Apple account-driven enrollment

With account-driven enrollment, users enroll their iPhone, iPad or Mac by signing in with their work account (a **Managed Apple Account**, for example *name@company.com*) in the device settings. No profile to download and no QR code: Cerberus Enterprise finds the user, applies the policy and sets the ownership by itself.

Two modes

- **User Enrollment** (personal devices): only the work apps, accounts and data are managed, in a separate area of the device. Cerberus can't see personal data, erase the device, locate it or read its serial number. The device is set as personally-owned. Needs iOS and iPadOS 15 or macOS 14 or later.
- **Device Enrollment** (company devices that aren't in Apple Business): the whole device is managed, like with a manual enrollment. A Mac enrolled this way is supervised; an iPhone or iPad isn't. The device is set as company-owned. Needs iOS and iPadOS 17.1 or macOS 14.1 or later.

> You choose the mode for iPhone and iPad and, separately, for Mac: for example User Enrollment for personal iPhones and Device Enrollment for Macs. You can change the ownership of a device later on the device page.

> Account-driven enrollment is available when Apple Management (APNs) is configured. If you have not completed APNs setup yet, read **Apple Management setup (APNs)**.

Set up Apple Business

Users sign in with Managed Apple Accounts, which are created in Apple Business. Before you start:

1. **Verify your domain** (for example *company.com*) in Apple Business, in the domains of your organization.

2. **Create the Managed Apple Accounts** of your users, or connect Apple Business to Google Workspace or Microsoft Entra ID: then the account of each user is their work e-mail address and they sign in with its password.
3. For User Enrollment, check in the access management settings that Managed Apple Accounts can sign in on **personal devices**: when they can sign in only on supervised devices, User Enrollment fails.
4. Only for the **Apple Business** option below: open **Devices** → **Management Services** → **Default Device Assignment** (Edit) and choose the Cerberus Enterprise device management service for iPhone, iPad and Mac.

> Keep the Cerberus Enterprise device management service and its token in Apple Business while devices are enrolled with Managed Apple Accounts: removing them can stop the accounts from working on the devices.

Set up Cerberus Enterprise

Open the **Enrollment** section of the dashboard and select the **Apple account sign-in** tab. A checklist at the top shows what is still missing. Only administrators can change the settings.

- **Allow enrollment by signing in with a work account**: turns account-driven enrollment on or off for the whole organization.
- **Domains**: the domains of your users' accounts (for example *company.com*), up to 20. Only accounts of these domains can enroll, and only after the domain is verified (see below).
- **iPhone and iPad** and **Mac**: Off, User Enrollment or Device Enrollment for each device family.
- **Policy** of each mode: applied to the devices as soon as they enroll. Without a policy, the devices enroll without one. A changed policy applies to the next enrollments.
- **Users**: *Only existing users* (the e-mail address of a user in Cerberus Enterprise must match the account typed on the device), or *Create a user for accounts of the domains that don't have one*.

> The account typed on the device is matched with the **Managed Apple Account** field of the users, then with their e-mail address. The code is always sent to the e-mail address of the user. A Managed Apple Account set on a user can enroll even when its domain isn't verified in Cerberus, for example an account of the reserved *org.appleid.com* domain of Apple Business. With Apple Business service discovery users always type their Managed Apple Account.

Verify the domains

After you save the settings, the **Domain verification** section shows a TXT record for each domain. Add it to the DNS of the domain, then click **Verify**. DNS changes can take some time to be visible. A verified domain stays verified: you can remove the record afterwards. Users of a domain that isn't verified can't enroll.

Service discovery: how devices find Cerberus Enterprise

When a user signs in, the device asks the domain of the account (for example *https://company.com*) which server manages it. Set up at least one of these three options. The **Service discovery** section of the tab shows the discovery URL of your organization and the exact text to copy for each option.

Option 1: Apple Business (recommended)

Click **Register in Apple Business**: Cerberus Enterprise stores its discovery URL in your Apple Business organization and nothing has to be published on your domains. **Check in Apple Business** shows the URL Apple Business has now, and **Remove from Apple Business** removes it.

- Needs iOS and iPadOS 18.2 or macOS 15.2 or later. Older devices need option 2 or 3.
- Needs Apple Business connected in Cerberus Enterprise (Automated Device Enrollment service token), and the default device assignment described above.
- The device asks Apple Business only when your domain doesn't answer: the address *https://company.com/.well-known/com.apple.remotemanagement* must not exist (an error such as "not found"). If your web site answers it with a web page, devices stop there. Use **Check configuration** to see what it answers.

> Apple Business keeps one discovery URL per organization: registering it sends every Managed Apple Account of the organization to this Cerberus Enterprise organization. Don't register it from two Cerberus Enterprise organizations that use the same Apple Business organization.

Option 2: Redirect from your web site

On the web server of each domain, redirect */.well-known/com.apple.remotemanagement* to the discovery URL of your organization, **keeping the query string** (it carries the account typed by the user). This works with every OS version that supports account-driven enrollment, and the mode can

be different for iPhone and Mac. Copy the text for Apache or nginx from the tab; it looks like this, with the key of your organization:

Apache (.htaccess or virtual host):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

On other web servers or services (IIS, Cloudflare, hosting control panels), create a redirect rule (302) from the same path to the discovery URL with the option that keeps or forwards the query string.

Option 3: Static file on your web site

If you can't add a redirect, publish a file at *https://company.com/.well-known/com.apple.remotemanagement* (no file extension), served with *Content-Type: application/json*. Copy its content from the tab. A static file can't choose the mode per device: it uses the same mode for iPhone, iPad and Mac. For User Enrollment it looks like this:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/byod"}]}
```

and for Device Enrollment:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/adde"}]}
```

> The mode of the file must also be the mode set in the tab for the device family, otherwise the enrollment is refused.

Check configuration

In **Check configuration**, choose a domain and a device (iPhone or Mac) and click **Check**: Cerberus Enterprise asks the domain what a device would ask and shows the answer, each redirect and a verdict. The domain pointing to Cerberus Enterprise means options 2 or 3 work; an error answer (such as "not found") is fine for option 1; a web page or a file pointing elsewhere stops the devices. The check also warns when a redirect drops the query string or the file isn't served as *application/json*.

Enrollment key

The discovery and enrollment URLs contain a key of your organization. If the URLs were published by mistake, click **Regenerate key**: the old URLs stop working at once, so update the redirects and static files on your web sites. Cerberus Enterprise registers the new URL in Apple Business by itself when option 1 is used.

How users enroll

1. iPhone and iPad: open *Settings → General → VPN & Device Management → Sign In to Work or School Account*. Mac: *System Settings → General → Device Management → Sign In* (on macOS 14: *Privacy & Security → Profiles → Sign In*).
2. Type the Managed Apple Account, or the work e-mail address of the user in Cerberus (for example *name@company.com*). When the Managed Apple Account of the user is different from what was typed, the device then asks to sign in with that account.
3. A Cerberus Enterprise page opens: tap *Send the code*, then enter the 6-digit code received by e-mail. The code expires after 10 minutes; after 5 wrong codes the user must close the page and sign in again.
4. Sign in with the password of the Managed Apple Account (or with the company's sign-in page when Apple Business is connected to Google Workspace or Microsoft Entra ID), then allow the device management.

> Accounts that can't enroll (domain not verified, no matching user when users aren't created automatically, several users with the same e-mail address) see "This account isn't set up for enrollment. Contact your IT administrator." The events are in the system logs of the dashboard.

After the enrollment

- The device page shows the **Managed Apple Account** used to enroll and the enrollment type (User Enrollment or Account-driven Device Enrollment). In the device list, User Enrollment devices show "User Enrollment".

- On User Enrollment devices, the commands and policy settings that Apple doesn't allow (erase, location, lost mode, OS updates, many restrictions) are not offered or not sent. App Store apps of the policy use a user license instead of a device license (see **Apps on personal devices** below).
- On User Enrollment devices, web clips appear on the Home Screen but aren't listed in *Settings → General → VPN & Device Management*.
- The MDM certificate of these devices isn't renewed automatically and **Return to Service** isn't available: before the MDM certificate expires (one year after the enrollment, see the device page), ask the user to enroll the device again.
- To leave management, the user signs out of the work account in the same place of the settings, or you disenroll the device from Cerberus Enterprise. With User Enrollment only the work apps, accounts and data are removed; personal data stays. A device that enrolls again appears as a new device.

> Right after the enrollment, some profiles of the policy (certificates, Wi-Fi networks, web clips) can be reported as failed with an unknown error, and the device can show as **Non-compliant** for a while. The device tries them again by itself and they install after a while, with no action needed. Don't save the policy again or enroll the device again because of this.

Apps on personal devices

iPhones and iPads enrolled with User Enrollment have no serial number, so Apps and Books can't give them a device license. Cerberus Enterprise gives the App Store apps of their policy a **user license** instead: the license goes to the Managed Apple Account signed in on the device. Nothing changes in the policy: the same policy serves company and personal devices, and Cerberus chooses the license type for each device.

- **Automatic**: at the first enrollment Cerberus registers the Managed Apple Account with Apps and Books, then asks Apple for a license of each App Store app of the policy. Free apps need a license too; Apple gives them unlimited licenses. A paid app uses one license per Managed Apple Account, shared by all the personal devices of that account.
- **Same organization**: the Managed Apple Accounts and the Apps and Books token of Cerberus Enterprise must belong to the same Apple Business organization, and the apps must be in the library of the token's location.
- **License first**: an app is sent to the device only after Apple confirms its license, usually within a few minutes. Until then the **Applications** panel of the device shows it as **Waiting for a user license**, with the reason.
- **Install prompt**: personal devices are never supervised, so iOS asks the user before installing each app, including the **Cerberus Enterprise** app, which Cerberus installs on these devices too (**Install** or **Cancel**); no Apple Account sign-in is needed. If the user cancels, the app shows **Waiting for the user to approve the installation**: use **Request again** on the device page to show the prompt again. Apps installed as **Required** can't be deleted by the user.

- **Apps installed before enrolling**: Apple doesn't let the organization take over an app that the user installed personally on a device enrolled with User Enrollment. Ask the user to delete their own copy before enrolling, or delete it and then use **Request again** on the device page: the organization then installs the managed copy.
- **Leaving management**: when the device is unenrolled, iOS removes the managed apps and their data. A license is released when no other enrolled device of the same Managed Apple Account needs it, for example when the app leaves the policy or the last device is unenrolled; licenses nobody needs any more are released by the daily check within a day.

> When Apple can't assign a license, for example because a paid app has no license left, the app shows **User license failed** with Apple's message. Add licenses in Apple Business, then use **Request again** on the device page; Cerberus also tries again by itself at the daily check. The line above the app list shows the Managed Apple Account and the status of its Apps and Books user; the same status is on the page of the user.

> User licenses are used only on iPhones and iPads: on Macs enrolled with User Enrollment the App Store apps of the policy aren't installed. Books and personal Apple Accounts aren't supported.

Revision #7
Created 2026-11-10 15:12:30 UTC by Admin
Updated 2026-11-12 09:52:16 UTC by Admin