Devices provisioning

Supported devices

In general, any device running Android 5.1+ with Google Play Services is compatible with Cerberus Enterprise.

For a better user experience we suggest to use devices that meets the Android Enterprise Recommended requirements.

> Some functionalities are limited to specific Android versions, or can behave differently on different OS versions. For more information about a specific functionality, please read the Policies section of the documentation.

Cerberus Enterprise supports both company-owned and personally-owned devices, and two management modes, device owner and profile owner.

Personally-owned devices can be managed through a **work profile**, so you can implement a BYOD solution keeping employee's data and apps separate from personal one, for a better security and privacy on both ends. This option is suitable for devices already owned by employees, that you can enroll into your organization for securely use also at work.

Company-owned devices can be managed through a work profile too, but you also have the **fully managed** option, that allow a more strict control over the device. Company-owned devices with work profile are suitable when you want to provide company devices to employees for use at work, still allowing to use this devices also for personal use. The fully managed option, instead, is better suited for devices that must only be used at work, or for **dedicated devices** (COSU or corporate-owned single-use) like kiosk.

For more information on device provisioning please read the Devices provisioning section.

Enrollment tokens

Cerberus Enterprise uses enrollment tokens to trigger the provisioning process. The enrollment token and provisioning method you use establishes a device's ownership (personally-owned or company-owned) and management mode (work profile or fully managed device).

To create a new enrollment token, go to **Enrollment tokens** section in the dashboard, then click the **New enrollment toke**n button.

1. Options

When creating a new enrollment token you can specify some parameters, that determines some aspects of the provisioning, depending on your needs.

1.1. Policy

Required field. This is the policy that will be automatically applied on all devices enrolled using the token. You can select one of the policy you created in your account. If you don't have any policy in your account, you must create one first.

1.2. User

The user that will be automatically associated to devices during provisioning.

1.3. Personal usage

Required field. Controls whether personal usage is allowed on a device provisioned with this enrollment token.
For **company-owned** devices: enabling personal usage allows the user to set up a work profile on the device. Disabling personal usage requires the user provision the device as a fully managed device.
For **personally-owned** devices: enabling personal usage allows the user to set up a work profile on the device. Disabling personal usage will prevent the device from provisioning.
Personal usage cannot be disabled on personally-owned device.

1.4. Duration

Required field. The length of time the enrollment token is valid, ranging from 1 minute to 30 days.

1.5. Allowed usages

Required field. Whether the enrollment token can be used multiple times or one time only.

2. Provisioning options

These additional options are applied during the provisioning of fully managed devices enrolled scanning a QR code. They do not apply to work profiles or devices enrolled using other provisioning methods.

If you set a WiFi configuration, a device can automatically connect to the specified network without user interaction during device provisioning for downloading the mobile device management application.

Personally-owned devices

Devices owned by employees can be set up with a **work profile**. A work profile provides a self-contained space for work apps and data, separate from personal apps and data. Most app, data, and other management policies apply to the work profile only, while the employee's personal apps and data remain private.
To set up a work profile on a personally-owned device, use one of the following provisioning methods (ensure that the enrollment token has ***Personal usage*** set to **Allowed**):

Enrollment token link

Android version
5.1+

You can provide the Enrollment URL to the end users. When an end user opens the link from their device, they will be guided through the work profile setup.

Add work profile from "*Settings*"

Android version
5.1+

To set up a work profile on their device, a user can:

1. Go to *Settings* > *Google* > *Set up & restore*.
2. Tap "*Set up your work profile*".

These steps initiate a setup wizard that downloads *Android Device Policy* on the device. Next, the user will be prompted to scan a QR code or manually enter an enrollment token to complete the work profile setup.

Download Android Device Policy

Android version
5.1+

To set up a work profile on their device, a user can download Android Device Policy from the Google Play Store. After the app is installed, the user will be prompted to scan a QR code or manually enter an enrollment token to complete the work profile setup.

Company-owned devices for work and personal use

Setting up a company-owned device with a **work profile** enables the device for both work and personal use. On company-owned devices with work profiles:

- Most app, data, and other management policies apply to the work profile only.
- The employee's personal profile remains private. However, enterprises can enforce certain device-wide policies and personal usage policies.
- Enterprises can use *Block scope* to enforce compliance actions on an entire device or only its work profile.
- Device disenrolling and device commands apply to an entire device.

To set up a company-owned device with a work profile, use one of the following provisioning methods (ensure that the enrollment token has **Personal usage** set to **Allowed**):

QR code method

Android version
8.0+

On a new or factory-reset device, the user (typically an IT admin) taps the screen six times in the same spot. This triggers the device to prompt the user to scan a QR code.

Company-owned devices for work use only

Full device management is suitable for company-owned devices intended exclusively for work purposes. Enterprises can manage all apps on the device and can enforce the full spectrum of Android Management API's policies and commands.
It's also possible to lock a device down (via policy) to a single app or small set of apps to serve a dedicated purpose or use case. This subset of fully managed devices is referred to as **dedicated devices**.
To set up full management on a company-owned device, use one of the following provisioning methods (ensure that the enrollment token has **Personal usage** set to **Disallowed**):

QR code method

Android version
7.0+

On a new or factory-reset device, the user (typically an IT admin) taps the screen six times in the same spot. This triggers the device to prompt the user to scan a QR code.

DPC identifier method

Android version
5.1+

If Android Device Policy can't be added via QR code a user or IT admin can follow these steps to provision a fully managed or dedicated device:

1. Follow the setup wizard on a new or factory-reset device.
2. Enter Wi-Fi login details to connect the device to the internet.
3. When prompted to sign in, enter **afw#setup**, which downloads Android Device Policy.
4. Scan a QR code or manually enter an enrollment token to provision the device.

Zero-touch

IT admins can provision company-owned devices using the zero-touch enrollment method, outlined in Zero-touch enrollment for IT admins. When a device is first turned on, the device is automatically forced into the settings defined by the IT admin.

IT admins can preconfigure devices purchased from authorized resellers and manage them using the Cerberus Enterprise dashboard. To link your Zero-touch account, go to **Zero-touch** section in the dashboard, then follow the instructions.

Android version	Work profile	Fully managed device	Dedicated device
8.0+ (Pixel 7.1+)	✓	✓	✓