Microsoft

Windows 10

SECOND EDITION

Exam Ref MD-100

Andrew Bettany
Andrew Warren

Microsoft

Exam Ref MD-100 Windows 10

Second Edition

Andrew Bettany
Andrew Warren

AZURE AD–JOINED DEVICE

Joining a Windows 10 device to Azure AD is like registering a device with Azure AD, but it allows enhanced management capabilities. Once a device has been joined to Azure AD, the local state of a device changes to enable your users to sign into the device using the work or school account instead of a personal account.

An enterprise will typically join its owned devices to Azure AD to allow for cloud-based management of the devices and to grant access to corporate apps and resources.

> ***NOTE*** **BULK-JOIN DEVICES TO AZURE AD**
>
> **Bulk joining of devices to Azure AD and Windows Autopilot deployment are outside the scope of the MD-100 Windows 10 exam, though you should expect to find these topics covered in the MD-101 Managing Modern Desktops exam.**

Organizations of any size can deploy Azure AD Join. Azure AD Join works well in a cloud-only (no on-premises infrastructure) environment. When Azure AD Join is implemented in a hybrid environment, users gain access to both cloud and on-premises apps and resources.

Azure AD–joined devices allow your users to access the following benefits:

- **Single-Sign-On (SSO)** Allows users simplified access to Azure managed SaaS apps, services, and work resources.
- **Enterprise-compliant roaming** User settings can be kept in sync across joined devices using their Azure AD–joined devices (without the need to sign in using a Microsoft account).
- **Access to Microsoft Store for Business** Users can access a Microsoft Store populated with apps chosen by your organization.
- **Windows Hello** Devices can be secured using the enterprise features of Windows Hello.
- **Restriction of access** Devices will only be able to access apps that meet the organizational compliance policy.
- **Seamless access to on-premises resources** Hybrid Azure AD–joined devices can access on-premises resources when connected to the domain network.

Organizations that already have Microsoft 365 or other SaaS apps integrated with Azure AD have the necessary components in place to have devices managed in Azure AD instead of being managed in Active Directory.

AZURE AD–REGISTERED DEVICES

Once a device is registered into management, it is “known” to Azure AD, and information relating to the device is stored in Azure AD. Effectively, the device is given an identity with Azure AD. You can create conditional access rules to determine whether access to resources from your devices will be granted.

Azure AD–registered devices enable users to use personally owned devices to access your organization's resources in a controlled manner. Azure AD supports bring-your-own-device (BYOD) scenarios for several types of devices, including devices running Windows 10, iOS, Android, and macOS.

With an Azure AD–registered device, the user will gain access to resources using a work or school Azure AD account at the time they access the resources. All corporate data and apps will be kept completely separated from the personal data and apps on the device. If the personal computer, tablet, or phone that is registered with Azure AD does not meet your corporate standards for security and compliance—for example, if a device is not running a supported version of the operating system, or it has been jail broken—then access to the resource will be denied.

Device Registration enables you to facilitate an SSO experience for users, removing the need for them to repeatedly enter credentials to access resources.

The main reasons to implement Device Registration are:

- To enable access to corporate resources from non-domain joined or personally owned devices
- To enable SSO for specific apps and/or resources managed by Azure AD

After you enable Device Registration, users can register and enroll their devices in your organizational tenant. After they have enrolled their devices:

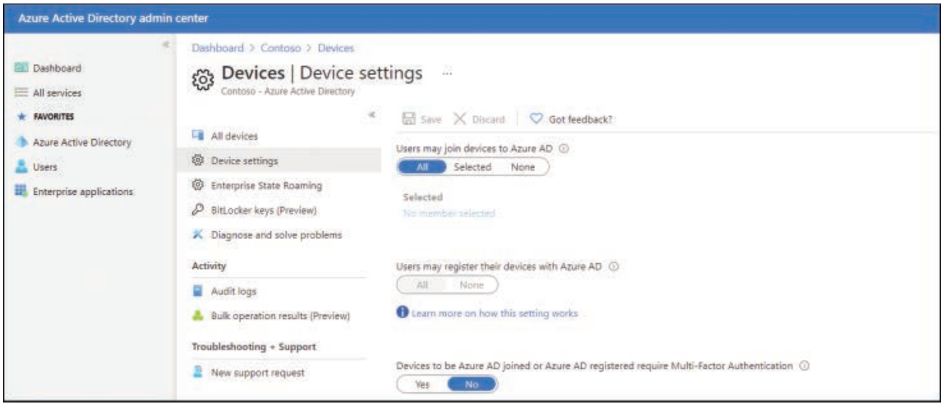
- Enrolled devices are associated with a specific user account in Azure AD.
- A device object is created in Azure AD to represent the physical device and its associated user account.
- A user certificate is installed on the user's device.

Configure device management

Device management requires configuration to ensure that when your users attempt Device Registration, the process will not fail. By default, the setting is enabled, and it allows all Windows 10 devices that present valid credentials to be managed by your Azure AD.

The Azure portal provides a cloud-based location to manage your devices. To allow registration of devices into Azure AD, follow these steps:

1. Sign in as an administrator to the Azure portal at *https://portal.azure.com*.
2. On the left navigation bar, select **Azure Active Directory**.
3. In the **Manage** section, select **Devices**.
4. Select **Device settings**.
5. On the **Device settings** blade, ensure that **Users may join devices to Azure AD** is set to **All**, as shown in Figure 2-6. If you choose **Selected**, then select the **Selected** link and choose the users who can join Azure AD. You can select both individual users and groups of users.
6. Select **Save**.


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Contoso > Devices
Devices | Device settings
Contoso - Azure Active Directory
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Save
Discard
Got feedback?
Learn more on how this setting works

Users may join devices to Azure AD: [✓ All] Selected None

Selected: No member selected

Users may register their devices with Azure AD: All None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication: Yes [✓ No]

FIGURE 2-6 Enabling Azure AD join

Within the Azure AD portal, you can fine-tune the process of registering and joining devices by configuring the device settings as listed in Table 2-4.

TABLE 2-4 Azure AD device configuration settings

Device Setting	Description
Users May Join Devices To Azure AD	The default is All. The Selected option allows you to select users who can join Windows 10 devices to Azure AD.
Users May Register Their Devices With Azure AD	Required to allow devices to be registered with Azure AD by users. Options include the following: ■ **None** Prevents devices from being registered with Azure AD. ■ **All** Automatically configured if Enrollment with Microsoft Intune or Mobile Device Management (MDM) for Office 365 is configured as they require Device Registration.
Additional Local Administrators On Azure AD Joined Devices	You can assign the users who are granted local administrator rights on a device and added to the Device Administrators role in Azure AD. By default, global administrators in Azure AD and device owners are granted local administrator rights. Requires an Azure AD Premium license.
Devices To Be Azure AD Joined Or Azure AD Registered Require Multi-Factor Authentication	Choose whether users are required to use multifactor authentication to join their devices to Azure AD. The default setting is No. This setting is only applicable to Azure AD Join on Windows 10 and BYOD registration for Windows 10, iOS, and Android. This setting does not apply to hybrid Azure AD–joined devices, Azure AD–joined VMs in Azure, and Azure AD–joined devices using Windows Autopilot self-deployment mode.
Maximum Number Of Devices Per User	By default, all users can have a maximum of 50 devices in Azure AD. Once this quota is reached, they are not able to add additional devices until one or more of the existing devices are removed. The device quota is across both Azure AD–joined and Azure AD–registered devices.
Enterprise State Roaming	You can configure the Enterprise State Roaming settings for specific users or groups. With Azure AD Premium, you can select a subset of your users and enable this feature for them. Without Azure AD Premium, you can only configure Enterprise State Roaming for all users at once.

EXAM TIP

Each device must be able locate the internet to allow you to authenticate using your Azure AD credentials. If a device cannot locate the cloud-based identity service, there will be a problem accessing resources managed by Azure AD.

DEVICE MANAGEMENT TASKS

Once devices have been registered or joined to Azure AD, they appear in the list within the All Devices section of the Azure Active Directory Admin Center. Devices managed by another management authority, such as Microsoft Intune, are also listed.

To locate a device, you can search using the device name or device ID. Once you have located a device, you can perform additional device management tasks, including the following:

- **Update devices** You can enable or disable devices. You need to be a global administrator in Azure AD to perform this task, which prevents a device from being able to authenticate with Azure AD and thus prevents the device from accessing any Azure AD resources.
- **Delete devices** When a device is retired, or it no longer requires access to your corporate resources, it should be deleted in Azure AD. Deleting a device requires you to be a global administrator in Azure AD or an Intune administrator. Once deleted, all details stored in Azure AD relating to the device—for example, BitLocker keys for Windows devices—are removed. If a device is managed elsewhere, such as in Microsoft Intune, you should ensure that the device has been wiped before deleting the device in Azure AD.
- **View device ID** Each device has a unique device ID that can be used to search for the device; the unique device ID can be used as a reference if you need to use PowerShell during a troubleshooting task.
- **View device BitLocker key** Windows devices managed by Azure AD can have their BitLocker recovery keys stored in Azure AD. You can access this key if the encrypted drive needs to be recovered. To view or copy the BitLocker keys, you need to be the owner of the device or have one of the following roles assigned: Global Administrator, Help desk Administrator, Security Administrator, Security Reader, or Intune Service Administrator.

NOTE **USE POWERSHELL TO BACK UP THE BITLOCKER RECOVERY KEY TO AZURE AD**

For Azure AD–joined computers, the BitLocker recovery password should be stored in Azure AD. You can use the PowerShell cmdlets `Add-BitLockerKeyProtector`, `Get-BitLockerVolume`, and `BackupToAAD-BitLockerKeyProtector` to add a recovery password and back it up to Azure AD before enabling BitLocker.

Connect devices to Azure AD

Once the prerequisites have been configured to allow the Device Registration service to take place, you are able to connect devices to Azure AD.

There are three ways to connect a Windows 10 device to Azure AD:

- Joining a new Windows 10 device to Azure AD
- Joining an existing Windows 10 device to Azure AD
- Registering a Windows 10 device to Azure AD

In this section, you will learn the steps required for each method of connecting Windows 10 to Azure AD.

JOIN A NEW WINDOWS 10 DEVICE TO AZURE AD

In this method, we will take a new Windows 10 device and join the device to Azure AD during the first-run experience. The device could have been previously prepared using an enterprise deployment method, or it could have been distributed by the original equipment manufacturer (OEM) directly to your employees.

If the device is running either Windows 10 Professional or Windows 10 Enterprise, the first-run experience will present the setup process for company-owned devices.

> ***NOTE*** **JOINING A DEVICE TO ACTIVE DIRECTORY DURING THE FIRST-RUN EXPERIENCE**
>
> **Joining an on-premises Active Directory domain is supported in Windows 10 during the Windows Out-of-Box Experience (OOBE). If you need to join a computer to an AD domain, during setup you should choose the option Set Up For An Organization and then select the Domain Join Instead link. You then need to set up the device with a local account and join the domain from the Settings app on your computer. For the MD-100 Windows 10 exam, you should expect that devices will be cloud- or hybrid cloud–enabled.**

To join a new Windows 10 device to Azure AD during the first-run experience, use the following steps:

1. Start the new device and allow the setup process.
2. On the **Let’s start with region. Is this right?** page, select the regional setting that you need and select **Yes**.
3. On the **Is this the right keyboard layout?** page, select the keyboard layout settings and select **Yes**.
4. On the **Want to add a second keyboard layout?** page, add a layout or select **Skip**.
5. The computer should automatically connect to the internet, but it if it does not, you will be presented with the **Let’s connect you to a network** page, where you can select a network connection.

6. On the **How would you like to set up?** page, choose **Set up for an organization** and select **Next**.
7. On the **Sign in with Microsoft** page, enter your organization or school account and password and select **Next**.
8. On the **Choose privacy settings for your device**, choose the settings and select **Accept**.
9. On the **Use Windows Hello with your account** page, select **OK**.
10. On the **More information required** page, select **Next**, provide the additional security verification information, and select **Next** again.
11. Depending on organizational settings, your users might be prompted to set up MFA. On the **Keep your account secure** page, select **Next** and set up the Microsoft Authenticator.
12. Depending on organizational settings, your users might be prompted to set up Windows Hello. By default, they will be prompted to set up a PIN. When prompted to set up a PIN, select **Set up PIN**. You should now be automatically signed in to the device, joined to your organization or school Azure AD tenant, and presented with the desktop.

JOIN AN EXISTING WINDOWS 10 DEVICE TO AZURE AD

In this method, we will take an existing Windows 10 device and join it to Azure AD. You can join a Windows 10 device to Azure AD at any time. Use the following procedure to join the device:

1. Open the **Settings** app and then select **Accounts**.
2. In **Accounts**, select the **Access work or school** tab.
3. Select **Connect**.
4. On the **Set up a work or school account** page, under **Alternate actions**, select **Join this device to Azure Active Directory**, as shown in Figure 2-7.
5. On the **Microsoft account** page, enter your email address and select **Next**.
6. On the **Enter password** page, enter your password and select **Sign In**.
7. On the **Make sure this is your organization** page, confirm that the details on screen are correct and select **Join**.
8. On the **You’re all set!** page, select **Done**.
9. To verify that your device is connected to your organization or school, check that your Azure AD email address is listed under the **Connect** button, indicating that it is connected to Azure AD.