* 5 minutes

In this part, you learn how Azure Active Directory (Azure AD) provides identity services that enable your users to sign in and access both Microsoft cloud applications and cloud applications that you develop. You also learn how Azure AD supports single sign-on (SSO).

Tailwind Traders already uses Active Directory to secure its on-premises environments. The company doesn’t want its users to have a different username and password to remember for accessing applications and data in the cloud. Can the company integrate its existing Active Directory instance with cloud identity services to create a seamless experience for its users?

Let’s start with how Azure AD compares to Active Directory.

Active Directory is related to Azure AD, but they have some key differences.

Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that’s managed by your own organization. Azure AD is Microsoft’s cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you’ve worked with Active Directory, Azure AD will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn’t monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

## Who uses Azure AD?

Azure AD is for:

* **IT administrators**
* Administrators can use Azure AD to control access to applications and resources based on their business requirements.
* **App developers**
* Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user’s existing credentials.
* **Users**
* Users can manage their identities. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
* **Online service subscribers**
* Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD.
* A *tenant* is a representation of an organization. A tenant is typically separated from other tenants and has its own identity.
* Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant.

Here’s a screenshot of what an IT administrator might see in the Azure portal when working with Active Directory:

![A screenshot of the Azure portal showing Azure Active Directory. The overview tab shows basic information about the current tenant.](data:image/png;base64;base64,)

A screenshot of the Azure portal showing Azure Active Directory. The overview tab shows basic information about the current tenant.

Azure AD provides services such as:

* **Authentication**
* This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
* **Single sign-on**
* SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
* **Application management**
* You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the *access panel*), and single sign-on provide a better user experience.
* **Device management**
* Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Azure AD helps users access both external and internal resources.

External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.

Internal resources might include apps on your corporate network and intranet, along with any cloud applications developed within your organization.

## What’s single sign-on?

Single sign-on enables a user to sign in one time and use that credential to access multiple resources and applications from different providers.

More identities mean more passwords to remember and change. Password policies can vary among applications. As complexity requirements increase, it becomes increasingly difficult for users to remember them. The more passwords a user has to manage, the greater the risk of a credential-related security incident.

Consider the process of managing all those identities. Additional strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they are disabled can be challenging. If an identity is overlooked, this might allow access when it should have been eliminated.

With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that’s tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and increases your security capabilities.

You’ll find resources at the end of this module about how to enable SSO through Azure AD.

## How can I connect Active Directory with Azure AD?

Connecting Active Directory with Azure AD enables you to provide a consistent identity experience to your users.

There are a few ways to connect your existing Active Directory installation with Azure AD. Perhaps the most popular method is to use Azure AD Connect.

Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems. Self-service password reset prevents users from using known compromised passwords.

Here’s a diagram that shows how Azure AD Connect fits between on-premises Active Directory and Azure AD:

![A diagram that shows two environments: Active Directory running on-premises and Azure AD. Azure AD Connect joins the two environments.](data:image/png;base64;base64,)

A diagram that shows two environments: Active Directory running on-premises and Azure AD. Azure AD Connect joins the two environments.

As Tailwind Traders integrates its existing Active Directory instance with Azure AD, it creates a consistent access model across its organization. Doing so greatly simplifies its ability to sign in to different applications, manage changes to user identities and control, and monitor and block unusual access attempts.

## Next unit: What are multifactor authentication and Conditional Access?

[Continue](https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/4-what-are-mfa-conditional-access/)