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**.

Revision #75
Created 2022-02-28 14:36:51 UTC by Admin
Updated 2026-11-12 09:52:19 UTC by Admin