Settings

The **Settings** page (*Dashboard → Settings*) summarizes account and license information, and provides actions to manage billing, platform setup (Android Management and Apple Management), and optional directory/token integrations.

License banner (expiring / expired)

When your license is **expiring**, **expired**, or **terminated**, a prominent banner is shown at the top of the page. Depending on your subscription state, it provides either a **Manage billing** action (Stripe customer portal) or a **Buy license** action.

> When the license is expired, the account becomes limited to device disenrolling only. After the grace period, the account may be canceled and devices can be automatically disenrolled.

Apple certificate and token banners (expiring / expired)

The Apple Push Certificate (APNs), the Apple Business token (Automated Device Enrollment) and the Apps and Books token (formerly VPP) must be renewed every year. Starting **30 days before the expiration**, a banner is shown at the top of the dashboard for each certificate or token that is **expiring** or **expired**, with the expiration date or the feature that has stopped working. The **How to renew** action opens this page with the matching renewal instructions expanded.

A banner is also shown when the MDM certificate of some Apple devices expires within 14 days and the automatic renewal hasn't completed, or has expired: those devices must be enrolled again. The **Show devices** action opens the devices list with the **MDM certificate expiring** filter.

> When the Apple Push Certificate expires, Apple devices can't receive commands or policy updates. When the Apple Business token expires, Automated Device Enrollment stops working. When the Apps and Books token expires, apps can't be distributed.

Cerberus Enterprise app banner

Cerberus installs its free **Cerberus Enterprise** app on iPhones and iPads (iOS and iPadOS 18.4 or later) with an Apps and Books device license. A banner is shown at the top of the dashboard when the app isn't in your Apple Business library, when the Apps and Books token is missing or expired, or when some iPhones and iPads are still waiting for the app (with their number). **How to add it** opens this page at the **Cerberus Enterprise app** row with the steps; **How to set it up** (shown when the Apps and Books token is missing or expired) opens the Apps and Books token instructions.

Enterprise manager access

The **Enterprise manager access** card is shown only for enterprises managed by a multi-tenancy account (for example, a managed service provider). It lets you see which manager accounts can operate on your enterprise and control their access.

The card shows:

- The **owner** of the enterprise. The owner always has access and its access can't be revoked.
- Each manager account of the multi-tenancy account, labeled as **Main manager** or **Sub-account**, with its name, username, and access status (**Granted**, **Revoked**, or **Not granted**).

Grant and revoke access

Use **Grant** to allow a manager account to enter and manage your enterprise, and **Revoke** to remove that access. Each action asks for confirmation. A manager whose access is revoked can no longer operate on the enterprise, even if it is currently working on it.

- As the enterprise administrator, you can grant or revoke access for any listed manager account.
- The main manager can grant or revoke access for its own sub-accounts, but only while its own access is granted. It can't grant access to itself, and it can't revoke its own access.

> Revoking access for the **Main manager** also revokes access for all of its sub-accounts. When this applies, the confirmation dialog lists the sub-accounts that will lose access.

Account information

The **Account Information** card shows read-only fields:

- **Username**
- **Enterprise name**
- **Enterprise id**

Change password

If you are not signed in with Google, Apple or Microsoft, the card also shows a **Change password** action. This opens a dialog to continue with the password change flow.

You can also change your password at any time from the user menu in the top toolbar, using **Change password**. This is useful for multi-tenancy accounts, which can change their password without entering an enterprise.

> If an administrator created your account or reset your password, you sign in with a temporary password and must choose a new password before continuing.

License information

The **License Information** card shows the current license state and your device limit. It also provides actions to contact sales and to manage billing or buy a license.

- **License status**: shown as **Active** or **Expired** (with an icon badge and tooltip).
- **Free trial**: shown when the account is currently in trial mode.
- **Licensed devices**: maximum number of devices allowed by the license. The *need more devices?* link opens a message to contact support. Enrolled devices count, whatever their state (for example Active, Lost or Disabled). Disenrolled devices don't, and neither do devices synced from Apple Business until they enroll. When the limit is reached, a new device isn't added and its enrollment is removed: the event is in the system log, and the account administrators get an email. On Apple devices the removal takes about a minute, and a device that's already counted can enroll again, as can one erased with Return to Service.
- **Next scheduled renewal**: shown for active subscriptions that renew automatically. Otherwise the card shows the **Expiration date**.

Android Management

The **Android Management** card shows Android Management status for your enterprise. If Android Management is not configured yet, the card provides a **Setup Android Management** action that opens the setup flow.

Configured state

When Android Management is configured, the card can show:

- **Management id**
- **Binding type**: identifies whether the enterprise uses a **Managed Google Play account** or a **Managed Google domain**.
- **Synced with Google Workspace** (badge shown when directory sync is active)
- **Sync with Google Workspace** (shown when directory sync is not configured; opens the instructions panel at the bottom of the page)

Android enterprise binding

Android Management can be associated with either a **Managed Google Play account** or a **Managed Google domain**. The **Binding type** field shows which option is currently associated with your enterprise.

A **Managed Google Play account** is a lightweight Android Enterprise account. It is suitable for managing Android devices and apps through Cerberus Enterprise, but it is separate from a Google Workspace or Cloud Identity organization. It does not provide the central Google administration experience available with a managed Google domain.

A **Managed Google domain** associates Android Enterprise with your organization’s Google identity. IT administrators can manage Google products such as Google Workspace, Cloud Identity, and Gemini from the Google Admin console, while continuing to manage Android apps and policies in Cerberus Enterprise. This provides a more streamlined, integrated approach to Android management and enables Google Workspace-based enrollment and user-management workflows.

When the enterprise uses a Managed Google Play account, the Settings card provides **Upgrade to managed Google domain** and an information action. The upgrade opens Google’s guided process to move the existing Android enterprise to a managed domain.

> During the upgrade, Google can bind an existing Google Admin account associated with your work email address or create a new free Google Admin account automatically. Use a work

email address such as *name@enterprise.com* to continue through Google's guided setup.

Apple Device Management

The **Apple Device Management** card shows Apple device management (MDM) status for your enterprise. If Apple management is not configured yet, the card provides a **Setup Apple Management** action that opens the setup flow.

Configured state

When Apple management is configured, the card can show:

- **Apple id**
- **Apple Push Certificate expiration**: shows the expiration date and an icon badge. If the certificate is expiring/expired, the badge is clickable and opens renewal instructions.
- **Apple Business token expiration**: shows the expiration of the Apple Business token used for Automated Device Enrollment (with a clickable badge when action is required).
- **Apps and Books token**: shows organization name and expiration for the Apple Apps and Books content token, formerly Volume Purchase Program (VPP) (with a clickable badge when action is required).
- **Cerberus Enterprise app**: on the Apps and Books token card, shows whether the app is in your Apple Business library: **In your library (unlimited licenses)**, **Not in your library** or **Not available: the Apps and Books token expired**, and how many iPhones and iPads are waiting for it. When the app is missing, the row lists the steps to add it (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). **Check again** reads the library again (at most every 5 minutes); the devices waiting for the app then get it.
- **Apple Business**: link to the Apple Business portal, shown when an Apple Business token is present.
- **Sync with Apple Business** and **Sync with Apple Apps and Books**: shown when tokens are missing.

Apple management requires the APNs certificate setup. If needed, see **Apple Management setup (APNs)**.

Preferences & Privacy

The **Preferences & Privacy** card contains a marketing preference toggle and links to the Terms of Service and Privacy Policy. Use **Save preferences** to apply changes (a progress indicator is shown while saving).

Send feedback

When subscriptions are enabled for the account, the page can show a **Send feedback** card with links to: **Make a feature request** and external review platforms.

Inline setup and renewal instructions

At the bottom of the page, the dashboard can show expandable instruction panels depending on the current state (for example when a certificate/token is missing or expiring).

Renew Apple Push Certificate (APNs)

When the APNs certificate is expiring or expired, the page shows a panel with steps to download a CSR, renew the certificate on Apple’s portal, and upload the new certificate into Cerberus Enterprise.

> While a certificate or token is still valid, the upload button next to it opens the same steps. Use it when you downloaded a new Apple Business or Apps and Books token, because the old one stops working, or to renew the Apple Push Certificate early. Always renew the current Apple Push Certificate: a different one is refused while Apple devices are enrolled, because they couldn't be reached anymore.

Sync with Apple Business

When the Apple Business token is missing, expired, or expiring, the page shows a panel with the steps to download a token from Apple Business and upload it into Cerberus Enterprise. For a new connection, generate the public key certificate in Cerberus Enterprise, then in Apple Business open **Devices** → **Management Services**, click **Add** under **Device Management Services**, choose **Connect external device management** and click **Continue**; enter a **Service Name** (for example Cerberus Enterprise), upload the certificate with **Upload Certificate**, click **Next**, then **Download Service Token** and **Done**. To renew the token, select the Cerberus Enterprise service

in **Management Services**, click the **…** (more) button at the top right and choose **Download Token**.

> Devices are enrolled with Cerberus Enterprise only when they are assigned to its service in Apple Business: open **Devices → Management Services → Default Device Assignment** to assign new devices automatically (per device type), or **Devices → Inventory**, select the devices and click **Assign Device Management**.

Sync with Apple Apps and Books (VPP)

When the Apps and Books token is missing, expired, or expiring, the page shows a panel with the steps to download a content token from Apple Business and upload it into Cerberus Enterprise: in Apple Business, open the organization menu at the top right (your organization name) → **Settings → Organizational Units**, select the organizational unit (the default unit is your organization) and click **Download** in the **Content Token** section. The token expires after one year, or earlier when the password of the Apple Account that downloaded it changes.

The last step of the Apps and Books setup adds the free Cerberus Enterprise app to your Apple Business library, so Cerberus can install it on your iPhones and iPads.

Sync with Google Workspace

When Google Workspace directory sync is not configured, the page shows a panel that explains the integration and provides an authorization button. It also lists the required Google OAuth scope: **https://www.googleapis.com/auth/admin.directory.user.readonly**.

> For initial Android setup, see **Android Management setup**.

Revision #57
Created 2026-01-16 17:47:52 UTC by Admin
Updated 2026-11-12 09:52:20 UTC by Admin