Filename: microsoft-ms101-2-1-2-determine-use-cases-for-device-compliance
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Manage Device Compliance
EpisodeName: Determine Use Cases for Device Compliance
Description: Adam and Wes discuss how to determine use cases for device compliance.

Determine Use Cases for Device Compliance

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

==========

Determine Use Cases for Device Compliance

Things to remember/know BEFORE we start:

```
1. Compliance Policies are nothing more than a series of rules that YOU define

2. The rules determine device compliance status

3. Compliance Policies MAY be able to remediate certain issues, but not all,
```

SO, quarantine is usually the outcome, followed by remediation if the user
choses to

```
4. User with devices that are not compliant will receive notifications
```

Use Cases:

Windows 10 -

```
Settings:

Minimum OS Version
Valid Operating System Builds
```

Example Use Case:

```
Devices not running the latest cumulative update are marked as NON-COMPLIANT

Devices running the latest release of <release #> are still valid while
```

upgrades are rolling

macOS -

```
Setting:

Require System Integrity Protection
```

Example Use Case:

```
Devices that do not have system integrity protection enabled are marked as
```

NON-COMPLIANT

Android -

```
Settings:

Rooted Devices
Encryption of data storage on device
```

Example Use Case:

```
Devices that are rooted are marked as NON-COMPLIANT

Devices that do not have data storage encryption enabled are marked as
```

NON-COMPLIANT

iOS -

```
Settings:

Jailbroken Devices
Restricted Apps
```

Example Use Case:

```
Jailbroken devices are marked as NON-COMPLIANT

Devices that have the <app name> installed are marked as NON-COMPLIANT
```