OneDrive Integration Configuration Guide

Connecting Microsoft OneDrive to Prakalpa

1. Overview

This guide explains how to connect Microsoft OneDrive (Microsoft 365) to Prakalpa .

The connection is made through an application registration in Microsoft Entra ID (formerly Azure Active Directory). You register an application in the Entra admin center, collect three values from it — Client ID, Tenant ID and Client Secret — and enter those into the Prakalpa Connected Apps screen. Prakalpa then calls the Microsoft Graph API to reach OneDrive.

The configuration runs in three parts:

- In Prakalpa — copy the Redirect URL from the Connected Apps screen.
- In Microsoft Entra ID — register an application, paste the Redirect URL, and collect the Client ID, Tenant ID and Client Secret.
- Back in Prakalpa — enter the three values, save, and authorise the connection.

> **Before you start:** Have a password manager or secrets vault ready. The Client Secret value is displayed only once, immediately after it is created, and cannot be retrieved afterwards.

2. Step 1 — Copy the Redirect URL from Prakalpa

Begin in Prakalpa. The Redirect URL that Entra ID requires is generated by Prakalpa and shown on the Connected Apps screen.

1. Sign in to Prakalpa as an Administrator.
2. Open Settings and select Connected Apps.
3. Locate the OneDrive card and click Configure.
4. Find the Redirect URL field and click the copy icon beside it.
5. Leave this browser tab open — you will return to it in Step 8.

> **Tip:** Paste the URL into a plain-text editor first. Copying from a styled web page can carry a trailing space, and Entra ID requires an exact match.

3. Step 2 — Open App registrations in the Entra admin center

Now switch to Microsoft Entra ID to create the application registration.

1. Sign in to the Microsoft Entra admin center at entra.microsoft.com using an administrator account.
2. Confirm the correct directory is selected — the tenant name is shown on the home page under Default Directory.
3. In the left-hand navigation, expand Entra ID and select App registrations.

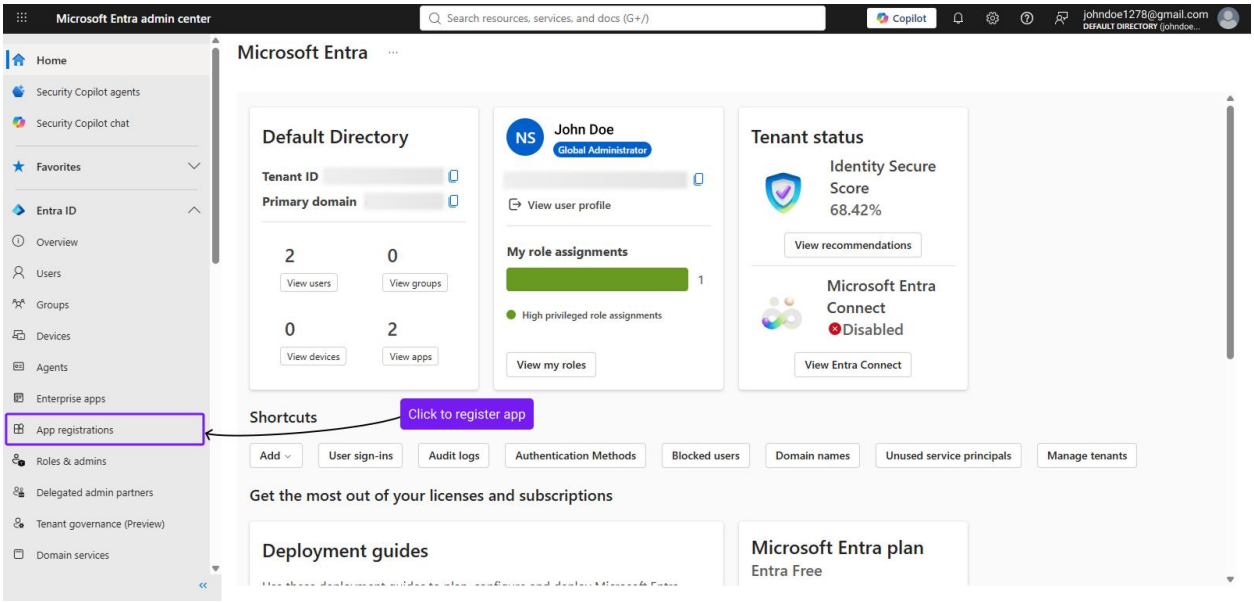


Figure 2 — The Microsoft Entra admin center home page, with App registrations in the left navigation

4. Step 3 — Register the application and enter the Redirect URL

On the App registrations page, click New registration and complete the form using the values below.

Field	Value to enter	Notes
Name	OneDrive App	The display name shown to users on the consent screen. Add an environment suffix, such as 'OneDrive App (Staging)', if you configure more than one instance.
Supported account types	Single tenant only — Default Directory	Restricts the application to your own organisation. Choose a multi-tenant option only if Prakalpa must reach OneDrive accounts in other tenants.
Redirect URI — platform	Web	Select Web from the platform dropdown before pasting the URL.
Redirect URI — value	The Redirect URL copied in Step 1	Must match exactly, including the protocol and any trailing path. This is the most

Field	Value to enter	Notes
		common source of configuration errors.

Click Register to create the application.

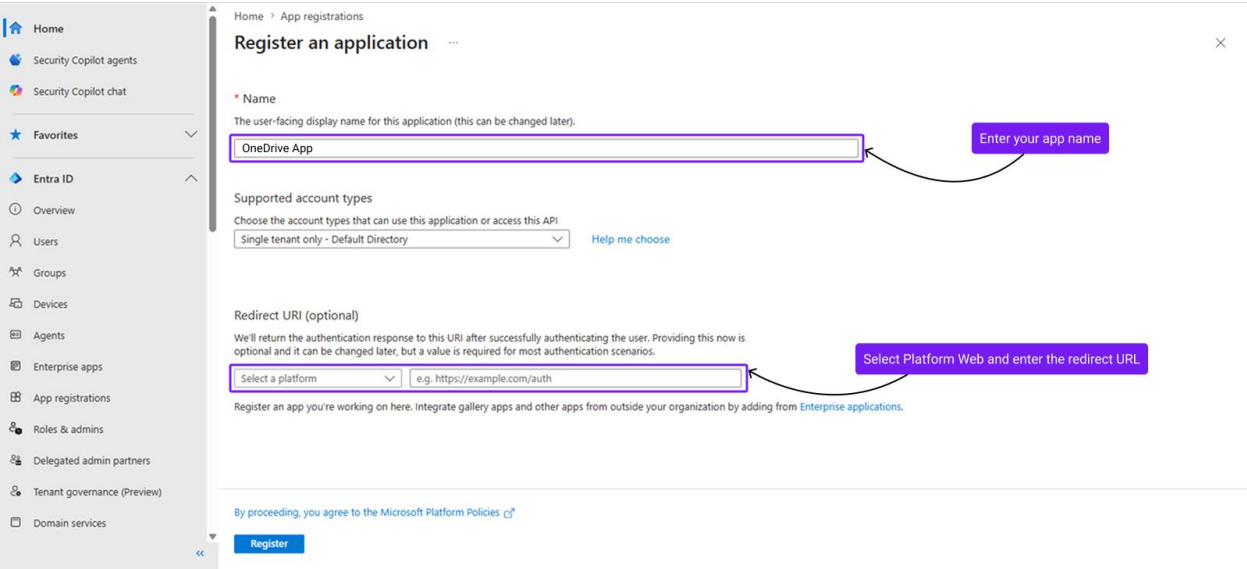


Figure 3 — The Register an application form, showing the app name and the Web platform Redirect URI

> **Redirect URL:** This is where the Redirect URL from the Prakalpa Connected Apps screen is used. If you need to change it later, open the application and go to Manage > Authentication, where web redirect URIs can be added or edited.

5. Step 4 — Copy the Client ID and Tenant ID

Entra ID opens the application's Overview page immediately after registration. Two of the three values Prakalpa needs are collected here.

1. On the Overview page, locate Application (client) ID under Essentials. Click its copy icon and save the value as the Client ID.
2. Locate Directory (tenant) ID directly below it. Click its copy icon and save the value as the Tenant ID.
3. Neither value is secret, and both can be retrieved from this page at any time.

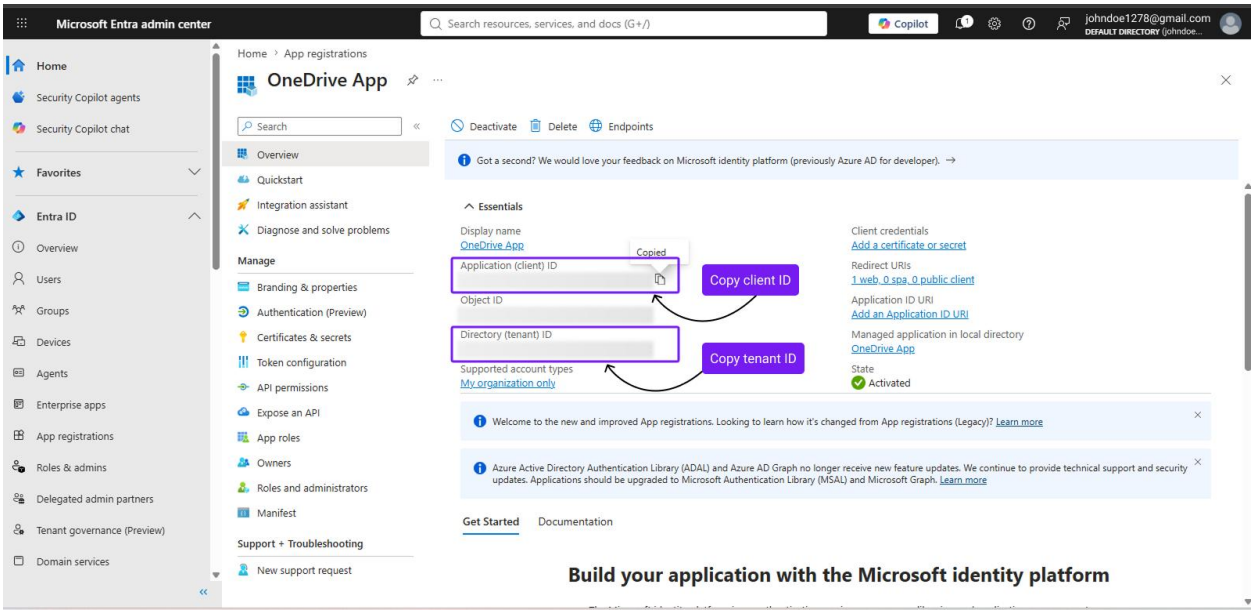


Figure 4 — The application Overview page, with Application (client) ID and Directory (tenant) ID highlighted

> **Do not confuse the identifiers:** Object ID sits between the two values you need and is not used by this integration. Copy Application (client) ID and Directory (tenant) ID only.

6. Step 5 — Open Certificates & secrets

The third value, the Client Secret, is created in a separate blade.

1. With the application still open, look at the Manage section of the left-hand menu.
2. Select Certificates & secrets.

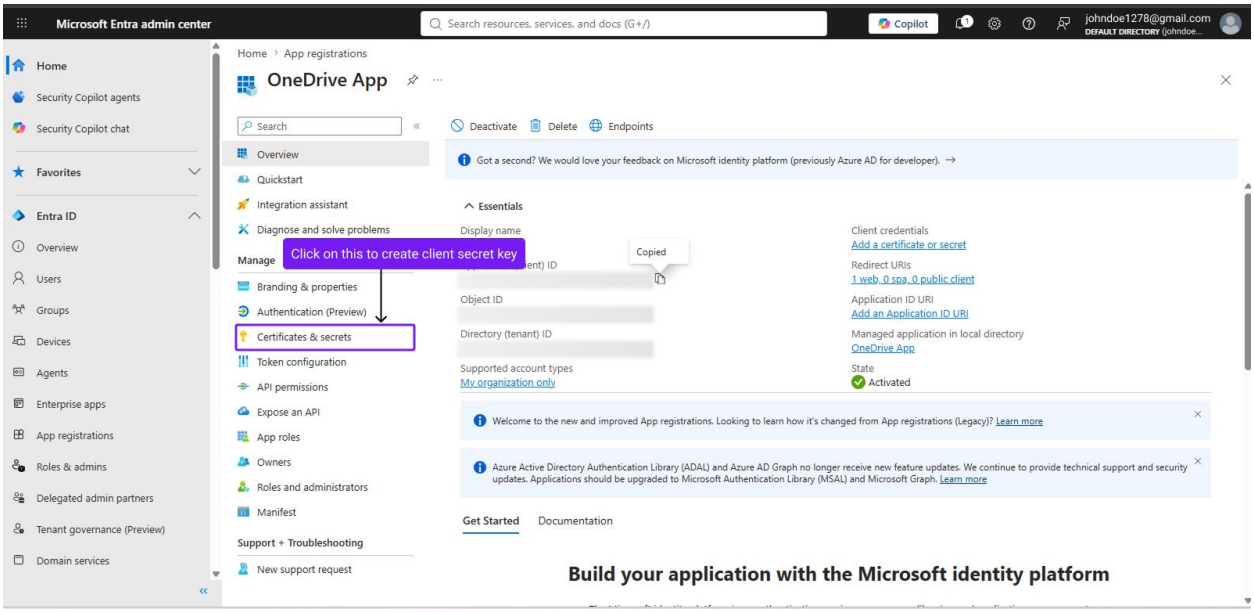


Figure 5 — The application Overview page, with Certificates & secrets selected in the Manage menu

7. Step 6 — Create a new client secret

On the Certificates & secrets page, open the Client secrets tab and create the secret.

1. Select the Client secrets tab, then click New client secret.
2. In the Add a client secret panel, enter a Description that identifies the integration — for example, OneDriveApp.
3. Choose an expiry period from the Expires dropdown. Record the expiry date in your calendar so the secret can be rotated before it lapses.
4. Click Add.

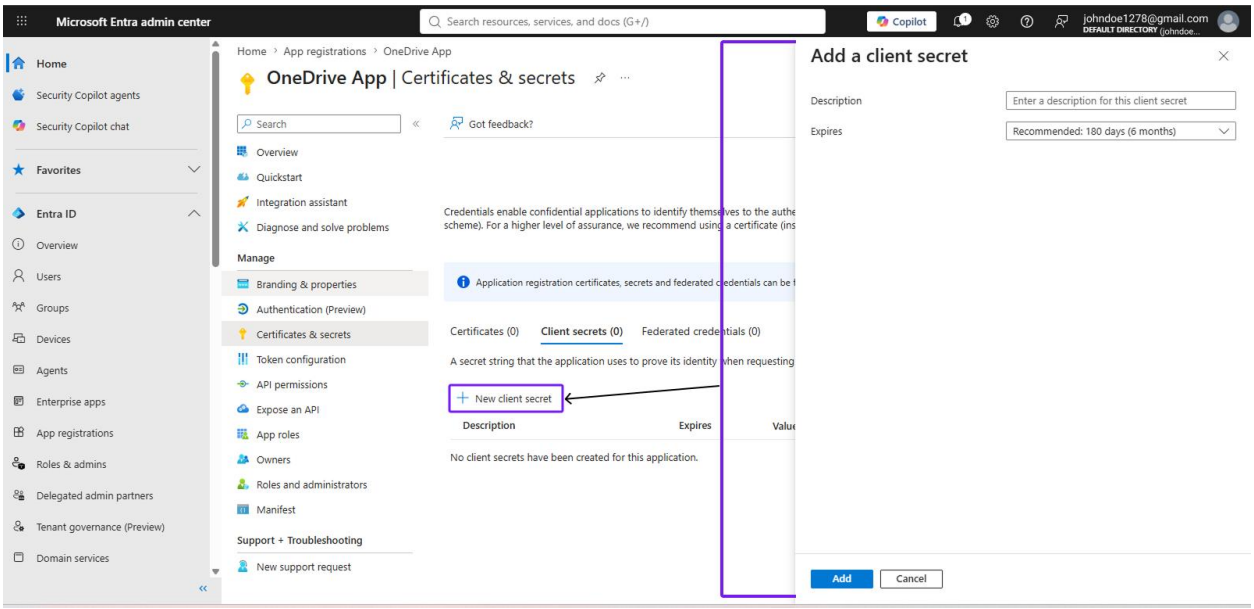


Figure 6 — The Add a client secret panel, opened from New client secret on the Client secrets tab

> **Plan for expiry:** When the secret expires the integration stops working, and the failure looks like an authentication error rather than an expiry notice. A shorter period is more secure; a longer period means fewer interruptions. Whichever you choose, diarise the renewal date.

8. Step 7 — Copy the client secret value

The new secret now appears in the list, and its value is visible for this one page view only.

1. Find the new row in the Client secrets table.
2. Click the copy icon in the Value column to copy the secret.
3. Paste it straight into your password manager or secrets vault before you navigate away or refresh the page.

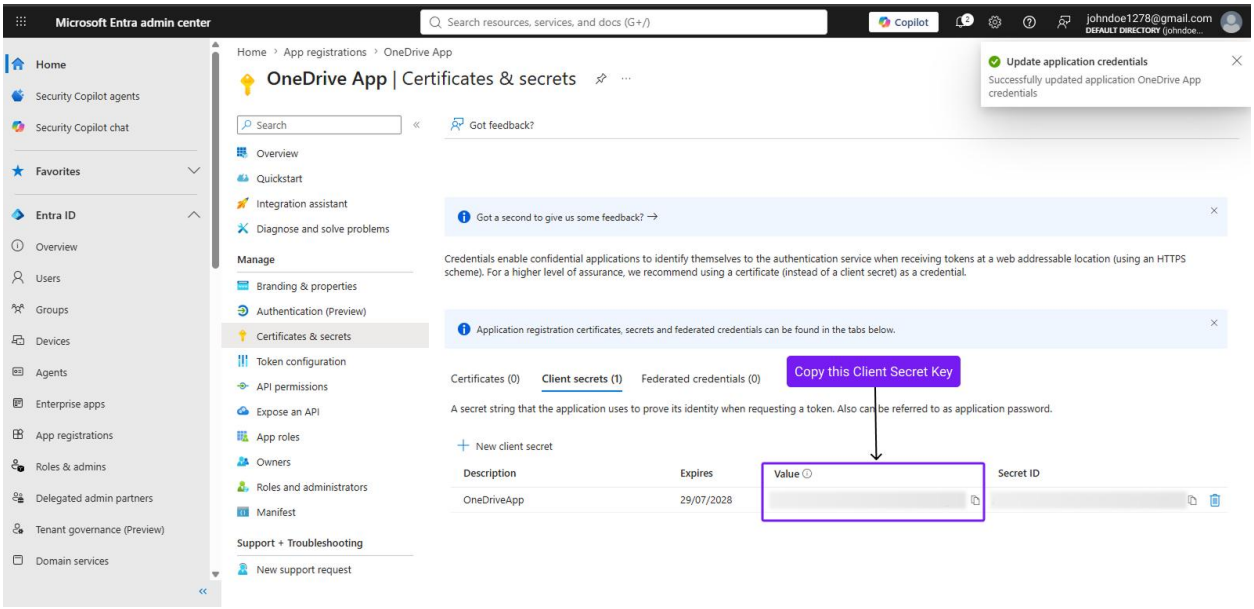


Figure 7 — The Client secrets tab after creation, with the secret Value ready to copy

> **Warning:** Copy the Value column, not the Secret ID column — the Secret ID is only an internal reference and cannot be used to authenticate. Once you leave this page the full value is masked permanently; if it is lost, delete the secret and create a replacement.

9. Step 8 — Add API permissions and grant admin consent

The application also needs permission to reach OneDrive through Microsoft Graph.

1. In the application's left-hand menu, select API permissions.
2. Click Add a permission, then choose Microsoft Graph.
3. Select the permission type — Delegated permissions if Prakalpa acts as the signed-in user, or Application permissions for unattended, tenant-wide access.
4. Add the permissions listed below, then click Add permissions.
5. Click Grant admin consent for [your directory] and confirm. The Status column should then show a green tick for every permission.

Permission	Type	Purpose
Files.ReadWrite.All	Delegated or Application	Read and write files in OneDrive — the core permission for the integration.
Files.Read.All	Delegated or Application	A narrower alternative if Prakalpa only needs to read files, never write them.
User.Read	Delegated	Sign in and read the connected user's basic

Permission	Type	Purpose
		profile.
offline_access	Delegated	Issue a refresh token so the connection survives without repeated sign-ins.
Sites.ReadWrite.All	Delegated or Application	Only required if SharePoint document libraries are in scope as well as OneDrive.

> **Confirm the exact scopes:** Prakalpa may request a specific set of Graph scopes. Check the requirement shown on the OneDrive card in Connected Apps and grant exactly that set — granting more than necessary widens your exposure, and granting less causes the connection to fail with a consent error.

10. Step 9 — Enter the credentials in Prakalpa and connect

Return to the Prakalpa browser tab you left open in Step 1.

1. On the OneDrive configuration panel under Connected Apps, paste the Application (client) ID into the Client ID field.
2. Paste the Directory (tenant) ID into the Tenant ID field.
3. Paste the secret you copied in Step 7 into the Client Secret field.
4. Click Save, then click Connect to begin the authorisation.
5. Sign in with the Microsoft account whose OneDrive should be connected, and accept the consent prompt.
6. You are returned to Prakalpa, and the OneDrive card status changes to Connected.

11. Configuration field reference

Use this table when repeating the configuration or handing it to another administrator.

Field	Description	Where to find it
Redirect URL	The address Entra ID returns the user to after authorisation.	Prakalpa > Settings > Connected Apps > OneDrive
Client ID	Application (client) ID — the public identifier of the app registration.	Entra admin center > App registrations > your app > Overview
Tenant ID	Directory (tenant) ID — the identifier	Entra admin center > App registrations >

Field	Description	Where to find it
	of your Microsoft 365 directory.	your app > Overview
Client Secret	The secret value proving the application's identity.	Your app > Certificates & secrets > Client secrets > Value
API permissions	The Microsoft Graph scopes granted to the application.	Your app > API permissions

12. Security best practices

- Store the Client Secret in a secrets vault — never in email, chat, or a shared document.
- Rotate the Client Secret on a schedule, and immediately when anyone with access to it leaves the team.
- Record the secret's expiry date in a shared calendar so renewal happens before an outage.
- Grant the narrowest Graph permissions that support your workflow — prefer Files.Read.All over Files.ReadWrite.All where read access is enough.
- Prefer single-tenant registration unless cross-tenant access is genuinely required.
- Authorise using a dedicated service account rather than an individual's personal account.
- Keep one app registration per environment, so revoking staging access never affects production.
- Review the app's sign-in logs in Entra ID periodically for unexpected activity.