

[Azure](#) / [Active Directory](#) / [Application management](#) /

Quickstart: Add an enterprise application

Article • 03/25/2022 • 2 minutes to read • [16 contributors](#)

In this article

[Prerequisites](#)[Add an enterprise application](#)[Clean up resources](#)[Next steps](#)

In this quickstart, you use the Azure Active Directory Admin Center to add an enterprise application to your Azure Active Directory (Azure AD) tenant. Azure AD has a gallery that contains thousands of enterprise applications that have been pre-integrated. Many of the applications your organization uses are probably already in the gallery. This quickstart uses the application named **Azure AD SAML Toolkit** as an example, but the concepts apply for most [enterprise applications in the gallery](#).

It is recommended that you use a non-production environment to test the steps in this quickstart.

Prerequisites

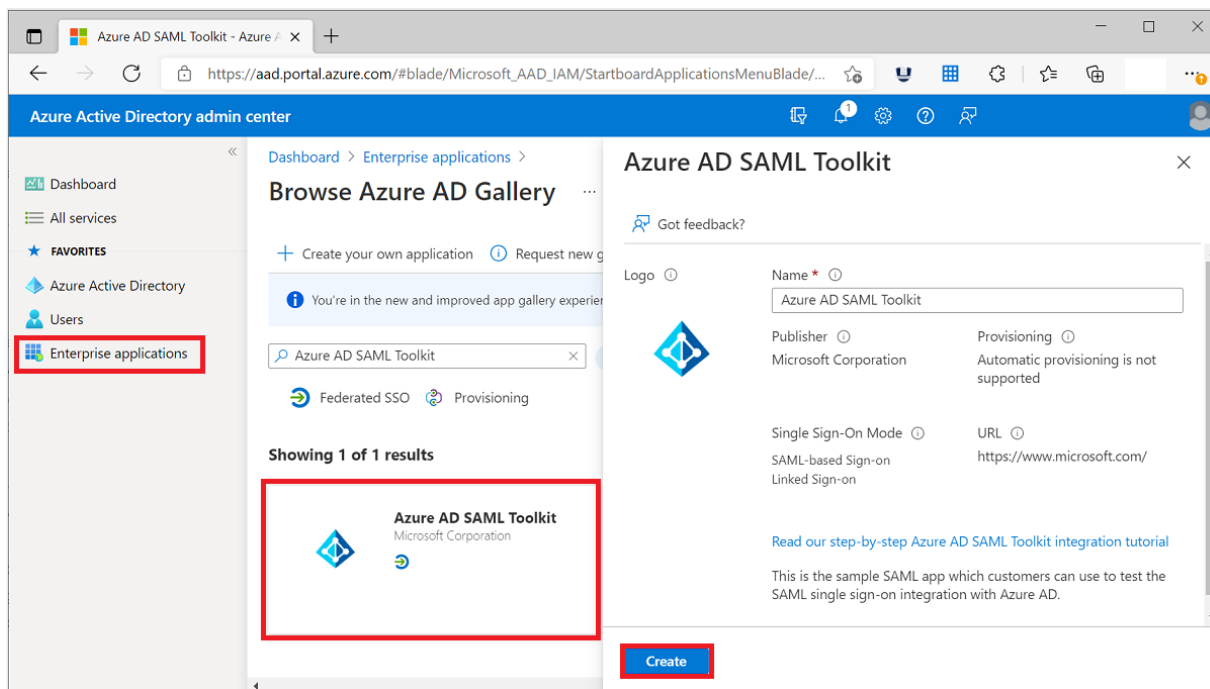
To add an enterprise application to your Azure AD tenant, you need:

- An Azure AD user account. If you don't already have one, you can [Create an account for free](#).
- One of the following roles: Global Administrator, Cloud Application Administrator, or Application Administrator.

Add an enterprise application

To add an enterprise application to your tenant:

1. Go to the [Azure Active Directory Admin Center](#) and sign in using one of the roles listed in the prerequisites.
2. In the left menu, select **Enterprise applications**. The **All applications** pane opens and displays a list of the applications in your Azure AD tenant.
3. In the **Enterprise applications** pane, select **New application**.
4. The **Browse Azure AD Gallery** pane opens and displays tiles for cloud platforms, on-premises applications, and featured applications. Applications listed in the **Featured applications** section have icons indicating whether they support federated single sign-on (SSO) and provisioning. Search for and select the application. In this quickstart, **Azure AD SAML Toolkit** is being used.



5. Enter a name that you want to use to recognize the instance of the application. For example, Azure AD SAML Toolkit 1.
6. Select **Create**.

If you choose to install an application that uses OpenID Connect based SSO, instead of seeing a **Create** button, you see a button that redirects you to the application sign-in or sign-up page depending on whether you already have an account there. For more information, see [Add an OpenID Connect based single sign-on application](#). After sign-in, the application is added to your tenant.

Clean up resources

If you are planning to complete the next quickstart, keep the enterprise application that you created. Otherwise, you can consider deleting it to clean up your tenant. For more information, see [Delete an application](#).

Next steps

Learn how to create a user account and assign it to the enterprise application that you added.

Create and assign a user account

Recommended content

[Configure enterprise application properties - Azure AD](#)

Configure the properties of an enterprise application in Azure Active Directory.

[Quickstart: View enterprise applications - Azure AD](#)

View the enterprise applications that are registered to use your Azure Active Directory tenant.

[Quickstart: Enable single sign-on for an enterprise application - Azure AD](#)

Enable single sign-on for an enterprise application in Azure Active Directory.

[Quickstart: Create and assign a user account - Azure AD](#)

Create a user account in your Azure Active Directory tenant and assign it to an application.

[Tutorial: Azure AD SSO integration with Azure AD SAML Toolkit](#)

Learn how to configure single sign-on between Azure Active Directory and Azure AD SAML Toolkit.

Azure Single Sign On SAML Protocol - Microsoft identity platform

This article describes the Single Sign-On (SSO) SAML protocol in Azure Active Directory

Properties of an enterprise application - Azure AD

Learn about the properties of an enterprise application in Azure Active Directory.

Customize app SAML token claims - Microsoft identity platform

Learn how to customize the claims issued by Microsoft identity platform in the SAML token for enterprise applications.

Show more ▼