



Mobile Device Management

Installing Intune on a University owned Android device – OS 13

This document describes how to install Intune Mobile Device Management (MDM) on to:

- A new out of the box, University owned Android device (operating system 13), or
- An existing, wiped University owned Android device (operating system 13).

Before you start

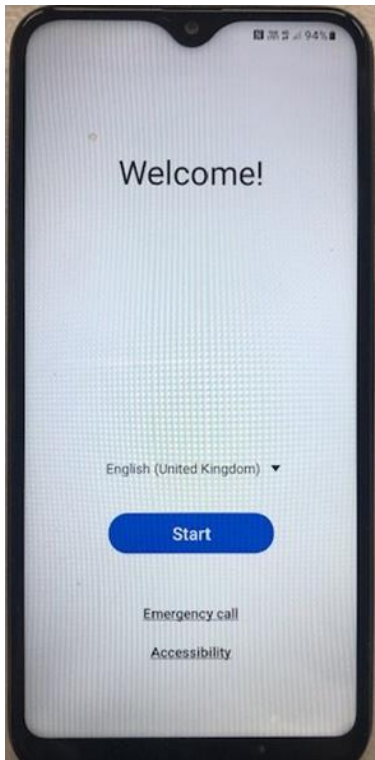
Before you start the installation process, please be aware of the following:

- You should ensure you have **Multi-Factor Authentication** set up, on a separate device before you install Intune – find out more at: <https://staff.napier.ac.uk/services/cit/infosecurity/Pages/Multi-Factor-Authentication.aspx>
- The Android device **must be wiped or new**, fresh out of the box.
- Your experience **may differ slightly depending on the Android** version and device vendor. The example device in this guide is the Samsung Galaxy but the procedure will be comparable with other Android devices.
- This method is for enrolling Android Devices into Intune as a **full Corporate controlled device**. No personal modifications are allowed, and only Edinburgh Napier approved apps and policies are available.
- This method requires the use of a **QR code reader**. Android 9 and newer devices have a QR reader installed. Android 7 and 8 devices will be prompted to install a QR reader.
- Ensure you are connected to a **Wi-Fi network, e.g. eduroam**.

Installation procedure

To install Intune MDM on to a new or wiped Android device:

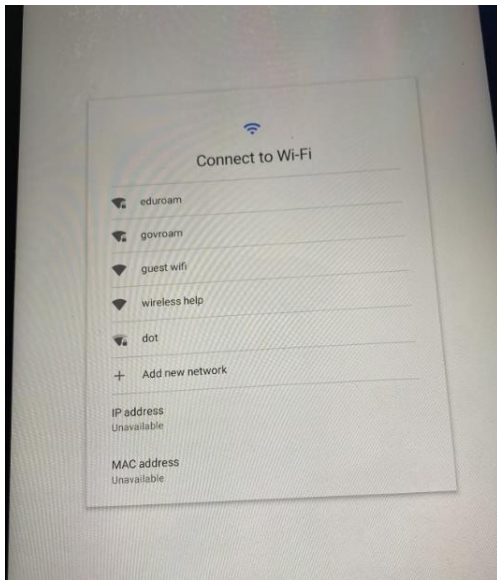
- **Switch on** the device and you'll see a white screen saying "Welcome", or "Let's Go":



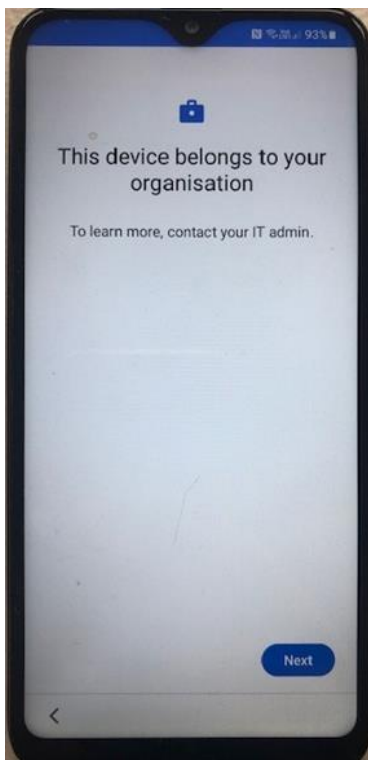
- **Tap 5 times** on the screen of the device. You should see a pop up displaying "**Tap 5 more times to open QR code scan**". Tap the device 5 more times and you should be prompted to scan a QR code.
- Point the camera to the **QR code** below, and tap on it to scan it:



- Once The QR code has been scanned, you will need to sign into and connect to a Wi-Fi network, if on campus this would be eduroam.



- To connect to eduroam, tap **eduroam** and enter your details as follows:
 - EAP method, select **PEAP**
 - Phase-2 authentication, select **MSCHAPV2**
 - CA certificate, select **Use System Certificates**
 - Domain, enter **napier.ac.uk**
 - Identity, enter StaffNumber@napier.ac.uk
 - Anonymous Identity, leave blank
 - Password, enter your **University password**
- Click **Connect**.
- You will see a “This device belongs to your organisation” screen, click **Next**:



- On the “Set up your phone” screen, read the guidance and select **Accept & continue**.

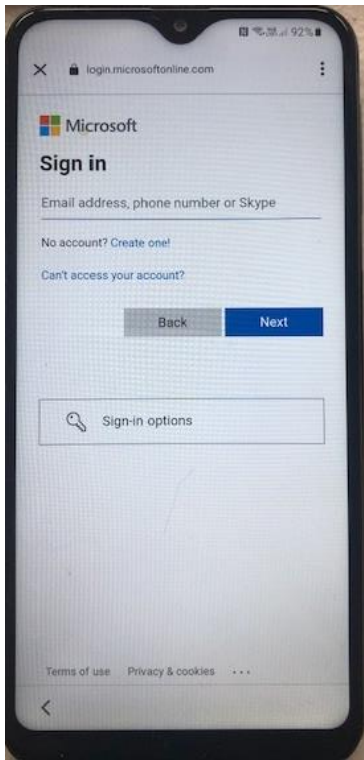
- You'll see a "This device isn't private message", click **Next**.



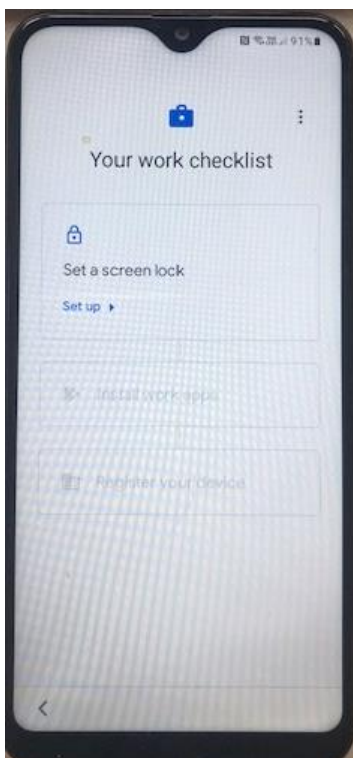
- The "Updating device" splash screen will appear, and you'll see the "Welcome to Chrome" screen. Select **Accept & Continue**:



- You'll be prompted to sign in. Enter your **Edinburgh Napier email** address and click **Next**:



- Choose **Work or school account**, click **Next**.
- Enter your University **password** and click **Sign in**.
- You may be prompted to **verify your identify** for Multi-Factor Authentication (MFA). If so enter the **verification code** in the space provided and click **Verify**.
- The **“Your work checklist”** screen will open.



- Set up the **Screen Lock** - then create a PIN (8 or more characters).
- Choose your **Notifications** options if prompted.
- Install the **Work apps** - the Authenticator and Intune apps are recommended. Some if not all apps will install automatically. Tap **Done** or **Next**.
- In the **Register Device** section click set up and the Intune sign in screen will appear:



- Click sign in and sign in with your **Edinburgh Napier email** address and your University **password**.
- If prompted, **verify your identify** for Multi-Factor Authentication and on the “Help us keep your device secure” screen click **Register**.
- You will now need to **agree** to Intune's policy and the device will be enrolled into Intune. Click **Done**:



Using your MDM enrolled Android Device

To view the available installed **Corporate Apps**:

- **Swipe** with an upwards motion on the **Home** screen.

To view the device registration details in Intune:

- **Open** the **Intune** app.

To view the Edinburgh Napier approved apps available for installing onto the device:

- **Open** the **Play Store** app.

Further information

Further information about the MDM service can be found on the staff intranet:

<https://staff.napier.ac.uk/services/cit/telecommunications/Mobile/Pages/Mobile-Device-Management.aspx>

If you have any queries, please contact the IS Service Desk in the first instance. Contact details can be found on the staff intranet:

<https://staff.napier.ac.uk/services/cit/ContactUs/Pages/ContactUs.aspx>