

Android Onboarding – Company Portal Enrollment

Purpose

This guide explains how to enroll an Android device into company Mobile Device Management (MDM) using **Microsoft Intune – Company Portal**. The steps below follow the standard Android + Intune enrollment flow. Some screens may vary slightly depending on device brand (Samsung, Xiaomi, Pixel, etc.) and Android version.

Step 1 – Install Required Applications

1. Open the **Google Play Store**.
 2. Search for **Company Portal** (by Microsoft) and install it.
 3. Search for **Microsoft Authenticator** and install it.
 4. Once both apps are installed, open **Company Portal**.
 5. **REQUIRED:** Ensure a **screen lock** is already set up on your device.
 - If not set, configure a screen lock first.
 - **Preferred:** PIN
 - **Recommended:** Enable fingerprint (if supported) for easier access.
 6. During setup, Android may ask for various permissions.
 - **Please give permissions when asked and tap Allow.**
 - If permissions are denied, company apps may not work properly.
-

Step 2 – Sign In and Change Password

1. Tap **Sign in**.
2. Enter your **company email address**, then tap **Next**.
3. Enter the **temporary password** provided by IT.
4. When prompted, **create a new password**.
 - Remember this password or write it down.
 - **IT does not store or know your password.**

Step 3 – Wait for Account Sync

1. After the password change, a message may appear asking you to **wait a couple of minutes**.
2. **Close the Company Portal app completely.**
3. Wait approximately **1 minute**.
4. Reopen **Company Portal**.

Step 4 – Multi-Factor Authentication Setup

1. Sign in to **Company Portal** using your company email and **newly changed password**.
2. On the **Keep your account secure** page, tap **Next**.
3. Because Microsoft Authenticator is already installed, tap **Next**.
4. Tap the blue text **“Pair your account to the app by clicking this link”**.
 - This may take a couple of tries.
 - If nothing happens, tap **Next** and try again.
 - The system will open Microsoft authenticator and try to setup the MFA, please give access to when prompted. If not, the app will not work properly. if your account is active on the Microsoft authenticator app, please go back to the company portal installation and then tap on **Next**.
5. Approve the notification by entering the same number shown on the screen in the Microsoft Authenticator prompt **“Are you trying to sign in?”**, then tap **Yes**.
6. When you see **“Notification approved”**, tap **Next**.
7. Register your phone number:
 - Change country to **Indonesia (+62)**
 - Enter your phone number
 - Tap **Next**
8. Complete the CAPTCHA, then enter the verification code sent to your phone number (via WhatsApp or SMS), and tap **Next**.
9. When you see **Success!**, tap **Done**.

Step 5 – Device Enrollment and Permissions

1. **Finish setting up MFA.**

When it's done, you will be taken back to **Company Portal automatically**.

2. On the **Company Access Setup** screen, tap **Begin**.

3. When you see **“We care about your privacy”**, tap **Continue**.

4. Company portal will continue the installation, please wait until its finished.

- On Samsung, you may need to tap on **Agree** with the Work profile creation.

5. When the **Work Profile is finished**, you'll be back on the **Company Access Setup** screen. Tap **Continue**.

6. Wait again until you see **“Your new work setup”**, then tap **Got it**.

7. Important to understand (Do not skip this):

- Android system creates a **separate Work Profile**.
- Work apps and data are **separate** from your personal apps.
- You **can copy personal data into work apps**, but you **cannot copy work data back to personal apps**.

8. **You're done.**

Company Portal will **automatically download and install work apps**.

- If apps don't show up yet, **open the Play Store app** inside the **Work Profile** to manually trigger the installation.

Step 6 – Logging in on Work Apps

1. After the work apps are installed, please don't forget to open the app and login using your work email and password.

Step 7 – Device Compliance Check and App Installation

1. Please take at least once a week to open the company portal app and signing in again. This makes sure that the apps stays logged in and will prevent frequent disconnection on the accounts.

Additional Information – Device Status

- Sometimes the status may not update immediately.
 - This can happen for several reasons.
 - The most common reason is that the **device screen lock (PIN / password)** does not meet company security requirements or needs to be updated.
 - If prompted, update your screen lock, then return to **Company Portal** and wait for the status to refresh.
4. Once the status is compliant, enrollment is complete.
- You may now open work apps and sign in when prompted.
-

Additional Notes

- IT **cannot** see personal data such as photos, messages, or personal apps.
-

Support

If enrollment fails or you see an error:

- Restart the device and try again
- Ensure Android is updated to the latest version
- Contact IT Support with the error message