Microsoft OneDrive API Provider Setup

Last Modified on 12/30/2019 8:50 pm EST

To authenticate a OneDrive connector instance you must register an app with Microsoft. Then when you authenticate, use the **Application Id**, **Password/PublicKey**, and **Redirect URL** from your registered app as the **API Key**, **API Secret**, and **Callback URL**. If you plan to monitor events, also configure the **Webhook URL**.

> **Note:** Microsoft now uses the v2.0 endpoint when you register an app at the app registration portal. Apps created through this process are considered **converged apps**. With converged apps you can accept sign-ins form Microsoft Accounts and Azure AD accounts. Any app that you create at the app registration portal is a converged app by default.

If you've already set up an app and just need to know how to find your **Application Id** and **Password/PublicKey**, see Locate Credentials for Authentication. If you need to register an app, see Create an Application.

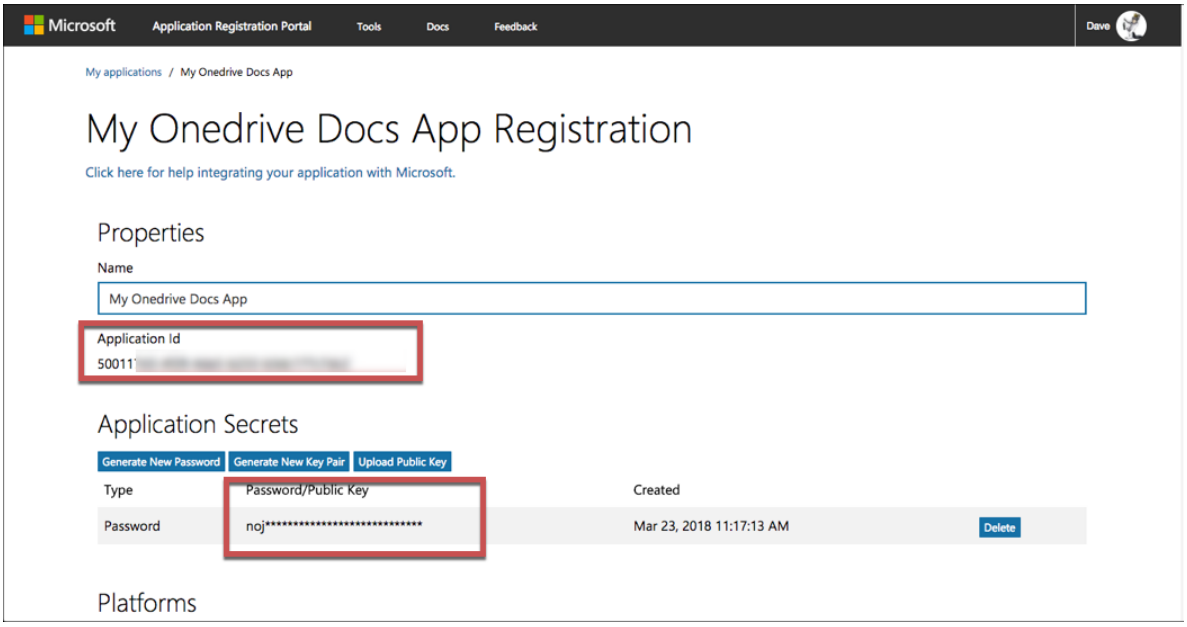
See the latest setup instructions in the Microsoft documentation.

Locate Credentials for Authentication

If you already created an application, follow the steps below to locate the **Application Id**, **Password/PublicKey**, and **Redirect URL**. If you have not created an app, see Create an Application.

To find your OAuth 2.0 credentials:

1. Log in to your account at Microsoft.
2. Click the application that you want to connect.
3. Record the **Application Id**.
4. If you don't know the **Password/PublicKey**, click **Generate New Password** to get a new one and record it.
5. Record the **Redirect URL** for your app.



Create an Application

If you have not created an application, you need one to authenticate with Microsoft.

To create an application:

1. Log in to your account at Microsoft.
2. Click **Add an App**.
3. Enter a name, and then click **Create**
4. Record the **Application Id**.

5. Under **Application Secrets**, click **Generate New Password**, record the **Password/PublicKey**, and then click **OK**.

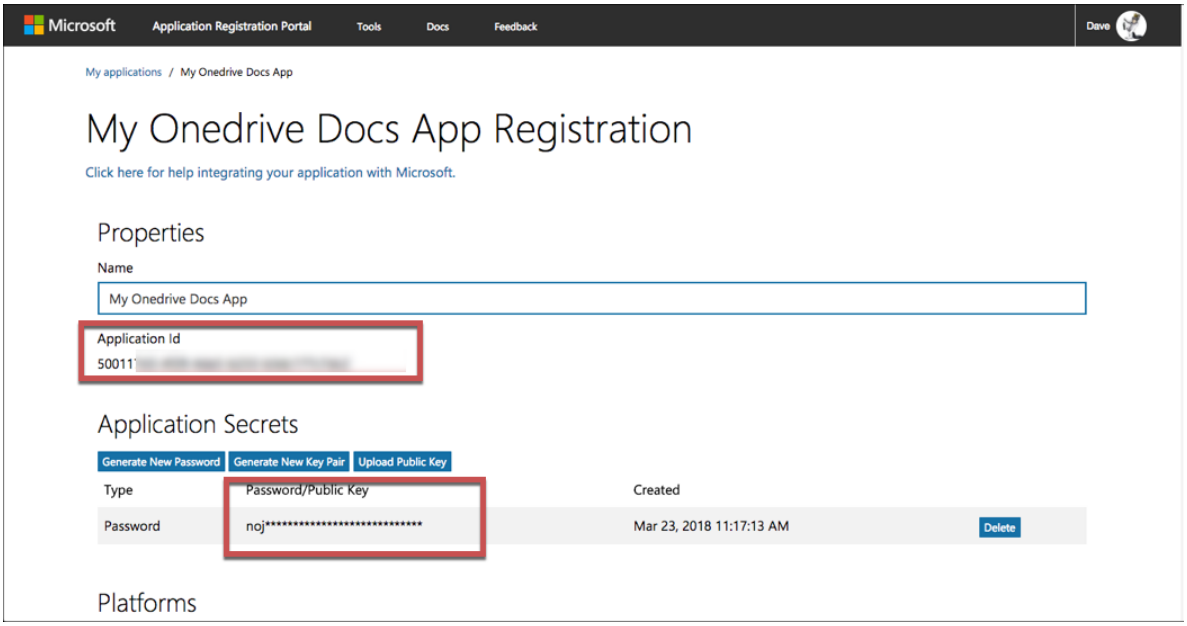
   > ⚠ **Important:** You cannot show the Password/Public Key again, so you will need to generate a new one if it's lost.

6. Under **Platforms**, click **Add Platform**, and then select **Web**.

7. In **Redirect URLs** enter the URL to redirect the user to at the end of the OAuth 2.0 authentication process. For example, the SAP Cloud Platform Open Connectors 2.0 callback URL is `https://auth.cloudelements.io/oauth`.

8. Under **Microsoft Graph Permissions** add the permissions needed to use your app. See Permissions for details.

9. Save your app.



Permissions

When creating your app be aware of the permissions that you set. You will pass the scopes that you select when you request an OAuth 2.0 URL from during the authentication process. See Authorization and sign-in for OneDrive in Microsoft Graph for more information.

Each OneDrive resource requires specific permissions. Review the OneDrive Permissions docs for the permissions to set for your app. Recommended permissions include:

Permission Type	Permissions
Delegated (work or school account)	Files.ReadWrite, Files.ReadWrite.All, Sites.ReadWrite.All offline_access
Delegated (personal Microsoft account)	Files.ReadWrite, Files.ReadWrite.All offline_access
Application	Files.ReadWrite.All, Sites.ReadWrite.All offline_access