Apple policies

Apple policies define management settings that Cerberus Enterprise applies to Apple devices via MDM. These settings are configured from the dashboard in the Apple policy editor.

Before you start

Apple device management requires Apple Management (APNs) to be configured. If needed, read the Apple Management setup (APNs) page.

Open the Apple Policy Editor

In the dashboard, open **Policies** and click **Create new Apple policy**. To edit an existing Apple policy, click its row in the policies table.

Editor layout

The Apple Policy Editor is organized as a set of expandable sections. At the top of the page you can always edit:

- **Name** (required)
- **Id** (read-only)
- **Description** (optional)

Policy sections

The sections below match the panels currently available in the Apple Policy Editor. When you open a saved policy, the sections with changed settings are already open and the others stay closed:

- **App management**: configure app-related restrictions, managed apps and the Cerberus Enterprise app settings.
- **Kiosk and Home Screen**: Single App Mode, allowed and blocked apps, Home Screen layout, web clips, notification settings and Lock Screen message.

- **Security**: control features such as Auto Unlock and biometric unlocking.
- **Passcode settings**: configure passcode requirements and related rules.
- **Multimedia**: allow/disallow camera and related features.
- **Cellular**: control cellular-related settings (app cellular data settings, eSIM, plan changes), and the cellular APN.
- **Networking**: Wi-Fi networks (also enterprise 802.1X), VPNs, certificates, global proxy, encrypted DNS and web content filter, and connectivity restrictions such as AirDrop and Bluetooth.
- **System and user interface**: restrict system features such as Handoff, the device name and the screen saver.
- **Software updates**: require an OS version by a deadline and control how updates are downloaded and installed.
- **macOS**: firewall, Gatekeeper, screen saver and lock, external and network storage, Screen Sharing, privacy permissions and login items of the Macs.
- **Apple apps and services**: restrict Apple apps and services such as iMessage, Game Center and Find My.
- **Siri and Apple Intelligence**: restrict Siri, dictation and the Apple Intelligence features.
- **iCloud**: allow or disallow specific iCloud services (backup, keychain sync, private relay, etc.).
- **Location and geofences**: areas where iPhones and iPads with the Cerberus Enterprise app report when they enter or leave, for event rules.
- **Accounts**: restrict account modification and configure Mail, Exchange, Google, calendar, contacts and directory accounts.
- **Compliance rules**: requirements (passcode, minimum OS version, supervision, FileVault) that make devices non-compliant, with an optional block.

> Many options in the Apple Policy Editor include a tooltip that documents requirements and supported OS versions.

Save, delete, and associated devices

Use **Save policy** to apply your changes. The button is disabled when there are no pending edits, or when the license is expired.

When editing an existing policy, the page also shows a **Delete policy** action. The editor can show an **Associated devices** list at the bottom, so you can see how many devices are currently using the policy.

Next pages

- Apps & profiles: configure installed apps and configuration profiles.
- Kiosk and Home Screen: Single App Mode, allowed apps, Home Screen layout and web clips.
- Passcode: configure passcode requirements and related security options.
- Restrictions: define allowed features and OS-level limitations.
- Networking: Wi-Fi networks, VPNs, certificates and connectivity restrictions.
- Software updates: required OS updates and software update settings.
- macOS: firewall, Gatekeeper, screen lock, storage, privacy permissions and login items of the Macs.
- Location and geofences: areas that iPhones and iPads report entering and leaving, and what they need to work.
- Accounts: mail, Exchange, Google, calendar, contacts and directory accounts.
- Compliance rules: requirements for the devices and blocking non-compliant devices.

Revision #60
Created 2026-01-15 15:41:15 UTC by Admin
Updated 2026-11-12 09:51:57 UTC by Admin