COMODO
Creating Trust Online®

Comodo
IT and Security Manager

Software Version 6.17

Quick Start Guide

Guide Version 6.17.040318

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo IT and Security Manager - Quick Start

This tutorial explains how to use Comodo IT and Security Manager (ITSM) to add users, enroll devices, create device groups and create/deploy device configuration profiles:

Step 1 - Enrollment and Configuration

Step 2 - Configure ITSM Communications

Step 3 - Add Users

Step 4 - Enroll Users' Devices

Step 5 - Create Groups of Devices (optional)

Step 6 - Create Configuration Profiles

Step 7 - Apply profiles to devices or device groups

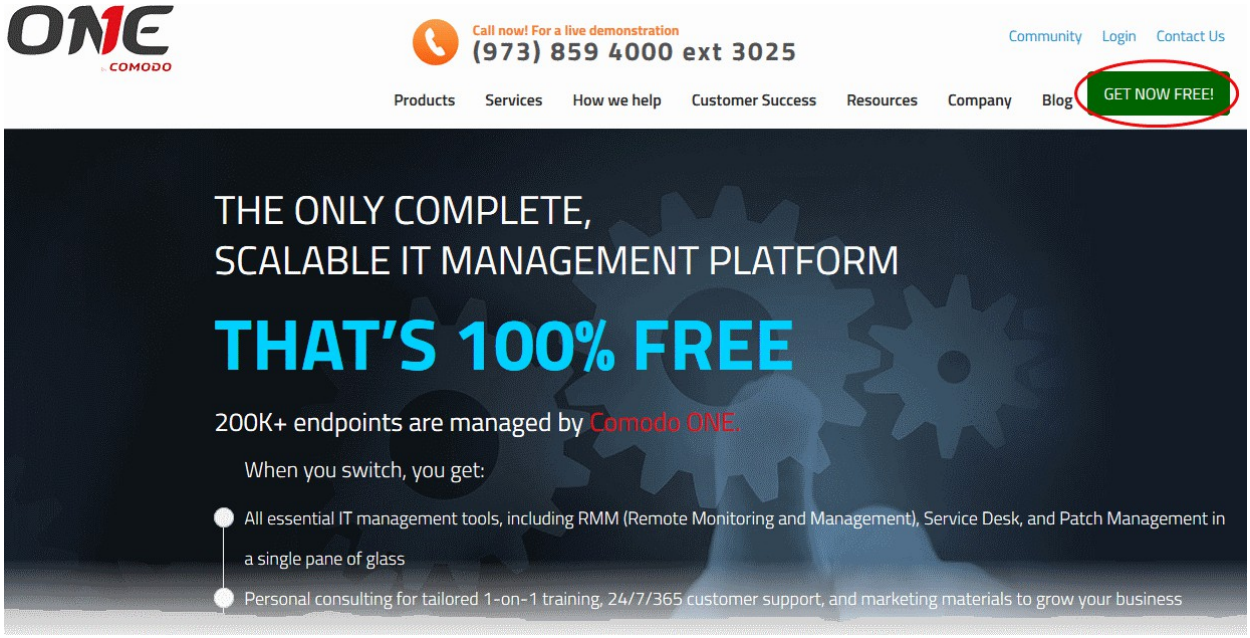
Note - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit files for analysis and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in Appendix 1.

Step 1 - Enrollment and Configuration

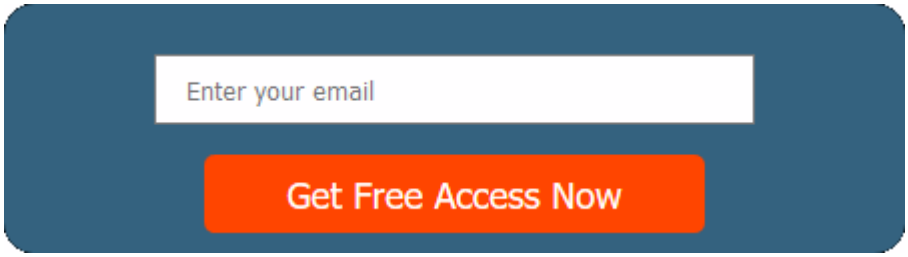
- Note: This step explains how to enroll to ITSM as a new customer.
- Existing Comodo One users can access ITSM by logging in at https://one.comodo.com/app/login then clicking 'Licensed Applications' > 'IT and Security Manager'.
- For more details on Comodo One services, see the online guide at https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html

Getting a new Comodo ITSM subscription is very easy and can be completed in a few steps.

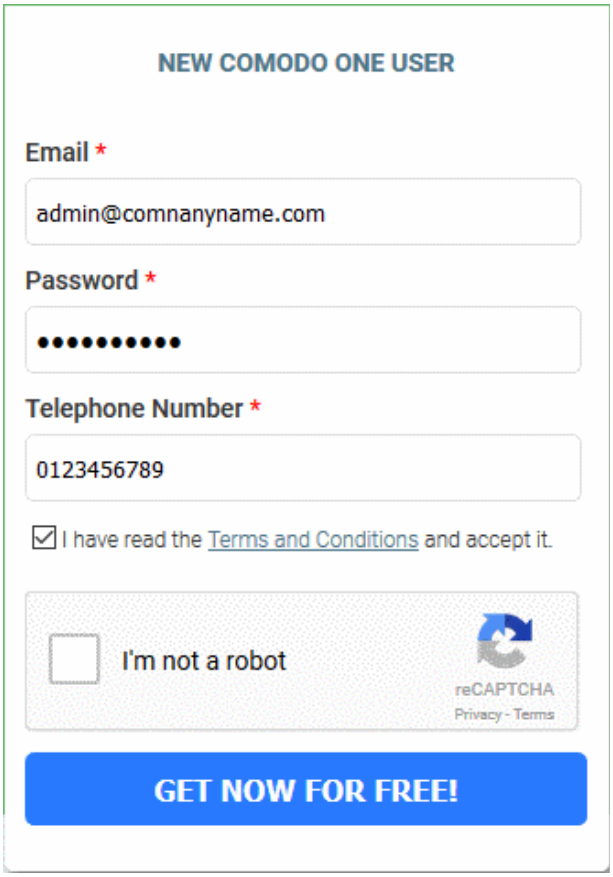
- Visit https://one.comodo.com/
- Click 'Get Now for Free!' at top-right



You will be taken to the Comodo One enrollment wizard:



- Enter your email address and click 'Get Free Access Now'
- Next, complete the short registration form:

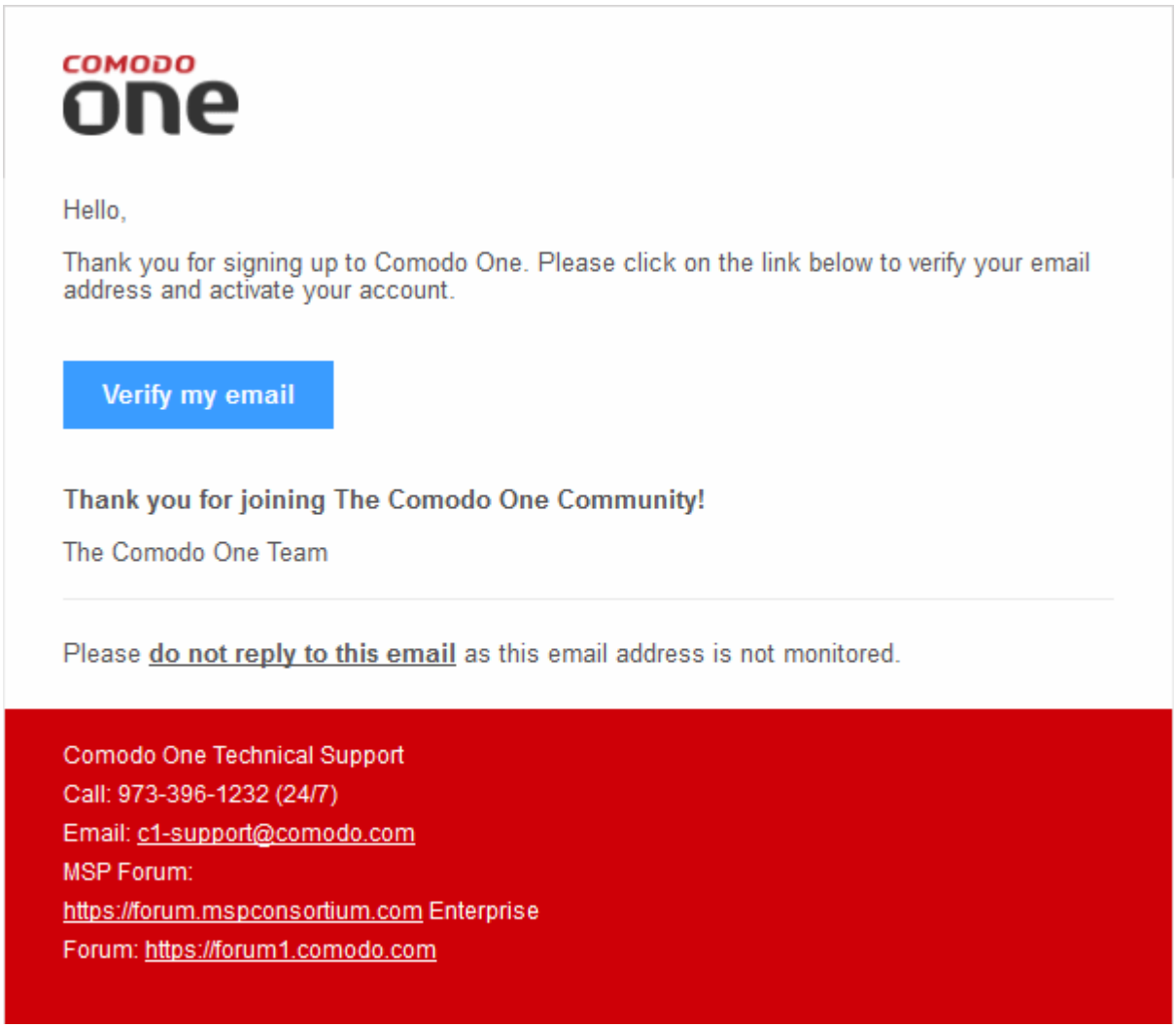


- **Email** - This will be pre-populated with the address you provided in the previous step. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
- **Password** - Create a password for your C1 account. Password rules:

  - At least eight characters long
  - Contain a mix off 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 'EULA' link and select the 'I have read EULA and accept it' check box.
- **Captcha**: Select 'I'm not a robot' and complete the verification test.

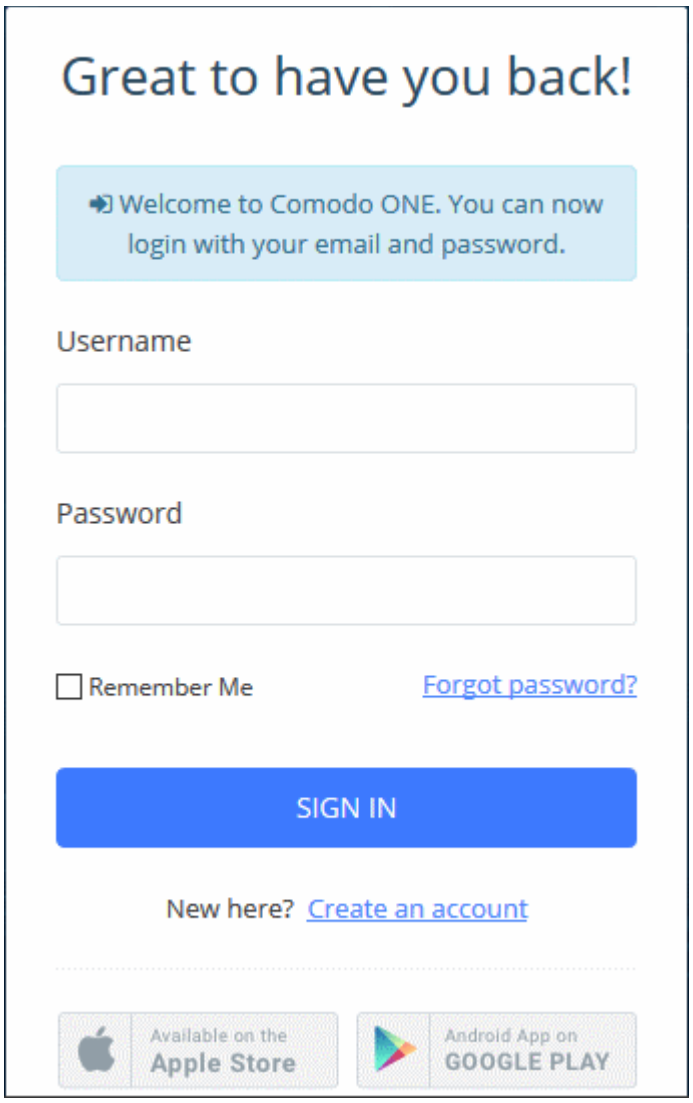
Click 'Get Now for Free'.

- You will receive a confirmation email to verify your account:

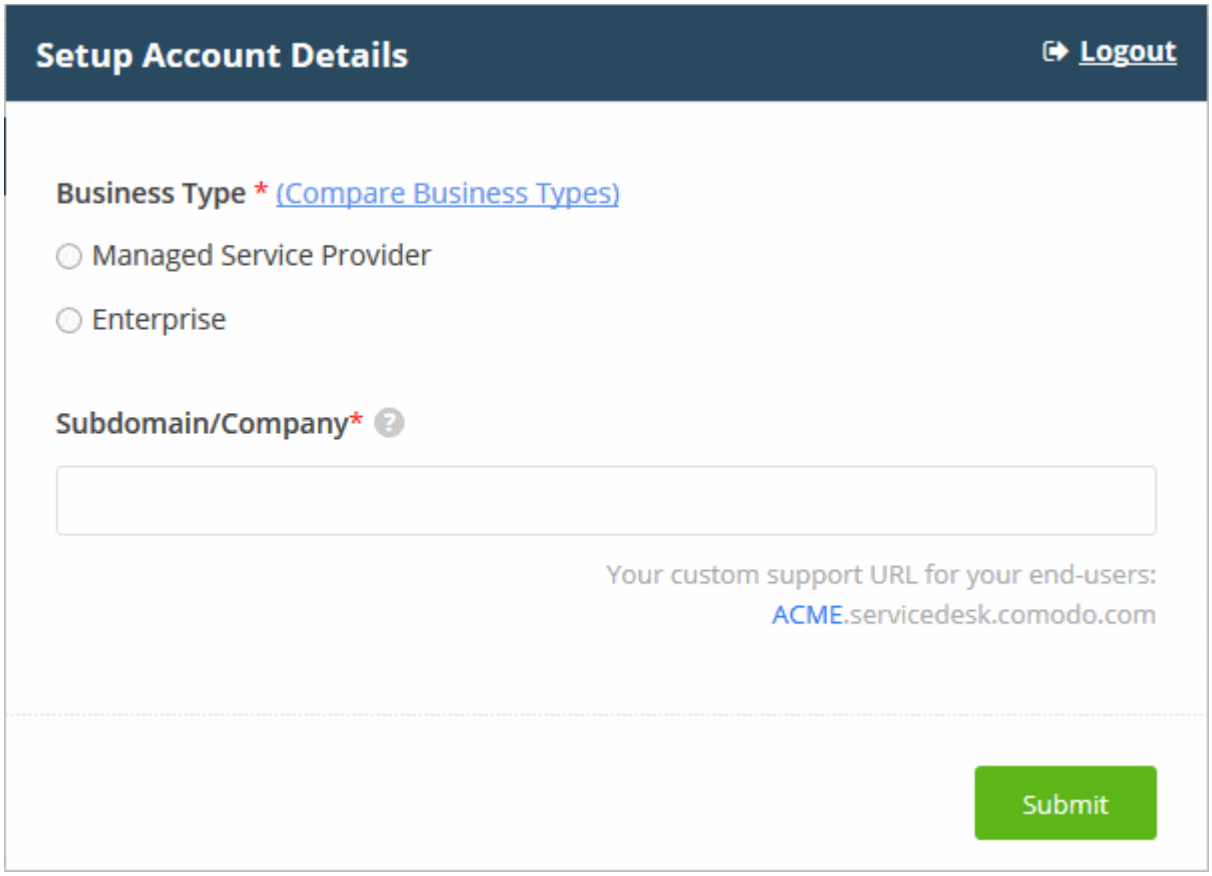


- Click the 'Verify my email' button in the mail to activate your account:

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



- Enter your email address and password and click 'Login'.
- You need to complete account registration after your first-login:



- **Business Type** - This determines which version of Comodo One you will receive. The two versions are 'C1 MSP' and 'C1 Enterprise'. The modules offered with each version are as follows:

Comodo One MSP	Comodo One Enterprise
Modules included in the Comodo One Base package	
Service Desk IT and Security Manager (ITSM) Dome Shield	Service Desk IT and Security Manager (ITSM) Dome Shield
Modules that can be added to the base package	
Stand-alone Patch Management Acronis Backup Comodo Quote Manager cWatch Comodo Dome Standard Comodo CRM Comodo Dome Antispam MSP Comodo Dome Firewall Virtual Appliance	Acronis Backup Comodo Quote Manager cWatch Comodo Dome Standard Comodo CRM Comodo Dome Firewall Cloud Comodo Dome Firewall Virtual Appliance Comodo Dome Data Protection Comodo Dome Antispam

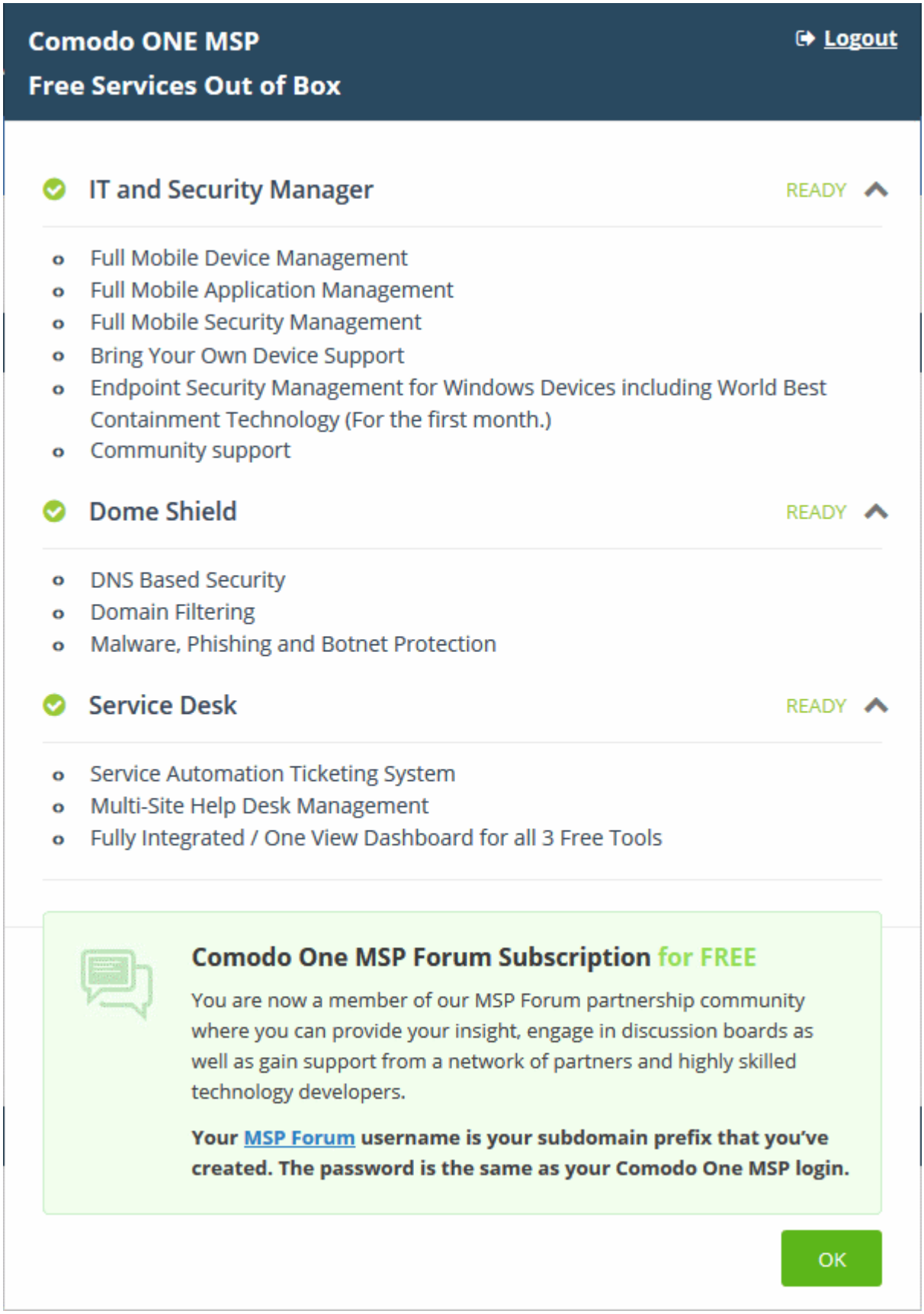
For more details on C1 modules, see https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html.

- **Subdomain** - The sub-domain will form part of the unique URL you use to access the standalone ITSM.

For example, if you enter the sub-domain 'dithers' then you will access ITSM 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 Comodo One Dashboard.
- Click 'Licensed Applications' > 'ITSM' to open the ITSM console
- This account will be given master 'Account Admin' privileges and cannot be deleted. You will be able to create administrators and staff under this account.
- Admins/users who enrolled via C1 can login at **https://one.comodo.com/app/login**
- Admins/users created in ITSM can login at https://<*company name*>.cmdm.comodo.com/

Step 2 - Configure ITSM Communications

In order for ITSM to communicate with enrolled devices, you need to install an Apple Push Notification (APN) certificate and/or a Google Cloud Messaging (GSM) Token on your portal.

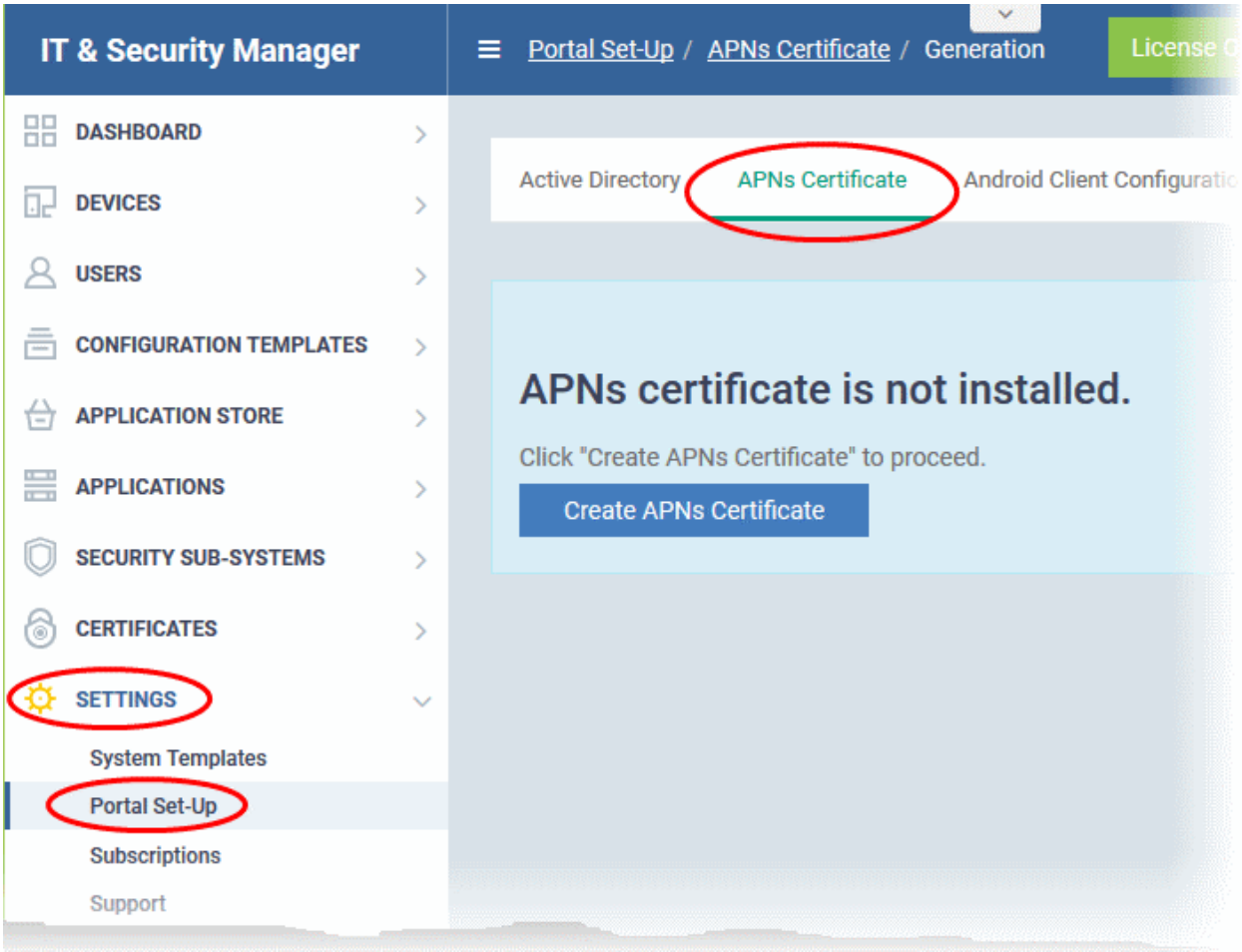
The following sections explain more about:

- Adding APN Certificate
- Adding GCM Token

Adding Apple Push Notification Certificate

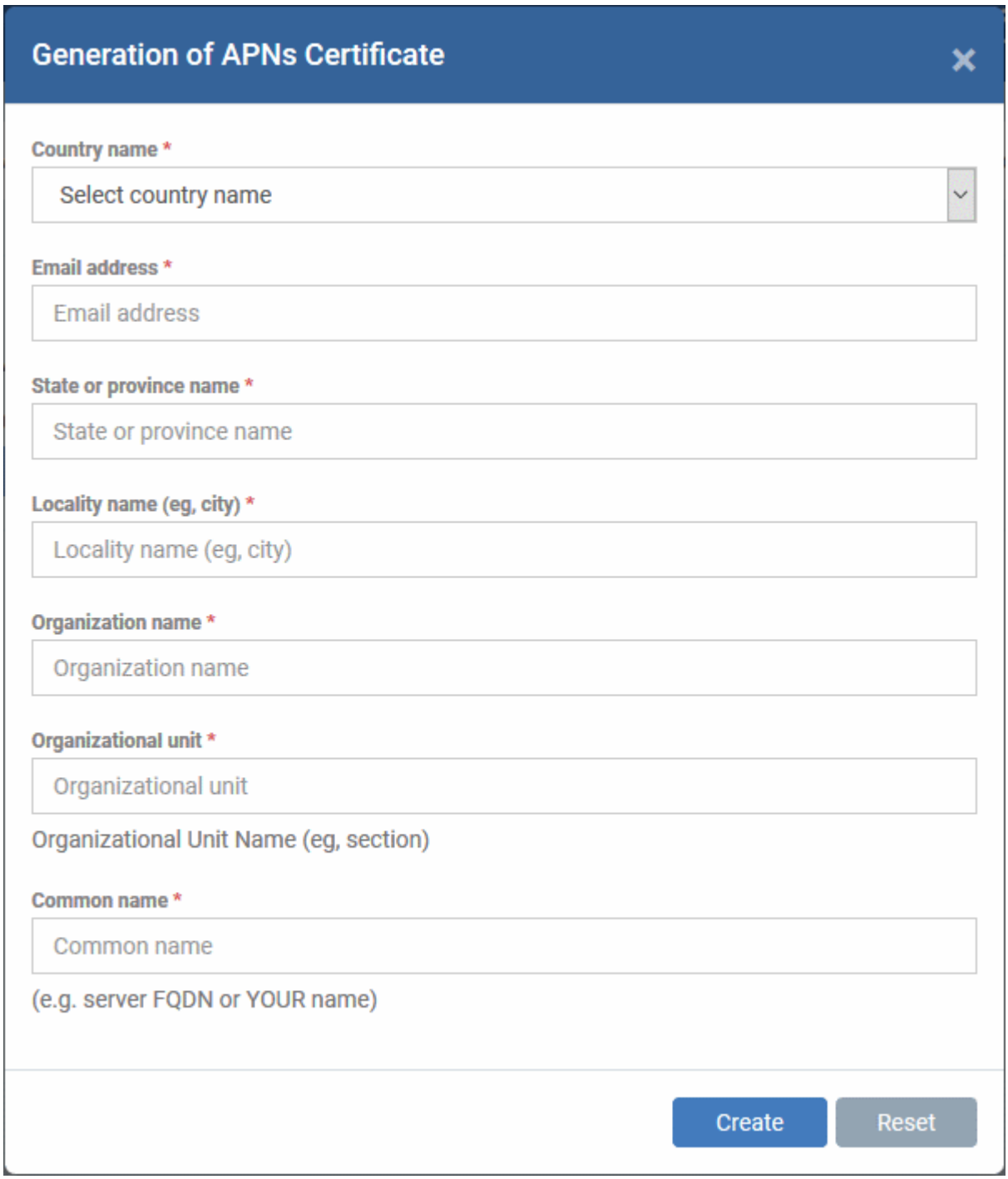
Apple requires an Apple Push Notification (APN) certificate installed on your ITSM portal to facilitate communication with managed iOS devices and Mac OS devices. To obtain and implement an APN certificate and corresponding private key, please follow the steps given below:

- **Step 1- Generate your PLIST**
  - Click 'Settings' on the left and select 'Portal Set-Up'
  - Click 'APNs Certificate' from the top.

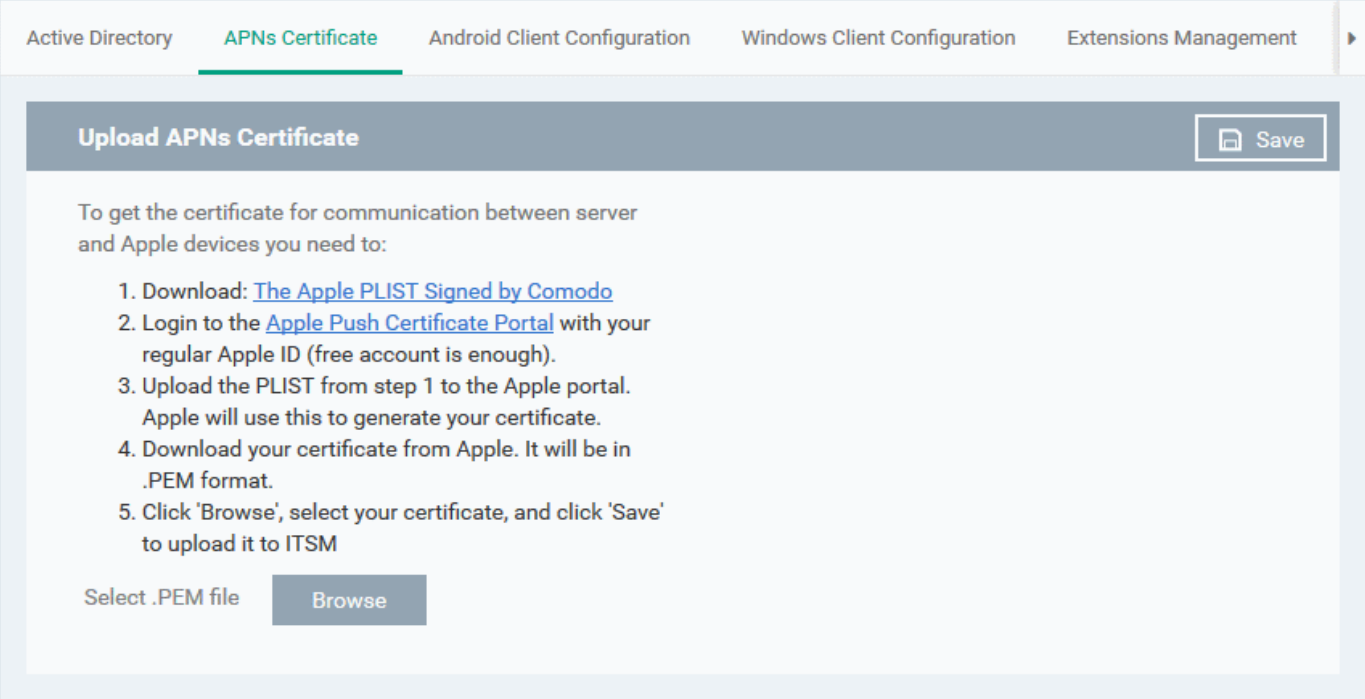


- Click the 'Create APNs Certificate' button to open the APNs application form.

The fields on this form are for generating a Certificate Signing Request (CSR):



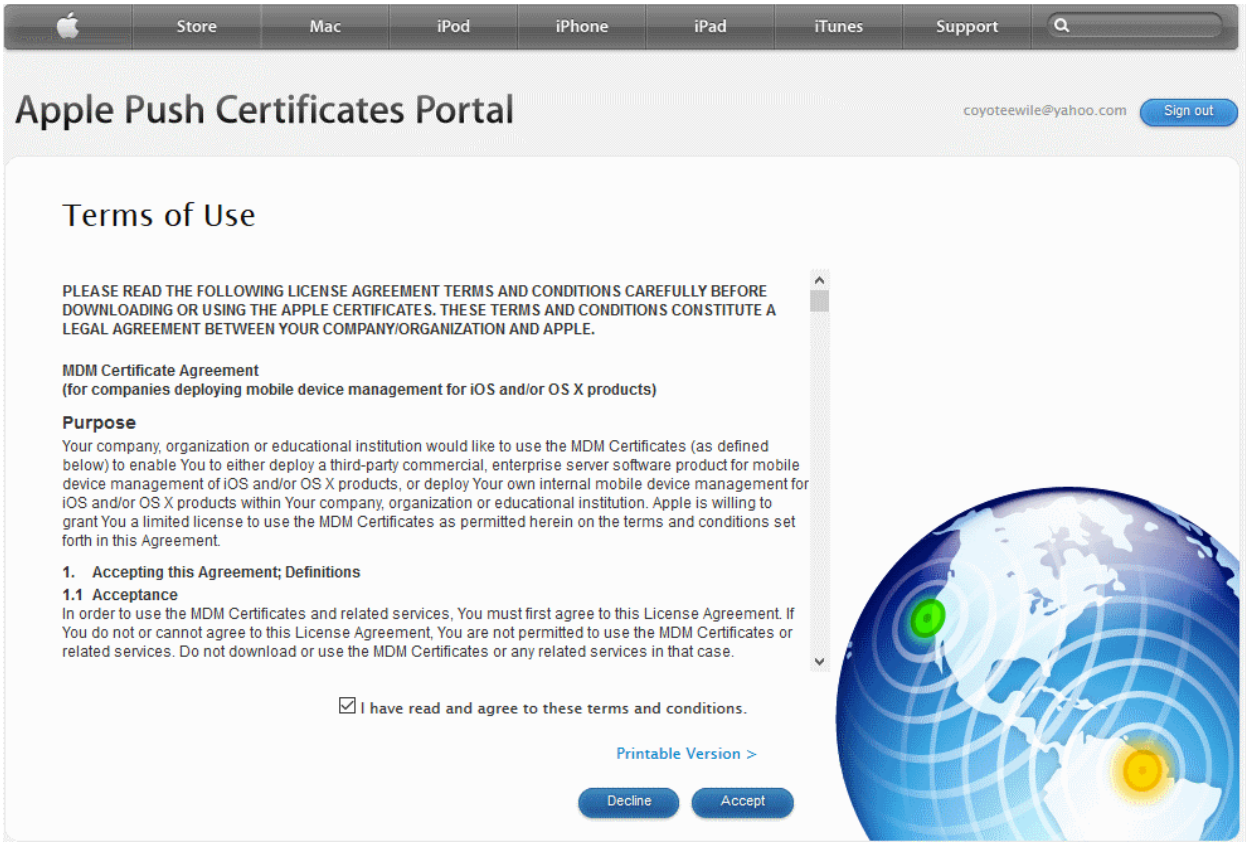
- Complete all fields marked with an asterisk and click 'Create'. This will send a request to Comodo to sign the CSR and generate an Apple PLIST. You will need to submit this to Apple in order to obtain your APN certificate. Usually your request will be fulfilled within seconds and you will be taken to a page which allows you to download the PLIST:



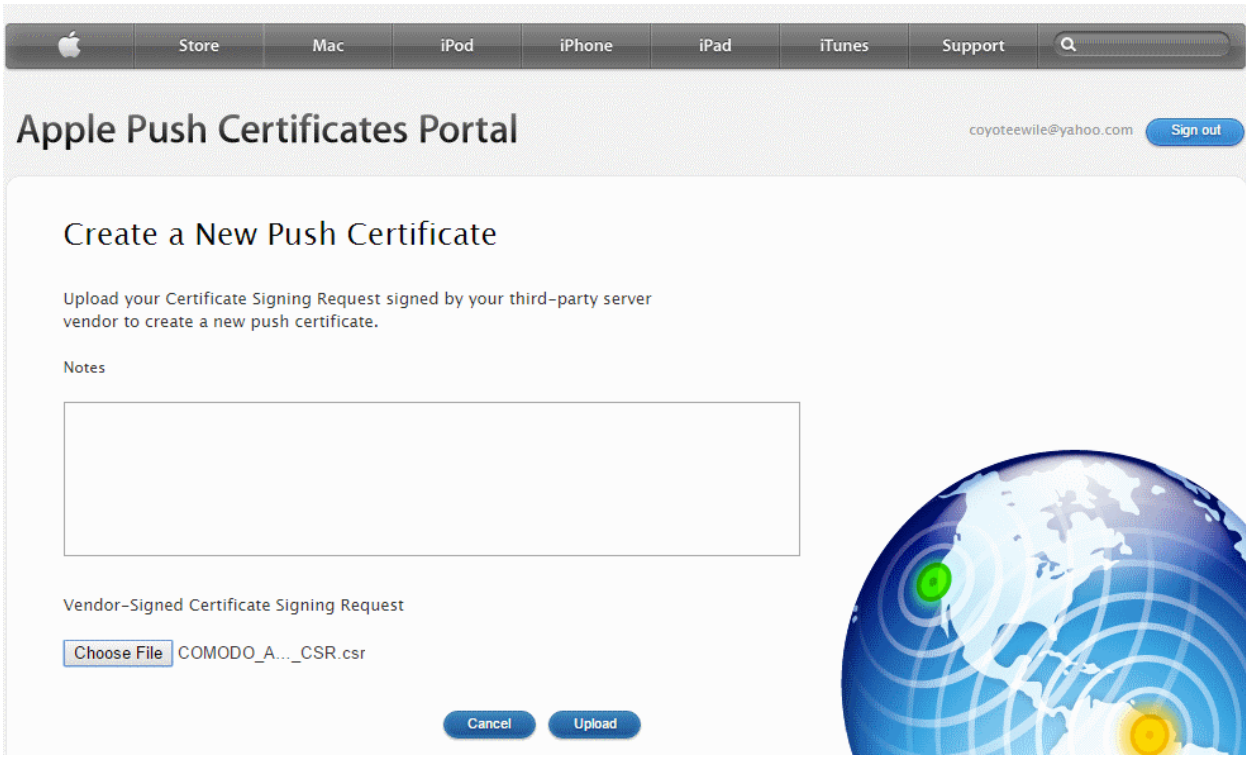
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.

- **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'.

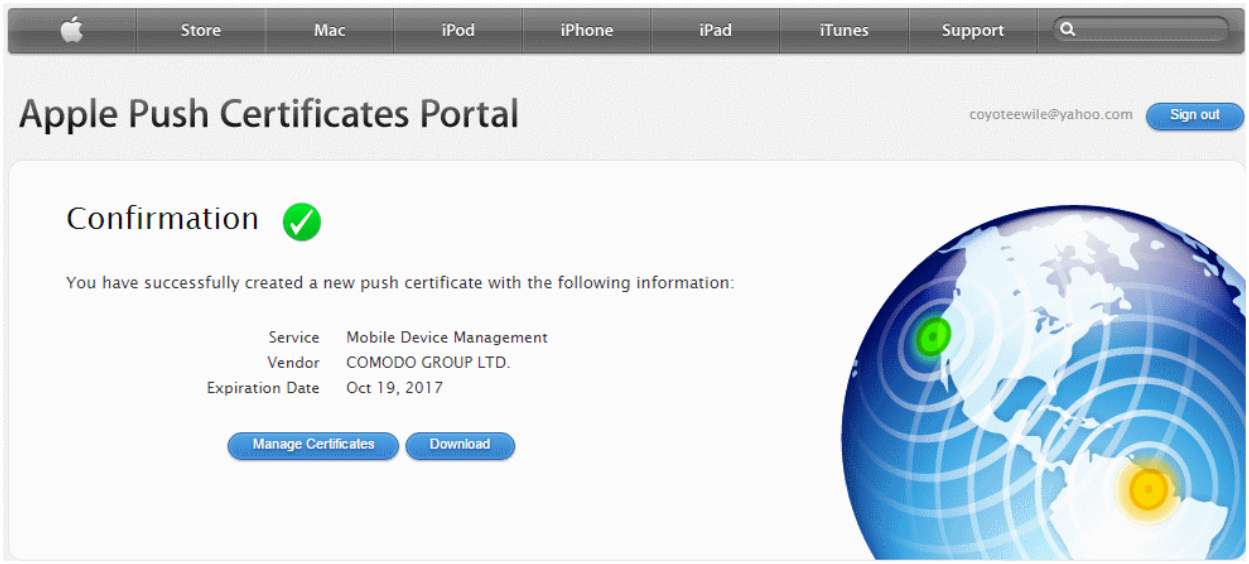
You will need to agree to Apple's EULA to proceed.



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

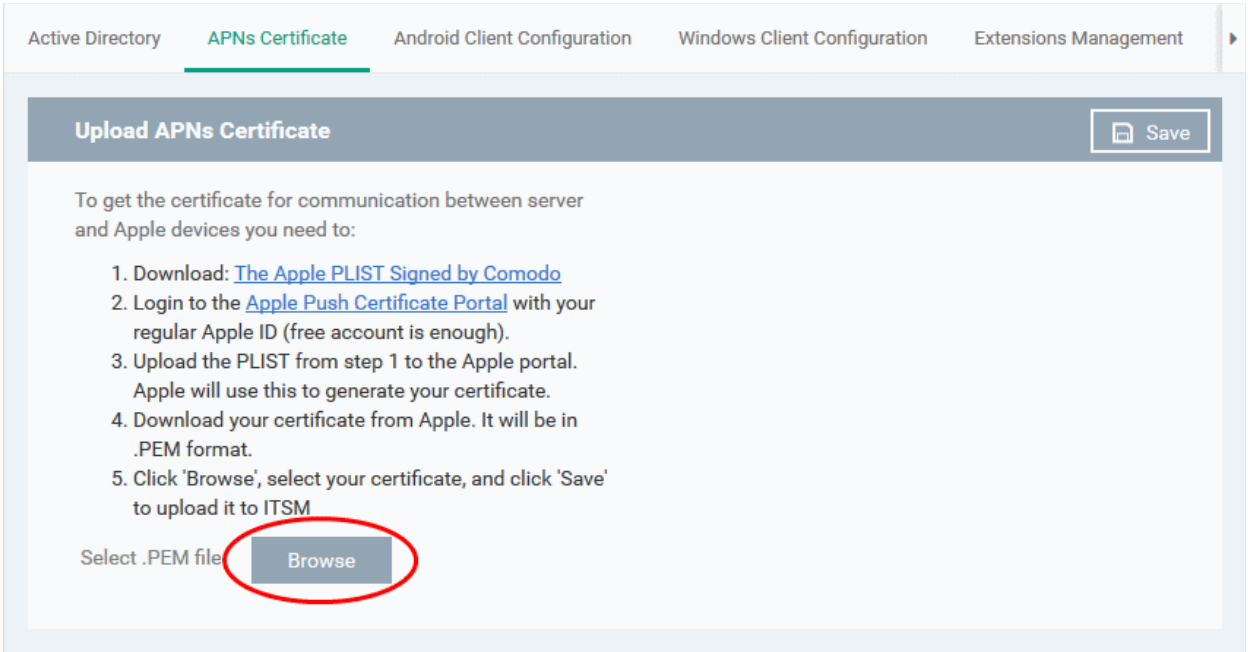


Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



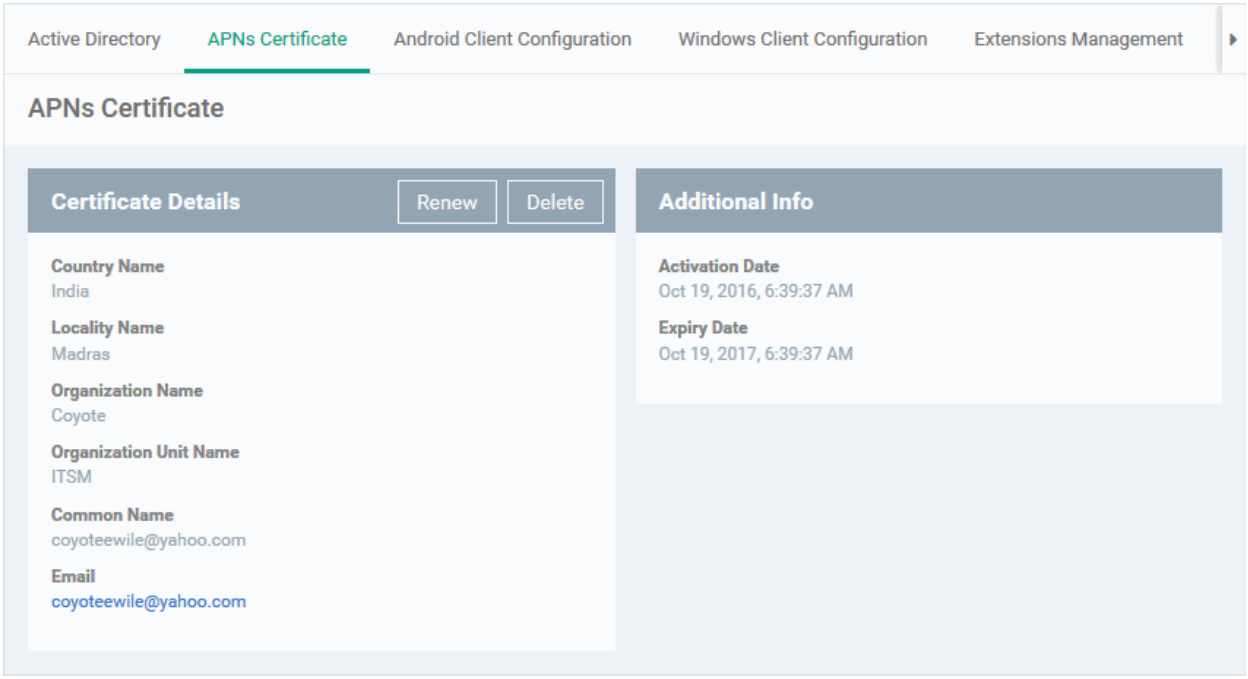
- Click the 'Download' button and save the certificate to a secure location. It will be a .pem file with a name similar to 'MDM_COMODO GROUP LTD._Certificate.pem'

- **Step 3 - Upload your certificate to ITSM**
  - Next, return to the ITSM interface and open the 'APNs Certificate' interface by clicking Settings > Portal Set-Up > APNs Certificate.
  - Click the 'Browse' button, locate your certificate file and select it.



- Click 'Save' to upload your certificate.

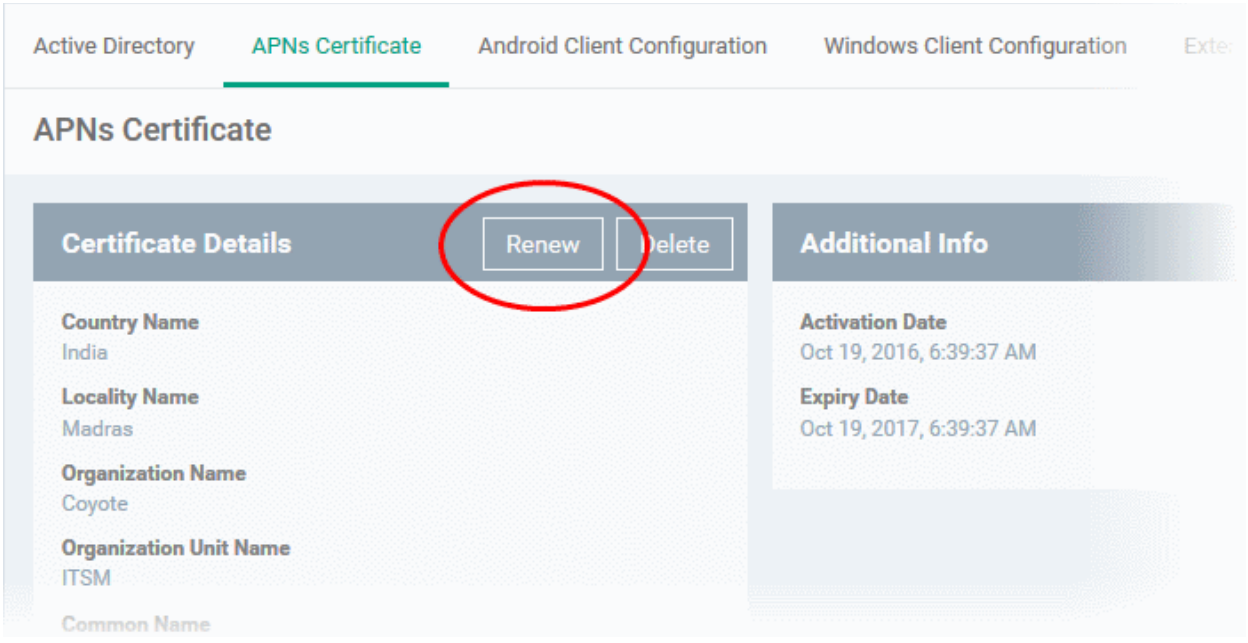
The APNs Certificate details interface will open:



Your ITSM Portal will be now be able to communicate with iOS devices. You can enroll iOS devices and Mac OS devices for management.

The certificate is valid for 365 days. 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 devices to enable the server to communicate with them.

- To renew your APN Certificate, click 'Renew' from the iOS APNs Certificate details interface.



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

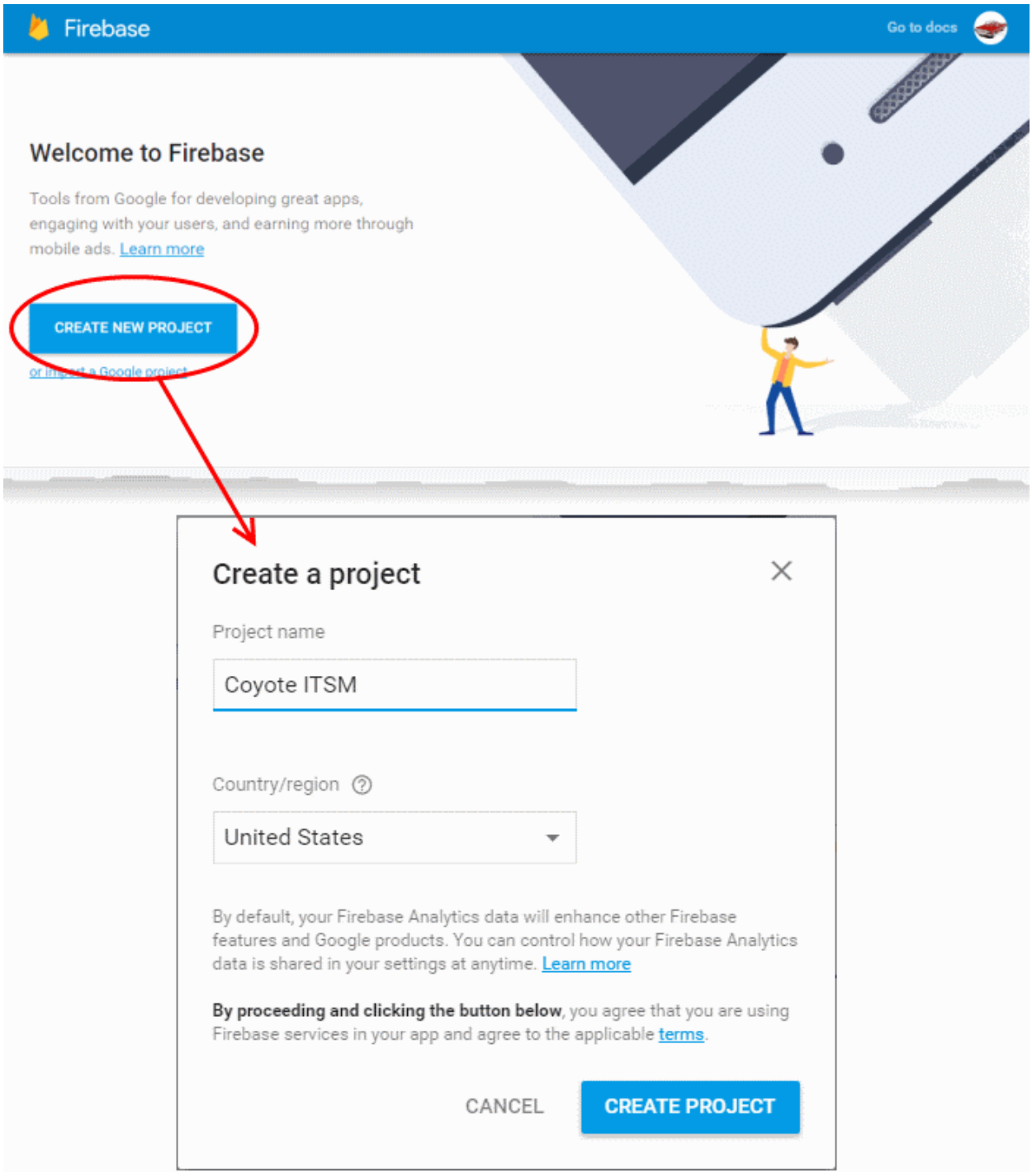
Adding Google Cloud Messaging (GCM) Token

Comodo IT and Security Manager requires a Google Cloud Messaging (GCM) token in order to communicate with Android devices. ITSM ships with a default API token. However, you can also generate a unique Android GCM token for your ITSM portal. To get a token, you must first create a project in the Google Developers console.

Please follow the steps given below to create a project and upload a token.

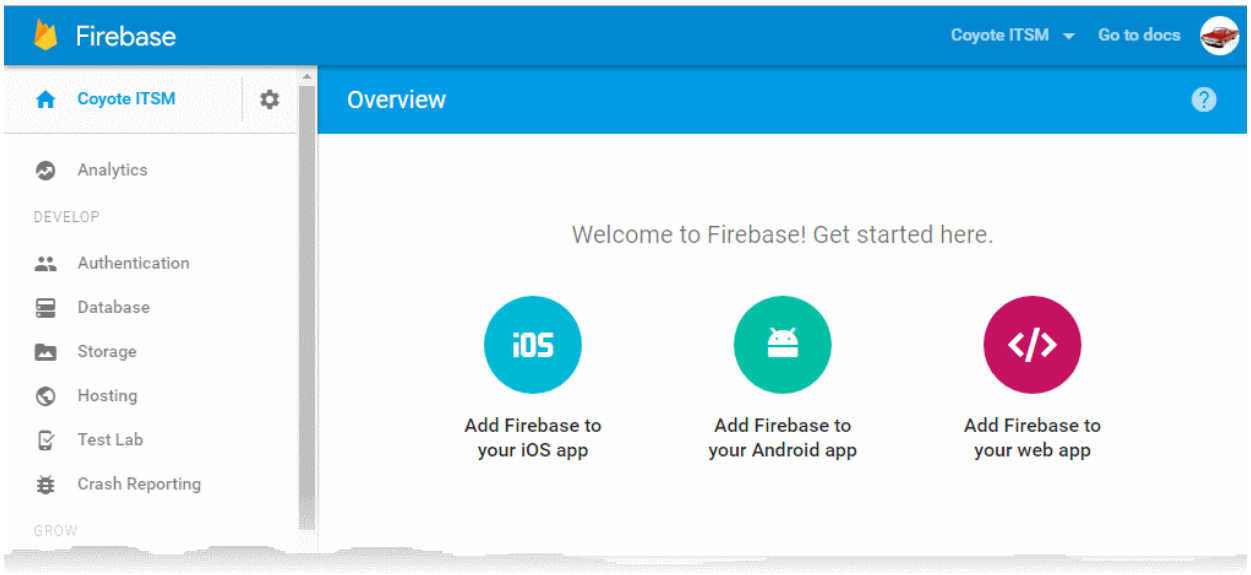
- **Step 1 - Create a New Project**

- Login to the Google Firebase API Console at https://console.firebase.google.com, using your Google account.

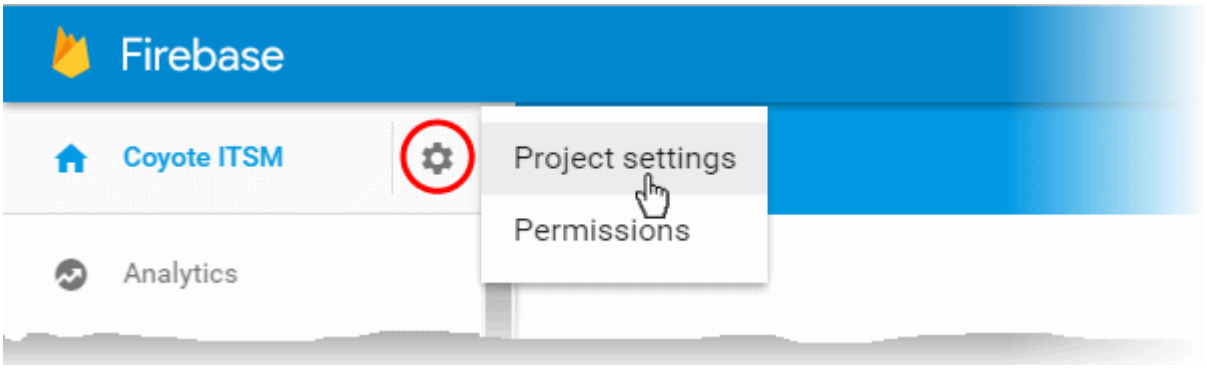


- Click 'Create Project'
- Type a name for the new project in the 'Project Name' field
- Select your country from the 'Country/region' drop-down
- Click 'Create Project'.

Your project will be created and the project dashboard will be displayed.

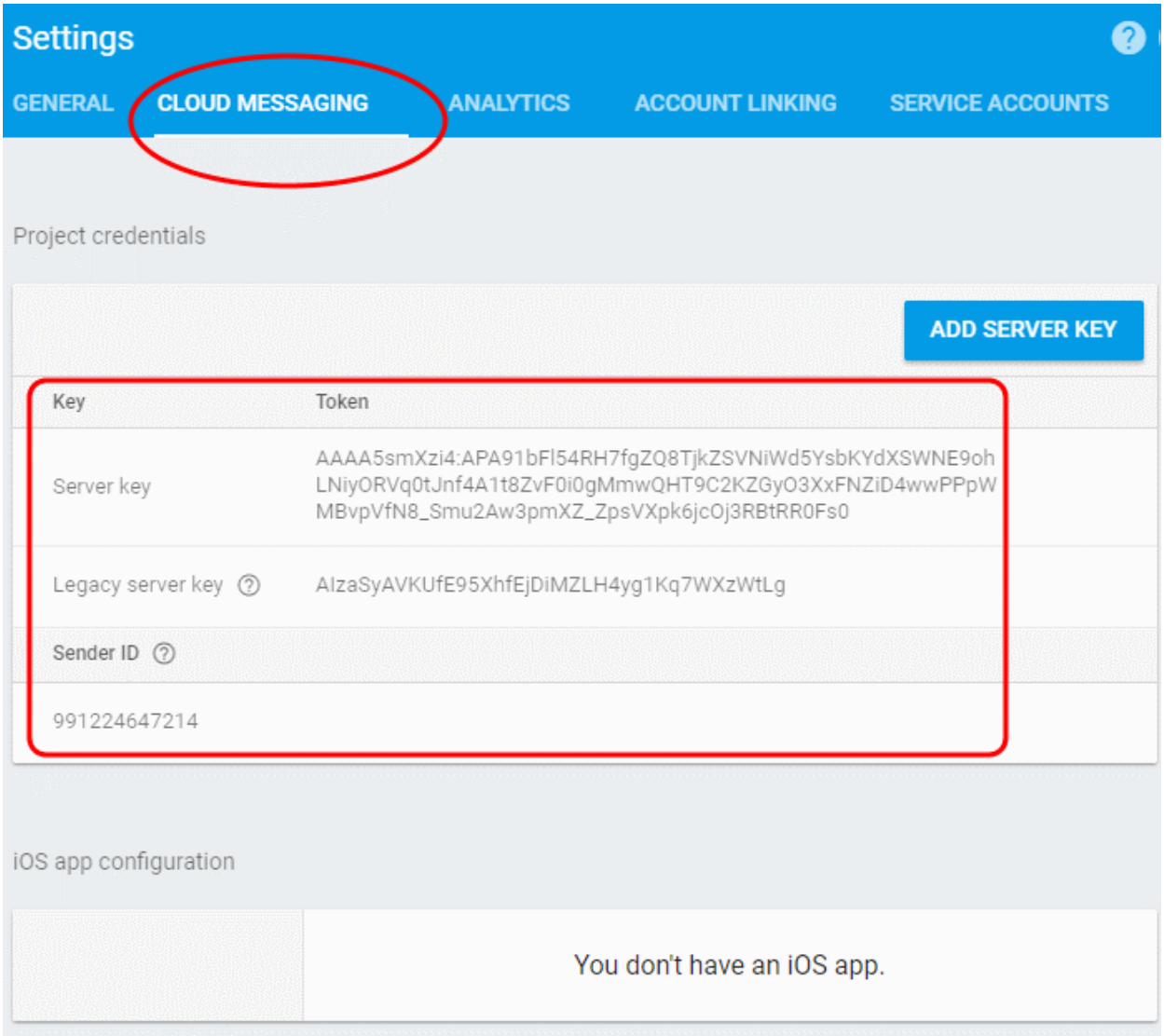


- **Step 2 - Obtain GCM Token and Project number**
  - Click the gear icon beside the project name at the left and choose Project Settings from the options.



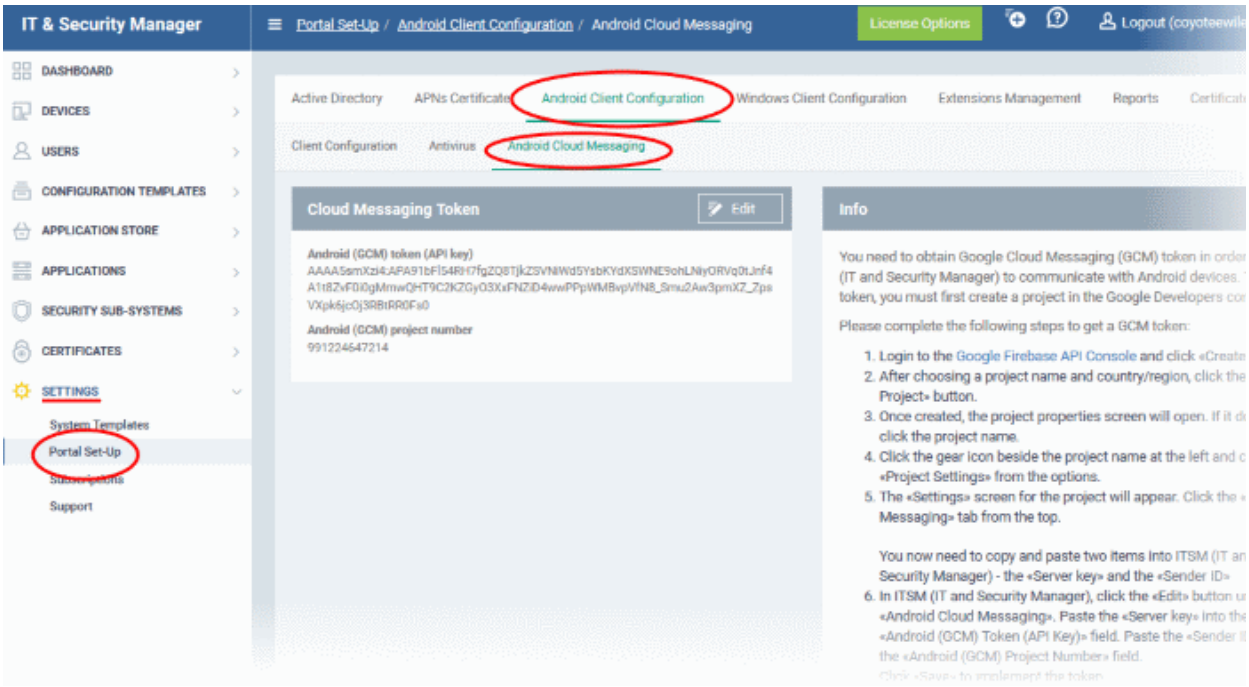
The 'Settings' screen for the project will appear.

- Click the 'Cloud Messaging' tab from the top.



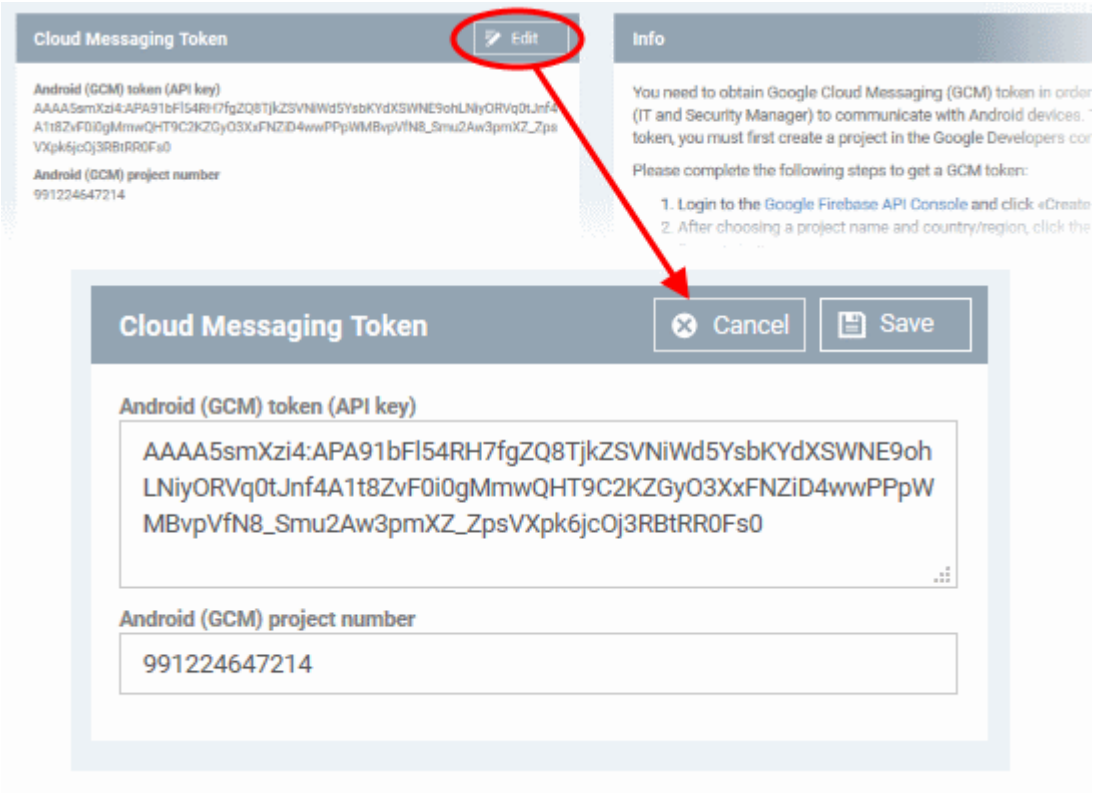
- Note down the Server key and Sender ID in a safe place

- **Step 3 - Enter GCM Token and Project number**
  - Login to ITSM.
  - Click 'Settings' > 'Portal Set-Up' > 'Android Client Configuration' and choose 'Android Cloud Messaging' tab

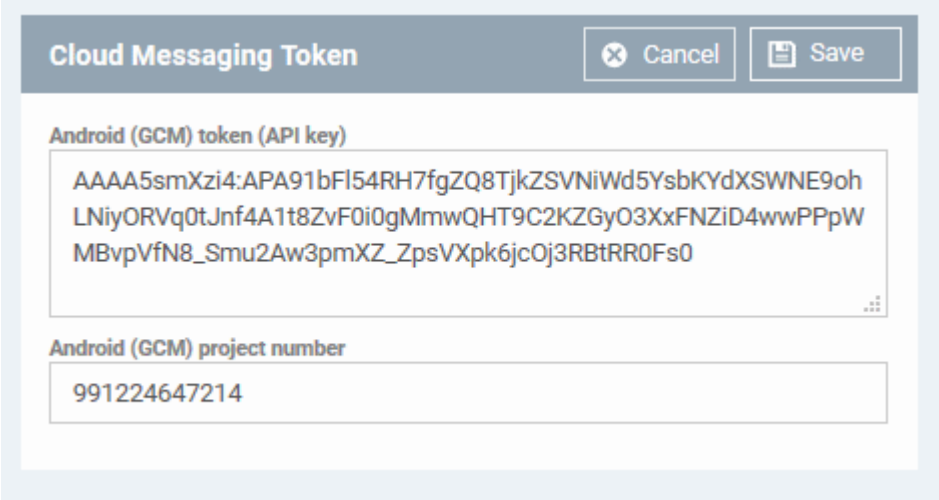


- Click on the edit button

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 will be displayed in the same interface.

Your ITSM Portal will be now be able to communicate with Android devices using the unique token generated for your ITSM portal.

Step 3 - Add Users

Users can be added via the Comodo One console or the ITSM interface.

- Staff added via Comodo One will be available in ITSM and other C1 applications like Service Desk. Users added via ITSM will only be available in ITSM.
- **ITSM Interface**
  - C1 enterprise and ITSM 'stand-alone' customers can add users for a single company
  - C1 MSP customers can create multiple companies and add users/staff to them accordingly. You can group users/devices under different companies as explained in **Step 5 - Create Groups of Devices**.
  - You can also import users in bulk from Active Directory using LDAP. Imported users will be placed into ITSM with the same group structure as used in AD. **Click here** to see the help page on this method.

- **Comodo One Console**
  - C1 Enterprise - Staff created in C1 will be automatically added as users in ITSM.
  - C1 MSP - Staff created in C1 will be automatically added as users in ITSM and will be available for all companies.

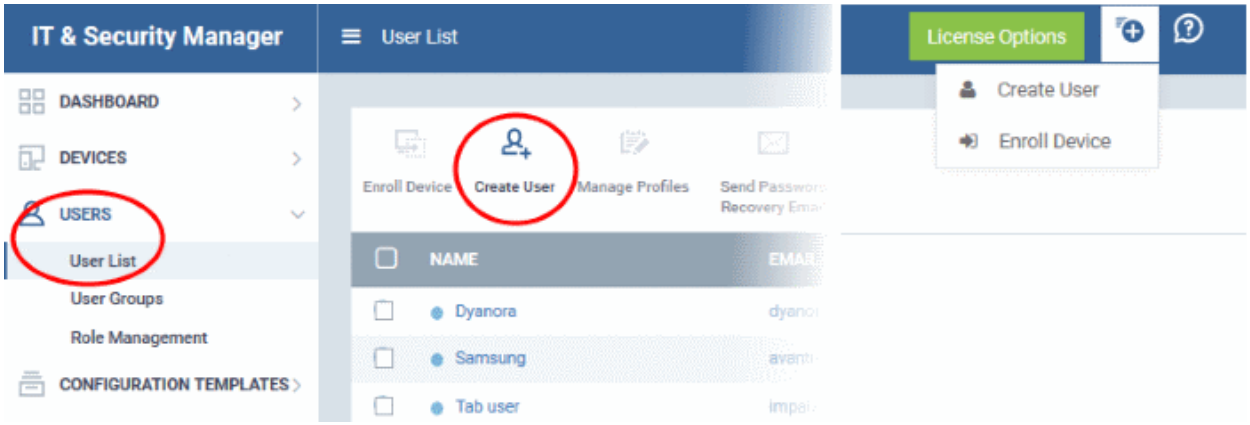
The following section explains how to manually add users via the ITSM interface:

To add a user

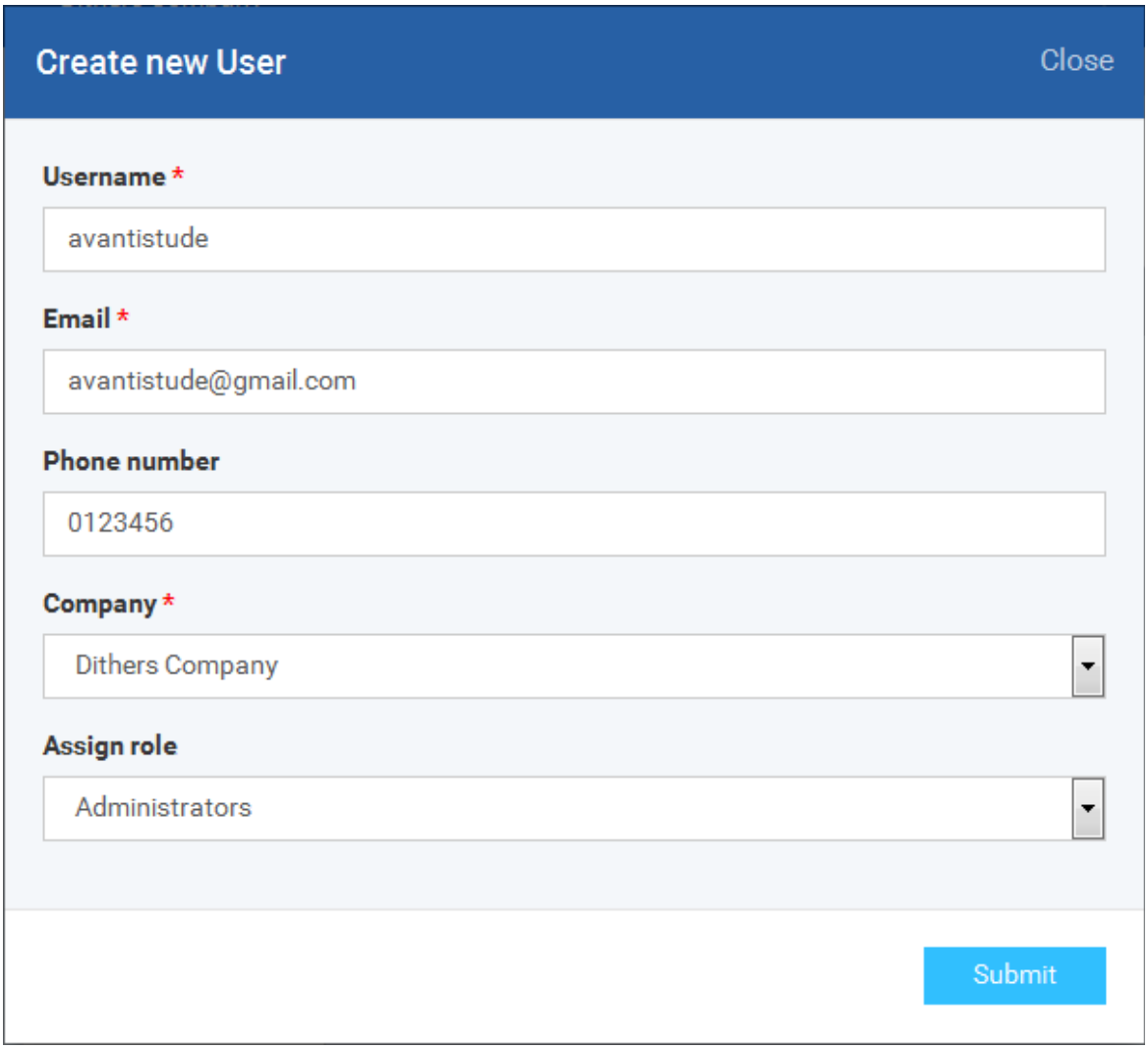
- Click 'Users' on the left then 'User List', then click the 'Create User' button

  or

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



The 'Create new user' form will open.



- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Choose user's company (mandatory)
  - Comodo One MSP Users - The drop-down will list companies added to C1. Choose which company the user should be enrolled under.
  - Comodo One Enterprise and stand-alone ITSM users - Leave the selection as 'Default Company'.
- Choose user role. A 'role' determines user permissions within the ITSM console itself. ITSM ships with four default roles:

- Account Admin - Can login to the ITSM administrative interface and access all management interfaces. This will not be listed here since it will be automatically assigned only to the person who opens a C1 account. This role is not editable.
- Administrators - Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
- Technician - Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
- Users - Can login to the ITSM interface and view only the dashboard part of the application. This role can be edited according to your requirements.

You can create roles with different permission levels via the 'Role Management' screen (click 'User' > Role Management'). You can edit the permissions of existing roles by clicking on the role in the list and add or remove permissions as required. Any new roles you create will become available for selection in the 'Roles' drop-down when creating a new user.

- Click 'Submit' to add the user to ITSM.

The user will be added to list in the 'Users' interface. The user's devices can be enrolled to ITSM for management.

- Repeat the process to add more users.

If you create an administrator then an account activation mail will be sent to their registered email address.

< deleted tip >

Step 4 - Enroll Users' devices

The next step is to enroll user devices for management.

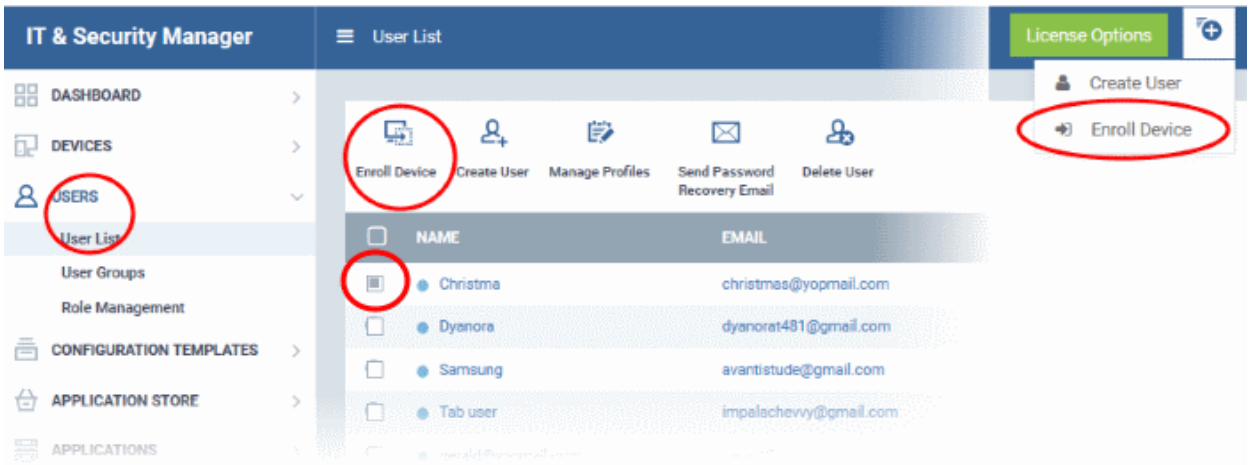
- Each license allows you to enroll up to five mobile devices or one Windows endpoint per user. So 1 user license will be consumed by 5 mobile devices and 1 license will be consumed by a single Windows endpoint.
- If more than 5 devices or 1 endpoint are added for the same user then an additional user license will be consumed. Administrators can purchase additional licenses from the Comodo website.

To enroll devices

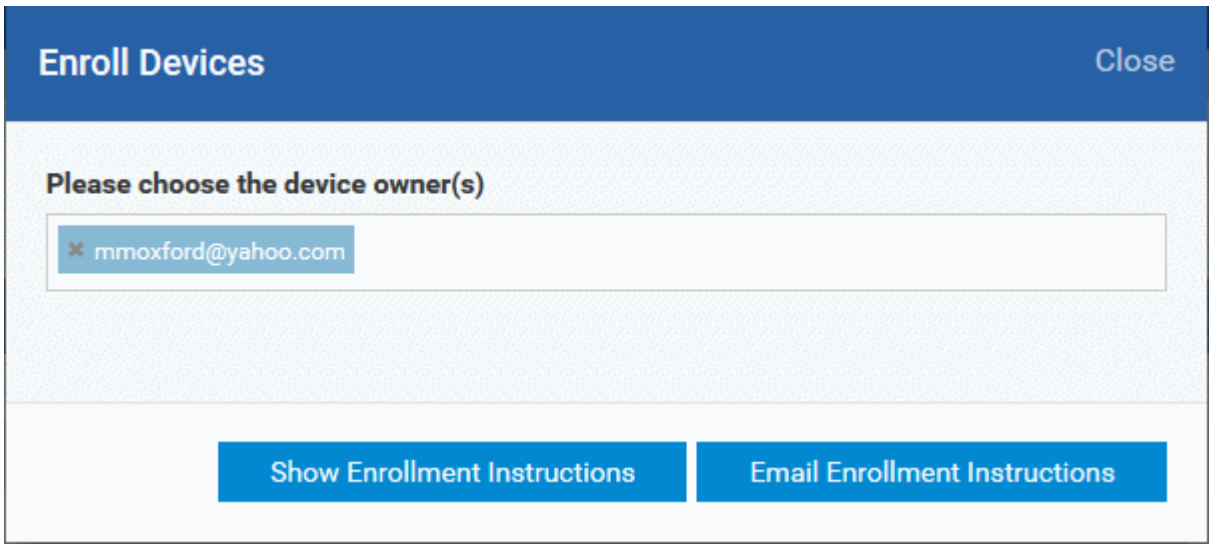
- Click 'Users' then 'User List'
- Select the user(s) whose devices you wish to enroll then click the 'Enroll Device' button above the table

Or

- Click the 'Add' button at the menu bar and choose 'Enroll Device'.

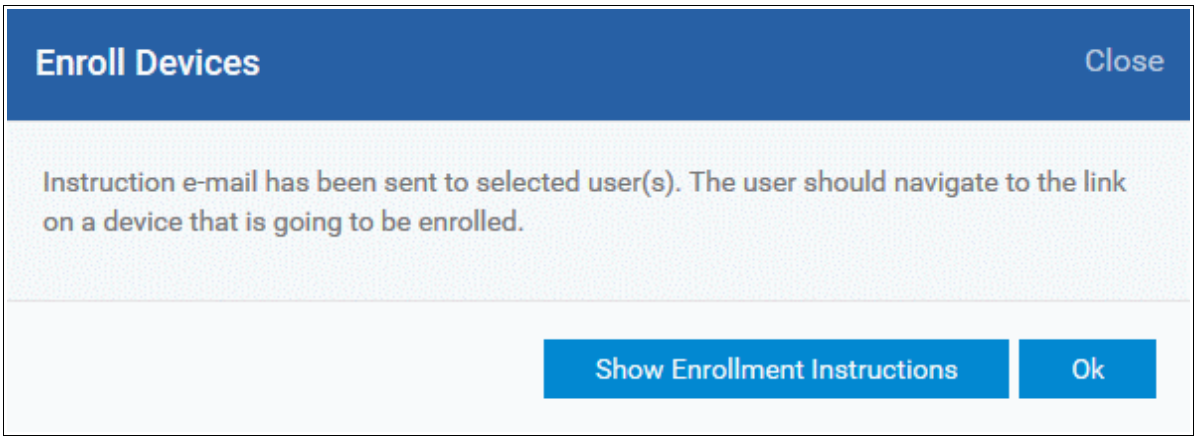


The 'Enroll Devices' dialog will open for the chosen users.

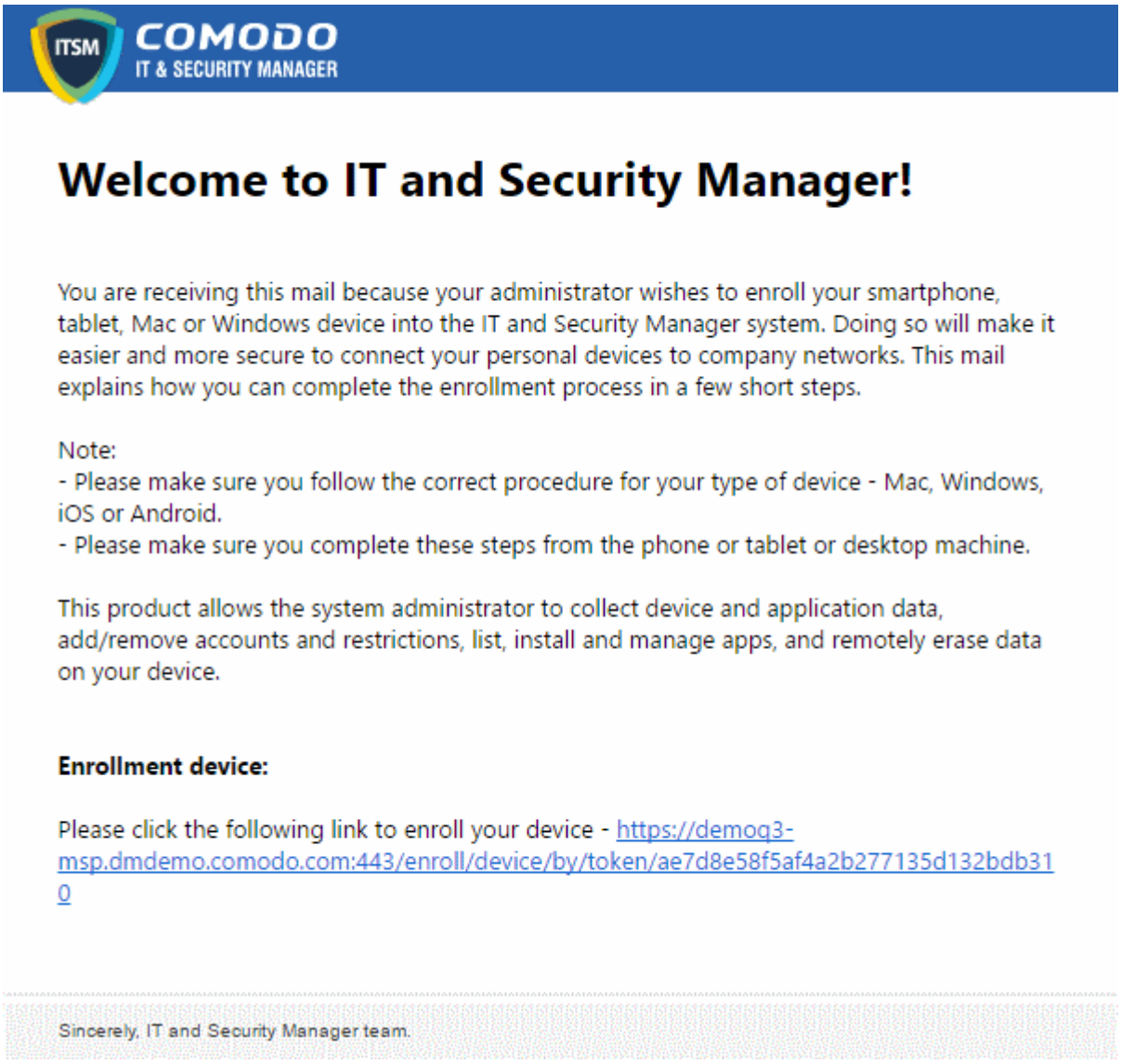


The 'Please choose the device owner(s)' field is pre-populated with any users you selected in the previous step.

- To add more users, start typing first few letters of the username and choose from the results
- If you want enrollment instructions to be displayed in the ITSM interface, click 'Show Enrollment Instructions'. This is useful for administrators attempting to enroll their own devices.
- If you want the enrollment instructions to be sent as an email to users, click 'Email Enrollment Instructions'.
- A confirmation dialog will be displayed.



A device enrollment email will be sent to each user. The email contains instructions that will allow them to enroll their device. An example mail is shown below.



COMODO
IT & SECURITY MANAGER

Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, Mac or Windows device into the IT and Security 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:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

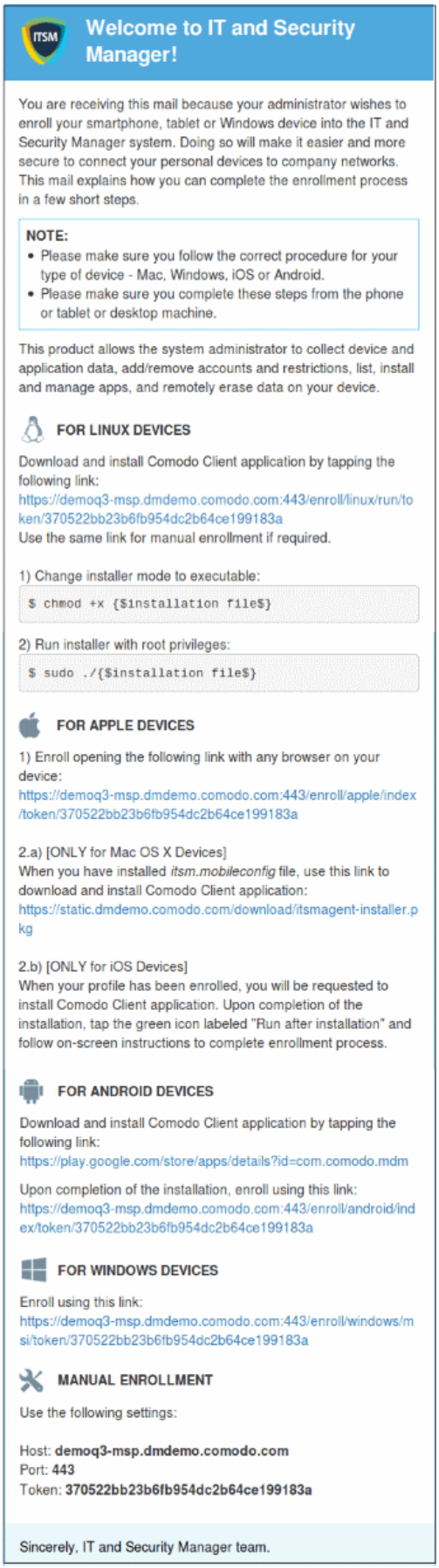
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Enrollment device:

Please click the following link to enroll your device - https://demoq3-msp.dmdemo.comodo.com:443/enroll/device/by/token/ae7d8e58f5af4a2b277135d132bdb310

Sincerely, IT and Security Manager team.

- Clicking the link will take the user to the enrollment page containing the agent/profile download and configuration links.



Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the IT and Security 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:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR LINUX DEVICES

Download and install Comodo Client application by tapping the following link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/linux/run/token/370522bb23b6fb954dc2b64ce199183a
Use the same link for manual enrollment if required.

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

FOR APPLE DEVICES

1) Enroll opening the following link with any browser on your device:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/apple/index/token/370522bb23b6fb954dc2b64ce199183a

2.a) [ONLY for Mac OS X Devices]
When you have installed *itsm.mobileconfig* file, use this link to download and install Comodo Client application:
https://static.dmdemo.comodo.com/download/itsmagent-installer.pkg

2.b) [ONLY for iOS Devices]
When your profile has been enrolled, you will be requested to install Comodo Client application. Upon completion of the installation, tap the green icon labeled "Run after installation" and follow on-screen instructions to complete enrollment process.

FOR ANDROID DEVICES

Download and install Comodo Client application by tapping the following link:
https://play.google.com/store/apps/details?id=com.comodo.mdm

Upon completion of the installation, enroll using this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/android/index/token/370522bb23b6fb954dc2b64ce199183a

FOR WINDOWS DEVICES

Enroll using this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/370522bb23b6fb954dc2b64ce199183a

MANUAL ENROLLMENT

Use the following settings:

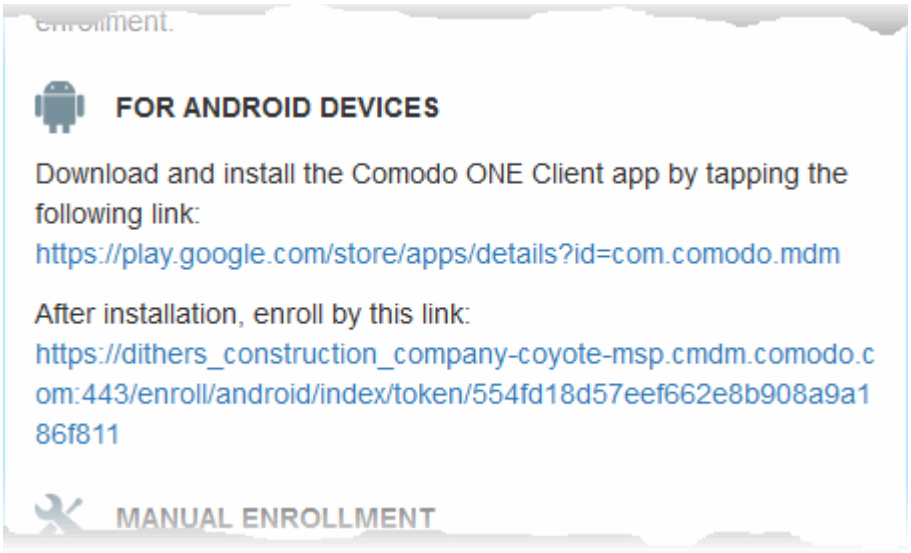
Host: **demoq3-msp.dmdemo.comodo.com**
Port: **443**
Token: **370522bb23b6fb954dc2b64ce199183a**

Sincerely, IT and Security Manager team.

The end-user should open the mail in the device to be enrolled and tap/click the link to view the device enrollment page in the same device.

Enroll Android Devices

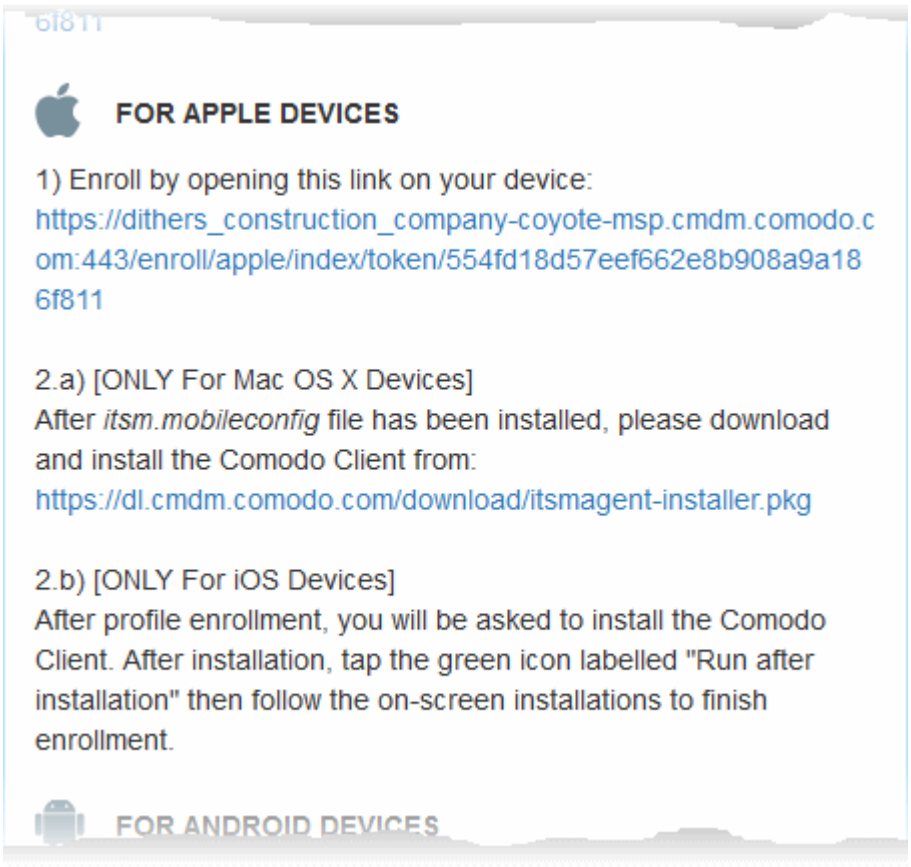
The device enrollment page contains two links under 'FOR ANDROID DEVICES'. The first to download the Android app and the second to enroll the device:



1. User opens the enrollment page on the target device and taps the 1st link to install the ITSM app.
2. After the app has been installed, the user clicks the 2nd link to enroll their device to ITSM. The app will connect to ITSM then request the user to tap 'Activate' to enroll the device.

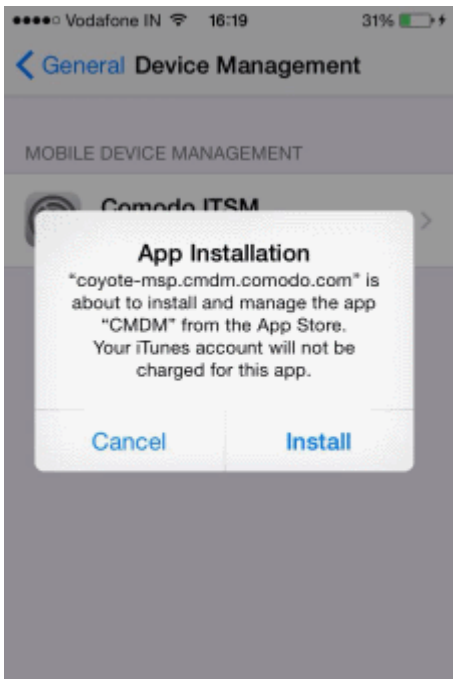
Enroll iPhones, iPods and iPads

The device enrollment page contains an enrollment link under 'FOR APPLE DEVICES'. Users should tap this link to install the ITSM client authentication certificate and ITSM profile.



Note: The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

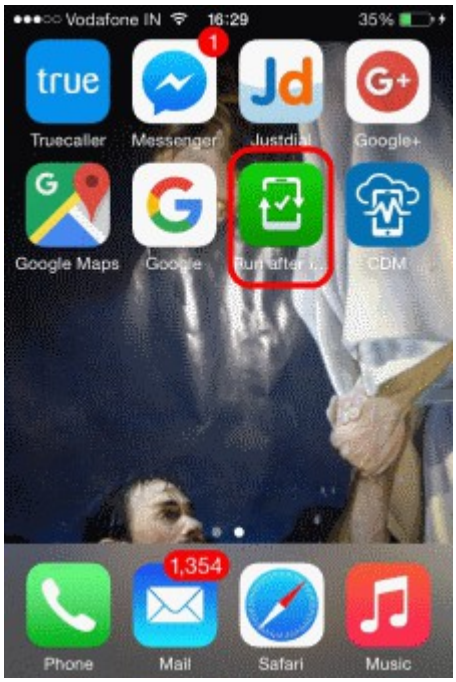
- After the profile has been installed, the client app installation will begin.
- The app is required so that ITSM can manage the remote device:



- The app will be downloaded and installed from the iTunes store. End-users may need to login with their

Apple ID.

- After installation, users should tap the green 'Run After Install' icon on the home screen to complete registration:

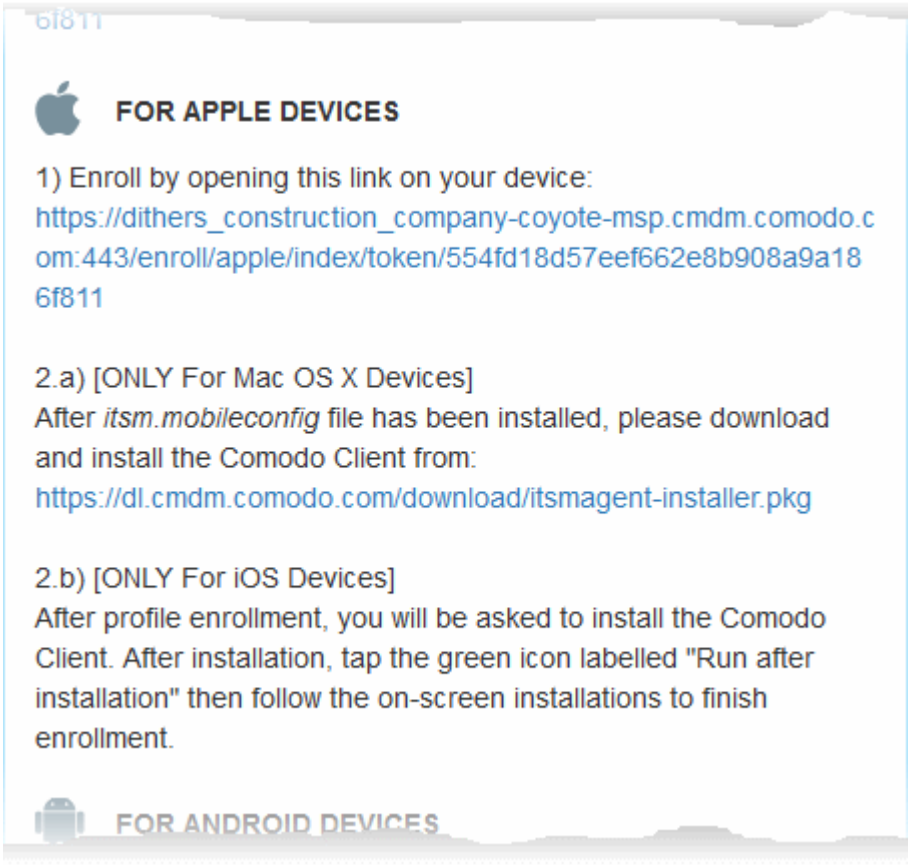


The device will be enrolled and connected to ITSM.

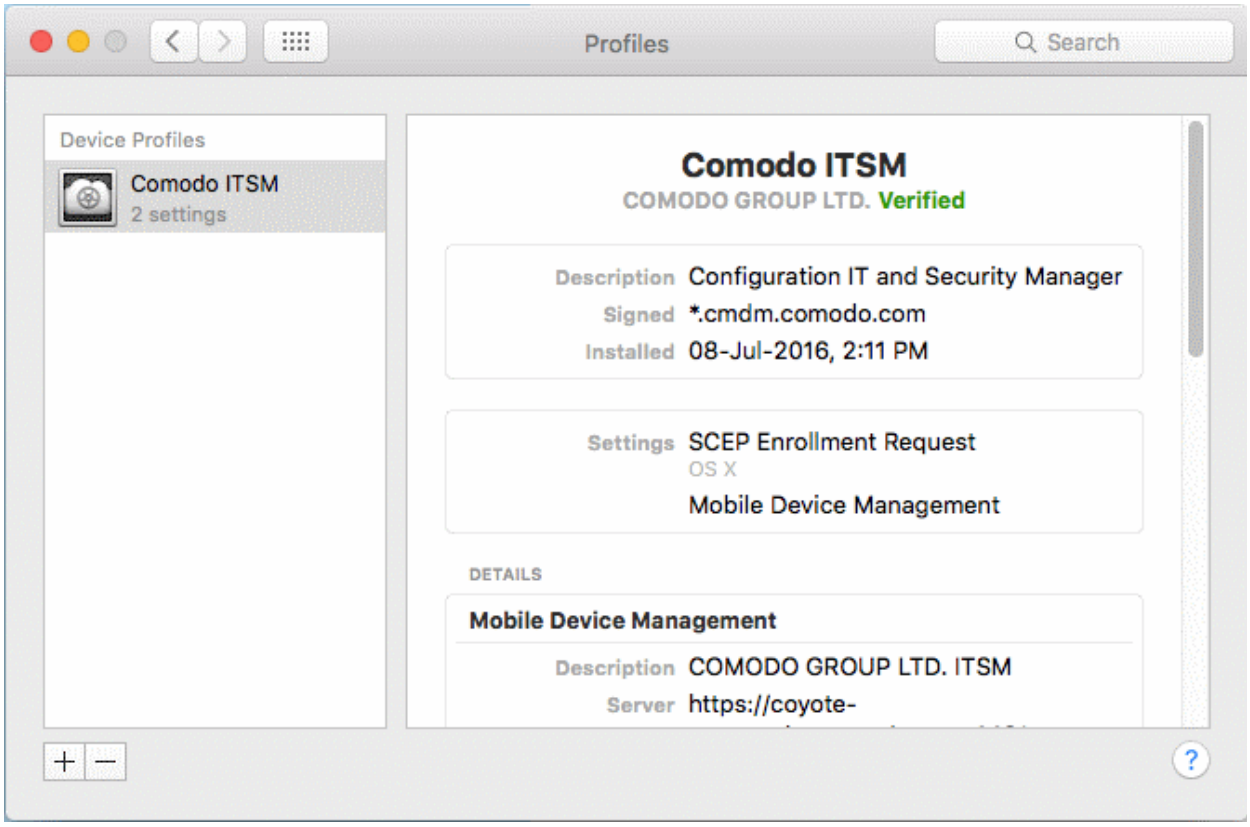
Enroll Mac OS Devices

Step 1 - Install the ITSM Configuration Profile

The device enrollment page contains an enrollment link under 'FOR APPLE DEVICES'. The user clicks this link to download the ITSM profile and install it.



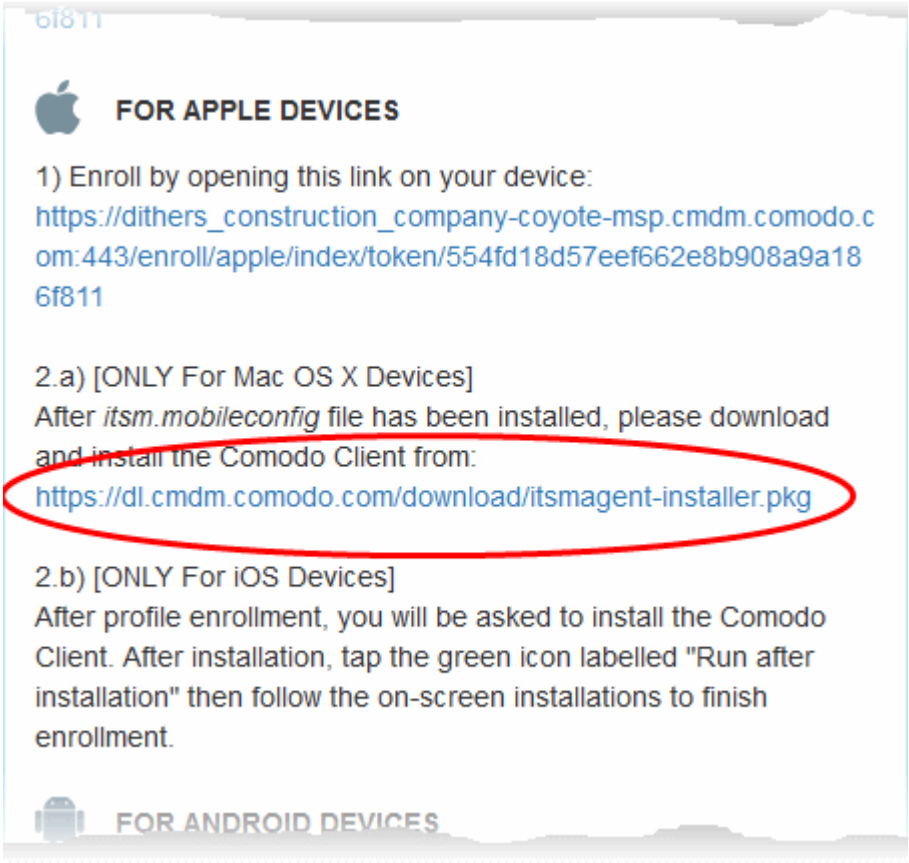
After installation, the profile will be added to the 'Device Profiles' list on the device:



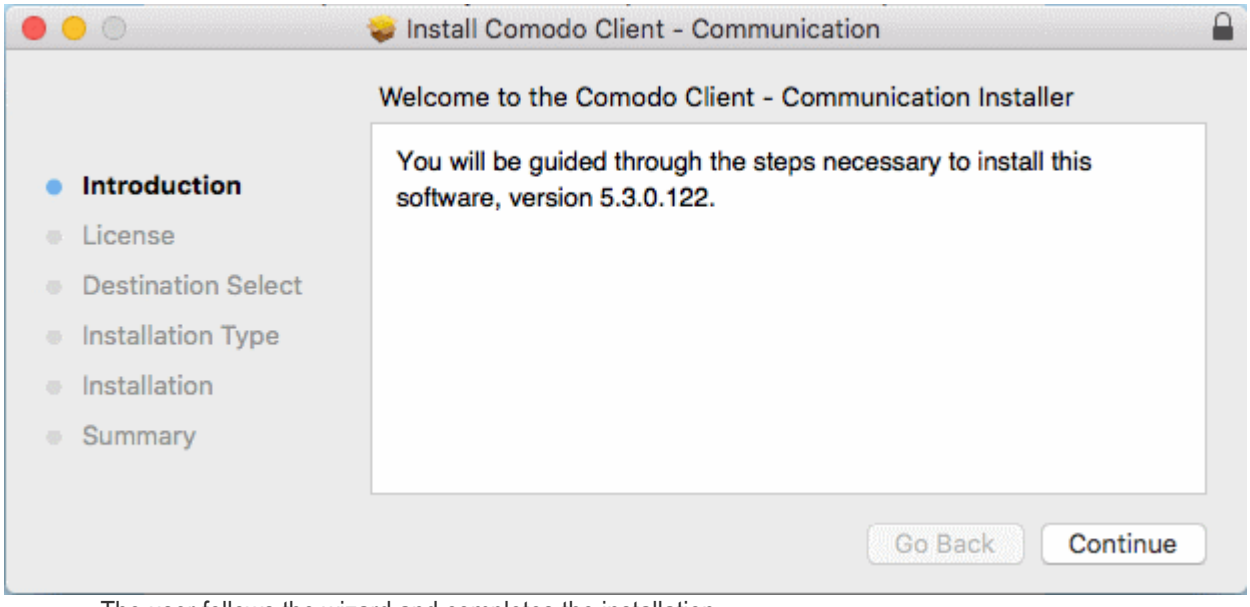
The next step is to install the ITSM agent for connection to the ITSM server and complete the enrollment.

Step 2 - Install ITSM Agent

- Next the user click the link under 'Only For Mac OS X Devices' to download the ITSM agent for Mac.

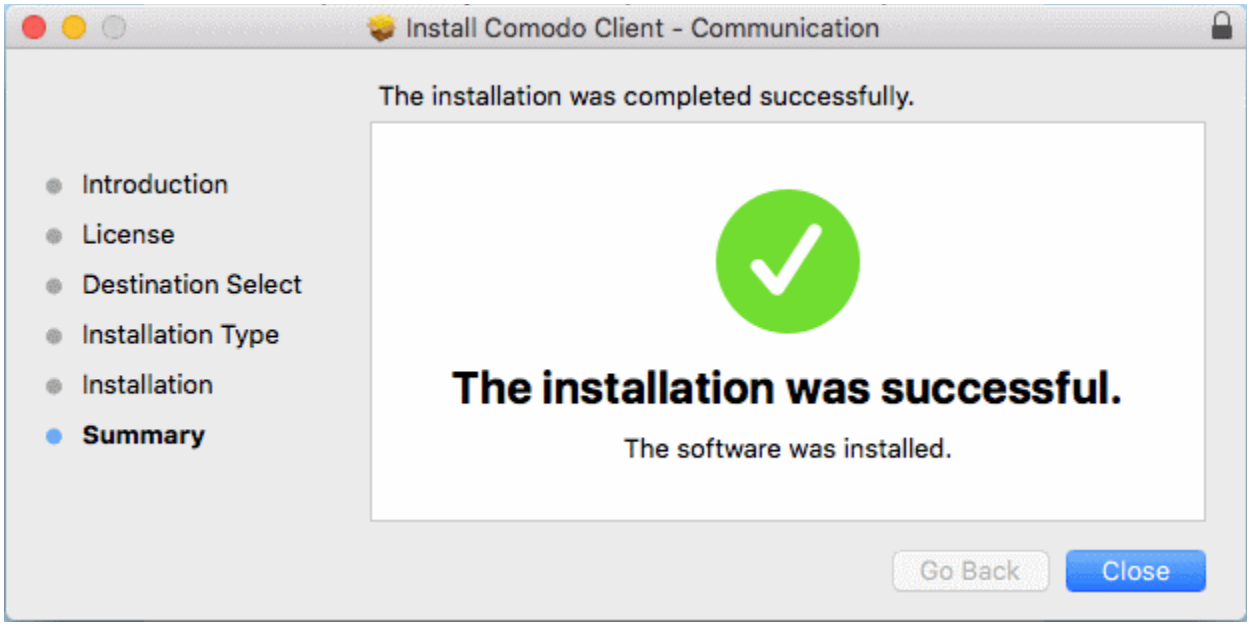


The agent setup package will be downloaded and the installation wizard will start.



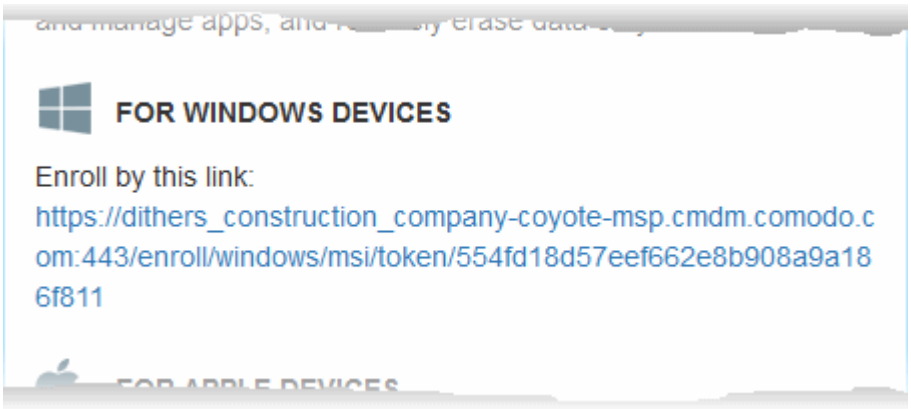
- The user follows the wizard and completes the installation.

Once installation is complete, the agent will start communicating with the ITSM server.



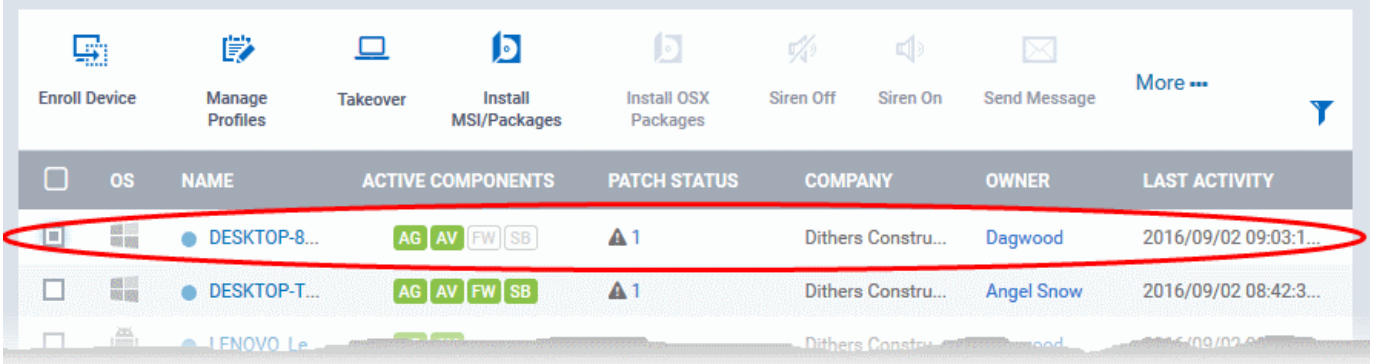
Enroll Windows PCs

The device enrollment page contains a single enrollment link under 'For Windows Devices'.



The user clicks this link to download the ITSM client app. Once installed, the app will enroll the device into ITSM.

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

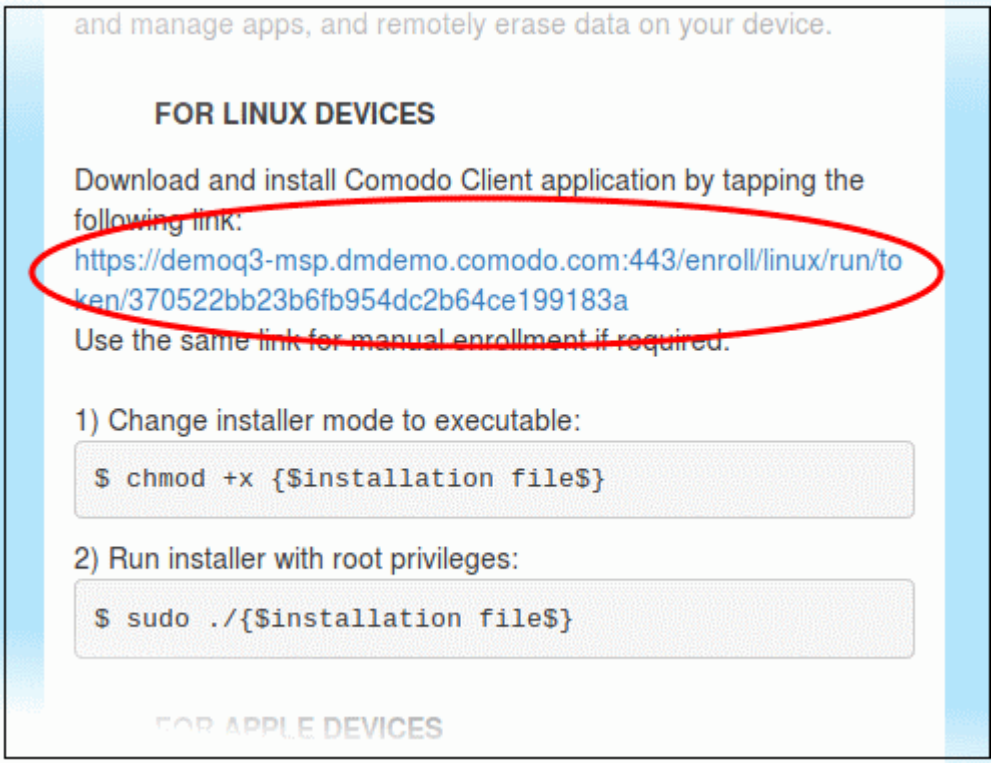


The 'Device List' interface contains a list of all enrolled devices with columns that indicate the device IMEI, owner,

platform and more. The interface allows you to quickly perform remote tasks on selected devices, including device wipe/lock/unlock/shutdown, siren on/off, install apps, password set/reset and more.

Enroll Linux Devices

The device enrollment page contains a single enrollment link under 'For Linux Devices'.



- Click on the enrollment link under 'For Linux Devices' and save the file.

The ITSM agent setup file will be downloaded.

You can install the ITSM agent in your Linux device by first changing installer mode to executable and running the installer with root privileges in the command terminal:

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

   $ chmod +x {$installation file$}

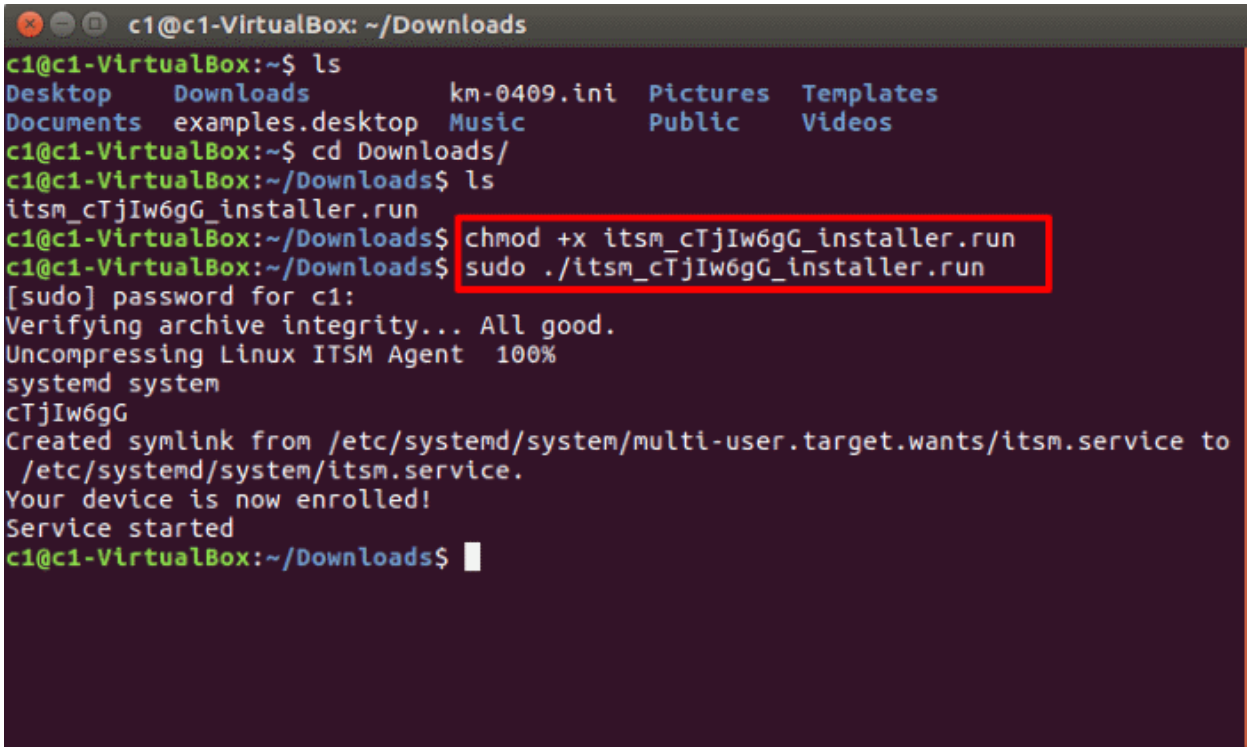
2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run



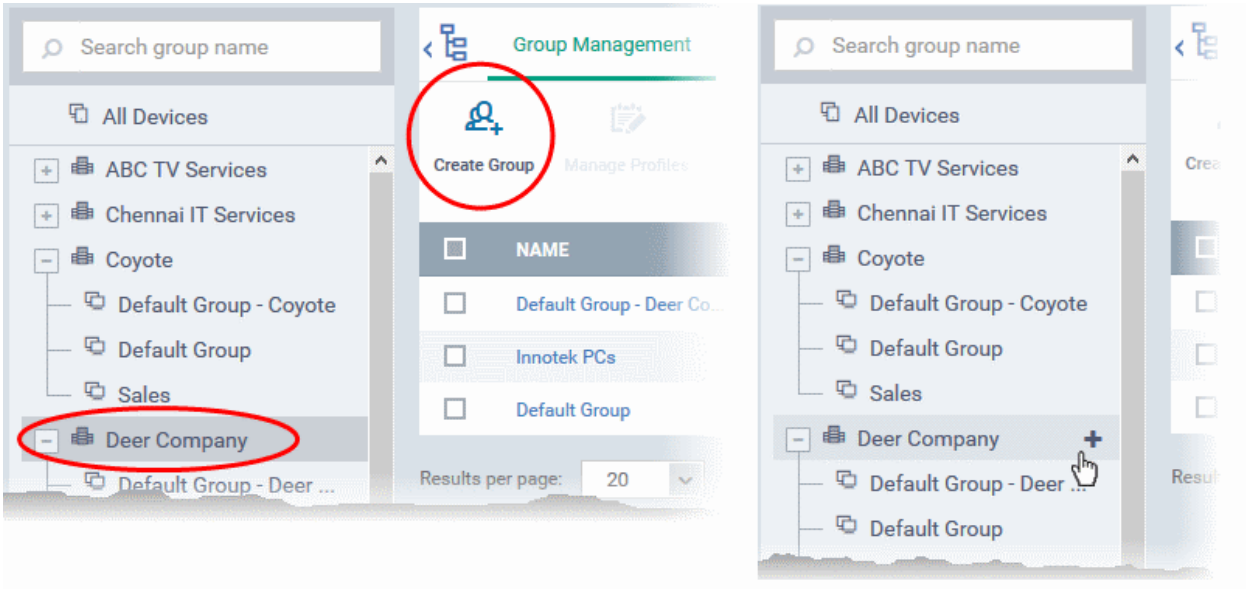
That's it. The Linux device will be enrolled and displayed in the devices list. Currently you can view the device status and online status. Other features such as security client, patch management, procedures and so on will be supported in future ITSM versions.

Step 5 - Create Groups of Devices (optional)

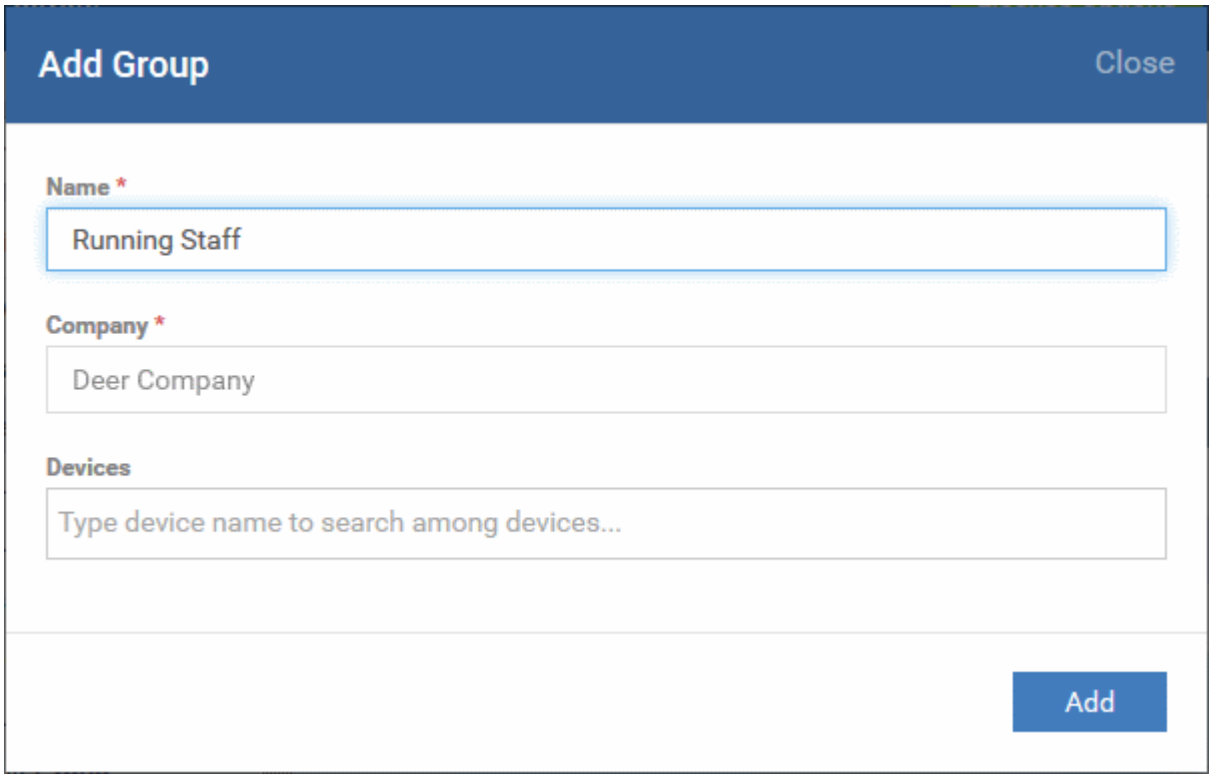
- Device groups let you deploy and manage configuration profiles on large numbers of devices.
- Groups can contain devices of different OS types. OS specific profiles which are applied to a group will be deployed appropriately.
    - C1 MSP customers can create separate device groups for each Company/Organization in their account.
    - C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.

To create a device group

- Click 'Devices' > 'Device List'
- Click the 'Group Management' tab
    - 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 and choose the device(s). Enter a name in the 'Name' field. Type the first few letters of the device name in the Devices field and choose the device from the drop-down that appears. Repeat the process to add more devices.
    - You can also add devices after the group is created. Click on the group name then click the 'Add to Group' button. You can then select devices from the list.
- Click 'OK'. Repeat the process to create more groups.

The next step is to create profiles, which is explained in the next section.

Step 6 - Create Configuration Profiles

- A configuration profile is a collection of settings which can be applied to iOS, Android, Windows or Mac OS

devices.

- Devices must have been enrolled to ITSM before a profile can be applied to them.
- Each profile allows you to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.
- You can designate a profile as 'Default'. Default profiles are automatically applied to newly enrolled devices. There are default profiles for all supported operating systems (Windows, Mac, iOS, Android).
- If no custom profile (based on user and user group) is specified, then the default profile(s) will be auto-applied to a device immediately after enrollment.

Multiple profiles can be created to cater to the different security and access requirements of devices in your network.

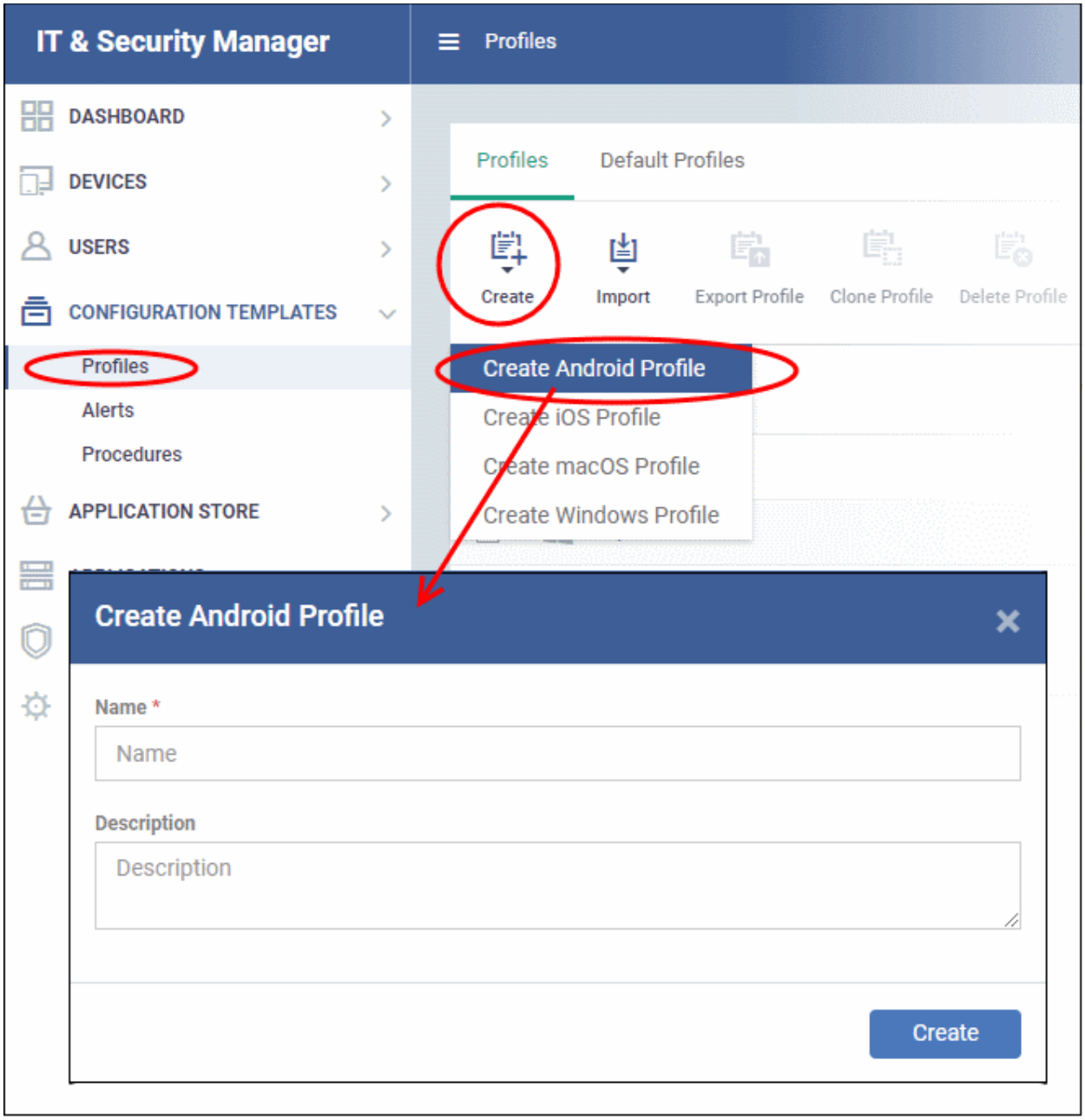
Profiles are applied at the time a device connects to the network. Profile settings will remain in effect until such time as the ITSM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

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

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

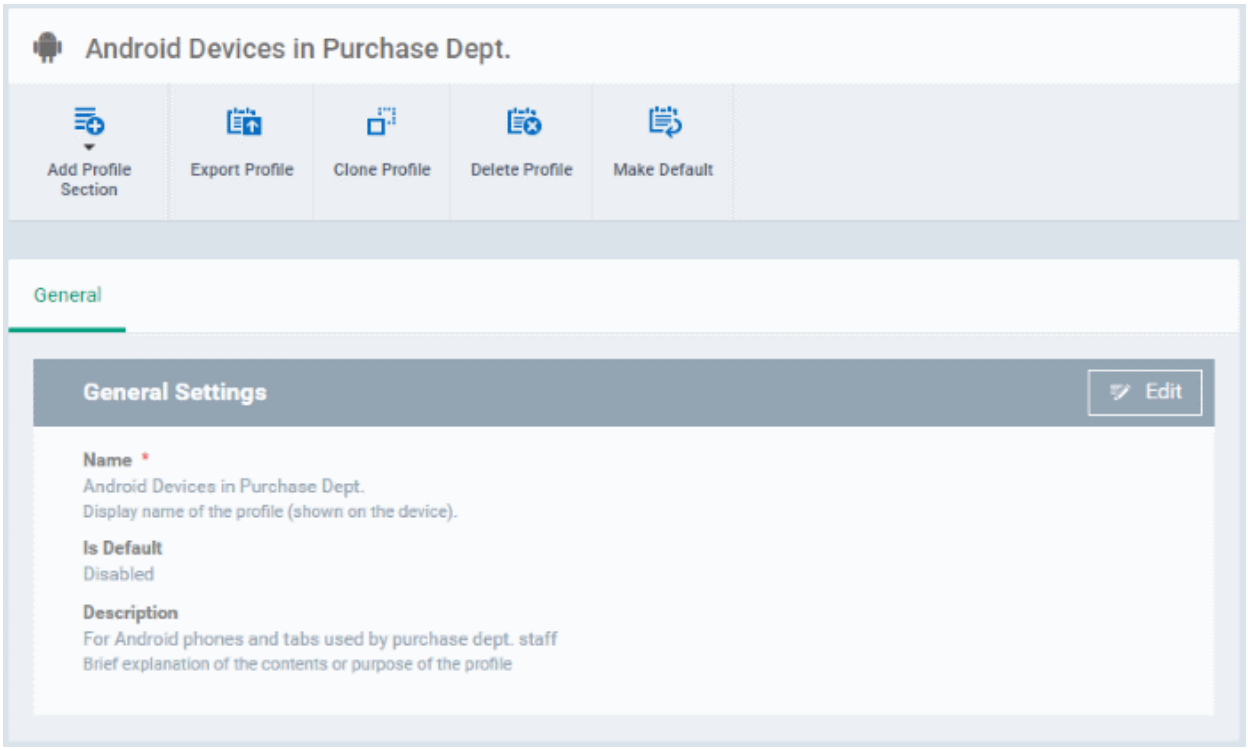
To create an Android Profile

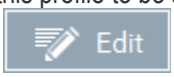
- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then choose 'Create Android Profile'.



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

The profile will be created and the 'General Settings' for the profile will be displayed.

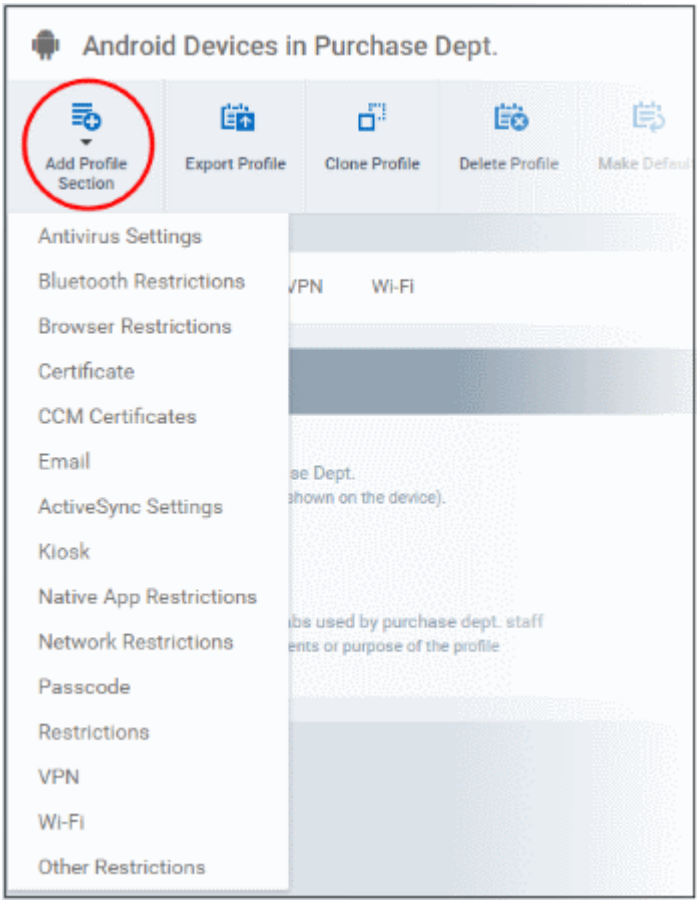


- If you want this profile to be a default policy, click the 'make default' button at the top. Alternatively, click the 'Edit' button 

on the top 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 and select the component from the list that you want to include for the profile



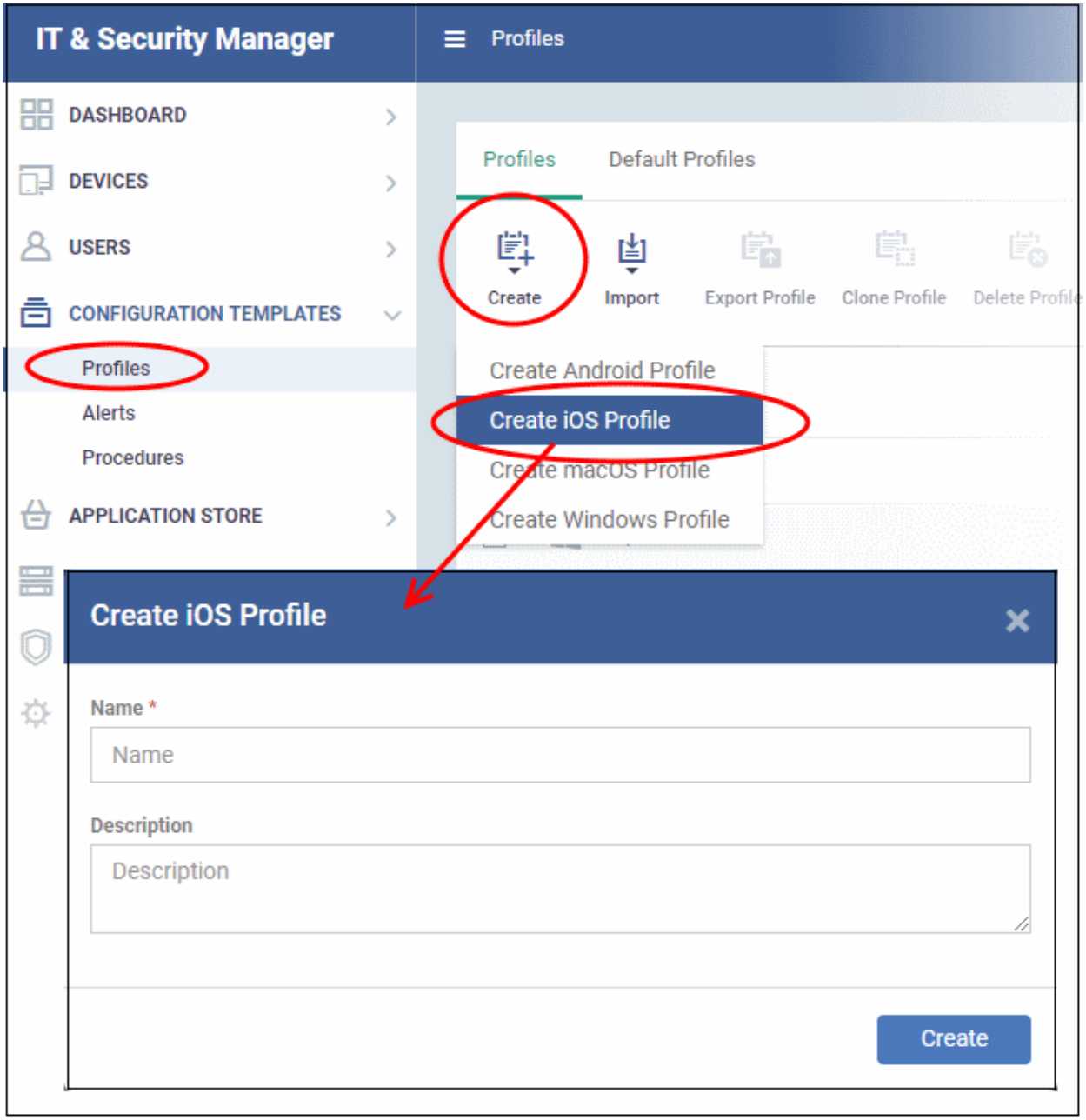
The settings screen for the selected component will be displayed and, after saving, the new section will become available as a link. You can configure passcode settings, feature restrictions, antivirus settings Wi-Fi settings and more. If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another ITSM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added 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.
- **Antivirus Settings** - Schedule antivirus scans on the device and specify trusted Apps to be excluded from AV scans.
- **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 and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi, 'Exchange Active Sync', 'VPN' and so on.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page **Integrating with Comodo Certificate Manager** in the ITSM online help guide.
- **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.

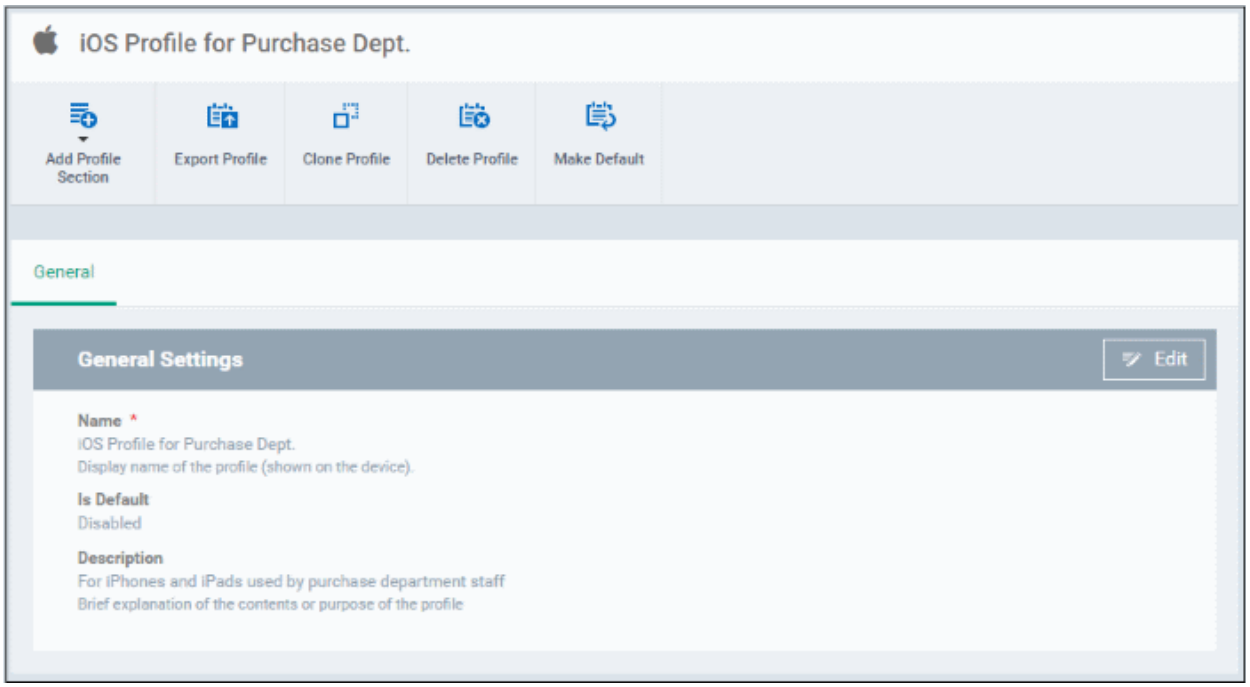
- **Kiosk** - Enable and configure Kiosk Mode for SAFE devices like the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices and whether SMS/MMS are allowed. This profile is supported for SAFE devices only.
- **Native App Restrictions** - Configure 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.

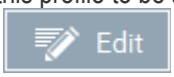
To create an iOS Profile

- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click the 'Create' drop-down above the table and then choose 'Create iOS Profile' from the profiles.



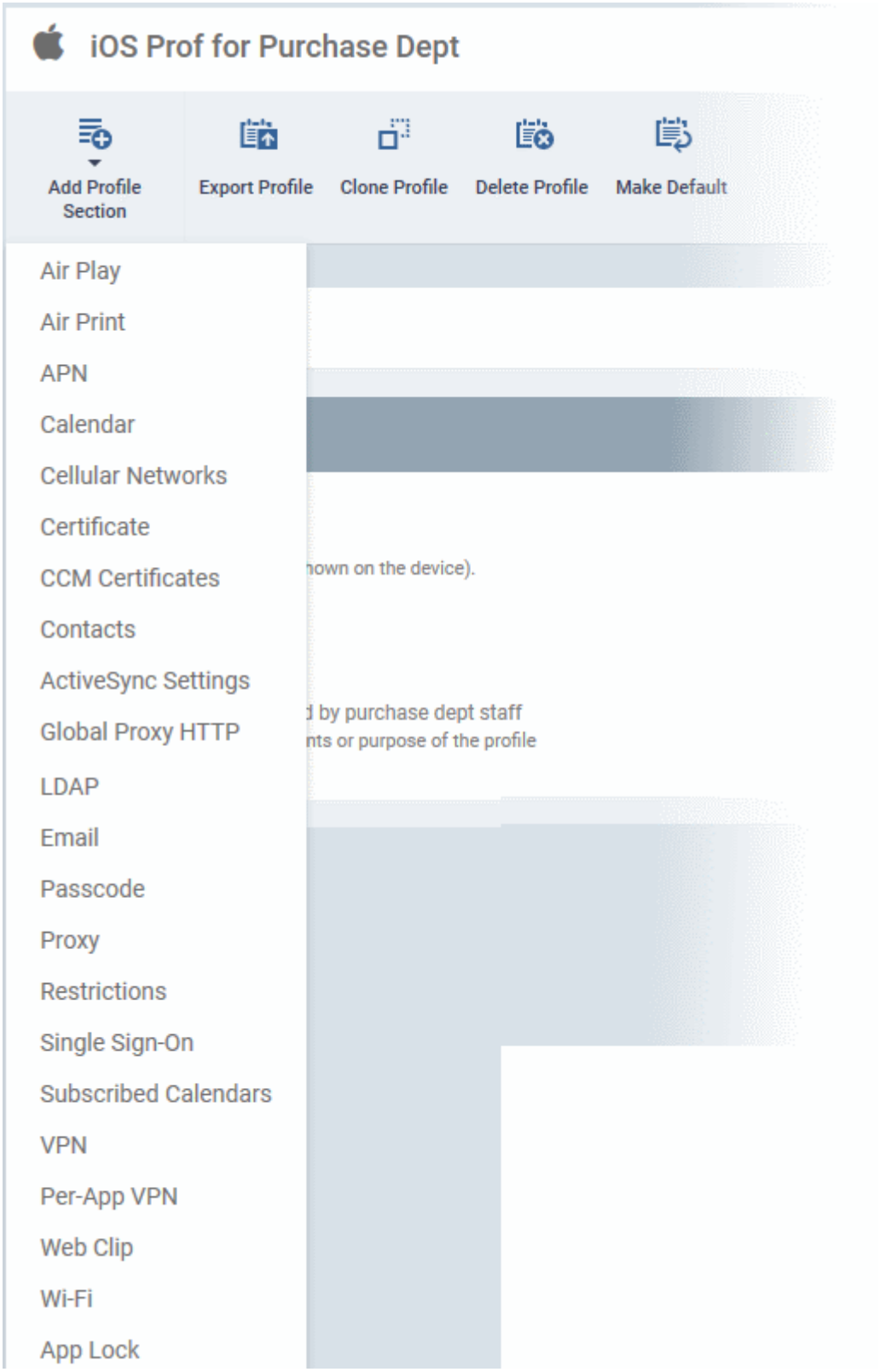
- Enter a name and description for the profile and click 'Create'.
- The profile will be created and the 'General Settings' for the profile will be displayed.



- 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 components for the profile.



- Click the 'Add Profile Section' drop-down 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 and, after saving, the new section will become available as a link. You can configure passcode settings, feature restrictions, VPN settings Wi-Fi settings 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 ITSM profile.

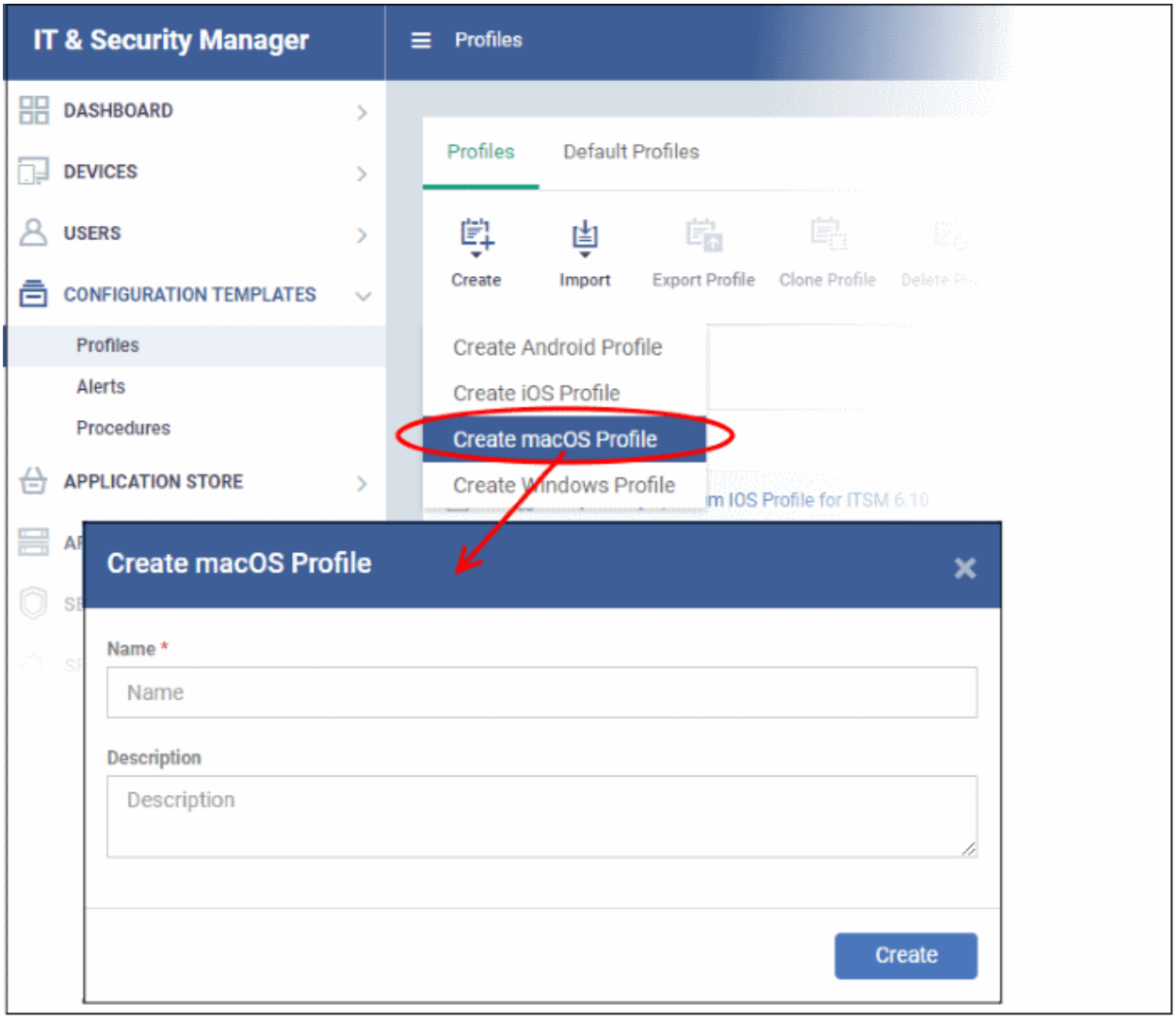
- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.
- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied 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 and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi, 'Exchange Active Sync', 'VPN' and so on.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page **Integrating with Comodo Certificate Manager** in the ITSM online help guide.
- **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.

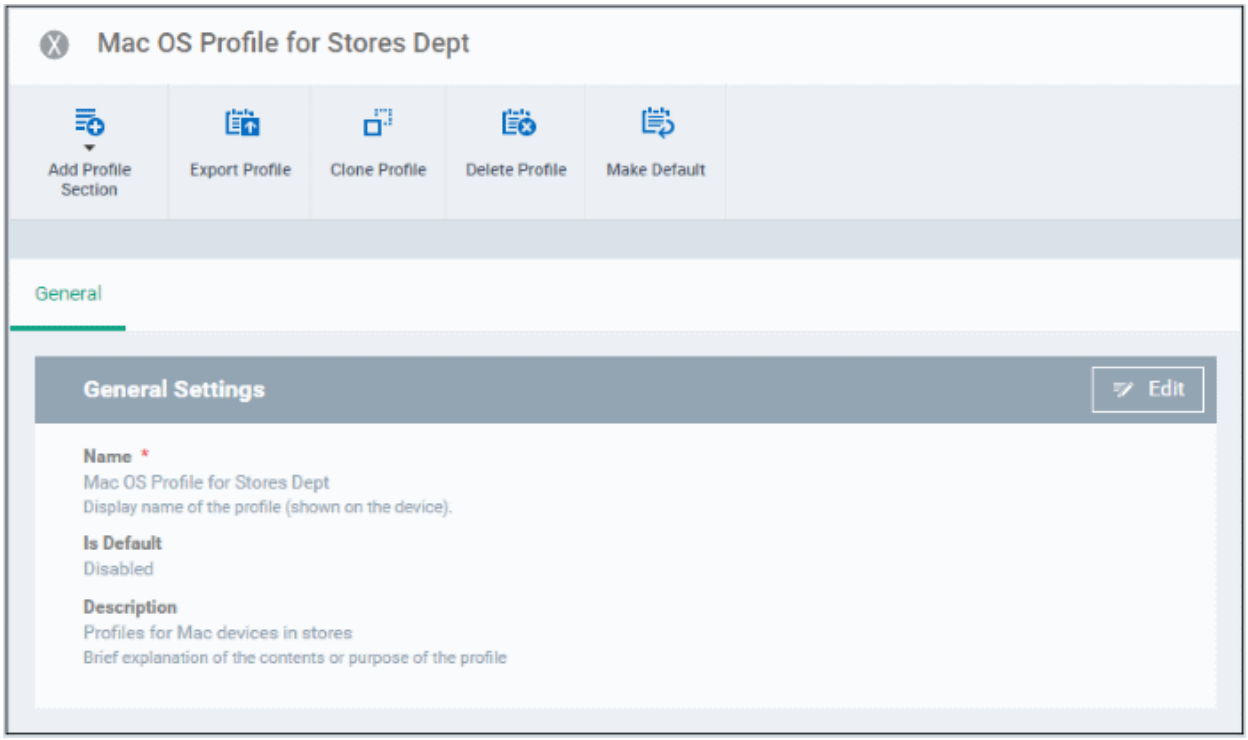
- **VPN Per App** - Configure VPN as above but on a per-application basis. This profile is supported for iOS 7 and above.
- **Web Clip** - Allows you to push a shortcut to a website onto the home-screen of target devices. This section allows you to choose an icon, label and target URL for the web-clip.
- **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.

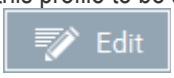
To create a Mac OS Profile

- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click the 'Create' drop-down then click 'Create macOS Profile'



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

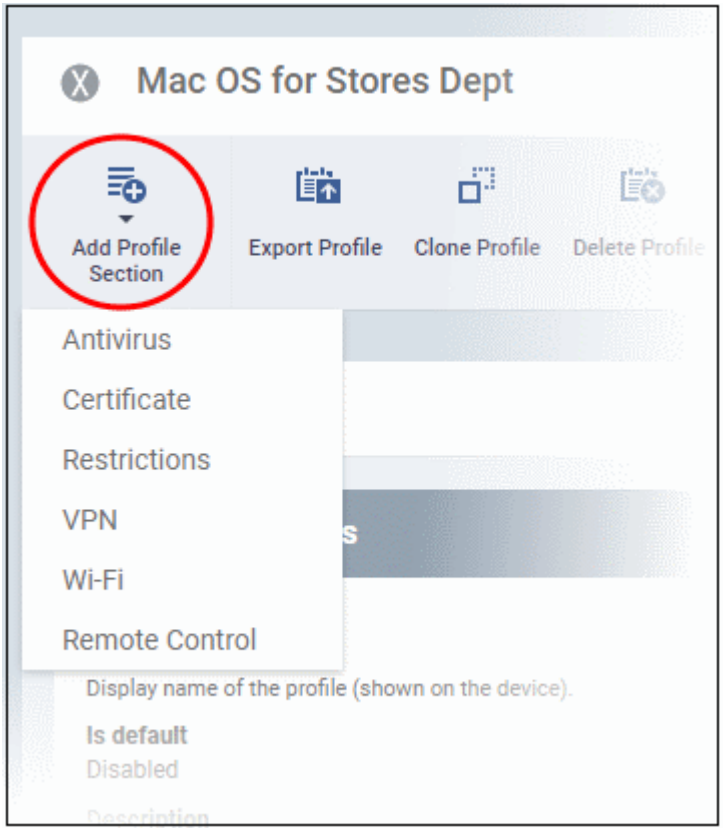


- If you want this profile to be a default policy, click the 'Make default' button at the top. Alternatively, click the 'Edit' button 

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

The next step is to add components for the profile.

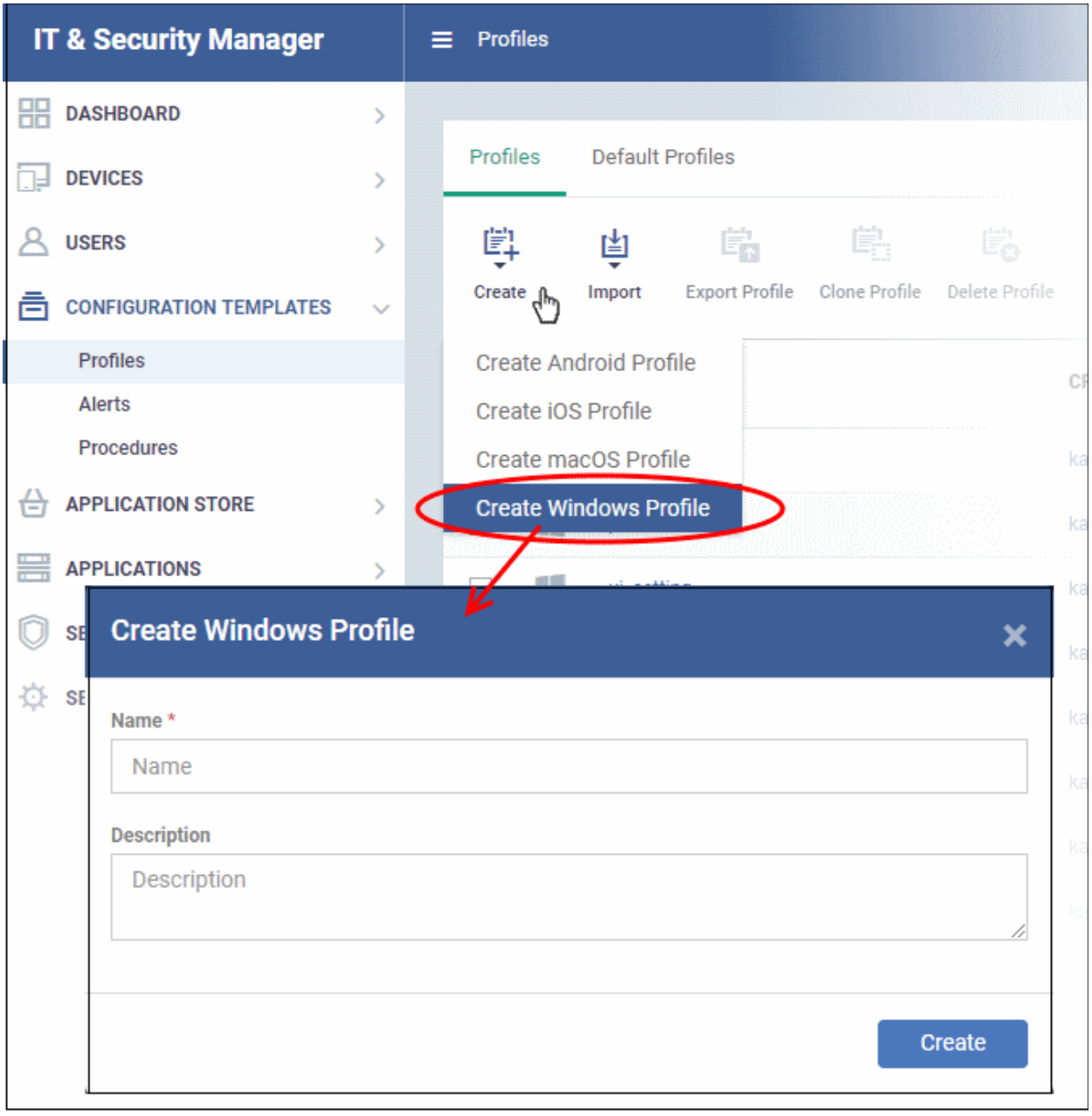
- Click the 'Add Profile Section' drop-down and select the component from the list that you want to include for the profile



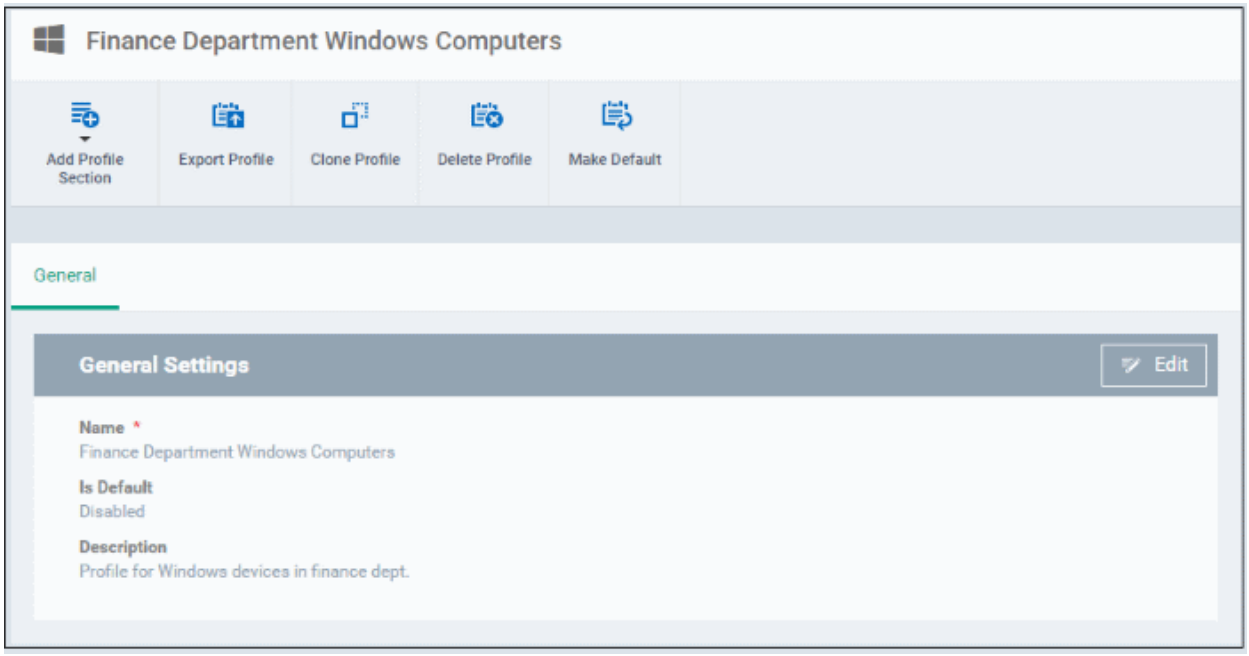
- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **Certificates** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings like 'Wi-Fi and 'VPN'.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page **Integrating with Comodo Certificate Manager** in the ITSM online help guide.
- **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.

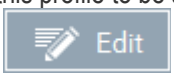
To create a Windows profile

- Click the 'Configuration Templates' tab on the left and choose 'Profiles List'.
- Click 'Create' drop-down above the table and then click '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.



- 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'.

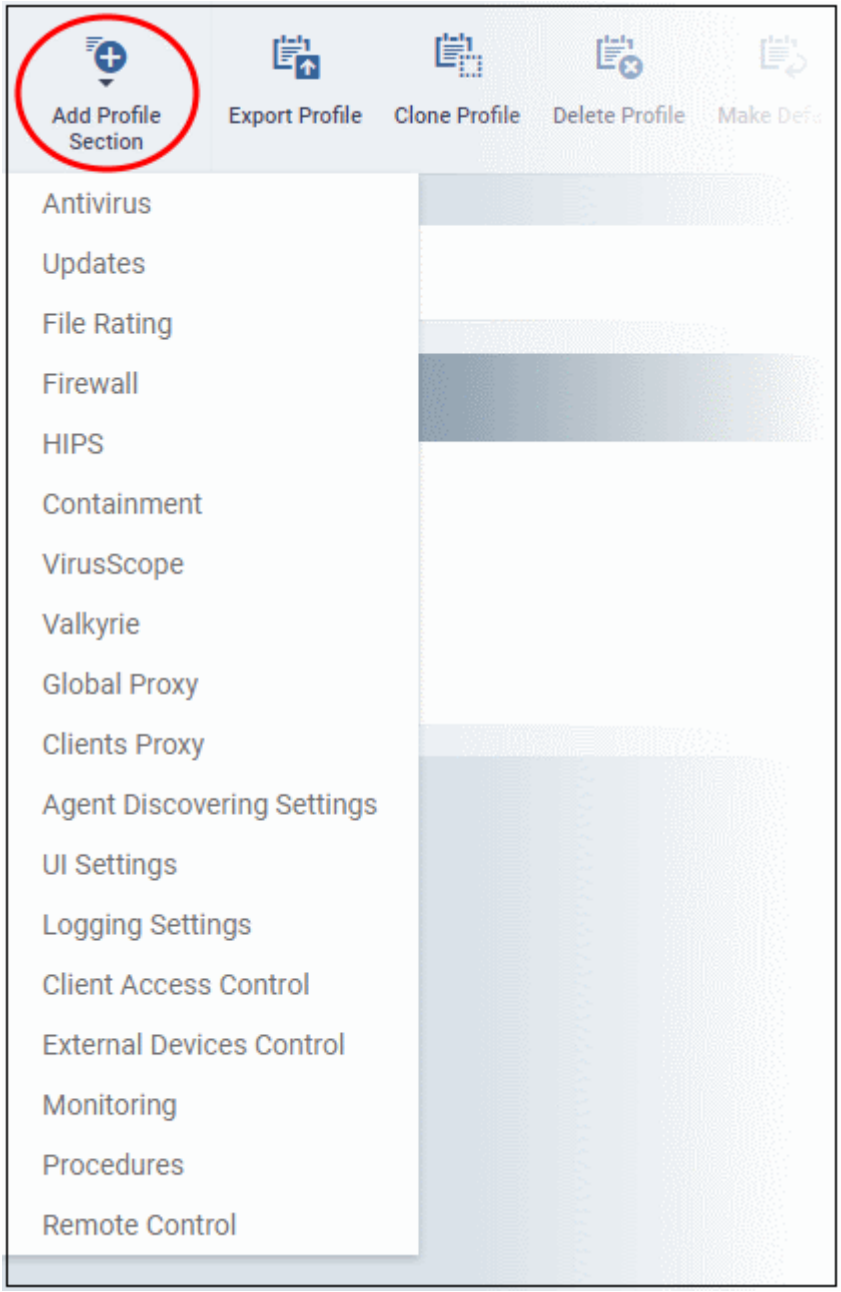
The next step is to add components for the profile.

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

The settings screen for the selected component will be displayed and, after saving, the new section will become available as a link in this interface. You can configure Antivirus, Firewall, Containment, File Rating, Valkyrie, HIPS, VirusScope and Update 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 ITSM profile.

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



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.
- **CCS Update Rule** - 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. For more details on Firewall in CCS, refer to the help page explaining Firewall Settings in CCS online help guide.
- **HIPS** - Enable Host Intrusion Prevention System (HIPS) and its behavior, configure HIPS rules and define Protected Objects at the endpoints. For more details on HIPS in CCS, refer to the help page explaining HIPS Settings in CCS online help guide
- **Containment** - Enable Auto-containment of unknown files, add exclusions, and configure containment

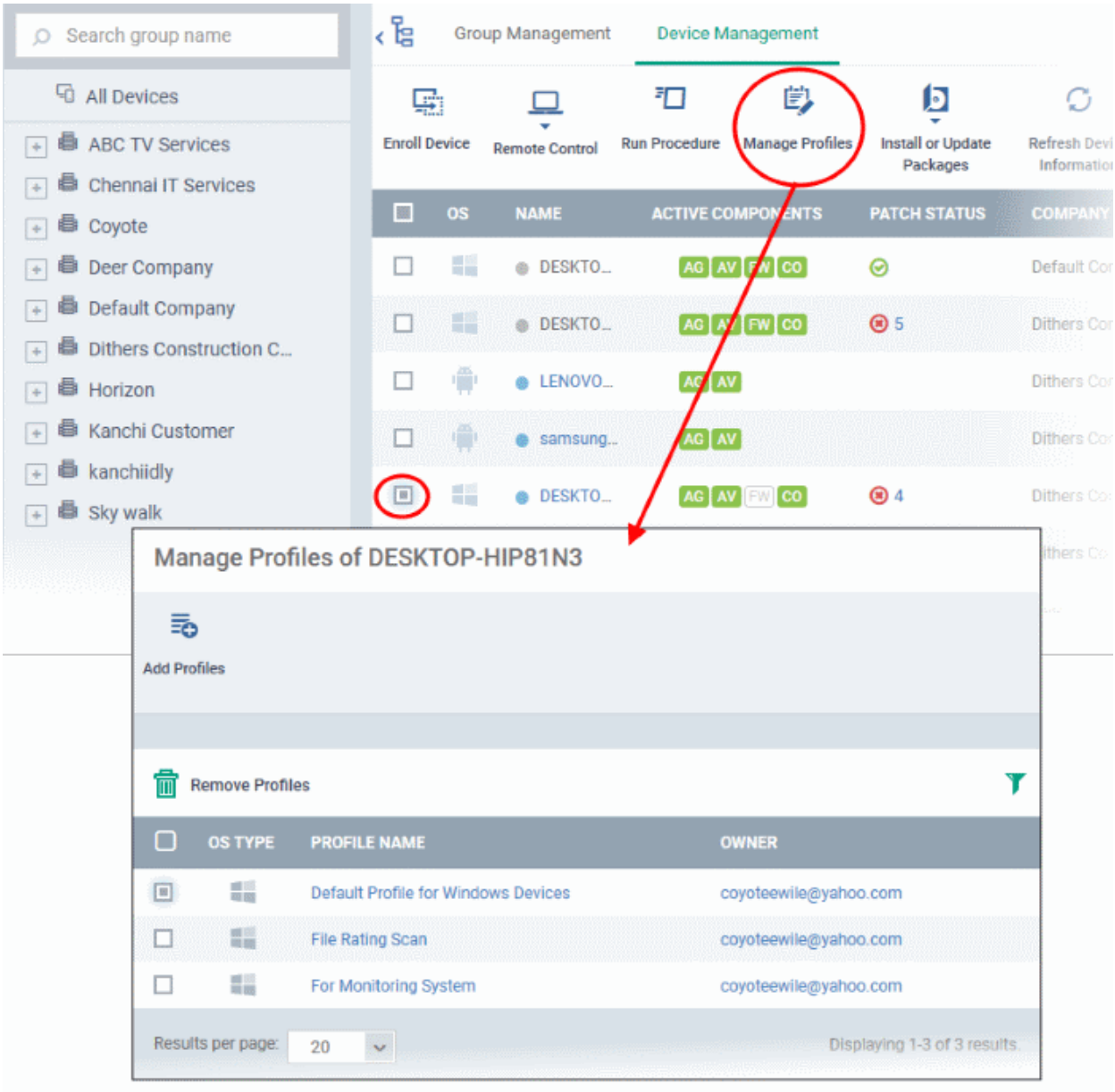
behavior and alert options and view and manage Containment Rules for auto-containing applications. For more details on Containment in CCS, refer to the help page explaining Containment in CCS online help guide.

- **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. For more details on VirusScope in CCS, refer to the help page explaining 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.
- **Proxy** - Allows you to specify a proxy server to be used by the device for network connections.
- **Agent Discovery Settings** - Allows you to specify whether or not Comodo Client should send logs to ITSM above antivirus and containment events.
- **UI Settings** - Change the appearance of Comodo Client Communication (CCC) and Comodo Client Security (CCS). You can re-brand CCC and CCS with your own company/product name and logos. You can also select which components of CCS should be visible to end-users.
- **Logging Settings** - Allows you to enable logging events from CCS, the maximum size of the log file and configure behavior once log file reaches the maximum file size.
- **Monitoring Settings** - Allows you to 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.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page Integrating with Comodo Certificate Manager in the ITSM online help guide.
- **Procedures** - Allows you to add, view, delete and prioritize procedures which have been added to a profile.
- **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.

Step 7 - Apply profiles to devices or device groups

- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
    - Select a Company and choose a group under it to view the list of devices in that group

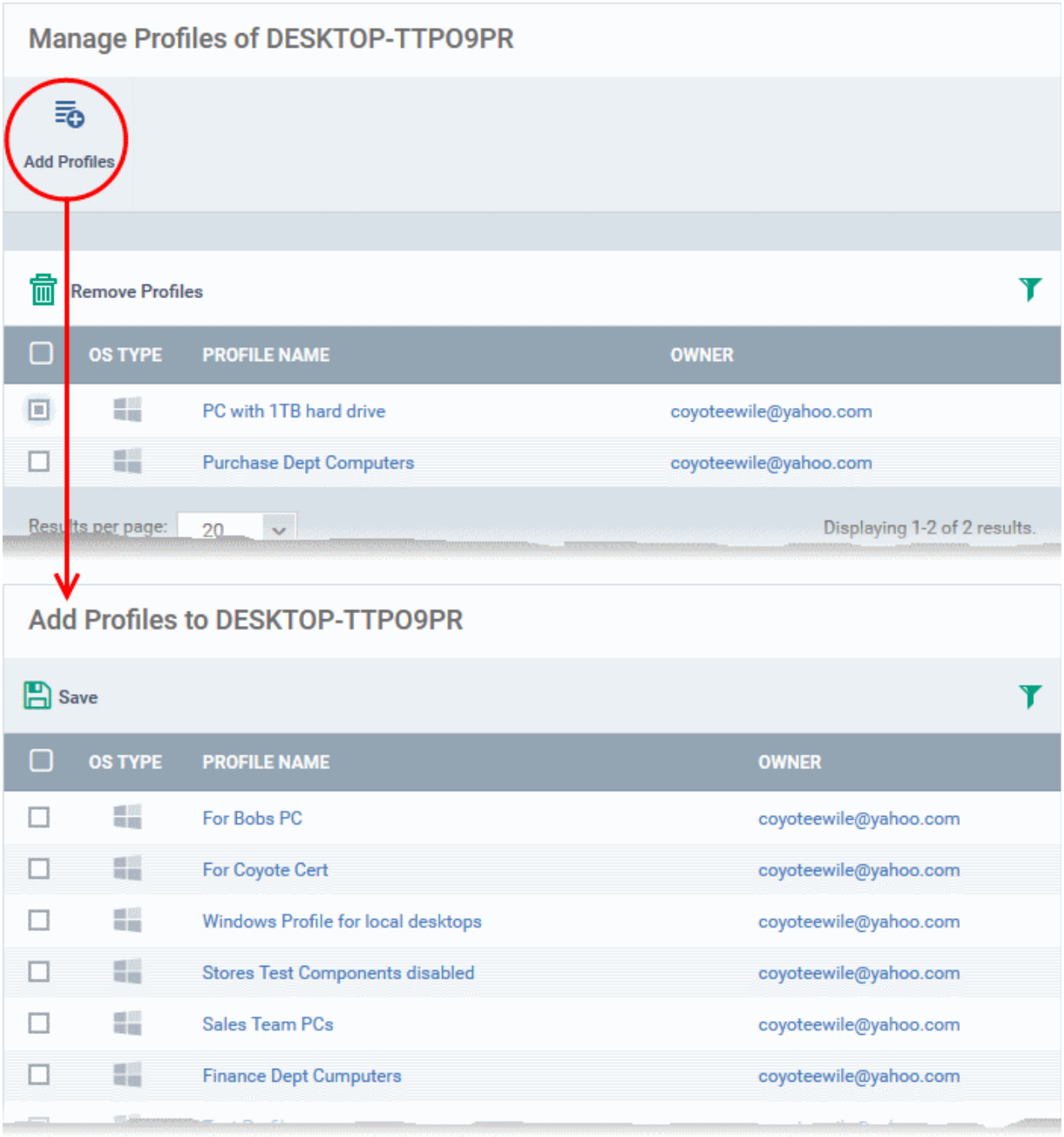
      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Select the device to be managed and click 'Manage Profiles' from the options at the top



The list of profiles currently active on the device will be displayed.

- To add a profile to the device, click 'Add Profiles' from the top left.

A list of all profiles applicable to the chosen device, excluding those that are already applied to the device will be displayed.



- Select the profile(s) to be applied to the device
- Click 'Save' at the top left to add the selected profile(s) to the device.

To apply profiles to a *group* of devices

The procedure is similar to adding profile(s) to a device 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 profile(s) to be applied to the devices in the group
7. Click 'Add Selected' on the top left to add the selected profile(s) 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.

The Comodo Threat Research Labs is a global team of IT security professionals, ethical hackers, computer scientists and engineers analyzing and filtering input from across the globe. The team analyzes millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day, using the insights and findings to secure and protect its current customer base and the at-large public, enterprise and internet community.

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. With offices in the US, China, Turkey, India, Romania and Ukraine, Comodo secures the online and offline eco-systems of thousands of clients worldwide.

Comodo Security Solutions, Inc.

Comodo Security Solutions, Inc

1255 Broad Street.

Clifton, NJ 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.6361

Email: EnterpriseSolutions@Comodo.com

For additional information on Comodo - visit http://www.comodo.com.