COMODO
Creating Trust Online®

Comodo
Endpoint Manager

Software Version 6.37

End User Guide

Guide Version 6.37.070120

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Introduction to Endpoint Manager....3
2. Enroll Your Device....3
2.1.Enroll Android Devices....5
2.2.Enroll iOS Devices....13
2.3.Enroll Windows Endpoints....17
2.4.Enroll Mac OS Devices....21
2.5.Enroll Linux OS Endpoints....24
3. Create a Support Ticket....26
4. Allow Remote Control Requests....28
5. Allow Remote Access Requests....28
About Comodo Security Solutions....30

1. Introduction to Endpoint Manager

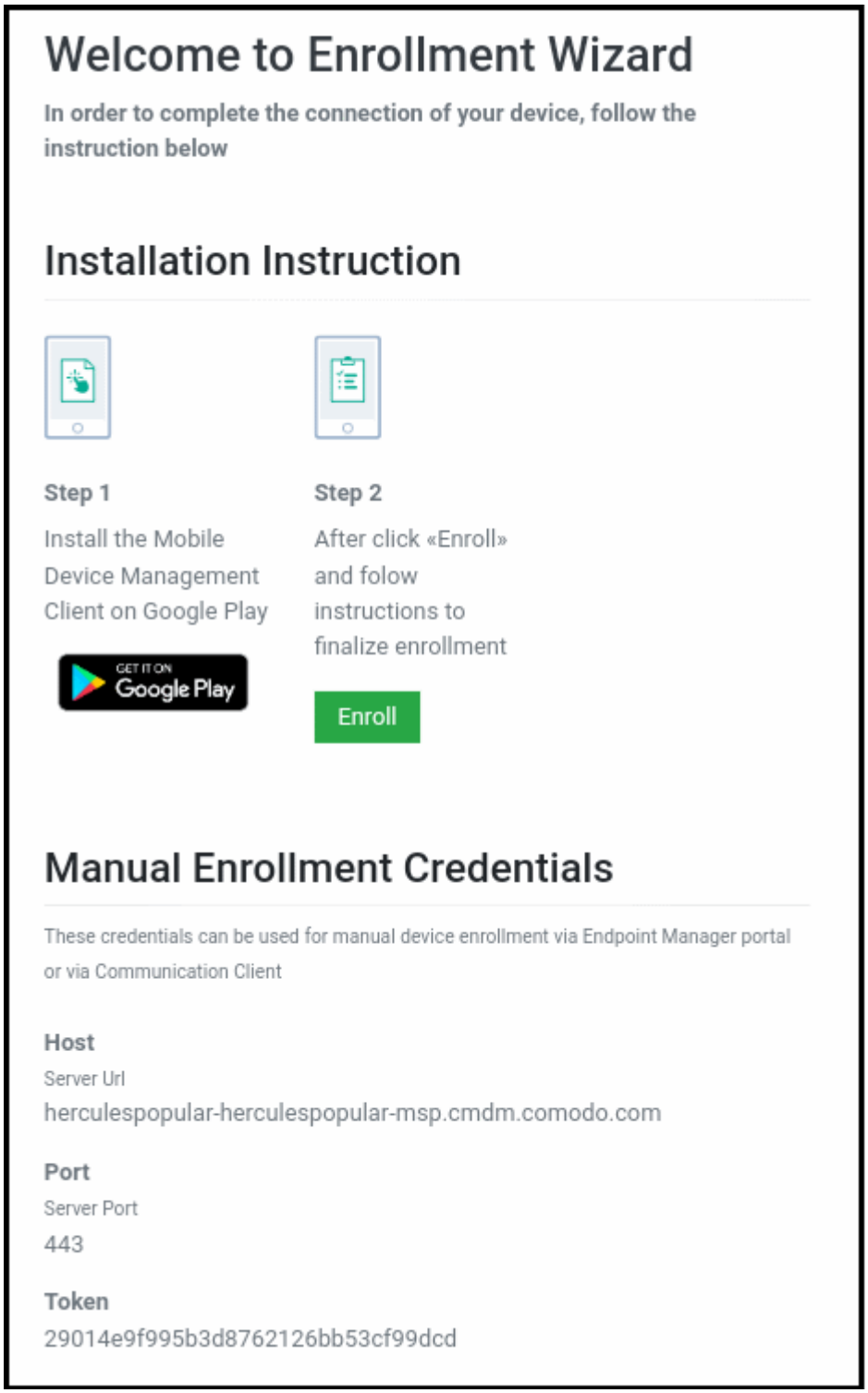
- Endpoint Manager (EM) is a centralized device management system that allows administrators to manage, monitor and secure devices which connect to enterprise networks.
- Once you have enrolled your Android, iOS, Windows, Mac OS or Linux device to EM, it will have a security policy applied to it which will authenticate it to your company network and protect it from malware.
- Endpoint Manager also allows you to create support tickets if you need assistance with issues on your Windows and Mac OS devices. Your support staff can even use EM to take remote control of a Windows or Mac OS computer to solve issues.

This guide explains how to enroll your device and create support tickets.

- **Enroll your Device**
  - **Android Devices**
  - **iOS Devices**
  - **Windows Devices**
  - **Mac OS Devices**
  - **Linux OS Devices**
- **Create a Support Ticket**
- **Allow Remote Control Requests**
- **Allow Remote Access Requests**

2. Enroll Your Device

- After your admin has added your device to Endpoint Manager, you will receive a device enrollment email.
- The mail contains a link to the software appropriate for your device. The software will connect your device to Endpoint Manager:



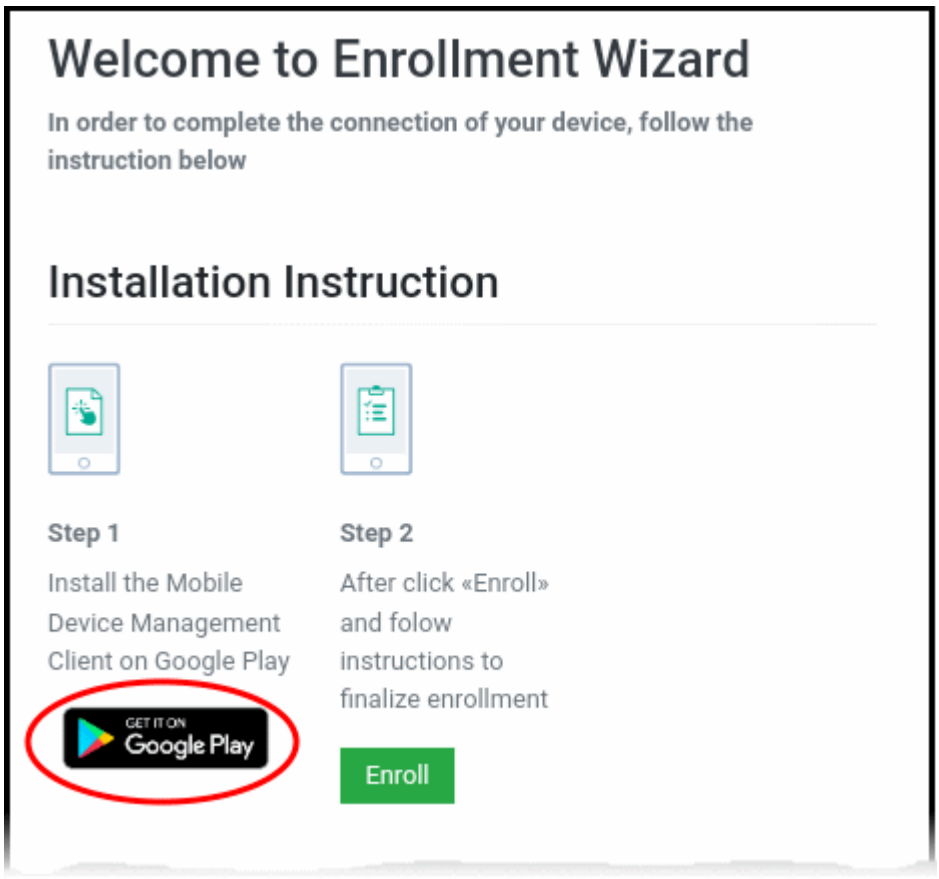
- You can use the same mail to enroll multiple devices. Please ensure you open the mail on the device you want to enroll.
- The following sections explain the enrollment process on different operating systems:
  - **Enroll Android Devices**
  - **Enroll iOS Devices**
  - **Enroll Windows Endpoints**
  - **Enroll Mac OS Devices**
  - **Enroll Linux OS Endpoints**

2.1. Enroll Android Devices

- There are two steps to enroll Android devices:
  - **Step 1 - Download and Install the communication client**
  - **Step 2 - Configure the client to enroll the device**

Step 1 - Download and Install the communication client

- Open the mail on the device you want to enroll
- Tap the 'Get it on Google Play' button:



- Download and install the client software from Google Play

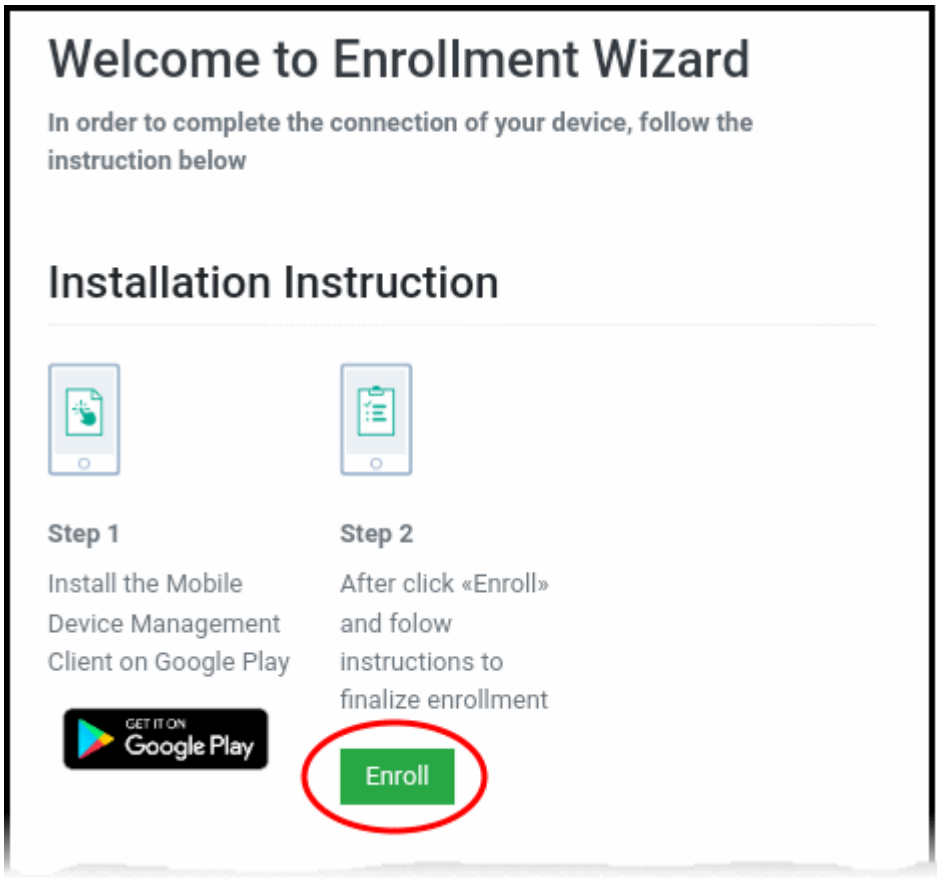
Step 2 - Configure the communication client

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

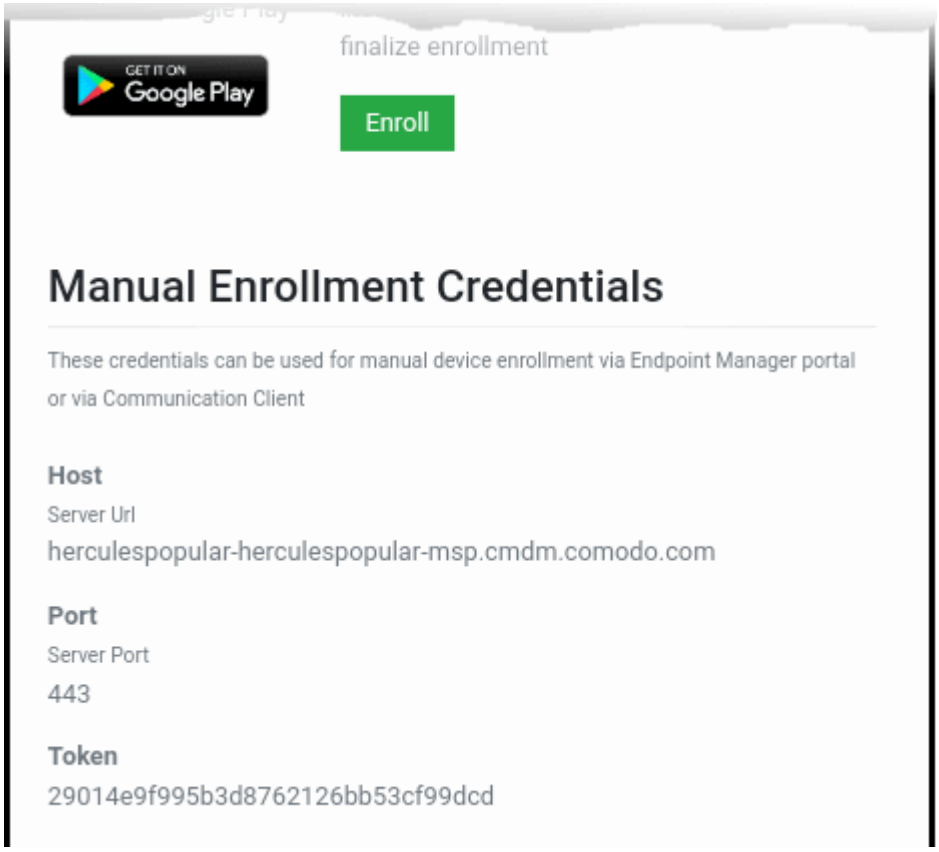
- After installation in step 1, go back to the device enrollment page and tap the 'Enroll' button under 'Step 2':



The client is automatically configured and the **End User License Agreement** screen appears.

Manual Configuration

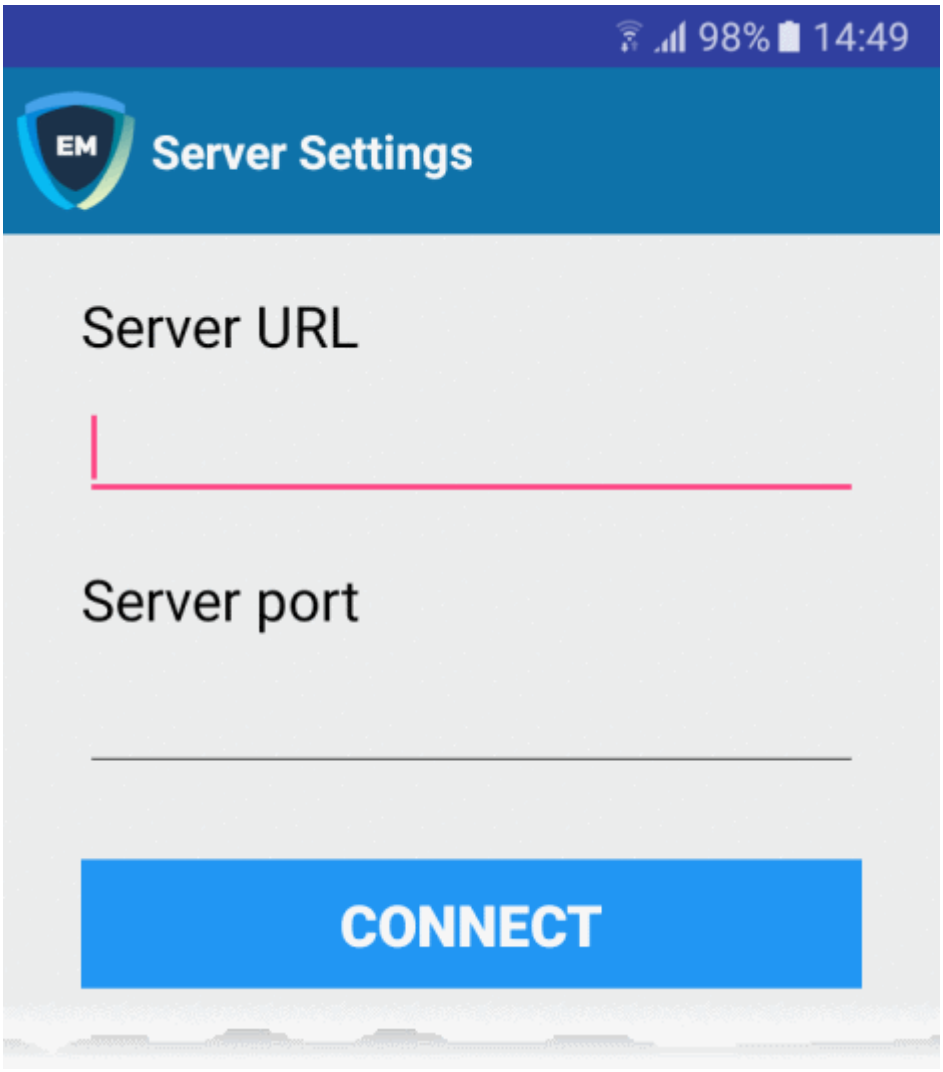
- You can manually configure the communication client to connect to Endpoint Manager by entering the server settings and token string (aka PIN). You can find these items on the enrollment page:



Manually configure the client

- 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 Settings



- **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.

- Tap the 'Connect' button. The 'Login' screen will open

Login to the Console

There are two ways to login to the console:

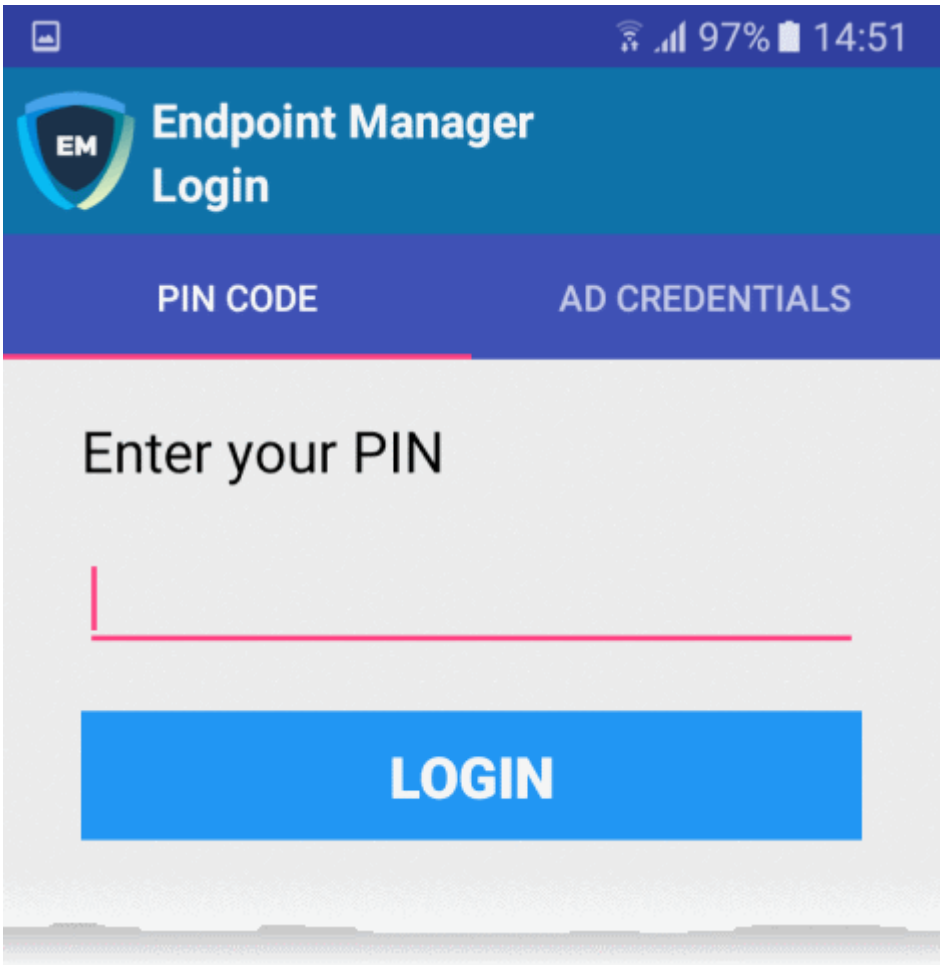
- **Enter the token from the enrollment page in the 'PIN Code' tab**

  OR

- **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**.

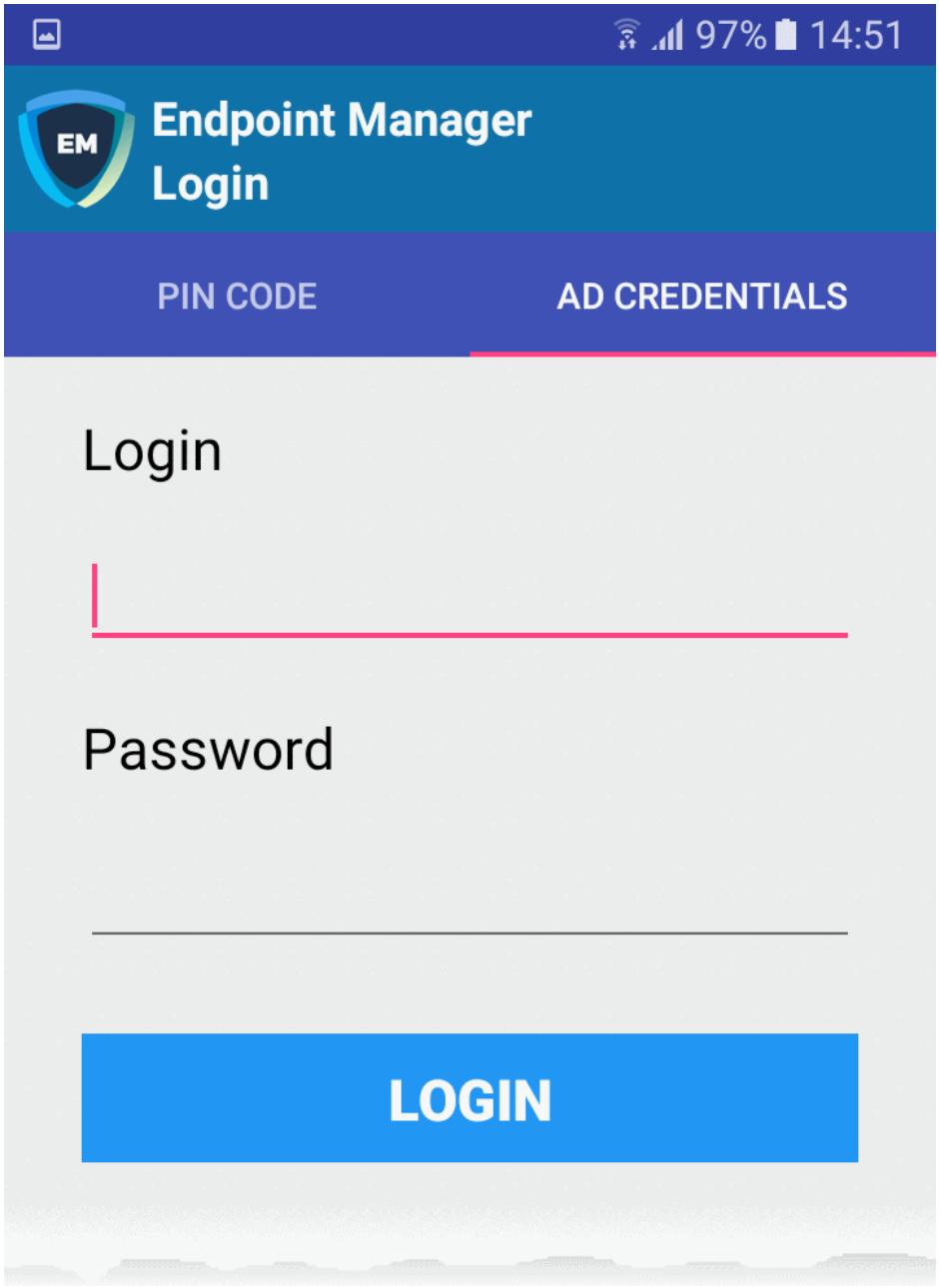
Domain username and password

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

Prerequisite: Please ensure the following to enroll your device using Active Directory:

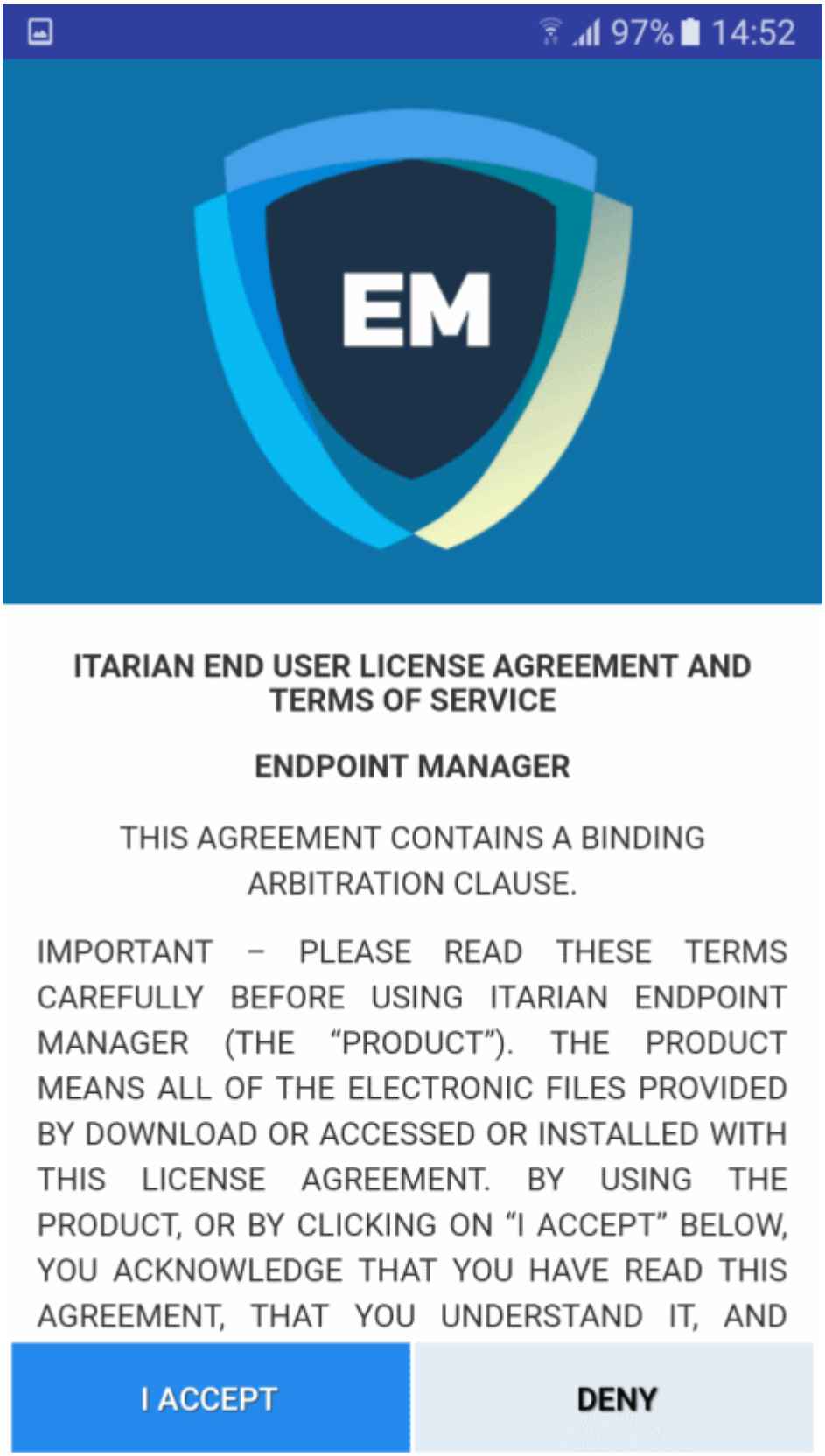
- Your network's AD server has been integrated with Endpoint Manager
- All users have been imported to Endpoint Manager from AD

Contact your administrator if you are having issues connecting.



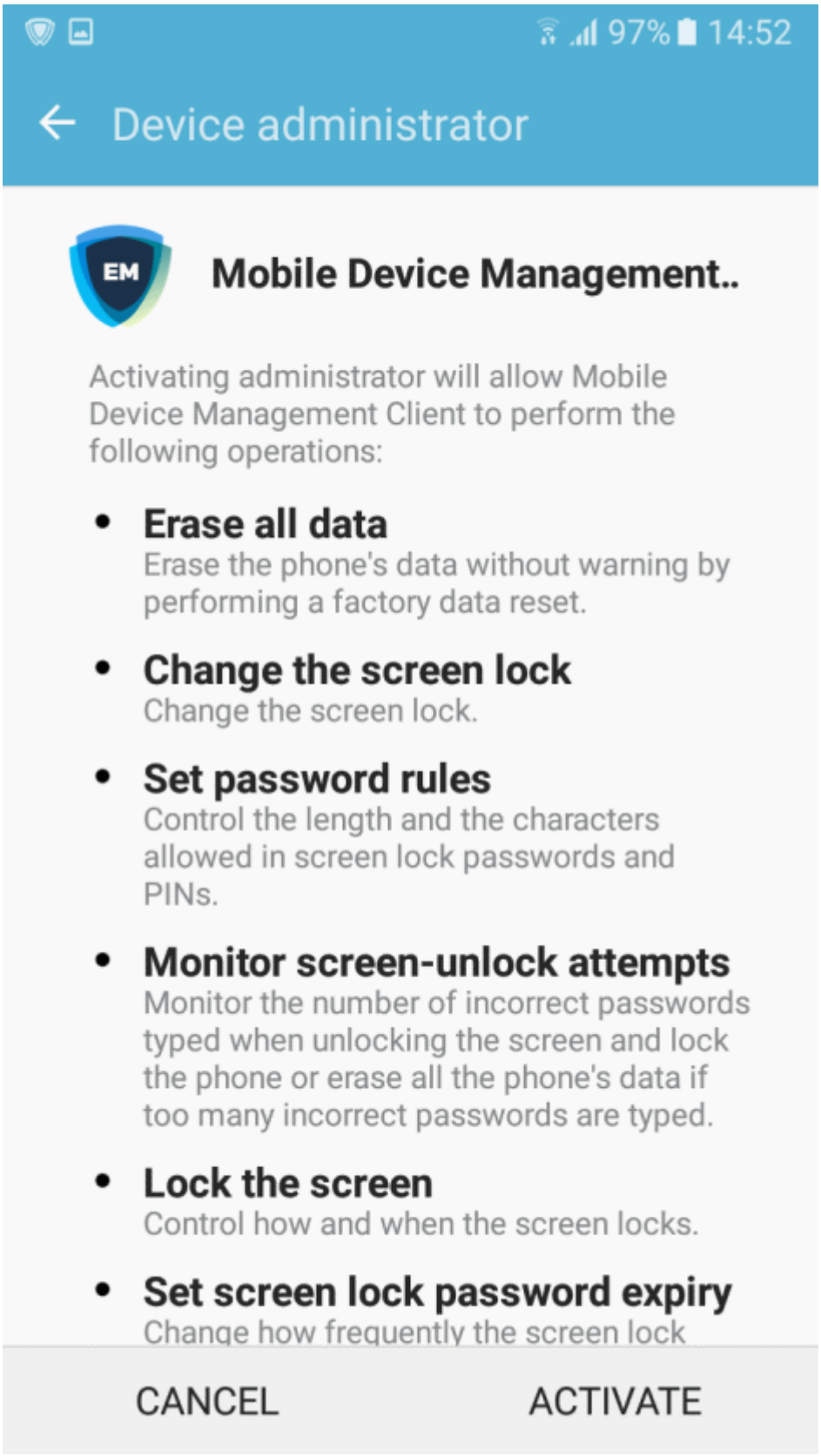
- Enter the username and password you use to login to your network domain.
- Tap the 'Login' button

End User License Agreement



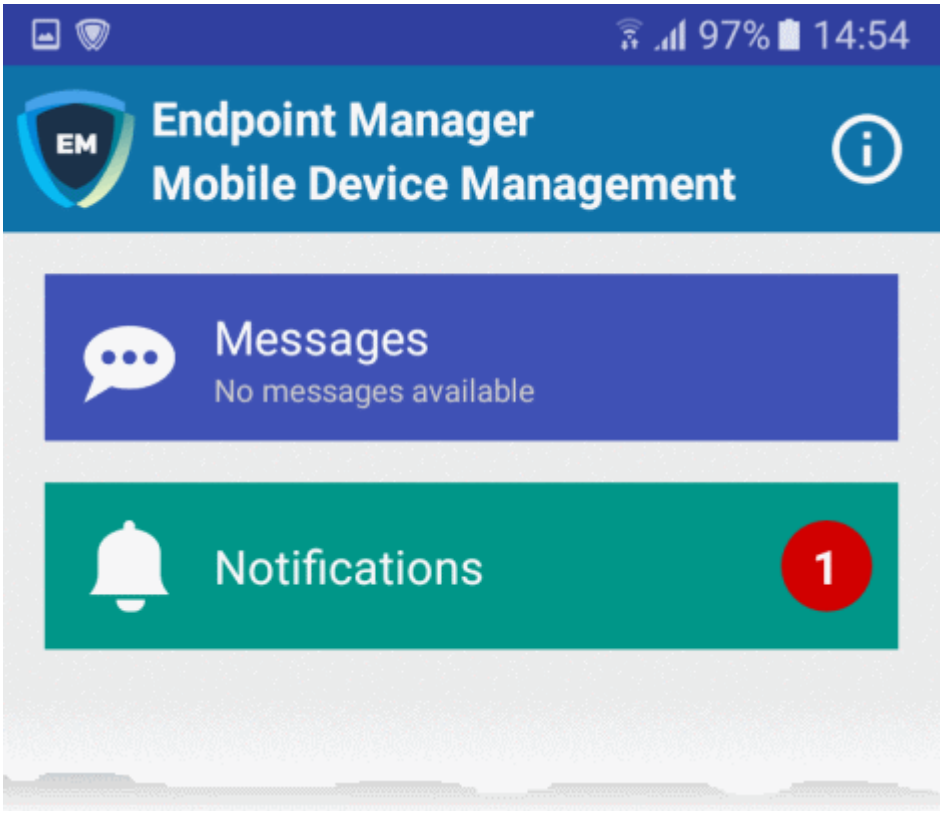
- Scroll down then click the 'I Accept' button

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 enrolled to Endpoint Manager and can be remotely managed from the EM console.

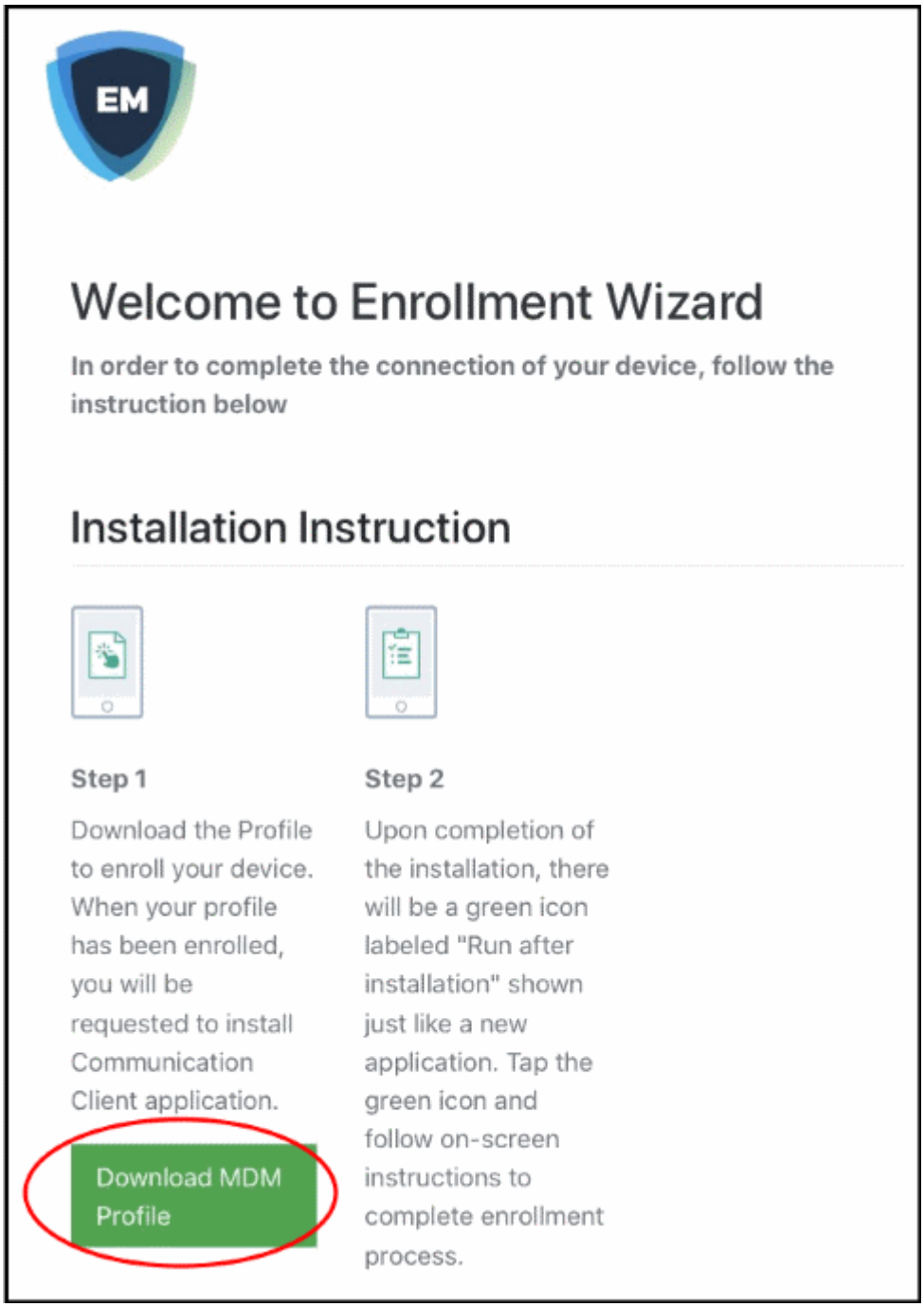
2.2. Enroll iOS Devices

- Open the enrollment email on the device you wish to enroll
- Tap the link in the mail to start the enrollment wizard
- Click 'Download MDM Profile' to install the authentication certificate and device profile

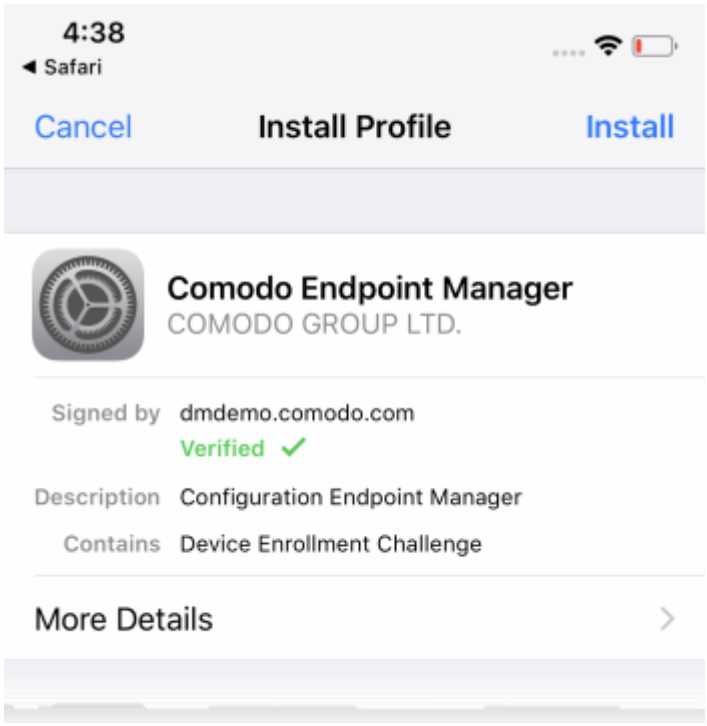
Note: You must keep your iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks or enters standby mode.

Enroll an iOS device

- Open the enrollment email on the device you wish to enroll.
- Tap the link in the mail to start the enrollment wizard
- Click 'Download MDM Profile' in 'Step 1':

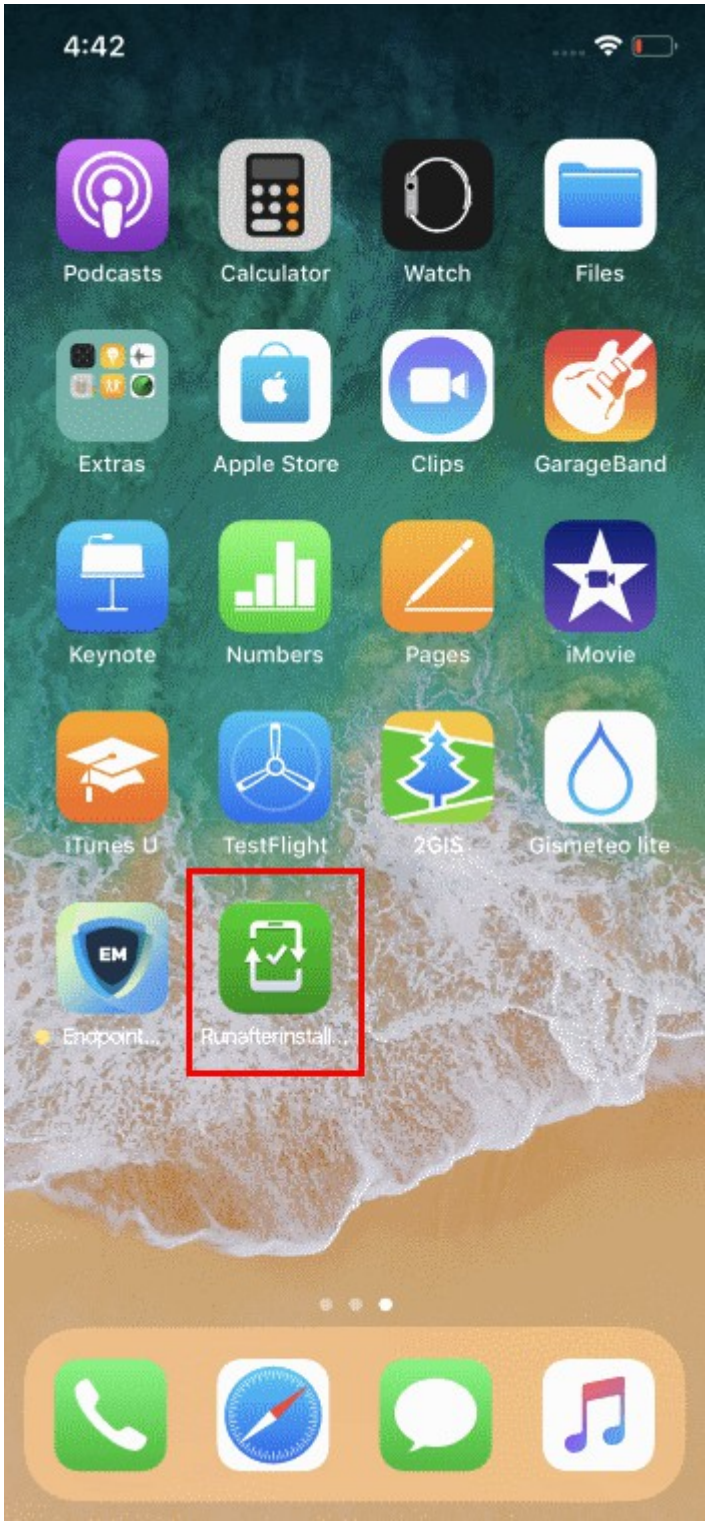


The 'Install Profile' wizard starts:



- Tap 'Install' and follow the steps in the wizard.
- Tap 'Install' at the app installation screen.
- The app is required to connect the device to Endpoint Manager:

- The app is downloaded from the Apple store using your account.
- After installation, tap the green 'Run After Install' icon on the home screen:



The device will be enrolled and connected to Endpoint Manager.

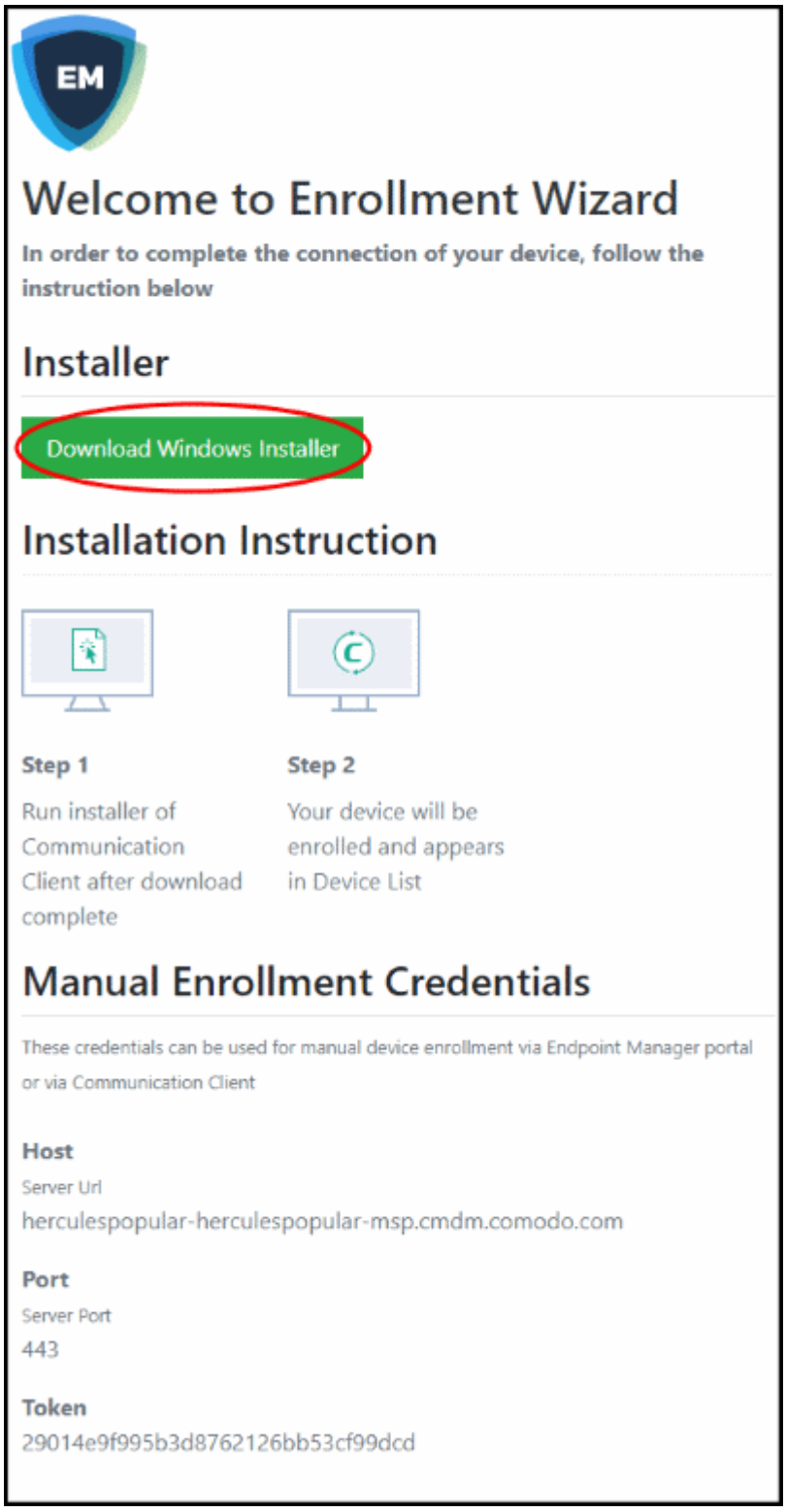
2.3. Enroll Windows Endpoints

Process in brief:

- Open the enrollment email on the device you want to enroll
- Click the enrollment link in the email
- Click the 'Download Windows Installer' button in the wizard.
- Install the client
- Your device will automatically connects to Endpoint Manager once the installation is complete

Enroll a Windows device

- Open the email on the device you want to enroll.
- Click the enrollment link in the email.
- The device enrollment wizard starts.
- Click the 'Download Windows Installer' button:



The EM client setup file gets downloaded.

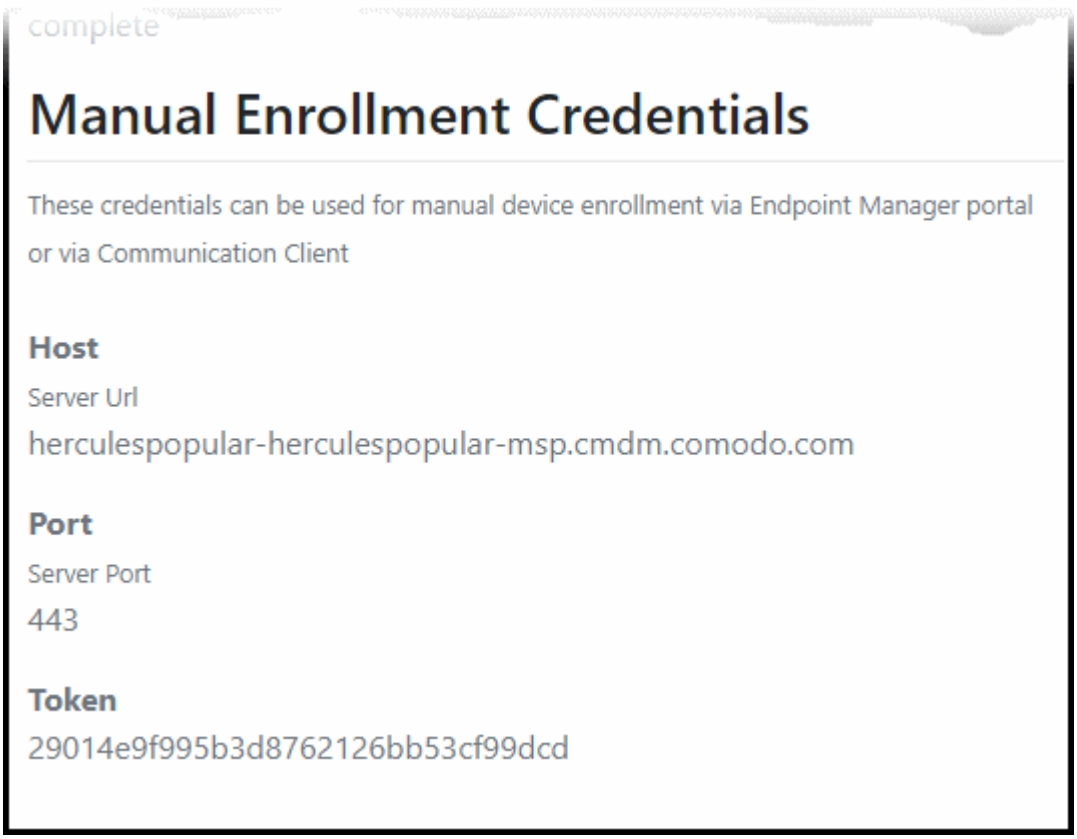
- Double-click on the file to install the communication client.

The device is automatically enrolled to Endpoint Manager when installation is over. Comodo Client Security is also installed if your administrator has included it.

The EM communication client icon appears at the bottom-right of the endpoint screen.

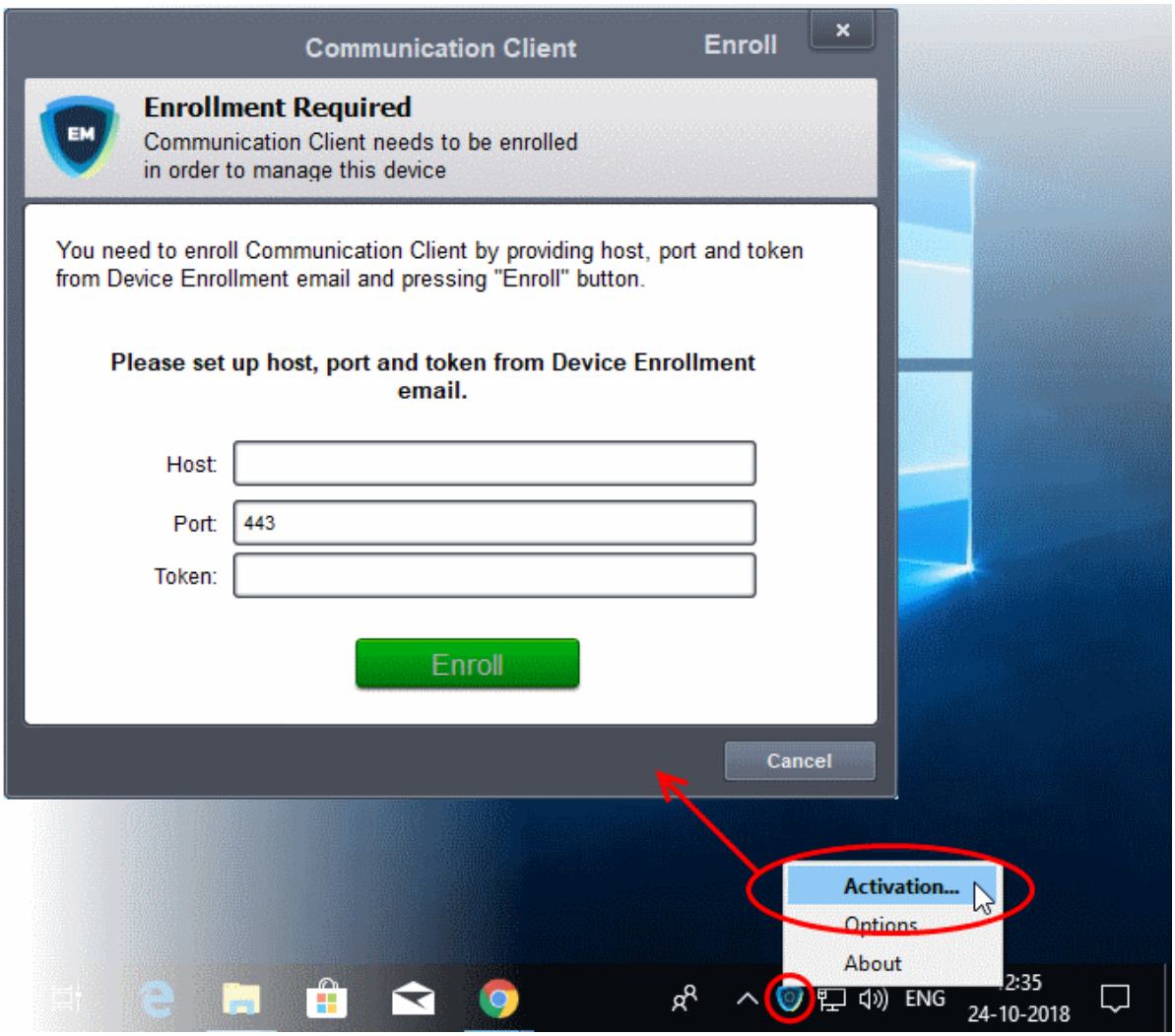
- If the device is not enrolled after installation, you can manually enroll the device at a later. This might happen, for example, if there are connectivity issues.

- You will need to enter the host, port and token ID to manually enroll. You can find these items at the end of the device enrollment page.

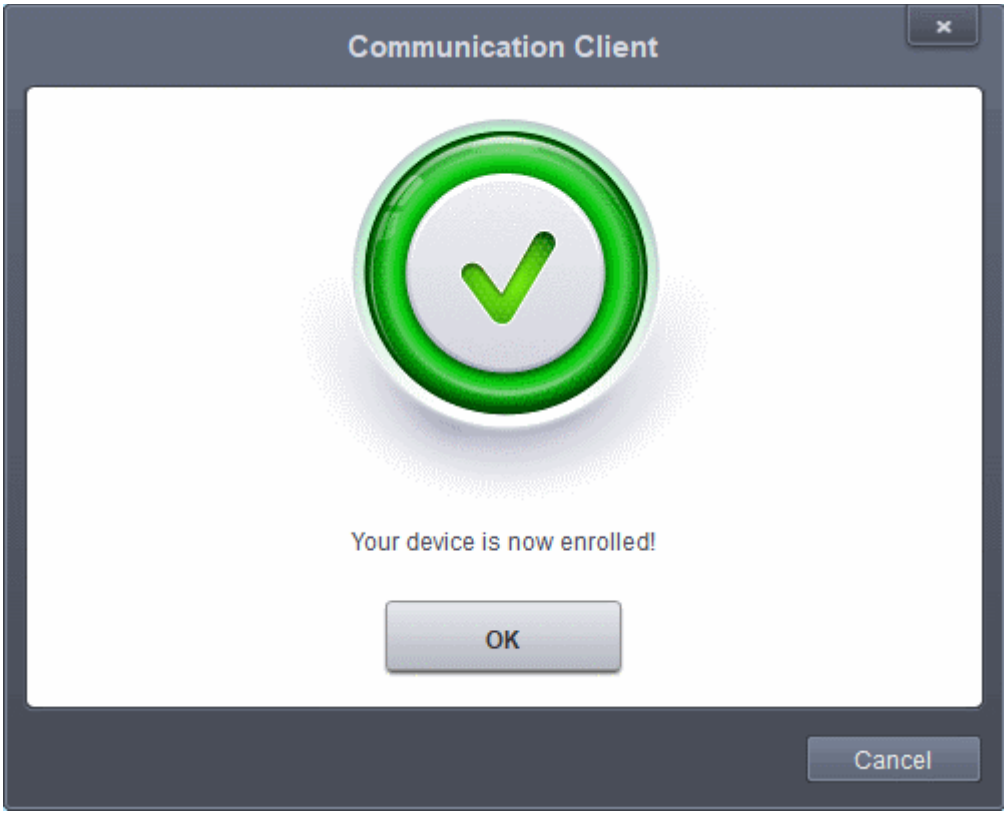


Manually enroll your device

- Right-click on the communication client tray icon and select 'Activation'



- Enter the host, port number and token in the respective fields. You can find these items in the device enrollment page.
- The client communicates with the EM server and enrolls the device.



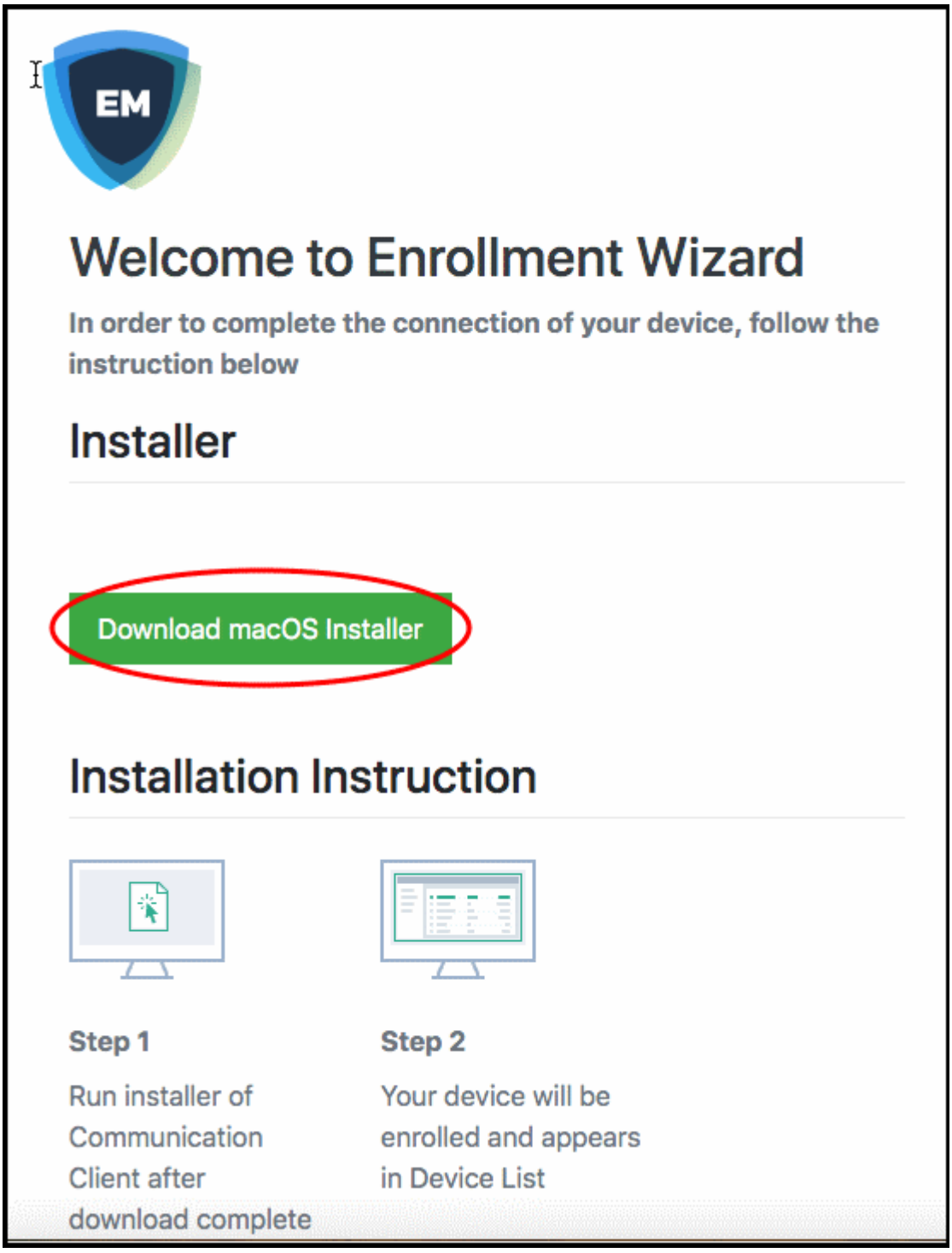
2.4. Enroll Mac OS Devices

Process in brief:

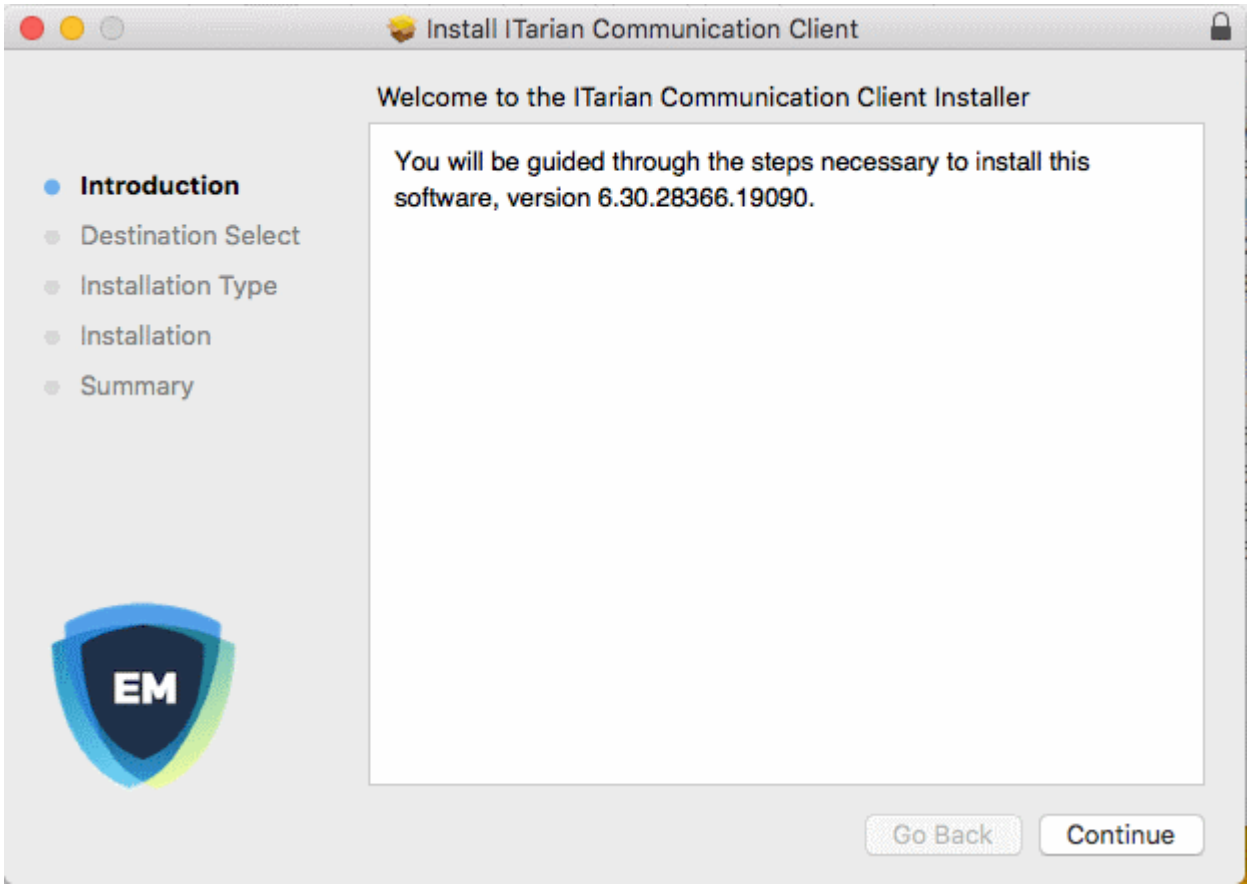
- Open the enrollment email on the device you want to add
- Click the link in the mail to start the setup wizard.
- Click 'Download mac OS Installer' in the wizard.
- Run the client installation package.
- Your device will automatically connect to Endpoint Manager once the installation is complete

Enroll a Mac OS device

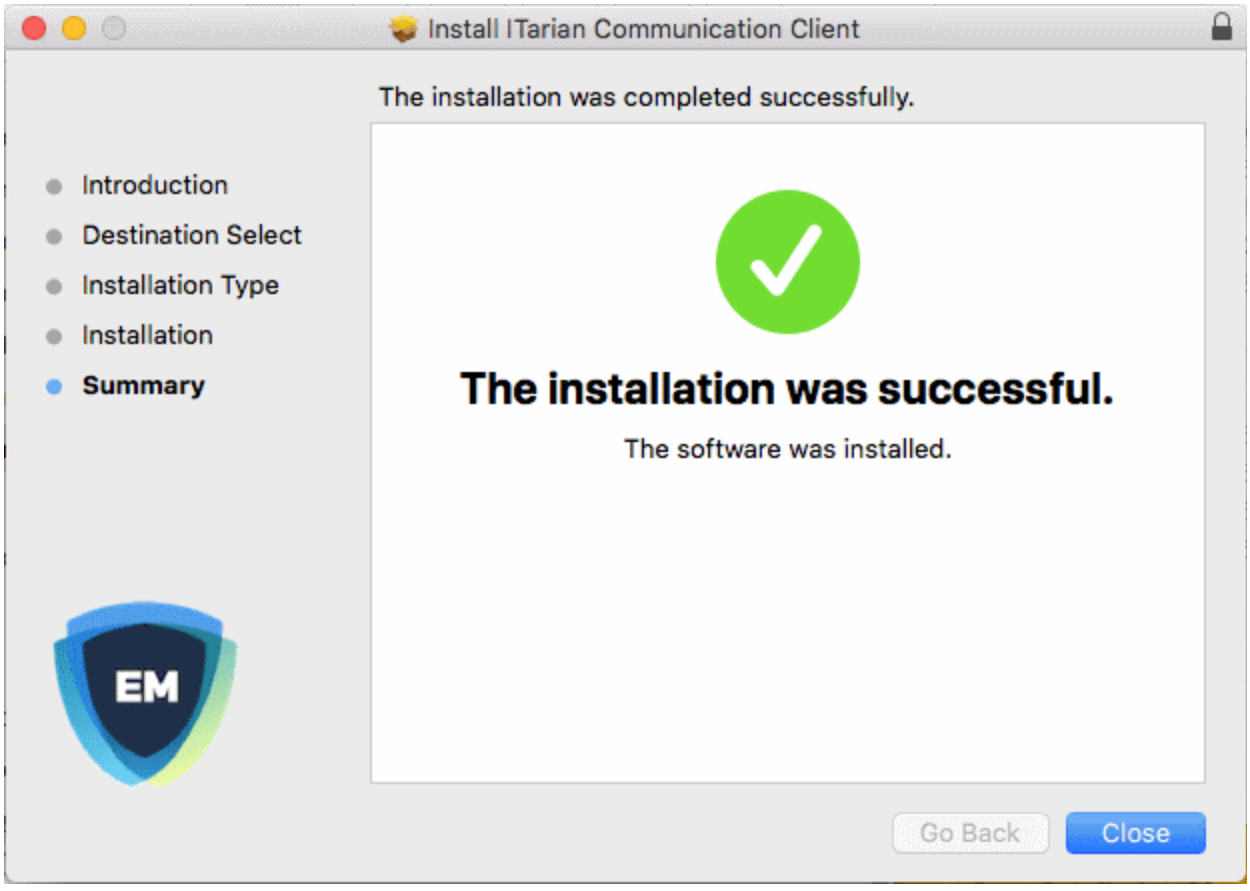
- Open the email on the device you want to add
- Click the link in the mail to start the setup wizard
- Click 'Download mac OS Installer' in the wizard:



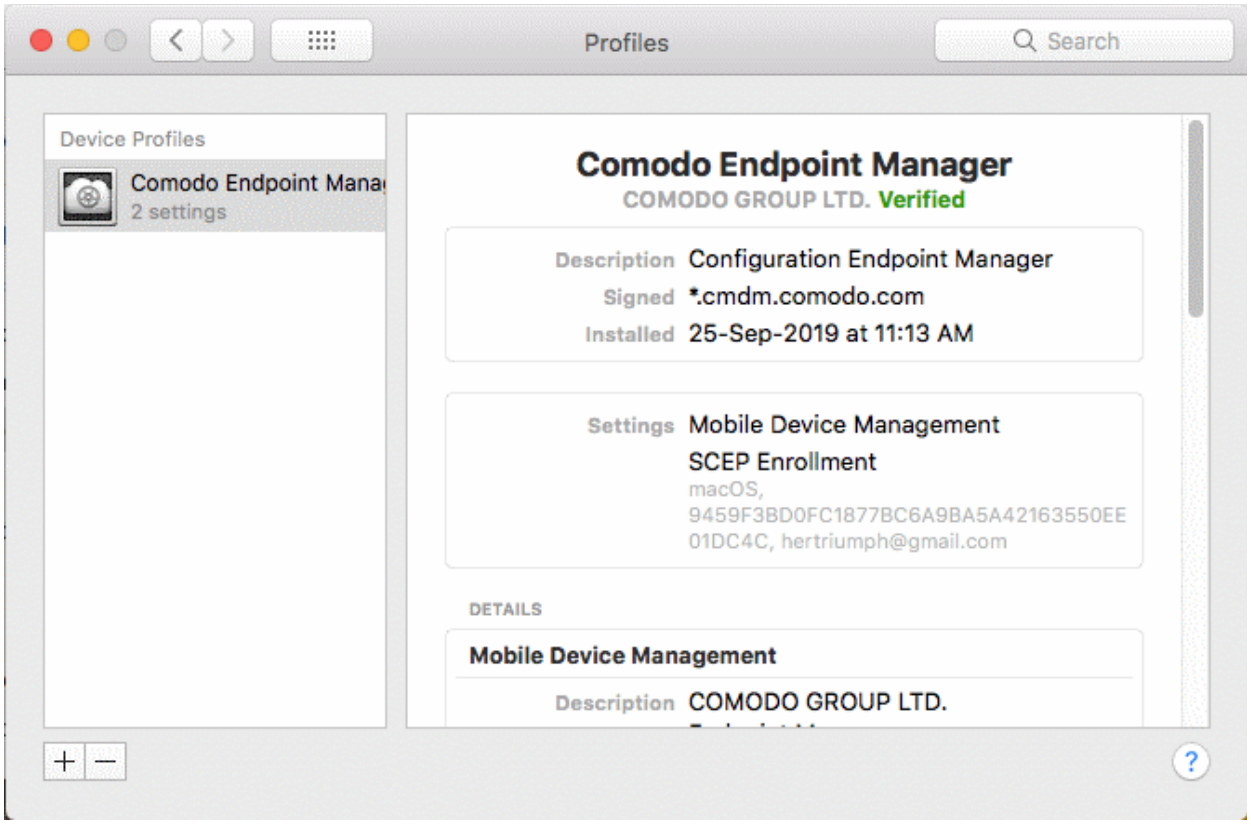
- Open the setup file to install the communication client.



- Follow the wizard to complete the installation.



- The profiles screen shows details about the Endpoint Manager profile, if your admin has chosen to install it:



- The device is automatically enrolled to Endpoint Manager when installation is over. Comodo Client Security is also installed if your administrator has included it.
- The Endpoint Manager icon will appear on your desktop.

2.5. Enroll Linux OS Endpoints

Process in brief:

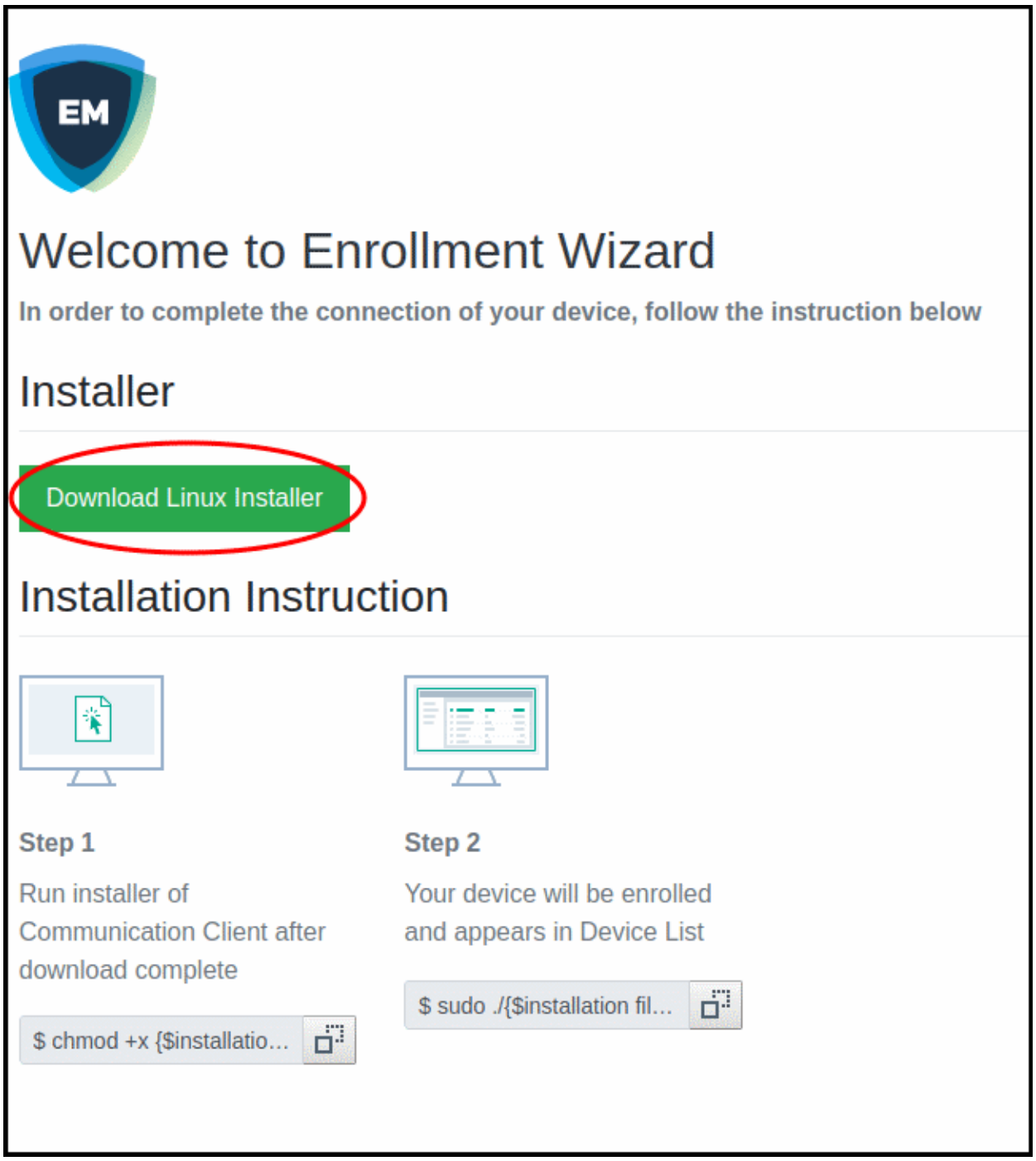
- Open the enrollment mail on the Linux device you want to enroll
- Click the link in the email to start the setup wizard
- Click the 'Download' button in the device enrollment wizard page and download the EM communication client.
- Install the client on the device
- After installation, your device automatically connects to the Endpoint Manager server.

Supported distributions

- Ubuntu 18
- Ubuntu 16.04.2
- Cent OS 7
- Debian 8.8
- Red Hat Enterprise 7

Enroll a Linux device

- Open the mail on the target device and click the enrollment link. This will start the setup wizard.
- Click the 'Download Linux Installer' button and save the file:



You can install the communication client on the Linux device by completing the following:

1. Change installer mode to executable - enter the following command:

   $ chmod +x {$installation file$}

2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run

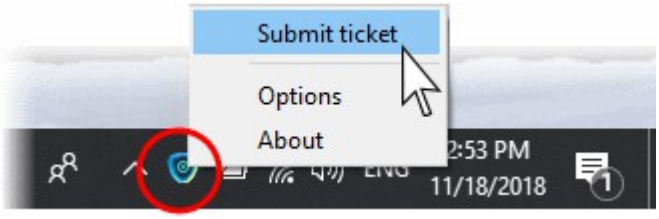
```
c1@c1-VirtualBox: ~/Downloads
c1@c1-VirtualBox:~$ ls
Desktop    Downloads         km-0409.ini  Pictures  Templates
Documents  examples.desktop  Music        Public    Videos
c1@c1-VirtualBox:~$ cd Downloads/
c1@c1-VirtualBox:~/Downloads$ ls
itsm_cTjIw6gG_installer.run
c1@c1-VirtualBox:~/Downloads$ chmod +x itsm_cTjIw6gG_installer.run
c1@c1-VirtualBox:~/Downloads$ sudo ./itsm_cTjIw6gG_installer.run
[sudo] password for c1:
Verifying archive integrity... All good.
Uncompressing Linux ITSM Agent  100%
systemd system
cTjIw6gG
Created symlink from /etc/systemd/system/multi-user.target.wants/itsm.service to
 /etc/systemd/system/itsm.service.
Your device is now enrolled!
Service started
c1@c1-VirtualBox:~/Downloads$
```

- The device is automatically enrolled to Endpoint Manager when installation is over. Comodo Client Security is also installed if your administrator has included it.

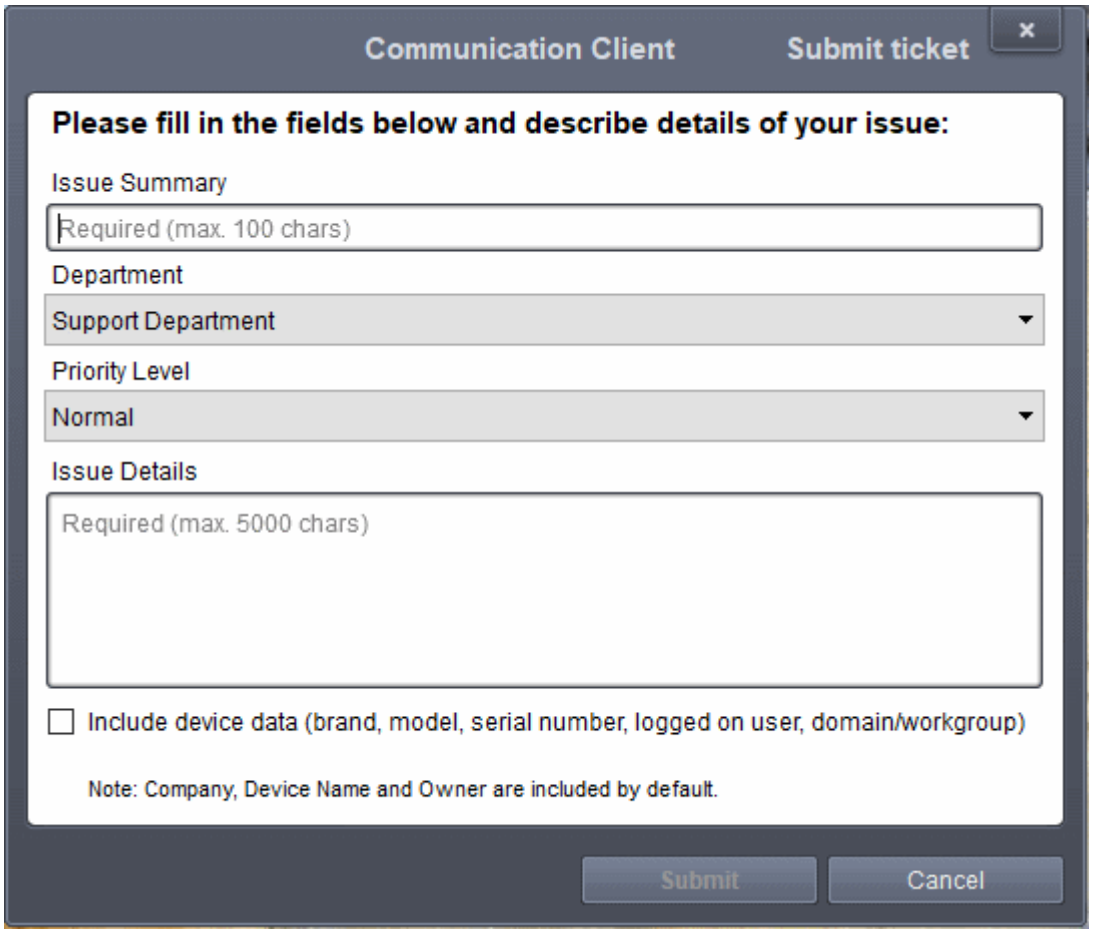
3. Create a Support Ticket

You can create a support ticket by right-clicking on the EM tray icon if you need help to resolve an issue. Click 'Submit Ticket' to contact Service Desk tech support with any issues you have:

- Right-click on the communication client tray icon and select 'Submit ticket'



Describe your issue in the 'Submit Ticket' form:



Note: The form may look slightly different to the screenshot above, depending on how your admin has configured it.

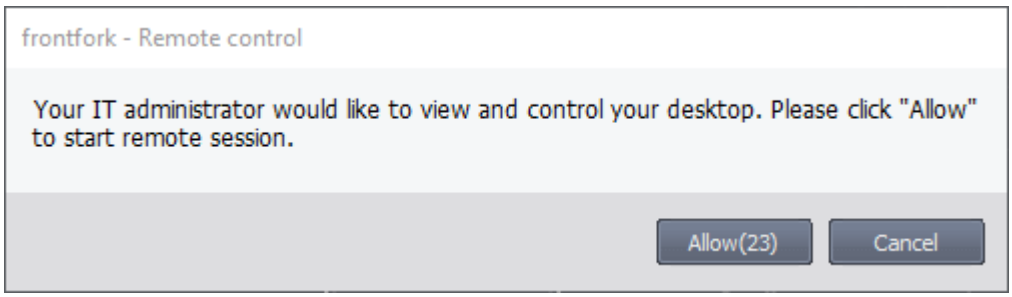
- **Issue Summary** - Type a short description of your issue. For example, 'Cannot connect to internet', or 'Cannot upload documents to the LAN drive', etc.
- **Department** - The Service Desk department to which the ticket should be assigned.
  - The departments available in the drop-down are configured by your administrator.
- **Priority Level** - Select the importance of the issue. The levels are: Low, Normal, High and Critical. As a rule of thumb:
  - **Critical** - Important systems or software have suffered complete loss of functionality, preventing or severely impairing your business/daily operations. No work-around is available.
  - **High** - Important systems or software are operating at reduced functionality, impairing or preventing your business/daily operations. A work-around is available, but very inconvenient and sub-optimal.
  - **Normal** - A system or software is operating at reduced functionality, but not to the point where it significantly impairs your business/daily operations. A work-around is available, but this is a sub-optimal experience.

  We recommend you leave the priority at 'Normal' for most non-emergency issues. The support staff will escalate the issue to a higher priority if required.
  - **Low** - Non-critical systems or software are operating at reduced functionality, but this has no meaningful impact on your daily operations/business. A work-around is available.
- **Issue Details** - Provide a detailed description of the issue.

Click 'Submit' to send your issue to the support team.

4. Allow Remote Control Requests

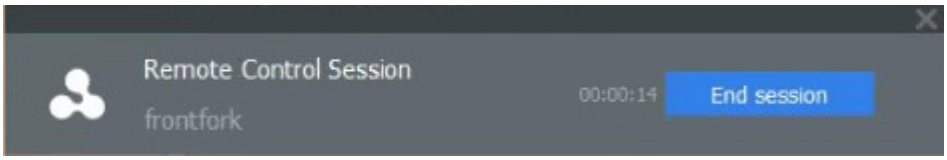
- Endpoint Manager allows admins in your company to remotely access your Windows/Mac device in order to solve issues, install software, run system maintenance and more.
- If your admin has so configured, you can view the remote session, respond to remote control notifications and terminate the session.
- You will be asked to accept or decline the initial connection request:



If no response is given, the connection will go ahead after the timeout period expires.

- Click 'Allow' to accept the remote control request

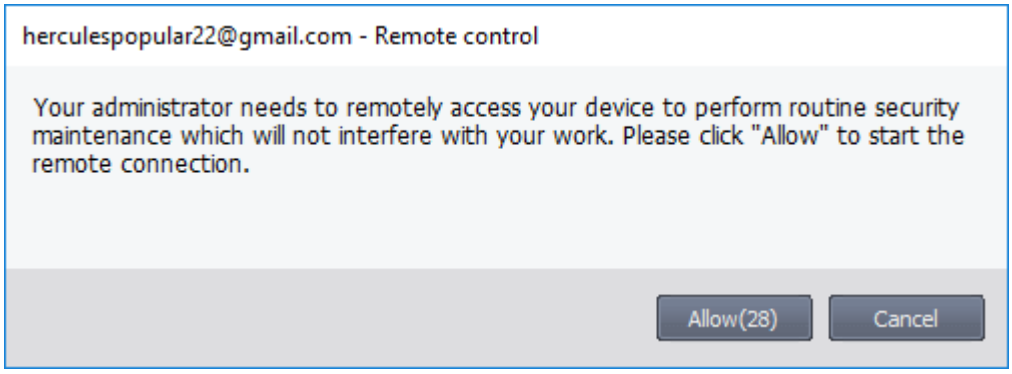
Once the connection is established, a notification appears on your desktop. The notification tells you who is connected to your computer and the duration of the session:



- You can terminate the session at any time by clicking 'End session'.

5. Allow Remote Access Requests

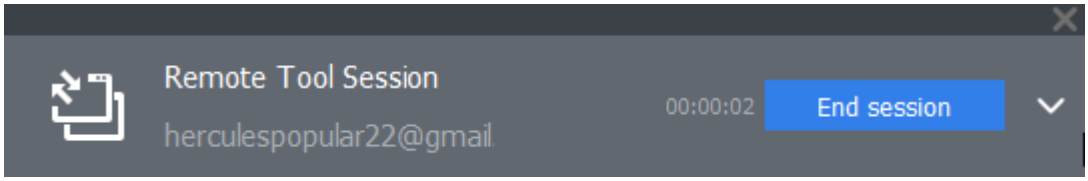
- Endpoint Manager lets admins remotely access your device to fix issues and run maintenance tasks.
- Admins can transfer files back and forth between their machine and your device. They can also create / rename / delete folders and files on your device.
- If your admin has so configured, you can view the remote session, respond to remote access notifications and terminate the session.
- You will be asked to accept or decline the initial connection request:



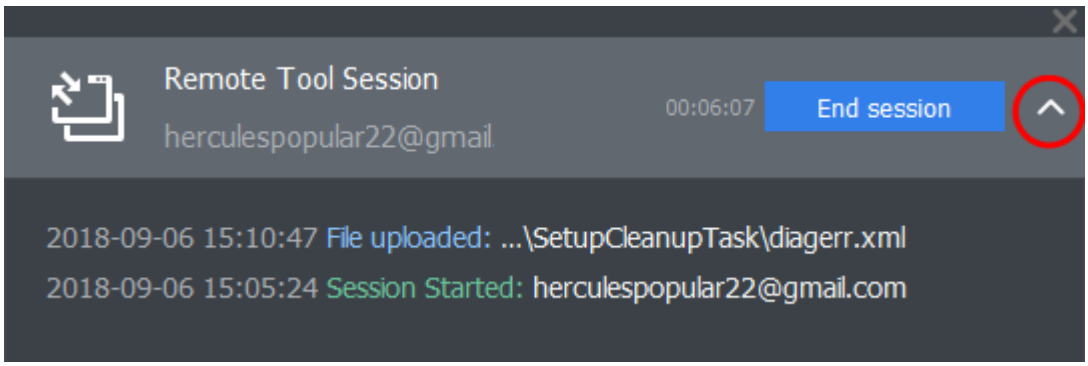
If no response is given, the connection will go ahead after the timeout period expires.

- Click 'Allow' to accept the remote control request

Once the connection is established, a notification appears on your desktop. The notification tells you who is connected to your computer and the duration of the session:



- Click the down arrow in the notification to view the activities of the administrator.



- Click 'End session' to terminate the session.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our blog. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**