Device Compliance

Android

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **Android**.
5. Choose **Settings Configure**. Enter the **Device Health**, **Device Properties**, and **System Security** settings, as described in this article.

Device health

- **Rooted devices**: Choose **Block** to mark rooted (jailbroken) devices as not compliant. When you choose **Not configured** (default), this setting isn't evaluated for compliance or non-compliance.
- **Require the device to be at or under the Device Threat Level**: Use this setting to take the risk assessment from the Lookout MTP solution as a condition for compliance. When you choose **Not configured** (default), this setting isn't evaluated for compliance or non-compliance. To use this setting, choose the allowed threat level to be:
  - **Secured**: This option is the most secure, as the device can't have any threats. If the device is detected with any level of threats, it's evaluated as noncompliant.
- **Google Play Services is configured**: **Require** that the Google Play services app is installed and enabled.
- **Up-to-date security provider**: **Require** that an up-to-date security provider can protect a device from known vulnerabilities.
- **Threat scan on apps**: **Require** that the Android **Verify Apps** feature is enabled.
- **SafetyNet device attestation**: Enter the level of SafetyNet attestation that must be met:
  - **Check basic integrity & certified devices**

System security settings

Password

- **Require a password to unlock mobile devices**: **Require** users to enter a password before they can access their device.
- **Minimum password length**: 8

- **Required password type**: **At least alphanumeric with symbols**
- **Maximum minutes of inactivity before password is required**: 10
- **Password expiration (days)**: 60
- **Number of previous passwords to prevent reuse**: 5

Encryption

- **Encryption of data storage on a device** (Android 4.0 and above, or KNOX 4.0 and above): Choose **Require** to encrypt data storage on your devices.

Device Security

- **Block apps from unknown sources**: Choose to **block** devices with "Security > Unknown Sources" enabled sources (supported on Android 4.0 – Android 7.x; not supported by Android 8.0 and later).
- **Company portal app runtime integrity**: Choose **Require** to confirm the Company Portal app meets all the following requirements:
  - Has the default runtime environment installed
  - Is properly signed
  - Isn't in debug-mode
  - Is installed from a known source
- **Block USB debugging on device** (Android 4.2 or later): Choose **Block** to prevent devices from using the USB debugging feature.

When done, select **OK** > **OK** to save your changes.

iOS

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **iOS**. Choose **Settings Configure**, and enter the **Email**, **Device Health**, **Device Properties**, and **System Security** settings. When you're done, select **OK**, and **Create**.

Device health

- **Jailbroken devices**: Block
- **Require the device to be at or under the Device Threat Level** (iOS 8.0 and newer): Choose the maximum threat level to mark devices as noncompliant. Devices that exceed this threat level get marked as noncompliant:
  - **Secured**: This option is the most secure, as the device can't have any threats. If the device is detected as having any level of threats, it is evaluated as noncompliant.

System security

Password

- **Require a password to unlock mobile devices**: **Require** users to enter a password before they can access their device.
- **Simple passwords**: Set to **Block** so users can't create simple passwords, such as **1234** or **1111**.
- **Minimum password length**: 6
- **Required password type**: **Numeric**
- **Maximum minutes of inactivity before password is required**: 10
- **Password expiration (days)**: 60
- **Number of previous passwords to prevent reuse**: 5

Windows

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **Windows Phone 8.1**, **Windows 8.1 and later**, or **Windows 10 and later**. Choose **Settings Configure**, and enter the **Device Health**, **Device Properties**, and **System Security** settings. When you're done, select **OK**, and **Create**.

System security

Password

- **Require a password to unlock mobile devices**: **Require** users to enter a password before they can access their device.
- **Simple passwords**: Set to **Block** so users can't create simple passwords, such as **1234** or **1111**.
- **Minimum password length**: 8
- **Password type**: **Alphanumeric**
    - **Number of non-alphanumeric characters in password**: If **Required password type** is set to **Alphanumeric**, this setting specifies the minimum number of character sets that the password must contain. The four character sets are:
        - Lowercase letters
        - Uppercase letters
        - Symbols
        - Numbers
- **Maximum minutes of inactivity before password is required**: 15
- **Password expiration (days)**: 90
- **Number of previous passwords to prevent reuse**: 5

Encryption

- **Require encryption on mobile device**: **Require**

Windows 10 and later policy settings

Device health

- **Require BitLocker**: Yes
- **Require Secure Boot to be enabled on the device**: Yes

Device properties

- **Minimum OS version**: `Microsoft Windows [Version 10.0.17134.1]`
- **Encryption of data storage on a device**: Choose **Require** to encrypt data storage on your devices.

Device Security

- **Antivirus**: When set to **Require**, you can check compliance using antivirus solutions that are registered with Windows Security Center, such as Symantec and Windows Defender.
- **AntiSpyware**: When set to **Require**, you can check compliance using antispyware solutions that are registered with Windows Security Center, such as Symantec and Windows Defender.

Windows Defender ATP

- **Require the device to be at or under the machine risk score**: Use this setting to take the risk assessment from your defense threat services as a condition for compliance. Choose the maximum allowed threat level:
    - **Medium**: The device is evaluated as compliant if existing threats on the device are low or medium level. If the device is detected to have high-level threats, it is determined to be noncompliant.