COMODO
Creating Trust Online®

Comodo
Endpoint Manager

Software Version 6.33

Quick Start Guide

Guide Version 6.33.012720

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Endpoint Manager - Quick Start

This tutorial explains how to add users and devices, create device groups and deploy configuration profiles.

Note - Endpoint Manager needs to communicate with Comodo servers and managed devices in order to send commands and run updates. You need to configure your firewall accordingly to allow these connections. Required IPs, host-names and ports are provided in **Appendix 1a** and **Appendix 1b** of the Admin Guide.

Step 1 - Enrollment and Configuration

Existing Comodo Dragon and Comodo One customers

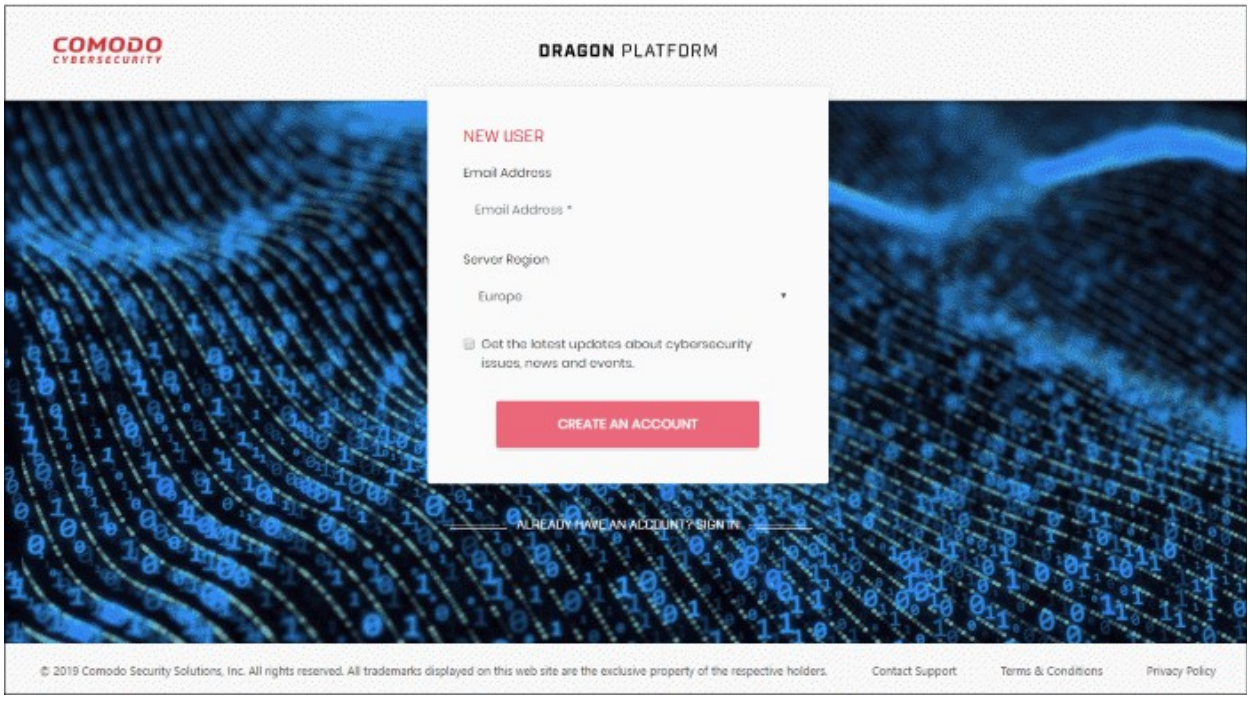
- Log in to your Comodo Dragon / Comodo One account
- Click 'Licensed Applications' > 'Endpoint Manager'.

New customers

You can subscribe for Endpoint Manager from Comodo Dragon or Comodo One.

Comodo Dragon

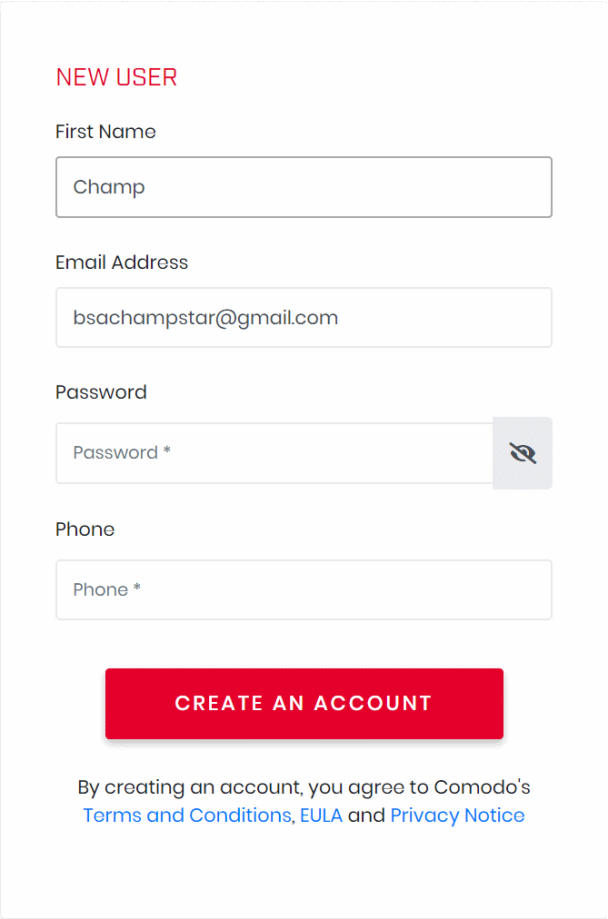
- Visit **https://platform.comodo.com/signup**



- Enter your email address. This will be used as your Comodo Dragon username.
- **Server Region** - Dragon Platform servers are located in two regions - Europe and the USA.

- Select your region
- You will be automatically directed to the selected region on logging in to your account.

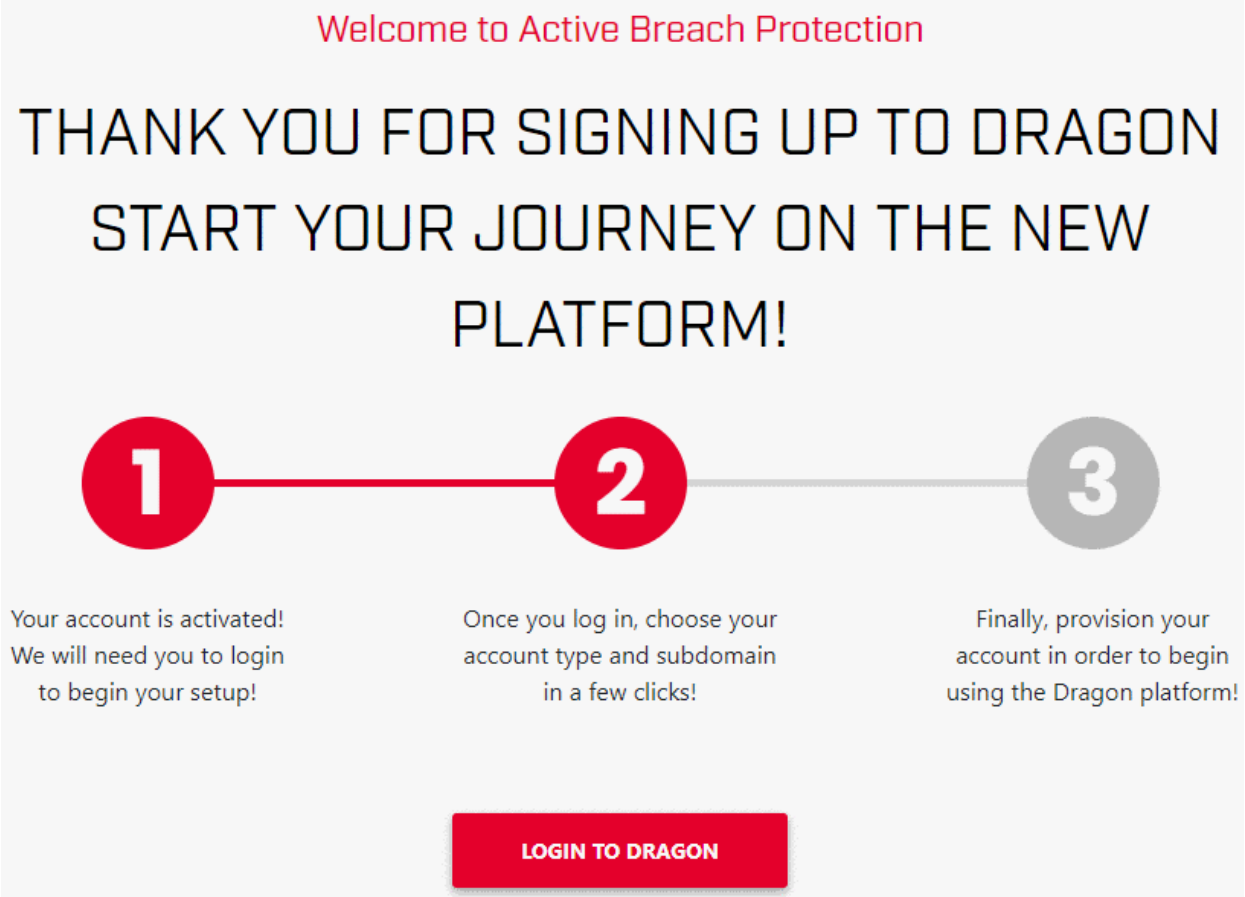
- **Get the latest updates about...**. - Select to receive news and product notifications.
- Click 'Create an Account'
- Next, complete the short registration form:



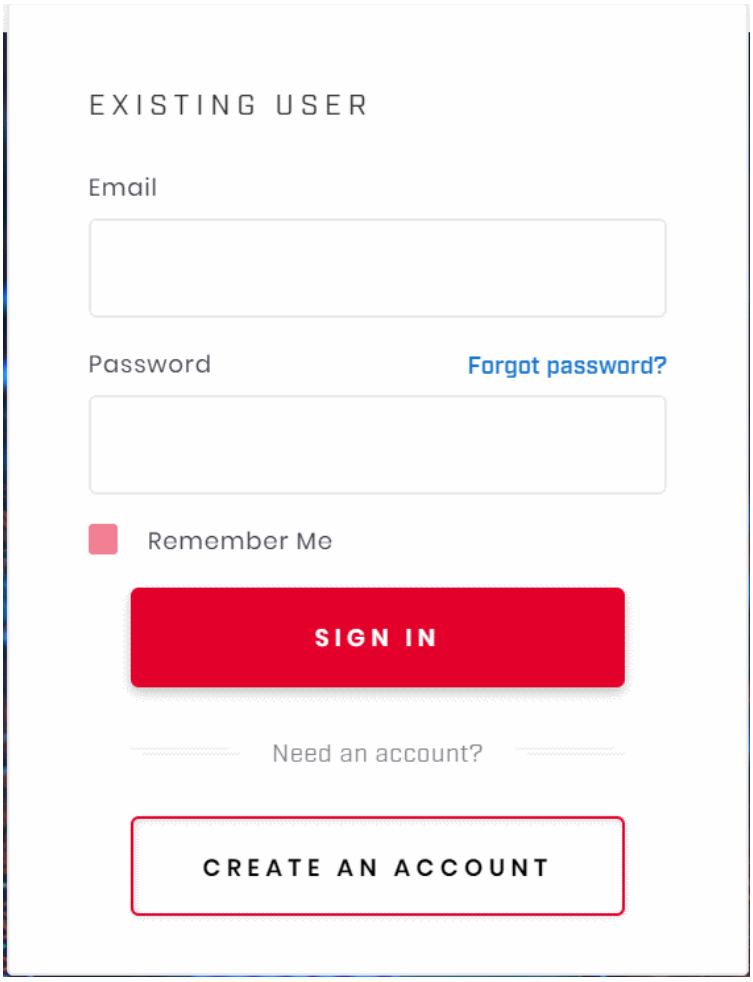
- **First Name -** Enter your name
- **Email** - This is pre-populated with the address you provided in the previous step. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
- **Password** - Create a password for your CD or C1 account. Passwords must:

  - Be at least eight characters long
  - Contain a mix of lower case and upper case letters
  - Contain at least one numeral
  - Contain at least one of the following special characters -)("!#$%^&*"
- **Telephone Number** - Primary contact number
- **End User License Agreement**: Read the EULA fully by clicking the 'terms and conditions', 'EULA' and 'Privacy Notice' links.

Click 'Create an Account'.



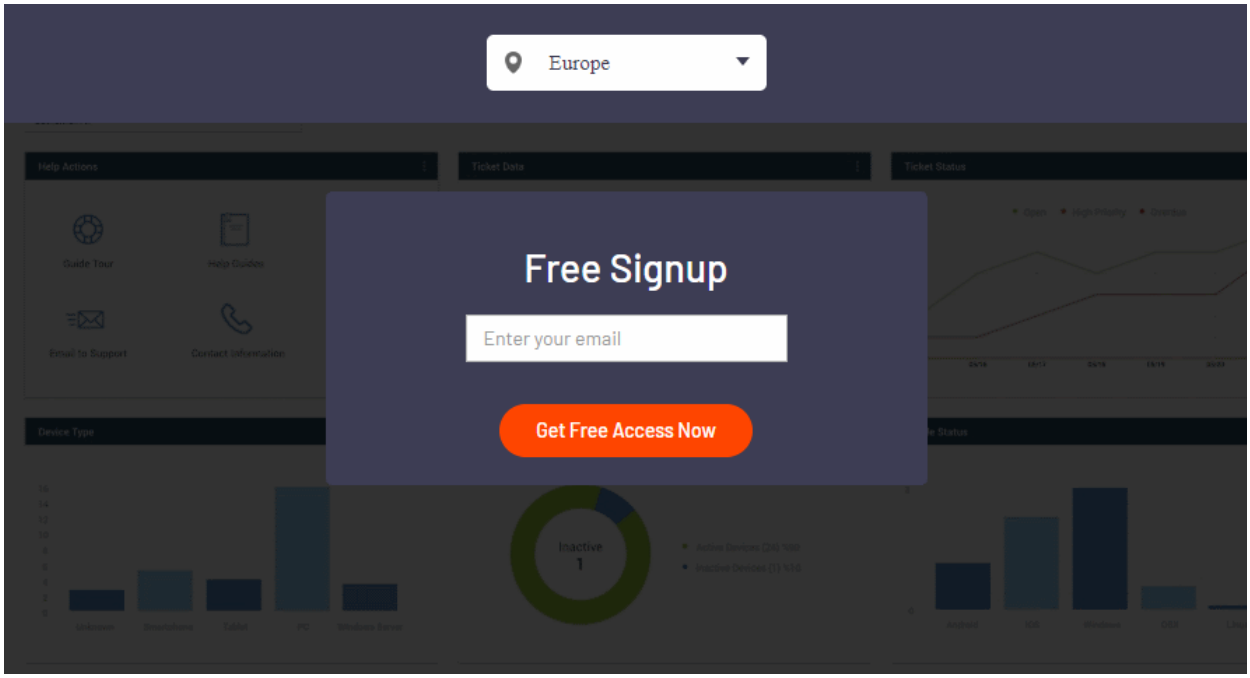
- Click 'Login to Dragon'



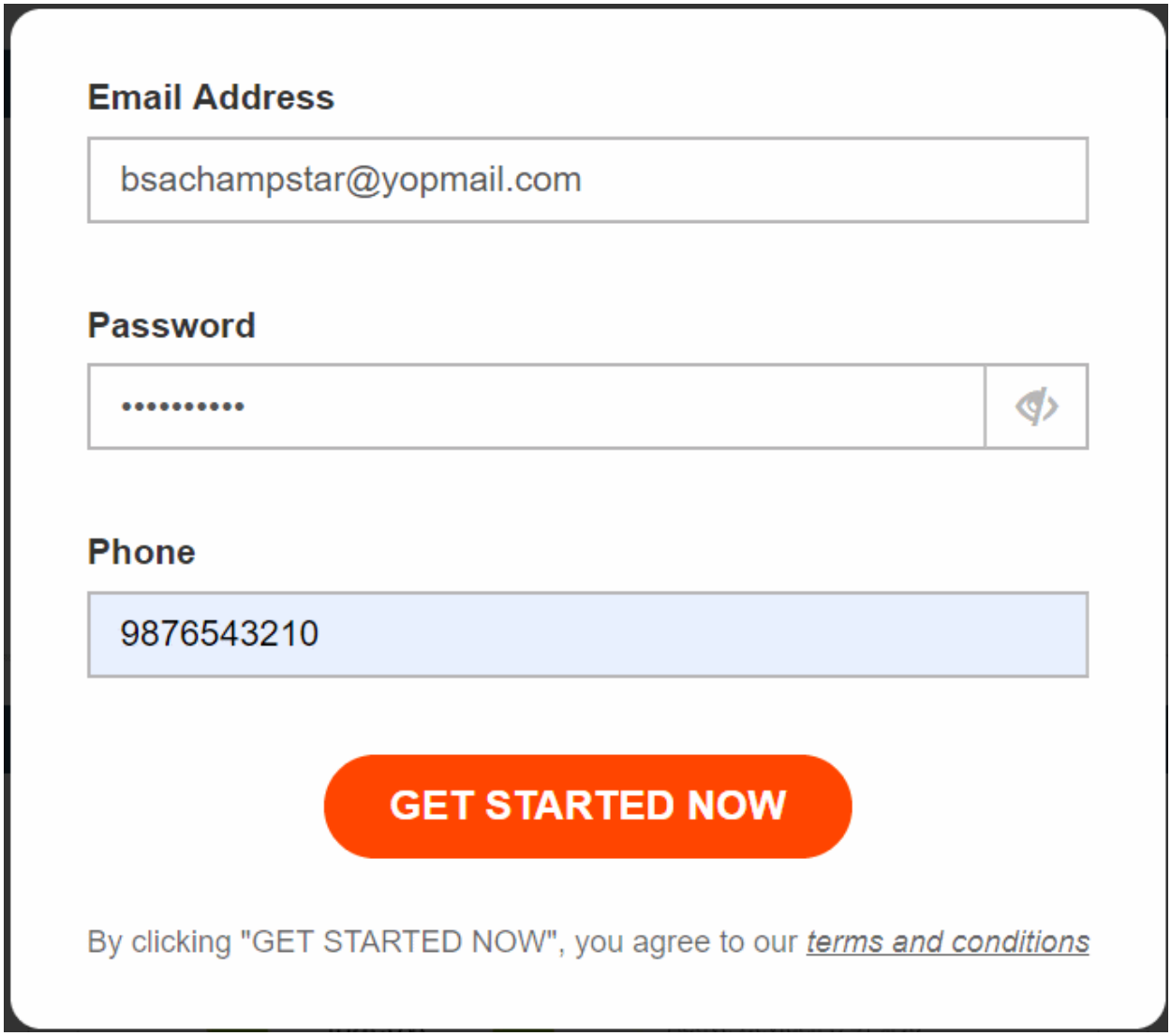
- Enter your username (email address from earlier), and your password
- Click 'Sign-in'
- You will be taken to the **product selection wizard**.

Comodo One:

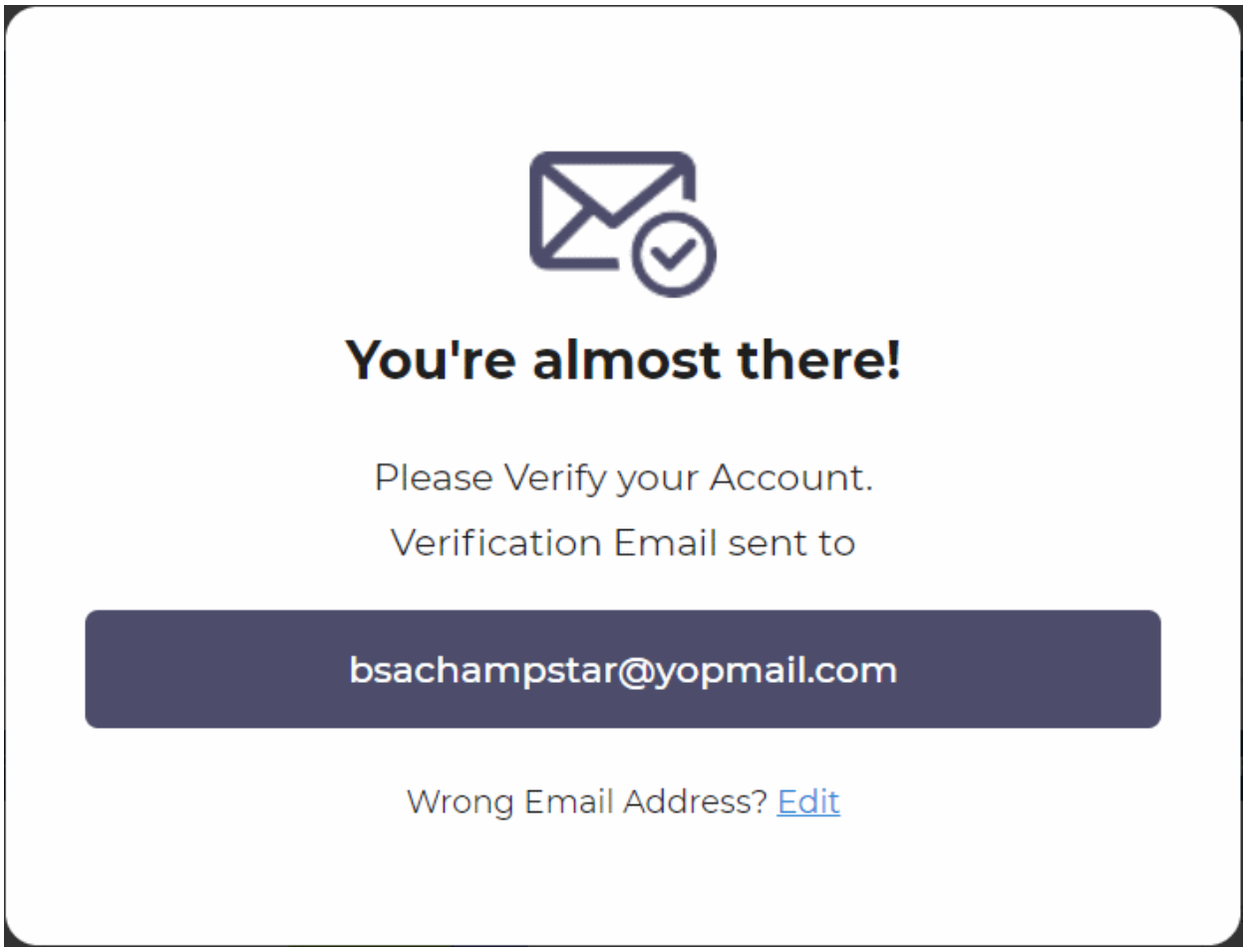
- Visit **https://one.comodo.com/signup/**



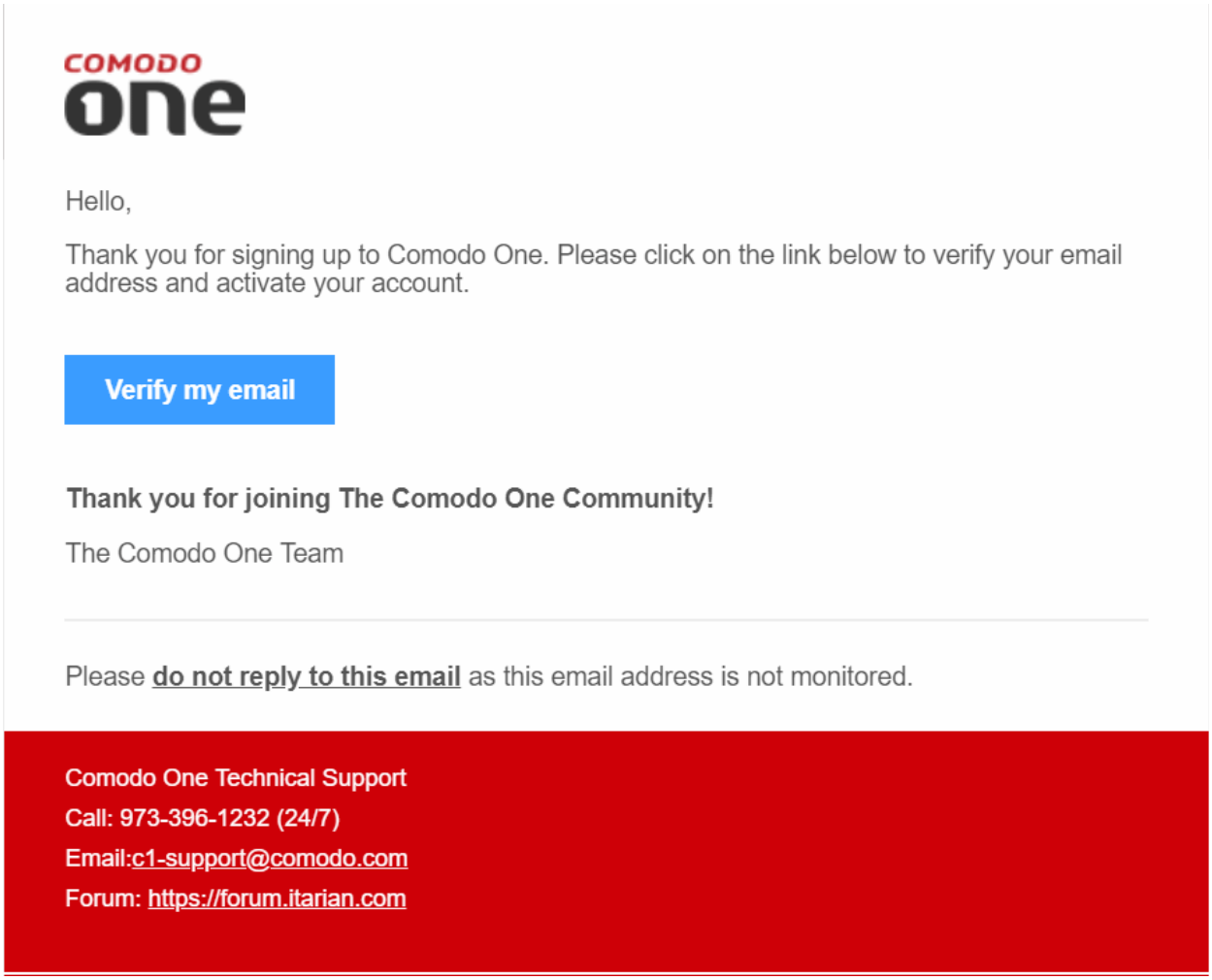
- Comodo One servers are located in two regions, Europe and the USA. Select the region suitable for you.
- Enter your email address
- Click 'Get Free Access Now'
- Next, complete the short registration form:



  - **Email** - This is pre-populated with the address you provided in the previous step. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
  - **Password** - Create a password for your CD or C1 account. Password rules:
    - At least eight characters long
    - Contain a mix of lower case and upper case letters
    - Contain at least one numeral
    - Contains at least one of the following special characters - '("!#$%^&*")'
  - **Telephone Number** - Primary contact number
  - **End User License Agreement** - Read the EULA fully by clicking the 'terms and conditions' link.
- Click 'Get Started now'.

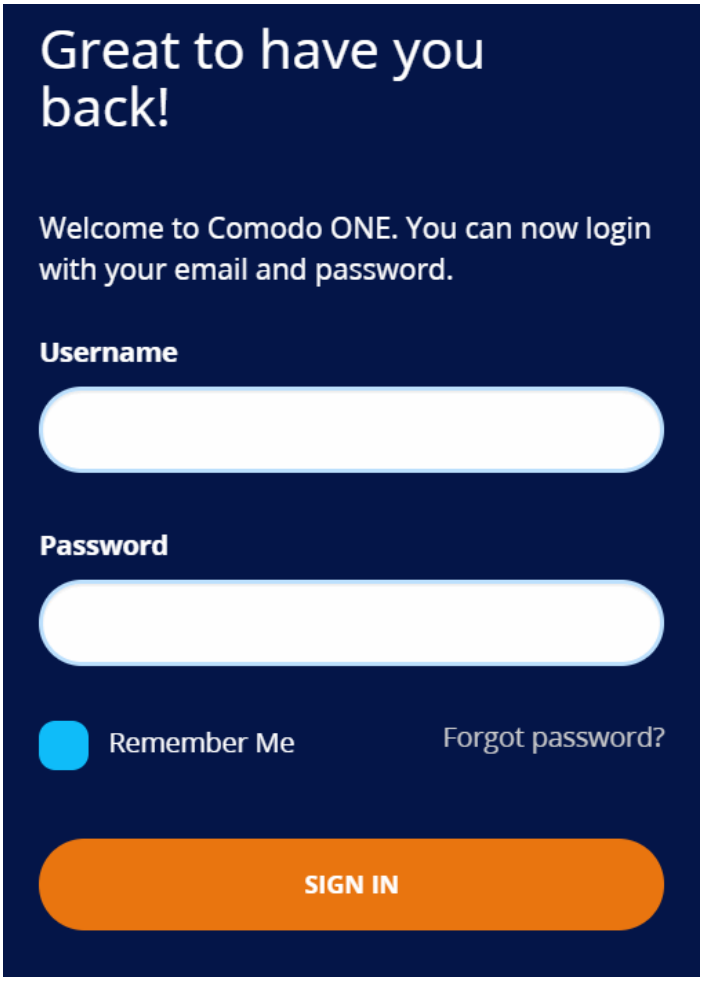


- An account confirmation email is sent to your address. An example is shown below:



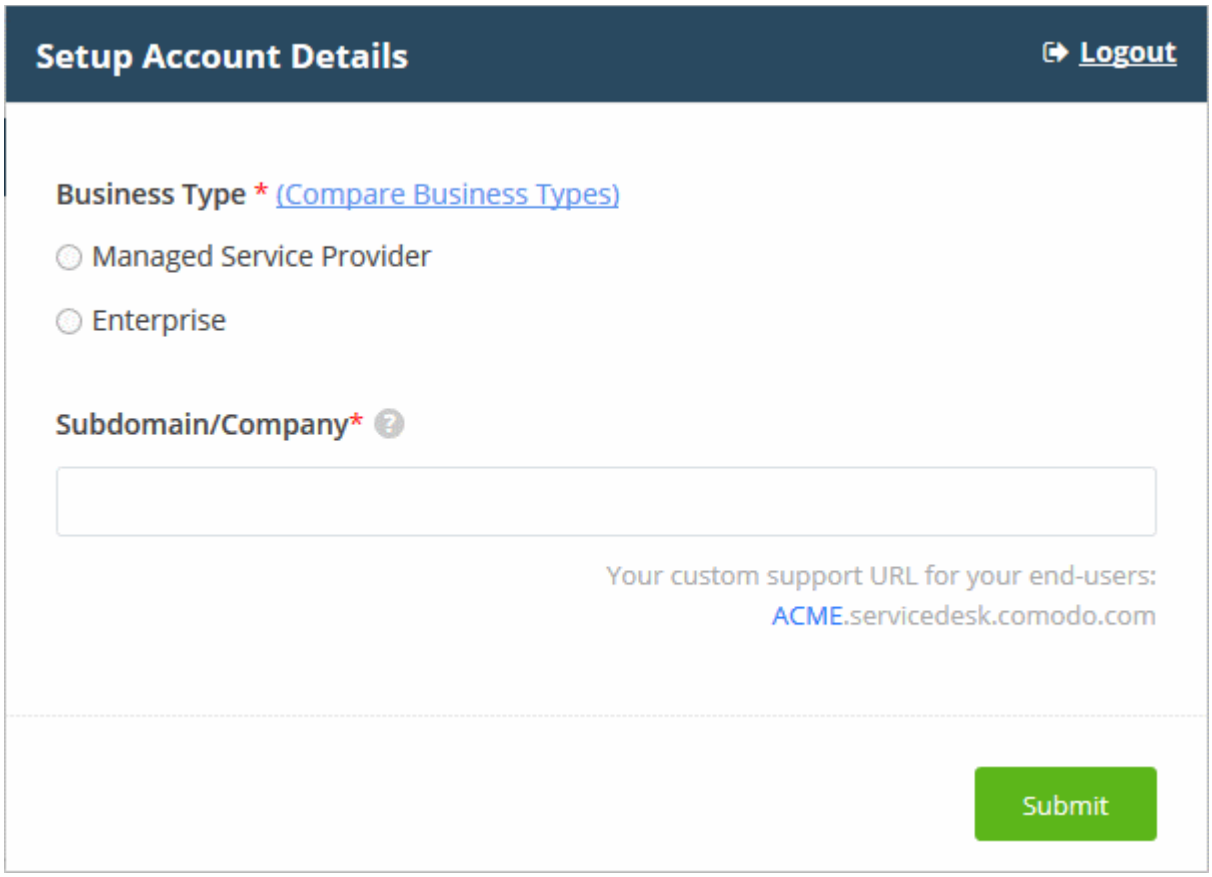
- Click 'Verify my email' to activate your account.

You will be taken to the C1 login page after successful verification:



- Enter your username (your email address), and your password
- Click 'Sign-in'
- You will be taken to the **product selection wizard**.

Product Selection Wizard



- **Business Type** - Choose the version of Comodo Dragon / Comodo One you require.
  The modules that come with each version are as follows:

MSP	Enterprise
Modules included in the Base package	
Service Desk Endpoint Manager (EM) Dome Shield	Service Desk Endpoint Manager (EM) Dome Shield
Modules that can be added to the base package	
Acronis Cloud Backup Quote Manager Customer Relationship Management (CRM) cWatch Comodo Dome Secure Web Gateway Comodo Dome Antispam MSP Comodo Dome Firewall Central Manager Comodo Dome Firewall Virtual Appliance cWatch EDR	Acronis Cloud Backup Quote Manager Customer Relationship Management (CRM) cWatch Comodo Dome Secure Web Gateway Comodo Dome Data Protection Comodo Dome Firewall Central Manager Comodo Dome Firewall Virtual Appliance Comodo Dome Antispam cWatch EDR

- **Subdomain** - Type the sub-domain domain you want to use for your account. The sub-domain forms part of

the URL you will use to access EM.

- For example, if you enter the sub-domain 'dithers'
- You will access Endpoint Manager at https://dithers.cmdm.comodo.com

- Click 'Submit'

The next screen shows a summary of your active services:

- Click 'OK' to finish setup. You will be taken to the console dashboard.
- Click 'Licensed Applications' > 'Endpoint Manager' to open the EM console
- This account you are currently logged in with is the 'Account Admin'. This is the master account and cannot be deleted. You can create product admins and staff under this account.
  - Dragon users can login at **https://platform.comodo.com/app/login**

- C1 can login at **https://one.comodo.com/app/login**
- Standalone EM users can login at https://<company name>.cmdm.comodo.com/

Step 2 - Configure EM Communications

You need to install an Apple Push Notification (APN) certificate and a Google Cloud Messaging (GSM) token on your portal so Endpoint Manager can communicate with your managed devices.

The following sections explain how to:

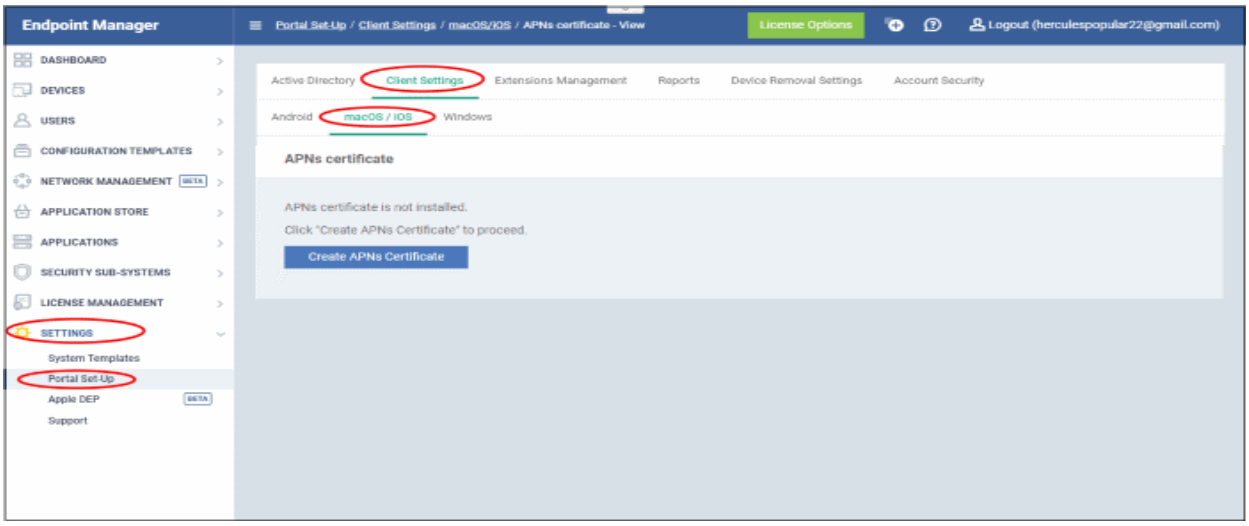
- **Add an APN Certificate**
- **Add a GCM Token**

Add Apple Push Notification certificate

- You need an Apple Push Notification (APN) certificate on your EM instance if you wish to manage iOS or Mac devices.
- You can enroll for an APN certificate using your Apple account. If you do not have an Apple account then please create one at **https://appleid.apple.com**. A free account is enough.
- The certificate is valid for one year. Endpoint Manager will remind you when your certificate is nearing expiry. It is free to renew the certificate each year.
- Follow the steps below to obtain and install an APN certificate:

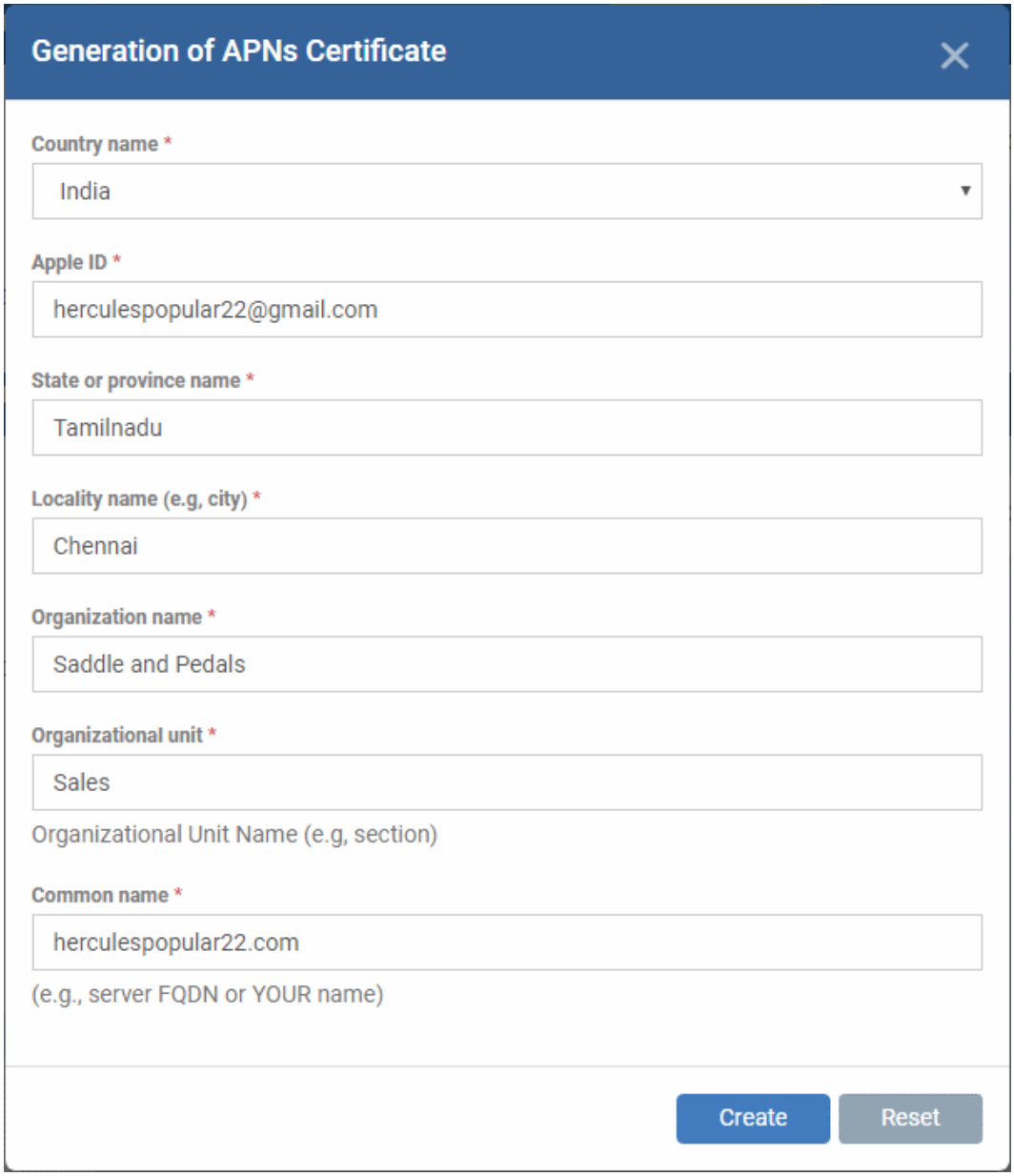
Step 1- Generate your PLIST

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click the 'macOS / iOS' tab.

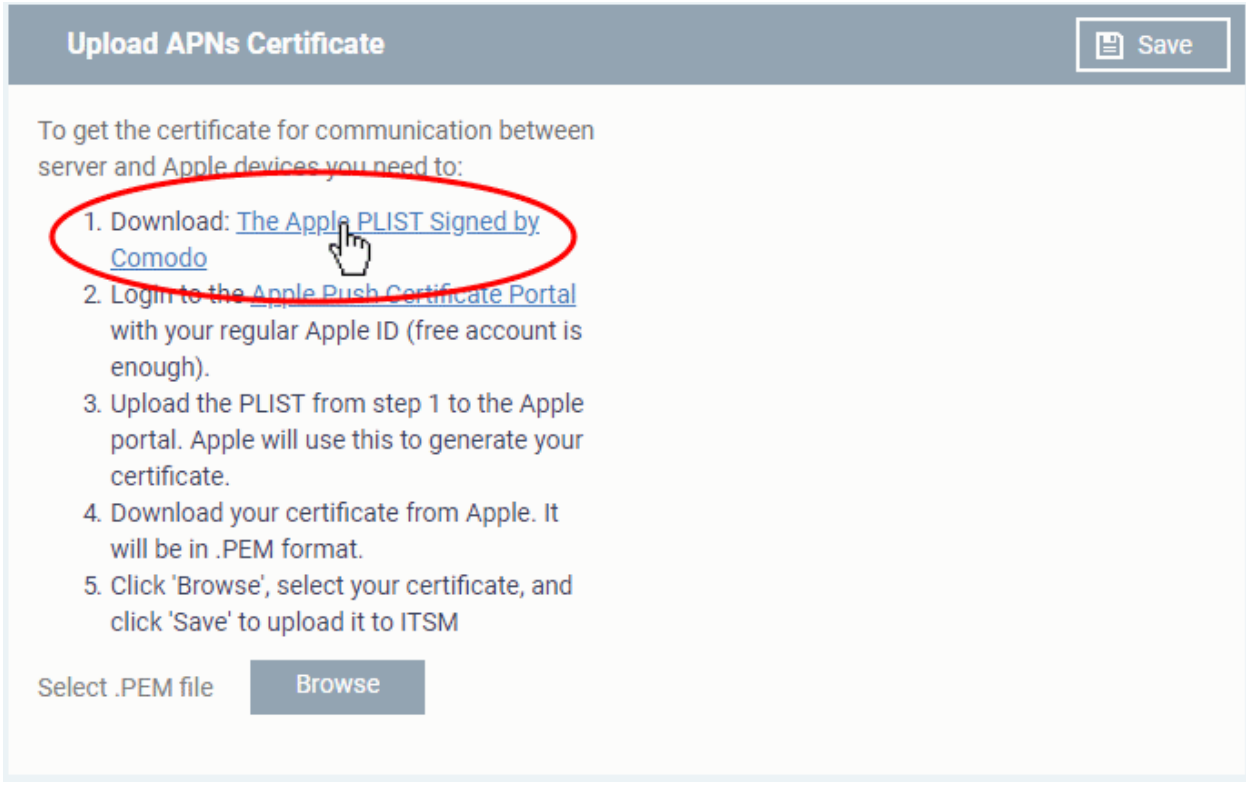


- Click 'Create APNs Certificate' to open the APNs application form.

Complete the application form to generate a certificate signing request (CSR):



- Complete all fields marked with an asterisk. The information in these fields will go into your certificate, so be as accurate as possible.
- Click 'Create'.
- This will send a request to Comodo to sign the CSR and generate an Apple PLIST.
- Usually your request will be fulfilled in seconds:

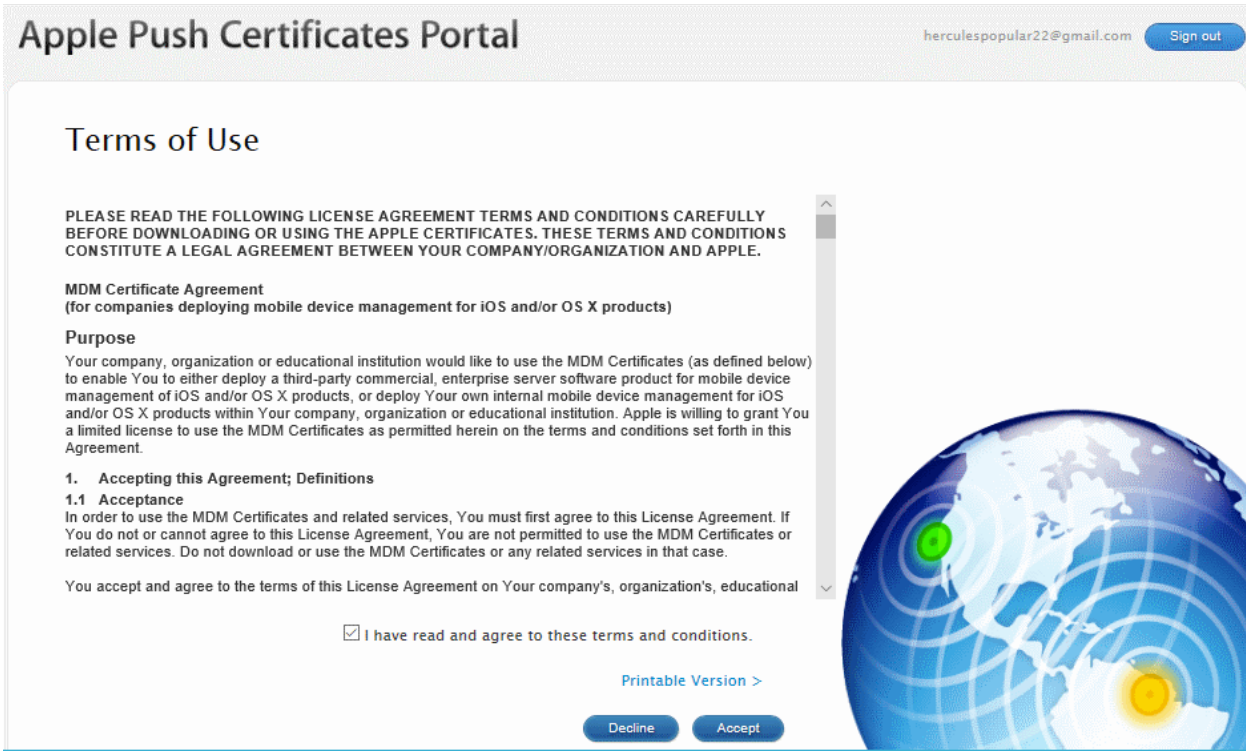


- Download the PLIST from the link in step 1. This is a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.
- Next, you need to submit this list to Apple to obtain your APN certificate.

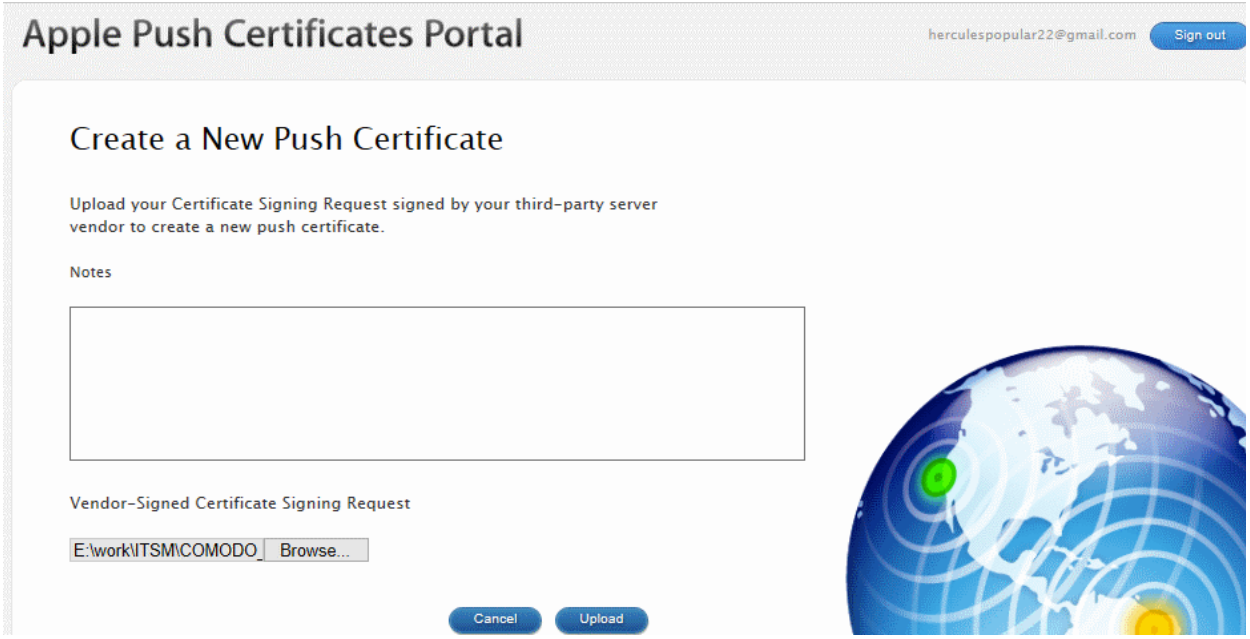
Step 2 - Obtain Your Certificate From Apple

- Login to the 'Apple Push Certificates Portal' with your Apple ID at **https://identity.apple.com/pushcert/**.
- If you do not have an Apple account then please create one at **https://appleid.apple.com**.
- Once logged in, click 'Create a Certificate'.

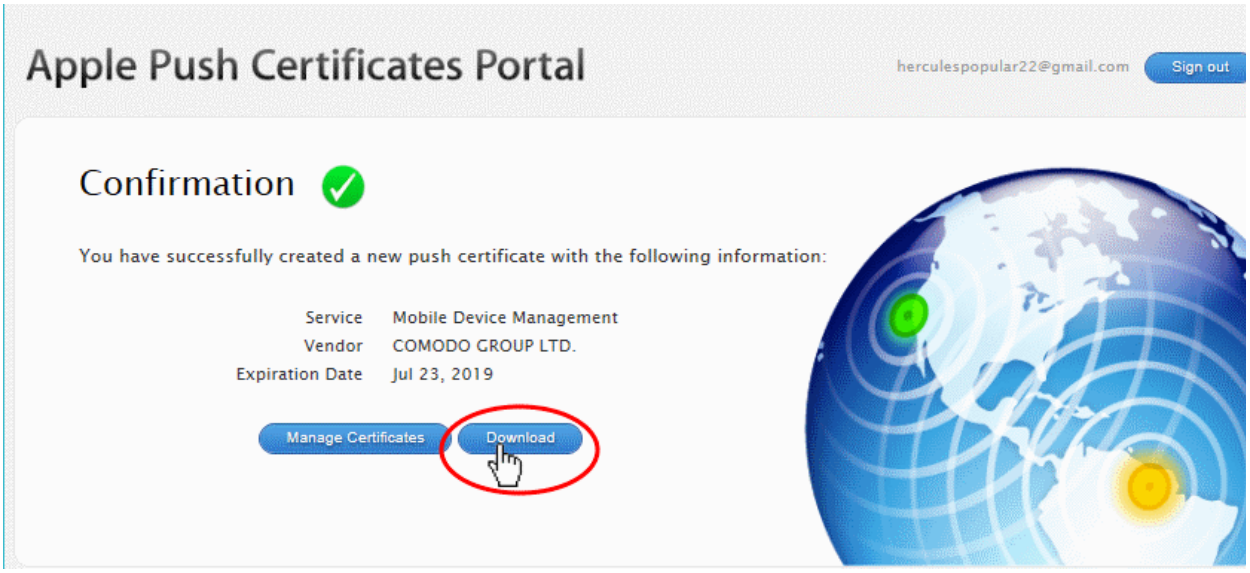
You will need to agree to Apple's EULA to proceed.



- On the next page, click 'Choose File', navigate to the location where you stored 'COMODO_Apple_CSR.csr' and click 'Upload'.



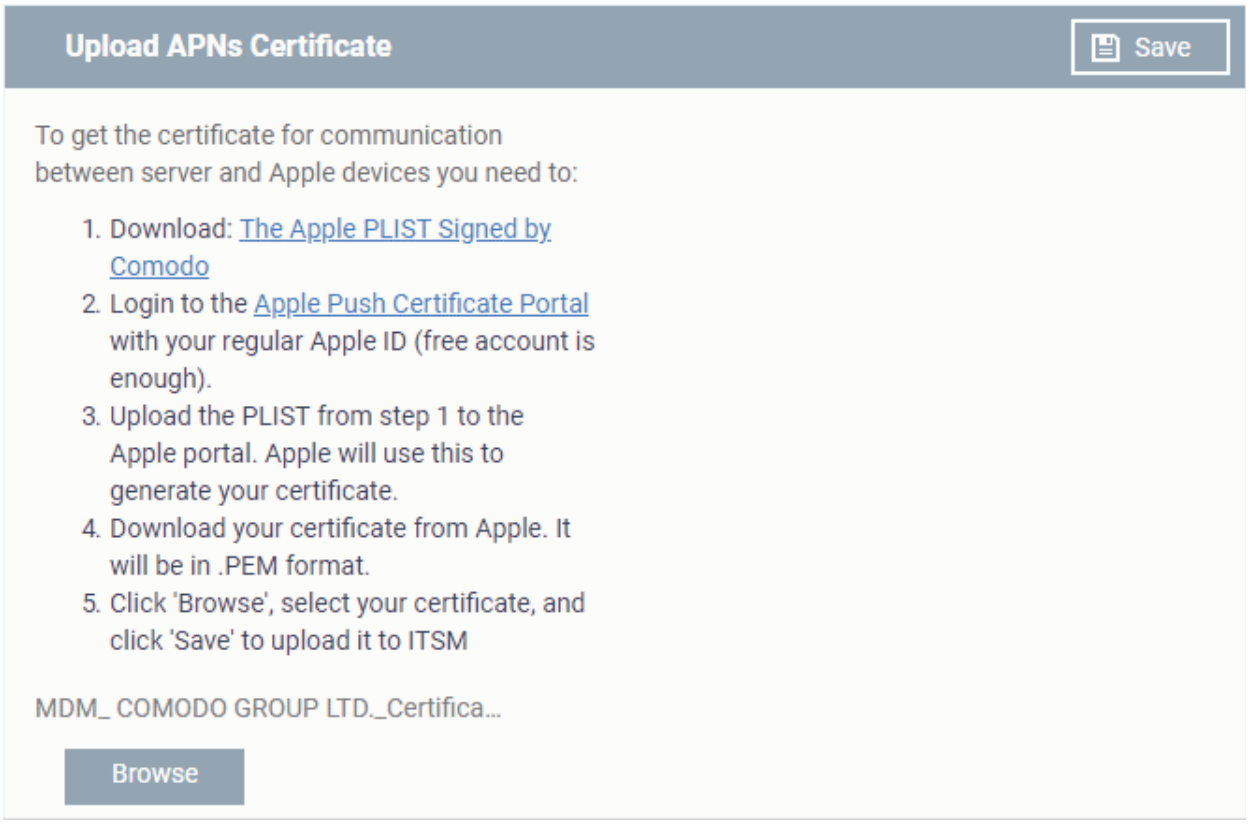
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



- Click the 'Download' button and save the certificate to a secure location. It is a .pem file with a name similar to 'MDM_COMODO GROUP LTD._Certificate.pem'

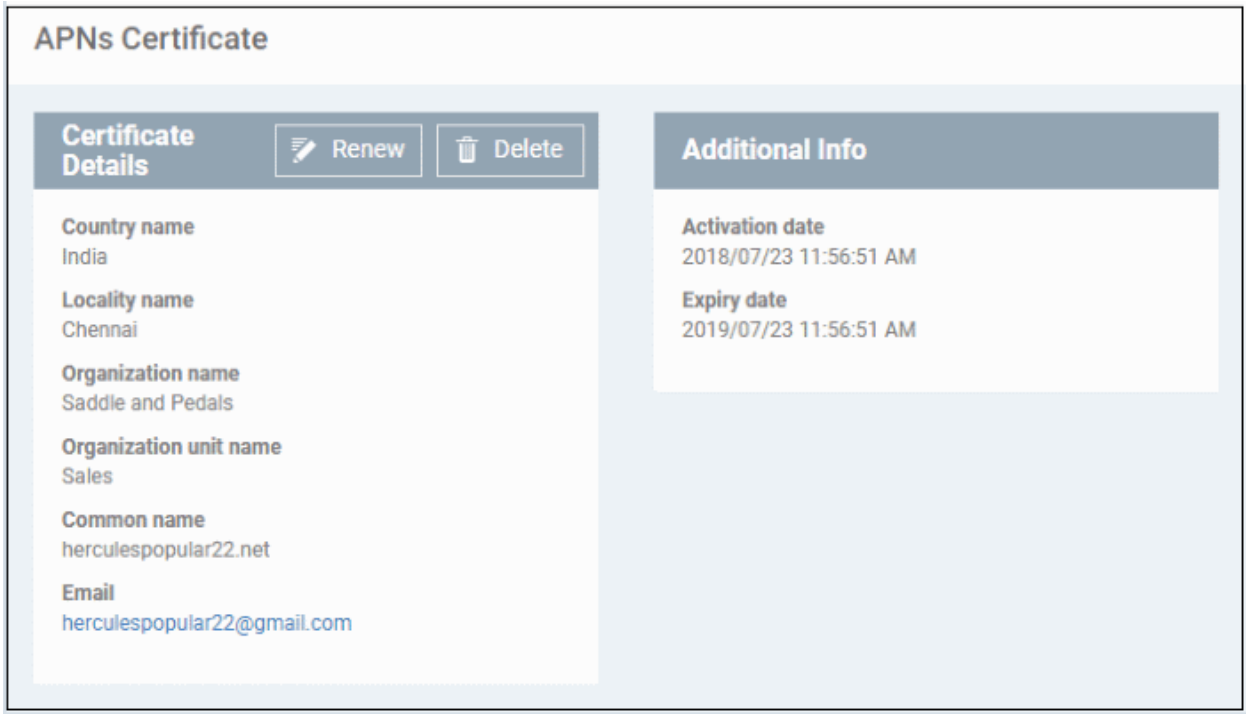
Step 3 - Upload your certificate to EM

- Return to EM, click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'macOS / iOS'
- Click the 'Browse' button, locate your certificate file and select it.



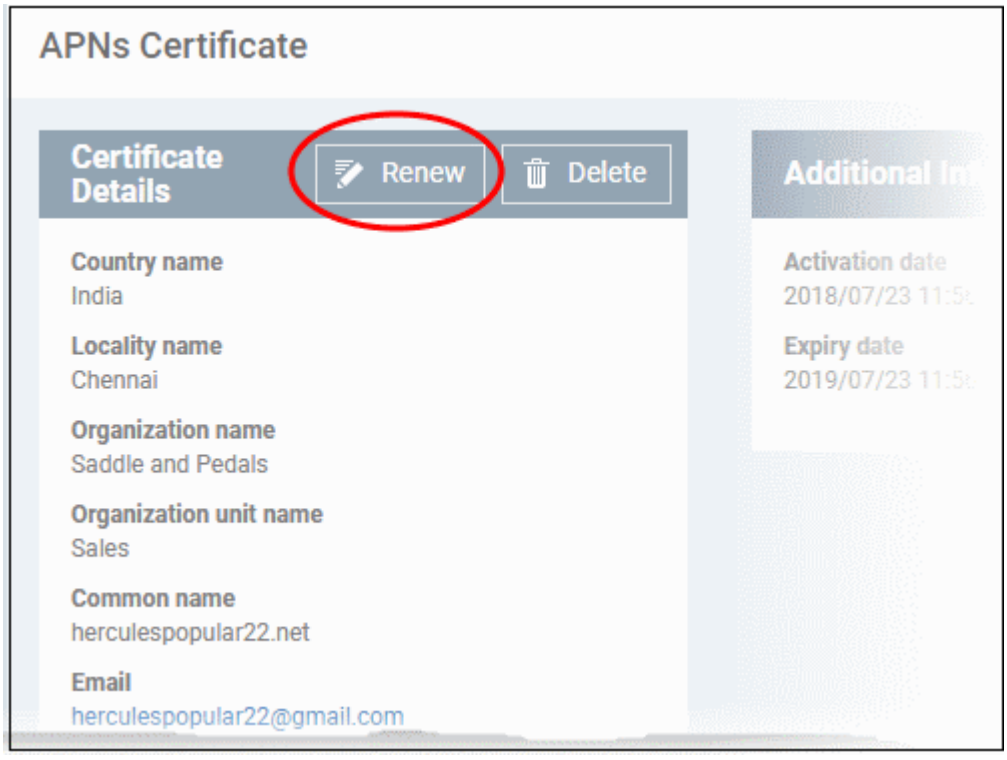
- Click 'Save' to upload your certificate.

The certificate details box shows your certificate fields and the start/end dates:



Endpoint Manager can now communicate with iOS and Mac OS devices. You can enroll iOS devices and Mac OS devices for management.

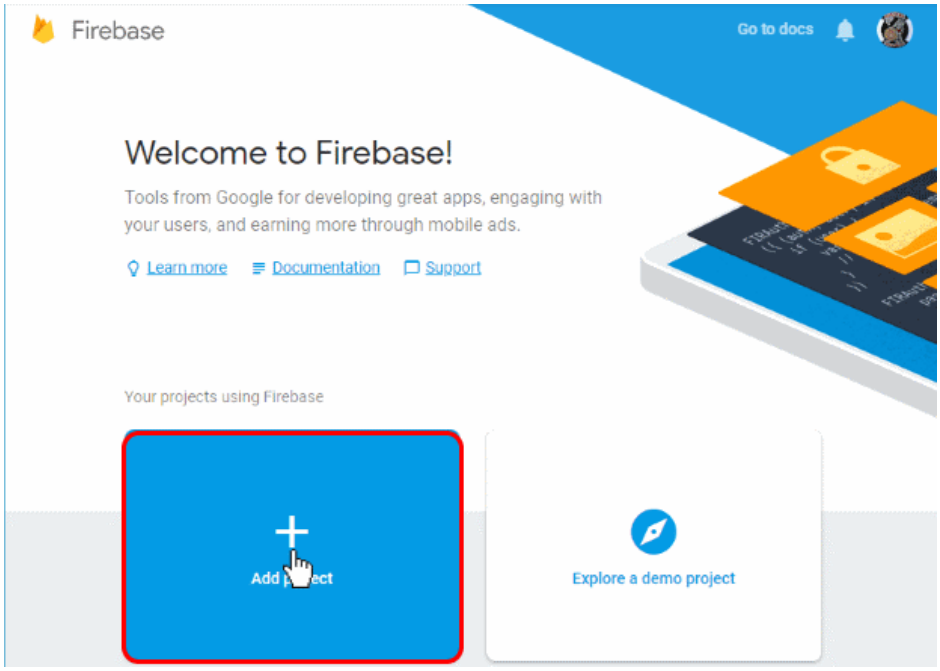
- The certificate is valid for 365 days. EM will remind you when your certificate is due to expire.
- We advise you renew your certificate at least 1 week before expiry. If it is allowed to expire, you will need to re-enroll all your iOS and Mac devices.
    - Click 'Renew' in the APNs certificate details interface to renew the cert:



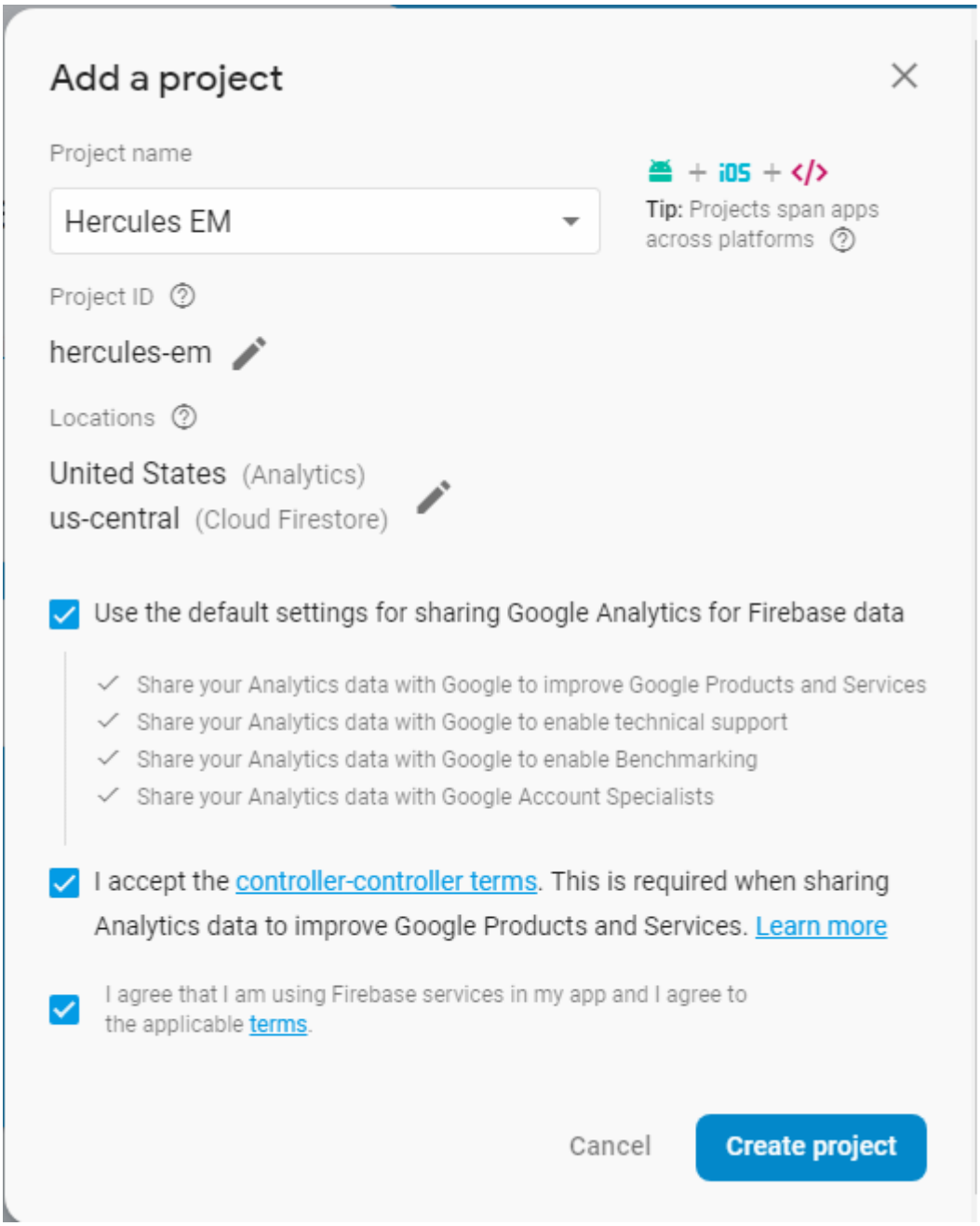
- Click 'Delete' only if you wish to remove the certificate so you can generate a new APNs certificate

Add Google Cloud Messaging (GCM) Token

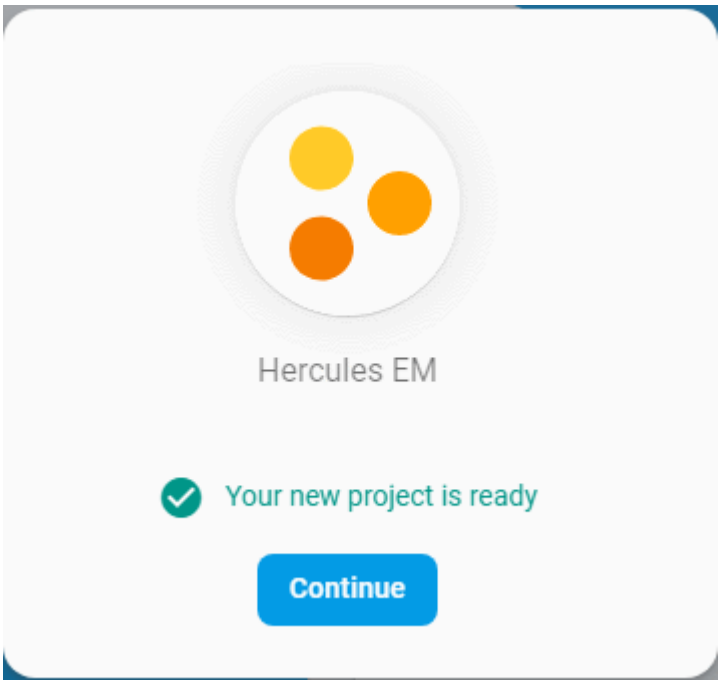
- Endpoint Manager requires a Google Cloud Messaging (GCM) token in order to communicate with Android devices.
- Endpoint Manager ships with a default token, but you can also generate a unique GCM token if required.
- To get a token, you must first create a project in the Google Developers console.
- Please follow the steps below to create a project and upload a token.
- **Step 1 - Create a New Project**
  - Login to the Google Firebase API console at **https://console.firebase.google.com** , using your Google account.



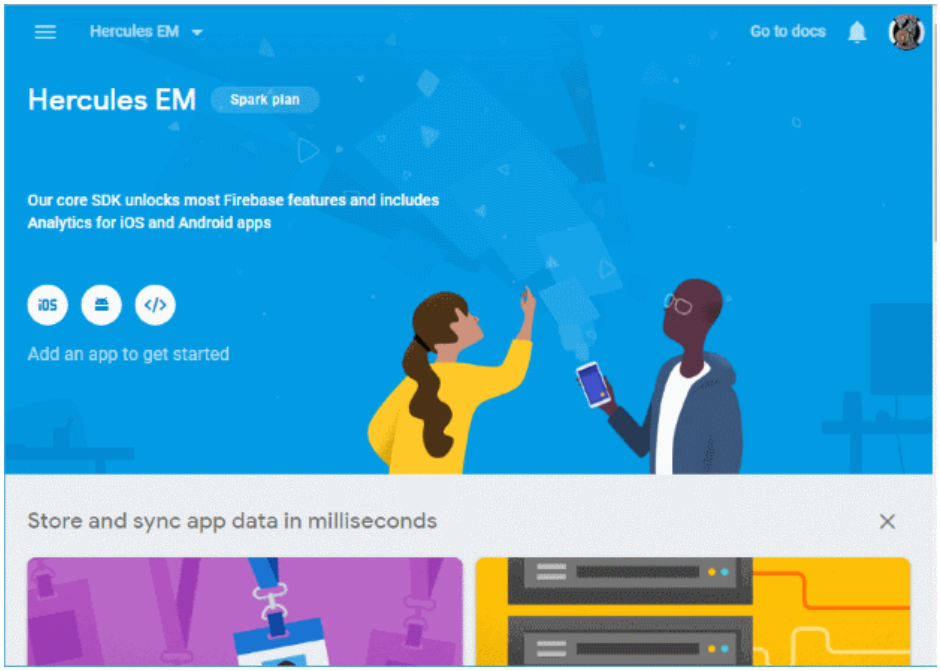
  - Click 'Add Project'



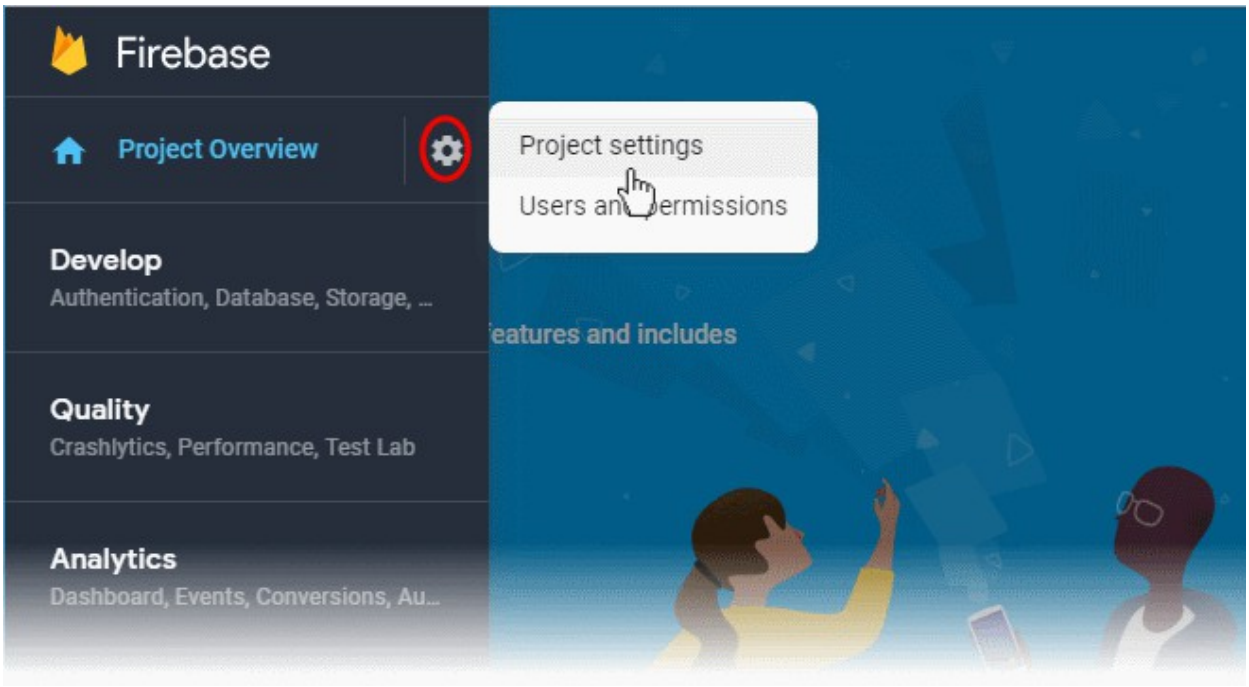
- Type a name for the new project in the 'Project name' field
- Click the pencil icon beside the 'Locations' field. Select your country and the Firestore server closest to you.
- 'Use default settings for sharing Google Analytics for Firebase data' - Leave this selected.
- Agree to the terms and conditions then click 'Create Project'.



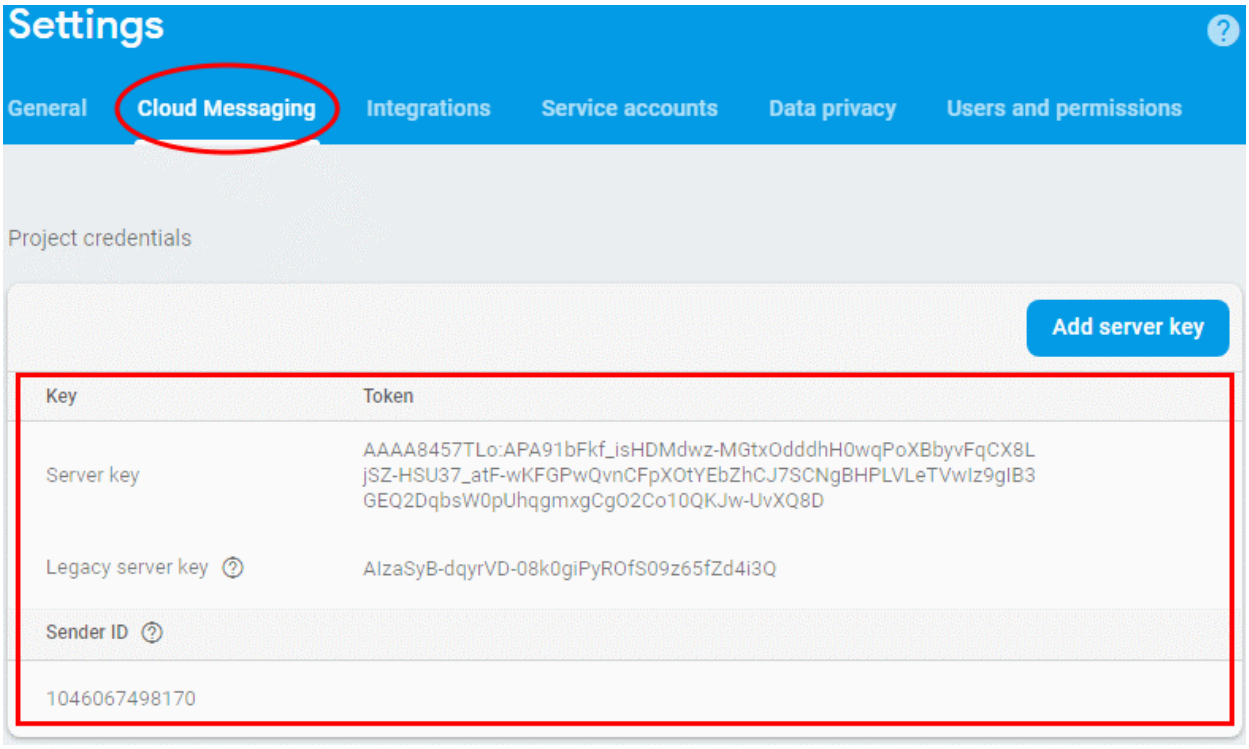
- Click 'Continue' to go to the project dashboard



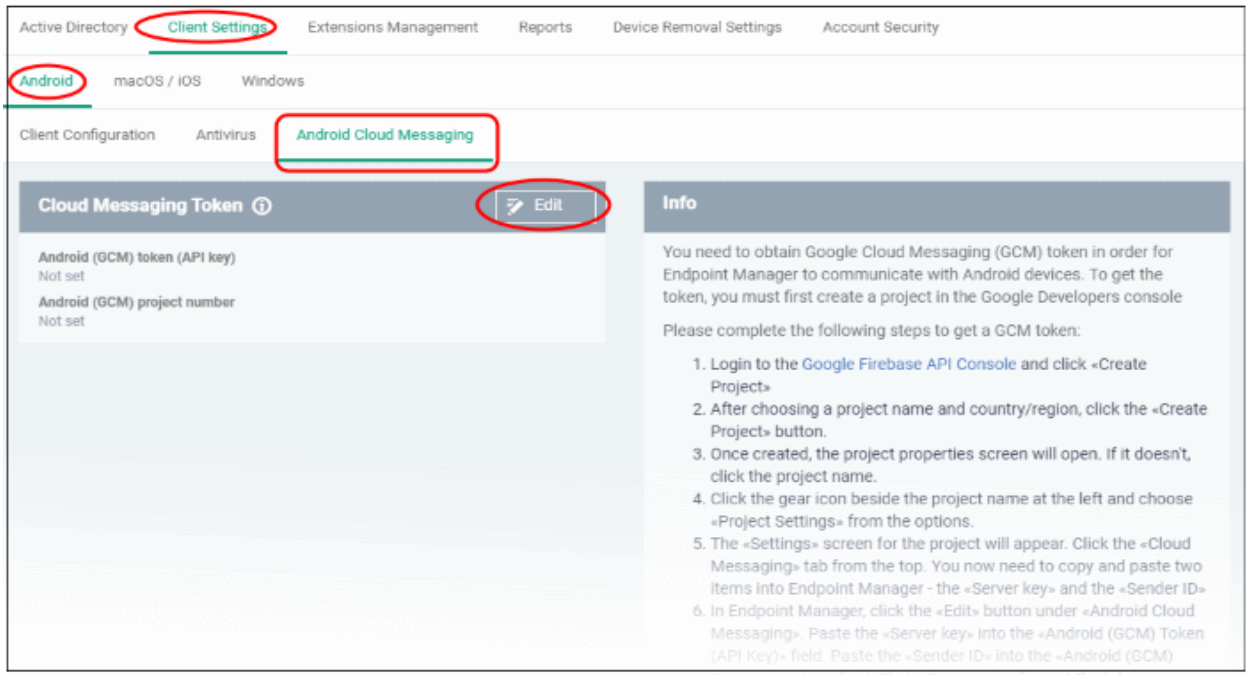
- **Step 2 - Obtain GCM Token and Project number**
  - Click the hamburger button at top-left
  - Click the gear icon beside 'Project Overview' and choose 'Project settings':



- The 'Settings' screen for the project will open.
- Click the 'Cloud Messaging' tab:

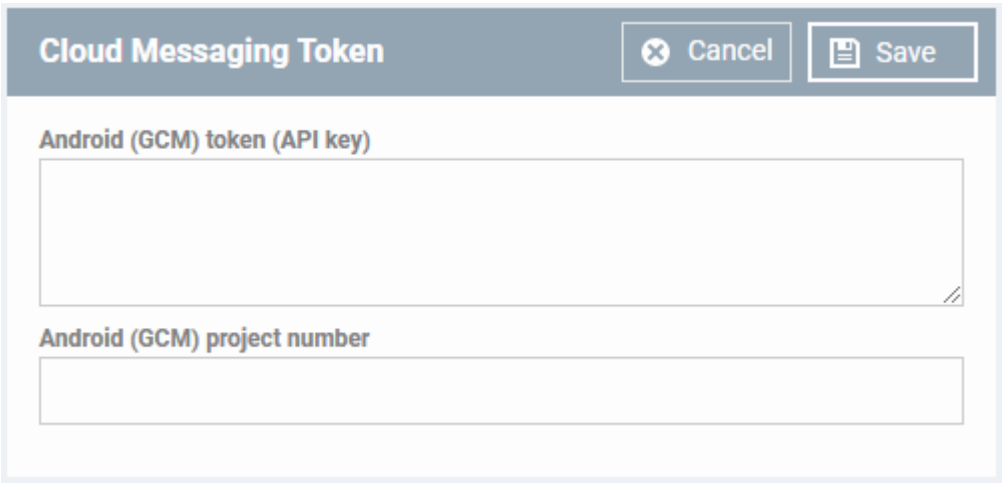


  - Copy the server key and sender ID
- **Step 3 - Enter GCM Token and Project number**
  - Login to Endpoint Manager
  - Click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'Android' > 'Android Cloud Messaging' tab

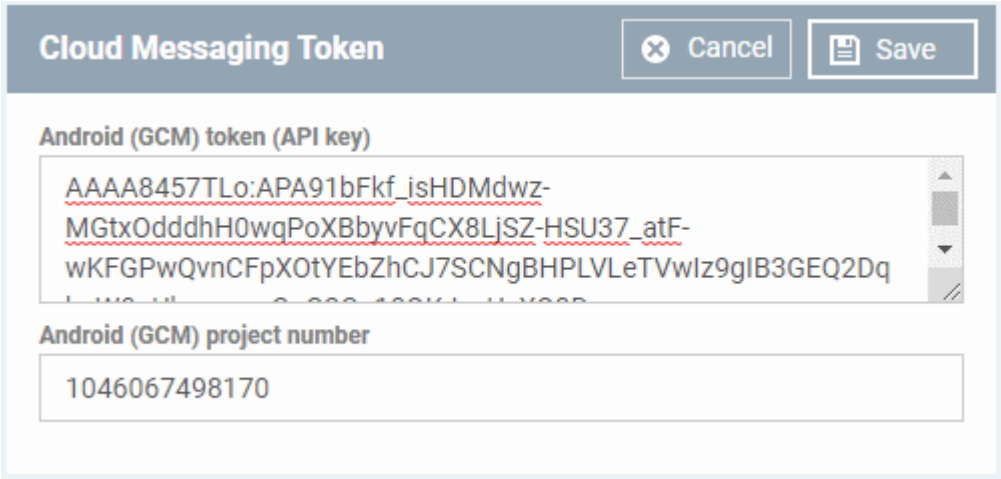


- Click the edit button 

at the top right of the 'Cloud Messaging Token' column, to view the GCM token and project number fields



- Paste the 'Server key' into 'Android (GCM) Token' field.
- Paste the Sender ID into 'Android (GCM) Project Number' field.



- Click 'Save'.

Your settings will be updated and the token/project number displayed in the same interface.

Endpoint Manager can now use the token to communicate with Android devices.

Step 3 - Add Users

You can add users and staff via the CD / C1 console, or add them directly in Endpoint Manager (EM).

- Staff added in Dragon / C1 are universal to the platform. They will be available in Endpoint Manager and other applications like Service Desk, CRM and Quote Manager.
- Users added to Endpoint Manager are only available in Endpoint Manager.

You can add new accounts using any of the following methods:

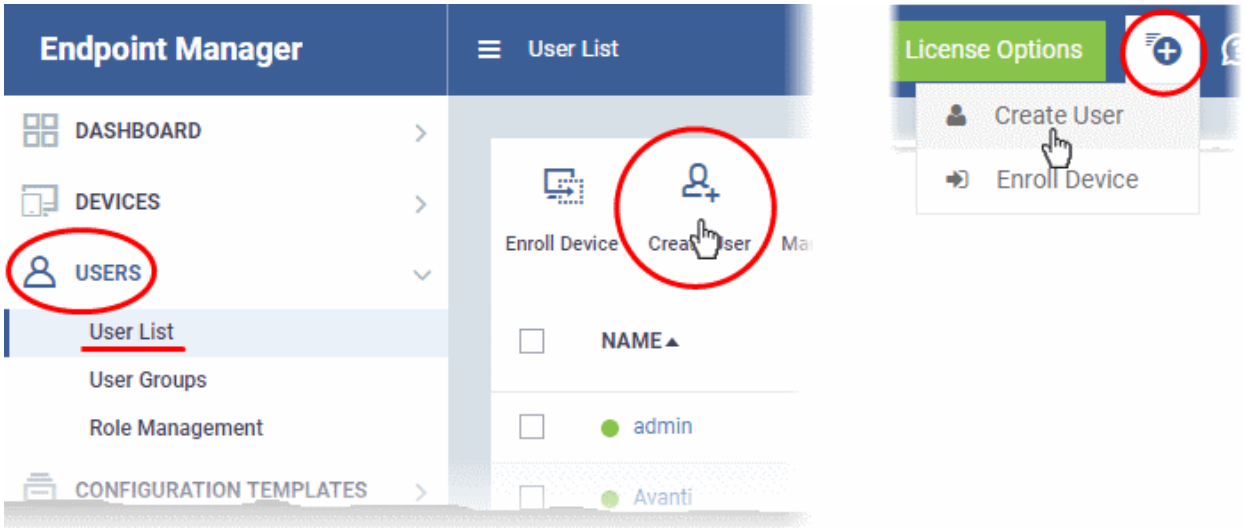
- **Manually add users**. Add individual users to EM. You need to specify their name, email address, the company they belong to and their EM role.
- **Import users from a CSV file**. Bulk import users from a comma separated values file.
- **Import users from Active Directory** (AD). This method is covered in the admin guide.

Manually Add Users

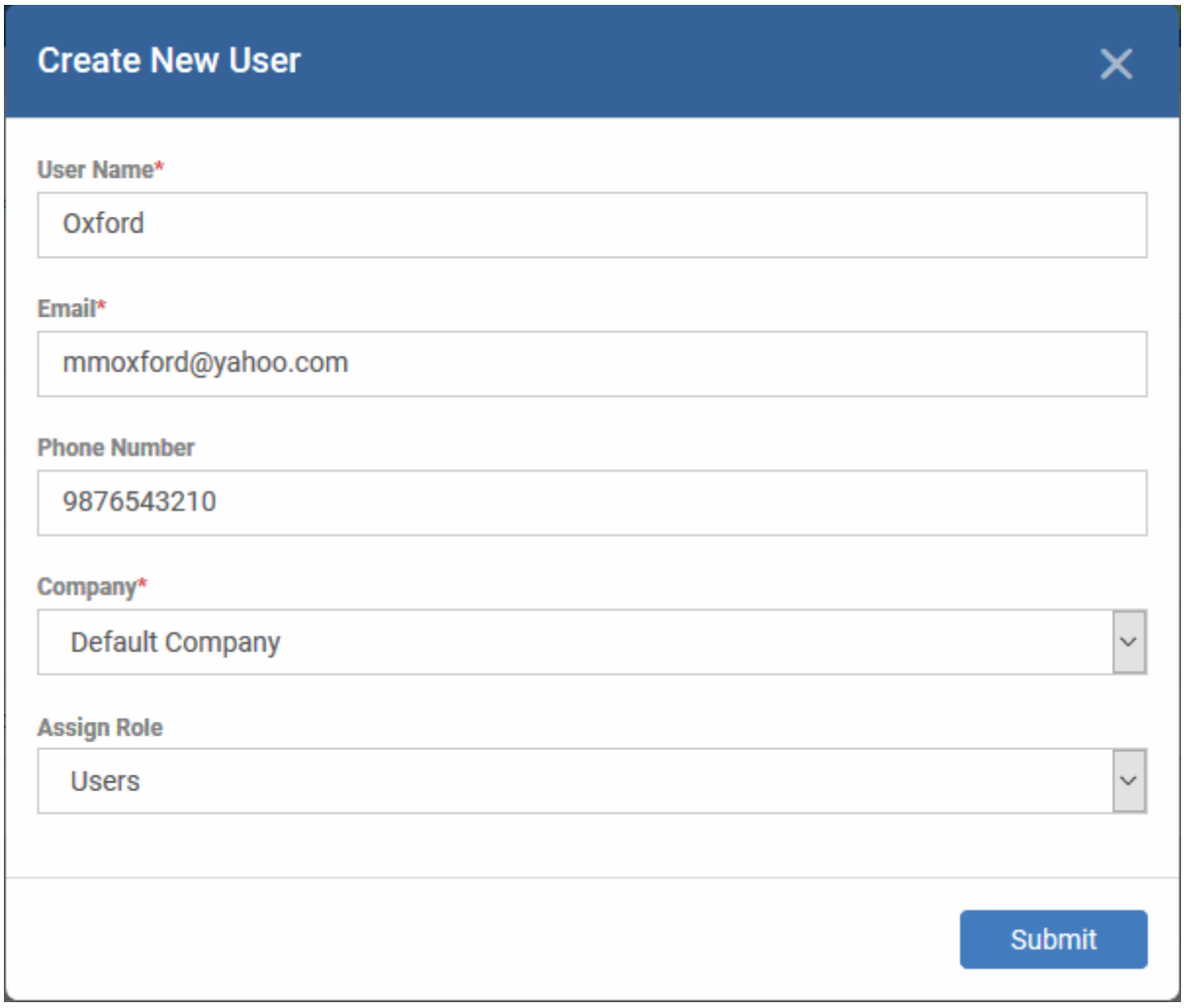
- Click 'Users' > 'User List'
- Click the 'Create User' button

or

- Click the 'Add' button  on the menu bar and choose 'Create User'.



The 'Create new user' form will open.



- Type a username, email address and phone number (optional) for the user
- Choose user's company (mandatory)
    - Dragon MSP and C1 MSP customers can add users from companies/organizations enrolled in their account.

- Dragon Enterprise, C1 Enterprise, and EM stand-alone customers can only add users to the default company.

- Choose a role. A 'role' determines user's permissions within Endpoint Manager. The product ships with three default roles:
  - **Administrators** - Can login to EM and access all management interfaces. This role can be edited as required.
  - **Technician** - Can login to EM and access all management interfaces. The technician role has fewer privileges than the administrator role. This role can be edited as required.
  - **Users** - Cannot login to EM. Generally speaking, a 'user' is simply an owner of a managed device. If required, you can change role permissions to have access to the admin console.

  You can create custom roles which grant access to selected areas of EM. These roles can be assigned to users as required. All roles created in EM and CD or C1 will appear in the 'Assign Role' drop-down when adding a new user. See online help page for **Configuring Role Based Access Control for Users** for more details.
- Click 'Submit' to add the user to EM.

The user is added to the 'Users' interface. The user's devices can be enrolled to EM for management.

- Repeat the process to add more users.

If you add a user with admin role then we will send them an account activation mail.

Import Users from a CSV File

Process in brief

- Create a CSV file containing the list of users you want to add.
- The file should contain the following, separated values: 'Username' (mandatory), 'Email address' (mandatory) and 'Phone number' (optional).
- The file should not contain column headers and each line should contain a single user.
- Click 'Users' > 'User List' > 'Import User' in the Endpoint Manager console
- Browse to your CSV file
- Select a company and a role for the imported users
- Click 'Import users from list'.
- The users will be imported and enrolled to EM

Requirements for .csv file

There are two mandatory fields and one optional field per user account:

- Username (mandatory)
- Email address (mandatory)
- Phone number (optional)

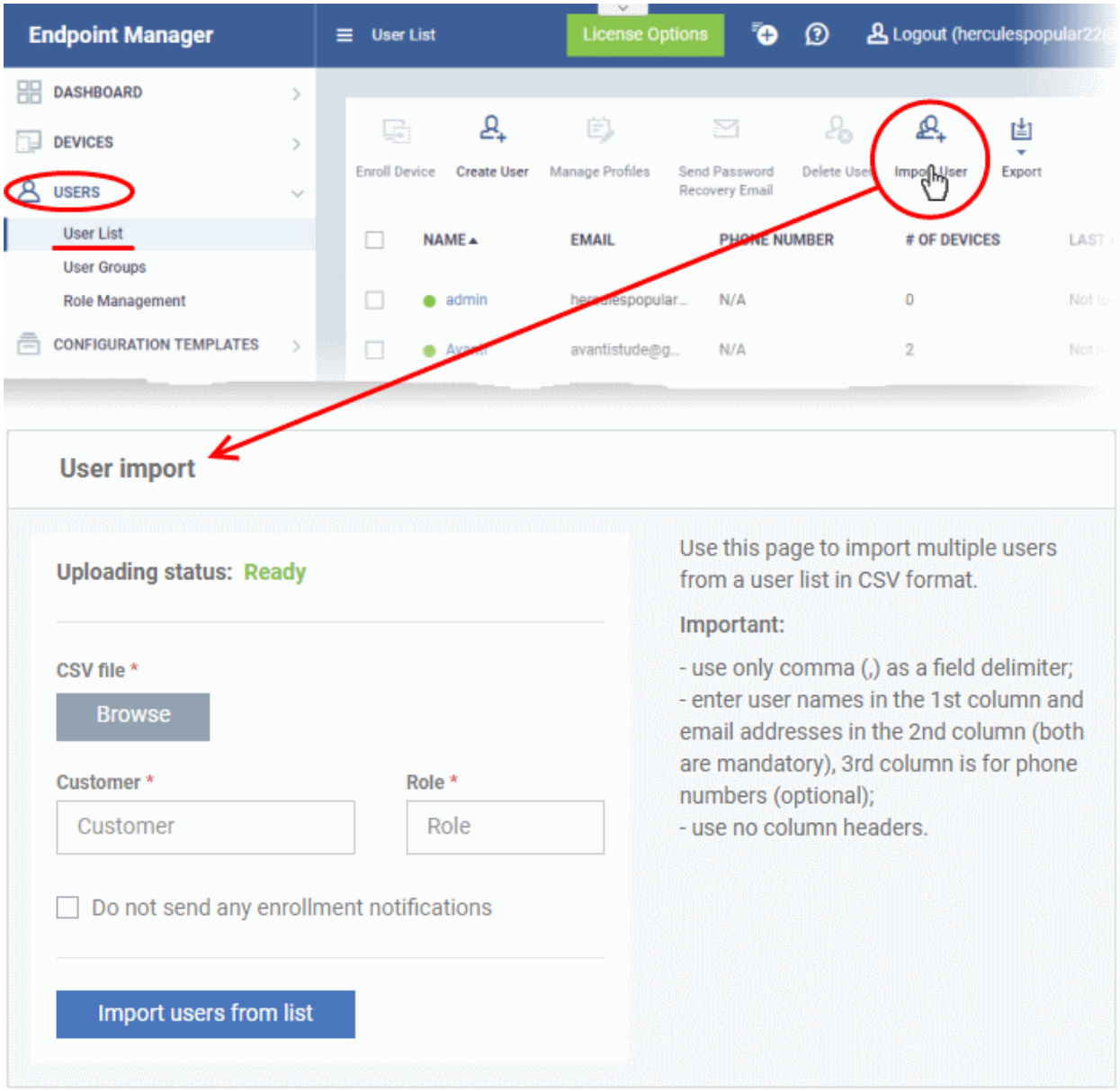
- Each line in the CSV file should contain one user entry
- The CSV file should not contain column headers

Example:

"james", "james@ditherscons.com", "9876543210"

Import users from a list

- Click 'Users' > 'User List' > 'Import User'



- Click 'Browse' to locate and open the CSV file you want to import
- Choose user's company (mandatory)
    - Dragon and C1 MSP customers can add users from any company added to their account.
        - Start entering first few letters of the company name and select the company from the options
    - Dragon Enterprise, C1 Enterprise, and EM stand-alone customers can only add users to the default company.
        - Enter 'Default Company' in the Company field
- Choose user role. See **above** if you need a recap on roles.
    - Type the first few letters of the role label and select from the suggestions.
- Click 'Import users from List'
- Imported users are added to the 'Users' interface. You can now add devices for the user.
- Users will receive an account activation mail if they are assigned a role that has access to the admin console. This includes the standard ' Administrator' and 'Technician' roles.

Tip - Enable 'Silent mode' in the import screen if you do not want to send these mails.

Step 4 - Enroll user devices

The next step is to add user devices for management.

- Each license covers one mobile device or one Windows / Mac / Linux endpoint per user.
- If you add more than one device for a user then an additional license is required. You can purchase additional licenses from the Comodo website.

Enroll user devices

- Click 'Users' > 'User List' on the left
- Select users for whom you want to enroll devices then click 'Enroll Device' above the table

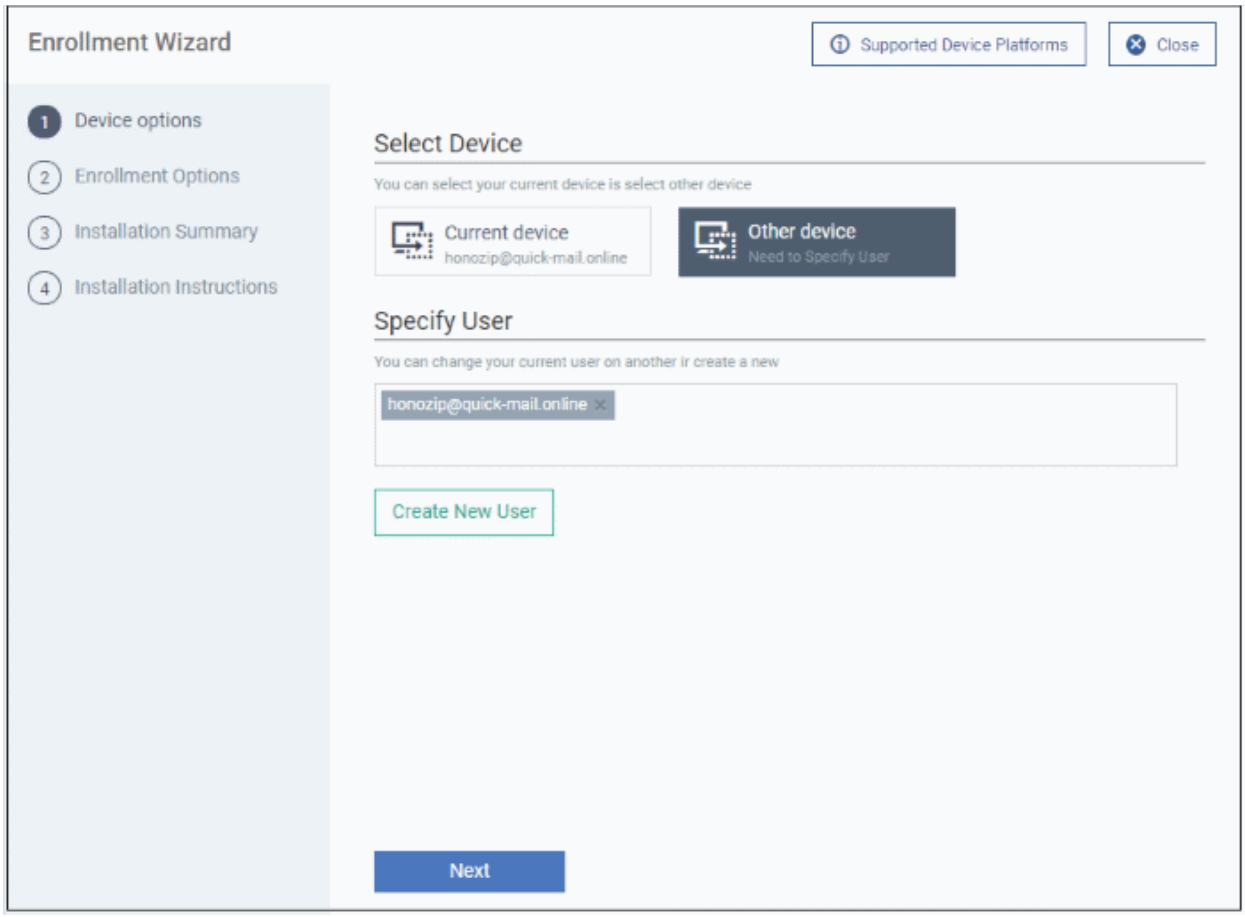
  Or

- Click the 'Add' button  on the menu bar then choose 'Enroll Device'.

This starts step 1 of the device enrollment wizard:

Step 1 - Device Options

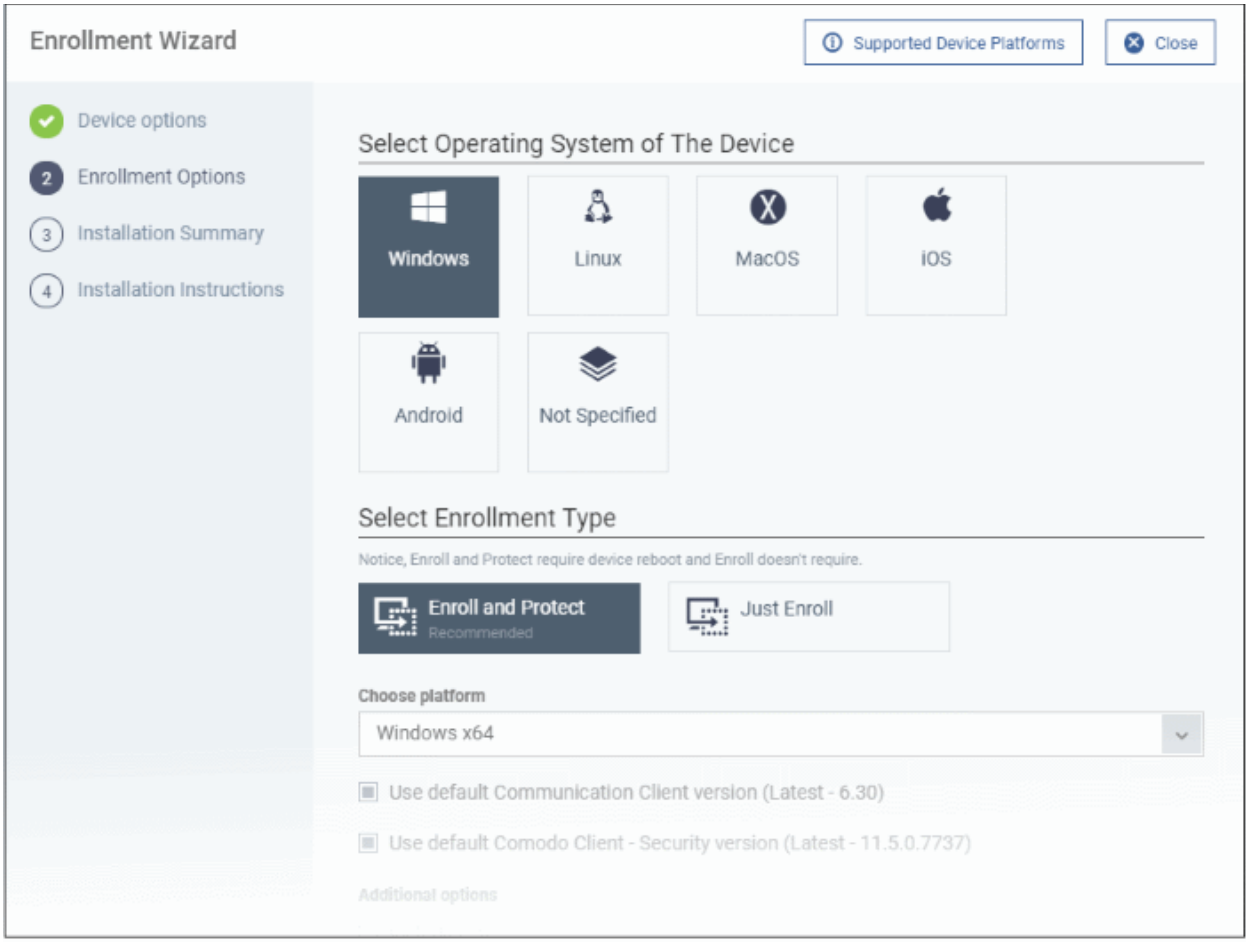
- **Current device -** Enrolls the device you are currently using. You may disregard this option at this stage as we are adding multiple devices with the 'Other device' option.
- **Other device** - Add devices owned by the users you selected previously. Those users should already be listed in the 'Specify 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.

- Click 'Next' to proceed to step 2.

Step 2 - Enrollment Options



TLDR -

- Click 'Not Specified' if you only want to install the communication client on target devices. The wizard will detect the target operating system and send the appropriate client to the device user.
- Click one of the operating system tiles if you also want to install the security client. Make sure the target devices use the operating system you selected.

There are two broad ways you can enroll devices:

Option 1 - Enroll + Protect - Single Operating System

- Click one of the operating system boxes to enroll devices of that type. Please make sure all your target devices use this operating system.
- The wizard will send enrollment mails that only provision the OS you chose.
- After choosing the OS, you can customize enrollment options as required. You can configure items such as enrollment type, reboot policy, client version, configuration profile and device name.

Option 2 - Enroll Only - Multiple Operating Systems

- Click the 'Not Specified' box. This option installs only the communication client, and doesn't install the security client.
- Your target devices can be a mix of operating systems rather than a single OS. This option auto-detects the OS of the device and emails the appropriate client link to the user.
- The latest version of the communication client is installed on each device. The MDM profile is installed on MAC devices

- Note - You can use this option to quickly connect devices to Endpoint Manager, then go back later and install the security client if required.

Enrollment Type

Applies to Windows, Mac and Linux devices.

- **Enroll and Protect** - Installs both the communication client and the security client.
- **Just Enroll** - Installs only the communication client

Background. There are two types of client:

- **Communication Client** - Connects the device to Endpoint Manager for central management. It is mandatory to install this client.
- **Security Client** - This is the security software. Depending on the operating system, it includes antivirus, firewall, threat-containment, web-filtering, and more. It is optional to install this client.

Click 'Next' to **skip to step 3** if you are happy with your choices on this page.

OR

Use the following links to read more about the various settings per OS:

- **Windows**
- **Linux**
- **Mac OS**
- **iOS / Android**

Windows

Setting	Description
Choose platform	Select Window OS version. 64 bit, 32 bit, or hybrid. The hybrid package will auto-detect and install the correct version.
Use default Communication Client version	This client enrolls the endpoint for central management. • You can only change the CCC version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed.
Use default Communication Client Security version	This client installs security software such as antivirus, firewall and auto-containment. • You can only change the CCS version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed.
Additional options	**AV Database** - Choose whether to include the latest virus database with the installation package. This increases the size of the package. If disabled, the client will download the latest database anyway when you run the first virus scan.
Configuration Profile	A configuration profile is a collection of settings which specify a device's network access rights, security settings, antivirus scan schedule, and more. The default is 'Windows - Security Level 1' profile. Choose a different profile if required. • The default profile is recommended for most users and can always be changed later if required. • If you want to change it, type the first few characters of a profile name and choose from the suggestions that appear.

	• You can view the settings in a profile at 'Configuration Templates' > 'Profiles'.
Set Reboot Options	Endpoints need to be restarted to complete CCS installation. You have the following restart options: • **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message is shown to the user prior to the restart. • **Suppress reboot** - Endpoint is not auto-restarted. The installation is finalized when the user next restarts the endpoint. • **Warn about reboot and let users postpone it** - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens. Optional. Type a custom message in the 'Reboot Message' field.
Device Name Options	• Do Not Change - The device's existing name is used to identify the device in Endpoint Manager. • Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.

- Click 'Next' to proceed to step 3

Linux

Setting	Description
Choose platform	Select Linux OS version • Ubuntu / Debian (Hybrid Package) • RHEL / CentOS (Hybrid Package) • 'Hybrid' just means the package is suitable for both types of OS.
Device Name Options	• Do Not Change - The device's existing name is used to identify the device in Endpoint Manager. • Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.

- Click 'Next' to proceed to step 3

Mac OS

Setting	Description
Select Method	• **With MDM profile** (recommended) - Installs both the communication client and the Endpoint manager configuration profile. You can use the full suite of Endpoint Manager tools on your devices • **Without MDM profile** - Installs only the communication client. 'Profile-less' enrollment lets you use Endpoint Manager to manage security while using another platform for general Mac management.
Device Name Options	• **Do Not Change** - The device's existing name is used as the device label in Endpoint Manager.

	• **Change** - Enter a new device name. Note - You can restore the original name from the device list screen if required.

- Click 'Next' to proceed to step 3

iOS / Android

Device Name Options:

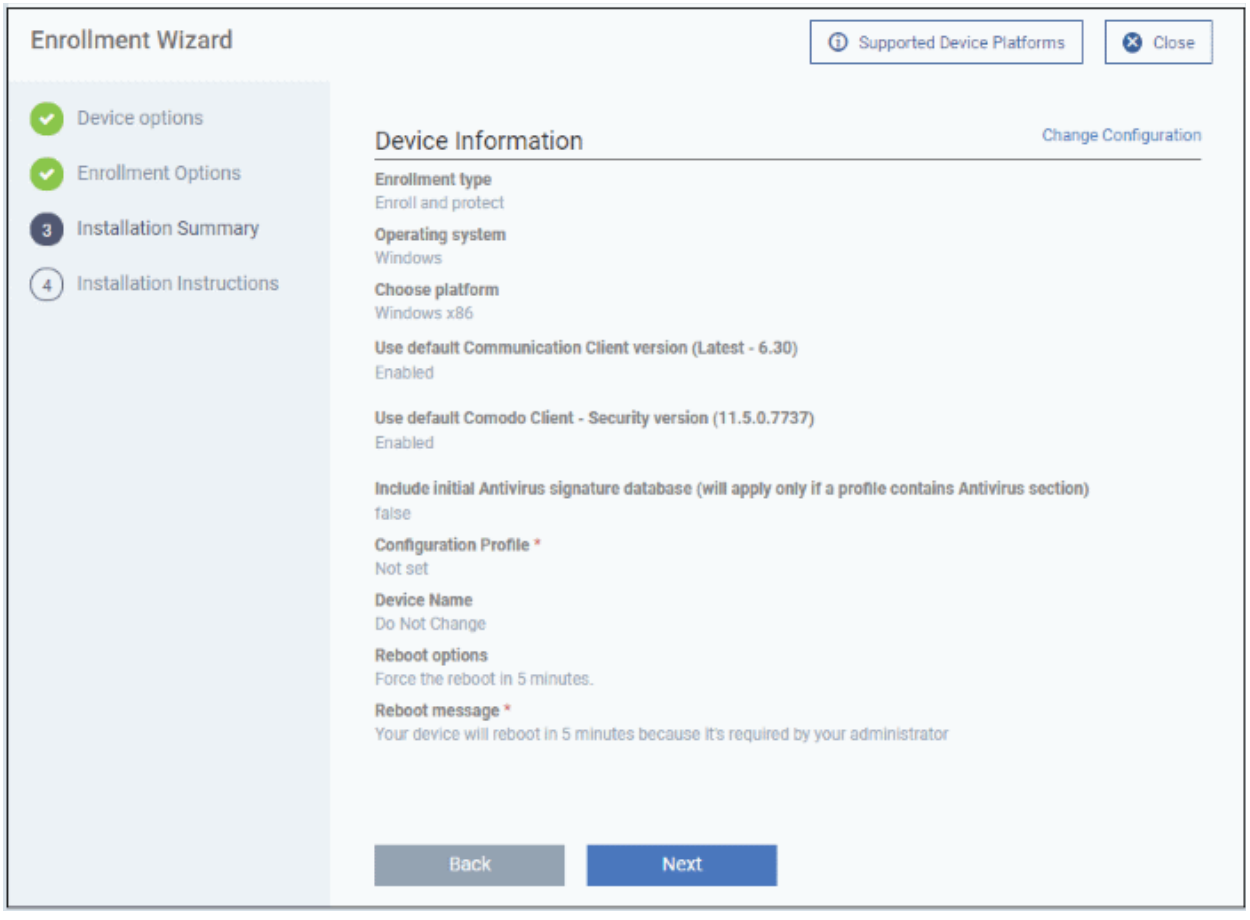
- **Do Not Change** - The device's existing name is used as the device label in Endpoint Manager.
- **Change** - Enter a new device name. Note - You can restore the original name from the device list screen if required.

Click 'Next' to proceed to step 3

Step 3 - Installation Summary

Review your choices so far.

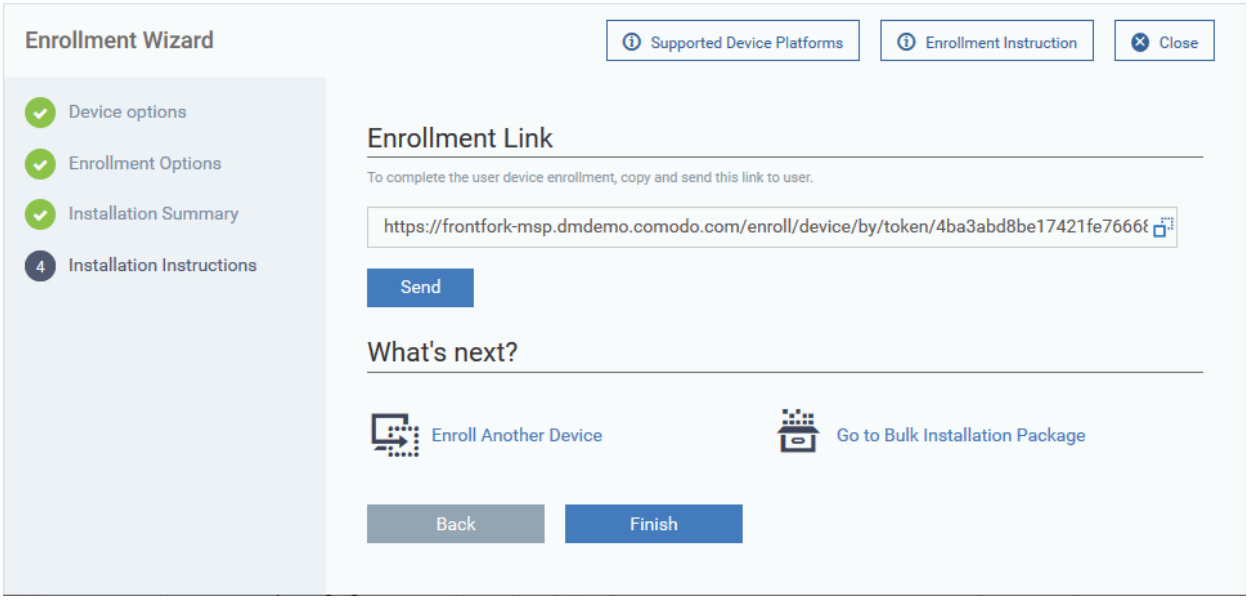
The summary you see depends on the operating system and enrollment type:



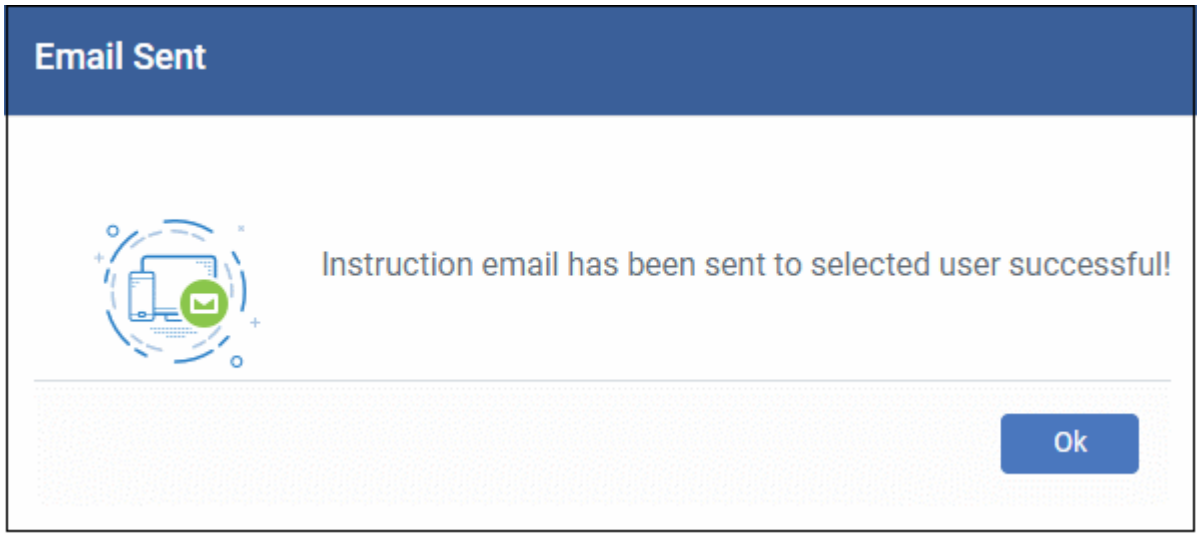
- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4

Step 4 - Installation Instructions

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



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



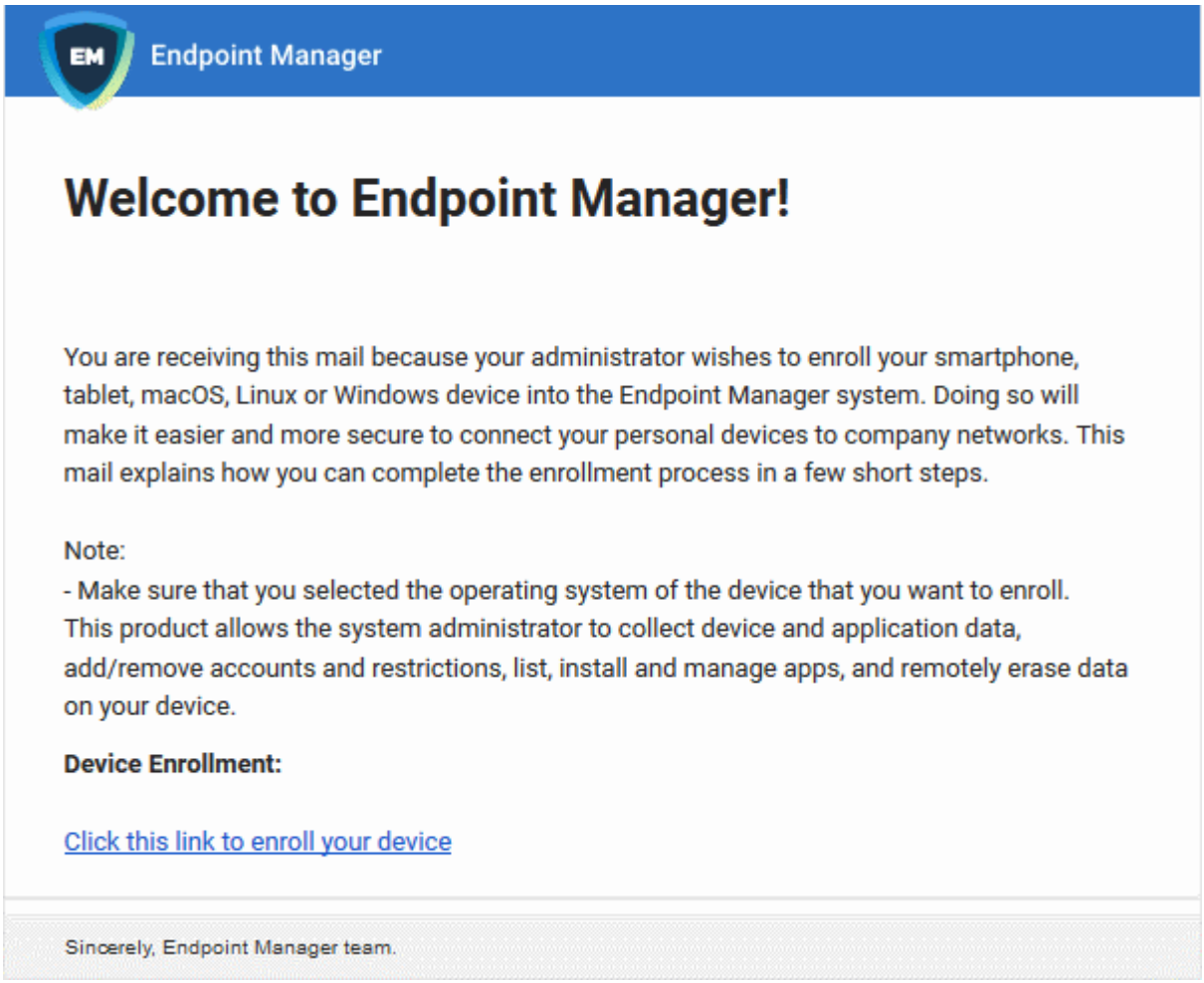
- **Enroll Another Device** - Takes you back to step 1
- **Go to Bulk Installation Package** - Takes you to bulk installation package screen to configure and enroll users in bulk. See '**Bulk Enrollment of Devices**'

- Click 'Finish' to close the window.

Note - If you chose 'Current Device' in step 1, then you can enroll your device in two ways:

1. Download the client in the final step. Follow the instructions and complete the enrollment procedure.
2. Click 'Enrollment Instructions' at top-right, click the appropriate enrollment link to your device and complete the procedure.

An example mail that is sent to users is shown below:



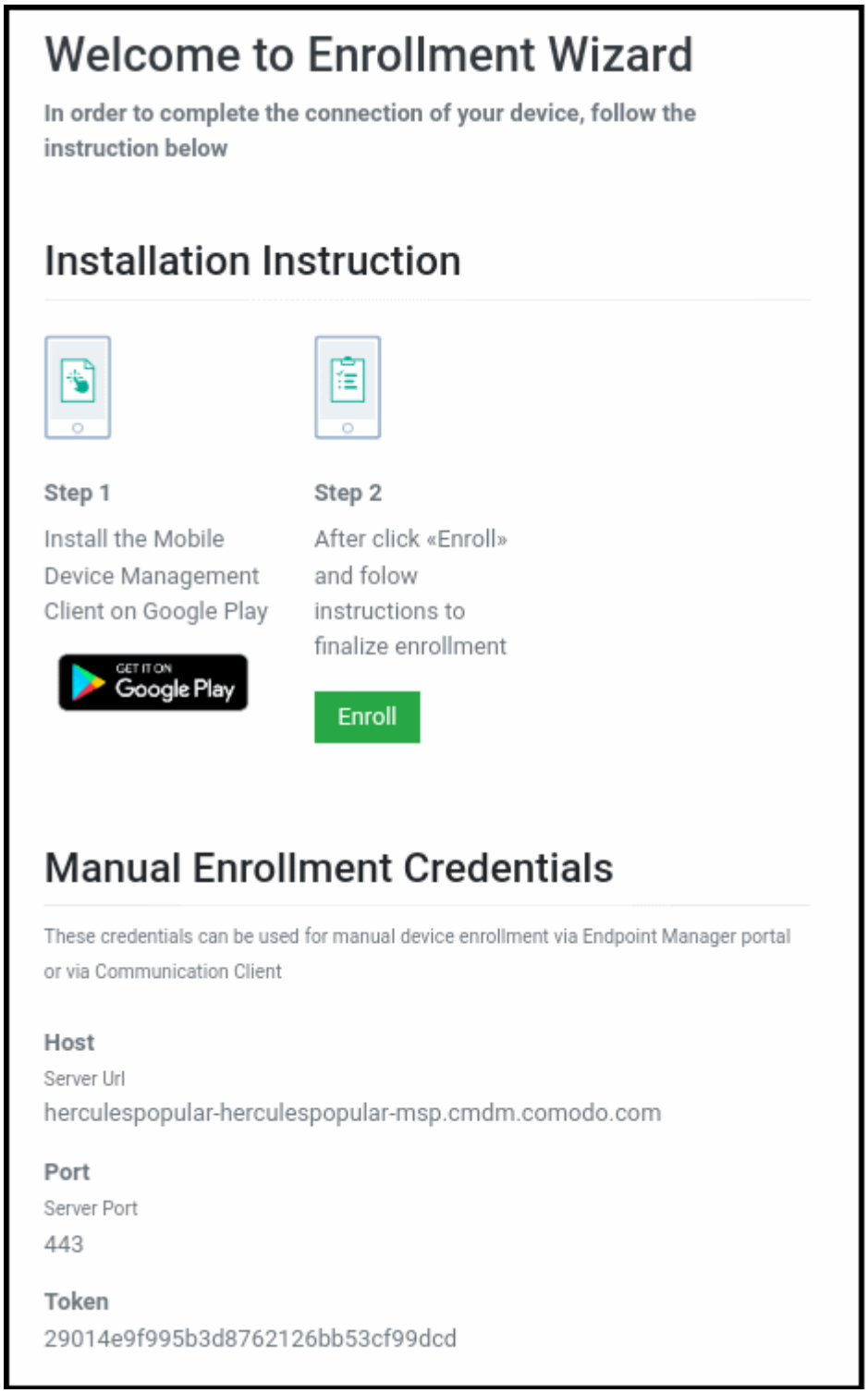
- Clicking the link will take the user to a page which lets them download the appropriate communication client/profile.

Tip: Here's two other ways you can enroll devices for users:

- Click 'Users' > 'User List' > click the name of a user to open their details screen > click 'Enroll Device'
- Click 'Devices' > 'Device List' > 'Enroll Device'

Enroll devices

- The user should open the mail on the device itself and click the device enrollment link.
- This starts a wizard which lets them download the appropriate client software for their device. An example is shown below:



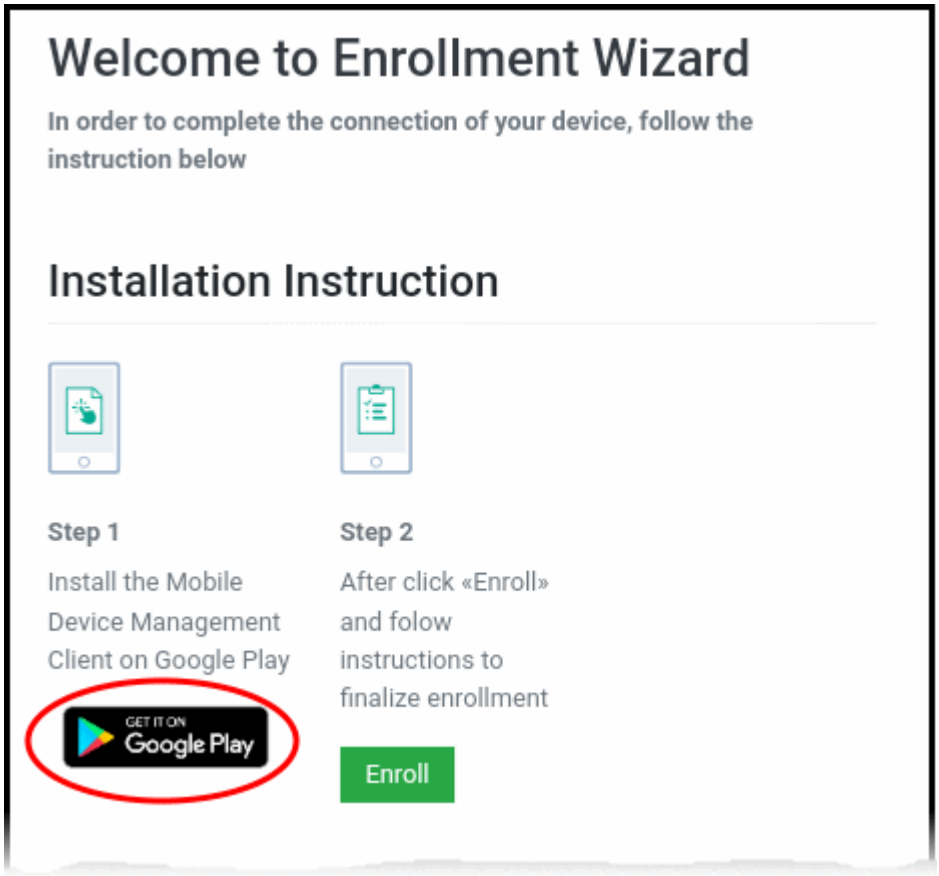
- Once installed, the client software will connect the device to Endpoint Manager.
- The following sections explain the enrollment process on different operating systems:
  - **Enroll Android Devices**
  - **Enroll iOS Devices**
  - **Enroll Windows Endpoints**
  - **Enroll Mac OS Devices**
  - **Enroll Linux OS Endpoints**

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**

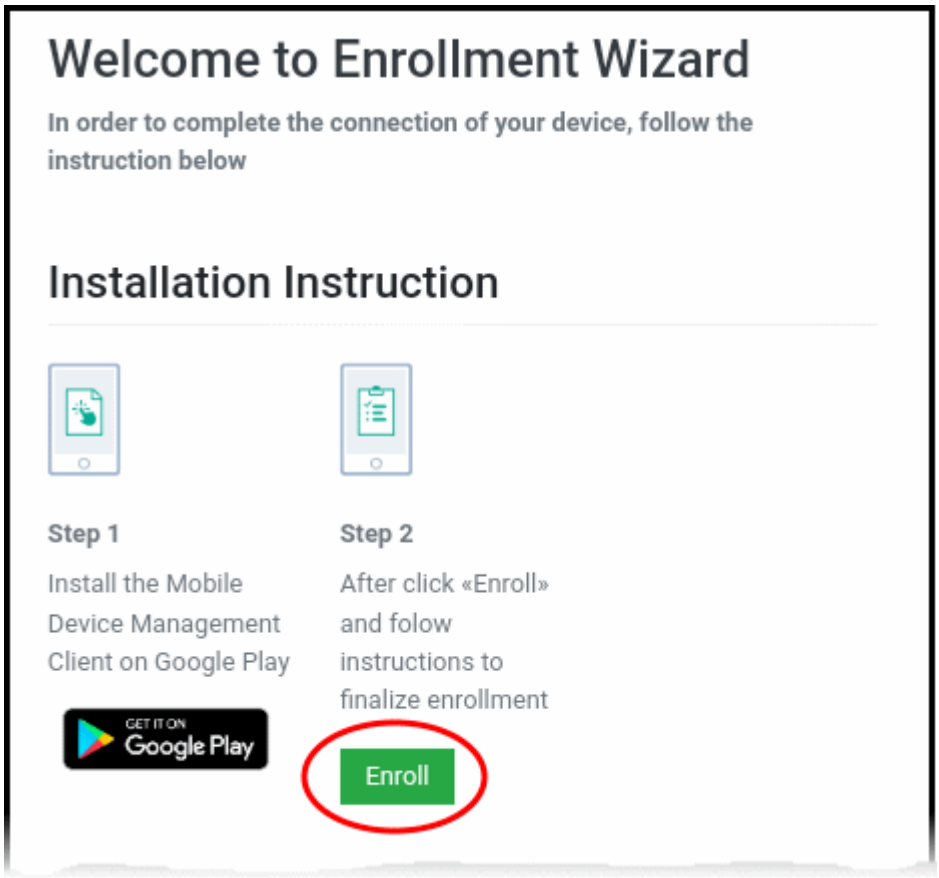
Step 1 - Download and Install the communication client

- The user should open the mail on the device itself and open the device enrollment link.
- Next, tap 'Get it on Google Play' to download and install the client software.



Step 2 - Configure the communication client

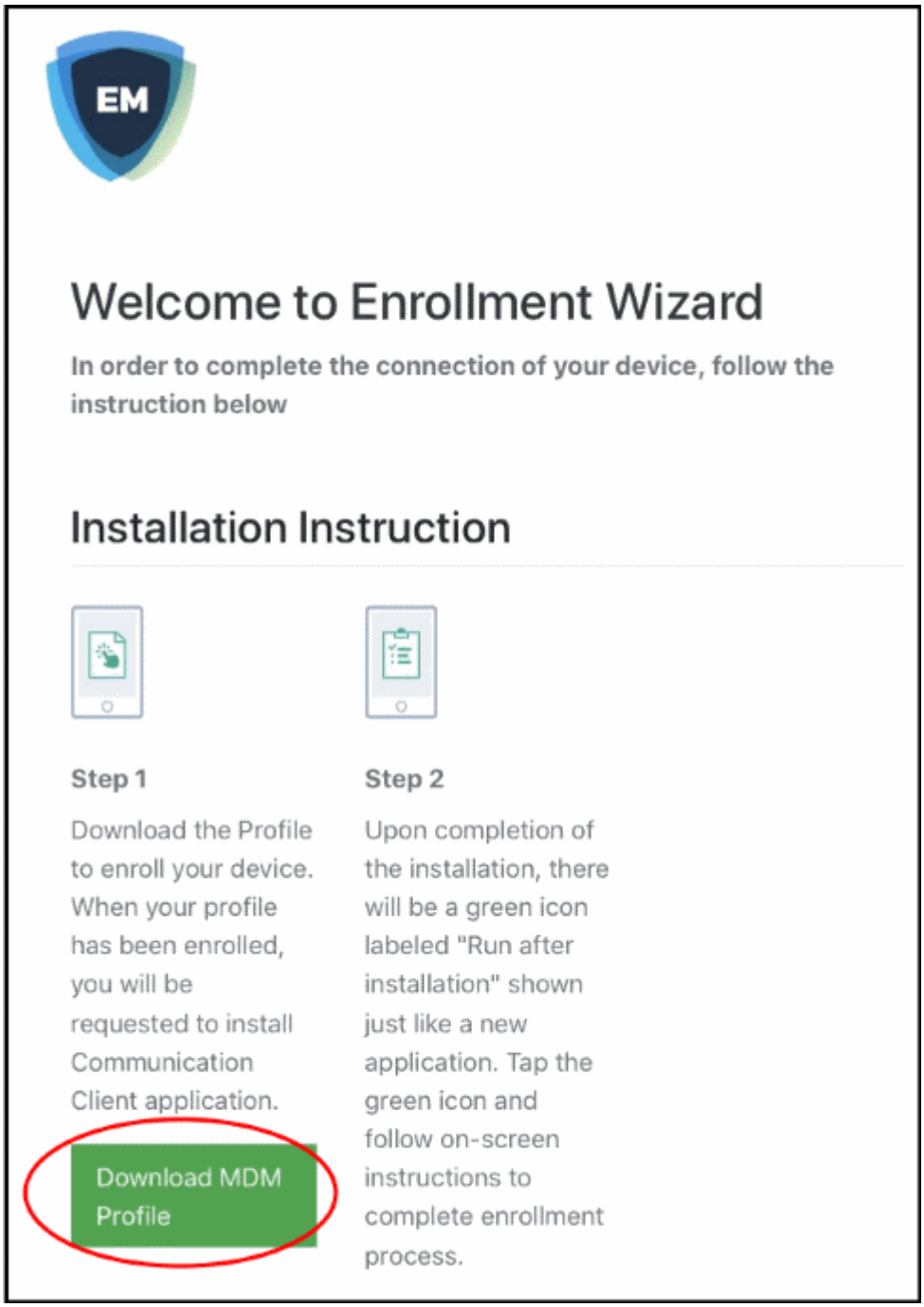
- After installation in step 1, the user should go back to the device enrollment page and tap the 'Enroll' button under 'Step 2':



Next, the user has to tap 'Activate' to enroll the device.

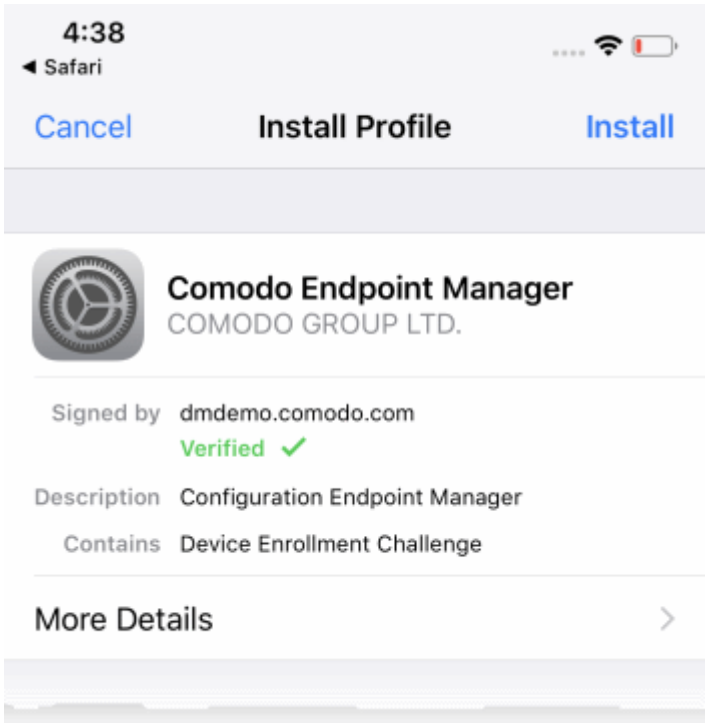
Enroll iPhones, iPods and iPads

- Device owners should open the mail on the device itself and tap the enrollment link. This will take them to the device enrollment wizard.



- Tap 'Download MDM Profile'.

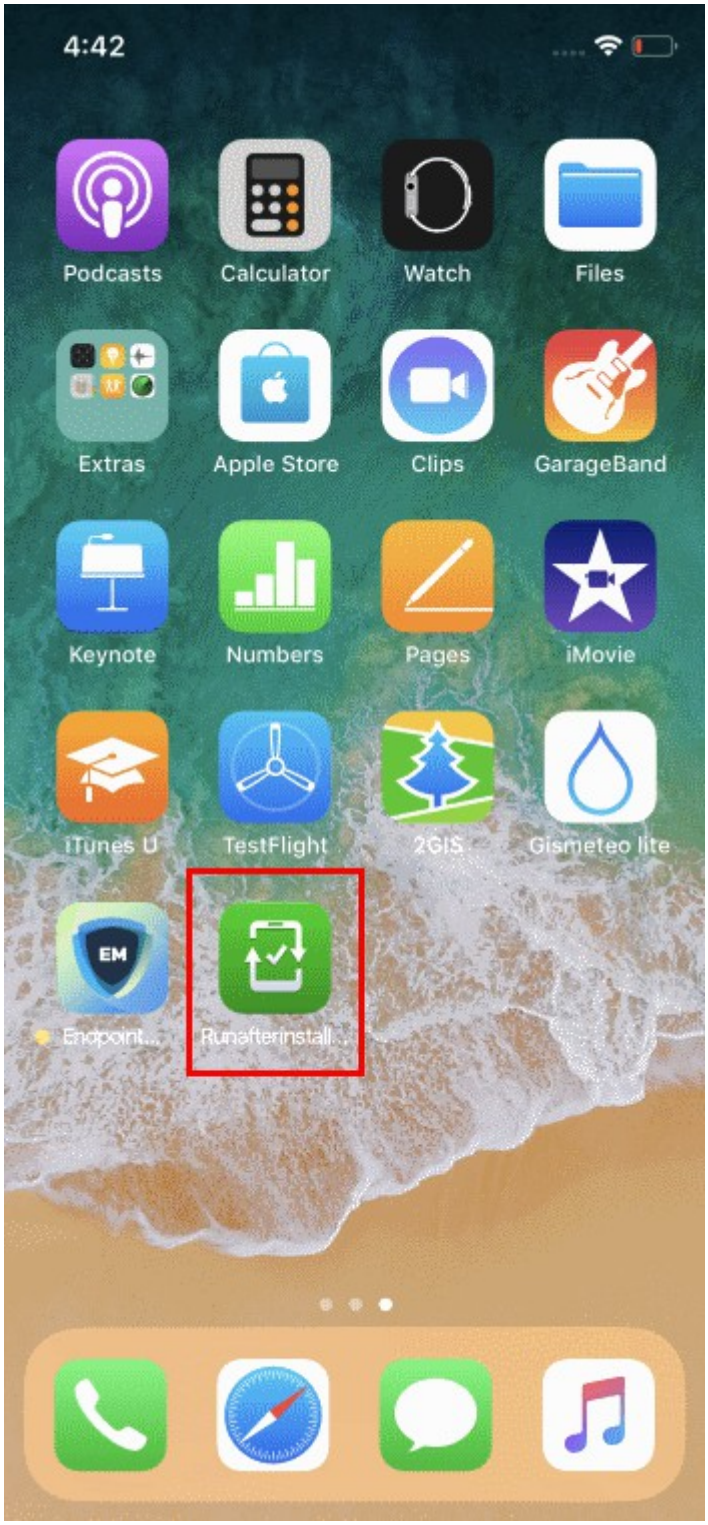
The 'Install Profile' wizard starts:



Note: Users must keep their device switched on at all times during enrollment. The enrollment process may fail if the device auto-locks or enters standby.

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

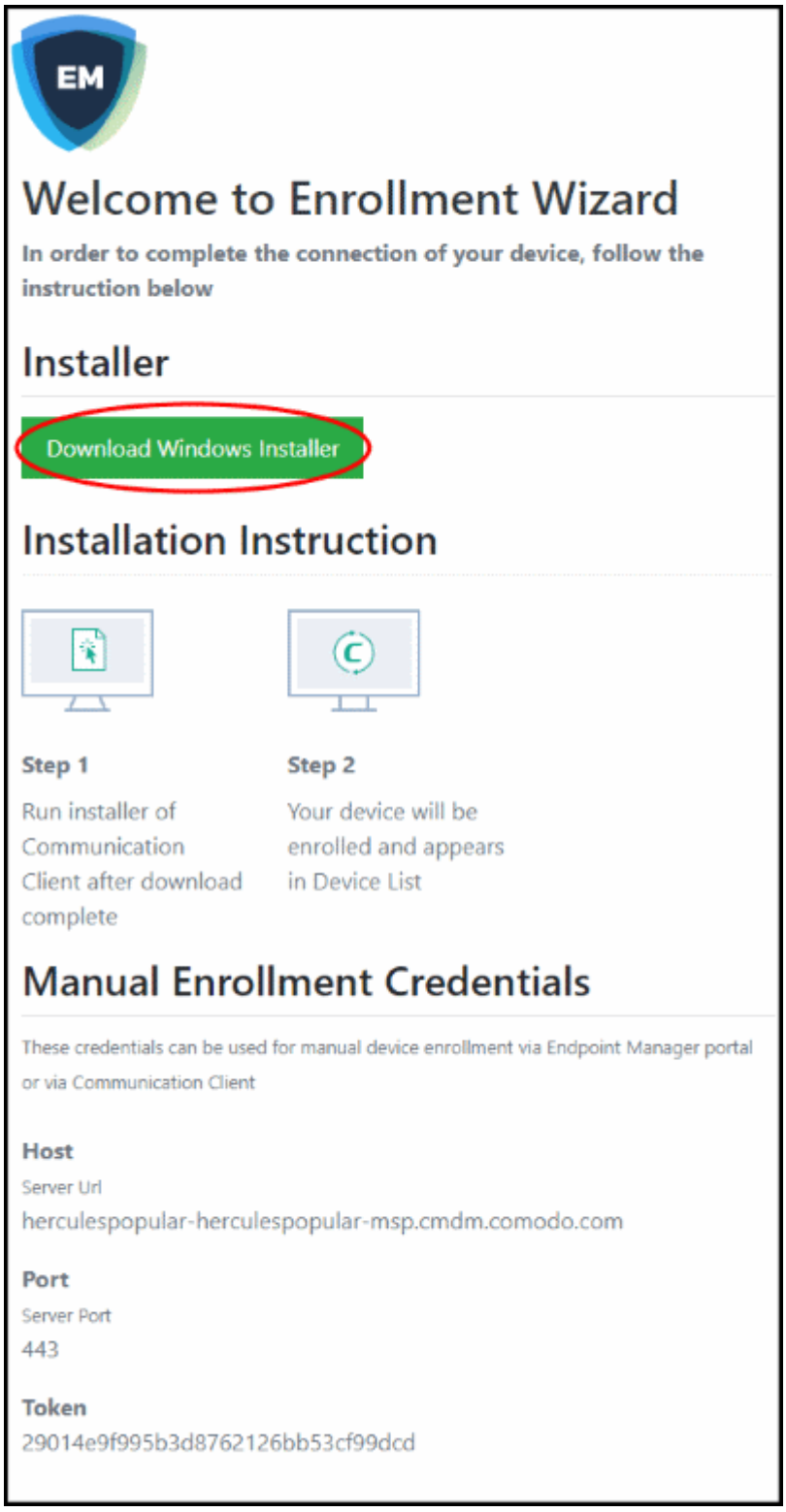
- The app is downloaded from the Apple store using the user's account.
- After installation, tap the green 'Run After Install' icon on the home screen:



The device will be enrolled and connected to EM.

Enroll Windows PCs

- Users should open the mail on the device itself and open the device enrollment link
- The following wizard opens:

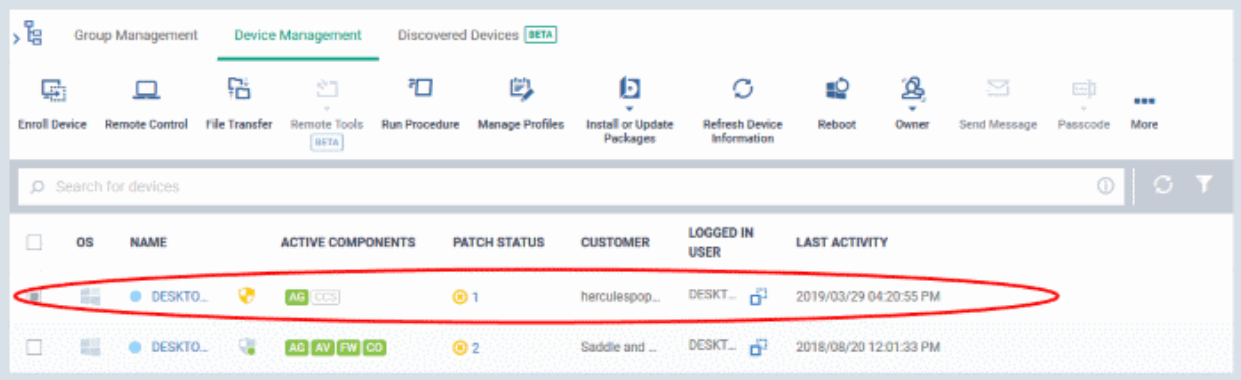


- Click the 'Download Windows Installer' button.
- The EM client setup file gets downloaded.
- Double-click on the file to install the communication client.

The device automatically gets added to Endpoint Manager once installation is complete. Comodo Client Security is installed if you chose it in the setup wizard. You also have the option to install CCS manually after device enrollment.

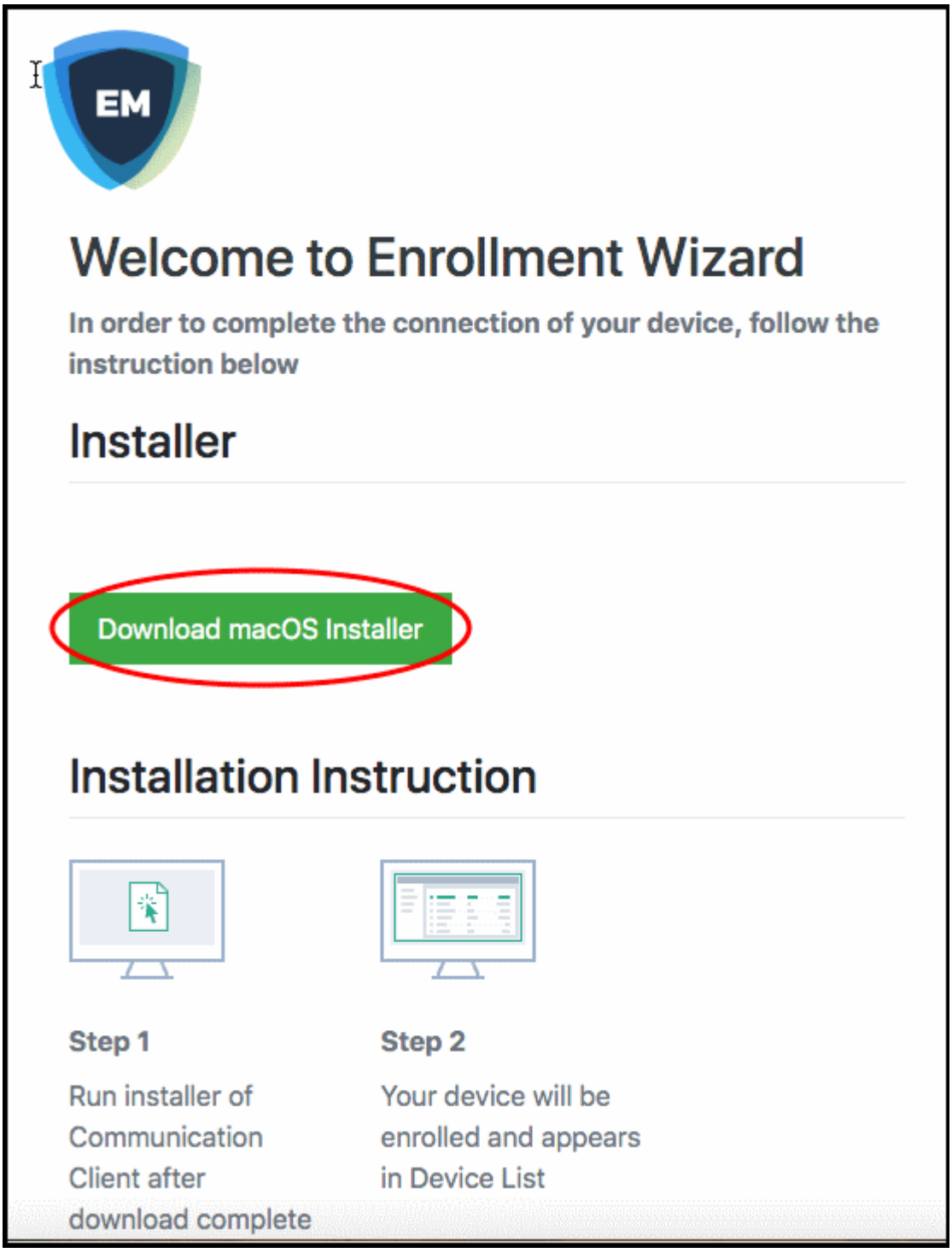
The client icon appears at the bottom-right of the endpoint screen.

- You can check whether the devices are successfully enrolled from the 'Devices' > 'Device List' interface.

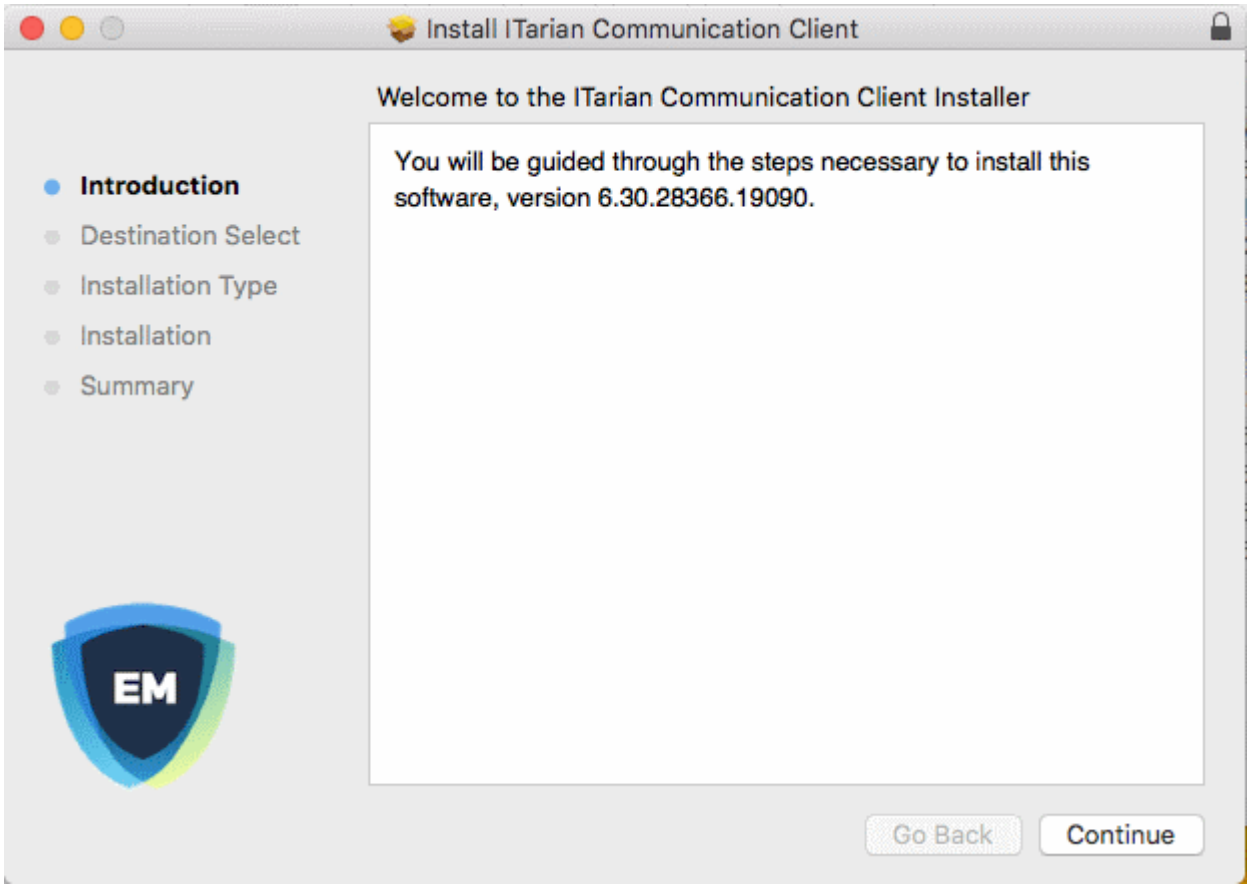


Enroll Mac OS Devices

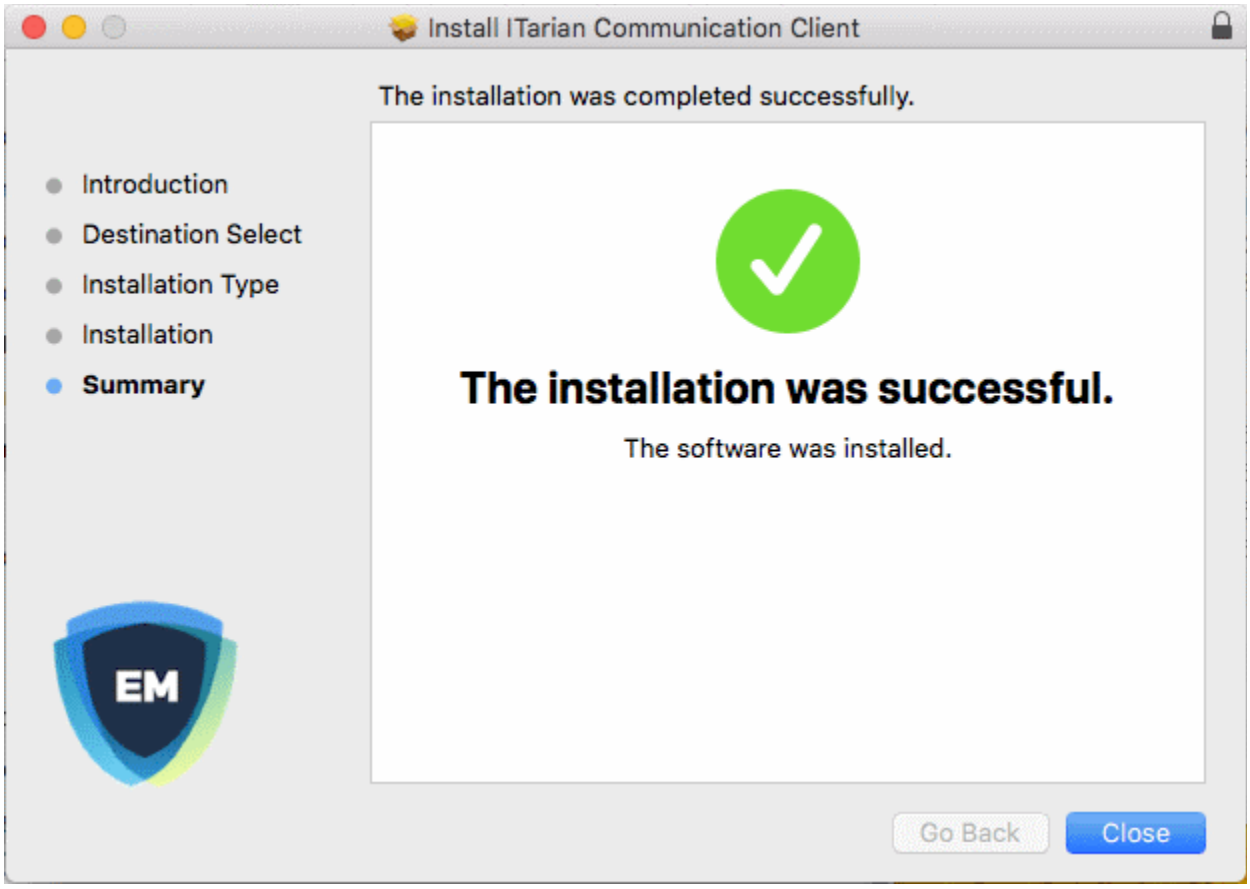
- Users should open the mail on the device itself and open the device enrollment link
- The device enrollment wizard starts:



- Click 'Download mac OS Installer' in the wizard and save the setup file
- Open the setup file to install the communication client.

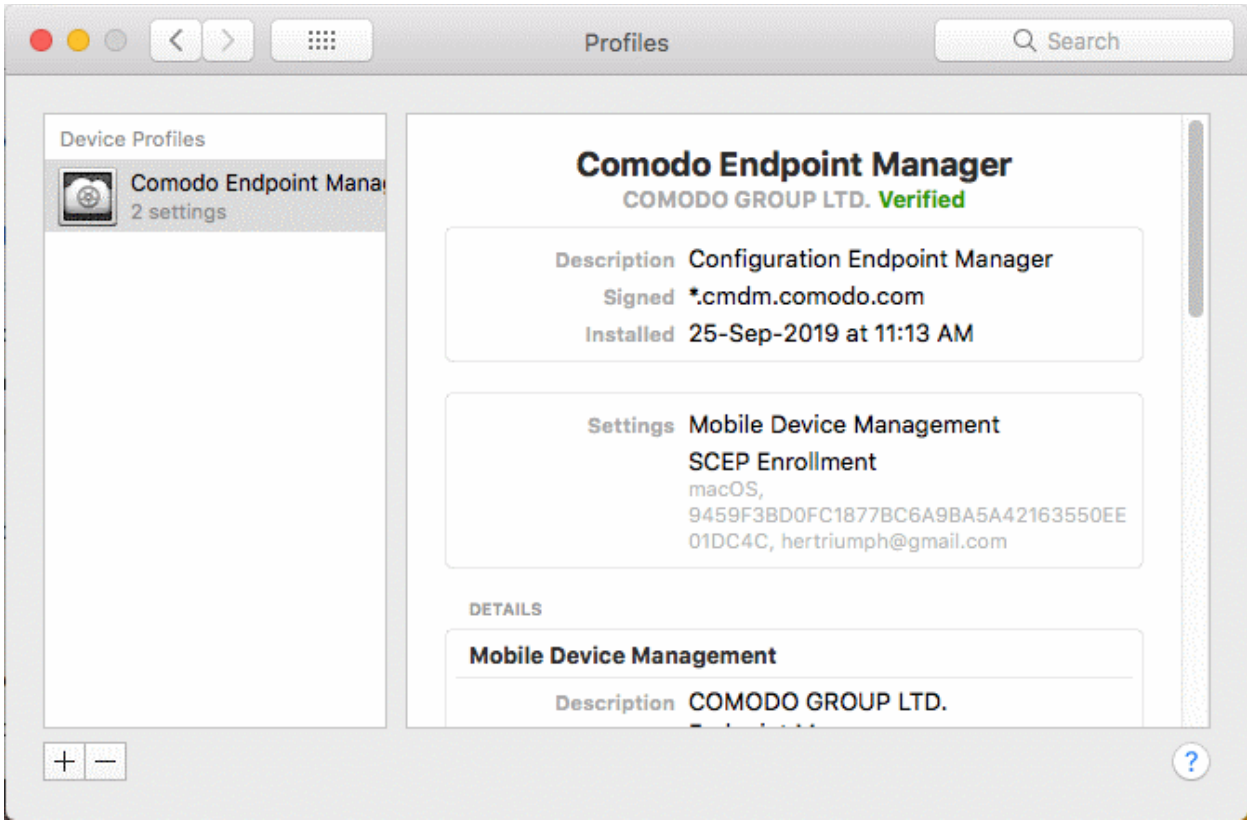


- Follow the wizard to complete the installation.



- The profiles screen will show you details of the Endpoint Manager profile, if you have chosen to

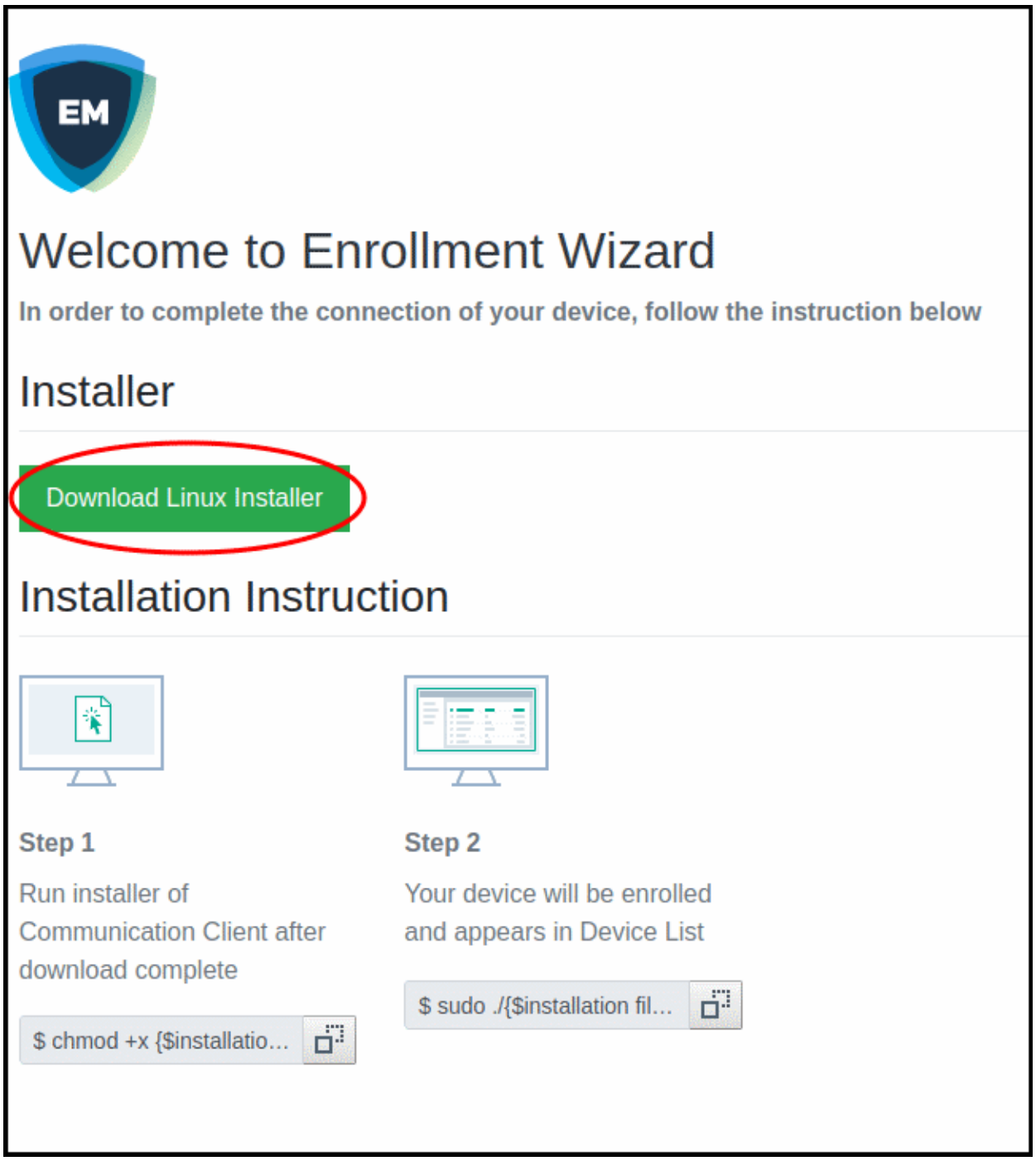
install it.



- The device is automatically added to Endpoint Manager once installation is complete. CCS is installed if you included it in the setup wizard.

Enroll Linux Devices

- Users should open the mail on the device itself and open the device enrollment link
- The device enrollment wizard starts:



- Click the 'Download Linux Installer' button and save the file:

The communication client can be installed the device by completing the following:

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

   $ chmod +x {$installation file$}

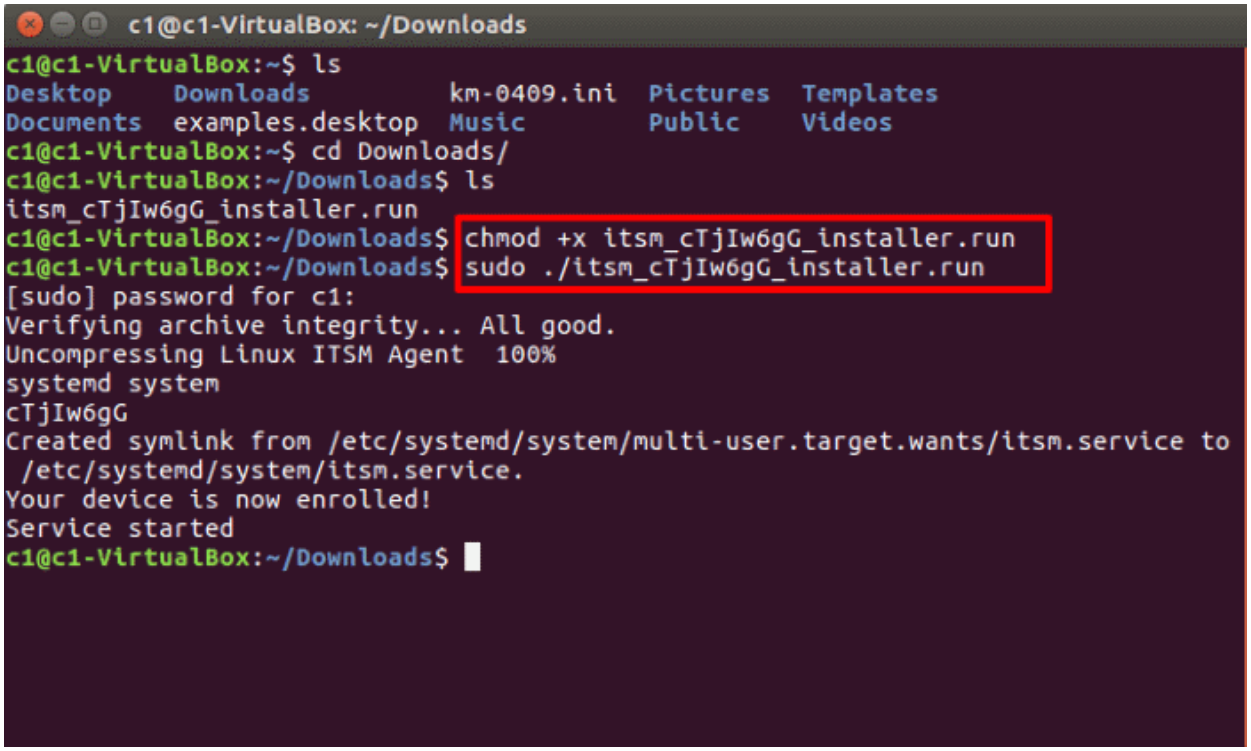
2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run



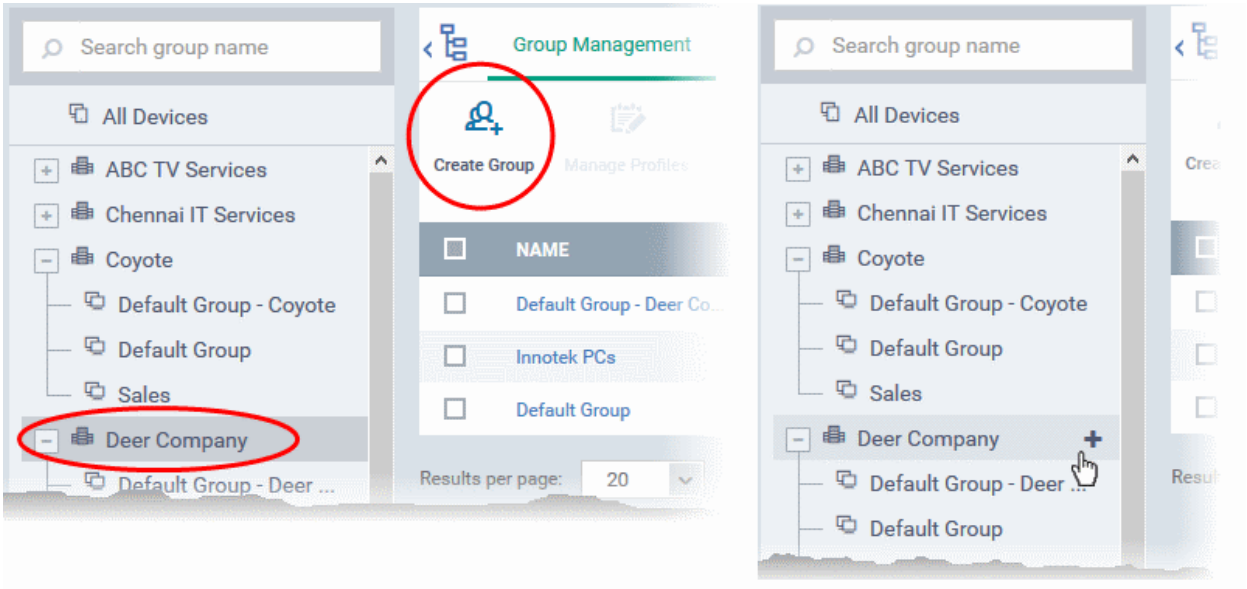
- The device is automatically added to Endpoint Manager once installation is complete. CCS is installed if you included it in the setup wizard.

Step 5 - Create Groups of Devices (optional)

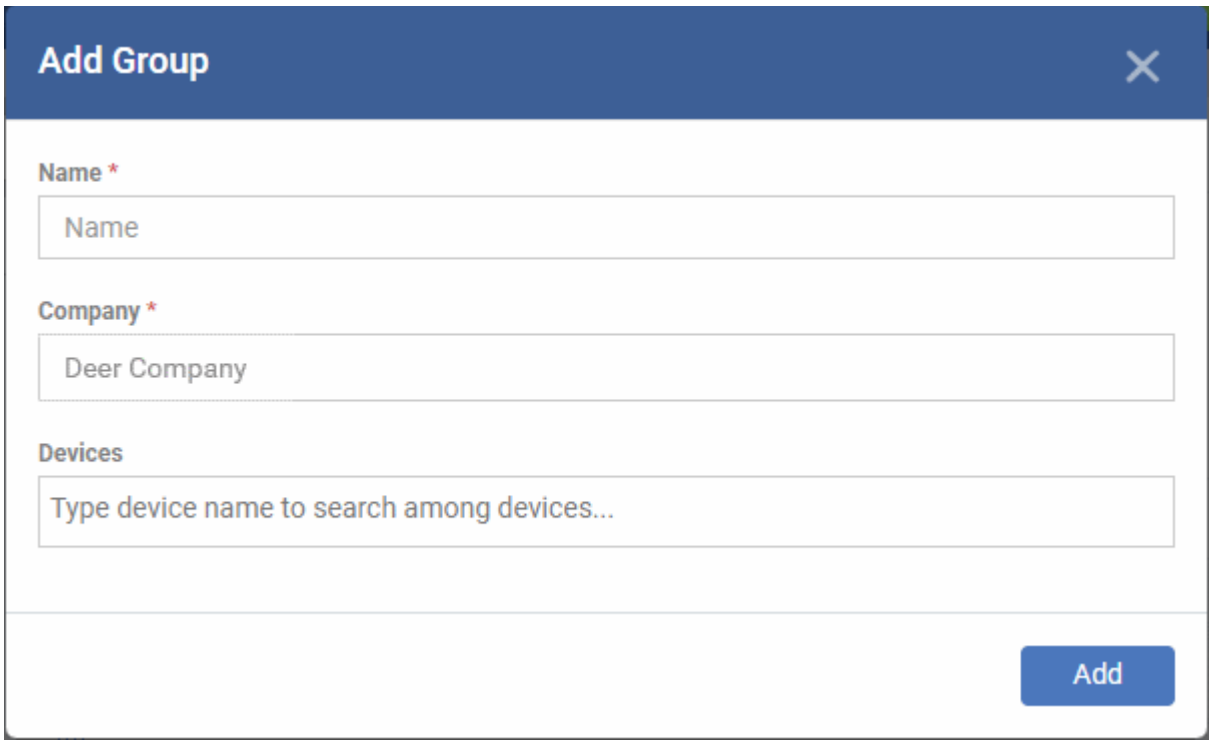
- Device groups allow you to apply profiles and actions to large numbers of devices. Dedicated configuration profiles can be created for each group.
- Groups can consist of devices of any OS type. Any OS-specific profiles you apply to a 'mixed' group will only get deployed those devices with a matching OS.
    - Dragon MSP / C1 MSP customers can create separate device groups for each company on their account.
    - Enterprise customers, and EM stand-alone customers, can only create groups under the 'Default Company'.

Create a device group

- Click 'Devices' > 'Device List'
- Click the 'Group Management' tab
    - CD MSP / C1 MSP customers should choose a company in the middle pane
- Click the 'Create Group' button
    - Alternatively, place your mouse over the company name and click the '+' sign that appears:



The 'Add Group' interface will open:



- You now have to name the group, assign it to a company, and choose its devices.
  - Type the first few letters of a device name in the field provided. Choose the required device from the suggestions that appear. Repeat the process to add more devices.
  - You can also add devices after the group is created.
- Click 'OK'. Repeat the process to create more groups.

The next step is to create profiles:

Step 6 - Create Configuration Profiles

- A configuration profile is a collection of settings which are applied to iOS, Android, Windows, Linux and Mac devices.
- Each profile lets you specify a device's network access rights, security settings, antivirus scan schedule, and other details.

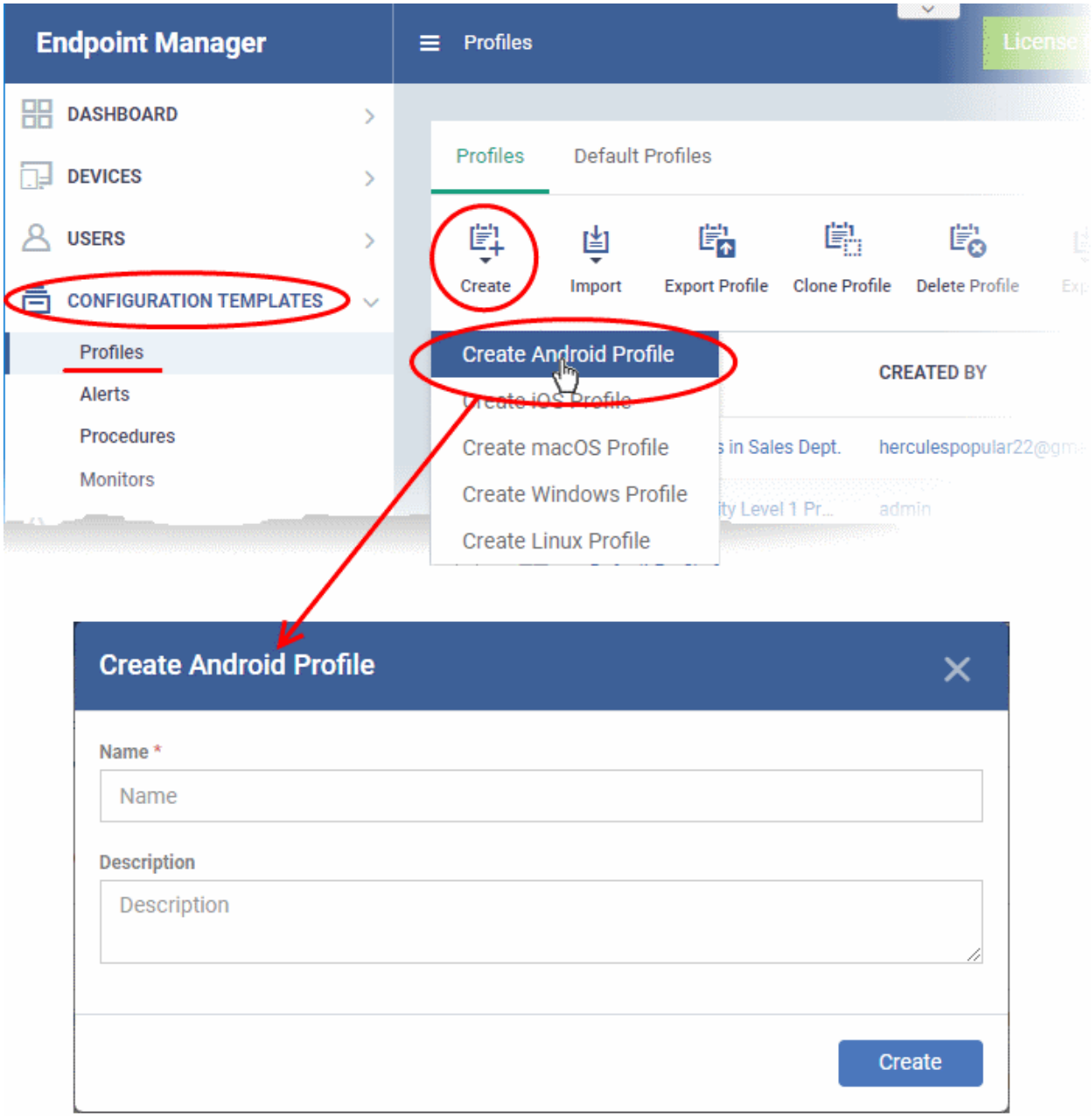
- There are two main types of profile - 'Custom' and 'Default'. You can create custom profiles for users and user groups.
- Default profiles are those that are applied if no custom profile exists. Default profiles are applied on a per-operating system basis. There are default profiles for all supported operating systems (Windows, Mac, iOS, Android and Linux).
    - This ensures all devices have a working profile installed. If you remove a custom profile then the default profile is automatically installed to take its place.
    - You can designate any profile you want as a 'default' profile. You can have multiple default profiles per operating system.
- Profiles are applied at the time a device connects to the network. Profiles remain in effect unless the communication client is uninstalled from the device, or the profile itself is removed/disabled.

Profile specifications differ between Android, iOS, Mac OS, Windows and Linux Devices:

- **Android profiles**
- **iOS profiles**
- **Mac OS profiles**
- **Windows Profiles**
- **Linux Profiles**

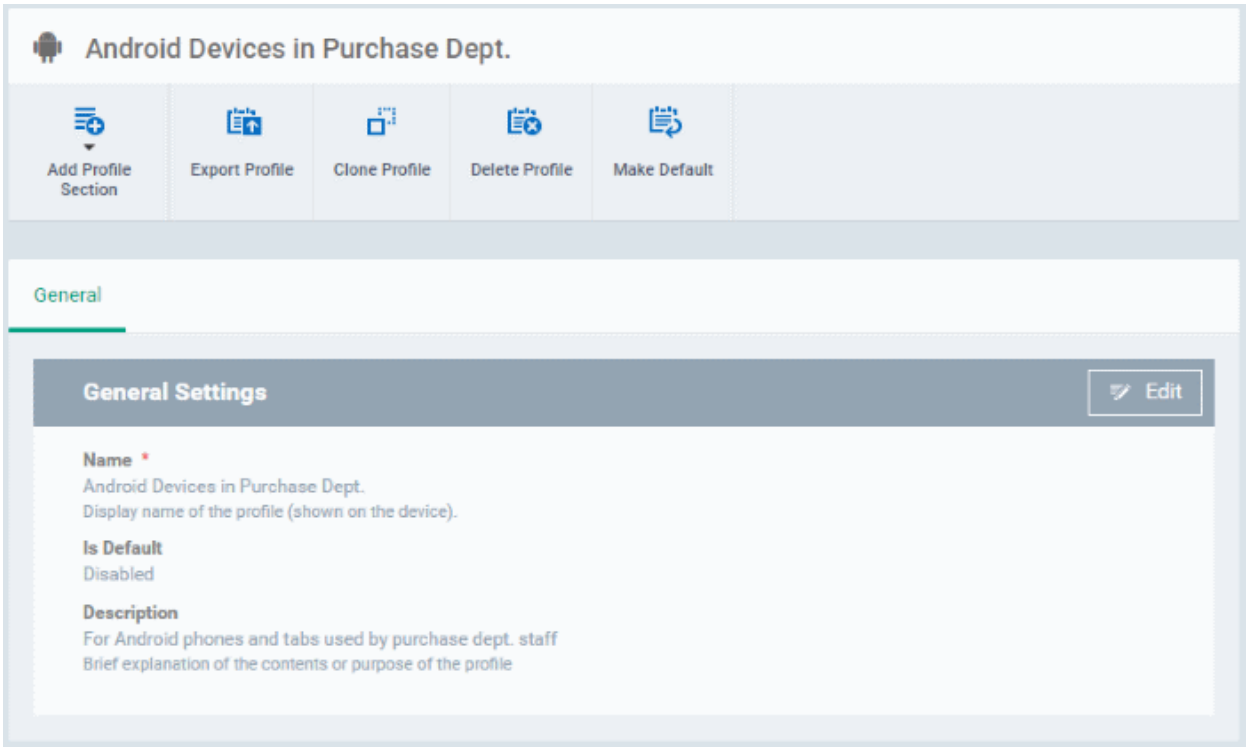
Create an Android Profile

- Click 'Configuration Templates' > 'Profiles'
- Click the 'Create' button > 'Create Android Profile':



- Enter a name and description for the profile and click 'Create'.

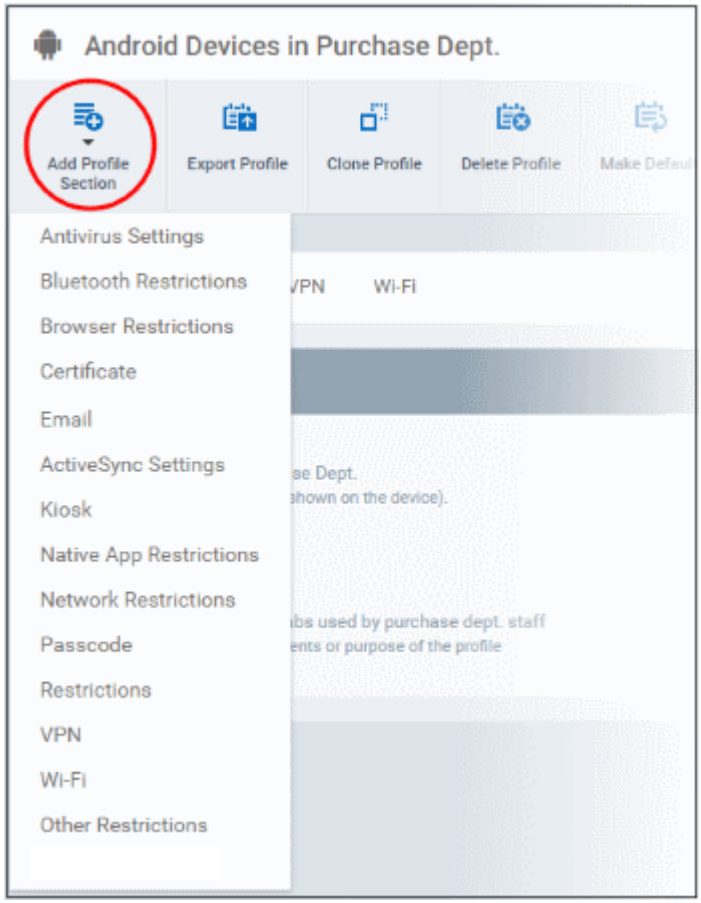
The profile opens at the 'General Settings' screen:



- Click the 'Make Default' button if you want to apply this profile to all devices with the target operating system.
  - Alternatively, click the 'Edit' button and enable the 'Is Default' check box.
- Click 'Save'.

The next step is to add components to the profile.

- Click the 'Add Profile Section' button and select a component that you want to add to the profile.



- The settings screen for the selected component will open. After saving, the new section will be available as a link when you open the profile.
- You can add as many sections as you require. Example sections include antivirus settings, feature restrictions and Wi-Fi settings.
- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

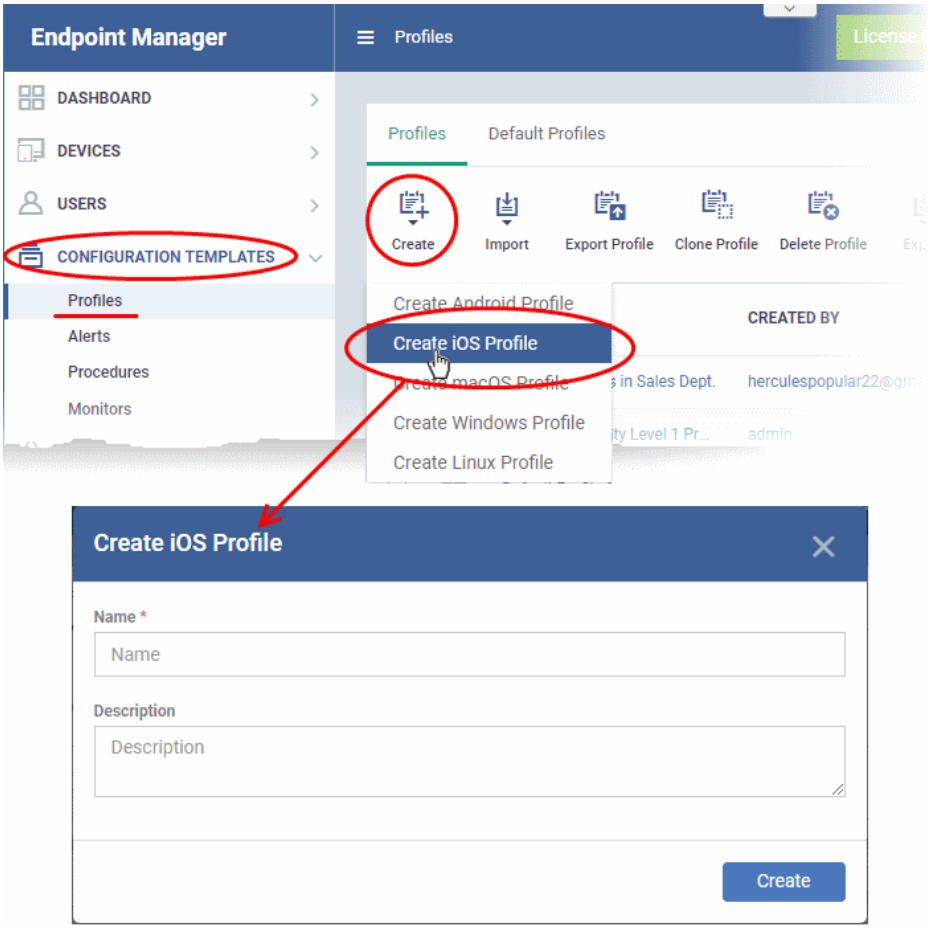
See **Profiles for Android Devices** in the full guide for more information on these settings. In brief:

- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. The 'Default' profiles are applied to every device which matches their operating system.
- **Antivirus Settings** - Schedule and configure antivirus scans on the device.
- **Bluetooth Restrictions** - Specify Bluetooth restrictions such as to allow device discovery via Bluetooth, allow outgoing calls and more. This profile is supported for SAFE devices only.
- **Browser Restrictions** - Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- **Certificate** - Upload certificates to Endpoint Manager. You can then choose these certificates when configuring specific features in Endpoint Manager. Examples include Wi-Fi, Exchange Active Sync and VPN.
- **Email** - Configure email account, connection and security details for users accessing incoming and outgoing mails from their devices. This profile is supported for SAFE devices only.
- **Active Sync Settings** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers. This profile is supported for SAFE devices only.
- **Kiosk** - Enable and configure Kiosk Mode for SAFE devices like the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices and whether SMS/MMS are allowed. This profile is supported for SAFE devices only.

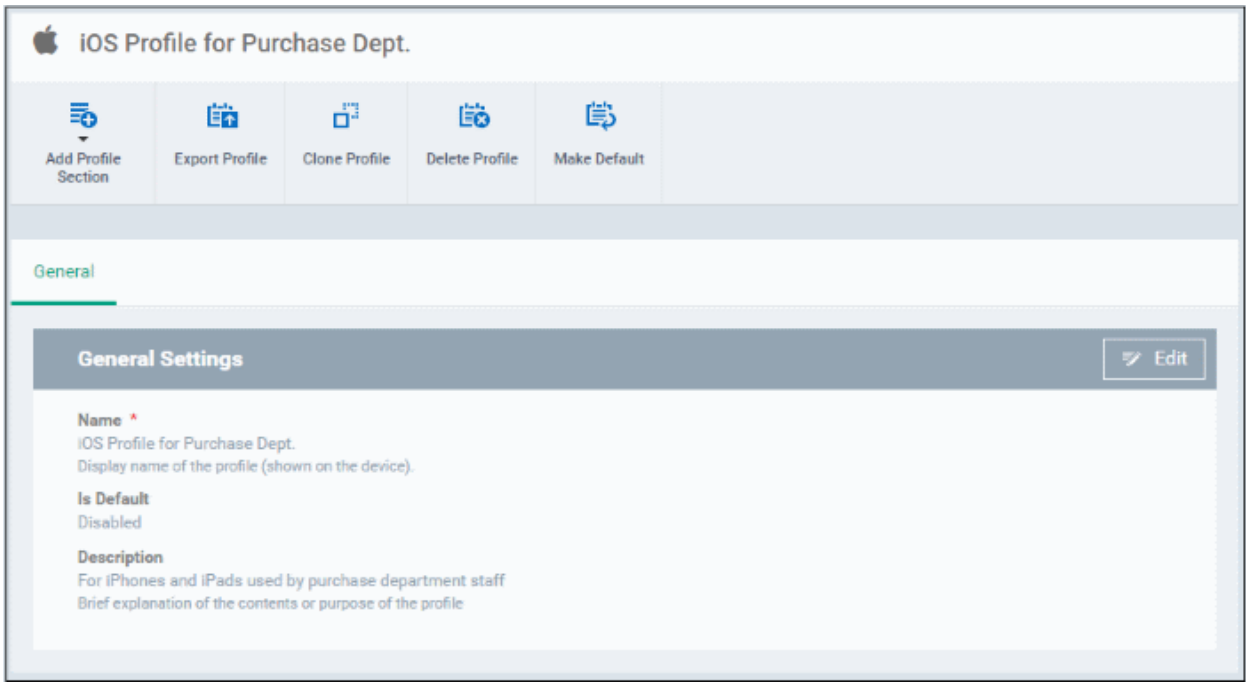
- **Native App Restrictions** - Configure which native applications should be accessible to users. Native applications are those that ship with the device OS and include apps like Gmail, YouTube, the default Email client and the Gallery. This feature is supported for Android 4.0+ and Samsung for Enterprise (SAFE) devices such as Galaxy smartphones, Galaxy Note devices and Galaxy tablets.
- **Network Restrictions** - Specify network permissions such as minimum level of Wi-Fi security required to access that Wi-Fi network, allow user to add more Wi-Fi networks in their devices, type of text and multimedia messages to be allowed and configure whitelist/blacklisted Wi-Fi networks. This profile is supported for SAFE devices only.
- **Passcode** - Specify passcode complexity, minimum length, timeout-before-lock, failed logins before wipe (0=unlimited/never wipe), failed logins before capturing the photo of the possessor and location to recover lost or mislaid device, maximum lifetime of passcode in days and number of previous passcodes from which the new passcode should be unique.
- **Restrictions** - Configure default device settings for Wi-Fi connection and cellular network connection, whether users should be able to disable app verification, background traffic, bluetooth on/off, whether camera use is allowed, whether the user is allowed to encrypt data stored on the device and whether or not they are allowed to install applications from unknown sources.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location, whether to forcibly maintain VPN connection and more. This profile is supported for SAFE devices only.
- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected. You can add other wireless networks by clicking 'Add new Wi-Fi section'.
- **Other Restrictions** - Configure a host of other permissions such as use of microphone, SD card, allow screen capture and more. This profile is supported for SAFE devices only.

Create an iOS Profile

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create iOS Profile'



- Enter a name and description for the profile and click 'Create'.
- The profile is created and the 'General Settings' for the profile is displayed.



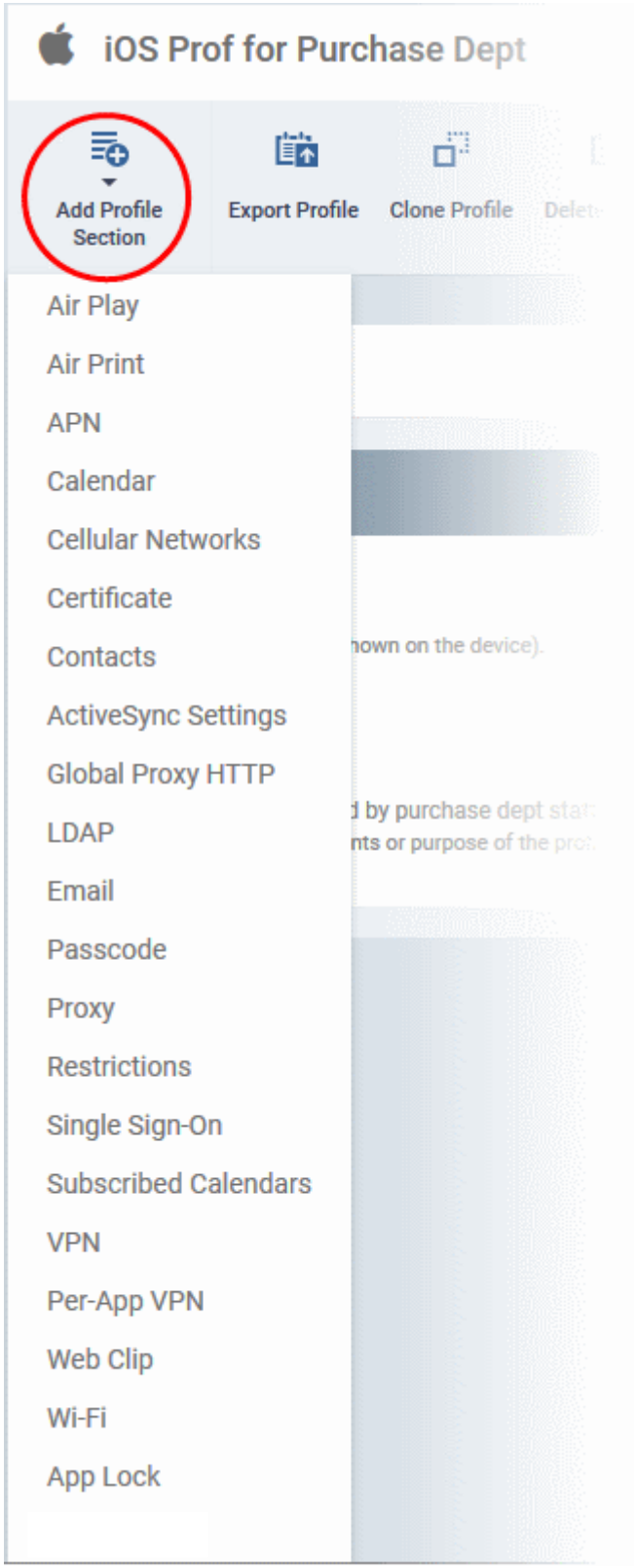
- If you want this profile to be a default policy, click the 'Make default' button at the top. Alternatively, click the 'Edit' button 

on the right of the 'General' settings screen and enable the 'Is Default' check box.

- Click 'Save'.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific management feature.
- For example, there are profile sections for 'Email', 'Single Sign-On', 'LDAP', 'Cellular Networks' and so on.
- You can add as many different sections as you want when building your device profile.
- To get started:
  - Click 'Add Profile Section'
  - Select the component that you want to add to the profile:



- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied upon device enrollment.
- **Airplay** - Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (iOS 7 +)
- **Airprint** - Specify the location of Airprint printers so they can be reached by devices under this profile (iOS 7 +)
- **APN** - Specify an Access Point Name for devices on this profile. APN settings define the network path for all cellular data. This area allows you to configure a new APN name (GPRS access point),

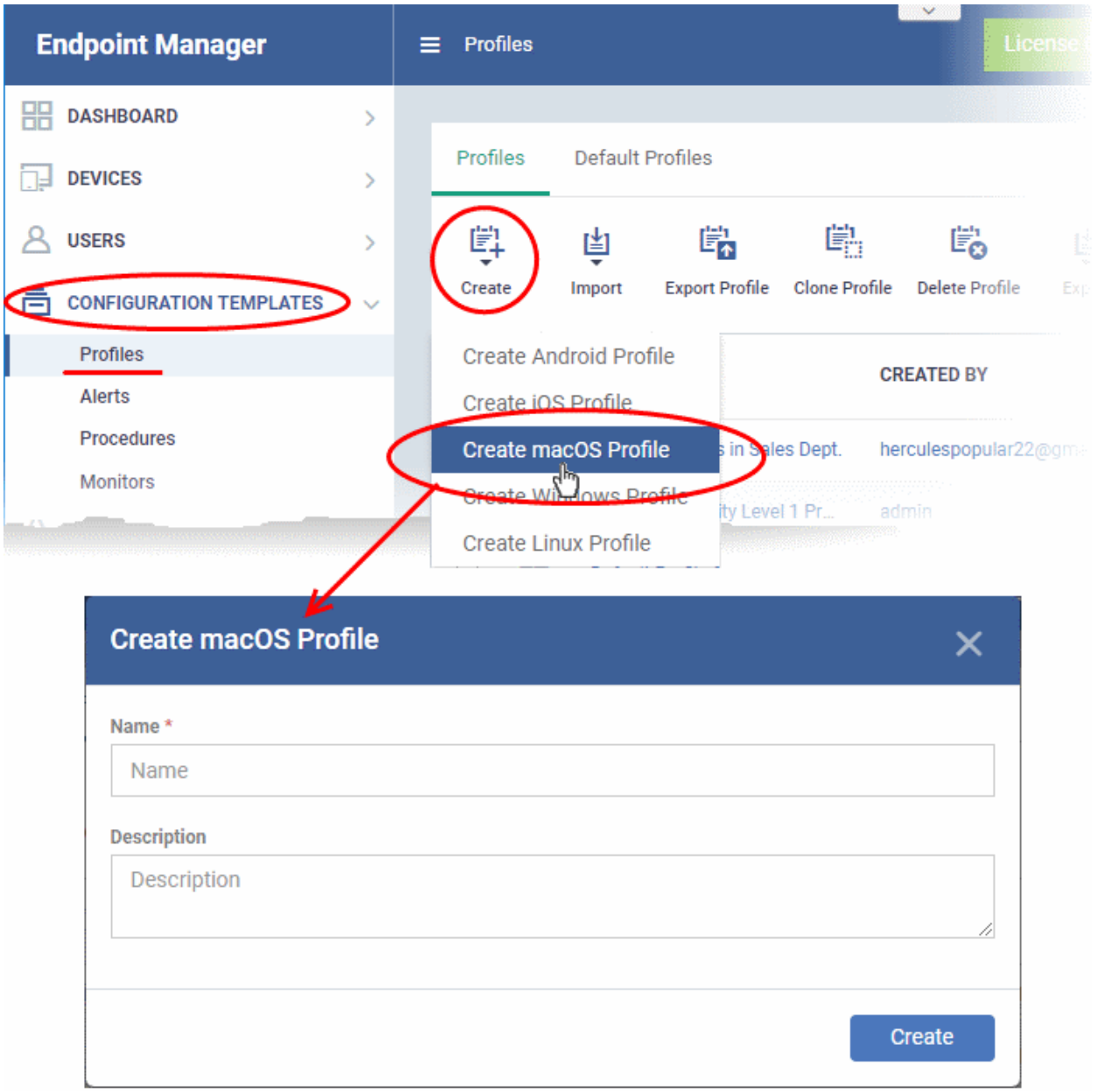
username/password and the address/port of the poxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.

- **Calendar** - Configure CalDAV server and connection settings which will allow device integration with corporate scheduling and calendar services.
- **Cellular Networks** - Configure cellular network settings. The 'cellulars' setting performs fulfills a similar role to the APN setting and actually replaces it in iOS 7 and above.
- **Certificate** - Upload certificates to Endpoint Manager. You can then choose these certificates when configuring specific features in Endpoint Manager. Examples include Wi-Fi, Exchange Active Sync and VPN.
- **Contacts** - Configure CardDAV account, host and user-settings to enable contact synchronization between different address book providers (for example, to synchronize iOS contacts and Google contacts).
- **Active Sync Settings**- Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.
- **Global HTTP Proxy** - Global HTTP proxies are used to ensure that all traffic going to and coming from an iOS device is routed through a specific proxy server. This, for example, allows the traffic to be packet-filtered regardless of the network that the user is connected through.
- **LDAP** - Configure LDAP account settings for devices under this profile so users can connect to company address books and contact lists.
- **E-mail** - Configure general mail server settings including incoming and outgoing servers, connection protocol (IMAP/POP), user-name/password and SMIME/SSL preferences.
- **Passcode** - Specify passcode complexity, minimum length, timeout-before-lock, failed logins before wipe (0=unlimited/never wipe), failed logins before capturing the photo of the possessor and location to recover lost or mislaid device, maximum lifetime of passcode in days and number of previous passcodes from which the new passcode should be unique.
- **Proxy** - Allows you to specify the proxy server, and their credentials, to be used by the device for network connections.
- **Restrictions** - Configure default device settings for Wi-Fi connection and cellular network connection, whether users should be able to disable app verification, background traffic, bluetooth on/off, whether camera use is allowed, whether the user is allowed to encrypt data stored on the device and whether or not they are allowed to install applications from unknown sources.
- **Single Sign-On** - iOS 7 +. Configure user credentials that can be used to authenticate user permissions for multiple enterprise resources. This removes the need for a user to re-enter passwords. In this area, you will configure Kerberos principal name, realm and the URLs and apps that are permitted to use Kerberos credentials for authentication.
- **Subscribed Calendars** - Specify one or more calendar services which you wish to push notifications to devices under this profile.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location. This profile is supported for iOS 7 and above.
- **VPN Per App** - Configure VPN as above but on a per-application basis. This profile is supported for iOS 7 and above.
- **Web Clip** - Allows you to push a shortcut to a website onto the home-screen of target devices. This section allows you to choose an icon, label and target URL for the web-clip.
- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected.
- **App Lock** - Configure restrictions on usage of device resources for selected applications.

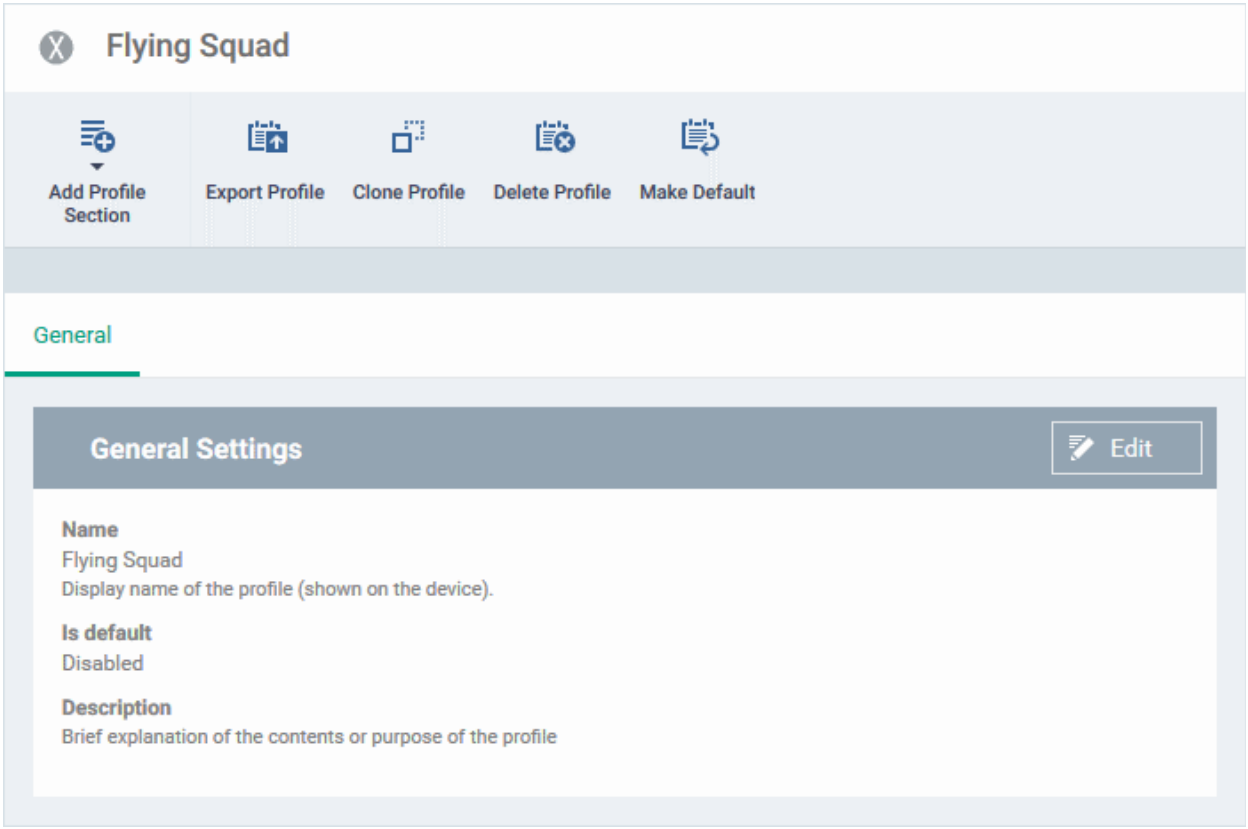
See **Profiles for iOS Devices** in the main guide for more details on this area. In brief, iOS device profiles are more detailed than Android profiles.

Create a Mac OS Profile

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create Mac OS Profile'



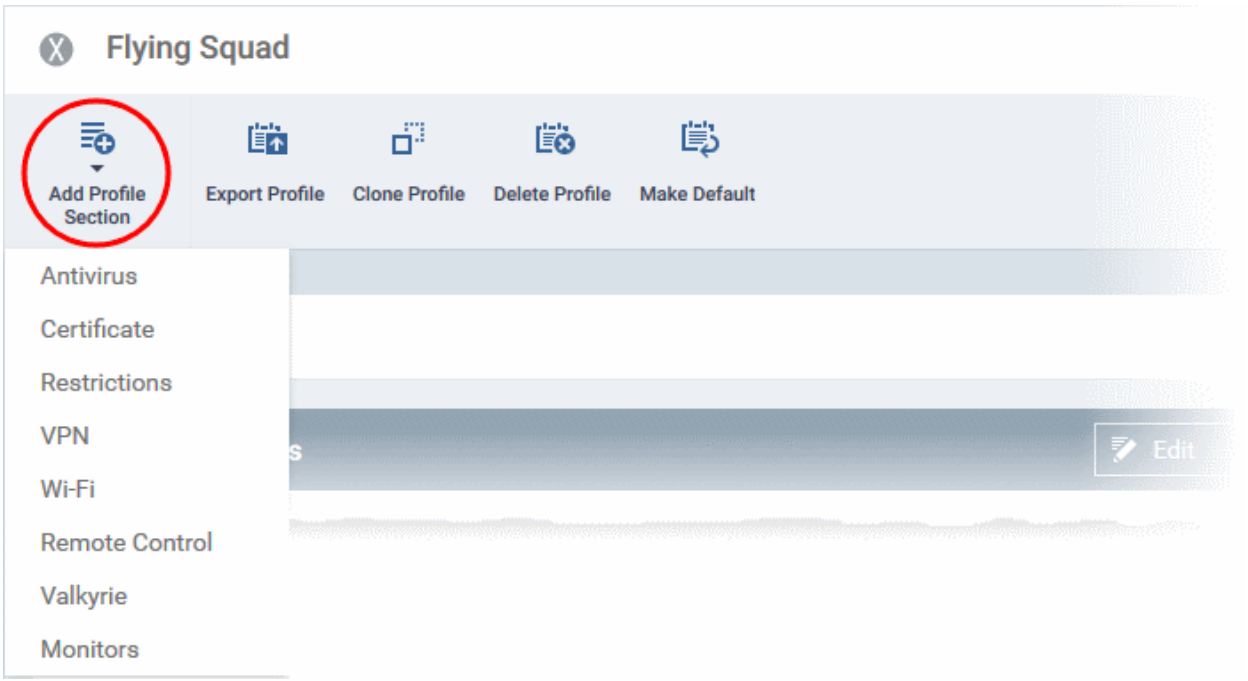
- Enter a name and description for the profile (for example, 'Sales Dept Mac machines', 'Mac Air Books' or 'Field Executives Laptops') and click 'Create'.
- The profile will be created and the 'General Settings' for the profile will be displayed.



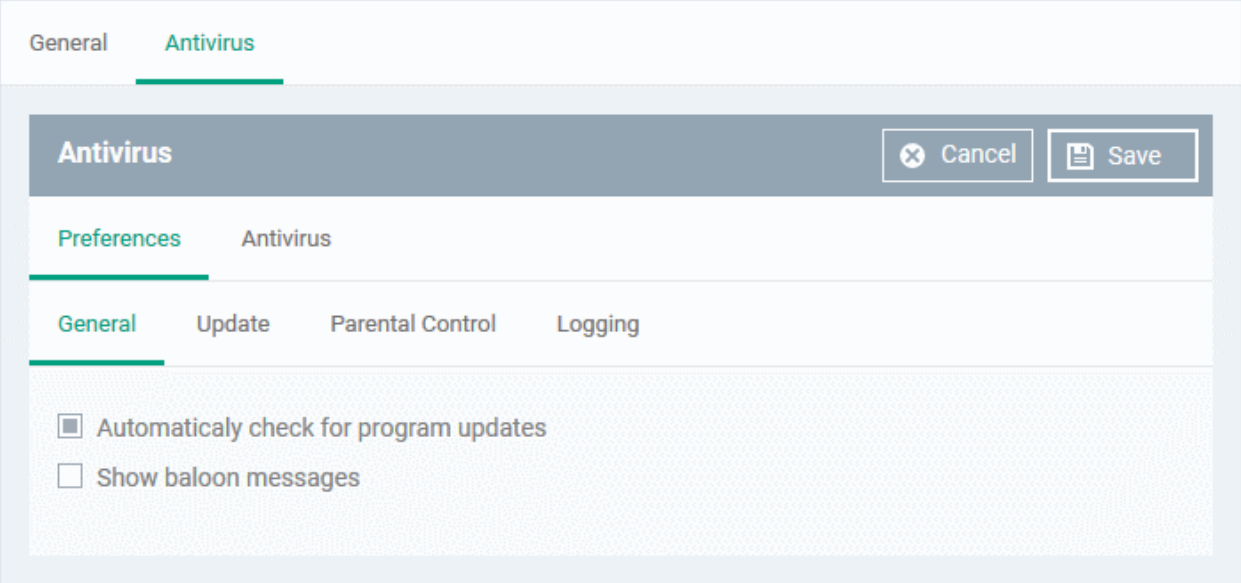
- **'Make Default'** - A 'default' profile is one that is applied automatically to any newly added device which matches its operating system. Click this button if you want all MAC OS devices to receive this profile.
- Click 'Save'.

The next step is to add sections to the profile. Each section lets you define settings for a particular security or management feature.

- Click 'Add Profile Section' then select the section you want to add from the list:



The new section will appear as a tab under the profile name. You can add as many sections as required to a profile.



- Configure the settings and click 'Save'.

The new section will become available as a tab. You can configure antivirus settings, certificate settings, device restrictions, VPN connection parameters, Wi-Fi connection parameters and more. If a component is not configured, the device will continue to use existing settings, or settings that have been applied by another EM profile.

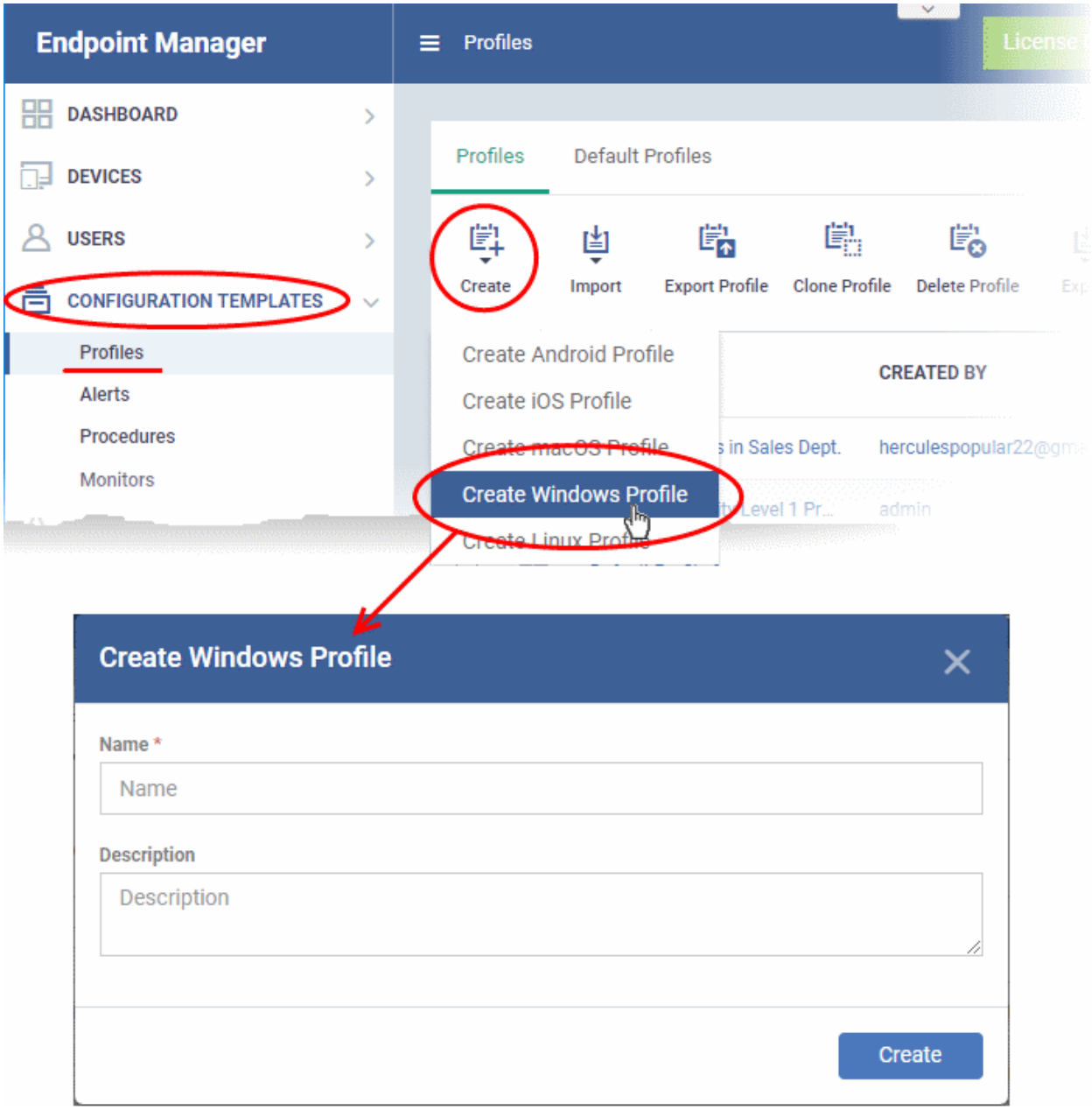
- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

See **Profiles for Mac OS Devices** in the main guide for more details on this area. In brief:

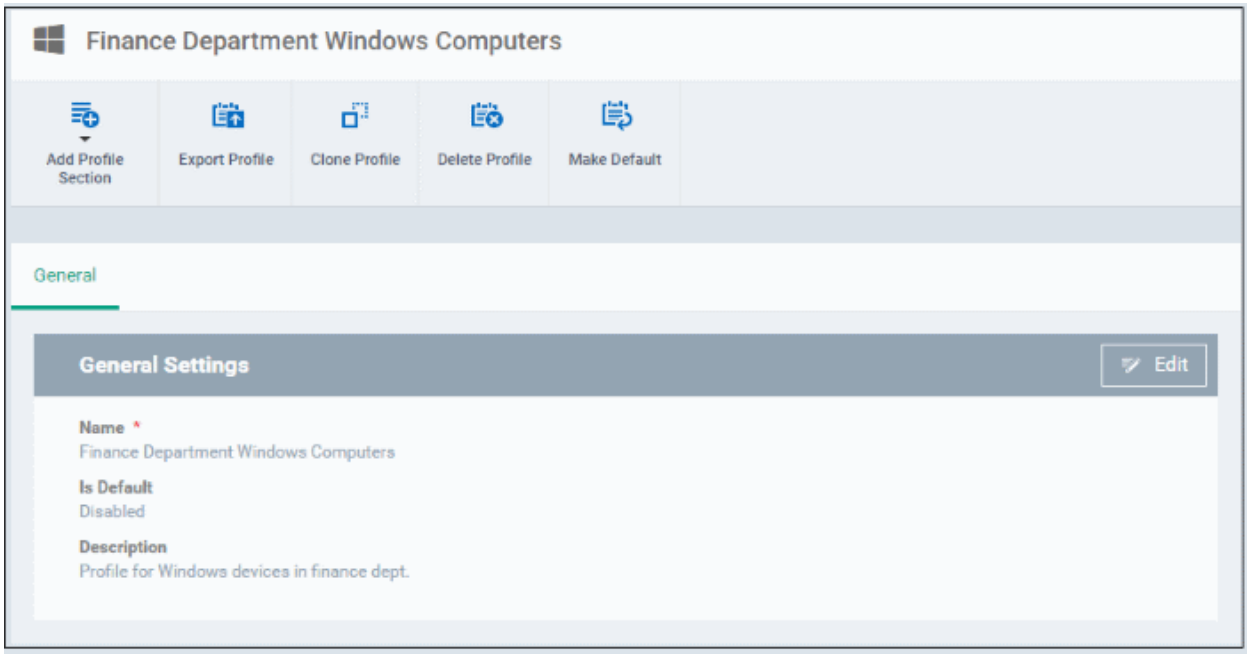
- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **Certificates** - Upload certificates to Endpoint Manager. You can then choose these certificates when configuring specific features in Endpoint Manager. Examples include Wi-Fi, Exchange Active Sync and VPN.
- **Restrictions** - Configure restrictions on device functionality and features, iCloud access and so on.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location and more.
- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected.
- **Remote Control** - Allows you to configure settings for remote takeover and notifications which are shown to end-users before and during a remote control session.
- **Valkyrie Settings** - Valkyrie is a cloud-based file verdict service that subjects unknown files to a range of tests in order to identify those that are malicious. Configure settings for Valkyrie cloud look up service.
- **Monitors** - Configure performance and availability conditions for various events. An alert is triggered if the conditions are breached. For example, you can monitor free disk space, CPU/RAM usage, device online status and more.

Create a Windows profile

- Click 'Configuration Templates' > 'Profiles' > 'Create' > 'Create Windows Profile':



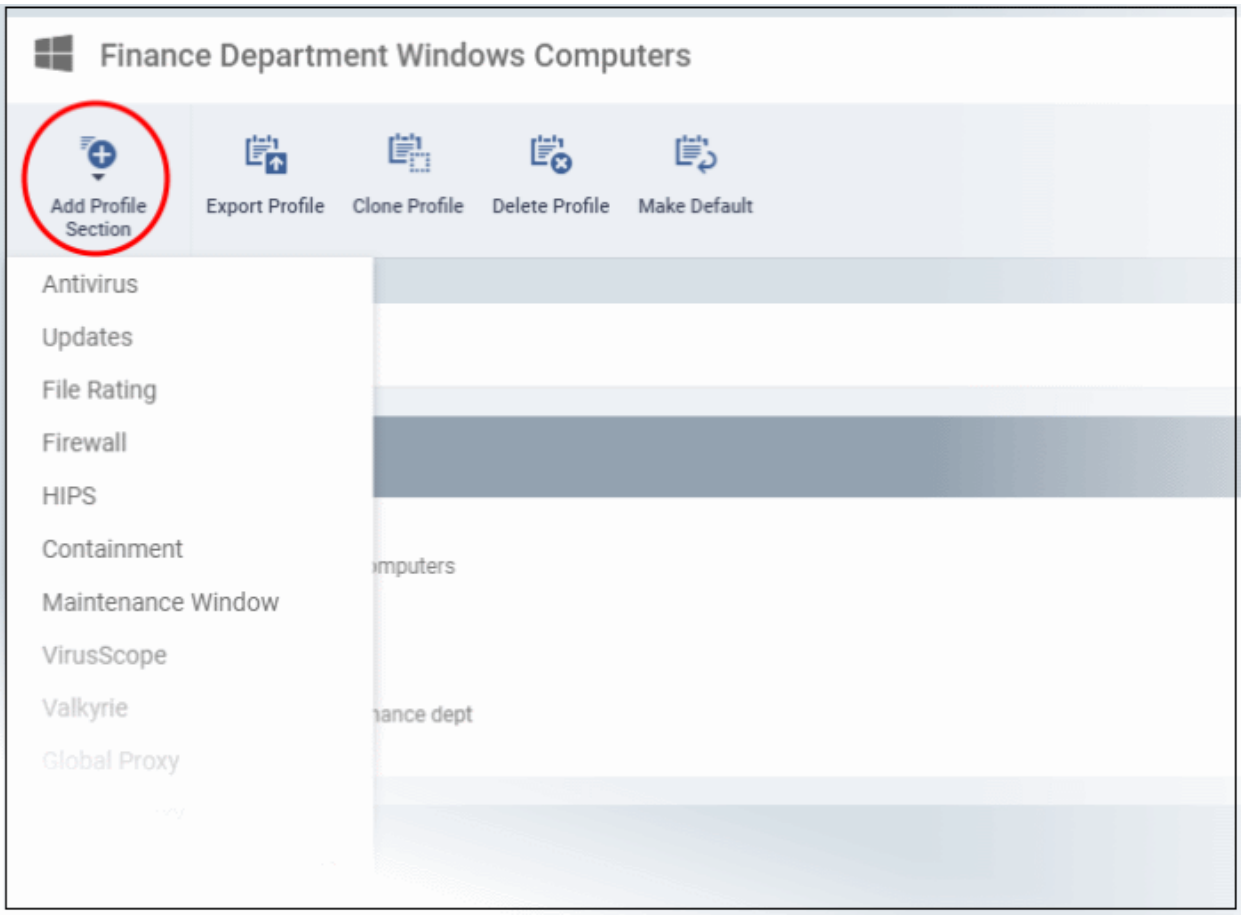
- Enter a name and description for the profile (for example, 'Sales Dept endpoints', 'Win7 Machines' or 'Field Executives Laptops') and click 'Create'.
- The profile will be created and the 'General Settings' for the profile will be displayed.



- Click 'Edit' if you wish to modify basic profile settings:
  - 'Is Default?' - If a policy is set as 'Default' then it is automatically applied to any Windows device that does not have a custom policy. You can have multiple 'default' policies to address different requirements.
- Click 'Save'.

The next step is to add the components for the profile.

- Click the 'Add Profile Section' drop-down button and select the component that you want to include in the profile.



The settings screen for the selected component will open.

- Configure the settings and parameters and click 'Save'

The new section will become available as a tab in this interface. You can configure Antivirus, Firewall, Containment, File Rating, Valkyrie, HIPS, Monitoring, Procedures, External devices control, Remote control, VirusScope, Logging, Update and Miscellaneous settings. In addition, you can configure the Proxy and Agent Discovery Settings for each profile, for use in Firewall and HIPS rules configured for the profile.

If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another EM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

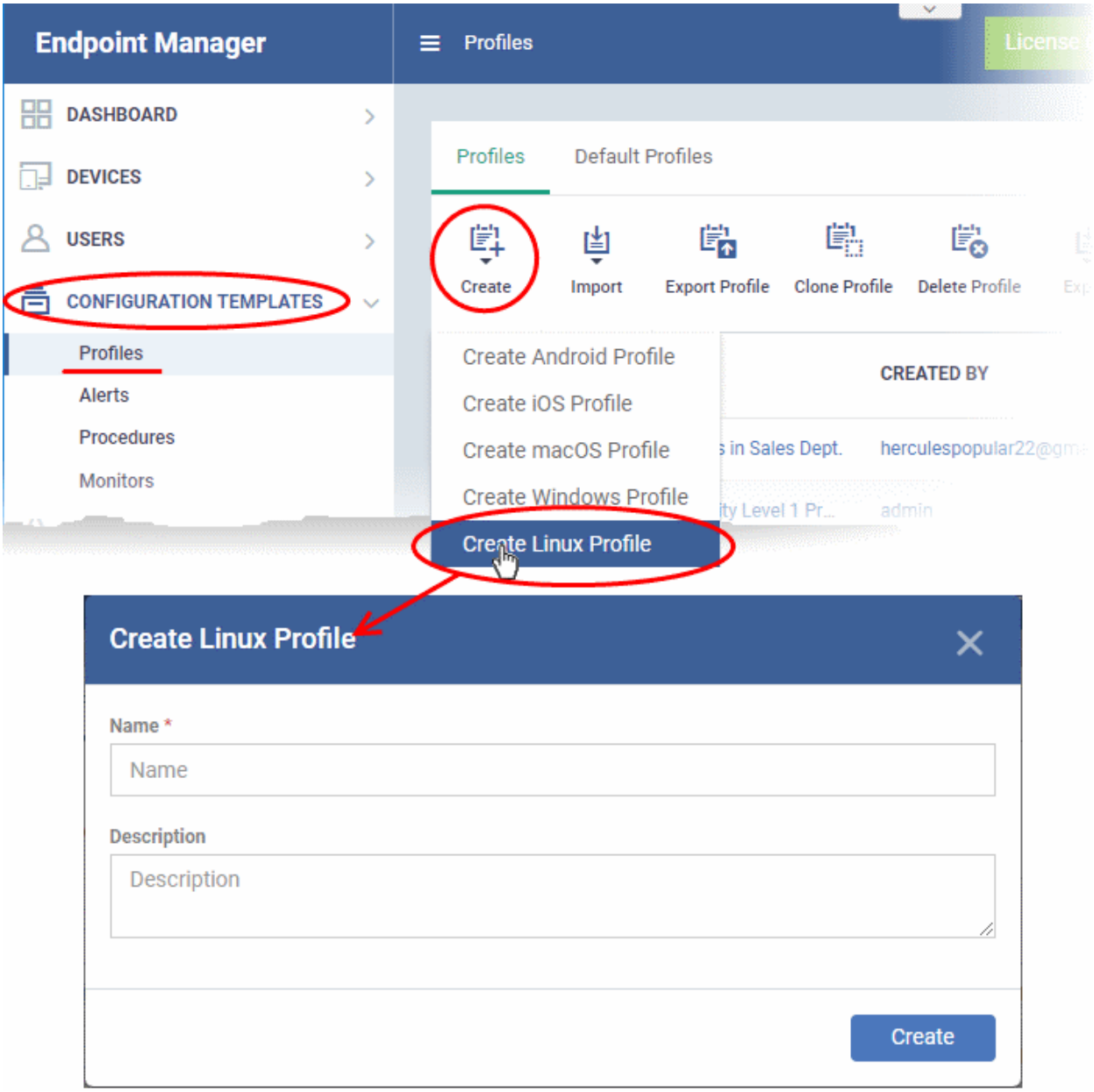
See **Profiles for Windows Devices** in the full guide for more information on these settings. In brief:

- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **Updates** - Set the conditions for Comodo Client Security (CCS) to automatically download and install program and virus database updates.
- **File Rating** - Enable cloud lookup for checking reputation of files accessed in real-time, configure options for files to be trusted and detecting potentially unwanted applications. For more details on File Rating in CCS, refer to the **help page explaining File rating Settings** in **CCS online help guide**.
- **Firewall** - Enable/Disable the Firewall component, configure Firewall behavior, add and manage Application and Global Firewall rules and more. See **help page explaining Firewall Settings** in **CCS online help guide**, for more details on Firewall in CCS.
- **HIPS** - Enable Host Intrusion Prevention System (HIPS) and its behavior, configure HIPS rules and define Protected Objects at the endpoints. See **help page explaining HIPS Settings** in **CCS online help guide**, for more details on HIPS in CCS.

- **Containment** - Enable auto-containment of unknown files, add exclusions, configure containment behavior, view and manage auto-containment rules and configure the Virtual Desktop. See help page explaining **Containment** in **CCS online help guide**, for more details on Containment in CCS.
- **Maintenance Window** - A maintenance window (MW) is a scheduled time-slot when admins can run important tasks on target devices. Admins can enable a warning if somebody attempts to run a task outside of a maintenance window.
- **VirusScope** - Enable VirusScope that monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten your privacy and/or security and configure options for alert generation. See **help page explaining VirusScope**, for more details on VirusScope in CCS online help guide.
- **Valkyrie** - Valkyrie is a cloud based file analysis system. look-up system. It uses a range of static and dynamic detectors including heuristics, file look-up, real-time behavior analysis and human expert to analyze the submitted files and determine if the file is good or bad (malicious). You can enable Valkyrie and its components and set a schedule for submitting unknown files identified from the endpoints.
- **Global Proxy** - Specify a proxy server through which endpoints should connect to external networks like the internet.
- **Clients Proxy** - Specify proxy servers through which Comodo endpoint clients should connect to Endpoint Manager and other Comodo services. Clients which will use this proxy are Comodo Client Security (CCS) and Comodo Communication Client (CC).
- **Agent Discovery Settings** - Specify whether or not communication client should send logs to EM about antivirus and containment events.
- **UI Settings** - Configure the appearance of the communication client (CC) and Comodo Client Security (CCS). You can re-brand CC and CCS with your own company name, logo, product name and product logo and select which components of CCS should be visible to end-users.
- **Logging settings** - Enable event logs, configure max. log file size and other settings.
- **Client Access Control** - Password-protect Comodo Client Security (CCS) and communication client (CC) on managed endpoints.
- **External Device Control** - Block or permit specific types of device from connecting to managed endpoints. Example devices you may want to control are USB storage devices and Bluetooth devices.
- **Monitors settings** - Configure performance and availability conditions for various events and services. An alert will be triggered if the conditions are breached. For example, you can monitor free disk space, service and web page availability, CPU/RAM usage, device online status and more.
- **Procedures** - Allows you to add, view, delete and prioritize procedures which have been added to a profile.
- **Remote Control** - Configure remote access settings.
- **Remote Tools** - Enable/disable remote access to endpoint files and processes. You can also configure how notifications are shown during a remote session.
- **Miscellaneous** - Monitor the registry for changes to auto-run items, services, and scheduled tasks by unrecognized files.
- **Script Analysis settings** - Enable / disable Heuristic command line analysis and embedded Code Detection and select programs to be monitored.
- **Data Loss Prevention settings** - Data loss prevention scans identify files containing sensitive information on managed Windows devices. For example, the scans find credit card numbers, social security numbers, bank account numbers, etc. You can then take actions to secure that data where required.

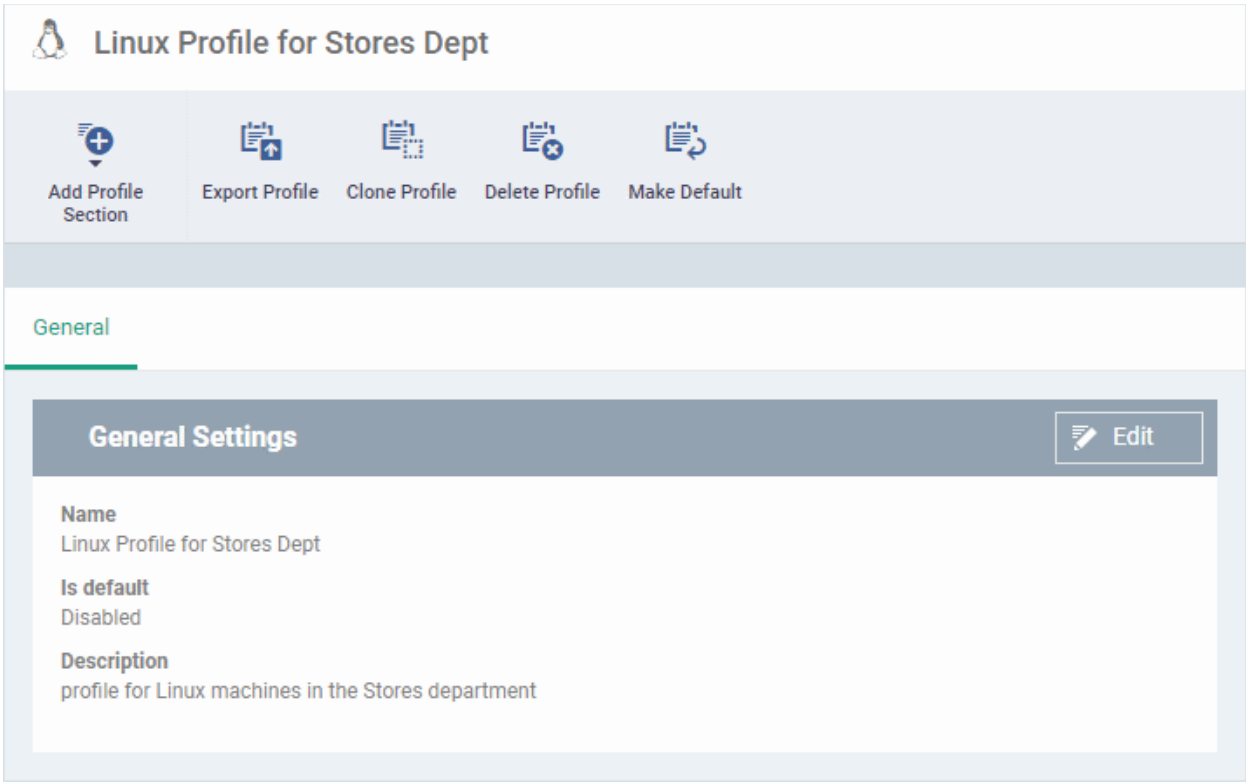
Create a Linux Profile

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create Linux Profile'



- Enter a name and description for the profile
- Click the 'Create' button

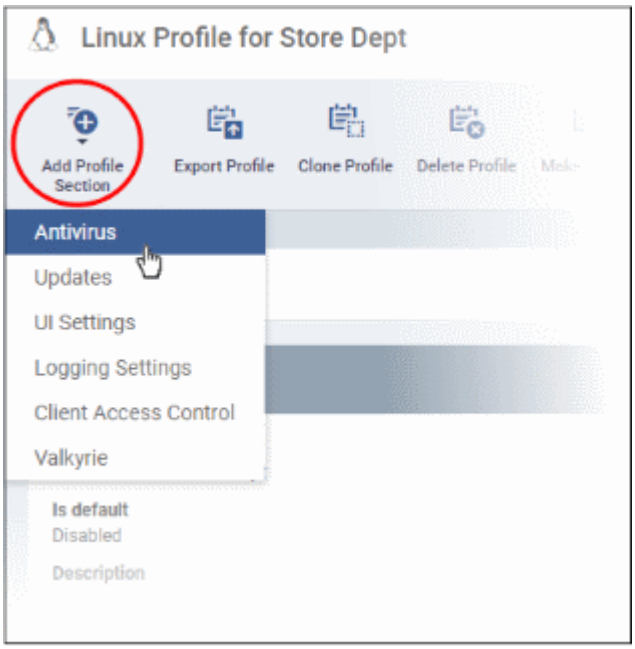
The Linux profile will be created and the 'General Settings' section will be displayed. The new profile is not a 'Default Profile' by default.



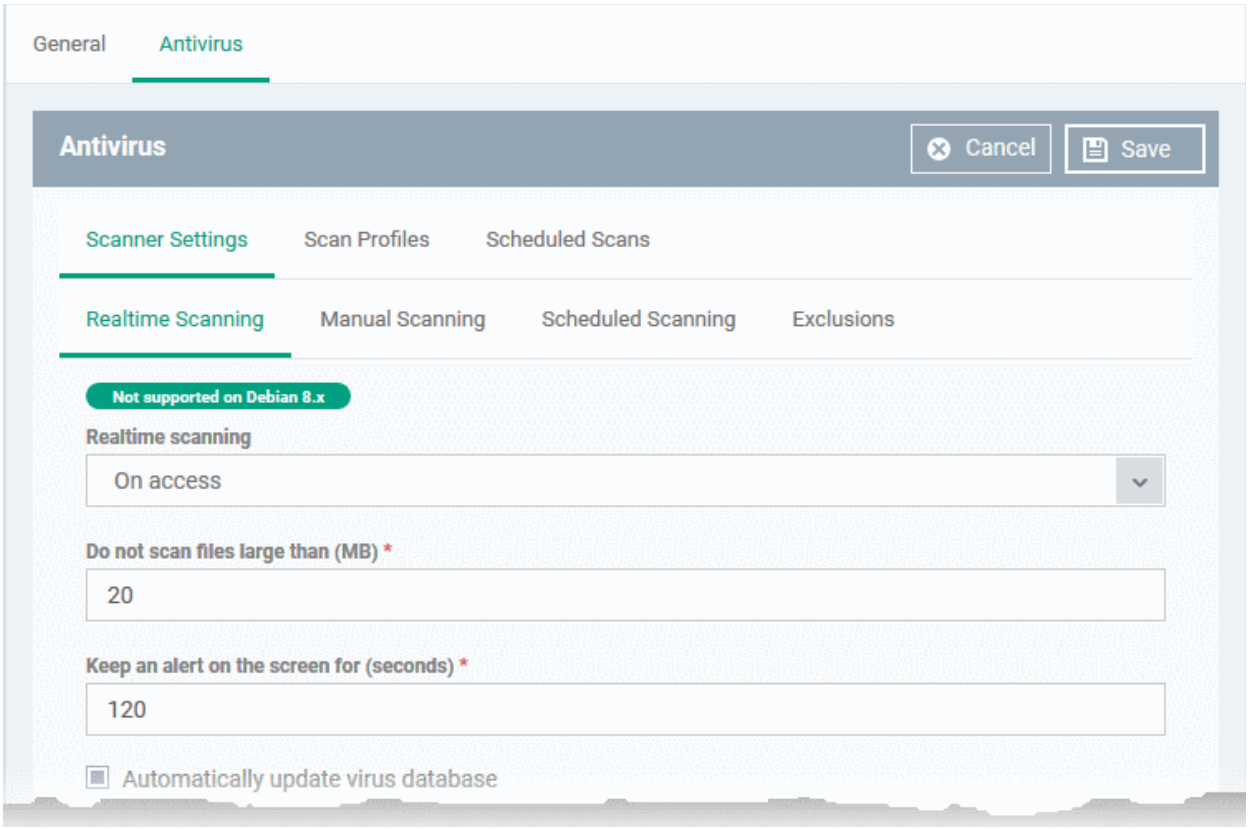
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

The next step is to add the components for the profile.

- Click the 'Add Profile Section' drop-down button and select the component from the list that you want to include for the profile.



The settings screen for the selected component will be displayed. An example is shown below:



- Configure the settings and click 'Save'.

The new section will become available as a tab. You can configure antivirus settings, interface language settings, logging settings, password protection to the CCS application on the endpoint and more. If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another EM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

See **Profiles for Linux Devices** in the main guide for more details on this area. In brief:

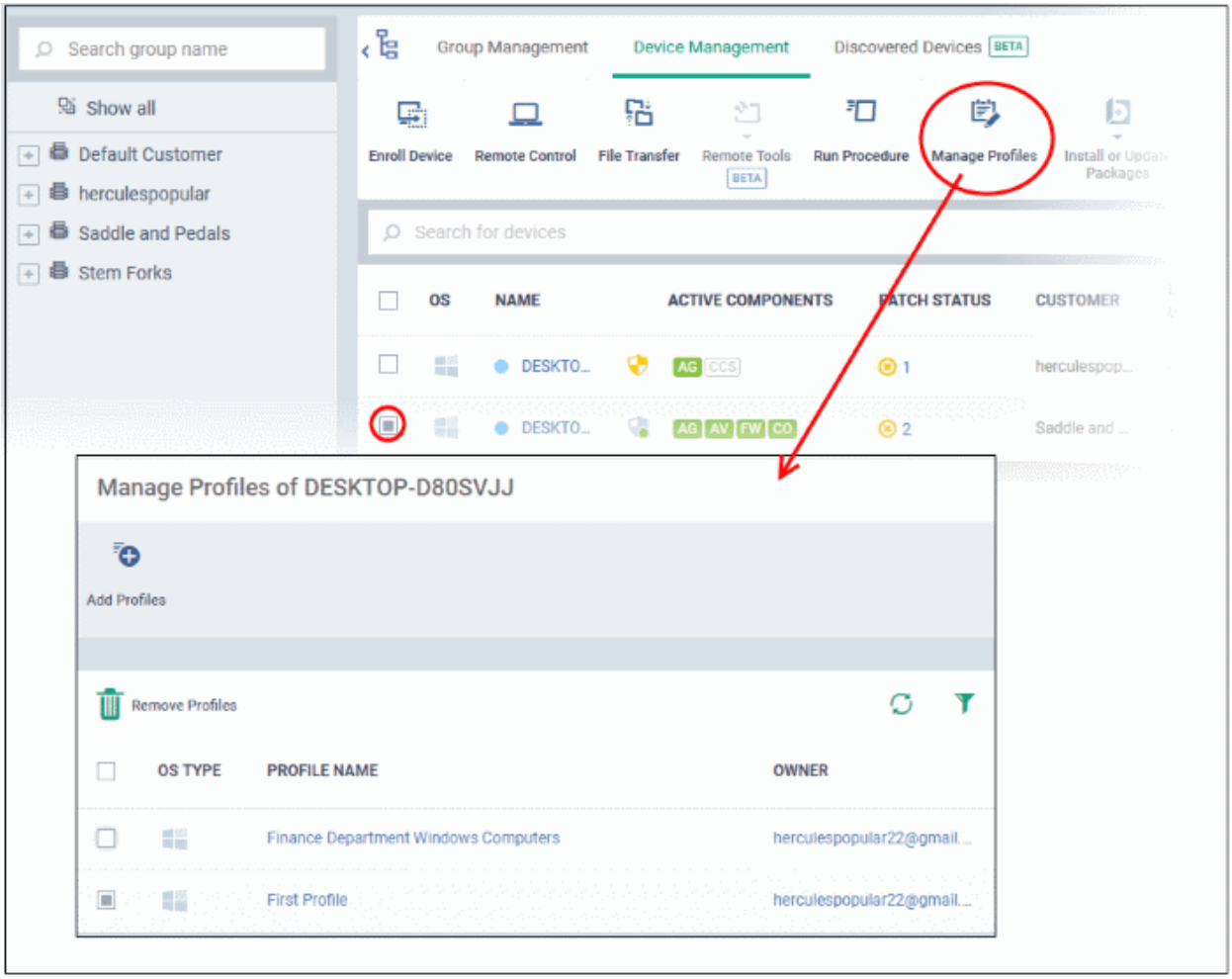
- **Antivirus** - Enable on-access scanning of files, configure scan profiles, timetable scheduled scans, set maximum size for files to be scanned, files to be excluded and more.
- **Updates** - Enable/disable program and virus signature database updates, configure the server from which the updates are to be downloaded and more.
- **UI Settings**- Select the interface language for CCS on the endpoint.
- **Logging Settings** - Enable event logs, configure max. log file size and other settings.
- **Client Access Control** - Password protect access to the CCS application on the endpoint.
- **Valkyrie Settings** - Valkyrie is a cloud-based file verdict service that subjects unknown files to a range of tests in order to identify those that are malicious. Configure settings for Valkyrie cloud look up service.

Step 7 - Apply profiles to devices or device groups

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM

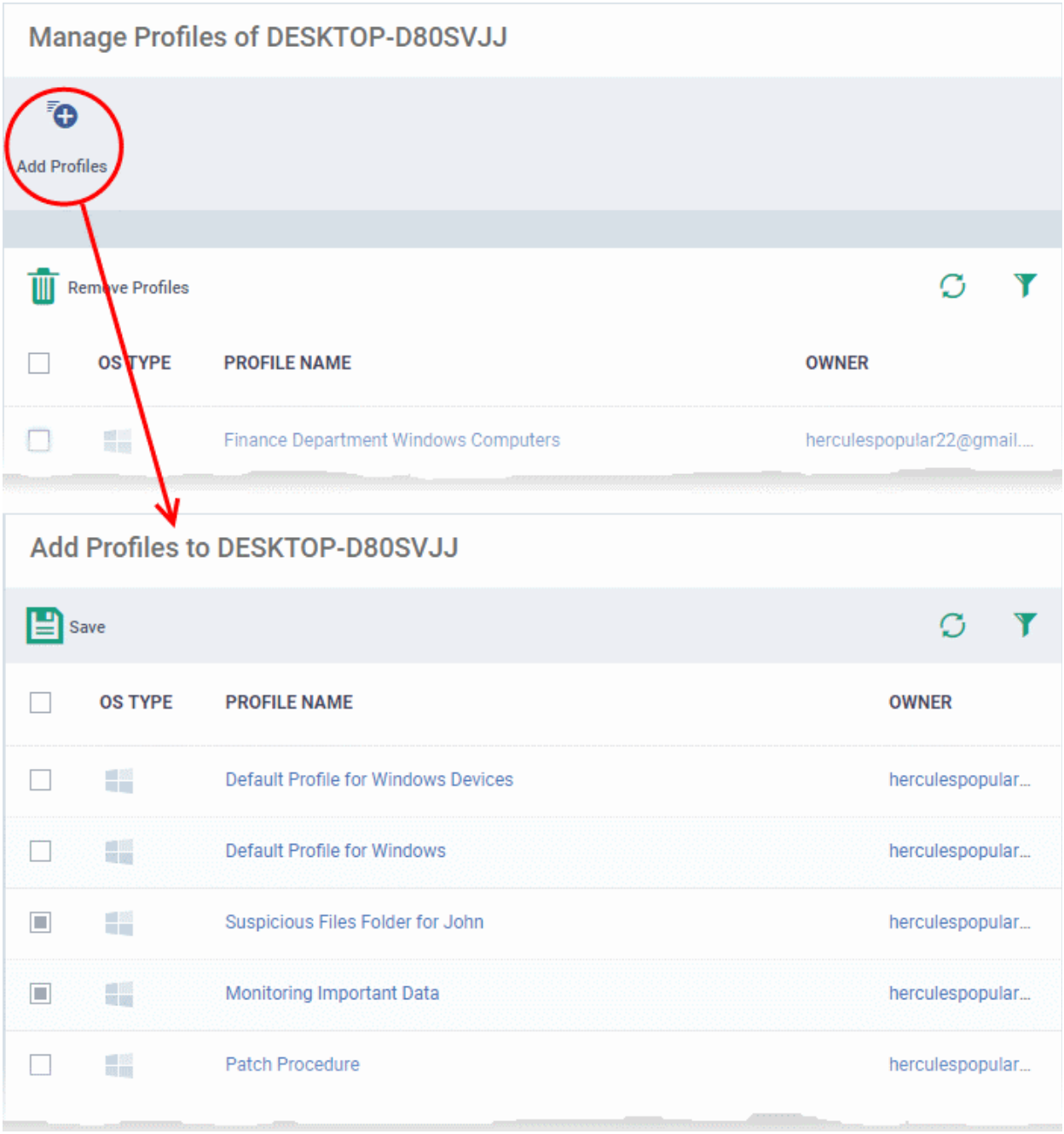
- Select the device you want to manage and click 'Manage Profiles':



The screen lists all profiles active on the device.

- Click 'Add Profiles'

This will open a list of all suitable profiles chosen device, excluding those that are already applied.



- Select the profiles you want to apply to the device
- Click 'Save' at top-left to apply the profiles to the device.

Apply profiles to a *group* of devices

This is the same as the single device process except for the second step.

1. Click the 'Devices' tab on the left and choose 'Device List ' from the options.
2. Click the 'Group Management' tab
3. Choose the Company to view the list of groups in the right pane (for C1 MSP customers)
4. Click the name of the device group
5. Click 'Manage Profiles'
6. Select the profiles to be applied to the devices in the group
7. Click 'Add Selected' at the top-left to add the profiles to the device group

If you have successfully followed all 7 steps of this quick start guide then you should have a created a basic working environment from which more detailed strategies can be developed.

Should you need further assistance, each topic is covered in more granular detail in the full administrator guide. If you have problems that you feel have not been addressed, then please contact **mdmsupport@comodo.com**.

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: **mailto:EnterpriseSolutions@Comodo.com**