



CLOUD CONNECTOR

Microsoft Purview Integration Guide:
Cloud Connector Configuration

Table of Contents

About CloudNine's Cloud Connector	3
Before you Begin.....	3
Information to Capture	3
Helpful Microsoft Resources	3
Step1: Register the Application in Microsoft Entra ID	4
Step 2: Create a Client Secret.....	4
Step 3: Add a Redirect URI (required)	5
Step 4: Assign API Permissions	5
Grant Administrator Consent	6
Step 5: Assign Microsoft Purview Roles and Permissions.....	6
Role Groups Overview	6
Step 6: Grant Access to eDiscovery Cases	6
Step 7: Create the Connector in CloudNine Review	7

About CloudNine's Cloud Connector

CloudNine's Cloud Connector provides a secure path for transferring Microsoft Purview eDiscovery data, including Exchange Online mailboxes and OneDrive content, into CloudNine Review. The connector reduces reliance on manual exports and mail-store handling by allowing approved Purview data to be ingested directly into the review platform.

This guide explains the two-part configuration process: first, creating and permissioning the third-party application connection in Microsoft Entra ID and Microsoft Purview; second, adding the resulting connection details in CloudNine Review so the connector can collect data.

Before you Begin

Ensure the following prerequisites are met before starting configuration.

Microsoft Requirements

- Microsoft Purview eDiscovery licensing is enabled for the tenant.
- A Microsoft Entra ID Global Administrator or Cloud Application Administrator is available to register an application and grant administrator consent.
- A Microsoft Purview administrator has permission to manage role groups and eDiscovery access.

CloudNine Requirements

- You have CloudNine Review Global Administrator permissions.
- You can access the Connectors administration area within CloudNine Review.

Information to Capture

During setup, record the following values:

- Application (Client) ID
- Directory (Tenant) ID
- Client Secret Value

You will need these values to configure the connector in CloudNine Review.

Helpful Microsoft Resources

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](#): A security feature for Microsoft Entra ID authentication, 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.
7. [Permissions in Microsoft Purview portal](#): Management of permissions for users performing tasks in Microsoft Purview.

Step 1: Register the Application in Microsoft Entra ID

Cloud Connector authenticates to Microsoft 365 through a dedicated application registration. This application establishes a secure trust relationship between your Microsoft environment and CloudNine Review.

Create the Application

1. Sign in to the **Microsoft Entra Admin Center**.
2. Navigate to **Identity-> Applications-> App registrations**.
3. Select **New Registration**.
4. Enter the following configuration:
 - a. **Name**: CloudNine Cloud Connector Purview Ingestion
 - b. **Supported Account Types**: Accounts in this organizational directory only (Single tenant).
5. Click **Register**.
6. **Copy** and **Save** the following; you will use these values later when creating the Cloud Connector.
 - a. **Application** (Client) ID
 - b. **Directory** (Tenant) ID

Step 2: Create a Client Secret

Cloud Connector uses a client secret to securely authenticate with Microsoft services.

1. Open the application registration.
2. Select **Certificates & secrets**.
3. Select **New Client Secret**.
4. Enter a description and expiration period.
5. Create the secret.

Important: Microsoft displays the secret value only once. Copy and securely store the secret immediately. Once you leave the page, you cannot view the value again.

Managing Secret Expiration

To avoid service interruptions:

- Monitor secret expiration dates.
- Create a replacement secret before the existing secret expires.
- Update the Cloud Connector configuration with the new secret value.

Step 3: Add a Redirect URI (required)

A Redirect URI is necessary for the desktop application, CloudNine Discovery Portal, and Cloud Connector to pull data from Purview and send data to CloudNine Review.

1. Select **Authentication**.
2. Choose **Add a platform**.
3. Select **Mobile and Desktop Applications**.
4. Enter **http://LocalHost:5000**.
5. Select **Configure**.

Step 4: Assign API Permissions

Cloud Connector requires access to Microsoft Graph and Microsoft Purview APIs to discover and collect approved eDiscovery content.

1. Navigate to **API Permissions -> Add a permission**.
2. Select **Microsoft Graph**, then choose **Application Permissions**.
3. Add the following permissions:

API / Permission name	Type	Description	Admin consent required
Microsoft Graph			
eDiscovery.Read.All	Delegated	Read all eDiscovery objects	Yes
eDiscovery.Read.All	Application	Read all eDiscovery	Yes
offline_access	Delegated	Maintain access to data you have given it access to	No
openid	Delegated	Sign users in	No
profile	Delegated	View users' basic profile	No
User.read	Delegated	Sign in and read user profile	No
Microsoft Purview			
Purview.ApplicationAccess	Application	Purview Application API Access	Yes
Purview.ApplicationAccess	Delegated	Purview Delegated API Access	No
MicrosoftPurviewEDiscovery			
eDiscovery.Download.Read	Application	eDiscovery.Download.Read	Yes
Office 365 Exchange Online			
User.Read.All	Delegated	Read all users' full profiles	Yes

Grant Administrator Consent

After permissions have been assigned:

1. Select **Grant Admin Consent**.
2. Confirm the request.
3. Verify all required permissions display a status of **Granted**.

Step 5: Assign Microsoft Purview Roles and Permissions

API permissions determine what the application can request. Microsoft Purview roles determine what content the application can access and manage.

Role Groups Overview

Add the service principal or authorized user to the appropriate Microsoft Purview role group based on the level of access required:

In the Microsoft Purview Portal, go to **Settings -> Roles and Scopes -> Role Groups**.

- **eDiscovery Manager:** Appropriate for scoped access. Members can create and manage their own cases and access cases where they are explicitly added.
- **eDiscovery Administrator:** Appropriate for tenant-wide eDiscovery administration. Members can access and manage all cases across the organization.
- **Compliance Administrator or Organization Management:** May provide broader compliance administration capabilities but should be assigned only when required by the organization's access model.

Step 6: Grant Access to eDiscovery Cases

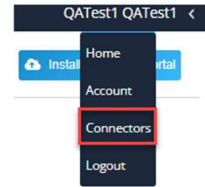
For case-scoped workflows, add the user or role group that will initiate the connector workflow to the relevant eDiscovery case. This step helps ensure the connector can access only the cases and data that the organization has approved.

1. Sign in to the [Microsoft Purview portal](#) with an account that has **Case Management** permissions (or as an **eDiscovery Administrator**).
2. In the navigation panel, go to **eDiscovery -> Cases**.
3. Select the case you want to modify.
4. Open **Case settings** tab, then select **Access and permissions**.
5. Select **Add User**.
6. Select the user(s) or role group(s) you wish to add.
7. Select **Add** to confirm. Save your changes.

Step 7: Create the Connector in CloudNine Review

Once Microsoft configuration is complete, create the Cloud Connector within CloudNine Review.

1. Sign in to CloudNine Review as a Global Administrator.
2. On the My Projects page, open the **User** menu in the top-right corner and select **Connectors**.
3. Select **Create New**.
4. Enter the following values:
 - a. **Connector Name:** Enter a unique descriptive name, such as Purview Connector.
 - b. **Connection Type:** Purview.
 - c. **Client ID:** Application (client) ID.
 - d. **Secret:** Client Secret Value
 - e. **Tenant ID:** Directory (Tenant) ID.
5. Select **Create New**.



The connector will appear in the Connectors list and will be available

Verify the Configuration: Validation Checklist

Before performing a production collection, CloudNine recommends validating the configuration.

Confirm the connector can:

- Authenticate successfully
- Connect to Microsoft Purview
- Display authorized eDiscovery cases
- Access approved mailboxes and data locations
- Complete a small test collection without errors

Security Best Practices

CloudNine recommends the following security controls:

- Follow least-privilege access principles.
- Review API permissions regularly.
- Rotate client secrets according to organizational policy.
- Limit connector administration access to authorized personnel.
- Use separate connectors when different matters, departments, or regions require distinct security boundaries.