macOS

The **macOS** section of the Apple Policy Editor manages the security, privacy and login settings of the Macs: FileVault, firewall, Gatekeeper, screen saver and lock, external and network storage, Screen Sharing, privacy permissions, login items, and the system and kernel extensions allowed to load. It also installs configuration files of system services and background tasks. The other devices of the policy don't get these settings. Turn on a setting to manage it; while it's off, the users keep their own choices.

> Most settings are installed on the Mac as configuration profiles, visible in System Settings > General > Device Management. FileVault, privacy permissions, login items and the extension settings need user-approved MDM: on a Mac enrolled with the enrollment URL or QR code, the user approves the enrollment profile in System Settings. The device page shows it in the **User-approved MDM** field. When the user approves it later, the Mac gets these settings automatically.

FileVault

FileVault encrypts the disk of the Mac. With this setting on, users are asked to turn on FileVault with their password, and the Mac sends its personal recovery key to Cerberus Enterprise, encrypted with a key that belongs to your organization only. The key is shown and changed from the **FileVault** field of the device page (see Device commands). The setting needs macOS 13 or later and user-approved MDM; without user-approved MDM the Mac isn't asked to turn on FileVault, but if a user turns it on, its key is stored.

- **Required at login**: at the next login, after a number of skips (the user is asked again at each login and at logout), or only when the user logs out.
- **Don't ask at logout**: the user is asked only at login. It can't be combined with "Only asked at logout".
- **Show the recovery key to the user**: off by default, so only the administrators know the key, from the device page.
- **Prevent turning off FileVault**: on by default.
- **Remove the key from memory on standby**: the user types the password again when the Mac wakes from standby.
- **Where the key is kept**: text shown to the user at the login window, for example who to call to recover the Mac (default "Cerberus Enterprise").

>

> A Mac that was already encrypted when it got the setting keeps its current key, which Cerberus Enterprise doesn't receive: the key is stored only after the user turns FileVault off and on again (with "Prevent turning off FileVault" off). Turning the setting off, or removing the Mac from management, doesn't turn off FileVault, and the stored key keeps working. The setting can't be saved when the server isn't configured to store recovery keys.

Firewall

- **Turn on the firewall**: when it's off, the firewall stays off and users can't turn it on.
- **Block all incoming connections**: only the basic network services (DHCP, Bonjour, IPSec) can receive connections.
- **Stealth mode**: the Mac doesn't answer ping requests and connections to closed ports.
- **Allow built-in software** and **Allow downloaded signed apps** to receive connections without asking the user (macOS 12.3 or later).
- **Rules for specific apps**: allow or block the incoming connections of an app, by bundle ID.

Gatekeeper

Gatekeeper checks the apps before they open. Choose whether the Macs open only App Store apps, or also the apps of identified developers. With Gatekeeper off, any app can be opened, also unsigned or damaged ones. On macOS 15 or later you can also choose whether users are asked to send blocked malware to Apple.

Screen saver and lock

Start the screen saver after a time of inactivity, and ask for the password when the screen saver starts or the display sleeps, at once or after a delay. A setting left as **Not managed** stays the user's choice.

External and network storage

Allow, make read only or block the external storage (USB drives, SD cards, external disks) and the network storage (file shares) of the Macs. Needs macOS 15 or later.

Screen Sharing

Limits of the people who connect to these Macs with Screen Sharing: copying files from or to the Mac, high-performance connections and the number of virtual displays. Turning on Screen Sharing stays a choice of the user. Needs macOS 14 or later.

Privacy permissions

Give or deny apps the access that users would otherwise allow in System Settings > Privacy and Security, for example Full Disk Access for a backup app, or deny the camera to an app. For each permission choose:

- **Permission**: Full Disk Access, Accessibility, Automation, the folders, contacts, calendars, photos, camera, microphone, screen recording and the others of Privacy and Security.
- **Access**: allow or deny. The camera, the microphone, screen recording and input monitoring can't be allowed by a profile, only denied; for screen recording and input monitoring you can let users allow them also without admin rights.
- **App**: the bundle ID of an app, or the path of a program (for example a command line tool).
- **Code requirement**: identifies the app by its signature. Get it in Terminal with `codesign -dr - /Applications/Example.app` and copy the text after `designated =>`.
- **Automation** also needs the controlled app (for example the Finder) and its code requirement.

Login and background items

The login items and background items that match the rules are managed: they run without asking, and users can't turn them off in System Settings > General > Login Items. A rule matches the developer team ID of an app, its bundle ID or the label of a launch daemon or agent (also by their first part). Needs macOS 13 or later.

System extensions

System extensions are the modern way for apps to extend macOS: network filters and VPNs, endpoint security agents and drivers. With this setting on, the system extensions of the listed developer teams load without asking the user. Needs macOS 10.15 or later and user-approved MDM.

- **Team ID**: the 10-character team ID of the developer (for example in the "Signed by" details of the app, or with `codesign -dv`). Each team can appear only once.
- **Allow**: every extension of the team, or only the extensions with the listed bundle IDs.
- **Types**: limits the team to drivers, network or endpoint security extensions. With none chosen, all types are allowed.
- **Removal** (only for listed extensions): the app can remove its extension without an administrator (macOS 12 and later), the extension can't be turned off or removed while System Integrity Protection is on, or it can't be removed in System Settings and the Finder (macOS 15 and later). Macs with an older macOS still allow the extension, without the removal option.
- **Users can approve other system extensions**: on by default. When off, only the extensions allowed by a profile can load; if any profile on the Mac turns it off, it's off.

> On macOS 11.3 and later, removing this setting turns off the system extensions it allowed, for example a security agent or a network filter. This happens when the setting is turned off, when the policy is deleted, and when the Mac moves to a policy without it. The editor asks for confirmation before turning the setting off.

Kernel extensions (legacy)

Kernel extensions are the older, deprecated way to extend macOS: prefer system extensions when the vendor offers them. The kernel extensions of the listed teams (every extension of a team, or only the listed bundle IDs) load without asking the user, after a restart. Needs macOS 10.13.2 or later and user-approved MDM.

- **Users can approve other kernel extensions**: off by default, so only the listed teams can load kernel extensions.
- **Standard users can approve them too**: with user approvals on, users without administrator rights can approve them too (macOS 11 and later).

> On Macs with Apple silicon, a profile alone isn't enough: someone must start the Mac in recoveryOS, choose Reduced Security in Startup Security Utility and allow the user management of kernel extensions from identified developers. The Mac may also need a Bootstrap Token escrowed in Cerberus Enterprise to approve them (see the Bootstrap Token field of the device page).

Mac files

The service configuration files and the background tasks use files that you upload to the **Mac files** of your organization: zip archives and property lists (.plist) up to 20 MB. Upload, check where they are used or delete them with the **Mac files** button of the macOS section, or with **Choose file** in a setting. A file used by a policy can't be deleted. To change a file, upload the new version and choose it in the policy: the Macs download it again.

Service configuration files

Installs the configuration files of a system service from a zip archive. The built-in services are the SSH server (sshd), sudo, PAM, printing (CUPS), the Apache web server, bash, zsh, smart card login and authorization. You can also use your own service, with a reverse DNS identifier like `com.example.service`: it finds the files with the managed configuration files library of macOS. Each service can have one setting. Needs macOS 14 or later.

> A built-in service uses only the files of the archive and ignores its own files, for example /etc/ssh for sshd: put the whole configuration in the archive, in folders that start from the root of the disk (for example `etc/ssh/sshd_config`). The files are read-only on the Mac, and they are removed with the setting. Test the archive on one Mac first: a wrong sudo or PAM configuration can stop users from signing in or from using administrator rights.

Background tasks

Programs and scripts that run in the background, started by launchd. Users can't turn them off, and they are removed with the setting. Needs macOS 15 or later. For each task choose:

- **Task identifier**: a reverse DNS identifier, like `com.example.task`, different for each task.
- **Programs and scripts** (optional): a zip archive that the Mac unpacks in `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` followed by the task identifier. Keep the execute permission of the files, and don't put property lists in it.
- **launchd property lists**: the jobs that start the programs, loaded as a daemon (for the whole system, as root) or as an agent (in each user session). Refer to the programs with their path in the folder above.

A task needs the programs or at least one property list. When the files change, the Macs restart the task.

Revision #7
Created 2026-11-10 15:12:14 UTC by Admin
Updated 2026-11-12 09:51:57 UTC by Admin