

200 XP 

# What is Azure AD join?

7 minutes

You now have a better understanding of device identity and conditional access. You want to investigate Azure Active Directory (Azure AD) join and how it might be used to improve device management for both Azure and on-premises Active Directory Domain Services.

In this unit, you'll learn about Azure AD join, and how to use it for infrastructure and device management.

## Basics of Azure AD join

With Azure AD join, you can join devices to your Azure Active Directory organization without needing to sync with an on-premises Active Directory instance. Azure AD join is best suited to organizations that are principally cloud based, although it can operate in a hybrid cloud and on-premises environment.

## Supported devices

Azure AD join works with Windows 10 or Windows Server 2019 devices. Windows Server 2019 Server Core installation isn't supported. If you're using an earlier Windows operating system, you'll need to upgrade to Windows 10 or Windows Server 2019.

## Identity infrastructure

Decide what identity infrastructure model best supports your organization's needs:

- **Managed environment:** This environment uses pass-through authentication or password hash sync to provide single sign-on (SSO) to your devices.
- **Federated environments:** These environments require the use of an identity provider. That provider must support the WS-Trust and WS-Fed protocols for Azure AD join to work natively with Windows devices. WS-Fed is required to join a device to Azure AD. WS-Trust is needed to sign in to an Azure AD joined device.
- **Smart cards and certificate-based authentication:** These methods aren't valid ways to join devices to Azure AD. But, if you have Active Directory Federation Services configured, you can use smart cards to sign in to Azure AD joined devices. We recommend that you use a service like Windows Hello for Business, which supports passwordless authentication to Windows 10 devices.

- **Manual user configuration:** If you create users in your on-premises Active Directory instance, you need to synchronize the accounts to Azure AD by using Azure AD Connect. If you create users in Azure AD, no additional setup is needed.

## Device management

Azure AD join uses the mobile device management (MDM) platform to manage devices attached to Azure AD. MDM provides a means to enforce organization-required configurations like requiring storage to be encrypted, password complexity, software installations, and software updates.

The latest versions of Windows 10 have a built-in MDM client that works with all compatible MDM systems.

To manage your Azure AD joined devices, there are two approaches:

- **MDM only:** All joined devices are managed exclusively through an MDM provider, like Intune. If your organization uses group policies, you'll need to review your MDM policy for support.
- **Co-management:** All joined devices use a combination of a locally installed System Center Configuration Manager agent and your MDM provider. Microsoft Intune provides co-management capabilities through Configuration Manager. You use Configuration Manager to manage the device while MDM delivers user-management policies.

We recommend that you use the MDM-only approach to manage all Azure AD joined devices.

## Considerations for resources and application access

For the best user experience and to improve access to your application, consider moving all applications and resources to Azure. Although that might be possible in some cases, it isn't always practical. In this section, we'll explore access options for your applications and resources:

- **Cloud-based applications:** Any migrated apps and all new applications will be added to the Azure AD app gallery. Users of Azure AD join can use SSO to access those applications. The majority of browsers support SSO. Azure AD join provides SSO support for device access to applications that are still using Win32.
- **On-premises web applications:** Any bespoke or custom-made software that's hosted on-premises can still be accessed through Azure AD join. Access to those applications needs each user to add the app to their trusted sites or intranet zone, depending on

where the app exists. This action allows the application to use Windows-integrated authentication without prompting the user to authenticate.

- **Other devices:** This option includes existing applications through earlier protocols, and on-premises network shares. Both are available to Azure AD joined devices through SSO, if the device is connected to your domain controller.
- **Printer resources:** These resources won't automatically be available through Azure AD join. Users can still connect to a printer directly, by using its UNC path.

## Provisioning options

When you're deploying Azure AD join, you have three choices for how devices are provisioned and joined to Azure AD:

- **Self-service:** Requires users to manually configure the device during the Windows out-of-box experience (OOBE) for new devices, or by using the Windows settings for older devices. Self-service is better suited to users who have a strong technical background.
- **Windows Autopilot:** Allows you to preconfigure Windows devices, including automatically joining the device to your Active Directory organization, automatic MDM enrollment, and creating customer OOBE content. This approach simplifies the management and deployment of devices across your organization. The Windows device can be provisioned and deployed. The user completes the OOBE as if they're a new user.
- **Bulk enrollment:** Lets you set up a provisioning package that applies to a large number of new Windows devices at the same time.

The following table shows the key features of each approach:

Feature	Self-service	Windows Autopilot	Bulk enrollment
User interaction during setup	Yes	Yes	No
IT involvement	No	Yes	Yes
Applicable flows	OOBE and settings	OOBE only	OOBE only
Local admin rights to primary user	Yes	Configurable	No
Required OEM support	No	Yes	No

# Device settings

In the Azure portal, you control how new devices are joined to your organization. Go to **Azure Active Directory > Devices > Device settings**. From there, you can configure the following features and turn on Azure AD join.

The screenshot shows the 'Devices | Device settings' page in the Azure portal. The left sidebar contains navigation links: 'All devices', 'Device settings' (selected), 'Enterprise State Roaming', 'Diagnose and solve problems', 'Activity', 'Audit logs', 'Troubleshooting + Support', and 'New support request'. The main content area has a header with 'Save', 'Discard', and 'Got feedback?' buttons. Below this, there are several sections with radio button controls: 'Users may join devices to Azure AD' (All, Selected, None), 'Additional local administrators on Azure AD joined devices' (Selected, None), 'Users may register their devices with Azure AD' (All, None), 'Require Multi-Factor Auth to join devices' (Yes, No), and 'Maximum number of devices per user' (50). At the bottom, there is a link for 'Enterprise State Roaming'.

Field	Description
Users may join devices to Azure AD	<b>All</b> allows for any user to join their device. <b>Selected</b> allows you to add specific users that can join devices. <b>None</b> prevents all users from joining their devices.
Additional local administrators on Azure AD joined devices	Lets you specify other users to be included as local administrators on all joined devices. By default, this option is enabled. Azure AD adds the global administrator and device administrator roles as local administrators on devices.

Field	Description
Users may register their devices with Azure AD	Allows users to register their devices with Azure AD join. If you're using Microsoft Intune or mobile device management for Microsoft 365, device registration is required. If either of these services is configured in your Azure AD organization, <b>All</b> is selected and this option is disabled.
Require Multi-Factor Authentication to join devices	Lets you enforce Azure AD Multi-Factor Authentication when the device joins Azure AD. For users who join devices to Azure AD by using Multi-Factor Authentication, the device itself becomes a second factor.
Maximum number of devices per user	Lets you specify the maximum number of devices a user can have in Azure AD. If a user reaches this maximum, they need to remove a device to add a new one.

For our scenario, we can add a pilot group of users to try AD join. In that case, choose **Users may join devices to Azure AD > Selected**, and then add members of your pilot group. When you're ready to deploy Azure AD join to your entire Azure AD organization, select **All**.

## Mobility settings

You might need to add an MDM provider before you can configure mobility settings. To add your MDM provider, go to **Azure Active Directory > Mobility (MDM and MAM) > Add application**.

Microsoft Azure

Search resources, services, and docs (G+)

Home


>

Contoso | Mobility (MDM and MAM)


>

Add an application


Add an application




AirWatch by V...




IBM MaaS360




Lightspeed Mo...




ManageEngine ...




Microsoft Intune



Miradore Online



MobileIron\_EMM



On-premises M...

When you have your MDM provider added, you can configure the following mobility settings:

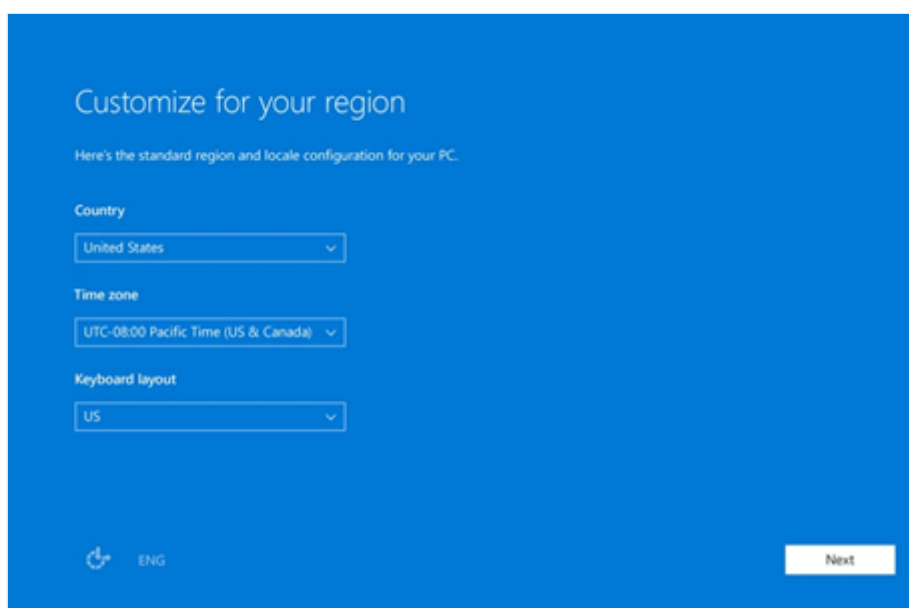
Mobility setting	description
MDM user scope	Select <b>None</b> , <b>Some</b> , or <b>All</b> . If the user <i>is</i> in the MDM scope and you have an Azure AD Premium subscription, MDM enrollment is automated along with Azure AD join. All users within the scope must have an appropriate license for your MDM. If not, the MDM enrollment fails and Azure AD join is rolled back. If the user <i>isn't</i> in the MDM scope, Azure AD join finishes without any MDM enrollment. The device is an unmanaged device.
MDM URLs	The three URLs related to your MDM configuration are <b>MDM terms of use URL</b> , <b>MDM discovery URL</b> , and <b>MDM compliance URL</b> . Each URL has a predefined default value. If these fields are empty, contact your MDM provider for more information.
MAM settings	Mobile application management (MAM) does not apply to Azure AD join.

Recall that you need to restrict access to the organization's resources to only devices that your organization manages and that your MDM system considers compliant. For our scenario, we'd want to add our organization's MDM provider and select **MDM user scope > All**.

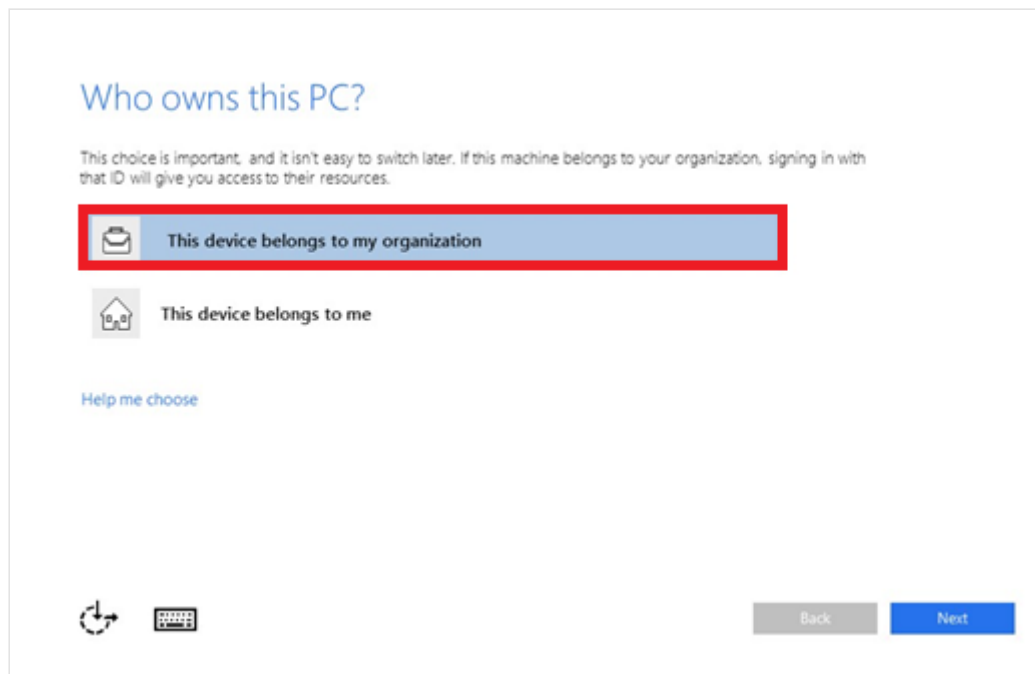
## User experience when joining a Windows 10 device

You've given a new device to a tech-savvy employee. They'll use the self-service approach to join the device to your Active Directory organization, which is using Multi-Factor Authentication. The following steps show you what that workflow looks like:

1. After starting the device, the employee follows the prompts to set it up, including customizing their region and selecting a language.



2. The employee accepts the Microsoft Software License Terms.
3. The employee selects the network connection for connecting to the cloud.
4. When asked **Who owns this PC?**, the employee selects **This device belongs to my organization**.



5. The employee signs in with the credentials that your organization has supplied.
6. The employee is prompted with a multifactor authentication challenge.
7. Azure AD checks the configuration settings to see if the device should be enrolled in MDM.
8. When the configuration check is successful, the device is registered with the organization's Azure AD instance. If MDM is being used, the device is enrolled and managed.

## Check your knowledge

1. What provisioning options are available through Azure AD join?

- ☐ Self-service by using the Windows out-of-box experience (OOBE), Windows Autopilot, or bulk enrollment
- ☐ Self-service by using MDM, Windows Autopilot, or bulk enrollment
- ☐ Windows Autopilot or bulk enrollment

2. What happens when a device isn't in the MDM scope?

- ☐ The user is asked to add the device to MDM before the device can join Azure AD.
- ☐ The device can't join Azure AD until the device has been registered with MDM.
- ☐ The Azure AD join finishes without the enrollment to MDM.



Check your answers

---