Device Status

- Device overview
- Location map
- SIMs management
- Commands

Device overview

Open a device from **Dashboard → Devices** by clicking the device row. The page title shows the device **Model** (when available) and the internal **Id**.

Historical data vs current enrollment

When a device has multiple enrollments, Cerberus Enterprise can show a read-only historical record. In that case, the page displays a **Historical data** banner and a button to return to the current enrollment data.

Top fields

The top section summarizes the device identity, assignment, and management state. Some fields are platform-specific and appear only for Android or Apple devices.

- **Id** and **Model**: read-only identifiers.
- **User**: shows the currently assigned user (if any). From the user menu you can **Open user** or **Change user**, or assign a user when none is set.
- **Management mode** and **Ownership**: displayed with tooltips in the UI.
- **State**: current device state (with icon and tooltip details). A device in lost mode shows **Lost** on both Android and Apple, and a banner at the top of the page says what to do next.
- **ADE profile** (Apple only): shows the assigned Automated Device Enrollment profile (if any) and lets you open or change it.
- **Policy**: shows the assigned policy and lets you open or change it, or assign one when none is set.
- **Policy compliance status** (when a policy is assigned): indicates whether the device is compliant.
- **Policy version** (when a policy is assigned): indicates whether the device has the latest policy version applied.
- **Cerberus Enterprise app** (iPhone and iPad only): the state of the Cerberus Enterprise app that Cerberus installs on the device. **Not available** (iOS or iPadOS older than 18.4, no serial number on a company device, or no Managed Apple Account on a personal device); **Not available on personal devices yet**; **Waiting for device information**; **Waiting**

for the user license of the Managed Apple Account (personal devices, while Apple confirms the license); **Not installed** (the app isn't in your Apple Business library or Apps and Books isn't set up, with a link to **Account settings**); **Installed · Apps and Books needs attention** (the token expired or the app left your library: the app stays installed); **Configuration unavailable**; **Installing…** (if the device sends no status report for 30 minutes, the tooltip suggests checking that it's online and restarting it, which usually starts the installation again); **Waiting for the user to approve**; **The user declined** and **Install failed** (both with **Retry**, which asks the device again); **Installed · waiting for the app to start** (the app hasn't been opened yet); **Installed · configuration not accepted**; and, once the app has registered, its version, its last contact and whether notifications are on.
- **Enrolled on** and **Last status report**: timestamps for enrollment and last reported status.
- **Disenrolled on**: shown when the device has been disenrolled.

> Some data and panels are available only when the corresponding category is enabled in the device policy. For more information read the **Status reporting** and **Location and geofences** pages.

Panels

The device page is organized in expandable sections. Depending on platform and state, you may see one or more of the following panels:

- **Location map**: a tabbed panel with **Location** history for the current device and, on Android devices, iPhones and iPads, a **Geofence** tab for geofence transitions.
- **SIMs management**: device EID and installed SIMs and eSIMs. On Android also the eSIM commands and their history; on company-owned iPhones and cellular iPads also data roaming, Personal Hotspot and **Refresh cellular plans**. See the dedicated **SIMs management** page.
- **Commands**: send commands to the device and view command history (platform-specific).
- **Security posture**: the security state of the device and its risks. On Android also the Play Integrity verdict. Until the device reports it, it says **Unspecified**, or **Not reported yet** on an Android device that hasn't sent any security data.
- **Why the device is non-compliant**: shown only when the device is non-compliant, with a red alert icon; open it to see the reasons. On Android it lists the policy settings that are out of compliance; on Apple it also says whether a compliance rule blocked the device.
- **Device status** (Apple only): OS version, software update progress, passcode, FileVault, battery and accounts reported by the device, and the OS updates available for it. See the

Commands page.

- **Applications** (Android): installed apps and their feedback and error reports.
- **Applications** (Apple only): the apps installed by the policy, the apps installed with commands and the apps installed by the user, with their installation state, errors and actions (retry, remove). On Macs it also lists the packages installed by the policy, with their state and **Install again**; packages installed as managed apps have a **Managed** chip, and a note tells when a package was installed unmanaged and why, or when its app wasn't found an hour after the download. On iPhones and iPads the Cerberus Enterprise app has the **Installed by Cerberus** chip; it isn't listed under the **Policy** filter. An app whose managed configuration the device didn't accept has the **Configuration not accepted** chip. On personal iPhones and iPads (User Enrollment) a line shows the Managed Apple Account whose user licenses the App Store apps use, the apps waiting for their license show **Waiting for a user license** or **User license failed**, an app whose install prompt the user cancelled shows **Waiting for the user to approve the installation**, and **Request again** asks Apple for the license again or shows the prompt again. See the **Commands** page.
- **Profiles, certificates and security** (Apple only): configuration profiles, certificates and security status reported by the device.
- **Inventory changes** (Apple only): a timeline of the apps, profiles and certificates installed, removed or updated on the device, searchable and filtered by kind and change. See the **Commands** page.
- **Shared iPad users** and **Mac users** (Apple only): the users of a Shared iPad and the users of a Mac. See the **Commands** page.
- **Status reports**: additional data reported by the device, displayed as a tree of categories and values.
- **Enrollment history**: previous enrollments for this same physical device, shown as a list.

Location panel tabs

The **Location map** panel uses tabs to keep location history and geofence transitions separate.

- **Location**: shows history filters, a date-range search, location markers, the accuracy circle, and live tracking controls for the current device.
- **Geofence** (Android, iPhone and iPad): shows geofence transition history on a dedicated map, with period filters, an optional archived-geofence toggle, and a side list of transitions. On iPhones and iPads a status line also tells when geofencing can't work on the device.

For the full behavior of these tabs, see **Location map**.

Actions

At the bottom of the page you can refresh data and perform actions depending on the platform, device state, and license status.

- **Refresh data**: reload the device record.
- **Disable device** / **Enable device** (Android only): available in supported states.
- **Disenroll device**: removes management from the device. The exact behavior depends on platform and ownership (for example, Android may wipe a work profile or factory reset).
- **Delete device**: available when the device is already disenrolled and its record can be removed.

Location map

This page documents the device-specific location tools available in **Device overview**. The panel contains a **Location** tab for position history and, on Android devices, iPhones and iPads, a **Geofence** tab for geofence transitions.

Prerequisites

On Android, device location data is shown only when location reporting is enabled in the device policy. To enable it, open the policy and turn on **Location and geofences** → **Report location**. For more details, see **Location and geofences**.

On iPhones and iPads, the location comes from the Cerberus Enterprise app, once the user allows it, or from the **Locate device** command while the device is in lost mode. Macs and other Apple devices don't report their location.

> On devices that are not fully managed, location data may still depend on the Cerberus Enterprise app having the required location permissions and on location services being enabled on the device.

> On personal devices (User Enrollment), location and geofences are available only when the Apple policy has **Location and geofences on personal devices** on, and only if the user allows location for the Cerberus Enterprise app. Otherwise their device page doesn't show the location actions or live tracking. Lost Mode is never available on personal devices.

> For the global multi-device map available from the dashboard, see **Dashboard location map**.

Loading and no-data state

- While location data is loading, the panel shows a loading overlay on the map.
- If the device has no location data available, the panel shows a message stating **No location data available**. On Android it adds a reminder to enable location reporting in

the assigned policy, when it's off. On Apple it says where the location comes from, or that this type of device doesn't report it.
- If a date filter is active and no samples match it, the panel shows **No data available in the selected date range**.

Location tab

Open the **Location** tab to inspect the history for a single device. The available filters include the last known location, recent history ranges, a custom date range, and live tracking.

- **Last**: shows the last known location.
- **Today**, **Last 7 days**, and **Last 30 days**: show recorded locations for the selected period.
- **Search**: lets you choose a custom date range.
- **Live**: starts or stops live tracking for the current device.

> Locations are kept for **90 days**: older ones are deleted automatically every night. The latest location of each enrolled device is always kept, so the device stays on the maps even when it hasn't reported for a long time. For removed devices and past enrollments, the locations older than 90 days are all deleted. For this reason the **Search** date range can't start more than 90 days ago.

Marker details

When you click a location marker, an information window opens with:

- The timestamp of the location record.
- The reported **accuracy** (in meters).
- The reported **speed**, when the device provides it.
- The reported **heading** or bearing, when the device provides it.

Accuracy circle

When the information window is open, an accuracy circle is displayed around the marker. The circle radius corresponds to the reported accuracy (in meters). Closing the information window hides the circle.

Live tracking

In the device history view, selecting the **Live** filter starts a real-time tracking request for that specific device. Cerberus Enterprise asks for confirmation before starting the request.

- Live tracking runs for up to **15 minutes**.
- While live tracking is active, Android devices show a notification and iPhones and iPads show the location indicator.
- While live tracking is active, the panel keeps refreshing the latest location and the live indicator stays visible.
- Selecting the live filter again lets you stop live tracking before the timeout ends.
- On **iPhone and iPad**, live tracking runs through the Cerberus Enterprise app, with location access set to **Always**. The request normally wakes the app even when it isn't open, and the app then sends locations for the whole session. iOS doesn't guarantee these requests: it can delay them or not deliver them, for example in Low Power Mode or without a network connection. If no location arrives within 2 minutes, the dashboard cancels the request: ask the user to open the app once, then try again.

Geofence tab

On Android devices, iPhones and iPads, the second tab shows geofence transitions generated from the geofences defined in the assigned policy.

- The map shows the current geofence areas together with the recorded transition points.
- The transition list on the right lets you inspect **enter** and **exit** events.
- The available filters are **Today**, **Last 7 days**, **Last 30 days**, and a custom date-range search.
- **Include archived** also shows transitions related to old geofence definitions that are no longer present in the current policy.
- Geofence transitions are kept for **90 days** and older ones are deleted automatically every night, so the custom date-range search can't start more than 90 days ago.

On iPhones and iPads, when the policy has active geofences, a status line at the top of the tab shows whether geofencing works on the device. It tells you when it can't work: the Cerberus Enterprise app hasn't contacted the server or must be updated, location access isn't set to **Always**, **Precise Location** or **Background App Refresh** is off, **Low Power Mode** was on when the app last reported its settings (geofence events and changes can then be delayed by hours), or the app hasn't applied the latest geofences yet. When everything works, it shows how many geofences the app monitors.

Geofence transition details

Selecting a transition opens its details on the map and highlights the corresponding list entry. When available, Cerberus Enterprise also shows the device coordinates and reported accuracy for that transition.

SIMs management

The device page provides a **SIMs management** panel. On Android devices it manages the SIMs and eSIM profiles installed on the device, adds or removes eSIM profiles and shows the history of the eSIM commands sent to the device. On company-owned iPhones and cellular iPads it shows the SIMs and eSIM plans reported by the device and lets the device download the eSIM plans prepared by the carrier: see **iPhone and iPad** below.

> SIM information is reported by fully managed devices when **Network info** reporting is enabled in the device policy (this option is always enabled by Cerberus Enterprise). See the **Status reporting** page.

Device EID

The EID (eUICC Identifier) identifies the eSIM hardware of the device. Carriers use it to bind eSIM profiles to the device, so retrieving it is usually the first step of an eSIM provisioning workflow.

- **Company-owned devices** (Android 13 and above): the EID is reported automatically with the device status and no user interaction is required.
- **Personally-owned devices** (Android 13 and above): use the **Request EID** button. The user will see a notification on the device asking to share the EID, and can approve or decline the request. The EID is shown only if the user approves. While the request is pending, the button remains disabled.

> Sending an EID request shows a confirmation dialog first, because the user will see a notification on the device.

Installed SIMs

The **Installed SIMs** table lists the SIMs currently known for the device, including physical SIMs and eSIM profiles. On personally-owned devices, eSIM profiles installed with the **Add eSIM** command are shown even when the device does not report SIM information.

- **Carrier**: the carrier name associated with the SIM (when reported).
- **Phone number**: the phone number associated with the SIM (when reported).
- **ICCID**: the Integrated Circuit Card Identifier of the SIM.

- **Activation state**: whether the eSIM is activated or not. Reported only for eSIMs on Android 15 and above.
- **Configuration mode**: whether the eSIM was configured by an administrator or by the user. Reported only for eSIMs on Android 15 and above.
- **SIM type**: shows whether the device reports the entry as an eSIM.

> eSIMs with an ongoing or executed (not failed) removal command show a temporary **Removing** activation state. The entry disappears from the list when the device reports the updated SIM list. While a removal is in progress, the remove button is not available, to avoid sending the same command twice.

Remove eSIM

Use the remove button next to an installed eSIM to remove its profile from the device. A confirmation dialog asks you to confirm the ICCID of the eSIM to be removed before the command is sent. Removing an eSIM is supported on Android 15 and above.

Add eSIM

The **Add eSIM** section installs a new eSIM profile on the device (supported on Android 15 and above). It requires:

- **Validity**: how long the command is valid if it cannot be executed immediately.
- **Activation code**: the activation code for the eSIM profile, provided by the carrier. You can enter the full code, or only the SM-DP+ address to let the device discover a profile the carrier already linked to its EID.
- **Activation state**: whether the eSIM profile should be activated automatically after download, or left not activated for manual activation by the user.

Command history

Below the Add eSIM section, the panel shows the history of the eSIM commands sent to the device: **Add eSIM**, **Remove eSIM**, and **Request EID**. The table is sortable and supports pagination. Some rows can be expanded to view the command parameters (for example the activation code or the ICCID) and the execution status, including the eSIM error details when an operation fails on the device.

- **Creation date**
- **Command**

- **Validity**
- **Status**
- **Error**: shows the eSIM error status (for example *User denied*, *Invalid activation code*, or *ICCID not found*) when the command execution reports it.
- **Execution date**

Wipe eSIMs on wipe and disenroll

When you wipe the device from the Commands panel, the **Wipe eSIMs** flag controls whether eSIM profiles are removed with the wipe. On personally-owned devices with a work profile this flag is enabled by default (managed eSIMs are removed, personally-owned eSIMs are not affected). The same flag is available in the **Disenroll device** confirmation dialog.

iPhone and iPad

The panel is shown for iPhones and for iPads that reported cellular data (a Wi-Fi-only iPad has none), only when the device is company-owned and isn't a User Enrollment. The device is asked for its cellular information with the device information: at enrollment, every day, with **Refresh device information**, when its ownership becomes company-owned, and a few minutes after **Refresh cellular plans**.

- **Device EID**: the EID reported with the SIMs, with a button to copy it for the carrier. If the device doesn't report it, the user finds it in Settings > General > About.
- **Reported**, **Data roaming**, **Personal Hotspot** and **Modem firmware**: when the device answered and the state it reported. Data roaming and Personal Hotspot can be changed with **Device settings** in the Commands panel, which shows the current state too.
- **SIMs**: one row per SIM or eSIM plan (dual SIM devices have two), with the slot as reported by the device, its label and its type (**eSIM** when the device reports the EID with it, **SIM card** otherwise), the carrier (the home carrier in a tooltip when the device is roaming on another network), phone number, ICCID, EID, IMEI, the SIM used for data and for calls, and roaming. An eSIM slot without a plan is shown greyed as **No plan**.
- **This device reported no SIM** means the device answered without any SIM; **No cellular information yet** means it hasn't answered yet: use **Refresh device information**.

> Phone numbers, ICCID, IMEI and EID identify the person and the line: they're never asked to personally-owned devices or User Enrollments. When a device becomes personally-owned, the information is removed at once and hidden in the results of the old device information commands in the command history. It isn't exported and isn't written in the system logs.

Refresh cellular plans

iPhone and iPad can't install an eSIM from an activation code. The carrier binds (reserves) the eSIM plan to the EID of the device on its eSIM server (SM-DP+) and gives you the address of that server; **Refresh cellular plans** then asks the device to download the plans waiting for it. The **Refresh cellular plans** button of the panel selects the command in the Commands panel, where you enter the **Carrier eSIM server URL**:

- **An https:// address**, sent as it is. Addresses with http://, a user name or password, or a # part aren't accepted.
- **A host name**, for example *smdp.carrier.example*, sent as https://smdp.carrier.example.
- **An LPA activation code** (LPA:1$server$code, the text of an eSIM QR code): only the server is used, because the command can't carry the code. The plan must be bound to the device EID by the carrier, otherwise the device finds nothing to download.

The device installs and activates the plan without asking the user, also when it isn't supervised. Success in the command history means the device accepted the request, not that a plan was installed: installing can take up to three minutes, and Cerberus Enterprise asks the device for its SIMs again about three minutes later, so the new plan appears in the panel. The errors 36001 (the device couldn't reach its cellular system), 36002 (no eSIM support) and 36003 (cellular system busy, try again later) are explained in the system logs. A plan downloaded once can't be downloaded again: if the installation fails, contact the carrier. The command is also available for several devices at once in the **Apple device actions** menu of the Devices page.

What Apple doesn't allow

- **Add eSIM** from an activation code: not possible, use **Refresh cellular plans** with a plan bound to the EID.
- **Remove eSIM**: an eSIM can't be removed remotely one at a time. Erasing the device with **Keep the eSIM data plan** off removes all eSIMs. To stop a single plan, ask the carrier to deactivate it: the plan stays on the device but can't connect.
- **Request EID**: not needed, the EID comes with the SIMs of company-owned devices.
- **Macs** have no cellular or eSIM management.

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.