



A MITEL
PRODUCT
GUIDE

MiCollab Solution Document — CloudLink Authentication and Synchronization

Release 9.7 SP1 FP1

October 2023

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) or its 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 2023, Mitel Networks Corporation

All rights reserved

Contents

1 CloudLink-based Authentication.....	1
1.1 Prerequisites and Supported Platforms.....	3
1.2 Microsoft Azure Active Directory to CloudLink.....	4
1.3 Setting up a CloudLink Account for Integration.....	4
1.4 Adding a user on Azure 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/Azure AD authentication for IDS.....	12
1.5.4 To disable CloudLink-based authentication.....	18
1.5.5 Using CloudLink-based Authentication on the MiCollab Clients.....	19
1.5.6 Manual login for native clients.....	22
2 CloudLink-based Synchronization.....	26
2.1 Prerequisites and Supported Platforms.....	26
2.2 Limitations.....	27
2.3 Setting up CloudLink Account for SCIM integration.....	28
2.4 Setting up the Provisioning Server (Azure AD).....	32
2.5 Setting up Mitel SCIM Enterprise Application.....	33
2.6 Setting up MiCollab for CloudLink-based Synchronization.....	46
2.7 Adding a user in Azure Mitel SCIM enterprise application.....	47
3 Troubleshooting Errors, Alarms and Reports.....	54
3.1 Alarms.....	54
3.2 Errors.....	54
3.3 User Summary Reports.....	55
4 External References and Links.....	56

CloudLink-based Authentication

1

This chapter contains the following sections:

- [Prerequisites and Supported Platforms](#)
- [Microsoft Azure Active Directory to CloudLink](#)
- [Setting up a CloudLink Account for Integration](#)
- [Adding a user on Azure 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 Azure Active Directory (AD) at the CloudLink backend. 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.

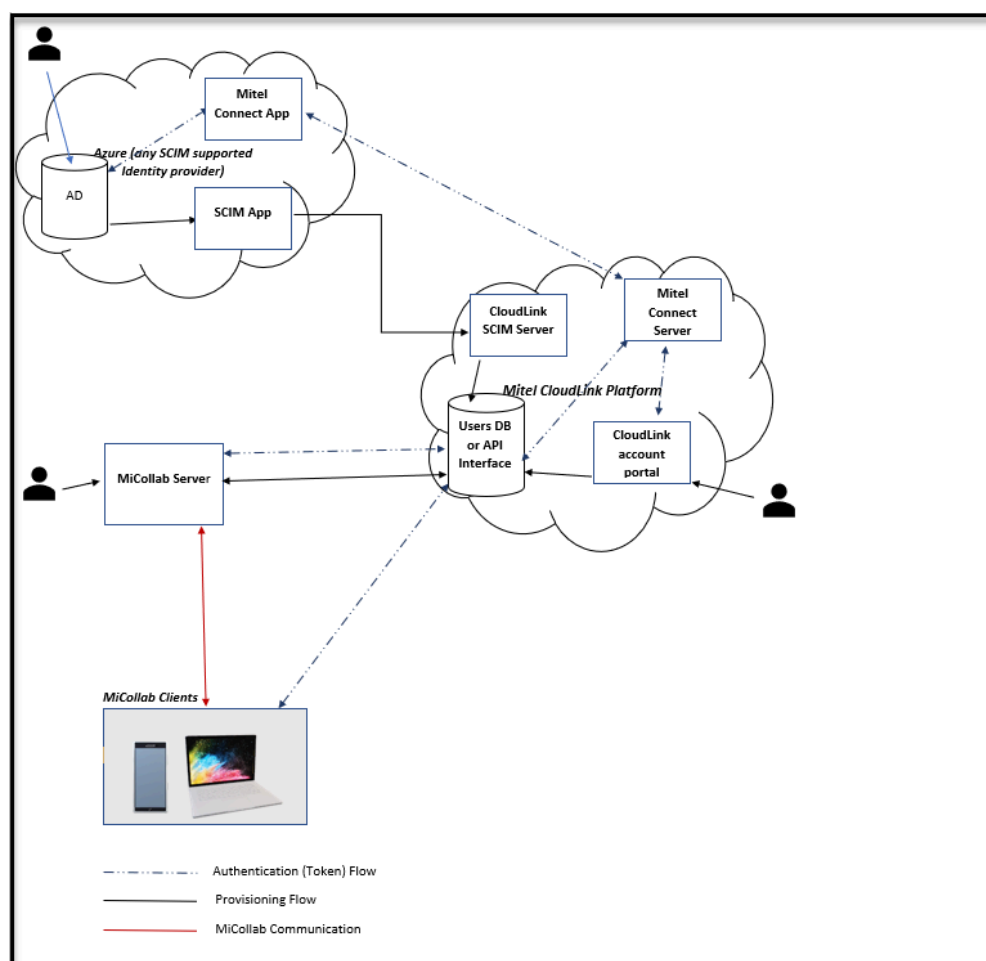


Figure 1: Data Flow Diagram between MiCollab, CloudLink and Azure

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, MiCollab for Microsoft and MiCollab Legacy desktop Clients.
- 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:

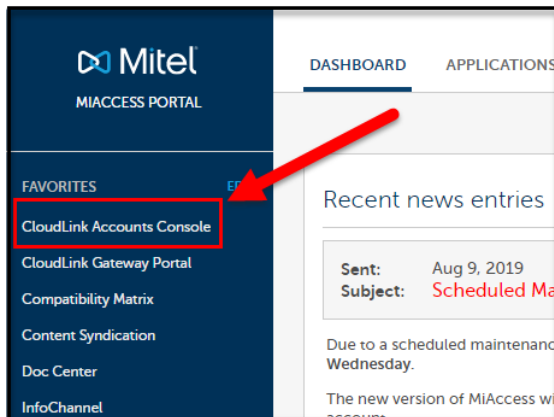
- An Azure AD subscription
- A Mitel CloudLink account

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.

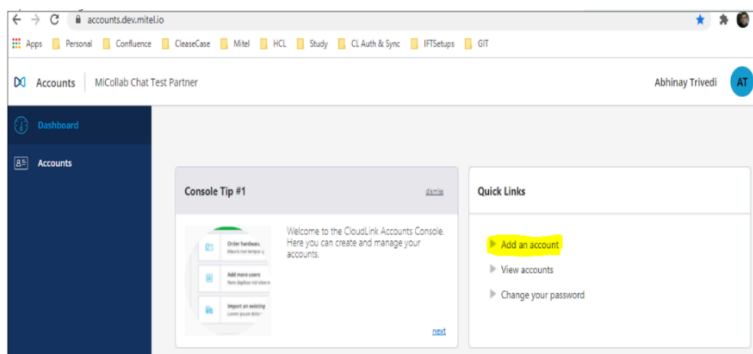
1. Log in to the MiAccess portal using your MiAccess credentials.

2. On the left tab, select **Mitel Administration**.



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.

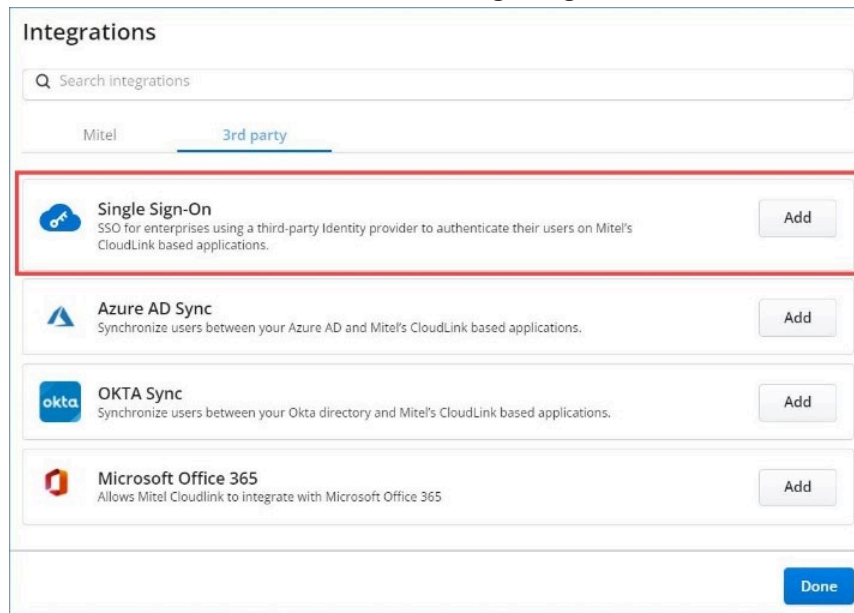
- Customer Name
- Country
- Province/State
- Address
- City
- Postal/Zip Code
- Default Language
- Business Type
- Support Contact

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.



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

Step 3
Fill in these values from your Identity provider integration.

Sign-in URL *

IDP Identifier (Entity ID) *

Signing Certificate(s)
Your provider's public key in PEM format. If you need to include multiple, paste them one after the other. *

Optional Mitel credentials

☐ Enable Mitel Credentials (Optional)
Note that this will show the option to all users on login. You will also need to manually send a 'Welcome email' to all users who you would like to give a Mitel Application account to.

[Remove](#) [Cancel](#) [Save](#)

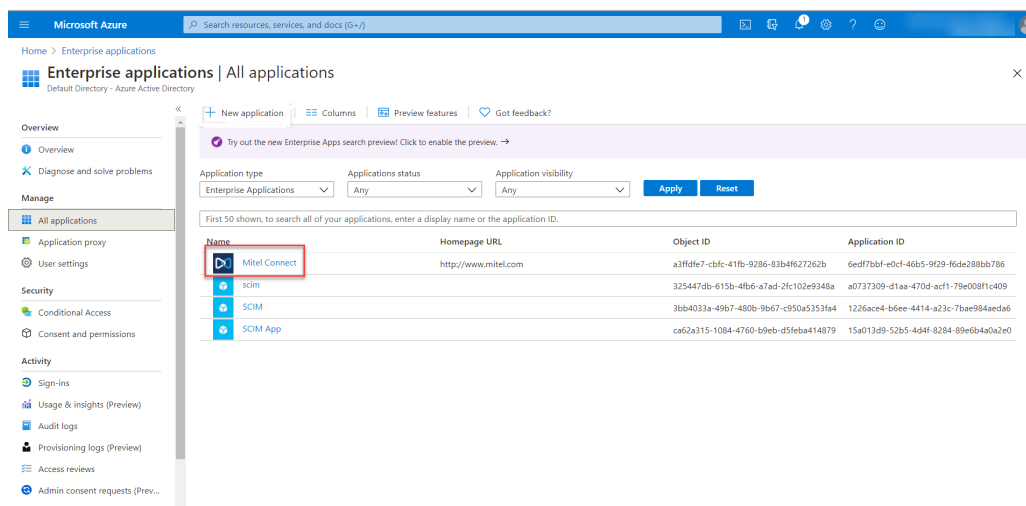
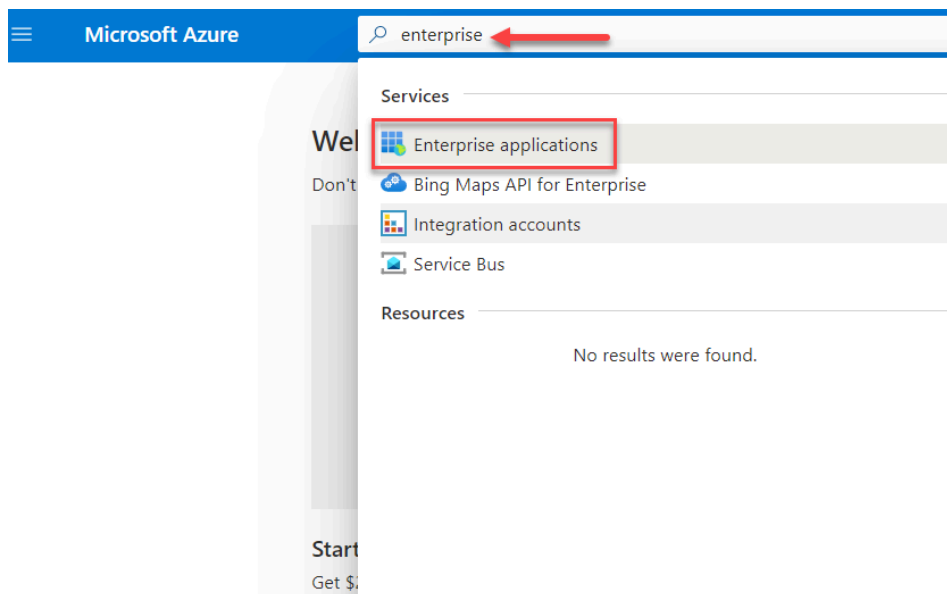
This completes the steps necessary to integrate the CloudLink Account with the customer Azure AD.

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.

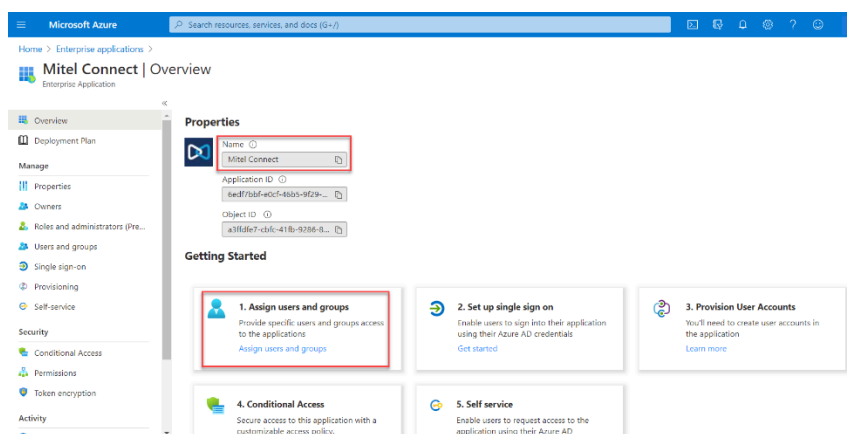
1.4 Adding a user on Azure in Mitel Connect

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.

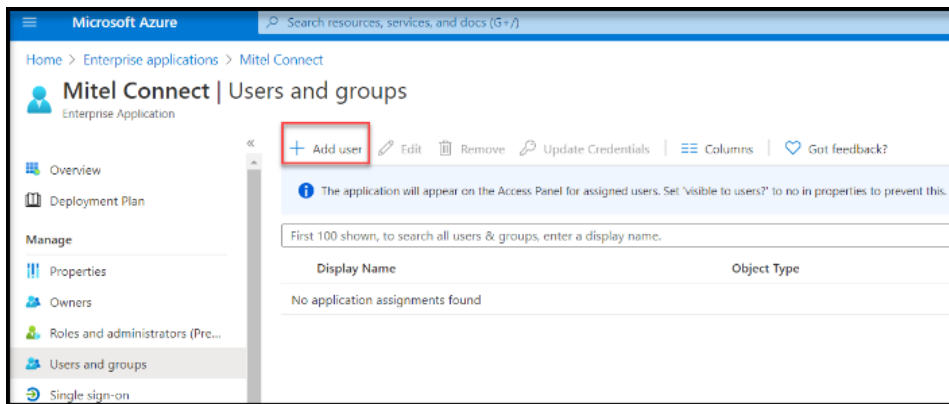
1. Search for Enterprise Applications on Azure AD and select **Mitel Connect** application.



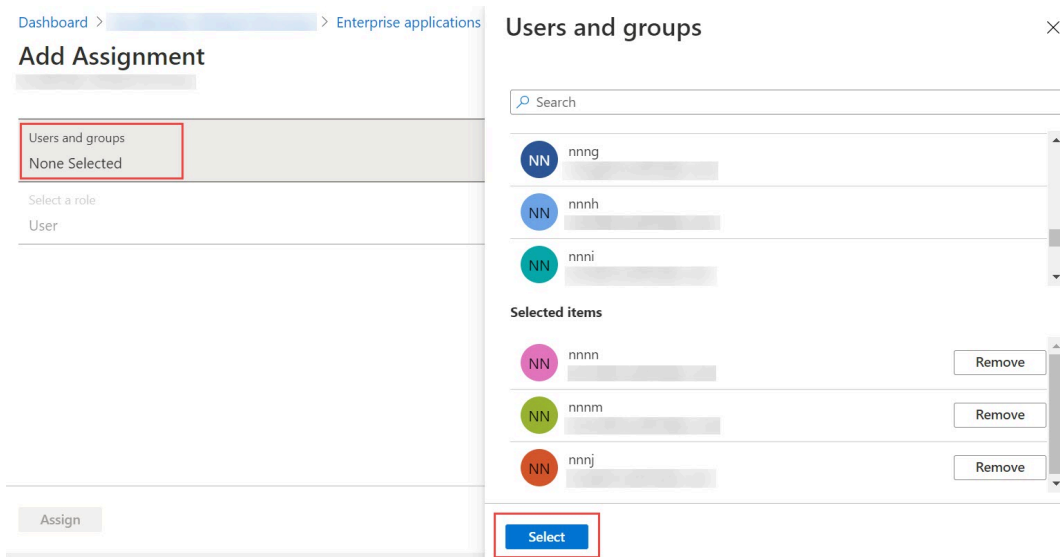
2. After clicking Mitel Connect, click **Assign user and group**.



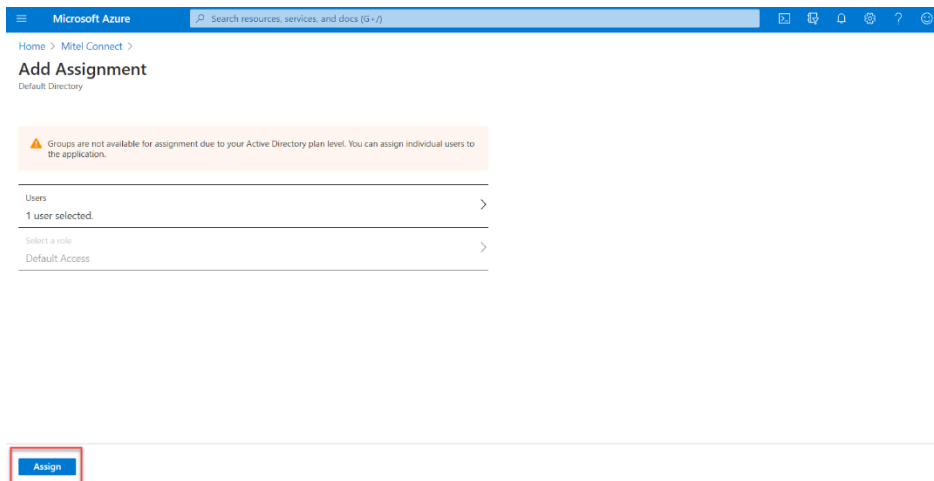
3. Click **Add user**.



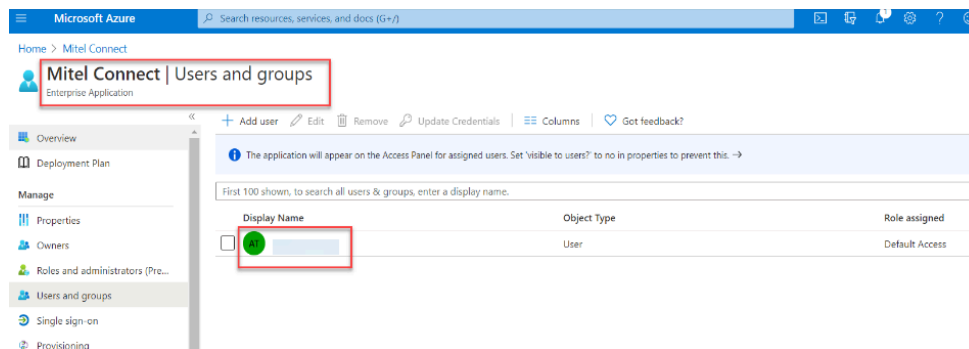
4. Search for the user and click to **Select** the user.



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



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



- 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

- In the MiCollab Server, under **Configuration**, click **Integrated Directory Service**.
- 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:

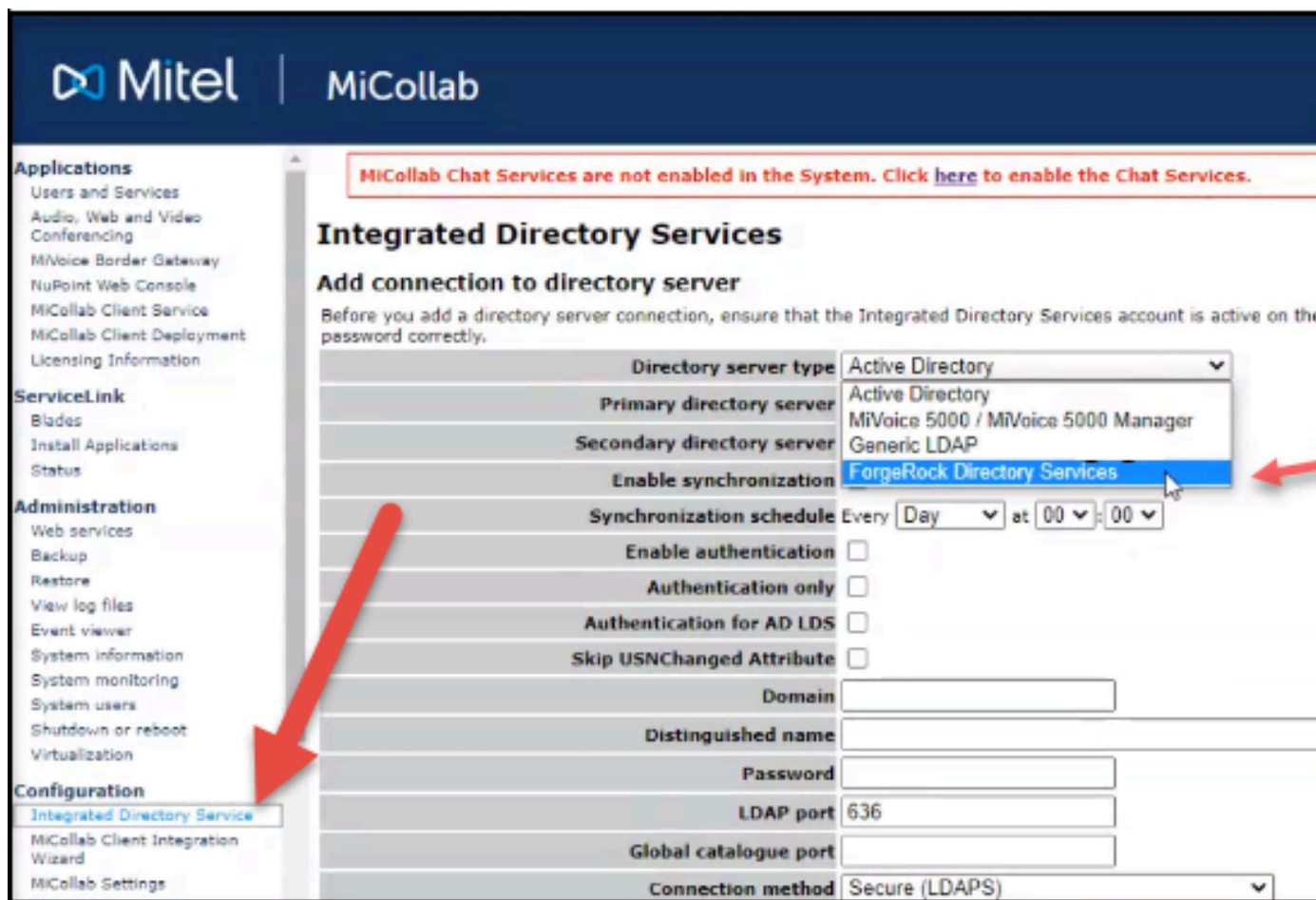
The following features are not supported with CloudLink IDS:

- 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

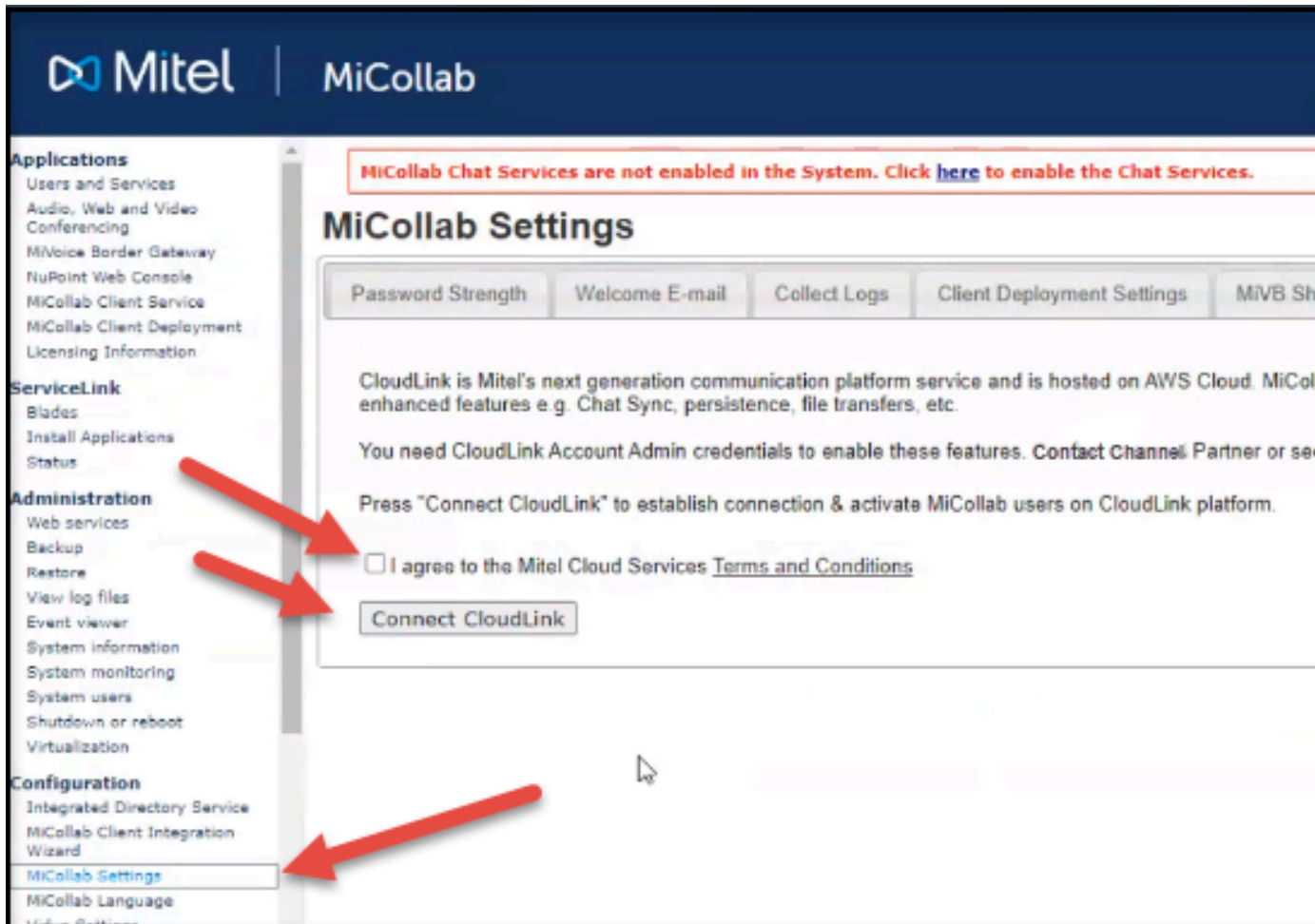


If CloudLink Integration is enabled, CloudLink Platform will be shown under available Directory Server Types. Refer from step 6 onwards for further configuration.

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.



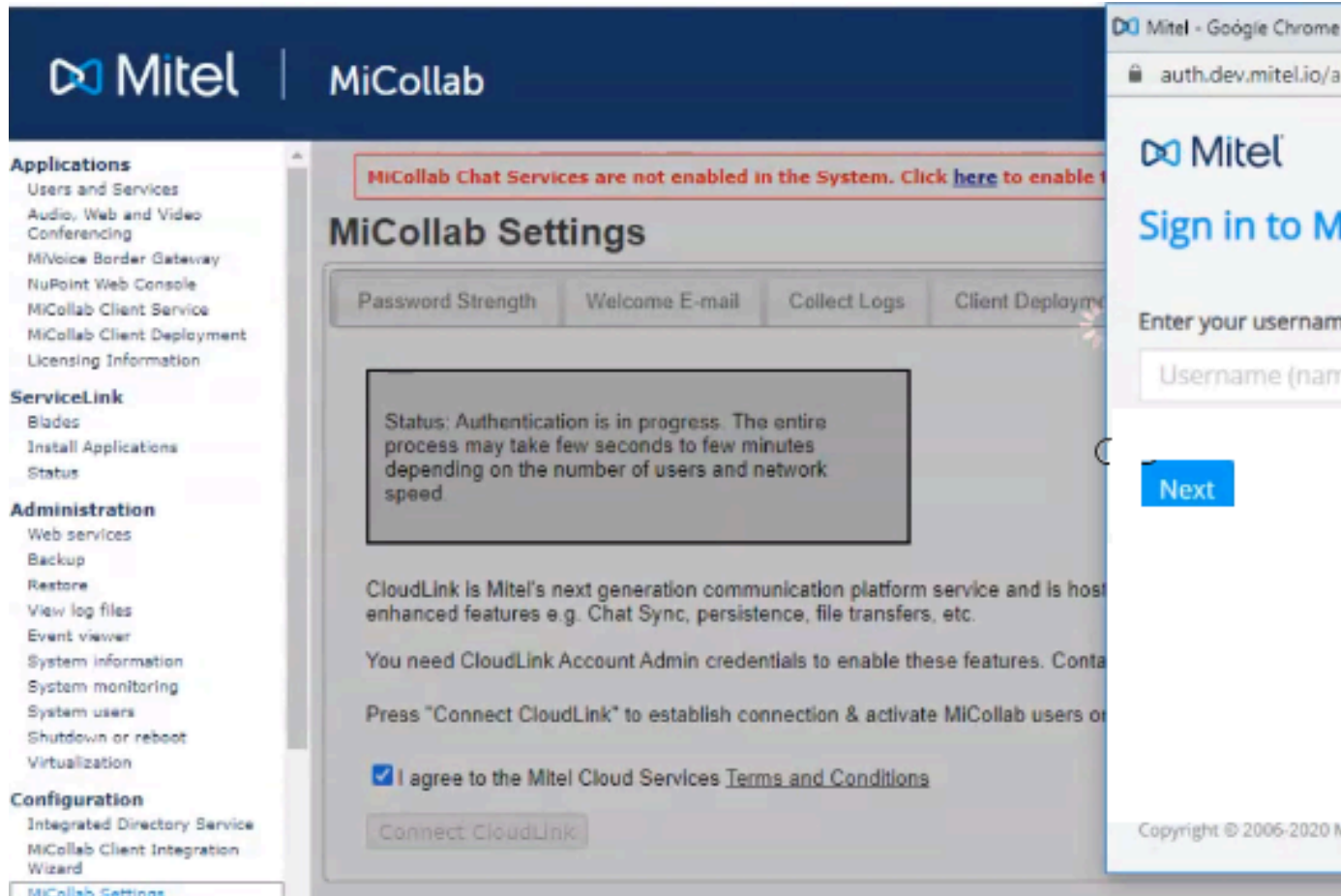
3. MiCollab will indicate: **You are being directed to Mitel Auth Portal for additional authentication. Make sure your web browser pop-up blocker is disabled. Do you want to proceed?**

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**.

Mitel | MiCollab

Applications

- Users and Services
- Audio, Web and Video Conferencing
- MiVoice Border Gateway
- NuPoint Web Console
- MiCollab Client Service
- MiCollab Client Deployment
- Licensing Information

ServiceLink

- Blades
- Install Applications
- Status

Administration

- Web services
- Backup
- Restore
- View log files
- Event viewer
- System information
- System monitoring
- System users
- Shutdown or reboot
- Virtualization

Configuration

- Integrated Directory Service**
- MiCollab Client Integration Wizard
- MiCollab Settings
- MiCollab Language

Integrated Directory Services

Add, edit, remove, and synchronize connections between MiCollab and external directory services.

[Add connection](#) [Manage detained entries \(0\)](#)

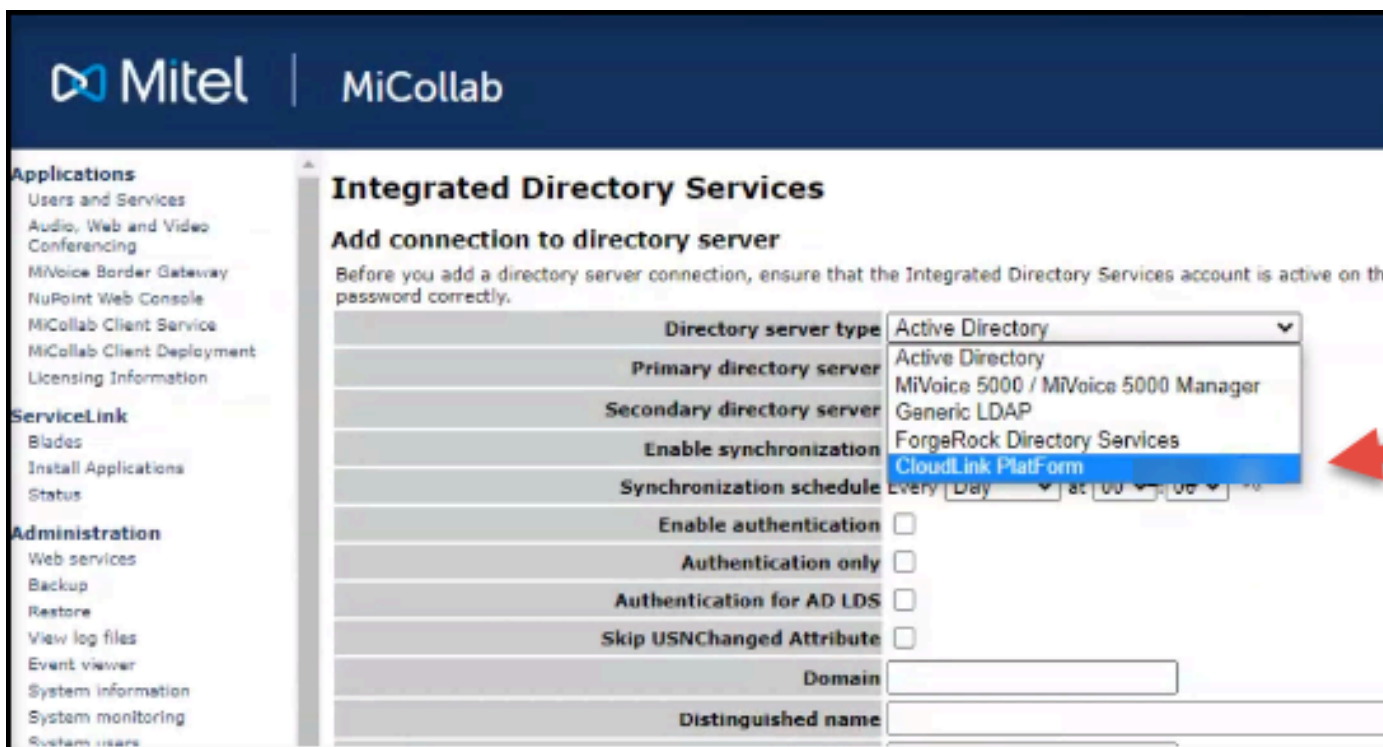
Domain	Last synchronization	Summary	Status	...

Default Attribute Mappings

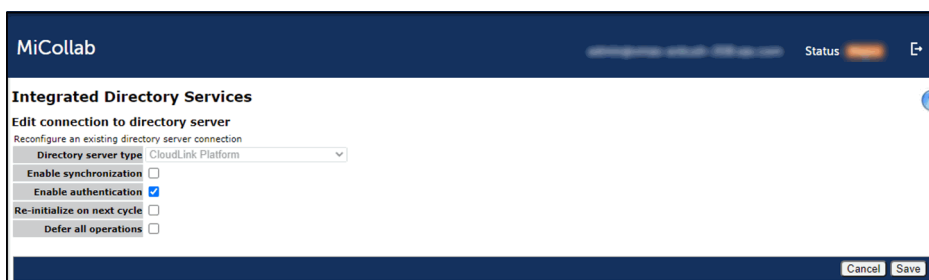
The following table maps the default directory services user data to the MiCollab user attributes. Each connection may use the default set or create its own set of mappings.

Directory Service Attribute	MiCollab Attribute
City	City
Company Name	Company Name
Country	Country
DID Number	DID Number
Department	Department
Distinguished Name	Distinguished Name
Email	Email
Fax	Fax
First Name	First Name
Home Element	Home Element

- 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.



- 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/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.

Home > Enterprise applications > scim > Provisioning >

Attribute Mapping

Save Discard

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	
displayName	displayName	
mail	emails[type eq "work"].value	
preferredLanguage	preferredLanguage	
givenName	name.givenName	
surname	name.familyName	
Join(" ", [givenName], [surname])	name.formatted	

Note:

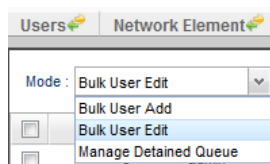
From R9.5 onwards, for performing the CloudLink Authentication procedure, the migrated user's login ID becomes the same as their Email ID. This behavior is valid for all the first-time users performing CloudLink Authentication. In case of manually or locally enabling and disabling CloudLink Auth from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

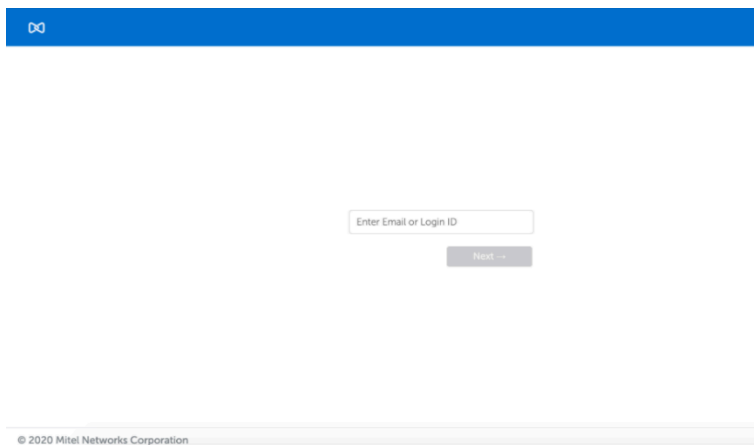
A **Password** pop-up will be opened.

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.

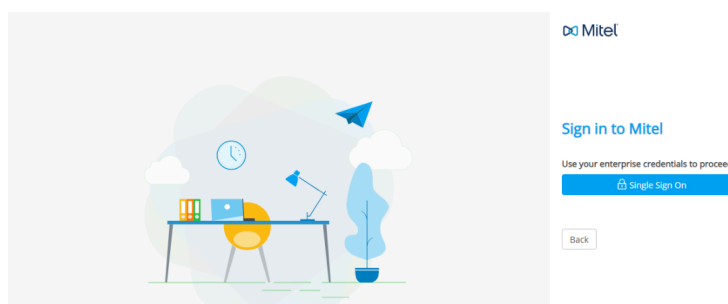
1.5.5 Using CloudLink-based Authentication on the MiCollab Clients

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**.



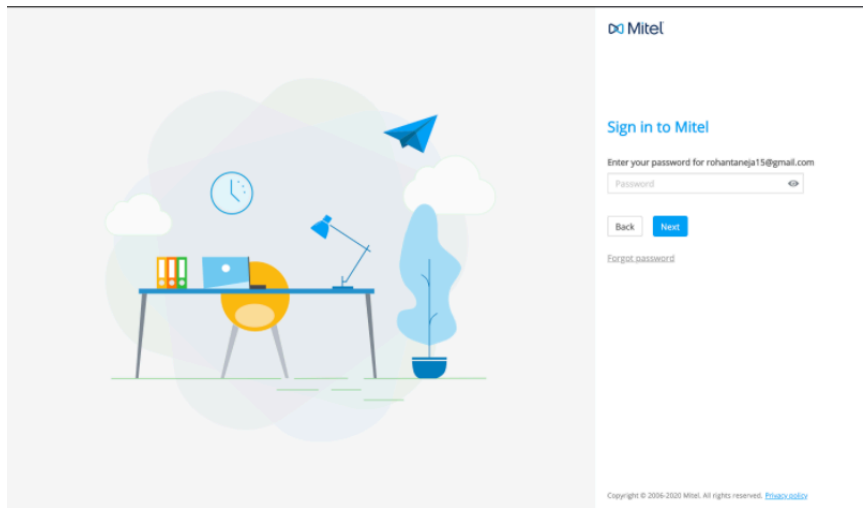
3. If CloudLink-based Authentication is enabled for the user, the MiCollab client will proceed for subsequent login through the CloudLink Unified login page.

- 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.

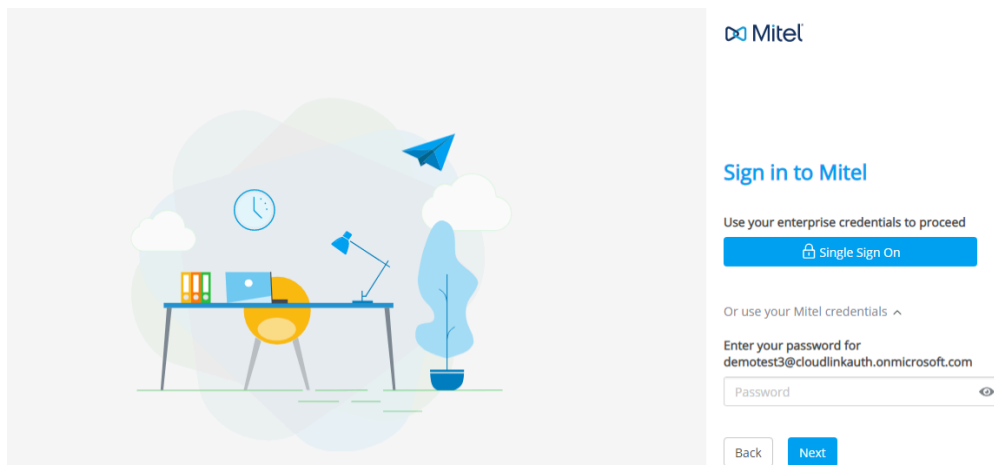


Note:

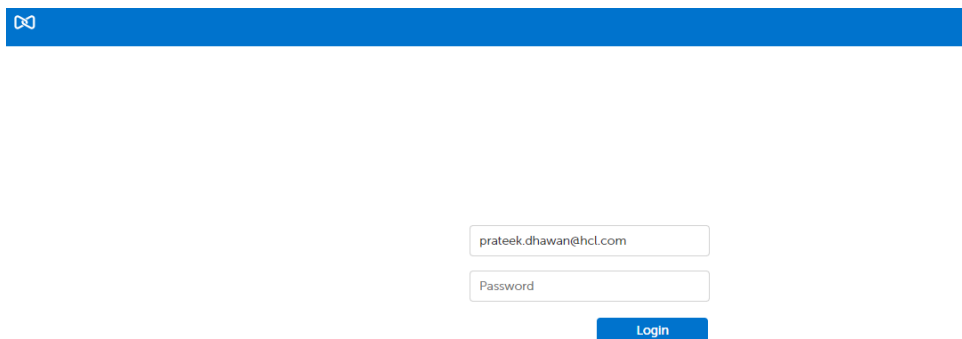
The Email ID is auto-populated on the CloudLink Sign-in page.



- 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).

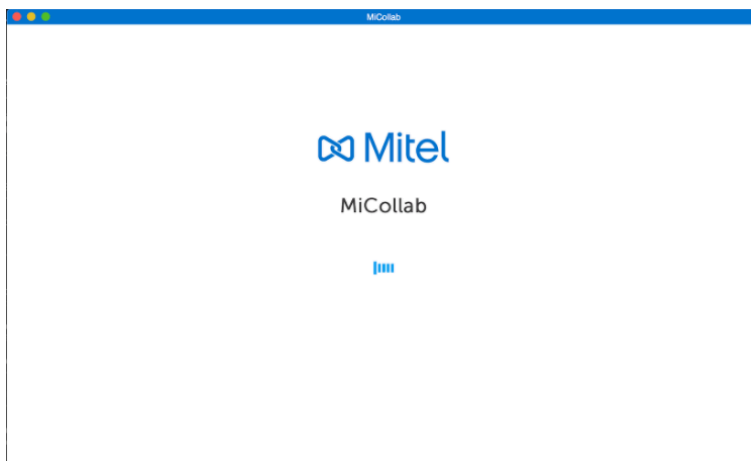


4. If CloudLink-based Authentication is not enabled, then the user proceeds for MiCollab Authentication and on providing the Email/Login ID on the same page, next the password field opens.

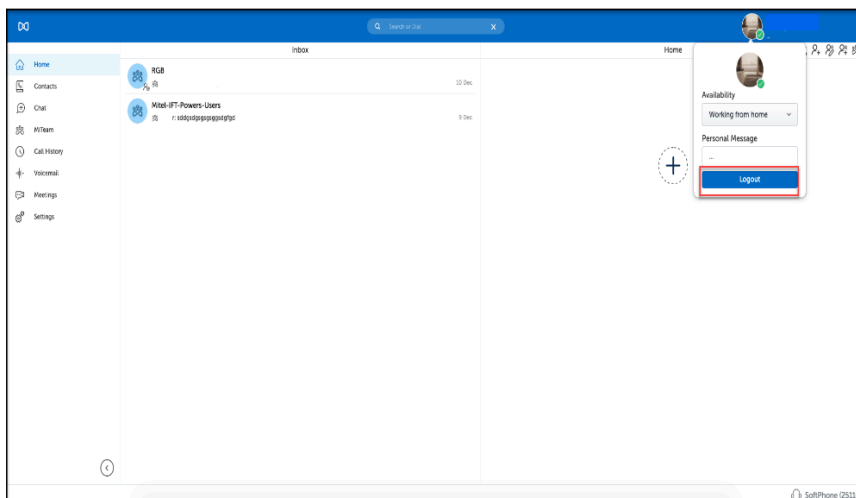


5. On successful password authentication, the user might be prompted to enter a second-factor authentication code, for example, OTP (based on Multifactor Authentication configuration done on Azure AD behind CL platform).
6. After the successful multifactor authentication, the client is presented with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

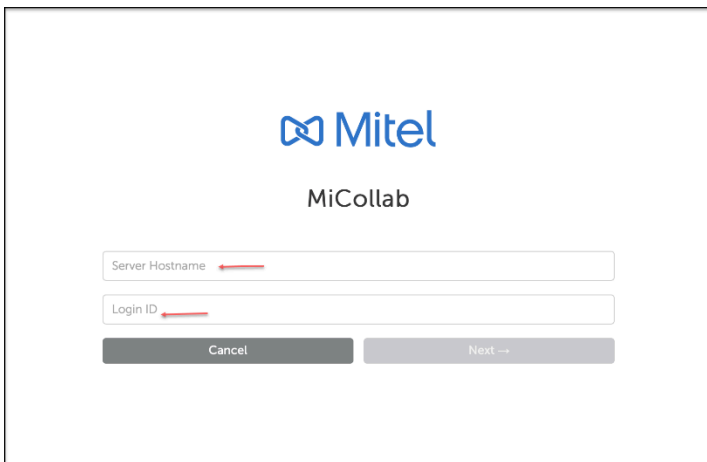
CloudLink Authentication also supports manual login in native clients (iOS, Android, PC, and MAC OS).

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

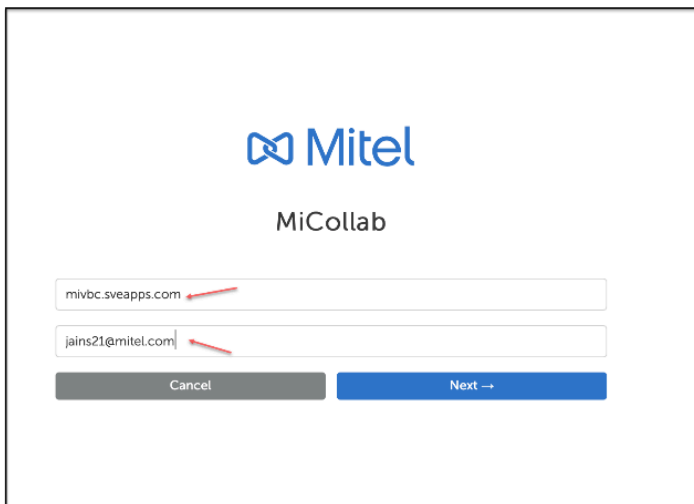
1. Tap on the Mitel logo three times to open the Manual Login screen.



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

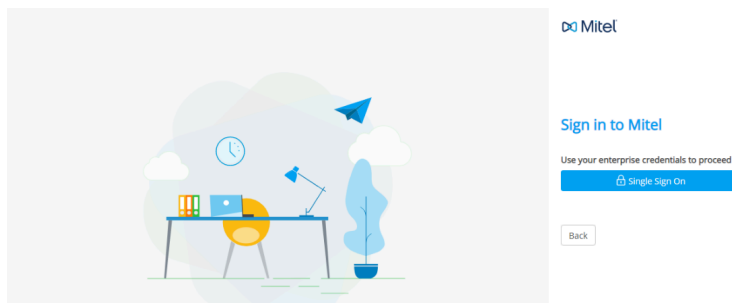


3. Click **Next**.



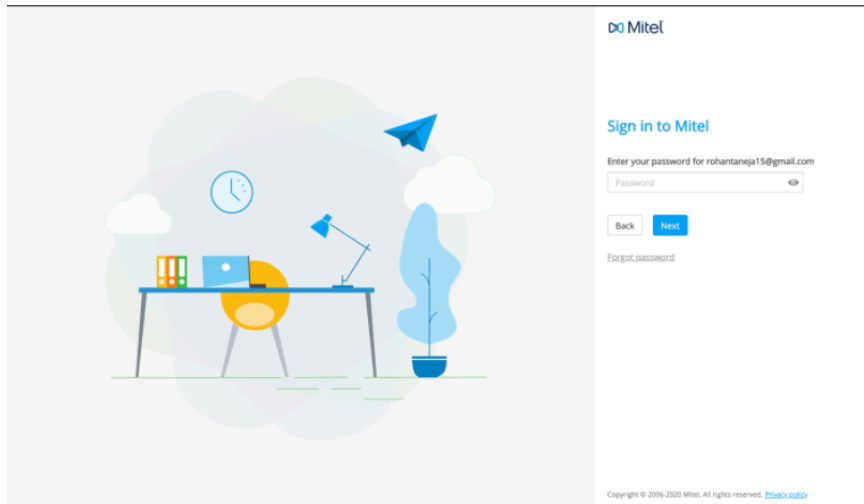
4. If CloudLink-based Authentication is enabled for the user, the MiCollab client will proceed for subsequent login through the CloudLink Unified login page.

- 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.io to setup your password if not done already.

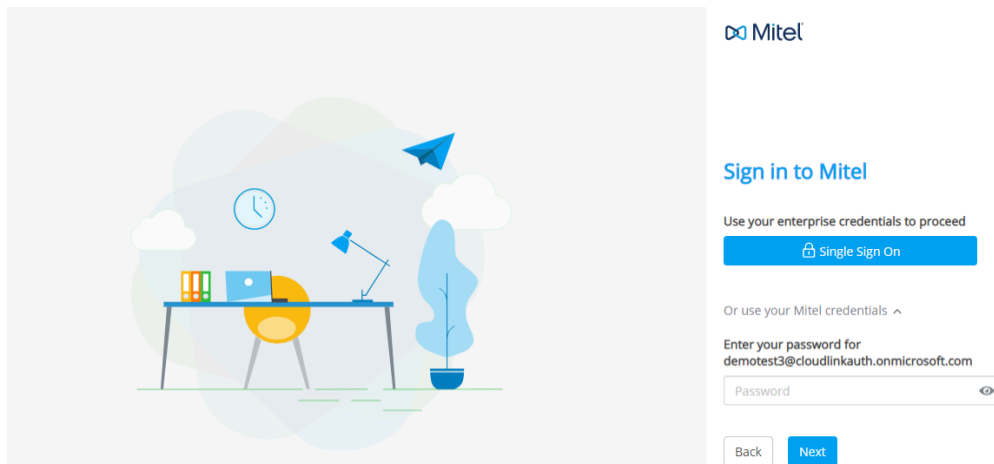


Note:

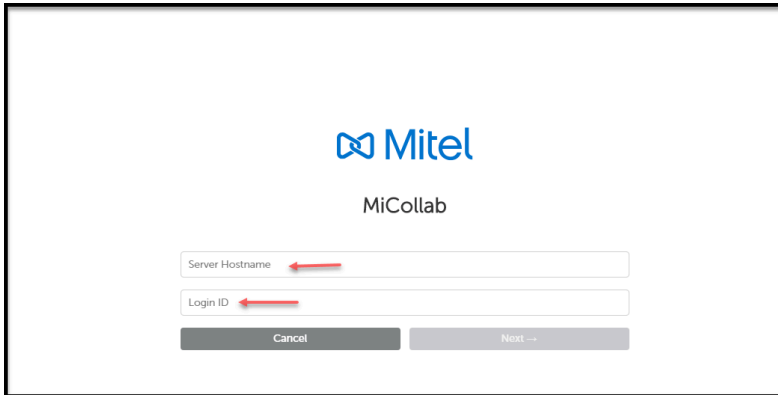
The Email ID is auto-populated on the CloudLink Sign-in page.



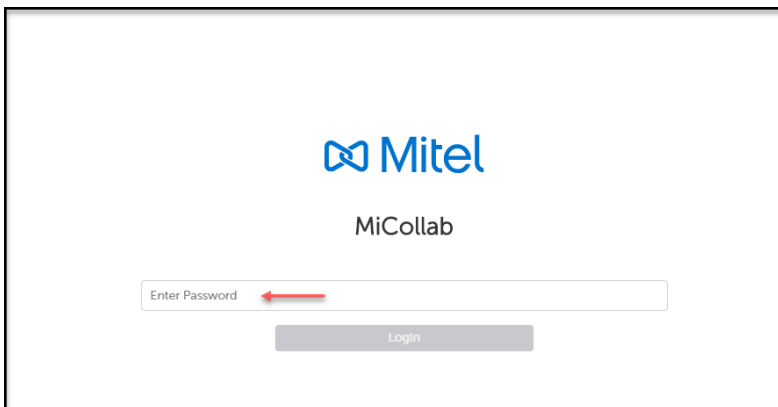
- Azure AD is integrated along with the field Enable Mitel Credentials (optional) over CloudLink Portal: In the CloudLink authorization page, you can use the credentials which were used to verify the account over CloudLink Portal (check Emails from no-reply@mitel.io to setup your password).



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.



The screenshot shows the Mitel MiCollab login interface. At the top is the Mitel logo, followed by the text "MiCollab". Below this are two input fields: "Server Hostname" and "Login ID". A red arrow points to the "Login ID" field. At the bottom are two buttons: "Cancel" and "Next -->".



The screenshot shows the Mitel MiCollab login interface. At the top is the Mitel logo, followed by the text "MiCollab". Below this is a single input field labeled "Enter Password". A red arrow points to this field. At the bottom is a "Login" button.

This chapter contains the following sections:

- [Prerequisites and Supported Platforms](#)
- [Limitations](#)
- [Setting up CloudLink Account for SCIM integration](#)
- [Setting up the Provisioning Server \(Azure AD\)](#)
- [Setting up Mitel SCIM Enterprise Application](#)
- [Setting up MiCollab for CloudLink-based Synchronization](#)
- [Adding a user in Azure Mitel SCIM enterprise application](#)

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.

CloudLink-based Synchronization

- 3rd Party Integrations will include Azure AD Sync as shown below:
- Select the **Add** button beside Azure AD 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

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

Integrations + Add new

MiCollab



MiTeam Meetings ⓘ



Azure AD Single Sign-On ⚙️



Azure AD Sync ⚙️



Click on **Complete setup**.

Integrations + Add new

Azure AD Sync

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 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.

 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

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

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/1...	Copy
Secret Token hEv@%B67RzX^M8dfkZKDwu+VHIC&#xyF	Copy

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.

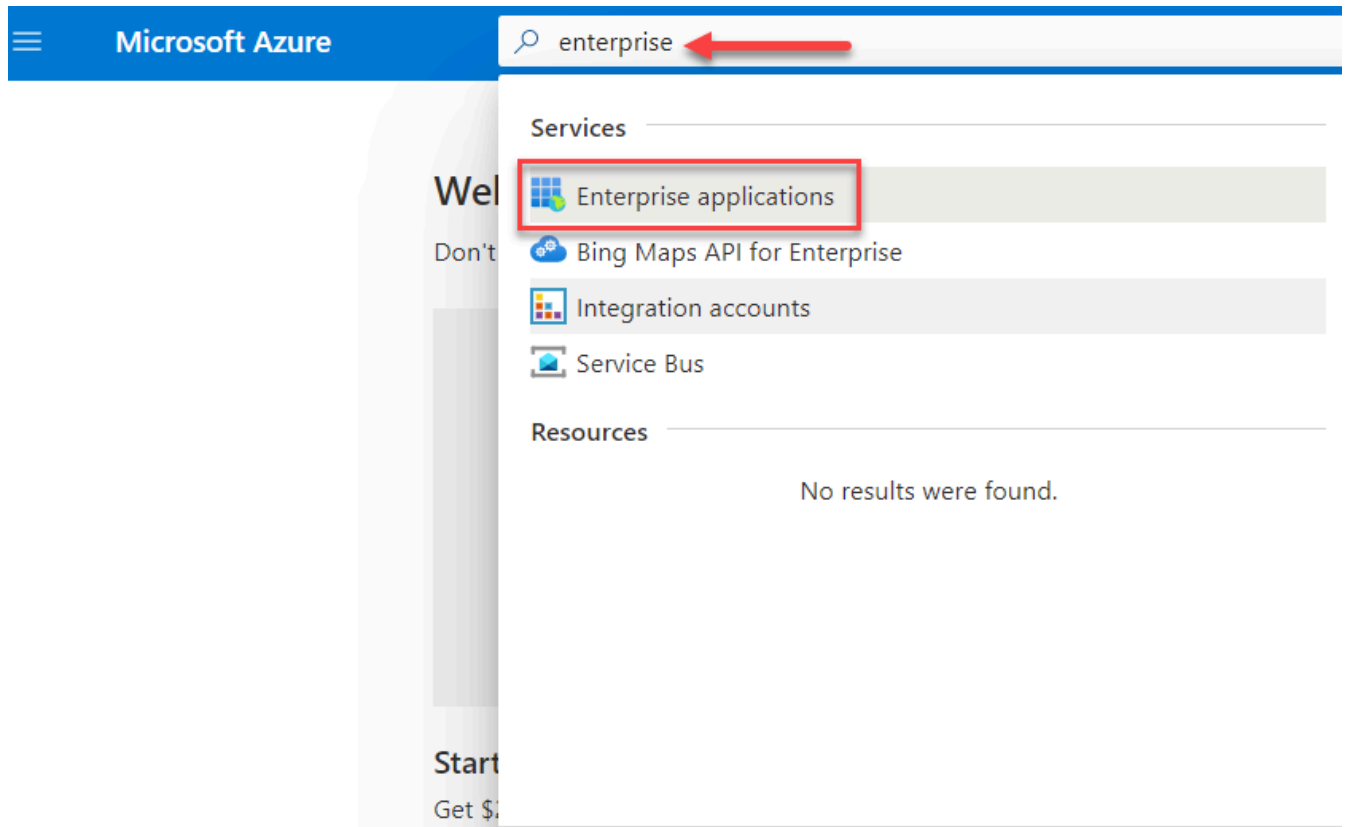
Note:

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.

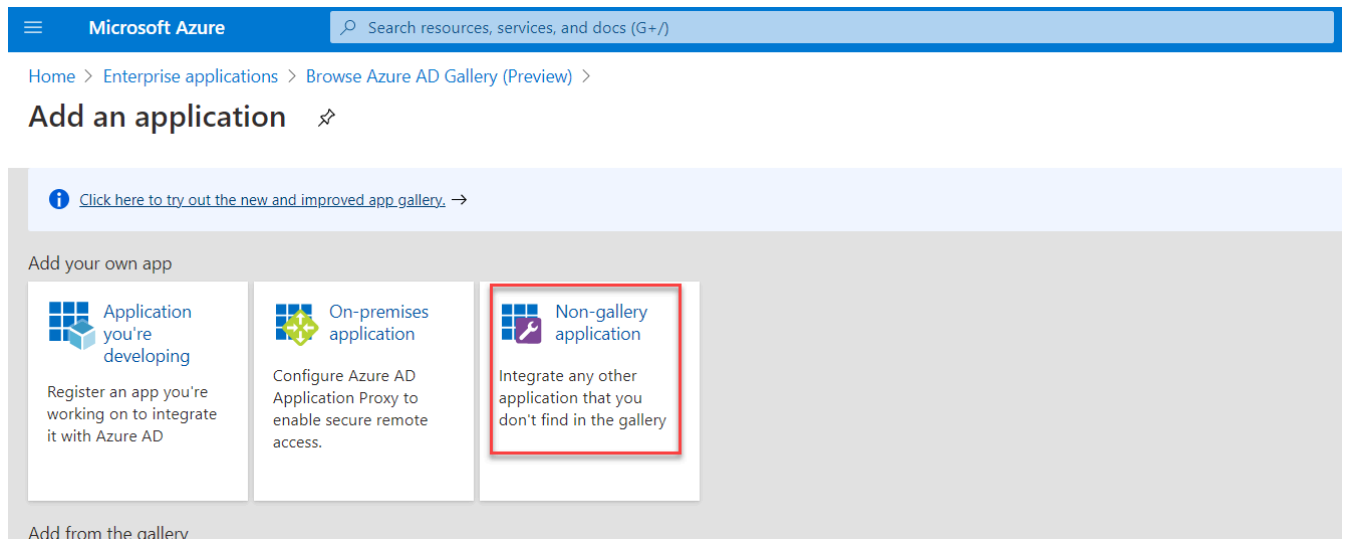
The screenshot shows the Microsoft Azure portal interface for Enterprise applications. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the user is in 'Home > Enterprise applications'. The main heading is 'Enterprise applications | All applications' with a subtext 'Default Directory - Azure Active Directory'. On the left sidebar, there are sections for 'Overview' (with links to Overview and Diagnose and solve problems) and 'Manage' (with links to All applications, Application proxy, User settings, Security, Conditional Access, and Consent and permissions). The 'New application' button is highlighted with a red box. Below this, there are filters for Application type (Enterprise Applications), Applications status (Any), and Application visibility (Any). A search bar prompts the user to enter a display name or application ID. A table lists applications with columns for Name and Homepage URL. The listed applications are Mitel Connect, scim, SCIM, and SCIM App.

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.

The screenshot shows the 'Browse Azure AD Gallery (Preview)' page in the Microsoft Azure portal. The title 'Browse Azure AD Gallery (Preview)' is highlighted with a red box. Below the title, there are links to 'Create your own application', 'Request new gallery app', and 'Got feedback?'. A link to 'Click here to switch back to the old app gallery experience. ->' is highlighted with a red box. The page features a search bar and filters for 'Single Sign-on: All', 'User Account Management: All', and 'Categories: All'. Under the 'Cloud platforms' section, there are four cards for Amazon Web Services (AWS), Google Cloud Platform, Oracle, and SAP. Under the 'On-premises applications' section, there are three cards: 'Add an on-premises application', 'Learn about Application Proxy', and 'Manage Application Proxy connectors'.

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



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 ✓

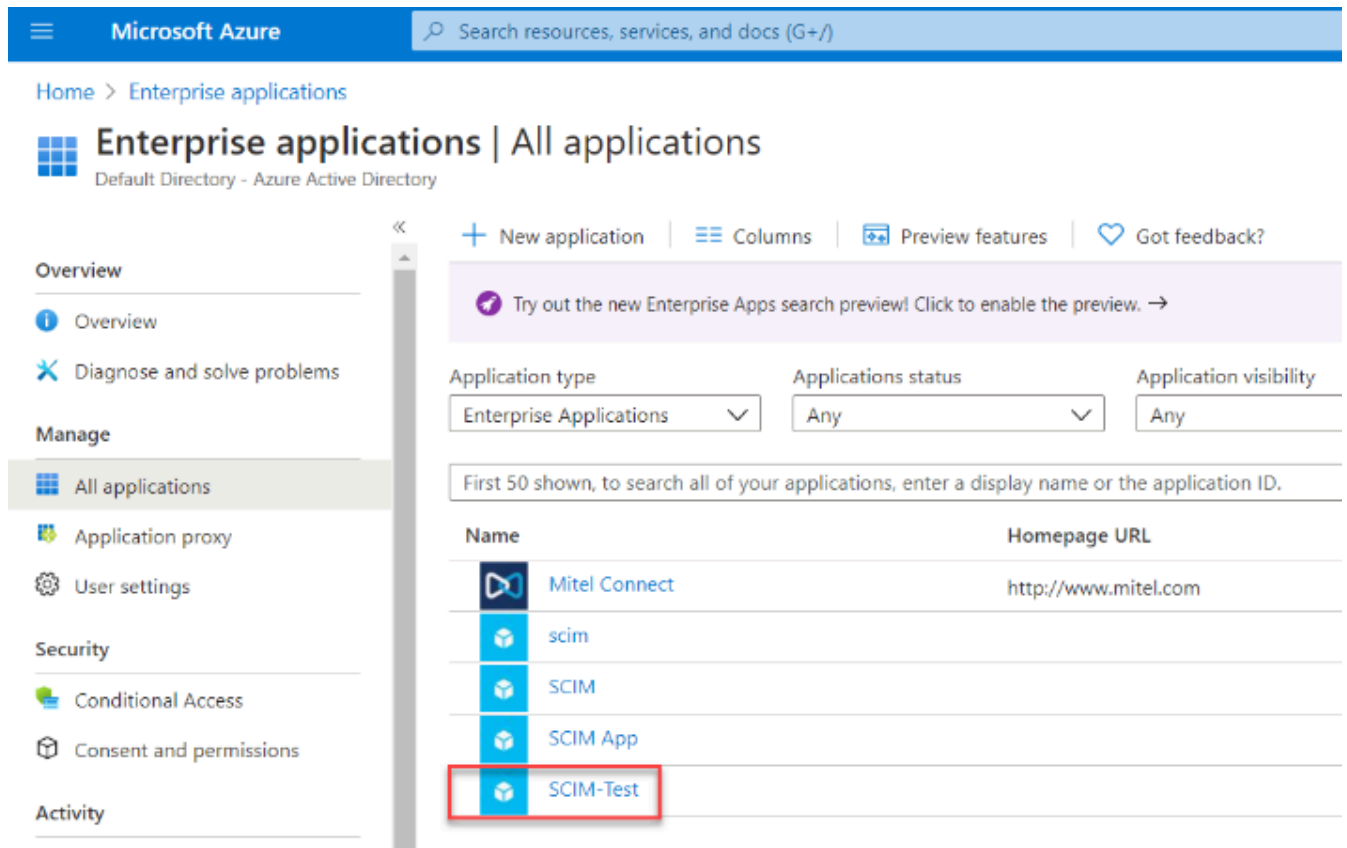
Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

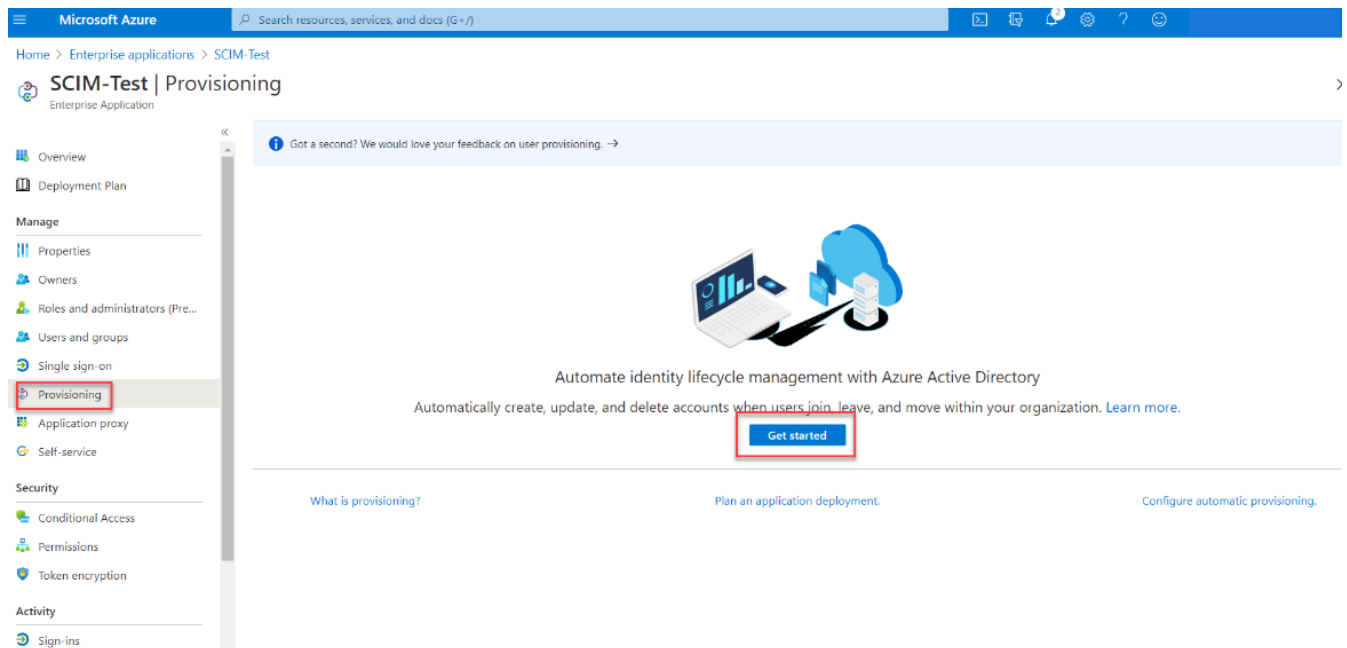
- SAML-based single sign-on
[Learn more](#)
- Automatic User Provisioning with SCIM**
[Learn more](#)
- Password-based single sign-on
[Learn more](#)

Add

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



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



- 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

Home > Enterprise applications > SCIMDoc >

Provisioning

Save Discard

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 *

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

Secret Token

Test Connection

Mappings

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

Microsoft Azure

Home > Enterprise applications > SCIMDoc >

Provisioning

Save Discard

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 *

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

Secret Token

Test Connection

Mappings

Settings

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

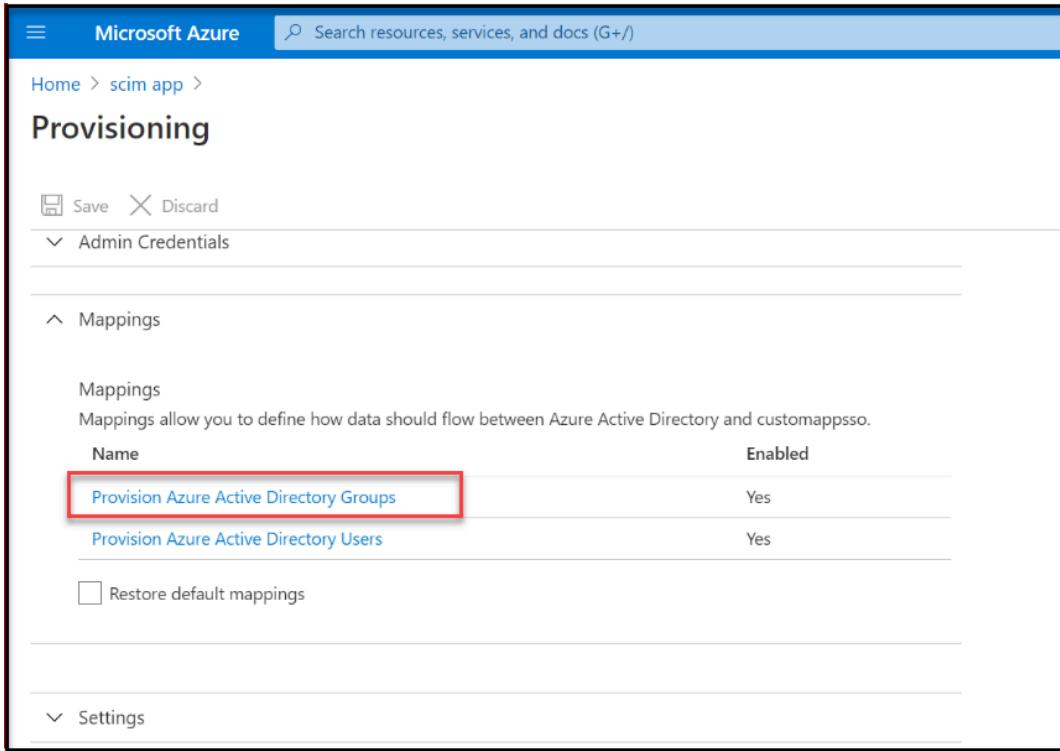
10. Under Mappings click on **Save your credentials to create mappings**.

The screenshot shows the Microsoft Azure portal interface for the 'Provisioning' section of an application named 'scim'. The breadcrumb trail is 'Home > Enterprise applications > scim > Provisioning'. At the top, there are 'Save' and 'Discard' buttons. The 'Provisioning Mode' is set to 'Automatic'. A note 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 fields for 'Tenant URL' and 'Secret Token'. The 'Tenant URL' contains the value 'https://admin.eu.dev.apimtel.io/2017-09-01/accounts/217baf22-0e83-4342-8d0e-edbf02...' and is marked as valid. The 'Secret Token' field is masked with dots. A 'Test Connection' button is located below these fields.

The 'Mappings' section is also expanded. It includes a description: 'Mappings allow you to define how data should flow between applications.' Below this is a table with two columns: 'Name' and 'Enabled'. The first row in the table has the text 'Save your credentials to create mappings' highlighted in yellow. Below the table is a button labeled 'Restore default mappings'.

The 'Settings' section is partially visible at the bottom, showing a 'Notification Email' field.

11. Click on Provision Azure Active Directory Groups.

The screenshot shows the Microsoft Azure portal interface for the 'scim app'. The page is titled 'Provisioning' and includes a search bar at the top. Below the title, there are buttons for 'Save' and 'Discard'. The main section is 'Mappings', which contains a table of mappings. The table has two columns: 'Name' and 'Enabled'. The first row is 'Provision Azure Active Directory Groups', which is highlighted with a red box. The second row is 'Provision Azure Active Directory Users'. Below the table, there is a checkbox for 'Restore default mappings'. At the bottom, there is a 'Settings' section.

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

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

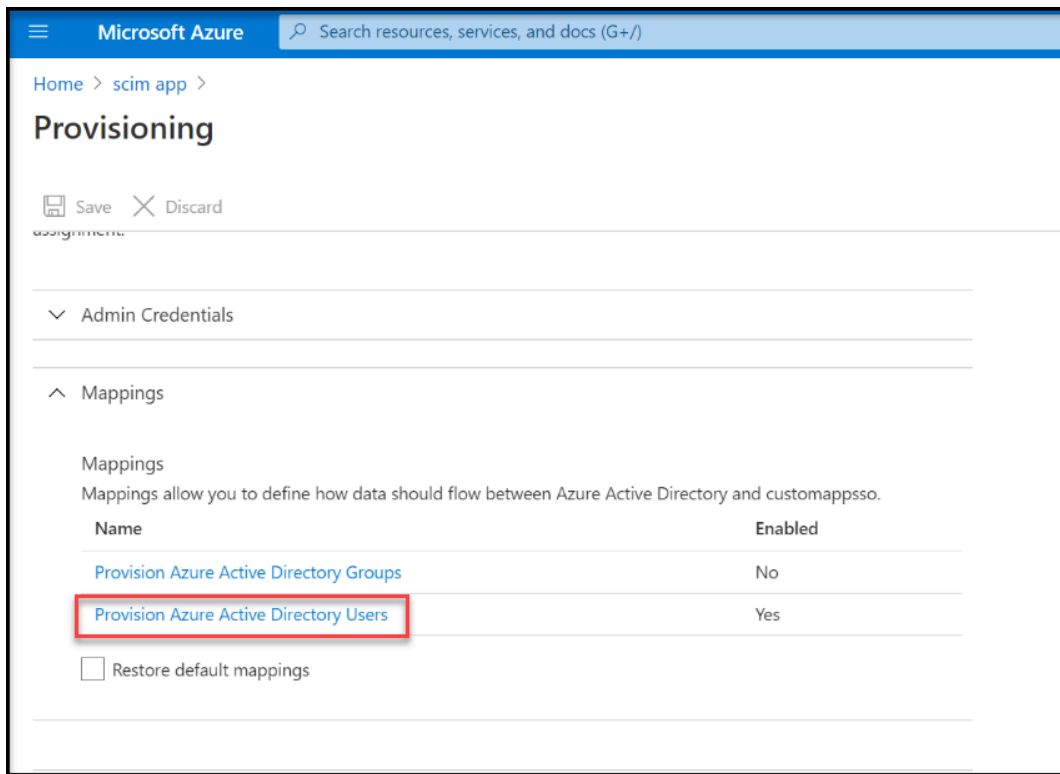
Source Object (Azure Active Directory)
Group

Source Object Scope
All records

Target Object (customappsso)
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 portal interface for the 'scim app'. The 'Provisioning' section is active, displaying a table of mappings. The 'Provision Azure Active Directory Users' mapping is highlighted with a red box. The table has two columns: 'Name' and 'Enabled'.

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

Below the table, there is a checkbox labeled 'Restore default mappings' which is currently unchecked.

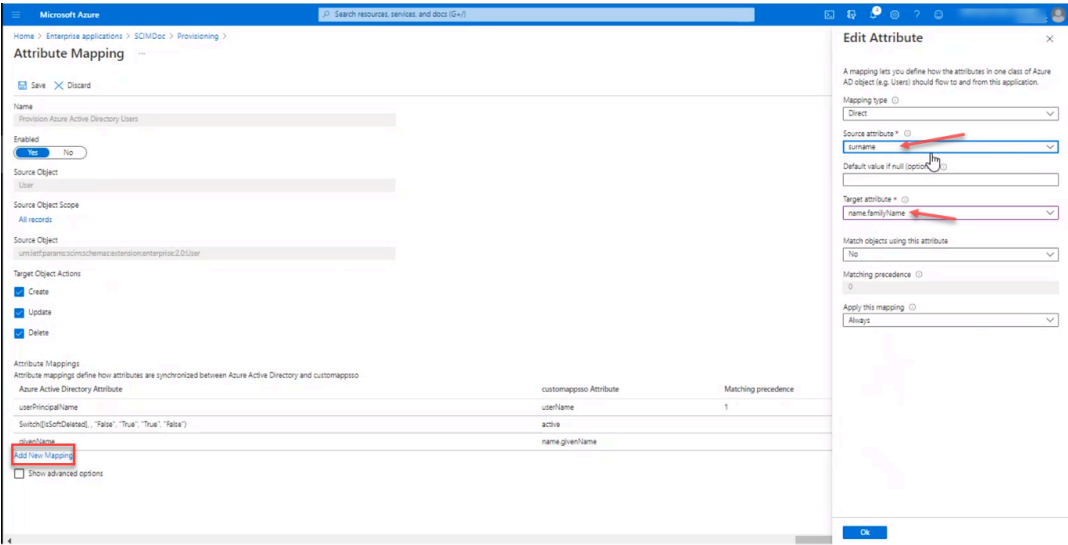
14. Add/Edit Attribute mappings

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.



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
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active

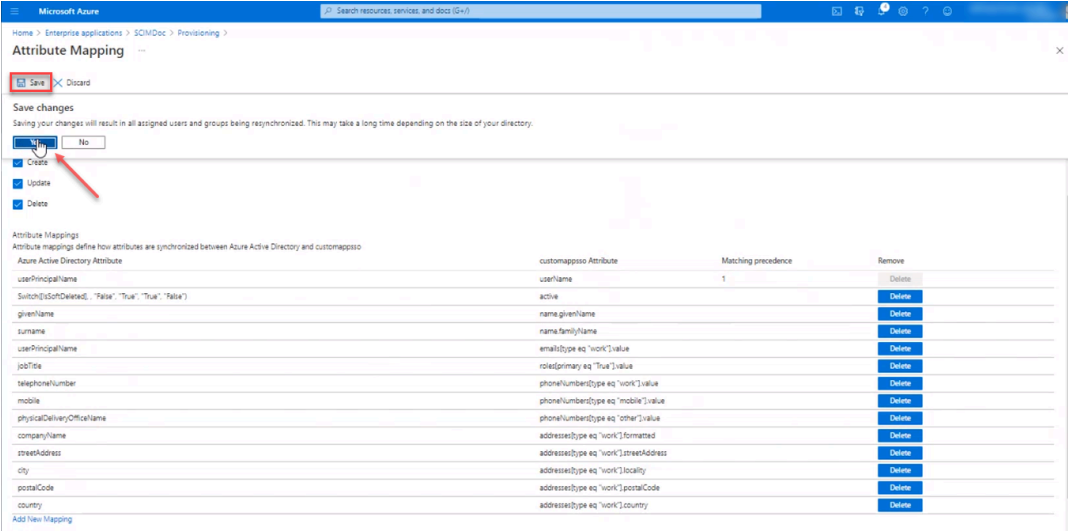
Azure AD Attributes	SCIM/Target Attributes
userPrincipalName	userName

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
telephoneNumber	phoneNumbers[type eq "work"].value	Primary Phone Directory Number (DN
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**.



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

Microsoft Azure

Home > Enterprise applications > scim >

Provisioning

Save **Discard**

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

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/Azure AD authentication for IDS step 1 to 6 for setting up CloudLink Integration and CloudLink Platform IDS.

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

- 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.
- 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.
- 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.

- 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:

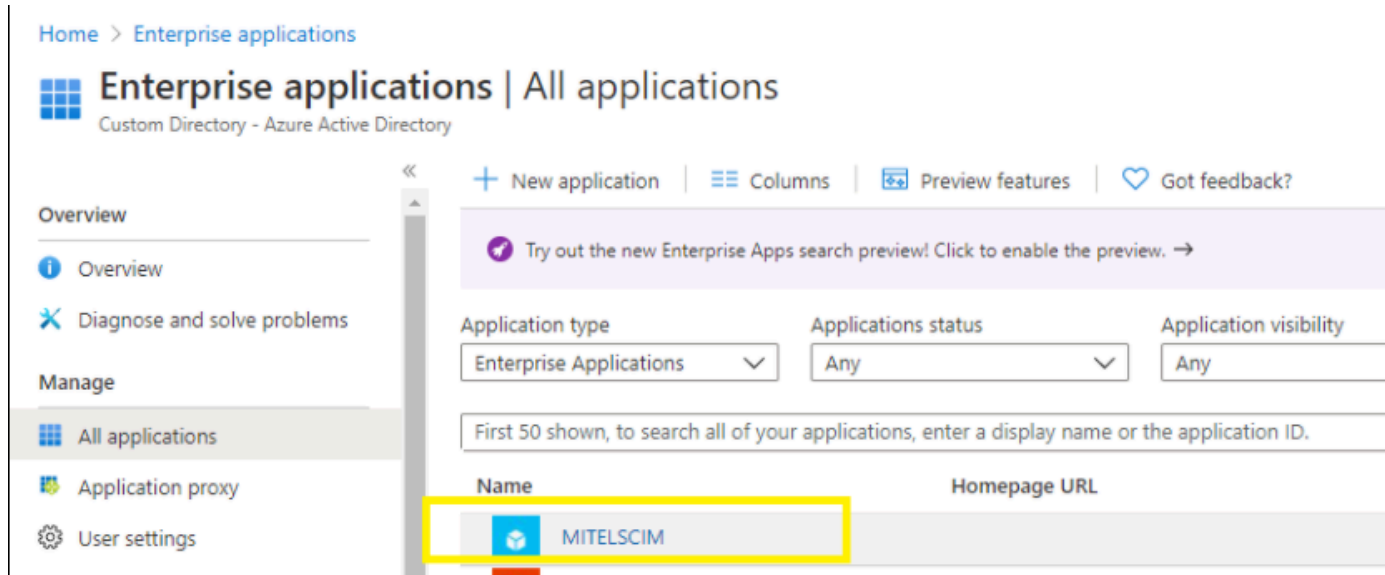
- Once the synchronization is enabled, the administrator will not be allowed to add a new user(s) from **Add**, and **Quick Add** options. Any new user addition and updates must be done from the provisioning server portal only. Refer to Table 1 Attribute Mappings for details on MiCollab attributes.
- 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**.



2. On the Mitel SCIM 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

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Pre...
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-ins

Properties

Name ⓘ

SCIM App

Application ID ⓘ

15a013d9-52b5-4d4f-828...

Object ID ⓘ

ca62a315-1084-4760-b9e...

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](#)
- 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 screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Enterprise applications > SCIM App. The main heading is 'SCIM App | Users and groups', with 'Enterprise Application' as a subtitle. A left-hand navigation pane lists various options under 'Manage', 'Security', and 'Activity'. The 'Users and groups' option is selected. The main content area features a toolbar with buttons: '+ Add user' (highlighted with a red box), 'Edit', 'Remove', 'Update Credentials', 'Columns', and 'Got feedback?'. Below the toolbar, a blue information banner states: '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 prompts the user to enter a display name to search all users and groups. Below this is a table with two columns: 'Display Name' and 'Object Type'. The table lists three users: 'Abhinay Trivedi' (AT), 'Addresstest' (AD), and 'createaftercodereview' (CR), all of which are of type 'User'.

Microsoft Azure

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

Home > Enterprise applications > SCIM App

SCIM App | Users and groups
Enterprise Application

Overview
Deployment Plan

Manage

Properties
Owners
Roles and administrators (Pre...
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

Security

Conditional Access
Permissions
Token encryption

Activity

Sign-ins

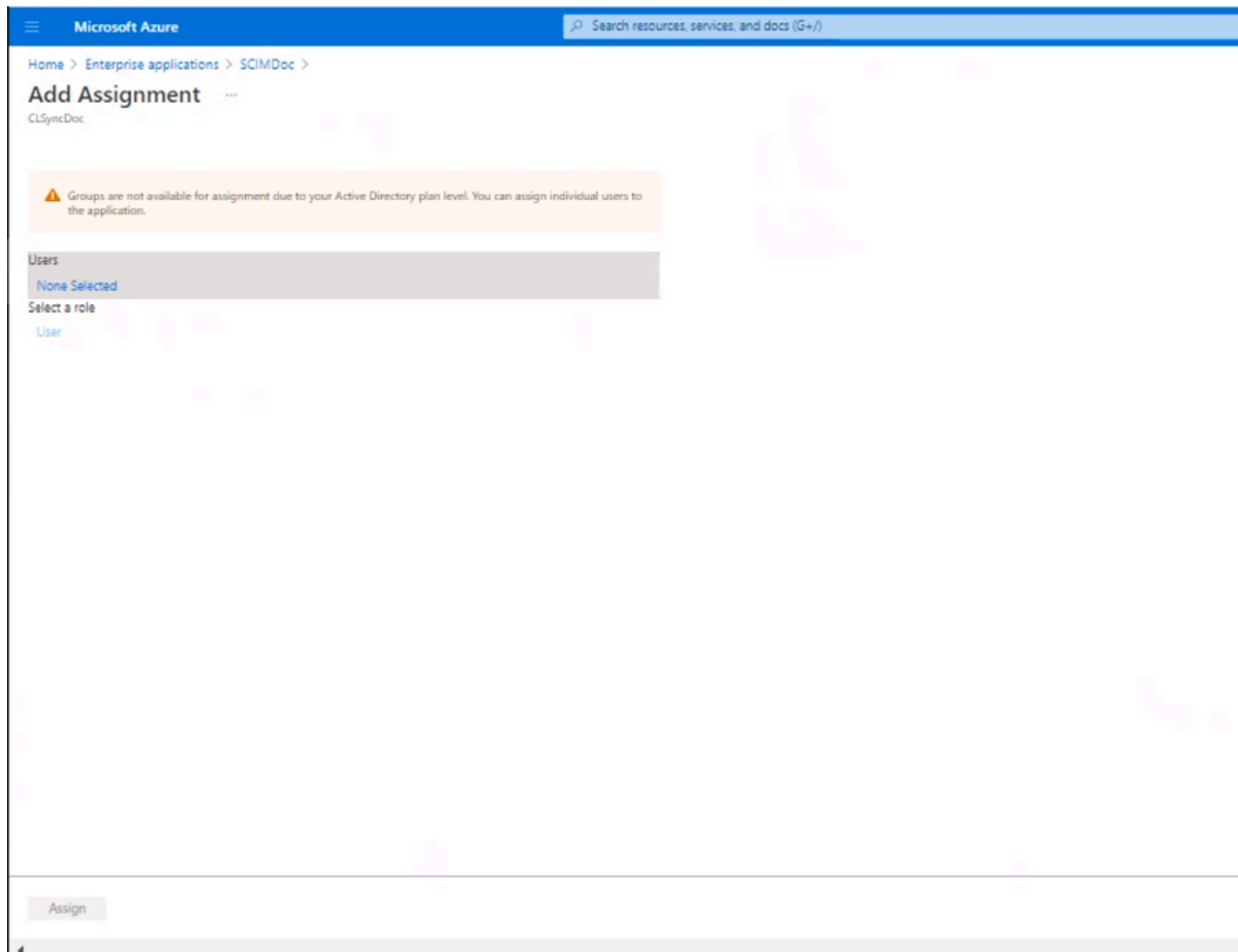
+ Add user Edit Remove Update Credentials Columns Got feedback?

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
☐ AT Abhinay Trivedi	User
☐ AD Addresstest	User
☐ CR createaftercodereview	User

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



5. Click **Assign**.

[Home](#) > [Enterprise applications](#) > [scim app](#) >

Add Assignment

HCL

Users and groups

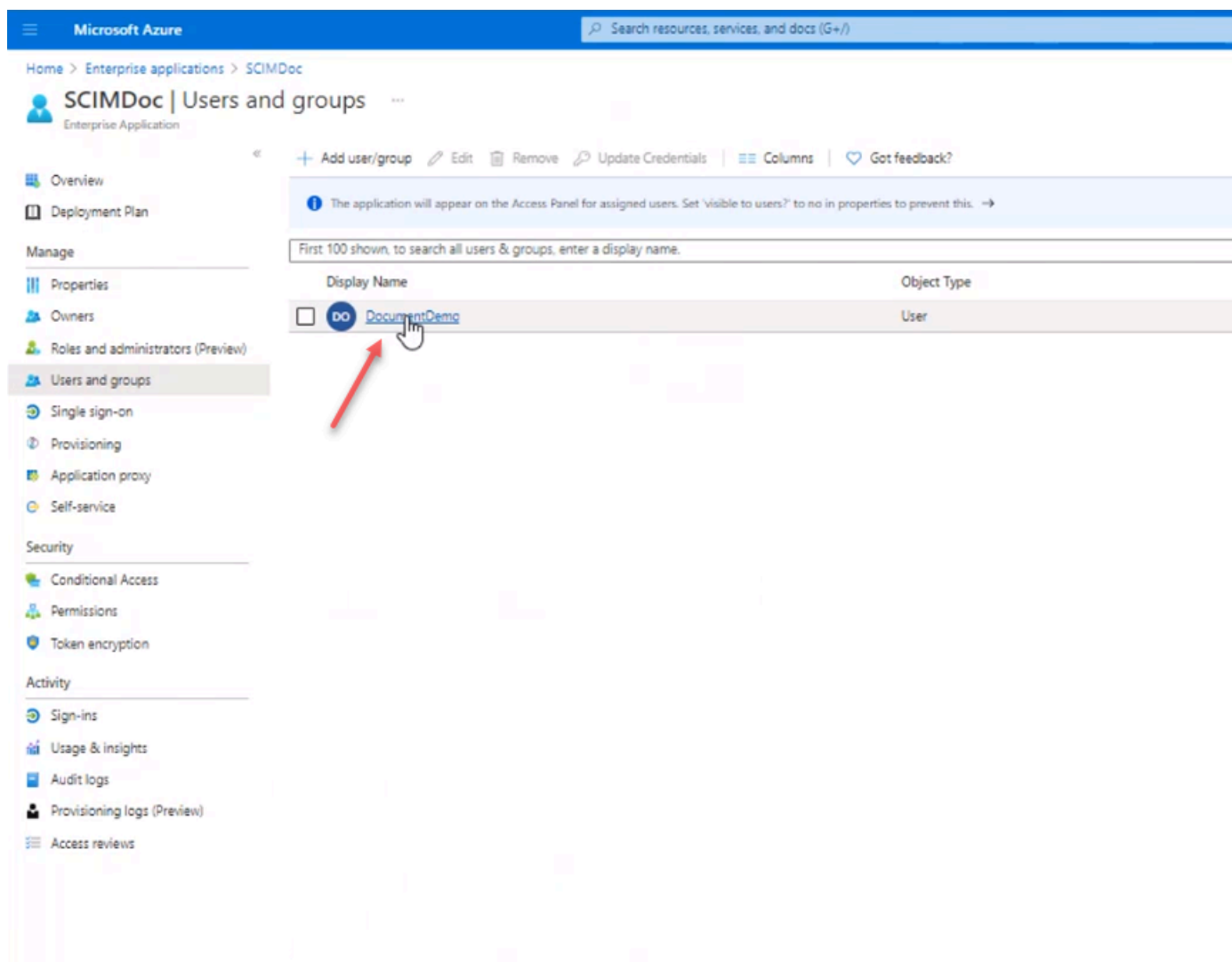
1 user selected.

Select a role

User

Assign

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



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 21 characters are present in the Email ID (characters before @ and shouldn't include @ and the domain part), the login ID will be truncated to 21 characters which will result in user creation failure and the users will be listed under the detained queue list.
- 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.

Troubleshooting Errors, Alarms and Reports

3

This chapter contains the following sections:

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

3.1 Alarms

Scenario	Alarm Text
When CL Adapter is down	ERROR – AUTHSERVICE_DOWN
When CL platform could not be connected from CL Adapter	ERROR – CL_CONNECT_FAILURE
SAS rest service is down	ERROR – REST_CONNECT_FAILURE
CL Adapter connection with CL platform breaks momentarily	ERROR – CL_CONNECT_FAILURE

3.2 Errors

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.
--	---

3.3 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

Table 3: 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

