A MITEL
PRODUCT
GUIDE

MiCollab Solution Document — CloudLink Authentication and Synchronization

Release 10.0

February 2025

Mitel
Powering connections

Notices

Trademarks

Contents

CloudLink-based Authentication 1

This chapter contains the following sections:

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 Azure Active Directory (AD) at the CloudLink back end. An Identity Provider such as Azure AD 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/Azure AD Authentication on MiCollab Clients can be used to cross-launch CloudLink applications such as MiTeam Meetings, thus providing a seamless single sign-on experience across Mitel Applications. This is not valid for 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.

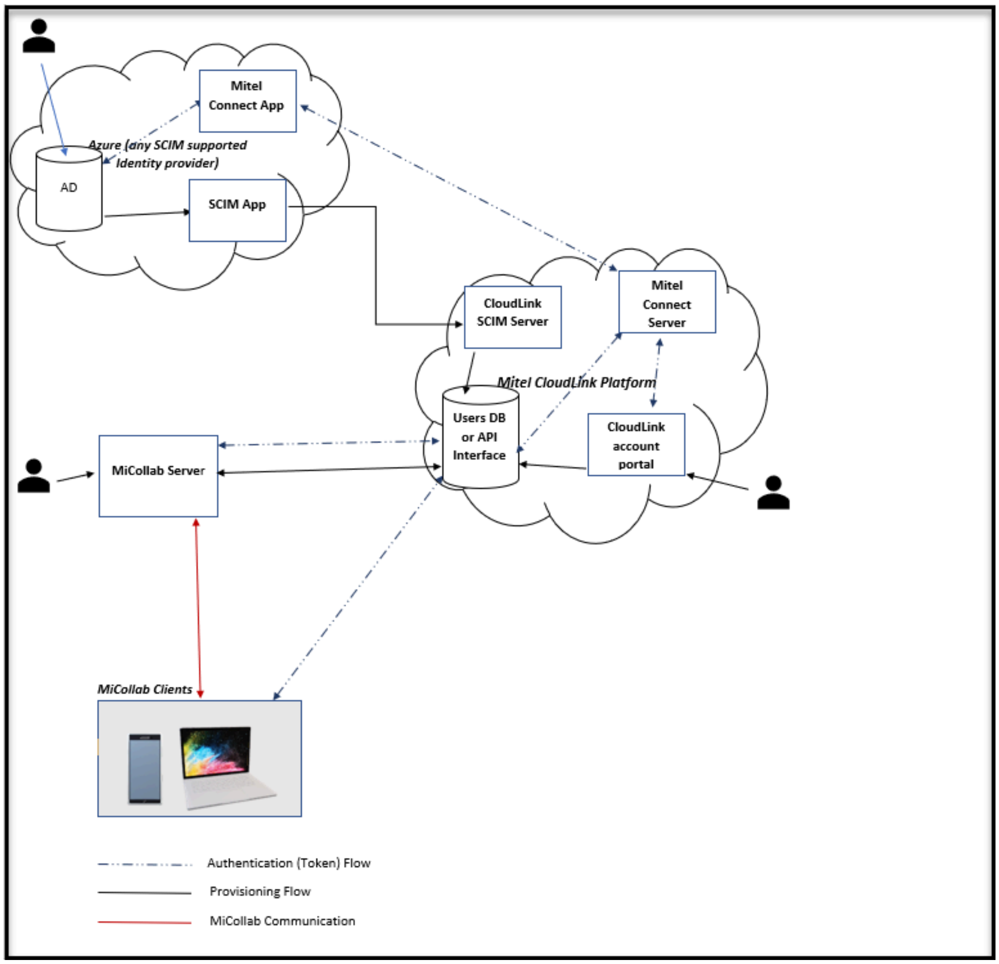


Figure 1: Data Flow Diagram between MiCollab, CloudLink and Azure

1.1 Prerequisites and Supported Platforms

- CloudLink/Azure AD 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/Azure AD 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 Azure AD 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 Azure AD CloudLink Sync MiCollab integrations

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

1.2 Microsoft Azure Active Directory to CloudLink

Note:
The information contained within this section on CloudLink or Azure 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 Azure AD.

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

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

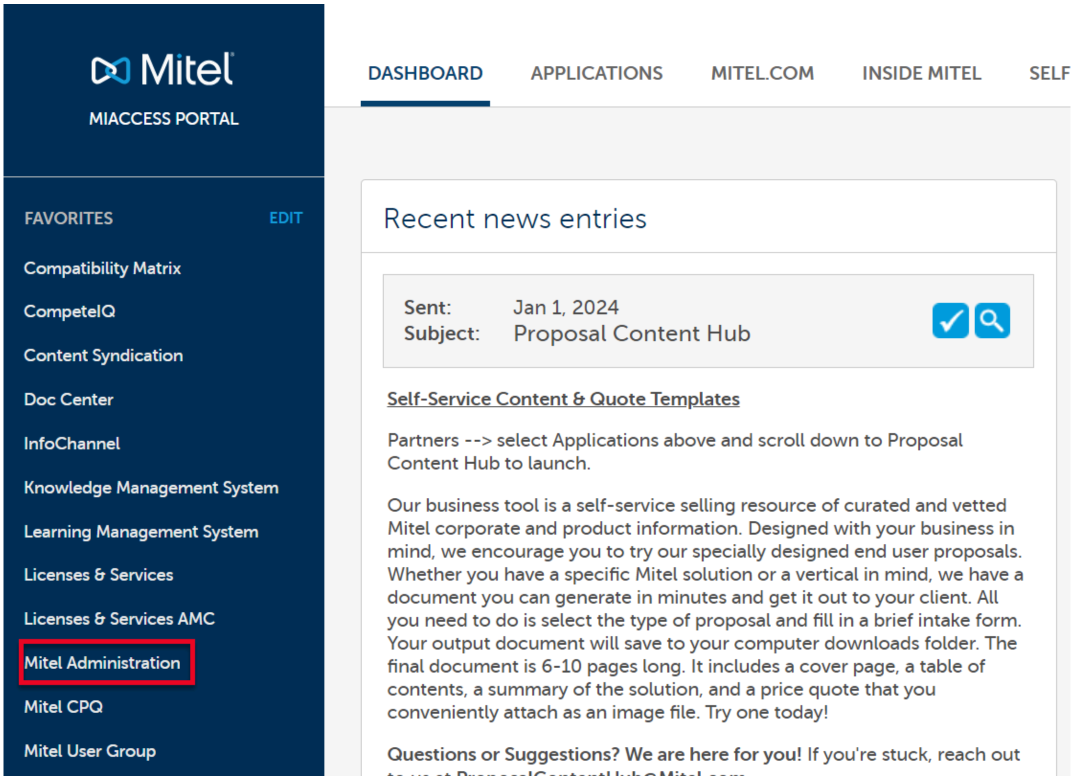
- An Azure AD subscription
- A Mitel CloudLink account

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**.



Recent news entries

Sent: Jan 1, 2024
Subject: Proposal Content Hub

Self-Service Content & Quote Templates

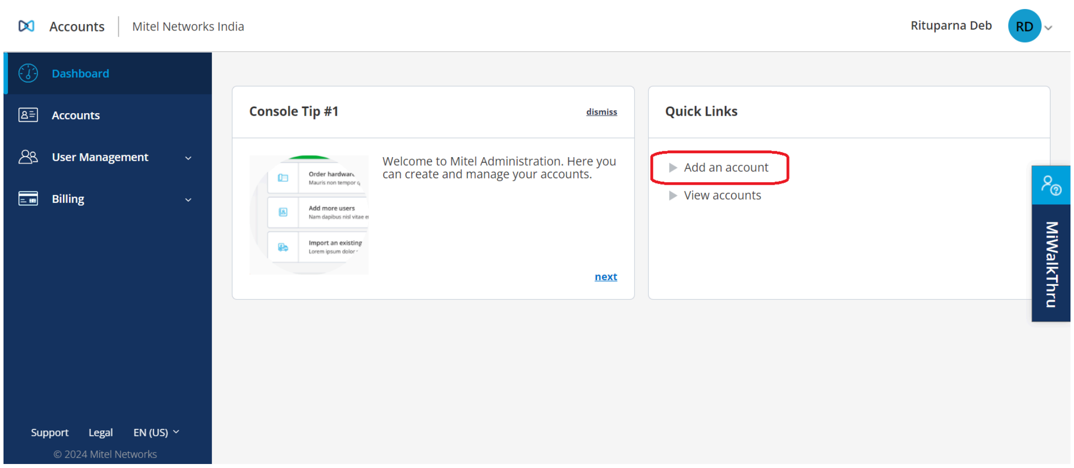
Partners --> select Applications above and scroll down to Proposal Content Hub to launch.

Our business tool is a self-service selling resource of curated and vetted Mitel corporate and product information. Designed with your business in mind, we encourage you to try our specially designed end user proposals. Whether you have a specific Mitel solution or a vertical in mind, we have a document you can generate in minutes and get it out to your client. All you need to do is select the type of proposal and fill in a brief intake form. Your output document will save to your computer downloads folder. The final document is 6-10 pages long. It includes a cover page, a table of contents, a summary of the solution, and a price quote that you conveniently attach as an image file. Try one today!

Questions or Suggestions? We are here for you! If you're stuck, reach out

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

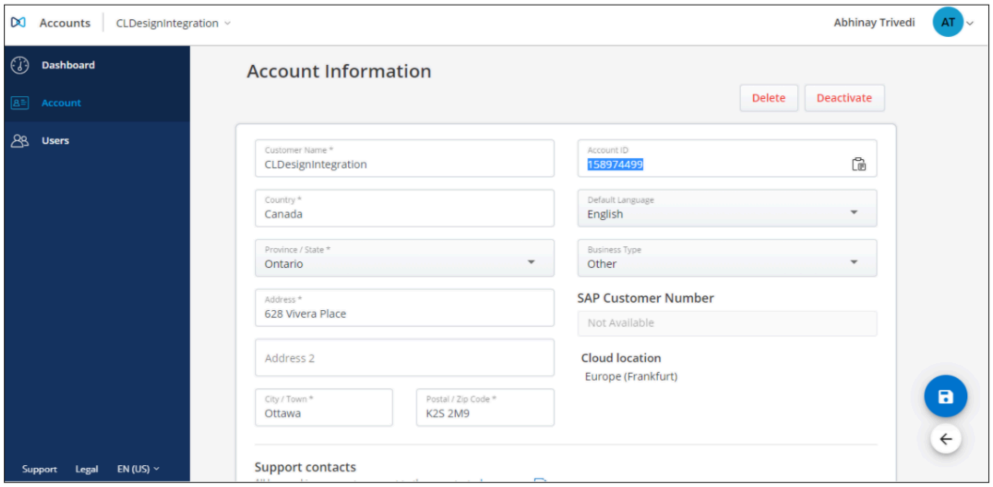
   If the customer account already exists, you can skip this step, search for the customer account under Accounts and proceed to step 4.



Welcome to Mitel Administration. Here you can create and manage your accounts.

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



Account Information

Customer Name * CLDesignIntegration

Account ID 158974499

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)

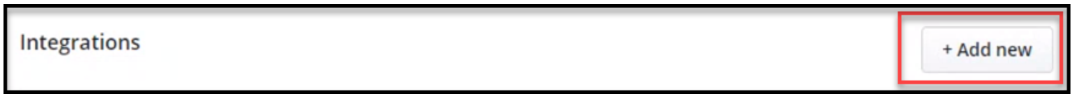
City / Town * Ottawa

Postal / Zip Code * K2S 2M9

Support contacts

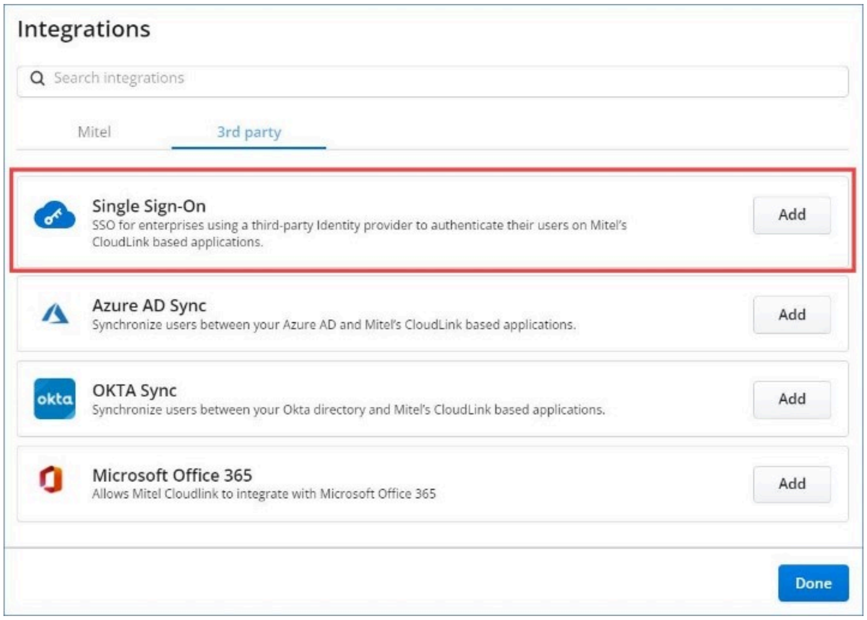
5. In the Integrations section, click **+ Add new**.

   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**.



Integrations

Single Sign-On
SSO for enterprises using a third-party Identity provider to authenticate their users on Mitel's CloudLink based applications.

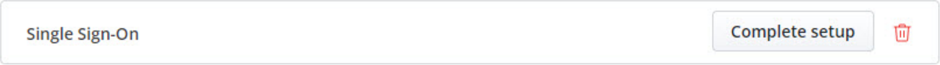
Azure AD Sync
Synchronize users between your Azure AD and Mitel's CloudLink based applications.

OKTA Sync
Synchronize users between your Okta directory and Mitel's CloudLink based applications.

Microsoft Office 365
Allows Mitel Cloudlink to integrate with Microsoft Office 365

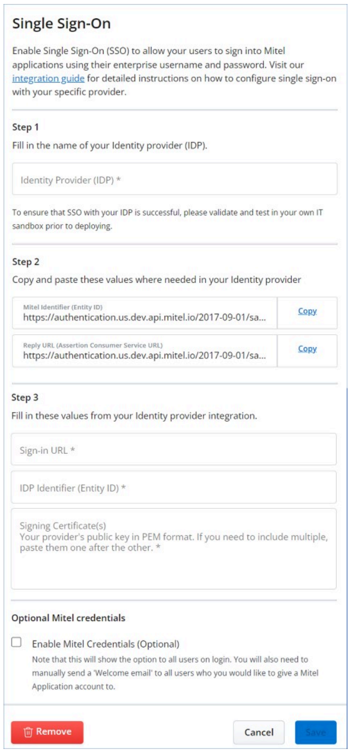
The **Single Sign-On** is enabled for the customer account and is added to the **Integrations** section of the **Account Information** page.

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



Single Sign-On

- An integration guide link is provided that will outline the rest of the setup for Single Sign-on and integration with Azure.



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.

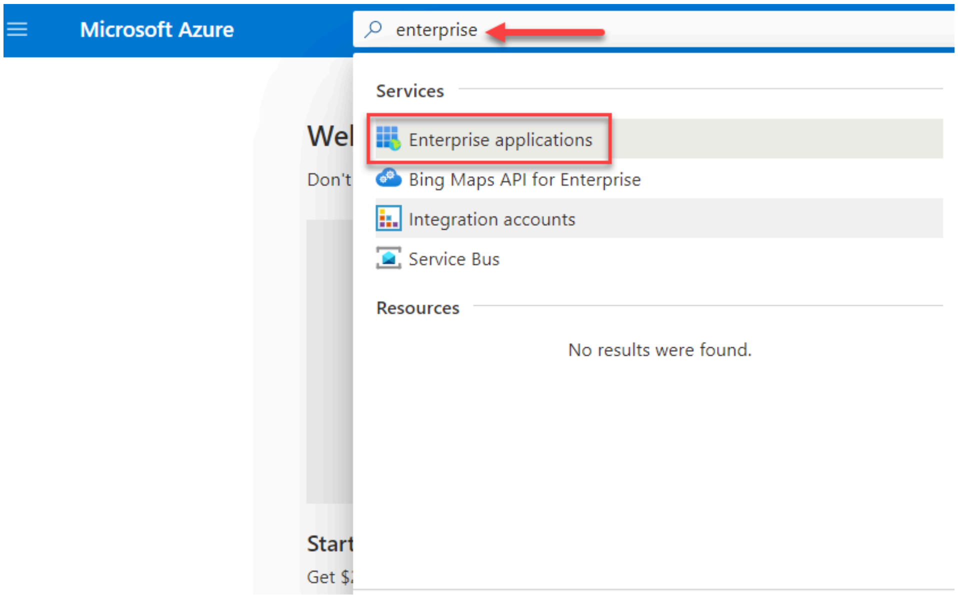
This completes the steps necessary to integrate the CloudLink Account with the customer Azure AD.

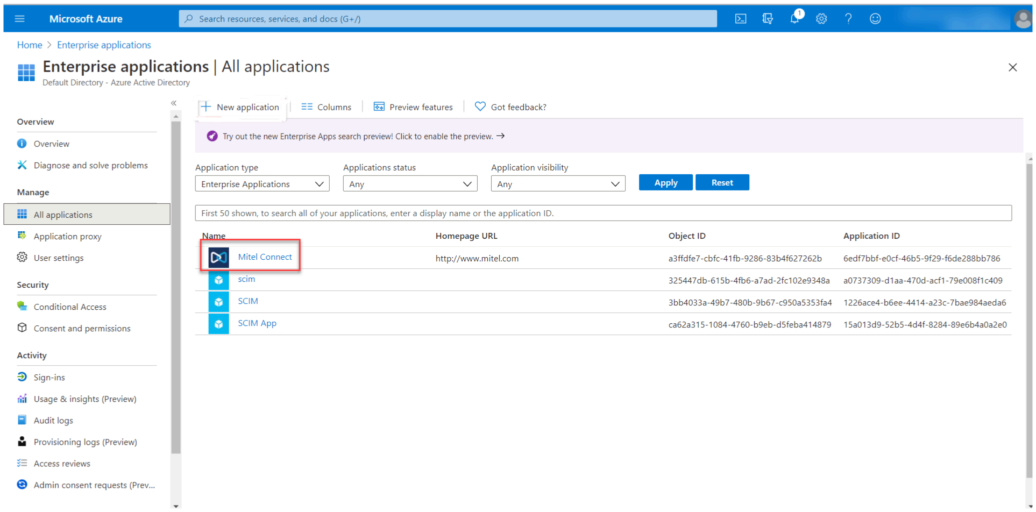
For new customer sites, the CloudLink Account must now be integrated with MiCollab. The steps required are identical to setting up the CloudLink based chat on MiCollab. See the MiCollab Solution Document-CloudLink for steps to Enable CloudLink Integration.

1.4 Adding a user on Azure in Mitel Connect

There are multiple ways to add users in Azure AD through UI, CSV import, PowerShell, etc. The user creation in Azure AD 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 Azure Mitel Connect app once the user is created in Azure AD.

1. Search for Enterprise Applications on Azure AD and select **Mitel Connect** application.



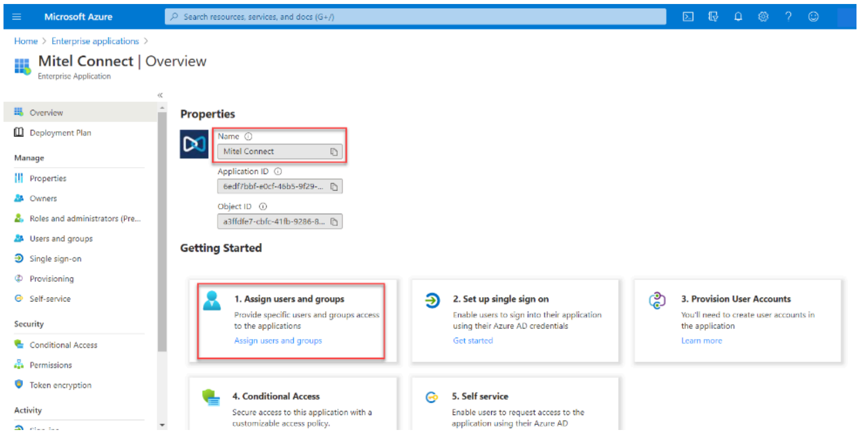

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications
Enterprise applications | All applications
Default Directory - Azure Active Directory
New application
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Consent and permissions
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Prev...
Try out the new Enterprise Apps search preview! Click to enable the preview. →
Apply
Reset

Application type: Enterprise Applications
Applications status: Any
Application visibility: Any

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

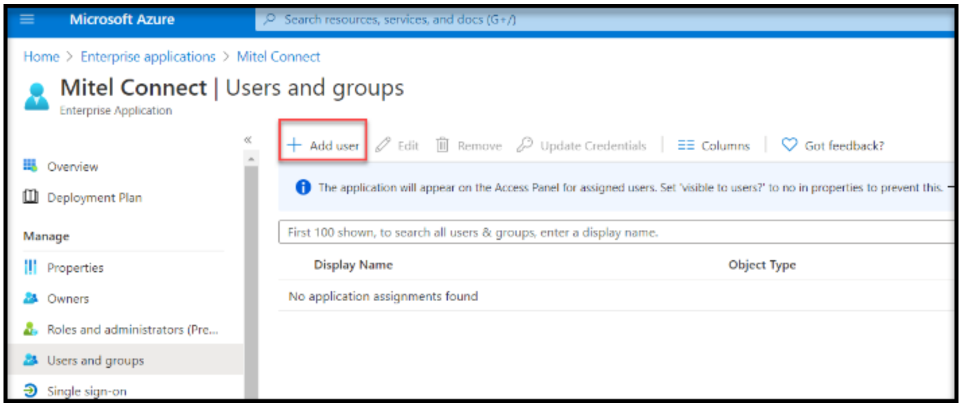
Name	Homepage URL	Object ID	Application ID
Mitel Connect	http://www.mitel.com	a3ffdfe7-cbfc-41fb-9286-83b4f627262b	6edf7bbf-e0cf-46b5-9f29-f6de288bb786
scim		325447db-615b-4fb6-a7ad-2fc102e9348a	a0737309-d1aa-470d-acf1-79e008f1c409
SCIM		3bb4033a-49b7-480b-9b67-c950a5353fa4	1226ace4-b6ee-4414-a23c-7bae984aeda6
SCIM App		ca62a315-1084-4760-b9eb-d5feba414879	15a013d9-52b5-4d4f-8284-89e6b4a0a2e0

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


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications >
Mitel Connect | Overview
Enterprise Application
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Pre...
Users and groups
Single sign-on
Provisioning
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Properties
Getting Started
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started
3. Provision User Accounts
You'll need to create user accounts in the application
Learn more
4. Conditional Access
Secure access to this application with a customizable access policy.
5. Self service
Enable users to request access to the application using their Azure AD

Name: Mitel Connect
Application ID: 6edf7bbf-e0cf-46b5-9f29-...
Object ID: a3ffdfe7-cbfc-41fb-9286-8...

3. Click **Add user**.

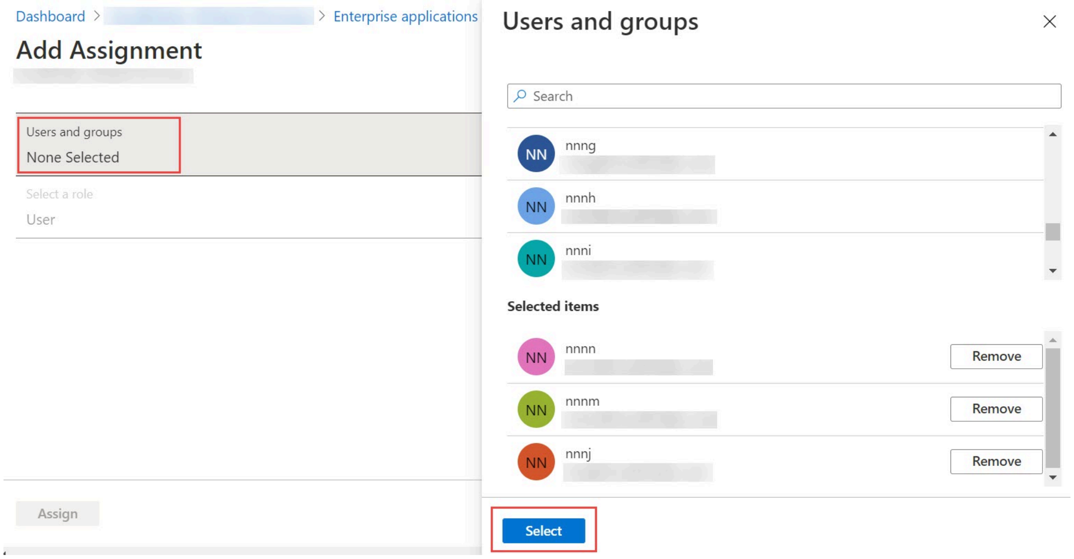


The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

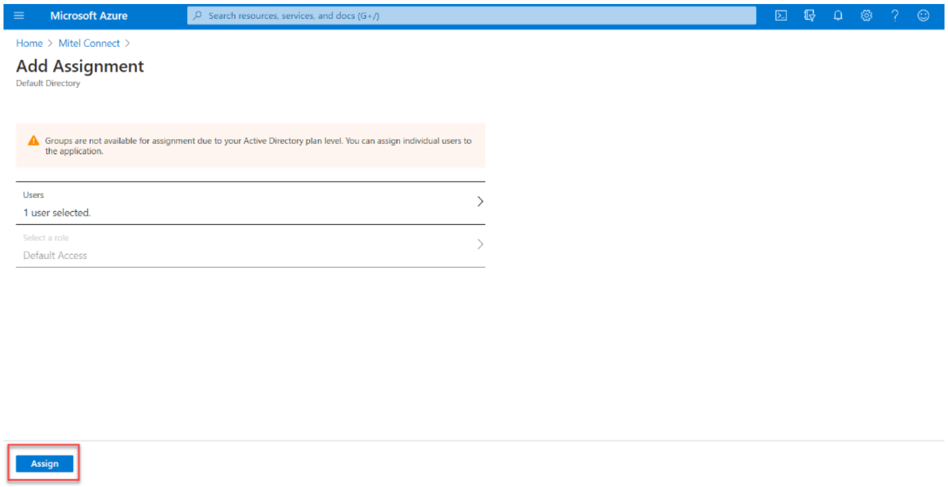
First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

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

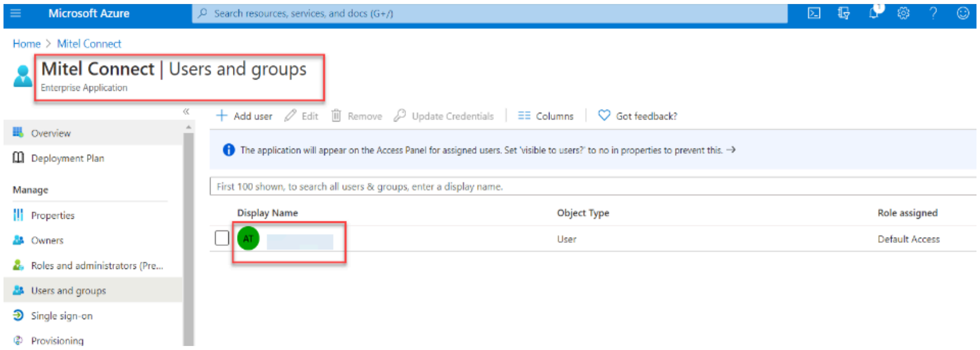


5. Once the user is selected, click on **Assign.**



Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

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



The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	AT [redacted]	User	Default Access

7. All users listed under the Enterprise Application - Mitel Connect should appear on CloudLink account portal. Before troubleshooting MiCollab, ensure that users from Azure AD 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 Azure AD 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/Azure AD authentication for IDS

Limitations:

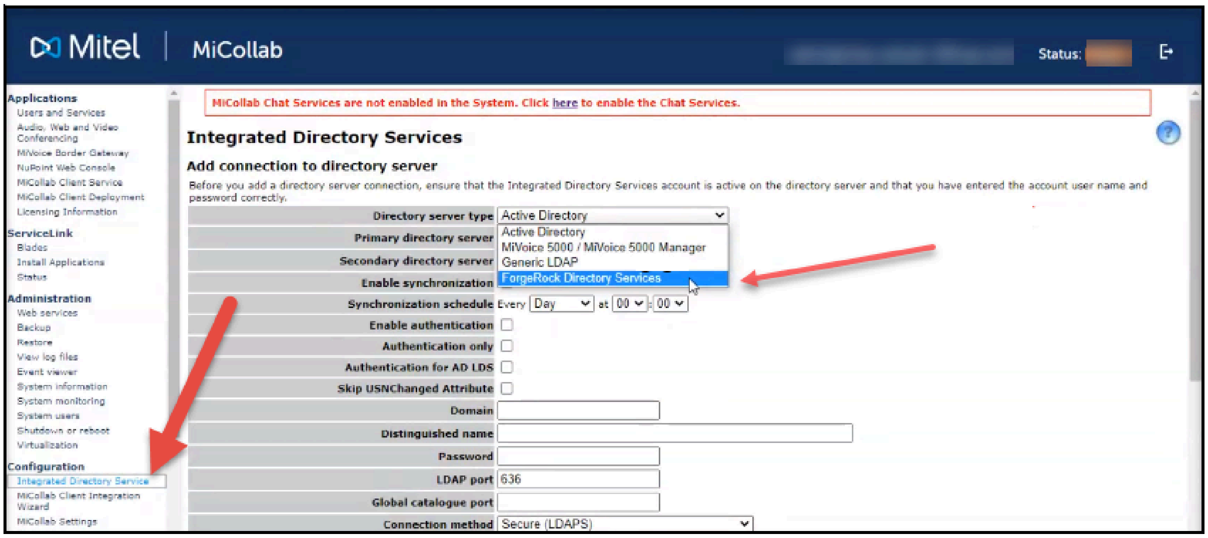
The following features are not supported with CloudLink IDS:

- 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



MiCollab Chat Services are not enabled in the System. Click here to enable the Chat Services.

Integrated Directory Services

Add connection to directory server

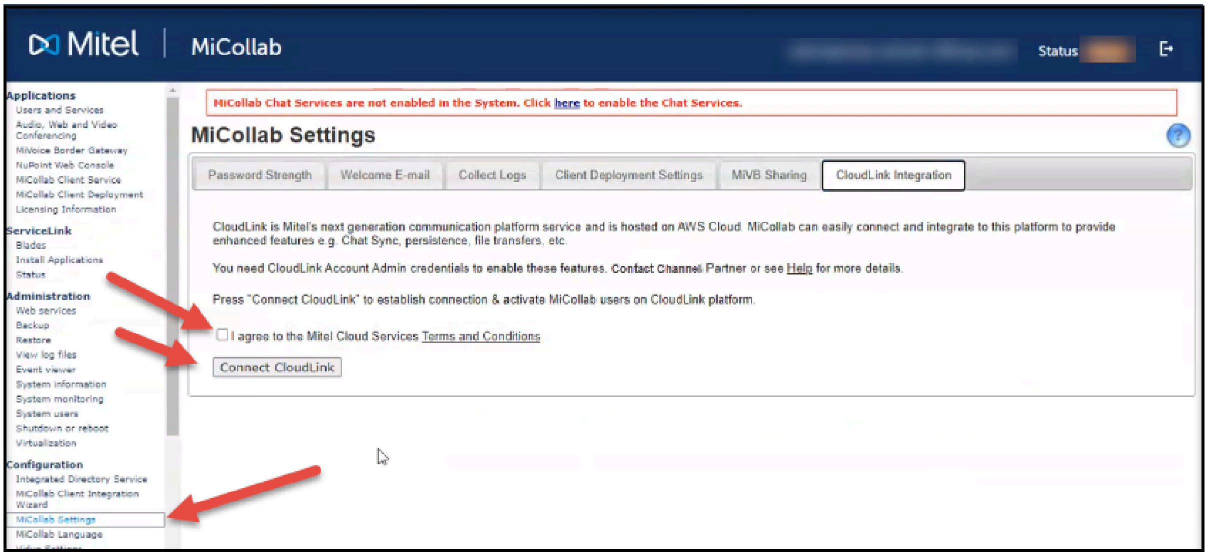
Before you add a directory server connection, ensure that the Integrated Directory Services account is active on the directory server and that you have entered the account user name and password correctly.

Directory server type	Active Directory
Primary directory server	
Secondary directory server	
Enable synchronization	
Synchronization schedule	Every Day at 00 : 00
Enable authentication	☐
Authentication only	☐
Authentication for AD LDS	☐
Skip USNChanged Attribute	☐
Domain	
Distinguished name	
Password	
LDAP port	636
Global catalogue port	
Connection method	Secure (LDAPS)

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.



MiCollab Chat Services are not enabled in the System. Click here to enable the Chat Services.

MiCollab Settings

CloudLink is Mitel's next generation communication platform service and is hosted on AWS Cloud. MiCollab can easily connect and integrate to this platform to provide enhanced features e.g. Chat Sync, persistence, file transfers, etc.

You need CloudLink Account Admin credentials to enable these features. Contact Channel Partner or see Help for more details.

Press "Connect CloudLink" to establish connection & activate MiCollab users on CloudLink platform.

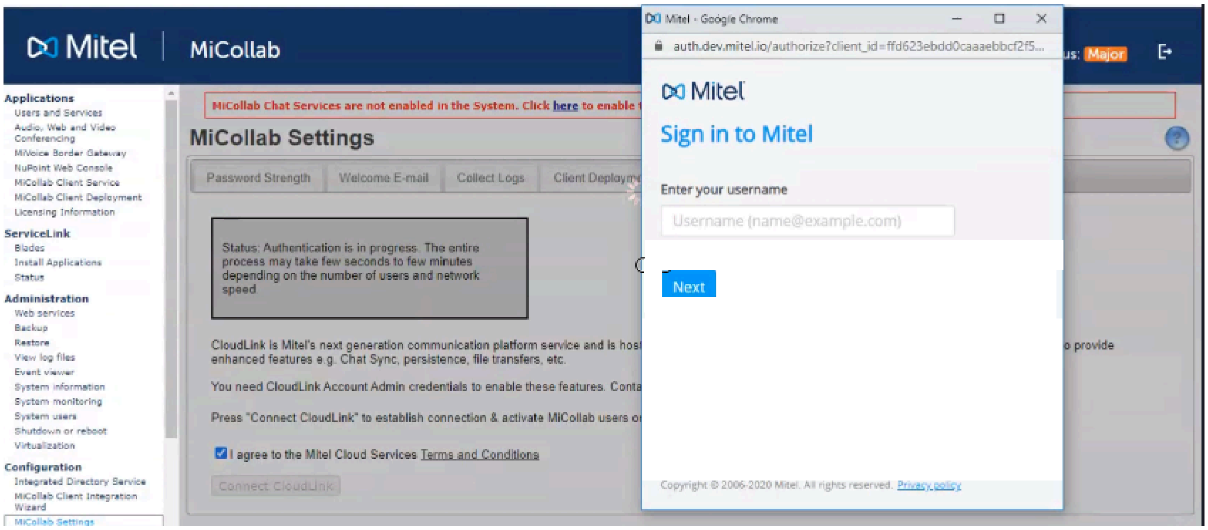
☐ I agree to the Mitel Cloud Services Terms and Conditions

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).



MiCollab Chat Services are not enabled in the System. Click here to enable t

MiCollab Settings

Status: Authentication is in progress. The entire process may take few seconds to few minutes depending on the number of users and network speed.

CloudLink is Mitel's next generation communication platform service and is host … o provide enhanced features e.g. Chat Sync, persistence, file transfers, etc.

You need CloudLink Account Admin credentials to enable these features. Conta

Press "Connect CloudLink" to establish connection & activate MiCollab users o

☑ I agree to the Mitel Cloud Services Terms and Conditions

auth.dev.mitel.io/authorize?client_id=ffd623ebdd0caaaebbcf2f5...

Sign in to Mitel

Enter your username

Username (name@example.com)

Copyright © 2006-2020 Mitel. All rights reserved. Privacy policy

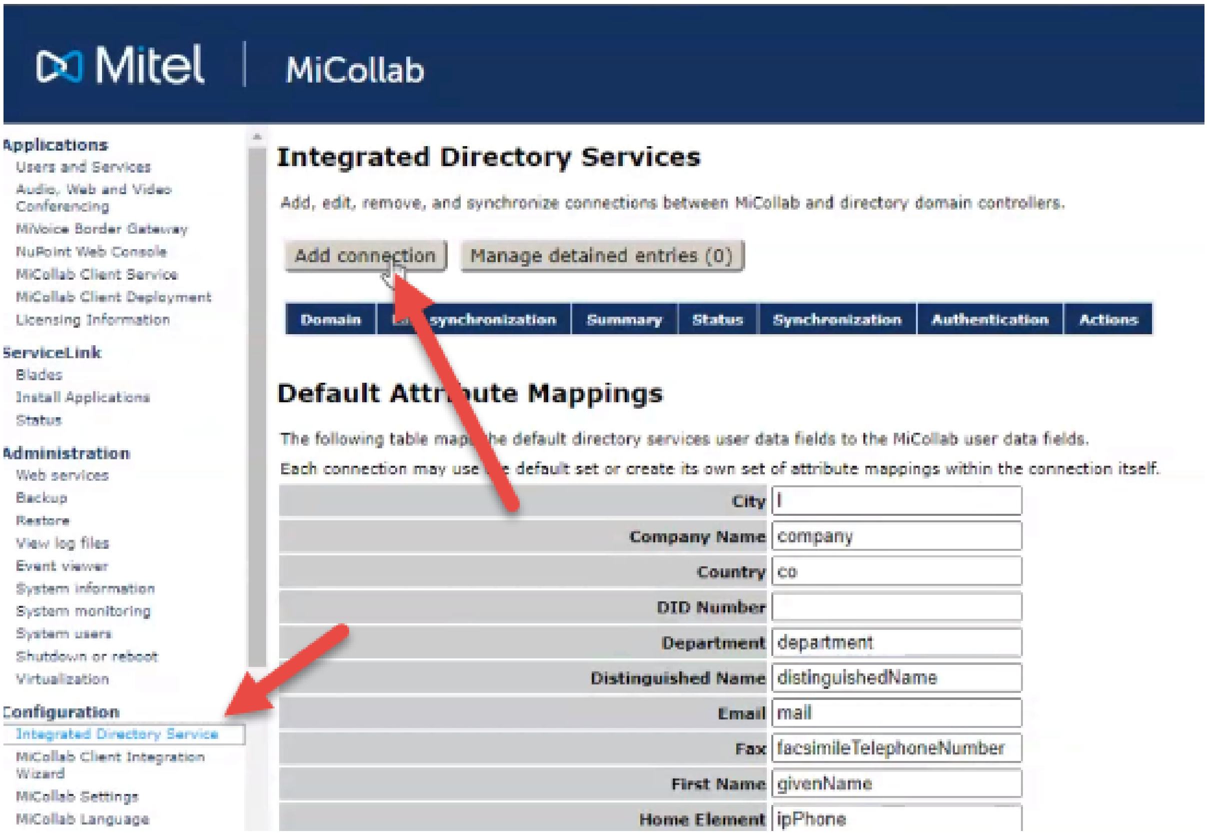
- Enter your Username (Email address)
- Enter your Password

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.

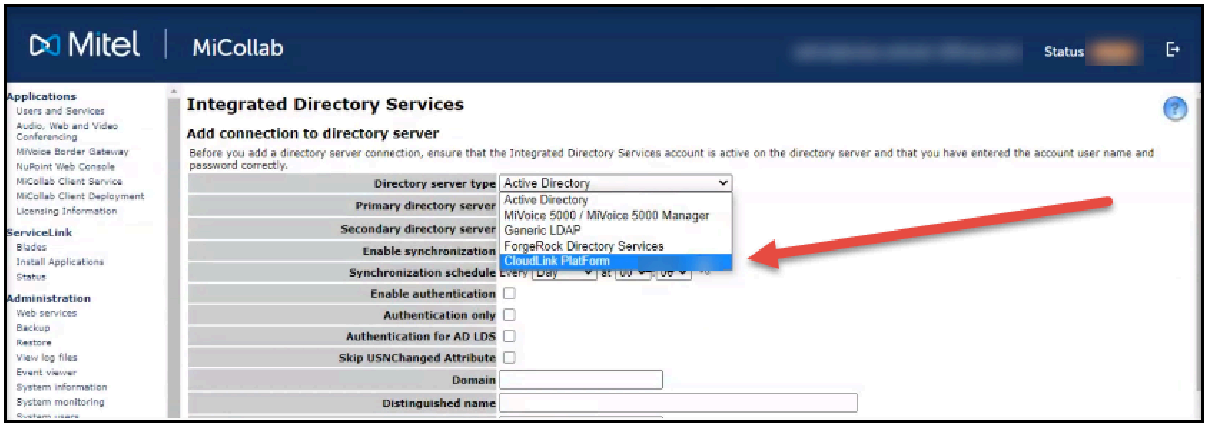
Default Attribute Mappings

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	l
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.



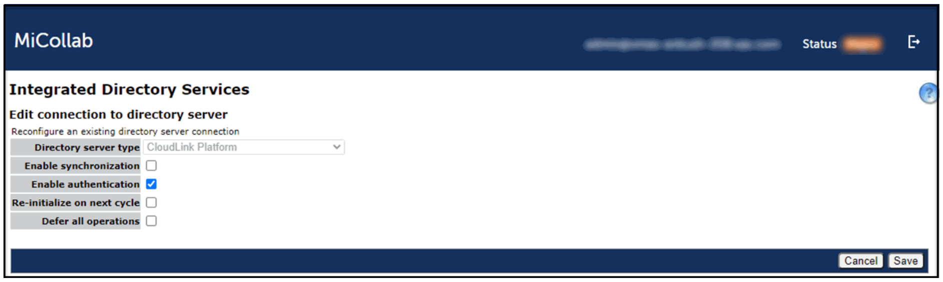
Integrated Directory Services

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	
Secondary directory server	
Enable synchronization	
Synchronization schedule	Every Day at 00 : 00
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.**



Integrated Directory Services

Edit connection to directory server

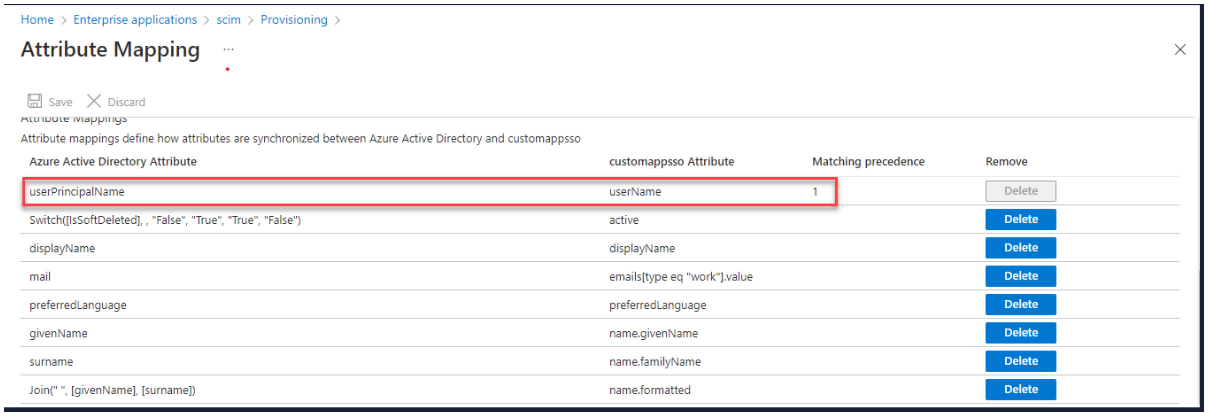
Reconfigure an existing directory server connection

Directory server type	CloudLink Platform
Enable synchronization	□
Enable authentication	☑
Re-initialize on next cycle	□
Defer all operations	□

Once the CloudLink/Azure AD 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 Azure AD (in this example) via CloudLink instead of MiCollab.

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.



Attribute Mapping

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
displayName	displayName		Delete
mail	emails[type eq "work"].value		Delete
preferredLanguage	preferredLanguage		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
Join(" ", [givenName], [surname])	name.formatted		Delete

Note:

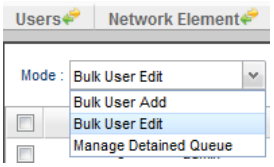
From R9.5 onwards, for performing the CloudLink Authentication procedure, the migrated user's login ID becomes the same as their Email ID. This behavior is valid for all the first-time users performing CloudLink Authentication. In case of manually or locally enabling and disabling CloudLink Auth from 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.



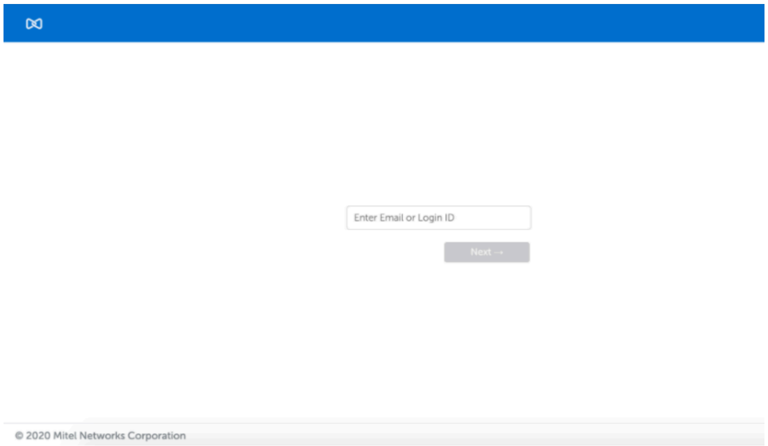
4. Click on **Load Users**.
5. Select the users for whom the CloudLink-based Authentication needs to be disabled.
6. Click on the **Disable CL Auth** button.

   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.

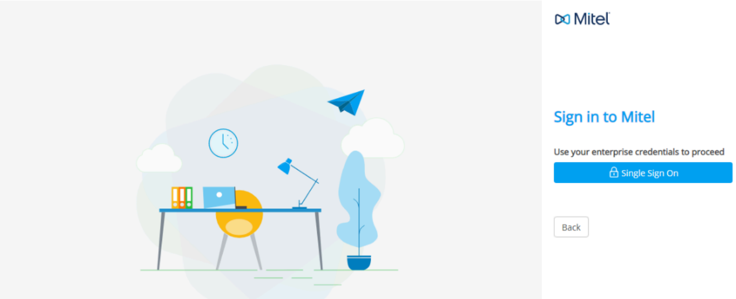
1.5.5 Using CloudLink-based Authentication on the MiCollab Clients

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.**



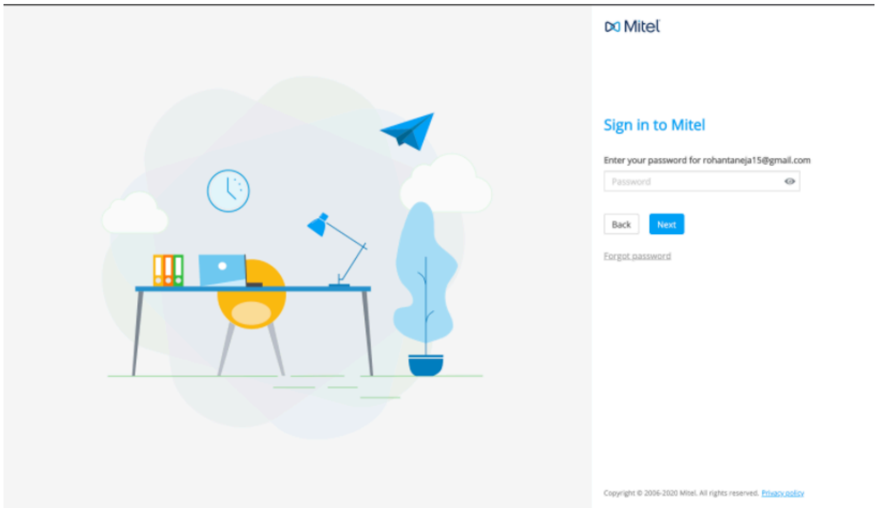
3. If CloudLink-based Authentication is enabled for the user, the MiCollab client will proceed for subsequent login through the CloudLink Unified login page.

- Azure AD is integrated: In the CloudLink Authorization page, use your enterprise credentials to login.
- Azure AD 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.



Use your enterprise credentials to proceed

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



Mitel

Sign in to Mitel

Enter your password for rohantaneja15@gmail.com

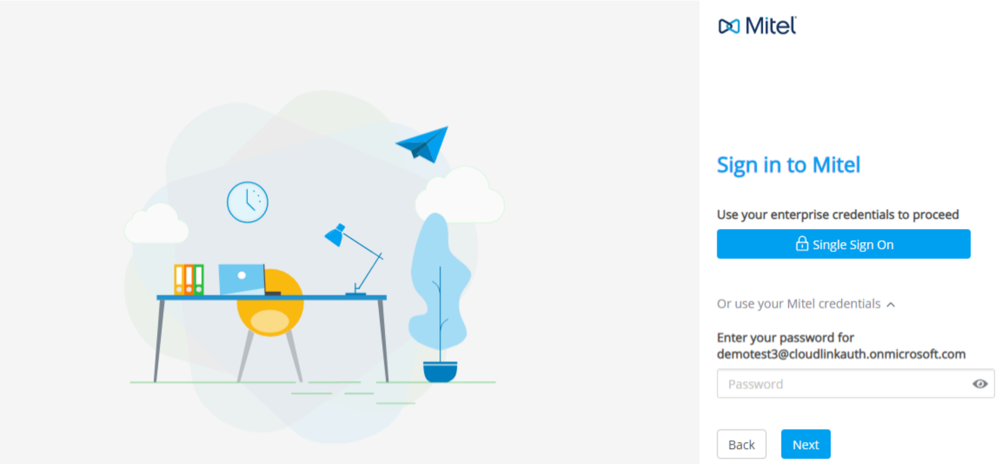
Password

Back Next

Forgot password

Copyright © 2006-2020 Mitel. All rights reserved. Privacy policy

- Azure AD 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.io to setup your password).



Mitel

Sign in to Mitel

Use your enterprise credentials to proceed

Single Sign On

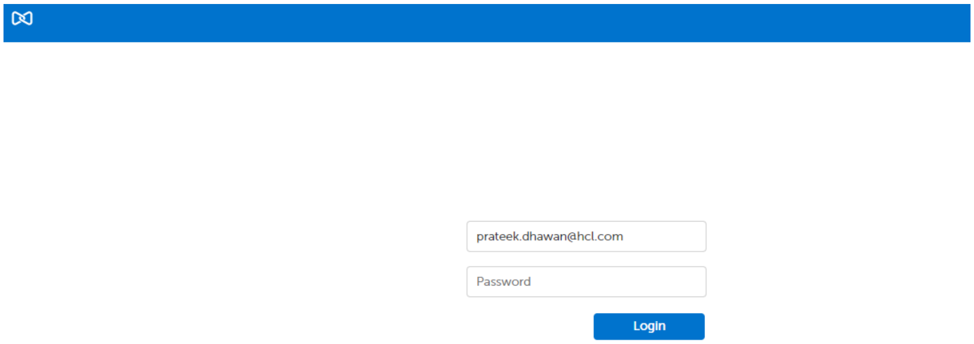
Or use your Mitel credentials ^

Enter your password for demotest3@cloudlinkauth.onmicrosoft.com

Password

Back Next

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.

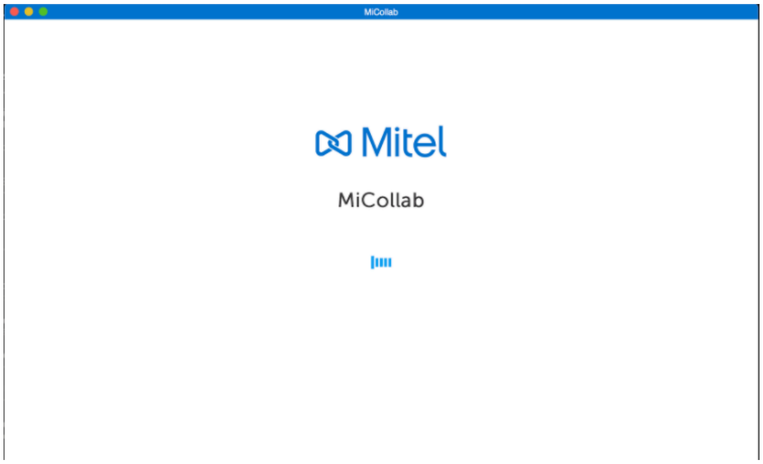


prateek.dhawan@hcl.com

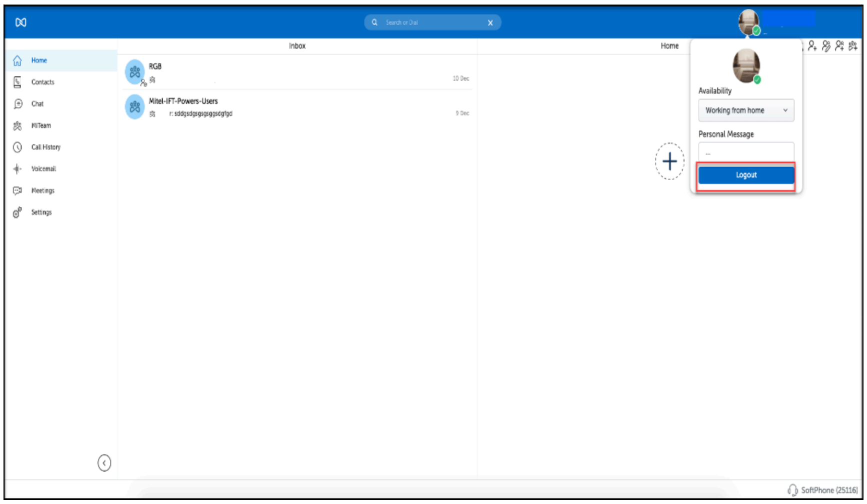
Password

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.



RGB — 10 Dec

Mitel-IFT-Powers-Users — r: sddgsdgsgsgsgsdgfgd — 9 Dec

Availability: Working from home

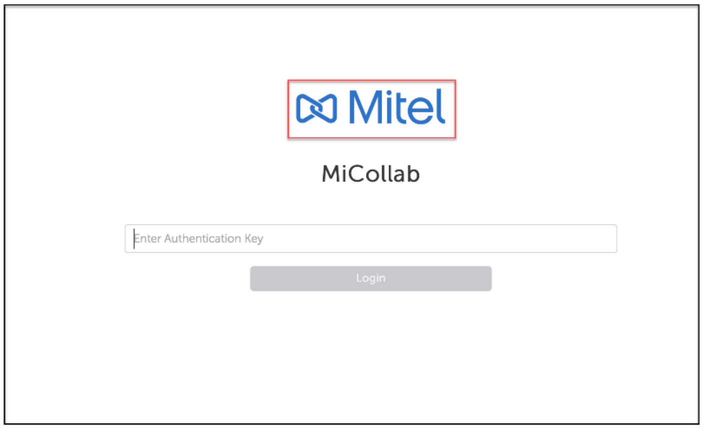
Personal Message: ...

1.5.6 Manual login for native clients

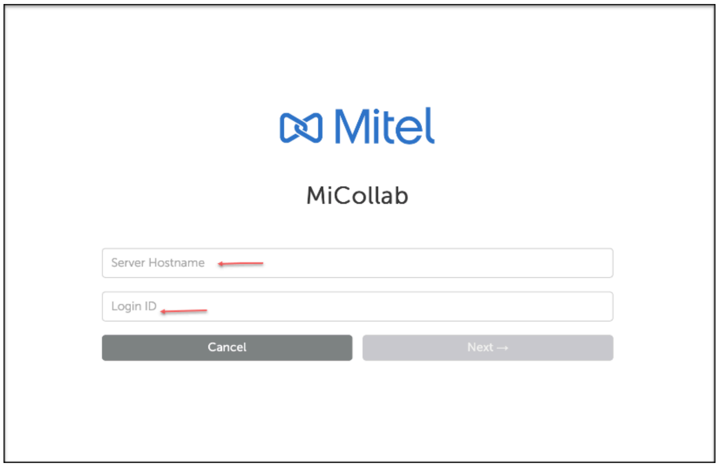
CloudLink Authentication also supports manual login in native clients (iOS, Android, PC, and MAC OS).

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

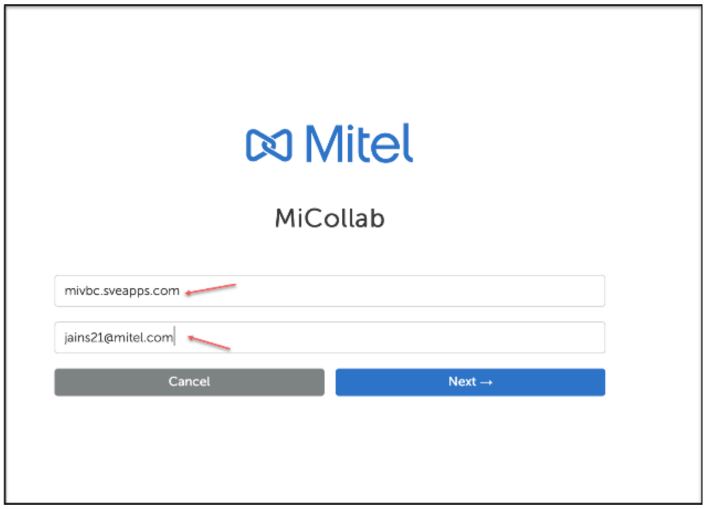
1. Tap on the Mitel logo three times to open the Manual Login screen.



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



3. Click **Next**.

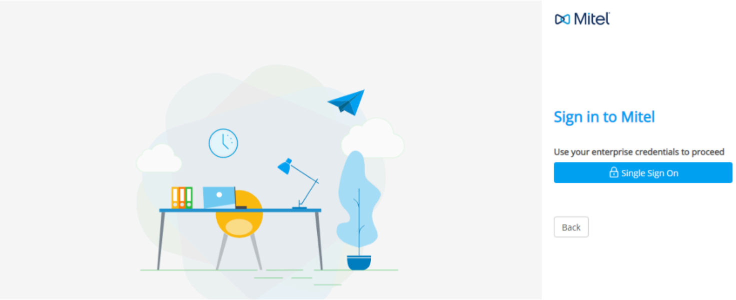


mivbc.sveapps.com

jains21@mitel.com

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

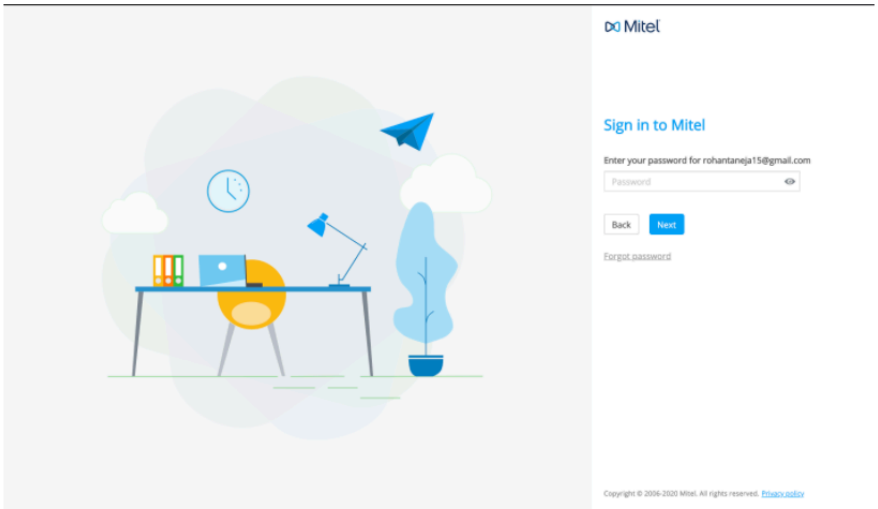
   - Azure AD is integrated: In the CloudLink Authorization page, use your enterprise credentials to login.
   - Azure AD is not integrated: In the CloudLink Authorization page, use your CloudLink password. This password must be set up with the help of CloudLink Welcome Email. Check Emails from no-reply@mitel.ioto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



Sign in to Mitel

Use your enterprise credentials to proceed

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

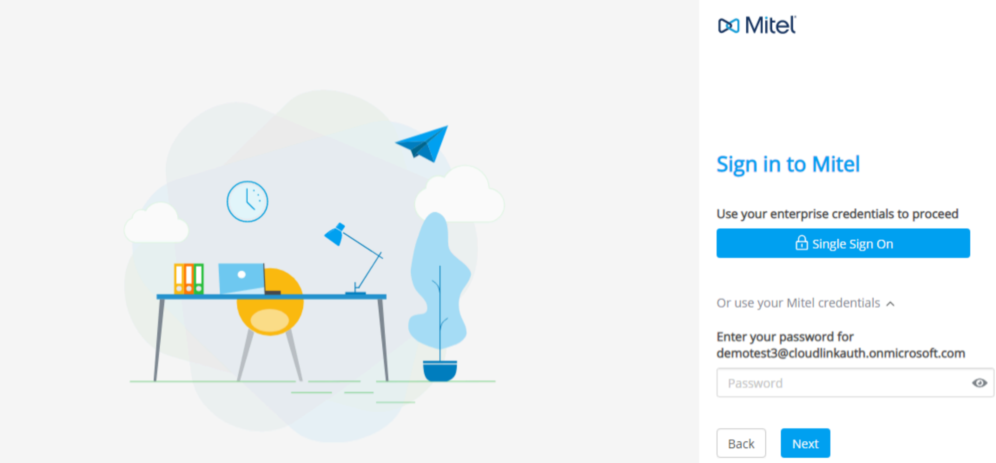


Sign in to Mitel

Enter your password for rohantaneja15@gmail.com

Copyright © 2006-2020 Mitel. All rights reserved. Privacy policy

- Azure AD 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).

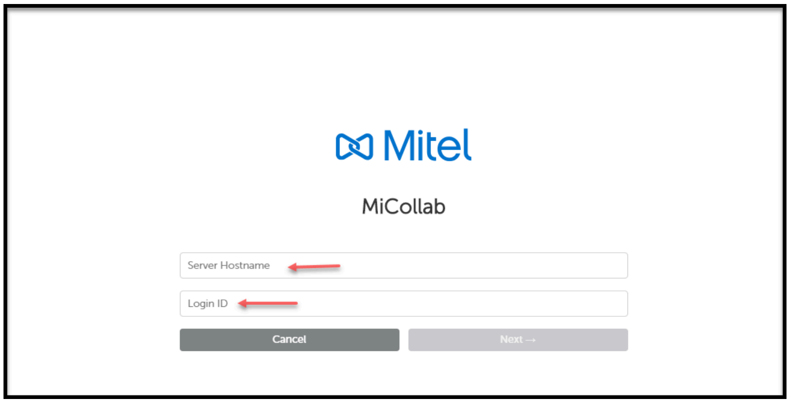


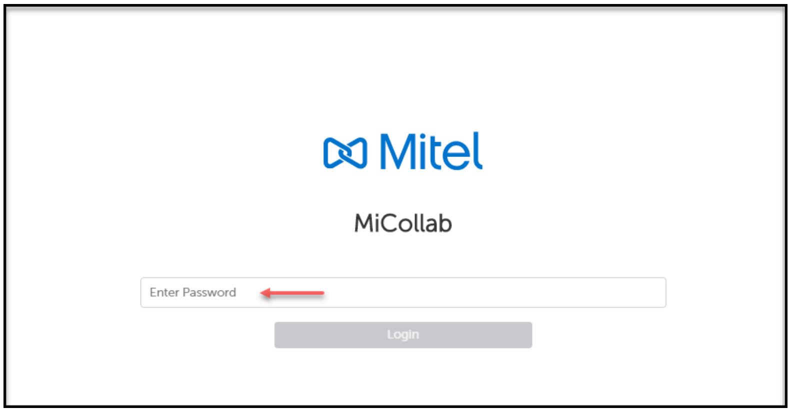
Sign in to Mitel

Use your enterprise credentials to proceed

Enter your password for demotest3@cloudlinkauth.onmicrosoft.com

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.





CloudLink-based Synchronization 2

This chapter contains the following sections:

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 Azure AD with the help of SCIM interface to extend the user provisioning and management directly from the Azure AD 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.

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.

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 Azure must be in **e.164** format. For example, +16135922122 and +441291436000.

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

2.2 Limitations

The following fields are not supported on Azure/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 Azure AD

   - 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 Azure AD 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 Azure AD side. As an alternate solution, the administrator can set a particular character like "-" or a string "<*blank*>" instead of null fields on Azure. 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.

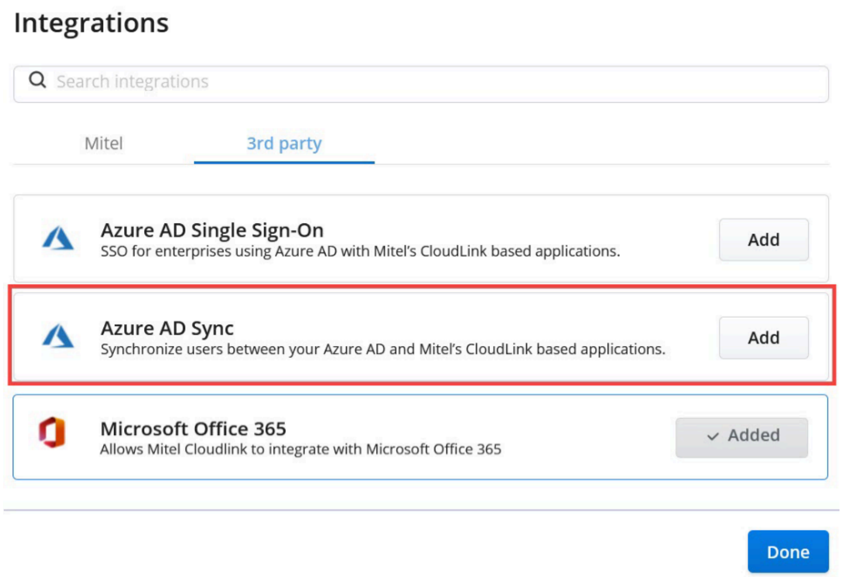
2.3 Setting up CloudLink Account for SCIM integration

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 Azure AD Sync as shown below:
  - Select the **Add** button beside Azure AD Sync.
  - Select **Done**.



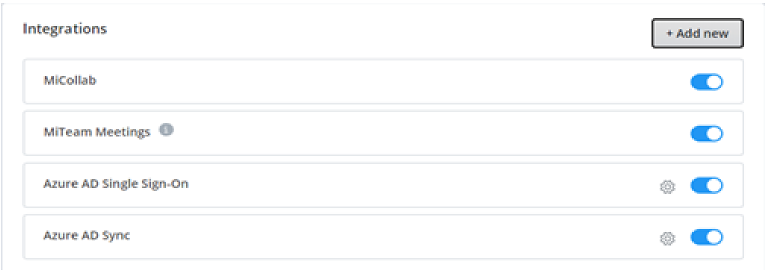
Integrations

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

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

Microsoft Office 365
Allows Mitel Cloudlink to integrate with Microsoft Office 365

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



Integrations

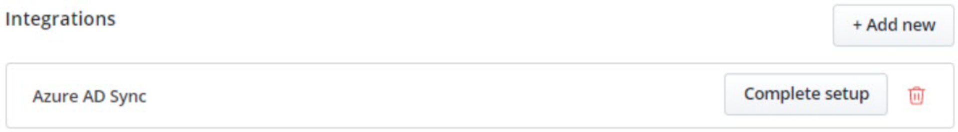
MiCollab

MiTeam Meetings

Azure AD Single Sign-On

Azure AD Sync

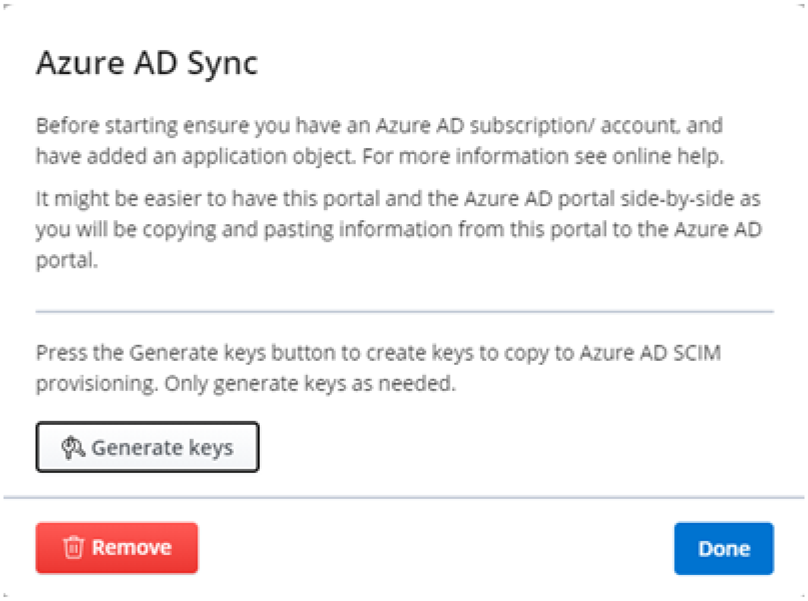
Click on **Complete setup**.



Integrations

Azure AD Sync

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.

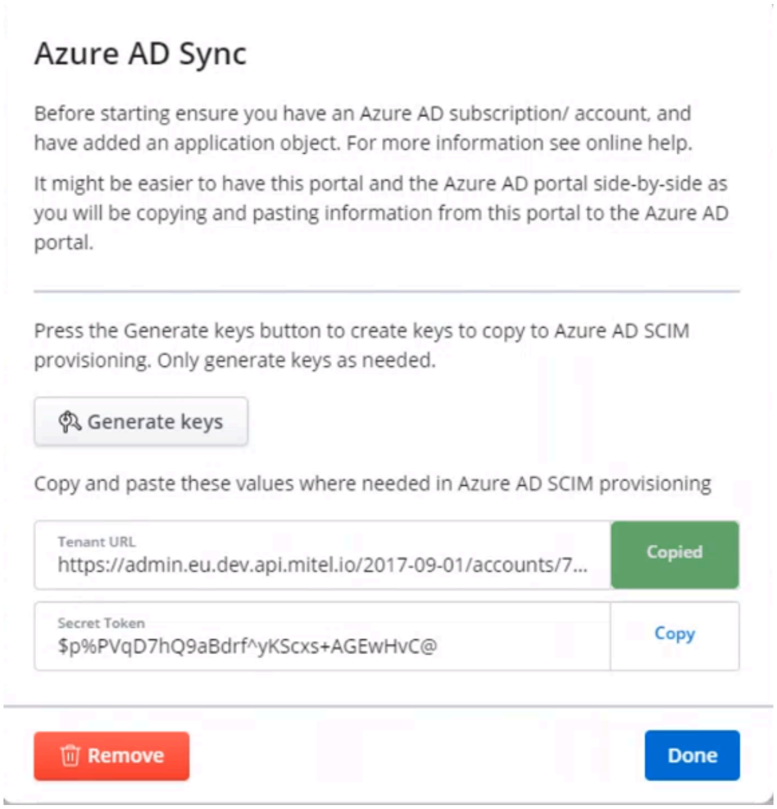
Click on **Copy** against the **Tenant URL** text field and **Secret Token** text field and save the values, as these values would be required to be entered on Azure portal SCIM app configuration.

The keys generated will be used by the customer site IT personal for the Azure AD 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 Azure AD 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.

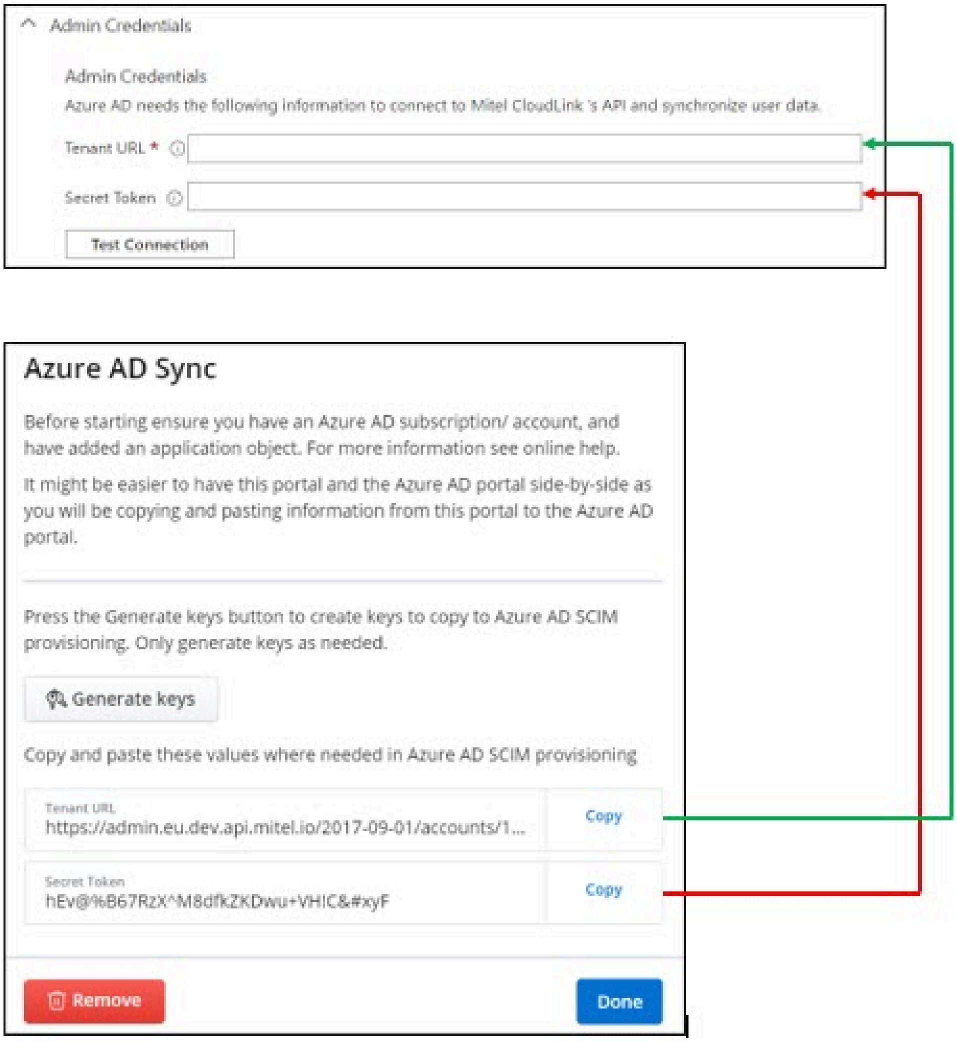
It might be easier to have this portal and the Azure AD portal side-by-side as you will be copying and pasting information from this portal to the Azure AD portal.

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

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...

Secret Token
$p%PVqD7hQ9aBdrf^yKScxs+AGEwHvC@



Admin Credentials

Admin Credentials

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

Tenant URL *

Secret Token

Test Connection

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/1... Copy

Secret Token
hEv@%B67RzX^M8dfkZKDwu+VHIC&#xyF Copy

Remove Done

2.4 Setting up the Provisioning Server (Azure AD)

The information contained within this section on CloudLink or Azure 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 Azure AD for the provisioning and management of MiCollab users.

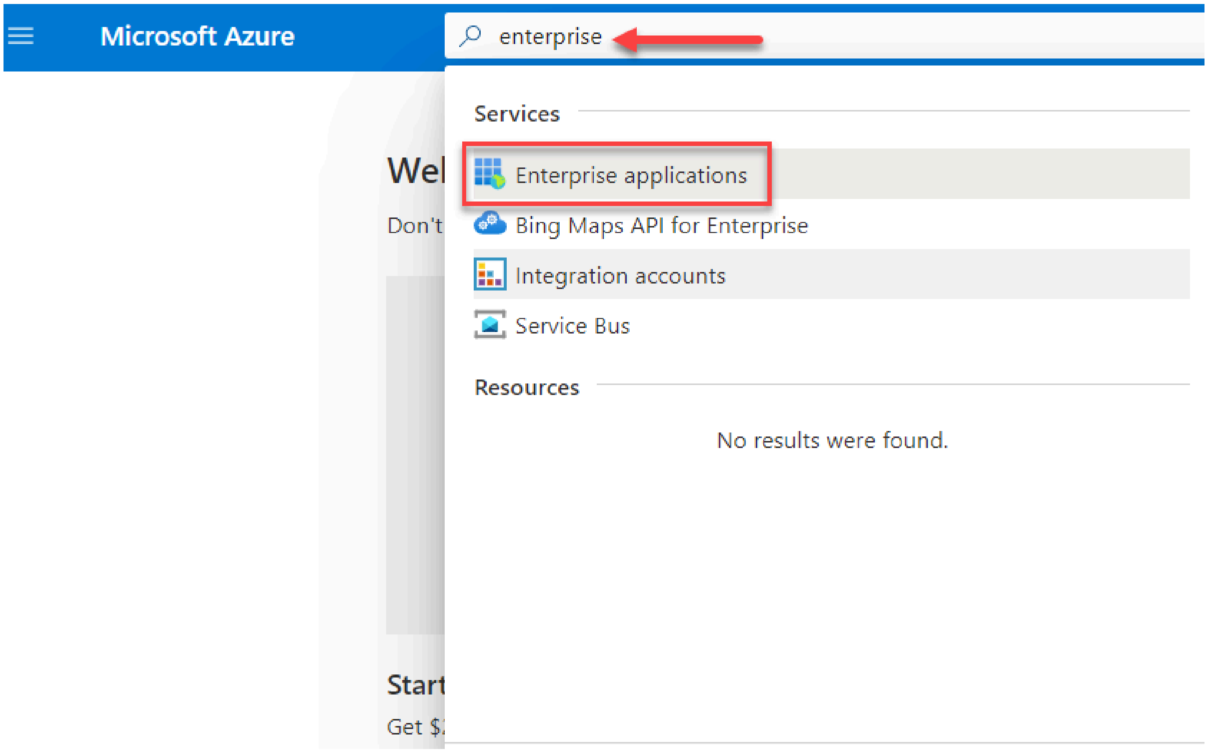
Note:

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

2.5 Setting up Mitel SCIM Enterprise Application

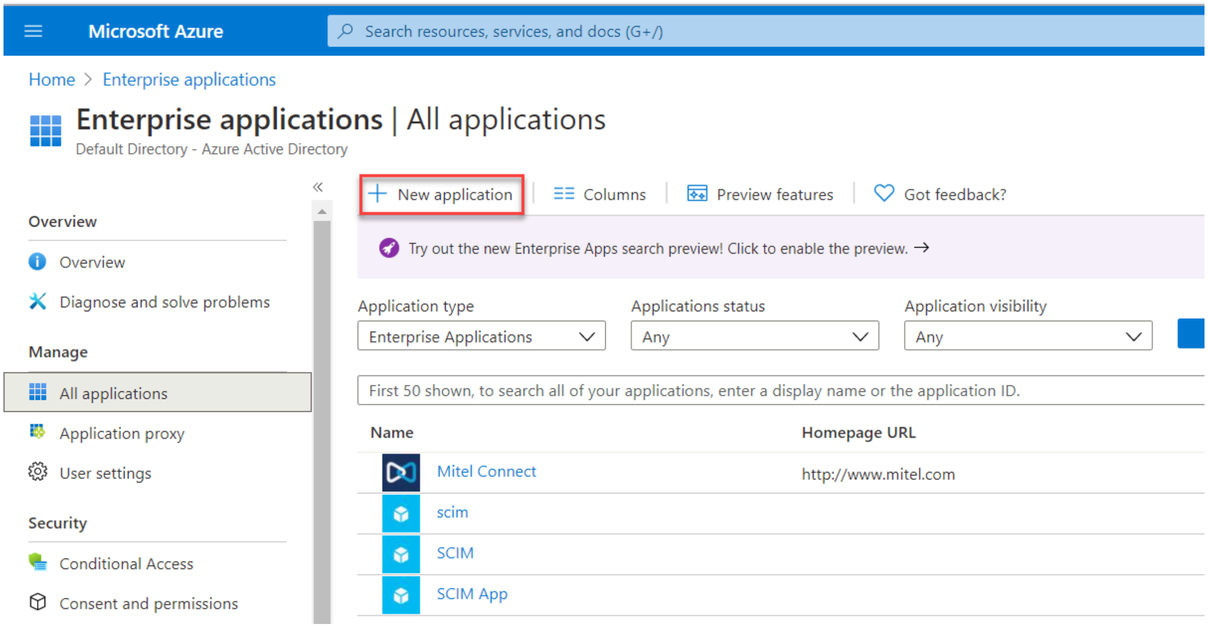
To set up the Mitel SCIM Enterprise app, the administrator should have access to the Azure Portal.

1. In the Azure portal, search for **Enterprise applications**.



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

   The **Browse Azure AD Gallery** opens.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications
Enterprise applications | All applications
Default Directory - Azure Active Directory
New application
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Consent and permissions

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

Application type: Enterprise Applications

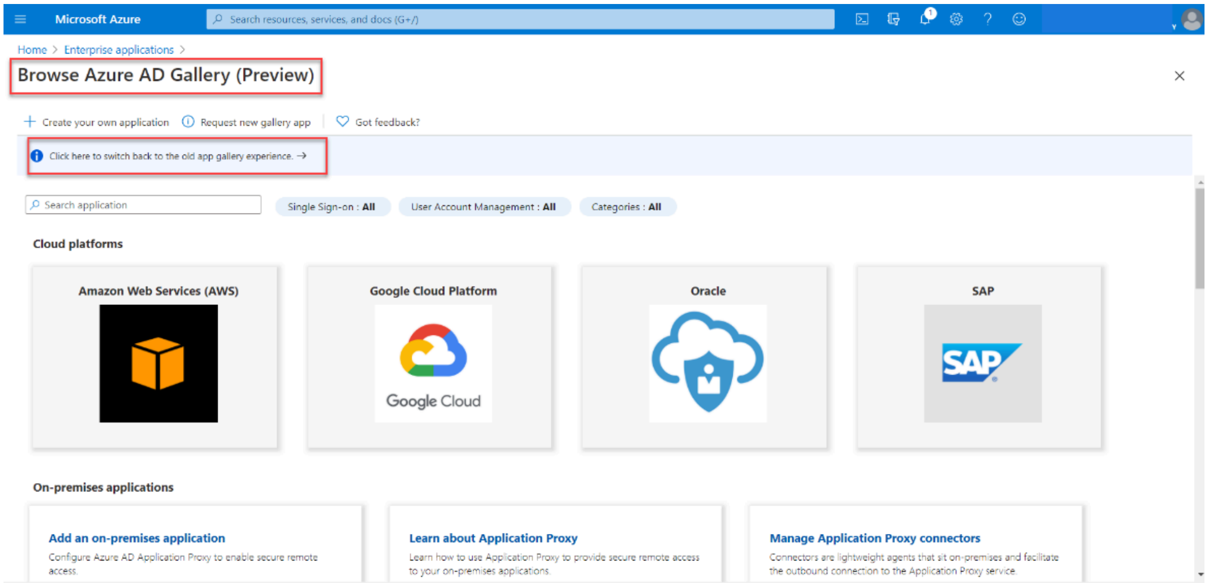
Applications status: Any

Application visibility: Any

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

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

3. In the **Browse Azure AD 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)
Create your own application
Request new gallery app
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Google Cloud
Oracle
SAP
On-premises applications

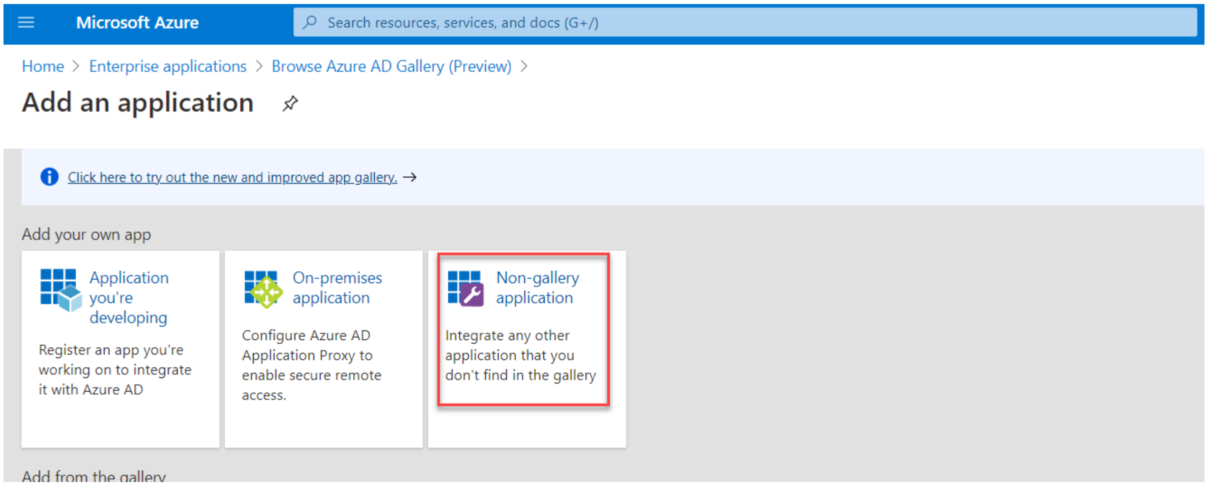
Click here to switch back to the old app gallery experience. →

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Manage Application Proxy connectors
Connectors are lightweight agents that sit on-premises and facilitate the outbound connection to the Application Proxy service.

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

Register an app you're working on to integrate it with Azure AD

On-premises application

Configure Azure AD Application Proxy to enable secure remote access.

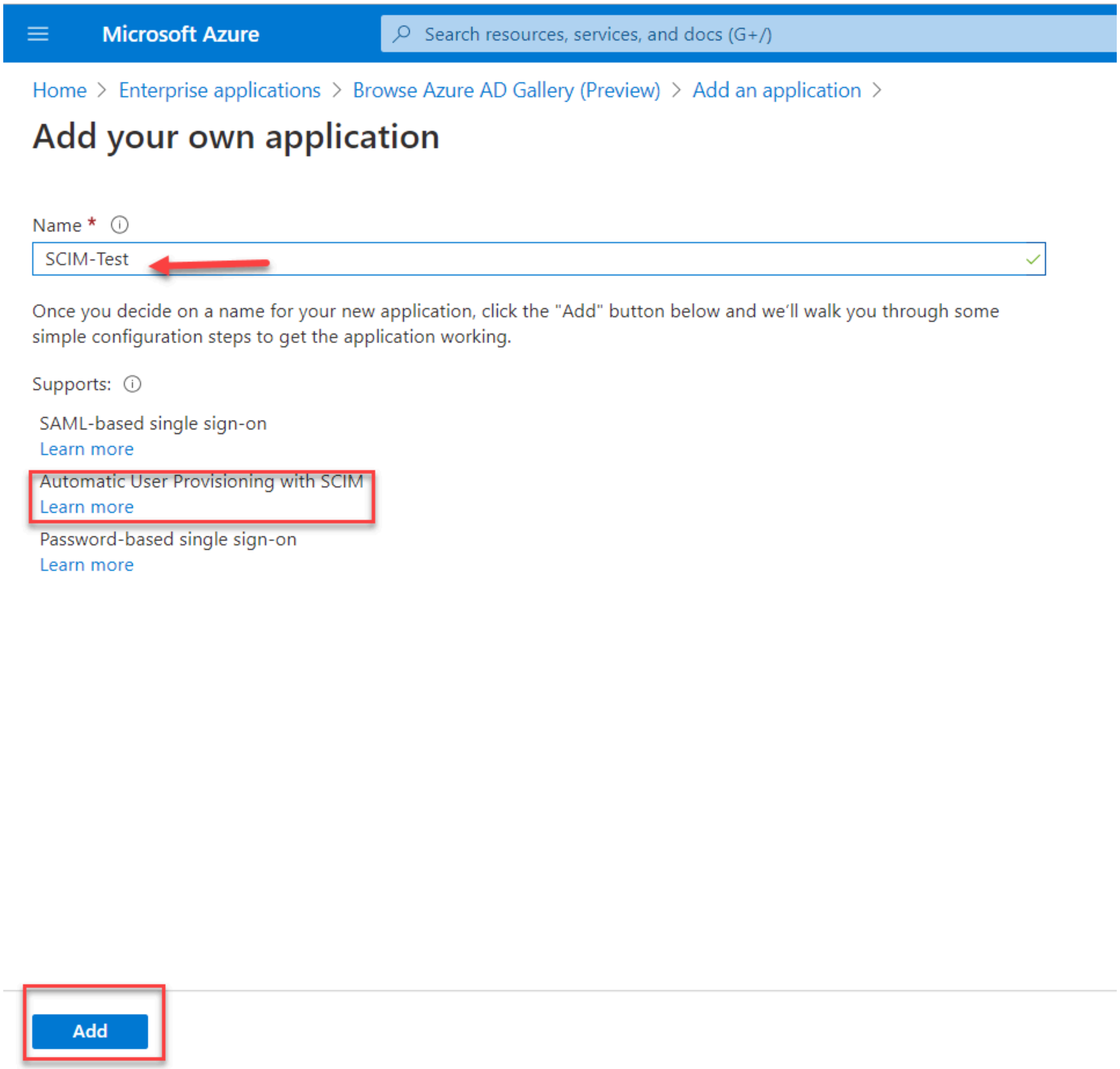
Non-gallery application

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.

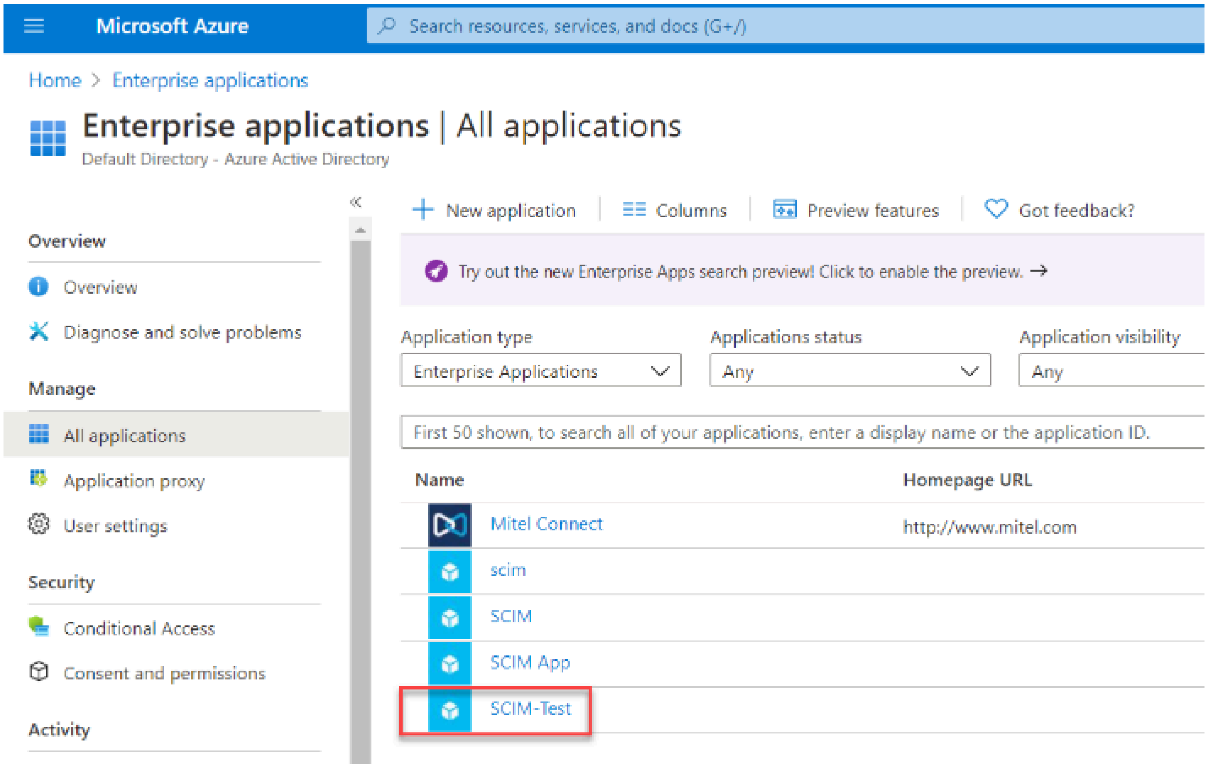
Supports:

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

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



Enterprise applications | All applications

Default Directory - Azure Active Directory

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

Application type: Enterprise Applications

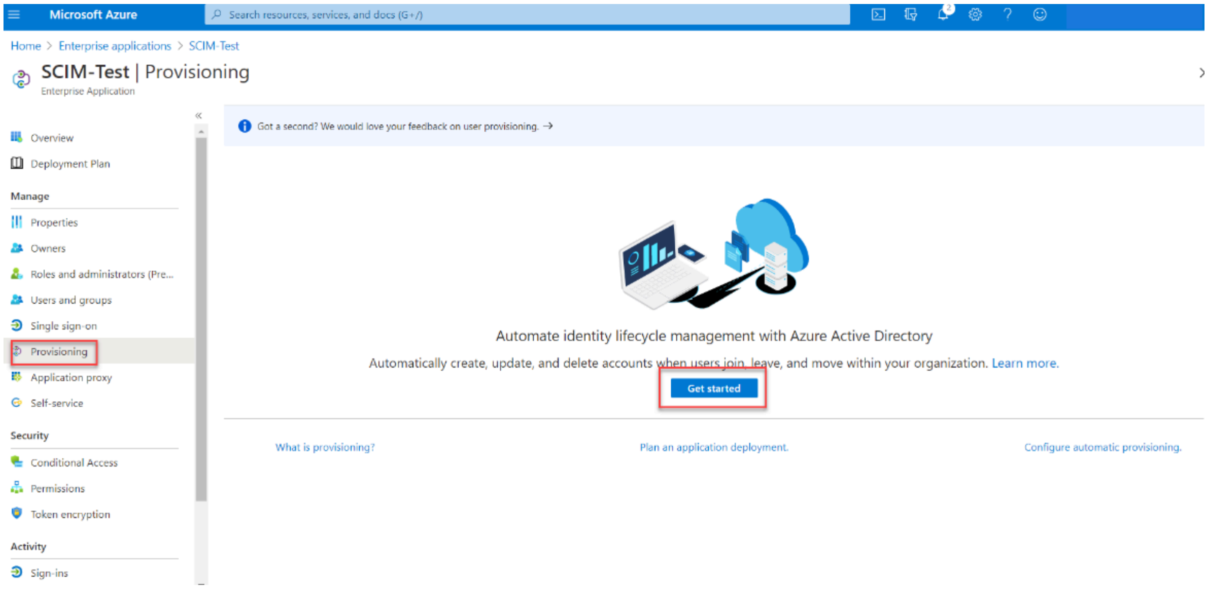
Applications status: Any

Application visibility: Any

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

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

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



SCIM-Test | Provisioning

Enterprise Application

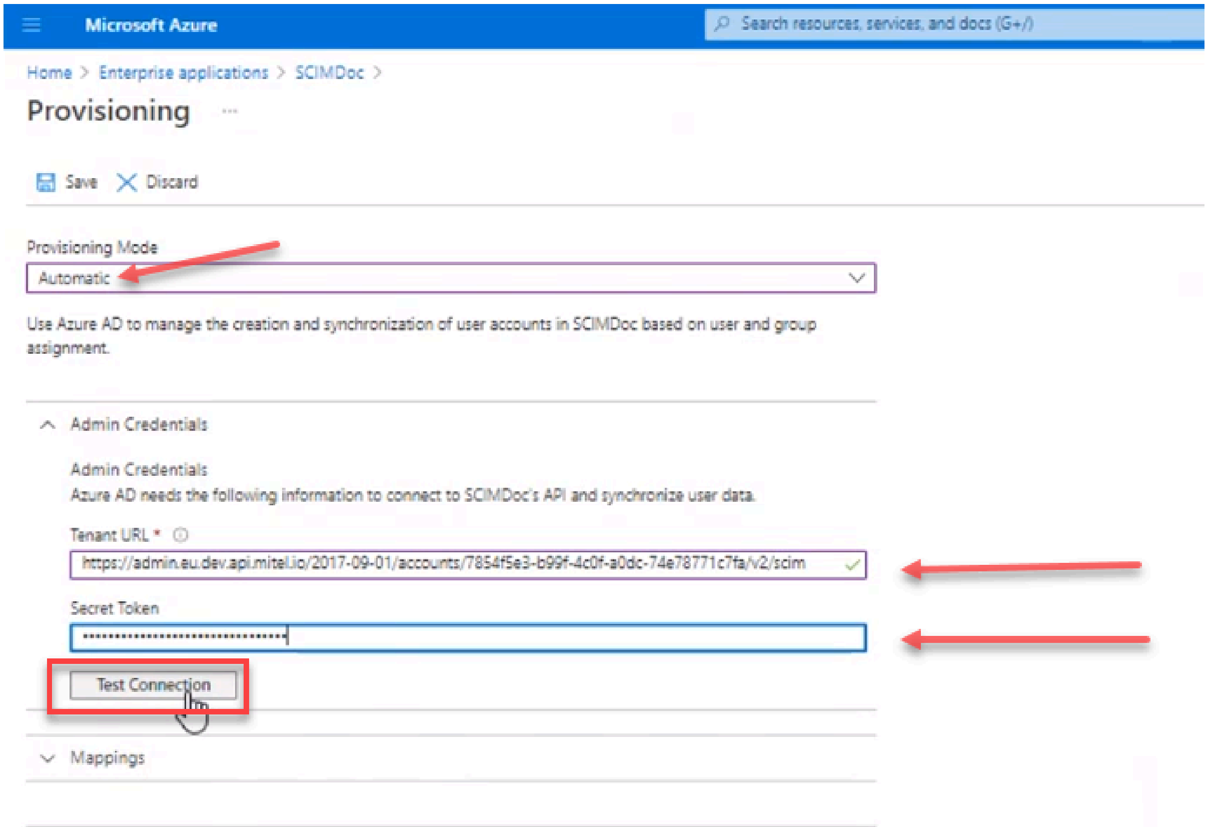
Got a second? We would love your feedback on user provisioning. →

Automate identity lifecycle management with Azure Active Directory

Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

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.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications > SCIMDoc >
Provisioning
Save
Discard
Admin Credentials
Test Connection
Mappings

Provisioning Mode: Automatic

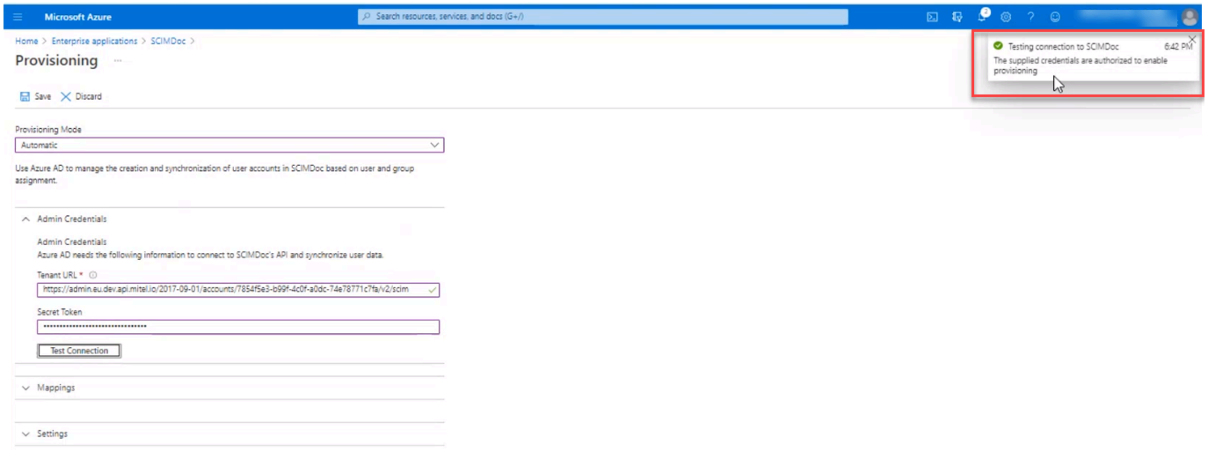
Use Azure AD to manage the creation and synchronization of user accounts in SCIMDoc based on user and group assignment.

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

Tenant URL *: https://admin.eu.dev.api.mitel.io/2017-09-01/accounts/7854f5e3-b99f-4c0f-a0dc-74e78771c7fa/v2/scim

Secret Token: ••••••••••••••••••••••••••••••••

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



Testing connection to SCIMDoc 6:42 PM
The supplied credentials are authorized to enable provisioning

Provisioning Mode: Automatic

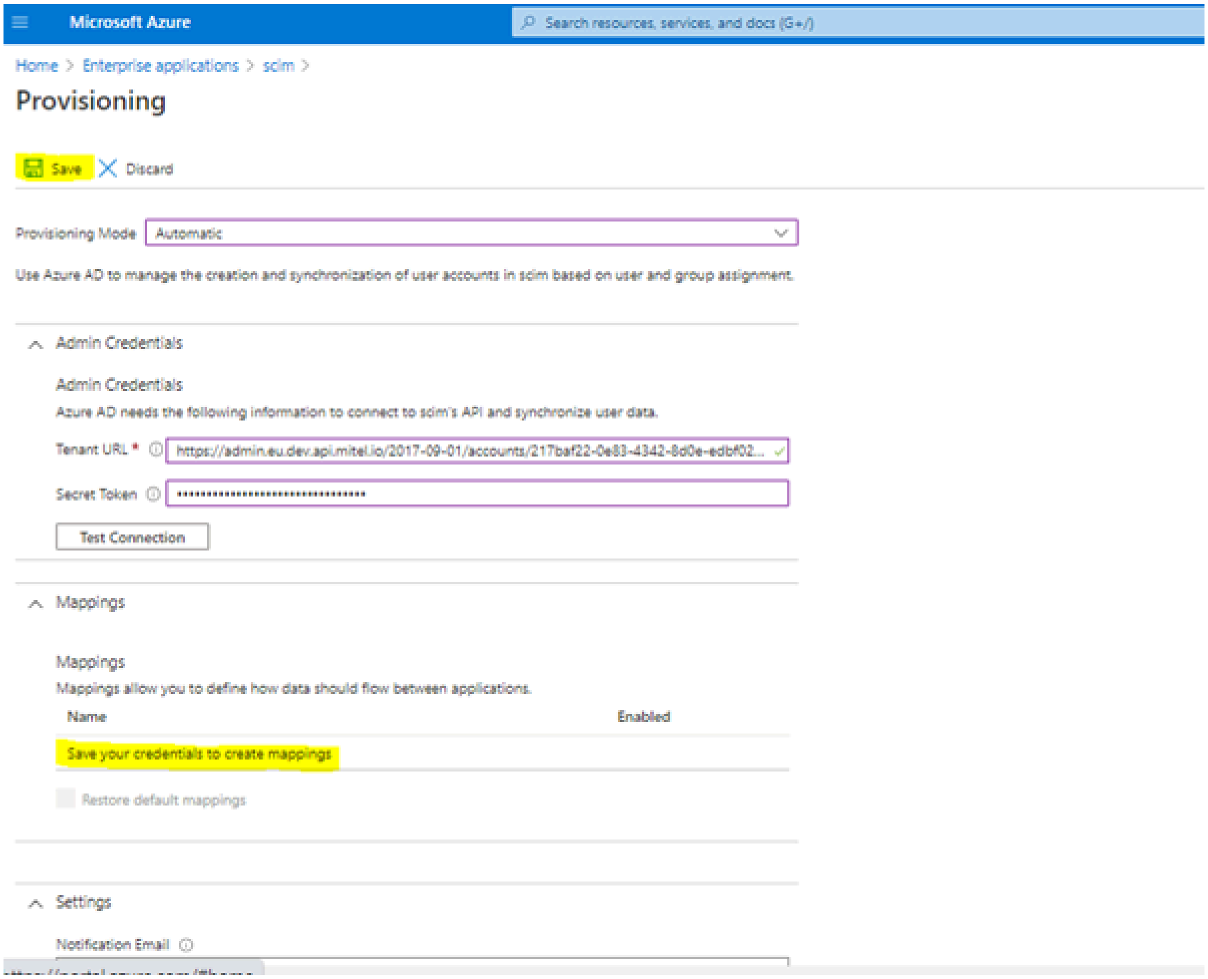
Use Azure AD to manage the creation and synchronization of user accounts in SCIMDoc based on user and group assignment.

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

Tenant URL *: https://admin.eu.dev.api.mitel.io/2017-09-01/accounts/7854f5e3-b99f-4c0f-a0dc-74e78771c7fa/v2/scim

Secret Token: ••••••••••••••••••••••••••••••••

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


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications > scim >
Save
Discard
Test Connection
Restore default mappings

Provisioning

Provisioning Mode: Automatic

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

Admin Credentials

Admin Credentials

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

Tenant URL *: https://admin.eu.dev.api.mitel.io/2017-09-01/accounts/217baf22-0e83-4342-8d0e-edbf02...

Secret Token: ••••••••••••••••••••••••••••••••

Mappings

Mappings

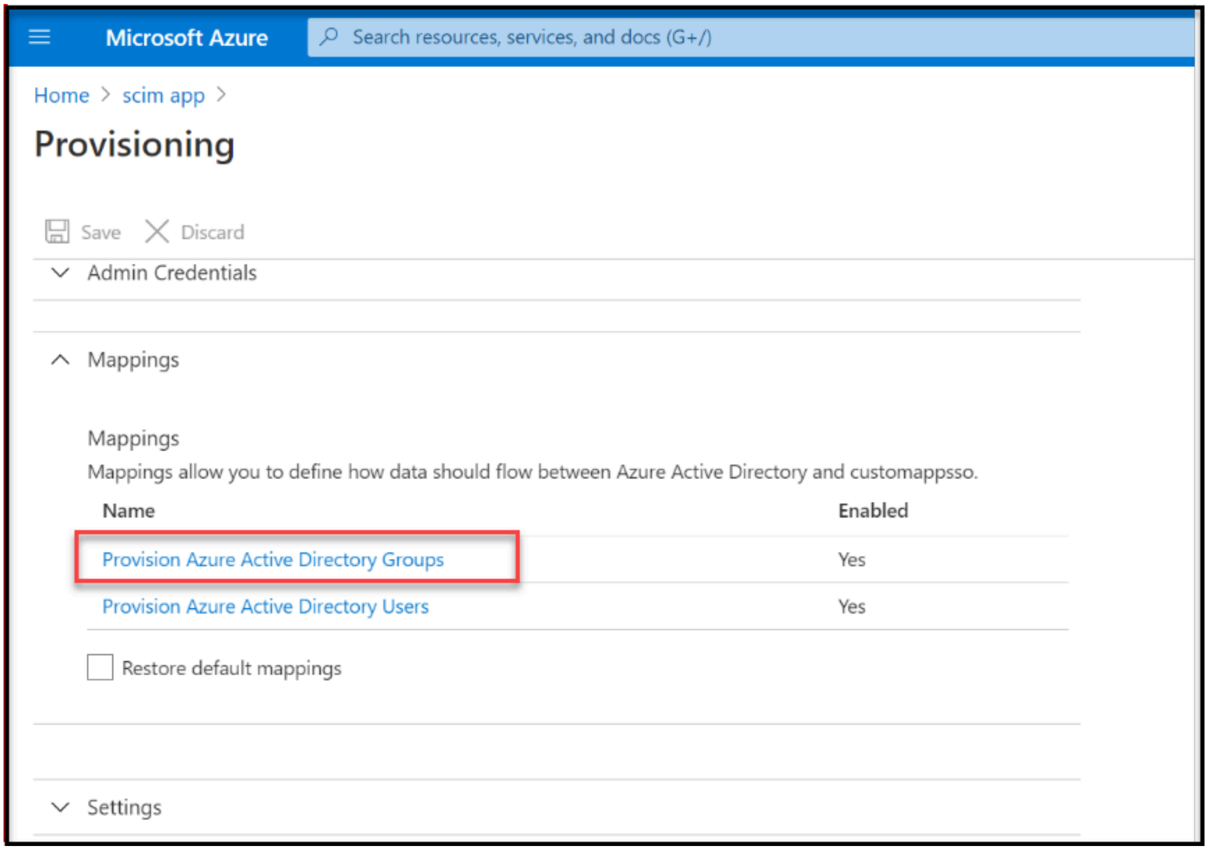
Mappings allow you to define how data should flow between applications.

Name	Enabled
Save your credentials to create mappings	

Settings

Notification Email

11. Click on **Provision Azure Active Directory Groups**.



Provisioning

Mappings

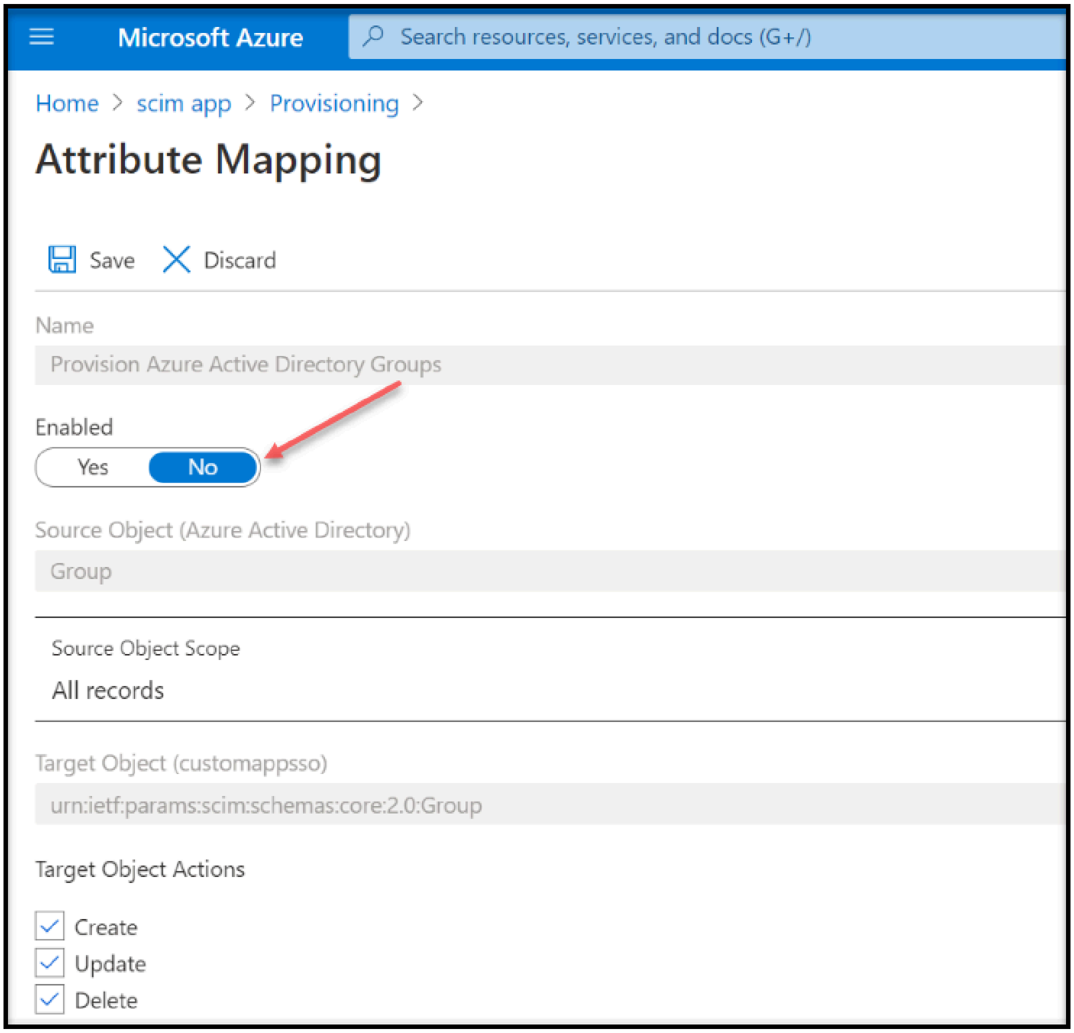
Mappings

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

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

Name: Provision Azure Active Directory Groups

Enabled: Yes [✓ No]

Source Object (Azure Active Directory): Group

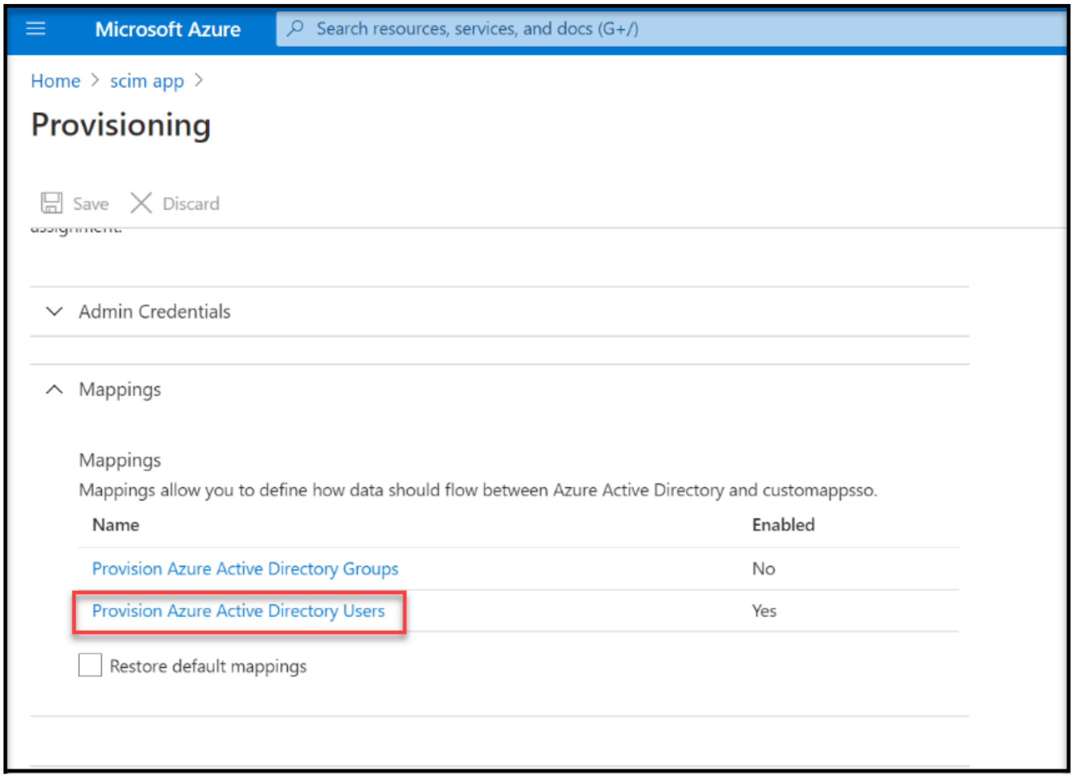
Source Object Scope: All records

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

Target Object Actions

☑ Create
☑ Update
☑ Delete

13. Click on **Provision Azure Active Directory Users**.



Provisioning

Mappings

Mappings

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

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

□ Restore default mappings

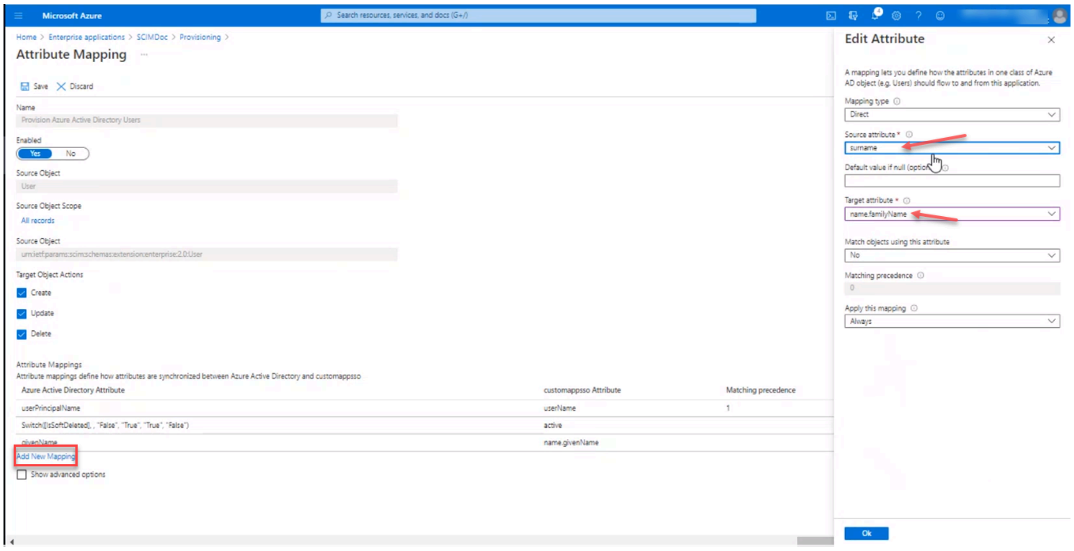
14. **Add/Edit** Attribute mappings

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

Note:

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

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications > SCIMDoc > Provisioning >
Save
Discard
Add New Mapping
Ok

Attribute Mapping

Name: Provision Azure Active Directory Users

Enabled: Yes No

Source Object: User

Source Object Scope: All records

Source Object: urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Target Object Actions

☑ Create

☑ Update

☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence
userPrincipalName	userName	1
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	
givenName	name.givenName	

□ Show advanced options

Edit Attribute

A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type: Direct

Source attribute *: surname

Default value if null (optional):

Target attribute *: name.familyName

Match objects using this attribute: No

Matching precedence: 0

Apply this mapping: Always

Note:

The following SCIM attributes are supported for programming from the provisioning server (in this case Azure AD). 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.

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

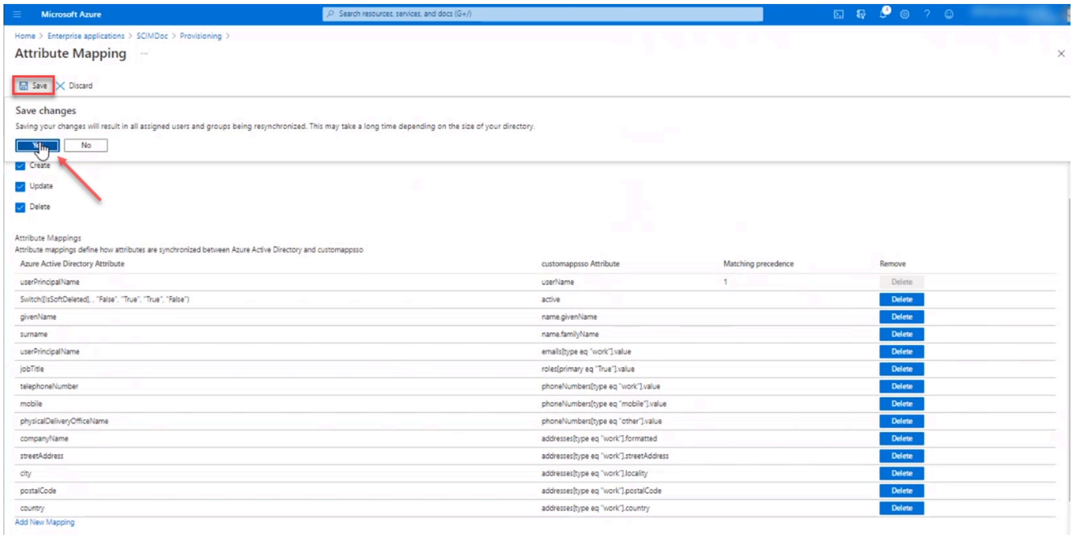
Azure AD Attributes	SCIM/Target Attributes	MiCollab Attributes
userPrincipalName	userName	
telephoneNumber	phoneNumbers[type eq "work"].value	Primary Phone Directory Number (DN

Table 2: Attribute Mappings

Azure AD 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

Azure AD Attributes	SCIM/Target Attributes	MiCollab Attributes
Extension attribute or any available UI attribute	address[type eq “work”].country	Country

15. Click on **Save mapping**.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications > SCIMDoc > Provisioning >
Save
Discard
Yes
No
Add New Mapping

Attribute Mapping

Save changes

Saving your changes will result in all assigned users and groups being resynchronized. This may take a long time depending on the size of your directory.

☑ Create

☑ Update

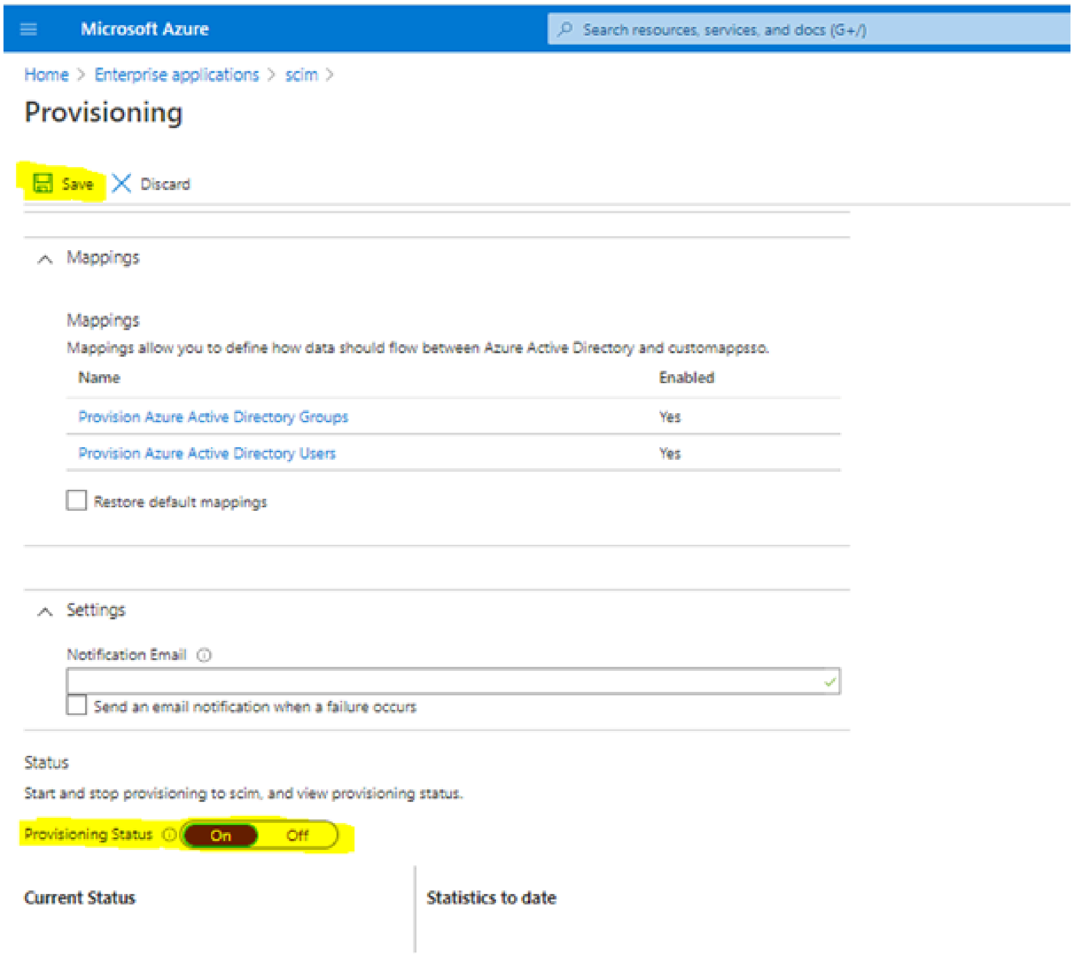
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
userPrincipalName	emails[type eq "work"].value		Delete
jobTitle	roles[primary eq "True"].value		Delete
telephoneNumber	phoneNumbers[type eq "work"].value		Delete
mobile	phoneNumbers[type eq "mobile"].value		Delete
physicalDeliveryOfficeName	phoneNumbers[type eq "other"].value		Delete
companyName	addresses[type eq "work"].formatted		Delete
streetAddress	addresses[type eq "work"].streetAddress		Delete
city	addresses[type eq "work"].locality		Delete
postalCode	addresses[type eq "work"].postalCode		Delete
country	addresses[type eq "work"].country		Delete

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications > scim >
Provisioning
Save
Discard
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

Notification Email

□ Send an email notification when a failure occurs

Status

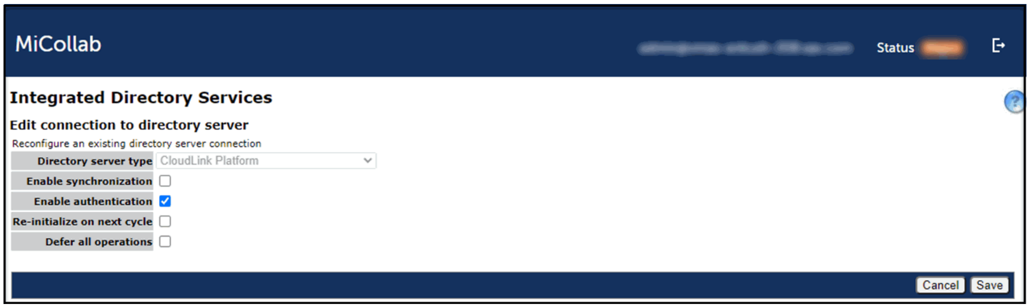
Start and stop provisioning to scim, and view provisioning status.

Provisioning Status [✓ On] Off

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/Azure AD 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**.



Integrated Directory Services

Edit connection to directory server

Reconfigure an existing directory server connection

Directory server type	CloudLink Platform
Enable synchronization	☐
Enable authentication	☑
Re-initialize on next cycle	☐
Defer all operations	☐

4. Once the Cloudlink-based synchronization is enabled, all existing users and new users created from the provisioning server (Azure AD) 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:

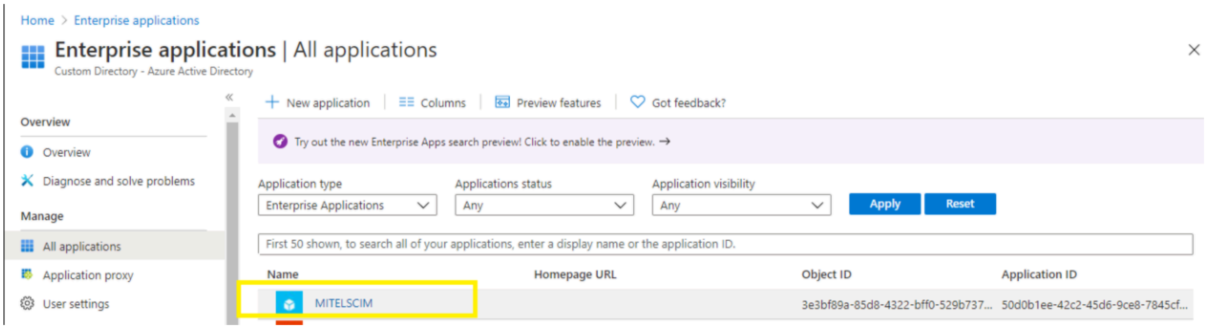
- Once the synchronization is enabled, the administrator will not be allowed to add a new user(s) from **Add**, and **Quick Add** options. Any new user addition and updates must be done from the provisioning server portal only. Refer to Table 1 Attribute Mappings for details on MiCollab attributes.
-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

2.7 Adding a user in Azure Mitel SCIM enterprise application

Prerequisites: The administrator needs to have an account in the azure portal (https://portal.azure.com/).

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

1. Under Enterprise Applications on Azure AD, select **Mitel SCIM**. To create a Mitel SCIM Application, refer to the section **Setting up Mitel SCIM Enterprise Application**.


Home > Enterprise applications
Enterprise applications | All applications
Custom Directory - Azure Active Directory
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
New application
Columns
Preview features
Got feedback?
Apply
Reset

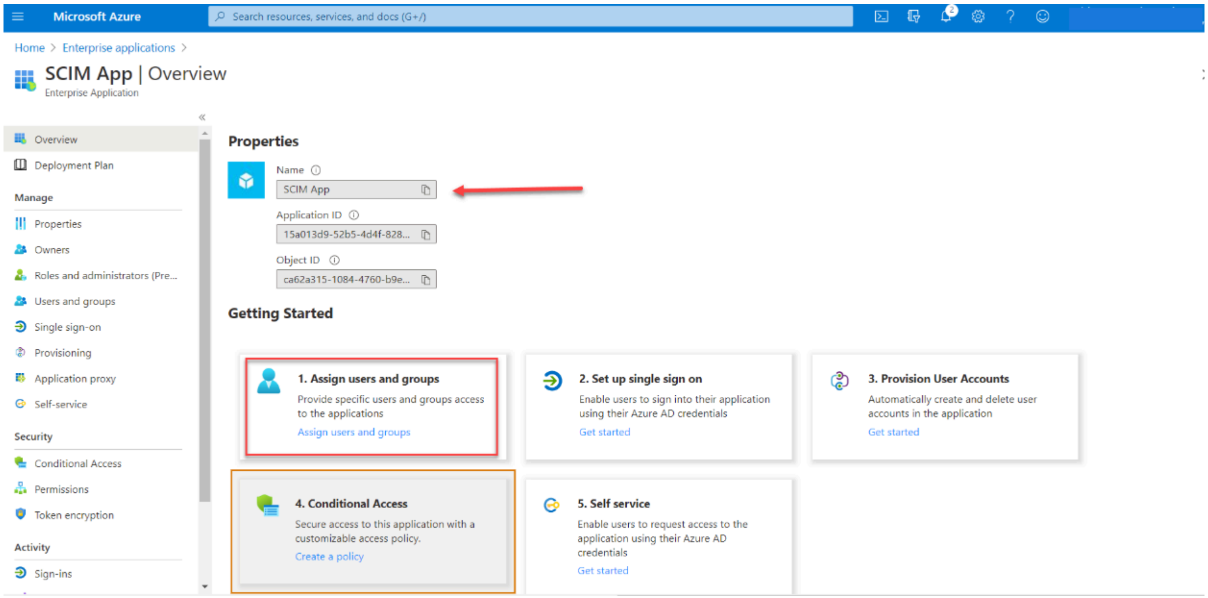
Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications
Applications status: Any
Application visibility: Any

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...

2. On the Mitel SCIM page, click on the **Assign users and groups option**.



Name: SCIM App
Application ID: 15a013d9-52b5-4d4f-828...
Object ID: ca62a315-1084-4760-b9e...

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

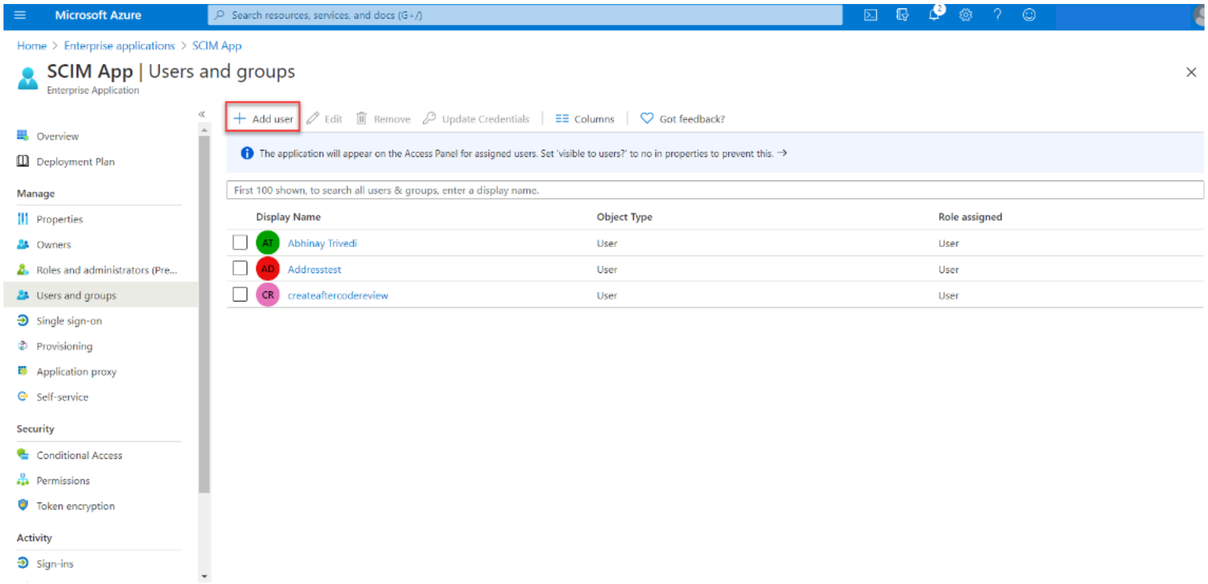
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

3. Click **Add user**.

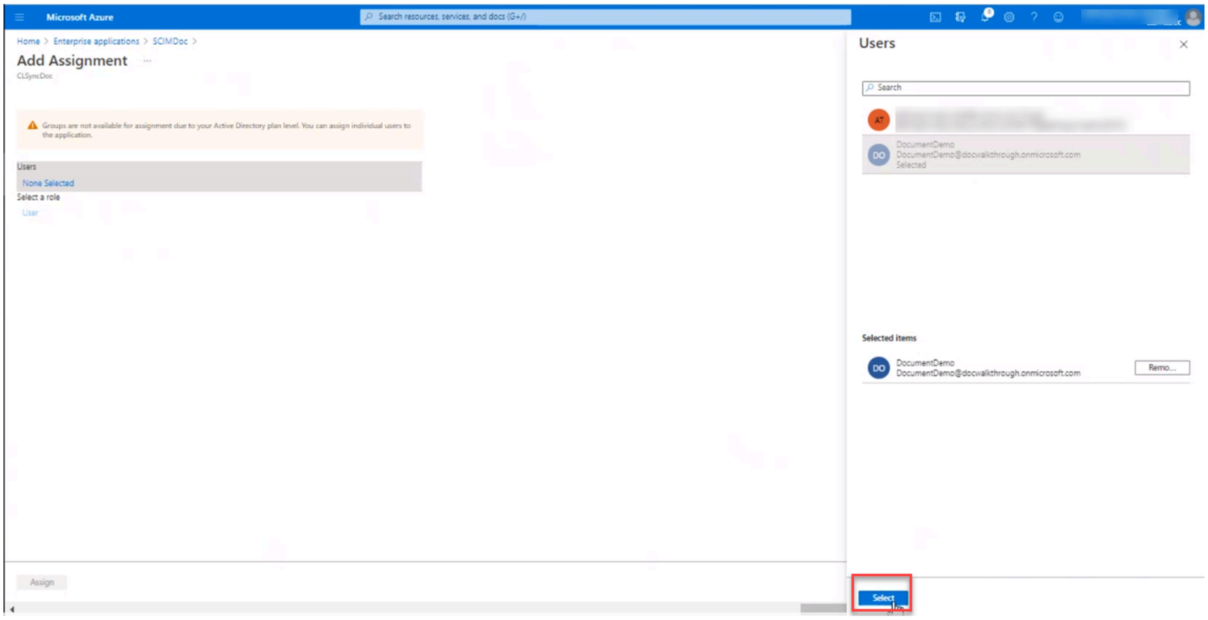


The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	AT Abhinay Trivedi	User	User
□	AD Addresstest	User	User
□	CR createaftercodereview	User	User

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



Microsoft Azure

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

Home > Enterprise applications > SCIMDoc >

Add Assignment

CLSyncDoc

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users
None Selected

Select a role
User

Assign

Users

Search

AT [redacted]

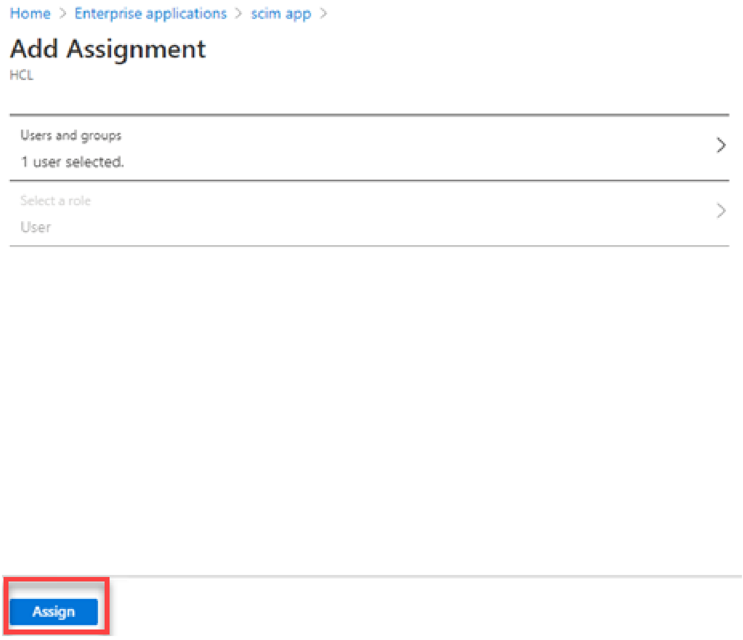
DO DocumentDemo
DocumentDemo@docwalkthrough.onmicrosoft.com
Selected

Selected items

DO DocumentDemo
DocumentDemo@docwalkthrough.onmicrosoft.com
Remo...

Select

5. Click **Assign**.



Home > Enterprise applications > scim app >

Add Assignment

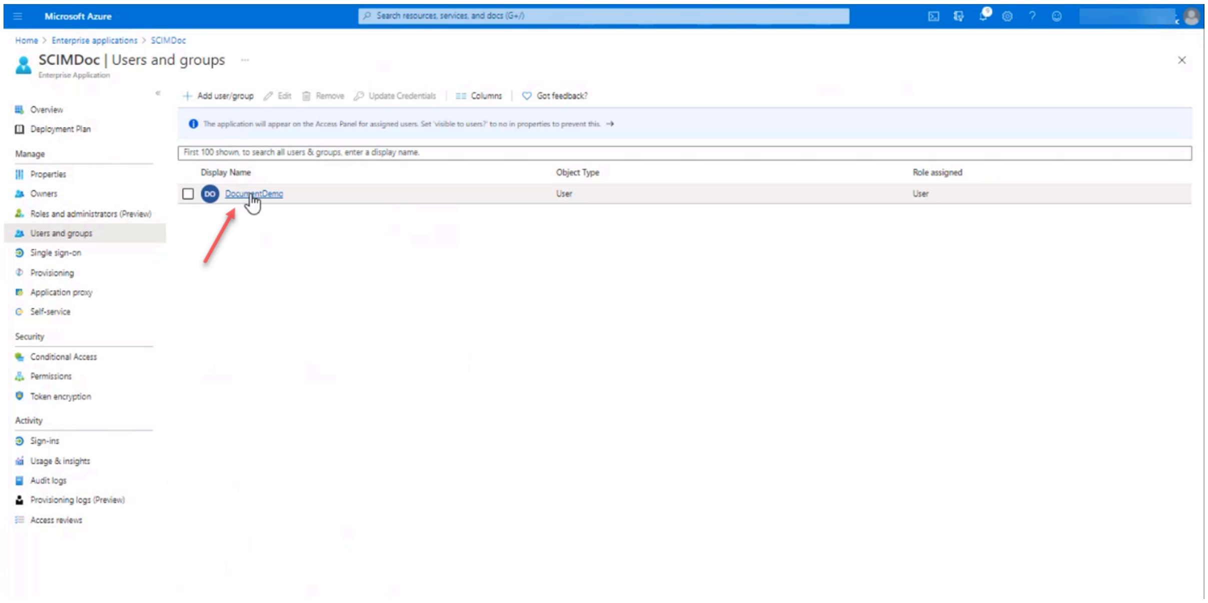
HCL

Users and groups
1 user selected.

Select a role
User

Assign

6. User should List under Enterprise Application – **Mitel SCIM** as shown below.



The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	DO DocumentDemo	User	User

Note:

- The last name of a user is not mandatory in Azure 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 that was provisioned by Azure AD

This section describes the procedure required to delete a user in MiCollab and CloudLink that was provisioned by Azure AD.

If the following procedure is not followed, the user will not be removed from CloudLink users which means in turn it will not send the delete command to MiCollab.

1. In Azure, under **Enterprise Applications**, click on the application that you have created.

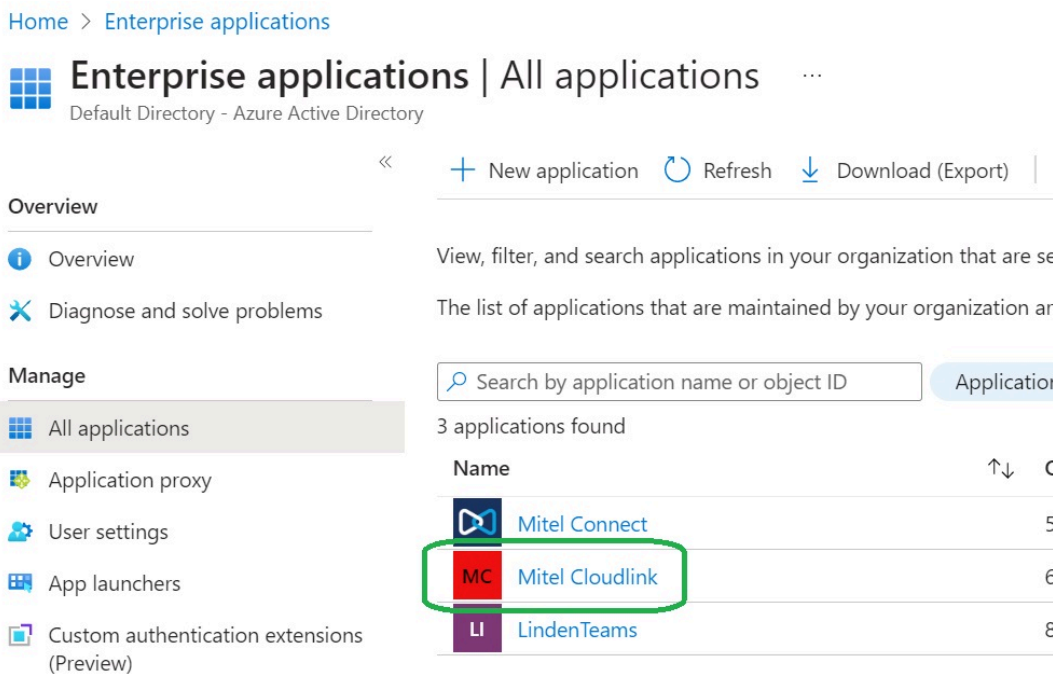
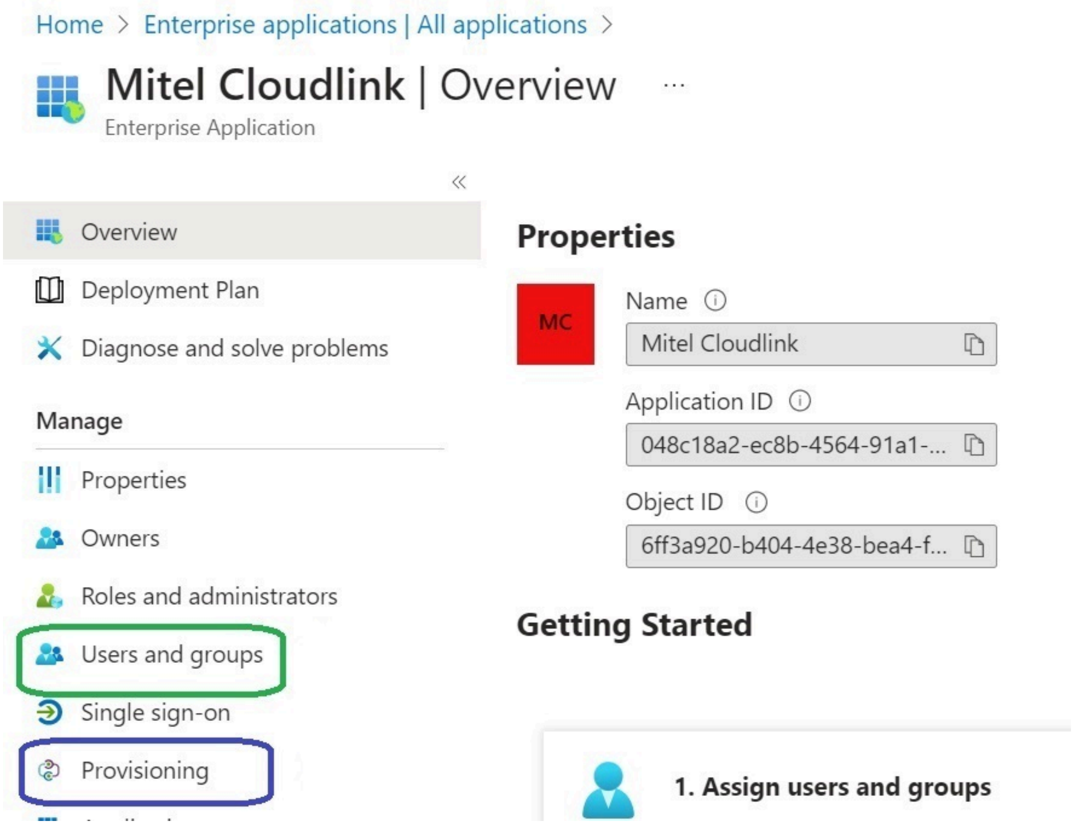

Home > Enterprise applications
Enterprise applications | All applications ...
Default Directory - Azure Active Directory
«
+ New application
Refresh
Download (Export)
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
App launchers
Custom authentication extensions (Preview)
View, filter, and search applications in your organization that are se
The list of applications that are maintained by your organization ar
Search by application name or object ID
Applicatio
3 applications found
Name
Mitel Connect
MC
Mitel Cloudlink
LI
LindenTeams

Figure 1: Enterprise Applications

2. On the selected application, click **Users and groups** from the left pane.
   The **Users and groups** displays the list of users or groups that are provisioned in the application group.



Name: Mitel Cloudlink

Application ID: 048c18a2-ec8b-4564-91a1-...

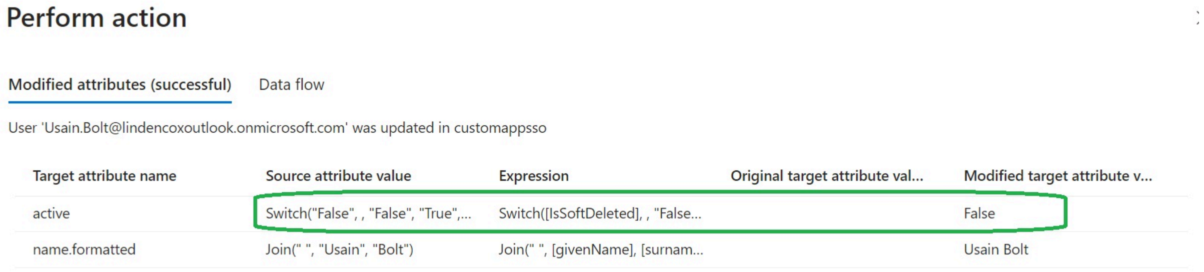
Object ID: 6ff3a920-b404-4e38-bea4-f...

Figure 2: Mitel CloudLink - Overview

3. Search and select the users or groups that need to be removed, and then click **Remove**.

4. On the selected application, click **Provisioning** from the left pane.
5. Search and select the users or groups, and then click **Provision**.

   The **Perform action** screen displays with the user details.



Perform action

Modified attributes (successful) Data flow

User 'Usain.Bolt@lindencoxoutlook.onmicrosoft.com' was updated in customappsso

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(" ", "Usain", "Bolt")	Join(" ", [givenName], [surnam...		Usain Bolt

Figure 3: Perform action

6. In the **Source attribute value**, the value should be **False**.

   The user is removed from the CloudLink account.
7. In **MiCollab**, navigate to the **Integrated Directory Service** option.
8. Select the **mitel.io** option and click **Sync**.

   A delete request is passed to MiCollab to action.
9. From the **Detained Queue**, select the deleted user checkbox and click **Save**.

The user has now been deleted from Azure AD, CloudLink, and MiCollab.

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 completedseparately; 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 4

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 Azure AD Admin programming. The AD attribute can be configured via the Azure AD 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 Azure AD 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	Azure portal	https://portal.azure.com/#home

Mitel
Powering connections

mitel.com