Setup

- Android Management setup
- Apple Management setup (APNs)

Android Management setup

To manage Android devices with Cerberus Enterprise, you must first connect your organization to Google Android Enterprise.

> The setup process usually takes a few minutes and requires a **work email address** (for example, *name@enterprise.com*) or, alternatively, a **personal Google email address**.

What happens during setup

- You will be redirected to Google Android Enterprise.
- You sign in with your work email address (or a personal Google email address).
- Google creates the Android Management account for your organization.
- You are redirected back to Cerberus Enterprise to complete the setup.

Important information

We recommend signing up with a work email address, not a personal Gmail account. If the email address is already associated with a Google Admin account, that existing account is reused and bound to Cerberus Enterprise; otherwise, a new free Google Admin account is created. A Google Admin account unlocks the full set of features — for example, enrolling devices using Google authentication with accounts managed by your Google Admin domain.

Don't have a work email address?

You can still sign up with a personal Google email address (for example, a Gmail account). In this case, Google creates a free managed Google Play account that is bound to Cerberus Enterprise.

Next steps

After completing the setup, create an **Enrollment token** and choose the appropriate provisioning method for the device.

Apple Management setup (APNs)

To manage Apple devices, Cerberus Enterprise requires the Apple Push Notification service (APNs) certificate.

> Use the Apple ID associated with your organization. The APNs certificate is valid for one year and must be renewed annually to continue managing devices.

Step 1: Download the CSR file

In the dashboard, start the Apple Management setup and download the Vendor-Signed Certificate Signing Request (CSR) file generated by Cerberus Enterprise.

Step 2: Create the Push Certificate on the Apple portal

- Sign in to the Apple Push Certificates Portal with your Apple ID.
- Click "*Create a Certificate*".
- Upload the CSR file from Step 1.
- Download the created Push Certificate.

Portal link: https://identity.apple.com/

Step 3: Upload the Push Certificate

Upload the Push Certificate you downloaded from Apple back into Cerberus Enterprise to complete the setup.

If the APNs certificate expires, Apple device management will stop working until the certificate is renewed.

Starting 30 days before the expiration, the dashboard shows a banner with a **How to renew** action. Always **renew** the existing certificate on the Apple Push Certificates Portal with the same Apple ID: a new certificate has a different topic, and devices already enrolled would need to be enrolled again.

Next steps

After APNs is configured, you can proceed with Apple device enrollment. Continue with **Apple provisioning overview**.