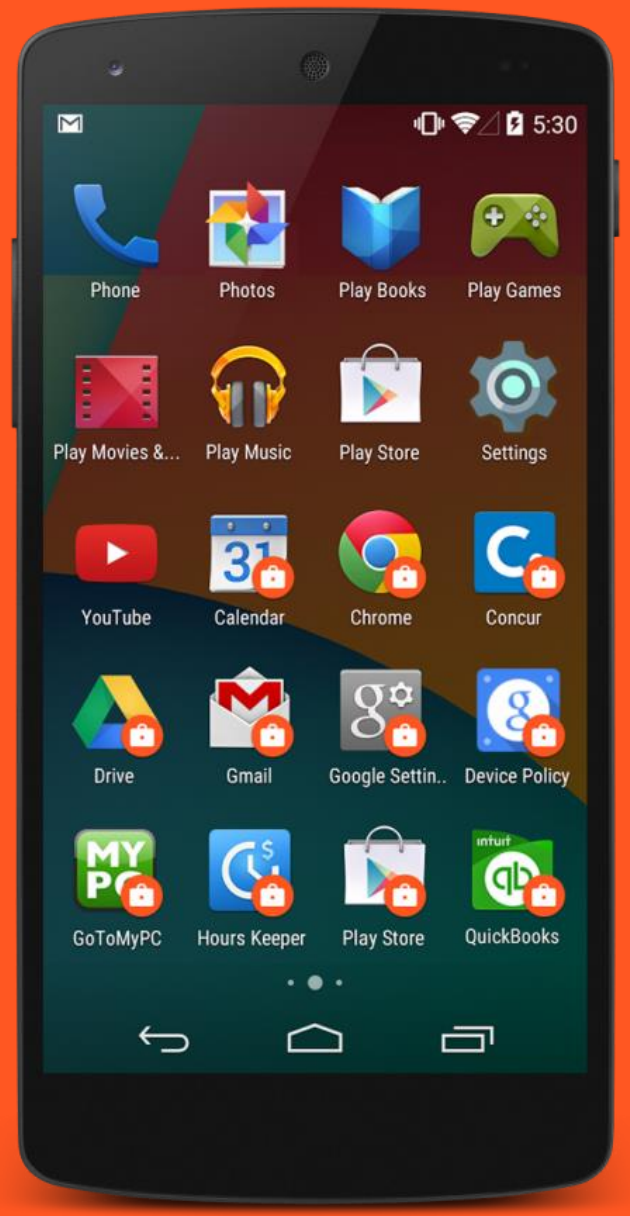


Android enterprise

Work-Managed enrolment
DPC identifier provisioning

MobileIron Core

Android 7.x

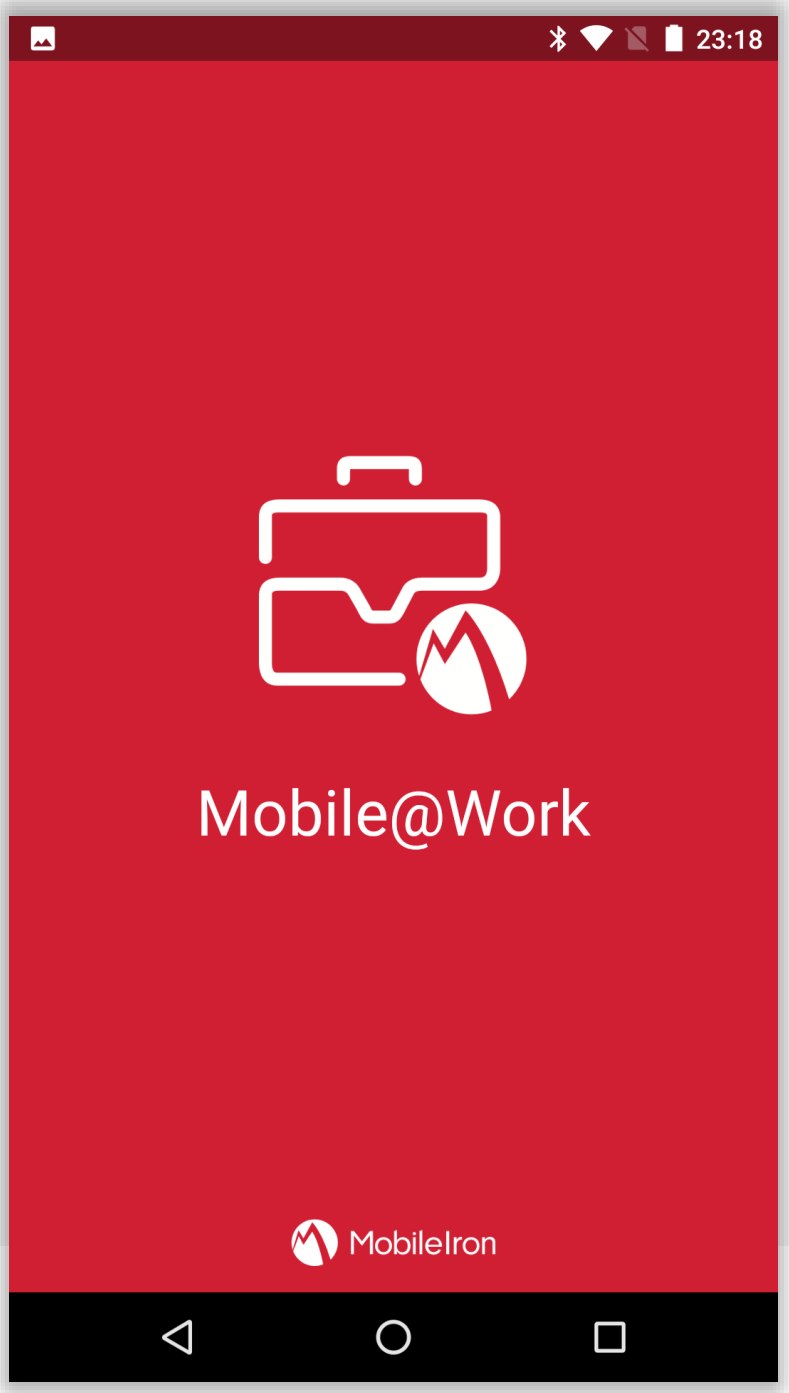
September 2017

Requirements

In order to proceed, you must have:

- Android 6.0 or later installed on the devices to be provisioned. Android 7.0+ recommended.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.

DPC identifier provisioning is simple, but may cause confusion for end-users as requesting they type a token into the Google account prompt may result in typos and/or misunderstandings. Consider as an alternative QR enrolment or NFC enrolment.



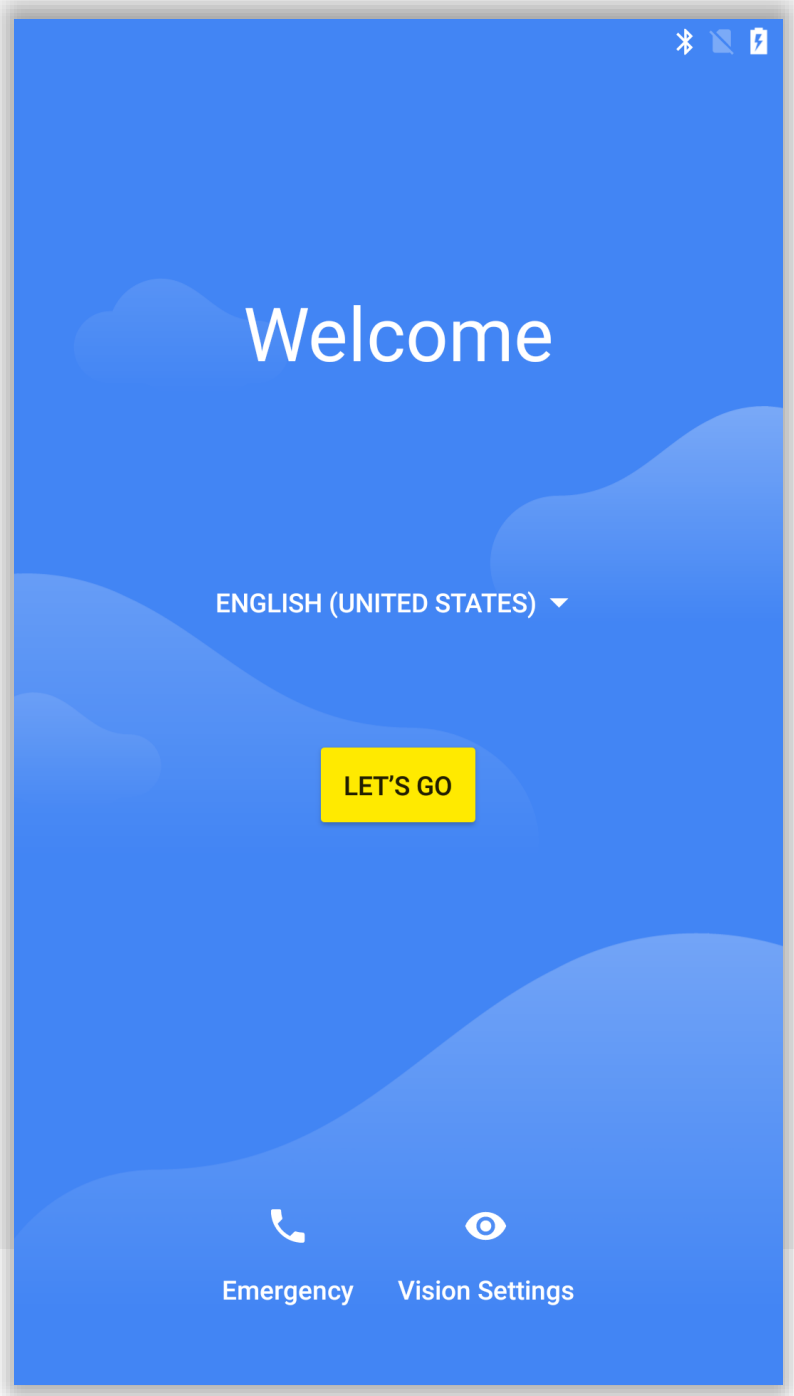
bayton

Begin device setup

For DPC identifier provisioning there are no special initial steps.

You must work through the first few steps of the Wizard, until a Google account is requested.

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

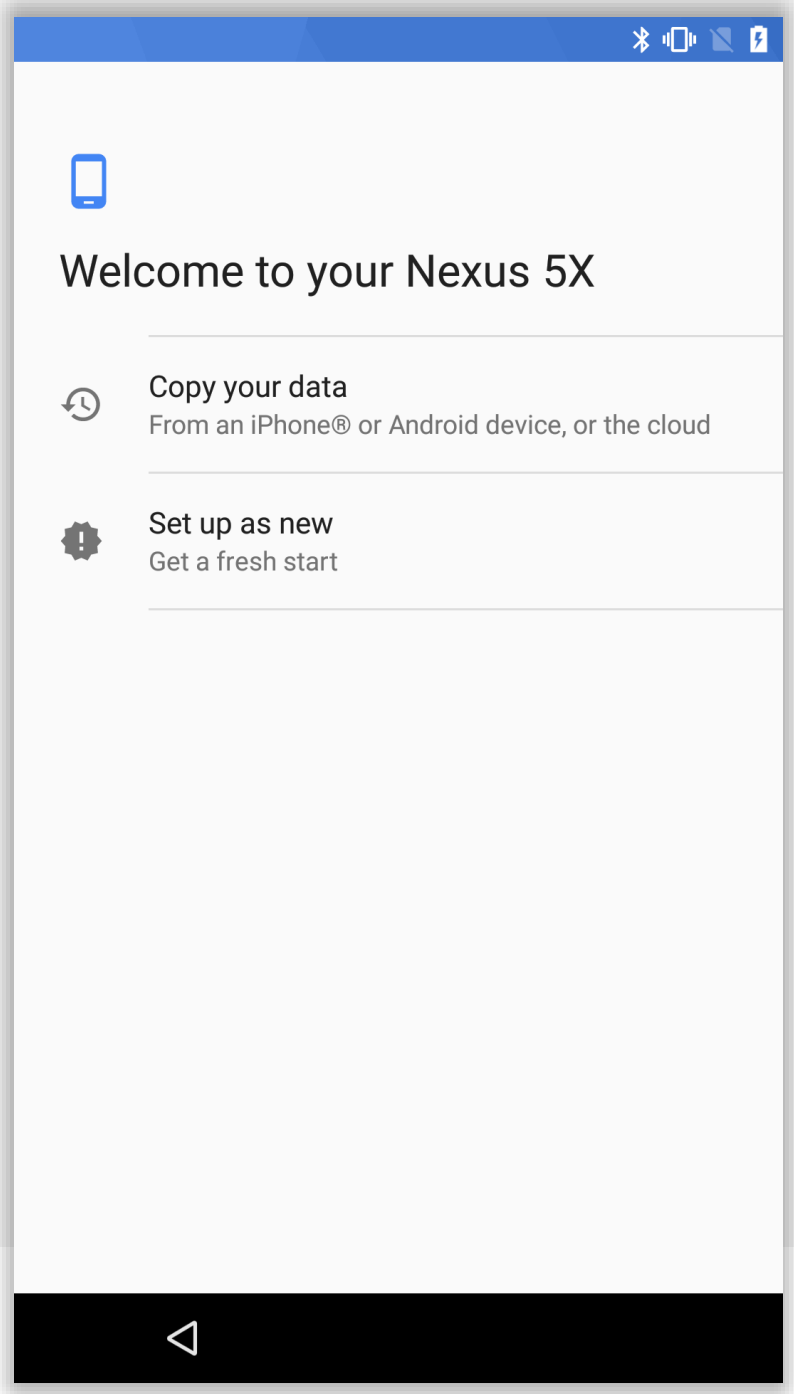


bayton

Continue device setup

Copying data from another device will result in an inability to provision the device again without undertaking a factory reset.

Tap **Set up as new**.



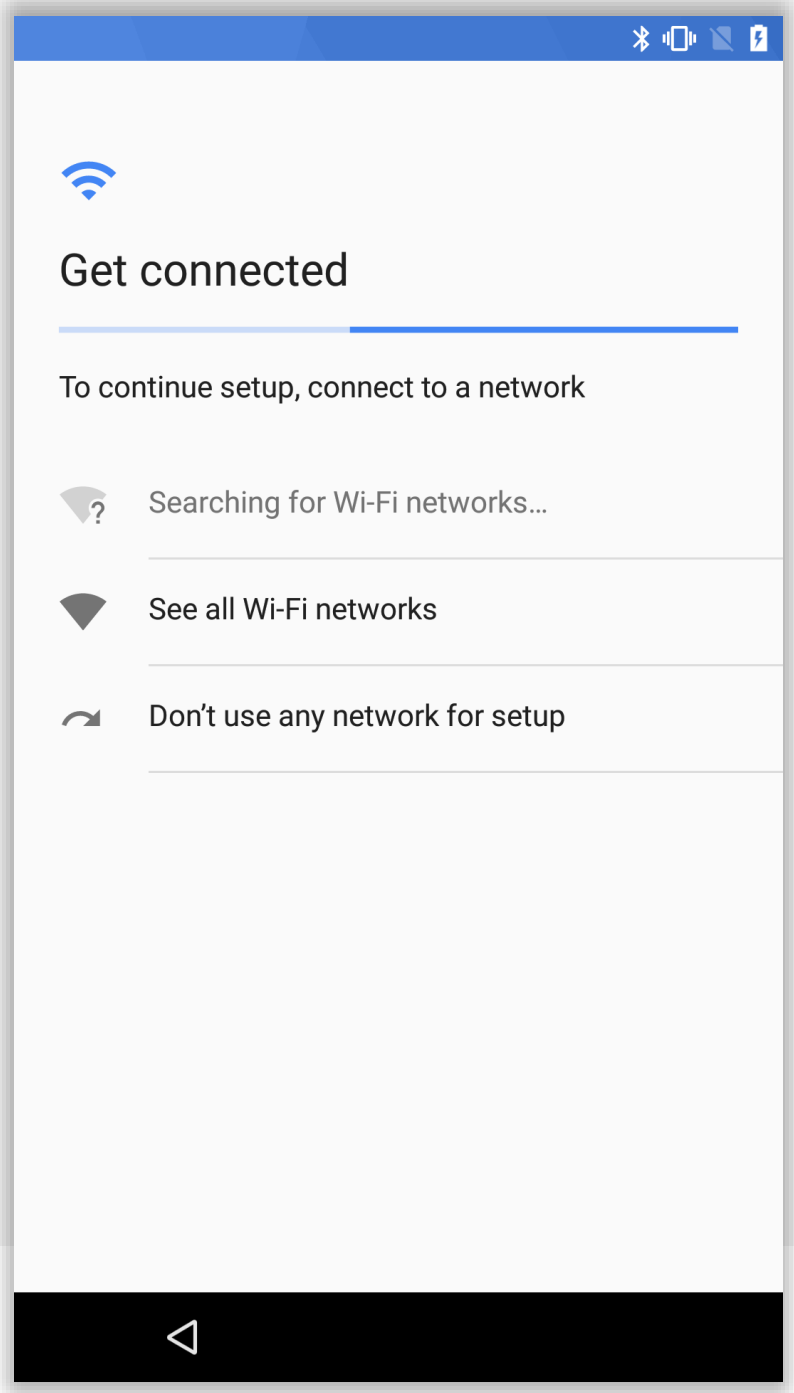
bayton

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.

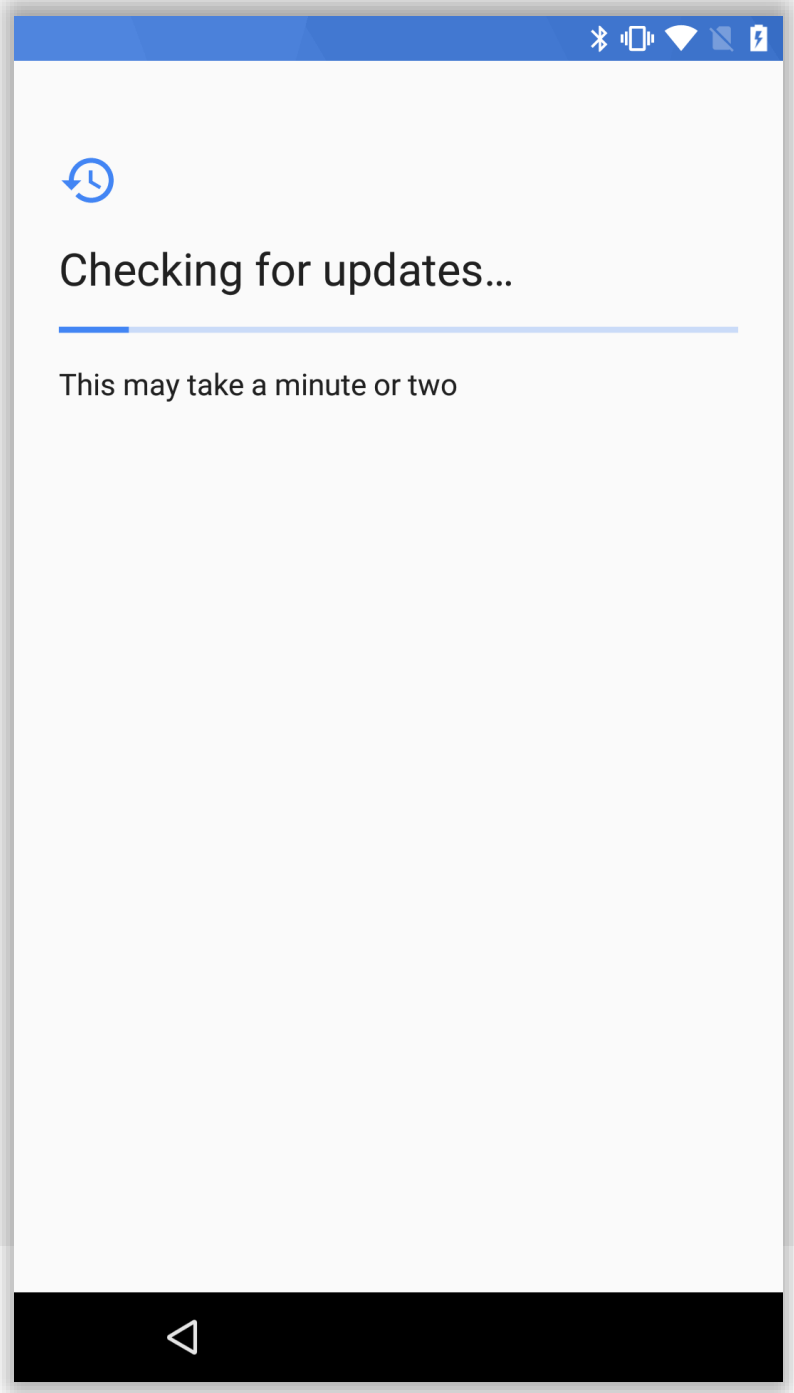
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup**.



bayton

Continue device setup

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



bayton

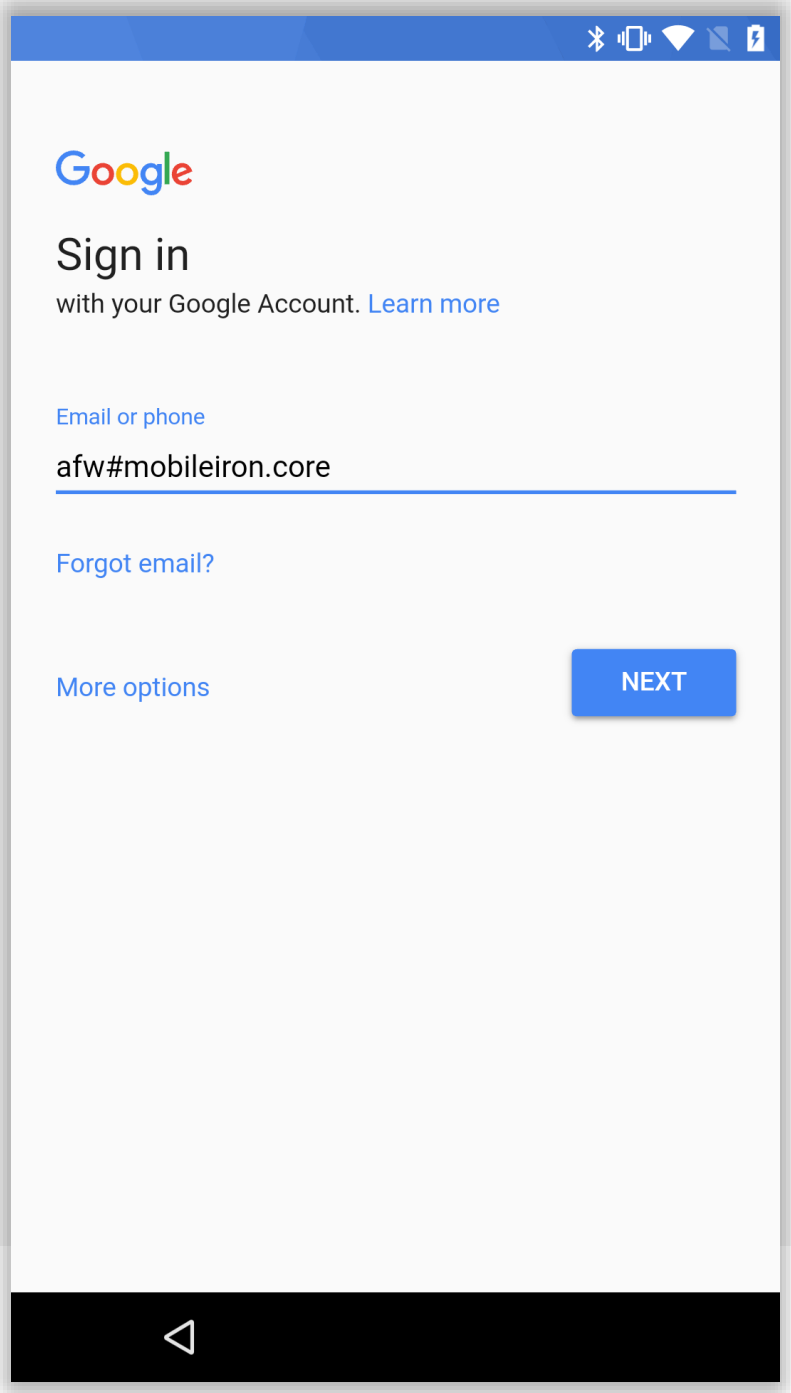
Input the DPC identifier

At the Google account sign in screen, input the following DPC identifier:

afw#mobileiron.core

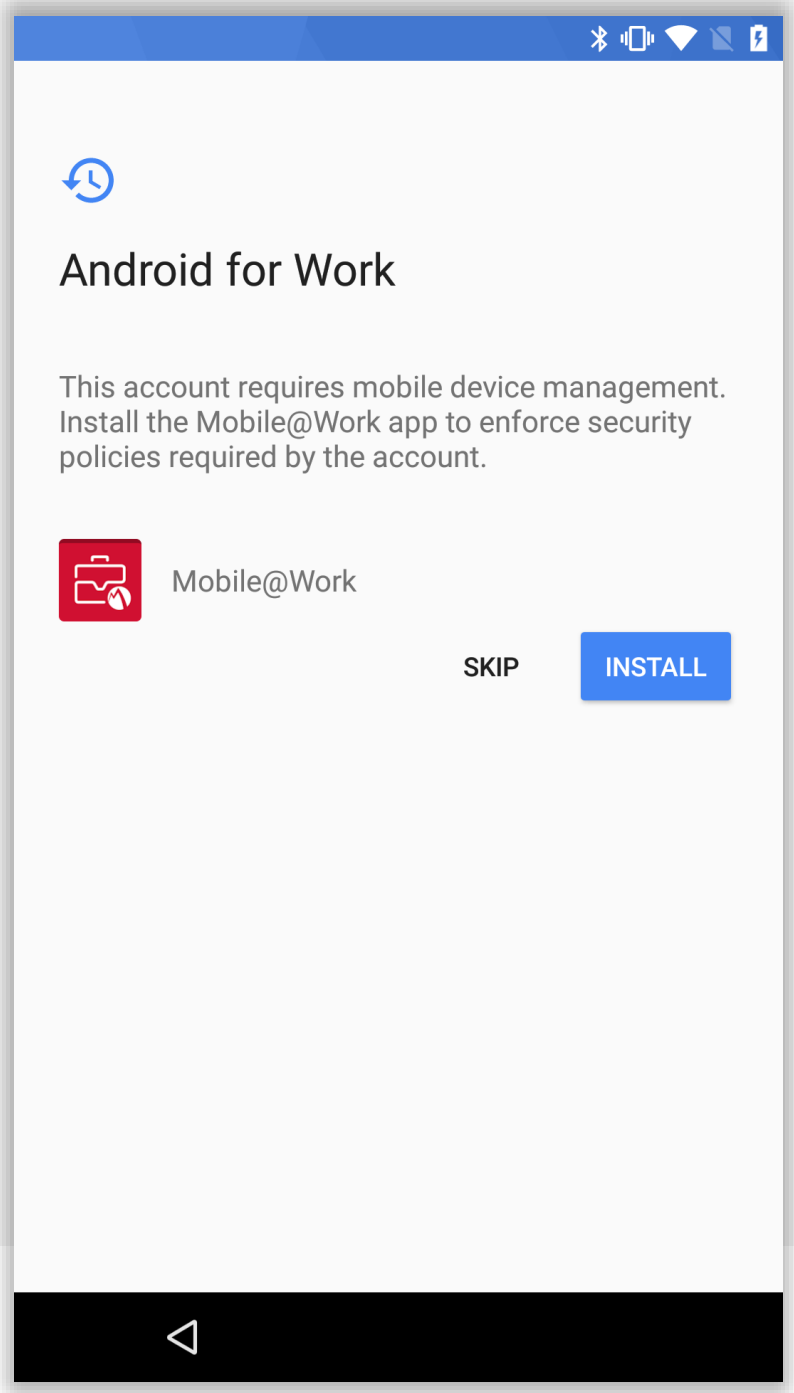
Each EMM provider has one or more of these unique tokens, each depicting the DPC that will be downloaded for enrolment.

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



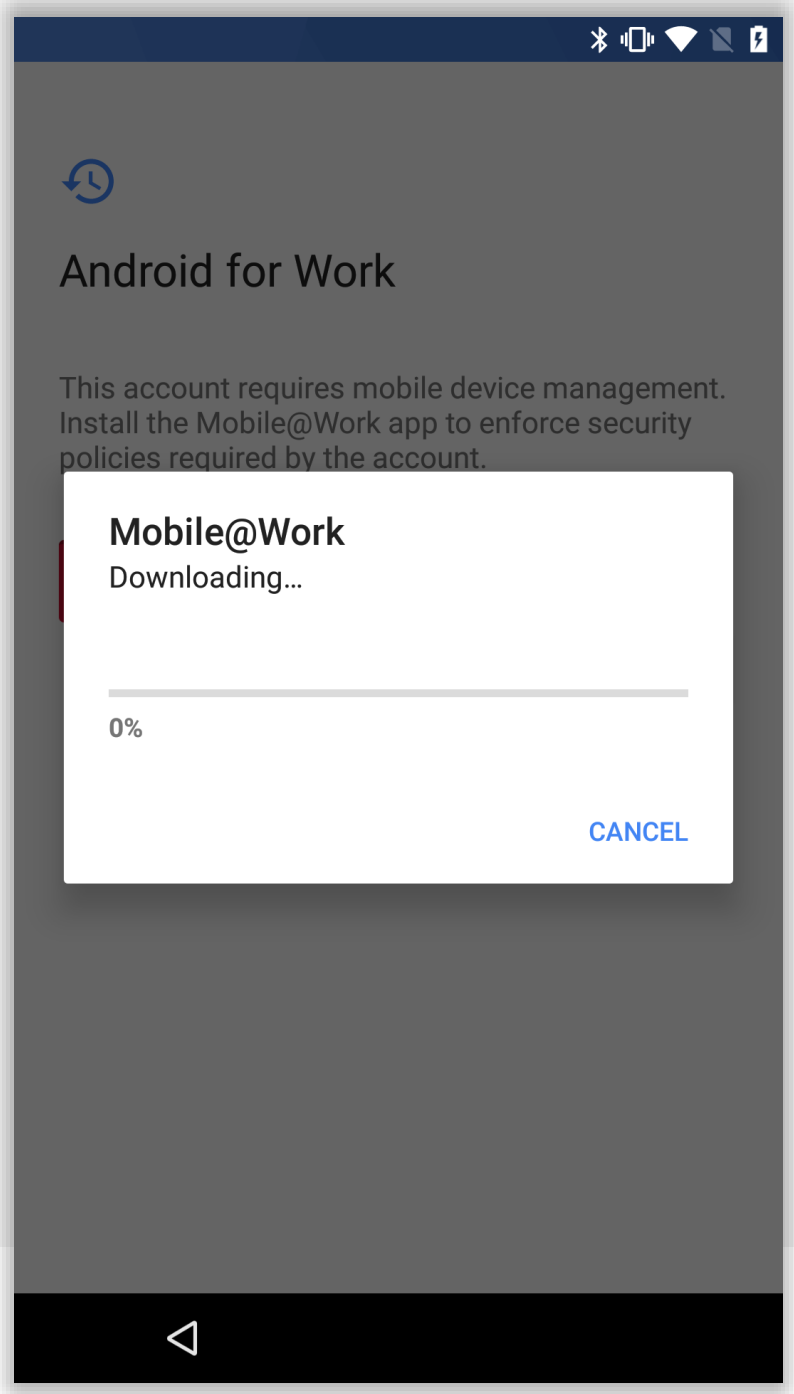
Provisioning in progress

The device will now prompt you to install the chosen DPC – Mobile@Work in this instance – and will begin to download in order to do so once INSTALL is tapped.



Provisioning in progress

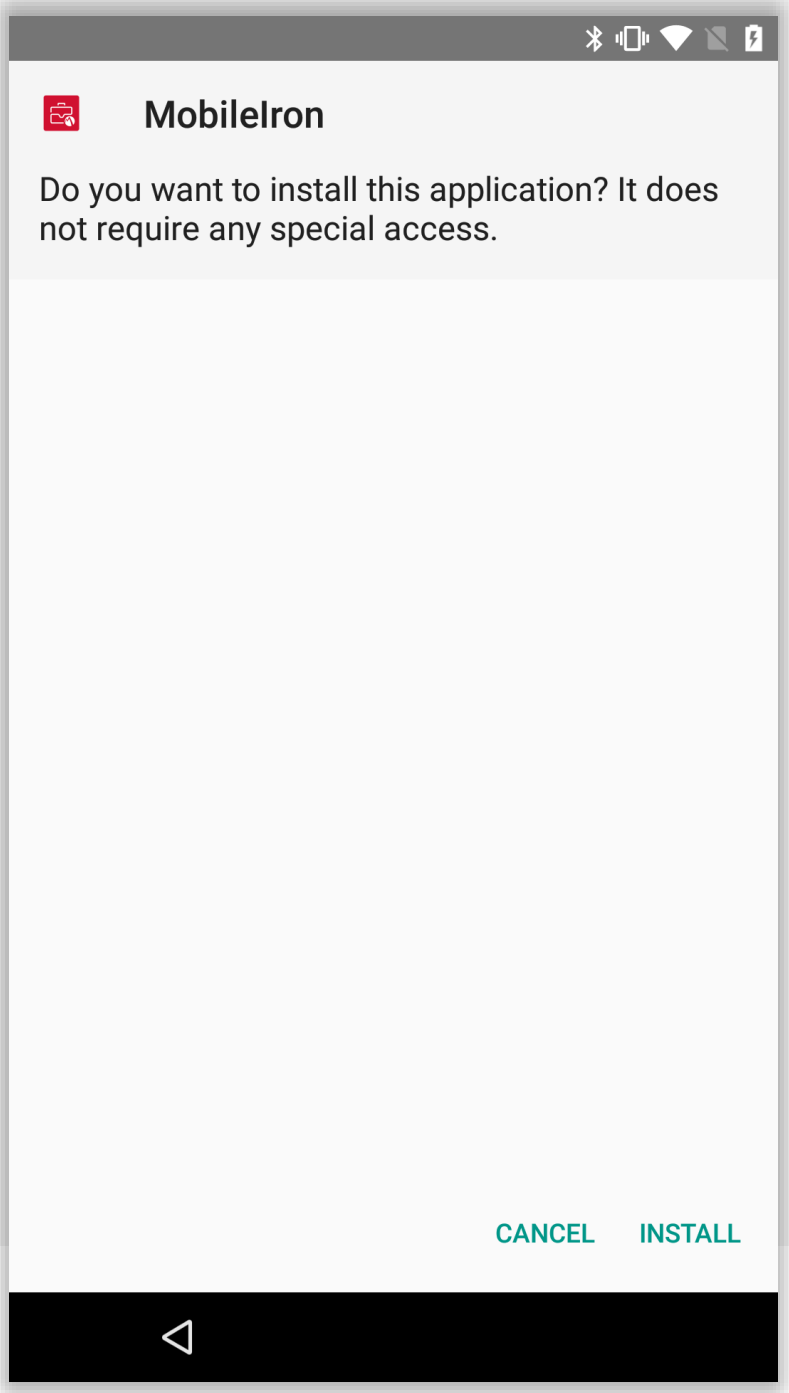
The device will now download the DPC and automatically move to the next step in the process.



Provisioning in progress

Unlike other provisioning options (NFC, QR), using token enrolment prompts you to install the DPC manually.

Tap **INSTALL** in order to continue.

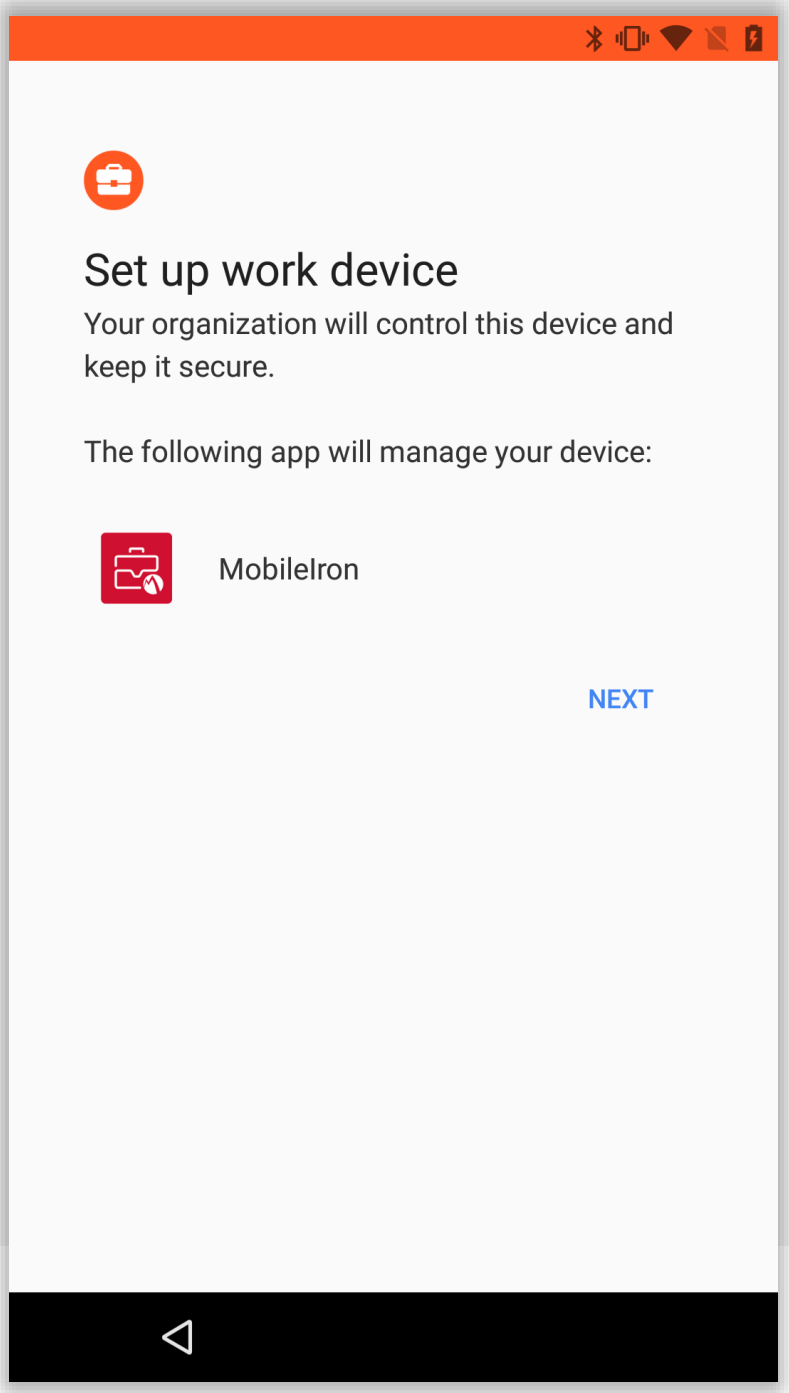


bayton

Provisioning in progress

Following installation, the device will prompt you to confirm you're aware that the organisation has full control over the device.

Tap **NEXT** to continue.

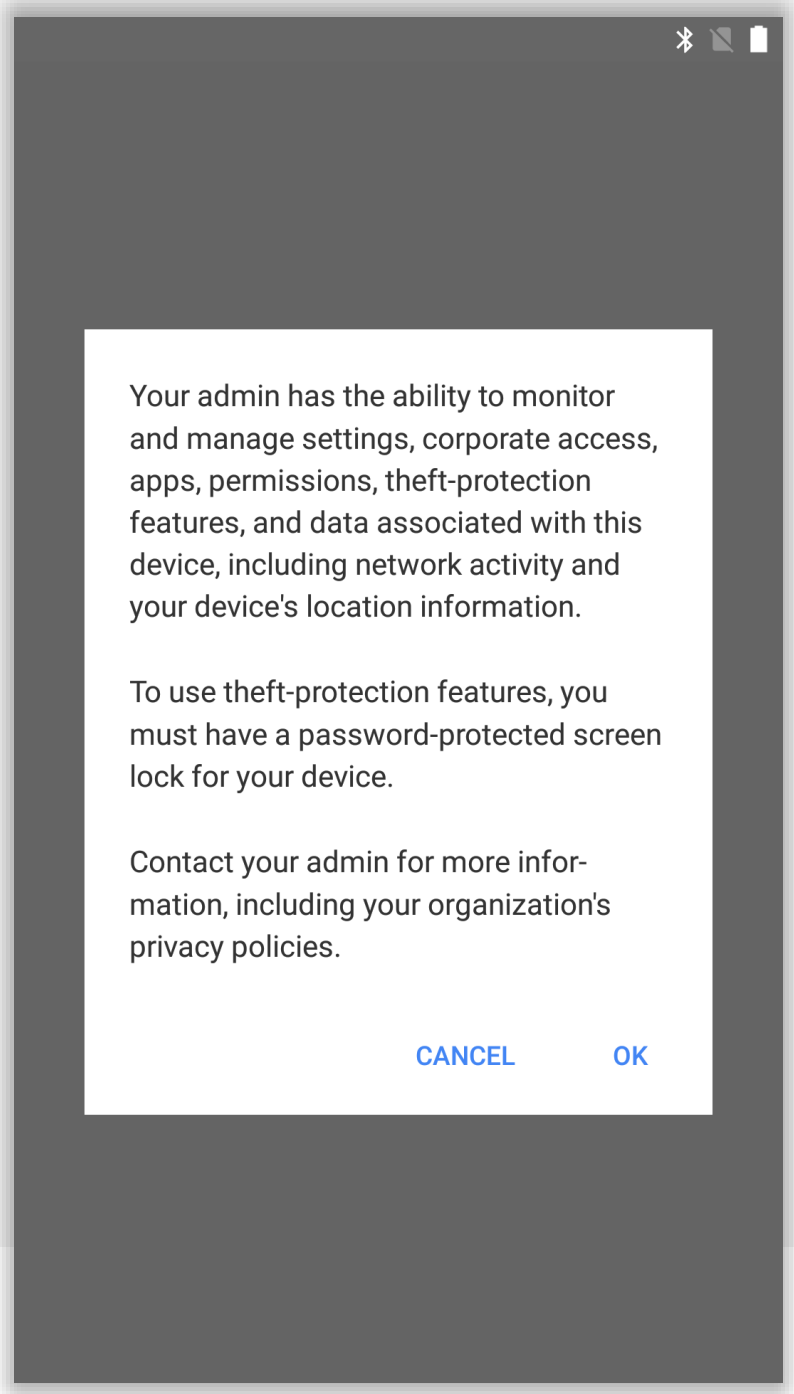


Provisioning in progress

The device being provisioned will again 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 **OK** to proceed.



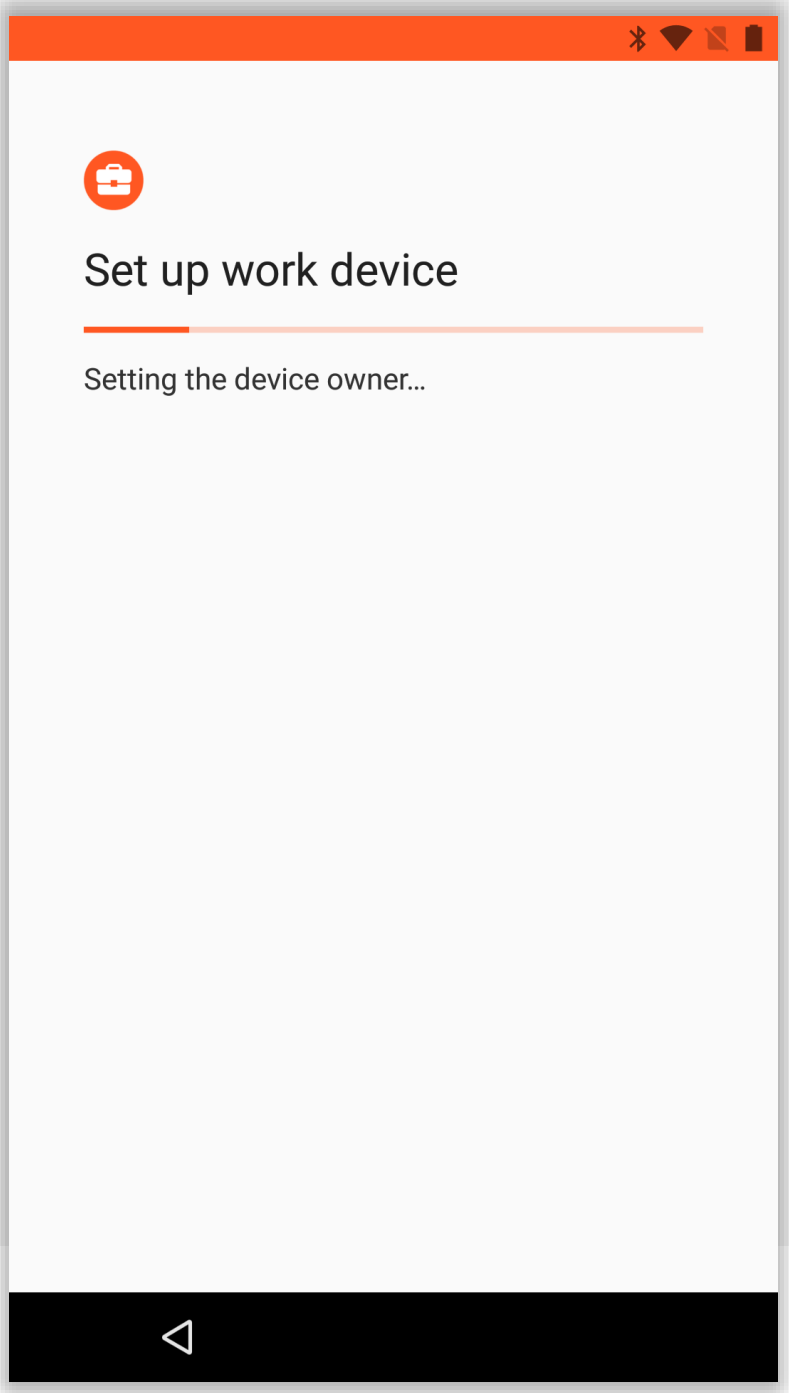
bayton

Provisioning in progress

The device will set the device owner and continue the provisioning process.

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 a sparse home screen before the DPC launches.

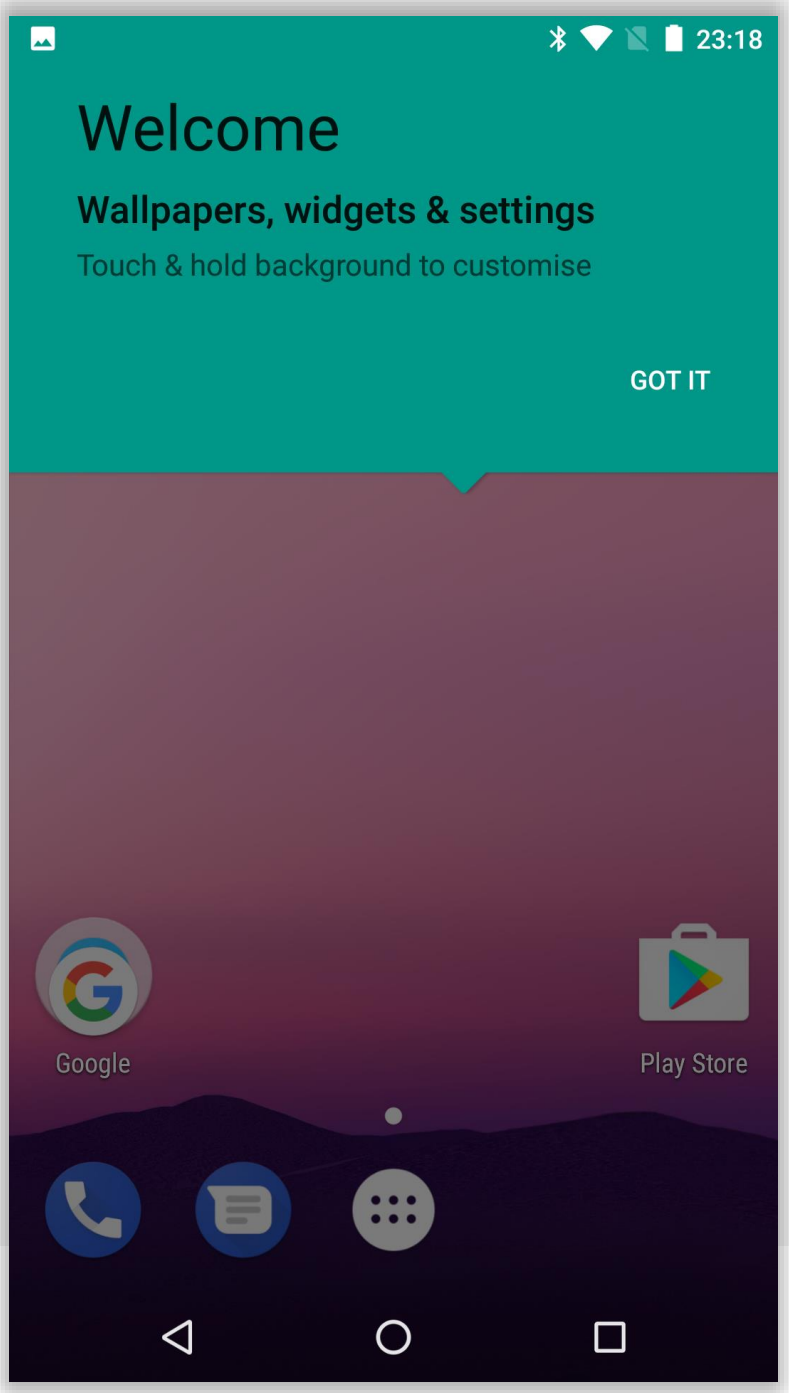


bayton

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.

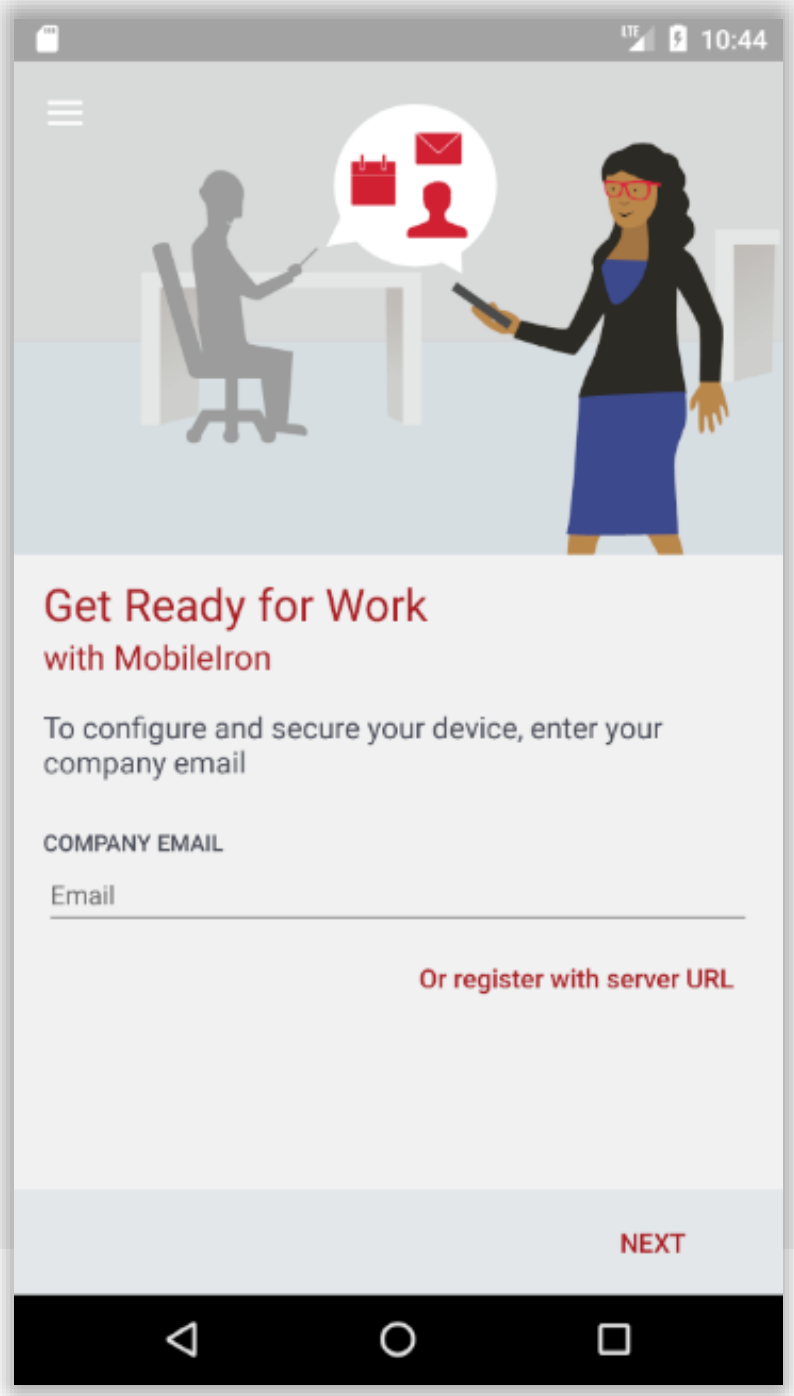


bayton

Begin enrolment

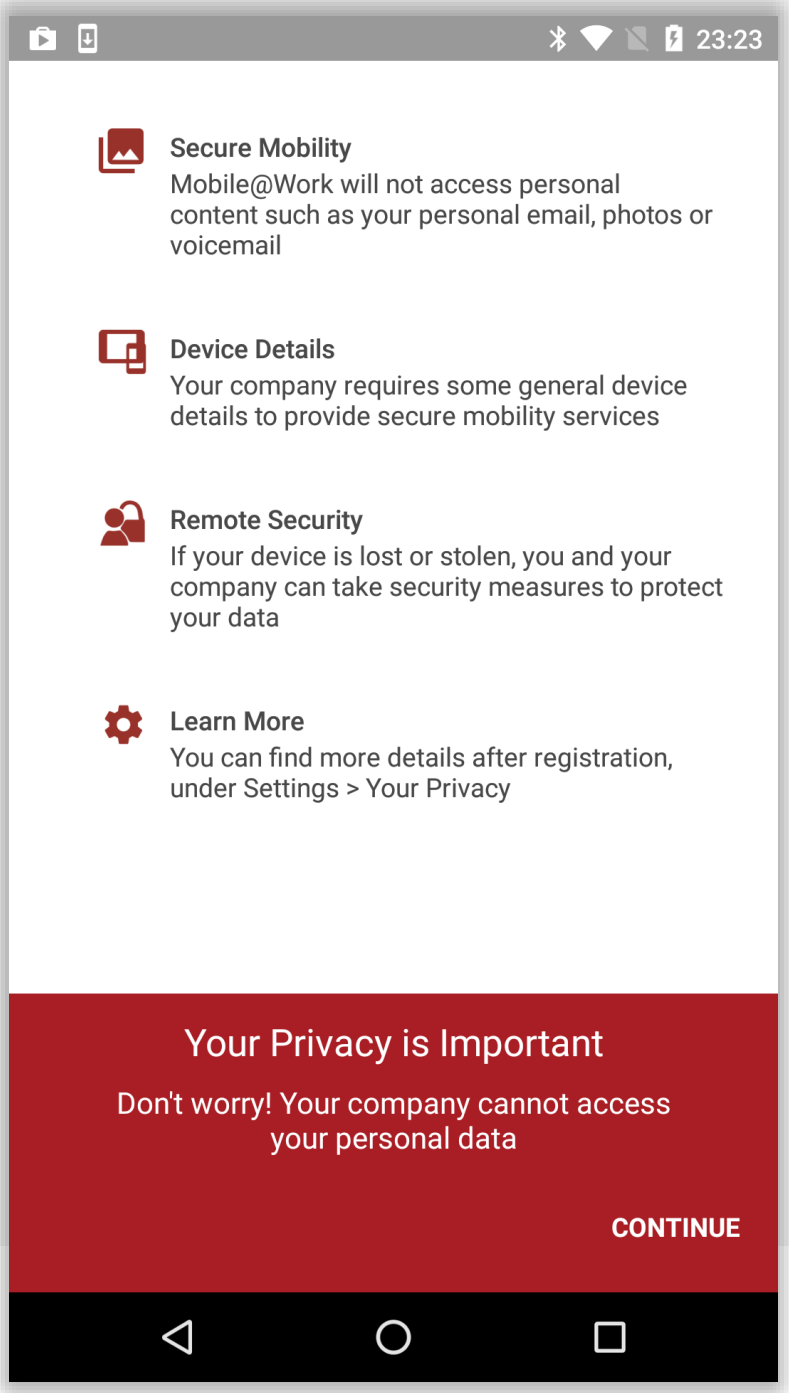
Input your email address (or switch to server URL if required).

Tap **NEXT**.



Continue enrolment

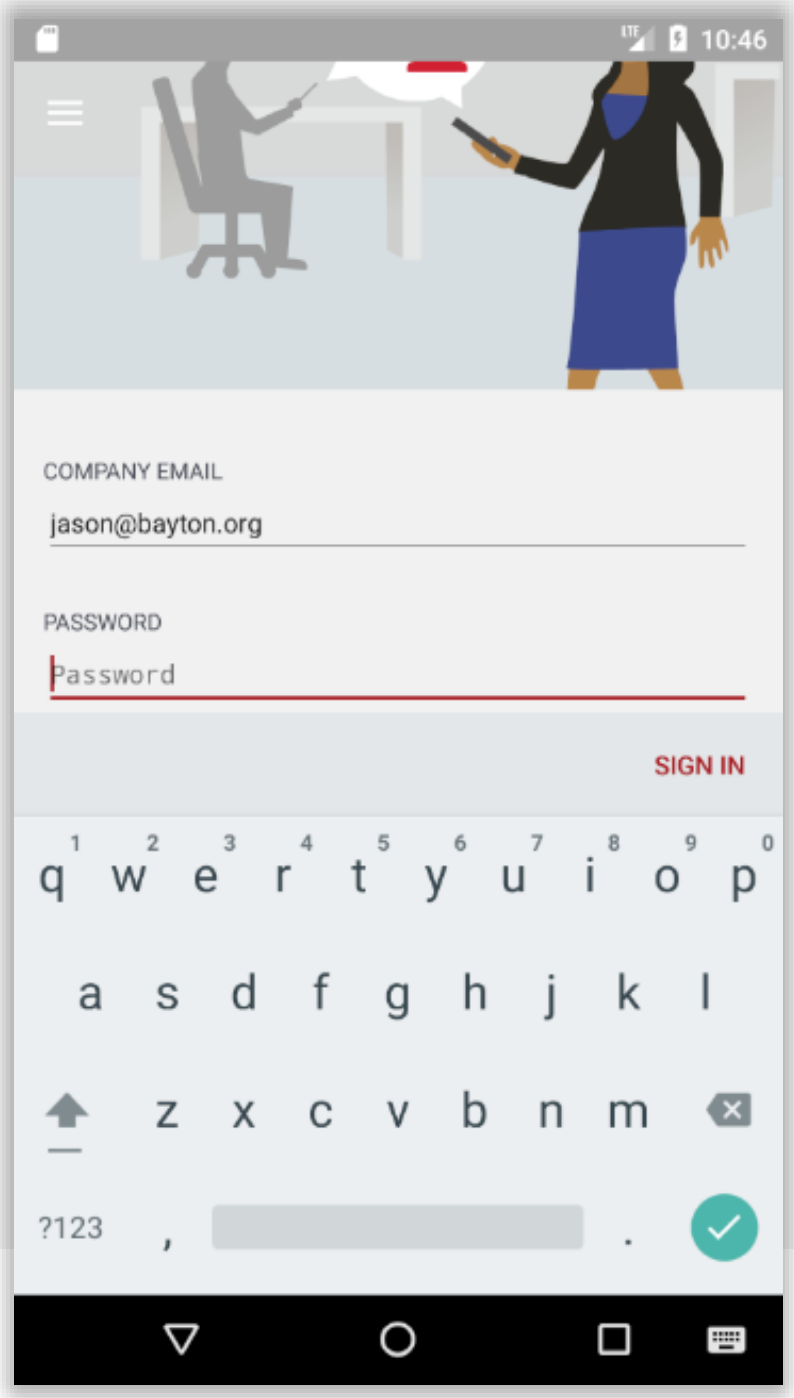
Accept the privacy alert by tapping **CONTINUE**.



Continue enrolment

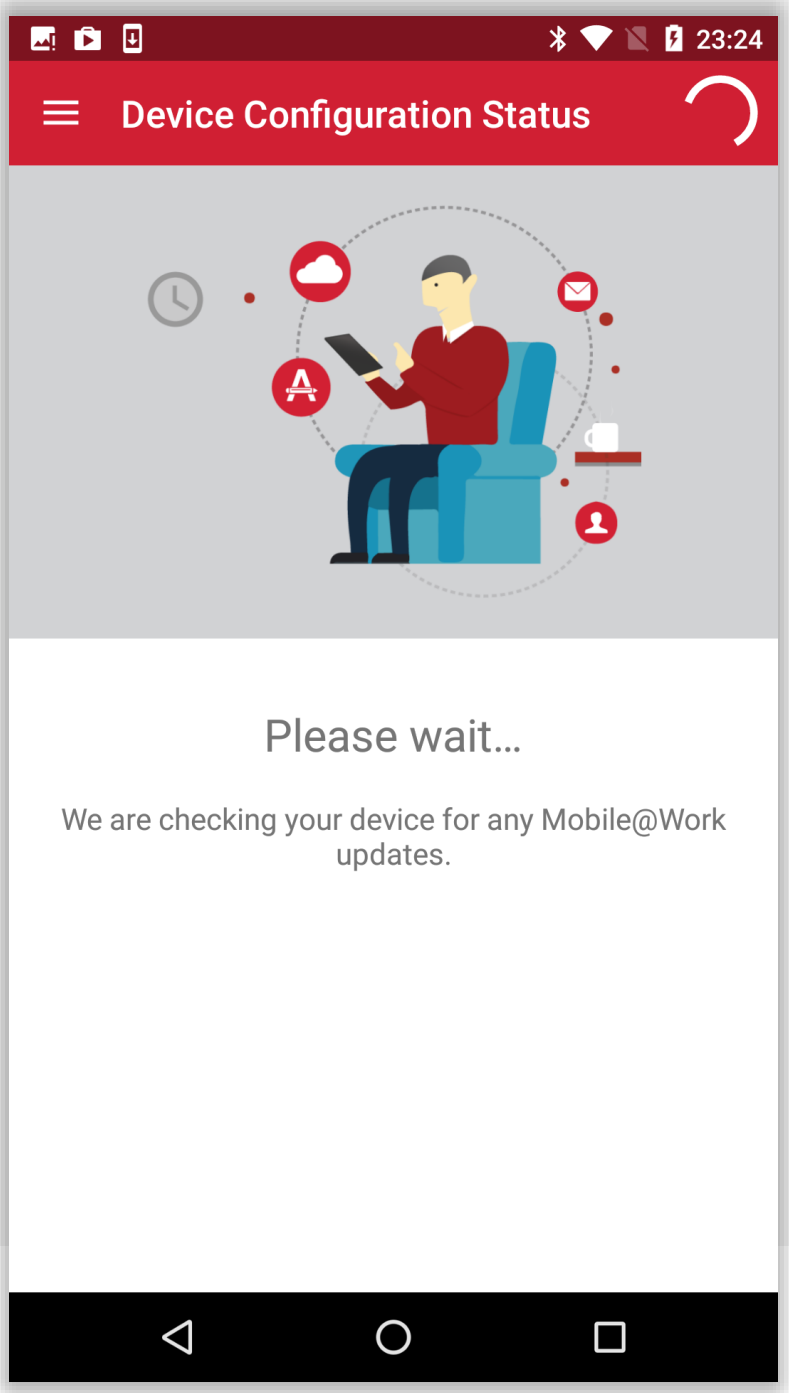
When your account has been found and validated, you'll be prompted for your password, PIN or both.

Enter the required fields and tap SIGN IN.



Device configuration

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



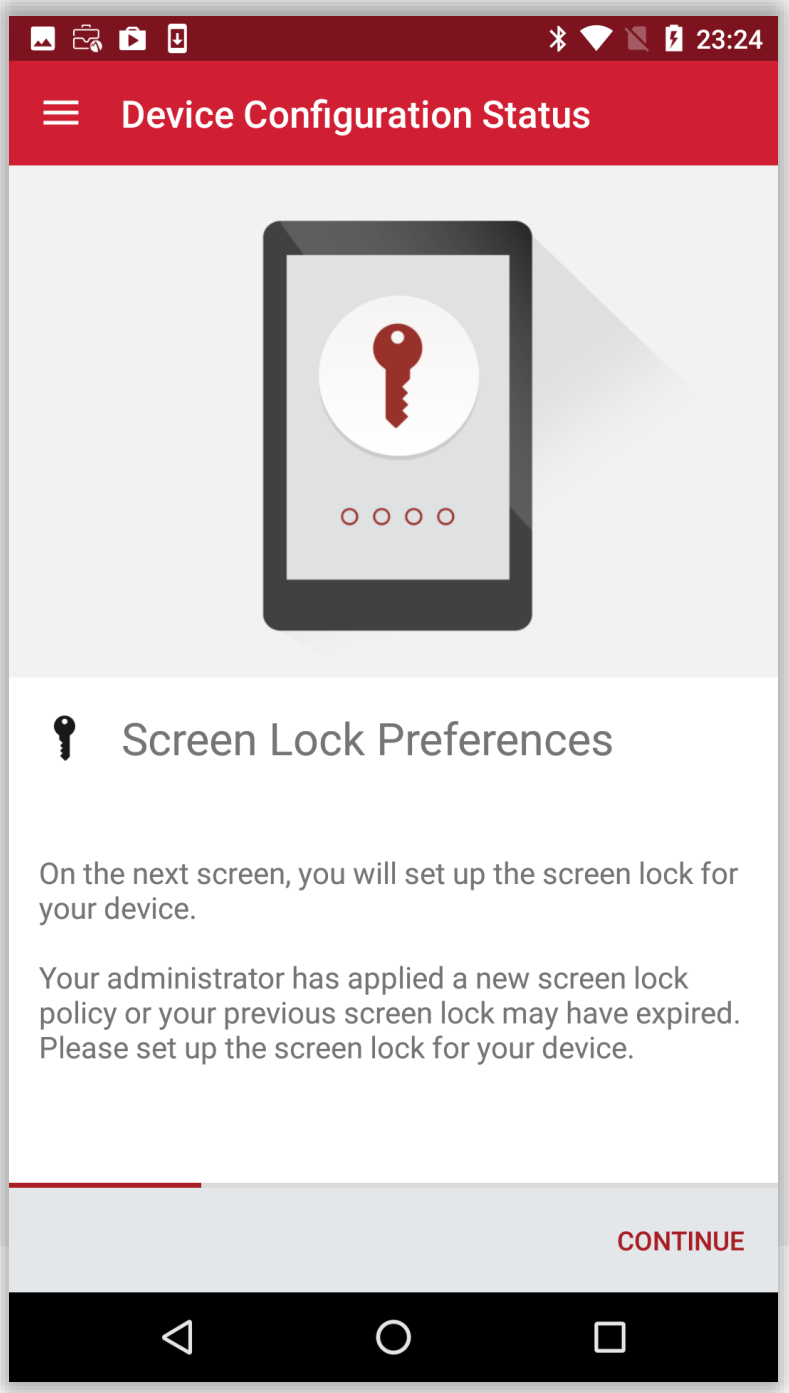
bayton

Device configuration

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.

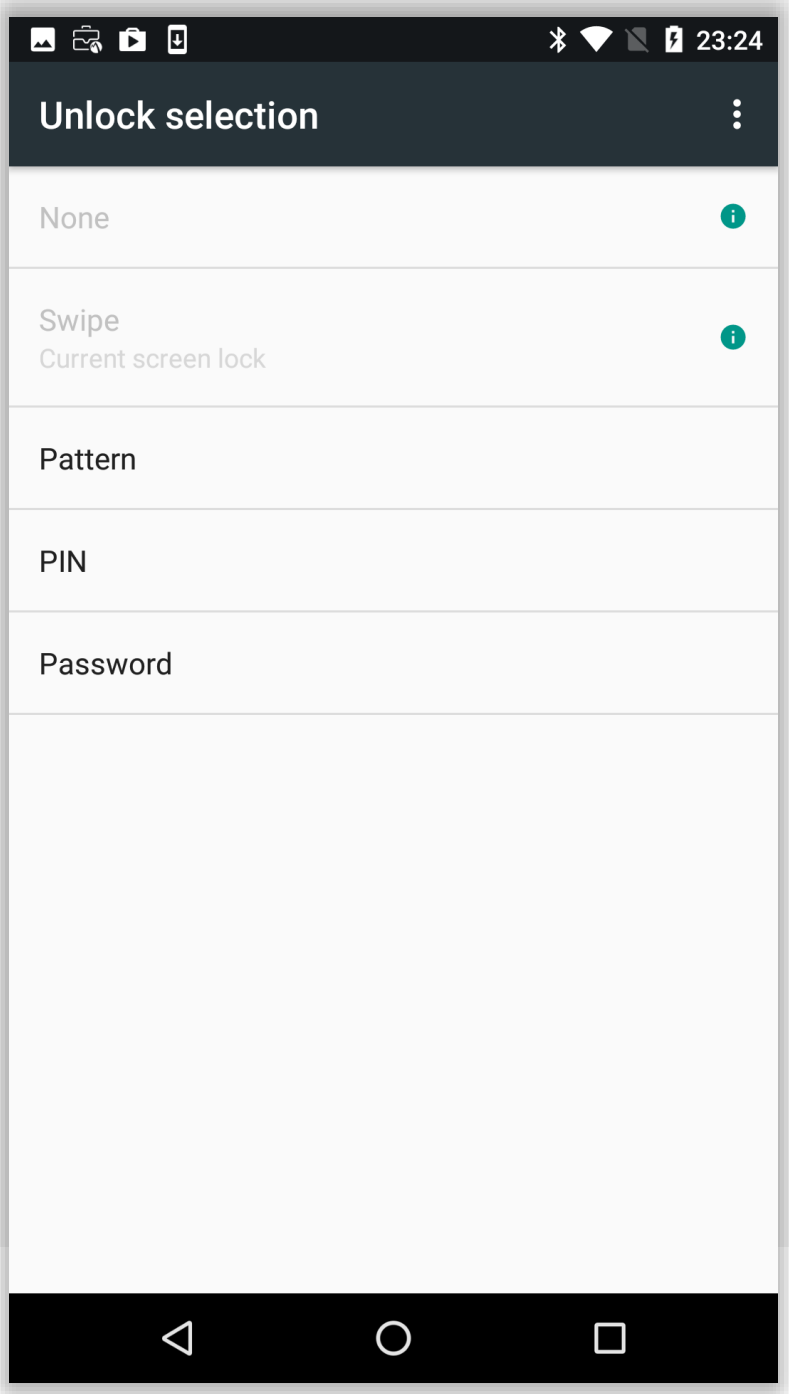
Tap **CONTINUE**.



bayton

Device configuration

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

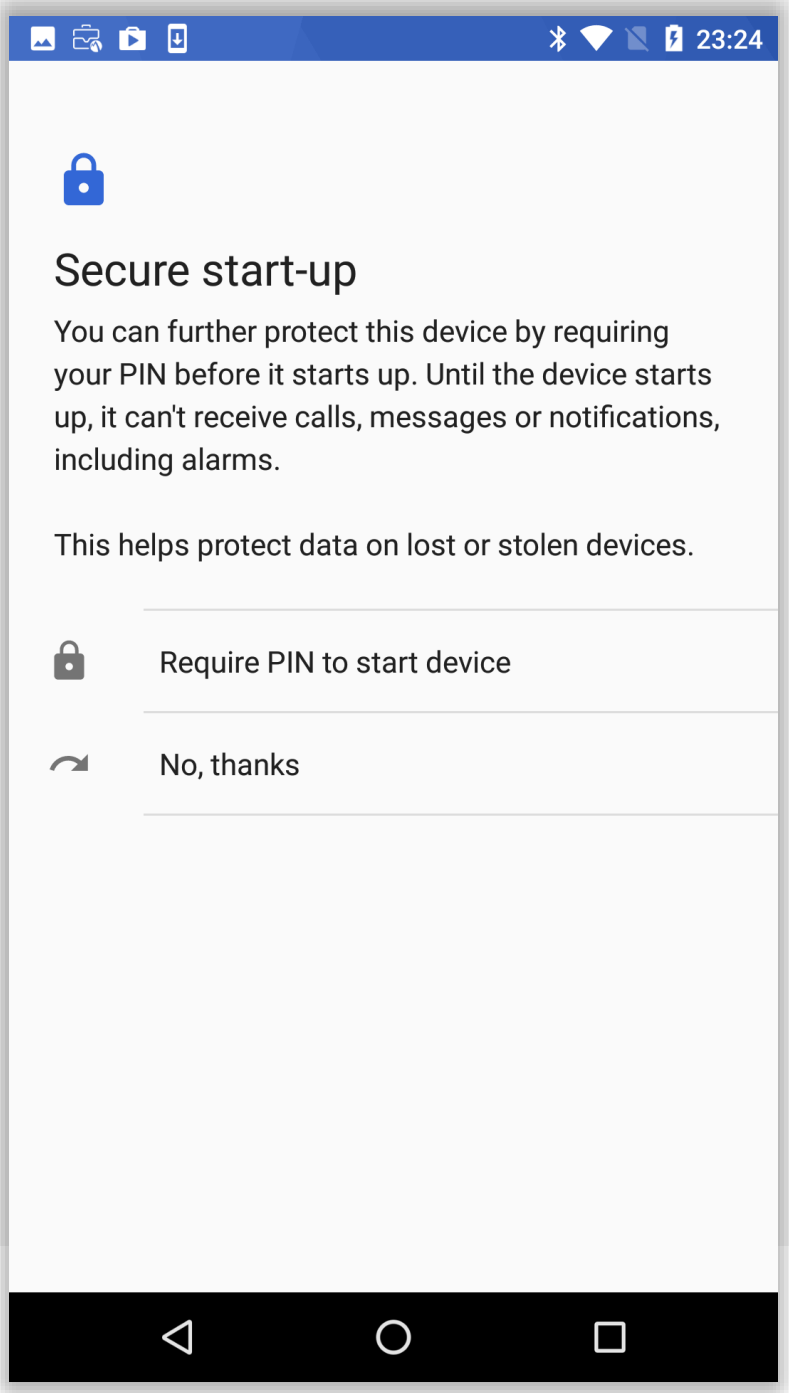


bayton

Device configuration

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

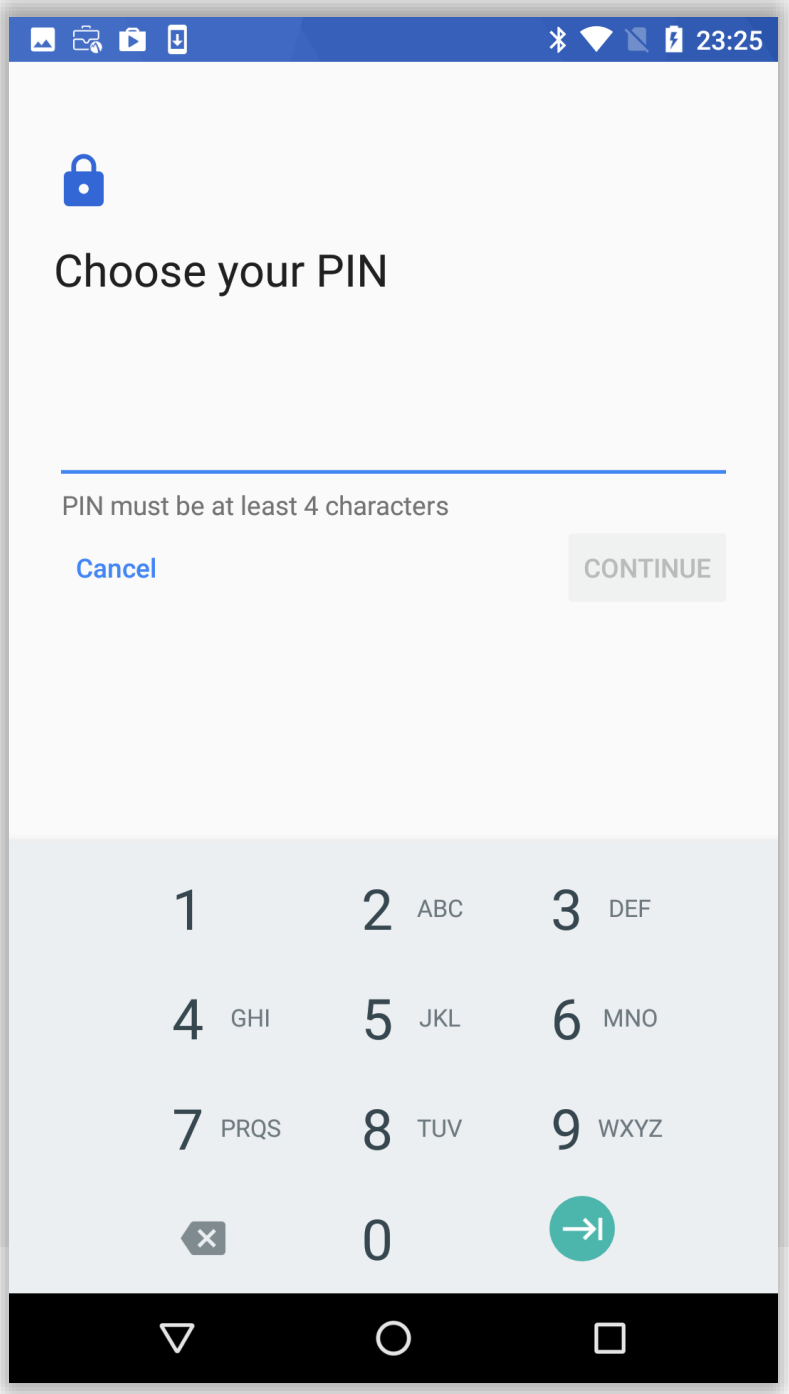
While it is more secure to require the passcode on device boot, it will result in a longer boot process.



bayton

Device configuration

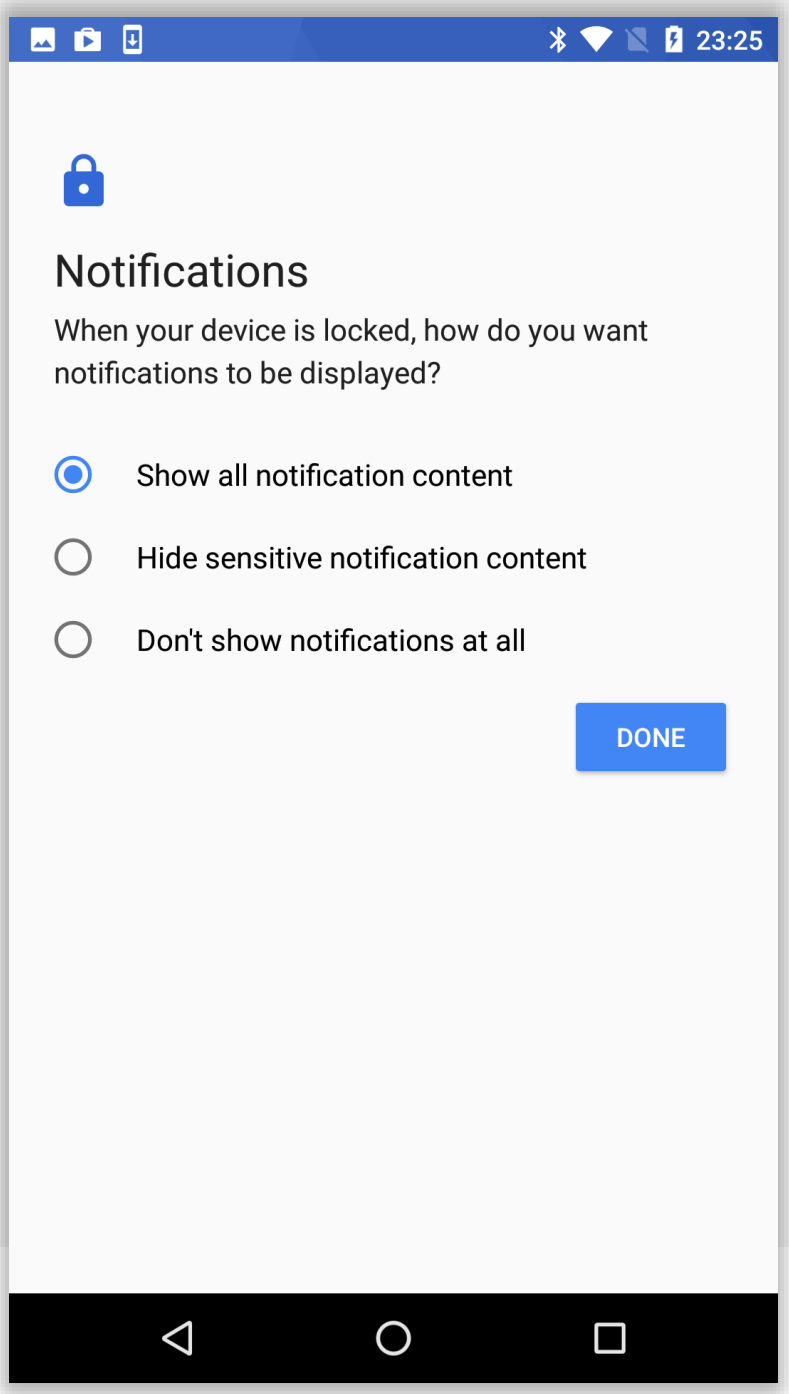
Input a PIN (or other passcode type) and tap **CONTINUE**.
Repeat to confirm.



bayton

Device configuration

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

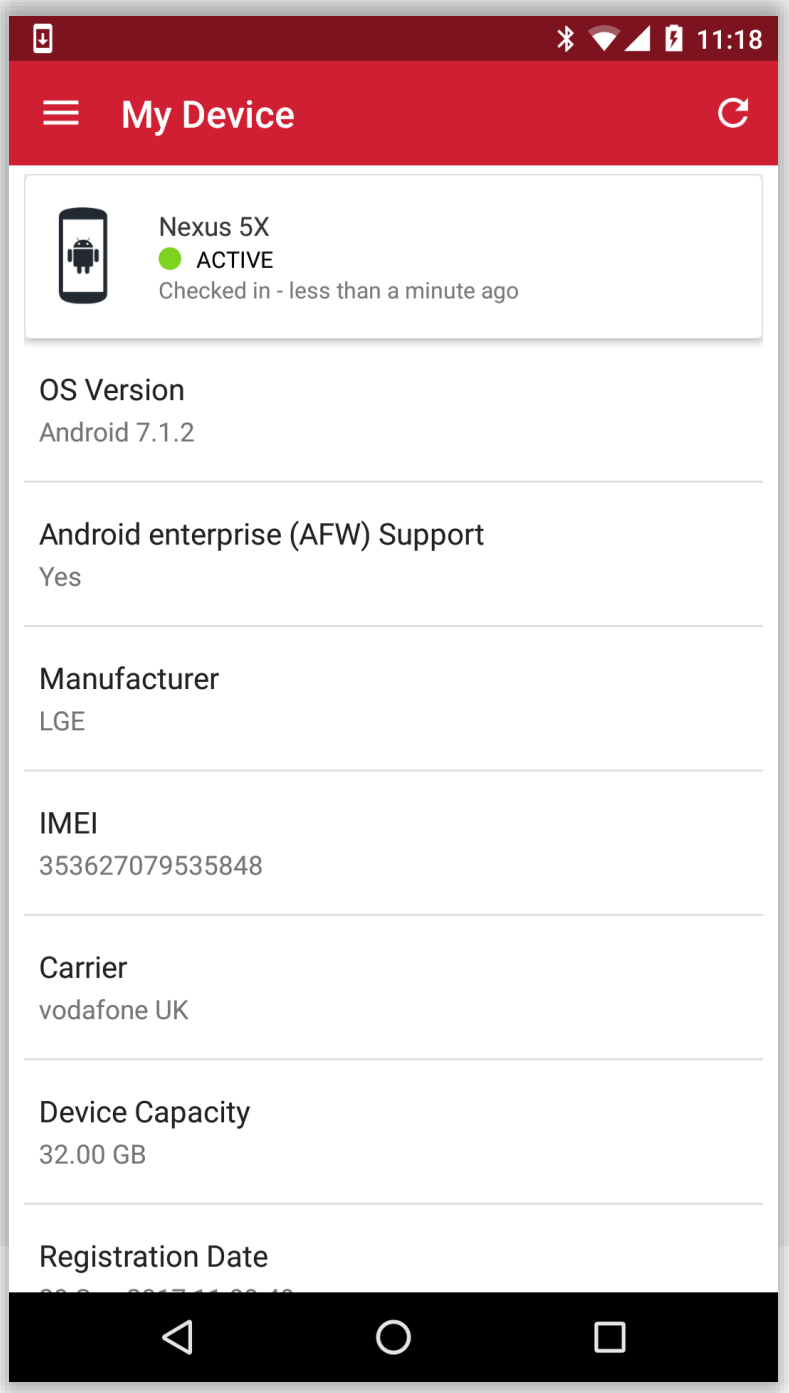


bayton

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