

Android enterprise

Fully managed work profile enrolment
NFC provisioning



MobileIron Core



Android 8.x



Sony UI

March 2018



SONY

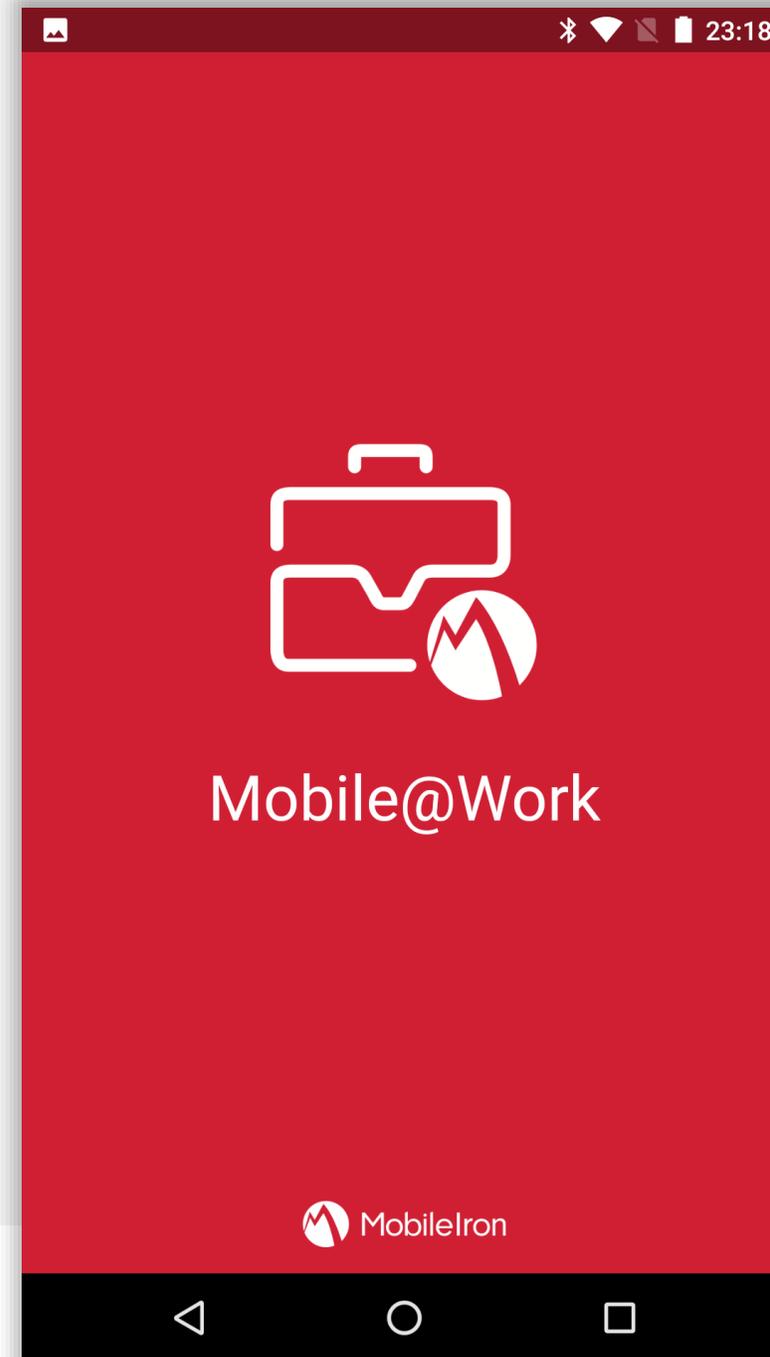


Requirements

In order to proceed, you must have:

- Android 8.0 or later installed on the devices to be provisioned.
- A spare device with NFC to “bump” the devices to be provisioned.
- NFC functionality enabled out of the box for devices to be provisioned.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.

NFC provisioning is the earliest form of Android enterprise Work-Managed enrolment and cannot be done remotely. Consider as an alternative QR enrolment or zero-touch enrolment; these do allow enrolment remotely.





Configure the provisioner

The provisioner app must be installed on a spare device that is not going to be enrolled onto the EMM platform.

Once downloaded from [Google Play](https://play.google.com/store/apps/details?id=com.bayton.provisioner), open the Provisioner app, then set the following:

- App for Provisioning (Mobile@Work).
- WiFi SSID.
- WiFi Security Type.
- WiFi Password.

All of these fields are mandatory, the time zone and locale are normally automatically set. Optionally, the Core URL and username may be added also.

Tap **CONTINUE** to begin the provisioning process.

The screenshot shows the Provisioner app interface on an Android device. The status bar at the top indicates 35% battery and the time 19:46. The app title "Provisioner" is displayed in a red header. The main content area contains the following fields and settings:

- Provisioning Method:** NFC
- App For Provisioning:** Mobile@Work
- Time Zone:** GMT+00:00 Greenwich Mean Time
- Locale:** English (United Kingdom)
- Enable All System Apps:**
- Wi-Fi Details:**
 - Wi-Fi Network SSID:** BAYTONET
 - Wi-Fi Security Type:** WPA
 - Wi-Fi Password:** [Redacted]
- For Bulk Enrollment:**
 - Hostname:** beta.core.bayton.org
 - Username:** [Redacted]

A red **CONTINUE** button is located at the bottom right of the screen.

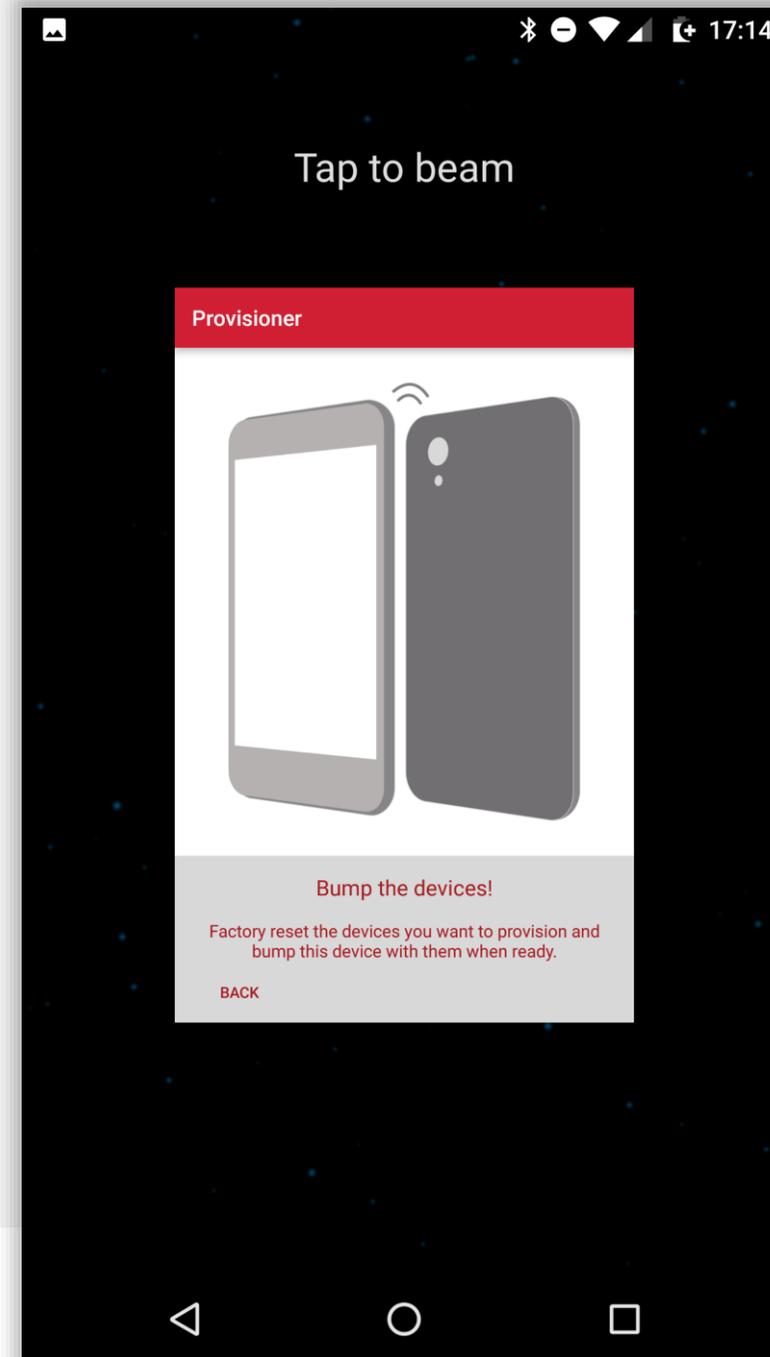


Bump the devices

Locate the NFC radios on both the provisioning device and the device to be provisioned.

Touch the two devices together until a sound is heard and an animation played on the provisioning device. The device to be provisioned should also indicate a successful connection has been made.

Tap the screen on the provisioning device in order to transmit the NFC payload.



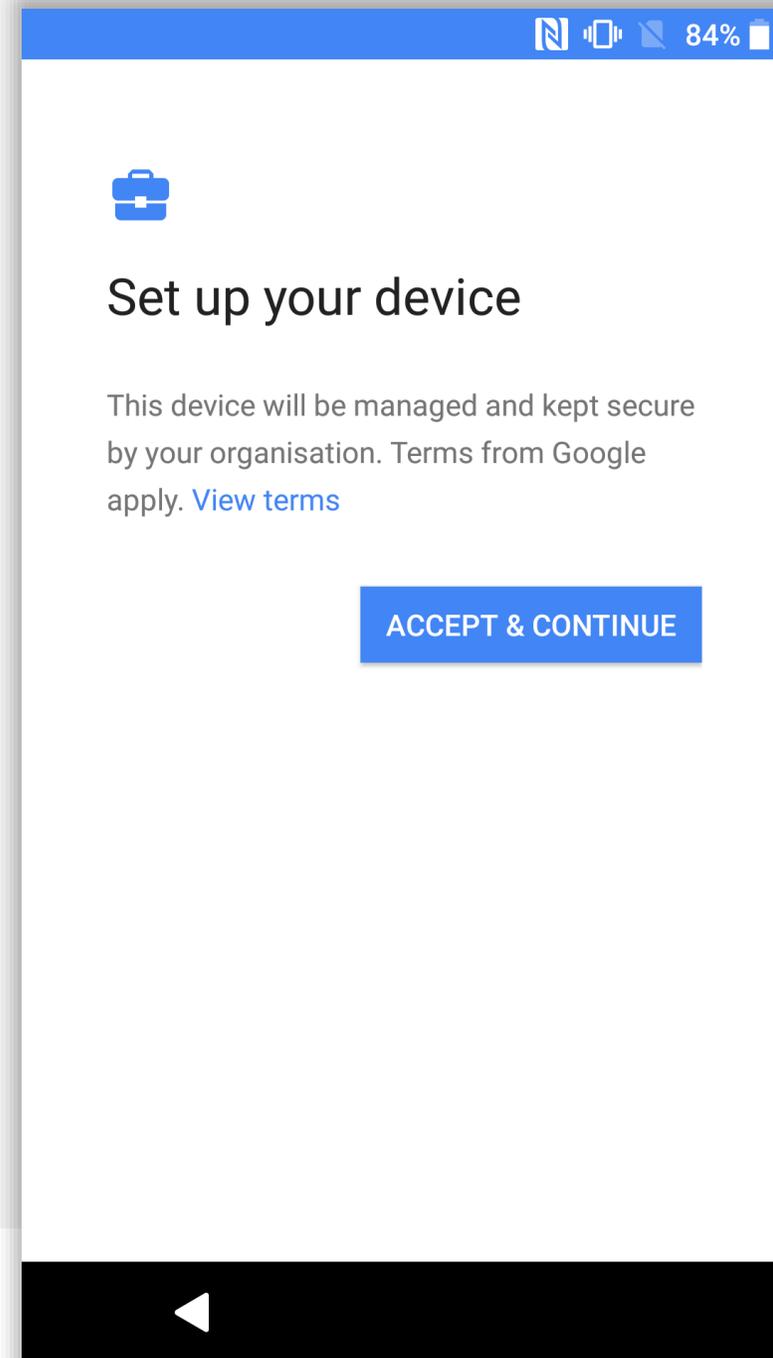


Begin provisioning

Once the NFC payload has been transmitted, the device being provisioned will display a prompt with an overview of terms of management.

You must accept the device being managed by the organisation in order to begin provisioning.

Tap **ACCEPT & CONTINUE** to proceed.

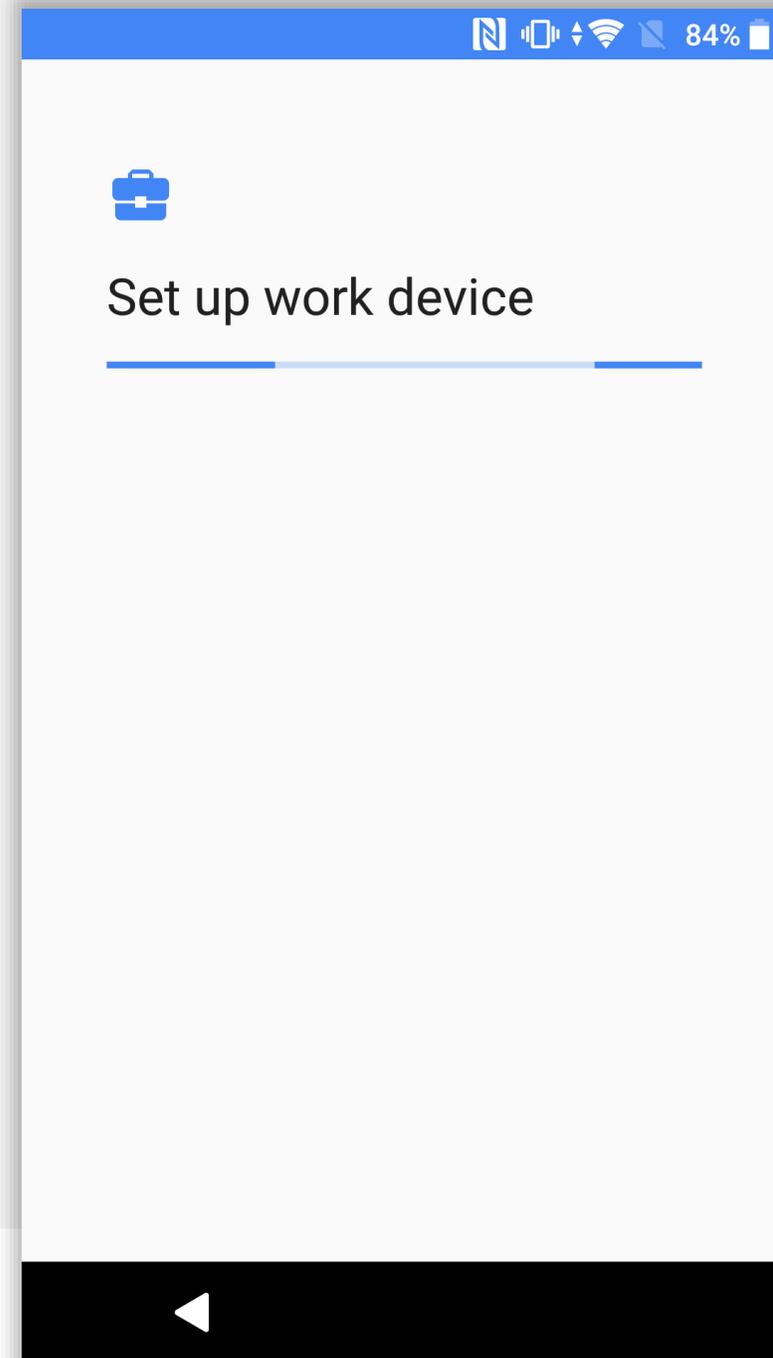




The device will provision

The device will attempt to connect to the WiFi network provided in the NFC payload and begin the provisioning process.

This may take a few minutes.

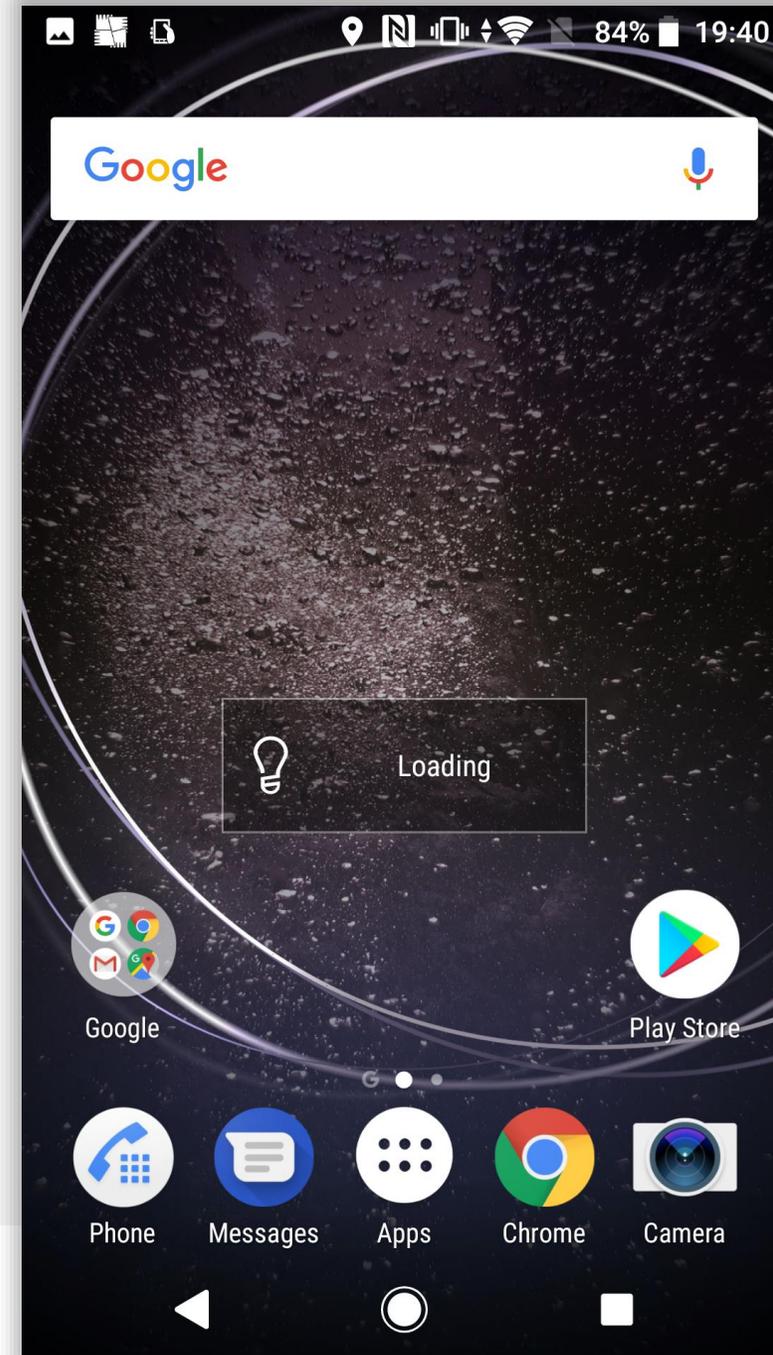




Provisioning complete

Shortly after Android enterprise provisioning is complete, the DPC will automatically launch and begin enrolment.

There is no need to manually open the DPC from the home screen.



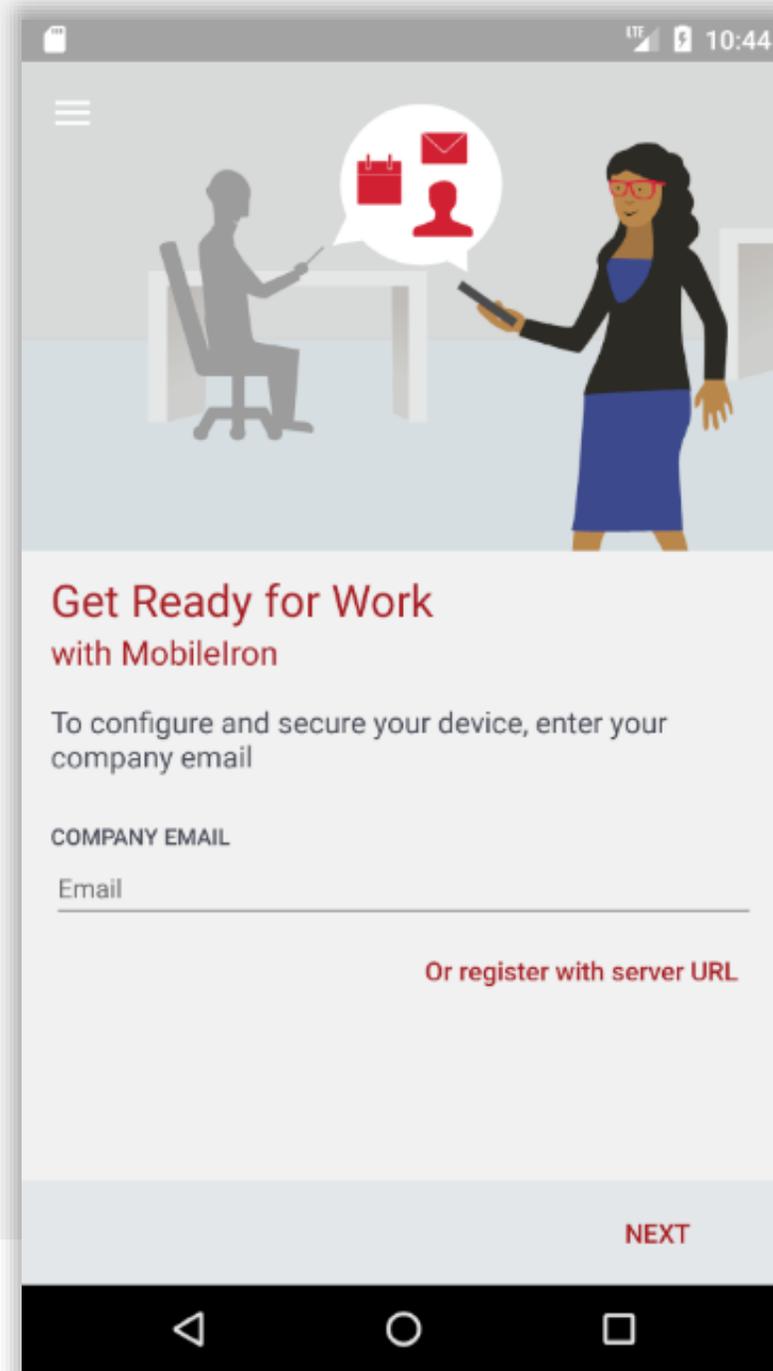


Begin enrolment

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.

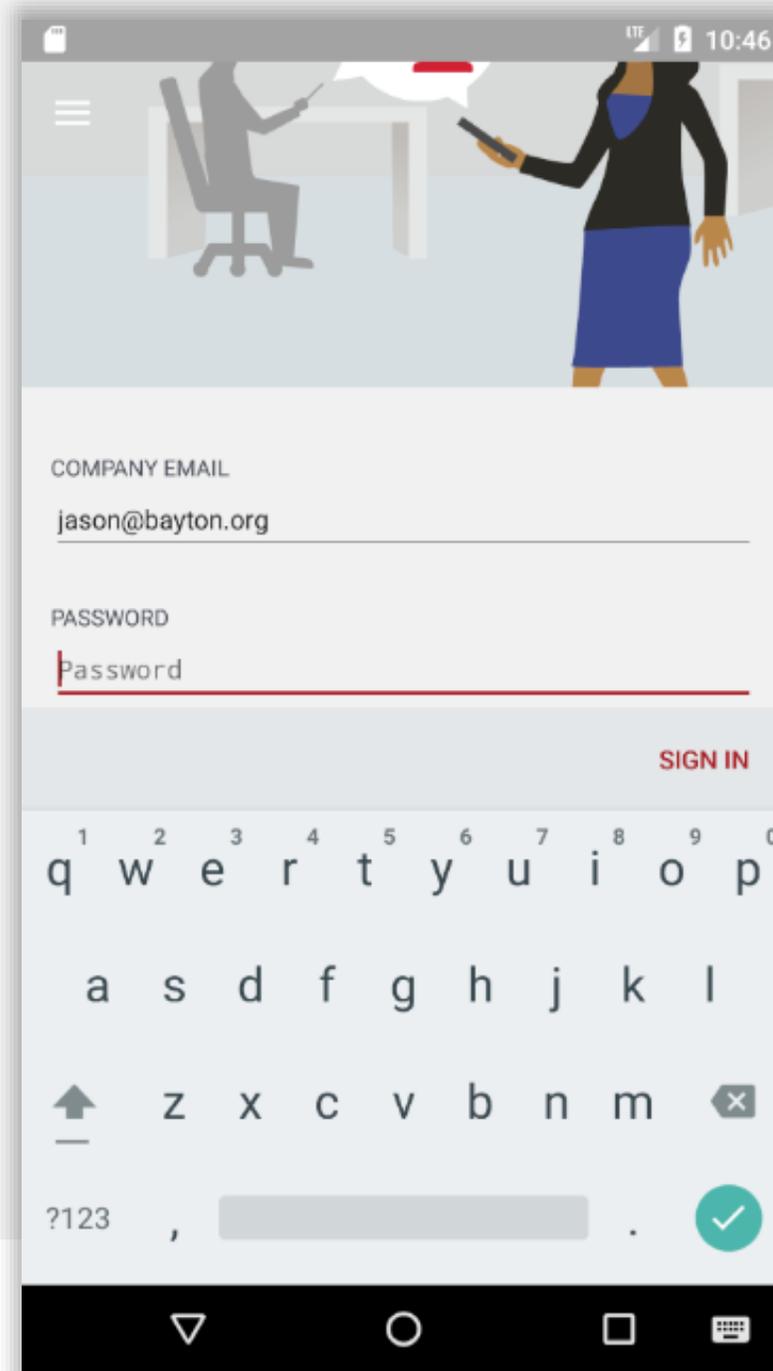




Continue enrolment

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

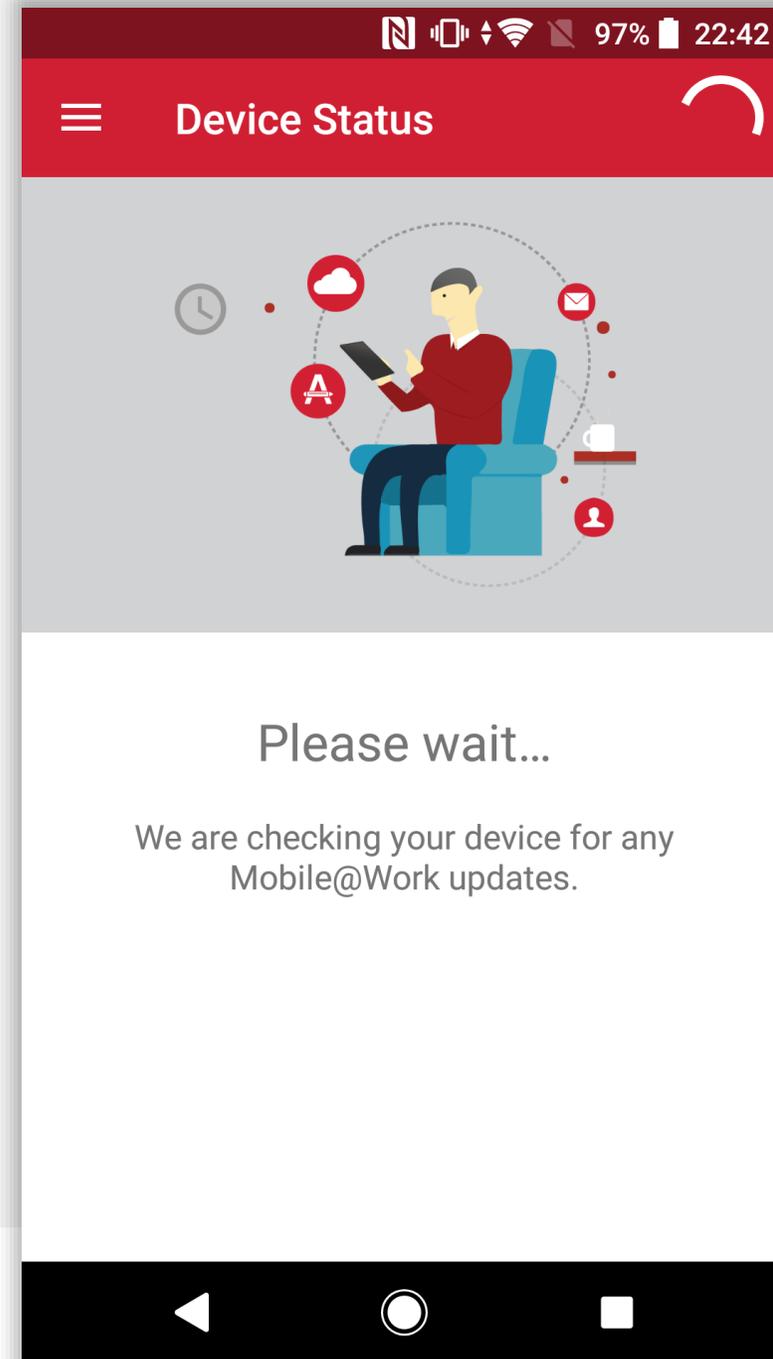
Enter the required fields and tap **SIGN IN**.





Device configuration

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



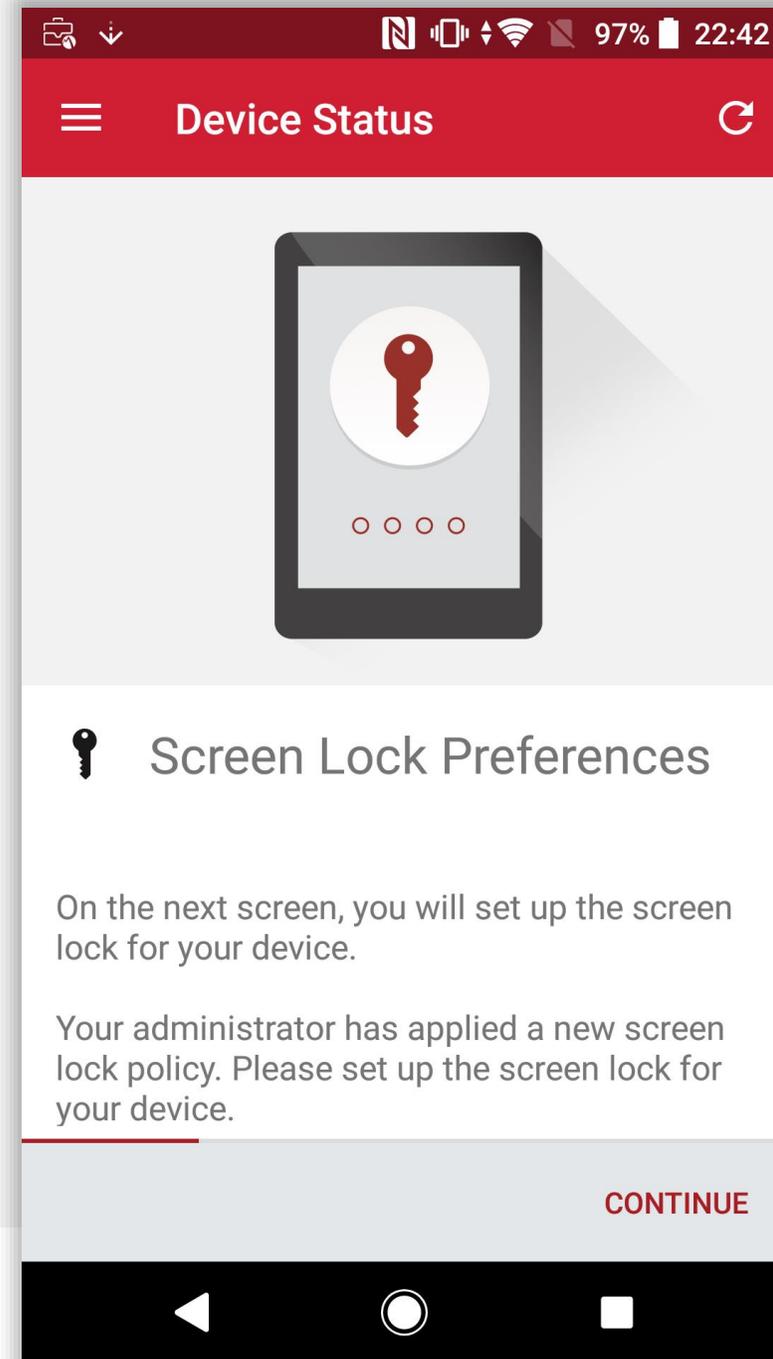


Device configuration

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.

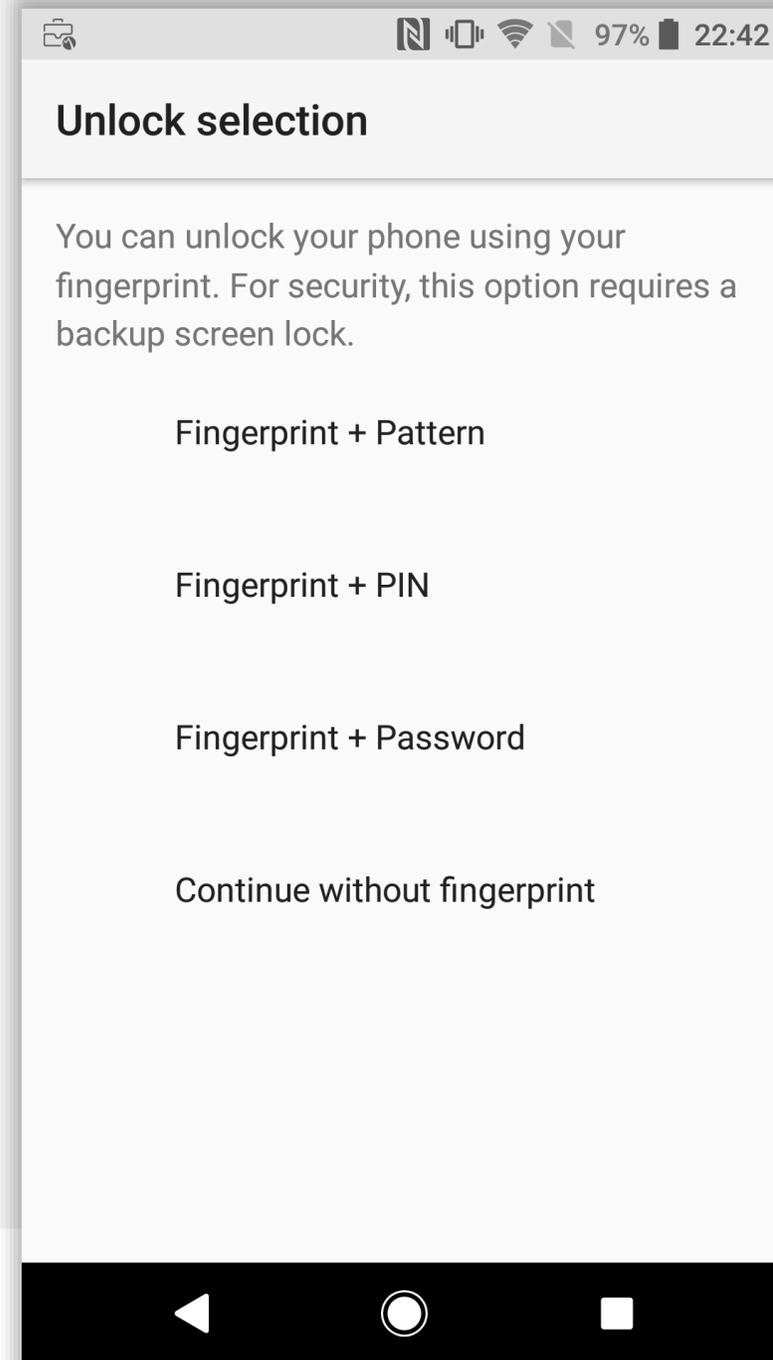
Tap **CONTINUE**.





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

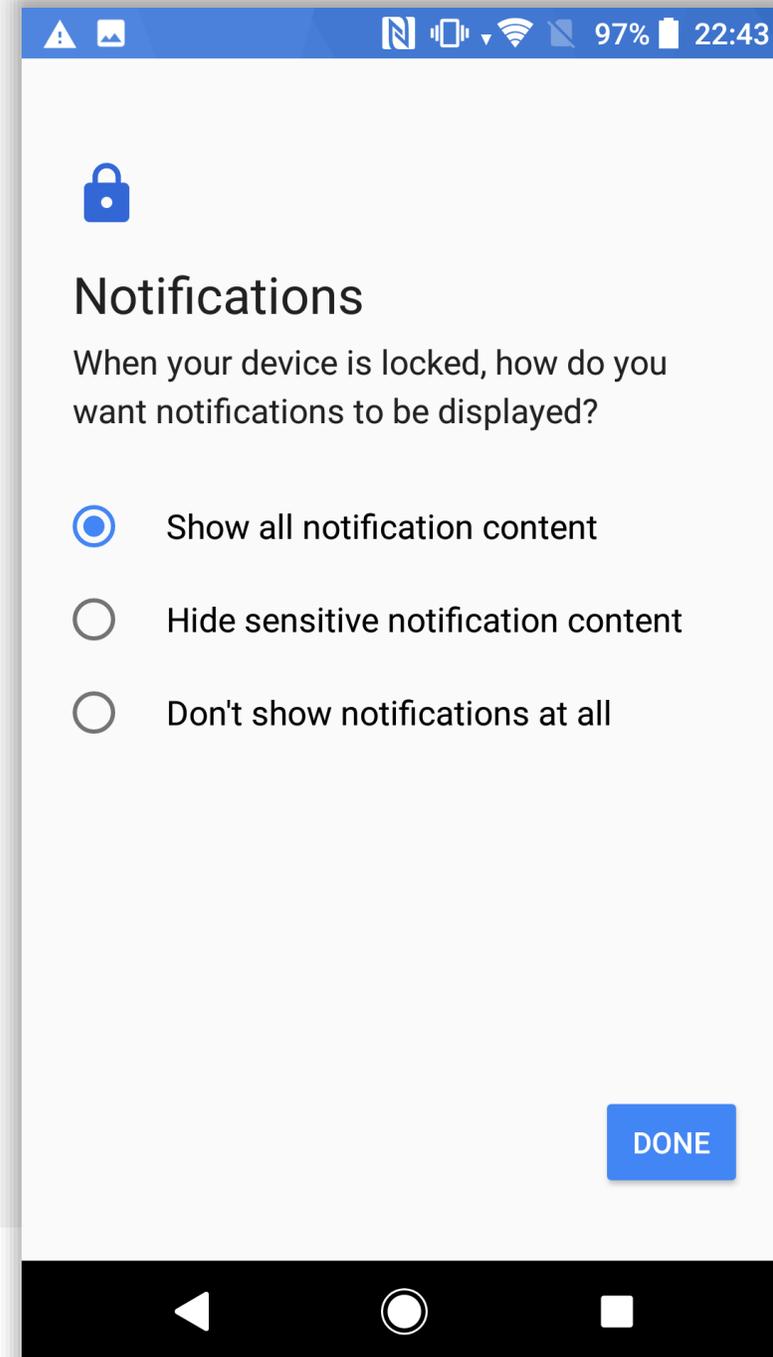
Input a PIN (or other passcode type) and tap **CONTINUE**.
Repeat to confirm.

A screenshot of a mobile application interface for setting a PIN. At the top, there is a blue status bar with icons for signal, Wi-Fi, and battery (97%), and the time 22:43. Below the status bar is a blue padlock icon. The main heading is "Choose your PIN". A horizontal line indicates the input field, with the text "PIN must be at least 4 digits" below it. At the bottom left is a blue "CANCEL" link, and at the bottom right is a grey "CONTINUE" button. Below these is a numeric keypad with buttons for digits 1-9, 0, a backspace key (X), and a right arrow key. The bottom of the screen shows the Android navigation bar with a triangle, circle, and square icon, and a keyboard icon on the right.



Device configuration

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

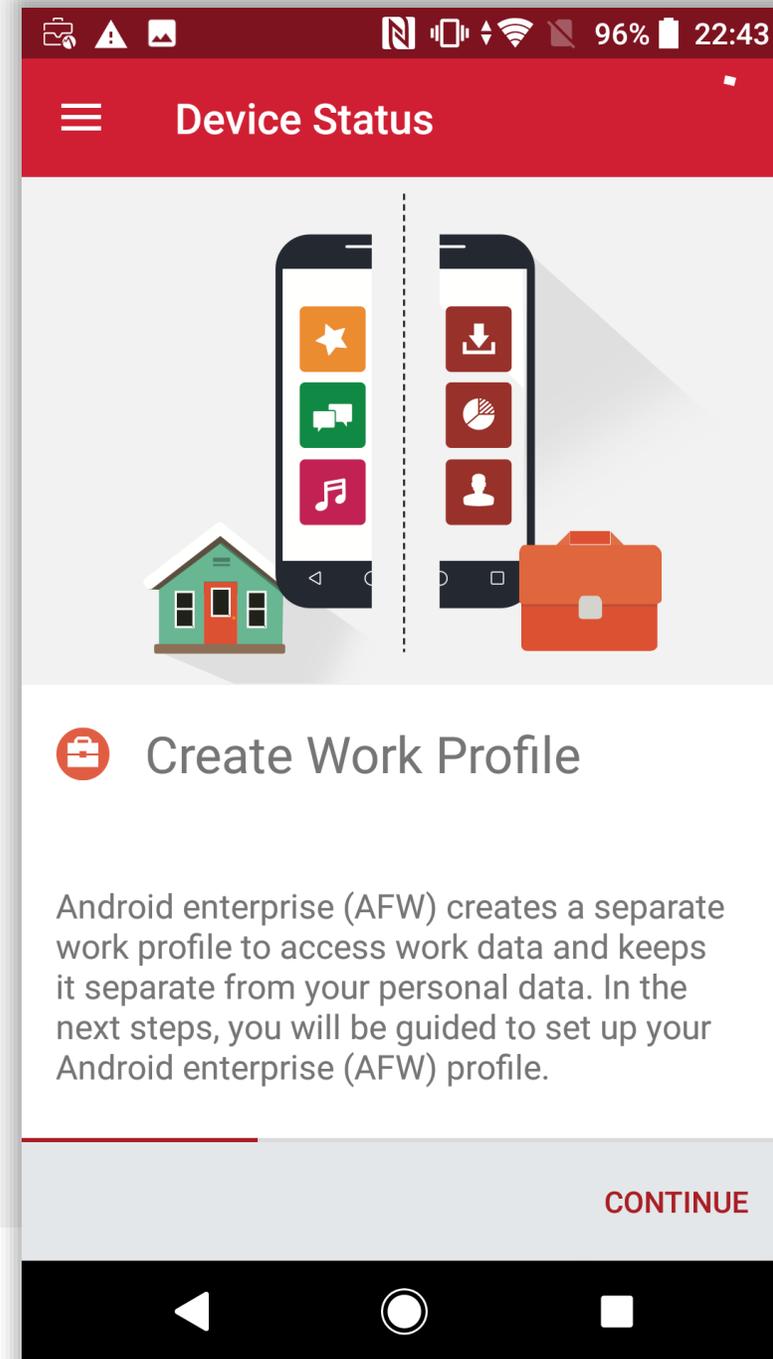




Work profile configuration

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.

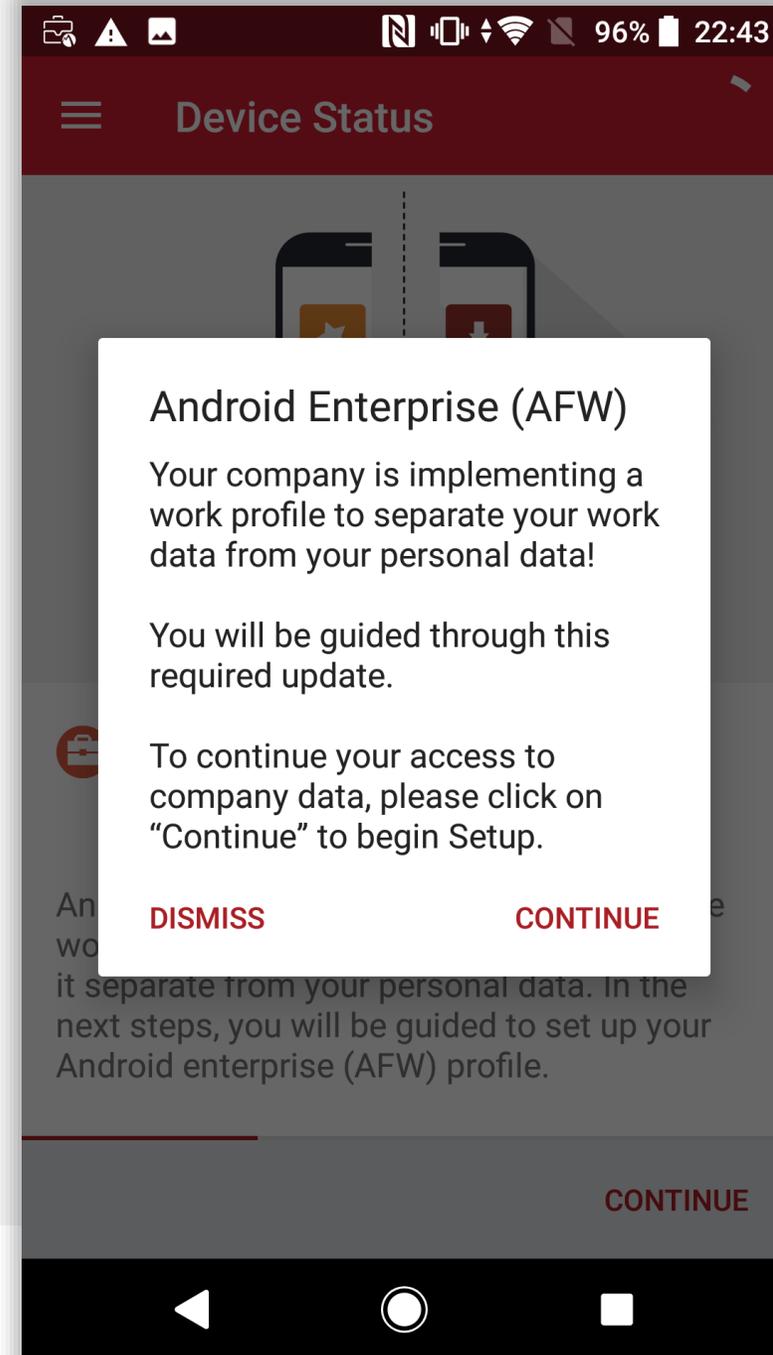
Tap **CONTINUE**.





Work profile configuration

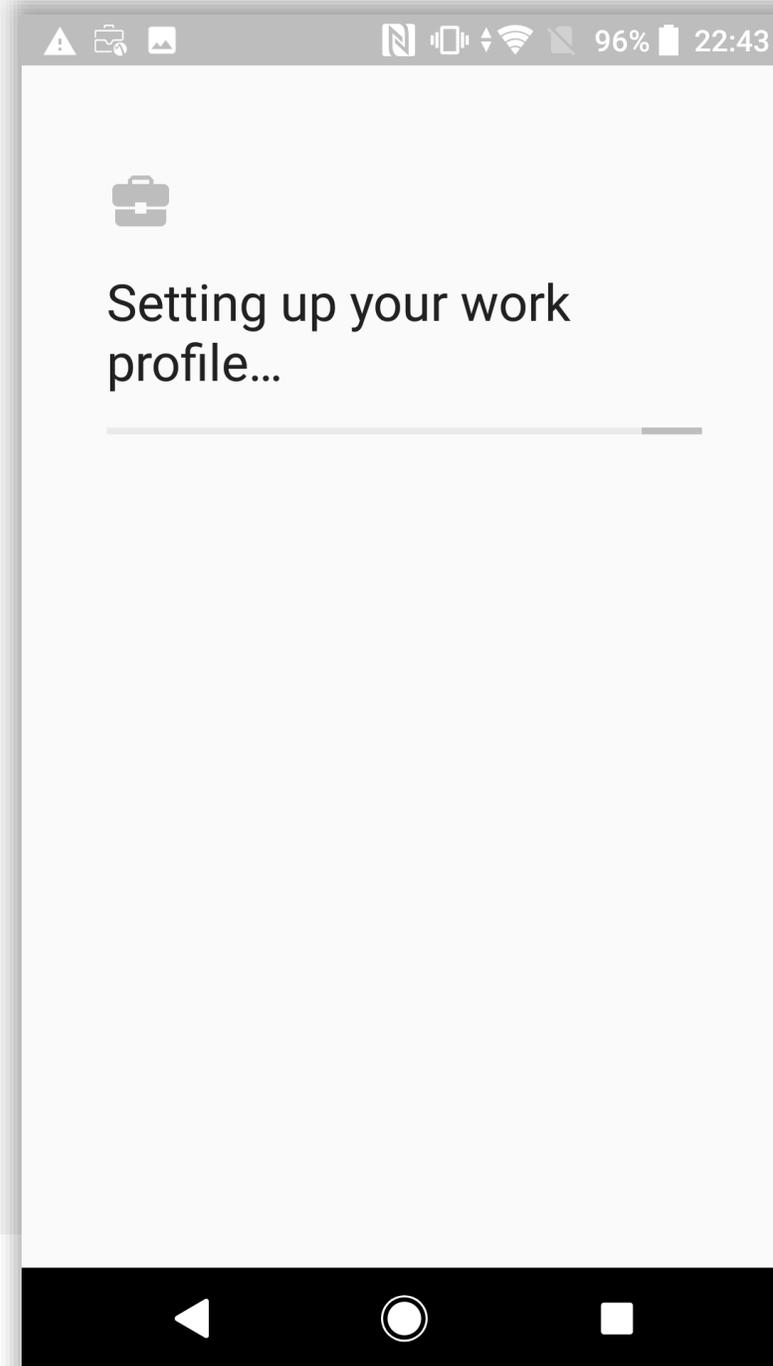
Accept the prompt, tap CONTINUE.





Work profile configuration

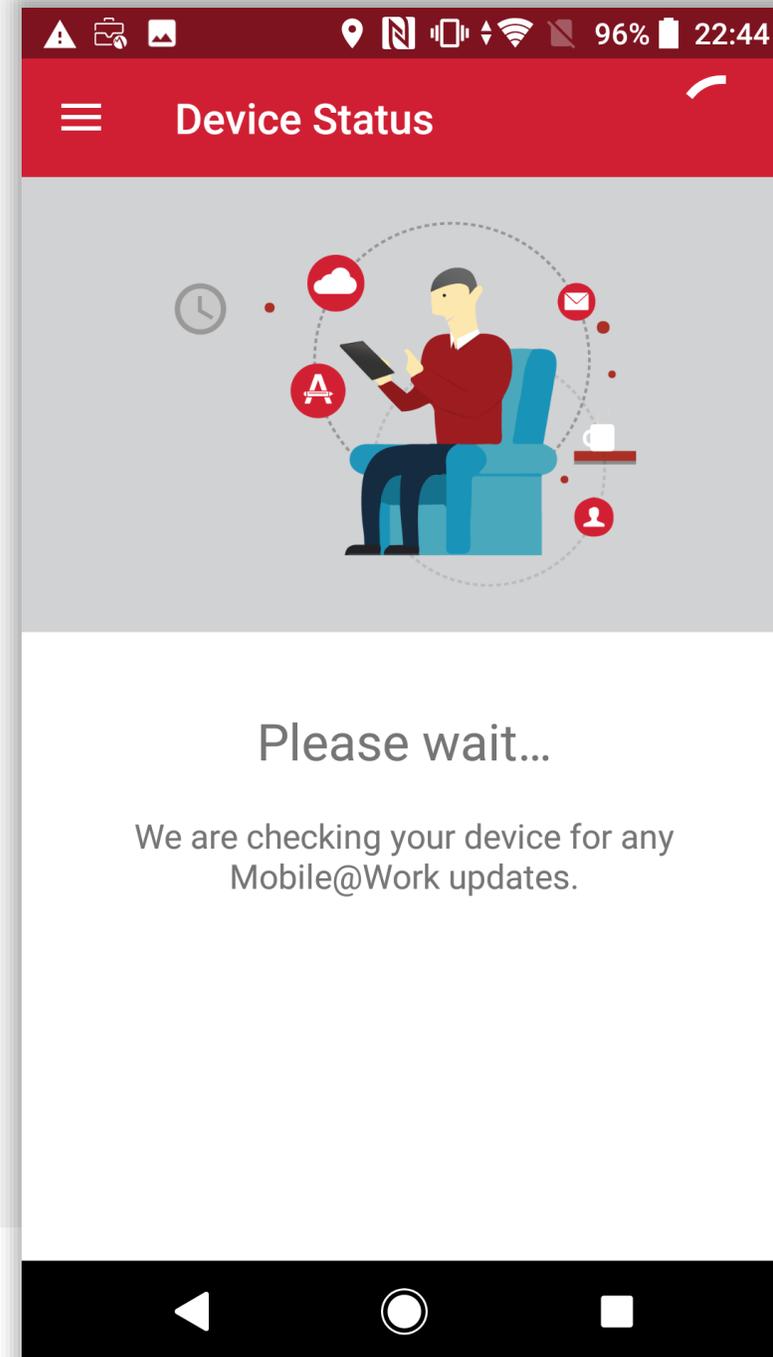
The device will now set up the work profile. This should be relatively quick and there is nothing needing to be done. This will automatically continue to the next step.





Work profile configuration

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



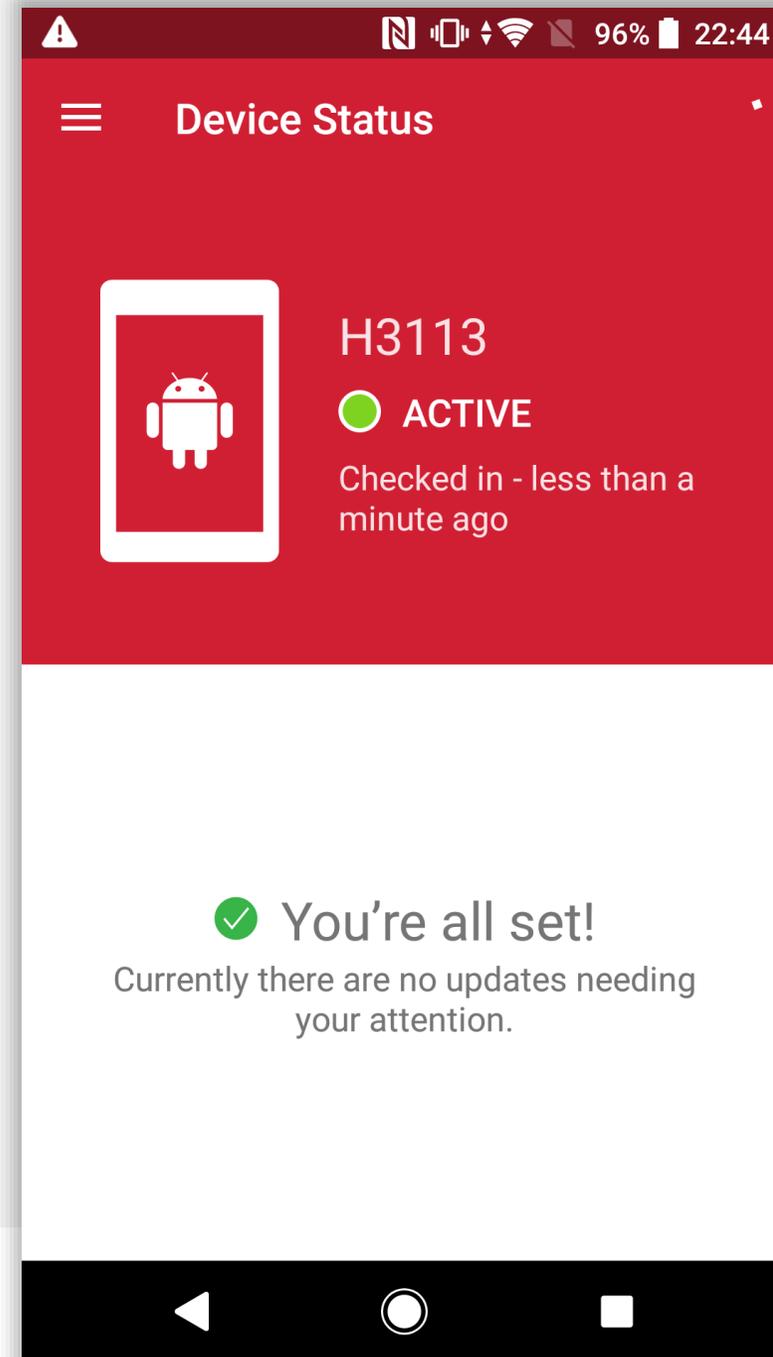


Enrolment complete

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.

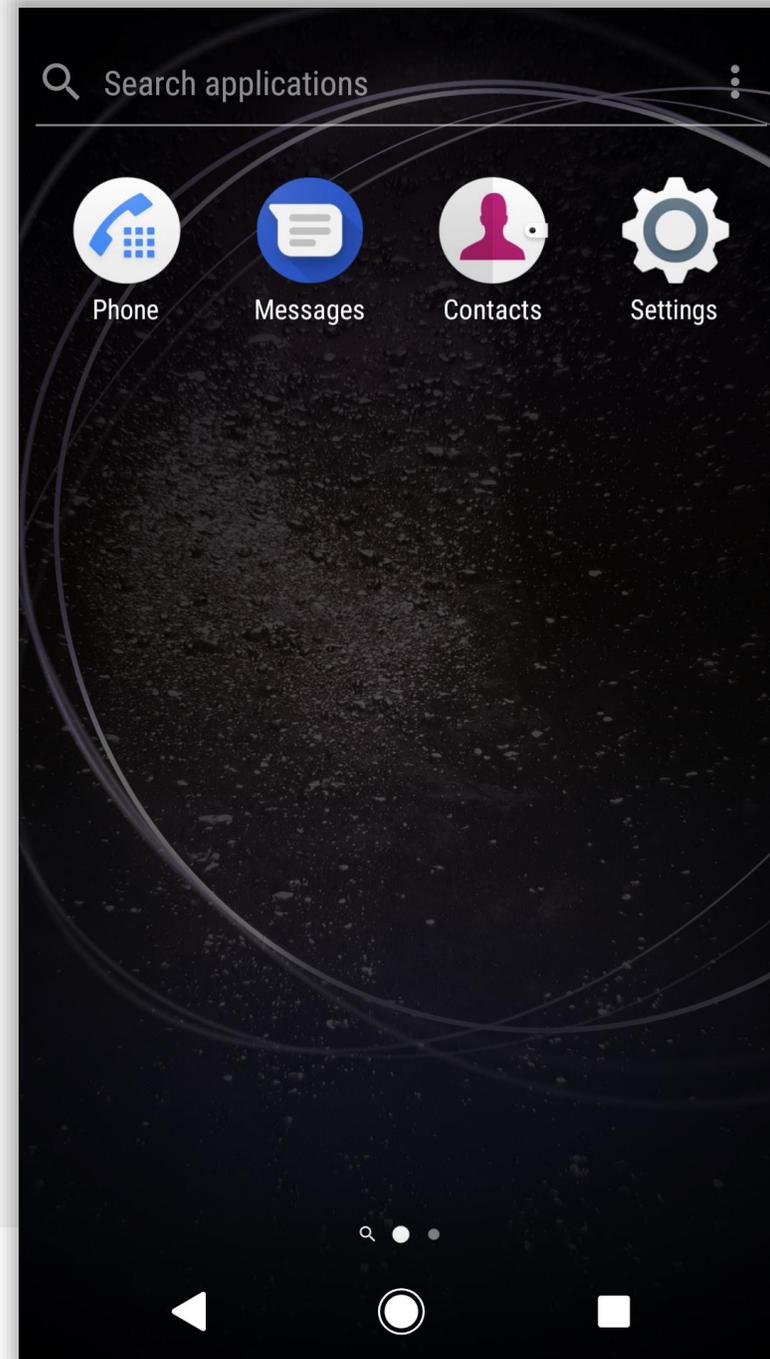




Add a personal account

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**.

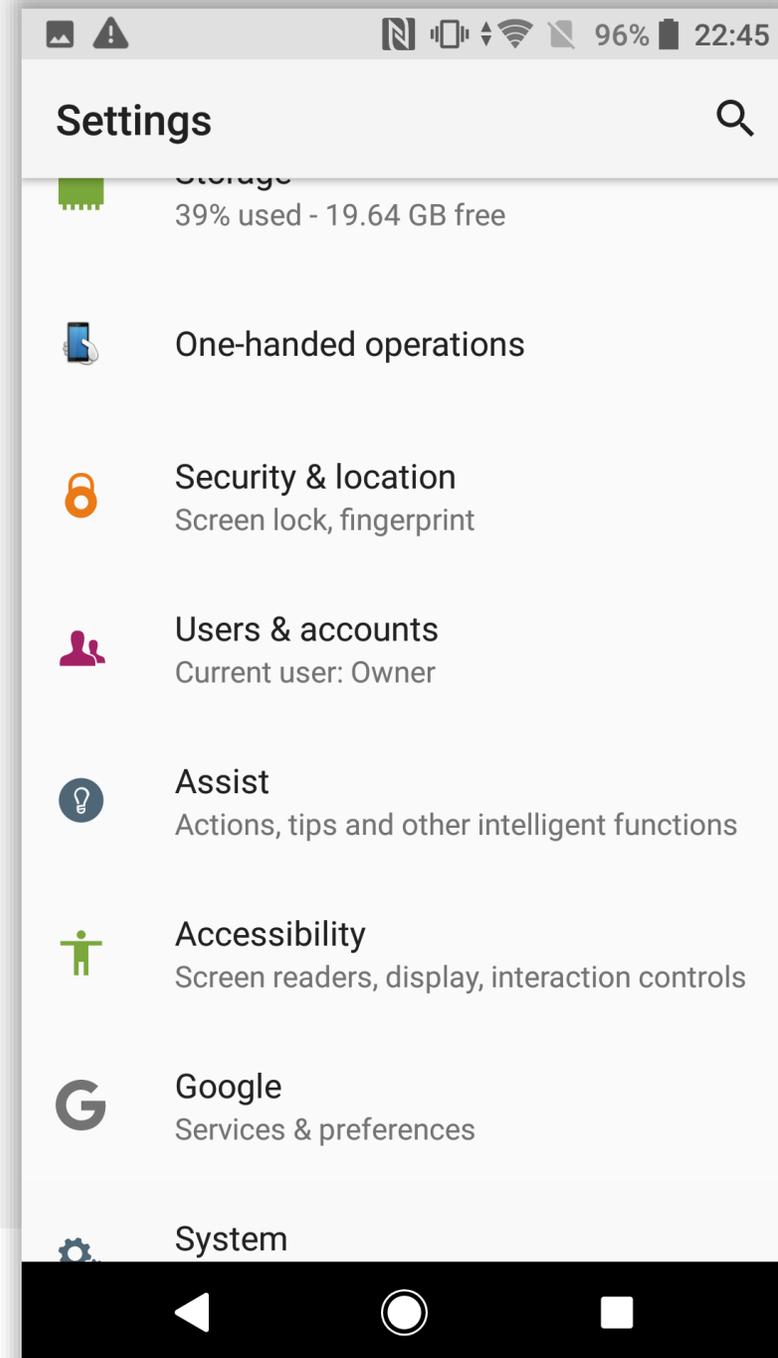




Add a personal account

Scroll down Settings until you find Users & accounts.

Tap Users & accounts.

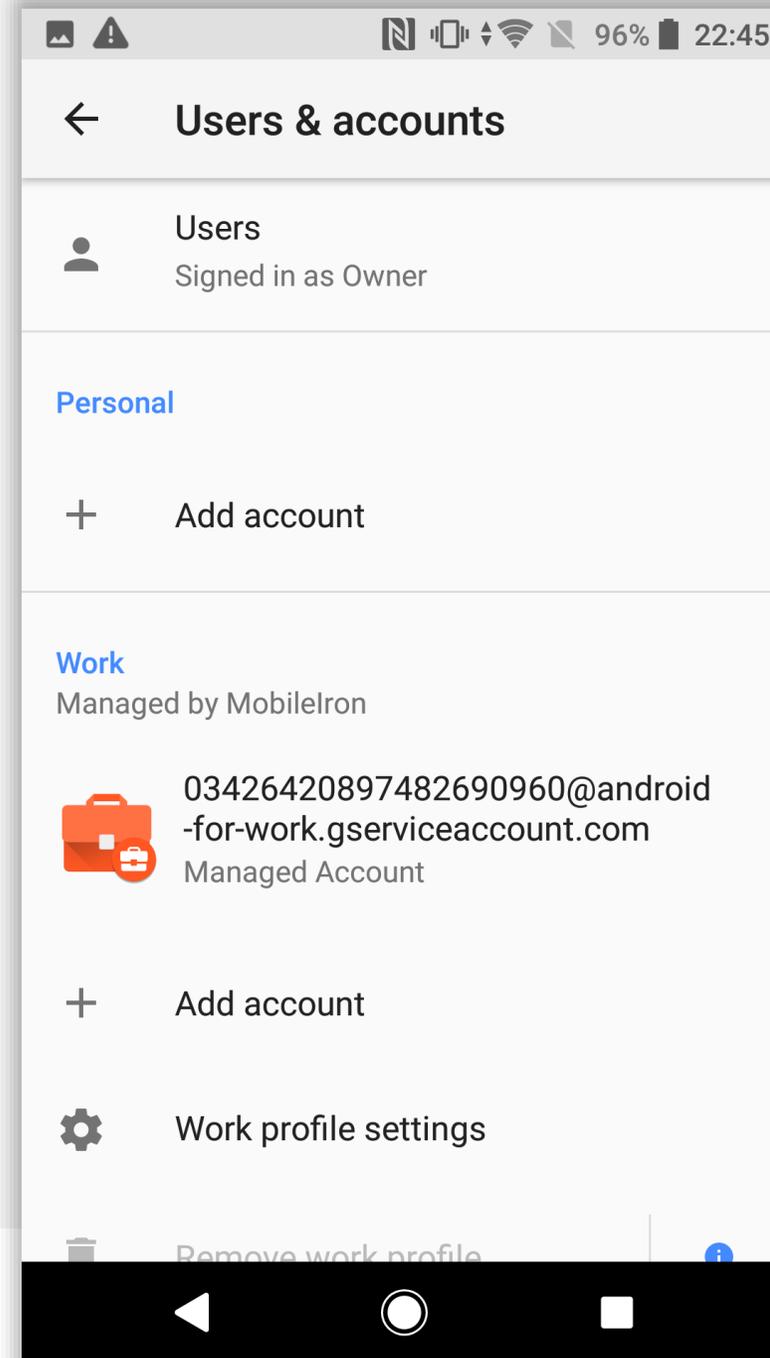




Add a personal account

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

Tap **Add account**.



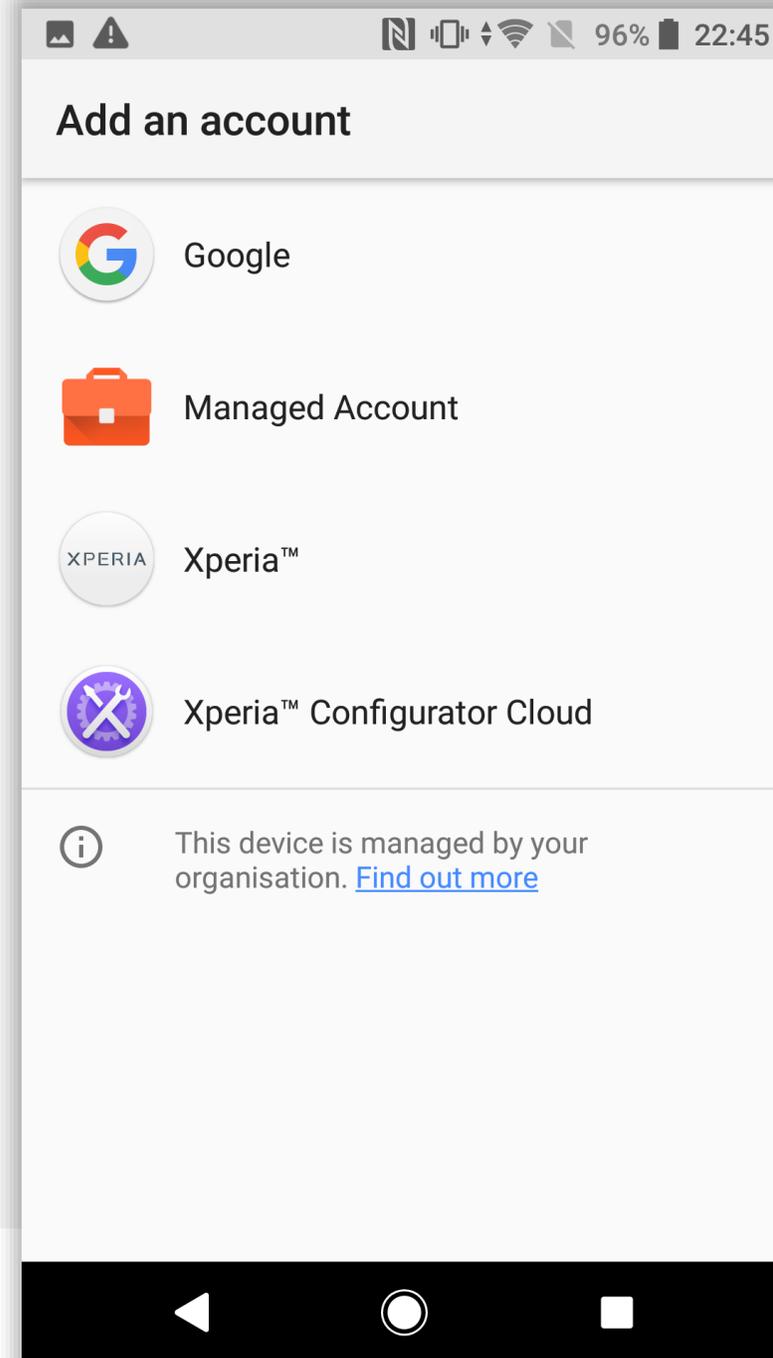


Setup complete

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](#)

