



SONY

Android enterprise

Fully managed work profile enrolment
Zero-touch provisioning



MobileIron Core



Android 8.x



Sony UI

March 2018

Enterprise Mobility documentation by baytuon



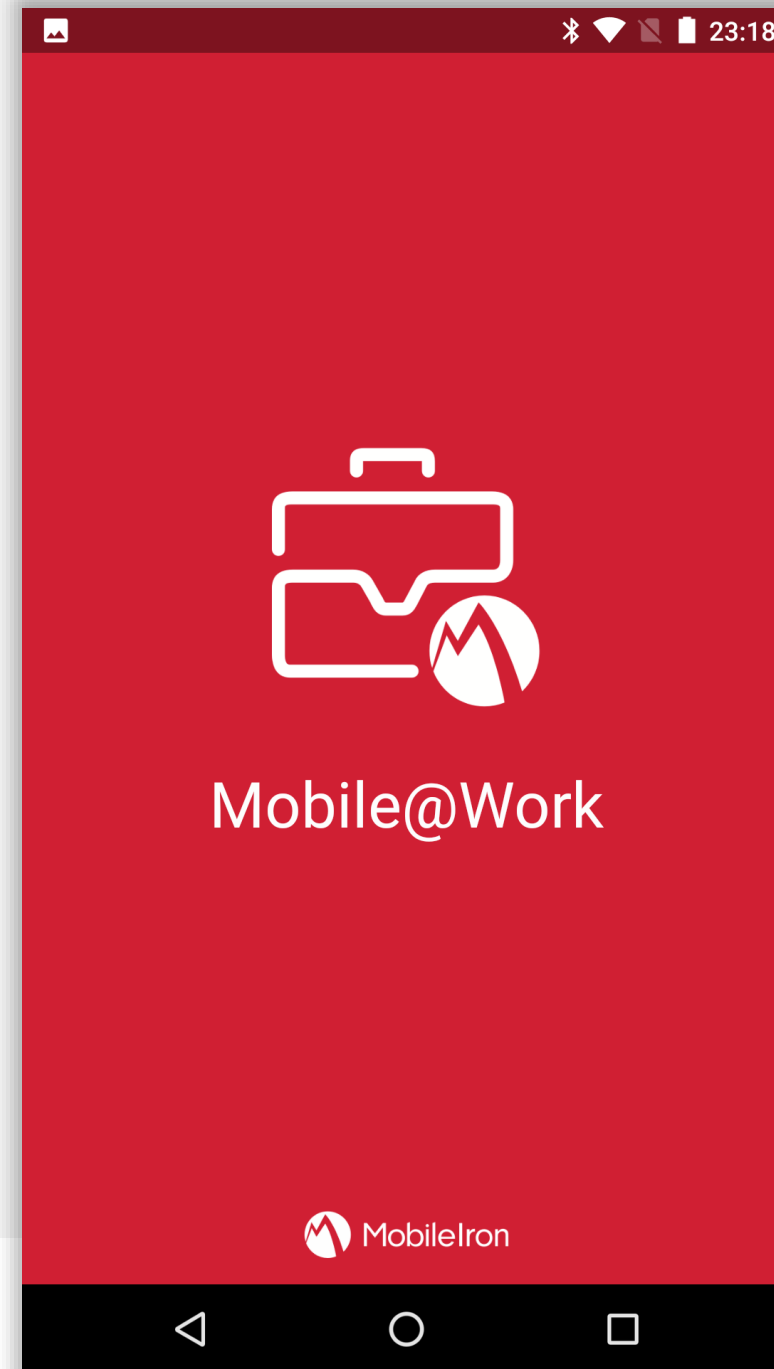
Requirements

In order to proceed, you must have:

- Android 8.0 or later installed on supported devices purchased from an authorised reseller.
- A functional MobileIron EMM solution in place of at least version 9.7 with Mobile@Work version 9.7
- An EMM and configurations assigned to devices in your zero-touch console.

Fully managed work profile offers a personally enabled, corporately controlled device environment suitable as a middle-ground between work profile and work-managed.

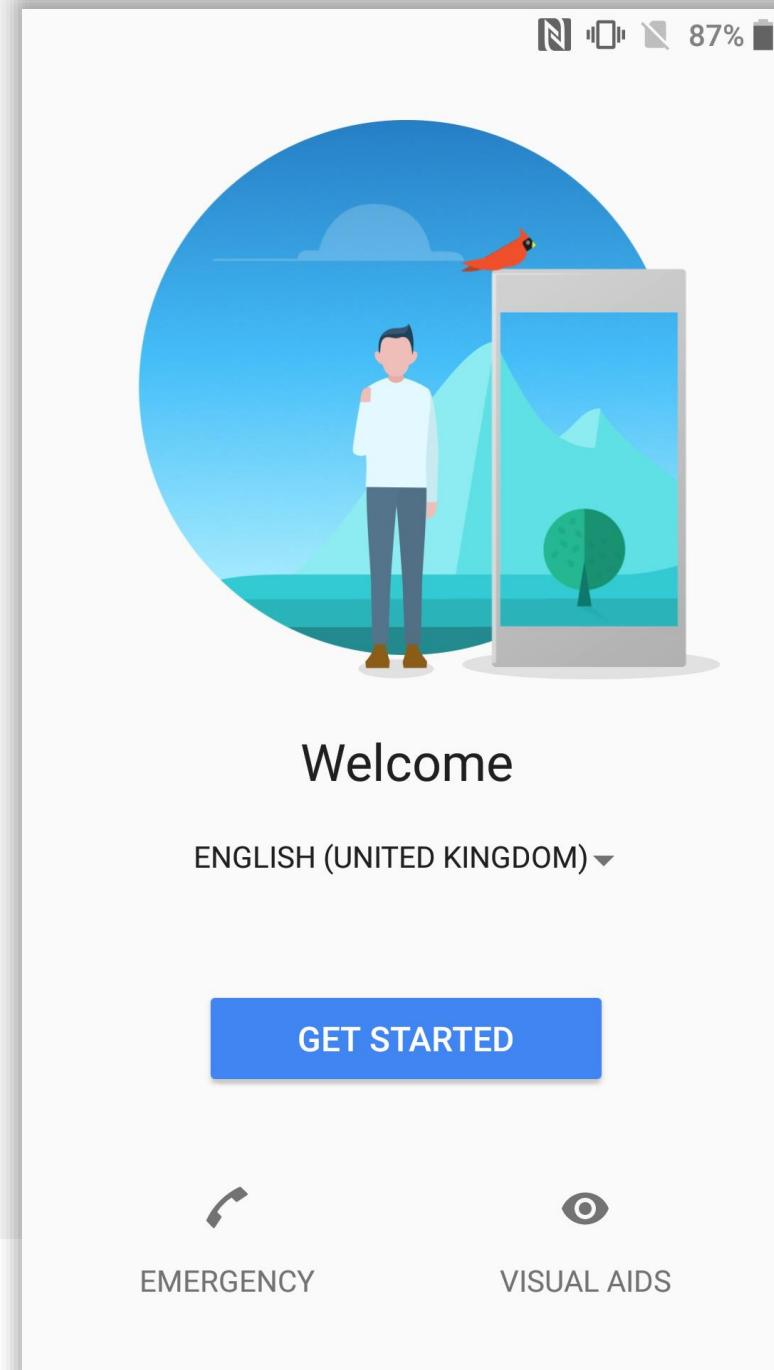
Zero-touch is currently limited to a small selection of devices and resellers. For devices running an Android version below 8.0 consider DPC identifier, QR or NFC provisioning.





Begin device setup


For zero-touch provisioning there are no special initial steps.
To begin, optionally change the language to reflect your locale
and tap **GET STARTED**.





Continue device setup


Tap **Accept** in order to continue, you may wish to opt out of Sony's Xperia diagnostics programme.



Important information

- ☒ I am aware of the [Important information](#) (warranty, safety, etc.)
- ☒ I am aware that [Data charges](#) may apply
- ☒ Yes, I want to help improve Xperia™ by sharing [Diagnostics](#) (optional)

ACCEPT



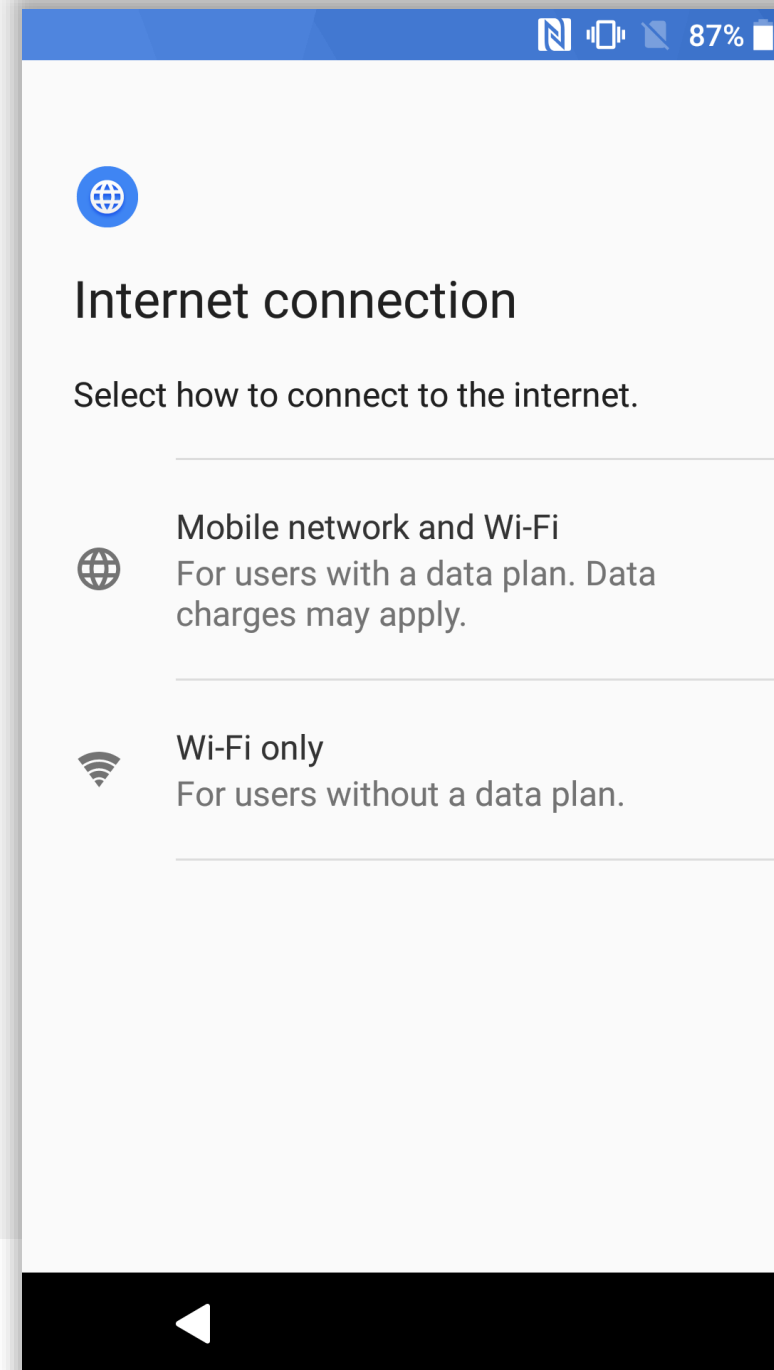


Continue device setup

The Xperia offers two connectivity options for setting up the device.

If you don't have a data plan, tap **Wi-Fi only** and this will not seek to use mobile data during setup.

Otherwise, it's recommended to tap **Mobile network and Wi-Fi** to allow the device to use either available option (WiFi will be set up in the following steps in either case).

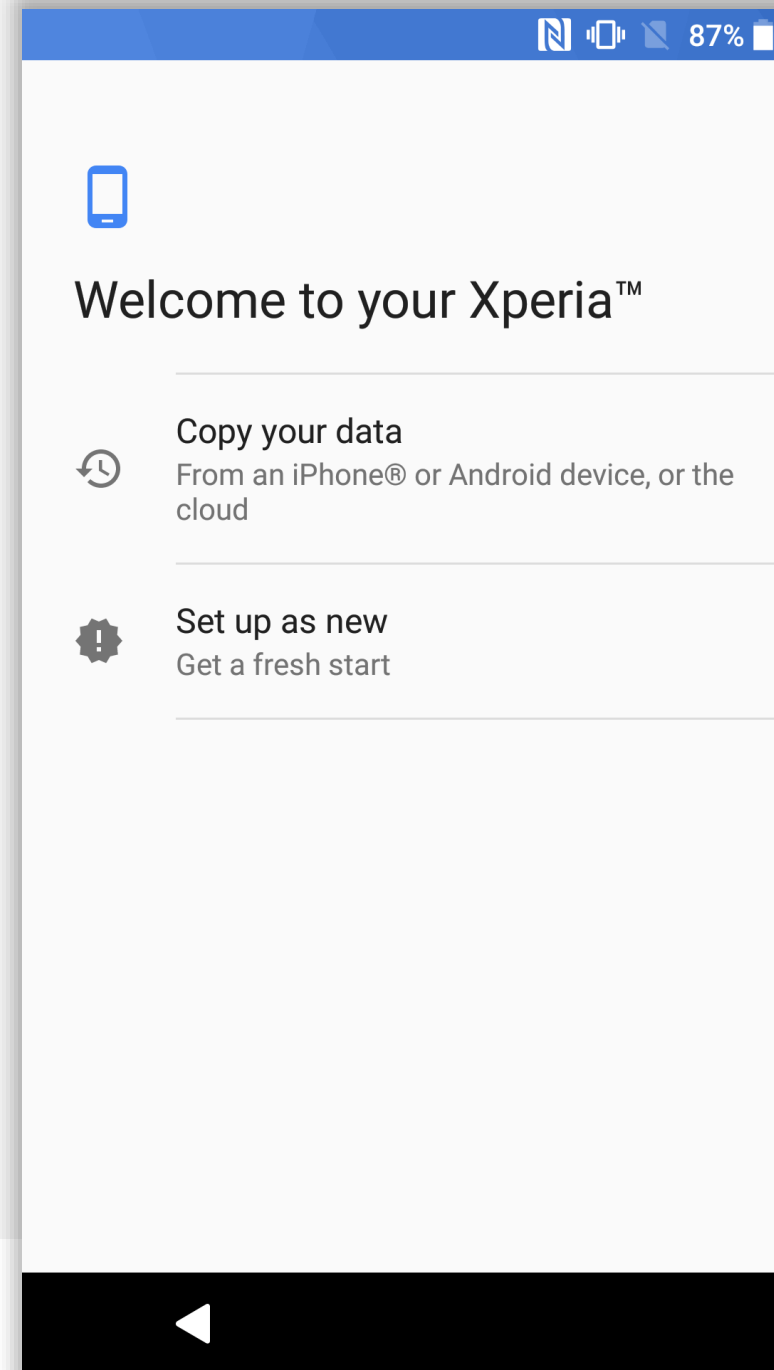




Continue device setup

Tap **Set up as new**.

Selecting **Copy your data** does not initiate the accounts copy with zero-touch even if it is accidentally (or purposefully) tapped.



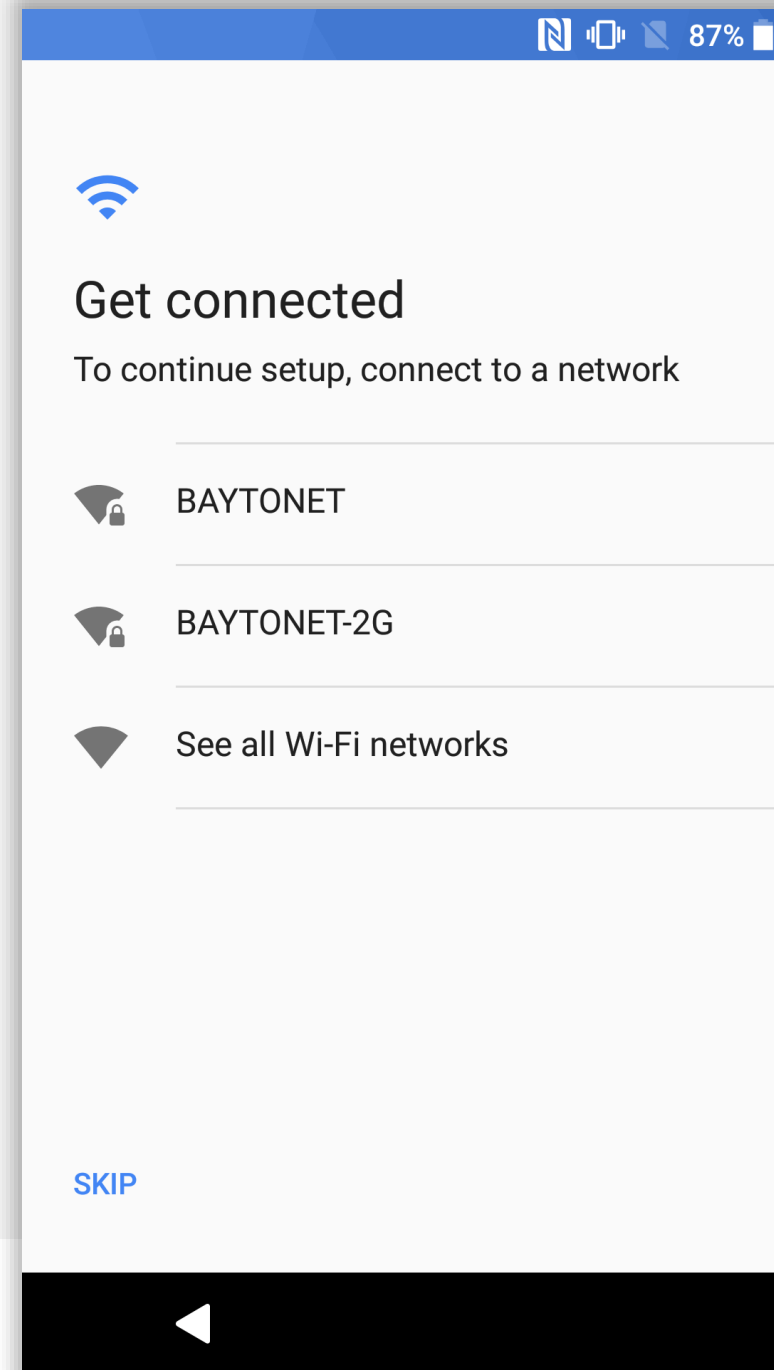


Continue device setup

The device requires connectivity in order to download the DPC and, later, policies & configs.

Connect to a WiFi network. The device will automatically progress once a connection has been made.

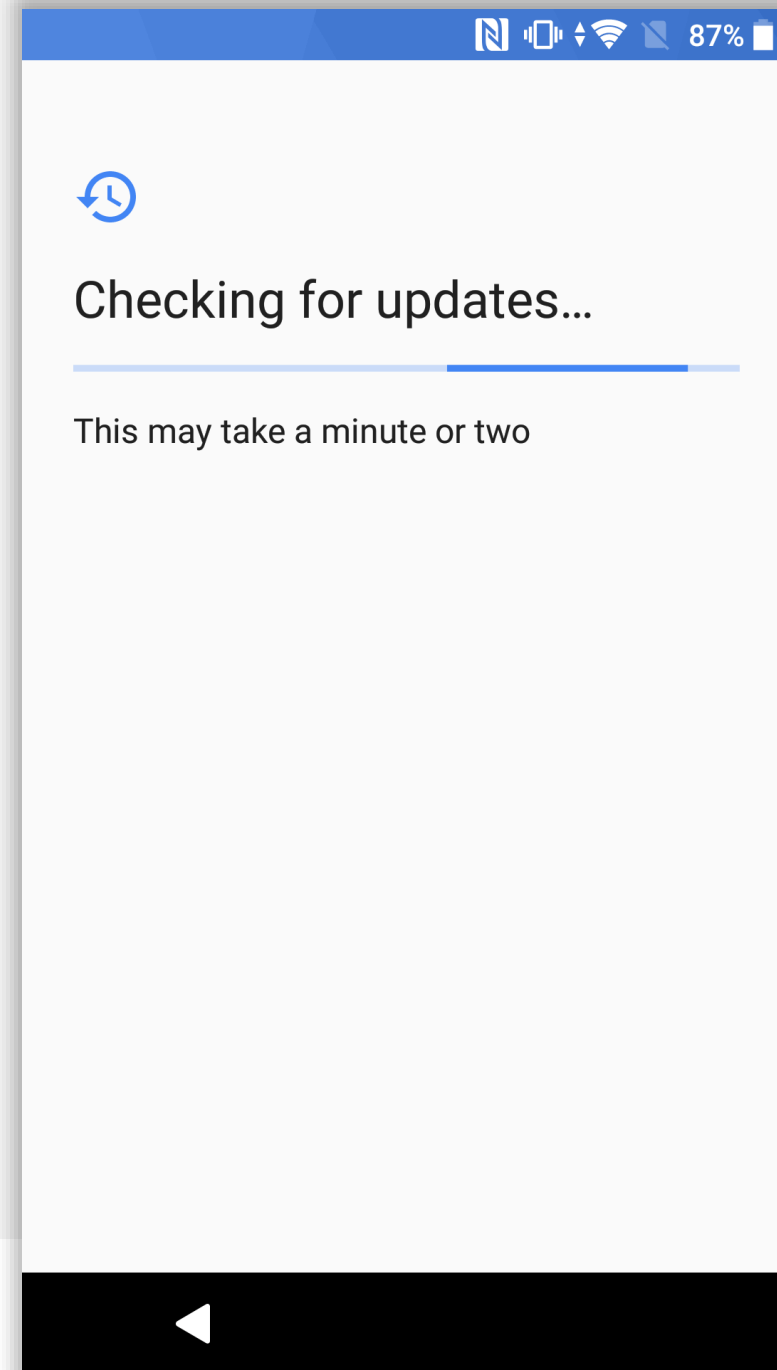
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup** (not pictured).





Continue device setup

Once connected, the device will check for updates and automatically continue when complete.





Provisioning in progress

The device will now prompt you with a notice stating the device will be managed by the organisation.

Tap **ACCEPT & CONTINUE**.



Set up your device

This device will be managed and kept secure by Bayton.org. Terms from Google apply.

[View terms](#)

If you have questions, contact your [organisation's admin](#).

Bayton.org will manage this device using the following app:



Mobile@Work

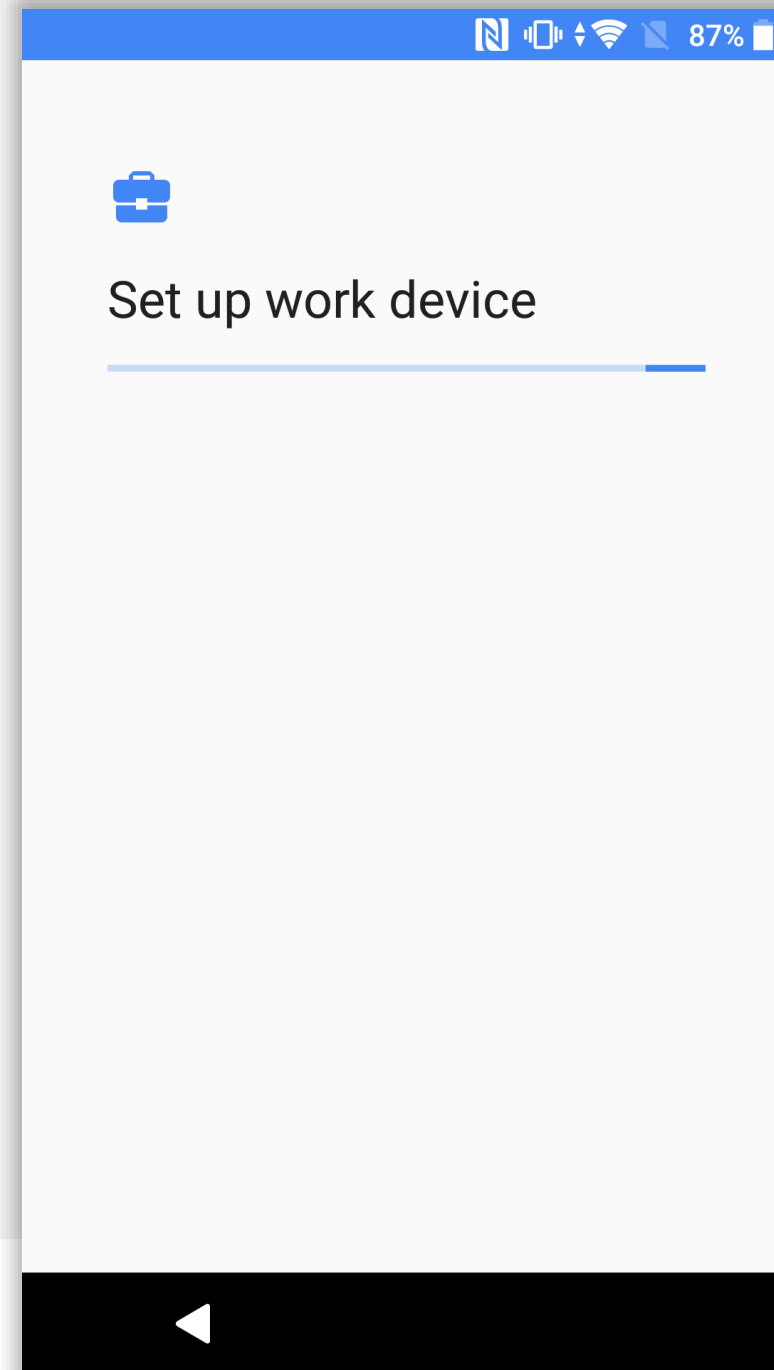
ACCEPT & CONTINUE





Provisioning in progress

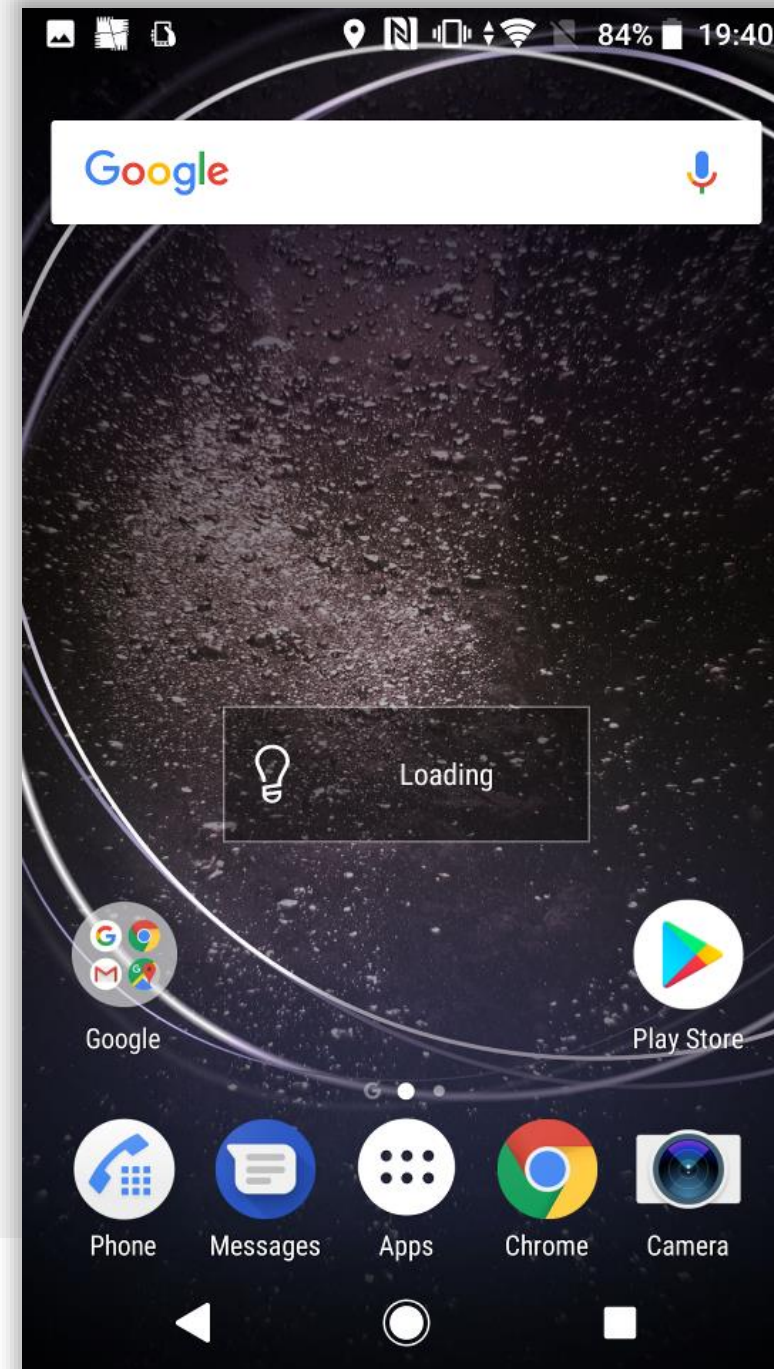
The device will now download the DPC and automatically move to the next step in the process.





Provisioning complete

When zero-touch provisioning is complete, the DPC will automatically launch from the home screen. There is no need to manually open the DPC.






Begin enrolment

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

Note: This may be skipped if you've configured DPC extras to pre-fill the URL.



10:44

Get Ready for Work with MobileIron

To configure and secure your device, enter your company email

COMPANY EMAIL

Email

Or register with server URL

NEXT



Continue enrolment

Once 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**.

COMPANY EMAIL
jason@bayton.org

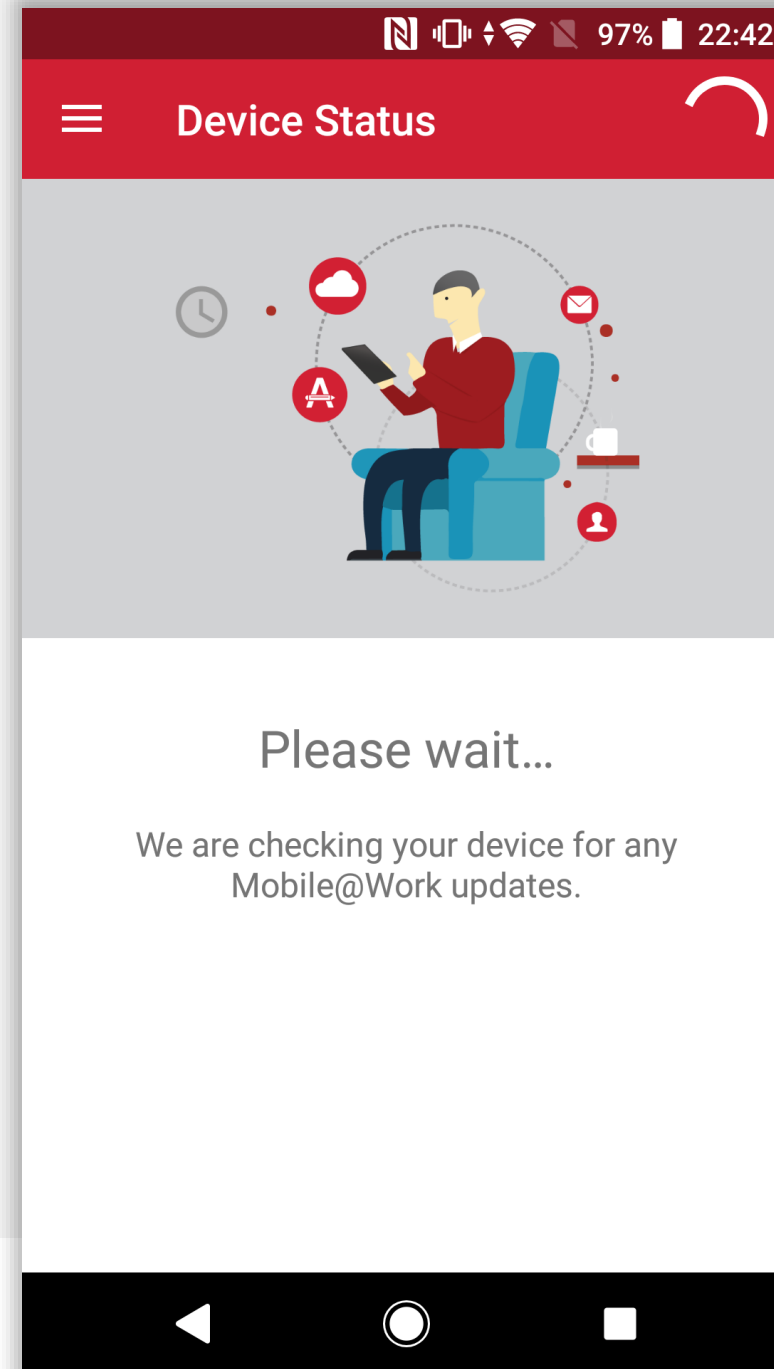
PASSWORD
Password

SIGN IN



Device configuration

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



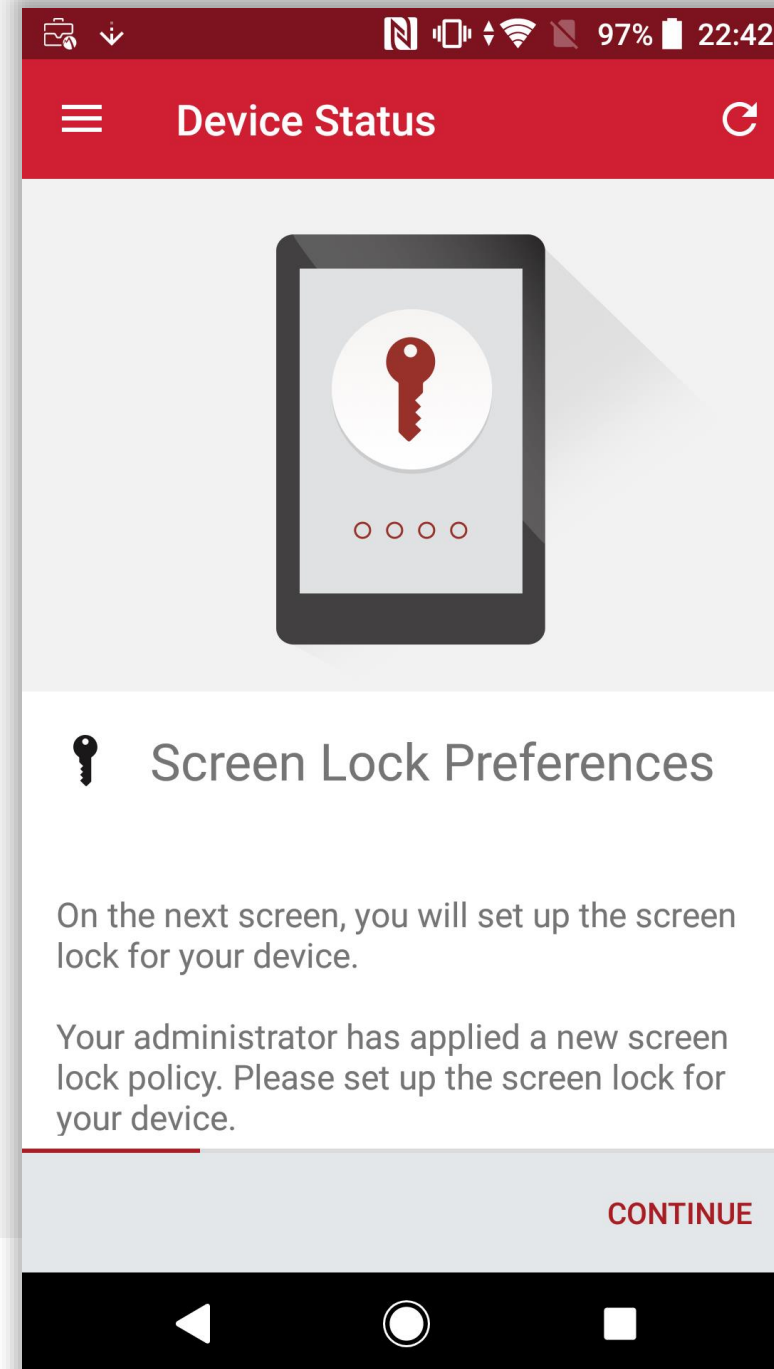


Device configuration

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.

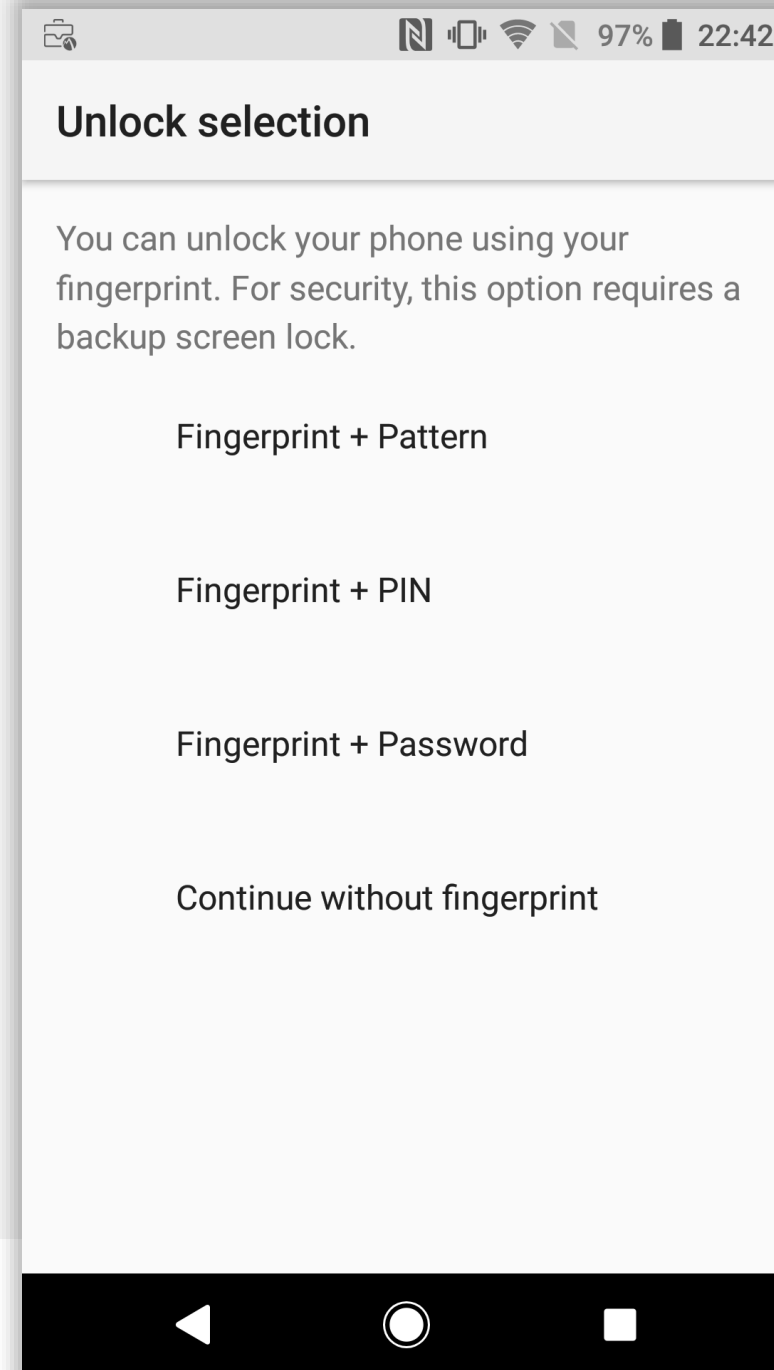
Tap **CONTINUE**.





Device configuration

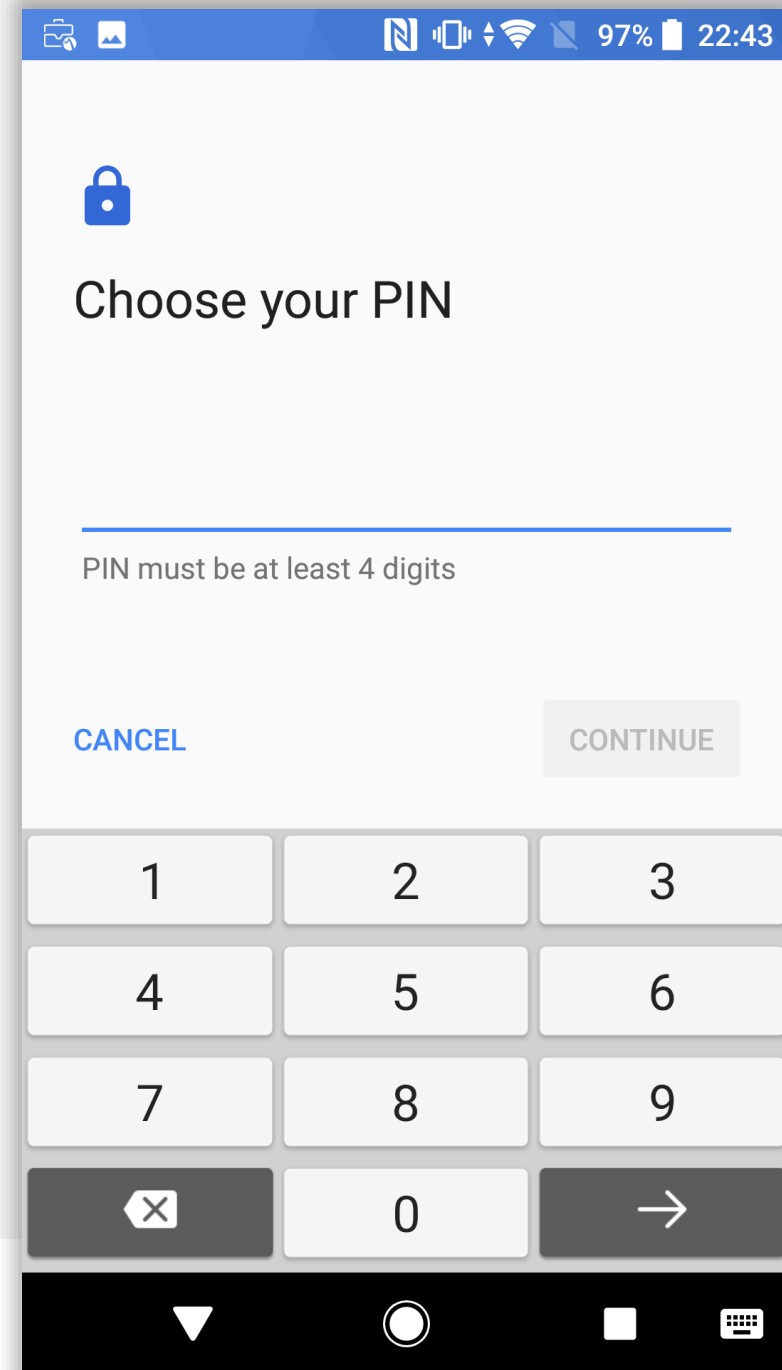
Select the relevant passcode, or skip fingerprint setup here and select a passcode on the following prompt, some options may not be available depending on the security policy deployed.





Device configuration

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



The image shows a smartphone screen with a blue status bar at the top displaying various icons and 97% battery. The main screen has a white background with a blue lock icon at the top. Below it, the text "Choose your PIN" is displayed. A horizontal line indicates the input field, with the text "PIN must be at least 4 digits" below it. At the bottom of the screen, there are two buttons: "CANCEL" in blue text and "CONTINUE" in a light gray box. Below these buttons is a numeric keypad with digits 1-9, 0, a backspace key (X), and a right arrow key. The bottom of the phone shows the standard Android navigation bar with a triangle, circle, and square icon, and a keyboard icon on the right.

Choose your PIN

PIN must be at least 4 digits

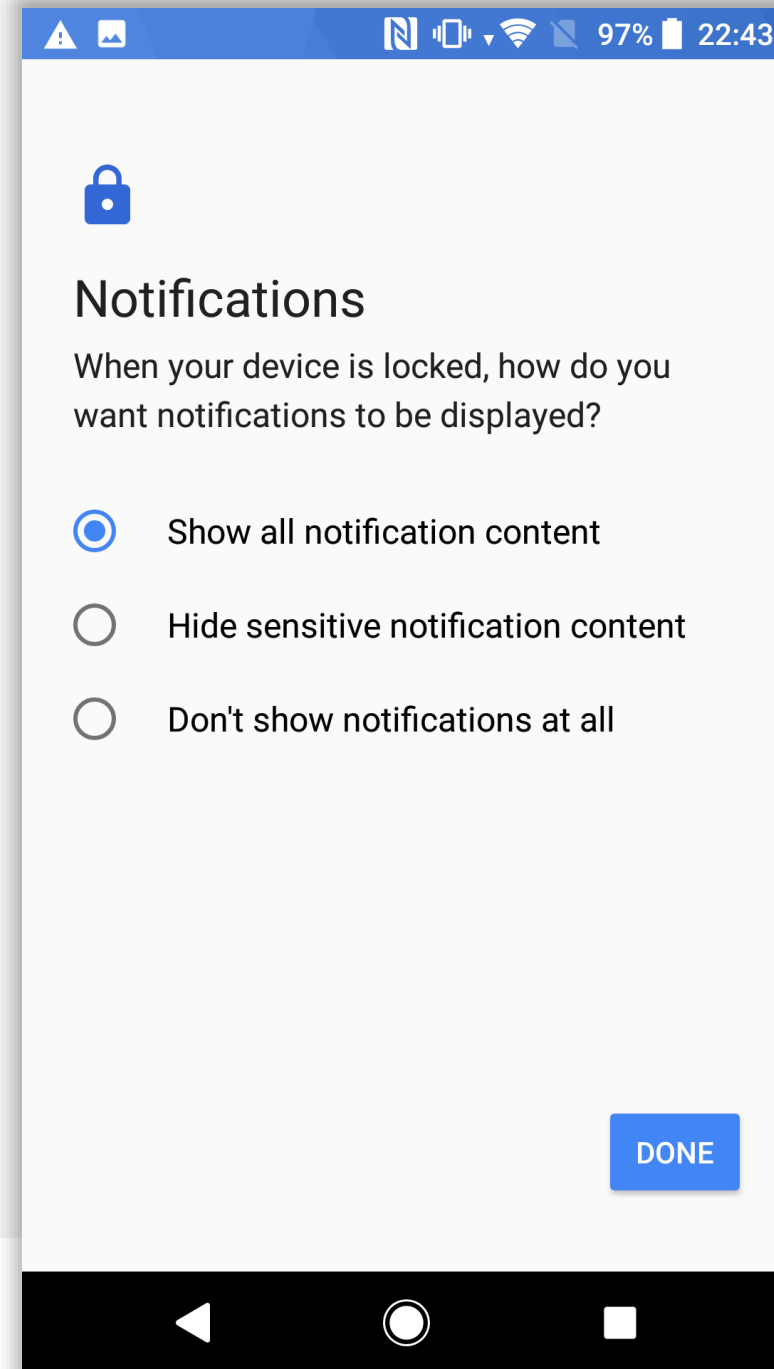
CANCEL CONTINUE

1 2 3
4 5 6
7 8 9
X 0 →



Device configuration

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



The image shows a screenshot of an Android phone's notification settings. At the top, the status bar displays various icons including a warning triangle, a picture icon, a lock icon, a signal strength indicator, a battery level of 97%, and the time 22:43. Below the status bar, there is a blue header with a white lock icon. The main title is "Notifications" in bold black text. Below the title, a subtitle reads "When your device is locked, how do you want notifications to be displayed?". There are three radio button options: "Show all notification content" (selected), "Hide sensitive notification content", and "Don't show notifications at all". At the bottom right, there is a blue button with the text "DONE". The bottom of the screen shows the standard Android navigation bar with a back arrow, a home circle, and a recent apps square.

Notifications

When your device is locked, how do you want notifications to be displayed?

- ☒ Show all notification content
- ☐ Hide sensitive notification content
- ☐ Don't show notifications at all

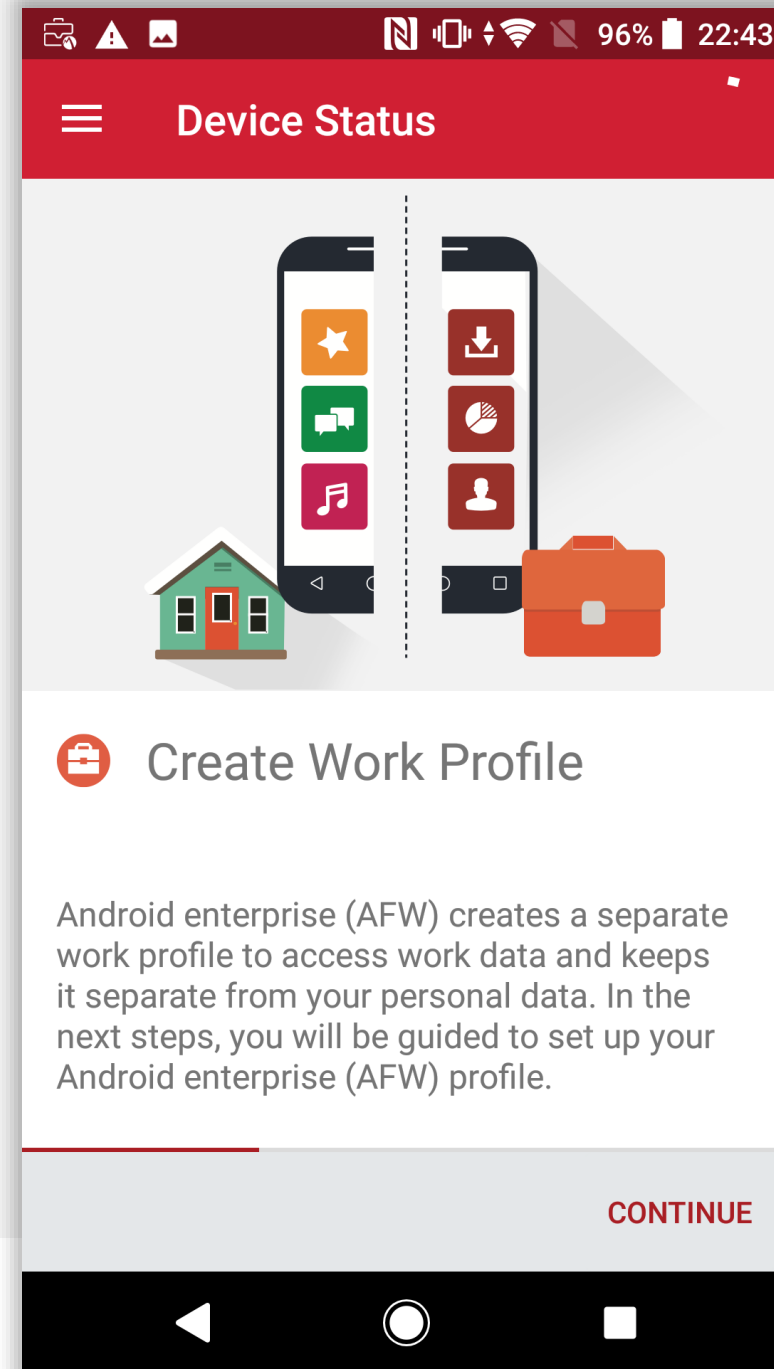
DONE



Work profile configuration

The device has now completed initial device configuration and will continue to set up the dedicated work profile. This will allow for separation of work apps from the personally-enabled parent profile on the device.

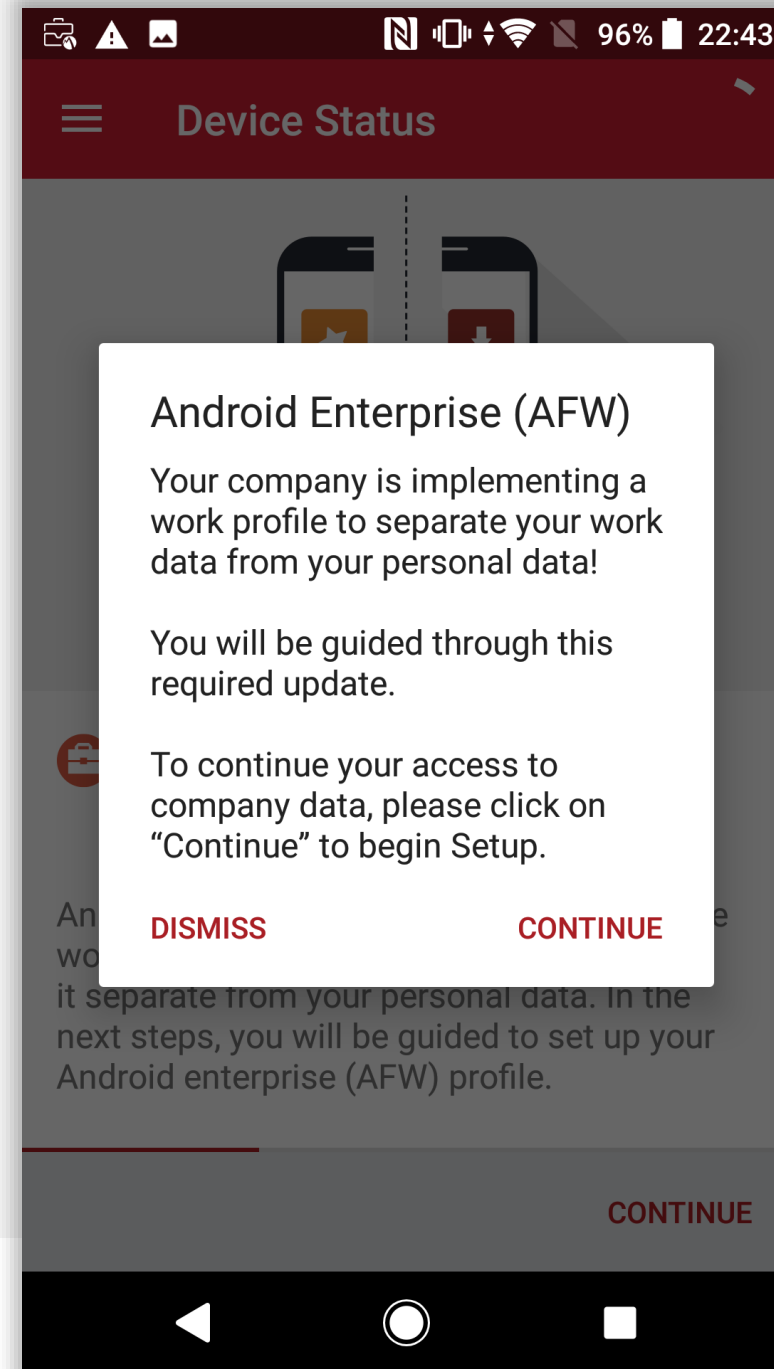
Tap **CONTINUE**.





Work profile configuration

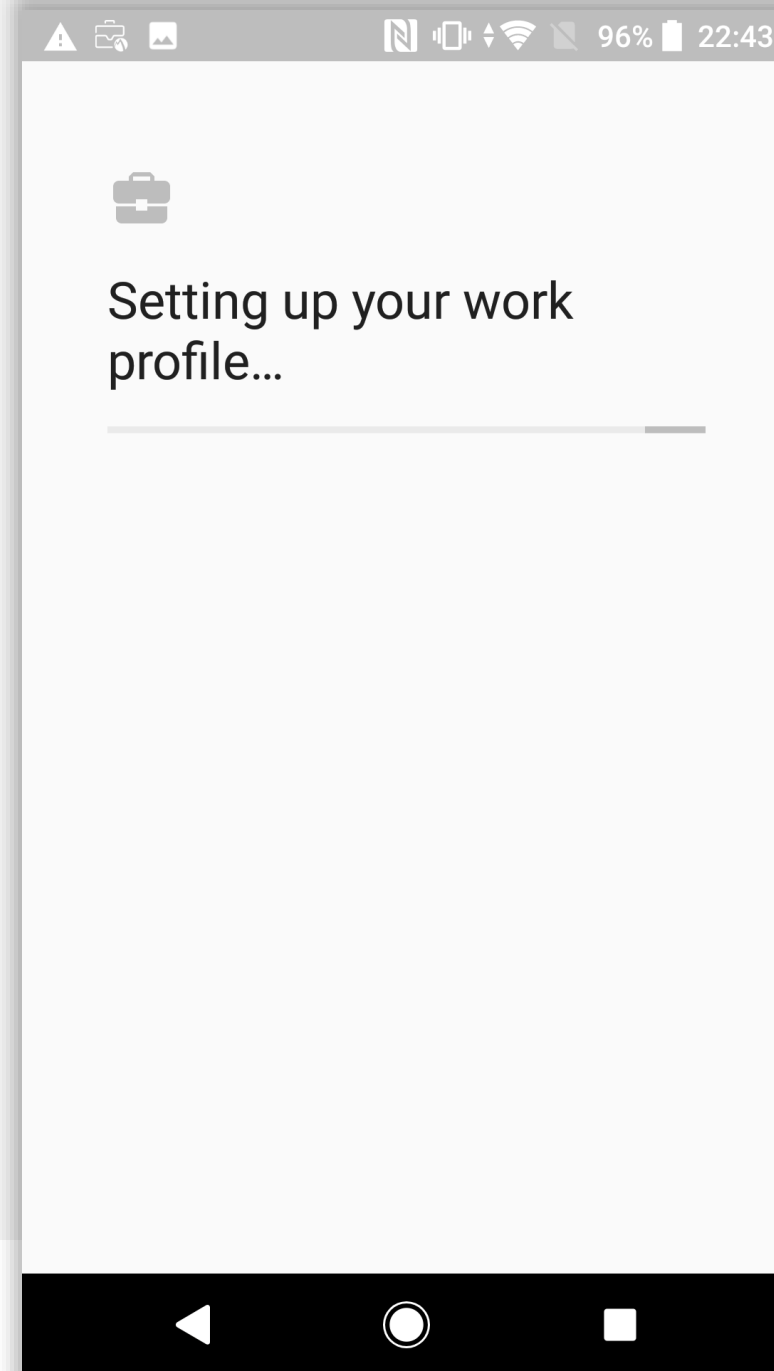
Accept the prompt, tap CONTINUE.





Work profile configuration

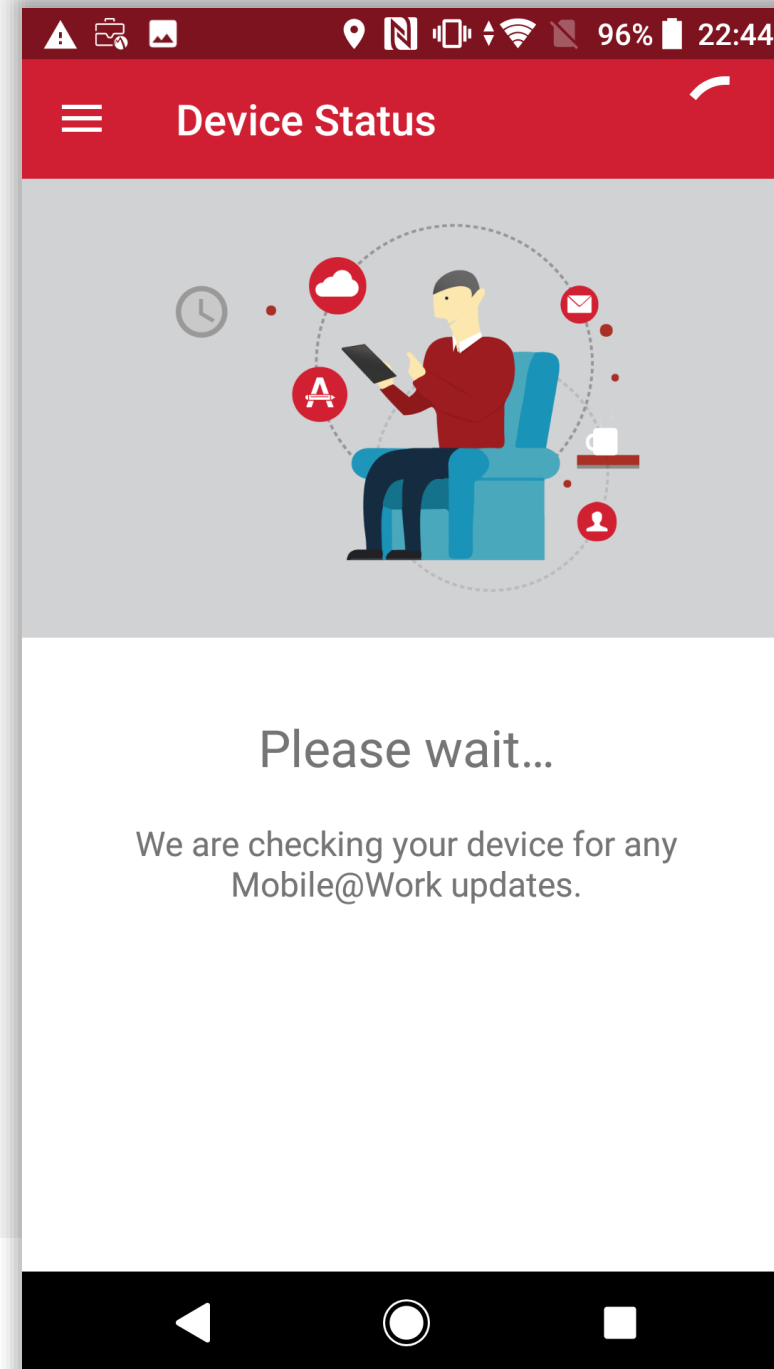
The device will now set up the work profile. This should be relatively quick and there is nothing needing to be done. This will automatically continue to the next step.





Work profile configuration

The device will now check-in to the Core, and begin undertaking tasks in the background. Once ready, enrolment will complete.



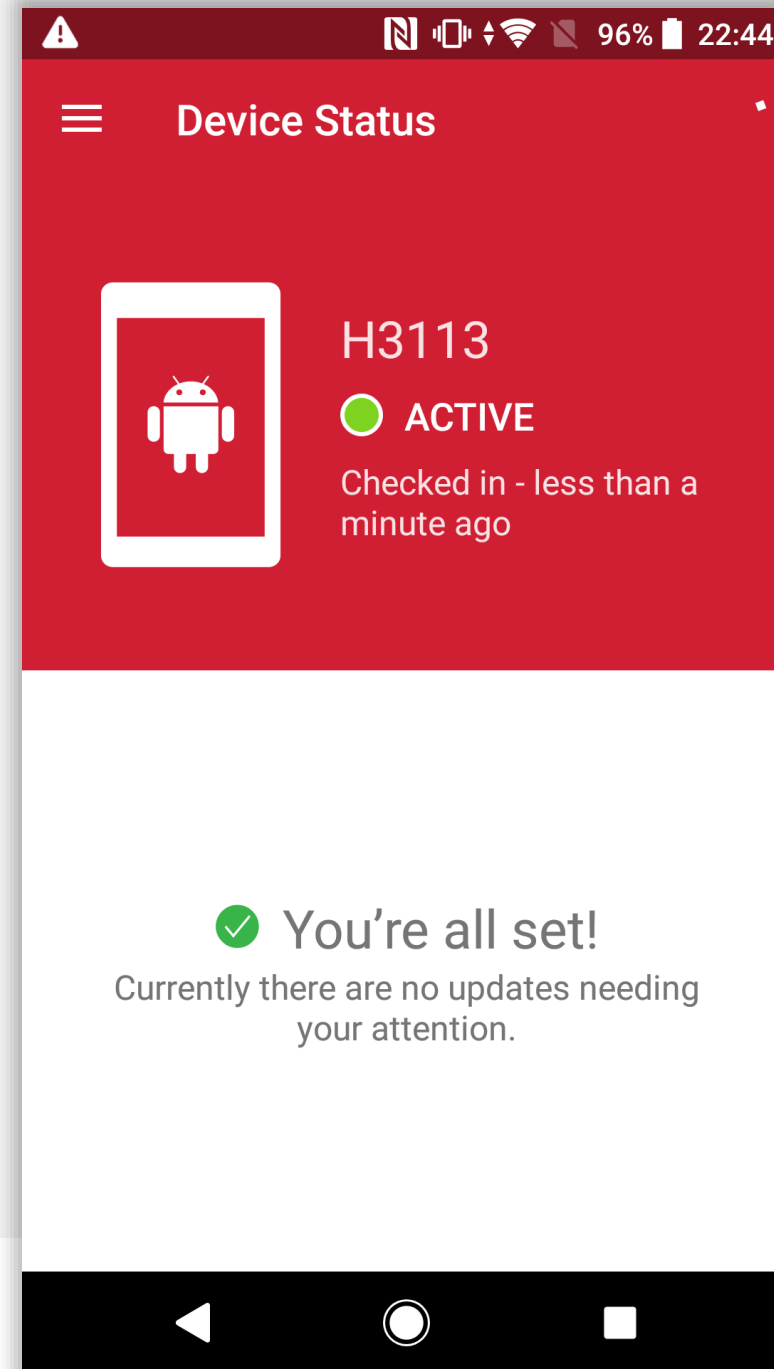


Enrolment complete

The device has now completed enrolment 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.

Continue the guide to add a personal account to the device.
If this is not required, finish the guide here.

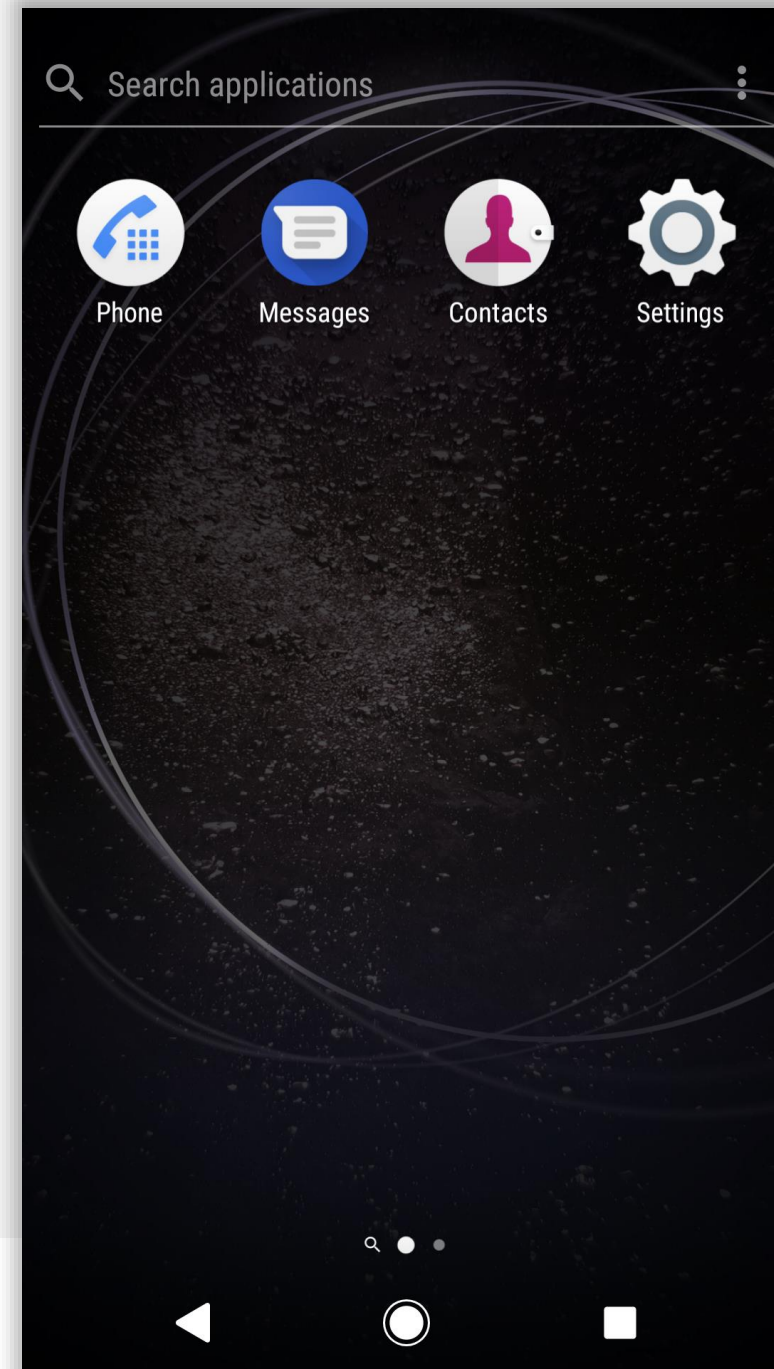




Add a personal account

The device will be relatively vanilla at this point on the parent profile. Unlike a normal BYOD setup, there is no setup wizard for the user in a fully managed work profile deployment, meaning it is necessary to add a personal account manually.

Open the app drawer, and tap **Settings**.

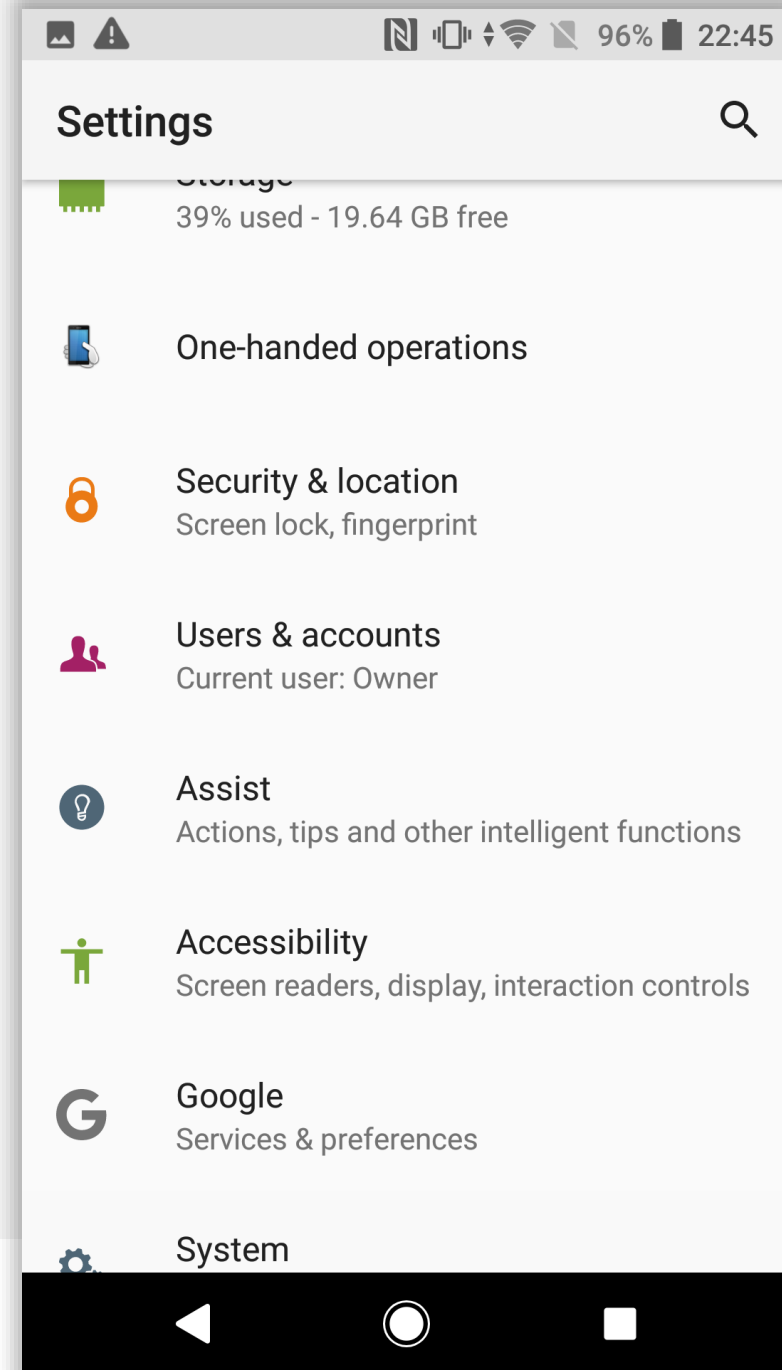




Add a personal account

Scroll down Settings until you find Users & accounts.

Tap Users & accounts.

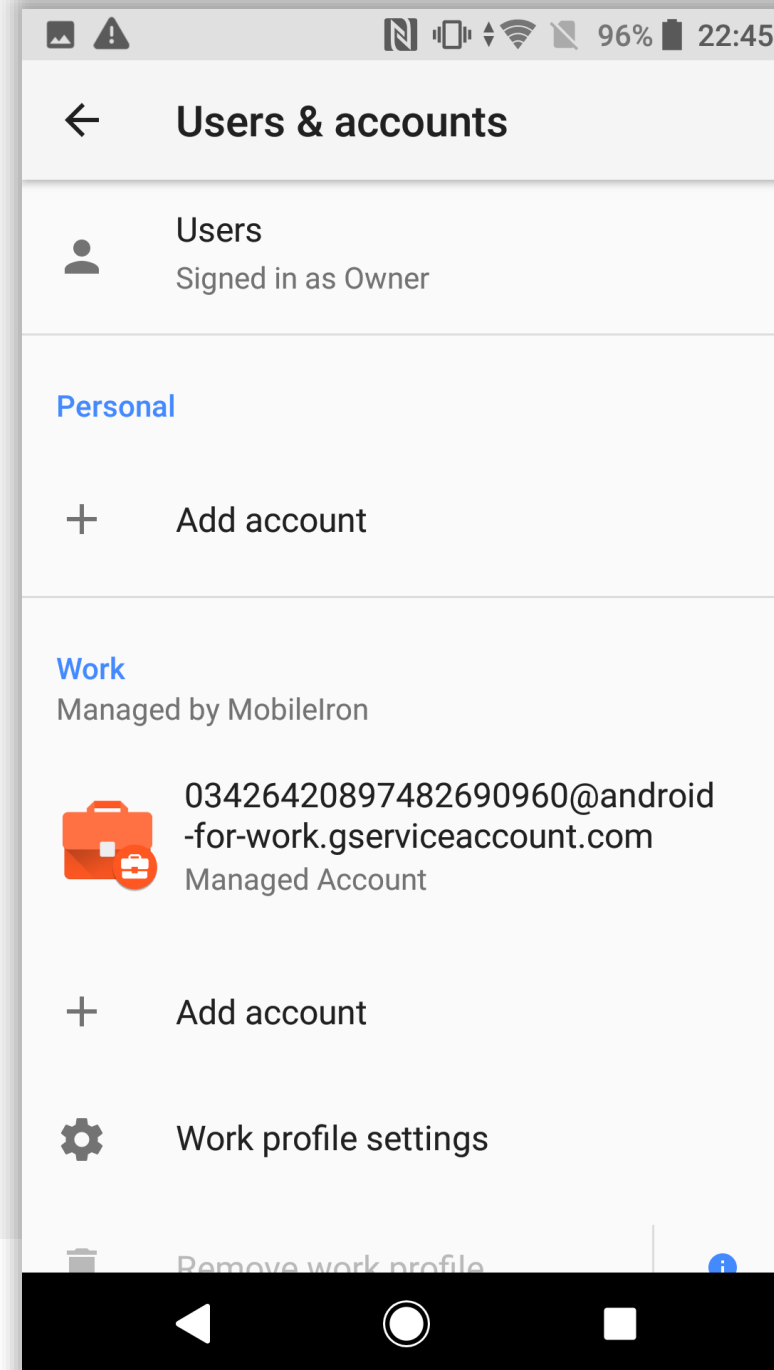




Add a personal account

You will notice there is a Work account configured, but the Personal side is empty.

Tap **Add account**.



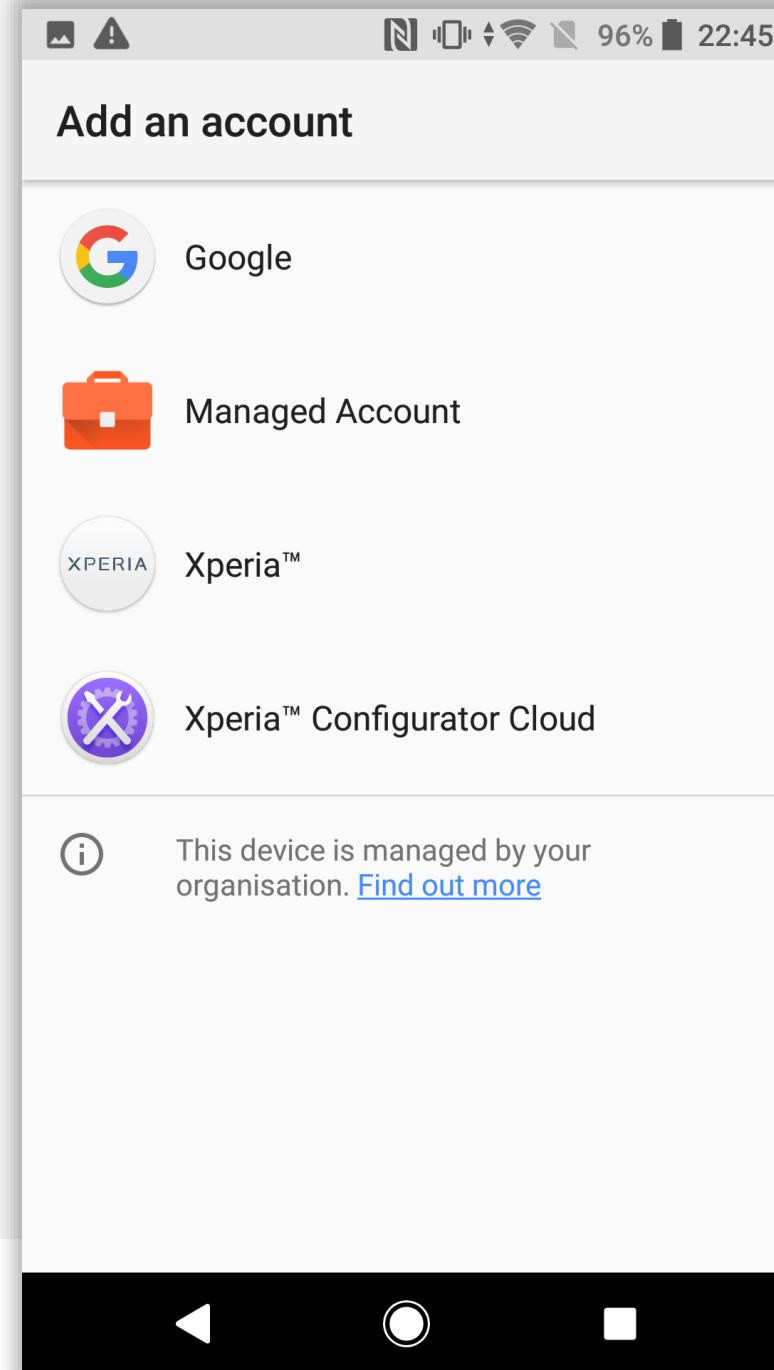


Setup complete

Tap the account you would like to add, then go through the sign-in process.

Note: More account options will show up here as applications are installed, however a good starting point to enabling that will be to add a Google account.

Warning: G Suite accounts are **not** supported in the parent profile, regardless of whether or not Android management is configured for the G Suite tenant. If a G Suite account is added then the Play Store will become managed and not allow unrestricted app downloads.



bayton



Jason Bayton



bayton.org



/in/jasonbayton



@jasonbayton



+JasonBaytonX



jason@bayton.org

Updates to this document can be found here:

[Android enterprise provisioning guides](#)

