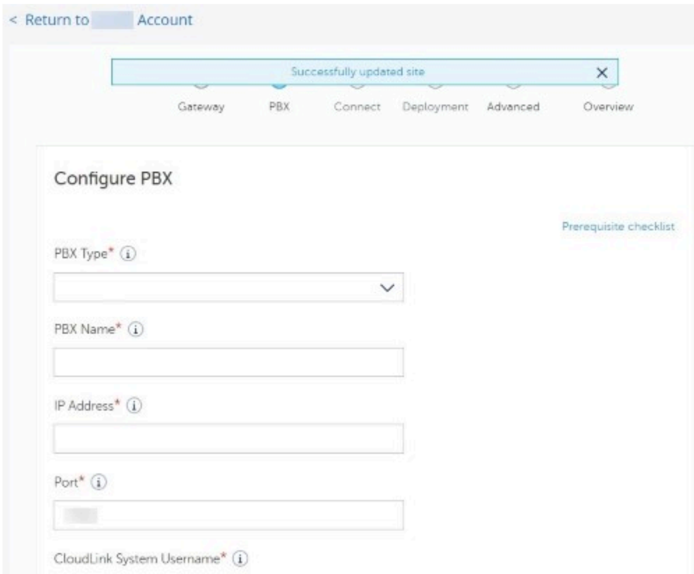
After entering these details, click **Next** to configure and register the gateway.



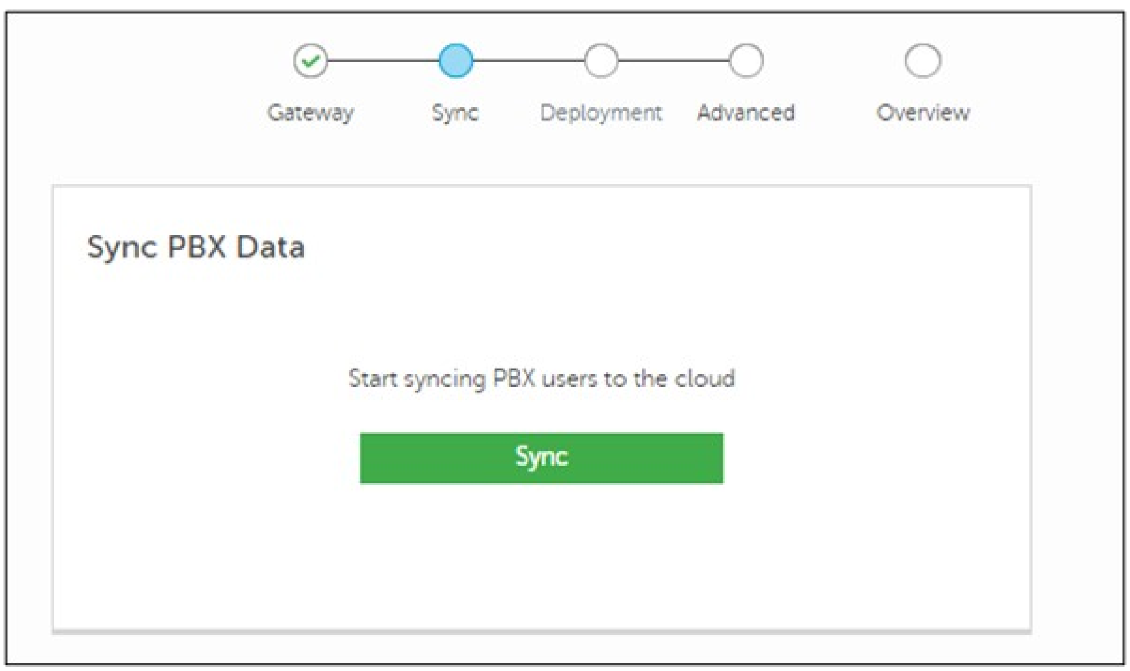
The Accounts console tries to establish a connection with the CloudLink Gateway. When a successful connection is established, the CloudLink Gateway is linked to the customer account, a pop-up message

Successfully updated site is displayed, and the following page opens depending upon the platform in which you are deploying the gateway.

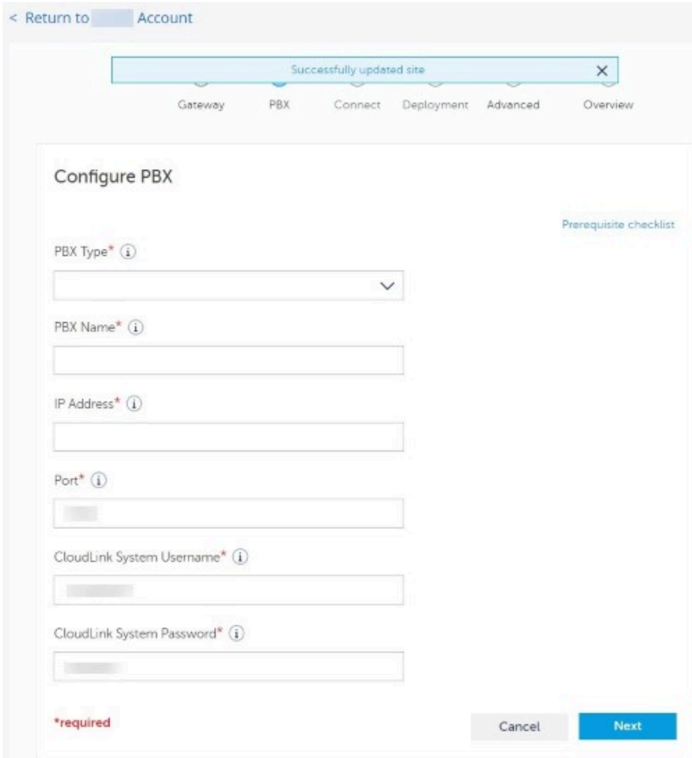
- For standalone platforms, the **PBX** page opens displaying the **Configure PBX** dialog. Proceed to Step 3 to provide the PBX details.



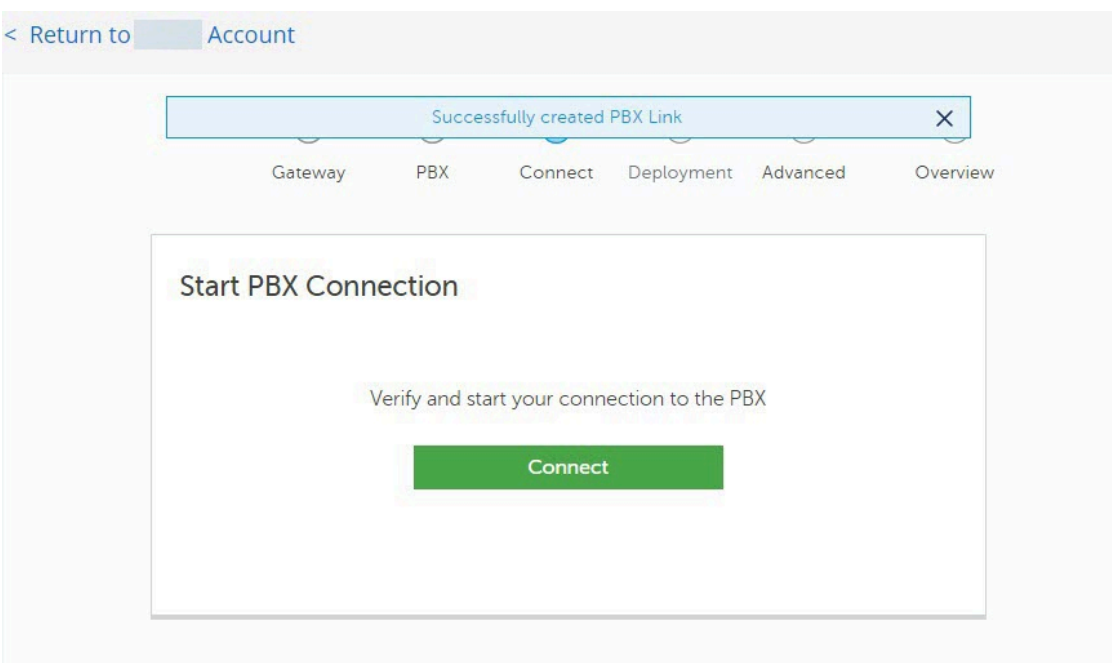
- For SMBC platforms, the **Sync** page opens displaying the **Sync PBX Data** dialog. Skip Step 3 and proceed to Step 4 to continue the onboarding process.



3. To add and configure the PBX for your account, enter the information specific to your PBX in the fields provided. For more information about entering the PBX details, see Enter PBX Information. After entering all the necessary details, click **Next**.

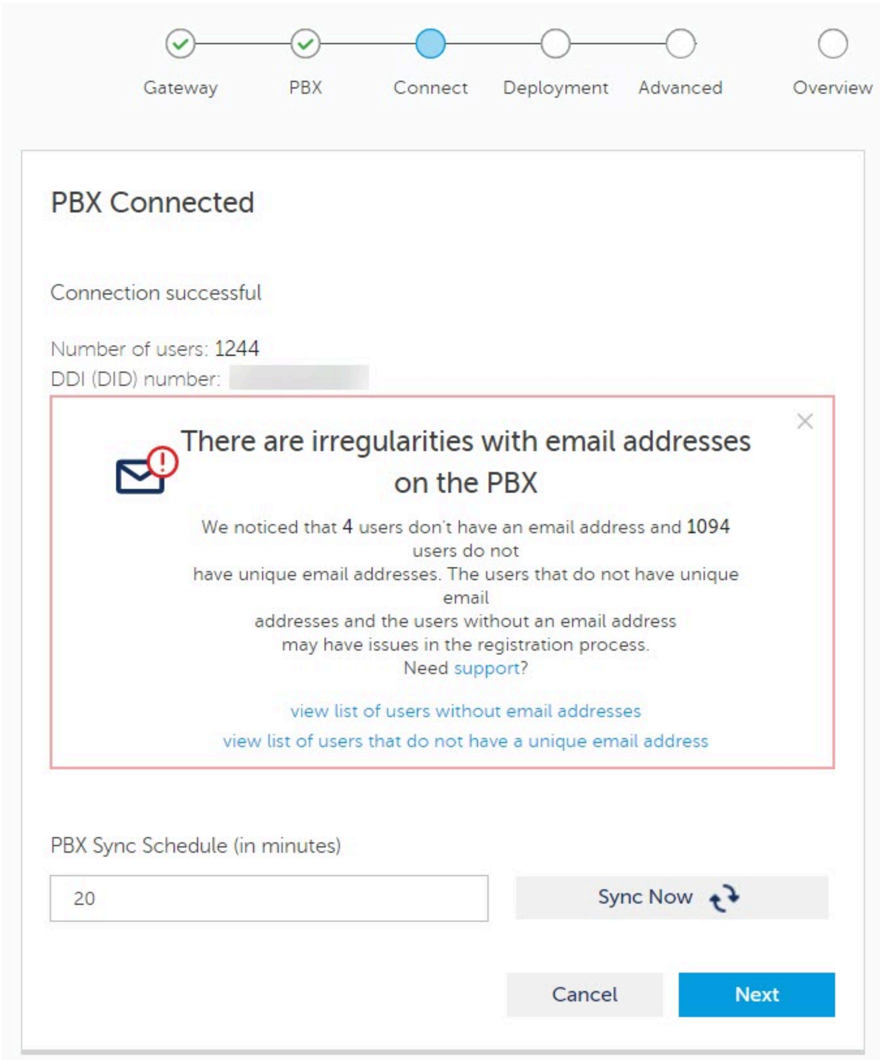


When the configuration is successful, a pop-up message **Successfully created PBX Link** is displayed, and the **Connect** page opens displaying the **Start PBX Connection** dialog.



4. To connect or sync the PBX with the customer account, click **Connect**. The Accounts console tries to establish a connection with the PBX. When a successful connection is established, the **PBX**

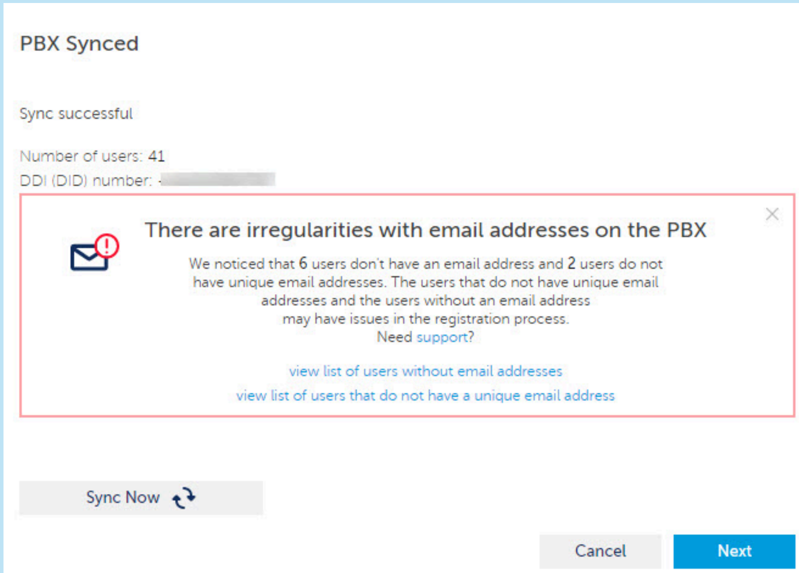
Connected dialog is displayed, along with the **Connection successful** message. For more details, see Connect or Sync the PBX.



By default, the synchronization occurs every 20 minutes. You can modify the sync interval by entering the number of minutes in the **PBX Sync Schedule** field.

Note:

- For SMBC platforms, you can not modify the sync interval. Following **PBX Synced** dialog box is displayed.

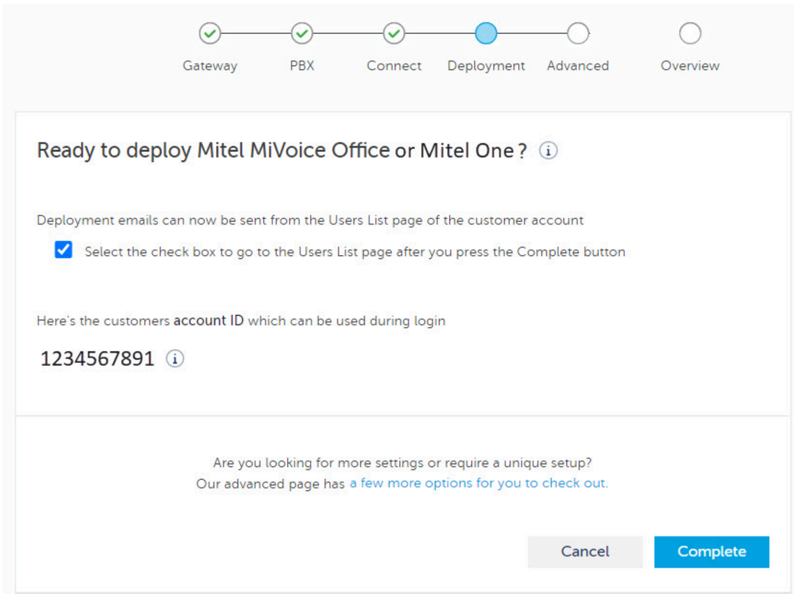


- Do not click **Sync Now** immediately after you have connected the PBX. By default, automatic synchronization is initiated.

If there is a warning regarding missing email addresses of users, make all the necessary corrections and modifications on the PBX. Then click **Sync Now** to manually trigger the synchronization without waiting for the next scheduled run. Once the warning messages are resolved, click **Next**. The **Deployment** page opens.

5. (Optional) You can use the **Deployment** page if you want to deploy the CloudLink application associated with your PBX by sending deployment emails to the imported users so they can register their account and receive introductory information about the application.

   Sending deployment emails can be done any time from the **Users** page in the Mitel Administration. To navigate to the **Users** page, select the **Select the check box to go to the Users List page after you press the Complete button** check box and click **Complete**.



   If you click **Complete** without selecting the check box, you will be taken to the previous page in Mitel Administration. You can then access the **Users** page by clicking the **Users** option displayed in the navigation menu in the left side of the Accounts Console.

   In the **Users** page:

   - To send deployment email to all the users in the customer account at once, click the **Manage** option and click **Send Mitel Office deployment emails to all** (for MiVoice Office 400).
   - To send deployment email to selected users, select the users from the **Users** page, click the **Manage** option, and click **Send Mitel Office deployment emails** (for MiVoice Office 400).

6. After successful configuration of the gateway, **CloudLink Gateway** will be listed in the **Integrations** panel as shown below.

   If an error message is displayed, see Troubleshoot Errors for information about resolving errors. Click the icon to view or modify the configuration.

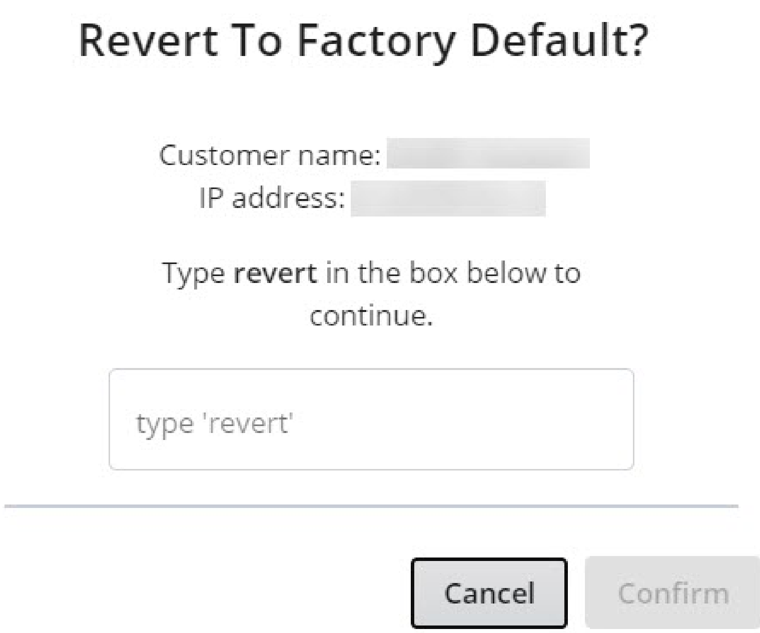
Deleting an Existing Integration

Use the following steps to delete the CloudLink Gateway integration for a customer account.

1. Depending on the stage of integration do either of the following:

   - For incomplete integration click the Delete icon ( ) associated with **CloudLink Gateway** from the **Integrations** section of the **Account Information** page.
   - For complete integration disable the toggle button associated with **CloudLink Gateway** from the **Integrations** section of the **Account Information** page.

   From the **Integrations** section of the **Account Information** page, click the Delete icon ( ) associated with **CloudLink Gateway**. A **Revert To Factory Default?** panel opens.

   > **Note**:
   > This panel is displayed only if you are deleting the integration in a customer account that has a physical gateway appliance onboarded. This panel will not be displayed if you onboard a virtual gateway appliance.

2. Type **revert** in the field provided and click **Confirm**. The CloudLink Gateway integration is deleted from the customer account and the gateway will be reset.

Note:
A CloudLink Gateway that is added to a customer account (for which integration is enabled and the gateway is connected) will reset if the customer account is deleted by a Partner.

3.1.2 MiVoice Business Integration

Mitel Partners and Account Admins can now integrate, enable, and manage MiVoice Business features from the Mitel Administration. It provides a seamless day-to-day user management experience. It allows the Mitel Partner and Administrators to manage the MiVoice Business solution from the Mitel Administration. You can manage features such as templates, telephony services, and call handling rules for a user.

Following are the instructions for integrating MiVoice Business with CloudLink Platform.

Prerequisites

Ensure that you have the following before you proceed to integrate MiVoice Business with CloudLink:

- Gateway integration enabled. For more information about enabling and configuring Gateway, see Integrating CloudLink Gateway with Mitel Administration on page 95.

Integrating MiVoice Business with CloudLink Account

To integrate MiVoice Business in a customer account, perform the following steps:

1. Log in to the Mitel Administration on page 1.
2. Access the **Integrations** panel from the **Account Information** page or from **Integrations & Apps** option. For more information about accessing the **Integrations** panel and adding integration to a customer account, see Adding an integration to a customer account on page 88.
3. In the **Integrations** panel, click **+Add new**. A pop-up screen displays the available integrations.
4. Click the **Add** button associated with **MiVoice Business**. Expand to display the features available under **MiVoice Business**. Enable **Customer Admin Portal**.
5. Click **Done**. MiVoice Business is integrated with the customer account.

After MiVoice Business integration is added to an account, **MiVoice Business** appears in the **Integrations** panel in the left navigation pane.

Removing MiVoice Business Integration

To remove MiVoice Business integration from a customer account, perform the following steps:

1. Access the **Integrations** panel from the **Account Information** page or the **Integrations & Apps** from the left navigation menu. For more information about accessing the **Integrations** panel and adding integration to a customer account, see Adding an integration to a customer account on page 88.

2. From the **Integrations and Applications** page, in the **Integrations** panel, slide the toggle button associated with **MiVoice Business** to the left. The **Remove MiVoice Business Integration** dialog box appears.
3. Click **Remove integration**. The MiVoice Business integration is removed from the customer account.

For more information about managing MiVoice Business features from the Mitel Administration see, Managing MiVoice Business Features.

CloudLink Daemon for MiVoice Business Integration

Introduction

The CloudLink page enables the CloudLink Daemon, a software component designed for integration with various call servers and platforms. Acting as a user interface, the CloudLink Daemon connects Mitel CloudLink services with on-premises systems like Private Branch Exchanges (PBXs). This integration ensures smooth communication between cloud-based services and traditional on-site telephony infrastructure, enhancing both the functionality and flexibility of communication systems. CloudLink Daemon is available in Mitel Standard Linux (MSL) by default, and the version supported in MSL is 11.0.110 and higher for MiVoice Business Release 10.2

Enabling CloudLink Daemon

To enable CloudLink Daemon, perform the following:

1. Log in to the Server Manager.
2. Under **Configuration**, click **CloudLink.**
3. In the **CloudLink** page that opens, click **Enable CloudLink Integration**.

> **Note**:
> You will see a progress screen. The latest version of the CloudLink Daemon is installed. You can now see the CloudLink Daemon dashboard, where the version details of the installed CloudLink Daemon is mentioned.

Linking CloudLink Daemon to CloudLink

To link CloudLink Daemon to CloudLink, perform the following:

> **Note**:
> Linking your system to CloudLink allows you to easily manage Cloud applications at the edge. Toactivate, you will need a CloudLink account with administrator rights.

1. After Cloudlink Daemon in enabled, in the CloudLink Daemon page or dashboard that opens, click **Link to CloudLink**.
2. After the enabled CloudLink Daemon is linked to the CloudLink platform, the CloudLink Daemon dashboard displays the following details:

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

> **Note**:
> For the details on each of these functionalities, see to the *CloudLink Daemon Solution Guide*.

Enabling the Tunnel

Perform the following to connect the CloudLink Daemon for each component or to enable the tunnel:

1. In the standard view of the CloudLink Daemon dashboard, under **Tunnels**, select a component to connect or link to, and then click **Start**.

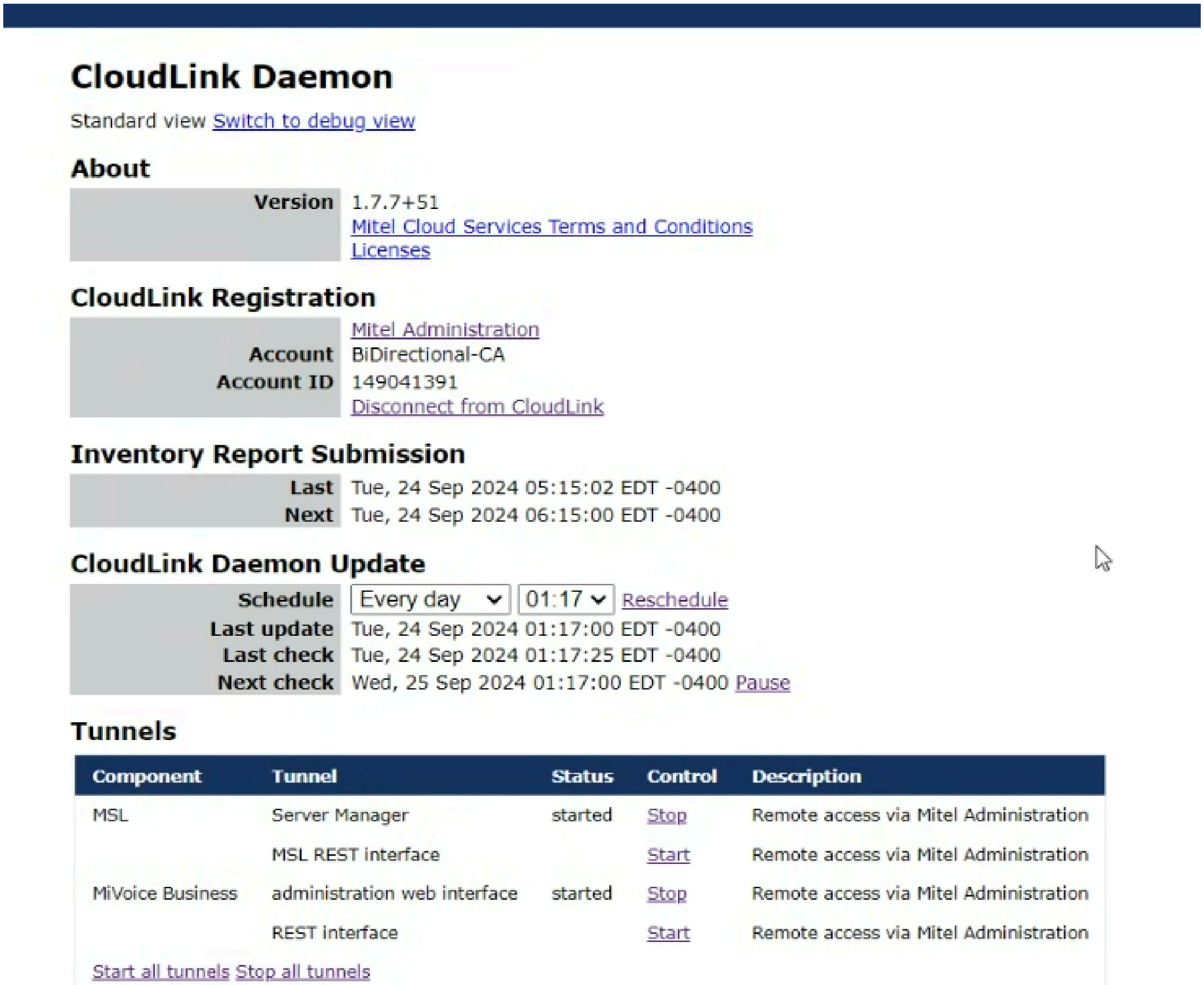


Figure 1: Enabling the tunnel

2. Click **Yes**.

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

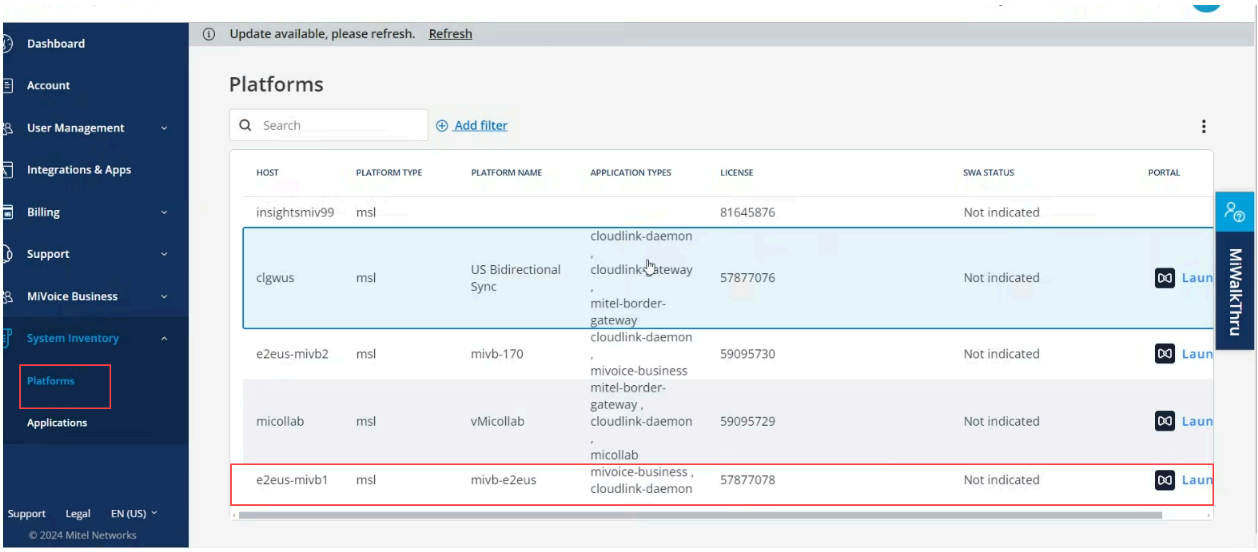


Figure 2: System Inventory > Platforms

4. Using the **Launch** button, you can remotely access the CloudLink Daemon for the respective platforms and applications. To use the remote management feature, you need to start the following tunnels:

- MSL Server Manager
- MiVoice Business

Note:
The System Inventory and Remote Management features will be enabled soon in the CloudLink on Mitel Administration.

Overview of MiVoice Business Submodules

The left navigation pane under **MiVoice Business** includes distinct configuration sections. Sub menu items appear in the following order, regardless of availability:

- Numbers
- Locations
- Emergency Services *(visible if Zoom integration is enabled)*
- Voice Gateway
- Tools *(visible if MiCollab is present)*

Numbers

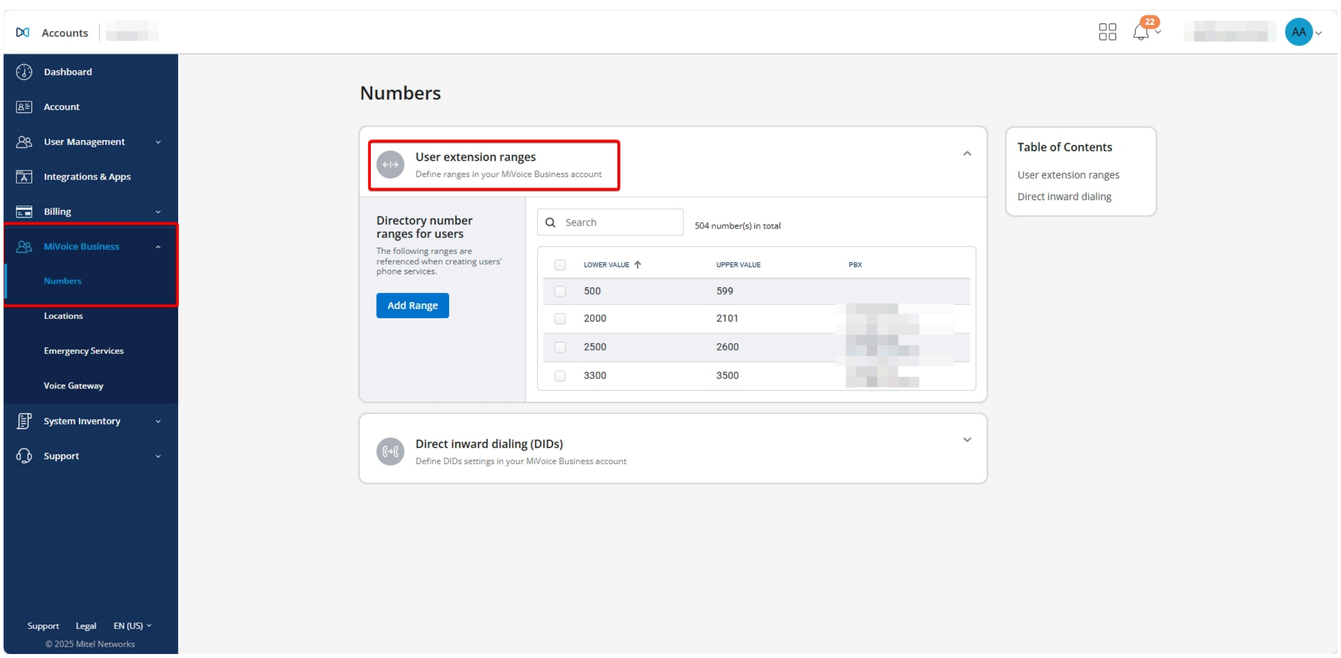
The **Numbers** submodule helps you manage extension ranges and assign Direct Inward Dialing (DID) numbers. You can use this section to configure number blocks, assign extensions to users or devices, and ensure accurate routing of incoming calls within the MiVoice Business system.

This submodule allows Mitel Partners or Account Administrators to add, edit, and delete user extension ranges and DID numbers. These ranges define the safe directory number (DN) blocks that can be used for user phone services.

Note:
The user extension ranges displayed here are defined by the Partner or the Customer Administrator as safe ranges to be used for the Users' phone services Directory Numbers (DNs). Do not overlap ranges for other purposes such as system groups, and so on. The next available DNs will be offered up, from these defined ranges, in the MiVoice Business Service edit when creating new Phone Services for a user.

User Extension Ranges

This section facilitates the ability of selecting the next available number when adding a directory number.



To add a user extension range, perform the following steps:

1. On the left navigation panel, click **MiVoice Business** and then click **Numbers**. The **MiVoice Business Settings** page is displayed.
2. In the **User extension ranges** section, click **Add Range**. The **Add Range** dialog box is displayed.

3. Enter a start and end number for the user extension range and click **Add**. The entered range will be displayed in the **User extension ranges** list.

To edit an existing user extension range, perform the following steps:

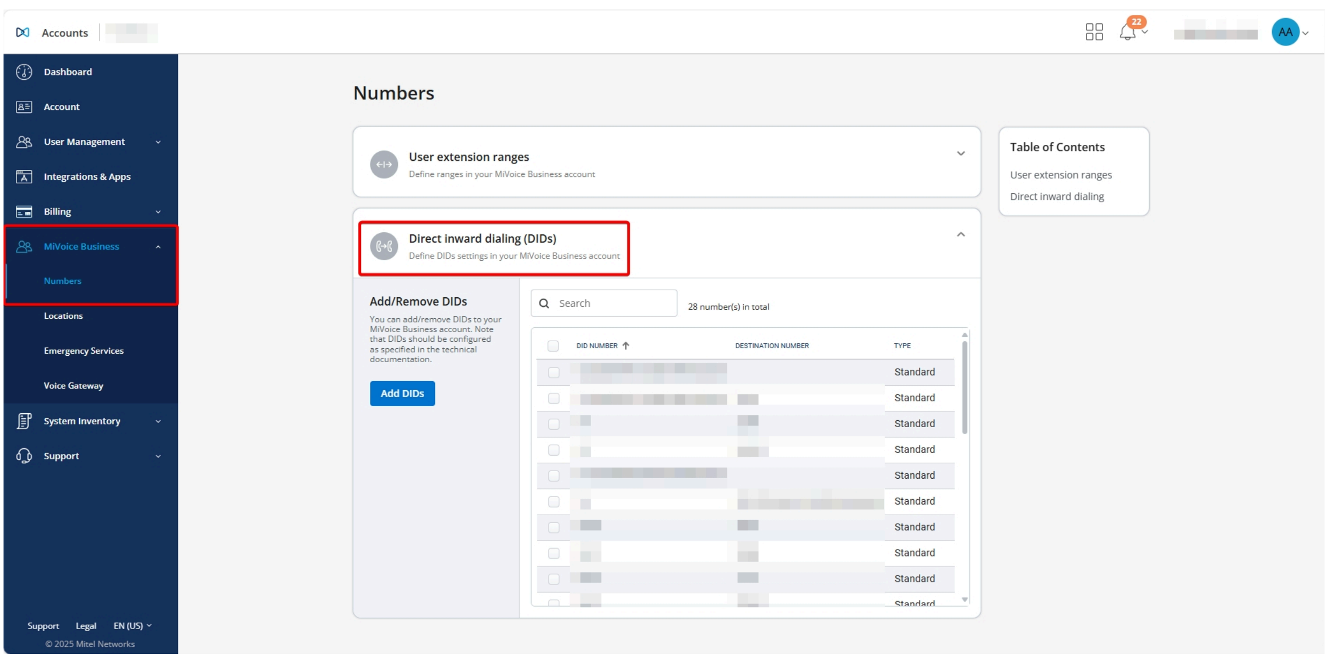
1. From the **User extension ranges** list, click the user extension range that you want to edit. The **Edit Range** dialog box is displayed.
2. Edit the user extension range and click **Save**. The modified extension range will be displayed in the **User extension ranges** list.

To delete user extension range(s), perform the following steps:

1. Select the check box(es) associated with the user extension(s) that you want to delete. The **Delete selected numbers** dialog box is displayed.
2. Click **Delete** to delete the selected user extension range(s). Clicking **Cancel** cancels the operation. The selected user extension range(s) will be deleted.

Direct Inward Dialing (DIDs)

This panel displays a pool of external DID numbers mapped to their destination numbers (that is, internal directory numbers or other answer points on the system) in your MiVoice Business.



To add a DID number or a DIDs range, perform the following steps:

1. On the left navigation panel, click **MiVoice Business** and then click **Numbers**.
2. In the **Direct Inward Dialing (DIDs)** section, click to expand DIDs.
3. Click **Add DIDs**. The **Add DID Number or Range** dialog box is displayed.

4. Enter a single DID number or enter a DIDs range in the **Range start** and **Range end** fields.
5. Click **Add** to save the DID number or DIDs range, or click **Cancel** to cancel the operation.The entered DID number or DIDs range will be displayed in the Direct Inward Dialing (DIDs) list.

To edit a DID number or DIDs range, perform the following steps:

1. From the **Direct Inward Dialing (DIDs)** list, click the DID number or the DIDs range you want to edit. The **Edit Direct Inward Dialing (DID) Number** dialog box is displayed.
2. Edit the DID number or DIDs range and click **Save**, or click **Cancel** to cancel the operation.

The modified DID number or DIDs range will be displayed in the **Direct Inward Dialing (DIDs)** list.

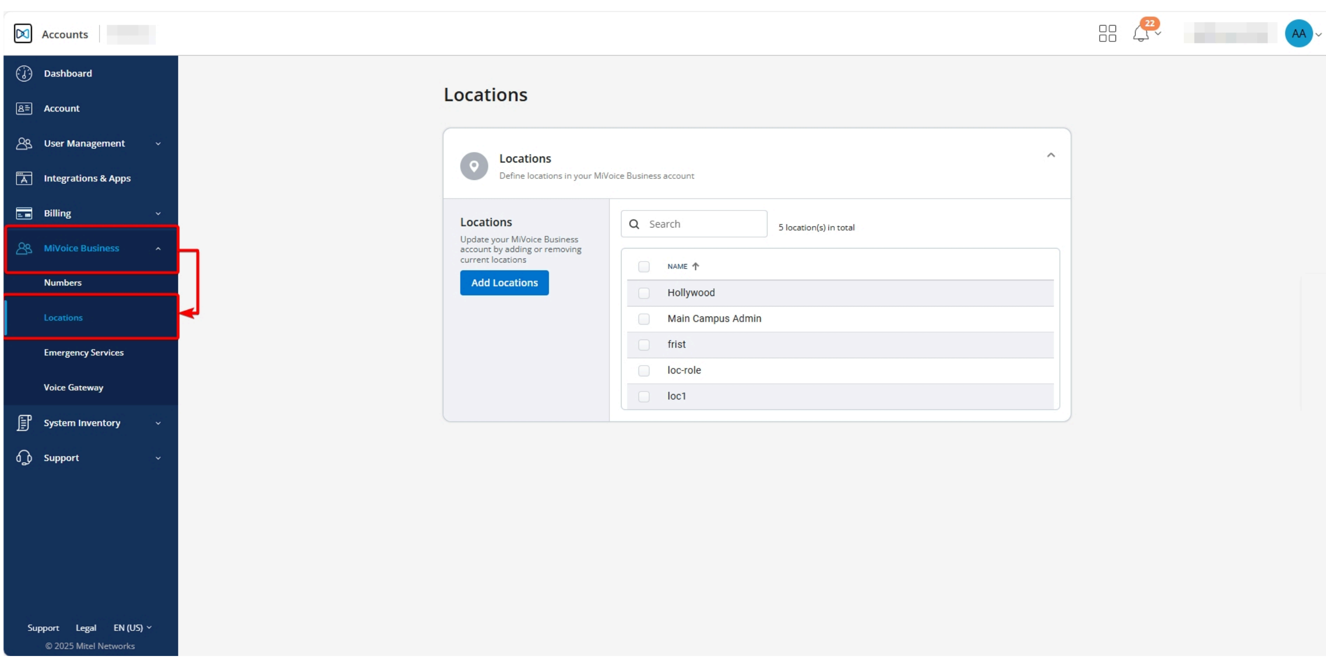
To delete DID number(s) or DIDs range(s), perform the following steps:

1. Select the check box(es) associated with the DID number(s) or DIDs range(s) you want to delete. The **Delete Selected** button appears.
2. Click **Delete Selected** to delete the selected DID number(s) or DIDs range(s). The **Delete selected number(s)** dialog box is displayed. Click **Delete** to complete deletion, or click **Cancel** cancel the deletion.

The selected DID number(s) or DIDs range(s) will be deleted.

Locations

The **Locations** submodule helps you add or remove locations in your MiVoice Business account.



Navigating to the Locations submodule:

1. In the left navigation panel, select **MiVoice Business**.

2. Click **Locations**.

Adding a Location:

1. In the **Locations** section, click **Add Locations**. The **Add Locations** dialog box appears.
2. Enter the name of the new location.

> **Note**:
> Press **Enter** after each location name to add multiple entries.

3. Click **Save**. A confirmation message appears when the location is added successfully.

> **Note**:
> If the action fails, a message appears explaining what went wrong.

Deleting a Location:

> **Note**:
> A location cannot be deleted if it is currently in use elsewhere in the system.

1. In the **Locations** section, select the checkbox located before the location name.

> **Note**:
> The **Delete Selected** button appears only when at least one location is selected.

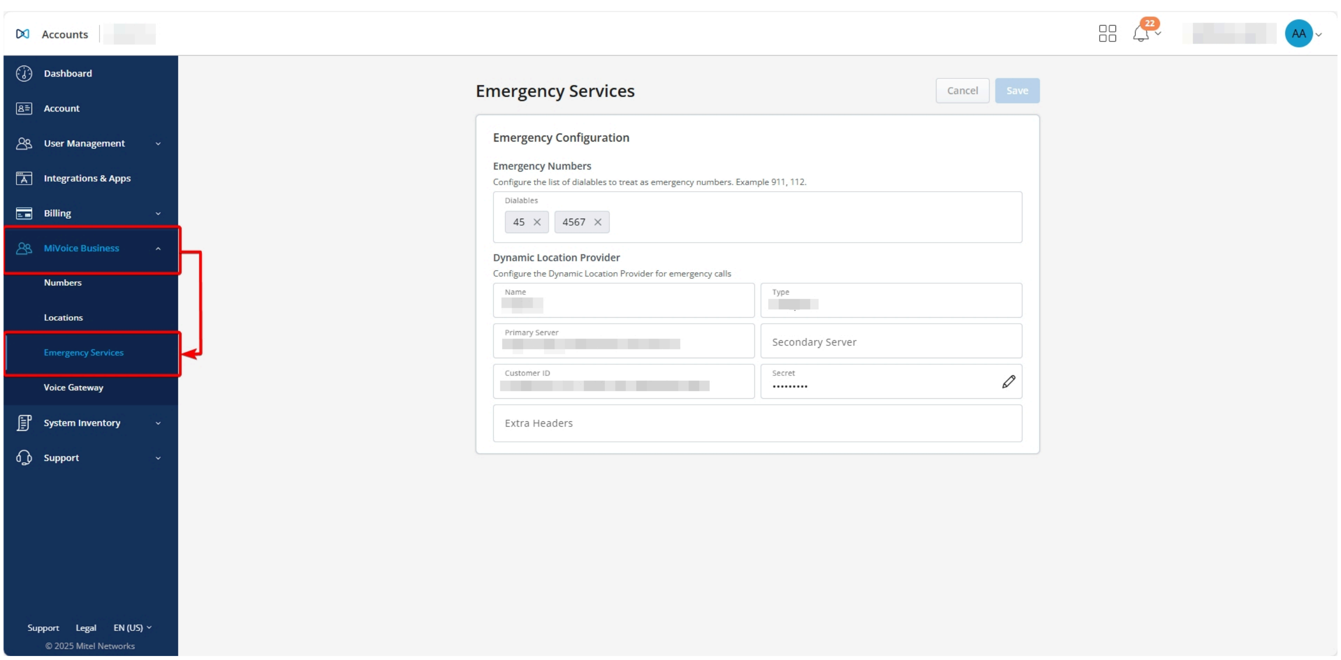
2. Click **Delete Selected**. The **Delete Locations** dialog box appears.
3. Click **Delete** to confirm. A confirmation message appears when the location is deleted successfully.

> **Note**:
>
> If a location is in use—for example, assigned to a user through the MiVB license service—an error message appears when you try to delete it:
>
> *"The location name specified is being referenced. Delete all references before attempting to delete this location."*
>
> To delete the location, remove all references and try again.

Emergency Services

Emergency Services involves setting up fallback emergency numbers and dynamic location providers to ensure a reliable and secure connection during emergency calls.

> **Note**:
> The Emergency Configuration settings are applicable and visible only if the account has both Zoom and MiVoice Business integrations added.



Navigating to the Emergency Services submodule:

1. On the left navigation panel, click **MiVoice Business**.
2. Click **Emergency Services**.

Configuring Fallback Emergency Numbers:

Configuring fallback emergency numbers involves adding, editing, and deleting emergency contact numbers to ensure reliable communication during emergencies.

Adding an Emergency Number:

1. Click **Dialables**.
2. Start typing a number for emergency calls, e.g., 911, 112.
3. Press **Enter**, **Space**, or add a **comma (,)** to add the number.

Editing an Emergency Number:

Double-click on the number to edit it as needed.

Deleting an Emergency Number:

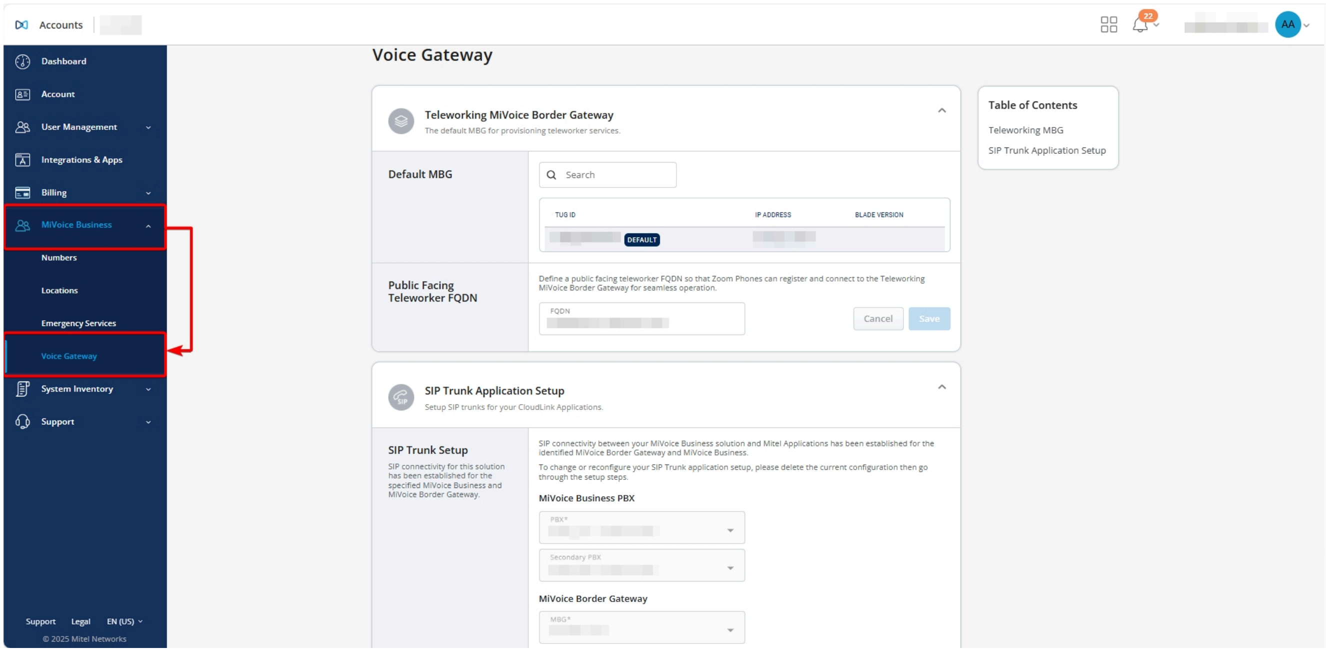
Click the **X** icon next to the number to remove it, if necessary.

Configuring a Dynamic Location Provider for Emergency Calls:

1. Enter the following information in the **Dynamic Location Provider** area:
    - **Name**
    - **Type**
    - **Primary Server**
    - **Secondary Server**
    - **Customer ID:** The unique identifier assigned to your organization by the service provider.
    - **Secret:** The private key or token issued by the service provider to secure communication between the 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.
2. Click **Save**.

Voice Gateway

The Voice Gateway submodule helps you set up MBG and SIP trunks for CloudLink services.



Navigating to Voice Gateway submodule:

1. On the left navigation panel, click **MiVoice Business**.
2. Click **Voice Gateway**.

Configure Teleworking MiVoice Border Gateway:

1. Expand the **Teleworking MiVoice Border Gateway** section
2. If multiple MBGs are part of the MiVoice Business solution, set the default MBG:

   a. Select **Set Default**.
   b. In the **Set Default MBG** pop-up, choose the default MBG from the drop-down list.
   c. Select **Save**.

> **Note**:
> The option to set a default MBG is available only when the **CloudLink Gateway** is deployed and the **CloudLink Daemon** is enabled on the relevant MiVoice Business nodes. This option is not available if the CloudLink Gateway is deployed separately from the MiVoice Business nodes.

3. If **Zoom integration** is enabled and teleworker resiliency for Zoom Phones is required:

    a. Enter the **Public Facing FQDN** for the Teleworker MiVoice Border Gateway Cluster in the **FQDN** field.
    b. Select **Save**.

    This FQDN ensures that Zoom Phones can register and connect to the Teleworker MiVoice Border Gateway for seamless and resilient operation.

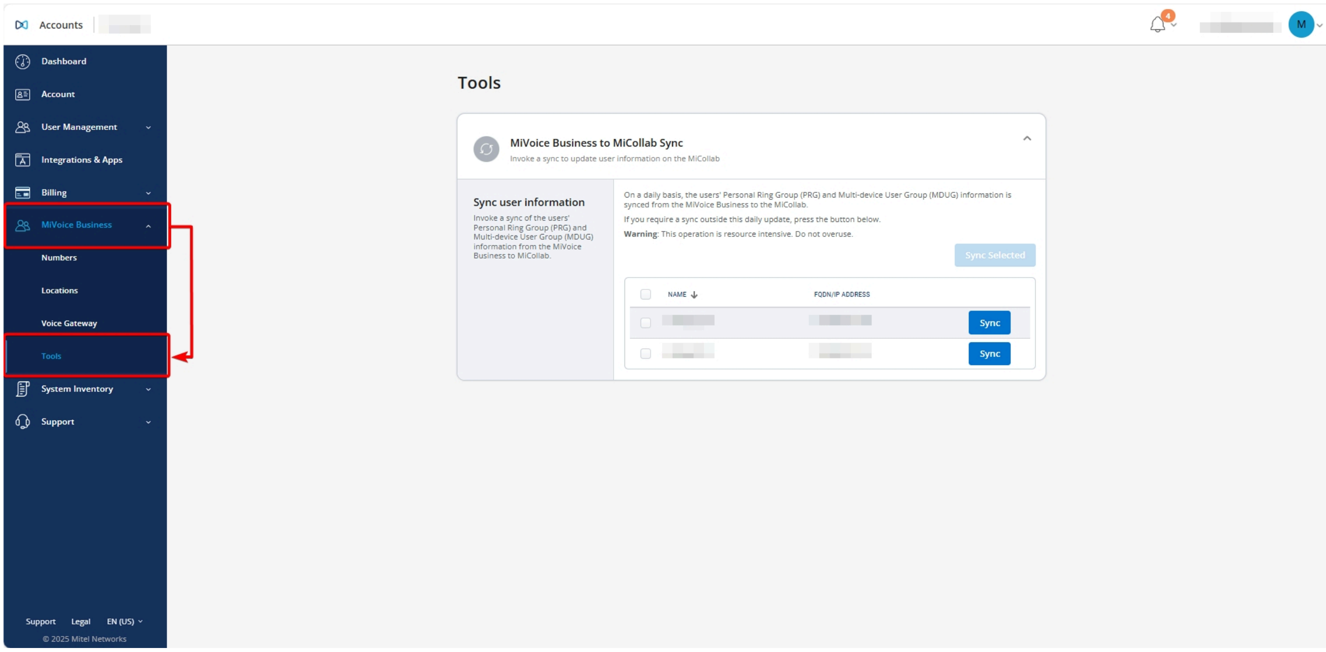
Configure SIP Trunk Application Setup:

1. From the drop-down list, select your **Primary** and **Secondary MiVoice Business PBX**.
2. From the drop-down list, select your **MiVoice Border Gateway**.
3. Select **Save**. A success message appears when the SIP trunk is configured successfully.

> **Note**:
> This setup creates:
>
> - A SIP trunk between the selected **MiVoice Border Gateway** and the **CloudLink Platform**.
> - A SIP trunk between the **MiVoice Business** and the same **MiVoice Border Gateway**.

Tools

The Tools submodule provides access to utilities such as triggering a resynchronization between MiCollab and MiVoice Business.



Navigating to Tools submodule:

1. On the left navigation panel, click **MiVoice Business**.
2. Click **Tools**.

Sync MiVoice Business to MiCollab:

You can manually trigger a sync to update user information—such as Personal Ring Group (PRG) and Multi-device User Group (MDUG) details—from MiVoice Business to MiCollab.

Note:
PRG and MDUG information is automatically synced daily. Use manual sync only when an immediate update is required.

Note:
This operation is resource intensive. Use it sparingly.

To sync individual items:

- Select the **Sync** button next to the item you want to update.

To sync multiple items:

- Select the checkbox before each **Name** you want to sync.
- Select **Sync Selected**.

  The selected user information is synced from MiVoice Business to MiCollab.

3.1.2.1 Managing MiVoice Business Features

After MiVoice Business is integrated on a customer account, you can manage the MiVoice Business features for users in that customer account. The Mitel Partner or Account Administrator can select the service category and set the various user configuration settings.

To access the MiVoice Business features, perform the following:

1. In the **Accounts** console, navigate to **User Management** > **Users** from the left navigation menu. The list of **Users** is displayed.
2. From the list of users, select the user for whom you want to manage the MiVoice Business features.
3. Scroll to the **Products and licenses** section, click **+ Add Product** button. Click the **Add** option next to **MiVoice Business Service** and click **Done** to save the changes.

MiVoice Business features list is displayed. You must complete setup to to select the service category for a user.

MiVoice Business Service

The Mitel Partner can select the type of service category for a user. The service category is the grouping or classification of specific features and services offered to users.

Complete the following steps to select the service category for a user:

1. Go to the **Products and licenses** section of the user, click the **Complete setup** button next to **MiVoice Business (no service assigned)**.
2. Click **Choose service category** to select the service type or click **Upgrade Service** to change or update the existing service type for the user.
3. Click **Select** associated with the service category that you want to choose, and click **Apply**.
4. Additionally, define **Directory Number** and **Direct Inward Dials** settings, under **MiVoice Business** > **System Settings** in the left navigation menu. Refer to Integrating MiVoice Business with CloudLink Account on page 106.

3.1.2.2 User Configuration

From the **User Configuration** section, the Mitel Partner can set the service programming, add phones, configure the selected phones, such as enabling Voicemail, setting advanced configurations, and so on.

3.1.2.2.1 Service Programming

From the **Service Programming** section, the Mitel Partner can select group, department, set user pin, and location. These fields are *optional*.

- **Group**: The **Group** is set as per the template chosen for the user. For more information about groups see, *Ring Groups- Personal* and *Multi-device User Group* in *System Administration Tool Help*. This field can be edited with Groups selected if configured on the PBX.
- **User pin**: A user pin is populated, by default. Click the icon or anywhere in the user pin field to edit the pin. You can choose to set a user pin that meets the **Password Requirements** or click **Auto-generate**. The system creates a new user pin if **Auto-generate** is selected.

  Click **Continue** to resume the process of setting service programming.
- **Location**: The location is set as per the template chosen for the user. This field can be edited with Groups selected if configured on the PBX.
- **Department**: The department is set as per the template chosen for the user. This field can be edited with Groups selected if configured on the PBX.

3.1.2.2.2 Phones

From the **Phones** section, the Mitel Partner can add phones, and then configure the phone. To add a phone for a user, complete the following steps:

1. Click **+ Add Phone**, **Select a phone** dialog box is displayed.
2. From the drop-down list under **Phones**, select the type of phone.
3. Depending on the type of phone you select, do either of the following:

   a. If you select **Desk Phone** or **Generic SIP Phone**, click **Add** to proceed.

   > **Note**:
   > Alternatively, to select Desk Phone, you can click on the drop-down list to add DN, and select phone type as Desk Phone.

   b. If you select **Hot Desk**, **Additional options** section is displayed. Options such as **ACD Agent** and **External Phone** are displayed. You can choose to select the additional options or choose to skip to add the additional options. Click **Add** to proceed. For more information about ACD Agent see, *ACD Agent Hot Desking- Programming* in *System Administrative Tools Help*.

> **Note**:
> You can modify **User Phone Keys**, see Programming User Phone Keys on page 122 for more details.

4. Click **Save** to apply changes.

The phone is added in the **Phones** section.

Note:
If the phone configuration is not successful, an error is displayed. Click the notification icon to view and fix the error.

To navigate to the location of the error, you can either

- click the error message in the **Table of Contents**
- or the error message at the bottom of the page
- or click on the icon associated with the phone

3.1.2.2.2.1 Programming User Phone Keys

Programmable keys act as convenient shortcuts for tasks that would otherwise require pressing two or three phone buttons to achieve the same result. As a Partner or Customer Administrator, you have the ability to create and assign these shortcuts after a user is created by programming the user's phone service keys.

Note:
If a user is created based on **Role**, then the phone keys for that user will be configured initially during that process.

The option to edit **Phone keys** can be accessed after adding phones to the user's configuration.

Assigning a Phone Key

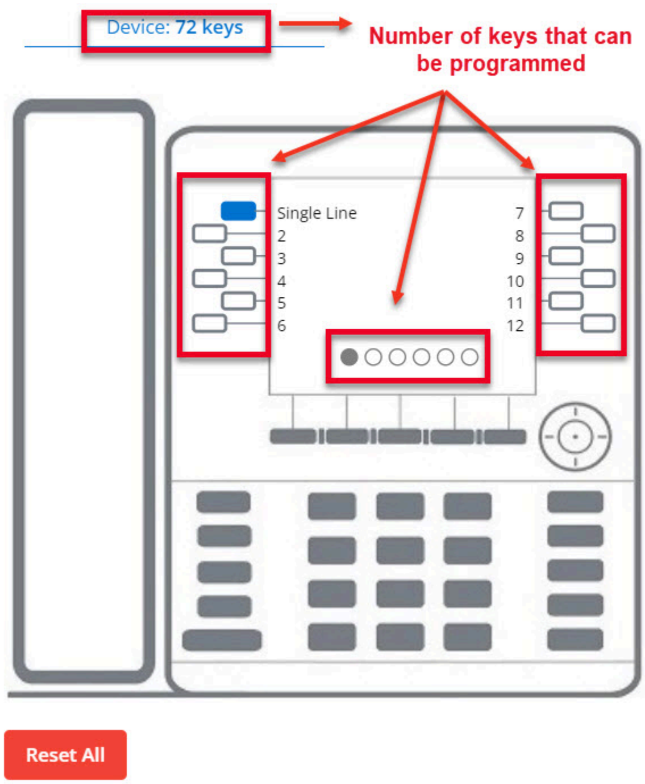
To assign a function using the phone service keys, do the following:

1. Click **User Management** > **Users**, list of users is displayed.
2. Click the **User** from the list whose phone keys you wish to program.
3. Under the **Products and licenses** section, click the **Settings** icon for MiVoice Business Service.

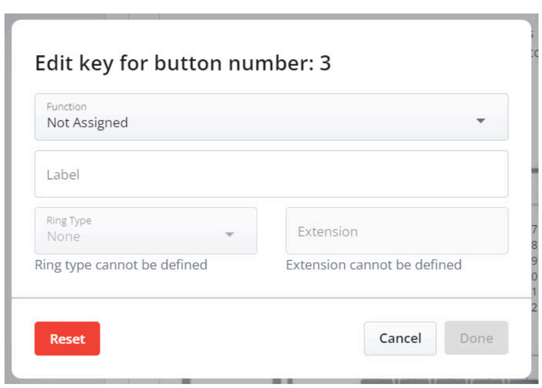
4. Scroll down to the **Phones** section in the **User Configuration** page, click the **Phone Service** you wish to program.

> **Note**:
> As an example for this procedure, **6930 IP phone** is used.

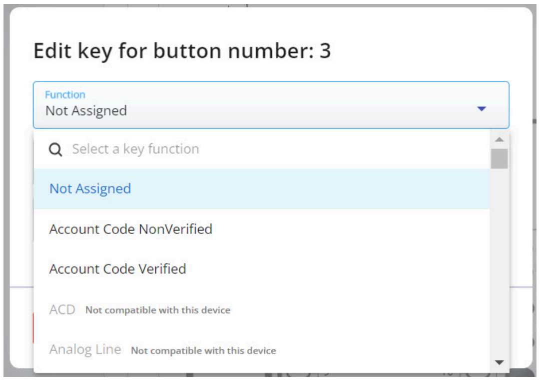
5. Scroll down and expand the **Programmable Keys** section. The total number of keys available for customizing is displayed for the selected **Phone Type**.



6. Click on the **Key**/**Button** to assign a function. The **Edit key** dialog is displayed.

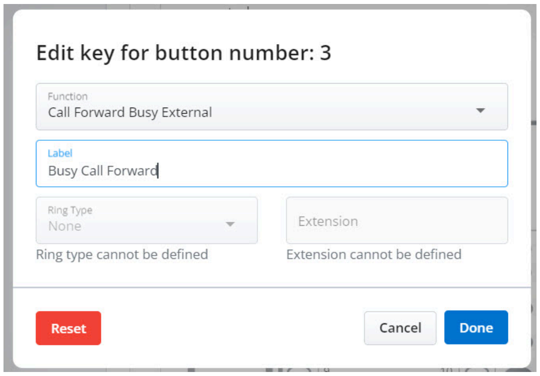


7. Assign a function for the phone key from the **Function** dropdown list.



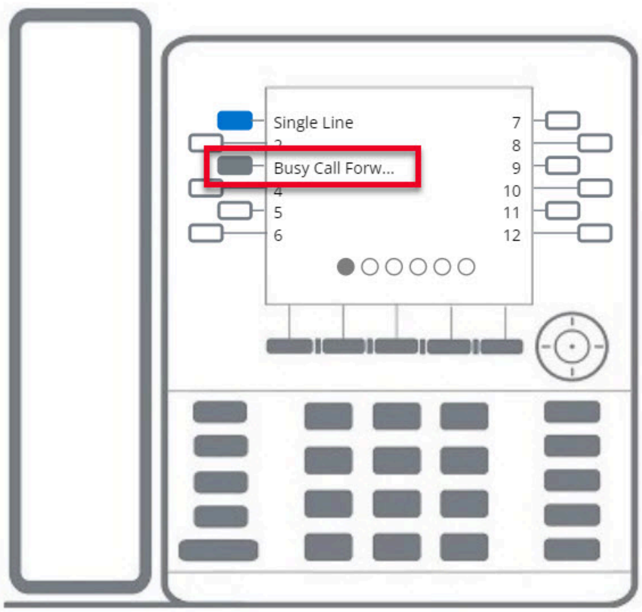
8. In the **Label** field, enter a name to display on the phone.

> **Note**:
> The **Ring Type** and **Extension** are optional fields that rely on the programmed Key type.



9. Click **Done** to save changes.

10. Click **Save** in the User Configuration page to send the changes to MiVoice Business and the newly programmed key will be displayed on the user's phone.



Click **Reset** to restart the form or click **Cancel** to abort the task.

Editing a Phone Key

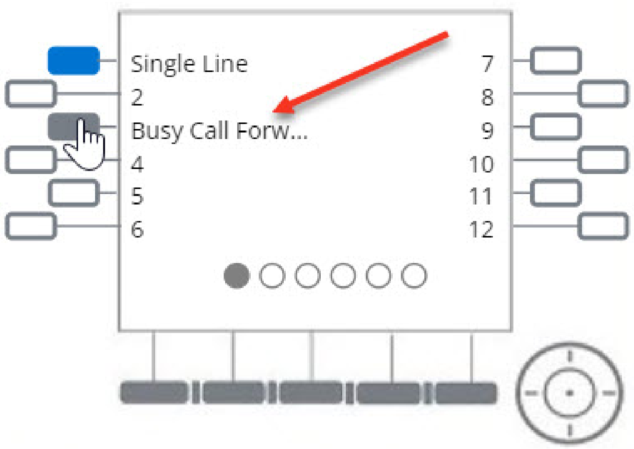
To edit or modify an assigned phone key, do the following:

1. Click **User Management** > **Users**, list of users is displayed.
2. Click the **User** from the list whose phone keys you wish to edit.
3. Under the **Products and licenses** section, click the **Settings** icon for MiVoice Business Service.

4. Scroll down to the **Phones** section in the **User Configuration** page, click the **Phone Service** you wish to edit.

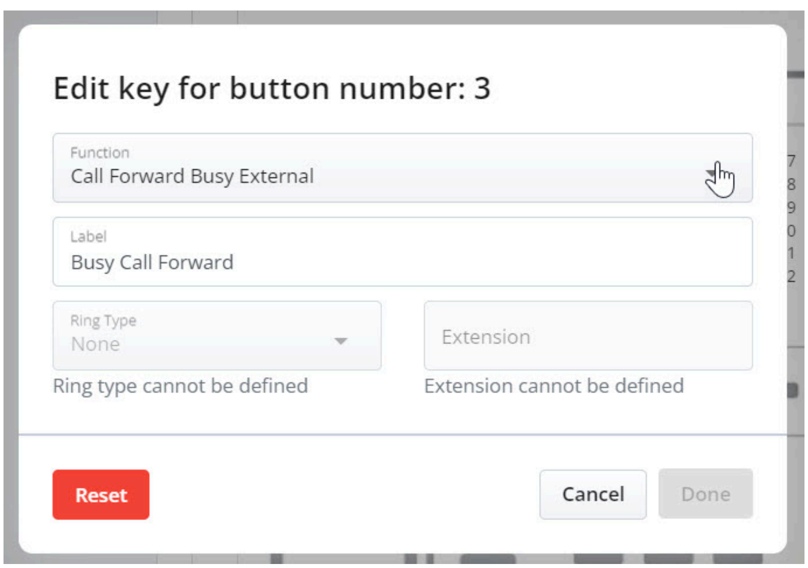
> **Note**:
> As an example for this procedure, **6930 IP phone** is used.

5. From the **User Configuration** page, scroll down to the **Phones** section.
6. Click the key that you wish to edit.



The **Edit Key** dialog is displayed.

7. Modify the details in the dialog as needed, and click **Done** to save the changes.



Phone Key Functions

The **Functions** dropdown menu provides a selection of features for programming the shortcut key. These **Feature Keys** enable you to activate features without dialing feature access codes.

Note:
Features that are not available for programming to a key may still be used by dialing feature access codes.

Refer to the *MiVB System Administrator Online Help* for comprehensive information. Listed below are descriptions of some common functions:

- **Account Code Verified** - refers to verified account codes that enable access to features typically unavailable at a station. These codes are entered before making a call, allowing changes to Class of Service (COS) and Class of Restriction (COR) settings at any station. Upon hanging up, the station returns to its normal state.
- **Account Code NonVerified** - refers to non-verified account codes that allow users to input codes on the Station Message Detail Recording (SMDR) record for billing or call management purposes. These codes can be entered multiple times during a call as needed.
- **Auto Answer** - picks up incoming calls automatically without the need for the user to manually accept the call.
- **Call Forward Always** - forwards all incoming calls to a designated phone number or extension regardless of the user's phone state.

3.1.2.2.2.2 Programming Float Keys

The **Float Keys** display unanswered ringing lines directly on the designated keys, ensuring they are readily visible without needing to navigate through different application pages on the phone. You can program up to six multi-function keys for one-touch feature access as Float Keys. These float keys are positioned in the upper-right row across all supported sets.

Float Keys are supported on the The 5340, 5360, 6930, and 6940 IP Phones, the 6970 IP Conference Phone and the 5560 IPT.

Refer to *Float Keys* in the *MiVoice Business System Admin Help* for more details.

Assigning a Float Key

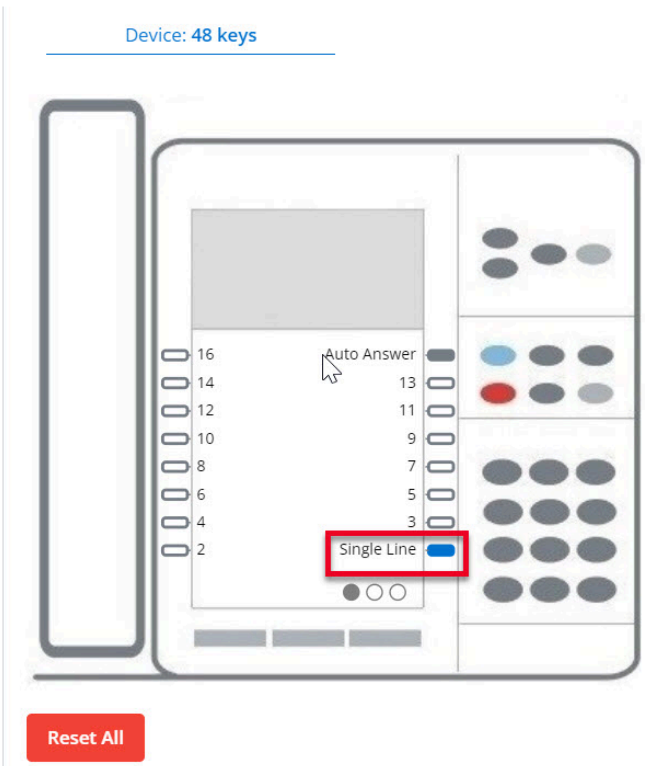
To assign a float key, do the following:

1. Click **User Management** > **Users**, list of users is displayed.
2. Click the **User** you wish to configure Float key for.
3. Click **Products and licenses** > **Settings**. The **User Configuration** page is displayed.
4. Scroll down to **Phones**, and click the **Phone Service** you wish to program.

Note:
Float Keys are supported on the 5340, 5340e, 5360, 5560, 6930/6930L/6930w, 6940/6940w IP phones, the 6970 IP Conference Phone, and for Single, Key system, and Multicall types.

Note:
As an example for this procedure, **5340 IP** is used.

5. Scroll down to expand the **Programmable Keys** section.
6. Select the **SINGLE_LINE** or **KEY_SYSTEM** or **MULTICALL** key to program from the Phone silhouette.



7. Select the **Float** check box.

8. Click **Done** to save Key.
9. Save **User**. After the save, verify the float value is saved successfully.

3.1.3 Mitel CX

CloudLink is Mitel's next-generation CPaaS (Communications Platform as a Service) product that enables communication between on-premises and feature-rich cloud-based applications.

To enable Mitel CX for the users in a customer account, the Mitel Partner or the Account Admin must add **Mitel CX** integration to the customer account. To do this, you must perform the following steps:

1. Log in to the Mitel Administration.
2. Add Mitel CX to the customer account. For information about adding Mitel CX integration, see Adding an integration to a customer account on page 88.

   After you have added **Mitel CX** integration to the customer account, **Mitel CX** will be listed in the **Integrations** panel.

3.1.3.1 Managing Mitel CX Features

After Mitel CX is integrated to a customer account, you can manage the Mitel CX features for the users in that customer account. The Mitel Partner or Account Administrator can select the service category and set the various user configuration settings.

To access the Mitel CX features, perform the following:

1. In the **Accounts** console, navigate to **User Management** > **Users** from the left navigation menu. The list of **Users** is displayed.
2. From the list of users, select the user for whom you want to manage the Mitel CX features.

   Scroll to the **Products and licenses** section and click **+ Add Product** button. Click the **Add** option next to **Mitel CX** and click **Done** to save the changes.

Note:
If the account is integrated with MiVoice Business, MiVoice Business Service will be displayed as the product and when it is added to the user, Mitel CX options can be assigned as well.

Mitel CX features list is displayed. You must click **Complete setup** to select the service category for a user.

Mitel CX Service

The Mitel Partner can select the type of service category for a user. The service category is the grouping or classification of specific features and services offered to users.

Complete the following steps to select the service category for a user:

Note:
Steps number 2 and 3 are applicable only if the account has MiVoice Business.

1. Navigate to **Products and licenses** section of the user details page and click the **Complete setup** button associated with **Mitel CX**. If the account is integrated with MiVoice Business, click the **Complete setup** button associated with **MiVoice Business (no service assigned)**.
2. Click **Choose service category** to select the service type or click **Upgrade Service** to change or update the existing service type for the user.
3. Click **Select** associated with the service category that you want to choose, and click **Apply**.
4. From the **Template** drop down list, select a user template. **Filter templates by category and tier selection** check box is selected by default.
5. Click **Apply Changes**. For information about user templates, see Mitel CX User Templates.

3.1.3.2 Mitel CX User Templates

Templates serve as a mechanism for defining the roles that a user will encompass. It helps you specify the roles assigned to a user.

Note:
No pre-defined templates for Contact Center are available for import.

Prerequisites

To be able to create/edit/view user templates that contain the Mitel CX product, the following are required:

- A user logging into Mitel Admin must have a matching email address in Mitel CX. However, apartner logging in does not need to be configured in Mitel CX, as they will automatically receivehigher permissions to create, edit, and view data from Mitel CX.
- The logged in user must have a security role defined in Mitel CX with read or higher access for Device Configuration.
- The CloudLink Daemon service must be configured and running on the Mitel CX server.

Viewing User Templates

To view User Templates, in the left navigation panel navigate to **User Management** > **User Templates**. In the **User Templates** page a list is displayed with existing user templates. The **PRODUCTS** column will indicate which products are supported by the template, based on the displayed icon(s).

Creating, Editing, and Deleting User Templates

To create a User Template, perform the following steps:

1. In the **User Templates** page, click **Create Template**. An empty template form is displayed.
2. Enter the template name in the **Template name** field.
3. Enter a description for the template in the **Description** field.
4. Select the check box associated with **Mitel CX**.

> **Note**:
>
> - The **Mitel CX** check box is is only visible for accounts integrated with MiVoice Business. To enable the template for MiVoice Business options, select the check box associated with **MiVoice Business**.
> - The **Mitel CX** check box will be disabled on accounts integrated with MiVoice Business when the logged on user does not have appropriate permission in Mitel CX, or the connection to Mitel CX is disabled. Hovering over the checkbox will display a tooltip indicating why it is disabled.

5. Click **Save** to save the template.

> **Note**:
> The **Save** button will be disabled until after the template is defined. All required fields must be entered.

To edit an existing User Template, select a template from the template list. Edit the template as needed and click **Save**. To maintain the original template and create a new template with the edited values, click **Save as new**.

Note:
If the logged in user has a read-only security role in Mitel CX, all of the Contact Center properties will be displayed as read-only and cannot be modified.

To delete a User Template, perform the following steps:

1. Select the user template(s) from the template list.
2. Click the icon and click **Delete**. **Delete Template?** dialog box is displayed.
3. Type 'delete' in the **type 'delete'*** field.
4. Click **Delete**.

The user template will be deleted.

For more information about viewing, creating, editing, and deleting a user template see, User Template.

3.1.3.3 User Configuration

From the **User Configuration** section, the Mitel Partner or the Account Admin can set the service programming, add phones, configure the selected phones, and also configure contact center settings for the user, such as enabling Chat, Email SMS and Open media.

For information about Service Programming and Phones see, Service Programming and Phones.

3.1.3.3.1 Contact Center

The **Contact Center** section displays Mitel CX configuration settings for the user. This section allows the Mitel Partner or Account Admin to modify contact center settings including the assigned site, security role, supported media types, and licenses.

1. From the drop down list of **Site**, select the site.
2. Select the **Security Role** that you want to assign to the user.
3. Select the check box(es) associated with **Media Types** that you want to assign to the user.

Note:

- If a Media Server is not configured in Mitel CX for the media type, the check box will be disabled.
- Employees/User - Only one voice agent can be configured per employee. If the employee is anACD Agent, clicking the Voice checkbox in the Contact Center template will automatically fill in theAgent Reporting and Agent Login.

4. From the **Workload Descriptor** drop down list, select workload descriptor.
5. From the feature options, **Print reports to desktop**, **Distribute reports from employee**, and **May see all queues** select the associated check box(s) that you want to assign.
6. Enter the network printer ID in the **Network Printer** field.
7. Under the **Licensing** section, from the **Supervisor License** drop down list, select the license that you want to assign to user.
8. Select the check box(s) associated with the license(s).

Note:
The check boxes for **Multimedia Contact Center License** and **Contact Center Voice License** are disabled. They will be automatically selected based on the Media types assigned to the user.

9. Select the type of phone from the **Phone Type License** drop down list.

The **Save** button will be disabled, if any of the required fields are not entered, or have invalid entries.

If any field has an error, an error message will be displayed at the bottom of the page.

The **Save and Deploy** button will save the user settings and send a deployment email to the user. Selecting just **Deploy** when no changes are made will send a deployment email to the user with the current configured settings.

3.1.4 Mitel One Integration

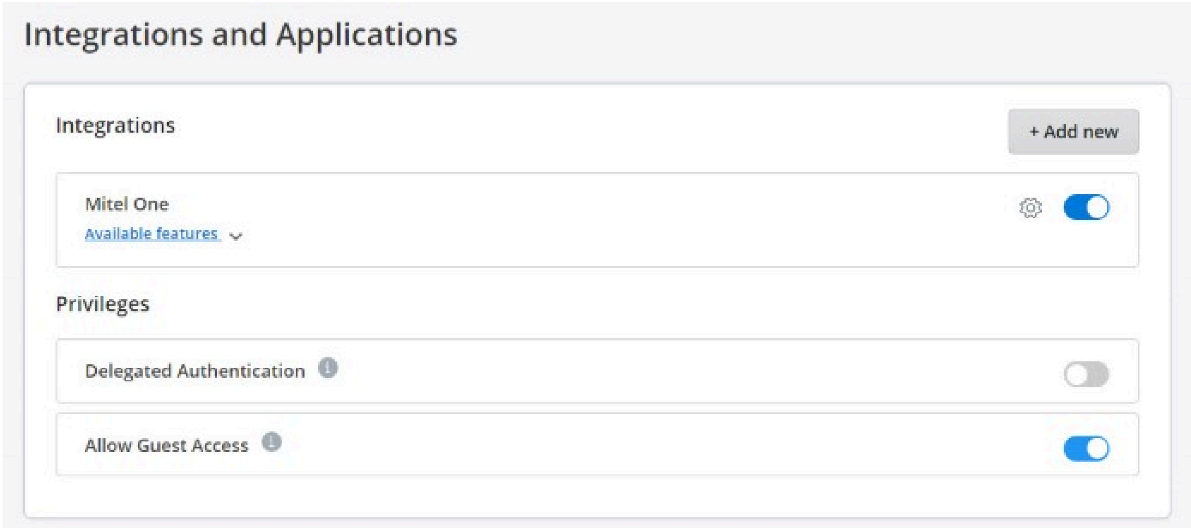
Mitel One application is a next-generation collaboration application that provides advanced communication features and integrates with your enterprise's call manager (Cloud and on-premise) to improve work efficiency and enhance workplace communication. It provides seamless transitions between voice, video, and chat capabilities for a complete collaboration experience. You can find and connect with individuals and groups through calls and chats, answer and maneuver multiple calls in real-time, and attend multi-party video conferencing with your contacts from your PC and Mac devices.

To enable Mitel One application for the users in a customer account, the Mitel Partner or the Account Admin must add **Mitel One** integration to the customer account. To do this, you must perform the following steps:

1. Log in to the Mitel Administration.

2. Add Mitel One integration to the customer account. For information about adding Mitel One integration, see Adding an integration to a customer account on page 88.

   After you have added Mitel One integration to the customer account, **Mitel One** will be listed in the **Integrations** panel.



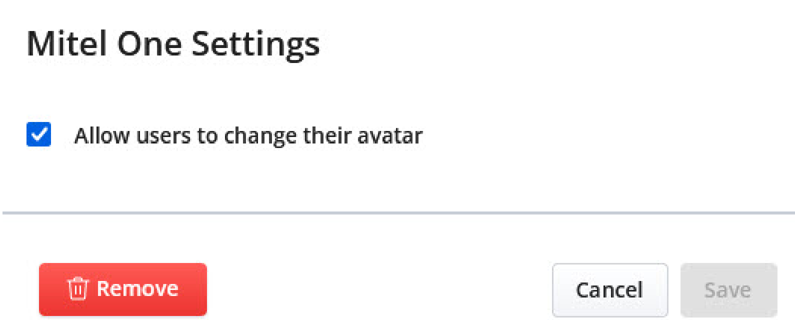
Managing Mitel One Features

After adding Mitel One integration to a customer account, you can manage the Mitel One features for users in that customer account.

- To enable or disable users from changing their avatar in the Mitel One application:

  By default, the users in a customer account can change their avatar in the Mitel One application. To disable this feature:

  1. Click the  icon associated with Mitel One. The **Mitel One Settings** page opens.

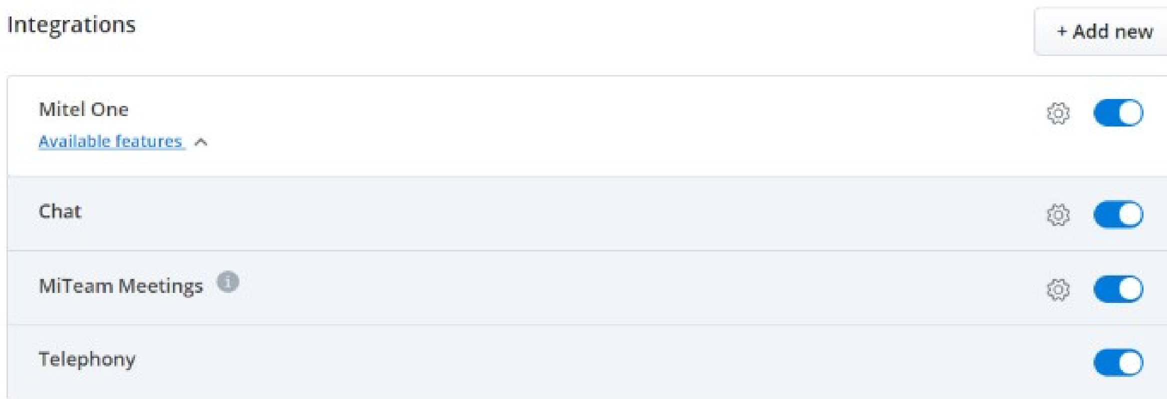
     

  2. Clear the **Allow users to change their avatar** check box.
  3. Click **Save** to save the settings. Clicking **Cancel** cancels the operation.

- To enable or disable the **Chat** feature in Mitel One application:

  The Chat feature in the Mitel One web application allows users to connect in real-time to any other Mitel One contact or group of contacts through messages. To disable this feature:

  1. Click the **Available features** drop-down list under **Mitel One** in the **Integrations** panel.

  2. Slide the **Chat** toggle button to the left.

  Note:

  - The  gear icon associated with **Chat** allows you to enable or disable the functionality for the users in the customer account to edit or delete chat messages shared in CloudLink applications. For more information, see Allow Users to Edit or Delete Chat Messages in CloudLink Applications.
  - Chat integration is enabled by default for all customer accounts, and is displayed in the **Integrations** panel. After enabling Mitel One integration, the Chat integration will no longer be displayed as a standalone integration option in the **Integrations** panel. It will be displayed as an option in the **Available features** drop-down list associated with **Mitel One**.

- To enable or disable **MiTeam Meetings** in the Mitel One application:

  By default, the MiTeam Meetings feature is enabled. To disable this feature:

  1. Click the **Available features** drop-down list under the **Mitel One** integration.
  2. Slide the **MiTeam Meetings** toggle button to the left.

Note:

- The ⚙ gear icon associated with **MiTeam Meetings** allows you to enable or disable functionality for the users in the customer account to specify, while scheduling a meeting, whether the waiting room will be available to guests who want to join the meeting using the MiTeam Meetings application. For information about managing MiTeam Meetings feature, see Allow Users to Manage Waiting Room in MiTeam Meetings.
- If you have already enabled **MiTeam Meetings** integration, after enabling **Mitel One** integration, **MiTeam Meetings** integration will no longer be displayed as a standalone integration option in the **Integrations** panel. It will be displayed as a feature in the **Available features** drop-down list associated with **Mitel One**.

- To enable or disable the **Telephony** feature in Mitel One application:

  By default, the Telephony feature is enabled. To disable this feature:

  1. Click the **Available features** drop-down list under **Mitel One** integration.
  2. Slide the **Telephony** toggle button to the left.

Removing Mitel One Integration

To remove Mitel One integration for a user in a customer account perform either of the following:

- From **Mitel One Settings** dialog box:

  1. Click the ⚙ icon associated with Mitel One. The **Mitel One Settings** page opens.
  2. Click **Remove** to remove Mitel One integration.
- From the **Integrations** panel:

  Slide the toggle button associated with **Mitel One** to the left. For more information about removing an integration from a customer account, see Removing an integration from a customer account on page 92.

3.1.4.1 Assigning Mitel One Licenses to Users

When a Mitel Partner purchases a user bundle for a customer, for example. MiVoice Office 400 UCC bundle (Entry, Premier, or Elite), the Mitel One subscription (which includes Mitel One Softphone, and Chat licenses) in the bundle is delivered to the CloudLink Platform and will be displayed in the Orders page of the Partner account.

The Mitel Partner then must assign these Mitel One subscriptions to the customer accounts. These subscriptions have licenses which must then be assigned to the users in these customer accounts by Account Administrator. Users require these licenses to be able to use Mitel One.

To assign Mitel One licenses to a user(s) do the following procedure:

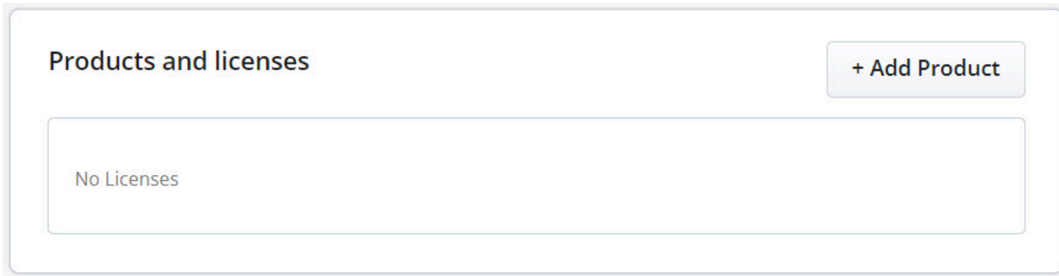
1. Log in to the Mitel Administration.
2. Click the **User Management** and then click **Users** from the navigation menu on the left side of the Accounts Console Dashboard. The **Users** page is displayed.

3. The Account Administrator can assign Mitel One license to an individual user or to a selected number of users in bulk.

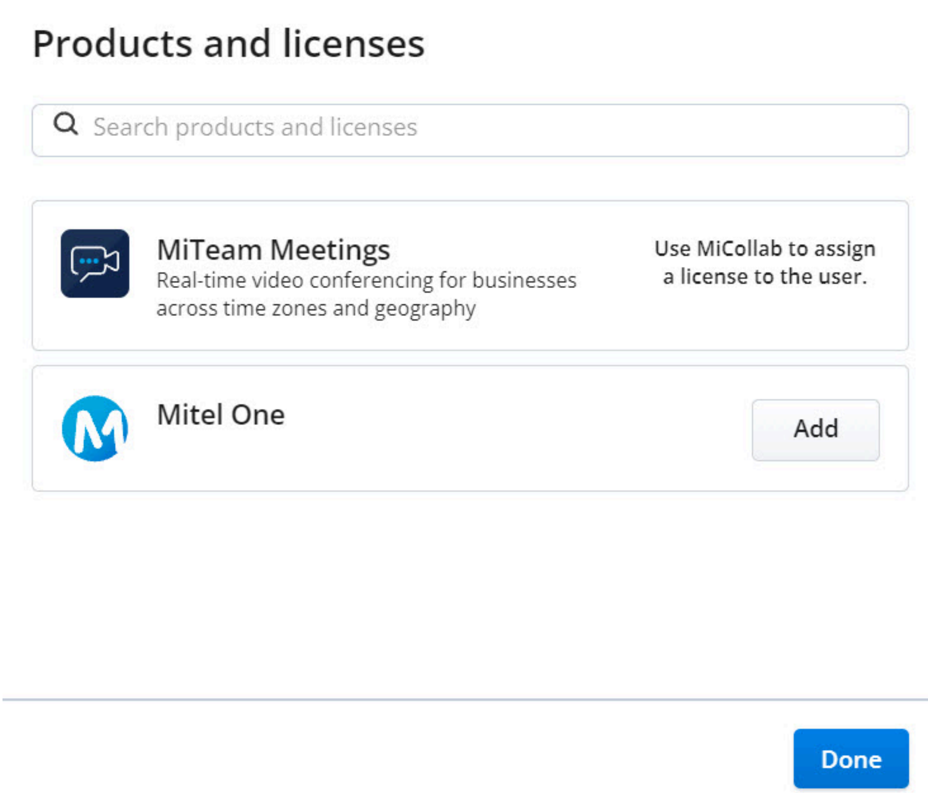
   - **To assign Mitel One license to an individual user do the following:**

     a. From the **Users** page, click the user for whom you want to assign the license. The details of the users are displayed.

     b. Click **+Add Product**. The **Product and licenses** dialog box is displayed.



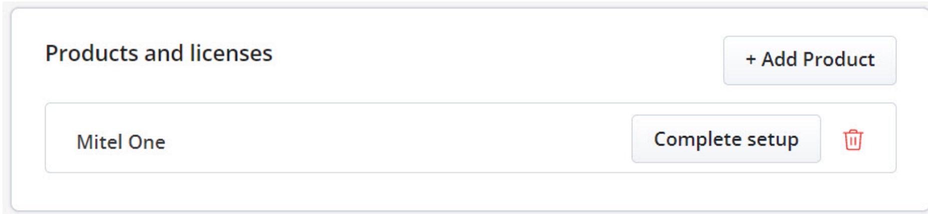
     c. Click the **Add** button associated with **Mitel One** and then click **Done**.



     Mitel One is added to the user's profile.

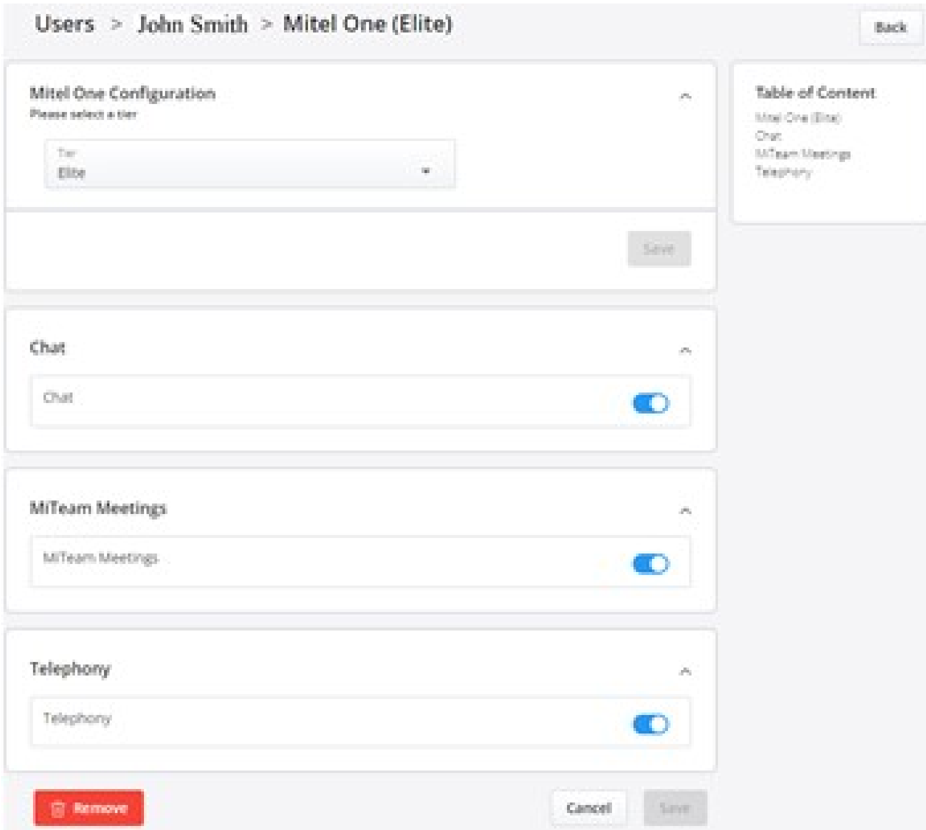
     After Mitel One is added to the user, then you must assign a license to the user. This can Essential, Premier, or Elite.

     d. To assign a license tier, click the **Complete setup** button associated with **Mitel One**. The product and licenses page is displayed.



e. From the drop-down list, select the tier which you want to assign to the user. Click **Save** to complete the process of assigning Mitel One license to the user. Clicking **Cancel** cancels the operation. Clicking **Remove** removes Mitel One for the users.

Mitel One license is assigned to the user and Mitel One Configuration page shown in the following screenshot is displayed.



Use this page to manage Mitel One licenses and features for a user. For more information about managing existing licenses and features for a user see, Manage Mitel One License and Features on page 143.

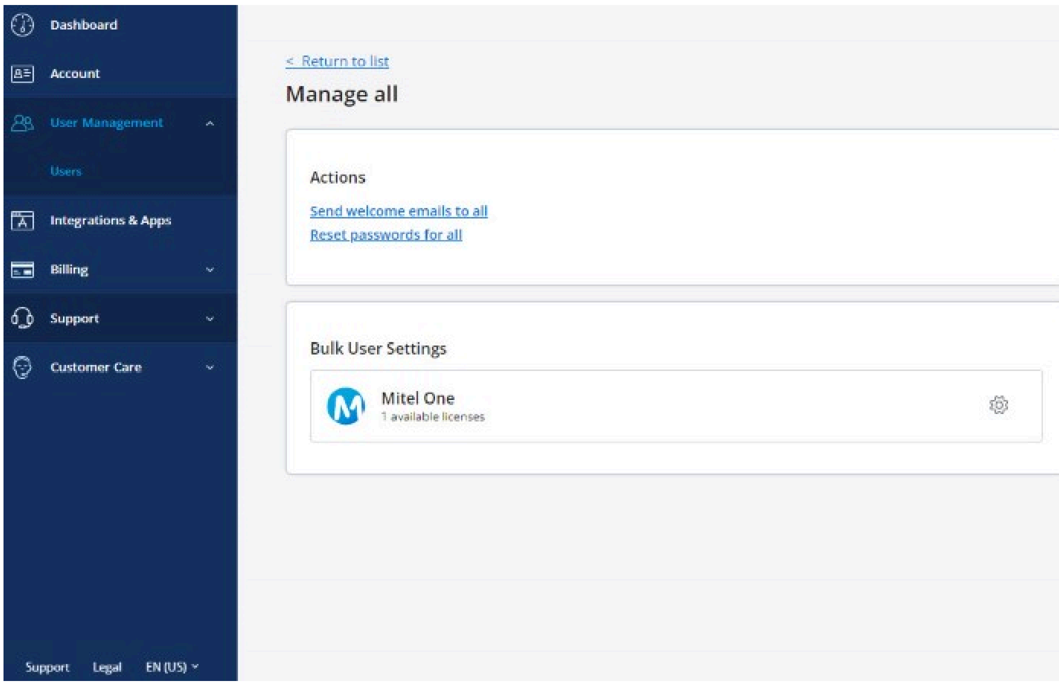
The Account Administrator can view a summary of the features that are enabled and disabled for a user from the **Users** page. In the **Products and licenses** panel, click the drop-down list under **Available feature** to view the list of enabled and disabled features.

- **To assign license to a selected number of users in bulk do the following:**

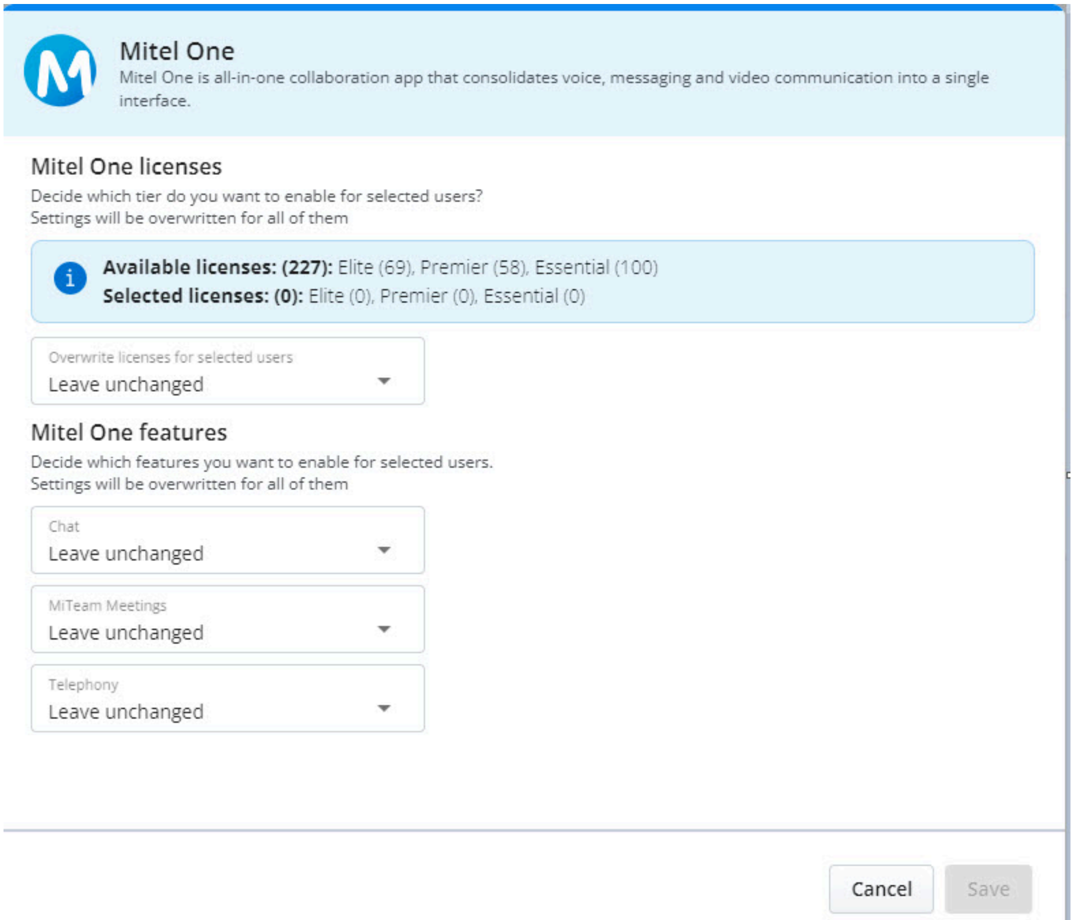
> **Note**:
> If you click **Manage** without selecting the users, then the changes made will be applicable to all the users in the account.

a. From the **Users** page, select the check boxes associated with the users for whom you want to assign the license.

b. Click **Manage**. The **Manage** page is displayed.



c. In the **Bulk User Settings** panel, click the icon associated with **Mitel One**. The **Mitel One** dialog box is displayed.



d. From the **Overwrite licenses for selected users** drop-down list, select the license tier that you want to assign to the users. Selecting **Leave unchanged** will retain the existing licenses and selecting **Unassign all** unassigns all existing Mitel One licenses for all the selected users.

> **Note**:
> The number of selected users must be equal or lesser than the sum of the number of available licenses and the number of licenses consumed by those selected users. If not, the console will not display the license tier in the Overwrite licenses for selected users drop-down list.

e. You can enable or disable the corresponding features for the selected users from the **Chat**, **MiTeam Meetings**, and **Telephony** drop-down lists.

Note:
An Account Administrator can choose to enable or disable Chat, MiTeam Meetings and Telephony features from the respective drop-downs under **Mitel One features**. However, those feature changes will be applied, only for those users who have a license that supports those features.

f. Click **Save** to assign the license to the selected users. Clicking **Cancel** will cancel the operation.

Mitel One license is assigned to the users.

Manage Mitel One License and Features

The Account Administrator can change the existing license tiers and features for individual or multiple users in an account by using the following procedures:

Note:
The number of selected users must be equal or lesser than the sum of the number of available licenses and the number of licenses consumed by those selected users. If not, the console will not display the license tier in the **Overwrite licenses for selected users** drop-down list.

The Account Administrator can navigate through the Mitel One Configuration page using the Table of Content.

- **To manage license for an individual user do the following:**

  1. From the **Users**page, click the user for whom you want to change the existing license tier or feature. The user details page is displayed.
  2. Click the icon associated with **Mitel One** in the **Product and licenses** panel. The **Mitel One Configuration** page is displayed.

     IMAGE
  3. From the **Tier** drop-down list, select the tier you want to assign to the user and click **Save**. To enable or disable chat, MiTeam Meetings, or the telephony feature in Mitel One for the user, slide the toggle button associated with the respective feature to the right or left respectively.

     After making the necessary changes, click **Save** to save the settings. Clicking **Cancel** cancels the changes. Clicking **Remove** removes Mitel One license for the user.
- **To manage licenses for all or selected number of users in bulk, do the following:**

> **Note**:
> If you click **Manage** without selecting the users, then the changes made will be applicable to all the users in the account.

1. From the **Users** page select the checkboxes associated with the users for whom you want to change the existing license tier.
2. Click **Manage** and from the page that opens, click the ⚙ icon associated with **Mitel One** in **Bulk User Settings**. The **Mitel One** dialog box opens displaying the Mitel One license summary for the account and selected users.
3. From the drop-down list under **Overwrite licenses for selected users** select the license tier you want to assign to the users.

> **Note**:
> An Account Administrator can choose to enable or disable Chat, MiTeam Meetings and Telephony features from the respective drop-downs under **Mitel One features**. However, those feature changes will be applied, only for those users who have a license that supports those features.

4. Click **Save**. The selected license tier is assigned to all the users or to the selected number of users.

3.1.5 MiTeam Meetings Integration

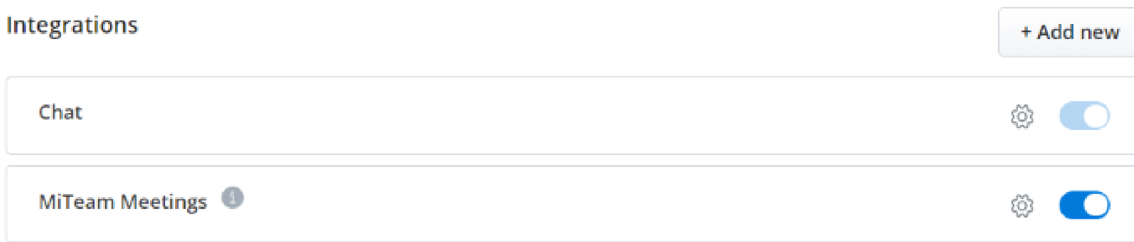
MiTeam Meetings is a multi-party video solution designed for users who want to improve work efficiency and enhance workplace communication with seamless transitions between voice, video, and chat capabilities for a complete collaboration experience. It enables users to access features such as:

- **Collaborate**: Perform audio, video, and web sharing
- **Chat**: Hold chat sessions and receive chat notifications within a meeting
- **File Sharing**: Store and share files

To enable MiTeam Meetings application for the users in a customer account, the Mitel Partner or the Account Admin must add **MiTeam Meetings** integration to the customer account. To do this, you must perform the following steps:

1. Log in to the Mitel Administration.
2. Add MiTeam Meetings integration to the customer account. For information about adding MiTeam Meetings integration, see Adding an integration to a customer account on page 88.

3. After you have added **MiTeam Meetings** integration to the customer account, **MiTeam Meetings** will be listed in the **Integrations** panel.



After adding **MiTeam Meetings** integration to a customer account, see the following topics to assign MiTeam Meetings licenses to individual users in the customer account; and enable or disable a functionality for the users in the customer account to specify whether the waiting room will be available to guests who want to join the meeting using the MiTeam Meetings application.

3.1.5.1 Assigning MiTeam Meetings License to Users

A Mitel Partner must purchase MiTeam Meetings licenses and assign them to customer accounts. These licenses must then be assigned to the users in these customer accounts. Users require these licenses to be able to use MiTeam Meetings.

The licenses purchased by a Partner can be viewed in the Orders page of the Mitel Administration. The Partner can assign these licenses to the customer accounts using the following steps:

1. Log in to the Mitel Administration.
2. To open the **Orders** page, click the **Billing** option from the navigation menu on the left side of the Accounts Console Dashboard and click the **Orders** option.
3. Click the **Assign** button adjacent to the Order you purchased. A panel opens.
4. From the drop-down list, choose the **Company** name (customer account) to which you want to assign the Order. Click **Assign**. All the licenses in that Order are assigned to the customer account. See **Orders** section of the **Account Information Page**to view the license details.

Managing Licenses when MiTeam Meetings is cross launched from MiCollab

The users in a customer account can cross launch MiTeam Meetings from MiCollab if MiCollab integration is enabled for that account. For more information about how to enable MiCollab integration for an account, see Integrating Mitel Applications with CloudLink and MiTeam Meetings Solution Document for MiCollab. After the integration is complete, the MiCollab server controls the MiTeam Meetings licensing, and hence the licenses cannot be individually managed in the Mitel Administration.

The following scenarios explain what happens in the Mitel Administration when you assign MiTeam Meetings licenses to a user in a customer account for which MiCollab integration is enabled.

- If MiTeam Meetings integration is disabled for an account, all the existing MiTeam Meetings licenses assigned to the users will continue to remain active.
- If MiTeam Meetings Integrations is enabled for a customer account, and if the users in the account have MiTeam Meetings licenses assigned to them, then the **Products and licenses** section in the user

information page of these users will display the MiTeam Meetings license with the associated toggle button enabled, but the toggle button will be read-only.

- If MiTeam Meetings Integrations is enabled for a customer account, and if the users in the account do not have MiTeam Meetings licenses assigned to them, then the **Products and licenses** section will display “No Licenses”.

If you disable MiTeam Meetings integration after disabling MiCollab integration for an account, then Mitel Administration will disable all existing MiTeam Meetings licenses for the users in that account. However, if you disable MiCollab integration after disabling MiTeam Meetings integration for an account, all the existing MiTeam Meetings licenses assigned to the users will continue to remain active.

Managing Licenses for MiTeam Meetings — When used as a Standalone Tool

To use MiTeam Meetings as a standalone tool the Mitel Partner or the Account Admin of a customer account must assign MiTeam Meetings licenses to individual users in that customer account. To assign licenses to a user:

- MiCollab integration must be turned off for the customer account in which the user is registered.
- MiTeam Meetings licenses must be assigned to the customer account.
- The user must be added in the customer account and MiTeam Meetings Integration must be enabled for that account.

The following steps describe how a Partner or Admin user can assign MiTeam Meetings licenses to a user in a customer account.

1. Log in to the Mitel Administration.
2. To assign licenses to individual users, access the **Users** page of a customer account:
   - Mitel Partner: Click the account from the **Accounts**page. The **Account Information** page opens and the **Users** option will be displayed in the navigation menu in the left side of the page. Click the **Users** option.
   - Account Admin: Click the **Users** option from the navigation menu in the left side of the Accounts Console Dashboard.
3. The **Users** page opens. Click the user to whom you want to assign the license. The user details form opens. In the **Products and licenses** section of this form, enable the **MiTeam Meetings** toggle button to assign the MiTeam Meetings license for that user.

The following scenarios explain what happens in the Mitel Administration when you try to assign MiTeam Meetings licenses to a user, but do not have valid license or MiTeam Meetings integration enabled.

- If MiTeam Meetings integration is enabled for an account but MiTeam Meetings licenses are not available to be assigned to users, then the **Products and licenses** section in the user information page will display the MiTeam Meetings license, but the associated toggle button will be disabled and the message “Licenses not available” will be displayed.
- If MiTeam Meetings Integration is not enabled for an account, then irrespective of users and availability of licenses in an account, the **Products and licenses** section in the user information page will display “No Licenses”.

3.1.5.2 Allow Users to Manage Waiting Room in MiTeam Meetings

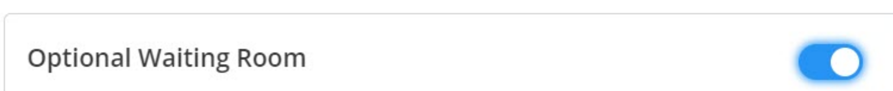
After enabling MiTeam Meetings integration for a customer account, the Mitel Partner or the Account Admin of the customer account can enable or disable a functionality for the users in that customer account to specify, while scheduling a meeting, whether the waiting room will be available to guests who want to join the meeting using the MiTeam Meetings application. To do this, the Mitel Partner or the Account Admin must perform the following procedure:

1. From the **Integrations** panel, click the  icon associated with **MiTeam Meetings** integration.

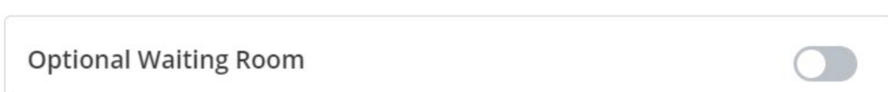
The **MiTeam Meetings** panel opens.

2. Enable or disable the option for users:

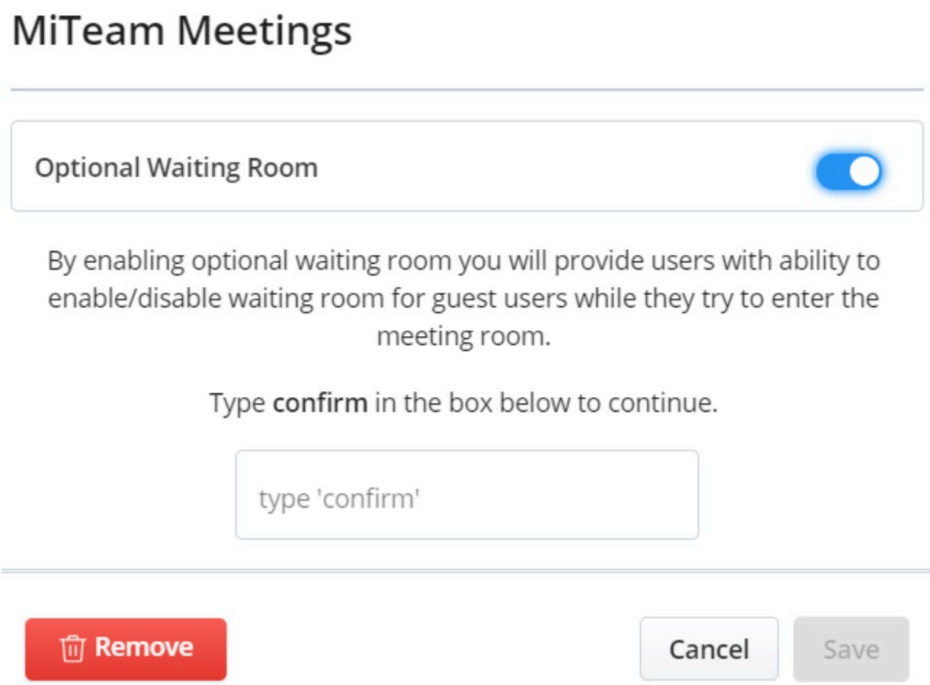
- To enable the option, slide the **Optional Waiting Room** toggle button to the right.



- To disable the option, slide the **Optional Waiting Room** toggle button to the left.



3. Type the word "confirm" in the text box that appears and click **Save**. Clicking **Cancel** will cancel the operation.



Note:
Clicking **Remove** will remove the MiTeam Meetings integration from the customer account.

3.1.6 Mitel Voice Assist Integration

Mitel Voice Assist serves as an auto-attendant for all PBXs that are CloudLink enabled. Utilizing the modern capabilities developed on CloudLink for use in the Mitel Voice Assist package, it presents a completely flexible voice IVR / Auto-attendant solution that can augment any voice platform connected to CloudLink. It includes features such as, Text-to-Speech (TTS), Automatic Speech Recognition (ASR), and Directory.

Prerequisites

To integrate Mitel Voice Assist with a CloudLink customer account, a Mitel Partner or an Account Admin must have CloudLink Gateway integration enabled for users in that account.

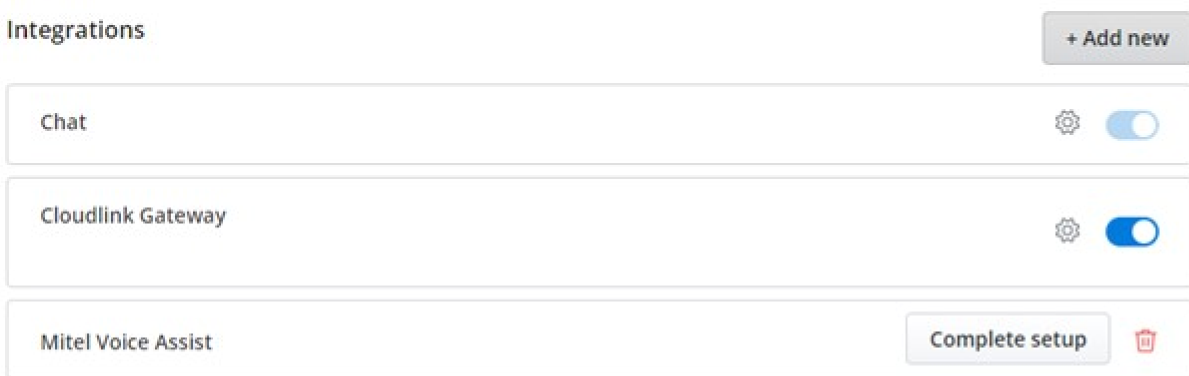
For information about deploying supported PBXs see, Deployment Guide with MiVoice 5000, Deployment Guide with MiVoice MX-ONE, CloudLink Integration with MiVoice Office 400, and Deployment Guide with MiVoice Business.

Procedure

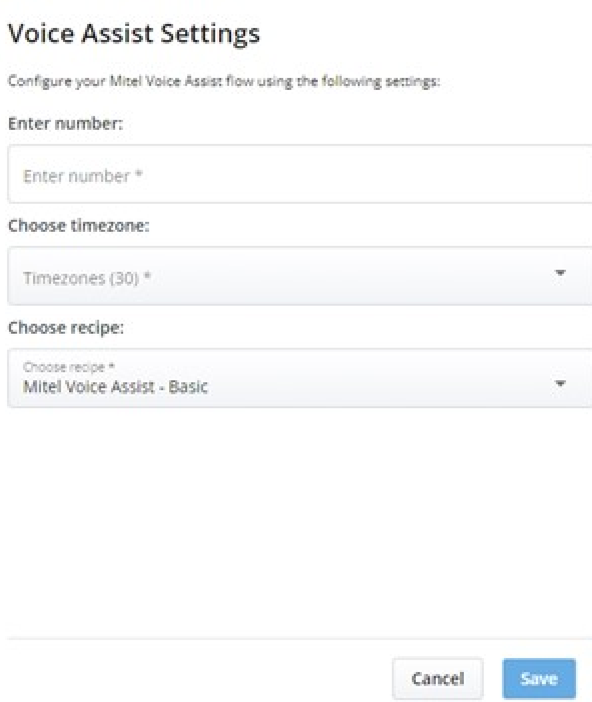
To enable the Mitel Voice Assist application for the customers in a customer account, the Mitel Partner or the Account Admin must add Mitel Voice Assist integration to the customer account. To do this, perform the following steps:

1. Log in to the Mitel Administration on page 1.
2. Access the **Integrations** panel from the **Accounts Information** page or from **Integrations & Apps** option. For more information about accessing **Integrations** panel and adding integration to a customer account see, Adding an integration to a customer account on page 88.
3. In the **Integrations** panel, click **+Add new**. A pop-up screen displays the available integrations.

   After you have added Mitel Voice Assist integration to the customer account, **Mitel Voice Assist** will be listed in the **Integrations** panel.



4. Click the **Complete setup** button to complete the integration. The **Voice Assist Settings** dialog box is displayed.



5. In the **Enter number** field, enter the number that will be used to reach your selected Mitel Voice Assist recipe.

> **Note**:
> The entered number is a pilot number (voice assist number) that is sent from PBX to CloudLink.

6. From the **Choose timezone** drop-down list, select the timezone. The selected timezone is used by the recipe to determine the opening and closing hours.
7. From the **Choose recipe** drop-down list, select the recipe. For more information about the types of recipes see, Mitel Voice Assist.
8. Click **Save** to save the settings.

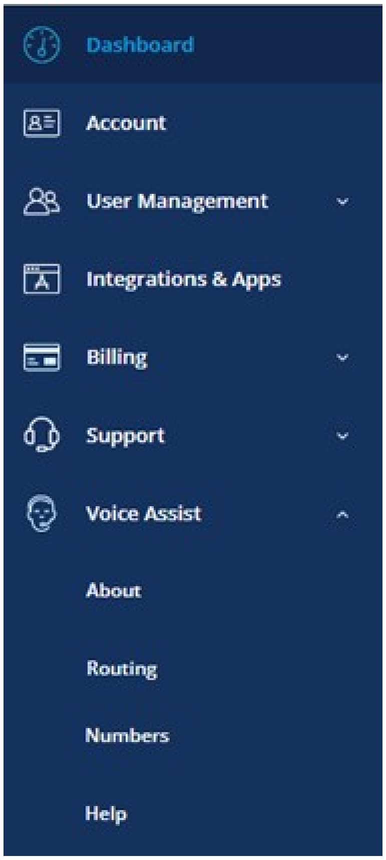
The **Integrations** panel indicates that **Mitel Voice Assist** has been successfully integrated as shown in the following screen capture.

After successful integration of Mitel Voice Assist you can integrate the following PBXs:

- Mitel Voice Assist Integration for MiVoice Business
- Mitel Voice Assist Integration for MX-ONE
- Mitel Voice Assist for MiV5000
- Mitel Voice Assist Integration for MiVoice Office 400

Voice Assist

When Mitel Voice Assist is integrated with a customer account, the **Voice Assist** option is displayed on the left navigation menu of the Accounts console.



Clicking **Voice Assist** displays the following options:

- About
- Routing
- Numbers
- Help

For more information about these options see, Mitel Voice Assist.

Removing Mitel Voice Assist

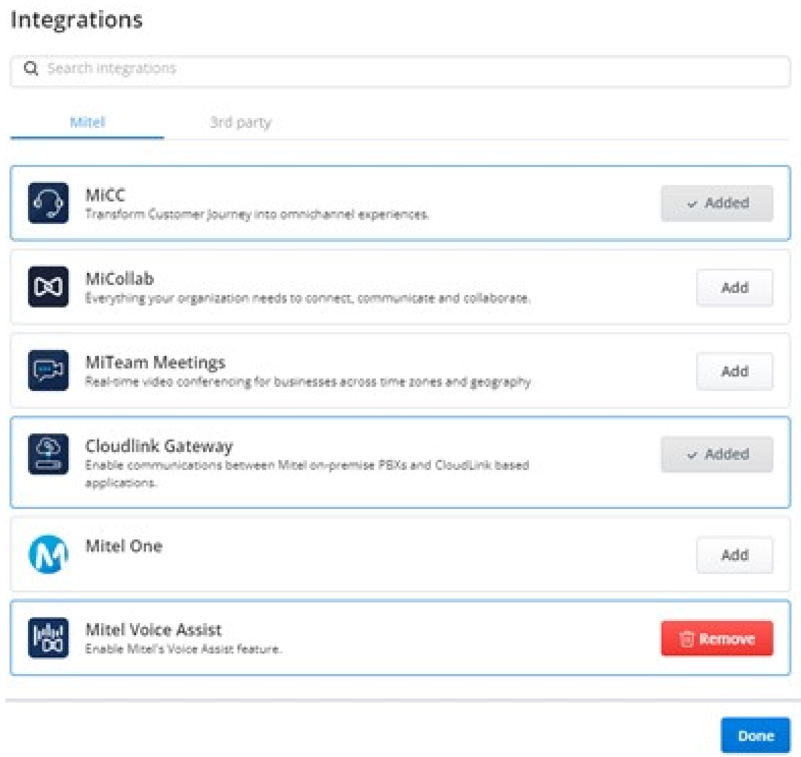
To remove Mitel Voice Assist integration for a user in a customer account perform either of the following:

- From the **Integrations** panel:

  1. Slide the toggle button associated with **Mitel Voice Assist** to the left. The **Remove Mitel Voice Assist Integration** dialog box is displayed.
  2. Click **Remove integration**. The Mitel Voice Assist integration is removed from the customer account.

- From the **Integrations and Applications** list:

1. Click the **+ Add new** button and hover over the **Added** button associated with **Mitel Voice Assist**. The **Remove** button is displayed.



2. Click **Remove** and then click **Done**. **Remove Mitel Voice Assist Integration** dialog box is displayed.
3. Click **Remove integration** to remove Mitel Voice Assist integration. Click **Cancel** to cancel the operation.

For more information about removing an integration from a customer account see, Removing an integration from a customer account on page 92.

3.1.6.1 Mitel Voice Assist Integration for MiVoice 5000

After integrating Mitel Voice Assist with a CloudLink customer account a Mitel Partner or an Account Admin can integrate Mitel Voice Assist for MiVoice 5000. To do this, you must create a Trunk, and set the characteristics.

To create a trunk in MiVoice Office 5000 portal, navigate to **Telephony services** > **Network and links** > **Network** > **Trunk Groups** > **Names (4.2.1.1)**.

To set the characteristics of the trunk, perform the following steps:

1. Navigate to **Telephony services** > **Network and links** > **Network** > **Trunk groups** > **Characteristics (4.2.1.2)**.
2. Select the **Subtype** as **CLOUDLINK** and click **Characteristics** button.

3. Provide port other than 5070 and select **Proxy checking** as **IP Address**.

After successfully creating Trunk and setting the characteristics, navigate to **Dialing plan** > **User dialing plan** > **Access to directions** > **Access to CLINK** and add the **Access code** and **Length of next number** to access the code for CloudLink.

To create routes, navigate to **Telephony service** > **Network and links** > **Network** > **Routes (4.2.2)**.

Note:
After successful Trunk configuration and subsequent changes to the setup, ensure that you perform resync from MiVoice 5000 in CloudLink Gateway menu

For more information about how to configure SIP Trunks see, Mitel 5000 Server - Operating Manual and for information about DID Numbers see, Managing DID Numbers.

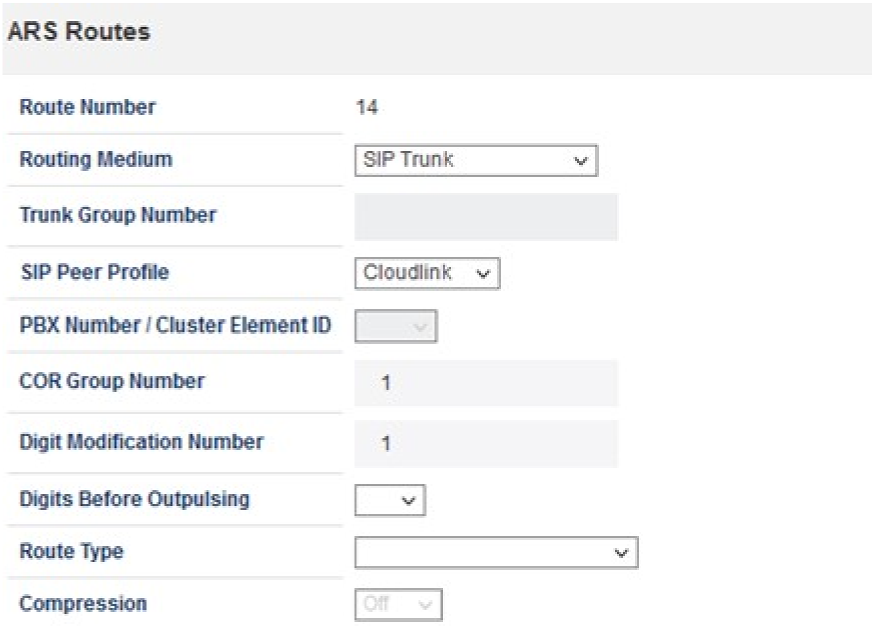
3.1.6.2 Mitel Voice Assist Integration for MiVoice Business

After integrating Mitel Voice Assist with a CloudLink customer account a Mitel Partner or an Account Admin can integrate Mitel Voice Assist for MiVoice Business.

To do this, you must create ARS Route, and add ARS Digits Dialed for CloudLink.

To create ARS Route, perform the following steps:

1. In the MiVoice Business System Administration Tool, navigate to **Call Routing** > **Automatic Route Selection (ARS)** > **ARS Routes**.



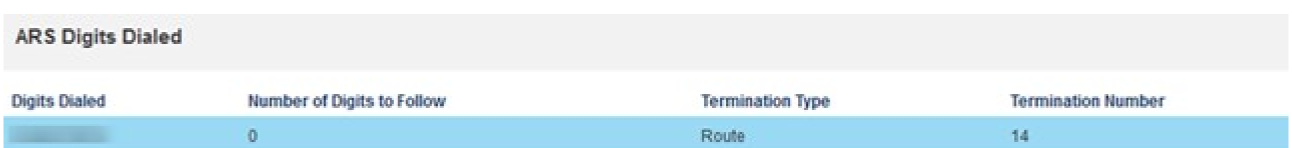
2. From the drop-down list under **Routing Medium** select **SIP Trunk**.
3. From the drop-down list under **SIP Peer Profile** select **CloudLink**.

> **Note**:
> **CloudLink** was created as SIP Peer Profile as a part of gateway onboarding process.

4. Click **Save**. For more information about creating ARS Routes see, ARS Routes in *MiVoice Business System Administration Tool Help*.

To add ARS Digits Dialed, perform the following steps:

1. In the MiVoice Business System Administration Tool, navigate to **Call Routing** > **Automatic Route Selection (ARS)** > **ARS Digits Dialed**.

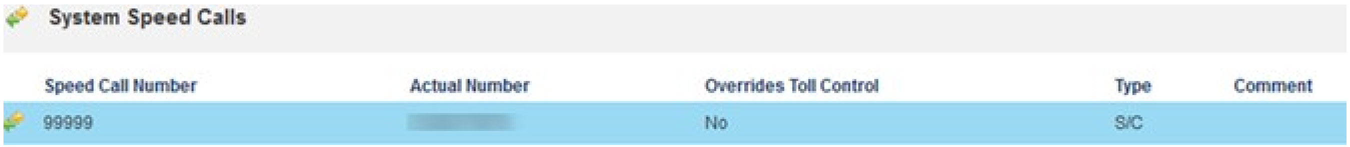


2. Click **Add** to add the entry for CloudLink.

The Mitel Partner or an Account Admin can make a PSTN call flow into CloudLink. To do so, the caller can dial the pilot number (voice assist number) that was entered while integrating Mitel Voice Assist Integration (Step number 4, under *Procedure*.

For internal calls to the Voice Assist Route, Mitel Partner or an Account Admin can create a System Speed Calls Numbers that is mapped to the Workflow Pilot Number. To do so, navigate to **System Properties** >

System Feature Settings > **System Speed Calls**. For more information about System Speed Calls see, System Speed Calls in *MiVoice Business System Administration Tool Help*.



3.1.6.3 Mitel Voice Assist Integration for MX-ONE

After integrating Mitel Voice Assist with a CloudLink customer account, a Mitel Partner or an Account Admin can integrate Mitel Voice Assist for MX-ONE. To do this, you must create a SIP route between MX-ONE and CloudLink Gateway and destination code must be assigned to it for routing of calls to Mitel Voice Assist.

Destination code is usually the same as the Pilot number of Mitel Voice Assist and must be part of the Direct In Dialling (DID) number range to be able to reach Mitel Voice Assist from the Public PSTN Network.

To create a SIP route, perform the following steps:

1. In the MX-ONE Service Node Manager navigate to **Telephony** > **External Lines** > **Route**.
2. Set the **Type of Signalling** to **SIP** and **Profile Name** to **CloudLink Gateway**.
3. Chose a suitable Route name and select an available route number.
4. Equip the route with trunk individuals for the server that connects to the CloudLink Gateway, i.e., Server 1 1-10. This would allocate 10 SIP channels to the route.
5. Enter the specific CloudLink Gateway information such as CloudLink Authentication username, CloudLink Authentication username password, and Remote Proxy IP of CloudLink Gateway and click **Apply**. The SIP route is created. For more information about deploying CloudLink with MX-ONE see, CloudLink Deployment Guide with MX-ONE.

> **Note**:
> For release MiVoice MX-ONE 7.5 SP0, configured SIP route must be modified using mml *sip_route* command to remove the "+" sign from -uristring0 (sip_route -set -route X -uristring0 sip:?@<clgw-ip).

To assign Destination Code to the created SIP route, perform the following steps:

1. In the MX-ONE Service Node Manager navigate to **Telephony** > **External Lines** > **Destination**.
2. Add a new **Destination Code**.
3. Select the **Start Position for Digit Transmission** from the drop-down list to send digits matching the Pilot Number only.
4. Click **Apply** to save.

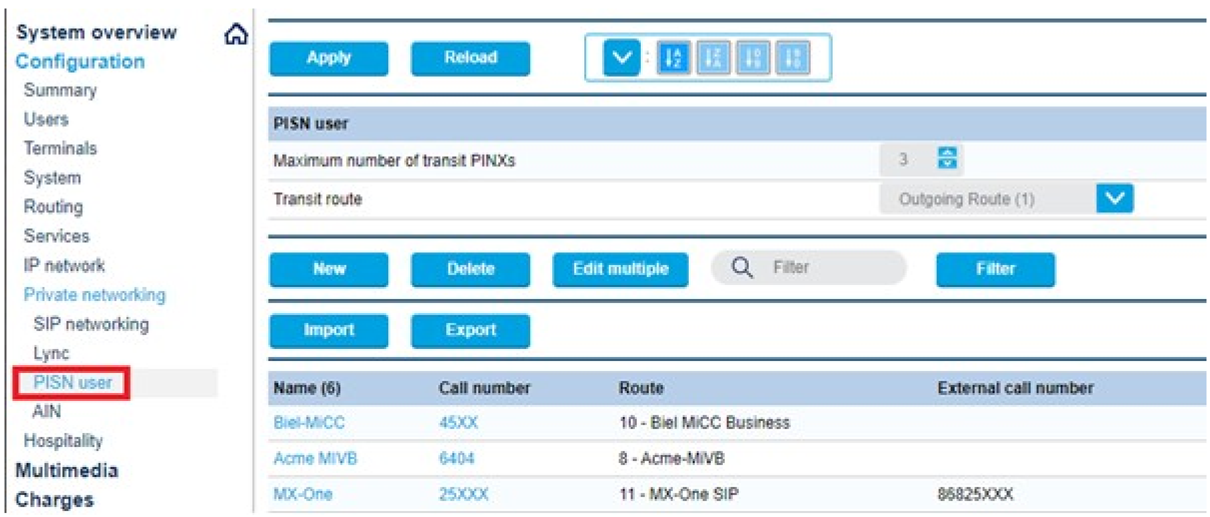
3.1.6.4 Mitel Voice Assist Integration for MiVoice Office 400

After integrating Mitel Voice Assist with a CloudLink customer account, a Mitel Partner or an Account Admin can integrate Mitel Voice Assist for MiVoice Office 400. To do this you must configure PISN Users.

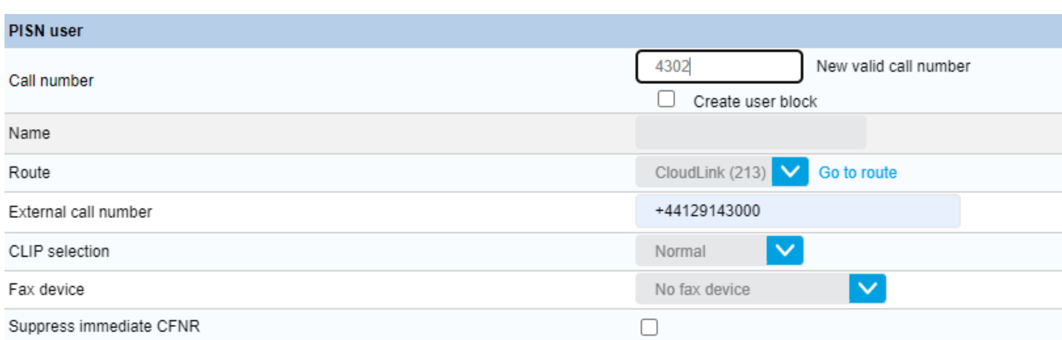
A PISN user refers to an internal directory number within a Private Integrated Services Network (PISN) that is used to route calls across the private network to a remote endpoint located on another SIP server, PBX or cloud-based service provider such as CloudLink.

To configure PISN User, perform the following steps:

1. Log in to MiVoice Office 400.
2. On the left navigation panel, navigate to **Configuration** > **Private networking** > **PISN User**.

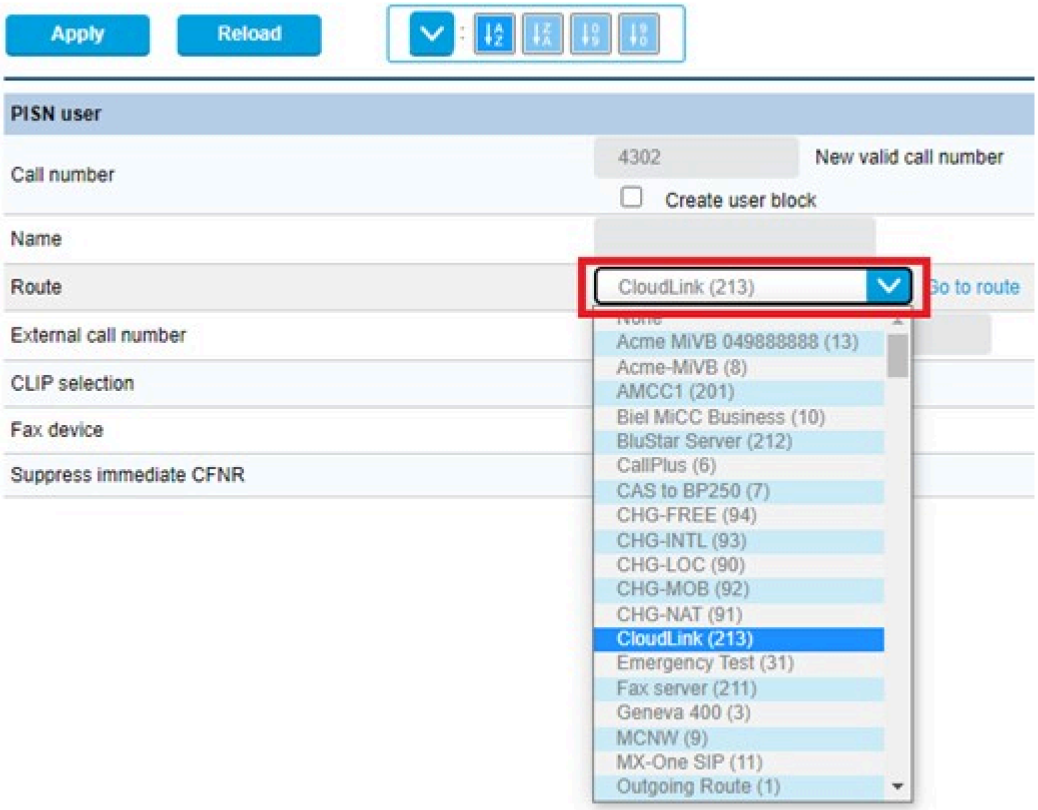


3. Click **New**. PISN user page is displayed.
4. Enter a unique **Call number**.



Note:
Ensure that you enter the same number manually, both in Voice Assist and in the PBX.

5. From the **Route** drop-down list, select **CloudLink(213)**.



Note:
The route is displayed in the **Route** drop down list only if the CloudLink Gateway is deployed successfully.

6. Enter an **External call number**. Once configured, the number is used for routing the call in **Voice Assist**, it can be a DDI/DID or a Toll Free Number etc. but it must match an entry in the **Number Table**. This number is also sent externally or to the MiVoice Office 400 depending on the workflow to help identify the callers origin or destination.
7. Click **Apply** to save the configuration.

Note:
After successful configuration of a PISN user, it can either be dialled internally or used as a routing destination for external calls. When dialed, it will direct the call to the Voice Assist call flow associated with that number and follow the configured flow.

3.1.7 Unify Phone Integration

Unify Phone is a communication application that was originally designed as a telephony client but has since been extended to offer additional collaboration features. Initially focused on voice calling, it now includes CloudLink Chat, providing businesses with a more comprehensive communication solution. Unify Phone integrates seamlessly with existing PBX systems, such as Mitel OpenScape PBXs and Mitel MiVoice PBXs, and is available on both desktop and mobile platforms, allowing users to stay connected from anywhere.

Adding Unify Phone Integration to a customer account supports two primary use cases:

- When **Unify Phone** is already configured to work with an **OpenScape PBX**, it enables CloudLink Chat within the Unify Phone application.
- When a **MiVoice PBX** is linked to the CloudLink customer account, it allows users who exist in both the PBX and the CloudLink account to access the Unify Phone application and use both telephony and CloudLink Chat features offered through the application.

The integration is currently supported with the following PBXs:

- **OpenScape PBXs**: OpenScape Business
- **MiVoice PBXs**: MiVoice 5000.

3.1.7.1 Adding the Unify Phone integration to a customer account

To add the Unify Phone integration to a customer account, perform the following steps:

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. In the **Integrations** panel, click **+ Add new**.

   The **Integrations** pop-up window opens.
3. Click **Add** next to the **Unify Phone** integration, then click **Done**.

   The Unify Phone integration is added to the customer account and it is displayed in the **Integrations** section of the **Account Information** page.
4. Make sure that the **Delegated Authentication** toggle button under the **Privileges** section is enabled (switched to ON).

> **Note**:
> By default, Delegated Authentication is enabled when the Unify Phone integration is added. If it is not already enabled, manually switch the **Delegated Authentication** toggle button to ON.

Note:
Mitel Partners 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. For more information about Partner Accounts, see Log in as a Mitel Partner.

3.1.7.2 Enabling the Unify Phone integration in a customer account

After adding the Unify Phone integration to a customer account, you need to provide the necessary details to enable the integration. You can either enter the details of an existing Unify Phone tenant or the information required to create a new tenant. Regardless of the option selected, the tenant will be linked to the customer's CloudLink account at the end of the process.

- Link a pre-existing Unify Phone tenant if Unify Phone is already configured to work with an OpenScape PBX (such as OpenScape Business), and you want to enable CloudLink Chat within the Unify Phone application.
- Create a new Unify Phone tenant if the customer uses a MiVoice PBX (such as MiVoice 5000), and you want users in the CloudLink account to be able to access the Unify Phone application.

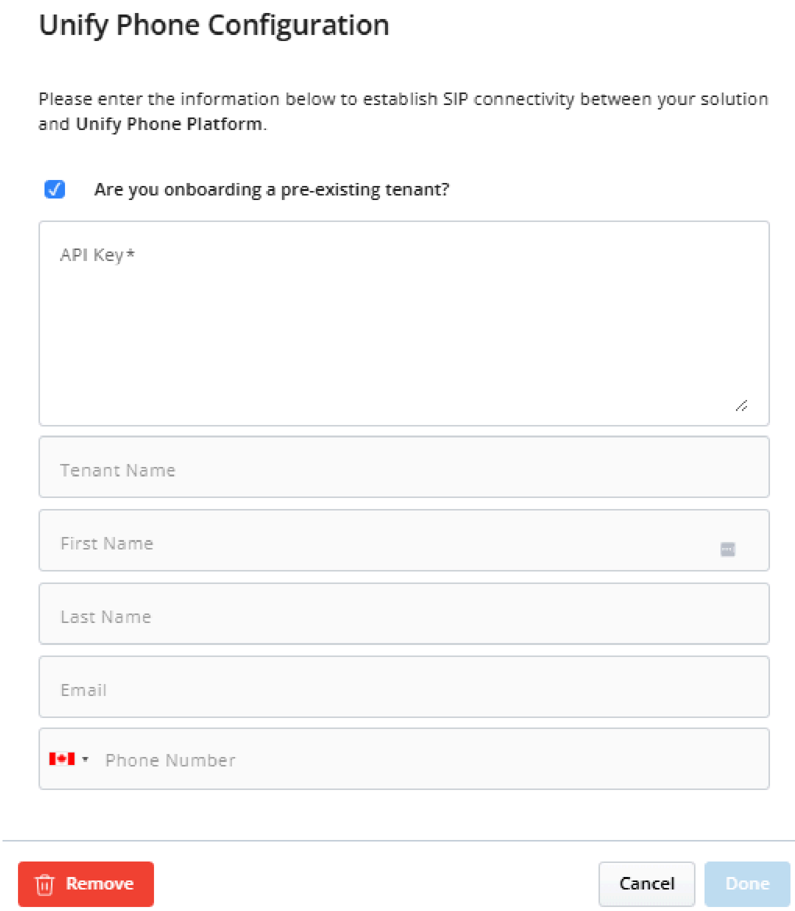
Perform the following steps to enable the integration:

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. Click **Complete Setup** next to the **Unify Phone** integration.

   The **Unify Phone Configuration** page opens.

3. If you are on-boarding a pre-existing tenant:

   a. Select the **Are you onboarding a pre-existing tenant?** checkbox.



   The **API Key*** field appears, and all other input fields are disabled.

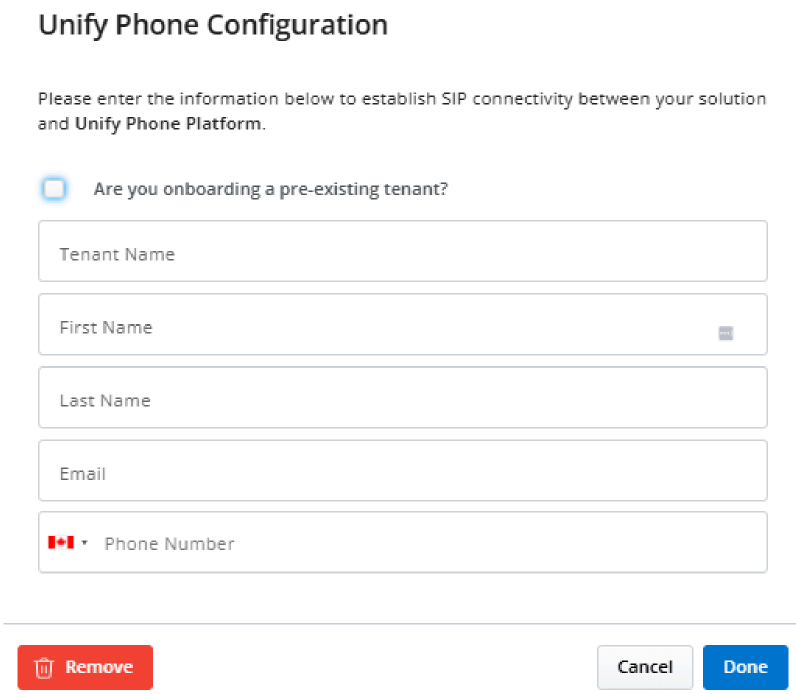
   b. Enter the API key that you can find in the **Telephony connector** tab of the Unify Phone administration app.

   The API key is a unique identifier used to authenticate a client or an application when making API (Application Programming Interface) requests. It is required to enable access to the existing Unify Phone tenant through the Unify Phone Administration and Admin REST API.

   c. Click **Done** to link the existing tenant to the customer's CloudLink account.

4. If you are creating a new Unify Phone tenant:

a. Make sure the **Are you onboarding a pre-existing tenant?** checkbox is not selected.



b. Enter a **Tenant name**. Although not required, it is highly recommended to enter a tenant name. The tenant name must be unique across all accounts.

c. Enter the following main contact details for the Unify Phone tenant. Leaving these fields empty will result in the tenant inheriting values from the Account Administrator:

- **First name**
- **Last name**
- **Email**
- **Country Code**
- **Phone number**

d. Click **Done** to create and link the new tenant to the customer account.

Note:

Once the Unify Phone integration is enabled, the tenant details—whether pre-existing or new—cannot be edited. If you need to update the tenant details, you must first remove the integration, then add it back and enable the integration again by providing the correct information.

3.1.7.3 Configuring SIP connectivity

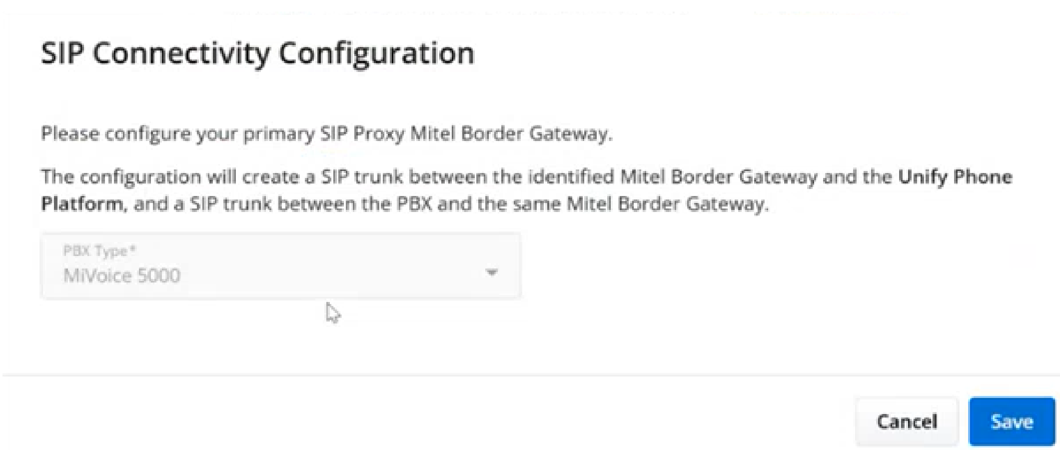
After enabling the Unify Phone integration, the next step is to configure SIP connectivity. This process establishes a secure communication path between the Unify Phone service and the customer's PBX system.

Note:
SIP connectivity configuration is currently applicable only for CloudLink accounts integrated with MiVoice 5000—meaning the account's system inventory must include a MiVoice 5000 system.

Starting the SIP connectivity configuration

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. Click the **Available features** drop-down list under the **Unify Phone** integration.
3. Click **Complete Setup** next to **SIP Connectivity**.

   The **SIP Connectivity Configuration** page opens.



4. Select the appropriate **PBX Type** from the drop-down list.

   If only one PBX type is available, it will be preselected and the field will be disabled.
5. Click **Save**.

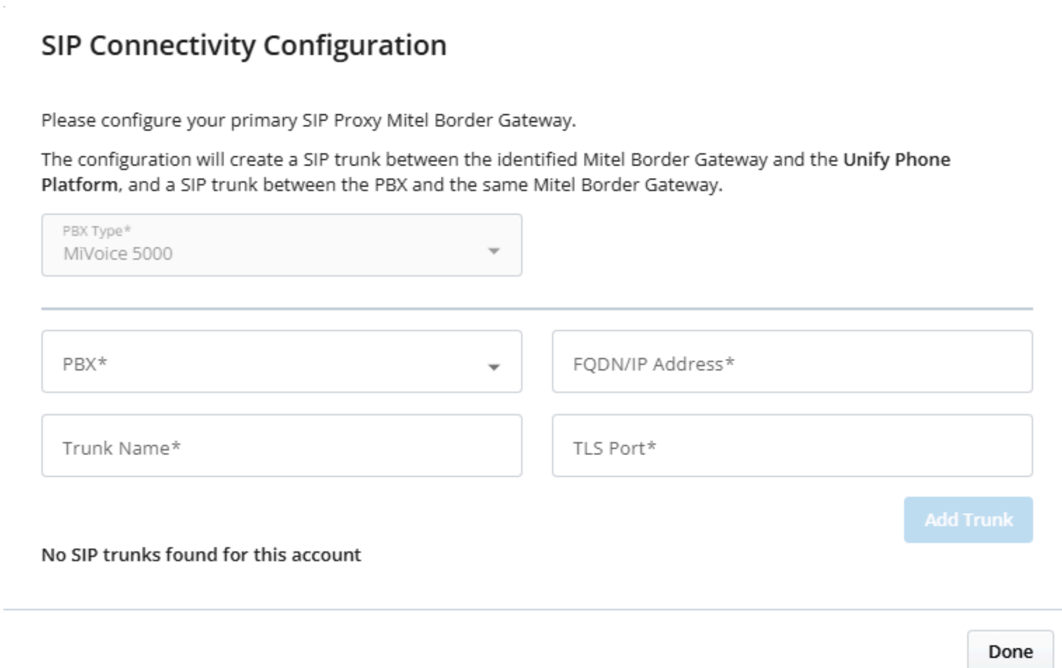
Important:
Once saved, the PBX type selection cannot be changed. To modify it, you have to remove the Unify Phone integration, re-add it to the account, and repeat the setup steps.

Adding and managing SIP trunks

After completing the initial SIP connectivity configuration, you can add SIP trunks to establish communication between Unify Phone and the customer’s PBX system. Youc an also edit, delete, sort, and search for trunks as needed.

1. To add the first SIP trunk:

   On the **SIP Connectivity Configuration** page, a form to add SIP trunk appears.



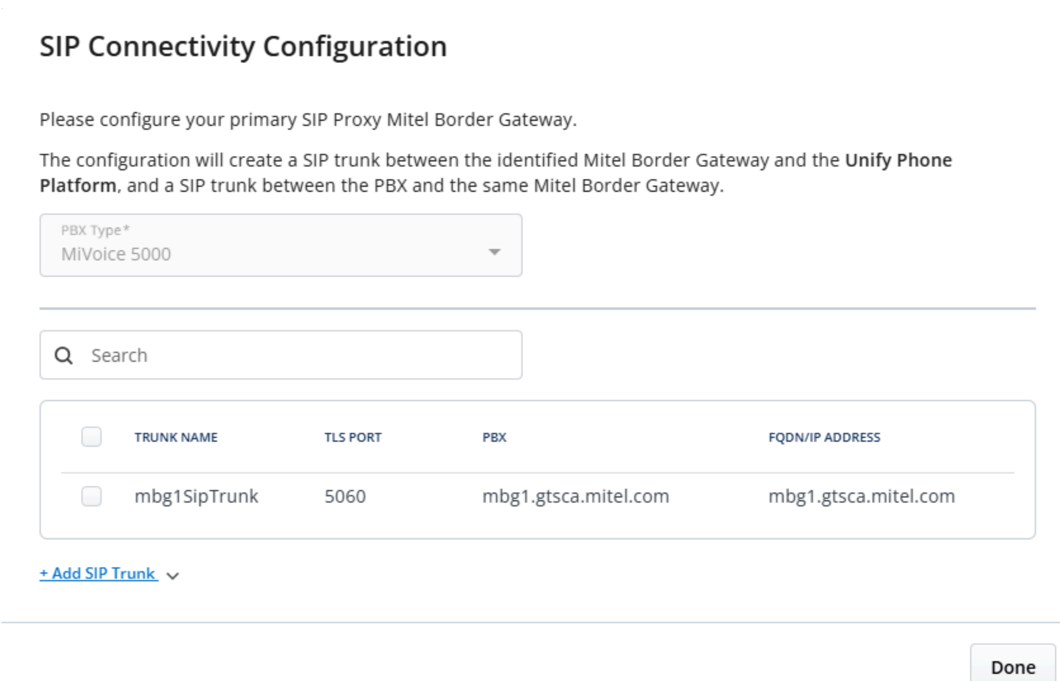
   a. Select a **PBX** from the drop-down list of available PBXs.
   b. In the **FQDN/IP Address** field, enter the Fully Qualified Domain Name (FQDN) or IP address of the selected PBX.

> **Note**:
> This field is auto-populated based on the selected PBX but can be manually overridden if needed.

c. In the **Trunk Name** field, enter the name of the SIP trunk.
d. In the **TLS Port** field, enter the port number on which the SIP trunk listens for incoming requests that use the TLS protocol.
e. Click **Add Trunk**.

The added SIP trunk appears in a table displaying the following details:

Name	Description
TRUNK NAME	The name of the SIP trunk
TLS PORT	The port number used for TLS-based incoming SIP requests
PBX	The PBX type followed by its IP address
FQDN/IP ADDRESS	The Fully Qualified Domain Name (FQDN) or IP address of the PBX



2. To add another SIP trunk:

   a. Click **+Add SIP trunk**.

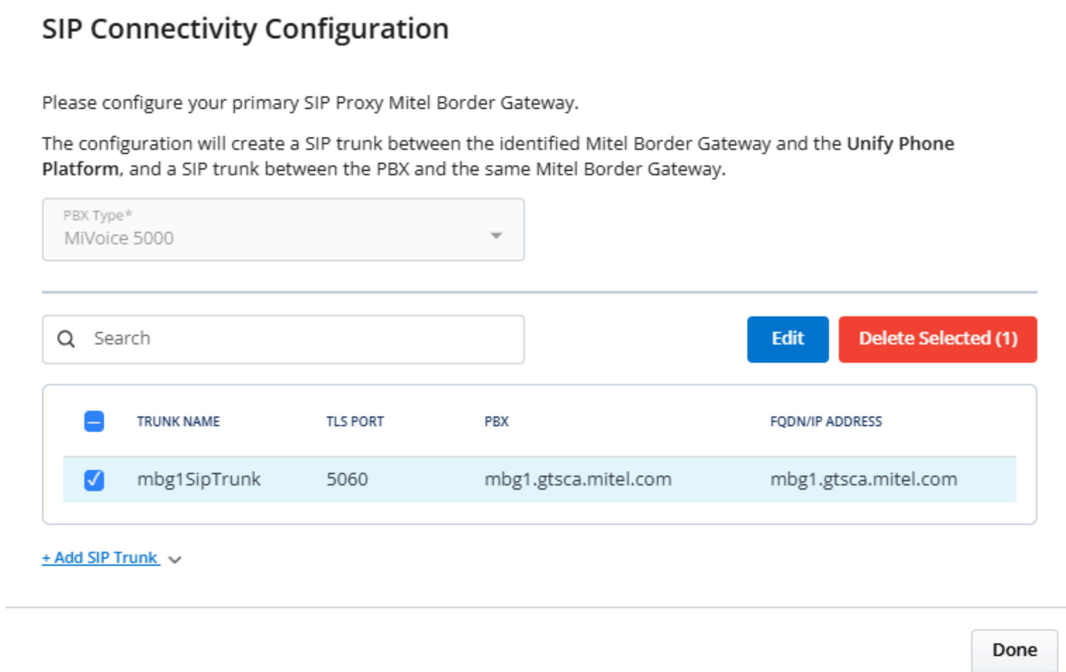
      The **Add SIP Trunk** section expands, displaying a blank form.

   b. Enter the new SIP trunk details as described above.
   c. Click **Add Trunk**.

   The new trunk is added to the SIP trunks table.

3. To edit an existing SIP trunk:

   a. Select the checkbox associated with the SIP trunk you want to edit.
   b. Click the **Edit** button that appears.



      The **Edit SIP Trunk** section appears and expands, displaying the current trunk details pre-filled for editing.

   c. Modify the fields as needed.
   d. Click **Save** to apply changes or **Cancel** to discard them.

   Changes are reflected immediately in the SIP trunks table.

4. To delete one or more SIP trunks:

   a. Select the checkbox(es) next to the SIP trunks(s) you want to delete.
   b. Click the **Delete Selected** button that appears.
   c. Confirm the deletion by clicking **Delete** or cancel the action by clicking **Cancel**.

   The selected trunk(s) will be removed from the SIP trunks table.

5. To sort the SIP trunks:

   a. Click a column header in the SIP trunks table to sort the entries by that column's values in ascending order.
   b. Click the same header again to toggle the sort to descending order.

   An upward-pointing arrow (↑) next to a column header indicates ascending order. An downward-pointing arrow (↓) next to a column header indicates descending order.

6. To search for a SIP Trunk:

   a. In the **Search** bar, type the **TRUNK NAME**, **TLS PORT**, **PBX** or **FQDN/IP ADDRESS** of the SIP trunk you are searching for.

      The table will display a list of matching trunks as you type.

7. To finalize the configuration and close the **SIP Connectivity Configuration** page, click **Done**.

3.1.7.4 Updating the SIP connectivity configuration

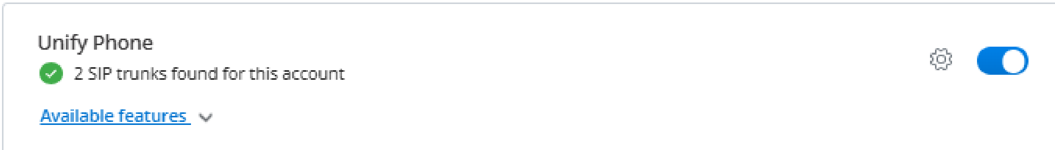
Once SIP connectivity is configured, you can update it at any time as needed. However, only SIP trunk information can be modified—the selected PBX type cannot be changed after the initial configuration.

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. Click the **Available features** drop-down list under the **Unify Phone** integration.
3. Click ⚙ next to **SIP Connectivity**.
   The **SIP Connectivity Configuration** page opens.
4. Add, edit, or delete SIP trunks as described in Adding and managing SIP trunks on page 164.

3.1.7.5 Viewing the Unify Phone integration status

Once the Unify Phone integration is added to a customer account, you can easily check its status to ensure it is set up correctly. The status provides insights into whether the integration is functioning as expected.

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. In the **Integrations** panel, locate the **Unify Phone** integration. Check the status icon and message next to it:



The icon indicates the current status of the integration, which can be one of the following:

- `Connected`
- `Error`
- `Incomplete`

The status message provides additional context about the integration's current state.

3.1.7.6 Viewing users with a Unify Phone license

Unify Phone licenses are assigned to users in a CloudLink account through the PBX's user provisioning tool. To view users in the account who have been assigned a Unify Phone license, follow the steps below:

1. Navigate to **User Management** > **Users** from the left main menu.

   The list of users is displayed.
2. In the user list, locate the **LICENSES** column. Use the filter options to show only users assigned the Unify Phone license:

   a. Click **Add Filter** Add Filter .
   b. From the drop-down list, select **Product**.
   c. From the list of properties that is displayed, select **Unify Phone**.

      The user list is updated to show only users with the Unify Phone license.
3. Click on an individual user in the list to view detailed information, including their assigned licenses.

3.1.7.7 Viewing the Unify Phone configuration

Once the Unify Phone integration is enabled, you can view the configuration details of the Unify Phone tenant linked to the customer account at any time.

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. In the **Integrations** panel, click next to the **Unify Phone** integration.

The **Unify Phone Configuration** page opens displaying the tenant name and the main contact details associated with the Unify Phone tenant.

Note:

Tenant details are view-only and cannot be edited.

3.1.7.8 Removing the Unify Phone integration from a customer account

To remove the Unify Phone integration from a customer account, follow the steps below:

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. If the integration setup is complete:
   - Switch the toggle button next to the **Unify Phone** integration to OFF.
   - Alternatively, click next to the **Unify Phone** integration, then click **Remove**.
3. If the integration setup is incomplete:
   - Click next to the **Unify Phone** integration.
   - Alternatively, click **Complete setup** next to the **Unify Phone** integration, then click **Remove**.
4. In the confirmation dialog, click **Remove integration** to proceed, or **Cancel** to abort the action.

Note:

- Removing the Unify Phone integration from a customer account will revoke the Unify Phone license from all users who had it previously assigned.
- Removing the Unify Phone integration from a customer account will not delete the Unify Phone tenant that is linked to the account.

3.1.8 Mitel Workflow Studio Integration

Mitel Workflow Studio is a subscription-based entitlement. It enables workflow automation capabilities within the CloudLink platform.

Table 2: Entitlement Quantities by Tier

Workflow Subscription Tier	WFS Entitlement Quantity
Essential	100 interactions
Premier	100 interactions

Table 3: SKU Mapping by Term

Term	SKU	Workflow Subscription Tier
Monthly	54014777	Premier
Monthly	54014776	Essential
12-month	54014772	Premier
36-month	54014773	Premier
60-month	54014774	Premier
12-month	54019078	Essential - free
36-month	54019079	Essential - free
60-month	54019080	Essential - free
12-month	54019081	Premier - free
36-month	54019082	Premier - free
60-month	54019083	Premier - free
12-month	54014769	Essential
36-month	54014770	Essential
60-month	54014771	Essential
N/A	54014775	Workflow Studio Base Kit - NC

Execution Limits:

- The **base subscription** includes:
  - **500 Essential** flow executions per billing period.
  - **500 Premier** flow executions per billing period.
- Additional entitlements can be added in **units of 100**.

Provisioning and Lifecycle Behavior

- Subscription upgrades increase WFS quantities accordingly.
- Subscription downgrades or cancellations revoke WFS licenses.
- Term changes (e.g., from 12-month to 36-month) trigger re-evaluation of WFS entitlements.

3.1.8.1 Adding the Mitel Workflow Studio integration to a customer account

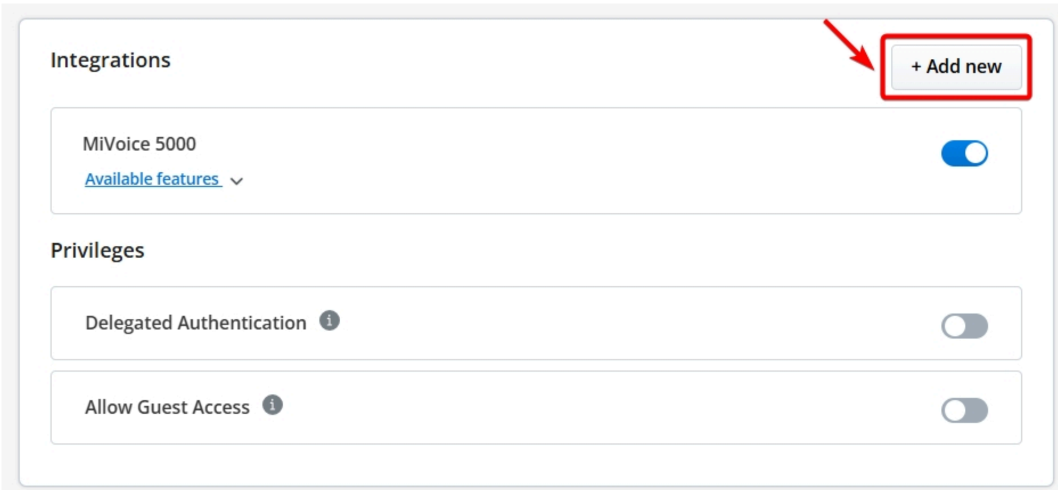
To add the Mitel Workflow Studio integration to a customer account, perform the following steps:

1. **Access the Integrations panel**.

   Do one of the following:

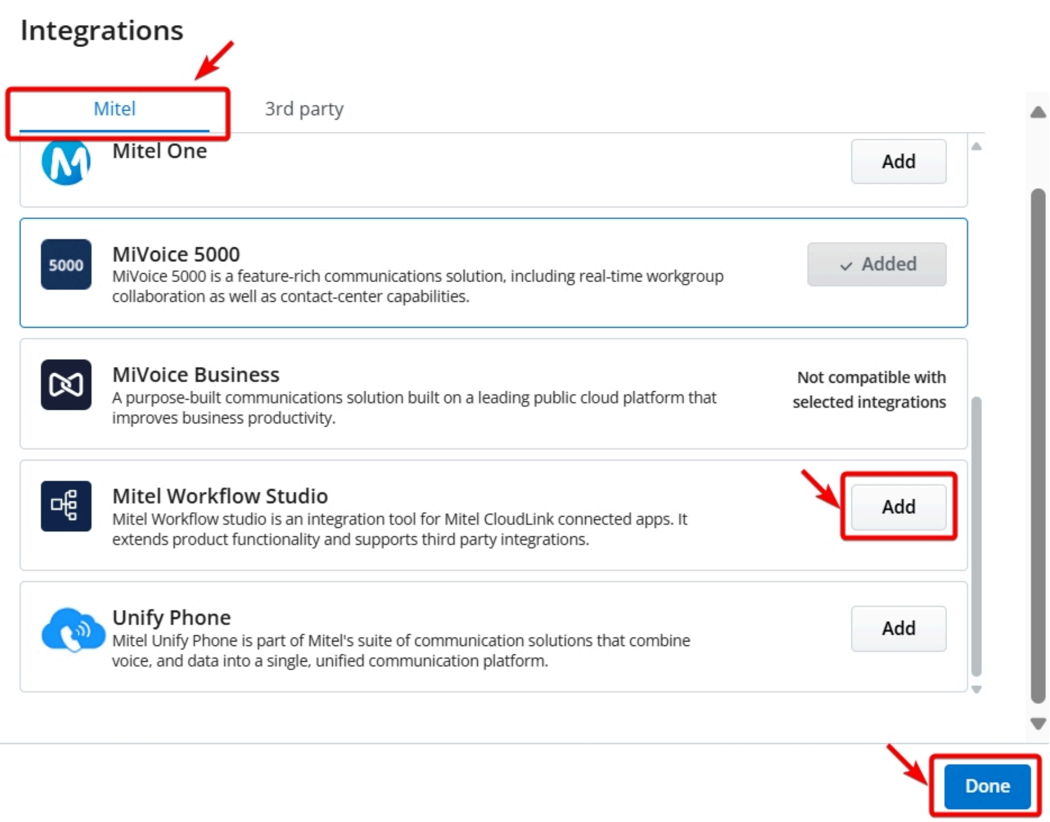
   - From the **Account Information** page, scroll to the **Integrations** section (or) from the left navigation menu, click **Integrations & Apps**.

2. Click **+ Add new**.



   The Integrations pop-up window opens.

3. In the **Mitel** tab, locate **Mitel Workflow Studio**, click **Add**, and then click **Done**.



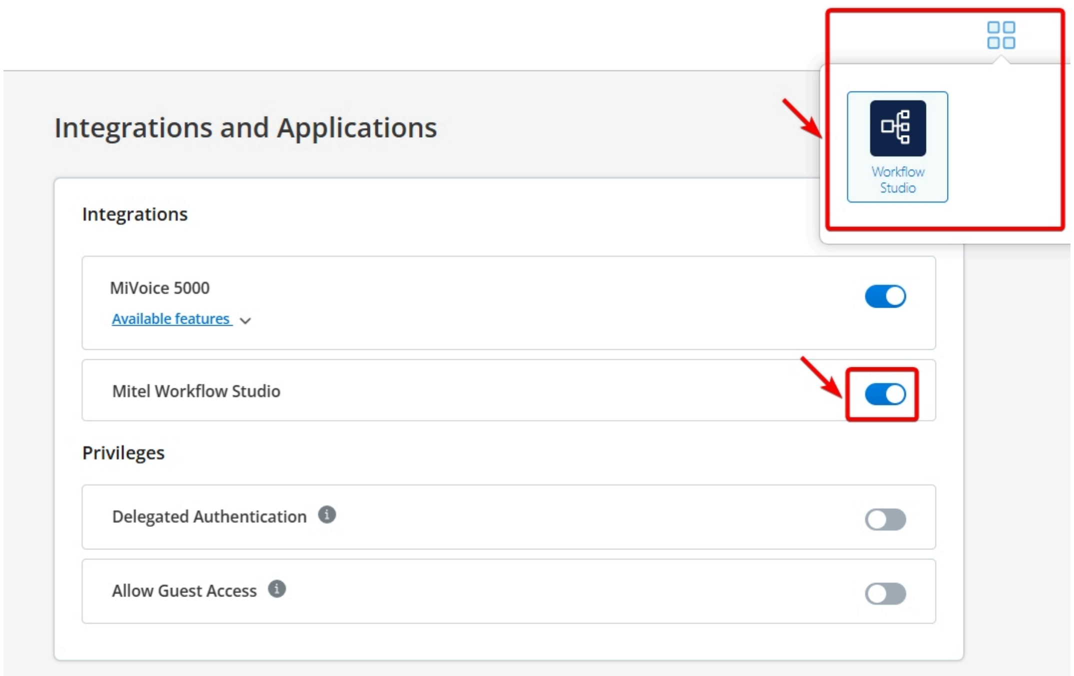
4. The **Mitel Workflow Studio** is added to the customer account and it is displayed in the **Integrations** section.

> **Note**:
> Mitel Partners 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. For more information about Partner Accounts, see Log in as a Mitel Partner.

3.1.8.2 Enabling the Mitel Workflow Studio integration in a customer account

To add the Mitel Workflow Studio integration to a customer account, perform the following steps:

1. Access the **Integrations** panel from the **Account Information** page or from the **Integrations & Apps** option.
2. Locate the **Mitel Workflow Studio** and slide the toggle switch to the **ON** position.



The Mitel Workflow Studio icon will now appear in the **Application Launcher** for users in the account.

3.1.8.3 Accessing Mitel Workflow Studio

Once enabled, users can access Mitel Workflow Studio through the **Application Launcher** in the **Mitel Administration Portal**:

- Click the **Application Launcher** icon in the top-right corner of the portal.
- Select **Mitel Workflow Studio** from the list of available applications.

3.1.8.4 Removing the Mitel Workflow Studio integration from a customer account

To remove the Mitel Workflow Studio integration from a customer account, perform one of the following:

From the Integrations panel:

1. Slide the toggle button associated with **Mitel Workflow Studio** to the **OFF** position.
2. The **Remove Mitel Workflow Studio Integration** dialog box is displayed.
3. Click **Remove integration**.

From the Integrations and Applications list:

1. Click **+ Add new** and hover over the **Added** button next to **Workflow Studio**.
2. Click **Remove**, then click **Done**.
3. In the confirmation dialog box, click **Remove integration**.

Result:

- The **Mitel Workflow Studio integration is removed** from the customer account.
- The **Mitel Workflow Studio icon** is no longer visible in the **Application Launcher** for users in that account.
- Users will **no longer have access** to Mitel Workflow Studio features unless the integration is re-enabled.

3.2 Integrating Third Party Applications with Mitel Administration

3.2.1 Integrating Zoom with Mitel Administration

Zoom is a cloud-based phone system that provides voice communication features such as call management, call forwarding, voicemail, and integration with Zoom Meetings.

Zoom is integrated with Mitel Administration to allow customers to extend their communication infrastructure through the CloudLink accounts.

You can configure integrations with Zoom using Mitel Administration.

If Zoom integration is enabled for a customer account, users in that account can integrate their Zoom account with their CloudLink applications.

Zoom Integration is supported with the following PBXs:

- OpenScape 4000
- OpenScape Voice
- MiVoice Business

Note:

For MiVoice Business, Zoom Integration is supported only in environments where both the CloudLink Gateway is deployed and the CloudLink Daemon is enabled on MiVoice Business nodes that function as primary user controllers, secondary resilient failover user controllers, or have a CloudLink SIP trunk. It is not supported if the CloudLink Gateway is deployed separately from the MiVoice Business nodes.

3.2.1.1 Adding Zoom integration to a customer account

To add the Zoom integration to a customer account perform the following steps:

1. Click **Account** from the left main menu.

   The **Account Information** page of the customer account opens.
2. In the **Integrations** section, click **+ Add new**.

   The **Integrations** pop-up window opens.
3. Click the **3rd party** tab.

   A list of supported third-party applications are displayed.
4. Click **Add** next to the **Zoom** integration and then click **Done**.
5. The Zoom integration is added to the customer account and it is displayed in the **Integrations** section of the **Account Information** page.

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.

3.2.1.2 Enabling Zoom integration in a customer account

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

Perform the following steps to enable the integration:

1. Click **Account** from the left main menu.
   The **Account Information** page of the customer account opens.
2. Click **Complete Setup** next to the **Zoom** integration in the **Integrations** section.
   The **Zoom Integration Configuration** page opens.
3. Click **Connect**.
   The Zoom Sign In window opens.

   If you have already signed in, then you will be redirected to the Zoom Authentication window.
4. Enter the credentials and click **Sign In**.
   The Zoom Authorization window opens.
5. Click **Allow** to give permission to Zoom application to access and use the CloudLink account information.

> **Note**:
> If you click **Decline**, the Zoom integration will not be enabled and the Zoom Authorization window will not close. To continue, close the Zoom Authorization window. Click **Connect** again on the Zoom Integration Configuration page and then click **Allow** on the Zoom Authorization window.

3.2.1.3 Removing Zoom integration from a customer account

You can remove an existing Zoom integration from a customer account.

Perform the following steps to remove the integration:

1. Click **Account** from the left main menu.
   The **Account Information** page of the customer account opens.
2. Locate the **Zoom** integration in the **Integrations** area.
3. Disable the toggle button associated next to the **Zoom** integration.
4. Click **Remove integration** in the pop up confirmation window.
   You can click **Cancel** to cancel the action.

The integration is not removed immediately. Once the integration is deleted and you are still logged in you will receive a notification message.

If the integration has been deleted but still appears in the Integrations list, click **Refresh** in the notification message. The Integrations list will be updated and the Zoom integration will be removed.

Note:
If there is an issue with the removal of the integration, an error message is displayed.

Note:
When the Zoom integration is removed from an account with MiVoice Business, the associated Zoom PSI license is revoked from all users who had it previously assigned. However, the MiVoice Business service itself remains intact and is not deleted for these users.

3.2.1.4 Viewing the Zoom integration status

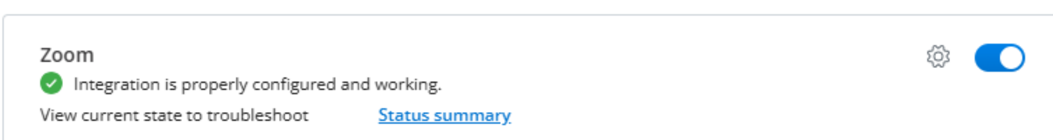
Once the Zoom integration is added to a customer account, you can check its status to ensure it is set up properly. The Zoom integration can have one of the following statuses:

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

Viewing a summary of the Zoom integration status

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

1. Access the **Integrations** panel from the **Accounts Information** page or from the **Integrations & Apps** option.
2. In the **Integrations** panel, locate the **Zoom** integration. Check the status icon and message next to it.



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

Viewing detailed information about the Zoom integration status

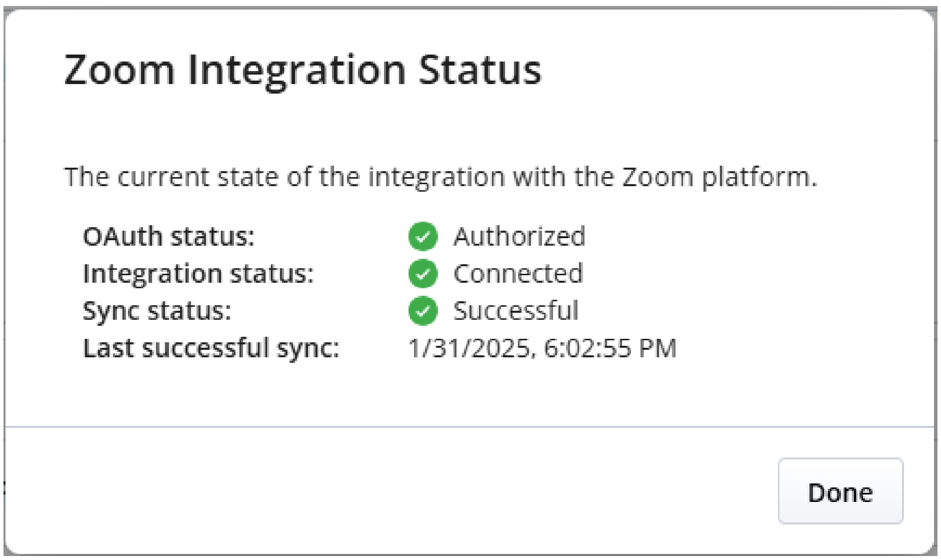
For a more in-depth view of the Zoom integration status, especially for troubleshooting, you can one of the following:

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

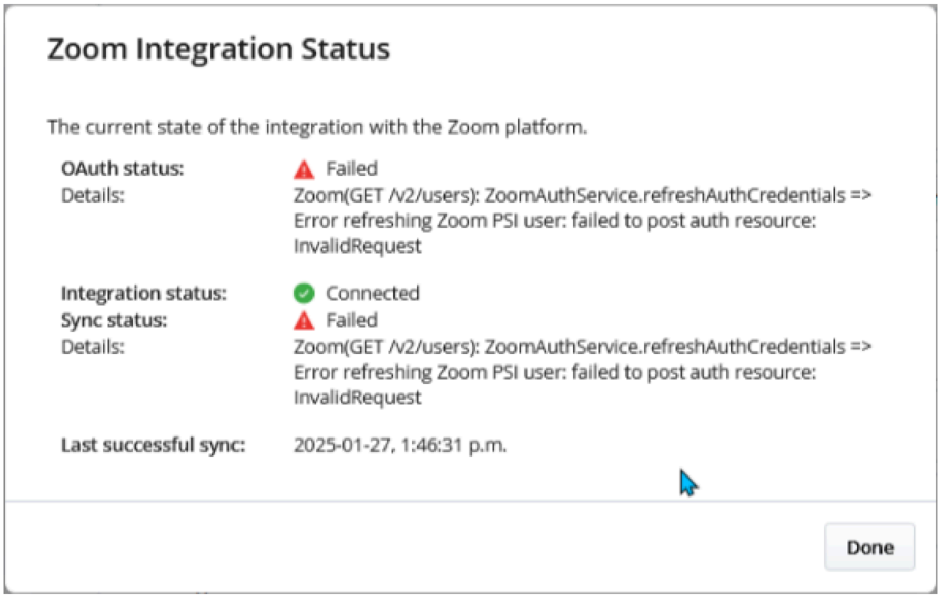
You can then view detailed information about the Zoom integration status, including the following:

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

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



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



In the second example, as shown in the details section below the failed **OAuth status** and **Sync status**, an error occurred while attempting to obtain a new refresh token from Zoom. To resolve this, a Mitel Partner or Account Admin will need to reauthorize the Zoom integration, as described in Reauthorizing the Zoom integration on page 178.

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**.

3.2.1.5 Reauthorizing the Zoom integration

Reauthorizing the Zoom integration may be necessary to maintain a seamless connection between CloudLink and Zoom, especially when the Zoom OAuth credentials have been updated.

To reauthorize the integration, 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, click next to the **Zoom** integration.
   The **Zoom Integration Configuration** page opens.
3. Click **Reconnect**.
4. If you are not signed in to Zoom, you are promoted to sign in. Enter the credentials and click **Sign in**.
5. On the Zoom Authorization window that opens, review the app permissions and click **Allow**.
6. After successful authorization, you are redirected back to Mitel Administration.

3.2.1.6 Configuring the PBX system settings

After configuring the Zoom integration you can configure the system setting of the PBX.

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

1. On the left navigation menu click on the name of the PBX e.g. **OpenScape Voice** and select **System Settings**.
2. In the **Voicemail** area add a **Pilot Number** to dial for accessing the voicemail messages.
3. In the **Feature Codes** area you can configure feature codes for the users.

   a. To add a feature code:

      - Select a **Feature** from the drop-down menu. The following features are available:

         - **Call Forward**
         - **Disable Call Forward**
         - **Do not Disturb**
         - **Disable Do not Disturb**
         - **Enable Call Forward**
         - **Enable Do not Disturb**
      - Enter the **Dialing access code**.
      - Click ⊕ **Add**.

   b. To edit a feature code:
      Select the feature code, click on the **Dialing access code** field and change the feature code.

   c. To delete a feature code:

      Select the feature code and click next to the feature code.
4. In the **Emergency Numbers** area you can configure the fallback emergency numbers.

   a. To add an emergency number:

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

   b. To edit an emergency number:
      Double click on the number and edit it.

   c. To delete an emergency number:
      Click X next to the number.

   You can add multiple emergency numbers.

5. In the **Dynamic Location provider** area configure a dynamic location provider for the emergency calls. Enter the following information:
   - **Name**
   - **Type**
   - **Primary Server**
   - **Secondary Server**
   - **Customer ID**: the unique 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.
6. Click **Save**.
   All mandatory fields must be completed before clicking save.

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

3.2.1.7 Reassigning Zoom Devices After Changing Zoom Tenant

When switching Zoom tenants in Mitel Administration, Zoom devices may remain assigned to users. This section explains how to reassign those devices correctly.

1. Remove the old Zoom integration.
   a. Navigate to **Mitel Administration** > **Integrations**.
   b. Select the existing Zoom integration.
   c. Click **Remove**.
2. Add the new Zoom integration.
   a. In **Integrations**, click **Add Integration > Zoom**.
   b. Sign in with the new Zoom tenant credentials.
   c. Confirm the integration is active.

3. Reassign Zoom devices to users.

   Case A: Users with Zoom devices in an existing profile.

   a. Navigate to **User Management**.
   b. Edit the user.
   c. Remove the Zoom devices.
   d. Click **Save**.
   e. Edit the user again.
   f. Add the Zoom devices back.
   g. Click **Save**.

   Case B: Users with only Zoom devices.

   a. Navigate to **User Management**.
   b. Edit the user.
   c. Click **Remove**.

   > **Note**:
   > This also removes **MiVoice Business** services.

   d. Recreate the user:
      - Add MiVoice Business services.
      - Choose a template that includes required phone services.
   e. Click **Save**.

Users are correctly linked to the new Zoom tenant, and old Zoom devices are removed from their profiles.

3.2.1.8 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. Click **Support > Zoom** from the left main menu.
   The **Zoom Sync & Provisioning Errors** page of the customer account opens.
2. Select the **User Comparison Report** tab.
3. 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.
4. 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.

3.2.1.9 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.

3.2.1.10 Viewing users with a Zoom PSI license

To view users with a Zoom PSI license in a customer account, follow the steps below:

1. Navigate to **User Management** > **Users** from the left main menu.
   The list of users is displayed.
2. In the user list, locate the **LICENSES** column. Use the filter options to show only users assigned the Zoom PSI license:
   a. Click **Add Filter** ⊕ Add Filter .
   b. From the drop-down list, select **Product**.
   c. From the list of properties that is displayed, select **Zoom PSI**.
      The user list is updated to show only users assigned the Zoom PSI license.
3. Click on an individual user in the list to view detailed information, including their assigned licenses.

3.2.1.11 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.

You can access the Event History table with one of the following options:

- Click **Support** > **Zoom** from the left main menu.

  The **Zoom Sync & Provisioning Errors** page of the customer account opens.

  Select the **Event History** tab.

  In this page you can view the events only for the Zoom integration.

Or

- Click **Support** > **Event History** from the left main menu.

  In this page you can view the events for all the integrations.

In the Event History tab for the Zoom integration you have the following options:

- Viewing the Event History table
- Customizing the Event History table
- Batch exporting event details
- Copying or exporting the details of a specific event
- Searching or filtering the Event History table

For more information, see Event History on page 72.

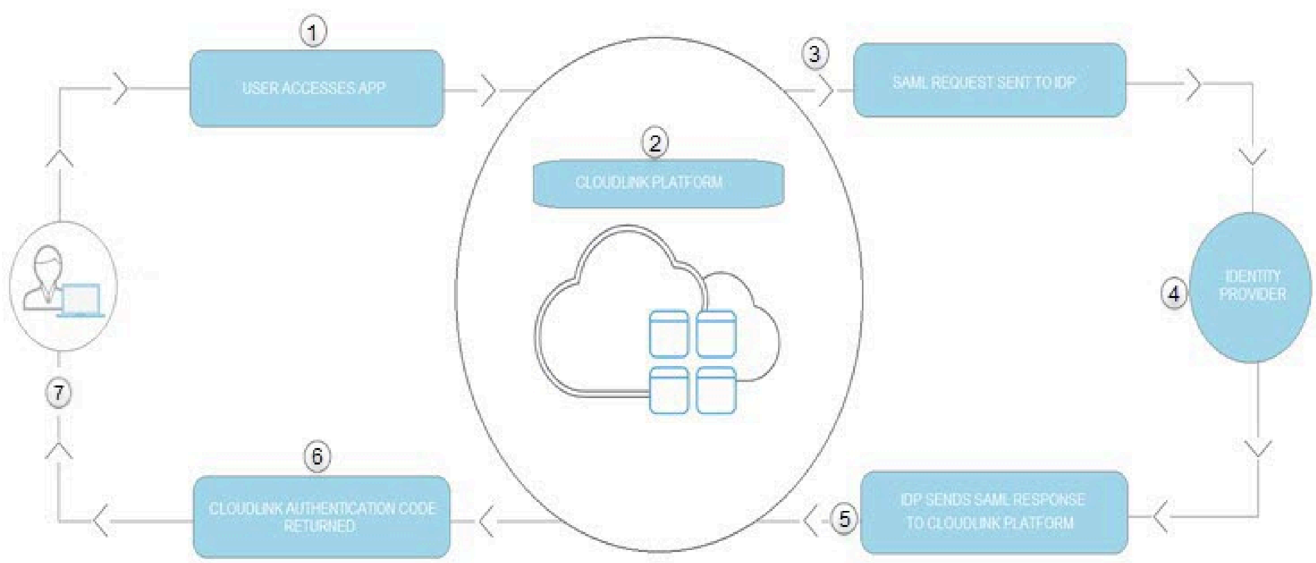
3.2.2 Integrating Single Sign-On with Mitel Administration

CloudLink supports integration with third-party Single Sign-On (SSO) enabling users to access multiple applications with a single set of login credentials. SSO reduces the need for multiple logins, promoting efficient and seamless navigation across various platforms.

CloudLink supports Identity Provider (IdP) integration using the Security Assertion Markup Language (SAML) 2.0 protocol, enabling users to utilize their current identity management systems with enhanced security and interoperability provided by SAML 2.0.

Microsoft's cloud-based, Azure Active Directory (Azure AD), provides authentication and authorization for users, devices, and applications.

Outlook 365 integrates cloud-based email, calendar, and collaboration services, ensuring seamless integration with Azure AD for secure user identity management.



1 The user accesses the CloudLink application on their mobile or web browser and the application loads. The application generates metadata and redirects the user to the CloudLink platform.

2 The CloudLink Auth Portal validates the application metadata and forwards the authentication request to the CloudLink Authentication microservice.

3 The CloudLink Authentication microservice initiates the SAML authentication request to the configured identity provider.

4 The user has an active session with the Identity Provider or a new session is created by logging into the Identity Provider. The IDP may enforce Multi-Factor Authentication depending on its configuration.

5 The CloudLink Platform validates the response using the associated X.509 certificate.

6 The authenticated user is granted access to CloudLink and redirected back to the application with an authentication code.

7 The application then exchanges the authentication code for a token and completes its initialization.

The following topics provide information on how to integrate a CloudLink account with the supported third-party applications.

3.2.2.1 Configuring SAML Single Sign-On Integration for CloudLink with Identity Providers (generic instructions)

Following are instructions for setting up SAML Single Sign-On (SSO) integration using a generic identity provider. To configure SSO for CloudLink with Microsoft Azure AD, see Configuring Single Sign-On for CloudLink with Microsoft Azure AD.

Prerequisites

To configure SAML SSO integration with CloudLink platform, you must have:

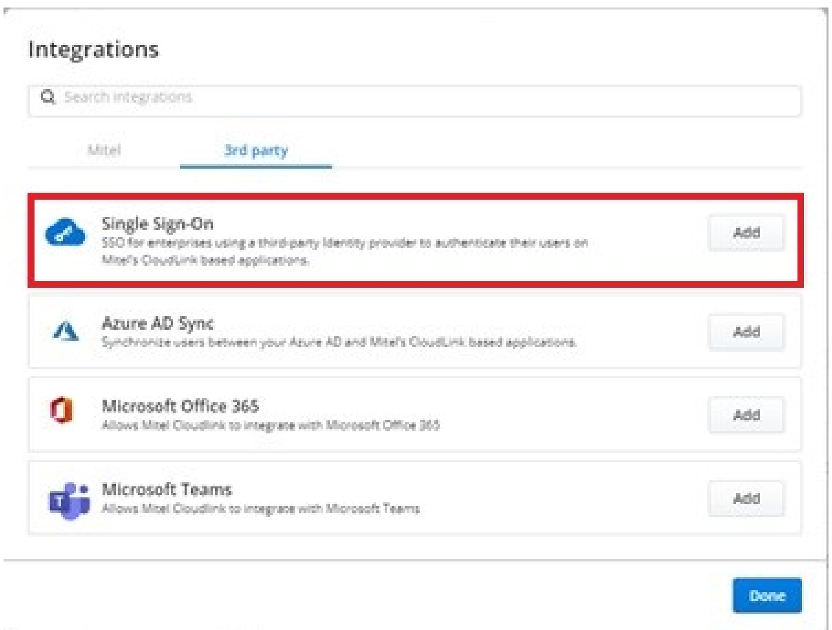
- An IdP subscription
- Mitel CloudLink account

Procedure

Note:
To configure SAML SSO integration, it is recommended that you open the IdP portal and the Mitel Administration side-by-side as you will need to copy some information from the Mitel Administration to the IdP portal and vice versa.

1. Enable the **Single Sign-On** integration in the Mitel Administration.

   a. Navigate to the **Account Information** page of the customer account for which you want to enable the integration.
   b. In the **Integrations** section, click **+ Add new**. A pop-up screen displays the **Integrations** panel.
   c. Click the **3rd party** tab. A list of supported third-party applications is displayed. Click the **Add** button associated with **Single Sign-On**, and click **Done**.

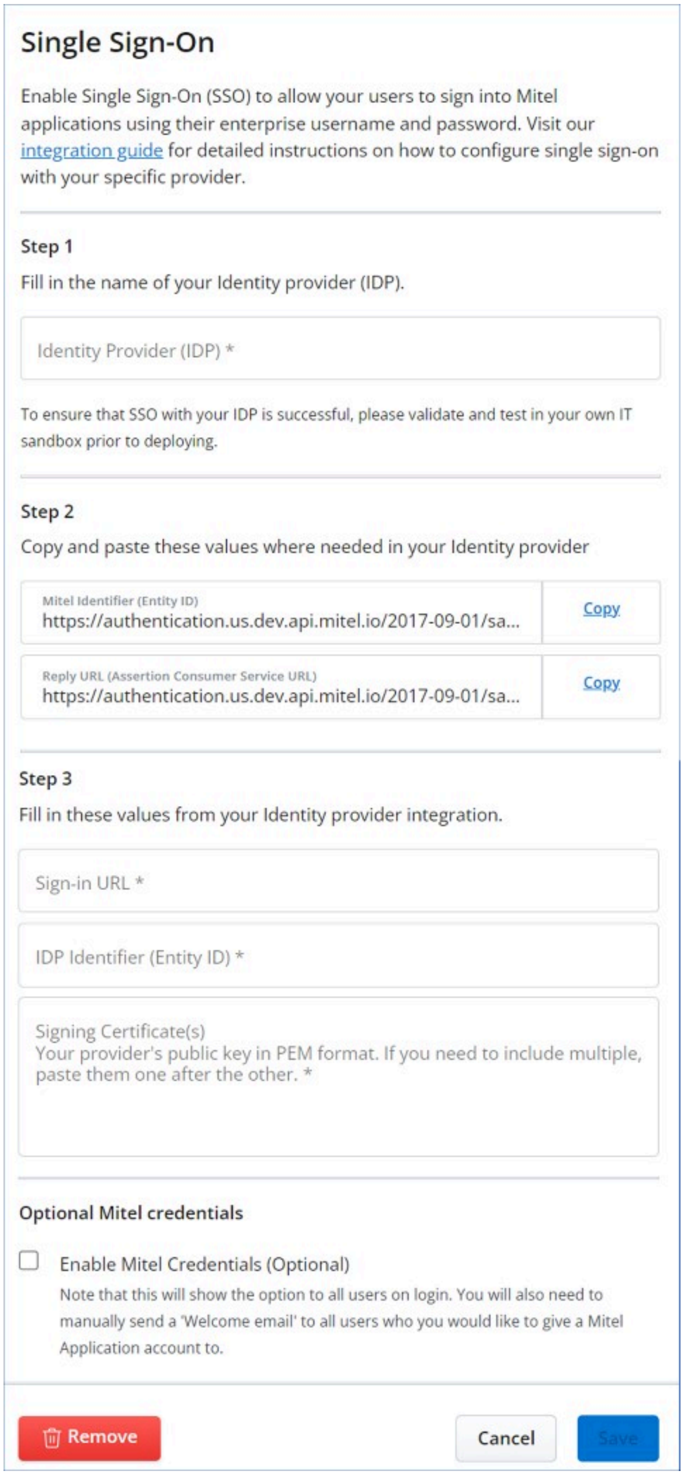


The **Single Sign-On** is enabled for the customer account and is added to the **Integrations** section of the **Account Information** page.

2. Accessing the **Single Sign-On** configuration dialog box.

   In the **Account Information** page, click **Complete setup**.

   The **Single Sign-On** configuration dialog box opens.


Single Sign-On
Enable Single Sign-On (SSO) to allow your users to sign into Mitel applications using their enterprise username and password. Visit our integration guide for detailed instructions on how to configure single sign-on with your specific provider.
Step 1
Fill in the name of your Identity provider (IDP).
Identity Provider (IDP) *
To ensure that SSO with your IDP is successful, please validate and test in your own IT sandbox prior to deploying.
Step 2
Copy and paste these values where needed in your Identity provider
Mitel Identifier (Entity ID)
https://authentication.us.dev.api.mitel.io/2017-09-01/sa...
Copy
Reply URL (Assertion Consumer Service URL)
https://authentication.us.dev.api.mitel.io/2017-09-01/sa...
Copy
Step 3
Fill in these values from your Identity provider integration.
Sign-in URL *
IDP Identifier (Entity ID) *
Signing Certificate(s)
Your provider's public key in PEM format. If you need to include multiple, paste them one after the other. *
Optional Mitel credentials
Enable Mitel Credentials (Optional)
Note that this will show the option to all users on login. You will also need to manually send a 'Welcome email' to all users who you would like to give a Mitel Application account to.
Remove
Cancel
Save

Note:

- All users even SSO only users are required to complete the welcome email process.
- Mitel recommends that the **Enable Mitel Credentials (Optional)** check box in the **Optional Mitel credentials** section is not selected. Select this check box **only** if you want the user to log in to the CloudLink application using the Mitel credentials in addition to the single sign-on option.
- If a CloudLink User is set as Admin in the CloudLink Portal they will always be offered the option to sign in using the Mitel credentials in addition to the single sign-on option.

3. Add the CloudLink Platform information into the IdP.

   While configuring the SAML application in the IdP portal, enter the following information about the CloudLink Platform into the IdP portal.

   - Service Provider Entity ID field: Copy the ID from the **Mitel Identifier (Entity ID)** field in the Mitel Administration and paste it into the entity ID field of the IdP portal.
   - Service Provider Login URL: Copy the URL from the **Reply URL (Assertion Consumer Service URL)** field in the Mitel Administration and paste it into the Login URL field of the IdP portal.
4. Add the IdP portal information into Mitel Administration.

   Once you have entered the above mentioned information into the IdP portal, the IdP portal should provide you with the same two pieces of information as above, except on the IdP side of the connection.

   - IdP Entity ID - Copy the ID from the entity ID field of the IdP portal and paste it into the **IDP Identifier (Entity ID)** field in the Mitel Administration.
   - IdP Login URL - Copy the URL from the Login URL field of the IdP portal and paste it into the **Sign-in URL** field in the Mitel Administration.
5. Upload the IdP certificate to Mitel Administration.

   To do this, from the IdP portal, download the public certificate X.509 certificate in PEM format provided by IdP and save it on your computer. After saving the certificate, open the certificate file in a text editor, copy all data in the file, and then paste the data into the **Signing Certificate** field in the Mitel Administration.

   Note:
   If you have more than one certificate, it is recommended that you paste them one after the other.
6. Once you have entered the three IdP fields and have uploaded the IdP certificate into Mitel Administration, click **Save** to save the SSO settings.

Renewing the SAML Signing Certificate

Renewing the SAML Signing Certificate updates the digital certificate used for secure communication in Single Sign-On (SSO) setups, ensuring continued security and validity.

Click here to learn more about how to renew the SAML signing certificate.

3.2.2.2 Configuring Single Sign-On for CloudLink with Microsoft Azure AD

Configuring your CloudLink platform with Microsoft Azure Active Directory (Azure AD) allows users on your account to access CloudLink applications using their enterprise credentials.

Note:
To configure CloudLink with other Identity Providers, see Configuring SAML Single Sign-On (SSO) for CloudLink with Identity Providers (generic instructions).

Prerequisites

To configure Azure AD integration with CloudLink platform, you must have:

- An Azure AD subscription

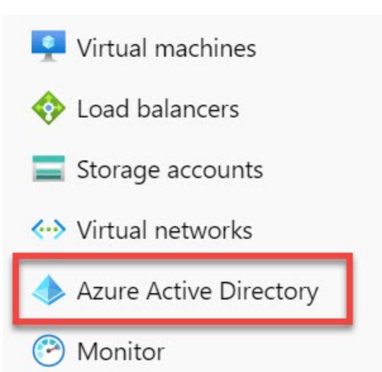
  If you do not have an Azure AD environment, you can get a free account.
- A Mitel CloudLink account

Adding Mitel Connect from the Gallery

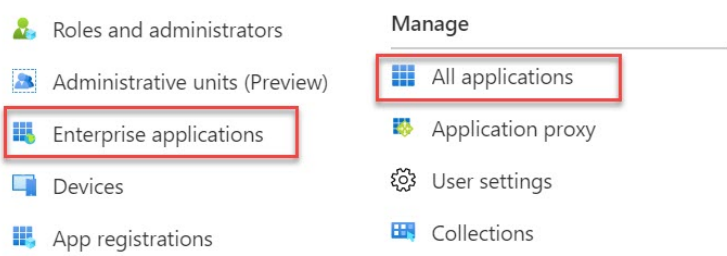
To configure Azure AD integration with CloudLink platform, you must add the **Mitel Connect** application from the gallery to your list of managed SaaS apps in the Azure portal.

To add Mitel Connect from the gallery:

1. In the Azure portal, on the left navigation panel, click **Azure Active Directory**. The **Azure Active Directory** panel opens.

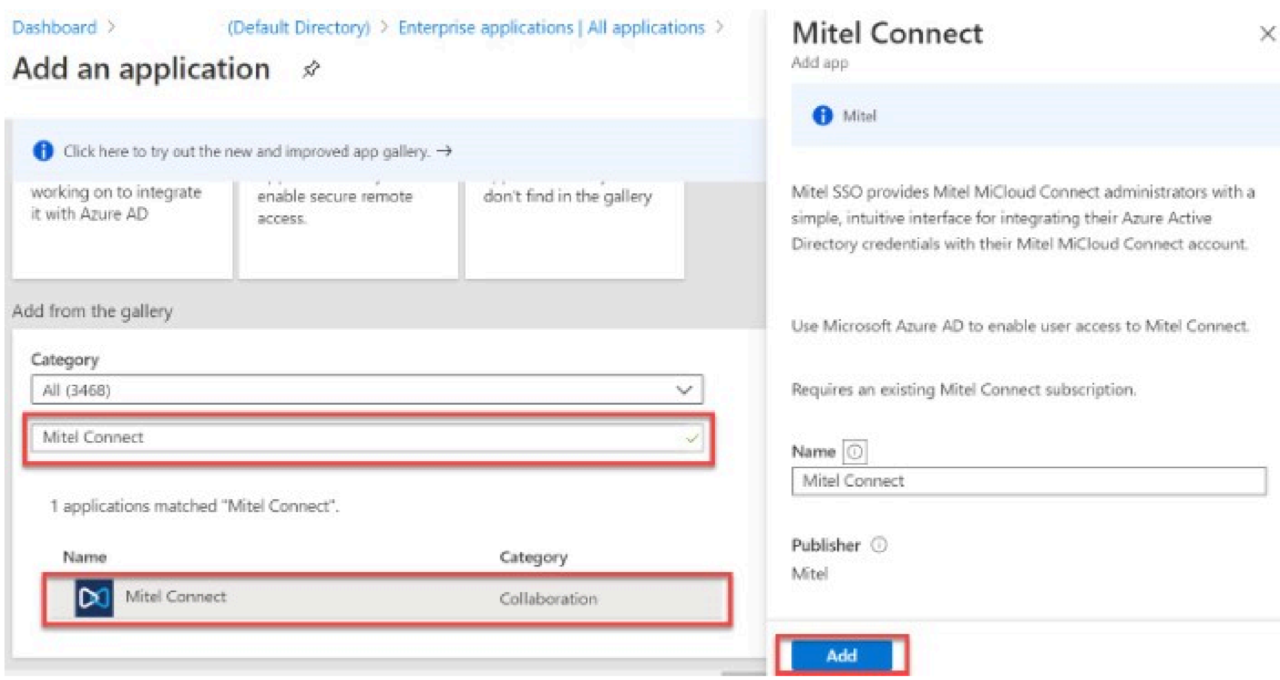


2. In the **Azure Active Directory** panel, select **Enterprise applications**. The **All applications** page opens and displays a list of applications in your Azure AD tenant.



3. Click **New application**. The **Add an application** page opens.

4. In the **Add from the gallery** section, type **Mitel Connect** in the **Enter a name** field. Click the **Mitel Connect** application from the results panel, and then click **Add** from the application information panel that opens.



Configure and Test Azure AD Single Sign-On

This section describes how to configure and test Azure AD single sign-on with CloudLink platform based on a test user named **John Smith**. For single sign-on to work, a link must be established between the user in the Azure AD portal and the corresponding user in the CloudLink platform.

To configure and test Azure AD single sign-on with CloudLink platform, complete the following steps:

1. Configure CloudLink platform for Single Sign-On with Azure AD on page 193 —to enable your users to use this feature and to configure the SSO settings on the application side.
2. Create an Azure AD Test User on page 201 —to test Azure AD single sign-on with **John Smith**.

3. Assign the Azure AD Test User on page 203 —to enable **John Smith** to use Azure AD single sign-on.
4. Create a CloudLink Test User on page 205 —to create a user for **John Smith** in the Mitel Administration that is linked to the corresponding user in the Azure AD portal.
5. Test Single Sign-On on page 206 —to verify that the configuration works.

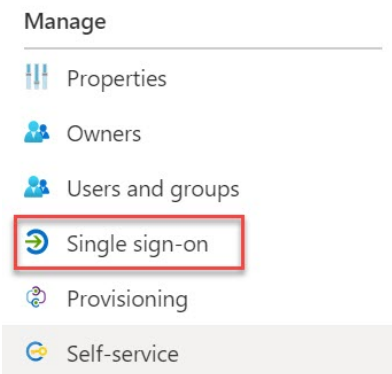
Configure CloudLink platform for Single Sign-On with Azure AD

This section describes how to enable Azure AD single sign-on for CloudLink platform in the Azure portal and how to configure your CloudLink platform account to allow SSO using Azure AD.

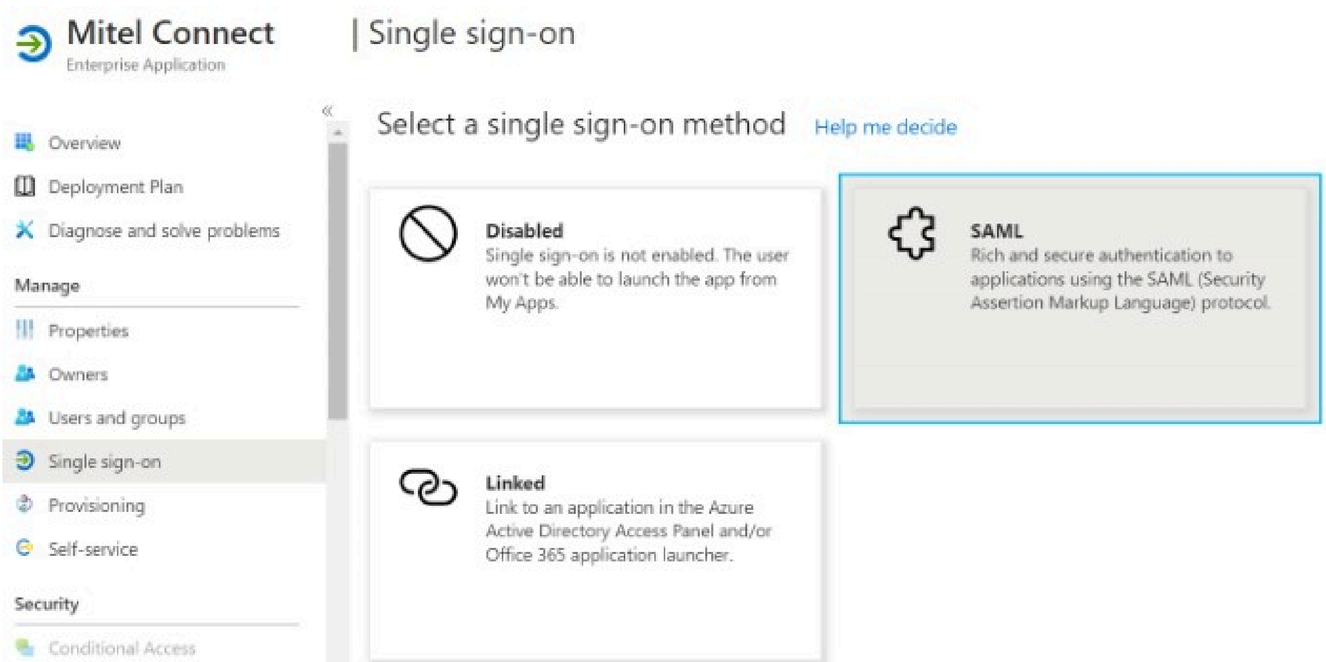
To configure CloudLink platform with SSO for Azure AD, it is recommended that you open the Azure portal and the Mitel Administration side-by-side as you will need to copy some information from the Azure portal to the Mitel Administration and vice versa.

1. 1. To access the **Basic SAML Configuration** page in the Azure portal, do the following:

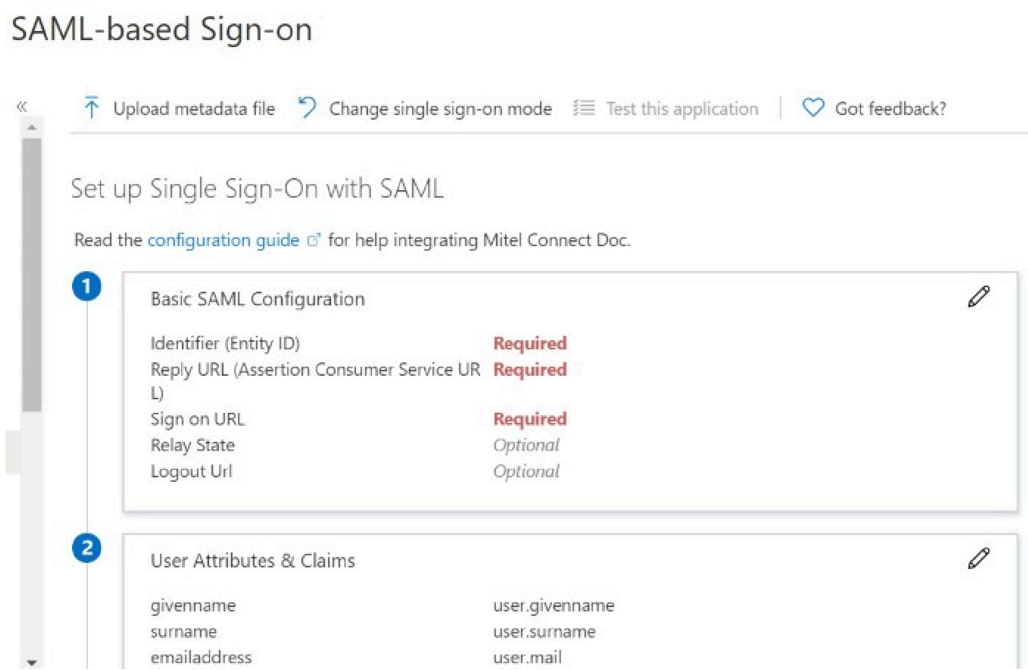
   a. Navigate to **Azure Active Directory** > **Enterprise applications**, and select **Mitel Connect** from the list. The **Mitel Connect Overview** page opens.
   b. Under the **Manage** section, select **Single sign-on**.



   c. In the **Select a Single sign-on method** page that opens, click **SAML**.

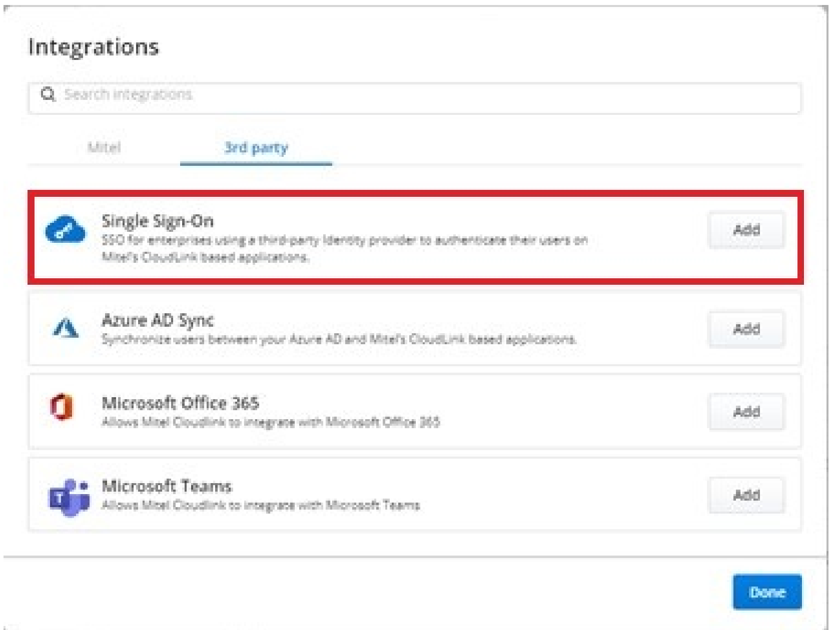


The **SAML-based Sign-on** page opens, displaying the **Basic SAML Configuration** section.


SAML-based Sign-on
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Set up Single Sign-On with SAML
Read the configuration guide for help integrating Mitel Connect Doc.
1
Basic SAML Configuration
Identifier (Entity ID)
Required
Reply URL (Assertion Consumer Service URL)
Required
Sign on URL
Required
Relay State
Optional
Logout Url
Optional
2
User Attributes & Claims
givenname
user.givenname
surname
user.surname
emailaddress
user.mail

2. To access the **Single Sign-On** configuration dialog box in the Mitel Administration, you must do the following:

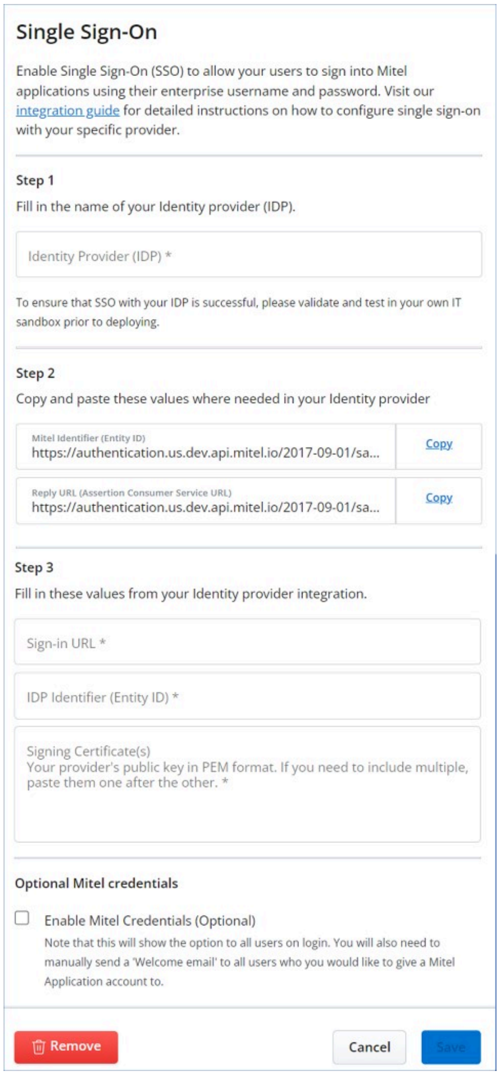
   a. Navigate to the **Account Information** page of the customer account with which you want to enable the integration.
   b. In the Integrations section, click **+ Add new**. A pop-up screen displays the **Integrations** panel.
   c. Click the **3rd party** tab. A list of supported third-party applications is displayed. Click the **Add** button associated with **Single Sign-On**, and click **Done**.



   The **Single Sign-On** is enabled for the customer account and is added to the **Integrations** section of the **Account Information** page.

   d. Click **Complete setup**.

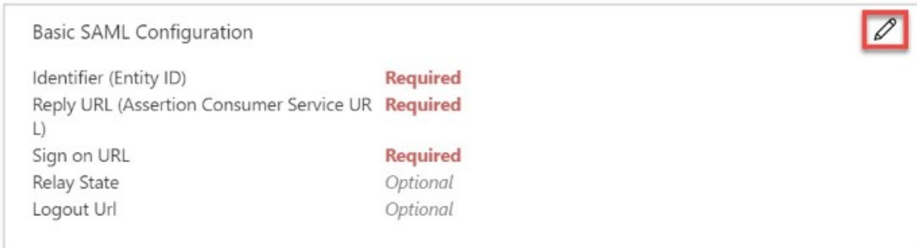
   The **Single Sign-On** configuration dialog box opens.



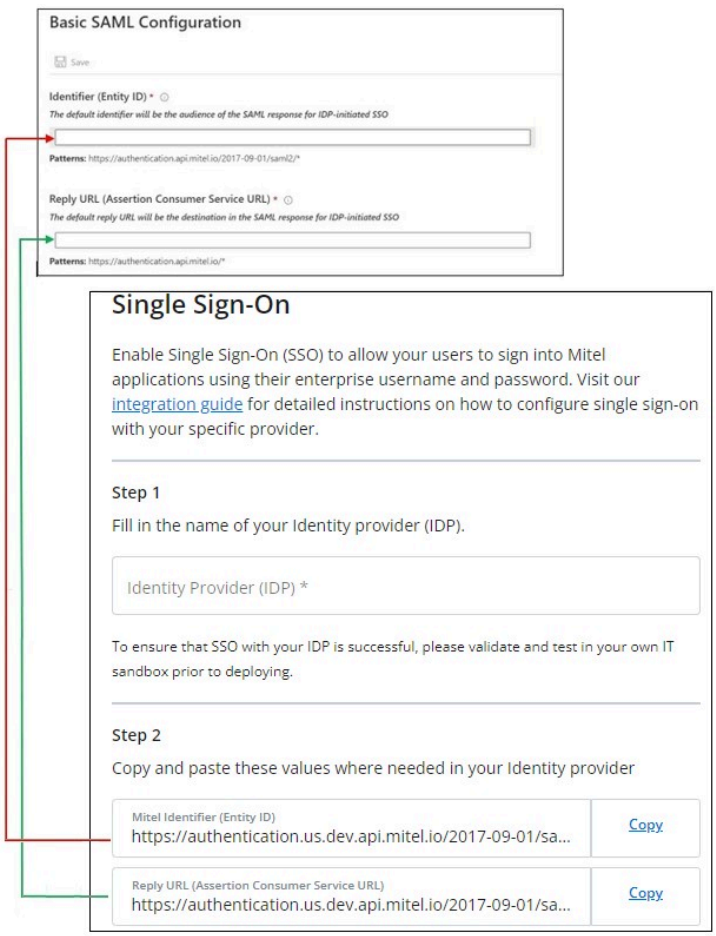
Note:

- All users even SSO only users are required to complete the welcome email process.
- Mitel recommends that the **Enable Mitel Credentials (Optional)** check box in the **Optional Mitel credentials** section is not selected. Select this check box **only** if you want the user to log in to the CloudLink application using the Mitel credentials in addition to the single sign-on option.
- If a CloudLink User is set as Admin in the CloudLink Portal they will always be offered the option to sign in using the Mitel credentials in addition to the single sign-on option.

3. In the Azure portal, from the **SAML-based Sign-on** page, click the Edit icon () in the **Basic SAML Configuration** section. The **Basic SAML Configuration** panel opens.



4. Copy the URL from the **Mitel Identifier (Entity ID)** field in the Mitel Administration and paste it into the **Identifier (Entity ID)** field in the Azure portal.
5. Copy the URL from the **Reply URL (Assertion Consumer Service URL)** field in the Mitel Administration and paste it into the **Reply URL (Assertion Consumer Service URL)** field in the Azure portal.



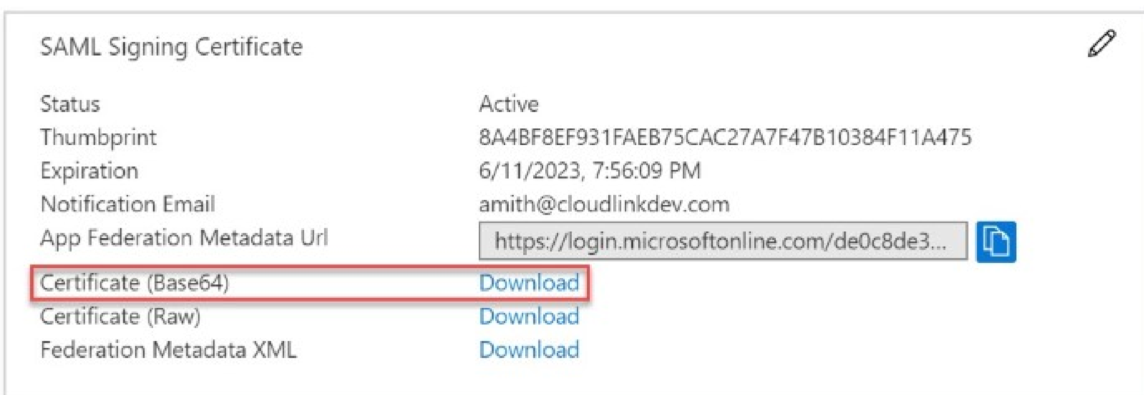
6. In the **Sign on URL** text box, type the following URL:

   https://accounts.mitel.io - to use the Mitel Administration as your default Mitel application.

> **Note**:
> The default Mitel application is the application accessed when a user clicks the Mitel Connect tile in the Access Panel. This is also the application accessed when performing a test setup from Azure AD.

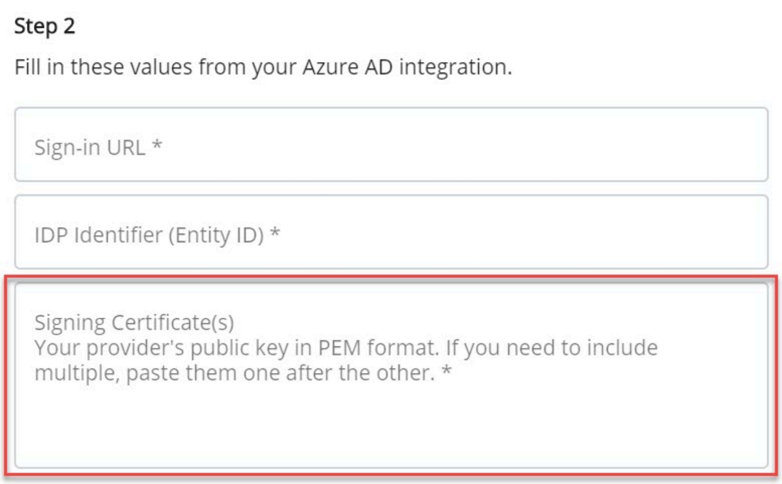
7. Click 

 in the **Basic SAML Configuration** panel.
8. In the **SAML Signing Certificate** section on the **SAML-based sign-on** page in the Azure portal, click **Download** beside **Certificate (Base64)** to download the **Signing Certificate**. Save the certificate on your computer.



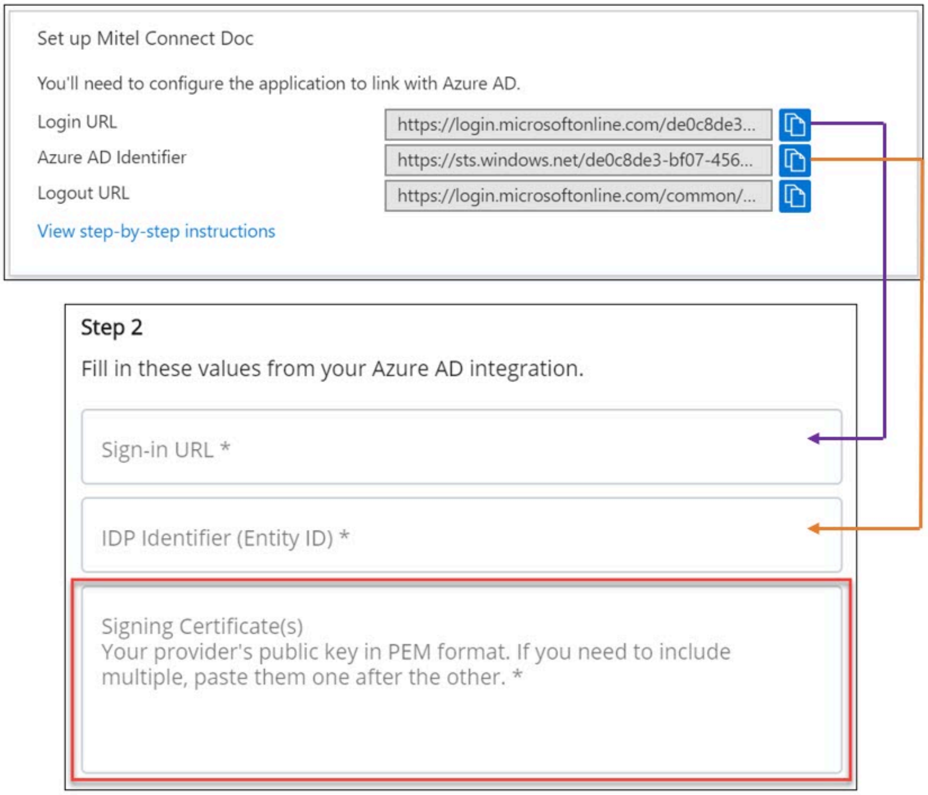
9. Open the Signing Certificate file in a text editor, copy all data in the file, and then paste the data into the **Signing Certificate** field in the Mitel Administration.

Note:
If you have more than one certificate, it is recommended that you paste them one after the other.



10. In the **Set up Mitel Connect** section on the **SAML-based sign-on** page of the Azure portal, do the following:

    a. Copy the URL from the **Login URL** field and paste it into the **Sign-in URL** field in the Mitel Administration.
    b. Copy the URL from the **Azure AD Identifier** field and paste it into the **IDP Identifier (Entity ID)** field in the Mitel Administration.

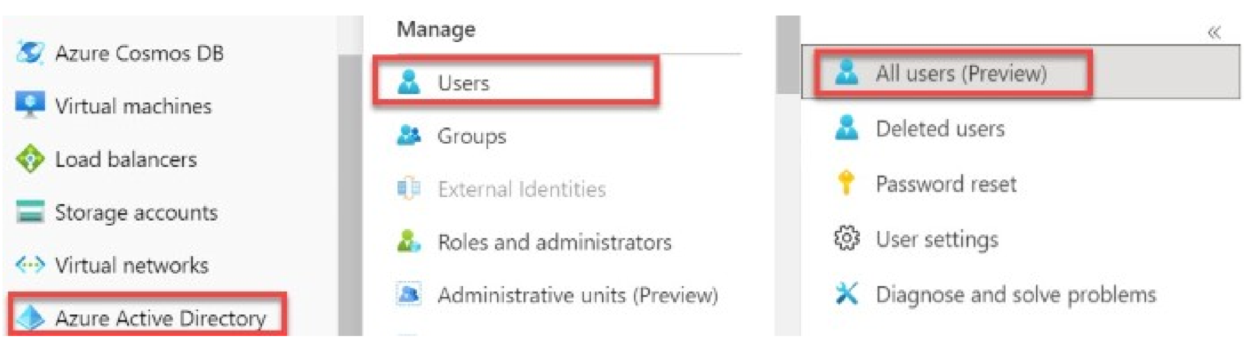


11. Click **Save** on the **Single Sign-On** panel in the Mitel Administration.

Create an Azure AD Test User

This section describes how to create a test user named **John Smith** in the Azure portal.

1. In the Azure portal, from the left pane, navigate to **Azure Active Directory** > **Users** > **All users**.



2. Click **New user** at the top of the screen.

3. In the **New user** details page that opens, enter the following details:

   a. In the **User name** field, type **JohnSmith@<yourcompanydomain>.<extension>**.

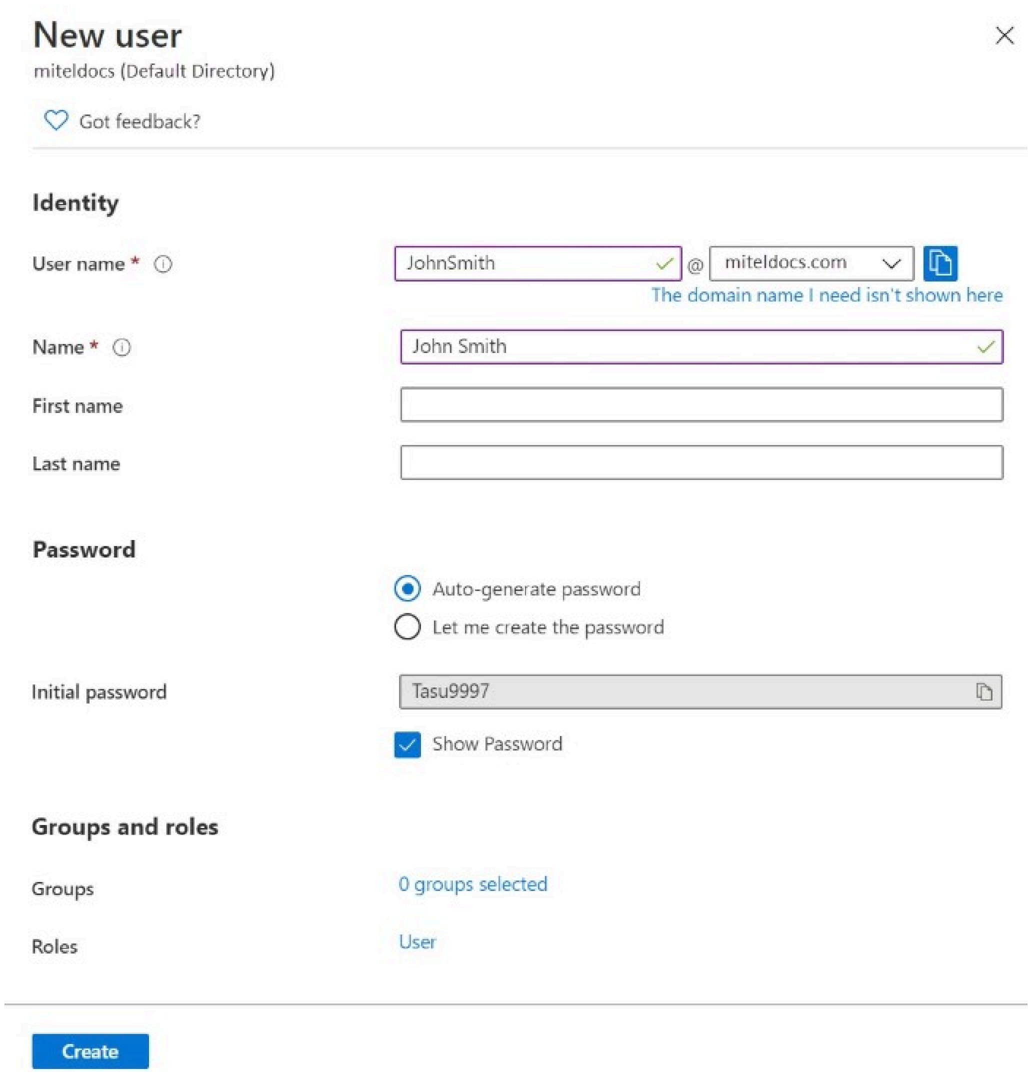
      For example: JohnSmith@miteldocs.com

   b. In the **Name** field, type **John Smith**.

   c. Select the **Show Password** check box, and then write down the auto-generated password that is displayed in the **Initial password** box. You can also choose to create your own password by selecting the **Let me create the password** check box.

> **Note**:
> This is the password a user must provide to log in to the Azure portal for the first time.

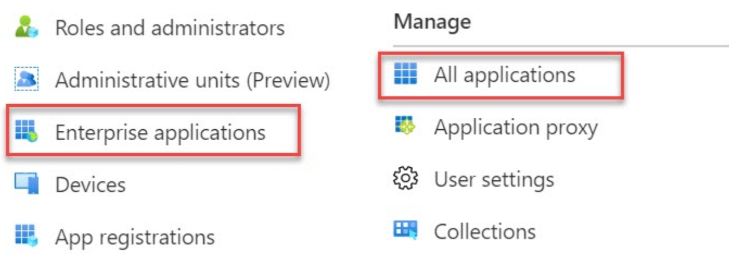
d. Click **Create**.



Assign the Azure AD Test User

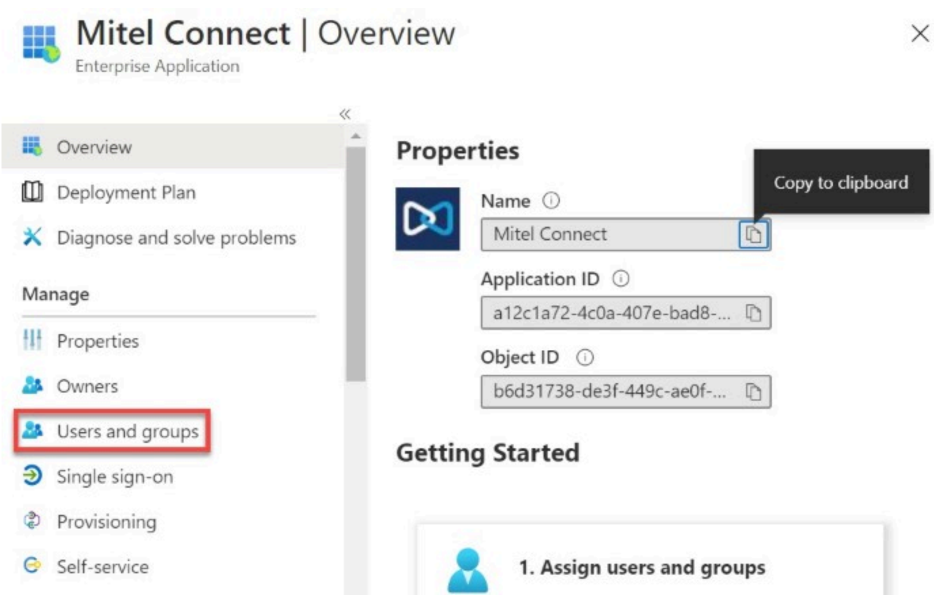
This section describes how to enable **John Smith** to use Azure single sign-on by granting access to Mitel Connect.

1. In the **Azure Active Directory** panel, select **Enterprise applications**. The **All applications** page opens, displaying a list of applications in your Azure AD tenant.



2. In the applications list, click **Mitel Connect**. The **Mitel Connect Overview** page appears.

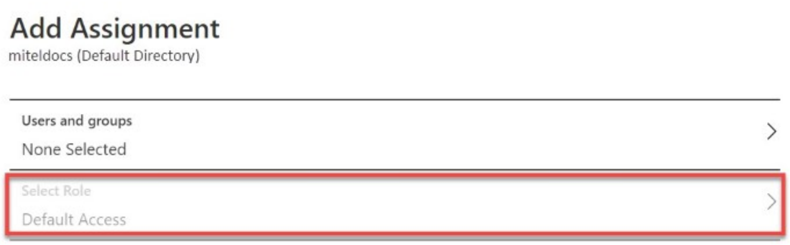
3. In the menu that appears, click **Users and groups**. The **Users and groups** page opens.



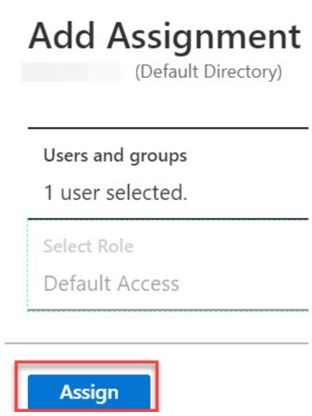
4. Click **Add user** and then click **Users and groups** in the **Add Assignment** page that opens.

5. In the **Users and groups** page that opens, select **John Smith** in the **Users** list and then click **Select** at the bottom of the screen.

6. By default, the role of a new user is **Default Access**. If you are expecting any role value in the SAML assertion, select the appropriate role for the user from the list in the **Select Role** page, and then click **Select** at the bottom of the screen.



7. In the **Add Assignment** page, click **Assign**.



Create a CloudLink Test User

This section describes how to create a test user named **John Smith** on your CloudLink platform. Users must be created and activated before they can use single sign-on.

For details about adding users in the Mitel Administration, see the **Managing Users** topic in Mitel Administration documentation.

Create a user on your Mitel Administration with the following details:

- Name: John Smith
- First Name: John
- Last Name: Smith
- Email: JohnSmith@miteldocs.com

Note:
The user's CloudLink email address must be identical to the **User Principal Name** in Azure AD portal.

Test Single Sign-On

In this section, you will test your Azure AD single sign-on configuration using the Access Panel.

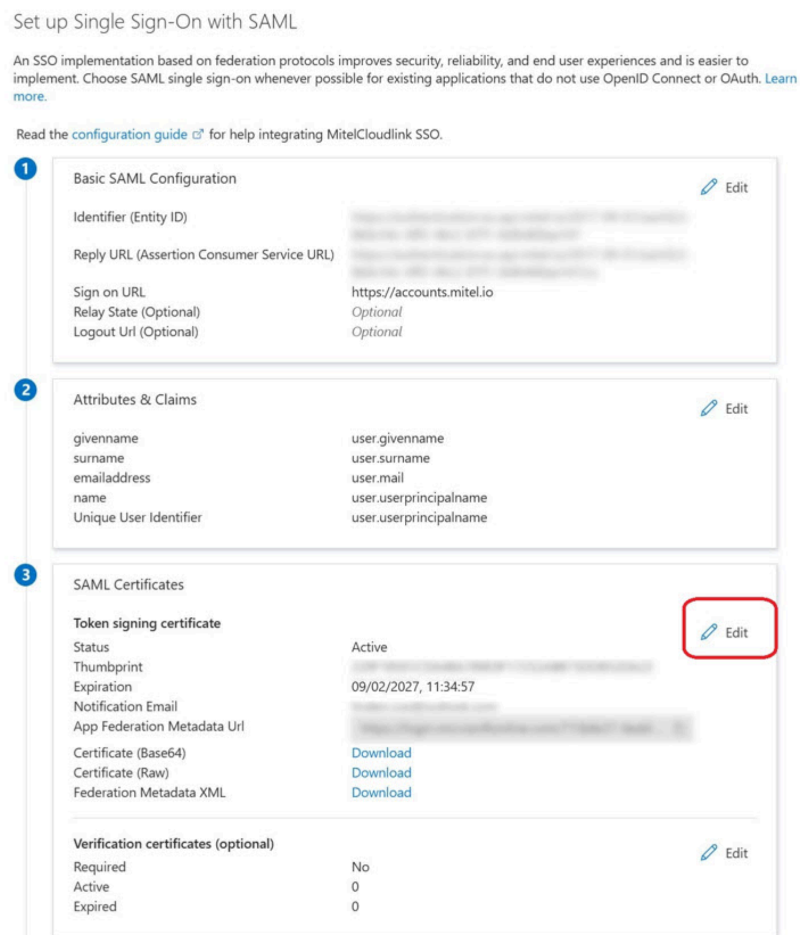
When you click the Mitel Connect tile in the Access Panel, you should be automatically redirected to sign in to the CloudLink application you configured as your default in the **Sign on URL** field. For more information about the Access Panel, see Introduction to the Access Panel.

Renewing a SAML Signing Certificate in Azure:

Renewing the SAML Signing Certificate updates the digital certificate used for secure communication inSingle Sign-On (SSO) setups, ensuring continued security and validity.

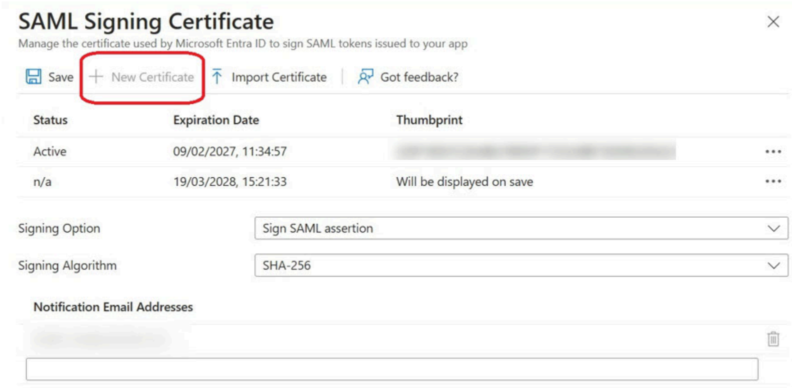
Note:
If Azure/Entra is configured, it will send an email warning when the certificate is about to expire, prompting you to update it.

1. **Navigate to the Existing Single Sign-On Setup:**
   - In Azure, under **Enterprise applications** > **SSO application**, click **Set up single sign on** > **Get started**.



2. **Edit SAML Certificates**:
   - In the **SAML Certificates** window, click **Edit**.

3. **Renew Certificate:**

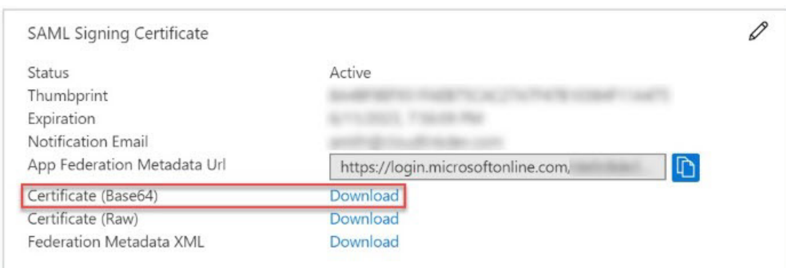


- In the **SAML Signing Certificate** window, click **New Certificate**.
- Click **Save**.

This ensures that a new certificate is generated and saved, which is crucial for maintaining secure communication in your SSO setup.

4. **Download the Signing Certificate:**

- In the **SAML Signing Certificate** section on the SAML-based sign-on page in the Azure portal, click **Download** beside **Certificate (Base64)** to download the Signing Certificate.



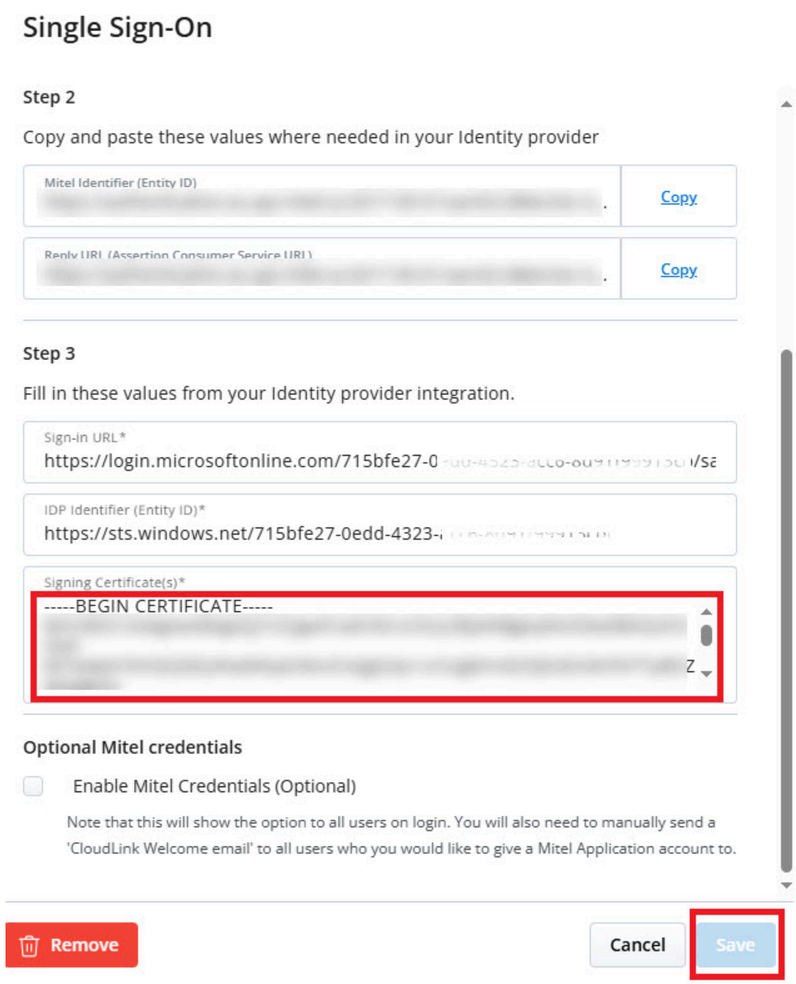
- Save the certificate on your computer.

5. **Update the Signing Certificate to Mitel Administration:**

   a. Navigate to Mitel Administration and Click the settings (Cog) against the Single Sign-On integration.

   b. Open the Signing Certificate file in a text editor.

   c. Copy all data in the file.



   d. Delete the existing contents in the Signing Certificate(s) field.

   e. Paste the new data into the Signing Certificate(s) field.

> **Note**:
> If you have more than one certificate, paste them one after the other.

f. Click **Save**.

The certificate is now renewed.

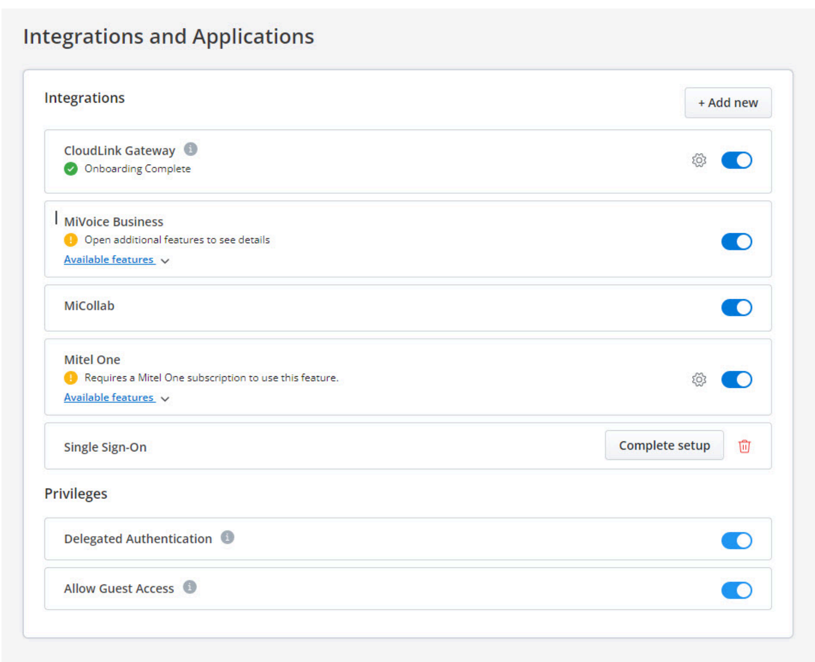
3.2.3 Integrating Microsoft Office 365 with Mitel Administration

If Microsoft Office 365 integration is enabled for a customer account, users in that account can integrate their Microsoft Office 365 account with their CloudLink applications.

Adding Microsoft Office 365 integration to a customer account

To add Microsoft Office 365 integration to a customer account:

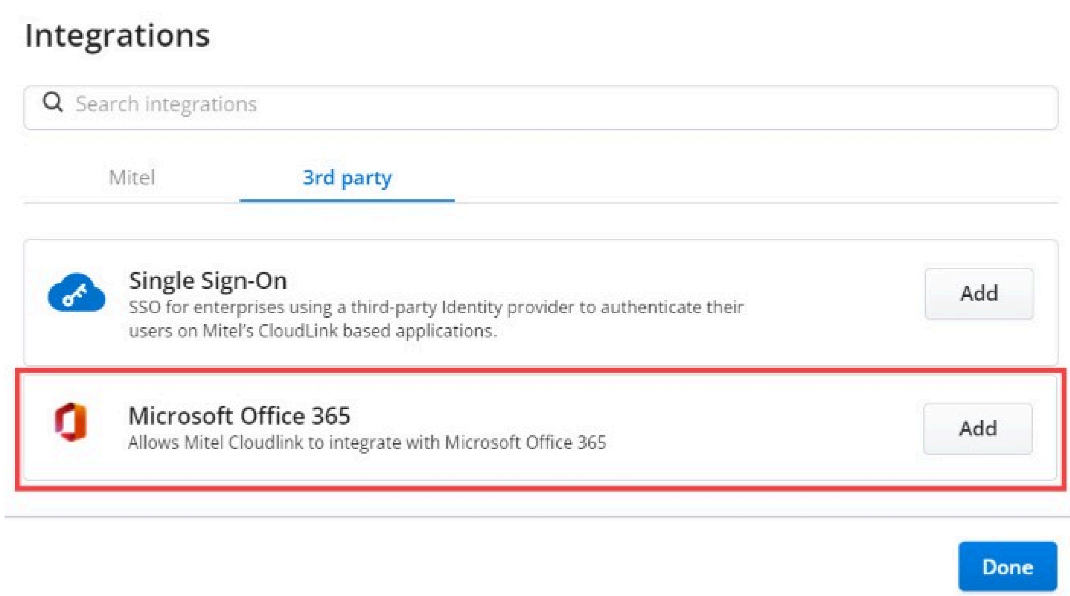
1. Navigate to the **Account Information** page of the customer account.
2. In the **Integrations** section, click **+ Add new**.



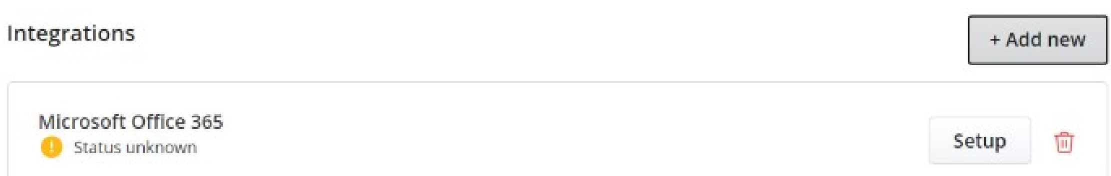
A pop-up screen displays the **Integrations** panel.

Note:
A Mitel Partner cannot enable integrations in the Partner Account because 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. Mitel recommends that you disable any existing integrations in the Partner Account to avail the full functionality of CloudLink features. For more information about Partner Accounts, see Log in as a Mitel Partner.

3. Click the **3rd party** tab. A list of supported third-party applications is displayed. Click the **Add** button associated with **Microsoft Office 365**, and click **Done**.



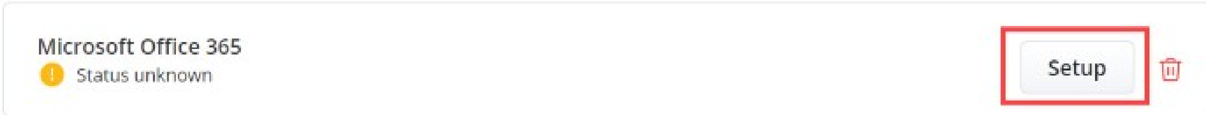
4. The Microsoft Office 365 integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.



Enabling Microsoft Office 365 integration in a customer account

After you add the Microsoft Office 365 integration to a customer account, you must provide consent for your CloudLink account to synchronize with your organization's Microsoft Office 365 account to enable the integration. The consent can be provided through Azure by a user who is an Office 365 administrator of your organization's Microsoft Office 365 account. To do this:

1. Click the **Setup** button associated with **Microsoft Office 365** in the **Integrations** section.

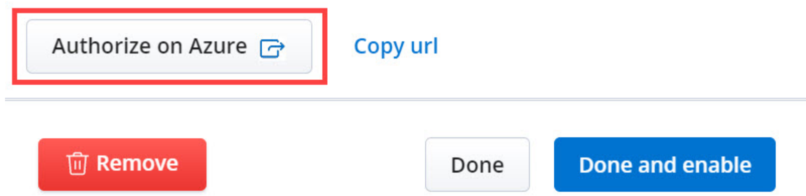


The Microsoft Office 365 configuration dialog box opens.

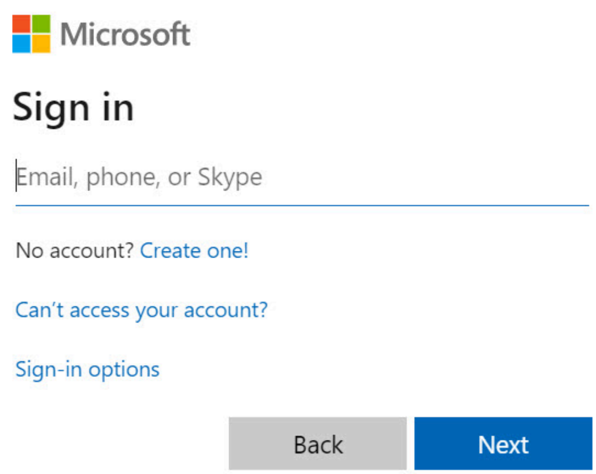
2. Further procedure depends on what admin rights the CloudLink administrator and the Office 365 administrator have.

   - **If the CloudLink administrator also has Office 365 admin rights:**

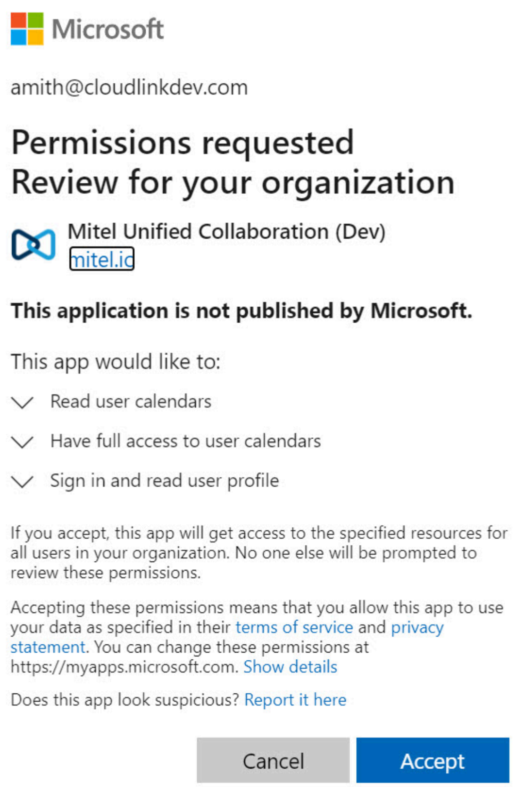
     a. Click **Authorize on Azure**.



The Microsoft **Sign in** page opens.

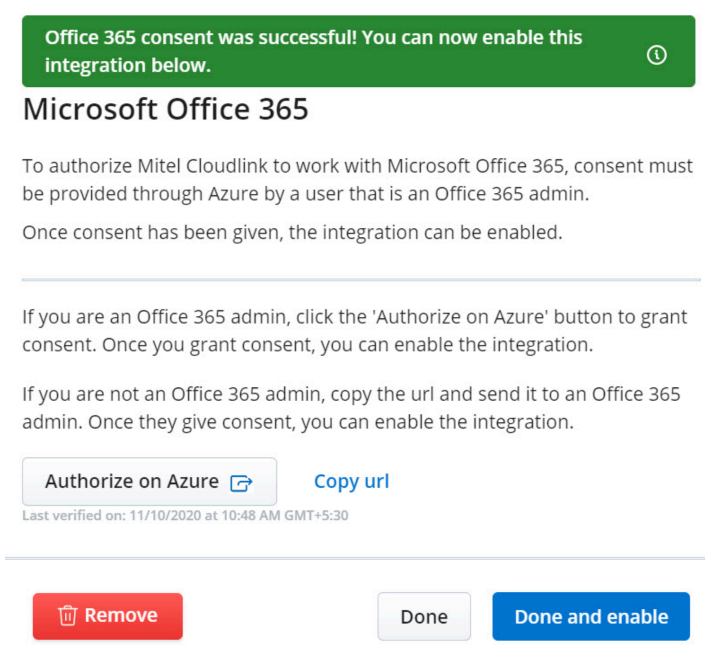


     b. Enter your credentials in the fields provided, and click **Sign in**.
     c. After successful sign in, a pop-up displays what information the Mitel Administration can access.

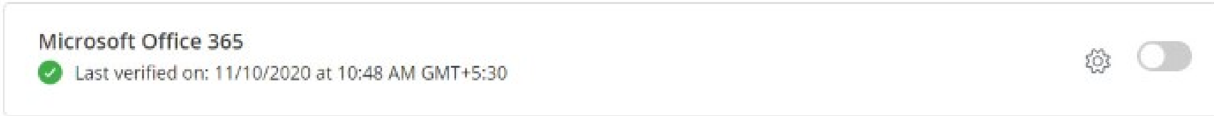


d. Click **Accept** to grant permission. The pop-up page will redirect to the Mitel Administration and then close automatically.

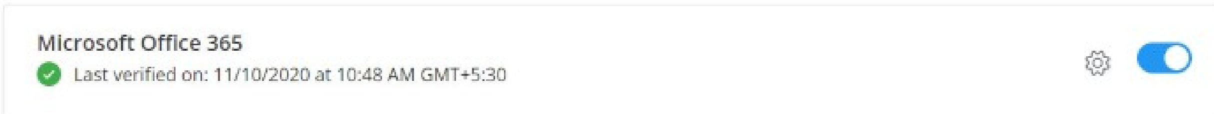
e. Return to the Microsoft Office 365 configuration dialog box. The message **Office 365 consent was successful! You can now enable this integration below.** appears.



f. Click **Done and enable** to enable the integration and close the dialog box. Clicking **Done** will close the dialog box, but will not enable the integration.



You must then enable the toggle button in the **Integrations** panel associated with **Microsoft Office 365** to enable the integration. The integration panel indicates successful integration as shown in the following screenshot.



Note:

a. If you force-close the pop-up page in the preceding step iv, the Mitel Administration will not recognize that the consent was successful.
b. If you close the Mitel Administration or the Microsoft Office365 integration dialog box before the pop-up page in the preceding step iv closes automatically, there will be no acknowledgment in the Mitel Administration that the consent was successful.

- **If the CloudLink administrator does not have Office 365 admin rights:**

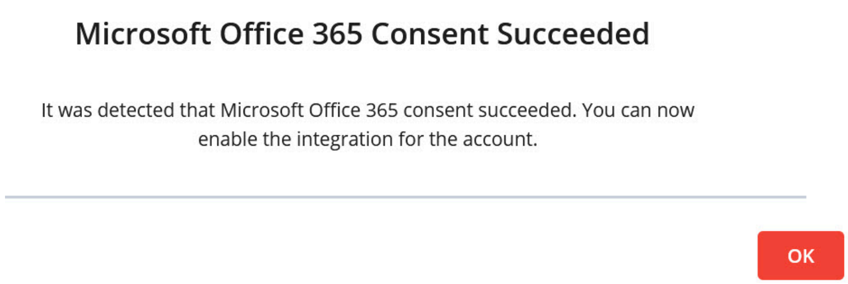
  a. Click **Copy url** to copy the URL from the Microsoft Office 365 configuration dialog box and share the URL with your organization’s Office 365 administrator.

> **Note**:
> If you click the **Authorize on Azure** button from the Microsoft Office 365 configuration dialog box, the Microsoft **Sign in** page is displayed. After you sign in, a pop-up page displays an alert that only an Office 365 administrator can grant permission. Click **Return to the Application without granting consent** to return to the Mitel Administration. The Microsoft Office 365 dialog box displays the message **Office 365 consent failed because you do not have the access. Copy the following URL and send to an Office 365 administrator.**

b. Further procedure depends on what admin rights the Office 365 administrator have.

- **If the Office 365 administrator also has CloudLink admin rights:**

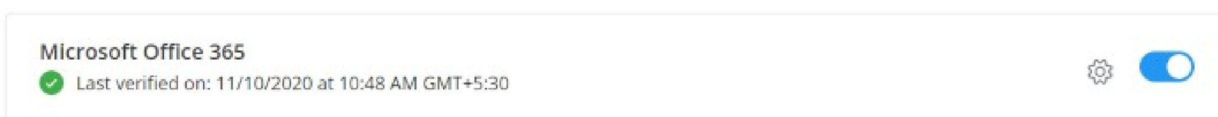
  After the Office 365 administrator grants permission by accepting the permission request, the pop-up page will redirect to the Mitel Administration login page. The Office 365 administrator must then log in to the console using CloudLink administrator credentials. After successful login, the Mitel Administration detects that the consent was successful and displays the following dialog box.



The Office 365 administrator informs the CloudLink administrator that consent has been granted.

If the Office 365 administrator denies permission, the pop-up page will redirect to the Mitel Administration login page. After logging in, the Mitel Administration displays the following dialog box.

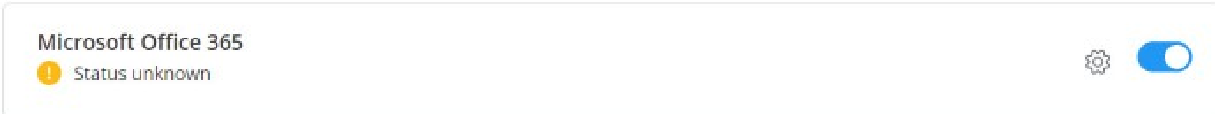
After the Office 365 administrator grants consent, click **Done and enable** in the Microsoft Office 365 configuration dialog box. If the Mitel Administration has detected that the consent was successful, the integration status will be as displayed as shown in the following image.



- **If the Office 365 administrator does not have CloudLink admin rights:**

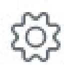
  After the Office 365 administrator grants permission by accepting the permission request, the pop-up page will redirect to the Mitel Administration login page. Because the Office 365 administrator cannot log in to the Mitel Administration, the console does not detect whether the consent is successful or not. However, the Office 365 administrator can inform the CloudLink administrator that consent has been granted.

  After the Office 365 administrator grants consent, click **Done and enable** in the Microsoft Office 365 configuration dialog box. If the Mitel Administration could not detect whether the consent was successful or not, the integration status will be as displayed as shown in the following image.

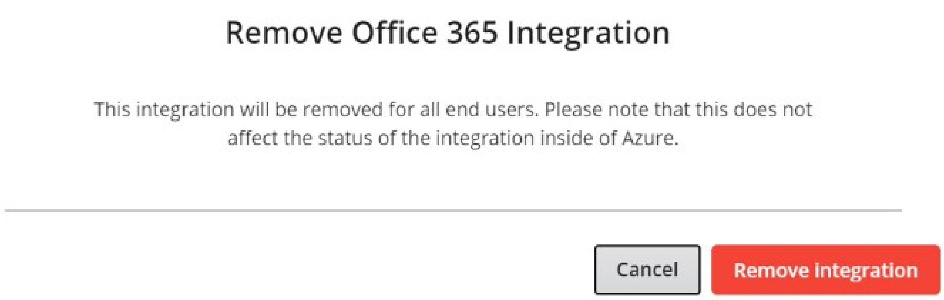


Removing Microsoft Office 365 integration from a customer account

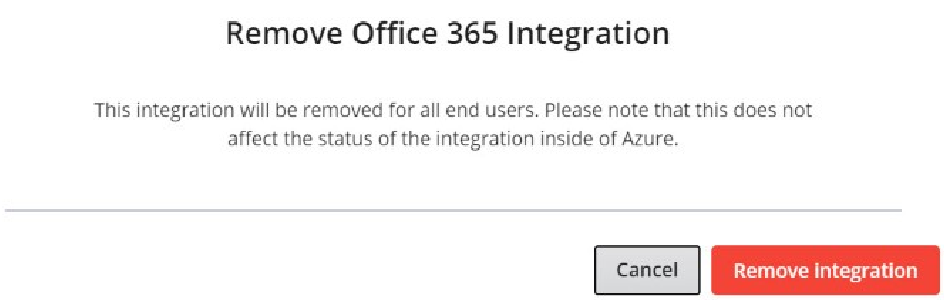
You can remove an existing Microsoft Office 365 integration from a customer account using one of the following methods:

- Click the  icon associated with the integration in the **Integrations** panel. The Microsoft Office 365 integration will be removed from the customer account.
- Click the **Remove** button from the Microsoft Office 365 configuration dialog box. To access the dialog box, do either of the following:
  - If the integration is added but not enabled, click the **Setup** button associated with the integration in the **Integrations** panel. The dialog box opens.
  - If the integration is added and enabled, click the  icon associated with the integration in the **Integrations** panel.

  From the **Remove Office 365 Integration** confirmatory panel than opens, click **Remove integration** to remove the integration. Clicking **Cancel** cancels the operation.



- Disable the toggle button associated with the **Microsoft Office 365 integration** in the **Integrations** panel. From the **Remove Office 365 Integration** confirmatory panel than opens, click **Remove integration** to remove the integration. Clicking **Cancel** cancels the operation.



3.2.4 Integrating Twilio with Mitel Administration

You can configure integrations with Twilio using Mitel Administration.

If Twilio integration is enabled for a customer account, users in that account can integrate their Twilio account with their CloudLink applications.

Adding Twilio integration to a customer account

To add Twilio integration to a customer account:

1. Click **Accounts** from the left main menu. The **Account Information** page of the customer account opens.
2. In the **Integrations** section, click **+ Add new**.

   A pop-up screen displays the **Integrations** panel.

> **Note**:
> Mitel Partner cannot enable integrations in the Partner Account because 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. Mitel recommends that you disable any existing integrations in the Partner Account to avail the full functionality of CloudLink features. For more information about Partner Accounts, see Log in as a Mitel Partner.

3. Click the **3rd party** tab. A list of supported third-party applications are displayed. Click the **Add** button associated with **Twilio** and click **Done**.
4. The Twilio integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.

Enabling Twilio integration in a customer account

After you add the Twilio integration to a customer account, you must provide required details for your CloudLink account to synchronize with your organization's Twilio account to enable the integration. To do this:

1. Click the **Complete Setup** button associated with **Twilio** in the **Integrations** section. The Twilio configuration dialog box opens.
2. Enter a name for the Twilio account integration.
3. Enter the Account SID. (This information is from Twilio account of the customer).
4. Enter the Auth Token. (This information is from Twilio account of the customer).
5. Click **Save**.

Removing Twilio integration from a customer account

You can remove an existing Twilio integration from a customer account, to do so, complete the following:

1. Disable the toggle button associated with the **Twilio integration** in the **Integrations** panel.
2. From the **Remove Twilio Integration** confirmatory panel than opens, click **Remove integration** to remove the integration. Clicking **Cancel** cancels the operation.

3.2.4.1 Integrating WhatsApp, Facebook, and SMS through Twilio for Mitel CX

This integration enables the flow of messaging between contact center agents and customers using channels, such as, WhatsApp, Facebook Messenger, and SMS, through CloudLink-enabled Chat Media Servers.

Adding a Channel

To add a new channel, complete the following steps:

1. Click **Integrations & Apps** from the left navigation menu. Scroll to the **Integrations** panel, click icon associated with Twilio. The Twilio management page is displayed.

   Note:
   The Twilio option is available *only* if Twilio integration is enabled for the customer account.

2. Click **Add Channels** button to create a new connection to WhatsApp, Facebook, or SMS. The **New Channel** dialog appears.

3. Select the **Channel** type from the dropdown list - WhatsApp Business, SMS, Facebook Messenger.

   a. If you are adding **WhatsApp Business** channel, use the checkbox to select the **Phone Number** to send the WhatsApp message to.
   b. Paste the **Queue ID** from the **Chat Queue** associated with the CloudLink-enabled Chat Media Server.

   > **Note**:
   > To locate the **Queue ID**, go to **YourSite** explorer, select the **Chat Queue** that is associated with the CloudLink-enabled Chat Media Server. Click the **Queue Tools** tab, and click **Copy queue ID** button.

   c. Click **Create** to create the channel. The new channel is added to the **Configured Channels** list.

   a. If you are adding **SMS** channel, use the checkbox to select the **Phone Number** to send the message to.
   b. Paste the **Queue ID** from the **Chat Queue** associated with the CloudLink-enabled Chat Media Server.
   c. Click **Create** to create the channel. The new channel is added to the **Configured Channels** list.

   a. If you are adding **Facebook Messenger** channel, manually locate and add the names of the Facebook page(s) in the **Page** field.
   b. Paste the **Queue ID** from the **Chat Queue** associated with the CloudLink-enabled Chat Media Server.
   c. Click **Create** to create the channel. The new channel is added to the **Configured Channels** list.

> **Note**:
> After the Twilio channel is created in Mitel Administration, the Twilio administrator must manually copy and paste the new webhook URL into the Twilio administrative portal for **WhatsApp** and **Facebook Messenger**. See Adding webhook URL into Twilio administrative portal on page 221. However, the webhook URL for **SMS** is automatically added to the Twilio administrative portal.

Adding webhook URL into Twilio administrative portal

The Twilio interface has not automated adding the webhook URL of the newly created **WhatsApp** and **Facebook Messenger** channels automatically, complete the following steps to add the webhook URLs:

1. Navigate to **Integrations & Apps** > **Integrations** > **Twilio**. Click . The channel configuration page opens.

2. From the list, in the **social.webhook** column, hover over the webhook to display the pop-up containing the full URL.
3. From the pop-up, copy the URL text and send it to the Twilio administrator. Instruct the administrator to paste the URL into the **Webhook URL for incoming messages** field within the Twilio **Endpoint configuration** section. Then, ensure that the **Webhook method for incoming messages** dropdown is set to **HTTP POST**.

> **Note**:
> The **Fallback URL for incoming messages** and **Status callback URL fields** are not supported at this time. Leave these fields blank to prevent unnecessary messages from being sent.

Deleting a Channel

To delete a channel, complete the following steps:

1. Click **Integrations & Apps** from the left navigation menu. Scroll to the **Integrations** panel, click icon against Twilio. The Twilio management page is displayed.
2. Select the channel(s) you want to delete using the checkbox, click **Delete Selected**. The Delete Channel(s) confirmation pop-up is displayed.
3. Type **confirm** in the **Type 'confirm'** field in the pop-up. Click **Delete**. The selected channel(s) is deleted.

3.2.4.2 Integrating SMS through Twilio for MiCollab

This integration enables the flow of messaging between contact center agents and customers using SMS through CloudLink-enabled Chat Media Servers.

Prerequisites

Before enabling the SMS feature, activate the following features on the Mitel Administration portal:

- CloudLink Chat
- Guest Access

> **Important**:
> It is recommended that the partner/customer register their brand with Twilio for A2P messaging from the Trust Hub.

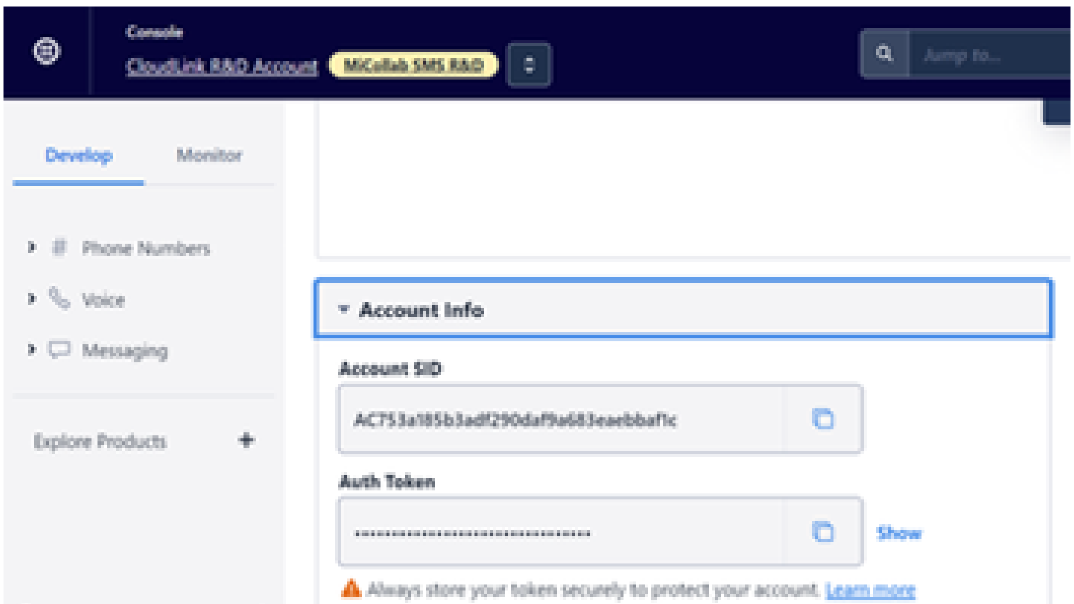
Enabling SMS and assigning provider numbers from Mitel Administration

To enable the SMS feature for a MiCollab account, proceed with the following steps:

1. From the Mitel Administration, click **Integrations & Apps** from the left navigation menu.
2. In the **Integrations** section, click **+Add new**.

   A pop-up screen displays the **Integrations** panel.
3. Select the **3rd party** tab. A list of supported third-party applications is displayed. Click the **Add** button associated with Twilio and click **Done**.

   The Twilio integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.
4. To configure the Twilio integration within the Mitel Administration, you need to access the Twilio console to retrieve the **Account SID** and **Auth Token**.



Enabling Twilio integration in a customer account

After you add the Twilio integration to a customer account, you must provide required details for your CloudLink account to synchronize with your organization's Twilio account to enable the integration. To do this:

1. Click the **Complete Setup** button associated with **Twilio** in the **Integrations** section. The Twilio configuration dialog box opens.
2. Enter a **Name** for the Twilio account integration.
3. Enter the **Account SID** (enter the information retrieved from Twilio console).
4. Enter the **Auth Token** (enter the information retrieved from Twilio console).
5. Click **Save**.

Integrating SMS

After a successful integration, you can assign Twilio phone number for MiCollab SMS. To do this:

1. Click **Integrations & Apps** from the left navigation menu. Scroll to the **Integrations** panel, click icon ⚙ associated with Twilio.

   The Twilio management page is displayed. This page displays a MiCollab entry in the table.
2. Select phone numbers that can be used within the MiCollab SMS Feature and click the **Edit** button. A list of active phone numbers configured in Twilio is displayed.
3. Select or search for the phone numbers from the **Phone Number** drop-down list.

   > **Note**:
   > If the phone numbers are actively used in the stream, a message "in-use" is displayed next to it. These phone numbers cannot be de-selected. To de-select, the phone number must be deactivated within the MiCollab Stream. Removing

4. Click **Save**.

   The numbers are assigned to MiCollab SMS.

Enable Guest Access from Mitel Administration

1. From the Mitel Administration, click **Integrations & Apps** from the left navigation menu.
2. In the **Privileges** panel, enable **Allow Guest Access** if it is not enabled.

Removing Integration

To remove the Twilio integration, all phone numbers associated with the MiCollab product must NOT be in-use. If the phone numbers are in-use, a dialogue appears to indicate that the numbers are actively being used.

3.2.5 Integrating CM.com with Mitel Administration

If CM.com integration is enabled for a customer account, users in that account can integrate their CM.com account with their CloudLink applications.

Adding CM.com integration to a customer account

To add CM.com integration to a customer account:

1. Click Accounts, **Account Information** page of the customer account opens.
2. In the **Integrations** section, click **+ Add new**.

A pop-up screen displays the **Integrations** panel.

> **Note**:
> A Mitel Partner cannot enable integrations in the Partner Account because 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. Mitel recommends that you disable any existing integrations in the Partner Account to avail the full functionality of CloudLink features. For more information about Partner Accounts, see Log in as a Mitel Partner.

1. Click the **3rd party** tab. A list of supported third-party applications are displayed. Click the **Add** button associated with **CM.com** and click **Done**.
2. The CM.com integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.

Enabling CM.com integration in a customer account

After you add the CM.com integration to a customer account, you must provide required details for your CloudLink account to synchronize with your organization's CM.com account to enable the integration. To do this:

1. Click the **Complete Setup** button associated with **CM.com** in the **Integrations** section. The CM.com configuration dialog box opens.
2. Enter a name for the CM.com account integration.
3. Enter the CM.com Account Id. (This information is from CM.com account of the customer).
4. Enter the Product Token. (This information is from CM.com account of the customer).
5. Click **Save**.

Removing CM.com integration from a customer account

You can remove an existing CM.com integration from a customer account, to do so, complete the following:

1. Disable the toggle button associated with the **CM.com integration** in the **Integrations** panel.
2. From the **Remove CM.com Integration** confirmatory panel than opens, click **Remove integration** to remove the integration. Clicking **Cancel** cancels the operation.

3.2.5.1 Integrating WhatsApp, Facebook, and SMS through CM.com

This integration enables the flow of messaging between contact center agents and customers using channels, such as, WhatsApp, Facebook Messenger, and SMS, through CloudLink-enabled Chat Media Servers.

Adding a Channel

To add a new channel complete the following steps:

1. Click **Integrations & Apps** from the left navigation menu. Scroll to the **Integrations** panel, click ⚙ against CM.com. The CM.com management page is displayed.

> **Note**:
> The CM.com option is available *only* if CM.com integration is enabled for the customer account.

2. Click **Add Channels** button to create a new connection to WhatsApp, Facebook, or SMS. The **New Channel** dialog appears.
3. Select the **Channel** type from the dropdown list - WhatsApp Business, SMS, Facebook Messenger.

   a. If you are adding **WhatsApp Business** or **SMS** channel, use the checkbox to select **Phone Number** to send the WhatsApp message or SMS.
   b. Select the **Queue** from the drop-down list.

   > **Note**:
   > The dropdown list of Chat Queues is being pulled from MiCC-B, if MiCC-B version is 10.1 or higher and the CloudLink Daemon is running on it.

   > **Note**:
   > If Mitel CX- version is below 10.1, you need to locate the Queue ID. To locate the Queue ID, go to **YourSite** explorer, select the **Chat Queue** that is associated with the CloudLink-enabled Chat Media Server. Click the **Queue Tools** tab, and click **Copy queue ID**button.

   c. Click **Create** to create the channel. The new channel is added to the Configured Channels list.

   a. If you are adding **Facebook Messenger** channel, select the **Page** from the list of pages available from the dropdown. You can select more than one page.

> **Note**:
> These pages are automatically added to the dropdown list from the configured Facebook Business pages in CM.com.

b. Paste the **Queue ID** from the Chat Queue associated with the CloudLink-enabled Chat Media Server.
c. Click **Create** to create the channel. The new channel is added to the Configured Channels list.

> **Note**:
> Once the channel is created, the CloudLink generated webhook URL is automatically added to the CM.com channel configuration.

Deleting a Channel

To delete a channel, complete the following steps:

1. Click **Integrations & Apps** from the left navigation menu. Scroll to the **Integrations** panel, click icon against CM.com. The CM.com management page is displayed.
2. Select the channel(s) you want to delete using the checkbox, click **Delete Selected**. The Delete Channel(s) confirmation pop-up is displayed.
3. Type **confirm** in the **Type 'confirm'** field in the pop-up. Click **Delete**. The selected channel(s) is deleted.

3.2.6 Provisioning Users from Azure Active Directory into CloudLink

CloudLink supports automatic provisioning of users from Azure Active Directory (Azure AD) into the CloudLink database. For this, the user data in this directory is synchronized with the CloudLink database using System for Cross-domain Identity Management (SCIM). This enables a Mitel Partner or an Account Admin to manage the users and application services in Azure AD and have them provisioned into the CloudLink database, which minimizes data entry and administration tasks.

Note:
For MiVoice Office 400, Mitel recommends the Active Directory (AD) integration to be configured through Mitel Open Interface Platform (OIP) as this method is used as a directory integration rather than the user creation. This allows all PBX users access to all the imported contacts, provided **PBX extended search** is enabled in the Contacts (Web client) or Contacts (Mobile client). For more details about AD integration using Mitel OIP, see Mitel Open Interfaces Platform - System Manual

Prerequisites

To configure provisioning of users from Azure AD into CloudLink, the Mitel Partner or Account Admin:

- Must have:
  - An Azure AD subscription

    If you do not have an Azure AD environment, you can get a free account.
  - A Mitel CloudLink account.
- The user ID, email address, mobile number, phone number, extension number, and login ID, must be unique while importing users from Azure AD into CloudLink.

In this document, it is assumed:

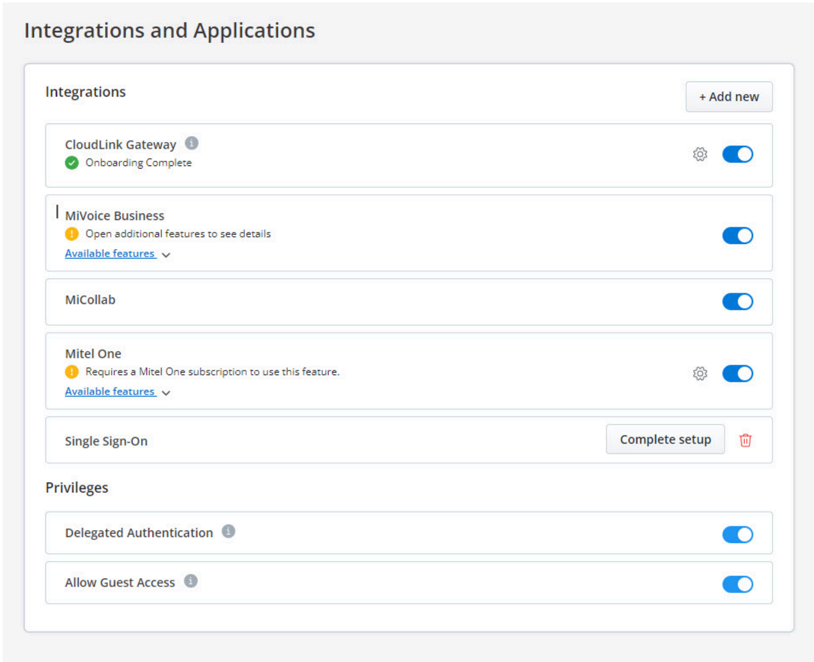
- The Azure AD environment and Azure accounts setup are available.
- The administrator has good knowledge of cloud technologies, especially, Microsoft Azure.
- The Azure integration with CloudLink is approved by the customer's IT or equivalent department.
- The connectivity between Azure and the customer premises is active and it supports real time applications, for example, the connectivity must have low latency.
- The HTTPS and SIP/TLS protocols (highly recommended) are used in the Azure setup.
- The NTP and DNS servers are configured and accessible from Azure, so the Mitel Administration can access these servers during the provisioning.

Adding Azure AD Sync integration to a customer account

Provisioning users from Azure AD into a customer account in Mitel Administration requires Azure AD Sync integration to be added to that customer account from the Mitel Administration. A Mitel Partner or an Account Admin can add Azure AD Sync integration to a customer account by using the following procedure:

1. Navigate to the **Account Information** page of the customer account.

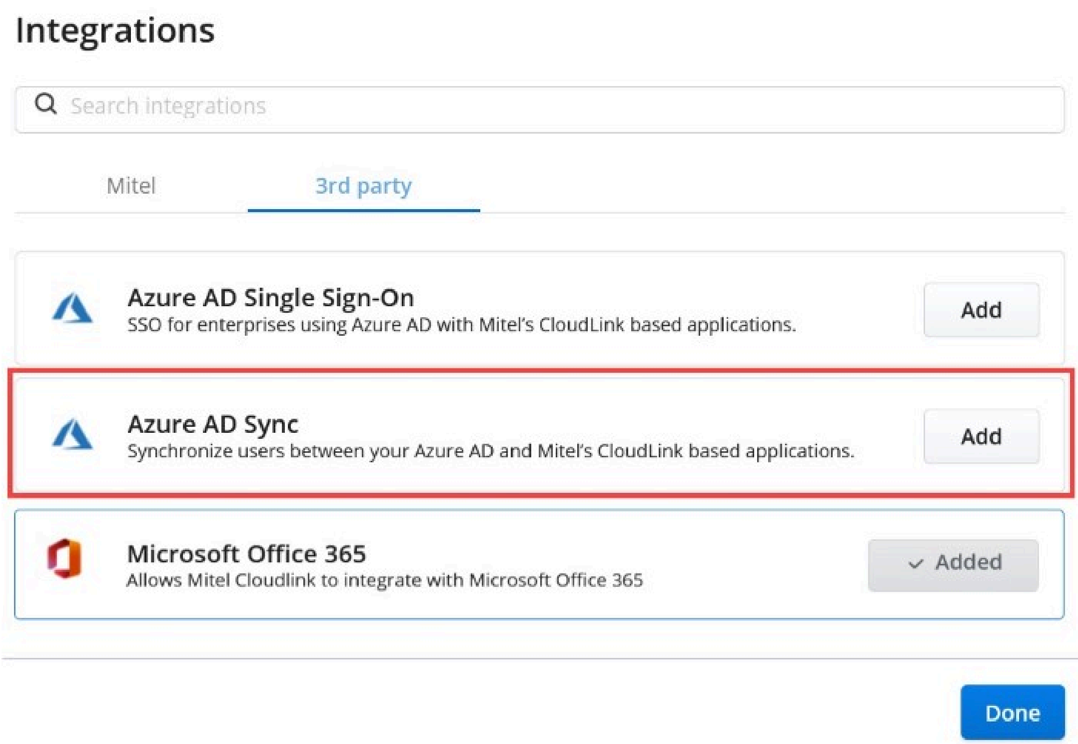
2. In the **Integrations** section, click **+ Add new**.



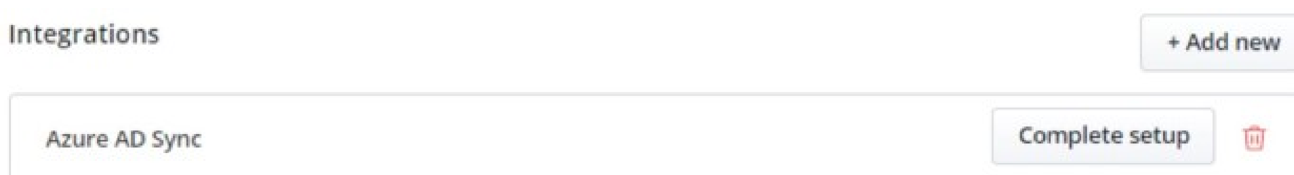
A pop-up screen displays the **Integrations** panel.

> **Note**:
> A Mitel Partner cannot enable integrations in the Partner Account because 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. Mitel recommends that you disable any existing integrations in the Partner Account to avail the full functionality of CloudLink features. For more information about Partner Accounts, see Log in as a Mitel Partner.

3. Click the **3rd party** tab. A list of third-party applications supported by CloudLink is displayed. Click the **Add** button associated with **Azure AD Sync**, and click **Done**.



The Azure AD Sync integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.



Provisioning Users from Azure AD into CloudLink using SCIM

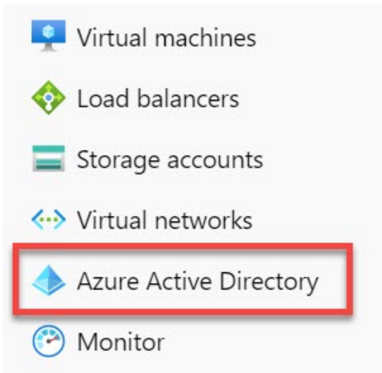
Provisioning users from the Azure AD to the CloudLink database using SCIM involves the following tasks:

1. Creating a SCIM application in Azure AD on page 231 — create a SCIM application to enable user provisioning.
2. Adding users to the SCIM application on page 232 — add users to the SCIM application.
3. Configuring the SCIM application on page 234 — configure the SCIM settings on the application side.
4. Testing the Connection on page 238 — verify that the configuration works.
5. Managing the attribute mappings on page 239 — review and customize the attribute mappings that will be synchronized with the CloudLink database during provisioning.
6. Start Provisioning on page 243 — start provisioning users to the CloudLink database.

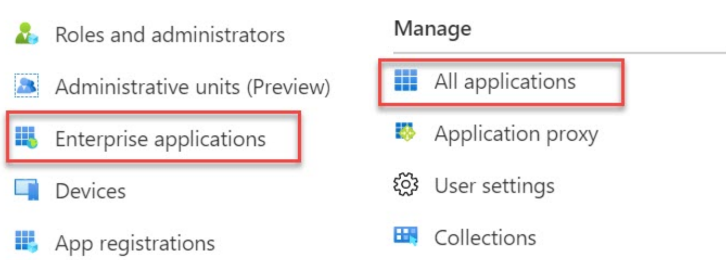
Creating a SCIM application in Azure AD

To create a SCIM application:

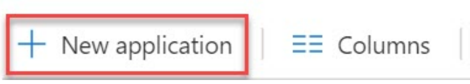
1. In the Azure portal, on the left navigation panel, click **Azure Active Directory**. The **Azure Active Directory** panel opens.



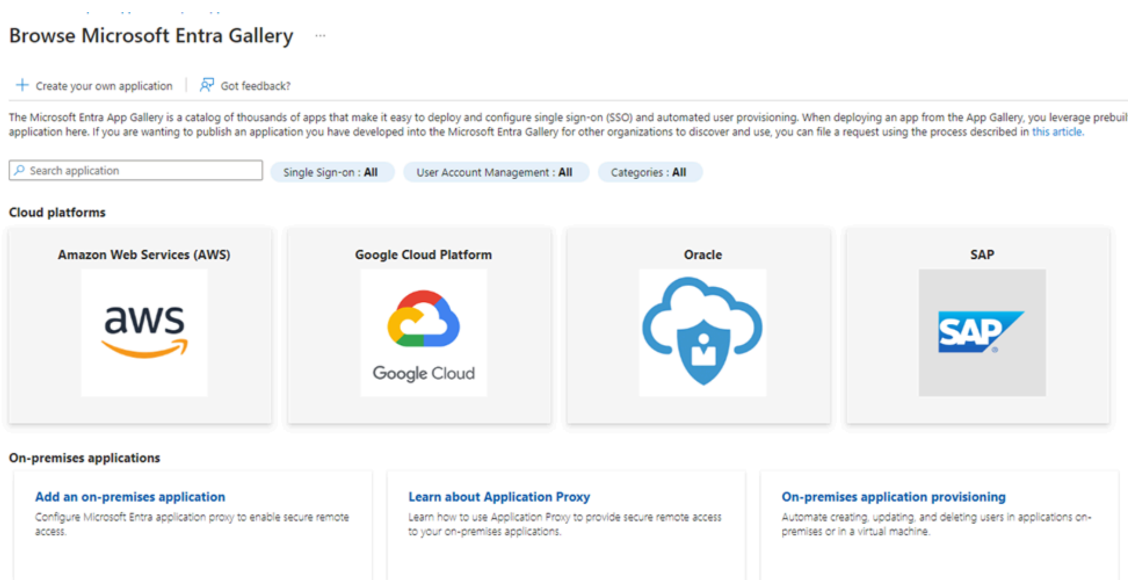
2. In the **Azure Active Directory** panel, select **Enterprise applications**. The **All applications** page opens, displaying a list of applications in your Azure AD tenant.



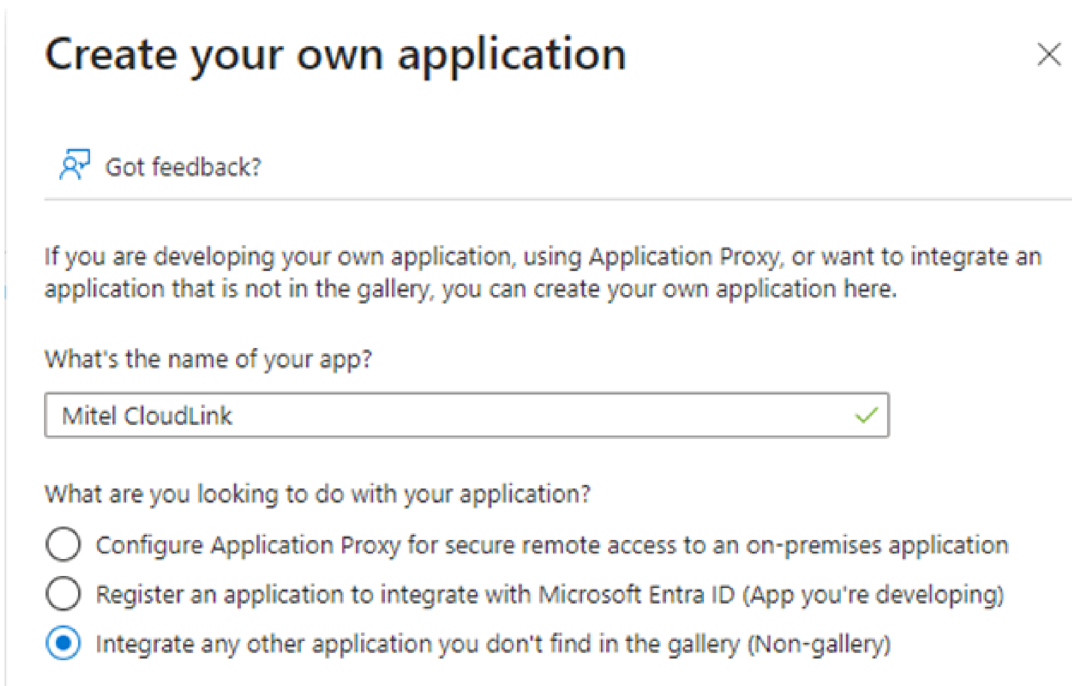
3. Click **New application**. The **Browse Microsoft Entra Gallery** page opens.



4. Click **+ create your own application**.



5. Type the name for your application (for example, Mitel CloudLink), and click **Add**.



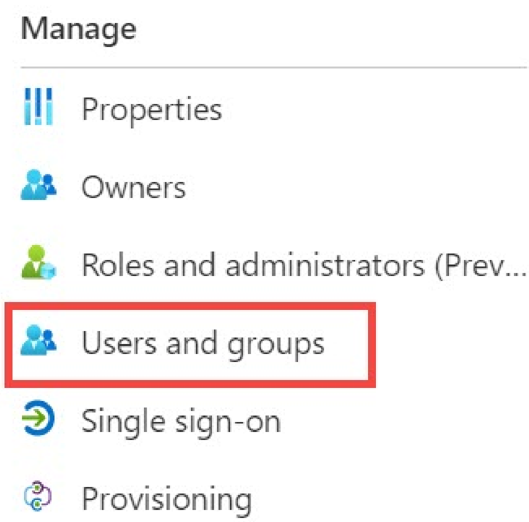
The application will be added to the Azure AD, and will be displayed in the **All applications** page.

Adding users to the SCIM application

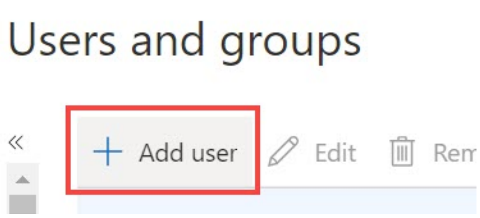
This section describes how to add users in the Azure Active Directory to the SCIM application to be provisioned to CloudLink.

1. Access the **Users and groups** page in the Azure portal, by doing the following:

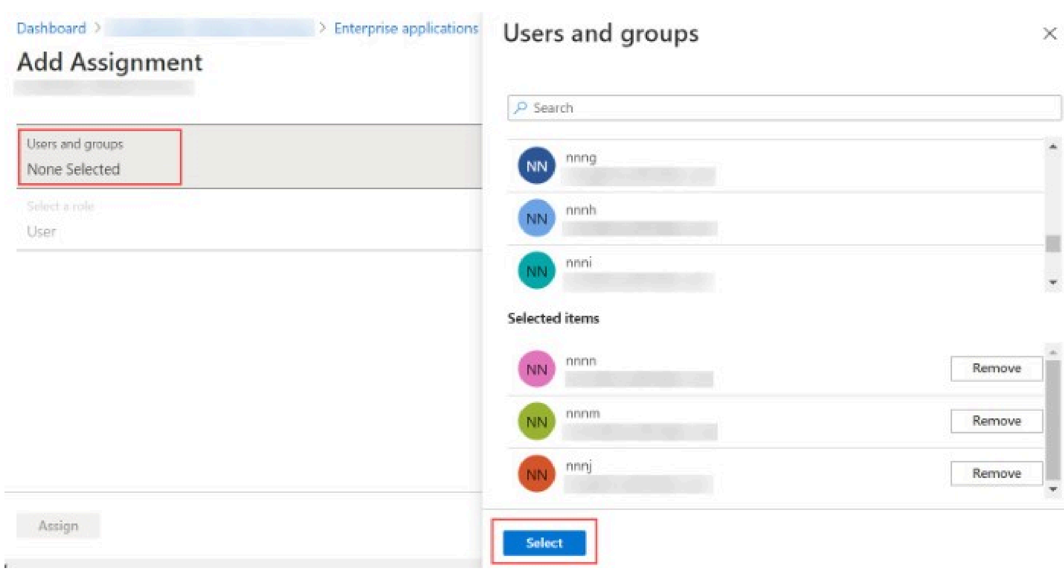
   a. Navigate to **Azure Active Directory** > **Enterprise applications**, and select your application from the list. The application's **Overview** page opens.
   b. Under the **Manage** section, select **Users and groups**.



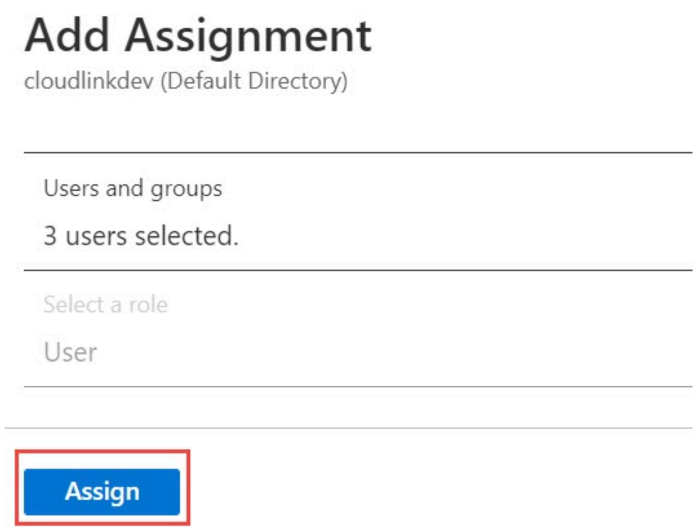
2. In the **Users and groups** page that opens, click **+ Add user**. The **Add Assignment** page opens.



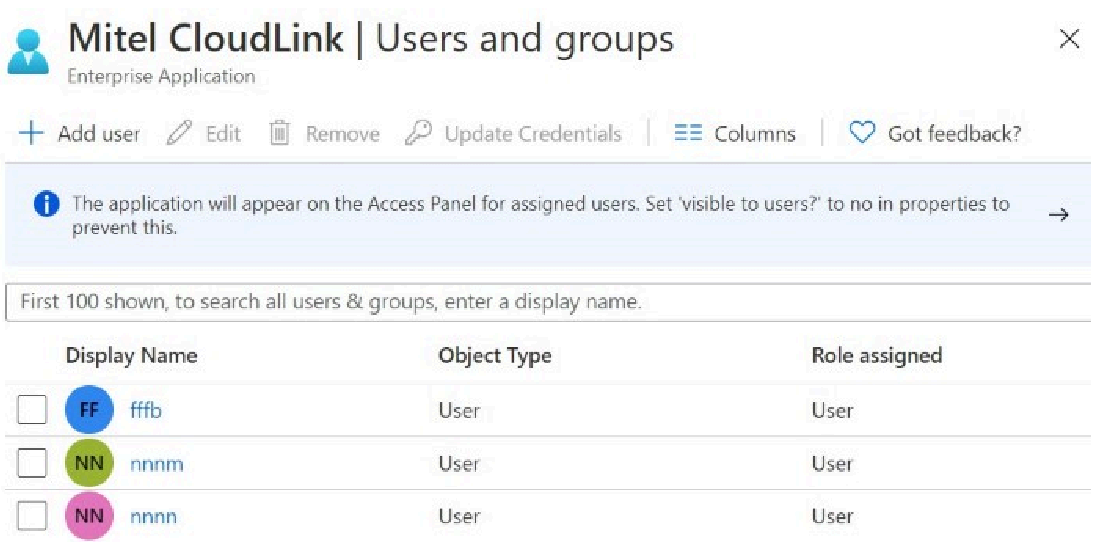
3. Click the **Users and groups** option. The **Users and groups** panel opens. From the list in the **Users and groups** panel, click the users you want to add to the SCIM application, and click **Select** to select these users. The selected users are listed under **Selected items**.



4. Click **Assign** to add these users to the SCIM application.



These users will be displayed in the **Users and groups** page.



Configuring the SCIM application

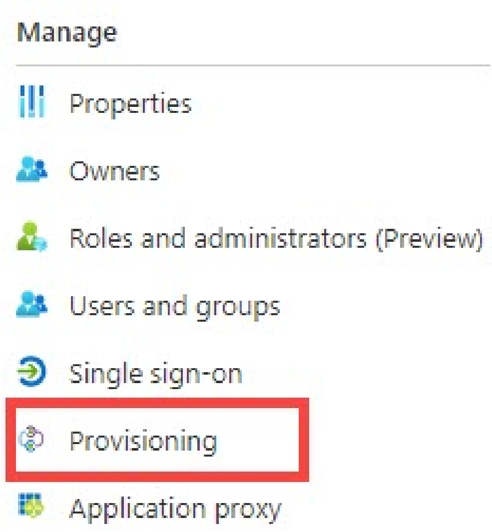
This section describes how to configure the SCIM application in Azure AD with the parameters supplied by the Mitel Administration to establish connection between the SCIM application and the Mitel Administration.

To configure the SCIM application, it is recommended that you open the Azure portal and the Mitel Administration side-by-side as you will need to copy some values from the Mitel Administration to the Azure portal.

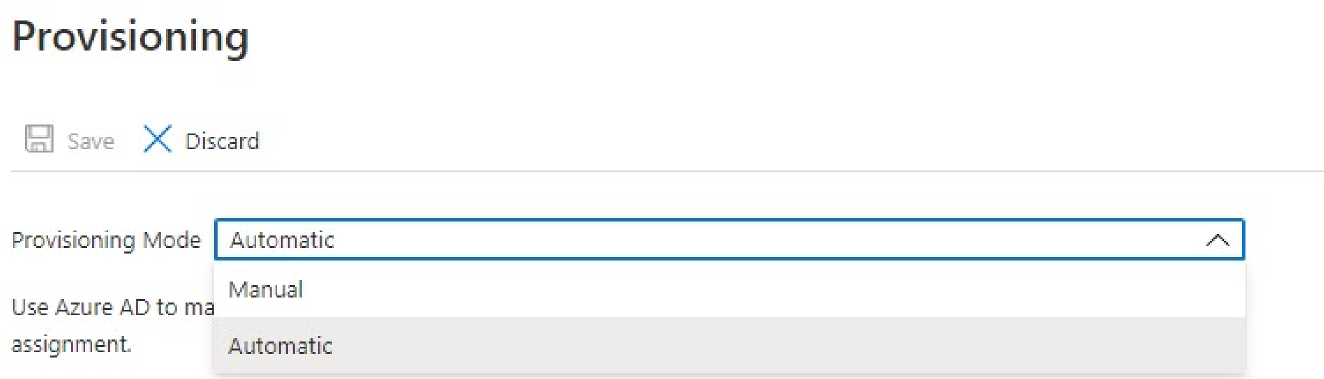
1. To access the **Provisioning** page in the Azure portal, do the following:

   a. Navigate to **Azure Active Directory** > **Enterprise applications**, and select your application from the list. The application's **Overview** page opens.

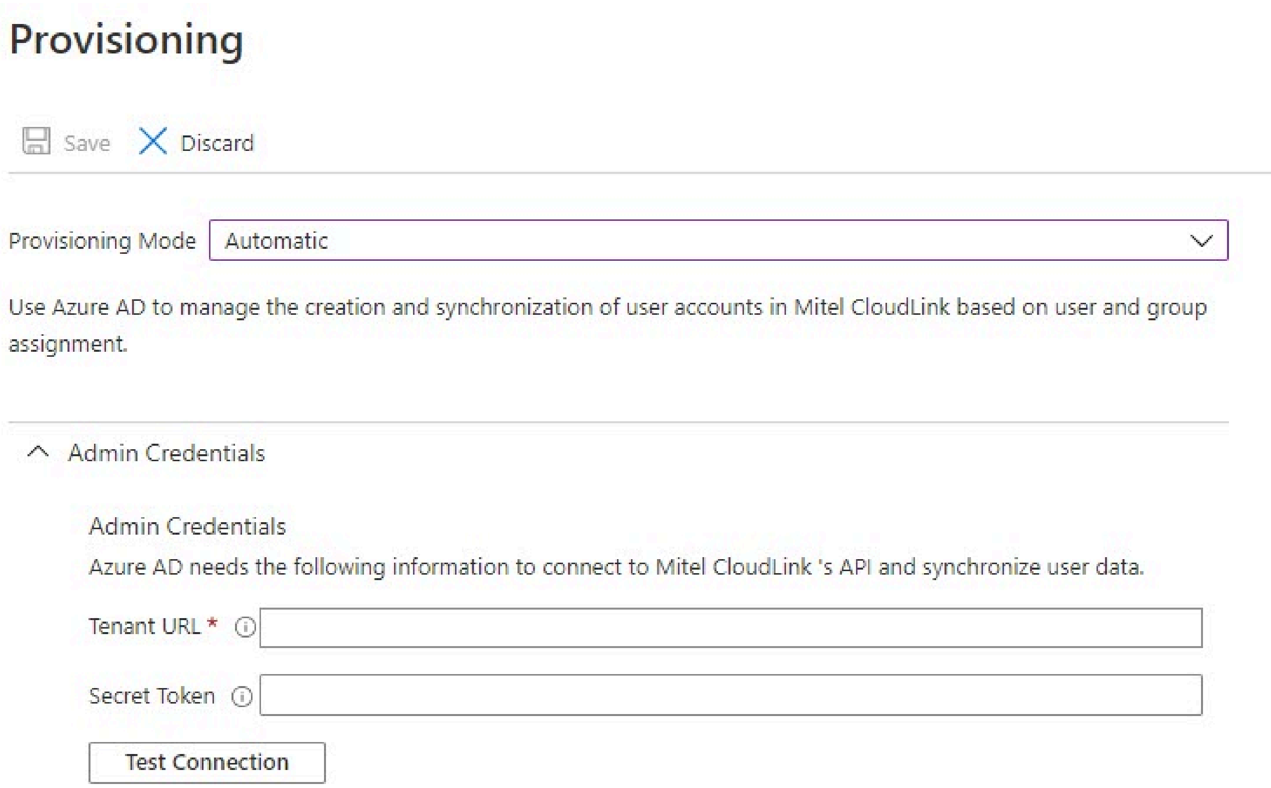
   b. Under the **Manage** section, select **Users and groups**.



2. In the **Provisioning** page that opens, select **Provisioning Mode** as **Automatic** from the drop-down menu.

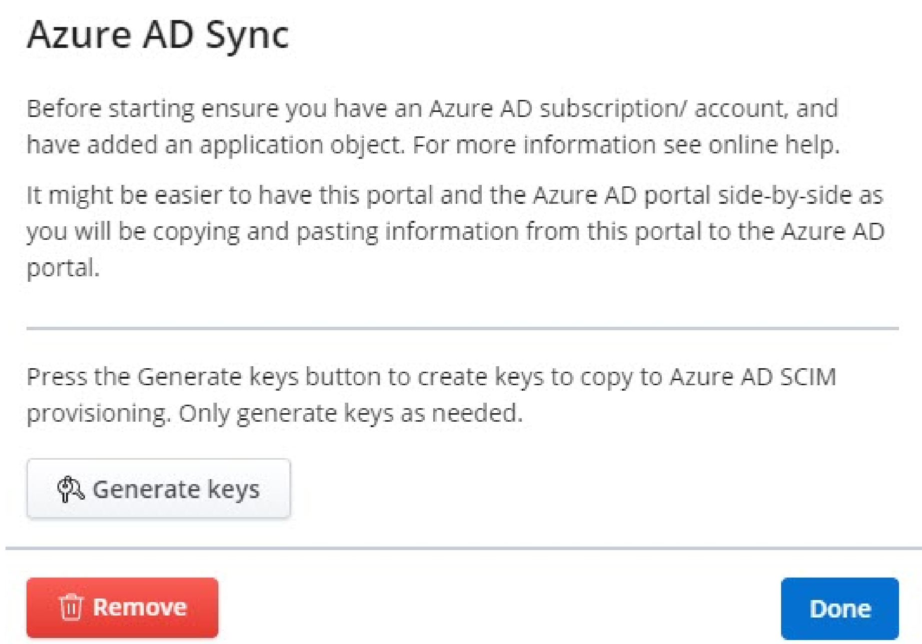


The **Admin Credentials** section is displayed.

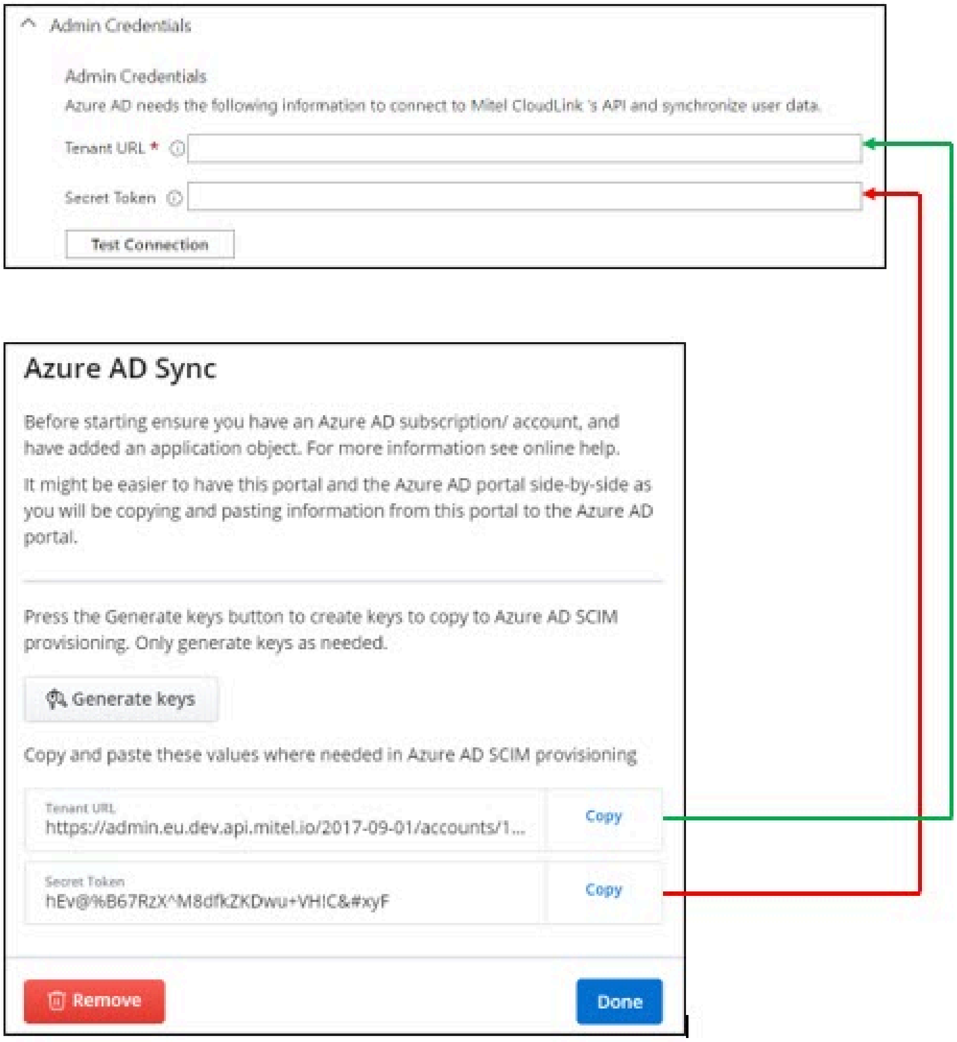


3. Provide the**Tenant URL** and the **Secret Token**. You can generate the URL and the token from the Mitel Administration by following these steps:

   a. From the **Integrations** section, click the **Complete setup** button associated with Azure AD Sync. The **Azure AD Sync** configuration dialog box opens.



   b. Click **Generate keys**. The **Tenant URL** and the **Secret Token** are generated. Click **Copy** and paste these values in the respective fields in the Azure AD portal.



Note:

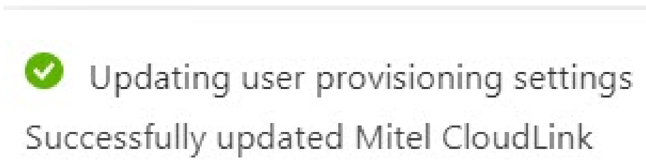
Every time **Generate keys** is clicked, any URL and token from a previous synchronization become invalid and the SCIM application must be configured with new ones.

Testing the Connection

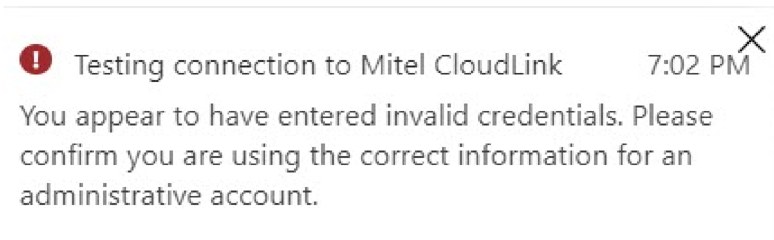
This section describes how to verify whether the configuration works, and to check whether the connection between the SCIM application and CloudLink is successful.

1. In the **Provisioning** page, within the **Admin Credentials** section, click **Test Connection**. The SCIM application attempts to connect to CloudLink.

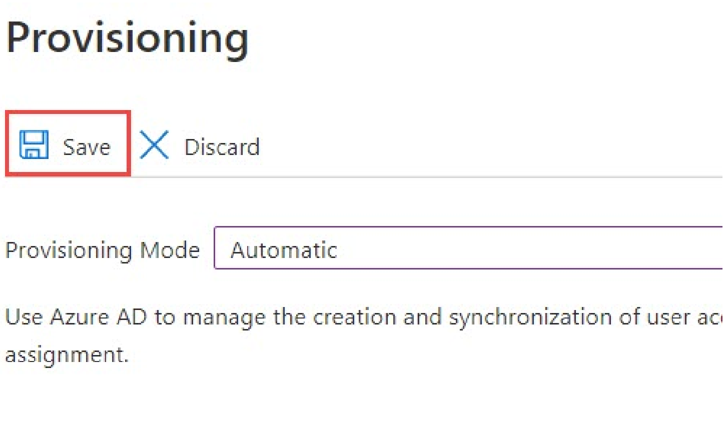
   If the connection is successful, the following message is displayed.

   If the connection fails, the following error message is displayed. Rectify the error and test the connection again.

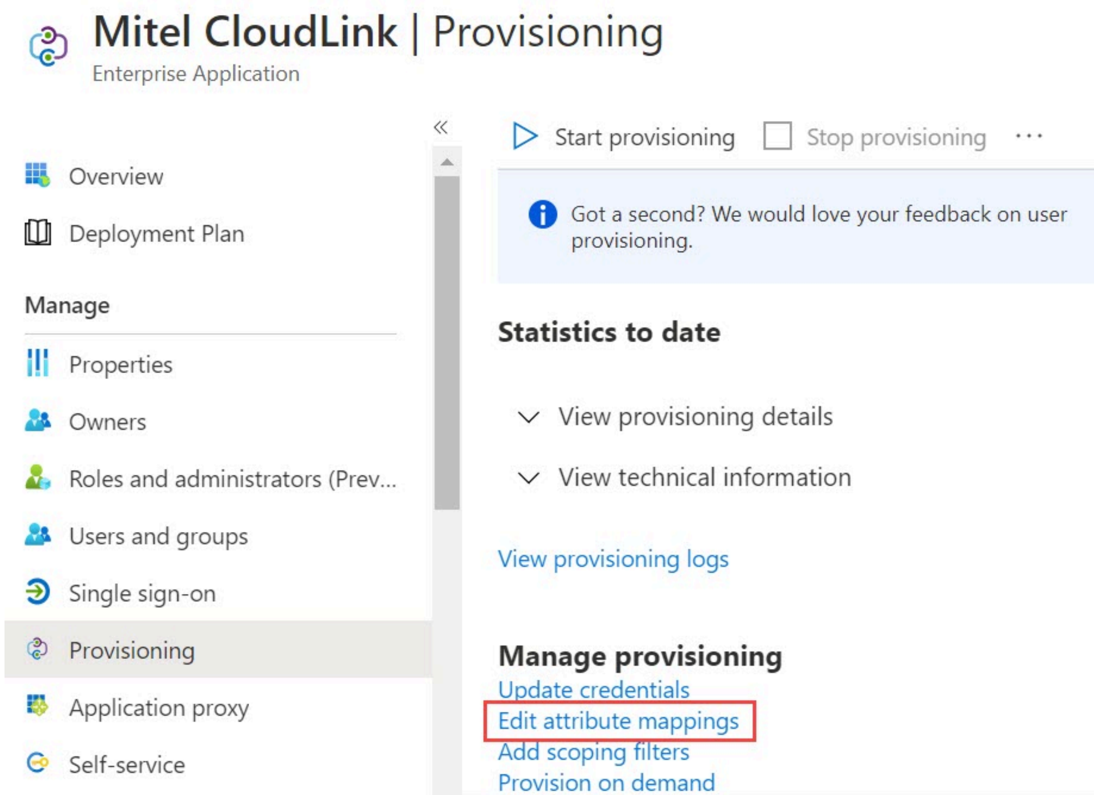
2. If the connection is successful, click **Save** to save the admin credentials for user provisioning. Clicking **Discard** will cancel the changes.

Managing the attribute mappings

This section describes how to customize the default attribute mappings in the SCIM application that define which user properties are provisioned from Azure AD to the CloudLink database. You can change or delete the current attribute-mappings, or create new attribute-mappings. To do this:

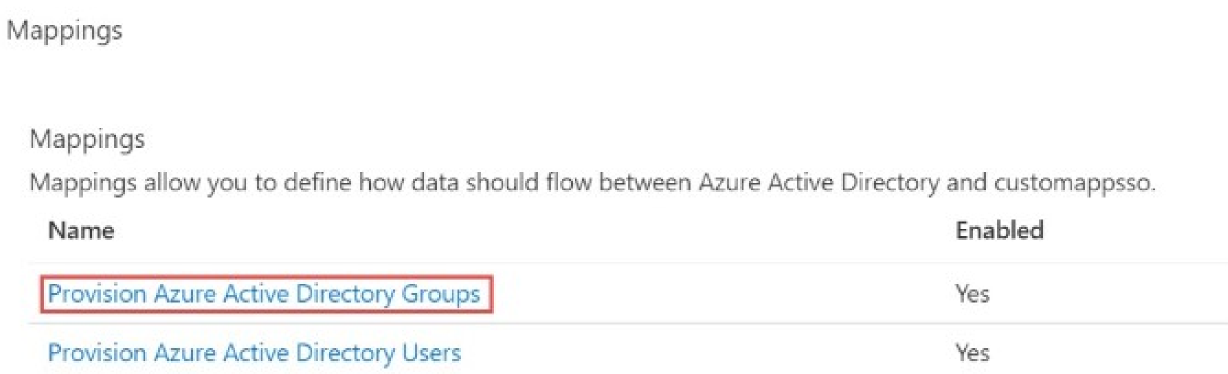
1. In the **Provisioning** page, click **Edit attribute mappings** from the **Manage provisioning** section.



2. In the page that opens, expand the **Mappings** tab, and do the following:

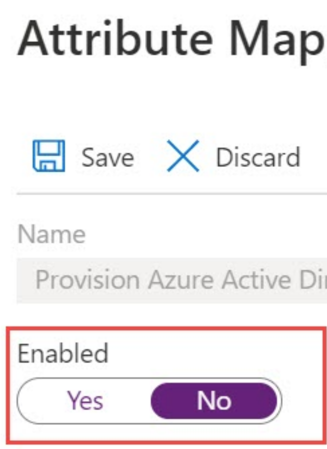
- **Disable Groups mapping**: You must disable the provisioning of group objects between the Azure AD and the CloudLink database. This is required because CloudLink database does not support provisioning group objects. To do this:

  a. Click **Provision Azure Active Directory Groups**.



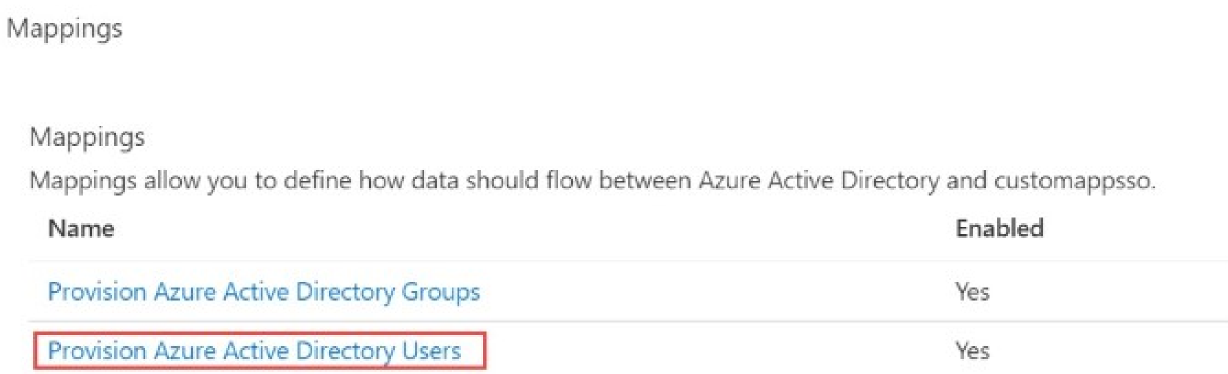
  b. In the **Attribute Mapping** page that opens, disable the **Enabled** option by clicking **No**. Click **Save** to save the changes.

> **Note**:
> By default, the **Enabled** option will be set to **Yes**.

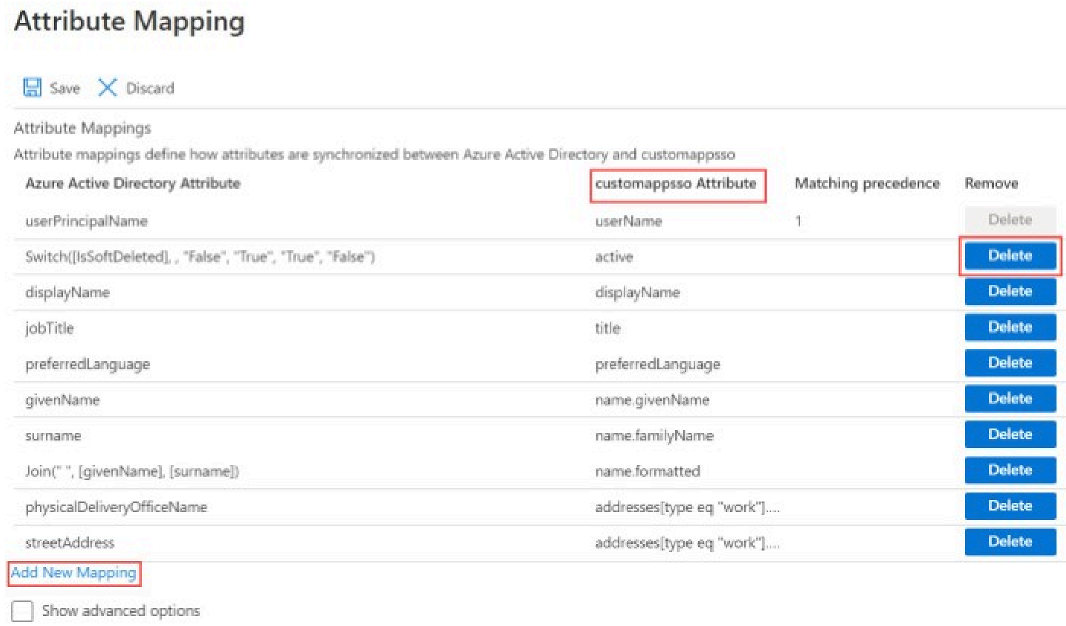


- **Customize attributes** : You must customize the attributes to be provisioned between Azure AD and the CloudLink database. To do this:

  a. Click **Provision Azure Active Directory Users**.



The **Attribute Mapping** page opens, displaying the list of default attributes in Azure AD.



b. You can choose to retain the default attribute mappings to be provisioned to the CloudLink database. You can also add new attribute mappings by clicking **Add New Mapping**. To delete a default attribute mapping, click the **Delete** option associated with the attribute.

You must ensure that the following conditions are met when you review the attributes to be provisioned between Azure AD and the CloudLink database.

- The following attributes listed under **customappsso Attribute** are mandatory and must not be deleted.
  - **userName**
  - one among **displayName**, **name.givenName**, or **name.familyName**
  - **emails[type eq "work"].value**
- CloudLink requires valid users to have an email address. To facilitate this requirement during provisioning, you must make sure that the attribute type **emails[type eq "work"].value** under **customappsso Attribute** is mapped to the attribute type under **Azure Active Directory Attribute** that contains the user's email address in Azure directory.
- In addition to the mandatory attributes mentioned above, CloudLink supports the following attributes listed under **customappsso Attribute**. You must select only the following attributes.
  - **active**
  - **externalId**
  - **emails[type eq "other"].value**
  - **phoneNumbers[type eq "mobile"].value**
  - **phoneNumbers[type eq "work"].value**
  - **phoneNumbers[type eq "other"].value**
  - **roles[primary eq "True"].value**
  - **all attributes related to addresses, MiCollab supports only the attributes related to the "work" type addresses.**

Note:

- In Azure AD, if you clear or leave blank any of the user details fields that is mapped to an attribute, the field will not be provisioned because Azure AD provisioning service does not support provisioning null values. For more information about attribute mapping properties, see Azure documentation.
- If you remove any attribute mapping in the Azure AD after you start provisioning, the modification will not be updated in the CloudLink database automatically.
- The Phone numbers must be in E164 format.

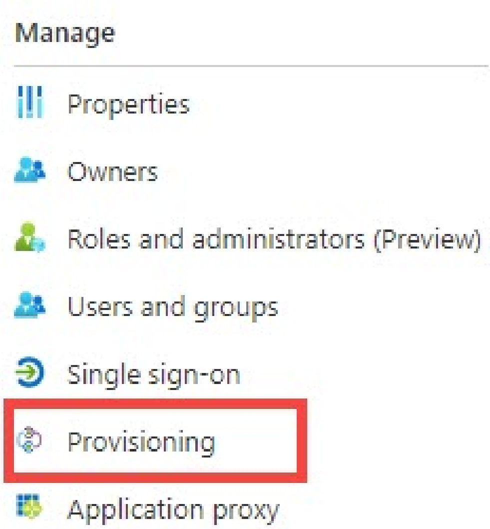
c. After you customize the necessary attribute mappings, click **Save** to save the changes. Clicking **Discard** will cancel the changes.

Start Provisioning

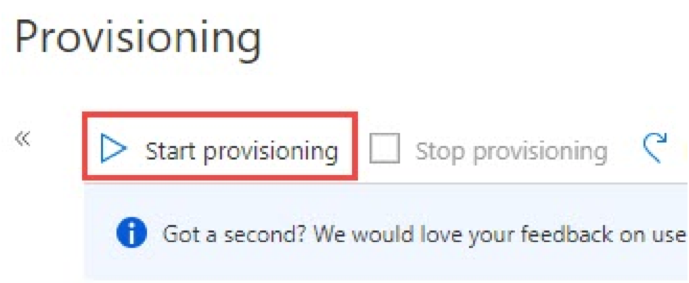
After you define the attributes, you must initiate the provisioning. To do this:

1. Access the **Provisioning** page in the Azure portal, by doing the following:

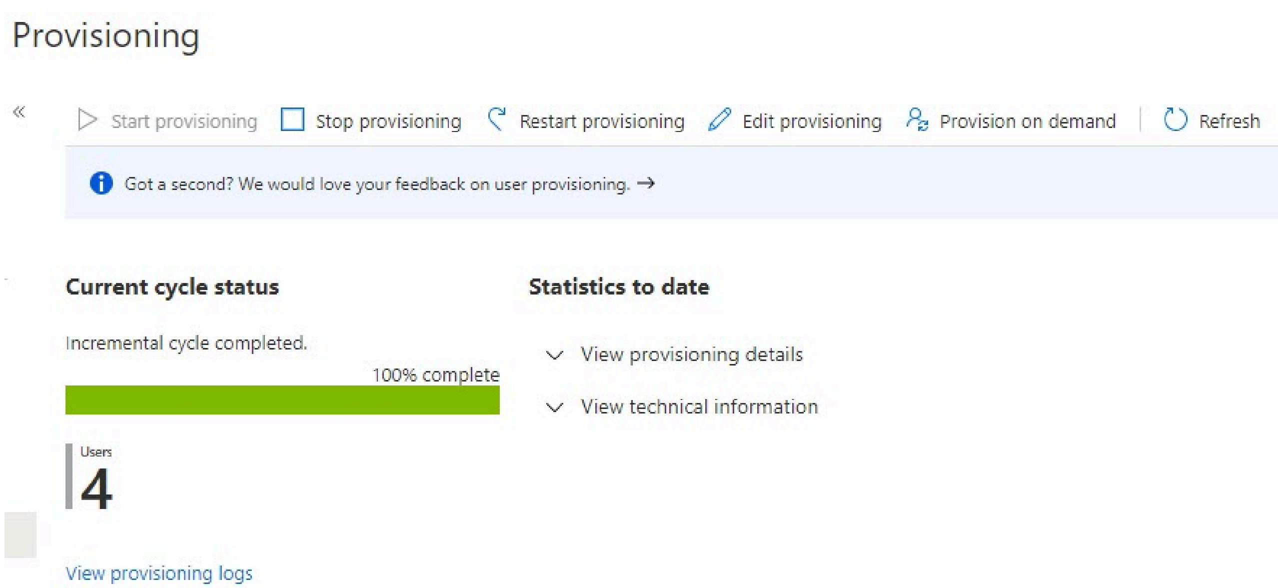
   a. Navigate to **Azure Active Directory** > **Enterprise applications**, and select your application from the list. The application's **Overview** page opens.
   b. Under the **Manage** section, select **Provisioning**.



2. In the **Provisioning** page that opens, click **Start provisioning**.



The Azure AD provisioning service runs an initial provisioning cycle. After the cycle is complete, the status of the cycle will be displayed in the **Provisioning** page as shown in the following screenshot.



The **Current cycle status** shows the completion status. This section also displays the number of users provisioned.

The initial provisioning cycle is followed by periodic incremental cycles. The incremental cycles happen every 40 minutes. For more information about provisioning cycles, see the Azure documentation.

Note:
If errors occur during a provisioning cycle, the synchronization is retried in the next cycle. If the errors continue to occur, then the retries will occur at a reduced frequency, that is, the frequency of scheduled provisioning will decrease. For more information, see the Azure documentation.

After the initial cycle is completed, you have the following options to manage the provisioning:

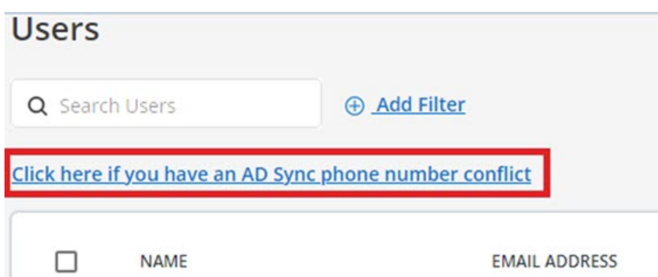
- **Stop provisioning**: Click this option to stop the provisioning process.
- **Restart provisioning**: Click this option to trigger the provisioning run manually without waiting for the next scheduled run.
- **Edit provisioning**: Click this option to edit the current configuration or to customize the attribute mappings.
- **Provision on demand**: Click this option to provision any changes to a single user. This is done manually. You can also use this option to validate and verify that the changes made to the configuration were applied properly and are being correctly synchronized with the CloudLink database.

Deleting a User with Phone Conflict

This feature allows administrators to search for users with phone number conflicts and delete them, including both active and inactive users.

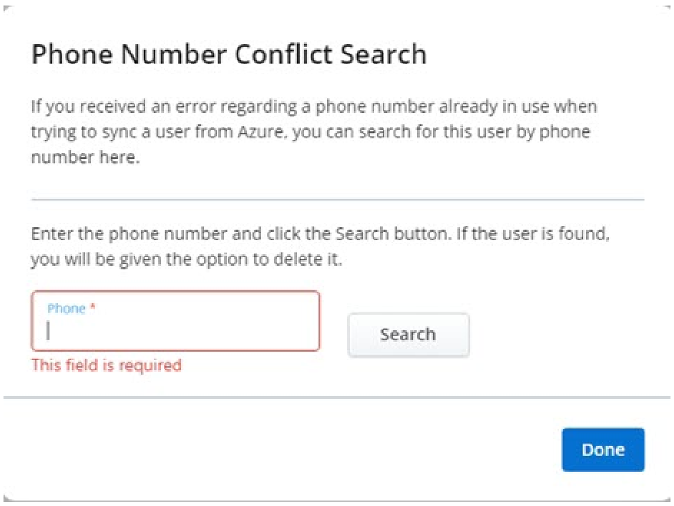
1. Navigate to the **Users** page.

> **Note**:
> For accounts with AD Sync integration, a link—'**Click here if you have an AD Sync phone number conflict**'—appears at the top of the Users page.



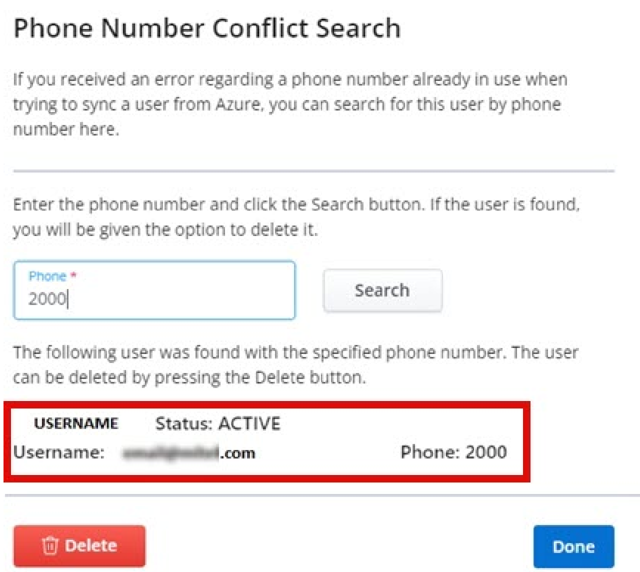
2. Select the **Click here if you have an AD Sync phone number conflict** link.

   The **Phone Number Conflict Search** dialog box appears.



3. Enter the phone number in the search box.
4. Click **Search**.

   The user appears at the bottom of the search box.



5. Verify the user.
6. Click **Delete** to remove the user.

3.2.7 Microsoft Teams Integration

Mitel provides the CloudLink to MS Teams Presence integration feature, which enables users to know the availability status of the users in the CloudLink account as part of their MS Teams presence. This is called a Unidirectional presence. This feature has now been expanded to enable the synchronization of Microsoft Teams presence of a user with their MiCollab client through CloudLink, and this is known as Bi-directional synchronization.

After the presence sync is enabled for users, the presence status displayed in MS Teams will be a combination of users' presence from the MS Teams clients and MiCollab presence.

3.2.7.1 Unidirectional presence

The integration of CloudLink to MS Teams presence of a user known as Unidirectional synchronization. To achieve this presence synchronization from CloudLink to MS Teams, follow the procedures that have been detailed out in this chapter. Following are the instructions for integrating Microsoft Teams with Mitel Administration.

Prerequisites

To configure Microsoft Teams integration with a CloudLink customer account, you must have:

- Gateway integration enabled. Depending on the PBX type, see the following documents for more information:
  - MiVoice Office 400: Configure MiVoice Office 400 PBX
  - MiVoice Office 5000: CloudLink Deployment Guide with MiVoice 5000
  - MiVoice Business: CloudLink Integration with MiVoice Business Deployment Guide
  - MX-ONE: Deployment Guide with MX-ONE

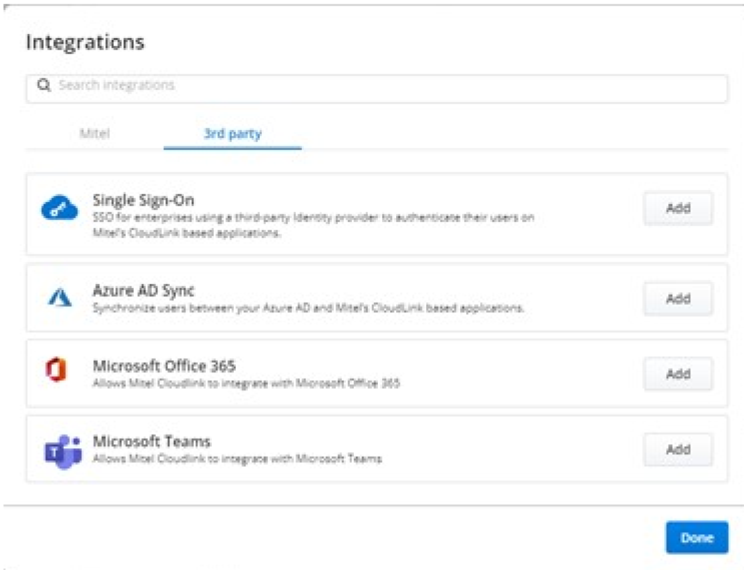
Note:
The email address of a user configured in the selected PBX must match the primary email address or the user principal name of the user in Azure AD.

Integrating Microsoft Teams with a Customer Account

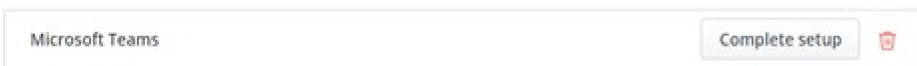
To integrate Microsoft Teams with a customer account, perform the following steps:

1. Log in to the Mitel Administration on page 1.
2. Access the **Integrations** panel from **Accounts Information** page or from **Integrations & Apps** option. For more information about accessing **Integrations** panel and adding integration to a customer account see, Adding an integration to a customer account on page 88.
3. In the **Integrations** panel, click **+ Add new**. A pop-up screen displays teh available integrations.

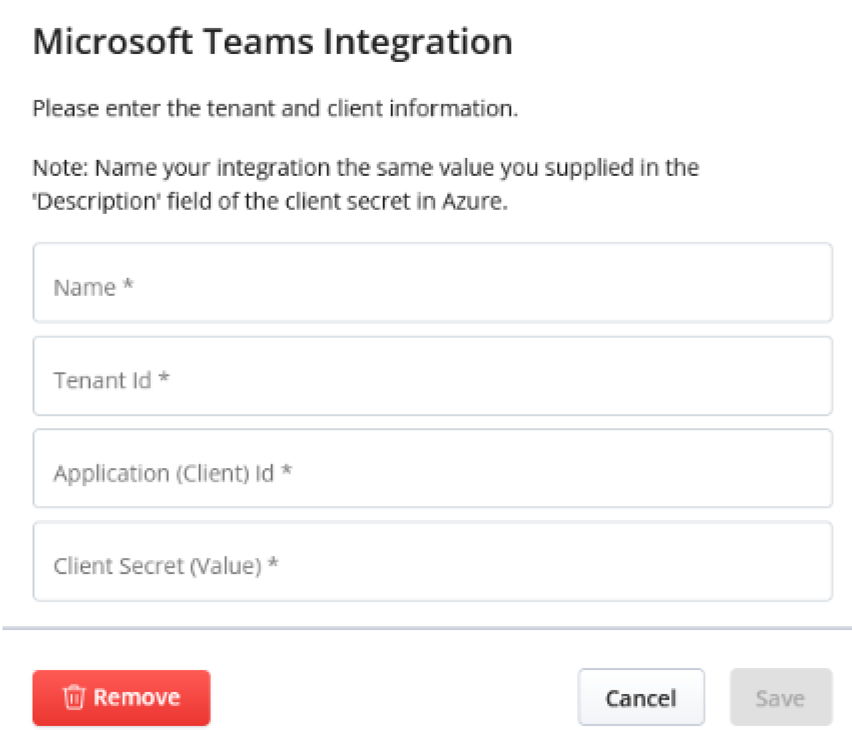
4. Click the **3rd party** tab. A list of supported third-party applications is displayed. Click the **Add** button associated with **Microsoft Teams**, and click **Done**.



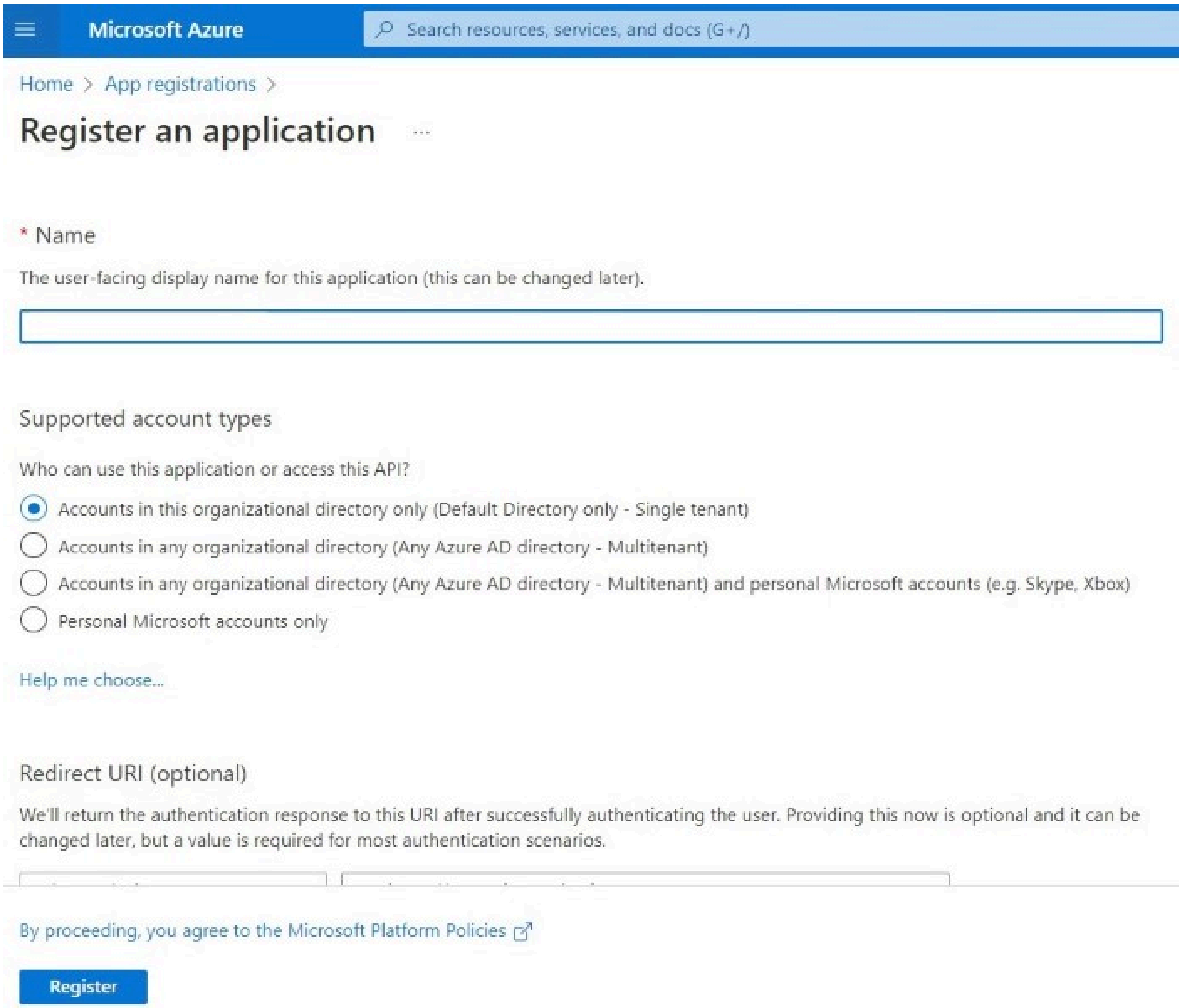
The Microsoft Teams integration is added to the customer account and is displayed in the **Integrations** section of the **Account Information** page.



5. Click **Complete setup**. The **Microsoft Teams Integrations** dialog box is displayed.

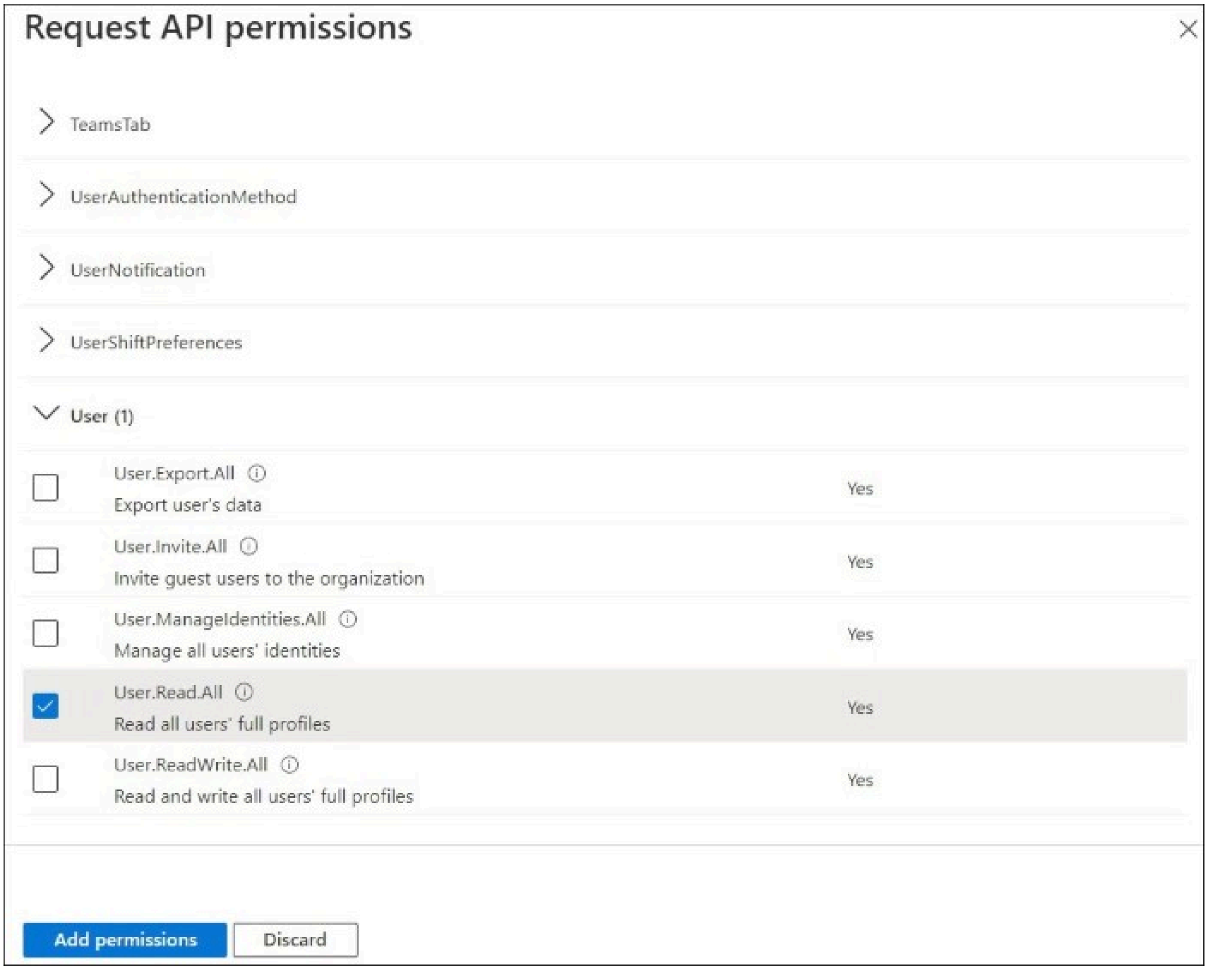


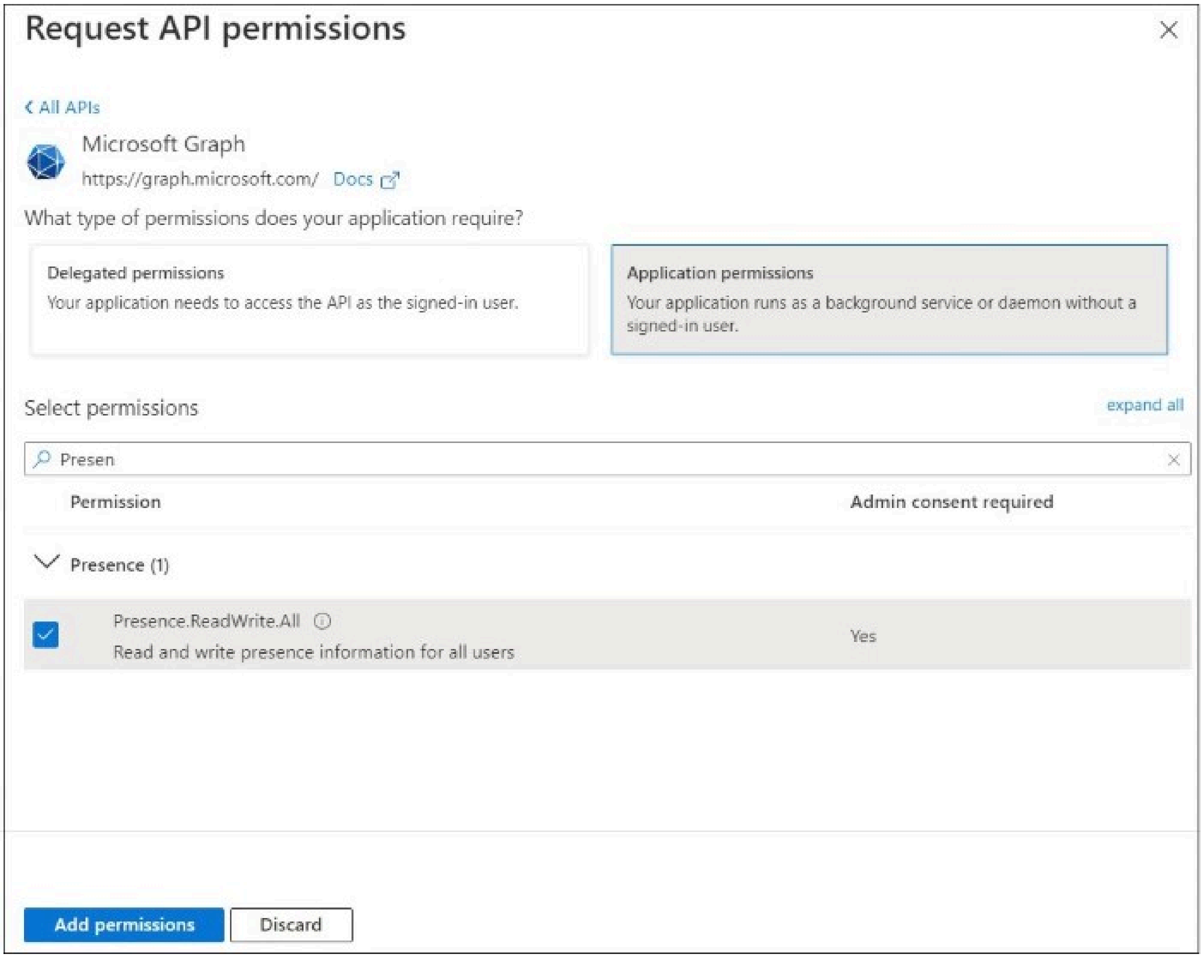
6. To create **Name**, **Tenant Id**, **Application (Client) Id**, and the **Client Secret (Value)**, you must create an Enterprise application. To create an Enterprise application, log in to Azure portal and click **App registration** > **New registration**. The **Register an application** page is displayed.



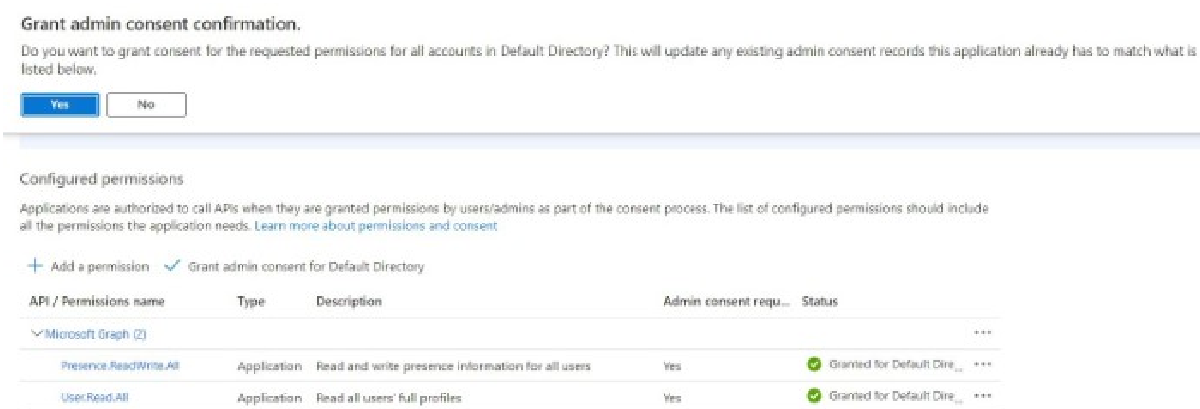
7. Enter the **Name** for the application and select the **Accounts in this organizational directory only (Default Directory only – Single tenant)** option under **Supported account types**.
8. Click **Register** to register the application.
9. Navigate to **API permissions** in the left navigation panel and click **+Add a permission**. The **Request API permissions** page is displayed.
10. Click **Microsoft Graph** and then select **Application permissions**.

11. Enable the **User.Read.All**, and **Presence.ReadWrite.All** permissions as shown in the following images.

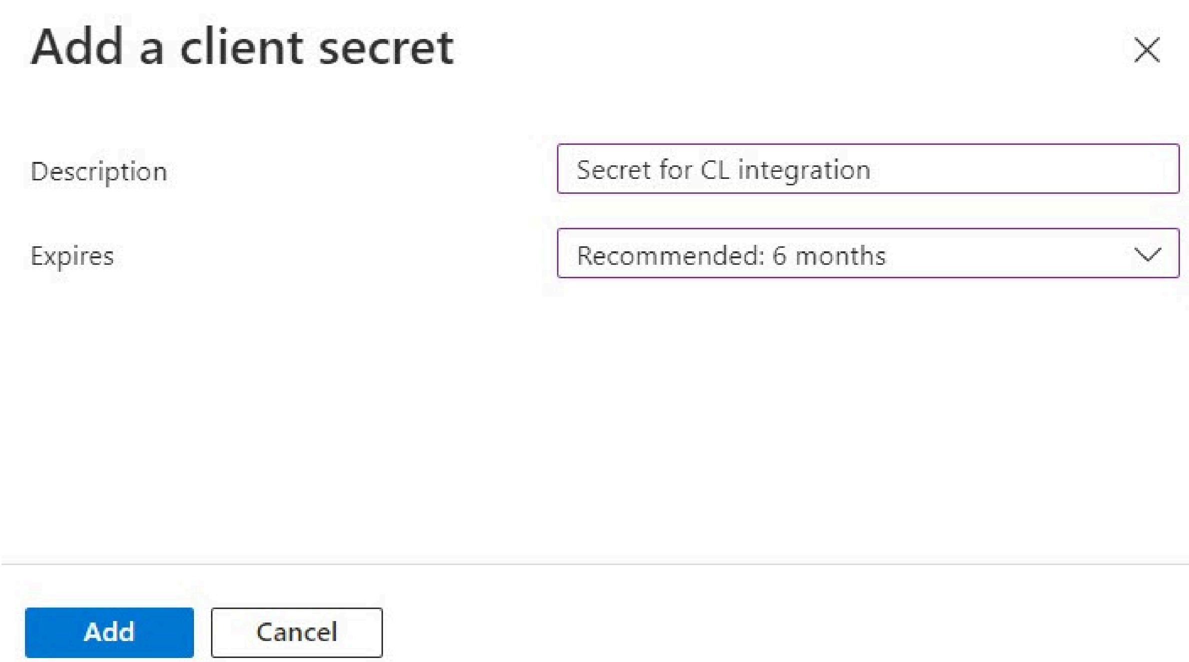




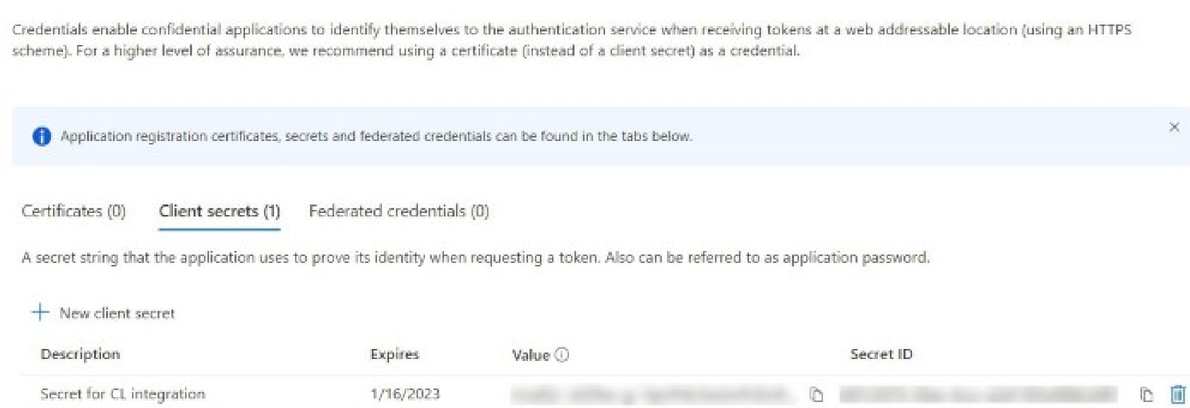
12. Click **Grant admin consent for XXXX** (directory name) and click **Yes** to grant consent.



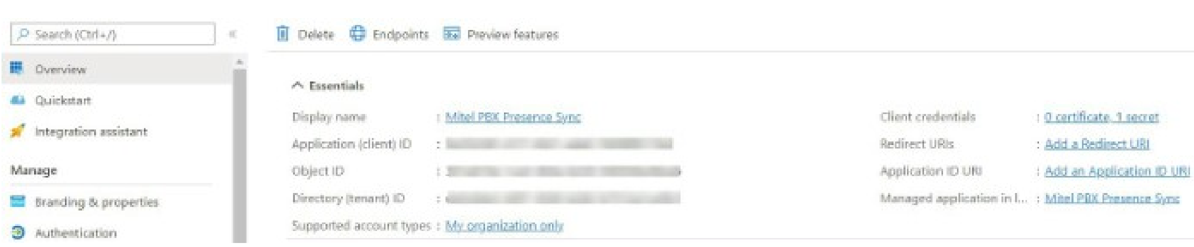
13. Navigate to **Certificate & secrets** in the left navigation panel and click the **Client secrets** tab. The **Add a client secret** dialog box is displayed.



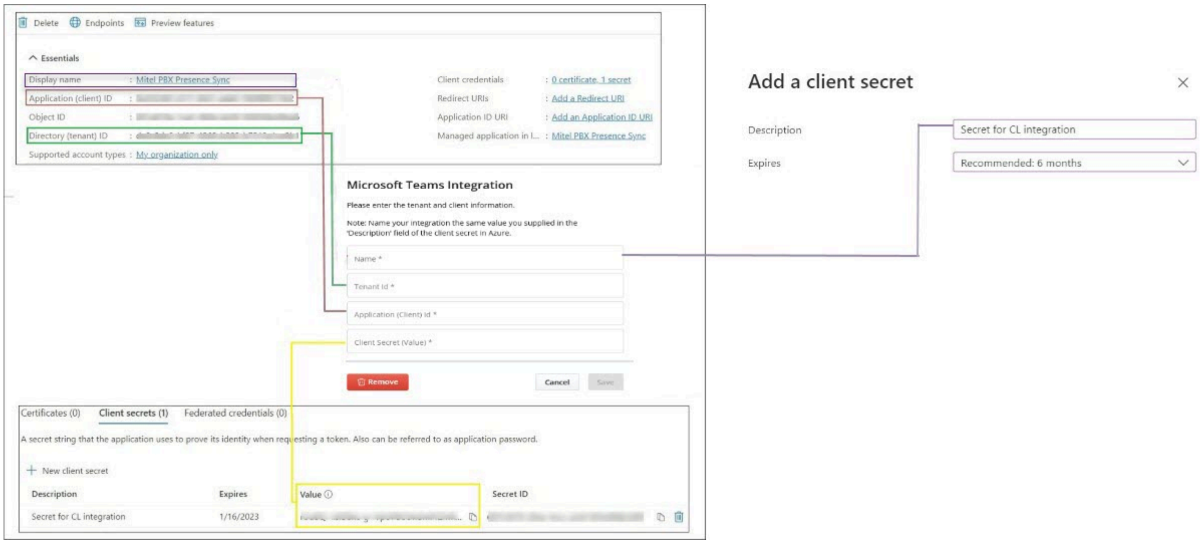
14. Enter the **Description** and select the expiry duration. You can select the expiry duration from a specific date till a specific date. Click **Add** to create the Client secrets.
15. Copy the value under the **Value** column.



16. Navigate to the Enterprise application that you created in Step 5 and copy the **Application (client) ID** and the **Directory (tenant) ID** values.

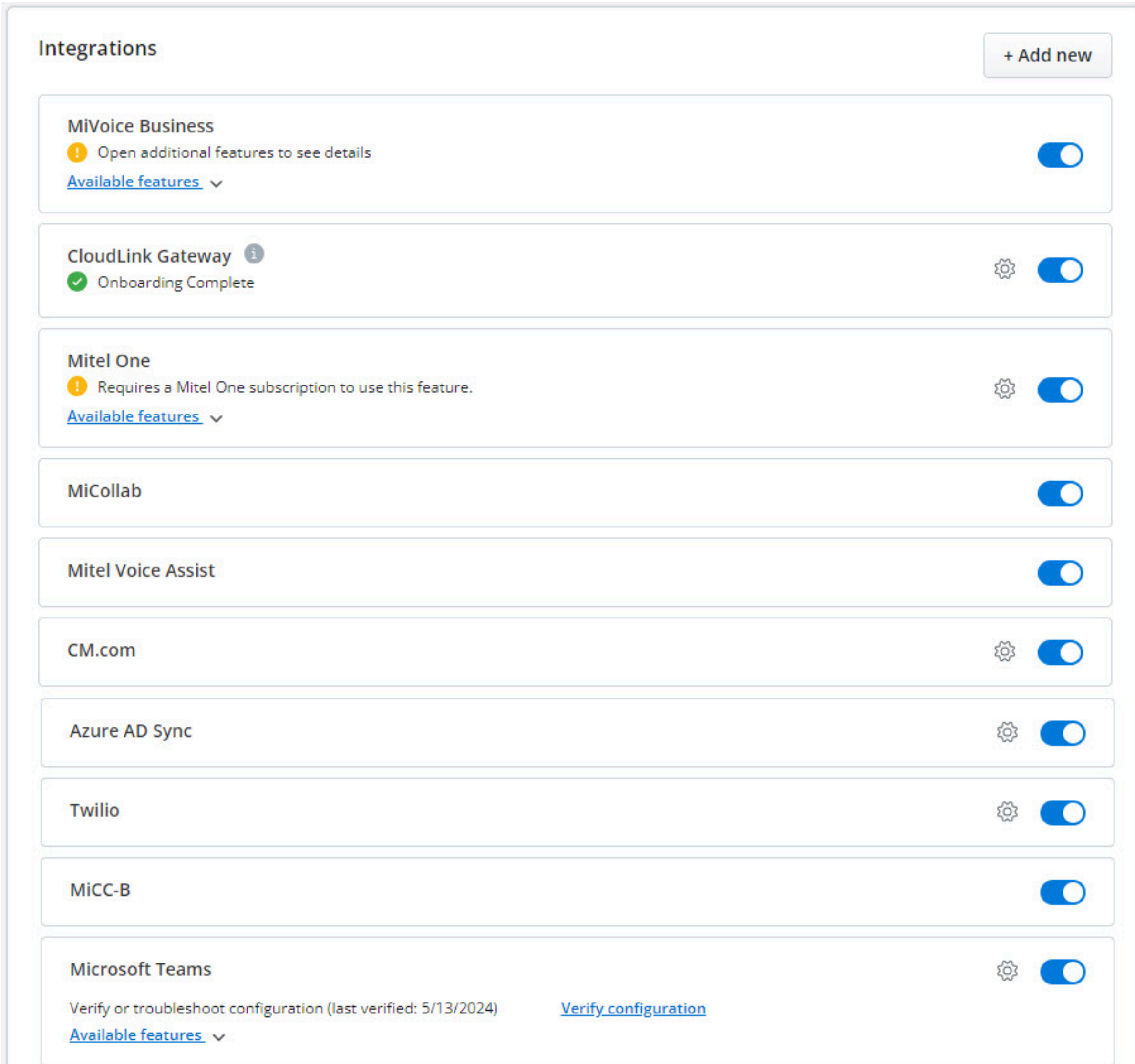


17. In the Mitel Administration, enter the **Name**, **Tenant Id**, **Application (Client) Id**, and the **Client Secret (Value)**.



18. Click **Save** to save the information. Clicking **Cancel** cancels the operation and clicking **Remove** removes the Microsoft Teams integration.

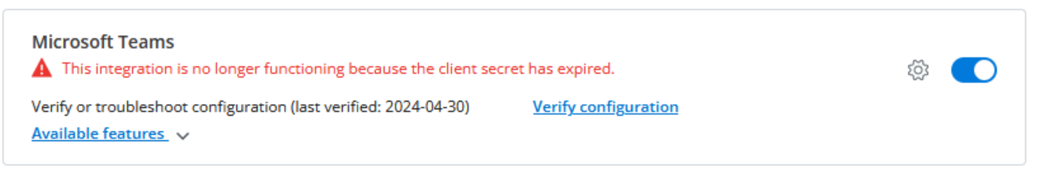
    After you have added Microsoft Teams integration to the customer account, **Microsoft Teams** will be listed in the **Integrations** panel.



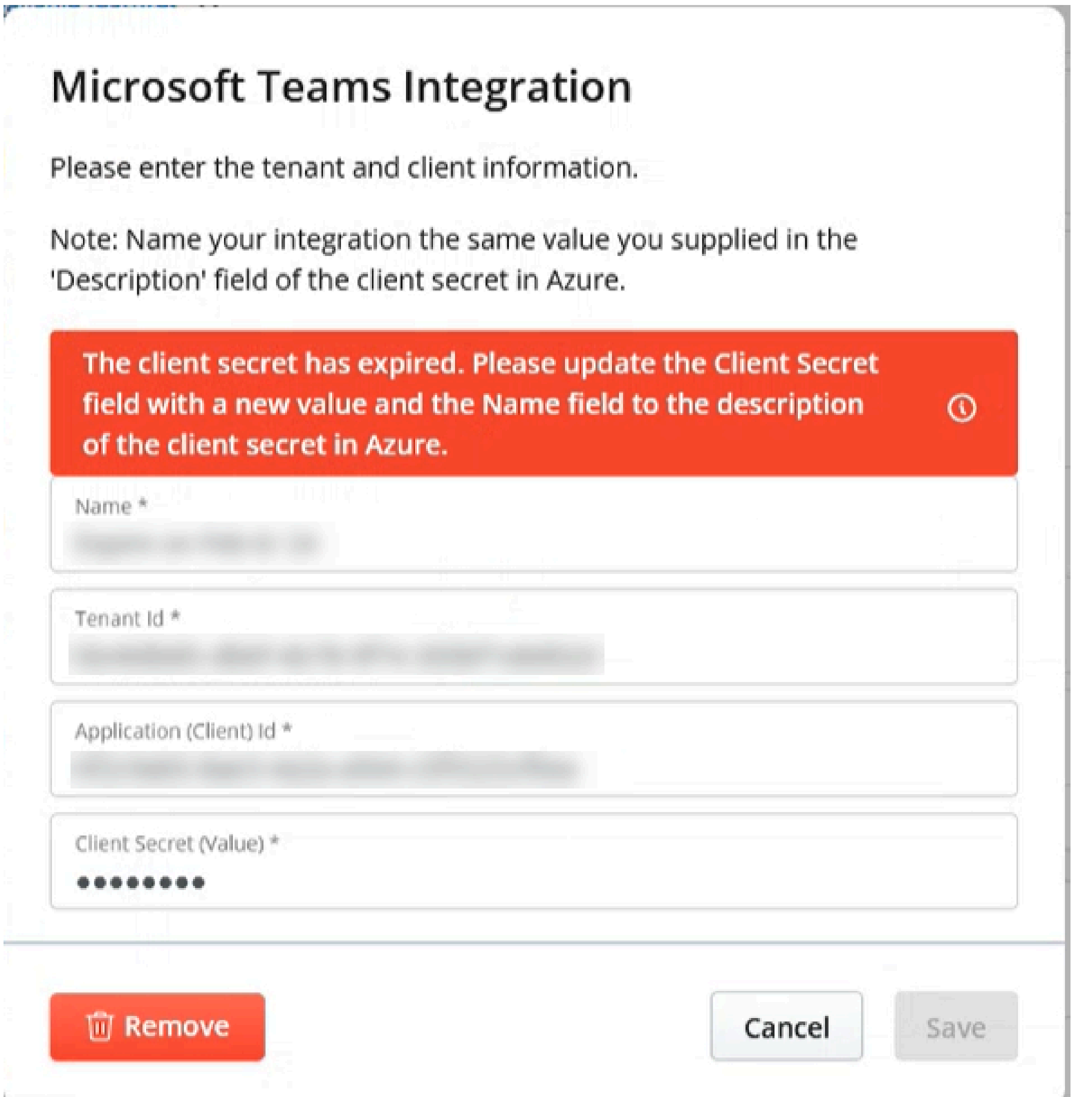
Client Secret Expired

Follow this procedure when the client secret expires:

1. Click the gear icon besides the Microsoft Teams Integration.



2. Replace the **Name** field with the description and **Client Secret (Value)**.



3. Click **Save**.
4. If you have used the same client secret for the main integration, you must also update the client secret for each presence monitor in **MS Teams to CloudLink Presence Configuration**. See Client Secret for more information.

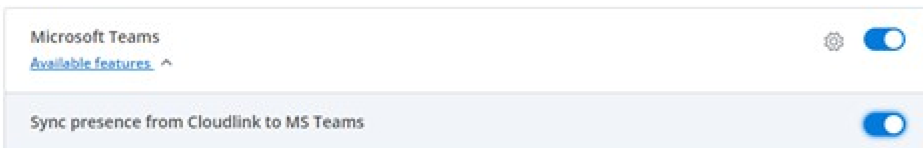
Enabling the Presence Feature

After integrating Microsoft Teams with a customer account, you can enable the Presence feature for that customer account. The Presence feature syncs the presence status of the user from CloudLink with MS Teams.

To enable the Presence feature, perform the following steps:

1. In the **Integrations** panel, click the drop-down arrow associated with **Available features** under Microsoft Teams.

2. Slide the toggle button to the right that is associated with **Sync presence from CloudLink to MS Teams**.



The Presence feature is now enabled for the customer account.

> **Note**:
> After enabling Presence feature, it takes few minutes for presence to reflect in MS Teams.

For more information about MS Teams Solution Guide see, MS Teams Solution Guide.

Microsoft Teams Integration Upgrade

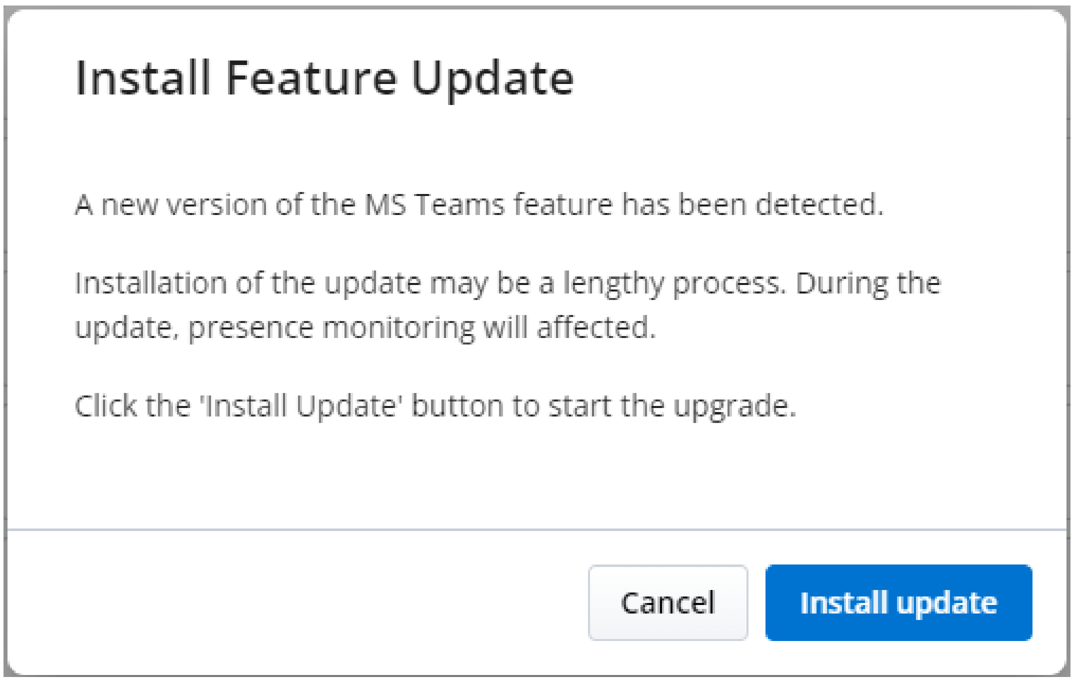
If there is a new Microsoft Teams integration feature update available, the **Install update** button is displayed next to Microsoft Teams.

> **Note**:
> If the Mitel Administration is already open and if there's any new update to the Microsoft Teams, you need to refresh the page to see the **Install update** button.

Perform the following steps to install feature update:

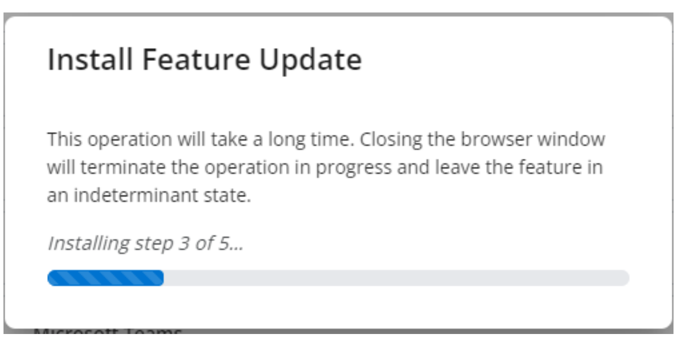
1. Click **Install Update** button.

   A new dialogue page is displayed.



2. Click **Install Update** button.

   A progress bar indicates the update's progress.



3. Once the update is complete, "Feature update complete" message is displayed. Click **Done**.

3.2.7.2 Bi-directional presence

The integration of MS Teams presence has been expanded to enable the synchronization of Microsoft Teams presence of a user with the MiCollab client through CloudLink, and this is known as Bi-directional presence synchronization. To achieve this presence synchronization from Microsoft Teams to MiCollab via CloudLink, follow the procedure below.

Bi-directional presence synchronization can be enabled for new users and existing users, for whom the Unidirectional presence is already enabled.

> **Note**:
> Presence status changes in MS Teams will take some time to be delivered and reflected in MiCollab. This includes manual presence changes and presence changes caused by calendar integration in MS Teams. According to Microsoft Documentation, the average expected latency is 10 seconds, with a maximum of 60 seconds.

The two primary procedures that enable the Microsoft Teams integration with Mitel Administration are:

1. Integrating Microsoft Teams with a Customer Account
2. Enabling the Presence Feature

> **Note**:
> If there is a new Microsoft Teams integration feature update available, refer Microsoft Teams Integration Upgrade.

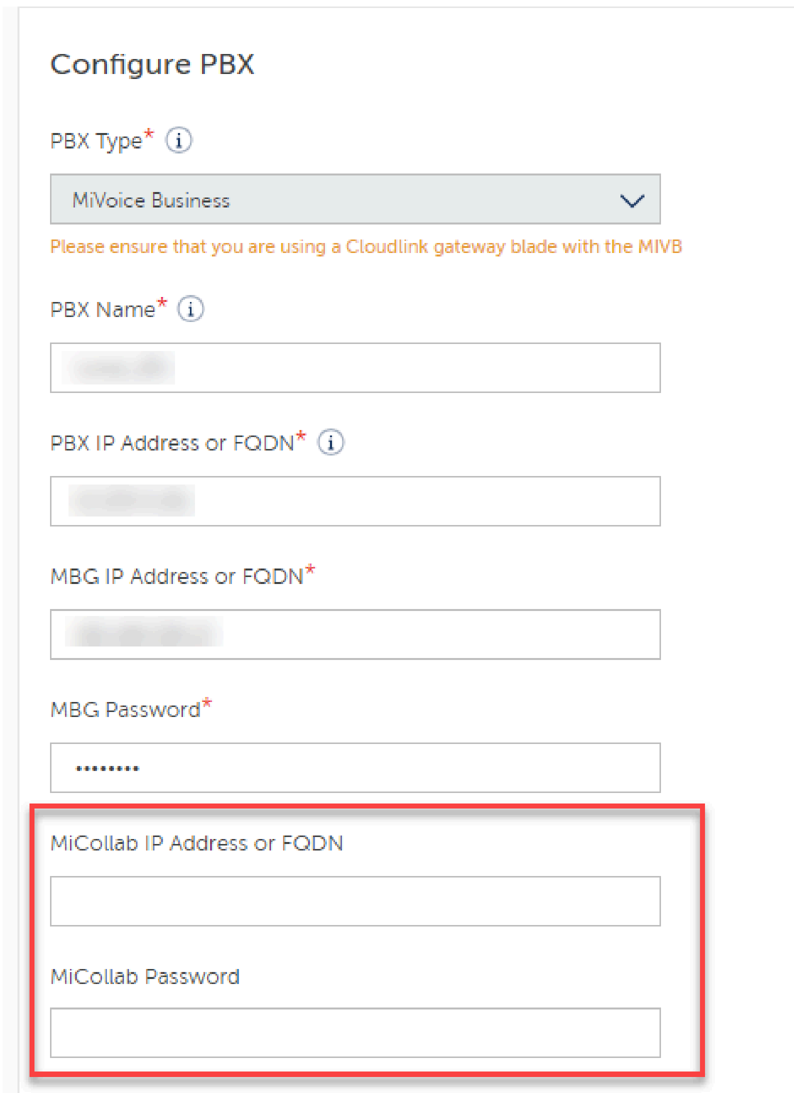
Prerequisites

To configure Microsoft Teams integration with a CloudLink customer account for Bi-directional presence synchronization, you must have:

- Gateway integration enabled for MiVoice Business. See the CloudLink Integration with MiVoice Business Deployment Guide for more details.
- The MiCollab version 9.8 SP1 or above with the Microsoft Teams Integration enabled.

Note:

- When enabling integrations that require MiCollab, such as Microsoft Teams Bi-Directional, it is mandatory to populate the **MiCollab IP Address or FQDN** and **MiCollab Password** in the CloudLink Gateway Configuration.
- The FQDN must resolve to the IP address of MiCollab's LAN interface.



Note:
The Microsoft Teams to CloudLink presence is only supported on MiVoice Business.

Dependencies

To set up the presence integration with Microsoft Teams, administrative-level access is required for the following:

1. Microsoft Azure Active Directory (AD) with Microsoft Office 365 Global admin access
2. Customer or Partner Admin Access to the Customer CloudLink Account

Integrating Microsoft Teams with a Customer Account (new customer)

To integrate Microsoft Teams with a customer account involves two separate procedures:

1. Configuring the feature requirements in Azure (as Azure Administrator) involves:
    a. App registration in Azure portal
    b. Configuring API permissions
    c. Creating Presence Monitor user(s)
2. Configuring the presence feature in Mitel Administration (as CloudLink Administrator)

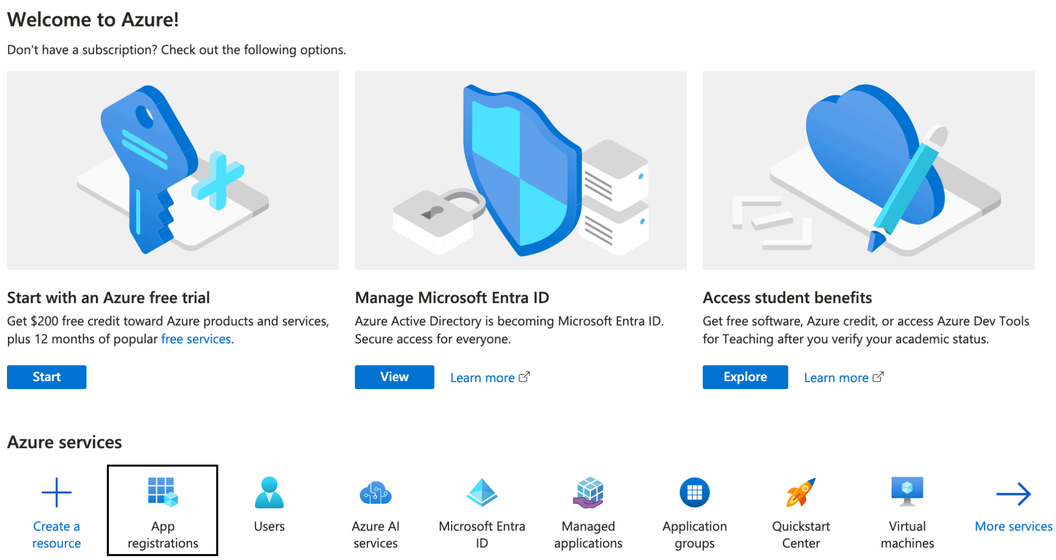
Configuring feature requirements in Azure for new customers

Setting up Azure configuration for a new customer involves several steps, including the registration of a new Azure application, configuration of secrets, defining redirect URIs, specifying API permissions, and the creation of new presence monitor users. The configuration steps for a new customer are outlined below.

App registration in the Azure portal

The registration of the Azure application is carried out to establish the presence synchronization from CloudLink to Microsoft Teams.

1. In the Azure Portal, click **App registrations**.

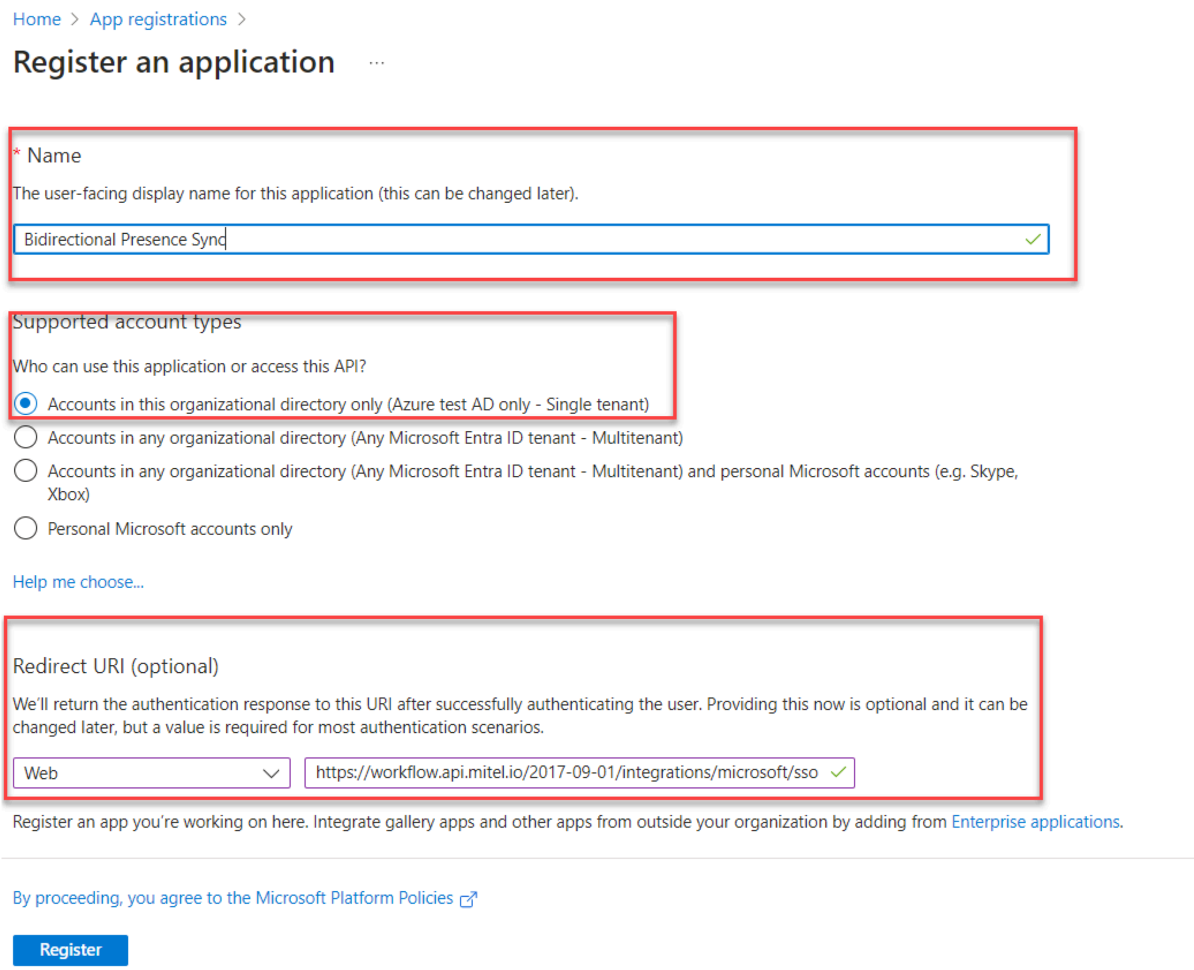


2. In the **App registrations** page, click **+ New Registration**.
3. In the **Register an application** page, enter a desired Name and keep the default **Supported account type**.
4. Under the **Redirect URI (optional)**, select the platform as ***Web*** and create a Web Redirect URI based on the region your account was initially created as mentioned below. For more information, see Redirect URI.

- **US** Cloud https://workflow.us.api.mitel.io/2017-09-01/integrations/microsoft/sso
- **EU** Cloud https://workflow.eu.api.mitel.io/2017-09-01/integrations/microsoft/sso
- **AP** Cloud https://workflow.ap.api.mitel.io/2017-09-01/integrations/microsoft/sso

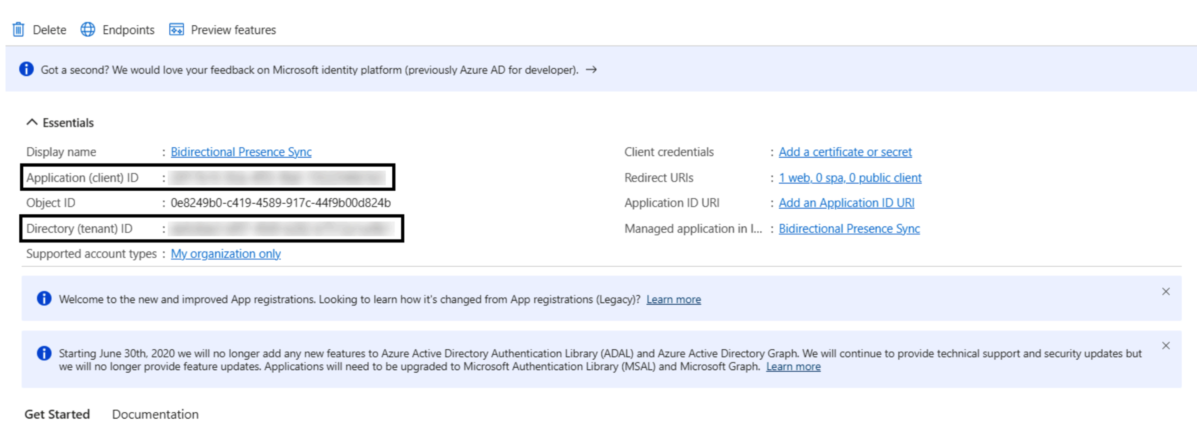
Note:
If you are unsure about your account's Cloud location, refer **Customer Admin Account Information**.

5. Click **Register**



6. The App gets created with the following details:

- Application (client) ID
- Directory (tenant) ID



Configure API permissions

1. After the app registration is complete, navigate to **API permissions** in the left navigation panel and click **+Add a permission**. The **Request API permissions** page is displayed.

   a. From the right pane, select **Microsoft APIs** tab and click **Microsoft Graph**. Select **Application Permissions**.

      The app requires the following permissions for bi-directional sync to work:

Microsoft Graph Permissions	Type	Description
Presence.ReadWriteAll	Application	This is necessary to synchronize presence information from Mitel to MS Teams
User.Read.All	Application	This is required to retrieve the user ID from MS Teams.
Application.ReadAll	Application	This permission is necessary to access and retrieve the permissions and client secret associated with the integration.
email	Delegated	This is required to view user's email address.
offline_access	Delegated	This is required to maintain access to data you have given it access to.
openid	Delegated	This is required to sign users in.
User.Read	Delegated	This is required for get the authorization status of a presence monitor
User.Read.All	Delegated	This is required for presence monitor users to read user ids of MS Teams users, for creating presence subscriptions

Microsoft Graph Permissions	Type	Description
Subscription.ReadAll	Delegated	Allows the app to read all webhook subscriptions on behalf of the signed-in user.
Presence.Read	Delegated	Allows the app to read presence information on behalf of the signed-in user
Presence.ReadWrite	Delegated	Allows the app to read the presence information and write activity and availability on behalf of the signed-in user. Presence information includes activity, availability, status note, calendar out-of-office message, timezone and location.
Presence.Read.All	Delegated	This is required for a presence monitor to read its presence status of all the 650 users.
profile	Delegated	This is required to view user's basic profile.

2. Click **Add Permissions**. For more details on the Application and Delegated Permissions, refer to the Microsoft documentation.

Global administrator consent for API Permissions

1. Navigate to **API permissions** in the left navigation panel.
2. Click on **Grant admin consent for Azure test AD** and click **Yes** in the *Grant admin consent confirmation* notification.

Client Secret

A client secret is an authentication technique that uses a string value in the Azure application. Essentially, it serves as an application password, utilized to authenticate tokens for accessing Azure applications. After successfully verifying the client secret, Azure AD issues a token, granting access to the specified resource.

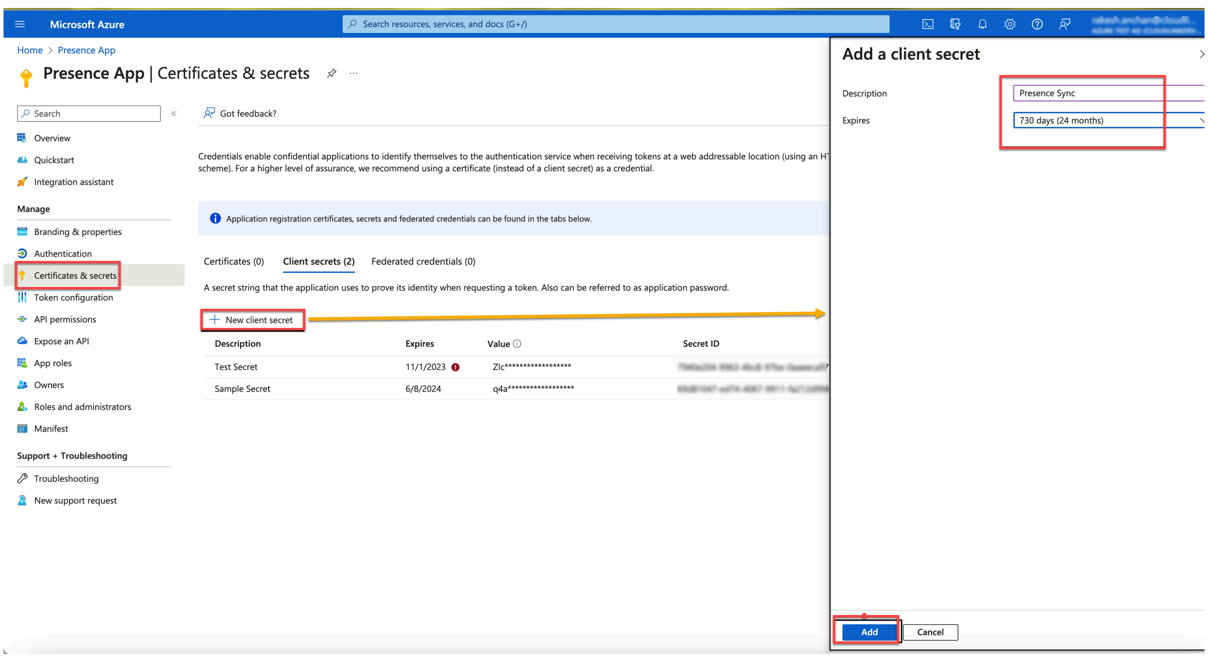
Creating Client Secrets

1. Navigate to **Certificate & secrets** in the left navigation panel and click the Client secrets tab.
2. Click on **+ New client secret**.

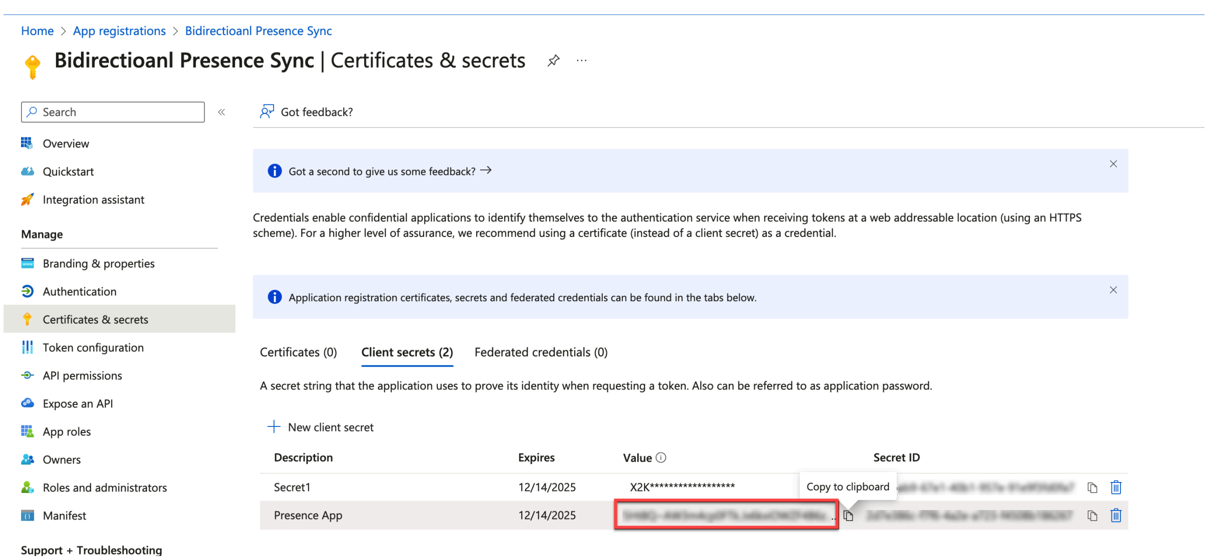
   The **Add a client secret** dialog box is displayed.

> **Note**:
> The client secret **Description** field is used for the **Name** of your integration on CloudLink. This field helps the application determine if the Client Secret is about to or has expired.

3. Enter the **Description** and select the expiry duration. You have the option to choose the expiration duration starting from a specific date to another specific date (with a maximum expiration period of 2 years). Click **Add** to create the Client secrets.



4. Once the client secrets are generated, copy the description of the client secret under the **Description** column and save the secret for account console configuration.



When creating client secrets, it's essential to adhere to best practices and consider key points to ensure the security and proper functioning of your application. Here are some points to remember:

- Create one secret for the MS Teams feature.
- Create individual client secret for each presence monitor. The best practice is to have a separate secure client secret for each monitor.
- It's recommended to enter a meaningful value in the **Description** field to help keep the client secrets organized.

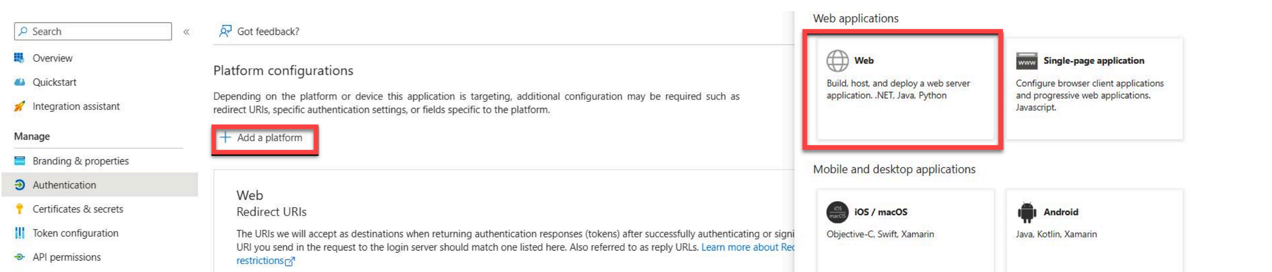
Redirect URIs

A redirect URI is the destination where the authorization server directs the user after the successful authorization of the app, resulting in the issuance of an authorization code or access token.

Adding new redirect URIs to an application

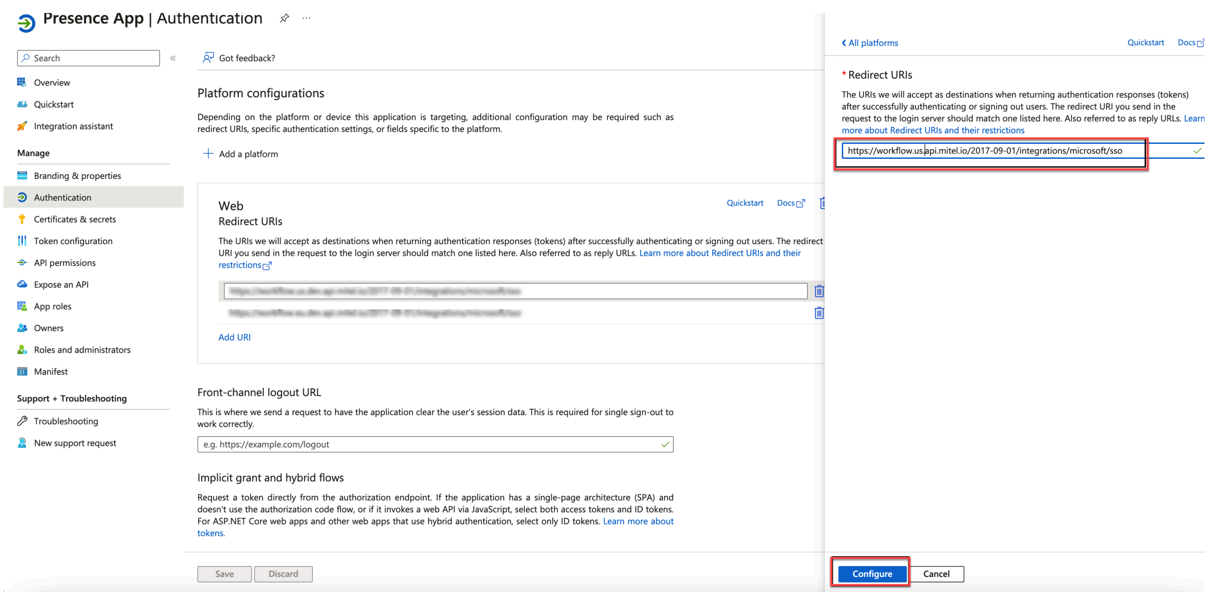
1. Navigate to home page of Azure application.
2. Open the **Redirect URIs** link.

3. Click on **Add a platform** and select **Web**.



4. Under the **Redirect URI (optional)**, select the platform as ***Web*** and create a Web Redirect URI based on the region your account was initially created as mentioned below.

   - **US** Cloud https://workflow.us.api.mitel.io/2017-09-01/integrations/microsoft/sso
   - **EU** Cloud https://workflow.eu.api.mitel.io/2017-09-01/integrations/microsoft/sso
   - **AP** Cloud https://workflow.ap.api.mitel.io/2017-09-01/integrations/microsoft/sso



5. Click **Configure**.

Create Presence Monitor users

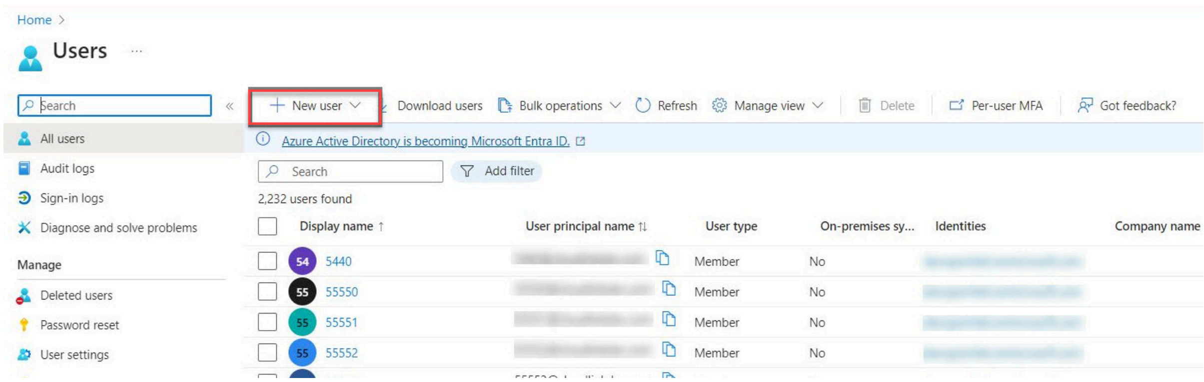
To facilitate the detection of presence changes in the MS Teams applications, Microsoft mandates the creation of a set of presence monitors. Presence Monitors are required for monitoring presence change in MS Teams. The Azure Administrator creates the required number of monitors for presence synchronization, as specified in the Mitel Administration.

Note:
A single presence monitor has the ability to monitor the presence of up to 650 users. Therefore, it is possible that the multiple presence monitors are required.

CAUTION:
Failure to include an adequate number of monitors to accommodate all users will lead to the absence of presence for users exceeding the cumulative limit of all monitors.

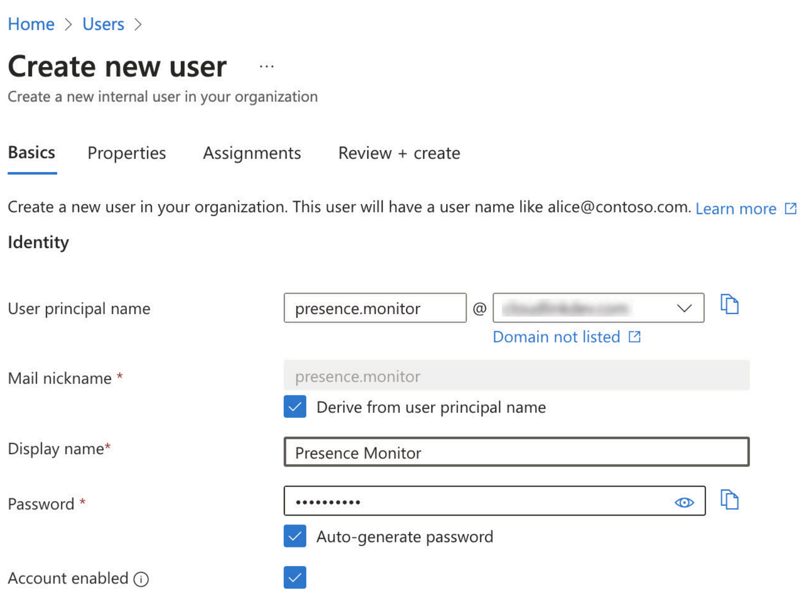
Perform the following steps to create Presence Monitors:

1. In the Azure Portal, navigate to the **Users** page and click on **+ New User**. Select the **Create new user** option.

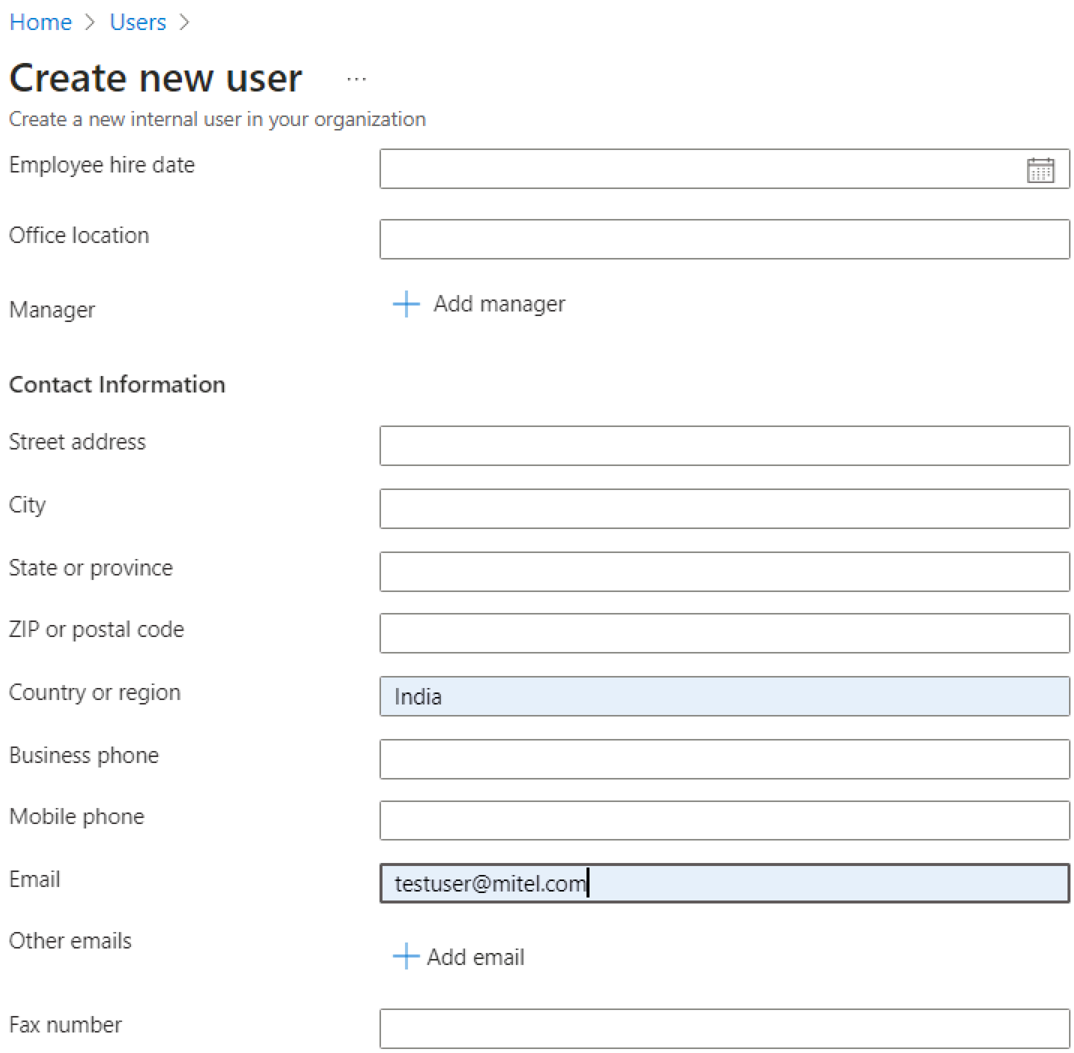


2. In the **Create new user** page, the following field values should be entered under the **Basics** tab:

- User principal name
- Display name
- Password - password can be auto-generated or manually created.
- Account enabled - this option should be enabled, otherwise the user will be blocked from logging in.



3. Next, under the **Properties** tab, set the **Email** of the user.



4. Click on **Review** and **+Create** to create a new user.

A new Presence Monitor User is created.

Note:

- Avoid setting up global administrators as presence monitors. As global administrators possess access to all resources, the workflow may receive unnecessary data that is not essential for its operation.
- Azure Administrator must have a list of users' principal names and client secrets for each created monitor and send them to the CloudLink Administrator. If the CloudLink Administrator authorizes these monitors, the passwords for each monitor must be then sent to CloudLink Administrator.

Integrating Microsoft Teams with a Customer Account (existing customer)

There are two options for the customers with Unidirectional presence sync feature enabled to configure Microsoft Teams:

1. Administrators can delete the existing Azure application, configure presence monitors and create new Azure applications with configuration as mentioned in Bi-directional presence on page 258 .
2. An alternative approach involves the Azure Administrator maintaining the current Azure application configuration outlined in the Unidirectional presence on page 247 section. Additional configuration steps, beyond those specified in the Unidirectional presence section, will be necessary in this scenario as follows:

    a. Create Presence Monitors. Refer to section Create Presence Monitor users on page 267 for the steps.
    b. Add Redirect URI, as outlined in section Redirect URIs on page 266.
    c. Create Client secrets as detailed out in Client Secret on page 264 section.
    d. Add the additional API permissions for the following from the Configure API permissions section:

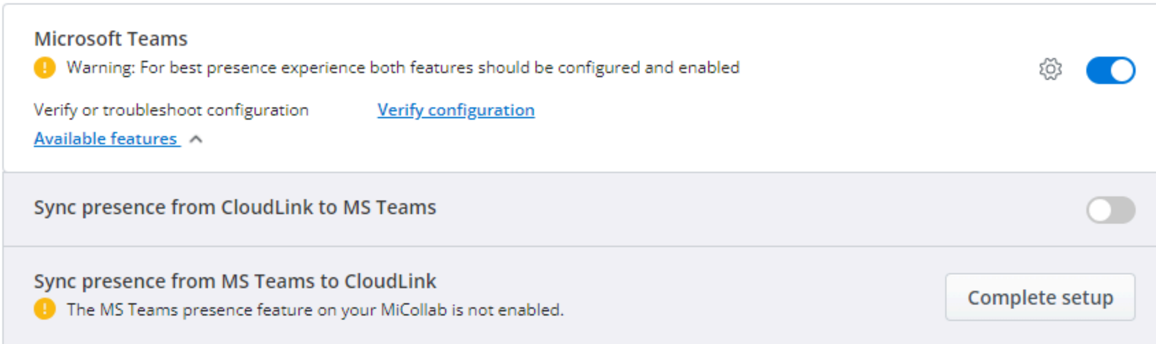
        - User.Read.All
        - Presence.Read.All
        - Presence.Read

Configuring the Bidirectional Presence feature in Mitel Administration (as CloudLink Administrator)

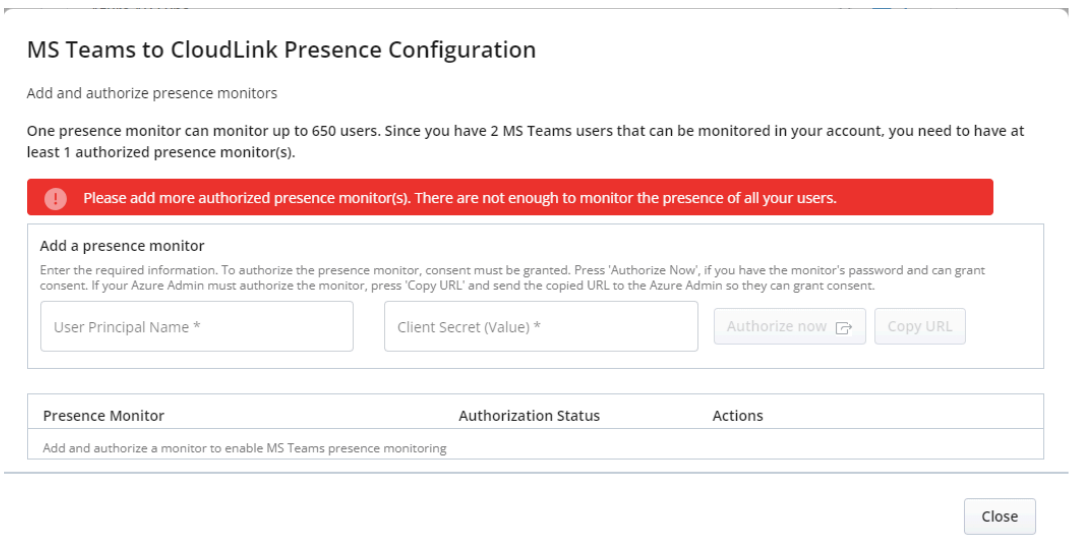
After integrating Microsoft Teams with a customer account, you can enable the Bidirectional Presence feature for the customer account. The synchronization of the Presence feature involves a two-step process. In the first step, the presence synchronization of the presence status of the user takes place from CloudLink to MS Teams which is also called as Unidirectional Presence (refer to the section on Unidirectional presence on page 247 for details), followed by the presence synchronization between MS Teams to CloudLink, which is also known as Bidirectional Presence.

To enable the Sync presence from MS Teams to CloudLink, perform the following steps:

1. In the Mitel Administration, navigate to the **Account** > **Integrations** panel. Under **Microsoft Teams**, slide the toggle button to the right and activate **Sync presence from MS Teams to CloudLink** option.



2. Click **Complete setup**. The **MS Teams to CloudLink Presence Configuration** window opens. If the monitor is not setup, it is highlighted in red in the window.



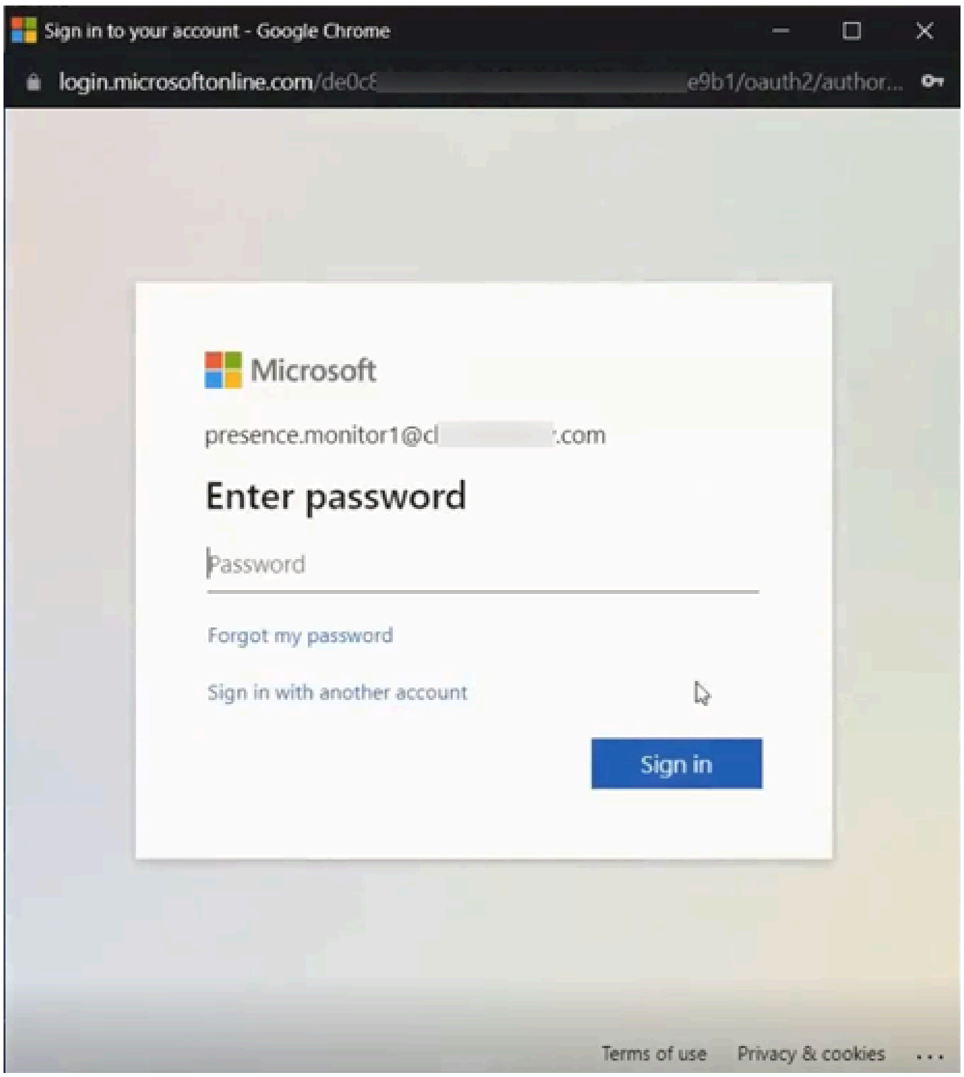
3. To add the Presence monitors that were created in the Azure portal, enter the values in the following fields:

   - **User Principal Name**
   - **Client Secret (Value)** - the value is found in Microsoft Azure Portal > App registrations > Certificate & secrets

4. There are two ways to authorize each monitor that is added: **Authorize now** and **Copy URL**.

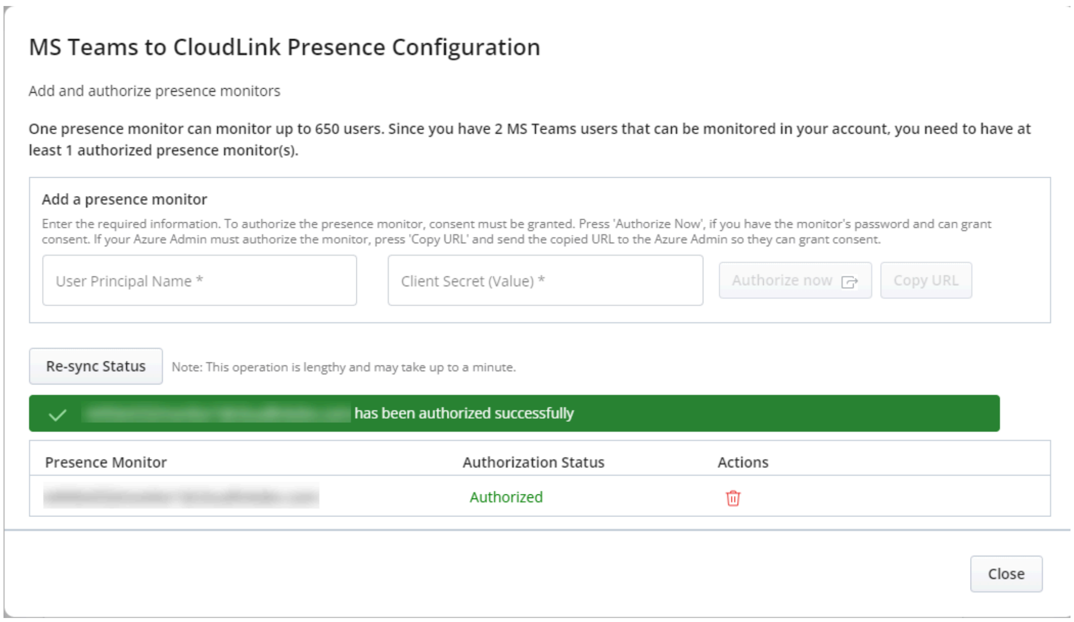
> **Note**:
> The **Authorize now** and **Copy URL** buttons will remain disabled until both the User Principal Name and Client Secret are specified.

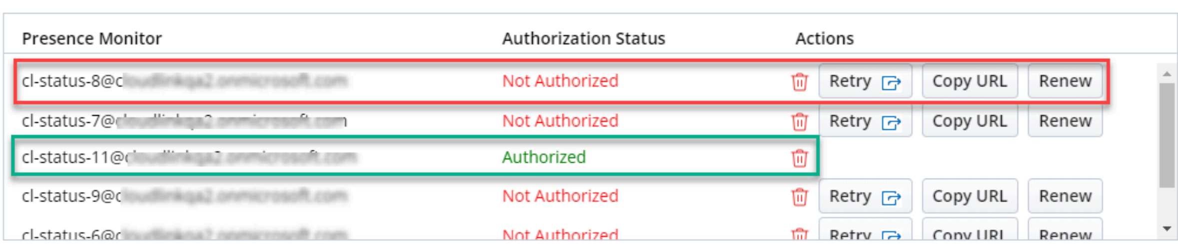
- **Authorize now** - assumes that the CloudLink Administrator (Mitel Administrator) has been provided passwords for each presence monitor. Once **Authorize now** button is clicked, the Mitel Administrator (CloudLink) is asked to provide a **Password** to the CloudLink Administrator for each Monitor entered.



> **Note**:
> If Multi-factor Authentication (MFA) or other security measures are in place, further steps may be required.

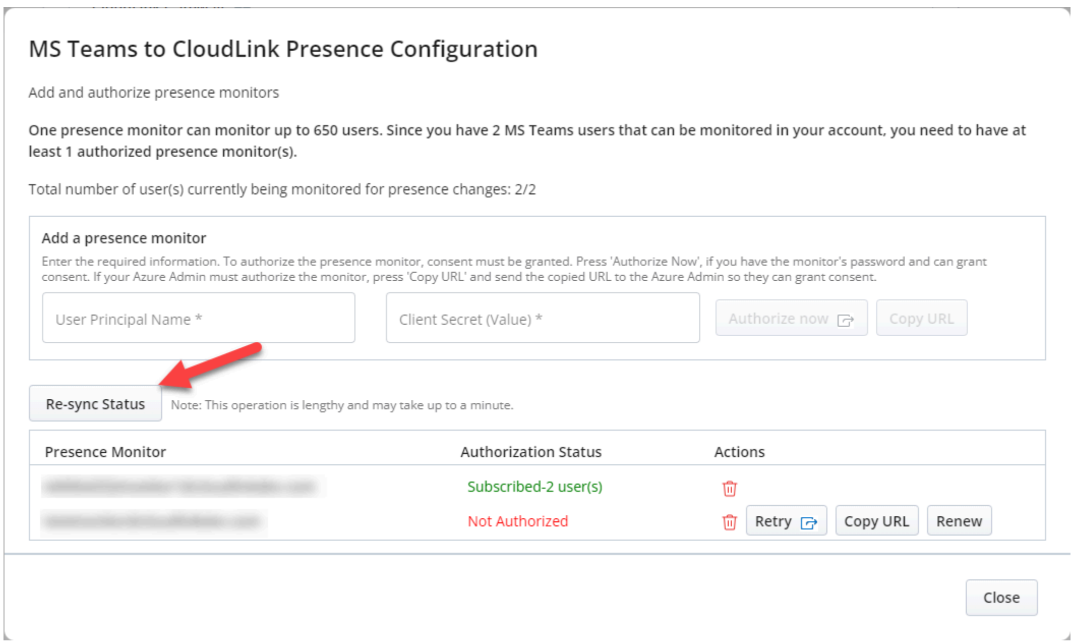
Once the authorization is successful, a notification stating the same appears in the **MS Teams to CloudLink Presence Configuration** window. The added Presence Monitors are displayed in the list below. The Authorization status of each Presence Monitor indicates whether it is authorized or not. The Actions column contains a set of actions that can be performed on a presence monitor, and these actions are dependent upon the monitor's authorization status.





> **Note**:
> The upper section of the dialog provides details on the number of users within the customer account that can be monitored, along with the corresponding information on how many presence monitors need to be created to effectively monitor those users. When the feature is on it also show the number of users subscribed

- **Copy URL** - allows the **Microsoft Azure Administrator** to authorize each presence monitor. If the presence monitor is not authorized, the Administrator has several options: The Mitel Administrator clicks the **Copy URL** button. The copied URL is sent to the Azure Administrator for authorization.
  - Once the authorization from the Azure administrator is completed, click **Re-sync Status**.

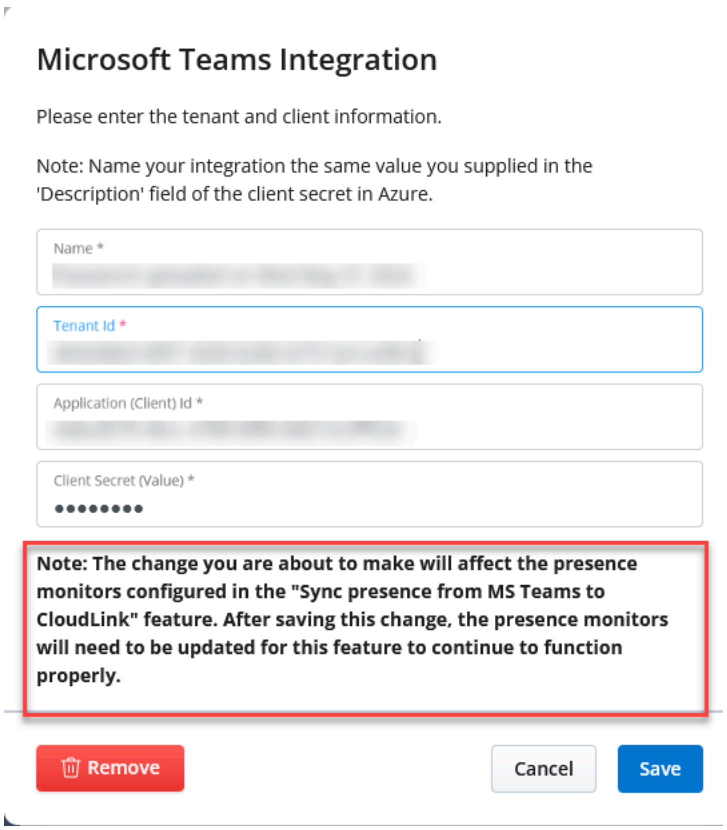


5. Action buttons:
   - Delete button: The administrator can delete the presence monitor by clicking the delete icon.
   - Renew button: If the client secret has expired or needs to be updated, clicking Renew button allows the user to update the client secret.
   - Retry button: When the monitor status shows "Not Authorized", Retry button can be used to invoke the authorization process. **Retry** button has the same functionality as **Authorize Now** button.
6. After all the monitors are added, click **Close** button.

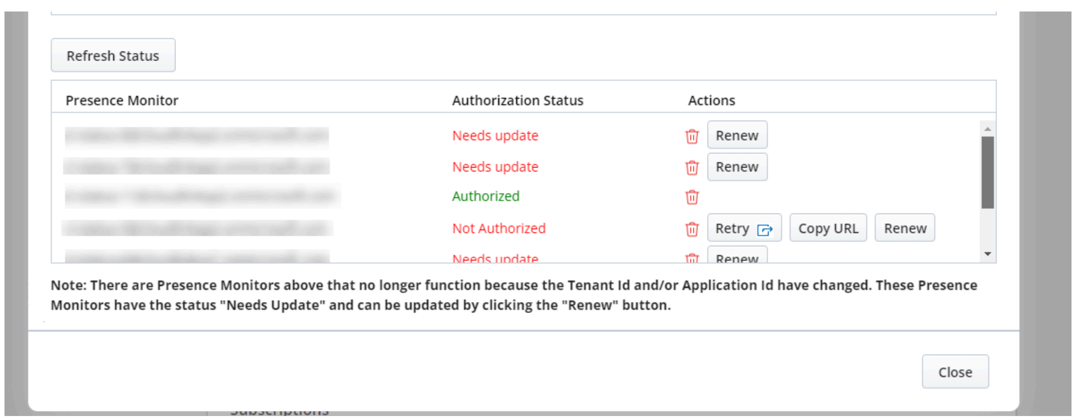
Updating the Microsoft Teams Tenant Id and/or Client Id

If the Microsoft Teams Integration tenant and/or client Id is required to be updated, this will also affect the presence monitors created for the **Sync presence from MS Teams to CloudLink** subfeature. This is due to them sharing the same tenant and client Id. If the tenant and\or client Id is updated, then the monitors subfeature will stop functioning until they are renewed.

1. Edit the Microsoft Teams Integration and change the tenant Id and/or the client Id. If there are existing monitors, the Administrator will be notified of this change.



2. Click **Save**.
3. Go to **MS Teams to CloudLink Presence Configuration** and click **Renew** button for each monitor that shows "Needs update".

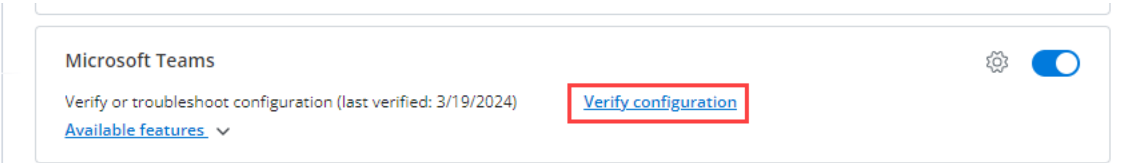


4. Enter the **New client secret**. Click **Authorize now**. This will update the monitor's Tenant Id and Client Id secret.

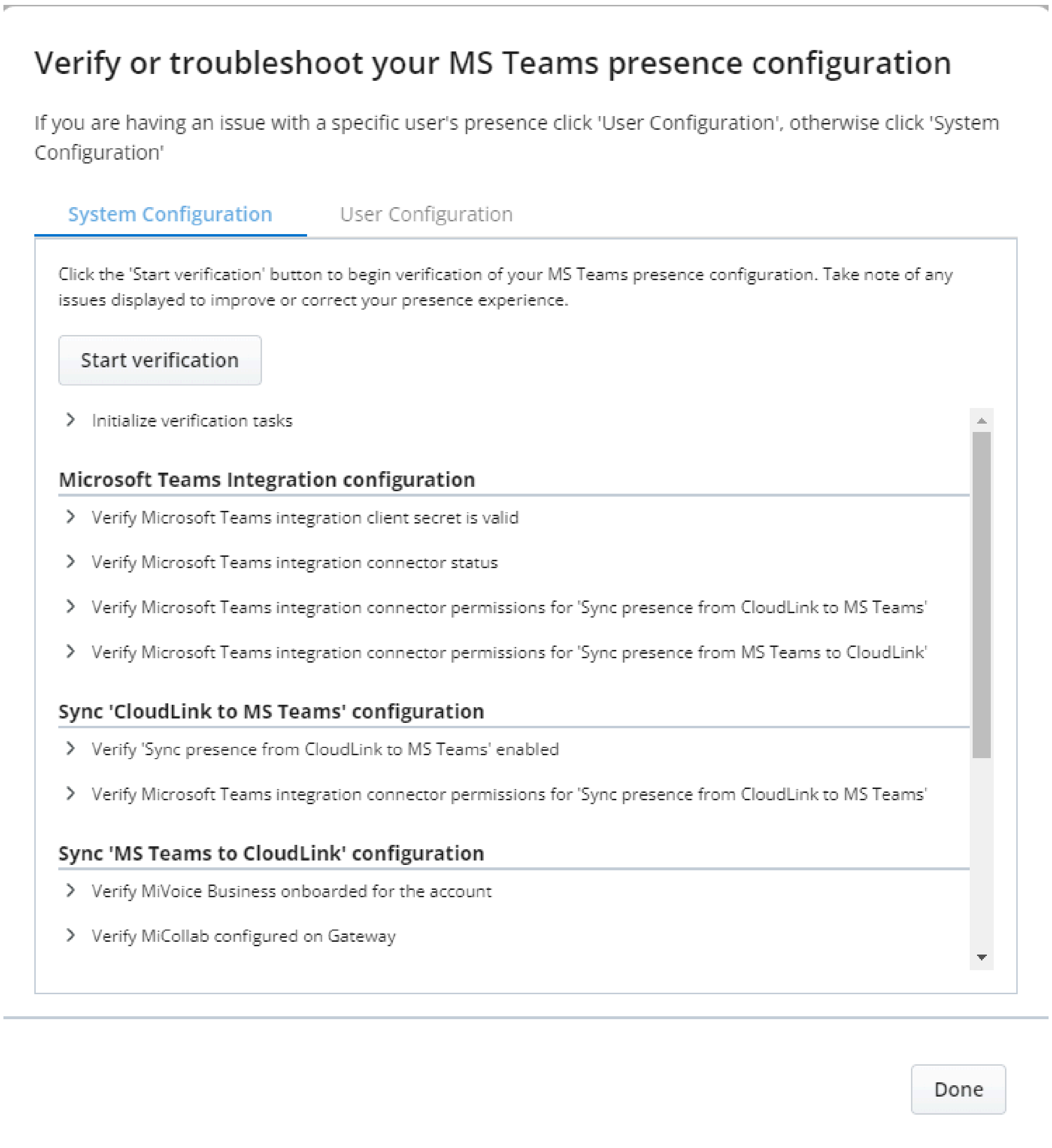
Verifying MS Teams configuration

To verify or troubleshoot the configuration of the MS Teams integration, follow the steps below:

1. In the Mitel Administration, navigate to **Integrations & Apps**. In the **Integrations** panel, click **Verify configuration** associated with **Microsoft Teams**.

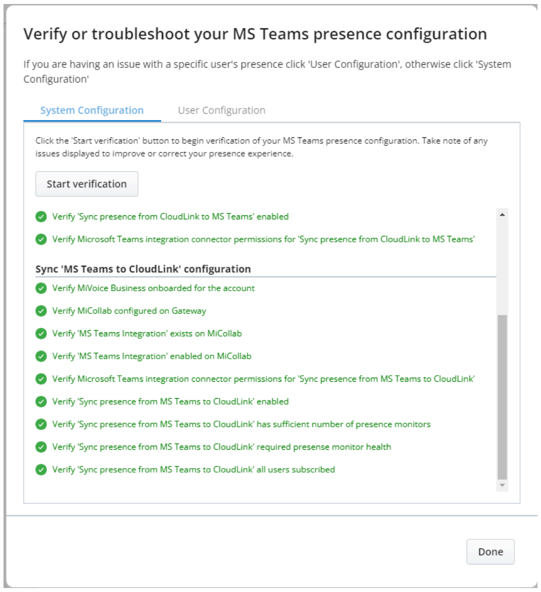


2. "Verify or troubleshoot your MS Teams presence configuration" window is displayed.

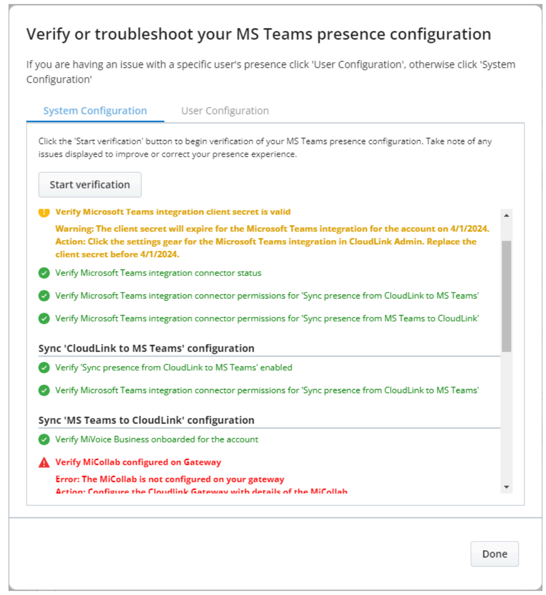


3. Click **Start verification**.

<table>
<tr><th>When all the tests run successfully</th><th>Configuration issues present</th></tr>
<tr><td>



</td><td>



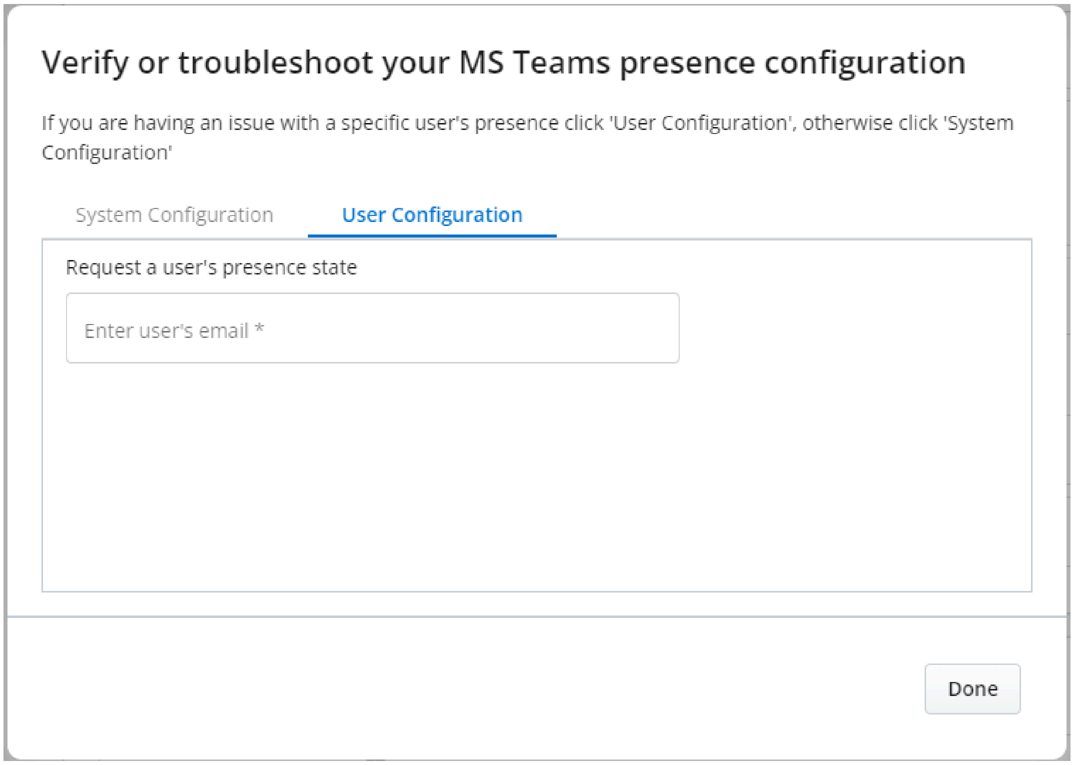
</td></tr>
</table>

For every error encountered, there's a corresponding action to rectify the error(s), click **Start Verification** until all the tests run successfully.

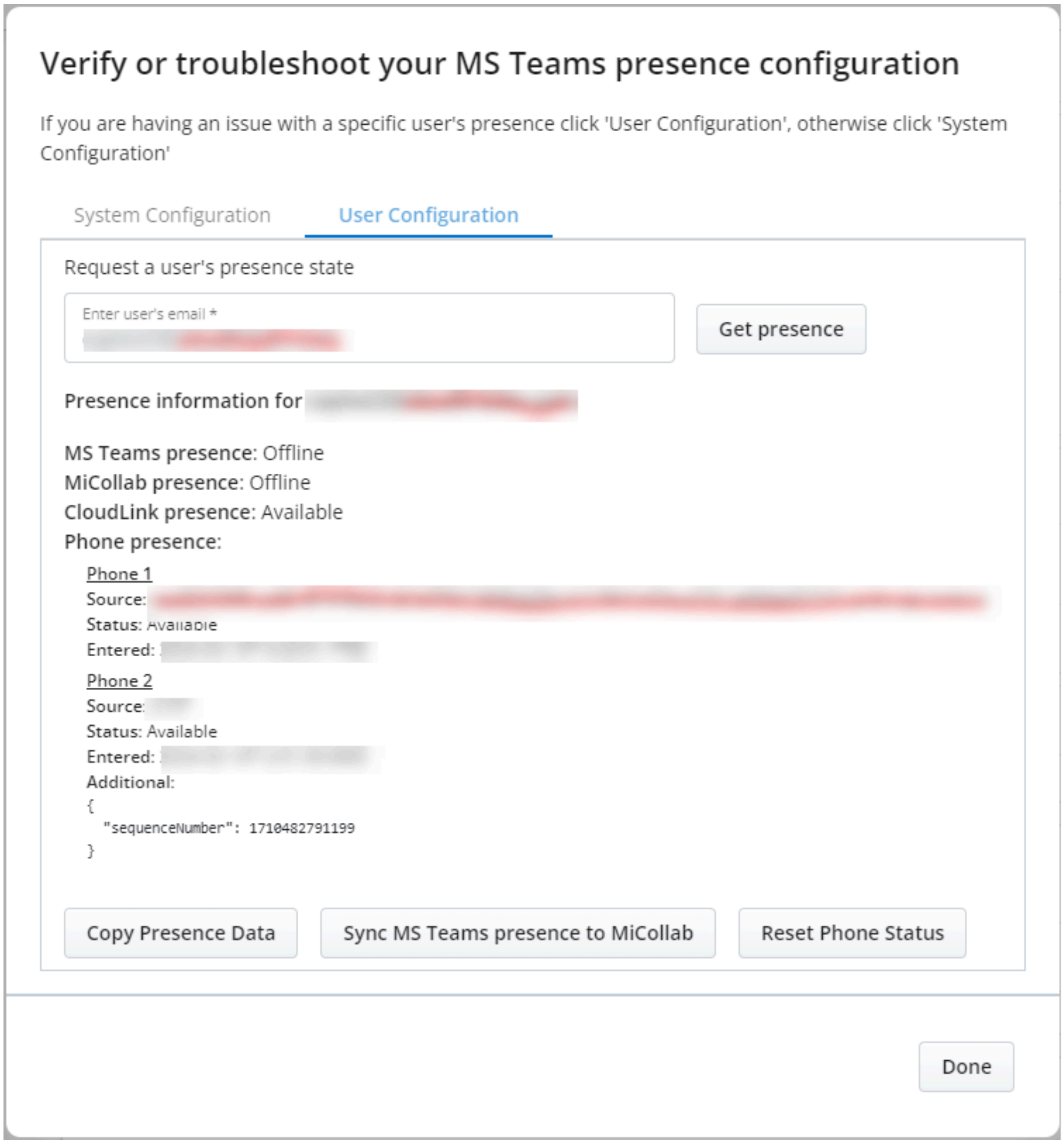
4. **User Configuration** - User Configuration enables the CloudLink Administrator to investigate the issue.

Use Case 1: Issue with a specific user's presence:

a. Select **User Configuration** tab.



b. Request a user's presence state by entering user's email. Once the email is provided, **Get presence** button appears.



c. Click **Copy Presence Data** to copy the data. Report the issue following your standard process.

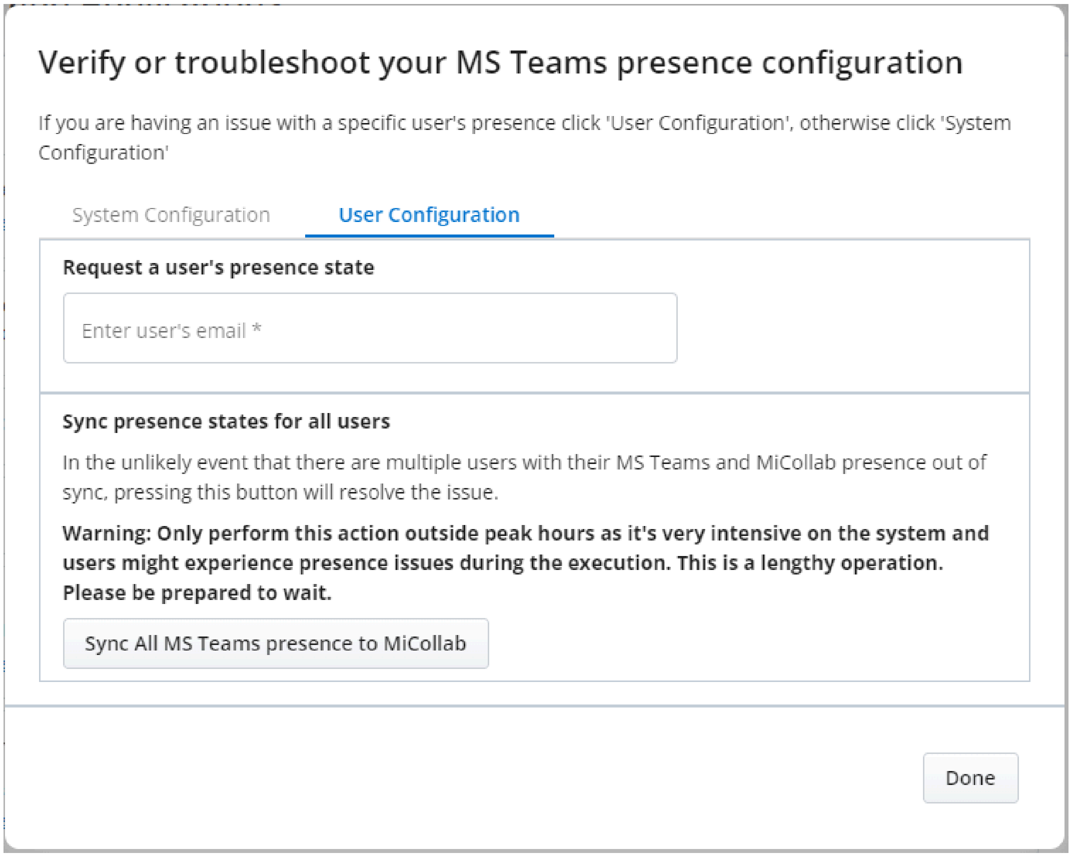
d. Click the **Reset Phone status** and then click **Sync All MS Teams presence to MiCollab**.

e. Click **Done**.

Use Case 2: Multiple number of users out of sync.

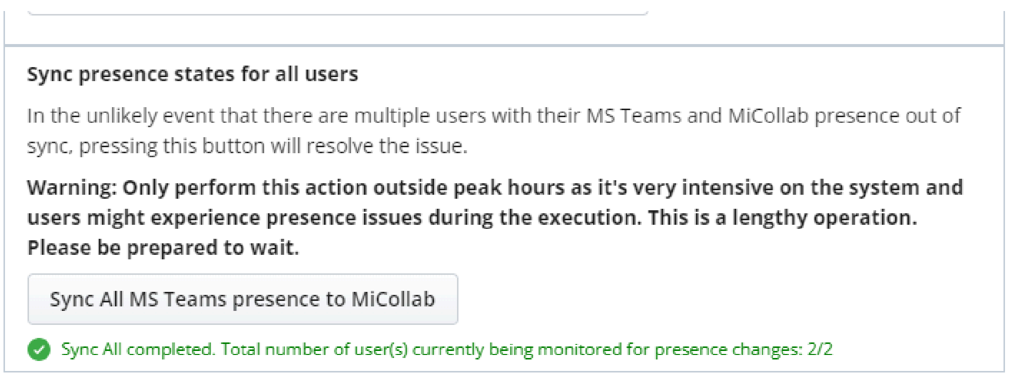
When all the tests run successfully after clicking **Start Verification** in the **System Configuration** tab, the following steps must be performed:

a. Select **User Configuration** tab.



b. Click **Sync All MS Teams Presence to MiCollab**.

"Sync all completed..." message is displayed.



c. Click **Done**