Apps & profiles

This section documents how to configure managed applications and account payloads for Apple devices.

App management

The **App management** panel contains both general app-related restrictions and a list of managed apps.

General app restrictions

- **Allow app clips**
- **Allow app installation**
- **Allow app removal**
- **Allow automatic app downloads**
- **Allow apps to be hidden**
- **Allow apps to be locked**
- **Allow In-App Purchases**
- **Allow default browser modification**
- **Allow enterprise app trust**

Managed apps

Use **Add application** to add an app to the policy. Each managed app is displayed as a card. You can expand the card to edit its settings and remove the app using the delete action.

- **App Store ID**: the App Store identifier of the managed app.
- **Bundle ID**: the app bundle identifier.
- **Install behavior**: controls whether the app must remain installed or can be installed/removed by the user.
- **Assignment**: the license type, chosen by Cerberus for each device: a device license on company devices, a user license of the Managed Apple Account on personal iPhones and iPads (User Enrollment). The field can't be changed.
- **VPP license**: VPP license type used for installation through the App Store.

The app selection list shows the available and total licenses of each app. Free apps show **Unlimited**: Apple gives them unlimited licenses. An app can be added to a policy only once: an

app with the same App Store ID or bundle ID as an app already in the policy is refused, and so is a policy that lists the same app twice when you save it.

The app selection list shows the apps of your Apple Business library. To add an app, in Apple Business open **Apps & Services** → **Apps & Books** → **App Store**, search for the app and click **View**. For a free app, click **Add**, select **All current and future** (or the organizational unit of your Apps and Books token) in **Organizational Units**, click **Add**, then **Review** and confirm. For a paid app, click its price, choose **Managed Licenses** as **License Type** (redemption codes can't be used by Cerberus Enterprise), select the **Organizational Unit** of your Apps and Books token, enter the number of **Licenses** (up to 1,000 per order), then **Review** and buy. A payment method must be set up first in **Settings** → **Payments & Billing** → **Apps & Services** → **Payment Methods**. The apps then appear in the app selection list.

Apps on personal devices (User Enrollment)

Personal iPhones and iPads enrolled with User Enrollment have no serial number, so they get the App Store apps of the policy with a **user license** of the Managed Apple Account signed in on the device. Cerberus registers the account with Apps and Books and assigns the licenses by itself, free apps included. The Managed Apple Accounts and the Apps and Books token must belong to the same Apple Business organization. A paid app uses one license per account, shared by all the personal devices of that account.

- **Waiting for a user license**: the app is sent to the device only after Apple confirms its license, usually within a few minutes. The **Applications** panel of the device shows the reason.
- **User license failed**: Apple couldn't assign the license, for example because a paid app has no license left. Add licenses in Apple Business, then use **Request again**; Cerberus also tries again by itself every day.
- **Install prompt**: iOS asks the user before installing each app. If the user cancels, the app shows **Waiting for the user to approve the installation**; **Request again** shows the prompt again.
- **Release**: removing the app from the policy, or unenrolling the last personal device of the account, removes the app and releases its license, unless another enrolled device of the same account still needs it.

For the details, see **Apple account-driven enrollment**.

Managed configuration

A managed configuration gives an app its settings (for example a server address or an account name), the way the app's vendor documents them. Open the app in the policy and click **Add**

managed configuration. It's sent to iPhones and iPads with **iOS or iPadOS 18.4 or later** and to Macs with **macOS 27 or later**; it isn't sent to Apple Vision Pro yet. The app must support managed configuration: an app that doesn't read it ignores it. The app panel shows the number of keys next to the app name.

- **Keys**: each row has a key, a type and a value. The types are Text, Integer, Decimal number, Boolean, Date, Text list and Integer list. Keys are case-sensitive and must be unique. **Add key** adds a row; **Remove configuration** removes all the keys.
- **Variables**: Text and Text list values can contain $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ and $UDID$, replaced with the values of each device and of its user. A variable with no value (for example $EMAIL$ on a device without a user) is left empty, and the system logs say so. When a user's details change, the devices get the new values; for users synchronized from Google Directory the values are updated at the next change of the policy or of the device.
- **Import a configuration**: open or paste the file that the app's vendor publishes for MDM, then click **Read**. An **AppConfig specfile** (specfile.xml) lists every key the app supports with its description, type, default value and allowed values: select the keys to import (those with a default value are already selected) and fill in the others after the import. A warning appears when the specfile is for another app. A **property list** (a whole property list or only its <dict>) is imported as it is. Then choose whether to replace the current keys or add to them. Nested dictionaries, data values and lists with mixed or unknown types aren't supported and are listed as skipped. Apple doesn't publish the configuration keys of apps, so ask the vendor for the file when it isn't in their documentation. **Copy as plist** copies the configuration as the device receives it, before the variables are replaced.
- **Limits**: up to 200 keys per app; keys up to 255 characters; text values up to 4,096 characters; lists up to 200 items of up to 1,024 characters each; dates between 1970 and 9999; 64 KB per app in all.
- **Not for passwords**: the configuration is sent only to the device it's built for and the logs show only key names and types, but dashboard administrators can read the values, and the address the device downloads it from changes with the values, so a value that is easy to guess (a boolean or a small number) could be inferred from it. Don't put passwords or other secrets in a managed configuration.
- **Status**: when the device reports that the app didn't accept its configuration, the Applications panel of the device shows **Configuration not accepted** next to the app. It doesn't make the device non-compliant. A configuration that the device can't download does make it non-compliant.

App options

Each app of the policy (App Store and custom apps) has these options. **Device default** leaves the choice to the device. Devices that don't support an option don't get it; the app is still installed.

- **Automatic updates**: App Store setting, Always or Never. iOS, iPadOS, macOS and visionOS 26 or later. For custom apps, App Store setting behaves like Never.

- **Downloads over cellular**: App Store setting, Always or Never, for automatic installs and updates. Supervised iPhones and iPads with iOS or iPadOS 26 or later only.
- **Back up the app data**: whether the app data is included in the device backups. Not on Mac.
- **User can hide the app** and **User can lock the app**: iOS and iPadOS 18.1 or later, enforced on supervised devices. Not allowing locking also prevents hiding. The restrictions **Allow apps to be hidden** and **Allow apps to be locked** apply to all apps.
- **Lock the device after Tap to Pay transactions that need the customer's PIN**: iPhone only.
- **Associated domains**: the domains the app is associated with (for example for universal links or password autofill), up to 50. Enter plain host names such as www.example.com, without applinks:, wildcards or ?mode=. Not on Mac.
- **Verify the domains directly**: the device checks the domains' site association file directly instead of through Apple's servers. Only turn it on for internal domains that can't be reached from the internet.
- **Removal**: apps installed as **Required** can't be removed by the user.

Mac App Store apps

The app selection list shows the platforms of each app (iPhone/iPad, Mac, Apple TV, Vision); an app that exists only for Mac shows its Mac icon. An app that exists only for Mac applies to Macs when you add it. An App Store app without a Mac version isn't sent to Macs: the policy shows "This app has no Mac version: it isn't sent to Macs" under **Applies to**. Macs get App Store apps by their App Store ID, so apps with a different bundle ID on Mac are installed correctly.

Cerberus Enterprise app

Cerberus installs its **Cerberus Enterprise** app on every iPhone and iPad with **iOS or iPadOS 18.4 or later**, with or without a policy. The app shares the device location and receives notifications and live tracking requests. It's installed as **Required**, with a device license from Apps and Books (a user license on personal devices), so the user can't delete it.

- **One-time setup**: add the free app to your library once. In Apple Business, open **Apps & Services** → **Apps & Books** → **App Store**, search for "Cerberus Enterprise", click **View**, then **Add**, select **All current and future** in **Organizational Units**, click **Add**, then **Review** and confirm. If the app shows **Manage**, it's already in your library: open it and check that its organizational units are **All current and future units**. Until then the dashboard shows a banner and the devices show the app as not installed. See **Account settings**.
- **Not in policies**: the app can't be added to a policy. It is disabled in the app selection list and refused as a custom app (same bundle ID). A policy that already lists it gets the entry removed when you open it: save the policy to confirm.

- **Not installed on**: devices with iOS or iPadOS older than 18.4. Shared iPad is supported for the install, but the app features aren't verified there.
- **Personal devices**: on iPhones and iPads enrolled with User Enrollment, the app is installed too, with an install prompt and a user license of the Managed Apple Account. It receives messages from your organization, and it doesn't access the location unless the policy turns on **Location and geofences on personal devices** and the user allows it.
- **Kept installed**: if the Apps and Books token expires or the app leaves your library, the app stays on the devices and the device page says that Apps and Books needs attention. It's removed only if the app is still missing from your library 24 hours later.

Custom apps

Custom apps are your own iPhone and iPad apps (.ipa files), distributed without the App Store. In Xcode, export the app for **Enterprise** distribution (Apple Developer Enterprise Program: it installs on every device) or **Ad Hoc** distribution (it installs only on the devices registered in its provisioning profile). App Store builds can't be uploaded.

Click **Add custom app** to open the custom apps of your organization. **Upload app** adds an .ipa file (up to 2 GB). Select an app and click **Add to the policy**. The list shows the version, the type of signing, the number of devices in the profile of ad hoc apps and the expiry date of the provisioning profile.

- **New version**: upload an app with the same bundle ID. It replaces the previous version, and the devices of the policies that use it update the app.
- **Requirements**: iPhone and iPad with iOS 17.2 or later. Devices that can't install the app don't get it: an iPad-only app on an iPhone, an older iOS than the app needs, a device that isn't in the profile of an ad hoc app, or an expired provisioning profile.
- **Expiry**: when the provisioning profile expires, the app no longer opens. Upload a version signed with a new profile before the expiry date.
- **Reserved bundle ID**: a custom app with the bundle ID of the Cerberus Enterprise app (com.lsdroid.Cerberus.Enterprise) can't be added to a policy, because Cerberus installs that app by itself.
- **Delete**: remove the app from its policies first; the devices then remove it.

Mac packages

The custom apps also accept Mac installer packages (.pkg files). The package must be a distribution package built with **productbuild** (a component package made only with pkgbuild is refused) and signed with a **Developer ID Installer** certificate. Notarizing it and stapling the ticket (**notarytool** and **stapler**) is recommended. Unsigned packages, packages changed after signing and packages signed with other certificates are refused.

Upload the .pkg file with **Upload app** and add it to the policy: it appears under **Mac packages**. iPhones and iPads ignore it.

Macs with **macOS 26 or later** (supervised, which includes Macs enrolled manually, but not User Enrollment) get the package as a **declaration**: the Mac downloads, installs, retries and updates it by itself and reports its state. Older Macs, and packages installed as managed apps, get it with an **MDM command**, on any macOS version. A Mac that is upgraded to macOS 26 moves to the declaration by itself; it may install each package once more. The same can happen when a Mac moves to another policy that has the same package.

- **New version**: upload a package with the same package identifier. It replaces the previous version, and the Macs of the policies that use it install the new one.
- **Skipped Macs**: Macs with an older macOS than the package allows, and Intel Macs for packages built only for Apple silicon. The device page shows the package as Skipped, with the reason; the version installed before stays on the Mac.
- **Install**: **Required** (default) installs the package on the Mac; **Optional** makes the package available on the Mac without installing it. macOS 26 doesn't show optional packages to the user in System Settings or the App Store (tested on macOS 26.3), so an app or a script on the Mac has to install them; choose Optional only if you have one. It applies to Macs with macOS 26 or later; older Macs always install the package. The choice isn't available for packages installed as managed apps.
- **Remove the package files when it leaves the policy (macOS 27 or later)**: when the package is removed from the policy, Macs with macOS 27 or later delete the files it installed. It's off by default. On older Macs the files stay. Not available for packages installed as managed apps.
- **Install as a managed app**: turn it on for a package of the policy to install its app as a managed app (macOS 11 or later, not with user enrollment). macOS then reports when the installation fails, and MDM can remove the app. The app must be installed directly in the Applications folder, signed with a **Developer ID Application** certificate and notarized; on macOS 11 to 13 the package must contain only that app (no other files or scripts). The custom apps show which packages qualify. When the option can't be applied on a Mac, the package is installed there as usual and the device page says why.
- **Removal options** of a managed app: **Remove the app when the package is removed from the policy** (on by default) and **Remove the app when the Mac leaves management**. Removing an app also deletes its data. If the user had already installed the same app, that copy becomes managed and is removed too.
- **Removal**: the MDM command can't uninstall a package. For a package installed as a managed app, removing it from the policy removes the app (when the option is on); its other files and the package receipt stay. Packages with **Remove the package files** on are removed from Macs with macOS 27 or later. Other packages: removing them from the policy only stops new installs, the files stay on the Macs. A Mac that is skipped (for example after a new version that needs a newer macOS) keeps the app while the package is in the policy; removing the package from the policy then removes it too. Remove leftover files on the Mac (for example with the package's own uninstaller), and run `sudo pkgutil --forget <identifier>` to forget the package receipt.
- **State on the device**: the Applications panel of the Mac shows each package of the policy as Queued, Accepted (the Mac accepted the command), Downloaded, Installed (only for packages that contain apps, when the apps are found on the Mac) or Failed (with the

error). macOS doesn't report the installation of a package sent with the command, so Downloaded is the last state for packages without apps. A package installed as a managed app also becomes Failed when macOS reports that the app couldn't be installed or was removed from the Mac. **Install again** sends the package to the Mac again.
- **State with the declaration**: packages delivered as a declaration show the **Declaration** chip and the state the Mac reports: Queued, Available (an optional package the user hasn't installed), Waiting for the user, Downloading, Installing, Installed or Failed (with the reason, for example a failed download or installation, or a declaration the Mac rejected). The **Files removed with the policy** chip marks packages whose files a macOS 27 Mac removes when they leave the policy. **Install again** appears only after a failure and asks the Mac to try again; it isn't offered when the Mac rejected the declaration.

Accounts

The **Accounts** panel lets you configure accounts that are applied to managed devices. It also includes a restriction toggle for account modification.

Restriction

- **Allow account modification**: when disabled, users cannot modify accounts such as Apple Accounts and internet accounts.

Add accounts

Use **Add Google account** or **Add mail account** to add account payloads to the policy. Each account appears as a card with its configuration fields.

Account credentials from users

Both Google and Mail account cards provide a **Account credentials from users** toggle. When enabled, the system applies account credentials on a per-user basis. When disabled, you enter the account identity in the policy.

Google account fields

- **Visible name**: the name shown to the user for the account.
- **Google email address**: the user email address.
- **Full name**: the user’s full name.

Mail account fields

Mail accounts include identity fields plus incoming/outgoing server configuration. Host names are required.

- **Visible name**: the name shown to the user for the mail account.
- **Email address**: the user email address.
- **Full name**: the user's full name.

Incoming server

- **Server type**: mail protocol (for example IMAP or POP).
- **Authentication Method**: authentication method for the server.
- **IMAP path prefix**: shown only when Server type is IMAP.
- **Host name**: required.
- **Port**: server port (1–65535).

Outgoing server

- **Authentication Method**
- **Host name**: required.
- **Port**: server port (1–65535).

S/MIME options

For Mail accounts, you can also configure S/MIME encryption and signing behavior.

Encryption

- **S/MIME encryption**
- **Identity user-overrideable**
- **Per-message switch enabled**
- **User overrideable**

Signing

- **S/MIME Signing**
- **Identity user-overrideable**
- **User overrideable**

> Account and restriction options include tooltips in the dashboard that document prerequisites and supported OS versions.

Revision #60
Created 2026-01-15 15:41:17 UTC by Admin
Updated 2026-11-12 09:52:00 UTC by Admin