

Android legacy

Traditional enrolment
Factory-reset state



MobileIron Core



Android 7.x

September 2017

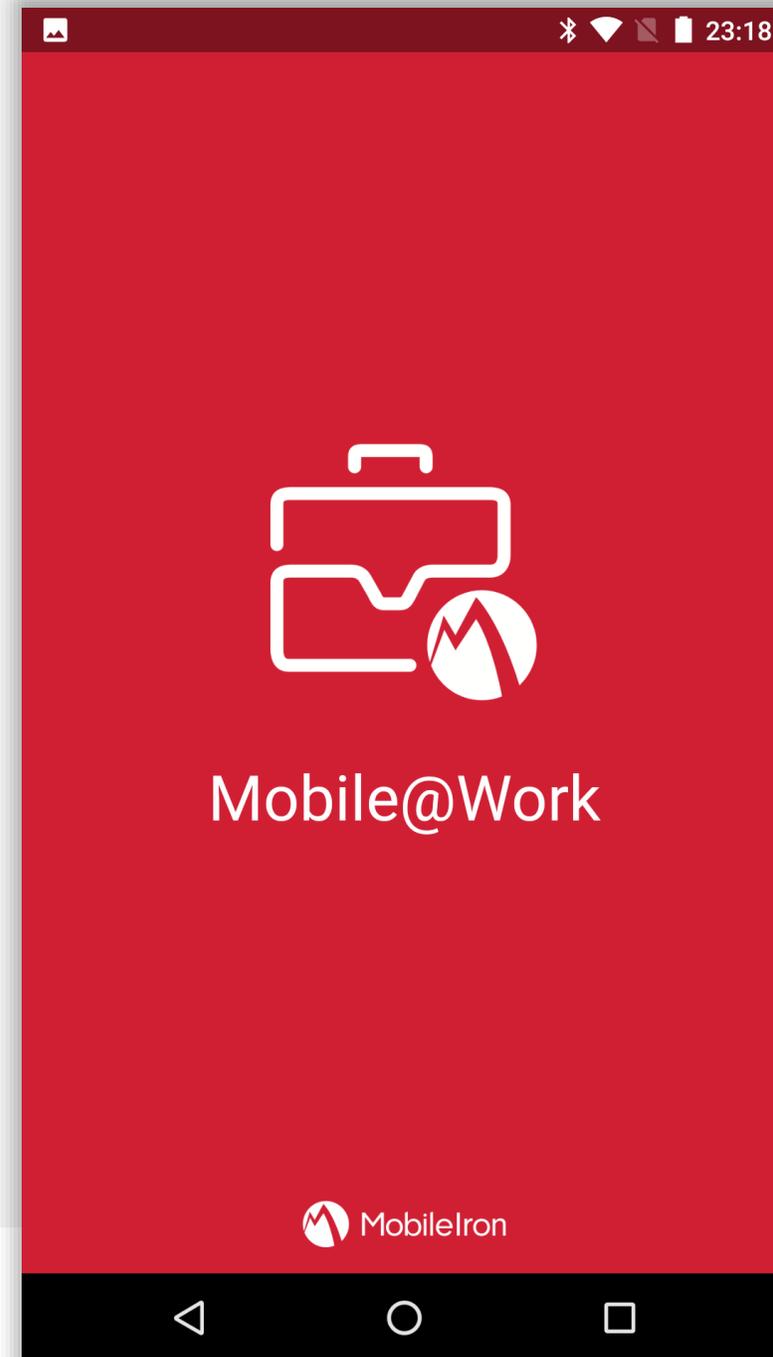




Requirements

In order to proceed, you must have:

- Android 4.x or later installed on the devices to be enrolled. Anything other than Samsung is unlikely to support more than minimal EMM capabilities.
- A functional MobileIron EMM solution in place.
- A Google account.



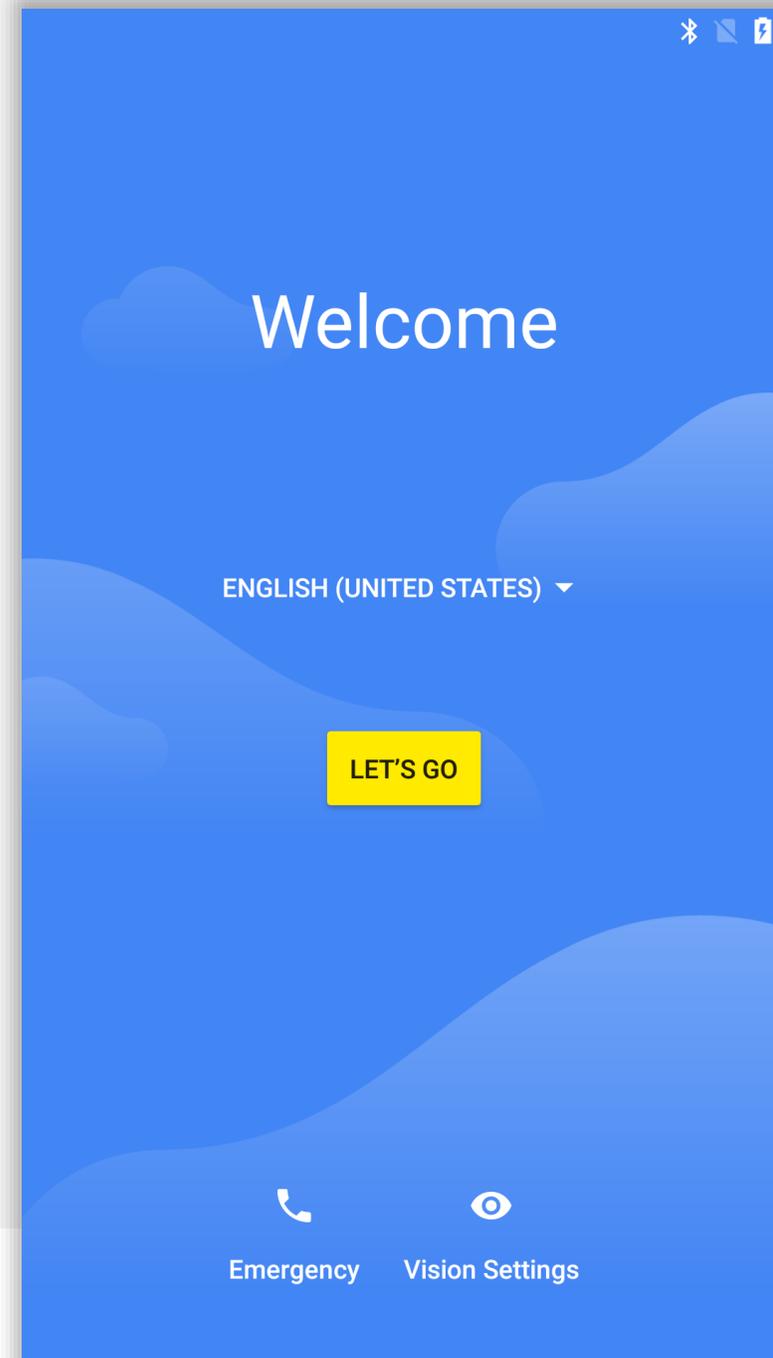


Begin device setup

For legacy 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**.

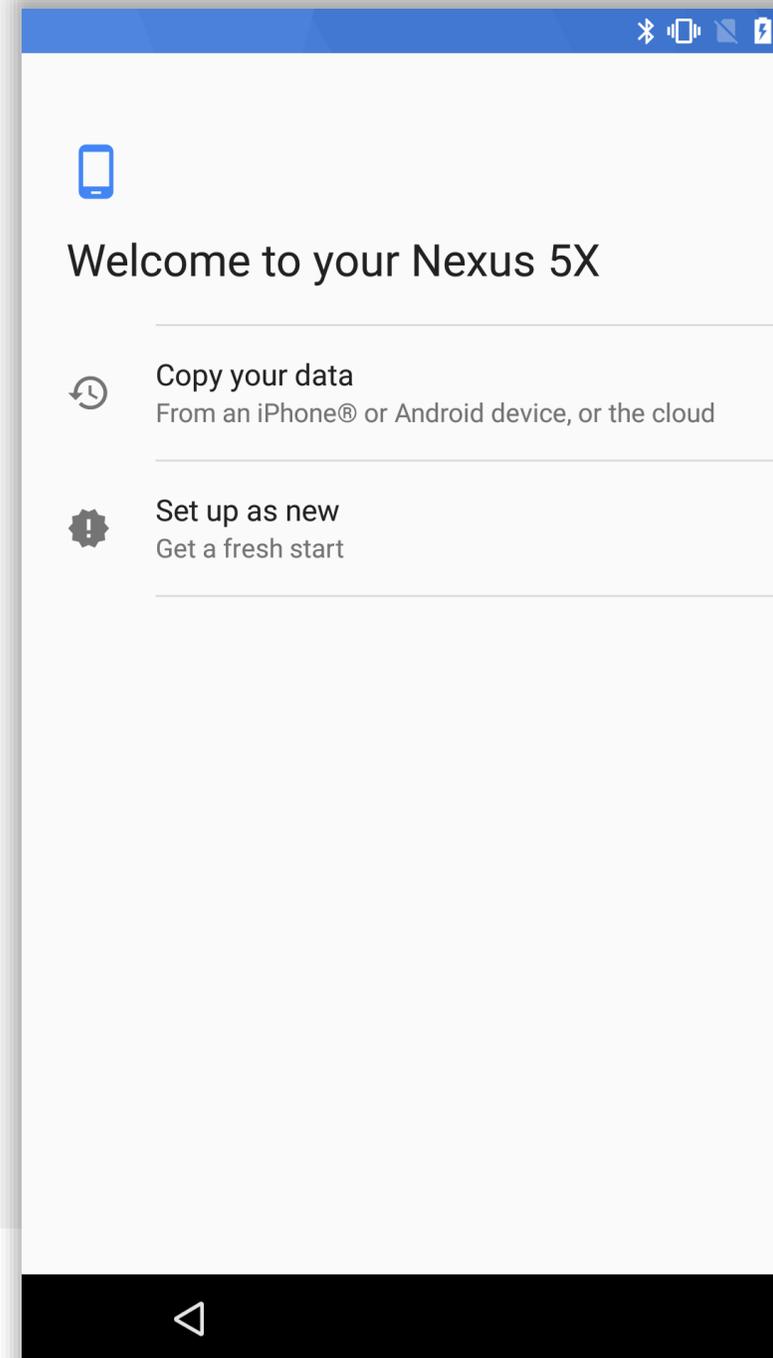




Continue device setup

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

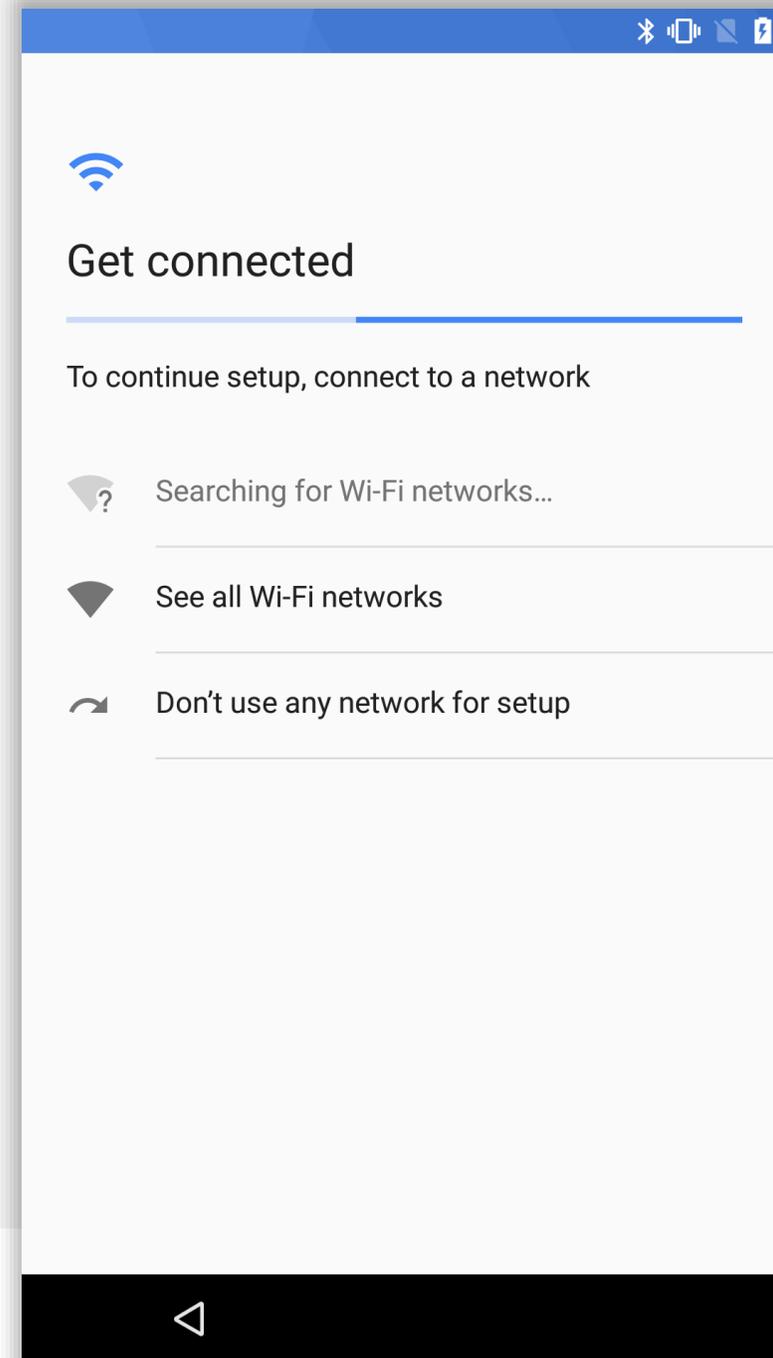




Continue device setup

Connect to a suitable WiFi network to continue.

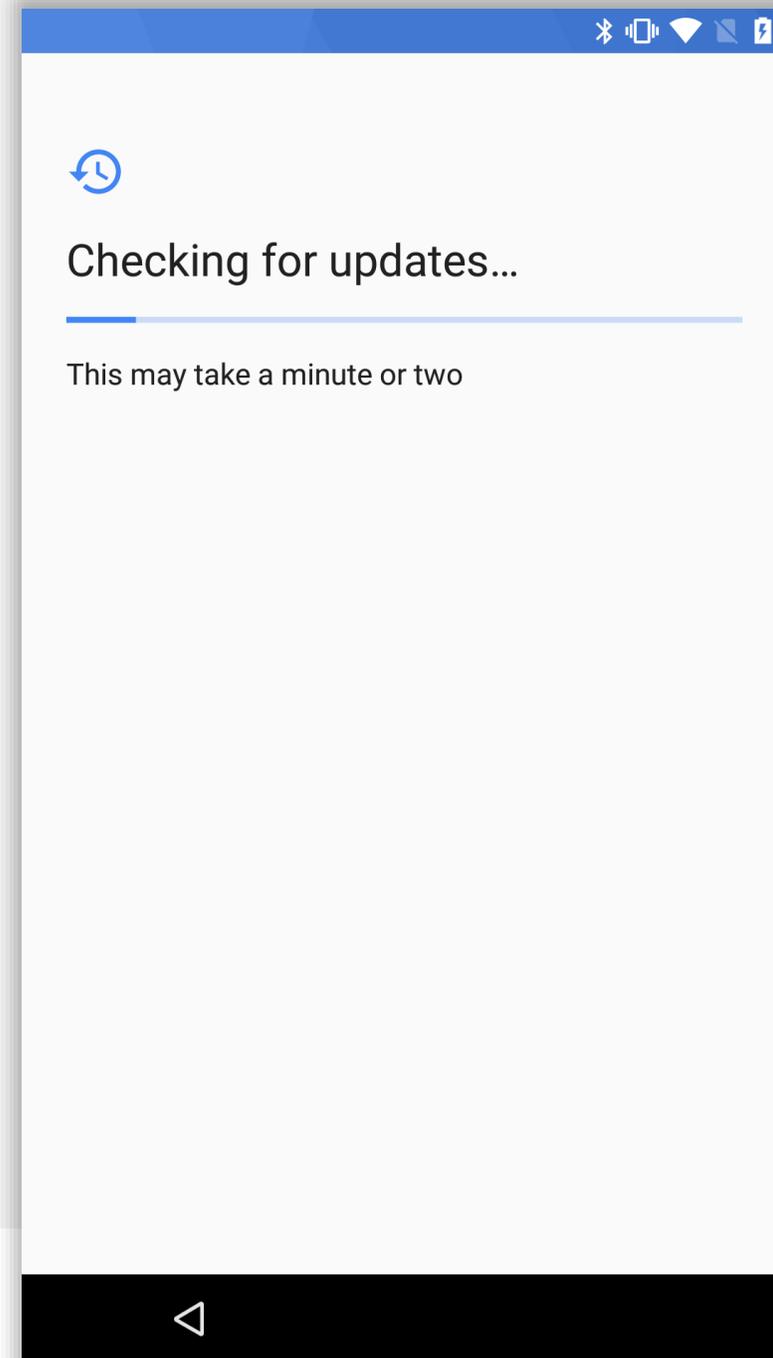
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup**.





Continue device setup

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





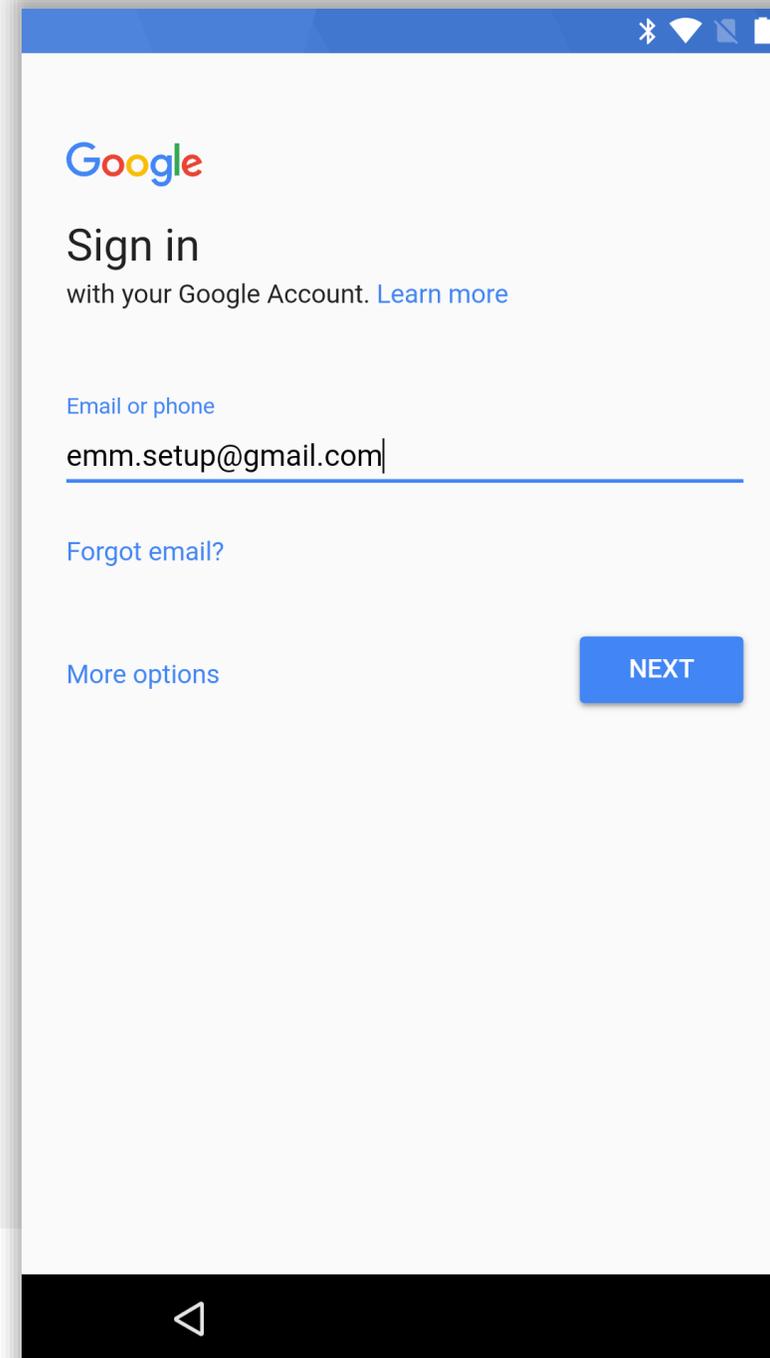
Continue device setup

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.

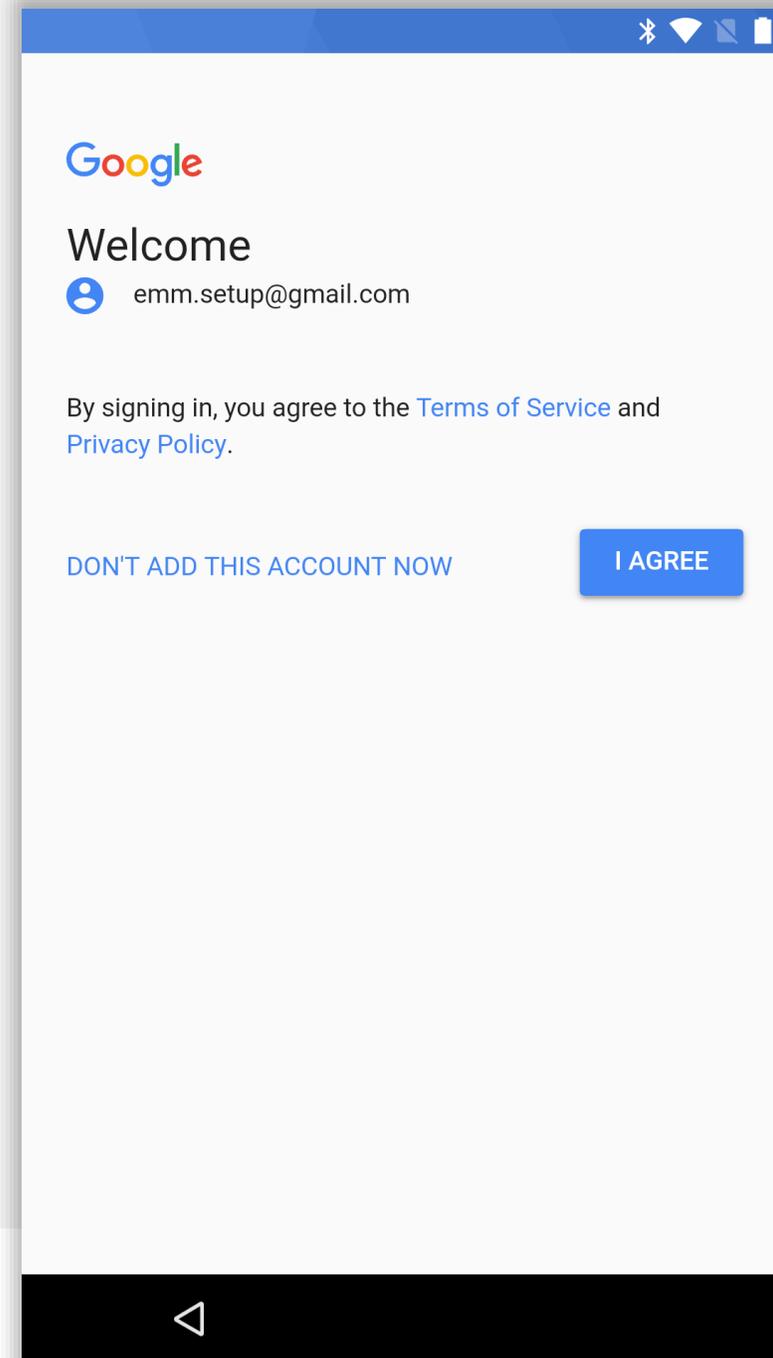




Continue device setup

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

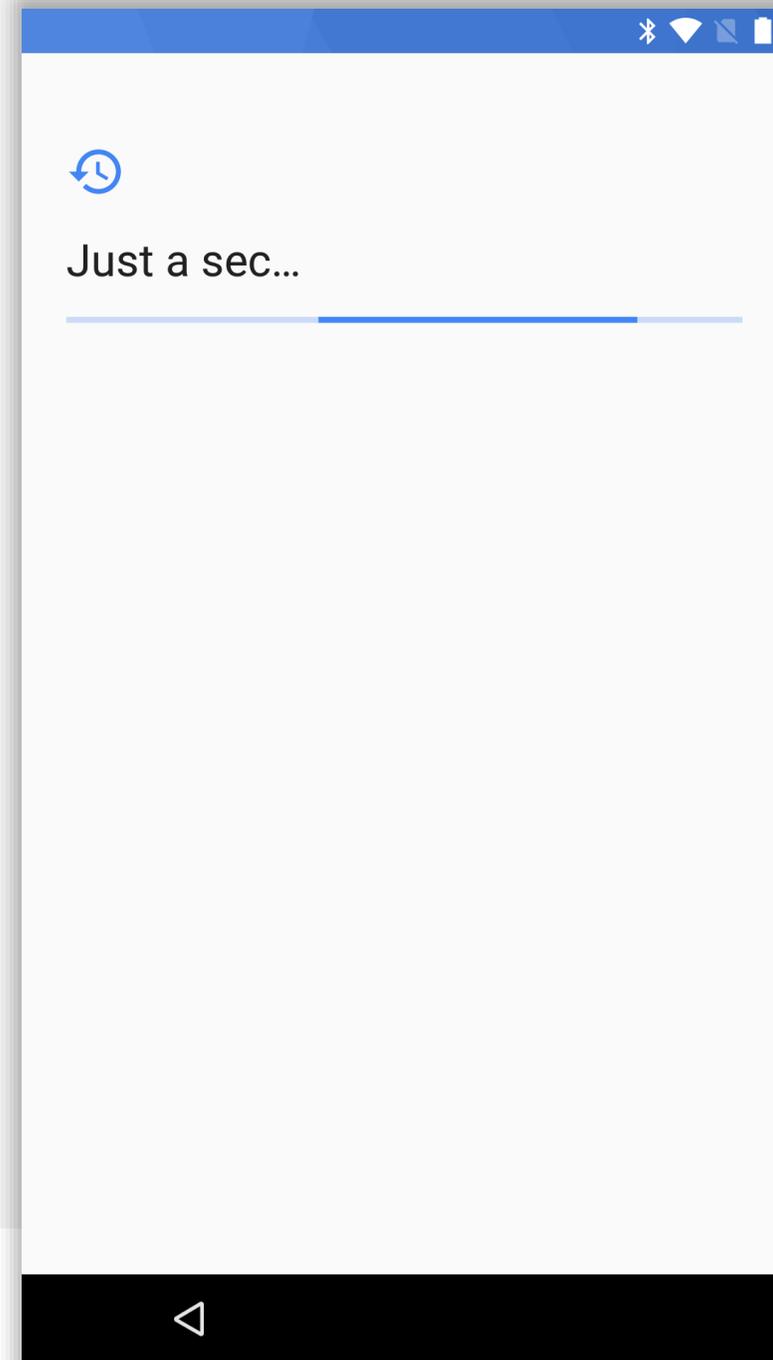
(After reading the ToS and Privacy Policy, naturally).





Continue device setup

The device will now add the account and automatically continue.



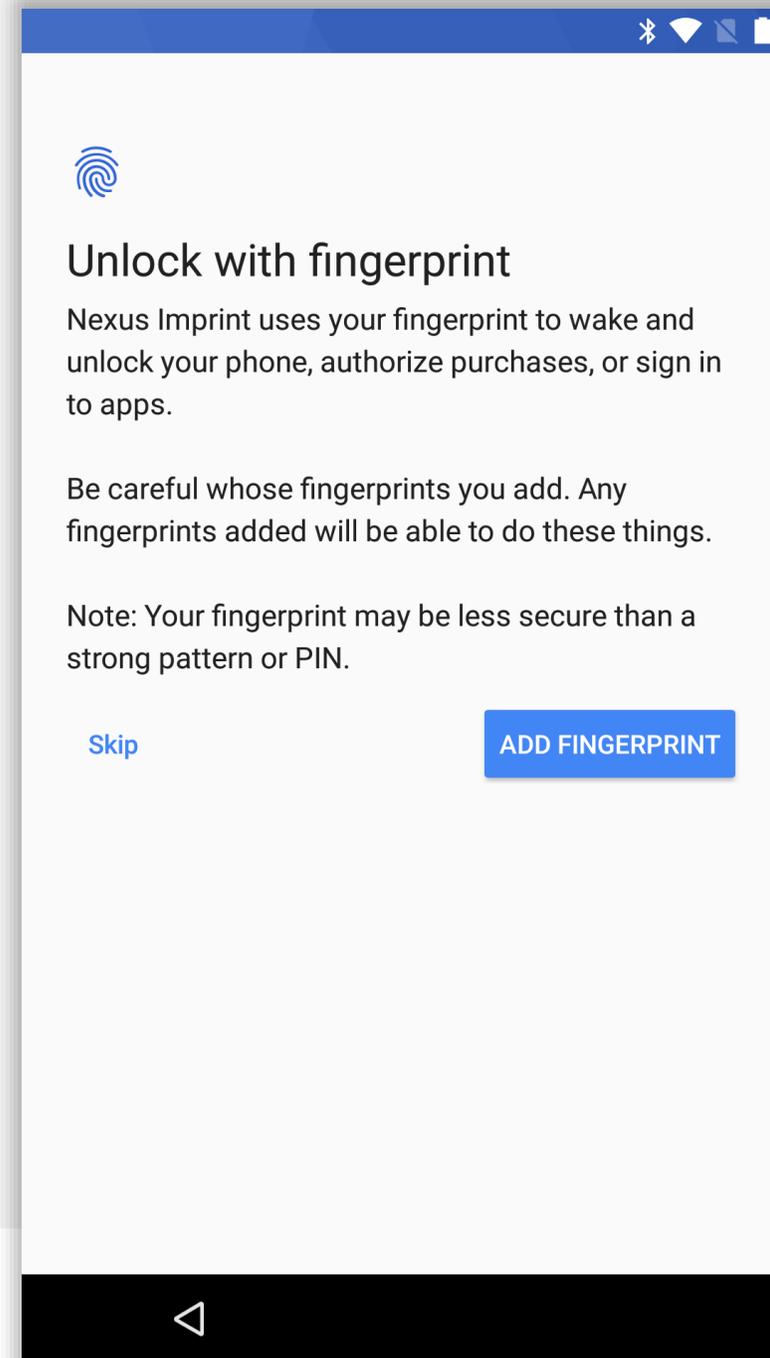


Continue device setup

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.

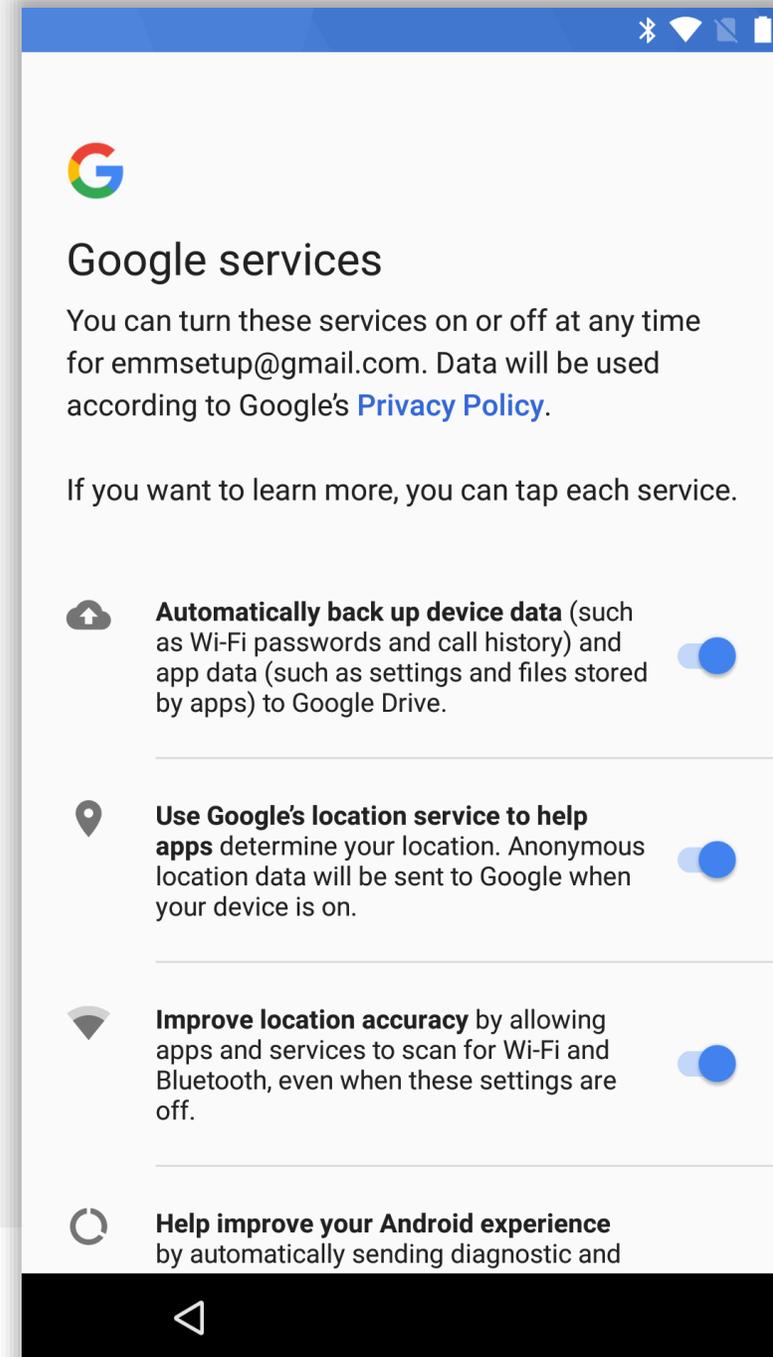
Note: Fingerprint setup is not documented in this guide as it is assumed corporate passcode policies are in place which may block its use. Passcode setup is documented in the following pages and as such the next page in this guide assumes **Skip** has been tapped.





Continue device setup

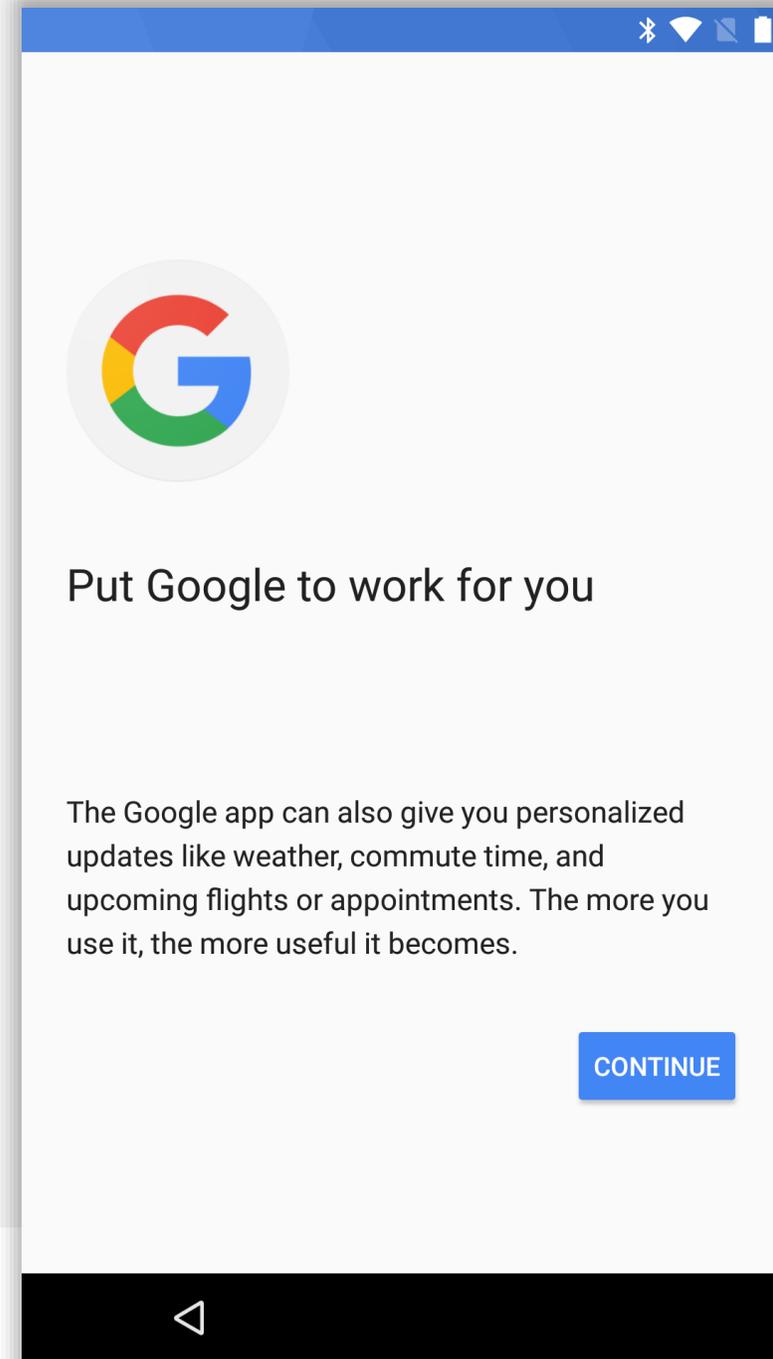
Disable relevant services and tap **NEXT** to continue to the next step.





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.



Give the Google app permission to help you

The Google app depends on these settings in order to best help you. Turn these settings on for:

emmsetup@gmail.com

 **Web & App Activity from this device** ▾

Includes Chrome history and content you browse on the web and in apps

 **Location History** ▾

Creates a private map of where you go with your signed-in devices

 **Device Information from this device** ▾

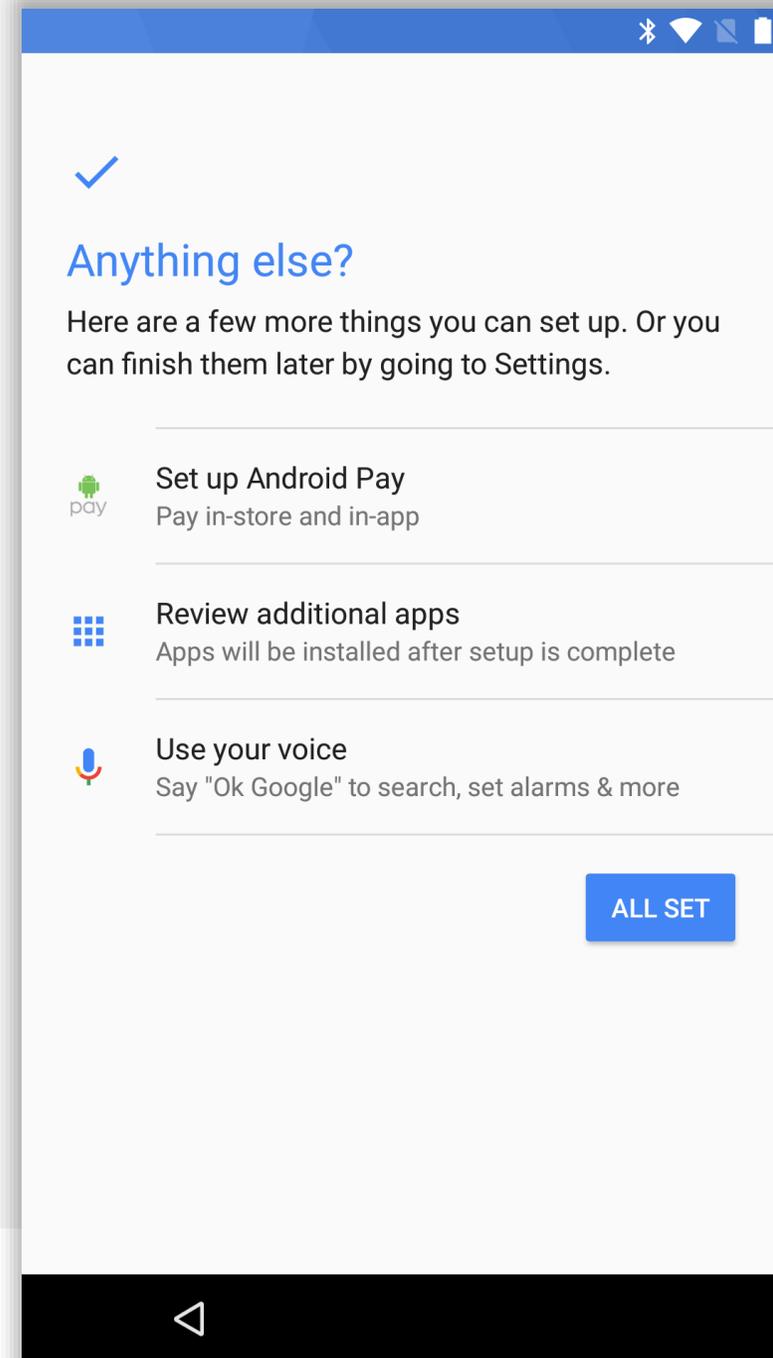
Includes contacts, calendars, apps, music, battery life, sensor readings

Please remember that the data governed by these settings may be saved from any of your signed-in devices



Continue device setup

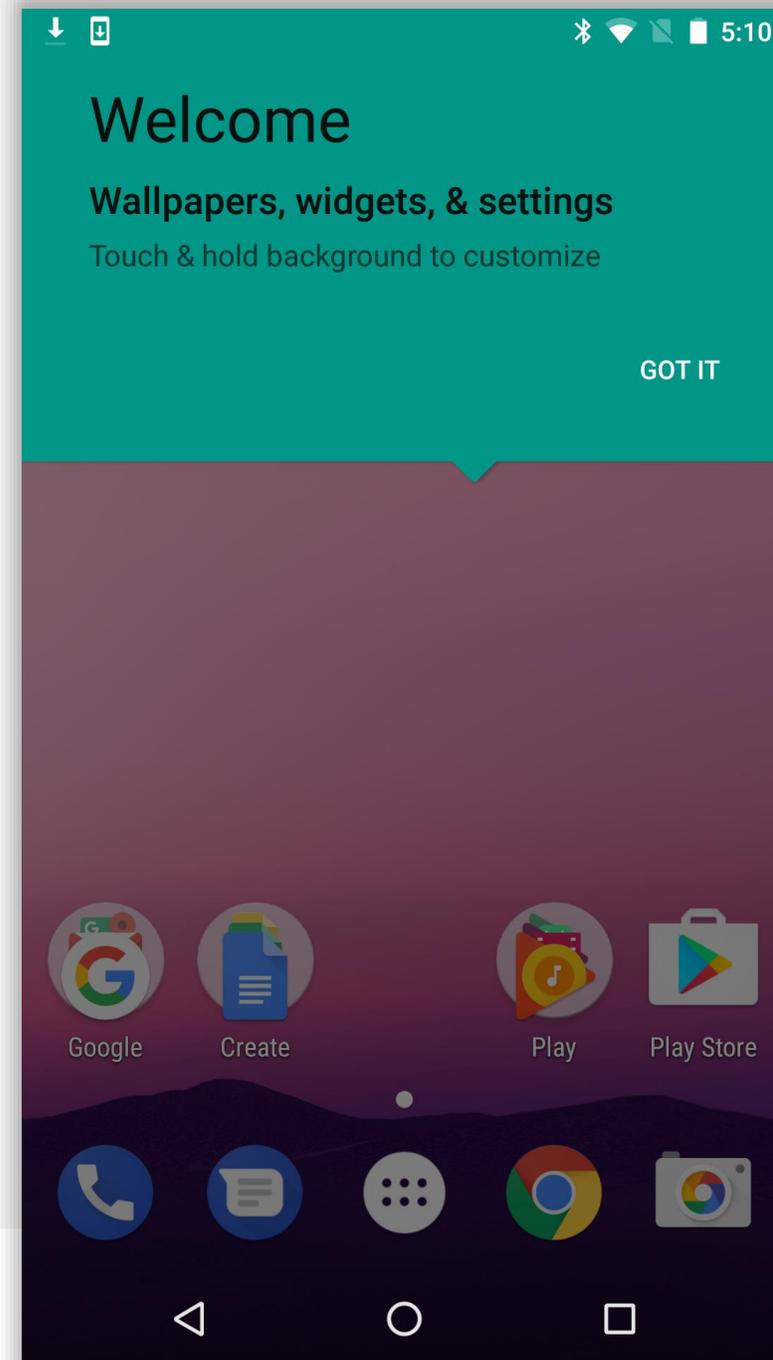
Tap **ALL SET** to exit the Wizard.





Device setup complete

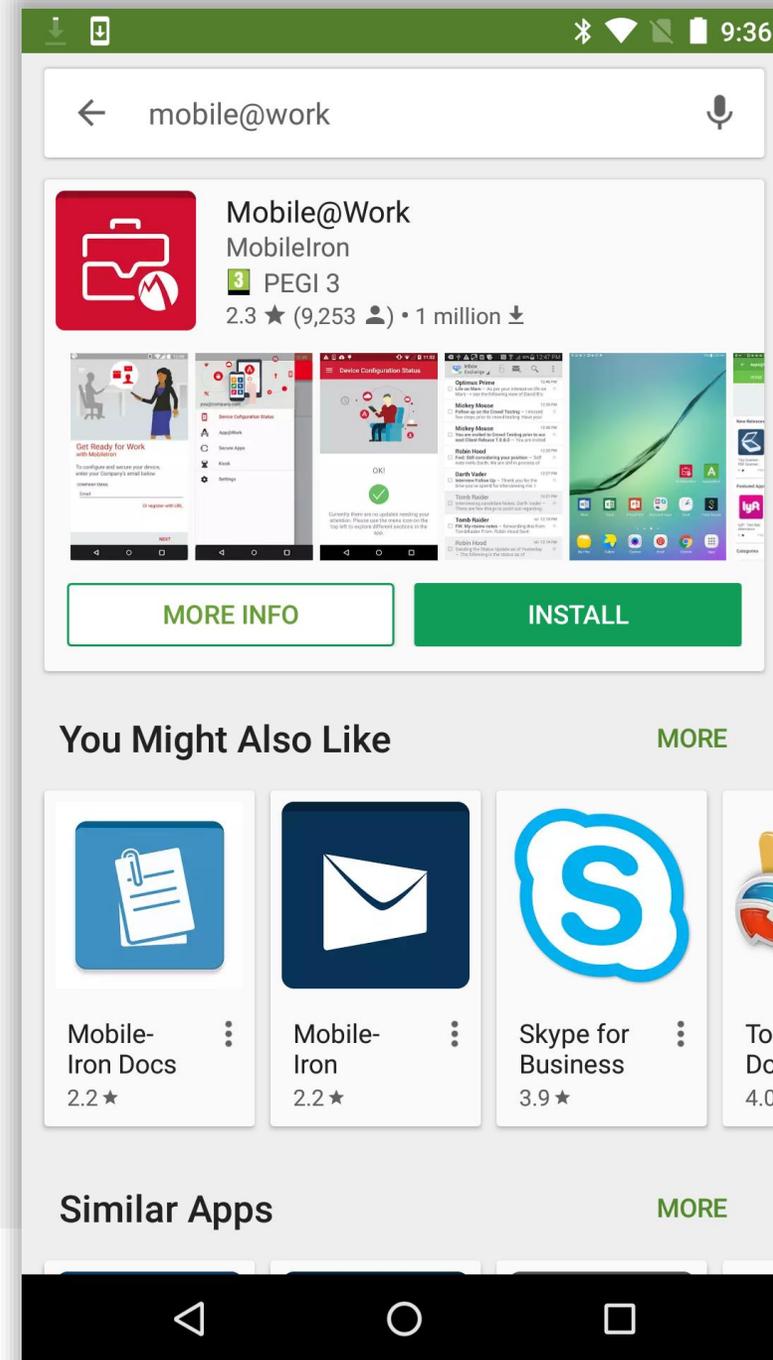
From the home screen, tap **GOT IT**, then open the Play Store.





Install the DPC

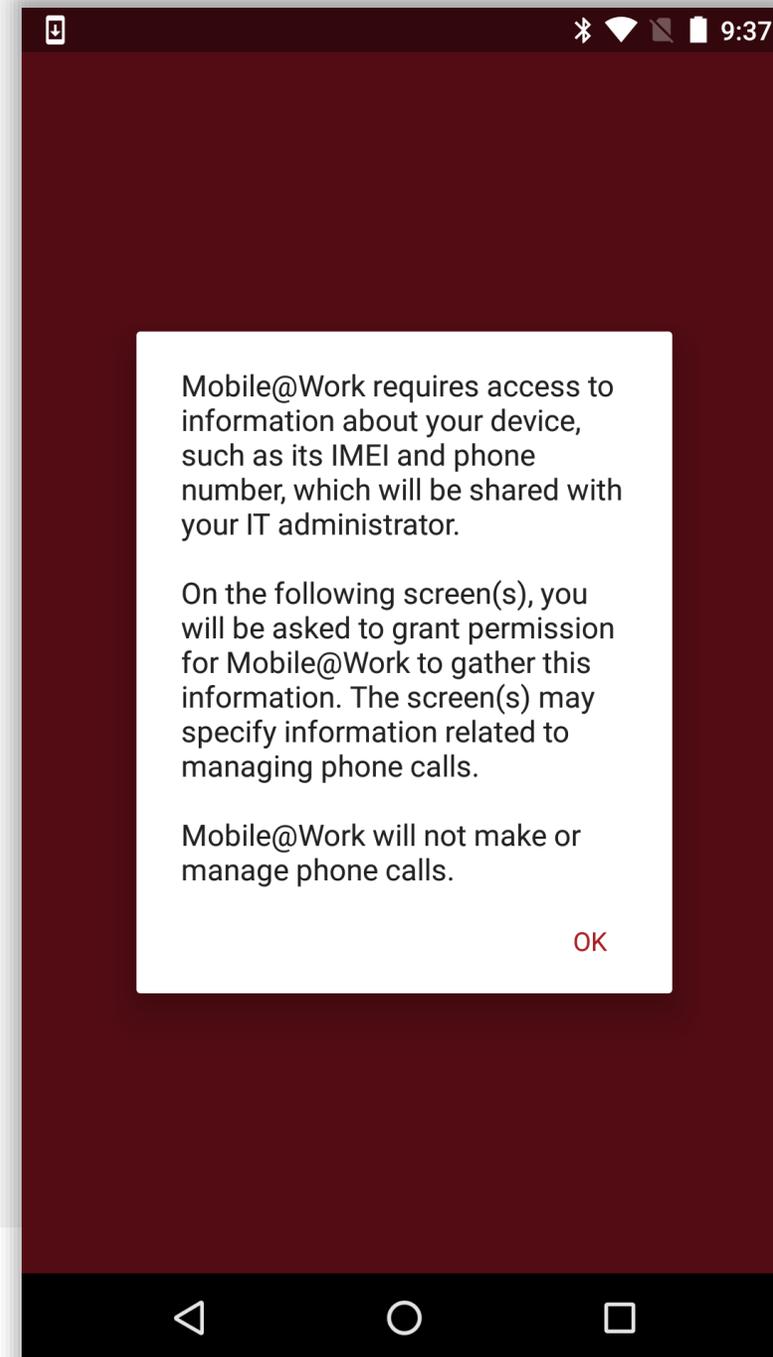
Search for Mobile@Work and tap **INSTALL** when located.





Open the DPC

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

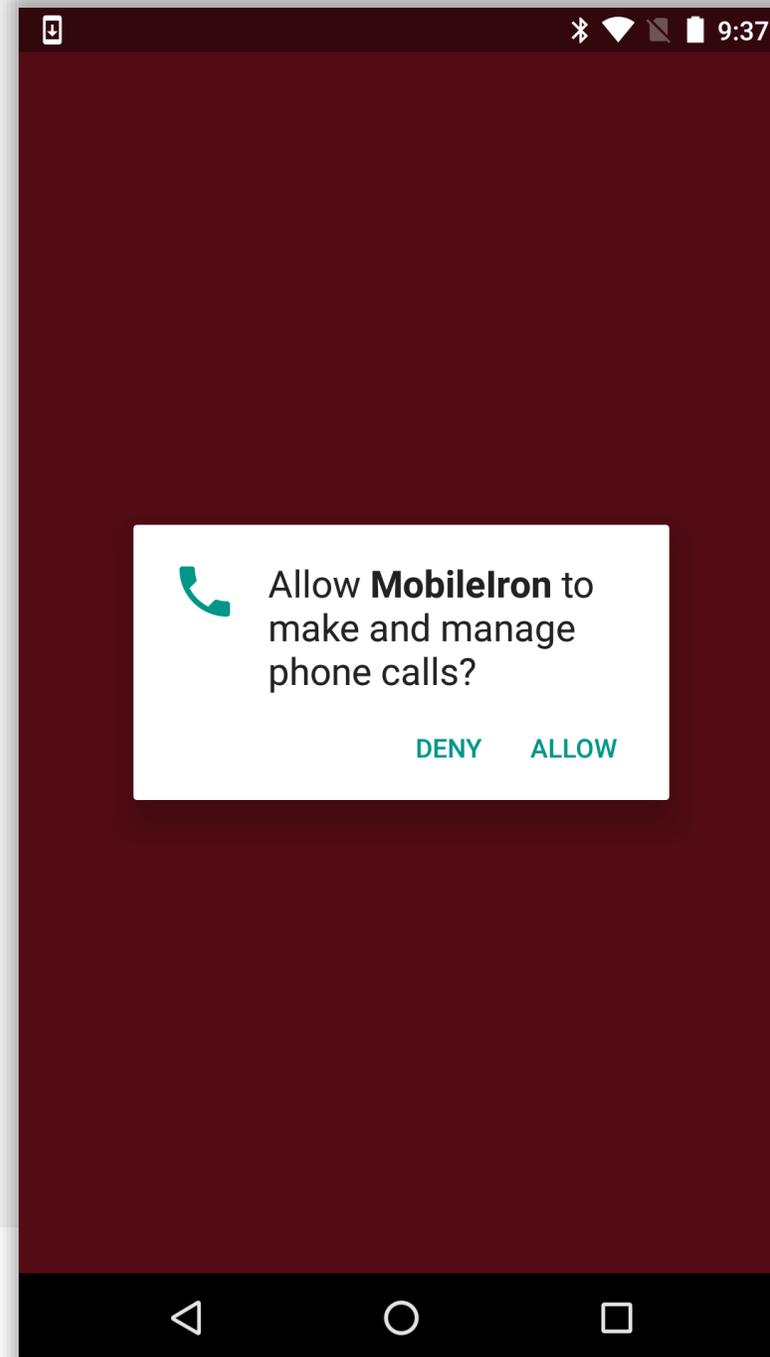




Grant permissions

Grant MobileIron the requested permissions.

Tap **ALLOW**.

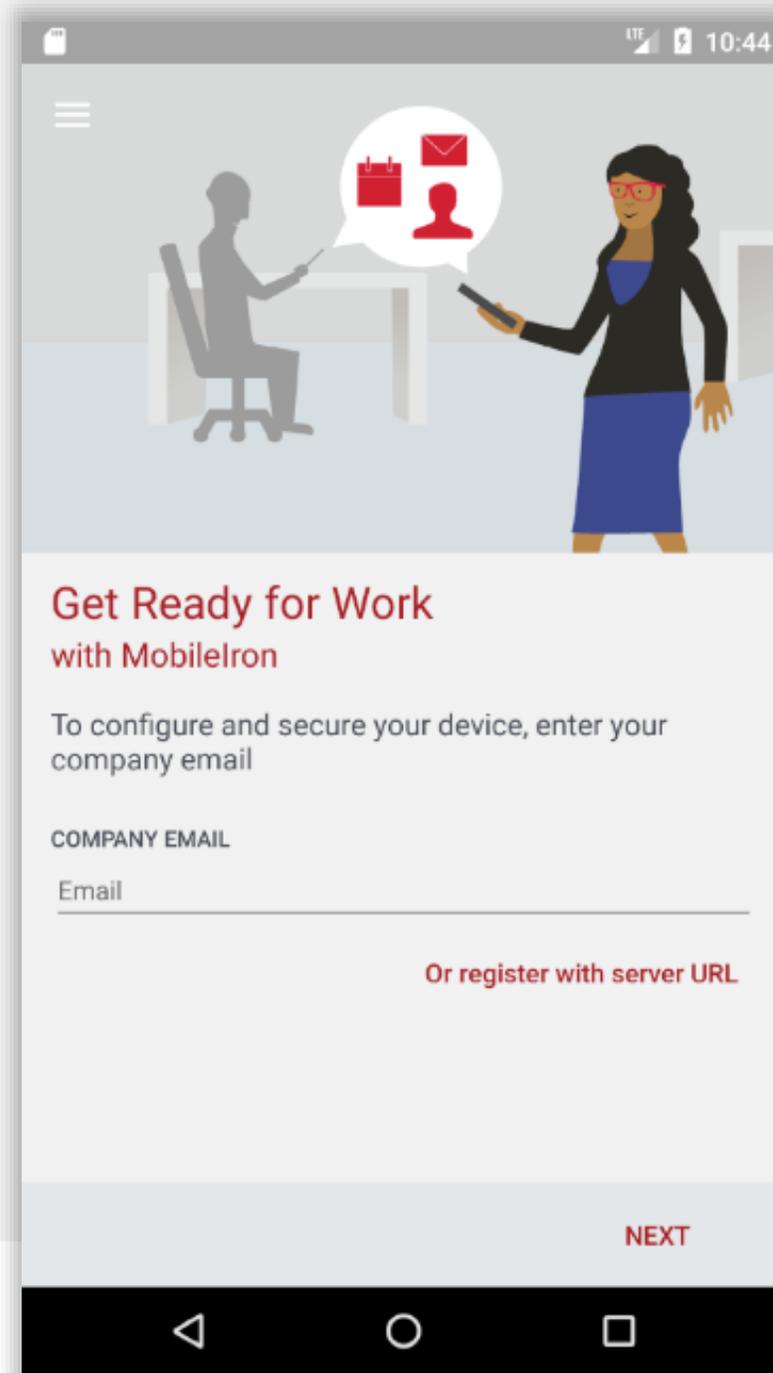




Begin enrolment

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

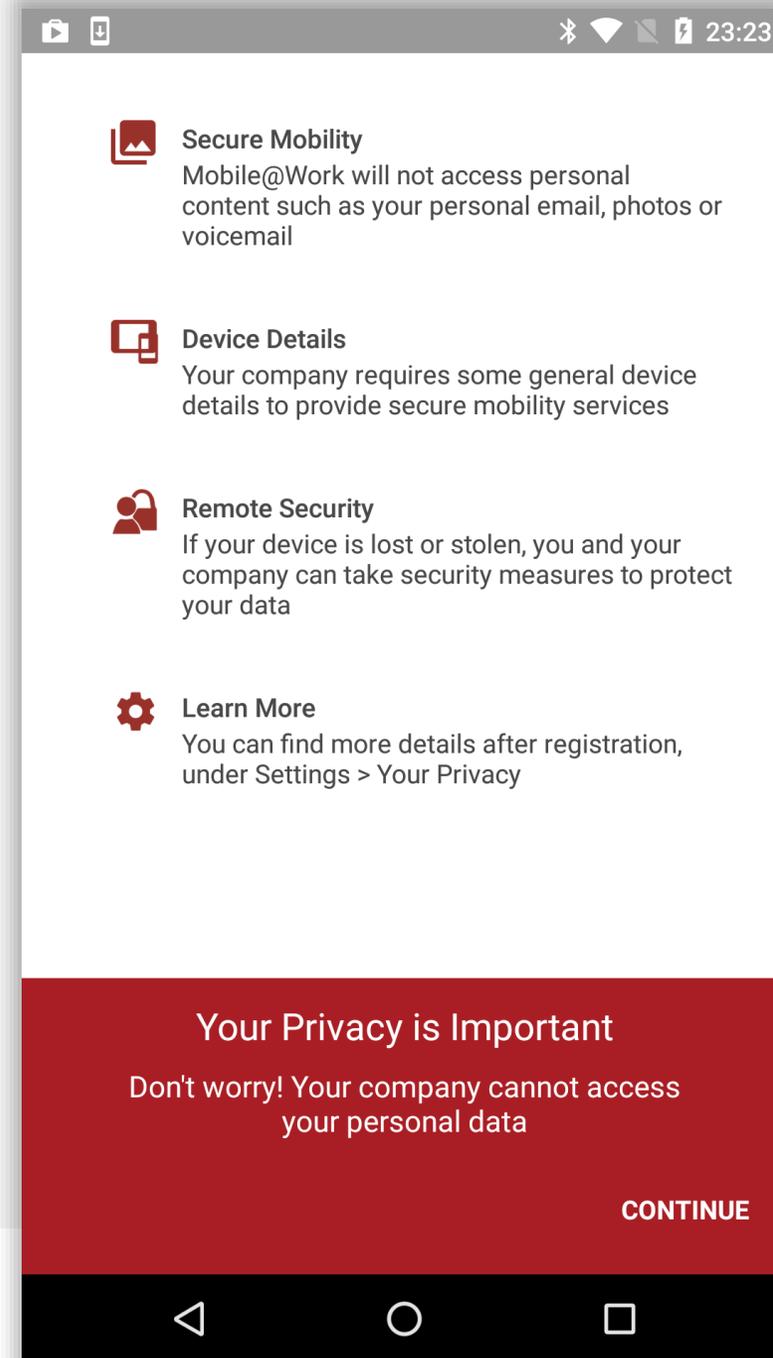
Tap NEXT.





Continue enrolment

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

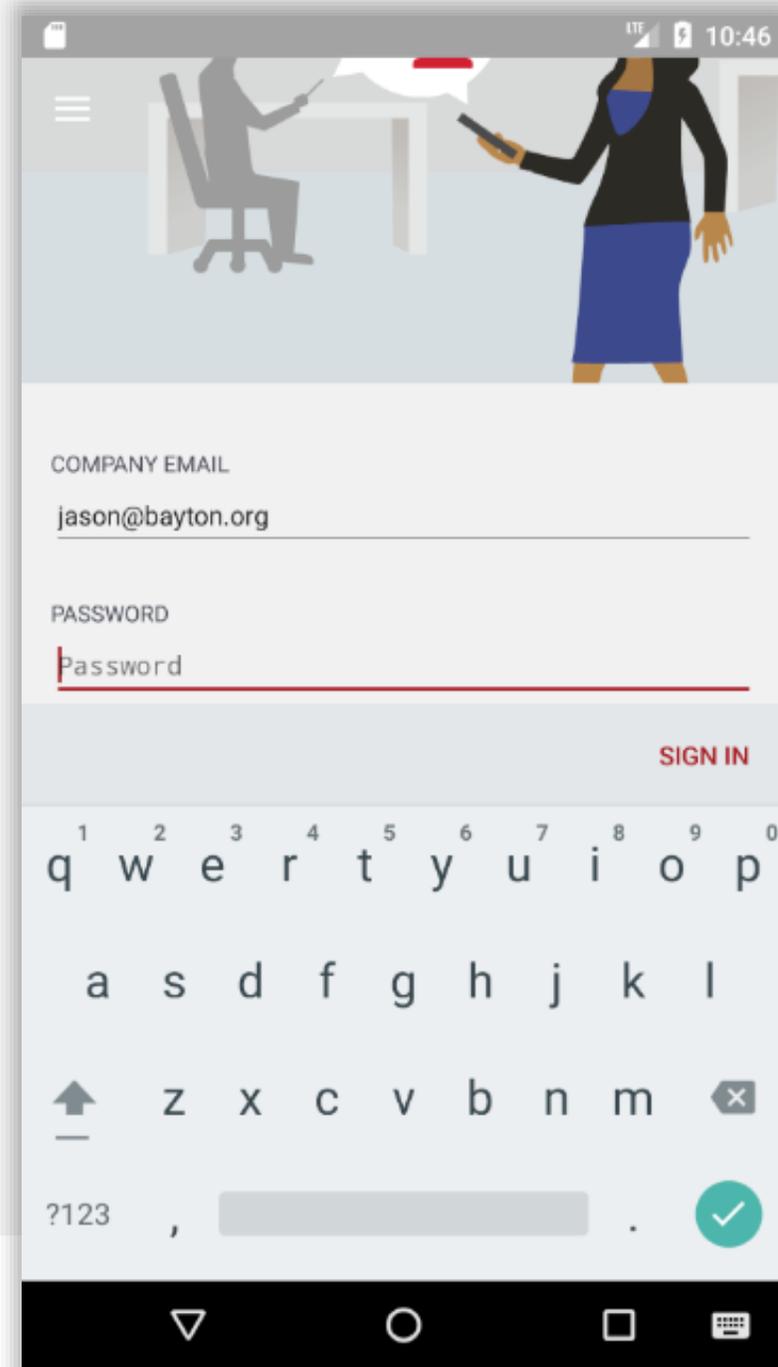




Continue enrolment

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

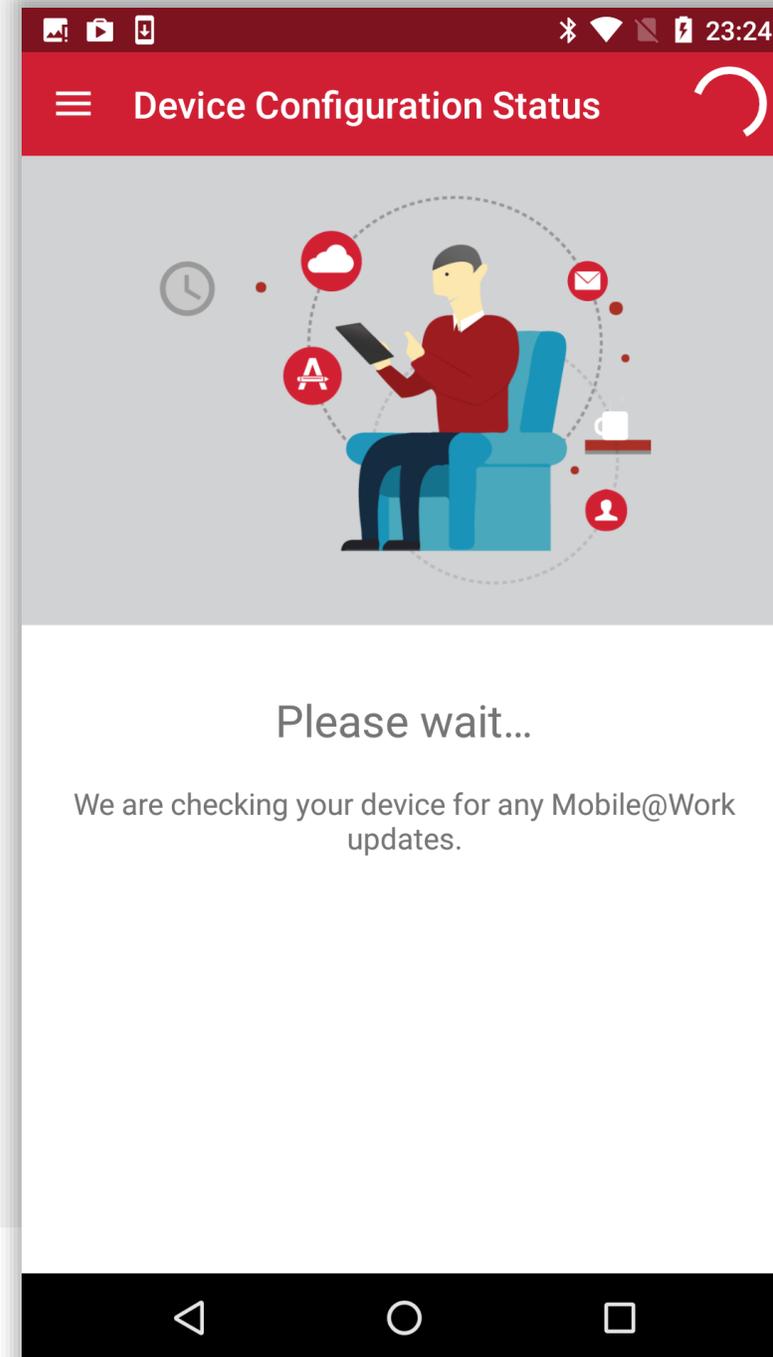
Enter the required fields and tap **SIGN IN**.





Device configuration

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

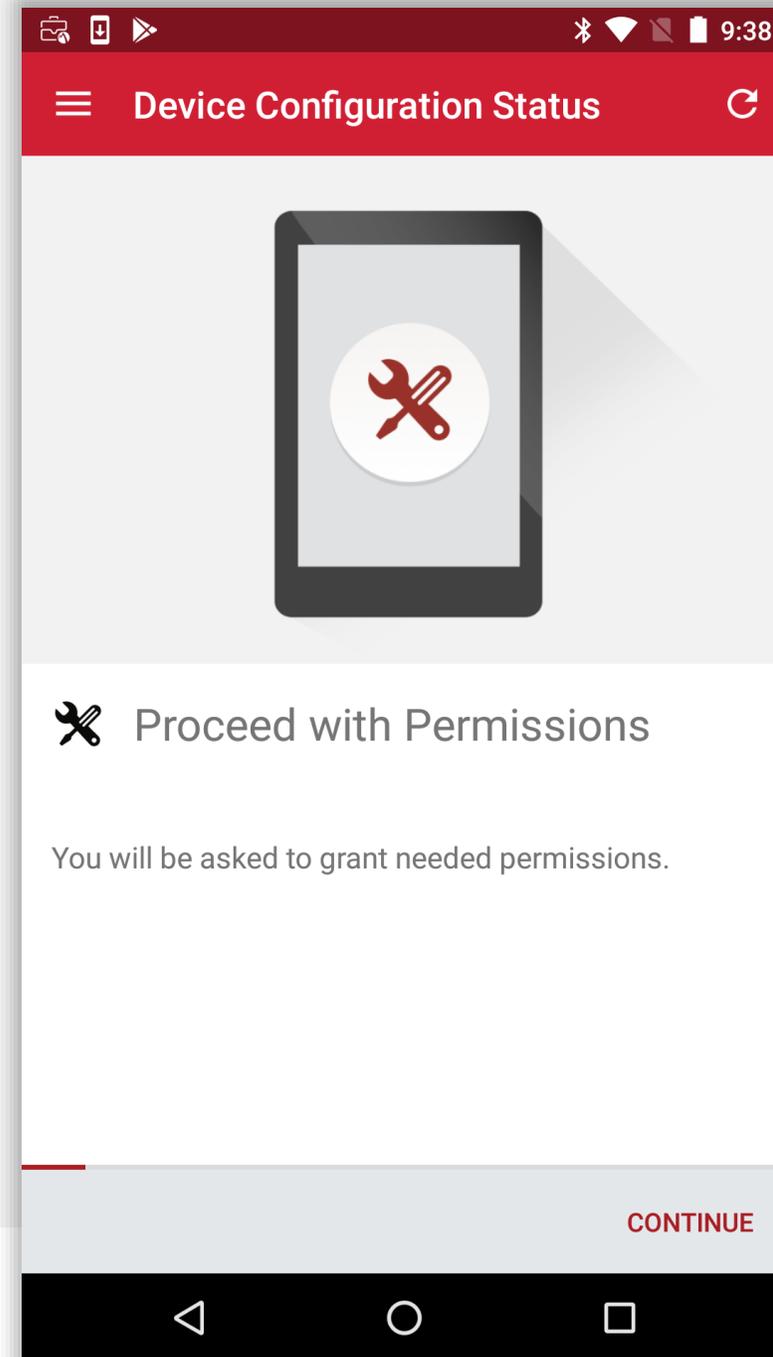




Device configuration

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

Tap **CONTINUE**.

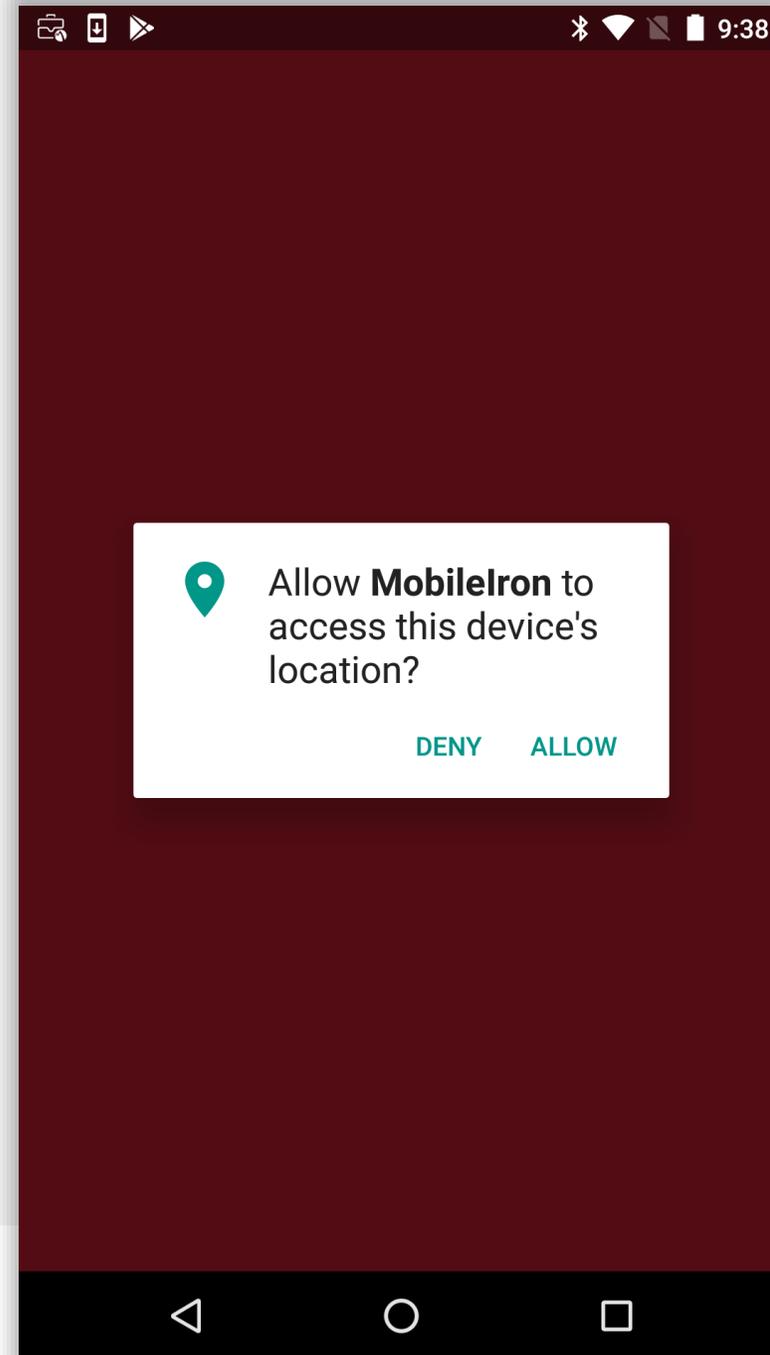




Grant permissions

Grant MobileIron the requested permissions.

Tap **ALLOW**.



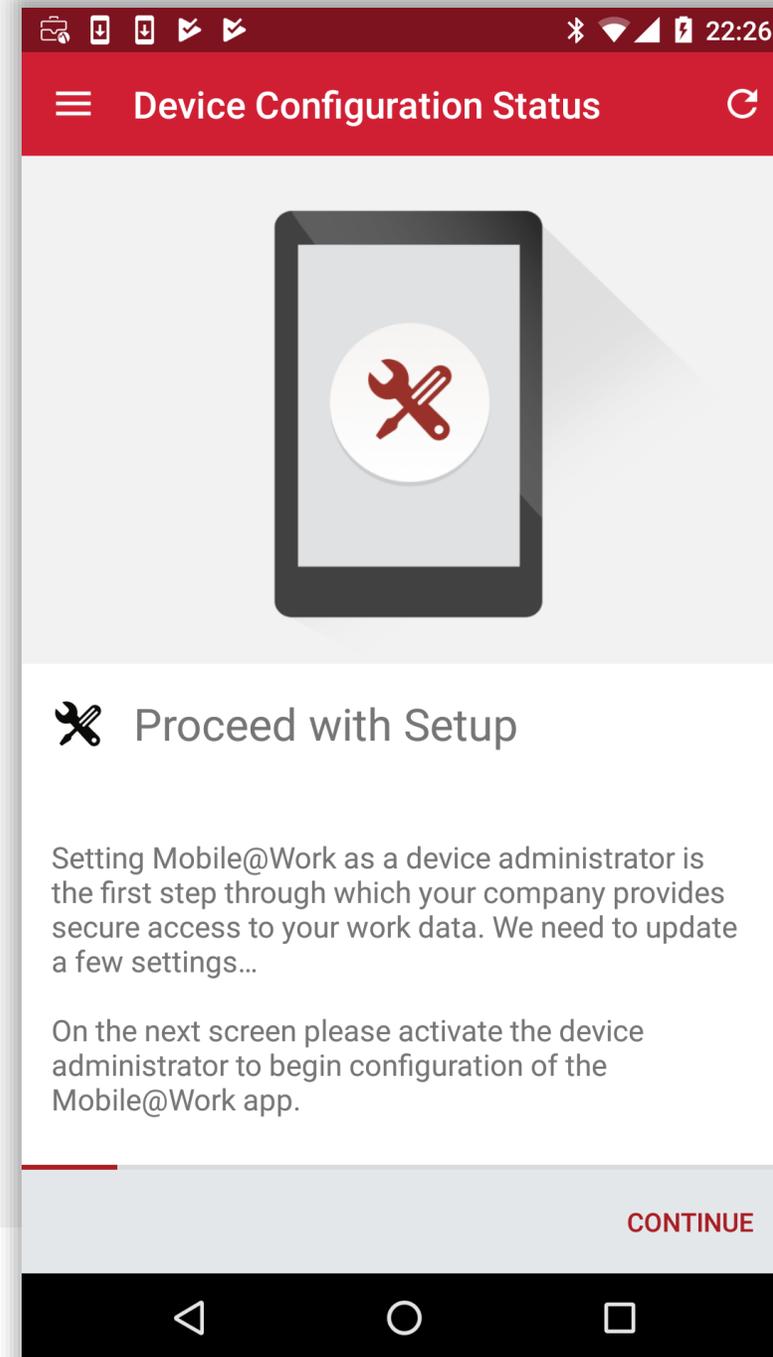


Device configuration

MobileIron requires device administrator permissions in order to effectively manage the device.

If this is not granted, or the administrator permission is later revoked, device management will not function.

Tap **CONTINUE**.





Activate administrator

MobileIron, like all EMMs, requires a number of permissions in order to effectively manage the device.

Scroll through the list of permissions until you reach the bottom.

Tap **Activate this device administrator** to continue.

Activate device administrator?

 **Mobile@Work**

In order to securely manage your device, this app needs to be activated as device administrator.

Activating this administrator will allow the MobileIron app to perform the following operations:

- **Erase all data**
Erase the phone's data without warning by performing a factory data reset.
- **Change the screen lock**
Change the screen lock.
- **Set password rules**
Control the length and the characters allowed in screen lock passwords and PINs.
- **Monitor**
Monitor the device when unlocked and erase all the passwords.
- **Lock the**
Control how the device is locked.
- **Set screen lock password expiry**
Change how frequently the screen lock password, PIN or pattern must be changed.
- **Set storage encryption**

Activate this device administrator

Cancel

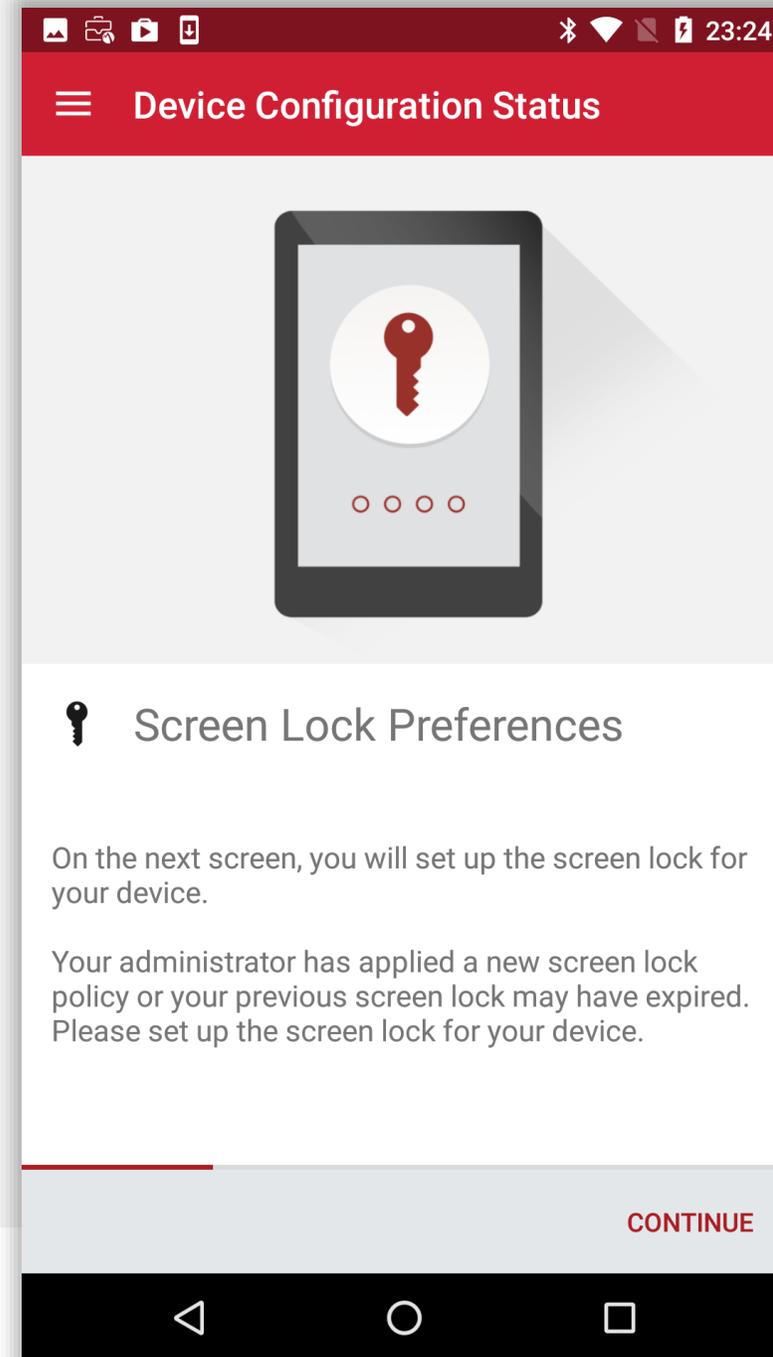
Uninstall app



Device configuration

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

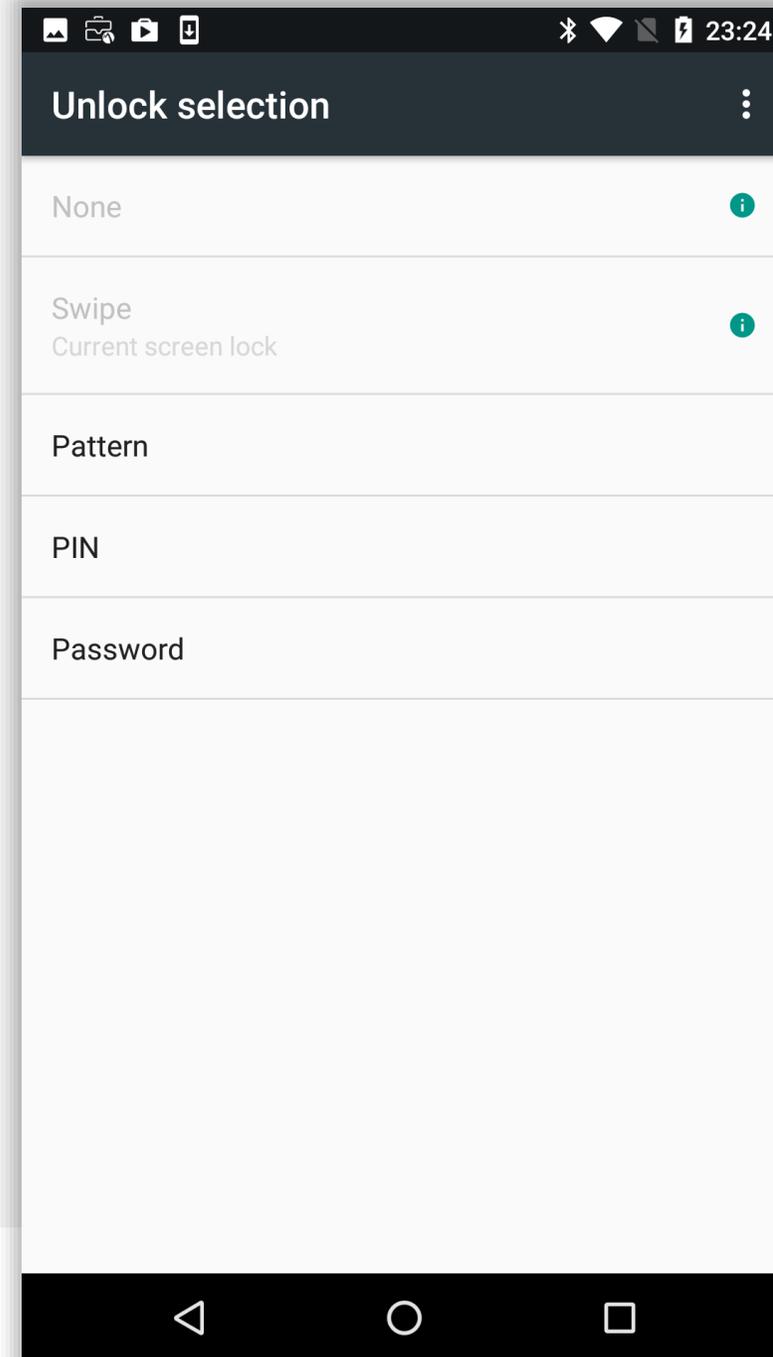
The type of passcode mandated may not be a PIN as depicted in the following steps. The process however is similar for all alpha/numeric passcode options.





Device configuration

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

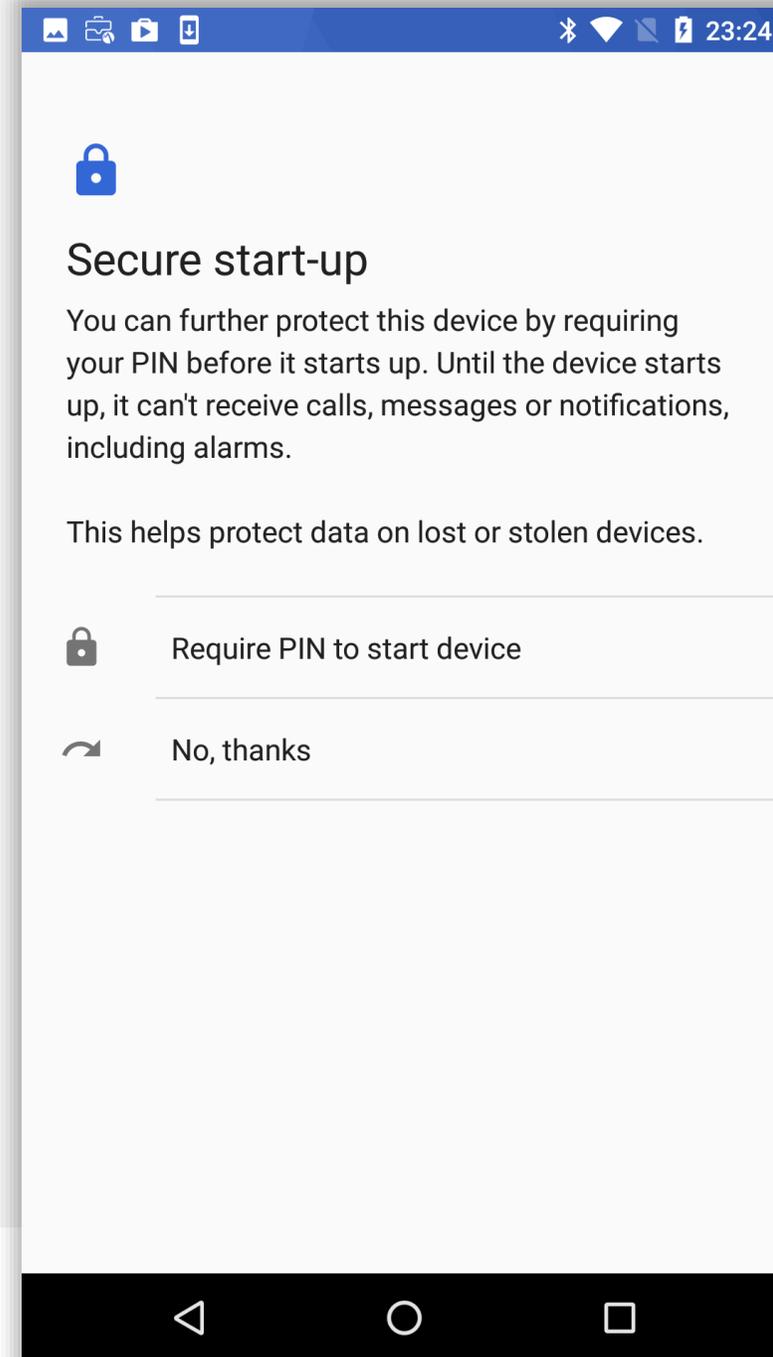




Device configuration

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

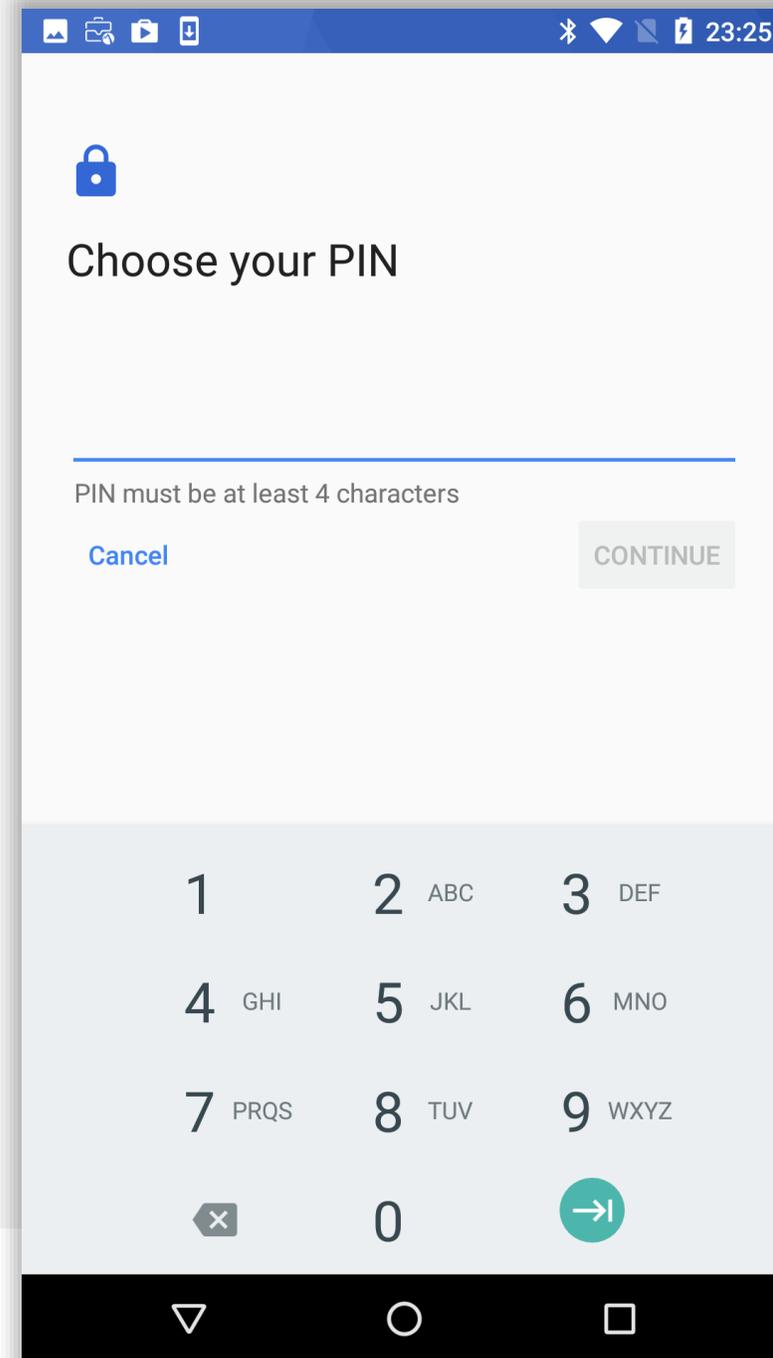
While it is more secure to require the passcode on device boot, it will result in a longer boot process.





Device configuration

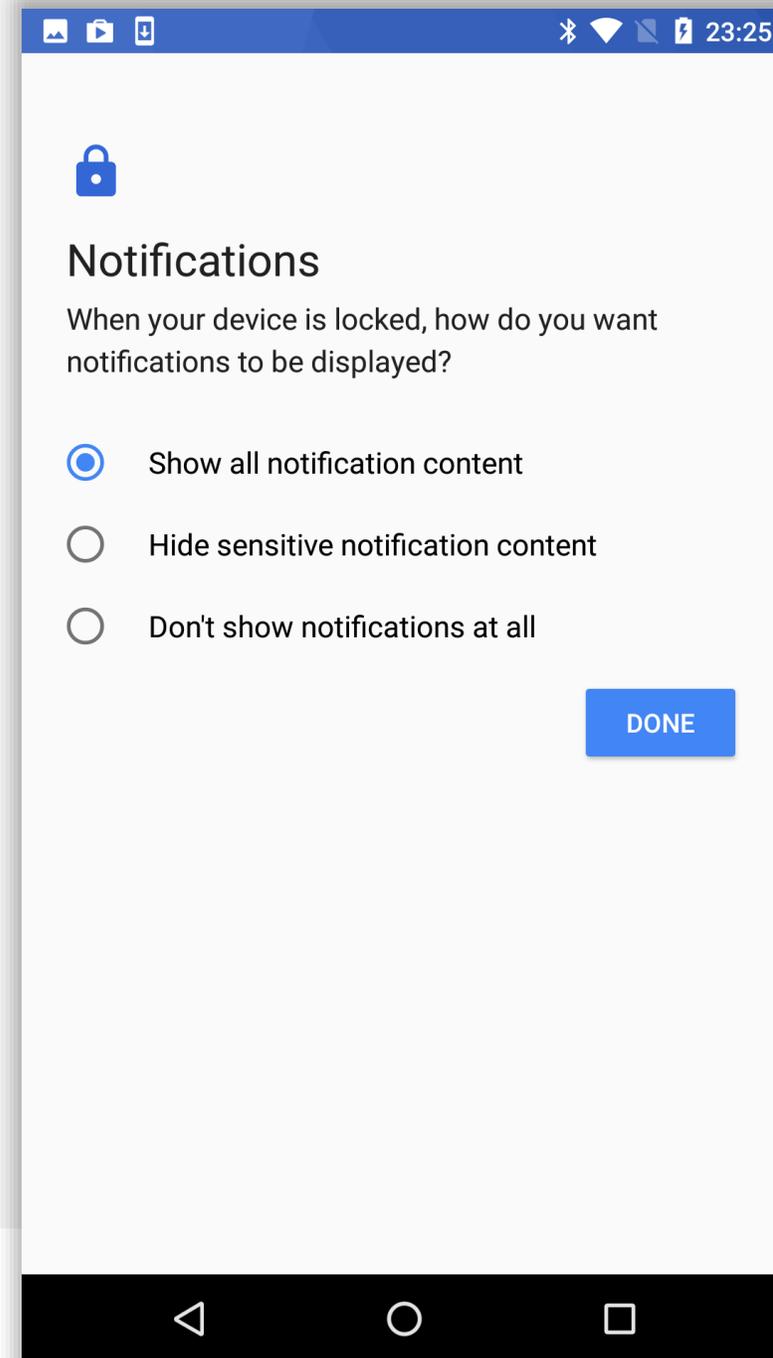
Input a PIN (or other passcode type) and tap **CONTINUE**.
Repeat to confirm.





Device configuration

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

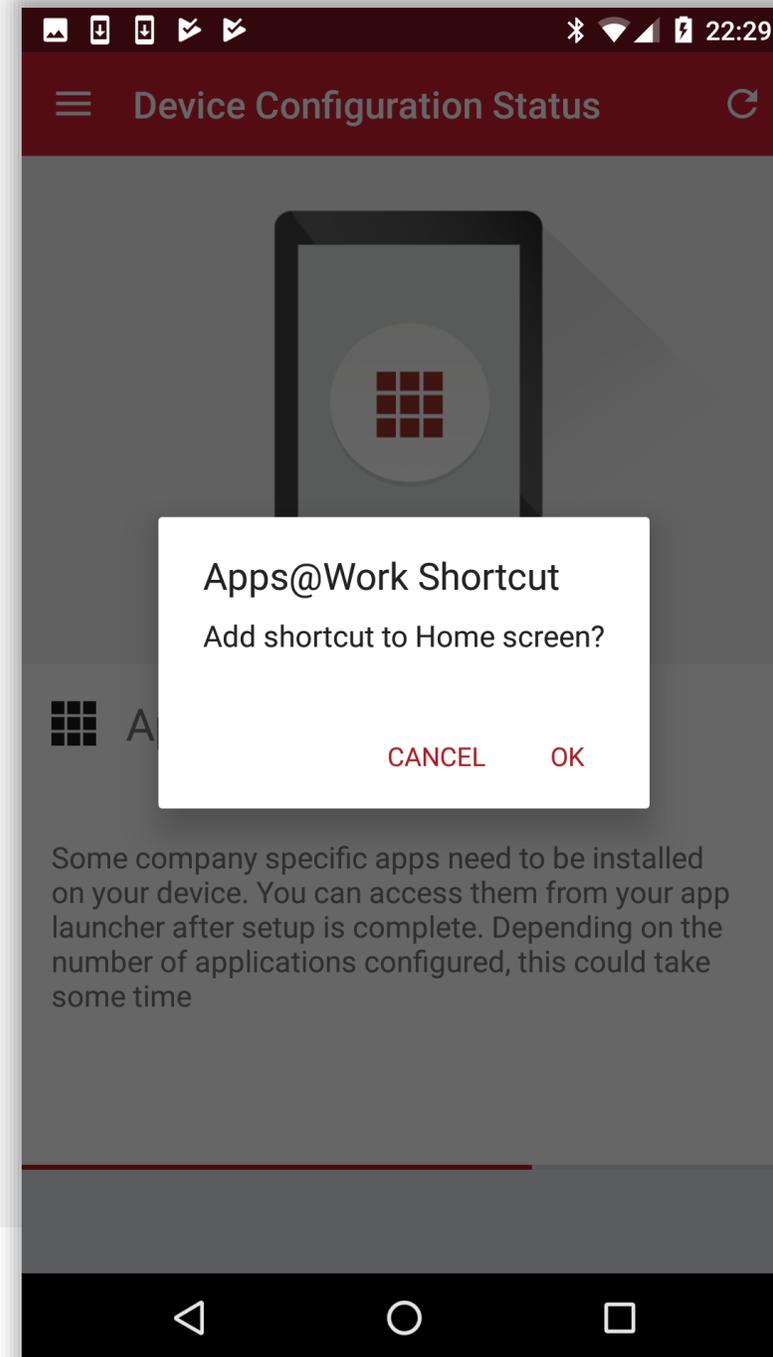




Device configuration

Legacy Android enrolment requires an EMM app catalogue on the device in order to install assigned applications.

Tap **OK** to add the Apps@Work shortcut to your home screen.

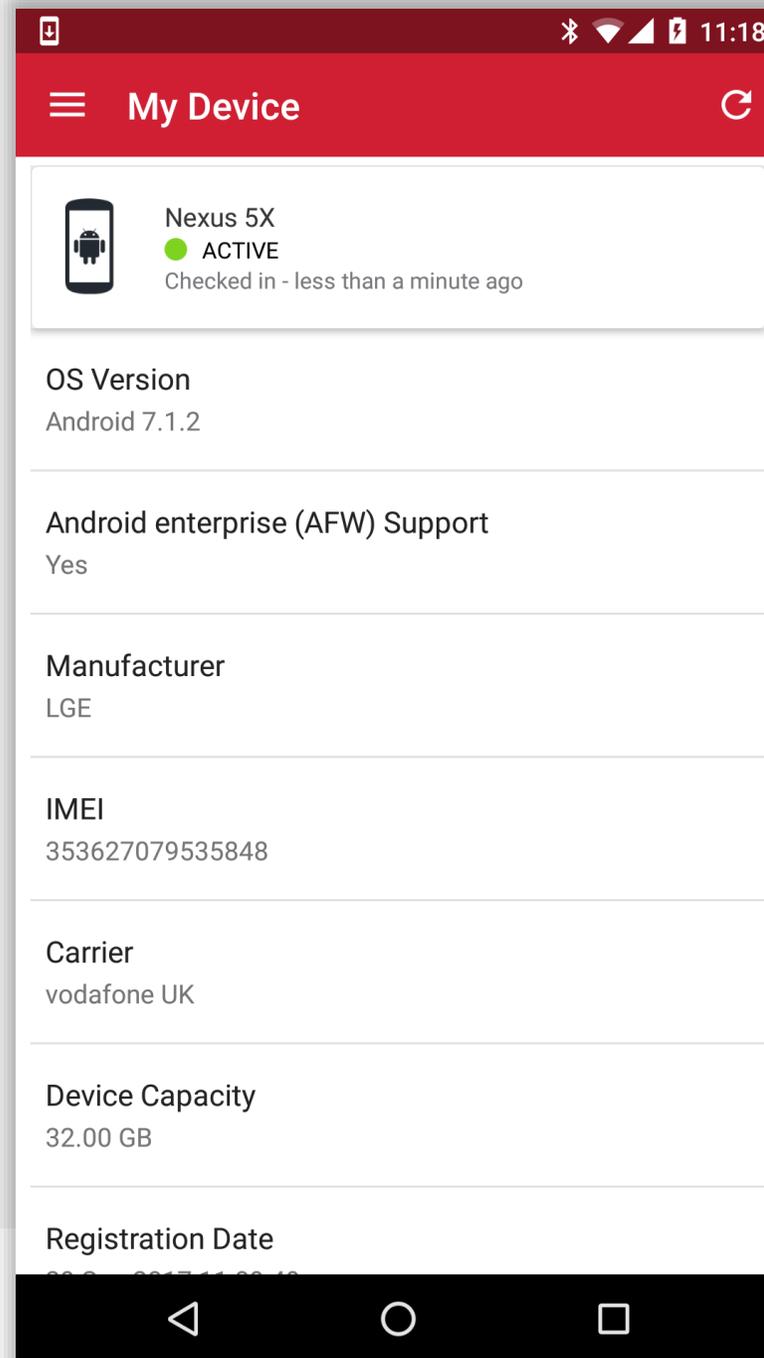




Configuration complete

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

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



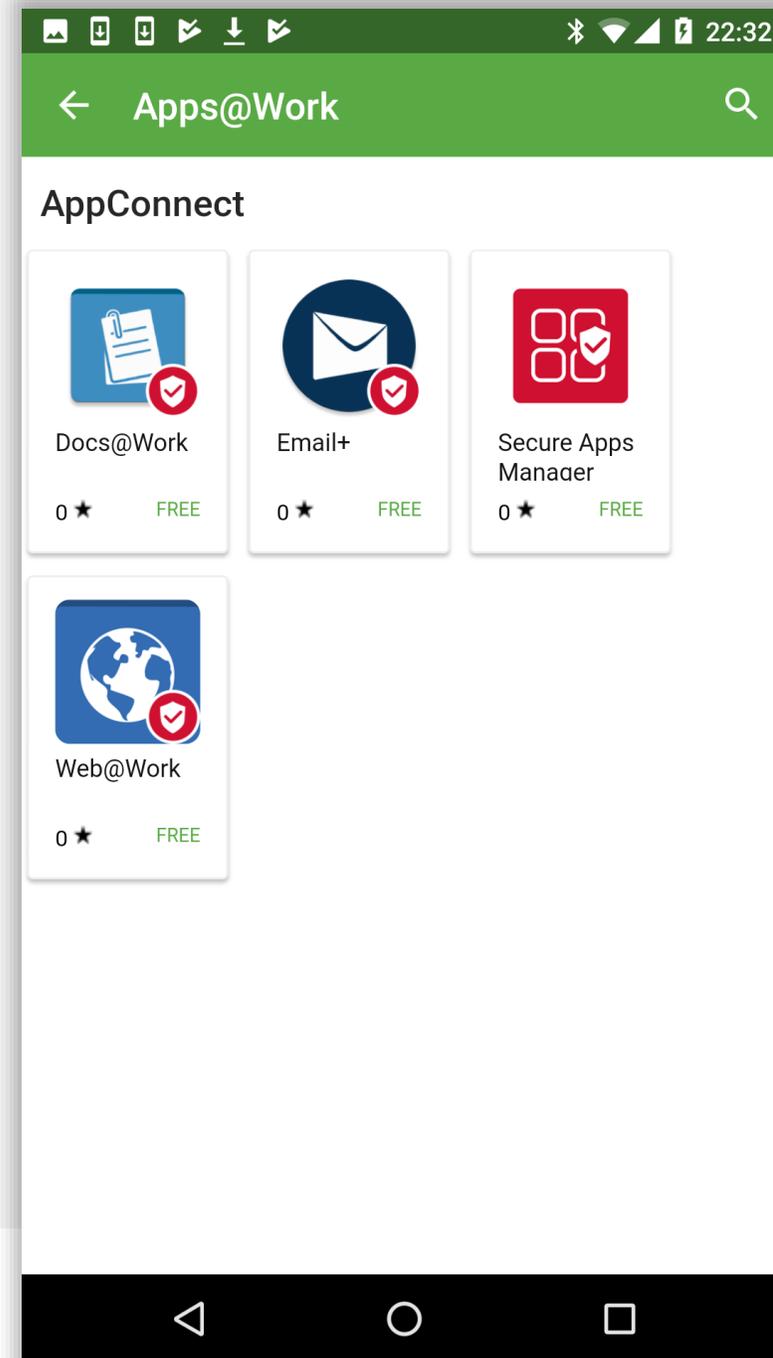


Installing applications

If you use a Samsung device, EMM-hosted applications like the AppConnect selection in the right-hand screenshot can be pushed down silently.

If you use any other device, such as the Nexus used for this guide, applications will not push and require you open the app catalogue in order to pull them down.

Public applications will redirect you to the Play Store for installation. They can't be installed silently.

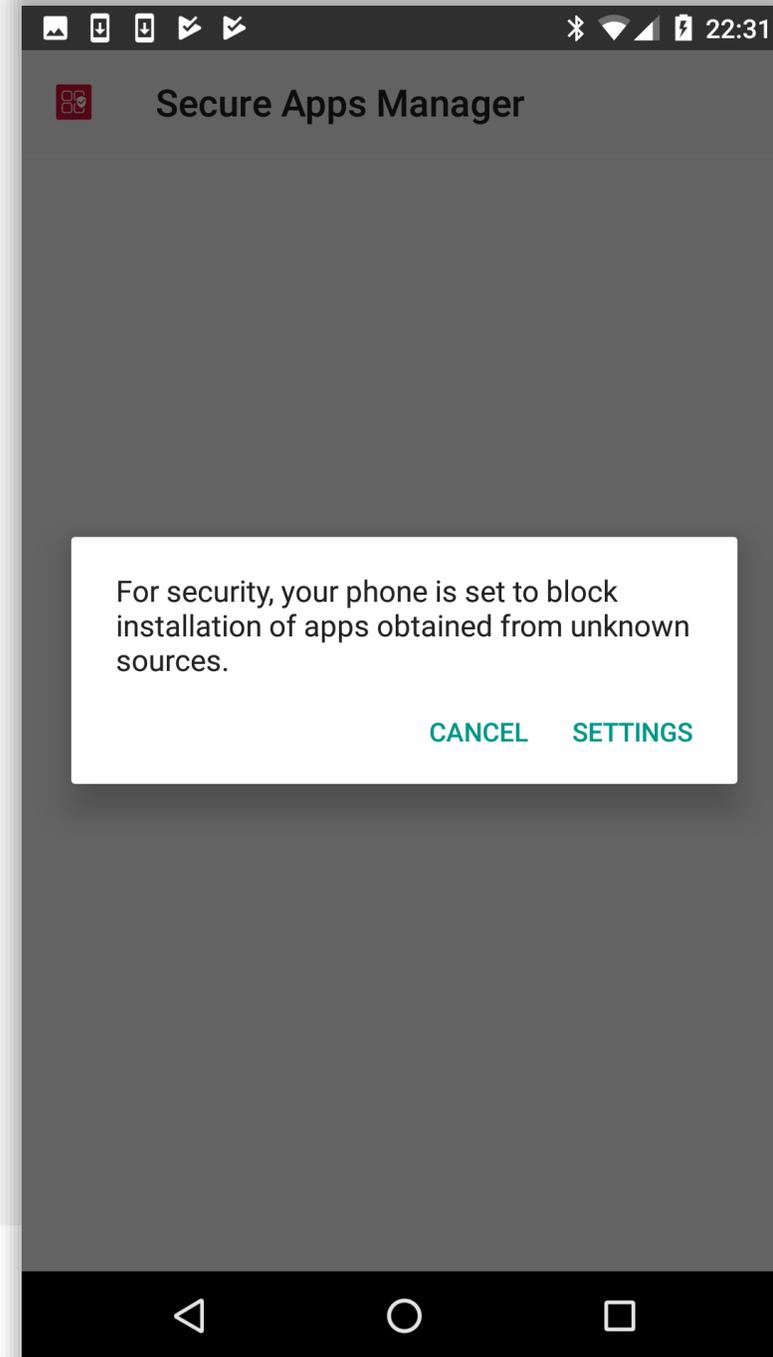




Installing applications

If installing in-house applications hosted and distributed through the EMM platform, unknown sources must be enabled on the device.

Tap **SETTINGS** to continue.



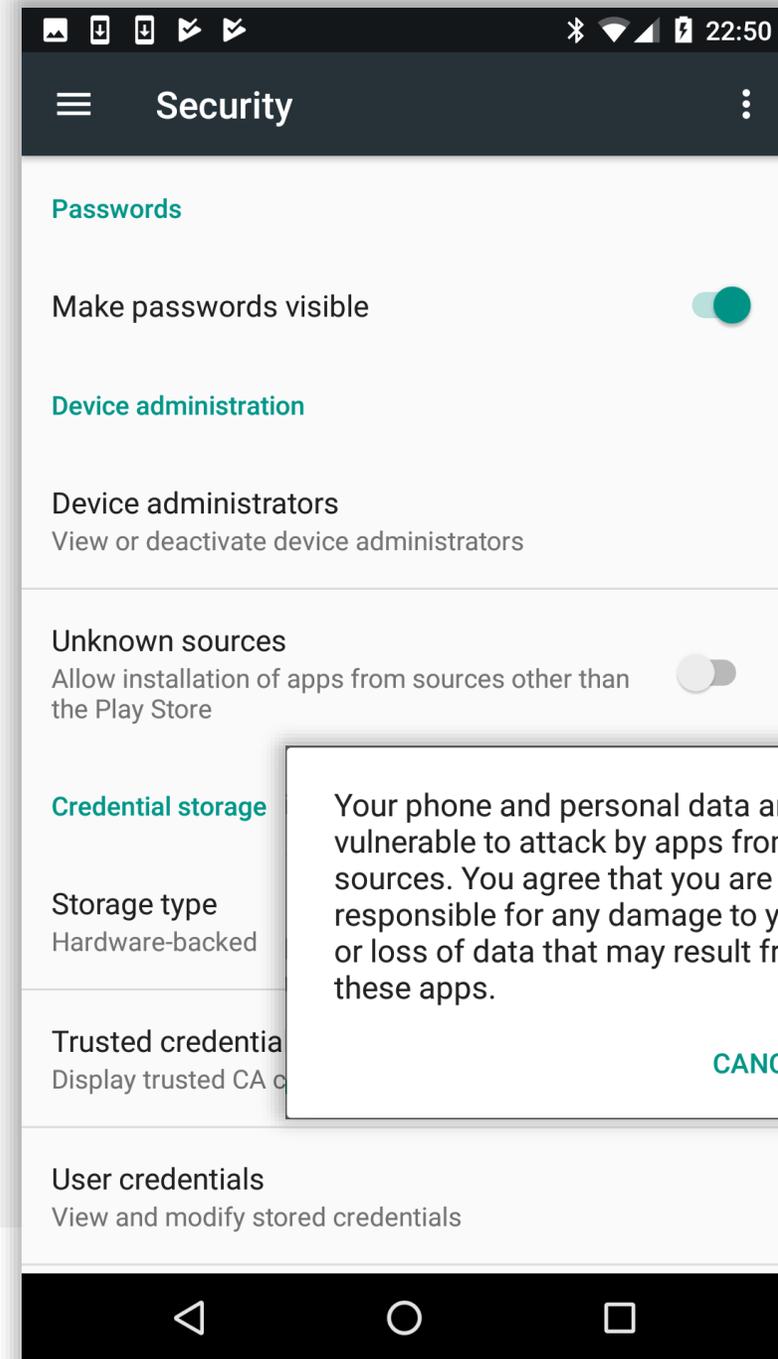


Installing applications

Scroll through settings until **Unknown sources** comes into view.

Tap the switch to enable unknown sources, then tap **OK** on the security warning that pops up to confirm you wish to continue.

You may now return to Apps@Work and tap to install the selected application once again.



bayton



Jason Bayton



bayton.org



/in/jasonbayton



@jasonbayton



+JasonBaytonX



jason@bayton.org

Updates to this document can be found here:

[Android enterprise provisioning guides](#)

