COMODO
Creating Trust Online®

# Comodo
# Endpoint Manager

Software Version 6.26

# End User Guide

Guide Version 6.26.021819

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

# Table of Contents

# 1. Introduction to Endpoint Manager

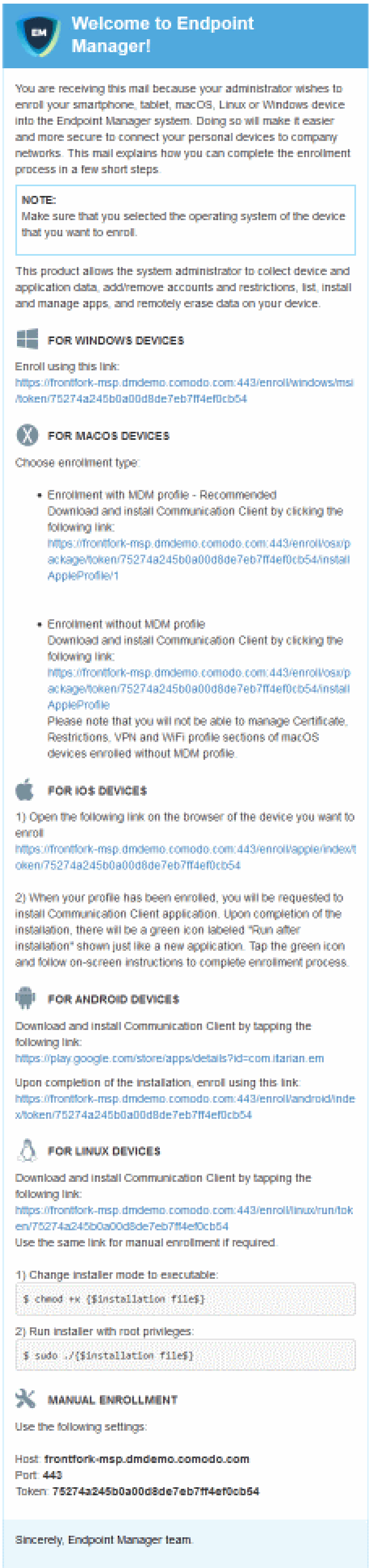
- Endpoint Manager (EM) is a centralized device management system that allows administrators to manage, monitor and secure devices which connect to enterprise networks.
- Once you have enrolled your Android, iOS, Windows, Mac OS or Linux device to EM, it will have a security policy applied to it which 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 administrator has added your device, you will receive a device enrollment mail.
- The mail contains a link to the enrollment software appropriate for your device.
- An example enrollment page is shown below:



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.

**FOR WINDOWS DEVICES**

Enroll using this link:
https://frontfork-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/75274a245b0a00d8de7eb7ff4ef0cb54

**FOR MACOS DEVICES**

Choose enrollment type:

- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

**FOR IOS DEVICES**

1) Open the following link on the browser of the device you want to enroll
https://frontfork-msp.dmdemo.comodo.com:443/enroll/apple/index/token/75274a245b0a00d8de7eb7ff4ef0cb54

2) When your profile has been enrolled, you will be requested to install Communication Client application. Upon completion of the installation, there will be a green icon labeled "Run after installation" shown just like a new application. Tap the green icon and follow on-screen instructions to complete enrollment process.

**FOR ANDROID DEVICES**

Download and install Communication Client by tapping the following link:
https://play.google.com/store/apps/details?id=com.itarian.em

Upon completion of the installation, enroll using this link:
https://frontfork-msp.dmdemo.comodo.com:443/enroll/android/index/token/75274a245b0a00d8de7eb7ff4ef0cb54

**FOR LINUX DEVICES**

Download and install Communication Client by tapping the following link:
https://frontfork-msp.dmdemo.comodo.com:443/enroll/linux/run/token/75274a245b0a00d8de7eb7ff4ef0cb54
Use the same link for manual enrollment if required.

1) Change installer mode to executable:

```
$ chmod +x {$installation file$}
```

2) Run installer with root privileges:

```
$ sudo ./{$installation file$}
```

**MANUAL ENROLLMENT**

Use the following settings:

Host: **frontfork-msp.dmdemo.comodo.com**
Port: **443**
Token: **75274a245b0a00d8de7eb7ff4ef0cb54**

Sincerely, Endpoint Manager team.

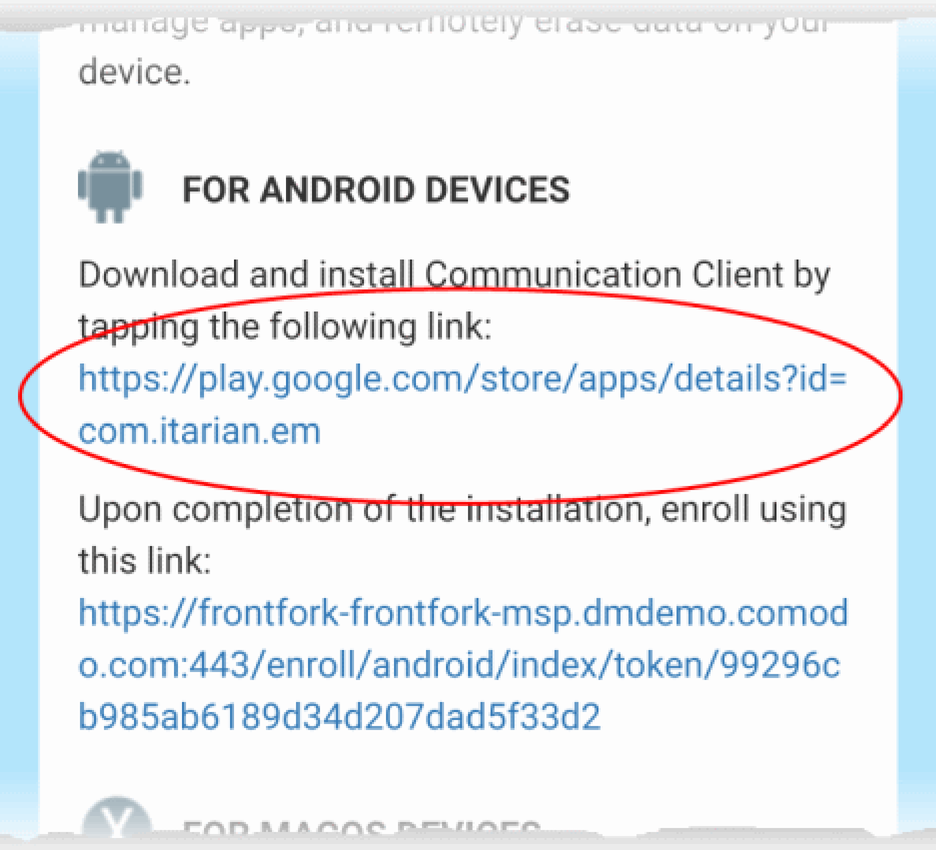
- You can use the same enrollment email to enroll multiple devices. Please ensure you open the mail on the device you wish to enroll.
- The following sections provide detailed explanations on enrolling devices with different operating systems.
  - **Enroll Android Devices**
  - **Enroll iOS Devices**
  - **Enroll Windows Endpoints**
  - **Enroll Mac OS Devices**
  - **Enroll Linux OS Endpoints**

## 2.1. Enroll Android Devices

- The device enrollment page contains two links under 'For Android Devices'.
- The first to download the Android communication client and the second to enroll the device.
  - **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 itself then tap the enrollment link to open the device setup page
- On the setup page, click the communication client download link under 'For Android Devices':



manage apps, and remotely erase data on your device.

FOR ANDROID DEVICES

Download and install Communication Client by tapping the following link:
https://play.google.com/store/apps/details?id=com.itarian.em

Upon completion of the installation, enroll using this link:
https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/android/index/token/99296cb985ab6189d34d207dad5f33d2

FOR MACOS DEVICES

- You will be taken to the Google play store to download and install the communication client.

### Step 2 - Configure the communication client

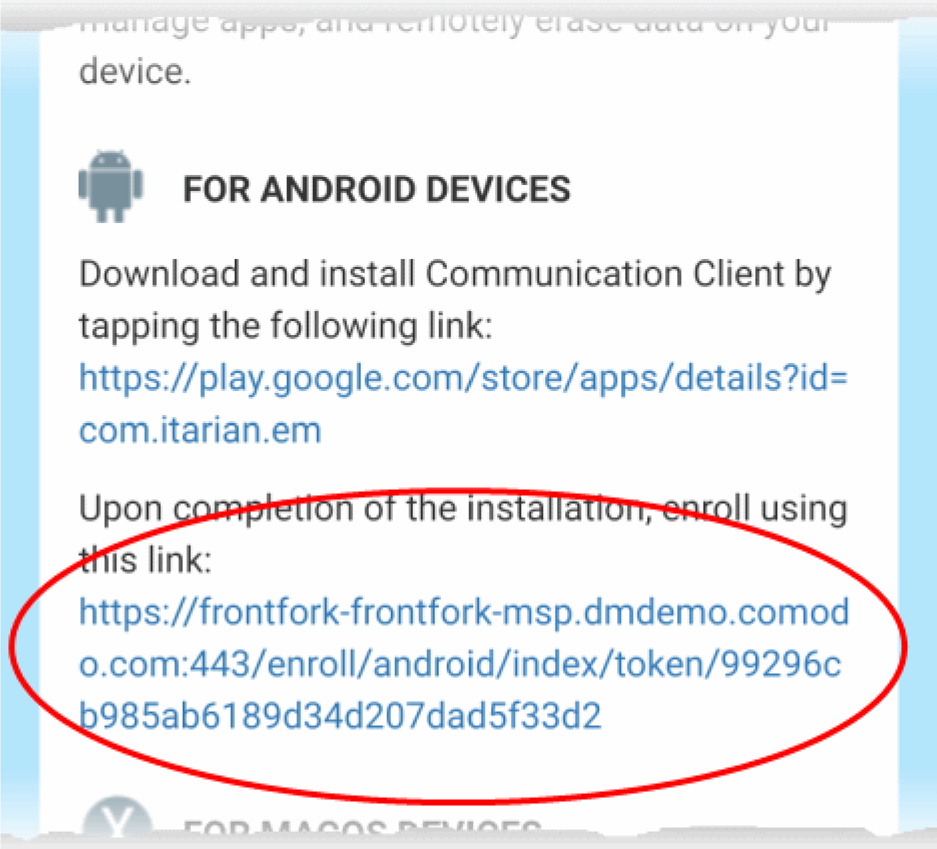
The communication client can be configured to connect to the Endpoint Manager server in two ways:

  - **Automatic Configuration**

- Manual Configuration

### Automatic Configuration

- After installation in step 1, go back to the setup page and tap the enrollment link as shown below:



manage apps, and remotely erase data on your device.

FOR ANDROID DEVICES

Download and install Communication Client by tapping the following link: https://play.google.com/store/apps/details?id=com.itarian.em

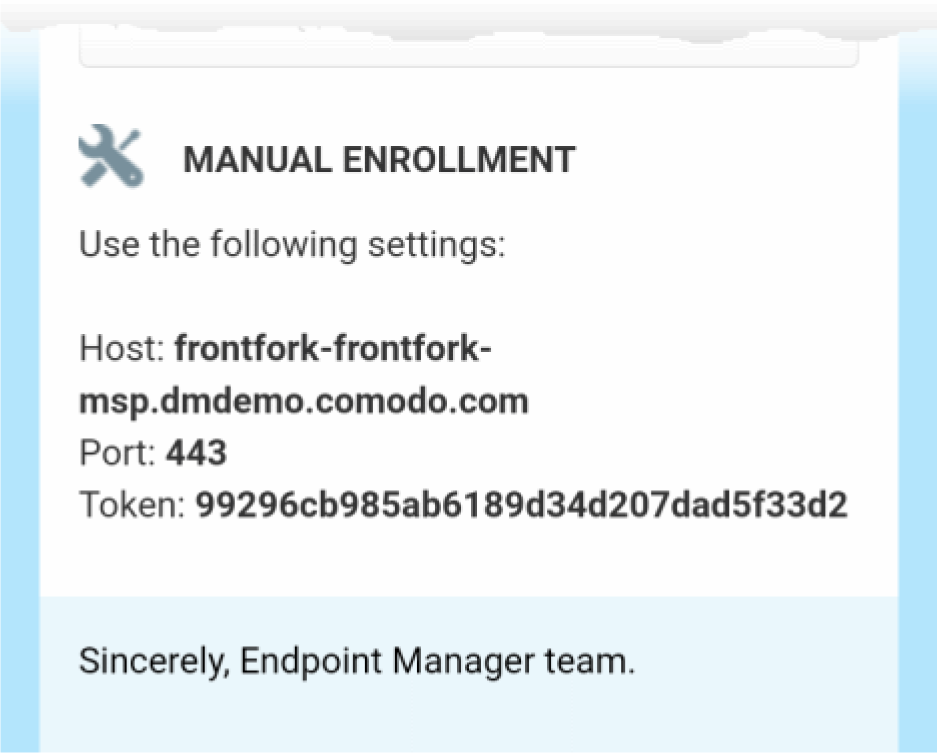
Upon completion of the installation, enroll using this link: https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/android/index/token/99296cb985ab6189d34d207dad5f33d2

FOR MACOS DEVICES

The communication 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 the token string (aka PIN). You can find these items on the setup page:



MANUAL ENROLLMENT

Use the following settings:

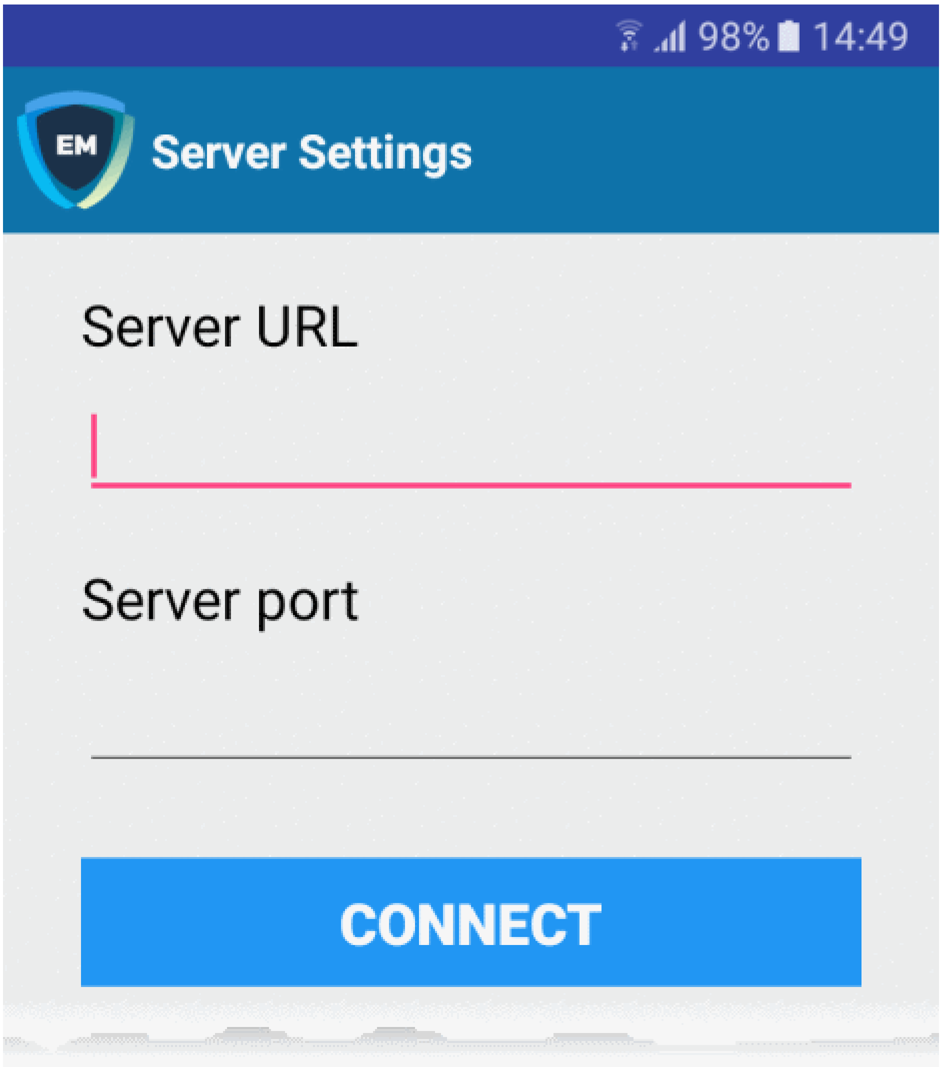
Host: **frontfork-frontfork-msp.dmdemo.comodo.com**
Port: **443**
Token: **99296cb985ab6189d34d207dad5f33d2**

Sincerely, Endpoint Manager team.

**To 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 Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Server URL | Text Field | Enter the url of the EM server contained in the device enrollment page. |
| Server port | Text Field | Enter the connection port of the server as specified in the mail. (Default = 443) |

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

## Login to the Console

You can login to the EM console via the Android client in two ways:

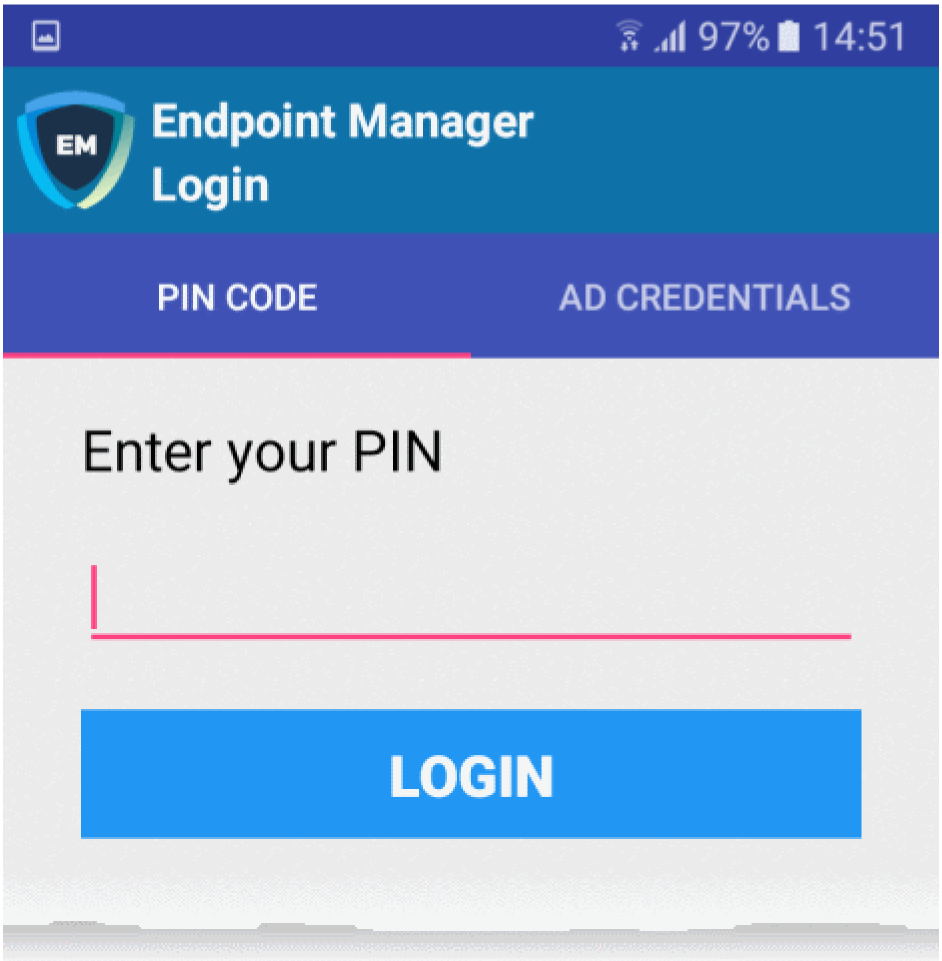
- Enter the personal identification number (PIN) contained in the page

  OR

- Enter your username and password

### Enter PIN (Token)

- Open the communication client
- Open the 'Pin Code' tab in the 'Login' screen



- Enter the PIN (token) contained in the enrollment page
- Tap 'Login'. The **End User License Agreement** appears.

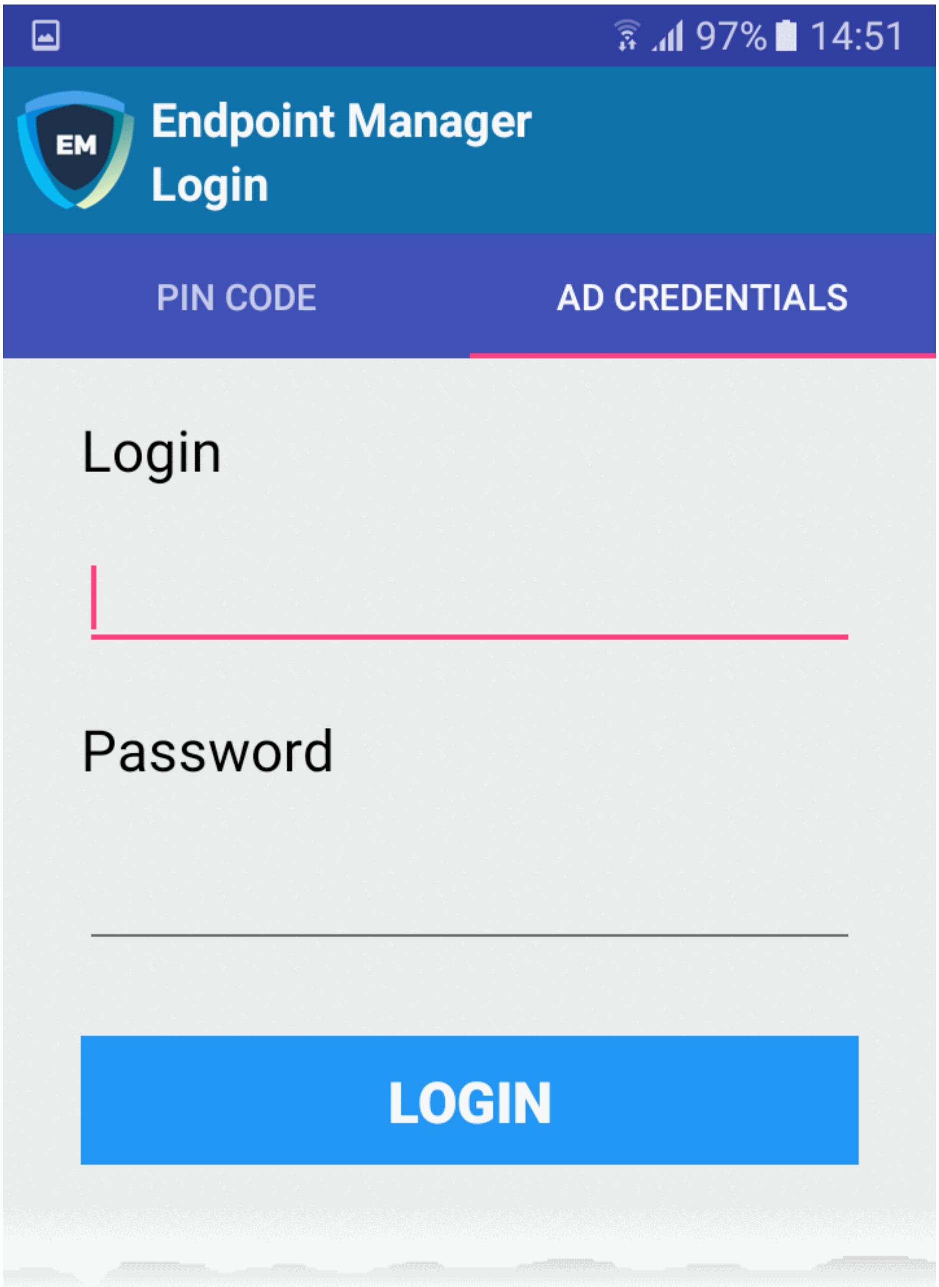
**Enter your username and password**

- Open the communication client
- Open the 'AD Credentials' tab in the 'Login' screen

**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

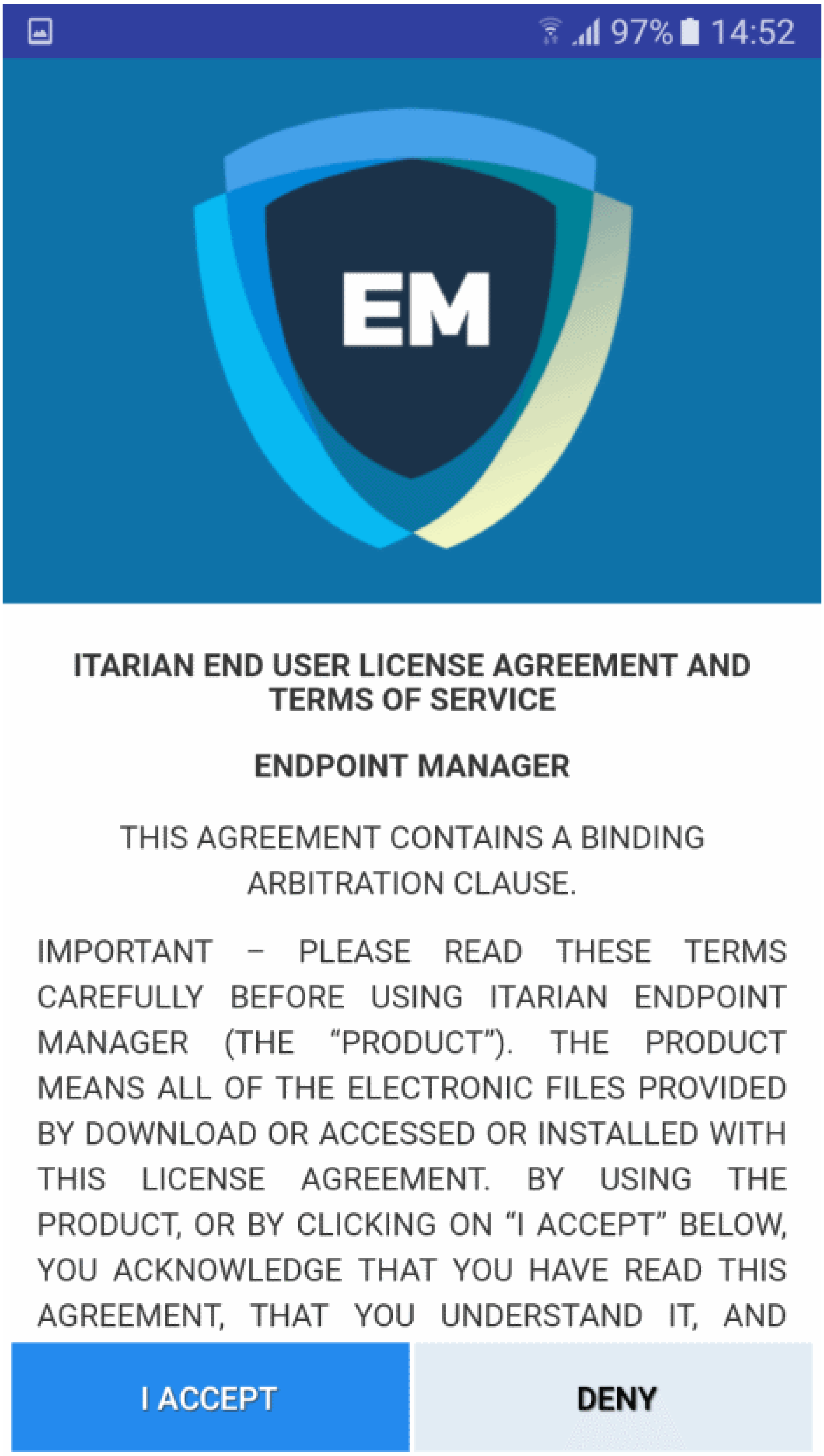
Contact your administrator if you are having issues connecting.



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

## End User License Agreement

The EULA screen will appear.



**ITARIAN END USER LICENSE AGREEMENT AND TERMS OF SERVICE**

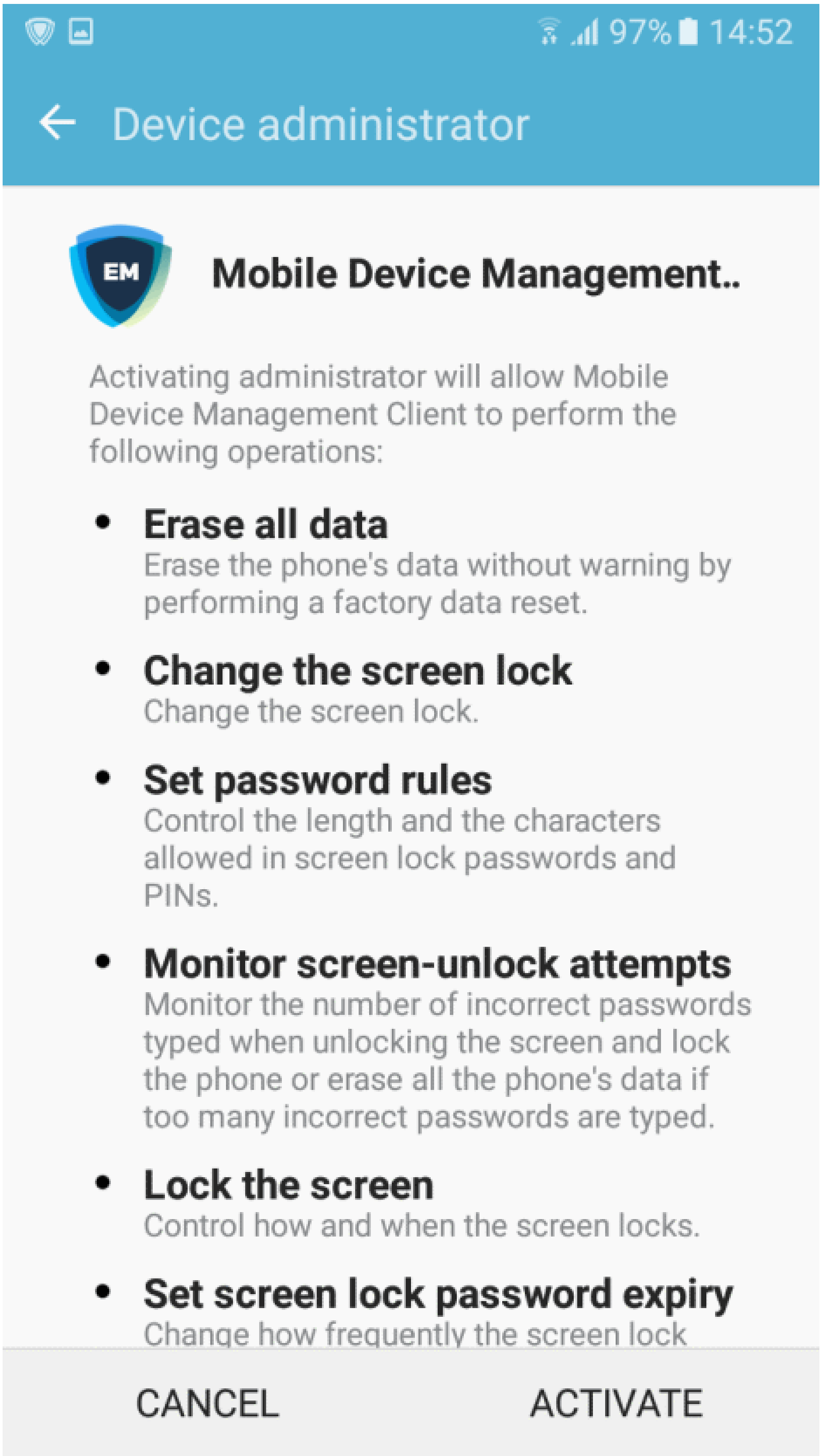
**ENDPOINT MANAGER**

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

- Scroll down the screen, read the EULA fully and click the 'I Accept' button at the bottom.

This opens the client activation screen. Activation requires the client given some admin privileges:



Device administrator

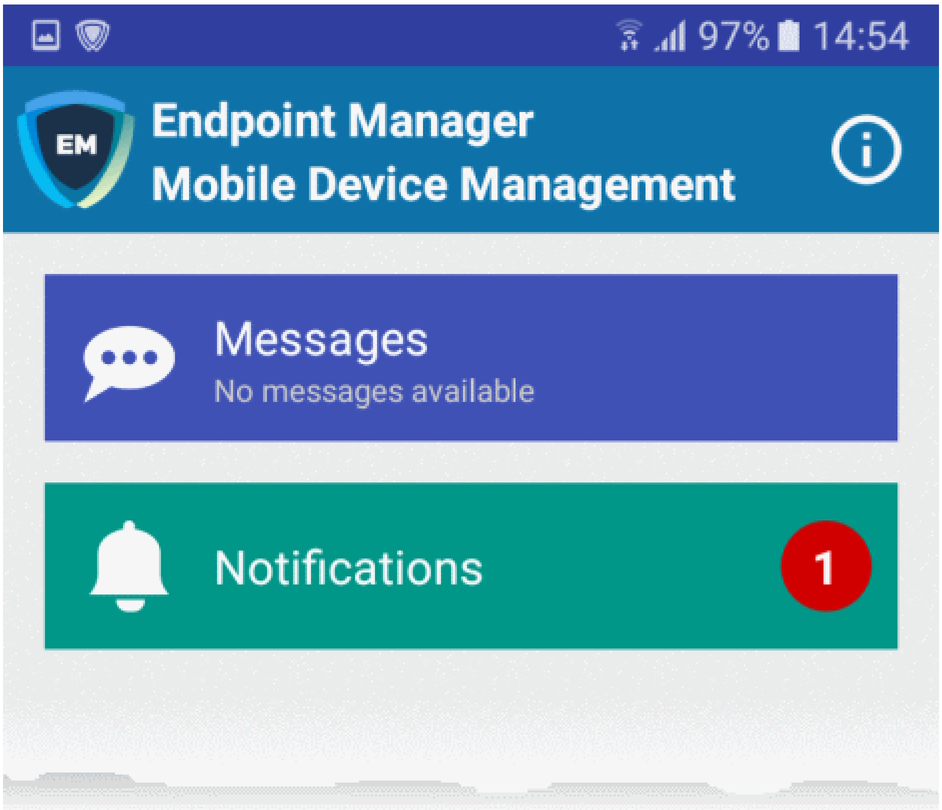
Mobile Device Management..

Activating administrator will allow Mobile Device Management Client to perform the following operations:

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen lock**
  Change the screen lock.
- **Set password rules**
  Control the length and the characters allowed in screen lock passwords and PINs.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set screen lock password expiry**
  Change how frequently the screen lock

- Tap 'Activate'.

The communication client home screen opens:



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

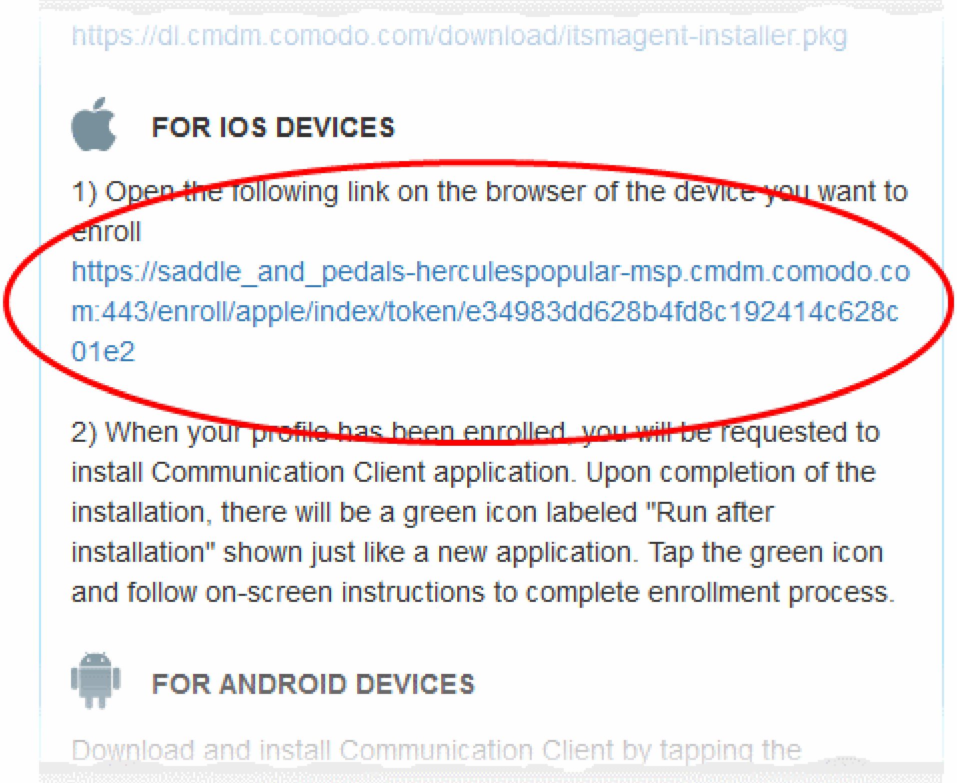
## 2.2. Enroll iOS Devices

- Open the enrollment email on the device you wish to enroll
- Click the link in the mail to open the device enrollment page
- Click the link under 'FOR IOS DEVICES' to install the client 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.

### To enroll an iOS device

- Open the enrollment email on the device you wish to enroll.
- Tap the enrollment link in the mail to open the device enrollment page
- Scroll to the 'FOR IOS DEVICES' section and tap the enrollment link:



https://dl.cmdm.comodo.com/download/itsmagent-installer.pkg

FOR IOS DEVICES

1) Open the following link on the browser of the device you want to enroll
https://saddle_and_pedals-herculespopular-msp.cmdm.comodo.com:443/enroll/apple/index/token/e34983dd628b4fd8c192414c628c01e2

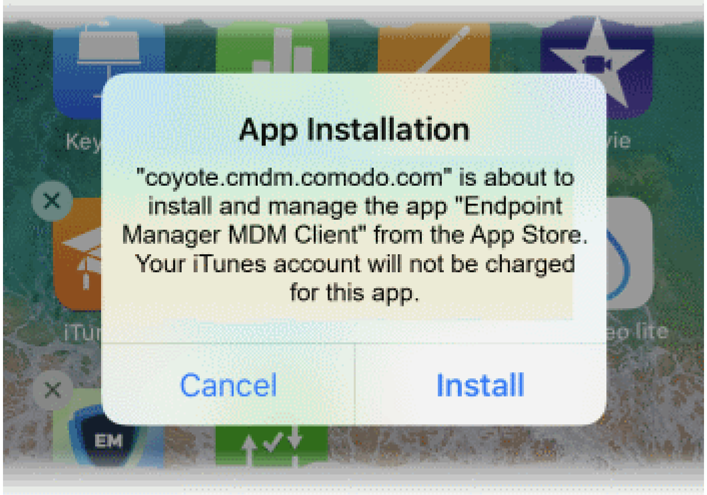
2) When your profile has been enrolled, you will be requested to install Communication Client application. Upon completion of the installation, there will be a green icon labeled "Run after installation" shown just like a new application. Tap the green icon and follow on-screen instructions to complete enrollment process.

FOR ANDROID DEVICES

Download and install Communication Client by tapping the

The 'Install Profile' wizard starts:

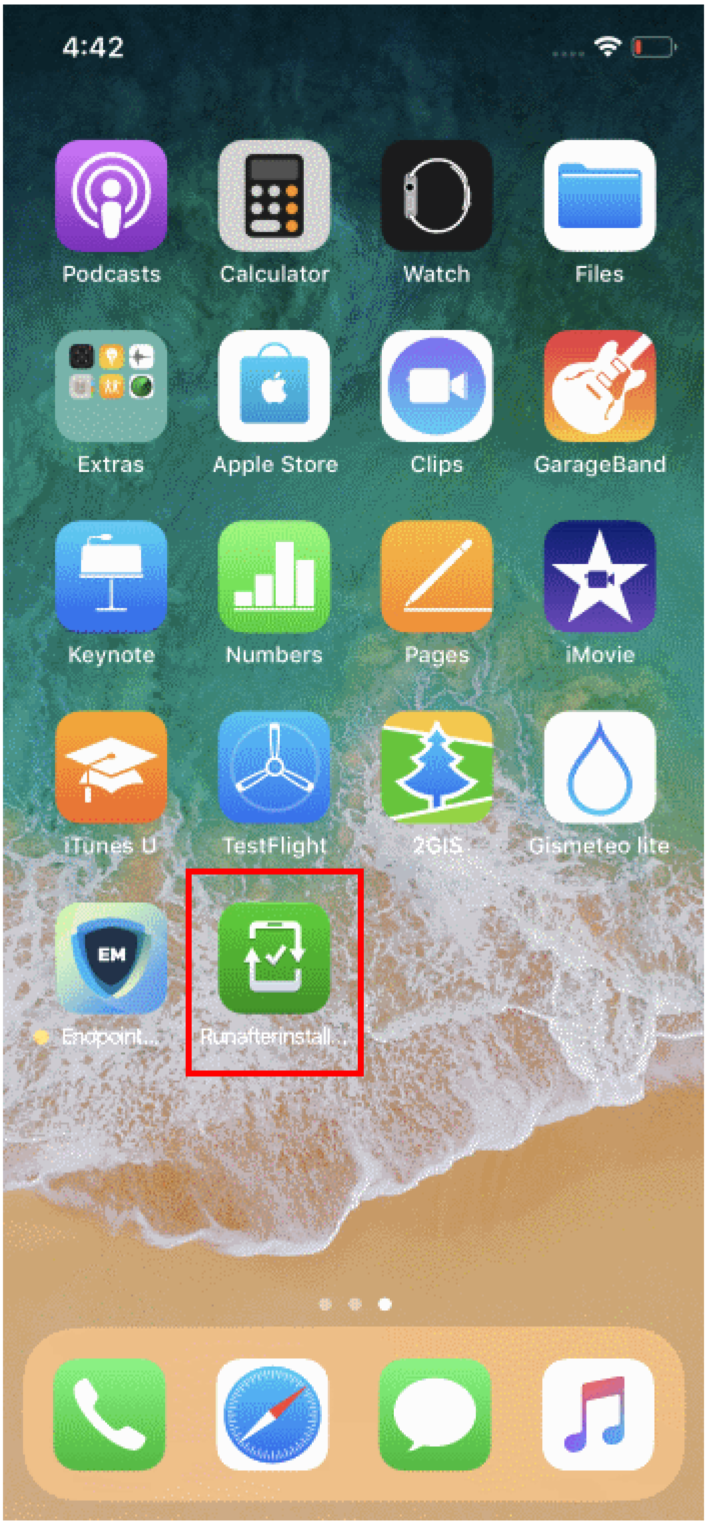
- Follow the wizard to install the EM profile
- After the profile has been installed, the communication client app installation will begin.
- The app is required so that EM can manage the remote device:



App Installation

"coyote.cmdm.comodo.com" is about to install and manage the app "Endpoint Manager MDM Client" from the App Store. Your iTunes account will not be charged for this app.

- The app is downloaded from the iTunes store using your iTunes 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

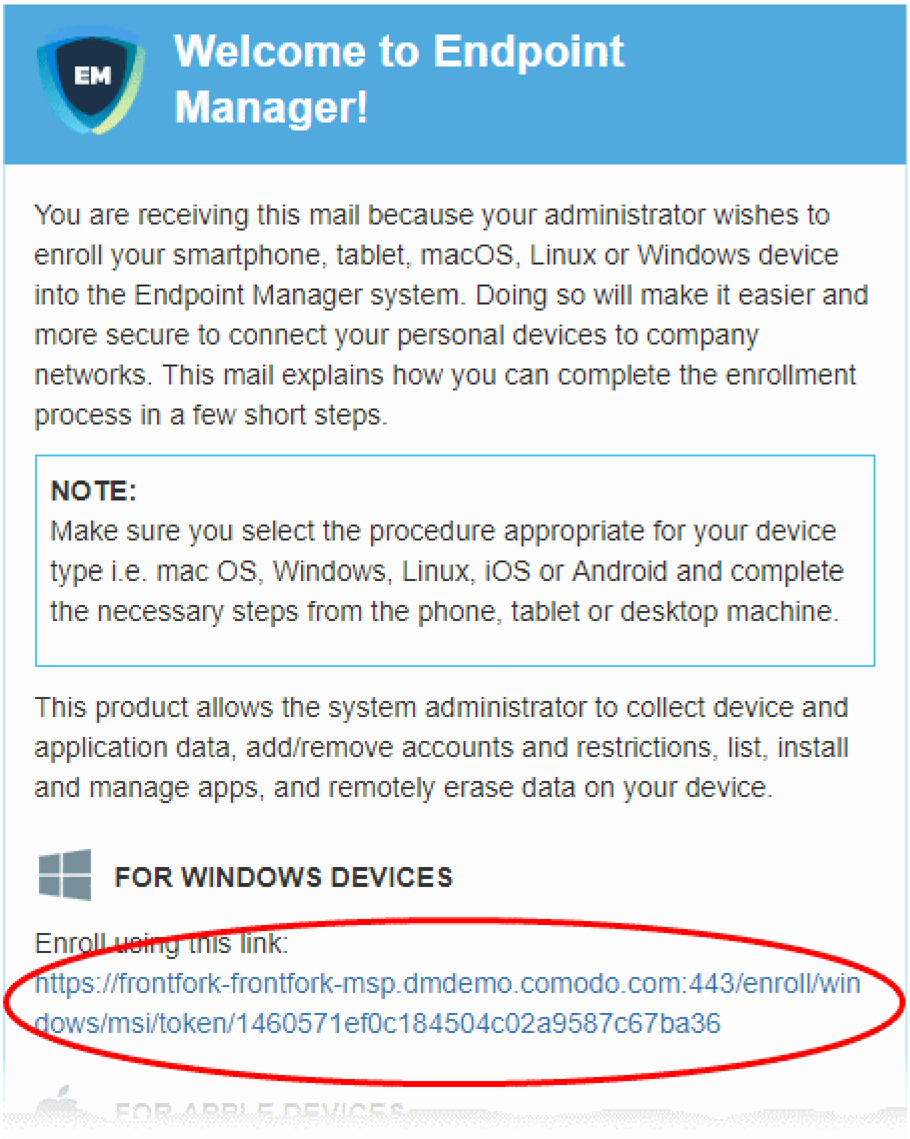
**Process in brief:**

- Open the enrollment email on the device you wish to enroll
- Click the link in the email to open the device enrollment page
- The device enrollment page contains a link to download the communication client for Windows.
- Download the client and install it on the device

- After installation, your device automatically connects to the Endpoint Manager server.

**To enroll a Windows device**

- Open the email on the device you want to enroll.
- Click the enrollment link in the email.
- The 'Device Enrollment' page opens.
- Click the link under 'For Windows devices':



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 you select the procedure appropriate for your device type i.e. mac OS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.

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.

FOR WINDOWS DEVICES

Enroll using this link:
https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/1460571ef0c184504c02a9587c67ba36

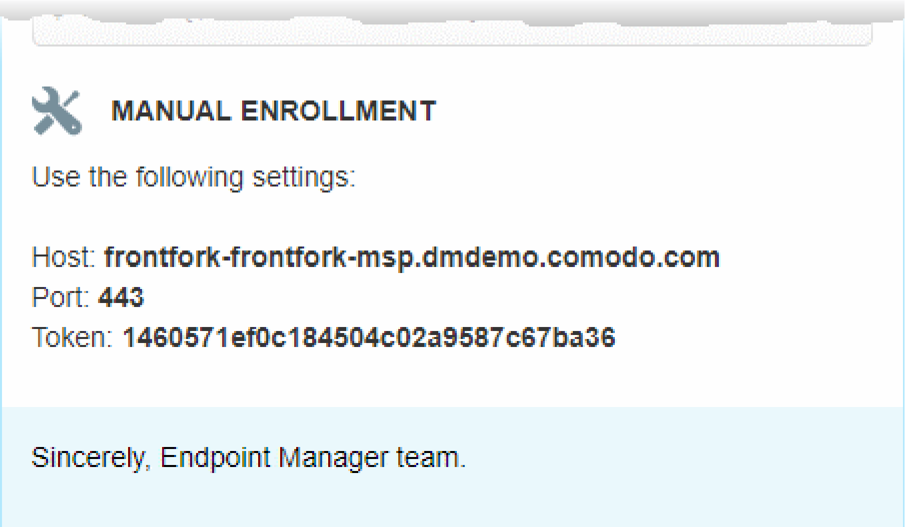
FOR APPLE DEVICES

The EM communication client setup file gets downloaded.

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

The device automatically gets enrolled to Endpoint Manager. once installation is complete. The EM communication client icon appears at the bottom-right of the endpoint screen.

- If the EM communication client is not automatically enrolled at the time of installation, for example, due to internet connectivity issues, you can manually enroll the device at a later time.
- For manual enrollment you will need to enter the host, port and token ID. You can find these items on the end of the device enrollment page.



MANUAL ENROLLMENT

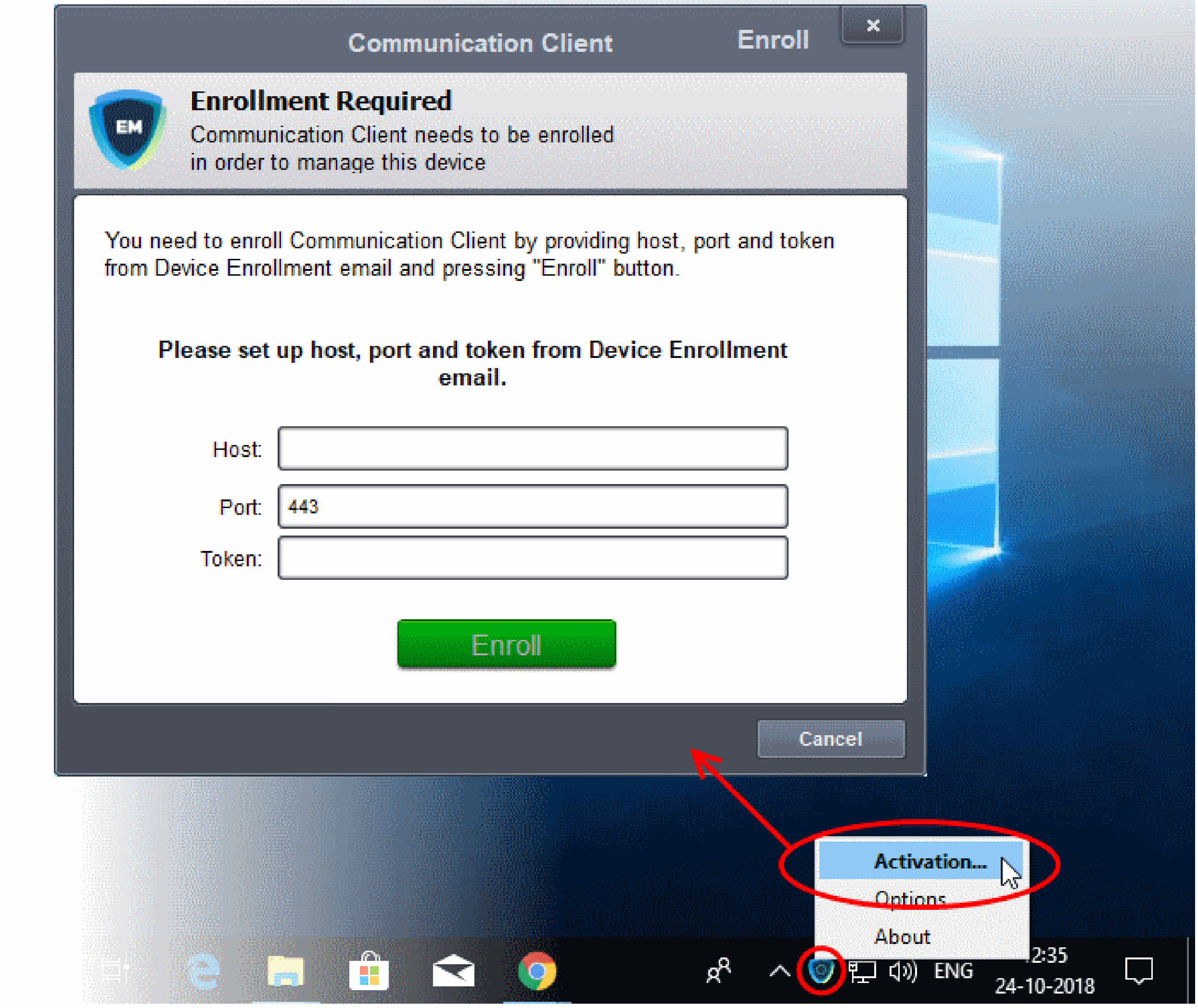
Use the following settings:

Host: **frontfork-frontfork-msp.dmdemo.comodo.com**
Port: **443**
Token: **1460571ef0c184504c02a9587c67ba36**

Sincerely, Endpoint Manager team.

**To manually enroll your device**

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



Communication Client — Enroll

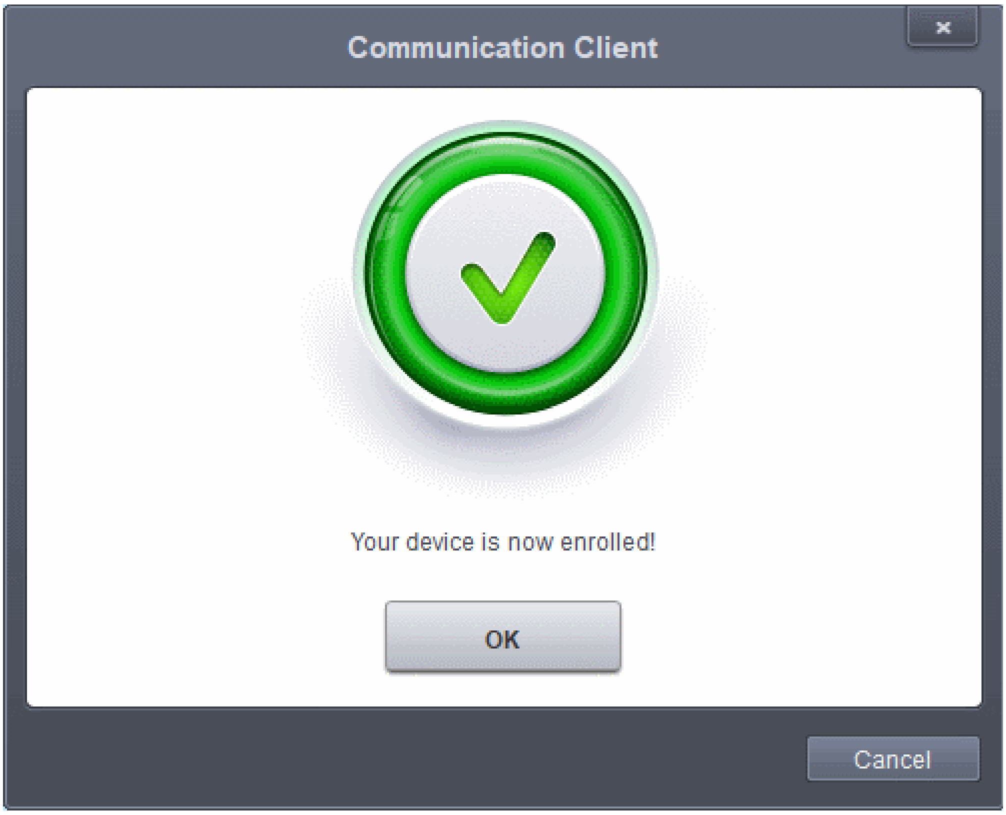
**Enrollment Required**
Communication Client needs to be enrolled in order to manage this device

You need to enroll Communication Client by providing host, port and token from Device Enrollment email and pressing "Enroll" button.

**Please set up host, port and token from Device Enrollment email.**

Host:
Port: 443
Token:

- Enter the 'host', 'port' and the 'Token' contained in the device enrollment page and click 'Enroll'.
- The communication client communicates with the EM server and enrolls the device.



Your device is now enrolled!

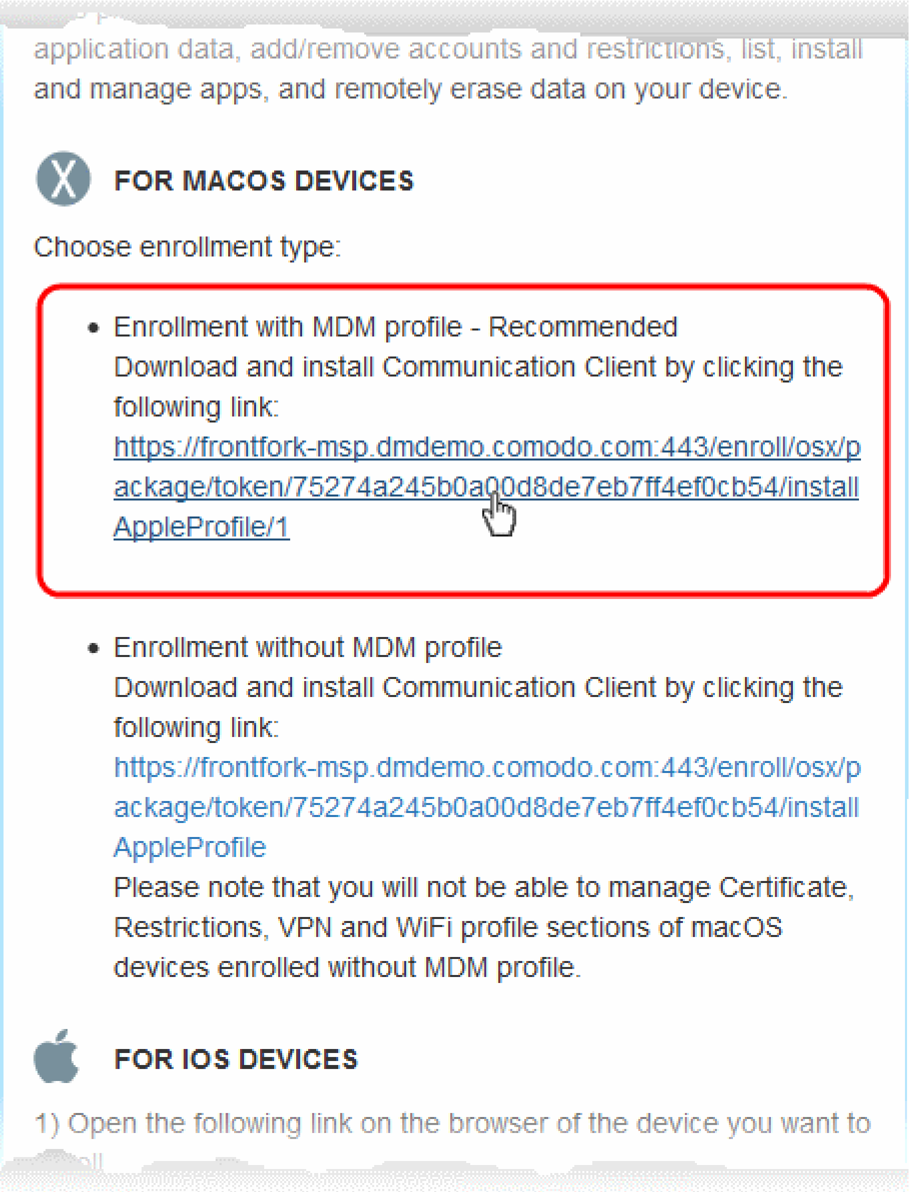
## 2.4. Enroll Mac OS Devices

MAC devices can be added either with or without installing the Endpoint Manager profile.

- Apple only allows one portal to use the protocol which manages devices. This causes issues with organizations who want to use Endpoint Manager in conjunction with another management platform.
- 'Profile-less' enrollment lets admins use Endpoint Manager to manage security while using another platform for general Mac management.
- Contact your administrator to confirm which type of enrollment you should choose.
- See the following for more guidance:
  - **Enrollment with MDM Profile**
  - **Enrollment without MDM Profile**

### Enroll with MDM Profile

- Open the enrollment mail on the device you want to add
- Click the link in the mail to open the device enrollment page
- Scroll down to the 'FOR MAC OS DEVICES' section.
- Click the link under 'Enrollment with MDM profile'



application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR MACOS DEVICES

Choose enrollment type:

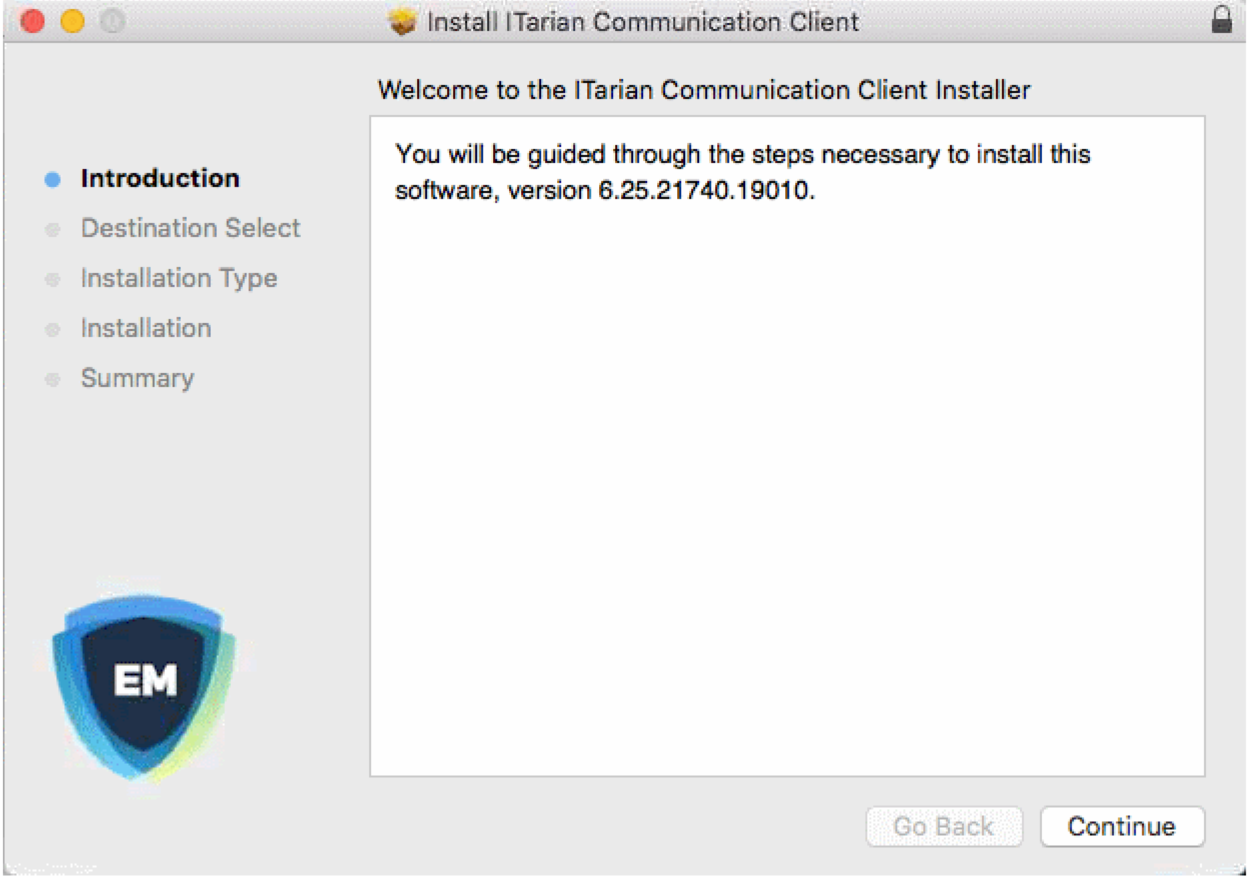
- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

FOR IOS DEVICES

1) Open the following link on the browser of the device you want to enroll

This will start the installation wizard:

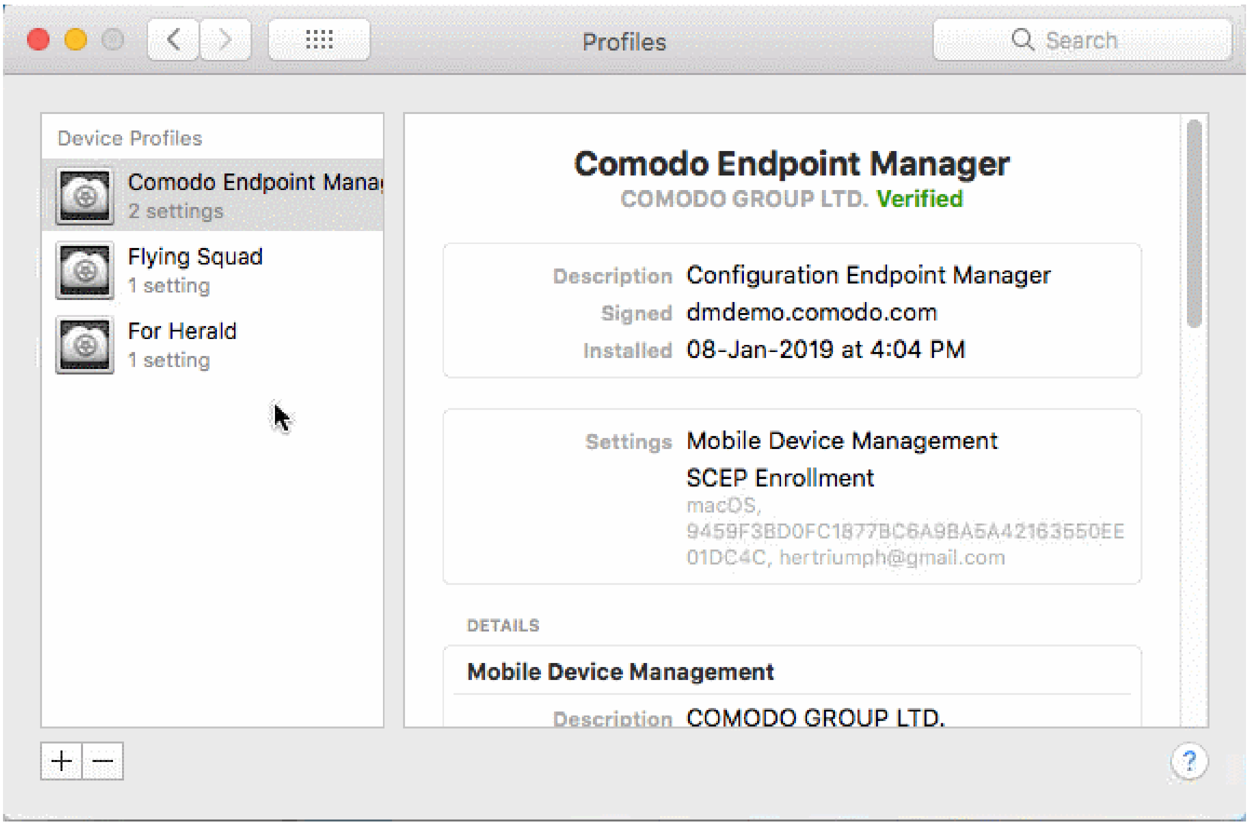


Welcome to the ITarian Communication Client Installer

You will be guided through the steps necessary to install this software, version 6.25.21740.19010.

- Follow the wizard to complete the installation.

The device profiles screen appears when installation is complete:



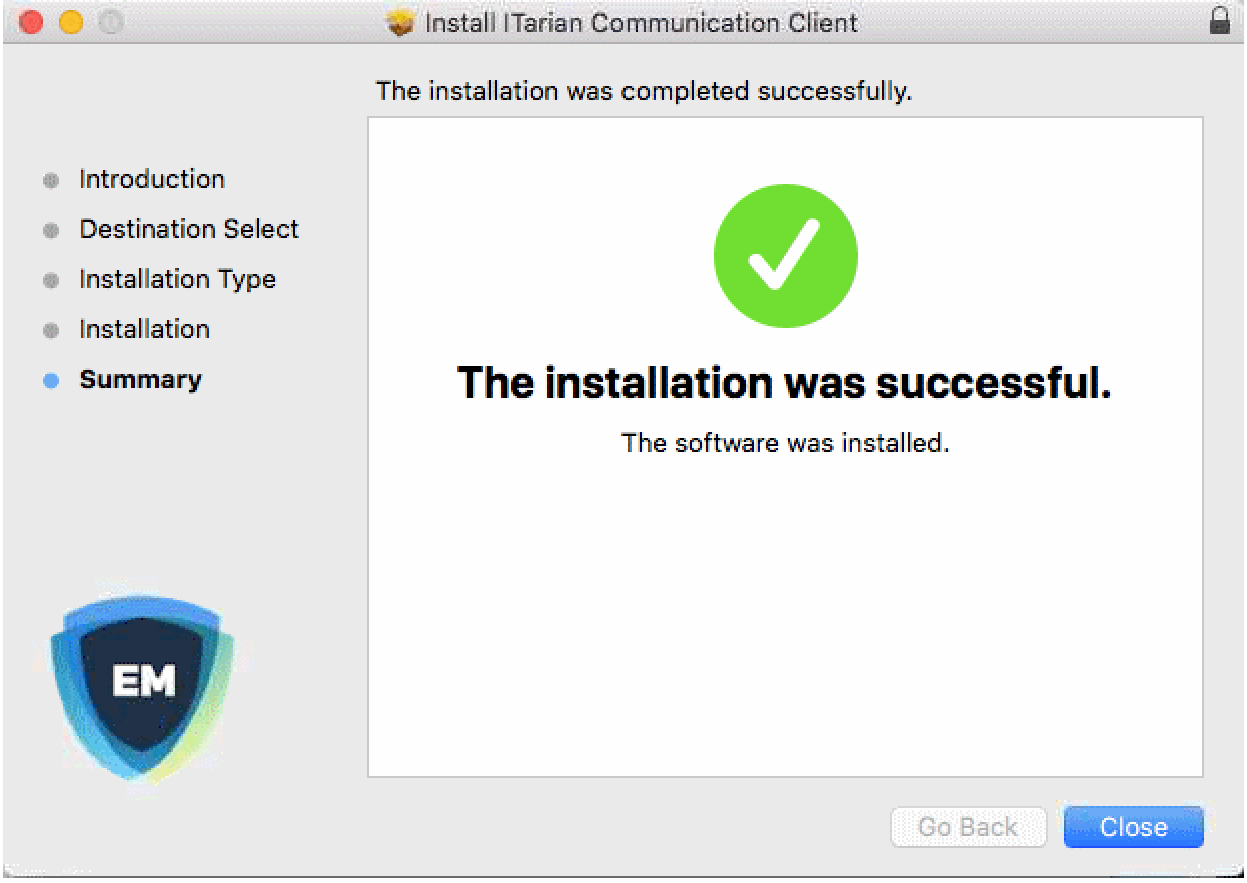
Comodo Endpoint Manager
COMODO GROUP LTD. Verified

Description Configuration Endpoint Manager
Signed dmdemo.comodo.com
Installed 08-Jan-2019 at 4:04 PM

Settings Mobile Device Management
SCEP Enrollment
macOS, 9459F3BD0FC1877BC6A9BA5A42163550EE 01DC4C, hertriumph@gmail.com

Mobile Device Management
Description COMODO GROUP LTD.

The client will connect to the EM server:



The installation was completed successfully.

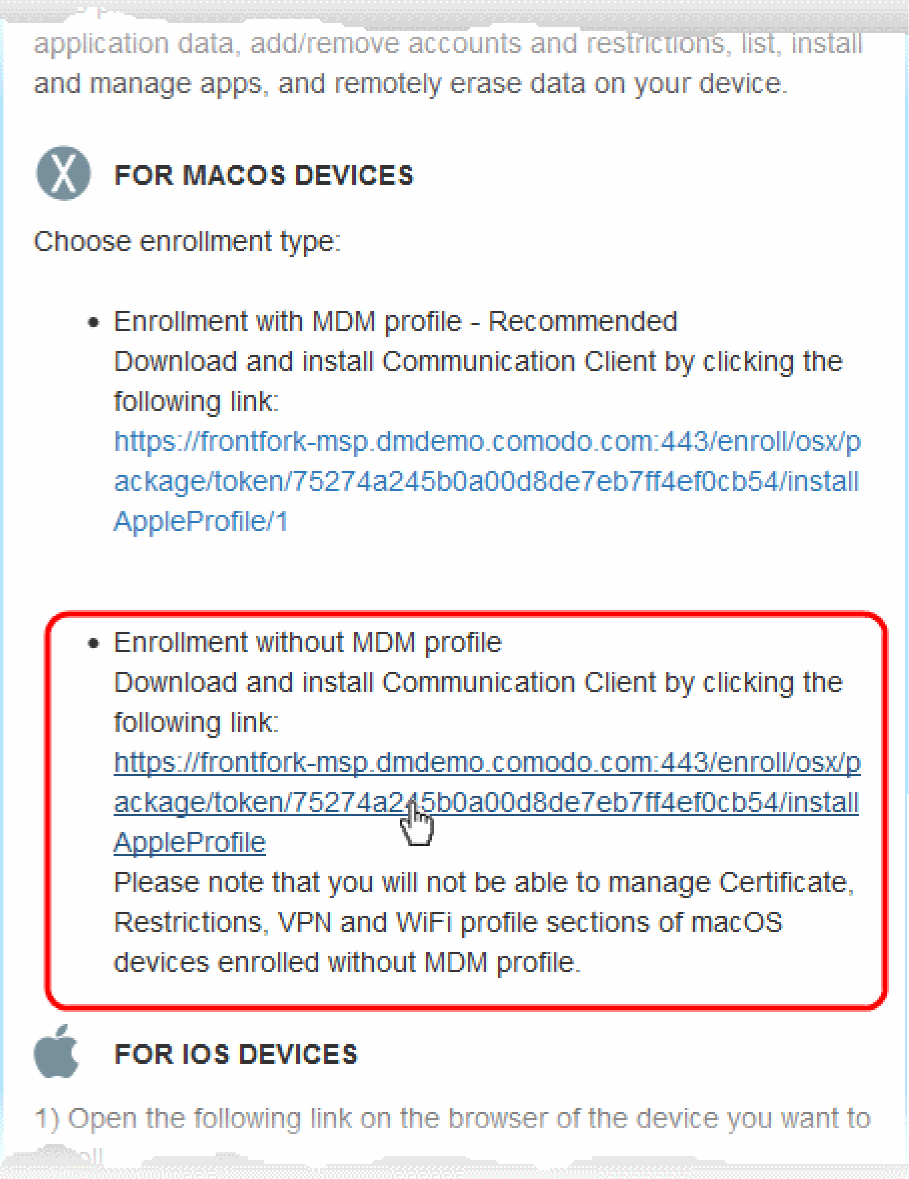
**The installation was successful.**

The software was installed.

The device is now enrolled to Endpoint Manager.

## Enroll without MDM Profile

- Open the enrollment mail on the device you want to add
- Click the link in the mail to open the device enrollment page
- Scroll down to the 'FOR MAC OS DEVICES' section.
- Open the link under 'Enrollment **without** MDM profile'



application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR MACOS DEVICES

Choose enrollment type:

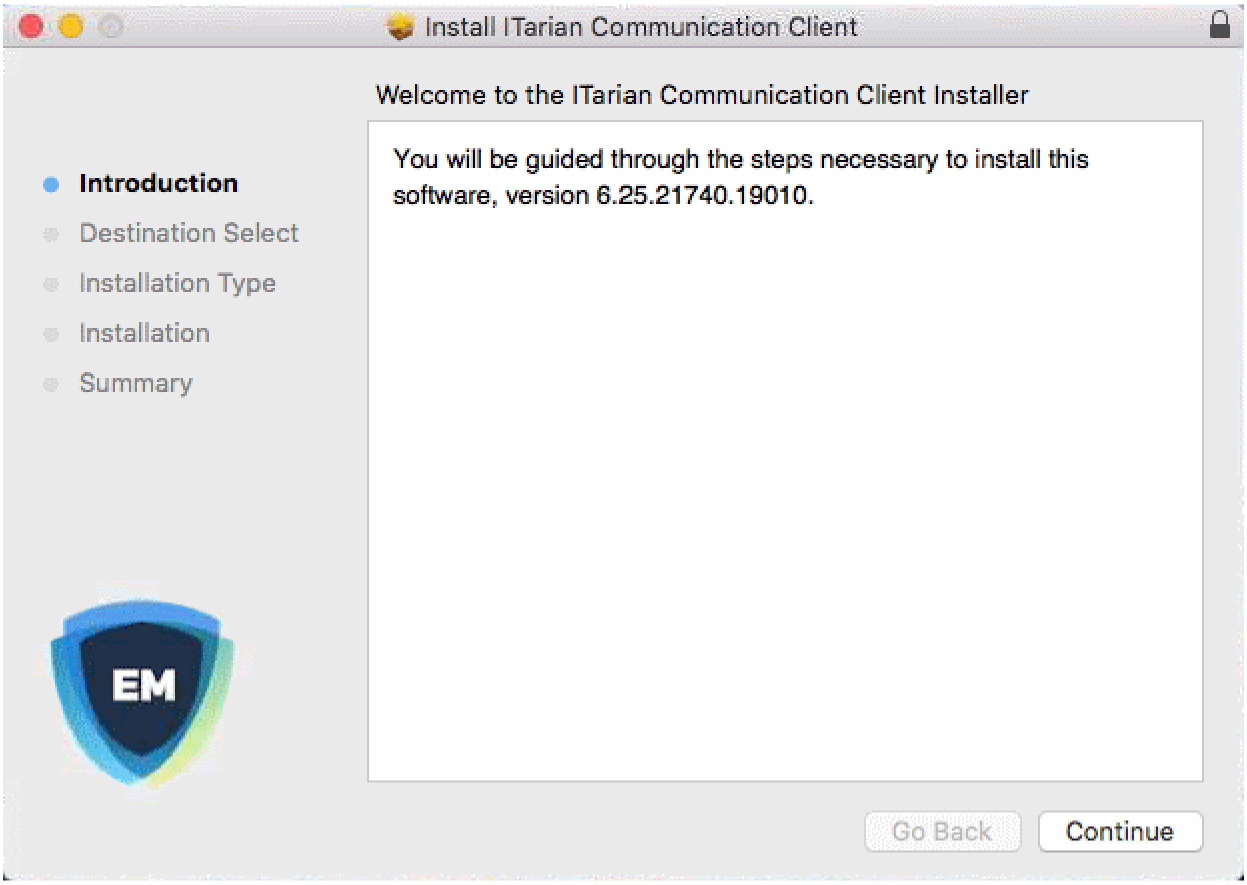
- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

FOR IOS DEVICES

1) Open the following link on the browser of the device you want to enroll

This will start the installation wizard:



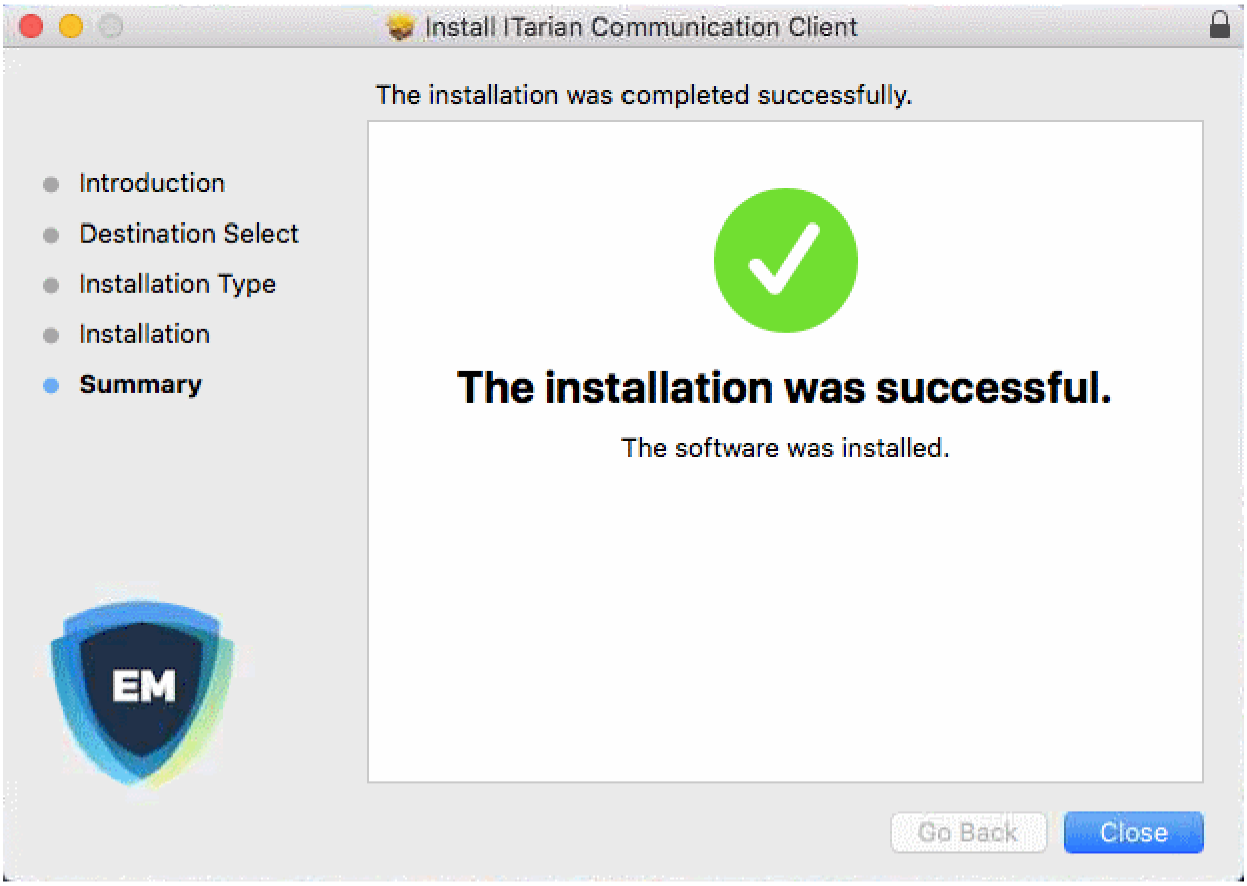
Install ITarian Communication Client

Welcome to the ITarian Communication Client Installer

You will be guided through the steps necessary to install this software, version 6.25.21740.19010.

- Follow the wizard to complete the installation

Once installation is complete, the client will connect to the EM server:



Install ITarian Communication Client

The installation was completed successfully.

The installation was successful.

The software was installed.

The device is now enrolled to Endpoint Manager.

## 2.5. Enroll Linux OS Endpoints

**Process in brief:**

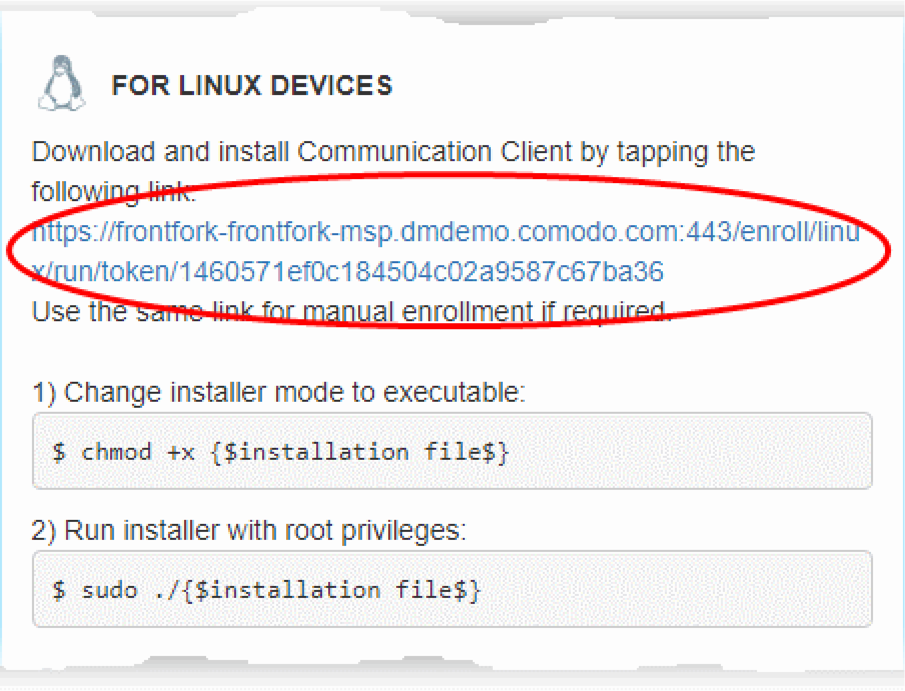
- Open the enrollment email on the Linux device you wish to enroll
- Click the link in the email to open the device enrollment page
- The device enrollment page contains a link to download the EM communication client.
- Download the client and install it on the device
- After installation, your device automatically connects to the Endpoint Manager server.

**Supported Linux OS**

- 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. You will be taken to open the device enrollment page
- Click on the link under 'For Linux Devices' and save the file:



FOR LINUX DEVICES

Download and install Communication Client by tapping the following link:
https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/linux/run/token/1460571ef0c184504c02a9587c67ba36
Use the same link for manual enrollment if required.

1) Change installer mode to executable:

```
$ chmod +x {$installation file$}
```

2) Run installer with root privileges:

```
$ sudo ./{$installation file$}
```

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 {$installation file$}

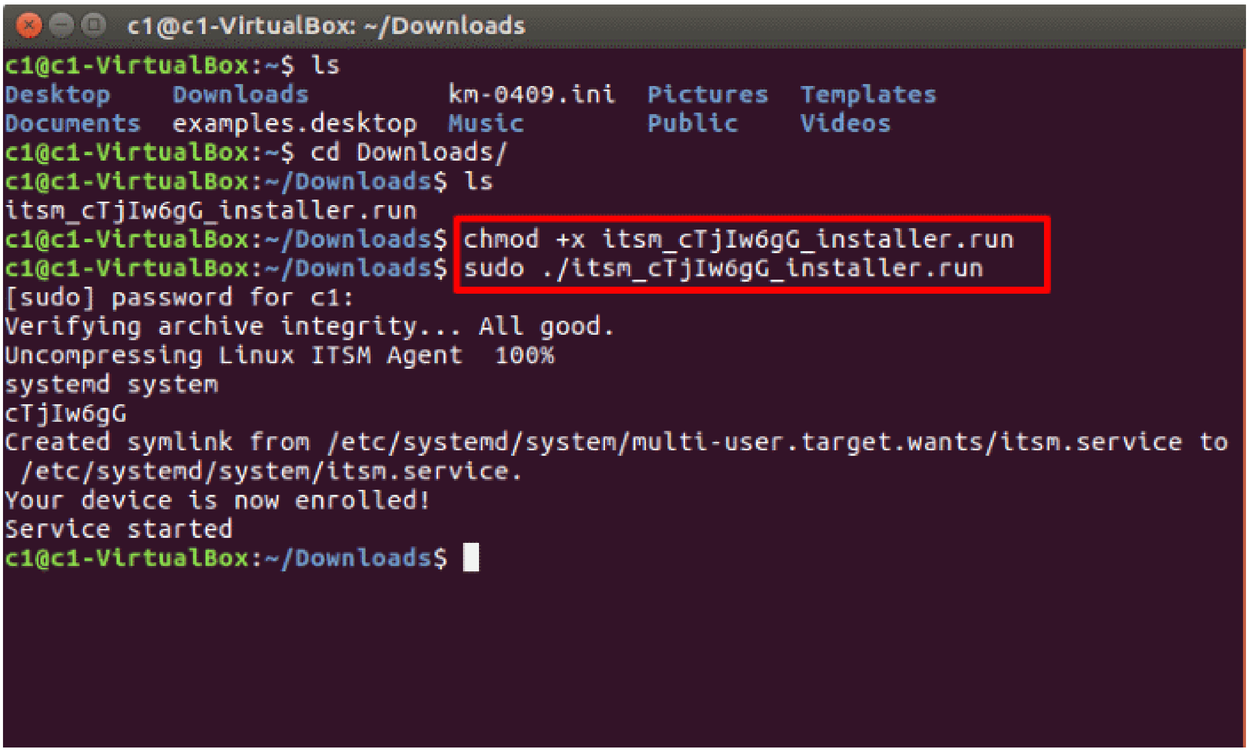
2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run



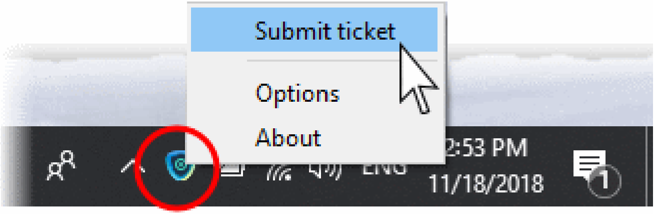
```
c1@c1-VirtualBox: ~/Downloads
c1@c1-VirtualBox:~$ ls
Desktop     Downloads           km-0409.ini  Pictures  Templates
Documents   examples.desktop    Music        Public    Videos
c1@c1-VirtualBox:~$ cd Downloads/
c1@c1-VirtualBox:~/Downloads$ ls
itsm_cTjIw6gG_installer.run
c1@c1-VirtualBox:~/Downloads$ 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$
```

- After installation, the communication client automatically connects to the EM server and enrolls the device.

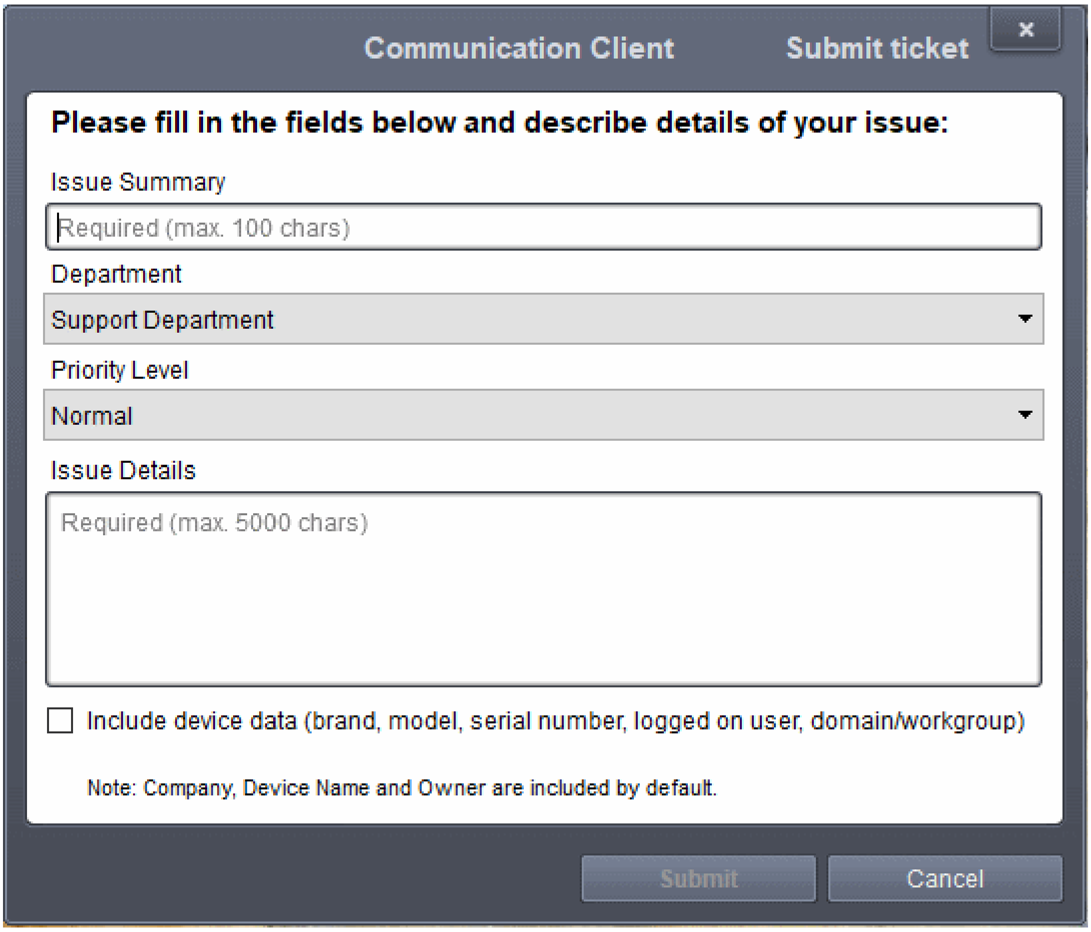
# 3.Create a Support Ticket

You can create a support ticket by right-clicking on the EM tray icon if you need help to resolve an issue.  A ticket will be created in Service Desk and assigned to the selected department.

- To submit a support ticket, right click on the communication client tray icon and select 'Submit ticket'



The 'Submit ticket' dialog opens:



Please fill in the fields below and describe details of your issue:

Issue Summary

Required (max. 100 chars)

Department

Support Department

Priority Level

Normal

Issue Details

Required (max. 5000 chars)

□ Include device data (brand, model, serial number, logged on user, domain/workgroup)

Note: Company, Device Name and Owner are included by default.

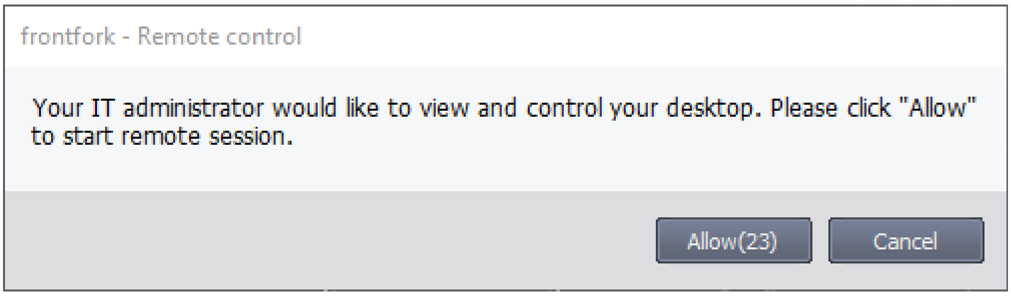
**Note**: Endpoint Manager allows administrators to rebrand the communication client (CC) with their company logo and details. The company name and the client name shown on the header may be different depending on the re-branding.

  - Issue Summary - Provide a short description of the issue.
  - Department - Select the department to whom the ticket should be assigned.
  - Priority Level - Select the priority from the drop-down. The levels are:  Low, Normal, High and Critical.
  - Issue Details - Provide a  detailed description of the issue.
- Click 'Submit'.

A support ticket will be created in Service Desk and assigned to the selected department.

# 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:



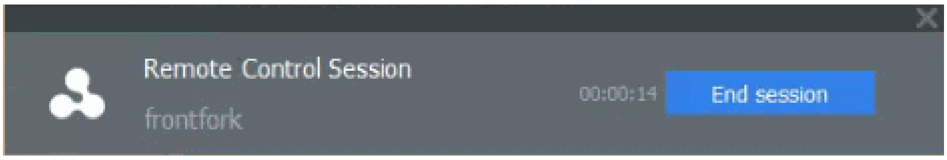
frontfork - Remote control

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

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:



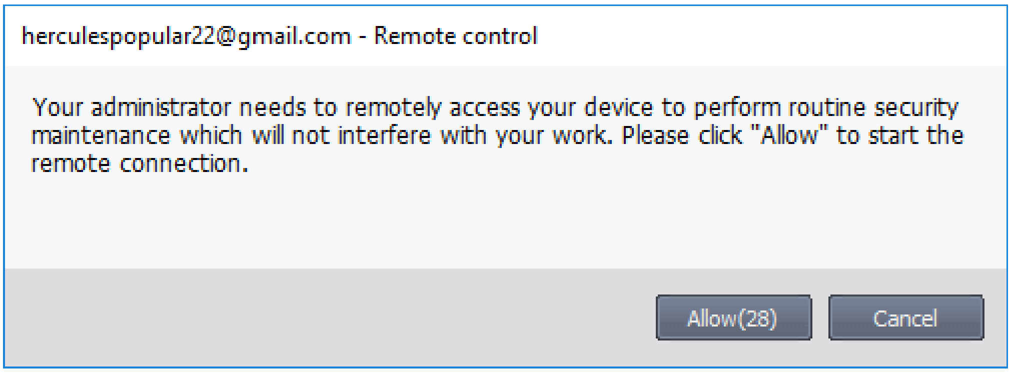
Remote Control Session

frontfork

- 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:



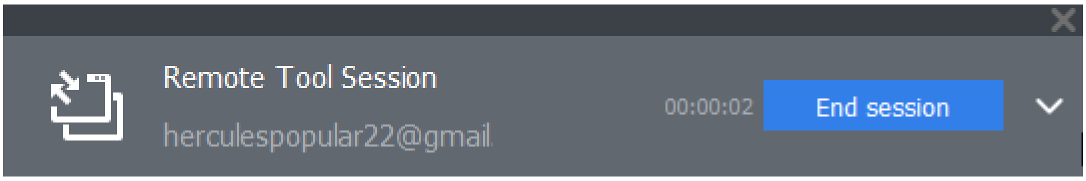
herculespopular22@gmail.com - Remote control

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work. Please click "Allow" to start the remote connection.

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

- Click 'Allow' to accept the remote control request

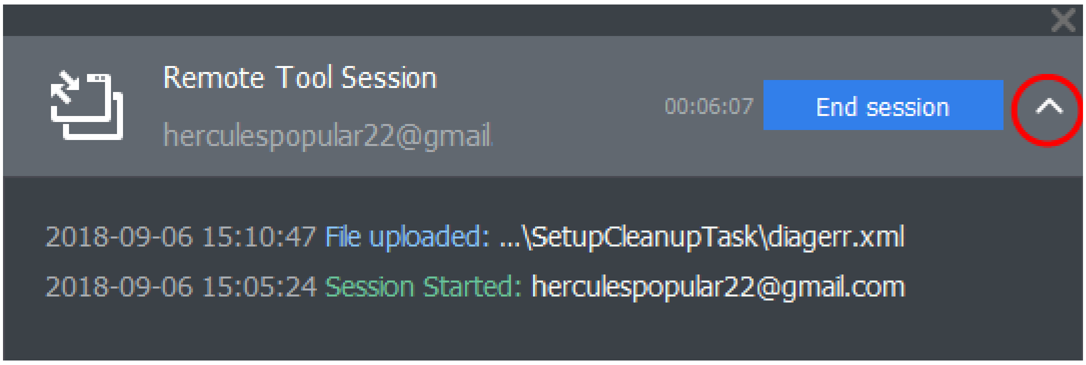
Once the connection is established, a notification appears on your desktop. The notification tells you who is connected to your computer and the duration of the session:



Remote Tool Session

herculespopular22@gmail

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



2018-09-06 15:10:47 File uploaded: ...\SetupCleanupTask\diagerr.xml

2018-09-06 15:05:24 Session Started: herculespopular22@gmail.com

- 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**