Commands

The device page provides a **Commands** panel to send remote commands to a managed device. Available commands depend on the platform (Android or Apple) and device state.

Commands can be sent only to a device that is currently enrolled. On a disenrolled device, on an ADE device that hasn't enrolled yet and on the historical record of a past enrollment, the panel shows only the command history.

> If the device is not currently online, the command will be delivered and executed as soon as the device connects to the Internet. For Android commands you can set the **Validity** parameter to determine for how long an undelivered command remains valid.

Android (AMAPI) commands

For Android devices, the Commands panel includes a **Validity** field (value + unit) and a **Command** selector. Some commands require additional parameters, which appear dynamically when you select the command.

Common parameters

- **Validity**: how long the command is valid if it cannot be executed immediately.
- **Command**: choose which action to send to the device.

Commands without additional fields

- **Lock device**: locks the device.
- **Restart device**: restarts the device. Requires Android 7.0 or later.
- **Disable lost mode**: takes the device out of lost mode.
- **Relinquish ownership**: removes the work profile and all policies from a company-owned device with Android 8.0 or later, and leaves it for personal use. Apps and data of the personal profile are kept. The device is deleted from the server after it acknowledges the command. This can't be undone.

Commands with additional fields

- **Reset password**: requires **New password** and **Confirm new password**. Optional toggles include **Lock now**, **Require entry**, and **Do not ask for credentials on boot**.
- **Clear app data**: requires the target **Package name**.
- **Enable lost mode**: requires a **Lost mode message** and supports optional contact fields (street address, organization, phone number, email). When the device reports it, its state becomes **Lost**, the device page shows a banner and this command is hidden until lost mode is disabled.
- **Erase device**: supports a **Wipe reason message** (shown to users on personal devices) and optional wipe flags, including **Wipe eSIMs**.

> The eSIM commands (**Add eSIM**, **Remove eSIM**, **Request EID**) are available in the dedicated **SIMs management** panel.

Command history

Below the send controls, the dashboard shows a command history table. The table is sortable and supports pagination. Some rows can be expanded to view additional parameters or execution details.

Android history columns

- **Creation date**
- **Command**
- **Validity**
- **Status**
- **Error**
- **Execution date**

Apple (MDM) commands

For Apple devices, the Commands panel provides a **Command** selector. Some commands require additional inputs. As with Android, a command history table is shown below.

Commands with additional fields

- **Install app**: requires the application **Bundle ID**.
- **Send notification**: requires a **Notification message** (maximum length 200 characters).

On iPhones and iPads, **Send notification** and live tracking reach the device through the **Cerberus Enterprise** app: they are disabled until the app is installed and has registered for notifications (see

the **Cerberus Enterprise app** field). Starting live tracking shows "Live tracking request sent to the device": tracking starts when the device sends its first location. iOS can delay the request or not deliver it, for example in Low Power Mode or without a network connection: if no location arrives within 2 minutes, ask the user to open the app once. When a request fails, the message gives the reason, for example the app hasn't registered yet, the server notification key is missing, or the device's notification token is no longer valid.

Device actions

Only the commands supported by the device are listed: some need a supervised iPhone or iPad, others aren't available on a Mac. The disruptive ones ask for a confirmation.

- **Lock device**: locks the screen, with an optional message and phone number. A Mac is restarted and locked with a six-digit PIN, shown once after sending the command and in the command details. iPhone shows the title "Lost iPhone" above your message, even though this command doesn't enable lost mode.
- **Enable lost mode** (supervised iPhone and iPad): locks the device and shows your message, phone number and footnote on the Lock Screen. While lost mode is on, the page shows a banner and the commands **Locate device** (the location appears on the Location map), **Play sound** and **Disable lost mode**.
- The device tells whoever is holding it that it was located: after **Locate device**, the Lock Screen shows **iPhone Located** with the time and the name of the server that received the location, and a **Continue** button. iOS shows this notice and it can't be turned off.
- **Clear passcode**: removes the passcode of an iPhone or iPad, for example when the user forgot it. If the policy requires a passcode, the user is asked to set a new one.
- **Refresh device information**: asks the device for its information (supervision, OS version, security status, MDM certificate) and its inventory.
- **Device settings**: opens a window to change the device name, the host name of a Mac, Bluetooth, data roaming, Personal Hotspot, time zone, wallpaper, whether Activation Lock is allowed and, on a Shared iPad, its settings (see below). Only the settings you change are sent; the ones the device doesn't support are disabled with the reason. A device can acknowledge data roaming or Personal Hotspot without applying them (for example when the SIM plan has no Personal Hotspot), so Cerberus Enterprise reads them back about 30 seconds later and writes a warning in the system logs if they didn't change.
- **Restart device** and **Shut down device**: restart or turn off the device right away, after a confirmation.
- **Erase device**: erases all content and settings and removes the device from management. On iPhone and iPad you can keep the eSIM data plan and skip proximity setup; a Mac gets a six-digit PIN.
- **Return to Service** (option of **Erase device**, iPhone and iPad with iOS 17 or later): after the erase the device sets itself up again, without anyone touching it, and enrolls again with its current policy, user and ownership. Choose a Wi-Fi network of the device policy for the setup, unless the device has Ethernet or cellular data: only personal networks (with a password, without certificates) can be used, because the device has no user or certificate

yet. Activation Lock must be off.

- **Refresh cellular plans** (iPhone and cellular iPad, iOS 13 or later, not User Enrollment): enter the **Carrier eSIM server URL** given by the carrier (an https:// address, a host name or an LPA activation code, of which only the server is used) and the device downloads the eSIM plans that the carrier bound to its EID. The device EID is shown under the field to send it to the carrier. See the **SIMs management** page.
- **Keep the eSIM data plan** turned off removes all the eSIMs with the erase. The policy restriction **Keep the eSIM when the device is erased** (supervised devices, iOS 17.2 or later) applies to erases started on the device (too many failed passcode attempts, Erase All Content and Settings): Apple doesn't document its effect on this command.
- **Log out user** (Shared iPad): logs out the current user and goes back to the login screen. The data not synced to iCloud yet stays on the iPad.

Shared iPad

A Shared iPad is used by several people, each with their own Managed Apple Account, or by guests with temporary sessions. It's set up with an ADE profile that enables Shared iPad (see the **Apple Automated Device Enrollment** page), and its **Enrollment type** field shows **Shared iPad**.

- **Shared iPad users**: the users of the iPad, with the user logged in, the storage they use and whether some data isn't synced to iCloud yet. Use **Refresh** to ask the iPad for the list again. A user can be deleted with their data, except the user logged in (log them out first); **Delete all users** needs iPadOS 14 or later. When the data isn't synced yet, the confirmation warns that it will be lost.
- **Device settings**: the storage for each user, the expected number of users, the inactivity time after which users and guest sessions are logged out, guest sessions only, the Managed Apple Account domains suggested on the login screen, how many days a user can sign in without checking the password online, and skipping the language and region setup for new users. Empty fields keep their current value; the settings that need a newer iPadOS are disabled.

Mac users

On a Mac, the **Mac users** panel lists the users enrolled in the management, usually the user who enrolled the Mac. The accounts of the policy are installed in their sessions. For each user it shows when they were enrolled, the last report of their session and the state of the accounts: **Up to date**, **Waiting for the user** (the Mac installs them when the user is logged in), **Not applied** with the reasons reported by the Mac, or **No accounts** when the policy has none. Use **Reload** to read the list again.

Activation Lock

The **Activation Lock** field shows whether Activation Lock is on. When it's on, an erased device can be set up again only with the user's Apple Account or with the device's bypass code. Supervised devices turn on Activation Lock only if it's allowed in **Device settings**. Cerberus Enterprise asks supervised devices for their bypass code and stores it: use **Show bypass code** in the field menu to see it (only administrators can, and each view is recorded in the system log), then enter it as the password on the Activation Lock screen of the device, leaving the Apple Account empty.

Recovery Lock and firmware password (Mac)

A Mac with Apple silicon shows the **Recovery Lock** field, an Intel-based Mac the **Firmware password** field. Both protect the Mac at startup: with Recovery Lock, recoveryOS asks for the password; with a firmware password, the Mac asks for it to start from another disk or from recovery. The field shows whether the Mac reports a password and, in its tooltip, when Cerberus Enterprise stored it and when it was last verified.

- **Set or change password**: Cerberus Enterprise generates a password of 20 letters that are on the same keys with any keyboard layout, or an administrator types one (8 to 64 characters without accents; other roles can only generate one, because they can't see stored passwords). The password is stored encrypted before it's sent, and replaces the stored one only when the Mac confirms it. If the Mac already has a password set outside Cerberus Enterprise, type it as the current password: it's used once and not stored.
- **Verify password**: asks the Mac whether the stored password is correct. The result is in the tooltip and in the system log.
- **Show password**: only administrators can see the stored password, and each view is recorded in the system log. Generated passwords are shown in groups of four letters: type them without spaces.
- **Clear password**: removes the password from the Mac.

An Intel-based Mac restarts to apply a firmware password change: until then the previous password is still needed (Show password lists it), and another change can't be sent. Apple also accepts only one firmware password command every 30 seconds. The passwords are hidden in the command history.

When a Mac leaves management (disenrolled, removed by the user or erased), macOS removes Recovery Lock by itself and Cerberus Enterprise drops the stored Recovery Lock password; it does the same when the Mac reports that it has no Recovery Lock, for example after it enrolls again. When you disenroll a Mac (or delete its policy), a stored firmware password is cleared first, the Mac restarts and then leaves management. If the clear fails, the Mac leaves management anyway and the password stays stored so you can still see it. A Mac removed from management by the user, or erased, keeps its firmware password: Cerberus Enterprise keeps it too. Deleting the device record deletes the stored password, so you're asked to confirm it first: write the password down, because without it only Apple can remove it.

FileVault (Mac)

The **FileVault** field shows whether the disk of the Mac is encrypted and, in its tooltip, whether Cerberus Enterprise stores its personal recovery key. A Mac sends the key when FileVault is turned on after it gets the FileVault setting of its policy (see the **macOS** page of Apple policies).

- **Show recovery key**: only administrators can see the key, and each view is recorded in the system log. Use it at the login window of the Mac to reset the user's password, or in recovery to unlock the disk. It stays available after the Mac leaves management; deleting the device record deletes it.
- **Change recovery key**: the Mac replaces its personal recovery key and sends the new one, encrypted; the old key stops working. It's possible only when the stored key can be read: the Mac is unlocked with it, and no user password is needed. The stored key is hidden in the command history and removed from the server once the Mac answers (or after 7 days without an answer).

Bootstrap Token (Mac)

A Mac with macOS 10.15 or later sends its **Bootstrap Token** to the management server when a user with a secure token logs in. The server keeps it and gives it back only to that Mac, which uses it to give new users a secure token and, on a Mac with Apple silicon, to install software updates and approve kernel extensions without asking for an administrator password. Nobody can see the token, in the dashboard or elsewhere. The **Bootstrap Token** field shows its state:

- **Escrowed**: the server has the token; the tooltip shows when the Mac sent it.
- **Escrowed earlier**: the stored token was sent before the latest enrollment or MDM certificate renewal of the Mac. After a renewal this is expected: the token is kept and the Mac doesn't send it again. After a new enrollment it may no longer be valid: run `sudo profiles install -type bootstraptoken` in Terminal on the Mac.
- **Not escrowed**: the Mac hasn't sent a token yet. To send it now, an administrator of the Mac runs `sudo profiles install -type bootstraptoken` in Terminal (`sudo profiles status -type bootstraptoken` shows whether it's escrowed).

The tooltip also tells whether the Mac allows the token for authentication. Macs set up with Automated Device Enrollment allow it automatically; on other Macs with Apple silicon a user can allow it in Startup Security Utility in recoveryOS. Intel Macs can't use the token for authentication (**Not supported**), but an escrowed token still gives new users a secure token. Each time a Mac sends, removes or asks for its token, it's recorded in the system log.

Device status and OS updates

The **Device status** panel shows what the device reports about itself: the OS version and build, the progress of a software update (pending version, deadline, what started it, failures), whether a passcode is set and complies with the policy, FileVault on a Mac, the battery health and the accounts configured on the device.

The **Available updates** list shows the OS updates the device can install, collected at enrollment and weekly. Use **Check for updates** to request it now, and **Install** to install an update right away (the device restarts, after a confirmation) or only download it and let the user install it. This works on supervised iPhones and iPads and on Macs, up to iOS, iPadOS and macOS 26: on later versions, and to update many devices, use the required updates of the policy (see the **Software updates** page of Apple policies).

A Mac with Apple silicon installs an update without asking for an administrator password only when it allows its Bootstrap Token for authentication and the token is escrowed (see Bootstrap Token above). Otherwise the confirmation says that a user may have to enter an administrator password before the update installs.

Applications and inventory

The **Applications** panel lists every app of the device in one table. The installation state of the apps installed by the policy or with a command is reported live by the device; versions, sizes and the apps installed by the user come from the last app list, collected at enrollment and weekly. Use **Ask the device** to request it now.

- **Management**: **Policy** for apps installed by the device policy, **Managed** for apps installed with a command such as **Install app**, **Not managed** for the ones installed by the user. The Cerberus Enterprise app has the **Installed by Cerberus** chip.
- **Needs attention**: apps that failed to install, were declined or removed by the user, or wait for the user. Open a row to see the error; failed policy apps can be installed again with the retry button. Built-in apps and App Store apps that the device reports as not validated aren't counted.
- **Remove app**: managed apps can be removed, with their data. To remove an app installed by the policy, remove it from the policy. The policy also sends this command itself when a Mac package installed as a managed app is removed from the policy.

The **Profiles, certificates and security** panel shows the configuration profiles, the certificates and the security status (passcode, encryption, FileVault and firewall on a Mac) reported by the device.

> On personally-owned devices the apps installed by the user aren't collected, and only the profiles and certificates managed by Cerberus Enterprise are listed.

The **Inventory changes** panel shows what changed between two lists sent by the device: apps installed, removed or updated (with the old and new version), profiles installed, removed or

updated, and certificates added or removed. A change is detected when the device sends a new list, weekly for apps and profiles, daily for certificates, or when you use **Ask the device**: the date shown is when it was detected, the change happened between the previous list and that one. The first list of a device, and the first one after a new enrollment or an ownership change, is only recorded as the starting point. Search by name or identifier, and filter by kind and change. Changes are kept for 365 days.

> When an OS update replaces many Apple apps at once, they are shown as one line (for example "23 Apple apps updated") that you can expand. A renewal of the MDM certificate is shown as **MDM certificate renewed**. On personally-owned devices only the changes of the items managed by Cerberus Enterprise are shown.

Apple history columns

- **Creation date**
- **Command**
- **Status**: **Sent** (waiting for the device, delivered as soon as it connects), **Success**, **Answered** (open the row to see the result), **Waiting for the device** (the device can't run the command right now), **Failed** (open the row to see the reason) or **Cancelled** (the command queue of the device was cleared, for example when it enrolled again).
- **Execution date**

Refresh

Use the refresh action in the Commands panel to reload the command history.

Revision #76
Created 2022-03-11 15:26:56 UTC by Admin
Updated 2026-11-12 09:52:13 UTC by Admin