Android for Work

Admin Guide v1.1

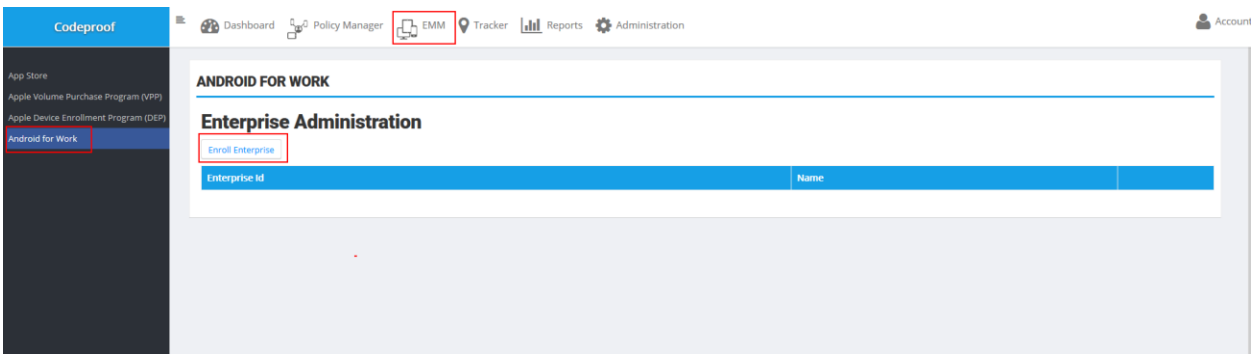
Required Steps

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

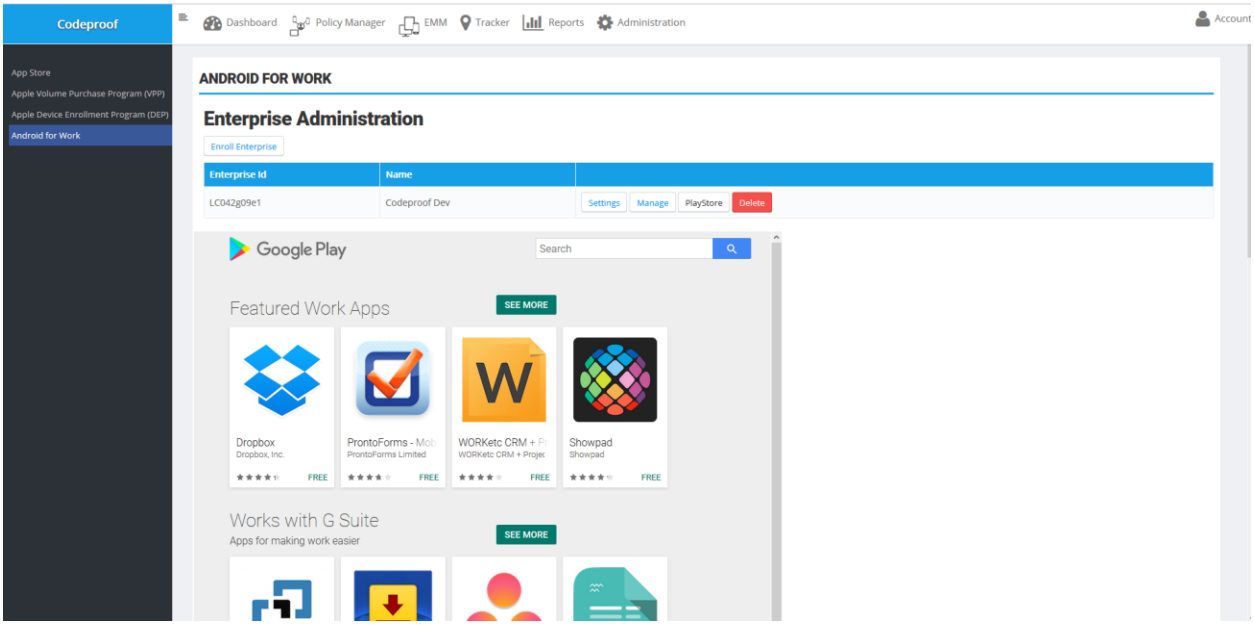
Login to Codeproof Cloud Console and then go to “EMM” menu option from the top. In the EMM section, select “Android for work”.

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

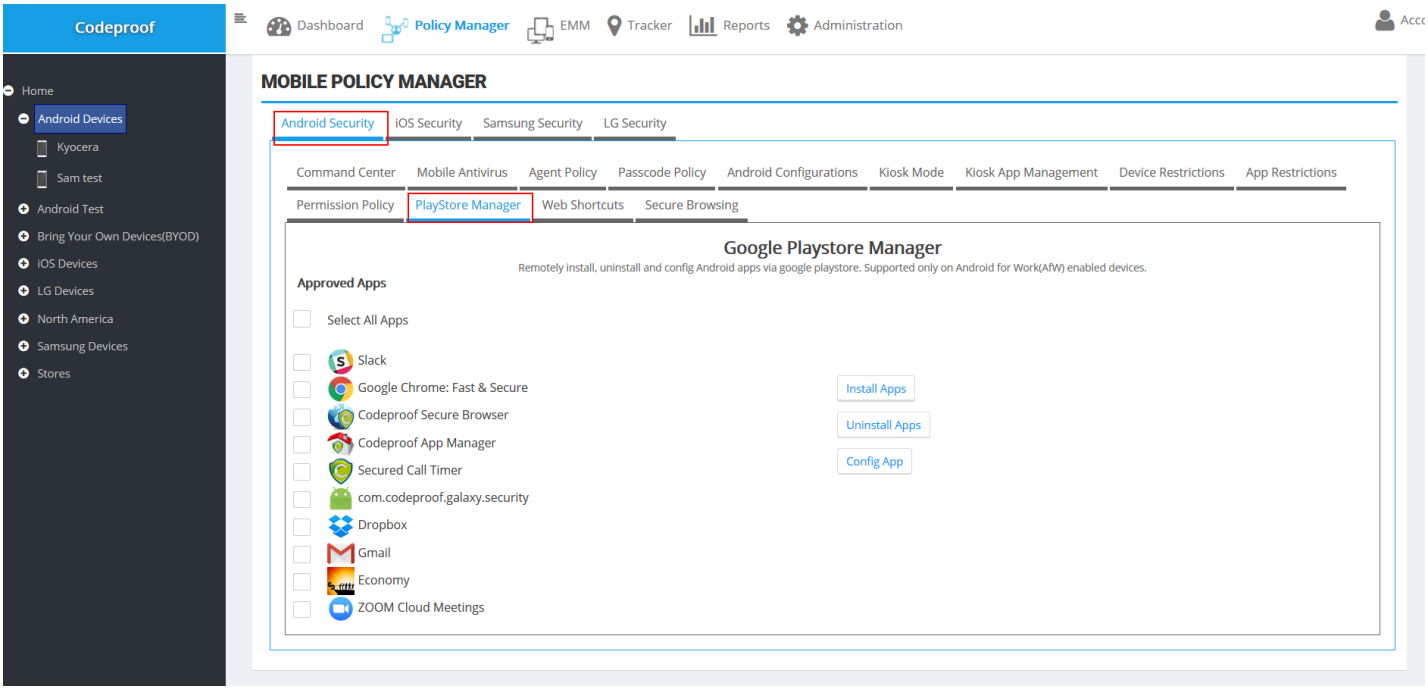
Reset the device and go to setup screen. Add the WiFi and then go to “Accounts” section. Don’t add Gmail account. Add following EMM token instead. Click on continue to install Codeproof MDM app automatically. Refer to device enrollment guide for more details.

Enter following EMM Token in the account box.

afw#codeproof

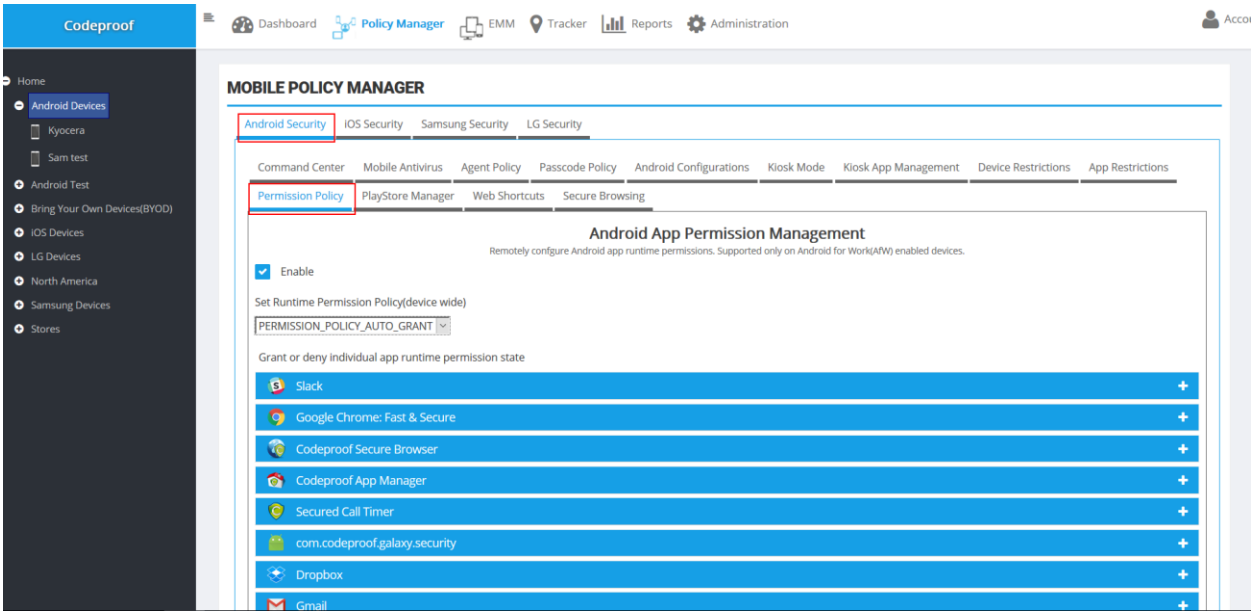
Manage Apps

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.

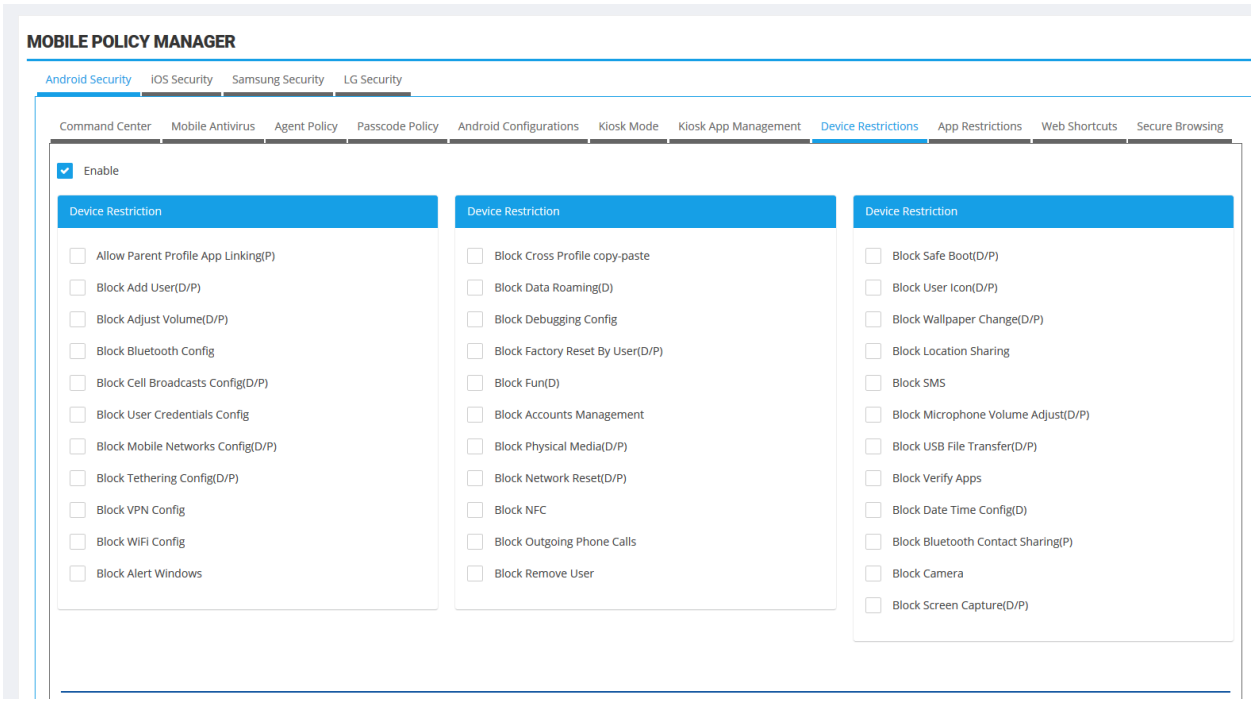


Manage Policies

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



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



Application Whitelisting

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