

# Comodo Dragon Enterprise Endpoint Protection Platform

Software Version 6.38

## Quick Start Guide

Guide Version 6.38.110520

# Dragon Enterprise - Endpoint Protection Platform - Quick Start

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

**Step 1 - Enrollment and Configuration**

**Step 2 - Configure Dragon Communications**

**Step 3 - Add Users**

**Step 4 - Enroll User Devices**

**Step 5 - Create Groups of Devices (optional)**

**Step 6 - Create Configuration Profiles**

**Step 7 - Apply profiles to devices or device groups**

**Step 8 - Upgrade to full version**

**Note** - Dragon Enterprise 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

- Getting a Dragon Enterprise Platform account is a simple process which can be completed in a few steps.
- You can sign-up for a 30 day trial account at <https://enterprise.platform.comodo.com/signup>
- Dragon Enterprise 30 day trial version ships with:
  - 10 Endpoint Detection and Response (EDR) trial licenses - You can install EDR agent on up to 10 Windows devices for EDR to collect the alerts and security events. The data retention period for these data is three days.
  - Advanced Endpoint Protection (AEP) Trial version - You can enroll any number of devices to Dragon. The term of AEP trial version is 30 days.
- Once signed-up, you can upgrade to full version by purchasing AEP and EDR licenses from Comodo Account Manager (CAM) at <https://cam.comodo.com/>.

### Sign-up for a trial account

- Visit <https://enterprise.platform.comodo.com/signup>

**DRAGON ENTERPRISE** **NEW ACCOUNT**

Email

Password

Confirm Password

First Name

Last Name

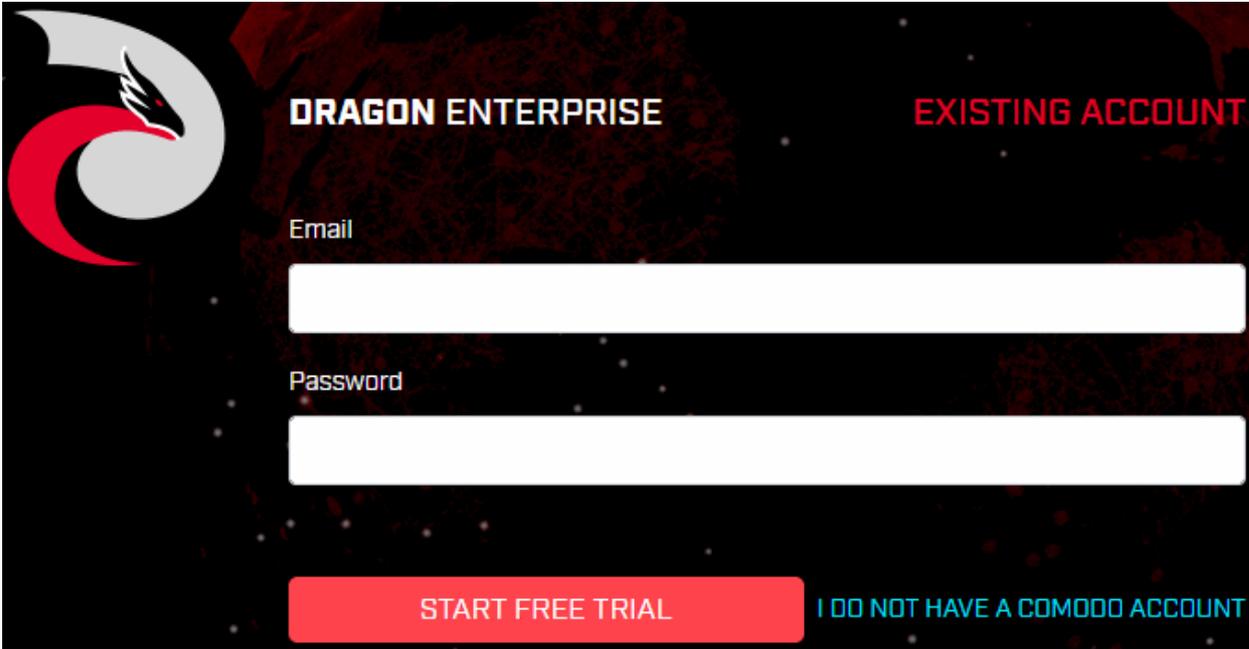
Phone Number

**START FREE TRIAL** **I HAVE A COMODO ACCOUNT**

If you are a new customer, enter the following details:

- **Email Address** - This will be used as your account contact address, and doubles-up as your Dragon Enterprise Platform username.
- **Password** - Create a password for your Dragon Platform account. Requirements:
  - At least eight characters long
  - Contain at least one lower and one upper case letter
  - Contain at least one numeral
  - Contain at least one of the following special characters - )(!#\$%^&\*"
- **Confirm Password** - Reenter the password
- **First Name and Last Name** - Your full name.
- **Phone** - Your contact number.
- Click 'Start Free Trial'
- Your account is created. You will receive your order confirmation emails on the registered email address.
- Next: [login page](#)

If you are already a Comodo customer, click 'I have a Comodo Account'



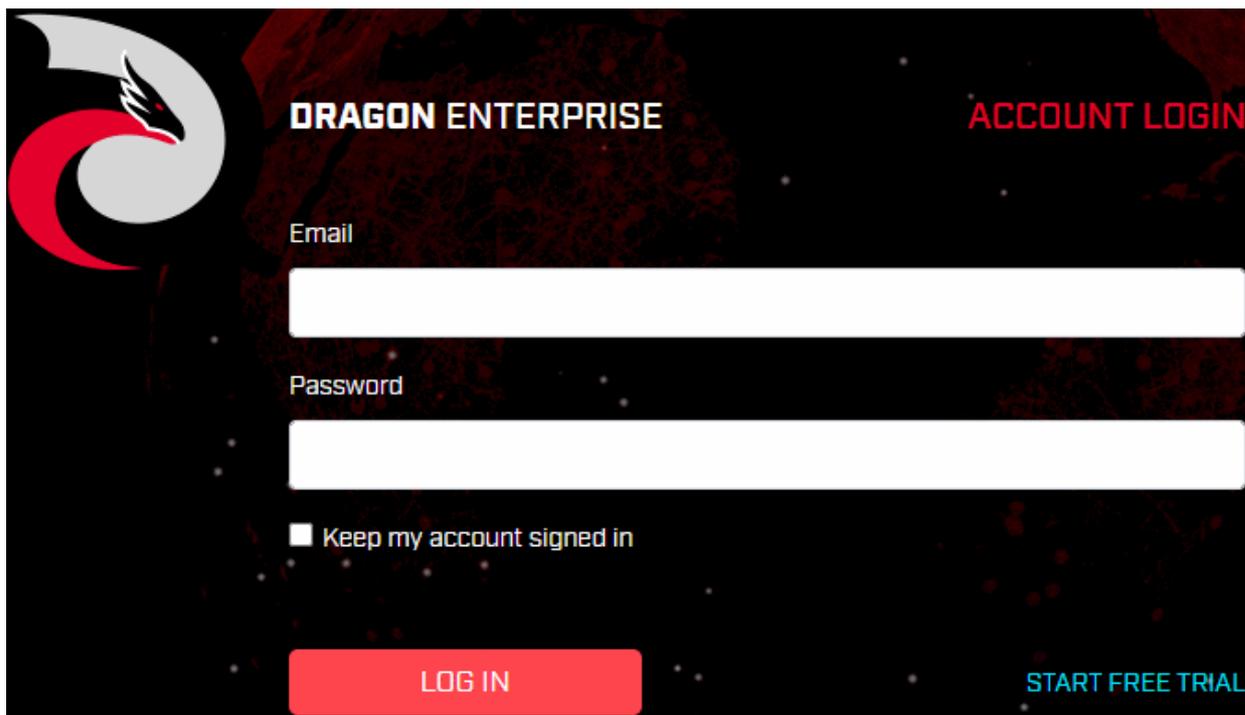
**DRAGON ENTERPRISE** **EXISTING ACCOUNT**

Email

Password

**START FREE TRIAL** **I DO NOT HAVE A COMODO ACCOUNT**

- Enter your username and password of your Comodo account and click 'Start Free Trial'
- You will be taken to the login page



**DRAGON ENTERPRISE** **ACCOUNT LOGIN**

Email

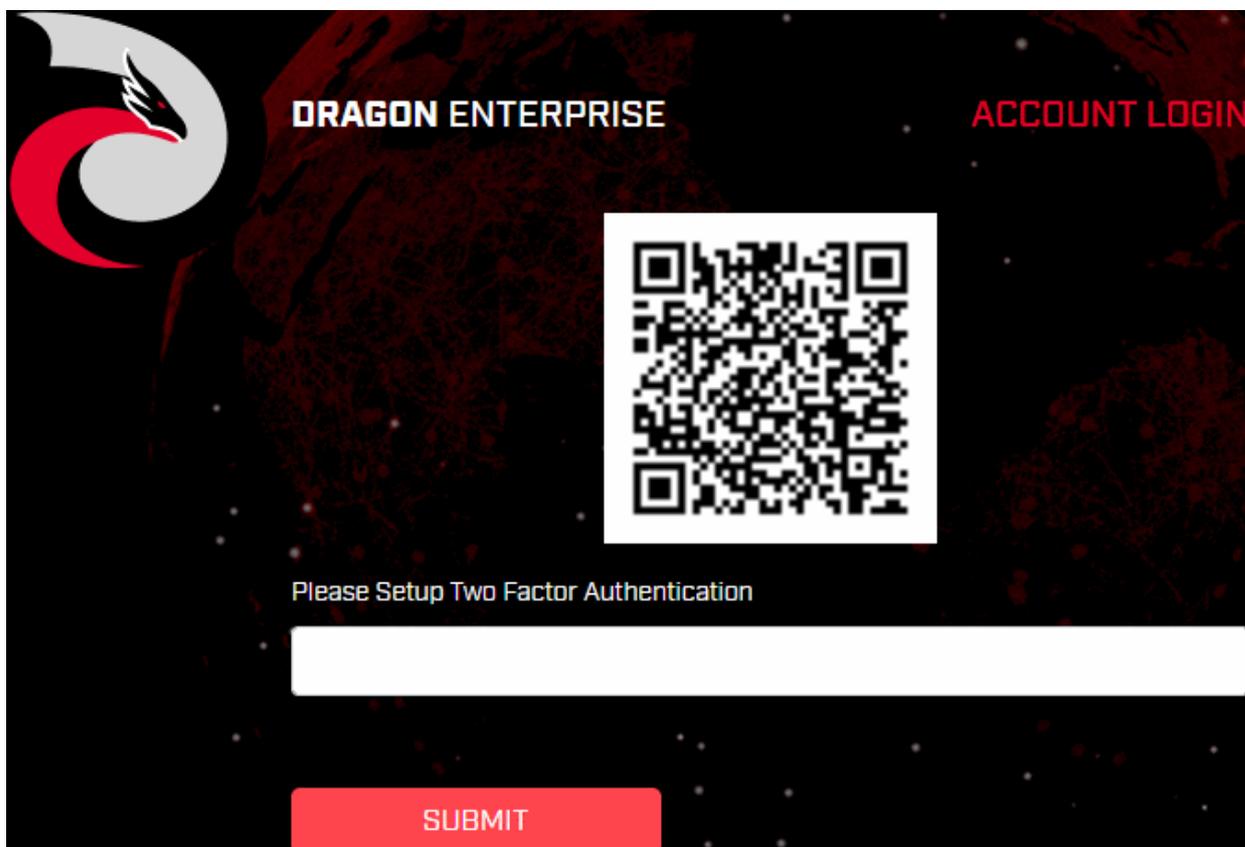
Password

Keep my account signed in

**LOG IN** **START FREE TRIAL**

- Enter your registered email address and password
- Click 'Log in'

You need to setup two factor authentication on your first login:



**DRAGON ENTERPRISE** **ACCOUNT LOGIN**

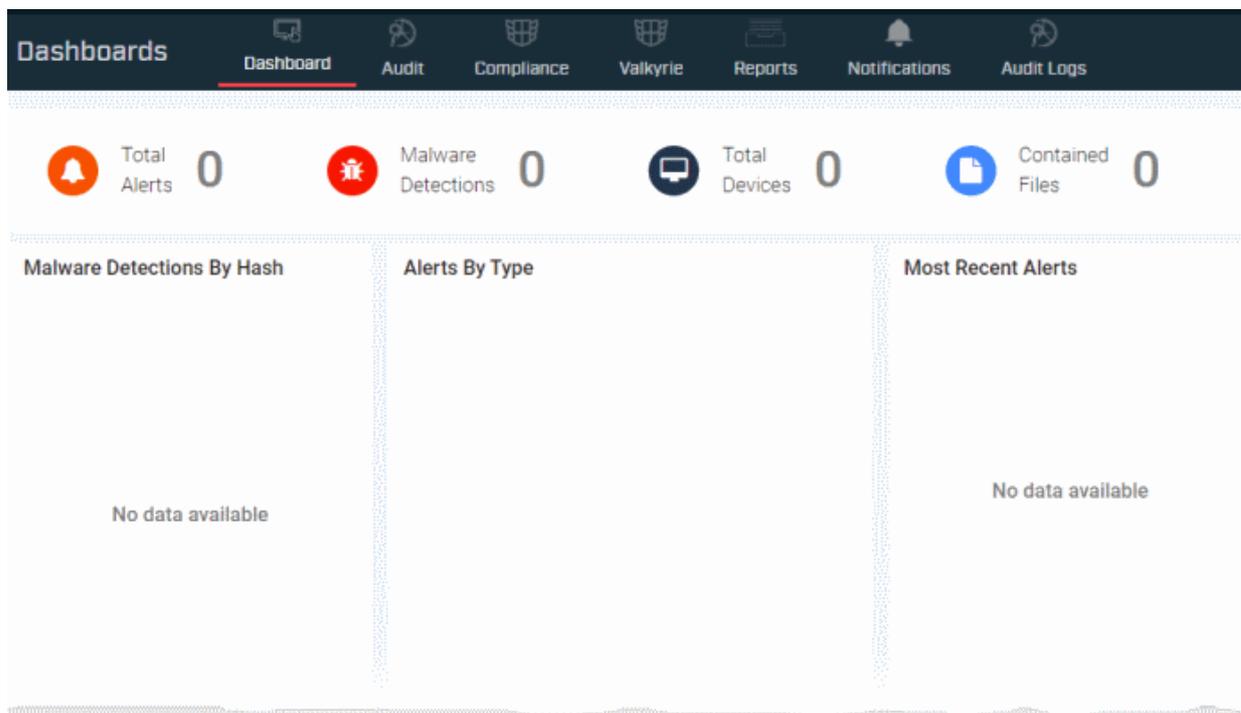
Please Setup Two Factor Authentication

**SUBMIT**

- **Step 1** - Download the 'Google Authenticator' app and install it on your iOS or Android device.
  - Open the 'Authenticator' app and tap the '+' icon'
- **Step 2** - Scan the QR code with the device camera. This will cause the Google app to generate the 6

digit code you need to complete pairing.

- **Step 3** - Enter the verification code in the field provided on the form.
- You will be taken to the Dragon Enterprise Platform Dashboard.



- That's it. You have successfully created a Dragon Enterprise account.
- Note - This account will be automatically granted 'Account Admin' privileges and cannot be deleted. You will be able to create 'Admins' and 'Technicians' under this account. See '**Step 3- Add Users**' for more details.
- You can login to your account anytime at <https://enterprise.platform.comodo.com/login>.
- You can also login at <https://cam.comodo.com/> with your Dragon Enterprise username and password to subscribe for new licenses, manage your license and account details.
- You can upgrade to full version by purchasing Advanced Endpoint Protection (AEP) and Endpoint Detection and Response (EDR) licenses for the number of devices you want to protect. See **Upgrade to Full Version** for more help.

## Step 2 - Configure Dragon Enterprise Communications

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

The following sections explain how to:

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

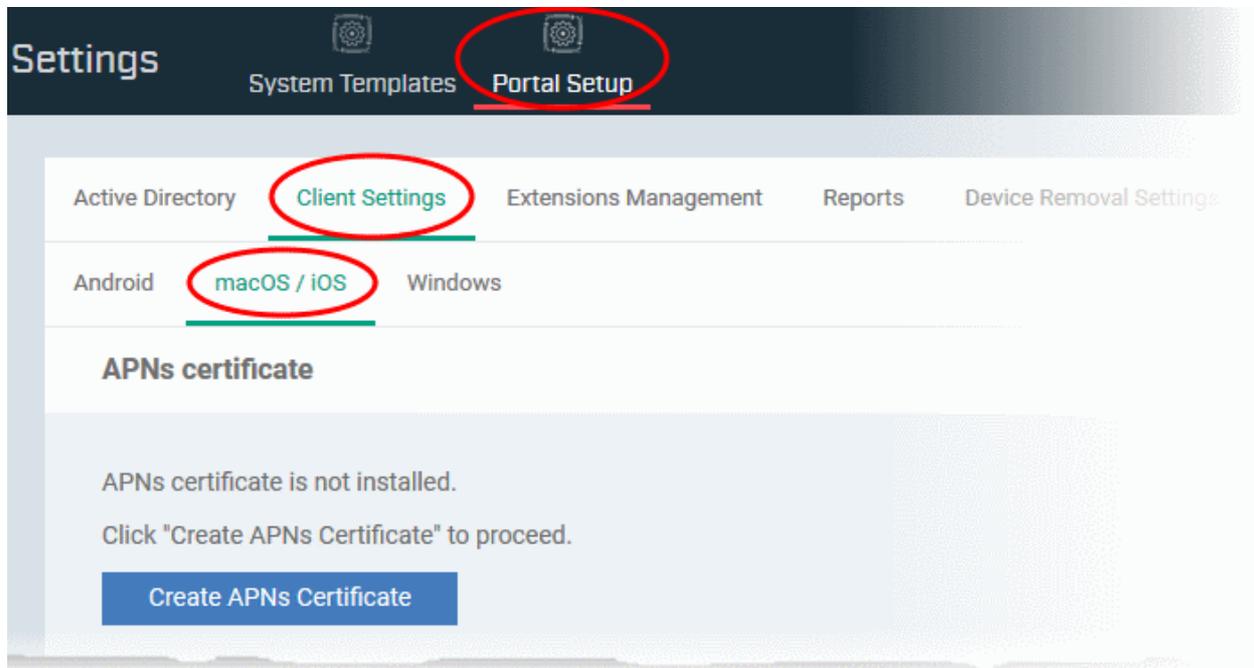
### Add Apple Push Notification certificate

- You need an Apple Push Notification (APN) certificate on your Dragon Enterprise 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. Dragon Enterprise 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' > '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):

### Generation of APNs Certificate ✕

**Country name \***  
India

**Apple ID \***  
herculespopular22@gmail.com

**State or province name \***  
Tamilnadu

**Locality name (e.g, city) \***  
Chennai

**Organization name \***  
Saddle and Pedals

**Organizational unit \***  
Sales  
Organizational Unit Name (e.g, section)

**Common name \***  
herculespopular22.com  
(e.g., server FQDN or YOUR name)

**Create** **Reset**

- 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 and you will be taken to a page which allows you to download the PLIST:

**Upload APNs Certificate**
Save

To get the certificate for communication between server and Apple devices you need to:

1. Download: [The Apple PLIST Signed by Comodo](#)
2. Login to the [Apple Push Certificate Portal](#) with your regular Apple ID (free account is enough).
3. Upload the PLIST from step 1 to the Apple portal. Apple will use this to generate your certificate.
4. Download your certificate from Apple. It will be in .PEM format.
5. Click 'Browse', select your certificate, and click 'Save' to upload it to ITSM

Select .PEM file

- 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.

Apple Push Certificates Portal herculespopular22@gmail.com [Sign out](#)

## Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

**MDM Certificate Agreement**  
(for companies deploying mobile device management for iOS and/or OS X products)

**Purpose**  
Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OS X products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

**1. Accepting this Agreement; Definitions**  
**1.1 Acceptance**  
In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational

I have read and agree to these terms and conditions.

[Printable Version >](#)

[Decline](#) [Accept](#)



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

Apple Push Certificates Portal herculespopular22@gmail.com [Sign out](#)

## Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

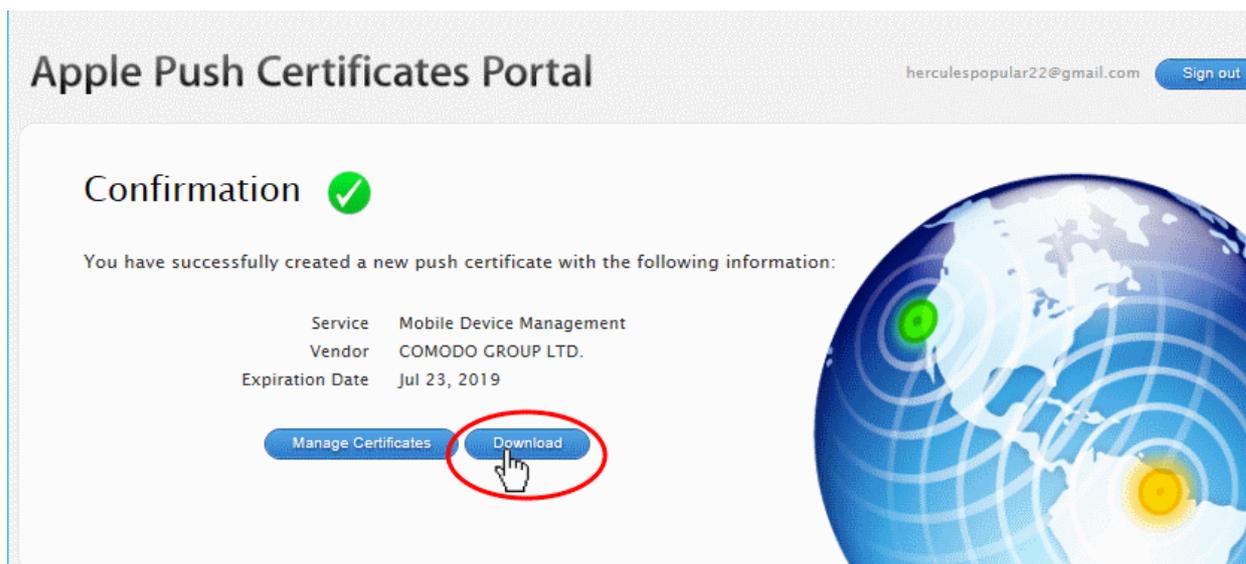
Vendor-Signed Certificate Signing Request

[Browse...](#)

[Cancel](#) [Upload](#)



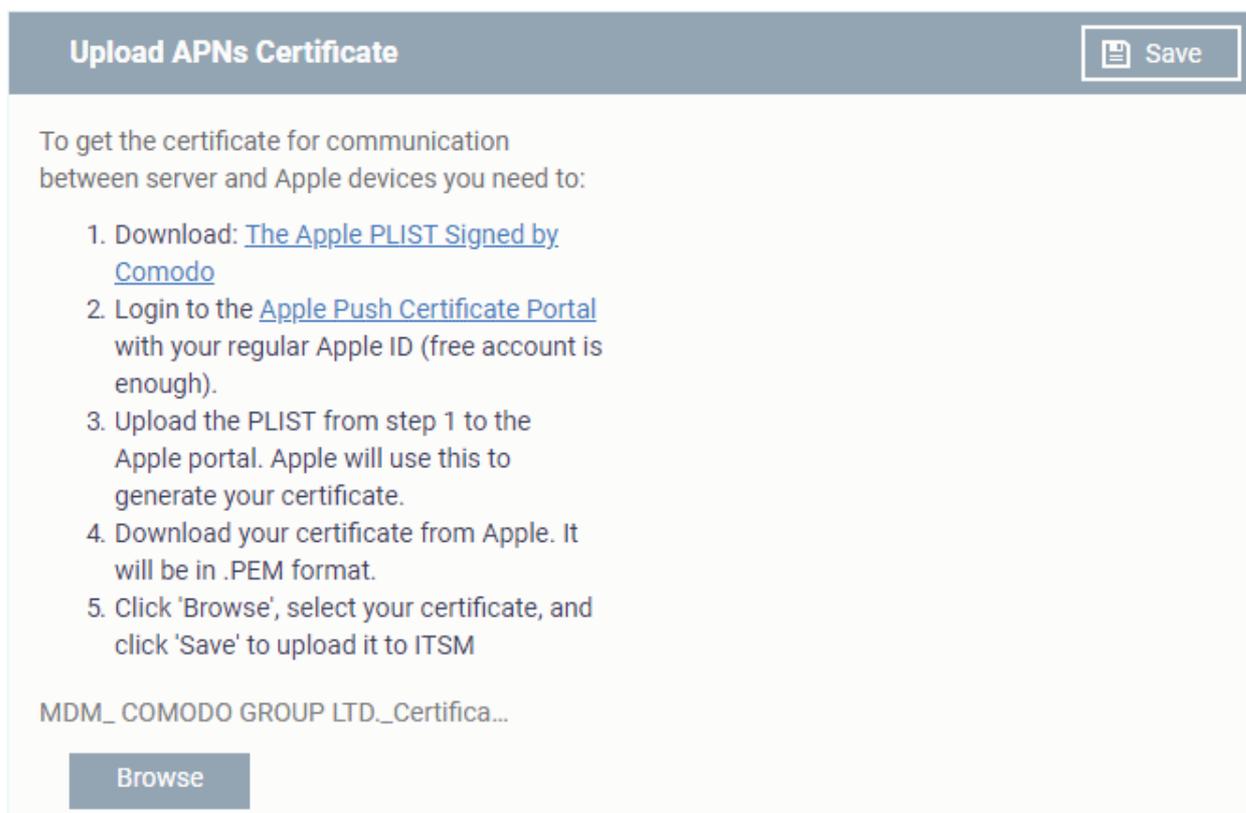
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



- 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 Dragon

- Return to Dragon, click 'Settings' > '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:

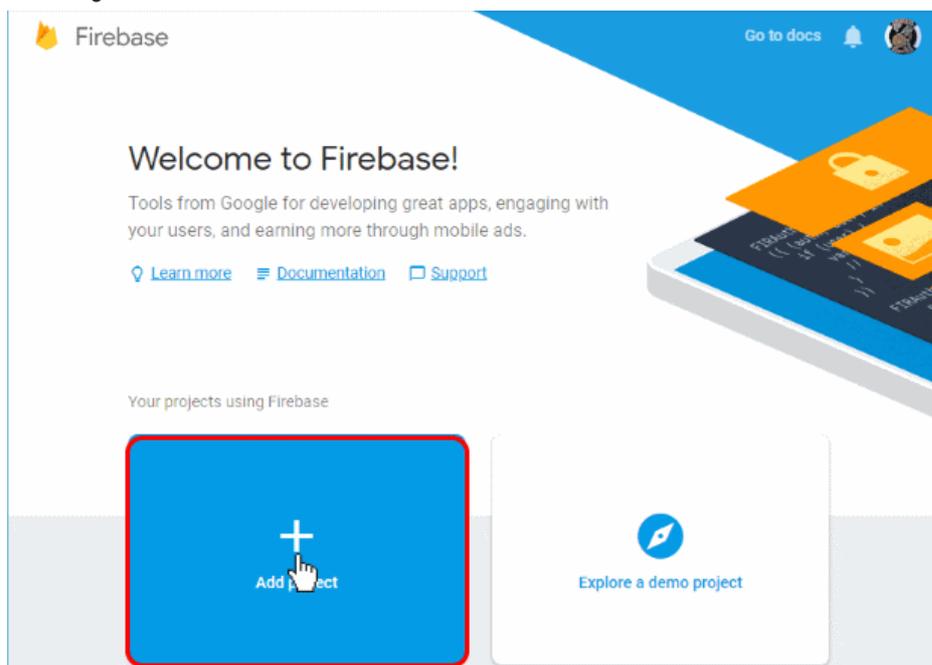
Dragon Enterprise can now communicate with iOS and Mac OS devices. You can enroll iOS devices and Mac OS devices for management.

- The certificate is valid for 365 days. Dragon 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

- Dragon Enterprise requires a Google Cloud Messaging (GCM) token in order to communicate with Android devices.
- Dragon 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'

### Add a project ✕

Project name 🤖 + iOS + </>

**Tip:** Projects span apps across platforms ?

Project ID ?

hercules-em ✎

Locations ?

United States (Analytics) ✎

us-central (Cloud Firestore) ✎

Use the default settings for sharing Google Analytics for Firebase data

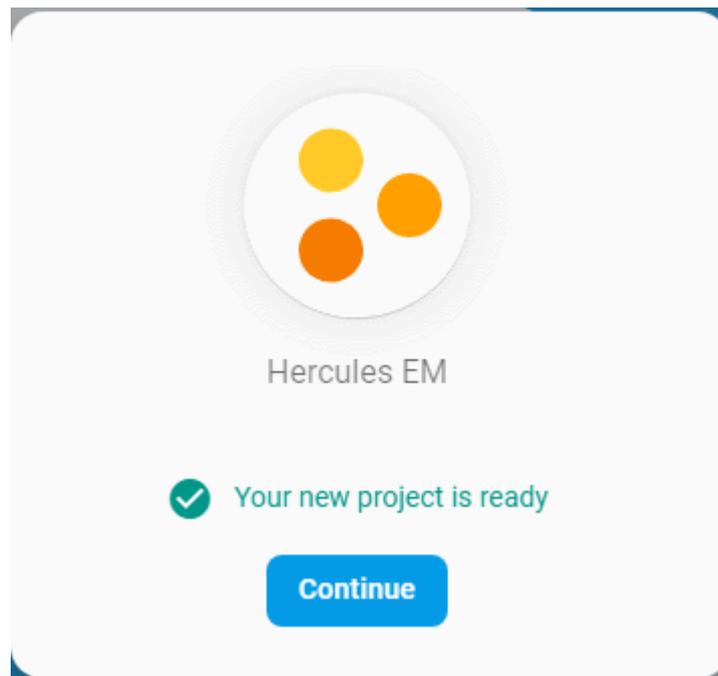
- Share your Analytics data with Google to improve Google Products and Services
- Share your Analytics data with Google to enable technical support
- Share your Analytics data with Google to enable Benchmarking
- Share your Analytics data with Google Account Specialists

I accept the [controller-controller terms](#). This is required when sharing Analytics data to improve Google Products and Services. [Learn more](#)

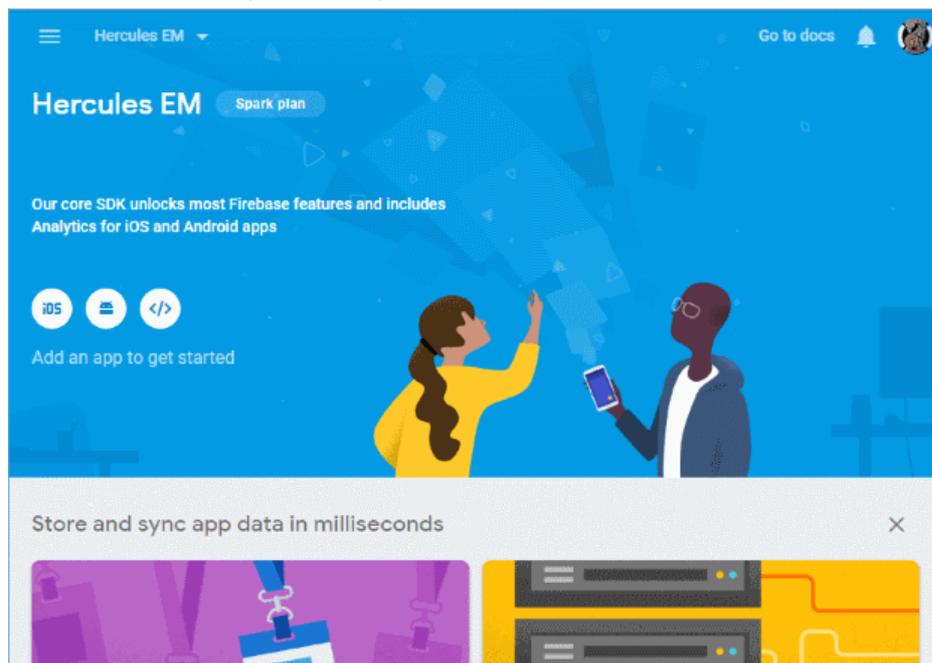
I agree that I am using Firebase services in my app and I agree to the applicable [terms](#).

Cancel Create project

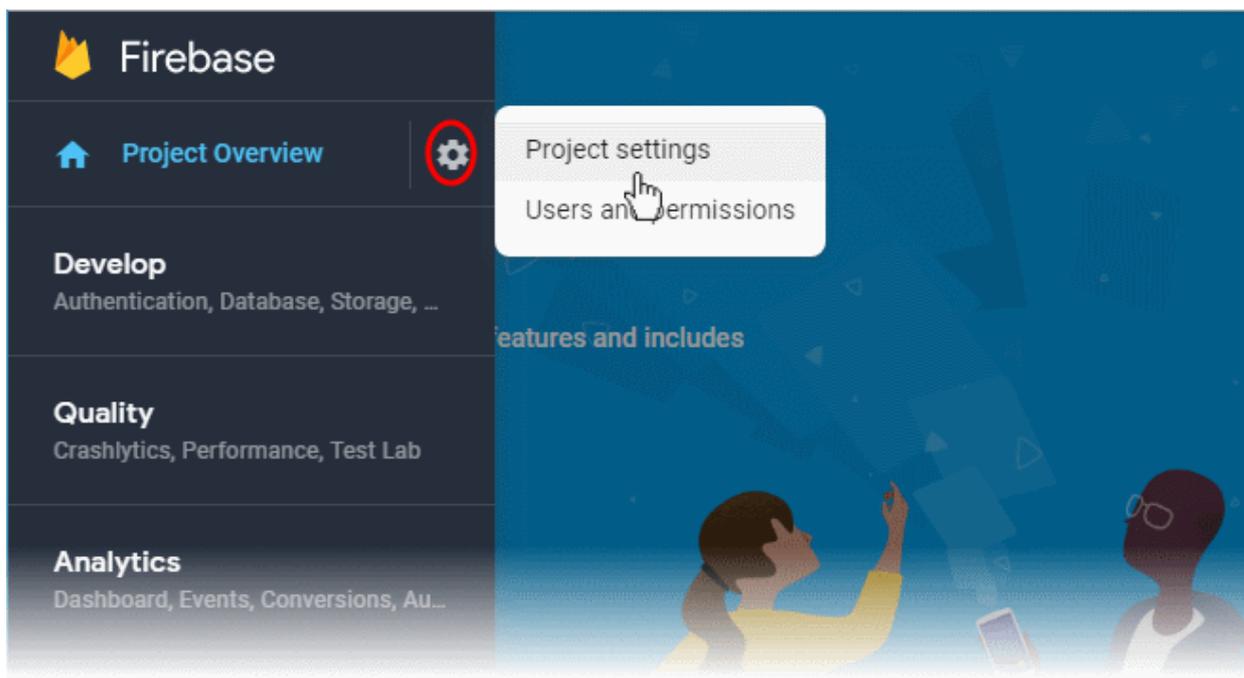
- Type a name for the new project in the 'Project name' field
- Click the pencil icon beside the 'Locations' field. Select your country and the Firestore server closest to you.
- 'Use default settings for sharing Google Analytics for Firebase data' - Leave this selected.
- Agree to the terms and conditions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



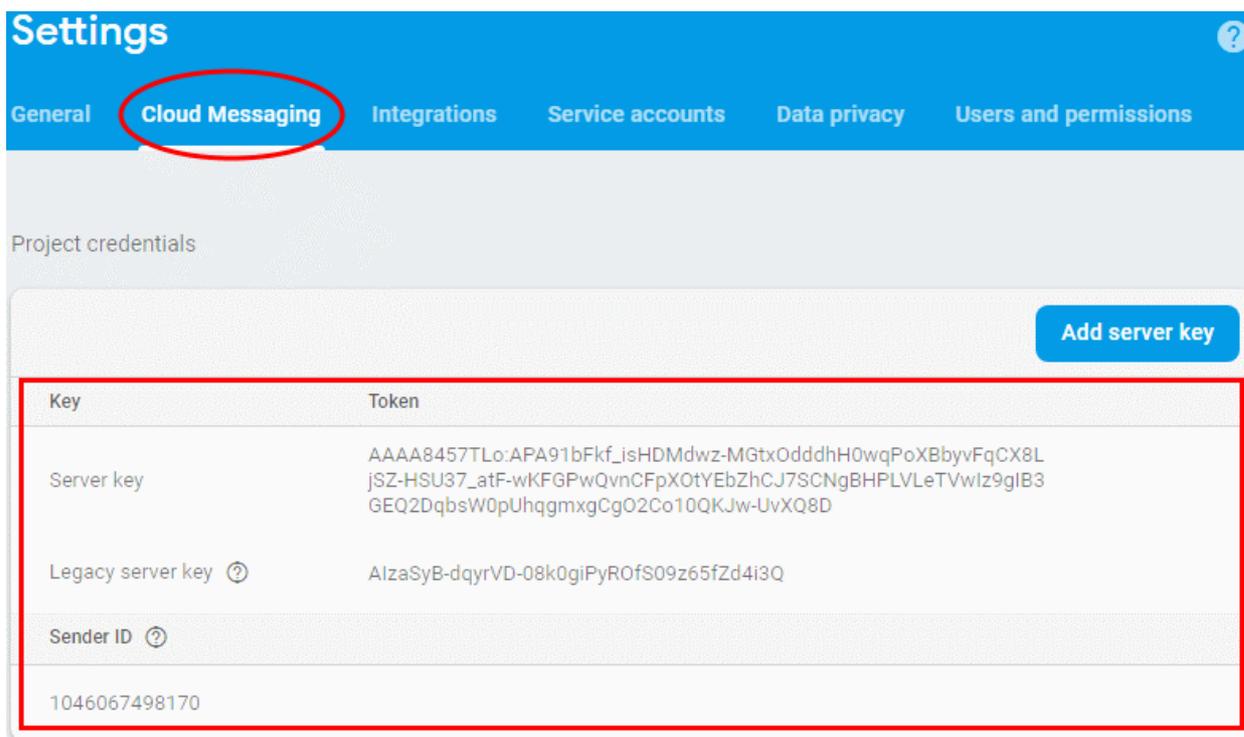
- Click 'Continue' to go to the project dashboard



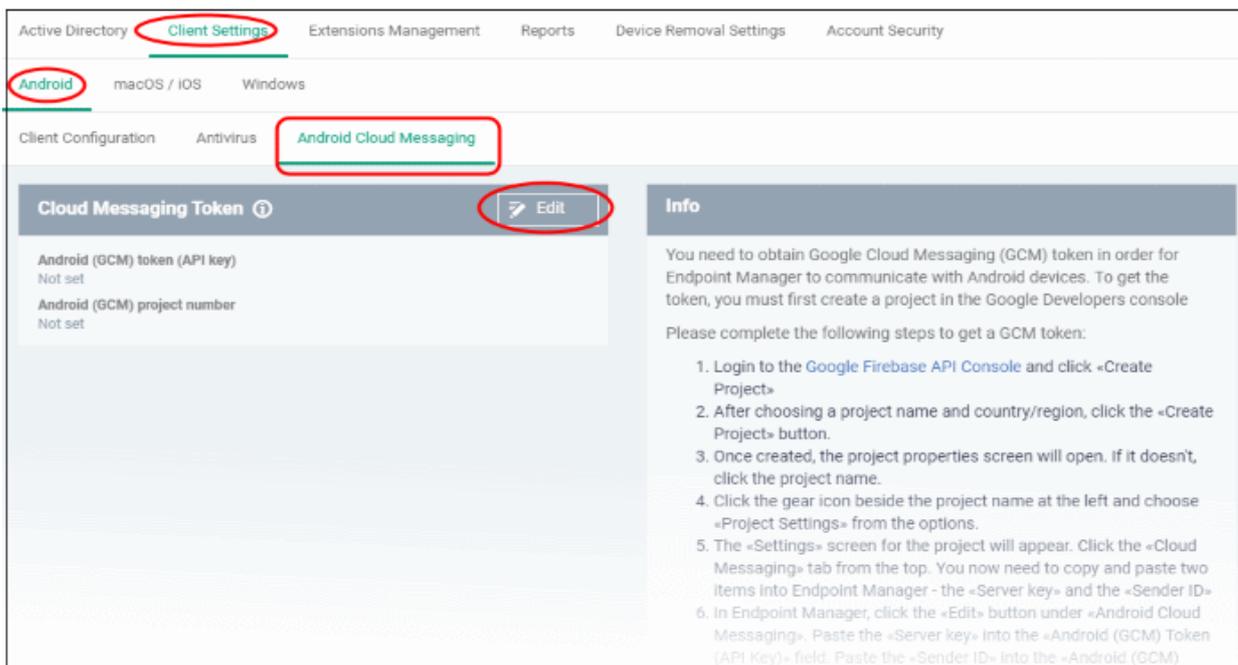
- **Step 2 - Obtain GCM Token and Project number**
  - Click the hamburger button at top-left
  - Click the cogwheel icon beside 'Project Overview' and choose 'Project settings':



- 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 Dragon Enterprise
  - Click 'Settings' > '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

**Cloud Messaging Token**
Cancel
Save

**Android (GCM) token (API key)**

**Android (GCM) project number**

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

**Cloud Messaging Token**
Cancel
Save

**Android (GCM) token (API key)**

AAAA8457TLo:APA91bFkf\_isHDMdwz-  
MGtxOdddH0wqPoXBbyvFqCX8LjSZ-HSU37\_atF-  
wKFGPwQvnCFpX0tYEbZhCJ7SCNgBHPLVLeTVwlz9gIB3GEQ2Dq

**Android (GCM) project number**

1046067498170

- Click 'Save'.

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

Dragon Enterprise can now use the token to communicate with Android devices.

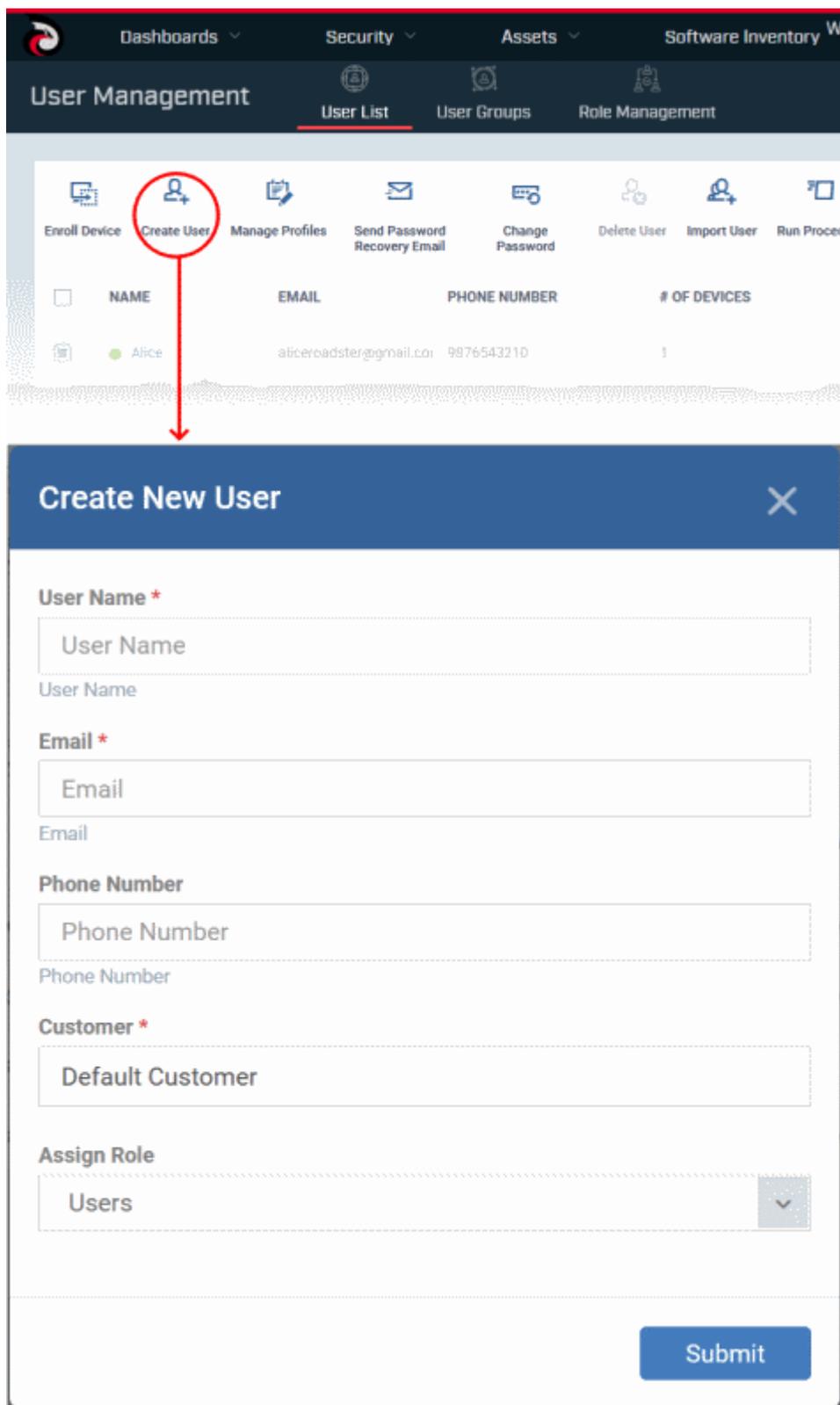
### Step 3 - Add Users

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

- **Manually add users.** Add individual users to Dragon. You need to specify their name, email address, and their 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 'Assets' > 'User Management' > 'User List'
- Click the 'Create User' button



The 'Create new user' form opens.

- **Username** - Enter the login username for the user.
- **Email** - The email address of the user for registration to Dragon. Account and device enrollment mails will be sent to this address. Please ensure users respond to the device enrollment mail from the device(s) you intend to enroll.
- **Phone Number** (Optional) - The contact number of the user.

- **Customer** - The company to which the user belongs. Leave the customer as 'Default Customer'.
- **Assign role** - Choose a role. A 'role' determines user's permissions within Dragon Enterprise console. The product ships with four default roles:
  - **Administrators** - Can login to Dragon and access all management interfaces. This role can be edited as required.
  - **Technician** - Can login to Dragon and access all management interfaces. The technician role has fewer privileges than the administrator role. This role can be edited as required.
  - **Login permission** - Can login to Dragon. Users with role cannot access any management interface by default. You can edit the role to assign access to required management interfaces.
  - **Users** - Cannot login to Dragon. 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 Dragon. These roles can be assigned to users as required. All roles created in Dragon will appear in the 'Assign Role' drop-down when adding a new user. See online help page for **Configure Role Based Access Control for Users** for more details.

- Click 'Submit' to add the user to Dragon Enterprise.

The user is added to the 'Users' interface. The user's devices can be enrolled to Dragon 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 'Assets' > 'User Management' > 'User List' > 'Import User' in the Dragon Enterprise console
- Browse to your CSV file
- Select a role for the imported users
- Click 'Import users from list'.
- The users will be imported and enrolled to Dragon

### 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 'Assets' > 'User Management' > 'User List' > 'Import User'

**User Management**

Enroll Device   Create User   Manage Profiles   Send Password Recovery Email   Change Password   Delete User   **Import User**   Run Process

<input type="checkbox"/>	NAME	EMAIL	PHONE NUMBER	# OF DEVICES
<input type="checkbox"/>	Alice	aliceroadster@gmail.com	9876543210	1

---

**User import**

Use this page to import multiple users from a user list in CSV format.

**Important:**

- use only comma (,) as a field delimiter;
- enter user names in the 1st column and email addresses in the 2nd column (both are mandatory), 3rd column is for phone numbers (optional);
- use no column headers.

**Uploading status:** Ready

**CSV file \***

Browse

**Customer \***

Customer

**Role \***

Role

Do not send any enrollment notifications  
The imported users will not be notified

Import users from list

- **CSV File** - Click 'Browse' to locate and open the CSV file you want to import
- **Customer** - The company to which the users belongs. Enter "Default Customer" in the customer field.
- **Role** - 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 'Do not send any enrollment notifications' 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.

#### Process in brief:

- Click 'Assets' > 'User Management' > 'User List' > select users > click 'Enroll Device'.
- Complete the wizard to send device enrollment mail to your users. Users must open the mail on the device itself. See the tutorial below.
- The mail contains an enrollment token. Multiple devices can be enrolled with the same token by the user simply responding to the mail from each device. Each token is valid for 720 days.
- Each AEP license covers one endpoint or 5 mobile devices per user. You will need additional licenses for each endpoint or mobile device (exceeding 5) you add for a user.
- Each EDR license covers one endpoint per user.

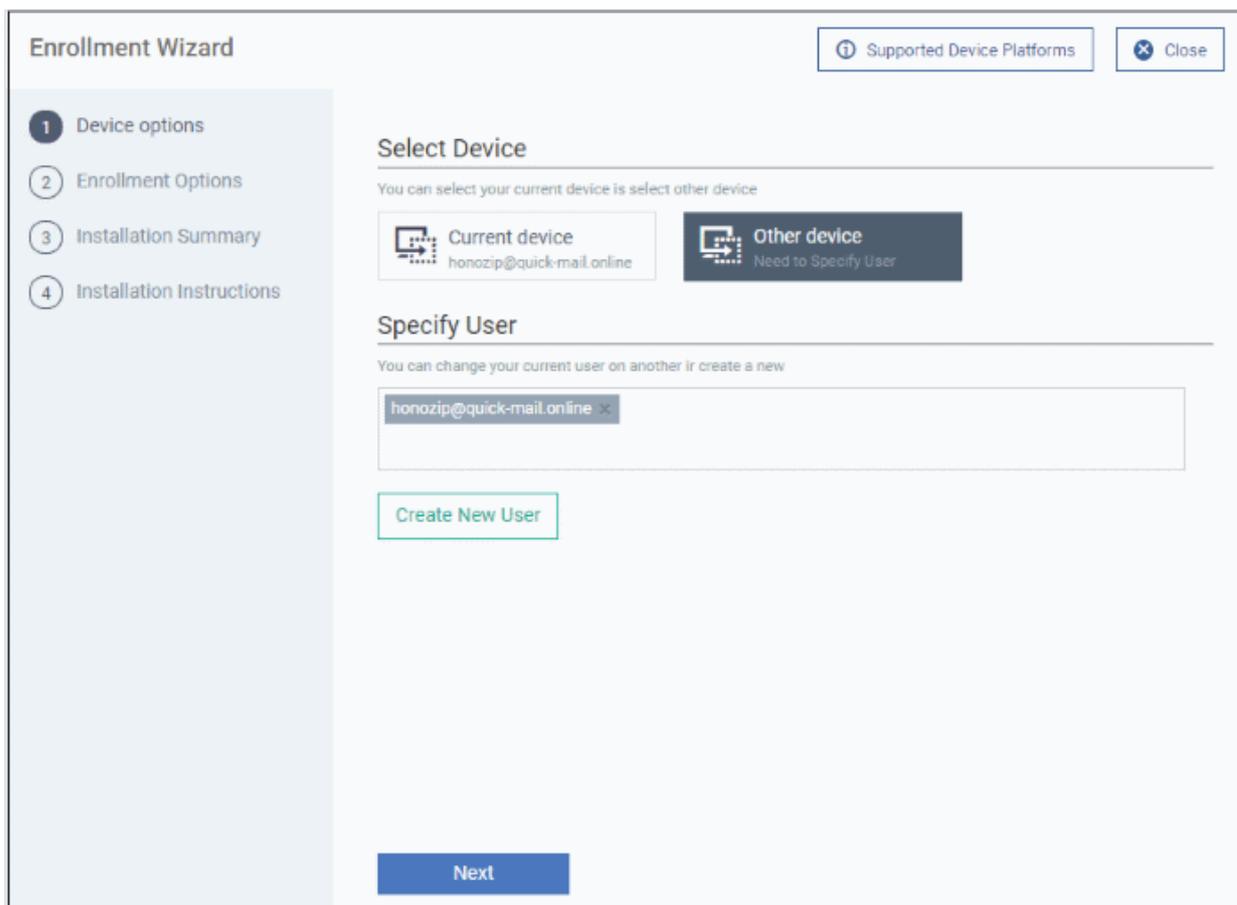
#### Enroll user devices

- Click 'Assets' > 'User Management' > 'User List'
- Select users for whom you want to enroll devices
- Click 'Enroll Device'

This starts step 1 of the device enrollment wizard:

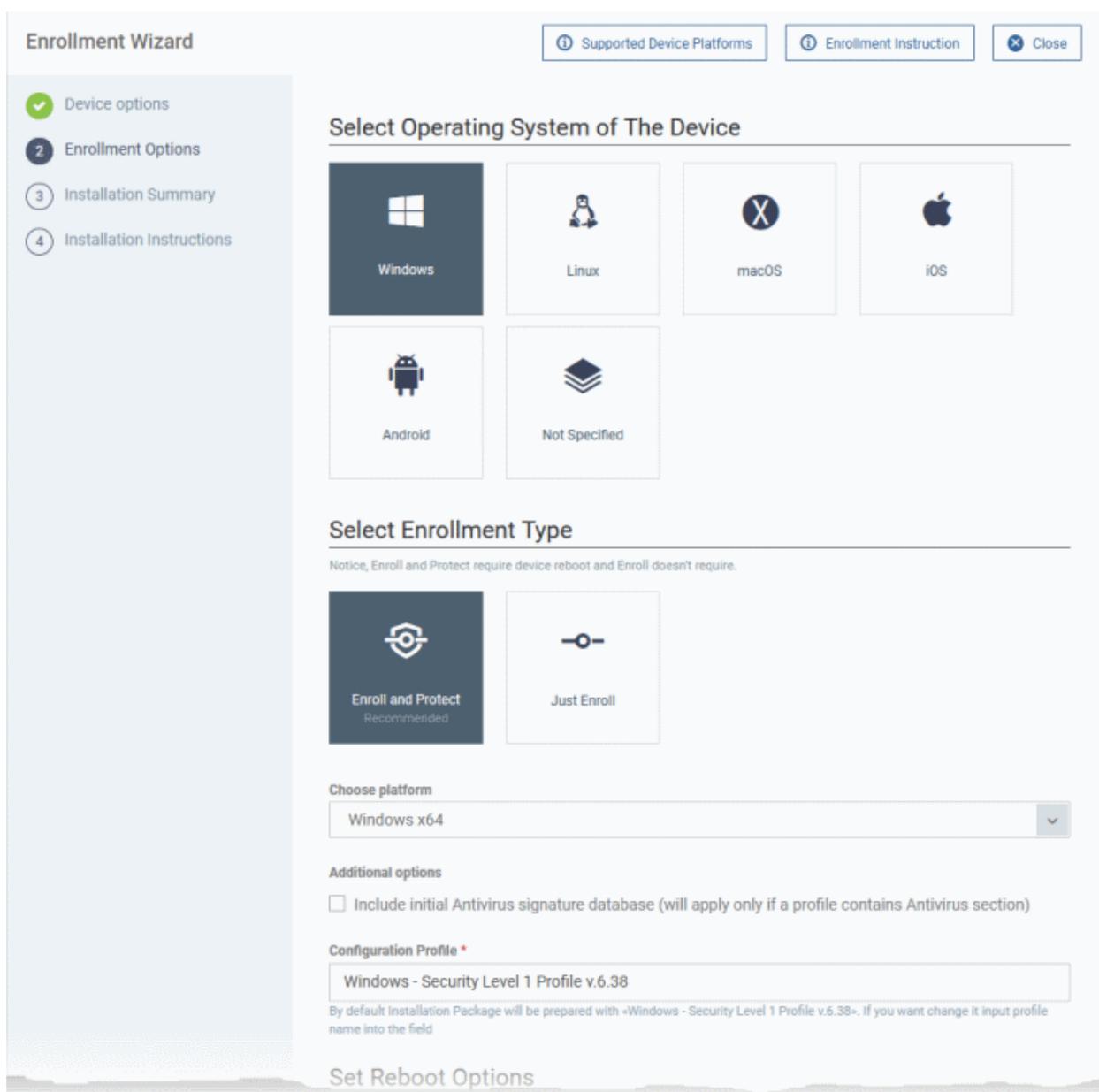
#### Step 1 - Device Options

- **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. Dragon will auto-suggest users that have already been created.
- **Create New User** - Click if you want to add a new user to Dragon. 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 Dragon Enterprise, 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 Dragon 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. <ul style="list-style-type: none"> <li>• You can only change the CCC version if enabled in <b>portal settings</b>. If the option is not enabled then the 'Default version' is deployed.</li> </ul>
Use default Communication Client Security version	This client installs security software such as antivirus, firewall and auto-containment. <ul style="list-style-type: none"> <li>• You can only change the CCS version if enabled in <b>portal settings</b>. If the option is not enabled then the 'Default version' is deployed.</li> </ul>
Additional options	<b>AV Database</b> - 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.

	<ul style="list-style-type: none"> <li>The default profile is recommended for most users and can always be changed later if required.</li> <li>If you want to change it, type the first few characters of a profile name and choose from the suggestions that appear.</li> <li>You can view the settings in a profile at 'Configuration Templates' &gt; 'Profiles'.</li> </ul>
Set Reboot Options	<p>Endpoints need to be restarted to complete CCS installation. You have the following restart options:</p> <ul style="list-style-type: none"> <li><b>Force the reboot in...</b> - 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.</li> <li><b>Suppress reboot</b> - Endpoint is not auto-restarted. The installation is finalized when the user next restarts the endpoint.</li> <li><b>Warn about reboot and let users postpone it</b> - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.</li> </ul> <p>Optional. Type a custom message in the 'Reboot Message' field.</p>
Device Name Options	<ul style="list-style-type: none"> <li>Do Not Change - The device's existing name is used to identify the device in Dragon.</li> <li>Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.</li> </ul>

- Click 'Next' to proceed to step 3

## Linux

Setting	Description
Choose platform	<p>Select Linux OS version</p> <ul style="list-style-type: none"> <li>Ubuntu / Debian (Hybrid Package)</li> <li>RHEL / CentOS (Hybrid Package)</li> <li>'Hybrid' just means the package is suitable for both types of OS.</li> </ul>
Device Name Options	<ul style="list-style-type: none"> <li>Do Not Change - The device's existing name is used to identify the device in the Dragon console.</li> <li>Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.</li> </ul>

- Click 'Next' to proceed to step 3

## Mac OS

Setting	Description
Select Method	<ul style="list-style-type: none"> <li><b>With MDM profile</b> (recommended) - Installs both the communication client and the Dragon Enterprise configuration profile. You can use the full suite of Comodo tools on your devices</li> <li><b>Without MDM profile</b> - Installs only the communication client. 'Profile-less' enrollment lets you use Dragon Enterprise to manage</li> </ul>

	security while using another platform for general Mac management.
Device Name Options	<ul style="list-style-type: none"> <li>• <b>Do Not Change</b> - The device's existing name is used as the device label in the Dragon Enterprise console.</li> <li>• <b>Change</b> - Enter a new device name. Note - You can restore the original name from the device list screen if required.</li> </ul>

- Click 'Next' to proceed to step 3

## iOS / Android

### Device Name Options:

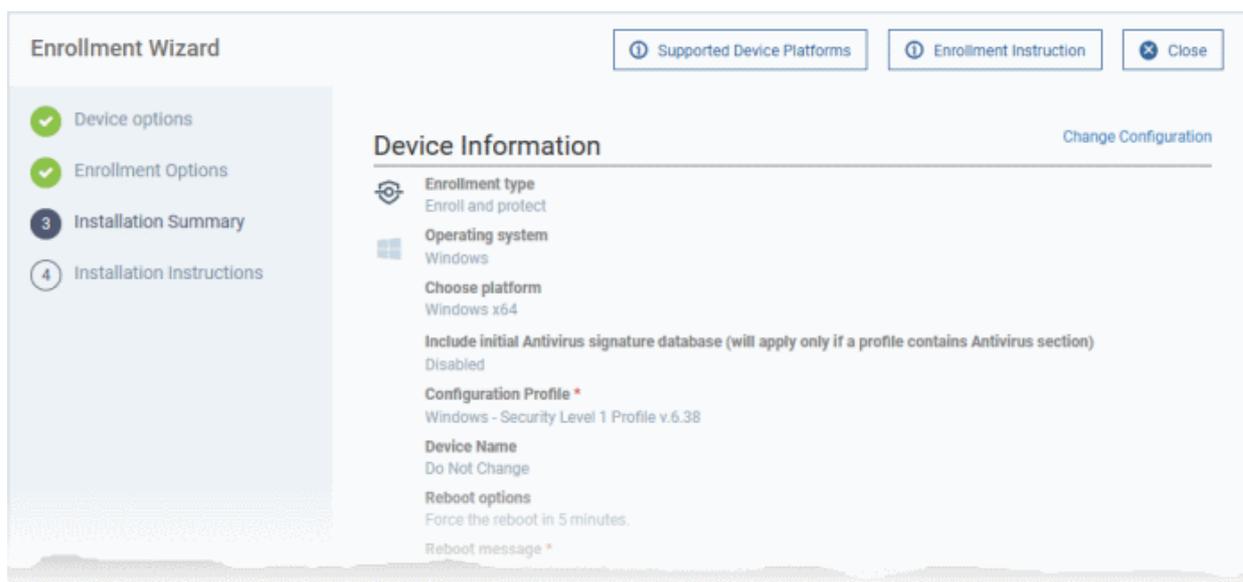
- **Do Not Change** - The device's existing name is used as the device label in Dragon Enterprise.
- **Change** - Enter a new device name. Note - You can restore the original name from the device list screen if required.

Click 'Next' to proceed to step 3

## Step 3 - Installation Summary

Review your choices so far.

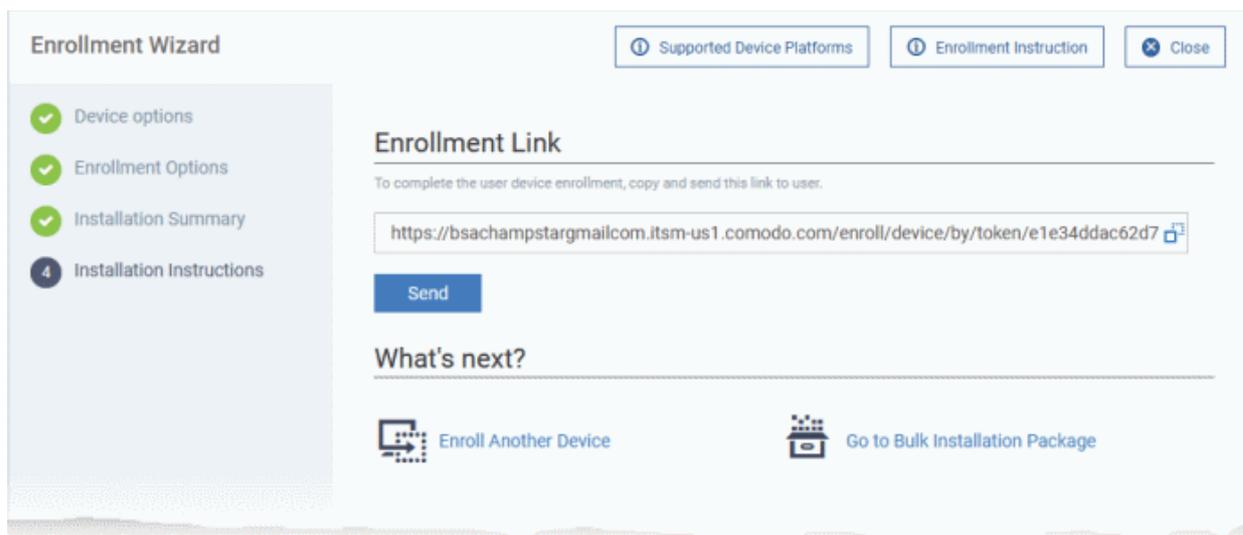
The summary you see depends on the operating system and enrollment type:



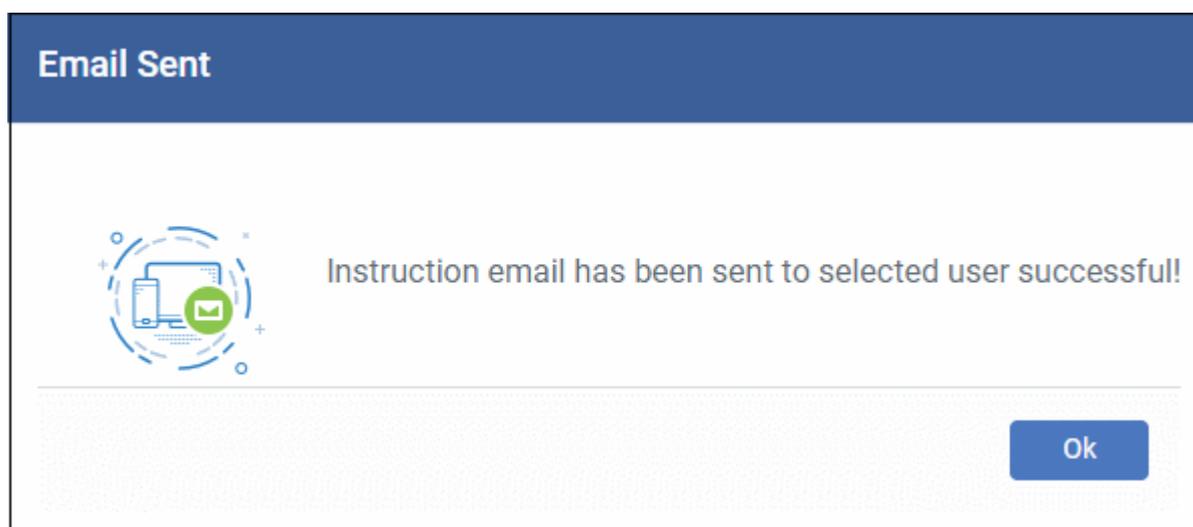
- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4.

## 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.

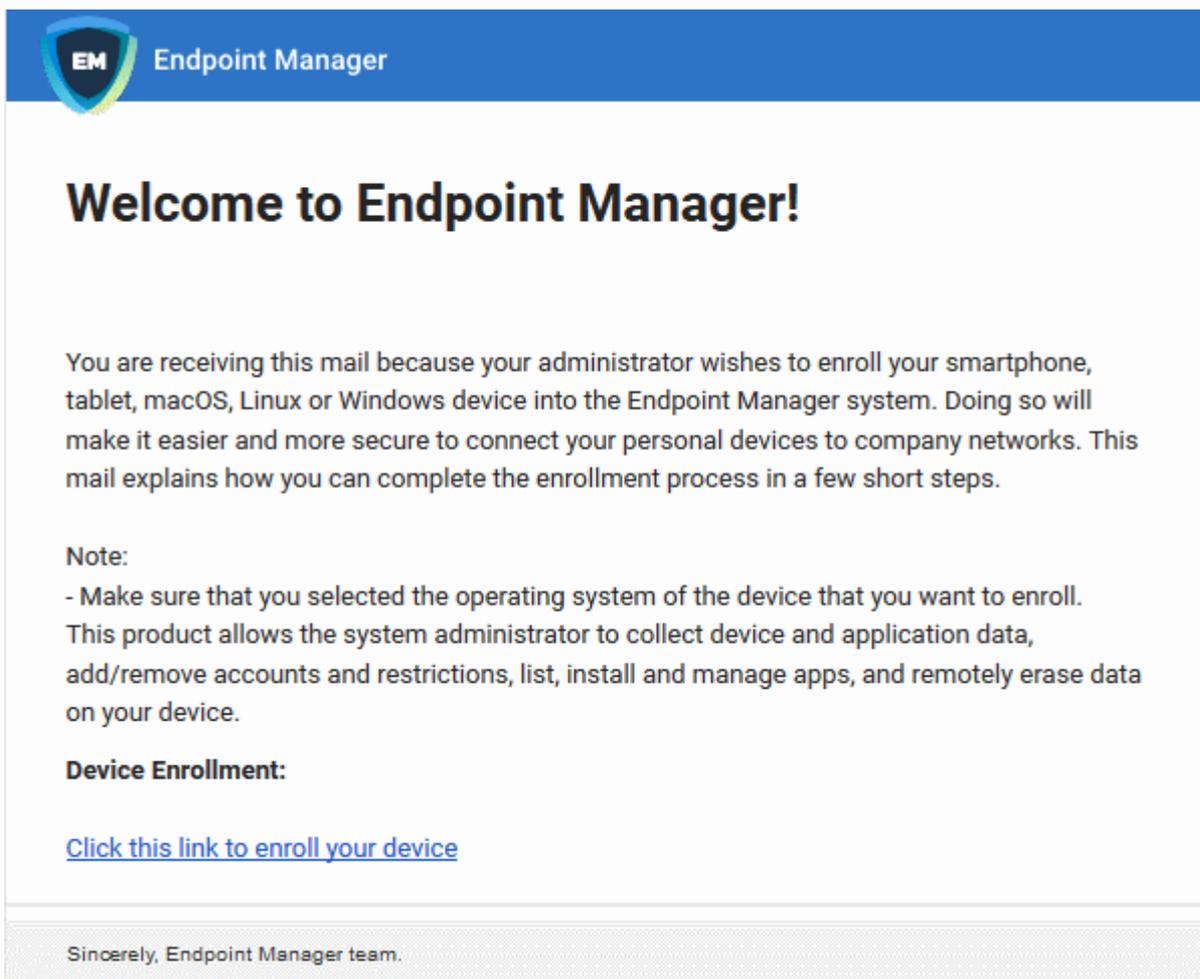


- **Enroll Another Device** - Takes you back to step 1
- **Go to Bulk Installation Package** - Takes you to bulk installation package screen to configure and enroll users in bulk. See '**Bulk Enrollment of Devices**' in the online admin guide.
- Click 'Finish' to close the window.

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:



**EM** Endpoint Manager

## Welcome to Endpoint Manager!

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

**Note:**

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

**Device Enrollment:**

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

Sincerely, Endpoint Manager team.

- 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 'Assets' > 'User Management' > 'User List' > click the name of a user to open their details screen > click 'Enroll Device'
- Click 'Assets' > '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:

## Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

---

### Installation Instruction



**Step 1**

Install the Mobile Device Management Client on Google Play





**Step 2**

After click «Enroll» and follow instructions to finalize enrollment



---

### Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

**Host**  
Server Url  
herculespopular-herculespopular-msp.cmdm.comodo.com

**Port**  
Server Port  
443

**Token**  
29014e9f995b3d8762126bb53cf99dcd

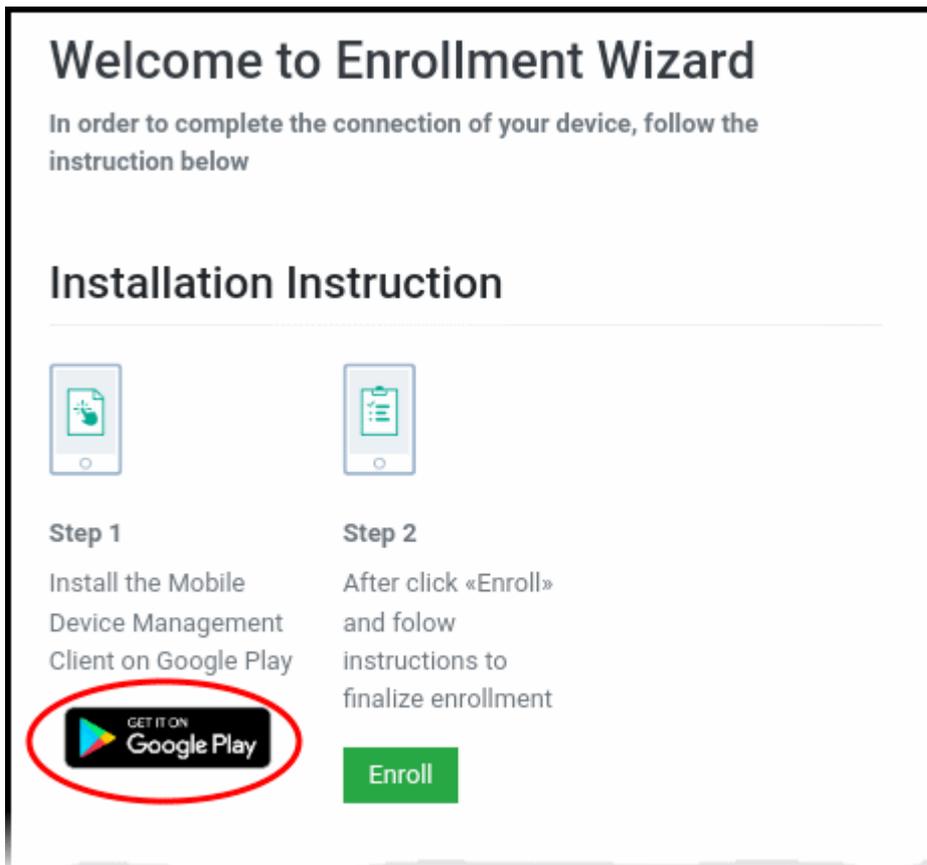
- Once installed, the client software will connect the device to Dragon Enterprise.
- The following sections explain the enrollment process on different operating systems:
  - [Enroll Android Devices](#)
  - [Enroll iOS Devices](#)
  - [Enroll Windows Endpoints](#)
  - [Enroll Mac OS Devices](#)
  - [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**

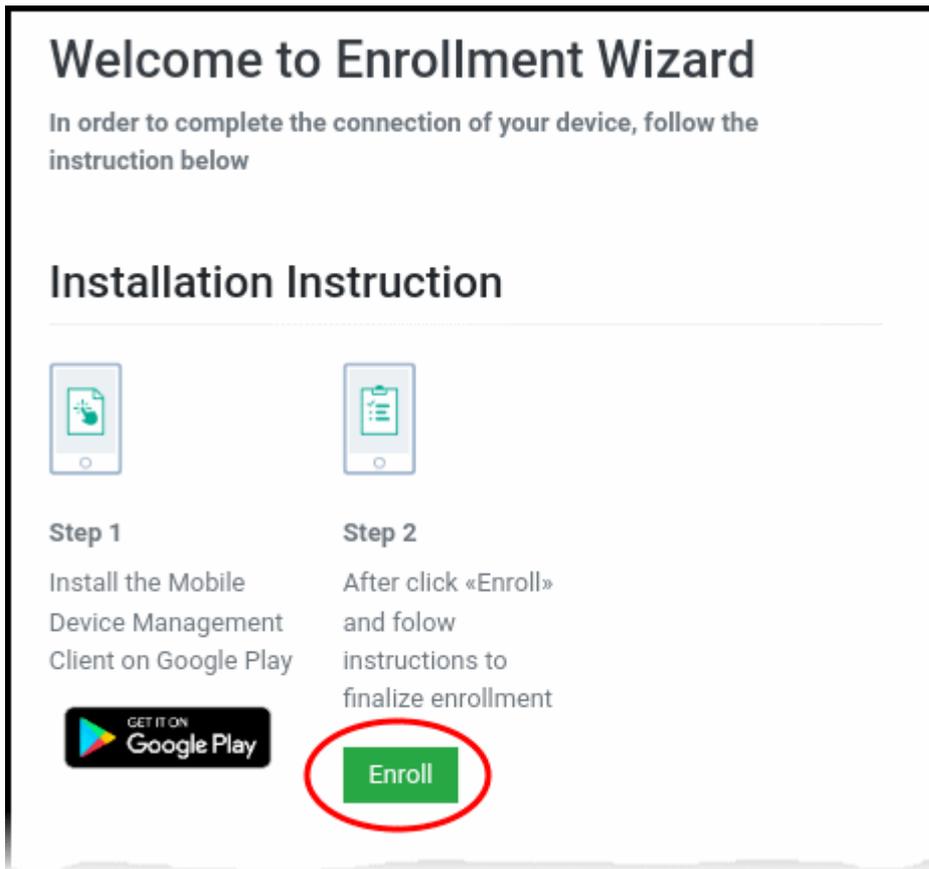
### Step 1 - Download and Install the communication client

- 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.



## Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

### Installation Instruction



**Step 1**

Download the Profile to enroll your device. When your profile has been enrolled, you will be requested to install Communication Client application.

Download MDM Profile

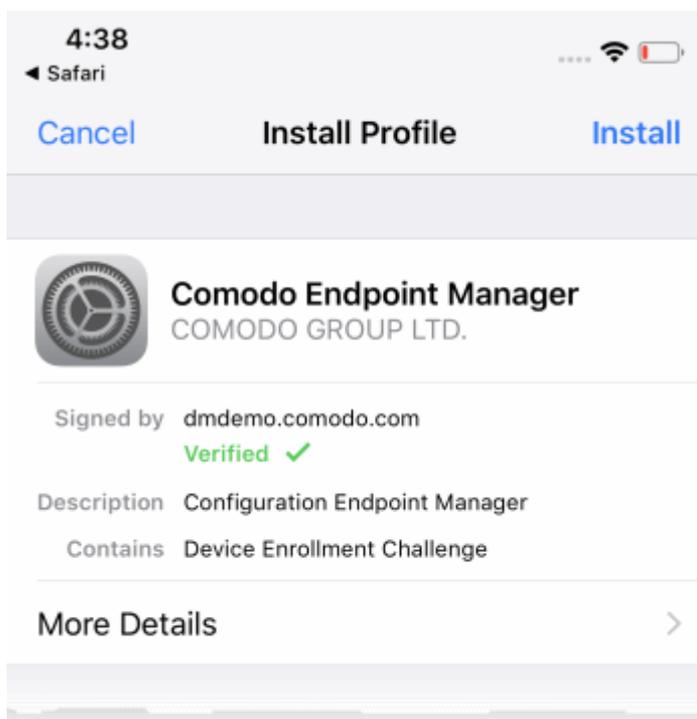


**Step 2**

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.

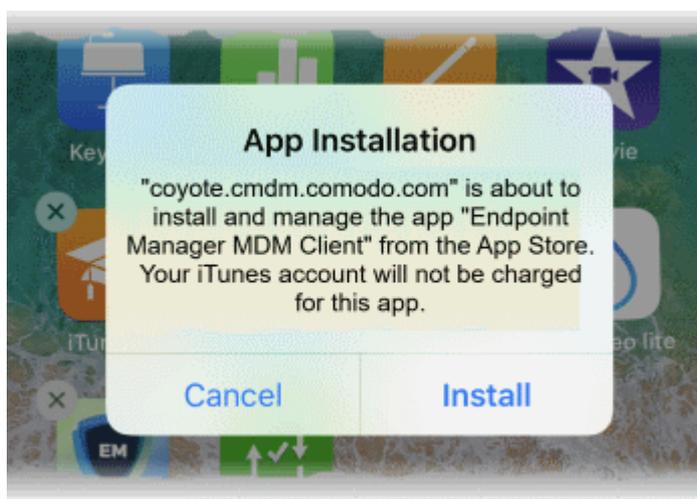
- Tap 'Download MDM Profile'.

The 'Install Profile' wizard starts:

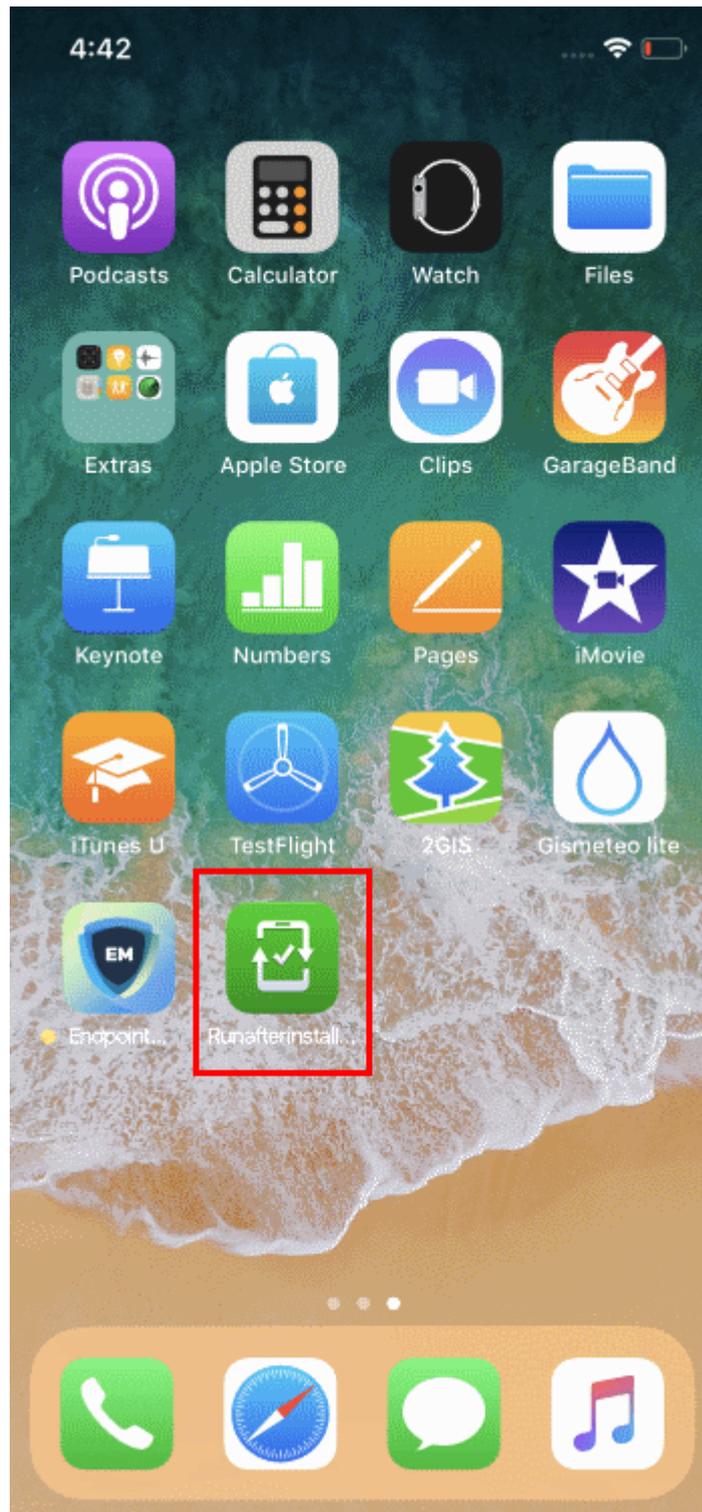


**Note:** Users must keep their device switched on at all times during enrollment. The enrollment process may fail if the device auto-locks or enters standby.

- 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 Dragon Enterprise:



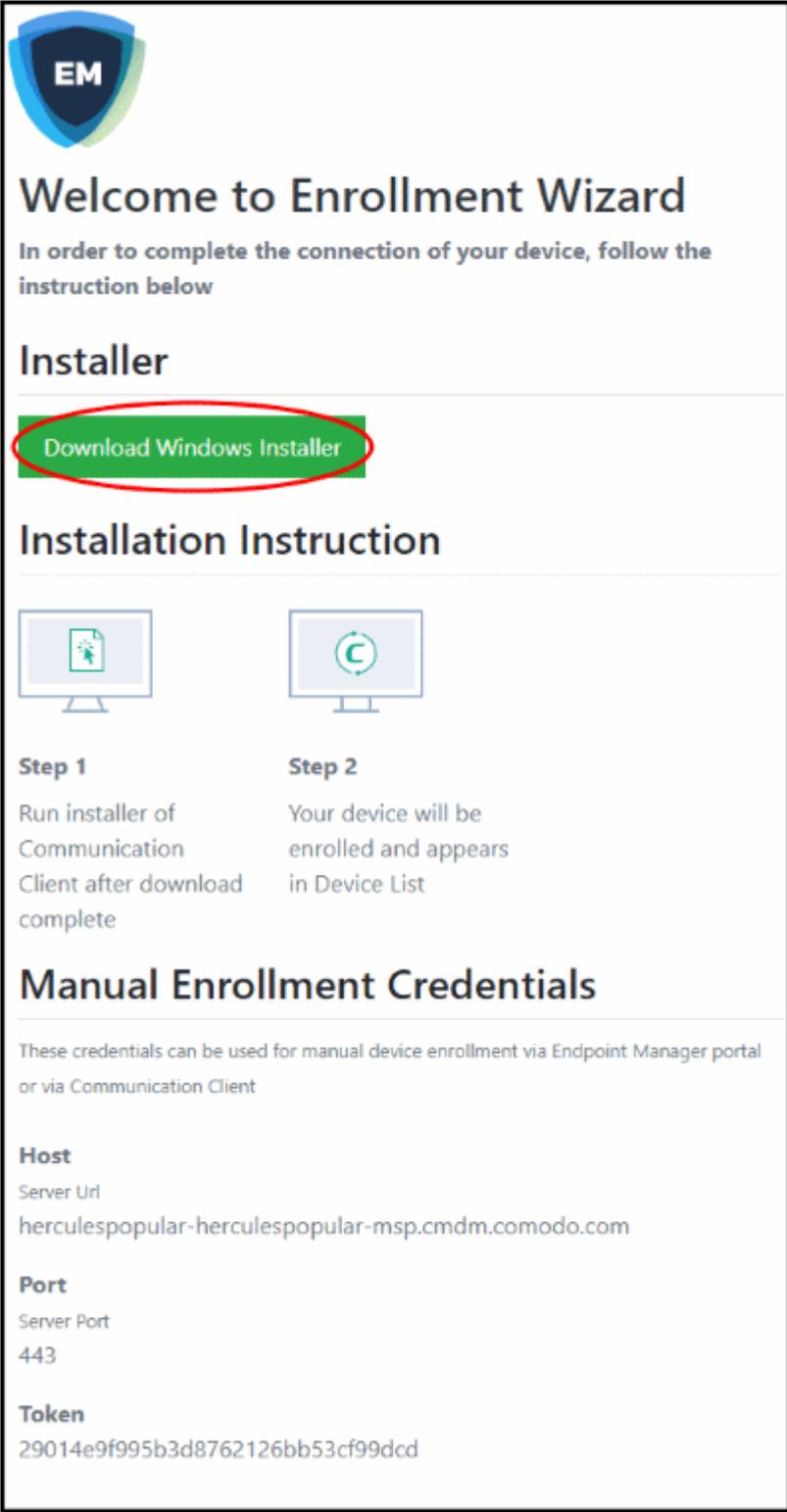
- The app is downloaded from the Apple store using the user's account.
- After installation, tap the green 'Run After Install' icon on the home screen:



The device is now enrolled and connected to Dragon.

## Enroll Windows PCs

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



**EM**

## Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

### Installer

[Download Windows Installer](#)

### Installation Instruction

	
<b>Step 1</b>	<b>Step 2</b>
Run installer of Communication Client after download complete	Your device will be enrolled and appears in Device List

### Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

**Host**  
Server Url  
herculespopular-herculespopular-msp.cmdm.comodo.com

**Port**  
Server Port  
443

**Token**  
29014e9f995b3d8762126bb53cf99dcd

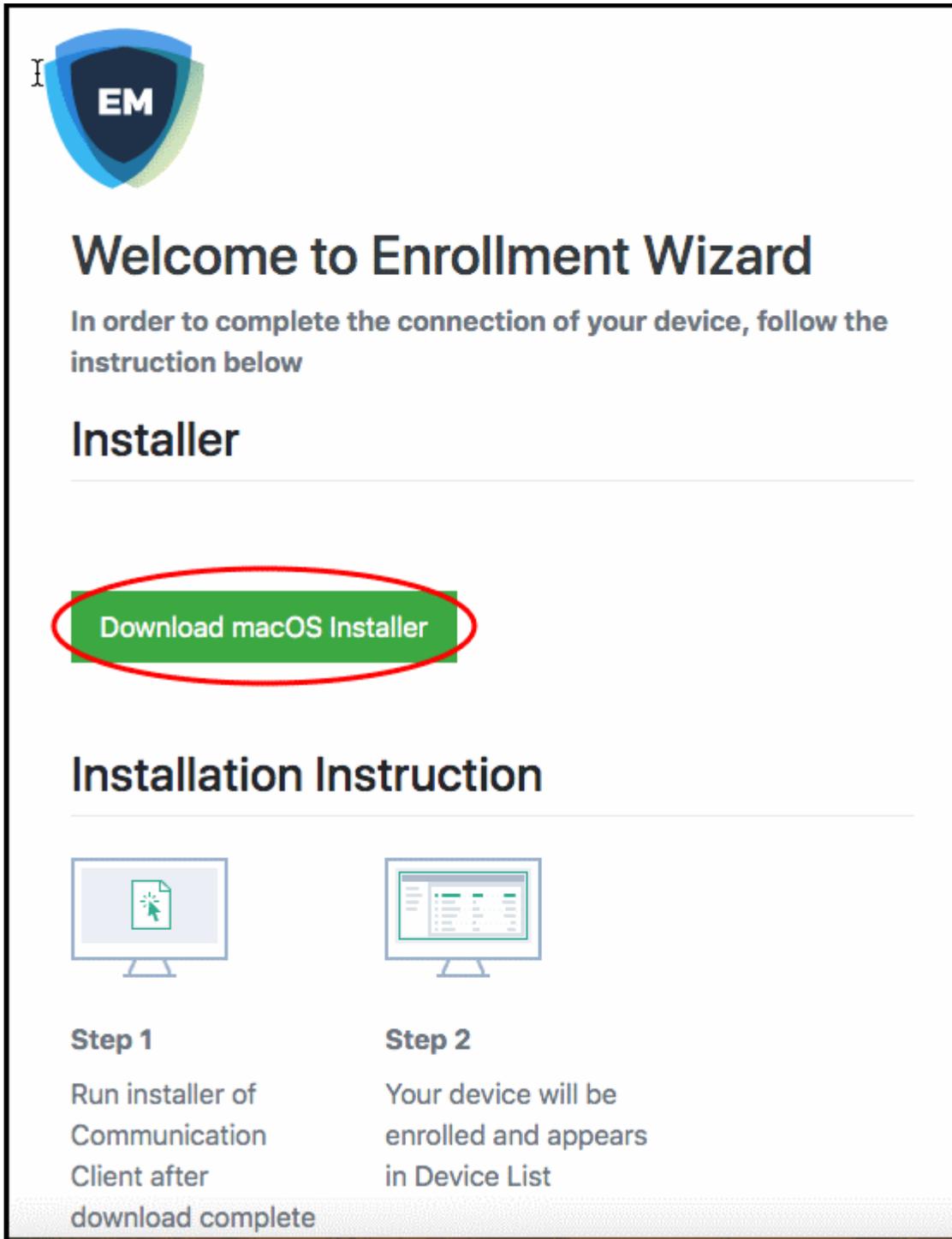
- Click the 'Download Windows Installer' button.
- The Dragon client setup file gets downloaded.
- Double-click on the file to install the communication client.

The device automatically gets added to Dragon Enterprise 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.

## Enroll Mac OS Devices

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



**EM**

## Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

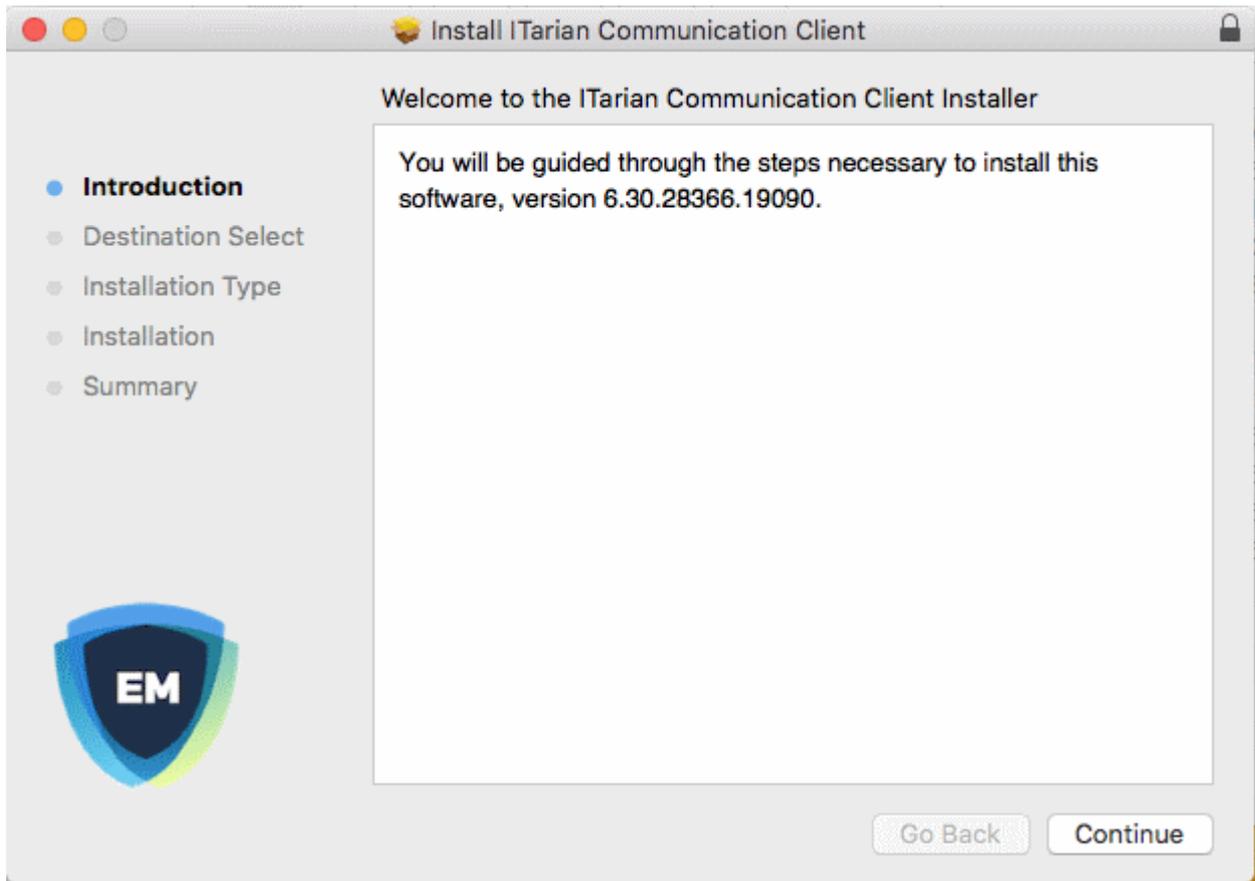
### Installer

**Download macOS Installer**

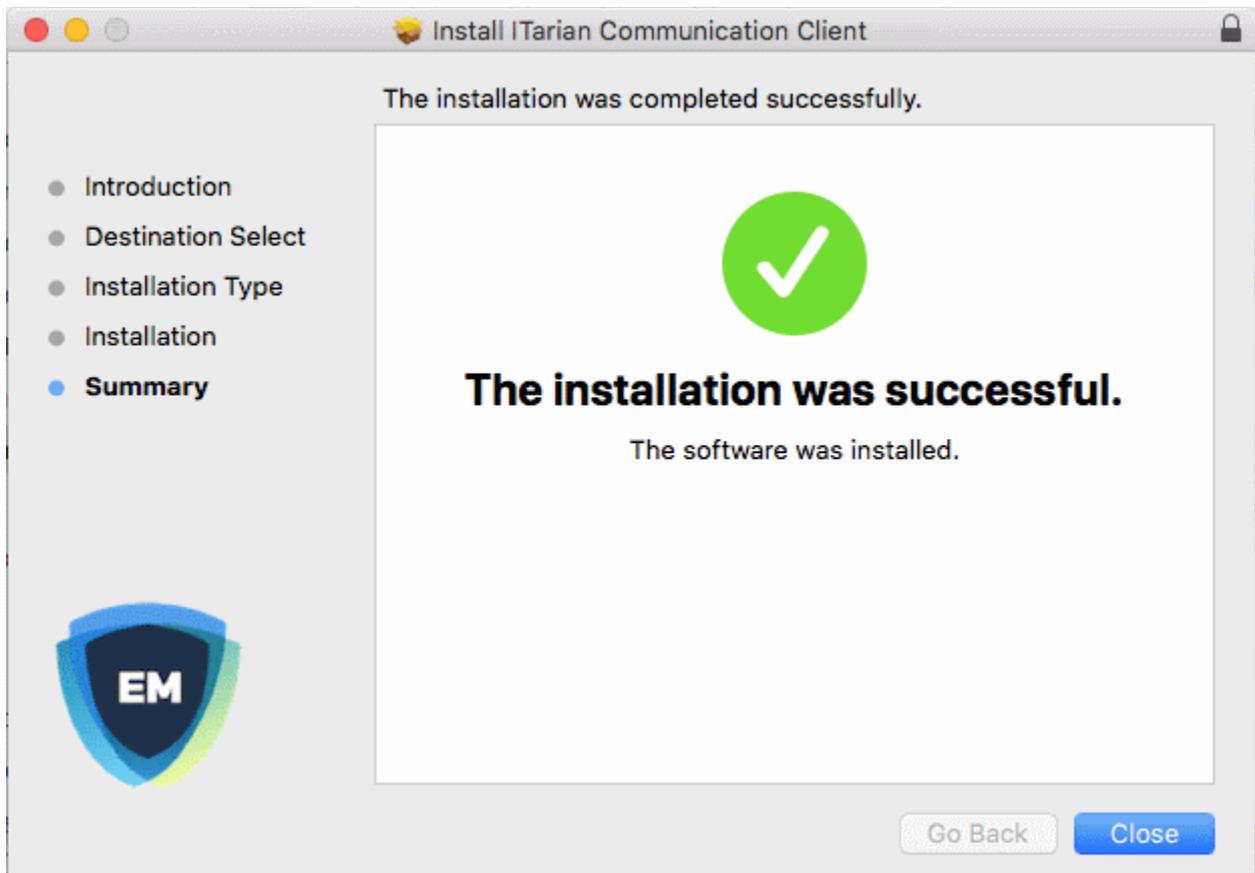
### Installation Instruction

	
<b>Step 1</b>	<b>Step 2</b>
Run installer of Communication Client after download complete	Your device will be enrolled and appears in Device List

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

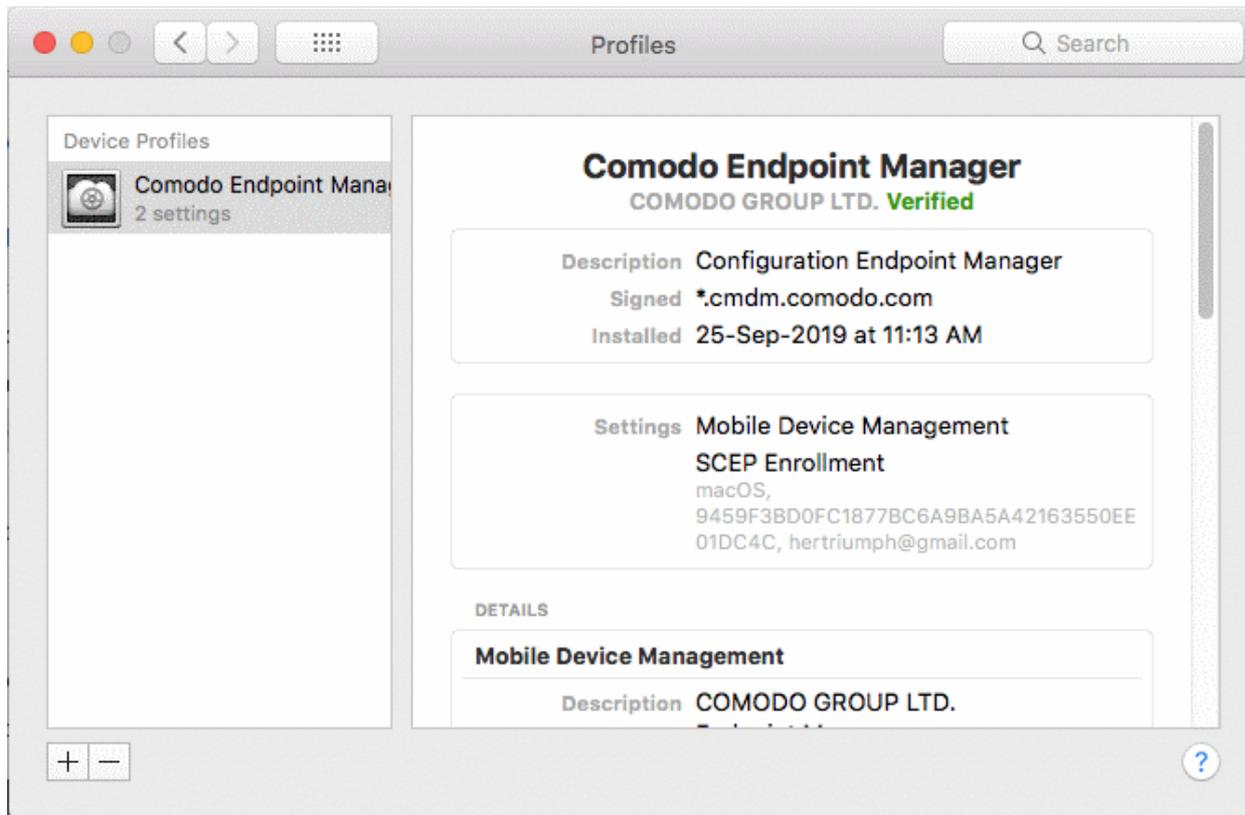


- Follow the wizard to complete the installation.



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

install it.



- The device is automatically added to Dragon Enterprise once the 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_cTjIw6gG_installer.run
sudo./itsm_cTjIw6gG_installer.run
```

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

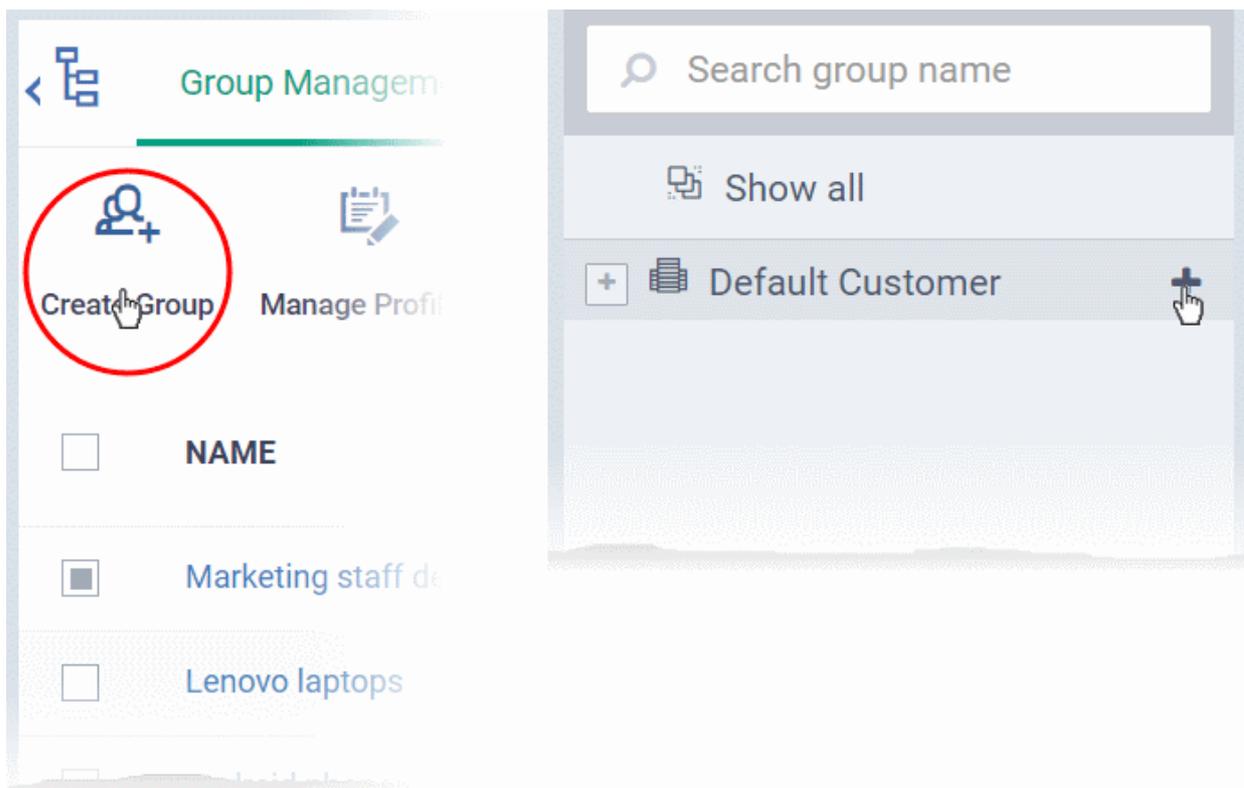
- The device is automatically added to Dragon Enterprise once the installation is complete. CCS is installed if you included it in the setup wizard.

### 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.

#### Create a device group

- Click 'Assets' > 'Devices' > 'Device List'
- Click the 'Group Management' tab
- Click the 'Create Group' button
  - Alternatively, place your mouse over the 'Default Customer' on the left and click the '+' sign that appears:



### Add Group ✕

**Name \***

**Customer \***

**Devices**

**Add**

- **Name** - Create a label to identify the group.

- **Customer** - The field is pre-populated with 'Default Customer'. You cannot edit this field.
- **Devices** - Choose devices which will be members of the group.
  - 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 'Add'. Repeat the process to create more groups.

The next step is to create profiles.

### Step 6 - Create Configuration Profiles

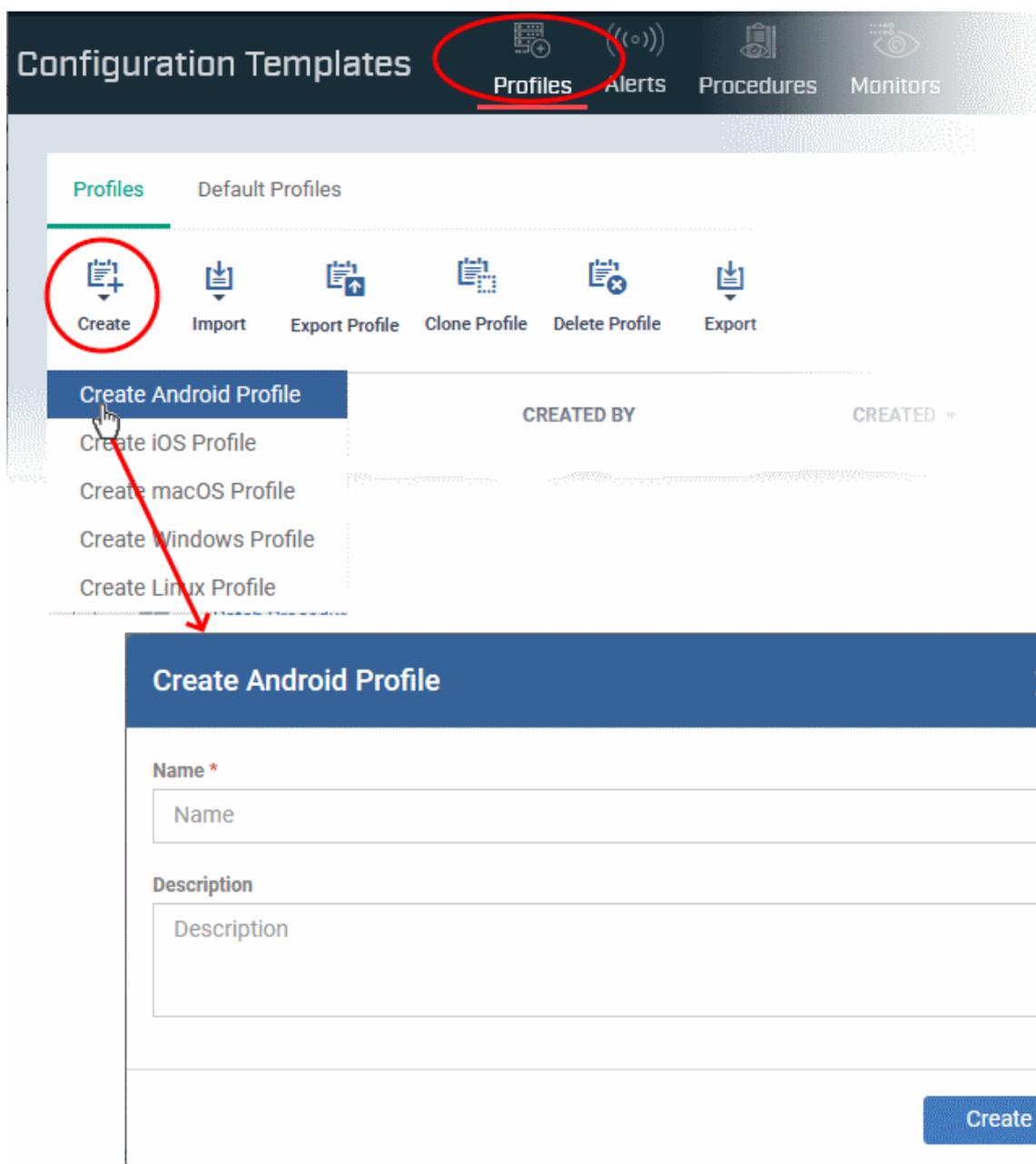
- A configuration profile is a collection of settings which are applied to iOS, Android, Windows, Linux and Mac devices.
- Each profile lets you specify a device's network access rights, security settings, antivirus scan schedule, and other details.
- There are two main types of profile - 'Custom' and 'Default'. You can create custom profiles for users, user groups, devices and device 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**

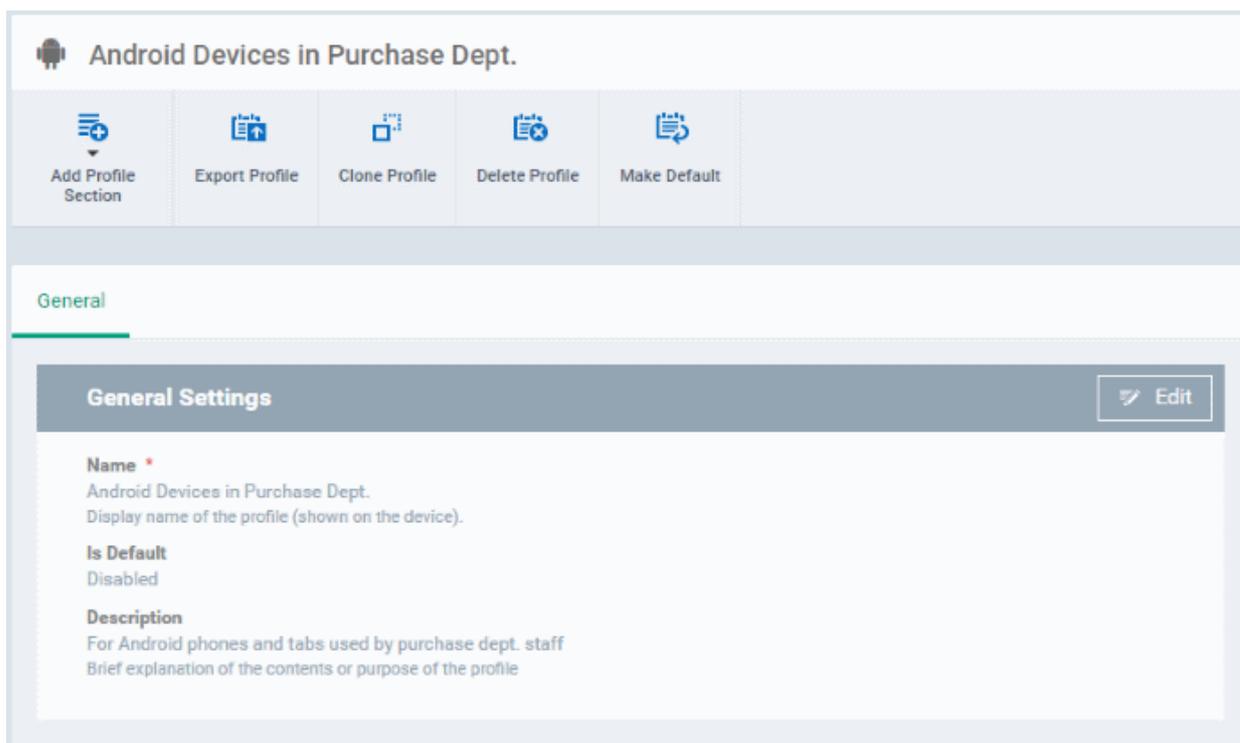
#### Create an Android Profile

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



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

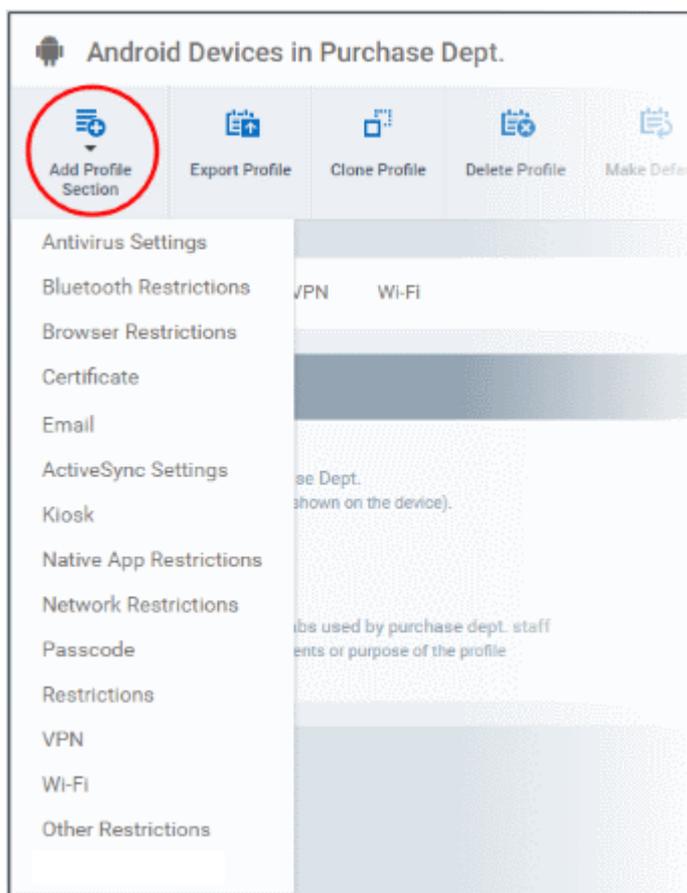
The profile opens at the 'General Settings' screen:



- 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.

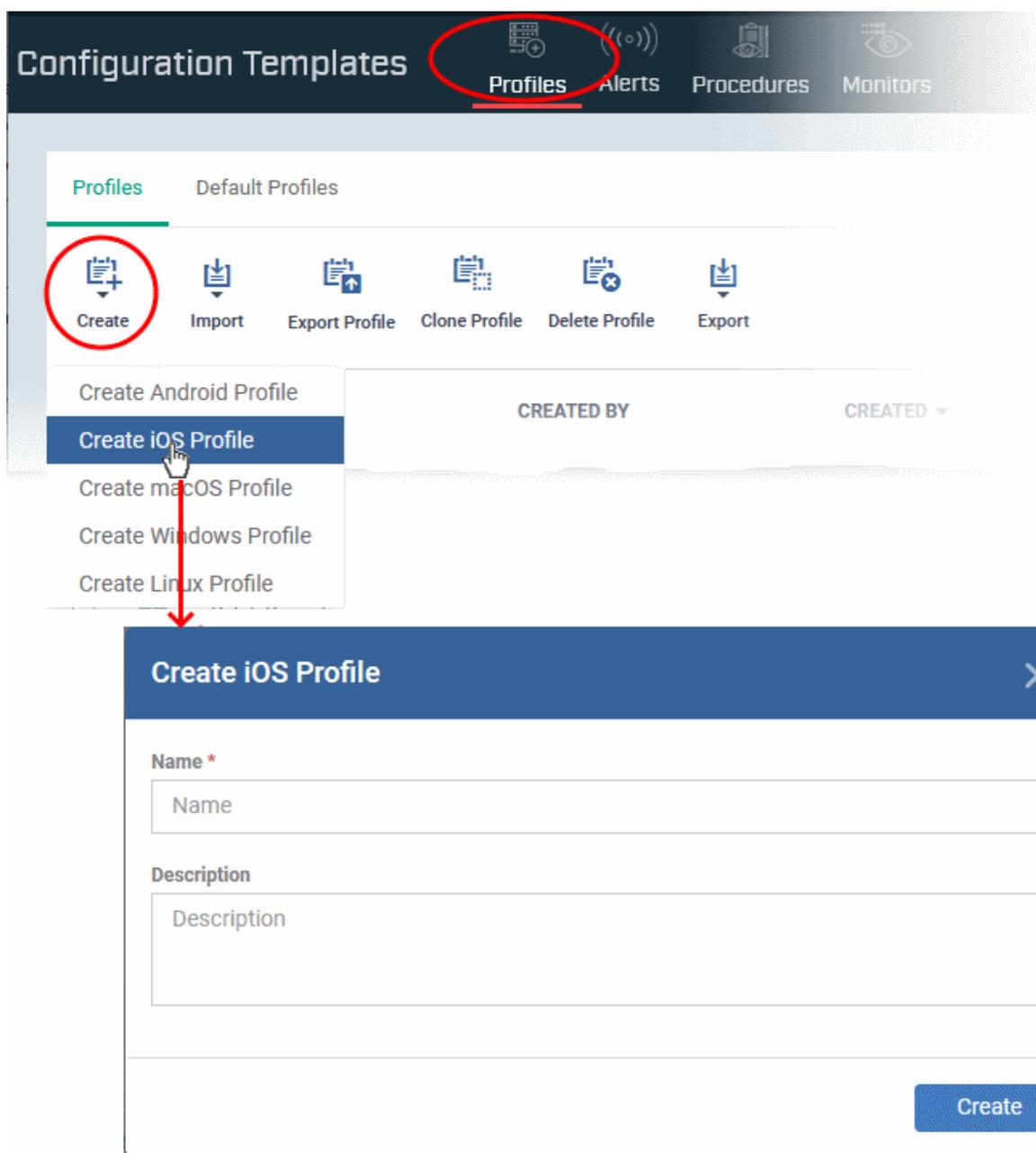
See **Profiles for Android Devices** in the full guide for more information on these settings. In brief:

- **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 Dragon Enterprise. You can then choose these certificates when configuring specific features in Dragon. 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.

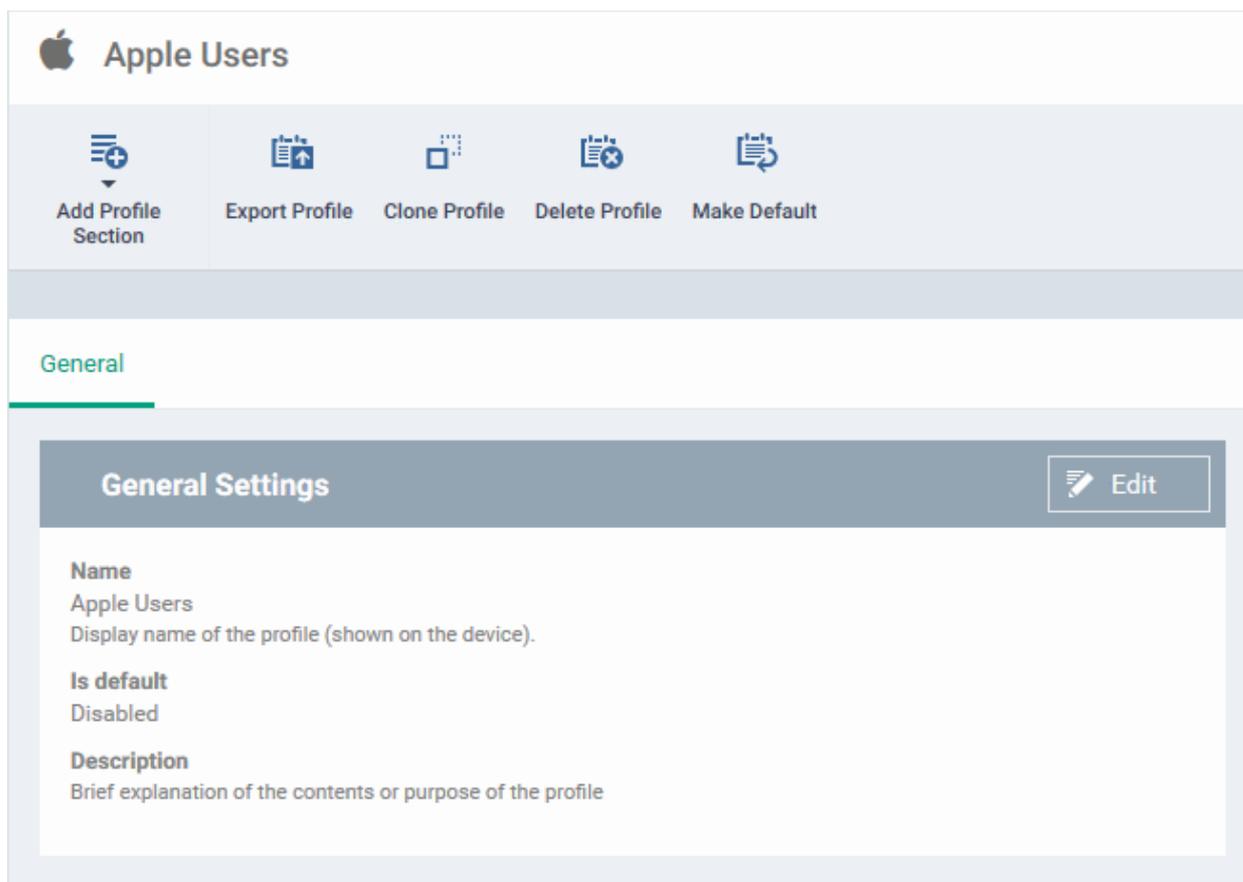
- **Native App Restrictions** - Configure which native applications should be accessible to users. Native applications are those that ship with the device OS and include apps like Gmail, YouTube, the default Email client and the Gallery. This feature is supported for Android 4.0+ and Samsung for Enterprise (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 'Assets' > 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create iOS Profile'



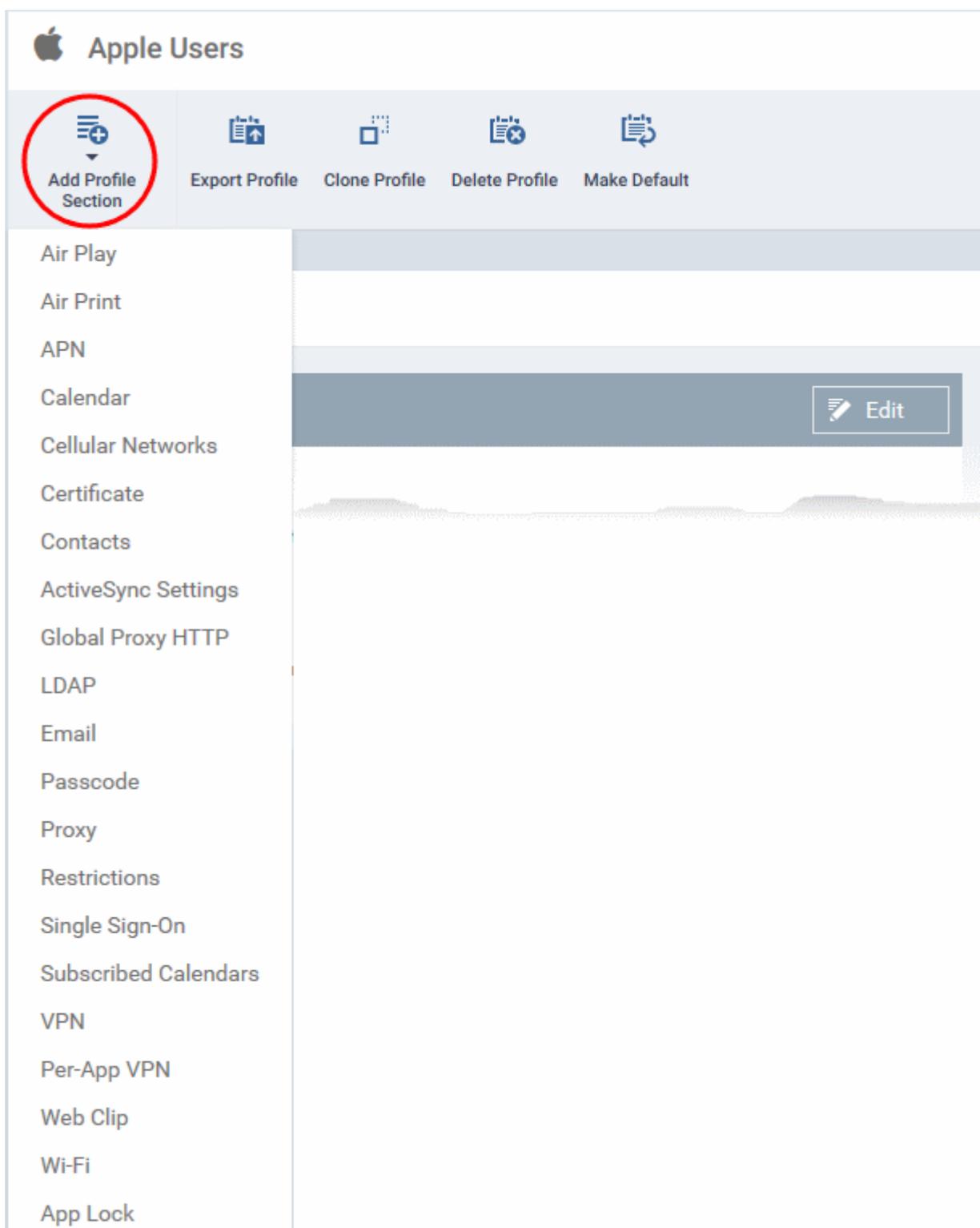
- Enter a name and description for the profile and click 'Create'.
- The profile is created and the 'General Settings' for the profile is displayed.



- 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:



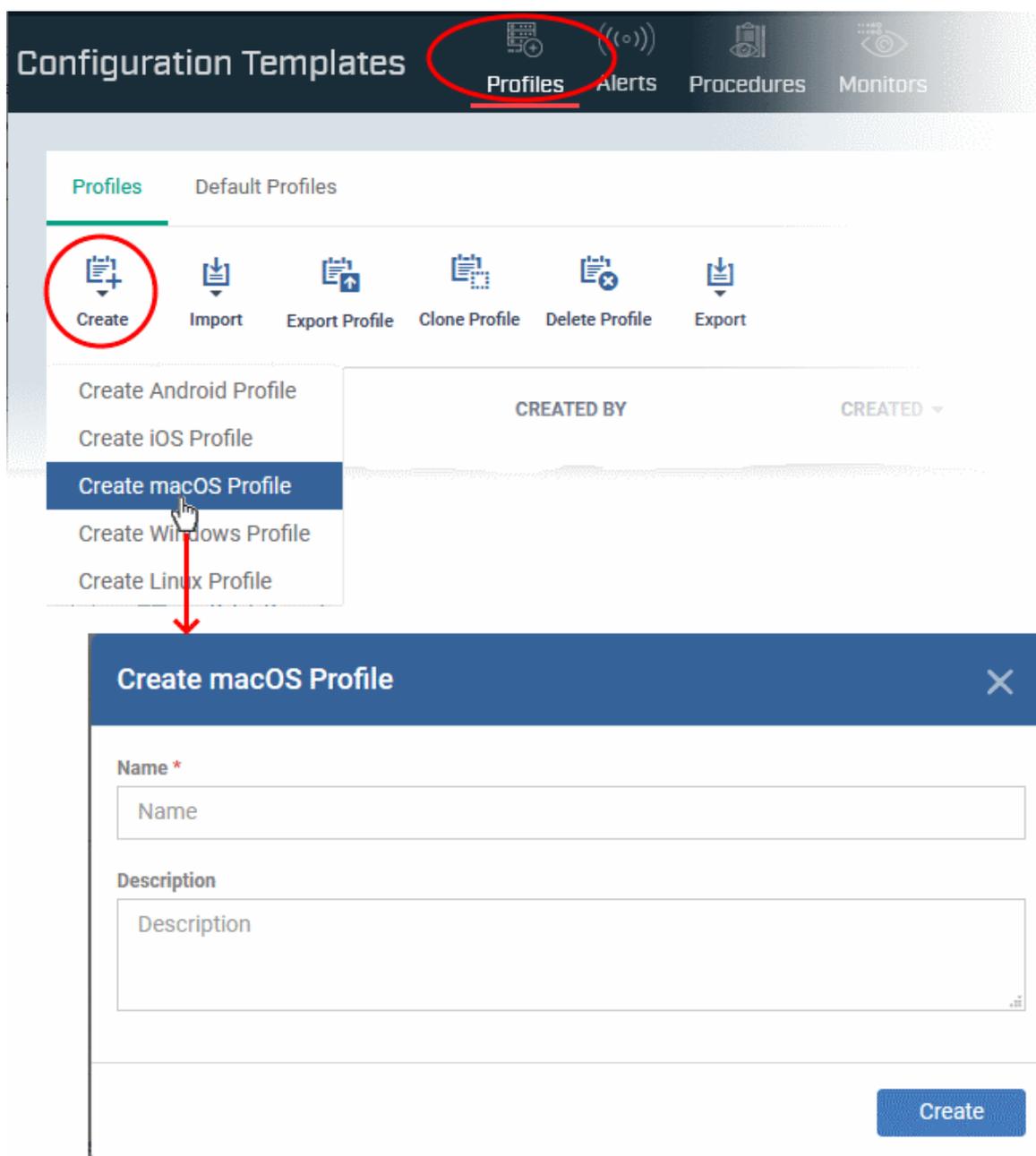
- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied upon device enrollment.
- **Airplay** - Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (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 proxy 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 a similar role to the APN setting and actually replaces it in iOS 7 and above.
- **Certificate** - Upload certificates to Dragon Enterprise. You can then choose these certificates when configuring specific features in Dragon. 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.

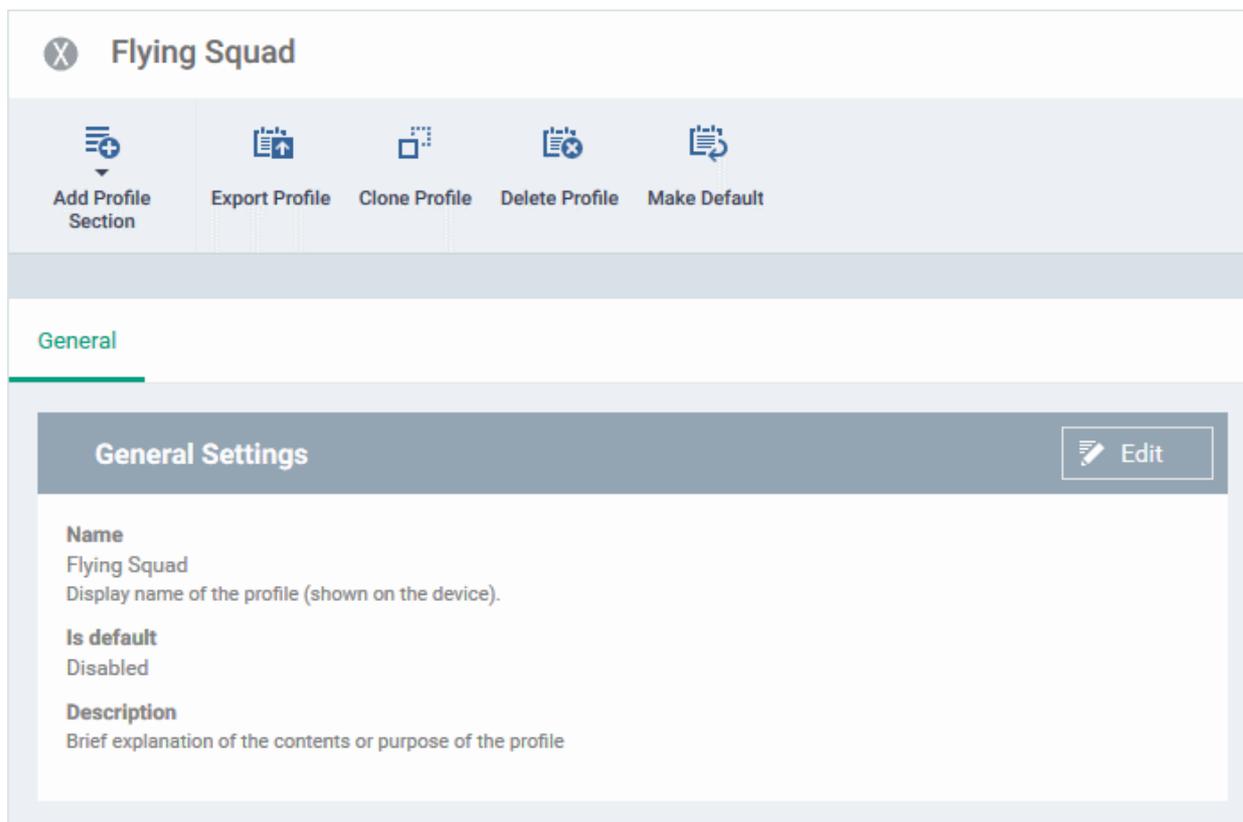
### Create a Mac OS Profile

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



- Name - Enter a label for the profile
- Description - Enter appropriate short notes for the profile
- Click the 'Create' button

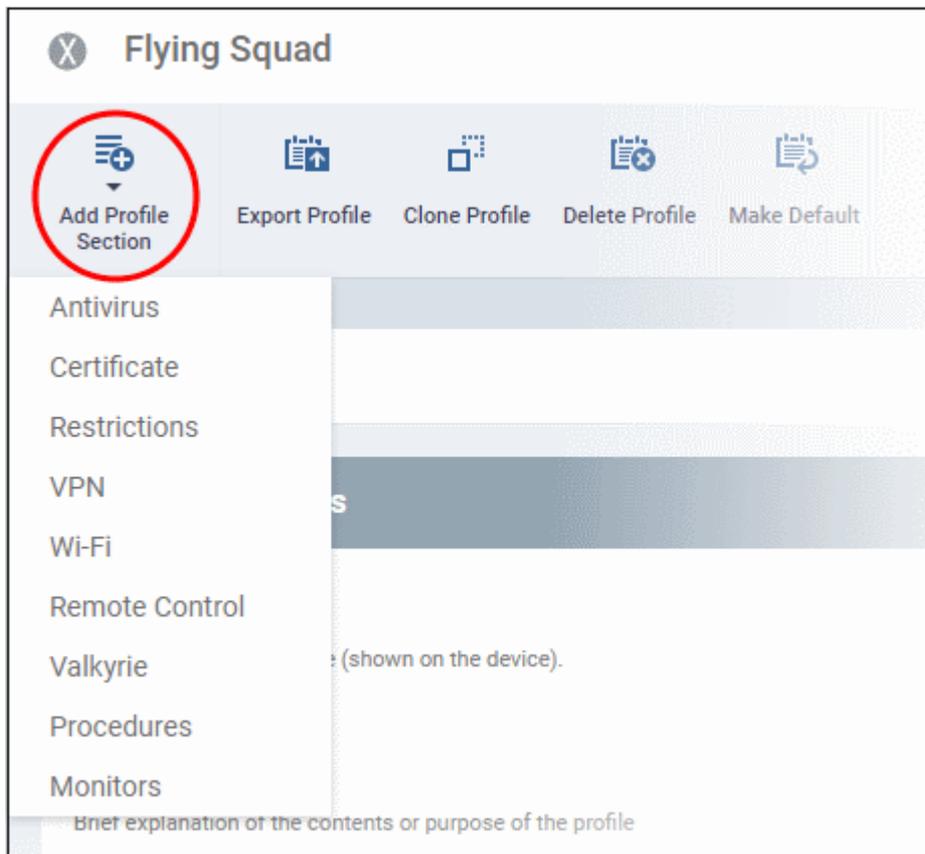
The new profile will open at the general settings page:



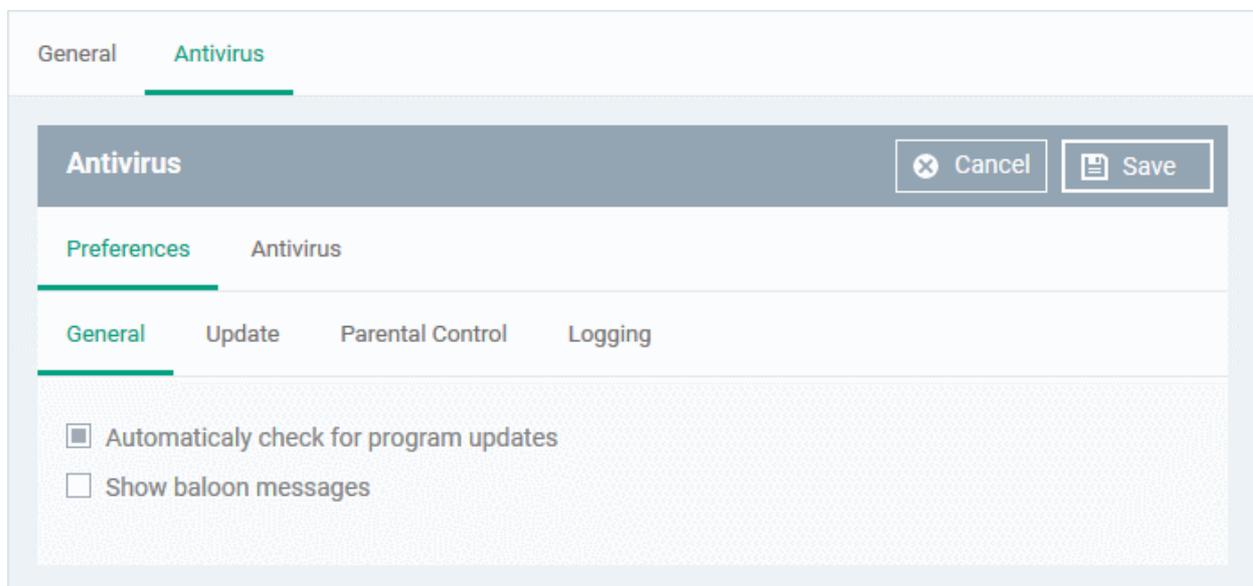
- **'Make Default'** - A 'default' profile is one that is applied automatically to any newly added device which matches its operating system. Click this button if you want all MAC OS devices to receive this profile.
- Click 'Save'.

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 Dragon profile.

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

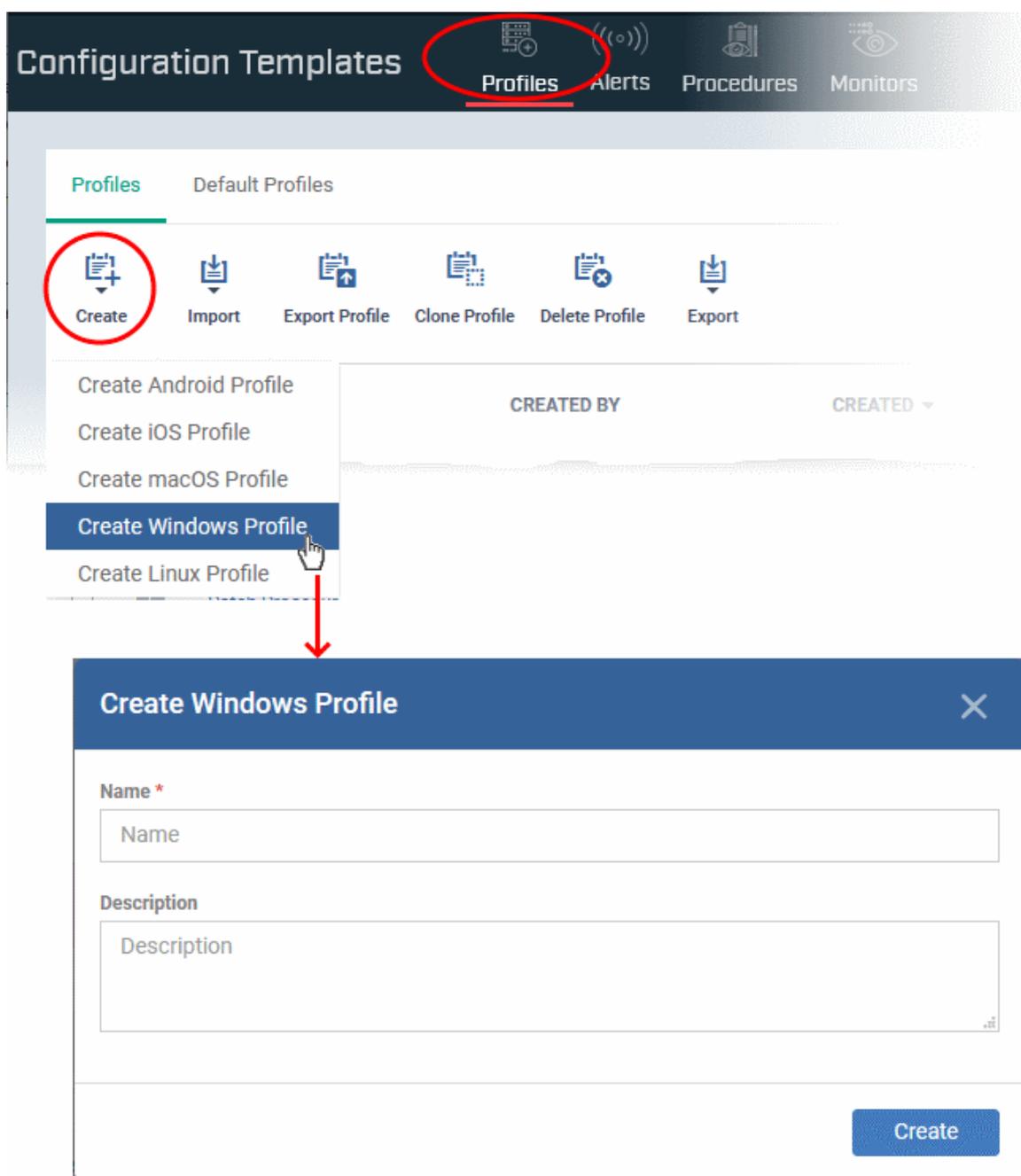
See **Profiles for Mac OS Devices** in the main guide for more details on this area. In brief:

- **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 Dragon Enterprise. You can then choose these certificates when configuring specific features in Dragon Enterprise. 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.
- **Procedures** - A procedure is a script designed to accomplish a specific task on target devices. For example, you can run procedures to change the permissions on specific folders on multiple devices, or lock a device after a certain period of time.
- **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.

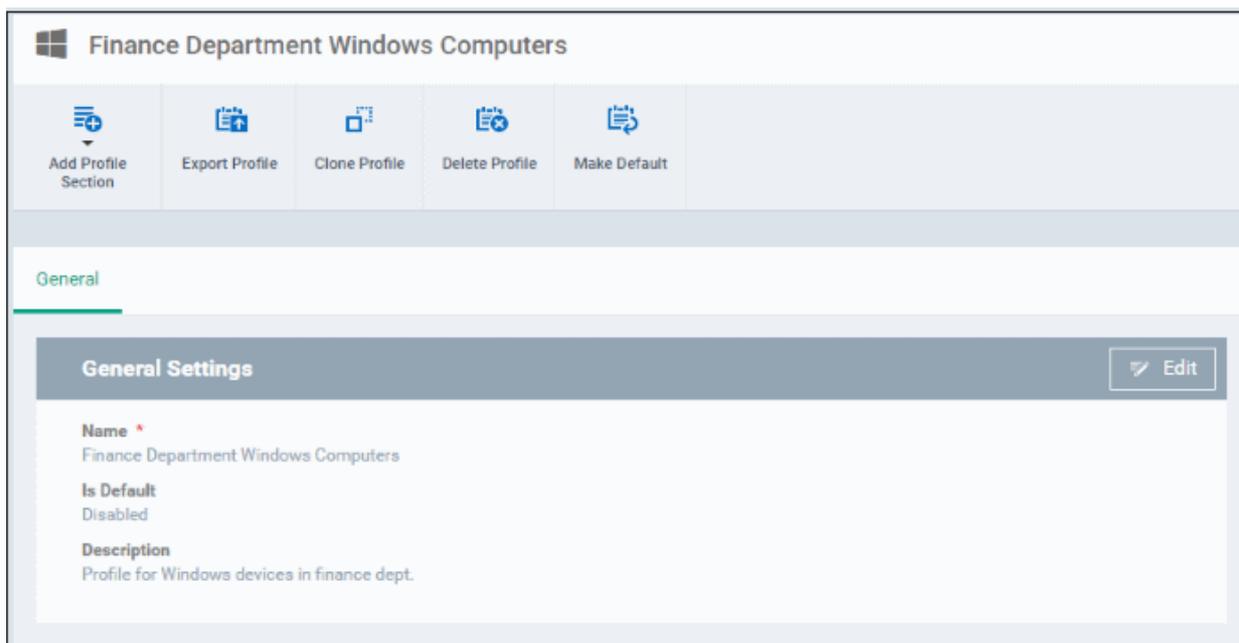
#### Create a Windows profile

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



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

Your profile will open at its configuration page:



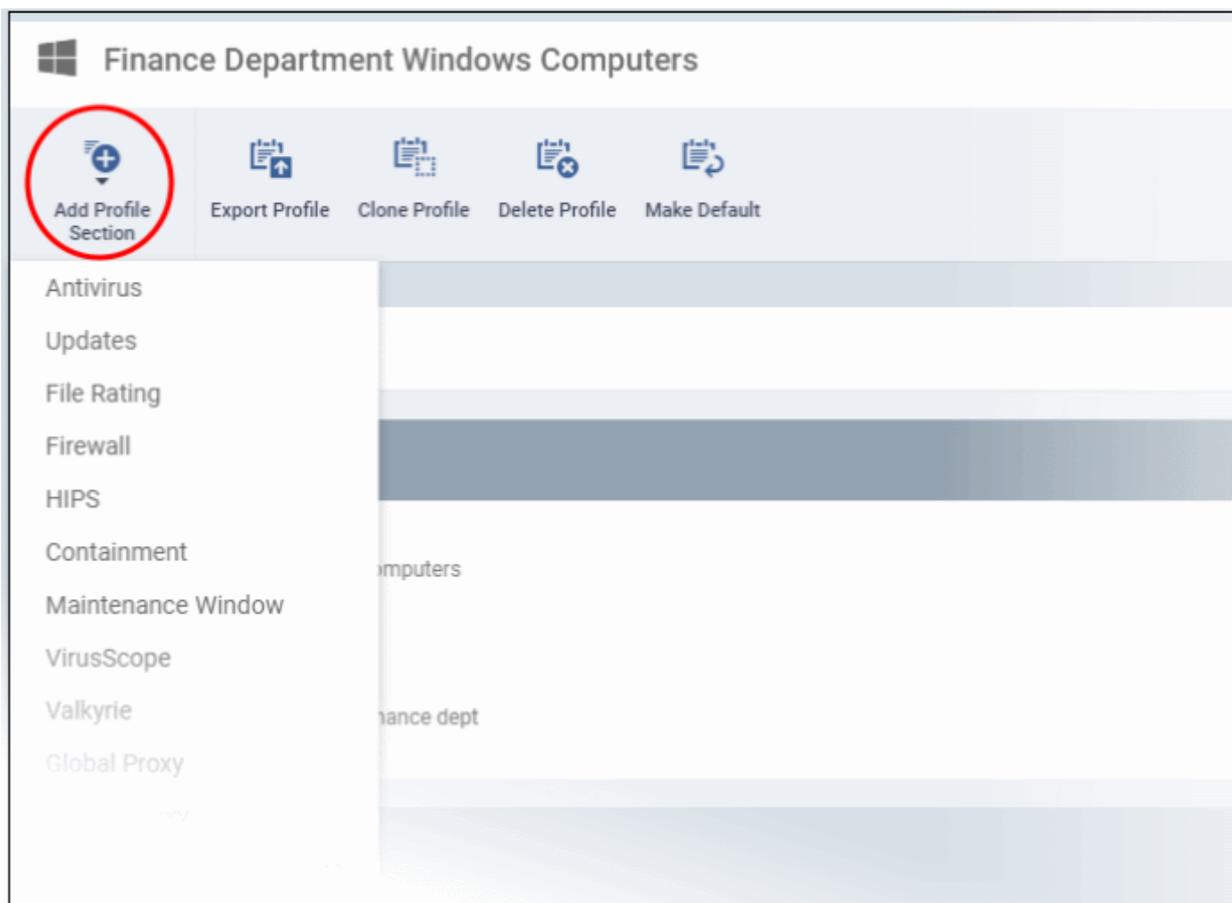
- Click 'Edit' if you wish to modify basic profile settings:
  - **'Is Default?'** - A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- Click 'Save'.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific security or management feature.
- For example, there are profile sections for 'Antivirus', 'External Device Control', 'Firewall', 'Procedures' and so on.
- You can add as many different sections as you want when building your profile.

To get started:

- Click 'Add Profile Section'
- Select the component that you want to add to the profile:



The settings screen for the selected component will open.

- Configure the settings and parameters and click 'Save'

The new profile section will become available as a tab in this interface.

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

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

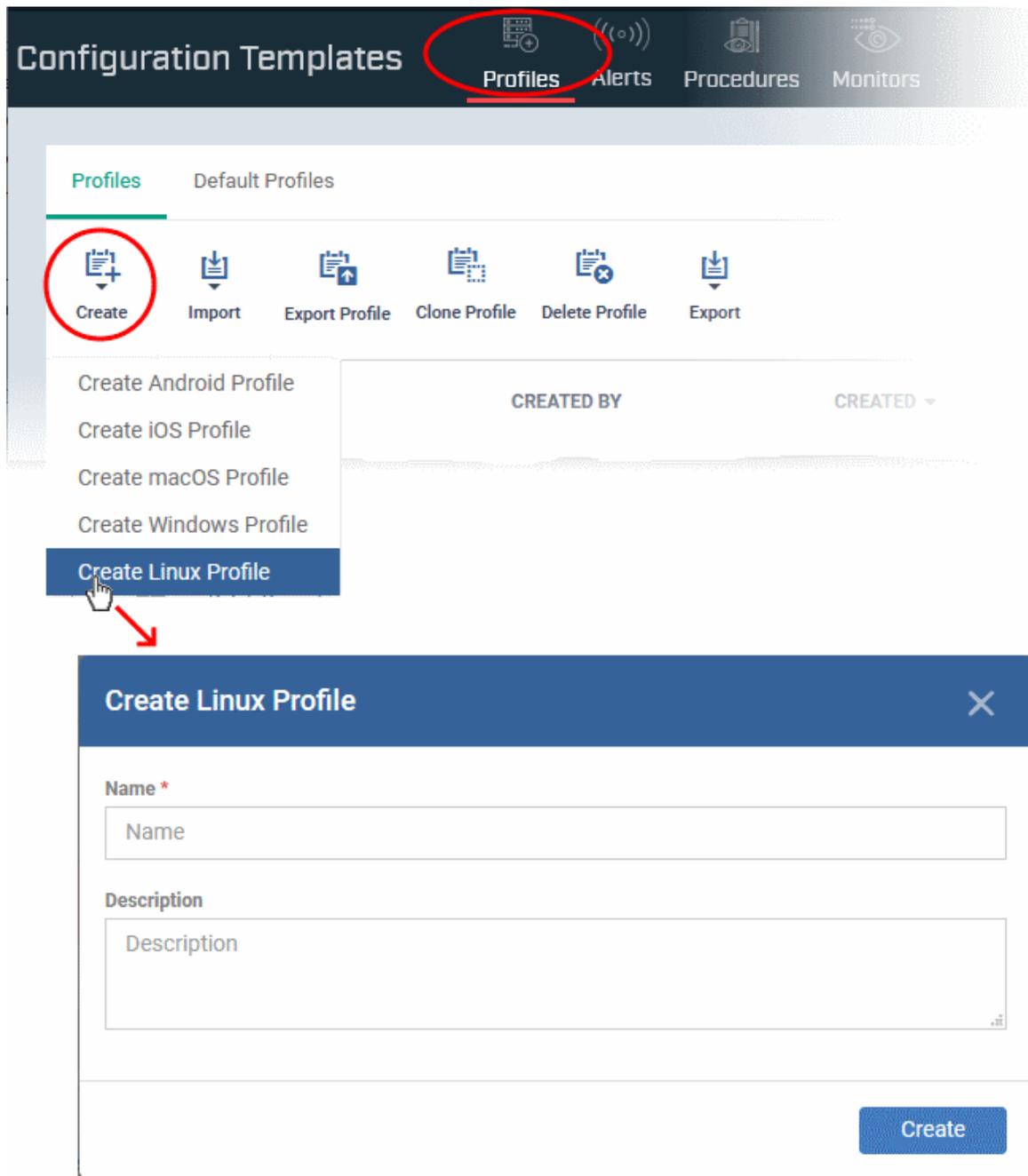
See **Profiles for Windows Devices** in the full guide for more information on these settings. In brief:

- **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 see the [help page explaining File rating Settings](#) in [Dragon Enterprise 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 [Dragon Enterprise online help guide](#), for more details.
- **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 [Dragon Enterprise online help guide](#) for more details.
- **Containment** - Enable auto-containment of unknown files, add exclusions, configure containment behavior, view and manage auto-containment rules and configure the Virtual Desktop. See the [help page explaining Containment settings](#) in [Dragon Enterprise online help guide](#), for more details.

- **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 the [help page explaining VirusScope](#) in [Dragon Enterprise online help guide](#) for more details.
- **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 Dragon Enterprise 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 Dragon 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** - Dragon is capable of scanning managed Windows devices and identify files containing sensitive information. 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.
  - **Note:** This feature will be available in future versions.
- **Patch Management** - Enable / disable patch operations on endpoints. The settings affect on-demand patch operations, scheduled patch operations and patch installations via procedures.

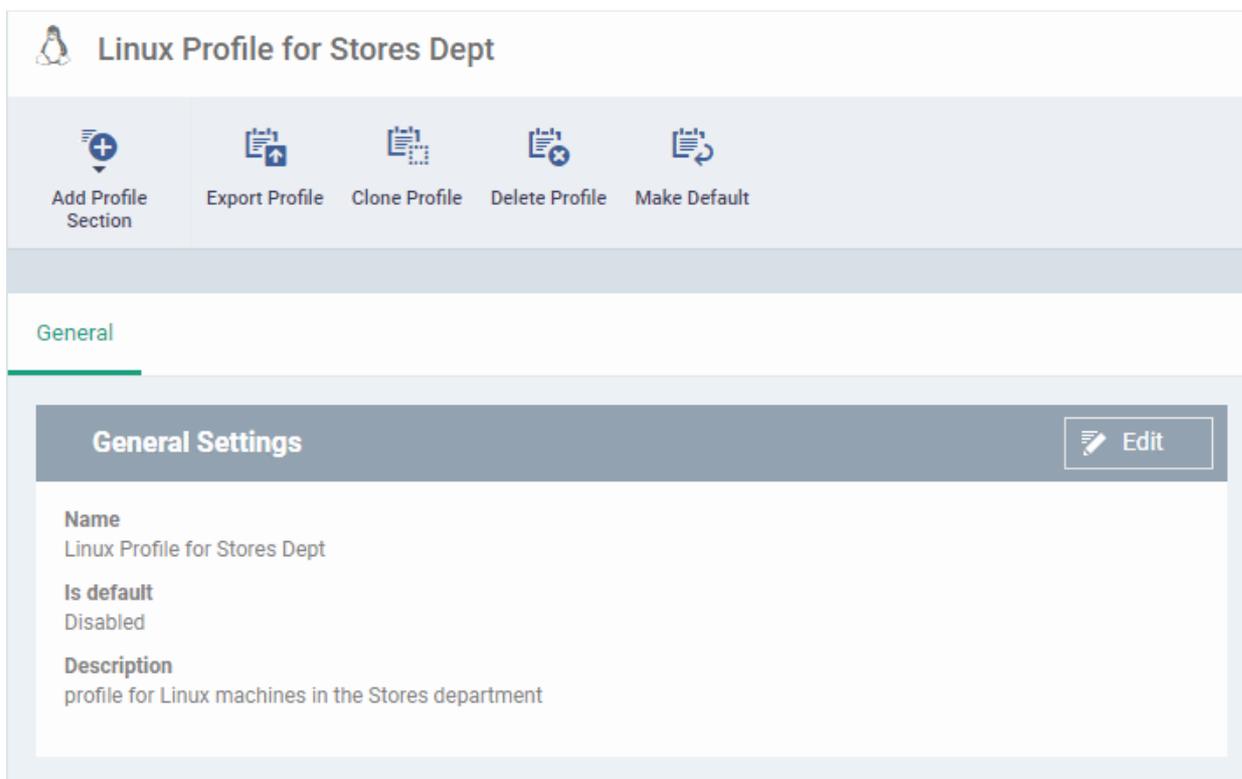
### Create a Linux Profile

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



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

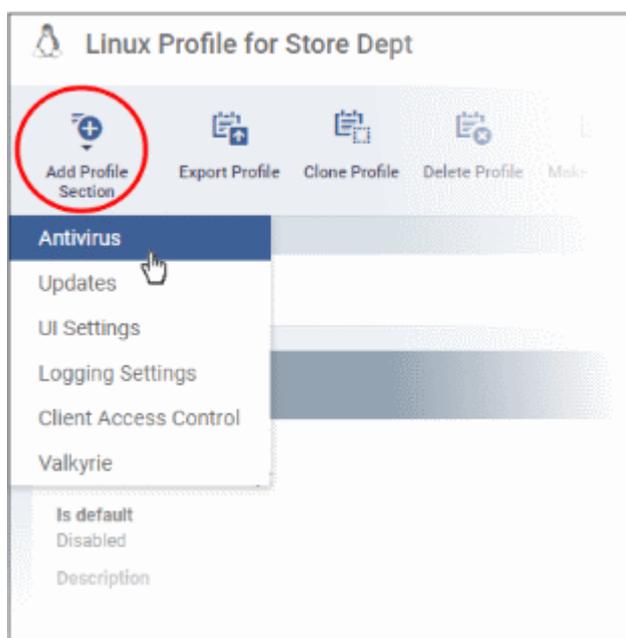
The Linux profile will be created and the 'General Settings' section will be displayed. The new profile is not a 'Default Profile' by default.



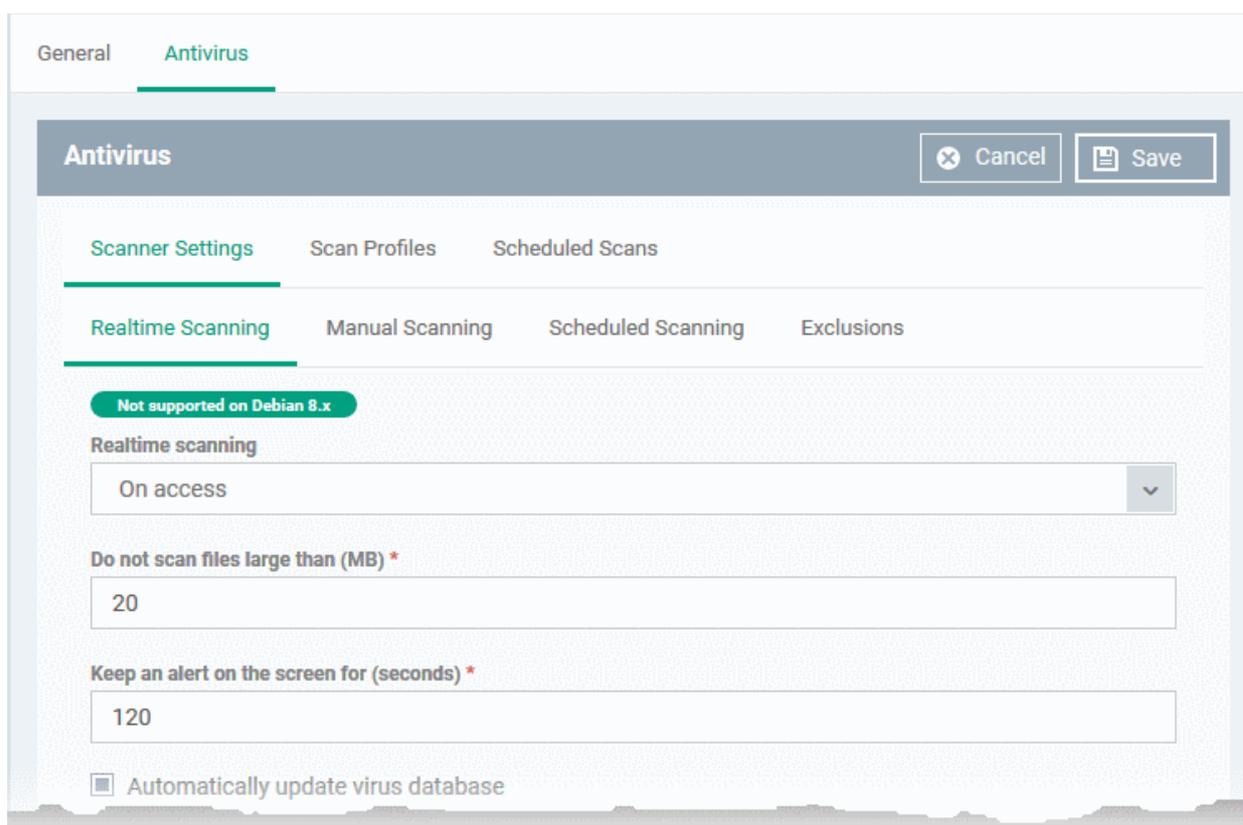
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

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 Dragon profile.

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

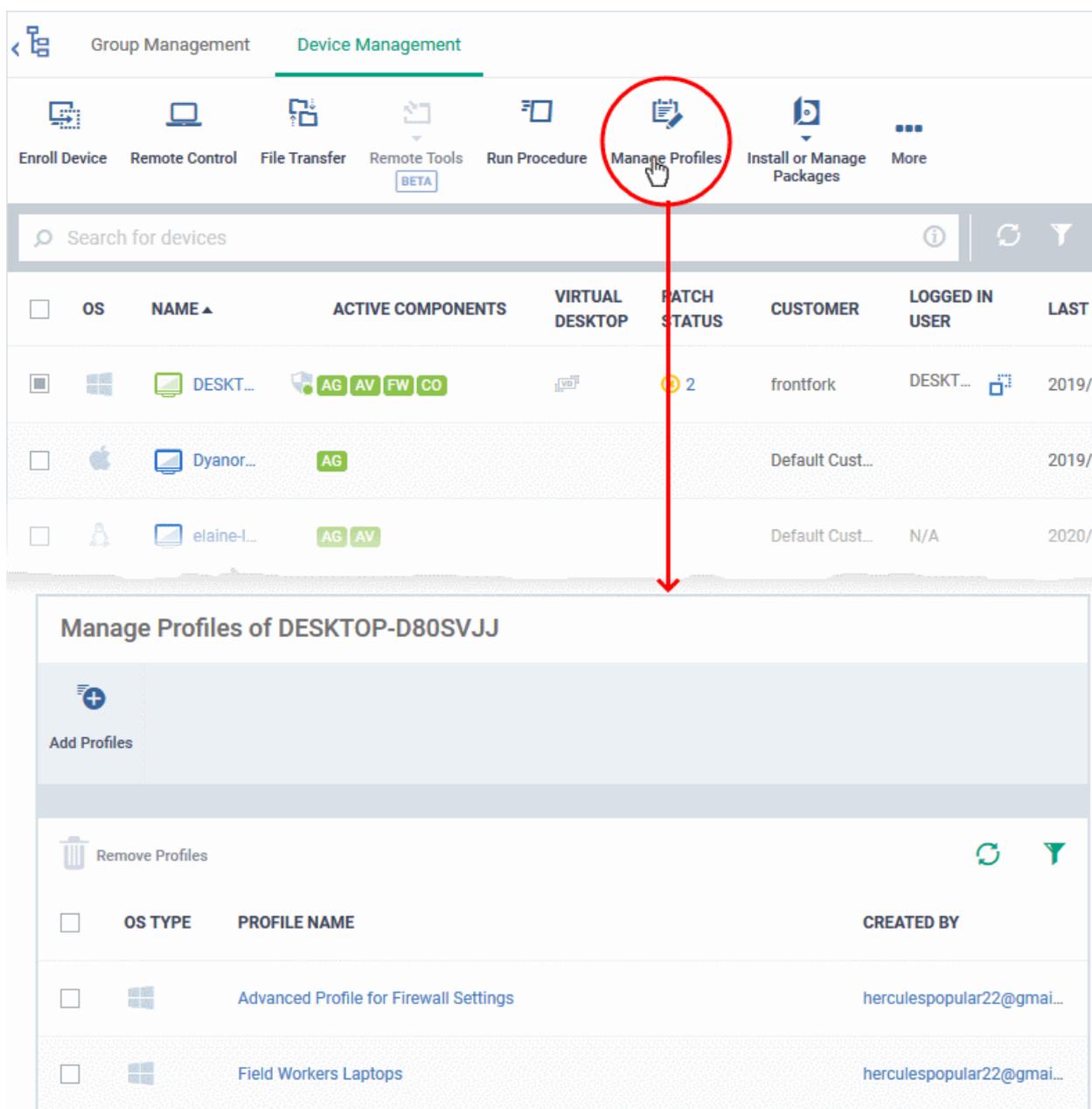
See **Profiles for Linux Devices** in the main guide for more details on this area. In brief:

- **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 'Assets' > 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a group to view just its devices
  - Or
  - Select 'Show all' to view every device enrolled to Dragon

- 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.

### Manage Profiles of DESKTOP-D80SVJJ

+ Add Profiles

Remove Profiles
↻ ⚙

	OS TYPE	PROFILE NAME	OWNER
<input type="checkbox"/>		Finance Department Windows Computers	herculespopular22@gmail...

---

### Add Profiles to DESKTOP-D80SVJJ

Save
↻ ⚙

	OS TYPE	PROFILE NAME	OWNER
<input type="checkbox"/>		Default Profile for Windows Devices	herculespopular...
<input type="checkbox"/>		Default Profile for Windows	herculespopular...
<input checked="" type="checkbox"/>		Suspicious Files Folder for John	herculespopular...
<input checked="" type="checkbox"/>		Monitoring Important Data	herculespopular...
<input type="checkbox"/>		Patch Procedure	herculespopular...

- 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 'Assets' > 'Devices' > 'Device List'.
2. Click the 'Group Management' tab
3. Expand 'Default Customer' on the left to view groups created for your company
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.

### Step 8 - Upgrade to full account

There are two types of licenses required for Dragon Enterprise platform:

- **Advanced Endpoint Protection (AEP)** - For management and protection of devices, installed with Comodo security products.
- **Endpoint Detection and Response (EDR)** - For event analysis, real-time monitoring and detection of malicious events on Windows endpoints. EDR requires an agent installed on the managed device. Only the devices that are covered by number of EDR licenses on your Dragon Enterprise account will get EDR protection.

You can subscribe for AEP and EDR licenses separately for the numbers of devices that require respective protection types.

- Each AEP or EDR license covers 1 active managed endpoint.
- Each AEP license covers 5 active mobile devices

An 'endpoint' is a workstation or server running Windows, Mac OS or Linux. Mobile = device running iOS or Android.

### Purchase licenses

#### AEP licenses

- Login to Comodo Accounts Manager (CAM) at <https://cam.comodo.com/login>
- The username and password are same as your Dragon Enterprise credentials
- Click 'Buy a Product'
- Click the 'AEP' tile
- Select 'Advanced Endpoint Protection Premium Edition (xxx-xxx devices)' license variant, depending on the number of devices you want to protect, from the 'Product' drop-down
- Select the term of the license
- Complete the customer information and payment details and click 'Signup'

Your order will be processed and the licenses are issued. See <https://help.comodo.com/topic-211-1-513-5915-purchase-comodo-products.html> if you need more help on this.

Your licenses will be automatically activated for your Dragon Enterprise account, on your next login to Dragon Enterprise.

#### EDR Licenses

- Login to Comodo Accounts Manager (CAM) at <https://cam.comodo.com/login>
- The username and password are same as your Dragon Enterprise credentials
- Click 'Buy a Product'
- Click the 'AEP' tile
- Select 'EDR 30 Days Data Retention (xxx-xxx)' license variant, depending on the number of devices you want to protect, from the 'Product' drop-down. The data retention period for this license type is 30 days.
- Select the term of the license
- Complete the customer information and payment details and click 'Signup'

Your order will be processed and the licenses are issued. See <https://help.comodo.com/topic-211-1-513-5915-purchase-comodo-products.html> if you need more help on this.

Your licenses will be automatically activated for your Dragon Enterprise account, on your next login to Dragon

Enterprise.

**Note:** If you do not have EDR paid licenses, but have paid AEP licenses, you can install EDR agent on the same number of devices covered by your paid AEP licenses. The EDR event collection is restricted only to unknown file events on the endpoints and the data retention period is 7 days.

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 [c1-support@comodo.com](mailto:c1-support@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 cyber attacks 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](https://www.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>