


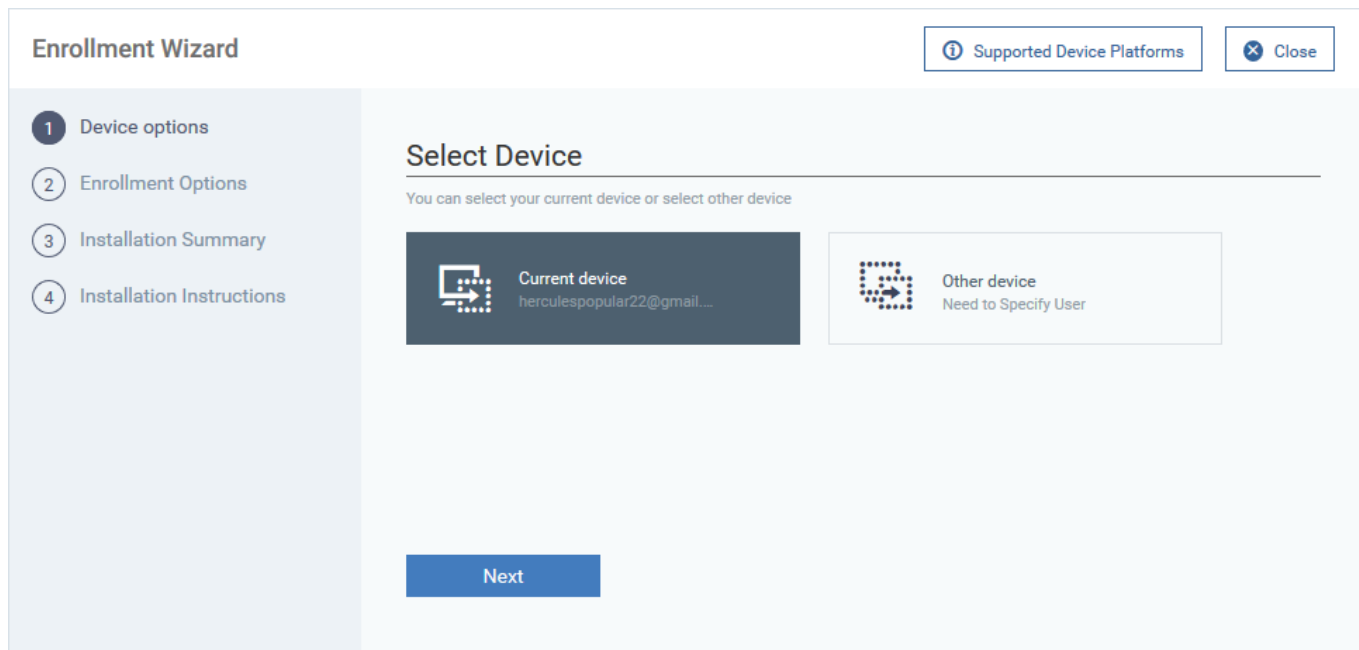
- This article explains how to add Android devices to Endpoint Manager.
- Once added, you can deploy profiles to manage device security, network access rights, browser restrictions and more.
- **Note** – You need to add users (device owners) before you can enroll their devices. Please see one of the following tutorials if you have not yet added users:
 - [Add users manually](#)
 - [Bulk import users from a .csv file](#)
 - [Bulk import users from Active Directory](#)
- Make sure target Android devices are connected to the internet and have enough space to install the Endpoint Manager app.
- Enrollment involves the following steps:
 - [Enroll user devices to Endpoint Manager](#)
 - [Install and configure the client](#)

Enroll user devices to Endpoint Manager

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Users' > 'User List' on the left
- Select the users whose devices you want to add
- Click the 'Enroll Device' button
- OR
- Click the 'Add' button  then select 'Enroll Device'.

The device enrollment wizard starts:

Step 1 – Device Options



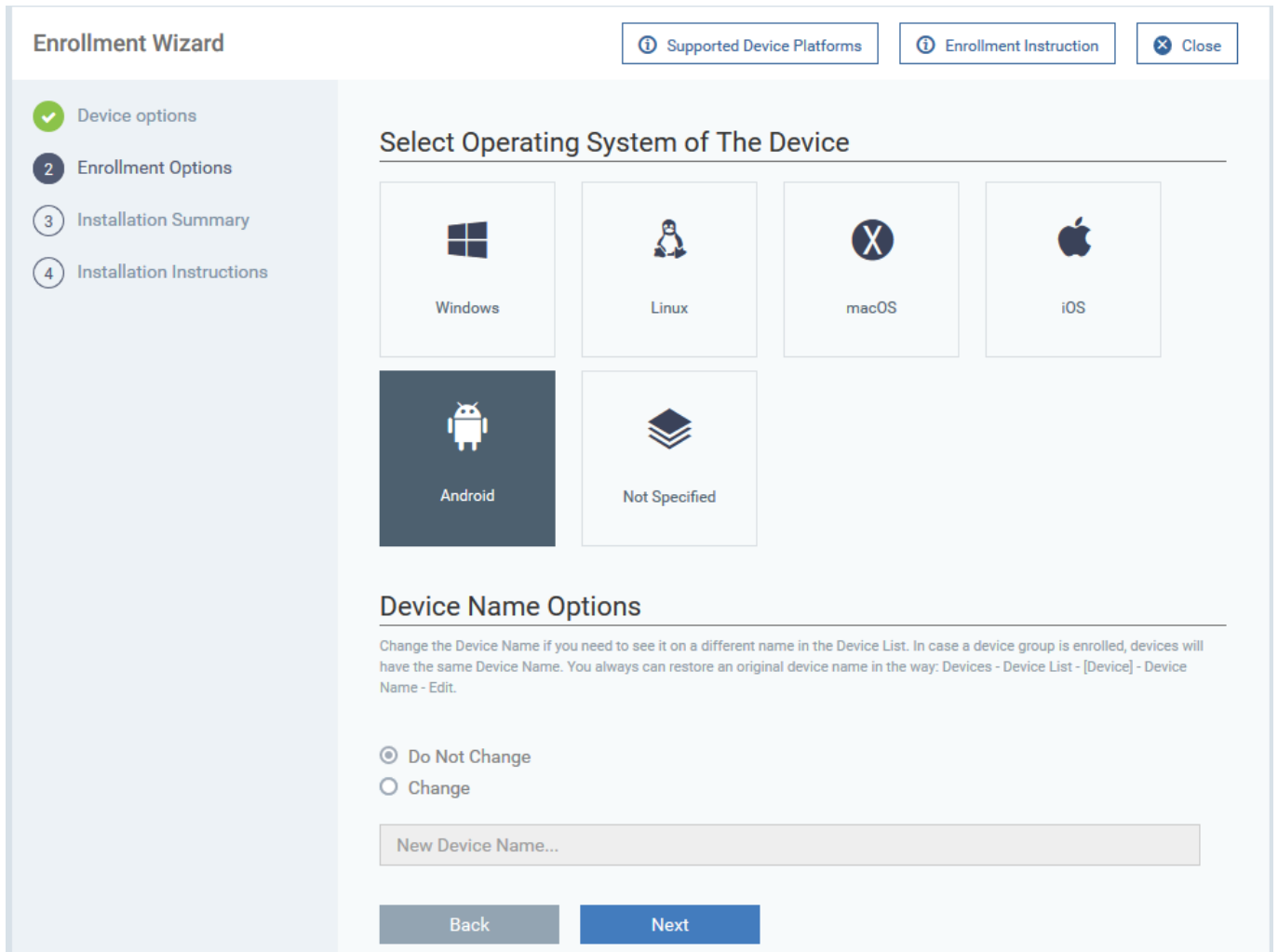
Select Device

- Choose 'Other device'

Specify User

- Any users you selected previously are listed in the 'Specify User' box
- You can add additional, existing users by simply typing their email address in the box. Endpoint Manager will auto-suggest users that have already been created.
- **Create New User** – Click if you want to add a new user to Endpoint Manager. You cannot add devices unless you have first added the users that own them. The add-user process is explained [here](#).
- Click 'Next' to proceed to step 2.

Step 2 – Enrollment options:



- **Select Operating System of the Device**

- Choose 'Android'

- **Device Name Options**

- **Do Not Change** - The device's existing name is used to identify it in Endpoint Manager
- **Change** - Enter a new device name.

Click 'Next' to proceed to step 3

Step 3 - Installation Summary

- Review your choices so far:

Enrollment Wizard

Supported Device Platforms | Enrollment Instruction | Close

Device options
Enrollment Options
3 Installation Summary
4 Installation Instructions

Device Information

Change Configuration

Operating system
Android

Device Name
Do Not Change

Back | Next

- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4

Step 4 - Installation Instructions

The final step is to send the enrollment emails to the device owners:

Enrollment Wizard

Supported Device Platforms | Enrollment Instruction | Close

Device options
Enrollment Options
Installation Summary
4 Installation Instructions

Enrollment Link

To complete the user device enrollment, copy and send this link to user.

`https://frontfork-msp.dmdemo.comodo.com/enroll/device/by/token/a084d9c8cc986f5e82d78t`

Send To Email

What's next?

Enroll Another Device | Go to Bulk Installation Package

Back | Finish

- **Send To Email** - Click this to send enrollment mails to users with the settings you choose in steps 1, 2 and 3.

Email Sent




Instruction email has been sent to selected user successful!

Ok

- Click 'Ok' to exit the wizard

An example email is shown below:

**Endpoint Manager**

Welcome to Endpoint Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux or Windows device into the Endpoint Manager system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete the enrollment process in a few short steps.

Note:

- Make sure that you selected the operating system of the device that you want to enroll. This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Device Enrollment:

[Click this link to enroll your device](#)

Sincerely, Endpoint Manager team.

Install and configure the client

- Users should open the enrollment mail on the device itself.

Enrollment involves two steps:

- [Step 1 - Download and Install the communication client](#)

- [Step 2 - Configure the client](#)

Step 1 - Download and Install the communication client

- Open the mail on the device you want to enroll
- Tap the link in the mail to start the enrollment wizard
- Touch the 'Get it on Google Play' button:



- Download and install the client software from Google Play

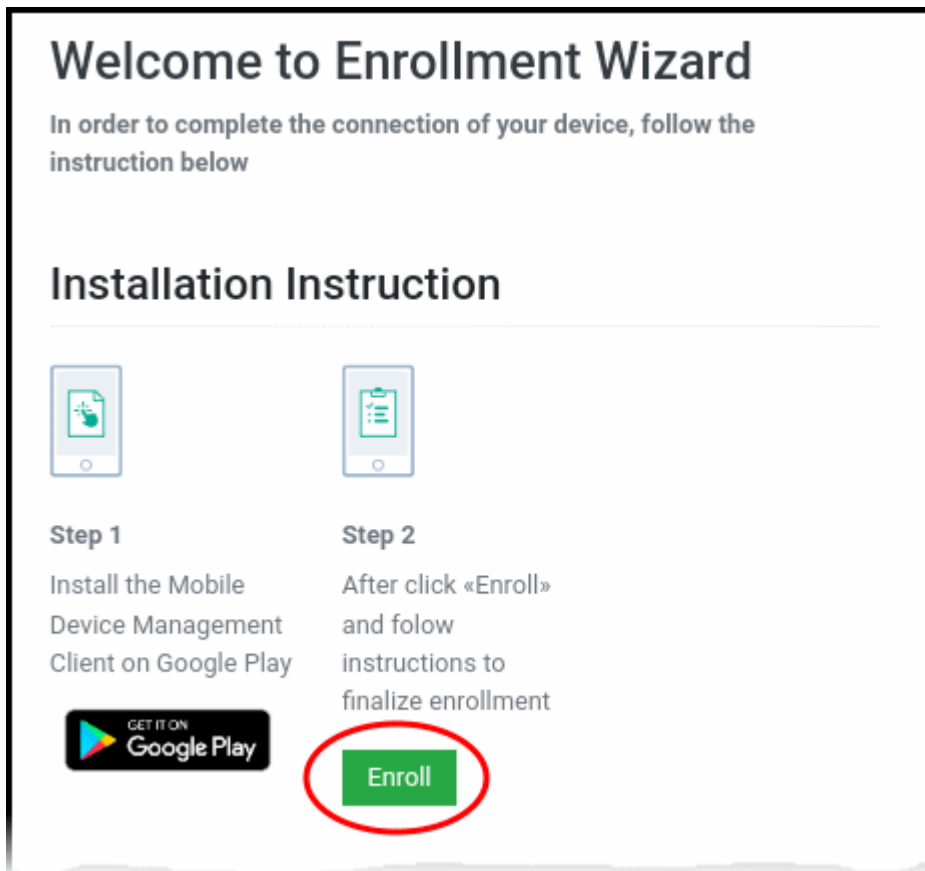
Step 2 - Configure the communication client

The next step is to configure the client to connect to Endpoint Manager. There are two ways to do this:

- [Automatic Configuration](#)
- [Manual Configuration](#)

Automatic Configuration

- After installation in step 1, go back to the device enrollment page and tap the 'Enroll' button under 'Step 2':

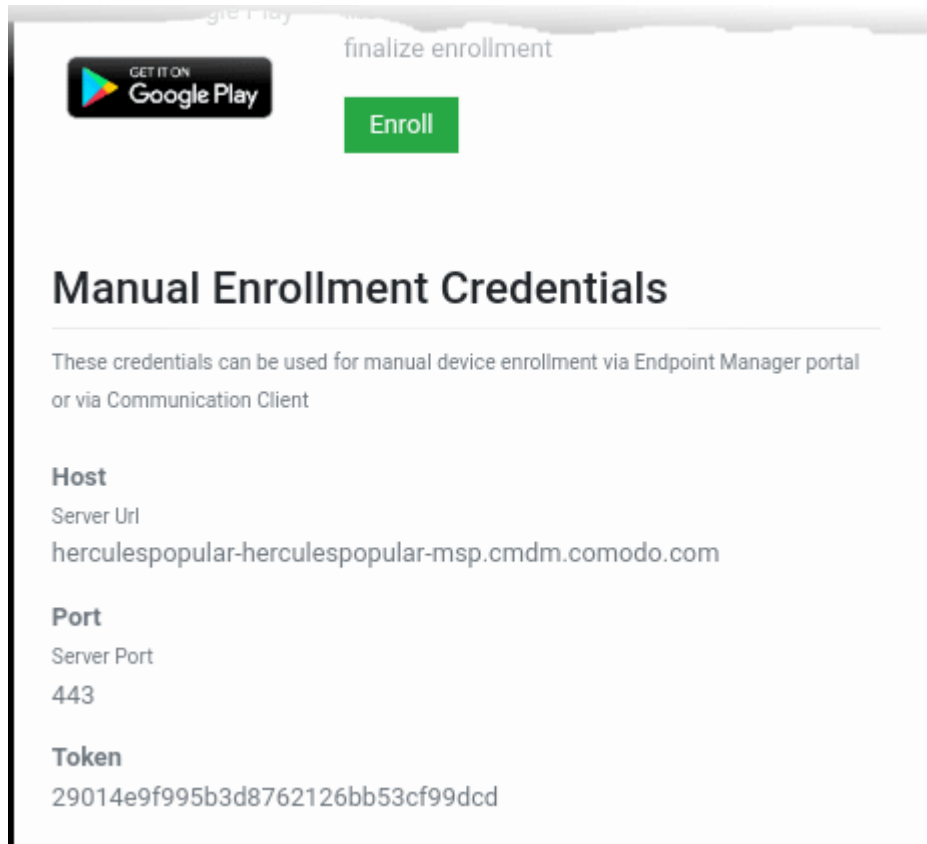


The client is automatically configured.

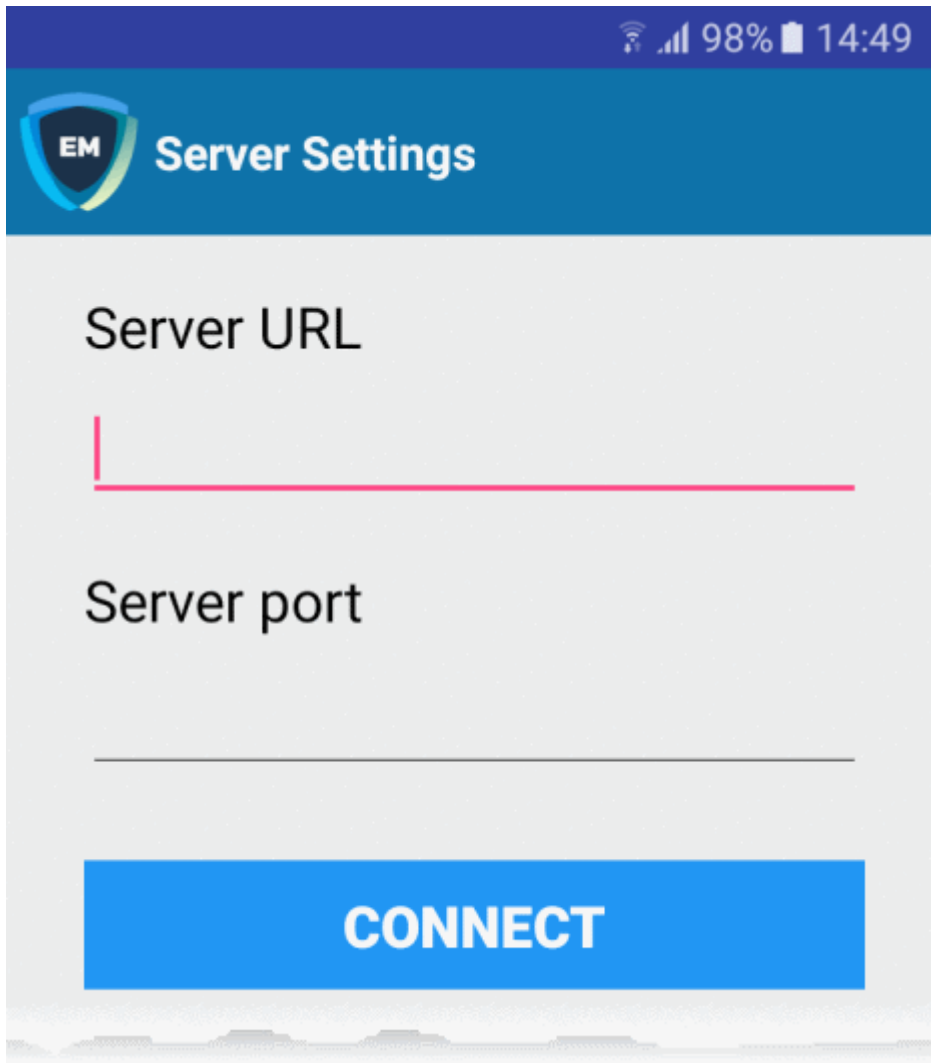
Users now skip to the EULA and [device activation screen](#).

Manual Configuration

Users can manually configure the communication client to connect to Endpoint Manager by entering the server settings and token string (aka PIN). You can find these items on the enrollment page:



- Open the client by tapping the client icon on your device.
- This starts the client configuration wizard. Enroll the device by entering the server settings and unique token:



- **Server URL** - The server URL is listed on the enrollment page as described above.
- **Server port** - The server port is also listed on the enrollment page. Default = 443.
- Hit the 'Connect' button to open the login screen.

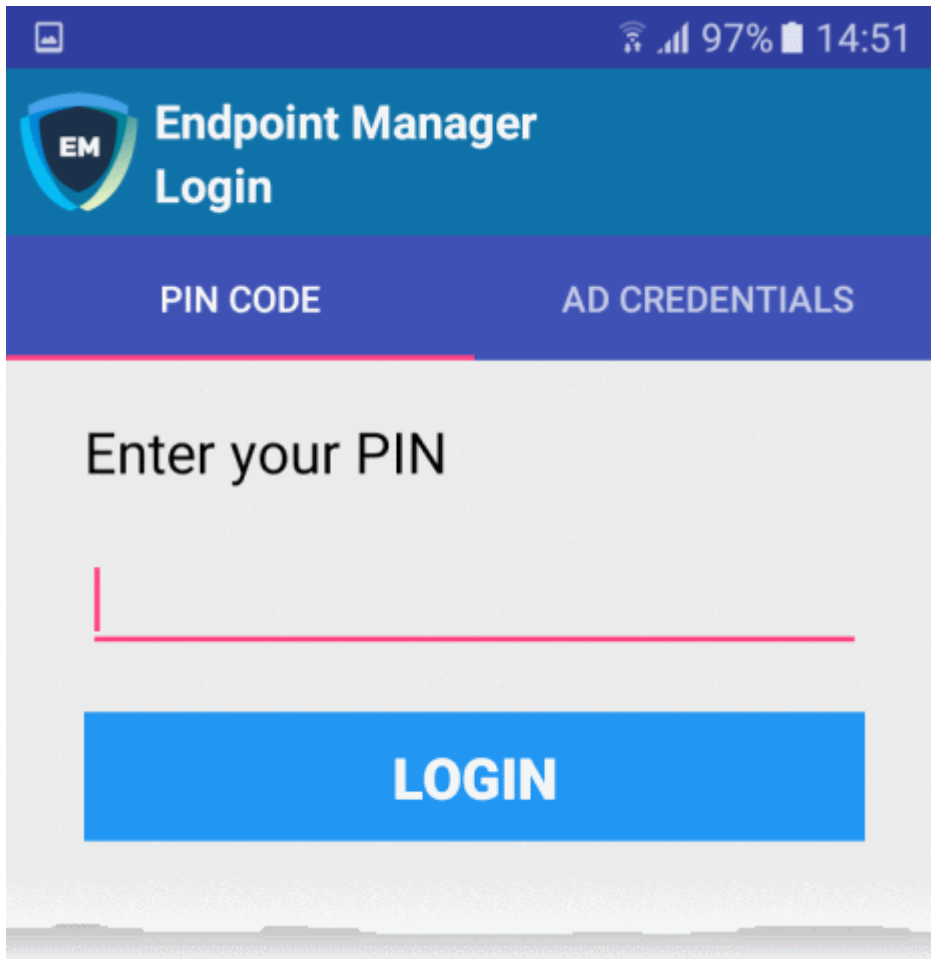
Login to the Console

There are two ways to login to the console:

- [Enter the token from the enrollment page in the 'PIN Code' tab](#)
- [Enter your domain username and password](#)

Enter the token from the enrollment page

- Open the communication client
- Open the 'Pin Code' tab:



- Enter the token from the enrollment page as the PIN
- Tap 'Login' then agree to the [EULA](#).

Domain username and password

- Open the communication client
- Open the 'AD Credentials' tab

Prerequisite: Enrollment of user devices using their Active Directory (AD) credentials requires:

- The AD server to be integrated with EM
- The users to be imported from AD to EM.
[Click here for on this process.](#)



Endpoint Manager Login

PIN CODE

AD CREDENTIALS

Login

Password

LOGIN

- Enter the username and password you use to login to your network domain.

- Tap the 'Login' button

End User License Agreement



ITARIAN END USER LICENSE AGREEMENT AND TERMS OF SERVICE

ENDPOINT MANAGER

THIS AGREEMENT CONTAINS A BINDING
ARBITRATION CLAUSE.

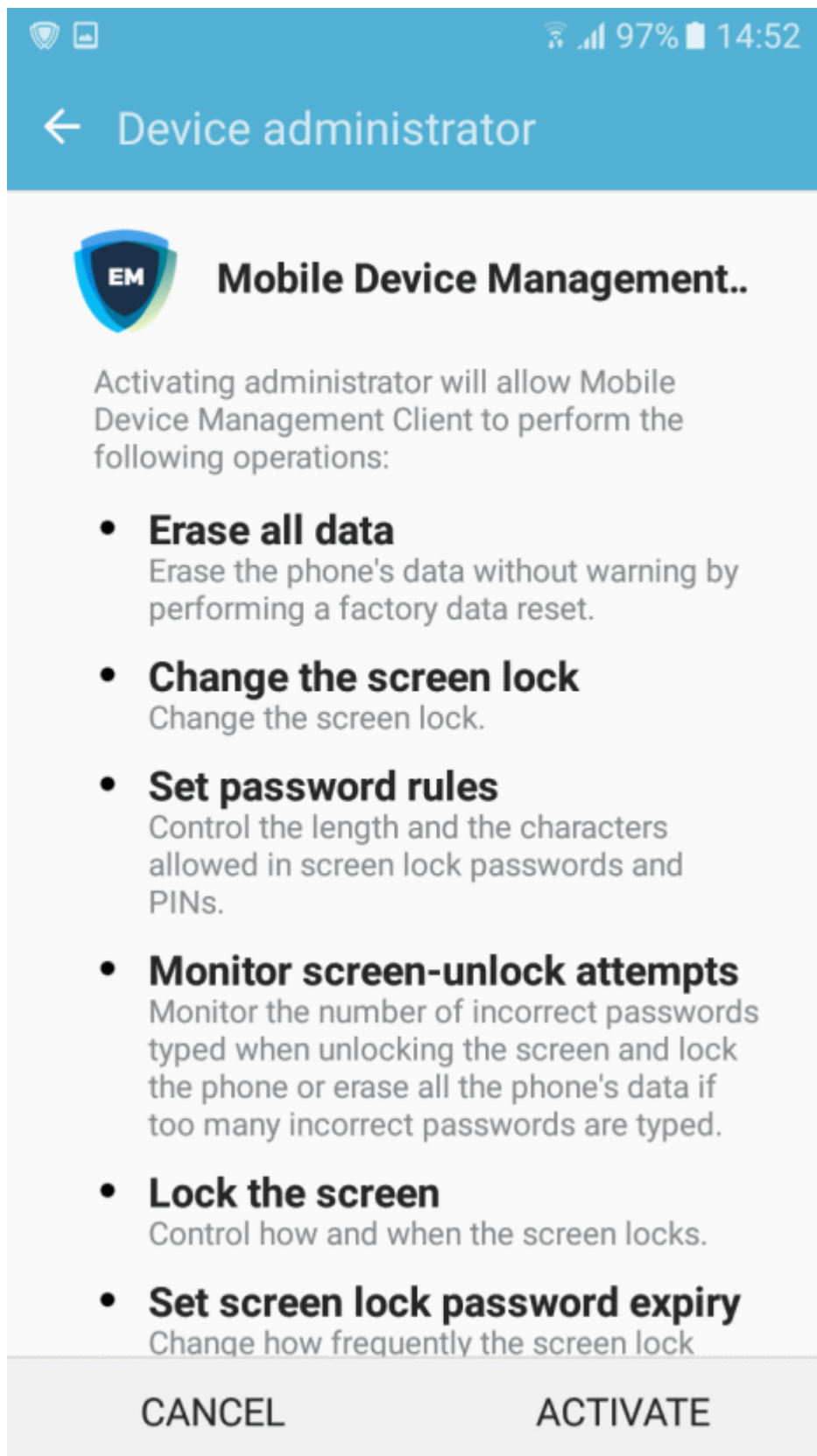
IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING ITARIAN ENDPOINT MANAGER (THE “PRODUCT”). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD OR ACCESSED OR INSTALLED WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON “I ACCEPT” BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND

I ACCEPT

DENY

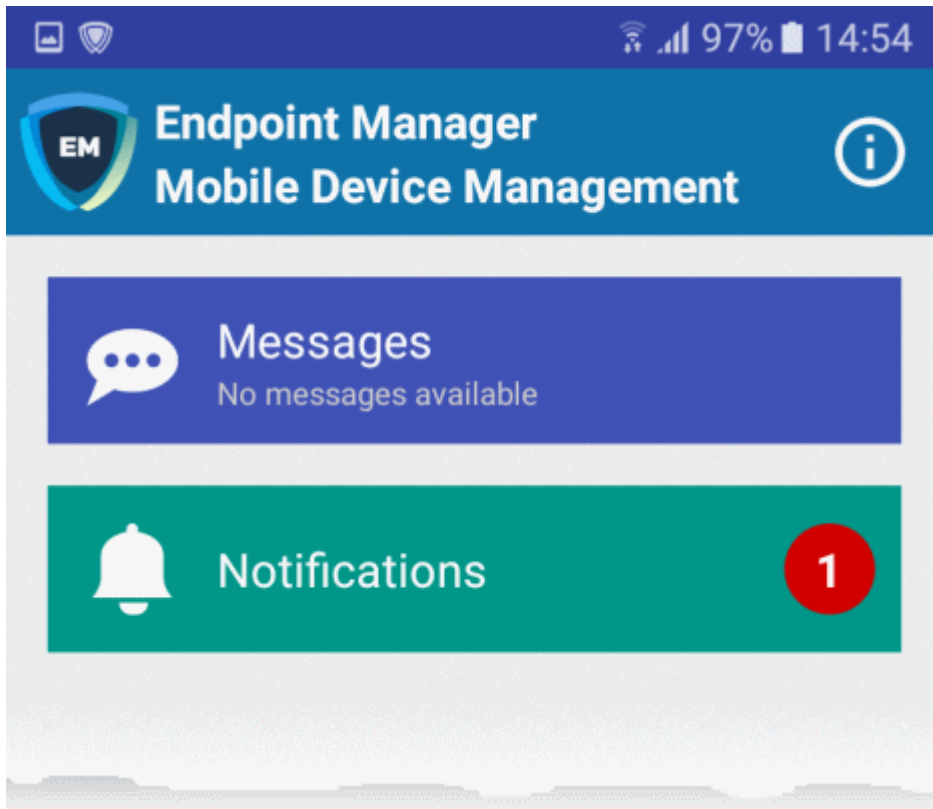
- Scroll down then click the 'I Accept' button

This starts the client activation screen. Activation requires the client is given some privileges:

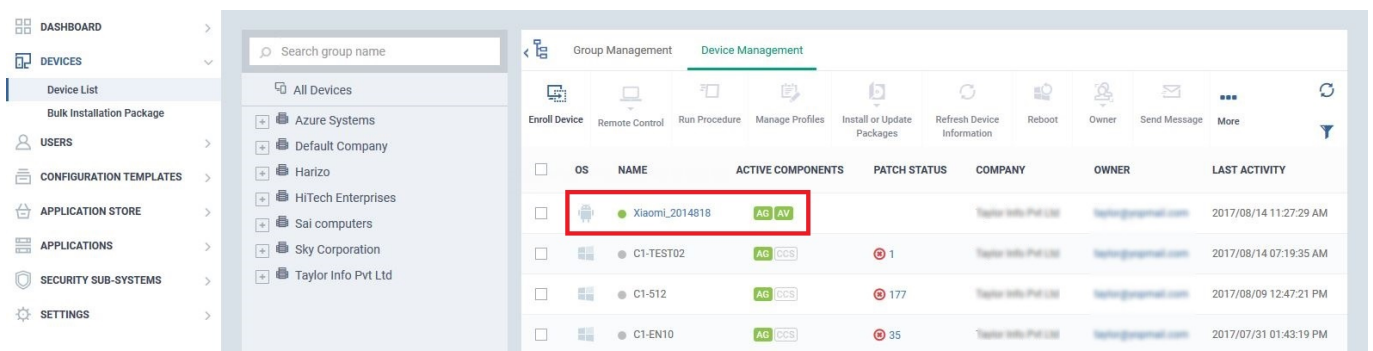


- Tap 'Activate'.

The communication client home screen opens:



The device is now enrolled to Endpoint Manager. All enrolled devices are shown in 'Devices' > 'Device List':



- You can now apply custom profiles to the devices if required. [Click here](#) to learn how to create and deploy a custom profile.