Previous Unit 2 of 5 Next

200 XP

What is device identity in Azure?

7 minutes

In this unit, you'll learn about device identity and registration options, and how they apply to various devices. You'll see how you can apply conditional access to improve access control with your devices. Finally, you'll look at the benefits, and the considerations, of using device identity in Azure.

Basics of device identity

Device identity in Azure Active Directory (Azure AD) helps you control the devices that you add to your organization's Azure AD instance. It also helps you control the data, resources, and assets that those devices can access. It provides a framework to implement device-based conditional access. You can use a device-based conditional access policy to limit device access to your organization's assets.

Today's work environment extends beyond the controllable boundaries of your on-premises workspace. Your staff can now work in various locations, not only in their home country or region but also abroad. Users can access a broader range of technologies. Some of these technologies are owned by your organization, but others aren't.

The challenge faced by IT staff is how to give users flexibility while protecting the company's data. You want to support your users and enable them to be productive wherever they're working, on whatever device they're using. But you still need to keep your organization's resources and assets safe.

Finding a balance between protecting assets and allowing users greater flexibility in the devices they use is at the heart of device identity. Every device that you want to connect to your network must be known. Tools such as Microsoft Intune can enhance what's known about a device by ensuring compliance with organizational requirements.

Combining Azure AD with single sign-on means that users can access services and apps through any device. This outcome meets your organization's need to protect its resources and assets, and gives users the flexibility they want.

Device registration options

You have three device registration options to add a device to Azure AD:

- **Azure AD registered**: These devices fall into the Bring Your Own Device (BYOD) category. They're typically privately owned, or they use a personal Microsoft account or another local account. This method of device registration is the least restrictive because it supports devices running Windows 10, iOS, iPadOS, Android, and macOS. Device security is typically provided from a password, a PIN, a pattern, or Windows Hello.

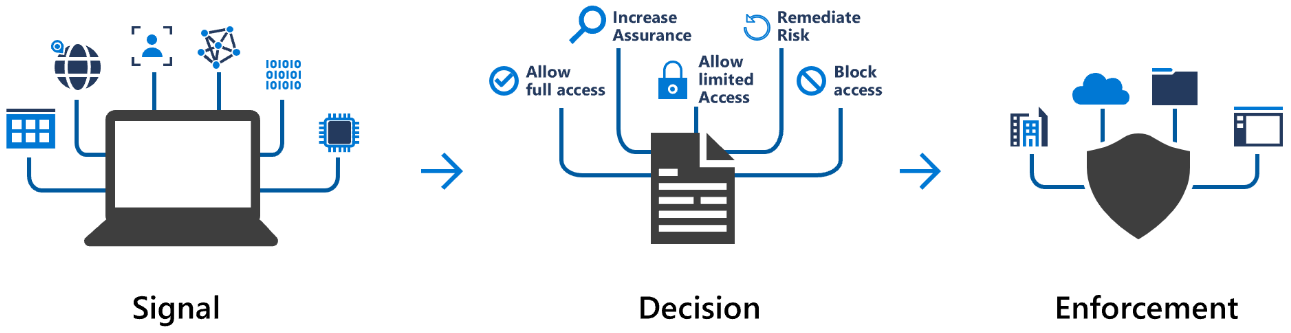
- **Azure AD joined**: These devices are owned by your organization. Users access your cloud-based Azure AD instance through their work account. Device identities exist only in the cloud. This option is available only to Windows 10 or Windows Server 2019 devices. Windows Server 2019 Server Core installation isn't supported. Security for this option uses either a password or Windows Hello.

- **Hybrid Azure AD joined**: This option is similar to Azure AD joined. The devices are owned by the organization, and they're signed in with an Azure AD account that belongs to that organization. Device identities exist in the cloud and on-premises. The hybrid option is better suited to organizations that need on-premises and cloud access. This option supports Windows 7, 8.1, and 10, and Windows Server 2008 or later.

Conditional access

Conditional access in Azure AD uses data from sources known as *signals*, validates them against a user-definable rule base, and chooses the best outcome to enforce your organization's security policies. Conditional access enables device identity management, but conditional access policies can be complex.

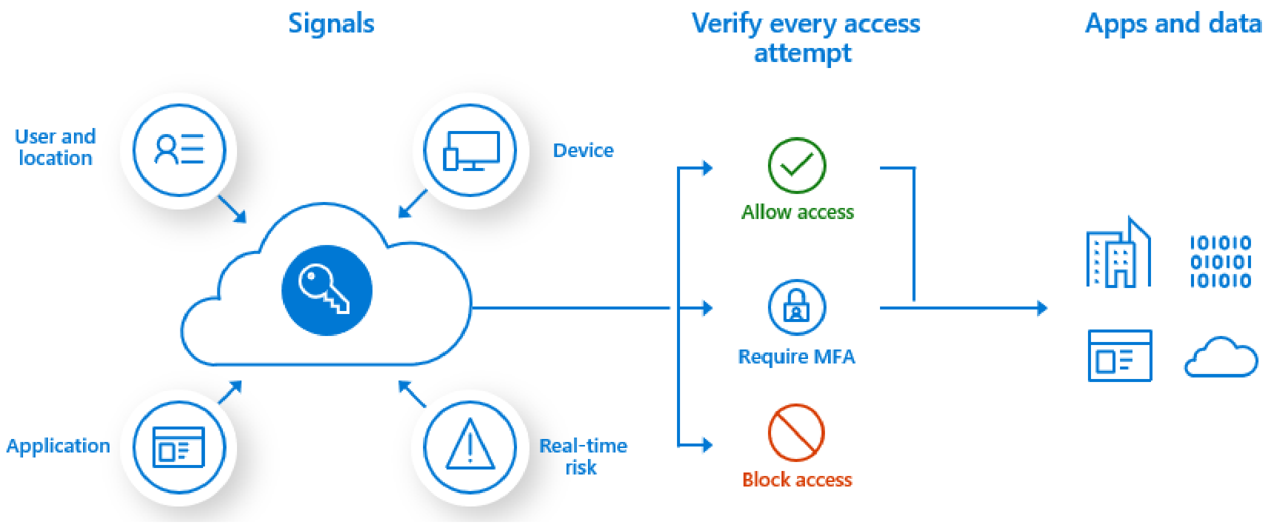
At their simplest, these policies can be thought of as "if-then" statements. If a user wants access to a resource, then they must fulfill the condition to complete the request. Example: A payroll manager wants to access the payroll application. The conditional access policy requires them to use a compliant device and to complete multifactor authentication to access the application.



Conditional access policies are applied after a user has successfully completed first-factor authentication, typically with a username and password. These policies aren't a substitute for first-factor authentication. They're used to assess factors like device, location, and application, and to assess the risk in real time.

Common signal types

Conditional access uses many common signal types to make a decision on which outcome to recommend.



Signals include the following types:

- **User or group membership** provides fine-grained access to resources.
- **IP location information** uses an allow list of trusted IP addresses, and a deny list of blocked or banned IP addresses.
- **Device** allows you to specify the type of device and its state.
- **Application** lets you control access to an application for a specific device.
- **Real-time and calculated risk detection** allows Azure AD to identify behaviors not only during sign-in but also throughout the user's session.
- **Microsoft Cloud App Security** provides real-time monitoring of the user's session and application access. Cloud App Security also helps you control your cloud environment.

Common decisions

Conditional access evaluates the signals and provides a decision:

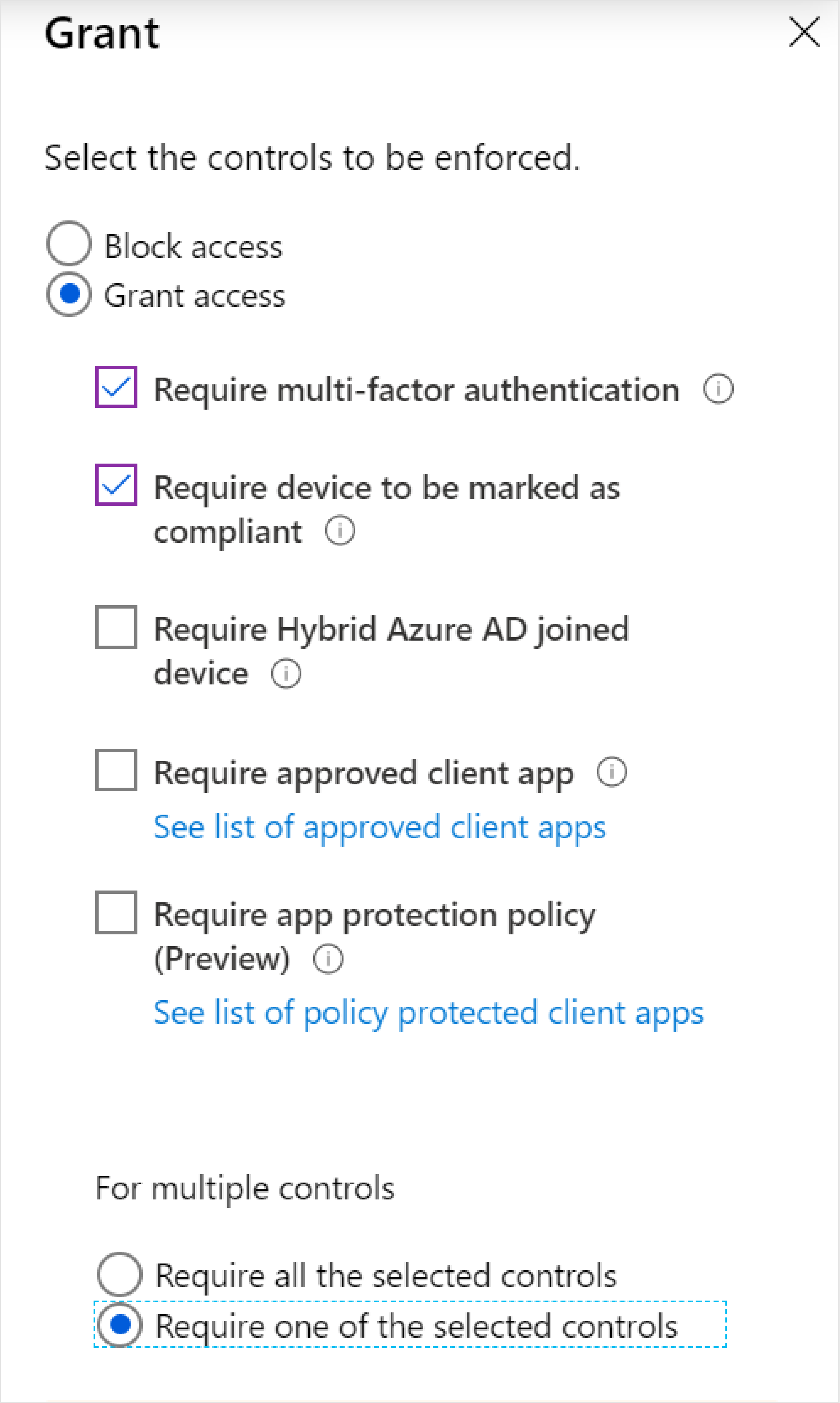
- **Block access**, which is the most restrictive.
- **Grant access**, which is the least restrictive but might require additional criteria before allowing access.

Those criteria can be one or more of:

- Multifactor authentication
- Device marked as compliant
- Device that's hybrid Azure AD joined
- Approved application

- Need for an app protection policy

If your organization uses Azure AD Multi-Factor Authentication, users don't have to do multifactor authentication when they're using a device that's mobile device management (MDM) compliant and Azure AD joined. You can select the option **Require one of the selected controls** with your grant controls selected. If you need extra security for something like a payroll app, select **Require all the selected controls** to require multifactor authentication and a compliant device.



Grant

Select the controls to be enforced.

○ Block access
● Grant access

☑ Require multi-factor authentication

☑ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

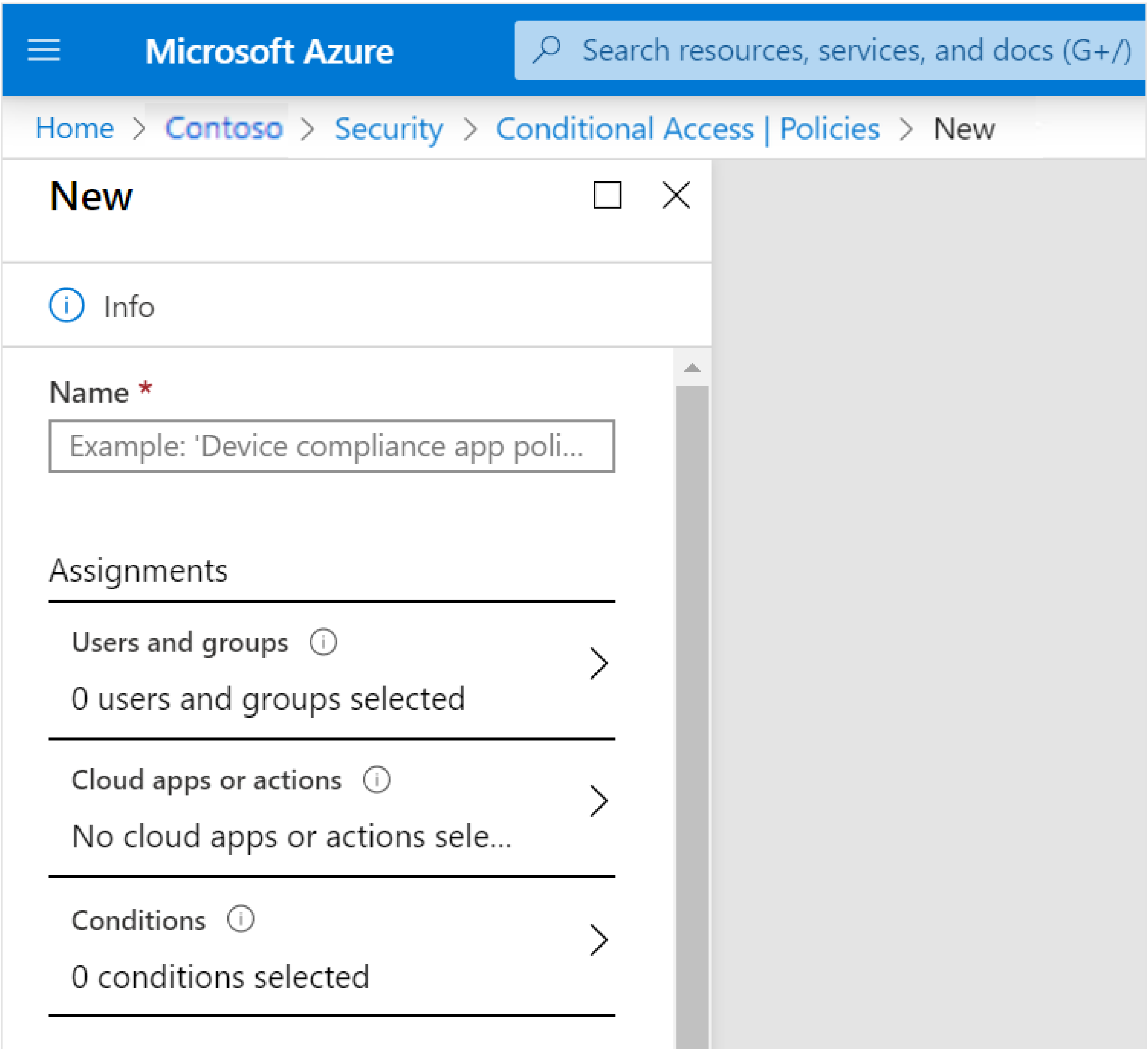
Commonly applied policies

Many organizations have common access concerns that conditional access policies can help with, such as:

- Requiring multifactor authentication for users who have administrative roles.
- Requiring multifactor authentication for Azure management tasks.
- Blocking sign-ins for users who are trying to use older authentication protocols.
- Requiring trusted locations for Azure AD Multi-Factor Authentication registration.
- Blocking or granting access from specific locations.
- Blocking risky sign-in behaviors.
- Requiring organization-managed devices for specific applications.

Selections to create a conditional access policy

To create a conditional access policy, go to **Azure Active Directory** > **Security** > **Conditional Access** > **New policy**.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso > Security > Conditional Access | Policies > New
New
Info

Name *

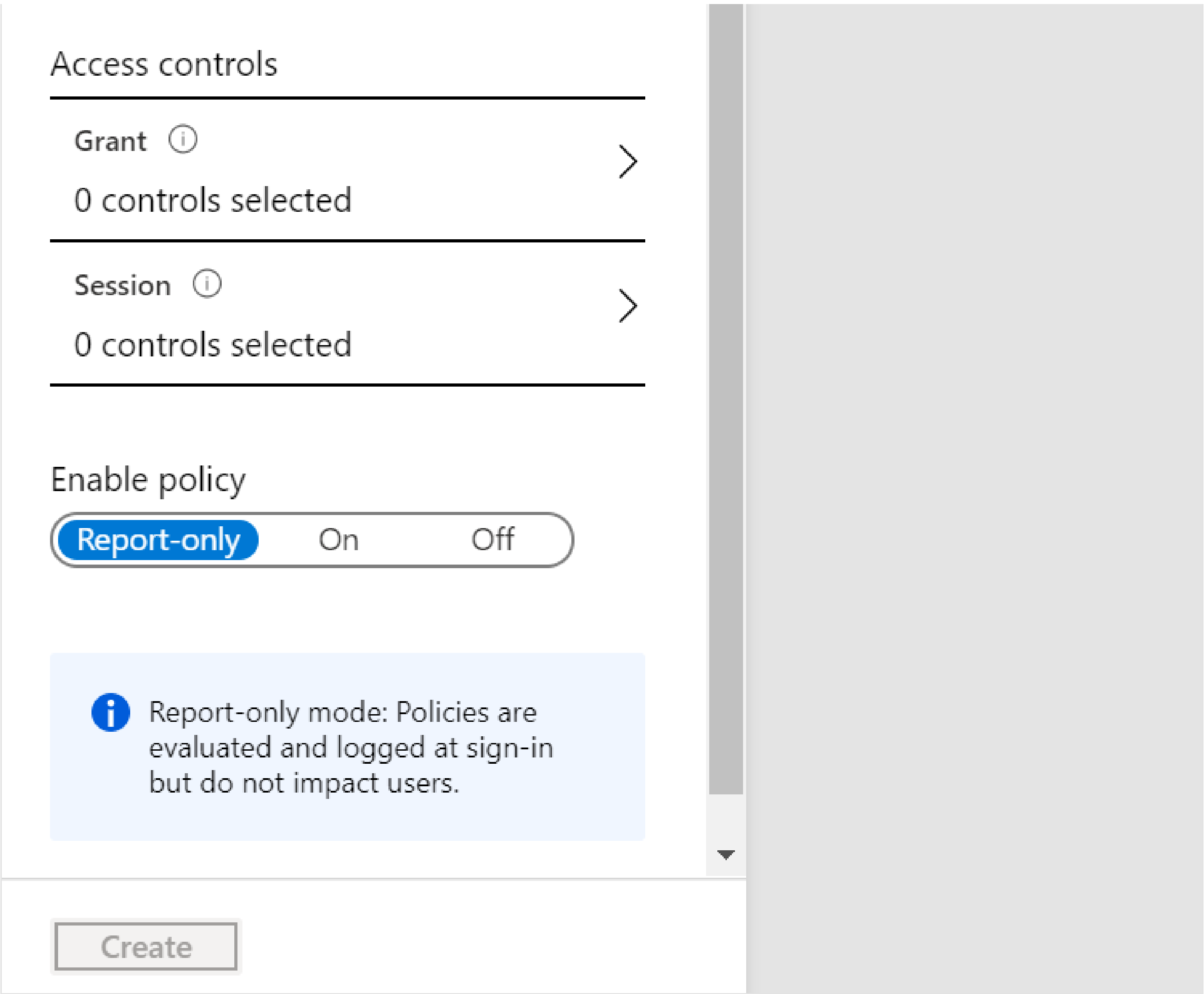
Example: 'Device compliance app poli...

Assignments

Users and groups
0 users and groups selected

Cloud apps or actions
No cloud apps or actions sele...

Conditions
0 conditions selected



Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only mode: Policies are evaluated and logged at sign-in but do not impact users.

To make your policy work, you must configure:

What	How	Why
Cloud apps	Select one or more apps.	The goal of a conditional access policy is to enable you to control how authorized users can access cloud apps.
Users and groups	Select at least one user or group that is authorized to access your selected cloud apps.	A conditional access policy that has no users and groups assigned is never triggered.
Access controls	Select at least one access control.	If your conditions are satisfied, your policy processor needs to know what to do.

Benefits of device identity management

Some of the benefits of using device identity, combined with conditional access in Azure AD, are:

- The combination simplifies the procedure for adding and managing devices in Azure AD.
- The combination reduces the friction for users when they're switching between devices.
- Azure AD supports MDM tools such as Microsoft Intune.
- You can use single sign-on (SSO) with any registered or joined device.

Considerations for using device identity management

When you're evaluating device identity, consider the following factors:

- Using the Azure AD joined or hybrid option limits you to using a Windows-based or Windows Server-based operating system on the device.
- Conditional access requires an Azure AD Premium P1 license or a Microsoft 365 Business license.

Check your knowledge

1. What operating systems do Azure AD registered devices support?

○ Windows 10, iOS, Android, and macOS

○ Windows 7, Windows 8.1, and Windows 10 only

○ Windows 10 and macOS

2. What device security sign-in options does Azure AD join support?

○ An Azure AD work account with password, PIN, pattern, or Windows Hello

○ An Azure AD work account with password or Windows Hello, and multifactor authentication

○ A Microsoft account with password, Windows Hello, and multifactor authentication

3. When is conditional access applied?

○ Before first-factor authentication

○ As part of first-factor authentication

○ After first-factor authentication

Check your answers