

COMODO
Creating Trust Online®



Comodo IT and Security Manager

Software Version 5.4

Quick Start Guide

Guide Version 5.4.091216

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 - Applying 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**.

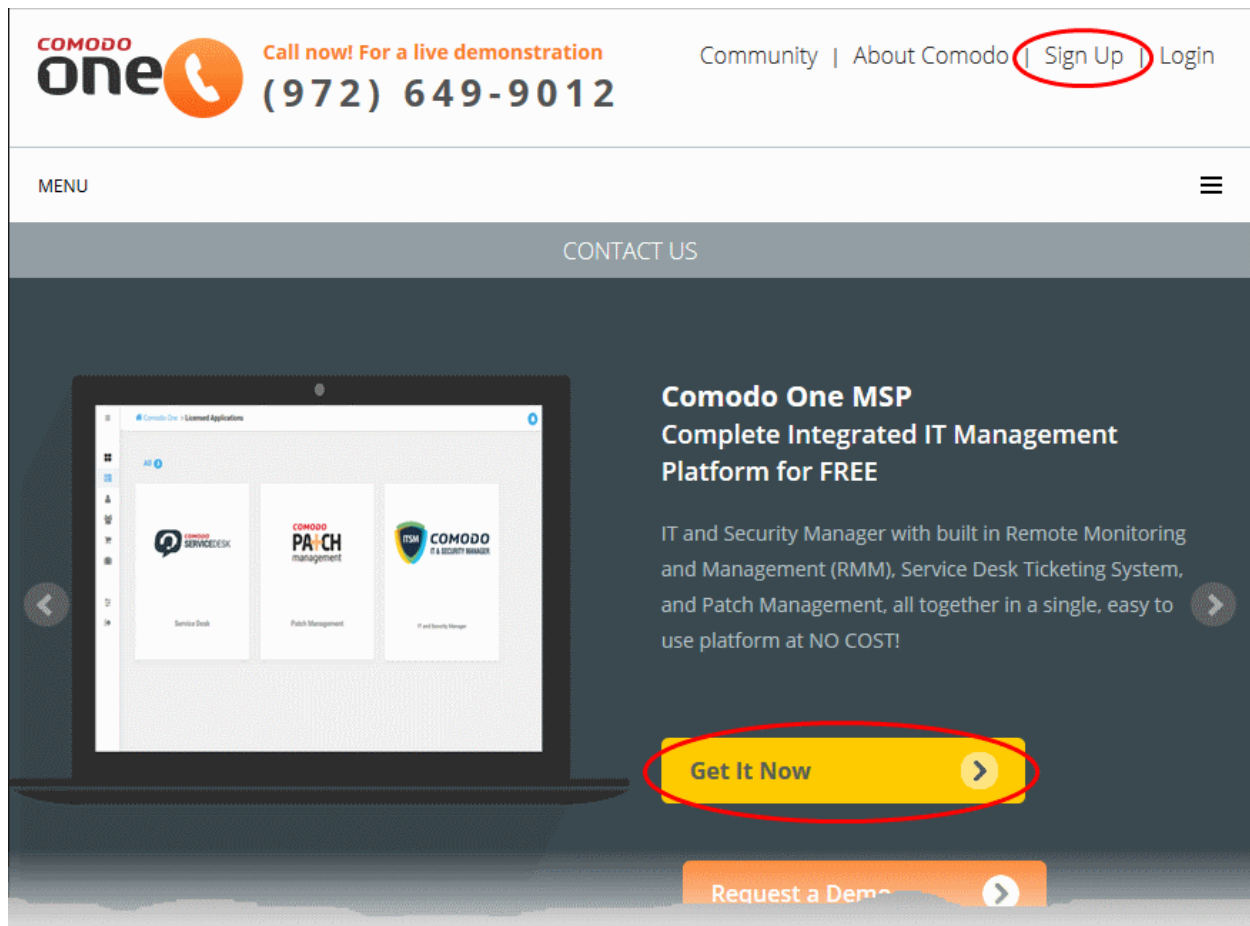
Step 1 - Enrollment and Configuration

Note – This portion of the guide explains about enrollment to ITSM as a new customer. If you have already signed-up for a **Comodo One MSP** or **Comodo One Enterprise** service, you can skip this step and can log-in to ITSM console from the Comodo One interface by clicking 'Licensed Applications' > 'IT and Security Manager'.

For more details on Comodo One and the services offered with the Comodo One Package, refer to the online help 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 'Sign up' at the top right or 'Get it for Now'



You will be taken to the enrollment wizard for Comodo One subscription.

A screenshot of the Comodo One enrollment wizard. The background is dark blue with white text. The text reads: 'Enter your email to start the sign-up process of Comodo ONE'. Below this is a white input field containing the email address 'juliusdither@dithers.com'. At the bottom of the form is a green 'SUBMIT' button.

- Enter your email address and click 'Submit'

A short enrollment form for your Comodo One subscription will appear.

- Choose the account type.
 - If you are a new customer, choose the 'I AM A NEW USER' tab and fill a short enrollment form

- **Email** - This field will be pre-populated with email address provided. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
- **Password** - Enter the password for logging-in to your C1 account. The password should be of at least eight characters, and must contain a combination of lower case and upper case characters, at least one numeral and at least one special character chosen from '(!#\$%^&*")'
- **Telephone Number** - Enter your telephone 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:** Enter the Captcha value to verify your application
- Click the 'Submit' button.

A verification email will be sent to the email address you provided in the 'Email' field.

- If you already have an account with Comodo, click the 'I HAVE A COMODO LICENSE ACCOUNT' tab and fill a short enrollment form
- **Comodo License Account Login / Email** - Enter your username or email address used to login to your Comodo account at <https://accounts.comodo.com>. You will receive the verification link to the email address you entered while registering your account with Comodo.
- **Password:** Enter your Comodo Account password. The same password should be used to logging-in to your C1 account.
- **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:** Enter the Captcha value to verify your application
- Click the 'Submit' button.

A verification email will be sent to the email address registered at the time of your Comodo account creation.



Hello,

Thank you for your interest on Comodo ONE. Please click on link below to verify your email address and set your password.

[Verify my email](#)

Thank you being part of the community!

The Comodo One Team

Please **do not reply to this email** as this email address is not monitored.

Support Telephone:

US: +1.703.637.9361

International: 1-88-256-26-08

Support Email: c1-support@comodo.com

Enterprise Forum: <https://forum1.comodo.com>

MSP Forum: <https://forum.mspconsortium.com>

- Click the 'Verify my email' link

Upon successful verification, you will be taken to the C1 login page.

COMODO ONE

→ Welcome to Comodo ONE. You can now login with your email and password.

Email or Login

Password

Remember Me [Forgot password?](#)

LOGIN

[I don't have an account > Sign Up](#)

- Enter your email address and password to login to C1. Upon your first log-in, 'Complete Account Details' form will be displayed.

Complete Account Details

Logout

Email

Business Type *

Enterprise
▼

Company Name *

Subdomain *

?

[dithers.servicedesk.comodo.com](#)
[dithers.cmdm.comodo.com](#)

Phone Number *

Country

State

Postal Code

SUBMIT

- Fill-in the form with the details for your C1 account
 - **Email** - This field will be pre-populated with the email address entered during account creation. You cannot edit this field.
 - **Business Type** - Select your business type. The available options are 'MSP' and 'Enterprise'. The modules offered with the Comodo One base package differ, depending on the business type.

Comodo One MSP	Comodo One Enterprise
Modules included in the Comodo One Base package	
Service Desk Patch Management IT and Security Manager (ITSM)	Service Desk IT and Security Manager (ITSM)

Modules that can be subscribed and added to base Comodo One	
Acronis Backup	Comodo Dome Standard
Comodo Quote Manager	Comodo Dome Shield
cWatch	Comodo CRM
Comodo CRM	Comodo KoruMail
Comodo Dome Standard	Comodo Antispam Gateway
Comodo Dome Shield	Comodo Korugan
Comodo CRM	
Comodo KoruMail	
Comodo Antispam Gateway	
Comodo Korugan	

For more details on the modules, refer to the Comodo One guide at <https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html>.

- **Company Name** - Enter the name of the company that you want to enroll for Comodo One.
- **Subdomain** - Enter the sub-domain name for creating the URL to access the Comodo One modules, like ITSM and Service Desk . For example, if you enter the sub-domain 'dithers' then you can access the ITSM module by entering the URL 'https://dithers.cmdm.comodo.com'.
- **Phone Number** - Enter the phone number of your company
- **Country** - Choose your country from the drop-down
- **State** - Choose your state/province country from the drop-down
- **Postal Code** - Enter the postal code/zip code of your city.
- Time Zone – Select the time zone followed in your region.
- Click 'Submit'

The activation dialog for your free products will appear.

IT and Security Manager Activation

Logout

Existing Licenses

⚠ There are no existing IT and Security Manager license. You can select an available license below.

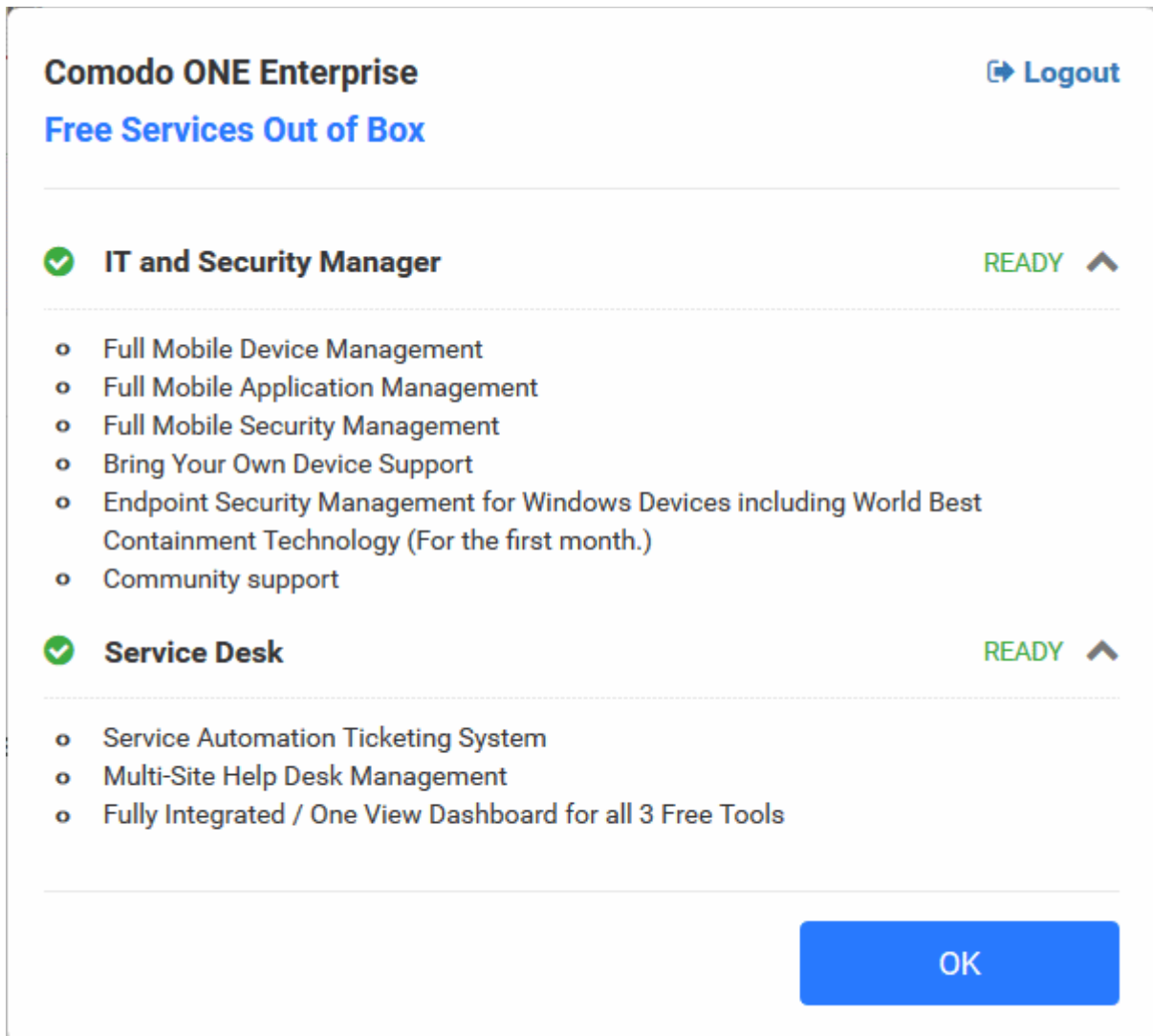
Available Licenses

- IT and Security Manager Subscription Basic Edition (Unlimited Users - Free)**

NEXT

- Click 'Next'

Your free modules will be activated.



The screenshot shows the Comodo ONE Enterprise dashboard. At the top left, it says "Comodo ONE Enterprise" and "Free Services Out of Box". In the top right corner, there is a "Logout" button with a right-pointing arrow. Below this, there are two main sections, each starting with a green checkmark icon and a title. The first section is "IT and Security Manager" with the status "READY" and an upward-pointing arrow. It lists several services: Full Mobile Device Management, Full Mobile Application Management, Full Mobile Security Management, Bring Your Own Device Support, Endpoint Security Management for Windows Devices including World Best Containment Technology (For the first month.), and Community support. The second section is "Service Desk" with the status "READY" and an upward-pointing arrow. It lists: Service Automation Ticketing System, Multi-Site Help Desk Management, and Fully Integrated / One View Dashboard for all 3 Free Tools. At the bottom right of the dashboard area, there is a large blue button labeled "OK".

- Click 'OK' on completion. You will be taken to Comodo One Dashboard.

That's it. You have successfully created a Comodo One account.

Please note that this account will be automatically granted 'Account Admin' privileges and cannot be deleted. This is effectively the 'Master Admin'. You will be able to create 'Admins' and Staff under this account. For more details, refer to the online help guide of Comodo One at <https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html>.

You can log-in to ITSM console in two ways:

- From C1 console - Login to C1 console, click 'Licensed Applications' > 'ITSM' from the C1 console
- Directly to ITSM – Enter the URL 'https://<your sub-domain>.cmdm.comodo.com/'



- Enter your email address as user name and password specified during sign-up and click 'Login'

Step 2 - Configure ITSM Communications

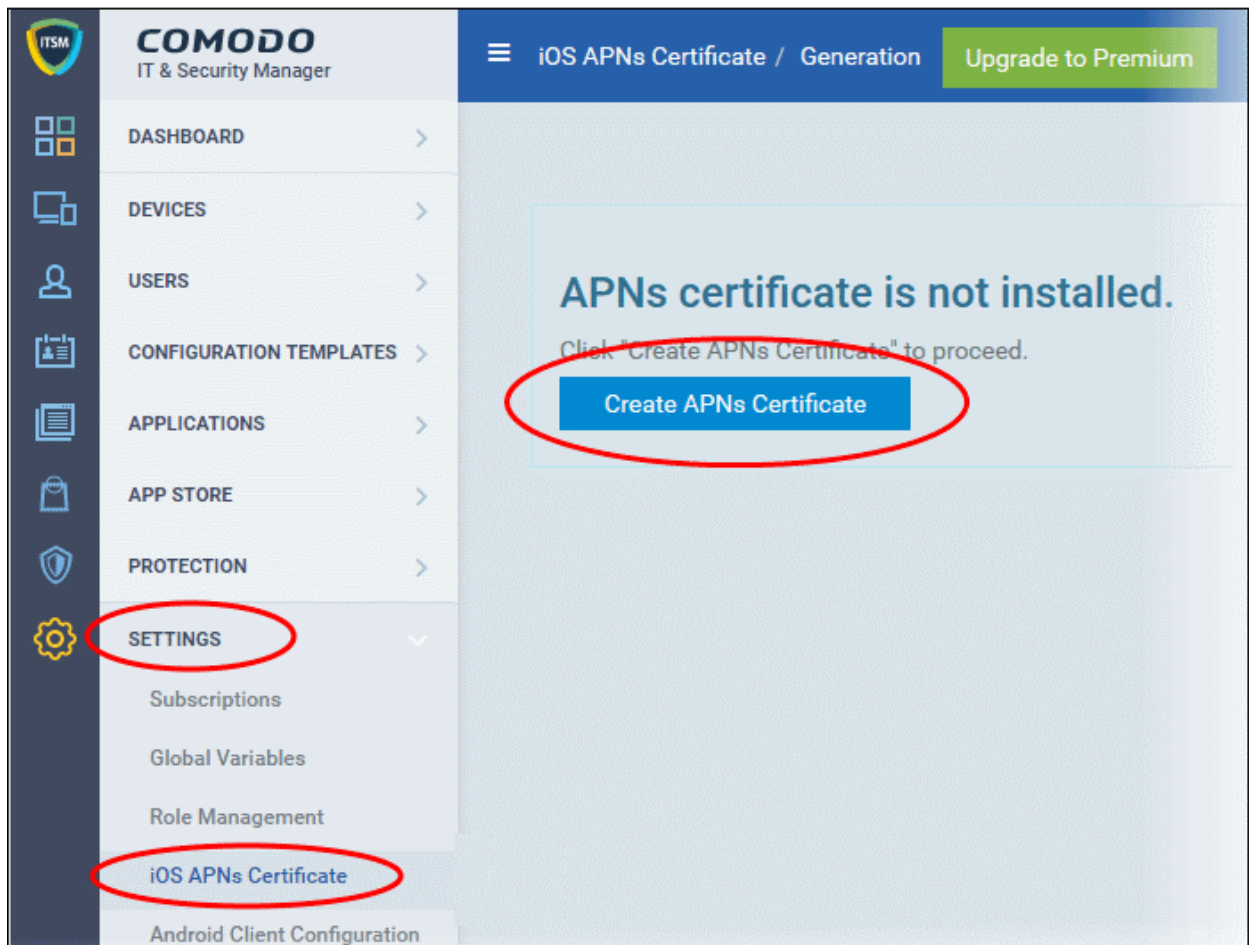
In order for your ITSM server to communicate with enrolled devices, you need to install Apple Push Notification (APN) certificate and/or Google Cloud Messaging (GSM) Token on your portal. The following sections explain more about:

- [Adding APN Certificate](#)
- [Adding GCM Token](#)

Adding Apple Push Notification Certificate

Apple requires an Apple Push Notification (APN) certificate to be installed on your 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' from the left of ITSM console interface and select 'iOS APN's Certificate'.



- Click the 'Create APNs Certificate' button on the right.

The application form for APN certificate will open. The fields on this form are for generating a Certificate Signing Request (CSR):

Generation of APNs Certificate Close

Country Name *

Email Address *

State Or Province Name *

Locality Name (eg, city) *

Organization Name *

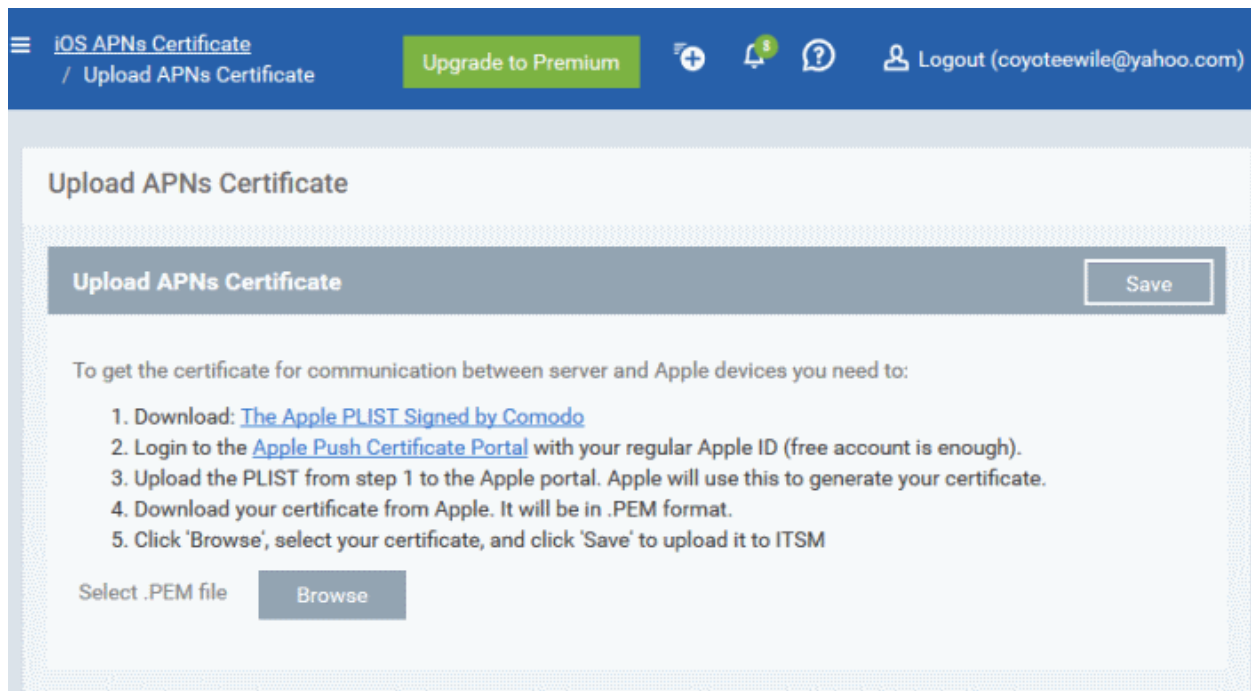
Organizational Unit *

Organizational Unit Name (eg, section)

Common Name *

(e.g. server FQDN or YOUR name)

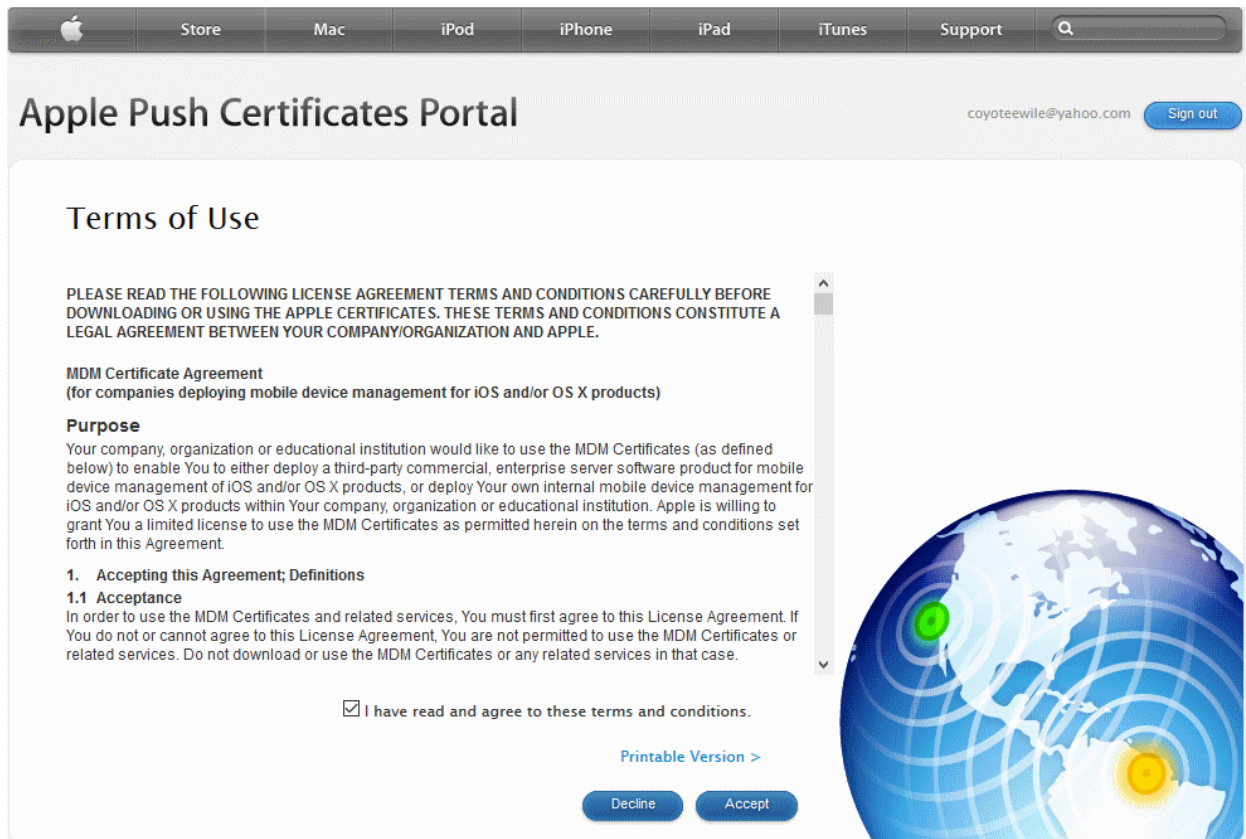
- Complete all fields marked with an asterisk and click 'Create'. This will send a request to Comodo to sign the CSR and generate an Apple PLIST. You will need to submit this to Apple in order to obtain your APN certificate. Usually your request will be fulfilled within seconds and you will be taken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



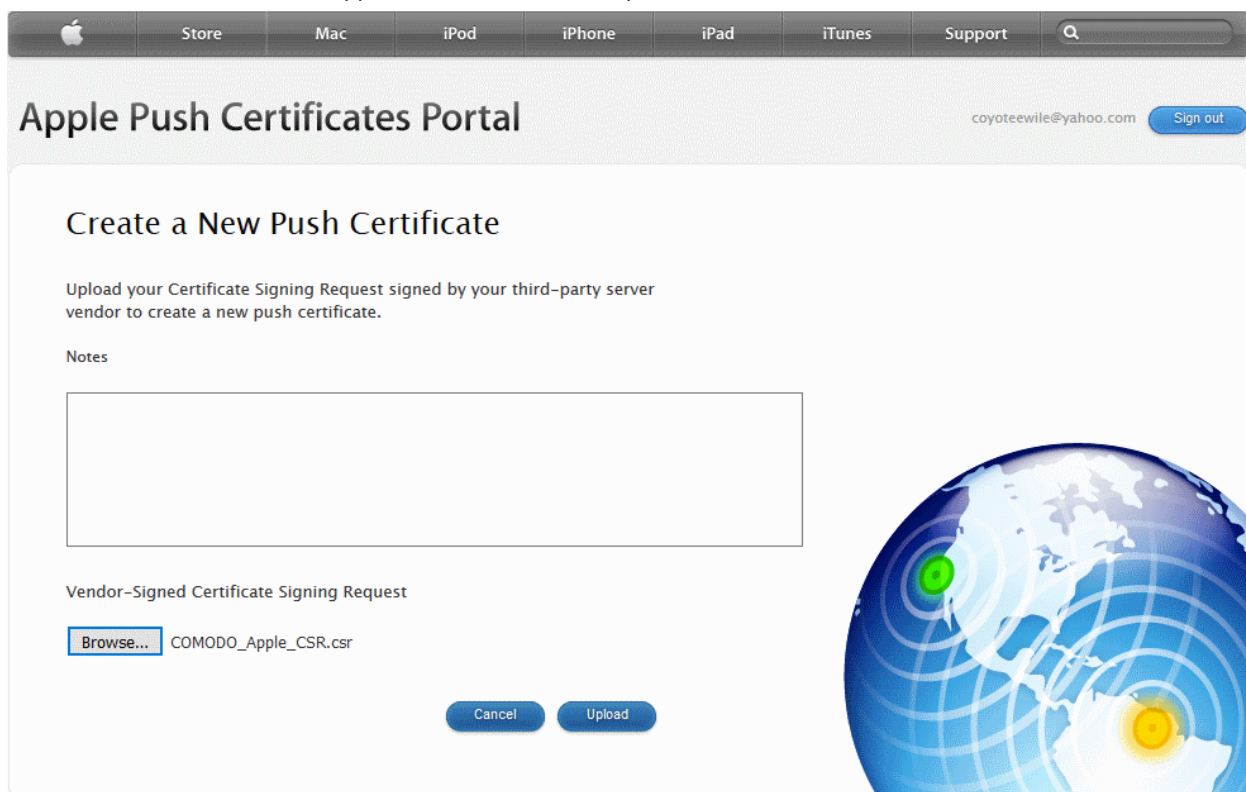
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.
- **Step 2 -Obtain Your Certificate From Apple**
 - Login to the 'Apple Push Certificates Portal' with your Apple ID at <https://identity.apple.com/pushcert/>.
 - If you do not have an Apple account then please create one at <https://appleid.apple.com>.
 - Once logged in, click 'Create a Certificate'.



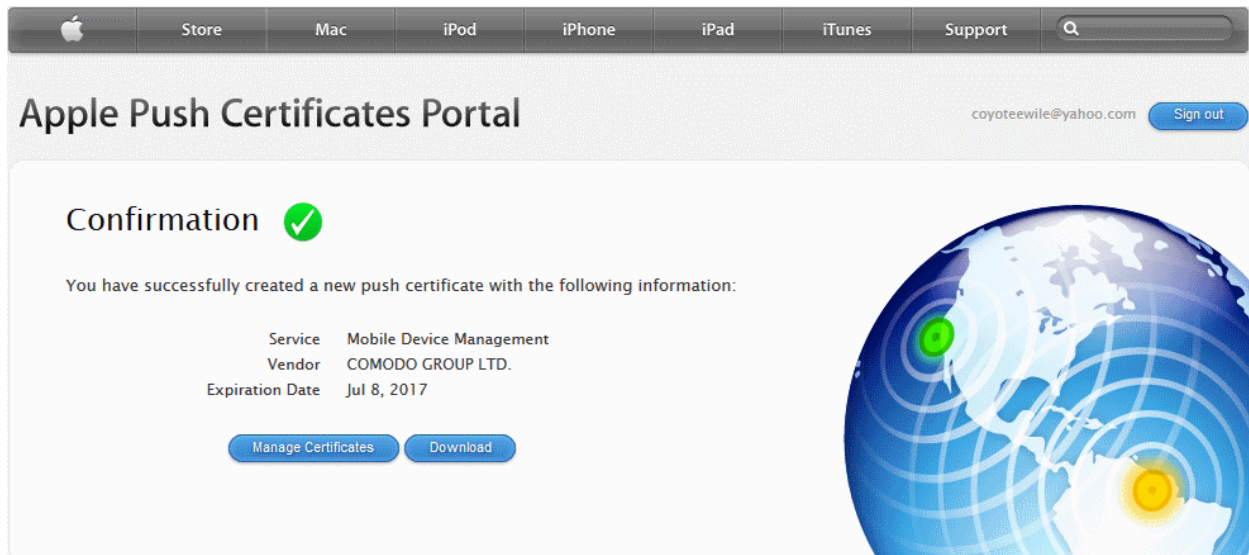
You will need to agree to Apple's EULA to proceed.



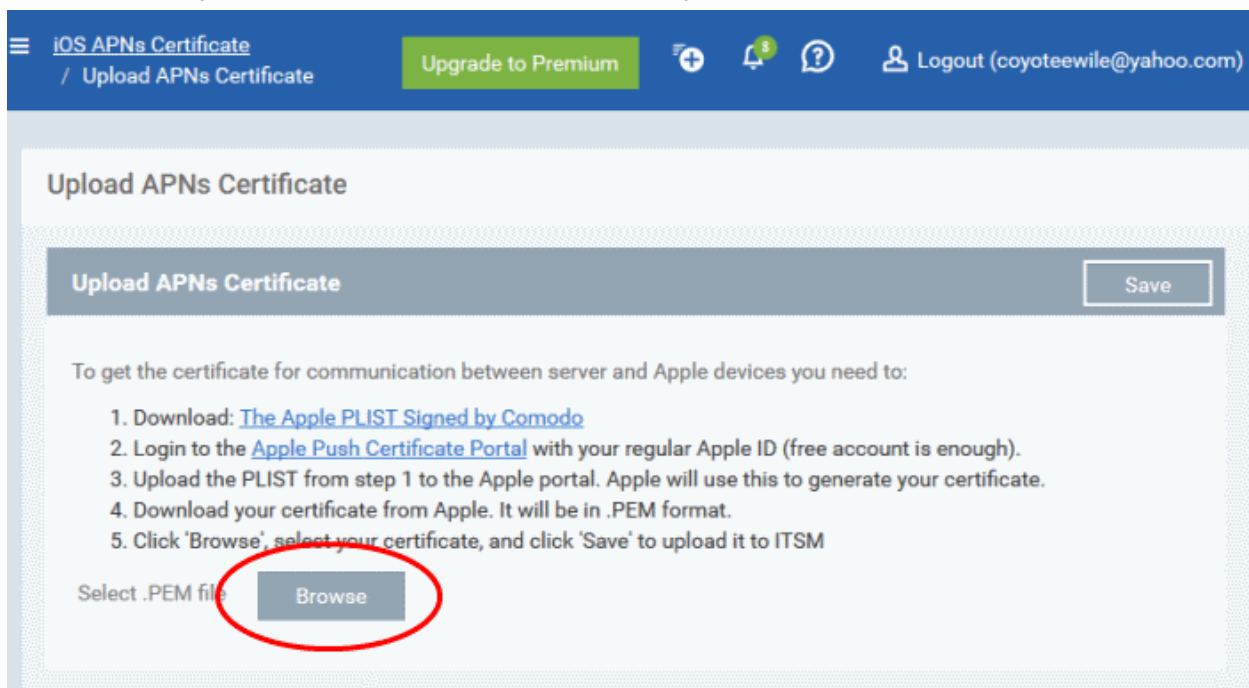
- On the next page, click 'Browse', navigate to the location where you stored 'COMODO_Apple_CSR.csr' and click 'Upload'.



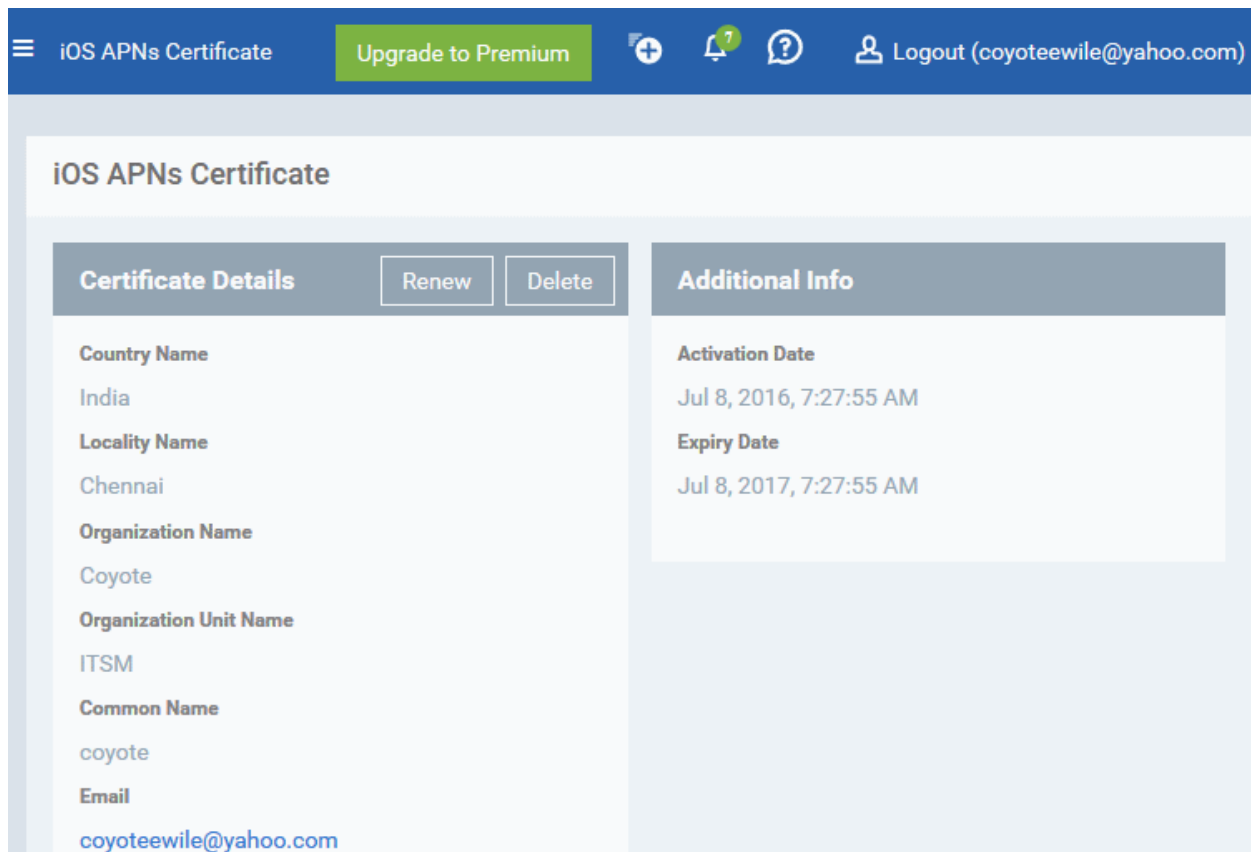
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



- 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 interface. Click the 'Browse' button to locate your certificate file then click 'Save' to upload your certificate.



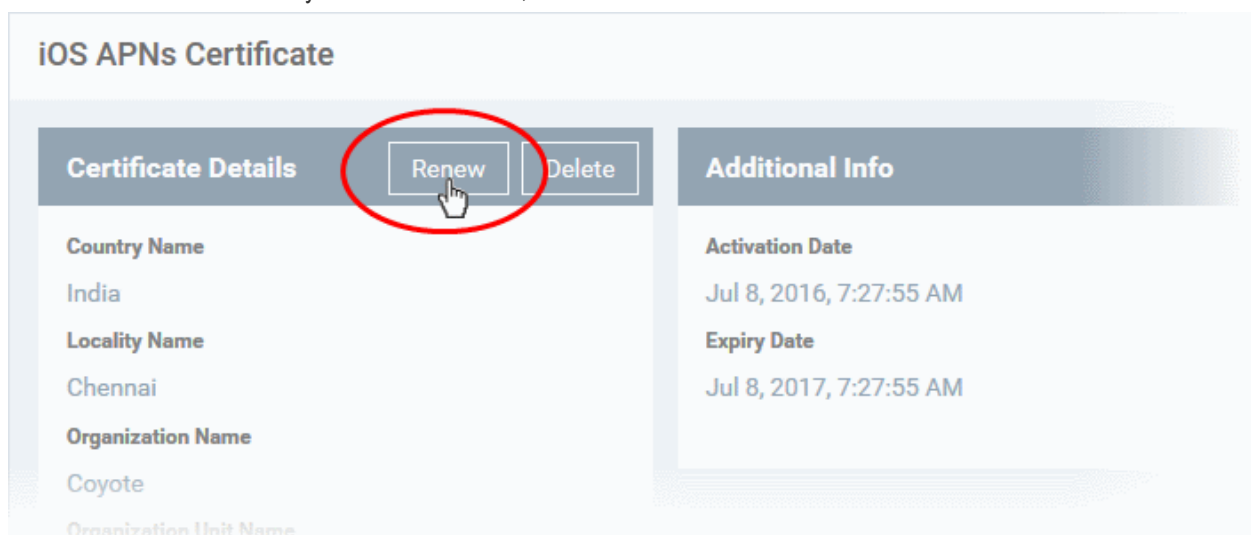
The APNs Certificate details interface will open:



Your ITSM Portal will 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

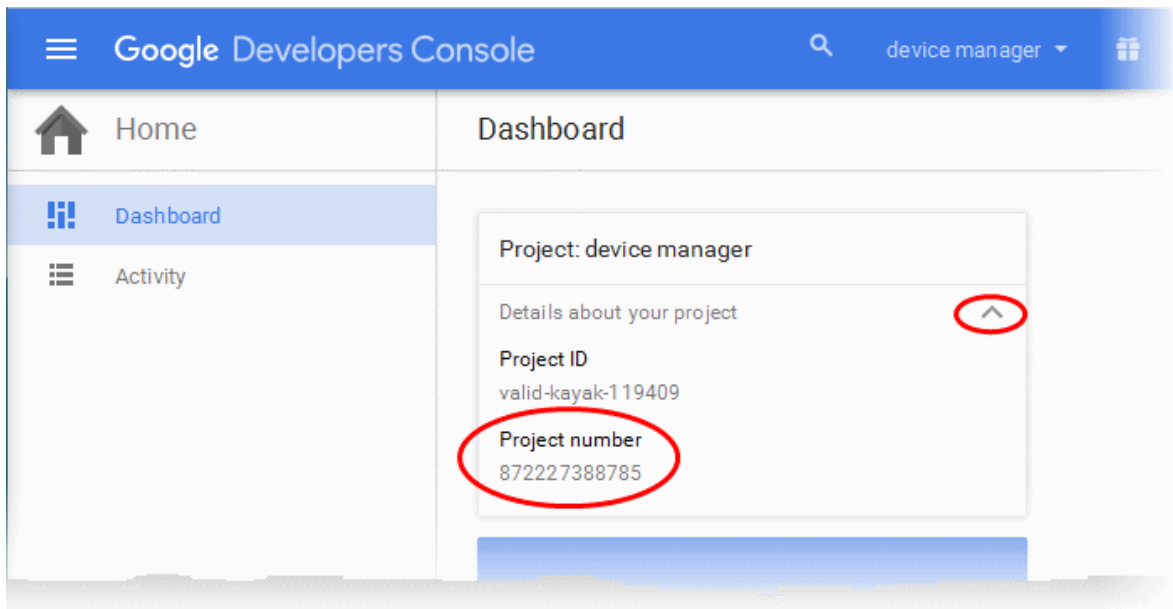
Adding Google Cloud Messaging (GCM) Token

You need to obtain a Google Cloud Messaging (GCM) token in order for ITSM to communicate with Android devices. To get the token, you must first create a project in the Google Developers console.

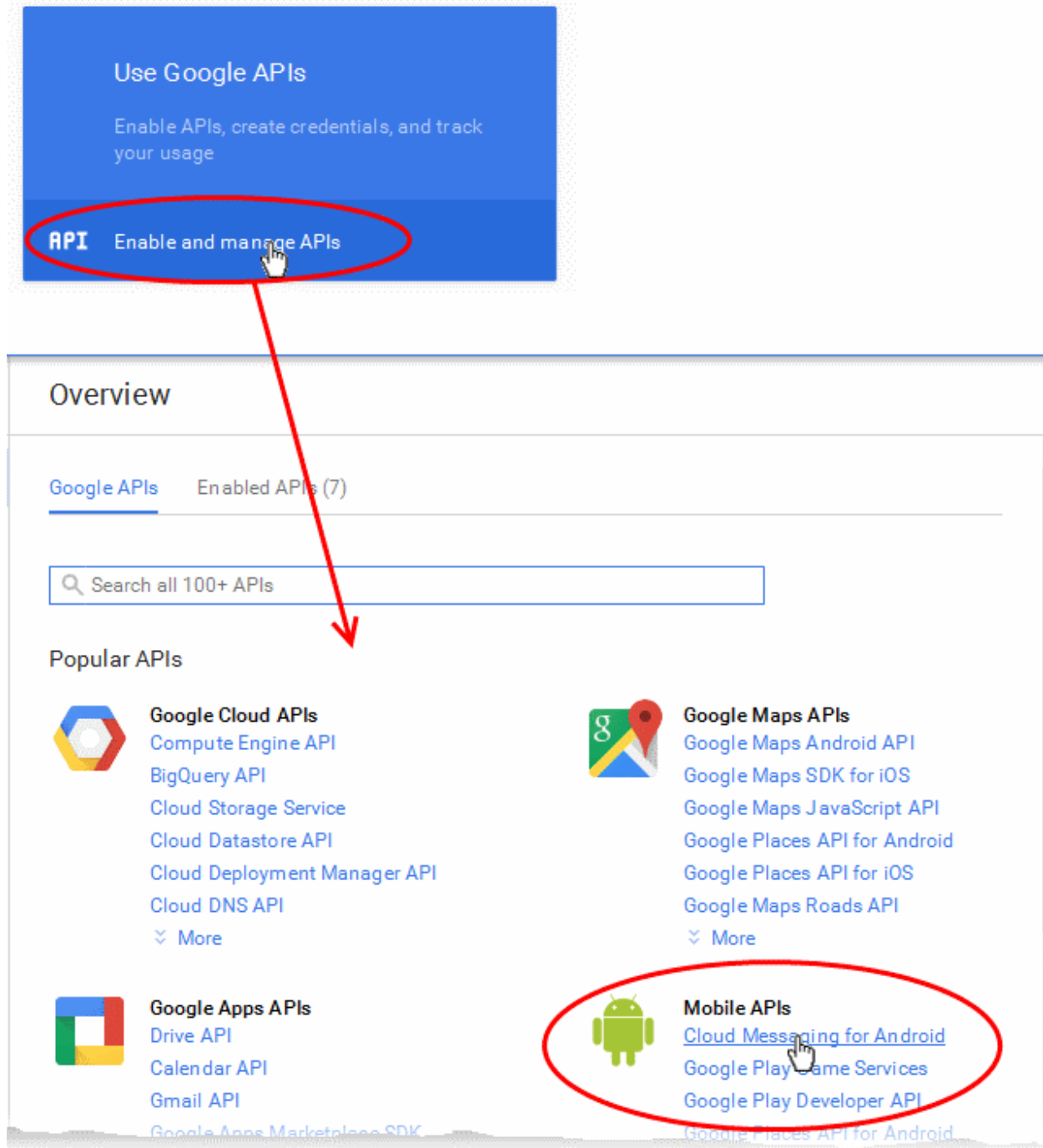
Comodo IT and Security Manager ships with a default API token which is hard-coded and not visible in the interface. However, you can also generate a unique Android GCM token for your ITSM account.

To generate a GCM token, you must have created a Mobile Backend Project at <https://console.developers.google.com/>. Please follow the steps given below to create a project and upload a token.

- **Step 1** - Login to the Google API Console at <https://console.developers.google.com/> and choose 'Create a project' from the 'Select a project' drop-down at the top right.
 - Type a name for the project and click 'Create'. Your project ID will be auto-generated.
- **Step 2** - After the project is created, the Project Dashboard screen will be displayed. If not, choose the project from the 'Select a project' drop-down at the top right:



- Click the drop-down beside Details about your project and note down the 'Project number'
- **Step 3** - Click 'Enable and Manage APIs' use 'Use Google APIs' from the same screen.



- **Step 4** - Click on "Cloud Messaging for Android" under 'Mobile APIs' in the list of available services.
 - In the next screen, ensure that the service is enabled for the project, else click the 'Enable API' at the top enable the service.

Overview

← Enable API

Google Cloud Messaging for Android

Overview

← Disable API

Google Cloud Messaging for Android

⚠ This API is enabled, but you can't use it in your project until you create credentials. Click "Go to Credentials" to do this now (strongly recommended). [Go to Credentials](#)

[Overview](#)

Google Cloud Messaging allows for push messaging to Android devices. [Learn more](#)

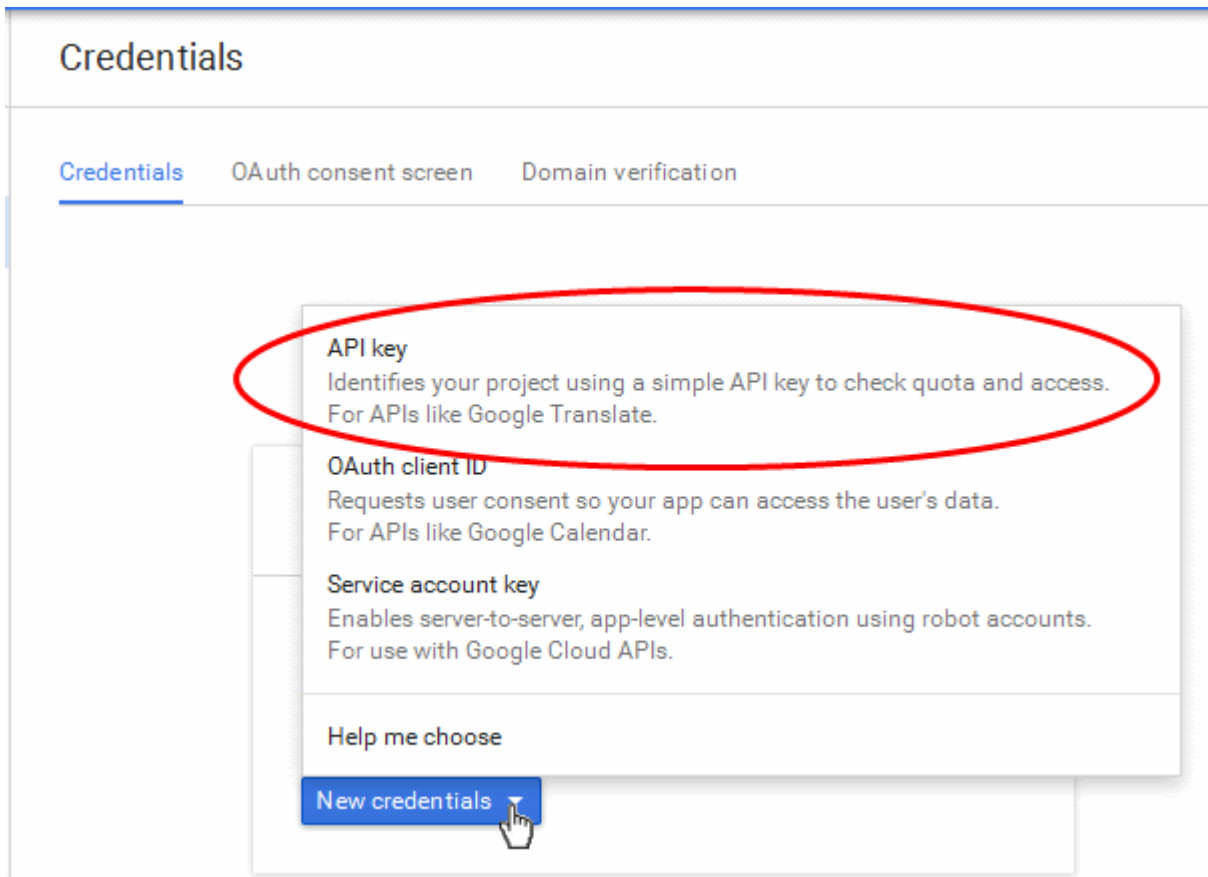
Using credentials with this API

Using an API key

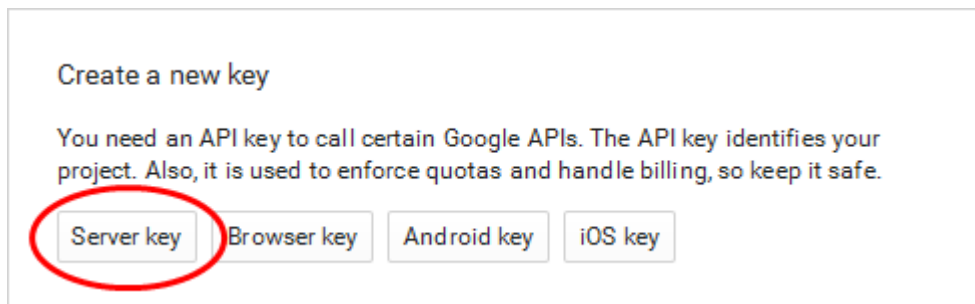
To use this API you need an API key. An API key identifies your project to check quotas and access. Go to the Credentials page to get an API key. You'll need a key for each platform, such as Web, Android, and iOS. [Learn more](#)

Your application API key

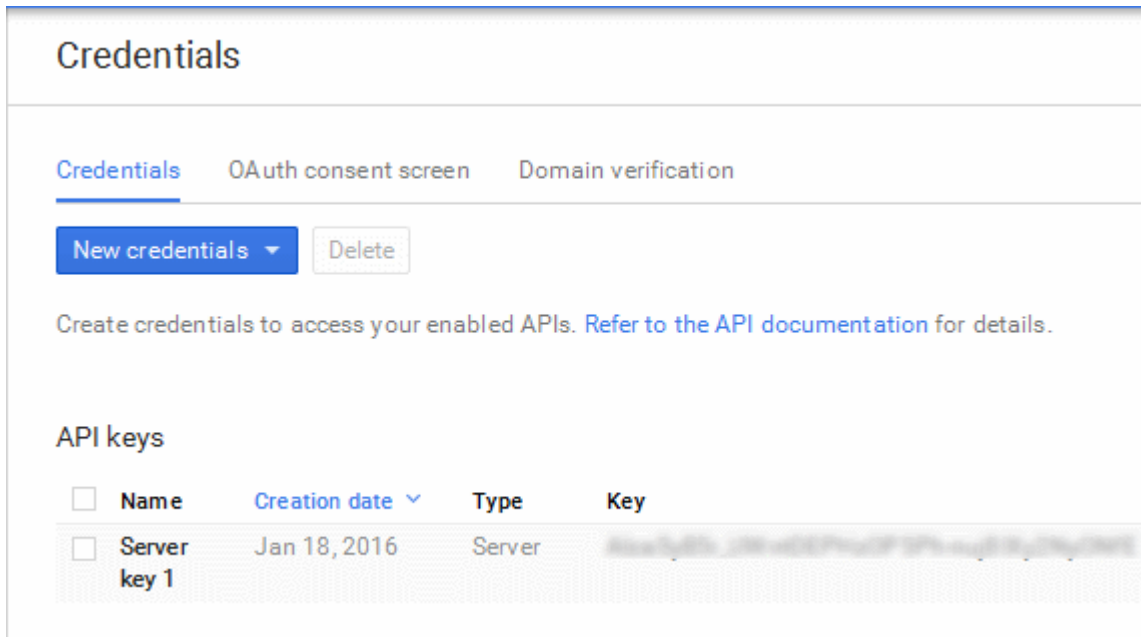
- **Step 5** - Choose 'Credentials' from the left hand side navigation and click on 'New Credentials' from the page at the right.



- **Step 6** - Choose 'API Key' from the New Credentials options and select 'Server Key' from the 'Create a new key' pop-up.

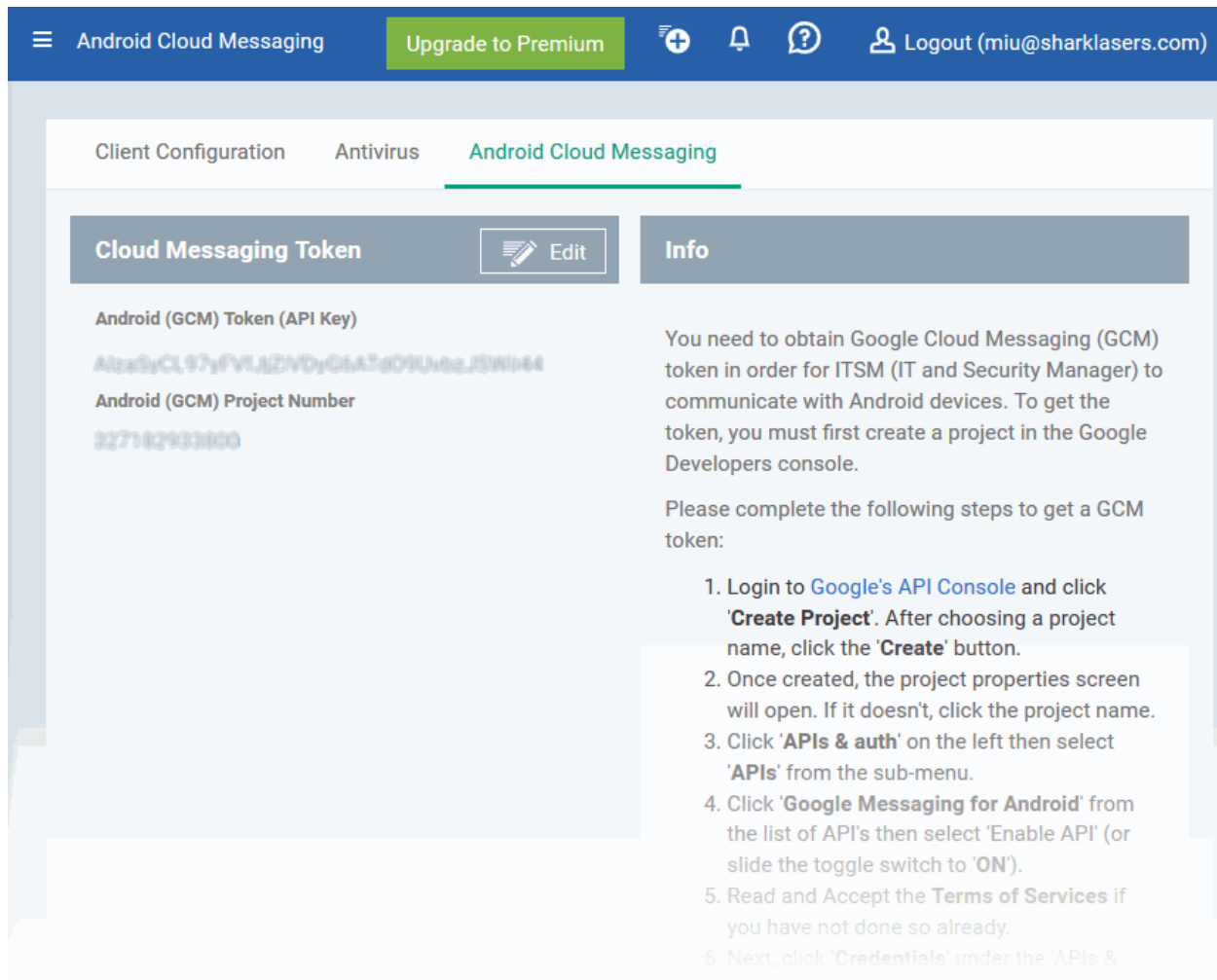


- **Step 7** - Enter a name for the key and leave the IP Address field blank in the next screen and click 'Create'.

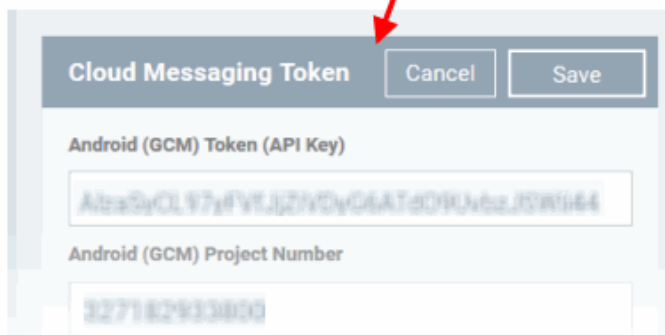
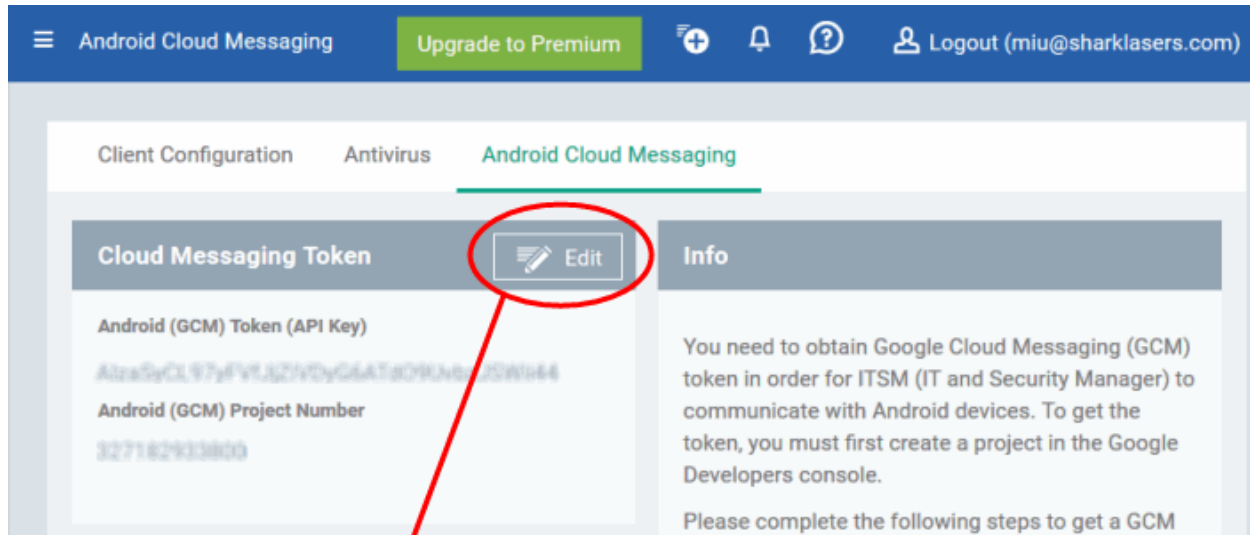


You need the API key and the project number to be entered in the ITSM interface.

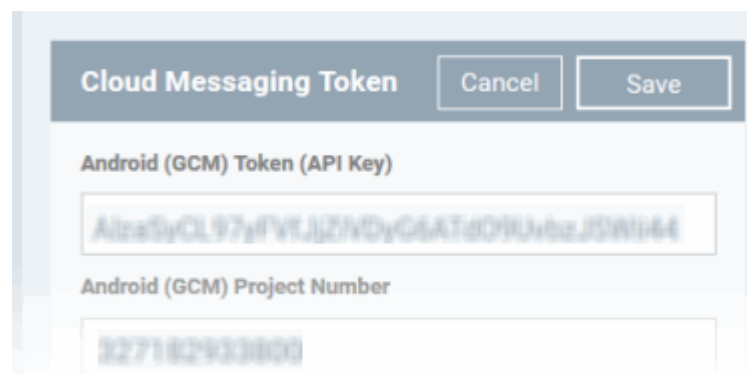
- Note down the API key in a safe place.
- **Step 9** - Next, login to ITSM. Click 'Settings' > 'Android Client Configuration' and choose 'Android Cloud Messaging' tab



- Click on the edit button  at the top right of the 'Cloud Messaging Token' column, to view the GCM token and project number fields

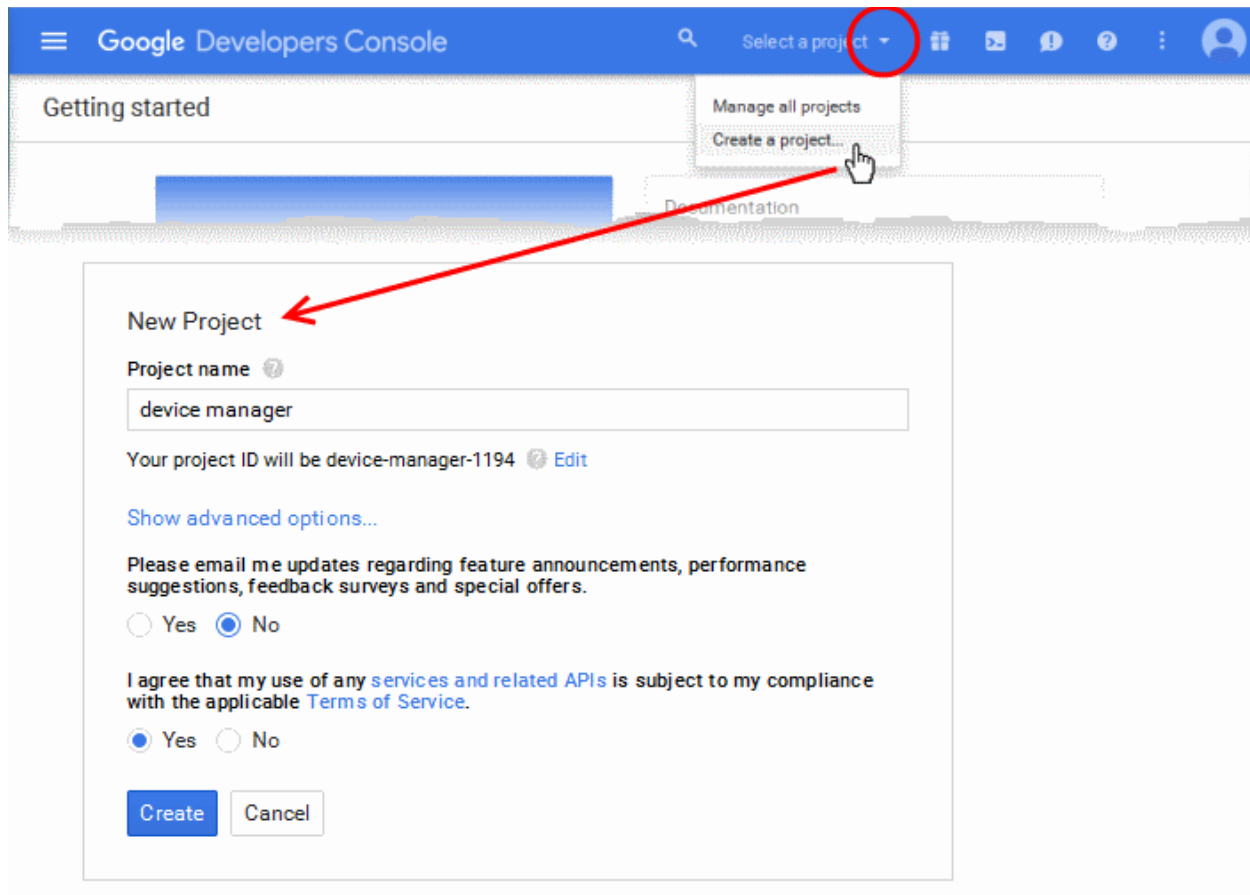


- Paste the API token to 'Android (GCM) Token' field.
- Enter the Project Number in the Android (GCM) Project Number field.



- 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.

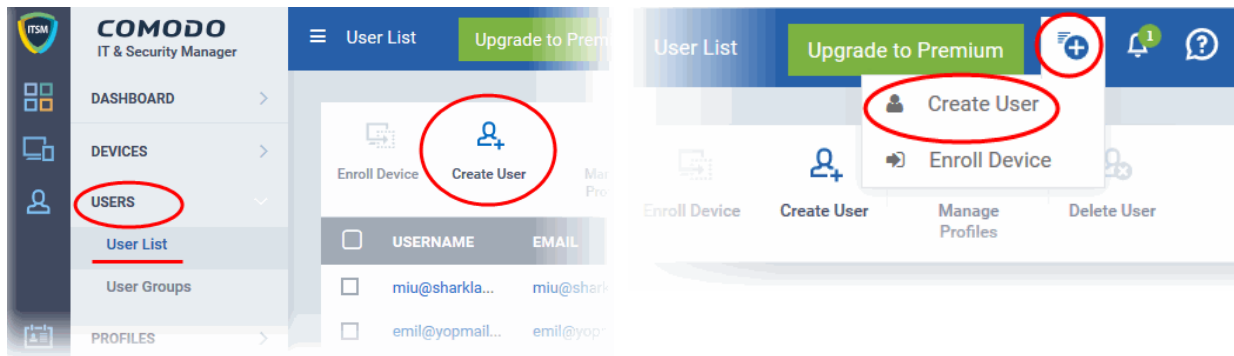
Step 3 – Add Users

The next step is to add users. Users' devices can be enrolled for management by ITSM only after adding them to the console.

- **Comodo One users** - if you created only one company in C1, then any users you enroll here will be automatically assigned to that company. If you created more than one company in C1, the 'Enroll User' dialog will allow you to choose the company to which you want to assign the user.
- **ITSM Users** - You can add users and enroll their devices without selecting any company. However, If you need the users/devices to be grouped under different companies, you can create companies in ITSM and add device groups under them as explained in **Step 5 - Create Groups of Devices**.

To add a user

- Click 'Users' on the left then 'User List', then click the 'Create User' button
or
- Choose 'Create User' from the drop-down at the top right:



The 'Create new user' form will open.

Create new User Close

Username *

Email *

Phone number

Company *

Assign role

- Type a login username (mandatory), email address (mandatory) and phone number of the user to be added.
- Choose the company (mandatory), from the 'Company' drop-down.
 - Comodo One Users - The drop-down will display the companies added to C1. You can choose the company to which the user belongs. The user will be enrolled under the chosen company.
 - ITSM users - Leave the selection as 'Default Company'.

- Choose a role for the user. A 'role' determines user permissions within the ITSM console itself. ITSM ships with two default roles:
 - **Administrators** - Full administrative privileges in the ITSM console. The permissions for this role are not editable.
 - **Users** - In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to ITSM.

You can create roles with different permission levels via the 'Role Management' screen (click 'Settings > 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. See [Configuring the Role-Based Access Control for Users](#) and [Managing Roles assigned to a User](#) for more details.

- 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 number of users.

If an administrator is added, an activation mail will be sent to their registered email address. The new administrator needs to activate their account and set the login password by clicking the activation link in the email.

Upon activation, the administrator will be able to login to ITSM with their user-name and password.

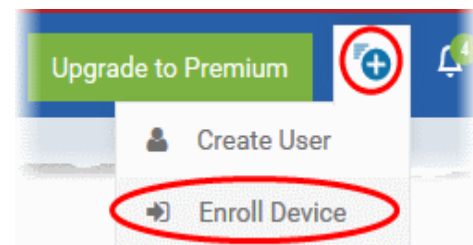
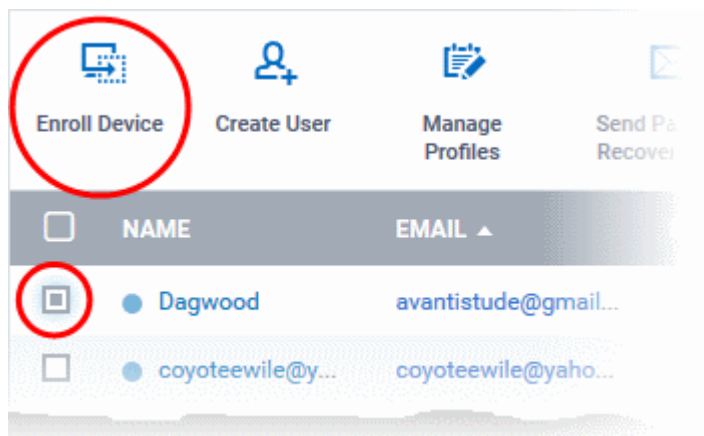
Step 4 - Enroll Users' Devices

The next step is to enroll users' devices for management.

Each user license allows you to enroll up to five mobile devices or one Windows endpoint per user (1 license will be consumed by 5 mobile devices. 1 license could also 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 if required.

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
- Choose 'Enroll Device' from the drop-down at top right



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

Enroll Devices Close

Please choose the device owner(s)

✕ Dagwood

Enroll Device(s)

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 the user from the search results drop-down.
- Click 'Enroll Device(s)'

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.



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://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/device/by/token/554fd18d57eef662e8b908a9a186f811

Sincerely, IT and Security Manager team.

- Clicking the link will open an enrollment page which contains links to download the ITSM app for Android, iOS, Mac OS X and Windows devices:




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:


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

 **FOR WINDOWS DEVICES**

Enroll by this link:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/windows/msi/token/554fd18d57eef662e8b908a9a186f811

 **FOR APPLE DEVICES**

1) Enroll by opening this link on your device:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/android/index/token/554fd18d57eef662e8b908a9a186f811

 **MANUAL ENROLLMENT**

Use the following settings:

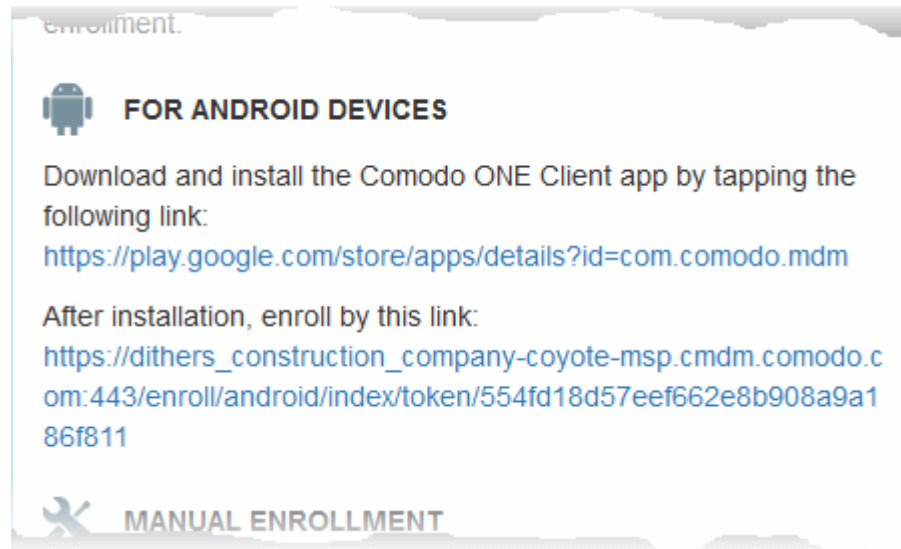
Host: **dithers_construction_company-coyote-msp.cmdm.comodo.com**
Port: **443**
Token: **554fd18d57eef662e8b908a9a186f811**

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

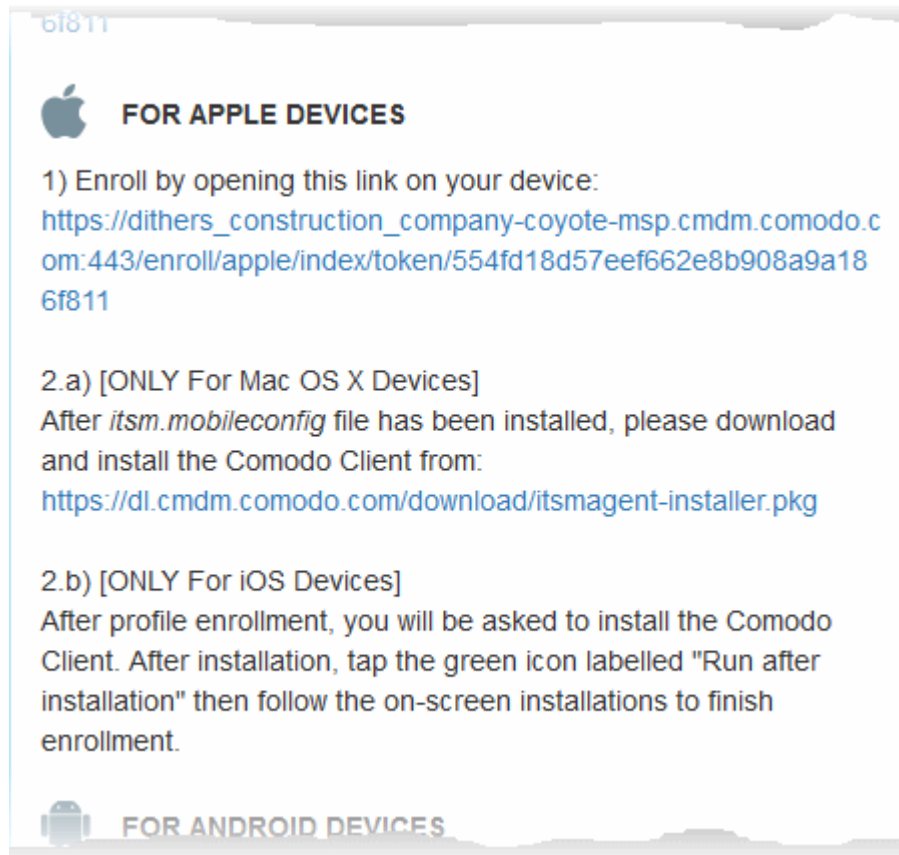
The device enrollment page contains two links under 'FOR ANDROID DEVICES'. The first to download the Android app and the second to enroll the device:



1. User opens the enrollment page on the target device and clicks the 1st link to install the ITSM app.
2. After app installation is complete, user clicks the 2nd link to enroll their device. The app will connect to ITSM and then the user needs to tap 'Activate' in the next screen. The app will automatically enroll the device with ITSM.

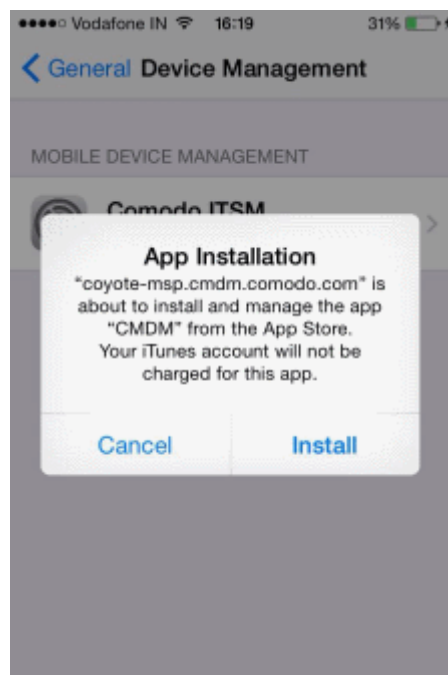
Enroll iPhones, iPods and iPads

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



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.

Upon successful completion of profile installation, the ITSM client app installation will begin. The app is essential for supporting the features such as apps management, GPS location and messaging from the ITSM console.



The app will be downloaded from iTunes store, using the user's iTunes account. The app is free, hence the user will not be charged for installing the app.

- The user needs to enter their Apple account password to access iTunes store.

The App will be installed.

- To complete the enrollment, the user needs to tap the green 'Run After Install' icon from the Home screen and accept to the EULA.

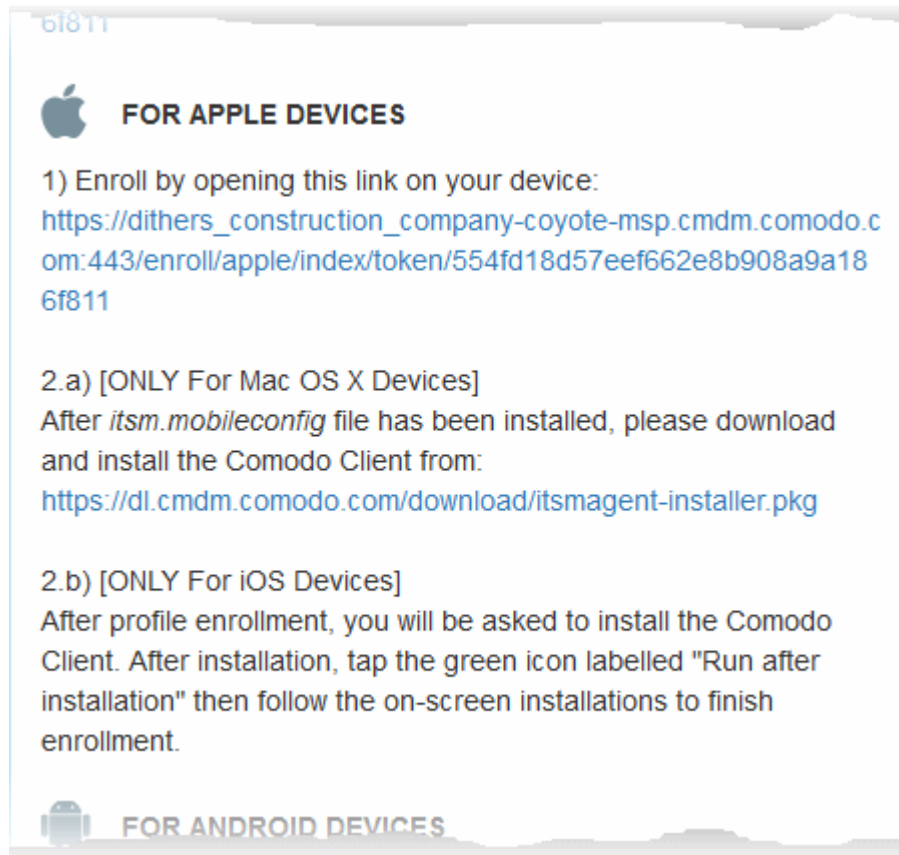


The device will be enrolled and connected to ITSM.

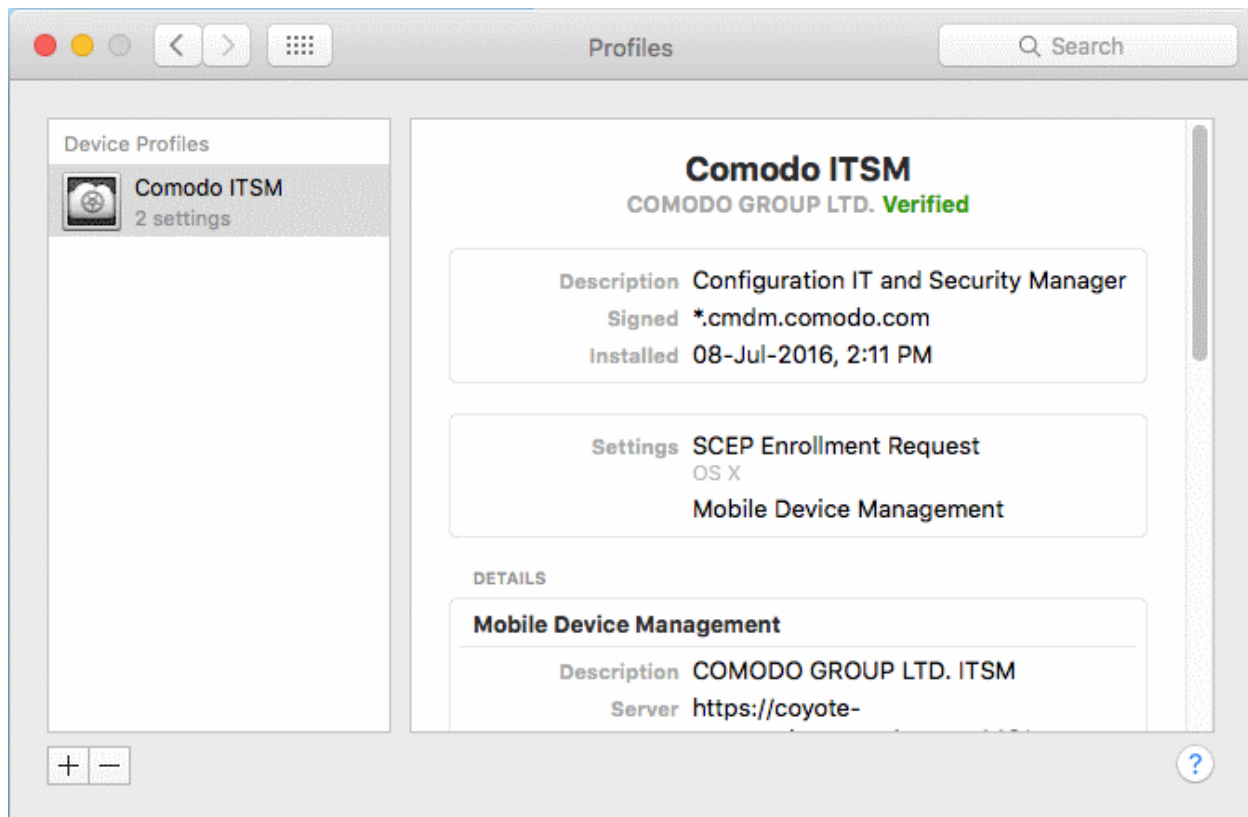
Enroll Mac OS X Devices

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.



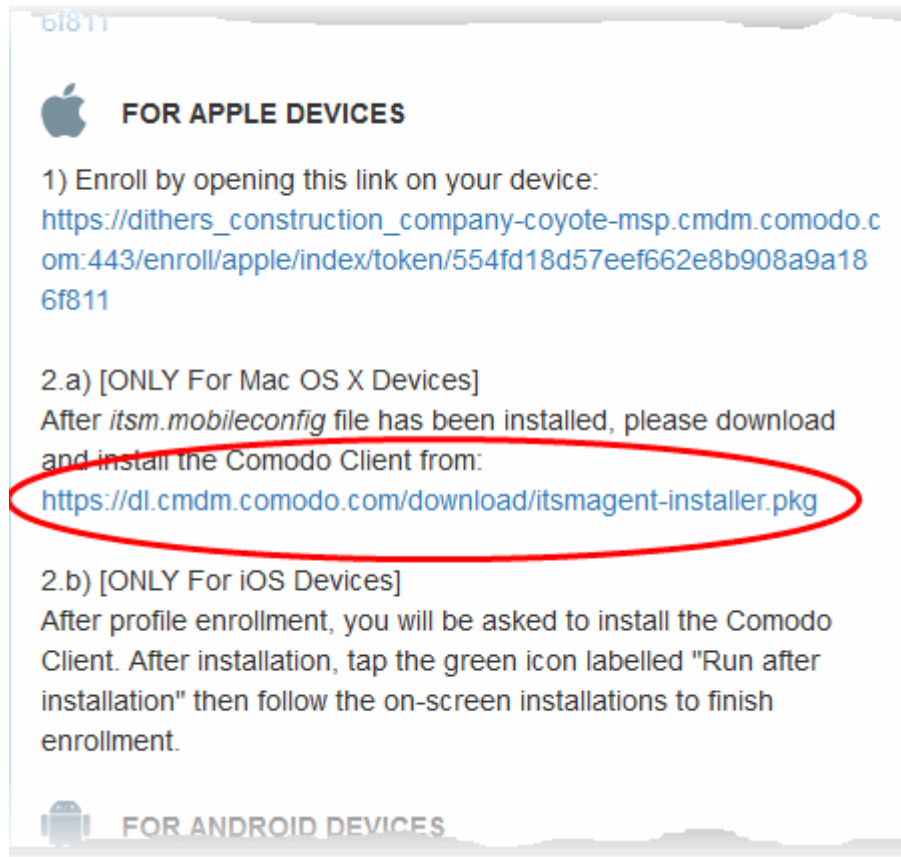
On completion of installation, the profile will be added to the Device Profiles list in the Mac OS X device.



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.

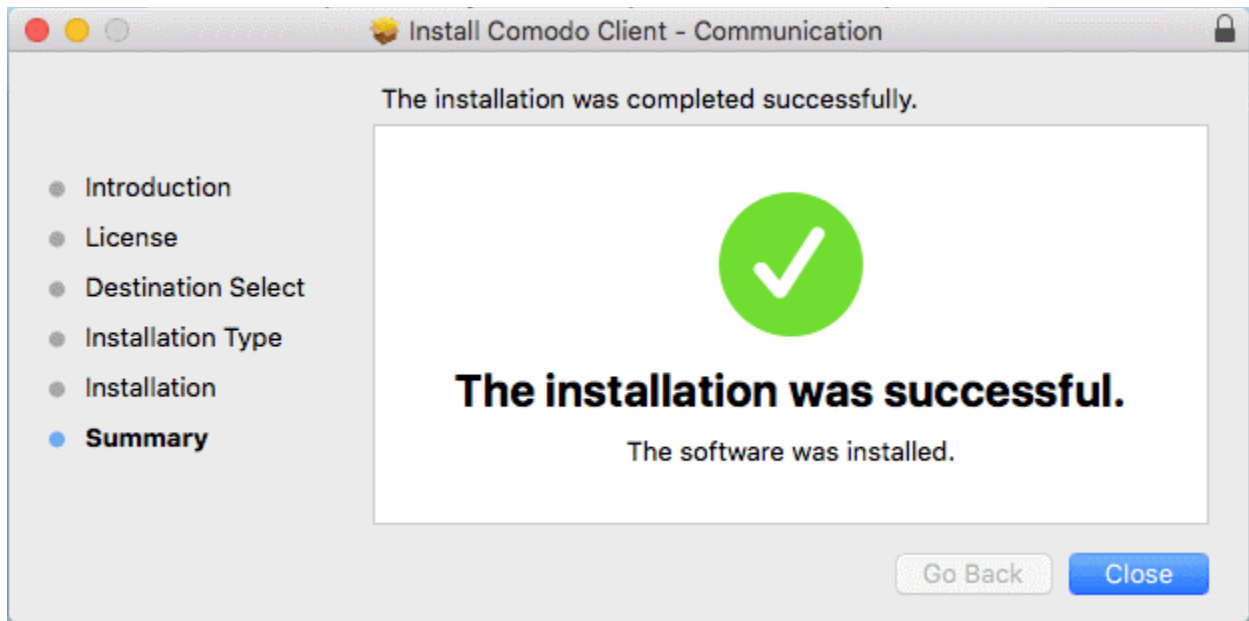


The agent setup package will be downloaded and the installation wizard will start.



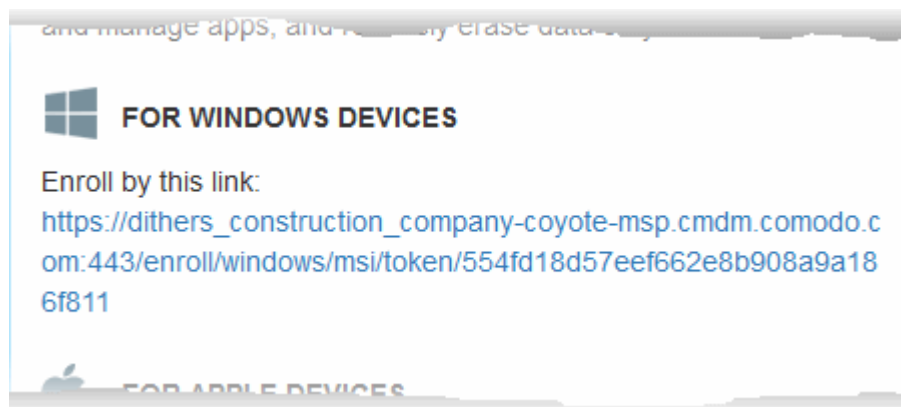
- The user follows the wizard and completes the installation.

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. Upon successful enrollment, ITSM will remotely install the endpoint security software Comodo Client Security (CCS) on to the device.

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

The screenshot shows the 'Device List' interface. At the top, there is a navigation bar with icons and labels for: Enroll Device, Manage Profiles, Takeover, Install MSI/Packages, Install OSX Packages, Siren Off, Siren On, Send Message, and More... Below this is a table with the following columns: OS, NAME, ACTIVE COMPONENTS, PATCH STATUS, COMPANY, OWNER, and LAST ACTIVITY. The first row is circled in red and contains the following data: OS: Windows, NAME: DESKTOP-8..., ACTIVE COMPONENTS: AG AV FW SB, PATCH STATUS: 1, COMPANY: Dithers Constru..., OWNER: Dagwood, LAST ACTIVITY: 2016/09/02 09:03:1... The second row contains: OS: Windows, NAME: DESKTOP-T..., ACTIVE COMPONENTS: AG AV FW SB, PATCH STATUS: 1, COMPANY: Dithers Constru..., OWNER: Angel Snow, LAST ACTIVITY: 2016/09/02 08:42:3... The third row is partially visible: OS: LENOVO Le..., ACTIVE COMPONENTS: AG AV FW SB, PATCH STATUS: 1, COMPANY: Dithers Constru..., OWNER: Angel Snow, LAST ACTIVITY: 2016/09/02 08:42:3...

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.

See [Devices](#) for more details.

Step 5 - Create Groups of Devices (optional)

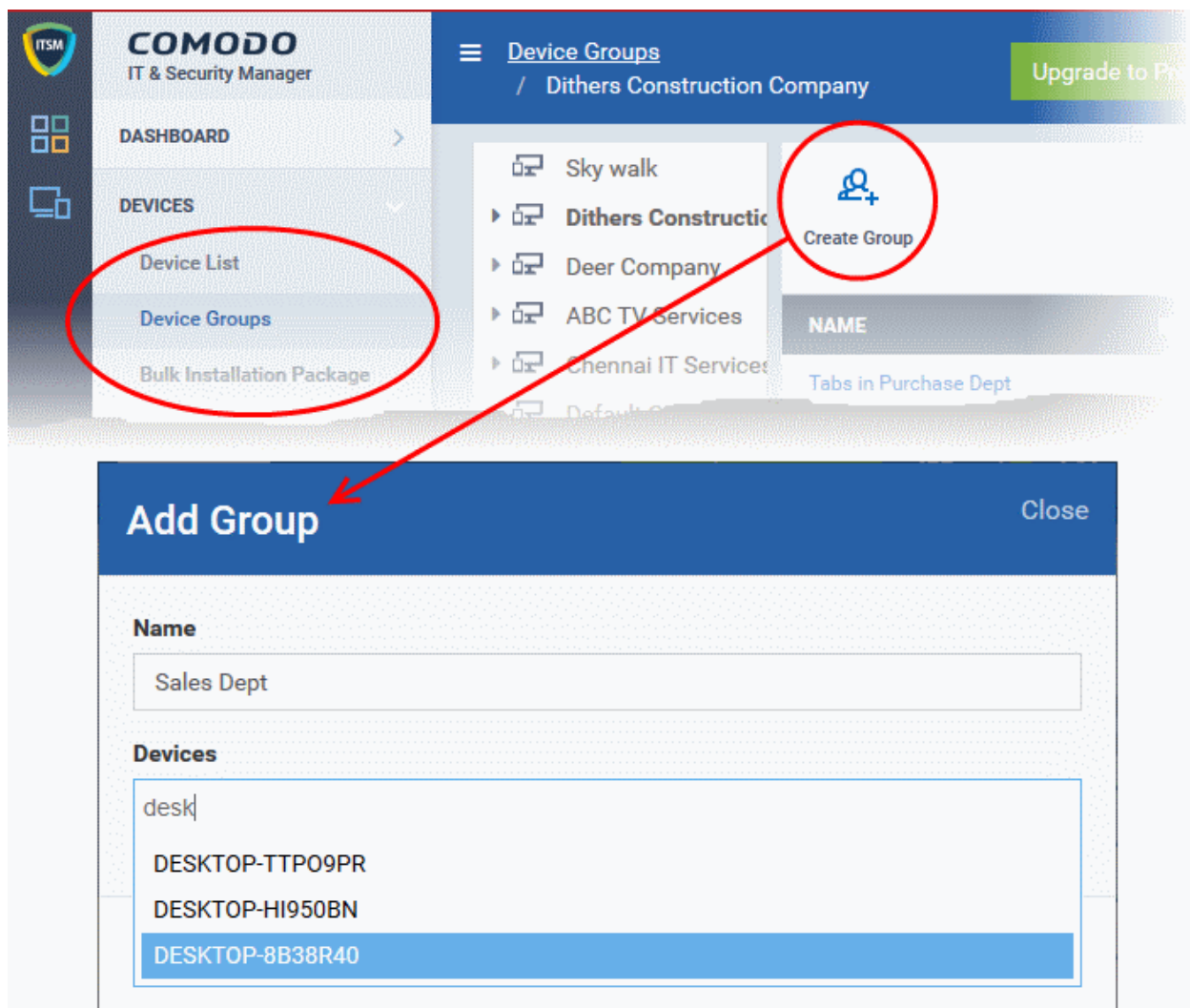
Administrators can create groups of Android, iOS and Windows devices that will allow them to view, manage and apply policies to large numbers of devices. Each group can contain devices of different OS types. Once created, the administrator can manage all devices belonging to that group together. Dedicated configuration profiles can be created for and applied for each group as per their requirements and the allowable user privileges and applied appropriately to the device groups. The profiles for different OS types applied to a group will be deployed on the devices of respective OS types.

Device Groups can be created under companies to which the device users belong. You should first have created at least one company in the Comodo One management console. Refer to [Managing Companies](#) if you need more help with this.

To create a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- Choose the Company under which you wish to create a new group from the left (optional)
- Click 'Create Group' from the top of the right pane

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 for adding more devices. You can also add devices after the group is created by clicking on the group name from the same screen > 'Add to Group' button and selecting the devices from the list.
- Click 'OK'. Repeat the process to create more groups. Refer to the section **Managing Device Groups** for more details.

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 mobile devices and PCs and Mac OS X devices that have been enrolled to Comodo IT and Security Manager. Each profile allows an administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.

If you designate a profile as 'Default', then it will be auto-applied to a device upon enrollment. Multiple profiles can be created to cater to the different security and access requirements of devices connecting to your network.

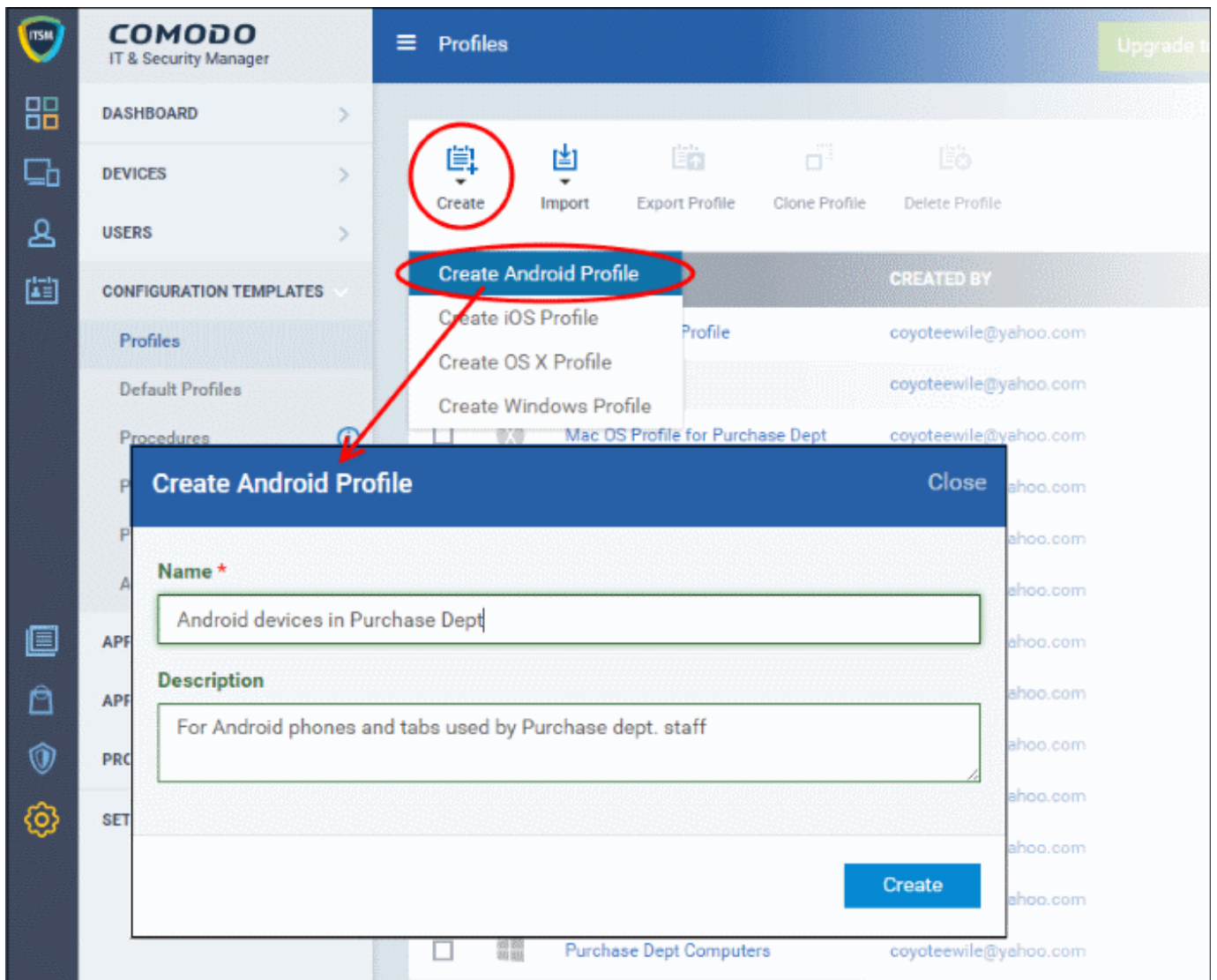
Profiles are applied at the time a device connects to the network. Profile settings will remain in effect until such time as the ITSM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

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

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

To create an Android Profile

- Click the 'Configuration Templates' tab at 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.

Android devices in Purchase Dept

Add Profile Section Export Profile Clone Profile Delete Profile


General

General Settings Edit

Name *
Android devices in Purchase Dept
Display name of the profile (shown on the device).

Is Default
Disabled

Description
For Android phones and tabs used by Purchase dept. staff
Brief explanation of the contents or purpose of the profile

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

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

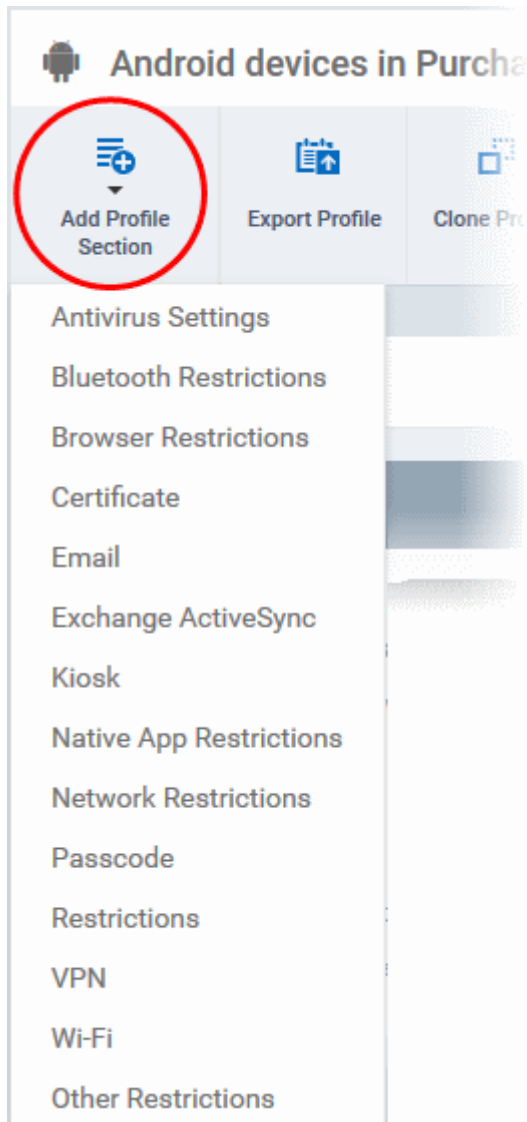
- Click the 'Add Profile Section' drop-down and select the component from the list that you want to include for the profile

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

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. 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.

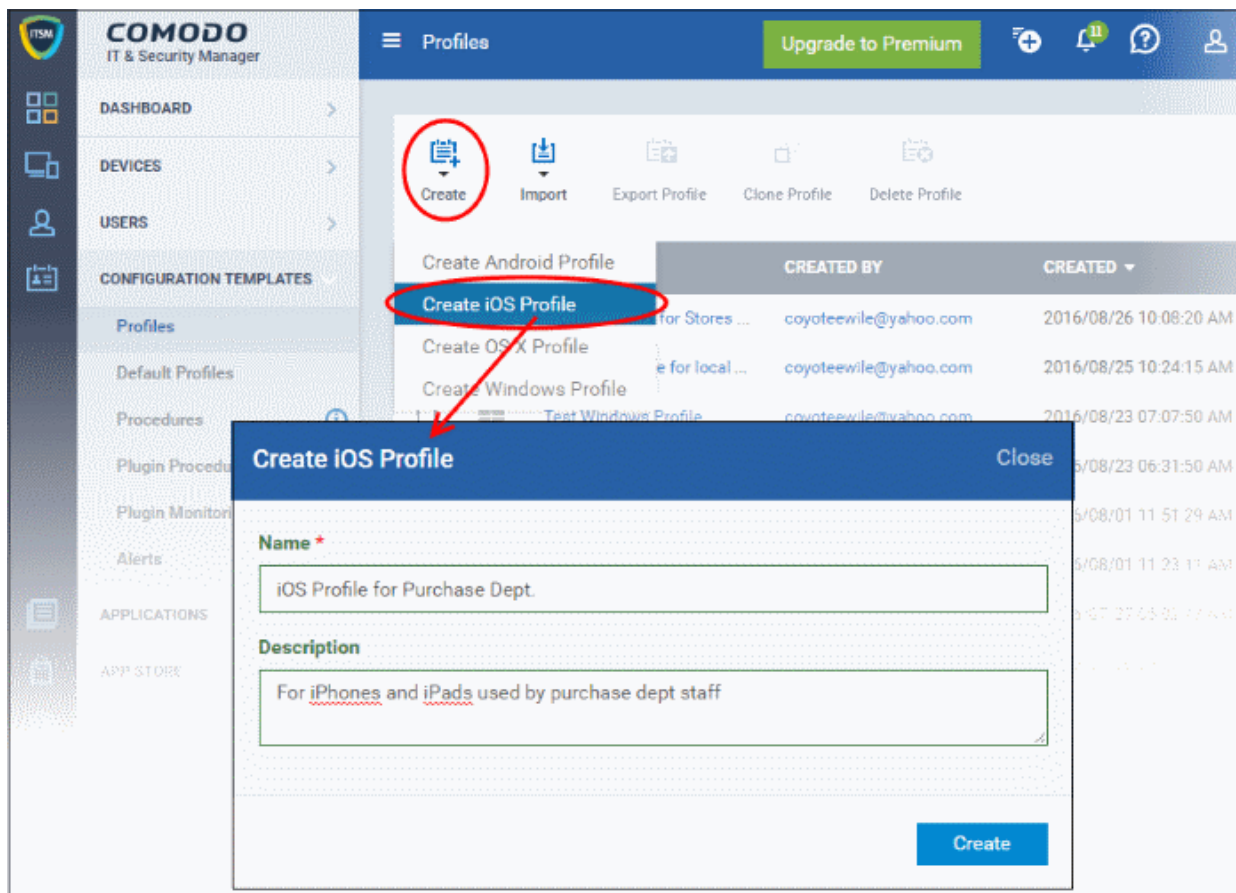


- **Browser Restrictions** - Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- **Certificate** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi', 'Exchange Active Sync', 'VPN' and so on.
- **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.
- **Exchange Active Sync** - 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.

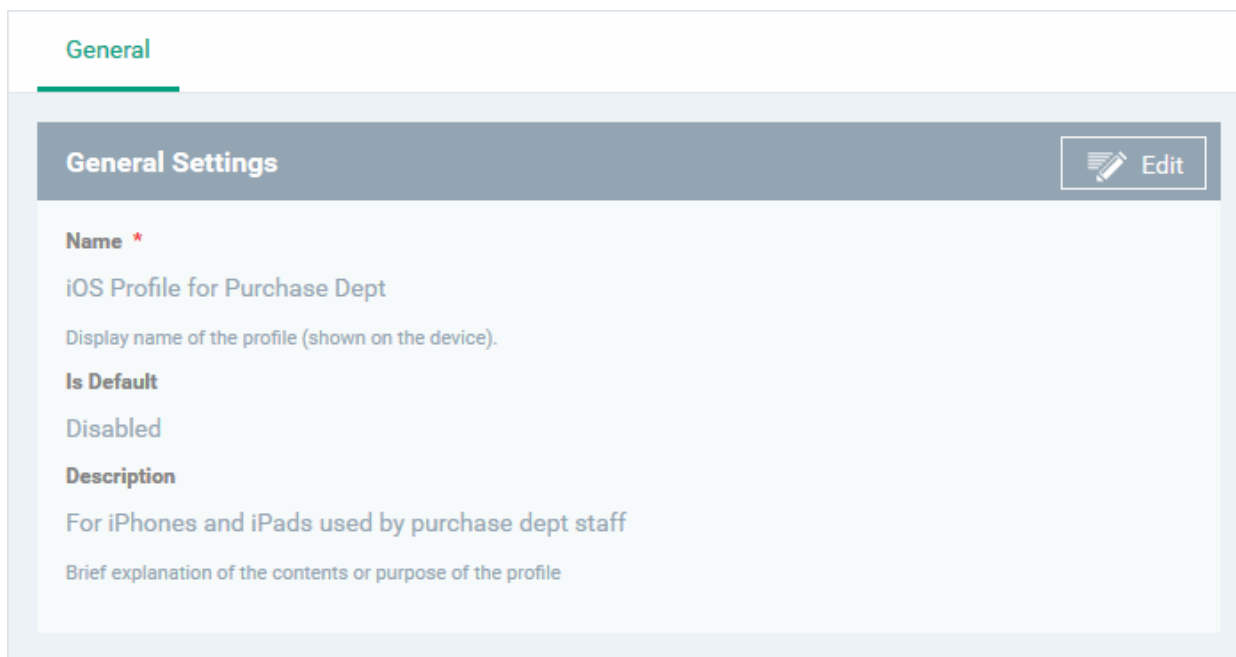
- **Network Restrictions** - Specify network permissions such as minimum level of Wi-Fi security required to access that Wi-Fi network, allow user to add more Wi-Fi networks in their devices, type of text and multimedia messages to be allowed and configure whitelist/blacklisted Wi-Fi networks. This profile 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 at the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then click 'Create iOS 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.



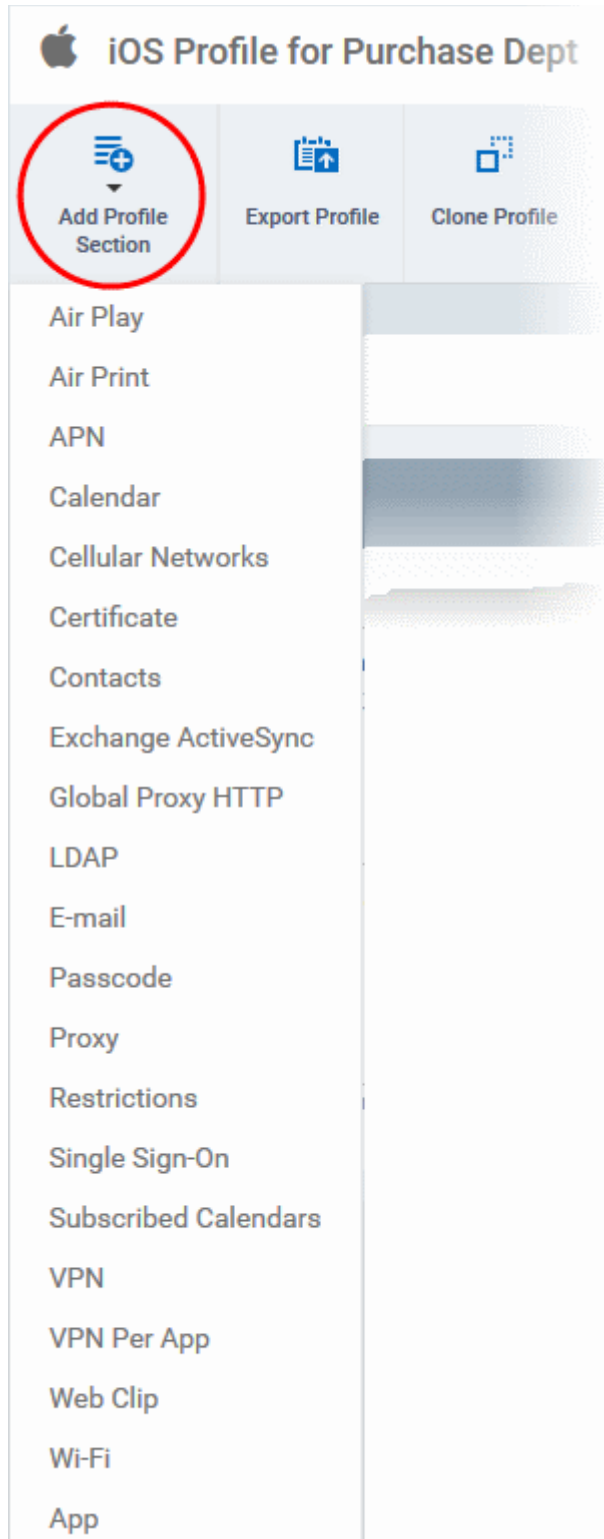
- If you want this profile to be a default policy, click on the 'Edit' button  at the top right of the

'General' settings screen and select the check box beside 'Is Default'.

- 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.

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:

- **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 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.

- **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).

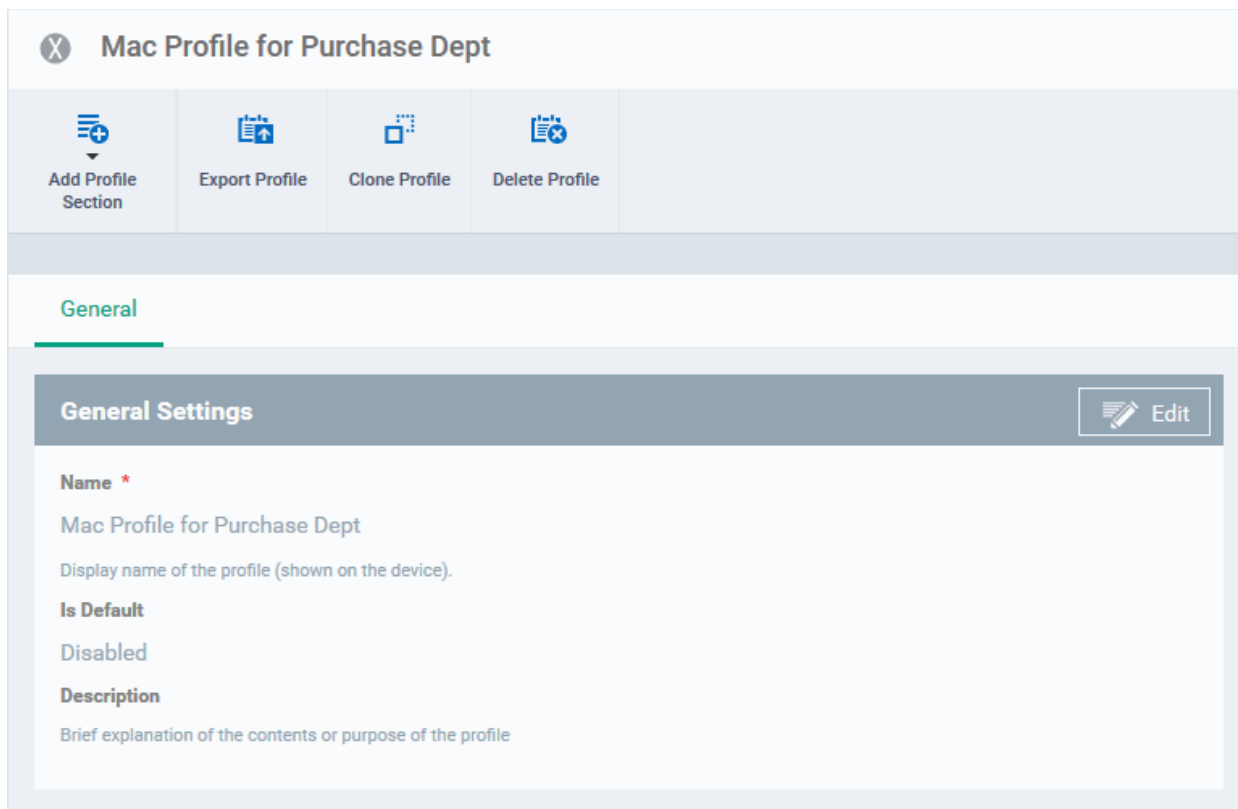
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.
- **Global HTTP Proxy** - Global HTTP proxies are used to ensure that all traffic going to and coming from an iOS device 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 Mac OS X Profile

- Click the 'Configuration Templates' tab at the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then click 'Create Mac OS X Profile'

The screenshot shows the Comodo IT & Security Manager interface. The left sidebar contains navigation options: DASHBOARD, DEVICES, USERS, CONFIGURATION TEMPLATES, and Profiles. The main content area is titled 'Profiles' and includes a 'Upgrade to Premium' button. Below the title are icons for 'Create', 'Import', 'Export Profile', 'Clone Profile', and 'Delete Profile'. A dropdown menu is open, showing options: 'Create Android Profile', 'Create iOS Profile', 'Create OS X Profile' (highlighted with a red circle), and 'Create Windows Profile'. A red arrow points from the 'Create OS X Profile' button to a modal window titled 'Create OS X Profile'. The modal window has a 'Close' button in the top right corner. It contains two text input fields: 'Name' (with a red asterisk indicating it is required) and 'Description'. A blue 'Create' button is located at the bottom right of the modal.

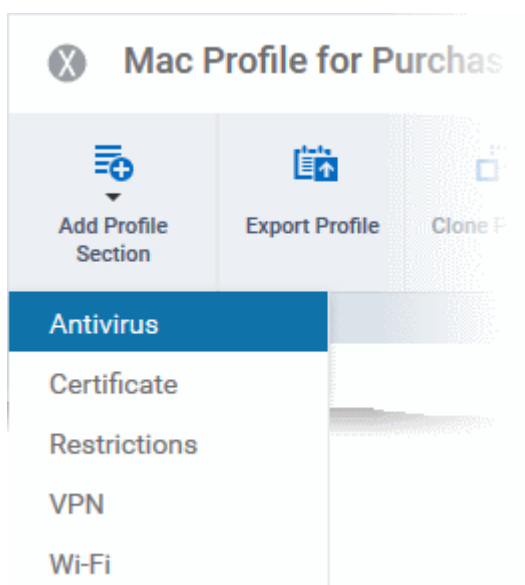
- Enter a name and description for the profile (for example, 'Sales Dept Mac machines', 'Mac Air Books' or 'Field Executives Laptops') and click 'Create'.
- The profile will be created and the 'General Settings' for the profile will be displayed.



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

The next step is to add components for the profile.

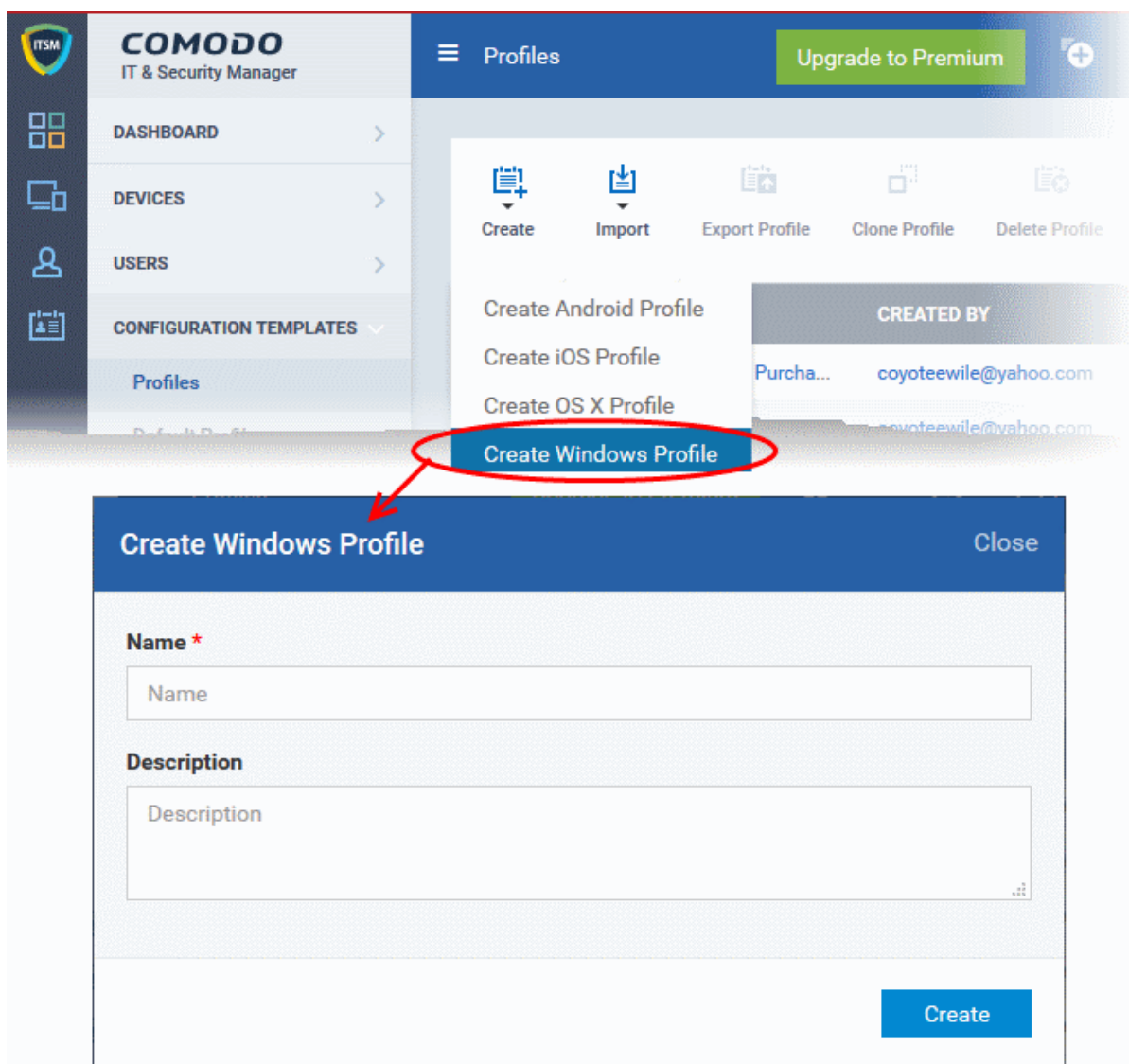
- Click the 'Add Profile Section' drop-down and select the component from the list that you want to include for the profile



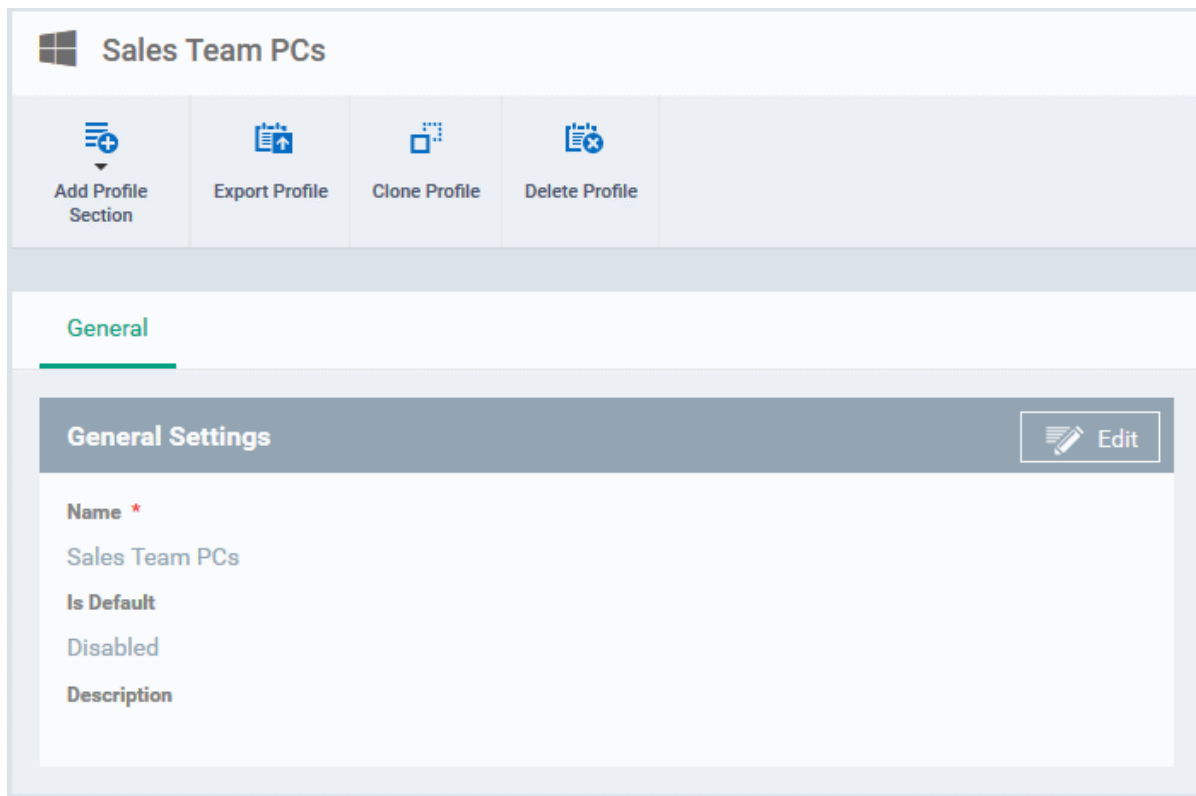
- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **Certificates** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings like 'Wi-Fi and 'VPN'.
- **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.


To create a Windows profile

- Click the 'Configuration Templates' tab at 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 on the 'Edit' button  at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- 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.

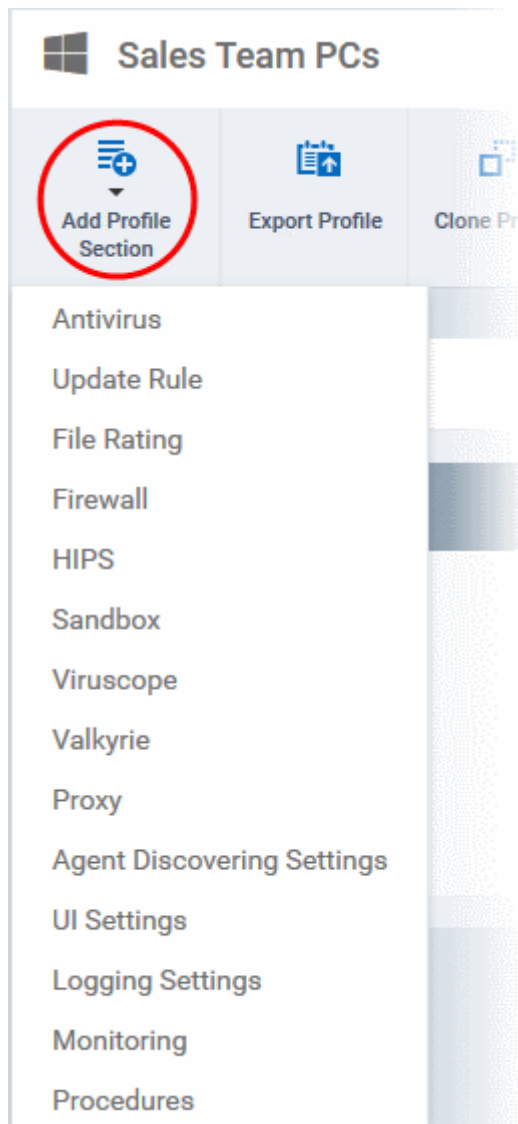
The settings screen for the selected component will be displayed and, after saving, the new section will become available as a link in this interface. You can configure Antivirus, Firewall, Sandbox, File Rating, Valkyrie, HIPS, Viruscope and Update settings. In addition, you can configure the Proxy and 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.

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.
- **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](#).



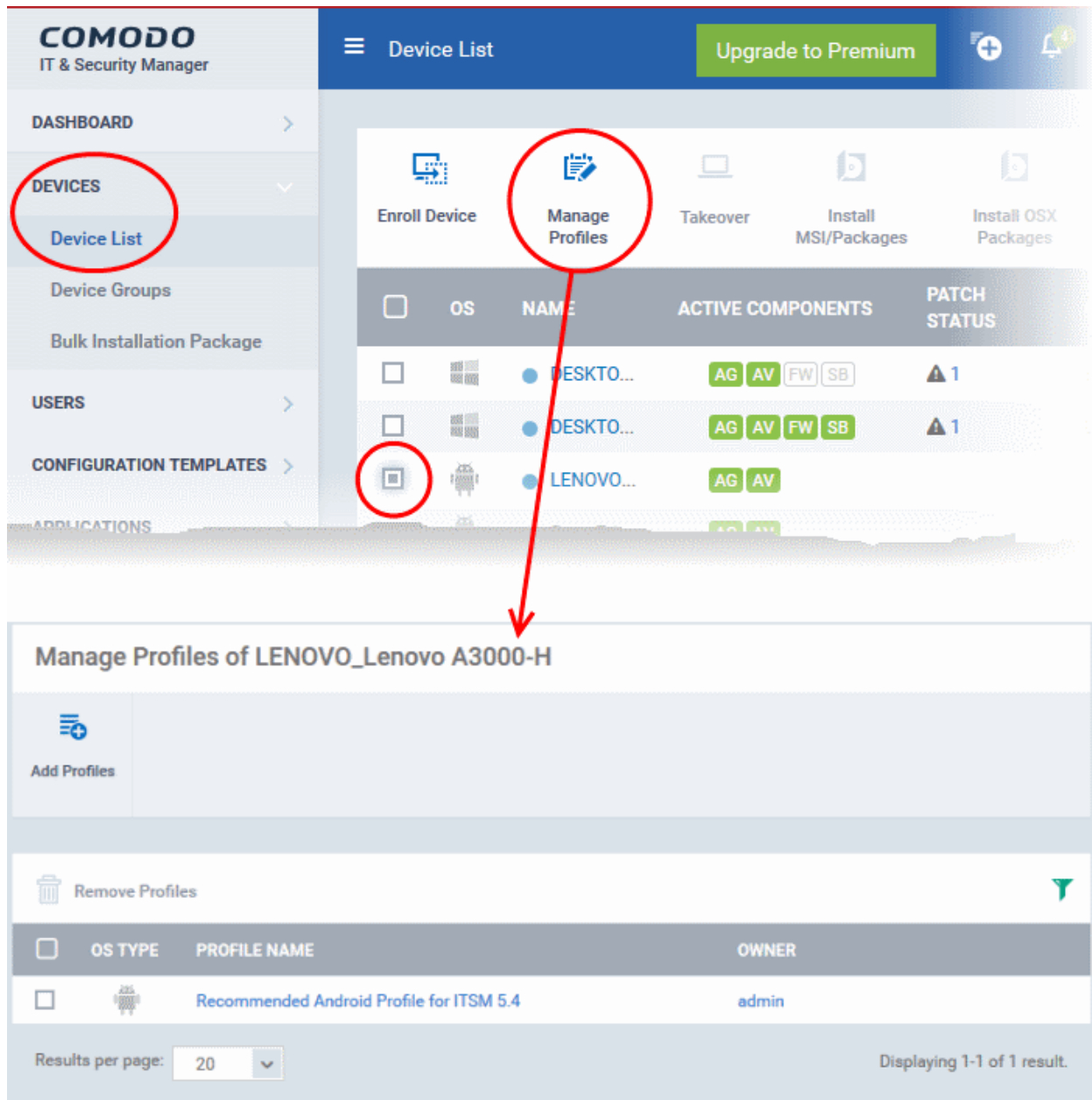
- **HIPS** - Enable Host Intrusion Prevention System (HIPS) and its behavior, configure HIPS rules and define Protected Objects at the endpoints. For more details on HIPS in CCS, refer to the [help page explaining HIPS Settings](#) in [CCS online help guide](#)
- **Sandbox** - Enable Auto-Sandboxing of unknown files, add exclusions, and configure sandbox behavior and alert options and view and manage Sandbox Rules for auto-sandboxing applications. For more details on Sandbox in CCS, refer to the [help page explaining Sandbox Settings](#) in [CCS online help guide](#).
- **Viruscope** - Enable Viruscope 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 Viruscope in CCS, refer to the [help page explaining Viruscope](#) 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 sandbox events.

- **CCS UI Settings** – Allows you to specify Comodo Client Security user interface settings.
- **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 and more.
- **Procedures** – Allows you to add, view, delete and prioritize procedures which have been added to a profile.

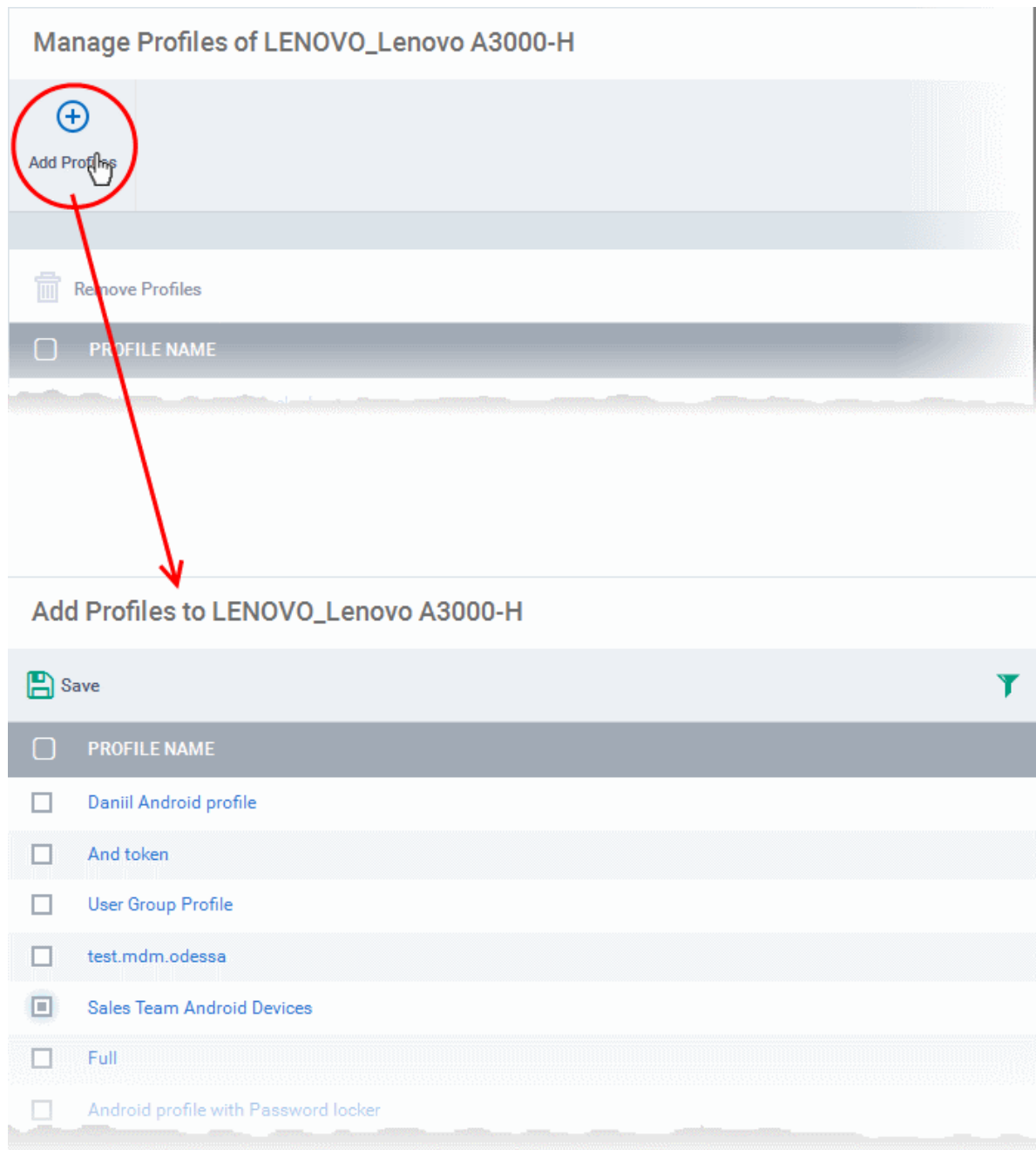
Step 7 - Apply Profiles to Devices or Device Groups

1. Click the 'Devices' tab from the left and choose 'Device List' from the options.
2. 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.

3. 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.

4. Select the profile(s) to be applied to the device
5. 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 from the left and choose 'Device Groups' from the options.
2. Choose the Company to view the list of groups in the right pane
3. Click on the name of the device group
4. Click 'Manage Profiles'
5. Select the profile(s) to be applied to the devices in the group

6. Click 'Add Selected' at the top left to add the selected profile(s) to the device group

If you have successfully followed all 6 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

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: EnterpriseSolutions@Comodo.com

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