Devices

The **Devices** section of the dashboard (*Dashboard → Devices*) lists all enrolled devices in your account. From this page, you can filter the list, open a device record, and perform device actions such as disabling or disenrolling.

Filters

At the top of the page you can enable one or more filters using the chip list. Selected chips represent the currently active filters.

The filters depend on the platforms set up in your account: filters for Apple or Android devices appear only when that platform is set up, and the Android and Apple filters appear only when both are.

Available filters

- **All**: show all devices.
- **Enrolled**: show enrolled devices, whatever their state (for example Active, Lost or Disabled). Disenrolled devices and ADE devices that haven't enrolled yet aren't shown. It's selected when the page opens: choose All to see disenrolled devices and devices synced from Apple Business that haven't enrolled yet.
- **Non-compliant**: show devices that are not policy-compliant.
- **Not secure**: show devices with a non-secure posture.
- **Apps error**: show Android devices whose apps have sent error feedback, and Apple devices with managed apps that need attention (failed to install, declined or removed by the user, or waiting for the user).
- **Lost**: show devices in lost mode, on Android and Apple. Their state is shown as Lost.
- **Status not updated**: show devices that have not reported status in the last 72 hours.
- **Policy not updated**: show devices that have pending policy changes.
- **MDM certificate expiring**: show Apple devices whose MDM certificate expired or expires within 14 days.
- **Android**: show Android devices only.
- **Apple**: show Apple devices only.
- **iPhone**, **iPad**, **Mac**: show these Apple devices only. You can select more than one.
- **Company-owned**: show company-owned devices only.
- **Personally-owned**: show personally-owned devices only.
- **Device owner**: show Android fully-managed devices only.

- **Profile owner**: show Android work profile devices only.
- **Supervised** / **Not supervised**: show Apple devices that are supervised, or that aren't.
- **Search**: enable a text search field.

Search

When you enable the **Search** filter, a text field appears with the label **Id, model, user, serial or OS**: it searches the device id, model, user name, serial number and OS version. The list is updated automatically after you stop typing.

Device table

Devices are displayed in a sortable, paginated table. Clicking a row opens the device editor.

Columns

- **Model**: device model.
- **User**: associated user (name, email, or id depending on availability).
- **State**: device state (with tooltip details).
- **Compliance**: compliance status indicator.
- **Security**: security posture (with tooltip details). On Apple devices: **At risk** without passcode, and on Macs with FileVault or secure boot off; **Potentially compromised** on Macs with System Integrity Protection or the signed system volume off. The device page lists the risks. Apple doesn't report jailbroken iPhones and iPads to device management.
- **Apps error**: apps error indicator.
- **Last status report**: most recent status report timestamp (when available).
- **Policy**: currently assigned policy.
- **OS**: operating system and version (for example iOS 17.7 or Android 14). Sorting orders by system, then by version.
- **Ownership**: company-owned or personally-owned (with tooltip details).
- **Management mode**: management mode (with tooltip details).
- **Id**: internal device identifier.

Refresh and pagination

- Use the refresh action to reload the list.
- The table is paginated (10/25/50 items per page).

Device actions

Each device row can provide actions, depending on the platform and device state. Some actions are disabled when your license is expired or terminated.

Per-device actions

- **Disable device** / **Enable device**: available for Android devices in supported states.
- **Disenroll device**: removes management. On Android this can wipe the work profile or factory reset (depending on ownership); on Apple this removes policy settings.
- **Delete device**: available for devices that were already disenrolled (removes the record from the system). A Mac whose firmware password is still stored in Cerberus Enterprise is deleted only after a confirmation, because the password is deleted with it.

Multi-row selection

You can enable multi-row selection from the action bar below the table. When enabled, you can select multiple rows and apply bulk actions (disable, enable, disenroll, or delete), depending on which devices are selected.

For Apple devices, the **Apple device actions** menu locks, restarts, shuts down, refreshes the information of or erases all the selected devices. An action is available when every selected device is an enrolled Apple device that supports it. The PINs of the Macs that are locked or erased are shown once after the command is sent. Disenrolling Apple devices removes their enrollment profile and policy settings, without erasing them.

Refresh cellular plans asks the selected iPhones and iPads to download the eSIM plans that the carrier bound to their EIDs, from one carrier eSIM server entered in a window for all of them. Unlike the other actions, it's sent only to the selected devices that support it: Macs, User Enrollments, devices with an older iOS and iPads that never reported cellular data are skipped and listed in the result. See the **SIMs management** page.

Apple Business sync

If Apple Management is configured and an Automated Device Enrollment token is present, the page may show the **Sync from Apple Business** action to import devices from Apple Business. A message says how many devices were added. When some were added, the list switches to the **All** filter, because devices that haven't enrolled yet aren't shown by the **Enrolled** filter.

Enroll a device

Use **Enroll a device** to open the Enrollment tokens section and start enrolling a new device.

Revision #58
Created 2026-01-16 17:47:44 UTC by Admin
Updated 2026-11-12 09:52:11 UTC by Admin