Filename: microsoft-ms101-2-5-1-manage-conditional-access-policies
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Manage Device Compliance
EpisodeName: Manage Conditional Access Policies
Description: Adam and Wes discuss how to manage conditional access policies.

Manage 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

==========

Manage Conditional Access Policies

How do you know what to expect from the Conditional Access policies in your environment? To answer this question, you can use the Conditional Access What If tool.

This tool enables you to evaluate a simulated sign-in of a user.

The simulation estimates the impact this sign-in has on your policies and generates a simulation report.

The report does not only list the applied Conditional Access policies but also classic policies if they exist.

Classic policies are Conditional Access policies, you have created in:

```
• The Azure classic portal
• The Intune classic portal
• The Intune App Protection portal
```

On the Conditional Access page, you can access your classic policies by clicking Classic policies in the Manage section.

Settings:

```
• User - You can only select one user. This is the only required field.


• Cloud apps - The default for this setting is All cloud apps. The default
```

setting performs an evaluation of all available policies in your environment. You can narrow down the scope to policies affecting specific cloud apps.

```
• IP address - The IP address is a single IPv4 address to mimic the location
```

condition. The address represents Internet facing address of the device used by your user to sign in.

```
• Device platforms - This setting mimics the device platforms condition and
```

represents the equivalent of All platforms (including unsupported).

```
• Client apps - This setting mimics the client apps condition. By default,
```

this setting causes an evaluation of all policies having Browser or Mobile apps and desktop clients either individually or both selected. It also detects policies that enforce Exchange ActiveSync (EAS). You can narrow this setting down by selecting:

```
    • Browser to evaluate all policies having at least Browser selected

    • Mobile apps and desktop clients to evaluate all policies having at least
Mobile apps and desktop clients selected


• Sign-in risk - This setting mimics the sign-in risk condition.
```

What about the Azure AD sign-ins report?