What is application management in Azure Active Directory?

Article • 02/24/2022 • 8 minutes to read • 13 contributors

In this article

Application management in Azure Active Directory (Azure AD) is the process of creating, configuring, managing, and monitoring applications in the cloud. When an application is registered in an Azure AD tenant, users who have been assigned to it can securely access it. Many types of applications can be registered in Azure AD. For more information, see Application types for the Microsoft Identity Platform.

In this article, you learn these important aspects of managing the lifecycle of an application:

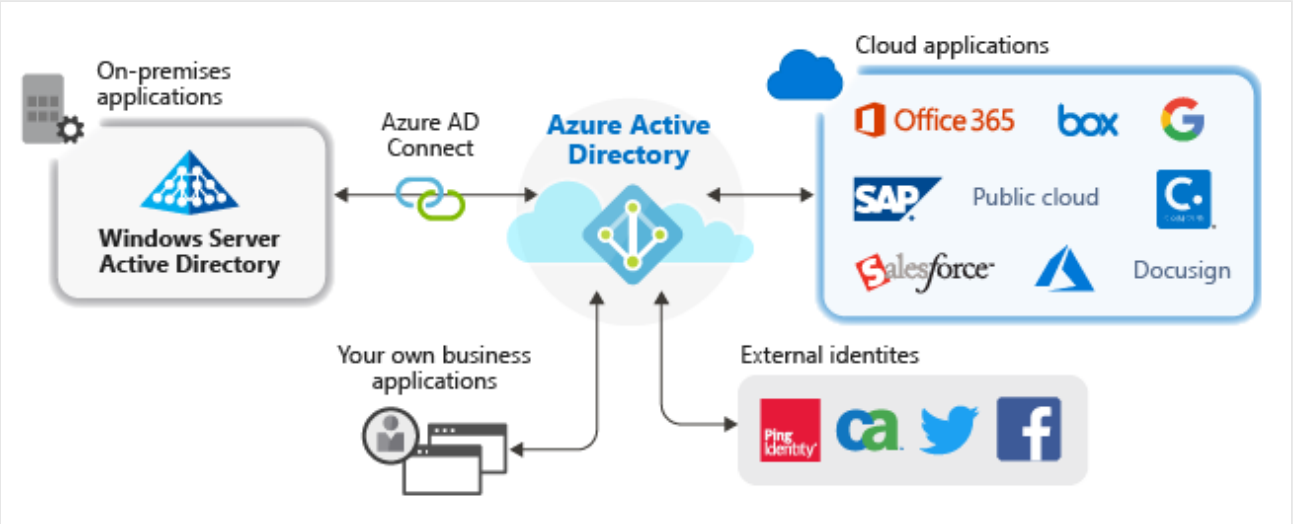
- **Develop, add, or connect** – You take different paths depending on whether you're developing your own application, using a pre-integrated application, or connecting to an on-premises application.
- **Manage access** – Access can be managed by using single sign-on (SSO), assigning resources, defining the way access is granted and consented to, and using automated provisioning.
- **Configure properties** – Configure the requirements for signing into the application and how the application is represented in user portals.
- **Secure the application** – Manage configuration of permissions, multifactor authentication (MFA), conditional access, tokens, and certificates.
- **Govern and monitor** – Manage interaction and review activity using entitlement management and reporting and monitoring resources.

- **Clean up** – When your application is no longer needed, clean up your tenant by removing access to it and deleting it.

Develop, add, or connect

There are several ways that you might manage applications in Azure AD. The easiest way to start managing an application is to use a pre-integrated application from the Azure AD gallery. Developing your own application and registering it Azure AD is an option, or you can continue to use an on-premises application.

The following image shows how these applications interact with Azure AD.



Pre-integrated applications

Many applications are already pre-integrated (shown as “Cloud applications” in the image above) and can be set up with minimal effort. Each application in the Azure AD gallery has an article available that shows you the steps required to configure the application. For a simple example of how an application can be added to your Azure AD tenant from the gallery, see Quickstart: Add an enterprise application.

Your own applications

If you develop your own business application, you can register it with Azure AD to take advantage of the security features that the tenant provides. You can register your application in **App Registrations**, or you can register it using the **Create your own**

application link when adding a new application in **Enterprise applications**. Consider how authentication is implemented in your application for integration with Azure AD.

If you want to make your application available through the gallery, you can submit a request to have it added.

On-premises applications

If you want to continue using an on-premises application, but take advantage of what Azure AD offers, connect it with Azure AD using Azure AD Application Proxy. Application Proxy can be implemented when you want to publish on-premises applications externally. Remote users who need access to internal applications can then access them in a secure manner.

Manage access

To manage access for an application, you want to answer the following questions:

- How is access granted and consented for the application?
- Does the application support SSO?
- Which users, groups, and owners should be assigned to the application?
- Are there other identity providers that support the application?
- Will it be helpful to automate the provisioning of user identities and roles?

Access and consent

You can manage user consent settings to choose whether users can allow an application or service to access user profiles and organizational data. When applications are granted access, users can sign in to applications integrated with Azure AD, and the application can access your organization's data to deliver rich data-driven experiences.

Users often are unable to consent to the permissions an application is requesting. Configure the admin consent workflow to allow users to provide a justification and request an administrator's review and approval of an application.

As an administrator, you can grant tenant-wide admin consent to an application. Tenant-wide admin consent is necessary when an application requires permissions that regular users aren't allowed to grant, and allows organizations to implement their own review processes. Always carefully review the permissions the application is requesting before

granting consent. When an application has been granted tenant-wide admin consent, all users are able to sign into the application unless it has been configured to require user assignment.

Single sign-on

Consider implementing SSO in your application. You can manually configure most applications for SSO. The most popular options in Azure AD are SAML-based SSO and OpenID Connect-based SSO. Before you start, make sure that you understand the requirements for SSO and how to plan for deployment. For a simple example of how to configure SAML-based SSO for an enterprise application in your Azure AD tenant, see Quickstart: Enable single sign-on for an enterprise application.

User, group, and owner assignment

By default, all users can access your enterprise applications without being assigned to them. However, if you want to assign the application to a set of users, your application requires user assignment. For a simple example of how to create and assign a user account to an application, see Quickstart: Create and assign a user account.

If included in your subscription, assign groups to an application so that you can delegate ongoing access management to the group owner.

Assigning owners is a simple way to grant the ability to manage all aspects of Azure AD configuration for an application. As an owner, a user can manage the organization-specific configuration of the application.

Automate provisioning

Application provisioning refers to automatically creating user identities and roles in the applications that users need to access. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change.

Identity providers

Do you have an identity provider that you want Azure AD to interact with? Home Realm Discovery provides a configuration that allows Azure AD to determine which identity

provider a user needs to authenticate with when they sign in.

User portals

Azure AD provides customizable ways to deploy applications to users in your organization. For example, the My Apps portal or the Microsoft 365 application launcher. My Apps gives users a single place to start their work and find all the applications to which they have access. As an administrator of an application, you should plan how the users in your organization will use My Apps.

Configure properties

When you add an application to your Azure AD tenant, you have the opportunity to configure properties that affect the way users can interact with the application. You can enable or disable the ability to sign in and user assignment can be required. You can also determine the visibility of the application, what logo represents the application, and any notes about the application. For more information about the properties that can be configured, see Properties of an enterprise application.

Secure the application

There are several methods available to help you keep your enterprise applications secure. For example, you can restrict tenant access, manage visibility, data, and analytics, and possibly provide hybrid access. Keeping your enterprise applications secure also involves managing configuration of permissions, MFA, conditional access, tokens, and certificates.

Permissions

It's important to periodically review and, if necessary, manage the permissions granted to an application or service. Make sure that you only allow the appropriate access to your applications by regularly evaluating whether suspicious activity exists.

Permission classifications allow you to identify the effect of different permissions according to your organization's policies and risk evaluations. For example, you can use permission classifications in consent policies to identify the set of permissions that users are allowed to consent to.

Multifactor authentication and conditional access

Azure AD MFA helps safeguard access to data and applications, providing another layer of security by using a second form of authentication. There are many methods that can be used for a second-factor authentication. Before you start, plan the deployment of MFA for your application in your organization.

Organizations can enable MFA with conditional access to make the solution fit their specific needs. Conditional access policies allow administrators to assign controls to specific applications, actions, or authentication context.

Tokens and certificates

Different types of security tokens are used in an authentication flow in Azure AD depending on the protocol used. For example, SAML tokens are used for the SAML protocol, and ID tokens and access tokens are used for the OpenID Connect protocol. Tokens are signed with the unique certificate that's generated in Azure AD and by specific standard algorithms.

You can provide more security by encrypting the token. You can also manage the information in a token including the roles that are allowed for the application.

Azure AD uses the SHA-256 algorithm by default to sign the SAML response. Use SHA-256 unless the application requires SHA-1. Establish a process for managing the lifetime of the certificate. The maximum lifetime of a signing certificate is three years. To prevent or minimize outage due to a certificate expiring, use roles and email distribution lists to ensure that certificate-related change notifications are closely monitored.

Govern and monitor

Entitlement management in Azure AD enables you to manage interaction between applications and administrators, catalog owners, access package managers, approvers, and requestors.

Your Azure AD reporting and monitoring solution depends on your legal, security, and operational requirements and your existing environment and processes. There are several logs that are maintained in Azure AD and you should plan for reporting and monitoring deployment to maintain the best experience as possible for your application.

Clean up

You can clean up access to applications. For example, removing a user's access. You can also disable how a user signs in. And finally, you can delete the application if it's no longer needed for the organization. For a simple example of how to delete an enterprise application from your Azure AD tenant, see Quickstart: Delete an enterprise application.

Next steps

- Get started by adding your first enterprise application with the Quickstart: Add an enterprise application.

Recommended content

Configure enterprise application properties - Azure AD

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

Quickstart: Add an enterprise application - Azure AD

Add an enterprise application in Azure Active Directory.

Properties of an enterprise application - Azure AD

Learn about 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.

Get started integrating Azure Active Directory with apps - Azure AD

This article is a getting started guide for integrating Azure Active Directory (AD) with on-premises applications, and cloud applications.

Overview of the Azure Active Directory application gallery - Azure AD

An overview of using the Azure Active Directory application gallery.

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.

Show more