Registering an application with Azure Active Directory

Before you can connect your Azure Key Vault to Workato, you must register an application with Azure Active Directory (AD).

Registering this application and giving it the appropriate permissions enables Workato to retrieve secrets from your key vault on your behalf.

To register the application, complete the following steps:

- Step 1: Create the app registration
- Step 2: Create the client secret
- Step 3: Grant permissions to the app

HAVE AN EXISTING SAML-BASED APPLICATION?

If you have already registered a SAML-based application that lets your users log into Workato with SAML SSO, you can use it to set up Workato's Azure Key Vault connection. When you configure the connector, simply enter your existing app's client ID and generate a new secret. Make sure the application also has the required permissions.

Step 1: Create the app registration

1. Log in to the Azure portal and navigate to **Azure Active Directory > App registrations**.
2. Select **+ New registration**.
3. Name your application. This is the user-facing display name for this application, such as `workato-akv`. Microsoft allows you to change this name later.
4. In **Supported account types**, select **Accounts in this organizational directory only (Default Directory only - Single tenant)**.
5. Leave the **Redirect URI** field blank and select the **Register** button.
6. The next page displays an overview of the newly-created application. Pay attention to the **Application (client) ID** and the **Directory (tenant) ID**. You will need these values later to authenticate in Workato.

App registration overview

Step 2: Create the client secret

1. From the overview of your app registration, select **Certificates & secrets** in the left navigation sidebar.
2. On the **Client secrets** tab, select **+ New client secret**.
3. In the **Description** field, enter a description for the client secret, such as `workatoAzureKeyVault`.
4. In the **Expires** field, select when the secret should expire. The default is after 180 days.
5. Select **Add**.
6. The Azure portal displays the new secret value and ID. Copy the **Value**.

WARNING

The secret value is only shown once. Make sure you copy it before leaving the page.

Copy the secret value

Step 3: Grant permissions to the app

Next, you must give the registered app permission to retrieve secrets from your key vault on Workato's behalf.

Azure offers two ways to grant permission to access key vaults:

- Role-based access control (RBAC)
- Access policies

To see which model your key vault uses, navigate to **Key vaults > {key vault name} > Access configuration**.

Step 3a: RBAC

If your key vault uses the RBAC permission model, you must assign the **Key Vault Secrets User** role to the registered application.

1. Navigate to **Key vaults > {key vault name} > Access control (IAM)**.
2. Select **Add > Add role assignment**.
3. Select the **Key Vault Secrets User** role and select **Next**.
4. In the **Assign access to** field, select **User, group, or service principal**.
5. In the **Members** field, choose **Select members** and search for the name of your registered application. When the application appears in the list, click the application name and choose **Select**.
6. Select **Next**.
7. In the **Review + assign** tab, select **Review and assign**.

Step 3b: Access policy

If your key vault uses the access policy permission model, you must assign the **Get** secret permission to the registered application.

1. Navigate to **Key vaults > {key vault name} > Access policies**.
2. Select **Create**.
3. In the **Permissions** tab, select **Get** in the **Secret permissions** column, then select **Next**.
4. In the **Principal** tab, search for the name of the registered app. When the application appears in the list, select the application name and then select **Next**.
5. In the **Application (optional)** tab, select **Next**.
6. In the **Review + create** tab, select **Create**.

FURTHER READING

- Set up Azure Key Vault for workspaces
- Set up Azure Key Vault for projects

← Using Azure Key Vault
IP Allowlists →

Last updated: 7/19/2023, 3:39:09 PM