Filename: microsoft-ms101-2-2-1-design-conditional-access-policies
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Manage Device Compliance
EpisodeName: Design Conditional Access Policies
Description: Adam and Wes discuss how to design conditional access policies.

Design Conditional Access Policies

Implement Modern Device Services (30-35%)

Manage Device Compliance
• Plan for Device Compliance
• Design Conditional Access Policies
• Create Conditional Access Policies
• Configure Device Compliance Policy
• Manage Conditional Access Policies

==========

Design Conditional Access Policies

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

A Conditional Access policy brings signals together, to make decisions, and enforce organizational policies.

Common signals that Conditional Access can take in to account when making a policy decision include the following:

```
• User or group membership
• IP Location information
• Device
• Application
```

Common decisions:

```
• Block access - Most restrictive decision

• Grant access - Least restrictive decision, can still require one or more of
```

the following options:

```
• Require multi-factor authentication
• Require device to be marked as compliant
• Require Hybrid Azure AD joined device
• Require approved client app
• Require app protection policy (preview)
```

Commonly applied policies:

```
• Requiring multi-factor authentication for users with administrative roles
• Requiring multi-factor authentication for Azure management tasks
• Blocking sign-ins for users attempting to use legacy authentication protocols
• Requiring trusted locations for Azure Multi-Factor Authentication registration
• Blocking or granting access from specific locations
• Blocking risky sign-in behaviors
• Requiring organization-managed devices for specific applications
```

License requirements

Azure AD Premium P1 license; provides the basic features only.

Azure AD Premium P2 license; enables identity protection which is necessary if you want to use sign-in risk

Intune; necessary if you want to use conditions that specify device compliance

NOTE: Customers with Microsoft 365 Business licenses also have access to Conditional Access features.

Permissions - You need the Conditional Access Administrator role.

What are the building blocks of a Conditional Access Policy?

Assignments - controls the who, what, and where of the Conditional Access policy.

Users and groups - assign who the policy will include or exclude. This assignment can include all users, specific groups of users, directory roles, or external guest users.

Cloud apps or actions - can include or exclude cloud applications or user actions that will be subject to the policy.

Conditions - A policy can contain multiple conditions.

Sign-in risk - For organizations with Azure AD Identity Protection, the risk detections generated there can influence your Conditional Access policies.

Device platforms - Organizations with multiple device operating system platforms may wish to enforce specific policies on different platforms.

The information used to calculate the device platform comes from unverified sources such as user agent strings that can be changed.

Locations - Location data is provided by IP geolocation data. Administrators can choose to define locations and choose to mark some as trusted like those for their organization's network locations.

Client apps - By default Conditional Access policies apply to browser apps, mobile apps, and desktop clients that support modern authentication.

This assignment condition allows Conditional Access policies to target specific client applications not using modern authentication. These applications include Exchange ActiveSync clients, older Office applications that do not use modern authentication, and mail protocols like IMAP, MAPI, POP, and SMTP.

Device state - used to exclude devices that are hybrid Azure AD joined, or marked as compliant in Intune. This exclusion can be done to block unmanaged devices.

Access controls - The access controls portion of the Conditional Access policy controls how a policy is enforced.

Block access - will block access under the specified assignments.

Grant access - The grant control can trigger enforcement of one or more controls.

```
• Require multi-factor authentication (Azure Multi-Factor Authentication)
• Require device to be marked as compliant (Intune)
• Require Hybrid Azure AD joined device
• Require approved client app
• Require app protection policy
```

Administrators can choose to require one of the previous controls or all selected controls using the following options. The default for multiple controls is to require all.

```
• Require all the selected controls (control and control)
• Require one of the selected controls (control or control)
```

Session - Session controls can limit the experience:

```
• Use app enforced restrictions - Currently works with Exchange Online and
```

SharePoint Online only. Passes device information to allow control of experience granting full or limited access.

```
• Use Conditional Access App Control - Uses signals from Microsoft Cloud App
```

Security to do things like:
• Block download, cut, copy, and print of sensitive documents
• Monitor risky session behavior
• Require labeling of sensitive files

```
• Sign-in frequency - Ability to change the default sign in frequency for
```

modern authentication.

```
• Persistent browser session - Allows users to remain signed in after closing
```

and reopening their browser window.

A Conditional Access policy must contain at minimum the following to be enforced:

```
• Name of the policy
• Assignments
• Users and/or groups to apply the policy to
• Cloud apps or actions to apply the policy to
• Access controls
• Grant or Block controls
```