



CLOUD CONNECTOR

Microsoft 365 & Purview Integration Guide:
Cloud Connector Configuration

Table of Contents

About CloudNine's Cloud Connector	3
Prerequisites & Required Roles	3
Helpful Links	3
Microsoft Entra ID Application Registration Requirements	4
Configuration Requirements	4
Required Permissions.....	4
1. Microsoft 365 API Permissions (Microsoft Graph API).....	4
2. Microsoft Purview Permissions (Data Governance & eDiscovery)	5
Compliance Role Group Mapping	6
Making the Connection in CloudNine Review	7

About CloudNine's Cloud Connector

CloudNine's Cloud Connector securely transfers Microsoft 365 and Microsoft Purview Email and OneDrive data directly into CloudNine Review. Instead of downloading content and creating manual mail stores (such as PST files), data is transferred and processed seamlessly within CloudNine Review.

To establish this connection, an administrator must register an application within Microsoft Entra ID to grant secure programmatic access to your organization's tenant.

Prerequisites & Required Roles

Before beginning the configuration, ensure your account possesses the necessary administrative roles:

- **Active Subscriptions:** An active Microsoft 365 subscription or Microsoft Purview eDiscovery (Premium) account.
- **Microsoft Entra ID Role:** Global Administrator, Application Administrator, or Application Developer (required to register the application).
- **Microsoft Purview Role:** Data Governance Administrator or Compliance Administrator (required to map permissions and view audit logs).

Helpful Links

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

Microsoft Entra ID Application Registration Requirements

To establish the third-party connection, an application must be registered within your Microsoft Entra ID tenant with the following parameters.

Configuration Requirements

- **Supported Account Types:** Single Tenant only.
- **Redirect URI:** Must be configured as a **Public client/native (mobile/desktop)** platform with the URI: <http://localhost:5000>.

Add a Redirect URI (required)

The Redirect URI is necessary for the desktop application, CloudNine Discovery Portal and Cloud Connector to send data 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 **http://localhost:5000**.
 5. Select **Configure** to complete.
- **Authentication Credentials to Capture:**
 - **Application (client) ID**
 - **Directory (tenant) ID**
 - **Client Secret Value** (*Note: This value must be copied immediately upon generation as it is permanently obscured once you navigate away from the page.*)
 - **Note:** When a client secret expires, delete the existing connector, then recreate as a new connector.

Required Permissions

1. Microsoft 365 API Permissions (Microsoft Graph API)

To allow the Cloud Connector to securely access email, calendar, and OneDrive data, the registered application requires the following Microsoft Graph API scopes:

API / Permission Name	Type	Admin Consent Required
Calendars.Read	Application	Yes
Files.Read.All	Application	Yes

API / Permission Name	Type	Admin Consent Required
Mail.Read	Application	Yes
User.Read.All	Delegated	Yes

Optional Access Control: Once registered, access can be restricted by enabling "Assignment Required" in the application properties, limiting data exposure only to specified users and groups.

2. Microsoft Purview Permissions (Data Governance & eDiscovery)

To allow interaction with your Purview tenant, the application's Service Principal must be mapped and authorized with compliance and eDiscovery permissions.

Required API Scopes

API / Permission Name	Type	Admin Consent Required
Microsoft Graph		
eDiscovery.Read.All	Delegated	Yes
eDiscovery.Read.All	Application	Yes
Goals-Export.Read.All	Delegated	Yes
Microsoft Purview		
Purview.ApplicationAccess	Application	Yes
Microsoft Purview eDiscovery		

API / Permission Name	Type	Admin Consent Required
eDiscovery.Download.Read	Application	Yes
Office 365 Exchange Online		
User.Read.All	Delegated	Yes

Compliance Role Group Mapping

The application's Service Principal must be added directly as a member of one of the following active Role Groups within the Microsoft Purview portal:

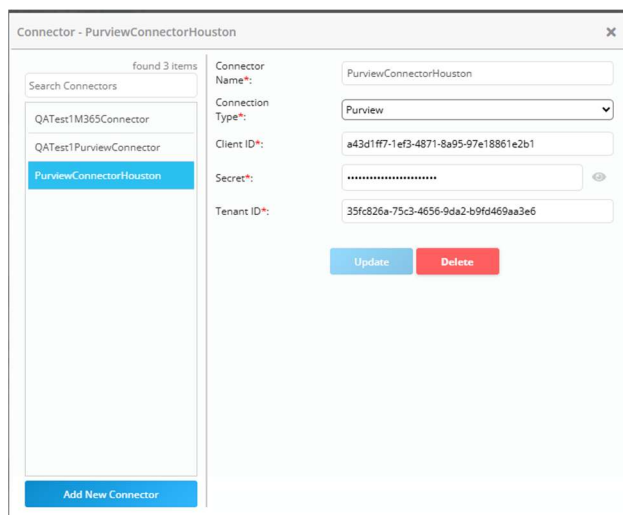
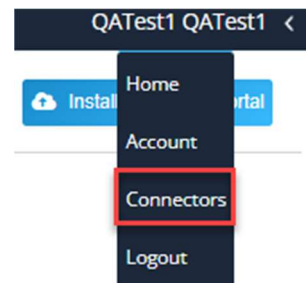
- **eDiscovery Manager** (Required for processing data for review)
- **Compliance Administrator**

Making the Connection in CloudNine Review

Once the application is registered in Microsoft Entra ID and permissions are assigned, follow these steps to set up the active connector in CloudNine Review.

Note: Only CloudNine Review Global Administrator users have rights to establish Connectors. If the option is unavailable, contact your administrator.

1. Log in to CloudNine Review.
2. On the My Projects page, select the User Menu in the top-right corner and choose **Connectors**.
3. In the **Connector - Create New** window, populate the following fields:
 - a. **Connector Name:** Type a unique identifying name (e.g., `365Connector` or `PurviewConnector`).
 - b. **Connection Type:** Select either **Purview** or **O/M 365** from the drop-down list.
 - c. **Client ID:** Paste the *Application (client) ID* copied from Microsoft Entra ID.
 - d. **Secret:** Paste the *Client Secret Value* generated in Microsoft Entra ID.
 - e. **Tenant ID:** Paste the *Directory (tenant) ID* copied from Microsoft Entra ID.



4. 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**.

Note: 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.