

Android for Work

Admin Guide v1.1

© 2017, Codeproof Technologies Inc

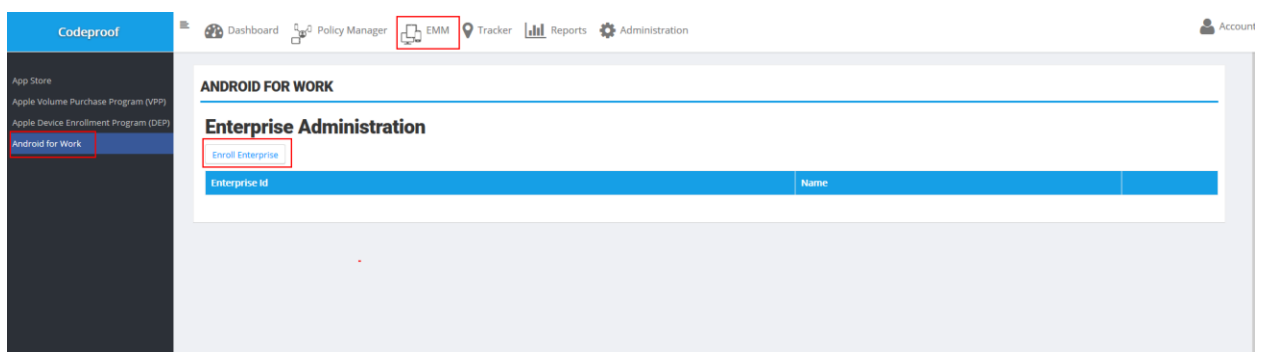
Required Steps

1. Enterprise Enrollment	The Enterprise needs to be enrolled into Google “Android for work(AfW)” using Codeproof EMM console
2. Purchase Apps	Add/Purchase required apps from Google work playstore.
3. Device Provisioning	Provision the device using Codeproof MDM app.
4. Distribute Apps	Silently install/uninstall apps from the device.
5. Managing Policies	Login to Codeproof Cloud Console manage policies.

Enterprise Enrollment

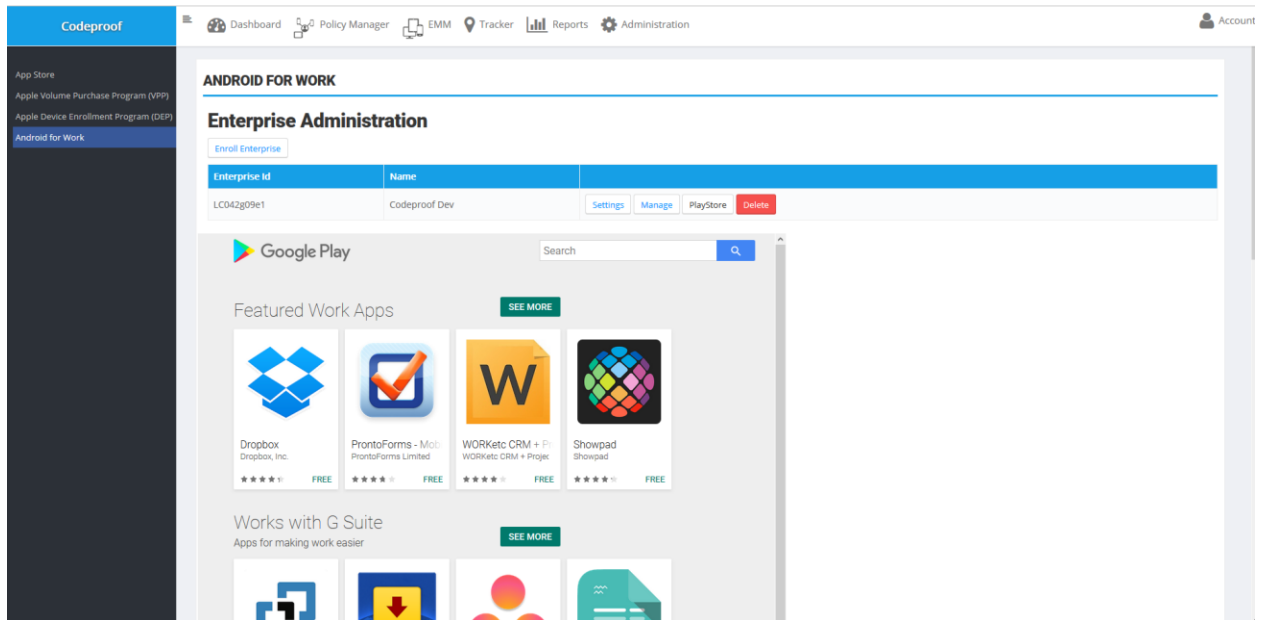
Login to Codeproof Cloud Console and then go to “EMM” menu option from the top. In the EMM section, select “Android for work”.

Click on “Enroll Enterprise” button and login to your organizations gmail account. Once the enrollment completes, click on “PlayStore” button. This will take you to “Google for work” playstore.



Purchase Or Approve Apps

Click on “PlayStore” button to go to Google Playstore and select apps you want to distribute across the enterprise.



Provision the device

Reset the device and go to setup screen. Add the WiFi and then go to “Accounts” section. Don’t add Gmail account. Add following EMM token instead. Click on continue to install Codeproof MDM app automatically. Refer to device enrollment guide for more details.

Enter following EMM Token in the account box.

afw#codeproof

Manage Apps

Go to “Policy Manager” from the top menu and select the group of Android devices and on right side go to “Play Store Manager” to push apps to the enrolled devices. See below image illustrations. You can select multiple apps and deploy them to a group of devices. Or select a single app and deploy it. Similarly, you can remotely uninstall apps from group of devices. You can also select a app and configure the managed settings remotely.

The screenshot displays the Codeproof Mobile Policy Manager interface. The top navigation bar includes 'Codeproof', 'Dashboard', 'Policy Manager', 'EMM', 'Tracker', 'Reports', and 'Administration'. The left sidebar shows a navigation menu with 'Home' and 'Android Devices' selected. The main content area is titled 'MOBILE POLICY MANAGER' and features a sub-menu with 'Android Security', 'iOS Security', 'Samsung Security', and 'LG Security'. Under 'Android Security', there are tabs for 'Command Center', 'Mobile Antivirus', 'Agent Policy', 'Passcode Policy', 'Android Configurations', 'Kiosk Mode', 'Kiosk App Management', 'Device Restrictions', and 'App Restrictions'. The 'PlayStore Manager' tab is active, showing a list of 'Approved Apps' with checkboxes and buttons for 'Install Apps', 'Uninstall Apps', and 'Config App'. The list includes Slack, Google Chrome: Fast & Secure, Codeproof Secure Browser, Codeproof App Manager, Secured Call Timer, com.codeproof.galaxy.security, Dropbox, Gmail, Economy, and ZOOM Cloud Meetings.

Codeproof Dashboard Policy Manager EMM Tracker Reports Administration

MOBILE POLICY MANAGER

Android Security iOS Security Samsung Security LG Security

Command Center Mobile Antivirus Agent Policy Passcode Policy Android Configurations Kiosk Mode Kiosk App Management Device Restrictions App Restrictions

Permission Policy **PlayStore Manager** Web Shortcuts Secure Browsing

Google Playstore Manager
Remotely install, uninstall and config Android apps via google playstore. Supported only on Android for Work(AW) enabled devices.

Approved Apps

- Select All Apps
- Slack
- Google Chrome: Fast & Secure
- Codeproof Secure Browser
- Codeproof App Manager
- Secured Call Timer
- com.codeproof.galaxy.security
- Dropbox
- Gmail
- Economy
- ZOOM Cloud Meetings

Install Apps
Uninstall Apps
Config App

Manage Policies

Manage Permissions: IT administrator can remotely accept/deney app runtime permissions remotely.

The screenshot shows the Codeproof Mobile Policy Manager interface. The left sidebar contains a navigation menu with options like Home, Android Devices, Kyocera, Sam test, Android Test, Bring Your Own Devices (BYOD), iOS Devices, LG Devices, North America, Samsung Devices, and Stores. The main content area is titled "MOBILE POLICY MANAGER" and has tabs for Android Security, iOS Security, Samsung Security, and LG Security. Under "Android Security", there are sub-tabs: Command Center, Mobile Antivirus, Agent Policy, Passcode Policy, Android Configurations, Kiosk Mode, Kiosk App Management, Device Restrictions, and App Restrictions. The "App Restrictions" sub-tab is active, showing "Android App Permission Management". The page has an "Enable" checkbox checked and a dropdown menu set to "PERMISSION_POLICY_AUTO_GRANT". Below this is a list of apps with their permission states, each with a plus icon for configuration:

- Slack
- Google Chrome: Fast & Secure
- Codeproof Secure Browser
- Codeproof App Manager
- Secured Call Timer
- com.codeproof.galaxy.security
- Dropbox
- Gmail

Device Restrictions: The following restriction policies are available in "Android for work" device owner mode.

The screenshot shows the Codeproof Mobile Policy Manager interface with the "Device Restrictions" sub-tab active. The "Enable" checkbox is checked. The page displays a list of device restriction policies, each with an unchecked checkbox:

- Allow Parent Profile App Linking(P)
- Block Add User(D/P)
- Block Adjust Volume(D/P)
- Block Bluetooth Config
- Block Cell Broadcasts Config(D/P)
- Block User Credentials Config
- Block Mobile Networks Config(D/P)
- Block Tethering Config(D/P)
- Block VPN Config
- Block WiFi Config
- Block Alert Windows
- Block Cross Profile copy-paste
- Block Data Roaming(D)
- Block Debugging Config
- Block Factory Reset By User(D/P)
- Block Fun(D)
- Block Accounts Management
- Block Physical Media(D/P)
- Block Network Reset(D/P)
- Block NFC
- Block Outgoing Phone Calls
- Block Remove User
- Block Safe Boot(D/P)
- Block User Icon(D/P)
- Block Wallpaper Change(D/P)
- Block Location Sharing
- Block SMS
- Block Microphone Volume Adjust(D/P)
- Block USB File Transfer(D/P)
- Block Verify Apps
- Block Date Time Config(D)
- Block Bluetooth Contact Sharing(P)
- Block Camera
- Block Screen Capture(D/P)

Application Whitelisting

You can also block default applications in the device. See below image illustrations.

The screenshot displays the 'MOBILE POLICY MANAGER' interface. At the top, there are tabs for 'Android Security', 'iOS Security', 'Samsung Security', and 'LG Security'. Below these, a navigation bar includes 'Command Center', 'Mobile Antivirus', 'Agent Policy', 'Passcode Policy', 'Android Configurations', 'Kiosk Mode', 'Kiosk App Management', 'Device Restrictions', 'App Restrictions' (which is highlighted), 'Web Shortcuts', and 'Secure Browsing'.

Under the 'App Restrictions' tab, there are several checked options:

- Enable
- Block App Installation
- Block App Uninstallation
- Block App Control
- Block Install Unknown Sources Config

Below these options is the 'Application Blacklist' section, which includes an 'Add Apps' button and a table:

App Name	Package Name	
Gmail	com.google.android.gm	Remove
YouTube	com.google.android.youtube	Remove

At the bottom of the interface, there is an unchecked checkbox labeled 'Inherit from parent (Inherit policies from parent node)' and a 'Save' button.