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.

Revision #59
Created 2026-01-15 15:47:26 UTC by Admin
Updated 2026-11-12 09:52:17 UTC by Admin