Policy enforcement rules

If a device or work profile fails to comply with any of the policy settings listed below, Android Device Policy immediately blocks usage of the device or work profile by default:

- **Password requirements**
- **Encryption policy**
- **Keyguard disabled**
- **Permitted input methods**
- **Permitted accessibility services**

If the device or work profile remains not compliant after 10 days, Android Device Policy will factory-reset the device or delete the work profile.

In this section you can override the default compliance enforcement rules or add new ones.

Rules

List of rules that define the behavior when a particular policy can not be applied on device.

Setting name

The top-level policy to enforce. For example, **Applications** or **Password requirements**.

Block after days

Number of days the policy is non-compliant before the device or work profile is blocked. To block access immediately, set to 0. **Block after days** must be less than **Wipe after days**.

Block scope

Specifies the scope of block action. Only applicable to devices that are company-owned.

> **Work profile**: Block action is only applied to apps in the work profile. Apps in the personal profile are unaffected.
>
> **Entire device**: Block action is applied to the entire device, including apps in the personal profile.

Wipe after days

Number of days the policy is non-compliant before the device or work profile is wiped.
Wipe after days must be greater than **Block after days**.

Preserve factory-reset protection

Whether the factory-reset protection data is preserved on the device. This setting doesn’t apply to work profiles.

Revision #2
Created 30 March 2022 09:35:31 by Admin
Updated 21 March 2023 13:03:02 by Admin