Connection Credentials

Overview

AWS Secrets Manager

HashiCorp Vault

Azure Key Vault

projects

Set up Azure Key Vault for workspaces Set up Azure Key Vault for

Using Azure Key Vault

Azure Key Vault app registration

IP Allowlists

IP Allowlists FAQs

Supported cloud regions

Security FAQs

Data Retention

Lifecycle & operations

Connector SDK

Developer API

DATA & SECURITY > CONNECTION CREDENTIALS > AZURE KEY VAULT

Registering an application with Azure Active **Directory**

Before you can connect your <u>Azure Key Vault</u> do Workato, you must <u>register an</u> <u>application</u> ☐ with Azure Active Directory (AD).

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

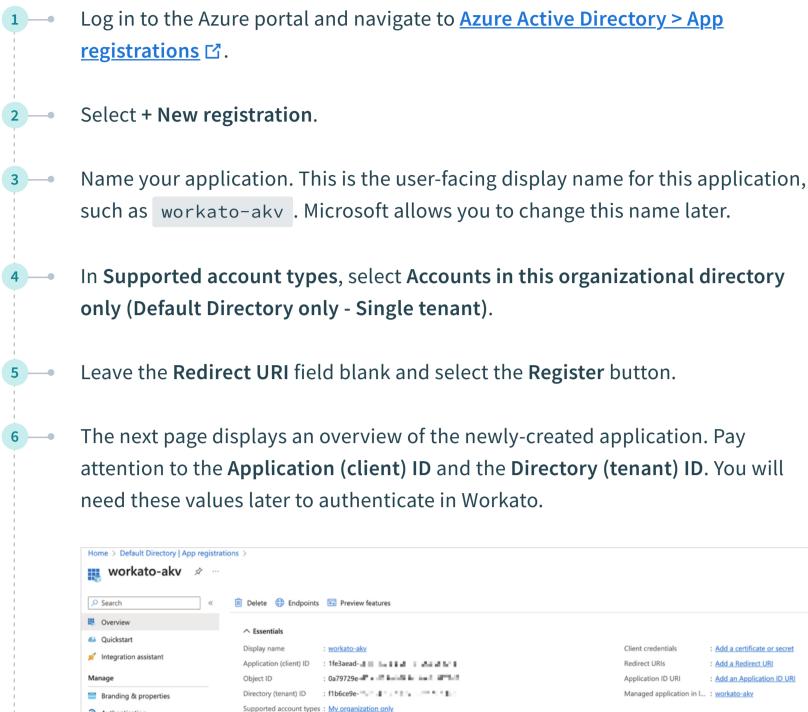
To register the application, complete the following steps:

- 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?

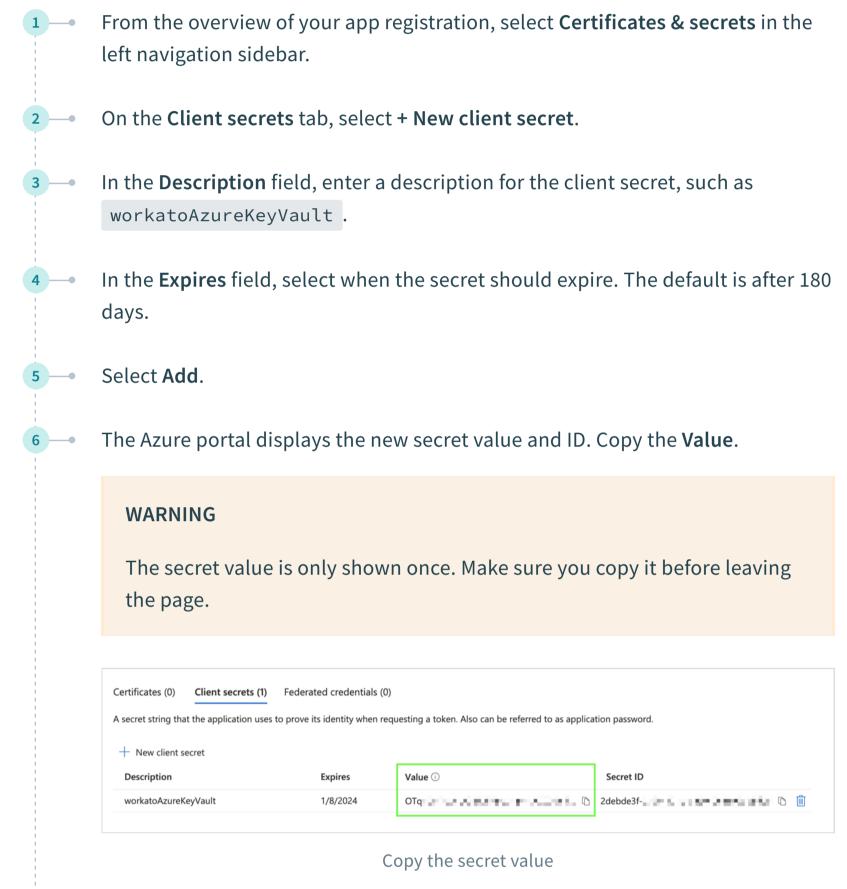
If you have already registered a <u>SAML-based application</u> I that lets your users log into Workato with SAML SSO, you can use it to set up Workato's Azure Key Vault <u>connection</u>. When you configure the connector, simply enter your existing app's client ID and generate a new secret. Make sure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

Step 1: Create the app registration



App registration overview

Step 2: Create the client secret



Next, you must give the registered app permission to retrieve secrets from your key vault

Step 3: Grant permissions to the app

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.

If your key vault uses the <u>RBAC permission model</u> ☑, you must assign the **Key Vault**

Step 3a: RBAC

Secrets User role to the registered application. Navigate to Key vaults > {key vault name} > Access control (IAM).

2 Select Add > Add role assignment. Select the **Key Vault Secrets User** role and select **Next**. In the Assign access to field, select User, group, or service principal.

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**. Select Next.

Step 3b: Access policy

In the **Review + assign** tab, select **Review and assign**.

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

Select Create.

Navigate to **Key vaults > {key vault name} > Access policies**.

In the **Permissions** tab, select **Get** in the **Secret permissions** column, then select Next. 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**. In the **Application (optional)** tab, select **Next**. In the **Review + create** tab, select **Create**.

FURTHER READING

← Using Azure Key Vault

- <u>Set up Azure Key Vault for workspaces</u>
- Set up Azure Key Vault for projects

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

IP Allowlists \rightarrow

Product Solutions **Applications** Resources Company Use cases How it works HR Product Led Sales Salesforce Docs About us Pricing Slack **Customer Success** Order to Cash Customers Sales **Content Library Employee Onboarding** What's New Marketing Marketo Blog **Systematic Community Embedded Integrations** NetSuite Recipes Finance Press Security Workato for Slack Enterprise iPaaS Support ServiceNow Careers Workday Documentation ΙT Workato for Microsoft Teams IT Help Desk **Partners** Product blog Product (Embed) All Apps > All use cases > **Events** Higher Ed **Revenue Operations**

ON THIS PAGE -

⊕ English
∨

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