Compliance rules

The **Compliance rules** section of the Apple Policy Editor sets requirements for the devices of the policy. A device that breaks a rule is non-compliant at once: the device page shows why, in **Why the device is non-compliant**, and the devices list shows it as non-compliant. A device is also non-compliant when a setting of the policy can't be applied on it.

Rules

- **Passcode**: the device has a passcode, and it meets the passcode settings of the policy.
- **Minimum OS version**: for iPhone and iPad, or for Mac. To update the devices, add a required update in Software updates.
- **Supervised device**: devices enrolled with the enrollment profile or with User Enrollment aren't supervised.
- **FileVault on (Mac)**: the disk of the Mac is encrypted with FileVault. Other devices aren't affected.

A rule is checked when the device sends its status, when the policy is saved, and every hour. A device whose status is unknown (for example a Mac that didn't report FileVault yet) doesn't break the rule.

Blocking the device

Turn on **Block the device if it's still non-compliant** and set after how many days (0 blocks at once). Supervised iPhone and iPad go into lost mode with the message you set. The other devices are locked once; a Mac restarts and asks for a PIN, shown in the details of the command in the command history.

- **Unblock**: when the device is compliant again, lost mode is turned off automatically.
- **Turning lost mode off yourself**: the device isn't blocked again until it becomes compliant and breaks a rule again. Use it to let the user fix the device.

> To be notified, or to react in other ways, create an event rule for **Device becomes non-compliant**: it also gets the reasons.

Revision #7
Created 2026-11-10 15:12:16 UTC by Admin
Updated 2026-11-12 09:51:59 UTC by Admin