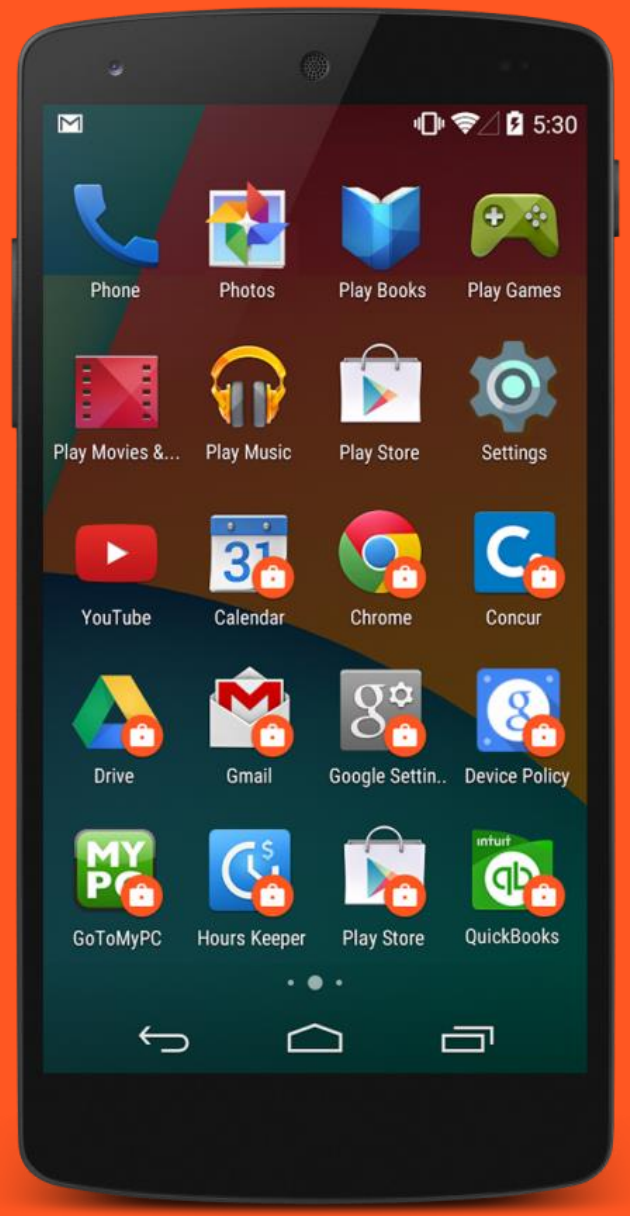


Android enterprise

Work Profile enrolment
Factory-reset state

MobileIron Core

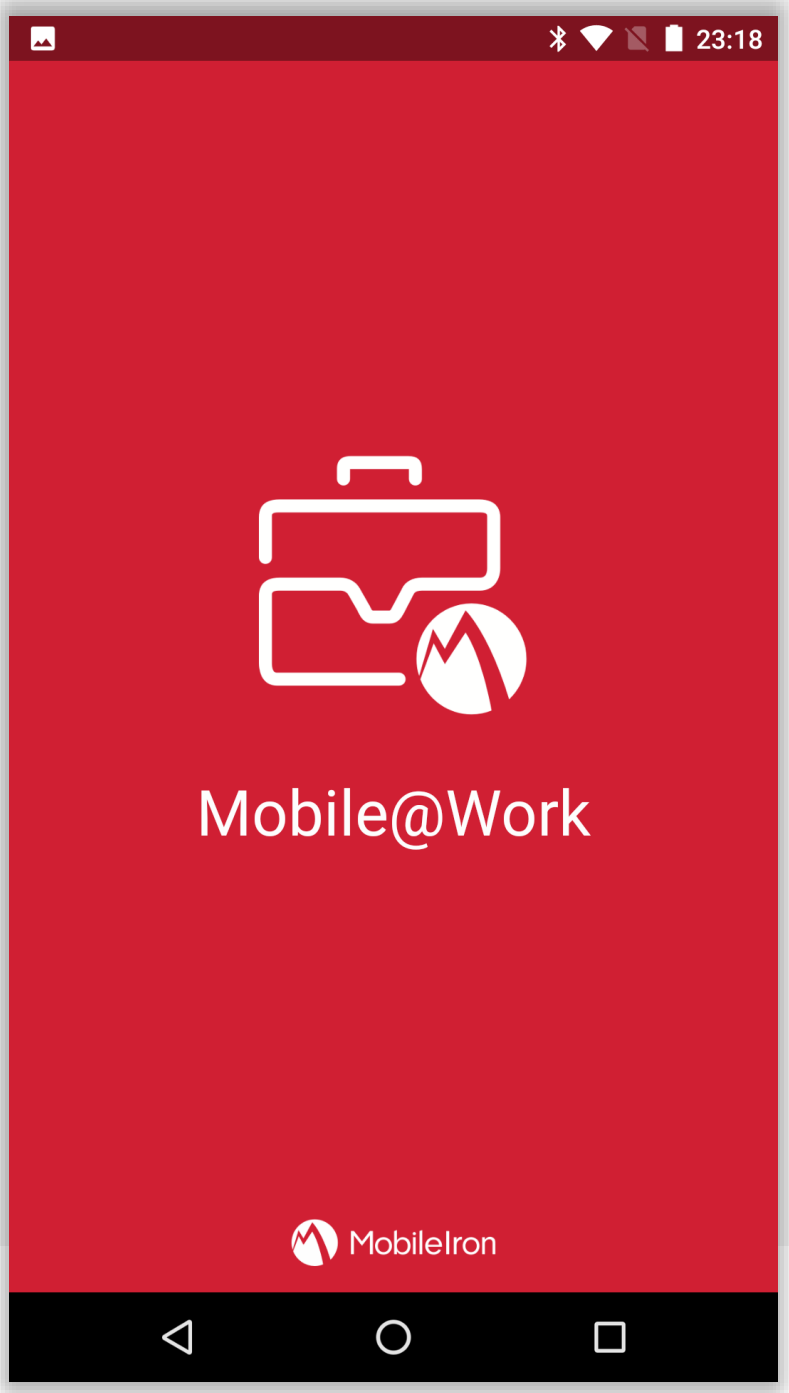
Android 7.x

September 2017

Requirements

In order to proceed, you must have:

- Android 5.0 or later installed on the devices to be provisioned. Android 6.0+ recommended.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.
- A Google account.



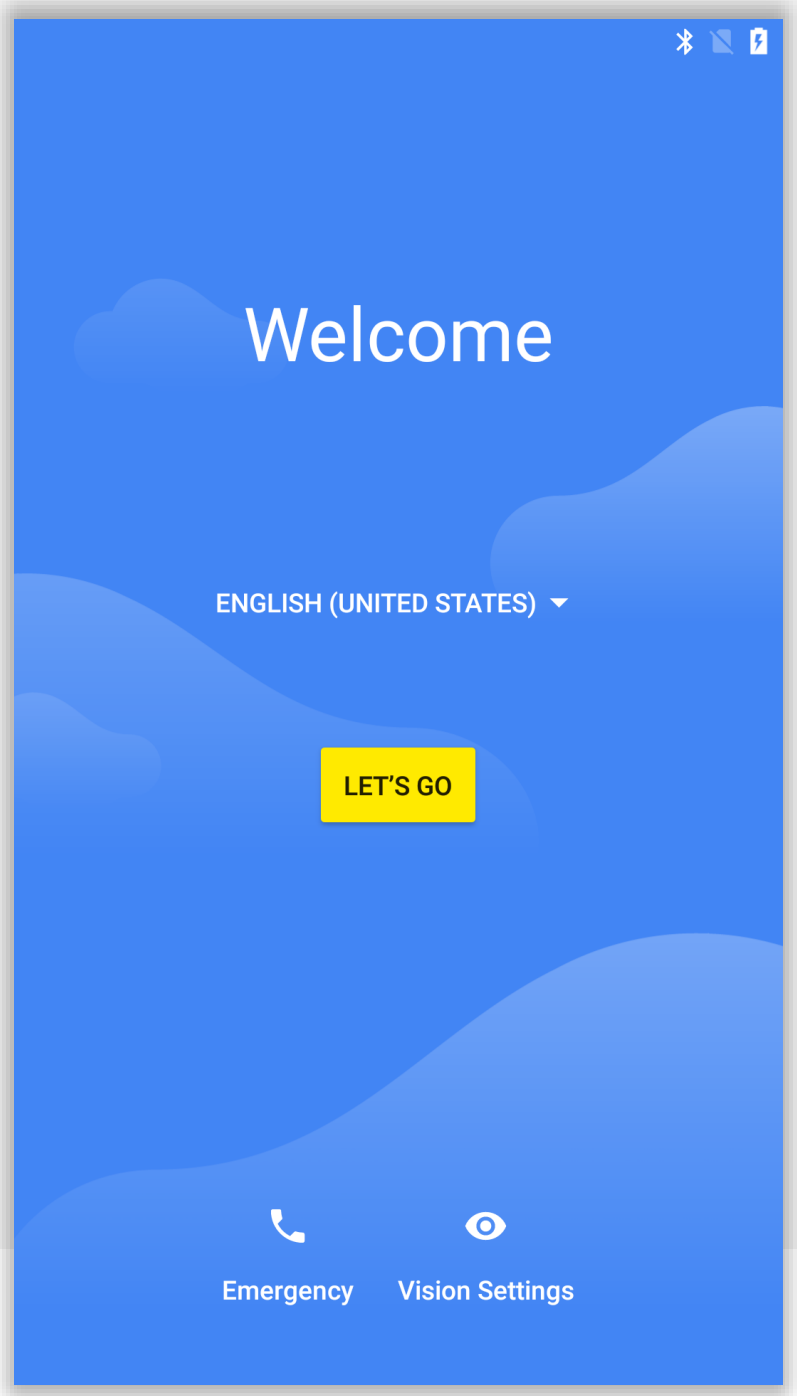
bayton

Begin device setup

For Work Profile enrolment there are no special initial steps.

You must work through all steps of the Wizard, until presented with the home screen.

To begin, tap **LET'S GO**.

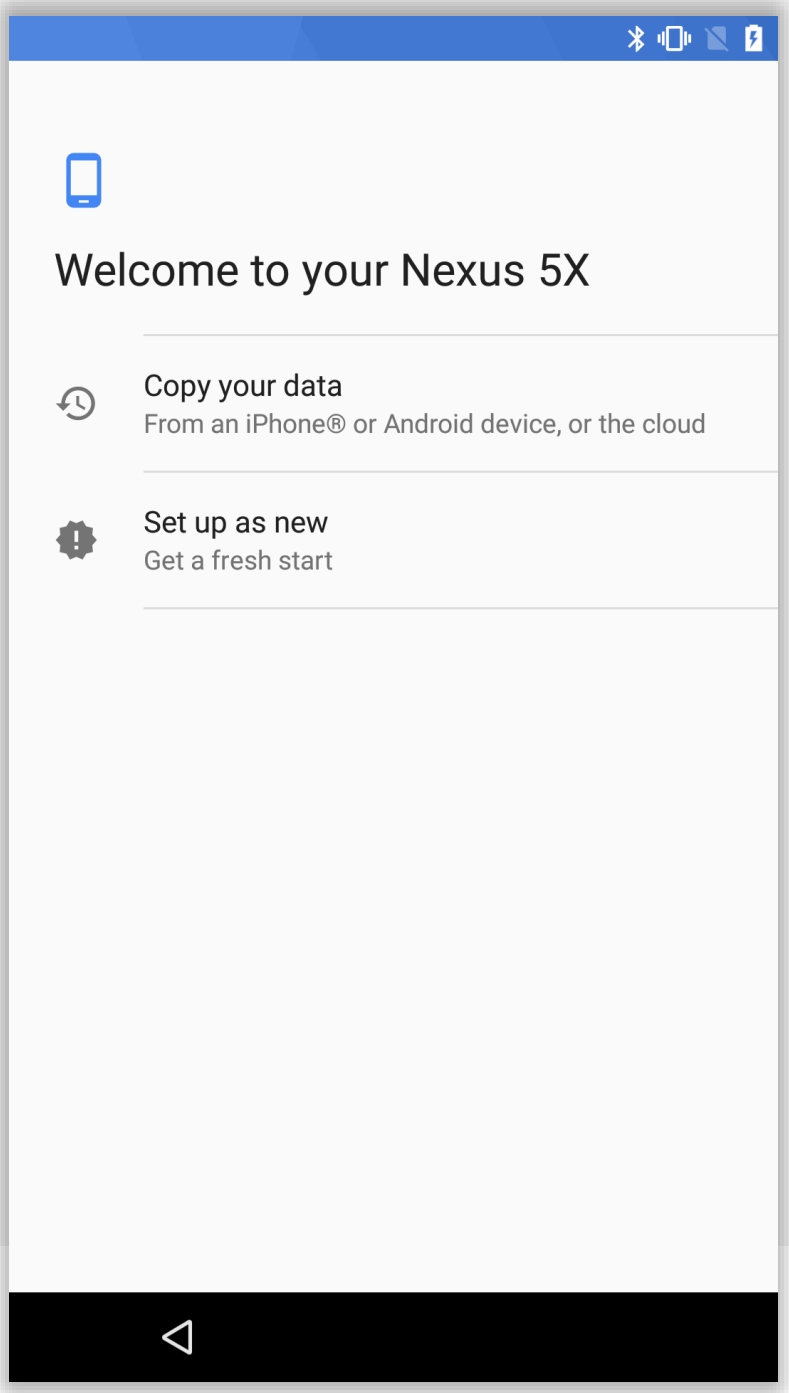


bayton

Continue device setup

There is no requirement to select one option over the other here as this does not impact Work Profile enrolment.

If being configured on behalf of a user, tap **Set up as new** and utilise a unique Google account. The user can add in their own account at a later point if desired.

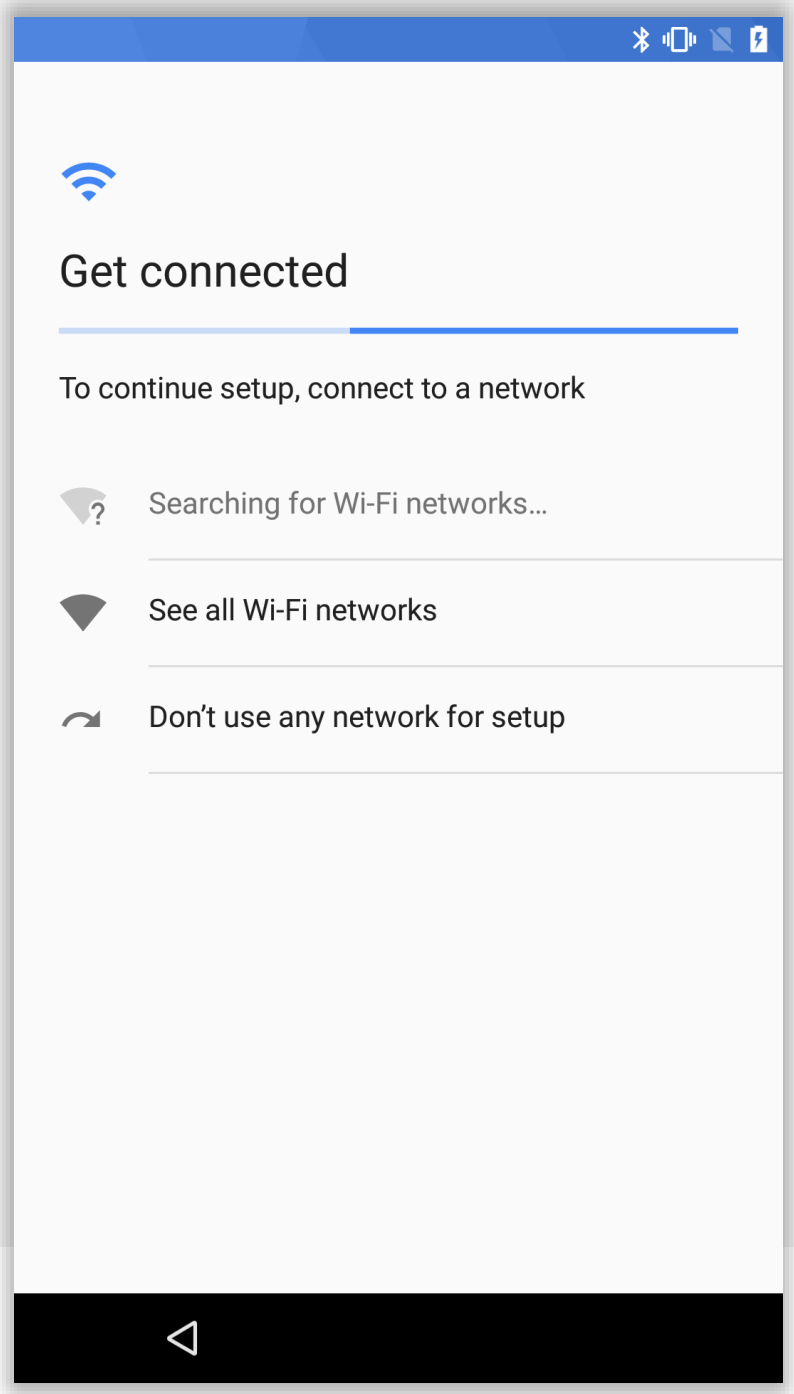


bayton

Continue device setup

Connect to a suitable WiFi network to continue.

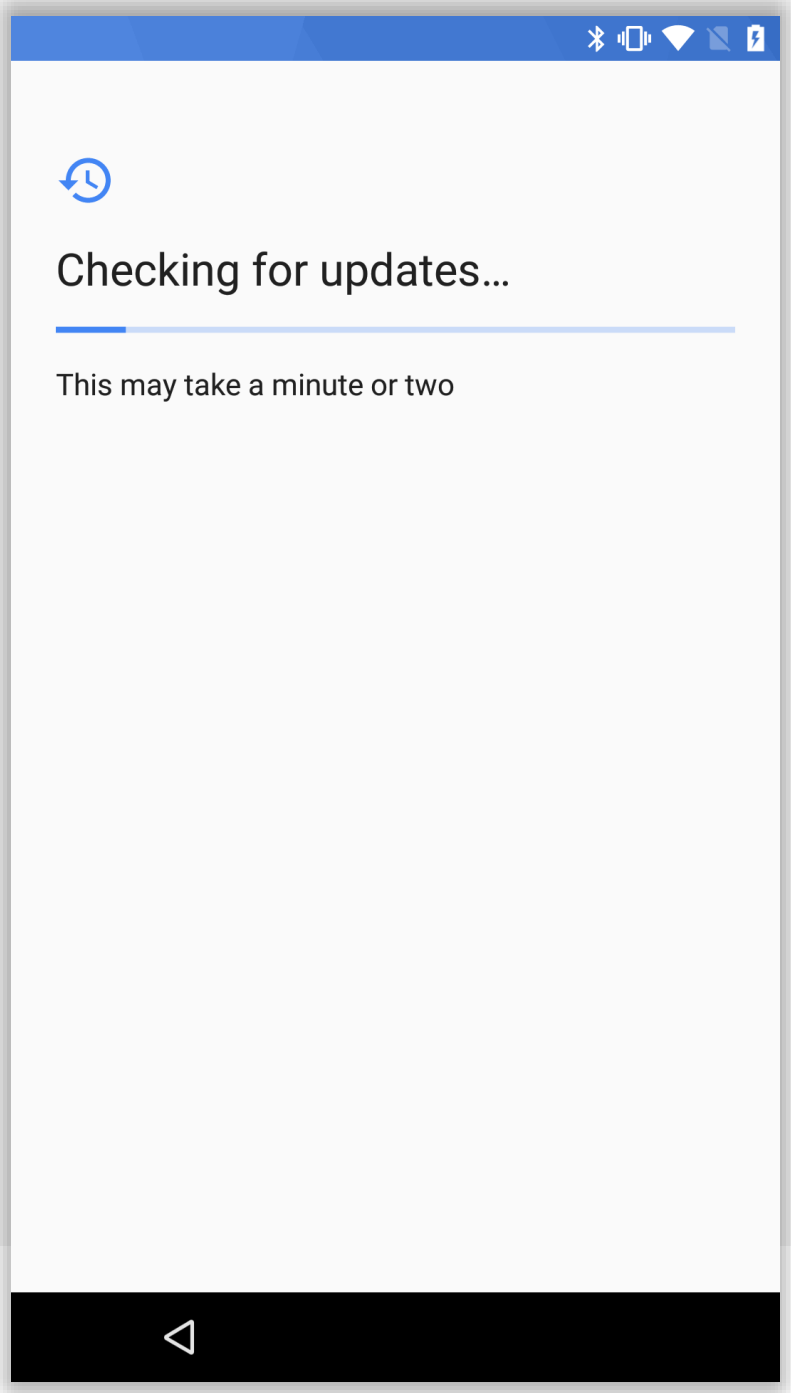
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup**.



bayton

Continue device setup

Once connected, the device will check for updates and automatically continue to the next step.

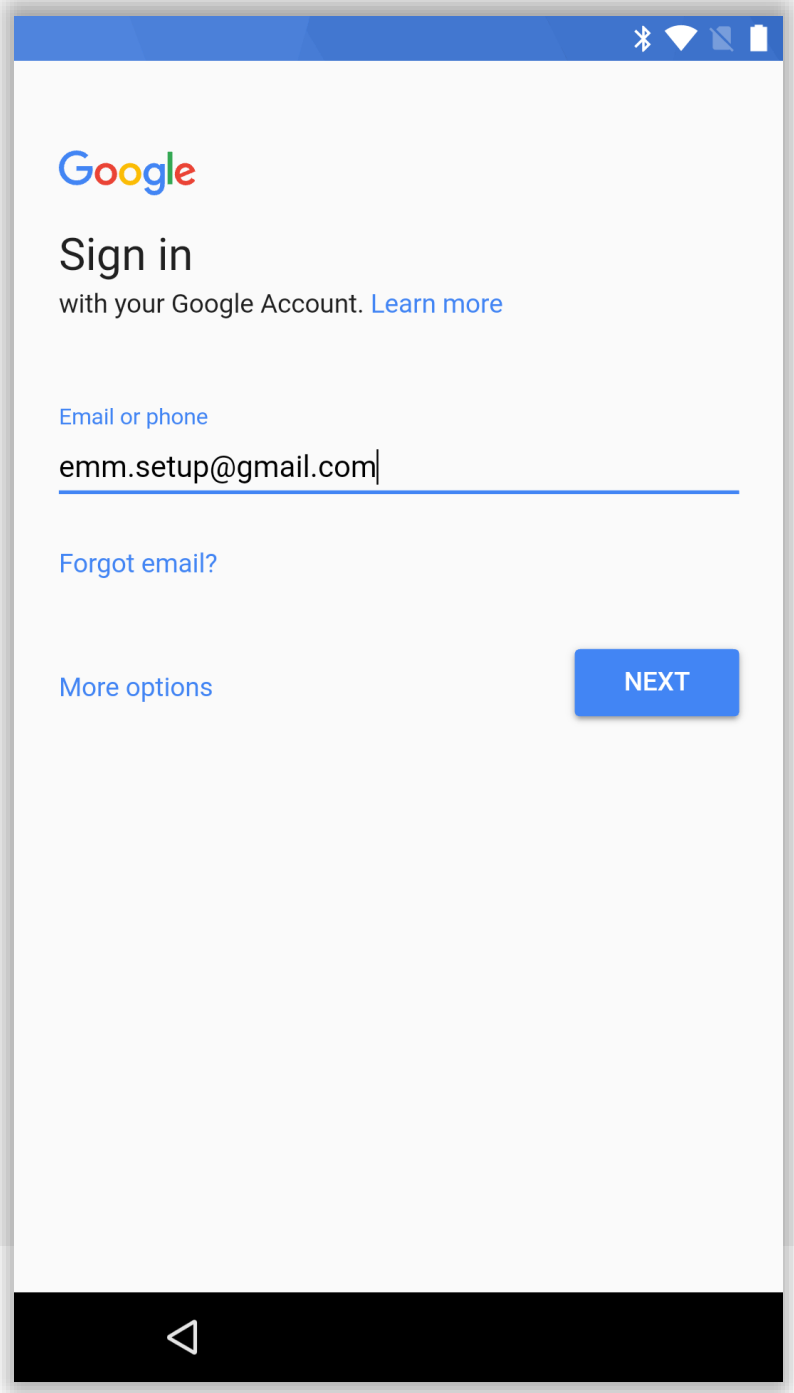


bayton

Continue device setup

At the Google account sign in screen, input an existing unique Google account address, or tap **More options** to create a new account.

When ready, tap **NEXT** to continue.



Why does a unique Google account matter?

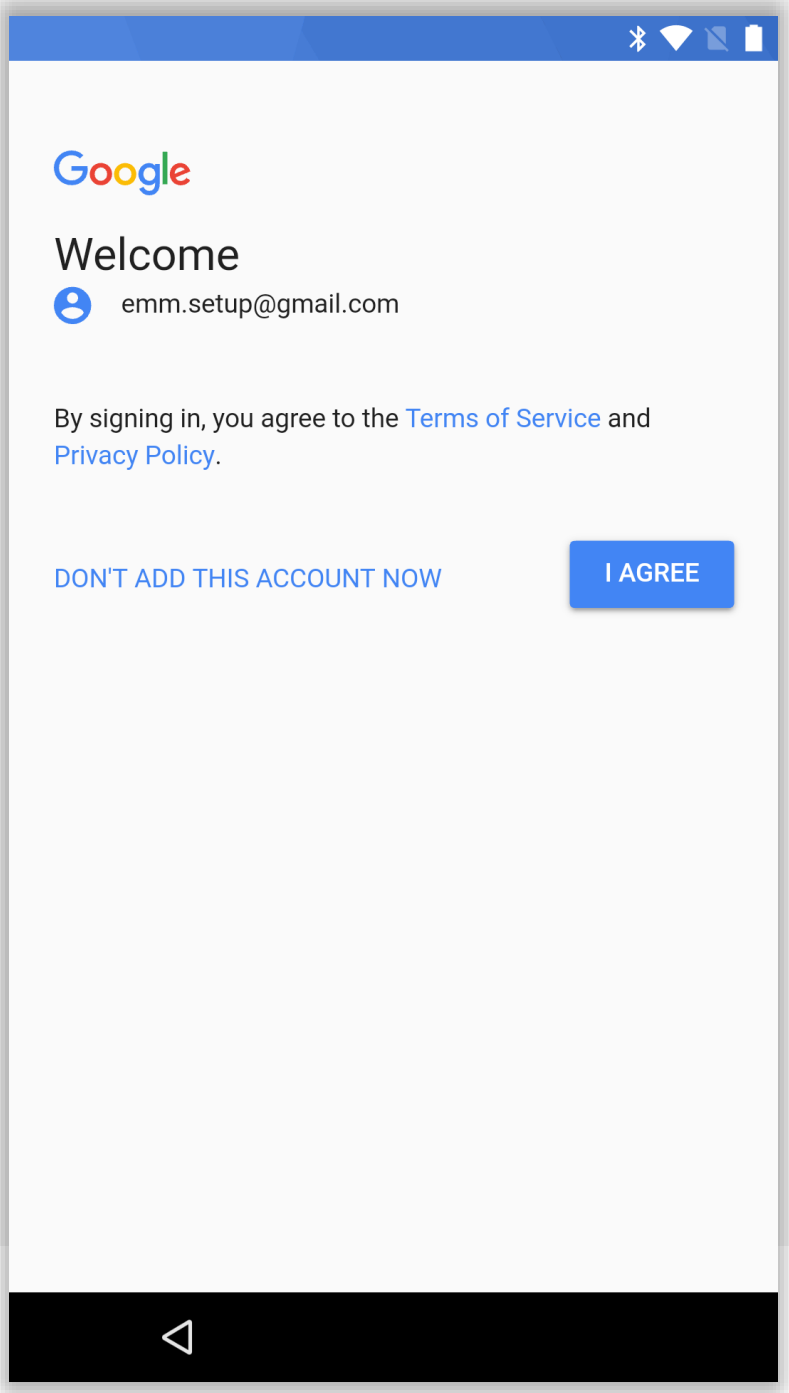
By default, when adding a Google account to an Android device it is set to automatically sync account data. Though it can be disabled manually later, if it is re-enabled for any reason many users may inadvertently share their contacts, calendars, histories and more with one another. In addition, account tools allowing devices to be located can also be considered an invasion of privacy. Finally, It's against Google's ToS and may result in the account being closed.

bayton

Continue device setup

Once authenticated with the unique Google account, tap I AGREE to continue.

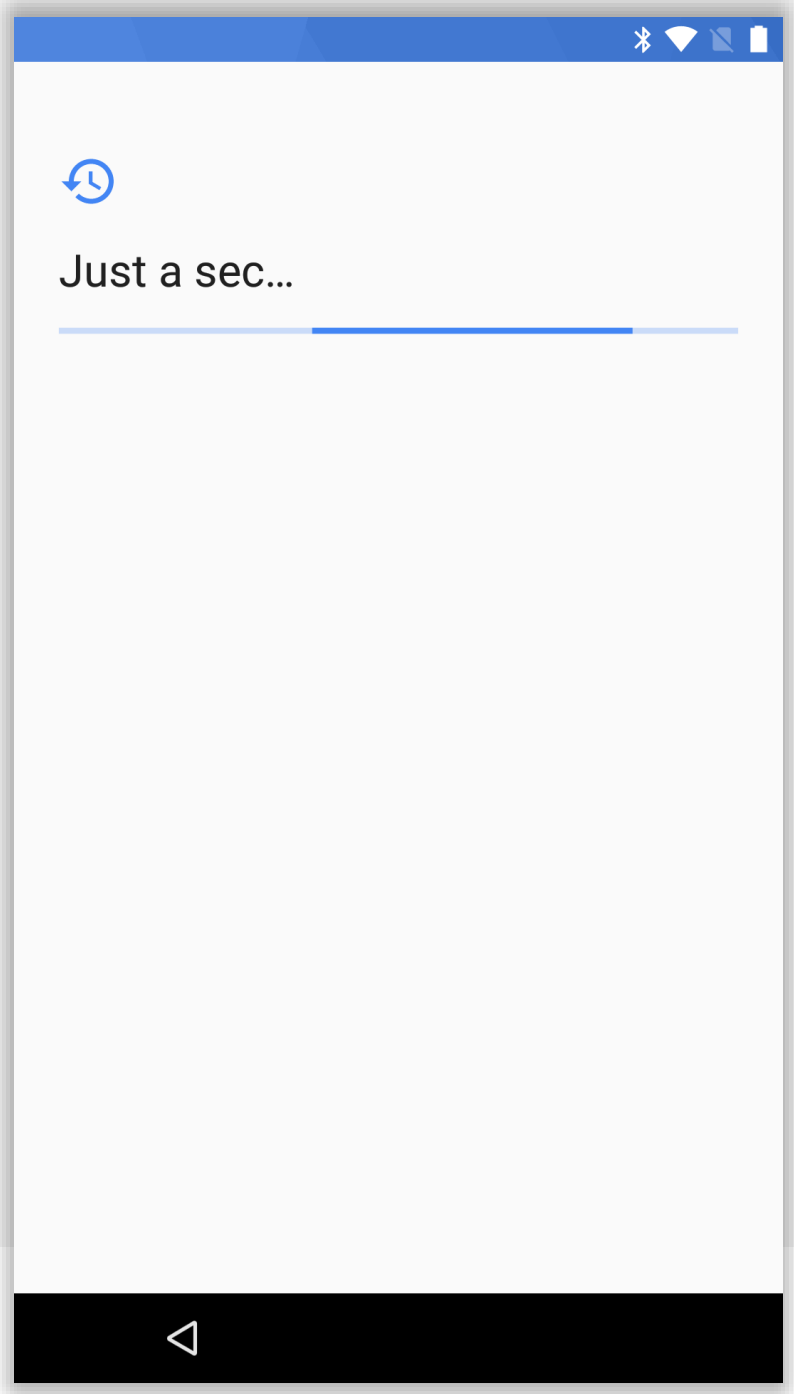
(After reading the ToS and Privacy Policy, naturally).



bayton

Continue device setup

The device will now add the account to the device and automatically continue.



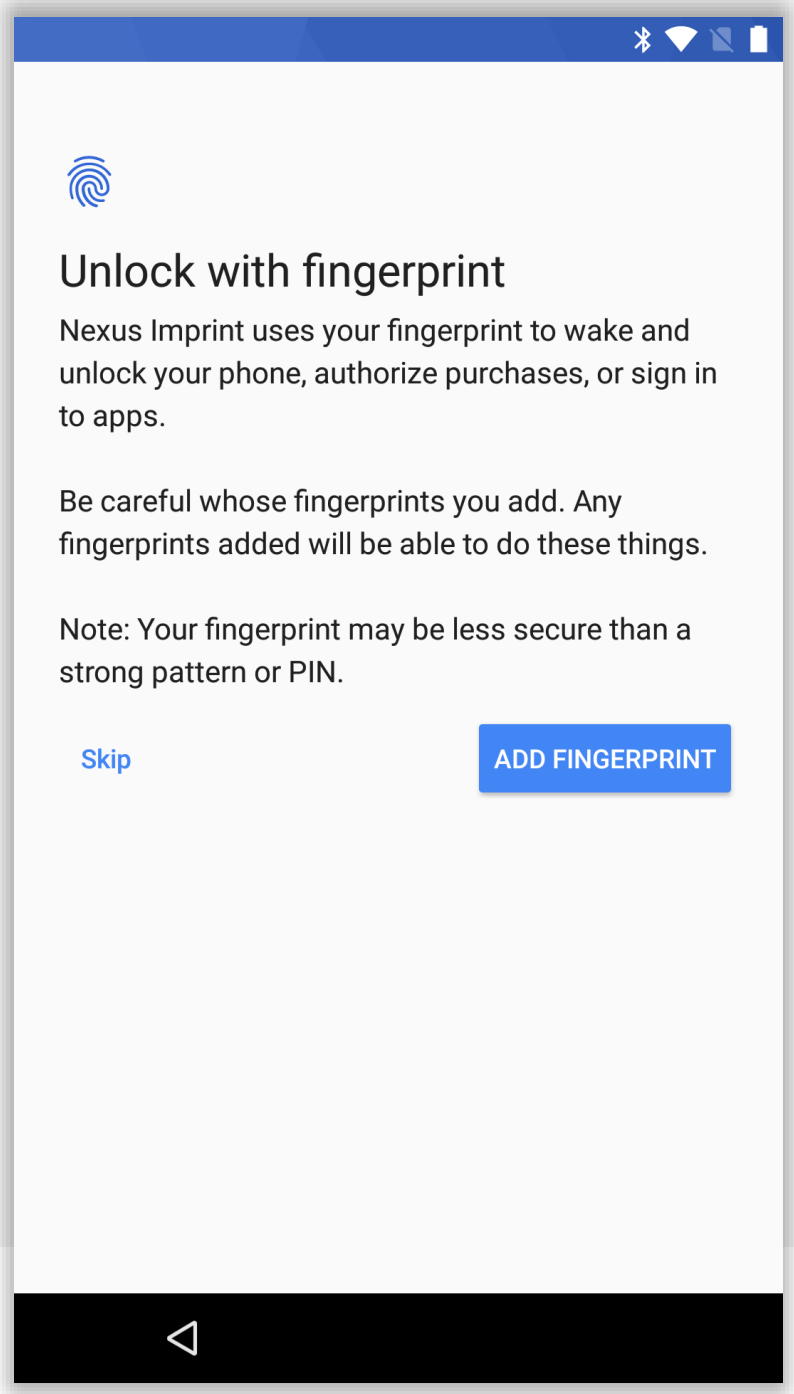
bayton

Continue device setup

Optionally configure fingerprint unlock, if supported. Keep in mind if the backup-passcode configured as part of fingerprint setup does not conform to corporate policies, you will be prompted to set a stronger passcode again later.

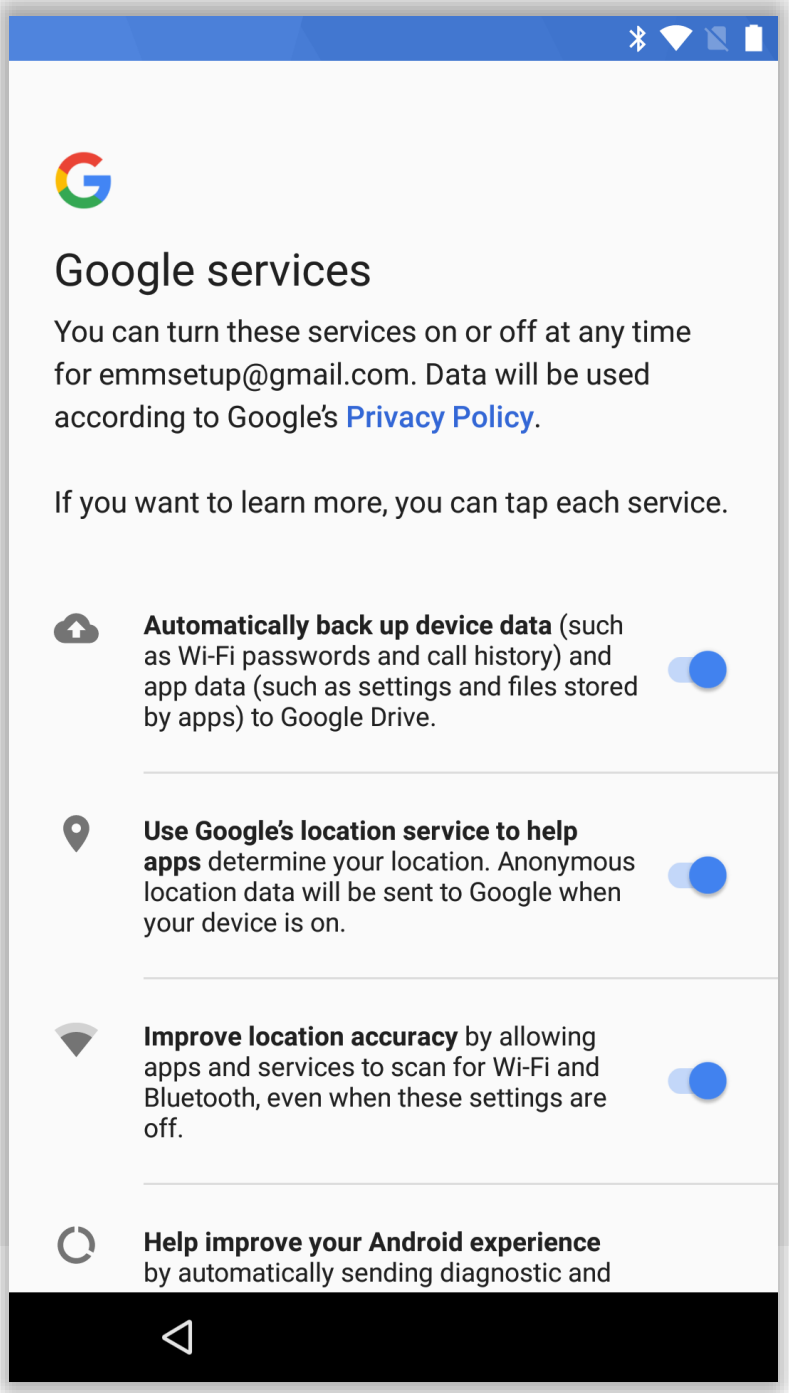
Tap ADD FINGERPRINT to begin this process, or Skip to continue.

Note: Fingerprint setup is not documented in this guide as it is assumed corporate passcode policies are in place which may block its use. Passcode setup is documented in the following pages and as such the next page in this guide assumes Skip has been tapped.



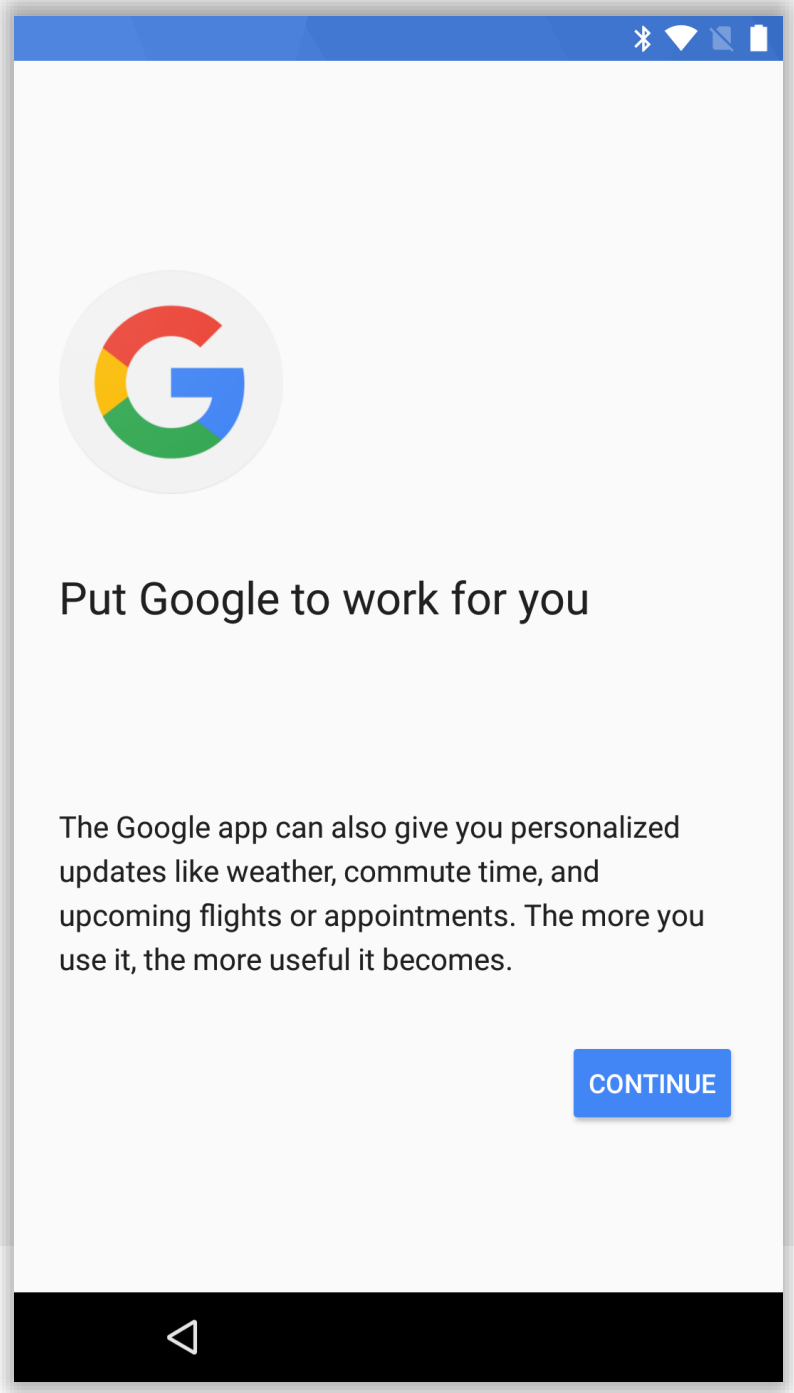
Continue device setup

Disable relevant services and tap **NEXT** to continue to the next step.



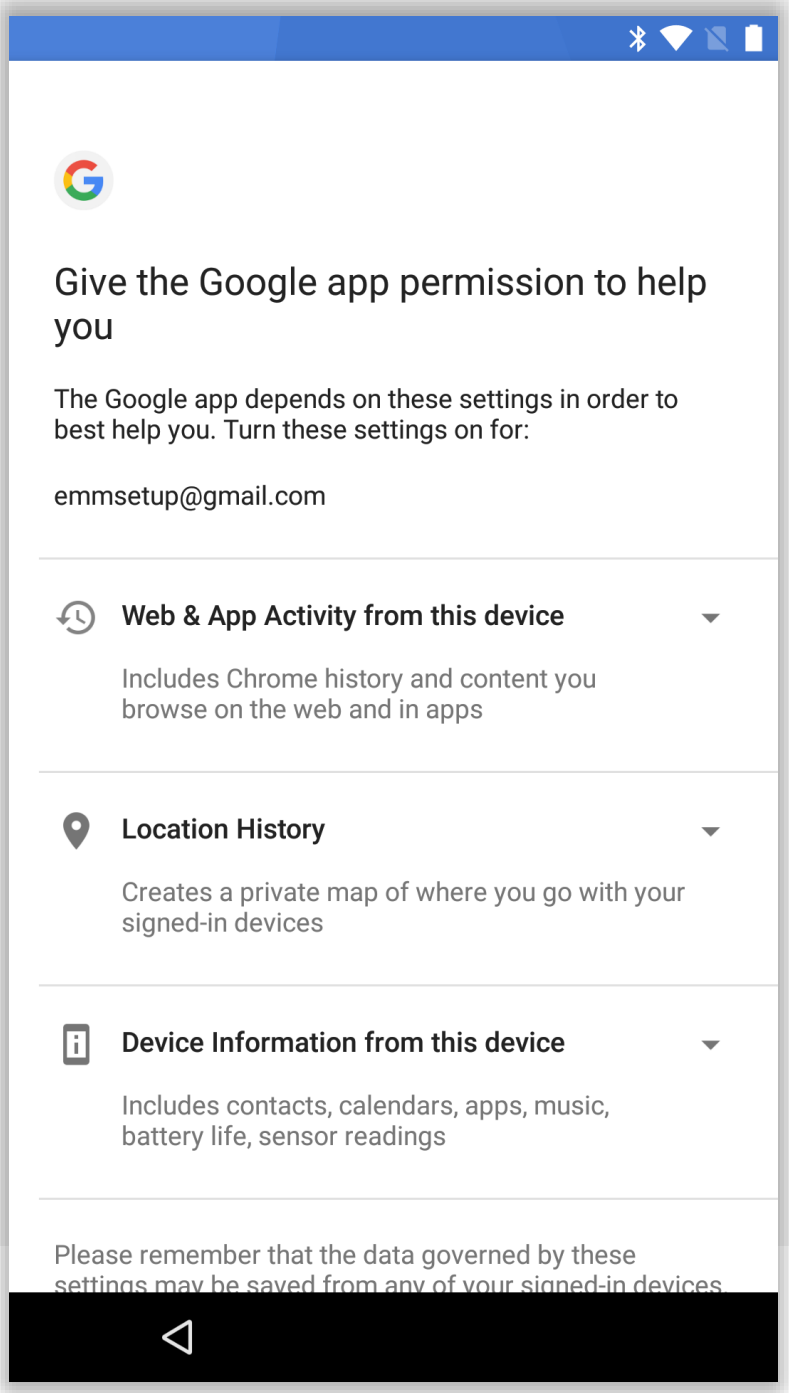
Continue device setup

Tap **CONTINUE** to progress to the next step.



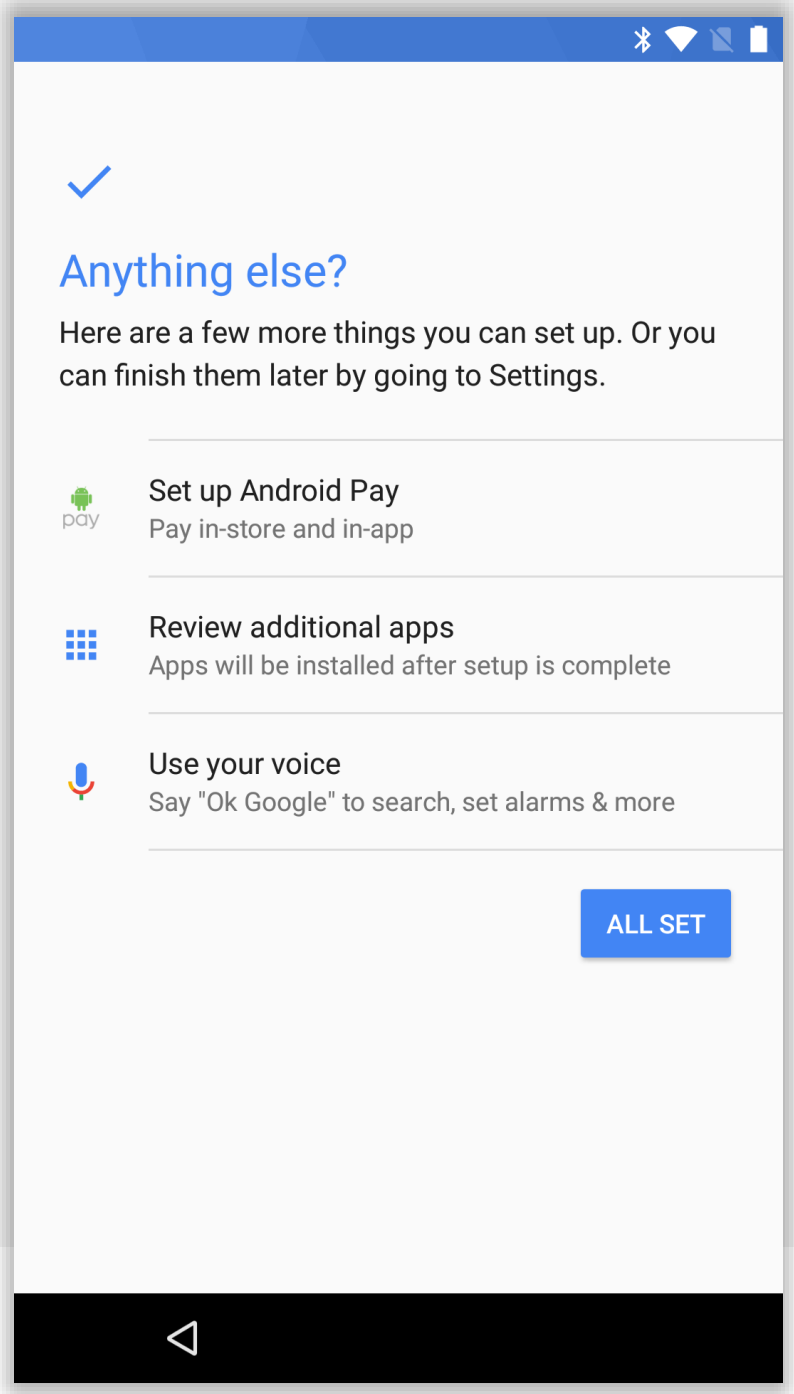
Continue device setup

If the Google app is desired, tap **YES I'M IN**, otherwise tap **No Thanks** to continue to the next step.



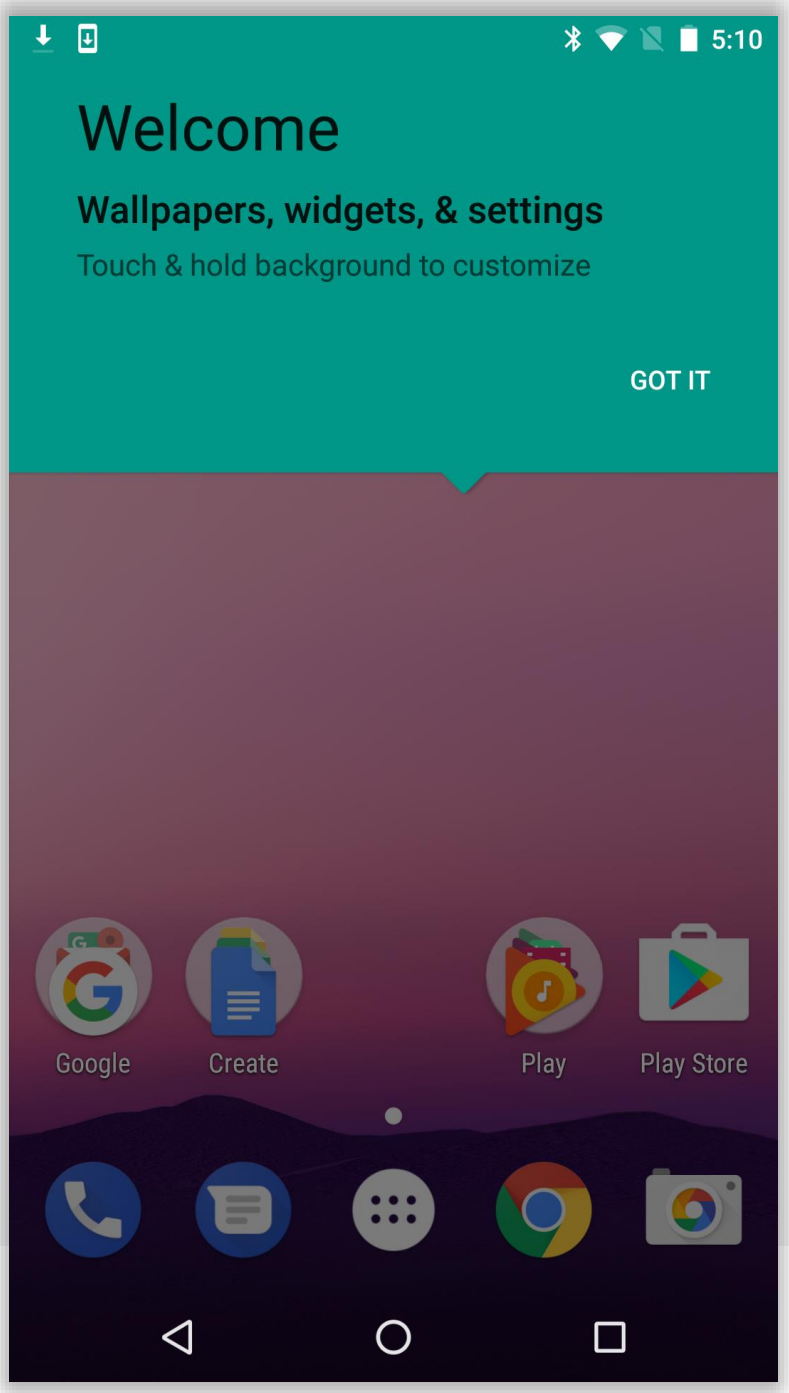
Continue device setup

Tap **ALL SET** to exit the Wizard.



Device setup complete

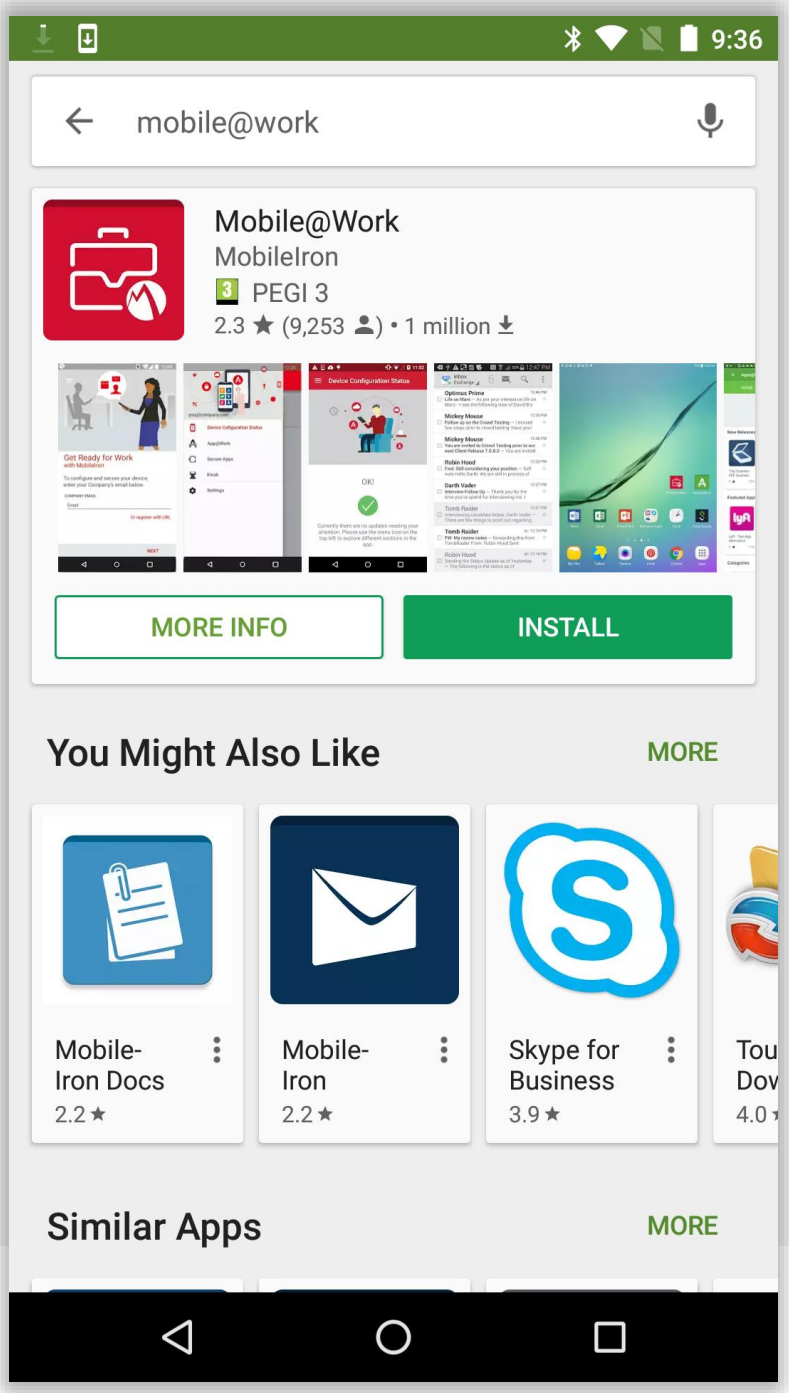
From the home screen, tap **GOT IT**, then open the Play Store.



bayton

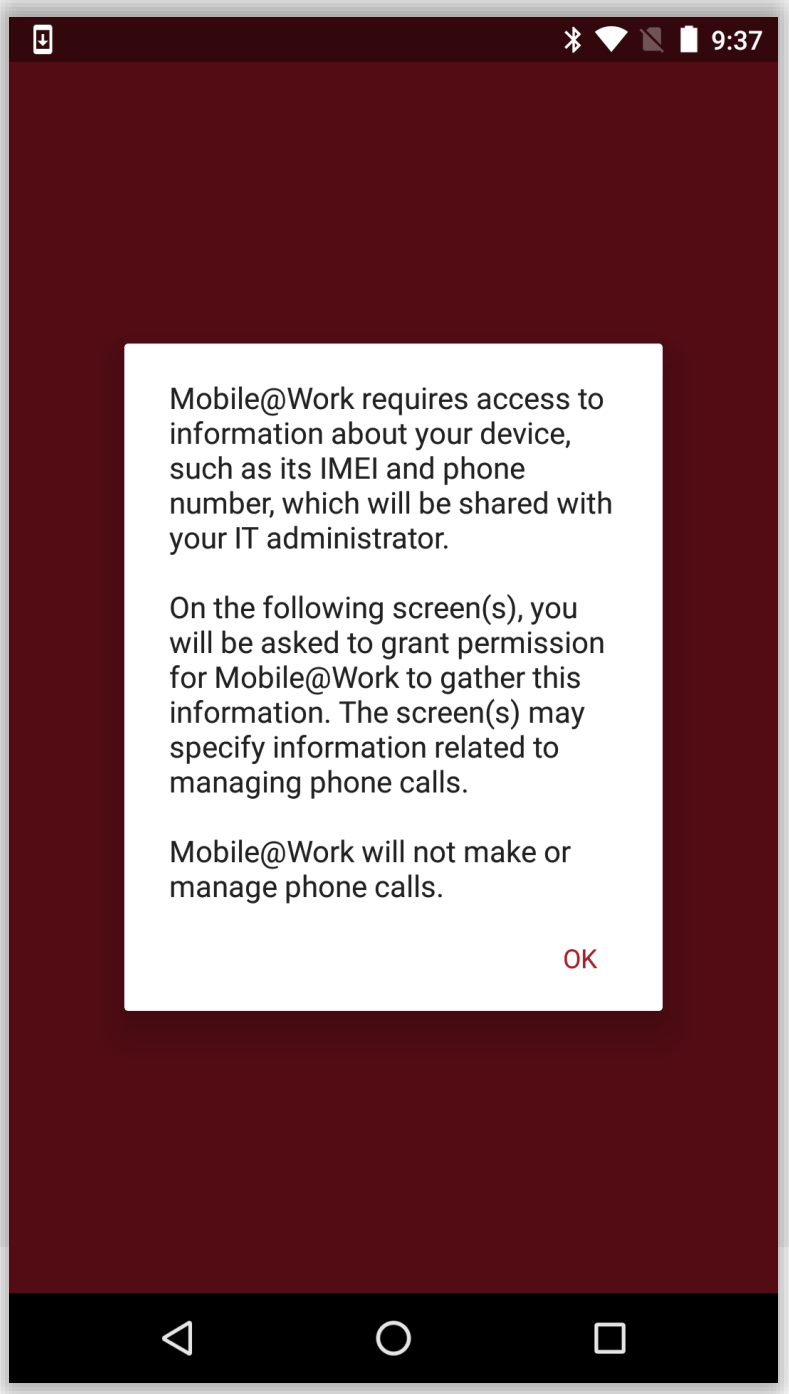
Install the DPC

Search for Mobile@Work and tap **INSTALL** when located.



Open the DPC

Once installed, open Mobile@Work and tap **OK** to agree to the prompt for permissions.

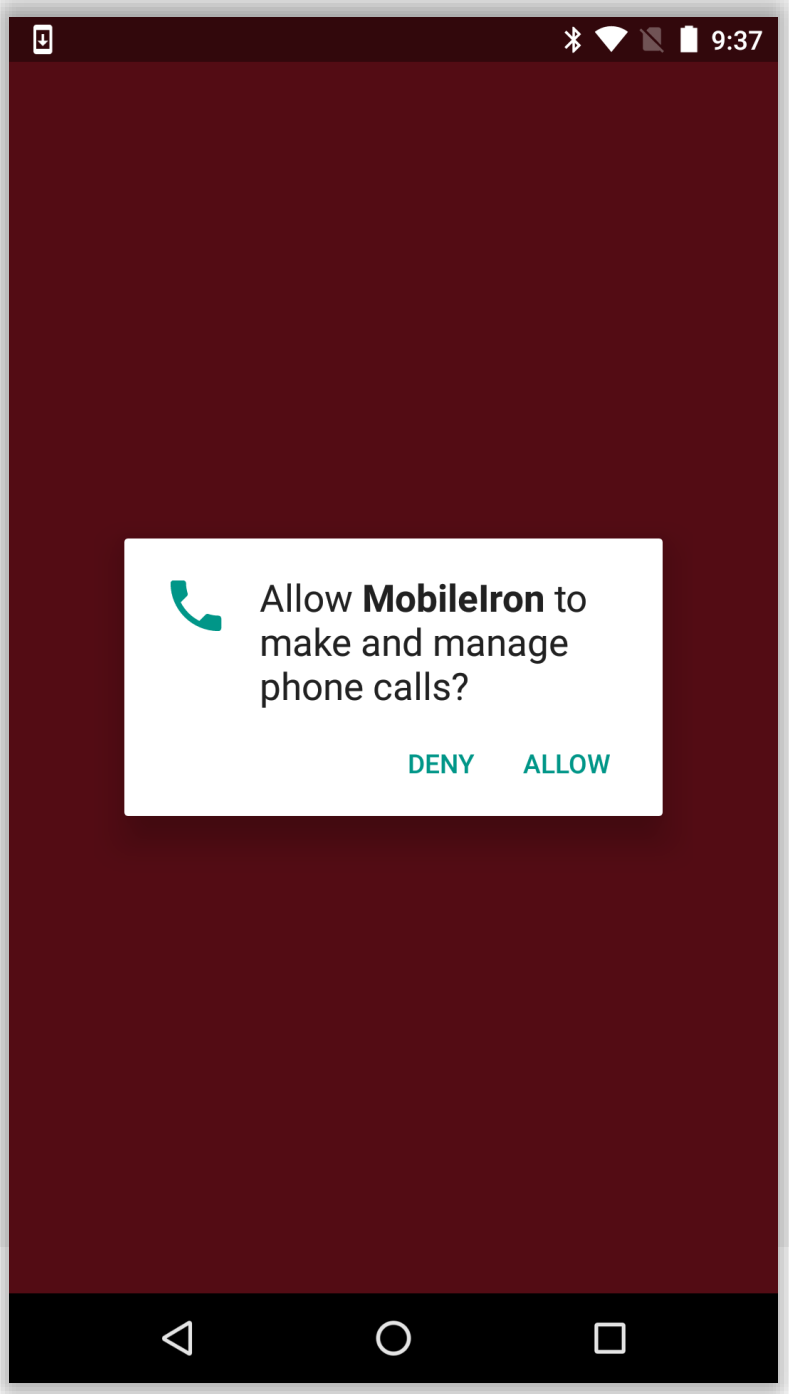


bayton

Grant permissions

Grant MobileIron the requested permissions.

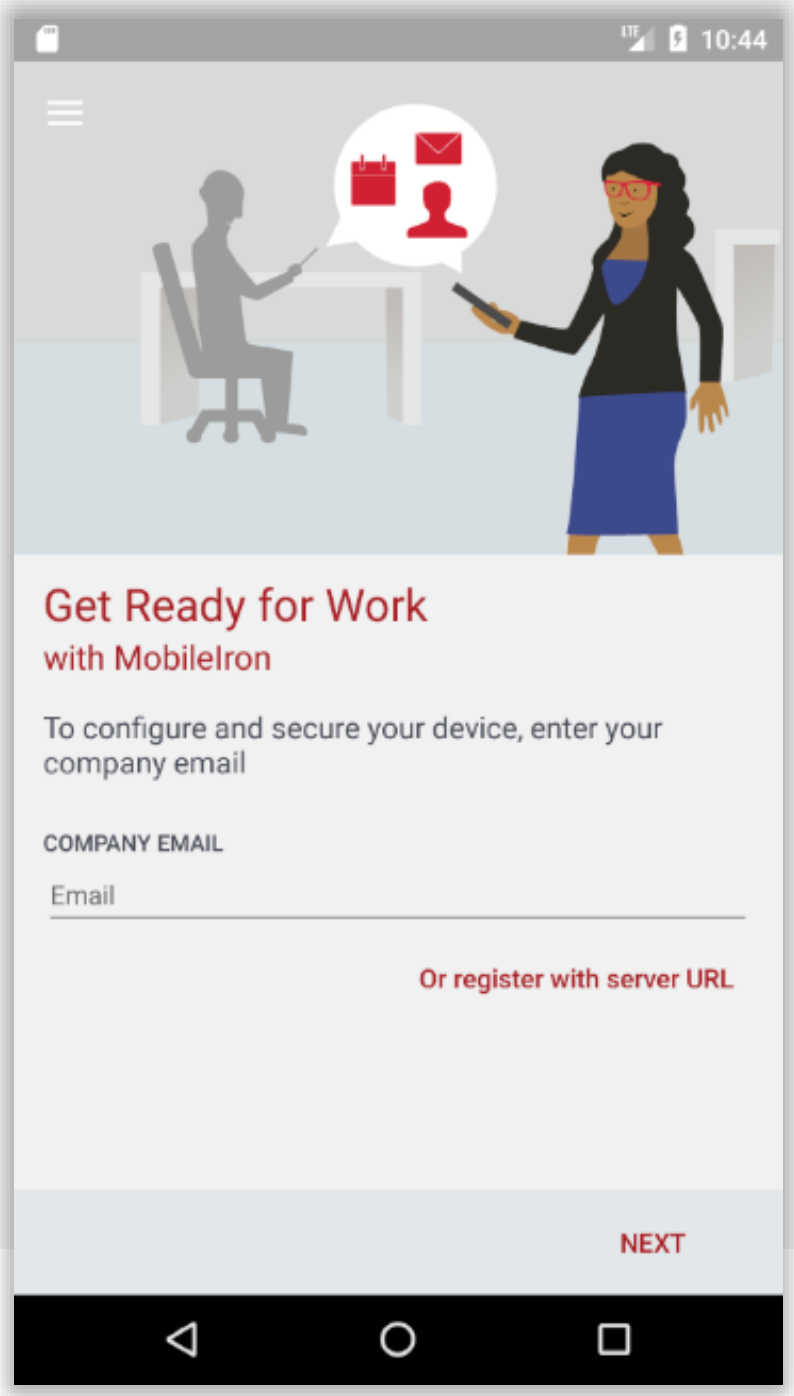
Tap **ALLOW**.



Begin enrolment

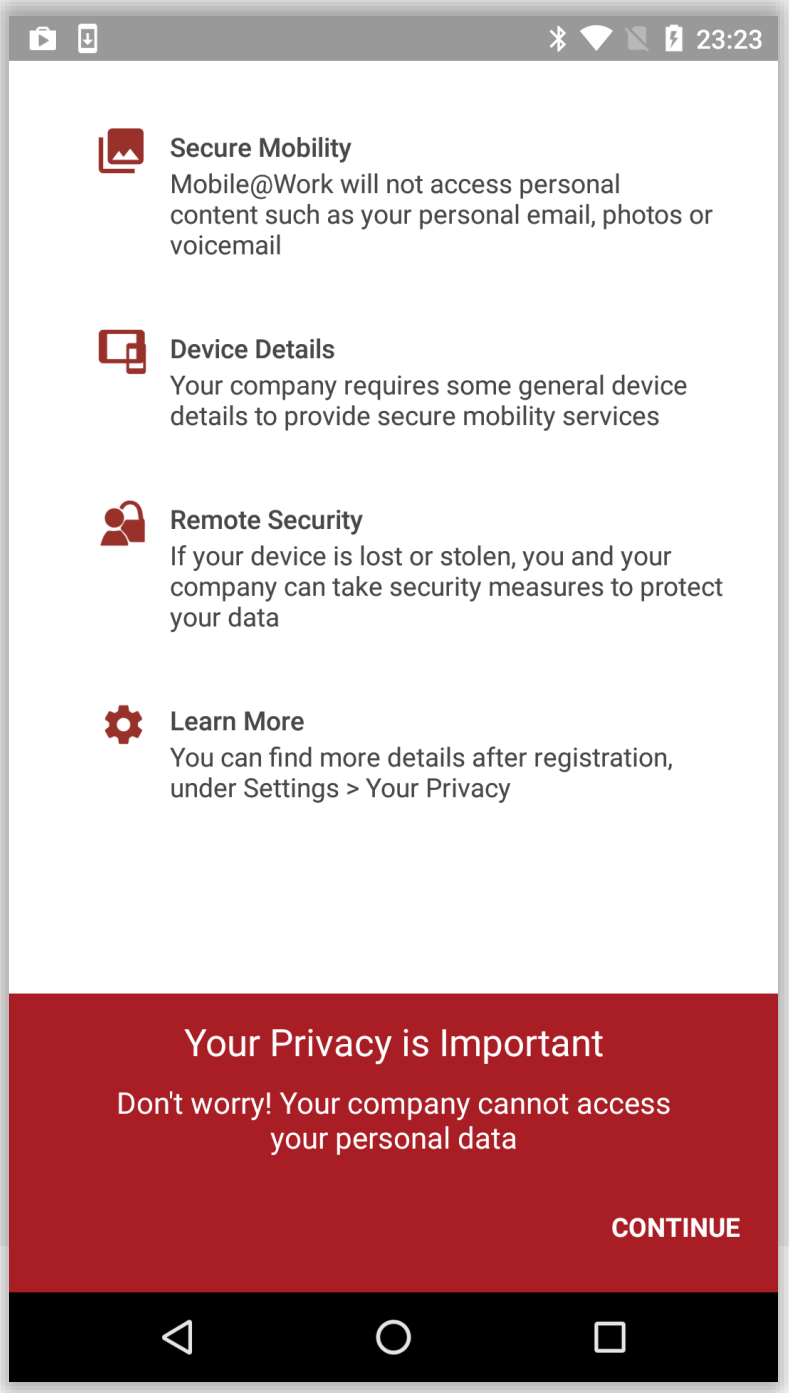
Input your email address (or switch to server URL if required).

Tap **NEXT**.



Continue enrolment

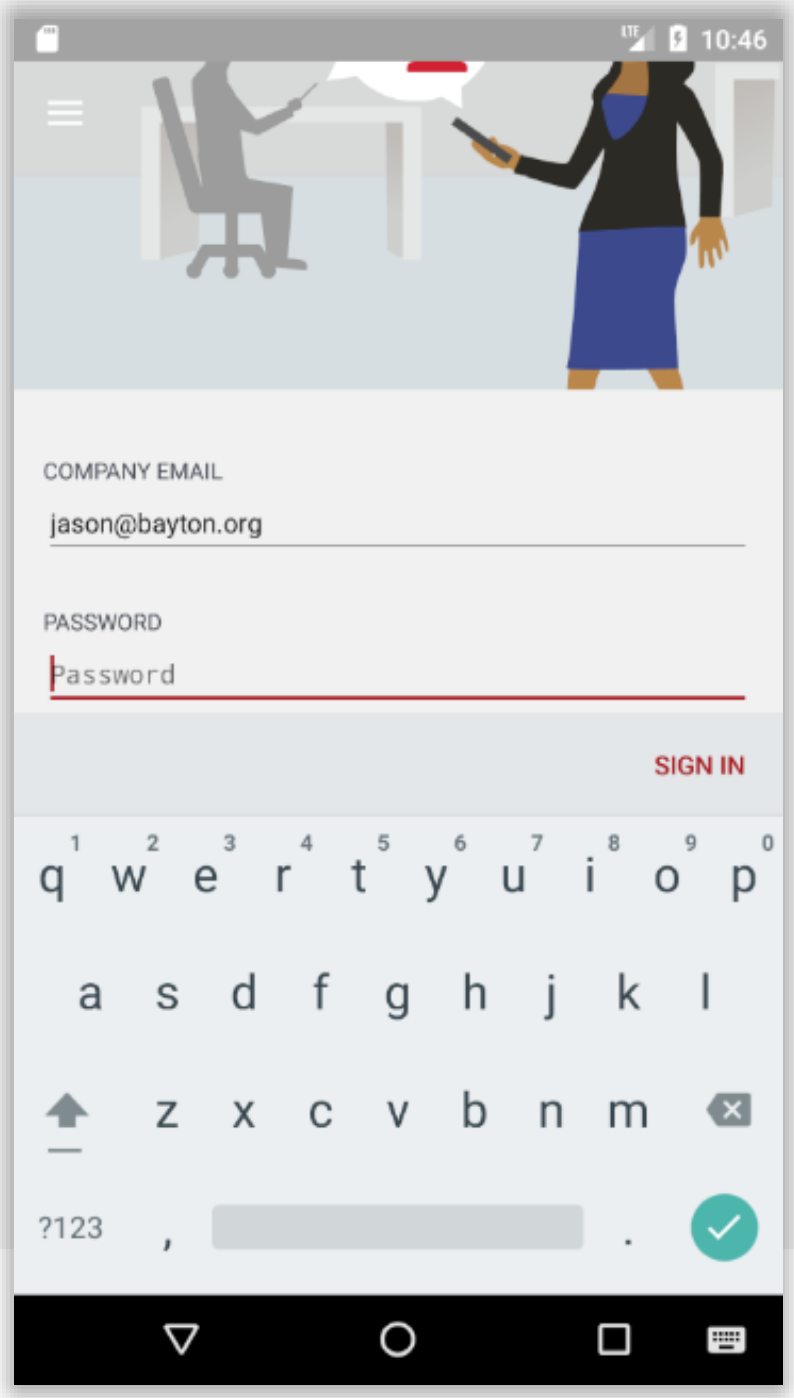
Accept the privacy alert by tapping **CONTINUE**.



Continue enrolment

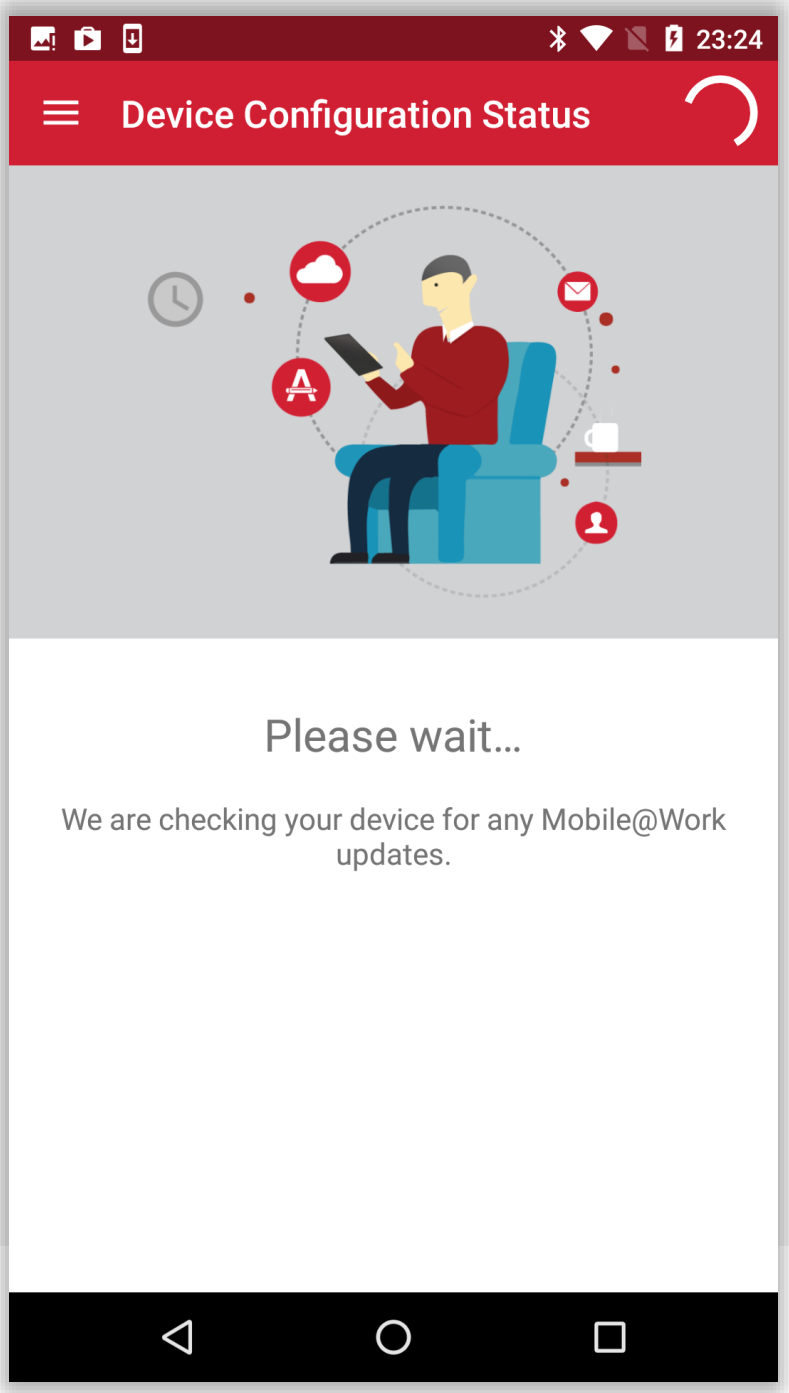
When your account has been found and validated, you'll be prompted for your password, PIN or both.

Enter the required fields and tap SIGN IN.



Device configuration

The DPC will now configure the device, bringing down the relevant policies and configurations.

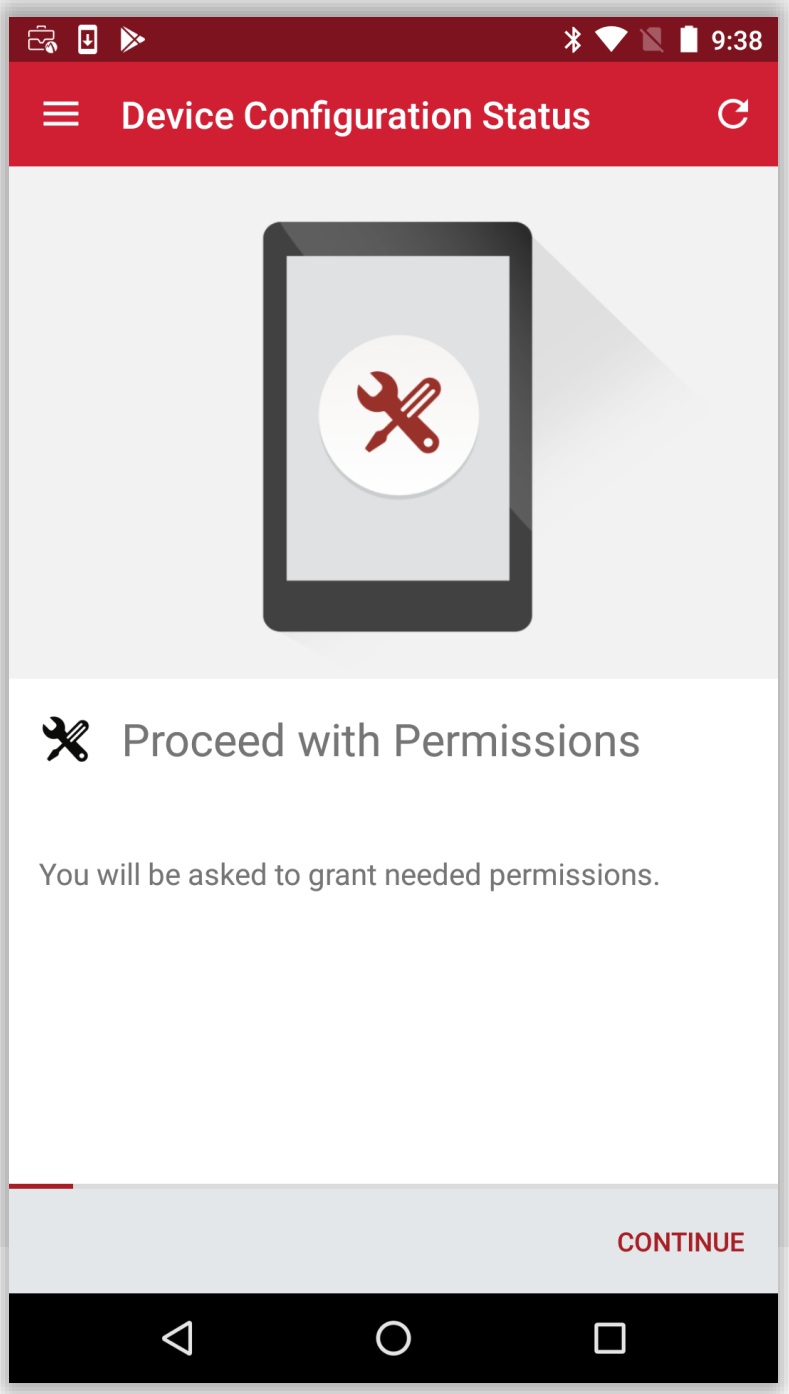


bayton

Device configuration

Once authenticated, MobileIron will request further permissions to effectively manage the device.

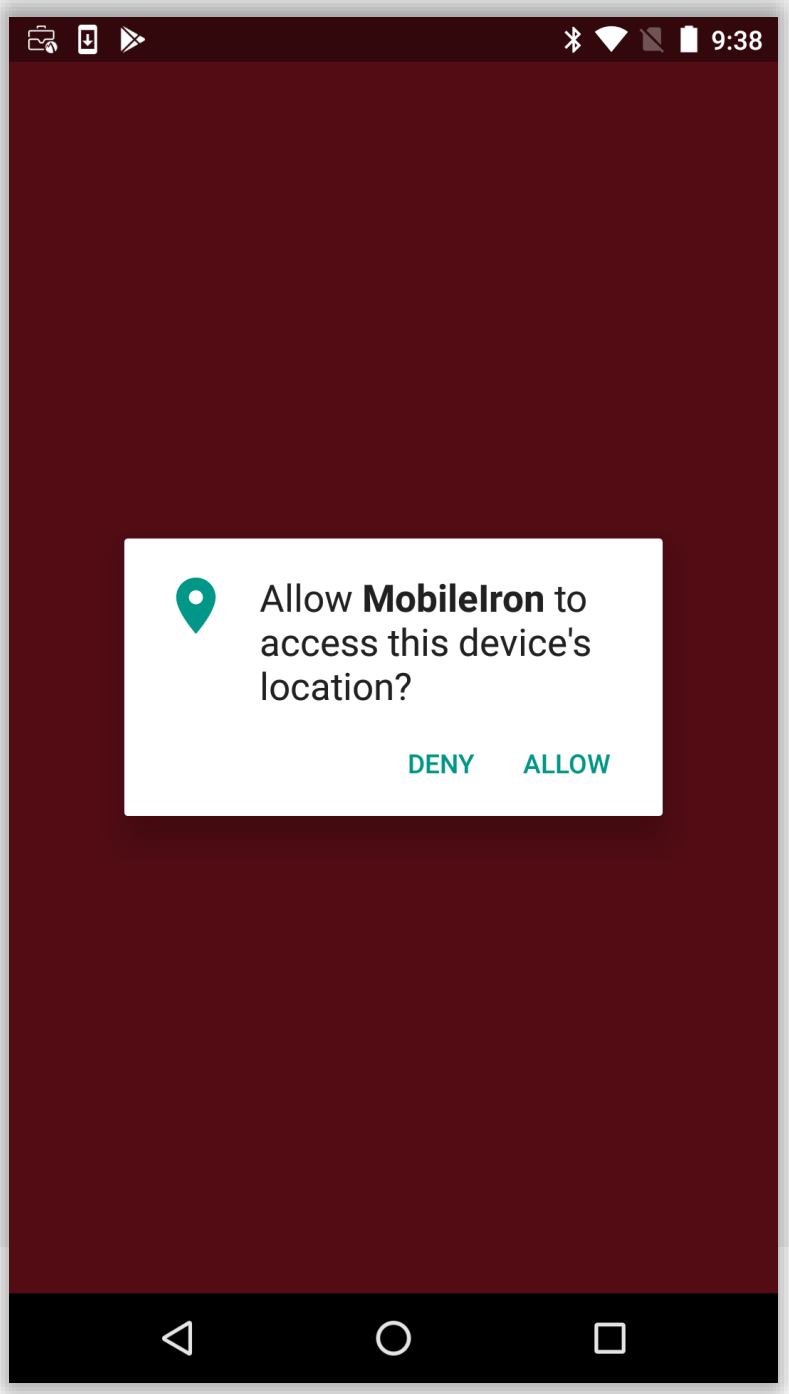
Tap **CONTINUE.**



Grant permissions

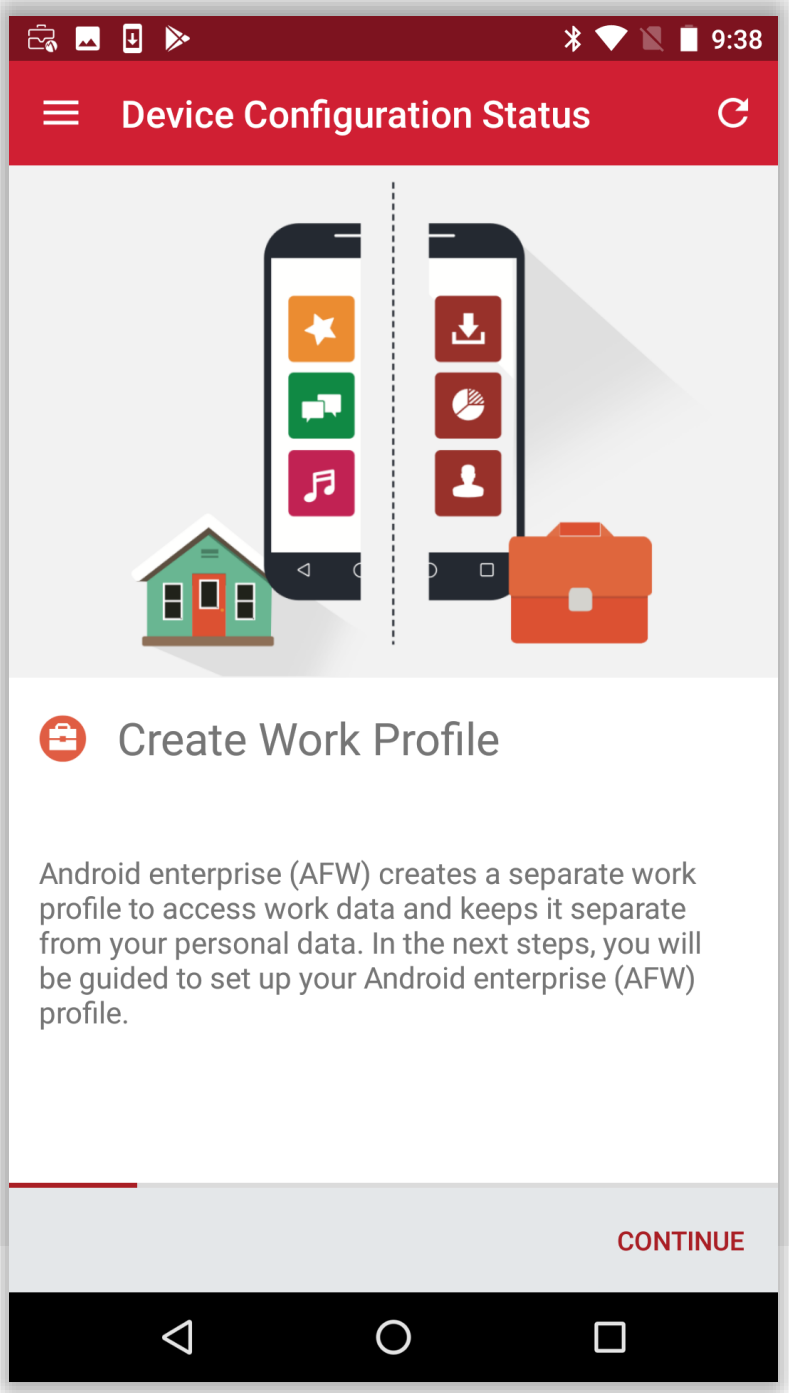
Grant MobileIron the requested permissions.

Tap **ALLOW**.



Work Profile setup

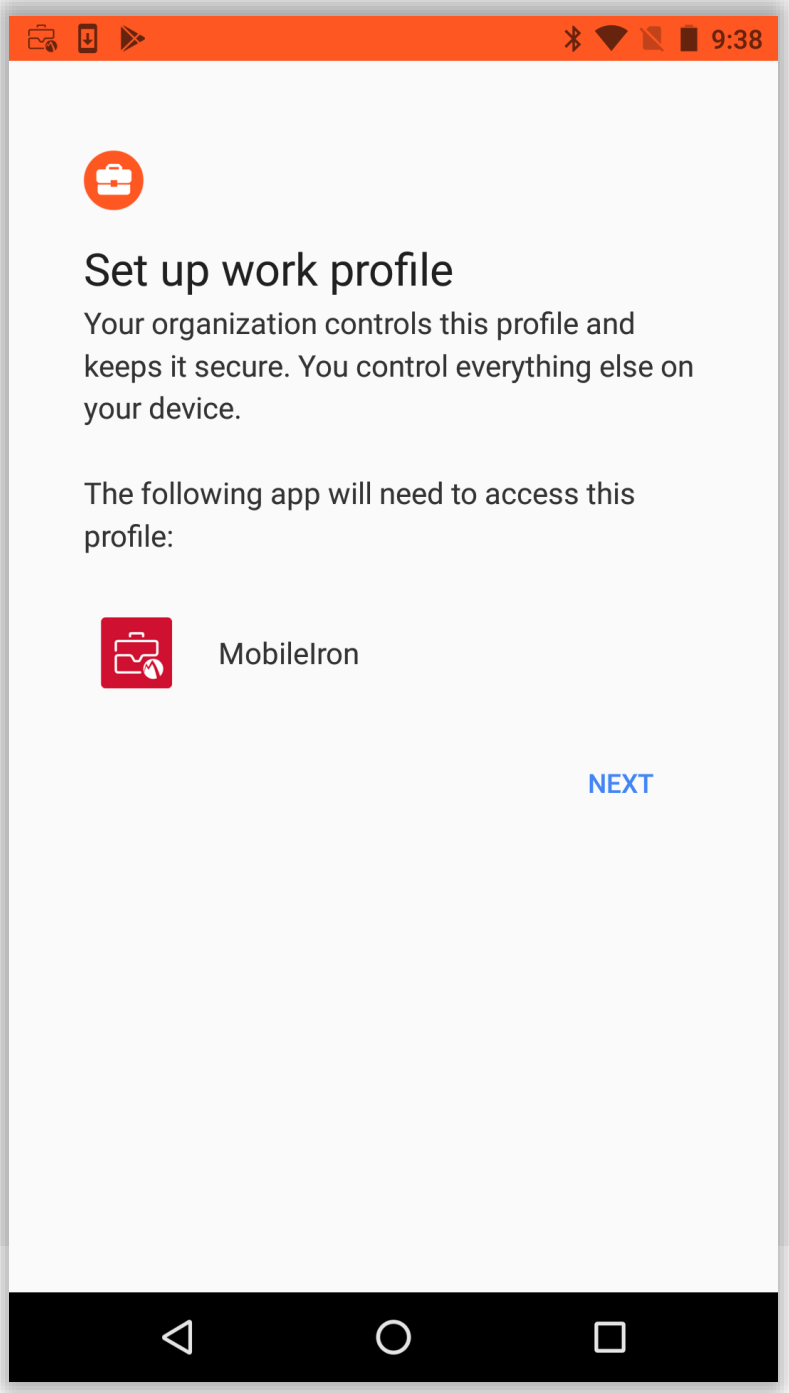
At this point Android enterprise setup initiates. By tapping **CONTINUE**, a new, corporately-managed profile (not dissimilar to a secondary user profile) will be created.



bayton

Work Profile setup

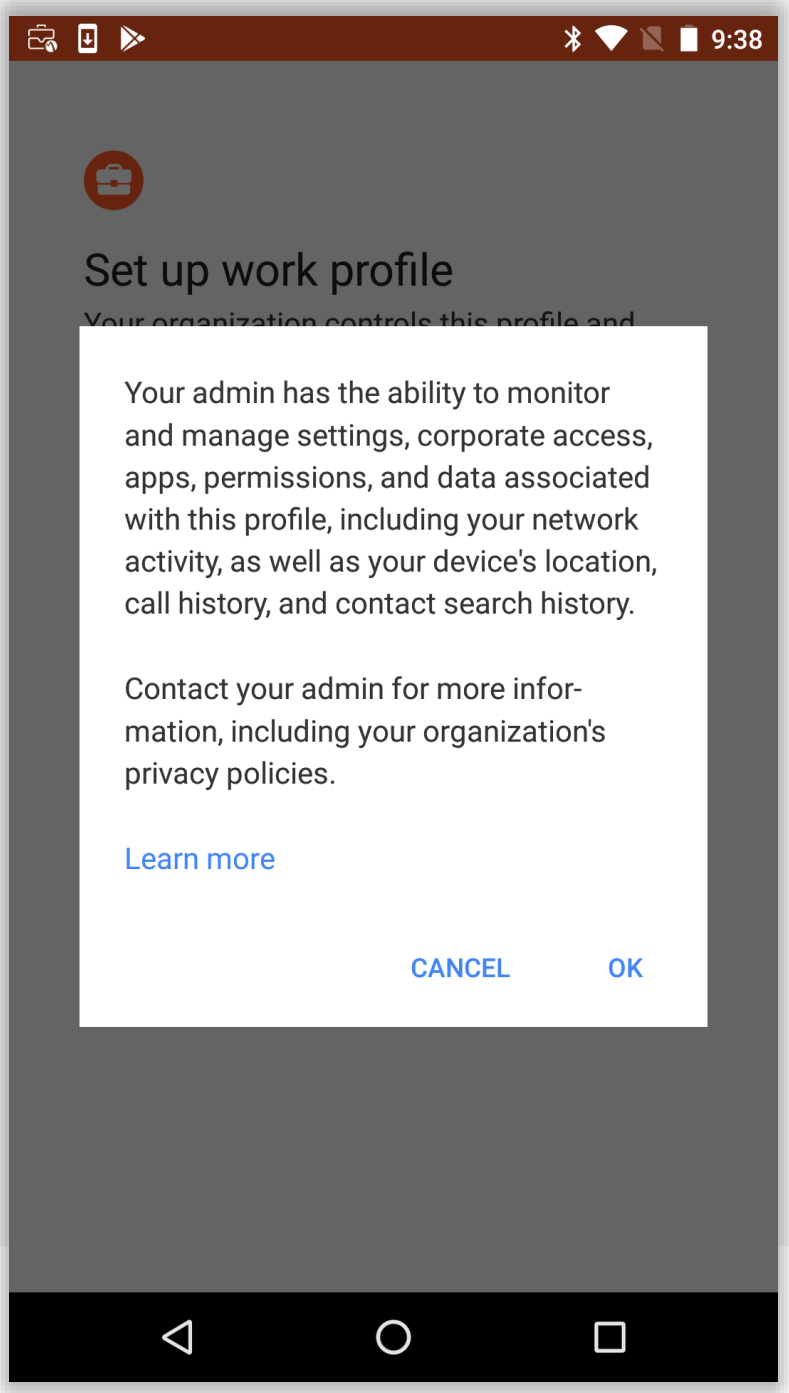
Grant MobileIron the requested access.



bayton

Work Profile setup

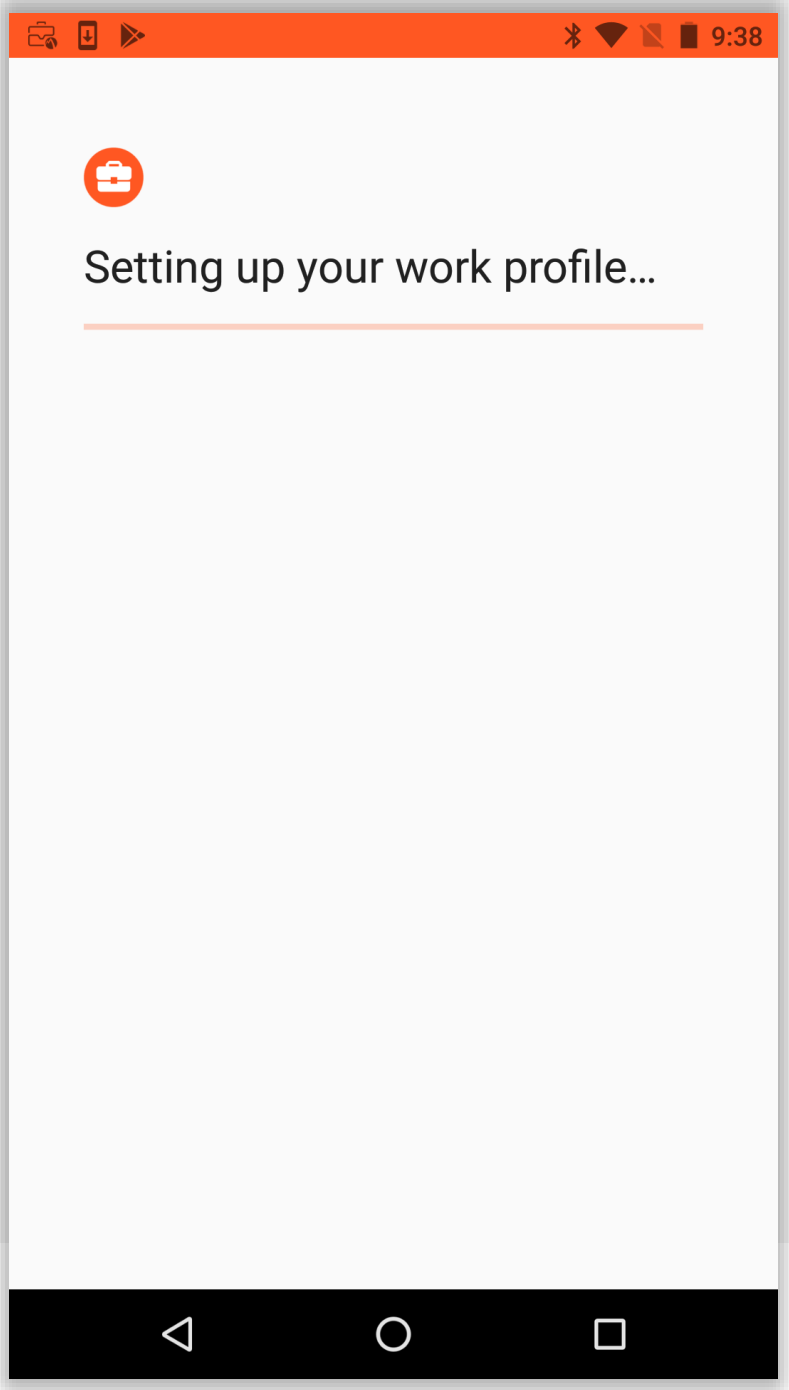
Tap **OK** to accept the privacy alert, or tap **Learn more** for more information about how it works and the monitoring/control capabilities the DPC has.



bayton

Work Profile setup

The Work Profile is being created. This will automatically progress to the next step.

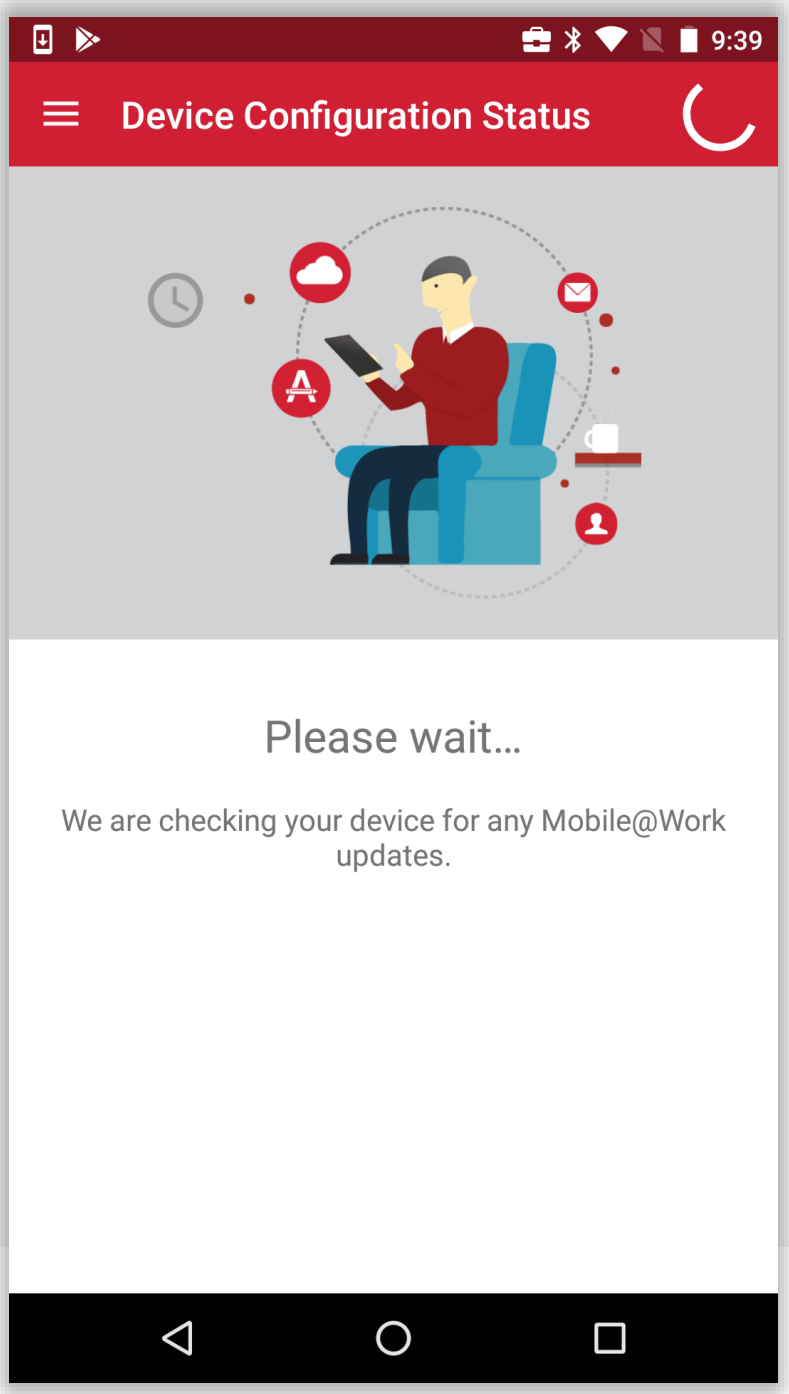


bayton

Work Profile setup

At this point the DPC will disable on the personal profile and open automatically in the Work Profile. Expect the DPC to vanish and relaunch.

MobileIron will check for any further policies or configurations to be applied to the **device** (not the Work Profile) before the Work Profile configuration is completed.

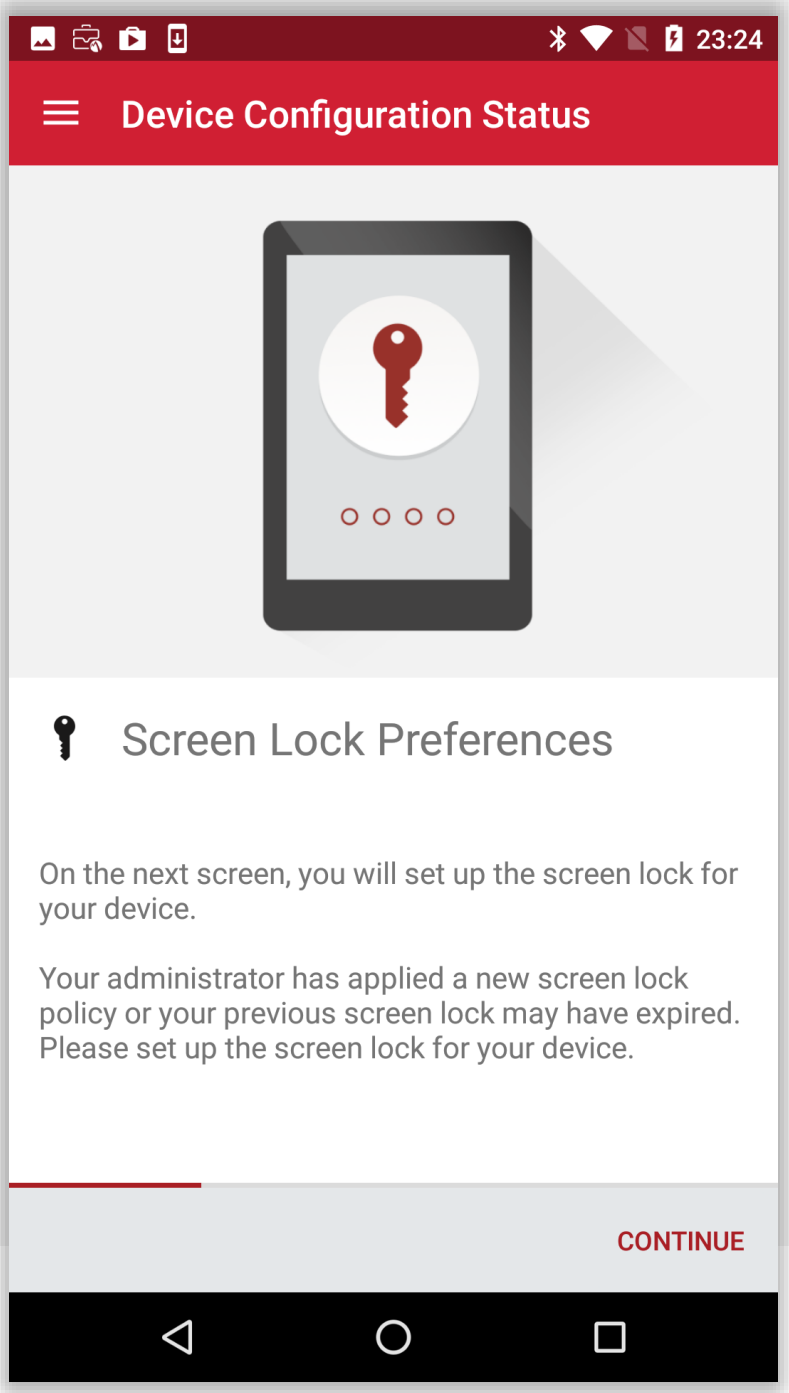


bayton

Device configuration

If the relevant security policy has been deployed, a passcode will be required.

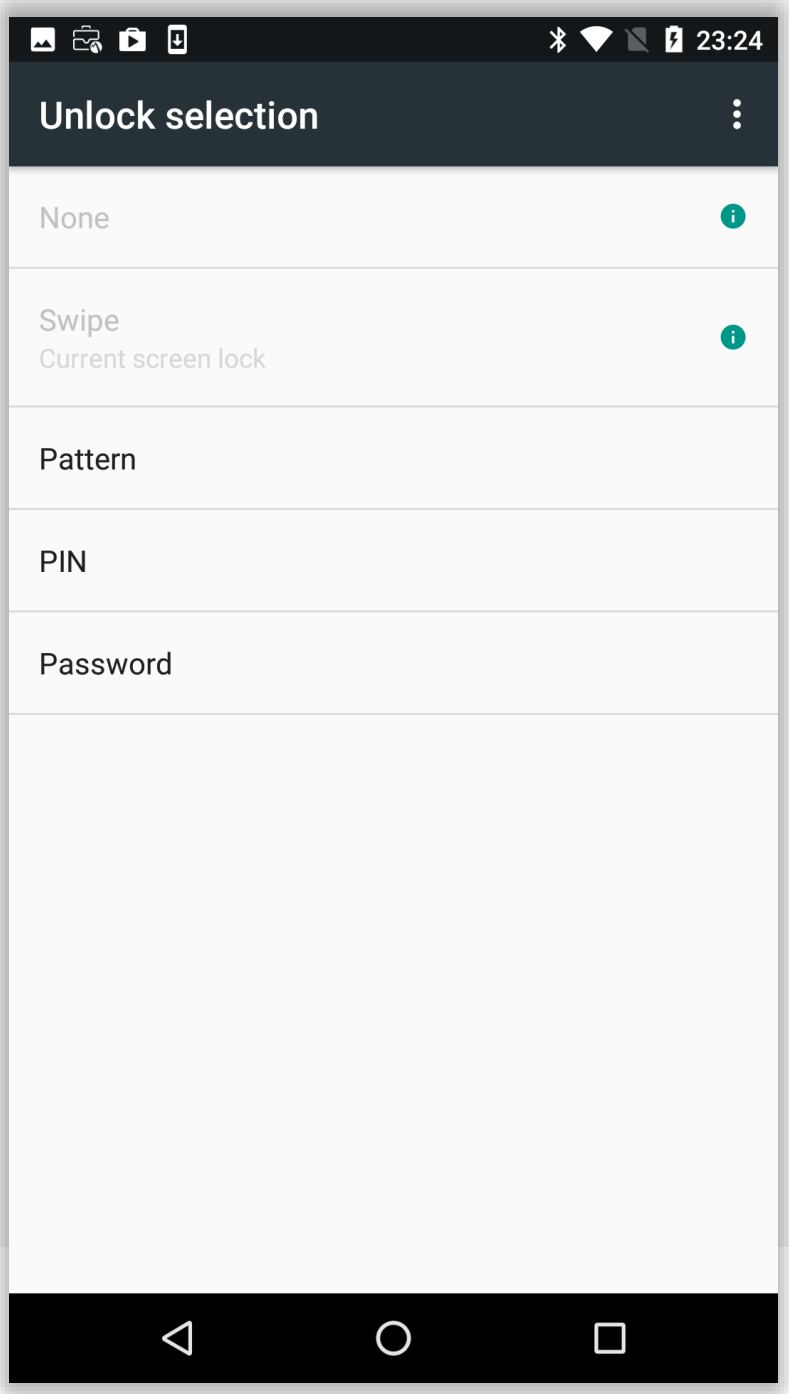
The type of passcode mandated may not be a PIN as depicted in the following steps. The process however is similar for all alpha/numeric passcode options.



bayton

Device configuration

Select the relevant passcode, some options may not be available depending on the security policy deployed.

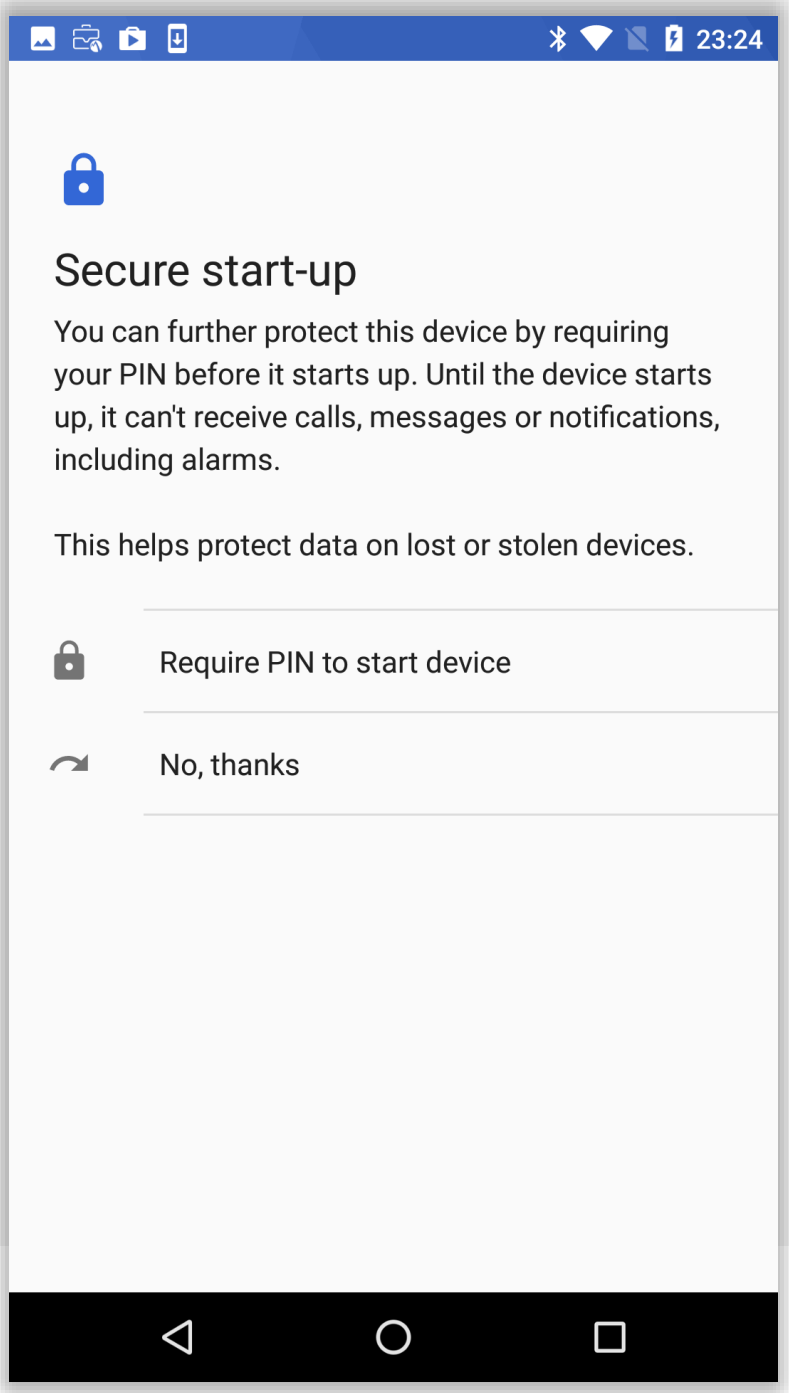


bayton

Device configuration

Before inputting a passcode, the device may display a prompt to opt in to secure start-up.

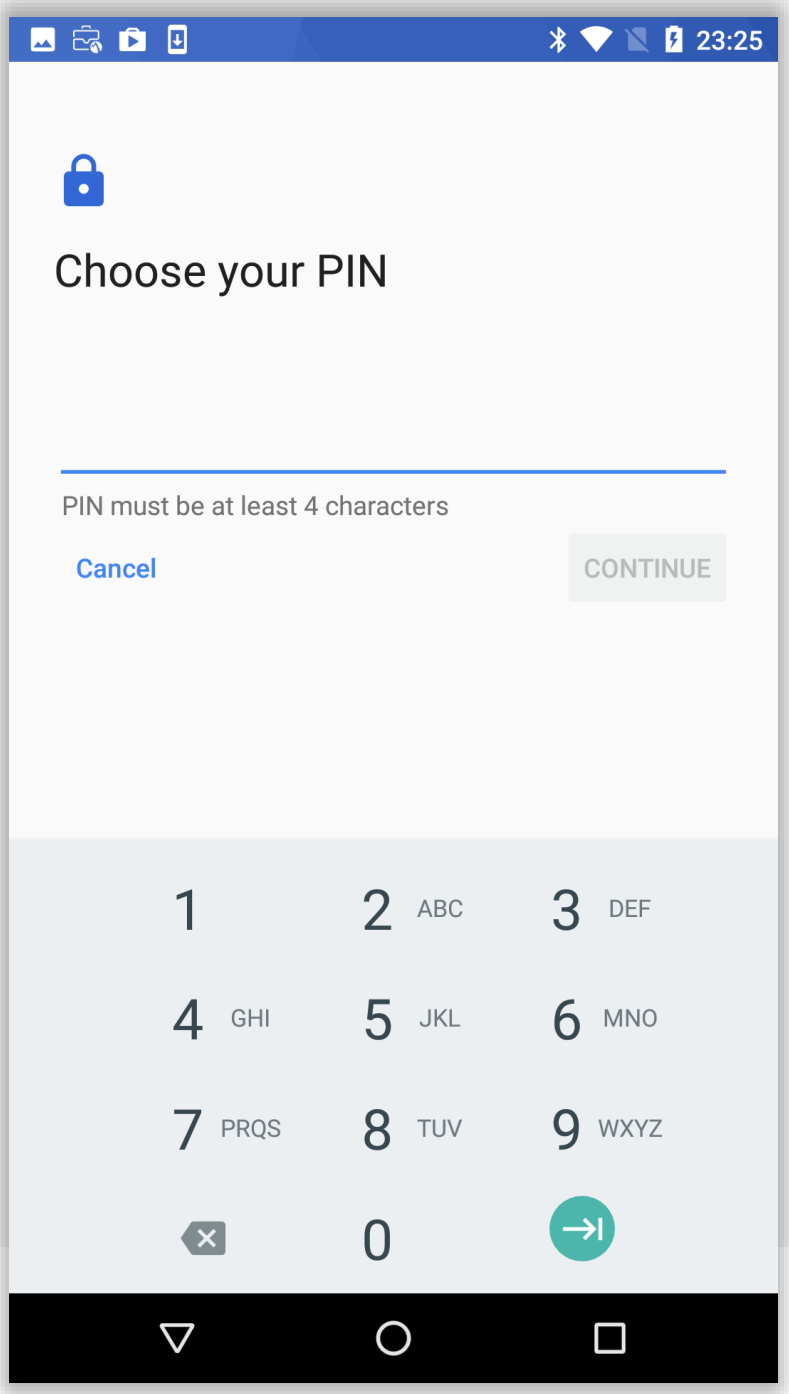
While it is more secure to require the passcode on device boot, it will result in a longer boot process.



bayton

Device configuration

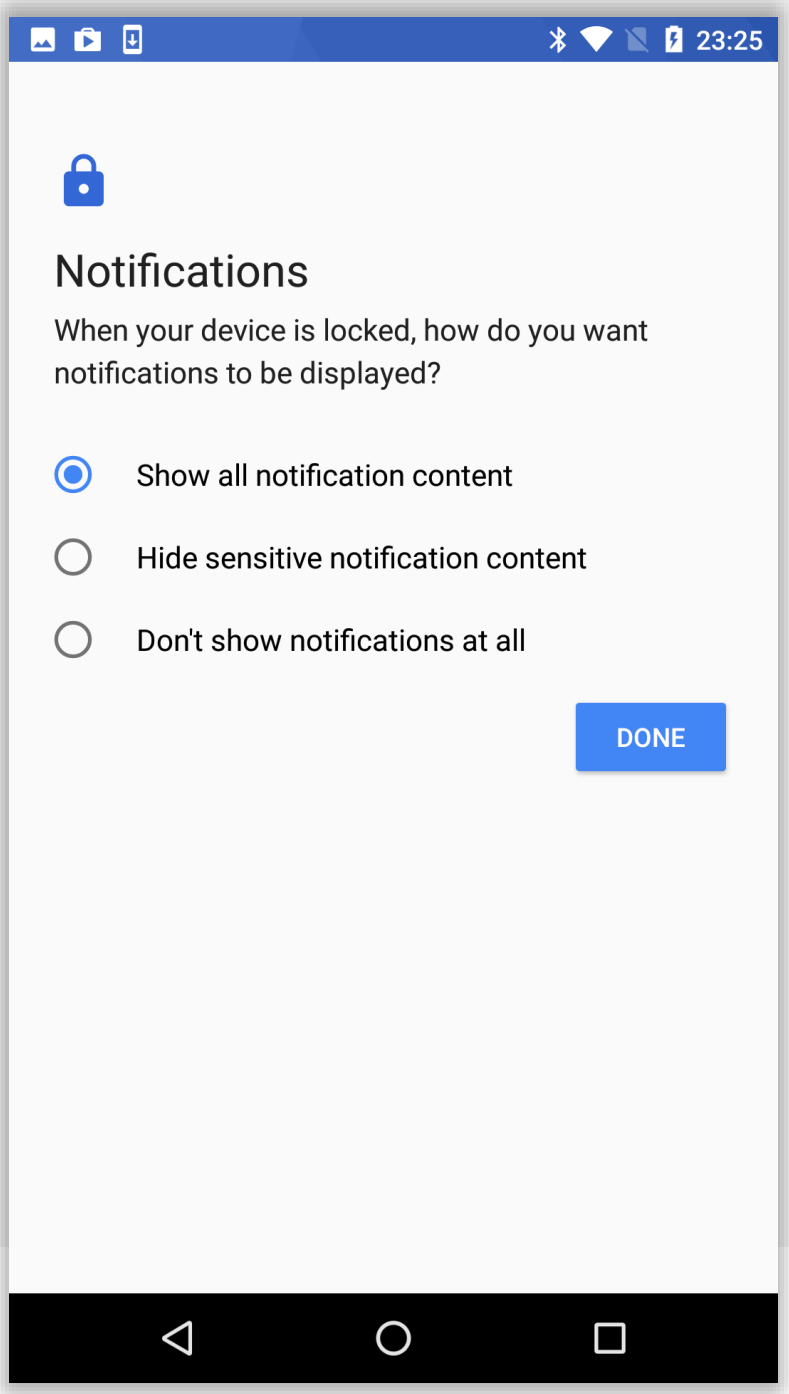
Input a PIN (or other passcode type) and tap **CONTINUE**.
Repeat to confirm.



bayton

Device configuration

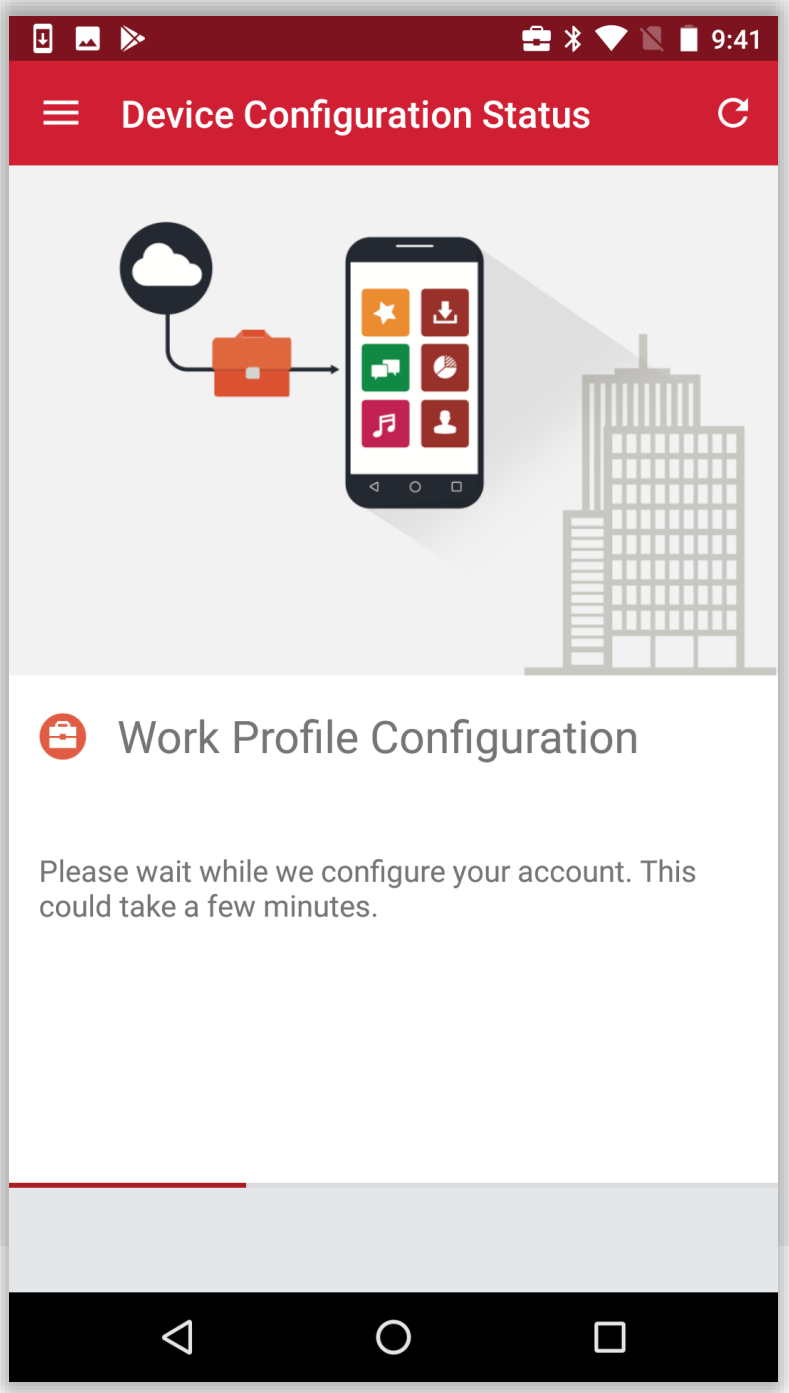
Permit or prohibit notification content and tap **DONE**.



bayton

Finalising Work Profile

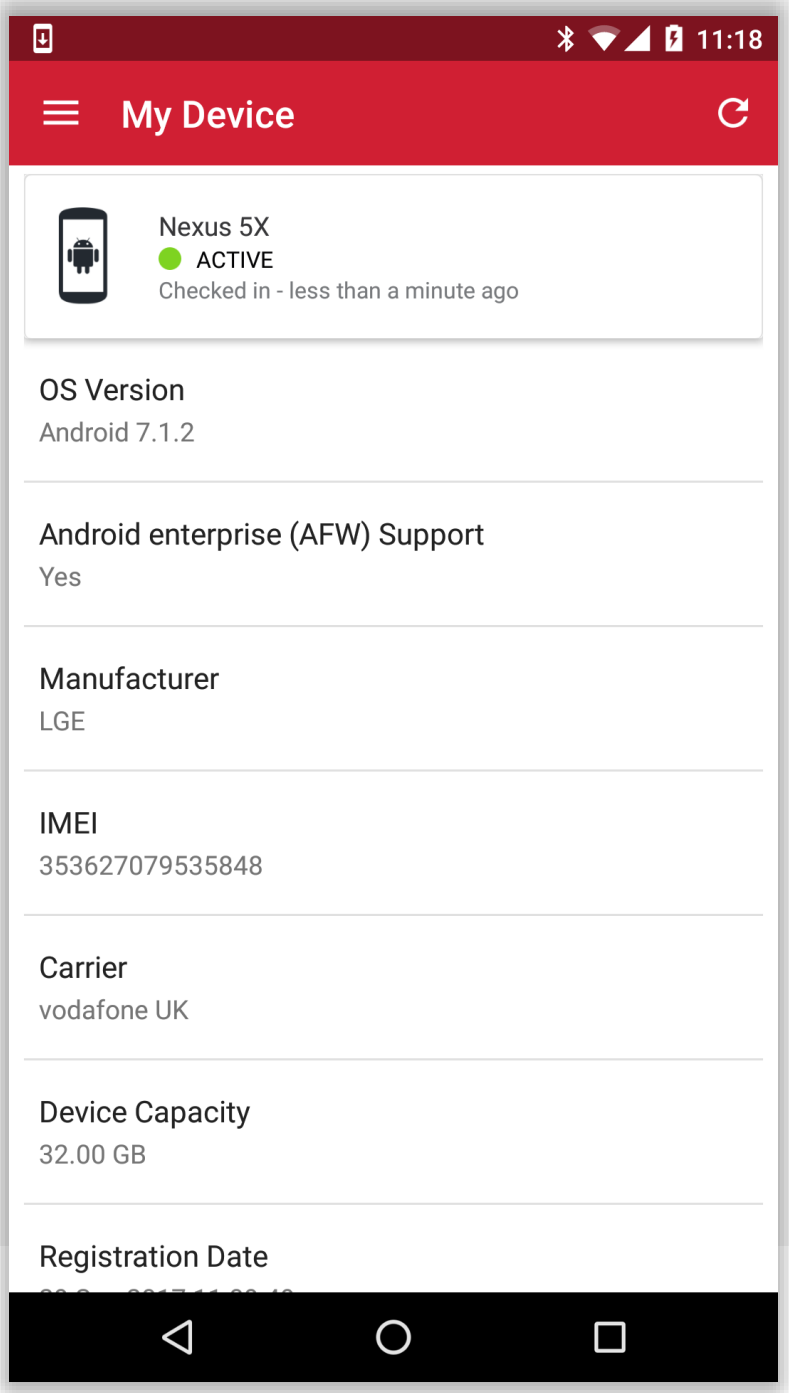
The Work Profile configuration will now finalise and automatically continue to the next step.



Configuration complete

The device has now completed initial configuration and will continue to pull down applications and resources in the background if configured.

You may tap the home (O) button to leave the DPC.



bayton

bayton

Jason Bayton

bayton.org

/in/jasonbayton

@jasonbayton

+JasonBaytonX

jason@bayton.org

Updates to this document can be found here:

Android enterprise provisioning guides