cloudnine™ REVIEW

CLOUD CONNECTOR

Third Party Connection Setup and Configuration

Table of Contents

About CloudNine's Cloud Connector

Use Cloud Connector to securely extract Microsoft 365 email and OneDrive data directly into CloudNine Review. Cloud Connector eliminates the need to download content and generate mail stores (PSTs) and related files; instead, Microsoft 365 data is transferred and processed directly in CloudNine Review. Before using Cloud Connector, you must configure Microsoft Entra ID to securely grant this third-party application access to your Microsoft 365 tenant.

Create the Connection in Microsoft Entra ID

This guide provides a high-level overview of how to register an application in Microsoft Entra ID. Your organization is responsible for determining how to securely connect Microsoft Entra ID—and your data—to third-party applications in accordance with your security and compliance requirements.

Helpful Links

1. **Register an Application**: The foundational guide for creating an app identity in Entra ID.
2. **Configure API Permissions**: Detailed steps on how to add and authorize permissions for your registered app.
3. **Add a Redirect URI:** Security feature for Microsoft Entra ID authentication is sent to the intended recipient.
4. **Microsoft Graph Permissions Reference**: A complete list of all scopes for emails (Mail.*) and files (Files.*).
5. **Granting Admin Consent**: Instructions for administrators to approve high-privilege permissions tenant-wide.
6. **Restrict App To Users:** Provides information on restricting users that can access the app.

Prerequisites

- Global Administrator or Application Administrator role in Microsoft Entra ID.
- Assumed knowledge of Microsoft Entra ID and how to register an application.
- Active Microsoft 365 Subscription.

Step-by-Step Configuration in Microsoft Entra ID

Step 1: Register the Application in Microsoft Entra ID

Create an app identity that allows the third-party connector to authenticate.

1. Sign in to the Microsoft Entra Admin center and navigate to **Manage-App Registrations**.
2. Select **New Registration**.
3. Enter a **Name** for the application: For example, CloudNine Cloud Connector.
4. Set the **Supported account types**.
5. Accounts in this organizational directory only (Single tenant).
6. Redirect URI (See Step 2: Add a Redirect URI):
    a. CloudNine Connector settings:
        i. Public client/native (mobile/desktop).
        ii. http://Localhost:5000.
7. Click **Register** to create the app.

Step 2: Add a Redirect URI (required)

This step establishes the desktop connections for CloudNine Discovery Portal to Cloud Connector to send data directly to CloudNine Review.

1. Under **Manage**, select **Authentication**.
2. Under **Platform Configurations**, select **Add a platform**.
3. Choose **Mobile and desktop** applications.
4. In the **Redirect URI field**, enter **LocalHost:5000**.
5. Select **Configure** to complete.

Step 3: Configure API Permissions

Next, Microsoft Graph permissions must be added to access emails and files.

1. In your app registration, under **Manage,** click **API Permissions – Add a permission – Microsoft Graph**.
2. Select the **Permissions** type.
    a. **Delegated Permissions** (accesses API as a signed-in user).
3. **Add the required scopes**, for example:
    a. Emails: Select Mail.Read.
    b. OneDrive Files: Files.Read.

c. Calendars: Calendar.Read

4. **Grant Admin Consent:** To apply these privileges across the organization, you must select Grant admin consent for [Tenant Name].

Step 4: Generate and Capture Authentication Credentials

To complete the configuration, the Cloud Connector needs the following credentials found on the **App Overview** page.

- **Application (client) ID**
- **Directory (tenant) ID**
- **Client credentials**: Next to Client credentials, click **Add a certificate or secret** to create a new client secret.
    - On the **Certificates & secrets** page, select **Client Secrets** tab.
    - Click **New client secret**. Add a client secret appears at the right.
        - Enter a Description for the secret.
        - Expires: Choose when the secret expires, the MS Recommended is 180 days (6 months) and is automatically selected.
        - Click **Add.**
- **Immediately Copy the Secret ID**
    - **Note:** The **Client Secret Value** is permanently hidden once you navigate away from the page. Until you are ready to use it, you may want to paste it into Notepad or another text editor program.

Copy these three values: **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** to make the connection in CloudNine Review.

Optional: Restricting User Access for Registered Apps

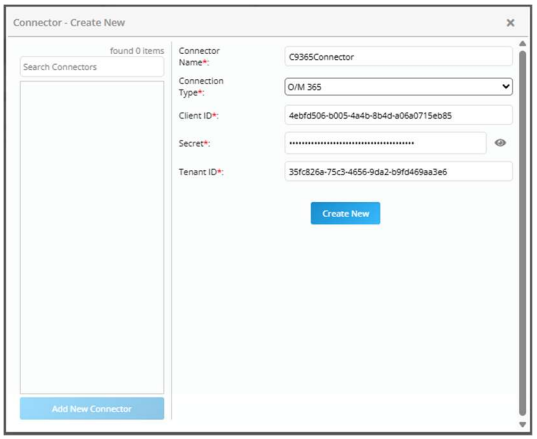
Once the Registered App is created, you can restrict the apps permission to selected users in the organization. Select **All Applications - <Registered Application> - Manage** to set user roles.

- **Properties - Enable Assignment Required**: Users must be assigned to access the registered app.
- **Users and groups:** Specify users that can access the app. Users not assigned to the registered app connection will fail.

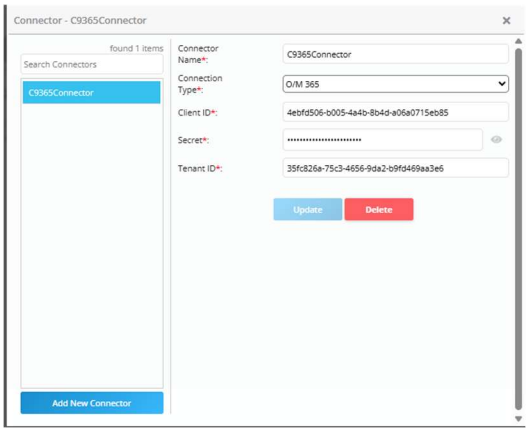
Making the Connection in CloudNine Review

You have the Registered Application in Microsoft Entra ID and have the required Credentials: **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret**. The next step is to add the Connector to CloudNine Review.

1. Log in to CloudNine Review.
2. On the **My Projects** page, select the **User** menu at the top right corner of the page to see drop-down menu options.
3. Choose **Connectors**.
    a. **Note:** Only CloudNine Review Global Admin users have rights to establish Connectors. If you do not have the Connectors option, contact a Global Admin to complete the connection.



4. The **Connector-Create New** window opens. Complete the following:
    a. **Connector Name:** Provide a name for the connector, such as 365 Connector.
    b. **Connection Type:** O/M 365.
    c. Paste the Authentication Credentials copied from Microsoft Entra ID.
        i. **Client ID:** This is the Application (client) ID.
        ii. **Secret.**
        iii. **Tenant ID:** This is the Direct (tenant) ID.
5. Click **Create New**. The Connector is created and appears under the Connectors list in the left column. To edit or delete the Connector, highlight the **Connector Name**, make any necessary changes, and then click **Update** or **Delete.**



Multiple Connectors can be added to CloudNine Review, allowing your IT administrator to register apps in Microsoft Entra ID to better control user access to specific data. For example, you may wish to have connectors created by location or department.

You have a Registered App in Microsoft Entra ID granting third party permissions to CloudNine's Cloud Connector and the Connector has been established in CloudNine Review. You will use CloudNine Discovery Portal to transfer the data from Cloud Connector to CloudNine Review.