Device Provisioning - Android

- Supported devices
- Enrollment tokens
- Personally-owned devices
- Company-owned devices for work and personal use
- Company-owned devices for work use only
- Zero-touch
- Authenticate Using Google enrollment

Supported devices

In general, any device running Android 6+ with Google Play Services is compatible with Cerberus Enterprise.

For a better user experience, we suggest using devices that meet the Android Enterprise Recommended requirements.

> Some features are limited to specific Android versions, or may behave differently across OS versions. For more information about a specific feature, see 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**. This enables a BYOD solution by keeping employees' work data and apps separate from personal data and apps, improving both security and privacy. This option is suitable for devices already owned by employees that you want to enroll in your organization for work use.

Company-owned devices can also be managed through a work profile, but you can also choose the **fully managed** option, which allows stricter control over the device. Company-owned devices with a work profile are suitable when you provide corporate devices to employees for work, while still allowing personal use. Fully managed devices are better suited for devices that must be used only for work, or for **dedicated devices** (COSU, corporate-owned single-use), such as kiosks.

For more information on device provisioning, see the Device provisioning overview page.

Enrollment tokens

Cerberus Enterprise uses enrollment tokens to start the Android device enrollment (provisioning) process. The token you select defines the initial policy applied to enrolled devices and influences which provisioning modes are allowed.

> The Android enrollment tokens tab is available only after completing **Android Management setup**.

Where to find enrollment tokens

In the dashboard, open **Enrollment tokens**. Depending on your account configuration, the page can show multiple tabs (Android tokens, Google sign-in enrollment, Apple manual enrollment, and Apple Automated Device Enrollment).

> If your Android enterprise is backed by a managed Google domain (Google Workspace), the dashboard can also show an **Authenticate Using Google Enrollment** tab. For details on enabling and using it, see **Authenticate Using Google enrollment**.

Enrollment tokens list (Android)

The Android tokens tab shows a table of all tokens. Clicking a row opens the token details page.

Columns

- **Status**: **Active** (devices can enroll with the token), **Expired** (the expiration date has passed) or **Used up** (a one-time token that was already used).
- **Policy**: the policy assigned to the token (the tooltip shows the policy id). **Deleted policy** means the policy was deleted after the token was created.
- **User**: optional user pre-assigned to devices enrolled with the token. **Deleted user** means the user was deleted after the token was created.
- **Enrollments**: how many devices enrolled with the token, shown as **n / 1** for a one-time token.

- **Personal usage**: Allowed / Disallowed / Dedicated device.
- **Created**: when the token was created. The table shows the newest tokens first.
- **Expiration**: expiration date/time, or **Never**.
- **Enrollment code**: the code of the token, the one you type on the device when you enroll it without a QR code.

Actions

- Each row has a delete action (**Delete enrollment token**). Deletion is disabled when the license is expired.
- The table supports multi-row selection: you can enable selection mode, select multiple tokens, and delete them with **Delete selected tokens**.
- Use the refresh action to reload the list. The table is paginated (10/25/50 items per page).

Create a new enrollment token

On the Android tokens tab, click **New enrollment token** to open the token creation page. If your license is expired, the create button is disabled.

Token options

1. Policy

Required. The policy automatically applied to all devices enrolled using this token. Select one of your **Android policies**. If you don't have any policy yet, create one first.

2. User

Optional. If set, newly enrolled devices are automatically associated with this user.

3. Personal usage

Controls whether personal usage is allowed on a device provisioned with this enrollment token:

- **Allowed**: suitable for personally-owned devices (work profile) and company-owned devices for work and personal use.
- **Disallowed**: suitable for company-owned devices for work use only (fully managed).
- **Dedicated device**: suitable for kiosk/dedicated devices (device is not associated with a single user).

4. Allowed usages

Select whether the token can be used multiple times (**Multiple**) or only once (**One time only**).

5. Expiration

Select the expiration unit (**Minutes**, **Hours**, **Days**, or **Never**). When not set to Never, enter the expiration value. The allowed range depends on the selected unit and can go up to 10,000 days.

6. Google auth

Controls whether the user must authenticate with a Google account during device enrollment:

- **Unspecified**: the enterprise-level Google authentication setting is used to determine whether the user needs to authenticate with Google during enrollment.
- **Optional**: the user can choose to skip Google authentication during enrollment.
- **Required**: the user must authenticate with a Google account to proceed with enrollment.

When **Required** is selected, an optional **Required account email** field appears. If set, the user must authenticate with that specific Google account during enrollment.

Provisioning options (QR code only)

These additional options are embedded into the QR code and are applied during provisioning of fully managed devices enrolled by scanning the QR code. They do not apply to work profiles or devices enrolled using the Enrollment URL or Token.

Wi-Fi configuration

Use this to let a device automatically connect to Wi-Fi during provisioning, so it can download and initialize the management app. Available fields include **SSID**, **Hidden SSID**, **Security**, and (when needed) **Passphrase**.

You can also configure an HTTP proxy (**Proxy**) and, depending on the mode, set **Host**/**Port**, **PAC URI**, and **Proxy bypass host**.

Other options

Additional options include **Locale**, **Time zone**, and **Skip encryption**.

Enrollment token details

When you open a token, the details page shows the token configuration and usage information:

- **Status**, **Expiration**, **Usage**, **Personal usage**, **Allowed usages**, and (when set) **Google auth** with the optional **Required account email**.
- **Token**: the raw enrollment token value (copyable).
- **Enrollment URL**: a Google Android Enterprise enrollment URL (copyable and sendable by email).
- **QR code**: shown on the right side of the page, used to enroll fully managed devices.

> For step-by-step provisioning procedures, follow the Android enrollment guides: **Personally-owned devices**, **Company-owned devices for work and personal use**, **Company-owned devices for work use only**, and **Zero-touch**.

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 employees' 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
6.0+

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
6.0+

To set up a work profile on their device, a user can open the device's ***Settings*** app, then use the search bar to find and tap the ***Set up your work profile*** option.

If the search is unsuccessful, the location of this option can vary. Here are a few possibilities:

- *Settings -> Google services and preferences -> All services -> Set up your work profile*.
- *Settings -> Google -> Set up & restore -> 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
6.0+

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.

Personal iPhones and iPads

Personal iPhones and iPads (and Macs) enroll with Apple **User Enrollment**: the user signs in with their Managed Apple Account in the device settings, and only the work apps, accounts and data are managed. On iPhones and iPads the App Store apps of the policy and the **Cerberus Enterprise** app are installed with a user license of that account. The location of personal devices is collected only if their policy turns on **Location and geofences on personal devices** and the user allows it.

Read **Apple account-driven enrollment**.

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.
- Employees' personal profiles remain 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+)	✓	✓	✓

Authenticate Using Google enrollment

Authenticate Using Google enrollment (also referred to as **Google Authentication for Enrollment**) lets users authenticate with their Google Workspace account during Android device enrollment.

> This feature is available only for Android enterprises backed by a managed Google domain (Google Workspace).

Where to find it

In the dashboard, open **Enrollment tokens** and select the **Authenticate Using Google Enrollment** tab. The tab is shown only when Android Management is configured and the Google Workspace integration is available for your enterprise.

Enable (or disable) Google Authentication

Google Authentication is enabled from the **Google Admin console**. After changing the setting, return to Cerberus Enterprise and use **Refresh Status** to reload the current configuration.

1. Log in to your **Google Admin console** with an administrator account.
2. Open **Devices**.
3. Go to **Mobile & endpoints → Settings → Third-party integrations**.
4. Find the **Android EMM integration** for Cerberus Enterprise and open it.
5. Click **Manage EMM providers**.
6. Toggle **Authenticate Using Google** to enable or disable Google authentication for enrollment.
7. Click **Save**.

8. Return to the Cerberus Enterprise dashboard and click **Refresh Status** on the **Authenticate Using Google Enrollment** tab.

Google Authentication Enrollment Token

When Google Authentication is enabled, the dashboard shows a dedicated enrollment token used for this enrollment mode. The page can show a **QR code**, an **Enrollment Token** value, and an **Enrollment URL** (copyable and sendable by email).

Key options

- **Allow Personal Usage**: controls whether the token can enroll devices for work and personal use (work profile scenarios) or work use only (fully managed / dedicated scenarios).
- **Fallback Default Policy**: the policy applied when the enrolling user does not have a specific Google Authentication default policy assigned.

Policy interaction

The policy setting **Work account setup authentication** (workAccountSetupConfig.authenticationType) controls how users authenticate during work account setup, but the Google Admin Console setting **Authenticate Using Google** and the enrollment token type can still require authentication.

For already enrolled devices, this policy only applies if the device is managed by a managed Google Play account (i.e., enrolled without **Authenticate Using Google Enrollment**).

> Some actions (for example changing token options) can be disabled when the license is expired.

Enroll a device

During enrollment, the user is prompted to authenticate with their Google Workspace account. After a successful enrollment, the device is associated with the authenticated user.

Work profile (personally-owned devices)

- Share the **Enrollment URL** with the user. When the user opens it on their Android device, they are guided through work profile setup and Google authentication.
- Alternatively, the user can start from Android Settings and choose the work profile setup flow, then scan the QR code or enter the enrollment token when prompted.

Company-owned devices

- **QR code method**: on a new or factory-reset device, tap the screen multiple times in the same spot until the QR code prompt appears, then scan the QR code shown in the dashboard.
- **DPC identifier method** (when QR scanning is not available): follow the setup wizard, connect to Wi-Fi, then when prompted to sign in enter **afw#setup** and proceed by scanning the QR code or entering the enrollment token. When prompted, authenticate with the Google Workspace account.

For general Android provisioning procedures (work profile vs fully managed), see the standard Android enrollment pages in this manual.