

Android enterprise

Fully managed work profile enrolment
QR code provisioning



MobileIron Core



Android 8.x



Sony UI

March 2018



SONY

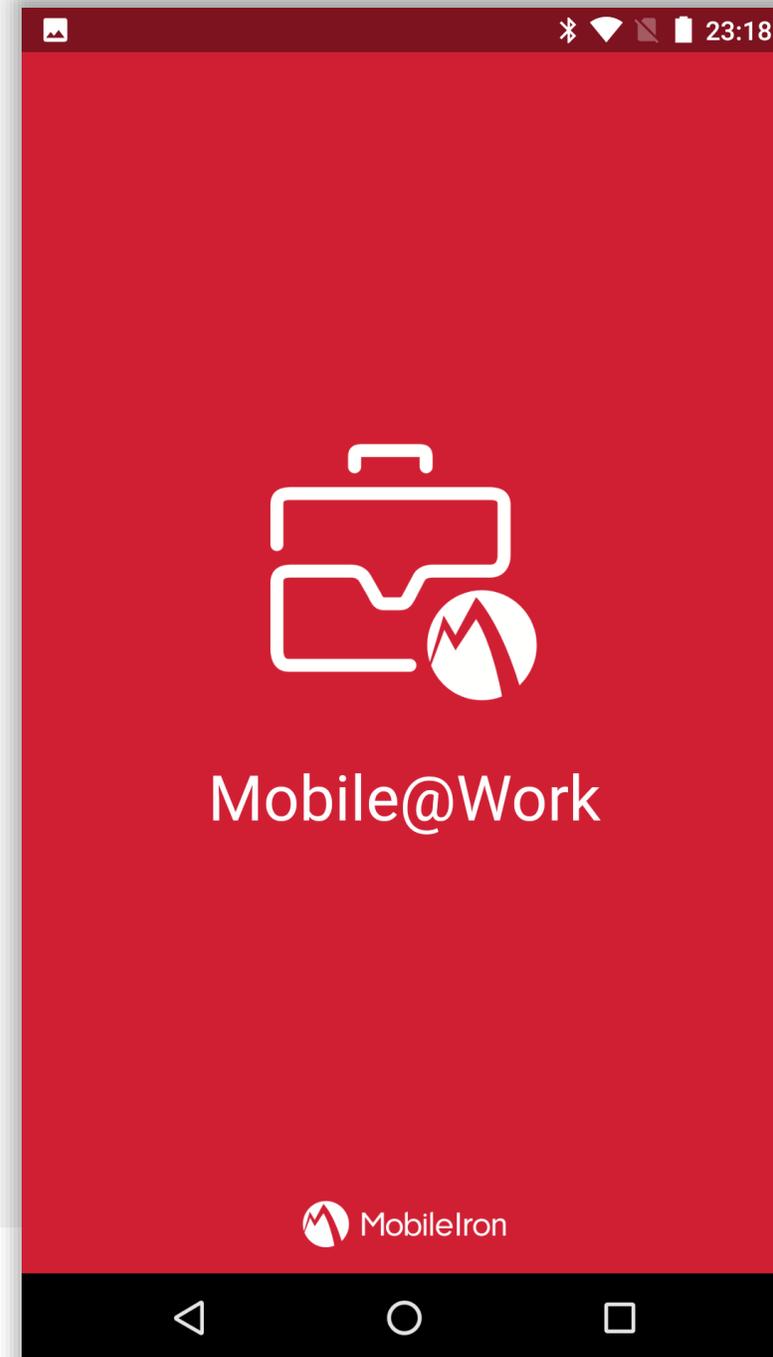


Requirements

In order to proceed, you must have:

- Android 8.0 or later installed on the devices to be provisioned. Earlier Android versions are incompatible.
- OEM support for QR code provisioning.
- A functional MobileIron EMM solution in place of at least version 9.7 with Mobile@Work version 9.7
- Android enterprise fully configured on your EMM platform.

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





Configure the QR code

Before Android enterprise QR enrolment can occur, you must generate a QR Code unique and up to date with your environment and the latest MobileIron DPC APK.

QR codes can be generated through the MobileIron Provisioner app ([Google Play](#)), or for manual QR generation, a good resource can be found [here](#).

Note: As this is a COPE deployment, it's a good idea to leave system apps enabled when configuring the QR code.



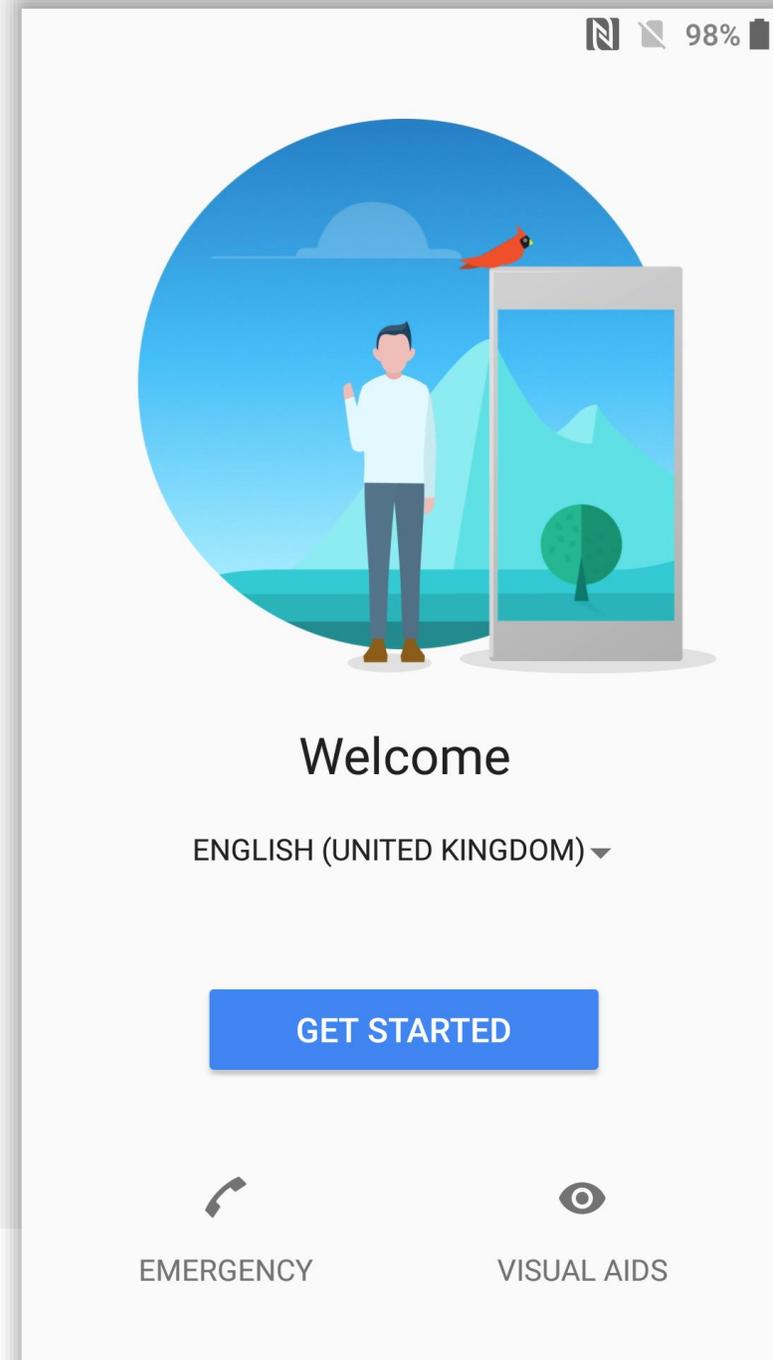


Initiate the QR reader

Hidden on the Welcome screen of many Android 7.0+ devices is a QR reader initiation process.

The simplest way of knowing if the device supports QR provisioning is by tapping on **Welcome** 6 times in quick succession.

Note: Not all OEMs support QR code enrolment, be sure to validate this before attempting to provision.

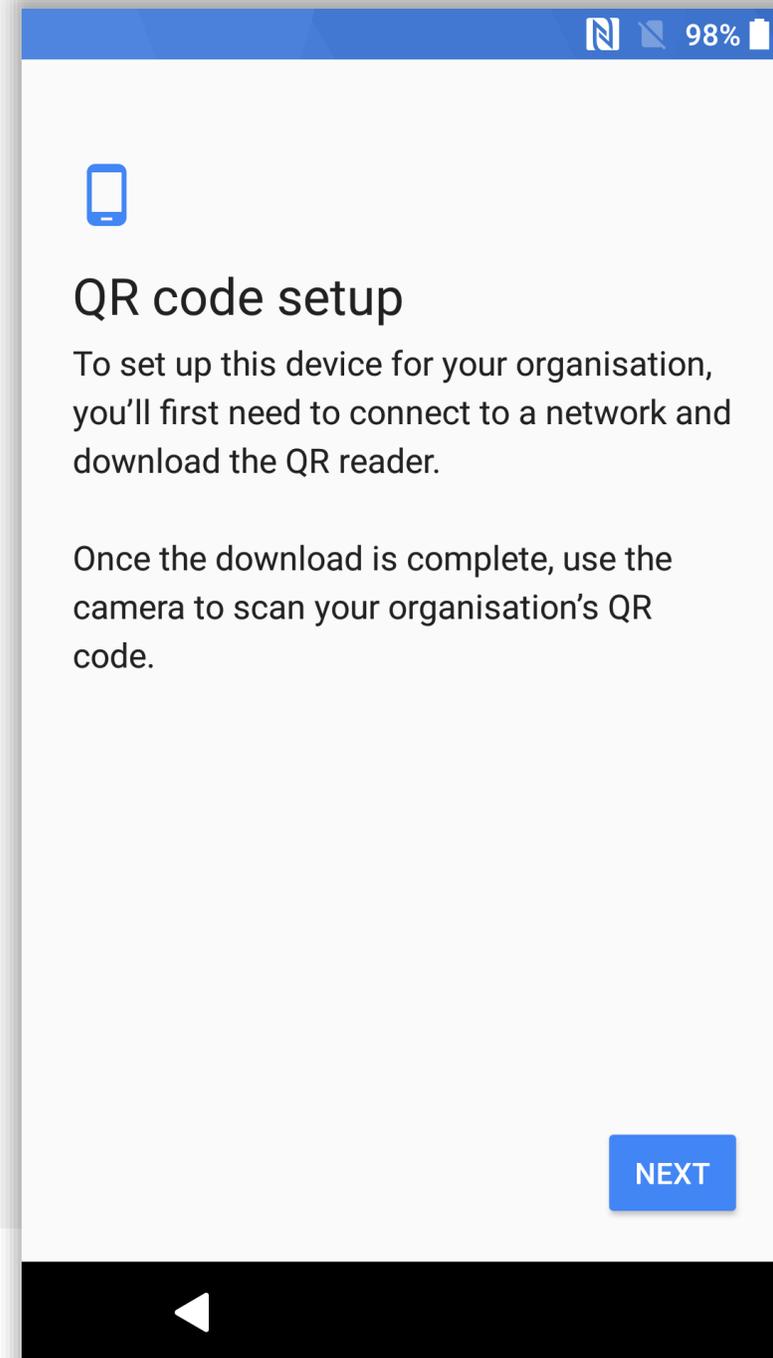




Initiate the QR reader

Once the QR process has successfully initiated, QR code setup will display.

Tap **NEXT** to continue.



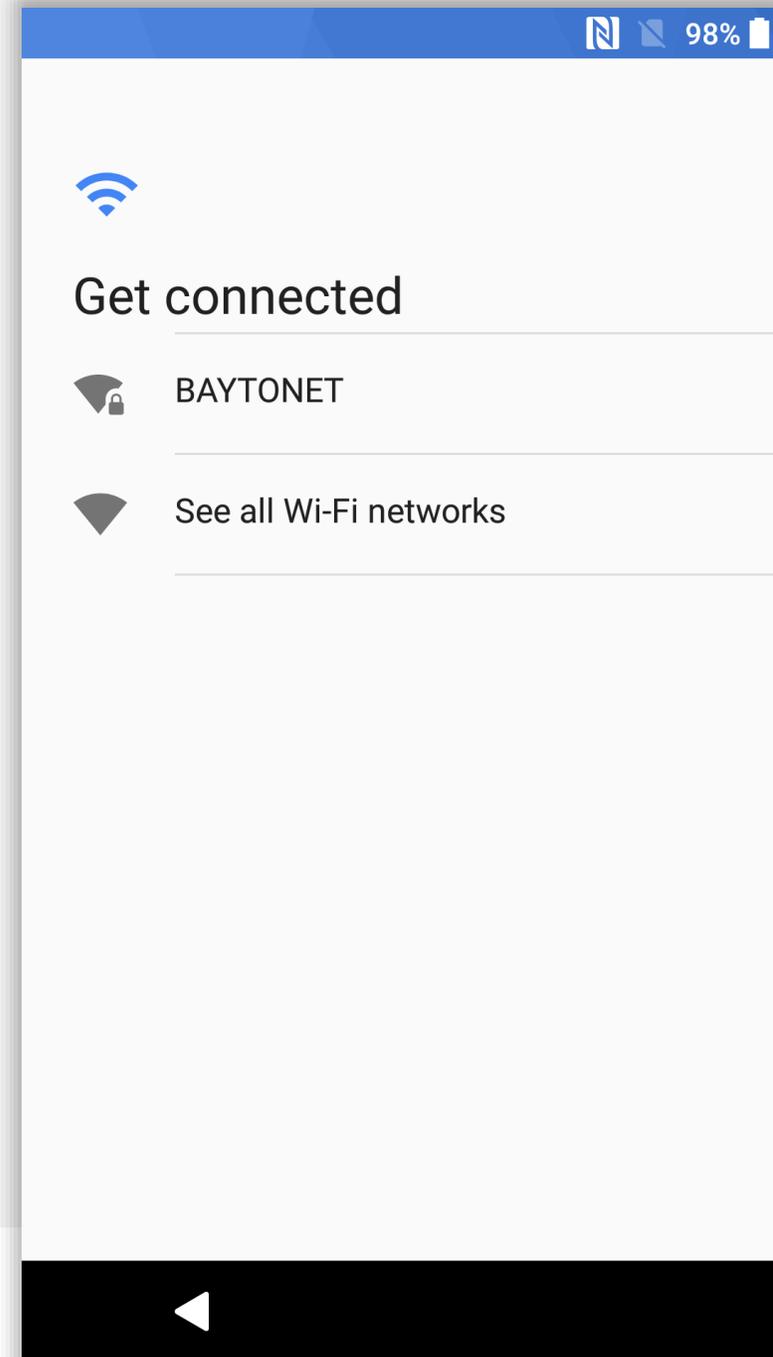


Initiate the QR reader

You will be prompted to connect to WiFi in order to continue the provisioning process.

Tap an SSID and authenticate to continue.

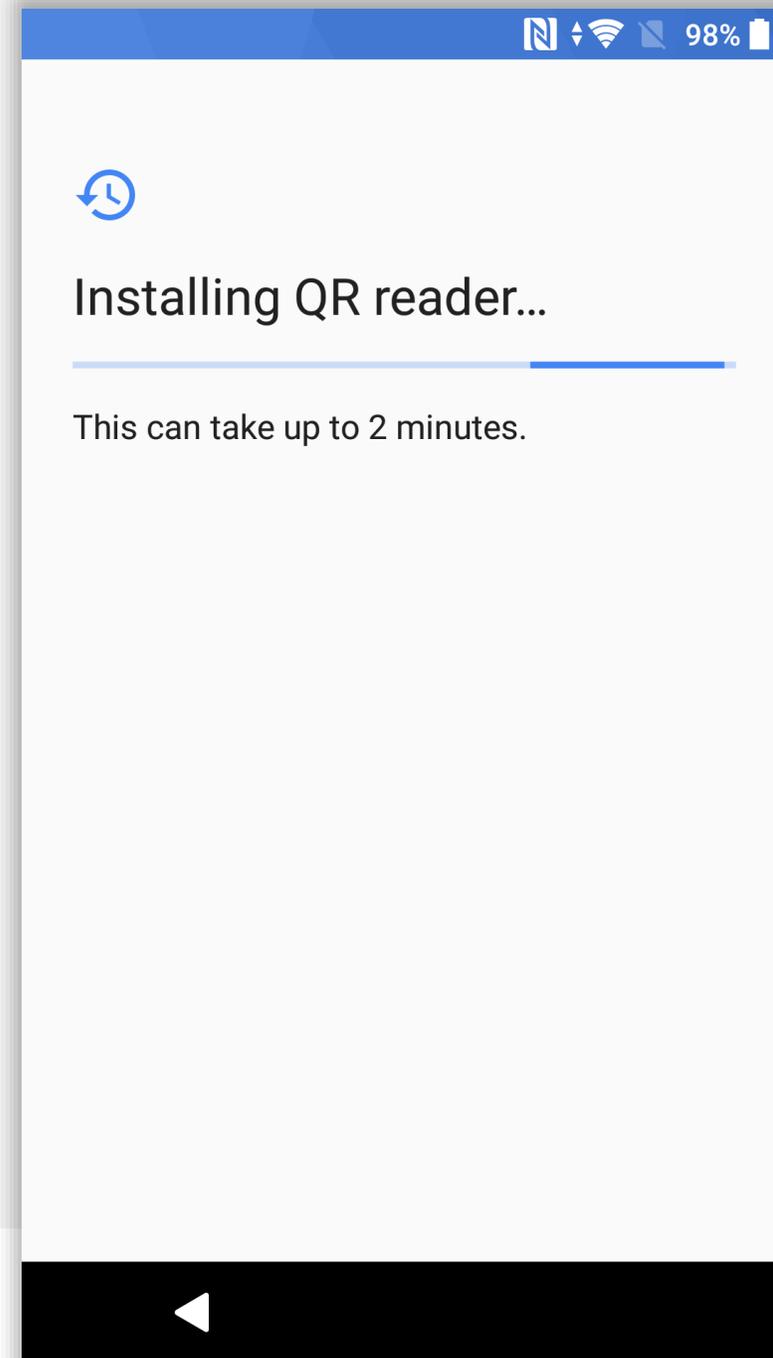
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup** (not displayed).





Initiate the QR reader

The device will check for updates, install the QR reader and continue automatically.



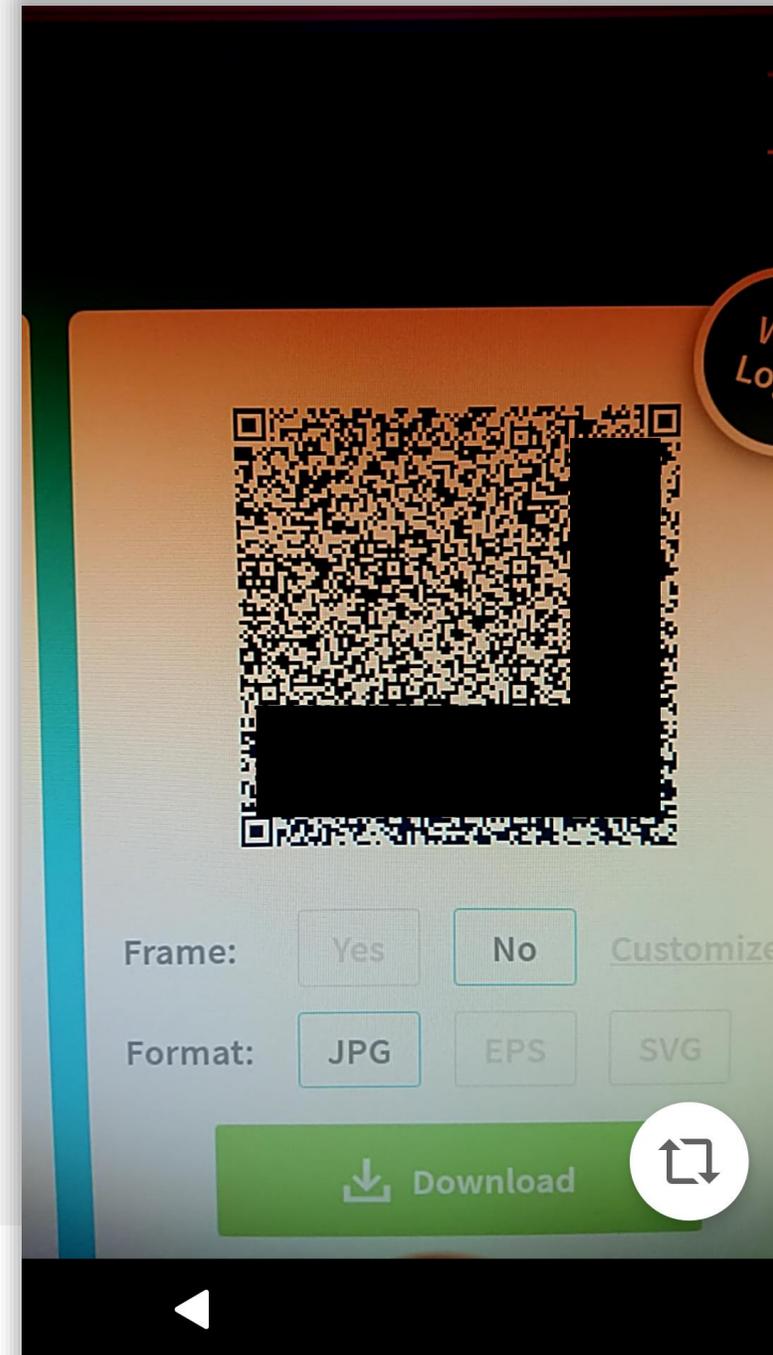


Scan the QR code

Once installed successfully, the QR reader will automatically launch.

At this point, locate the QR code using the device camera. Both front and rear-facing cameras may be used.

Note: If the QR code is not valid, the device will fail to provision and may request a factory reset. This is a time-consuming process so do ensure the QR code being scanned is valid.



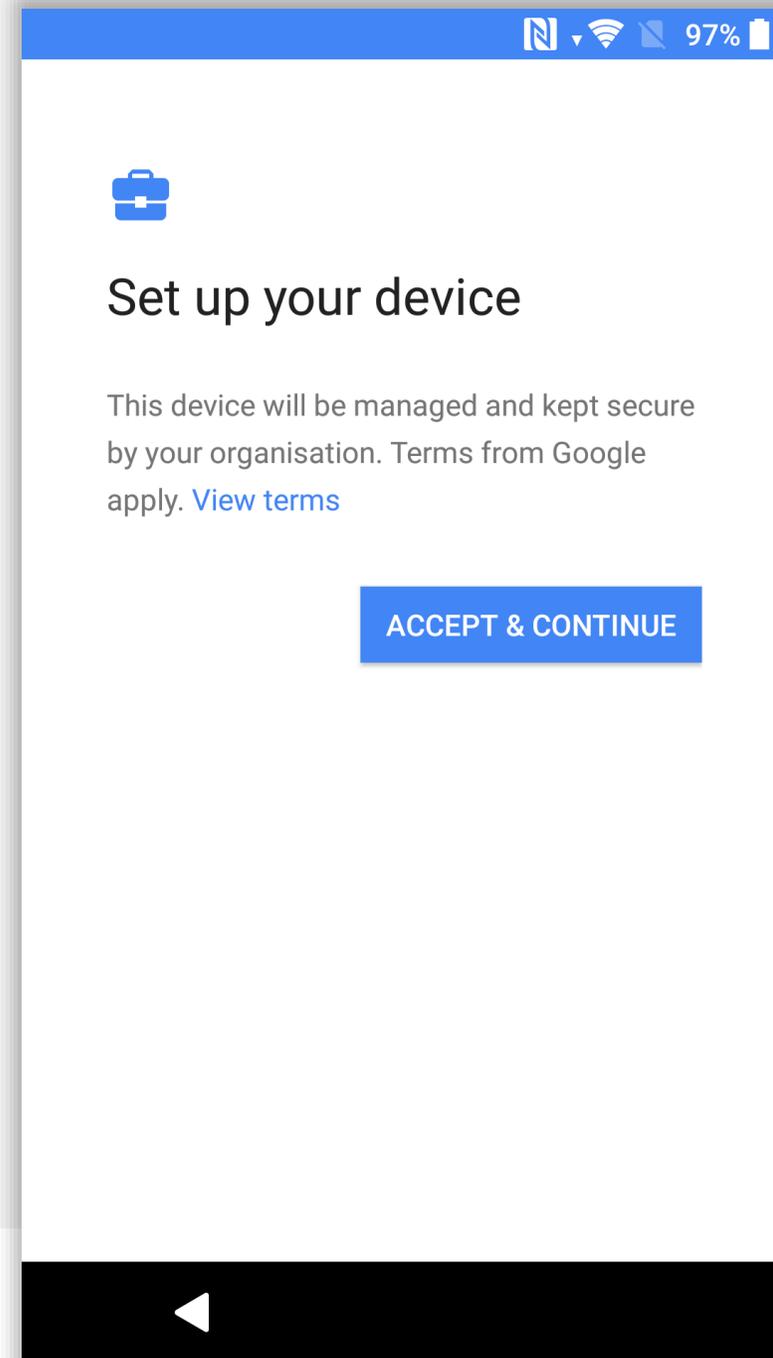


Begin provisioning

Once the QR payload has been transmitted, the device being provisioned will display a prompt with an overview of monitoring capabilities.

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

Tap **ACCEPT & CONTINUE** to proceed.



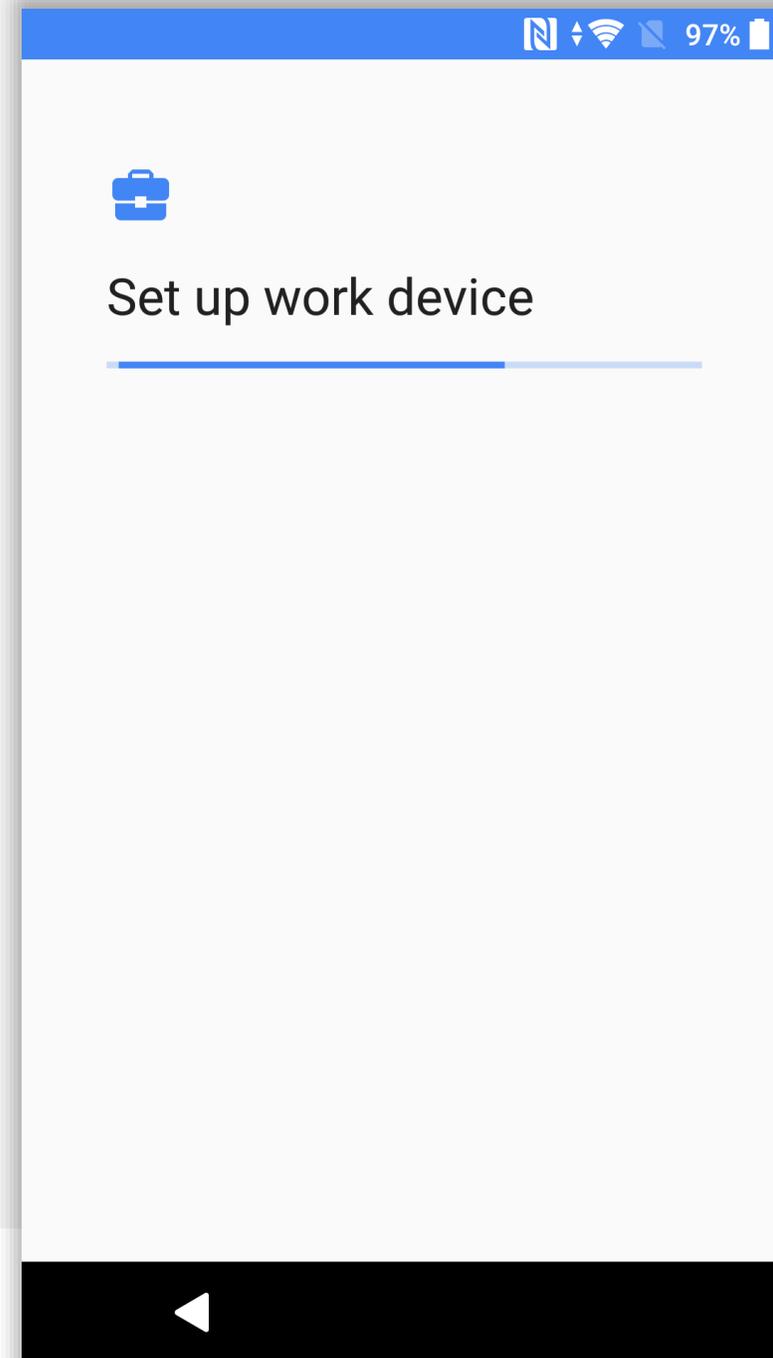


The device will provision

The device will attempt to download the DPC provided in the QR payload, install it and set MobileIron as the device owner.

This may take a few minutes.

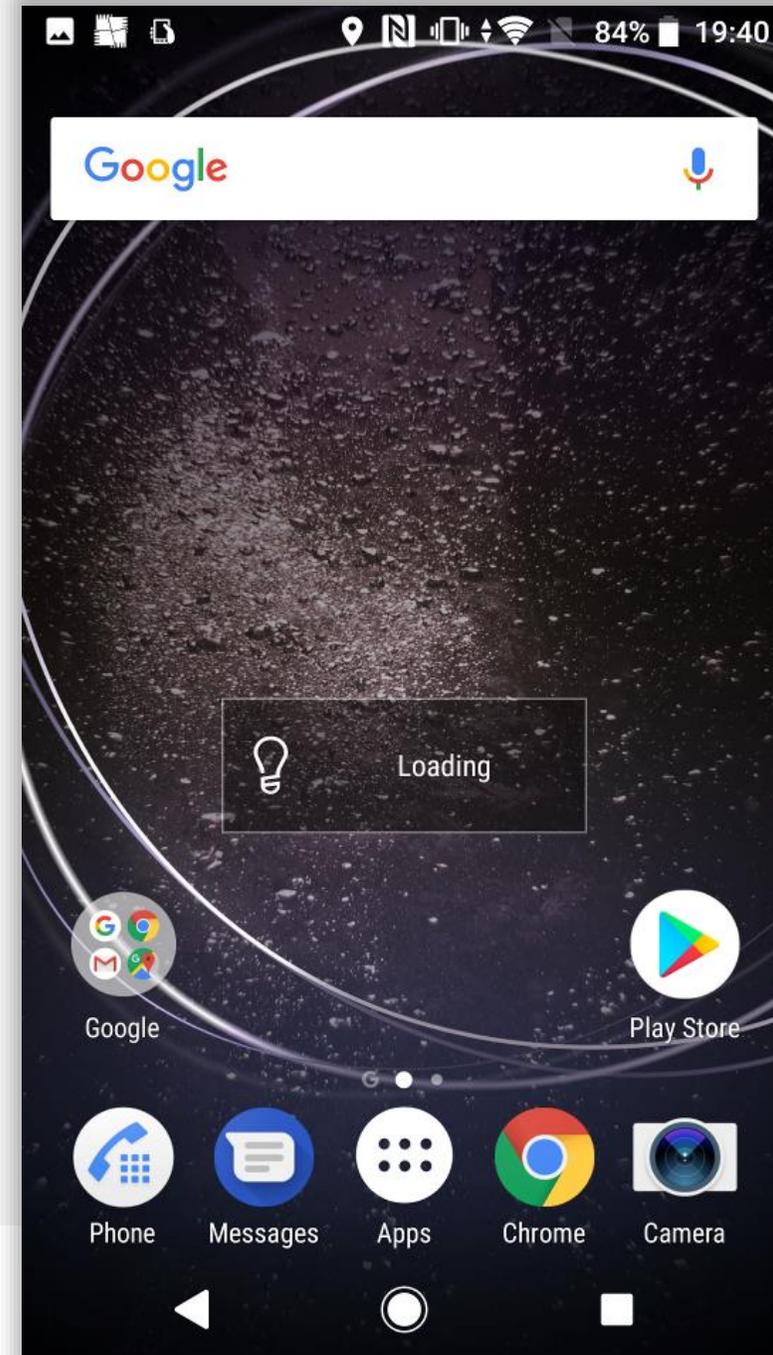
The following prompts may include license acceptance, agreement to services or finishing the setup Wizard. This varies between OEMs, however when complete the device will display the home screen before the DPC launches.





Provisioning complete

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



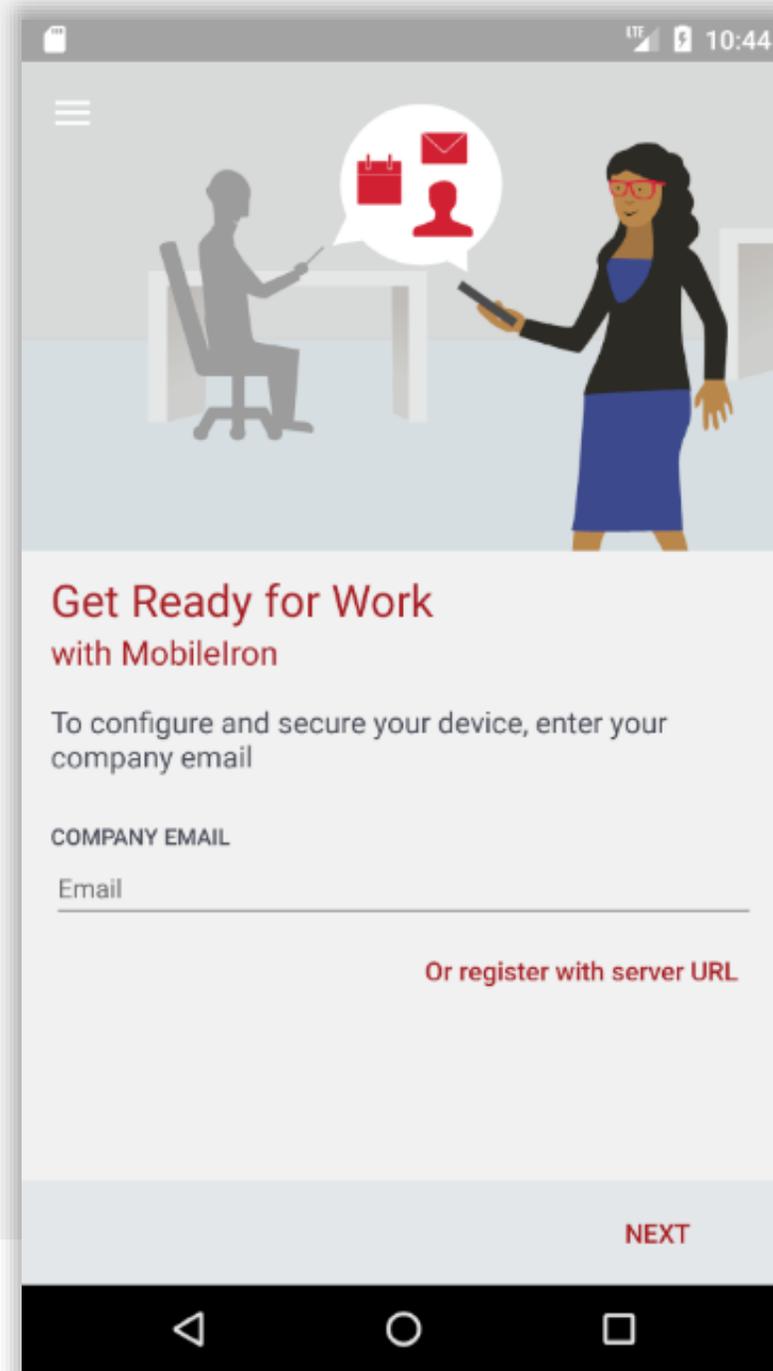


Begin enrolment

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.





Continue enrolment

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

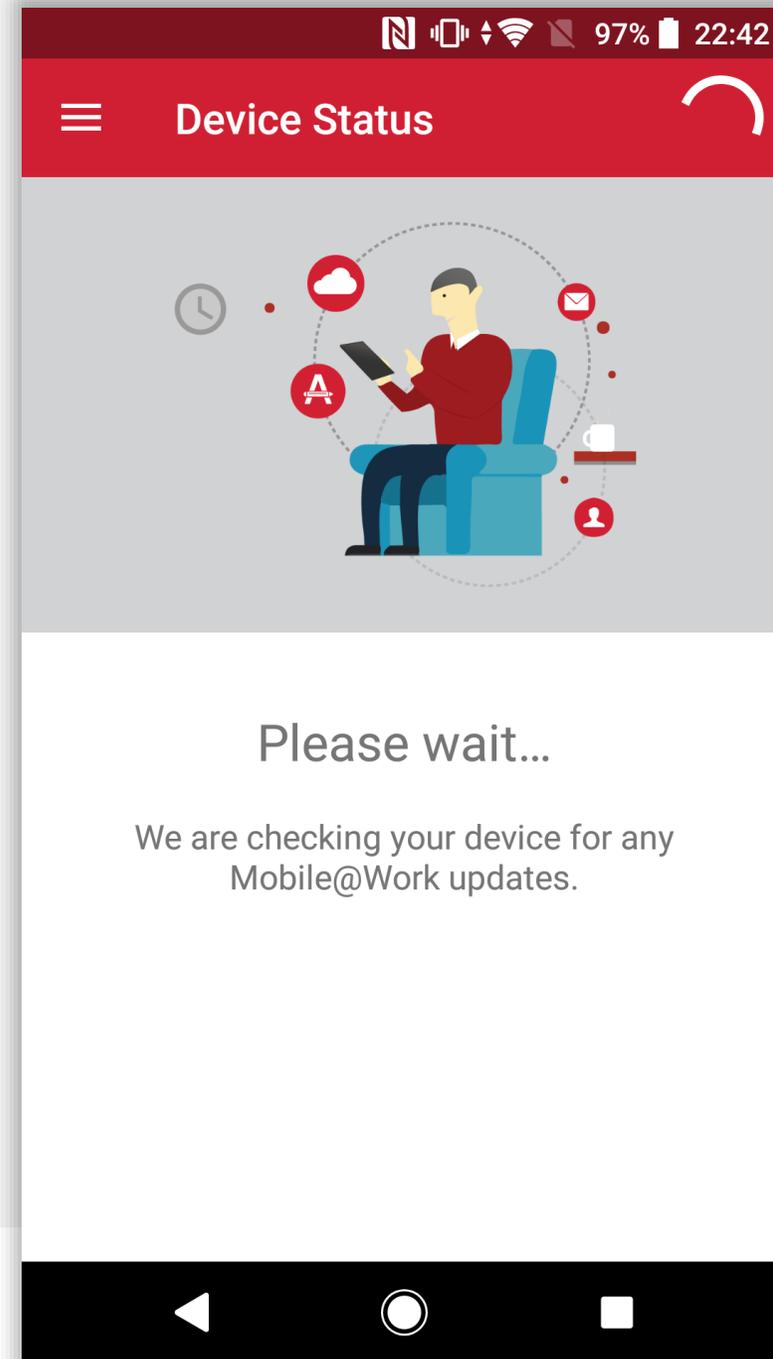
Enter the required fields and tap **SIGN IN**.

A screenshot of a mobile application's login screen. At the top, there's a header with a hamburger menu icon, a status bar showing '10:46', and an illustration of a person sitting at a desk talking to a person standing and holding a phone. Below the header, there are two input fields: 'COMPANY EMAIL' with the text 'jason@bayton.org' and 'PASSWORD' with the text 'Password'. A red underline is under the password field. To the right of the password field is a red 'SIGN IN' button. At the bottom, there is a standard QWERTY keyboard with a checkmark icon on the right side. The bottom of the screen shows the Android navigation bar.



Device configuration

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



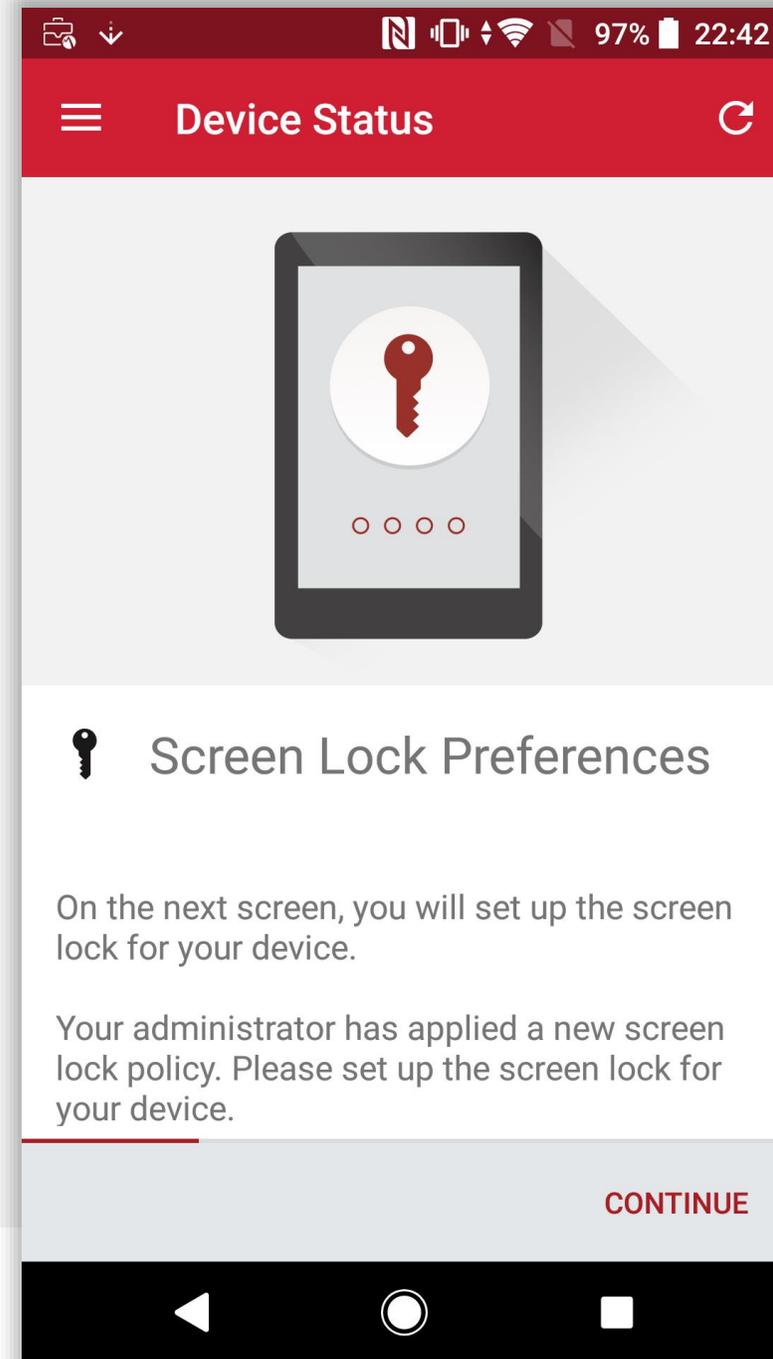


Device configuration

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.

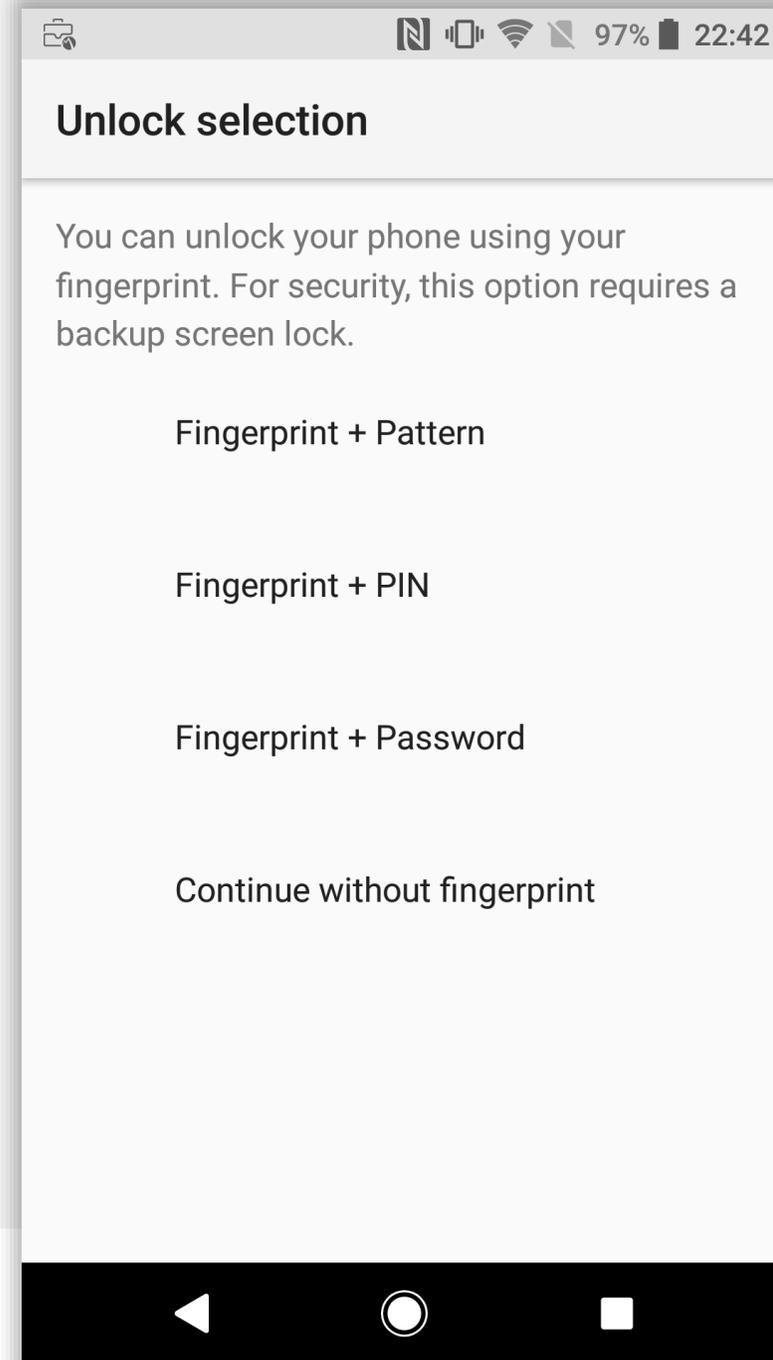
Tap **CONTINUE**.





Device configuration

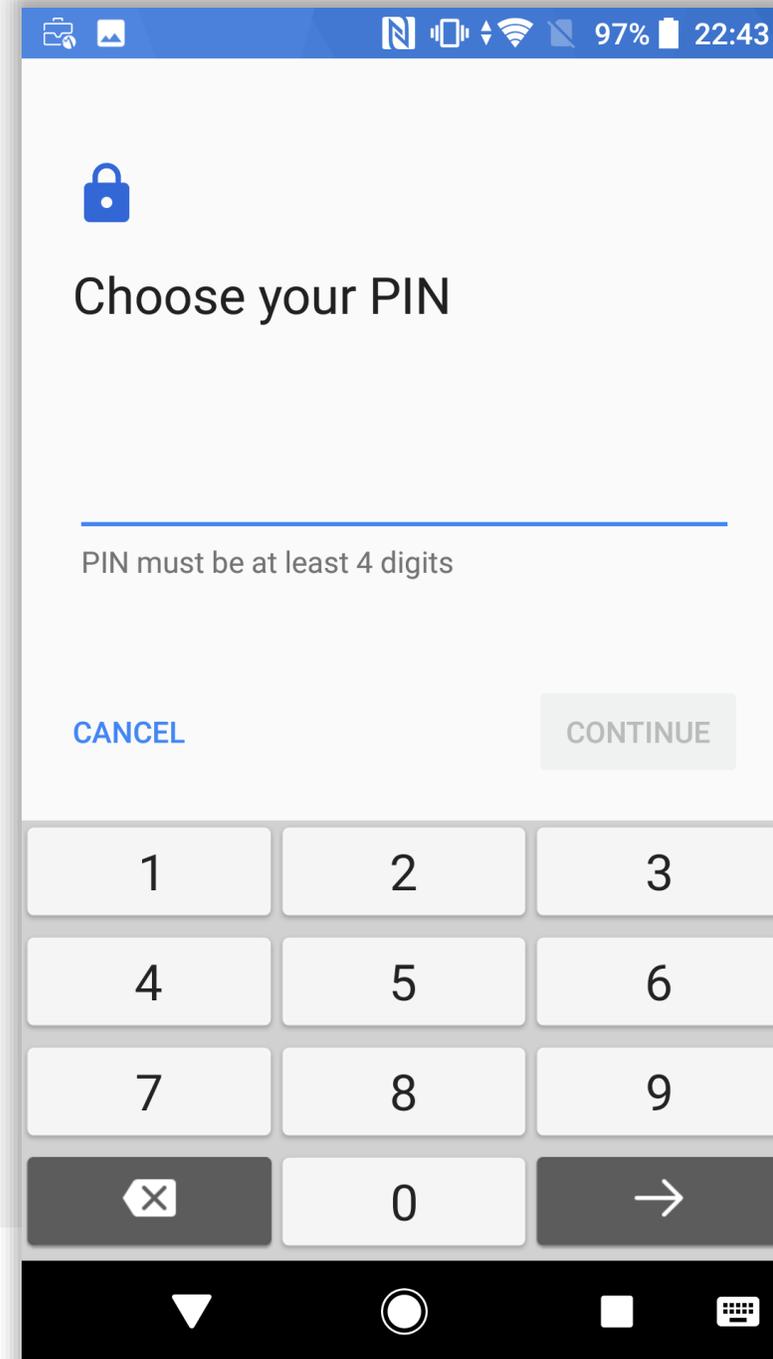
Select the relevant passcode, or skip fingerprint setup here and select a passcode on the following prompt, some options may not be available depending on the security policy deployed.





Device configuration

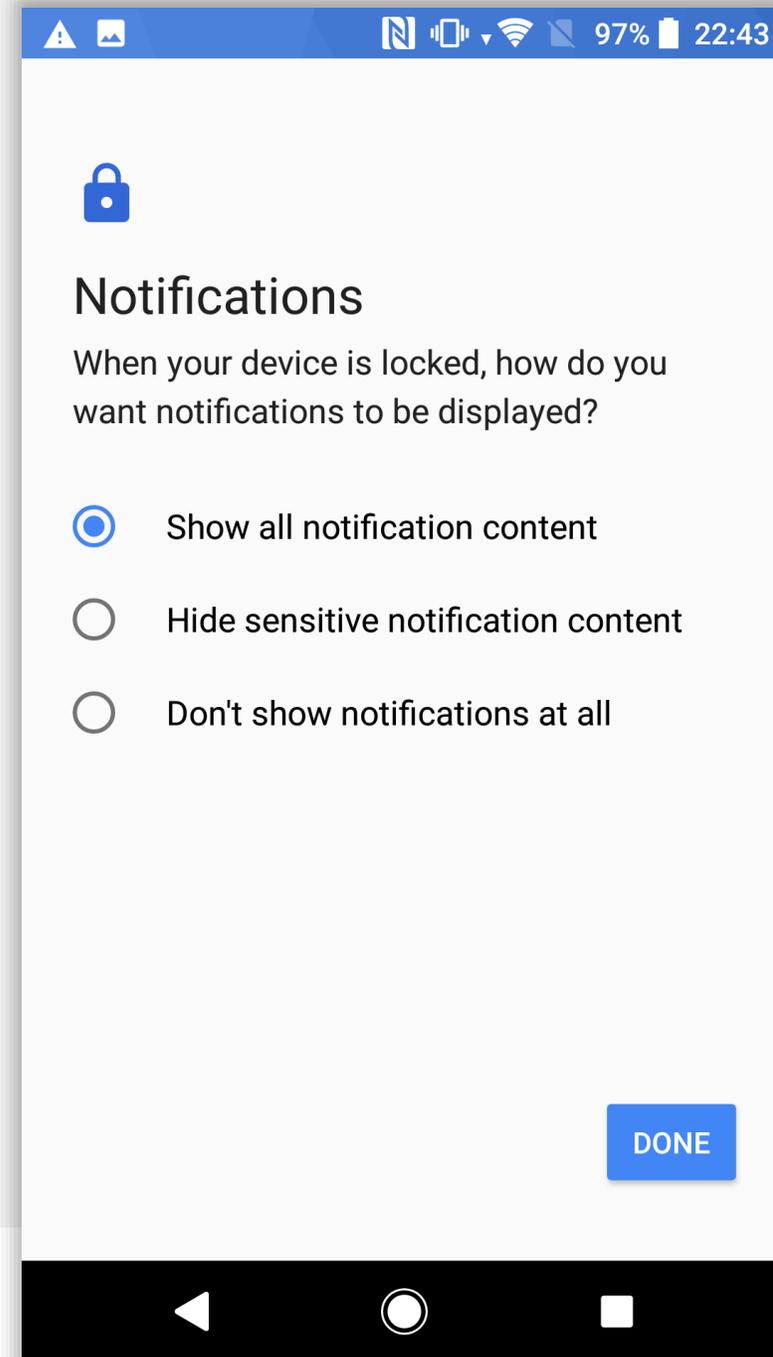
Input a PIN (or other passcode type) and tap **CONTINUE**.
Repeat to confirm.





Device configuration

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

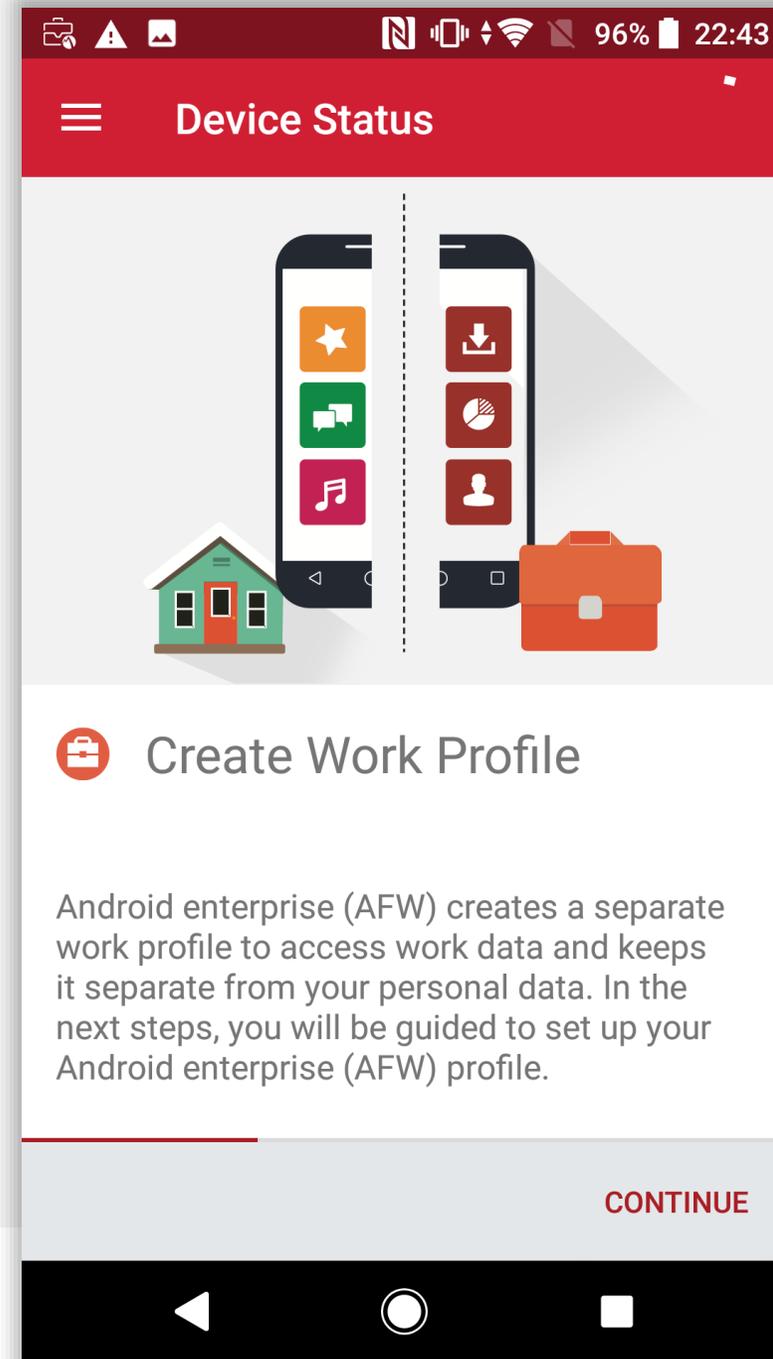




Work profile configuration

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.

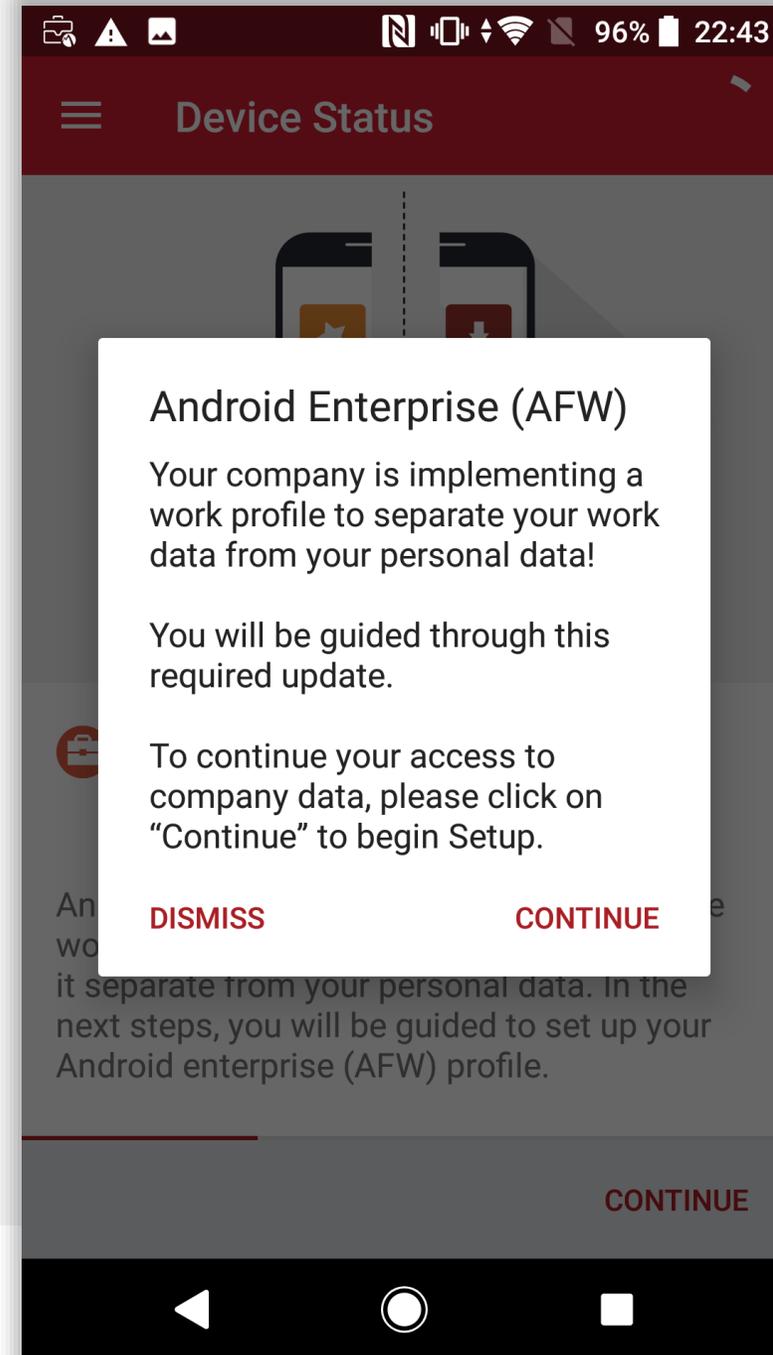
Tap **CONTINUE**.





Work profile configuration

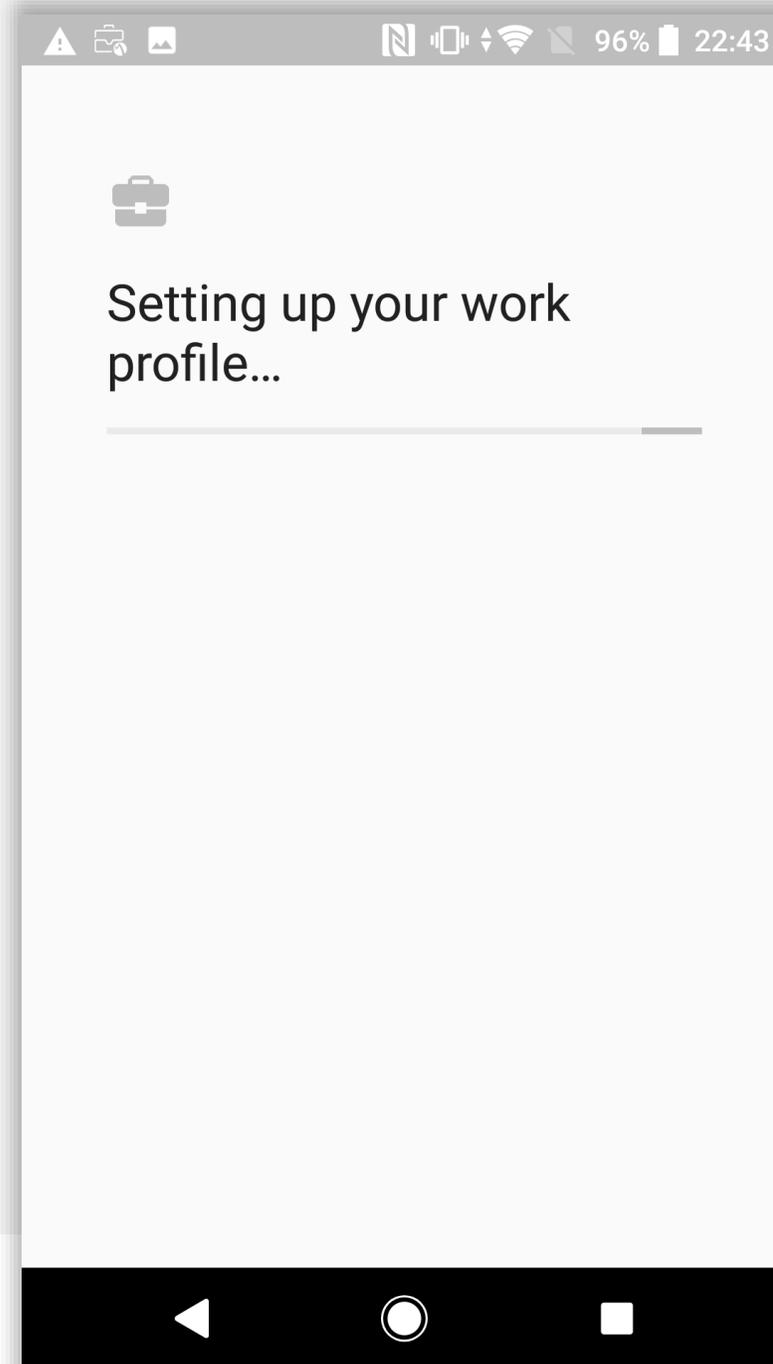
Accept the prompt, tap CONTINUE.





Work profile configuration

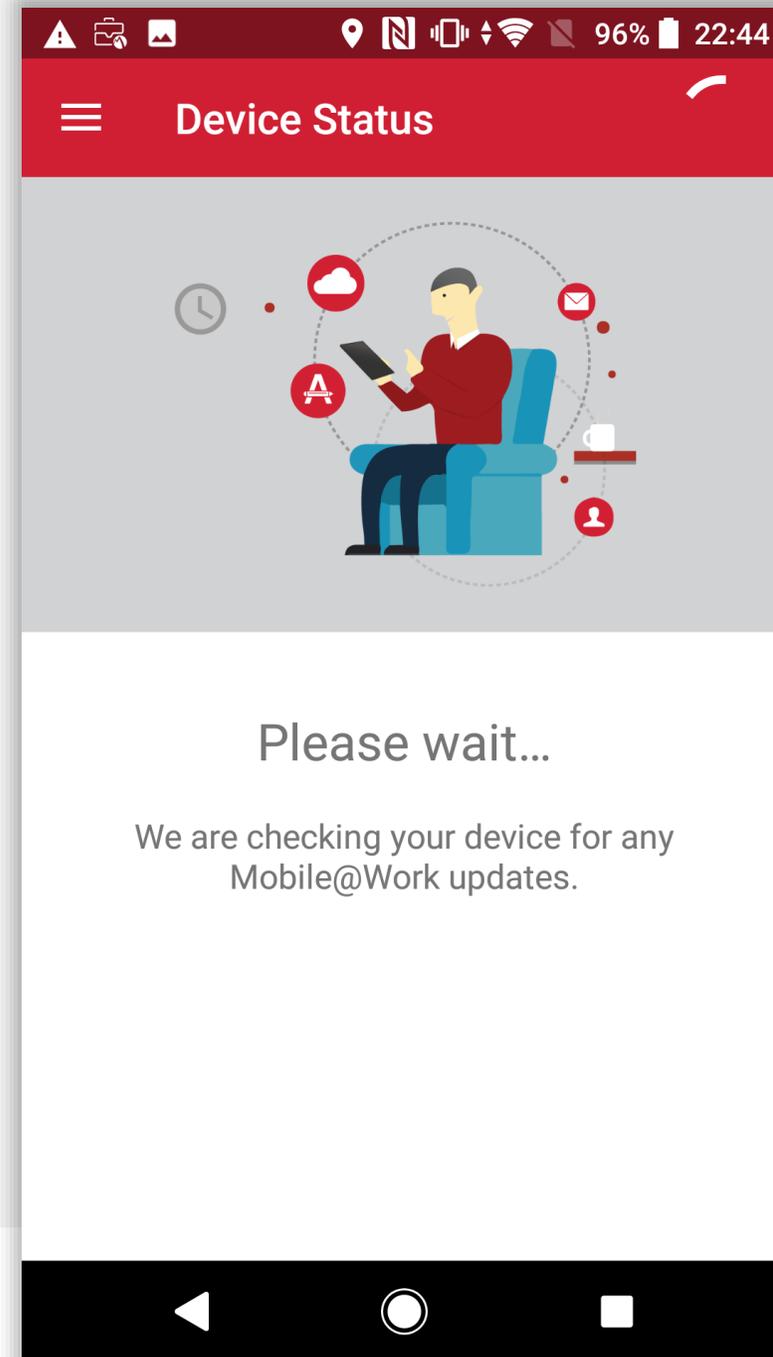
The device will now set up the work profile. This should be relatively quick and there is nothing needing to be done. This will automatically continue to the next step.





Work profile configuration

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



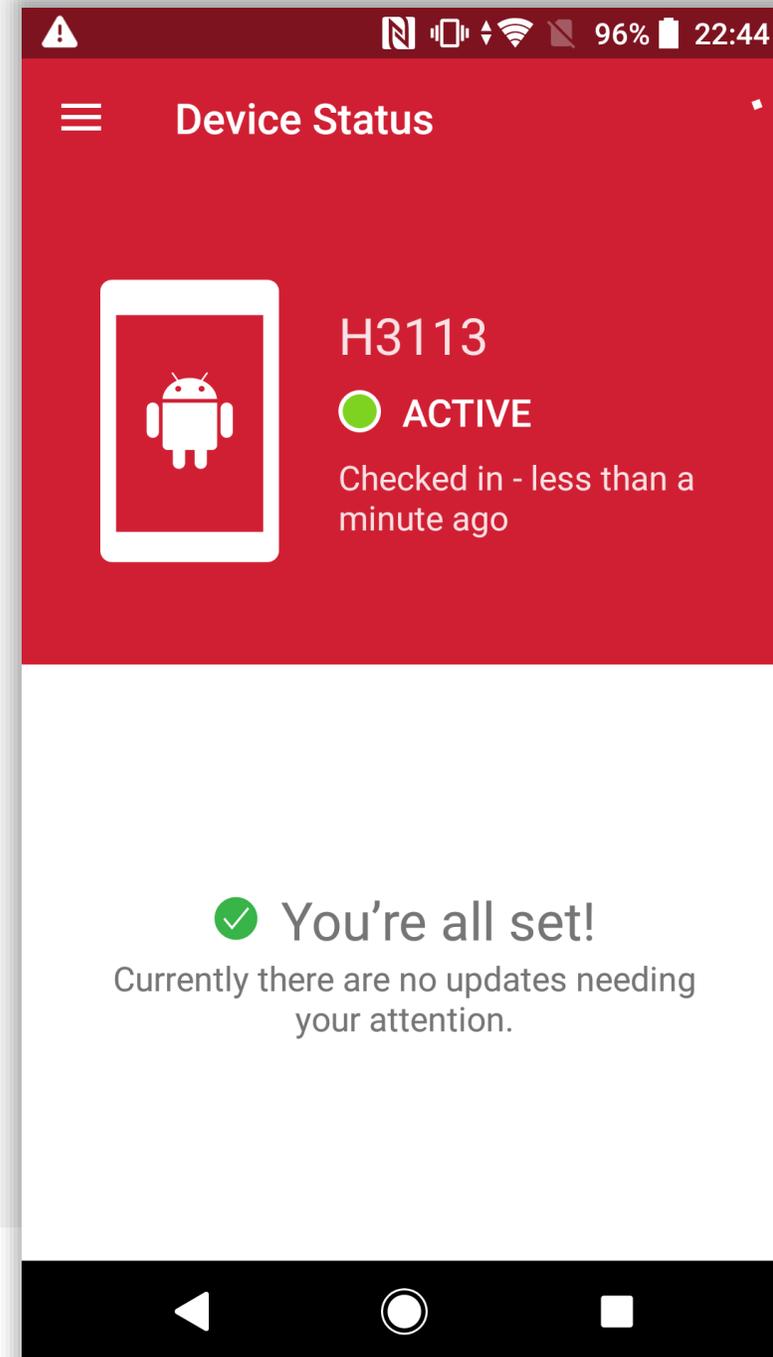


Enrolment complete

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.

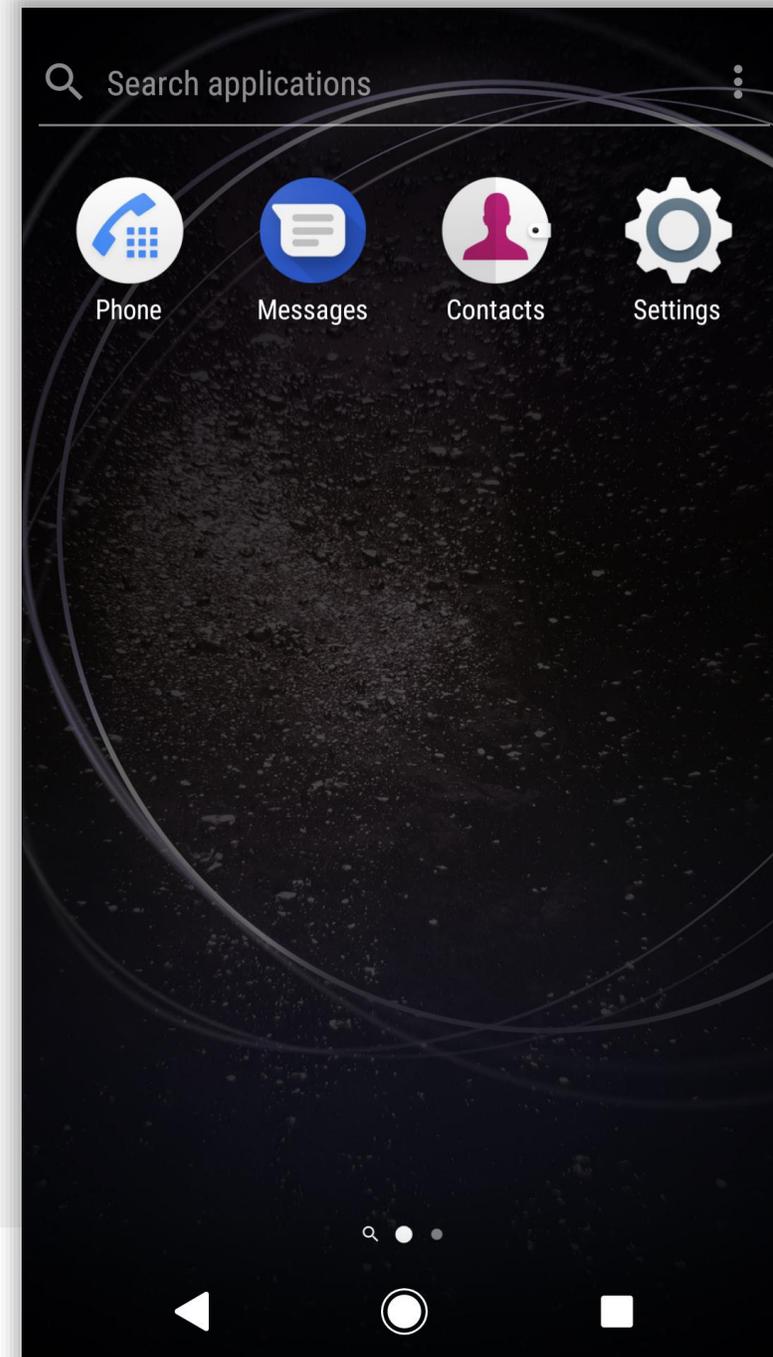




Add a personal account

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**.

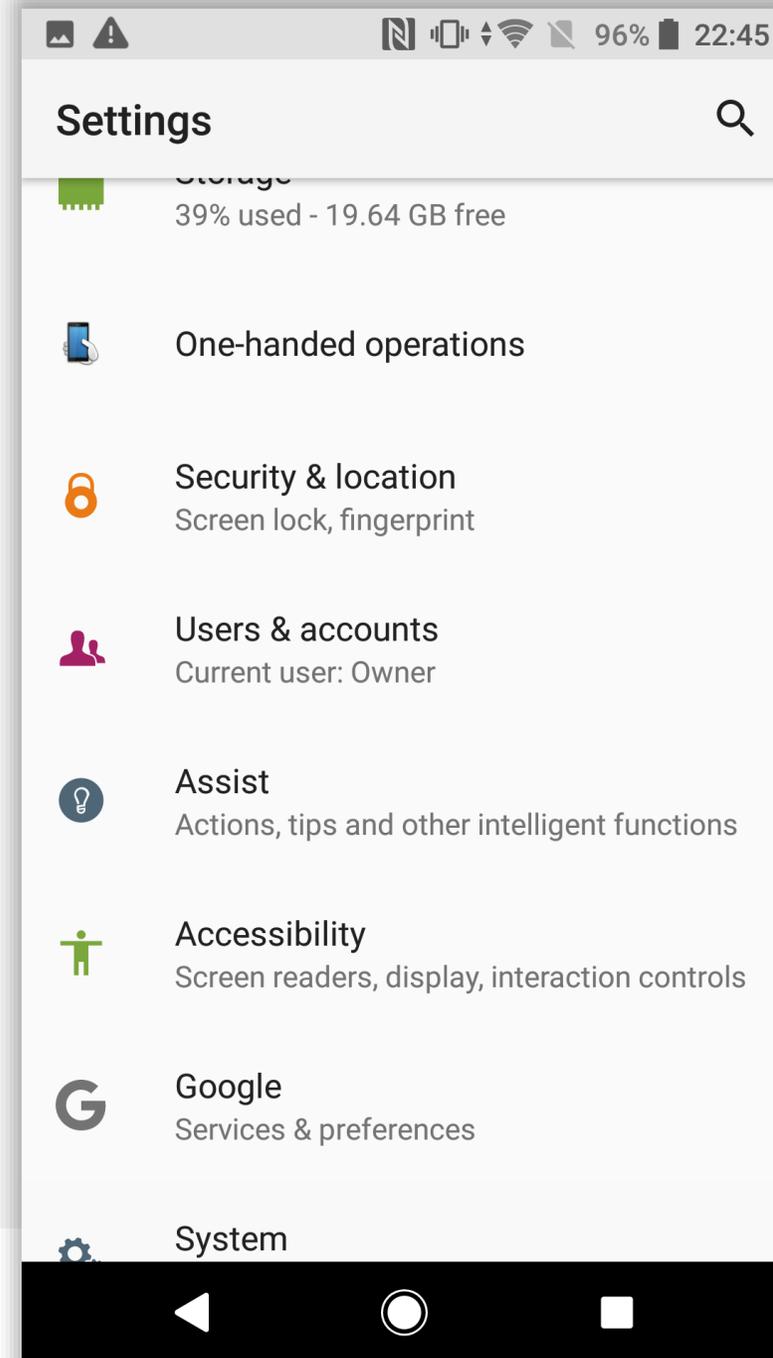




Add a personal account

Scroll down Settings until you find Users & accounts.

Tap Users & accounts.

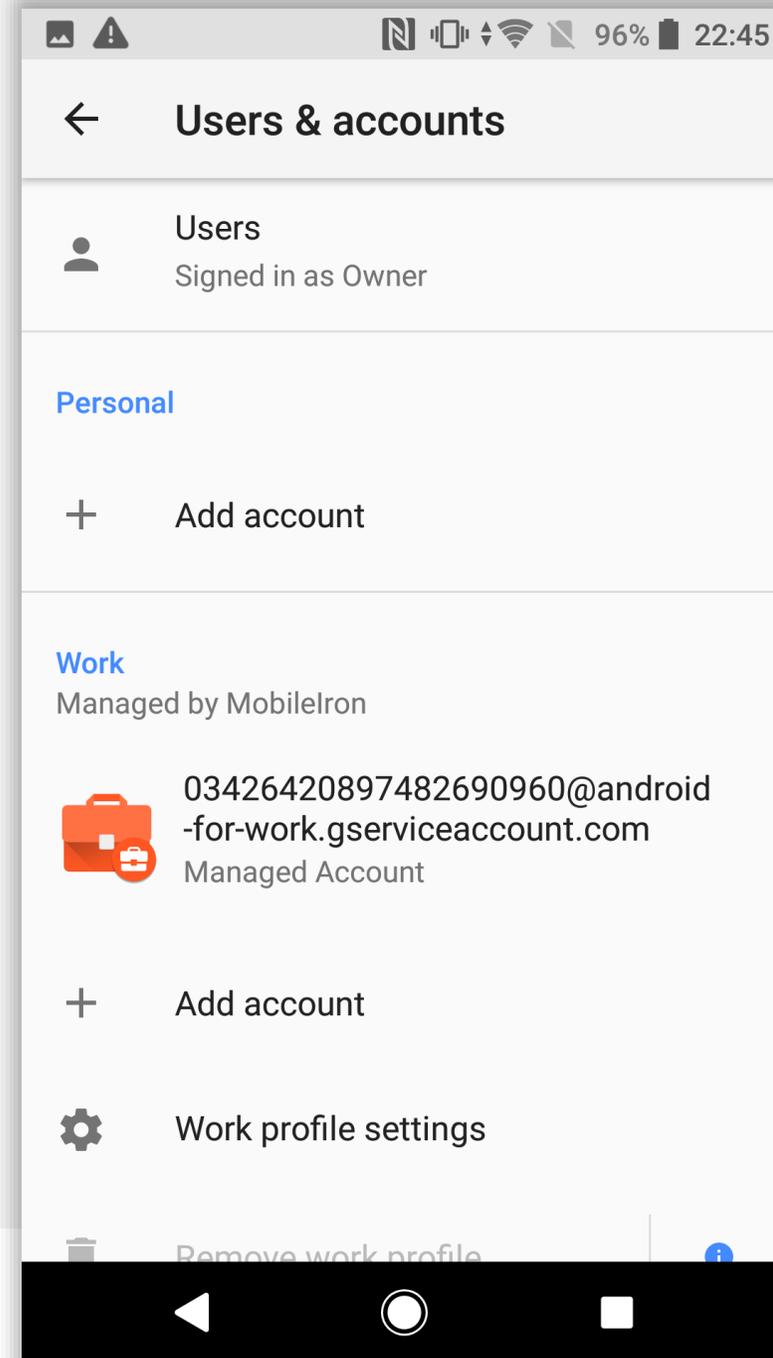




Add a personal account

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

Tap **Add account**.



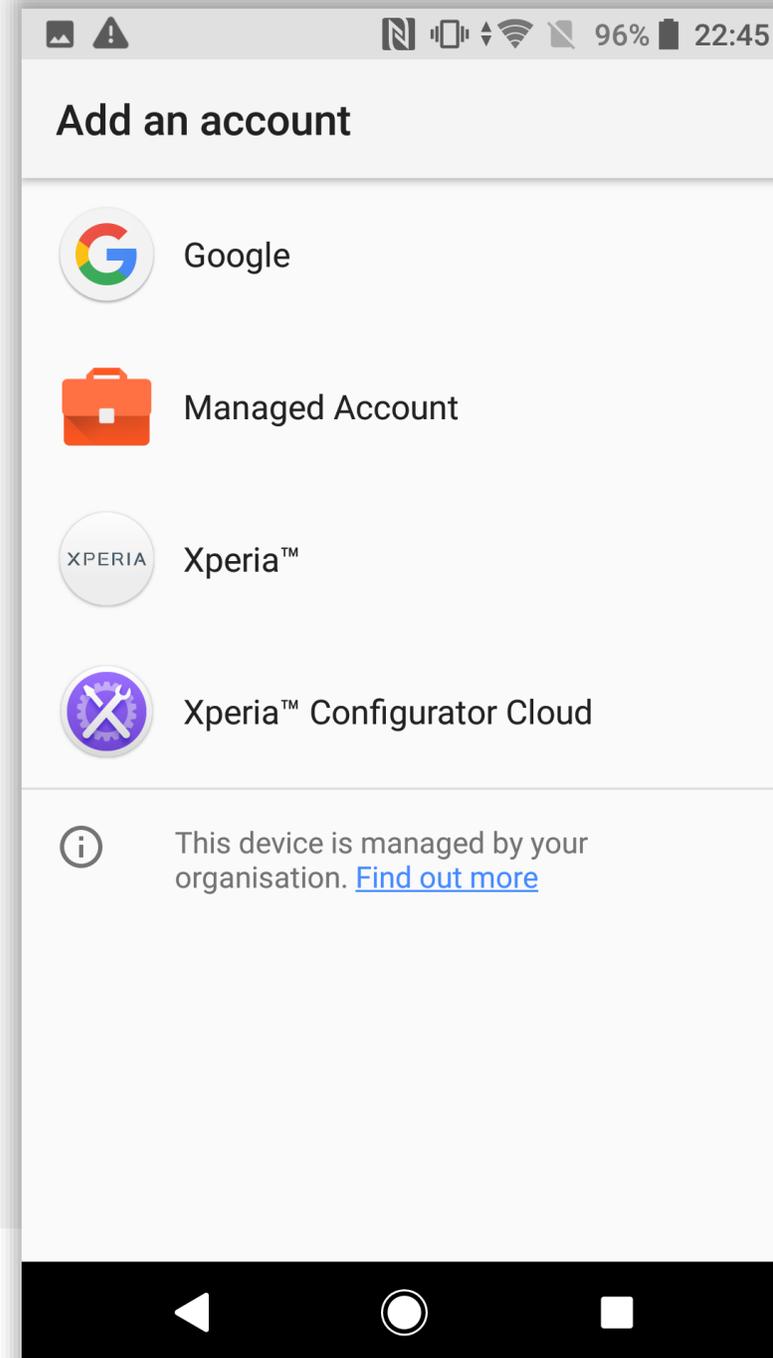


Setup complete

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](#)

