Use compliance policies to set rules for devices you manage with Intune

03/04/2025

Microsoft Intune compliance policies are sets of rules and conditions that you use to evaluate the configuration of your managed devices. These policies can help you secure organizational data and resources from devices that don't meet those configuration requirements. Managed devices must satisfy the conditions you set in your policies to be considered compliant by Intune.

If you also integrate the compliance results from your policies with Microsoft Entra Conditional Access, you can benefit from an extra layer of security. Conditional Access can enforce Microsoft Entra access controls based on a devices current compliance status to help ensure that only devices that are compliant are permitted to access corporate resources.

Intune compliance policies are divided into two areas:

- Compliance policy settings are tenant-wide configurations that act like a built-in compliance policy that every device receives. Compliance policy settings establish how compliance policy works in your Intune environment, including how to treat devices that aren't assigned an explicit device compliance policy.
- Device compliance policies are discrete sets of platform-specific rules and settings you deploy to groups of users or devices. Devices evaluate the rules in the policy to report a device compliance status. A noncompliant status can result in one or more actions for noncompliance. Microsoft Entra Conditional Access policies can also use that status to block access to organizational resources from that device.

Compliance policy settings

Compliance policy settings are tenant-wide settings that determine how Intune's compliance service interacts with your devices. These settings are distinct from the settings you configure in a device compliance policy.

To manage the compliance policy settings, sign in to Microsoft Intune admin center and go to **Endpoint security** > **Device compliance** > **Compliance policy settings**.

Compliance policy settings include the following settings:

- **Mark devices with no compliance policy assigned as**

This setting determines how Intune treats devices that aren't assigned a device compliance policy. This setting has two values:

- **Compliant** (*default*): This security feature is off. Devices that aren't sent a device compliance policy are considered *compliant*.
- **Not compliant**: This security feature is on. Devices without a device compliance policy are considered noncompliant.

If you use Conditional Access with your device compliance policies, change this setting to **Not compliant** to ensure that only devices that are confirmed as compliant can access your resources.

If an end user isn't compliant because a policy isn't assigned to them, then the Company Portal app shows No compliance policies have been assigned.

- **Compliance status validity period (days)**

  Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.

  By default, the period is set to 30 days. You can configure a period from 1 to 120 days.

  You can view details about a devices compliance to the validity period setting. Sign in to Microsoft Intune admin center and go to **Devices** > **Monitor** > **Setting compliance**. This setting has a name of **Is active** in the *Setting* column. For more information about this and related compliance status views, see Monitor device compliance.

Device compliance policies

Intune device compliance policies are discrete sets of platform-specific rules and settings you deploy to groups of users or devices. Use compliance policies to:

- Define the rules and settings that users and managed devices must meet to be compliant. Examples of rules include requiring devices run a minimum OS version, not being jail-broken or rooted, and being at or under a *threat level* as specified by threat management software that integrates with Intune.
- Support actions for noncompliance that apply to devices that don't meet that policies compliance rules. Examples of actions for noncompliance include marking the device as

noncompliant, being remotely locked, and sending a device user email about the device status so they can fix it.

When using device compliance policies:

- Some compliance policy configurations can override the configuration of settings that you also manage through device configuration policies. To learn more about conflict resolution for policies, see Compliance and device configuration policies that conflict.
- Policies can deploy to users in user groups or devices in device groups. When a compliance policy is deployed to a user, all the user's devices are checked for compliance. Using device groups in this scenario helps with compliance reporting.
- If you use Microsoft Entra Conditional Access, your Conditional Access policies can use the device compliance results to block access to resources from noncompliant devices.
- Like other Intune policies, compliance policy evaluations for a device depend on when the device checks in with Intune, and policy and profile refresh cycles.

The available settings you can specify in a device compliance policy depend on the platform type you select when you create a policy. Different device platforms support different settings, and each platform type requires a separate policy.

The following subjects link to dedicated articles for different aspects of device configuration policy.

- **Actions for noncompliance** - By default, each device compliance policy includes the action to mark a device as noncompliant if it fails to meet a policy rule. Each policy can support more actions based on the device platform. Examples of extra action include:
  - **Sending email alerts** to users and groups with details about the noncompliant device. You might configure the policy to send an email immediately upon being marked as noncompliant, and then again, periodically, until the device becomes compliant.
  - **Remotely lock devices** that have been noncompliant for some time.
  - **Retire devices** after they've been noncompliant for some time. This action marks a qualifying device as ready to be retired. An admin can then view a list of devices marked for retirement and must take an explicit action to retire one or more devices. Retiring a device removes the device from Intune management and removes all company data from the device. For more information about this action, see Available actions for noncompliance.

- **Create a compliance policy** – With the information in the linked article, you can review prerequisites, work through the options to configure rules, specify actions for noncompliance, and assign the policy to groups. This article also includes information about policy refresh times.

  View the device compliance settings for the different device platforms:
  - Android device administrator
  - Android Enterprise
  - Android Open Source Project (AOSP)
  - iOS
  - Linux
  - macOS
  - Windows Holographic for Business
  - Windows 10/11
  - Windows 8.1 and later

  > **Important**
  >
  > On October 22, 2022, Microsoft Intune ended support for devices running Windows 8.1. Technical assistance and automatic updates on these devices aren't available.
  >
  > If you currently use Windows 8.1, then move to Windows 10/11 devices. Microsoft Intune has built-in security and device features that manage Windows 10/11 client devices.

- **Custom compliance settings** – With custom compliance settings you can expand on Intune's built-in device compliance options. Custom settings provide flexibility to base compliance on the settings that are available on a device without having to wait for Intune to add those settings.

  You can use custom compliance settings with the following platforms:
  - Linux – Ubuntu Desktop, version 20.04 LTS and 22.04 LTS
  - Windows 10
  - Windows 11

Monitor compliance status

Intune includes a device compliance dashboard that you use to monitor the compliance status of devices, and to drill-in to policies and devices for more information. To learn more about this dashboard, see Monitor device compliance.

Integrate with Conditional Access

When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies.

When a device enrolls in Intune it registers in Microsoft Entra ID. The compliance status for devices is reported to Microsoft Entra ID. If your Conditional Access policies have Access controls set to *Require device to be marked as compliant*, Conditional Access uses that compliance status to determine whether to grant or block access to email and other organization resources.

If you use device compliance status with Conditional Access policies, review how your tenant configures the *Mark devices with no compliance policy assigned as* option, which you manage under Compliance policy settings.

For more information about using Conditional Access with your device compliance policies, see Device-based Conditional Access.

Learn more about Conditional Access in the Microsoft Entra documentation:

- What is Conditional Access
- What is a device identity

Reference for noncompliance and Conditional Access on the different platforms

The following table describes how noncompliant settings are managed when a compliance policy is used with a Conditional Access policy.

- **Remediated**: The device operating system enforces compliance. For example, the user is forced to set a PIN.

- **Quarantined**: The device operating system doesn't enforce compliance. For example, Android and Android Enterprise devices don't force the user to encrypt the device. When the device isn't compliant, the following actions take place:

- If a Conditional Access policy applies to the user, the device is blocked.
- The Company Portal app notifies the user about any compliance problems.

Expand table

Policy setting	Platform
Allowed Distros	**Linux** *(only)* - Quarantined
Device encryption	- **Android 4.0 and later**: Quarantined - **Samsung Knox Standard 4.0 and later**: Quarantined - **Android Enterprise**: Quarantined - **iOS 8.0 and later**: Remediated (by setting PIN) - **macOS 10.11 and later**: Quarantined - **Linux**: Quarantined - **Windows 10/11**: Quarantined
Email profile	- **Android 4.0 and later**: Not applicable - **Samsung Knox Standard 4.0 and later**: Not applicable - **Android Enterprise**: Not applicable - **iOS 8.0 and later**: Quarantined - **macOS 10.11 and later**: Quarantined - **Linux**: Not applicable - **Windows 10/11**: Not applicable
Jailbroken or rooted device	- **Android 4.0 and later**: Quarantined (not a setting) - **Samsung Knox Standard 4.0 and later**: Quarantined (not a setting) - **Android Enterprise**: Quarantined (not a setting) - **iOS 8.0 and later**: Quarantined (not a setting) - **macOS 10.11 and later**: Not applicable - **Linux**: Not applicable - **Windows 10/11**: Not applicable
Maximum OS version	- **Android 4.0 and later**: Quarantined - **Samsung Knox Standard 4.0 and later**: Quarantined - **Android Enterprise**: Quarantined

Policy setting	Platform
	- **iOS 8.0 and later**: Quarantined - **macOS 10.11 and later**: Quarantined - **Linux**: See *Allowed Distros* - **Windows 10/11**: Quarantined
Minimum OS version	- **Android 4.0 and later**: Quarantined - **Samsung Knox Standard 4.0 and later**: Quarantined - **Android Enterprise**: Quarantined - **iOS 8.0 and later**: Quarantined - **macOS 10.11 and later**: Quarantined - **Linux**: See *Allowed Distros* - **Windows 10/11**: Quarantined
PIN or password configuration	- **Android 4.0 and later**: Quarantined - **Samsung Knox Standard 4.0 and later**: Quarantined - **Android Enterprise**: Quarantined - **iOS 8.0 and later**: Remediated - **macOS 10.11 and later**: Remediated - **Linux**: Quarantined - **Windows 10/11**: Remediated
Windows health attestation	- **Android 4.0 and later**: Not applicable - **Samsung Knox Standard 4.0 and later**: Not applicable - **Android Enterprise**: Not applicable - **iOS 8.0 and later**: Not applicable - **macOS 10.11 and later**: Not applicable - **Linux**: Not applicable - **Windows 10/11**: Quarantined

> ⓘ **Note**

The Company Portal app enters the enrollment remediation flow when the user signs into the app and the device has not successfully checked in with Intune for 30 days or more (or the device is non-compliant due to a *Lost contact* compliance reason). In this flow, we attempt to initiate a check-in one more time. If that still does not succeed, we issue a retire command to allow the user to re-enroll the device manually.

Next steps

- Create and deploy policy and review prerequisites
- Monitor device compliance
- Common questions, issues, and resolutions with device policies and profiles in Microsoft Intune
- Reference for policy entities has information about the Intune Data Warehouse policy entities