



A MITEL
PRODUCT
GUIDE

MiCollab Solution Document — CloudLink Authentication and Synchronization

Release 10.2

December 2025

Notices

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

Trademarks

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

[®], [™] Trademark of Mitel Networks Corporation

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 CloudLink-based Authentication.....	1
1.1 Prerequisites and Supported Platforms.....	3
1.2 Microsoft Entra ID to CloudLink.....	3
1.3 Setting up a CloudLink Account for Integration.....	4
1.4 Adding a user on Entra ID in Mitel Connect.....	8
1.5 Setting up MiCollab for CloudLink-based authentication.....	11
1.5.1 Enable CloudLink-based Authentication on MiCollab server.....	11
1.5.2 To delete or disable on-prem AD authentication.....	11
1.5.3 To add CloudLink Platform/Entra ID authentication for IDS.....	12
1.5.4 To disable CloudLink-based authentication.....	16
1.5.5 Using CloudLink-based Authentication on the MiCollab Clients.....	17
1.5.6 Manual login for native clients.....	20
2 CloudLink-based Synchronization.....	24
2.1 Prerequisites and Supported Platforms.....	24
2.2 Limitations.....	25
2.3 Setting up CloudLink Account for SCIM integration.....	26
2.4 Setting up the Provisioning Server (Entra ID).....	29
2.5 Setting up Mitel SCIM Enterprise Application.....	29
2.6 Setting up MiCollab for CloudLink-based Synchronization.....	42
2.7 Adding a User with Microsoft Extra Sync.....	43
2.8 Deleting a User with Microsoft Entra ID Sync.....	47
3 CloudLink and CloudLink Daemon updates for MiCollab.....	50
4 Troubleshooting Errors, Alarms and Reports.....	51
4.1 Alarms.....	51
4.2 Errors.....	52
4.3 User Summary Reports.....	52
5 External References and Links.....	53

CloudLink-based Authentication

1

This chapter contains the following sections:

- Prerequisites and Supported Platforms
- Microsoft Entra ID to CloudLink
- Setting up a CloudLink Account for Integration
- Adding a user on Entra ID in Mitel Connect
- Setting up MiCollab for CloudLink-based authentication

With MiCollab Release 9.3, MiCollab has introduced CloudLink (CL)-based Authentication (known as CL Auth) for its end-users (i.e. for the MiCollab Clients).

Customers are provided with a MiCollab Client authentication choice between using MiCollab (i.e. local) or from CloudLink (i.e. CloudLink Authentication). CloudLink can be integrated with an Identity Provider such as Entra ID.. An Identity Provider such as Entra ID provides Single Sign-on capabilities (where users use enterprise credentials to login to Mitel Applications) and safeguards access to data and applications while maintaining simplicity for users.

At the same time, the credentials for CloudLink/Entra ID Authentication on MiCollab Clients can be used to cross-launch CloudLink applications such as MiTeam Meetings, providing a seamless single sign-on experience across Mitel Applications.

 Note: Cross-launching is not supported on mobile clients.

 Note:

While the intent is to allow Identity Providers to provide Single Sign-on capabilities, CloudLink with no integrations to an Identity Provider can also provide CloudLink Authentication. However, the user will be provided with an Email with links to CloudLink to complete the CloudLink authentication process (i.e. setting password). The benefit of having CloudLink Authentication (even without an Identity Provider) is that Single-Sign on Credentials are still provided for CloudLink applications such as MiTeam Meetings.

 Note:

Enabling CloudLink Authentication is a time-consuming activity, and it depends on the number of users for whom the authentication is enabled. This activity should be performed during off-hours. For example, onboarding 500 users, the system will take approximately 60 minutes or so.

Note:

Creating users with CloudLink Authentication being enabled takes a little longer than creating users with CloudLink Authentication being disabled. For example, to onboard 100 users with CloudLink Authentication using UCC Standard Role, the system will take approximately 60 minutes or so.

Note:

AWV doesn't support CloudLink Authenticated users. But to make the AWV desktop client work for CloudLink Authentication enabled user, perform the following:

- Remove any preconfigured user credentials.
- Log in with the name-only option in the client.
- Provide access code to join or use join link provided to join the conference

The CloudLink authenticated users will only be able to join the conference as participants, using the participant access code or participant link provided by the conference owner.

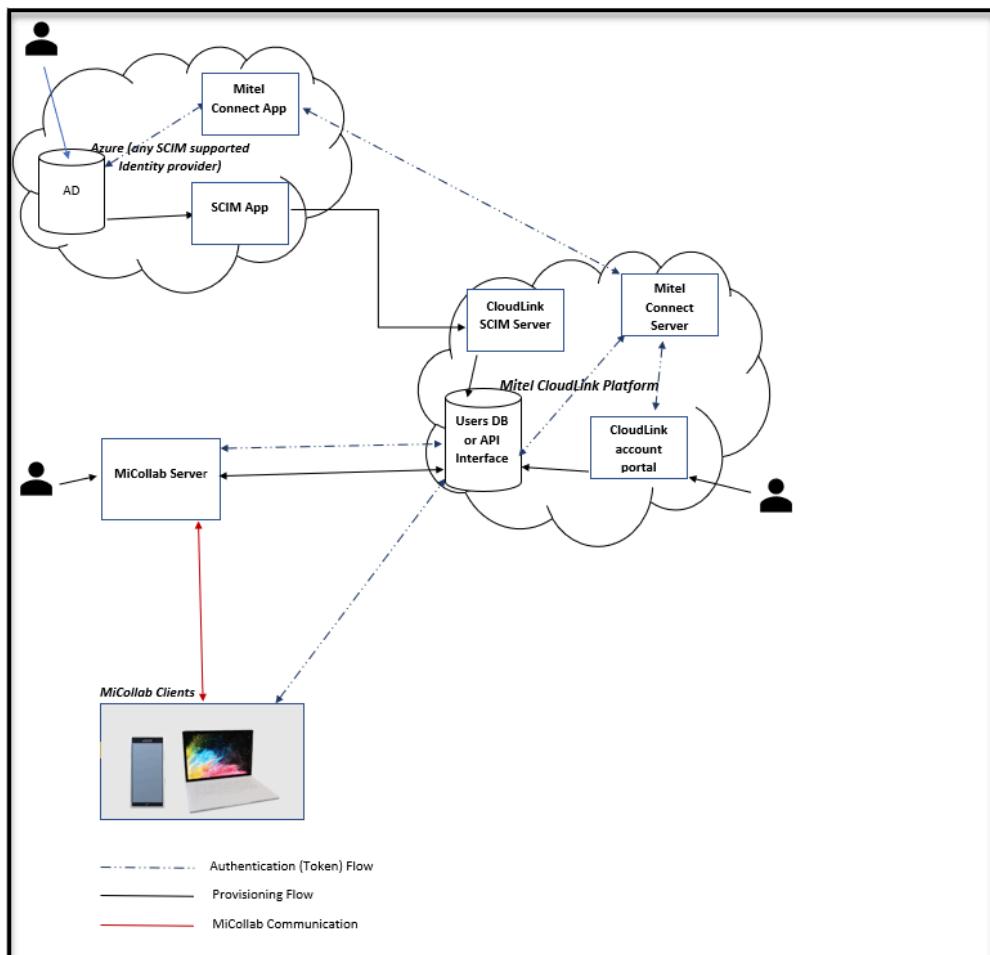


Figure 1: Data Flow Diagram between MiCollab, CloudLink and Entra ID.

1.1 Prerequisites and Supported Platforms

- CloudLink/Entra ID based Authentication is supported on MiCollab Web, PC, Android, iOS, and MAC clients; however, it is not supported on End-user portal, AWV - Outlook portal/desktop client/Web Client, and MiCollab for Microsoft.
- Users who have enabled CloudLink-based Authentication will not be able to use AWV (with leader capabilities) and create AWV conferences through End-User Portal, Outlook plugin, and Ad-hoc AWV meeting, that is, users with CloudLink-based authentication cannot be AWV users. However, these users can still join the AWV meetings as participants.
- Users who have enabled CloudLink-based Authentication can use the Meeting Centre but only to join meetings from other participants or their old meetings (created before they moved to CloudLink-based authentication).
- The CloudLink-based Authentication feature should only be turned on once the CloudLink Integration is done, and the MiCollab Clients are upgraded to Release 9.3 and above loads.
- Administrators have a choice to enable and disable CloudLink/Entra ID based Authentication for a specific set of users.
- MiCollab can only be configured with a single source of authentication - CloudLink or OnPrem-Active Directory. Before moving to CloudLink-based Authentication, they must disable the On-Prem AD authentication if configured already.
- The CloudLink-based Authentication feature is supported with MiVoice Business (on Enterprise and Flex deployments), MiVoice MX-ONE, MiVoice 5000, MiVoice Office 400 platforms.
- MiCollab Web Clients opened on Internet Explorer does not support CloudLink Authentication.
- For CloudLink-based authentication to work, the User Principal Name on Entra ID should be the same as MiCollab user's Primary Email Address.

CL Auth SSO Client authentication using SSO and multi-factor authentication is supported by the following configurations:

- User provisioning via non AD MiCollab integrations
- User provisioning via IDS - AD on-premise MiCollab integrations
- User provisioning via Entra ID CloudLink Sync MiCollab integrations

The following subsections describe the MiCollab Client behaviors and CloudLink/Entra ID/MiCollab server configurations to enable the CloudLink/Entra ID based authentication.

1.2 Microsoft Entra ID to CloudLink

Note: The information contained within this section on CloudLink or Entra ID do not follow MiCollab release cadences and content. The purpose of this section is to provide information on the basics of integrating CloudLink with Microsoft Entra ID

Configuring the CloudLink Platform with Microsoft Entra ID allows users for your customer account to access CloudLink applications such as MiTeam Meetings using their enterprise credentials (i.e. Entra ID credentials: Email and password).

To proceed with this section, you must have the following:

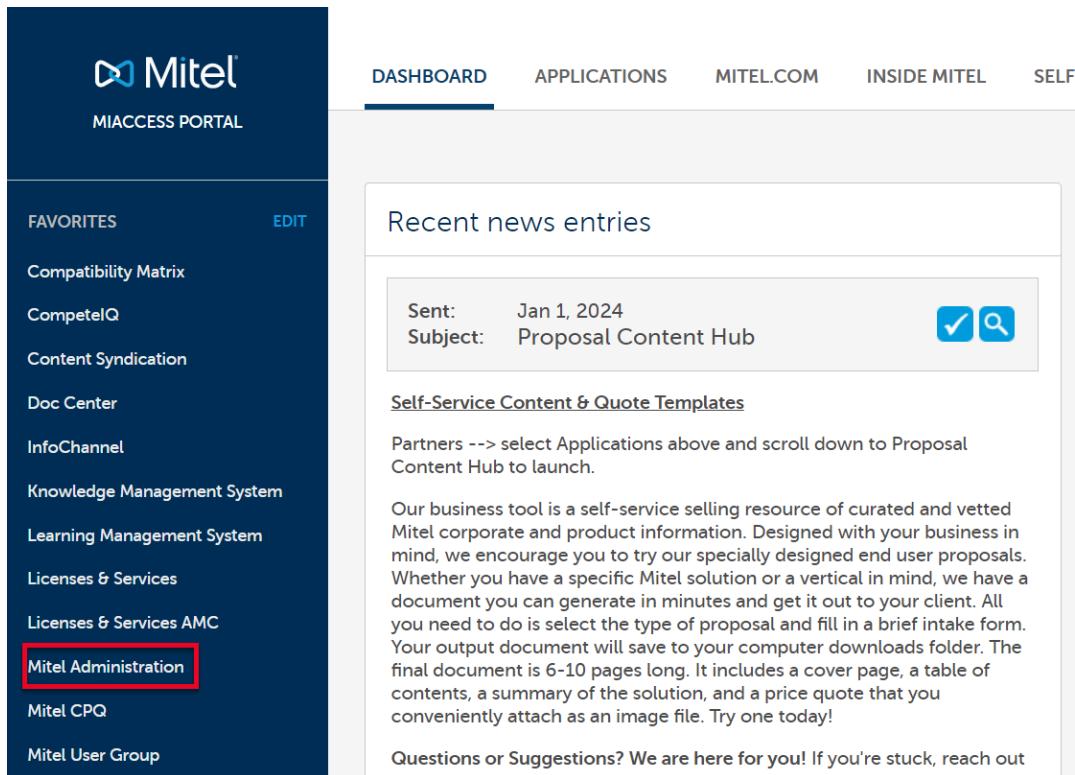
- An Entra ID subscription
- A Mitel CloudLink account

i **Note:** Entra ID authentication (formerly known as Azure Active Directory or Azure AD) is not supported in the native application browser on Windows 10 clients. As a result, with CloudLink-based authentication configured to use Entra ID and Conditional Access, the Windows 10 client will now launch the authentication process through an external browser instead of relying on the native application browser. This change will ensure a smoother and more secure authentication experience.

1.3 Setting up a CloudLink Account for Integration

Some of these steps are consistent with steps to enable CloudLink based Chat or MiTeam Meetings. However, for completeness, all steps will be included.

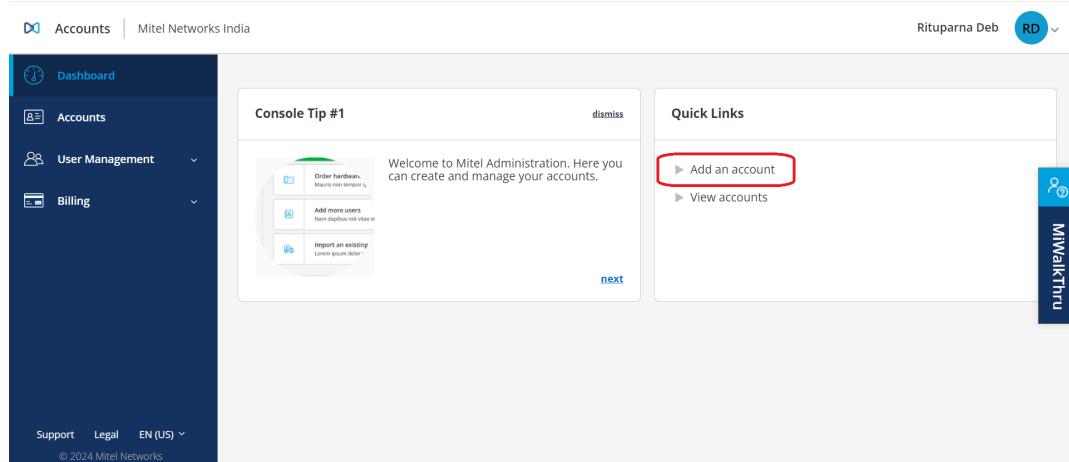
1. Log in to the MiAccess portal using your MiAccess credentials.
2. On the left tab, select **Mitel Administration**.



The screenshot shows the MiAccess Portal dashboard. The top navigation bar includes links for DASHBOARD, APPLICATIONS, MITEL.COM, INSIDE MITEL, and SELF. The left sidebar, titled 'FAVORITES' and 'EDIT', lists various links: Compatibility Matrix, CompetelQ, Content Syndication, Doc Center, InfoChannel, Knowledge Management System, Learning Management System, Licenses & Services, Licenses & Services AMC, Mitel Administration (which is highlighted with a red box), Mitel CPQ, and Mitel User Group. The main content area displays 'Recent news entries' with a card showing 'Sent: Jan 1, 2024' and 'Subject: Proposal Content Hub'. Below this is a section titled 'Self-Service Content & Quote Templates' with a description of the tool's purpose and a note about selecting applications and using the Proposal Content Hub. At the bottom, there is a 'Questions or Suggestions?' section.

3. Partner can log in to the CloudLink account portal and select the **Add an account** link (i.e. customer account).

If the customer account already exists, you can skip this step, search for the customer account under Accounts and proceed to step 4.



4. Fill in the required details under Account Information.

- Customer Name
- Country
- Province/State
- Address
- City
- Postal/Zip Code
- Default Language
- Business Type
- Support Contact

Customer Name *	CLDesignIntegration	Account ID	1589774499
Country *	Canada	Default Language	English
Province / State *	Ontario	Business Type	Other
Address *	628 Vivera Place	SAP Customer Number	Not Available
Address 2		Cloud location	Europe (Frankfurt)
City / Town *	Ottawa	Postal / Zip Code *	K2S 2M9
Support contacts			

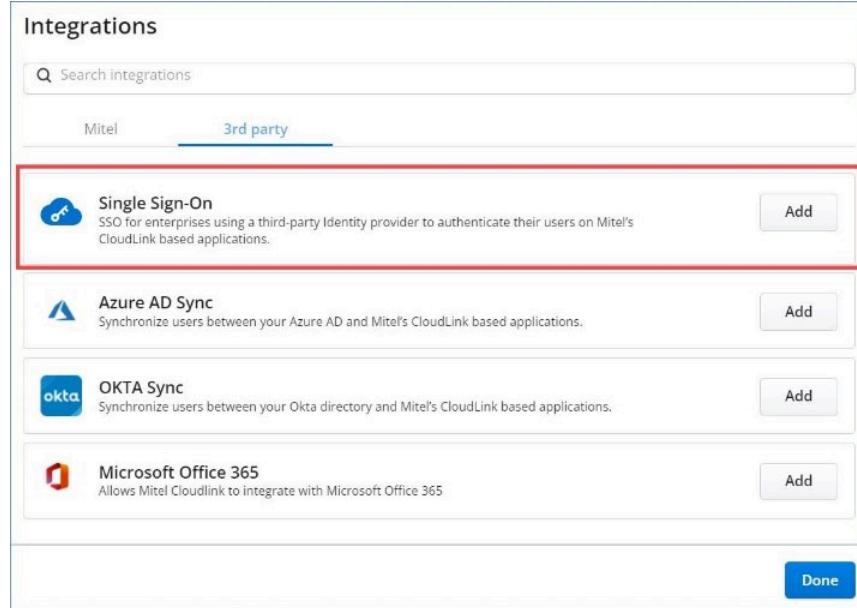
5. In the Integrations section, click **+ Add new**.

A pop-up screen displays the Integrations panel.



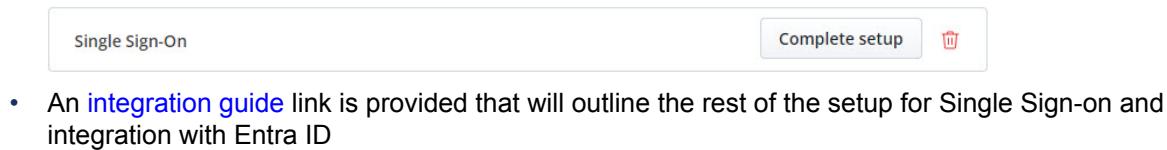
6. Integrations will include **Mitel** and **3rd Party**. Click the **3rd party** tab.

- Mitel Integrations include (not discussed here): MiCollab, MiTeam Meetings, and MiCC.
- 3rd Party Integrations will include **Single Sign-On** as shown below:
 - 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.

- At this point, the Single Sign-On procedure is not complete. Click the **Complete Setup** button.



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...>

Reply URL Assertion Consumer Service URL
<https://authentication.us.dev.api.mitel.io/2017-09-01/sa...>

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.

This completes the steps necessary to integrate the CloudLink Account with the customer Entra ID

For new customer sites, the CloudLink Account must now be integrated with MiCollab. The steps required are identical to setting up the CloudLink based chat on MiCollab. See the [MiCollab Solution Document-CloudLink](#) for steps to Enable CloudLink Integration.

1.4 Adding a user on Entra ID in Mitel Connect

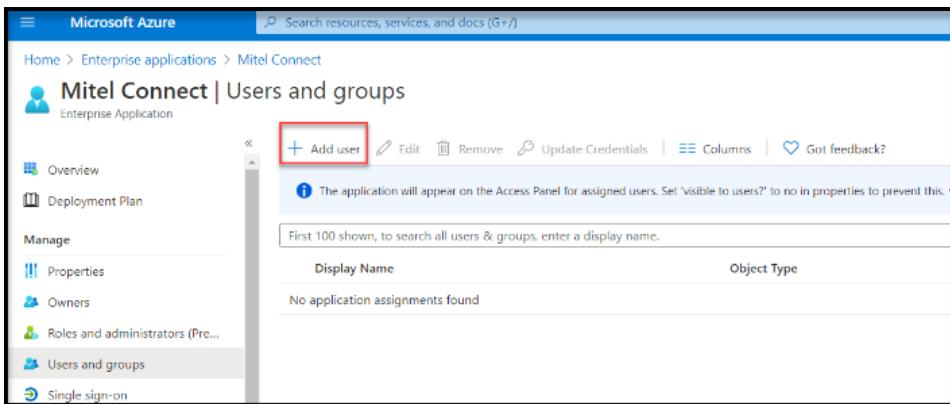
There are multiple ways to add users in Entra ID through UI, CSV import, PowerShell, etc. The user creation in Entra ID is not considered and described in this document. Please refer <https://portal.azure.com/> for details. This section only describes adding a user in the Entra ID Mitel Connect app once the user is created in Entra ID

1. Search for Enterprise Applications on Entra ID and select **Mitel Connect** application.

Name	Homepage URL	Object ID	Application ID
Mitel Connect	http://www.mitel.com	a3ffafe7-cbf6-41fb-9286-83b4f627262b	6ed7bbef-e0cf-46b5-9f29-f6de288bb786
scim		325447db-615b-4fb6-a7ad-2fc102e9348a	a0737309-d1aa-470d-acf1-79a008f1c409
SCIM		3bb4033a-49b7-480b-9b67-c950a5353fb4	1226ace4-b6ee-4414-a23c-7bae984aed46
SCIM App		ca62a315-1084-4760-b5eb-d5feba414879	15a013d9-52b5-4d4f-8284-89e6b4a0a2e0

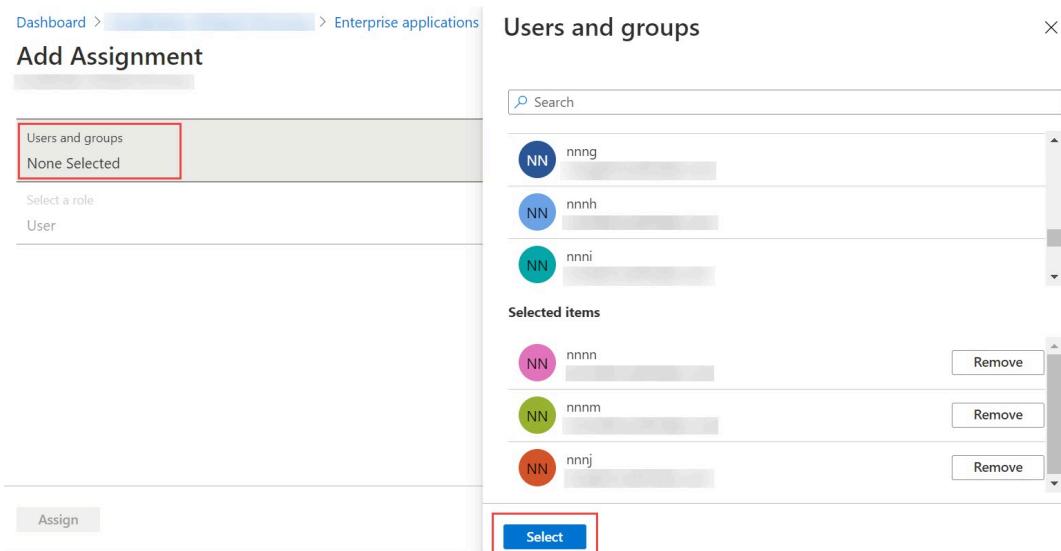
2. After clicking Mitel Connect, click **Assign user and group**.

3. Click Add user.



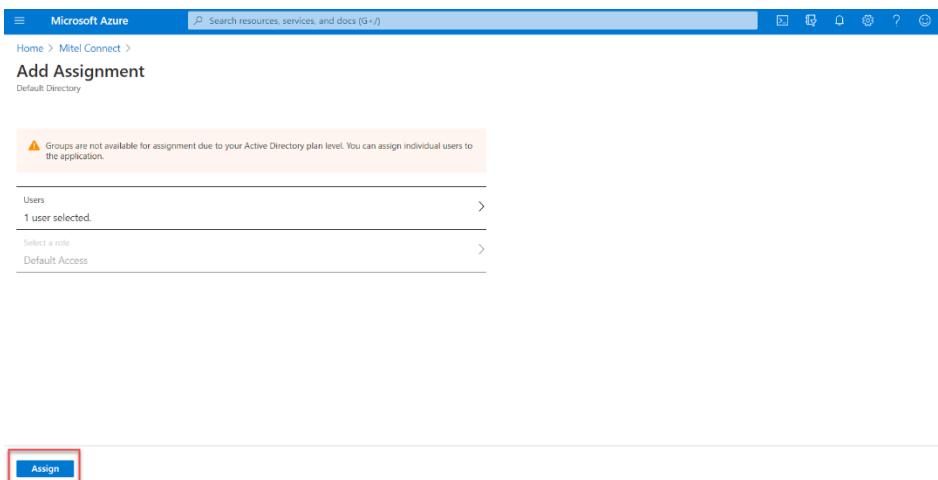
The screenshot shows the 'Mitel Connect | Users and groups' page in Microsoft Azure. The left sidebar has 'Overview', 'Deployment Plan', 'Manage', 'Properties', 'Owners', 'Roles and administrators (Pre...)', 'Users and groups' (which is selected and highlighted in grey), and 'Single sign-on'. The main area has a '+ Add user' button highlighted with a red box. Below it is a note: 'The application will appear on the Access Panel for assigned users. Set "visible to users?" to no in properties to prevent this.' A search bar says 'First 100 shown, to search all users & groups, enter a display name.' and a table with 'Display Name' and 'Object Type' columns shows 'No application assignments found'.

4. Search for the user and click to Select the user.



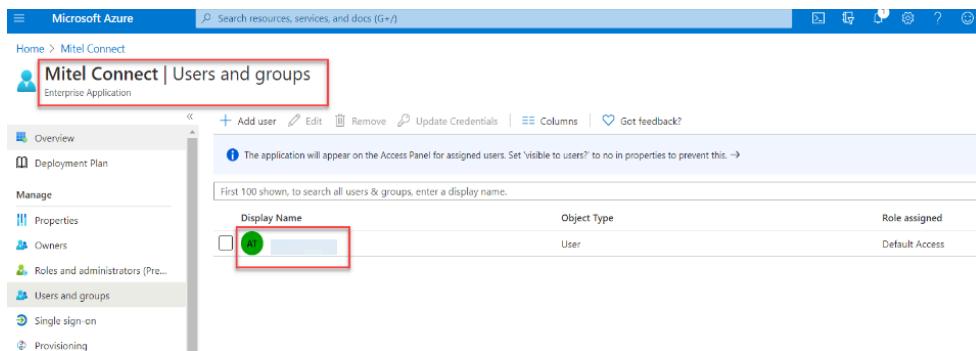
The screenshot shows the 'Add Assignment' page. On the left, under 'Users and groups', a 'None Selected' button is highlighted with a red box. Below it are 'Select a role' and 'User' buttons. On the right, a 'Users and groups' search interface shows a list of users (nnng, nnnh, nnni) and a 'Selected items' list with three users (nnnn, nnnm, nnnj), each with a 'Remove' button. A 'Select' button is highlighted with a red box at the bottom of the selected items list.

5. Once the user is selected, click on Assign.



The screenshot shows the 'Add Assignment' page. A message at the top says 'Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.' Below it, under 'Users', '1 user selected.' is shown. Under 'Select a role', 'Default Access' is selected. At the bottom, a 'Assign' button is highlighted with a red box.

6. The user should list under the Enterprise Application – Mitel Connect.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. Below the navigation is a breadcrumb trail: 'Home > Mitel Connect'. The main content area is titled 'Mitel Connect | Users and groups' and is described as an 'Enterprise Application'. On the left, a sidebar lists several options: Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators (Pre-), Users and groups (which is selected and highlighted in blue), Single sign-on, and Provisioning. The main table displays user information with columns: Display Name, Object Type, and Role assigned. A single user entry is shown: 'Mitel Connect' (Object Type: User, Role assigned: Default Access). A red box highlights the 'Display Name' column for this entry.

7. All users listed under the Enterprise Application - Mitel Connect should appear on CloudLink account portal. Before troubleshooting MiCollab, ensure that users from Entra ID within the Enterprise Application – Mitel Connect are shown on CloudLink for the customer Account.

Note:

For CloudLink-based Authentication to work, the User Principal Name on Entra ID should be the same as the MiCollab user's Primary Email Address.

1.5 Setting up MiCollab for CloudLink-based authentication

1.5.1 Enable CloudLink-based Authentication on MiCollab server

Note:

If you have an On-Prem AD connection currently being used for user authentication, you must disable the authentication first as only one source of authentication is allowed. If On-Prem AD connection is used only for user authentication and not for synchronization, you may proceed for deletion. Refer below steps for deletion.

1.5.2 To delete or disable on-prem AD authentication

1. In the MiCollab Server, under **Configuration**, click **Integrated Directory Service**.
2. In the Actions column for the desired domain, click **Remove**.
3. Click **Remove**.
4. If Authentication was enabled, you will be prompted to enter a temporary end-user login password. Enter a temporary password, confirm the password, and then click **Save**. The system automatically

sends the users a Service (Welcome) Email with the temporary password and deployment Email with the QR code.

Note:

To prevent the system from sending a Welcome Email with a temporary password and a deployment Email, the administrator must disable the welcome Email before Step 1 and should enable it after Step 4 is completed.

1.5.3 To add CloudLink Platform/Entra ID authentication for IDS

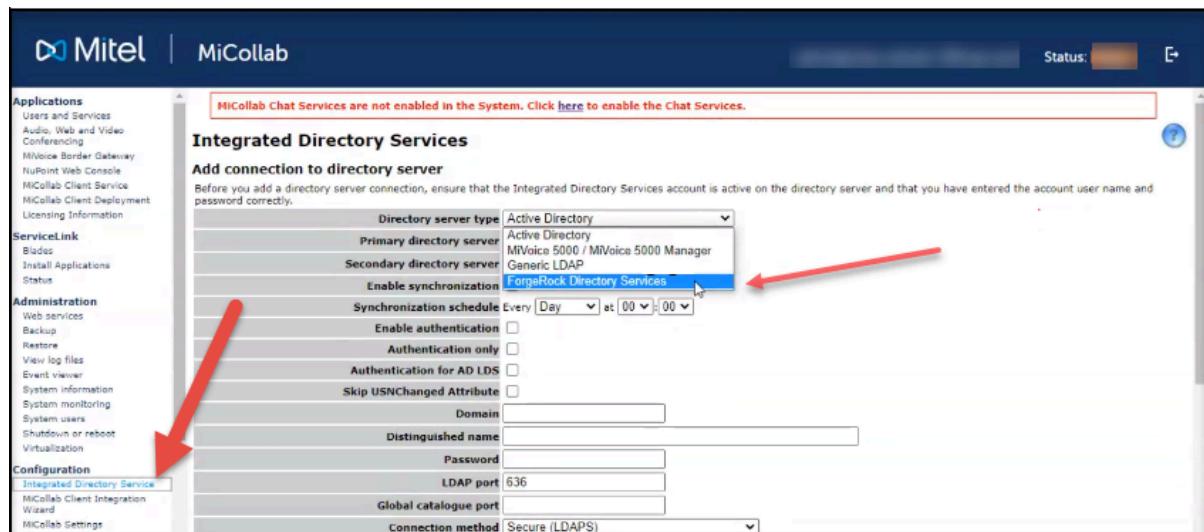
Limitations:

The following features are not supported with CloudLink IDS:

- External Search
- External Reverse Lookup
- Search Context, i.e. OU based search
- Query String

Prior to the enabling of CloudLink-based Integration on MiCollab you will notice that there are only four Directory Server types under Integrated Directory Services:

- Active Directory
- MiVoice 5000 / MiVoice 5000 Manager
- Generic LDAP
- ForgeRock Directory Services

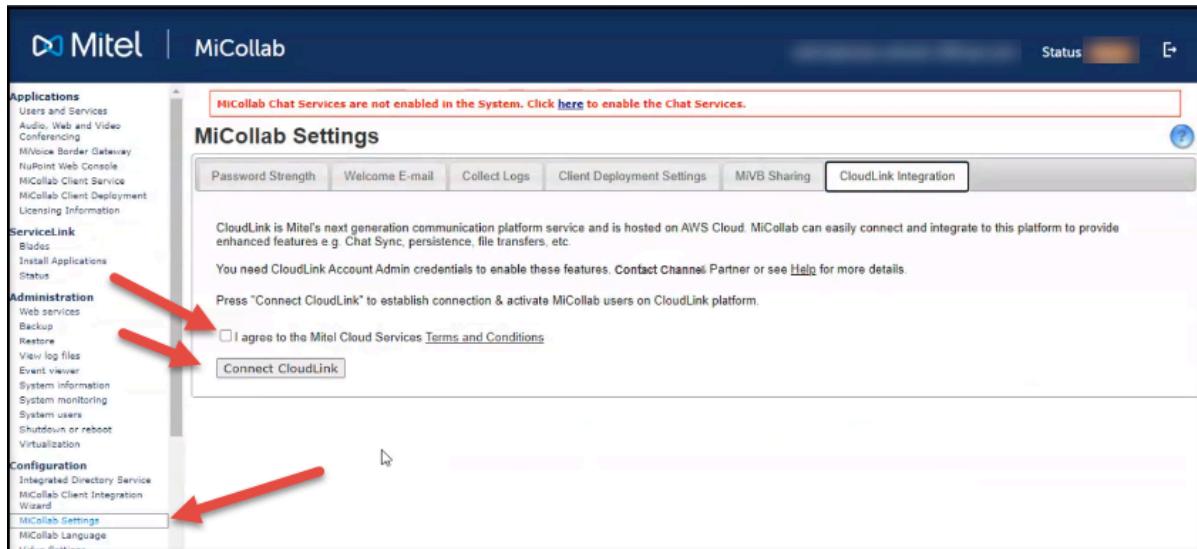


CloudLink-based Authentication

If CloudLink Integration is enabled, CloudLink Platform will be shown under available Directory Server Types. Refer from step 6 onwards for further configuration.

If CloudLink Integration is not enabled, then the following steps will be required to enable CloudLink on MiCollab.

1. From Configuration > MiCollab Settings proceed to the **CloudLink Integration** tab.
2. Check the box **I agree to the Mitel Cloud Services Terms and Conditions** and then click the **Connect CloudLink** button.



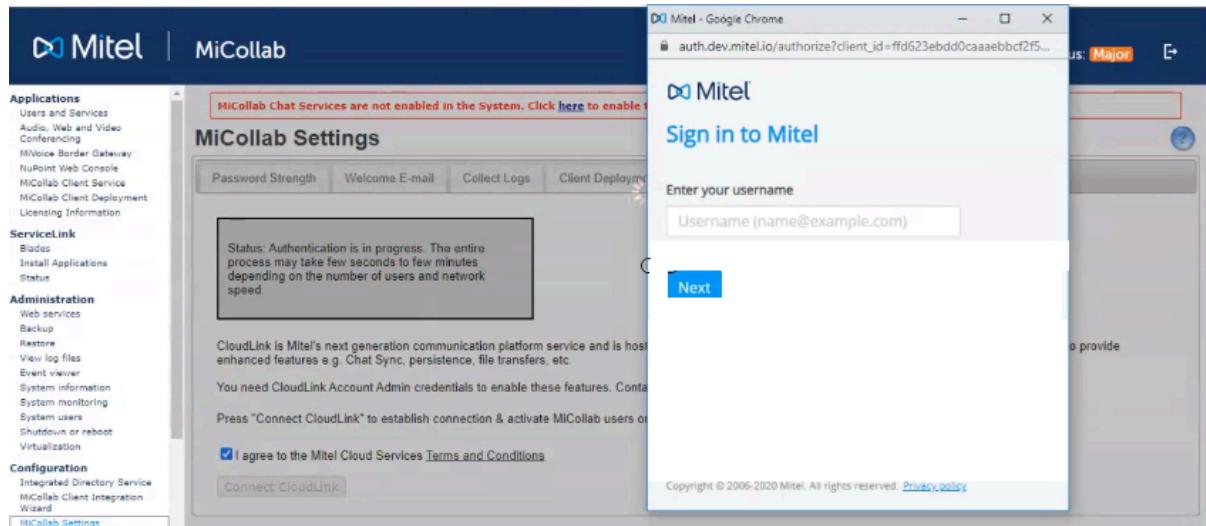
3. MiCollab will indicate: **You are being directed to Mitel Auth Portal for additional authentication. Make sure your web browser pop-up blocker is disabled. Do you want to proceed?**

Click **OK** to proceed.

4. As a Mitel Administration user administrator you will be asked by CloudLink to:

Note:

It is assumed that CloudLink has already been setup to include a user (administrator) and an account (customer).



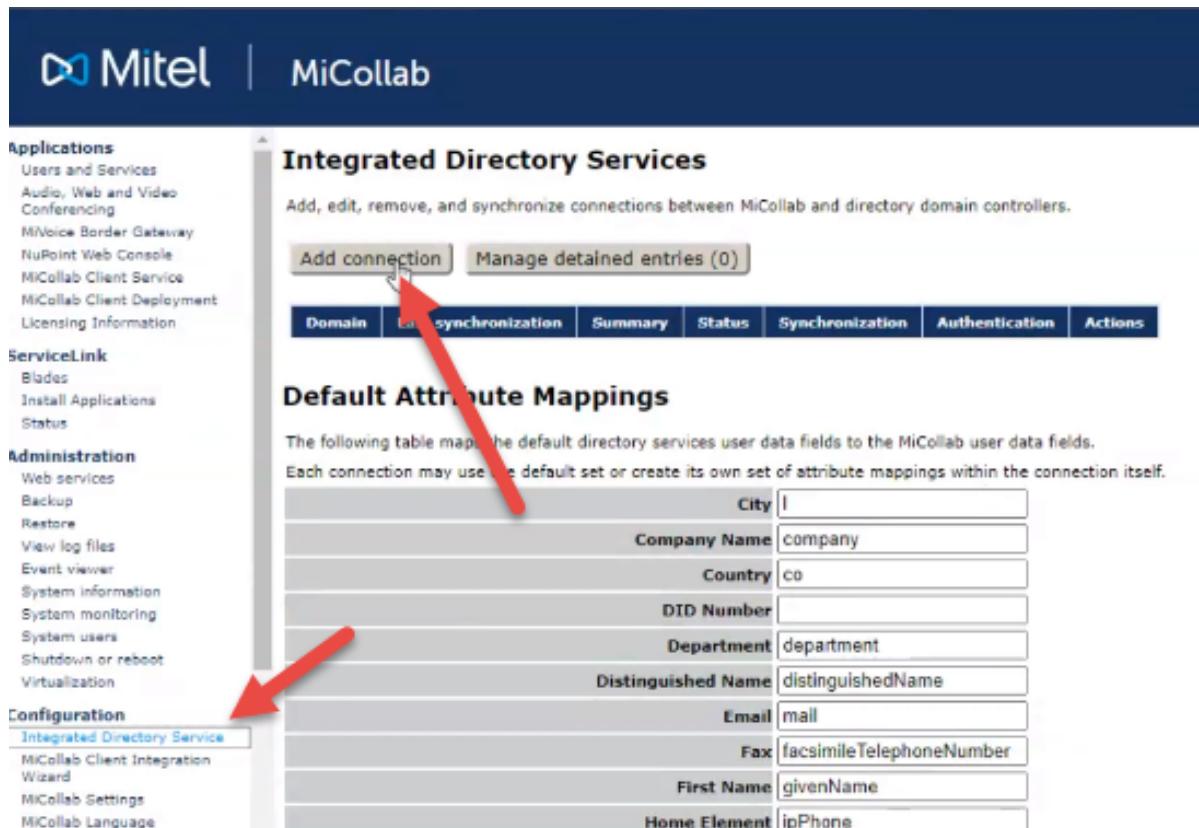
- Enter your Username (Email address)
- Enter your Password

Any users that exist on MiCollab will be sent to CloudLink. This can be confirmed by looking at the users on CloudLink and comparing them with MiCollab.

Note:

At this point, CloudLink-based Authentication has not been enabled.

5. Return to Configuration > Integrated Directory Services and click Add Connection.



Integrated Directory Services

Add, edit, remove, and synchronize connections between MiCollab and directory domain controllers.

Add connection Manage detailed entries (0)

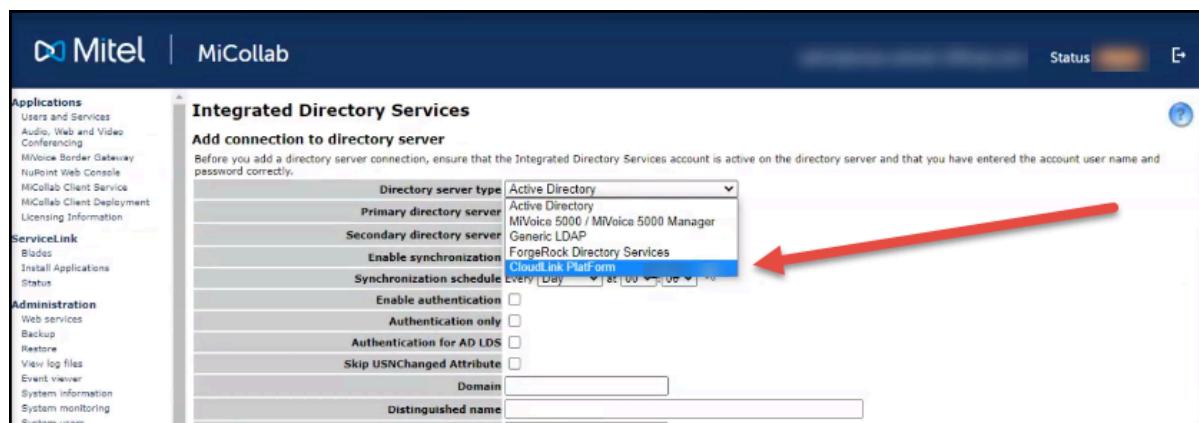
Domain **synchronization** Summary Status Synchronization Authentication Actions

Default Attribute Mappings

The following table maps the default directory services user data fields to the MiCollab user data fields. Each connection may use the default set or create its own set of attribute mappings within the connection itself.

City	I
Company Name	company
Country	co
DID Number	
Department	department
Distinguished Name	distinguishedName
Email	mail
Fax	facsimileTelephoneNumber
First Name	givenName
Home Element	ipPhone

6. When the new connection page is provided, select the **Director Server Type** dropdown field. You will notice that CloudLink Platform will now appear. Select CloudLink Platform.



Integrated Directory Services

Add connection to directory server

Before you add a directory server connection, ensure that the Integrated Directory Services account is active on the directory server and that you have entered the account user name and password correctly.

Directory server type: Active Directory

Primary directory server: MiVoice 5000 / MiVoice 5000 Manager

Secondary directory server: Generic LDAP

Enable synchronization: CloudLink Platform

Synchronization schedule: Every Day

Enable authentication:

Authentication only:

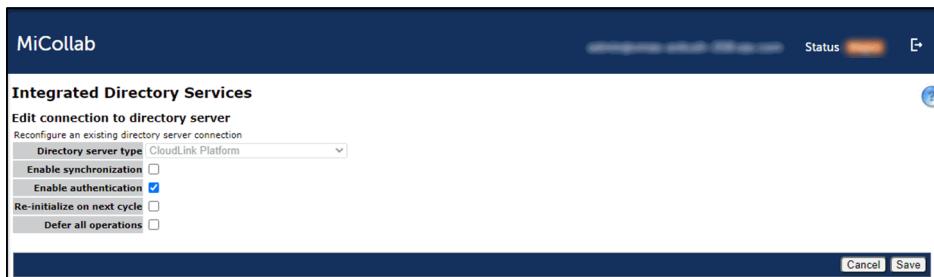
Authentication for AD LDS:

Skip USNChanged Attribute:

Domain:

Distinguished name:

7. Once **CloudLink Platform** is selected, the following **Integrated Directory Services** page will open to further define the connection type. Click on the **Enable authentication** checkbox and **Save**.



Once the CloudLink/Entra ID based authentication is enabled, all existing users and new users created will be provided with CloudLink Unified Login as detailed in the subsequent sections.

At this point, once MiCollab is integrated with CloudLink for CloudLink authentication, MiCollab Client Users (Web, PC, Android, iOS, and MAC Client) login in will be authenticated by Entra ID (in this example) via CloudLink instead of MiCollab.

Note:

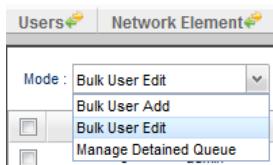
From R9.5 onwards, for performing the CloudLink Authentication procedure, the migrated user's login ID becomes the same as their Email ID. This behavior is valid for all the first-time users performing CloudLink Authentication. In case of manually or locally enabling and disabling CloudLink Auth from Bulk User Provisioning (BUP)page, no changes would be seen.

1.5.4 To disable CloudLink-based authentication

MiCollab administrator can disable/enable CloudLink-based Authentication for a set of users (one or multiple) through Bulk User Provisioning (BUP). This might be required for cases where the administrator wishes to manage authentication locally through MiCollab for few users, for e.g. temporary users which do not have accounts in AD.

To disable CloudLink-based authentication for specific set of users/user, please follow the below steps.

1. Under **Applications**, click **Users and Services**.
2. Click the **Bulk User Provisioning** tab.
3. In the **Mode** drop-down window, select the **Bulk User Edit** option.



4. Click on **Load Users**.
5. Select the users for whom the CloudLink-based Authentication needs to be disabled.

6. Click on the **Disable CL Auth** button.

A **Password** pop-up will be opened.

7. Enter the default password of those selected users in the **Default Password** and **Confirm Password** fields and click **Submit**.

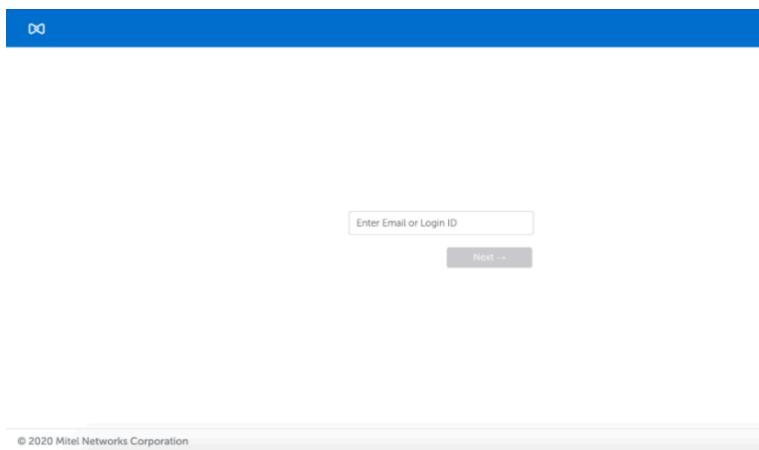
8. Click on **Yes** to confirm. The CloudLink-based Authentication of the selected users will be disabled.

In case of any error, the error message would be displayed. Refer the Troubleshooting Errors, Alarms and Reports for details.

1.5.5 Using CloudLink-based Authentication on the MiCollab Clients

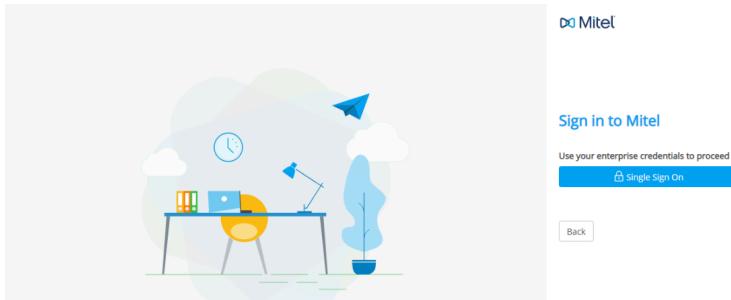
1. Open the MiCollab client in the web browser.

2. Enter the Email ID or login ID (received in MiCollab Welcome Email) and click **Next**.



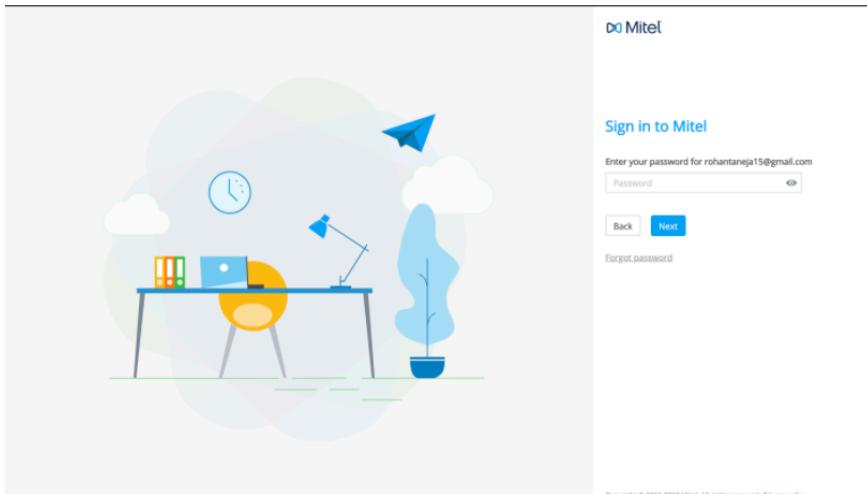
3. If CloudLink-based Authentication is enabled for the user, the MiCollab client will proceed for subsequent login through the CloudLink Unified login page.

- Entra ID is integrated: In the CloudLink Authorization page, use your enterprise credentials to login.
- Entra ID is not integrated: In the CloudLink Authorization page, use your CloudLink password. This password must be setup with the help of CloudLink welcome Email. Check Emails from no-reply@mitel.io to setup your password if not done already.

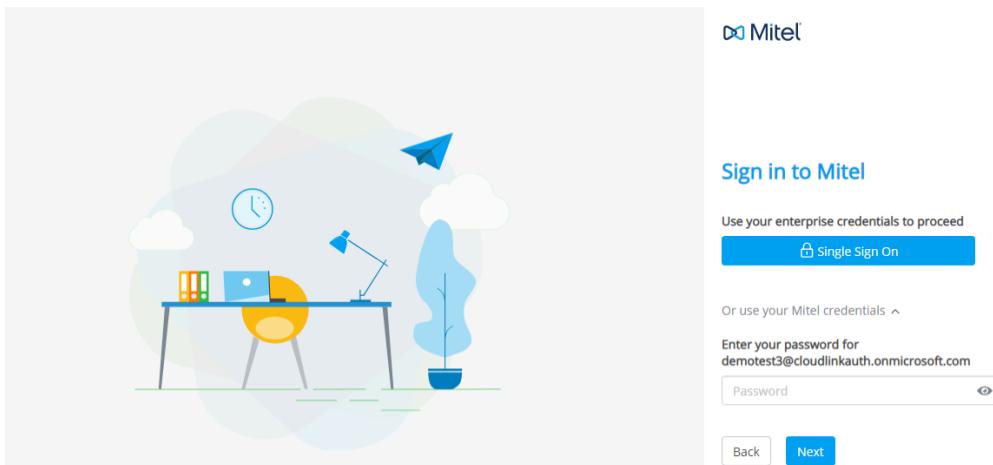


 Note:

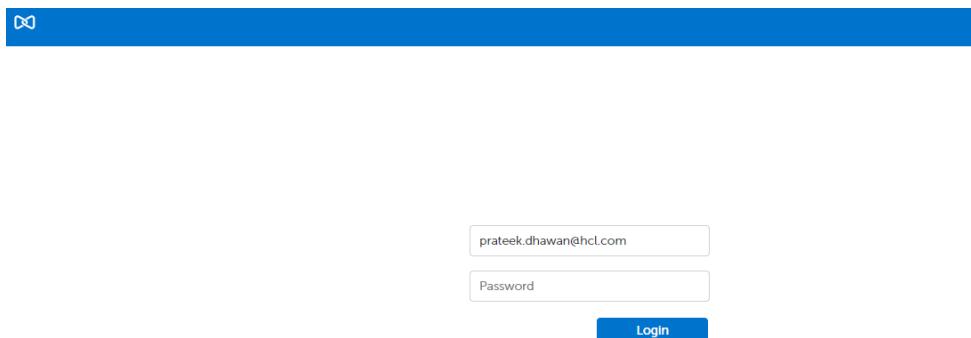
The Email ID is auto-populated on the CloudLink Sign-in page.



- Entra ID is integrated along with the Enable Mitel Credentials (optional) field in the CloudLink Portal: On the CloudLink authorization page, you can use the credentials which were used to verify the account in the CloudLink Portal (check Emails from no-reply@mitel.io to setup your password).

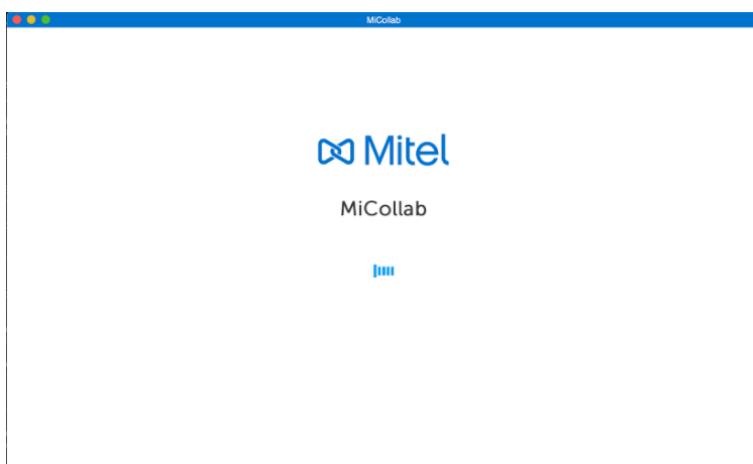


4. If CloudLink-based Authentication is not enabled, then the user proceeds for MiCollab Authentication and on providing the Email/Login ID on the same page, next the password field opens.

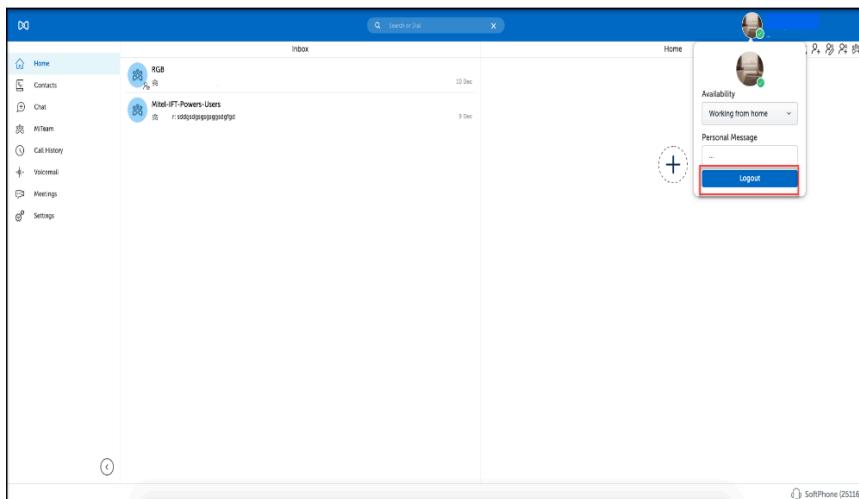


5. On successful password authentication, the user might be prompted to enter a second-factor authentication code, for example, OTP (based on Multifactor Authentication configuration done on Azure AD behind CL platform).
6. After the successful multifactor authentication, the client is presented with the progressing screen followed by MiCollab Home Screen.

With this the CloudLink-based authentication is complete and user can use the MiCollab Client features.



7. For CL authenticated users they can use the Logout functionality to logout of the Web client.



1.5.6 Manual login for native clients

CloudLink Authentication also supports manual login in native clients (iOS, Android, PC, and MAC OS).

Perform the following steps for manual login for the native clients:

1. Tap on the Mitel logo three times to open the Manual Login screen.



2. In the Manual login screen, enter the **Server Hostname** and **Login ID/Email ID**.



The screenshot shows the Mitel MiCollab manual login interface. At the top, the Mitel logo and the text "MiCollab" are displayed. Below this are two input fields: "Server Hostname" and "Login ID". The "Server Hostname" field contains the placeholder "Server Hostname" and has a red arrow pointing to its left edge. The "Login ID" field contains the placeholder "Login ID" and has a red arrow pointing to its left edge. At the bottom of the screen are two buttons: "Cancel" on the left and "Next →" on the right.

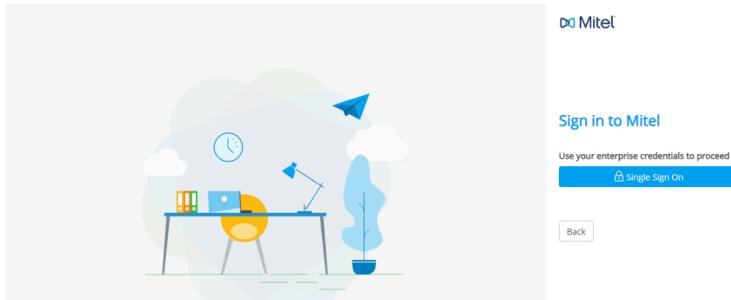
3. Click **Next**.



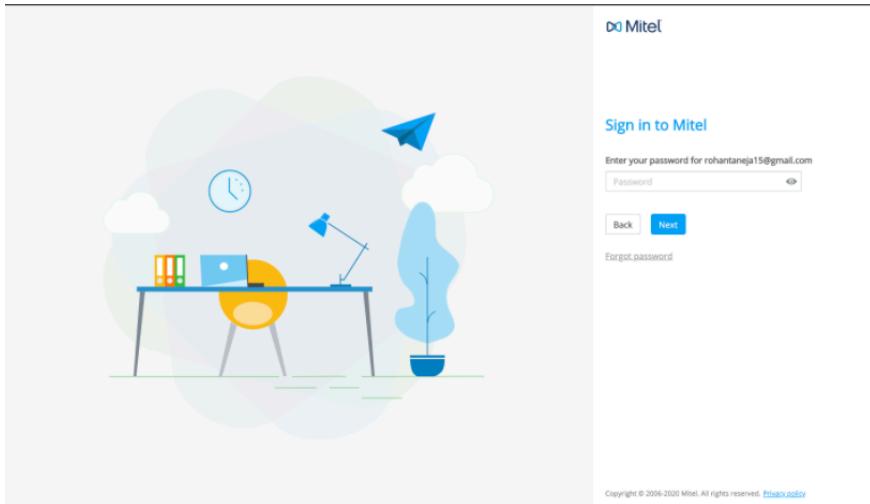
The screenshot shows the Mitel MiCollab manual login interface after the user has entered data. The "Server Hostname" field now contains the value "mivbc.sveapps.com" and has a red arrow pointing to its left edge. The "Login ID" field now contains the value "jains21@mitel.com" and has a red arrow pointing to its left edge. The "Cancel" and "Next →" buttons are visible at the bottom.

4. If CloudLink-based Authentication is enabled for the user, the MiCollab client will proceed for subsequent login through the CloudLink Unified login page.

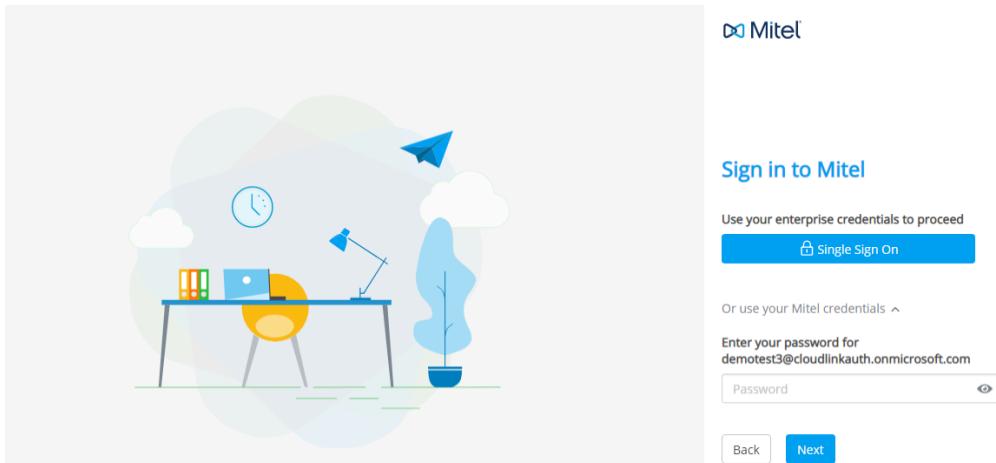
- Entra ID is integrated: In the CloudLink Authorization page, use your enterprise credentials to login.
- Entra ID is not integrated: In the CloudLink Authorization page, use your CloudLink password. This password must be set up with the help of CloudLink Welcome Email. Check Emails from no-reply@mitel.ioto setup your password if not done already.



i Note: The Email ID is auto-populated on the CloudLink Sign-in page.



- Entra ID is integrated along with the field Enable Mitel Credentials (optional) over CloudLink Portal: In the CloudLink authorization page, you can use the credentials which were used to verify the account over CloudLink Portal (check Emails from no-reply@mitel.ioto setup your password).



5. If CloudLink-based Authentication is not enabled, then the user proceeds for MiCollab Authentication, and on providing the Email/Login ID on the same page, next the password page opens.

A screenshot of the MiCollab login interface. It features the Mitel logo and the text 'MiCollab'. Below this are two input fields: 'Server Hostname' and 'Login ID', both with red arrows pointing to them. At the bottom are 'Cancel' and 'Next →' buttons.A screenshot of the MiCollab password input page. It shows the Mitel logo and 'MiCollab' text. There is a single input field labeled 'Enter Password' with a red arrow pointing to it. Below the input field is a 'Login' button.

CloudLink-based Synchronization

2

This chapter contains the following sections:

- Prerequisites and Supported Platforms
- Limitations
- Setting up CloudLink Account for SCIM integration
- Setting up the Provisioning Server (Entra ID)
- Setting up Mitel SCIM Enterprise Application
- Setting up MiCollab for CloudLink-based Synchronization
- Adding a User with Microsoft Extra Sync
- Deleting a User with Microsoft Entra ID Sync

CloudLink (CL)-based synchronization provides single point of user provisioning and management of MiCollab users from the CloudLink Accounts Portal. CloudLink can further be integrated with a provisioning service such as Entra ID with the help of SCIM interface to extend the user provisioning and management directly from the Entra ID service portal. This feature can be turned on/off with Cloudlink-based authentication.

2.1 Prerequisites and Supported Platforms

- Cloudlink-based synchronization is supported in Integrated mode and only with MiVB platforms (On-premise and Flex deployments).
- Once Cloudlink-based synchronization is enabled, the administrator will not be able to add new users from MiCollab USP but from CloudLink (or 3rd party provisioning server) portal only. At the same time attributes updates for existing users will only be allowed for limited fields.
- Users can be created by Bulk User Provisioning and MiVB platform as well.
- Cloudlink-based Synchronization can only be turned on one IDS connection.

i Note:

CloudLink Synchronization does not support importing contacts into MiCollab, as it can be done with on-premise AD synchronization. You can create contacts as Basic users from the Bulk User Provisioning tab on MiCollab.

i Note:

it is not necessary to enable CloudLink-based Synchronization in order to take advantage of CloudLink-based Authentication.

Note:

For Cloudlink synchronization to work, the mobile number which is entered in Entra ID must be in **e.164** format. For example, +16135922122 and +441291436000.

The following subsections describe the MiCollab Client behaviors and CloudLink/ Provisioning server (Entra ID)/MiCollab server configurations to enable the Cloudlink-based synchronization.

2.2 Limitations

The following fields are not supported on Entra ID/CloudLink Synchronization, but they can be modified or changed as per the below-mentioned methods:

1. Fields that can be modified from MiCollab USP

- Department
- Language
- Location

2. MiCollab user fields that cannot be populated from Entra ID

- Info
- Info 2
- Position
- Title
- Home Element
- Secondary Phone directory Number
- Mobile Phone Number 2
- Fax
- Distinguished Name

3. Not supported on SCIM Interface; Administrator can update their photo on Azure and the user can update their photo in MiCollab Client.

- Photograph

Note:

On migration from AD Sync to CloudLink Sync, the above-mentioned field values would be maintained and not cleared. After the migration, these values can be updated or modified using the methods specified against the field values.

Note:

Due to a limitation of the Microsoft Azure SCIM solution, a user details field in Entra ID that has been mapped to an attribute will not be provisioned if the field is left blank and hence it cannot be pushed to CloudLink. Therefore, an update of the blank field is neither received by CloudLink nor by MiCollab. That means any field that is provisioned with a non-blank value cannot subsequently be blanked out from the Entra ID side. As an alternate solution, the administrator can set a particular character like "-" or a string "<blank>" instead of null fields on Entra ID. Updates using these characters or strings will be pushed to MiCollab via Cloudlink.

For removing the services like DID, External Number, etc. the administrator needs to update it to a random unique number. After the user is created with a service along with the provided random unique number, delete the service from MiCollab.

2.3 Setting up CloudLink Account for SCIM integration

Prerequisite : Provide a heads-up to the Customer IT administrator that SCIM Field Attribute mapping needs to be planned. The actual mappings will be set up in [Step 14](#) below, but they need to be aware of this requirement.

Follow steps mentioned in Setting up a CloudLink Account for Integration ([Step 1](#) and [Step 2](#)) in Chapter 1, for setting up CloudLink Account. Once the Integration is done, at the bottom of the page you will find the option **Integrations**. Integrations will include Mitel and 3rd Party.

- Mitel Integrations include (not discussed here): MiCollab, MiTeam Meetings, and MiCC.
- 3rd Party Integrations will include Entra ID Sync as shown below:
 - Select the **Add** button beside Entra ID Sync.
 - Select **Done**.

Integrations

Search integrations

Mitel 3rd party

Azure AD Single Sign-On
SSO for enterprises using Azure AD with Mitel's CloudLink based applications. **Add**

Azure AD Sync
Synchronize users between your Azure AD and Mitel's CloudLink based applications. **Add**

Microsoft Office 365
Allows Mitel Cloudlink to integrate with Microsoft Office 365. **Added**

Done

CloudLink-based Synchronization

At this point the Entra ID Sync setup has not been completed. Click on the **Settings** icon.



Click on **Complete setup**.



Click on **Generate keys**.

Azure AD Sync

Before starting ensure you have an Azure AD subscription/ account, and have added an application object. For more information see online help.

It might be easier to have this portal and the Azure AD portal side-by-side as you will be copying and pasting information from this portal to the Azure AD portal.

Press the Generate keys button to create keys to copy to Azure AD SCIM provisioning. Only generate keys as needed.

Generate keys

Remove

Done

Click on **Copy** against the **Tenant URL** text field and **Secret Token** text field and save the values, as these values would be required to be entered on Entra ID portal SCIM app configuration.

The keys generated will be used by the customer site IT personal for the Entra ID part of this configuration. Copy the Tenant URL and Secret Token and send this information to the Customer IT person via Email.

Click **Done** to complete the configuration on CloudLink.

Note:

Click on **Generate Keys** button to create the keys and copy them to the Entra ID SCIM app.

Azure AD Sync

Before starting ensure you have an Azure AD subscription/ account, and have added an application object. For more information see online help.

It might be easier to have this portal and the Azure AD portal side-by-side as you will be copying and pasting information from this portal to the Azure AD portal.

Press the Generate keys button to create keys to copy to Azure AD SCIM provisioning. Only generate keys as needed.

 **Generate keys**

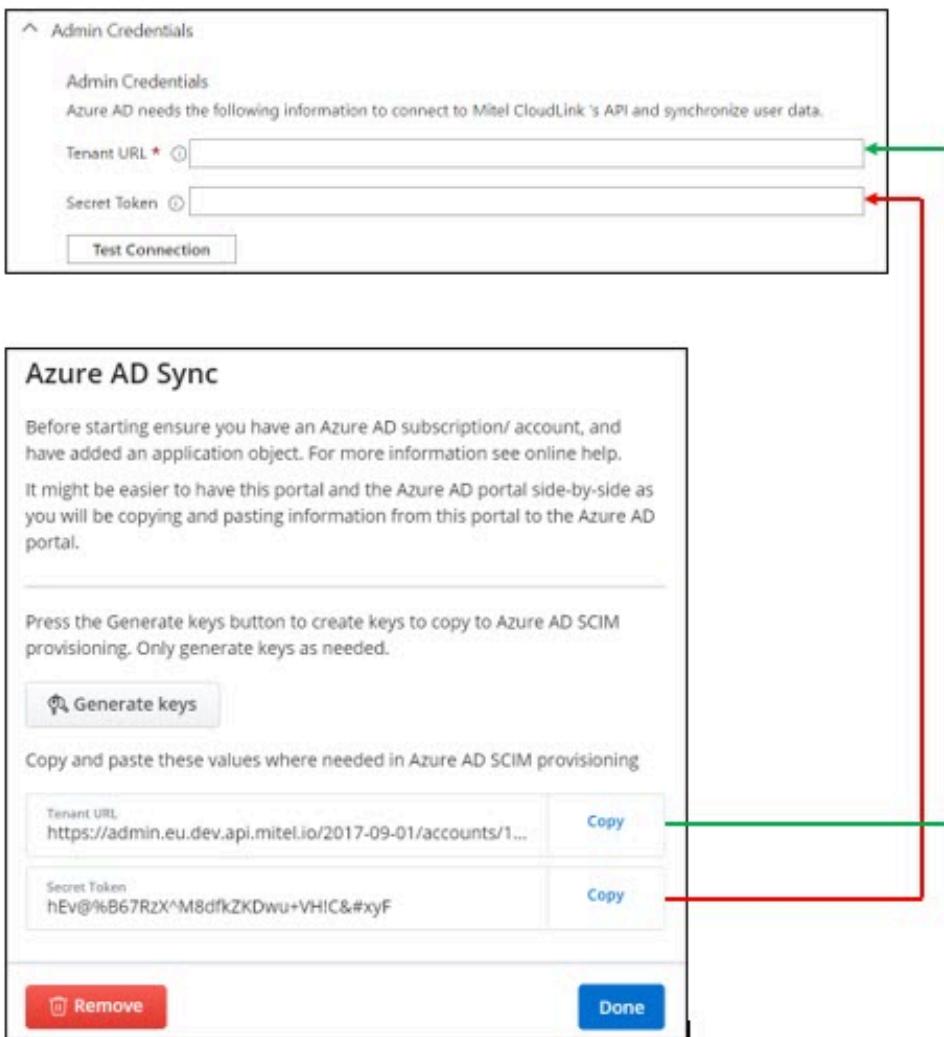
Copy and paste these values where needed in Azure AD SCIM provisioning

Tenant URL	https://admin.eu.dev.api.mitel.io/2017-09-01/accounts/7...	Copied
------------	---	---------------

Secret Token	\$p%PVqD7hQ9aBdrf^yKScxs+AGEwHvC@	Copy
--------------	---	-------------

 **Remove**

Done



2.4 Setting up the Provisioning Server (Entra ID)

The information contained within this section on CloudLink or Entra ID does not follow MiCollab release cadences and content. The purpose of this section is to provide information on the basics of integrating CloudLink with Microsoft Entra ID for the provisioning and management of MiCollab users.

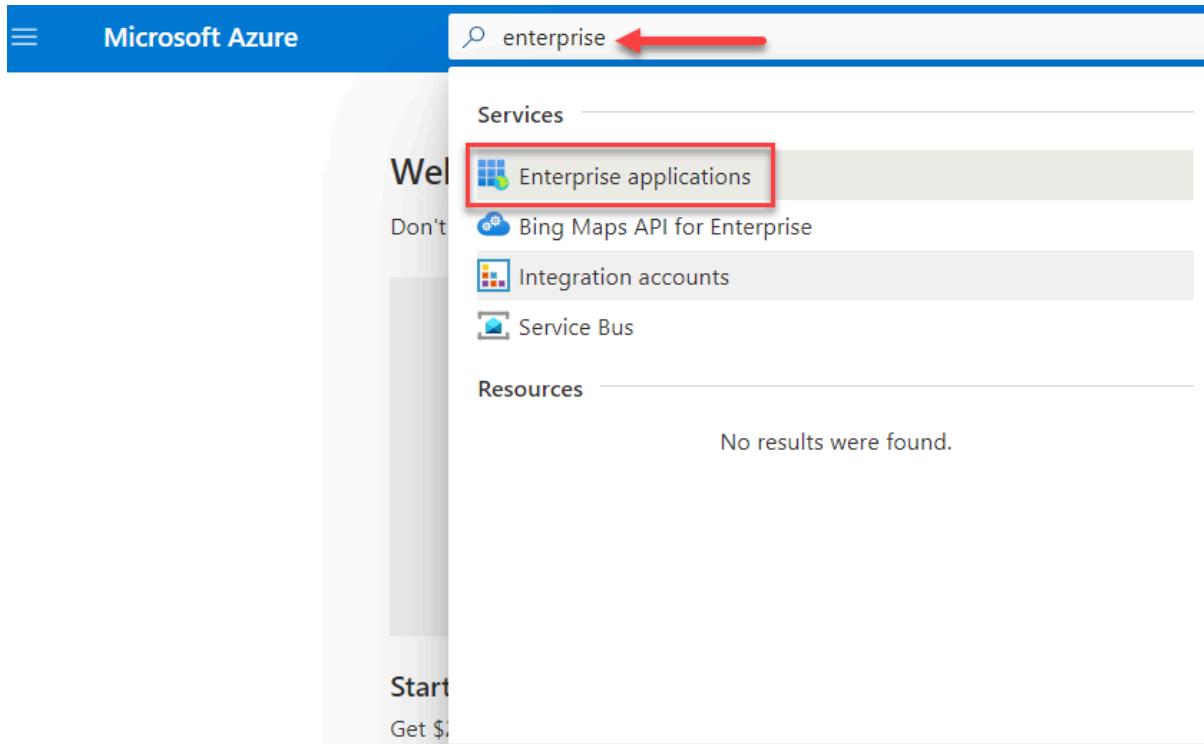
Note:

Role change and Directory Number change are not allowed when done through Entra ID; similarly, they are not allowed in the case of AD synchronization.

2.5 Setting up Mitel SCIM Enterprise Application

To set up the Mitel SCIM Enterprise app, the administrator should have access to the Entra ID Portal.

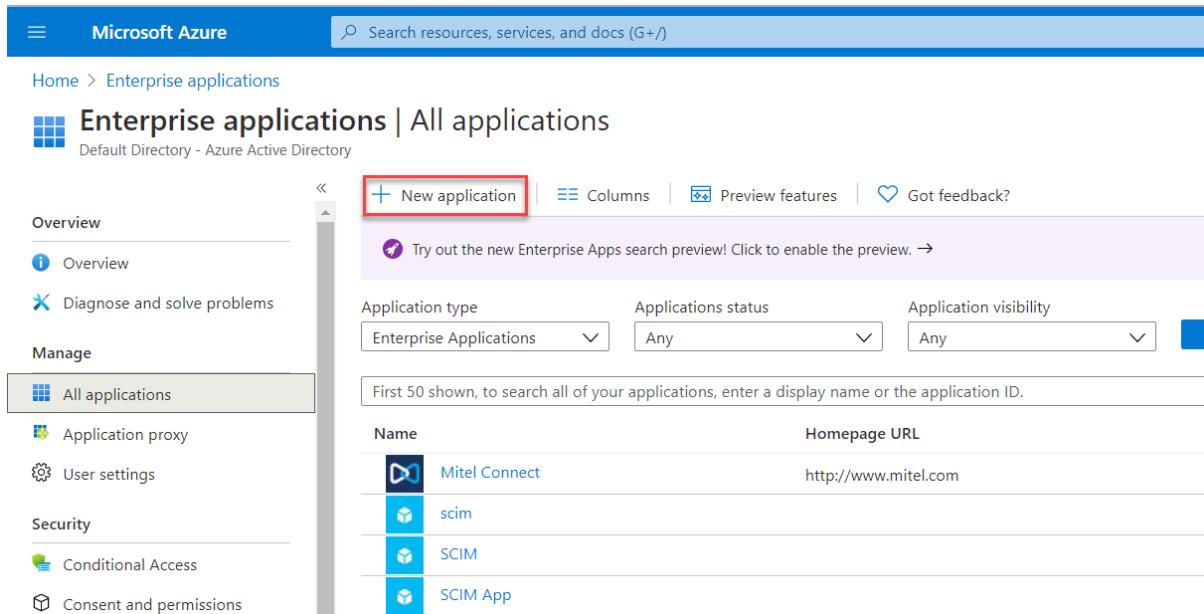
1. In the Entra ID portal, search for **Enterprise applications.**



The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text 'enterprise' and a red arrow pointing to it. Below the search bar, the 'Services' section is visible, containing several items: 'Enterprise applications' (which is highlighted with a red box), 'Bing Maps API for Enterprise', 'Integration accounts', and 'Service Bus'. Below the services, there is a 'Resources' section with the message 'No results were found.'

2. Once the Enterprise application opens, click on the **New application option.**

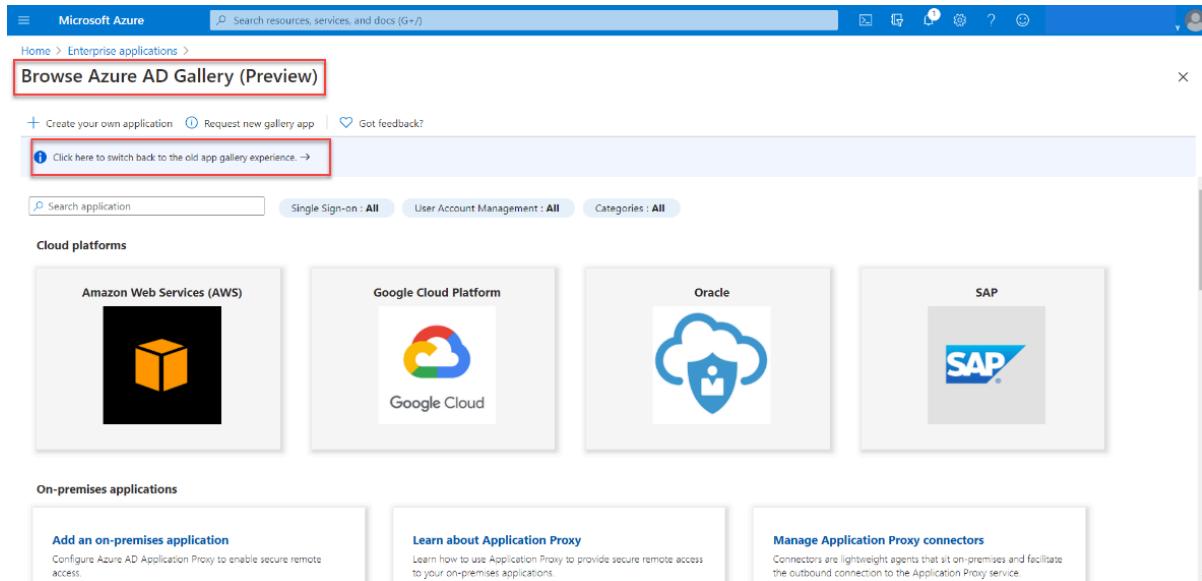
The **Browse Entra ID Gallery** opens.



The screenshot shows the 'Enterprise applications | All applications' page in the Microsoft Azure portal. The left sidebar has sections for 'Overview', 'Manage' (with 'All applications' highlighted), and 'Security'. The main area has a header with 'New application' (highlighted with a red box), 'Columns', 'Preview features', and 'Got feedback?'. Below the header, there is a note: 'Try out the new Enterprise Apps search preview! Click to enable the preview. →'. The main table has columns for 'Application type', 'Applications status', and 'Application visibility'. The 'Name' column lists 'Mitel Connect', 'scim', 'SCIM', and 'SCIM App'. The 'Homepage URL' column shows the URL for 'Mitel Connect'.

Name	Homepage URL
Mitel Connect	http://www.mitel.com
scim	
SCIM	
SCIM App	

3. In the **Browse Entra ID Gallery (Preview)**, switch to the old app gallery experience.



Microsoft Azure

Search resources, services, and docs (G+)

Home > Enterprise applications > **Browse Azure AD Gallery (Preview)**

Click here to switch back to the old app gallery experience.

Search application

Single Sign-on : All User Account Management : All Categories : All

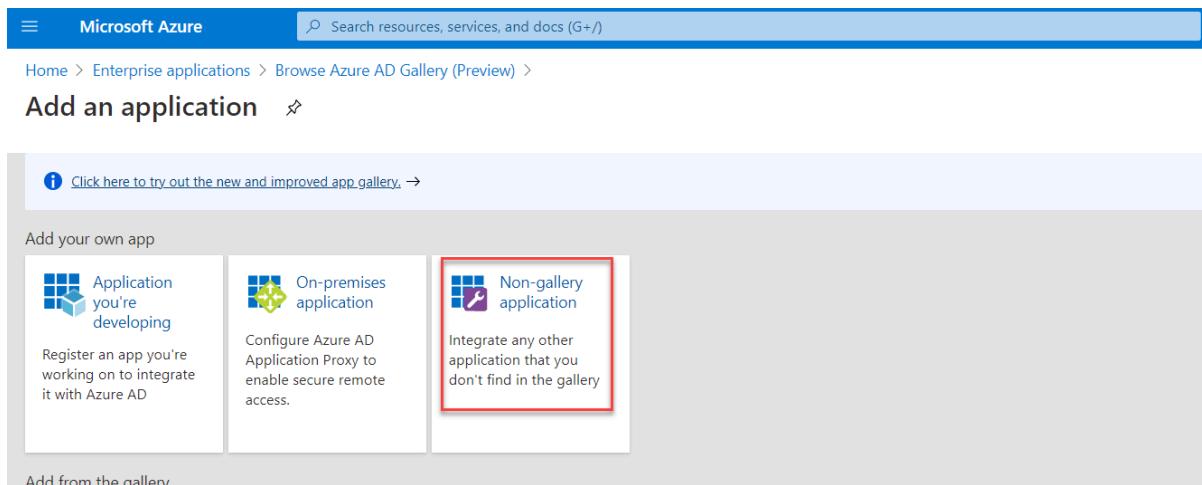
Cloud platforms

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle
- SAP

On-premises applications

- Add an on-premises application
- Learn about Application Proxy
- Manage Application Proxy connectors

4. Select the **Non-gallery application**.



Microsoft Azure

Search resources, services, and docs (G+)

Home > Enterprise applications > Browse Azure AD Gallery (Preview) > **Add an application**

Click here to try out the new and improved app gallery. →

Add your own app

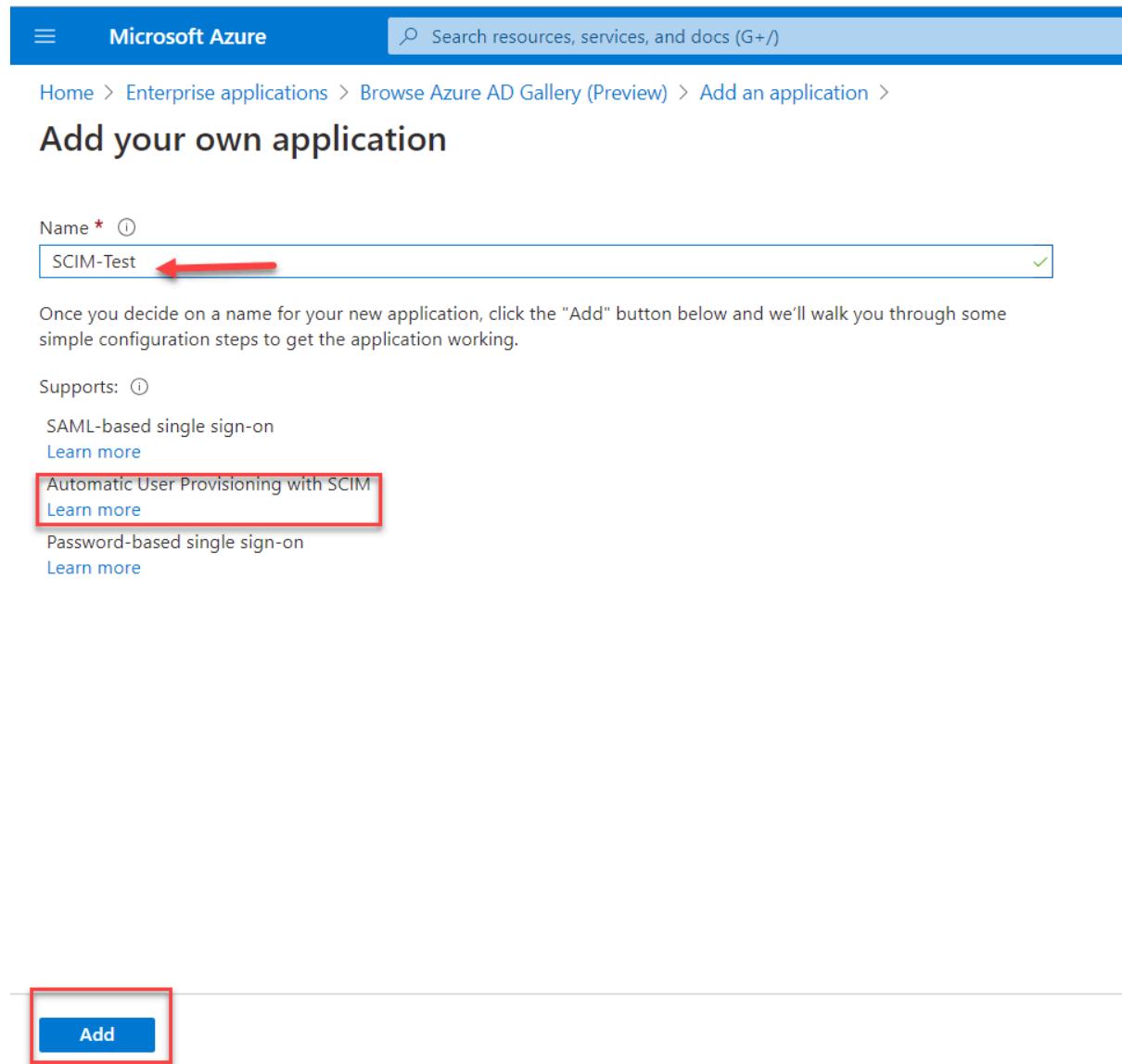
- Application you're developing
- On-premises application
- Non-gallery application**

Integrate any other application that you don't find in the gallery

Add from the gallery

5. Under the **Add your own application** field, add the application with a name of your preference like Mitel SCIM and click on **Add**.

You can click on **Learn more** under **Automatic User Provisioning with SCIM** to learn more on SCIM.



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Enterprise applications > Browse Azure AD Gallery (Preview) > Add an application >

Add your own application

Name * ⓘ

SCIM-Test

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

SAML-based single sign-on

[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

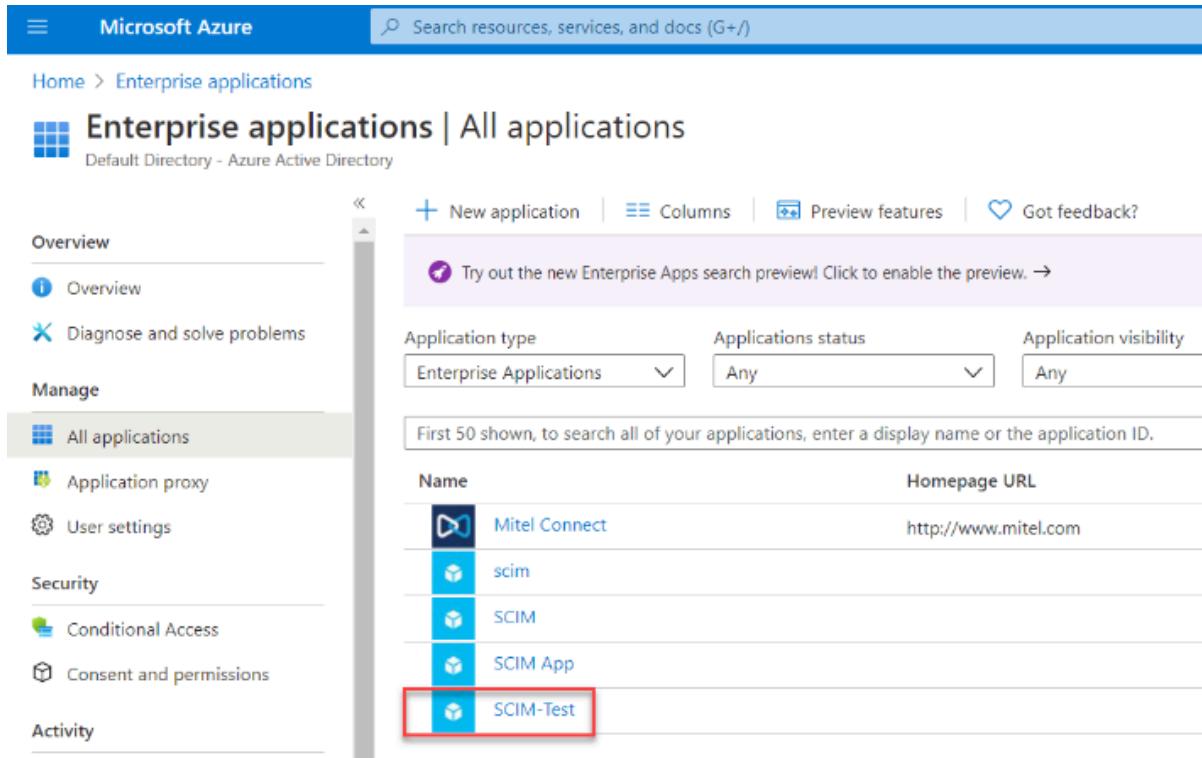
Password-based single sign-on

[Learn more](#)

Add

CloudLink-based Synchronization

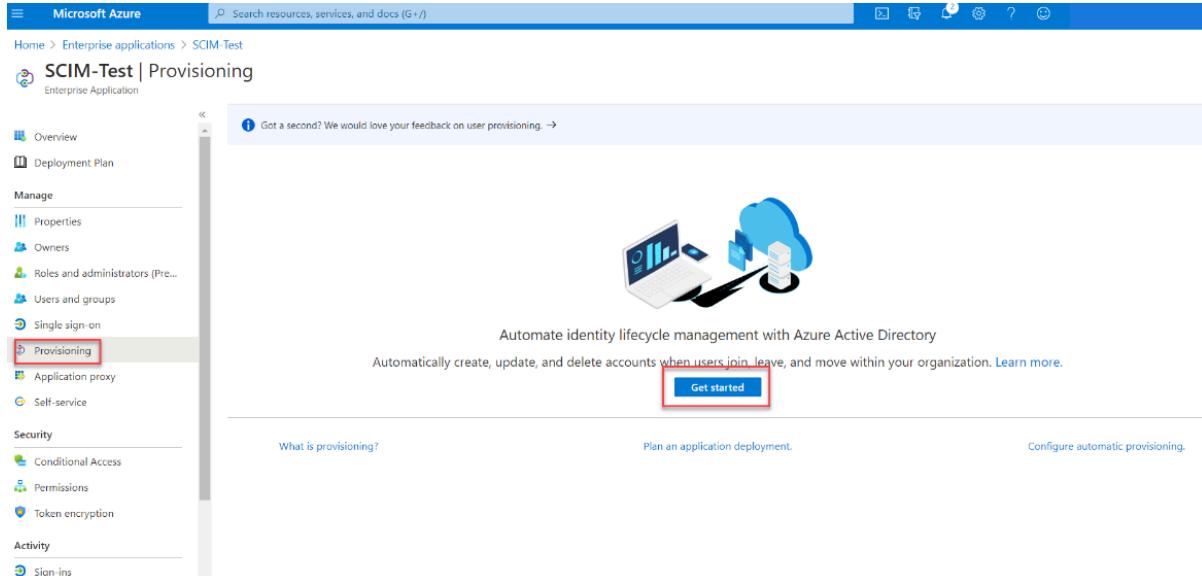
6. Click on the configured SCIM application to set it up with CloudLink.



The screenshot shows the Microsoft Azure Enterprise applications page. The left sidebar has sections for Overview, Manage (with All applications selected), Security, and Activity. The main area shows a table of applications with columns for Name, Application type (Enterprise Applications), Applications status (Any), and Application visibility (Any). The table lists several applications: Mitel Connect, scim, SCIM, SCIM App, and SCIM-Test. The SCIM-Test application is highlighted with a red box.

Name	Application type	Applications status	Application visibility
Mitel Connect	Enterprise Applications	Any	Any
scim			
SCIM			
SCIM App			
SCIM-Test			

7. Click on **Provisioning**, followed by **Get started**.



The screenshot shows the SCIM-Test Provisioning page. The left sidebar has sections for Overview, Deployment Plan, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning (which is selected and highlighted with a red box), Application proxy, and Self-service. The main area features a cloud and laptop icon with the text "Automate identity lifecycle management with Azure Active Directory" and "Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more." A "Get started" button is highlighted with a red box.

8. Select the **Provisioning Mode** as Automatic from the drop-down list. Fill in the fields for **Tenant URL** and **Secret Token** from CloudLink. (Refer to previous section for details. These values were copied and

saved by the user). Refer to the [Tenant URL](#) details mentioned in the previous section. These values were copied and saved by the user.

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIMDoc based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to SCIMDoc's API and synchronize user data.

Tenant URL *

Secret Token

Test Connection

Mappings

9. Click on Test Connection. Test connection should be successful.

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIMDoc based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to SCIMDoc's API and synchronize user data.

Tenant URL *

Secret Token

Test Connection

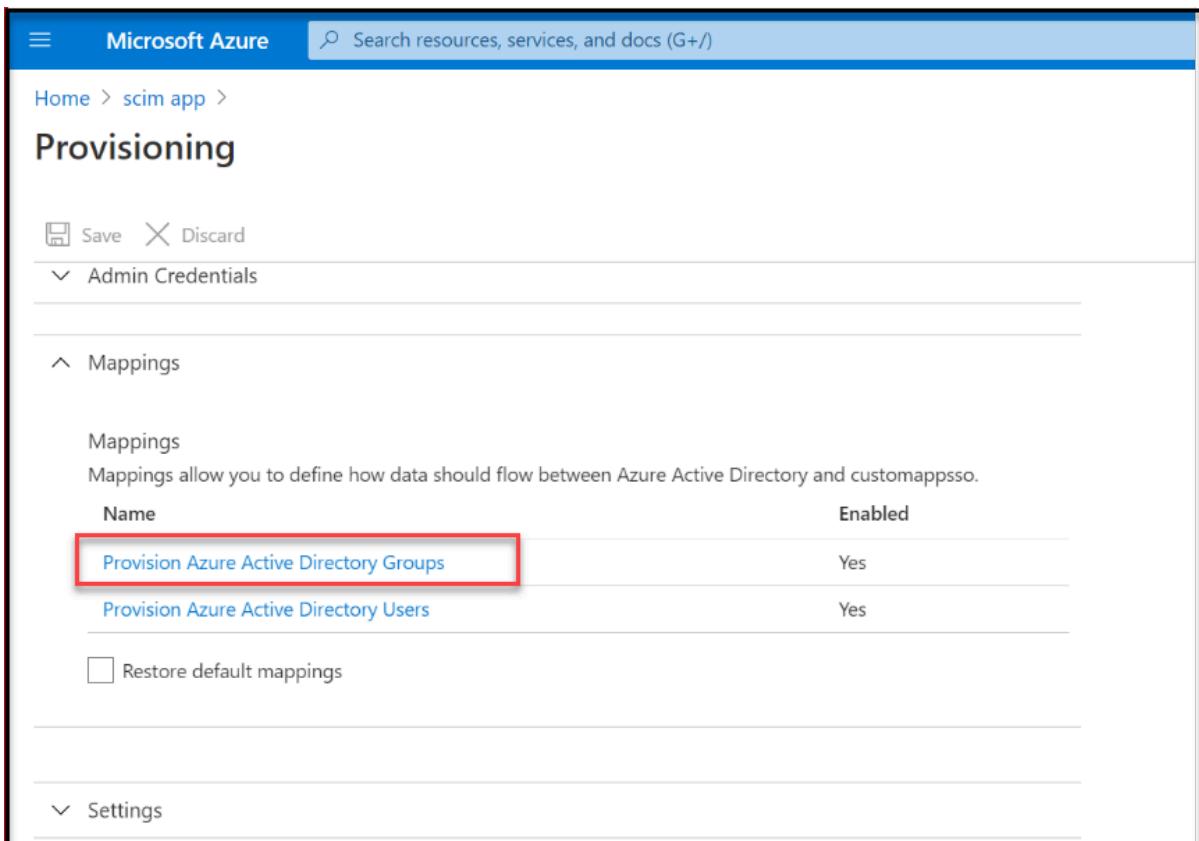
Mappings

Settings

Testing connection to SCIMDoc
The supplied credentials are authorized to enable provisioning

10. Under Mappings click on **Save your credentials to create mappings**.

The screenshot shows the Microsoft Azure 'Provisioning' configuration page for the 'scim' application. At the top, there are 'Save' and 'Discard' buttons. The 'Provisioning Mode' is set to 'Automatic'. A note below states: 'Use Azure AD to manage the creation and synchronization of user accounts in scim based on user and group assignment.' The 'Admin Credentials' section is expanded, showing 'Admin Credentials' and a note: 'Azure AD needs the following information to connect to scim's API and synchronize user data.' It includes fields for 'Tenant URL' (containing a URL) and 'Secret Token' (containing a masked value). A 'Test Connection' button is present. The 'Mappings' section is expanded, showing 'Mappings' and a note: 'Mappings allow you to define how data should flow between applications.' It lists a single mapping entry: 'Name' (highlighted in yellow) and 'Enabled'. A 'Save your credentials to create mappings' button is also highlighted in yellow. A 'Restore default mappings' link is present. The 'Settings' section is partially visible at the bottom.

11. Click on Provision Azure Active Directory Groups.

Microsoft Azure Search resources, services, and docs (G+ /)

Home > scim app >

Provisioning

Save Discard

Admin Credentials

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Restore default mappings

Settings

12. Under Attribute Mapping, turn off the **Enabled** and click **Save**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > scim app > Provisioning >

Attribute Mapping

Save Discard

Name: Provision Azure Active Directory Groups

Enabled: Yes No

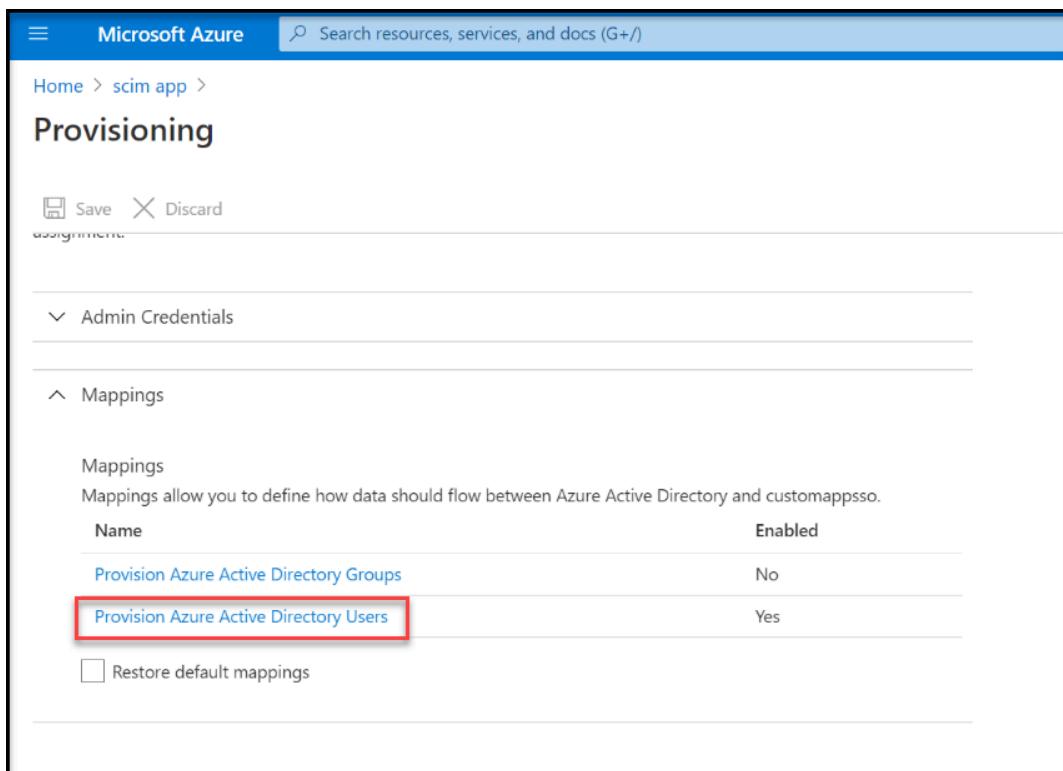
Source Object (Azure Active Directory): Group

Source Object Scope: All records

Target Object (customappssso): urn:ietf:params:scim:schemas:core:2.0:Group

Target Object Actions:

- Create
- Update
- Delete

13. Click on Provision Azure Active Directory Users.

The screenshot shows the Microsoft Azure 'Provisioning' page. At the top, there are 'Save' and 'Discard' buttons. Below them, there are two sections: 'Admin Credentials' (collapsed) and 'Mappings' (expanded). The 'Mappings' section title is 'Mappings' with a sub-instruction 'Mappings allow you to define how data should flow between Azure Active Directory and custom apps'. It lists two items: 'Provision Azure Active Directory Groups' (Enabled: No) and 'Provision Azure Active Directory Users' (Enabled: Yes). A red box highlights the 'Provision Azure Active Directory Users' row. At the bottom of the 'Mappings' section, there is a checkbox for 'Restore default mappings'.

Name	Enabled
Provision Azure Active Directory Groups	No
Provision Azure Active Directory Users	Yes

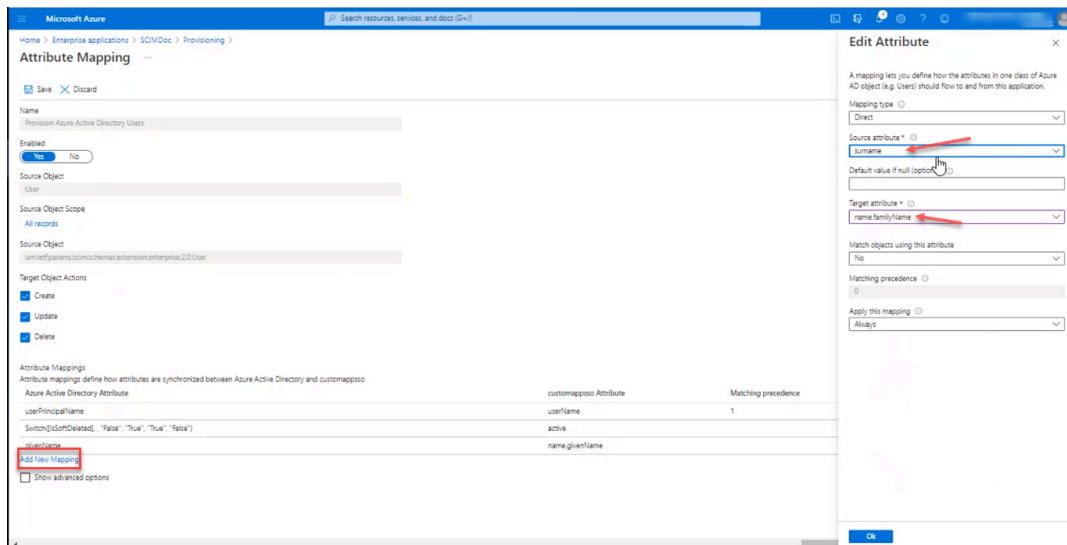
14. Add/Edit Attribute mappings

Add/Edit source to target attribute mappings. All the target attributes will be auto-populated in Entra ID

i Note:

Edit attribute mapping can be done for AAD users and not for AAD groups.

Mappings determine the user attributes that flow between Entra ID and the MiCollab application (via CloudLink SCIM) when user accounts are provisioned or updated.



i Note:

The following SCIM attributes are supported for programming from the provisioning server (in this case Entra ID). All the mandatory fields mentioned below in the table should be programmed from Azure. In absence of mandatory fields, the updates will first land in the detained queue and require Manual Intervention to save on MiCollab.

Table 1: Attribute Mapping for 'only' CloudLink Attributes

These attributes are mandatory and only needed by Cloudlink, and therefore they should not be deleted nor any changes should be made.

Entra ID Attributes	SCIM/Target Attributes	MiCollab Attributes
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	

Entra ID Attributes	SCIM/Target Attributes	MiCollab Attributes
userPrincipalName	userName	
telephoneNumber	phoneNumbers[type eq "work"].value	Primary Phone Directory Number (DN)

Table 2: Attribute Mappings

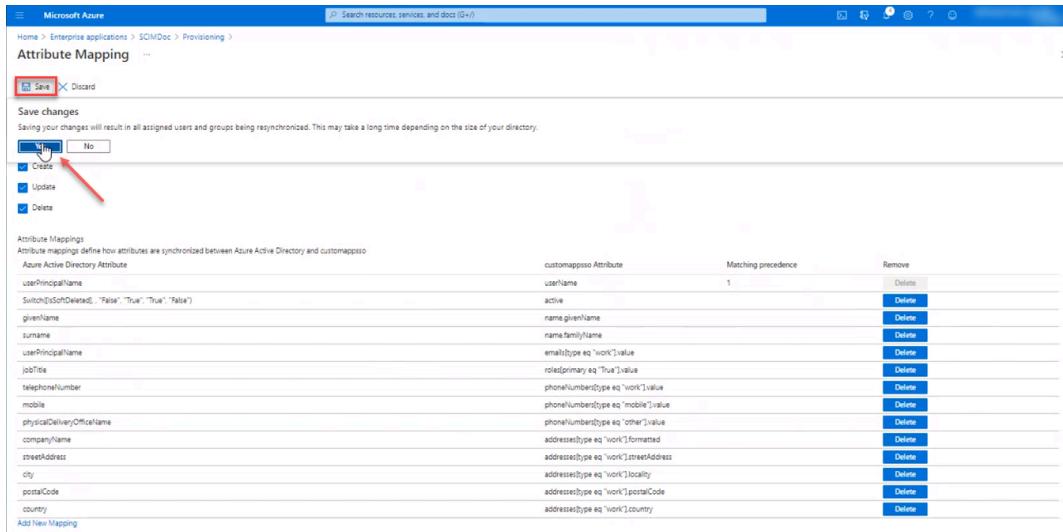
Entra ID Attributes	SCIM/Target Attributes	MiCollab Attributes
givenName	name.givenName	First Name
surName	name.familyName	Last Name
userPrincipalName	emails[type eq "work"].value	Email address
Extension attribute or any available UI attribute	roles[primary eq "True"].value	Role
mobile	phoneNumbers[type eq "mobile"].value	Mobile
Extension attribute or any available UI attribute	phoneNumbers[type eq "other"].value	DID
physicalDeliveryOfficeName	address[type eq "work"].formatted	Company name
Extension attribute or any available UI attribute	address[type eq "work"].streetAddress	Street Address
Extension attribute or any available UI attribute	address[type eq "work"].locality	City
Extension attribute or any available UI attribute	address[type eq "work"].postalCode	Postal Code

Entra ID Attributes	SCIM/Target Attributes	MiCollab Attributes
Extension attribute or any available UI attribute	address[type eq "work"].country	Country

i Note:

If the user synchronization is enabled from On-Prem AD and authentication is enabled from CloudLink, the Admin must change the IDS mapping for the login id to the **"userPrincipalName"** field.

15. Click on **Save mapping.**



16. Turn on the **Provisioning Status** and **Save** configuration to complete.

Microsoft Azure

Home > Enterprise applications > scim > Provisioning

Save **Discard**

Mappings

Mappings
Mappings allow you to define how data should flow between Azure Active Directory and custom appss.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Restore default mappings

Settings

Notification Email ⓘ
 Send an email notification when a failure occurs

Status
Start and stop provisioning to scim, and view provisioning status.

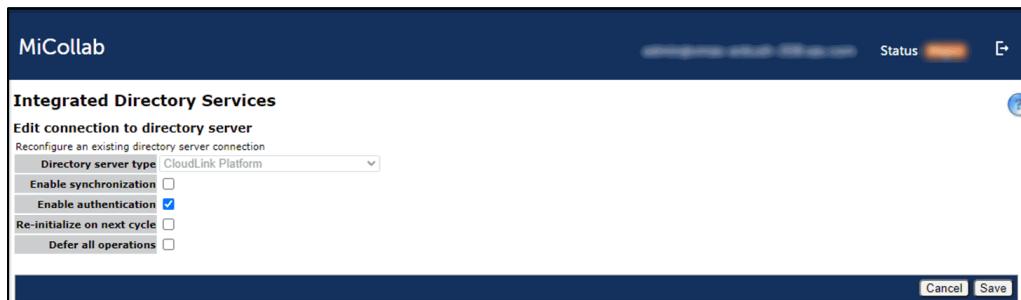
Provisioning Status **On** Off

Current Status | Statistics to date

2.6 Setting up MiCollab for CloudLink-based Synchronization

1. If you have an On-Prem AD connection or any other IDS connection which is currently being used for user synchronization, you must disable the synchronization first, as only one source of synchronization is allowed. If On-Prem AD connection is only used for user synchronization and not for authentication, you may proceed for deletion.
2. Refer To add CloudLink Platform/Entra ID authentication for IDS step 1 to 6 for setting up CloudLink Integration and CloudLink Platform IDS.

3. Click on the **Enable synchronization** checkbox and **Save**.



4. Once the Cloudlink-based synchronization is enabled, all existing users and new users created from the provisioning server (Entra ID) will be synced to MiCollab.
5. Select **Defer all operations** to preview the synchronization updates in the detained updates queue. From the queue, you can view, apply, modify, or cancel (delete) the updates as required.
6. Select **Re-initialize on next cycle** to re-initialize the user sync from CloudLink.

This option effectively forces a full synchronization on the next scheduled sync event. A full synchronization queries the directory server for the entire set of users. This option can be used to recover the MiCollab database from the directory server. It will most likely result in a large number of detained user updates.

7. Once the IDS connection is made, a sync button is also provided to check for any database changes on the provisioning server and applies the updates to the MiCollab database. This might be required when changes are done on CloudLink (or provisioning server) when MiCollab is offline.

Note:

- Once the synchronization is enabled, the administrator will not be allowed to add a new user(s) from **Add**, and **Quick Add** options. Any new user addition and updates must be done from the provisioning server portal only. Refer to Table 1 Attribute Mappings for details on MiCollab attributes.
- Updates made from the provisioning server (Entra ID portal in this case) to MiCollab are synced at periodic intervals (few mins to few hours depending on the Entra ID configuration). To push the updates immediately, use the 'Provision on demand' feature from Entra ID portal.

2.7 Adding a User with Microsoft Extra Sync

Note:

The administrator needs to have an account in the Entra ID portal (<https://portal.azure.com/>)

There are multiple ways to add users in Entra ID through UI, CSV import, PowerShell, etc. The user creation in Entra ID is not considered and described in this document. Please refer <https://portal.azure.com/> for details. This section only describes adding a user in Entra ID Mitel SCIM app once the user is created in Entra ID

- Under Enterprise Applications on Entra ID, select the application you have created to sync with CloudLink SCIM. In this example, the application is named **Mitel SCIM**.

To create an Application, refer to [Setting up Mitel SCIM Enterprise Application](#) on page 29.

Home > Enterprise applications

Enterprise applications | All applications

Custom Directory - Azure Active Directory

Overview

Diagnose and solve problems

Manage

All applications

Application proxy

User settings

+ New application | Columns | Preview features | Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications | Applications status: Any | Application visibility: Any | Apply | Reset

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
MITELSCIM		3e3bf89a-85d8-4322-bff0-529b737...	50d0b1ee-42c2-45d6-9ce8-7845cf...

- On the Application page, click on the **Assign users and groups** option.

Microsoft Azure

Search resources, services, and docs (G+/-)

Home > Enterprise applications >

SCIM App | Overview

Enterprise Application

Properties

Name: SCIM App

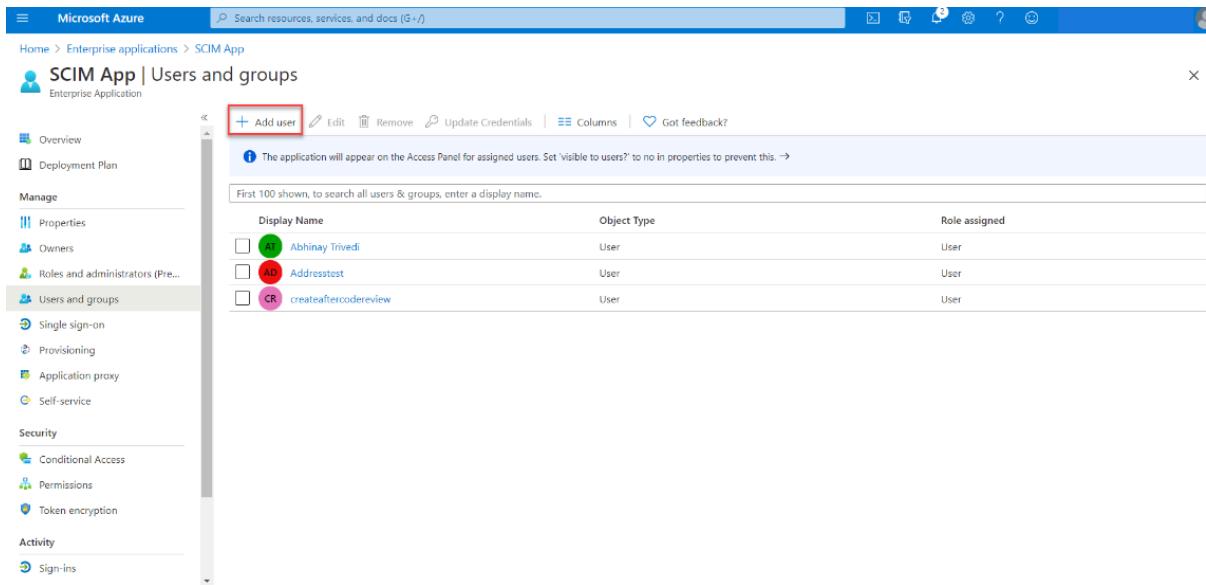
Application ID: 15a013d9-52b5-4d4f-828...

Object ID: ca62a315-1084-4760-b9e...

Getting Started

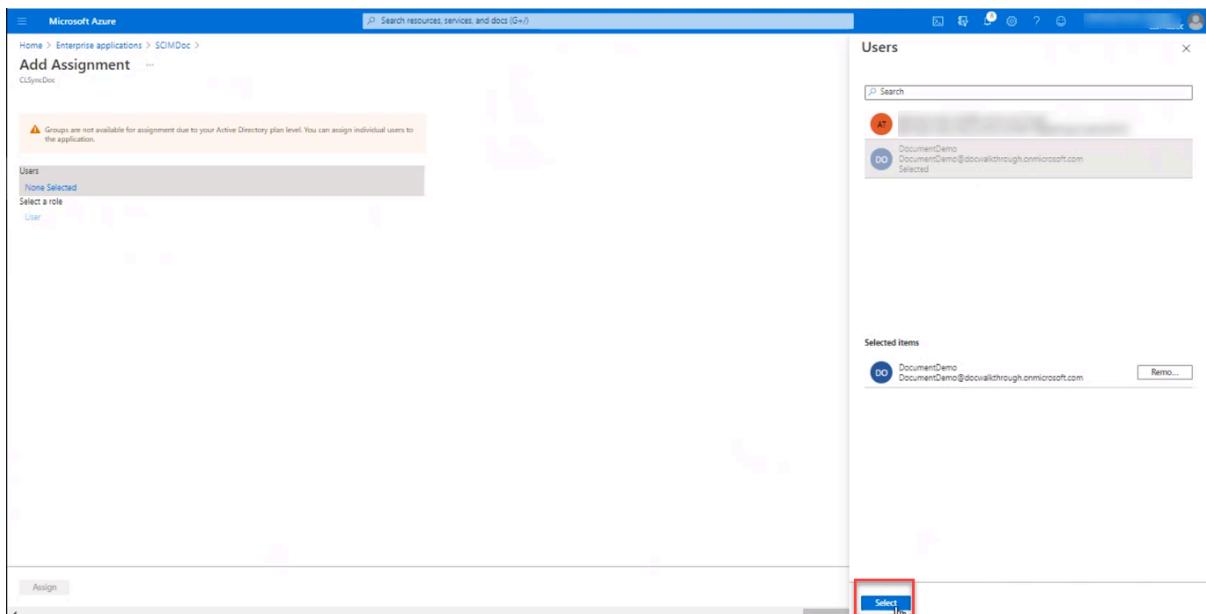
- 1. Assign users and groups
- 2. Set up single sign on
- 3. Provision User Accounts
- 4. Conditional Access
- 5. Self service

3. Click Add user.



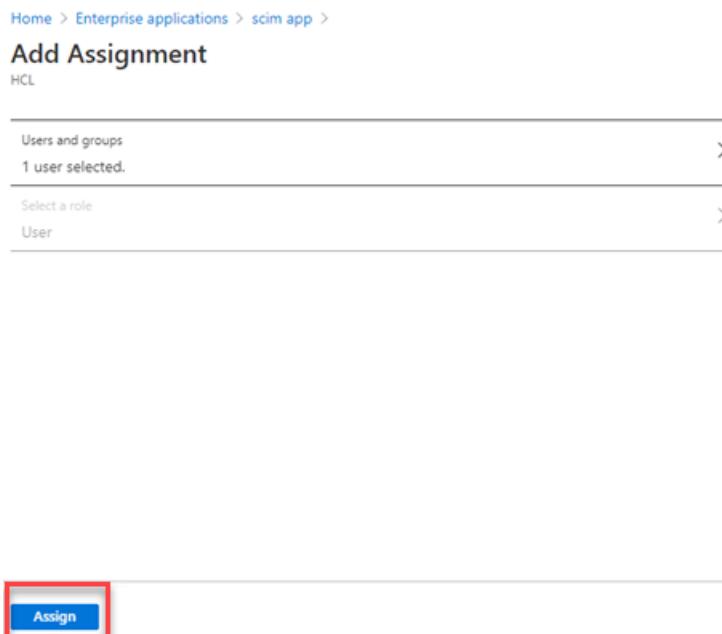
The screenshot shows the Microsoft Azure interface for managing enterprise applications. The left sidebar shows navigation options like Overview, Deployment Plan, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service), Security (Conditional Access, Permissions, Token encryption), and Activity (Sign-ins). The main content area is titled 'SCIM App | Users and groups' and shows a list of users. The top navigation bar includes a search bar, a 'Home' link, and a 'Enterprise applications' link. The 'Users and groups' section is selected in the sidebar. A red box highlights the '+ Add user' button in the top right of the main content area.

4. Search for the applicable users and Select the user.



The screenshot shows the 'Add Assignment' page for the 'SCIMDoc' application. The left sidebar shows 'None Selected' under 'Users' and 'Select a role'. The main content area shows a message: 'Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.' A red box highlights the 'Select' button in the 'Selected Items' list on the right side of the screen.

5. Click Assign.



6. User should now appear in the **Users and groups tab as shown below.**

Display Name	Object Type	Role assigned
DocumentDemo	User	User

Note:

- The last name of a user is not mandatory in Entra ID while it is mandatory in MiCollab. So, if the last name of the user is missing, in this scenario the user creation fails in MiCollab.
- If more than 64 characters are present in the Email ID (characters before @ and should not include @ and the domain part), the login ID will be truncated to 64 characters which will result in user creation failure.
- If Defer All Operations is selected under IDS, all users will be listed in detained queue list. In case the option is not selected, then only the failed users are listed.

2.8 Deleting a User with Microsoft Entra ID Sync

The administrator needs to have an account in the Entra ID portal (<https://portal.azure.com/>).

There are multiple ways to delete users in Entra ID, such as through the UI, CSV import, and PowerShell. User deletion in Entra ID is not covered in this document. For more details, please refer to the Entra ID portal (<https://portal.azure.com/>).

This section only describes deleting a user that was created via Microsoft Entra ID Sync.

1. In the Entra ID portal, navigate to **Users**.
2. Locate the user to be removed from MiCollab, click on the user, and select **Edit Properties**.
3. Click on **Settings**, uncheck **Account Enabled**, and click **Save**.

Seat Toledo ...

Properties

Refresh Got feedback?

All Identity Job Information Contact Information Parental controls **Settings** On-premises

This view only contains properties that can be updated. [Learn more](#)

Search "Settings" properties

Showing 2 results under "Settings"

Account enabled	<input checked="" type="checkbox"/>
Usage location	<input type="button" value="▼"/>

4. In Entra ID, navigate to **Enterprise Applications**. Select your CloudLink provisioning application. In this example, the application is named CloudLink Provision.

Enterprise applications | All applications ...

New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == **Enterprise Applications** Application ID starts with Add fi

7 applications found

Name	Object ID	Application ID	Homep
ProvisionMVB5V1	1d722ccf-ab48-4a85-b5c5-1564b8ac2d33	d4bc2de5-8377-49cf-bf7a-b785928bf90d	https://
Cloudlink Provision	3d9de668-8ab8-49be-88cf-ccc3adc9a10d	761673f0-a2d8-4490-bed7-168a6edd944a	https://

5. Go to **Provisioning**. The deactivated user will be marked with "active": `false` during the next automatic sync cycle.
6. Optional: To immediately push the deactivation, select **Provision on Demand**, search for the user, and click **Provision**.
7. In the **Perform Action** screen, confirm that the target attribute name is "active" and the value is "false".

Target attribute name	Source attribute value	Expression	Original target attribute val...	Modified target attribute v...
active	Switch("False", "False", "True", ...)	Switch([IsSoftDeleted], "False..."		False
name.formatted	Join(" ", [Seat], " Toledo")	Join(" ", [givenName], [surname])	Seat Toledo	

Note: Using Provision on Demand is not required. Microsoft Entra ID automatically sets "active": `false` during the scheduled provisioning cycle when a user is deactivated.

8. Log in to `accounts.mitel.io` and Navigate to **Account**.
9. Navigate to **User Management**, and select **Users**. Search for the user. The user should not be visible.
10. Click **Add Filter**, select **Property**, and choose **Inactive**.

This displays a list of all inactive users.

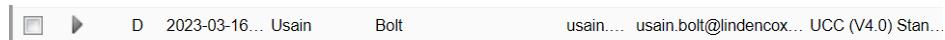
11. In MiCollab, under Configuration, navigate to the **Integrated Directory Service** option.

Domain	Last synchronization	Summary	Status	Synchronization	Authentication	Actions
mitel.io	-	Enabling authentication: 100% entries: 40 errors: 7	Finished	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Remove"/> <input style="background-color: red; color: white; border: 1px solid red;" type="button" value="Sync"/>

12. Select the **mitel.io** option and click **Sync**.

Domain	Last synchronization	Summary	Status	Synchronization	Authentication	Actions
mitel.io	-	Enabling authentication: 100% entries: 40 errors: 7	Finished	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Remove"/> <input style="background-color: red; color: white; border: 1px solid red;" sync"="" type="button value="/>

13. The user will be marked for deletion (D). Select the user to complete the deletion from MiCollab and MiVB.



Note: The actual deletion of the user typically occurs 30 days after the account is deactivated in Microsoft Entra ID, following the standard deprovisioning process.

14. Click on **Manage Detained Entries**.

15. From the Detained Queue, select the deleted user checkbox and click **Save**.

When a user is deactivated in Microsoft Entra ID, they are deleted from Entra ID and MiCollab after syncing. However, MiCollab typically does not delete the user from CloudLink, since the user might still be using other CloudLink services. If a CloudLink Gateway is deployed, the MiVB Provisioning microservice may delete the user from CloudLink, but this depends on the site configuration.

CloudLink and CloudLink Daemon updates for MiCollab

3

All the information pertaining to CloudLink Daemon, onboarding procedure, integration details, are available in the [CloudLink Daemon Solution Guide](#).

With the option to integrate CloudLink under CloudLink Integration in the MiCollab Settings panel and the CloudLink connection under CloudLink Daemon settings in the CloudLink panel, MiCollab administrators should take note of the following:

- **Integration Requirements** - The server must be connected to the CloudLink platform using the CloudLink Daemon settings in the Server Manager panel for the following.
 - System Inventory and SWA Status - When the server is connected to CloudLink platform using the controls in the CloudLink panel, the CloudLink Daemon will send system inventory to the CloudLink panel which can be accessed in the Mitel Administration portal.
 - Remote management interfaces - When the tunnels for MSL Server Manager, MiCollab administration web interface, and MBG administration web interface are started, the administrator can access these applications remotely in the Mitel Administration portal.

Once enabled, the launch buttons within the Mitel Administration console will open the remote management interfaces.

i **Note:** The procedure to connect the server to CloudLink platform in the CloudLink Daemon dashboard (in the CloudLink panel) is almost identical to the procedure to connect the MiCollab applications to CloudLink platform (in the MiCollab settings panel). The procedure for CloudLink Daemon integration is done in the new CloudLink panel under Configurations, in the Server Manager. See the [CloudLink Daemon Solution Guide](#) for detailed information.

- **Activation Process** - The procedure to connect to the CloudLink platform is identical, and in both cases the account administrator will log into the CloudLink in order to create the connection.
- **Separate Integrations:** Although similar, these are two distinct integrations. Both must be completed separately; connecting just one will not enable full functionality..
- **CloudLink Account:** Ensure that the same CloudLink account is used for connecting both integrations.
- **Single Server Onboarding:** Only one MiCollab server should be connected to a CloudLink account. Connecting multiple servers may result in the features not functioning properly.

Troubleshooting Errors, Alarms and Reports

This chapter contains the following sections:

- [Alarms](#)
- [Errors](#)
- [User Summary Reports](#)

4.1 Alarms

Table 3: List of Alarms and its Resolution

Scenario	Alarm Text	Severity	Resolution
When CL Adapter is down	ERROR – AUTHSERVICE_DOWN	High	Restart the CL Adapter service using command: service cladapter restart
When CL platform could not be connected from CL Adapter	ERROR – CL_CONNECT_FAILURE	High	Check the network connection between MiCollab and CL Platform
SAS rest service is down	ERROR – REST_CONNECT_FAILURE	High	Restart the SAS Rest service using command: service restserver restart
CL Adapter connection with CL platform breaks momentarily	ERROR – CL_CONNECT_FAILURE	Medium	Check the network connection between MiCollab and CloudLink Platform

4.2 Errors

Table 4: List of Errors and its Resolution

Scenario	Error String	Resolution
When Administrator tries to enable CL Auth from BUP	Failed to enable CloudLink Authentication.	Check the connection to CL platform. Restart mom-server using command service mom-server restart Contact Mitel Support with issue and log details
When Administrator tries to disable CL Auth from BUP	Failed to disable CloudLink Authentication.	
When Administrator tries to re-send CL Account setup Email	Failed to send CloudLink Account setup Email.	

4.3 User Summary Reports

This report lists the following information for the MiCollab users:

- User's First Name
- User's Last Name
- Email Address
- UCC Bundle
- Department
- Location

External References and Links

5

Table 5: External references

Serial number	Description	External Link
1	This is an attribute mapping link for Entra ID Admin programming. The AD attribute can be configured via the Entra ID portal.	https://docs.microsoft.com/en-us/powershell/azure/active-directory/using-extension-attributes-sample?view=azureadps-2.0
2	CloudLink documentation for setting up Entra ID Sync	https://www.mitel.com/en-ca/document-center/technology/cloudlink/all-releases/en/cloudlink-accounts-html
3	MiCollab Solution Document - CloudLink	https://www.mitel.com/document-center/applications/collaboration/micollab/micollab-server/913/en/micollab-cloudlink-solution-document
4	Entra ID portal	https://portal.azure.com/#home

