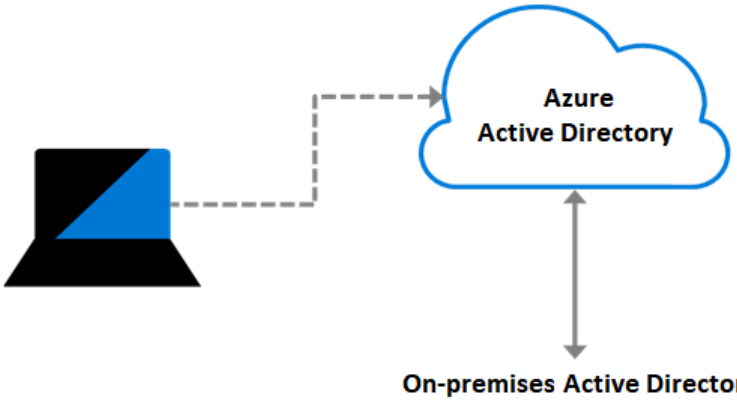
100 XP

Implement Azure Active Directory join

2 minutes

Azure Active Directory enables single sign-on (SSO) to devices, applications, and services from anywhere. To support SSO, IT admins must ensure corporate assets are protected, and devices meet standards for security and compliance.



The Azure AD join feature works with SSO to provide access to organizational apps and resources, and to simplify Windows deployments of work-owned devices.

Things to know about the Azure AD join feature

Let's look at some of the benefits of using joined devices:

Benefit	Description
Single-Sign-On (SSO)	Joined devices offer SSO access to your Azure-managed SaaS apps and services. Your users won't have extra authentication prompts when they access work resources. The SSO functionality is available even when users aren't connected to the domain network.
Enterprise state roaming	Starting in Windows 10, your users can securely synchronize their user settings and app settings data to joined devices. Enterprise state roaming reduces the time to configure a new device.
Access to Microsoft Store for Business	When your users access Microsoft Store for Business by using an Azure AD account, they can choose from an inventory of applications pre-selected by your organization.
Windows Hello	Provide your users with secure and convenient access to work resources from joined devices.
Restriction of access	Restrict user access to apps from only joined devices that meet your compliance policies.
Seamless access to on-premises resources	Joined devices have seamless access to on-premises resources, when the device has line of sight to the on-premises domain controller.

Things to consider when using joined devices

Your organization is interested in using joined devices in their management strategy. As you plan for how to implement the feature, review these configuration points:

- **Consider connection options**. Connect your device to Azure AD in one of two ways:

  - **Register** your device to Azure AD so you can manage the device identity. Azure AD device registration provides the device with an identity that's used to authenticate the device when a user signs into Azure AD. You can use the identity to enable or disable the device.
  - **Join** your device, which is an extension of registering a device. Joining provides the benefits of registering, and also changes the local state of the device. Changing the local state enables your users to sign into a device by using an organizational work or school account instead of a personal account.

- **Consider combining registration with other solutions**. Combine registration with a mobile device management (MDM) solution like Microsoft Intune, to provide other device attributes in Azure AD. You can create conditional access rules that enforce access from devices to meet organization standards for security and compliance.
- **Consider other implementation scenarios**. Although AD Join is intended for organizations that have an on-premises Windows Server Active Directory infrastructure, it can be used for other scenarios like branch offices.

Next unit: Implement Azure Active Directory self-service password reset

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆