COMODO
Creating Trust Online®

Comodo
IT and Security Manager

Software Version 6.2

Administrator Guide

Guide Version 6.2.021517

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

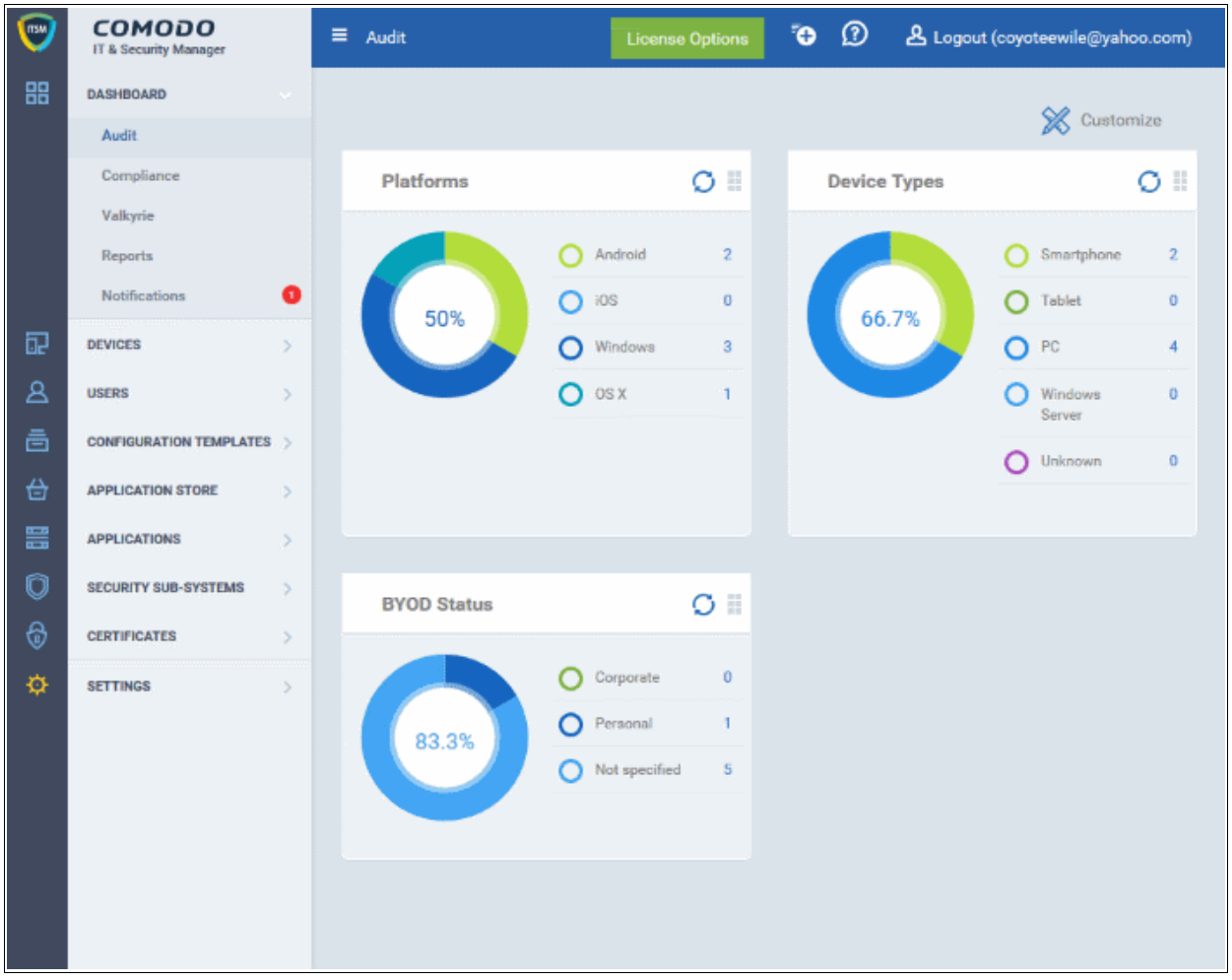
Table of Contents

1. Introduction to Comodo IT and Security Manager

Comodo IT and Security Manager (ITSM) allows administrators to manage, monitor and secure mobile devices and Windows and Mac OS endpoints which connect to their enterprise wired and wireless networks.

Administrators must first add users to the ITSM console and can then enroll devices like Android and iOS mobile devices and/or Mac OS X and Windows endpoints for those users. Once a device has been enrolled, administrators can remotely apply configuration profiles which determine that device's network access rights, security settings and general preferences. ITSM also allows you to obtain client certificates and device authentication certificates which can be used for user authentication, signing and encrypting email and device authentication (requires integration with Comodo Certificate Manager).

Administrators can monitor device location; run antivirus scans; install/uninstall apps; remotely lock or wipe devices; manage running services; generate extensive reports; reset user passwords; import users from Active Directory, manage Windows patches and more.



Each user license covers up to five mobile devices or one Windows endpoint for a single 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.

Guide Structure

This guide is intended to take you through the configuration and use of Comodo IT and Security Manager and is broken down into the following main sections.

Introduction to Comodo IT and Security Manager - Contains a high level overview of the service and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide.

The Administrative Console - Contains an overview of the main interface of ITSM and guidance to navigate to different areas of the interface.

The Dashboard - Describes the Dashboard area of the interface that allows the administrator to view a snapshot summary of devices and their statuses as pie-charts.

Users and User Groups - Covers the creation and management of users and user groups, enrollment of devices and assigning configuration profiles to devices.

- Managing Users
  - Creating New User Accounts
  - Enrolling Users Devices for Management
  - Viewing the Details of a User
  - Assigning Configuration Profile(s) to Users' Devices
  - Removing a User
- Managing User Groups
  - Creating a New User Group
  - Editing a User Group
  - Assigning Configuration Profiles to a User Group
  - Removing a User Group
- Configuring Role Based Access Control for Users
  - Creating a New Role
  - Managing Permissions and Assigned Users of a Role
  - Removing a Role
  - Managing Roles Assigned to a User

Devices - Covers management and control of enrolled devices, remotely generating sirens, wiping, locking and powering off enrolled devices, remotely installing and managing apps on devices and managing device groups.

- Device List
  - Managing Windows Devices
  - Managing Mac OS Devices
  - Managing Android/iOS Devices
  - Viewing the User Information
  - Removing a Device
  - Remote Management of Windows Devices
  - Remotely Installing Packages onto Windows Devices
  - Remotely Installing Packages on Mac OS Devices
  - Installing Apps on Android and iOS Devices
  - Generating Alarm on Device
  - Locking/Unlocking Selected Devices
  - Wiping Selected Devices
  - Assigning Configuration Profiles to Selected Devices
  - Setting / Resetting Screen Lock Password for Selected Devices
  - Updating Device Information
  - Sending Text Message to Devices
  - Restarting Selected Windows Devices
  - Changing A Device's Owner

App Store - Covers the management of applications that can be pushed to enrolled devices from the ITSM console.

- iOS Apps
  - Adding iOS Apps and Installing them on Devices
  - Managing iOS Apps
- Android Apps
  - Adding Android Apps and Installing them on Devices
  - Managing Android Apps

Security Sub-Systems- Describes how obtain trust ratings for files on your devices, run AV scans, run AV scans, view threats, manage quarantined items and more.

- Viewing Contained Applications
- Viewing Applications Installed on Windows Devices
  - Viewing and Managing Unrecognized Files
  - Viewing and Managing Trusted Files
  - Viewing and Managing Malicious Files
  - Viewing and Managing Quarantined Items
- Viewing and Managing Quarantined Items on Mac OS Devices
- Viewing list of Valkyrie Analyzed Files
- Antivirus and File Rating Scans
  - Running On-Demand Antivirus Scans on Devices
  - Running Rating Scans on Windows Devices
  - Handling Malware on Scanned Devices
  - Updating Virus Signature Database on Windows Devices
  - Updating Virus Signature Database on Mac OS Devices
- Viewing and Managing Identified Malware
- Viewing Threats History
- Viewing History of External Device Connection Attempts

Managing Certificates Installed on Devices - Manage client and device authentication certificates issued through Comodo Certificate Manager to enrolled users and devices

Configuring Comodo IT and Security Manager - Explains how to set up your ITSM portal to communicate with enrolled Android and iOS devices, how to integrate AD servers and import user groups and how to configure the Windows client and various ITSM components. Also covers management of subscriptions and renewal/upgrade of licenses.

- Email Notifications, Templates and Custom Variables
  - Configuring Email Templates
  - Configuring Email Notifications
  - Creating and Managing Custom Variables
  - Creating and Managing Registry Groups
  - Creating and Managing COM Groups
  - Creating and Managing File Groups
- ITSM Portal Configuration
  - Importing User Groups from LDAP
  - Adding Apple Push Notification Certificate
  - Configuring the ITSM Android Agent
  - Configuring ITSM Windows Client

1.1. Key Concepts

Mobile Device - For the purposes of this guide, a mobile device is any Android or iOS smart phone or tablet that is allowed to connect to the enterprise network through a wireless connection. Comodo IT and Security Manager allows network administrators to remotely configure device access rights, security settings, general preferences and to monitor and manage the device. Mobile devices may be employee or company owned.

Windows Endpoints - For the purposes of this guide, a Windows Endpoint is any Windows laptop, desktop or server computer that is allowed to connect to the enterprise network through a wireless or wired connection. Comodo IT and Security Manager allows administrators to install Comodo Client Security, manage security settings on them, view and manage installed applications, run antivirus scans manage OS update/security path installation and more. Windows Endpoints may be employee or company owned.

Mac OS X - For purpose of this guide, Mac OS X is Mac Endpoints with version 10 of the Apple Macintosh operating system. ITSM allows administrators to install Comodo Antivirus for Mac, manage secure settings on them, deploy required profiles on them and more.

User - An employee or guest of the enterprise whose device(s) are managed by the ITSM console. Users must be created before their devices can be added. Users can be added manually or by importing user groups from an AD server.

Device Group - An administrator-defined grouping of Android, iOS and/or Windows devices that allows administrators to apply configuration profile(s) to multiple devices at once.

Quarantine - If the antivirus scanner detects a malicious application on an Android device then it may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any infected files moved into quarantine are encrypted so they cannot run or be executed.

Configuration Profile - A configuration profile is a collection of settings applied to enrolled device(s) which determine network access rights, overall security policy, antivirus scan schedule and other preferences. Profiles are split into iOS profiles, Android profiles and Windows profiles. Profiles can be applied to an individual device, to a group of devices, selected users' devices or designated as a 'default' profile.

Comodo Client Security - Comodo Client Security (CCS) is the remotely managed endpoint security software installed on managed Windows devices. It offers complete protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, an advanced host intrusion prevention system (HIPS) and Containment feature that runs unknown and unrecognized applications in an isolated environment at the endpoints. Each component of CCS can be configured to offer desired security level by applying configuration profiles.

Default Profile - Default profiles are immediately applied to a device when it is first enrolled into ITSM. Default profiles are split into four types - iOS default profiles, Mac OS X default profiles, Android default profiles and Windows default profiles. Multiple default profiles can be created and applied to a device or group of devices.

ITSM Agent - The agent is an app which needs to be installed on all enrolled devices to facilitate communication with the ITSM server. The agent app is responsible for receiving and executing tasks such as implementing configuration profiles, fetching device details, running antivirus scans, adding or removing apps and to lock or wipe the device.

Notifications - Notifications are sent to devices by ITSM after events like the installation or removal of an app or

because a threat has been identified on the device. For identification of threats during on-access, scheduled or on-demand scanning on Android and Windows devices, the notifications are generated at the web interface for the administrator.

Patch Management - The Patch Management involves monitoring the security and update patches for various versions of Windows operating systems released from time to time by software vendors, identifying patches appropriate for the OS version of each managed Windows device and installing missing patches on to them. ITSM is capable identifying patch status of each managed endpoint and apply missing patches.

Remote Monitoring and Management - Remote Monitoring and Management (RMM) Module is an efficient endpoint monitoring application that allows administrators to monitor and manage multiple endpoints from one centralized console. RMM is available as a ITSM extension to Comodo One customers and can be accessed from the ITSM interface.

Valkyrie - Valkyrie is a cloud-based file verdicting service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. CCS on managed Windows computers can automatically submit unknown files to Valkyrie for analysis. The results of these tests produce a trust verdict on the file which can be viewed from the ITSM interface.

Active Directory - ITSM allows administrators to add multiple Lightweight Directory Access Protocol (LDAP) accounts for the purpose of importing user groups and users.

1.2. Best Practices

1. Default profiles are automatically applied to a device when it is first enrolled. It is prudent, therefore, to keep them as simple as possible as you can always deploy more refined profiles later. For example, you can set up passcode complexity and encryption profiles that will provide immediate, protection for enrolled devices. Default profiles will also be applied to devices when:
    - Currently active policies are removed
    - A device is removed from a device group

    See Managing Default Profiles for more information.

2. Though it is possible to save all settings in a single profile, an option worth considering is to create separate profiles dedicated to the implementation of a single setting group (remember, many profiles can be applied at once to a device or group). For example, you could name a profile 'Android_passcode_profile' and configure only the passcode rules. You could create another called 'Android_VPN_settings' and so on. A system like this would allow you to construct bespoke profiles on-the-fly from a pool of known settings. Adding or removing a profile from a device would let you quickly troubleshoot if a particular setting is causing issues.

    See Creating Configuration Profiles for more details.

3. Each ITSM license allows you to enroll up to five mobile devices or one Windows/ Mac endpoint for a single user. If more than 5 devices or 1 endpoint are enrolled for one particular user, then an additional license will be consumed. We encourage admins to evaluate the average number of devices per user and to set max. enrollments accordingly.

    Refer to Enrolling Users' Devices for Management for more details.

4. Creating a group of devices is a great time-saver if the policies applied to them are going to be the same.

    Refer to the section Managing Device Groups for more details.

5. The first level of defense on any device is to set a complex passcode policy. ITSM allows you specify passwords which are a combination of numbers, letters, special symbols and of a minimum length set by you. You can also set passcode lifetimes, reuse policy and define whether data should be automatically wiped after a certain number of failed logins.

6. Decide what restrictions are required for *your* company and *your* users. For example, disabling cell-phone cameras might be expected and mandatory in certain corporate environments but could be seen as a

savage affront to liberties in more relaxed offices. ITSM offers flexible restrictions for Android devices over items such as Wi-Fi, packet data, bluetooth connectivity and use of camera. iOS restrictions are much more granular and also include App purchases, game center, voice dialing and more.

Refer to the restriction sections in Profiles for Android Devices and Profiles for iOS Devices for more details.

7. Keeps an eye on the apps you allow in your organization. Apps can be useful and productive to your employees but some may pose a malware or data-leak risk for your organization. ITSM provides you the ability to blacklist and whitelist apps, to govern how apps behave and to determine whether users are allowed to install apps from 3rd party vendors.

   Refer to the section Viewing Applications Installed on Enrolled Devices for more details.

8. Keeping enrolled devices free from malware is vital to your organization's security. It is advisable to run antivirus scans on devices regularly per your company's needs. ITSM allows you to create a scheduled antivirus scan profile that automates the process of AV scans. If needed, AV scans can also be run instantly for selected devices or all enrolled devices.

9. ITSM interface can be accessed by administrators with different administrative roles and the activities performed by them depends on the roles assigned to them. Privileges to administrative roles should be according to organizational hierarchy and requirements. ITSM allows to configure different roles with different privileges and assign them to administrators as per organizational needs. Refer to the section Configuring the Role-Based Access Control for Users for more details.

10. Check the devices statuses regularly for compliance of deployed profiles and other reports. ITSM provides at-a-glance view of platform details of devices, types of devices and other reports. Refer to the sections The Dashboard and Device List for more details.

1.3. 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.

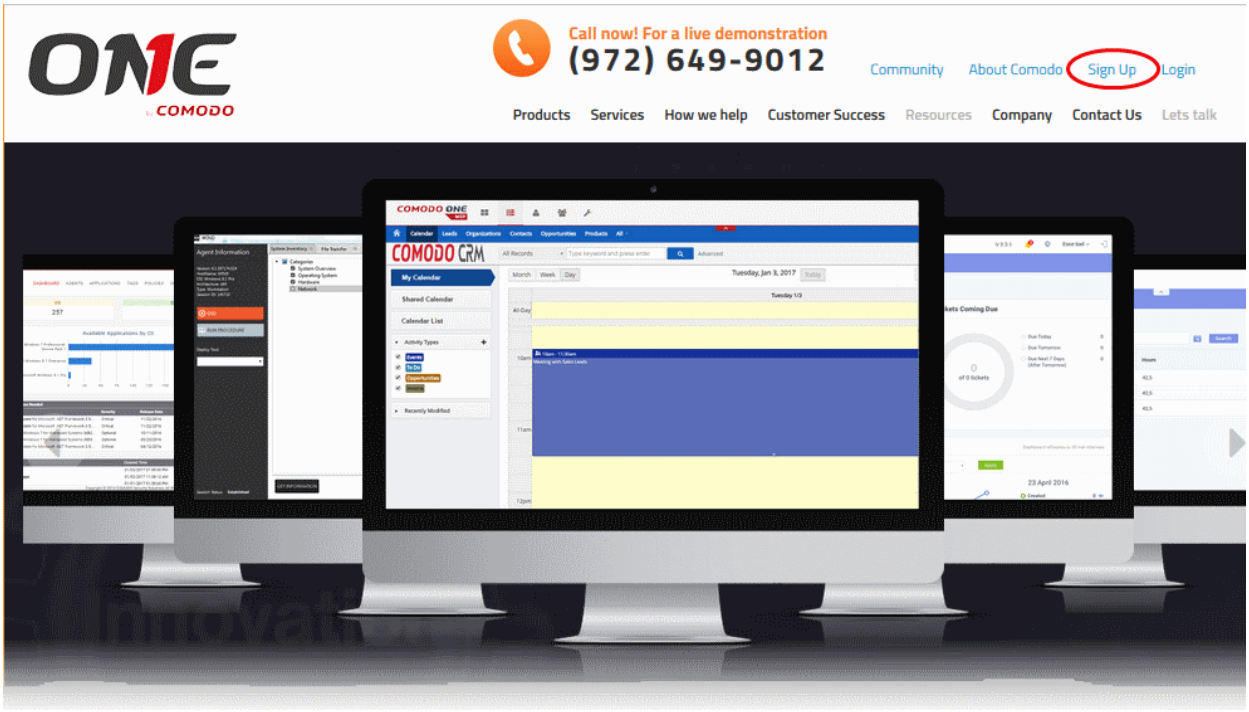
Step 1 - Enrollment and Configuration

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** account then you can access the ITSM console by logging in at https://one.comodo.com/app/login then clicking 'Licensed Applications' > 'IT and Security Manager'.

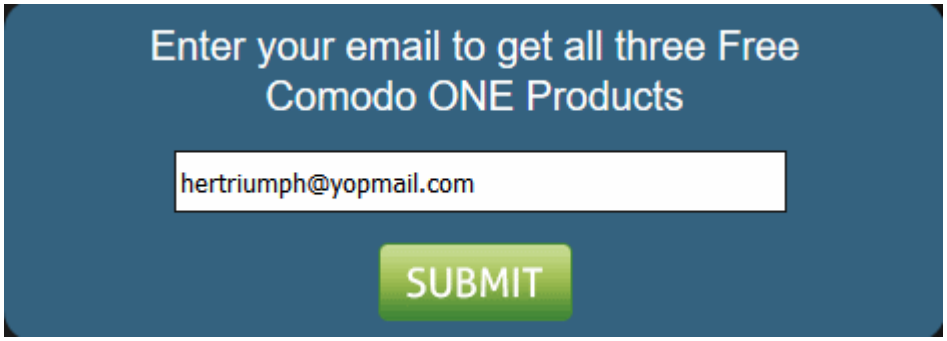
For more details on Comodo One and the services offered with the Comodo One Package, refer to the online help guide at https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html

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



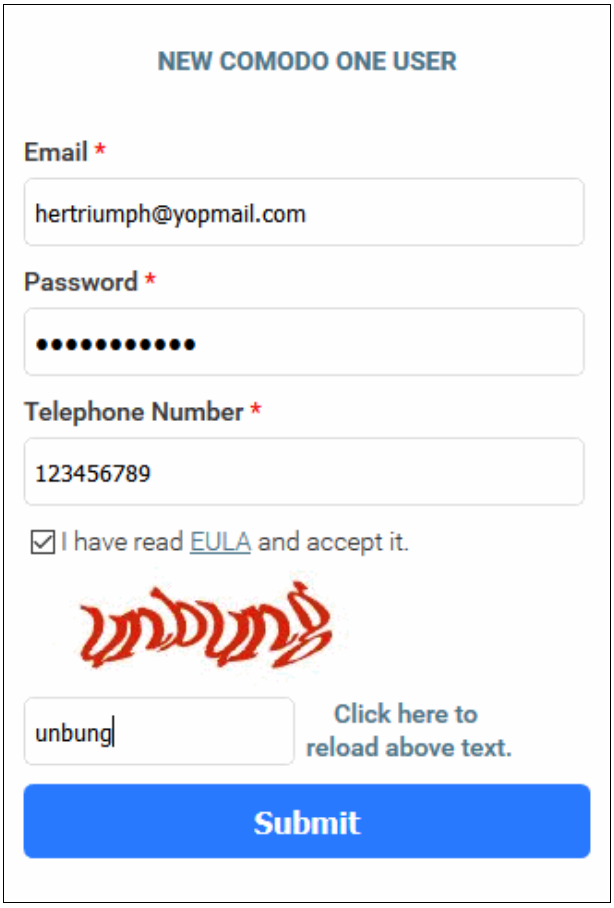
You will be taken to the enrollment wizard for Comodo One subscription.



- Enter your email address and click 'Submit'

Next, complete the short enrollment form:

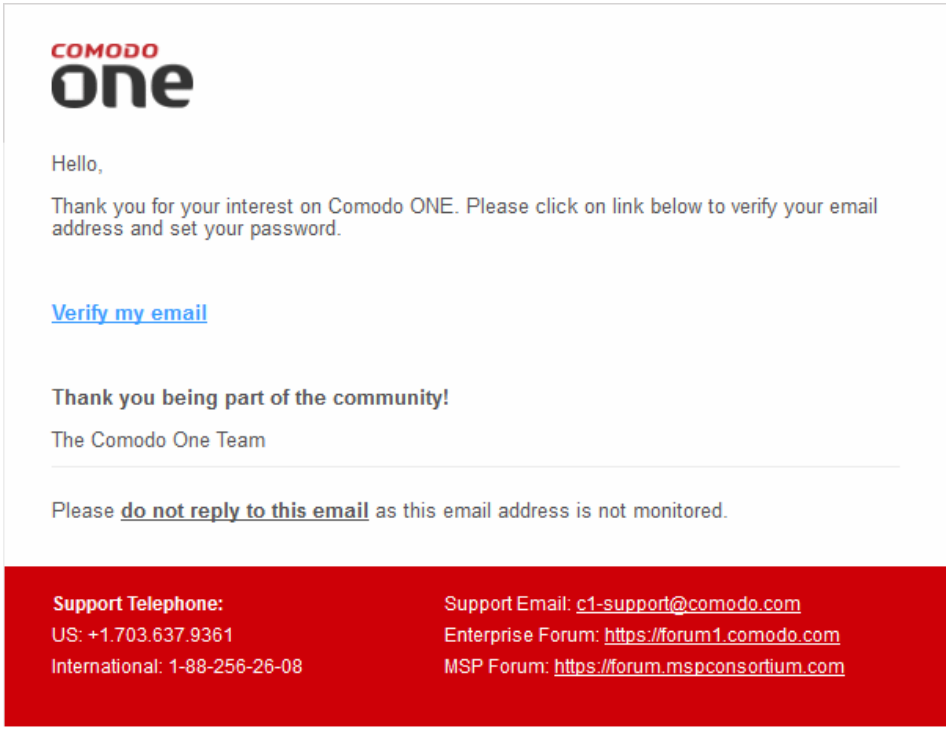
- To register as a new customer fill a short enrollment form:



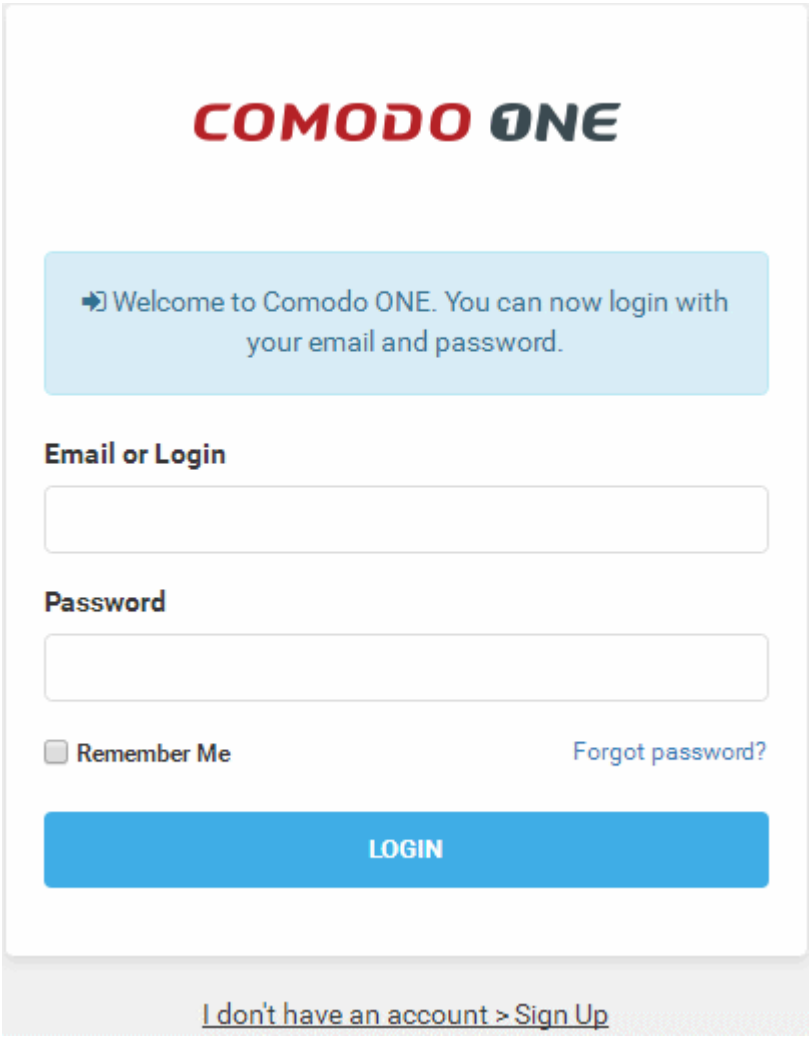
- **Email** - This field will be pre-populated with email address provided. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
- **Password** - Create a password for logging-in to your C1 account. The password should be at least eight characters, and must contain a combination of lower case and upper case letters, 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.

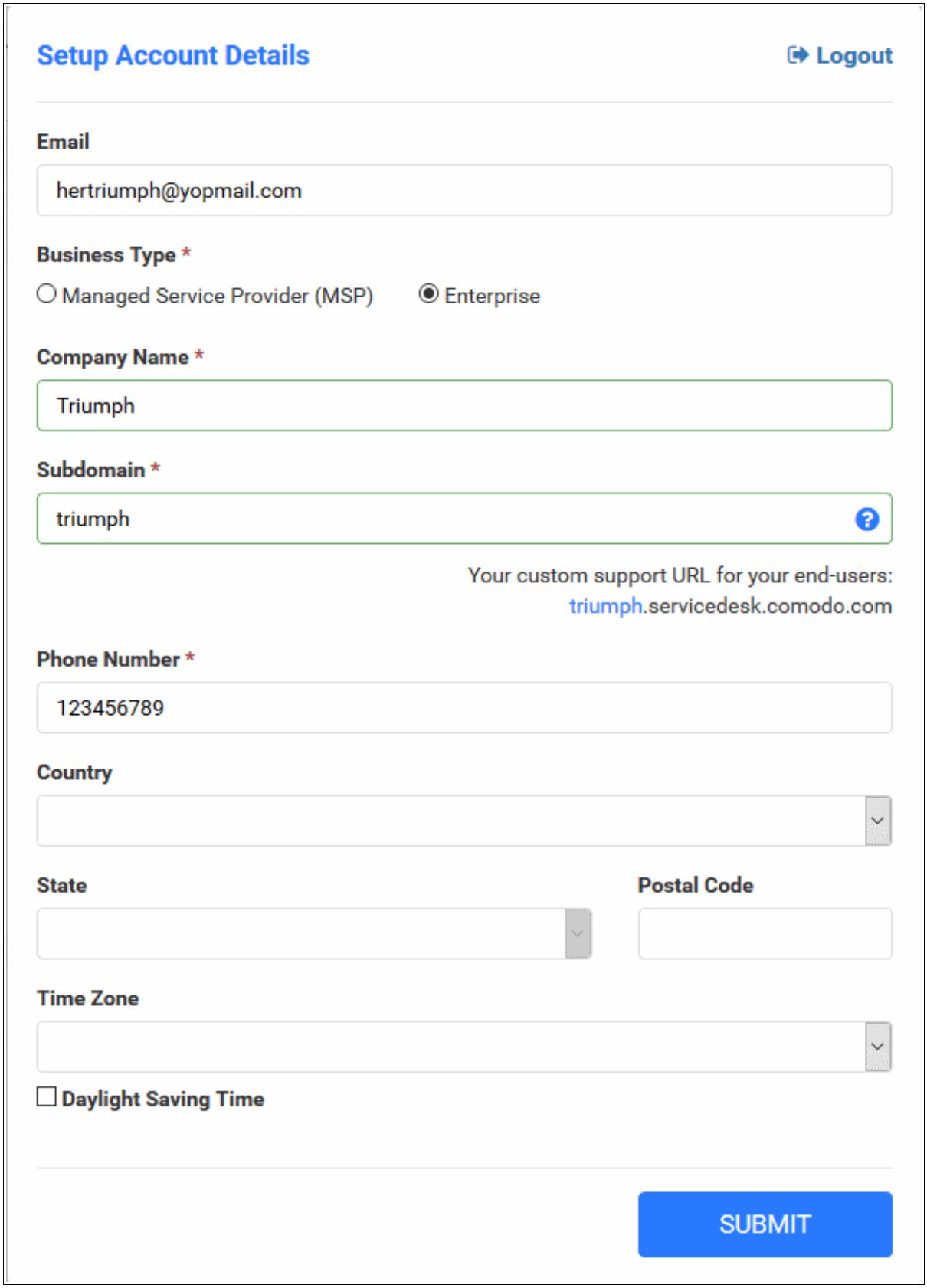
- A verification email will be sent to your email address. Click the link in the mail to verify your application:



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



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



- Complete the form with your company, location and sub-domain details to finalize account setup:
  - **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.

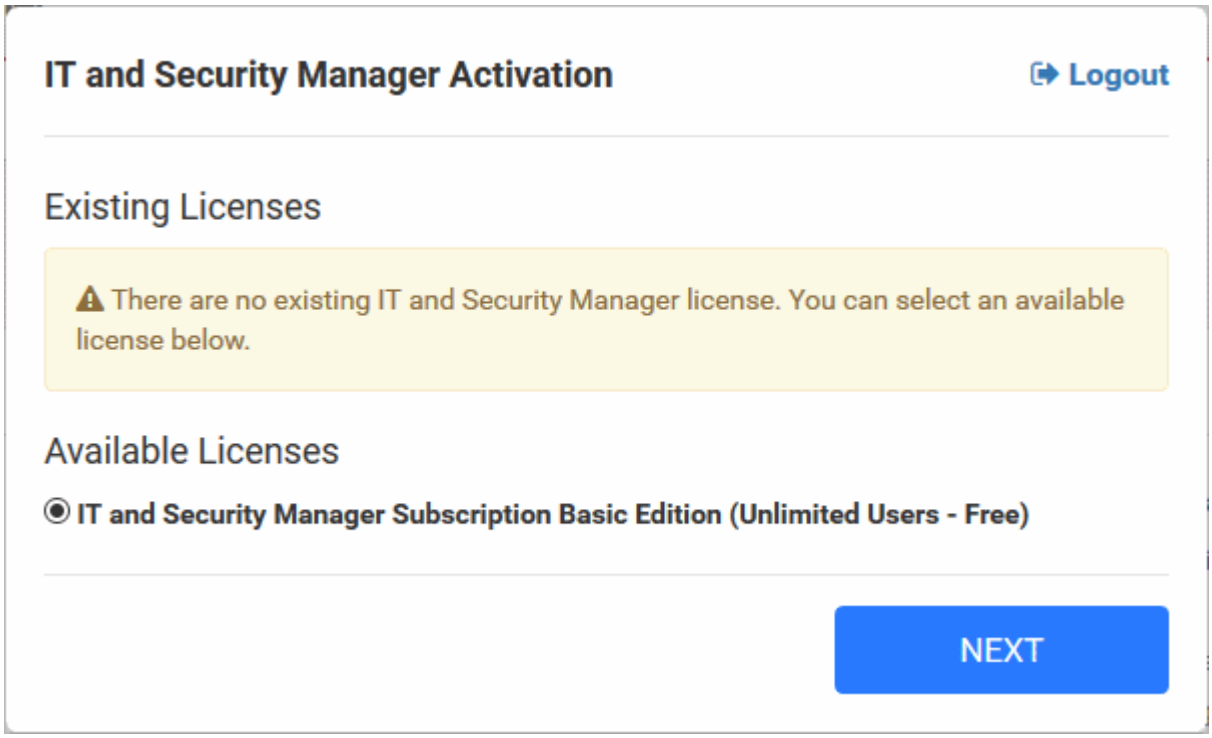
Comodo One MSP	Comodo One Enterprise
Modules included in the Comodo One Base package	
Service Desk Patch Management IT and Security Manager (ITSM)	Service Desk IT and Security Manager (ITSM)
Modules that can be subscribed and added to base Comodo One	
Acronis Backup Comodo Quote Manager cWatch Comodo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

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.

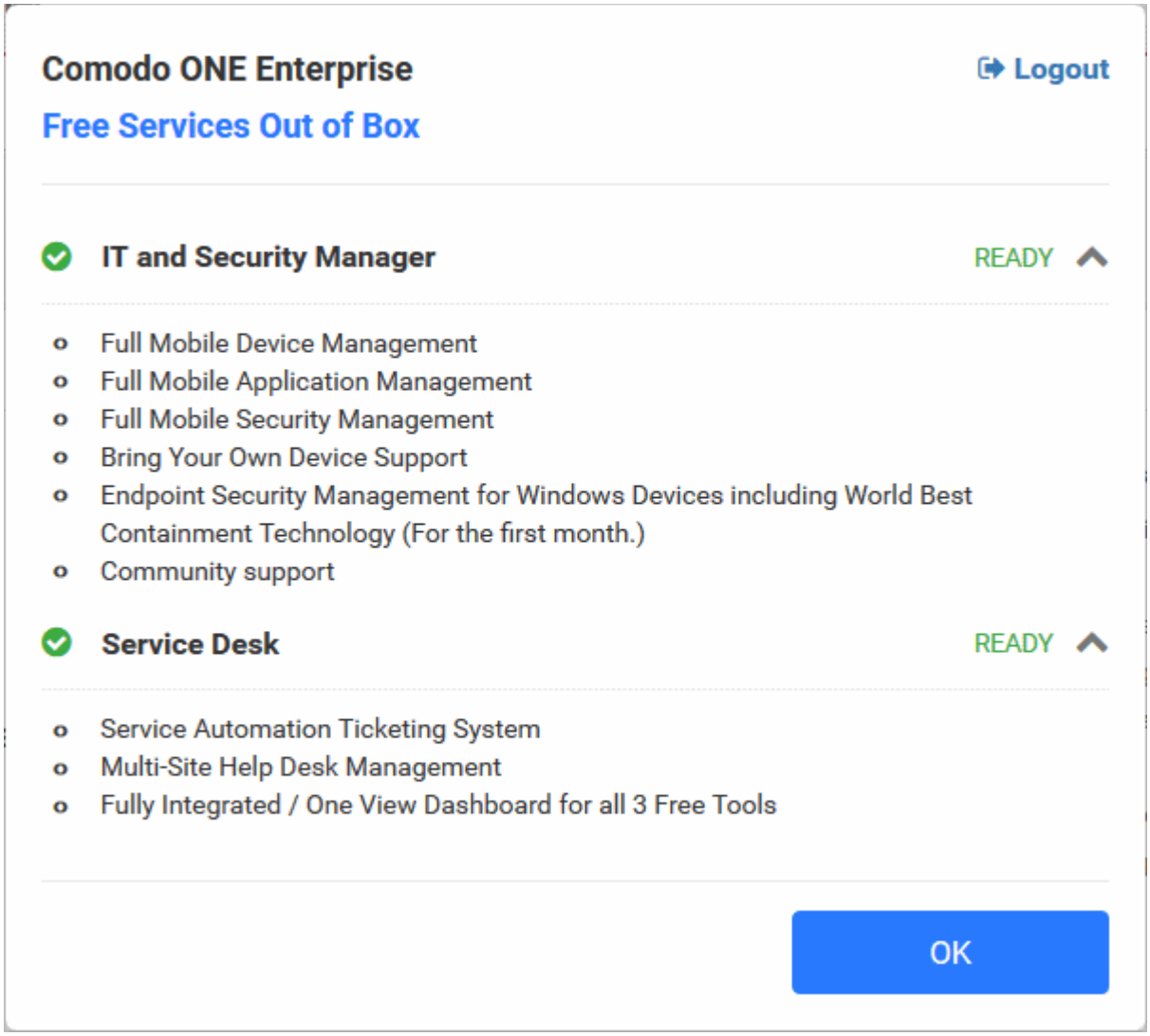
- Click 'Submit'

The activation dialog for your free products will appear.



- Click 'Next'

Your free modules will be activated.



- Click 'OK' to complete the setup process. You will be taken to the Comodo One Dashboard.

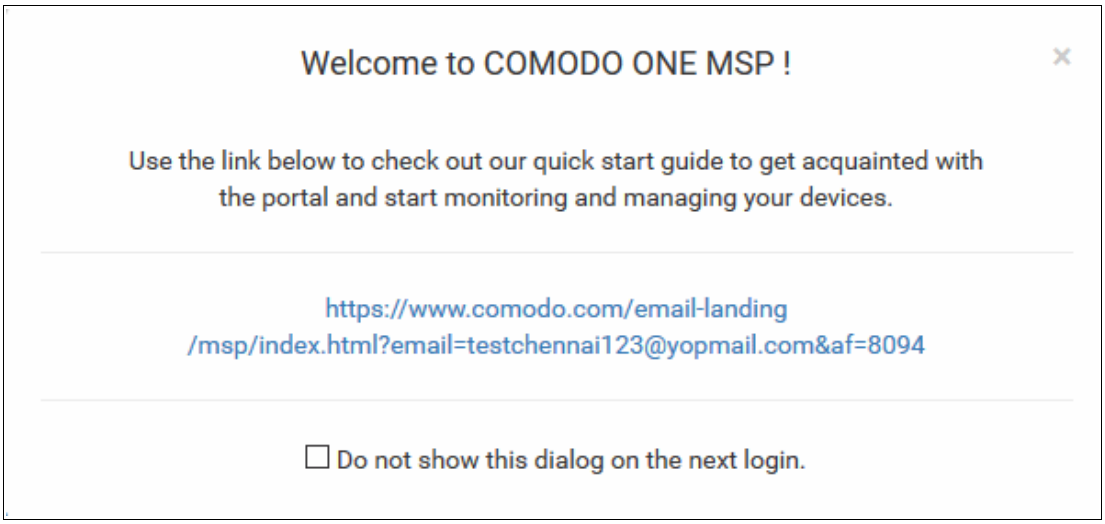
Please note that this account will be automatically granted 'Account Admin' privileges and cannot be deleted. This is effectively the 'Master Admin'. You will be able to create administrators and staff under this account. For more details, refer to the online help guide of Comodo One at https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.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

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

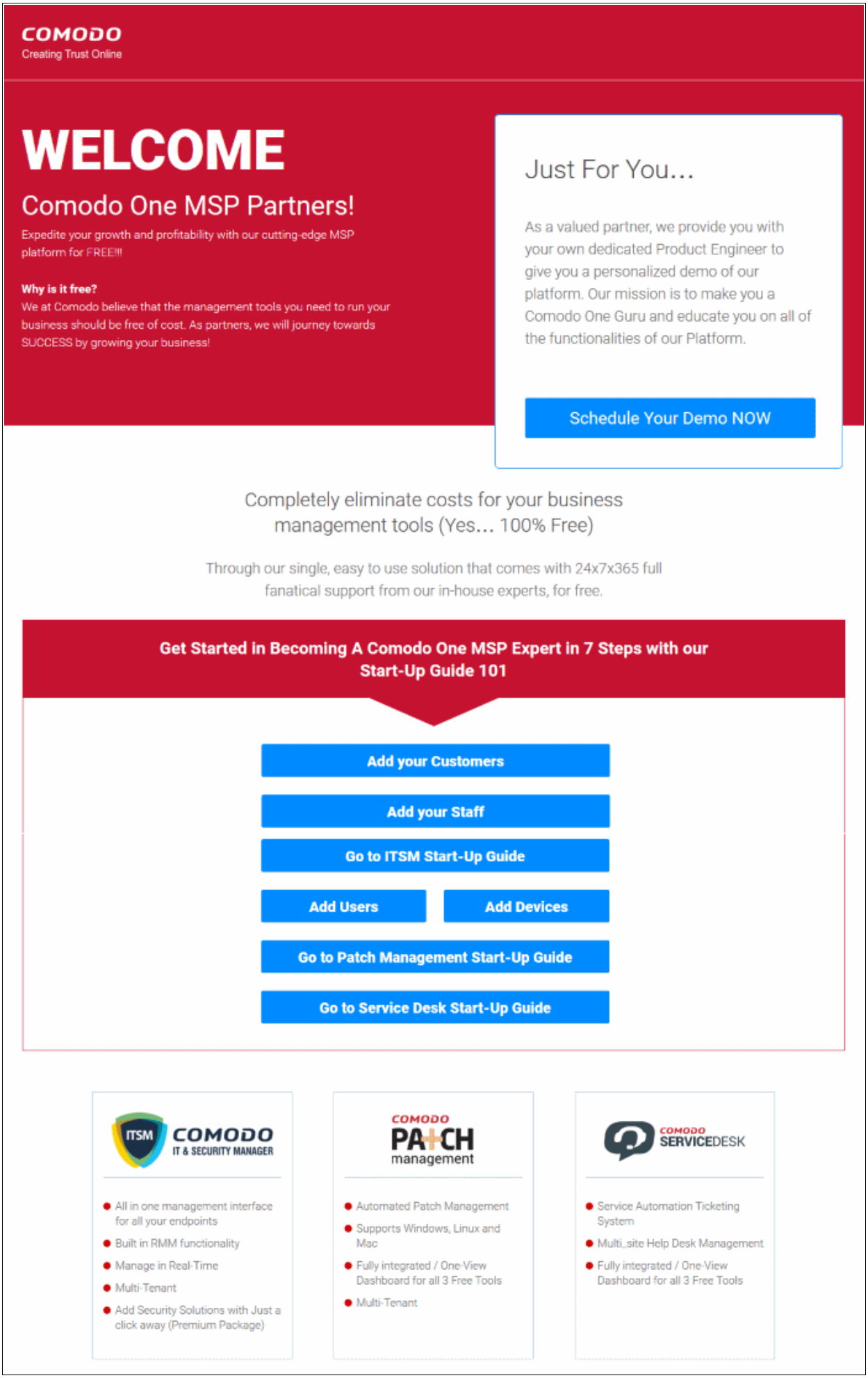
- From C1 console - Login to C1 console, click 'Licensed Applications' > 'ITSM' from the C1 console
- Directly to ITSM - Enter the URL 'https://<.cmdm.comodo.com/'

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

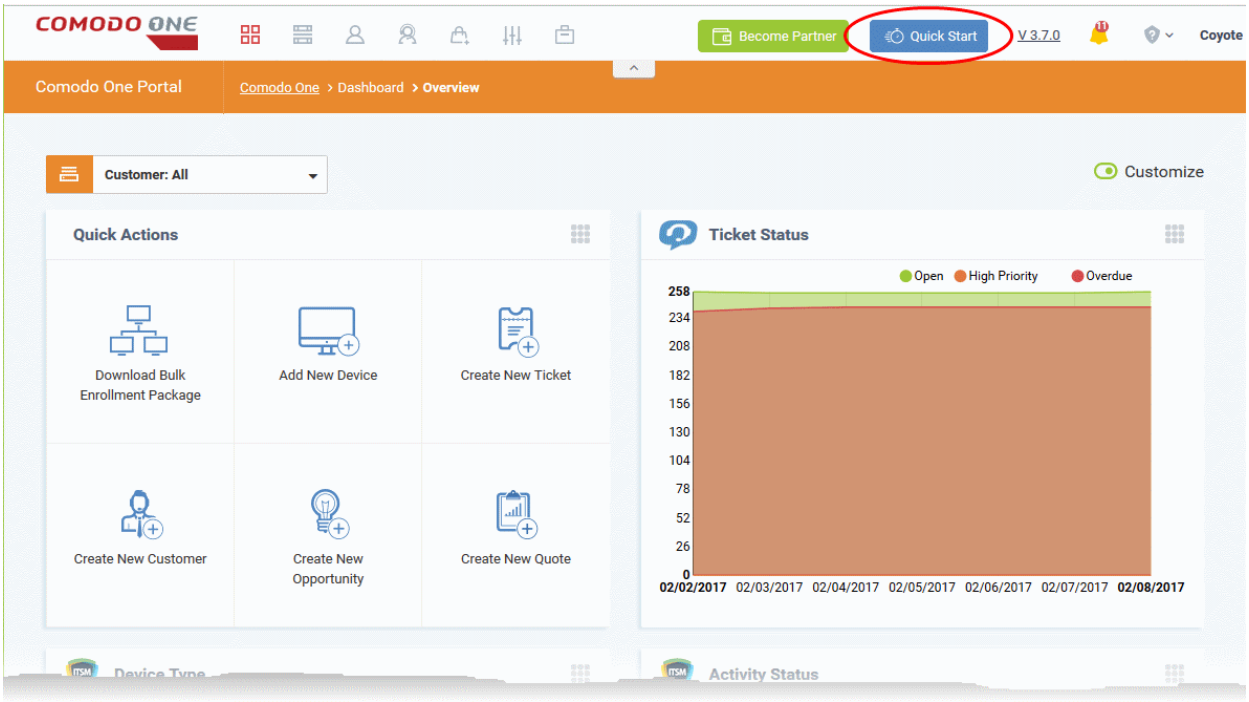
After logging into your account you will see the following message:



- Click the link in the message to go to the welcome and quick start page. The welcome page will be slightly different depending on whether you signed up for a C1 MSP or C1 Enterprise account:


COMODO
Creating Trust Online
WELCOME
Comodo One MSP Partners!
Expedite your growth and profitability with our cutting-edge MSP platform for FREE!!!
Why is it free?
We at Comodo believe that the management tools you need to run your business should be free of cost. As partners, we will journey towards SUCCESS by growing your business!
Just For You...
As a valued partner, we provide you with your own dedicated Product Engineer to give you a personalized demo of our platform. Our mission is to make you a Comodo One Guru and educate you on all of the functionalities of our Platform.
Schedule Your Demo NOW
Completely eliminate costs for your business management tools (Yes... 100% Free)
Through our single, easy to use solution that comes with 24x7x365 full fanatical support from our in-house experts, for free.
Get Started in Becoming A Comodo One MSP Expert in 7 Steps with our Start-Up Guide 101
Add your Customers
Add your Staff
Go to ITSM Start-Up Guide
Add Users
Add Devices
Go to Patch Management Start-Up Guide
Go to Service Desk Start-Up Guide
ITSM
COMODO
IT & SECURITY MANAGER
All in one management interface for all your endpoints
Built in RMM functionality
Manage in Real-Time
Multi-Tenant
Add Security Solutions with Just a click away (Premium Package)
COMODO
PATCH
management
Automated Patch Management
Supports Windows, Linux and Mac
Fully integrated / One-View Dashboard for all 3 Free Tools
Multi-Tenant
COMODO
SERVICEDESK
Service Automation Ticketing System
Multi_site Help Desk Management
Fully integrated / One-View Dashboard for all 3 Free Tools

You can refer to the Quick Start guide at any point by clicking the 'Quick start' button at the top of the C1 application:



Step 2 - Configure ITSM Communications

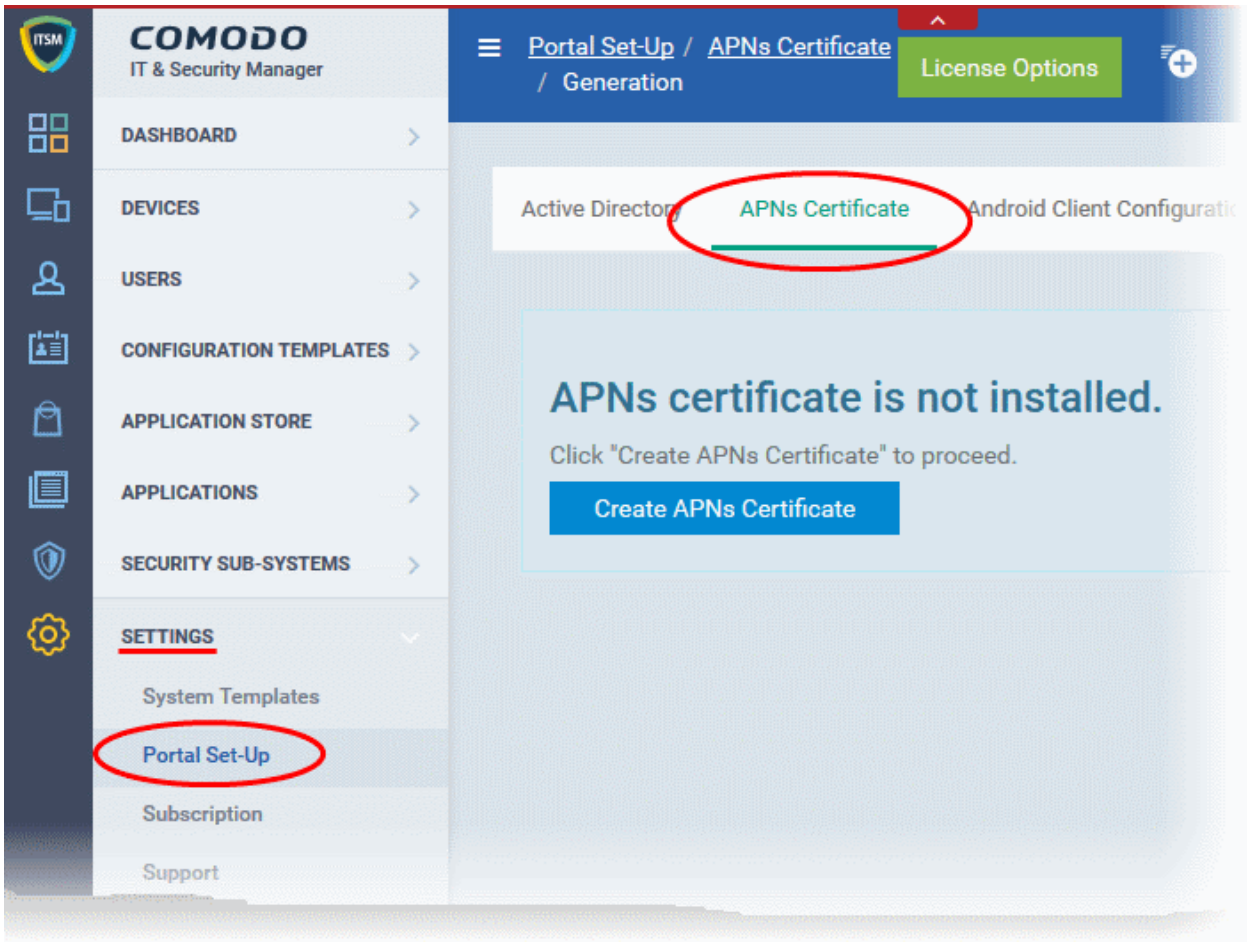
In order for your ITSM server to communicate with enrolled devices, you need to install Apple Push Notification (APN) certificate and/or Google Cloud Messaging (GSM) Token on your portal. The following sections explain more about:

- Adding APN Certificate
- Adding GCM Token

Adding Apple Push Notification Certificate

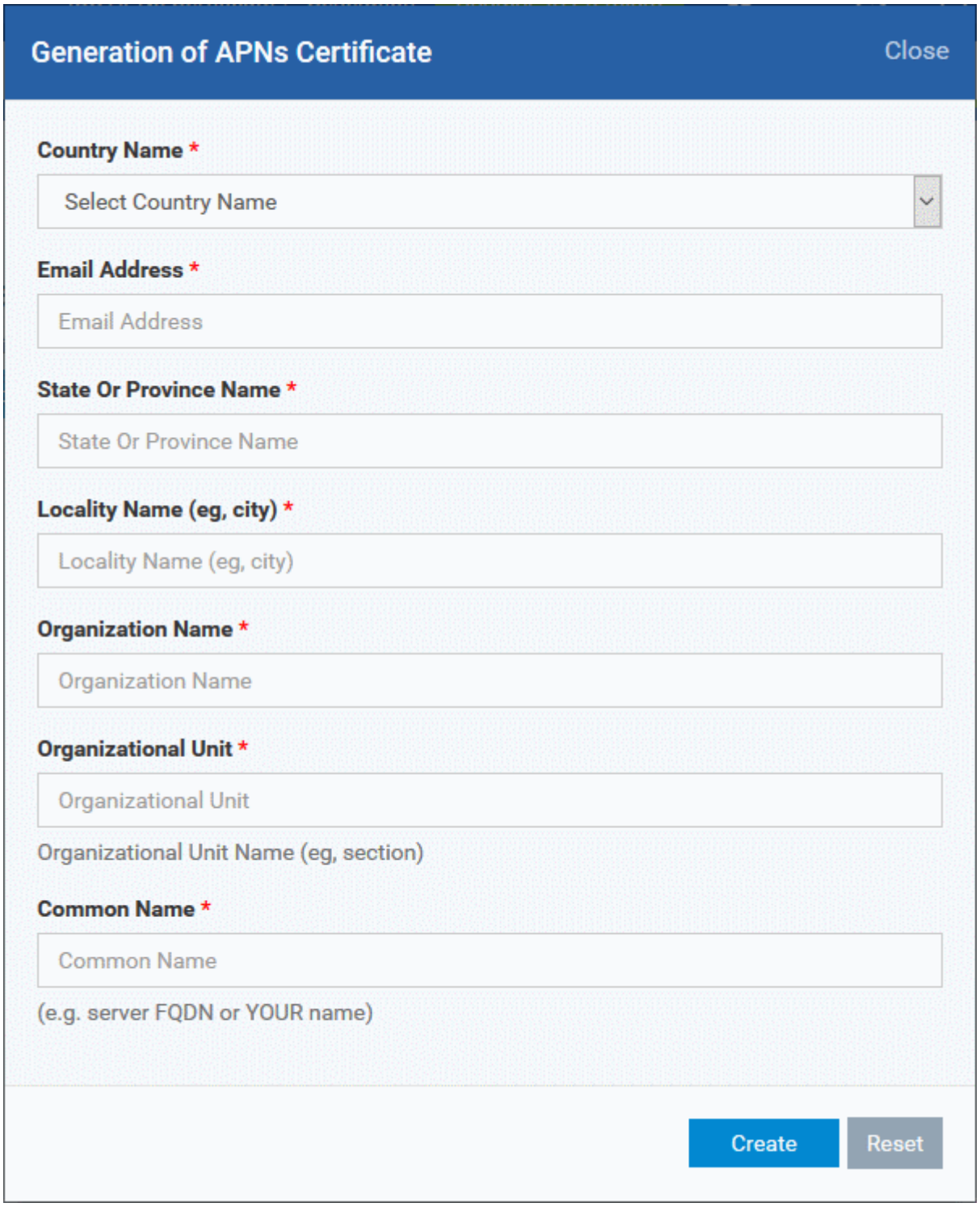
Apple requires an Apple Push Notification (APN) certificate installed on your ITSM portal to facilitate communication with managed iOS devices and Mac OS devices. To obtain and implement an APN certificate and corresponding private key, please follow the steps given below:

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

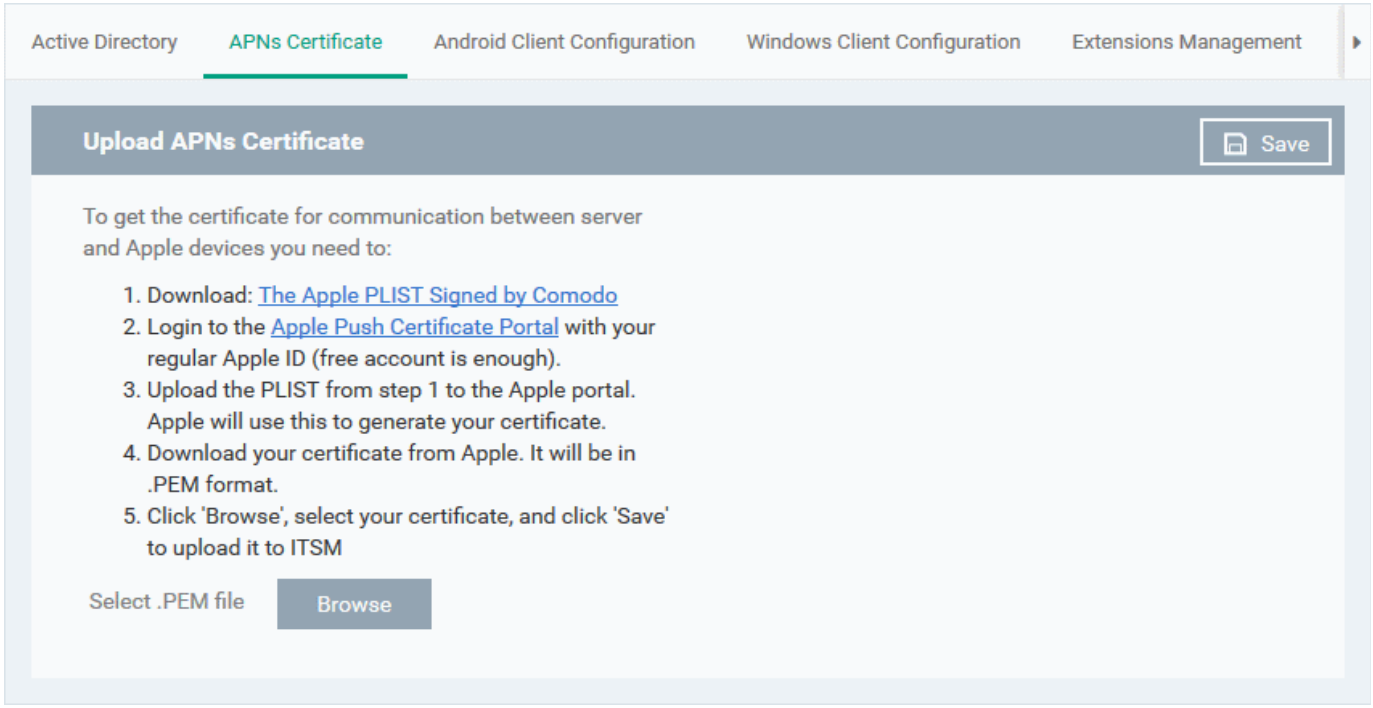


- Click the 'Create APNs Certificate' button to open the APNs application form.

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



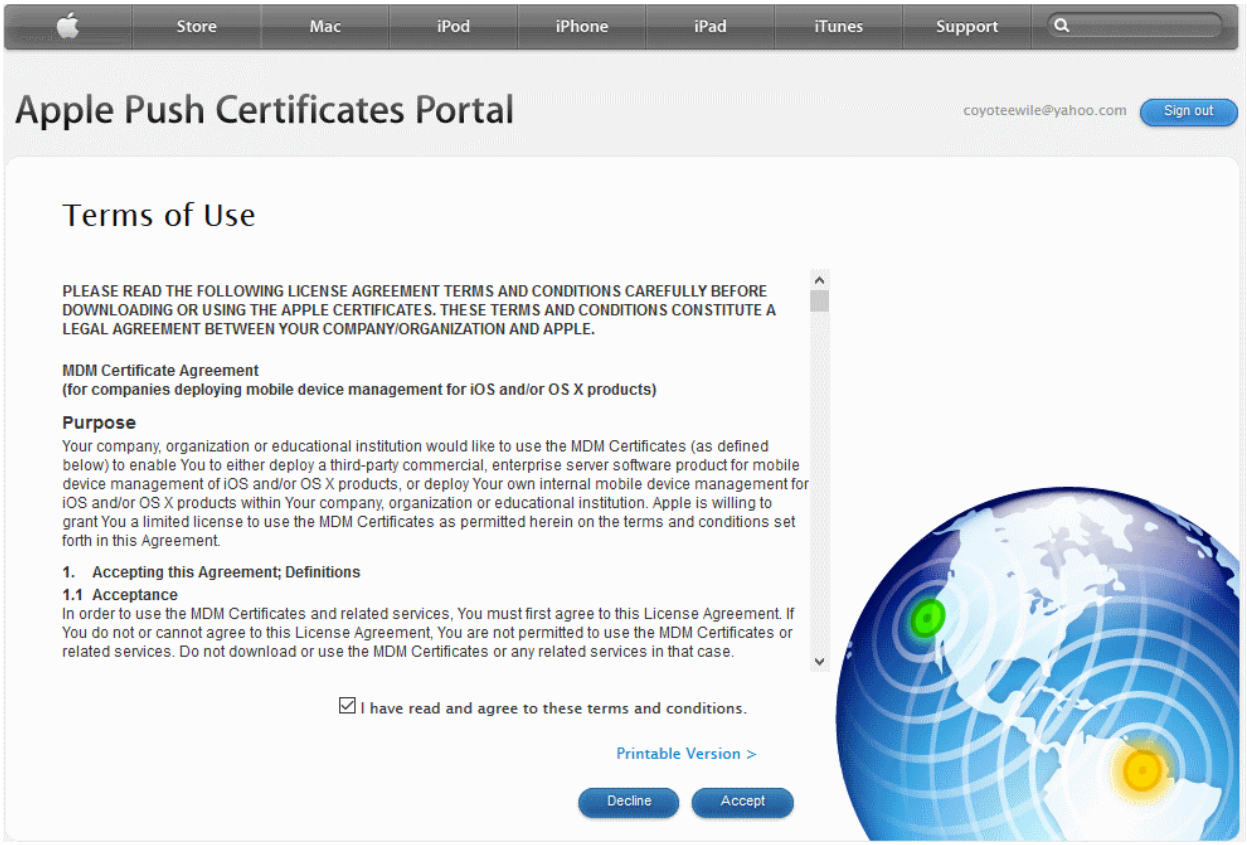
- Complete all fields marked with an asterisk and click 'Create'. This will send a request to Comodo to sign the CSR and generate an Apple PLIST. You will need to submit this to Apple in order to obtain your APN certificate. Usually your request will be fulfilled within seconds and you will be taken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



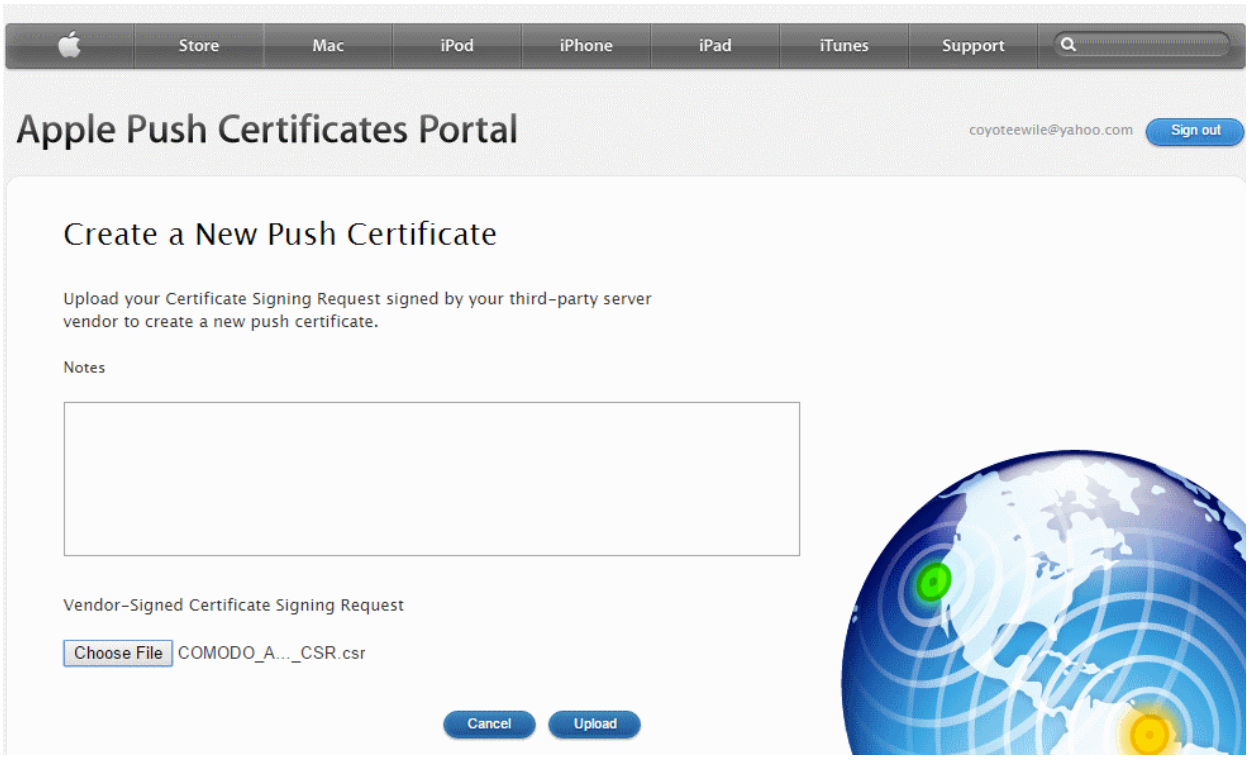
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.

- **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'.

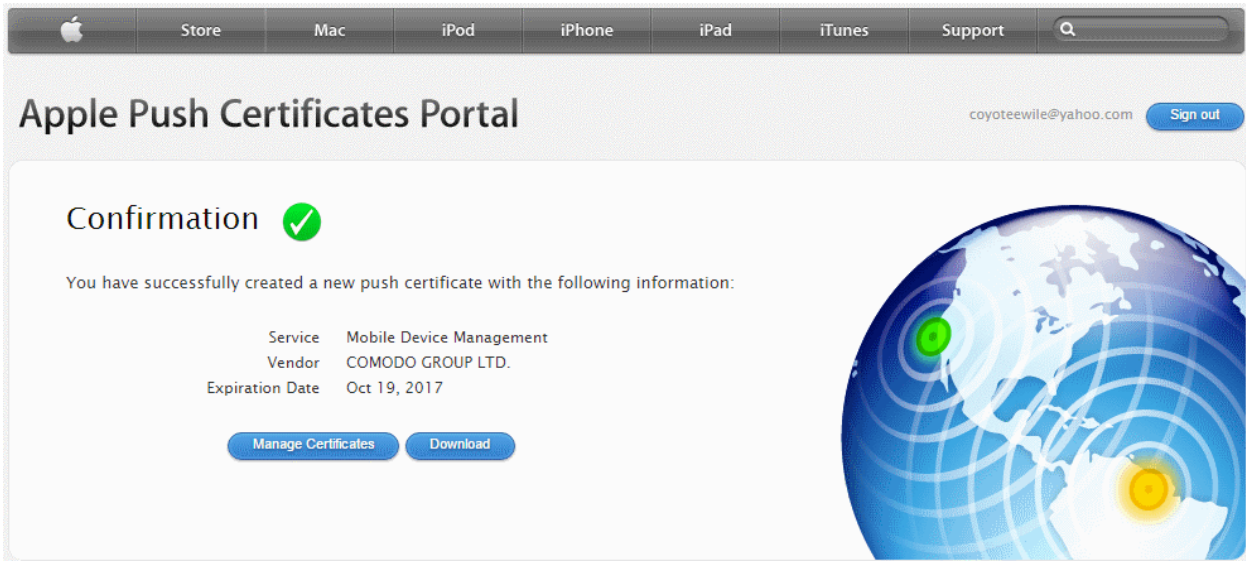
You will need to agree to Apple's EULA to proceed.



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

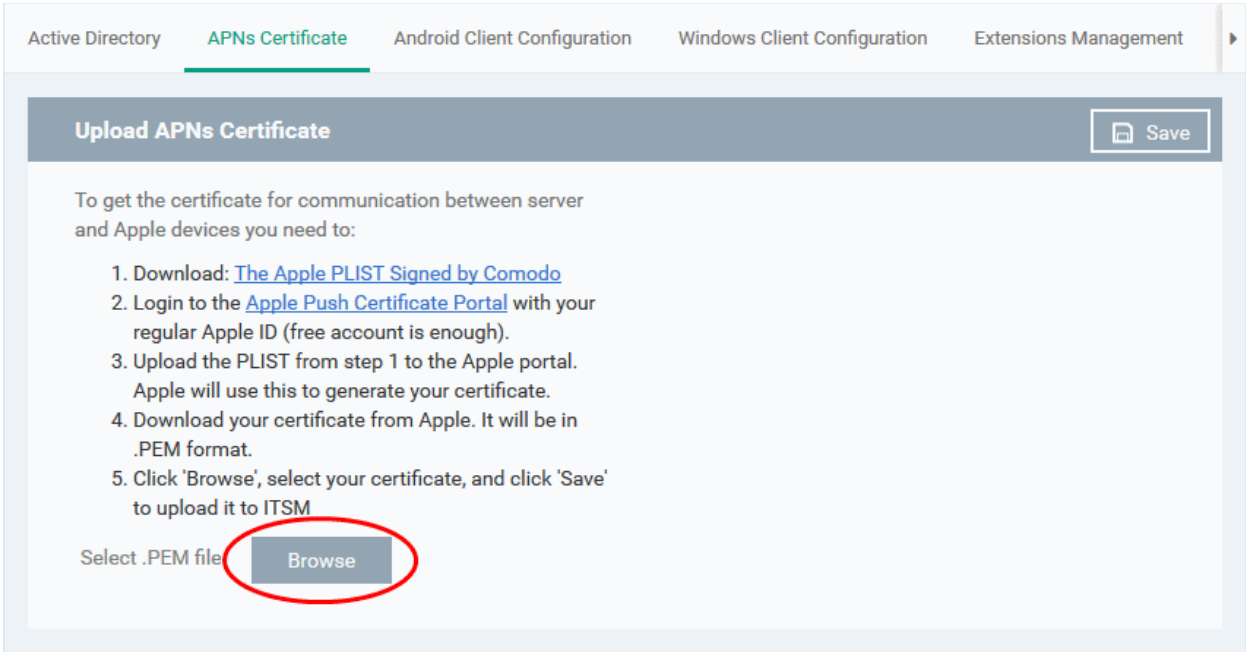


Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



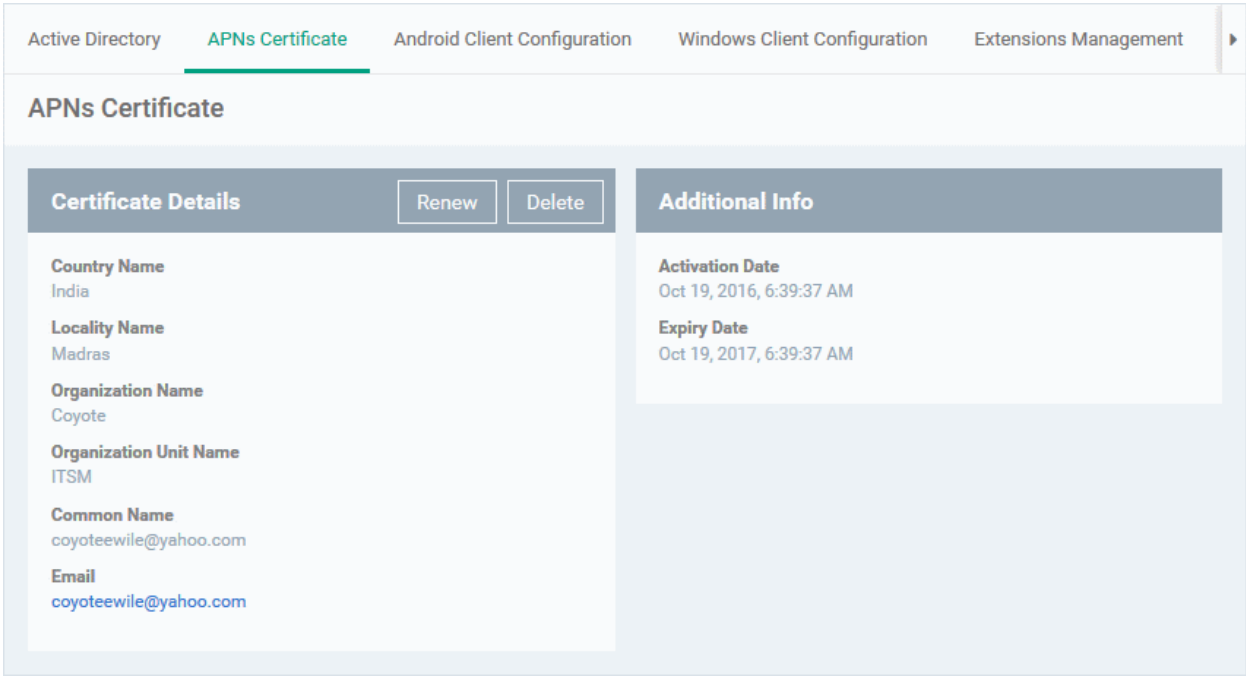
- Click the 'Download' button and save the certificate to a secure location. It will be a .pem file with a name similar to 'MDM_COMODO GROUP LTD._Certificate.pem'

- **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.

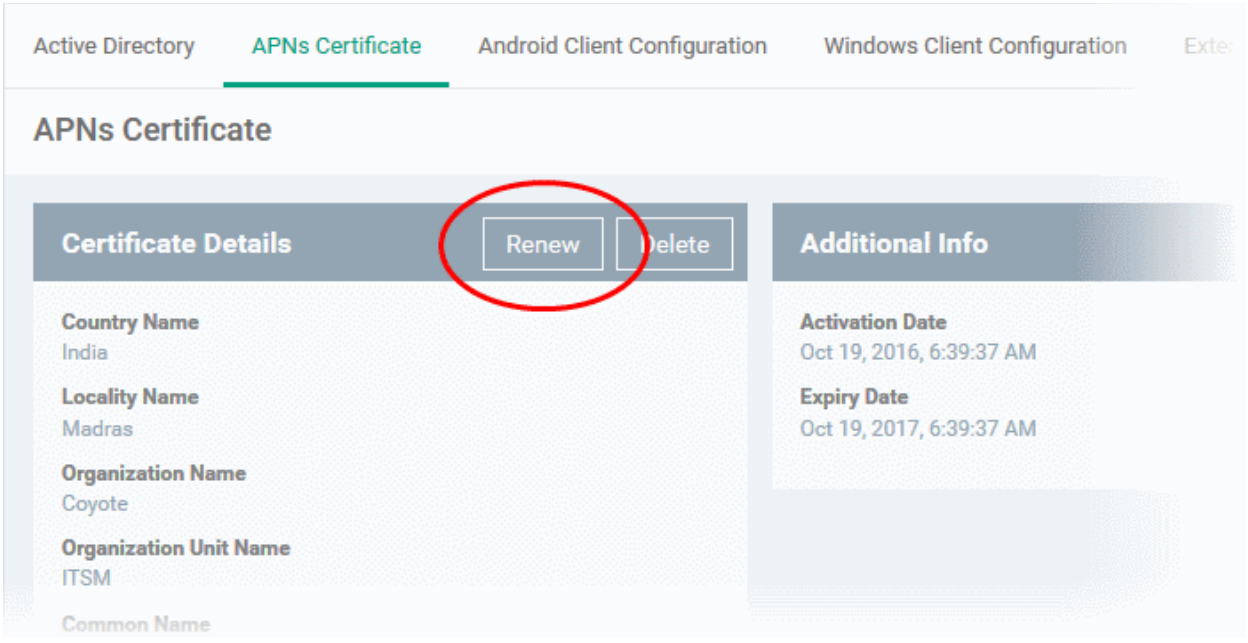
The APNs Certificate details interface will open:



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

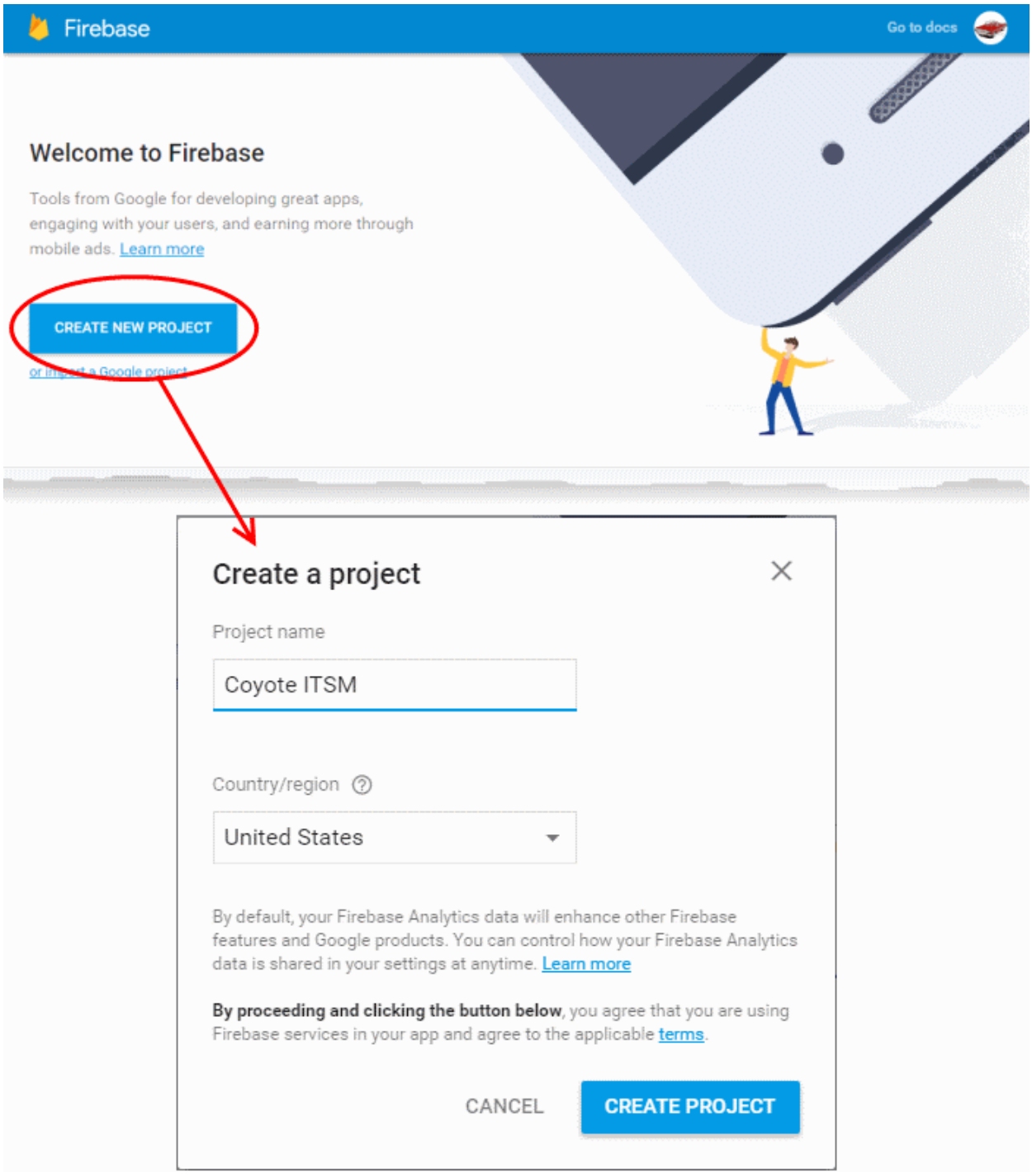
Adding Google Cloud Messaging (GCM) Token

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.

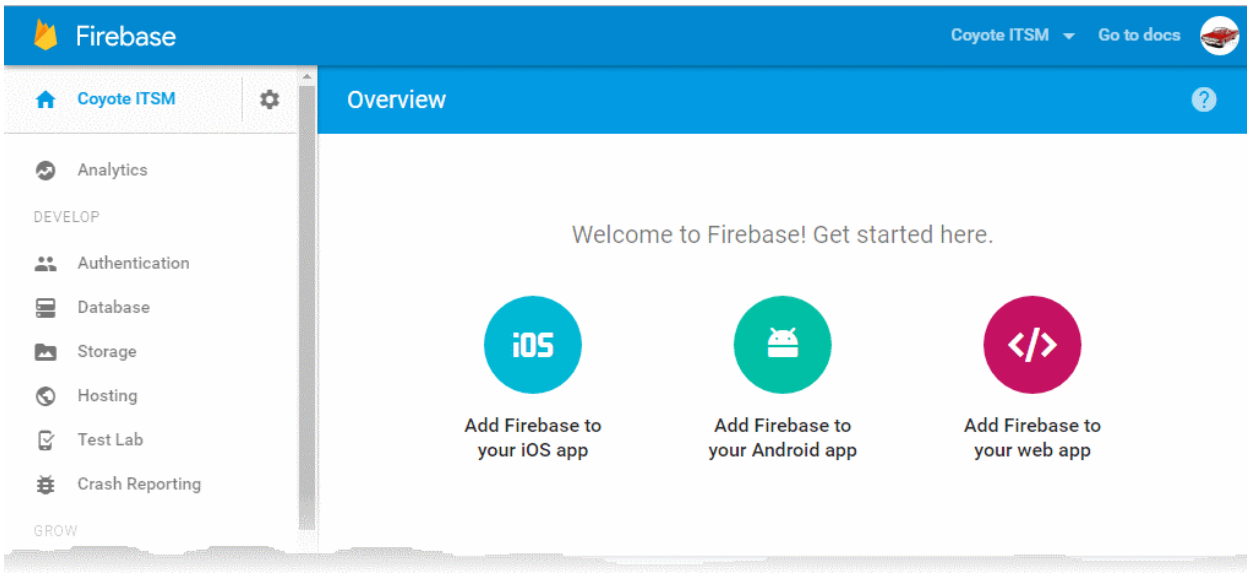
- **Step 1 - Create a New Project**

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

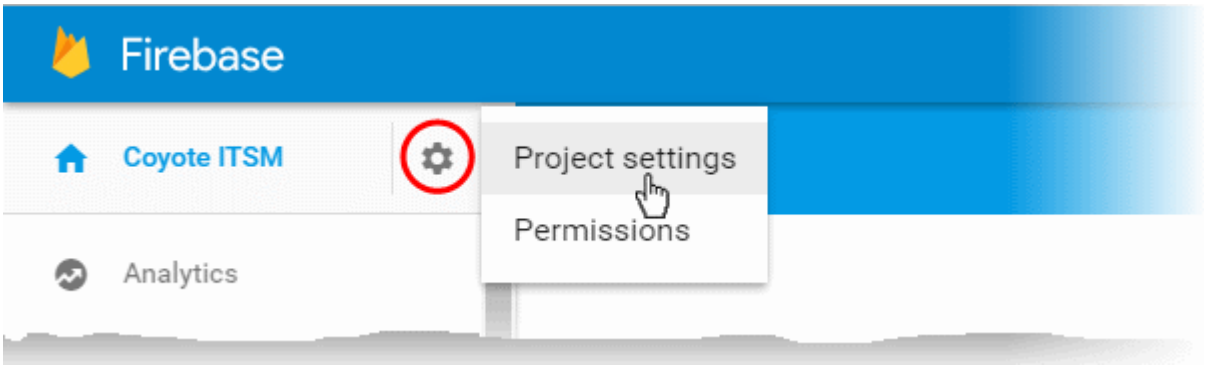


- Click 'Create Project'
- Type a name for the new project in the 'Project Name' field
- Select your country from the 'Country/region' drop-down
- Click 'Create Project'.

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

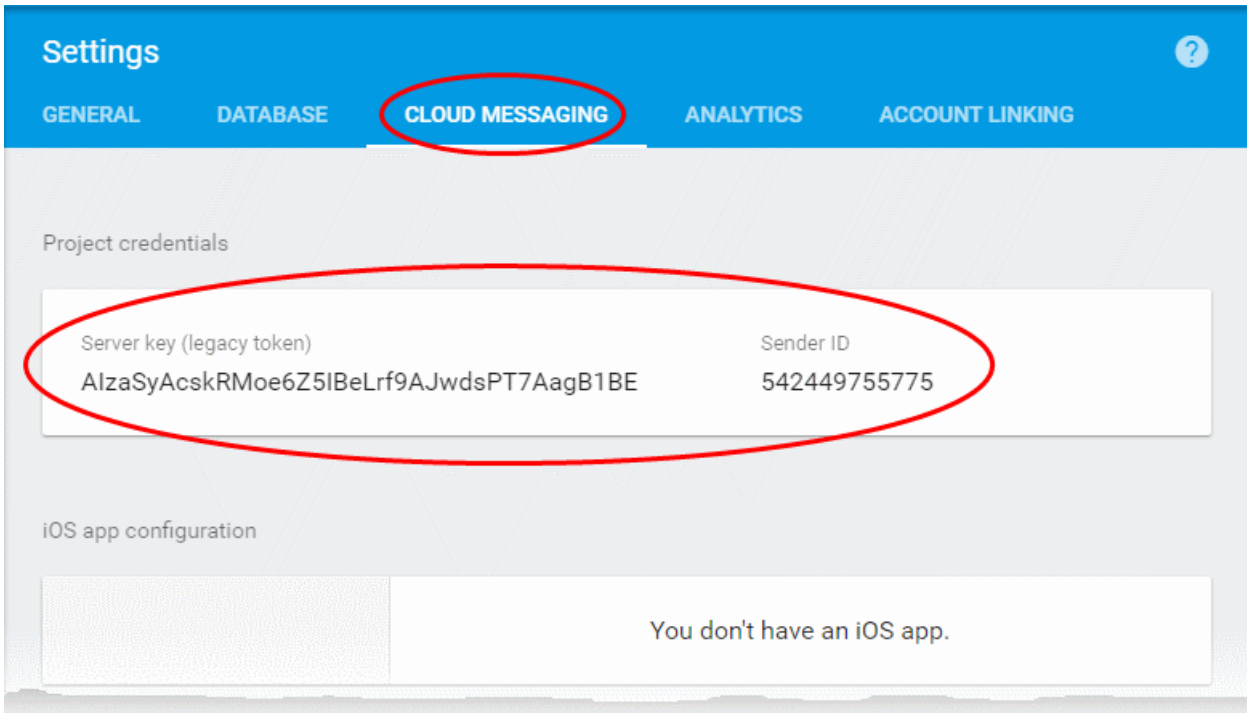


- **Step 2 - Obtain GCM Token and Project number**
  - Click the gear icon beside the project name at the left and choose Project Settings from the options.



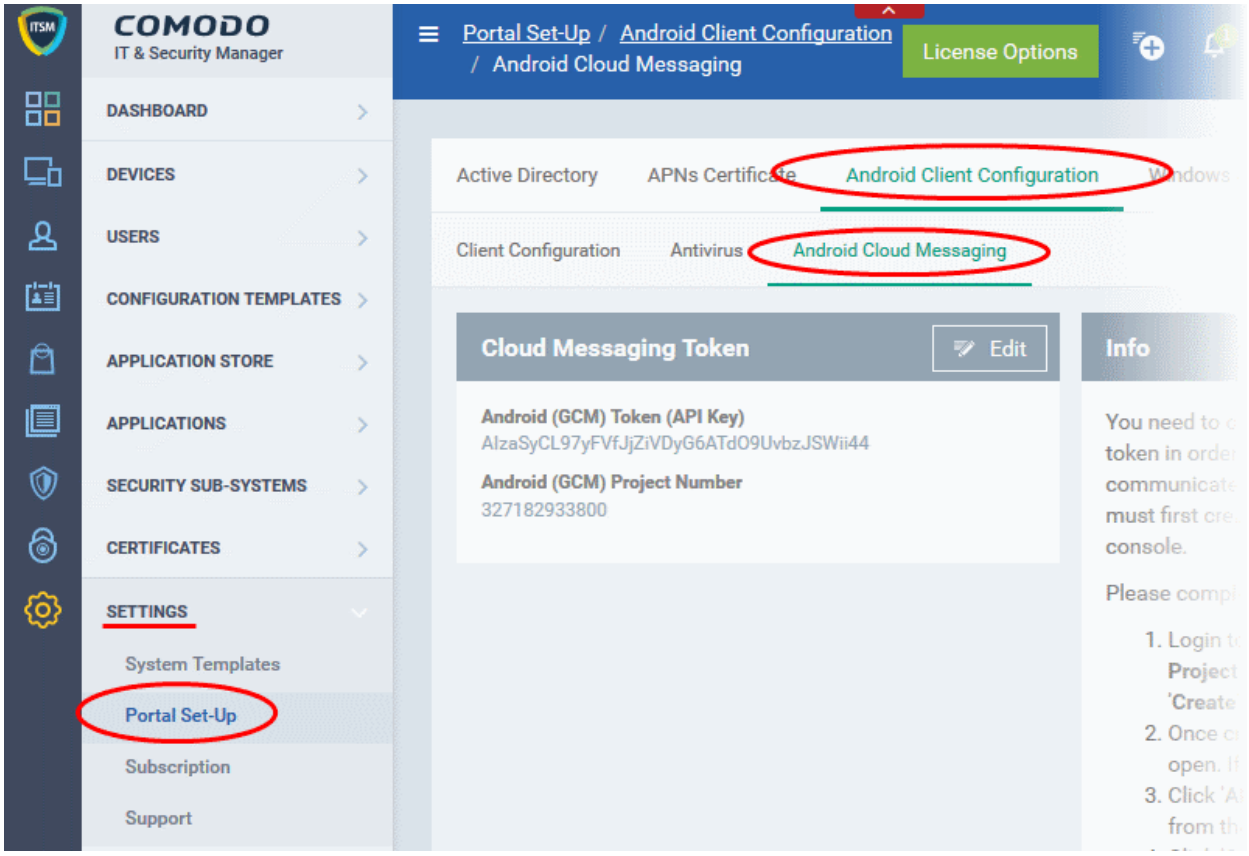
The 'Settings' screen for the project will appear.

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



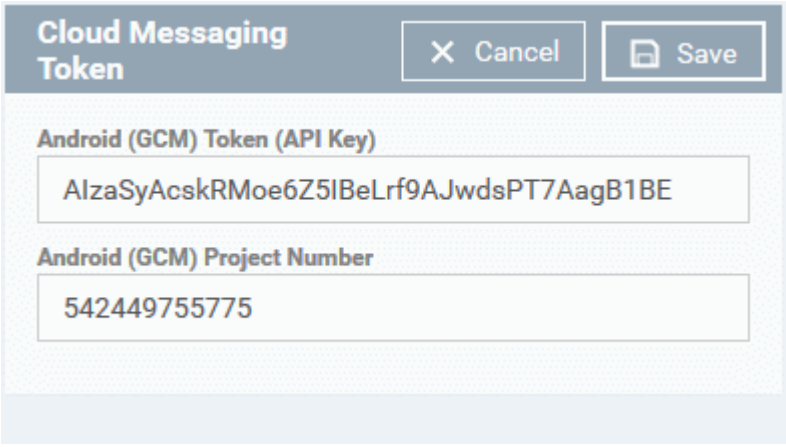
- Note down the Server key and Sender ID in a safe place

- **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 User

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** - Users added by C1 enterprise customers will be automatically added to ITSM with the selected role. Users added by C1 MSP customers will automatically be added to all the companies available in the account.

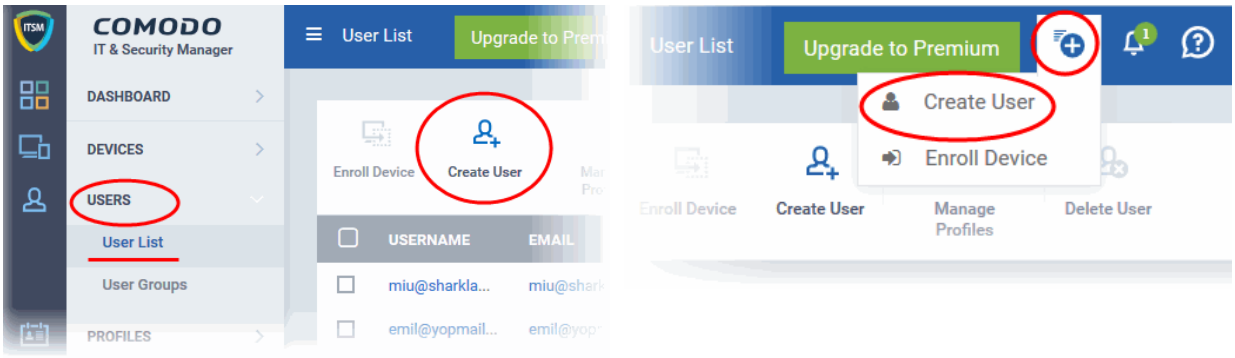
- **ITSM Users** - C1 enterprise and ITSM stand-alone customers can add users for their company only via ITSM. C1 MSP customers can add users via ITSM to the required company. You can group users/devices under different companies (for C1 MSP customers) as explained in Step 5 - Create Groups of Devices.

To add a user

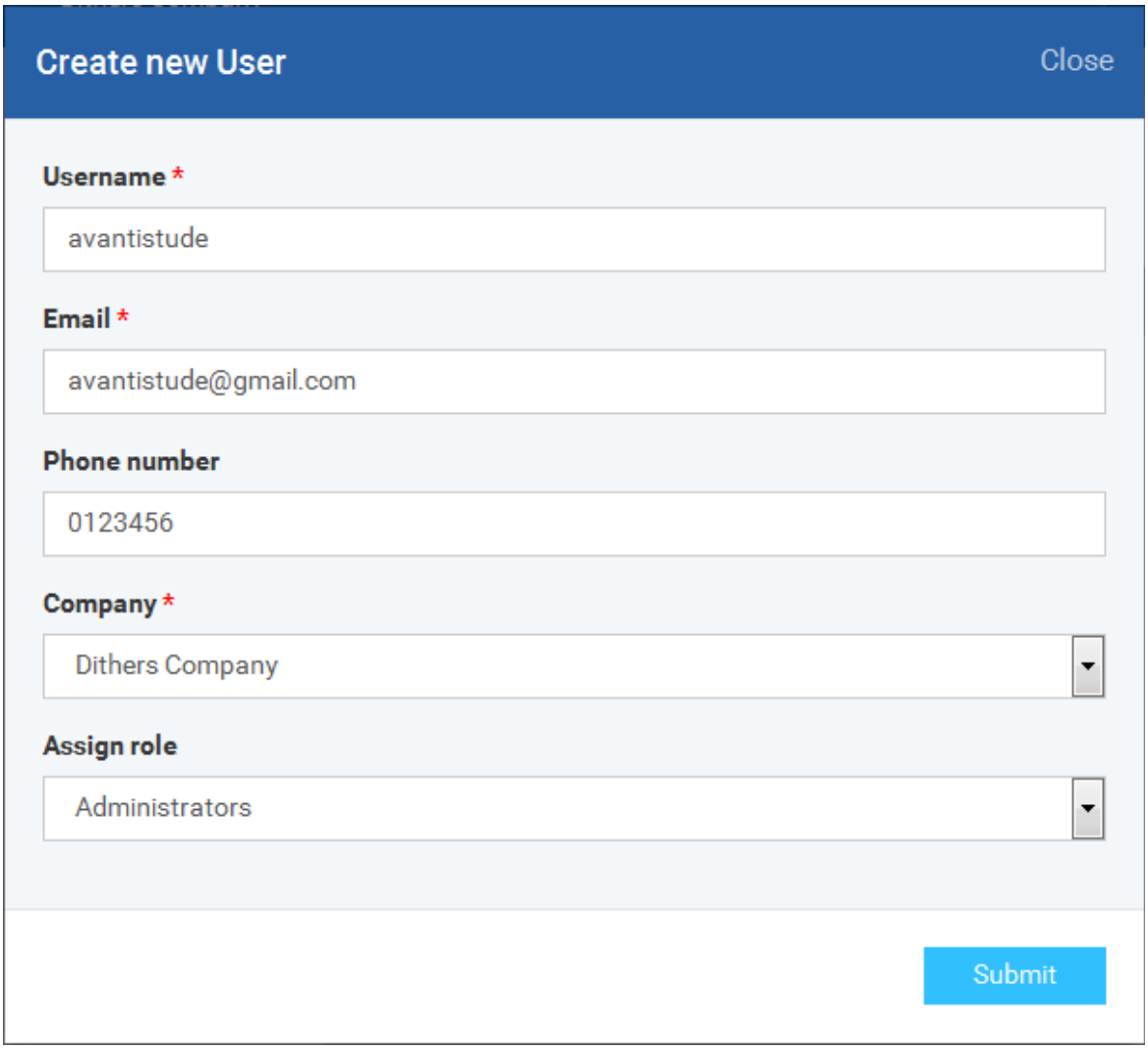
- Click 'Users' on the left then 'User List', then click the 'Create User' button

  or

- 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 of the user to be added.
- Choose the company (mandatory), from the 'Company' drop-down.
  - Comodo One MSP 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.
  - Comodo One Enterprise and stand-alone 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 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. 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

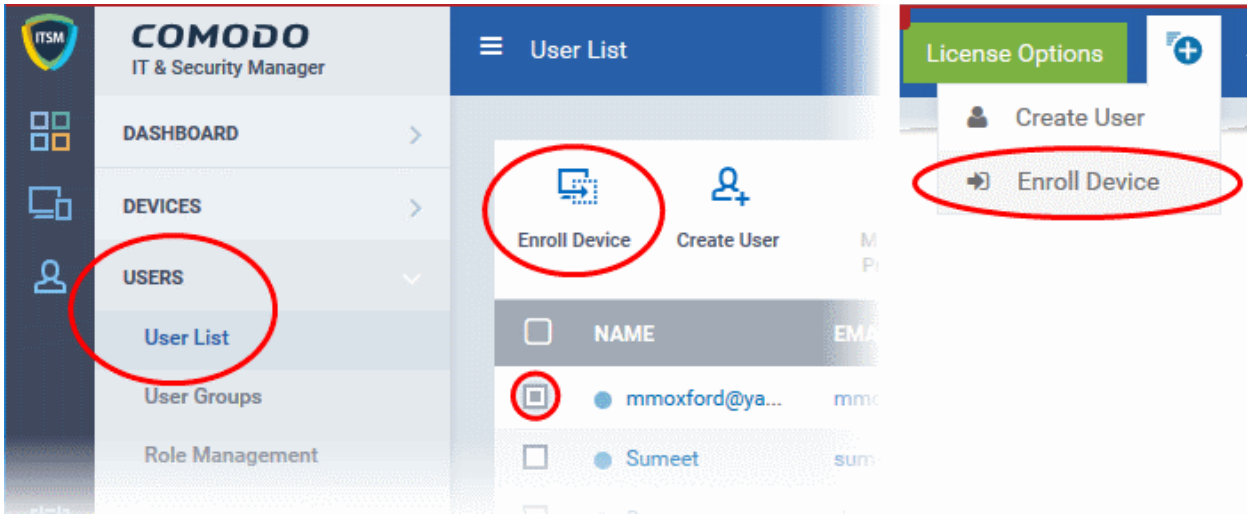
The next step is to enroll users' devices for management.

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.

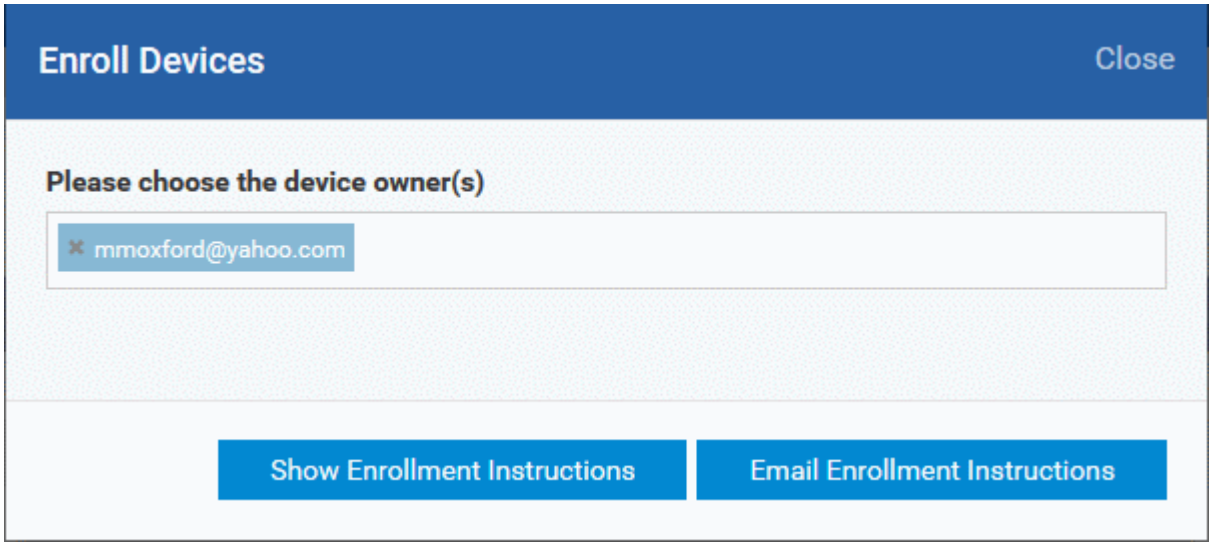
To enroll devices

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

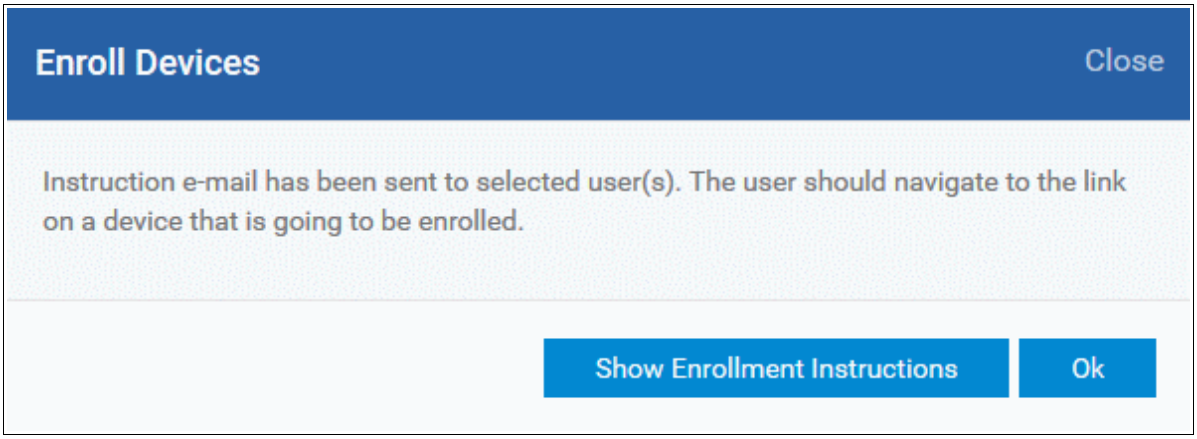


The 'Enroll Devices' dialog will open for the chosen users.



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.

ITSM 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.

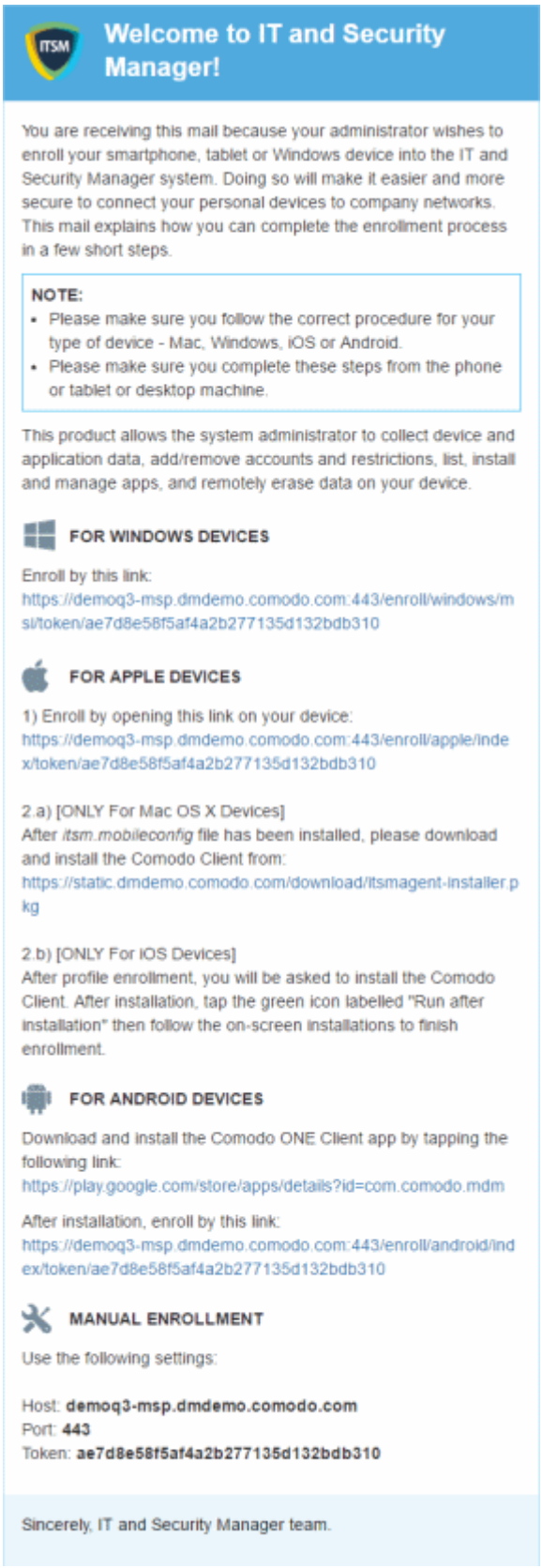
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

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 WINDOWS DEVICES

Enroll by this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/ae7d8e58f5af4a2b277135d132bdb310

FOR APPLE DEVICES

1) Enroll by opening this link on your device:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/apple/index/token/ae7d8e58f5af4a2b277135d132bdb310

2.a) [ONLY For Mac OS X Devices]
After *itsm.mobileconfig* file has been installed, please download and install the Comodo Client from:
https://static.dmdemo.comodo.com/download/itsmagent-installer.pkg

2.b) [ONLY For iOS Devices]
After profile enrollment, you will be asked to install the Comodo Client. After installation, tap the green icon labelled "Run after installation" then follow the on-screen installations to finish enrollment.

FOR ANDROID DEVICES

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

After installation, enroll by this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/android/index/token/ae7d8e58f5af4a2b277135d132bdb310

MANUAL ENROLLMENT

Use the following settings:

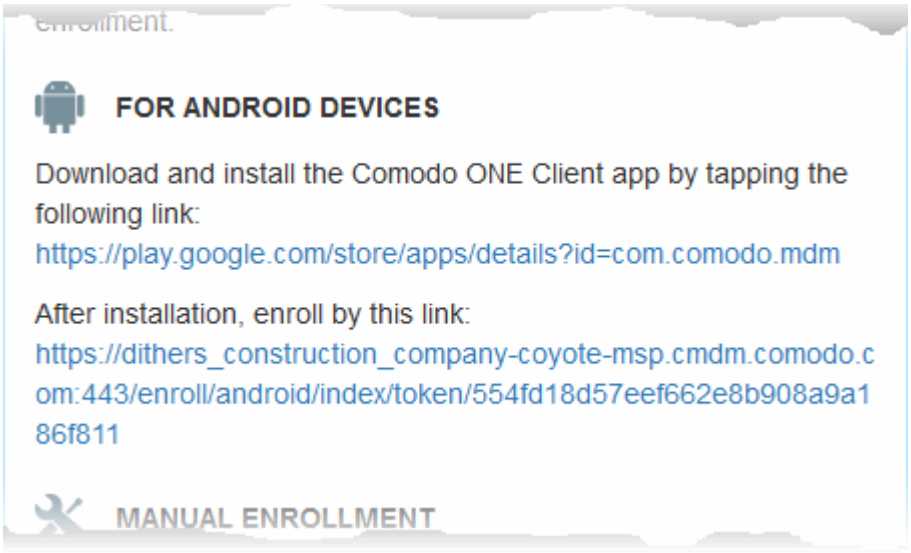
Host: **demoq3-msp.dmdemo.comodo.com**
Port: **443**
Token: **ae7d8e58f5af4a2b277135d132bdb310**

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

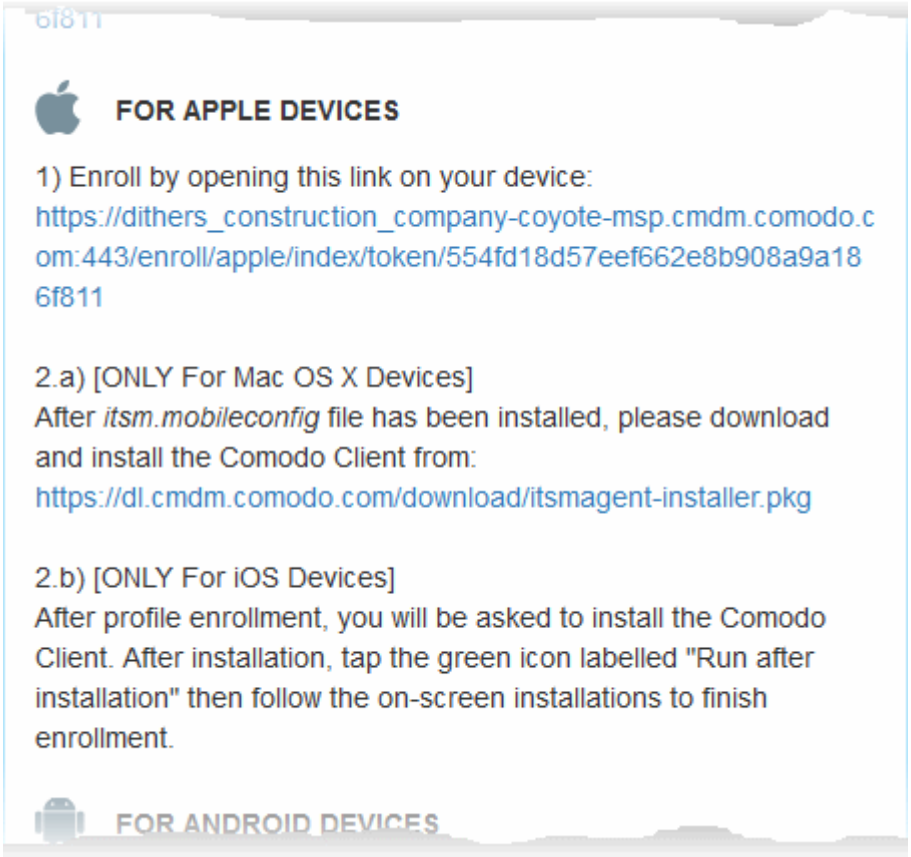
The device enrollment page contains two links under 'FOR ANDROID DEVICES'. The first to download the Android app and the second to enroll the device:



1. User opens the enrollment page on the target device and taps the 1st link to install the ITSM app.
2. After 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.

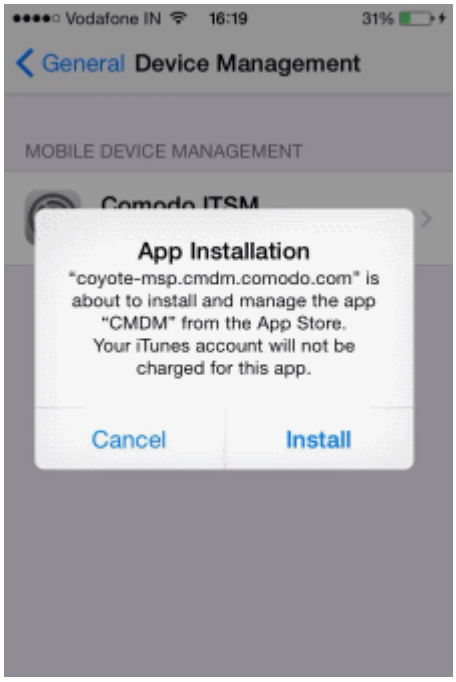
Enroll iPhones, iPods and iPads

The device enrollment page contains an enrollment link under 'FOR APPLE DEVICES'. The user taps 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.

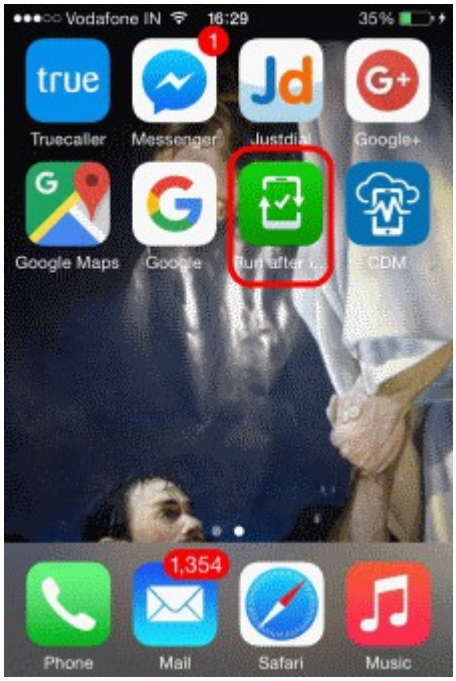


The app will be downloaded from iTunes store, using the user's iTunes account. The app is free, hence the user will not be charged for installing the app.

- 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.

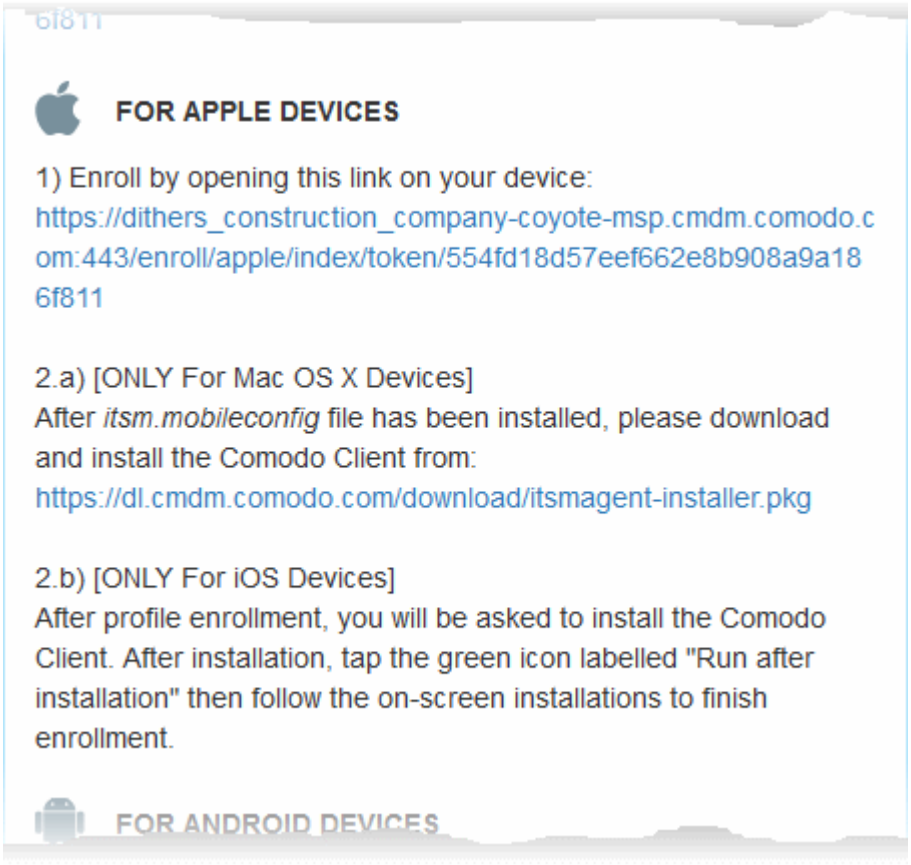


The device will be enrolled and connected to ITSM.

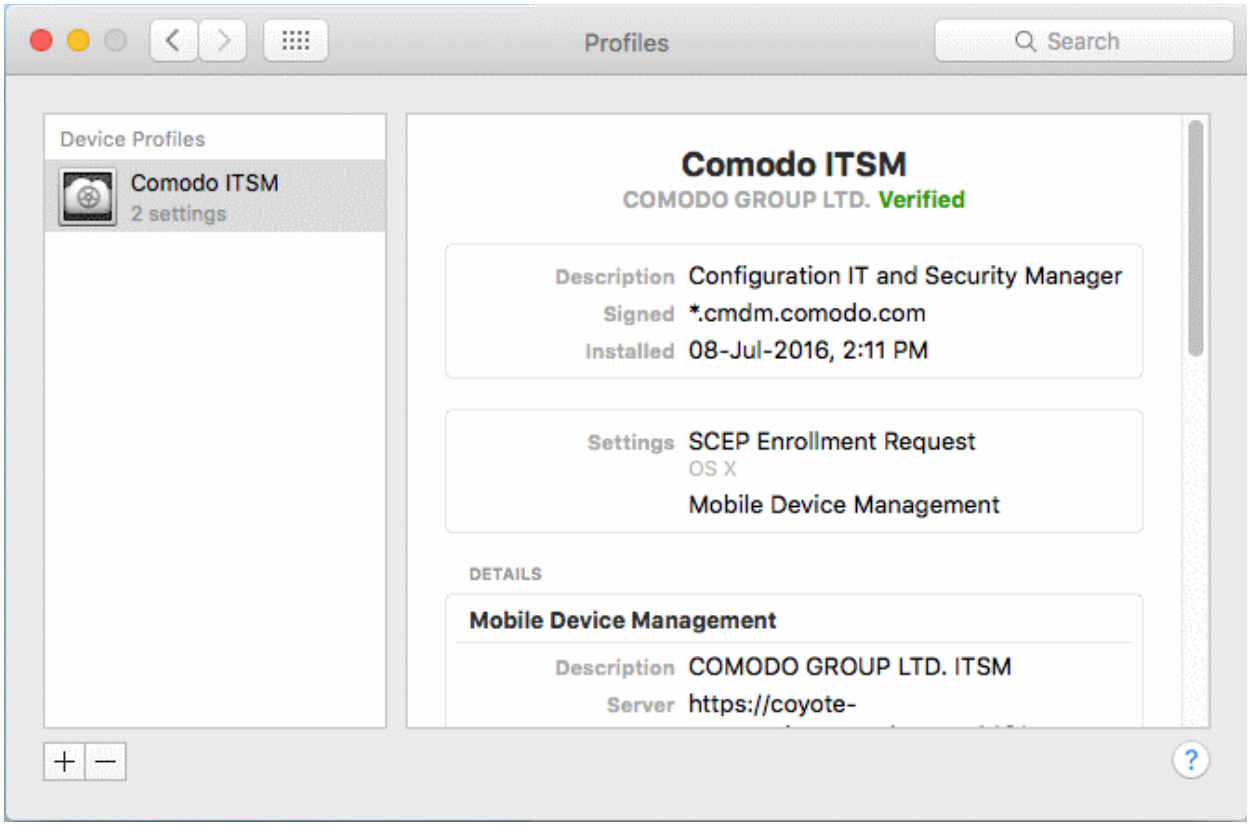
Enroll Mac OS X Devices

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.



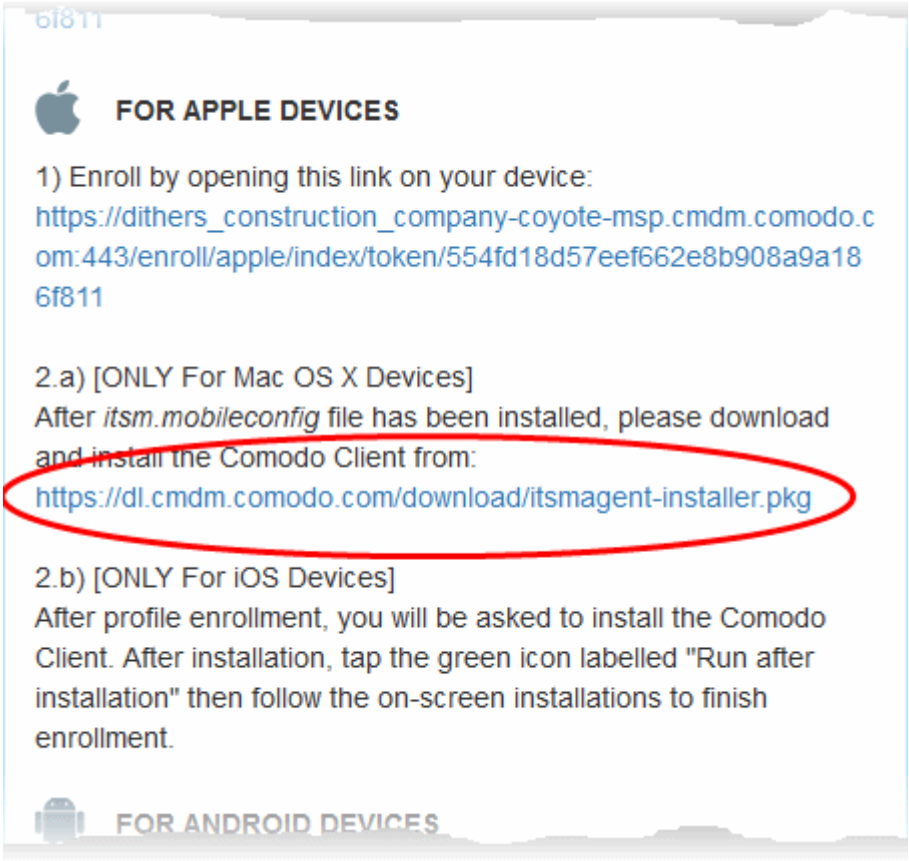
On completion of installation, the profile will be added to the Device Profiles list in the Mac OS X device.



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

Step 2 - Install ITSM Agent

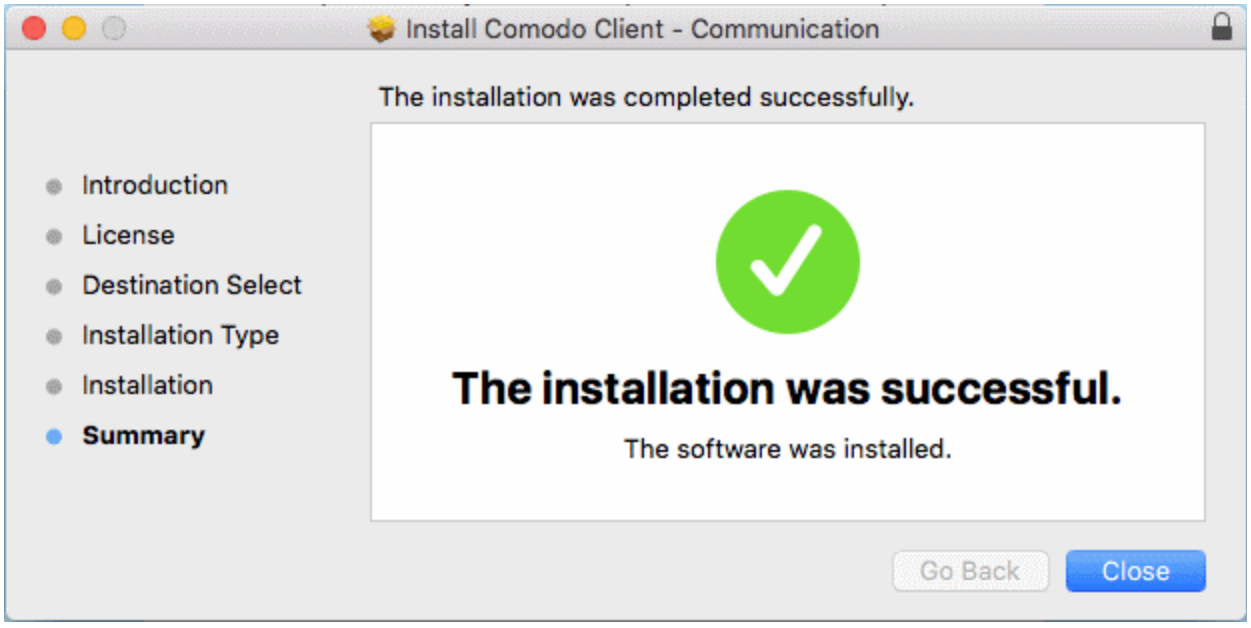
- Next the user click the link under 'Only For Mac OS X Devices' to download the ITSM agent for Mac.



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

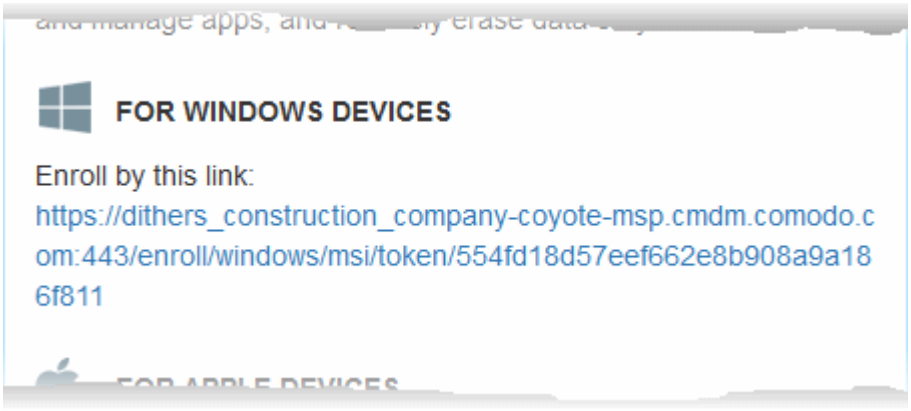
- The user follows the wizard and completes the installation.

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



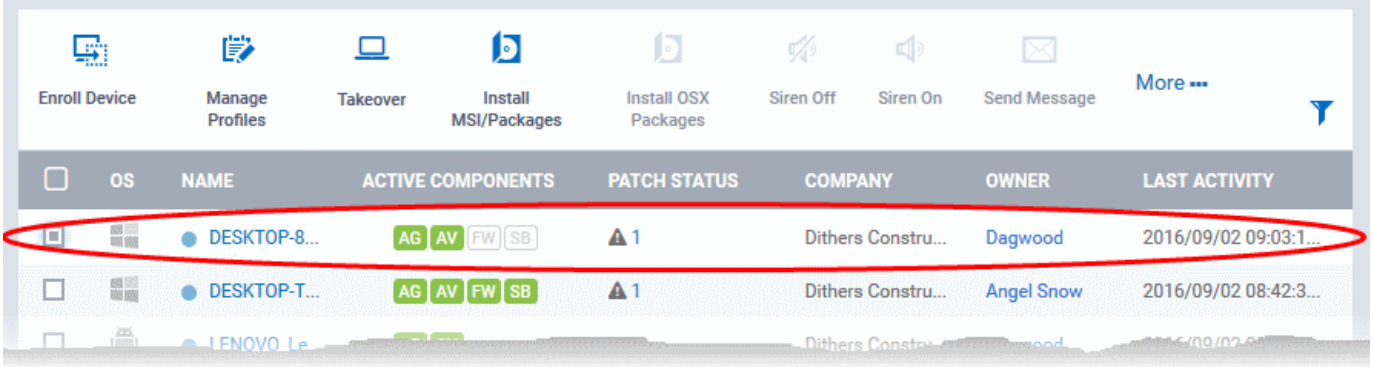
Enroll Windows PCs

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 '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 each group. OS specific profiles which are applied to a group will be deployed appropriately to devices.

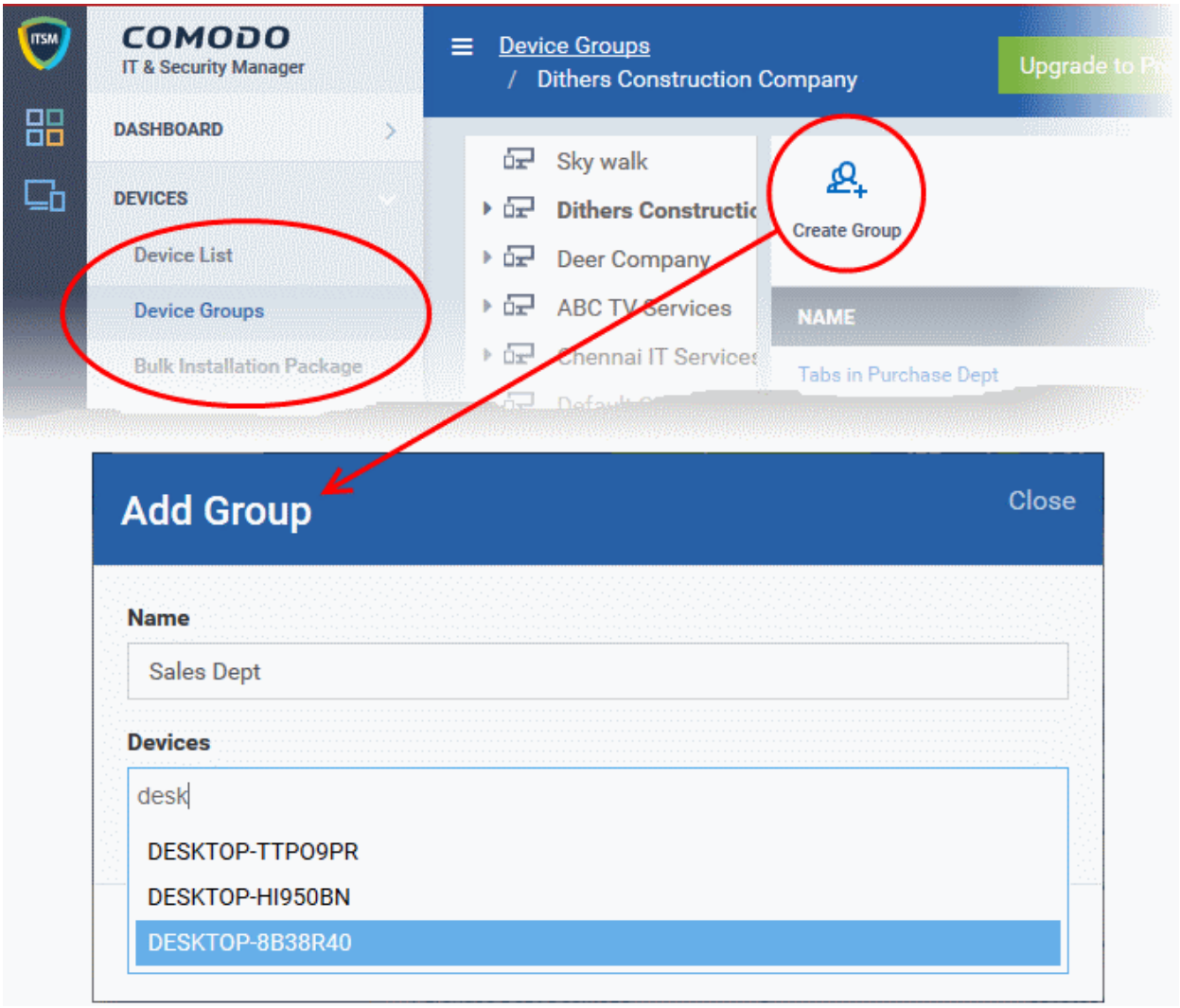
- C1 MSP customers can create separate device groups for each Company/Organization enrolled in their Comodo One account.
- C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.

Refer to Managing Companies if you need more help with this.

To create a device group

- Click the 'Devices' tab on the left and choose 'Device Groups'
- C1 MSP customers should choose the company whose devices they wish to manage on the left
- Click 'Create Group' on the top 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.

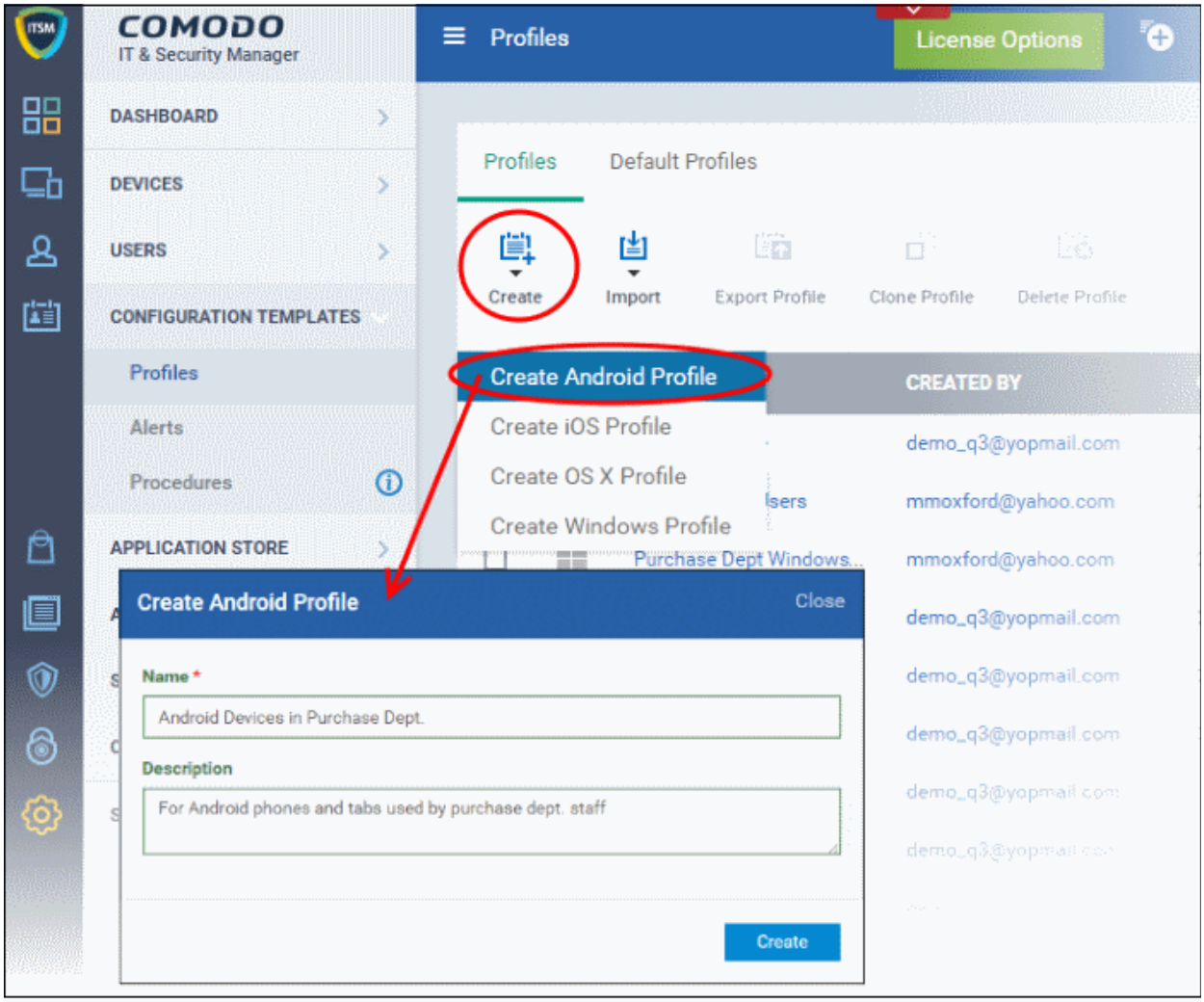
Profile specifications differ between Android, iOS, Mac OS X and Windows Devices:

- Android profiles
- iOS profiles
- Mac OS X profiles

- Windows Profiles

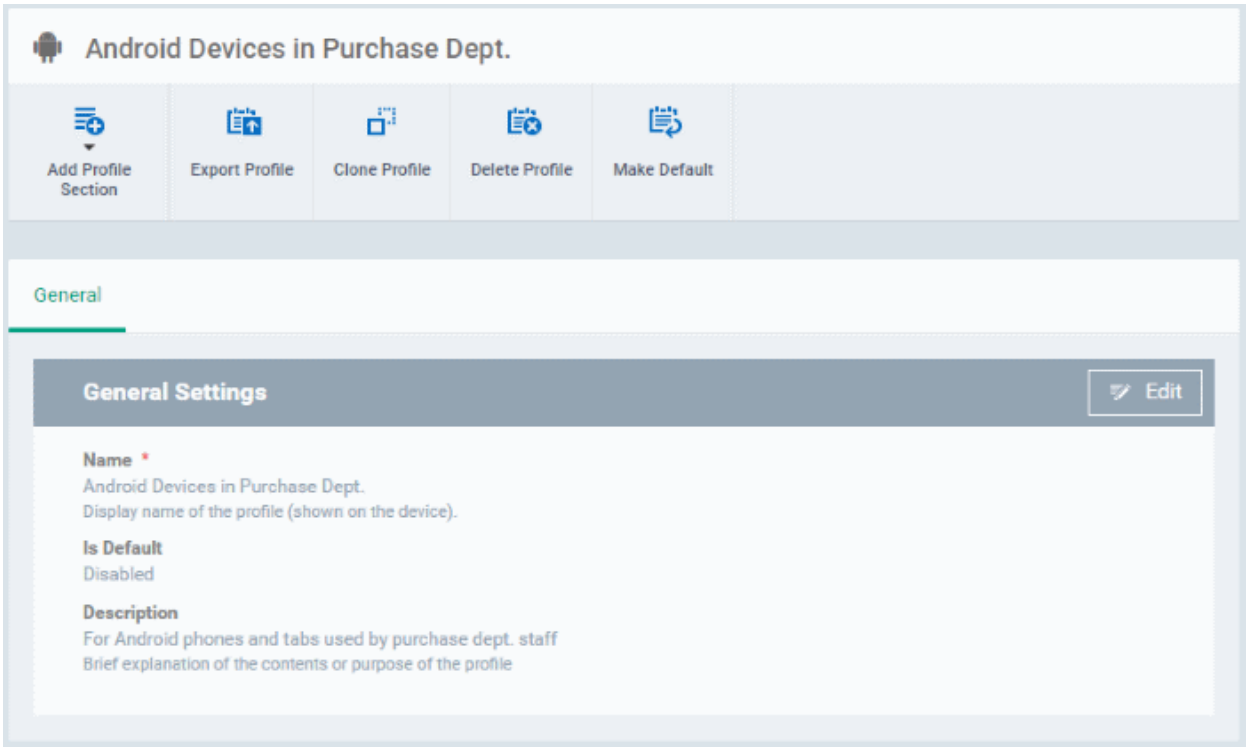
To create an Android Profile

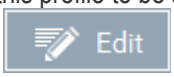
- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then choose 'Create Android Profile'.



- 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.

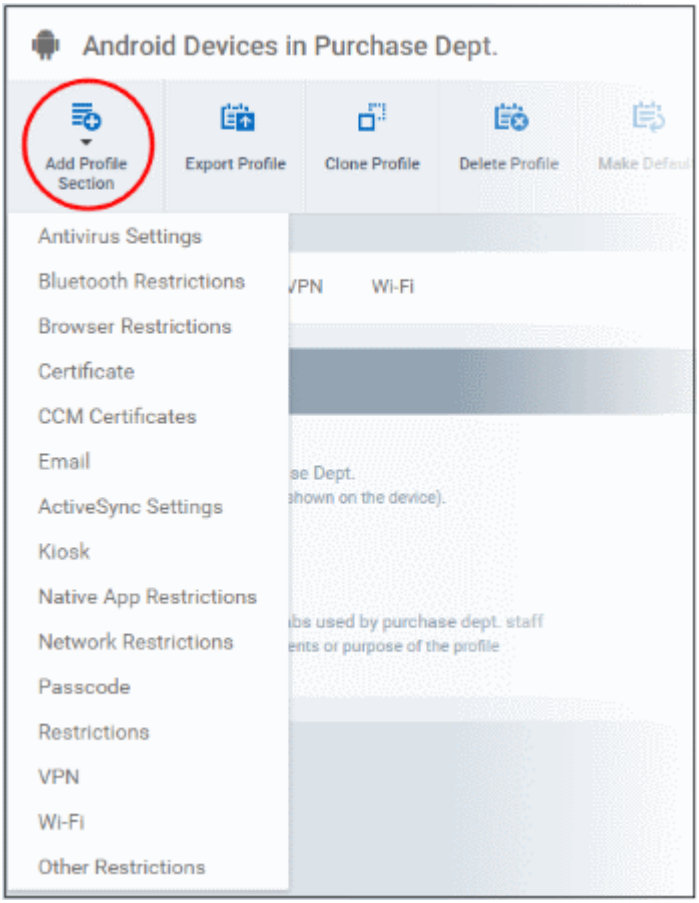


- If you want this profile to be a default policy, click the 'make default' button at the top. Alternatively, click the 'Edit' button 

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.

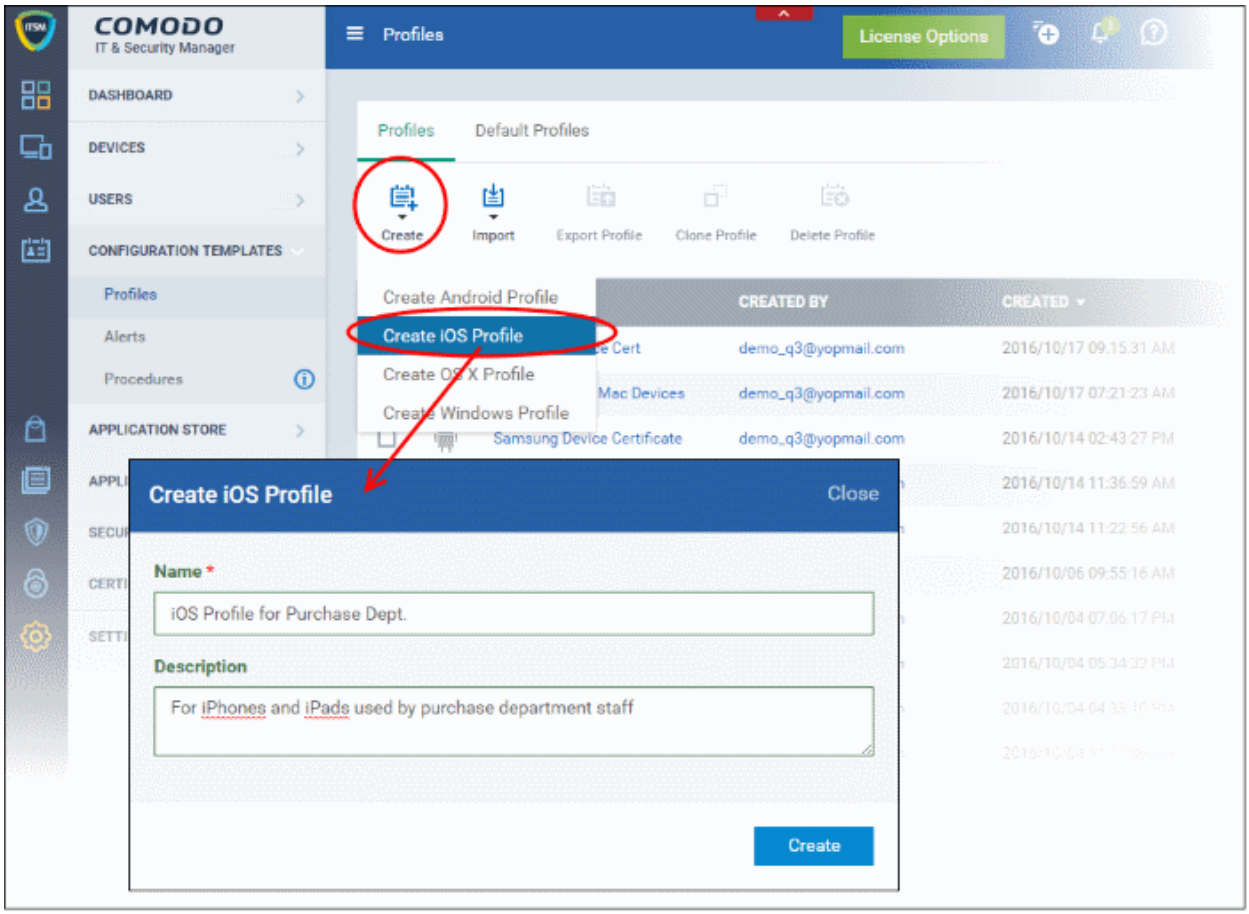
See Profiles for Android Devices in the full guide for more information on these settings. In brief:

- **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.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM).
- **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.

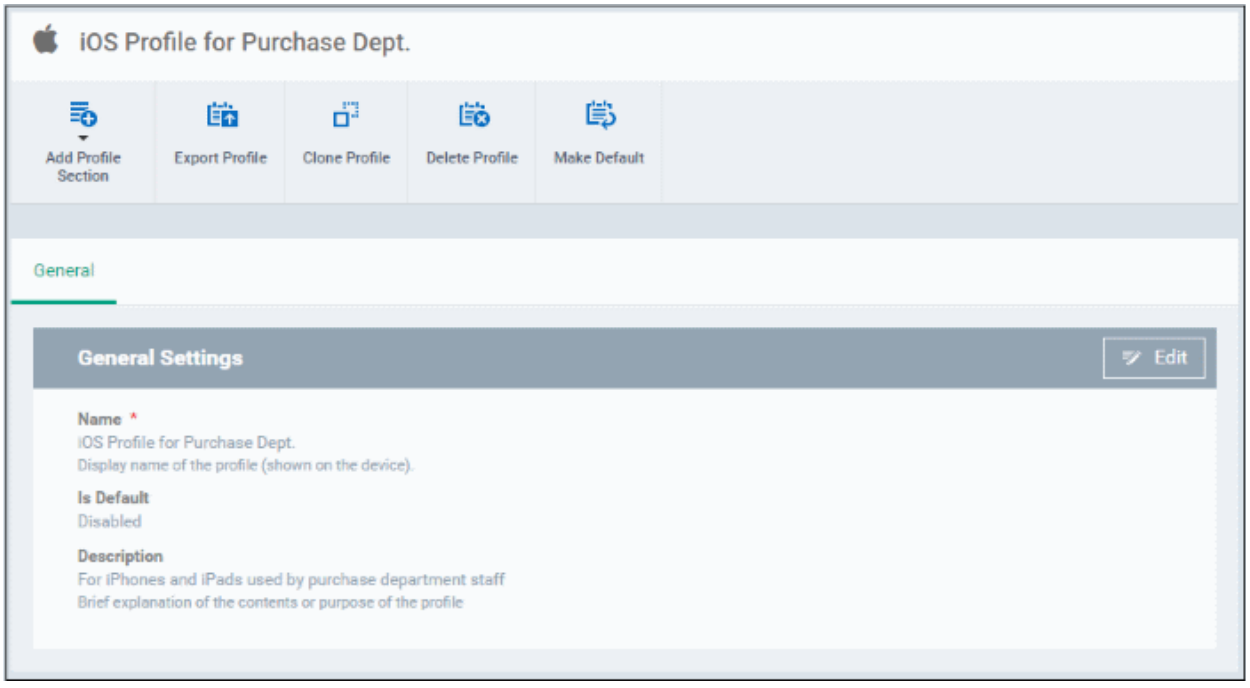
- **Kiosk** - Enable and configure Kiosk Mode for SAFE devices like the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices and whether SMS/MMS are allowed. This profile is supported for SAFE devices only.
- **Native App Restrictions** - Configure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



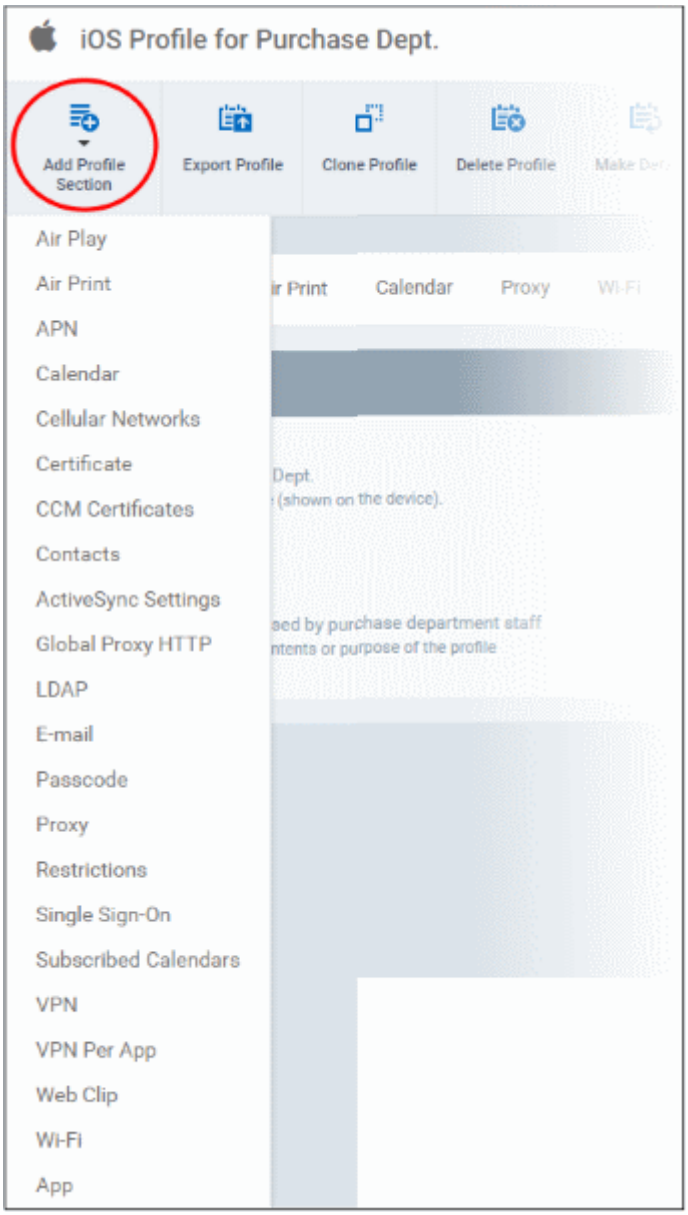
- If you want this profile to be a default policy, click the 'Make default' button at the top. Alternatively, click the 'Edit' button 

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.

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

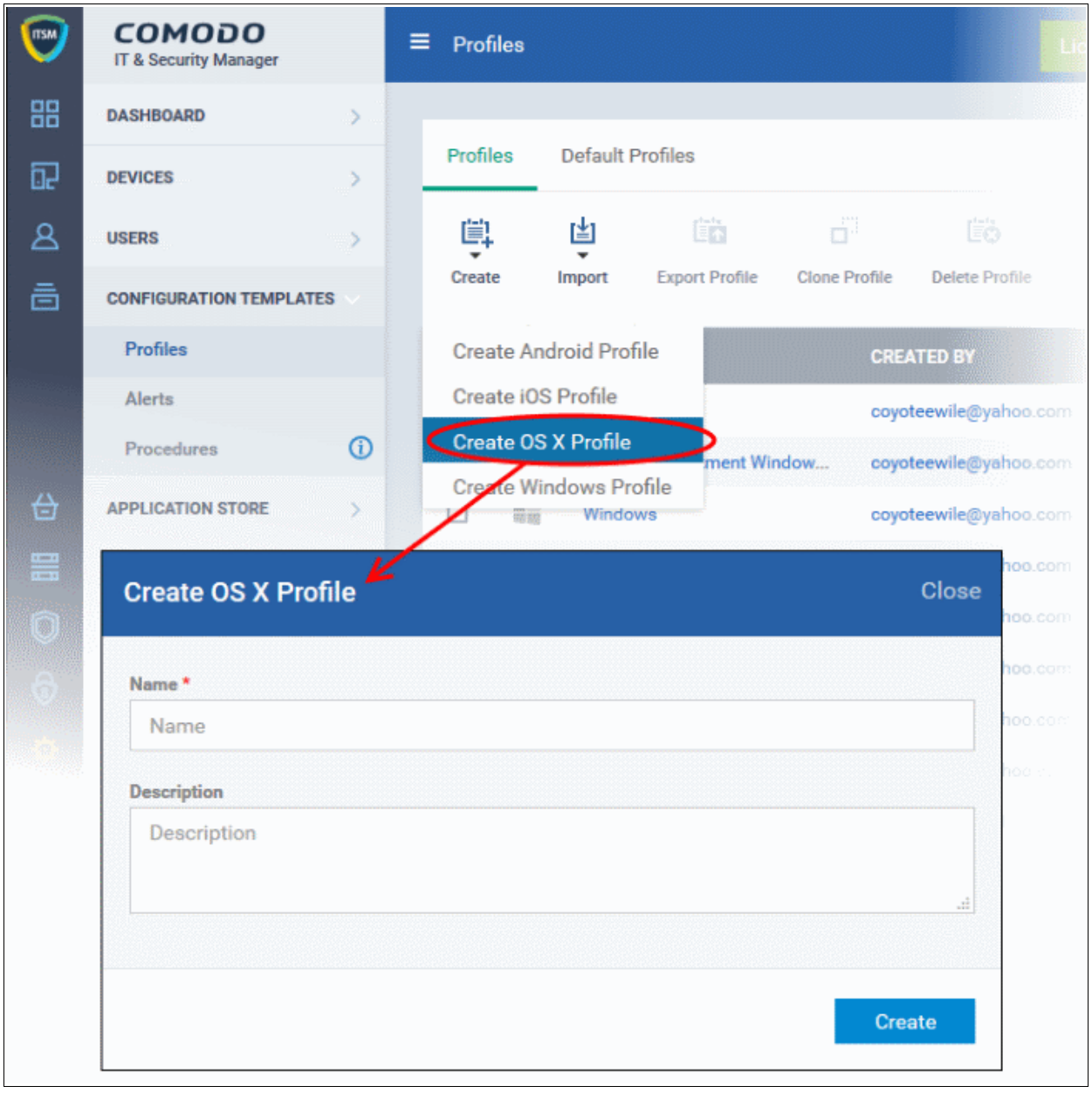
+)

- **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 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).
- **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.

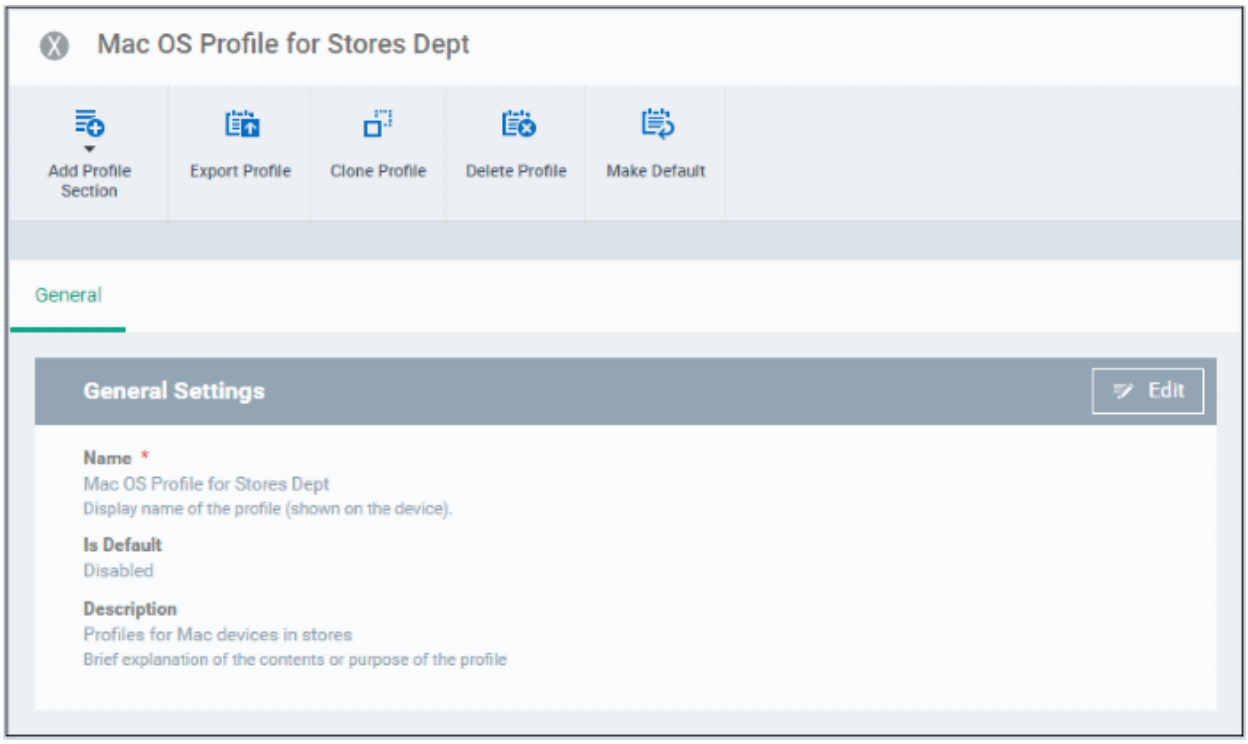
- **App Lock** - Configure restrictions on usage of device resources for selected applications.

To create Mac OS X Profile

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



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

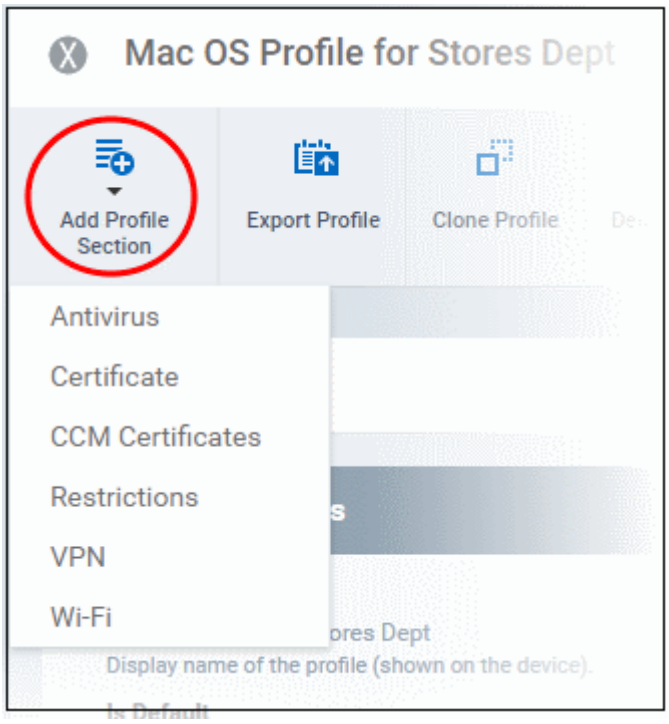


- If you want this profile to be a default policy, click the 'Make default' button at the top. Alternatively, click the 'Edit' button 

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.

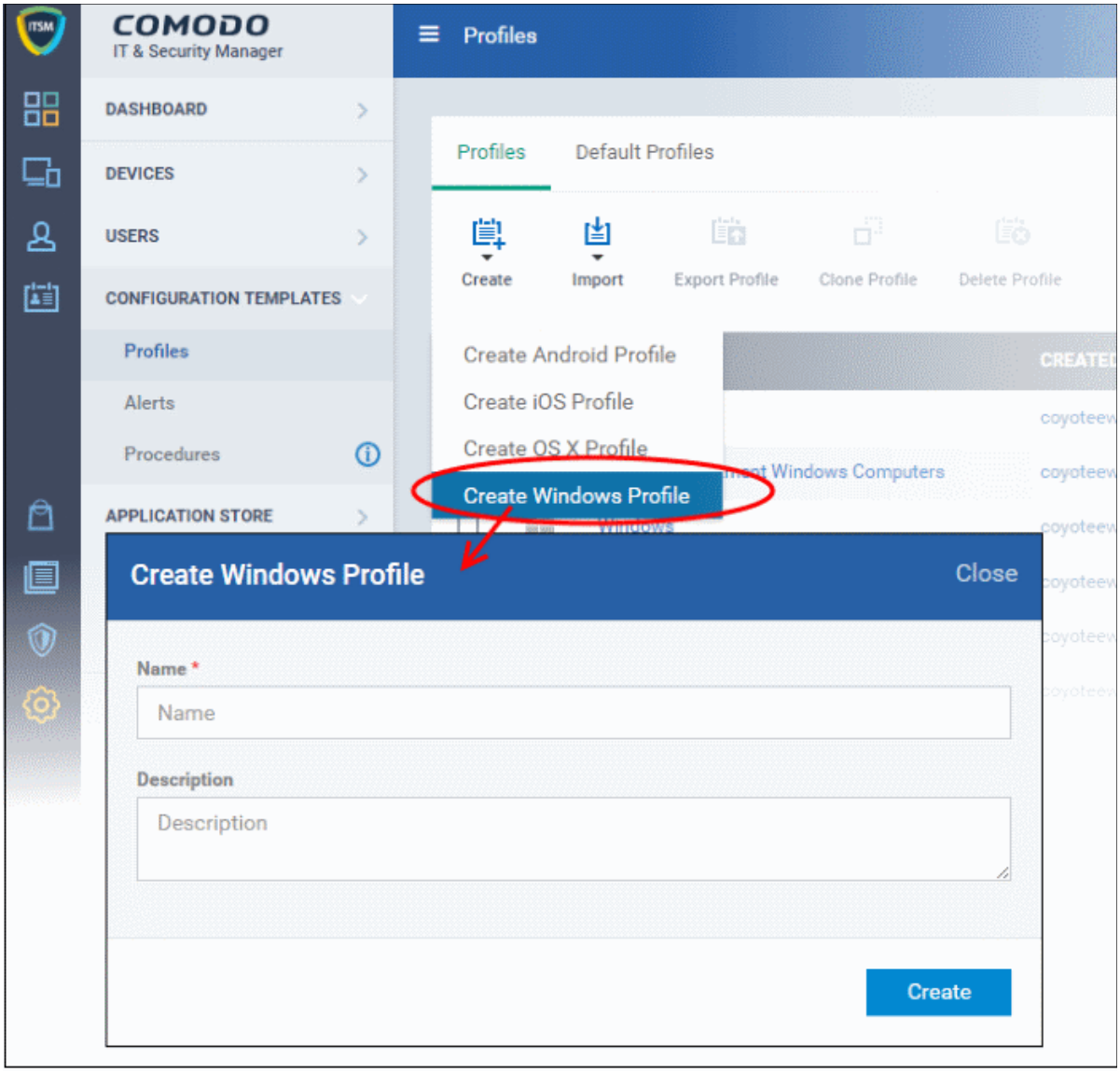
- Click the 'Add Profile Section' drop-down and select the component from the list that you want to include for the profile



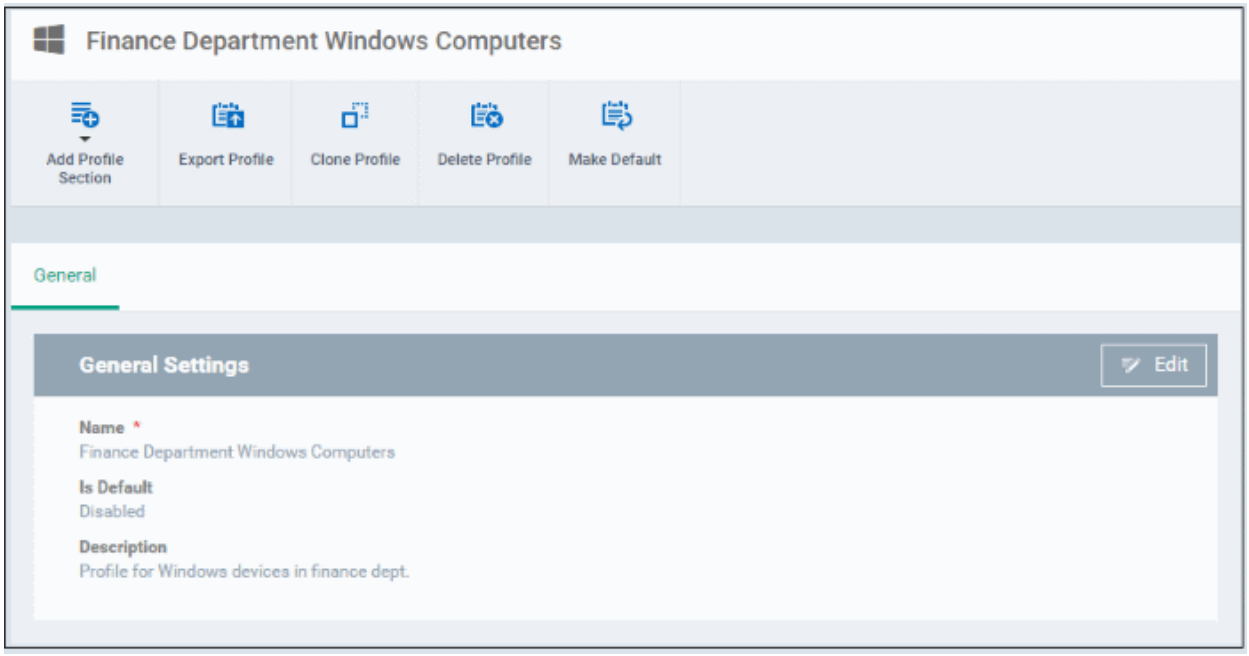
- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **Certificates** - Upload certificates and this will act as a certificate store from which the certificates can be 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).
- **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.

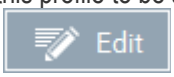
To create a Windows profile

- Click the 'Configuration Templates' tab 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'.

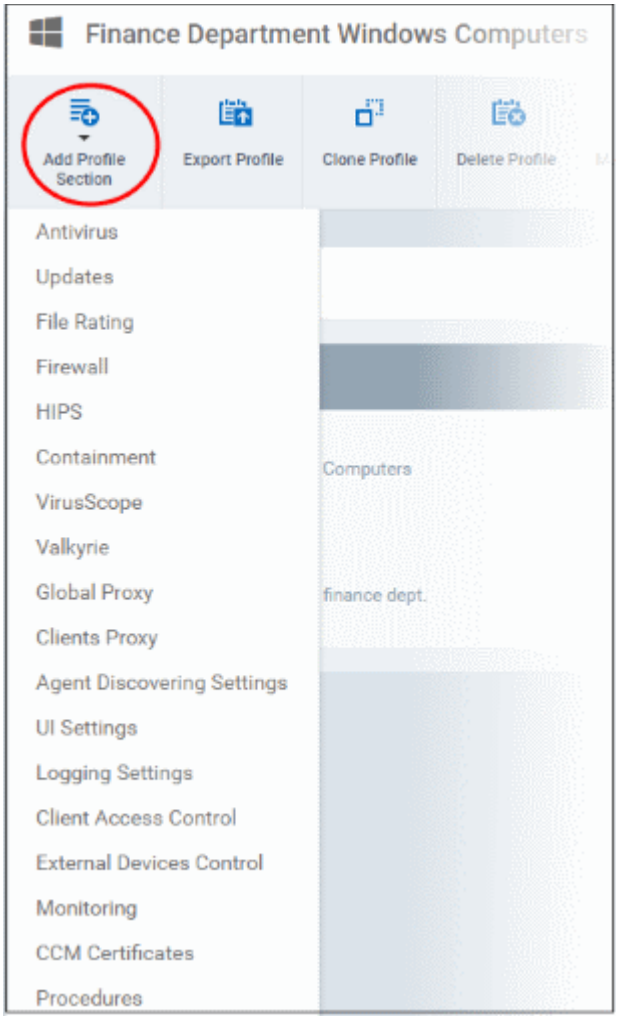
The next step is to add components for the profile.

- 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.



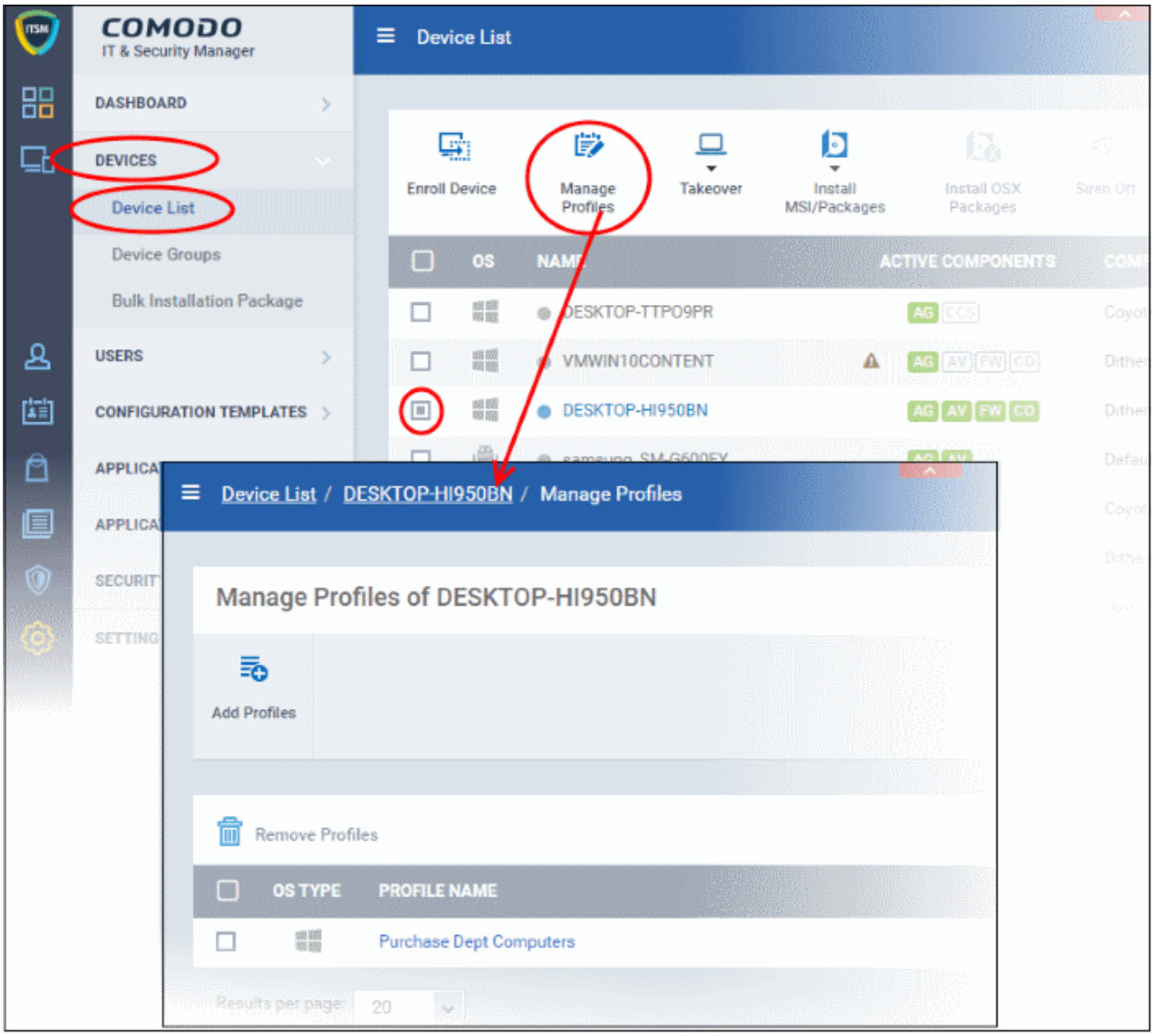
See **Profiles for Windows Devices** in the full guide for more information on these settings. In brief:

- **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**
- **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.
- **CCS UI Settings** - Allows you to 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, device online status and more.
- **Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM).
- **Procedures** - Allows you to add, view, delete and prioritize procedures which have been added to a profile.

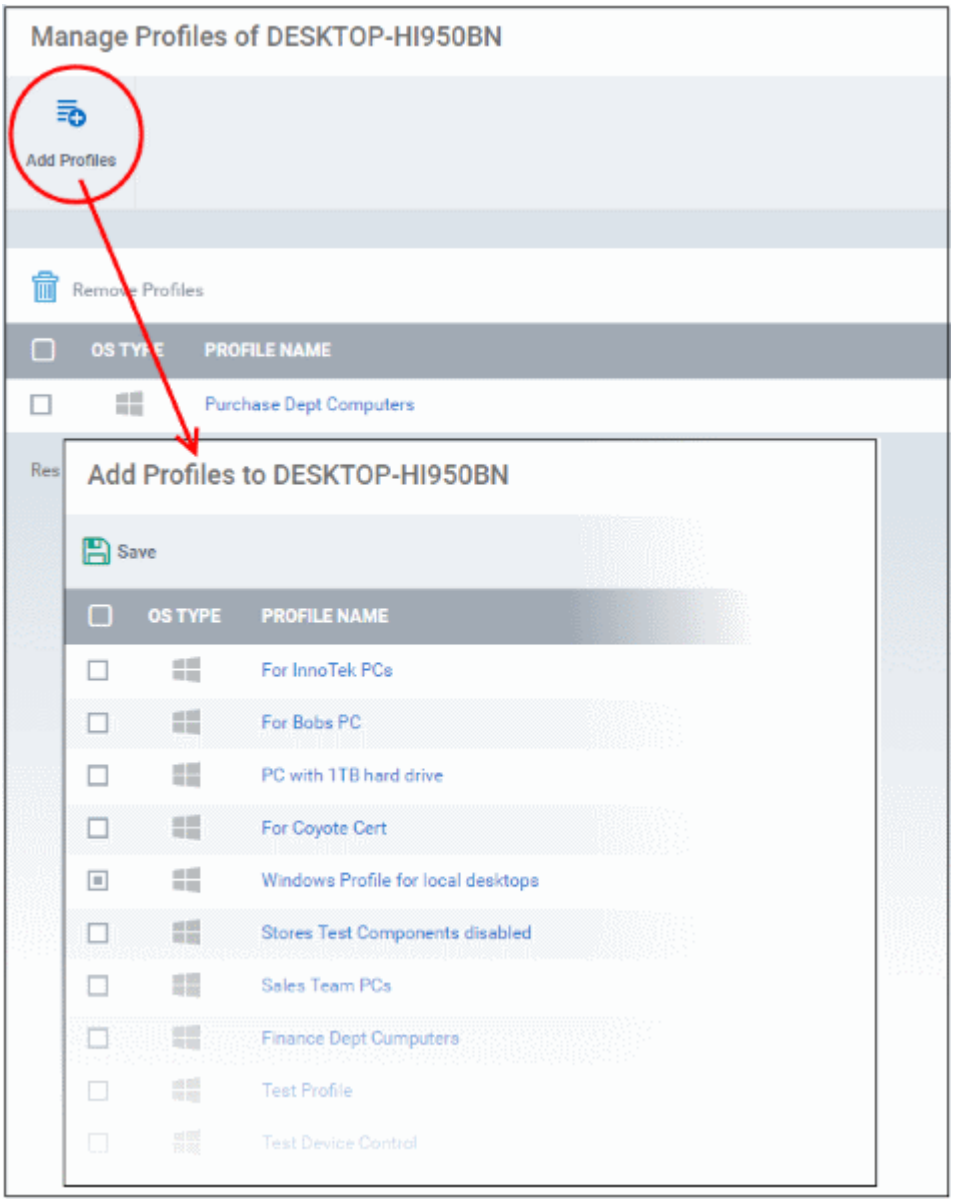
Step 7 - Apply profiles to devices or device groups

1. Click the 'Devices' tab on 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 on the left and choose 'Device Groups ' from the options.
2. Choose the Company to view the list of groups in the right pane (for C1 MSP customers)
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' 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.

1.4. Logging into the Admin Console

Upon successful subscription of the service, the administrator will receive an account activation email containing the username and the activation link. The administrator can click the link to activate the account and set a password. Once activated, the administrator can login to the web based ITSM application using any Internet browser, by entering the URL of the ITSM interface.

- Enter your username and password and click 'LOGIN'.

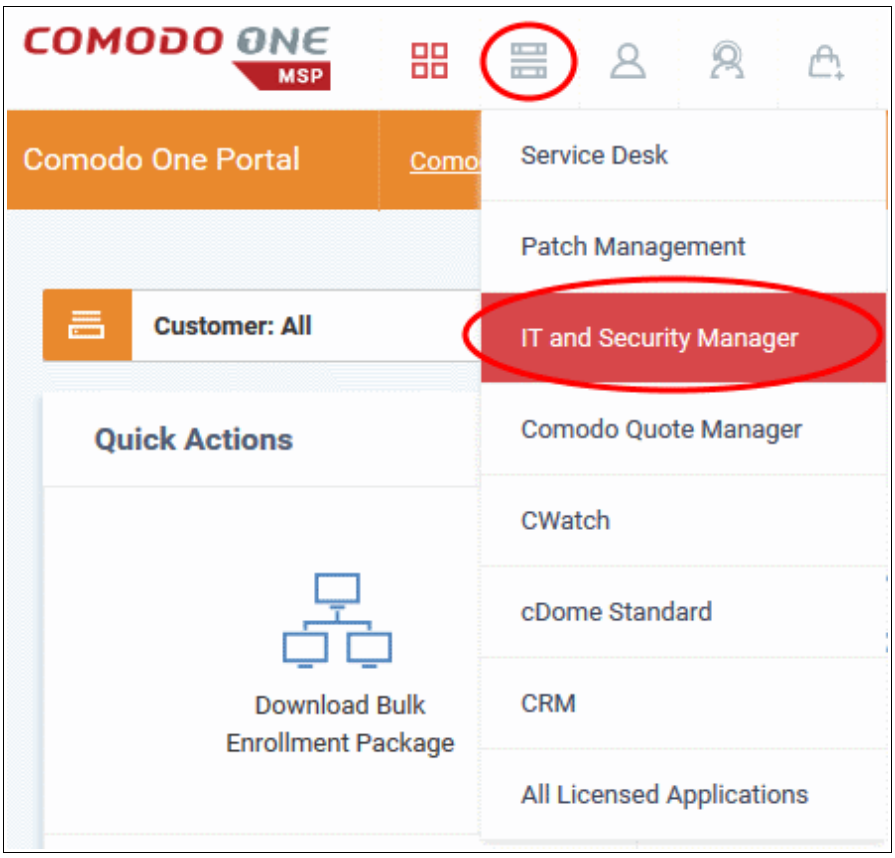
Important Note: Password is case sensitive. Please make sure that you are entering it in proper case and Caps Lock is set OFF.

If you have forgotten your password, click the 'I forgot my password' link below the Login button. In the 'Password recovery' page, complete the procedure. A mail will be sent to your registered email id, where by clicking the 'Reset password' link you can reset a new a password.

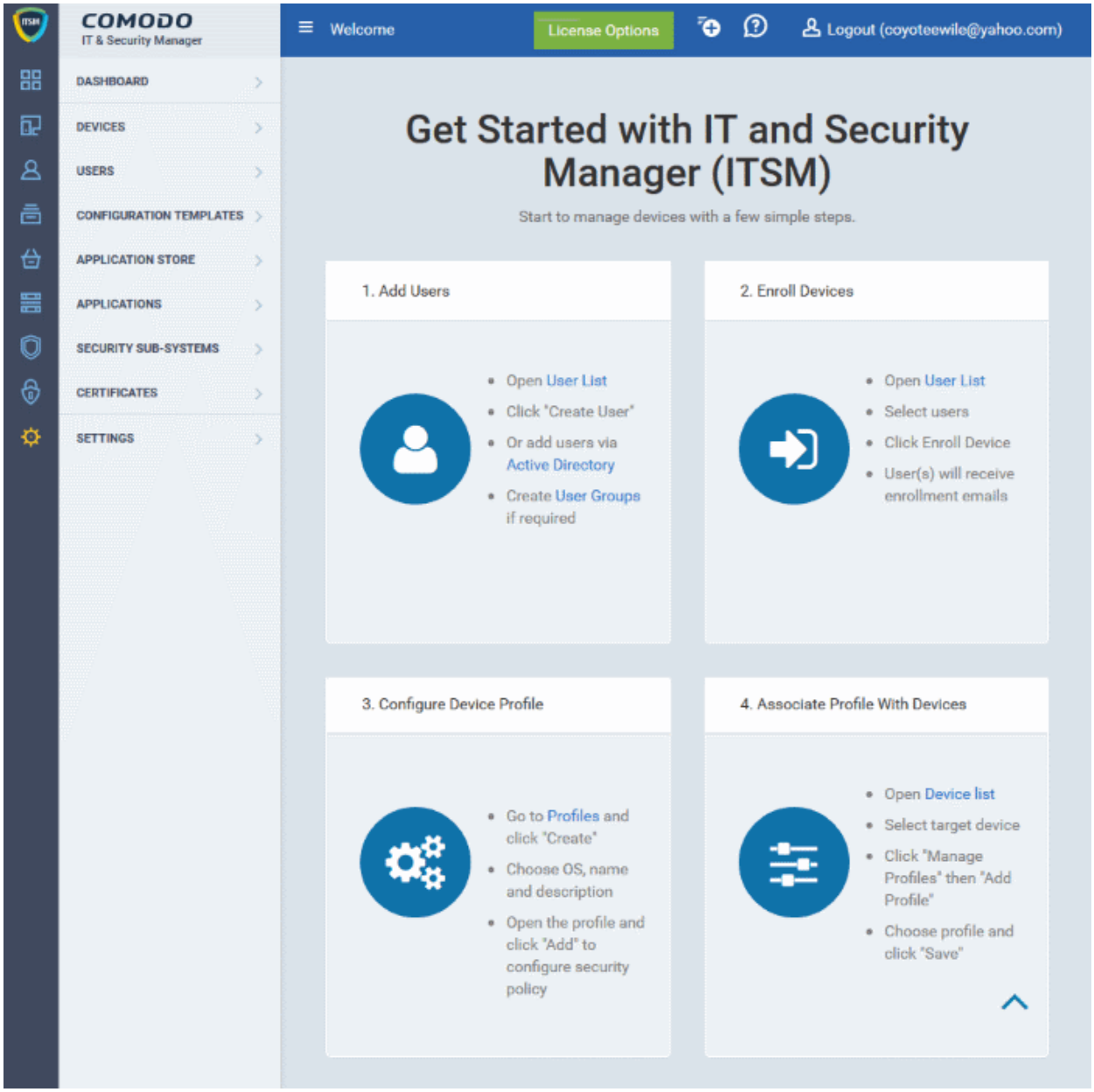
After successful login, the ITSM welcome screen will be displayed.

C1 customers can open the ITSM module after logging-in to their C1 account at https://one.comodo.com/app/login.

- Click 'Licensed Application' at the top, then 'IT and Security Manager' from the licensed applications.



The ITSM welcome screen will be displayed.



The screen contains shortcuts to enroll users and start managing devices in a few steps:

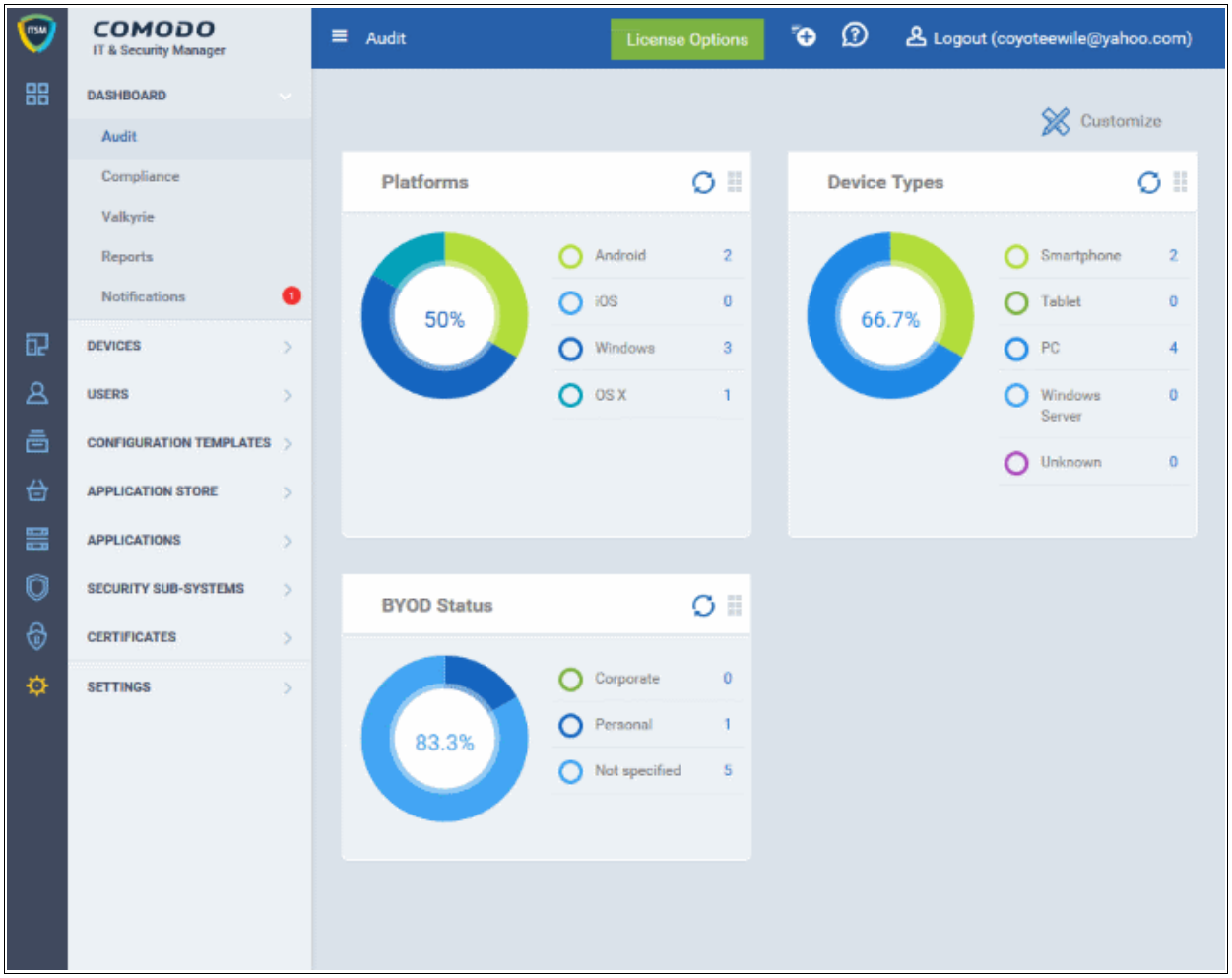
- **Add Users** - Allows you to add new users by clicking the icon and choosing 'Create User' from the 'User List' interface. Refer to the section '**Creating New User Accounts**' for more details. The tile also contains shortcut to 'Active Directory' settings interface to integrate an AD server and import the user groups from it. Refer to the section '**Importing User Groups from LDAP**' for more details.
- **Enroll Devices** - Allows you to enroll users' devices for management by clicking the icon and selecting the user(s) from the 'User List' interface and clicking 'Enroll Devices' from the top. Refer to the section **Enrolling User Devices for Management** for more details.
- **Configure Device Profile** - Allows you to create and manage configuration profiles for Android, iOS and Windows devices by clicking the icon. Refer to the section **Configuration Profiles** for more details.
- **Associate Profile With Devices** - Allows you to deploy and manage configuration profiles on devices by clicking the icon. Refer to the section **Devices** for more details.

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.

2. The Administration Console

The Administrative Console is the nerve center of Comodo IT and Security Manager (ITSM), allowing administrators to add or import users, enroll devices, create groups of devices, apply configuration profiles, run Antivirus (AV) scans and more.



Once logged-in, administrators can navigate to different areas of the console by clicking the tabs on the left hand side.

Dashboard - Allows administrator to view snapshot summaries of details like operating systems, device types, AV scan status, Compliance status of devices enrolled to ITSM, Valkyrie analysis results and more, as pie-charts. See The Dashboard for more details.

Devices - Allows administrators to manage and control enrolled devices, remotely install applications, generate sirens, wipe, lock and power off enrolled devices, remotely install and manage apps on devices, manage device groups and more. Refer to the section Devices for more details.

Users - Allows administrators to create and manage users and user groups, enroll of their devices and assign configuration profiles to devices. Refer to the section Users and User Groups for more details.

Configuration Templates - Create and manage configuration profiles to be applied to enrolled iOS and Android Smartphones and Tablets, Windows and Mac OS X endpoints. Refer to the section Configuration Templates for more details.

Application Store - Allows administrators to add apps to be pushed to managed iOS and Android devices. Refer to

the section App Store for more details.

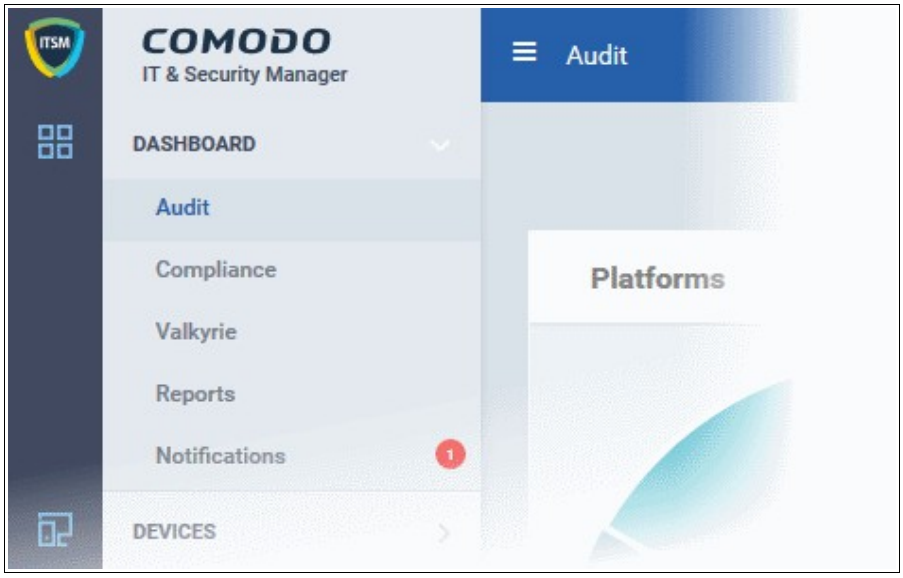
Applications - Allows administrators to view and manage applications installed on enrolled Android and iOS devices, view files installed on managed Windows devices, contained programs, view and manage software vendors list and manage OS patch installation on to managed Windows devices. Refer to the section Applications for more details.

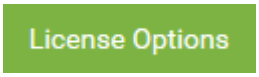
Security Sub-Systems - Allows administrators to run AV scans and virus signature database updates on the enrolled devices, manage identified malware, view threats, manage quarantined items, view and manged contained applications and more. Refer to the section Security Sub-Systems for more details.

Certificates - Allows administrators to view and manage client and device certificates issued to end-users and enrolled devices by Comodo Certificate Manager (CCM). The Certificates tab will be available only if you have integrated your CCM account to ITSM. Refer to the section Managing Certificates Installed on Devices for more details.

Settings - Allows administrator to create admin and user roles with different privilege levels and appropriately assign them to users, configure the behavior of various ITSM components and agents, renew/upgrade licenses and more. See Configuring Comodo Mobile IT and Security Manager for more details.

The buttons on the top of the interface allows to view the ITSM notifications, create users and enroll devices, expand/collapse the left side tabs and logout.

	Clicking this button will display the 'Create User' and 'Enroll Device' drop-down. Refer to the sections 'Creating New User Accounts' and 'Enrolling Users' Devices for Management' for more details.
	The number beside the bell icon indicates the unread ITSM notifications. Click this to view the notification in the drop-down. On clicking the notification, or on 'See all notifications' link the 'List of Notifications' screen will open. If the user logs in directly through the ITSM url, the bell icon will appear on the top right corner of the ITSM title bar whereas when the user logs into ITSM through the Comodo One website, then the bell icon will appear in the top right corner of the C1 title bar. Refer to the explanation of 'Notifications' in the section The Dashboard for more details.
	Contains links to the online user guide, to the Comodo One MSP and Enterprise forums and allows you to email our support department.
	Clicking the menu button will expand/collapse the menu tabs at the left tabs. When the menu tabs are in collapsed state, placing the mouse cursor over a menu will display the sub menus under it. 

	Clicking the logo will open the 'Welcome' screen. Refer to the section 'Logging into your Administrative Console' for more details.
	Displays the username of the person currently logged in. Click this to log out of ITSM interface.
	Allows you to upgrade to the Premium or Platinum version of ITSM.

3. The Dashboard

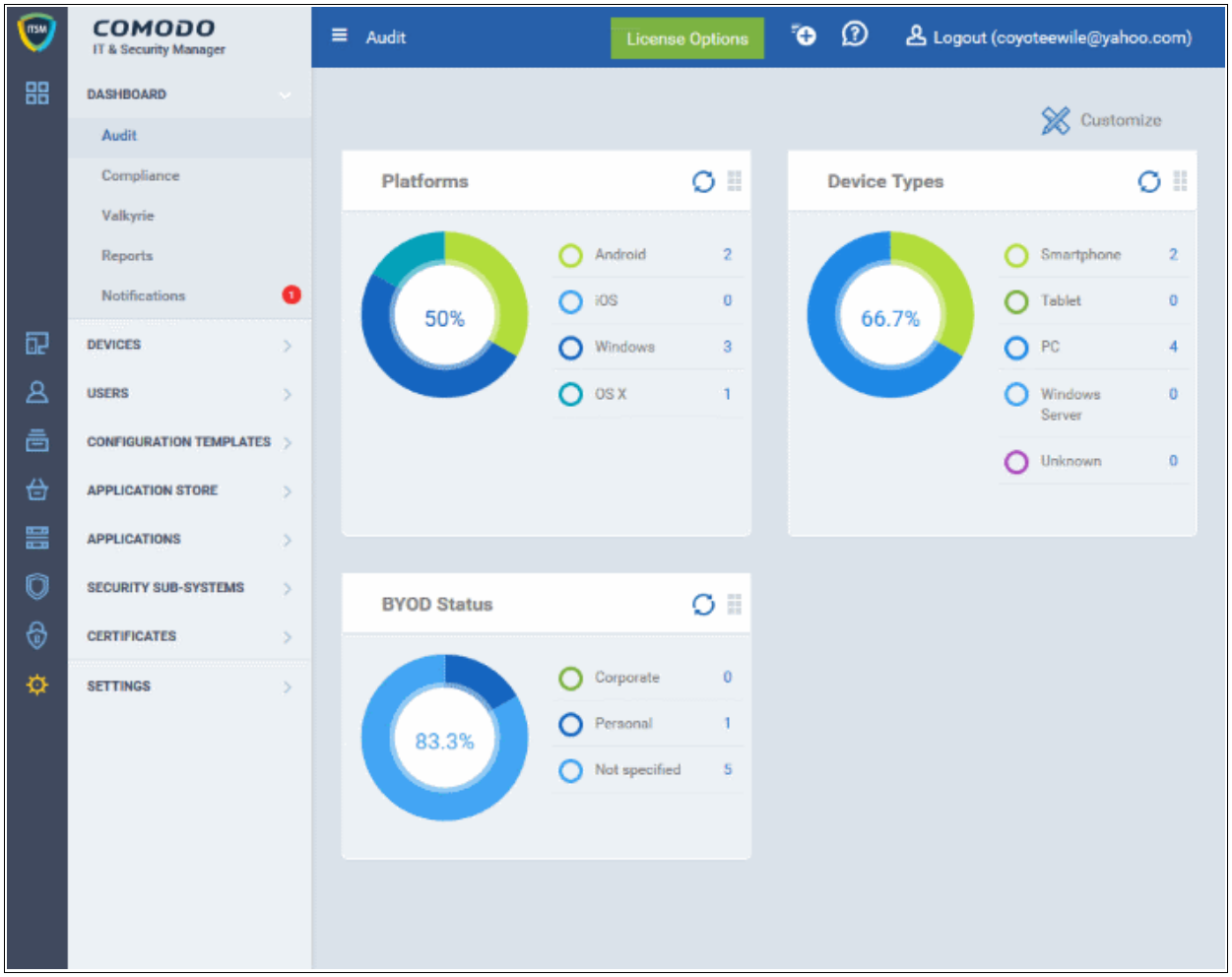
The Dashboard displays a snapshot summary of devices enrolled to Comodo IT and Security Manager (ITSM). It contains pie charts displaying device types, platforms, ownership, antivirus scan status and compliance status. The dashboard also enables you to view Valkyrie results, a list of notifications and to generate reports.

To open the 'Dashboard', click the Dashboard tab from the left hand side. It is divided into five sections:

- Audit - Displays statistical information of types of managed devices and ownership details as pie-charts. Refer to the Audit section for more details.
- Compliance - Displays statistical information about managed devices such as devices that are active and inactive for the past 24 hrs, devices with viruses, devices with blacklisted applications, devices responses for virus scan, rooted and jailbroken devices, devices that are online and devices scan statuses. Refer to the section Compliance for more details.
- Valkyrie - Displays the results of analysis of unknown files automatically uploaded from managed Windows devices from Valkyrie, as pie-chart. Refer to the section Valkyrie for more details.
- Reports - Displays a list of reports generated by ITSM and enables you to generate new reports. Refer to the Reports section for more information.
- Notifications - Displays a list of notifications sent to the administrator by ITSM. Refer to the section Notifications for more details.

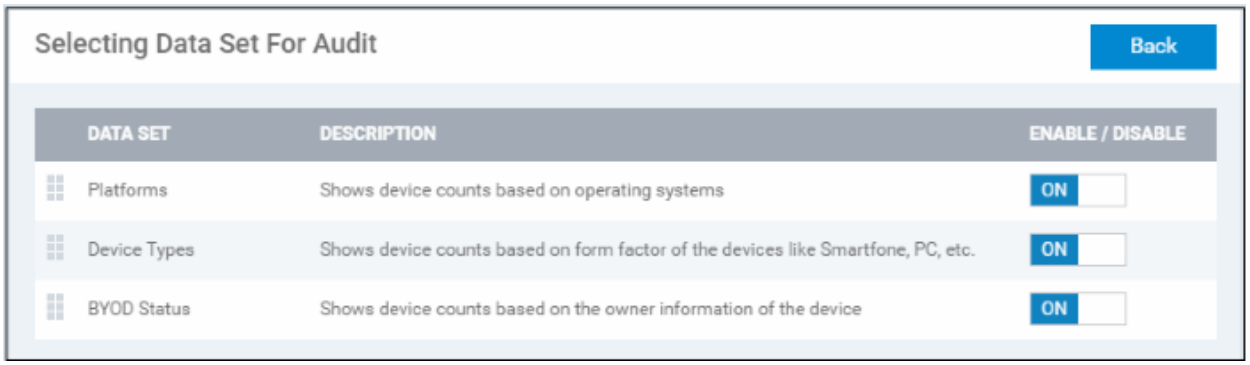
Audit

The Audit screen provides a snapshot summary of devices enrolled to Comodo IT and Security Manager (ITSM), their types and ownership as pie charts.



To set which charts are shown, first open either the 'Audit', 'Compliance' or 'Valkyrie' dashboard using the links on the left then click 'Customize' at top of the interface.

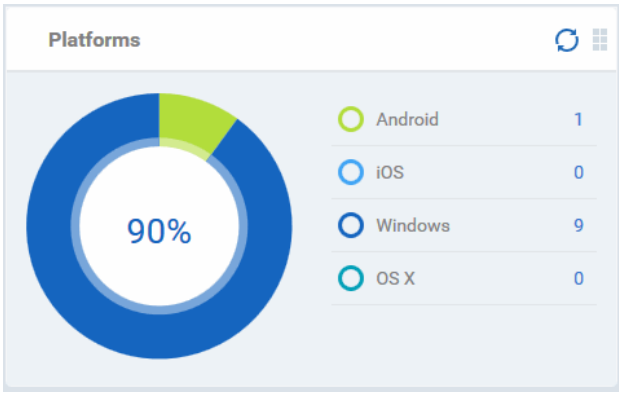
The 'Options' interface will be displayed.



- Use the 'On/Off' switches to add or remove a specific chart from the dashboard
- Click 'Back', to return to the main interface

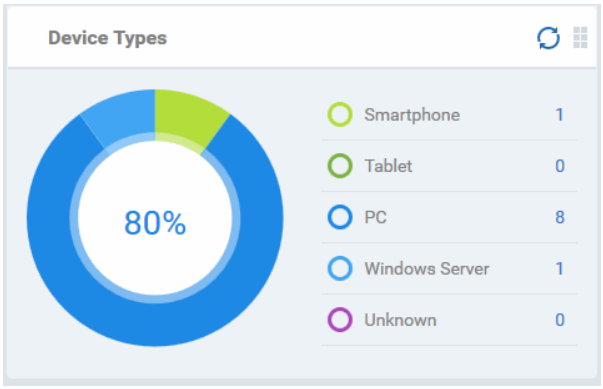
- To refresh data in a tile, click the 'Refresh' icon at top right
- To swap tiles as per your preference, click and hold the grid icon at top right and move it.

Platform Details



The 'Platform details' chart shows devices by operating system. Placing the mouse cursor over a sector or on the respective legend displays the details.

Clicking on any of the legend will open the respective 'Device List' page. For example, clicking on 'Android' in the legend will open the 'Device List' page displaying the list of Android devices. Refer to the section '**Devices**' for more details.

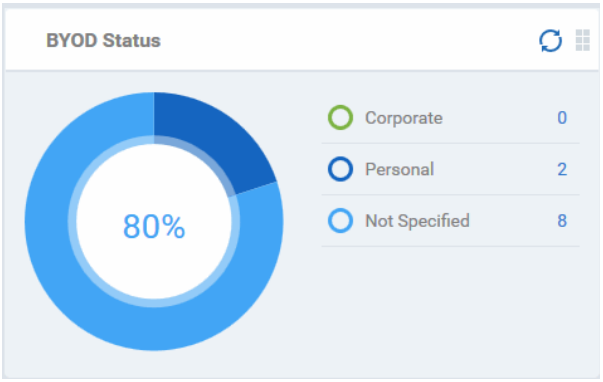


Device Types

The 'Device Types' pie chart shows the composition of your device fleet by device type. Placing the mouse cursor over a sector or on the respective legend displays the details.

Clicking on any of the legend will open the respective 'Device List' page. For example, clicking on 'Tablet' in the legend will open the 'Device List' page displaying the list of tablet devices. Refer to the section '**Devices**' for more details.

BYOD Status



The 'BYOD status' pie chart shows devices by ownership type. This can be 'Corporate', 'Personal' or 'Not Specified'. Placing the mouse cursor over a sector or on the respective legend displays the details.

Clicking on any of the legend will open the respective 'Device List' page. For example, clicking on 'Personal' in the legend will open the 'Device List' page displaying the list of devices that are categorized as personal. Refer to the section '**Devices**' for more details.

Note: The device ownership type can be changed by administrators from the device details screen > Change BYOD and then selecting the ownership type from the options.

Compliance

The compliance dashboard monitors the status of managed devices with regards to various security and activity criteria. Charts shown include, devices with viruses, devices with blacklisted applications, device requiring database updates, rooted and jail-broken devices, devices which are unresponsive and more.

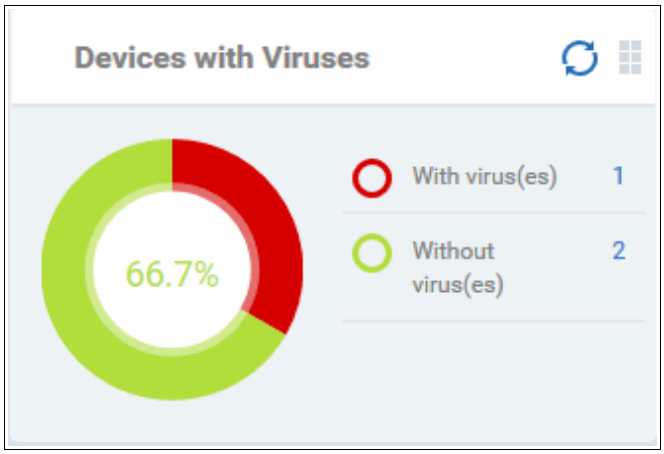
To view the compliance status of devices, click 'Dashboard' in the left navigation then 'Compliance'.


COMODO
IT & Security Manager
DASHBOARD
Audit
Compliance
Valkyrie
Reports
Notifications
DEVICES
USERS
CONFIGURATION TEMPLATES
APPLICATION STORE
APPLICATIONS
SECURITY SUB-SYSTEMS
CERTIFICATES
SETTINGS
Compliance
License Options
Logout (coyoteewile@yahoo.com)
Customize
Active and Inactive Devices Last 24 Hours
50%
Active devices 3
Inactive devices 3
Devices with Viruses
66.7%
With virus(es) 1
Without virus(es) 2
Devices with Blacklisted Applications
100%
With blacklisted applications 0
Without blacklisted applications 2
Devices Responses for Virus Scan
50%
Scan response received 3
No response received 3
Rooted and Jailbroken Devices
100%
Rooted and jailbroken 0
Normal 6
Devices with Device Management Apps
100%
With device management app 6
Without device management app 0
Device Online
100%
Online 0
Offline 6
Scan Status
50%
Unknown 3
Scan canceled 0
Complete 1
Scanning 1
Viruses found 1
Antivirus DB Update
83.3%
Unknown 5
Complete 1
Updating 0
Security Product Configuration
83.3%
Safe 5
Not protected 1

- To customize the charts shown in the interface, click the 'Customize' button
- To refresh the data in a tile, click the 'Refresh' icon at top right
- To move tiles around, click and hold the grid icon in the top right corner and drag the tile to the desired position.

Devices With Viruses

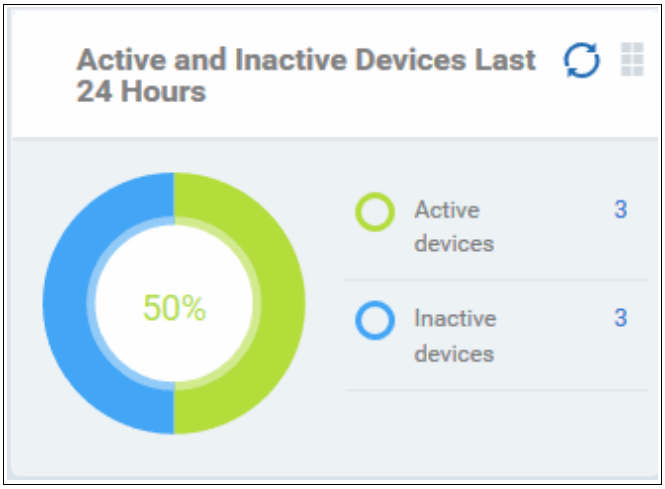
Shows how many enrolled devices are affected by viruses and how many are clean. Placing the mouse cursor over a sector or the legend displays further details. Refer to the section Antivirus Scans for details about scanning for viruses on enrolled devices.



Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'With virus(es)' will open the 'Device List' page displaying devices that contain viruses. Refer to the section 'Devices' for more details.

Active and Inactive Devices Last 24 Hours

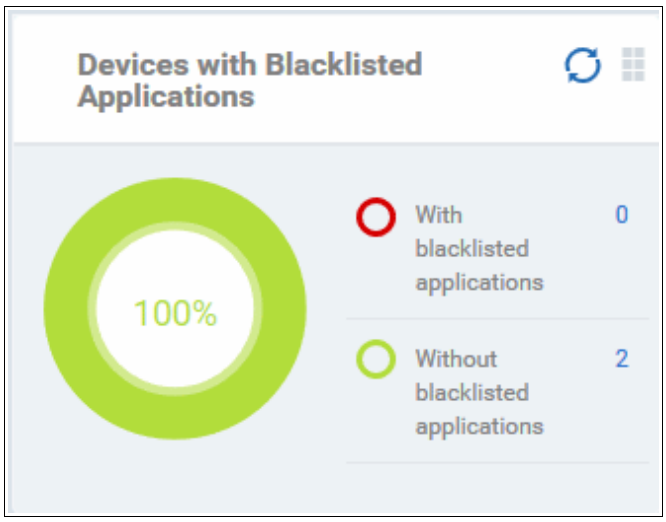
Shows the connectivity status of enrolled devices. Devices which have not contacted ITSM for more than 24 hours are marked as 'inactive'. Placing the mouse cursor over a sector or the legend displays the further details.



Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'Active Devices' will open the 'Device List' page displaying the list of active devices. Similarly clicking on the 'Inactive Device' legend will open the 'Device List' page displaying the list of inactive devices. The devices screens allow you to manage the enrolled devices. Refer to the section 'Devices' for more details.

Devices with Blacklisted Applications

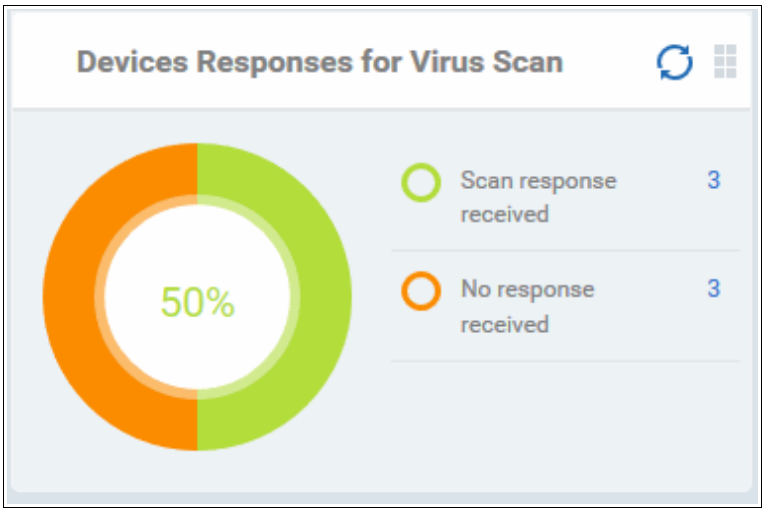
Displays how many devices contain blacklisted apps versus those that are free of blacklisted apps. Placing the mouse cursor over a sector or the legend displays further details. Refer to the section Applications for details about adding and removing apps from blacklist.



Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'With Blacklisted Applications' legend will open the 'Device List' page displaying the list of devices that have blacklisted applications on them. Refer to the section 'Devices' for more details.

Devices Responses for Virus Scan

Shows how many devices have responded to virus scan requests. Placing the mouse cursor over a sector or the legend displays the further details. Refer to the section Antivirus Scans for details about scanning for viruses on enrolled devices.

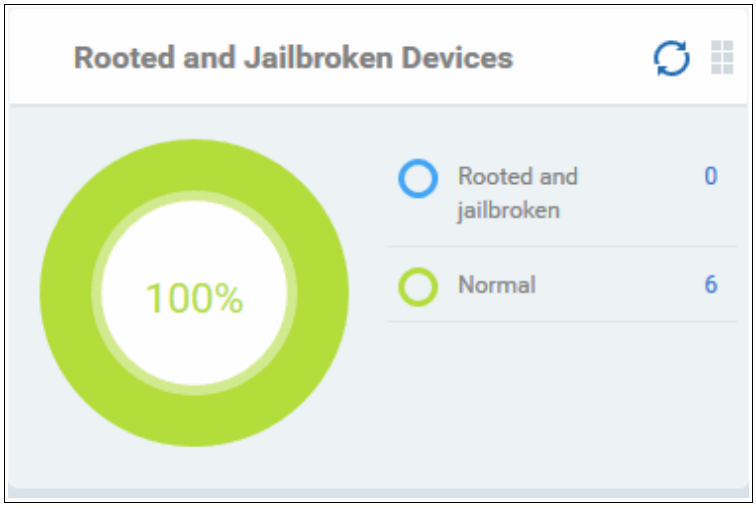


Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'With response on virus scan' legend will open the 'Antivirus Device List' page displaying the list of devices that are responding to scan command.

The 'Antivirus Device List' page allows you to run antivirus scans on selected devices. Refer to the section Antivirus Scans for more details.

Rooted And Jail-broken Devices

Shows how many devices in your fleet are are rooted or jail-broken. Placing the mouse cursor over a sector or the legend displays the further details.

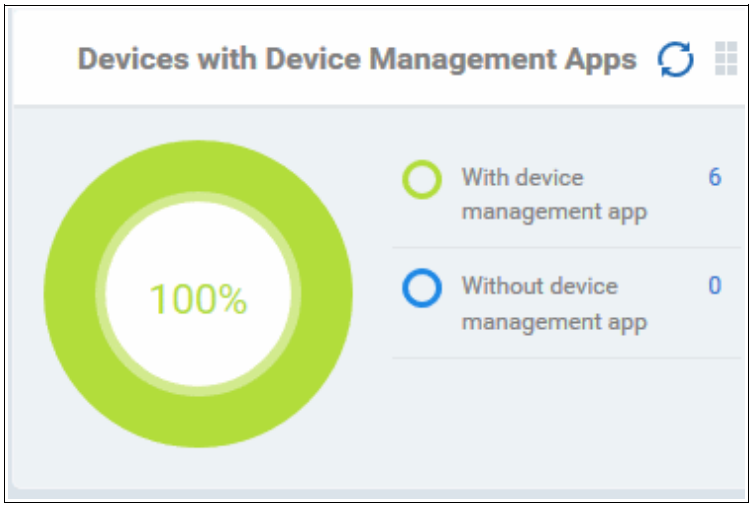


Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'Normal' in the legend will open the 'Device List' page displaying the list of devices that are normal, that is, not rooted or jail-broken. Refer to the section 'Devices' for more details.

Devices With Device Management Apps

Shows how many devices have the ITSM app. Android and Windows devices can only be enrolled with the ITSM app. iOS devices communicate with ITSM via the ITSM profile that was installed during enrollment and do not require the app. However, installing the app will provide enhanced functionality such as device location and the ability to send messages to the device from the admin panel.

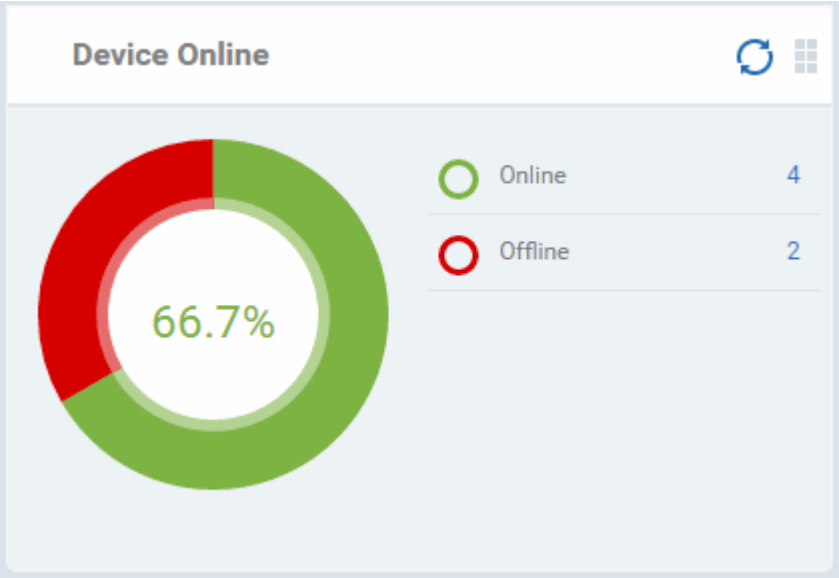
Placing the mouse cursor over a sector or the legend displays the further details.



Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'With ITSM App' will open the 'Device List' page displaying the list of devices that have the ITSM app. Refer to the section 'Devices' for more details.

Device Online

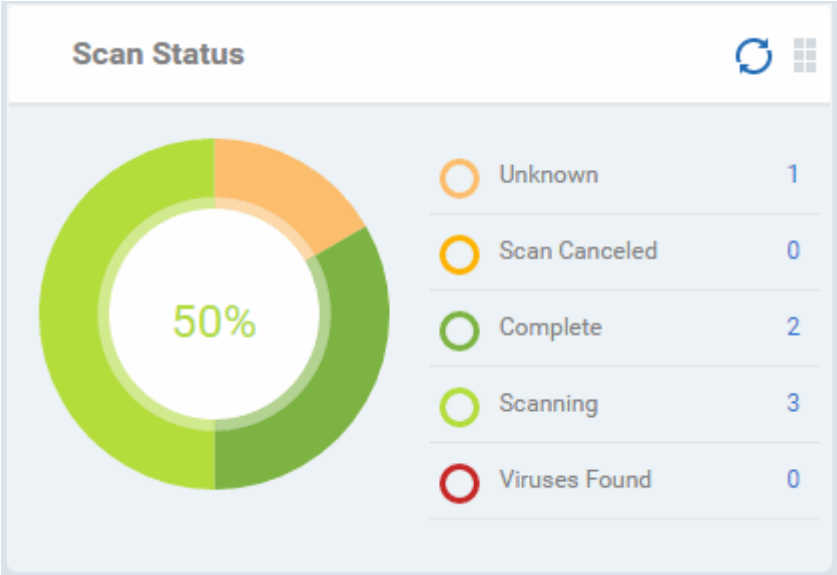
Shows enrolled devices by online/offline status. Devices will shown as offline if they are turned-off, are not communicating with ITSM for other reasons, or if Comodo Client Security is not running. Placing the mouse cursor over a sector or the legend displays the further details.



Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'Online' will open the 'Device List' page displaying the list of devices that are online. Refer to the section 'Devices' for more details.

Scan Status

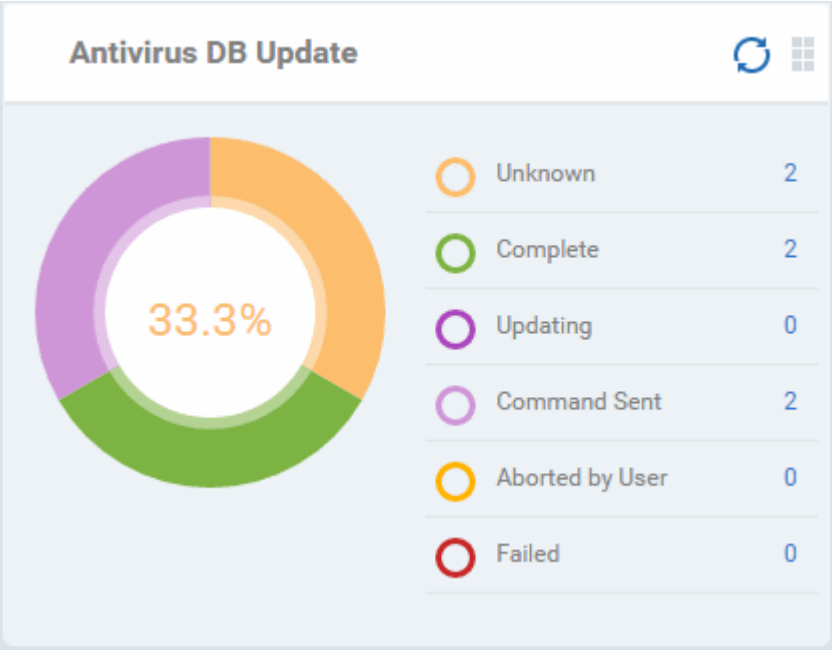
Shows the progress and results of antivirus scans on enrolled devices. Placing the mouse cursor over a sector or the legend displays the further details.



Clicking on any of the legend will open the 'Antivirus Device List' page with devices in that category. For example, clicking on 'Virus Found' in the legend will open the 'Antivirus Device List' page displaying the list of devices in which the malware were detected. Refer to the section 'Antivirus Scans' for more details.

Antivirus DB Update

Shows the progress and results of AV database updates on enrolled devices. Placing the mouse cursor over a sector or the legend displays the further details.



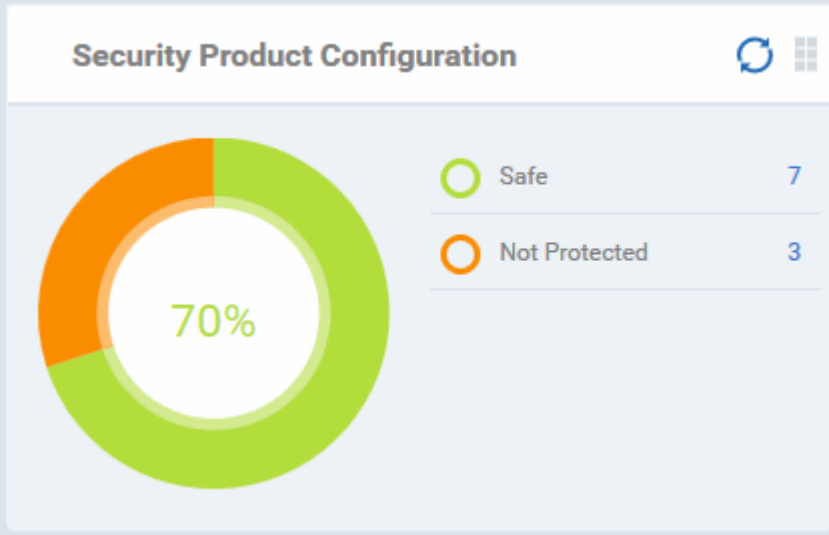
Clicking on any of the legend will open the 'Antivirus Device List' page with devices in that category. For example, clicking on 'Complete' in the legend will open the 'Antivirus Device List' page displaying the list of devices in which the AV database is completed. Refer to the section 'Antivirus Scans' for more details.

Security Product Configuration

Displays how many of your enrolled devices have 'Safe' or 'Not Protected' statuses. 'Not Protected' means:

- Comodo Client Security (CCS) is not installed on the devices
- CCS is installed but Anti-virus is not enabled in the deployed profiles on the devices

Placing the mouse cursor over a sector or on the respective legend displays the details.



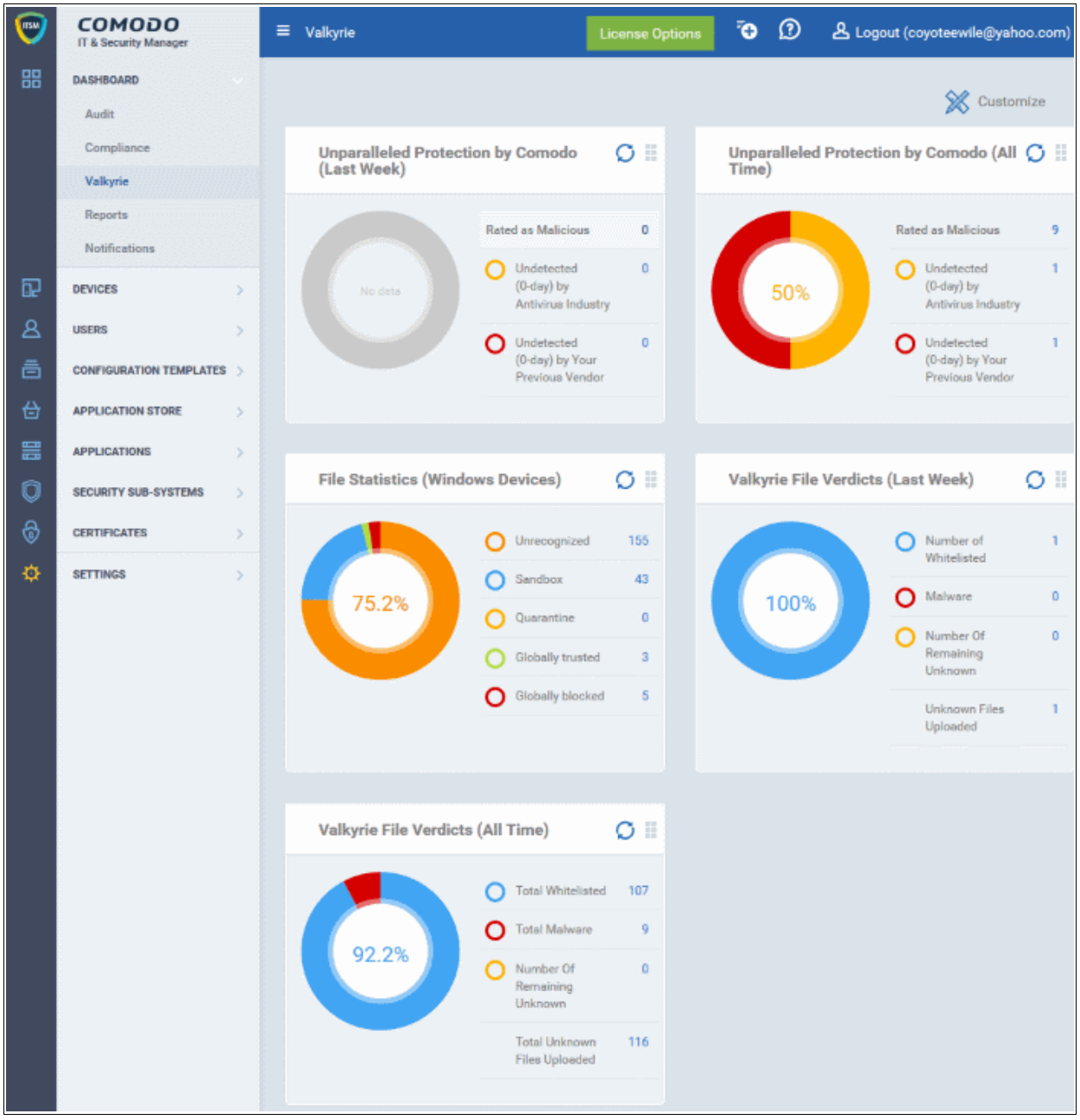
Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'Safe' will open the 'Device List' page displaying the list of devices that have Antivirus installed. Refer to the section 'Devices' for more details.

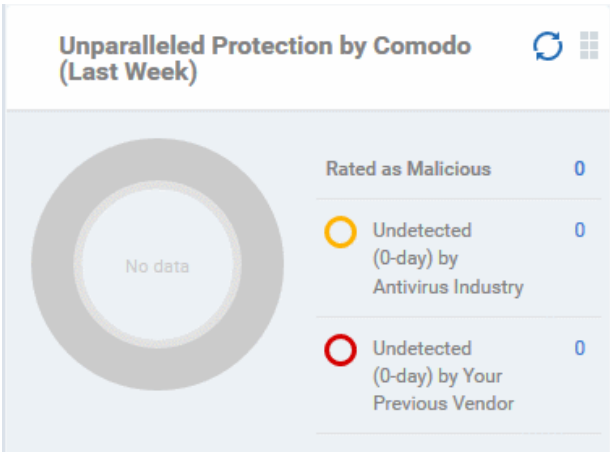
Valkyrie

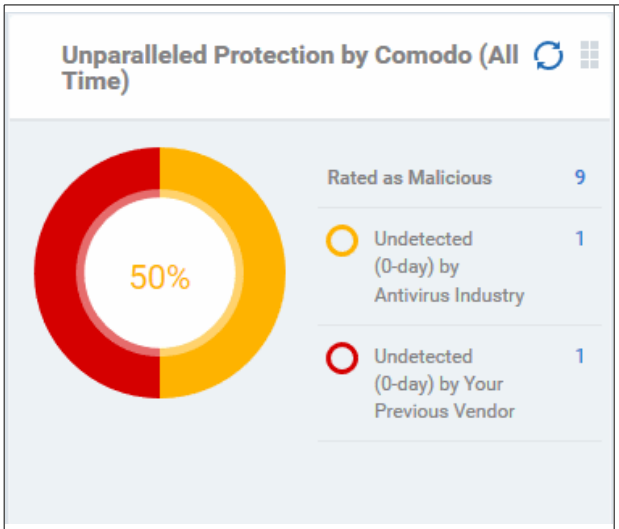
Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Administrators can take advantage of this service by applying a

configuration profile to Comodo Client Security which will automatically schedule unknown files for upload. All results will be displayed in the Valkyrie dashboard. For new ITSM customers, the license for Valkyrie comes activated. For more details on configuring Valkyrie Settings in ITSM, refer to Creating Windows Profile.

Note: The version of Valkyrie that comes with the free version of ITSM is limited to the online testing service. The Premium version of ITSM also includes manual testing of files by Comodo research labs, helping enterprises quickly create definitive whitelists of trusted files. Valkyrie is also available as a standalone service. Contact your Comodo Account manager for further details.



Unparalleled Protection by Comodo (Last Week) The 'Unparalleled protection by Comodo' pie-chart displays the number of threats identified by Valkyrie over the past week versus the user 's previous vendor and the antivirus industry as a whole. Placing the mouse cursor over a sector or on the respective legend displays the percentage of number of files in that category among the total number of files analyzed. For more details on Windows File List screen, refer to the section Viewing Applications Installed on Windows Devices.	



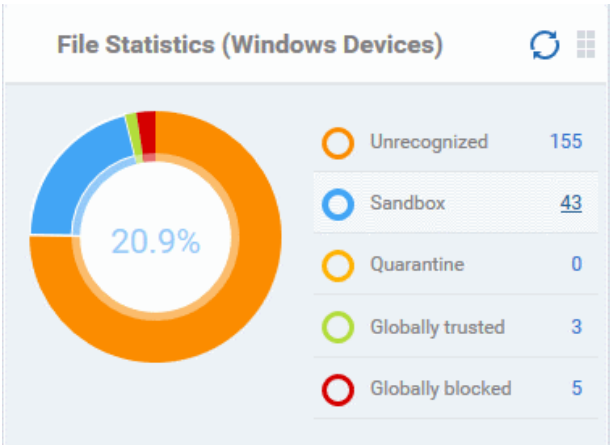
Unparalleled Protection By Comodo (All Time)

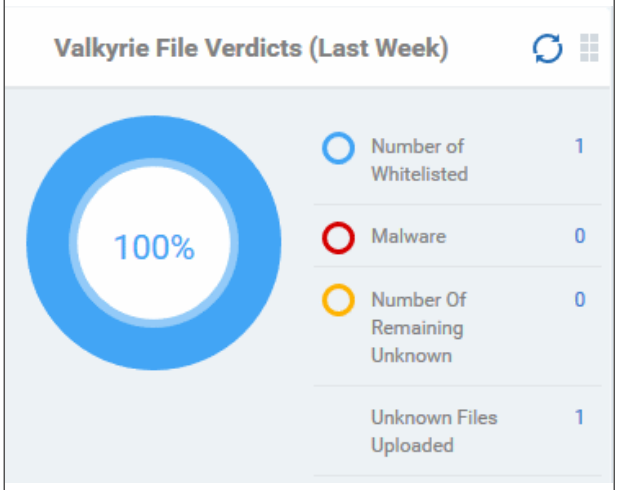
The 'Unparalleled protection by Comodo' pie-chart displays the number of threats identified by Valkyrie since installation versus the user 's previous vendor and the antivirus industry as a whole. Placing the mouse cursor over a sector or on the respective legend displays the percentage of number of files in that category among the total number of files analyzed. For more details on Windows File List screen, refer to the section Viewing Applications Installed on Windows Devices.

File Statistics (Windows Devices)

The 'File Statistics (Windows Devices)' pie-chart displays the number of files identified with different ratings as per local file rating analysis and Valkyrie analysis. Placing the mouse cursor over a sector or on the respective legend displays the percentage of number of files in that category among the total number of files analyzed. For more details on Windows File List screen, refer to the section Viewing Applications Installed on Windows Devices.

Clicking on any item in the legend will open the respective 'File List' page. For example, clicking on 'Unrecognized' will open the 'Application Control' > 'Unrecognized' page displaying the list of unrecognized files detected from enrolled devices. Refer to the section 'Viewing Applications Installed on Windows Devices' for more details.



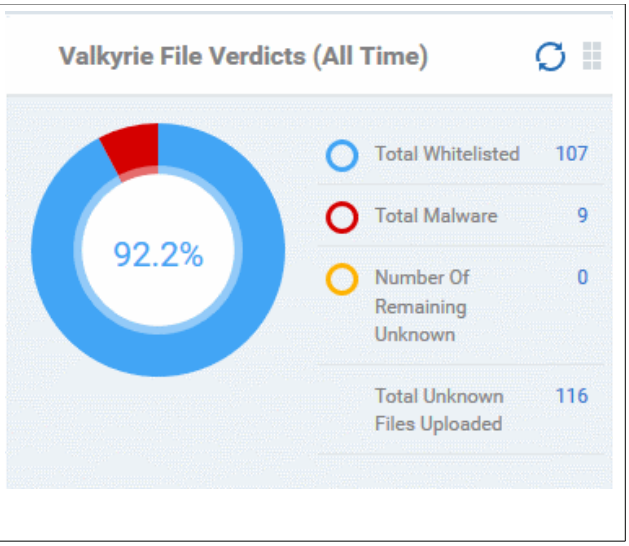


Valkyrie File Verdicts (Last Week)

The 'Valkyrie File Verdicts (Last Week)' pie-chart displays the number of files identified as malicious, or determined as 'Unknown' or that are whitelisted, total number of unknown files in the Valkyrie database as per last week. Placing the mouse cursor over a sector or on the respective legend displays the percentage of number of files in that category among the total number of files analyzed. For more details on Windows File List screen, refer to the section Viewing Applications Installed on Windows Devices.

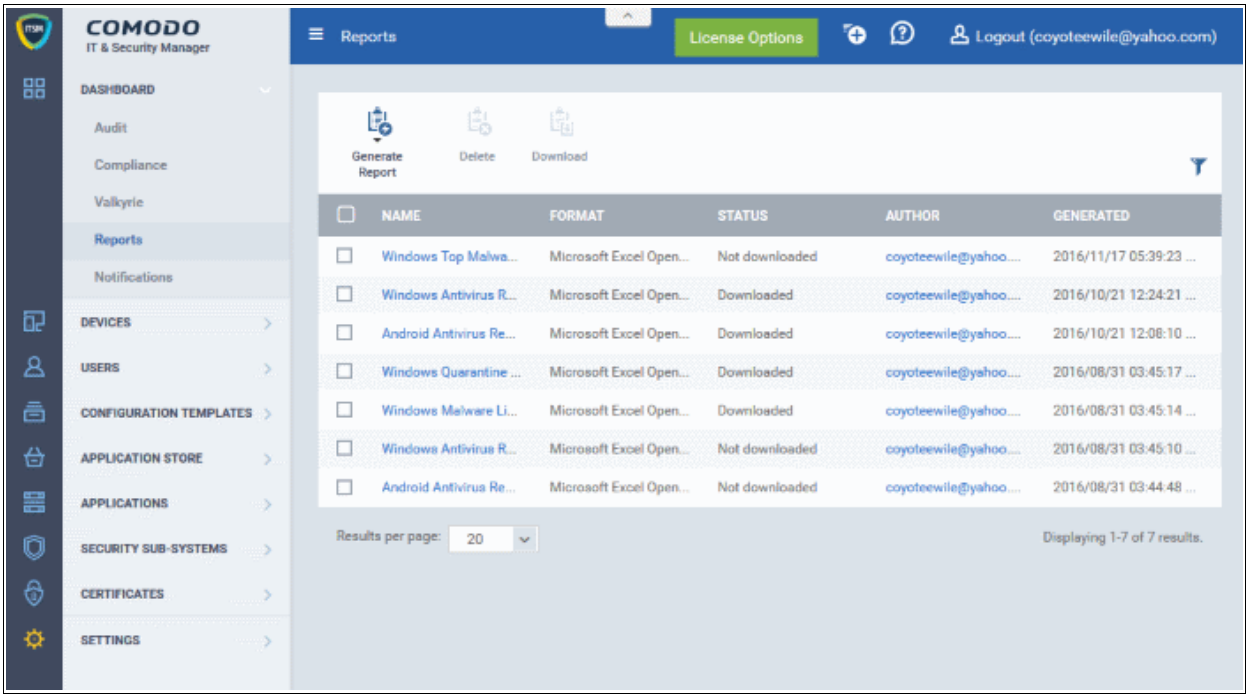
Valkyrie File Verdicts (All Time)

The 'Valkyrie File Verdicts All Time)' pie-chart displays the number of files identified as malicious, or determined as 'Unknown' or that are whitelisted, total number of unknown files in the Valkyrie database as per entire period. Placing the mouse cursor over a sector or on the respective legend displays the percentage of number of files in that category among the total number of files analyzed. For more details on Windows File List screen, refer to the section Viewing Applications Installed on Windows Devices.



Reports

ITSM is capable of generating a wide variety of reports covering system and malware activity across you entire fleet of devices. The generated reports are in spreadsheet (.xls) format. The Reports interface under the Dashboard allows you to generate new reports and to view and download them.

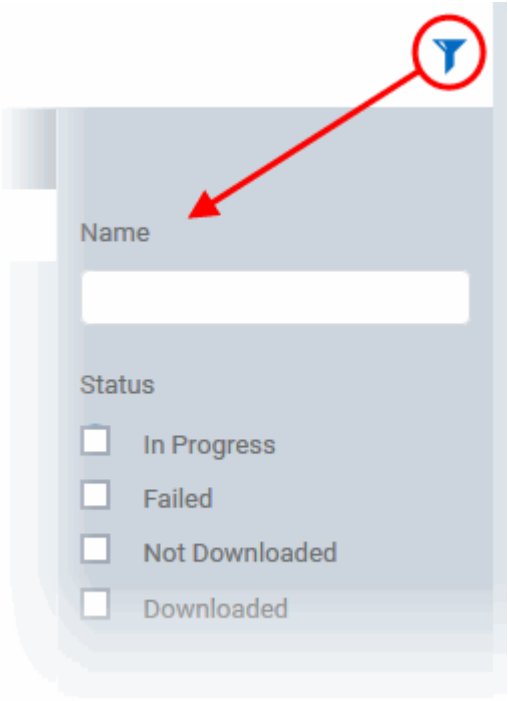


The types of reports available are:

- Android Antivirus
- Windows Antivirus
- Windows Malware List
- Windows Top Malware
- Windows Quarantine
- Hardware Inventory

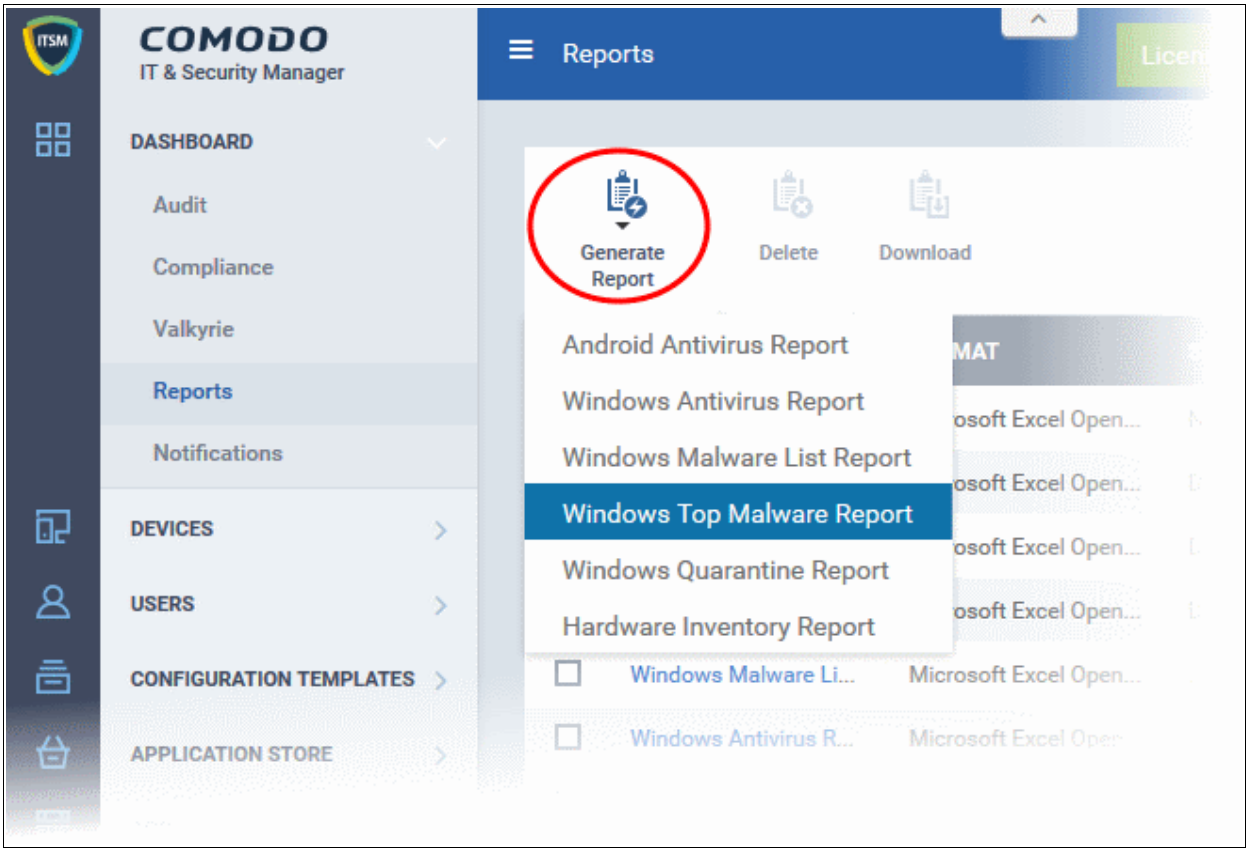
Search and filtering option

- To filter or search for a specific report, click the funnel icon at the top right, enter the name of the report in part or full and/or choose the status of the report.

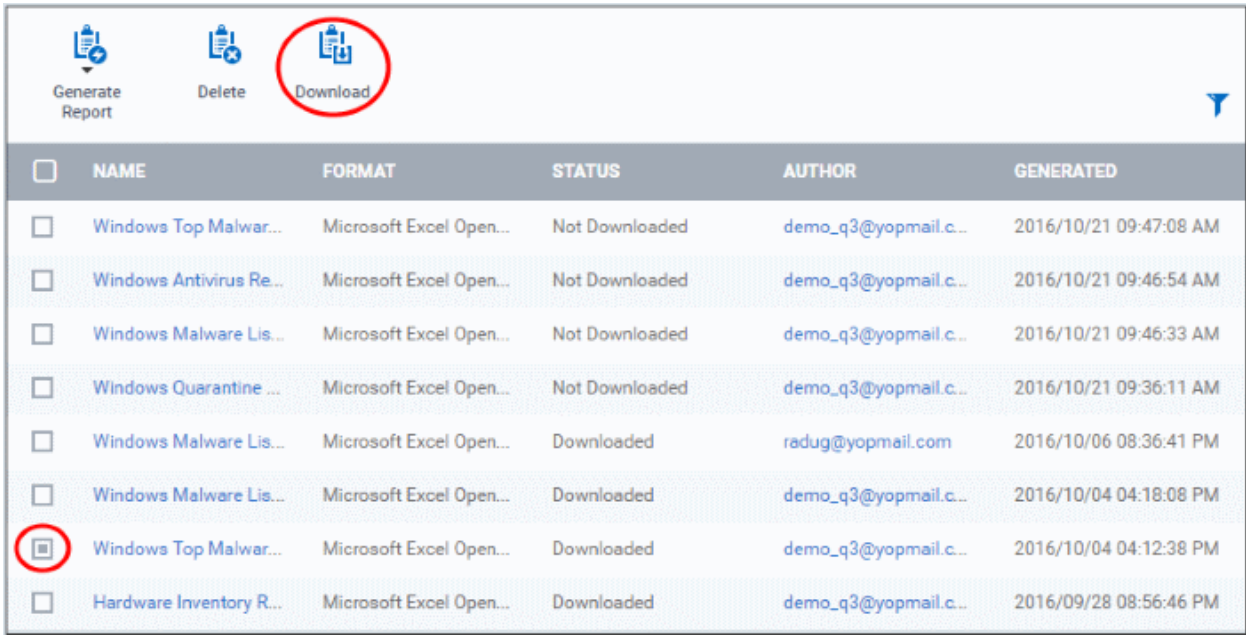


To generate a report

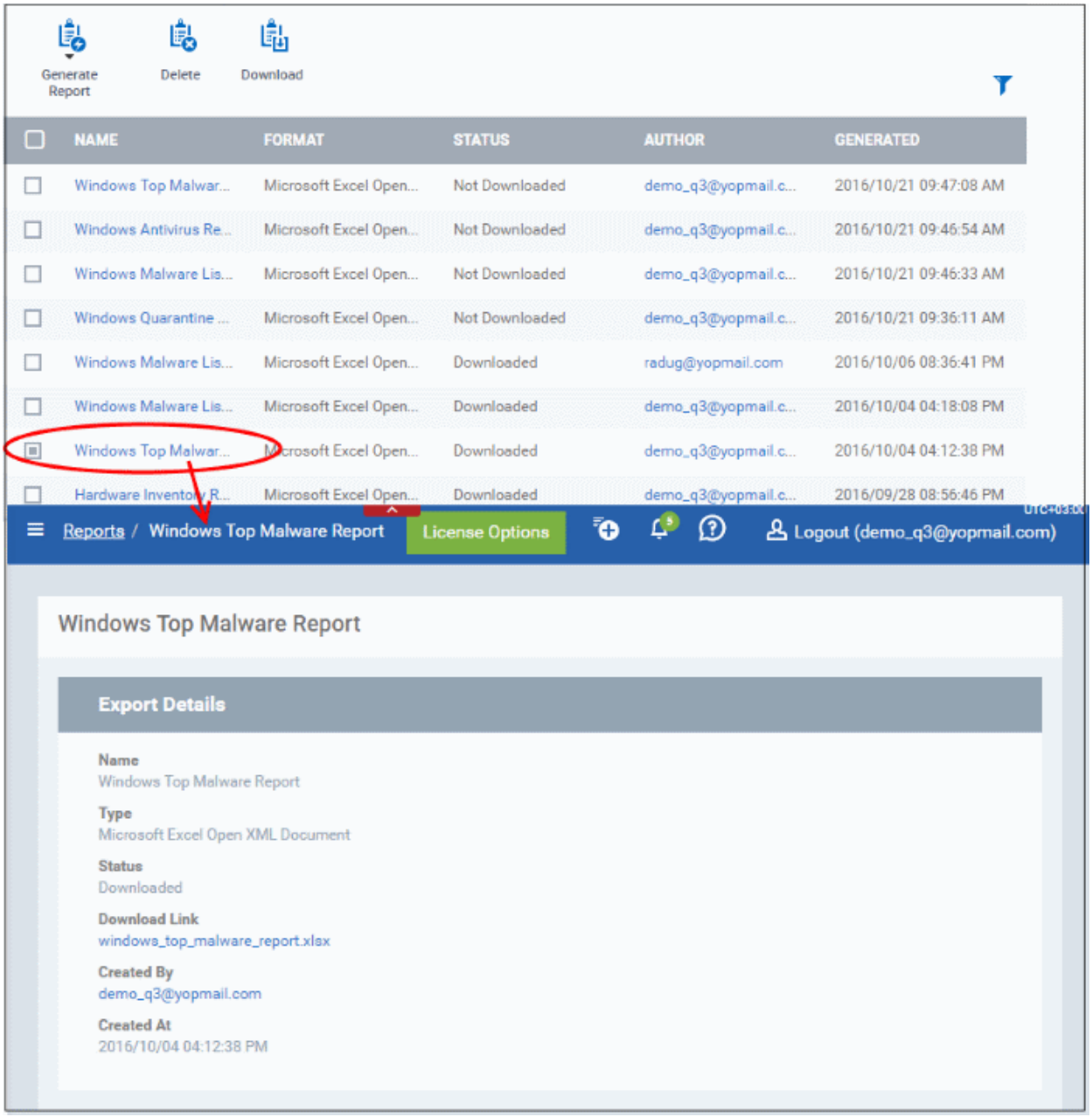
- Click 'Generate Report' from the top and then click on the report type from the drop-down.



A new report will be generated for the selected report type.



- To download the report, select it and click 'Download' from the top. The report will be available as an Excel file (in .xls format).
- To view the details of the report click on the report name.



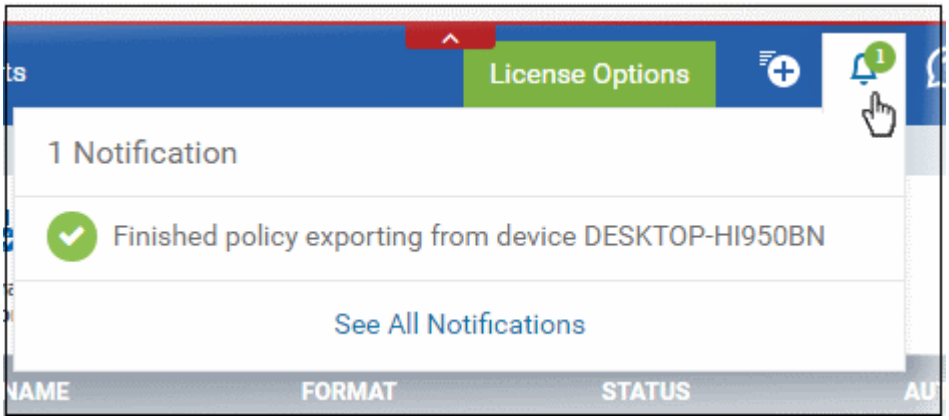
- To remove a report from the list,select it and click 'Delete'.

Notifications

The 'Notifications' dashboard allows administrators to view the notifications from ITSM. ITSM generates notifications on various events like:

- Installation of Comodo Client on a device
- Identification of malware on Android devices from real-time, scheduled scans and on-demand scans
- Identification of threats and items moved to quarantine by the Comodo Client on Windows endpoints.
- Monitoring and procedure alerts

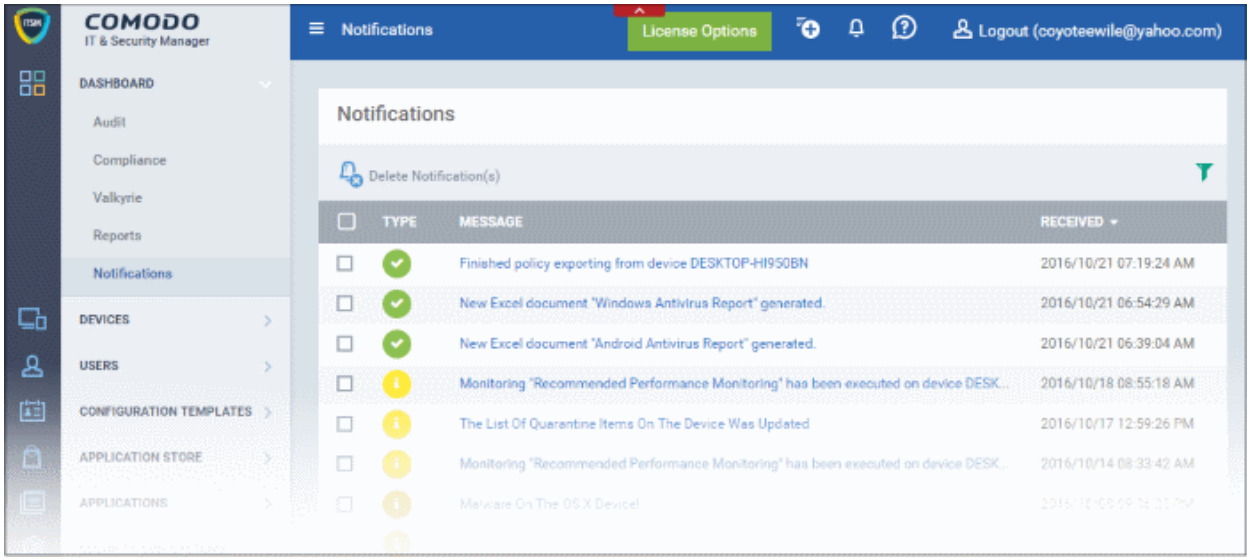
New notifications are alerted to the user by the Notification icon  in the title bar. Clicking the icon displays the list of new notification messages as a drop-down.



- Clicking on the notification will take you to the respective details interface. For example, clicking on 'Finished policy exporting from device....' message will open the respective device details screen with 'Exported Configurations' tab pre-selected.

Tip: ITSM is capable of sending notifications as emails. You can instruct ITSM to send automated email notifications to selected administrators by configuring 'Email Notifications' under Settings. Refer to the section **Configuring Email Notifications**.

- To view all notifications, click 'See All Notifications' from the notification drop-down or click 'Notifications' on the left menu under Dashboard.

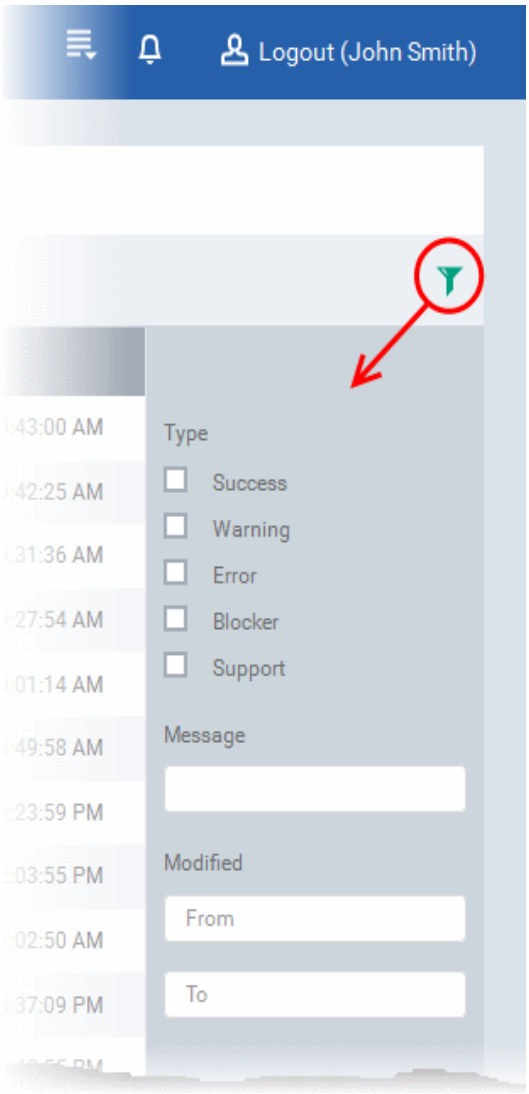


List of All Notifications - Column Descriptions	
Column Heading	**Description**
Type	Indicates whether the notification is generated for a successful operation, Warning, Error, Blocker or support event.
Message	The message content of the notification, shortly describing the event.
Received	The date and time at which the notification was received.

- The message also acts as a shortcut to view the details of the notification. Clicking on a message will open

the interface relevant to the message for more details. For example, clicking on 'Malware Found on Windows device' message will open the 'Antivirus Current Malware List' screen with the list of malware identified.

- To sort the filter in ascending/descending order of the date/time at which they were generated, click on the Modified column header.
- To filter or search for specific notification, click the funnel icon at the top right choose the notification type, enter the message to be searched in part or full and/or specify the date range within which the notification was generated.



- To remove notification(s) select it/them and click 'Delete Notifications' above the table.

4. Users and User Groups

One of the first steps in setting up Comodo IT and Security Manager is to add users. Once users have been added, you can enroll iOS, Android, Windows or Mac OS devices associated with each user. After enrolling a device, you will be able remotely manage and apply security policies to it. You may also create user groups in order to apply policies to multiple devices. You can also assign users to an ITSM administrator role.

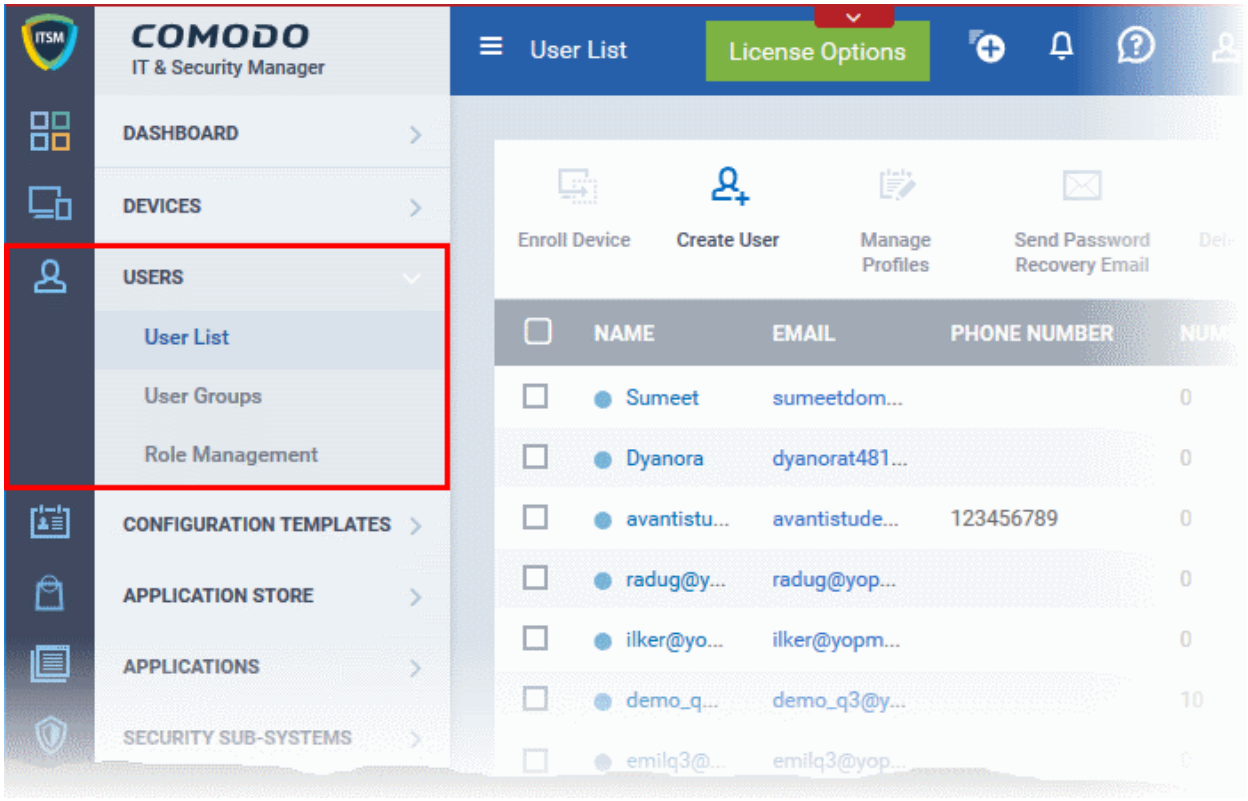
Users can access the ITSM interface according to the privileges assigned to them. Privilege levels are assigned by applying a 'role' to a user.

Users can be added to ITSM in two ways:

- From the the C1 interface
- From the ITSM interface

A staff member or user added via C1 interface can access C1 and other licensed modules, including ITSM. A user added via ITSM can only access ITSM. Please refer to the page at https://help.comodo.com/topic-289-1-716-8482-Managing-Administrators-and-Roles.html for details on how to add users via C1. The following sections describe how to add users via the ITSM interface.

The 'Users' menu at the left allows you to add, view and manage users/user groups and to manage roles:



The following sections explain more about each area:

- Managing Users
  - Creating New User Accounts
  - Enrolling Users' Devices for Management
  - Viewing the Details of a User
  - Assigning Configuration Profile(s) to a Users' Devices
  - Removing a User
- Managing User Groups
  - Creating a New User Group
  - Editing a User Group
  - Assigning Configuration Profile to a User Group
  - Removing a User Group
- Configuring Role Based Access Control for Users
  - Creating a New Role
  - Managing Permissions and Assigned Users of a Role
  - Removing a Role
  - Managing Roles Assigned to a User

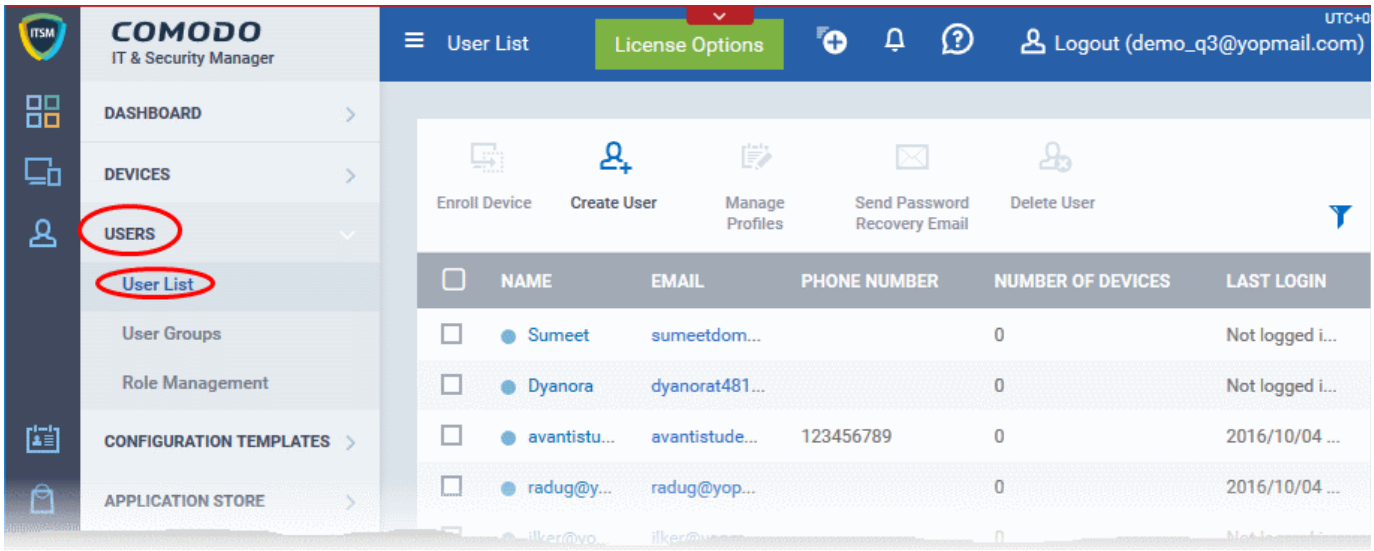
4.1. Managing Users

Administrators can enroll user accounts to ITSM and assign them roles with differing privilege levels (as 'administrators' or 'end users'). Devices belonging to a user can only be enrolled after adding their user account to ITSM.

C1 customers. Staff added via the C1 interface will also be added as users in ITSM with their assigned roles. For details about adding users via C1 and assigning roles, refer to https://help.comodo.com/topic-289-1-716-8482-Managing-Administrators-and-Roles.html

The 'Users List' interface displays a list of user accounts that are enrolled to ITSM and allows the administrator to add/manage users, enroll new devices belonging to users, manage configuration profiles applied to devices and so on.

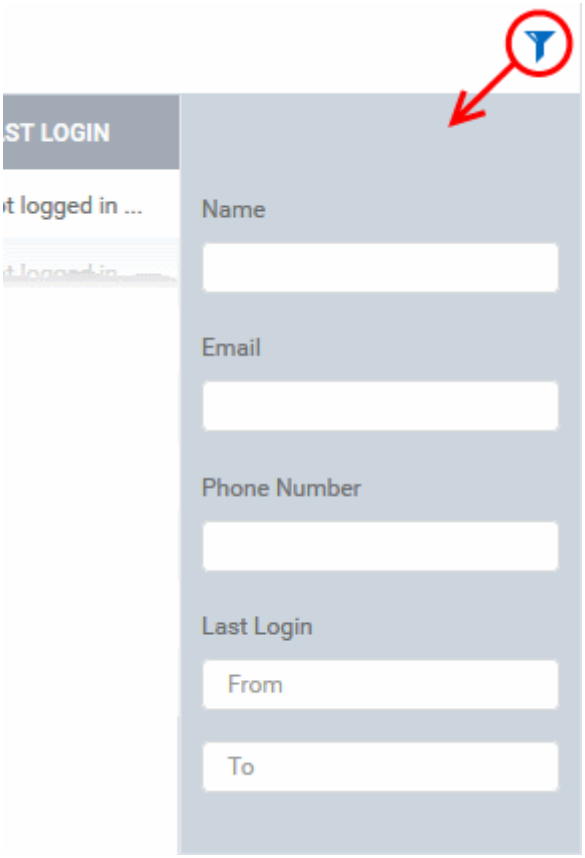
- To open the 'User List' interface, click the 'Users' tab on the left and select 'User List'



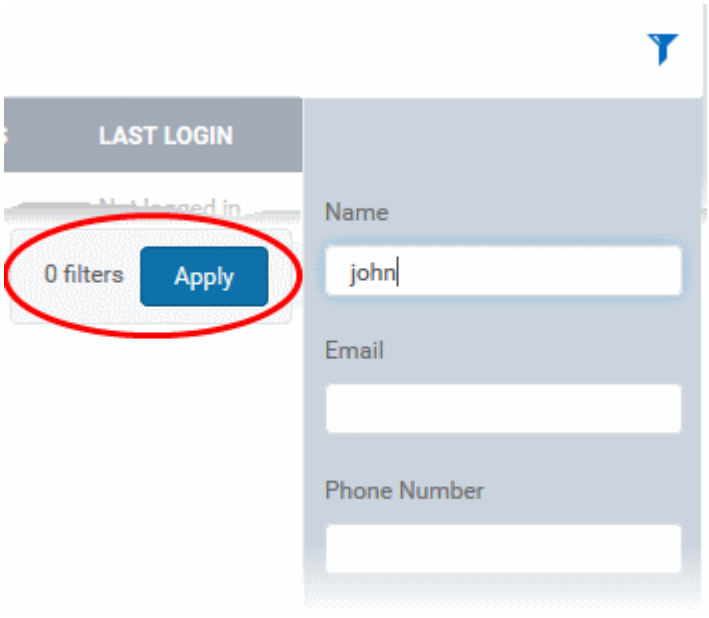
User List Table - Column Descriptions	
Column Heading	**Description**
Name	The login username of the user. Clicking the username will open the user details screen where you can edit user details. See 'Viewing the Details of a User' for more details.
Email	The registered email address of the user. Account and device enrollment mails will be sent to this email address. Clicking the email address allows you to send an email to the user through your default email client.
Phone Number	The registered phone number of the user.
Number of Devices	The total number of devices enrolled for the user.
Last Login	The precise date and time of the user's last login.

Sorting, Search and Filter Options

- Clicking on the column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific user based on username, email address and/or phone number, enter the search criteria in part or full and click 'Apply'



- To filter the users that have logged-in within a specific time period or whose token expire within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields using the calendars that appear on clicking inside the respective field and click 'Apply'.

You can use any combination of filters at-a-time to search for specific users.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Refer to the following sections for more details about:

- Creating New User Accounts
- Enrolling Users' Devices for Management
- Enrolling Android Devices
- Enrolling iOS Devices
- Enrolling Windows Endpoints
- Enrolling Mac OS Endpoints
- Viewing the Details of a User
- Updating the Details of a User and Resetting Password
- Assigning Configuration Profile(s) to a Users' Devices
- Removing a User

4.1.1. Creating New User Accounts

The 'User List' interface allows administrators to create new administrator and end-user accounts. After a user is created they will receive an enrollment mail which requests them to activate their account and set their account password.

C1 customers. Staff added via the C1 interface will also be added as users in ITSM with their assigned roles. For details about adding users via C1 and assigning roles, refer to https://help.comodo.com/topic-289-1-716-8482-Managing-Administrators-and-Roles.html

ITSM also allows administrators to bulk enroll users from and enroll Windows endpoints via Active Directory (AD) group policy. Please refer to the sections 'Enroll Windows Devices by Installing the ITSM Agent Package' and 'Importing User Groups from LDAP' for more details. This section explains how to enroll users from the 'User List' interface.

Important Note: User device(s) can only be enrolled after the user has been added to the system.

Each user license covers up to five mobile devices or one Windows/Mac OS endpoint for a single user (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows/Mac OS 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.

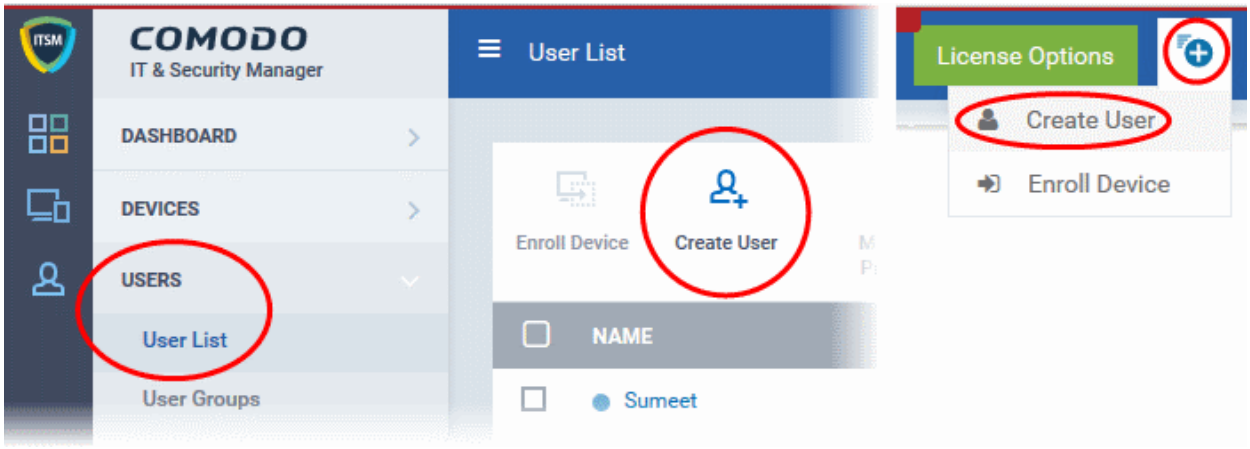
Refer to the section Viewing and Managing Licenses for more details.

To add a new user

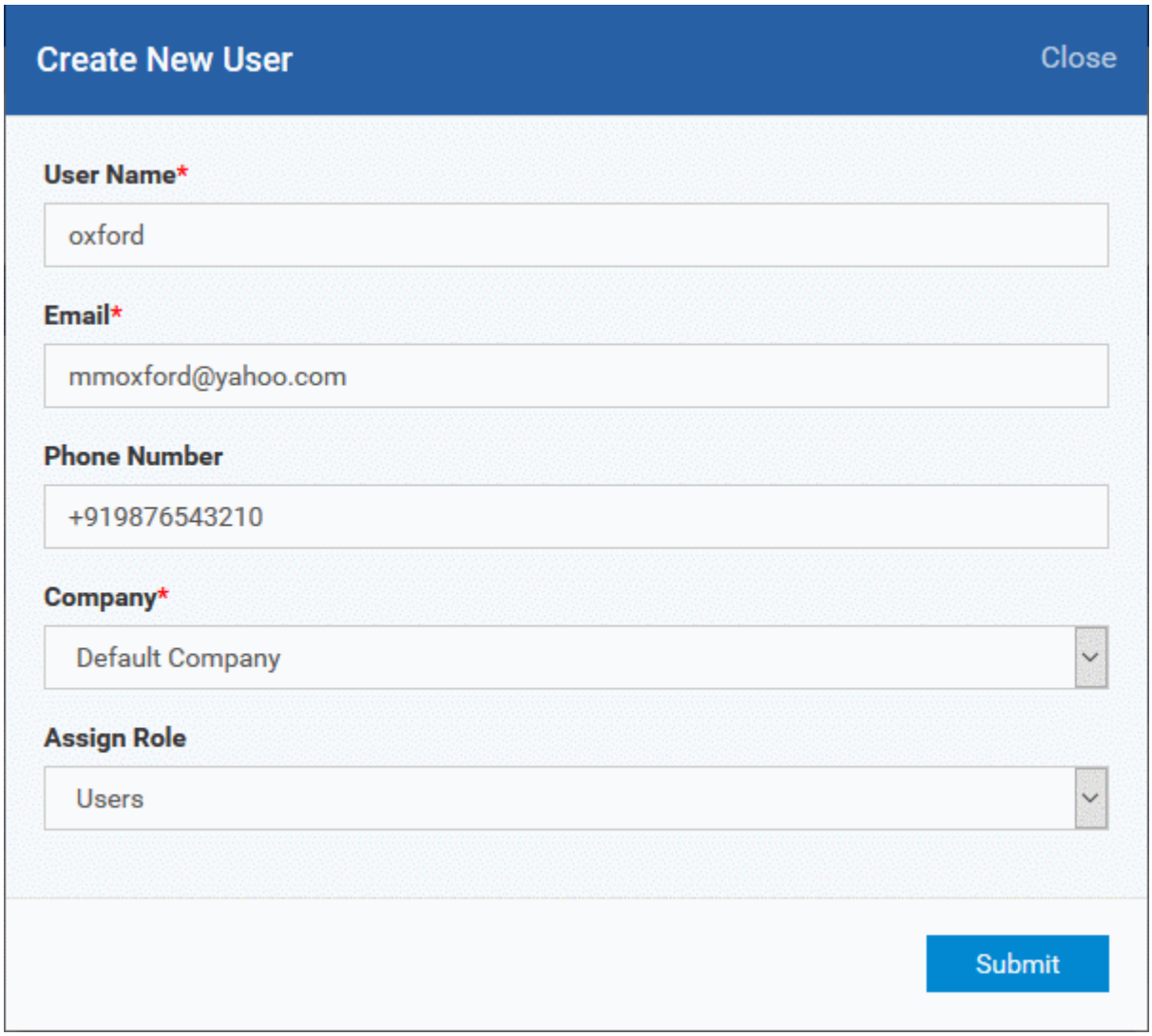
- Click 'Users' > 'User List' from the left then click the 'Create User' button

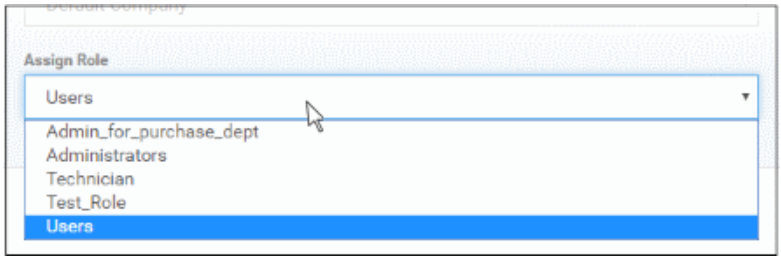
  or

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



The 'Create New User' form will open:

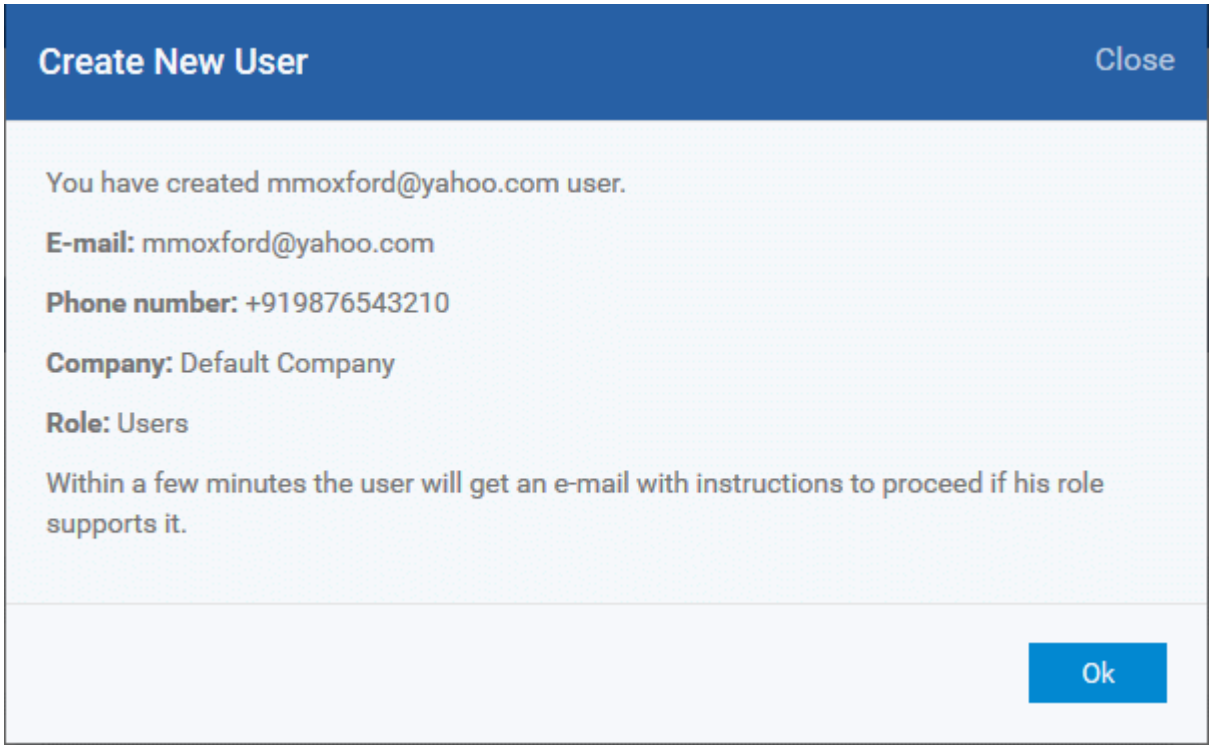


'Create new user' Form - Table of Parameters		
Form Element	**Type**	**Description**
Username	Text Field	Enter the login username for the user.
Email	Text Field	The registered email address of the user. Account and device enrollment mails will be sent to this address. Please ensure users respond to the device enrollment mail from the device(s) you intend to enroll.
Phone Number (Optional)	Text Field	Enter the phone number of the user.
Company	Drop-down	Choose the company to which the user belongs. • Comodo One MSP customers can add users from Companies/Organizations enrolled in their Comodo One account. • Comodo One Enterprise and ITSM stand-alone customers can only add users to the default company.
Assign role	Drop-down	Select the role to be assigned to the new user from the 'Assign role' drop-down.  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 custom roles with access to selected areas of the administrative console and can assign them to users as required. All roles created in ITSM and C1 will appear in the 'Assign Role' drop-down when adding a new user. Refer to the section Configuring Role Based Access Control for Users for more details.

- Enter the details, select the role for the new user and click the 'Submit' button.

Tip: User roles can be changed at any time from the 'Role Management' interface ('Users' > 'Role Management'). See Managing Permissions and Assigned Users of a Role for more details.

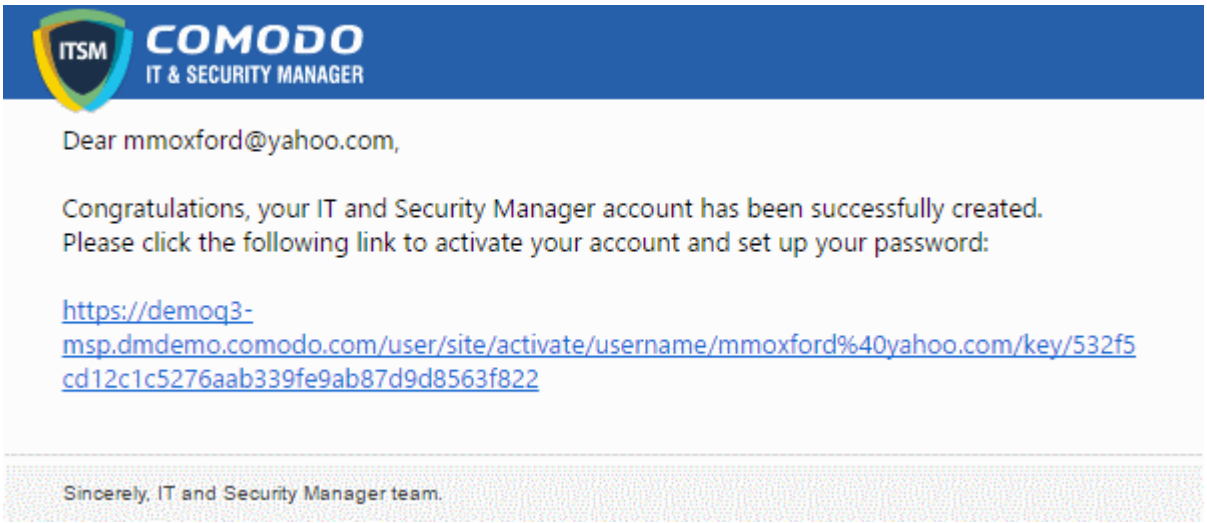
A confirmation will be displayed,



- Repeat the process to add more users.

Successfully added users will be listed in the 'Users' interface. The user's devices can now be enrolled to ITSM.

ITSM will send account activation mails to the newly added administrators. They can activate their account and set their login password by clicking the link in the email. An example mail is shown below:



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

Note: By default, enrolled users with the role 'Users' do not receive an account activation mail nor gain console login rights. Only personnel with the default roles 'Administrator', 'Technician', or a custom role with access to the administrative console, will receive an activation email.

Should you wish, you can change role permissions to allow the default 'User' role to have access to the admin console. See Configuring Role Based Access Control for Users for more details.

4.1.2. Enrolling User Devices for Management

In order to centrally manage mobile/laptop/desktop devices, each device needs to be enrolled to Comodo IT and Security Manager (ITSM). To do this, you first create or select the user(s) whose devices are to be enrolled. They will then receive a device enrollment mail which they should answer from the device itself.

ITSM generates enrollment token for each user and sends them a mail containing enrollment instructions and the token. Multiple devices can be enrolled with the same token by the user simply responding to the mail from each of their devices. The validity of the token is 72 hours and a new token should be generated for adding more devices after this period expires.

Administrators can bulk enroll users and Windows endpoints by downloading the client software from ITSM and creating a software installation group policy for their Active Directory (AD) server. Please refer to the sections '**Enroll Windows Devices by Installing the ITSM Agent Package**' and '**Importing User Groups from LDAP**" for more details. This section explains how to enroll users' devices from the 'User List' interface.

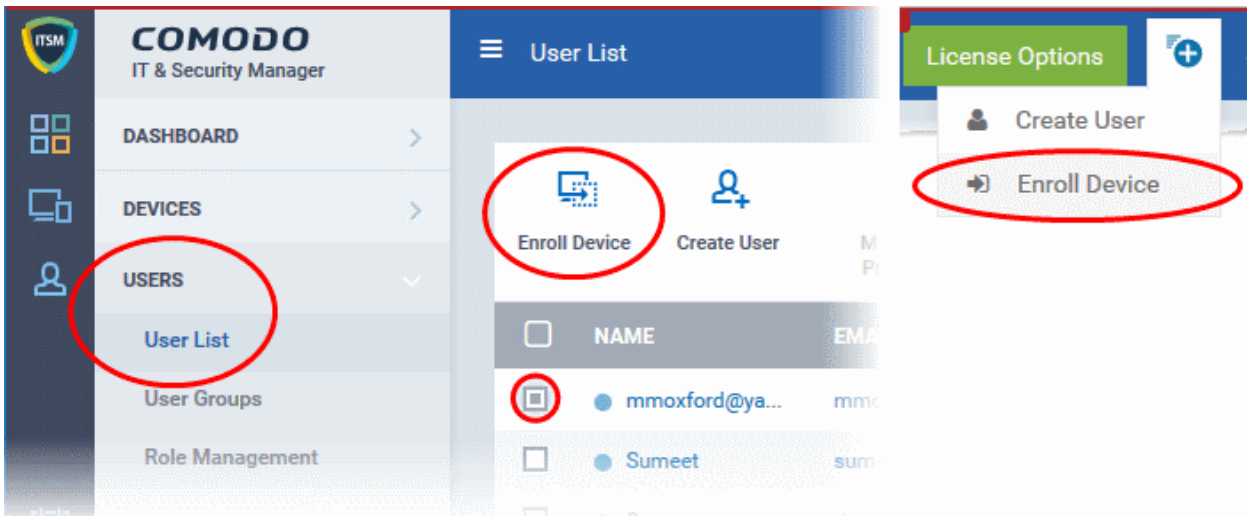
> **Important Note**: Each user license covers up to five mobile devices or one Windows/Mac OS endpoint for a single user (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows/Mac OS endpoint). If more than 5 devices or 1 endpoint are added for the same user, then an additional user license will be consumed. Administrators can purchase additional licenses from the Comodo website if required.
>
> Refer to the section **Viewing and Managing Licenses** for more details.

To enroll devices

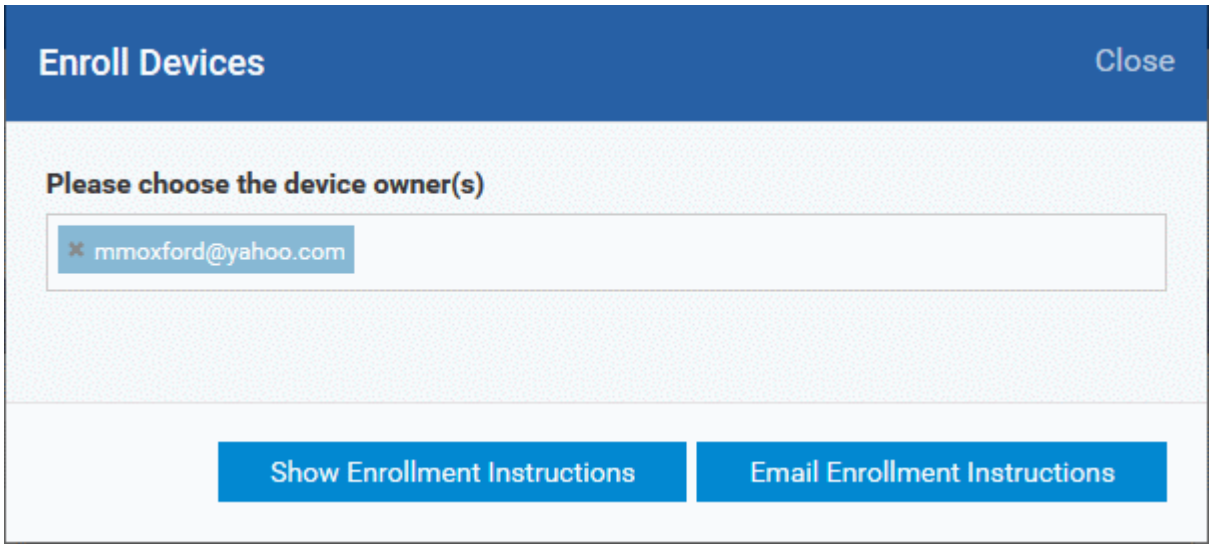
- Click 'Users' > 'User List' from the left
- Select users for whom you want to enroll devices and click the 'Enroll Device' button above the table

  Or

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



The 'Enroll Devices' dialog will then open for the chosen users:



Tip: Alternatively, you can open the 'Enroll Devices' dialog by:

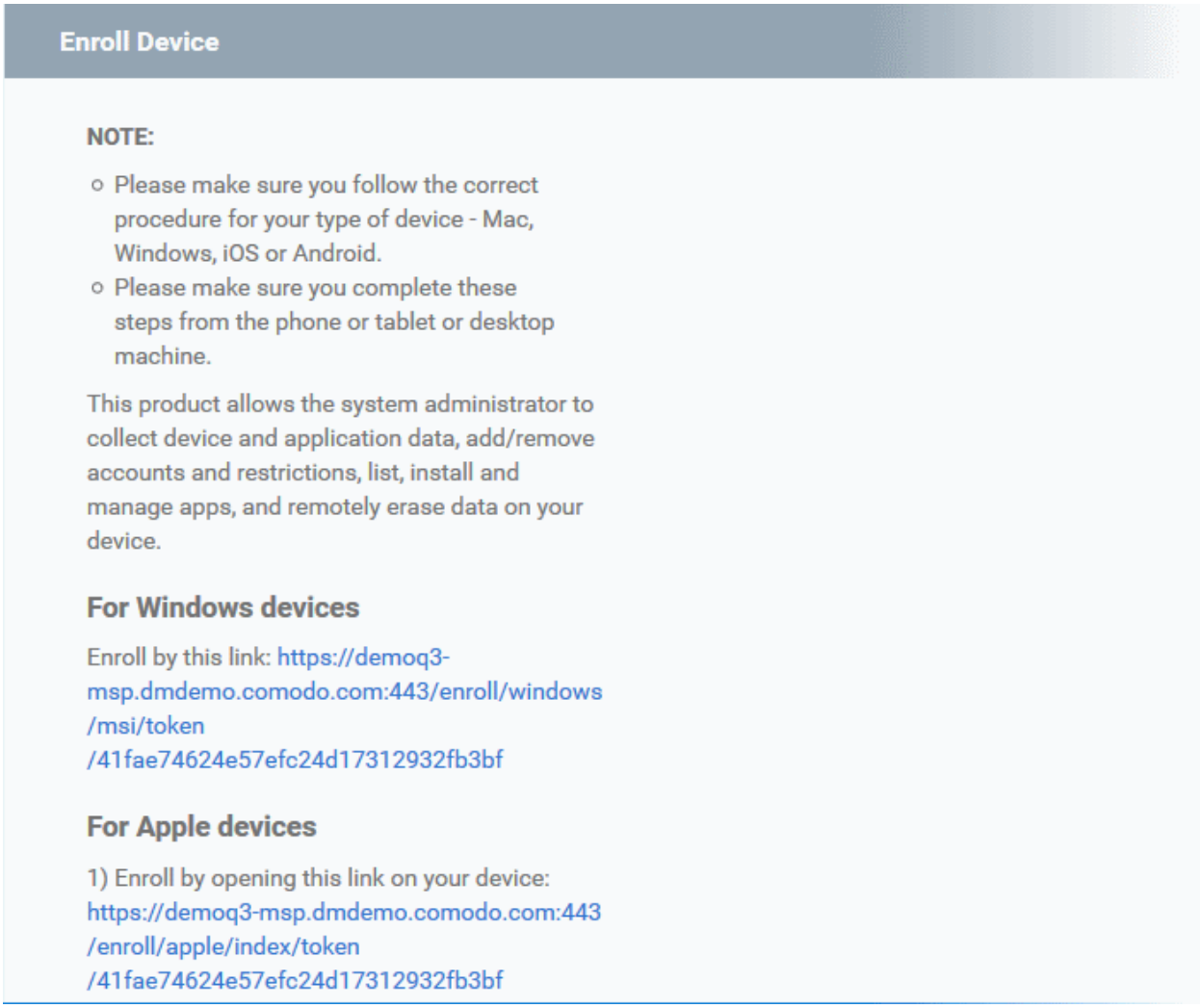
- Opening the 'User Info' screen of a user by clicking on the username and selecting 'Enroll Device' at the top
- Opening the 'Device List' interface by clicking 'Devices' > 'Device List' from the left and selecting 'Enroll Device'

The 'Choose Users' field is pre-populated with the users you selected in the 'User List' interface.

- To add more users, type the first the few letters of a user-name then choose users from the search results.

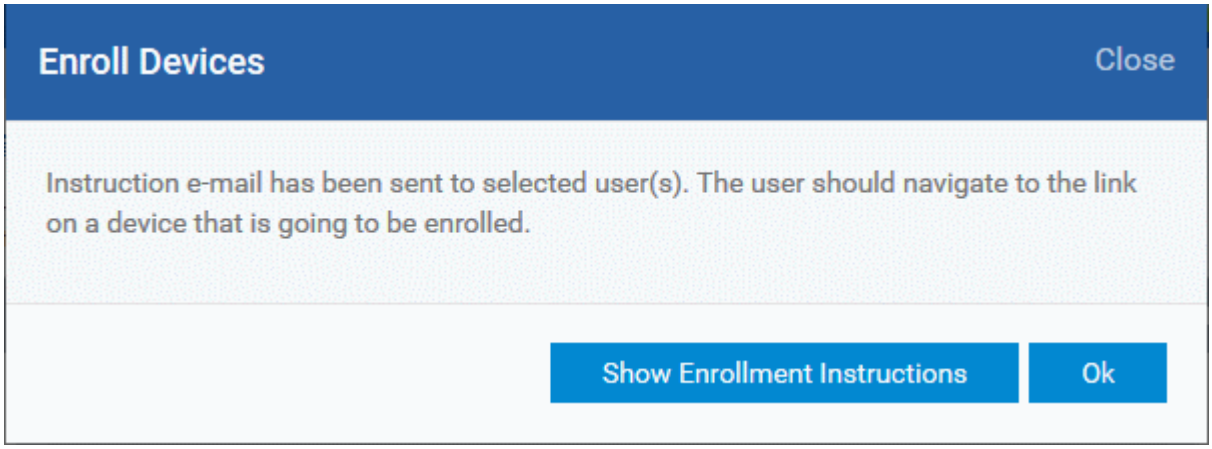
Once the user is enrolled, the enrollment instructions with links to download the ITSM agent for Android, iOS/Mac OS and Windows devices and to activate the agent(s) will be provided to the user.

- If you want the enrollment instructions to be displayed in the ITSM interface, click 'Show Enrollment Instructions'. This is useful for administrators attempting to enroll their own devices. The page also contains instructions for enrolling devices of users imported to ITSM through Active Directory (AD) integration.

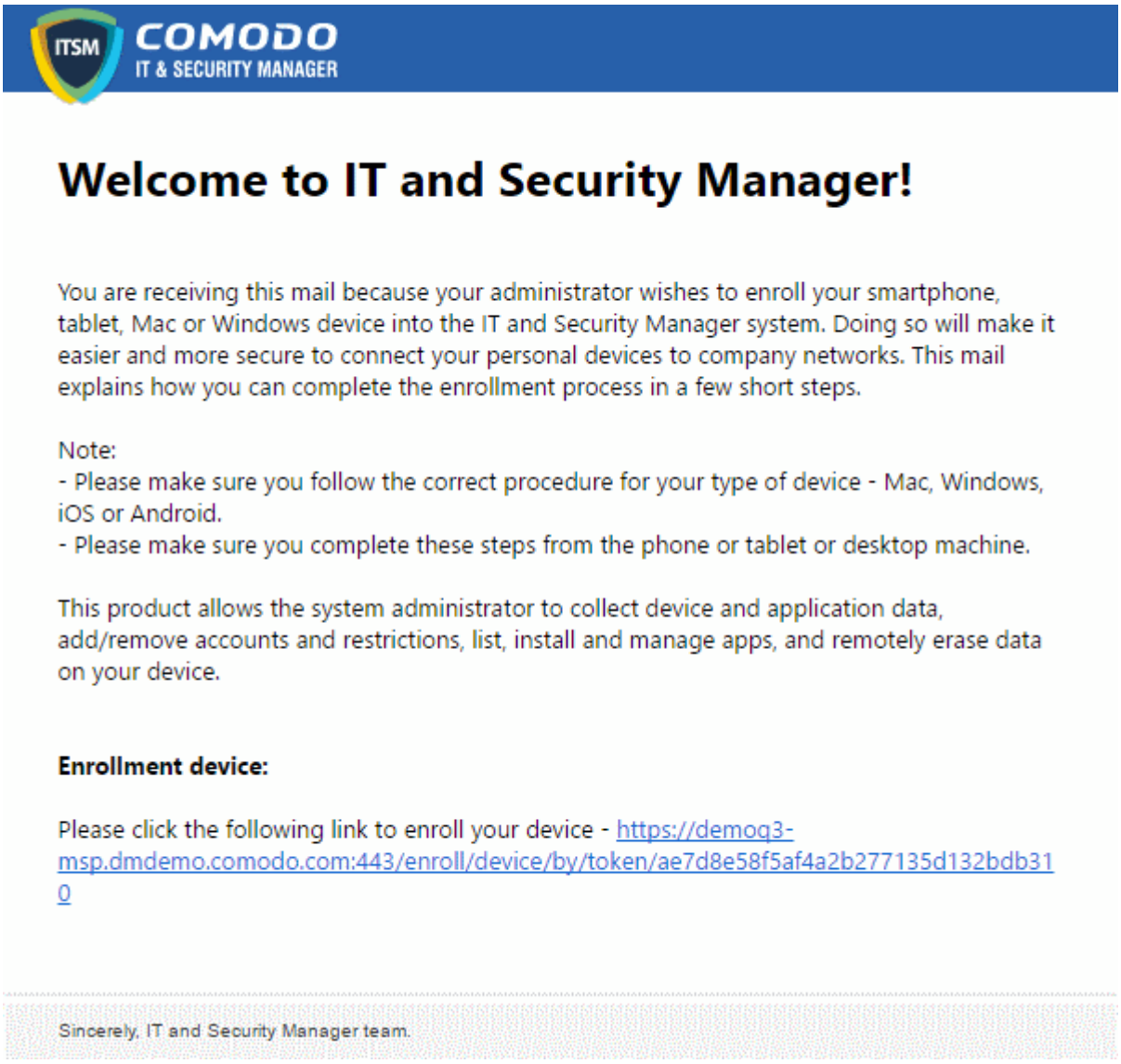


- If you want the enrollment instructions to be sent as an email to the users, click 'Email Enrollment Instructions'.

A confirmation dialog will be displayed.



A device enrollment email will be sent to each user. The email will contain a link to a page containing instructions and links to download the ITSM agent/profile for the 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.

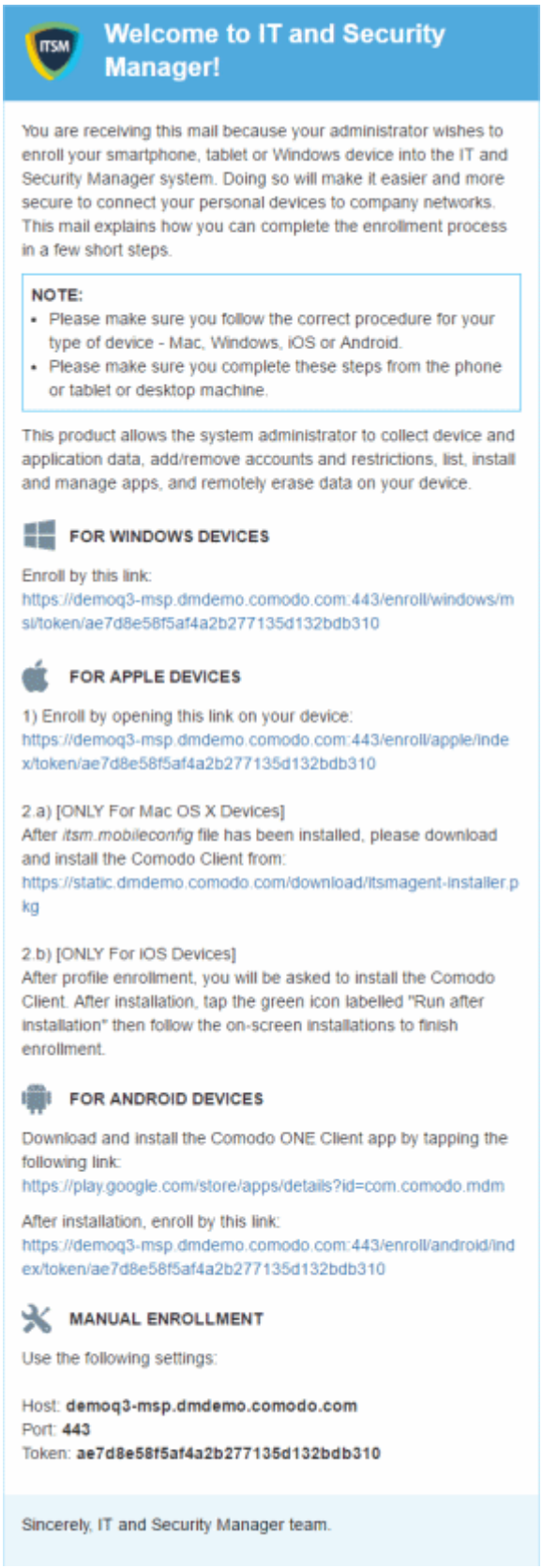
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

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 WINDOWS DEVICES

Enroll by this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/ae7d8e58f5af4a2b277135d132bdb310

FOR APPLE DEVICES

1) Enroll by opening this link on your device:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/apple/index/token/ae7d8e58f5af4a2b277135d132bdb310

2.a) [ONLY For Mac OS X Devices]
After *itsm.mobileconfig* file has been installed, please download and install the Comodo Client from:
https://static.dmdemo.comodo.com/download/itsmagent-installer.pkg

2.b) [ONLY For iOS Devices]
After profile enrollment, you will be asked to install the Comodo Client. After installation, tap the green icon labelled "Run after installation" then follow the on-screen installations to finish enrollment.

FOR ANDROID DEVICES

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

After installation, enroll by this link:
https://demoq3-msp.dmdemo.comodo.com:443/enroll/android/index/token/ae7d8e58f5af4a2b277135d132bdb310

MANUAL ENROLLMENT

Use the following settings:

Host: **demoq3-msp.dmdemo.comodo.com**
Port: **443**
Token: **ae7d8e58f5af4a2b277135d132bdb310**

Sincerely, IT and Security Manager team.

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**.

The following sections explain more on:

- Enrolling Android Devices
- Enrolling iOS Devices
- Enrolling Windows Endpoints
- Enrolling Mac OS Endpoints

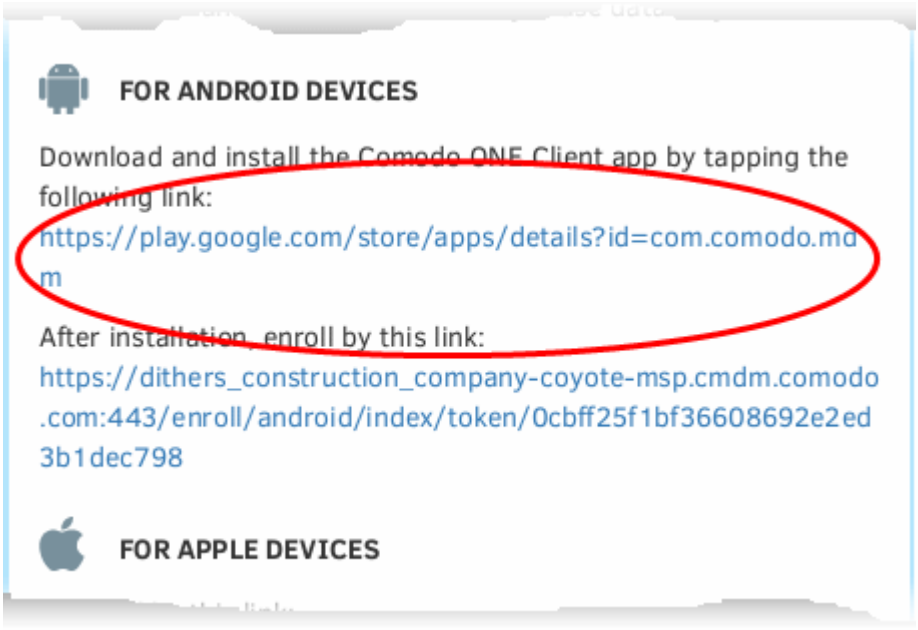
4.1.2.1. Enrolling Android Devices

After adding a user's devices, the user will receive an email containing enrollment instructions and links to download the android ITSM agent. The user should open the email on the Android device to be enrolled and follow the instructions. Android device enrollment involves two steps:

- Step 1 - Downloading and Installing the agent
- Step 2 - Configuring the agent

Step 1 - Downloading and Installing the agent

- Open the mail in the device and tap the enrollment link in it. You will be taken to the enrollment page through your browser in the device.
- Tap the first link under 'For Android Devices'



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

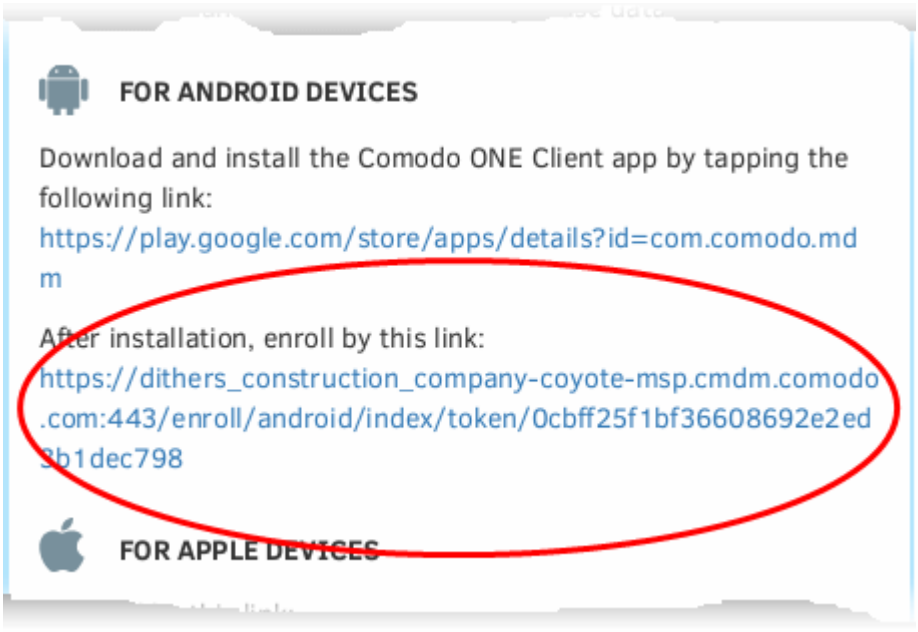
Step 2 - Configuring the agent

The agent can be configured to connect to the ITSM management server in two ways:

- Automatic Configuration
- Manual Configuration

Automatic Configuration

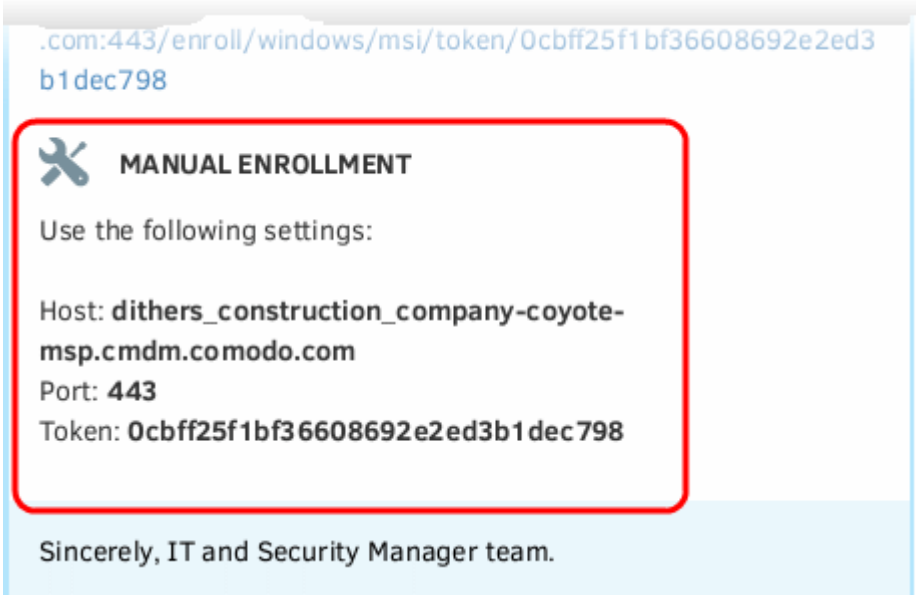
- Tap the enrollment link contained in the enrollment page after the completion of installation.



The agent will be automatically configured and the End User License Agreement screen will appear.

Manual Configuration

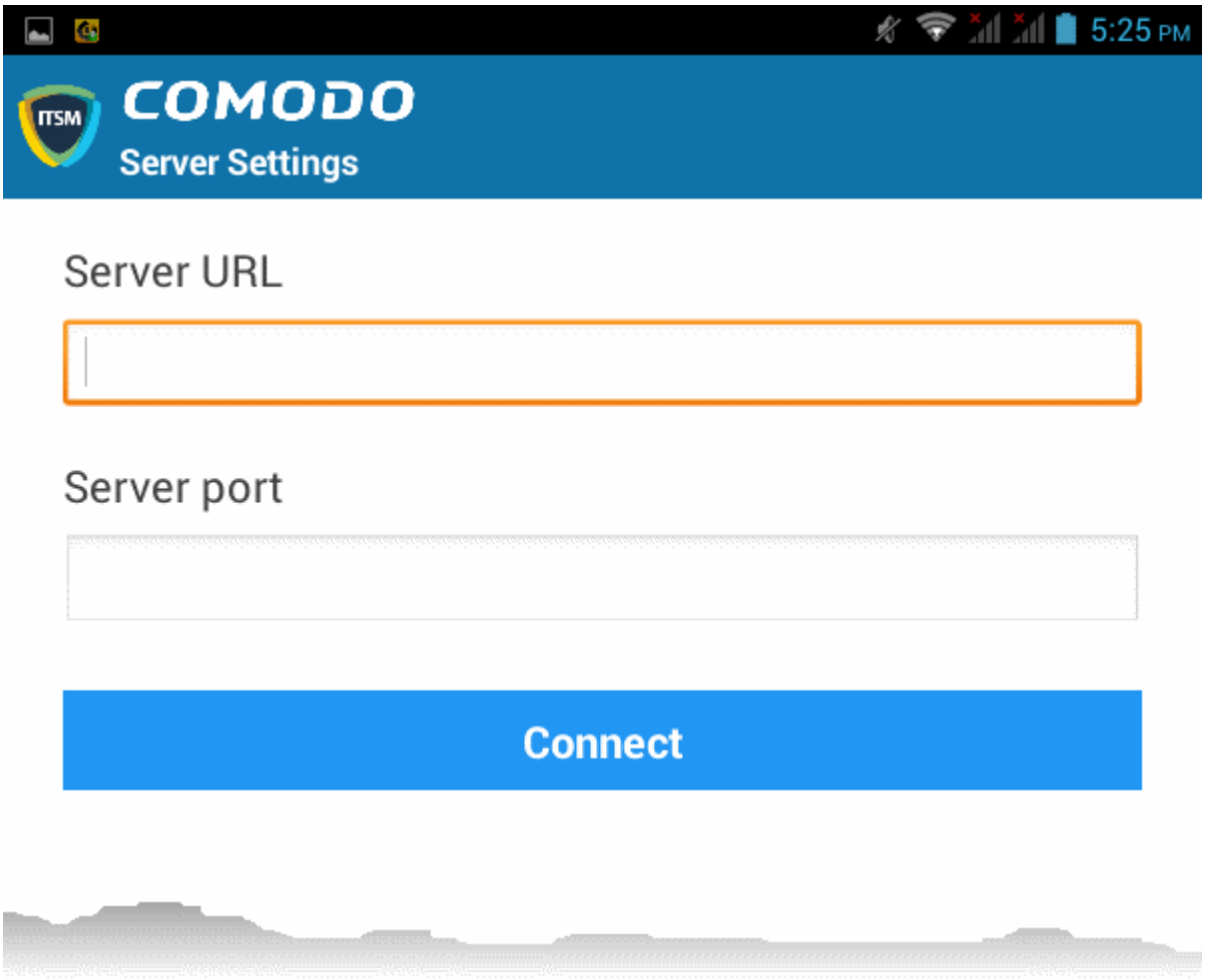
The user can manually configure the agent to connect to ITSM server by entering the server settings and the token ID contained in the enrollment page.



To manually configure the agent

- Open the agent by tapping the agent icon from your device. The agent configuration wizard will start enabling you to enroll the device by configuring the Server settings and unique token.

Server Settings



Server Settings - Table of Parameters		
Form Element	**Type**	**Description**
Server URL	Text Field	Enter the url of the ITSM server contained in the mail.
Server port	Text Field	Enter the connection port of the server for your device to connect, as specified in the mail. (Default = 443)

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

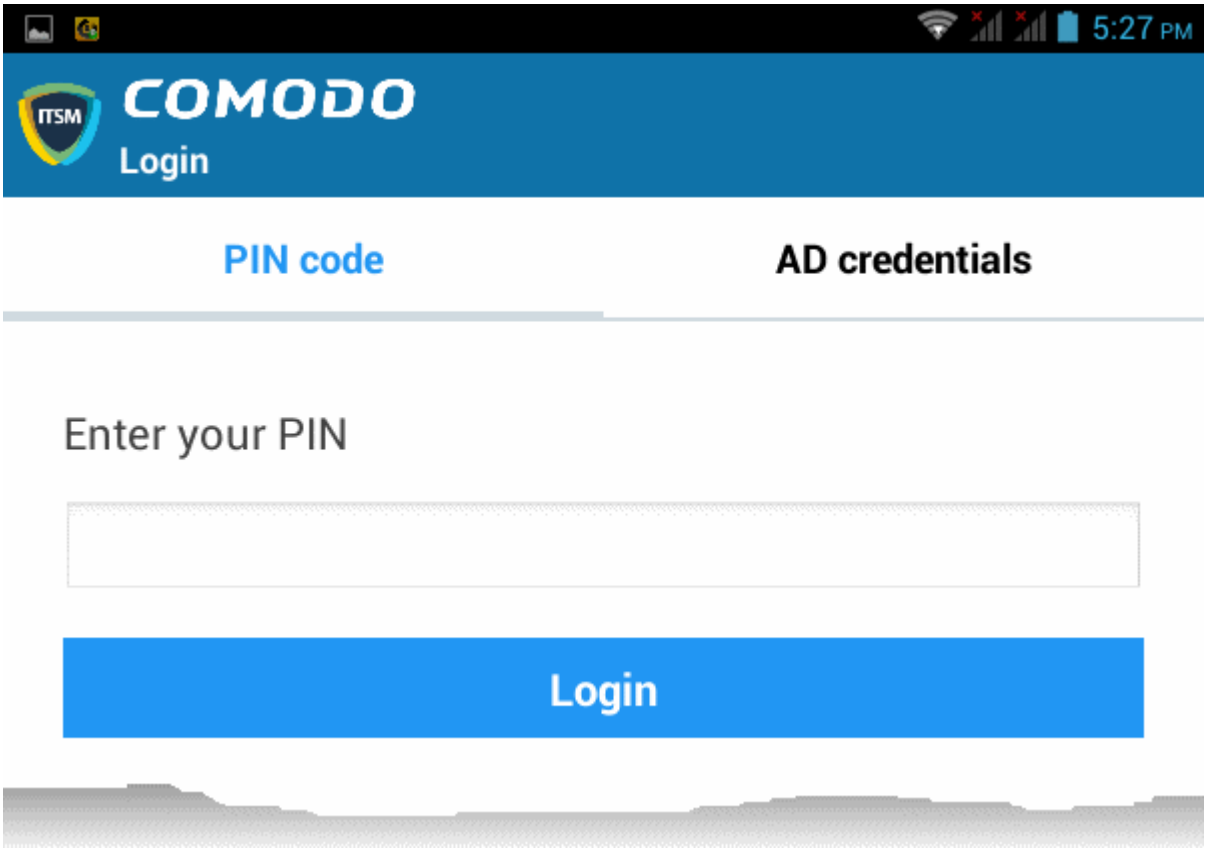
Logging-in to the Console

You can make the app to login to the ITSM console in two ways:

- By entering the personal identification number (PIN) contained in the email
- By entering your username and password

Entering PIN

- Tap the '**Pin Code**' tab in the 'Login' screen



- Enter the PIN (token) contained in the enrollment email
- Tap 'Login'. The **End User License Agreement** screen will appear.

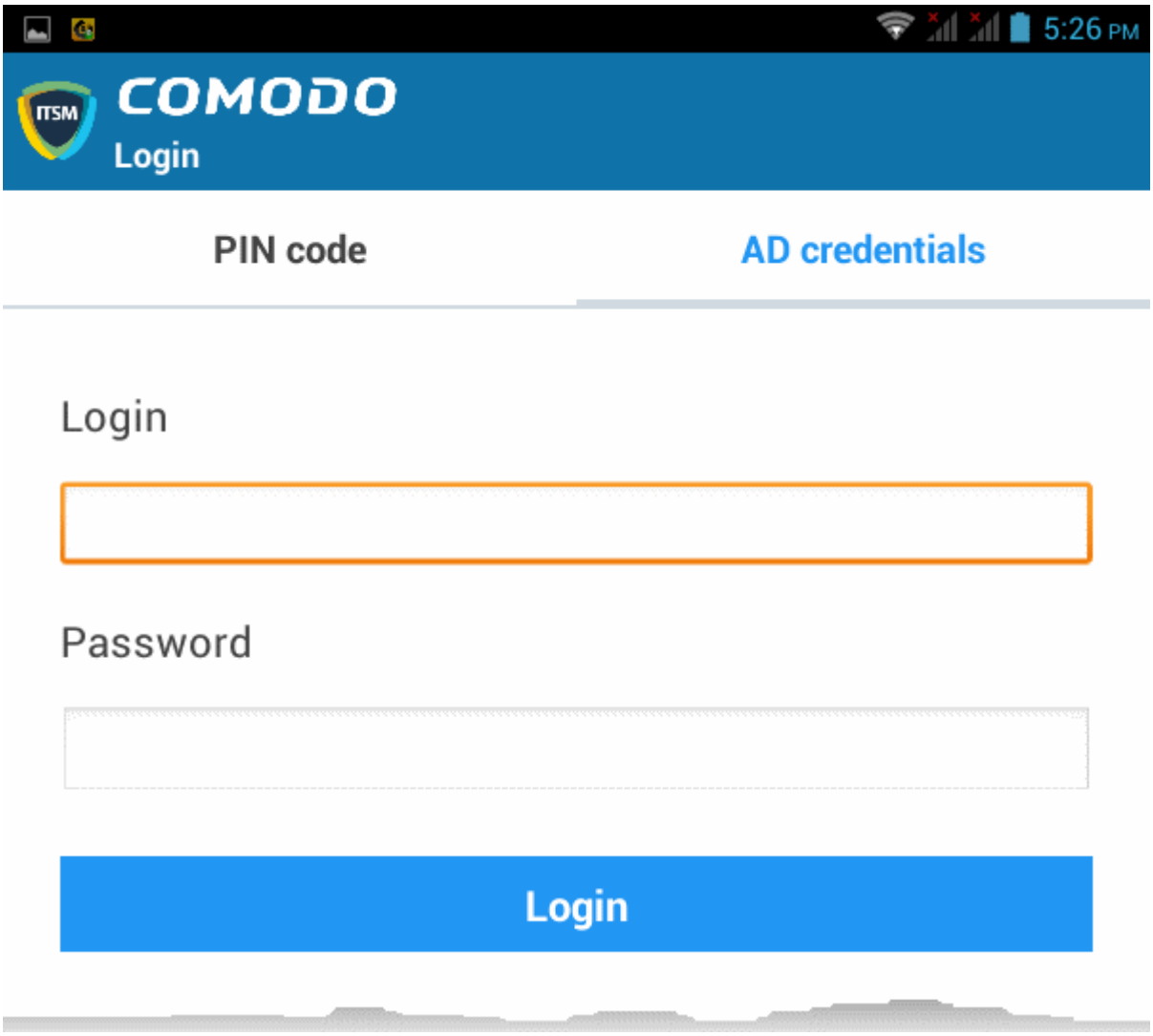
Entering your username and password

- Tap the '**AD Credentials**' tab in the 'Login' screen

Prerequisite: Enrollment of user devices using their Active Directory (AD) credentials requires:

- The AD server to be integrated with ITSM
- The users to be imported from AD to ITSM.

Refer to the section **Importing User Groups from LDAP** for more details



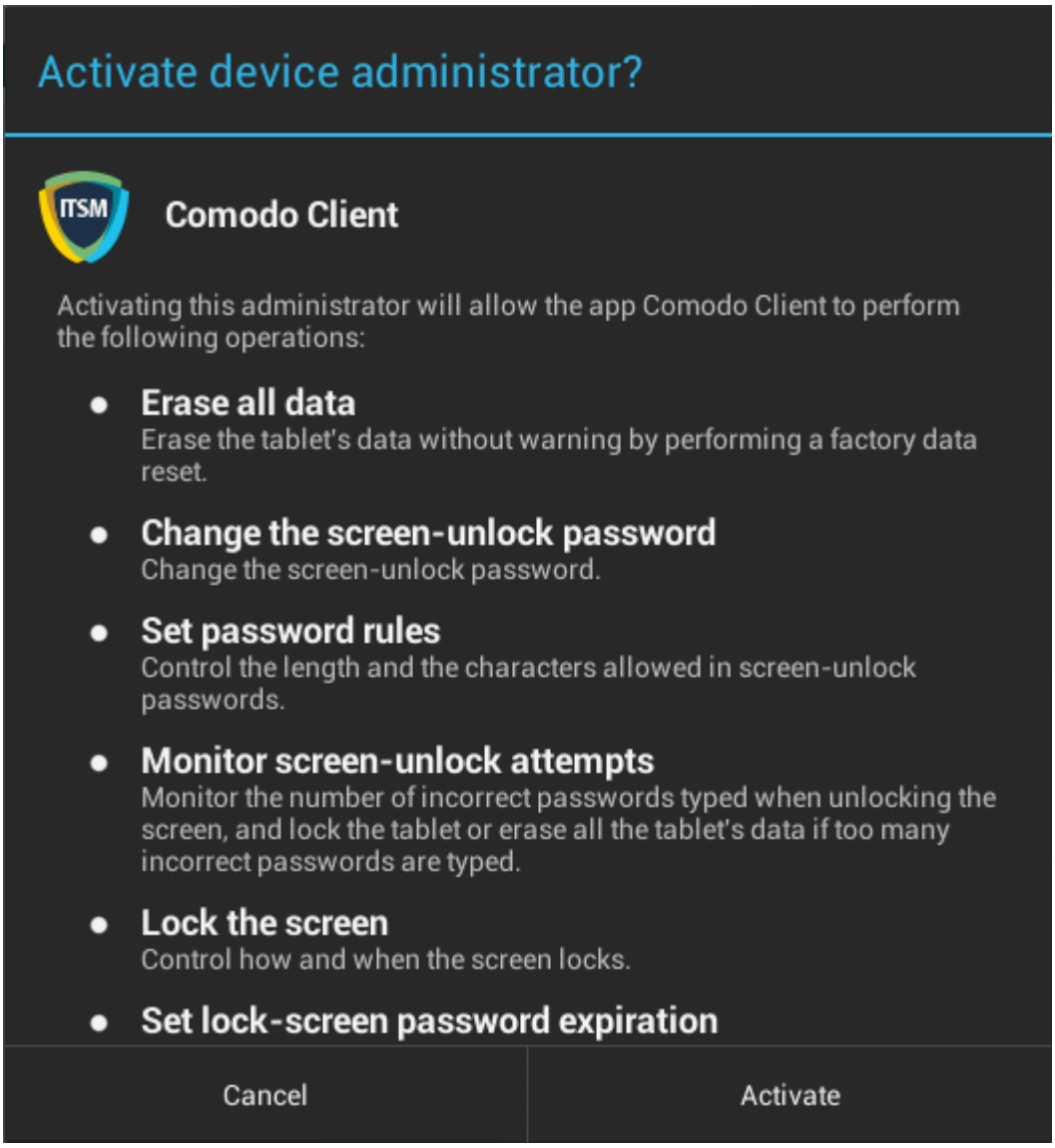
- Enter your username and password for logging-in to your network domain.
- Tap the 'Login' button

End User License Agreement

The EULA screen will appear.

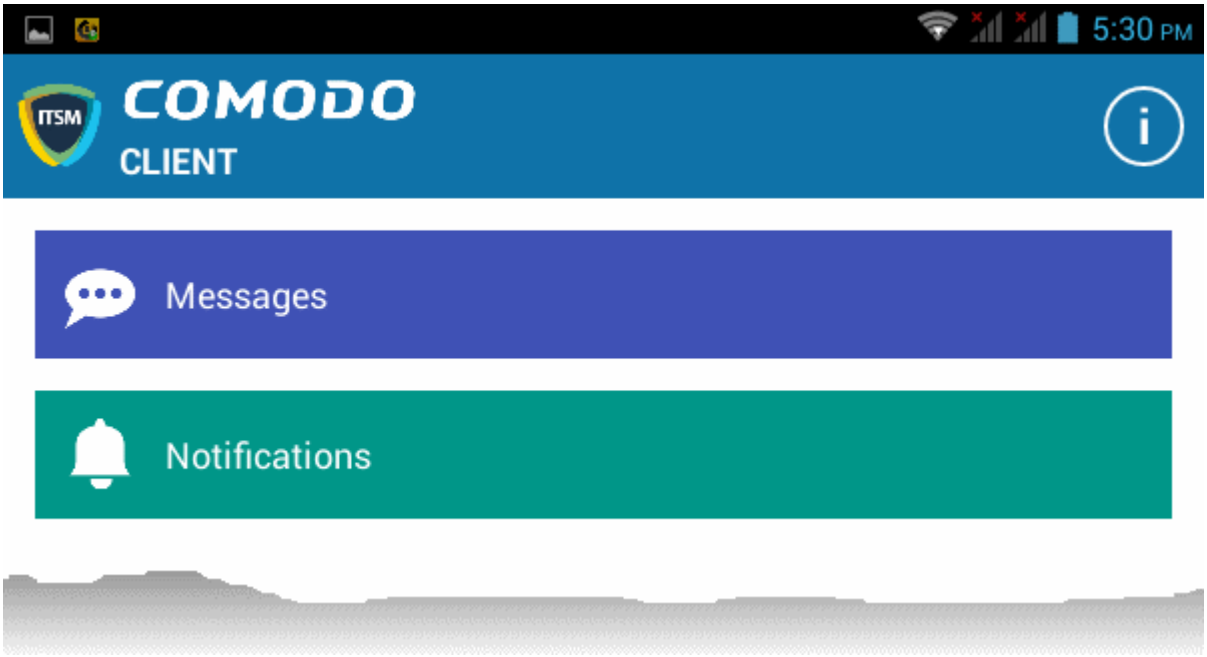
- Scroll down the screen, read the EULA fully and click the 'I ACCEPT' button at the bottom.

The screen for activating the ITSM client as Device Administrator will appear.



- Tap 'Activate'.

The ITSM agent home screen will appear.



The device is enrolled to ITSM and can be remotely managed from the ITSM console.

4.1.2.2. Enrolling iOS Devices

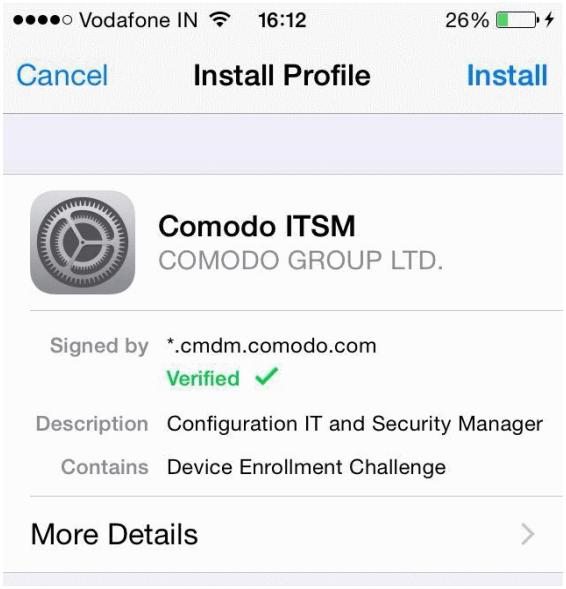
After the administrator has added devices for a user, the user will receive an enrollment email with a link to a page containing the enrollment instructions and links to download the ITSM profile and the server certificate. The user should open the email in the iOS device to be enrolled and follow the instructions.

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.

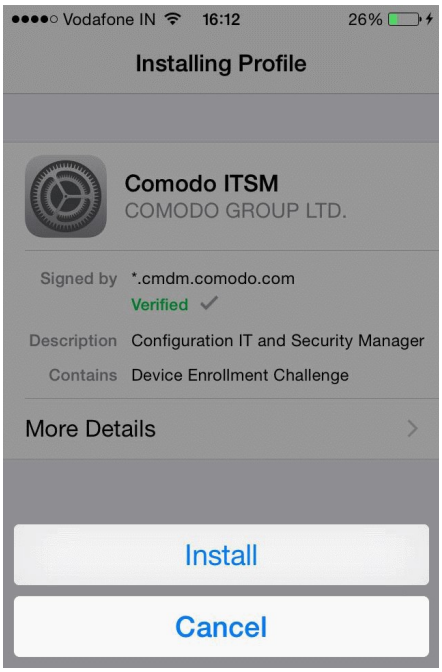
To enroll an iOS device

- Open the mail in the device and tap the enrollment link in it. You will be taken to the enrollment page through your browser in the device.
- Tap the enrollment link under "For Apple Devices"

The 'Install Profile' wizard will start.

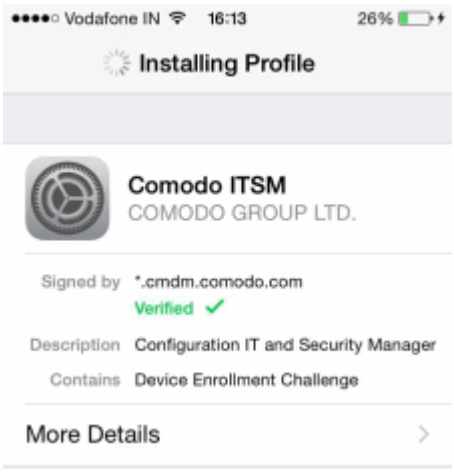


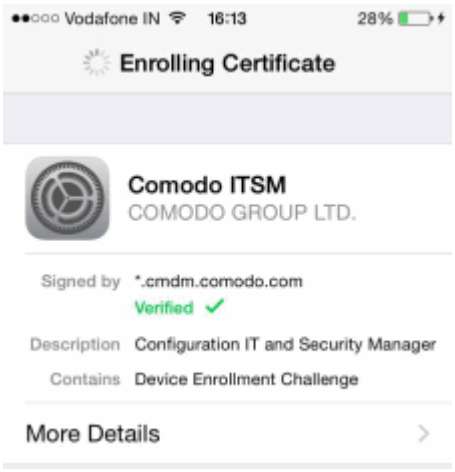
- Tap 'Install'. A confirmation dialog will be displayed.



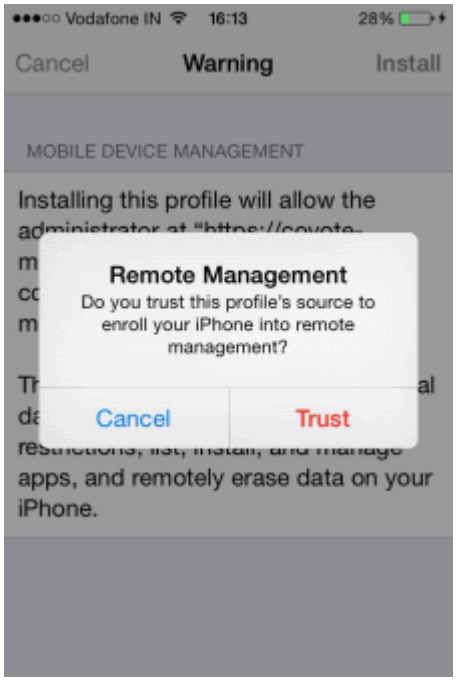
- Tap 'Install'.

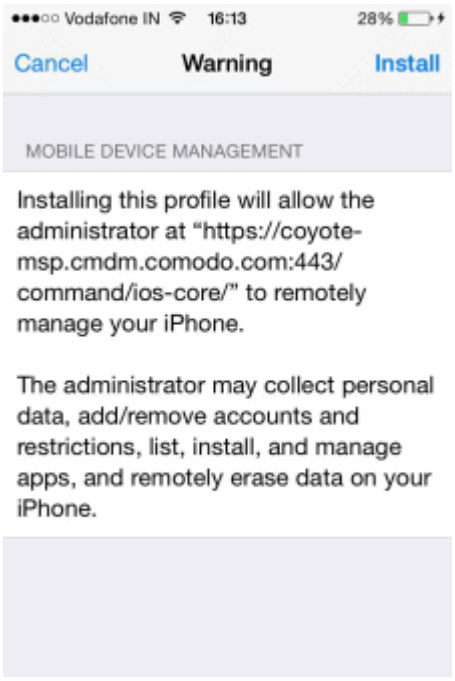
The ITSM Profile installation progress will be displayed.





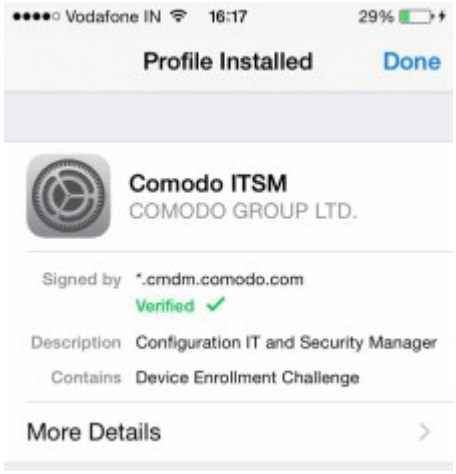
- A privacy warning screen with the privileges granted to the administrator by installing this profile will be displayed during the installation process. Read the warning fully and tap 'Trust' to proceed.





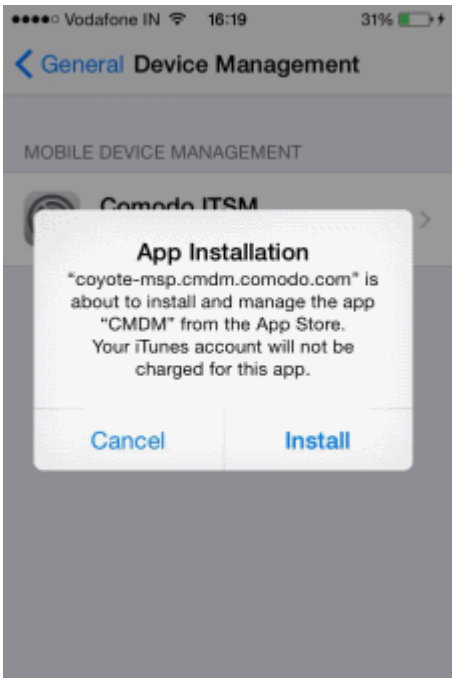
- Click Install in the 'Warning' screen

The installation process will continue and when completed the 'Profile Installed' screen will be displayed.

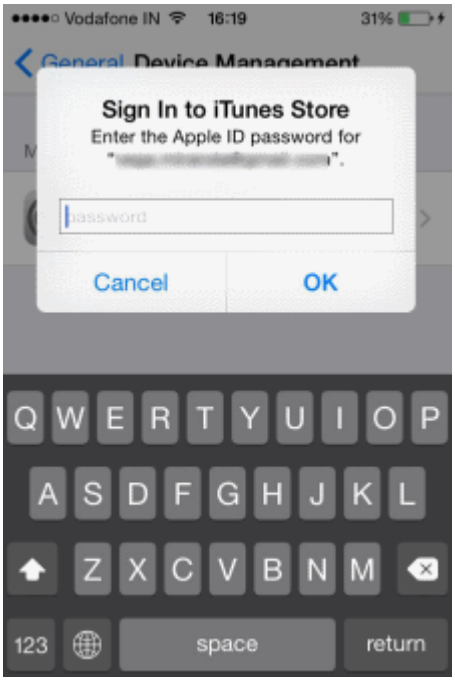


- Tap 'Done' to finish the ITSM profile installation wizard.

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.



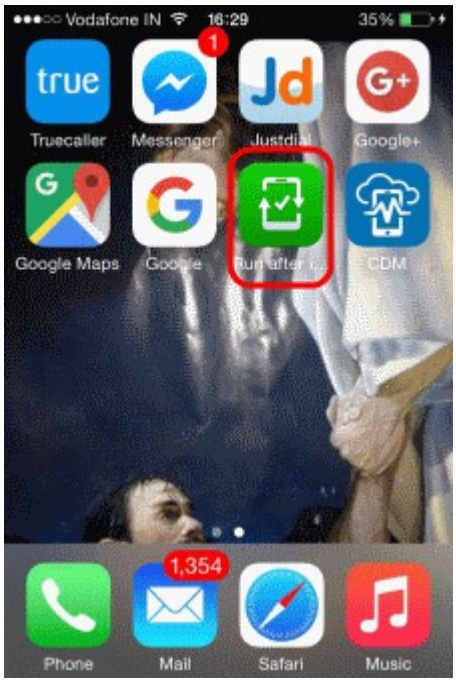
The app will be downloaded from iTunes store, using the user's iTunes account. The app is free, hence the user will not be charged for installing the app.



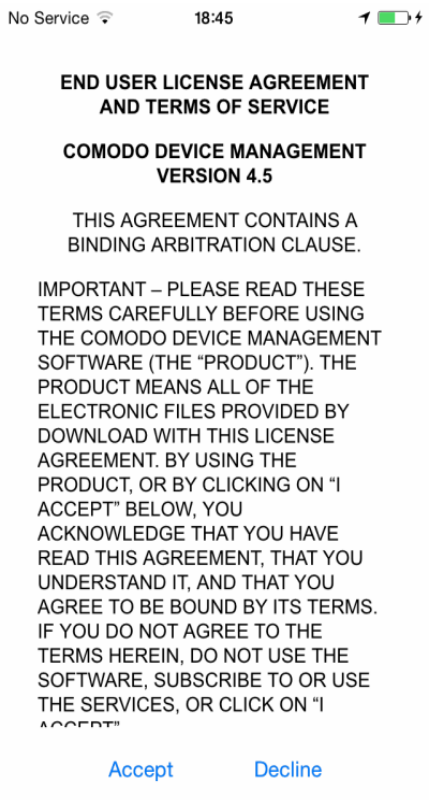
- The user needs to enter their Apple account password to access iTunes store.

The App will be installed.

- To complete the enrollment, tap the green 'Run After Install' icon from the Home screen

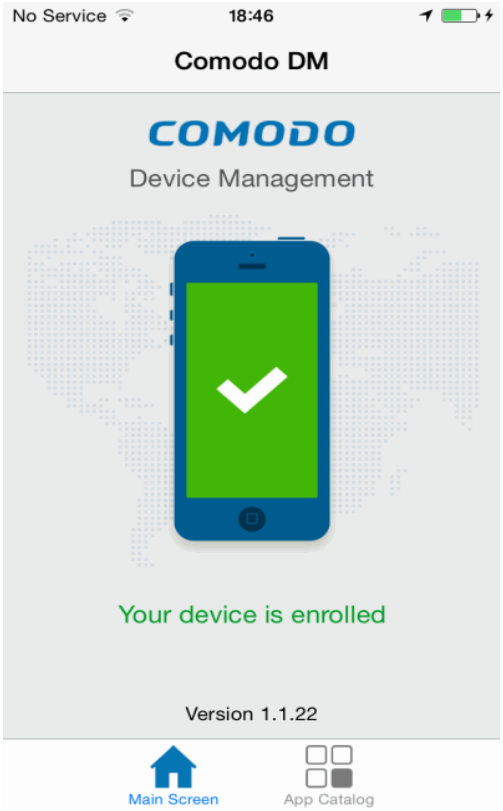


- The EULA screen for device management app will be displayed.

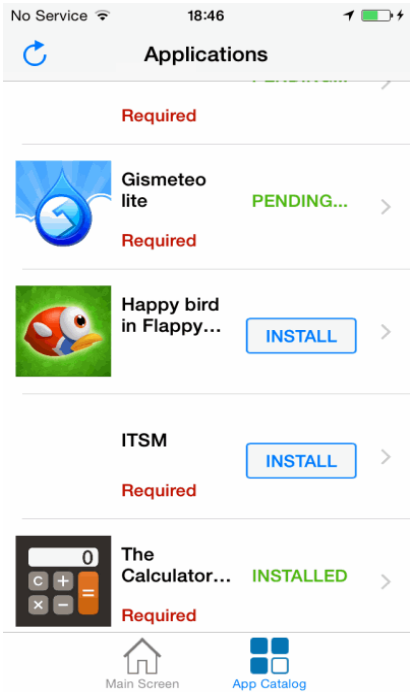


- Read the End User License Agreement fully and tap 'Accept'
- Tap 'OK'.

The device will be successfully enrolled.



Tapping 'App Catalog' will display the iOS apps that are installed, required to be installed and available for installing.

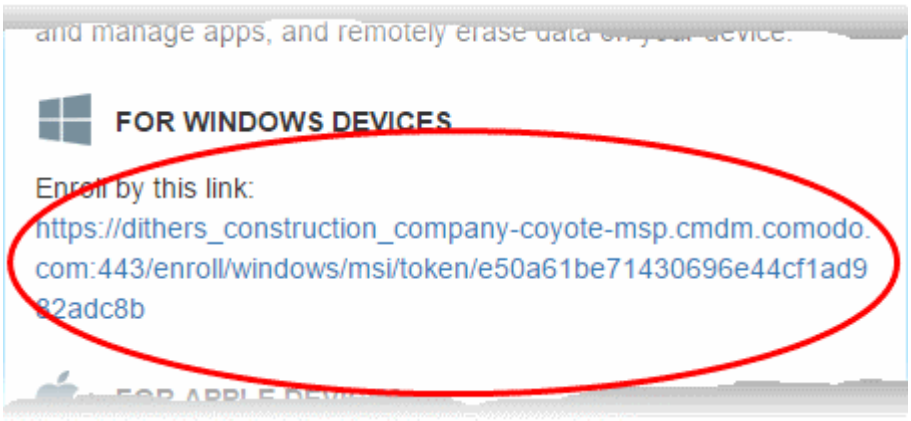


4.1.2.3. Enrolling Windows Endpoints

After the administrator has added devices for a user, the user will receive an enrollment email with a link to the enrollment page. The enrollment page will contain the enrollment instructions and a link to download the ITSM agent for Windows endpoints. The user should open the email at the Windows endpoint to be enrolled and follow the instructions. Upon successful enrollment, the ITSM agent will be installed on the endpoint and automatically configured to connect to the ITSM server.

To auto enroll a Windows device

- Open the mail in the device and click the enrollment link in it. You will be taken to the enrollment page through the default browser of the endpoint computer.



- Click on the enrollment link under 'For Windows Devices'.

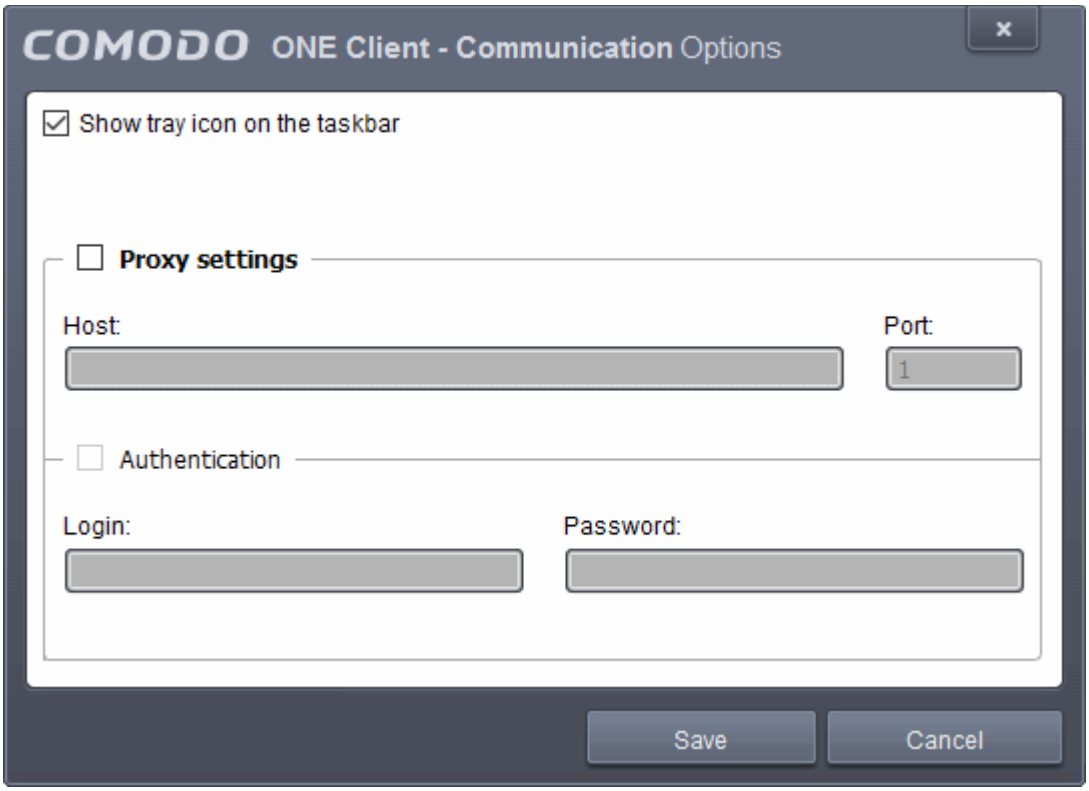
The ITSM agent setup file will be downloaded.

- Double click on the file to install the agent.

The installation runs silently on the background. On completion of installation, the device will be automatically enrolled to the ITSM server and the ITSM system tray icon  will appear at the bottom right of your screen.

Once the device is enrolled, the next step is to install CCS onto the endpoint in order for the default or assigned Windows profiles to take effect. Refer to the section **Remotely Installing Packages onto Windows Devices** for more details.

For a manual device enrollment type host, port and token ID specified in the device enrollment form.



4.1.2.4. Enrolling Mac OS Endpoints

After a device has been added for a user, they will receive an email containing enrollment instructions and links to download the ITSM profile and agent for Mac OS devices. The user should open the email on the target Mac OS device and follow the instructions.

Enrolling a Mac OS device involves two steps:

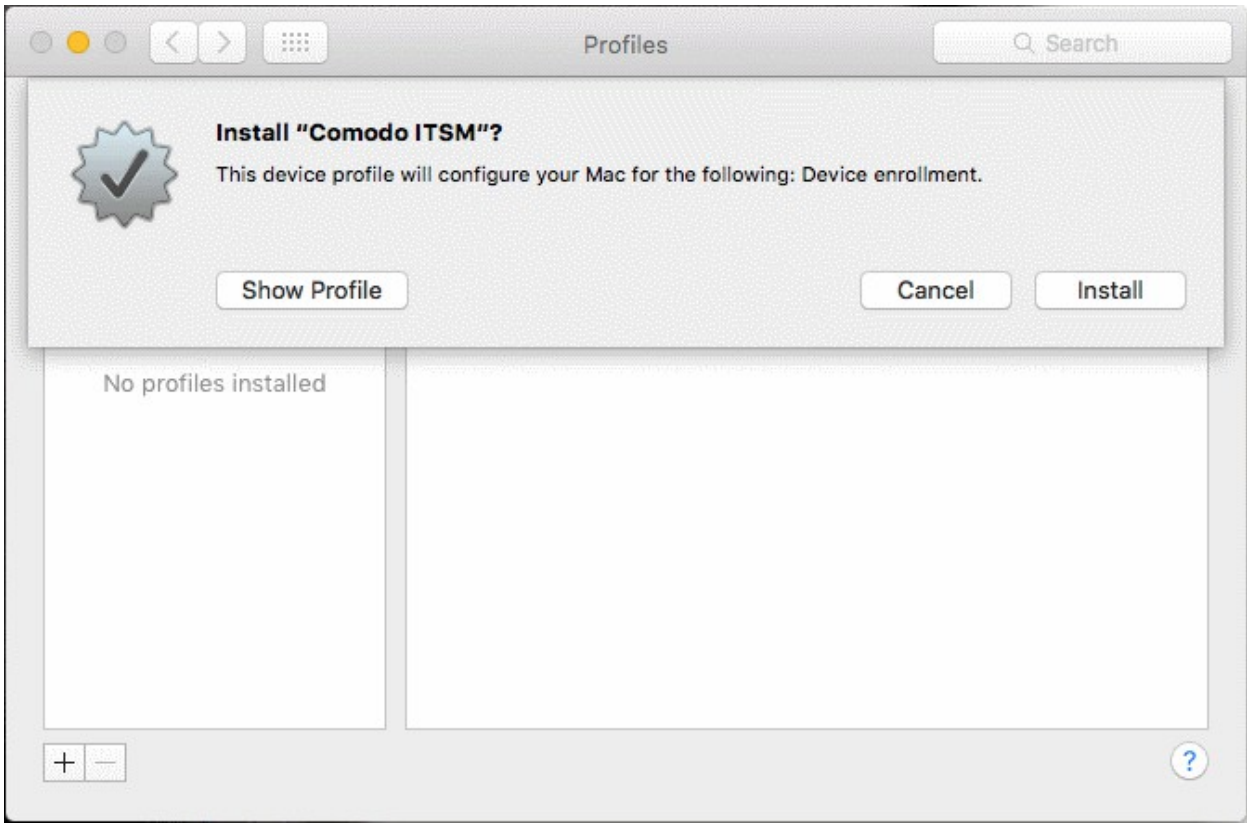
- Step 1 - Installing the ITSM Configuration Profile
- Step 2 - Installing the ITSM Agent

Step 1 - Installing the ITSM Configuration Profile

To install the configuration profile

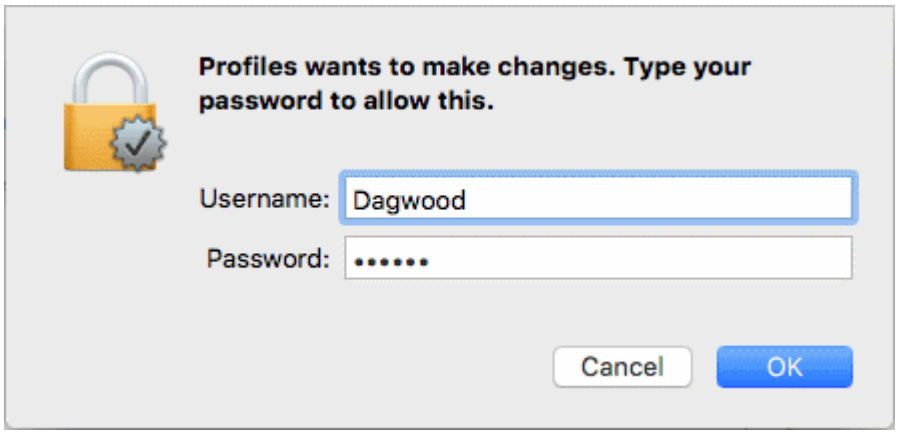
- Open the enrollment mail on the target device then tap the enrollment link. This will open the device enrollment page.
- Next, click the link under "For Apple Devices":

The configuration file 'itsm.mobileconfig' will be downloaded and the 'Install Profile' wizard will be started.



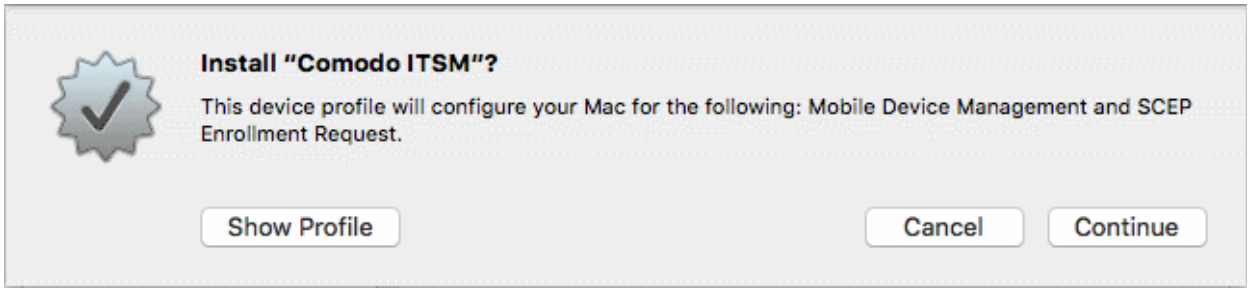
- Tap 'Install'.

You need to enter your password to install the profile.



- Enter your device username and password and click OK to continue the installation

Confirmation dialogs will appear for profile installation.

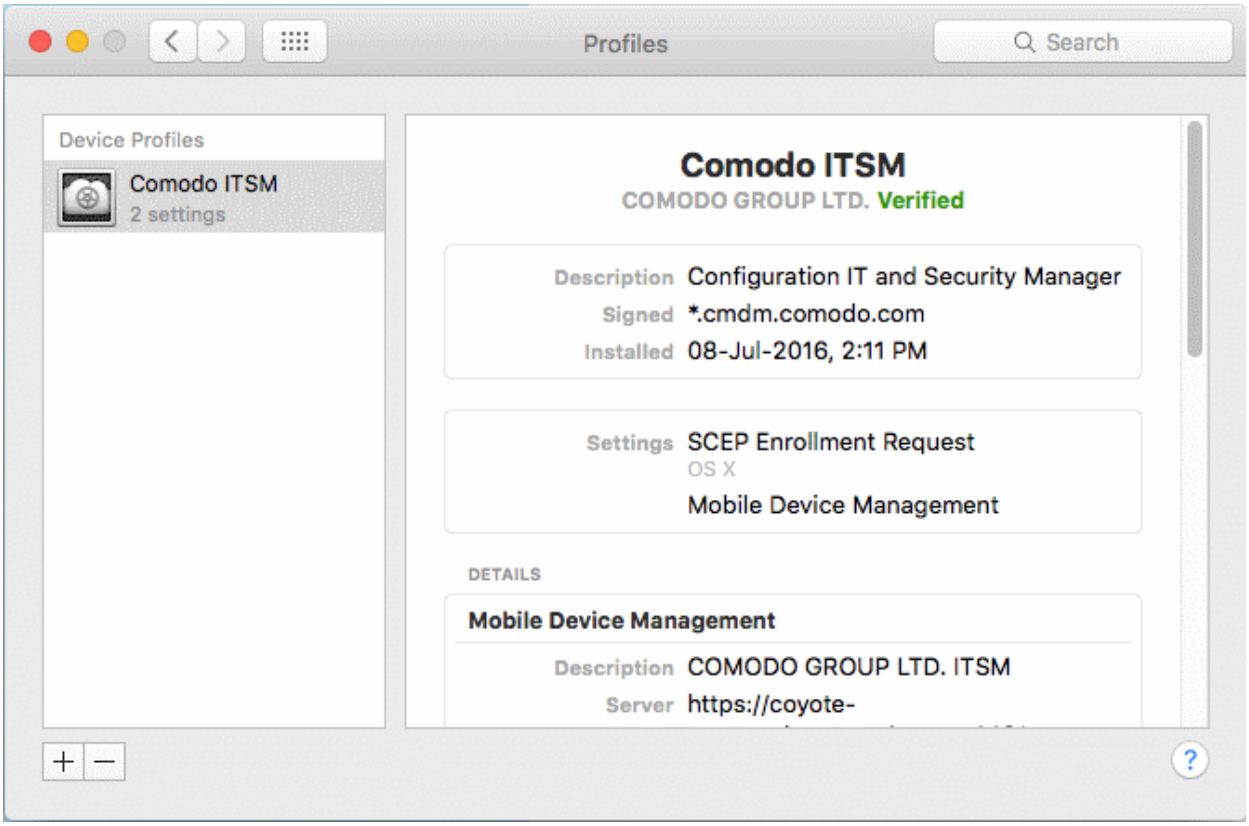


- To view the profile details, click 'Show Profile'

- Click 'Continue'

- Click 'Install'

The profile will be installed.

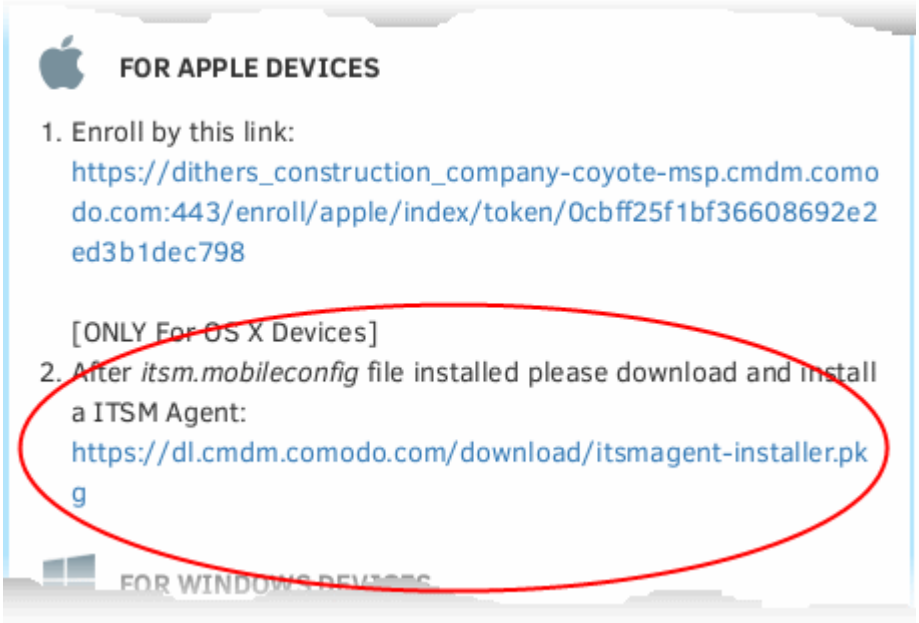


Step 2 - Installing the ITSM Agent

After installing the profile, the ITSM agent needs to be installed so the device can communicate with the ITSM server.

To download and install the ITSM agent

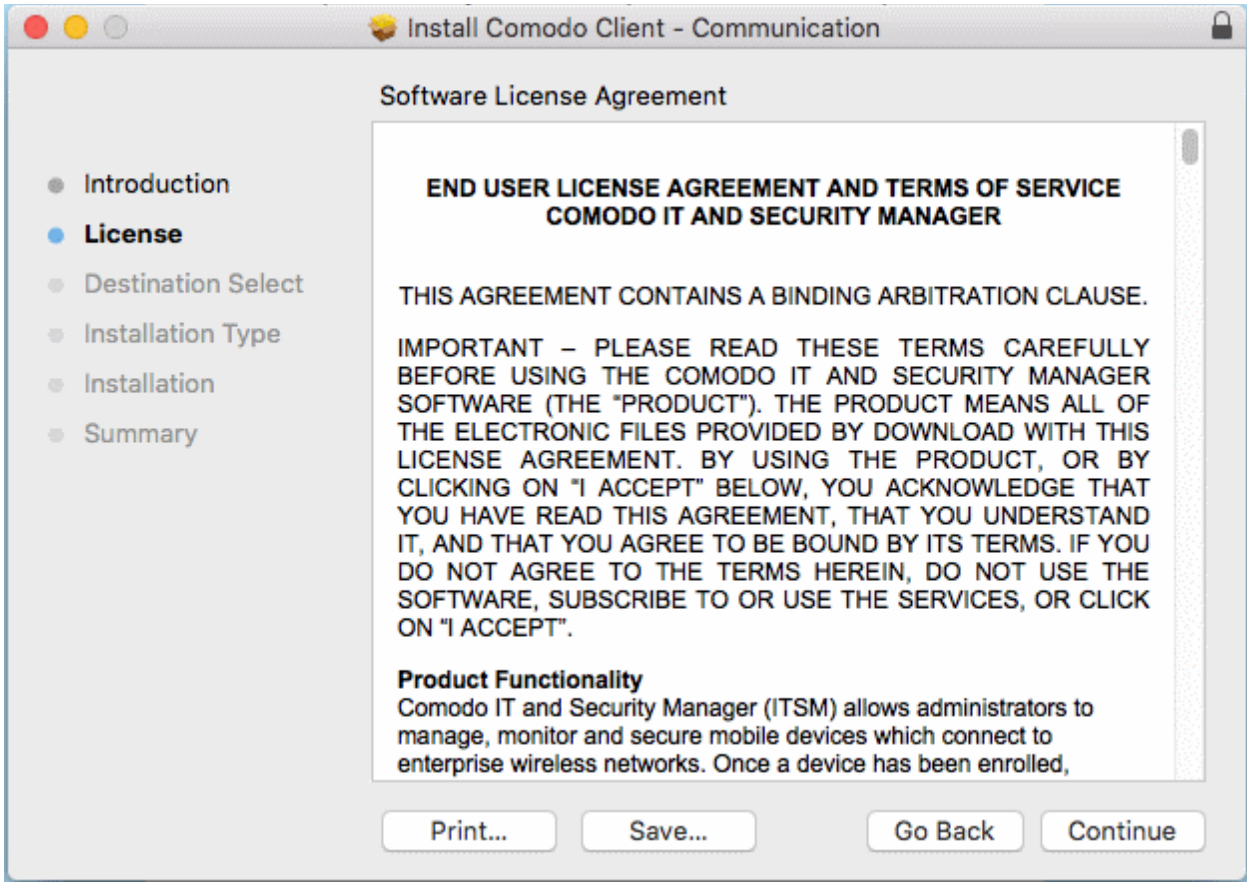
- Open the device enrollment page and click the link to download the agent as shown below:



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

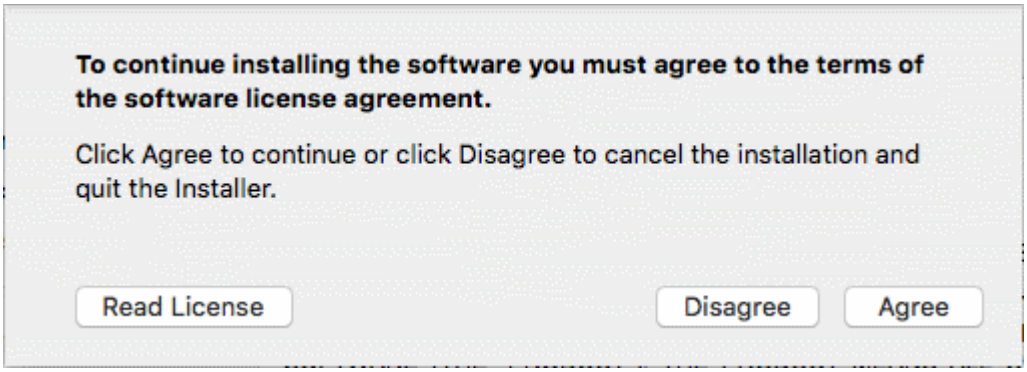
- Click 'Continue'

The End User License Agreement will be displayed.



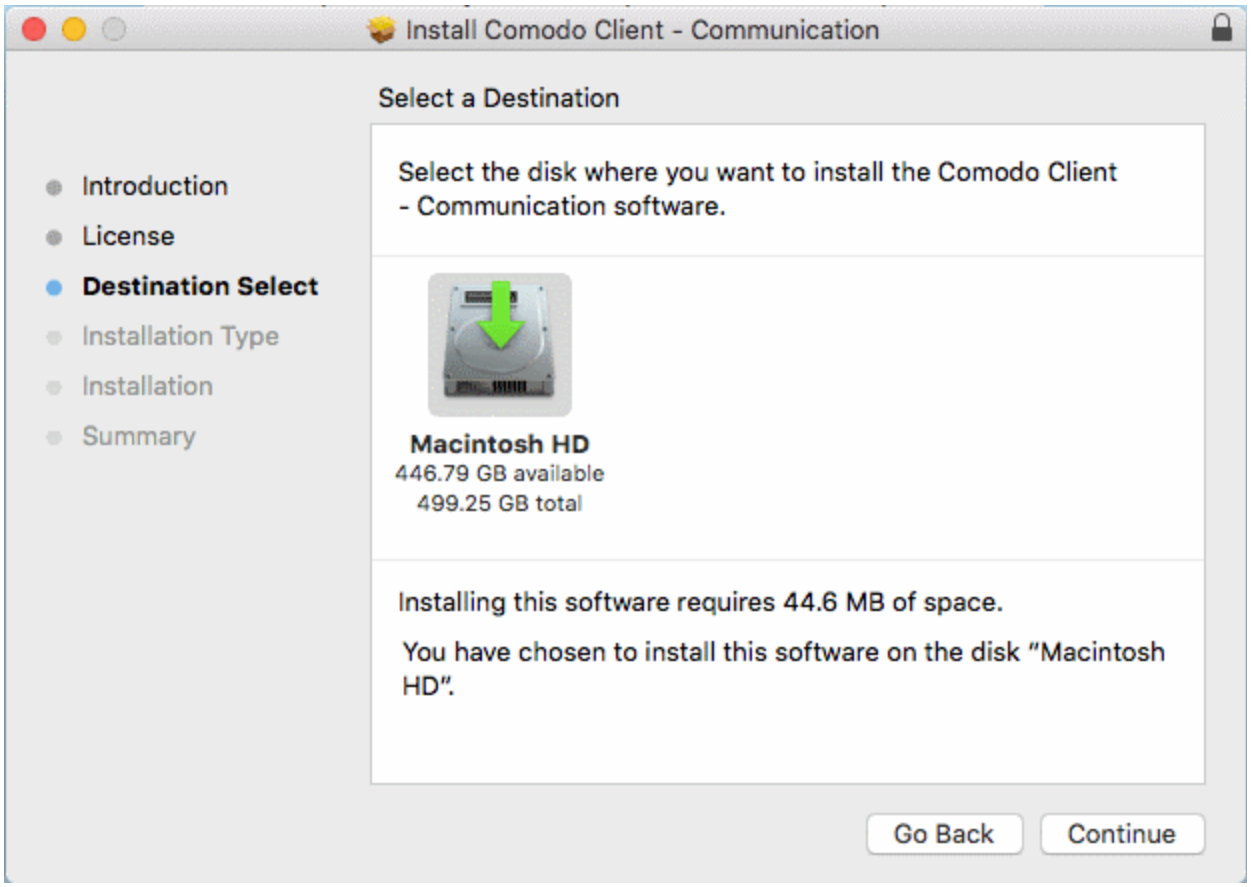
- Read the EULA and click 'Continue'.

A confirmation dialog will appear.



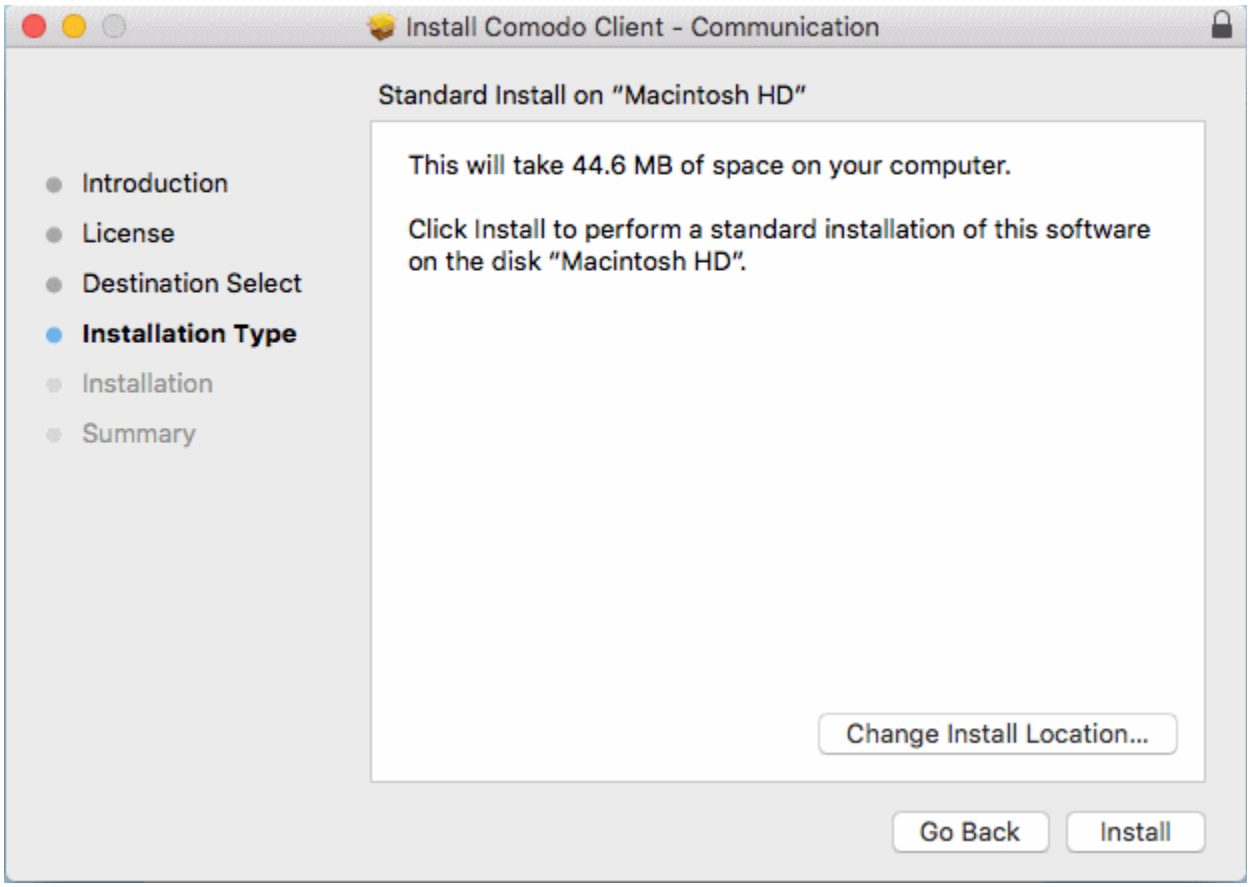
- Click 'Agree'

The next step allows you to choose the location at which the agent is to be installed.



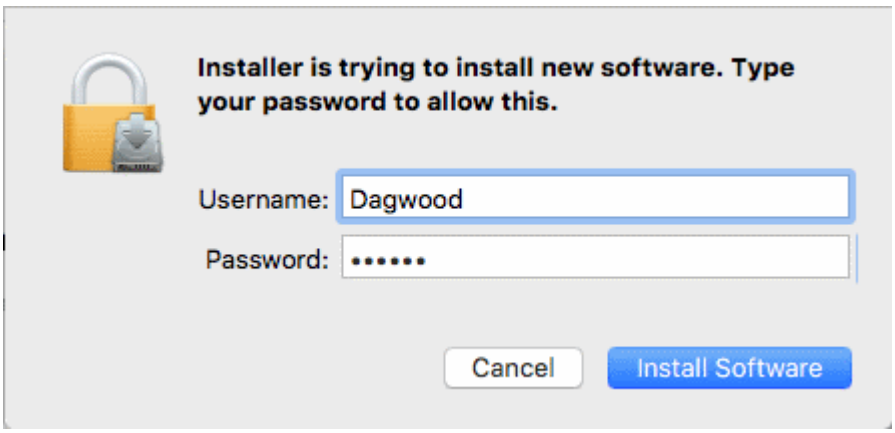
- To install the agent in the default location, click 'Continue'. To install the agent in a different location, click the disk icon, navigate to the new location and click 'Continue'.

The next step allows you to choose the installation type and start the installation.

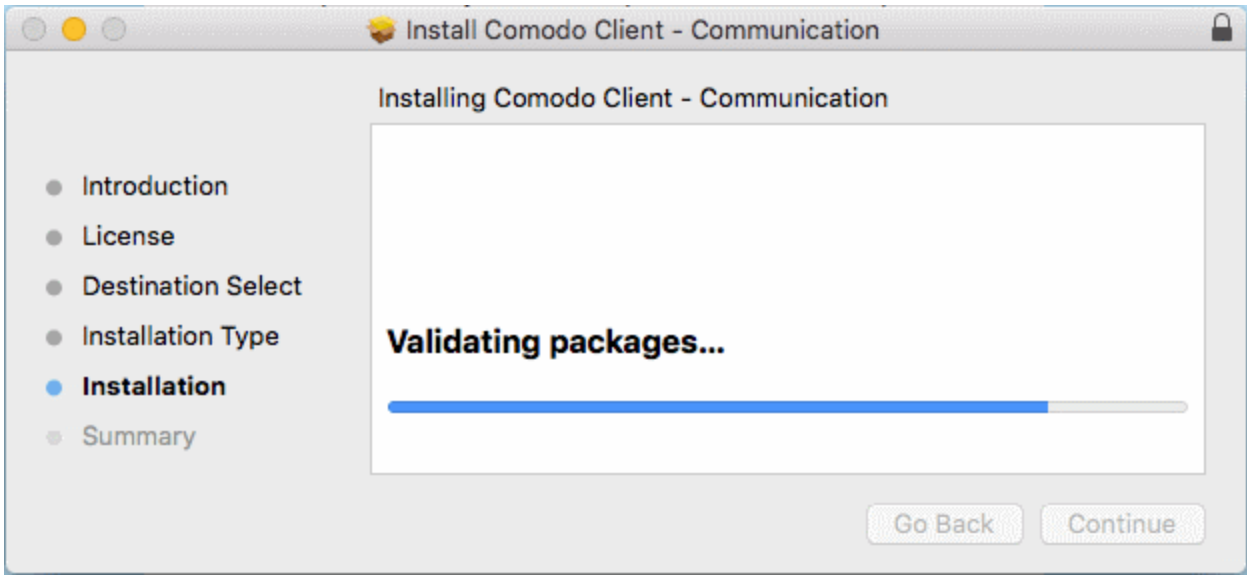


- Click 'Install'

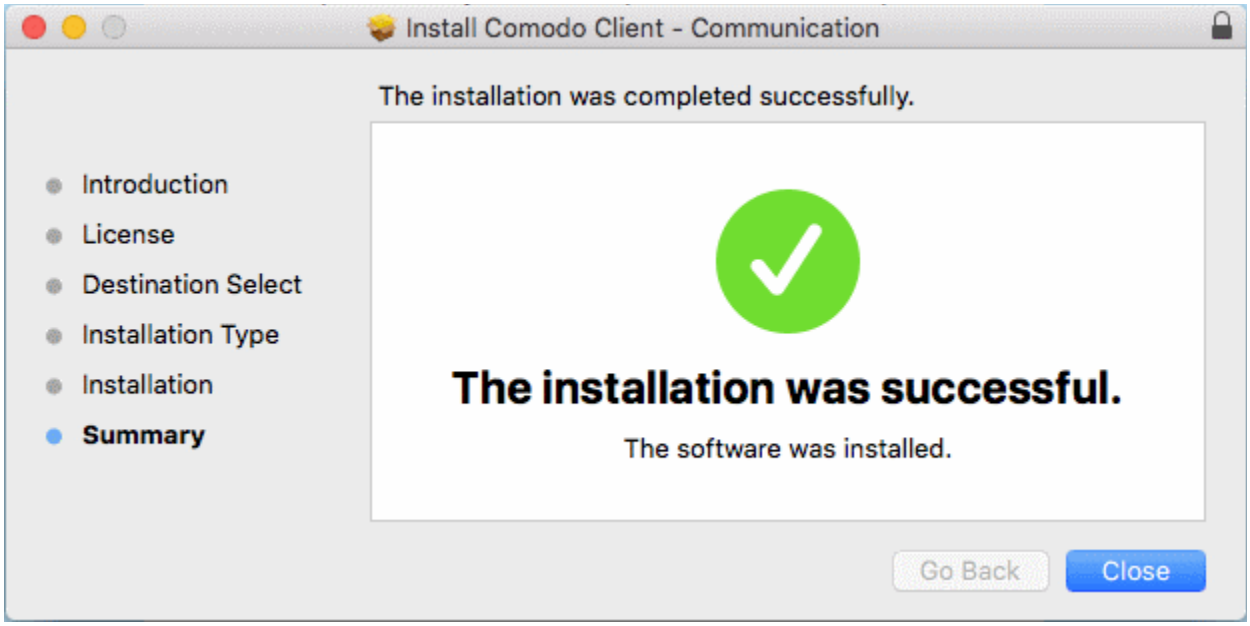
You need to enter your device password to allow the installation:



- Enter your username and password and click 'Install Software'



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



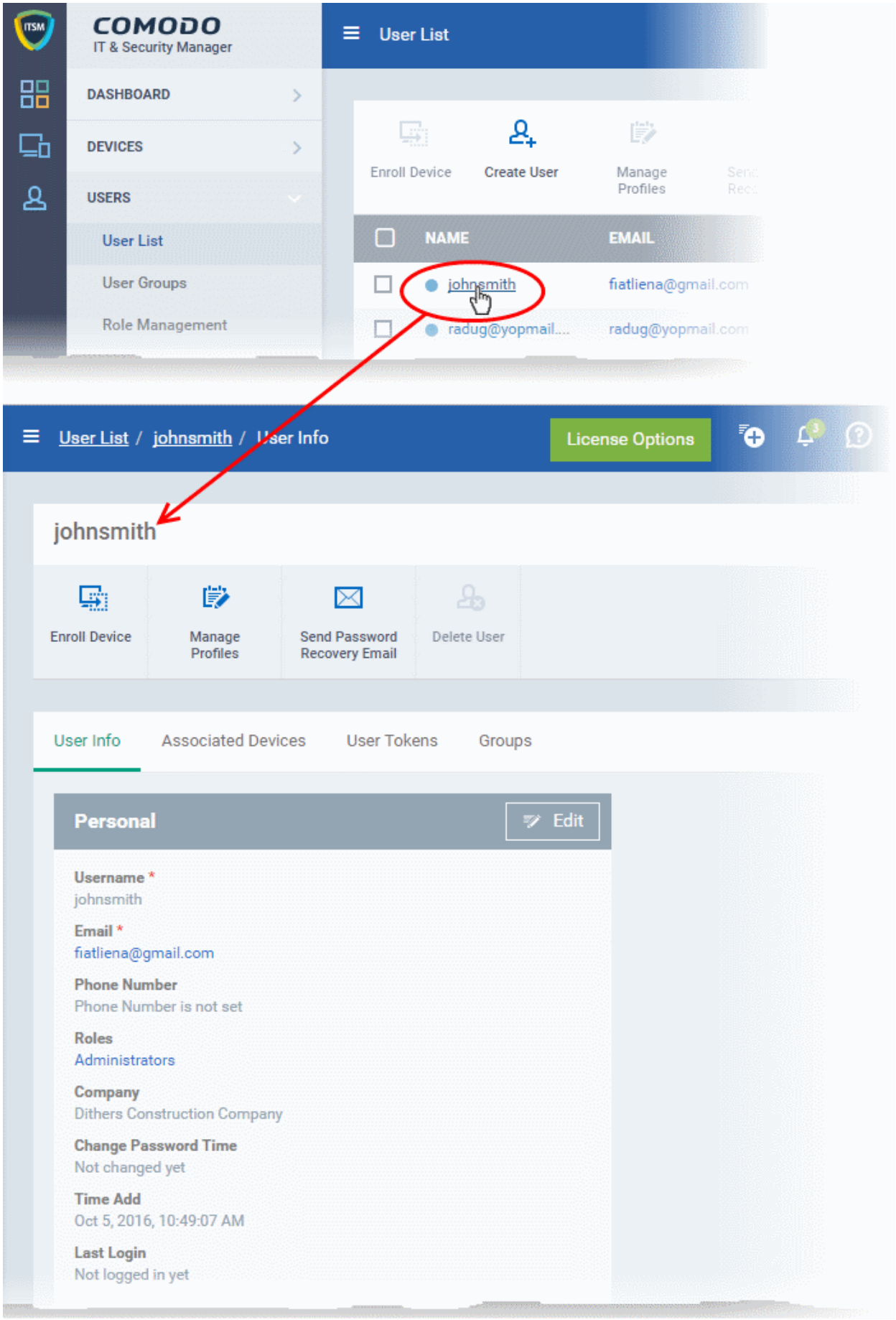
4.1.3. Viewing User Details

Administrators can view user account details at anytime from the 'Users' interface.

To view user details

- Open the 'Users' interface by clicking 'Users' > 'User List'
- Click the name of a user

The 'User Details' screen will open:



You can update these details by clicking the 'Edit' button at top right. Refer to Updating Details of a User for more

details. Please note you cannot edit the details of users that are added via the C1 management portal.

The User Details screen also allows administrators to:

- Enroll new devices for users
- Apply configuration profiles to devices
- Send password recovery emails for users to access the ITSM console
- View and manage devices enrolled for users
- View device enrollment tokens generated for users
- View and manage Groups to which the user is a member

Enroll new devices for users

- Click 'Enroll Device' at the top of the details interface

The 'Enroll Devices' dialog will open with the user pre-populated. Refer to **Enrolling User Devices for Management** for more on enrolling user devices.

Apply Configuration Profiles to user devices

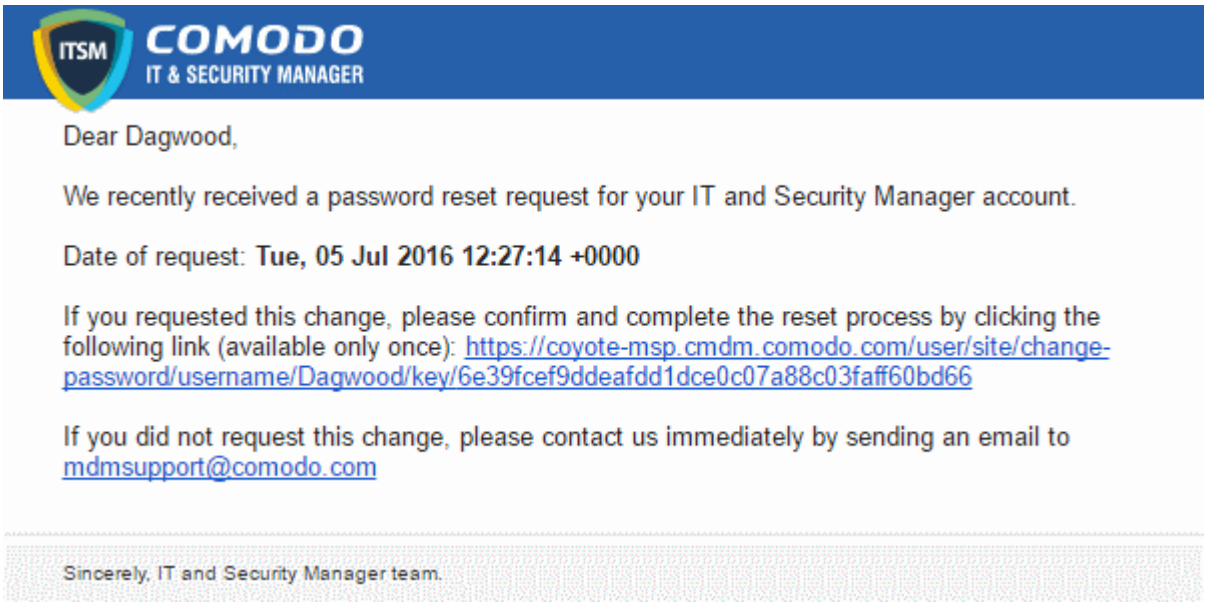
- Click 'Manage Profiles' at the top of the User Details interface

The 'Manage Profiles' interface will open with a list of profiles added to user's devices. You can add new profiles to the user which will be applied to their enrolled devices. See **Assigning Configuration Profile(s) to a Users' Devices** for more details.

To send Password Recovery emails to users

- Click 'Send Password Recovery Email' at the top of the 'User Details' interface. Please note that this option will not be enabled for users that were added via the C1 management portal.

An email will be sent to the user with a link to set a new password:

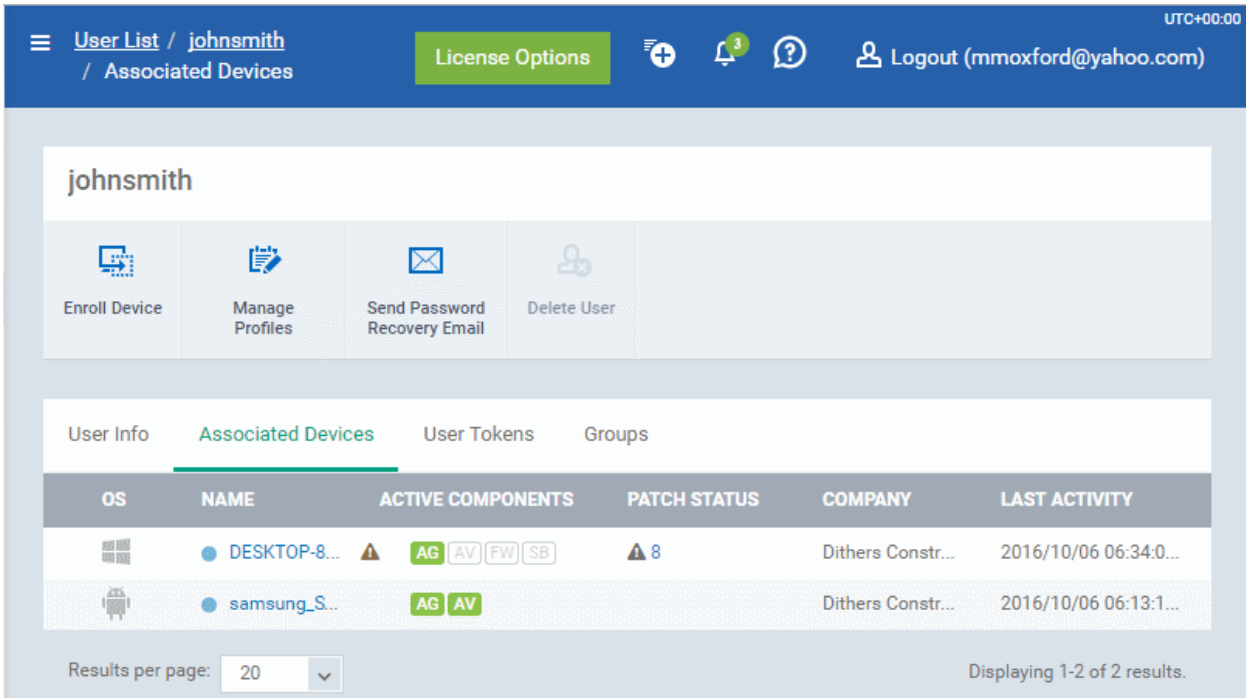


Tip: Alternatively, you can send the password reset mail from the 'User List' interface. Select the user from the list and click 'Send password Recovery Email' at the top.

To view the devices associated with a user

- Click the 'Associated Devices' link

The devices that are enrolled for the user will be displayed:

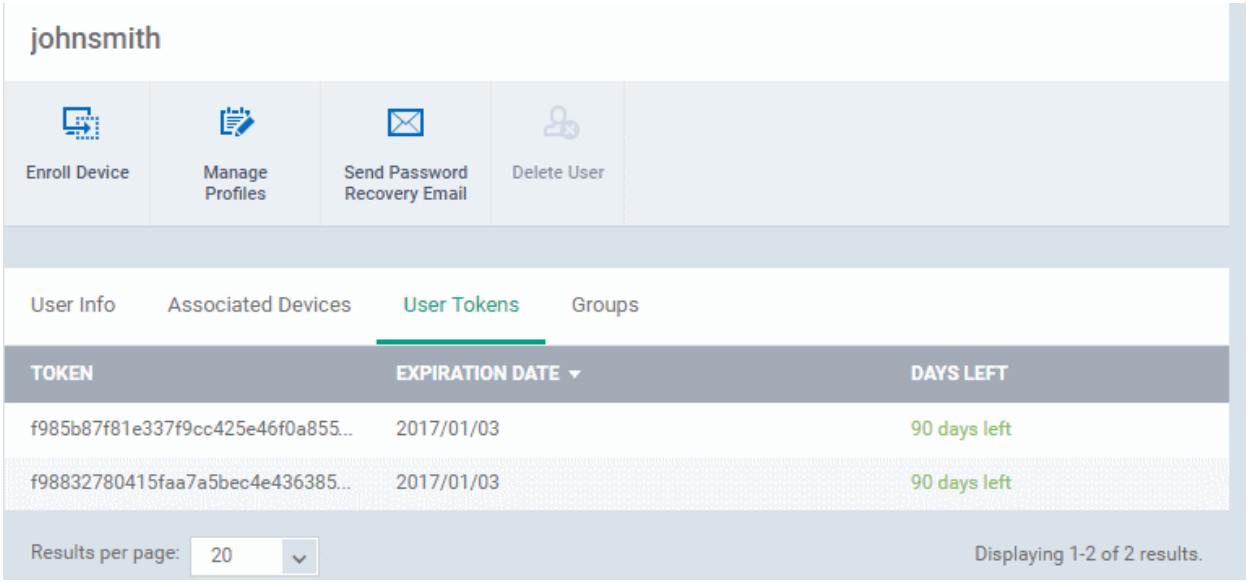


Associated Devices - Column Descriptions	
Column Header	**Description**
OS	Displays the Operating System of the device.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the 'Summary' screen of the device details interface. Refer to the section 'Viewing Summary Information' for more details.
Active Components	Indicates which endpoint security components are installed on the device. For example, Antivirus, Firewall, Containment etc.
Patch Status	Indicates how many OS patches are awaiting installation on the endpoint. Clicking the number will open the 'Patch Management' tab of the 'Device Properties' interface, enabling you to initiate installation of the missing patches. Refer to the section Viewing and Installing Windows Patches for more details.
Company	Indicates the company to which the device was registered.
Last Activity	Indicates the date and time at which the device last communicated with the ITSM agent.

To view user tokens

- Click the 'User Tokens' link

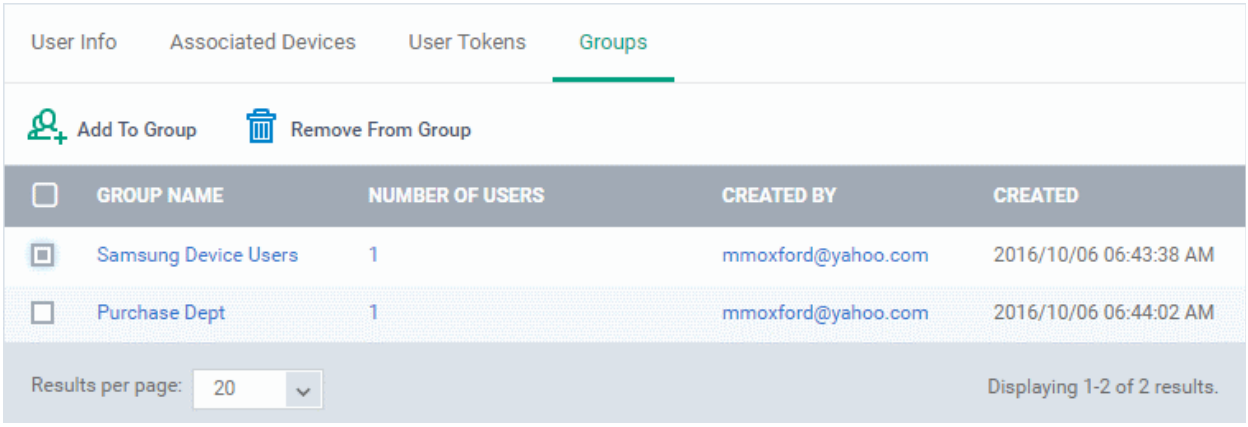
The page will list all tokens generated for the user to enroll their devices:



User Tokens - Column Descriptions	
Column Heading	**Description**
Token	Displays the unique serial number of each enrollment token.
Expiration Date	Date that the token expires. Users can enroll devices using the same token until expiry.
Days left	Indicates how many days remain until the token expires.

To view and manage user groups to which the user belongs

- Click the 'Groups' link to view all groups to which the user belongs:



Groups - Column Descriptions	
Column Header	**Description**
Group Name	The name assigned to the user group by the administrator. Clicking the Group Name will take you to the Group Details interface. Refer to the section Editing a User Group for more details.
Number of Users	Indicates the total number of users in the group. Refer to the section Editing a User Group for more details.
Created By	Indicates the administrator that created the group. Clicking the name opens the User

	Details interface of the administrator. Refer to the section Viewing the Details of a User for more details.
Created	Indicates the date and time at which the group was created.

4.1.3.1. Updating the Details of a User

Administrators can update the username, email address and phone number of a user at any time through the user details interface. The interface also allows you to view devices that are associated with the user as well as send a password recovery email.

Note: The 'Edit' option is not available for users that were added via the C1 management portal. Those users must be edited in the C1 interface. All changes will be reflected in the ITSM interface.

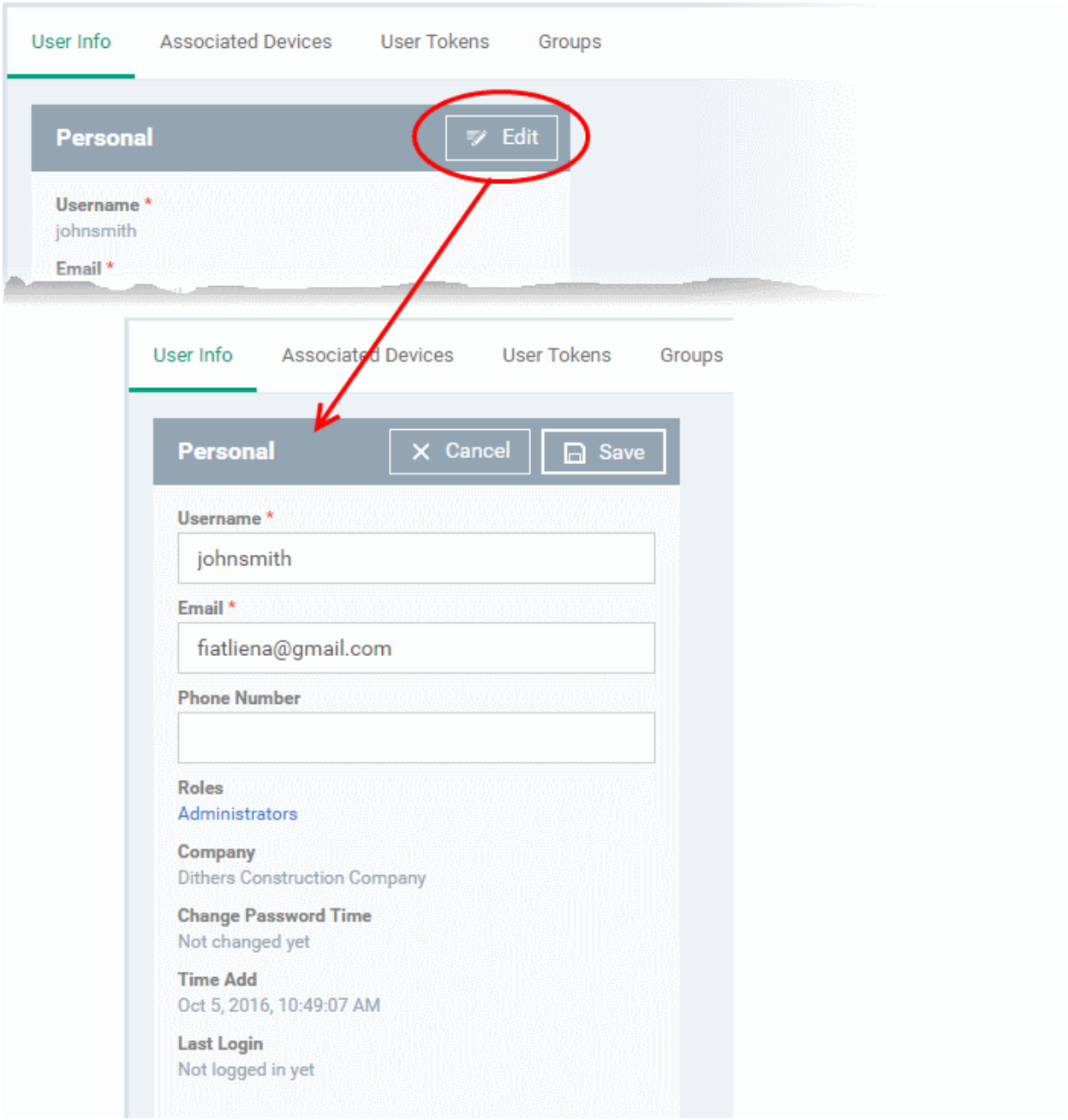
To update the details of a user

- Open the 'User List' interface by clicking 'Users' > 'User List'
- Click on the user whose details you want to update.

The user details screen will open.

- Click the 'User Info' link and then the 'Edit' button 

at the top right



Update User Form - Table of Parameters		
Form Element	**Type**	**Description**
Username	Text Field	Allows you to change the login username of the user.
Email	Text Field	Allows you to change the email address of the user.
Phone Number (Optional)	Text Field	Allows you to change the phone number of the user.

- Click 'Save' at the top for your changes to take effect

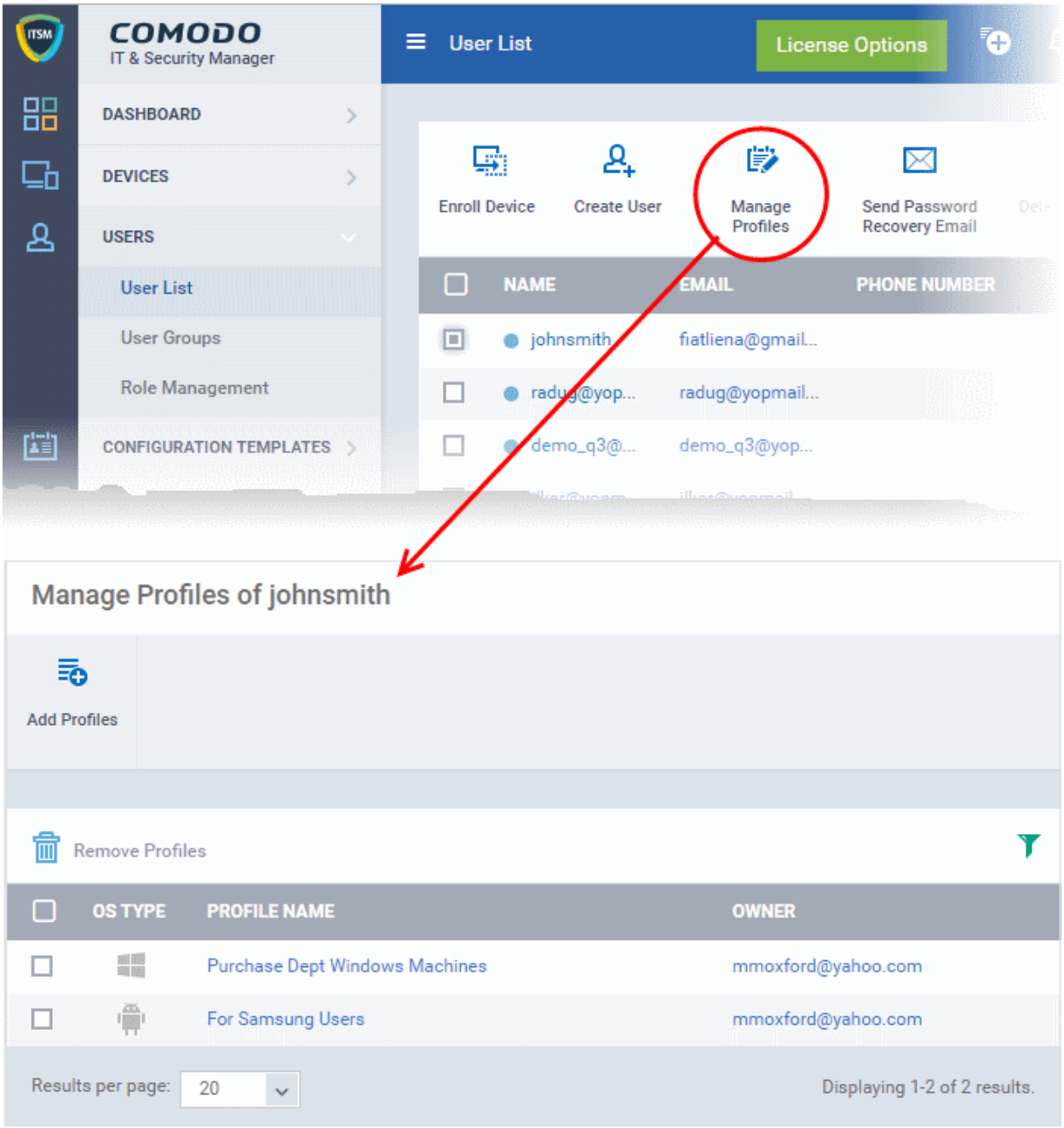
The role assigned to the user is displayed under 'Roles'. Clicking the role name allows you to change the role if required. Refer to the section '**Managing Roles Assigned to a User**' for more details.

4.1.4. Assigning Configuration Profile(s) to a Users' Devices

ITSM allows administrators to assign profile(s) to users which will be deployed on all devices associated with those users. Administrators can select profiles for multiple OS types for the same user and each profile will be applied to the appropriate device. This is useful if an organization prefers to roll out profiles to devices on a user basis.

To manage configuration profiles assigned to a user

- Click the 'Users' tab from the left and click 'User List'
- Select the user for whom you want to assign profile(s)



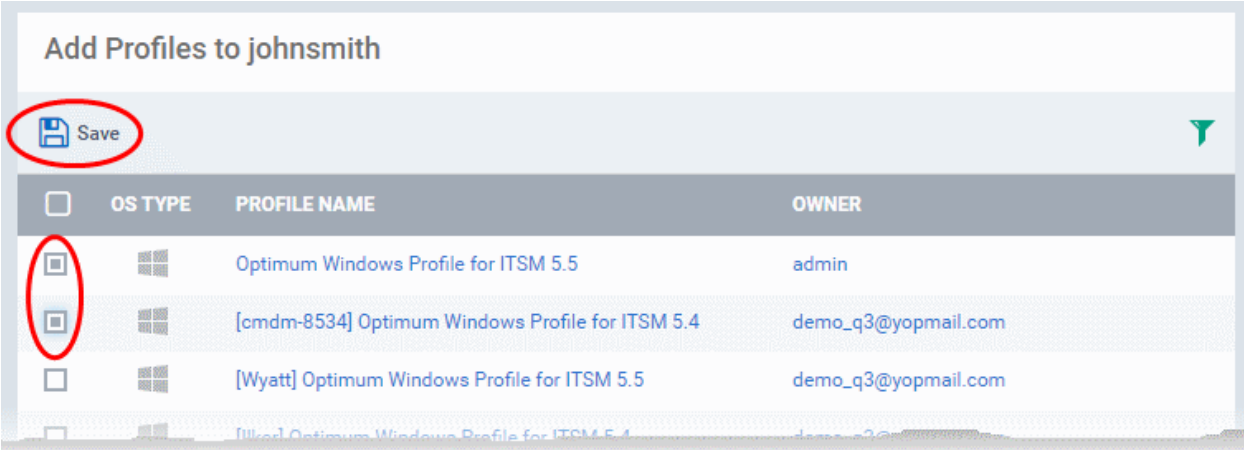
- Click 'Manage Profiles'.

The 'Manage Profiles For User' interface will open with a list of all configuration profiles associated with the user.

Tip: The 'Manage Profiles' interface for a user can also be opened from the 'User Details' interface (open the 'User List' interface, click a username then select 'Manage Profiles').

To add new profiles to the user

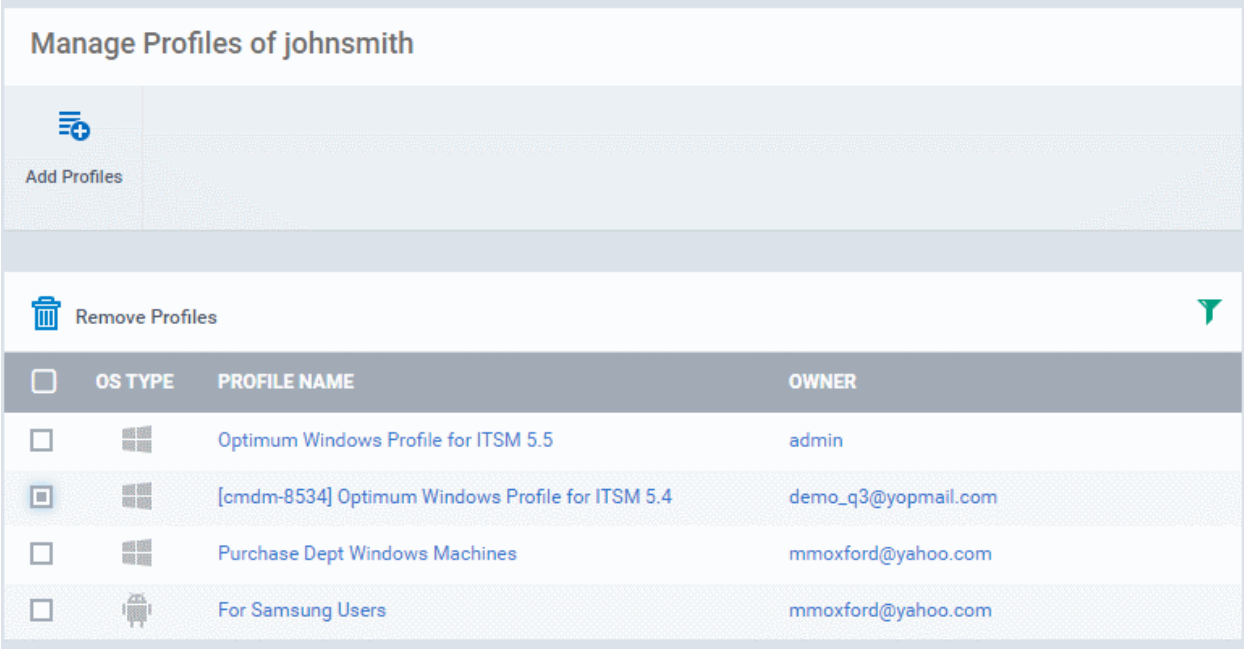
- Click 'Add Profiles'



The 'Add Profiles to User' interface will appear with a list of all the profiles available with ITSM excluding those already applied to the user.

- Click the funnel icon at the right to search for particular profile(s)
- Select the the profile(s) to be added and click 'Save'.

The selected profiles will be associated with the user and applied to all the devices enrolled for the user. Also, if any new device is enrolled for the user, the profiles will be applied by default.



To remove a profile

- Select the profile(s) from the 'Manage Profiles for User' interface and click 'Remove Profiles'.

The selected profile(s) will be removed.

4.1.5. Removing a User

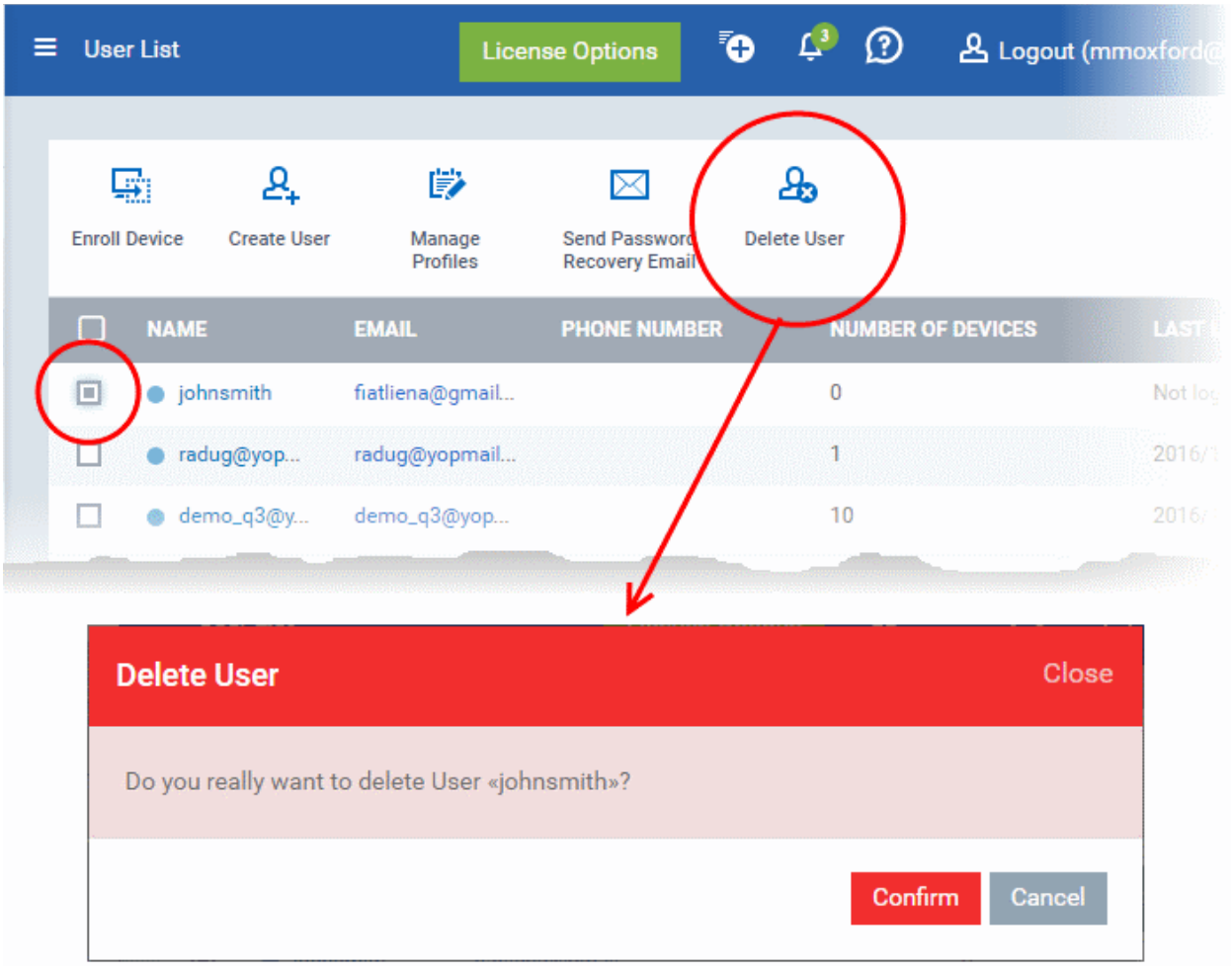
Administrators can remove users from the 'Users' interface if their device(s) no longer need to be managed by ITSM. Users that are assigned privileges to manage ITSM can also be removed if no longer required.

Note 1: Users added via the C1 management portal cannot be removed via the ITSM interface. They can be removed only from C1 and once removed they will be automatically deleted from the user list in ITSM.

Note 2: Users cannot be removed until their device(s) is/are managed by ITSM. Before removing a user, ensure all devices associated with him/her are removed from ITSM or reassigned to another user. Refer to the sections **Removing a Device** and **Changing Device's Owner** for more details.

To remove a user

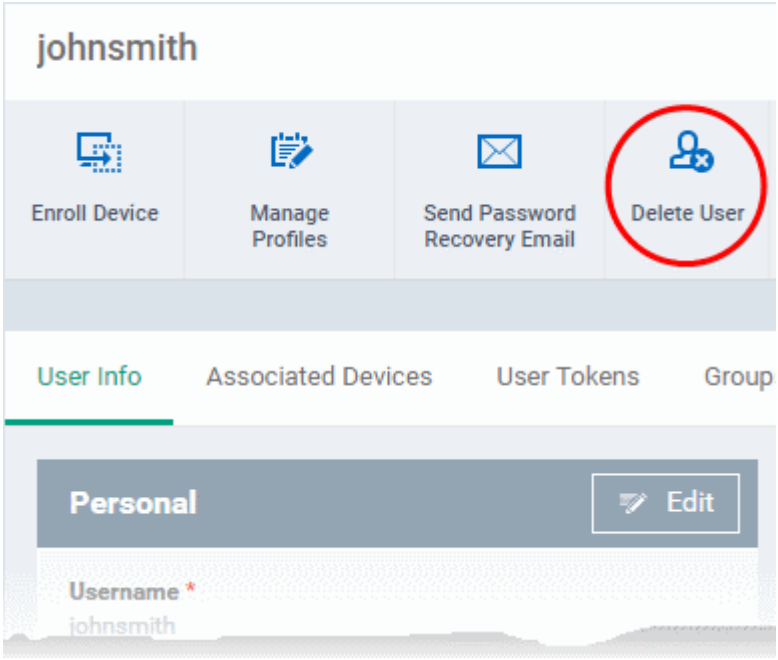
- Open 'User List' interface by clicking 'Users' > 'User List'
- Select the user to be removed and click 'Delete User'



- Alternatively, click on the name of the user to be removed.

The user details screen will open.

- Click 'Delete User' at the top



The user will be removed from ITSM.

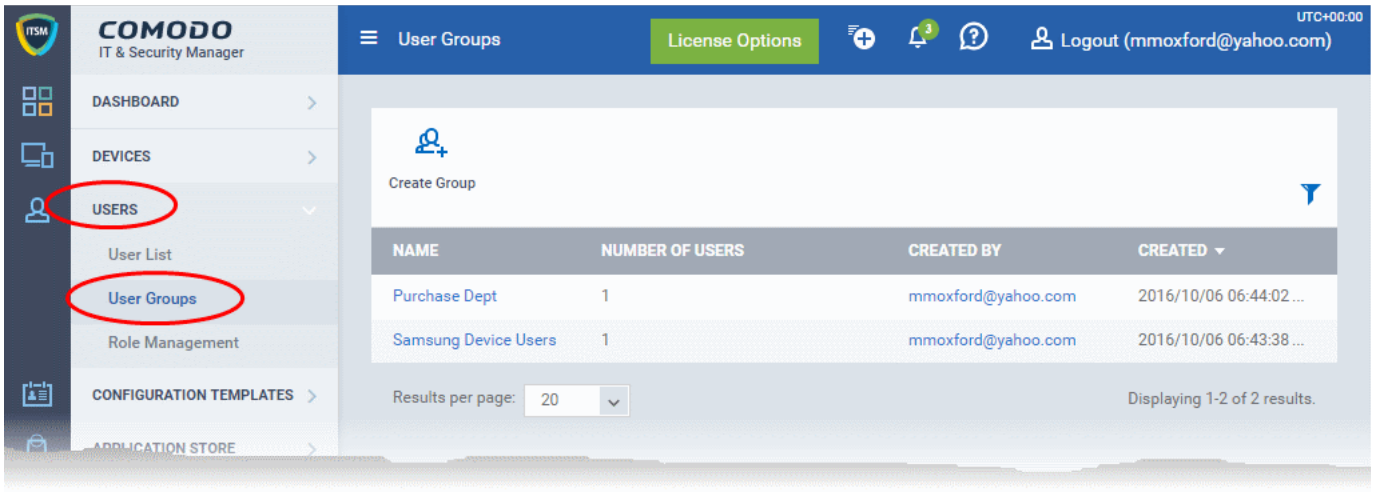
4.2. Managing User Groups

Comodo IT and Security Manager allows administrators to create logical groups of users for convenient management. For example, users can be grouped according to existing corporate units (such as 'Sales Dept.' or 'Accounts Dept.'), and/or by type of user.

Once created, dedicated configuration profiles can be applied to each user group as per administrator requirements. For more details on creating and managing configuration profiles, refer to the chapter Configuration Profiles.

The 'User Groups' interface lists all existing groups and allows you to create and edit groups, and assign configuration profiles to groups.

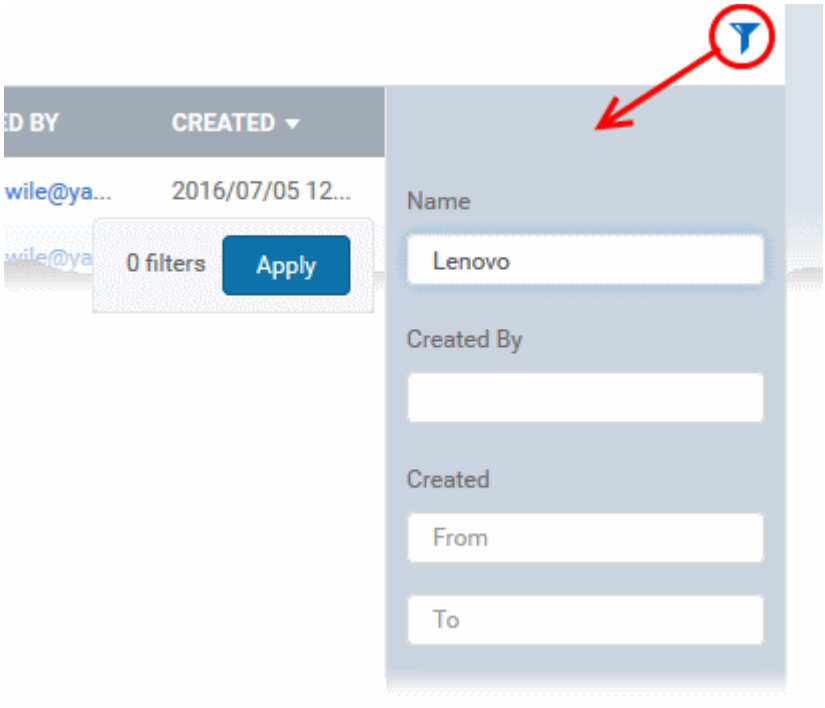
- To open the 'User Groups' interface, click the 'Users' tab from the left and choose 'User Groups' from the options.



User Groups - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the user group by the administrator. Clicking the name of a group will open the group details interface containing the list of users included in the group. The 'Group Details' interface allows you to add and manage users in the group. Refer to the section Editing a User Group for more details.
Number of Users	Displays the number of users currently in the group.
Created By	Indicates the administrator that created the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section Viewing the details of a User for more details.
Created	Indicates the date and time at which the group was created.

Sorting, Search and Filter Options

- Clicking on the column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific user based on group name and/or owner name , enter the search criteria in part or full in the respective field and click 'Apply'.
- To filter the user groups that have been created within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under 'Created' using the calendars that appear on clicking inside the respective field and click 'Apply'.

You can use any combination of filters at-a-time to search for a specific user group.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Refer to the following sections for more details about:

- Creating a New User Group
- Editing a User Group
- Assigning Configuration Profile(s) to a User Groups
- Removing a User Group

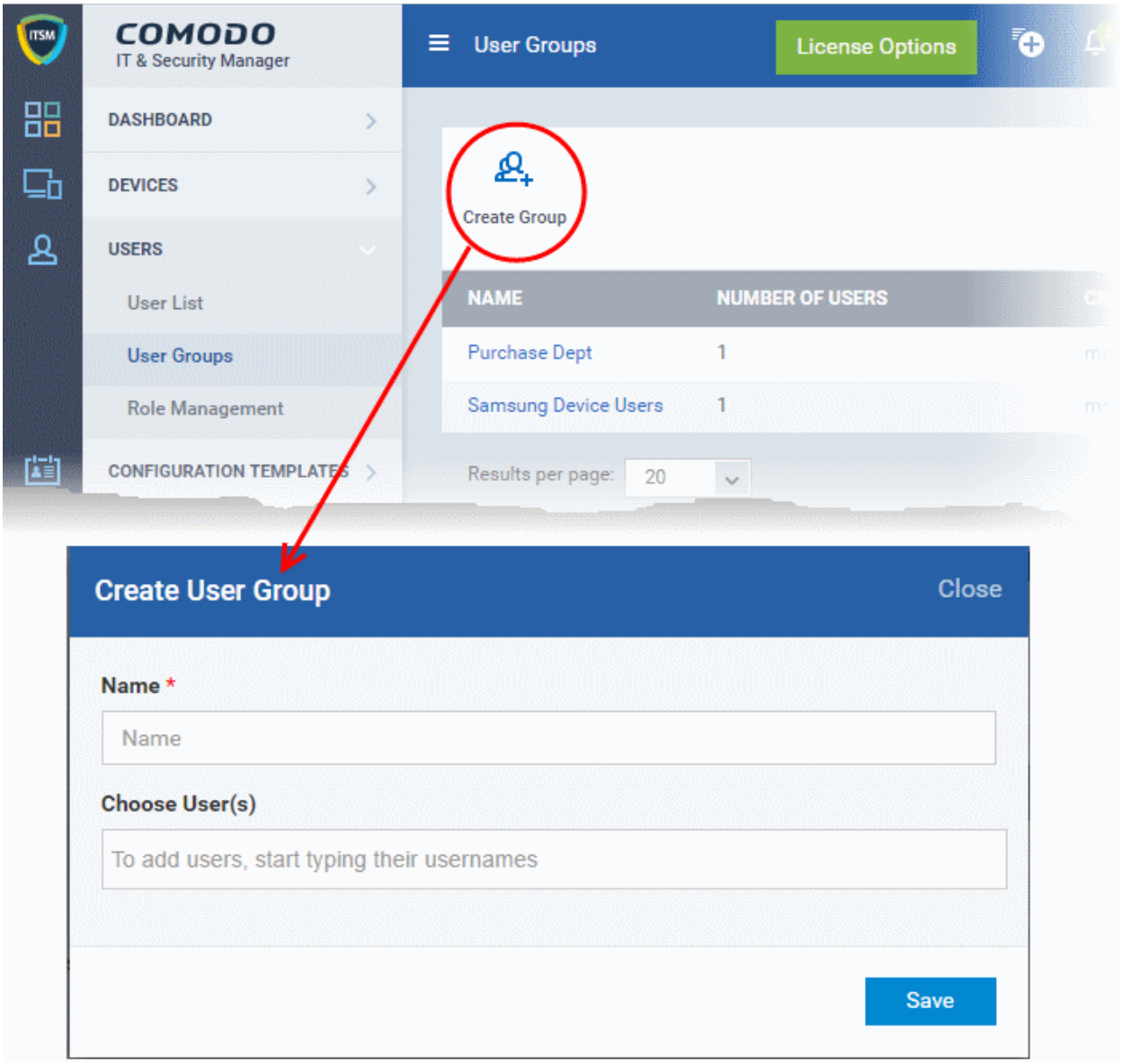
4.2.1. Creating a New User Group

The 'Create Group' button allows you to add and populate a new user group. Configuration profiles applied to the group will then be pushed to all devices owned by users in the group.

To create a new user group

- Open the 'User Groups' interface by clicking the 'Users' tab from the left and choosing 'User Groups' from the options.
- Click 'Create Group' above the table.

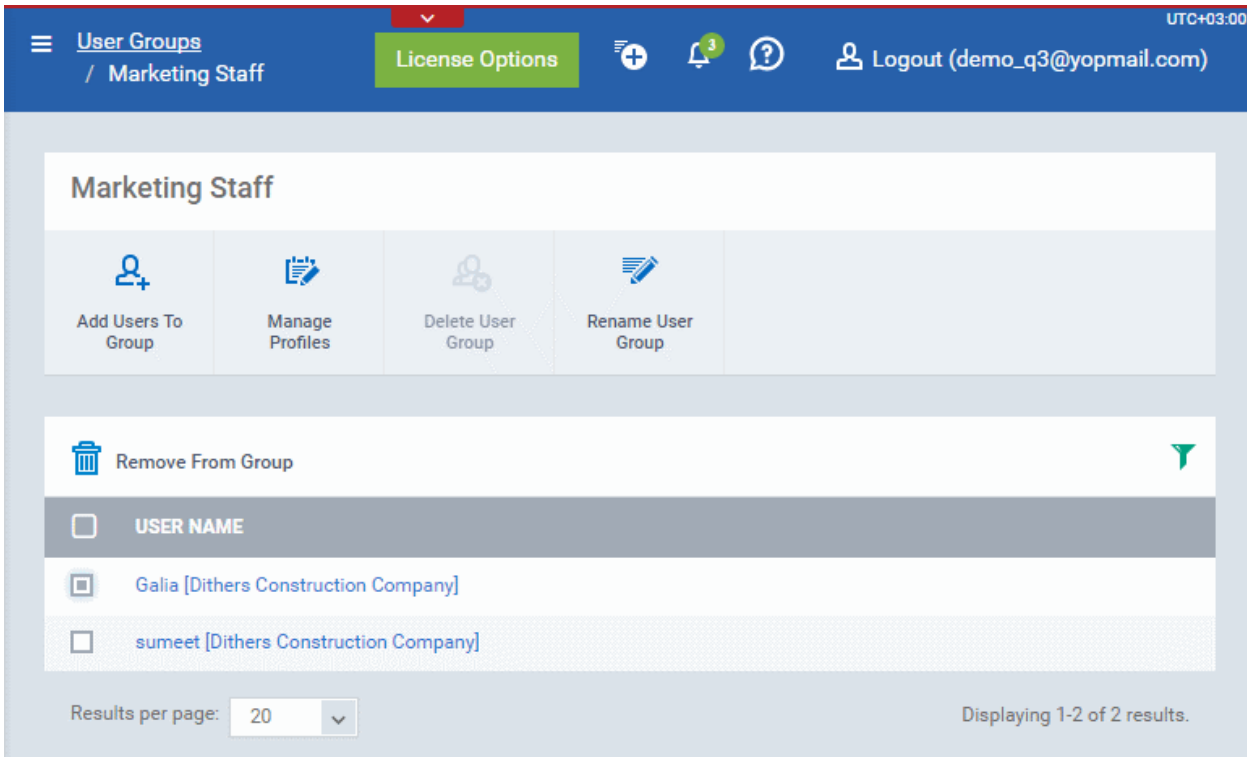
The 'Create User Group' dialog will open.



'Create User Group' dialog - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Allows you to enter a name shortly describing the group of users.
Choose User(s)	Text Field	Allows you to add the users to the group. To add a user, start typing the first few letters of the username and select the user from the predictions drop-down. Repeat the process for adding more number of users. • Note: You can add users at a later stage too. See the following section Editing a User Group for more details.

- Fill the details and click 'Save'.

The new group will be created and the group details screen will be displayed with the list of users in the group .



- Repeat the process to add more groups.

The users can be added to or removed from the groups at anytime. Refer to the section **Editing a User Group** for more details.

Appropriate configuration profiles can now be applied to the new user groups. Refer to **Assigning Configuration Policy to a User Group** for more details.

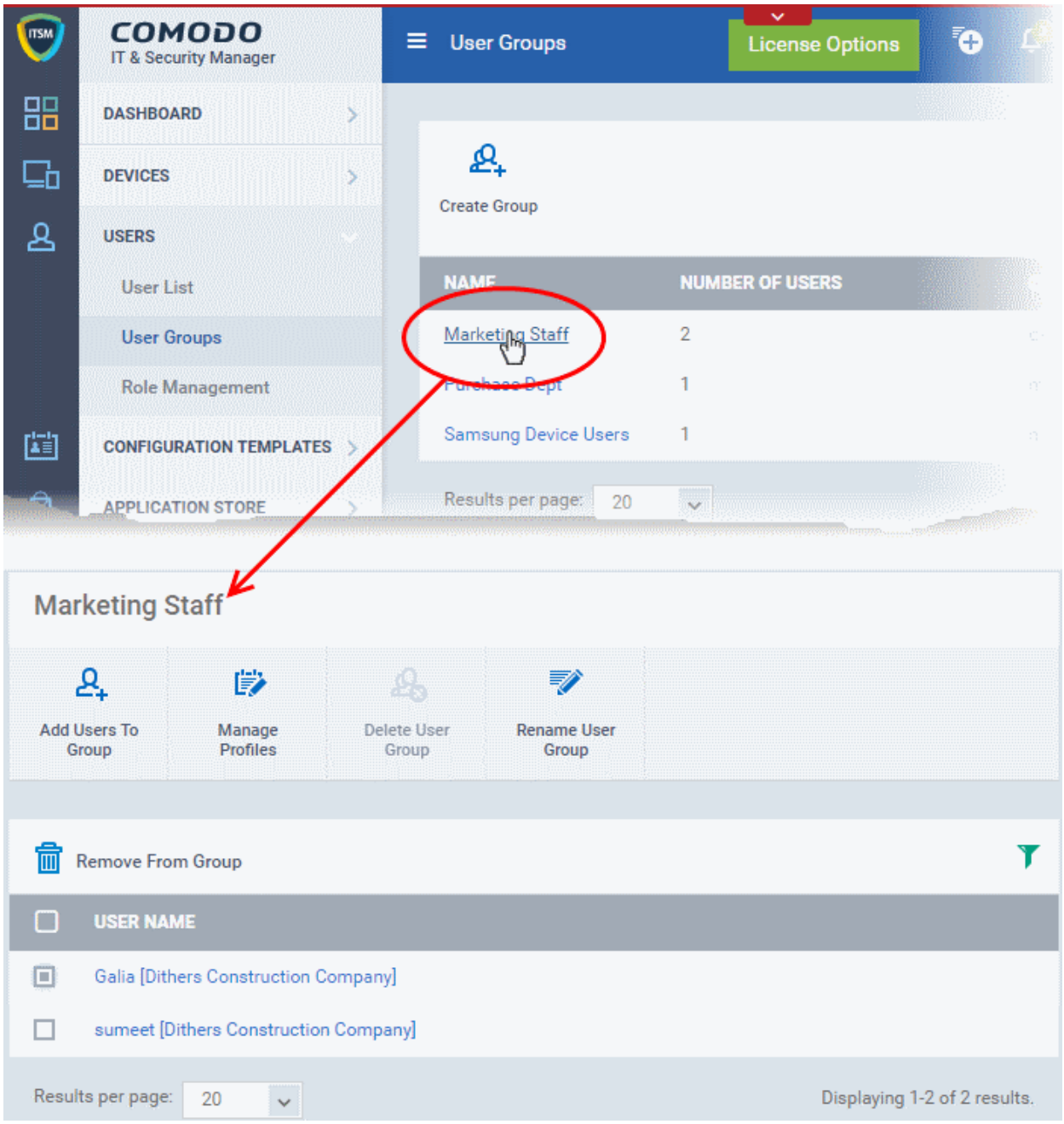
Note: A single user can be a member of more than one group. The configuration profiles applied to the all the groups to which a user is a member of, will be applied to the devices belonging to the user. In case the settings in a profile clashes with another profile, ITSM follows the 'Most Restricted' policy. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

4.2.2. Editing a User Group

The group detail interface allows administrators to view the group members, add or remove members, rename groups and delete groups.

To view and edit user groups

- Open the 'User Groups' interface by clicking the 'Users' tab from the left and choosing 'User Groups' from the options.
- Click on the group name to be edited.



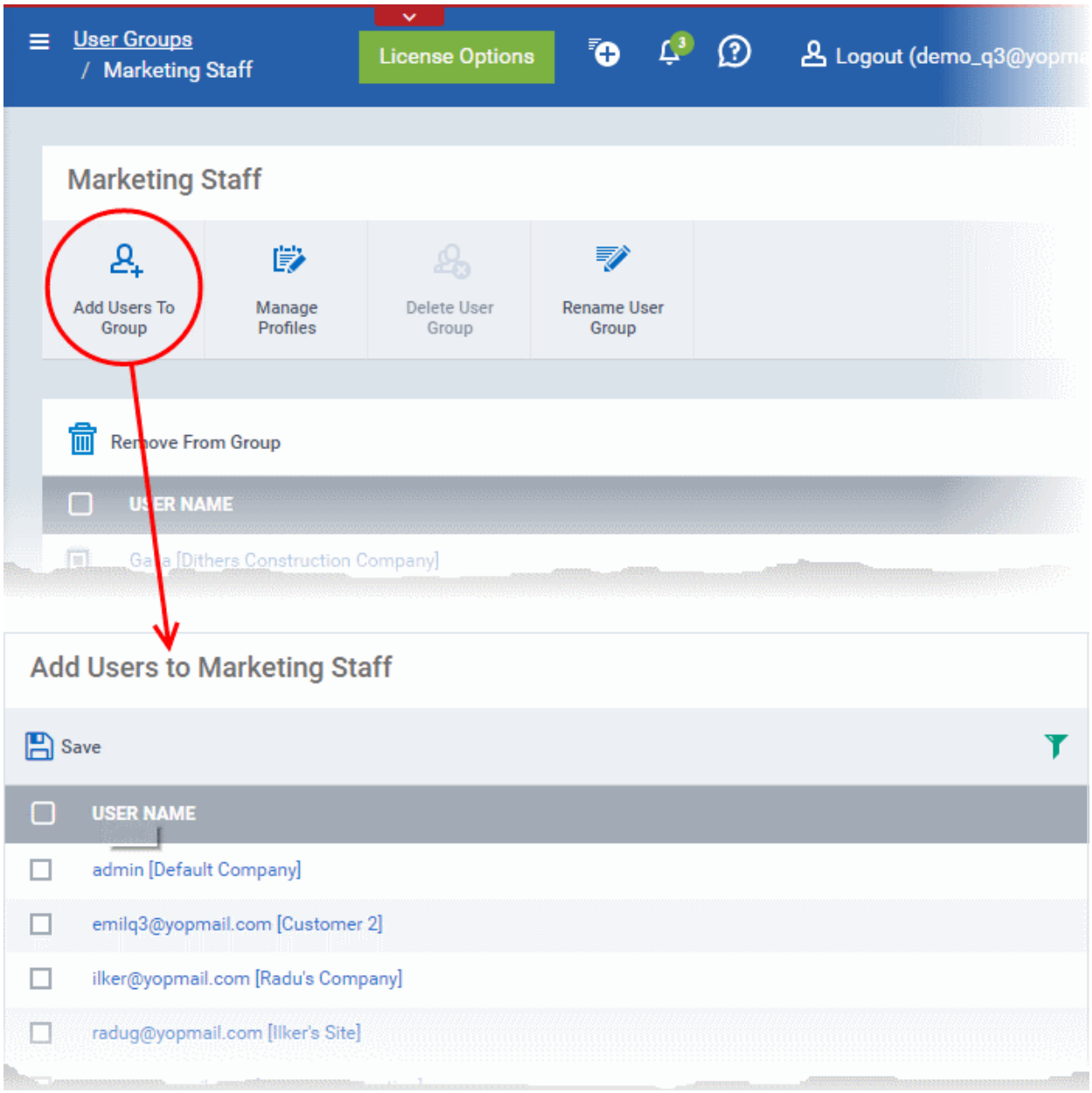
The user group details interface will open with the list of users in the group and allows you to:.

- Add new users to the group
- Remove users from the group
- Rename the group
- Assign Configuration profiles to the user group
- Remove the group

To add new user(s) to the group

- Click 'Add Users To Group'.

A list of all users enrolled to ITSM, excluding those in the group will be displayed.

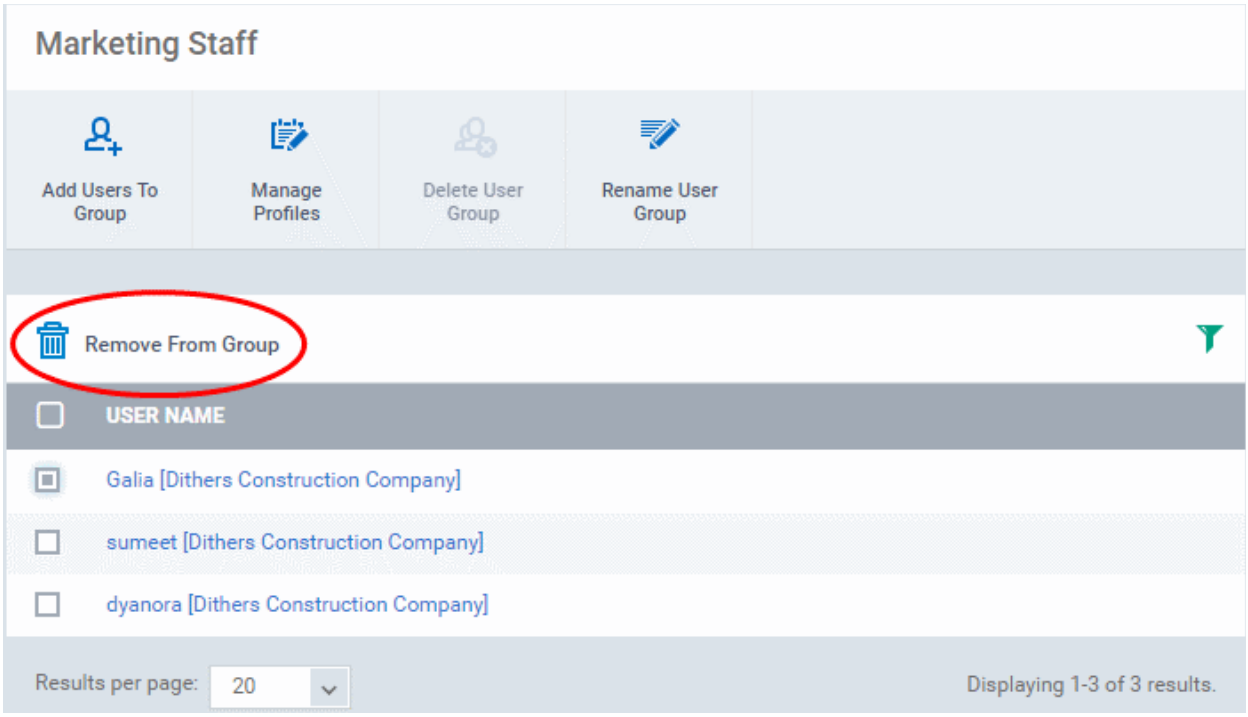


- Select the users to be added to the group and click 'Save'.

If a new user is imported into a group, the configuration profiles in effect on the group will be applied to the user's device(s).

To remove a user from the group

- Choose the user from the users in the 'Group Details' interface
- Click 'Remove from Group'

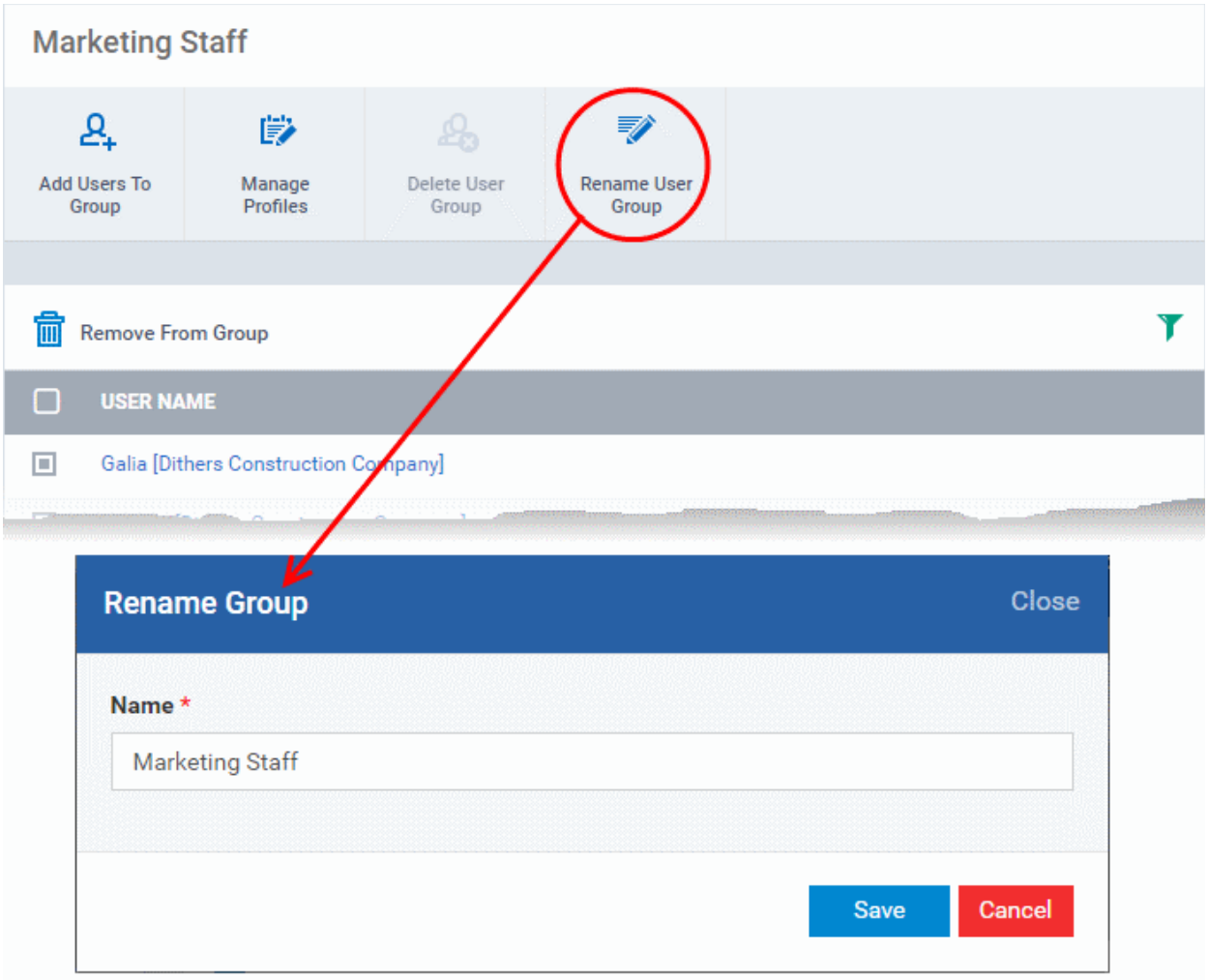


If a user is removed from a group, the profiles in effect on the user's device because of association with the group, will also be removed.

To rename a group

- Click 'Rename User Group' at the top

The 'Rename Group' dialog will open:



- Enter the new name for the group in the 'Name' text box and click 'Save'.

The group will be updated with the new name.

The group details interface also allows the administrator to apply configuration profiles to devices associated with all the users in a group at-once. Refer to the next section **Assigning Configuration Profiles to a User Group** for more details.

4.2.3. Assigning Configuration Profiles to a User Group

Administrators can view the configuration profiles currently applied to a user group and also apply new configuration profiles. The profiles will be applied instantly to all the devices belonging to all users in the group. This is particularly useful if organizations wants to roll out profiles to devices on user group basis. Administrators can select profiles for different operating systems and these will be applied to the respective devices.

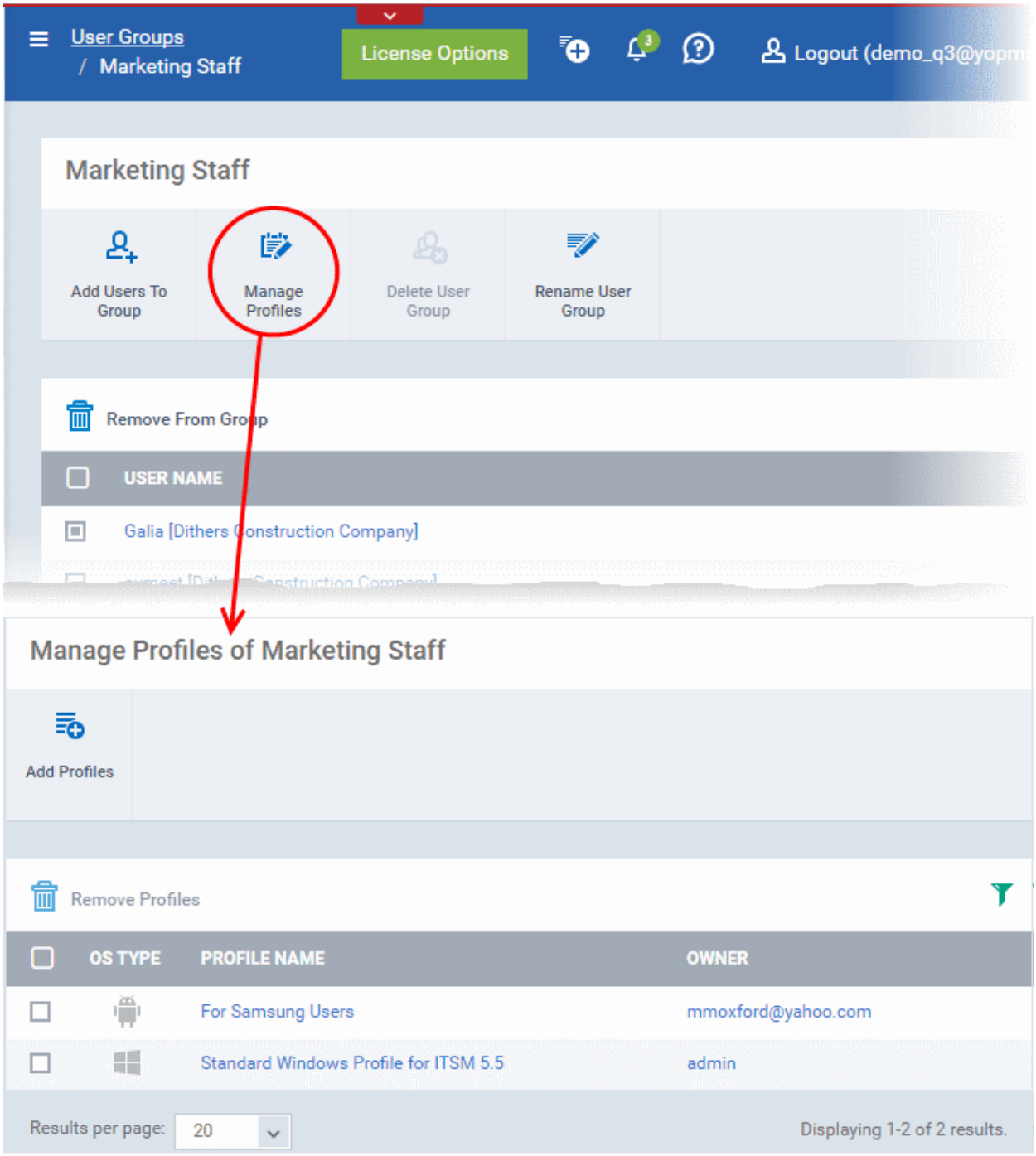
For more details on profiles, refer to the chapter **Configuration Profiles**.

To view and manage the profiles applied to a group

- Open the 'User Groups' interface by clicking the 'Users' tab from the left and choose 'User Groups'.
- Click on the name of the group whose profile you wish to manage.

The group details interface will be displayed, listing all users in the group.

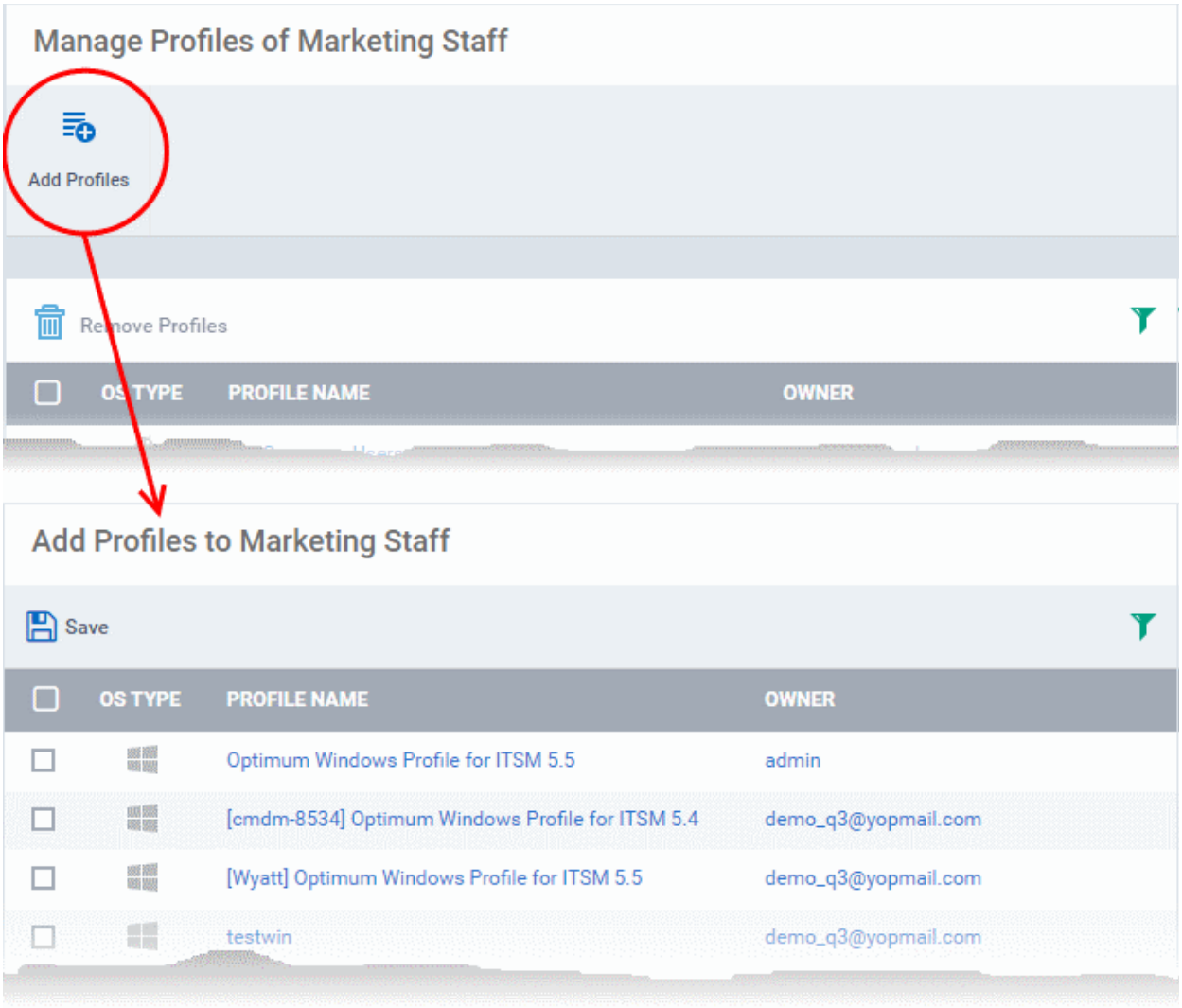
- Click 'Manage Profiles' at the top.



The 'Manage Profiles For User Group' interface will open displaying the profiles associated with the group.

To add a new profile

- Click 'Add Profiles'



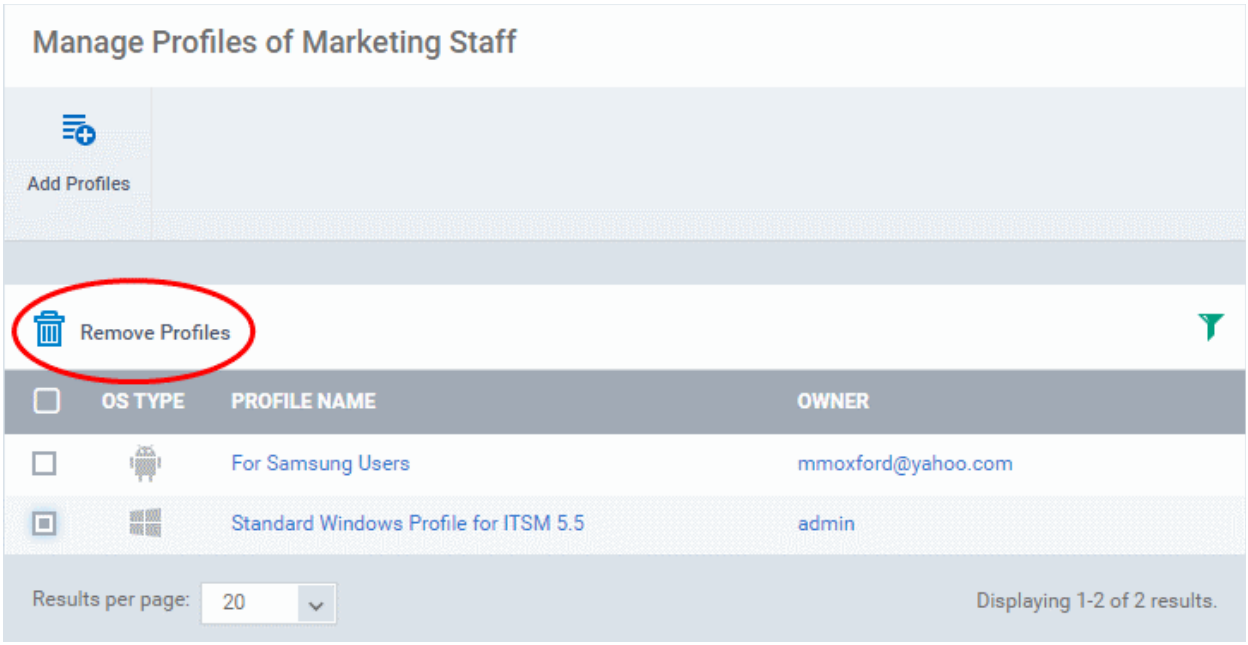
A list of all configuration profiles, available in ITSM, excluding those already applied to the group will be displayed.

- Select the profiles to be applied to the users in the group and click 'Save'.

The profile will be associated with the group and applied to all the devices used by the members in the group.

To remove a profile from a group

- Select the profile from the 'Manage Profiles' interface and click 'Remove Profiles'



The profile(s) will be removed from all the devices belonging to the members of the group.

4.2.4. Removing a User Group

Administrators can remove unwanted user group(s) in ITSM. Doing so will remove the group but will not delete the users from ITSM. However, any profile(s) associated with the group will be removed from the devices of group members.

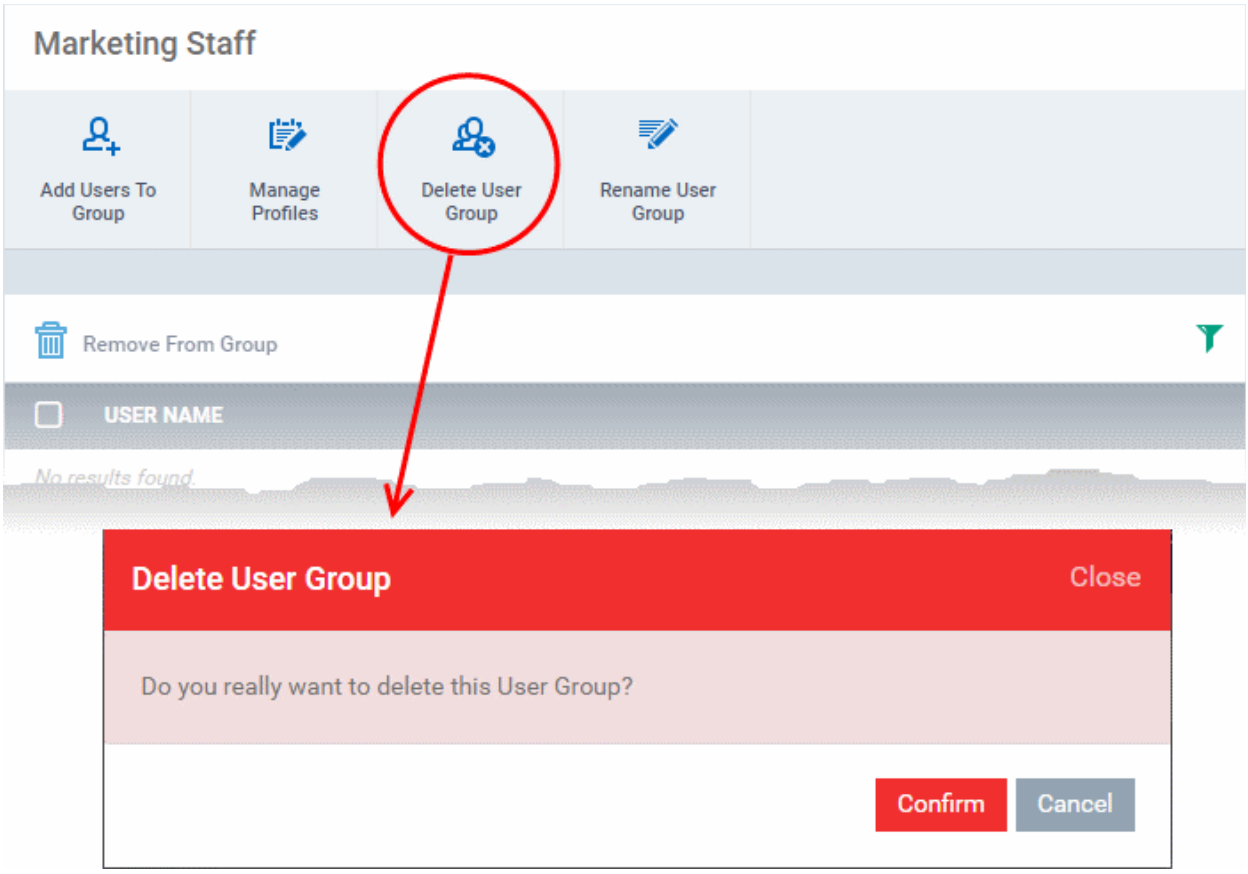
Note: Only Groups that do not contain any members in it can be removed. Ensure that all users are removed from the group before removing it. Refer to the explanation of removing users from a group in the section Editing a User Group for more details.

To remove a user group

- Open the 'User Groups' interface by clicking the 'Users' tab from the left and choosing 'User Groups' from the options.
- Click on the name of the group to be removed.

The group details interface will be displayed with the list of users in the group.

- Click 'Delete User Group' at the top.



- Click 'Confirm' in the confirmation dialog. The user group will be removed from ITSM.

4.3. Configuring Role Based Access Control for Users

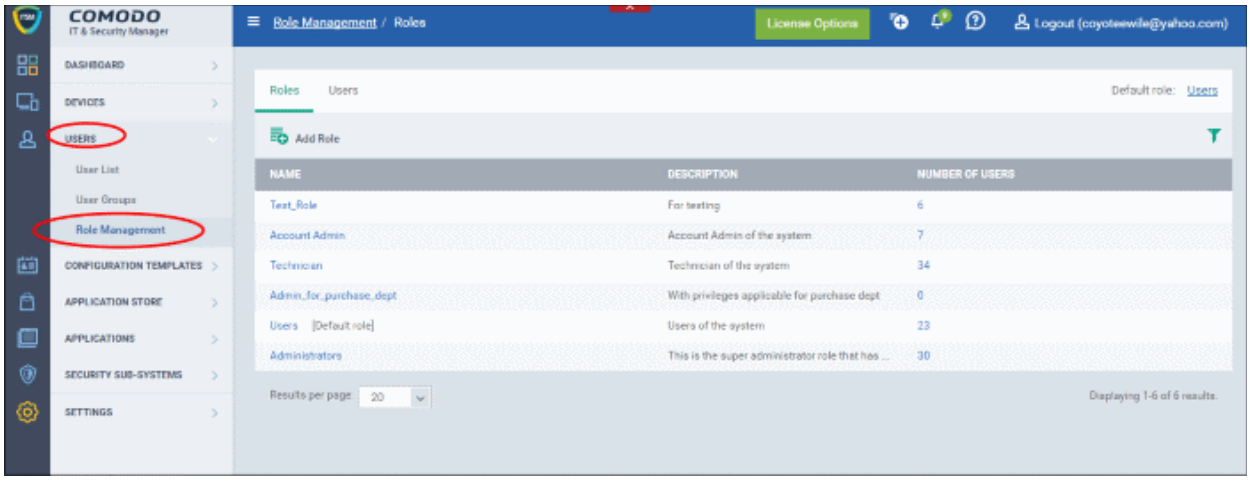
The privileges of users added to ITSM via C1 or via ITSM depends on the roles assigned to them. Administrators can create different roles with different access privileges and assign them to enrolled users as required. A single user can be assigned any number of roles.

Note. All staff created in the C1 interface will be available for selection in all roles, and for all companies in the account. This allows you to assign different roles to the same staff member for different companies.

- To open the 'Role Management' interface, click 'Users' > 'Role Management'.

There are two tabs:

- Roles - allows you to view and edit each role's permissions. You can also create custom roles here.
- Users - allows you to view users and assign them to roles



Roles

The 'Roles' interface allows administrators to create roles with differing access rights and privileges for users and staff. ITSM ships with four roles, Account Admin, Administrators, Technician and Users. While the role permissions for Account Admin are non editable, the other three built-in roles can be modified. You can also create custom roles according to your requirements.

Custom roles and built-in roles will be available for selection while adding a new user. Administrators can add or remove roles at any time. When a new user is created in ITSM, the default role assigned to them is 'User'. However, you have the option to make any role the default. Likewise, you can change the role of any user at any time.

Roles - Column Descriptions	
Column Heading	**Description**
Name	The name of the role. Clicking on the name will open the 'Role Management > Permissions screen, allowing you to view and manage the permissions assigned to the role. 'Managing Permissions and Assigned Users of a Role' for more details.
Description	The short description of the role.
Number of Users	Displays the number of users to whom the role is assigned. Click the number to open the 'Assign Users' screen, which allows you to assign the role to new users / remove the role from users. Refer to the section 'Viewing users assigned to a role' for more details.

- Click a column header to sort the table according to the items in the column.
- Click the funnel on the right to implement more filters.

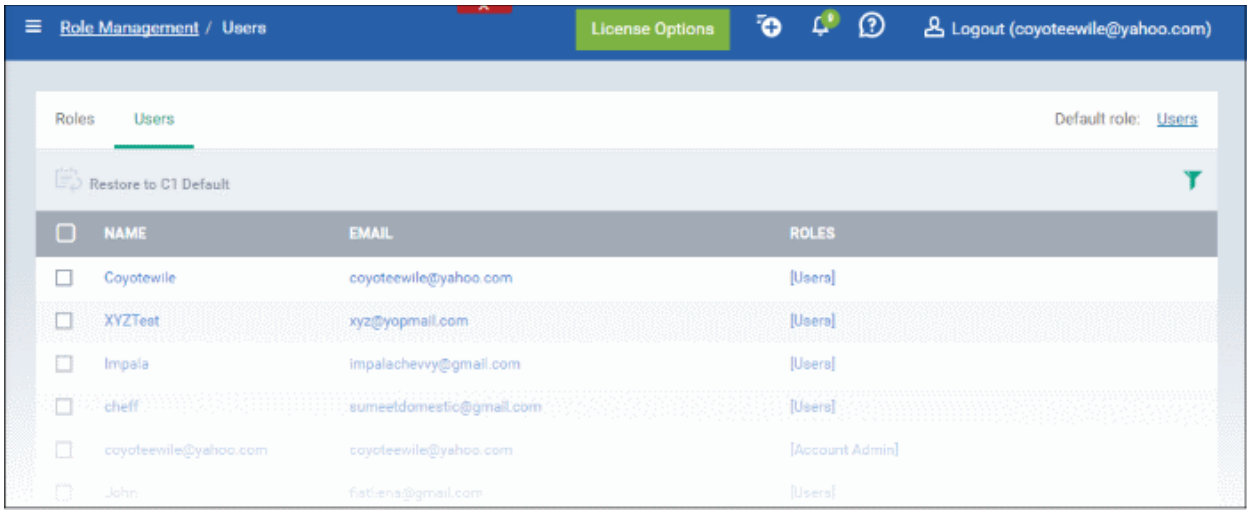
The roles interface allows admins to:

- Create a new role
- Manage Roles
  - Edit a role name and description of a role
  - Manage the permissions assigned to a role
  - Manage the users assigned with a role
- Remove a Role

Users

The 'Users' interface allows administrators to view the list of users added to ITSM and the roles assigned to them. The administrator can also edit the roles assigned to each user from this interface.

- To switch to the 'Users' interface, click on the 'Users' tab.



Users - Column Descriptions	
Column Heading	**Description**
Name	The login username of the user. Clicking a username will open the 'Users' screen, allowing you to assign new roles to a user or to remove existing roles. Refer to the section Managing Roles assigned to a User for more details.
Email	The registered email address of the user.
Roles	The roles assigned to the user. Clicking on a role opens the permissions of the role. Refer to the section 'Managing Permissions and Assigned Users of a Role' for more details.

- Click a column header to sort the table according to the items in the column.
- Click the funnel on the right to implement more filters.

The Users interface allows administrators to:

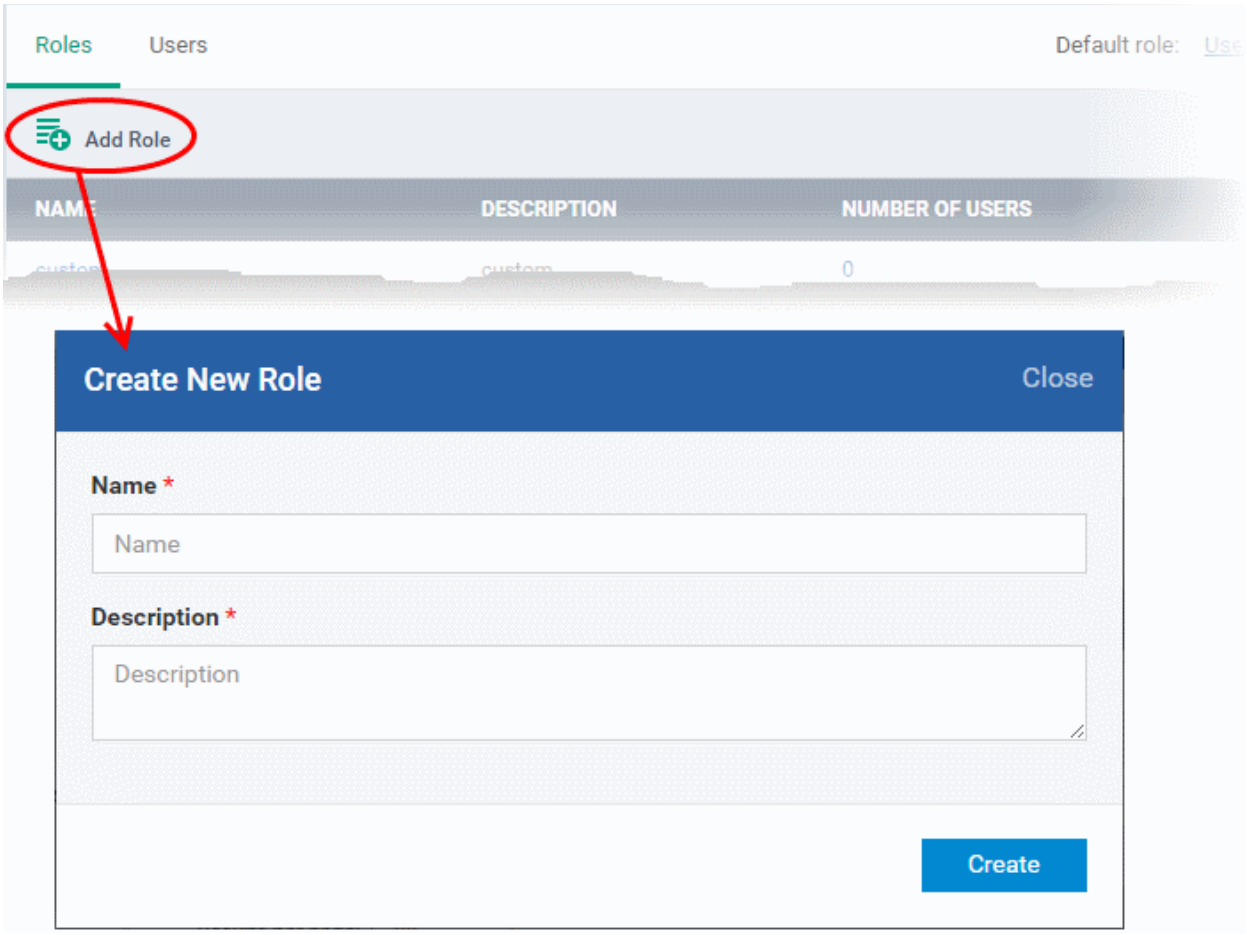
- Managing Roles Assigned to a User

4.3.1. Creating a New Role

Administrators can create roles featuring different permissions for staff and users.

To create a new role

- Click 'Users' on the left and select 'Role Management'.
- Click the 'Roles' tab.
- Click 'Add Role' above the table.

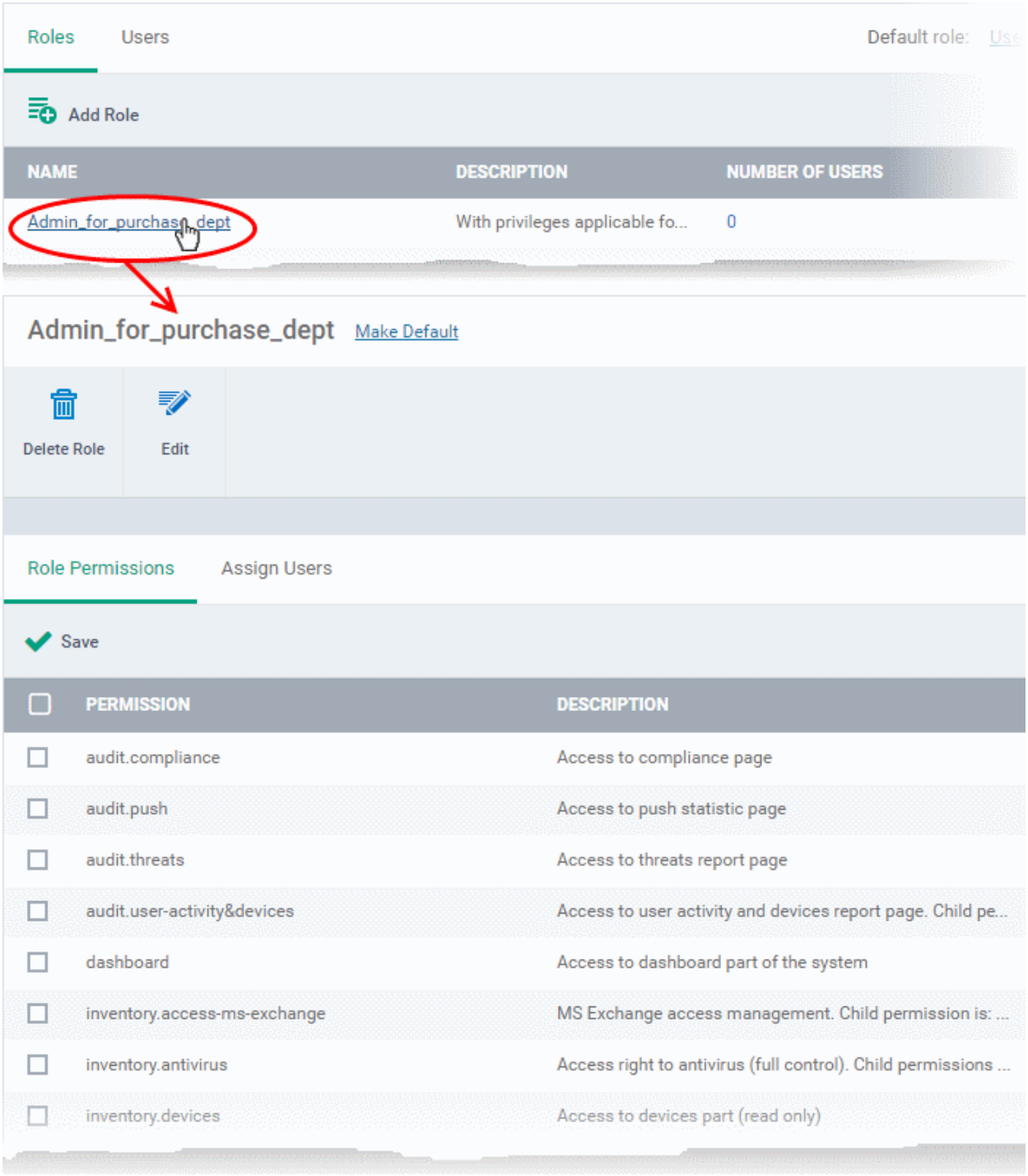


The 'Create New Role' wizard will start.

- Specify a name for the role in the 'Name' text box.
- Enter a short description for the role in the 'Description' box.
- Click 'Create'.

The new role will be created and listed in the 'Roles' screen. The next step is to define the privileges for the role.

- Click on the new role to open its permissions:



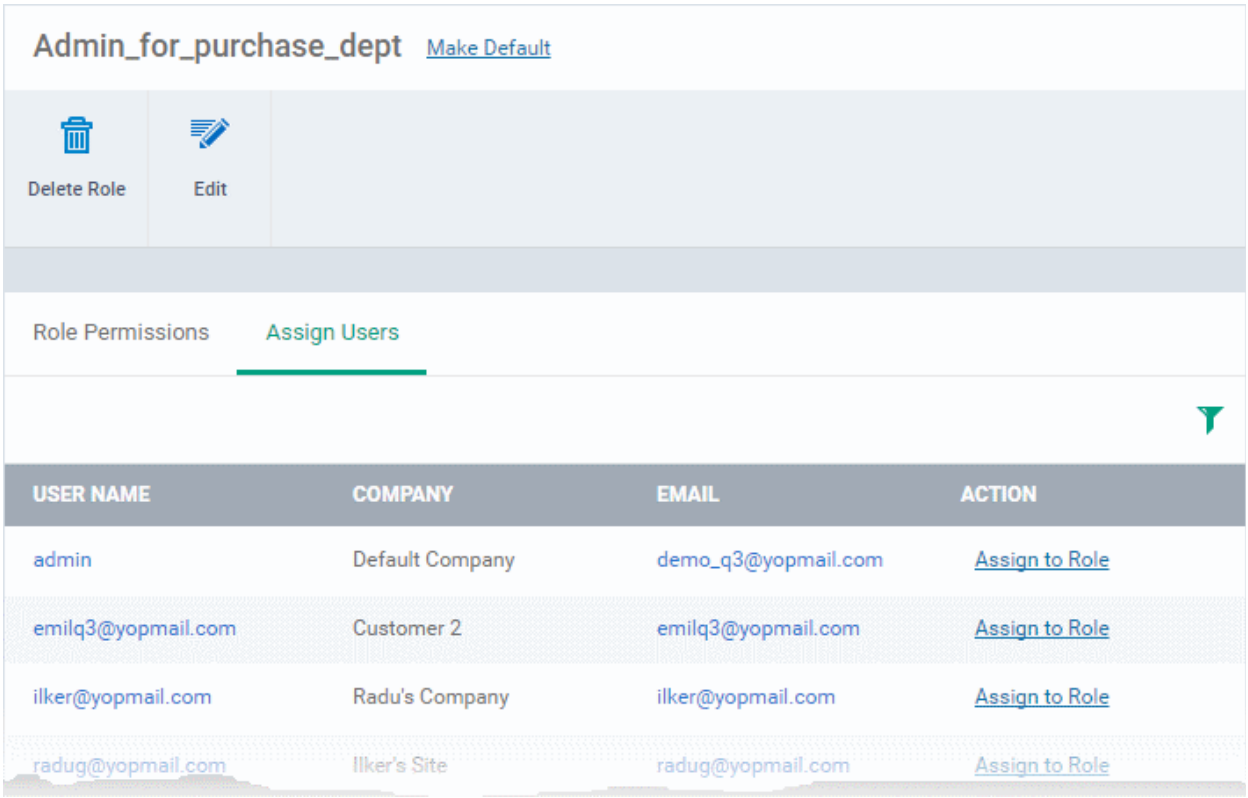
- Select the permissions you wish to assign to the new role
- Click the edit button Edit to modify the role's name and description. Please note that you cannot modify the built-in roles, Account Admin, Administrators and Technician.
- Click 'Make Default' if you want this to be the role that is initially assigned to new users. Please note 'Account Admin' role cannot be made as a default role.
- Click 'Save' for your changes to take effect.

You can assign the new role to users by clicking the 'Assign Users' tab.

To assign the new role to selected users

- Click the 'Assign Users' tab.

This will open a list of all users enrolled in ITSM so far.



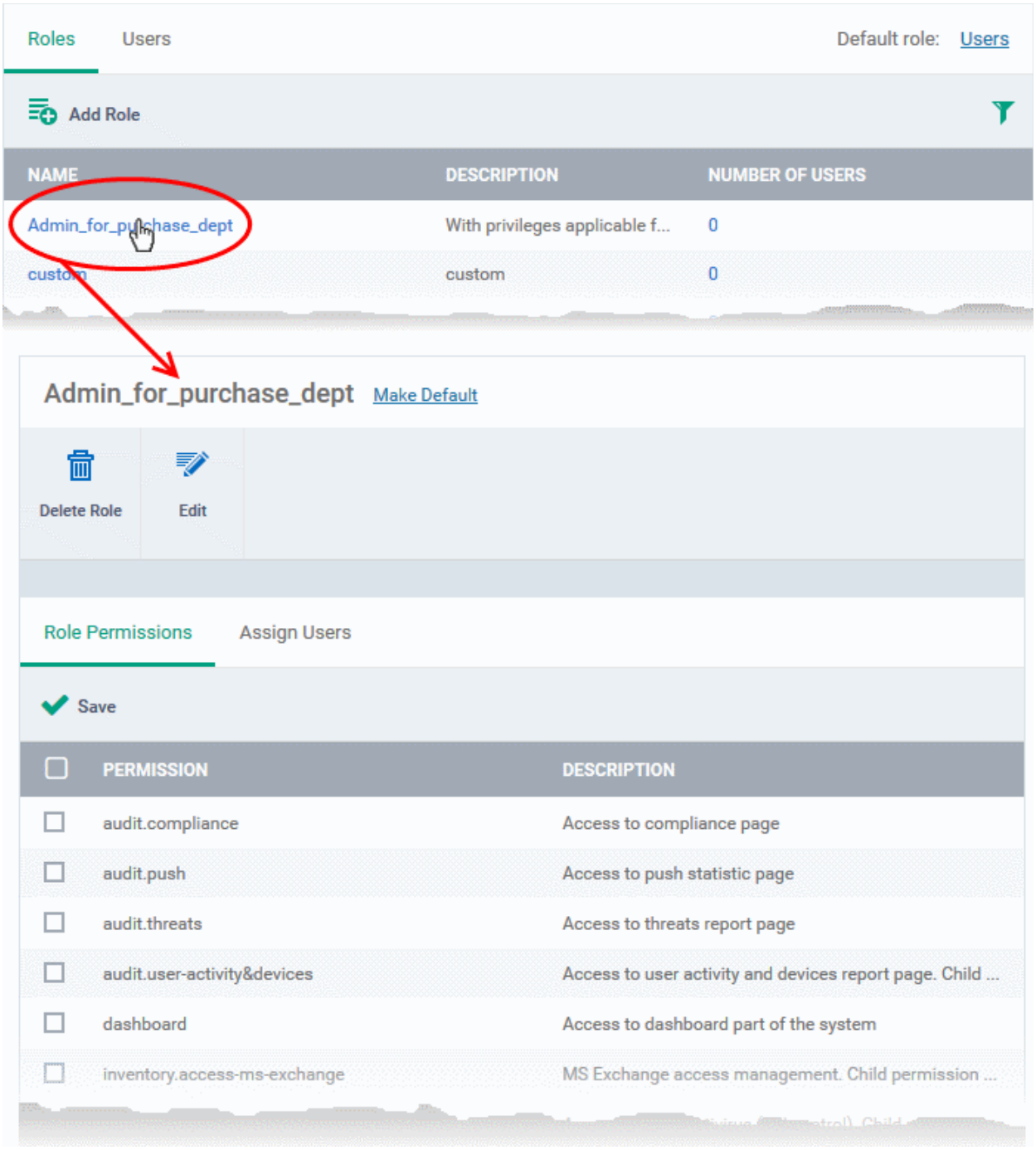
- To assign the role to a user, click the 'Assign to Role' link under the 'Action' column.
- Repeat the process to assign the role to other users
- To remove the role from a user, click the 'Remove from Role' link in the 'Action' column

4.3.2. Managing Permissions and Assigned Users of a Role

Administrators can view and modify any ITSM role from the 'Roles' interface.

To view and manage a role

- Click 'Users' on the left and select 'Role Management'.
- Click the 'Roles' tab.
- Click the 'Role' name to view the details of the role

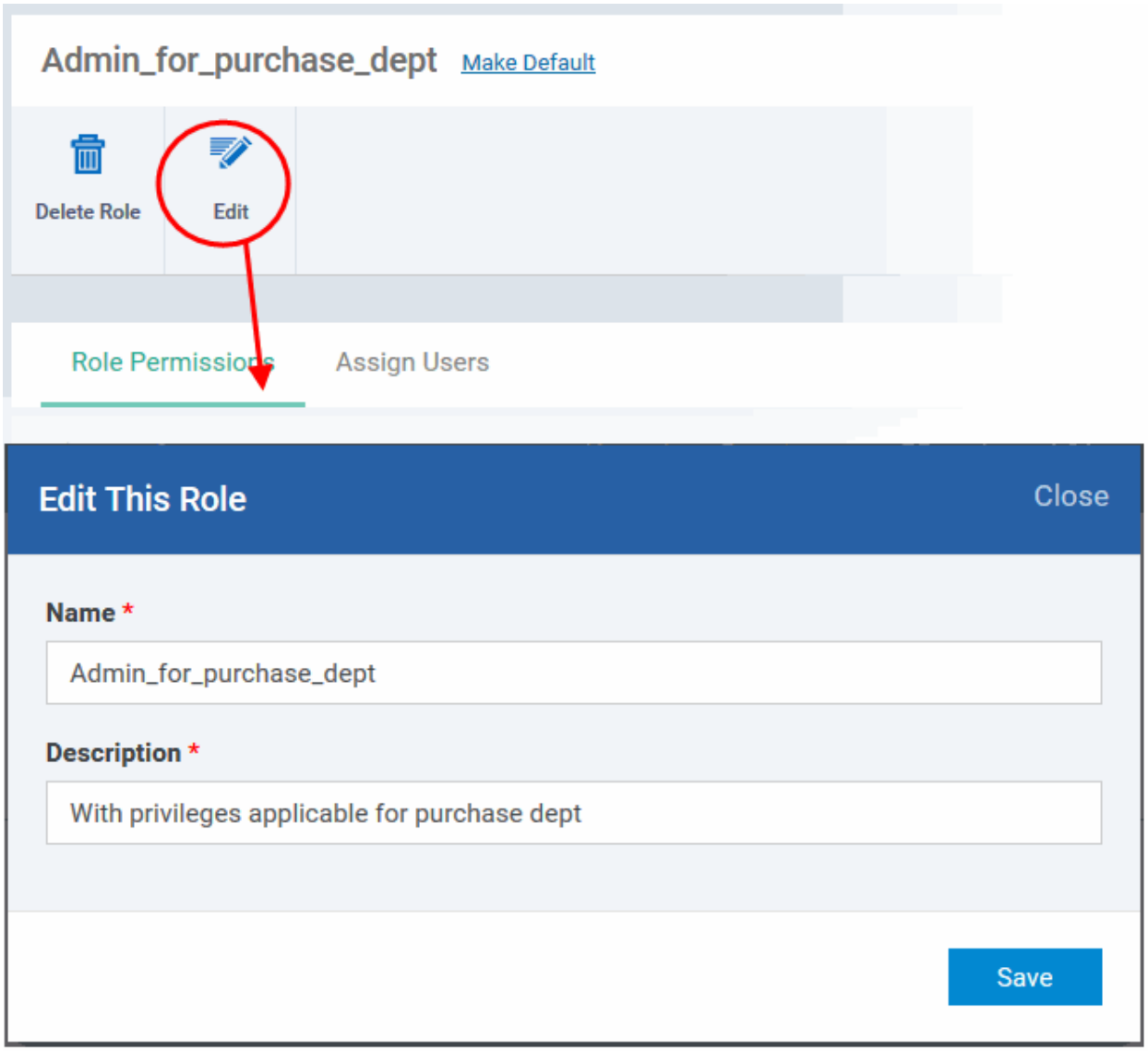


The 'Role Management' interface allows you to:

- Edit the name and description of a role
- Manage the permissions assigned to a role
- View users assigned to a role
- Assign / remove a role to / from users
- Set a role as the default role

To edit the name and description of the role

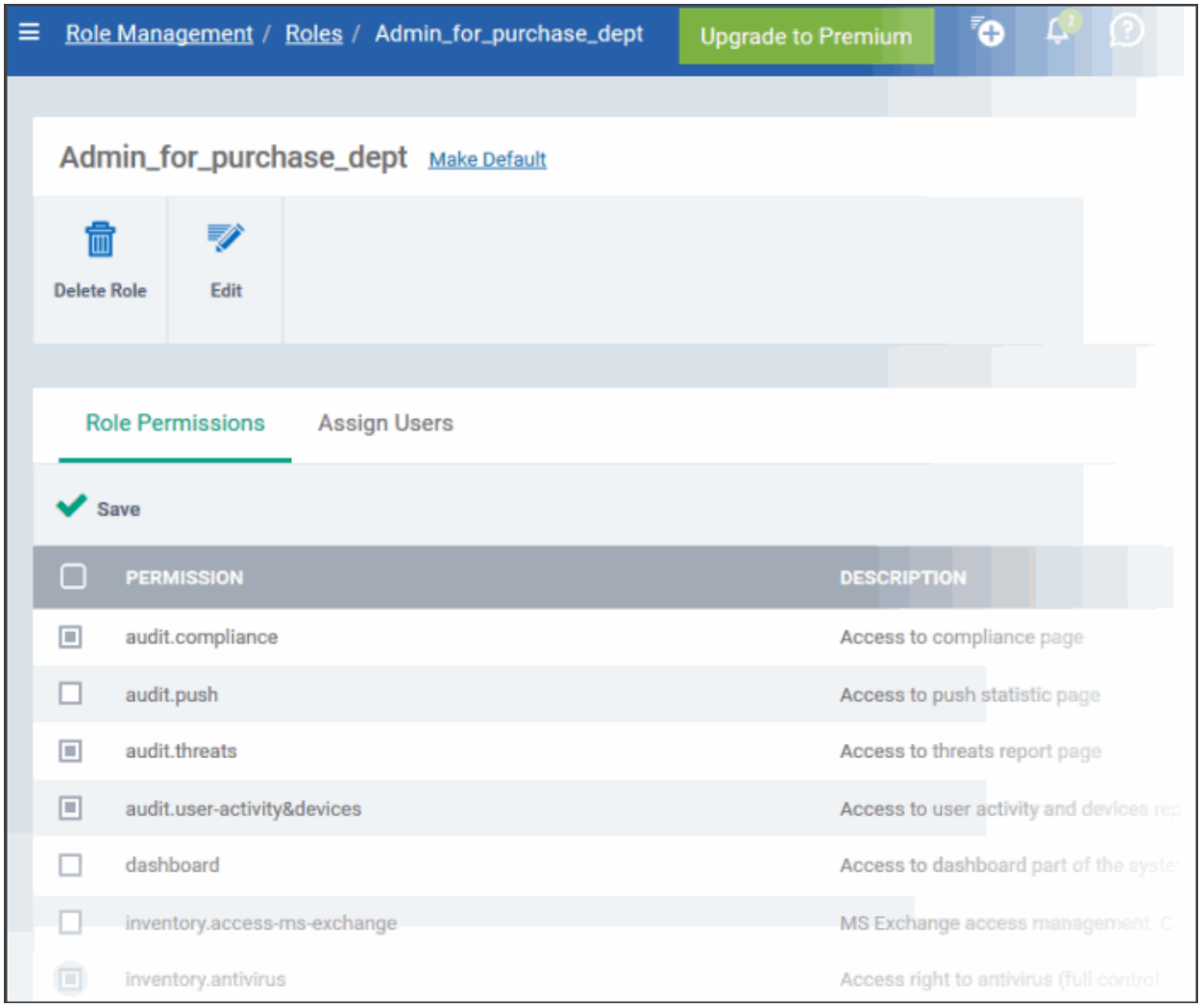
- Click the 'Edit' button Edit at the top



- Click 'Save' for your changes to take effect.

To manage the permissions assigned to a role

- Click the name of the role to open the 'Role Management' interface
- Click the 'Role Permissions' tab

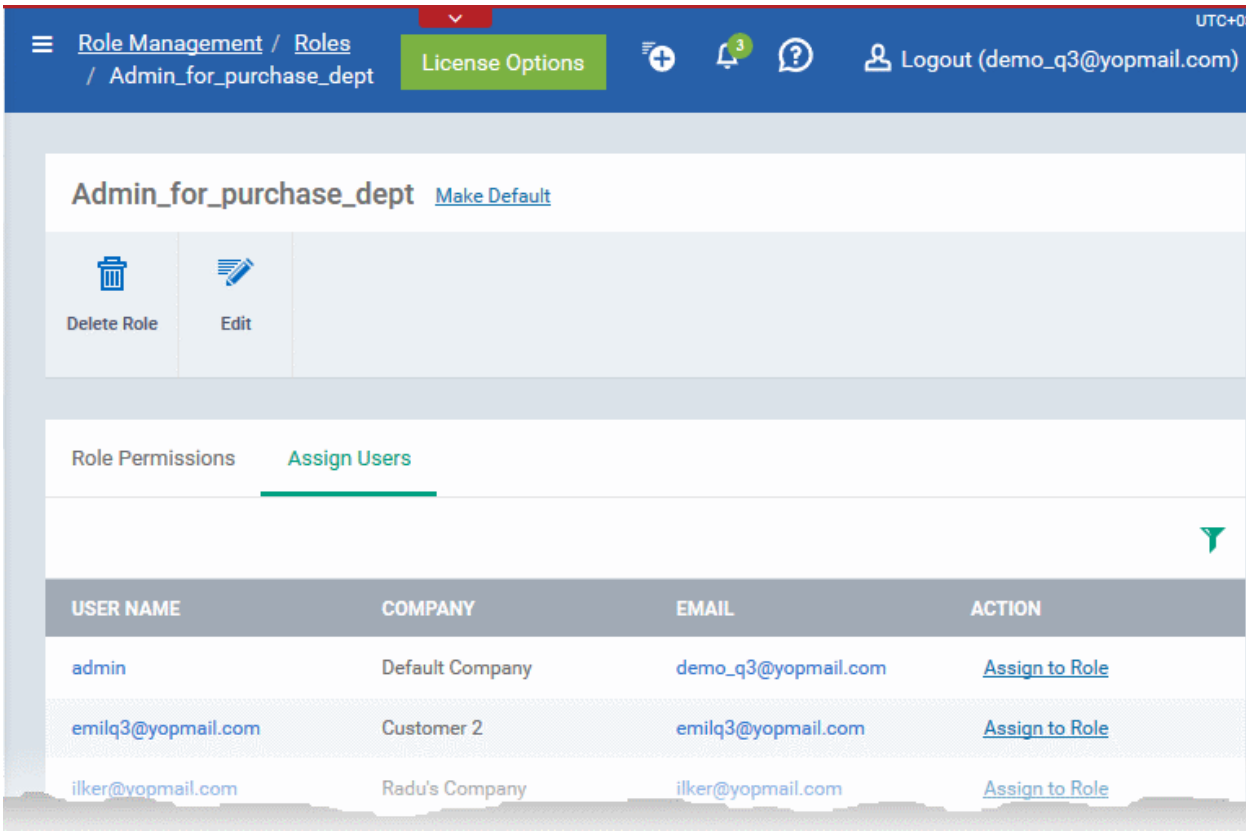


- Select the new permissions to be assigned to the role.
- Deselect the permissions to be removed from the role.

- Click 'Save' for your changes to take effect.

To view users assigned to a role

- Click on the name of a role to open the 'Role Management' interface
- Click the 'Assign Users' tab



The links in the 'Action' column indicate which users are assigned the role.

- To assign the role to a user, click 'Assign to Role'
- To remove the role from an assigned user, click 'Remove from Role'

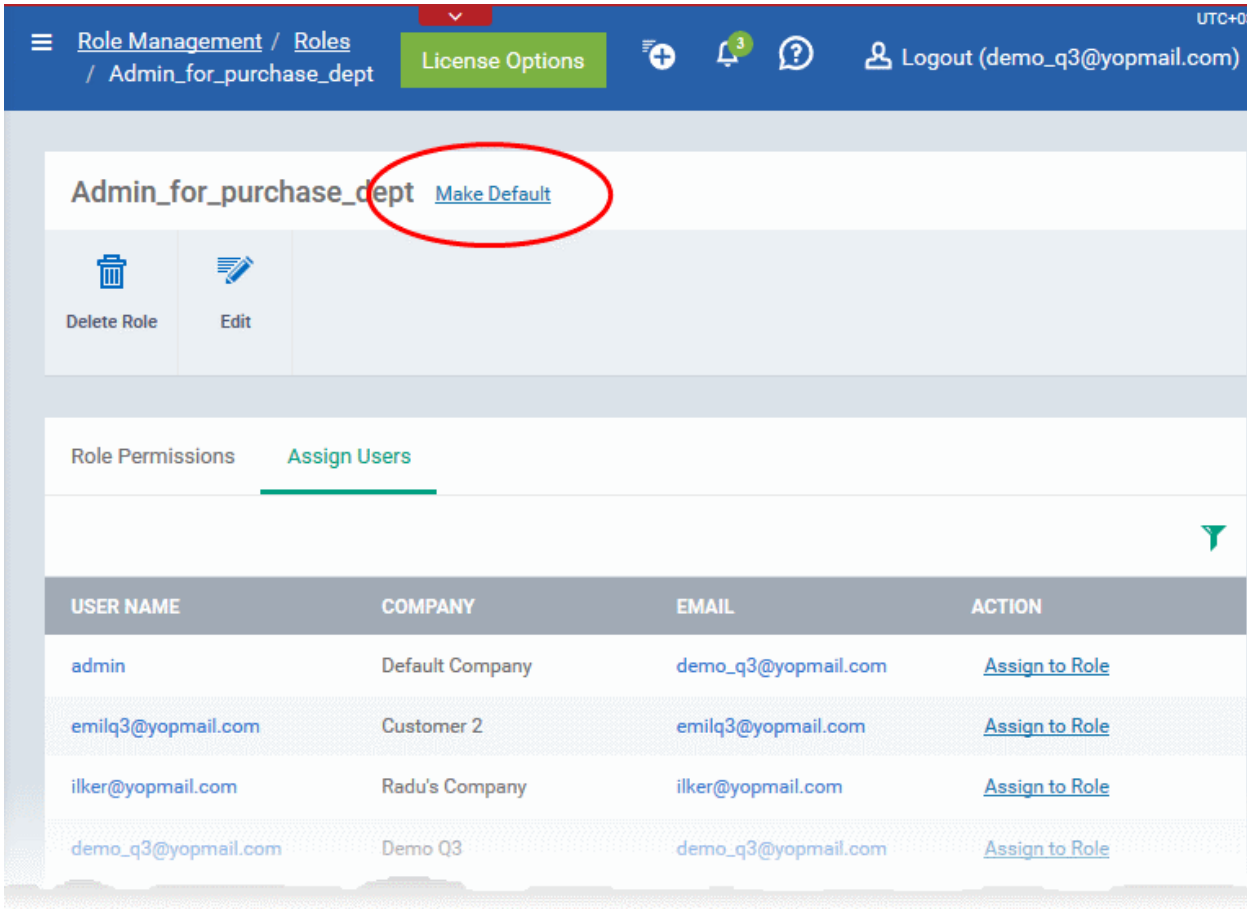
Clicking on a username opens a list of all roles assigned to that user, allowing you to add or remove roles from the user as required. Refer to **Managing Roles assigned to a User** for more details.

To set a role as the default role

The default role will be automatically selected in the 'Assign Role' drop-down in the 'Create New User' dialog.

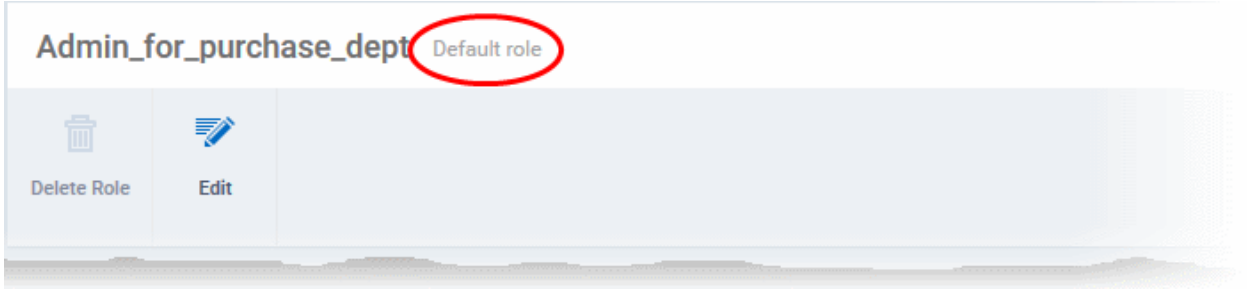
To set the default role:

- Click 'Users' > 'Role Management' to open the 'Roles' interface.
- Click the name of the role you wish to make default to open the 'Role Management' interface



- Click 'Make Default' beside the role name at the top

The role will be set as the default role. This will be indicated as follows:



4.3.3. Removing a Role

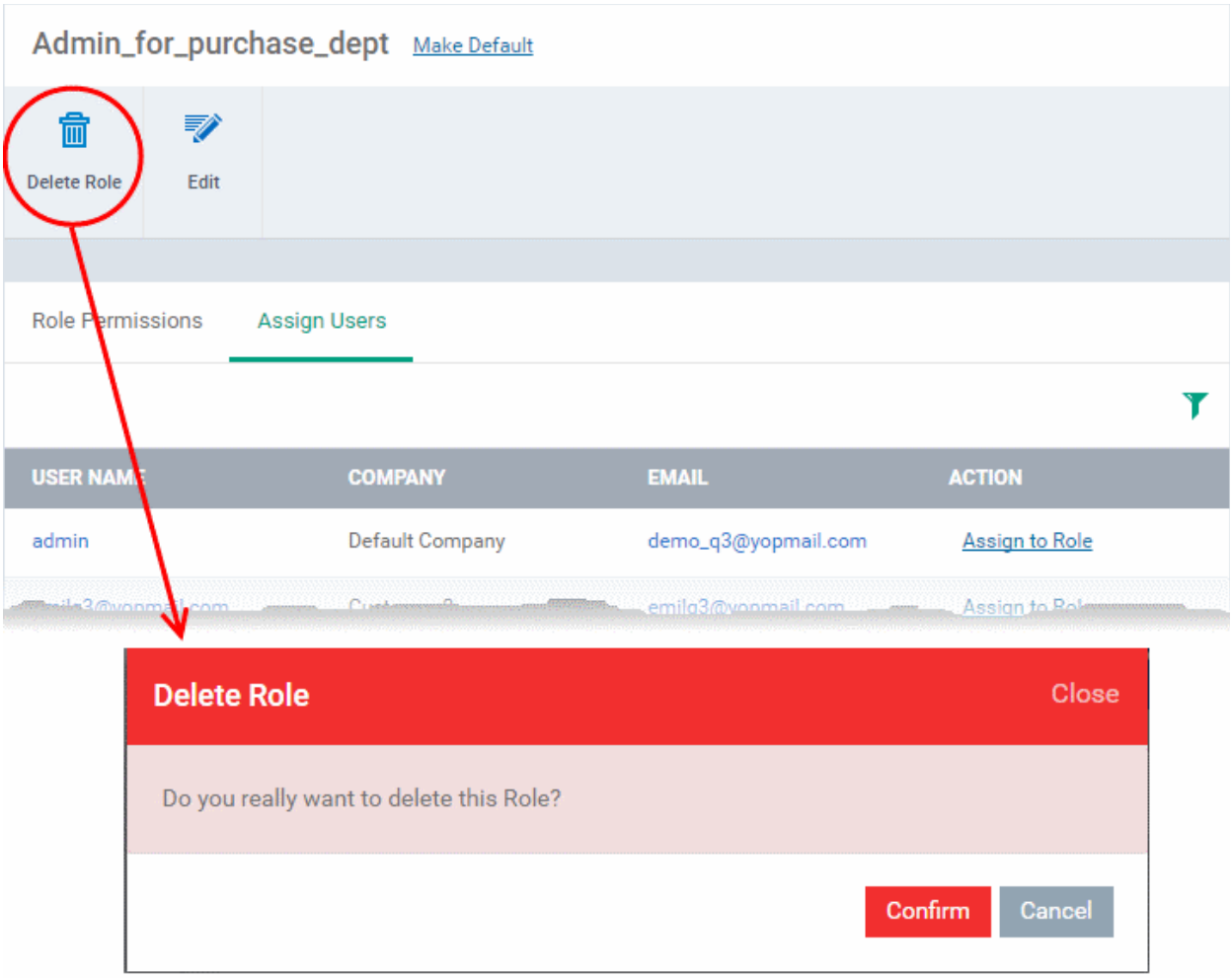
Administrators can delete roles that are no longer deemed necessary.

- Roles that are currently assigned to users cannot be removed. You should remove all users from any role you wish to delete.
- The current 'Default' role cannot be deleted. You should make another role the default first.
- The built-in roles ('Account Admin', 'Administrators' and 'Technicians') cannot be removed either.

To remove a role

- Click 'Users' on the left and select 'Role Management'.
- Click the 'Roles' tab.
- Click the 'Role' name to open the 'Role Management' interface

- Click 'Delete Role' at the top



A confirmation dialog will appear.

- Click 'OK' to remove the role.

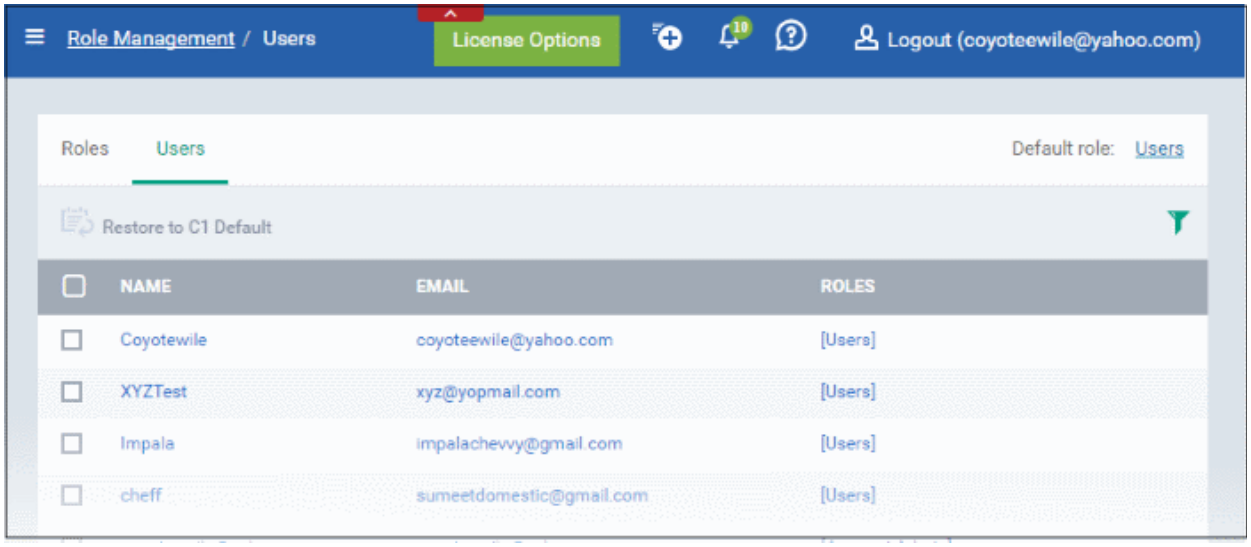
4.3.4. Managing Roles Assigned to a User

The 'Users' interface lets administrators add and remove roles from a user. Please note you cannot assign or remove the 'Account Admin' role. This role is automatically assigned to the person that created the C1 account.

Note. All staff created in the C1 interface will be available for selection in all roles, and for all companies in the account. This allows you to assign different roles to the same staff member for different companies. You can also reset the roles of users added via C1 to default C1 roles.

To open the Users interface

- Choose 'Users' from the left and select 'Role Management'.
- Click the 'Users' tab.



A list of users and roles assigned to them will be displayed.

To manage roles assigned to a user

- Click the name of the user whose roles you want to manage

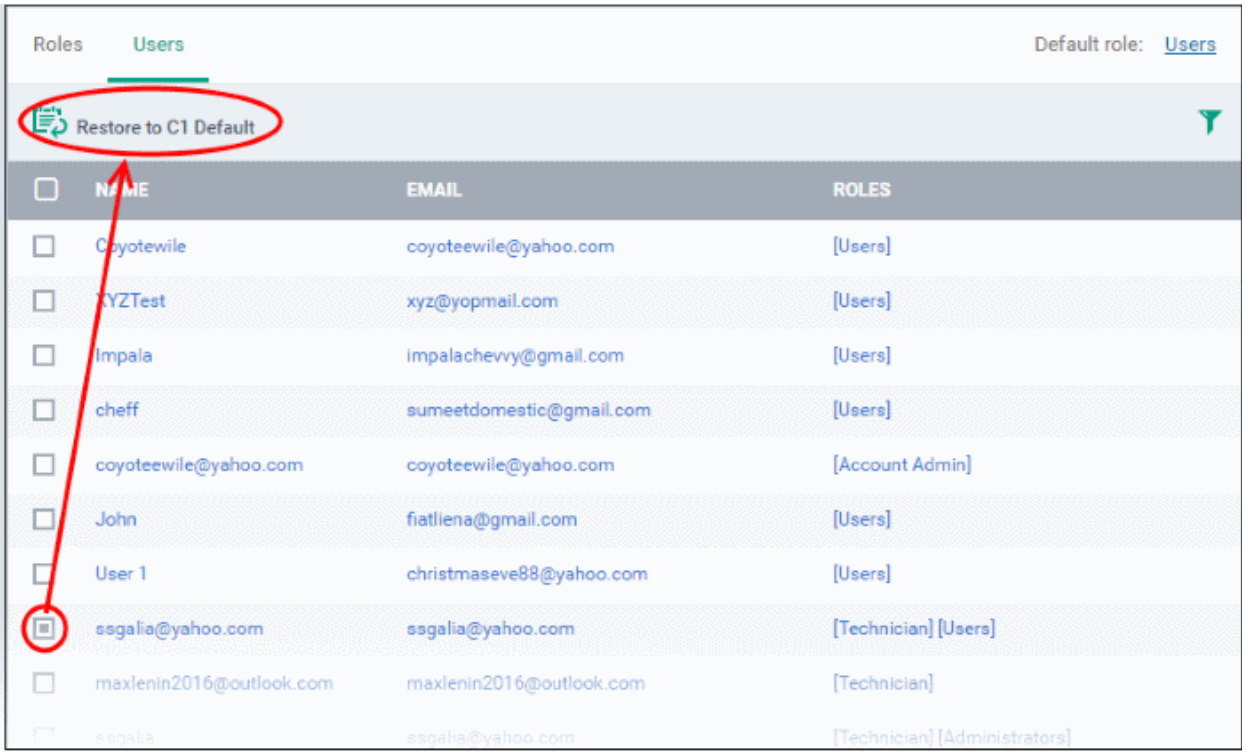
The interface will list of all available roles for the user. You can add a new role by clicking 'Assign to Role' in the 'Action' column. Roles that are already assigned to the user state 'Remove from Role' under the 'Action' column.

- To add a new role to the user, click 'Assign to Role' from the list.
- To remove a role for the user, click 'Remove from Role' beside the role.

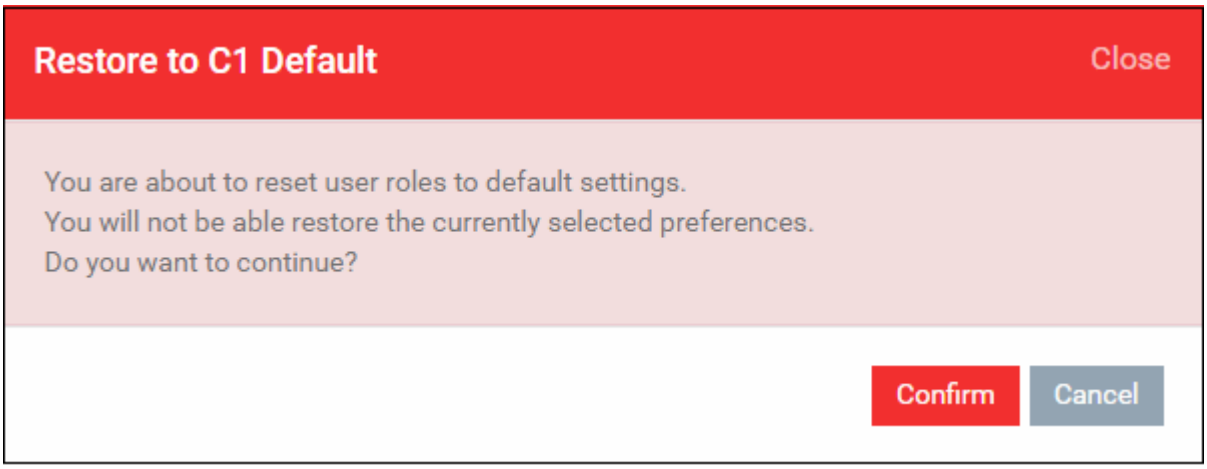
To reset the roles to C1 default

This is applicable for users that are added via C1 only.

- Choose 'Users' from the left and select 'Role Management'.
- Click the 'Users' tab.



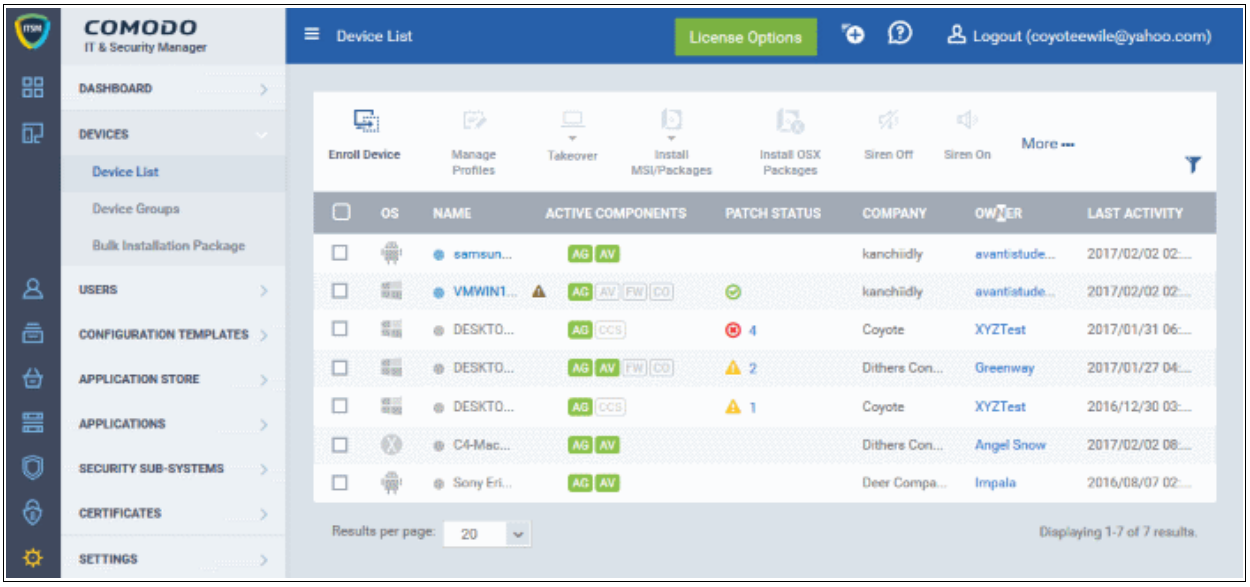
- Select the user and click 'Restore to C1 Default' button. Use the filter option on the top right to search for users from the list.



- Click 'Confirm' to restore the user with C1 default role

5. Devices

The 'Devices' area allows administrators to view, manage and take actions upon enrolled devices and device groups.



Note: Before you can enroll devices, you should first have installed an Apple Push Notification (APN) certificate (iOS devices) and/or Google Cloud Messaging (GCM) token (Android devices). Refer to **step 2** of the quick start guide if you have not yet added an APN certificate and/or GCM token.

Please use the following links to find out more:

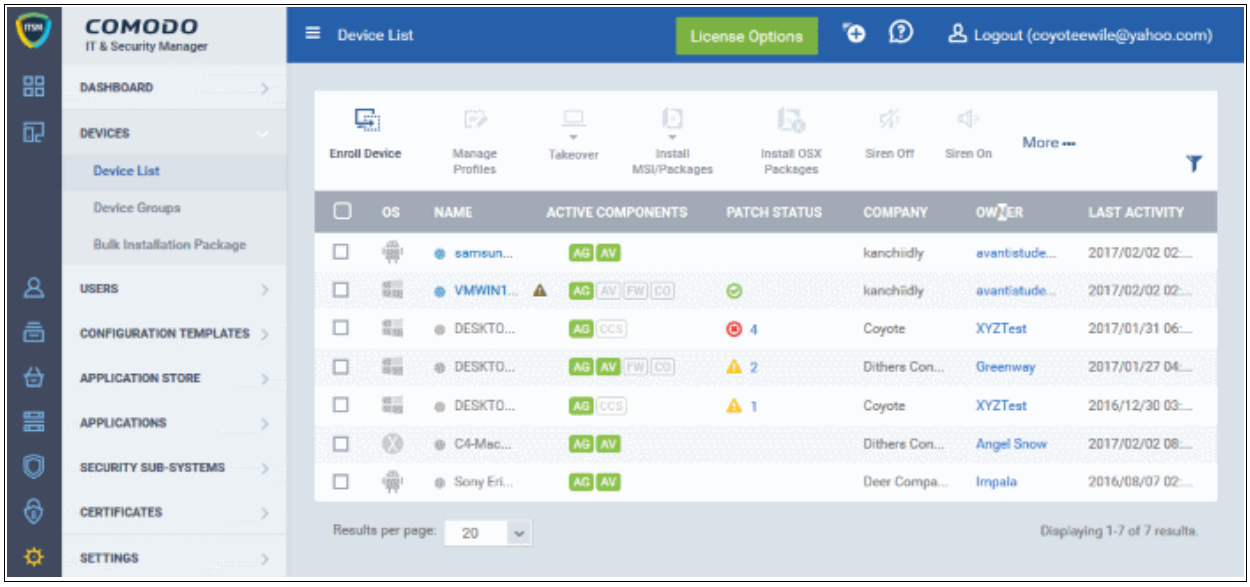
- The Device List
  - Managing Windows Devices
  - Managing Mac OS Devices
  - Managing Android/iOS Devices
  - Viewing the User Information
  - Removing a Device
  - Remote Management of Windows Devices
  - Remotely Installing Packages onto Windows Devices
  - Remotely Installing Packages on Mac OS Devices
  - Installing Apps on Android/iOS Devices
  - Generating Alarm on Devices
  - Locking/Unlocking Selected Devices
  - Wiping Selected Devices
  - Assigning Configuration Profile to Selected Devices
  - Setting / Resetting Screen Lock Password for Selected Devices
  - Updating Device Information
  - Sending Text Message to Devices
  - Rebooting a Selected Device
  - Changing a Device's Owner
  - Changing BYOD status of a Device
  - Applying Procedures for Windows Devices

5.1. Device List

The 'Device List' interface displays a full inventory of all mobile devices, Windows and Mac OS endpoints that have been enrolled to Comodo ITSM. From this area you can:

- Enroll new devices for management
- Add or remove profiles on any selected device
- Install Comodo Client Security and other packages on Windows endpoints
- Install Comodo Antivirus on and other packages on Mac OS endpoints
- Update Comodo Client Security and Comodo Client Communications on windows endpoints
- Take remote control of Windows devices
- Remotely install apps on mobile devices
- Run antivirus scans remotely and manage items identified as malware
- Sound an alarm on mobile devices
- Send custom text messages to mobile devices
- Remotely wipe mobile devices
- Set and reset mobile device lock-screen passcodes
- Remotely lock mobile devices
- Remove devices from ITSM management
- View detailed information about any device by simply clicking the device name
- View and edit device owner information by clicking the owner name
- Install the latest OS patches on Windows and Mac OS devices

To open the 'Device List' interface, click 'Devices' at the left and choose 'Device List':



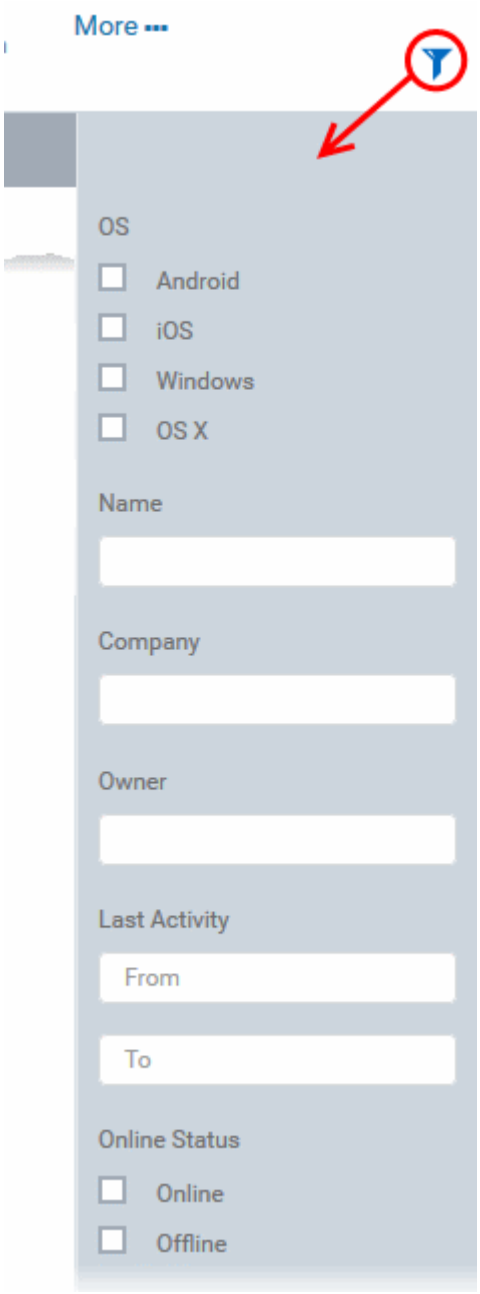
The Devices interface will open with a list of devices enrolled to ITSM.

Devices - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system of the device.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Grey text color indicates the device has been offline for the past 24 hours. Clicking the device name will open the granular device details interface. Refer to the sections Managing Windows Devices, Managing Mac OS Devices and Managing Android / iOS Devices for more details.
Active Components	Indicates which components are installed on the device (Agent only, Antivirus, Firewall, Containment) • Android devices - The agent will automatically install the AV (antivirus) component. • iOS devices - Only the agent (ITSM client) will be installed • Windows endpoints - Available components are - Agent, AV, FW (firewall) and Containment. • Mac OS endpoints - Available components are - Agent and AV
Patch status	Indicates the number patches available for all added windows endpoints. Patch status icons are as follows: • - Number of patches successfully installed • - Number of critical patches awaiting installation • - Number of optional patches awaiting installation Clicking the number next to the patch status opens the device properties interface at the 'Patch Management' tab.
Company	Indicates the name of the company to which the device is enrolled. • Comodo One MSP customers can enroll devices to any of the companies they have created in C1. • Comodo One Enterprise customers / ITSM standalone customers can only use

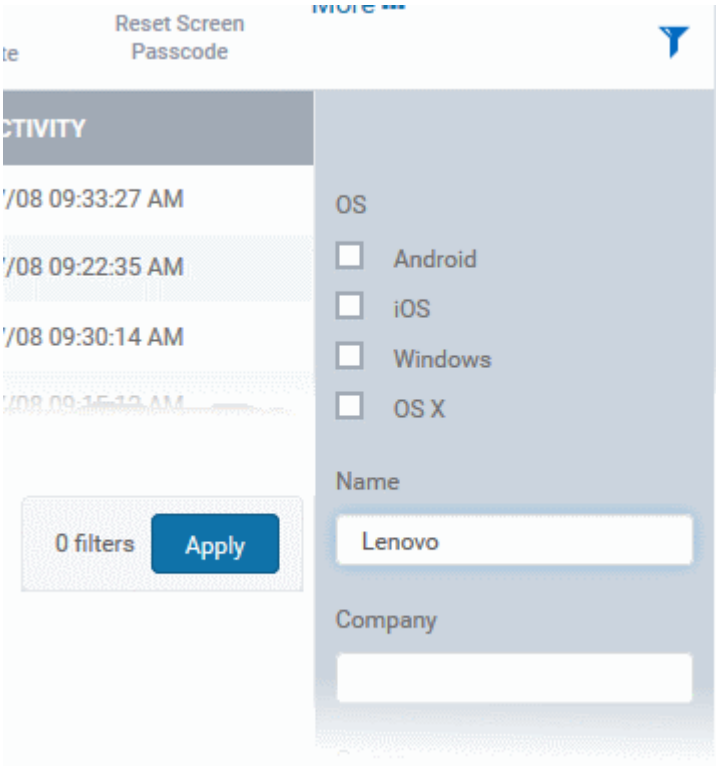
	the 'default company'.
Owner	Indicates the device user. Clicking the user name will open the 'View User' interface. Refer to Viewing the User Information for more details.
Last Activity	Indicates the date and time at which the device last communicated with the ITSM agent.

Sorting, Search and Filter Options

- Clicking on 'OS', 'Name', 'Owner' and 'Last Activity' column headers sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter items based on operating system, select the OS types of the devices to be displayed in the list
- To filter or search for a specific device based on device name, company and/or owner, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- Enter the start and end dates in the 'From' and 'To' fields to filter devices based on their last activities within the time period.
- You can also filter devices based on their current patch status:
  - Up to date endpoints
  - Critical patches available
  - Missing patches

You can use more than one filter at a time to create more granular searches.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Refer to the following sections for more details on:

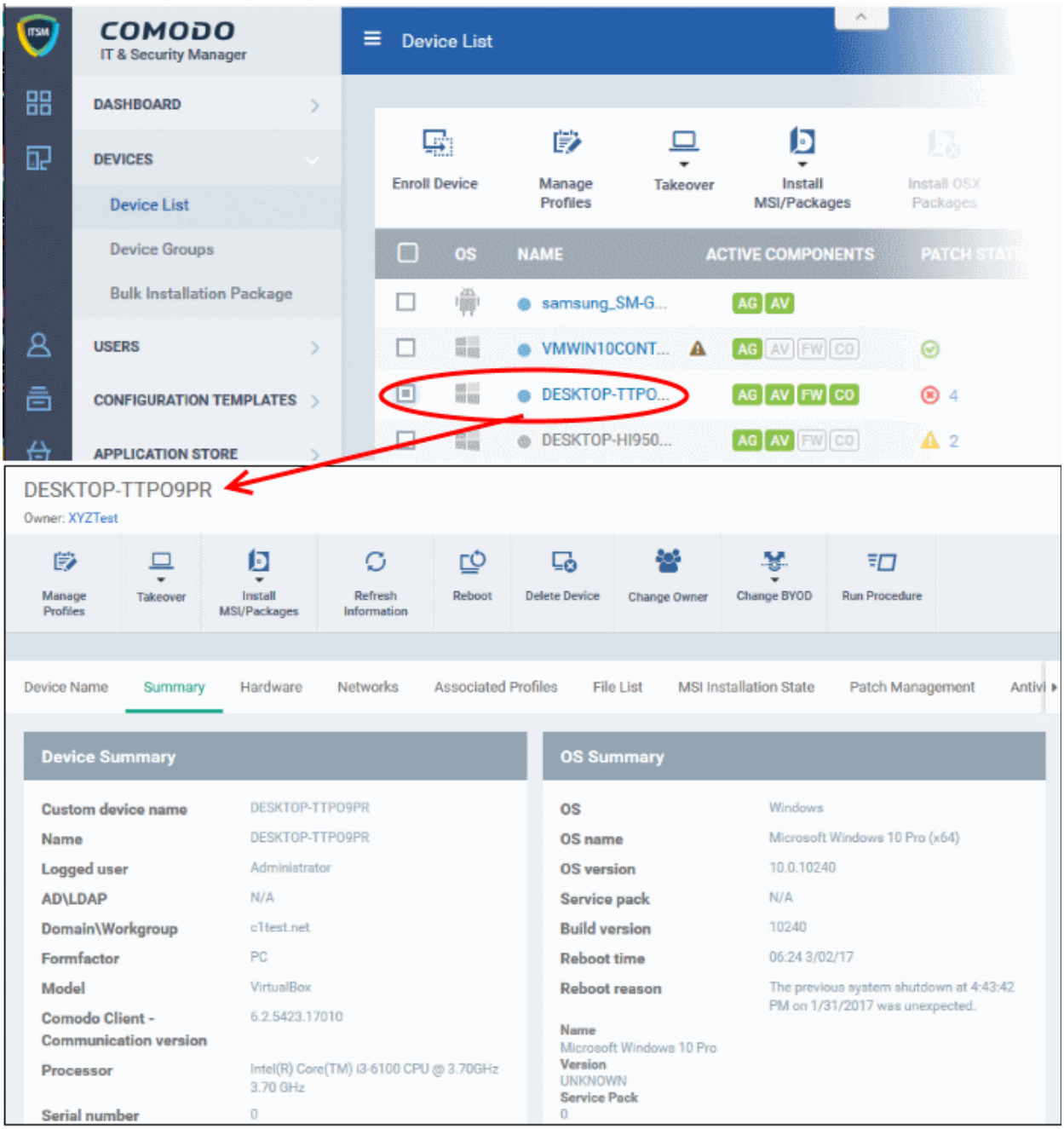
- Managing Windows Devices
  - Viewing and Editing Windows Device Name
  - Viewing Summary Information
  - Viewing Hardware Information
  - Viewing Network Information
  - Viewing and Managing Profiles Associated with Windows Device
  - Viewing List of Files on the Device
  - Viewing CCS Configuration Exported from the Device
  - Viewing MSI Files Installed on the Device through ITSM
  - Viewing and Installing Windows Patches
  - Viewing Antivirus Scan History
  - Viewing and Managing Device Group Memberships
  - Viewing Alert Logs
  - Viewing Monitoring Logs

5.1.1. Managing Windows Devices

The Windows device details page allows administrators to view device hardware and software details, installed components and network connection details. Administrators can also manage the configuration profiles in effect on the endpoint, deploy Windows patches and manage membership of the device to different groups.

To view details of and manage a Windows device

- Click 'Devices' and choose 'Device List'
- Click on the name of any Windows device



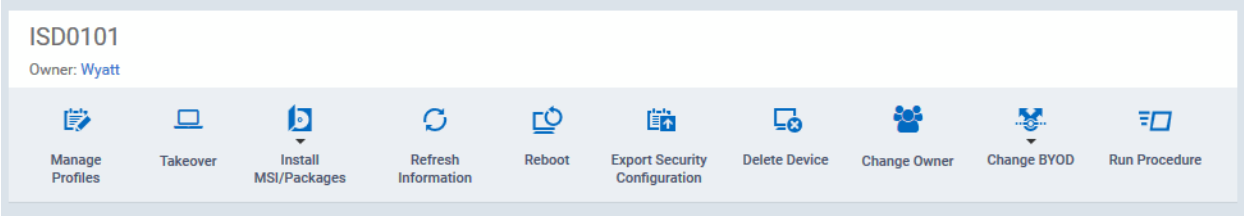
The Windows device details pane will open, displaying the details of the selected device under eleven tabs. By default, the 'Summary' tab will be displayed.

- **Device Name** - Displays the name of the device. You can change this as per your preferences. Refer to the section **Viewing and Editing Device Name** for more details.
- **Summary** - Displays general details about the device, including device and OS information and performance metrics like CPU, RAM, network and disk usage. Refer to the section **Viewing Summary Information** for more details.
- **Hardware** - Displays the hardware configuration of the selected device. Refer to the section **Viewing Hardware Information** for more details.
- **Networks** - Displays the device's network details such as its MAC address, its IP address, currently connected networks and more. Refer to the section **Viewing Network Information** for more details.
- **Associated Profiles** - Displays the details of the profiles deployed on the device. Refer to the section **Viewing and Viewing and Managing Profiles Associated with the Devices** for more details.
- **File List** - Displays a list of files on the device along with their file rating ('Unrecognized', 'Trusted' or

'Malicious'). Refer to the section **Viewing List of Files in the Device** for more details.

- **Exported Configurations** - Displays details of exported Comodo Client Security configuration files. Refer to the section **Viewing CCS Configurations Exported from the Device** for more details.
- **MSI Installation State** - Displays MSI files that have been installed on the device via ITSM. Refer to the section **Viewing MSI Files Installed on the Device through ITSM** for more details.
- **Patch Management** - Lists available patches for the devices and whether they are installed or not. Refer to the section **Viewing and Installing Windows Patches** for more details.
- **Antivirus Scan History** - Displays a history of threats identified on all devices and the actions taken by ITSM in response. Refer to the section **Viewing Antivirus Scan History** for more details.
- **Groups** - Displays a list of device groups to which the endpoint belongs and allows administrators to manage group membership. Refer to the section **Viewing and Managing Device Group Memberships** for more details.
- **Alert Logs** - Lists alerts generated because of a breach of monitoring conditions or procedure deployment. Refer to the section **Viewing Alert Logs** for more details.
- **Monitoring Logs** - Displays details of monitoring breaches that occurred for the past 24 hours on the endpoints. Refer to the section **Viewing Monitoring Logs** for more details.
- **Procedure Logs** - Displays details about procedures that were run on the Windows device manually as well as automatically via scheduling in a profile. Refer to the section **Viewing Procedures Logs** for more details.

Administrators can remotely perform various tasks on the device using the options at the top of the interface.



- **Manage Profiles** - Allows you to add or remove device profiles. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details.
- **Takeover** - Allows you to download Comodo Remote Monitoring and Management (RMM) Console and remotely monitor, manage and take control of the endpoint. Refer to the online help guide for RMM at **https://help.comodo.com/topic-289-1-719-8539-Introduction-to-Remote-Monitoring-and-Management-Module.html** for more details. Another remote take over tool, Comodo Client Viewer, can also be used to take endpoints remotely for solving issues. Refer to the section '**Remote Management of Windows Devices**' for more details.
- **Install MSI Packages** - Allows you to remotely install Comodo endpoint security software and third party Windows packages. Refer to the section **Remotely Installing Packages onto Windows Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. Refer to the section **Updating Device Information** for more details.
- **Reboot** - Allows you to remotely restart the device. Refer to the section **Rebooting a Selected Device** for more details.
- **Export Configurations** - Allows you to export the devices current CCS configuration as a profile. Exported profiles can be viewed under the **Exported CCS Configurations** tab. These can then be imported later as a Windows profile, potentially for deployment to other devices. Refer to the section **Importing Windows Profiles** for more details.
- **Delete Device** - Removes the device from ITSM. Refer to the section **Removing a Device** for more details.
- **Change Owner** - Allows you to change the user to whom the device is associated. Refer to the section **Changing a Device's Owner** for more details.

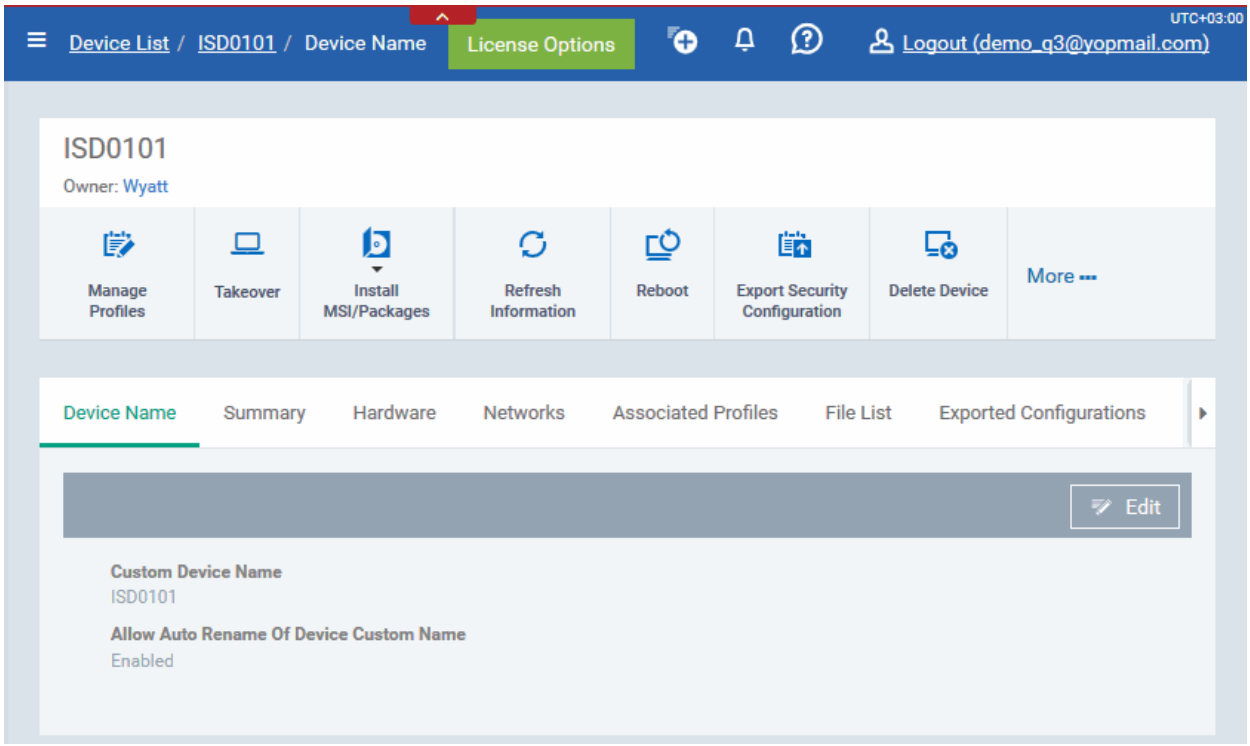
- Change BYOD - Changes the BYOD status of the device. Refer to the section 'Changing BYOD status of a Device' for more details.
- Run Procedure - Allows you to apply procedures on Windows devices. Refer to the section 'Applying Procedures for Windows Devices for more details.

5.1.1.1. Viewing and Editing Device Name

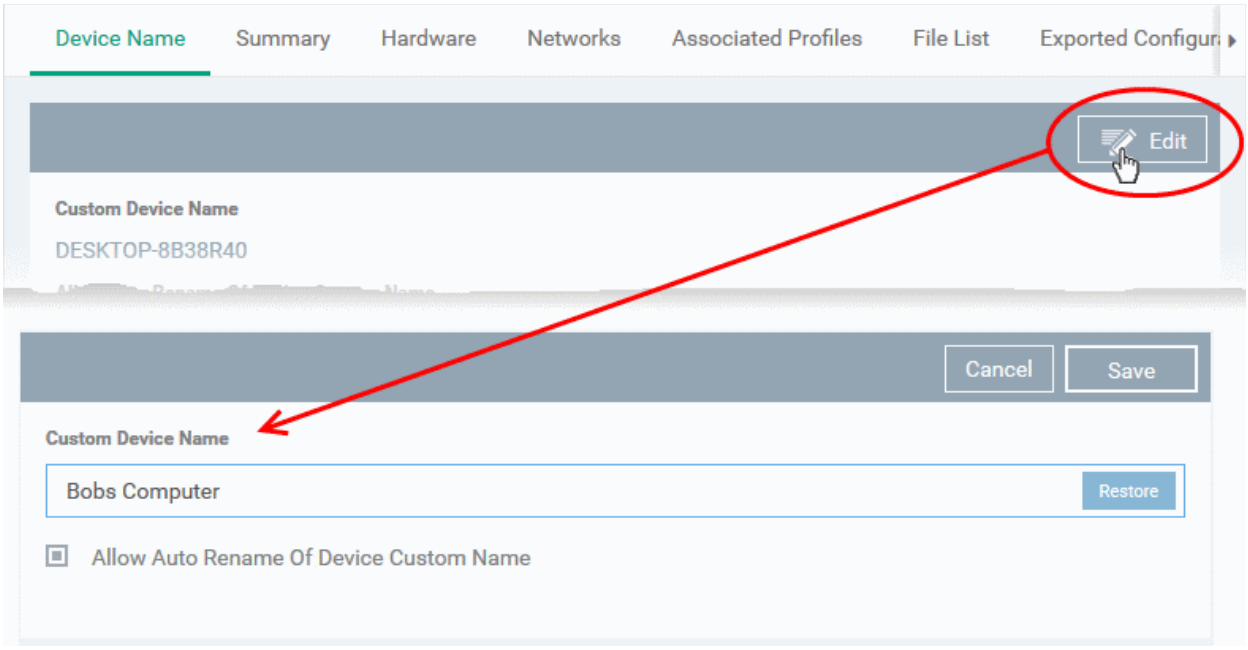
Enrolled devices are listed by the name assigned to them by their owner. If no name was assigned then the model number of the device will be listed. Admins can change the device name according to their preferences. If you change a device name, the name will apply in ITSM but will not change the name on the endpoint itself. Please note if the option, 'Allow Auto Rename of Device Custom Name' is enabled then the custom name will be replaced automatically by device name or model number during the next sync with the ITSM agent on the device. To retain the custom name for the device in the list, make sure to disable this option.

To change a device name

- Click 'Devices' and choose 'Device List'
- Click the name of any Windows device then select the 'Device Name' tab from the 'Device Details' interface



  - Custom Device Name - The current name of the device.
  - Allow Auto Rename of Device Custom Name - Indicates whether the device's name will automatically replace the custom name in the list during the next sync with ITSM agent.
- To change the name of the device, click the 'Edit' button at the right.



- Enter the new name in the 'Custom Device Name' field
- Make sure the 'Allow Auto Rename of Device Custom Name' is disabled to retain the custom name in the list. If this is enabled, the custom name will be automatically replaced with the device's name or model number during the next sync with the ITSM agent on the device.

- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

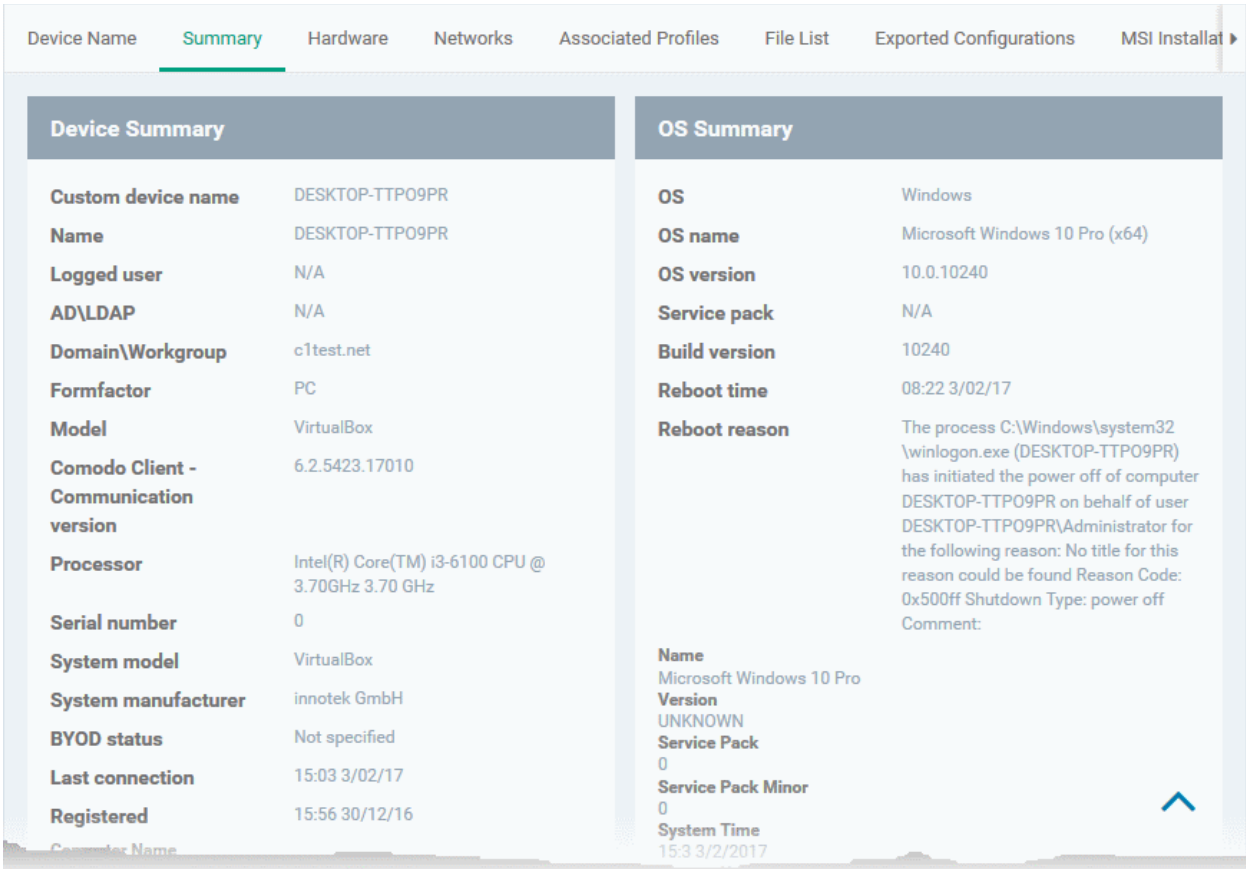
- To restore the name of the device as it was at the time of enrollment, click 'Edit' from the 'Device Name' interface, click 'Restore' at the right and click 'Save'.

5.1.1.2. Viewing Summary Information

The 'Summary' tab displays general device information such as operating system details, hardware details, last activity, Comodo software configuration, device user and more.

To view the device information summary

- Click 'Devices' and choose 'Device List'.
- Click the name of any Windows device. Open the 'Summary' tab (if it is not already open).



- **Device Summary** - General device details, including device name, type, OS, model, manufacturer, currently logged-in user, active directory domain, system info, BYOD status and more.
- **OS Summary** - Detailed information about the endpoint OS, service pack status, number of installed applications, last restart time, reason for last reboot, currently running processes and services and more.
- **Comodo ONE Client - Security Info** - Displays details about the Comodo One Client application installed on the endpoint, active security components, virus signature database update status and more.
- **Performance Metrics** - Displays current resource usage, including CPU usage, RAM usage, Network usage and Disk usage.

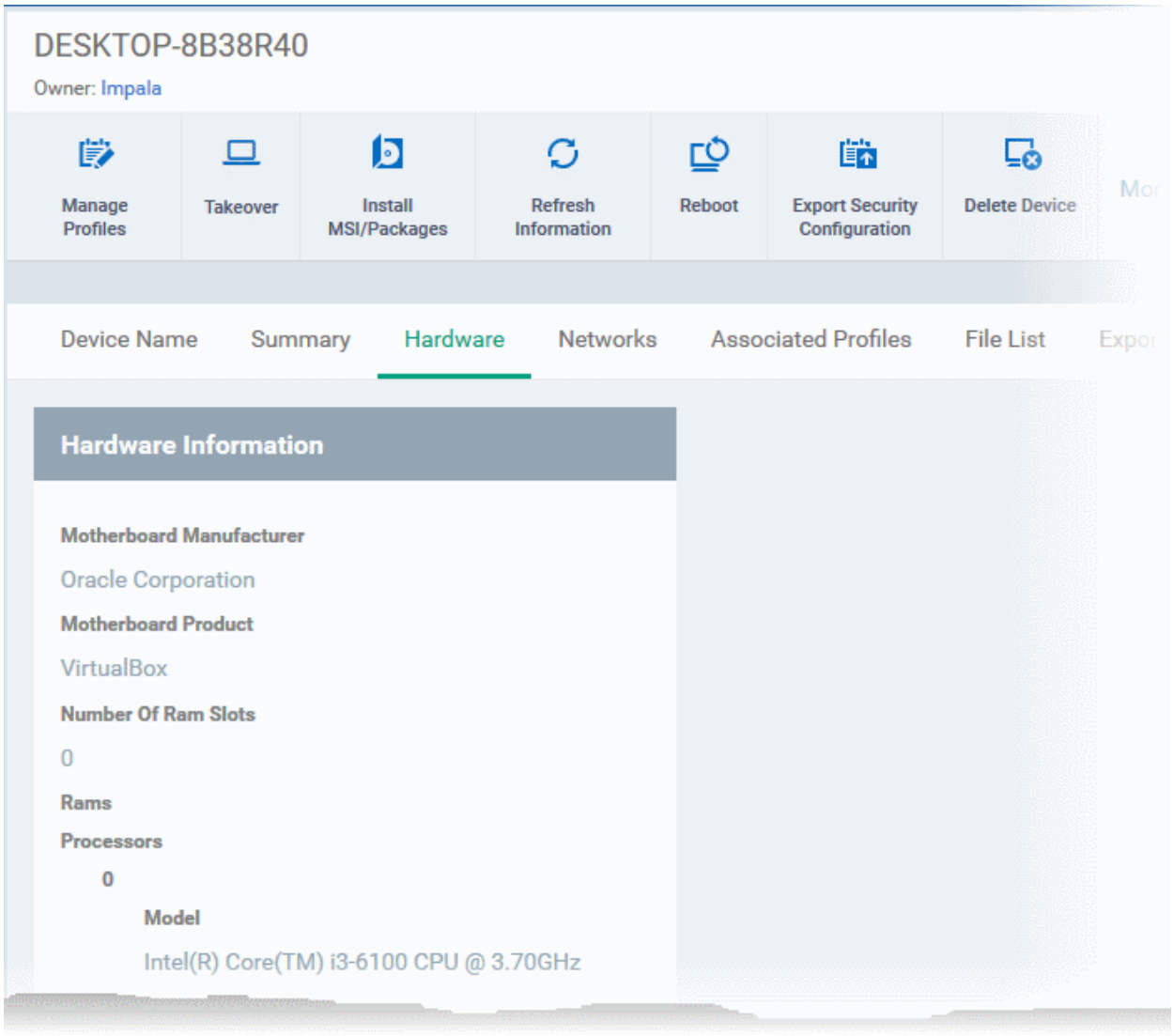
5.1.1.3. Viewing Hardware Information

This screen contains basic details about the hardware component of the Windows endpoint.

Note: Hardware details will only be available for devices that have the Comodo RMM agent installed. Refer to Managing ITSM Extensions and **Remotely Installing Packages onto Windows Devices** for more details.

To view a device's hardware details

- Click 'Devices' and choose 'Device List'
- Click the name of any Windows device, then select the 'Hardware' tab

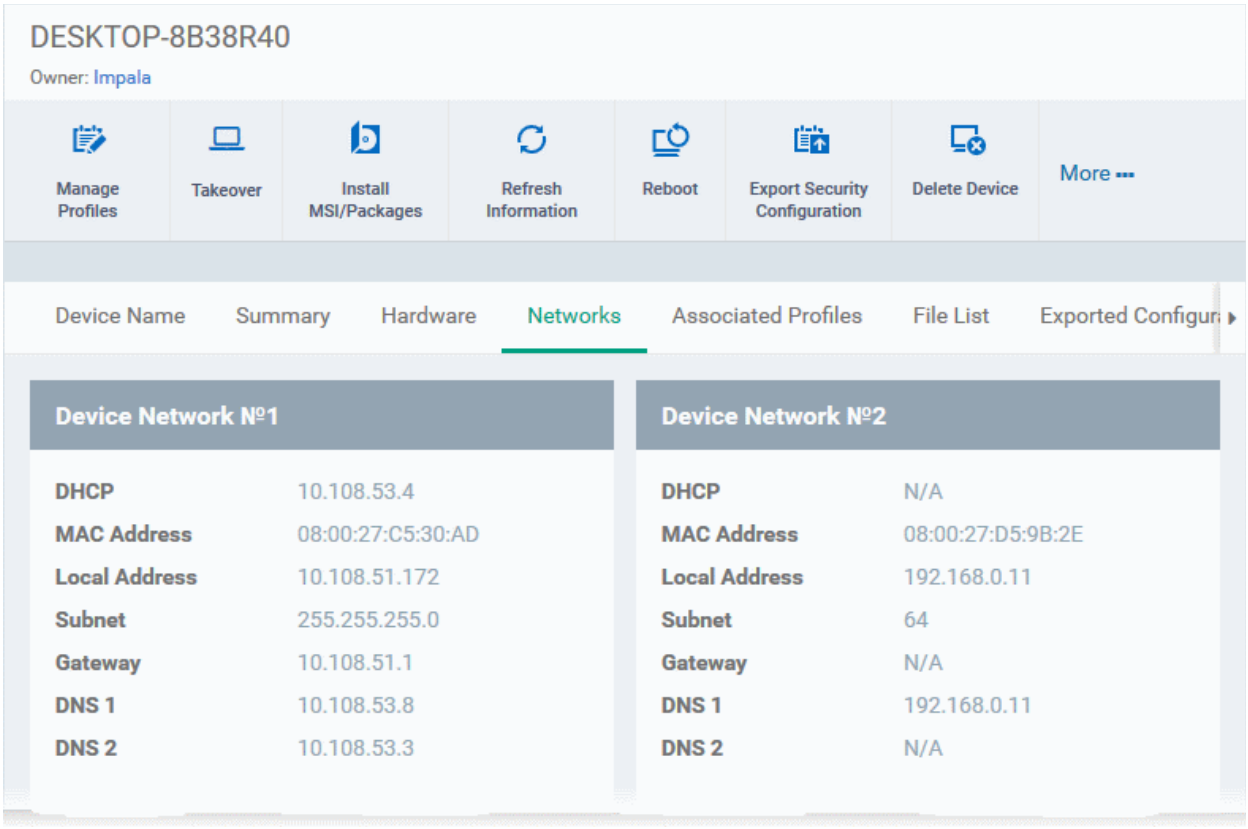


5.1.1.4. Viewing Network Information

The 'Networks' screen shows details about the network(s) to which an endpoint is connected.

To view a device's network details

- Click 'Devices' and choose 'Device List'
- Click the name of any Windows device, then select the 'Networks' tab



5.1.1.5. Viewing and Managing Profiles Associated with a Device

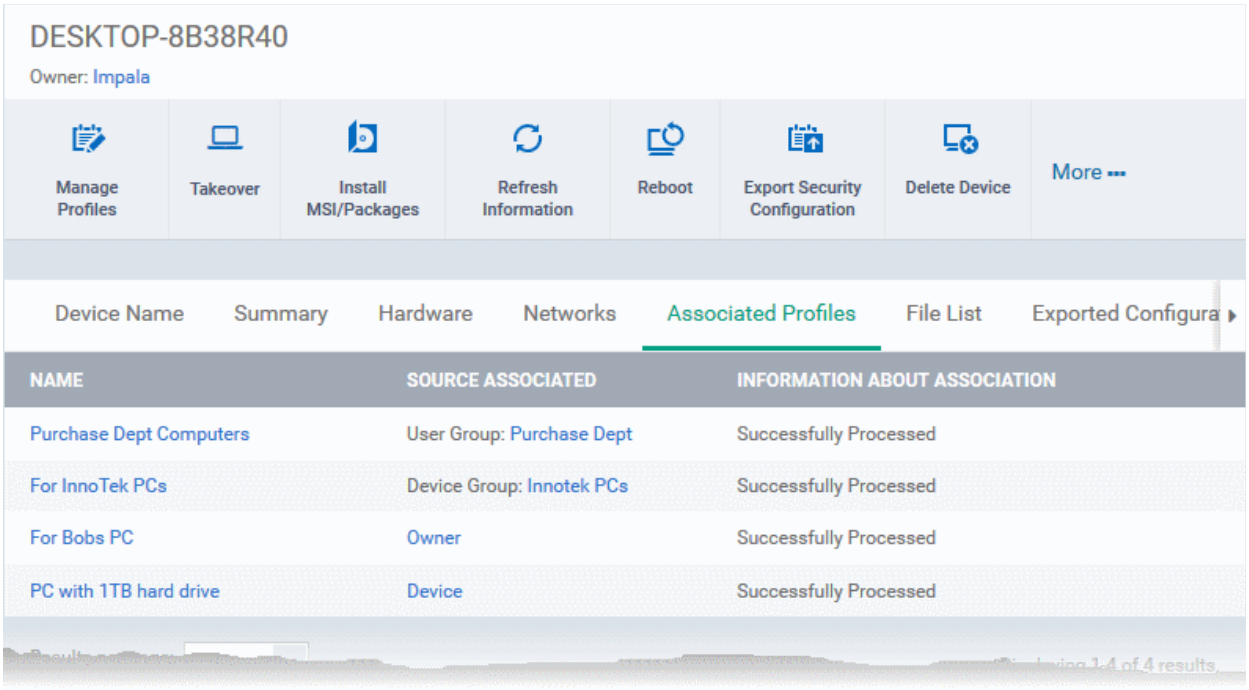
The 'Associated Profiles' tab displays a list of all currently active configuration profiles on an endpoint. A profile may have been applied for any of the following reasons:

- Because it is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- Because the device belongs to a device group
- Because the user belongs to a user group

For more details on profiles and groups of profiles, refer to the chapter Configuration Profiles.

To view and manage the profiles associated with a device

- Click 'Devices' and choose 'Device List'
- Click the name of any Windows device, then select the 'Associated Profiles' tab



Associated Profiles - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section **Editing Configuration Profiles** for more details.
Source Associated	Indicates the source through which the profile has been applied to the device. Configuration profiles are applied to a device in different ways: • Profiles can be directly applied to the device. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. Refer to the section **Assigning Configuration Profile(s) to a Users' Devices** for more details • Profiles applied to a user group are deployed to all devices owned by group members. Refer to the section **Assigning Configuration Profile to a User Group** for more details • Profiles applied to a device group are deployed to all member devices in the group. Refer to the section **Assigning Configuration Profile to a Device Groups** for more details Clicking on the source opens the respective details interface.
Information about Association	Indicates the status of profile application to the device.

- Clicking the 'Name' column header sorts the items in the alphabetical order of the names of the items

Adding or Removing Profiles

Profiles can be added or removed from the device clicking 'Manage Profiles' option at the top. Refer to the section **Assigning Configuration Profile to Selected Devices** for more details.

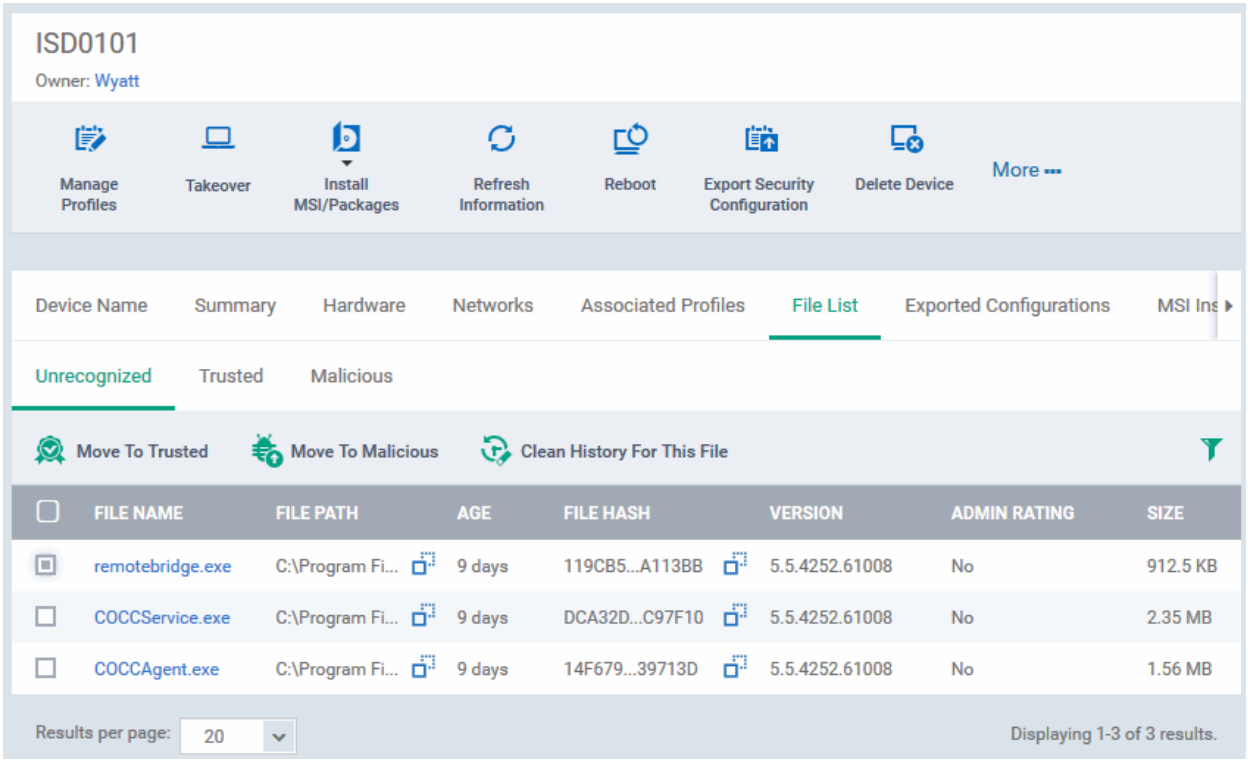
5.1.1.6. Viewing Files on a Device

Comodo Client Security monitors all file activities on a Windows endpoint. New executables are scanned against the Comodo files database and rated as 'Unrecognized', 'Trusted' or 'Malicious'. File ratings can be configured as part of a Windows profile - see File Rating settings for more details. The File List screen allows you to view and change the ratings of discovered files on a particular device, and to clear the rating history of files.

Note - if you wish to see all files across all managed devices, please view the 'Applications' and 'Application Control' interfaces. Refer to the sections 'Applications > Mobile Applications' and 'Viewing Applications Installed on Windows Devices' for more details.

To view and manage file ratings on a device

- Click 'Devices' and choose 'Device List'
- Click the name of any Windows device, then select the 'File List' tab



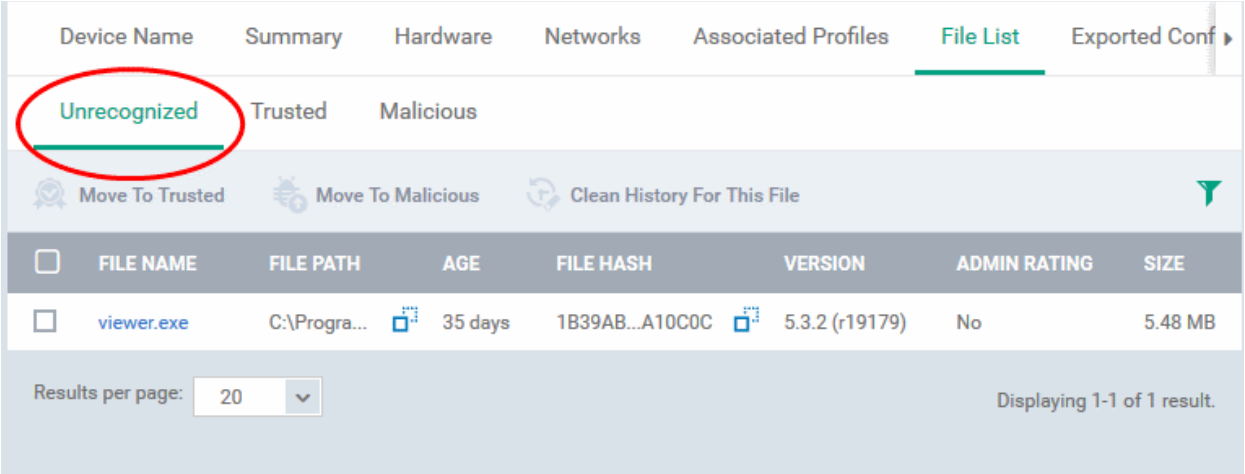
The interface contains three tabs:

- Unrecognized - Displays the list of files reported as 'Unrecognized' by the CCS installations at the endpoint. The administrator can move items to 'Trusted Files' list or 'Malicious Files' list, depending on the trustworthiness of the files from this interface. Refer to the section 'Viewing and Managing Unrecognized Files on the Device' for more details.
- Trusted - Displays the 'Trusted Files' list on the device. Administrators can move items to this list from the Unrecognized Files or Malicious Files lists. Refer to the section 'Viewing and Managing Trusted Files on the Device' for more details.
- Malicious - Displays the 'Malicious Files' list on the device. Administrators can manually add files or move items to this list from Unrecognized Files or Trusted Files lists, and move false positives to Unrecognized Files or Trusted Files lists. Refer to the section 'Viewing and Managing Malicious Files on the Device' for more details.

Viewing and Managing Unrecognized Files on a Device

The 'Unrecognized' interface displays files whose trust level is 'Unknown' (neither 'known-safe' nor 'known-malicious').

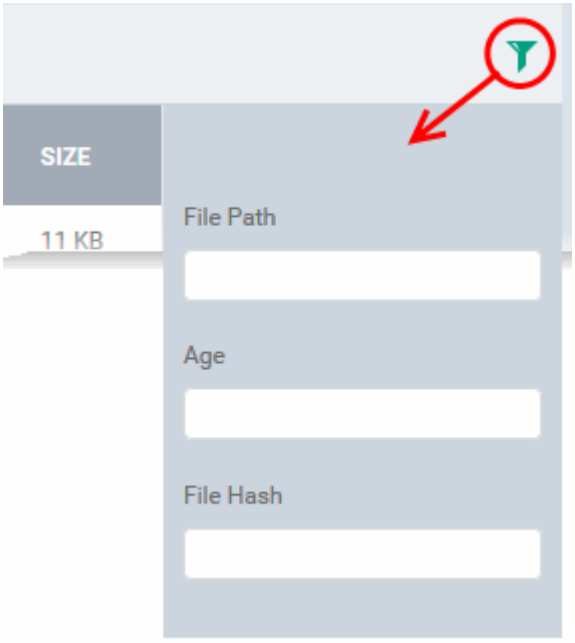
- Click the 'Unrecognized' tab



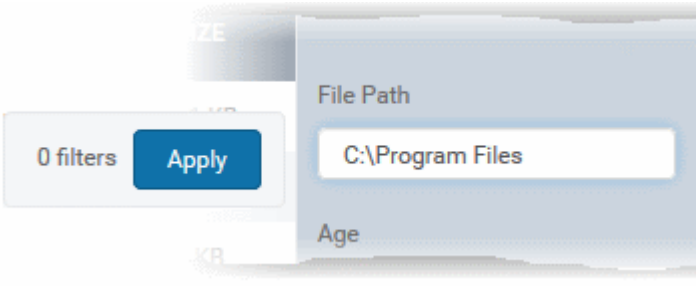
The 'Unrecognized' Files List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the 'Unrecognized' item. Clicking the file name will open the 'File Info' screen of the file, that displays the details of the file and the list of all devices that contain the same file. Refer to the section Viewing and Managing Unrecognized Files for more details.
File Path	The installation location of the file on the endpoint. Clicking the copy icon copies the path to the clipboard.
Age	The duration from the time of installation of the executable file.
File Hash	Displays the hash value of the file derived using SHA1 hash algorithm. Clicking the copy icon copies the hash to the clipboard.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to the 'Unrecognized Files' list from 'Trusted' Files or 'Malicious' file list here by the administrator.
Size	The size of the unrecognized file.

Sorting, Search and Filter Options

- Clicking on 'File Name' or 'File Path' column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific item based on the file path, age of the file and SHA1 hash value name, package or version, enter the search criteria in full or part in the respective text box and click 'Apply'



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

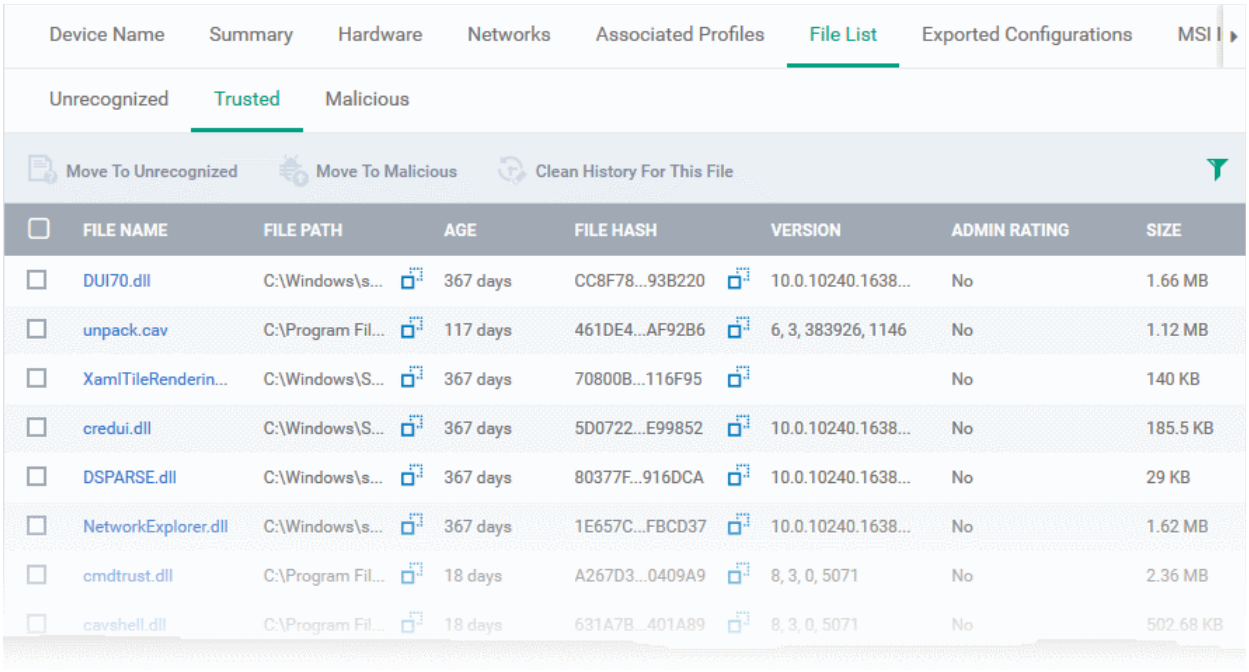
Managing Unrecognized Files

The 'Unrecognized' interface displays a full list of unrecognized files reported by the CCS installation at the endpoint. You can move the unrecognized files to the trusted or malicious file list. This is similar to moving unrecognized files to trusted or malicious list from the Applications interface. Refer to the section 'Viewing and Managing Unrecognized Files' for more details.

Viewing and Managing Trusted Files on the Device

Files included in the 'Trusted Files' list are automatically given CCS trusted status.

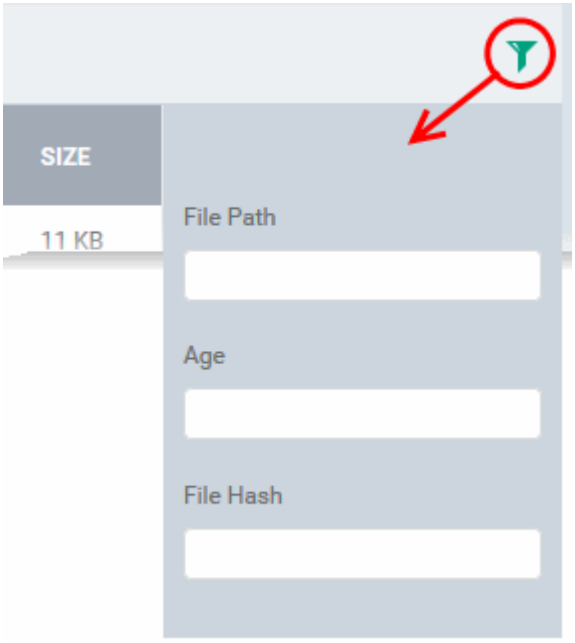
- Click the 'Trusted' tab



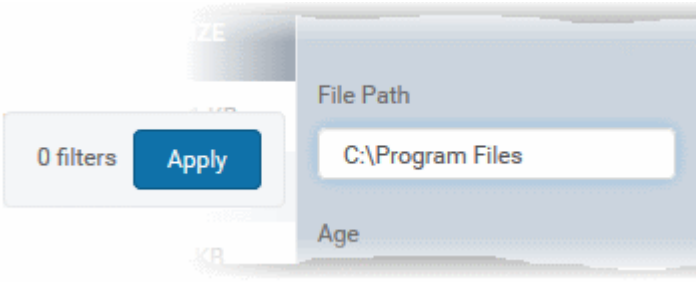
The 'Trusted ' Files List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the 'Trusted' item. Clicking the file name will open the 'File Info' screen of the file, that displays the details of the file and the list of all devices that contain the same file. Refer to the section Viewing and Managing Unrecognized Files for more details.
File Path	The installation location of the file at the endpoint. Clicking the copy icon copies the path to the clipboard.
Age	The duration from the time of installation of the executable file.
File Hash	Displays the hash value of the file derived using SHA1 hash algorithm. Clicking the copy icon copies the path to the clipboard.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to 'Trusted' files list by the administrator.
Size	The size of the file.

Sorting, Search and Filter Options

- Clicking on 'File Name' and 'File Path' column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific item based on the file path, age of the file and SHA1 hash value name, package or version, enter the search criteria in full or part in the respective text box and click 'Apply'



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

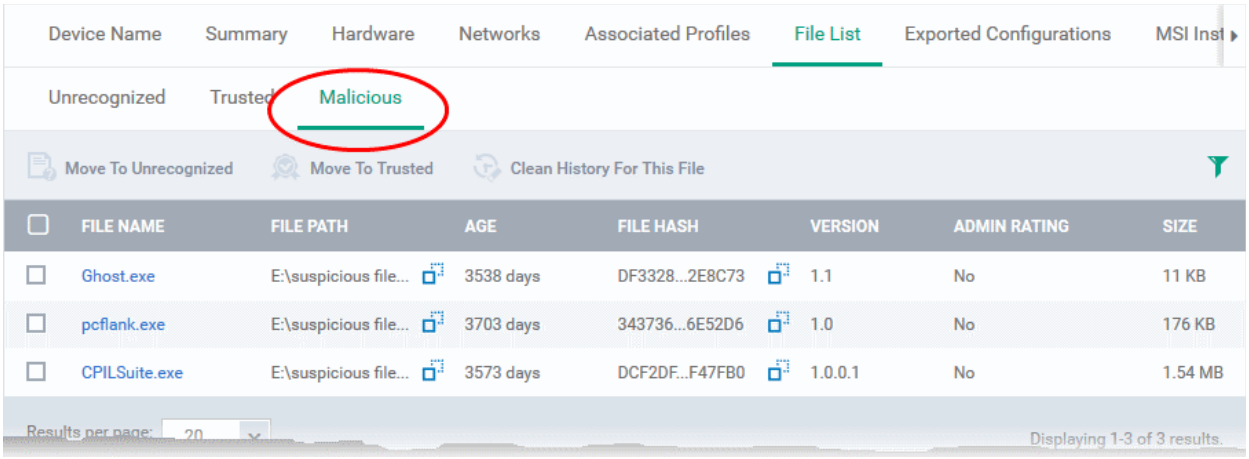
Managing Trusted Files

The 'Trusted' file interface displays a full list of trusted files reported by the CCS installation at the endpoint. You can move the trusted files to the unrecognized or malicious list. This is similar to moving trusted files to unrecognized or malicious list from the 'Applications' interface. Refer to the section '**Viewing and Managing Trusted Files**' for more details.

Viewing and Managing Malicious Files on the Device

Files that are identified as malicious from the File Look up Service (FLS) by the local CCS installation will be given 'Malicious' rating and will not be allowed to run by default.

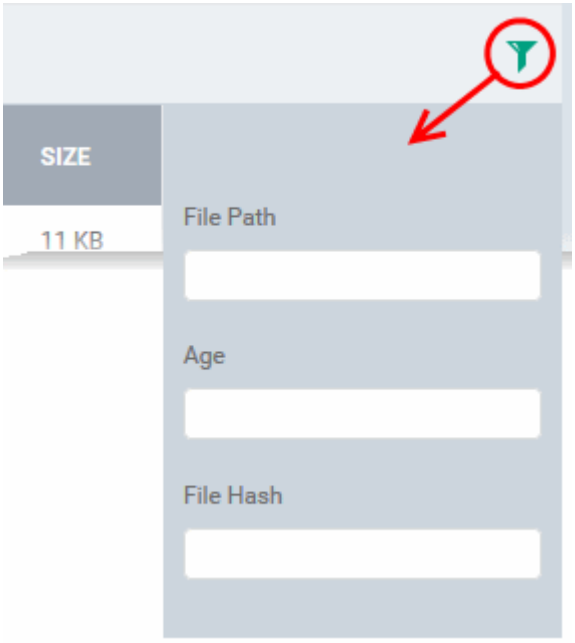
- Click the 'Malicious' tab



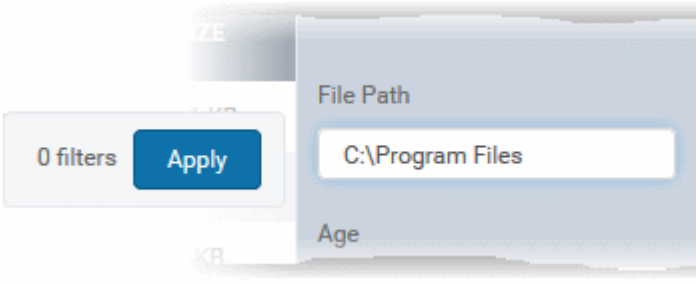
The 'Malicious' Files List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the 'malicious' item. Clicking the file name will open the 'File Info' screen of the file, that displays the details of the file and the list of all devices that contain the same file. Refer to the section Viewing and Managing Unrecognized Files for more details.
File Path	The installation location of the file at the endpoint. Clicking the copy icon copies the path to the clipboard.
Age	The duration from the time of installation of the executable file.
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm. Clicking the copy icon copies the path to the clipboard.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to 'Malicious' files list by the administrator.
Size	The size of the file.

Sorting, Search and Filter Options

- Clicking on 'File Name' or 'File Path' column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific item based on the file path, age of the file and SHA1 hash value name, package or version, enter the search criteria in full or part in the respective text box and click 'Apply'



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Malicious Files

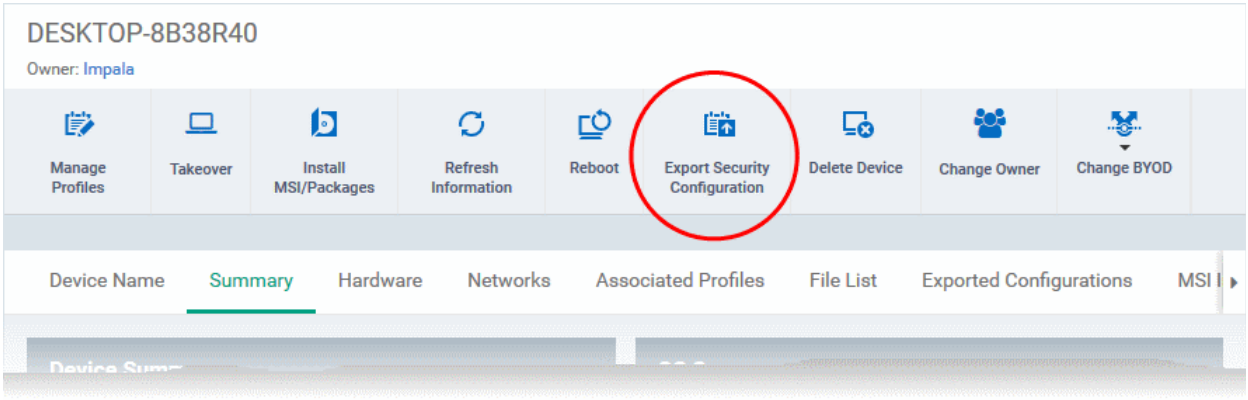
The 'Malicious' file interface displays a full list of malicious files reported by the CCS installation at the endpoint. You can move the malicious files to the trusted or unrecognized list. This is similar to moving malicious files to trusted or unrecognized list from the 'Applications' interface. Refer to the section '**Viewing and Managing Malicious Files**' for more details.

5.1.1.7. Viewing CCS Configurations Exported from the Device and Importing Profiles

ITSM allows you to create a new Windows profile using the existing CCS configuration on an endpoint. This is useful if you want the current configuration on an endpoint to be rolled out to a number of endpoints.

To export a CCS configuration

- Open the Device List interface by clicking Devices > Device List
- Click on the Windows device whose configuration you wish to export to open its 'Device Details' interface

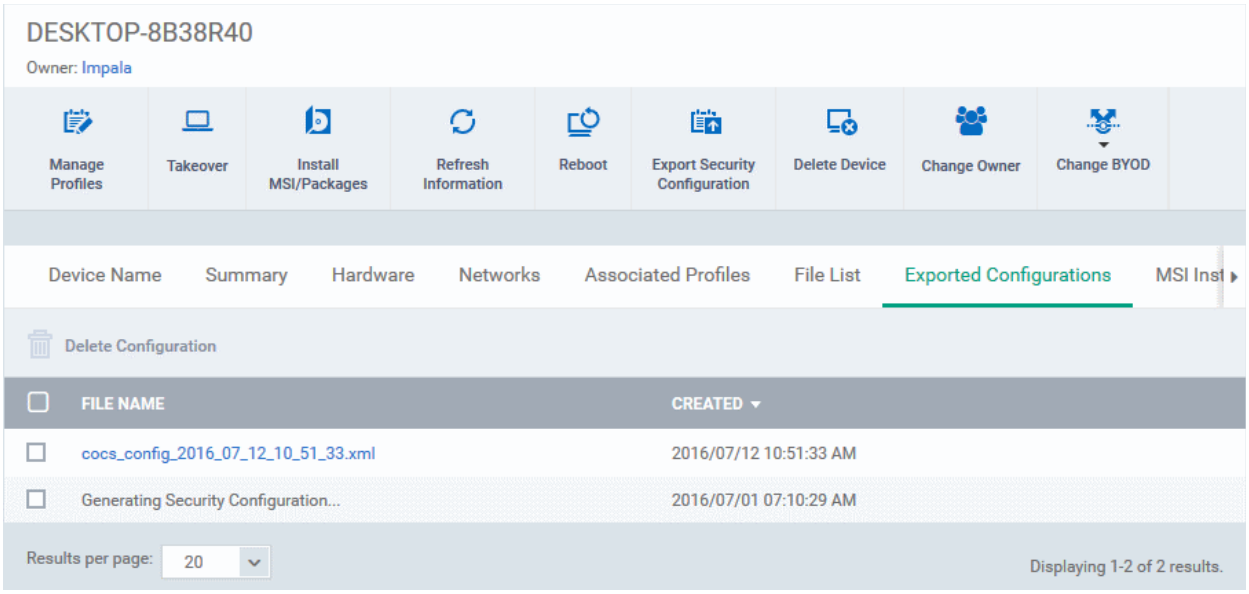


- Click the 'Export Security Configuration' button at the top.

The CCS configuration will be exported as an .xml file with date/time stamp suffix in the file name. The profile will be saved on the ITSM server and can be viewed by clicking the 'Exported Configurations' tab of the device details interface of the same device.

To view and manage exported profiles

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device, then select the "Exported Configurations' tab

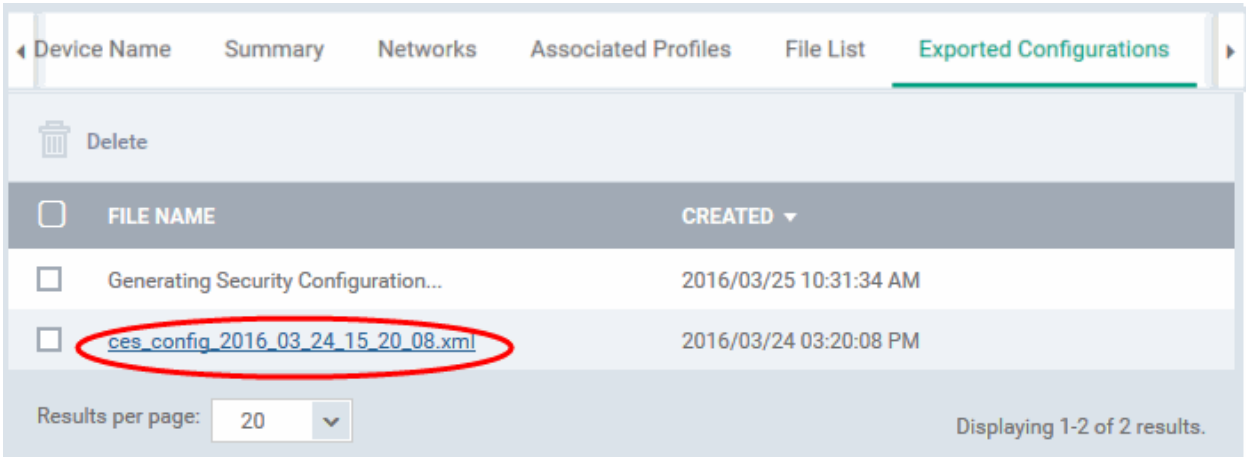


The 'Exported Security Configuration' List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the exported file.
Created	The date and time at which the CCS configuration was exported

- Clicking on any column header sorts the items based on alphabetical or ascending/descending order of entries in that column.

To import and save the security configuration

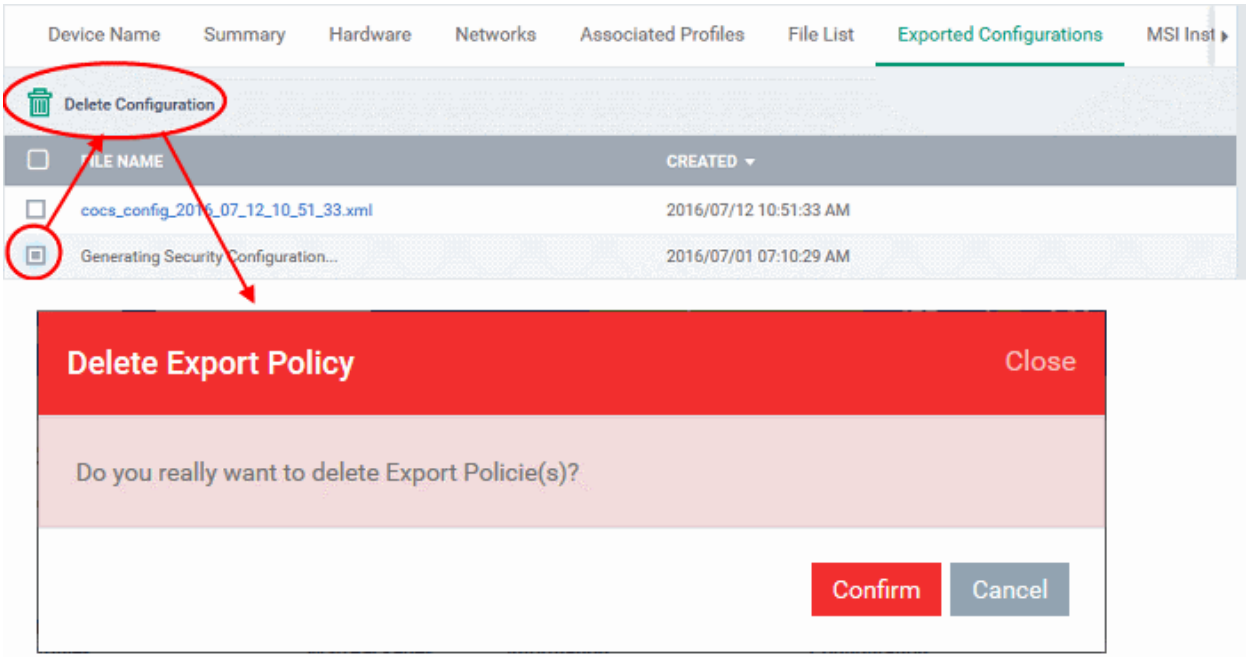
- Click on the file name that you want to import as a profile



The file will be imported as a .xml file.

To import the saved configuration file as a Windows profile, refer to '**Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)** in the section '**Importing Windows Profiles**'.

- To delete a file from the list, select it and click 'Delete'
- Click 'Confirm' to remove the file from the list



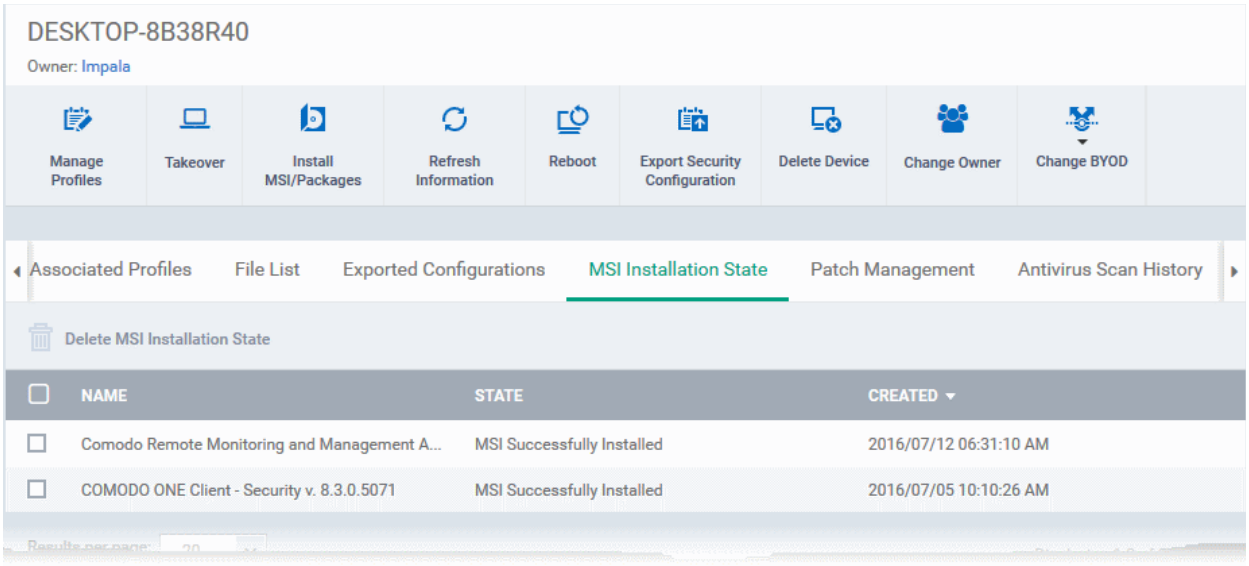
5.1.1.8. Viewing MSI Files Installed on the Device through ITSM

ITSM allows remote installation of ITSM packages like Comodo One Client - Security (COCS) and Remote Monitoring and Management (RMM) agent and third-party MSI packages on to required endpoints. For more information on remote deployment of MSI packages, refer to the section **Remotely Installing Packages onto Windows Devices**.

Administrators can view the list of MSI packages installed on an endpoint through ITSM with the details of them.

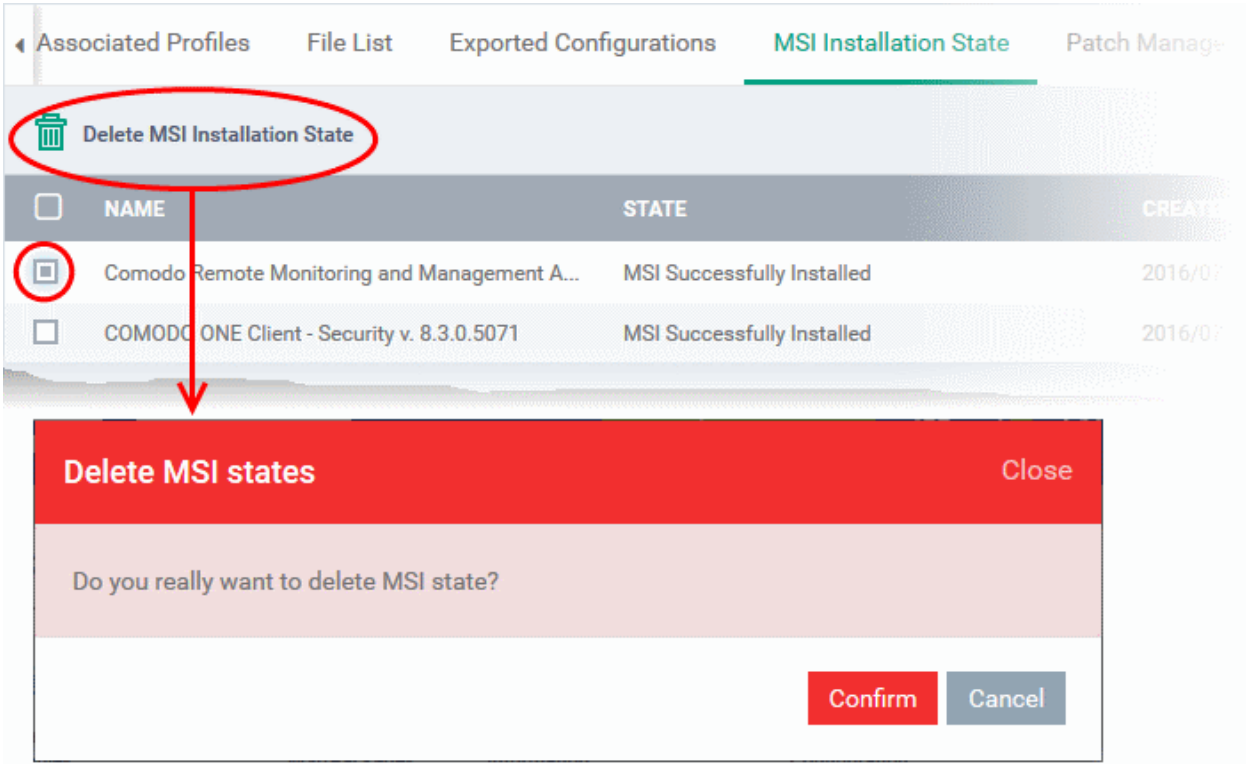
To view MSI file installation list on the device

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device, then select the 'MSI Installation State' tab



MSI Installation State - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the URL/file name of the MSI file.
State	Indicates the installation status of the MSI file.
Created	Indicates the date and time the MSI file installation command was sent.

- Clicking on any column header sorts the items based on alphabetical or ascending/descending order of entries in that column.
- To delete an entry from the list, select it and click 'Delete MSI Installation State'.



Only the chosen entry will be removed from the list but the package will not be uninstalled from the endpoint.

- Click 'Confirm' to remove the file from the list

5.1.1.9. Viewing and Installing Windows Patches

Windows machines have to be kept up-to-date with OS patches in order to protect them from vulnerabilities and malicious attacks. The Patch Management feature allows administrators to view available patches and deploy new patches remotely. Administrators can install multiple patches simultaneously.

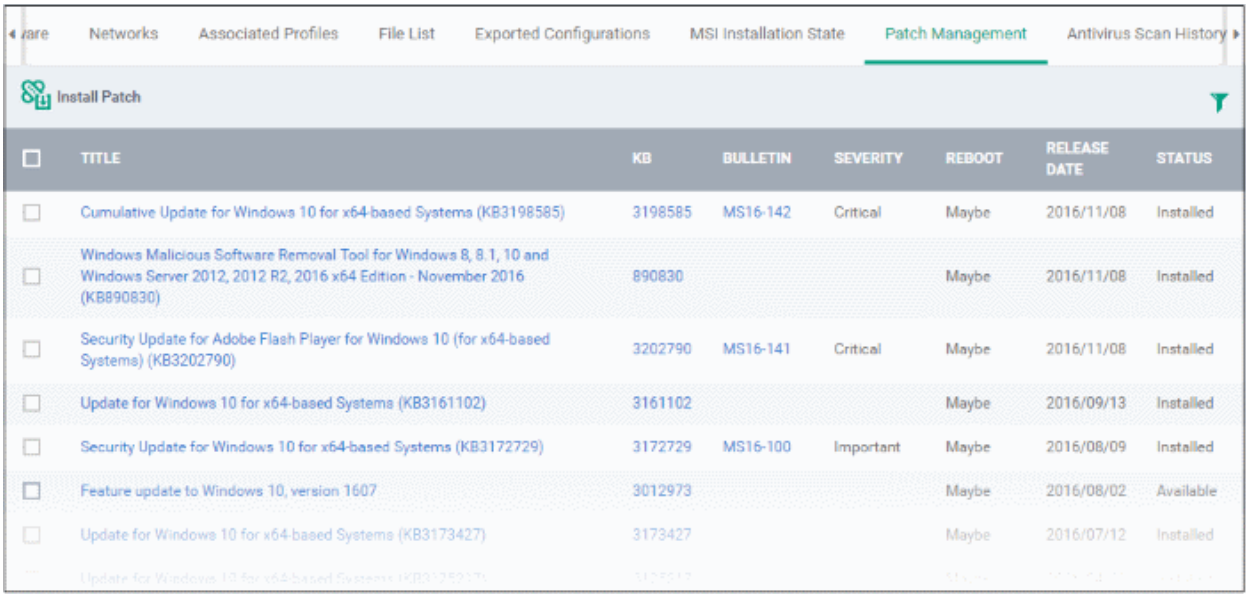
While you can install patches to selected devices from the 'Devices' screen, ITSM also allows you to install patches to all managed endpoints from the 'Applications' section. Refer to '**Installing OS Patches on Windows Endpoints**' for more details.

Important Note: Patches that are hidden by administrators will not be displayed in the device's Patch Management screen. Refer to the section ' **Installing OS Patches on Windows Endpoints**' for more details.

To view and install patches on Windows endpoints

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device to open the device details interface
- Open the 'Patch Management' tab

A list of all previously installed and pending patches will be displayed.

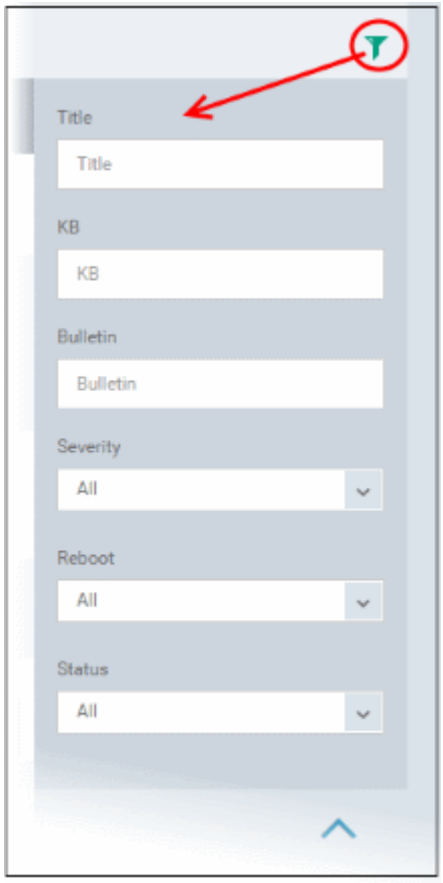


Patch Management Table - Column Descriptions	
Column Heading	**Description**
Title	The name of the patch
KB	Displays the article number of the Microsoft knowledge base article on the patch. Clicking the number takes you to the respective knowledgebase article.
Bulletin	Displays the bulletin number of the Microsoft TechCenter security bulletin on the patch. Clicking the number takes you to the respective security bulletin.
Severity	Indicates the level of severity of the patch as determined by Microsoft. The severity levels are:

	• Unknown • Critical • Important • Low • Moderate • None
Reboot	Indicates whether a reboot is required after patch installation
Release Date	The date on which the patch was released by Microsoft
Status	Indicates the status of installation of the patch on the endpoint.

Sorting, Search and Filter Options

- Clicking any column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- Clicking the funnel icon at the right end opens the filter options.



- To filter or search for a specific patch, start typing the name of the patch then select from the drop-down and click 'Apply'.
  - Title - Filters the items based on the name of the patch
  - KB - Filters the items based on the KB number
  - Bulletin - Filters the items based on the entered bulletin details

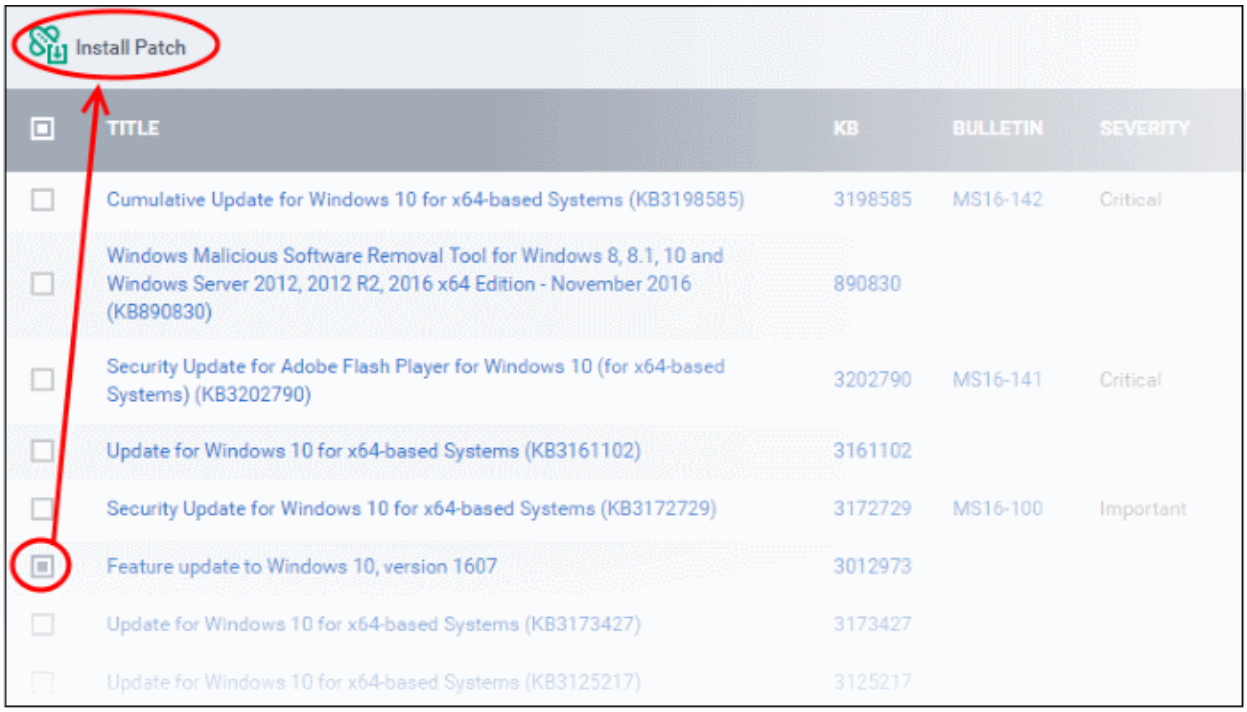
- Severity - Filters the items based on the selected severity level
- Reboot - Filters the items based on the selected reboot option
- Install Status - Filters the items based on the selected installation status(es)

You can use any combination of filters at-a-time to search for a specific patch.

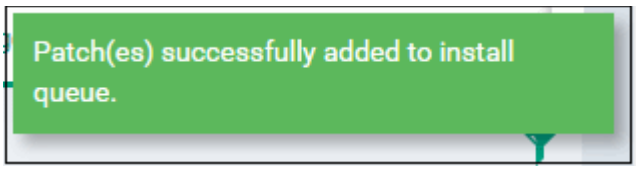
- To display all the items again, remove / deselect the search key from the filters and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

To install patch(es) on an endpoint

- Identify and review patch(es) with a status of 'Available'
  - To simplify this, use the filter funnel to display only patches that are 'Available'
- Select the check-box(es) next to the patches you wish to install
- Click 'Install Patch'



A success message will be displayed.



The command will be sent and a schedule will be created for installation of the selected patch(es) on the endpoint.

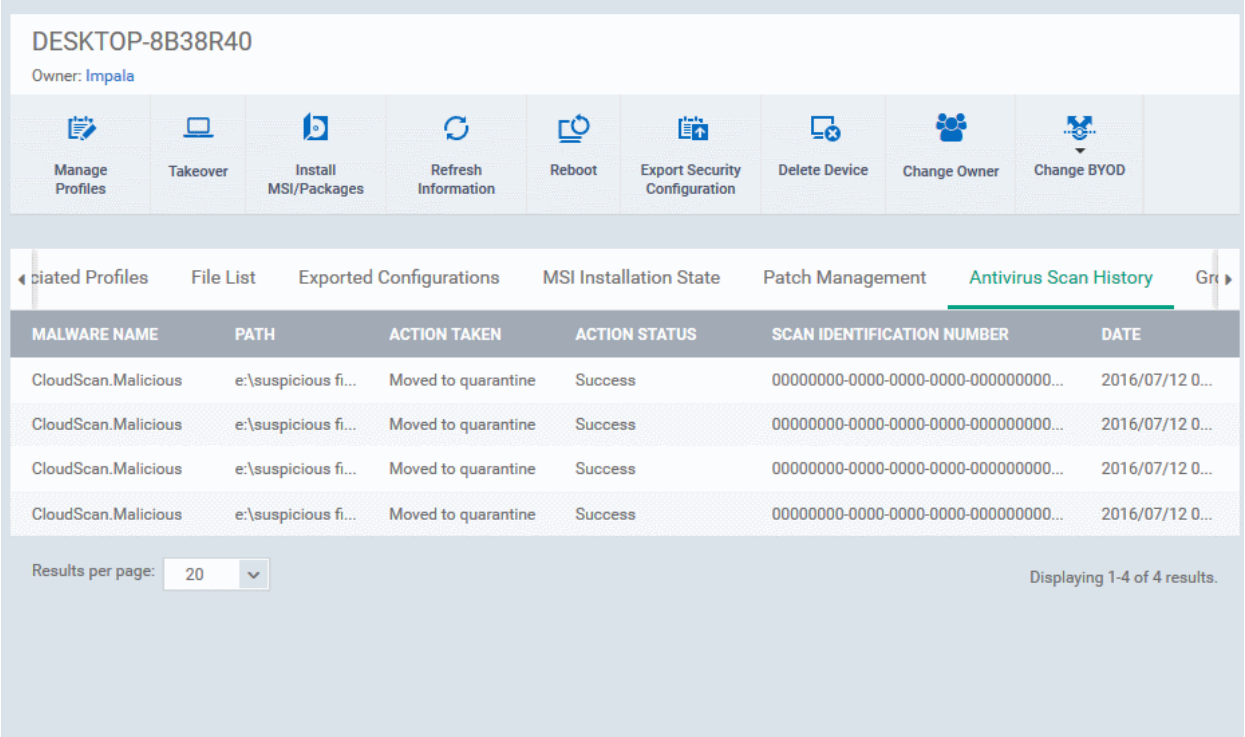
5.1.1.10. Viewing Antivirus Scan History

Administrators can view the threats identified from an endpoint by real-time and on-demand Antivirus scans run on it. The 'Antivirus Scan History' tab of the 'Device Details' interface displays the list of items identified as malware from the endpoint with the details like their installation path and action taken against them.

To view Antivirus Scan history of the device

- Click 'Devices' and choose 'Device List'

- Click the name of the Windows device, then select the 'Antivirus Scan History' tab



Antivirus Scan History- Table of Column Descriptions	
Column Heading	**Description**
Malware Name	Displays the name of the item identified as malicious.
Path	Displays the installation path/storage location malicious item.
Action Taken	Indicates the action that has been taken on the item.
Action Status	Indicates the status of the action taken on the item.
Scan Identification Number	Indicates the a unique identifier assigned to the AV scan during which the item was identified.
Date	Indicates the date and time at which AV scan was performed.

Sorting, Search and Filter Options

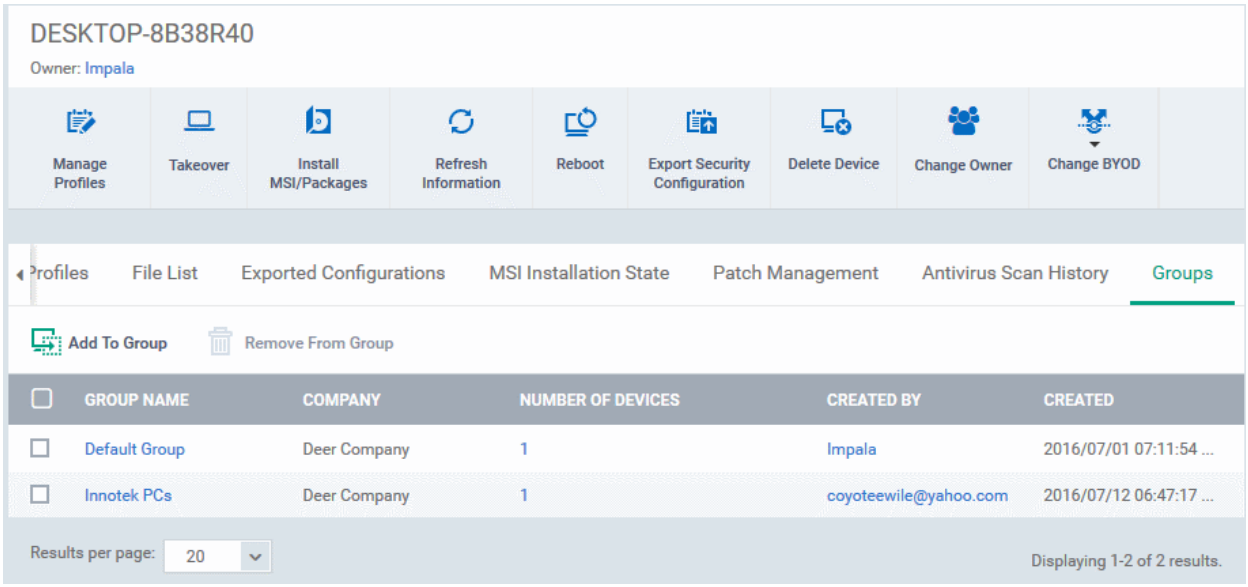
- Clicking on any column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

5.1.1.11. Viewing and Managing Device Group Membership

The 'Groups' tab in the Device Details interface displays a list of device groups to which the Windows endpoint belongs. Administrators can remove the device from a group or add it to a new group.

To view and manage device group membership

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device, then select the 'Groups' tab

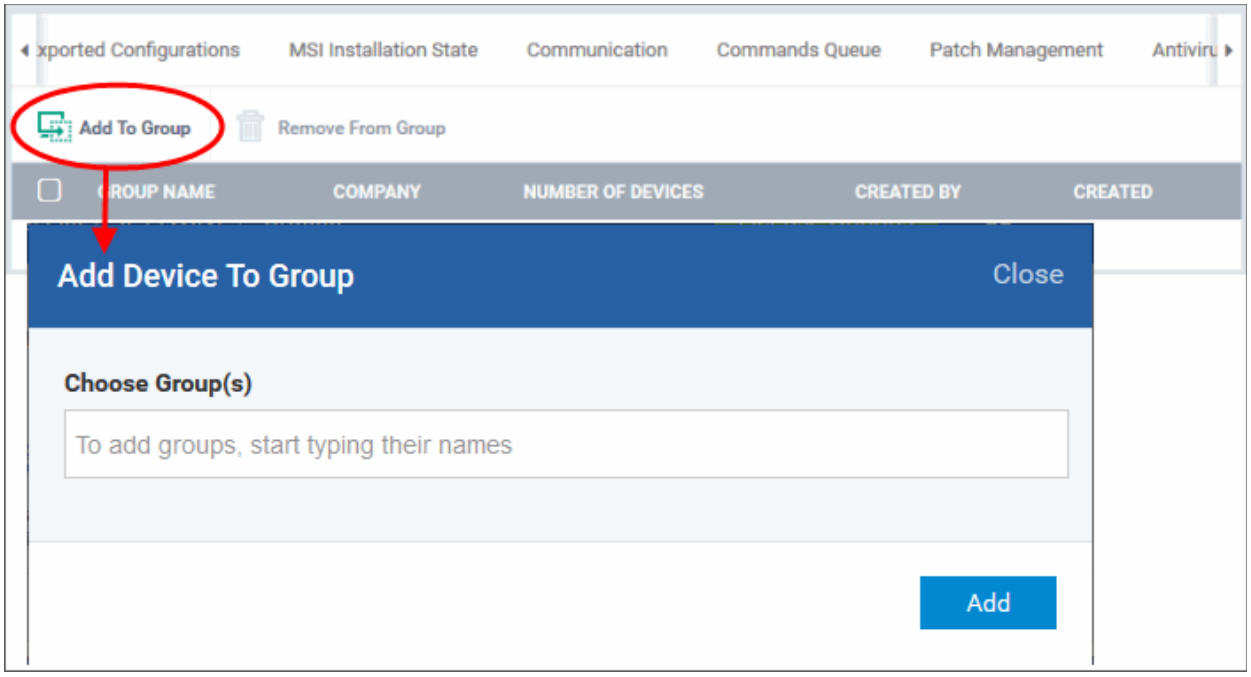


The interface lists those groups of which the device is a member. The groups profiles will be applied to the endpoint. For more details on application of configuration profiles to device groups, refer to the section **Assigning Configuration Profiles to a Device Group**.

Device Groups - Table of Column Descriptions	
Column Heading	**Description**
Group	Displays the name of the group. Clicking the group name allows you to view and edit group details. Refer to the section **Editing a Device Group** for more details.
Company	Displays the name of the company for which the group was created.
Number of Devices	Indicates the total number of devices in the group. Clicking the number allows you to view and edit group details. Refer to the section **Editing a Device Group** for more details.
Created By	Displays the name of the administrator that created the group. Clicking the name will open the user details interface. Refer to the section **Viewing the Details of a User** for more details.
Created	Indicates the date and time at which the group was created.

To add the device to a new group

- Click 'Add to Group'



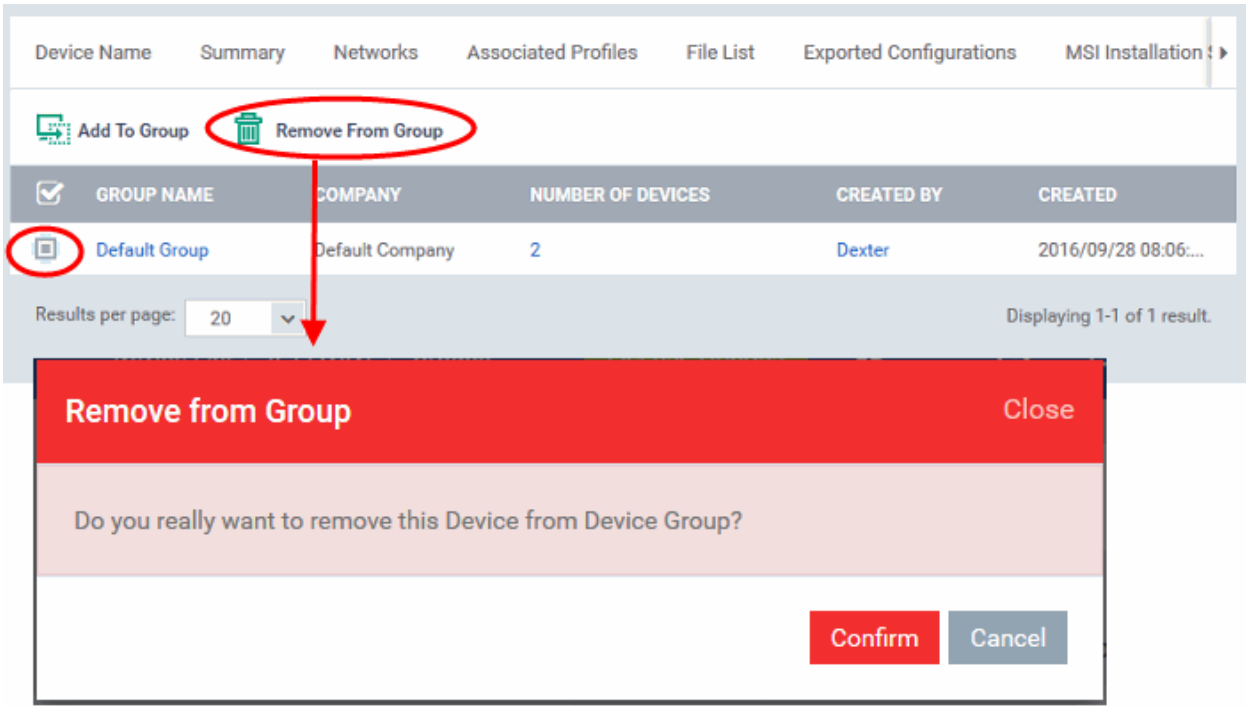
The 'Add Device to Group' dialog will appear.

- Start typing the name of the group which you want the endpoint to join in the 'Choose Group(s)' field. Select the correct group from the list of suggestions.
- Repeat the process to add the device to other groups.
- Click 'Add'.

The device will be added to the group.

To remove the device from a group

- Select the group from the list and click 'Remove from Group'.



A confirmation dialog will appear.

- Click 'Confirm' to remove the device from the group.

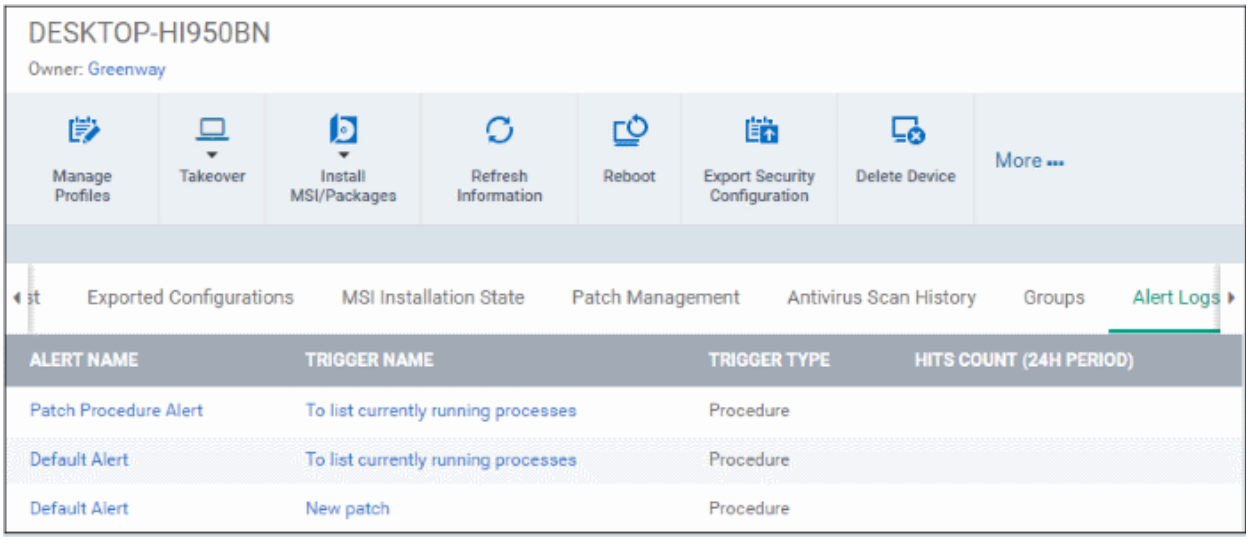
The device will be removed from the group. Group profiles will also be removed from the device.

5.1.1.12. Viewing Alert Logs

The 'Alerts Logs' tab in the Device Details interface displays the details of alerts that were generated for procedure deployment and monitoring parameters conditions breach.

To view alert logs

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device, then select the 'Alert Logs' tab



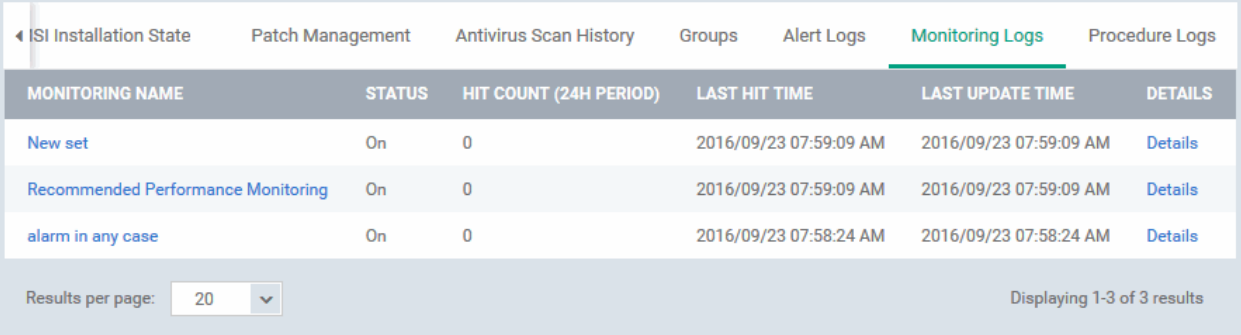
Alert Logs - Table of Column Descriptions	
Column Heading	**Description**
Alert Name	The alert that was generated for the procedure deployment failed and monitoring parameters breach. Different alerts can be configured for different procedures and monitoring parameters breach. Refer to the section 'Managing Alerts' for more details.
Trigger Name	The name of the procedure that failed to run and monitoring conditions that was broken and alert generated. Clicking on the name will take you to the respective parameter settings interfaces.
Trigger Type	Displays the name of the condition that was breached whether monitoring or procedure breach.
Hits Count (24 H Period)	The number of procedure failures and monitoring breaches that occurred during the past 24 hours.

5.1.1.13. Viewing Monitoring Logs

The 'Monitoring Logs' tab shows events detected as breaches on a device. The conditions of a breach are specified in the 'Monitoring' section of the profiles in effect on the device. Logs are displayed for the past 24 hours. For more details on Monitoring Settings, refer to the section Monitoring Settings under Profiles for Windows Devices.

To view monitoring logs

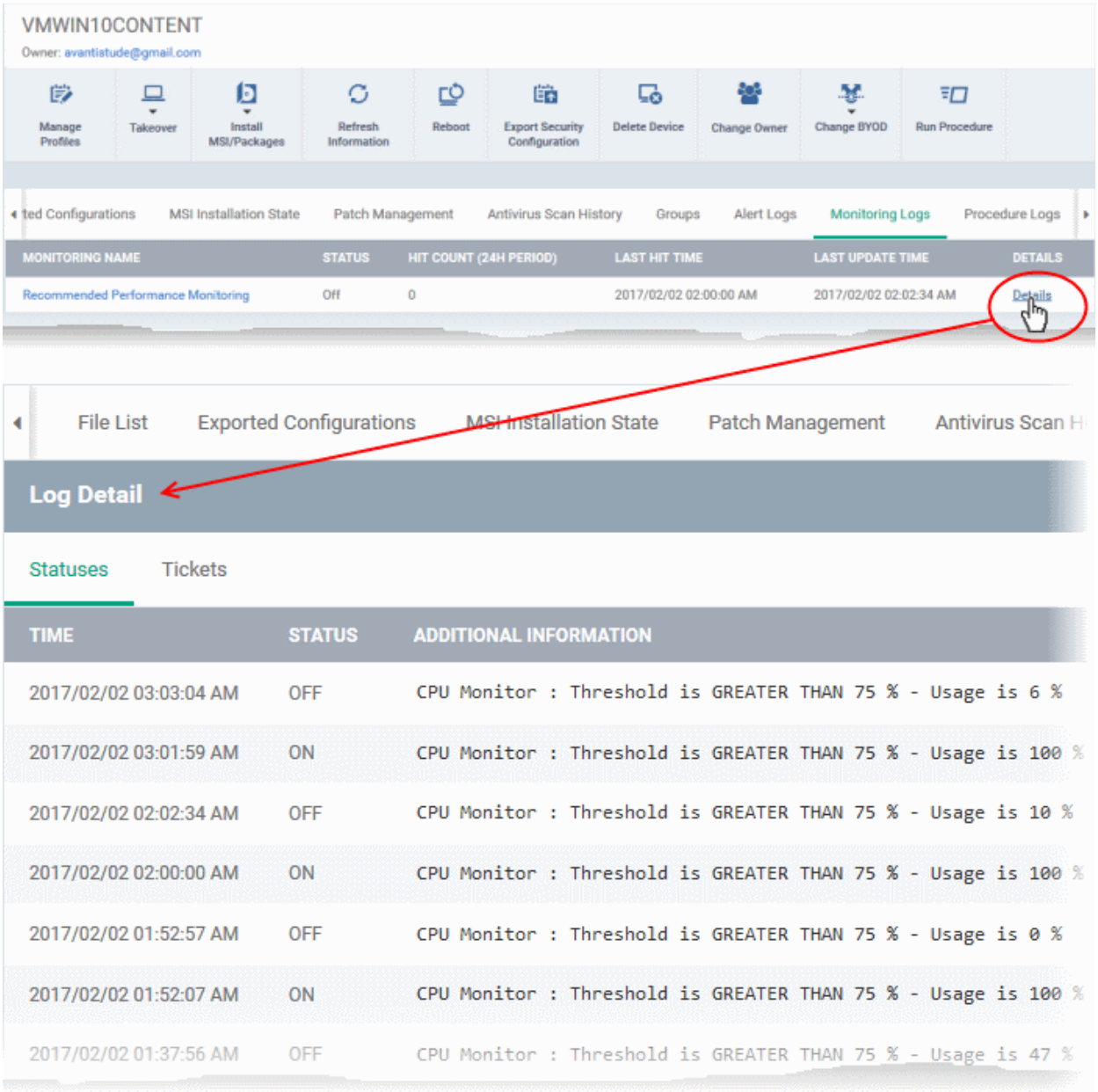
- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device, then select the 'Monitoring Logs' tab



Monitoring Logs - Table of Column Descriptions	
Column Heading	**Description**
Monitoring Name	The name of the monitoring condition in the Windows profile that was violated. Clicking on the name will take to you the monitoring condition configuration screen in the Windows profile. Refer to the section '**Monitoring Settings**' for more details.
Status	Displays the status of the device at the time of last monitoring
Hit Count	Indicates the number of times the monitoring condition was breached during the last 24 hours.
Last Hit Time	Displays the date and time the monitoring rule was broken last.
Last Update Time	Indicates the date and time when the information was updated last.
Details	Clicking the 'Details' link opens the log related to the breach. Refer to the explanation of **Viewing Details of Monitoring Logs** given below.

Viewing Details of Monitoring Logs

- To view the conditions of a monitoring rule, click the 'Details' link:

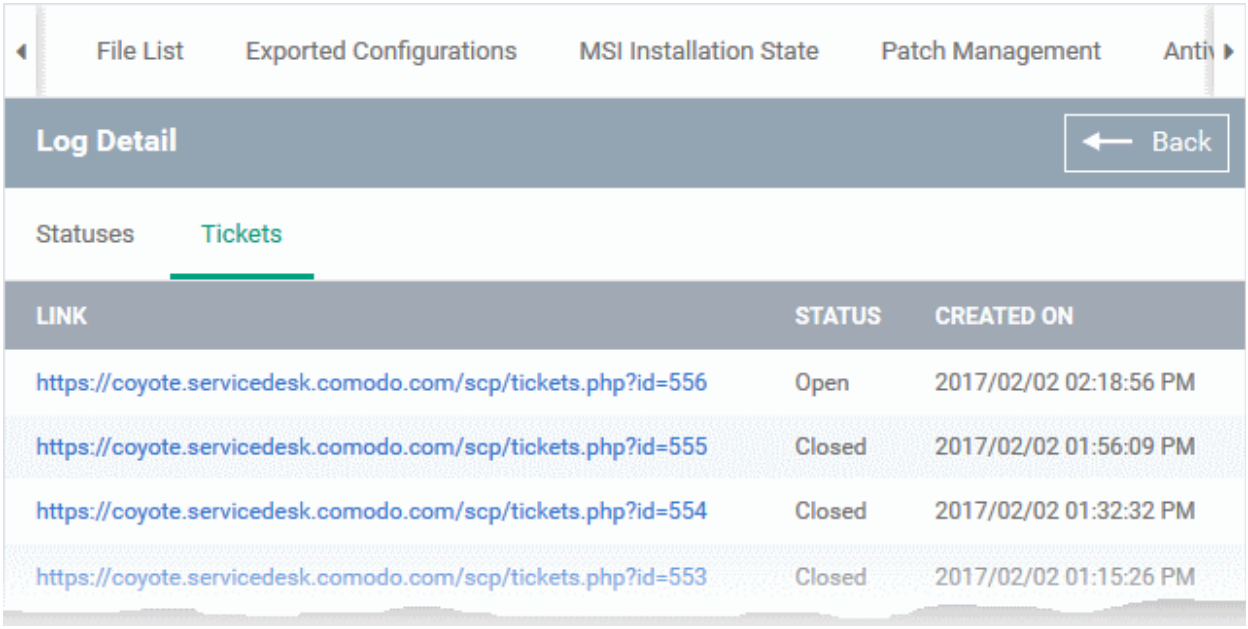


Details are displayed under two tabs:

Statuses - Displays the date and time when the breach occurred. Also displays details of the monitoring rule that was broken.

Monitoring Log Details - 'Statuses' tab - Table of Column Descriptions	
Column Heading	**Description**
Time	Precise date and time of the breach event.
Status	Displays the status of the device at the time of monitoring.
Additional Information	Provides details on the condition monitored and the breach

Tickets - Details about any tickets raised for the alert. This includes ticket links which open the respective ticket in service desk.



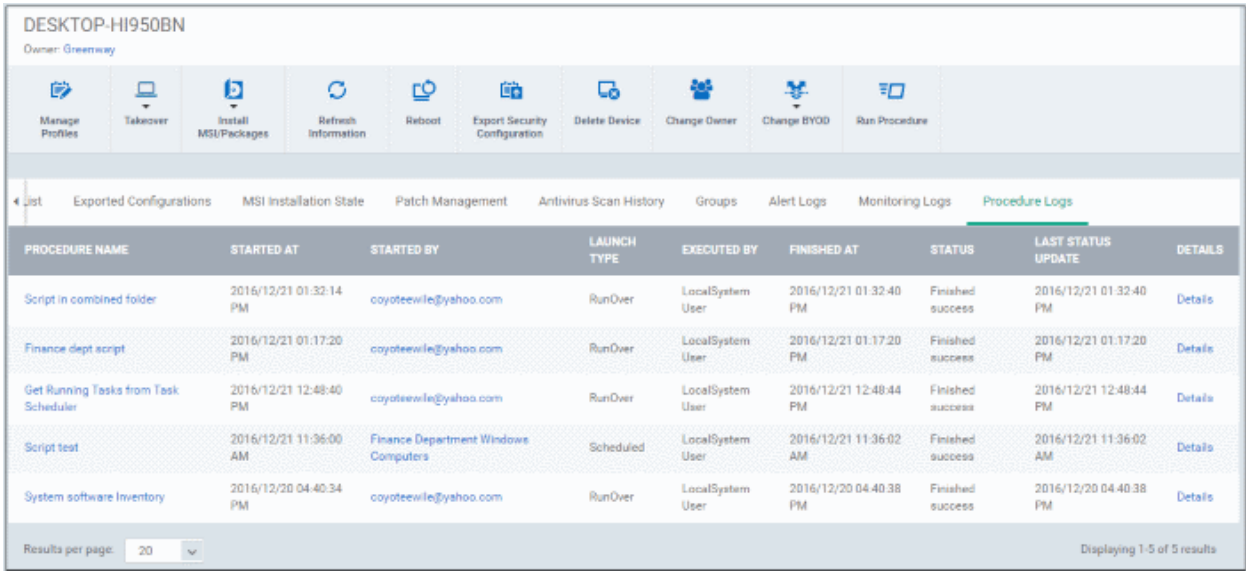
Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions	
Column Heading	**Description**
Link	A link to the support ticket created for the breach event. Clicking the link will open the ticket in service desk.
Status	Displays whether the ticket is open or closed
Created On	Displays the precise date and time at which the ticket was created.

5.1.1.14. Viewing Procedures Logs

The 'Procedure Logs' tab shows script procedures that were manually run on Windows devices as well as those run automatically via a profile. Patch procedure logs can be viewed from the patch procedure interface itself. Refer to 'Viewing Patch Procedure Results' in the section 'Viewing Procedure Results'.

To view procedures logs

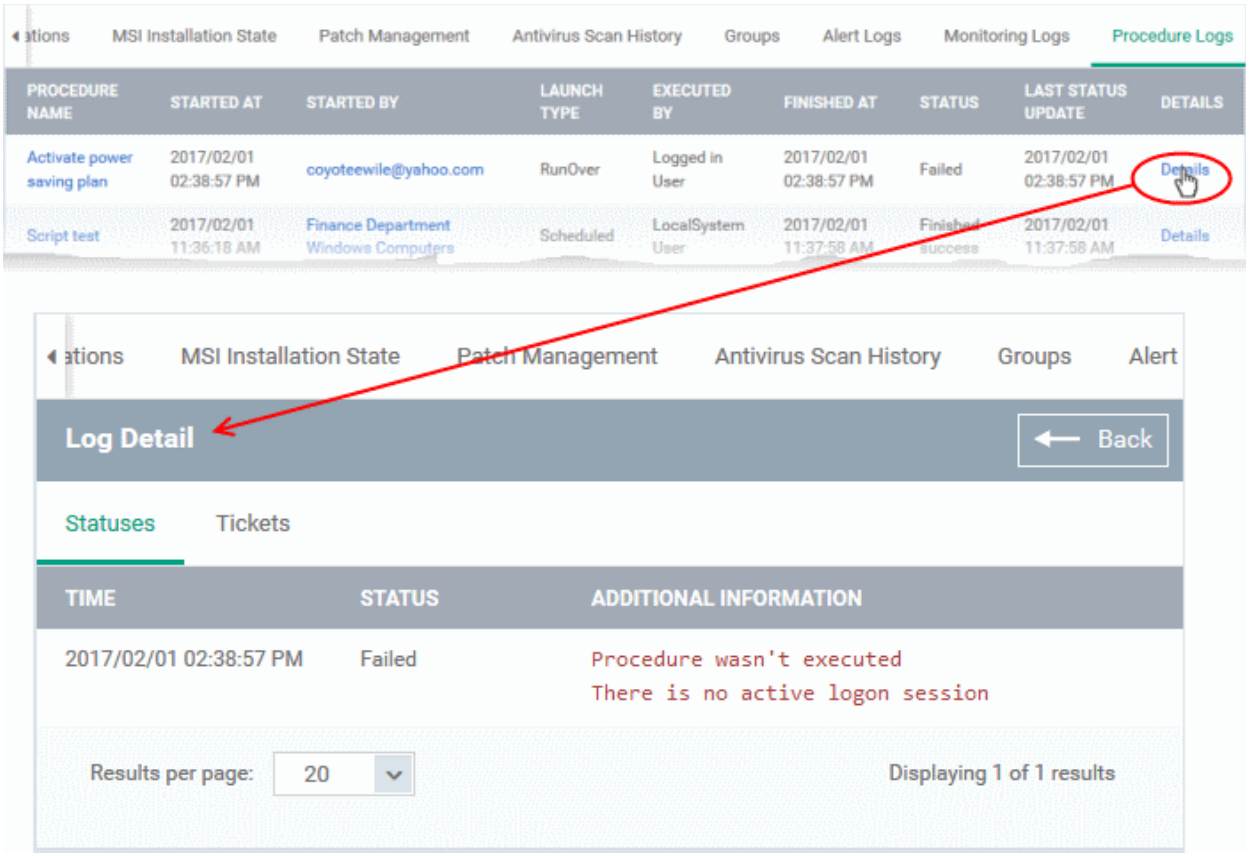
- Click 'Devices' and choose 'Device List'
- Click on a Windows device, then select the 'Procedure Logs' tab



Procedure Logs - Table of Column Descriptions	
Column Heading	**Description**
Procedure Name	The name of the procedure that was run on the device. Clicking the name will take you to the respective procedure management screen. Refer to the section 'Managing Procedures' for more details.
Started At	The date and time when the procedure commenced.
Started By	Indicates how the procedure was launched whether by an administrator manually or scheduled in a profile. If scheduled in a profile, its name will be displayed. If run manually, the logged in name of the administrator will be displayed. Clicking the profile name will take you to the page at Procedure Settings of the Windows profile and clicking the user name will take you to the User Details page.
Launch Type	Indicates how the procedure was started whether scheduled or run manually.
Executed By	Type of user that executed the procedure.
Finished At	The date and time when the procedure was completed.
Status	Indicates the status of the procedure deployment whether fail or success. You can configure to generate an alert if a procedure deployment fails. Refer to the section 'Managing Procedures' for more details.
Last Status Update	Indicates the date and time when the information was updated last.
Details	Click the 'Details' link to view a log of the procedure's execution. Refer to the explanation of Viewing Details of Procedure Logs given below.

Viewing Procedure Log details

- Click the 'Details' link to view details about a procedure's execution:

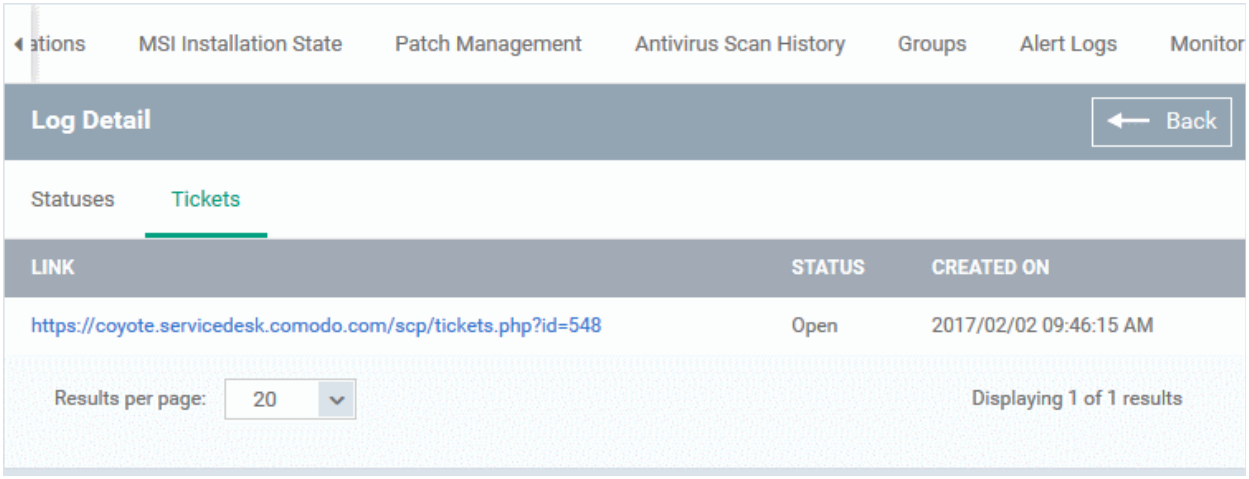


The details are displayed under two tabs:

Statuses - Displays the precise date and time at which the procedure was run, its success status and results.

Procedure Log Details - 'Statuses' tab - Table of Column Descriptions	
Column Heading	**Description**
Time	Precise date and time of the procedure execution.
Status	Indicates whether the execution was successful or not.
Additional Information	Provides details on the execution: • If failed, displays the reason for not running the procedure • If successful, displays the results of the procedure execution

Tickets - Displays tickets raised for any failed procedures.



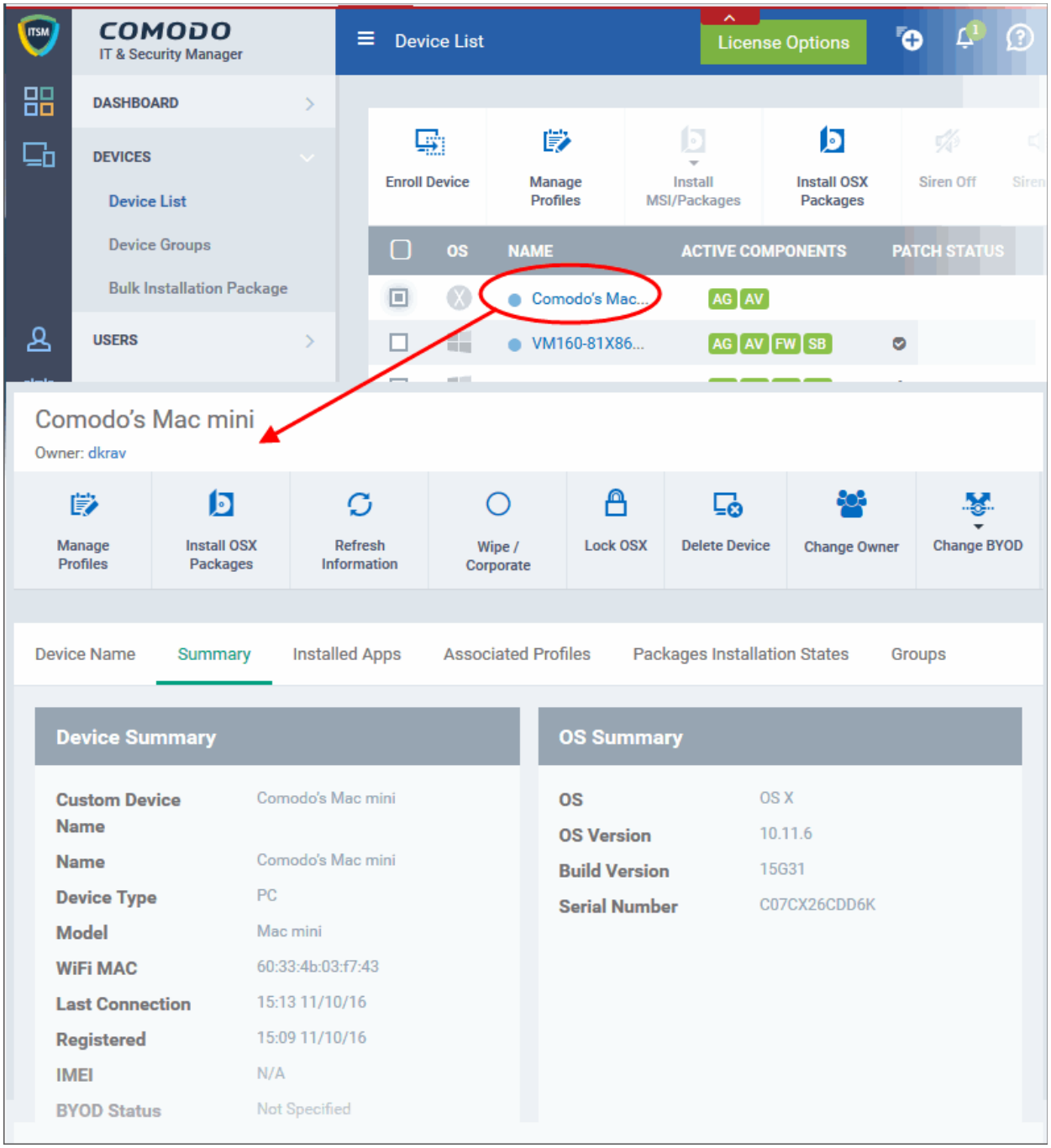
Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions	
Column Heading	**Description**
Link	Links to the support ticket created for the failed execution of the procedure. Clicking the link will the respective ticket in the Service Desk interface.
Status	Displays whether the ticket is open or closed
Created On	Displays the precise date and time at which the ticket was created.

5.1.2. Managing Mac OS Devices

The Mac OS device details page allows administrators to view OS and software details, installed applications, security information from Comodo Antivirus. network connection details and more. Administrators can also manage configuration profiles in effect on the endpoint, remotely install OSX packages and manage group membership.

To view and manage a Mac OS device

- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS device

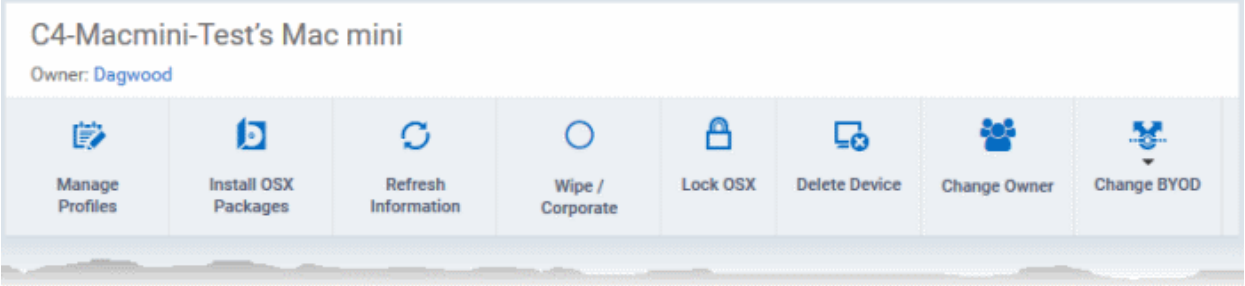


The Mac OS device details pane will open, displaying details of the selected device under six tabs. By default, the 'Summary' tab will be displayed.

- **Device Name** - Displays the name of the device. You can change this as per your preferences. Refer to the section **Viewing and Editing Mac OSX Device Name** for more details.
- **Summary** - Displays general details of the device including device information, OS details, Network details and security configuration. Refer to the section **Viewing Summary Information** for more details.
- **Installed Apps** - Displays a list of applications currently installed on the device, along with their versions. Refer to the section **Viewing Installed Applications** for more details.
- **Associated Profiles** - Displays details of the profiles deployed on the device. Refer to the section **Viewing and Managing Profiles Associated with the Device** for more details.
- **Package Installation State** - Displays Mac OS packages that have been installed on the device via ITSM. Refer to the section **Viewing OSX Packages Installed on the Device through ITSM** for more details.
- **Groups** - Displays a list of device groups to which the endpoint belongs and allows administrators to

manage group membership. Refer to the section Viewing and Managing Device Group Memberships for more details

Administrators can remotely perform various tasks on the device using the options at the top of the interface.



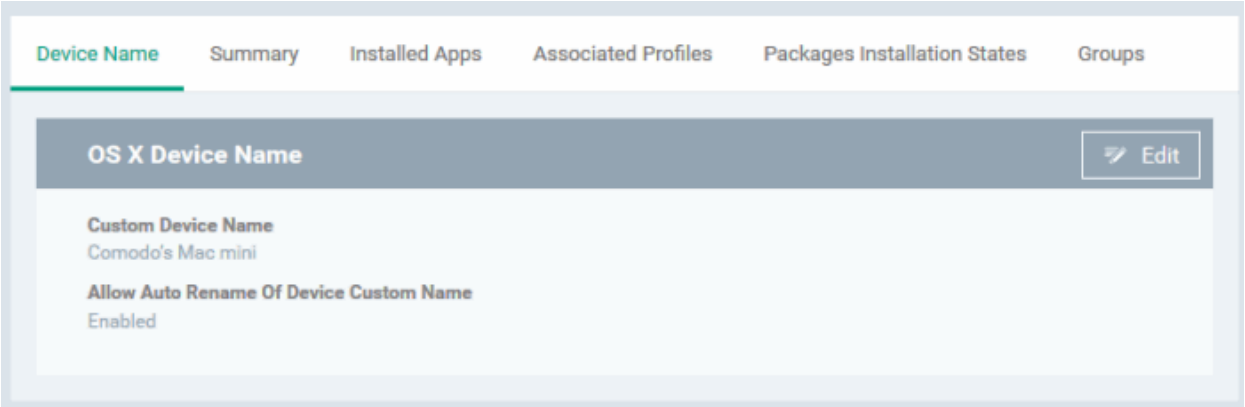
- Manage Profiles - Allows you to add or remove device profiles. Refer to the section Assigning Configuration Profiles to Selected Devices for more details.
- Install OSX Packages - Allows you to remotely install Comodo Antivirus for Mac and other Mac OSX packages. Refer to the section Remotely Installing Packages onto Mac OS Devices for more details.
- Refresh Information - Contacts the device and updates displayed information. Refer to the section Updating Device Information for more details.
- Wipe / Corporate - Allows you to delete data stored on the device if it is lost or stolen. Refer to the section Wiping Data from Devices for more details
- Lock/Unlock OSX - Allows you to remotely lock or unlock the device if it is lost, misplaced or stolen. Refer to the section Locking/Unlocking Devices for more details
- Delete Device - Removes the device from ITSM. Refer to the section Removing a Device for more details.
- Change Owner - Allows you to change the user to whom the device is associated. Refer to the section Changing a Device's Owner for more details.
- Change BYOD - Changes the BYOD status of the device. Refer to the section 'Changing BYOD status of a Device' for more details.

5.1.2.1. Viewing and Editing Mac OSX Device Name

Enrolled devices are listed by the name assigned to them by their owner or by model number if no name was assigned. Admins can change device name according to their preferences. If you change a device name, the name will apply in ITSM but will not change the name on the endpoint itself.

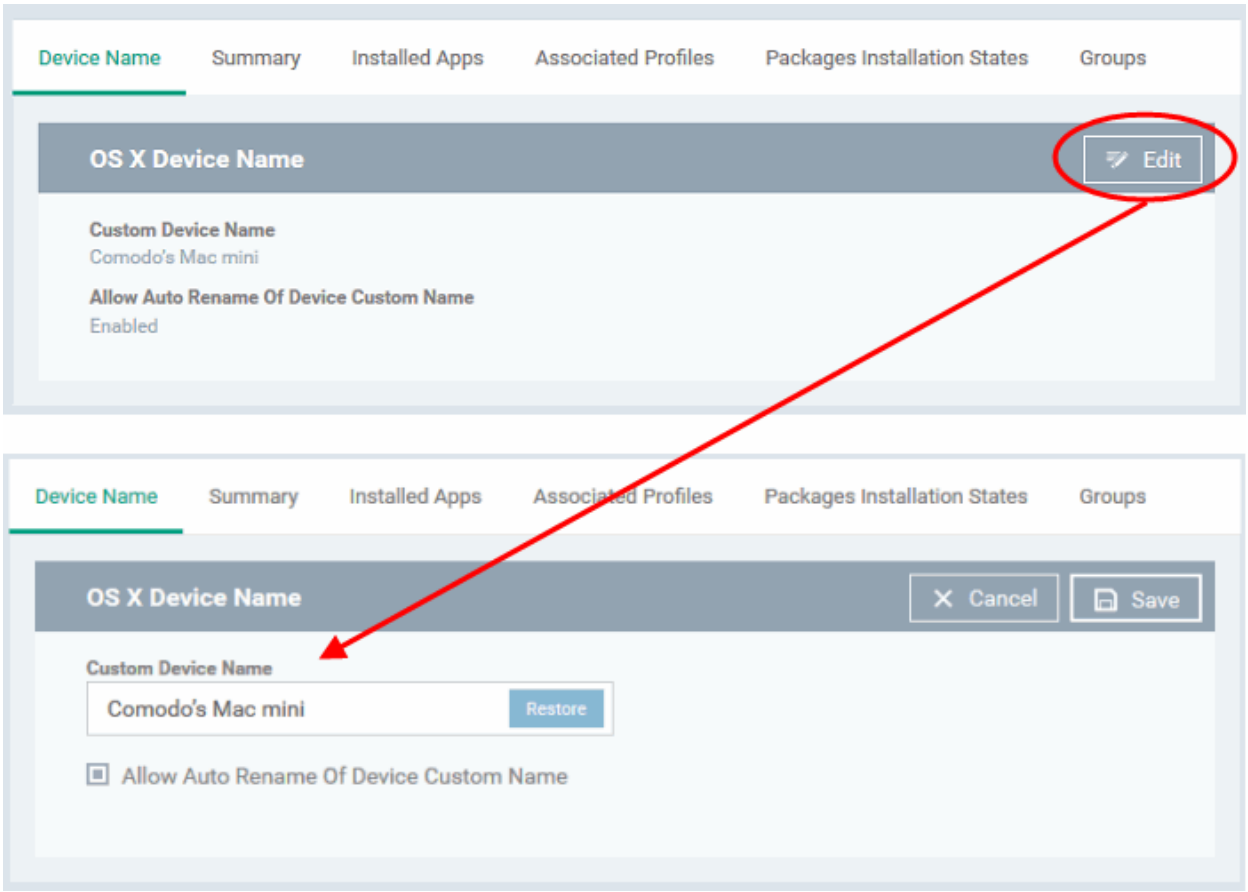
To change a device name

- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS device then select the 'Device Name' tab from the 'Device Details' interface



- Custom Device Name - The current name of the device

- Allow Auto Rename of Device Custom Name - Indicates whether the device's name can be changed or not.
- To change the name of the device, click the 'Edit' button at the right.



- Enter the new name in the 'Custom Device Name' field
- Make sure the 'Allow Auto Rename of Device Custom Name' is enabled.
- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

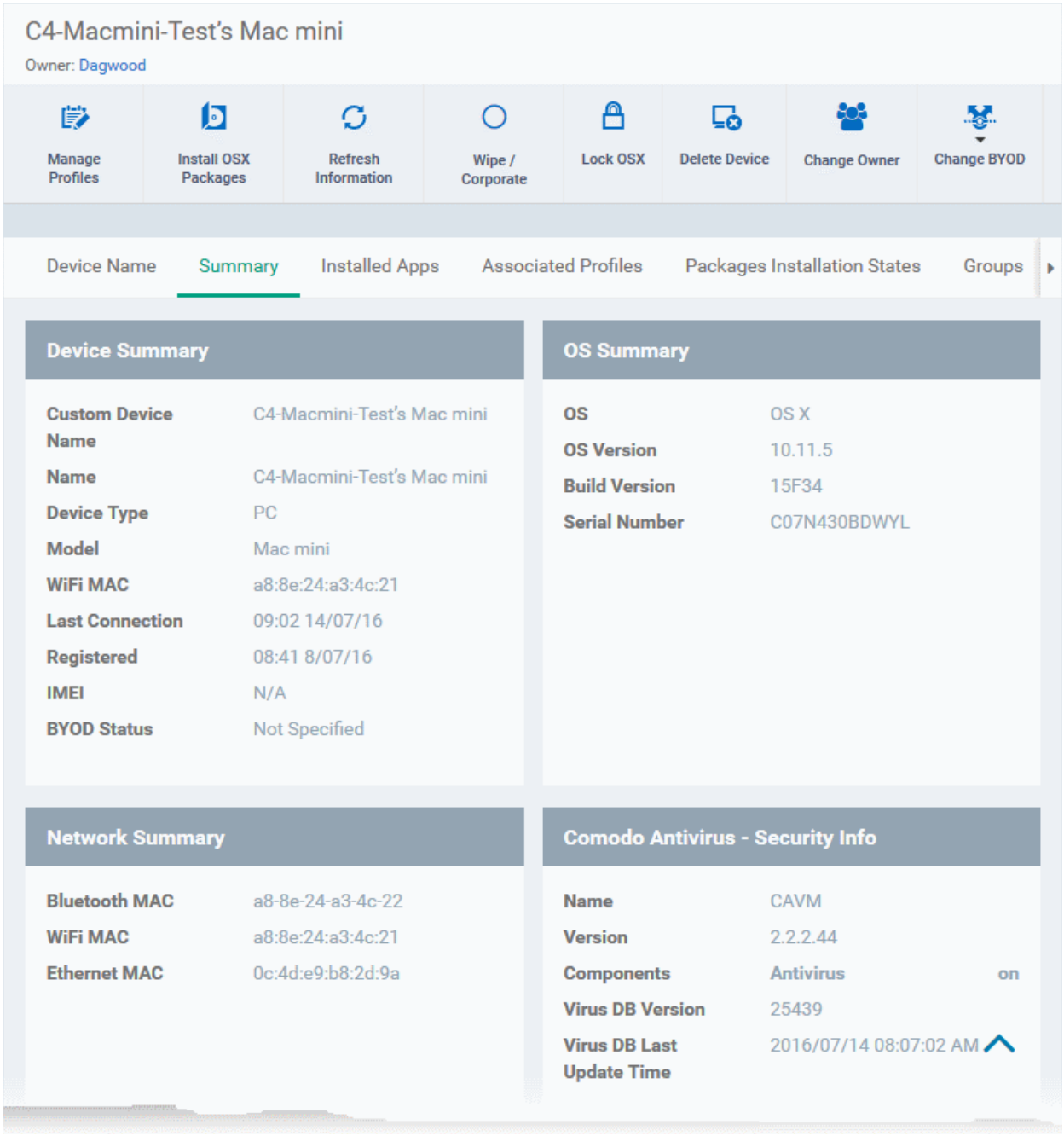
- To restore the name of the device as it was at the time of enrollment, click 'Edit' from the 'Device Name' interface, click 'Restore' at the right and click 'Save'.

5.1.2.2. Viewing Summary Information

The 'Summary' tab displays general information about the device, its operating system, network and installed Comodo software.

To view the device information summary

- Click 'Devices' and choose 'Device List'.
- Click the name of the Mac OS device. Open the 'Summary' tab (if it is not already open).



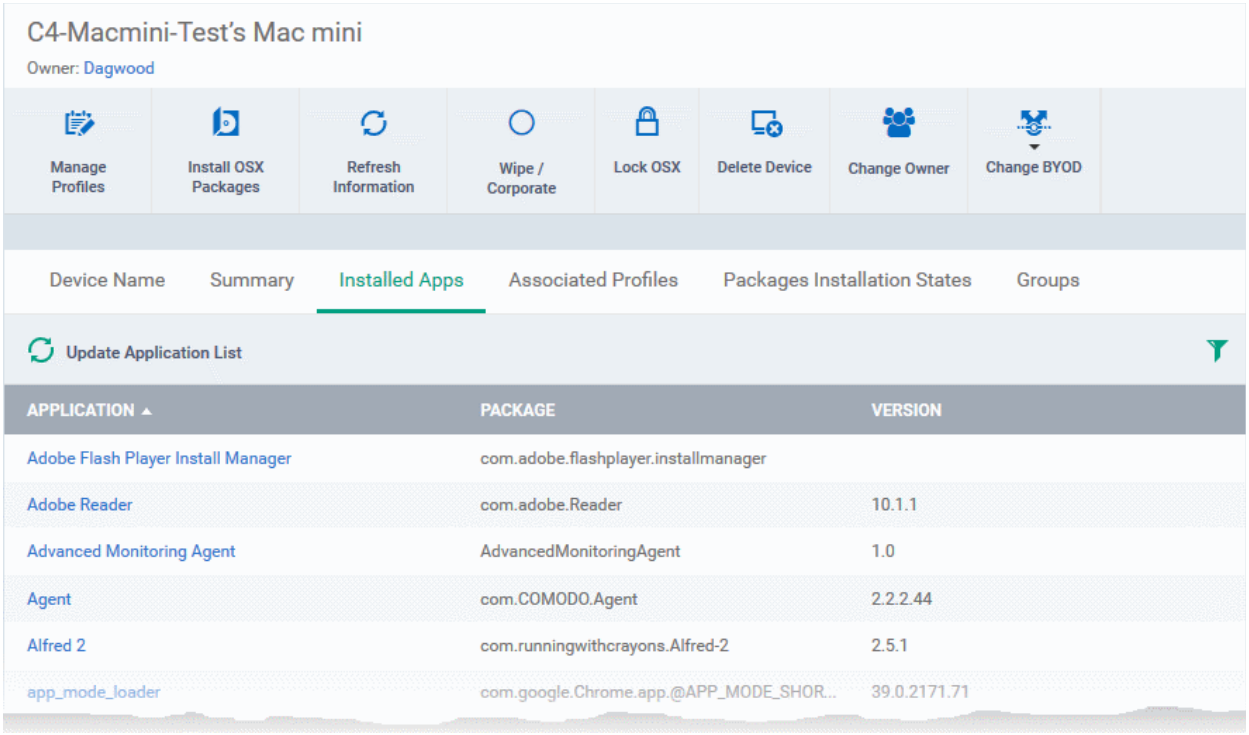
- **Device Summary** - Provides details such as device name, type, model, last polling time of the Comodo Client, BYOD status and more.
- **OS Summary** - Provides details about the Operating System (OS) of the device, OS version and Build version
- **Network Summary** - Displays the MAC addresses of the device for connection through Bluetooth, WiFi and Ethernet to the network.
- **Comodo Antivirus** - Security Info - Displays details about the Comodo Antivirus for Mac (CAVM) installed on the device, its versiin number, virus database version and its update status.

5.1.2.3. Viewing Installed Applications

Administrators can view the list of applications installed on any managed Mac OS device from the Device Details interface.

To view the list of applications

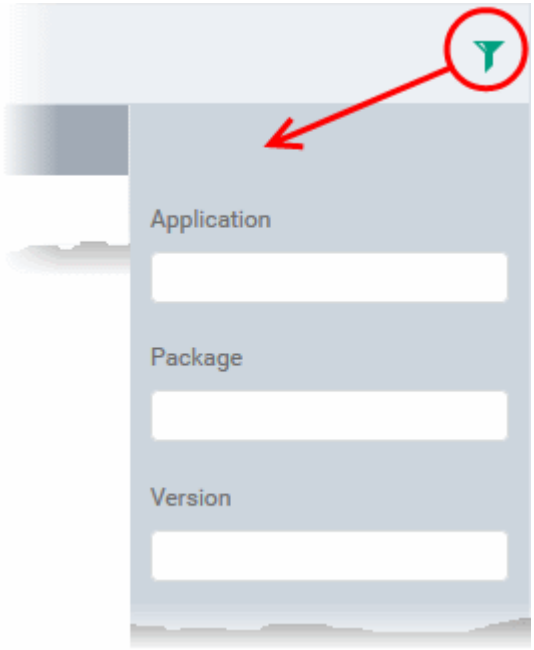
- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS device then select the 'Installed Apps' tab



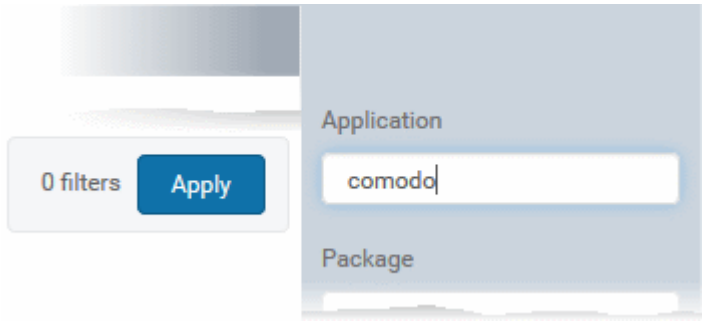
Installed Apps - Column Descriptions	
Column Heading	**Description**
Application	The name of the application. Clicking the name of the application will open the 'Devices' interface, listing only the devices in which the same application is installed.
Package	Indicates the source of the application, i.e downloaded OSX package, from which the application was installed.
Version	Indicates the version number of the application.

Sorting and Filtering Options

- Clicking on any column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel icon at the right end opens the filter options.



- To filter the items or search for a specific item based on the app name, package or version, enter the search criteria in full or part in the respective text box and click 'Apply'



You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.
- To reload the list with latest applications, click 'Update Application List'

5.1.2.4. Viewing and Managing Profiles Associated with the Device

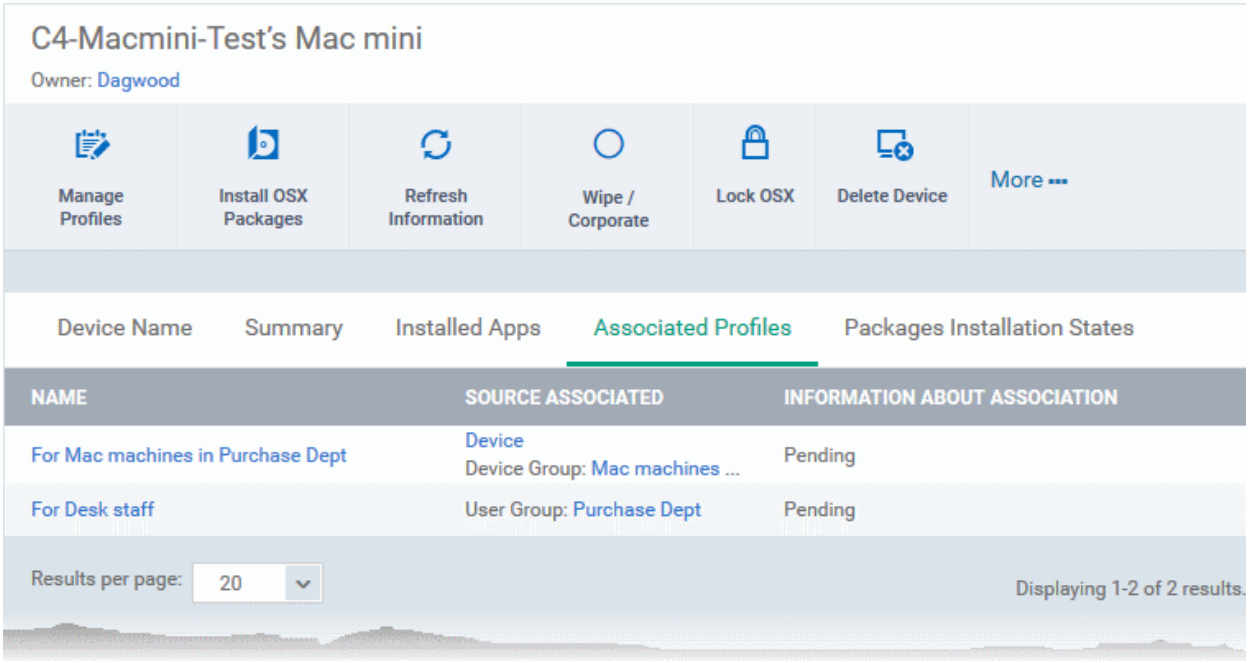
The 'Associated Profiles' tab displays a list of all currently active configuration profiles on an endpoint. A profile may have been applied for any of the following reasons:

- Because it is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- Because the device belongs to a device group
- Because the user belongs to a user group

For more details on profiles and groups of profiles, refer to the chapter Configuration Profiles.

To view and manage the profiles associated with a device

- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS endpoint, then select the 'Associated Profiles' tab



Associated Profiles - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section **Editing Configuration Profiles** for more details.
Source Associated	Indicates the source through which the profile has been applied to the device. Configuration profiles are applied to a device in different ways: • Profiles can be directly applied to the device. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. Refer to the section **Assigning Configuration Profile(s) to a Users' Devices** for more details • Profiles applied to a user group are deployed to all devices owned by group members. Refer to the section **Assigning Configuration Profile to a User Group** for more details • Profiles applied to a device group are deployed to all member devices in the group. Refer to the section **Assigning Configuration Profile to a Device Groups** for more details Clicking on the source opens the respective details interface.
Information about Association	Indicates the status of profile application to the device.

- Clicking the 'Name' column header sorts the items in the alphabetical order of the names of the items

Adding or Removing Profiles

Profiles can be added or removed from the device clicking 'Manage Profiles' option at the top. Refer to the section **Assigning Configuration Profile to Selected Devices** for more details.

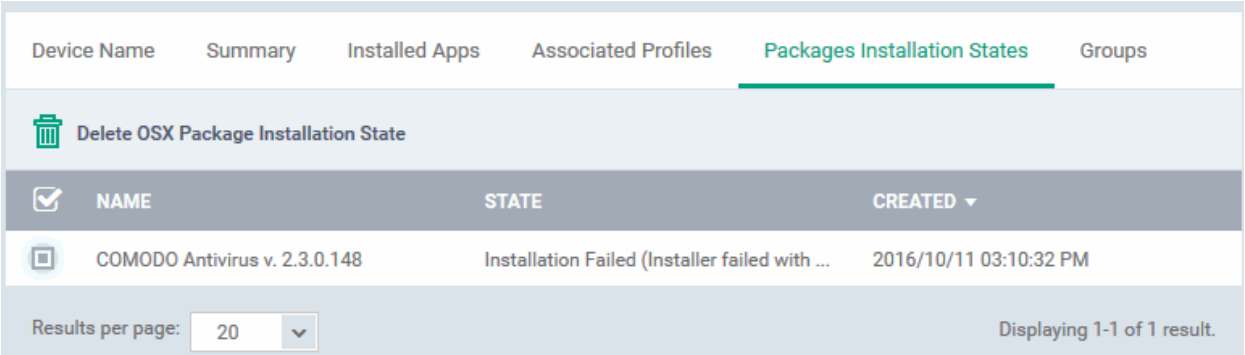
5.1.2.5. Viewing OSX Packages Installed on the Device through ITSM

ITSM allows remote installation of ITSM packages like Comodo Antivirus for Mac (CAVM) and third-party OSX packages on to required Mac OS endpoints. For more information on remote deployment of OSX packages, refer to the section Remotely Installing Packages on Mac OS Devices.

Administrators can view the list of OSX packages installed on an endpoint through ITSM with the details of them.

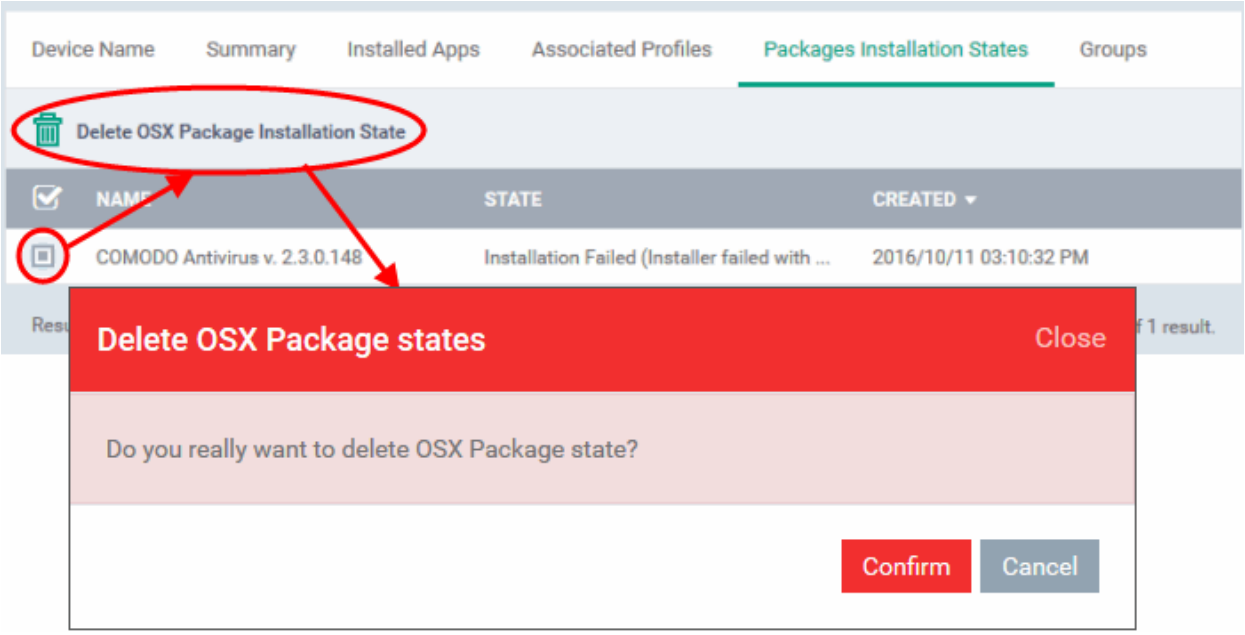
To view list of OSX packages installed on an endpoint through ITSM

- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS device, then select the 'Packages Installation States' tab



MSI Installation State - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the URL/file name of the OSX package.
State	Indicates the installation status of the package.
Created	Indicates the date and time at which the installation command was sent.

- Clicking on any column header sorts the items based on alphabetical or ascending/descending order of entries in that column.
- To delete an entry from the list, select it and click 'Delete OSX Package Installation State'.



Only the chosen entry will be removed from the list but the package will not be uninstalled from the endpoint.

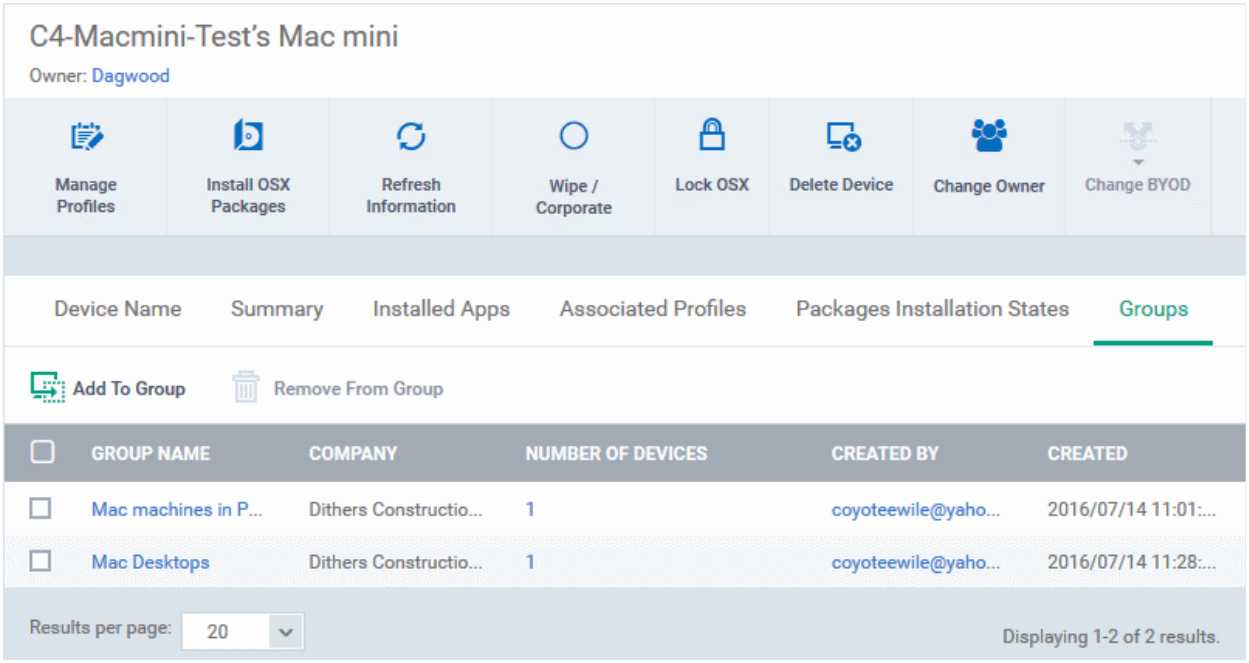
- Click 'Confirm' to remove the file from the list

5.1.2.6. Viewing and Managing Device Group Memberships

The 'Groups' tab in the Device Details interface displays a list of device groups to which the Mac OS endpoint is associated. Administrators can remove the membership of the device from a group or add the device to a new group from this interface.

To view and manage the device group membership

- Click 'Devices' and choose 'Device List'
- Click the name of the Mac OS device, then select the 'Groups' tab

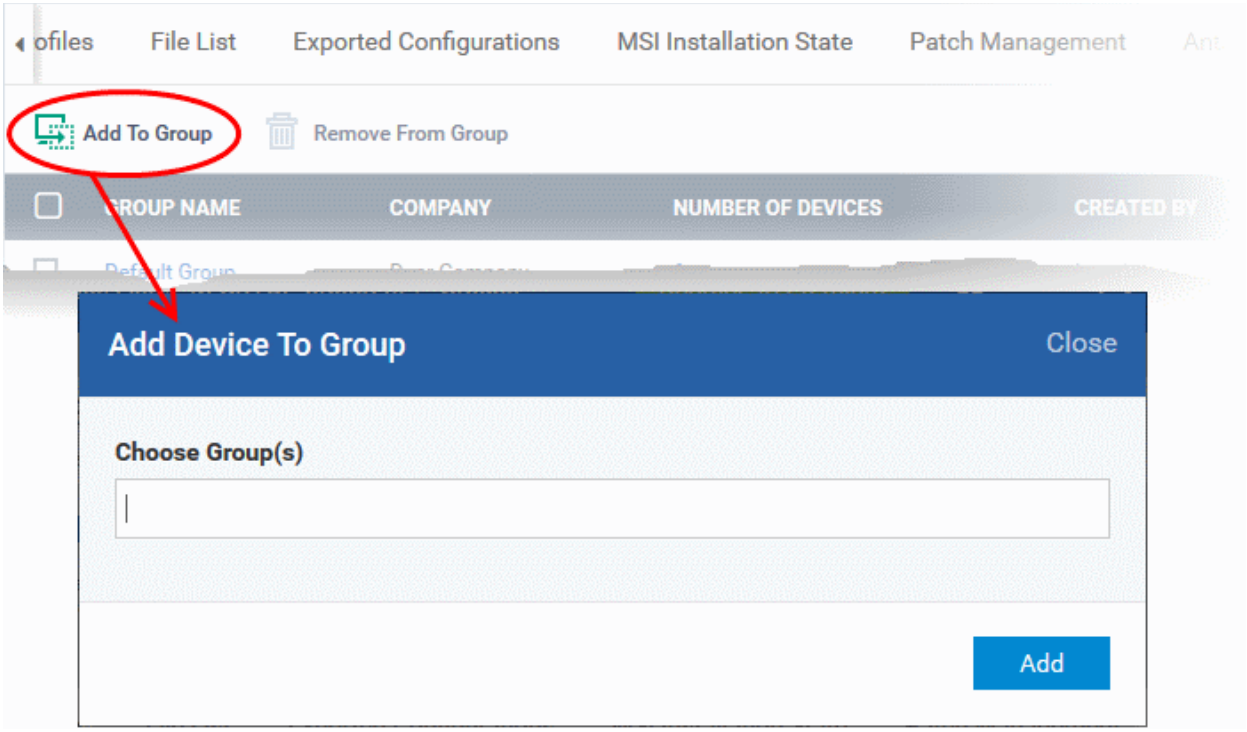


The interface displays the list of device groups to which the device is a member. The endpoint will be applied with all configuration profiles associated with each group. For more details on application of configuration profiles to device groups, refer to the section **Assigning Configuration Profiles to a Device Group**.

Device Groups - Table of Column Descriptions	
Column Heading	**Description**
Group Name	Displays the name of the group. Clicking the group name will open the Group Details interface that allows you to view the full details of the group and edit the group. Refer to the section **Editing a Device Group** for more details.
Company	Displays the name of the company for which the group was created.
Number of Devices	Indicates the total number of devices in the group. Clicking the number will open the Group Details interface that allows you to view the full details of the group and edit the group. Refer to the section **Editing a Device Group** for more details.
Created By	Displays the name of the administrator that created the group. Clicking the name will open the user details interface. Refer to the section **Viewing the Details of a User** for more details.
Created	Indicates the date and time at which the group was created

To add the device to a new group

- Click 'Add to Group'



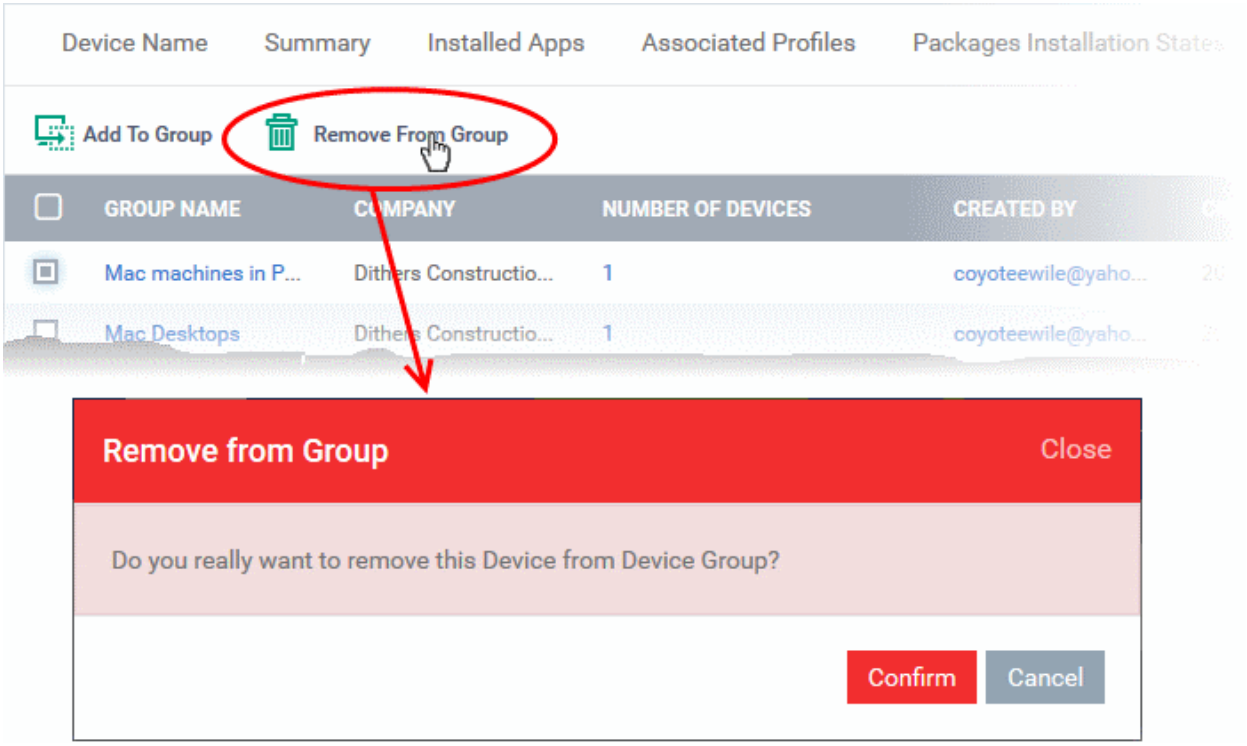
The 'Add Device to Group' dialog will appear.

- Start entering the name of the group to which the device has to be associated in the 'Choose Group(s)' field and choose the group from the options.
- Repeat the process to add the device to other groups.
- Click 'Add'.

The device will be added to the group.

To remove the device from a group

- Select the group from the list and click 'Remove from Group'.



A confirmation dialog will appear.

- Click 'Confirm' to remove the device from the group.

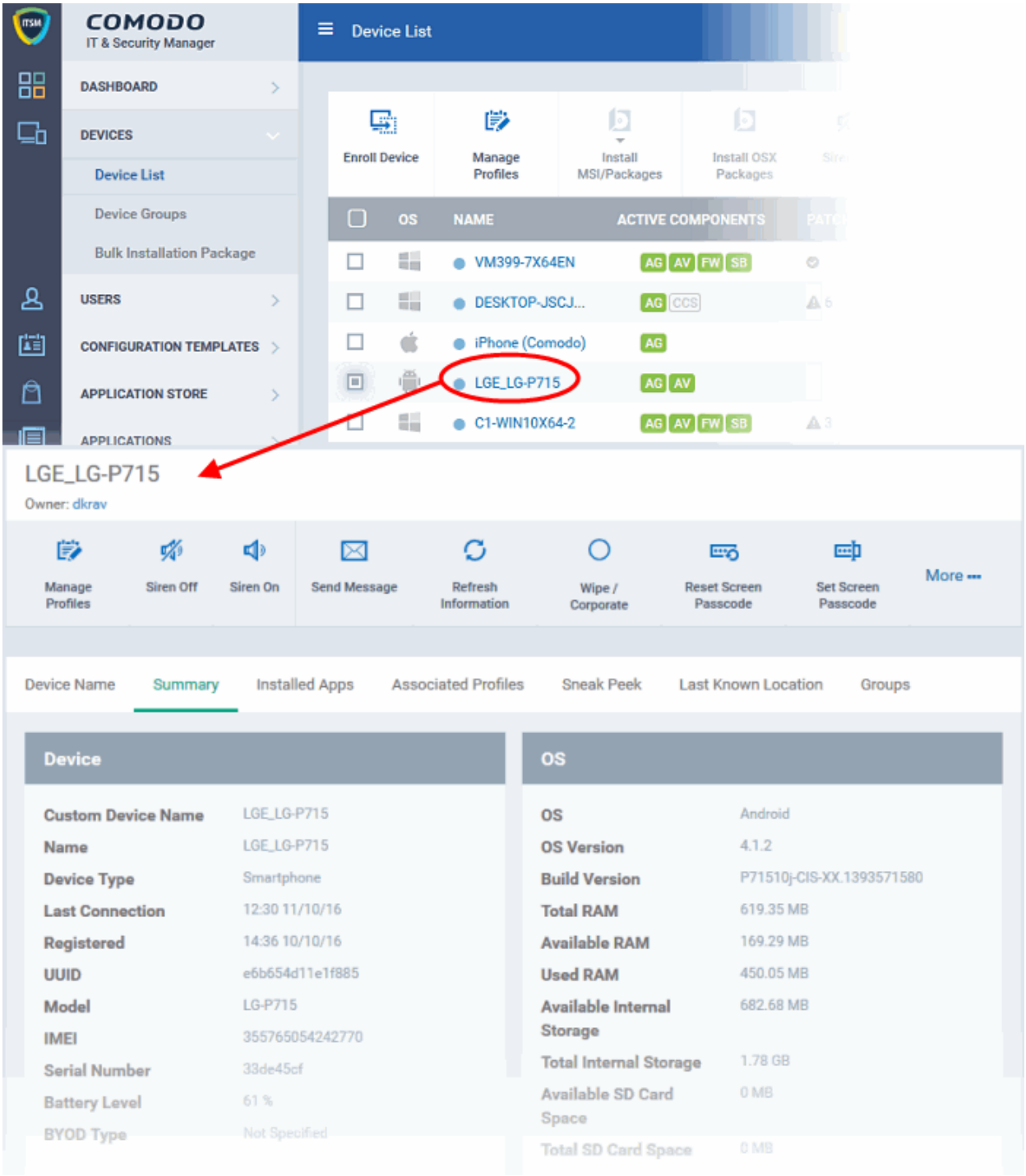
The device will be removed from the group, The configuration profiles in effect on the device because of the device associated with the group, will also be removed from the device.

5.1.3. Managing Android/iOS Devices

Administrators can view complete hardware and software details of enrolled mobile devices and manage any installed applications and configuration profiles in effect. Administrators can also send messages to the device, sound an alarm on lost/misplaced devices, remotely lock devices, view device location and view Sneak Peek photographs.

To view details of and manage an individual device

- Click 'Devices' and choose 'Device List'
- Click the name of any Android/iOS device

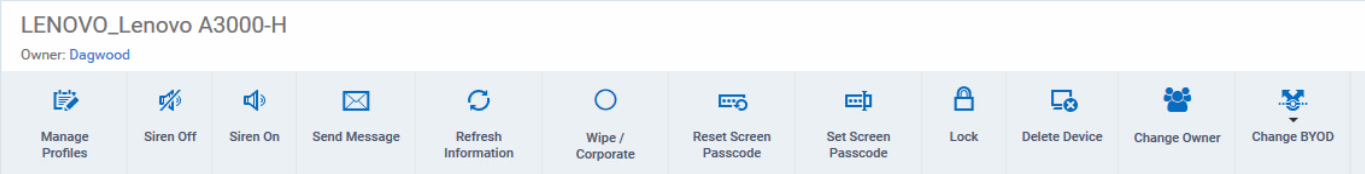


The device details pane will open, displaying the details of the selected device under six tabs:

- **Device Name** - Displays the name of the device. You can change this as per your preferences. Refer to the section **Viewing and Editing Device Name** for more details.
- **Summary** - Displays the general details of the device including device information, OS details, Network details and security configuration. Refer to the section **Viewing Summary Information** for more details.
- **Installed apps** - Displays a list of applications currently installed on the device along with their versions. You can remotely block/release apps or uninstall unwanted applications from the device. Refer to **Managing Apps Installed on a Device** for more details.
- **Associated Profiles** - Displays details of the profiles deployed on the device and enables you to add new profiles or remove existing profiles. Refer to the section **Managing Profiles associated with the Device** for more details.

- **Sneak Peek** - Displays pictures captured by the Sneak Peek feature of ITSM. If enabled on a profile associated with the device, the Sneak Peak feature photographs the holder of a device who tries to login using guessed passcodes. This enables the administrator to identify the possessor, or immediate surroundings, of lost devices. Refer to the section **Viewing Sneak Peek Pictures to Locate Lost Devices** for more details.
- **Last Known Location** - Displays the location of the device during its last polling cycle, on a map. The administrator can also view the current location of the device by updating the location information. Refer to the section **Viewing the Location of the Device** for more details.
- **Groups** - Displays a list of device groups to which the Android/iOS device belongs and allows you to manage group membership. Refer to the section **Viewing and Managing Device Group Memberships** for more details

The administrator can remotely perform various tasks on the device using the options at the top of the interface.



- **Manage Profiles** - Allows you to add or remove device profiles. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details.
- **Siren Off/Siren On** - Allows you to generate an alarm on the device to locate it, if it is misplaced. Refer to the section **Generating Alarm on Devices** for more details.
- **Send Message** - Allows you to send a text message to the user. Refer to the section **Sending Text Message to Devices** for more details
- **Refresh Information** - Allows you to obtain the updated details from the device. Refer to the section **Updating Device Information** for more details.
- **Wipe/Corporate** - Allows you to delete the data stored in the device if it is lost or stolen. Refer to the section **Wiping Data from Devices** for more details
- **Reset Screen Passcode** - Allows you to reset screen lock password of the device, if the user has forgotten it and requested for a reset. Refer to the section **Setting / Reseting Screen Lock Password for Devices** for more details
- **Set Screen Passcode** - Allows you to create a new screen lock password for the device. Refer to the section **Setting / Resetting Screen Lock Password for Devices** for more details
- **Lock/Unlock** - Allows you to remotely lock or unlock the device, if the device is lost, misplaced or stolen. Refer to the section **Locking/Unlocking Devices** for more details
- **Delete Device** - Allows you to remove the device from ITSM. Refer to the section **Removing a Device** for more details.
- **Change Owner** - Allows you to change the user to whom the device is associated. Refer to the section **Changing a Device's Owner** for more details.
- **Change BYOD** - Changes the BYOD status of the device. Refer to the section '**Changing BYOD status of a Device**' for more details.

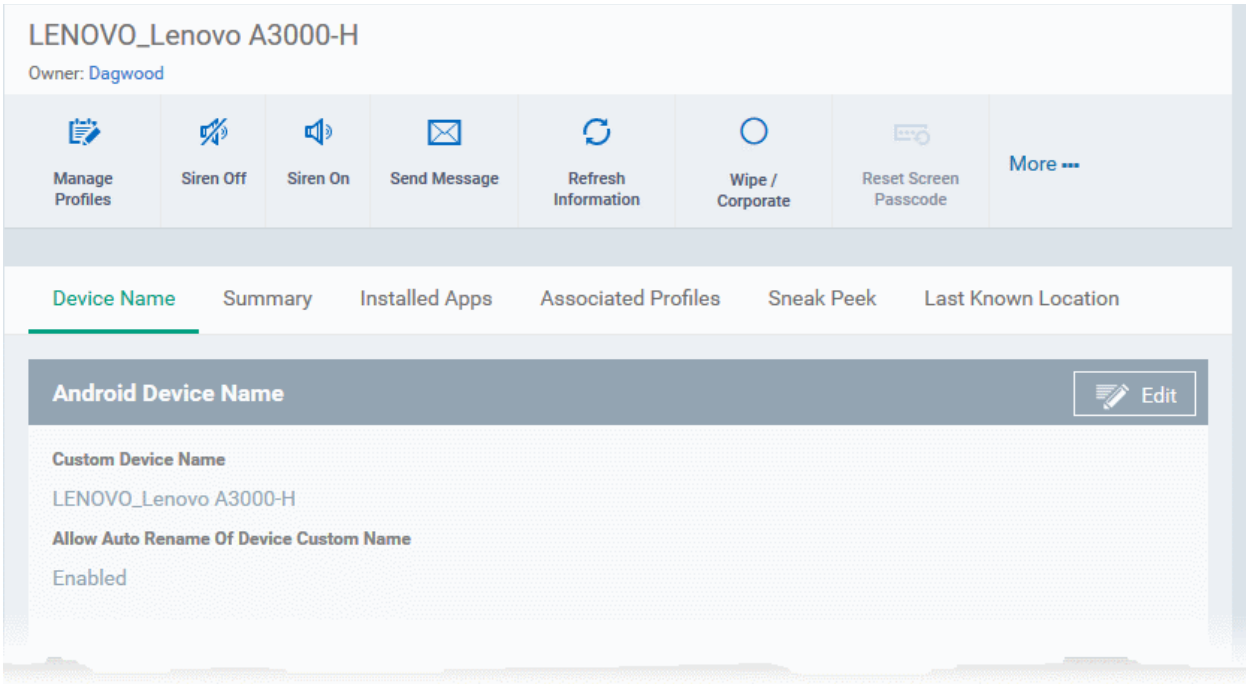
5.1.3.1. Viewing and Editing Device Name

Enrolled Android and iOS devices are listed by the name assigned to them by their owner or by model number if no name was assigned. Admins can change device name according to their preferences. If you change a device name, the name will apply in ITSM but will not change the name on the device itself.

To change the device's name

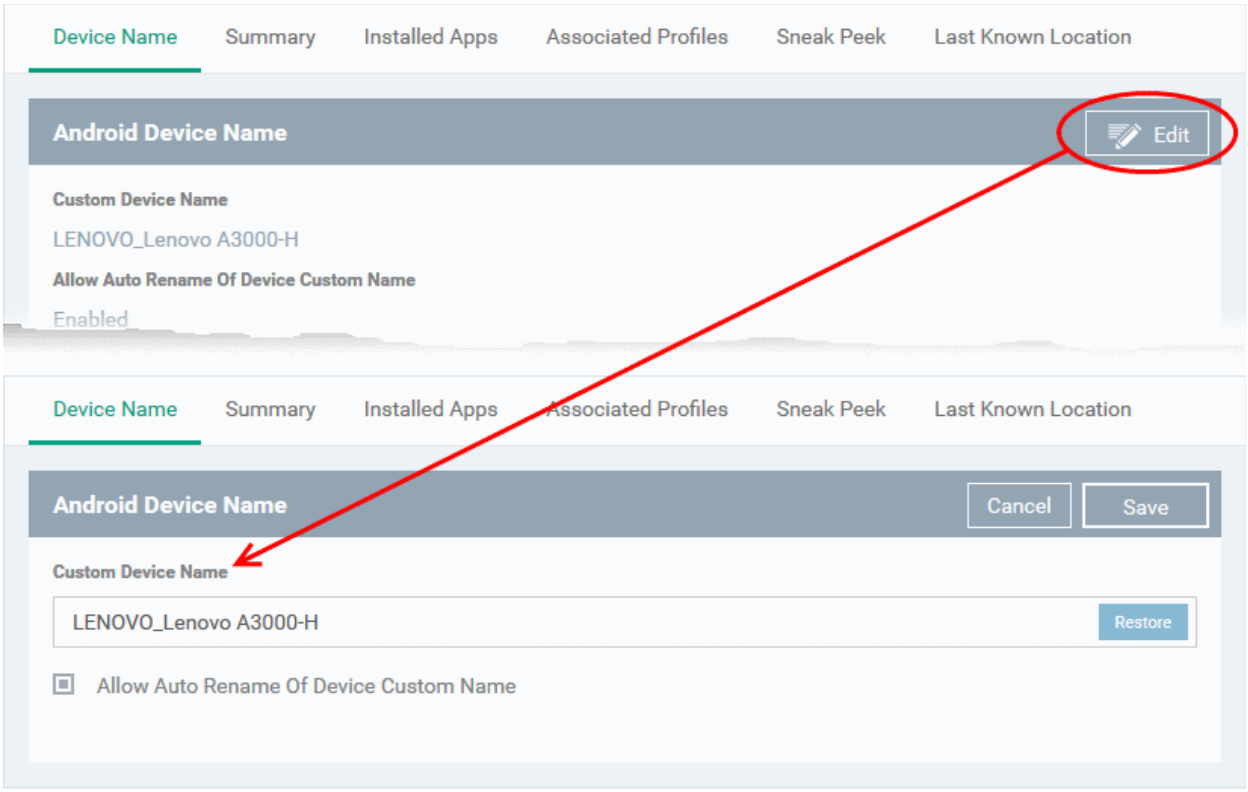
- Click 'Devices' and choose 'Device List'

- Click the name of the device then select the 'Device Name' tab



- Custom Device Name - The current name of the device
- Allow Auto Rename of Device Custom Name - Indicates whether the device's name can be changed or not.

- To change the name of the device, click the 'Edit' button at the right.



- Enter the new name in the 'Custom Device Name' field
- Make sure the 'Allow Auto Rename of Device Custom Name' is enabled.

- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

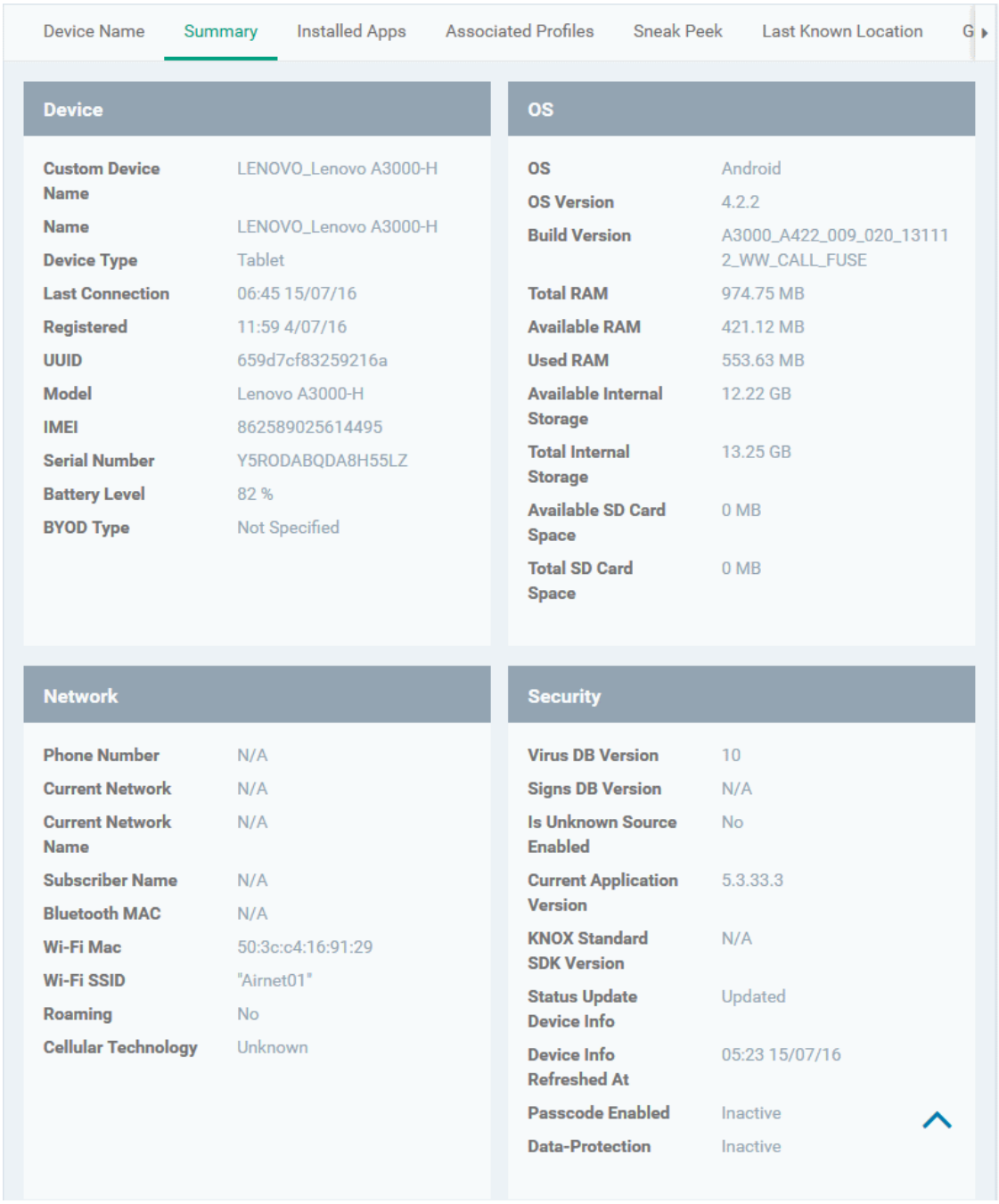
- To restore the name of the device as it was at the time of enrollment, click 'Edit' from the 'Device Name' interface, click 'Restore' at the right and click 'Save'.

5.1.3.2. Viewing Summary Information

The 'Summary' tab displays general information about the device, its operating system, network and security status.

To view the device information summary

- Click 'Devices' and choose 'Device List'.
- Click the name of the Android/iOS device. Open the 'Summary' tab (if it is not already open).



- **Device Summary** - Provides device details such as brand, model, International Mobile Equipment Identification (IMEI) number, last connection time, device battery level (at last connection time) and BYOD

type of the device.

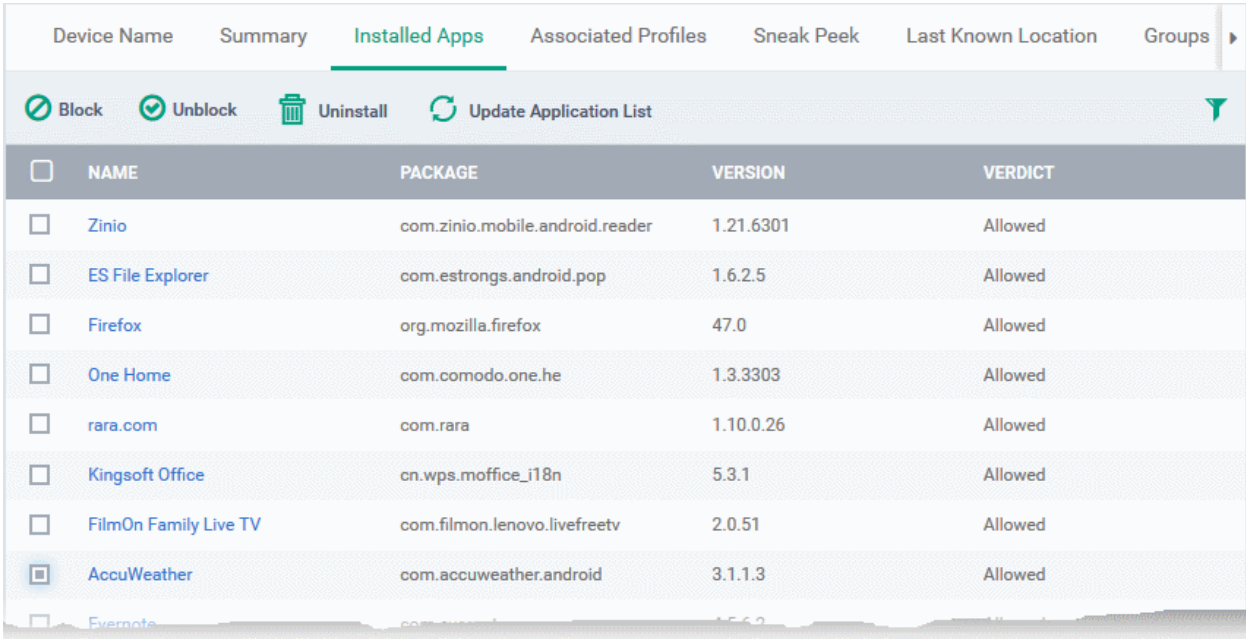
- **OS Summary** - Provides details about the device's Operating System, including version number, memory usage and available internal and external storage space.
- **Network Summary** - Provides details about the mobile and WiFi networks to which the device is connected, including the MAC addresses of the device for connection through Bluetooth and WiFi.
- **Security** - Provides details about important security settings of the device. For Android devices, details from Comodo Mobile Security (CMS) like Virus Signature Database version and update status are displayed.

5.1.3.3. Managing Installed Applications

The 'Installed Apps' tab displays a list of all applications installed on a device. The interface shows package names and version numbers; allows administrators to selectively block or unblock apps and offers the ability to uninstall suspicious or junk apps. Administrators can also identify which other devices have the same application installed so they can apply corrective actions to all affected devices.

To manage installed apps

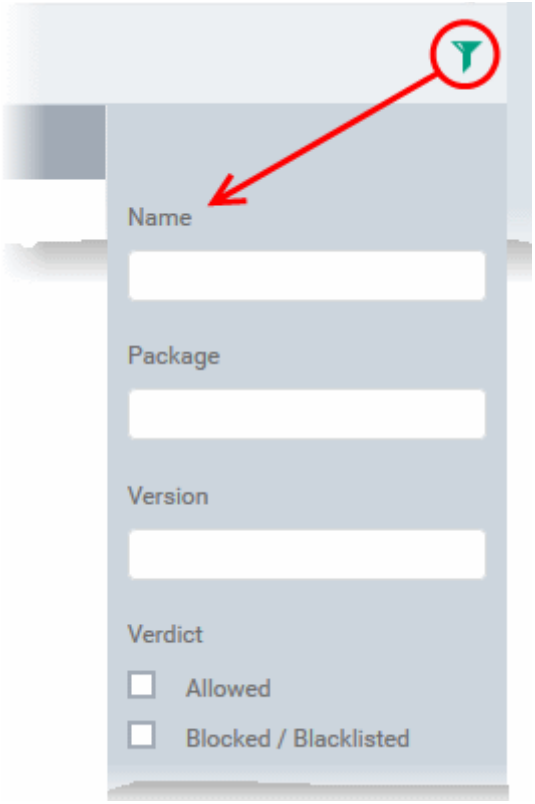
- Click 'Devices' and choose 'Device List'
- Click the name of the Android/iOS device then select the 'Installed Apps' tab



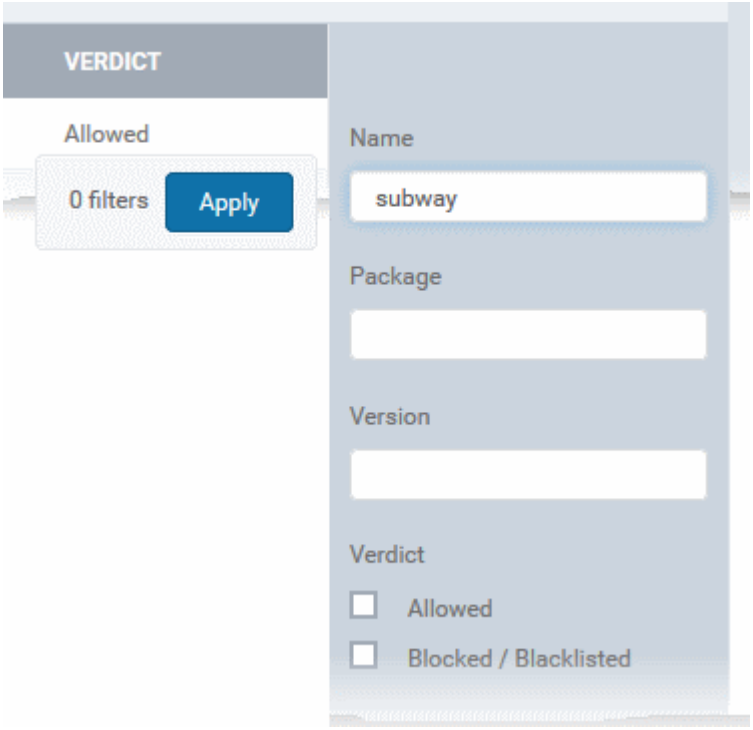
Installed Apps - Column Descriptions	
Column Heading	**Description**
Name	The name of the application. Clicking the application name will show all devices which have this app installed. This makes it easier for administrators to apply an action to all devices which feature a certain app.
Package	Indicates the application ID on the vendor app store. For example, 'cn.wps.moffice_i18n' can be found at https://play.google.com/store/apps/details?id=cn.wps.moffice_i18n
Version	Indicates the version of the application.
Verdict	Indicates whether the application is allowed, blocked or blacklisted.

Sorting and Filtering Options

- Clicking any column header sorts column entries in alphabetical order.
- Clicking the funnel icon at the right opens the filter interface:



- You can filter/search specific items based on app name, package or version. To start, enter the search criteria in full or part in the respective search field and click 'Apply'



- Use the check-boxes under 'Verdict' if you wish to see only allowed or only blocked applications in the

search results.

You can use any combination of filters to search for specific devices.

- To display all items again, clear the search box(es) and click 'Apply'.
- By default ITSM returns 20 results per page. Use the 'Results per page' drop-down to increase the number of results displayed up to a maximum of 200.

Blocking Unwanted Apps

Administrators can remotely block apps that are identified as malicious, suspicious or junk. The app will not be uninstalled from the device but will not be allowed to run. Blocked apps can be released at a later date and allowed to run.

To block selected apps

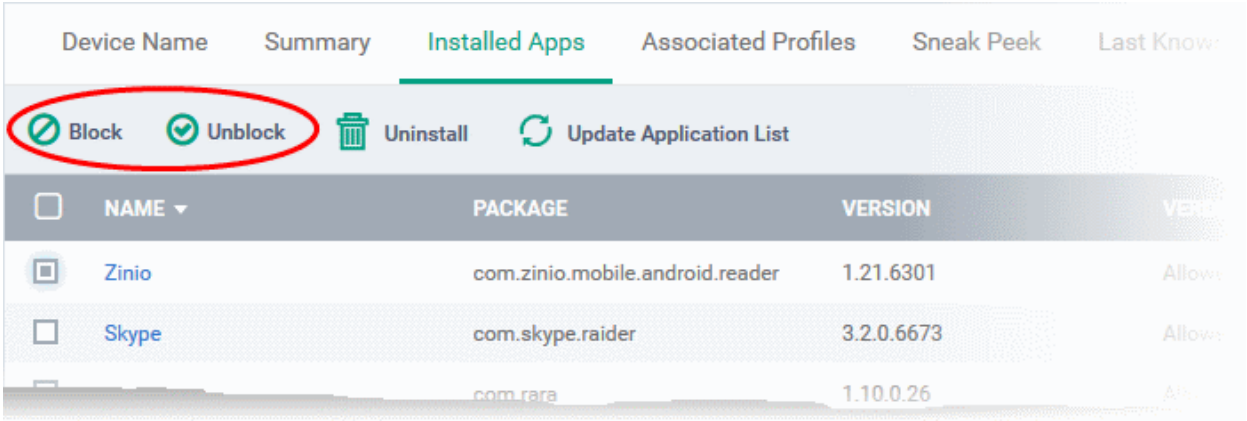
- Choose the app(s) that you wish to block and simply click the 'Block' button.

The verdict of the app(s) will change to 'Blocked' and they will not be allowed to run on the device.

To release blocked apps

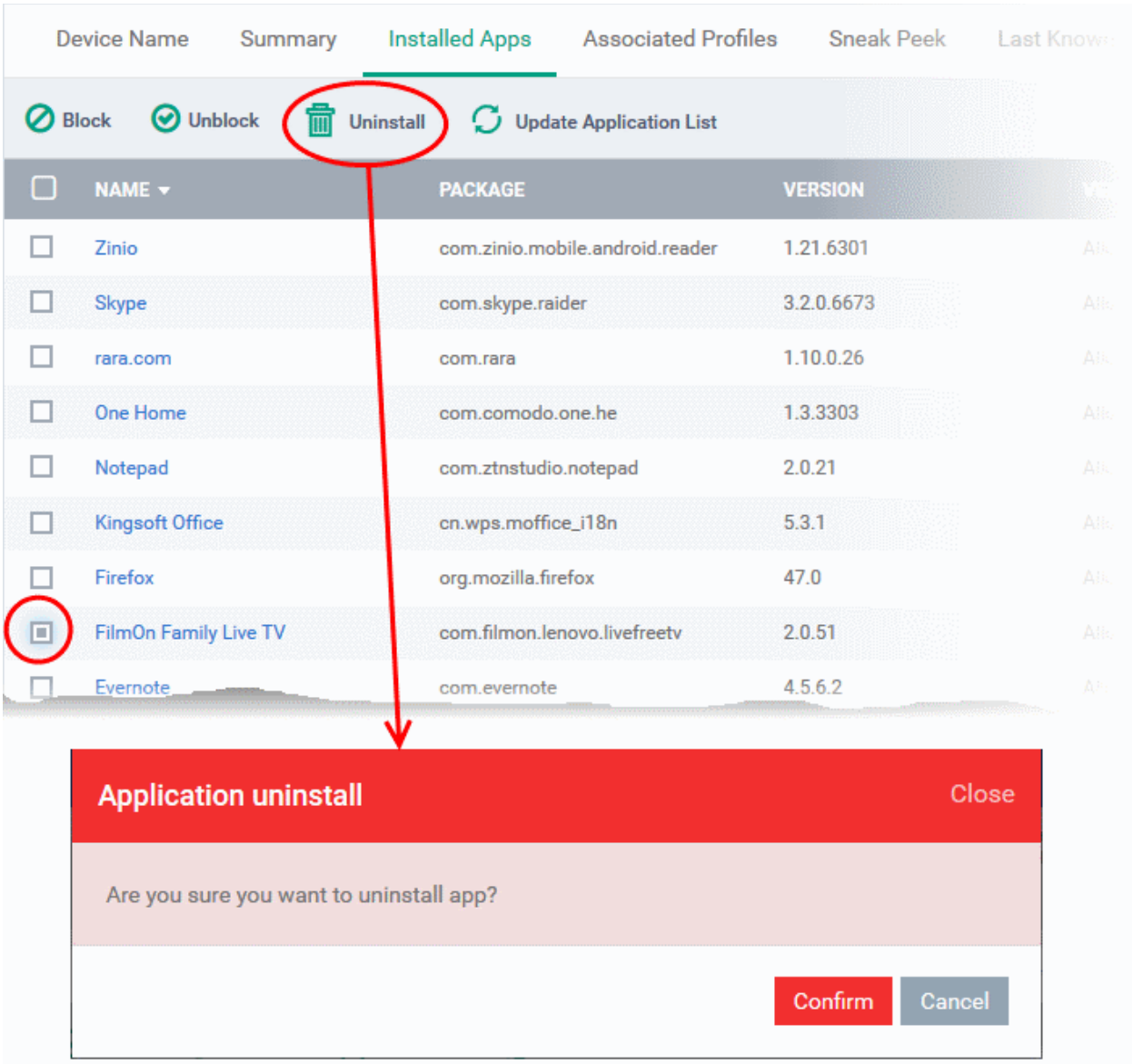
- Select the blocked app(s) and click 'Unblock'.

The verdict of the app(s) will change to 'Allowed' and they will be allowed to run on the device.



Uninstalling and updating the application list

- To uninstall malicious or junk app(s) from the device, select the app(s) and click 'Uninstall'. A notification will be sent to the device requesting uninstallation and the app will be immediately blocked. Upon receiving the notification, the end user needs to select 'Uninstall'.



A confirmation dialog will be displayed.

- Click 'Confirm' to uninstall the selected app(s).

- The list of apps on a device is updated in ITSM every 24 hrs. To refresh the list immediately, click 'Update Application List'.

5.1.3.4. Viewing and Managing Profiles Associated with a Device

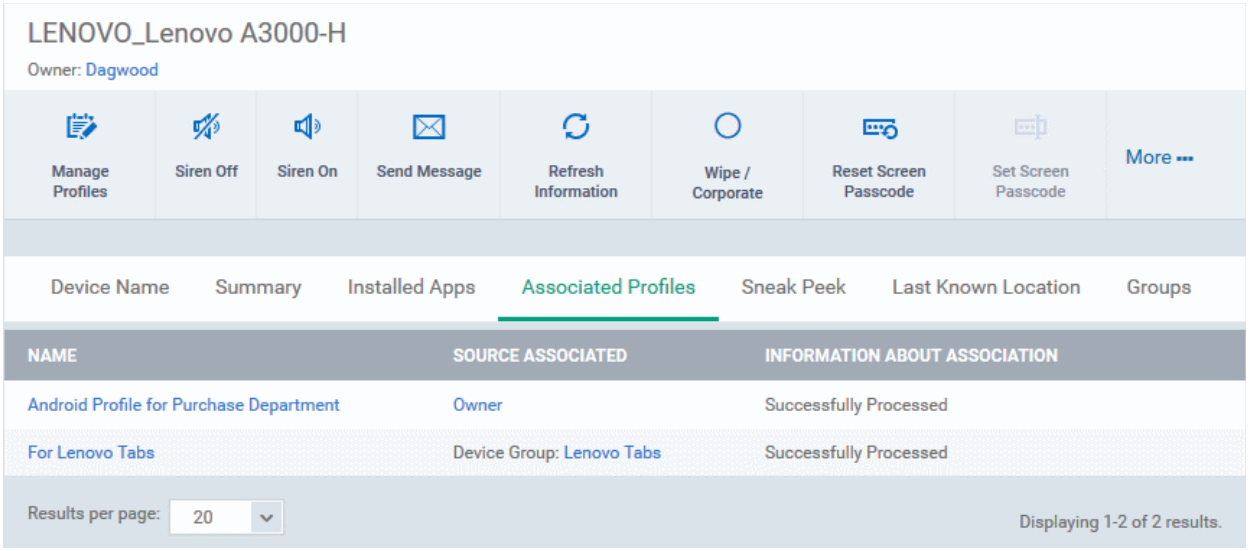
The 'Associated Profiles' tab displays a list of all currently active configuration profiles on an Android/iOS device. A profile may have been applied to a device because:

- It is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- The device belongs to one or device groups and inherited profiles from the group
- The user belongs to one or user groups and inherited profiles from the group

For more details on profiles and default profiles, refer to the chapters 'Profiles for Android Devices', 'Profiles for iOS Devices', 'Viewing and Managing Profiles' and 'Managing Default Profiles'.

To view and manage associated profiles

- Click 'Devices' and choose 'Device List'
- Click the name of any Android/iOS device then select the 'Associated Profiles' tab



Associated Profiles - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section **Editing Configuration Profiles** for more details.
Source Associated	Indicates the source through which the profile has been applied to the device. Configuration profiles are applied to a device in different ways: • Profiles can be directly applied to the device. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. Refer to the section **Assigning Configuration Profile(s) to a Users' Devices** for more details • Profiles applied to a user group are deployed to all devices owned by group members. Refer to the section **Assigning Configuration Profile to a User Group** for more details • Profiles applied to a device group are deployed to all member devices in the group. Refer to the section **Assigning Configuration Profile to a Device Groups** for more details Clicking on the source opens the respective details interface.
Information about Association	Indicates the status of profile application to the device.

Adding or Removing Profiles

Profiles in effect on the device can be removed or new profiles can be added to the device by clicking Manage Profiles option at the top. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details.

5.1.3.5. Viewing Sneak Peek Pictures to Locate Lost Devices

The 'Sneak Peek' tab displays photographs grabbed by devices via the 'Sneak Peek' feature.

The 'Sneak Peek' feature can help administrators to recover mislaid Android phones and tablets. If somebody enters the wrong password on a lost or stolen device, the device will automatically take a photo of the device holder and save it to the server with their picture and location.

The Sneak Peek feature can be enabled in the device profile and admins can also specify how many incorrect attempts should be allowed. To view this in the interface, open 'Add/Edit Android Profile' > 'Passcode' (or refer to the portion explaining configuration of Passcode settings under Profiles for Android Devices in this guide).

Administrators can view Sneak Peak images by going to 'Device' > 'Device List' > click device name > 'Sneak Peak'.

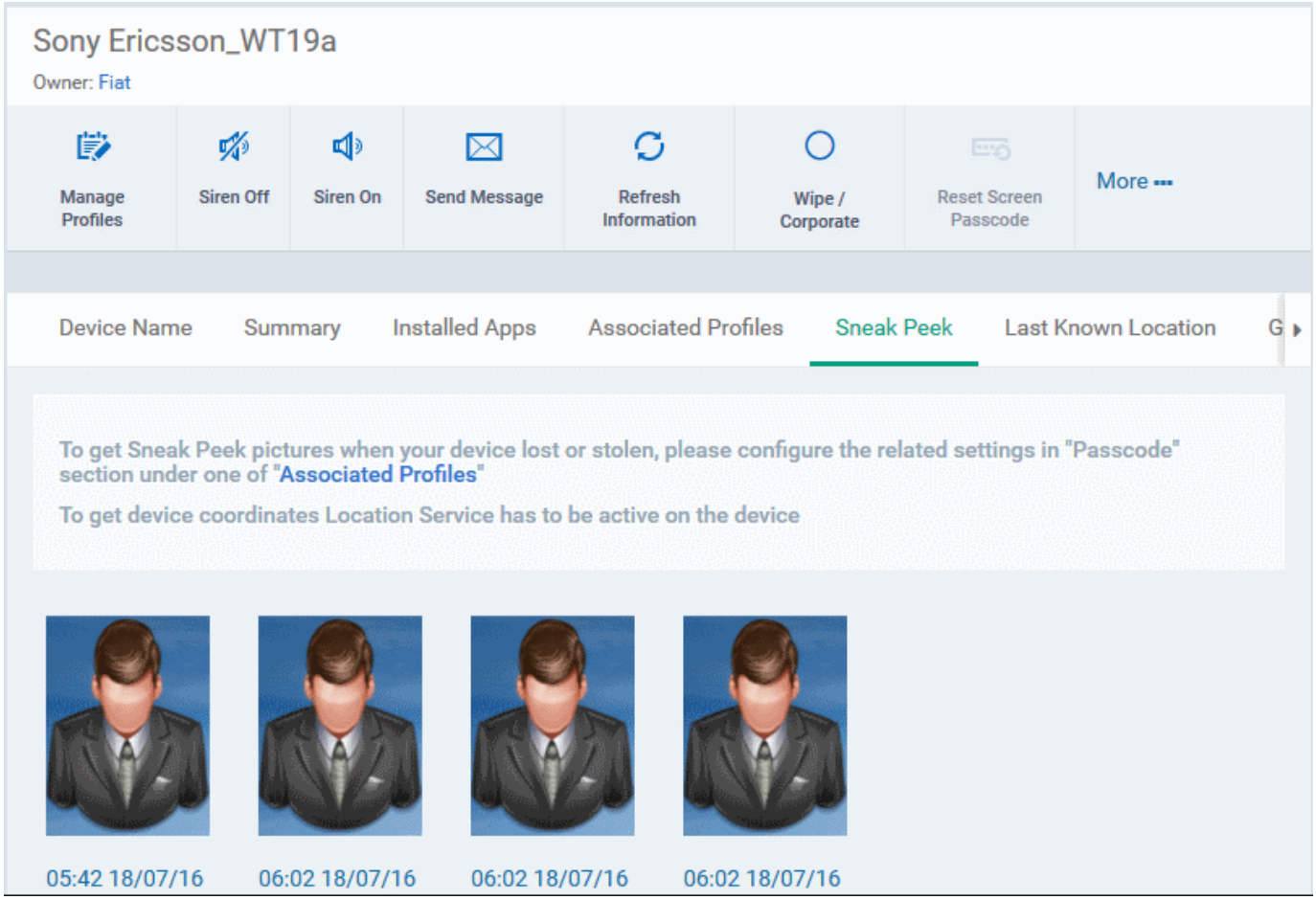
If the front camera is not available on the device, a photograph is taken using the rear facing camera.

Note: The 'Sneak Peak' tab is available only for Android devices.

To view Sneak Peak pictures

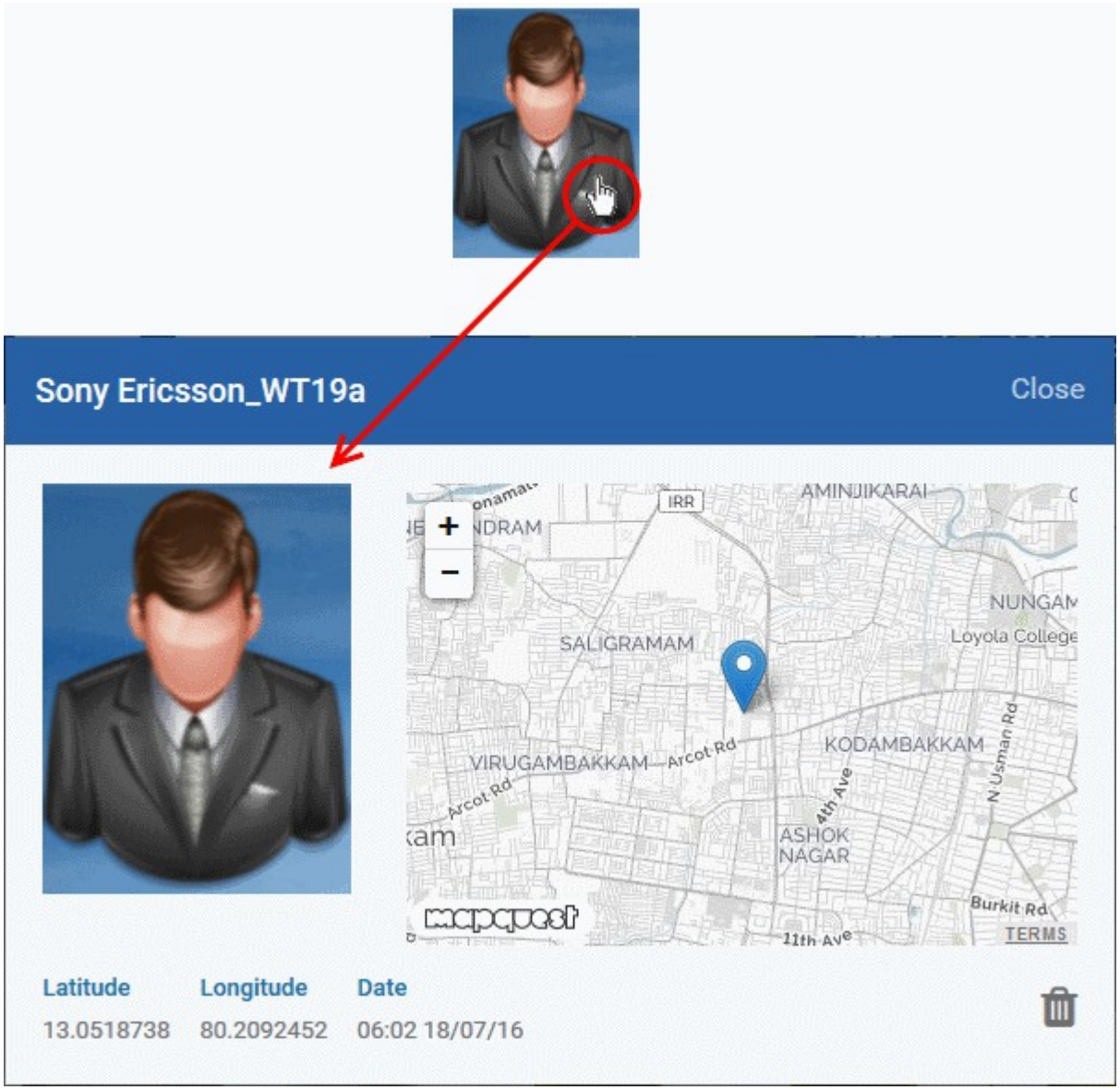
- Click 'Devices' and choose 'Device List'
- Click the name of the Android device then select the 'Sneak Peek' tab

The page will display all Sneak Peek photographs collected by devices after a series of incorrect passcode entries:



Note: The images shown above are for illustration purposes only. The interface will actually show photographs picked-up by the device camera.

- Clicking on a picture will display an enlarged view of the photograph and the location of the device at the time the photo was taken.



- To remove the sneak peek picture, click the trash can icon at bottom right.

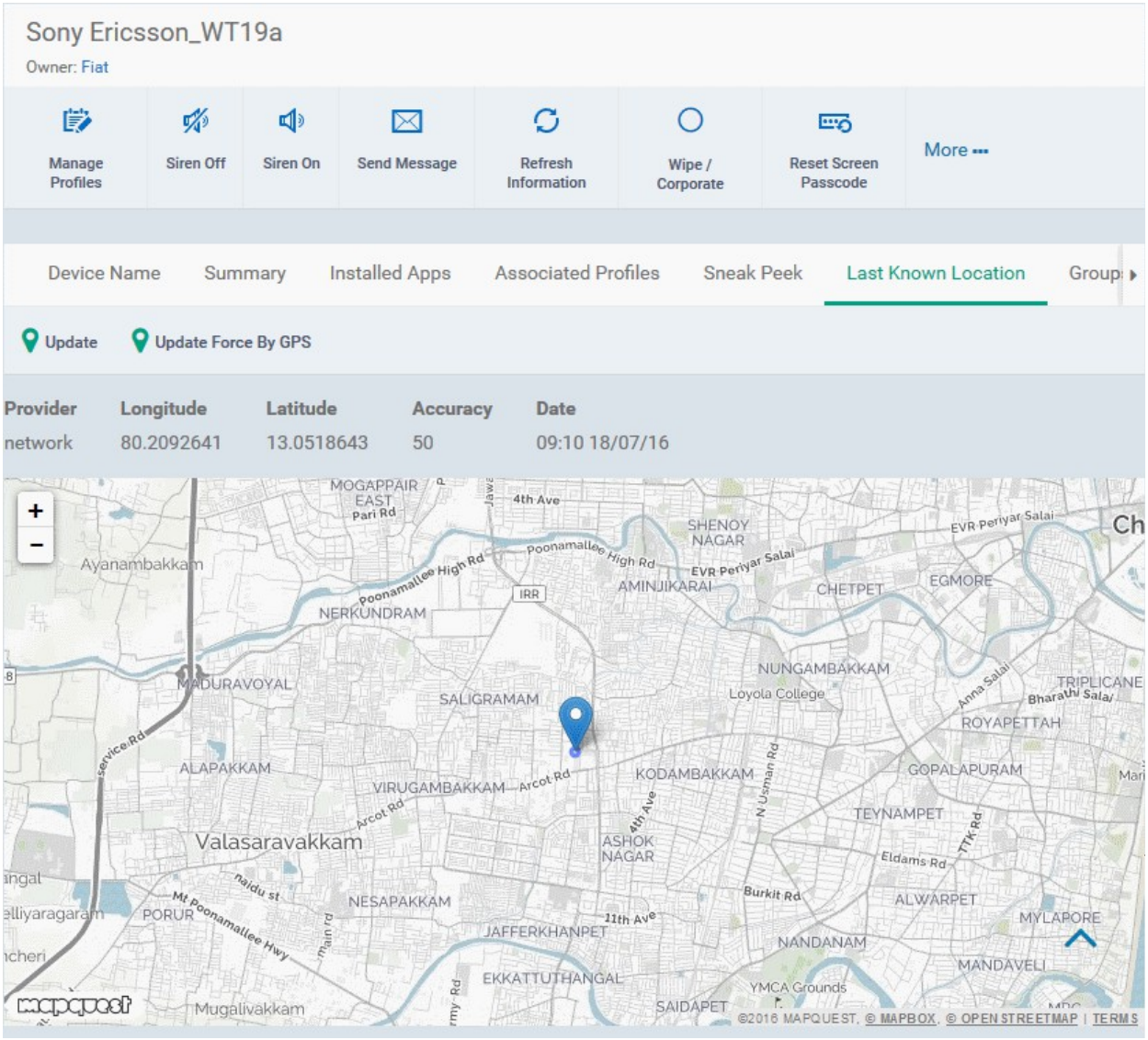
5.1.3.6. Viewing the Location of the Device

The 'Last Known Location' tab displays the map location of the device at the time it last contacted the ITSM portal. Administrators can refresh and view the current/latest location of the device by clicking the 'Update' link. This is useful if the phone is lost or stolen or if the administrator wishes to track the device for other reasons.

To view the location

- Click 'Devices' and choose 'Device List'
- Click the name of any Android / iOS device then select the 'Last Known Location' tab

The location of the device will be shown on a map.



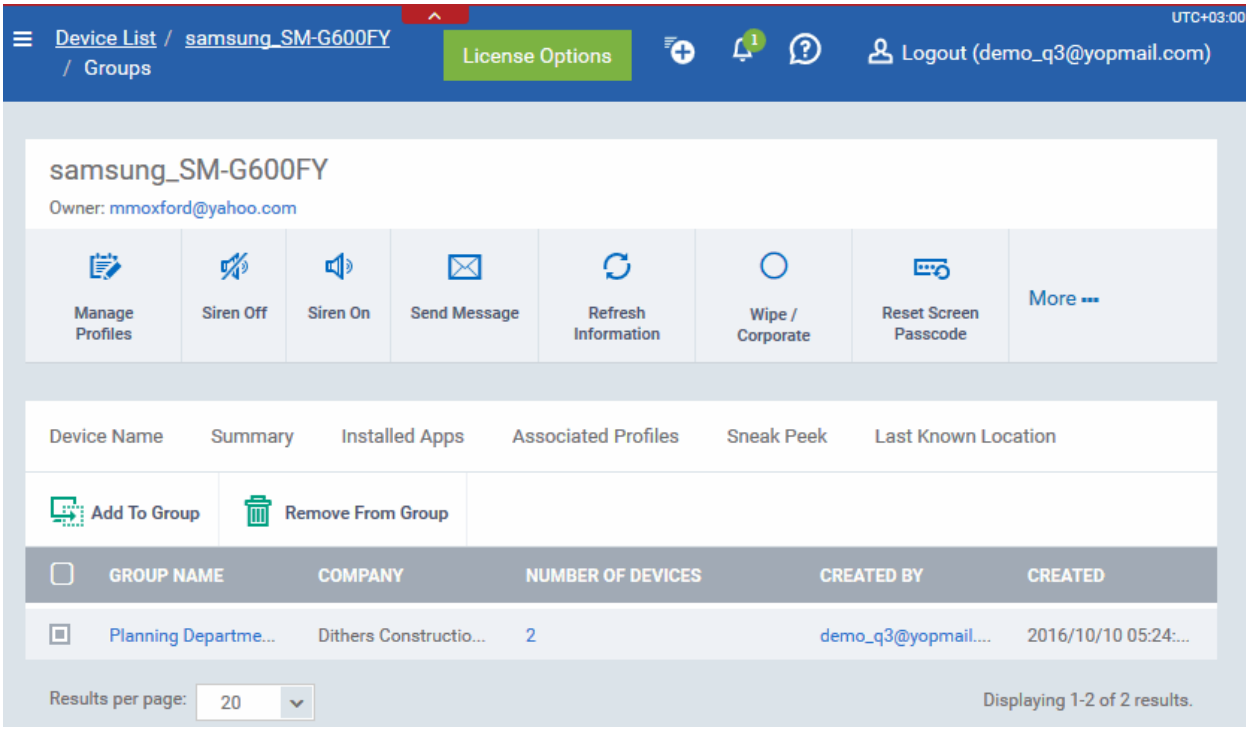
- To view the current location of the device, click 'Update'.
- To update the device location device instantly using device GPS, click 'Update Force GPS'.

5.1.3.7. Viewing and Managing Device Group Memberships

The 'Groups' tab in the Device Details interface displays a list of device groups with which the Android/iOS device is associated. Administrators can remove membership of the device from a group or add the device to a new group from this interface.

To view and manage device group membership

- Click 'Devices' and choose 'Device List'
- Click the name of the Android or iOS device then select the 'Groups' tab

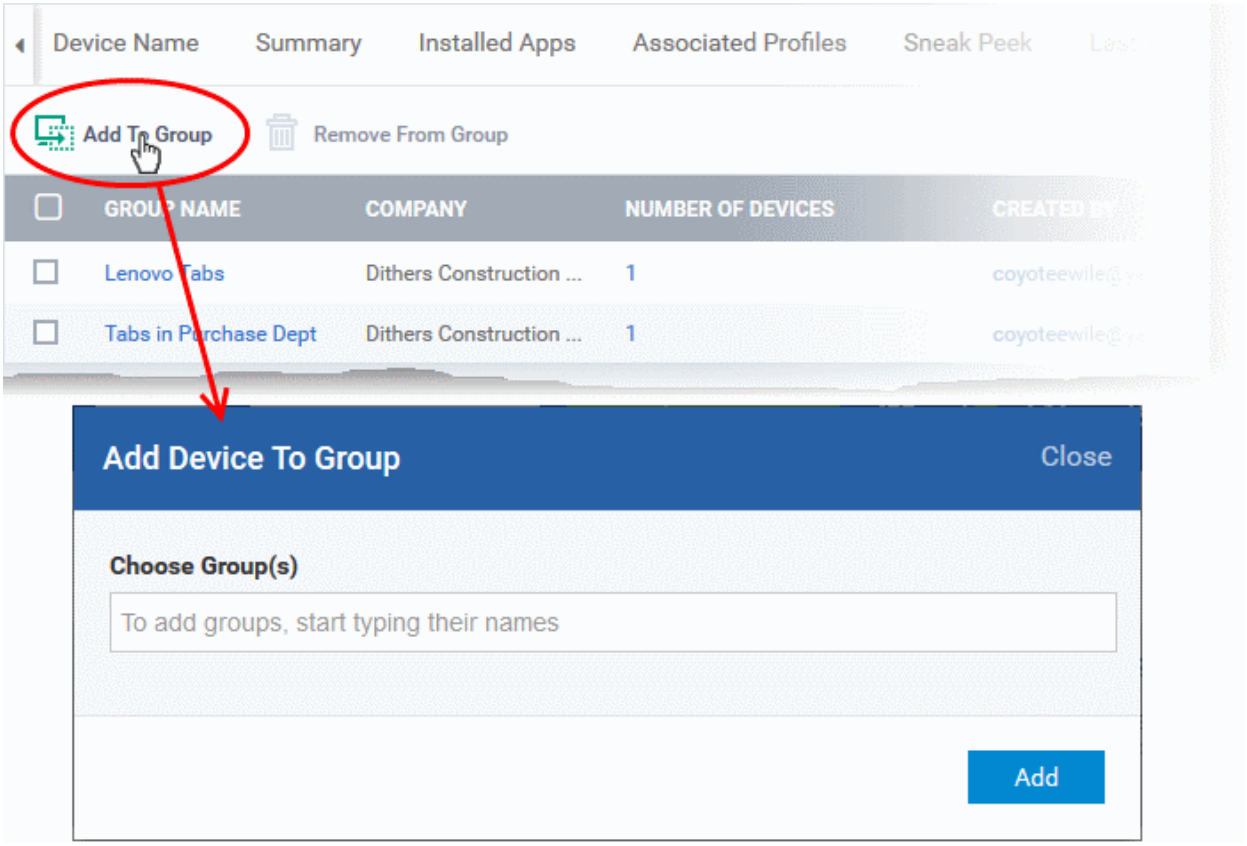


The interface lists all device groups of which the device is a member. All configuration profiles associated with each group will be applied to the device. For more details on applying configuration profiles to device groups, refer to Assigning Configuration Profiles to a Device Group.

Device Groups - Table of Column Descriptions	
Column Heading	**Description**
Group Name	Displays the name of the group. Clicking the group name will open the Group Details interface where you can view and edit group details. Refer to the section Editing a Device Group for more details.
Company	Displays the name of the company for which the group was created.
Number of Devices	Indicates the total number of devices in the group. Clicking the number will open the Group Details interface. Refer to the section Editing a Device Group for more details.
Created By	Displays the name of the administrator that created the group. Clicking the name will open the user details interface. Refer to the section Viewing the Details of a User for more details.
Created	Indicates the date and time at which the group was created.

To add the device to a new group

- Click 'Add to Group'



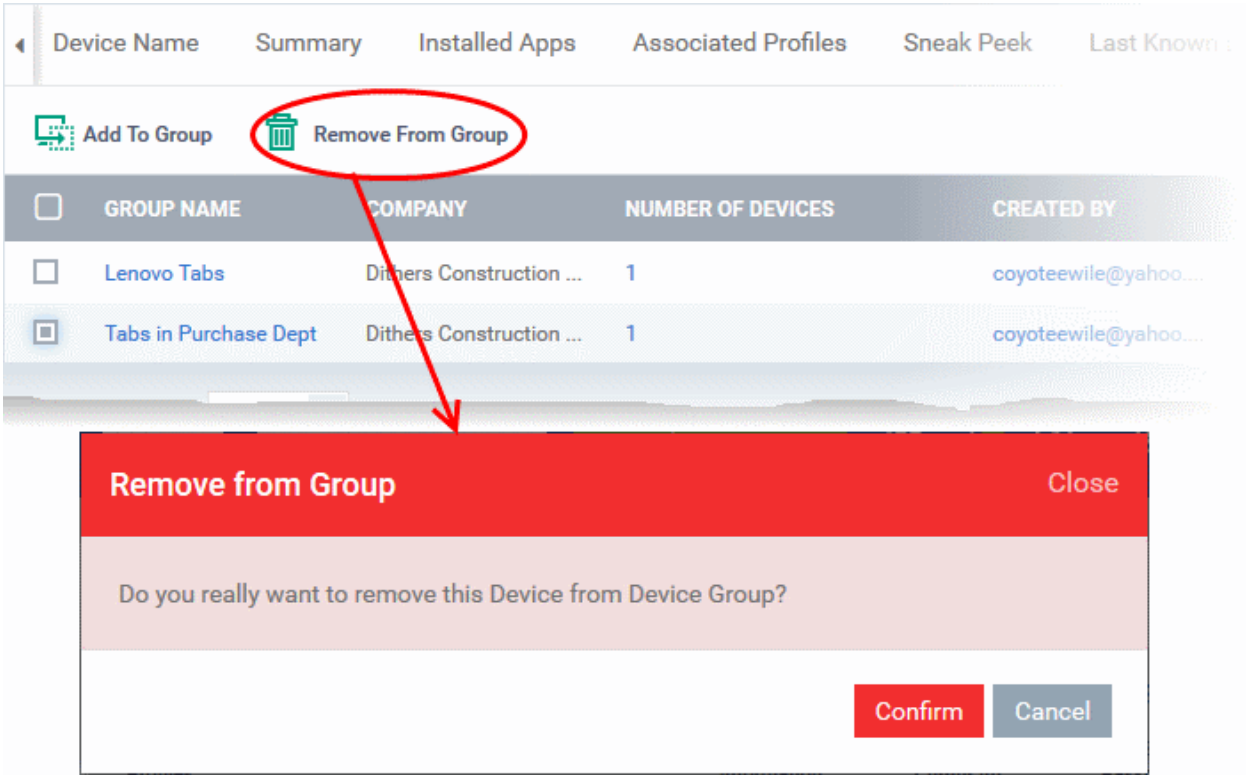
The 'Add Device to Group' dialog will appear.

- In the 'Choose Group(s)' field, start typing the name of the group to which you want to add the device. Select the desired group from the recommendations which appear.
- Repeat the process to add the device to other groups.
- Click 'Add'.

The device will be added to the group.

To remove the device from a group

- Select the group from the list and click 'Remove from Group'.



A confirmation dialog will appear.

- Click 'Confirm' to remove the device from the group.

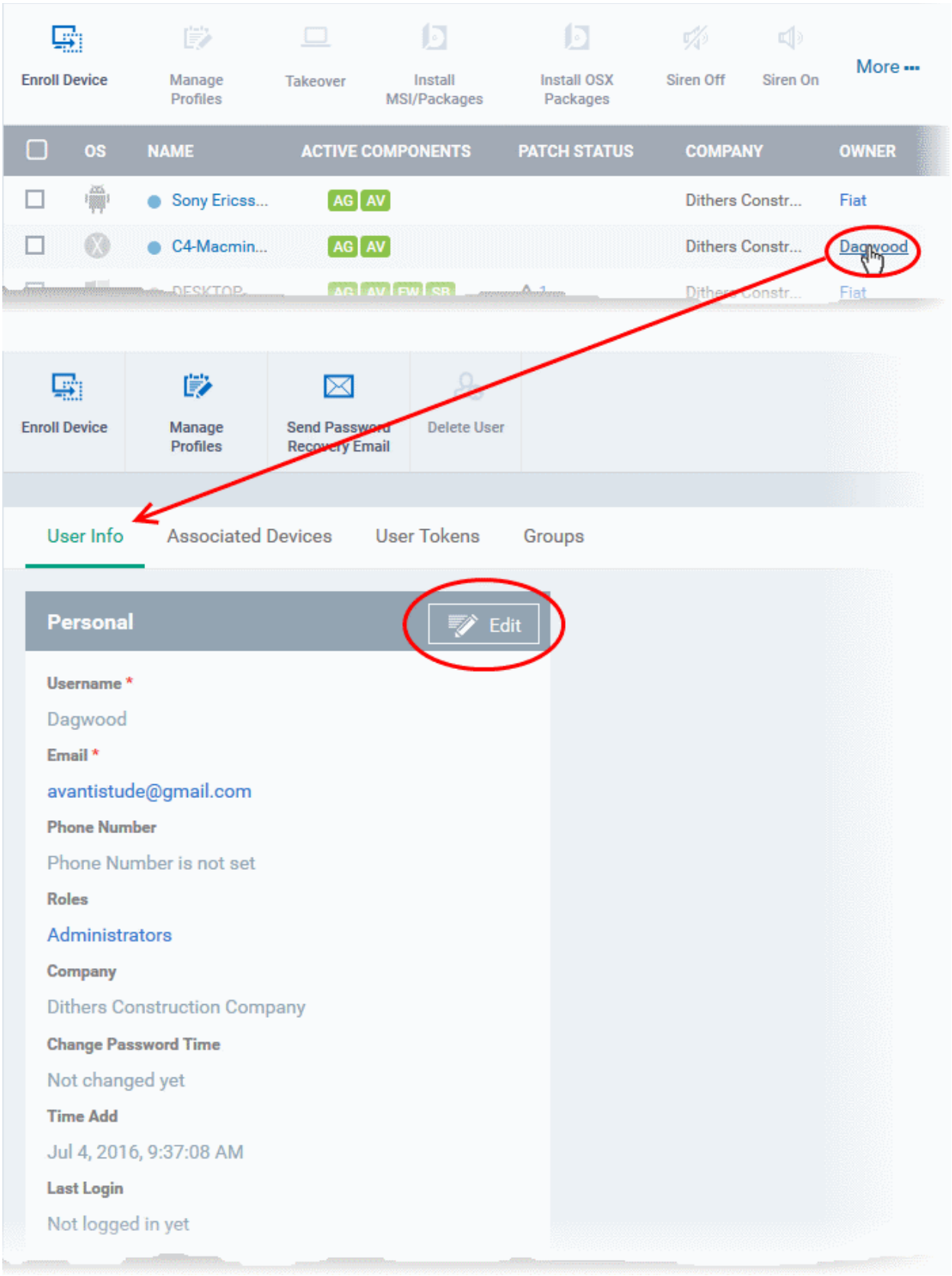
The device will be removed from the group. Any group configuration profiles will also be removed from the device.

5.1.4. Viewing User Information

Administrators can view and update user details such as email address and phone number from the 'Devices' interface.

To view the user information of a device

- Click 'Devices' and choose 'Device List'
- The users of each device are listed in the 'Owner' column. Click a user's name to open the 'User Details' pane.



- Click the 'Edit' button to modify user details. For more details on this area, see '**Viewing the Details of a User**' section.

5.1.5. Removing a Device

Devices that no longer require management can be removed by selecting 'Delete Device' from the 'More...' menu.

Warning: Once a device is deleted from ITSM, all configuration profiles and apps installed by ITSM will also be removed from the device.

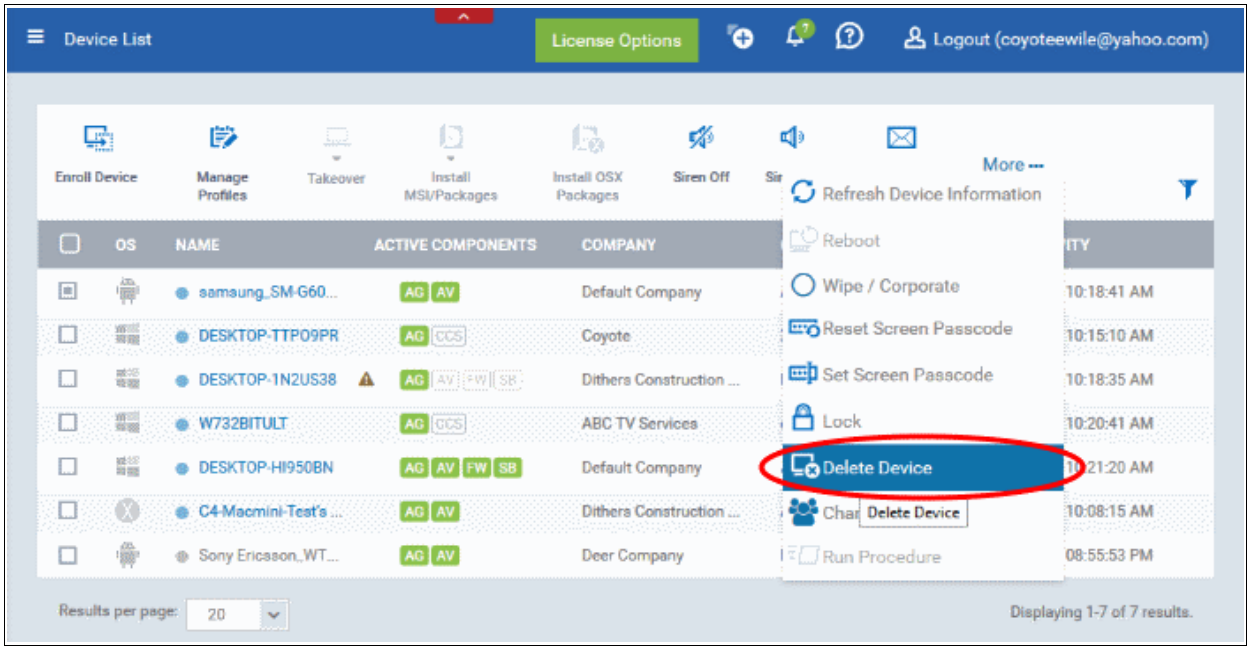
Windows Devices - You can also choose to uninstall the Comodo One Client Communication agent and/or the Comodo One Client Security software from the devices when removing the device.

Android, iOS and Mac OS devices - End users can manually uninstall the communication client and security software or the iOS profile from their devices. **Instructions for uninstalling the agent/software** are available at the end of this section.

If you wish to reinstate the device in future then a new token should be sent to the user and the device should be re-enrolled as explained in **Enrolling User Devices for Management.**

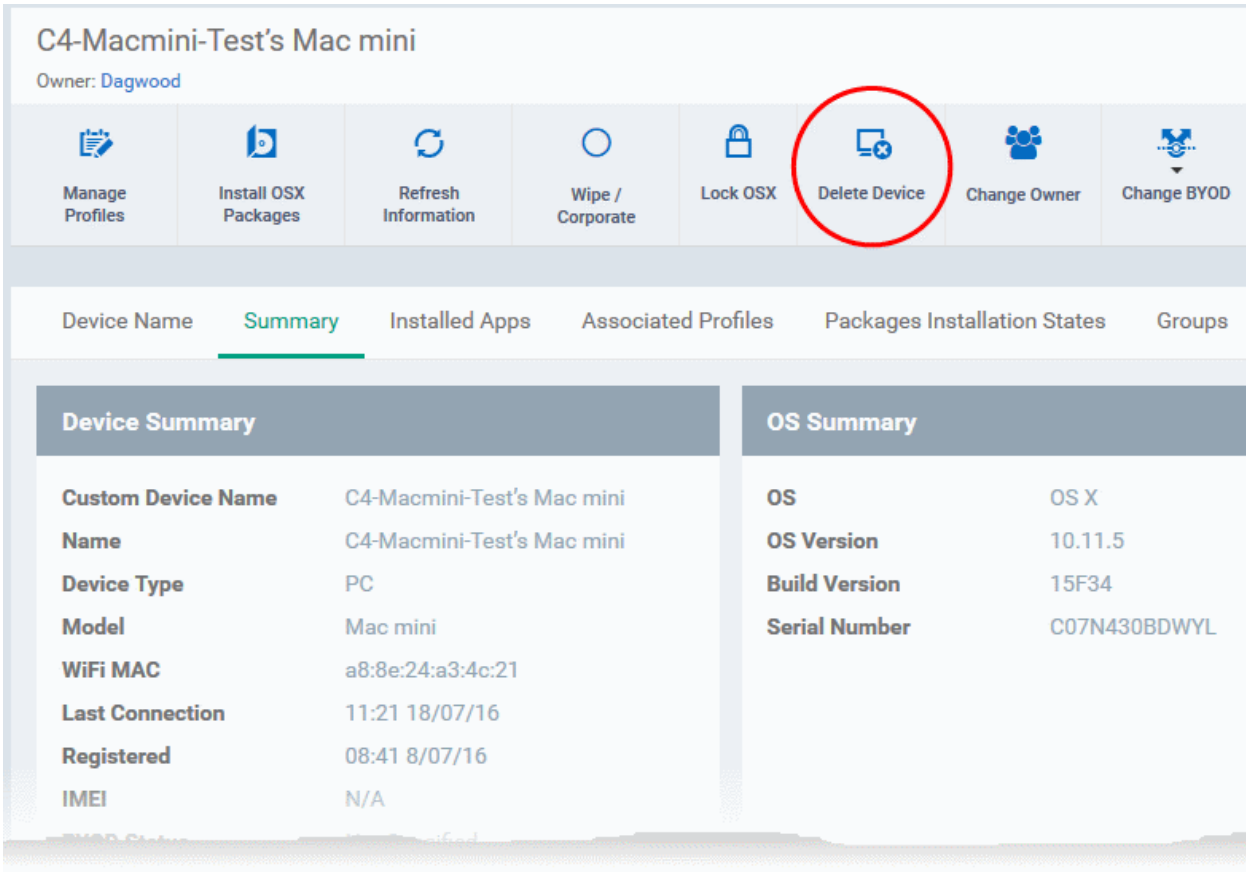
To remove a device from ITSM

- Click 'Devices' and choose 'Device List'.
- Select the device(s) to be removed from the list.
- Click 'Delete Device' from the options at the top. If Delete Device is not available, click 'More' at the top right and choose 'Delete Device' from the options.



Alternatively, you can remove a device from its device details interface.

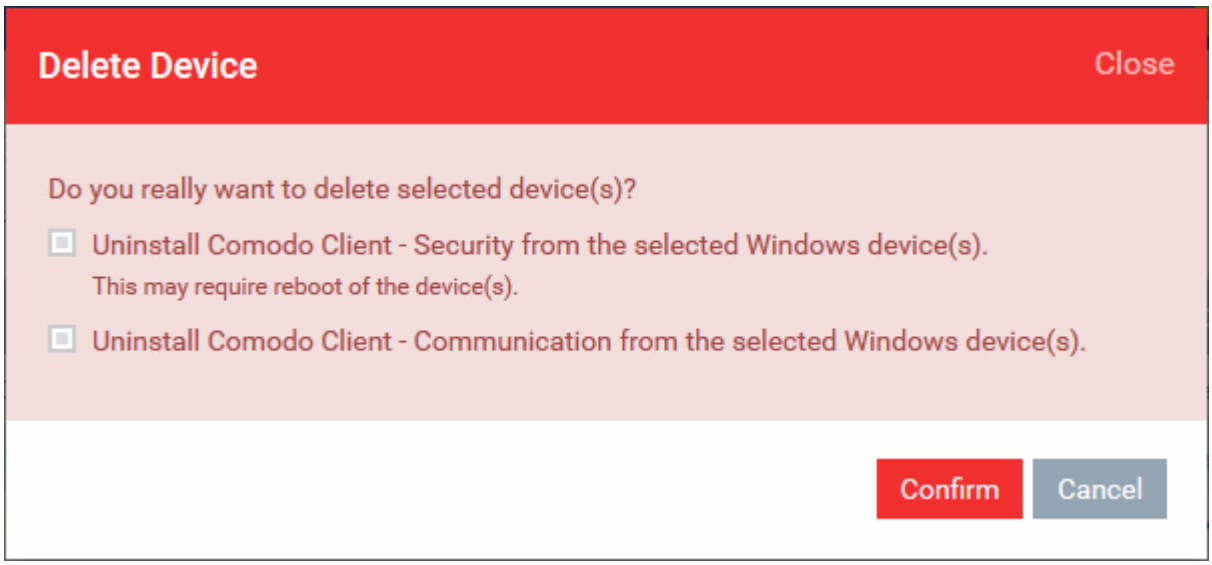
- Click 'Devices' and choose 'Device List'.
- Click on the name of the device to be removed to open the device details interface. If 'Delete Device' is not available here, click 'More' at the top right and choose 'Delete Device' from the options.



- Click 'Delete Device' from the options at the top

The 'Delete Device' dialog will appear.

For Windows devices, you can choose to uninstall the agent and/or the CCS software.



- Click 'Confirm' to remove the device from ITSM.

To remove the ITSM app from an Android device

- Navigate to 'Settings' > 'Apps' on the Android device
- Select 'Comodo ITSM'
- Tap the 'Uninstall' button.

The ITSM app will be removed from the device.

To remove the ITSM profile from an iOS device

- Navigate to 'Settings' > 'General' on the iOS devic
- Select 'Profile' > 'Comodo Profiles' (certificate and ITSM)
- Tap the 'Remove' button.

The ITSM profile will be removed from the device.

To remove the ITSM profile from OS X devices

- Navigate to 'Settings' > 'General' on the OS X endpoint.
- Select 'Profile' > 'Comodo Profiles' (certificate and ITSM)
- Click the 'Remove' button.

The ITSM profile will be removed from the device.

5.1.6. Remote Management of Windows Devices

The 'Takeover' feature allows administrators to remotely access and control Windows devices to solve issues, install third party software and run system maintenance. Takeover currently works with Windows devices only, with support for MAC OS coming soon.

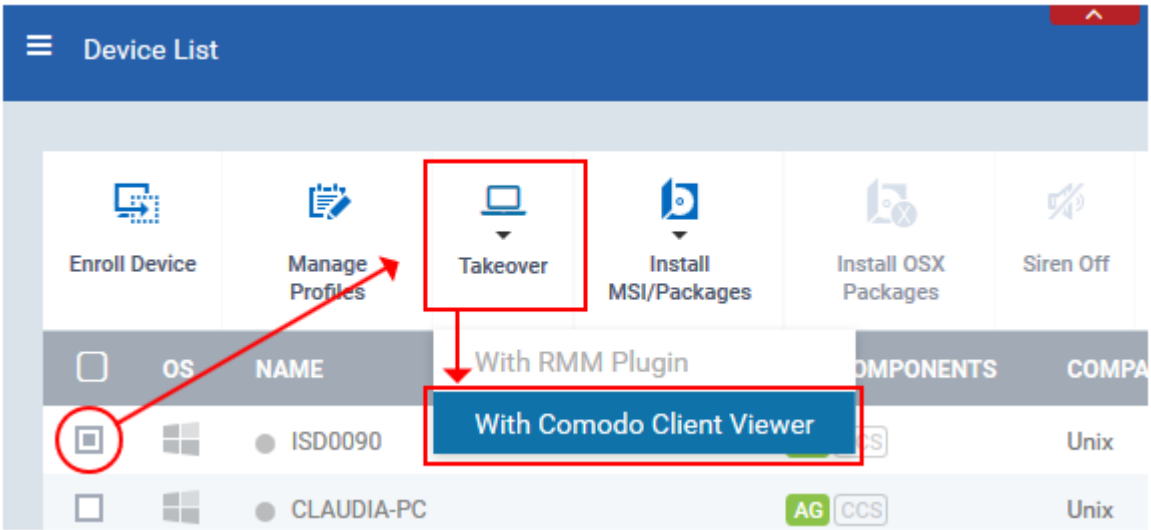
You can takeover Windows devices using the following tools:

- Comodo Client Viewer
- Comodo Remote Monotiring and Management (RMM)

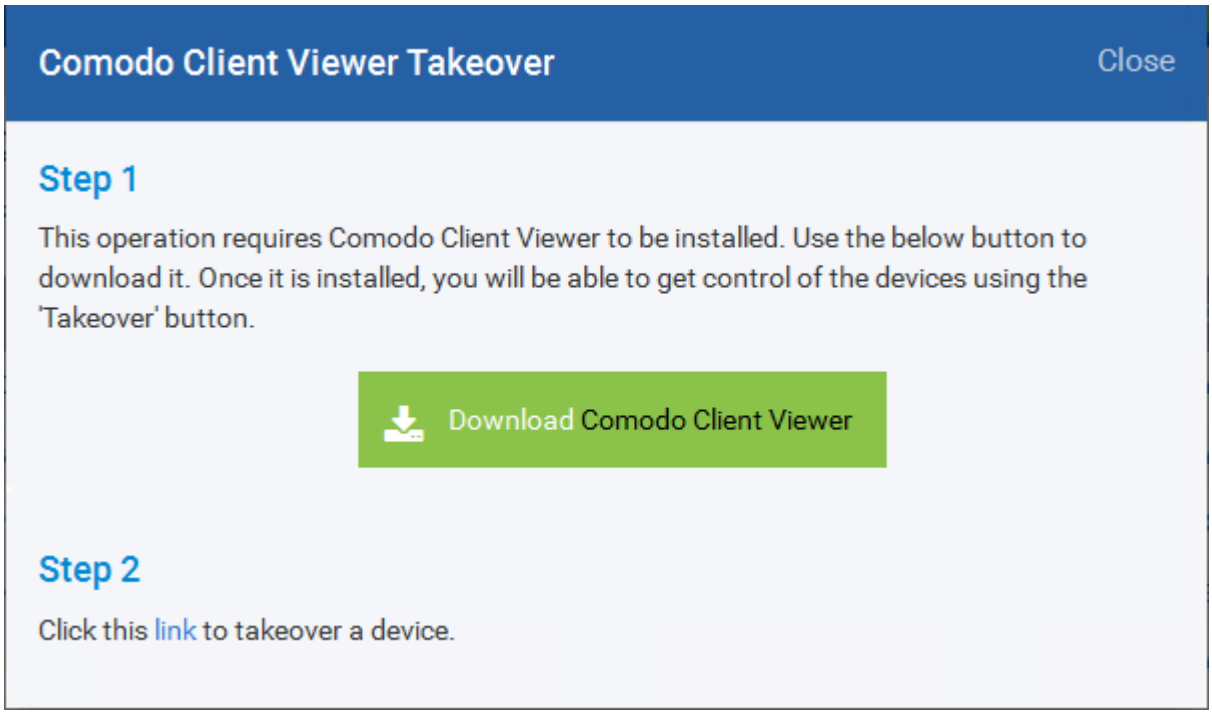
Comodo Client Viewer

To initiate a remote desktop connection

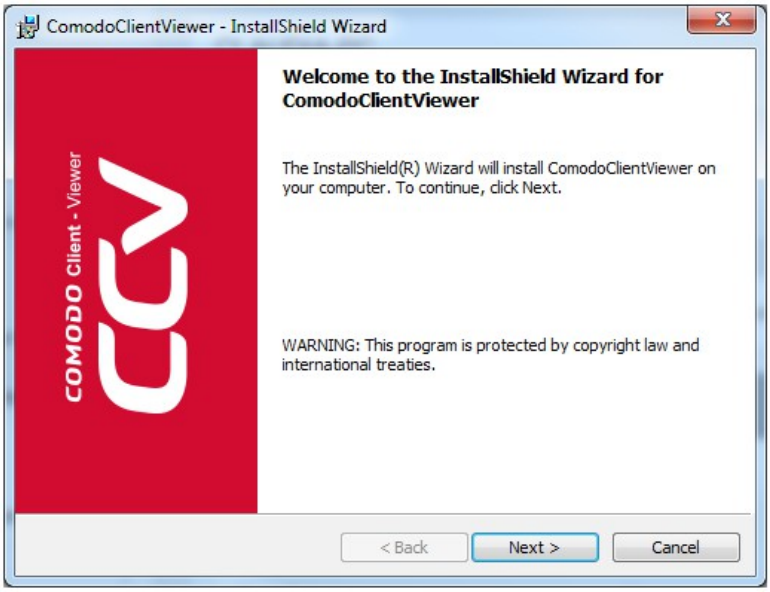
- Open Devices > Device List and select a Windows device
- Click the 'Takeover button' and select 'With Comodo Client Viewer'.



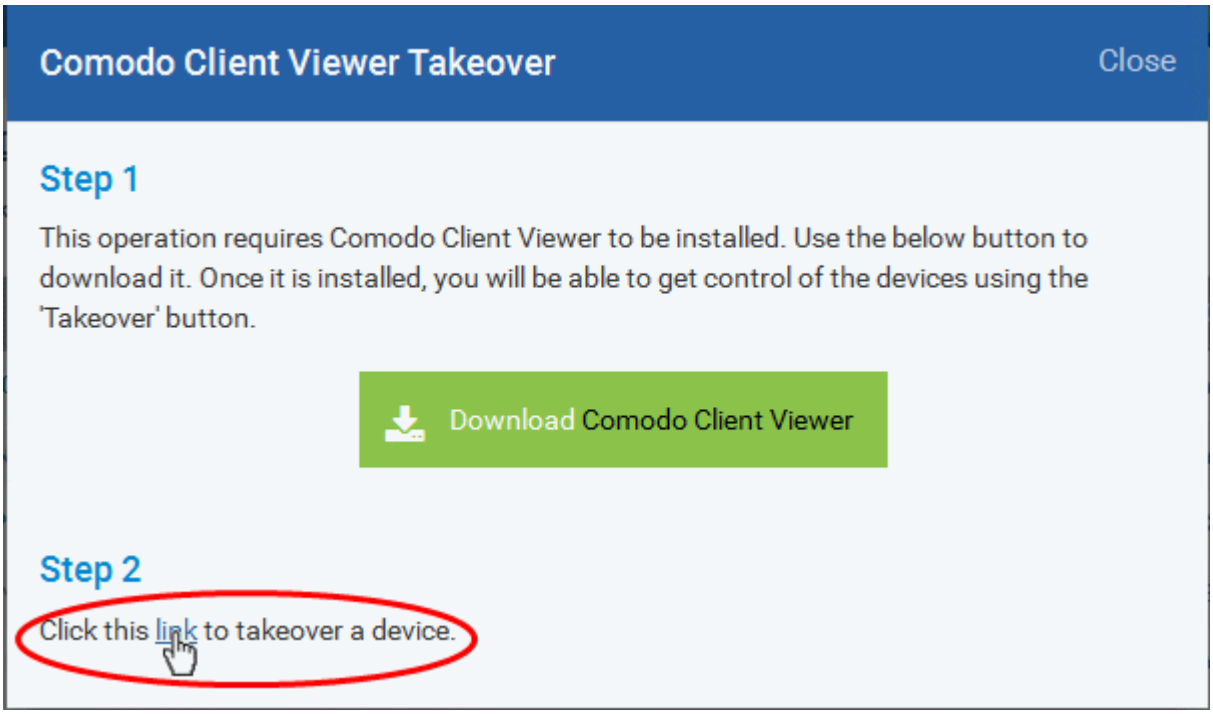
- If this is the first time you have used this feature then you will need to install the client viewer application:



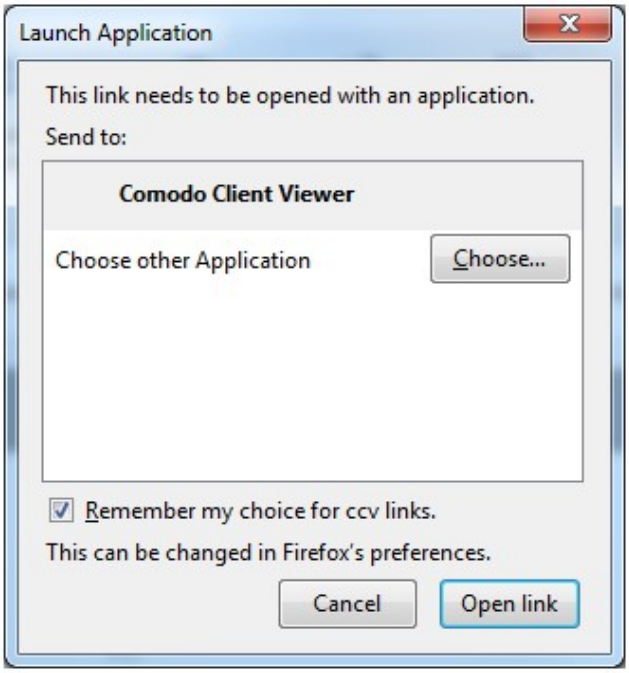
- Click 'Download Comodo Client Viewer' under 'Step 1'
- After downloading the setup file, double click on it to install the application.



- After installation, click 'link' under step 2:

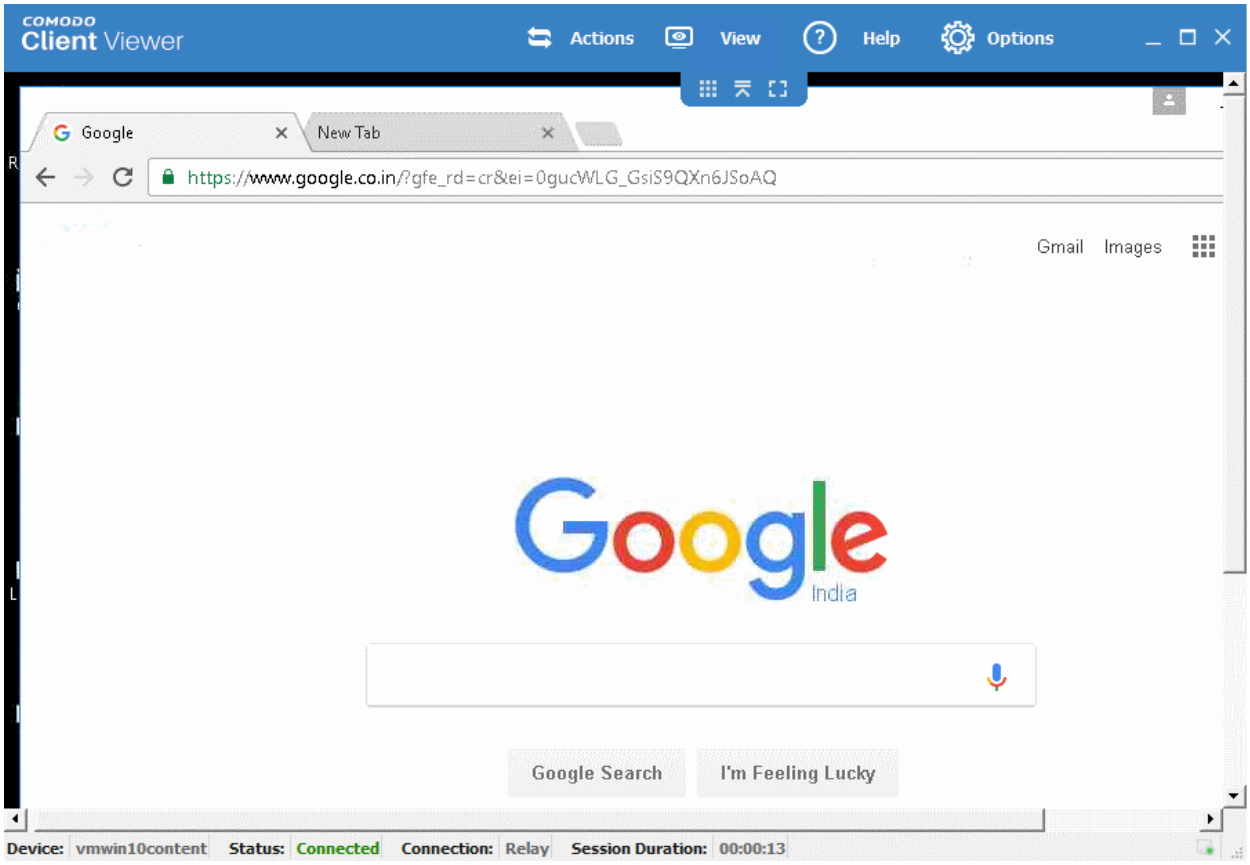


- Click 'Open Link' in the 'Launch Application' dialog to connect to the target desktop:

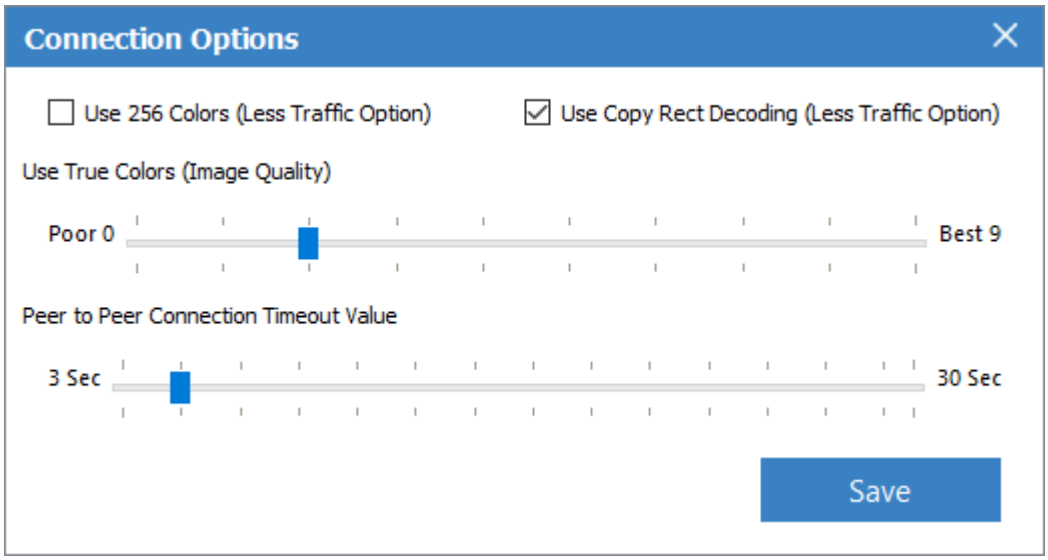


Note - If a newer version of the viewer is available, please download it to continue.

- Once connected, the client viewer interface will display the desktop of the remote computer:



- Administrators can now interact with the target device to perform tasks as required.
- The client interface contains the following menus and settings:
  - **Actions** - Allows you to change the display size of the remote desktop as you perfer. The available options are 'Full Screen', 'Fit to Height', 'Fit to Width' and 'Fit to Origin'
  - **View** - Contains options to send control commands to the endpoint. The available options are:
    - **Send Ctrl + Alt + Del** - Will send the Ctrl+Alt+Del key combination to the remote machine to open the Windows security screen. This allows you to lock the computer, log off the current user, change passwords, view the task manager or shut down/restart/hibernate the machine.
    - **Send Ctrl + Esc** - Will open the Windows 'Start' menu, allowing you to launch subsequent tasks..
  - **Options** - Clicking the  icon allows you to configure connection and display quality. Lower quality settings are preferable if your connection is slow.



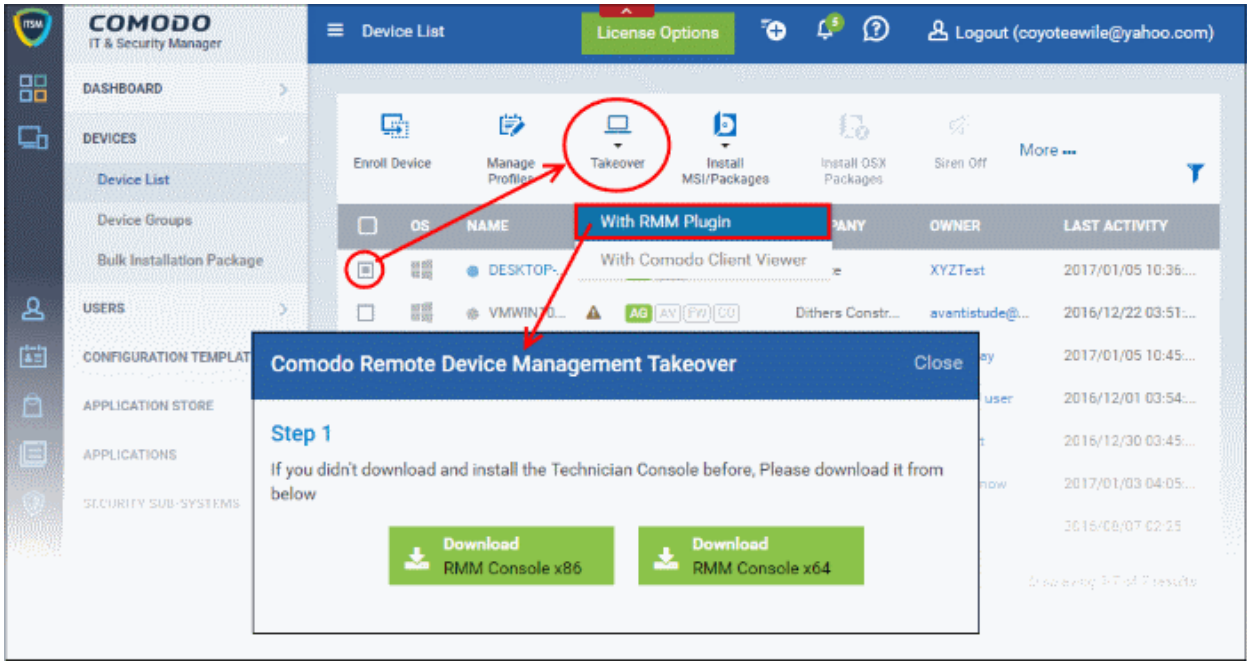
Comodo Remote Monitoring and Management (RMM)

Comodo's Remote Monitoring and Management (RMM) grants MSPs complete visibility and control over the systems they manage. C1 customers can use RMM to takeover Windows devices. In order to do that, administrators should:

- Install the RMM plugin agent on target Windows devices. For details about how to install RMM agent, refer to the section '**Remotely Installing Packages onto Windows Devices**'
- **Install the RMM Administrative Console**

To download the RMM admin console

- Click 'Devices' and choose 'Device List'.
- Choose a 'Windows' device, click 'Takeover' from the top then 'With RMM Plugin'



The 'Remove Device Management Takeover Wizard' will be displayed.

- Download the appropriate version of the RMM Console and install it on your target machines.

Once installed, select a Windows device from the 'Device List' interface and click 'Takeover' > 'With RMM Plugin' to remotely monitor, manage and take control of the device. See https://help.comodo.com/topic-289-1-719-8569-Support-Sessions-Interface-%E2%80%93-An-Overview.html for more details.

You can also open the RMM console from the system where it is installed and remote manage all the Windows devices that are enrolled for your C1 account. Please note that you can open only one instance of RMM console at a time. For more details on using RMM, refer to its guide at https://help.comodo.com/topic-289-1-719-8539-Introduction-to-Remote-Monitoring-and-Management-Module.html.

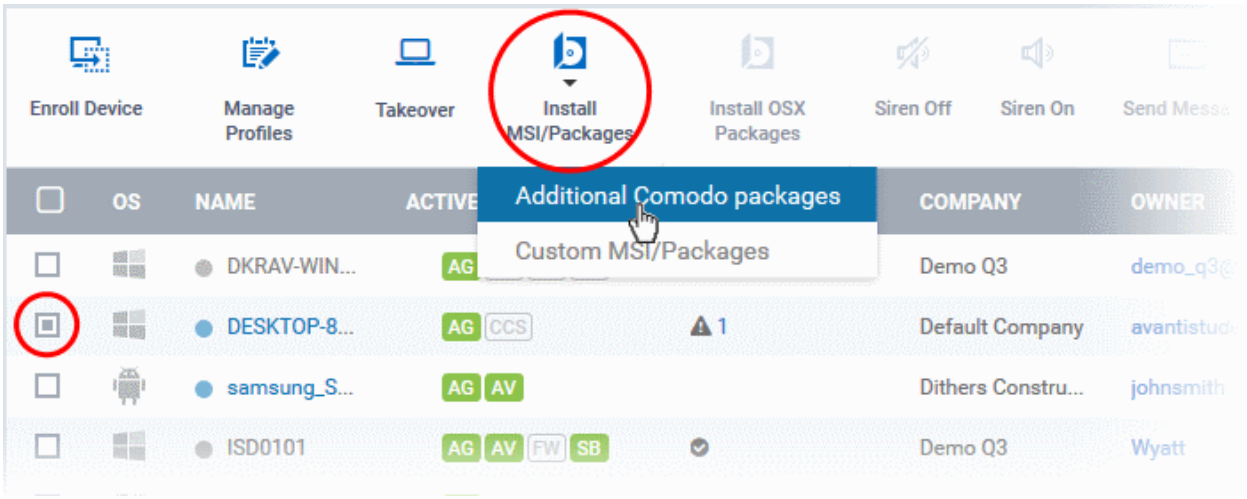
5.1.7. Remotely Installing and Updating Packages on Windows Devices

The 'Device List' interface allows administrators to install Comodo applications such as Comodo Client Security (CCS), the RMM agent and other third-party MSI packages. Administrators can also update ITSM packages which are installed on endpoints such as the Comodo Client Communication and Comodo Client Security agents.

Note: The option to install the RMM agent onto Windows endpoints is available for administrators that have logged into ITSM via the Comodo One interface.

To install MSI / ITSM packages

- Click 'Devices' and choose 'Device List'
- Select the Windows device(s) on which you want install the packages
- Click 'Install MSI/Packages'



- Alternatively, click the name of the device to open the 'Device Details' interface and click 'Install MSI/Packages' from the options at the top.

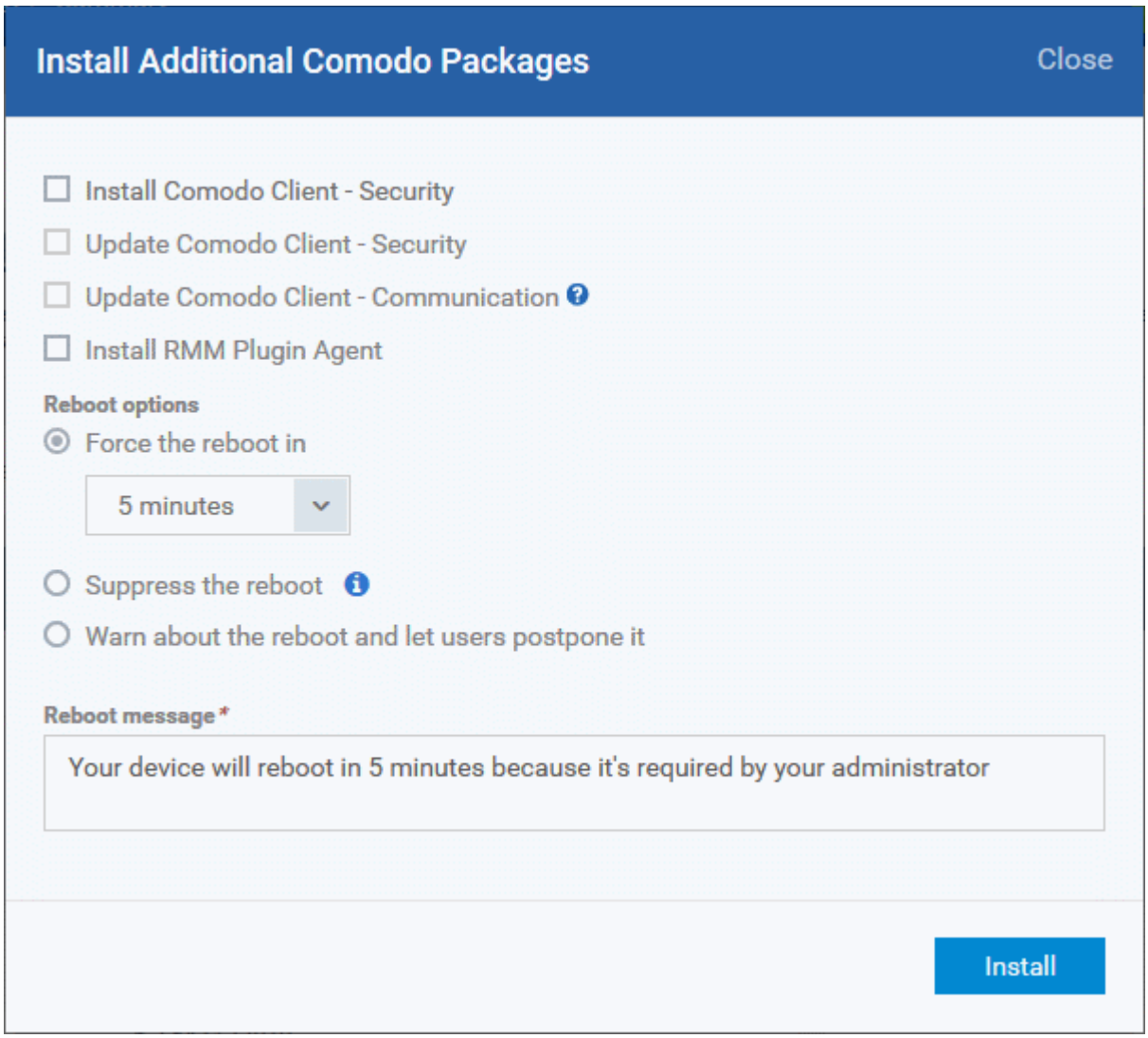
The drop-down displays options for:

- Installing and Updating ITSM Packages
- Installing Third Party MSI Packages

To install or update ITSM packages

- Select 'Additional Comodo packages' from the Install MSI Packages drop-down.

Note: Please note the packages should be enabled in the 'Extensions Management' interface to appear in this screen. Refer to the section 'Managing ITSM Extensions' for more details.



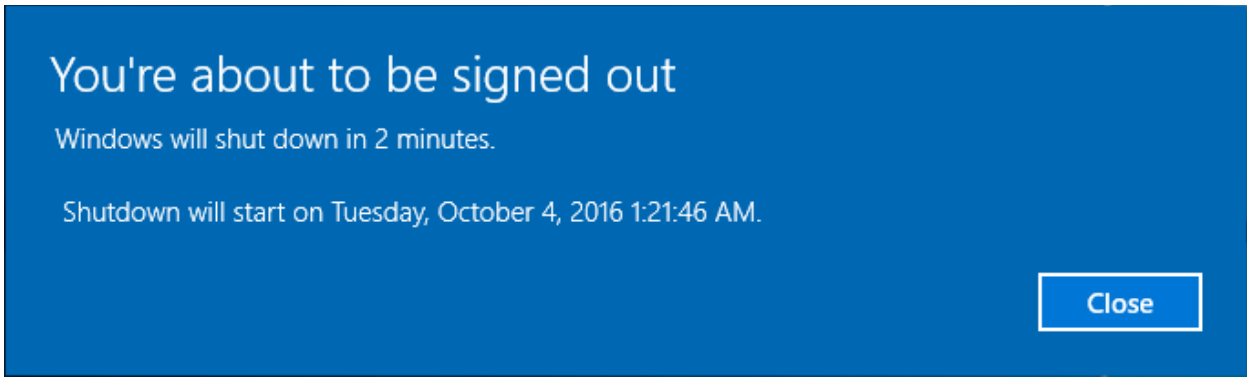
The list of available additional packages will be displayed. The available packages are:

- **Install Comodo Client - Security** - CCS is a complete endpoint security suite which features a powerful antivirus, enterprise class firewall, advanced host intrusion prevention and automatic containment of unknown files. ITSM allows you to configure which CCS security components are installed by applying configuration profiles. Also, you can remotely run on-demand AV scans, manage detected malware and more. Select this option if you want to install Comodo Client - Security software on the endpoint. Note: This option will be available only for endpoints on which CCS is not previously installed.
- **Update Comodo Client - Security** - Select this option to update the AV database and install software updates for CCS on the endpoint. This option is only available for endpoints with an out-dated version of CCS.
- **Update Comodo Client - Communication** - Select this option if you want to update the Comodo Client - Communication agent software on the endpoint. This option is only available for endpoints with an out-dated version of CCC agent.
- **Install RMM Plug-in Agent** - The RMM agent is a small piece of software which is installed on endpoints in order to communicate with ITSM. Select this option if you want to install RMM plug-in agent on the endpoint.

CCS requires the endpoint to be restarted in order for the installation to take effect. You can choose how the endpoint(s) are to be restarted from the 'Reboot Options'.

- To restart the end-point a certain period of time after installation, choose 'Force the reboot in...' , select a delay period and click 'Install'.

The following message will be displayed on the device:



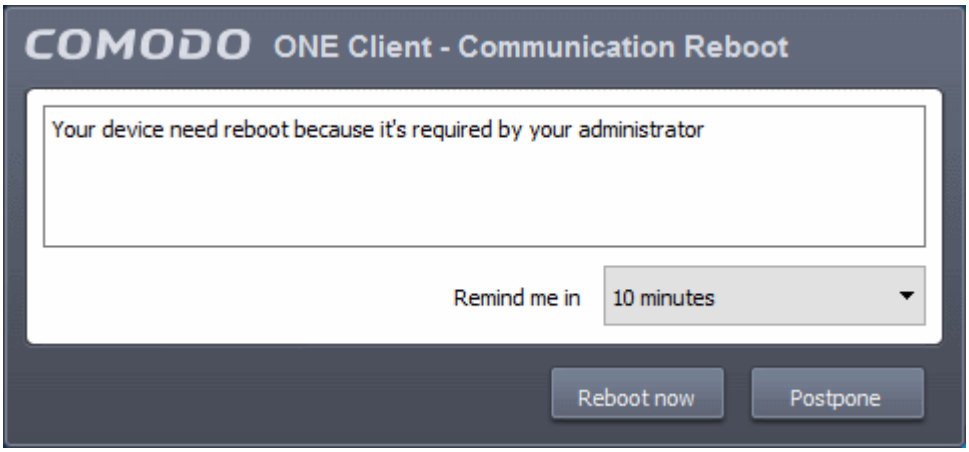
The device will be restarted automatically when the time period elapses.

- If you do not want the endpoint to restart automatically, then choose 'Suppress the reboot' and click 'Install'.

The endpoint will not restart on completion of the installation. However, the COCS installation will become fully functional only upon the next restart of the endpoint.

- To restart the end-point at user's convenience Choose 'Warn about the reboot and let users postpone it, enter the message to be displayed to the user in the 'Reboot message' field and click 'Install'.

On completion of installation, the message will be displayed at the device as shown below:



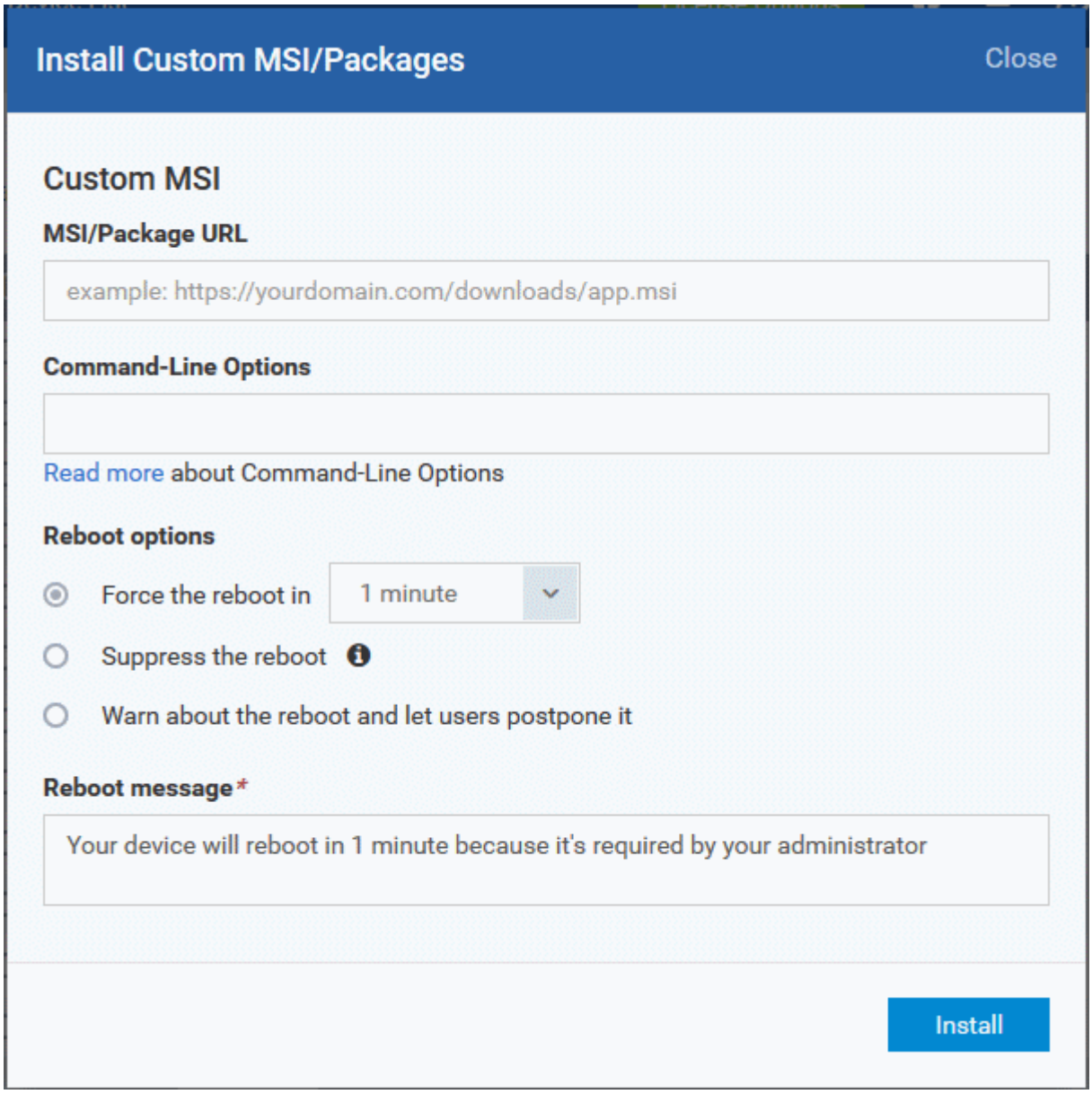
Users can choose to restart the endpoint immediately by clicking 'Reboot now', or postpone the restart by using the 'Remind me in' drop-down. The installation will be active only after the endpoint is restarted.

After CCS installation is complete, the security components that are active depends on the applied profile. Refer to the sections Assigning Configuration Profile to Selected Devices, Assigning Configuration Profile(s) to a Users' Devices, Assigning Configuration Profile to a User Group and Assigning Configuration Profile to a Device Group for more details.

To install third-party MSI packages

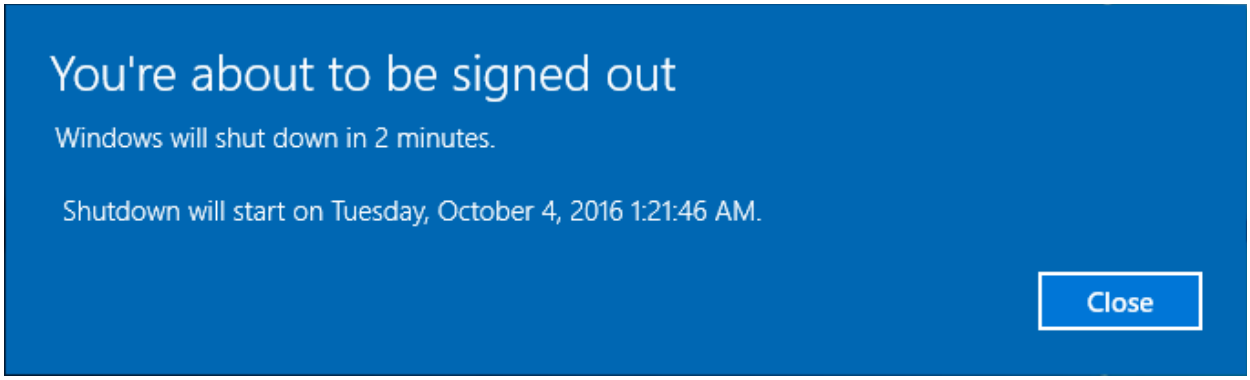
- Choose 'Custom MSI/Packages' from the 'Install MSI/Packages' drop-down

The 'Install Custom MSI/Packages' dialog will appear.



- Enter the URL of the MSI installer in full in the 'MSI URL' field, and make sure it is from a https site. For example, https://www.hass.de/files/nodes/story/45/npp.6.8.4.installer.msi
- Enter the MSI installation command line parameters in the 'Command-line Options' field. This is optional. Click the 'Read more' link to know more about command-line options.
- Select the 'Reboot Options' depending on whether the installation requires restart of the endpoint to take effect.
    - To restart the end-point after a certain period of time on completion of installation, choose 'Force the reboot in' and select the delay period and click 'Install'.

The following message will be displayed on the device:



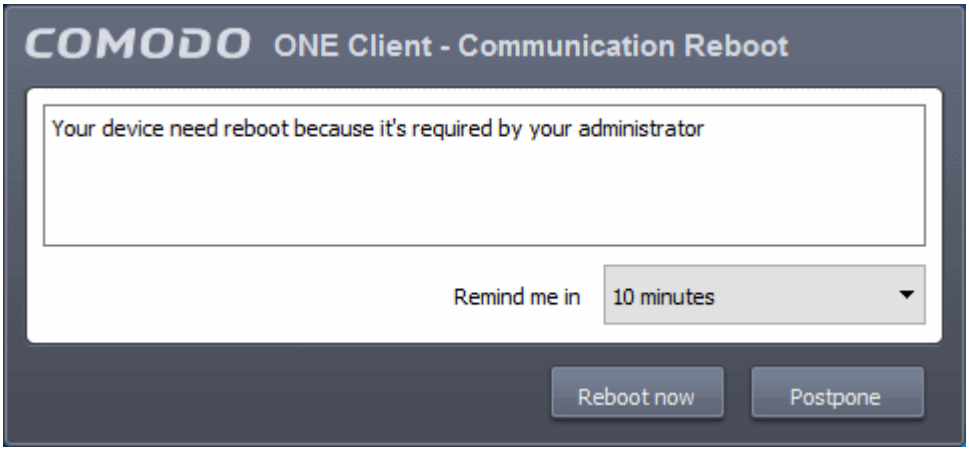
The device will be restarted automatically when the time period elapses.

- If you do not want the endpoint to restart automatically, then choose 'Suppress the reboot' and click 'Install'.

The endpoint will not restart on completion of the installation.

- To restart the end-point at user's convenience Choose 'Warn about the reboot and let users postpone it, enter the message to be displayed to the user in the 'Reboot message' field and click 'Install'.

The following message will be displayed on the device:



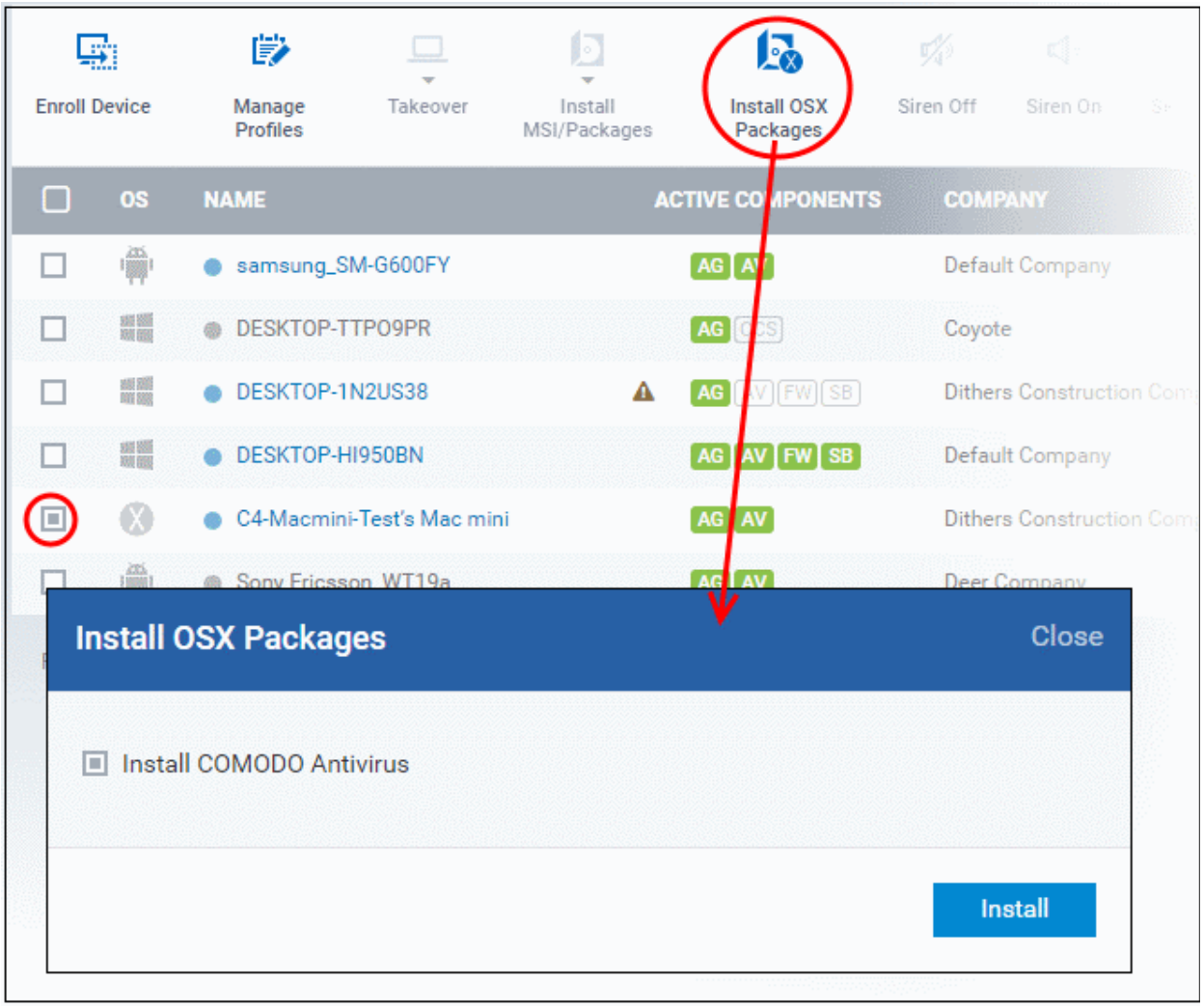
Users can choose to restart the endpoint immediately by clicking 'Reboot now', or postpone the restart by using the 'Remind me in' drop-down. The installation will be active only after the endpoint is restarted.

5.1.8. Remotely Installing Packages on Mac OS Devices

Administrators can remotely install Comodo Antivirus for Mac (CAVM) from the 'Device List' interface of ITSM.

To install OSX packages

- Click 'Devices' and choose 'Device List'
- Select the Mac OS device(s) to which you want install the packages



- Alternatively, click on the name of the device to open the 'Device Details' interface and click 'Install OSX Packages' from the options at the top.

The 'Install OSX Packages' screen displays the ITSM packages that can be installed on the Mac OS endpoint(s).

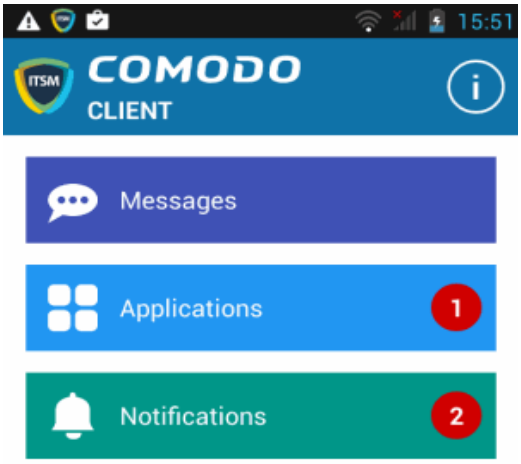
- Select the packages to be installed (currently only Comodo Anti-virus for Mac (CAVM) is available).
- Click the 'Install' button

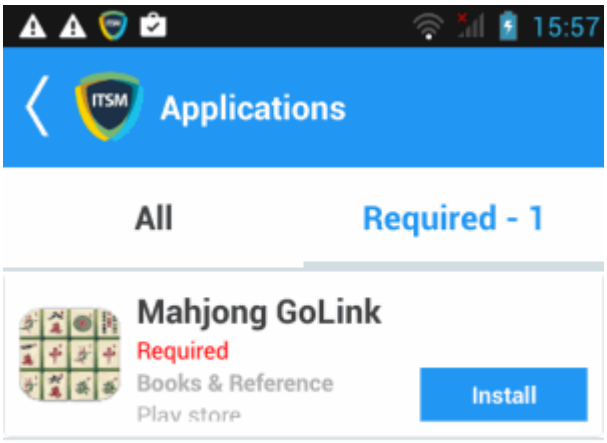
The command to install will be sent from ITSM for the process to begin. The security components that are active once CAVM is installed depends on the security profile applied. Refer to the sections **Assigning Configuration Profile to Selected Devices**, **Assigning Configuration Profile(s) to Users' Devices**, **Assigning Configuration Profile to a User Group** and **Assigning Configuration Profile to a Device Group** for more details.

5.1.9. Installing Apps on Android/iOS Devices

ITSM allows administrators to push applications to all enrolled mobile devices. Applications that the administrator intends to roll-out to user devices can be added to the ITSM Application Store. The sync between the ITSM server and the devices takes place every 24 hours. Alternatively, you can sync immediately if you click 'Inform Devices Now' in the iOS or Android store interfaces. For more on uploading application packages to the app store, see Application Store.

The 'Applications' stripe in the ITSM app on the device shows the number of mandatory apps that are waiting to be installed from the app store:

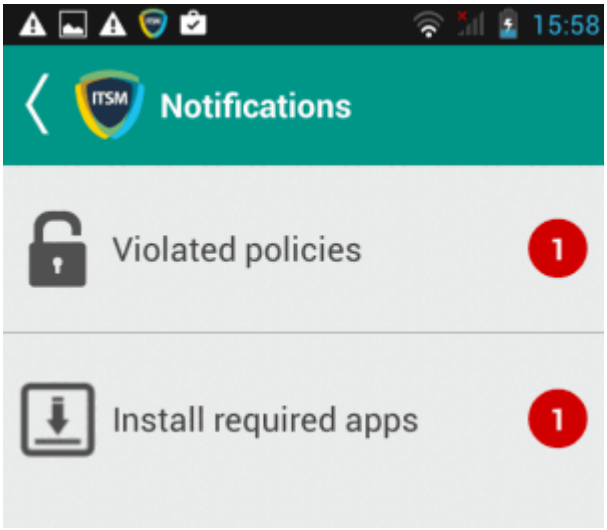




- **All** - Displays all apps available for installation, including mandatory and optional apps.
- **Required** - Displays apps that must be installed on the device to comply with the ITSM profile applied to the device.

- Tap 'Install' to download and install the apps.

ITSM also sends notification alerts to the devices if a mandatory app or a recommended app is uploaded to the Application Store.



- Tap 'Install required apps' to install the mandatory apps.

5.1.10. Generating an Alarm on Devices

If a device is mislaid, lost or stolen, administrators can make the device sound an alarm to help locate it. The alarm will sound at full volume, even if it is set to silent mode. Administrators can stop the alarm from the same interface.

The alarm can also be generated on several devices at once to grab the attention of users.

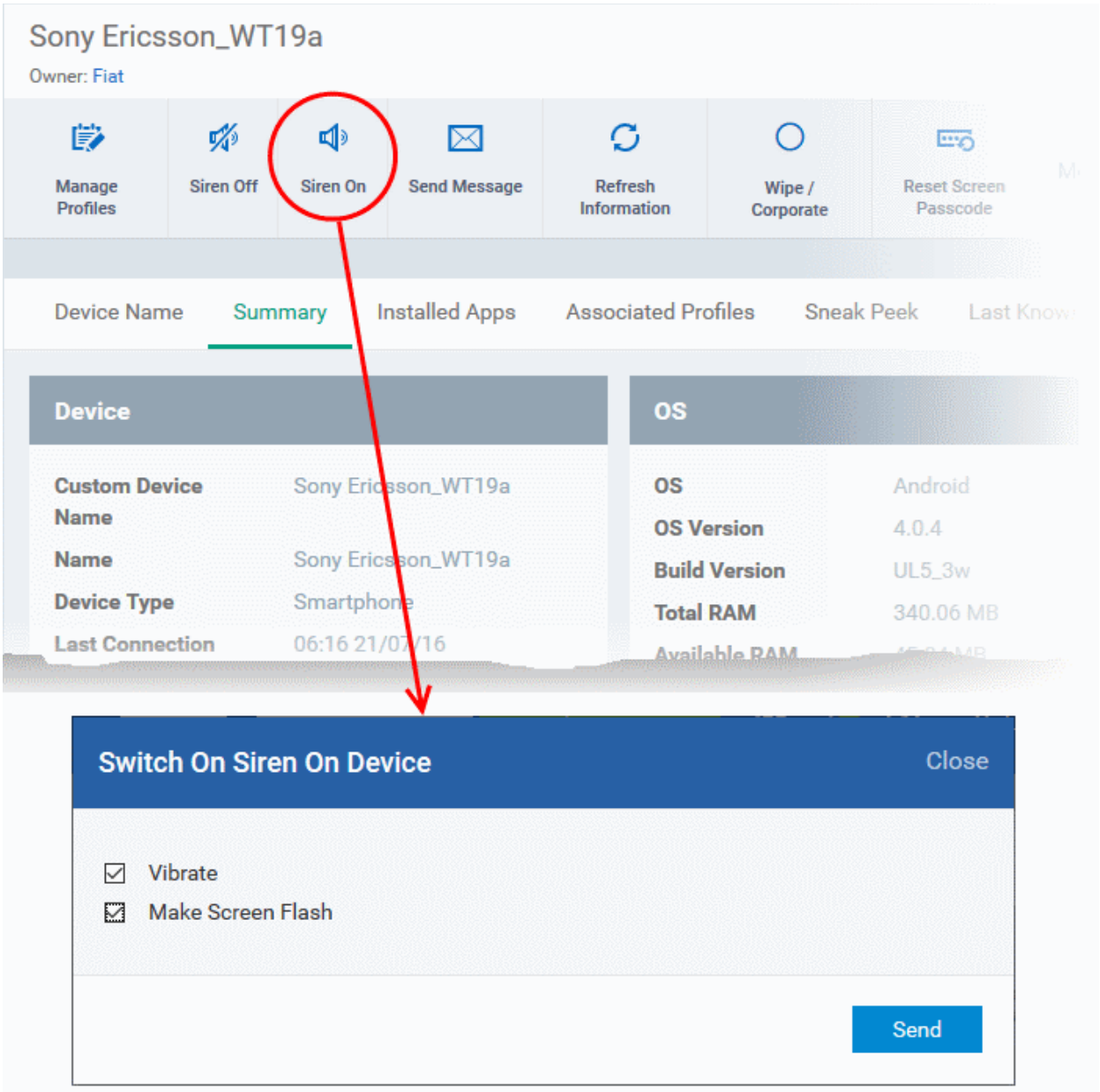
Note: This feature is available only for Android devices.

The following sections contain more information on:

- Generating alarm on a single device
- Generating alarm on several devices

To generate alarm on a single device

- Click 'Devices' and choose 'Device List'
- Click the name of the device on which you want to sound an alarm
- Click the 'Siren On' option in the 'Device Details' interface



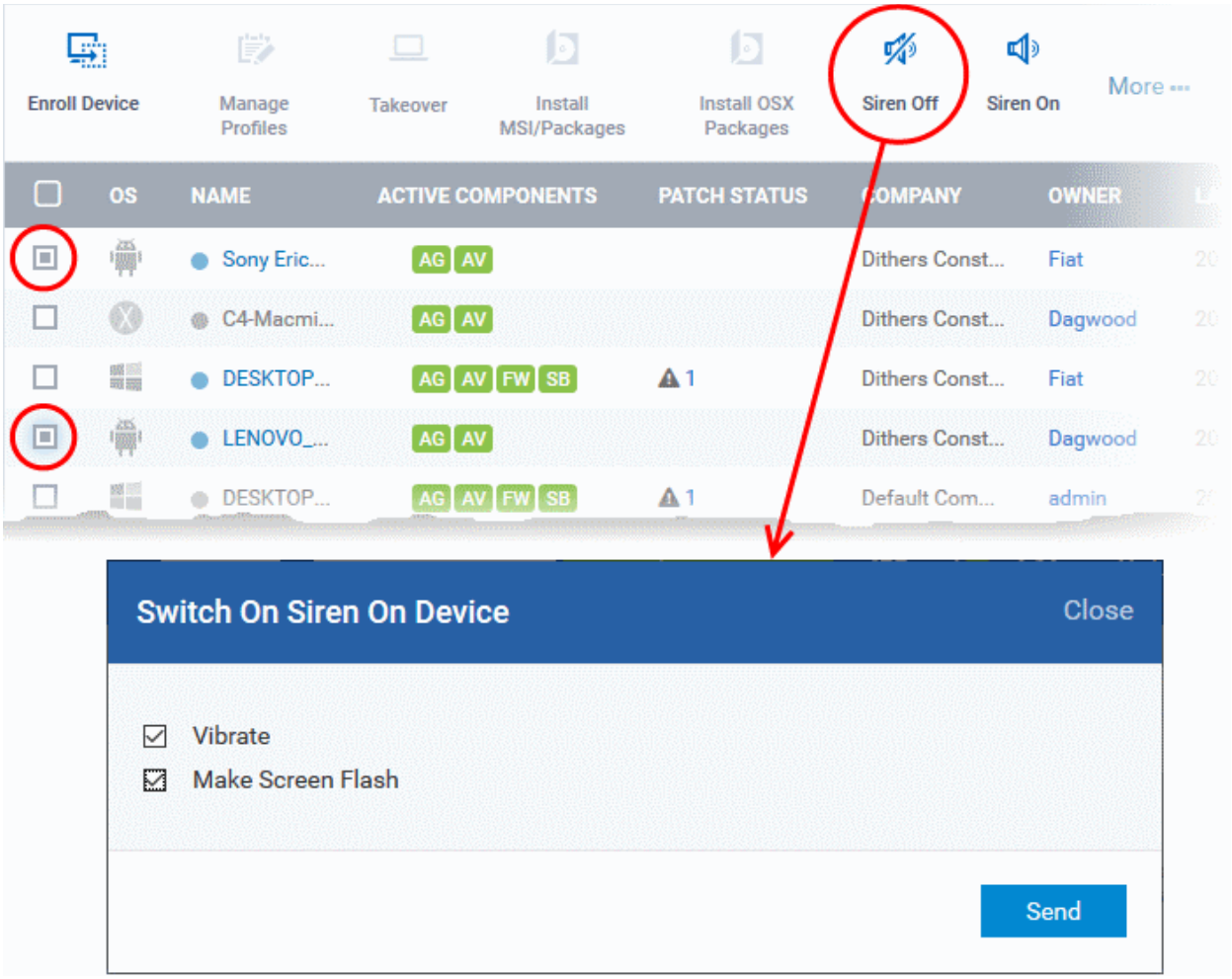
You can choose from the following options:

- Vibrate - The device will vibrate along with the siren
- Make screen flash - The device screen will flash intermittently along with the siren

- Click the 'Send' button to issue the alarm.
- To switch off the alarm, click 'Siren Off' from the same interface.

To generate alarm on several devices

- Click 'Devices' and choose 'Device List'
- Select the devices on which you want to sound an alarm
- Click the 'Siren On' option at the top



You can choose from the following options:

- Vibrate - The devices will vibrate along with the siren
- Make screen flash - The devices' screen will flash intermittently along with the siren

- Click the 'Send' button to issue the alarm

To stop the alarm

- Select the device(s) which should stop sounding an alarm, from the 'Device List' interface.
- Click 'Siren Off' from the options at the top.

5.1.11. Locking/Unlocking Selected Devices

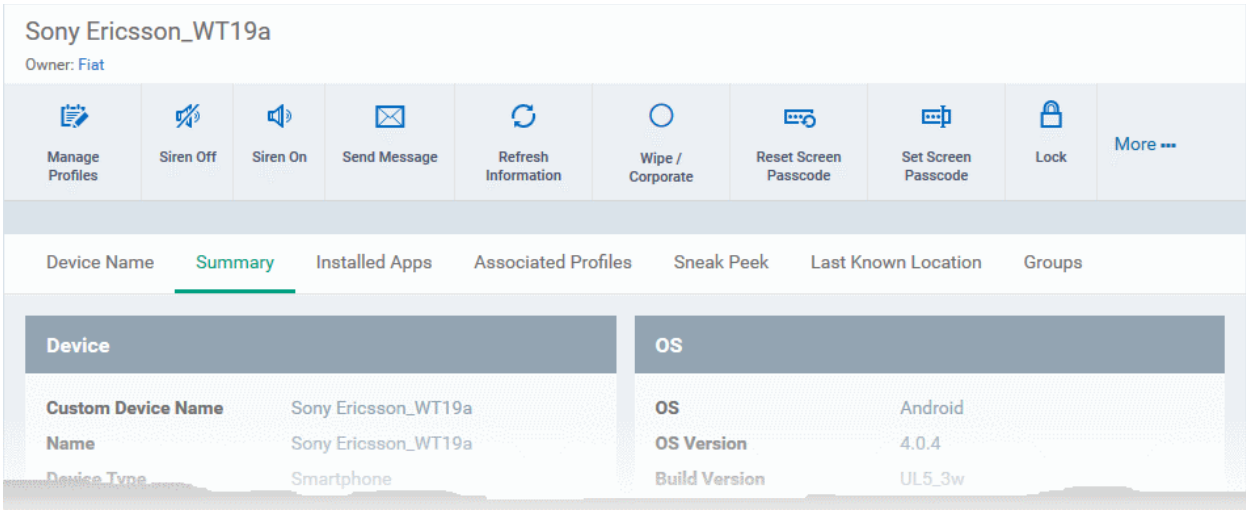
Administrators can remotely send a lock command to a device to prevent mislaid devices from being accessed by unauthorized persons, or to generally block access to the device. Locked devices can only be opened by entering a password on the device.

The following sections contain more information on:

- Locking a single device
- Locking several devices at-once

To remotely lock a single device

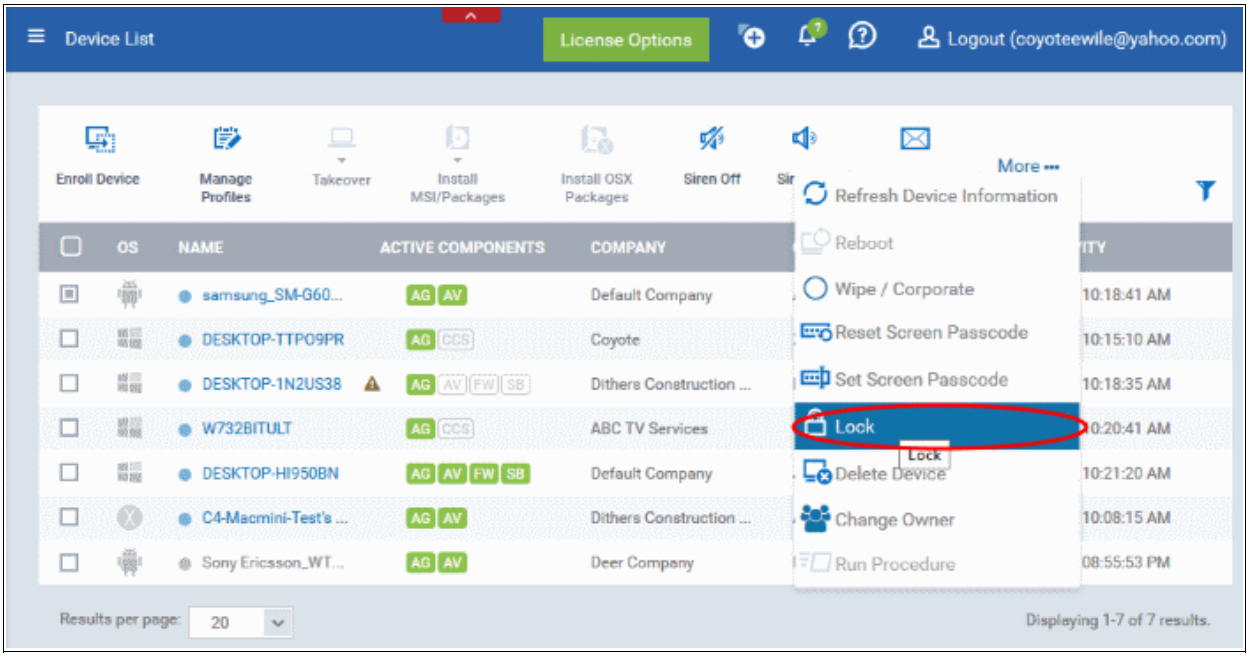
- Click 'Devices' and choose 'Device List'.
- Click the name of the device to be locked, to open the device details interface.
- Click the 'Lock' option from the top. If 'Lock' is not displayed, click 'More...' and choose 'Lock' from the options



The lock command will be sent. The device will be locked and the user can unlock the device by entering the screen lock password.

To remotely lock several devices at-once

- Click 'Devices' and choose 'Device List'
- Select the devices to be locked, from the list
- Click the 'Lock' option from the top or click 'More...' and choose 'Lock' from the options



The lock command will be sent. The devices will be locked and the user(s) can unlock the device(s) by entering the screen lock password.

5.1.12. Wiping Selected Devices

Confidential corporate documents and sensitive information can be stolen from a lost or stolen device. In order to prevent such information from leaking, administrators can remotely erase the contents of a lost device from the 'Device List' interface.

Tip: Administrators can also configure the device to automatically wipe itself if somebody enters the wrong password a certain number of times. The automatic wipe feature can be enabled in the device profile along with the

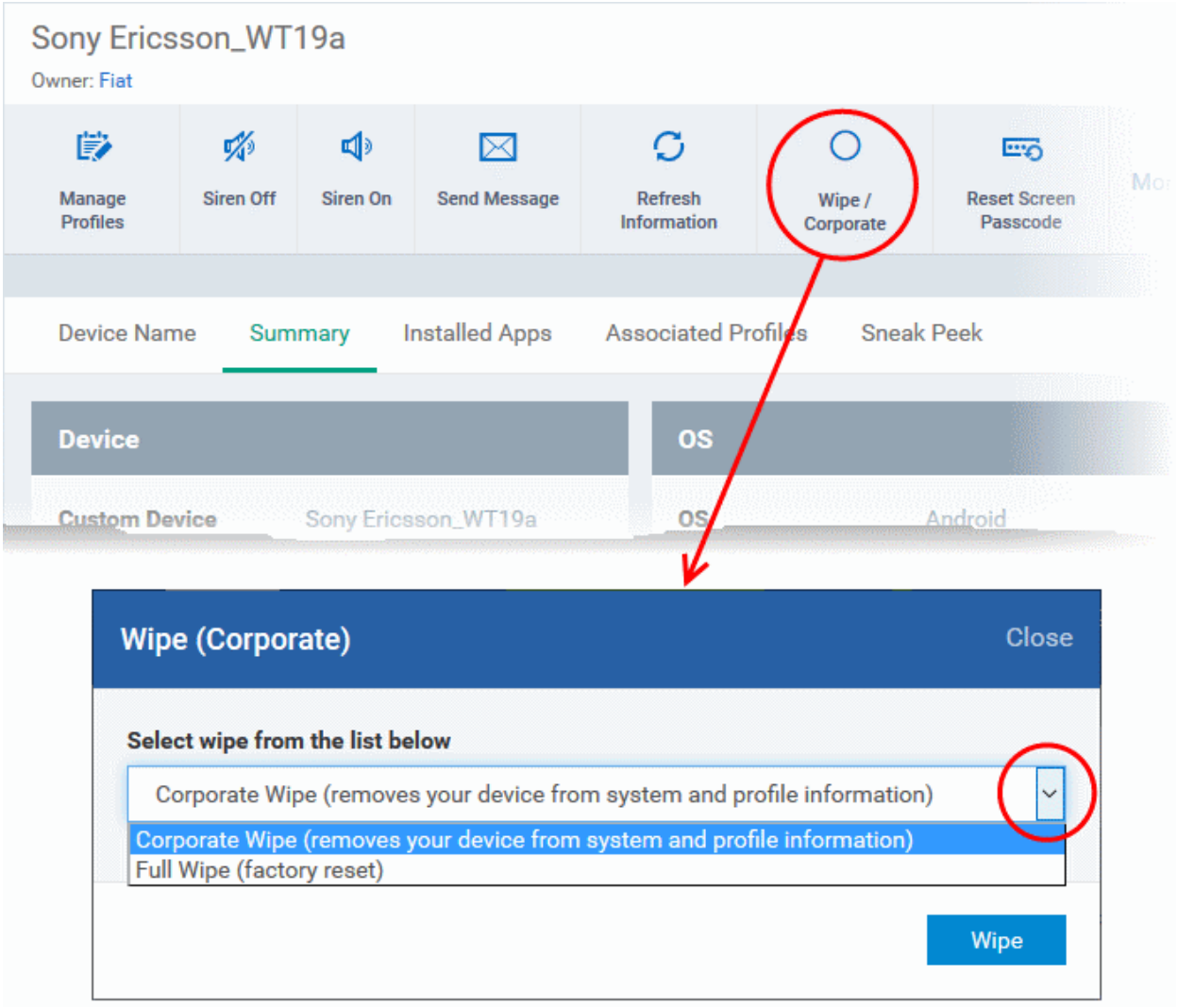
threshold of how many incorrect attempts should be allowed. To view this section, open 'Add/Edit Android Profile / iOS Profile > 'Passcode' (or refer to Passcode settings sections under Profiles for Android Devices and Profiles for iOS Devices in this guide).

The following sections explain more about:

- Wiping a single device
- Wiping several devices at-once

To erase the contents stored in a selected device

- Click 'Devices' and choose 'Device List'
- Click on the name of the device to be wiped to open the device details interface
- Click 'Wipe / Corporate' from the options at the top or click 'More...' and choose 'Wipe / Corporate' from the options



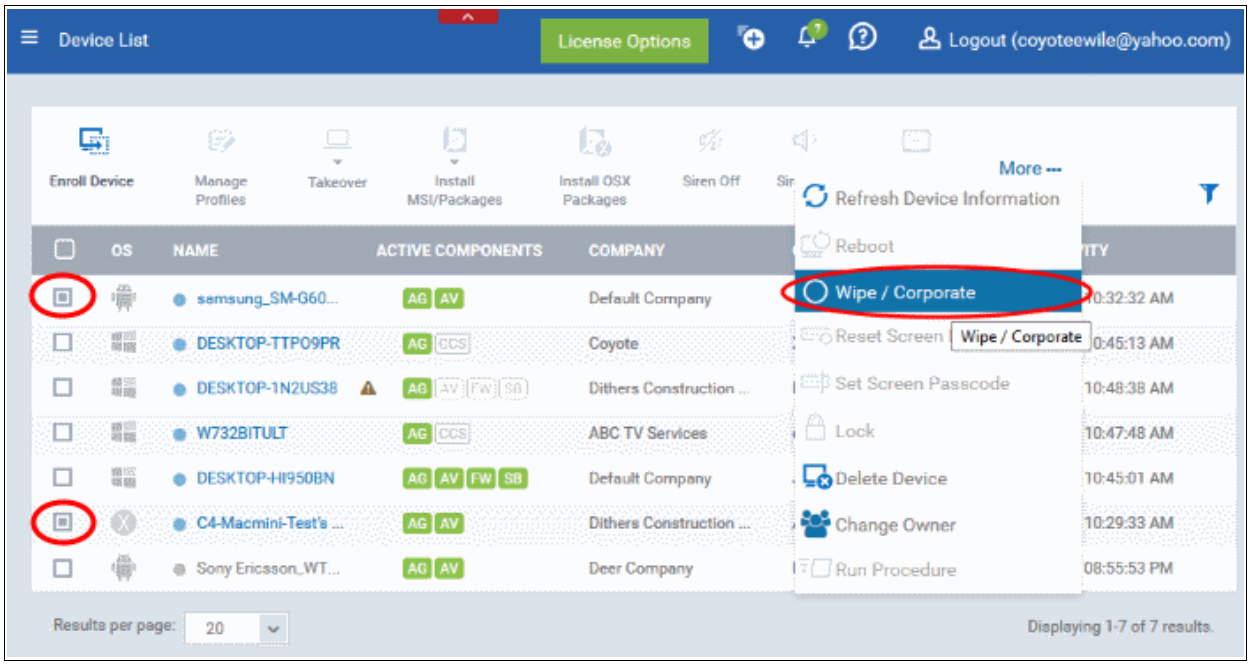
The 'wipe' dialog will open.

- Select the content to be erased.
  - To remove only ITSM agent and configuration profiles, select 'Corporate Wipe' from the drop-down
  - To erase all the data from the device and the SD card, select 'Full Wipe' from the drop-down. The device will be returned to default factory settings after the wipe operation.
- Click the 'Wipe' button.

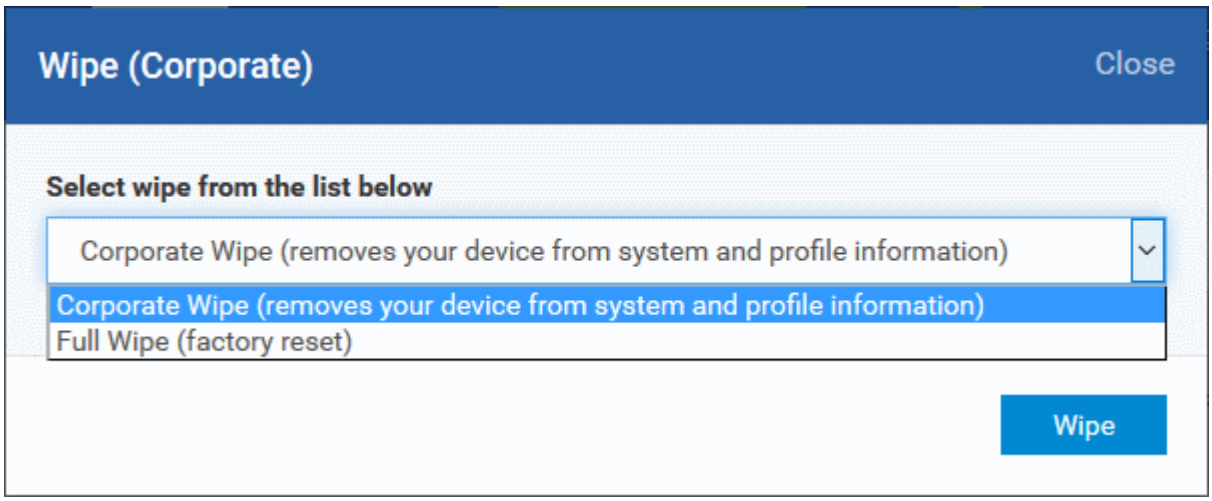
The wipe command will be sent and the data stored in the device will be deleted as per the wipe option chosen.

To erase the contents from several devices

- Click 'Devices' and choose 'Device List'
- Select the devices to be wiped
- Click 'Wipe / Corporate' from the options at the top or click 'More...' and choose 'Wipe / Corporate' from the options



The 'wipe options' dialog will open.



- Select the content to be erased.
  - To remove only ITSM agent and configuration profiles, select 'Corporate Wipe' from the drop-down
  - To erase all the data from the device and the SD card, select 'Full Wipe' from the drop-down. The device will be returned to default factory settings after the wipe operation.
- Click the 'Wipe' button.

The wipe command will be sent and the data stored in the devices will be deleted as per the wipe option chosen.

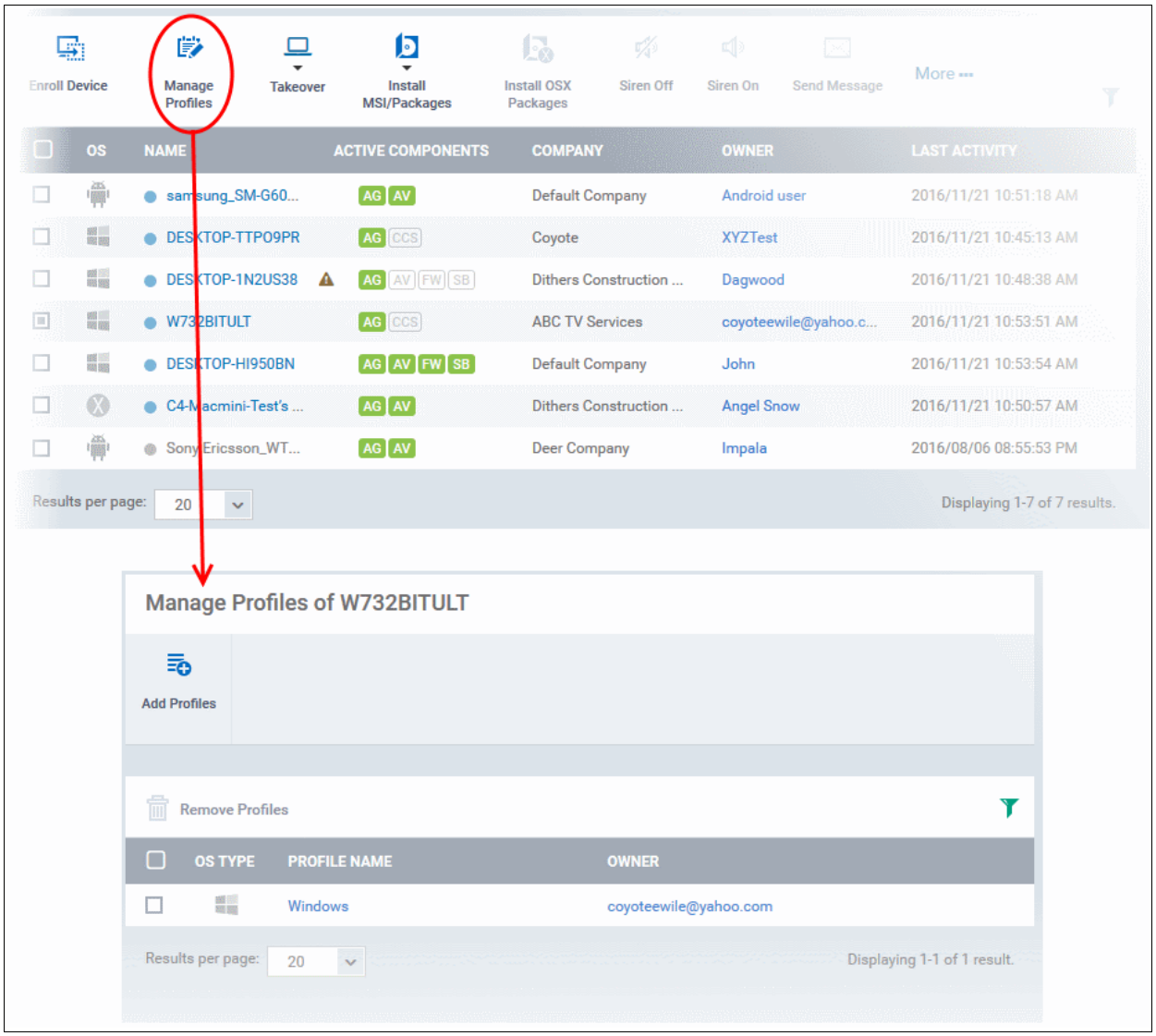
5.1.13. Assigning Configuration Profiles to Selected Devices

The device list interface allows administrators to view current configuration profiles in effect on selected devices. You can also apply new configuration profiles or remove profiles. Profiles applied from this interface will be added to any existing profiles on the device (such as profiles from a device group or user group). In case the settings in a profile clash with those in another profile, ITSM follows the 'Most Restrictive' policy. For example, if a profile allows the use of the camera and another restricts its use, the device will not be able to use the camera.

For more details on profiles, refer to the chapter Configuration Profiles.

To manage profiles applied to a device

- Click 'Devices' and choose 'Device List'
- Select the device to be managed and click 'Manage Profiles' from the options at the top



- Alternatively, click on the name of the device to be managed to open the device details interface and choose 'Manage Profiles' from the options at the top

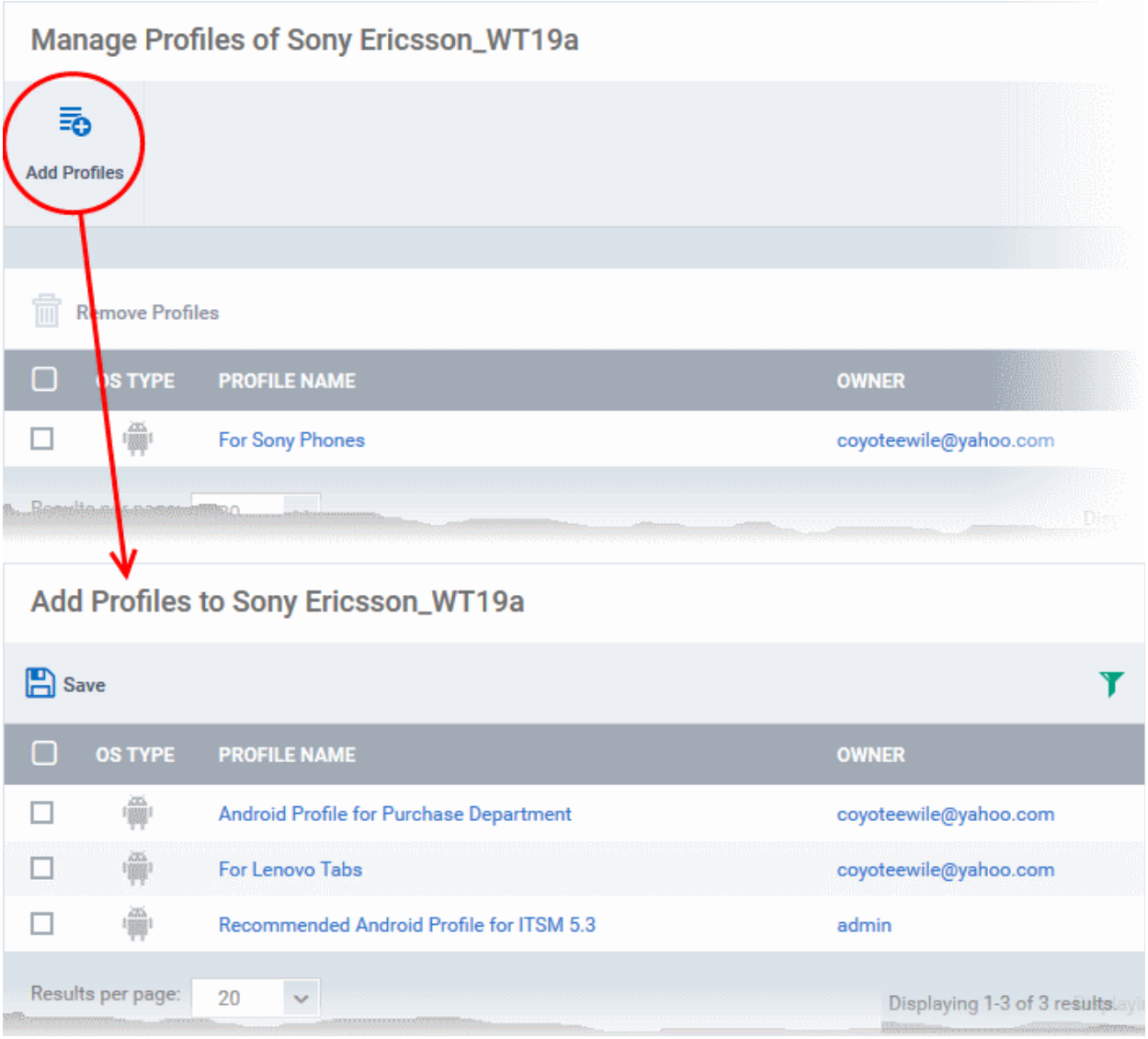
The list of profiles currently active on the device will be displayed.

Manage Profiles - Column Descriptions	
Column Heading	**Description**
OS Type	Indicates the operating system of the device.

Profile Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section Editing Configuration Profiles for more details.
Owner	Indicates the Administrator that created the profile. Clicking the administrator name will open the user information interface of the administrator. Refer to the section Viewing the Details of a User for more details.

Note: Device group and user group profiles applied to the device will not be shown here. To view the profiles applied to a device group refer to the section Viewing and Managing Profiles Associated with a Device.

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



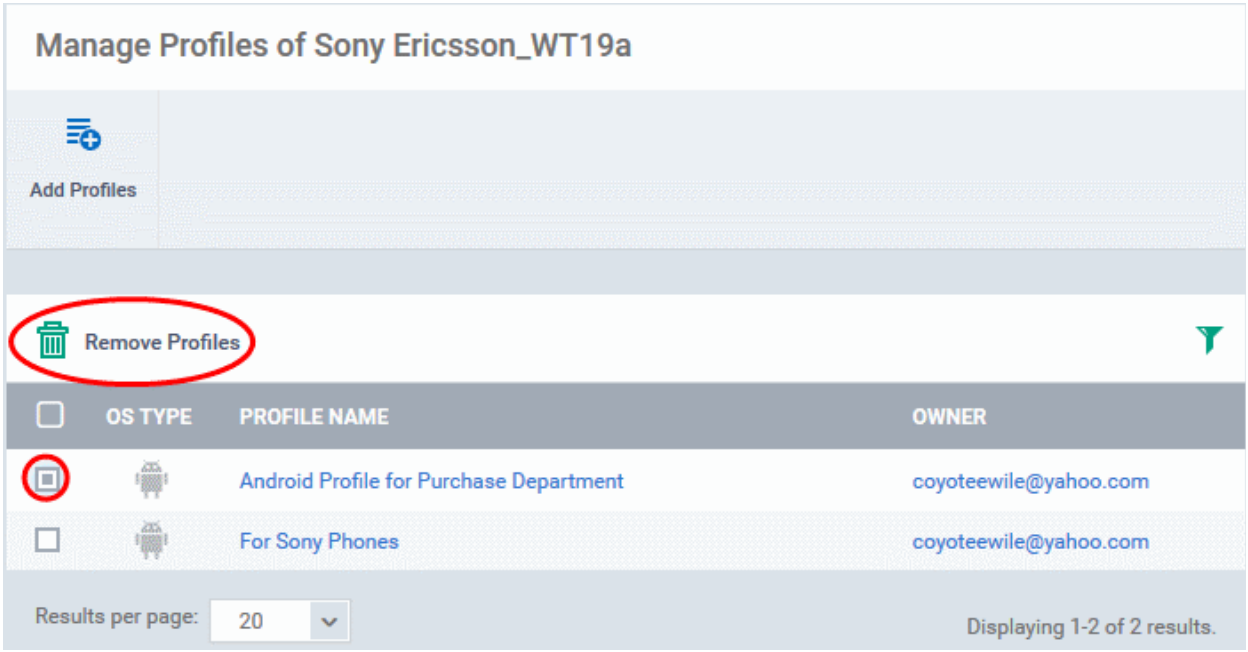
A list of all profiles applicable to the chosen device, excluding those that are already applied to the device will be displayed.

- Select the profile(s) to be applied to the device

Tip: You can use the search and filter options that appear on clicking the funnel icon at the top right to search for the profile(s) to be applied.

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

- To remove existing profile(s), select the profiles to be removed from the 'Manage Profiles' interface and click on 'Remove Profiles' from the options that appear on top.



The selected profile(s) will be removed from the device immediately.

5.1.14. Setting / Resetting Screen Lock Password for Selected Devices

Administrators can remotely set a new screen lock passcode (or reset the existing code) for enrolled devices from the 'Device List' interface.

Note: Setting new passcode from ITSM is not supported for iOS devices.

The following sections explain more about:

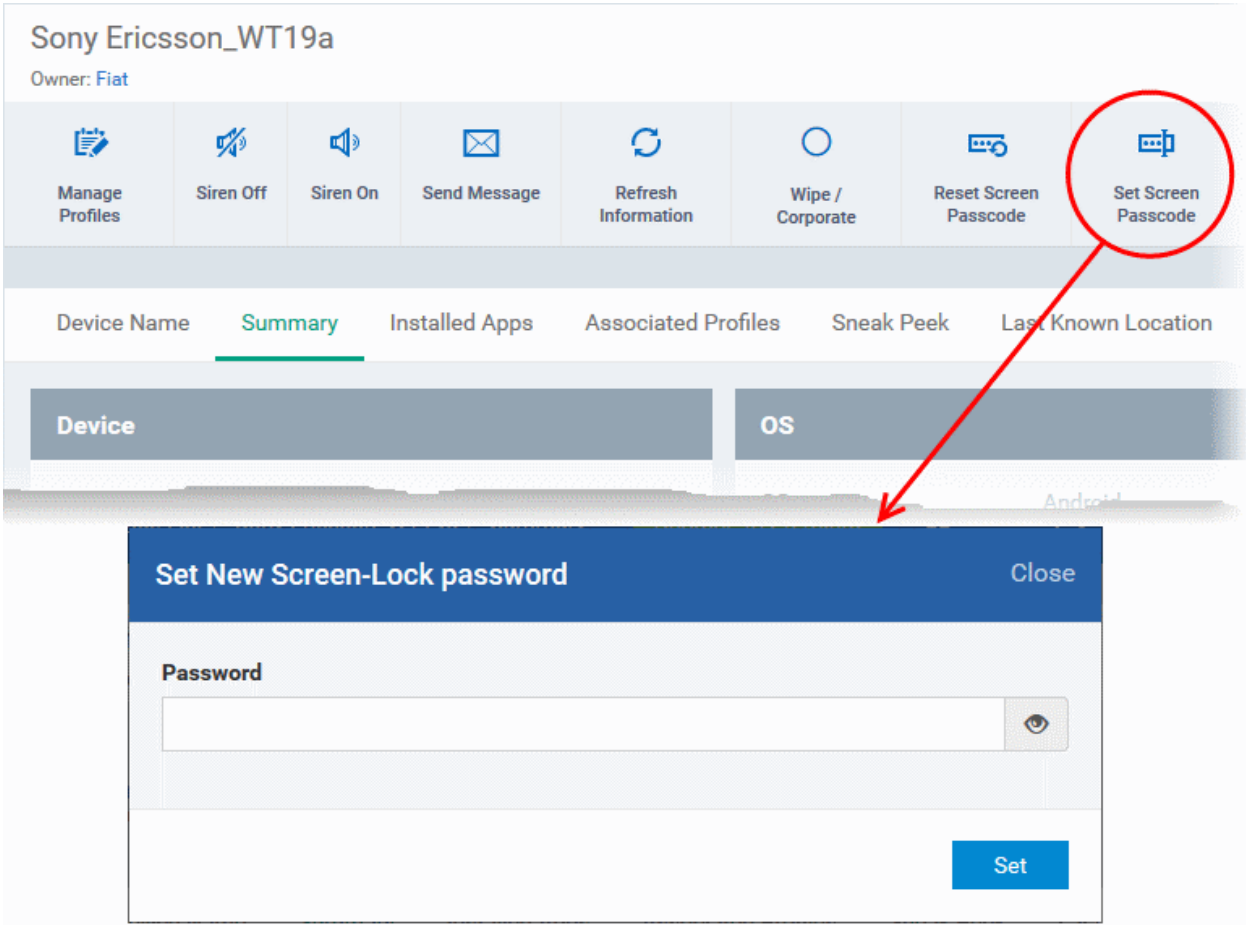
- Settings and resetting password for a single device
- Settings and resetting password for several devices at-once

To set a new screen lock password or remove password for a single device

- Click 'Devices' and choose 'Device List'
- Click on the name of the device for which a new passcode is to be created or existing passcode is to be reset

The device details interface will open.

- To set a new password, choose 'Set Screen Passcode' from the options at the top or click 'More...' and choose 'Set Screen Passcode' from the options.



The 'Set New Screen-Lock password' dialog will appear.

- Enter the new password in the 'password' text field.

Tip: You can use the eye icon  at the right end of the text field to display of hide the typed password.

- Click 'Set'.

The command will be sent to the device. This new password should be entered on the device to unlock it.

Note: If a passcode profile has been configured for the selected device, make sure to enter the new password that complies with the profile.

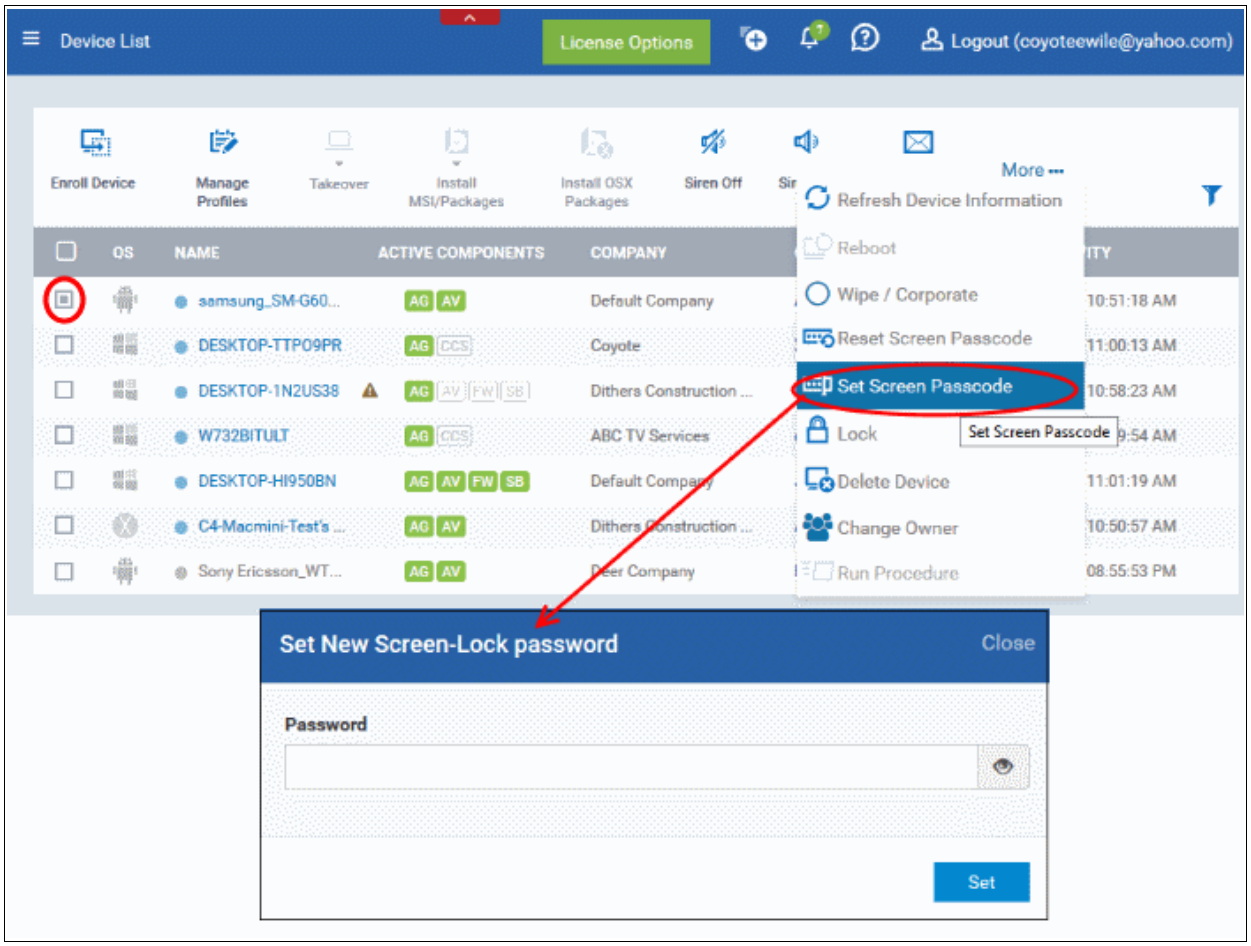
- To clear the existing password on the device choose 'Reset Screen Passcode' from the options at the top, or click 'More...' and choose 'Reset Screen Passcode' from the options.

The command will be sent to the device and the current screen lock password will be cleared. A message will also be sent to the device regarding the password change. If a password profile is applied the device, the user will be required to enter a new password that complies with the profile.

To set a new screen lock password or remove password for several devices

- Click 'Devices' and choose 'Device List'
- Select the devices to set/reset password.
- To set a new password, choose 'Set Screen Passcode' from the options at the top or click 'More...' and

choose 'Set Screen Passcode' from the options.



The 'Set New Screen-Lock password' dialog will appear.

- Enter the new password in the 'password' text field.

Tip: You can use the eye icon  at the right end of the text field to display of hide the typed password.

- Click 'Set'.

The command will be sent to all the devices at-once. From the next unlock operation, the users should enter the new password to unlock the device.

Note: If a Passcode profile has been configured for the selected devices, make sure to enter the new password that complies with the profile.

- To clear the existing passwords of the devices, select the devices and choose 'Reset Screen Passcode' from the options at the top or click 'More...' and choose 'Reset Screen Passcode' from the options.

The command will be sent to all the devices and the current screen lock password will be cleared. A message also will be sent to the device regarding the screen lock password change. If a Password profile is configured in the device, the user will be required to enter a new password that complies with the profile.

5.1.15. Updating Device Information

The agent on an enrolled device sends full information about the device to the ITSM console. This includes OS version, memory status, network details, IMEI number, location, MAC address of Bluetooth, MAC address of WiFi

and so on. The interval at which the device sends this information can be configured in the 'Settings' interface. If required, device information can be fetched in real time by clicking 'Refresh Device Information' in the 'Device List' interface.

The following sections explain more about:

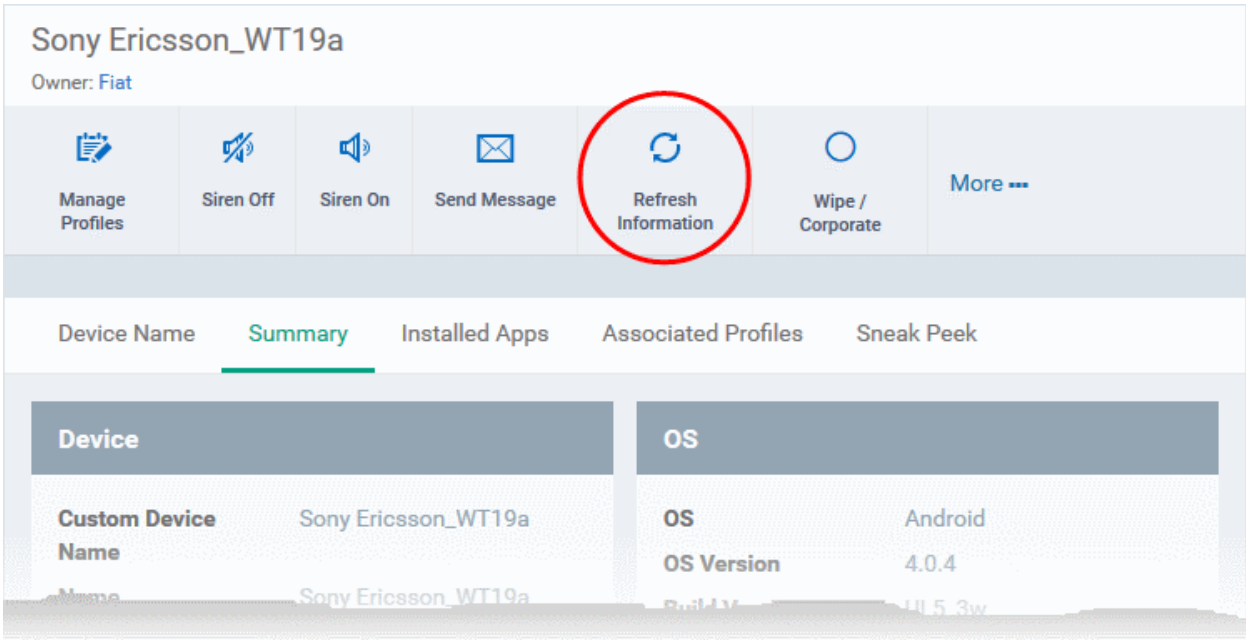
- Getting updated information from a single device
- Getting updated information from several devices at once

Getting updated information from a single device

- Click 'Devices' and choose 'Device List'
- Click on the name of the device

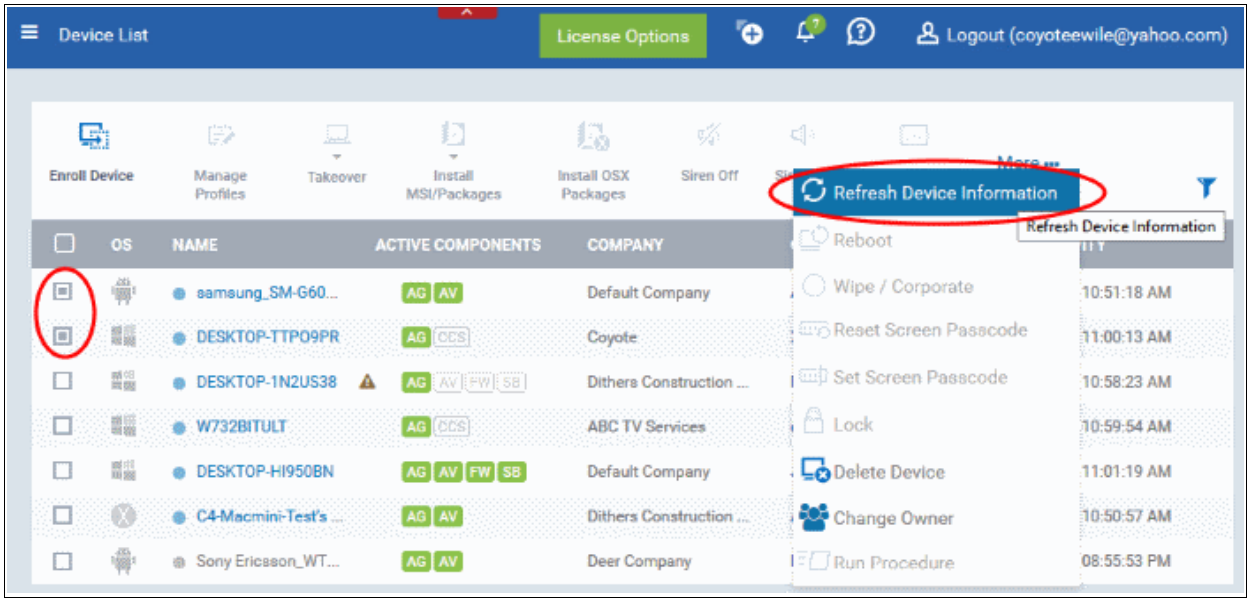
The device details interface will open with information on the device fetched from last polling time of the agent installed on the device.

- Click 'Refresh Information' from the options at the top



Getting updated information from several devices

- Click 'Devices' and choose 'Device List'
- Select the devices to refresh information from.
- Click 'Refresh Device Information' from the options at the top or click 'More...' and choose 'Refresh Device Information' from the options.



5.1.16. Sending Text Message to Devices

ITSM allows administrators to send text messages to enrolled Android and iOS devices. This will come in handy if you need to send important device or company notifications to all users.

Note: For iOS devices, the ITSM client should be installed for this feature to be supported.

The following sections explain more about:

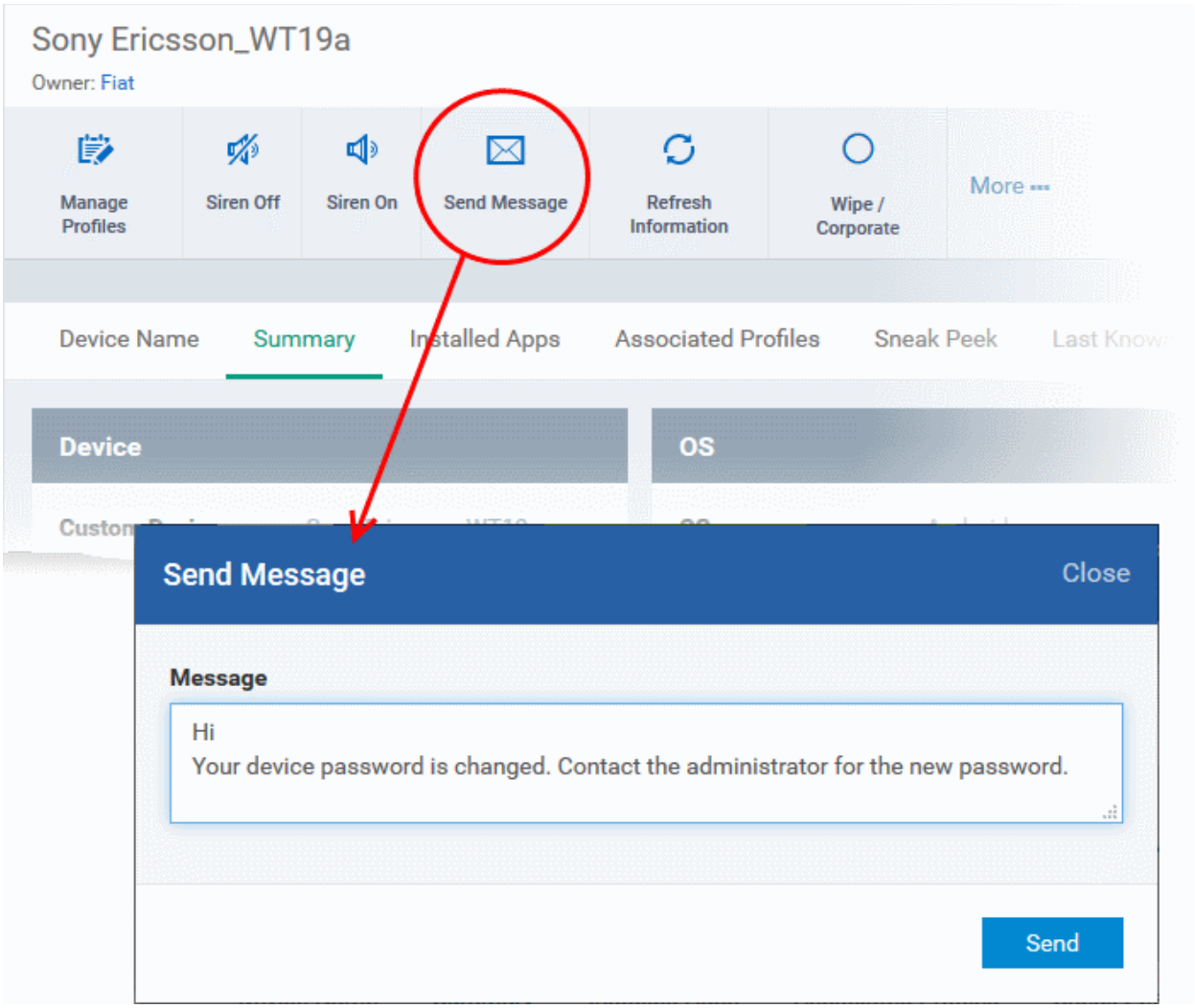
- Sending message to a single device
- Sending message to several devices at-once

To send a text message to a single device

- Click 'Devices' and choose 'Device List'
- Click on the name of the device to send the message.

The device details interface will open.

- Click 'Send Message' from the options at the top.



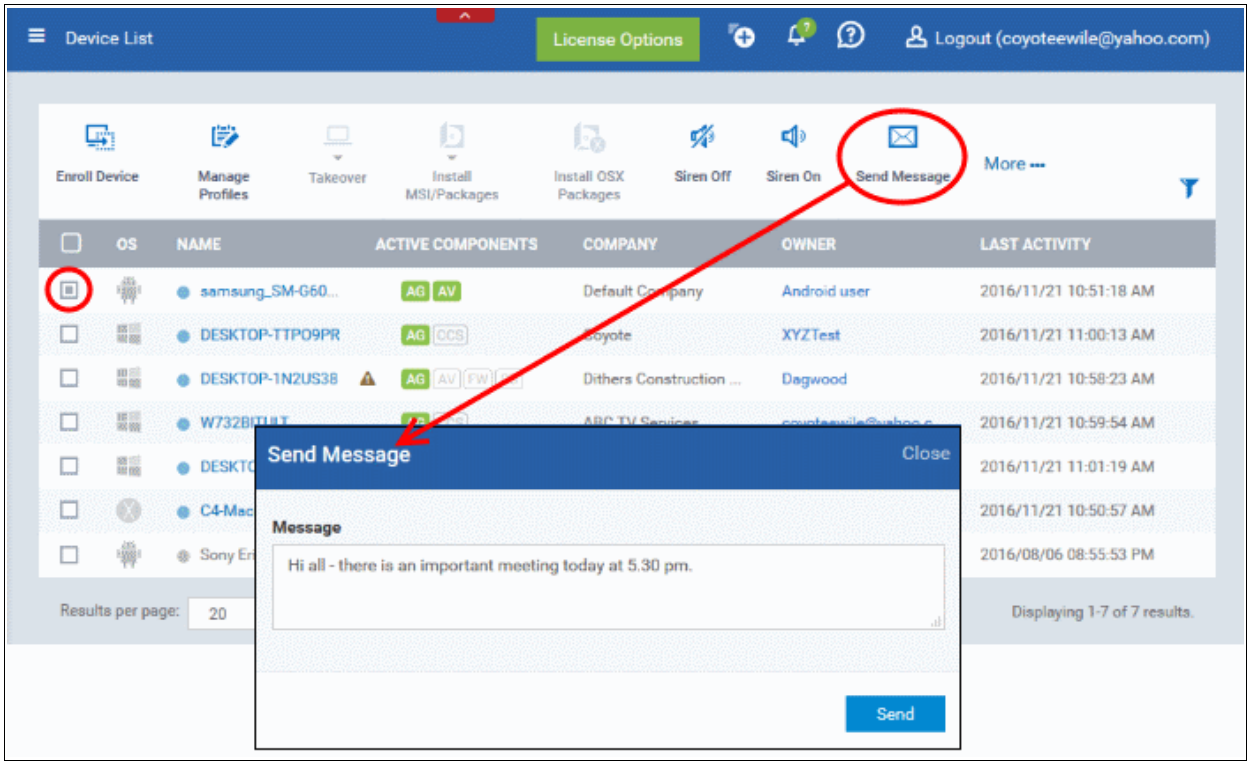
The 'Send Message' dialog will open.

- Enter the text message in the 'Message' field.
- Click on the 'Send' button.

The message will be sent to the device for the user's attention.

To send a text message to several devices at-once

- Click 'Devices' and choose 'Device List'
- Select the devices to which you wish to send messages
- Click 'Send Message' from the options at the top



The 'Send Message' dialog will open.

- Enter the text message in the 'Message' field.
- Click on the 'Send' button.

The message will be sent to the selected devices for the users' attention.

5.1.17. Restarting Selected Windows Devices

ITSM allows administrators to remotely restart Windows machines as required. Administrators can specify how long to delay the restart and add a warning message that will be displayed to users after the restart command has been sent. Administrators can also choose to allow end-users to postpone the restart.

Note: The reboot option is only available for Windows devices.

The following sections explain more about:

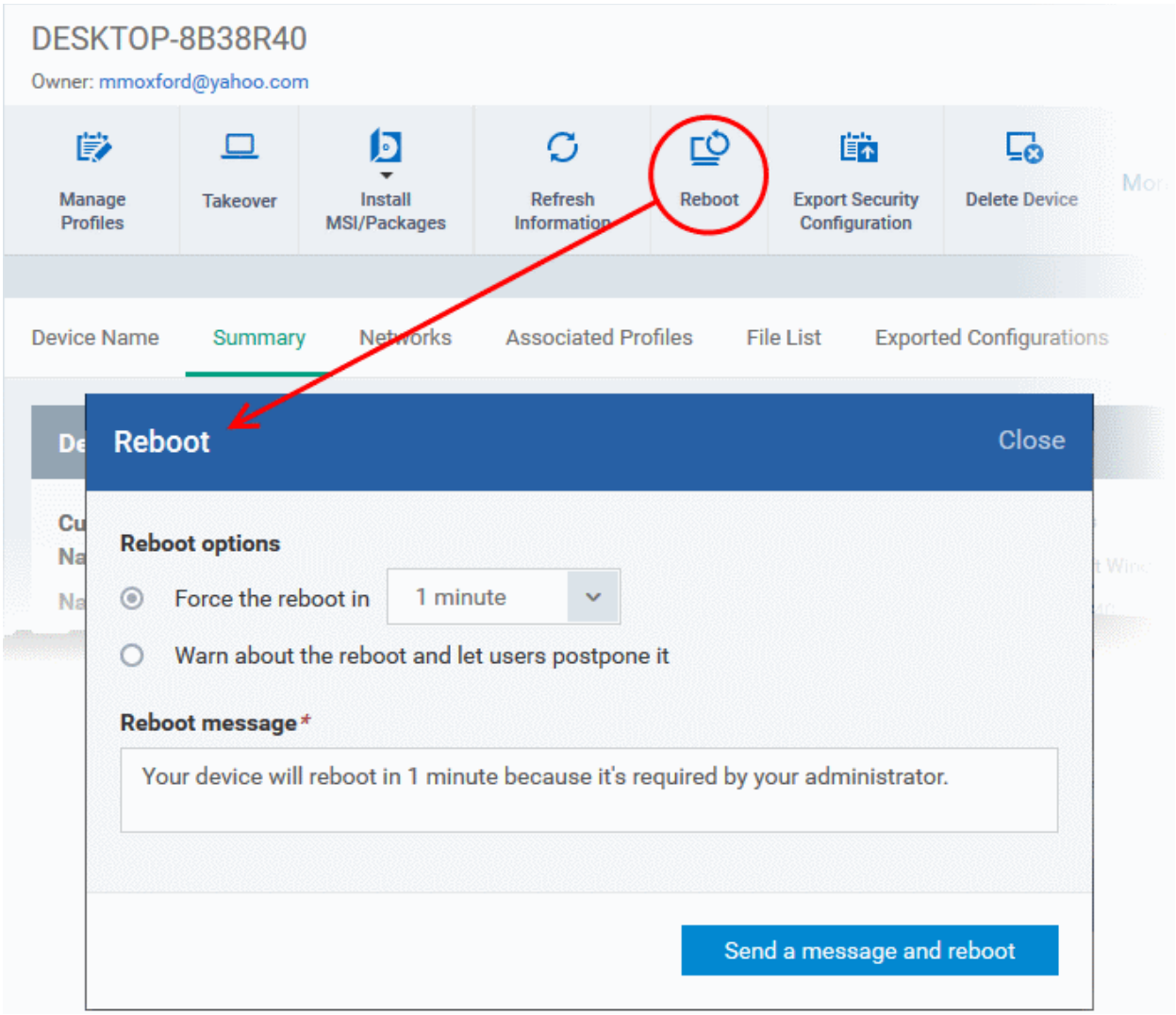
- Restarting a single device
- Restarting several devices at-once

To restart a single device

- Click 'Devices' and choose 'Device List'
- Click the name of the Windows device to be restarted

The device details interface will open.

- Click the 'Reboot' option at the top.

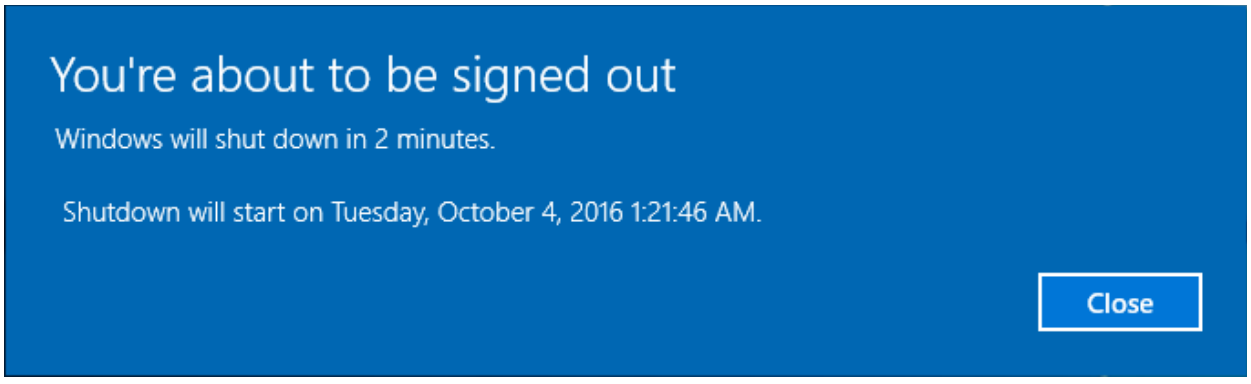


The 'Reboot' dialog will open.

To restart the end-point after a certain period of time

- Choose 'Force the reboot in' and select the delay period.
- Click 'Send a message and reboot'

The message will be displayed at the device as shown below:



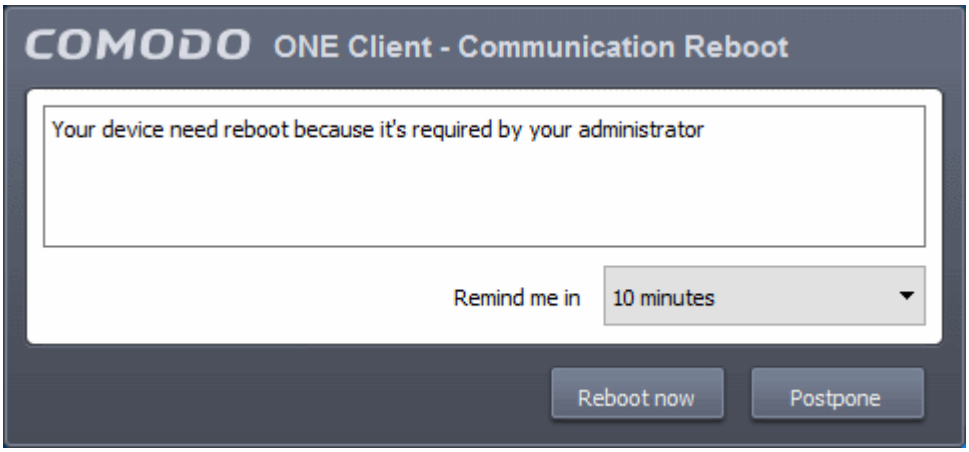
The device will be restarted automatically when the time period elapses.

To restart the end-point at user's convenience

- Choose 'Warn about the reboot and let users postpone it.

- Enter the message to be displayed to the user in the 'Reboot message' field.
- Click 'Send a message and reboot'

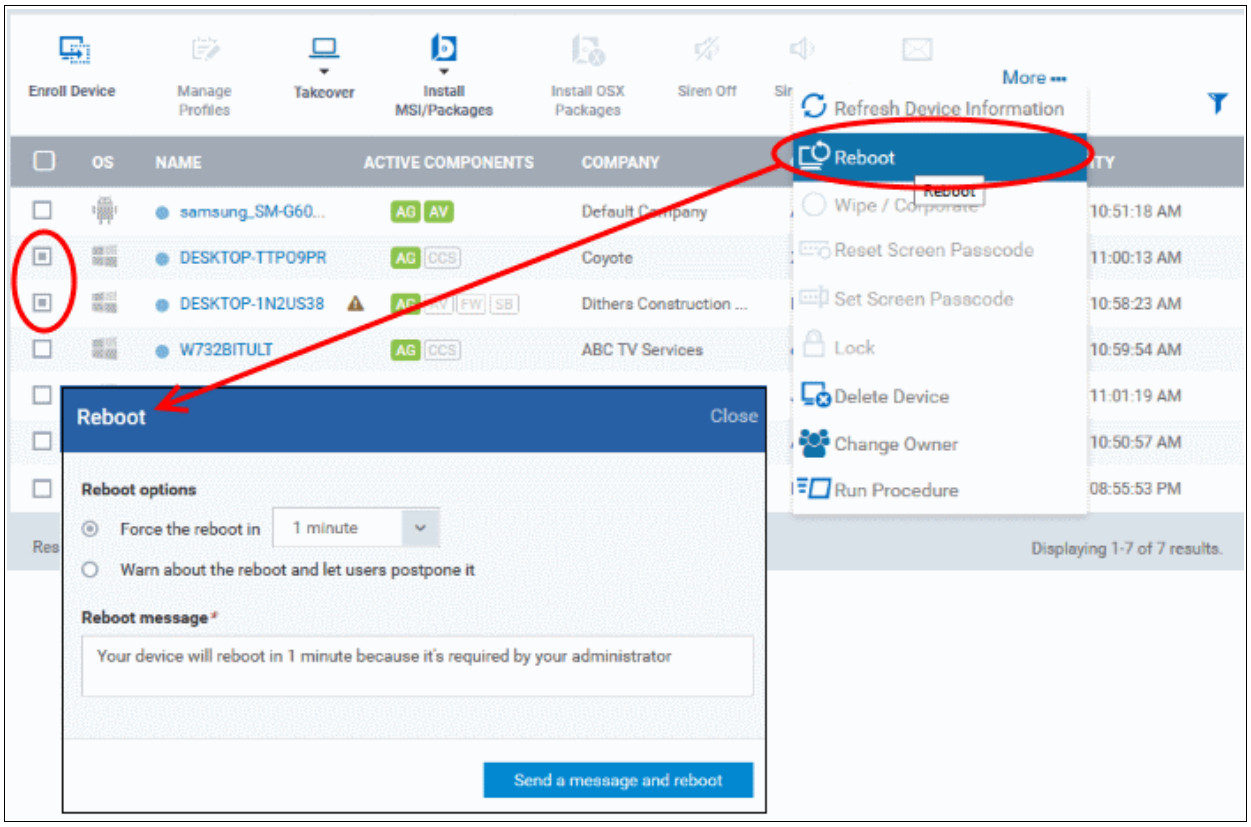
The message will be displayed at the device as shown below:



- The user can choose to restart the endpoint immediately by clicking 'Reboot now' or postpone the restart operation by selecting the period from the 'Remind me in' drop-down and clicking 'Postpone'.

To restart several devices at once

- Click 'Devices' and choose 'Device List'
- Select the devices to be restarted
- Click 'Reboot' from the options at the top or click 'More' and choose 'Reboot' from the options



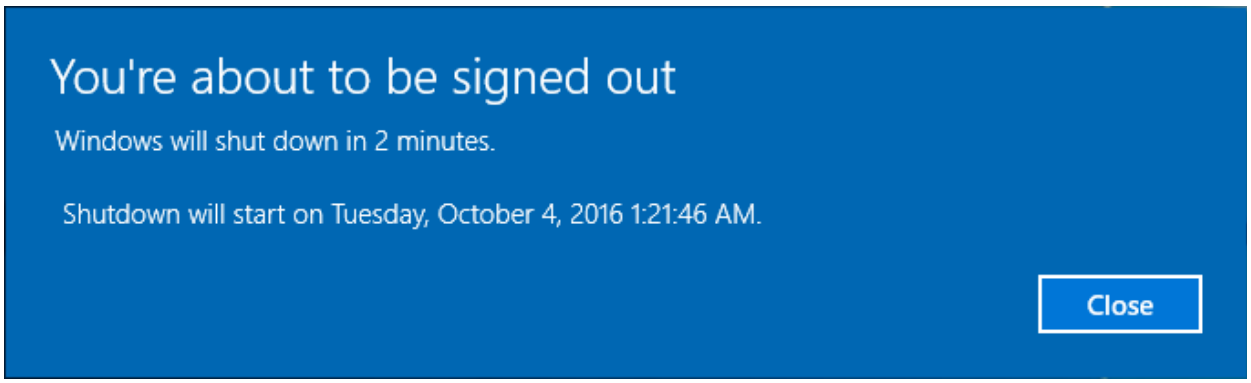
The 'Reboot' dialog will open.

To restart the end-points after a certain period of time

- Choose 'Force the reboot in' and select the delay period.

- Click 'Send a message and reboot'

The message will be displayed at the device as shown below:

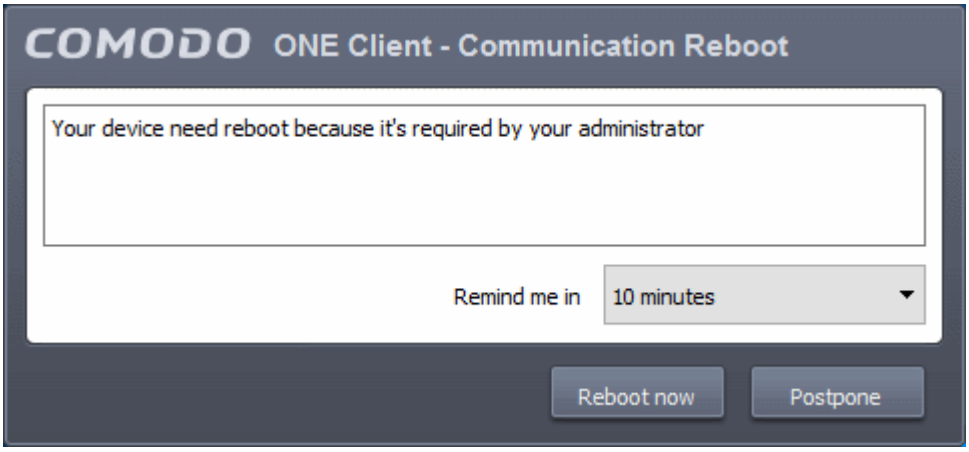


The device will be restarted automatically when the time period elapses.

To restart the end-point at user's convenience

- Choose 'Warn about the reboot and let users postpone it'.
- Enter the message to be displayed to the users in the 'Reboot message' field.
- Click 'Send a message and reboot'

The message will be displayed at the devices as shown below:



- Users can choose to restart their endpoints immediately by clicking 'Reboot now'. They can delay the restart by selecting a time-period from the 'Remind me in...' drop-down and clicking 'Postpone'.

5.1.18. Changing a Device's Owner

ITSM allows administrators to assign device ownership to another user.

The following sections explain more about:

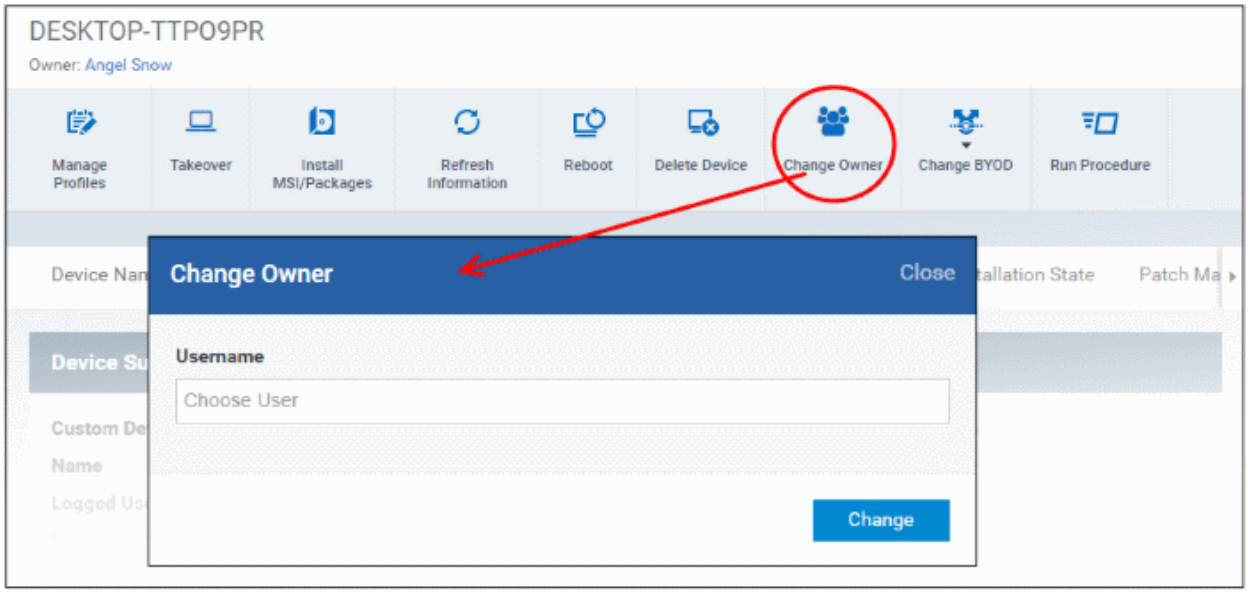
- Changing ownership of a single device
- Assigning multiple devices to single owner at-once

To change the device ownership of a single device

- Click 'Devices' and choose 'Device List'
- Click the name of the device whose ownership is to be changed

The device details interface will open.

- Click 'Change Owner' from the options at the top or click 'More...' and choose 'Change Owner' from the options



- Start typing the first few characters of the name of the new user to whom the device is to be assigned and choose the user from the options
- Click 'Change'

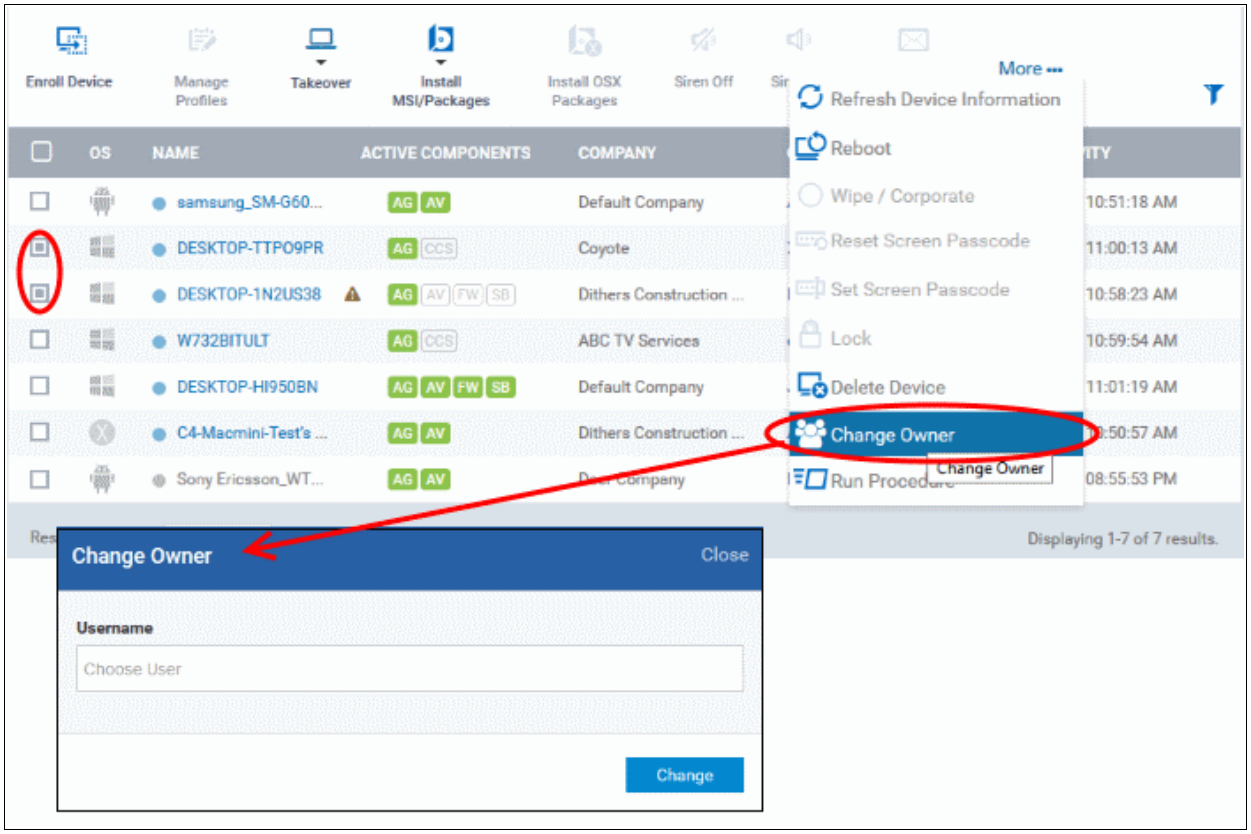
The ownership of the device will be changed to the new user. The configuration profiles in effect on the device, associated with the previous user and the user group to which the previous user is a member, will be removed and the profiles, pertaining to the new user and the user group to which the new user is a member, will be applied to the device.

To assign several devices to a user at-once

- Click 'Devices' and choose 'Device List'
- Select the devices to be associated with a new user

Tip: You can change devices pertaining to different users to be assigned to a single new user.

- Click 'Change Owner' from the options at the top or click 'More' and choose 'Change Owner' from the options



- Start typing the first few characters of the name of the new user to whom the device is to be assigned and choose the user from the options
- Click 'Change'

All selected devices will be assigned to the new user. The configuration profiles in effect on the device, associated with the previous users and the user groups to which the previous users are members, will be removed and the profiles, pertaining to the new user and the user group to which the new user is a member, will be applied to the device.

5.1.19. Changing BYOD status of a Device

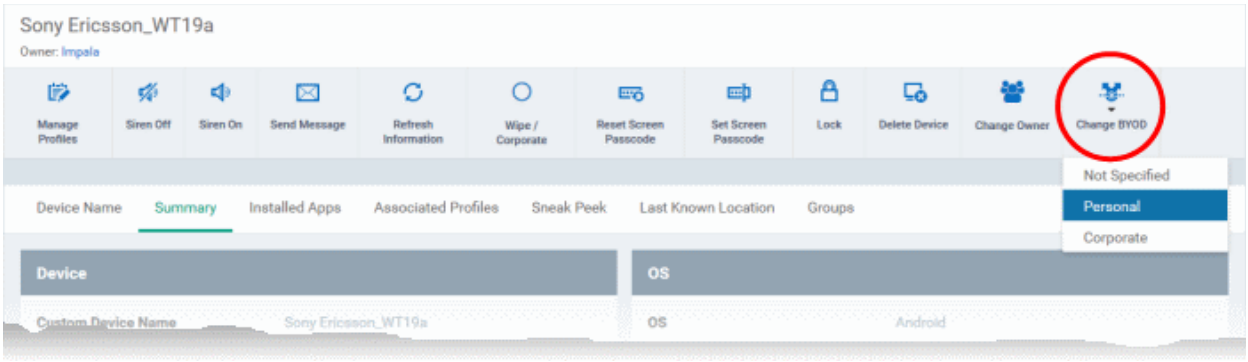
Depending on whether a device is owned by the user or is lent to the user by the company, administrators can set the Bring Your Own Device (BYOD) status of the device and can change it at anytime from the Device List interface. The device will be indicated as 'Personal' or 'Corporate' under the Summary tab of the 'Device Details' interface accordingly.

Note: By default, any new device enrolled to ITSM will have BYOD state as 'Not Specified'.

To set the BYOD state of a device

- Click 'Devices' and choose 'Device List'
- Click the name of the device whose BYOD state is to be set

The device details interface will open.



- Click 'Change BYOD' drop-down and choose the state from the options. The available options are:
  - Personal
  - Corporate

5.1.20. Applying Procedures for Windows Devices

Procedures are standalone instruction scripts and patches that can be executed on devices from the procedures interface. Procedures can also be executed via a profile and from the device list interface. Refer to the sections Directly Apply Procedures to Devices and Procedure Settings for details about the first two methods. This section explains how to run procedures from the device list interface.

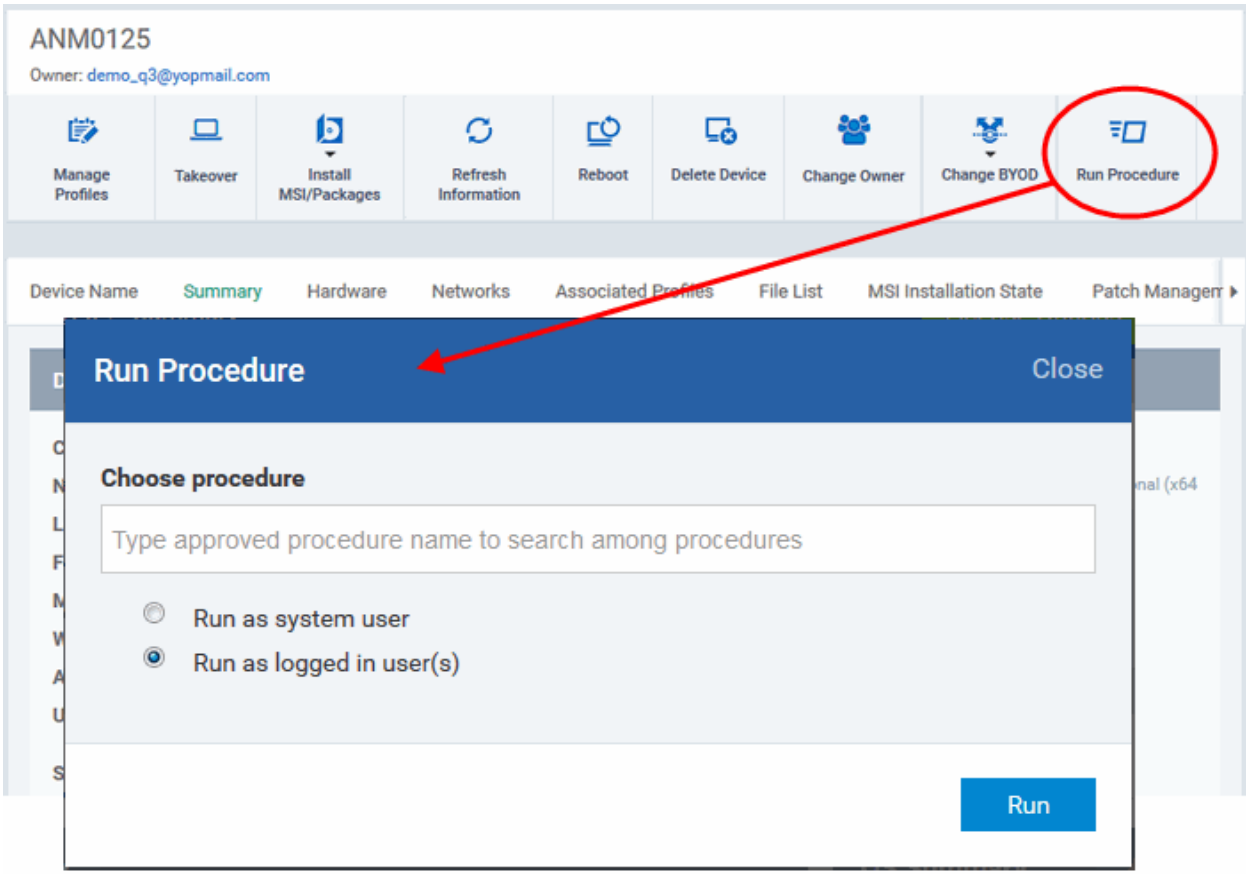
- Applying procedures on a single device
- Applying procedures on multiple devices at once

To run a procedure on a single device

- Click 'Devices' and choose 'Device List'
- Click the name of the device on which procedures should be applied

The device details interface will open.

- Click 'Run Procedure' from the options at the top or click 'More...' and choose 'Run Procedure' from the options



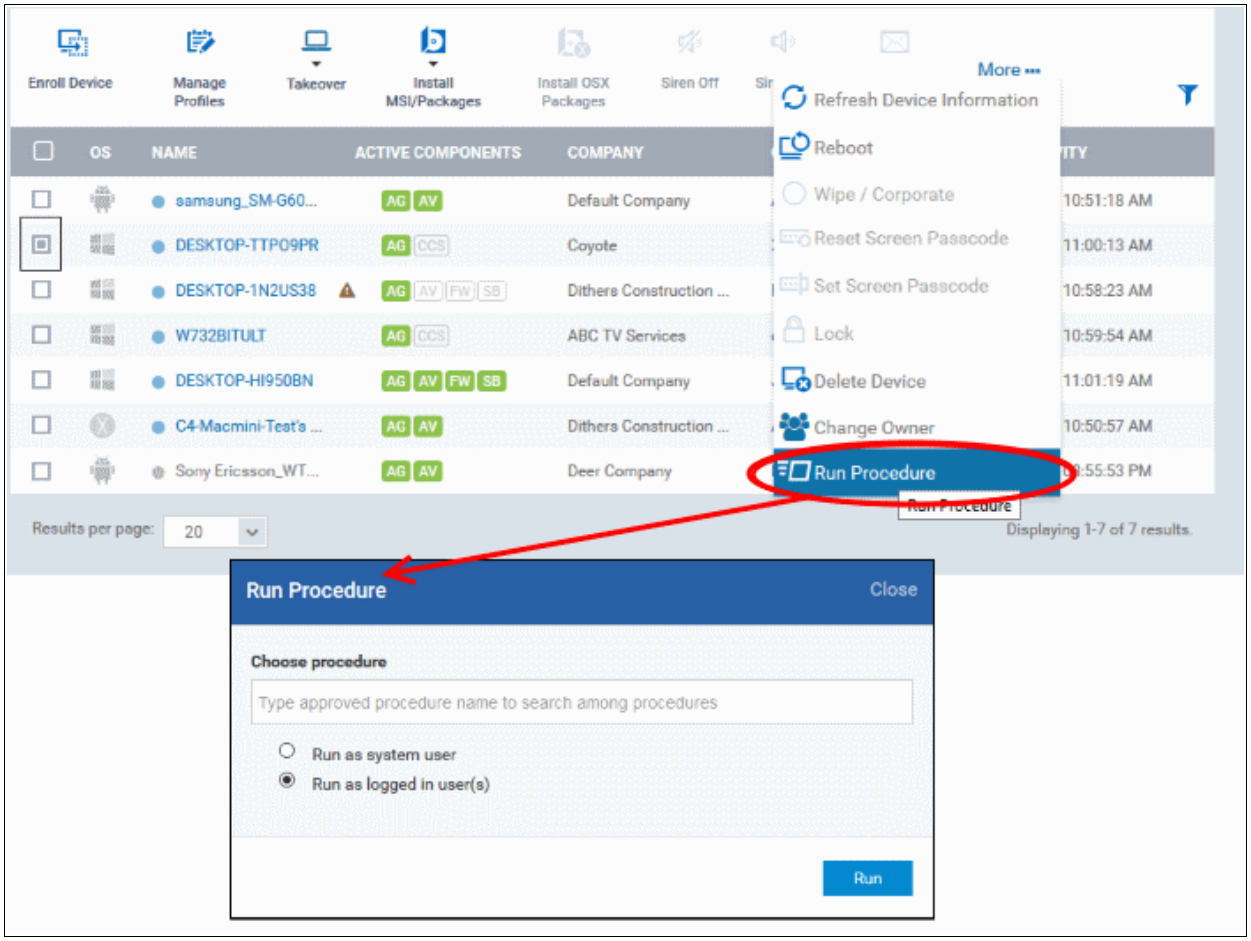
- Run as system user-defined
- Run as logged in user(s) (default)

- Start typing the first few characters of the name of the procedure that you want to apply and select it from the options. Only one procedure can be run at a time. Please note only approved procedures will be listed.
- Click 'Run'

The command will sent to the device and the selected procedure will be run on the device. If the procedure deployment fails, an alert will be generated if configured. The process will be logged and you can view the details in the Procedure Logs screen for script procedures and patch procedure logs will be available in the respective patch procedure itself.

To run procedures on multiple devices at once

- Click 'Devices' on the left and choose 'Device List'
- Select the check box beside the devices that you want to run a procedure
- Click 'Run Procedure' from the options at the top or click 'More...' and choose 'Run Procedure' from the options



The 'Run Procedure' dialog will be displayed.

- Start typing the first few characters of the name of the procedure that you want to apply and select it from the options. Only one procedure can be run at a time. Please note only approved procedures will be listed.
- Click Run.

The command will sent to the device and the selected procedure will be run on the device. If the procedure deployment fails, an alert will be generated if configured. The process will be logged and you can view the details in the Procedure Logs screen for script procedures and patch procedure logs will be available in the respective patch procedure itself.

5.2. Managing Device Groups

Comodo ITSM allows administrators to create logical device groups of Android, iOS, Mac OS and Windows devices in order to conveniently manage large numbers of devices. For example, devices can be grouped by company department and/or by device type. Administrators can, for example, create groups of devices called 'Sales Department', 'Accounts Department' , 'Android Tablets', 'Windows 10 Computers', ' iPads', 'Android Smart Phones', 'iPhones', 'Executive Laptops' or 'All Managed Mobile Devices'.

The ability to create device groups depends on your account type. See the table below for details:

Comodo One MSP Customers:	Comodo One Enterprise / ITSM Stand-alone Customers:
C1 MSP customers can create separate device groups for each Company/Organization enrolled in their Comodo One account.	C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.

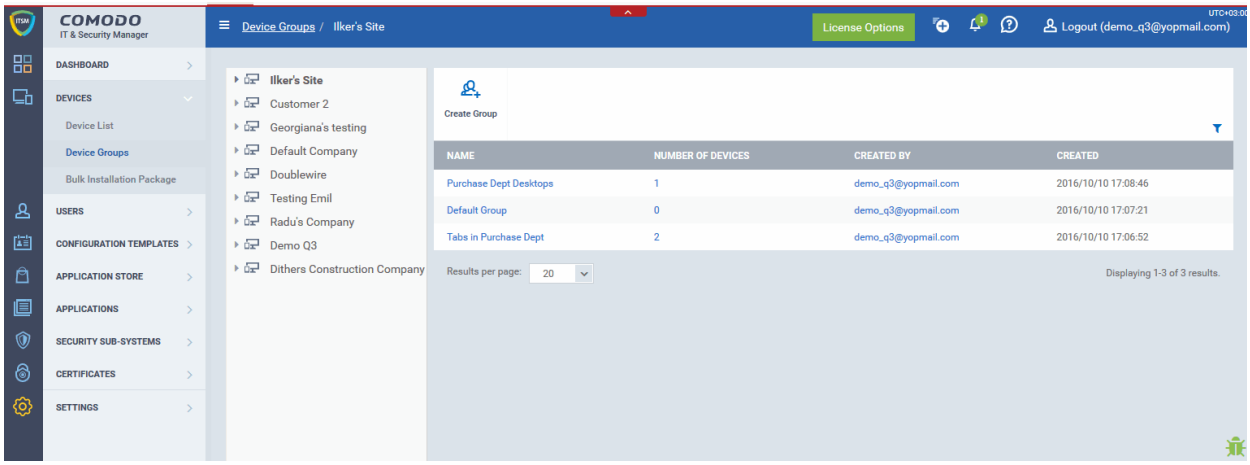
Dedicated configuration profiles containing specific user privileges can be created for any group. If a device is enrolled in multiple groups, then the group profiles of all groups are applied to the device. If the settings in one group profile clash with those of another, ITSM follows the most restrictive policy. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera.

For more details on creating and managing configuration profiles, see Configuration Templates.

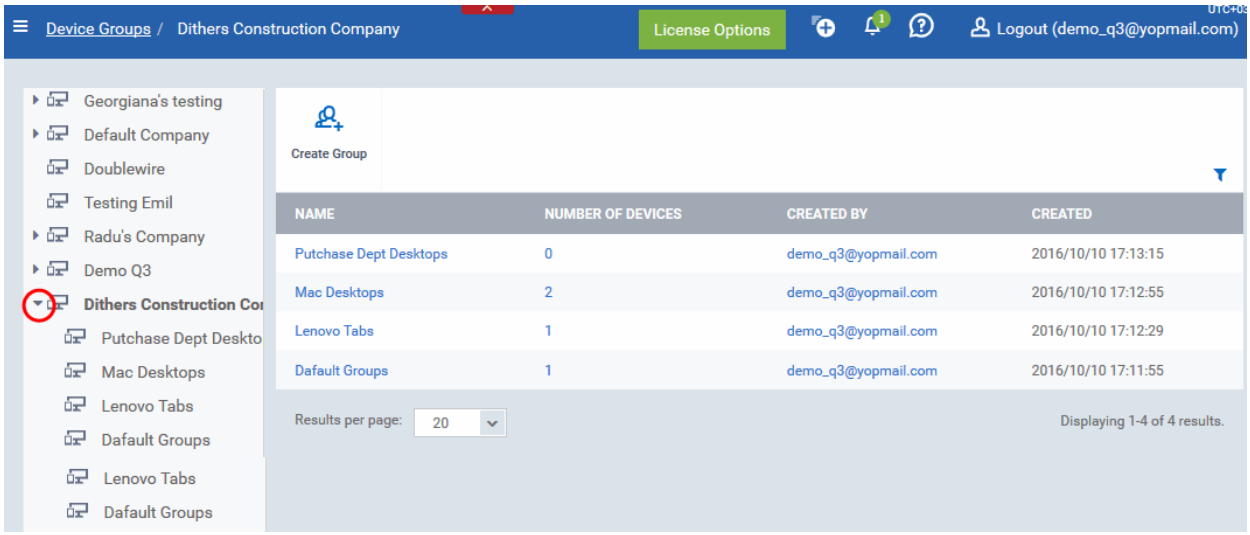
The 'Device Groups' interface displays all device groups and allows administrators to create new groups, import devices into groups and assign configuration profiles to groups.

- To open the 'Device Groups' interface, click the 'Devices' tab on the left and choose 'Device Groups' from the options.

C1 MSP customers should choose the company whose devices they wish to manage on the left:



The groups pertaining to the selected company are displayed on the right. You can also view the groups under a company/department by clicking the arrow beside the company name:

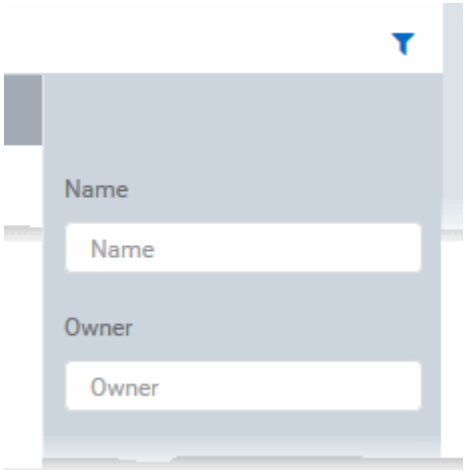


The group screen contains the following information:

Device Groups - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the device group by the administrator. Clicking the name of a group will open the 'Group Details' interface which lists the devices in the group. You can add or remove devices to/from the group and manage configuration profiles applied to the group. Refer to the section **Editing Device Groups** for more details.
Number of Devices	Shows the number of devices in the group. Clicking the number will open the group details interface.
Created By	Shows which administrator created the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section **Viewing the details of the User** for more details.
Created	Indicates the date and time at which the group was created.

Sorting, Search and Filter Options

- Clicking any of the column headers sorts the items in alphabetical or numerical order
- Clicking the funnel button on the right opens the filter options.



- You can filter items by group name or by admin that created the group. Type the group or admin name in the respective box and click 'Apply'.

You can use any combination of filters at-a-time to search for specific device groups.

- To display all items again, delete the search string and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. Use the drop-down underneath the results to increase results per page up to 200.

Refer to the following sections for more details about:

- Creating Device Groups
- Editing a Device Group
- Assigning Configuration Profiles to a Device Group
- Removing a Device Group

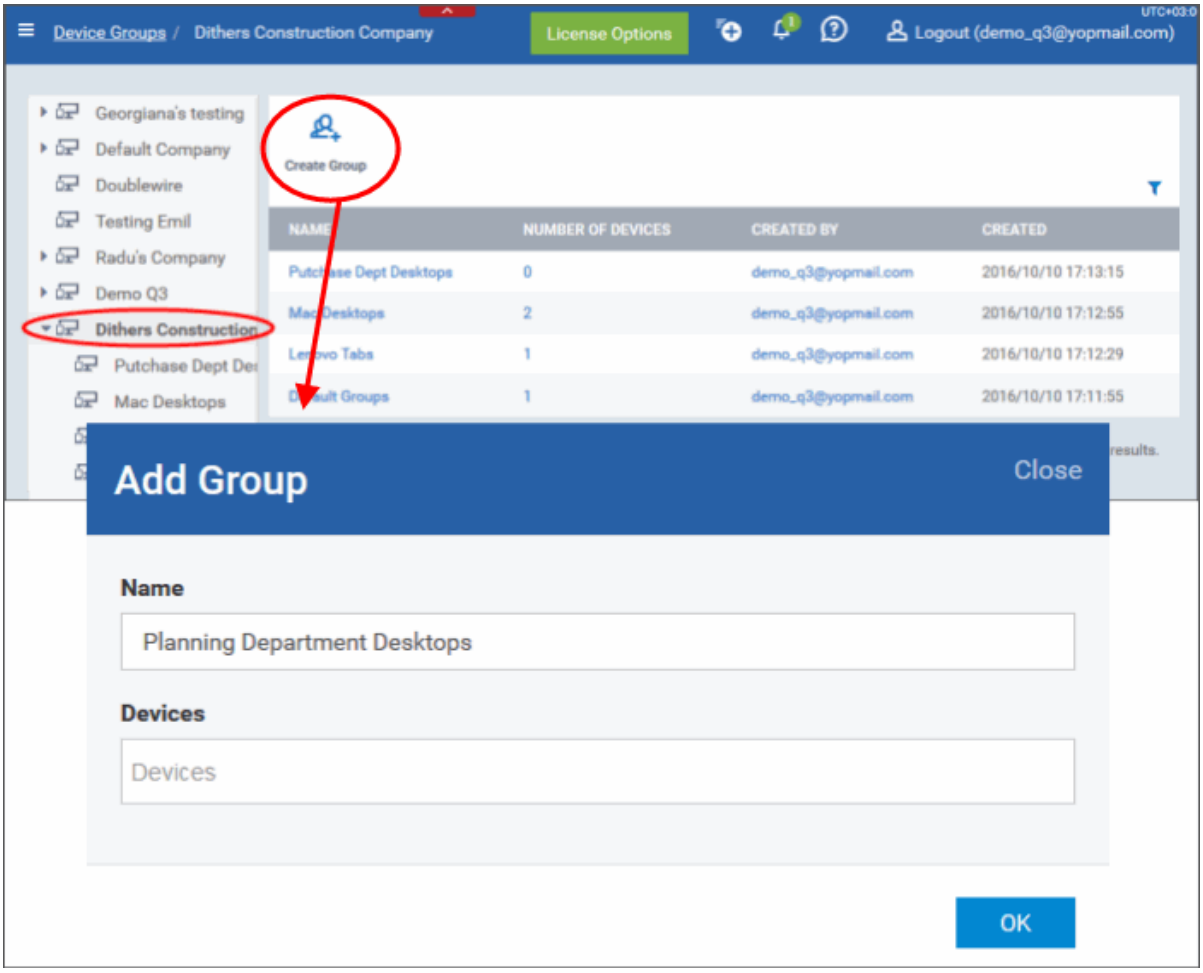
5.2.1. Creating Device Groups

Placing devices into a group allows administrators to push configuration profiles to multiple devices simultaneously. OS-specific profiles will be automatically applied to the relevant devices.

To create a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- C1 MSP customers should choose the company/department under which to create the group from the left
- Click 'Create Group' from the top left

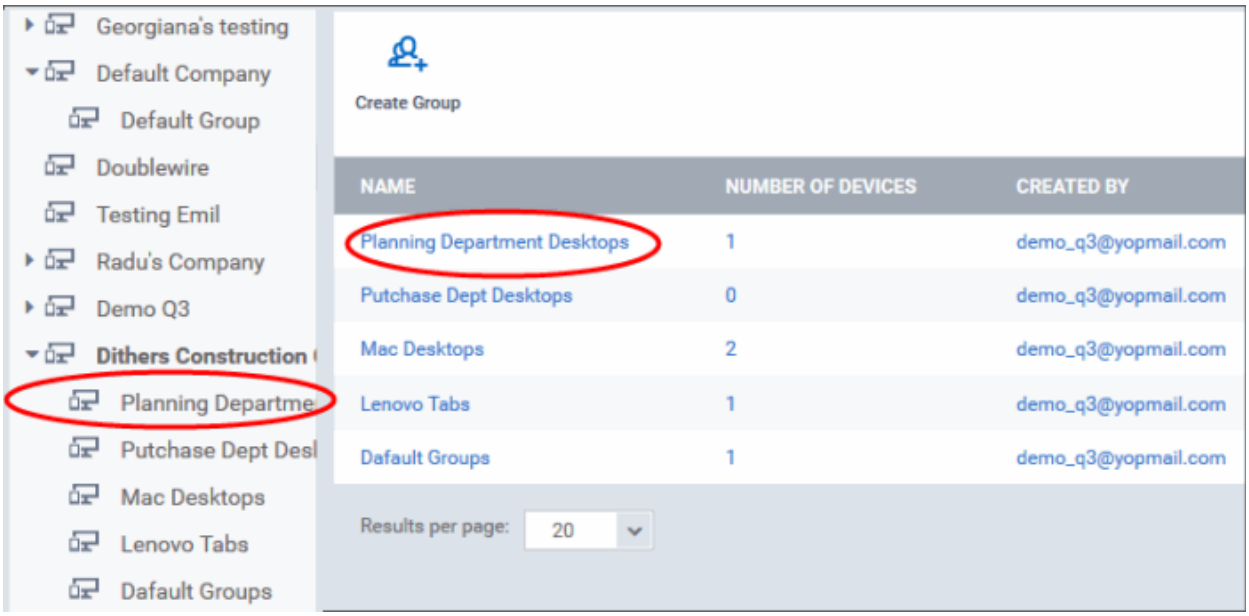
The 'Add Group' interface will open.



'Add Group' dialog - Table of Parameters	
Form Element	**Description**
Name	Enter a descriptive name for the group.
Devices	Allows you to add devices to the group. To add a device, start typing the first few letters of the device name and select the device from the options. Repeat the process for adding more number of devices. Note: You can add devices at a later stage too.

- Fill the details and click 'Save'.

The new group will be created and the device group details screen will be displayed with the list of devices in the group allowing you to add or remove devices and to manage profiles applied to the devices in the group. Refer to the section Editing a Device Group for more details.



- Repeat the process to add more groups.

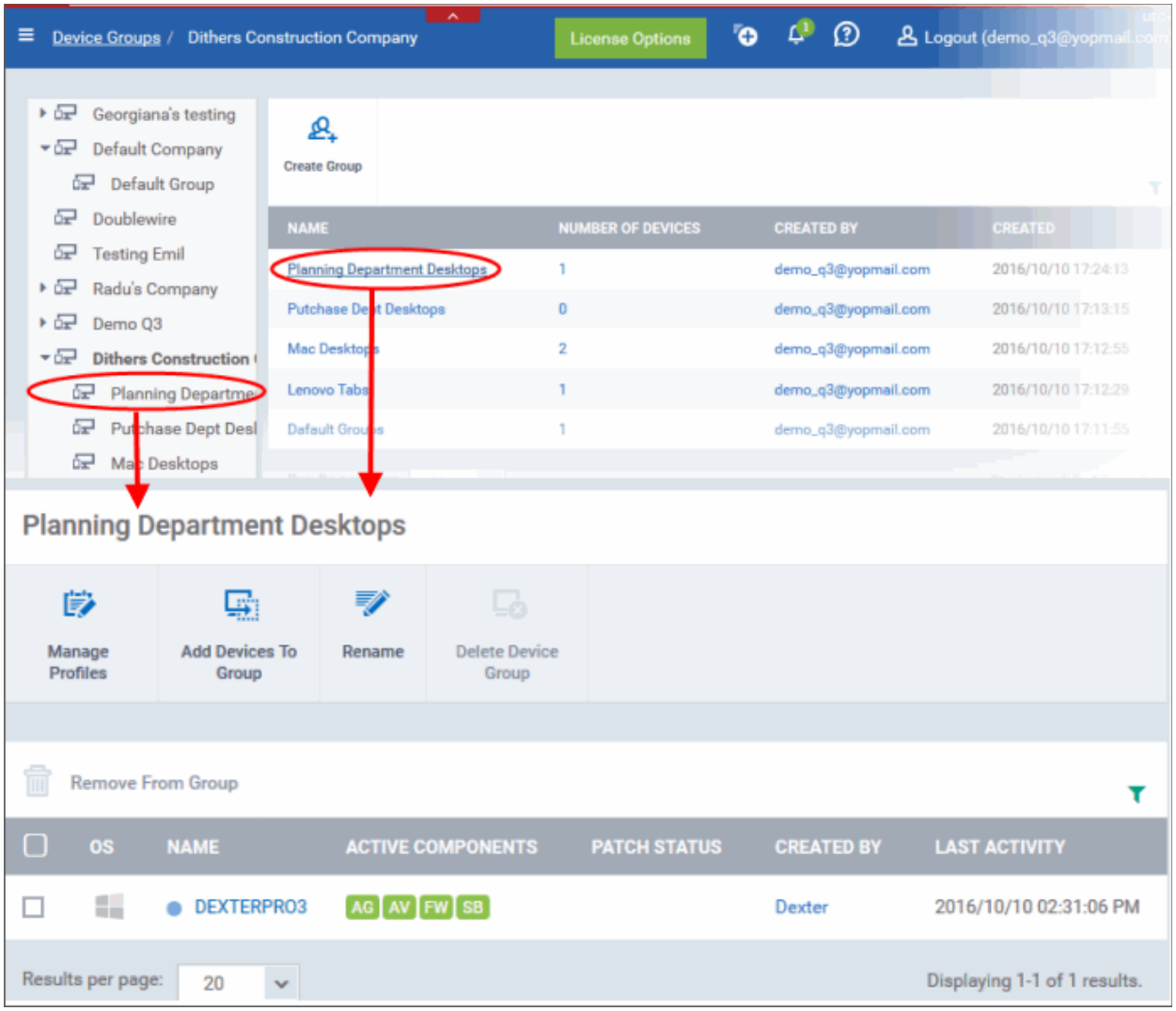
The new groups will be listed for the selected company/department. The added groups will also be listed in the hierarchical structure on the left for the company/department. Appropriate configuration profiles can now be applied to each new group. Refer to Assigning Configuration Profiles to a Device Group for more details.

5.2.2. Editing a Device Group

The device group details interface allows admins to view group devices, add or remove devices, rename the group and manage policies applied to each device.

To view and edit device a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- C1 MSP customers should choose the company/department whose group they wish to edit from the left
- Click the name of the group to be edited, either from the hierarchical structure at the left or from the list on the right. The group details interface for the selected group will open. C1 Enterprise / ITSM stand-alone customers simply click on the device group name.



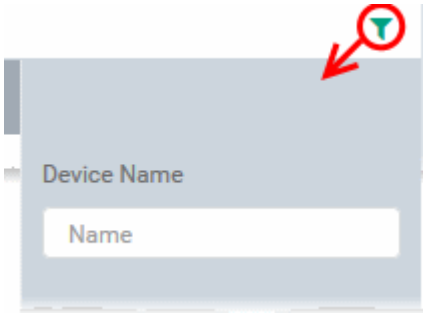
The list of devices included in the group will be displayed, with their details.

Device Group Details - Column Descriptions	
Column Heading	**Description**
OS	Indicates the Operating System of the device.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Grey text color indicates the device is offline for the past 24 hours. Clicking the device name will open the granular device details interface. Refer to the sections **Managing Windows Devices**, **Managing Mac OS Devices** and **Managing Android / iOS Devices** for more details.
Active Components	Indicates which components are installed on the device (Agent only, Antivirus, Firewall, Containment) • Android devices - The agent will automatically install the AV (antivirus) component. • iOS devices - Only the agent (ITSM client) will be installed • Windows endpoints - Available components are - Agent, AV, FW (firewall) and Containment. • Mac OS endpoints - Available components are - Agent and AV

Created By	Indicates the device user. Clicking the user name will open the 'View User' interface. Refer to Viewing the User Information for more details.
Last Activity	Indicates the date and time at which the device last communicated with the ITSM agent.

Sorting, Search and Filter Options

- Clicking on any of the 'OS', 'Name', 'Company', 'Owner' and 'Last Activity' column header sorts the items based on alphabetical or ascending/descending order of entries in that column.
- Clicking the funnel button at the right end opens the filter options that allows to search for a particular device.



- To filter the items or search for a device based on its name, enter the search criteria in part or full in the text box and click 'Apply'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

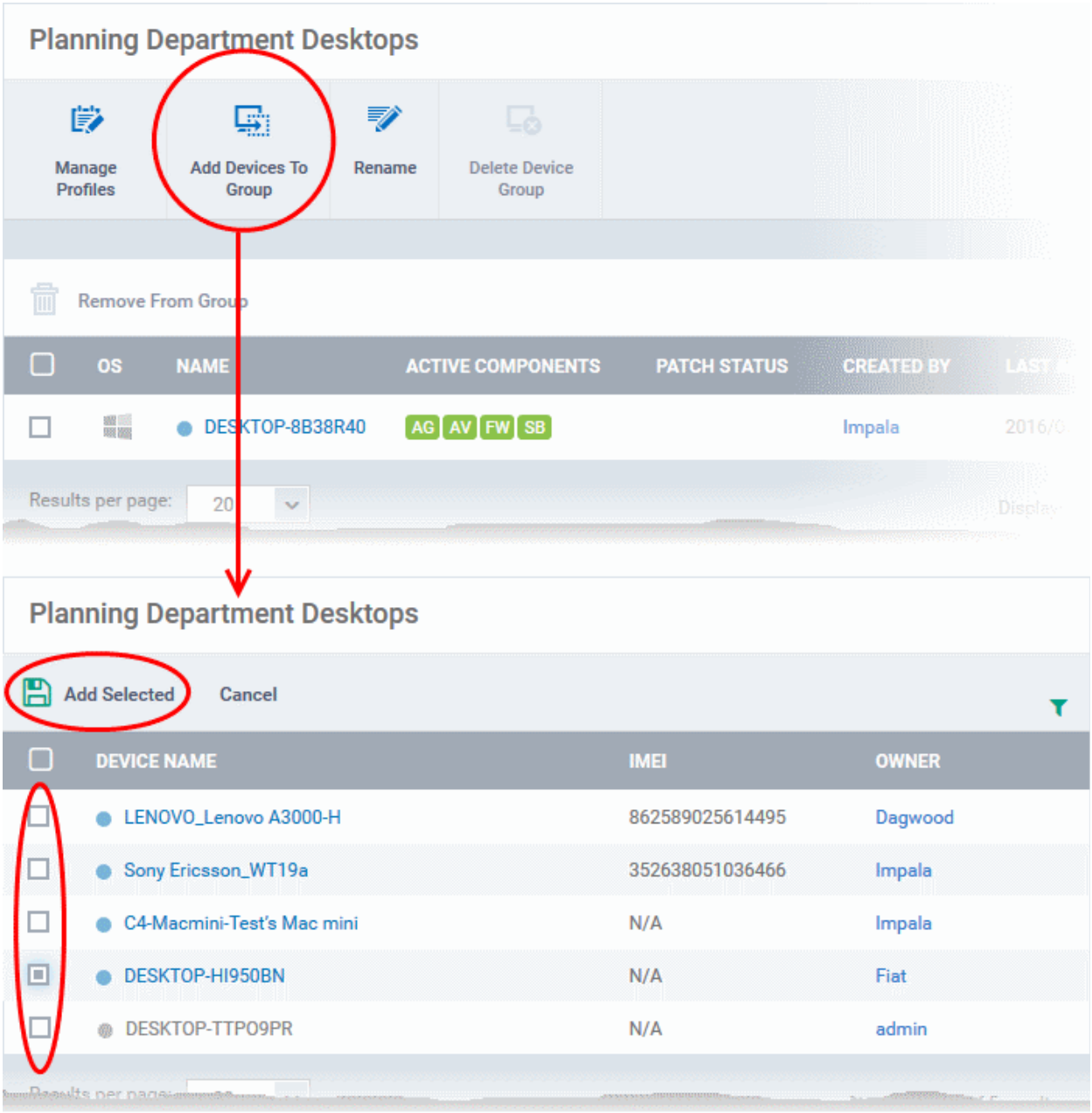
The device group details interface allows you to:.

- Add new devices to the group
- Remove devices from the group
- Rename the group
- Assign Configuration profiles to the device group
- Remove the group

To add new devices to the group

- Click 'Add Devices to Group' at the top.

A list of all devices enrolled to ITSM, excluding those in the group will be displayed.



- Select the devices to be added to the group and click 'Add Selected'.

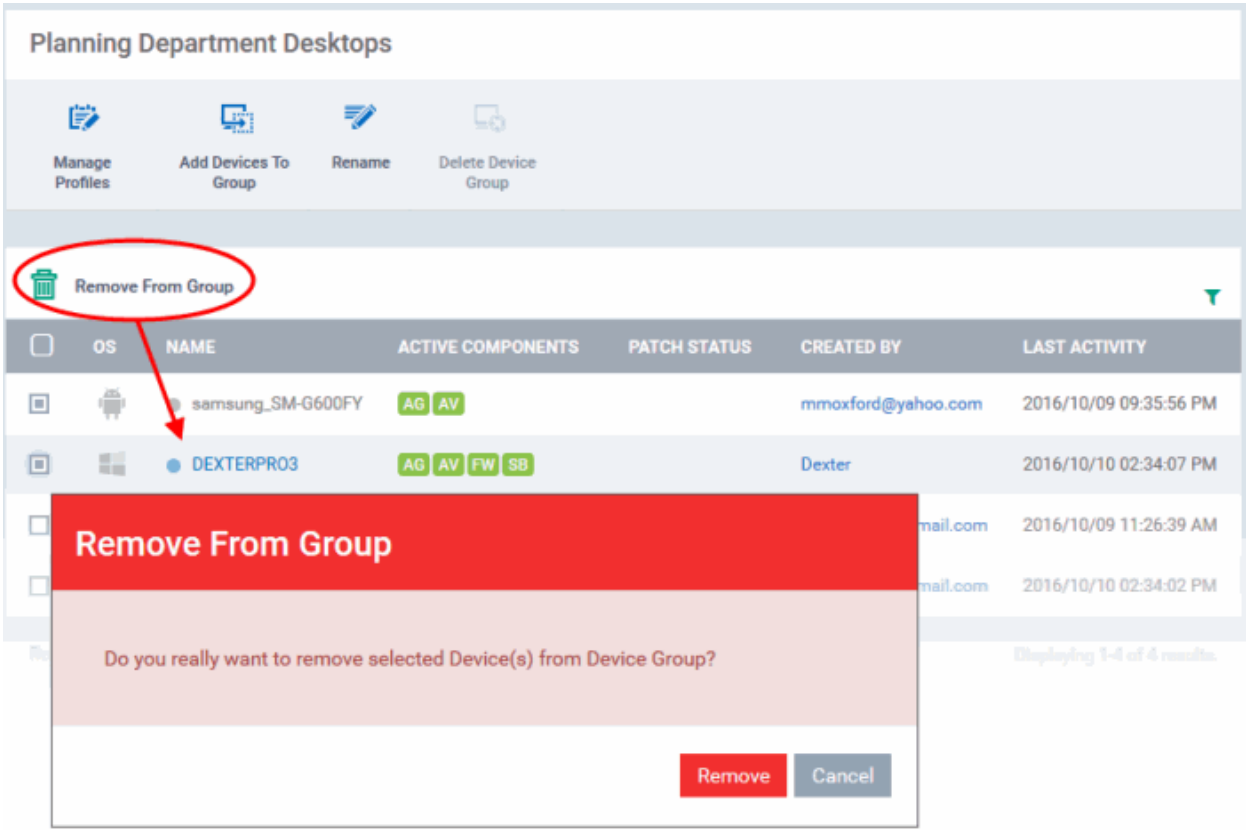
Tip: You can filter or search for specific devices using the filter options that appear on clicking the funnel icon at the top right.

Once the device(s) are added to the group, the configuration profiles, associated with the group, will be applied to the device, in addition to the profiles, which are already in effect on the device.

Tip: You can add a device to a group from the 'Device Details' interface too. For more details, refer to the section Viewing and Managing Device Group Membership.

To remove devices from the groups

- Choose the devices to be removed from the device group details interface
- Click 'Remove from Group'



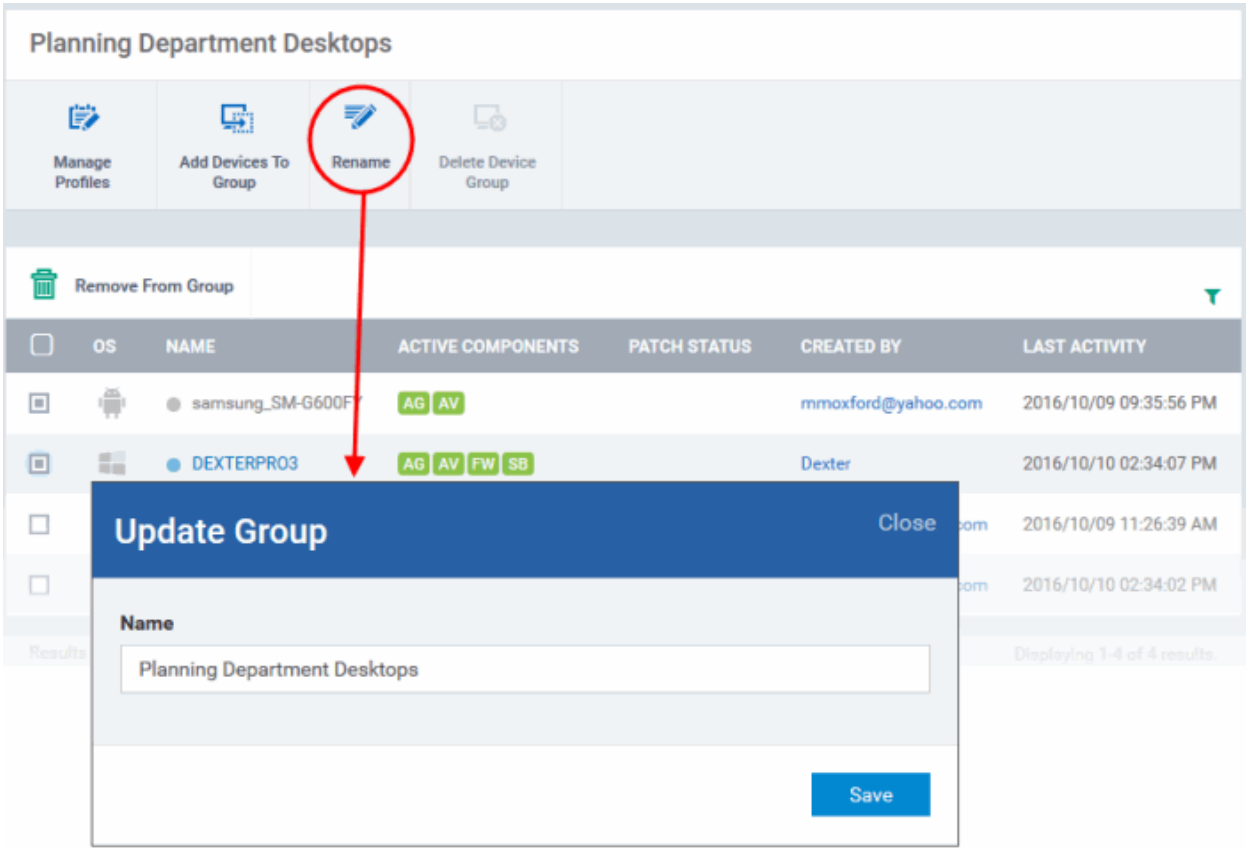
- Click 'Remove' in the confirmation dialog.

If a device is removed from a group, the profiles in effect on the device because of association with the group, will also be removed.

Tip: You can remove the membership of a device to a group, from the 'Device Details' interface too. For more details, refer to the section Viewing and Managing Device Group Membership.

To rename a group

- Click on the 'Rename' button at the top



The 'Update Group' dialog will open

- Enter the new name for the group in the 'Name' text box and click 'Save'.

The group will be updated with the new name.

The group details interface also allows the administrator to apply configuration profiles to devices associated with all the devices in a group at-once. Refer to the next section **Assigning Configuration Profiles to a User Group** for more details.

5.2.3. Assigning Configuration Profiles to a Device Group

Administrators can view configuration profiles currently assigned to the device group, add new profiles or remove existing profiles from the device group details interface.

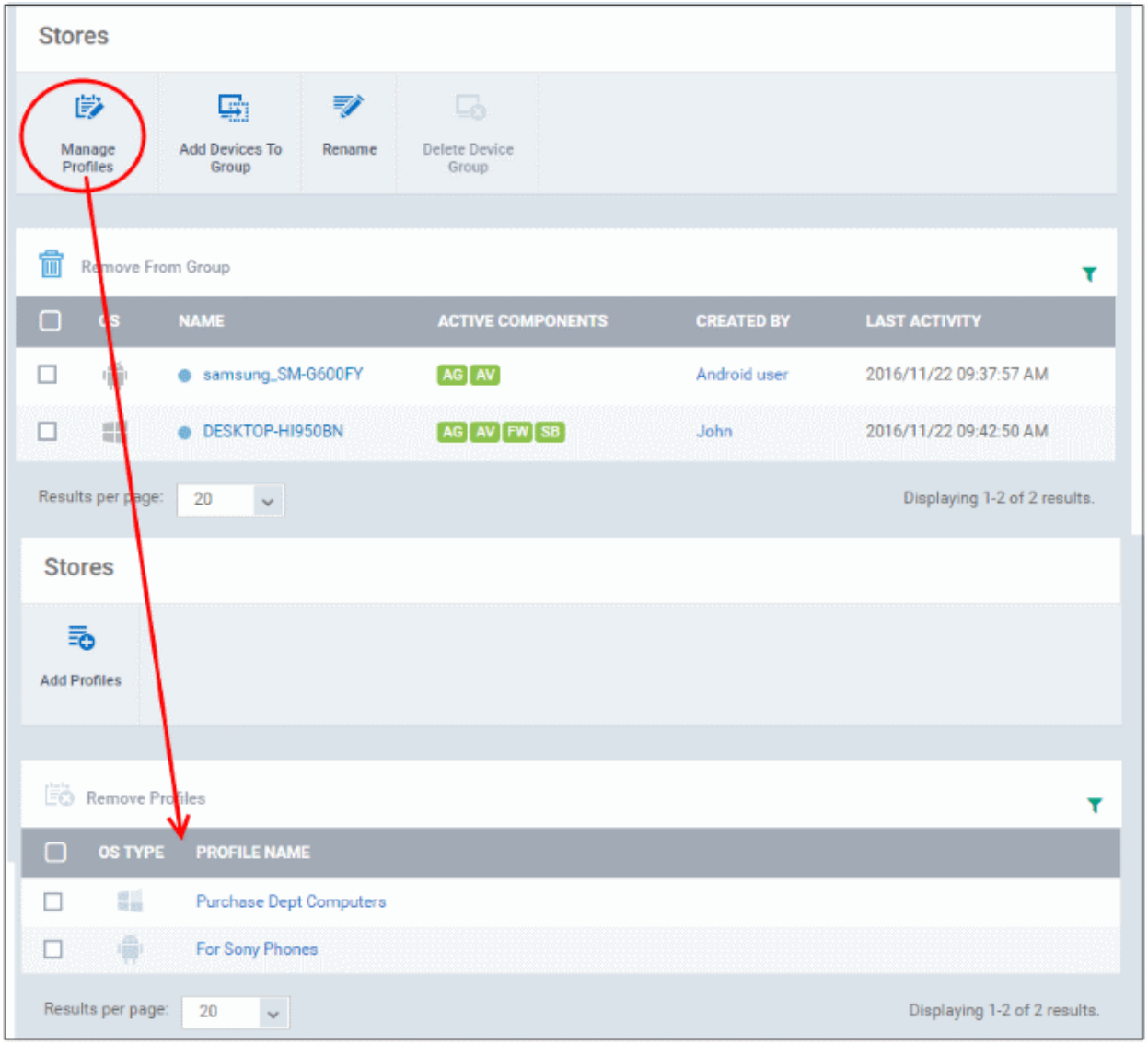
For more details on profiles, refer to the chapter **Configuration Profiles**.

To view and manage the profiles applied to a group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- C1 MSP customers should choose the company/department whose group they wish to edit from the left
- Click the name of the group to be edited, either from the hierarchical structure at the left or from the list on the right. C1 Enterprise / ITSM stand-alone customers simply click on the device group name.

The 'Group Details' interface for the selected group will open.

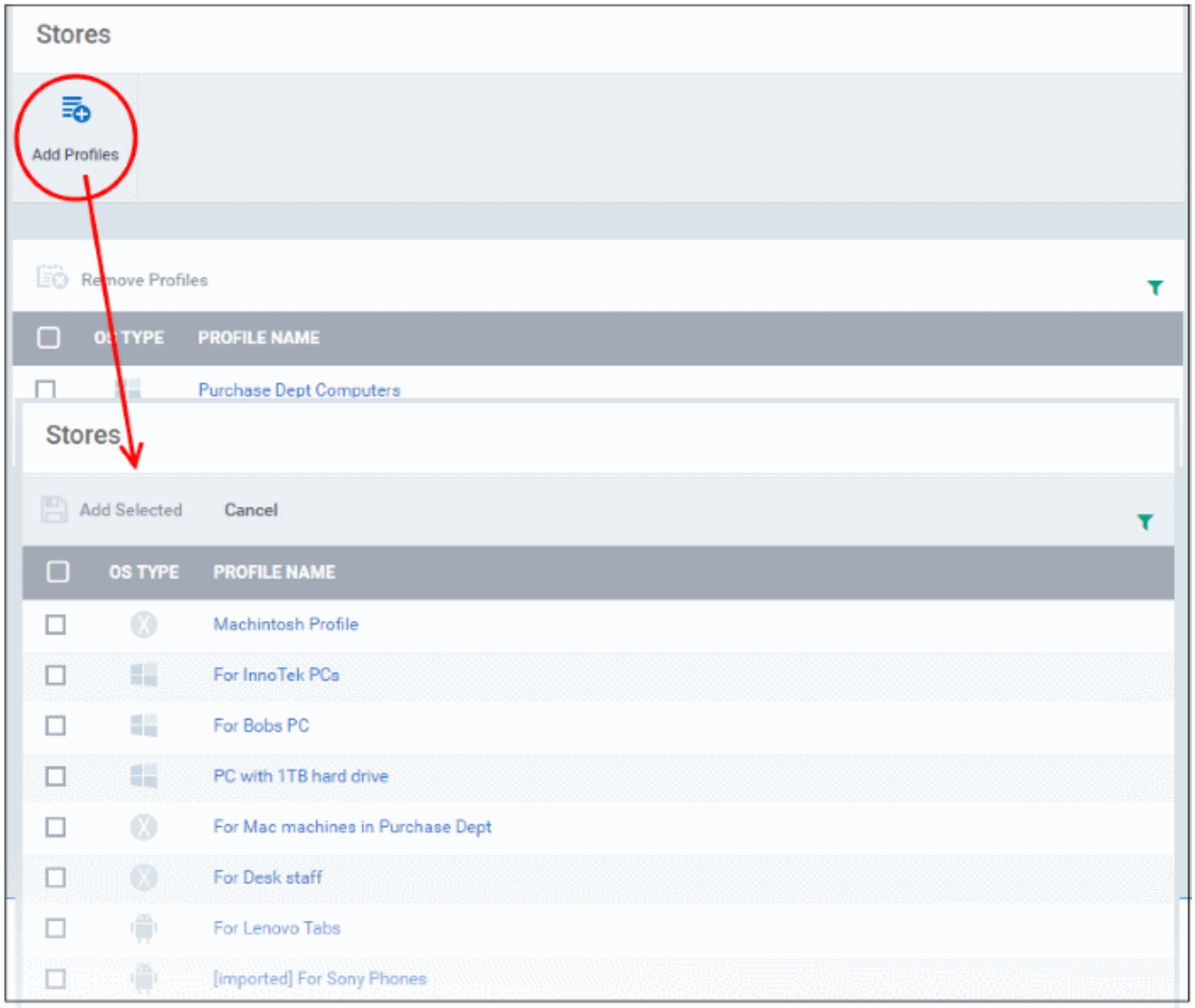
- Click the 'Manage Profiles' from the options at the top.



The list of profiles in effect on the device group will be displayed.

To add a new profile

- Click 'Add Profiles' from the top.



A list of all configuration profiles, available in ITSM, excluding those already applied to the group will be displayed.

- Select the profiles to be applied to the devices in the group and click 'Add Selected'.

Tip: You can filter the list or search for a specific profile by using the filter options that appear on clicking the funnel icon at the top right.

The profile will be associated with the group and applied to all the member devices in the group appropriate to the OS type of each device.

To remove a profile from a group

- Select the profile(s) to be removed, from the 'Manage Profiles' interface and click 'Remove Profiles'

The profile(s) will be removed from member devices of the group, where applied, according to their operating system(s).

Note: Disassociating a profile from a device group will remove the profile from devices only if it is applied because the device is a member of that group. If the same profile is applied to a member device through some other source, (like the profile is applied to the user of the device or a group to which the user belongs), then the profile will not be removed.

5.2.4. Removing a Device Group

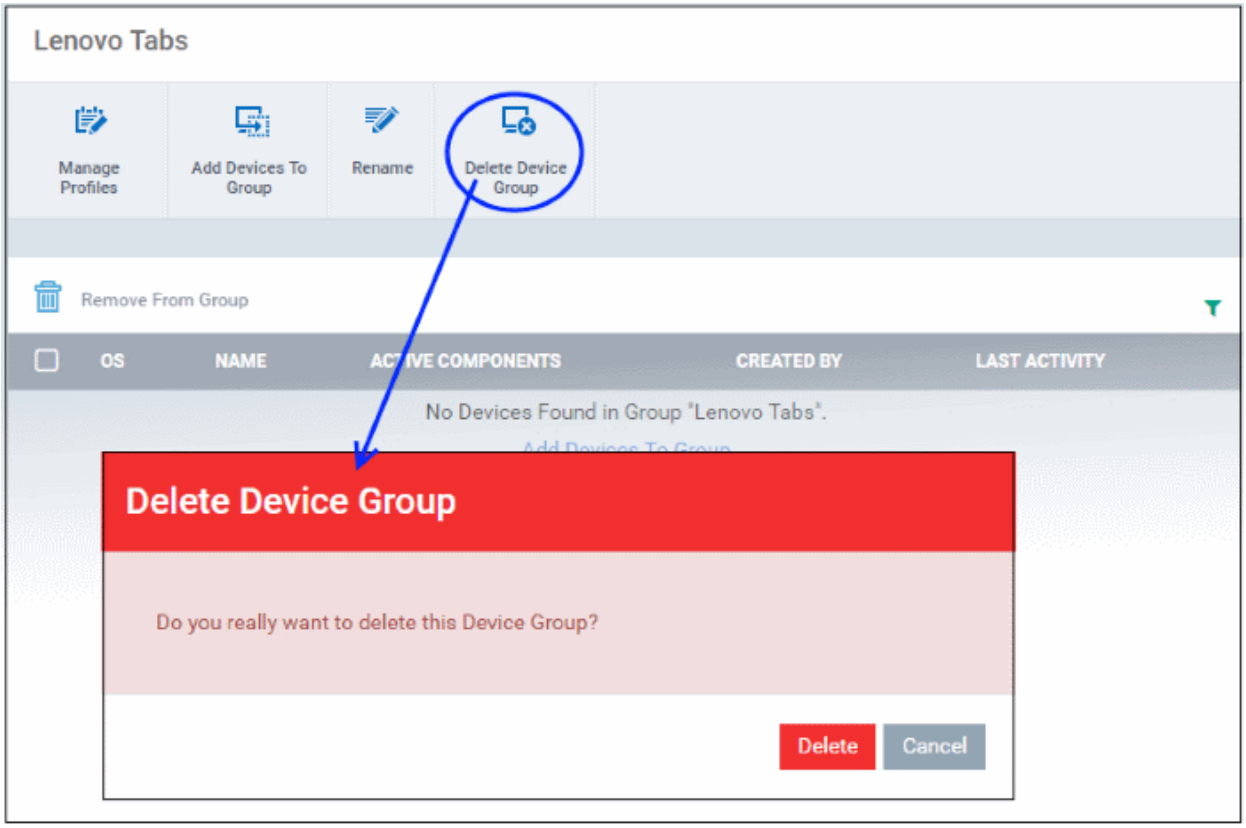
Administrators can quickly remove unwanted device group(s) from ITSM. Please note you cannot delete a device group unless all member devices are removed first.

To remove a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- C1 MSP customers should choose the company/department whose device group is to be removed
- Click the name of the group to be removed, either from the hierarchical structure at the left or from the list on the right. C1 Enterprise / ITSM stand-alone customers simply click on the device group name.

The 'Group Details' interface for the selected group will open.

- Ensure that there are no devices included in the group. Refer to the section **explaining removal of devices from the group** in the section **Editing a Device Group** for more details.
- Click 'Delete Device Group' at the top.



- Click 'Delete' in the confirmation dialog.

The device group will be removed from ITSM.

5.3. Bulk Enrollment of Devices

ITSM allows bulk enrollment of Android, iOS, Windows and Mac OS devices in the following ways.

Windows and Mas OS devices:

- Admins can download the C1 Communication agent installer and create a group policy object (GPO) on an AD server to install the package on endpoints which have been added to the AD domain.
- Alternatively, devices can be enrolled by using Comodo Auto Discovery and Deployment Tool (ADDT), or by manual installing the agent on endpoints.

Once the agent is installed, it communicates with your ITSM portal and enrolls the device automatically. Refer to the following sections for more details:

- Enroll Windows and Mac OS Devices by Installing the ITSM Agent Package
  - Enroll Windows Devices Via AD Group Policy
  - Enroll Windows and Mac OS Devices by Offline Installation of Agent
  - Enroll Windows Devices using Comodo Auto Discovery and Deployment Tool

Android and iOS Devices:

- Bulk enrollment of iOS and Android devices is possible for devices belonging to users that were imported to ITSM via Active Directory integration. Help to import users from AD is available in Importing User Groups from LDAP.
- After importing the users, Android devices can be enrolled by installing the agent. iOS devices can be enrolled by deploying a configuration profile.

For help to bulk enroll iOS and Android devices, see Enroll Android and iOS Devices of AD Users.

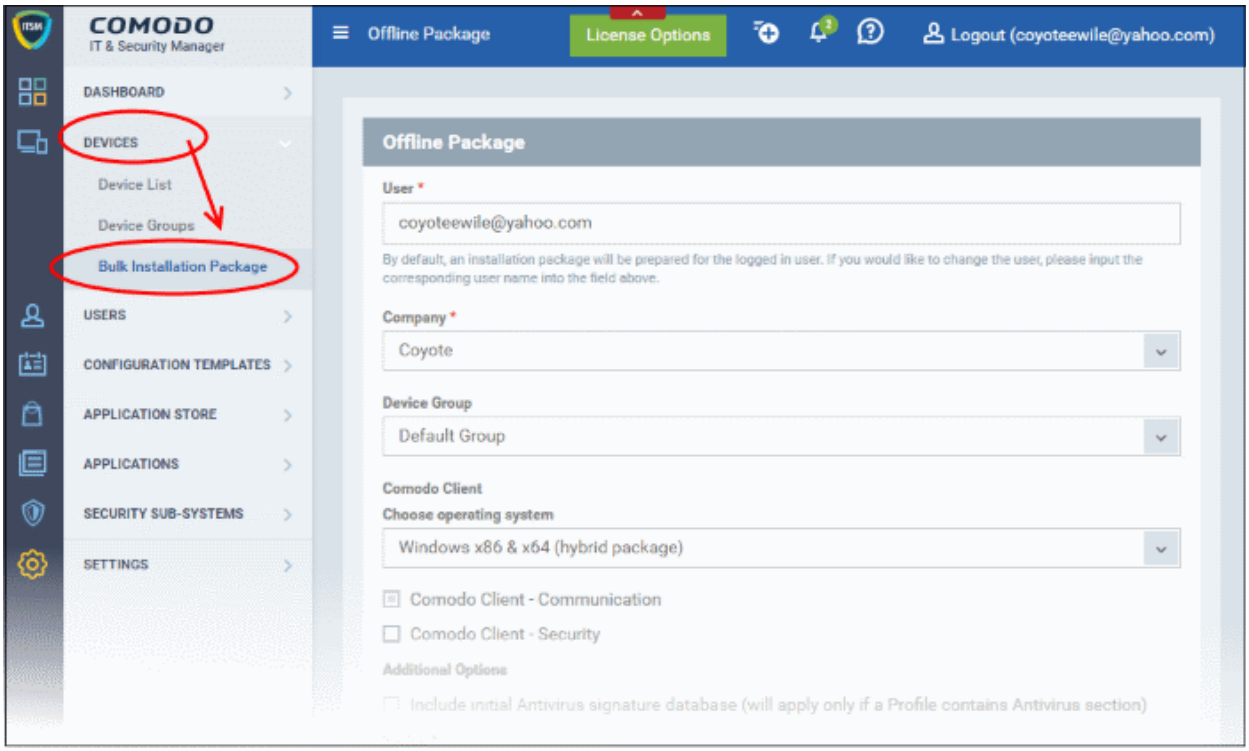
5.3.1. Enroll Windows and Mac OS Devices by Installing the ITSM Agent Package

Comodo ITSM requires an agent to be installed on each managed Windows and Mac OS device to enable communication with the ITSM Central Service Server. The following options are available:

- For individual devices, the agent will be automatically installed during enrollment and will establish a connection to the server. Refer to the sections **Enrolling Windows Endpoints** and **Enrolling Mac OS Endpoints** for more details.
- Administrators can bulk enroll devices by downloading the agent package from ITSM and creating a software installation group policy for their Active Directory (AD) server.
- Administrators can also manually enroll devices by downloading the installation package from ITSM and installing it on a target device.
- Administrators can also bulk enroll networked devices using Comodo Auto Discovery and Deployment Tool. This can be downloaded from the 'Tools' section of the Comodo One interface.

The 'Bulk Installation Package' interface allows administrators to download the agent and Comodo One Client packages for offline installation and for installation via Active Directory rules. The package can be configured to include Comodo One Client Security (CCS) and to apply selected configuration profiles to target devices.

- To open the Bulk Installation Package screen, click 'Devices' on the left and select 'Bulk Installation Package'.



You can download MSI/MST packages for deployment via AD server and a .EXE package for offline installation to individual endpoints. Refer to the following sections for more details:

- **Enrollment of Windows Devices Via AD Group Policy**.
- **Enrollment of Windows and Mac OS Devices by Offline Installation of Agent**
- **Enrollment of Windows Devices using Comodo Auto Discovery and Deployment Tool**

5.3.1.1. Enroll Windows Devices Via AD Group Policy

Installation via Active Directory (AD) group policy allows for the bulk enrollment of network devices for management by ITSM. You can download the default ITSM agent package (MSI) for installation and, if required, the transformed

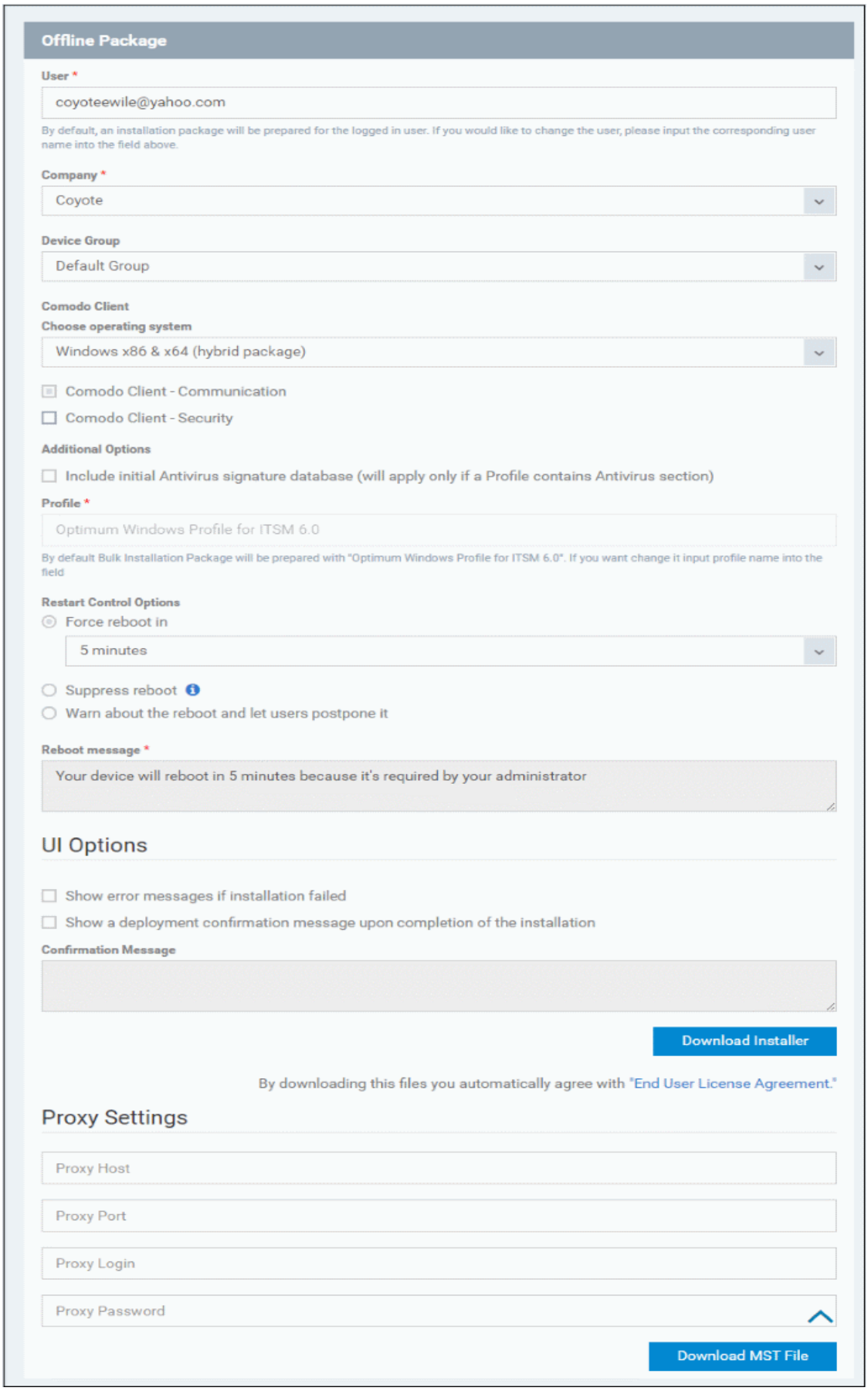
MST installation file to add to the GPO. The MST file includes the details of the proxy server that ITSM agent (CCC) and CCS should use to connect to ITSM and Comodo servers.

All devices enrolled by bulk installation through AD rules will be assigned to the currently logged-in administrator by default. If required, administrators can specify a different user to whom the devices should be assigned during the package download process. You can re-assign the devices to the correct owners from the 'Devices' interface at a later time. Refer to the section Changing a Device's Owner for more details.

Note: Enrollment of Windows devices via AD group policy allows you to install only the ITSM agent on the endpoints. You can remotely install the endpoint security software, Comodo Client - Security (CCS) at a later time from the ITSM interface. Refer to the section Remotely Installing Packages onto Windows Devices for more details.

To download the installation package

- Click 'Devices' on the left and choose 'Bulk Installation Package'



Offline Package - Form Parameters

Parameter	Description
User	Devices that are enrolled by installing the agent through AD Group Policy are assigned to the currently logged-in administrator by default. If you want the devices to be assigned to a different user, specify the user. • Start typing the first few characters of the name of the user in the text field and choose the user from the options that appear.
Company	Choose the company to which the endpoints should be assigned. This field only applies to C1 MSP customers and is not available for C1 Enterprise or ITSM stand-alone customers.
Device Group	The drop-down displays the list of device groups added to ITSM • Choose the device group, to which the enrolled devices are to be added. On completion of enrollment, the group configuration profiles will be applied to the endpoint. Refer to the section Assigning Configuration Profiles to a Device Group for more details.
Comodo Client	Allows you to choose the components to be added to the installation package. The available options are: • Choose operating system - Select the operating system of the target endpoints. The options are: Windows x64, Windows x86, Windows x86 & 64 and Mac OS. • Communication - Adds Comodo Client - Communication agent to the installation package. • Security - Adds the security product, 'Comodo Client - Security' (CCS) to the installation package. To create an installation package in MSI/MST file format for bulk enrollment through AD Group Policy, leave only the 'Communication' selected and 'Security' unselected. You can remotely install CCS at a later time on required endpoints from the ITSM. Refer to the section Remotely Installing Packages onto Windows Devices for more details. The rest of the configuration options related to CCS will not be enabled, if 'Security' is not selected under 'Comodo Client'.
Proxy Settings	Proxy settings allows you to specify a proxy server through which Comodo Client Security (CCS) and Comodo Client Communication (CCC) in the endpoints should connect to ITSM management portal and Comodo servers. If you choose not to set these, then CCS and CCC will connect directly as per the network

	settings. • Enter the IP address/hostname of the proxy server and port in the respective fields. • Enter the user-name and password of an administrative account on the proxy server in the Proxy Login and Proxy Password fields Note: If proxy is used then it is mandatory to configure the same proxy settings in client proxy settings in the profile(s) applied to the enrolled devices.

- Click 'Download Default MSI' to download the agent setup file for installation via Group Policy Object (GPO),

The agent package will be downloaded in .msi format. You can transfer the file to the required network location and create a software installation policy for deployment to network endpoints. Once the agent is installed, it establishes communication with the ITSM server to begin importing the device.

- To download the installation file to include a proxy server for CCC and CCS communication to ITSM and Comodo servers, click 'Download MST File'

ITSM will create a .mst transform file containing the proxy server installation commands. As above, you can save the file on the AD server from where you want to enroll the endpoints, and add to the GPO created for .msi file. After the agent is installed, it will establish communications with ITSM via the configured proxy servers to begin importing the device.

For more details about how to create a GPO for bulk enrollment see https://help.comodo.com/topic-399-1-856-11229-ITSM-%E2%80%93-Bulk-Enrollment-via-Active-Directory.html

Upon successful enrollment, any configuration profiles assigned to the user and groups to which the user belongs will be automatically applied to the devices.

Tip: For more details on creating Group Policy Object for remote installation of software, please refer to https://support.microsoft.com/en-us/kb/816102.

5.3.1.2. Enroll Windows and Mac OS Devices by Offline Installation of Agent

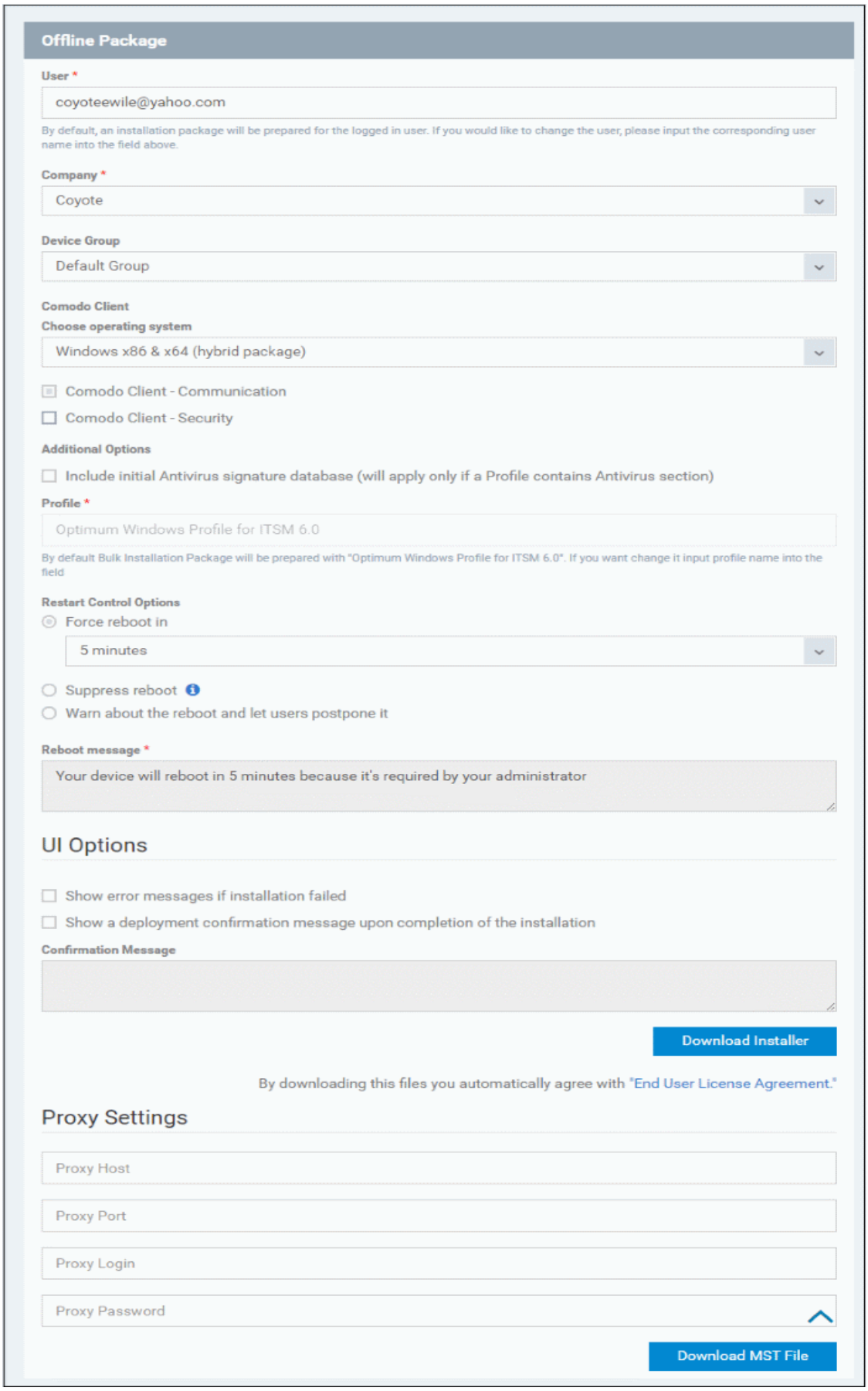
Administrators can download an installation package containing the agent and the Comodo Client - Security (CCS) software for offline installation. This is useful for endpoints which could not be reached by ITSM for auto-installation of the agent during enrollment.

ITSM allows administrators to specify the user to whom the enrolled device should be assigned and the initial configuration profile to be applied to the device. This will provide you with a package which is pre-configured for the user and the device.

Prerequisite - The end-user of the device should have been already added to ITSM. Administrators can download installation packages only for existing users.

To download the installation package

- Click 'Devices' on the left and choose 'Bulk Installation Package'



Offline Package - Form Parameters

Parameter	Description
User	Allows you to specify the user to whom the endpoint(s) should be assigned upon enrollment. By default, the 'User' field is pre-populated with the currently logged-in administrator. • Start typing the first few characters of the name of the user in the text field and choose the user from the options that appear.
Company	Choose the company to which the endpoints should be assigned. This field only applies to C1 MSP customers and is not available for C1 Enterprise or ITSM stand-alone customers.
Device Group	The drop-down displays a list of device groups added to ITSM • Choose the device group to which the enrolled devices should be added. On completion of enrollment, the group configuration profiles will be applied to the endpoint. Refer to the section Assigning Configuration Profiles to a Device Group for more details.
Comodo Client	Allows you to choose the components to be added to the installation package. The available options are: • Choose operating system - Select the operating system of the target endpoints. The options are: Windows x64, Windows x86, Windows x86 & 64 and MacOS. • Communication - Adds Comodo Client - Communication agent to the installation package. • Security - Adds the security product, 'Comodo Client - Security' (CCS) to the installation package. Choose both the options to create a package for offline installation.
Enrollment Link	This field will be available if you select Mac OS as the operating system. This is pre-populated with the URL to download the configuration profile pertaining to the selected company and group.
Comodo Client - Security	Allows you to choose whether or not CCS is to be included in the package.
Additional Options	Allows you to choose whether or not the latest virus signature database should be included in the installation package. Note: Selecting this option ships the latest database with the CCS software and allows the application to run the initial antivirus scan without needing to update its

	local database. This enables CCS to identify the very latest malware, even if the endpoint is offline. You can choose whether or not to include the database, depending on the network resources you are currently using. If you choose to not to include the signature database at this time, it will be automatically updated at the endpoint during the first run of CCS scan.
Profile	Allows you to choose a configuration profile to be applied to the endpoint(s) upon enrollment. • Start typing the first few characters of the profile to be applied in the text box and choose the profile from the options that appear. This is optional. If you do not choose a profile, only the default profiles will be applied upon device enrollment. Tip: You can apply additional profiles or remove existing profiles later. Refer to the section Viewing and Managing Profiles Associated with the Device for more details.
Restart Control Options	CCS requires endpoint(s) to be restarted for the installation to take effect. You can configure the restart options: • To restart the end-point a certain period of time after installation, choose 'Force the reboot in...' and select the delay period from the drop-down. A warning message will be displayed to the user and the endpoint will be restarted automatically when the time period elapses. • To continue without restarting, choose 'Suppress reboot'. The installation will take effect only when the user restarts the endpoint. • To restart the end-point at the user's convenience, choose 'Warn about reboot and let user(s) postpone the reboot'. Enter a message to be displayed to the user in the 'Reboot Message' field. The message dialog will be displayed to the user when installation is complete. The user can choose to restart the endpoint immediately by clicking 'Reboot now' or postpone the restart until a later time.
UI Options	Allows you configure the messages to be displayed to the user regarding the CCS installation status. If you wish the user to be notified about an unsuccessful installation, select 'Show error messages if installation failed' If you wish the user to be notified about a successful installation, choose 'Show a confirmation message upon completion of installation' and enter a message in the 'Confirmation Message' field.
Proxy Settings	Leave these blank as these settings are not required for the offline installation package.

- Click 'Download Installer'.

For Windows Devices

ITSM will create a custom installation file in .msi (if only agent is selected) or .exe format (if both agent and CCS are selected) for installation on to the user's device. Administrators should transfer the file to the target device for manual installation. Upon successful installation, CCS will be applied with the chosen profile irrespective of the online status of the endpoint(s). Once connected the agent will establish communication with the ITSM server and the device will be automatically enrolled.

For Mac OS X Devices

ITSM will create a custom installation file in .pkg format for installation on to the user's Mac OS X devices. Administrator should transfer the file to the target device for manual installation. After successful installation of agent and CCS, administrators should forward the enrollment link to the end user for installing the configuration file. The link should be clicked from the user's device for installing the configuration profile. Mac OS X devices will be enrolled to ITSM only after both the agent and the configuration profile are installed on the devices.

5.3.1.3. Enroll Windows Devices using Comodo Auto Discovery and Deployment Tool

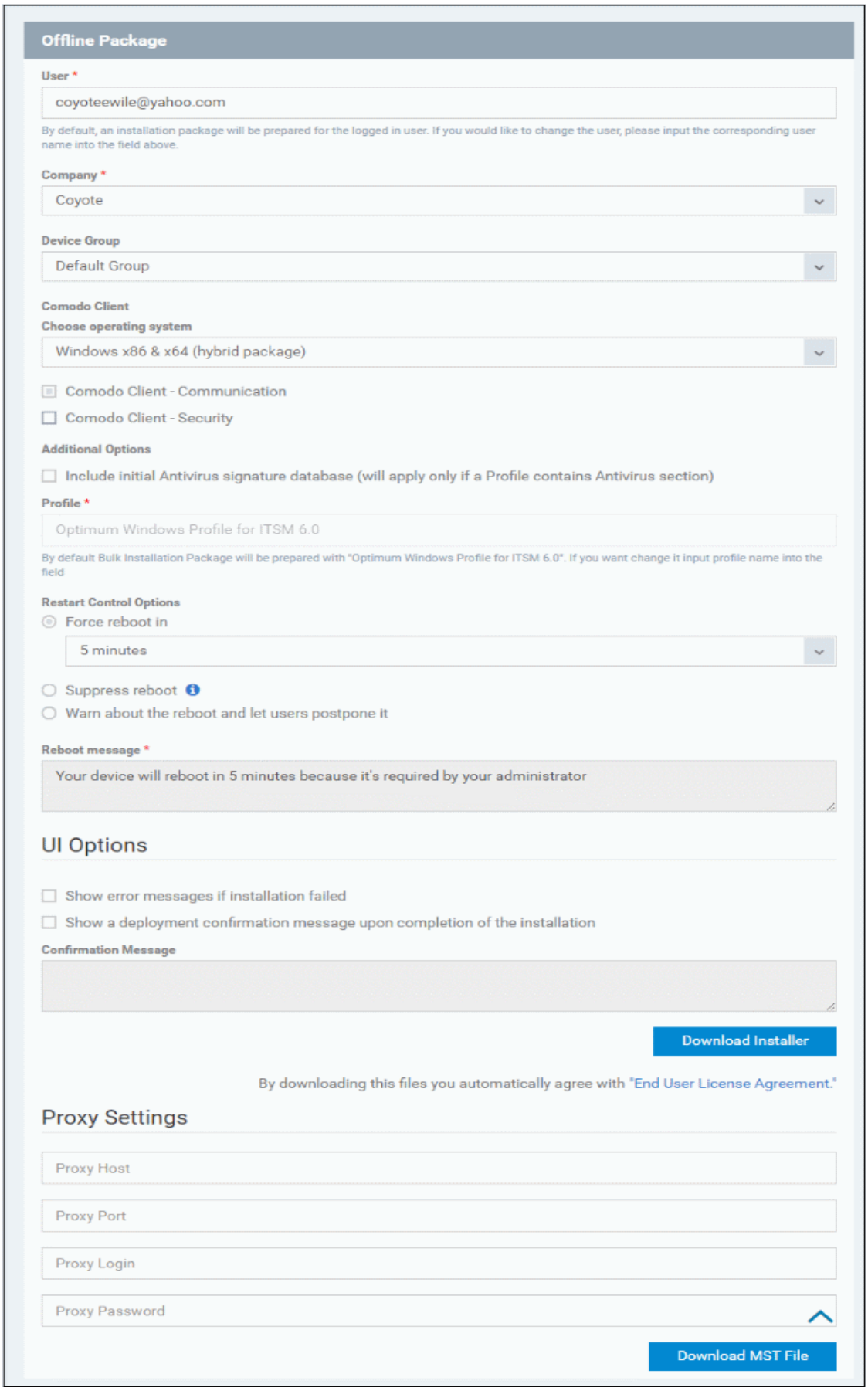
Comodo Auto Discovery and Deployment Tool (CADDT) allows network admins to remotely deploy the ITSM agent and client security application to multiple endpoints. You can install via Active Directory, Workgroup, IP address/range or host-name.

- You first need to create your installation packages using the 'Bulk Installation Package' interface in 'Devices'
- After creating your packages, you will be given the opportunity to download the 'Auto-Discovery and Deployment Tool' (ADDT).
- If you have already created your packages, you can download ADDT directly from the Comodo One 'Tools' interface. Help to use ADDT can be found at https://help.comodo.com/topic-289-1-851-11043-Introduction-to-Comodo-Auto-Discovery-and-Deployment-Tool.html

Prerequisite - The user of the device should already have been added to ITSM. Administrators can download installation packages only for existing users.

To download CADDT and installation packages

- Click 'Devices' on the left and choose 'Bulk Installation Package'


Offline Package
User *
coyoteewile@yahoo.com
By default, an installation package will be prepared for the logged in user. If you would like to change the user, please input the corresponding user name into the field above.
Company *
Coyote
Device Group
Default Group
Comodo Client
Choose operating system
Windows x86 & x64 (hybrid package)
Comodo Client - Communication
Comodo Client - Security
Additional Options
Include initial Antivirus signature database (will apply only if a Profile contains Antivirus section)
Profile *
Optimum Windows Profile for ITSM 6.0
By default Bulk Installation Package will be prepared with "Optimum Windows Profile for ITSM 6.0". If you want change it input profile name into the field
Restart Control Options
Force reboot in
5 minutes
Suppress reboot
Warn about the reboot and let users postpone it
Reboot message *
Your device will reboot in 5 minutes because it's required by your administrator
UI Options
Show error messages if installation failed
Show a deployment confirmation message upon completion of the installation
Confirmation Message
Download Installer
By downloading this files you automatically agree with "End User License Agreement."
Proxy Settings
Proxy Host
Proxy Port
Proxy Login
Proxy Password
Download MST File

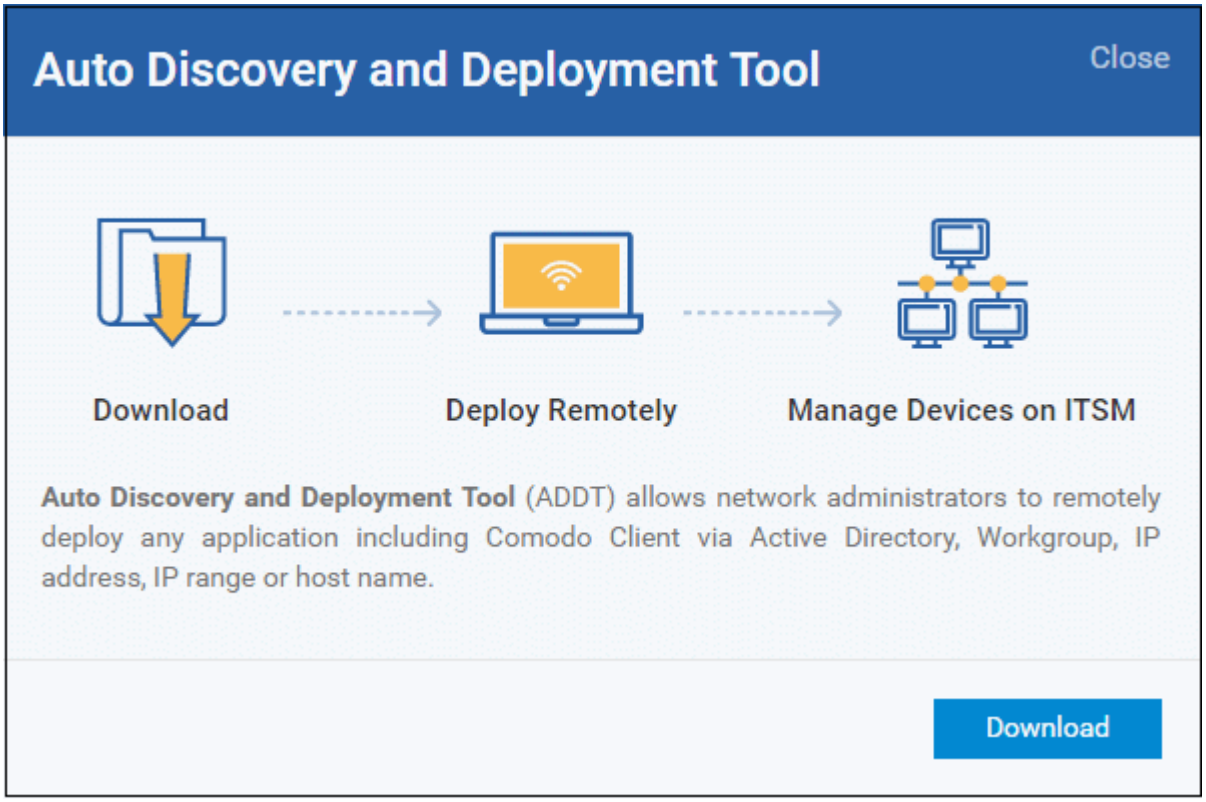
Offline Package - Form Parameters	
Parameter	**Description**
User	Allows you to specify the user to whom the endpoint(s) should be assigned upon enrollment. By default, the 'User' field is pre-populated with the currently logged-in administrator. • Start typing the first few characters of the name of the user in the text field and choose the user from the options that appear.
Company	Choose the company to which the endpoints should be assigned. This field only applies to C1 MSP customers and is not available for C1 Enterprise or ITSM stand-alone customers.
Device Group	The drop-down displays a list of device groups added to ITSM • Choose the device group to which the enrolled devices should be added. On completion of enrollment, the group configuration profiles will be applied to the endpoint. Refer to the section Assigning Configuration Profiles to a Device Group for more details.
Comodo Client	Allows you to choose the components to be added to the installation package. The available options are: • Choose operating system - Select the operating system of the target endpoints. The options are: Windows x64, Windows x86, Windows x86 & 64 and MacOS. • Communication - Adds Comodo Client - Communication agent to the installation package. This is required for the endpoints to connect to ITSM. • Security - Adds the security product, 'Comodo Client - Security' (CCS) to the installation package. Choose both the options to create a package for offline installation.
Comodo Client - Security	Allows you to choose whether or not CCS is to be included in the package.
Additional Options	Allows you to choose whether or not the latest virus signature database should be included in the installation package. Note: Selecting this option ships the latest database with the CCS software and allows the application to run the initial antivirus scan without needing to update its local database. This enables CCS to identify the very latest malware, even if the endpoint is offline. You can choose whether or not to include the database,

	depending on the network resources you are currently using. If you choose to not to include the signature database at this time, it will be automatically updated at the endpoint during the first run of CCS scan.
Profile	Allows you to choose a configuration profile to be applied to the endpoint(s) upon enrollment. • Start typing the first few characters of the profile to be applied in the text box and choose the profile from the options that appear. This is optional. If you do not choose a profile, only the default profiles will be applied upon device enrollment. Tip: You can apply additional profiles or remove existing profiles later. Refer to the section Viewing and Managing Profiles Associated with the Device for more details.
Restart Control Options	CCS requires endpoint(s) to be restarted for the installation to take effect. You can configure the restart options: • To restart the end-point a certain period of time after installation, choose 'Force the reboot in...' and select the delay period from the drop-down. A warning message will be displayed to the user and the endpoint will be restarted automatically when the time period elapses. • To continue without restarting, choose 'Suppress reboot'. The installation will take effect only when the user restarts the endpoint. • To restart the end-point at the user's convenience, choose 'Warn about reboot and let user(s) postpone the reboot'. Enter a message to be displayed to the user in the 'Reboot Message' field. The message dialog will be displayed to the user when installation is complete. The user can choose to restart the endpoint immediately by clicking 'Reboot now' or postpone the restart until a later time.
UI Options	Allows you configure the messages to be displayed to the user regarding the CCS installation status. If you wish the user to be notified about an unsuccessful installation, select 'Show error messages if installation failed' If you wish the user to be notified about a successful installation, choose 'Show a confirmation message upon completion of installation' and enter a message in the 'Confirmation Message' field.
Proxy Settings	Leave these blank as these settings are not required for the offline installation package via CADDT.

- Click 'Download Installer'

Your packages will be created and downloaded to your default download location. Next, you need to deploy the packages to your target endpoints.

At the end of the package creation process, you will be given the opportunity to download the 'Auto Discovery and Deployment Tool' (ADDT):



- Click 'Download'

Comodo ADDT is a portable app which does not require installation. ADDT allows you to deploy the ITSM agent and CCS onto endpoints via Active Directory, Workgroup or by Network Address. For more details about how to deploy applications via ADDT, visit https://help.comodo.com/topic-289-1-851-11043-Introduction-to-Comodo-Auto-Discovery-and-Deployment-Tool.html

5.3.2. Enroll Android and iOS Devices of AD Users

Prerequisite: The devices you want to bulk enroll belong to users who were imported to ITSM via integration with your Active Directory server. Refer to the section Importing User Groups from LDAP for more details.

- Enrolling the Android devices of users who were imported from an AD domain requires the ITSM agent to be installed on the device. After installation, the user should login to the client using their domain username and password.
- Instructions on enrolling via active directory are available in the ITSM interface. The instructions contain the agent download URL and the enrollment link.
  Open the enrollment instructions

  Import Android devices

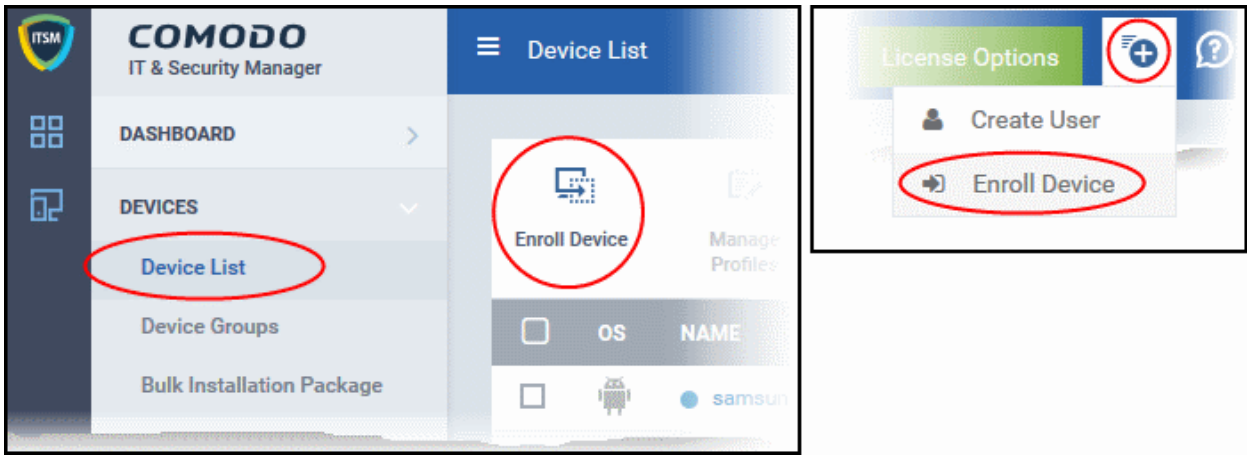
  Import iOS devices

To view enrollment instructions

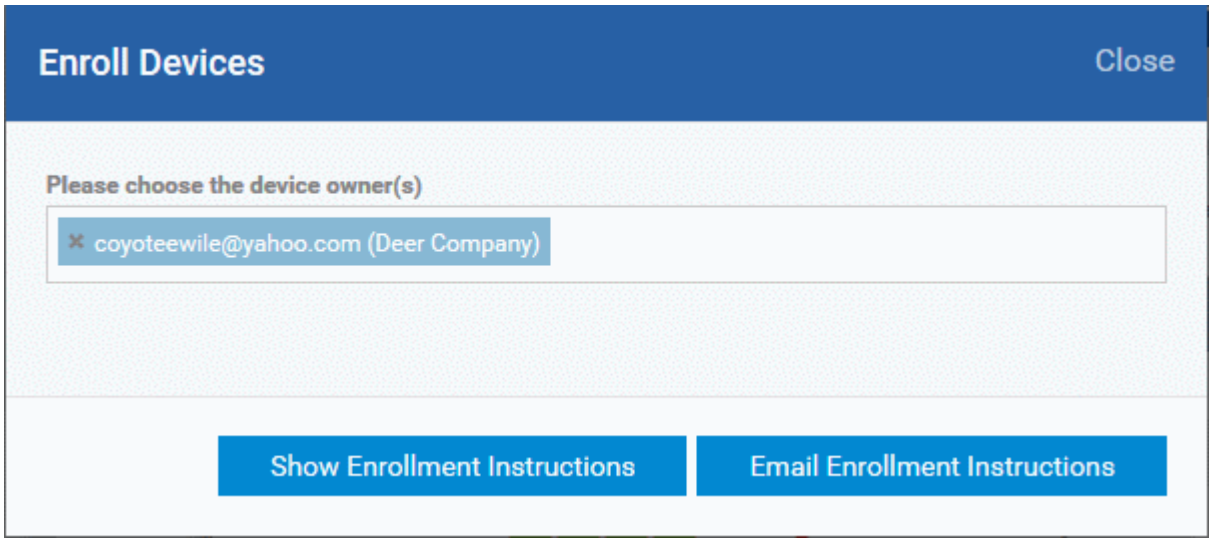
- Click 'Devices' > 'Device List' on the left
- Click the 'Enroll Device' button above the table

Or

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

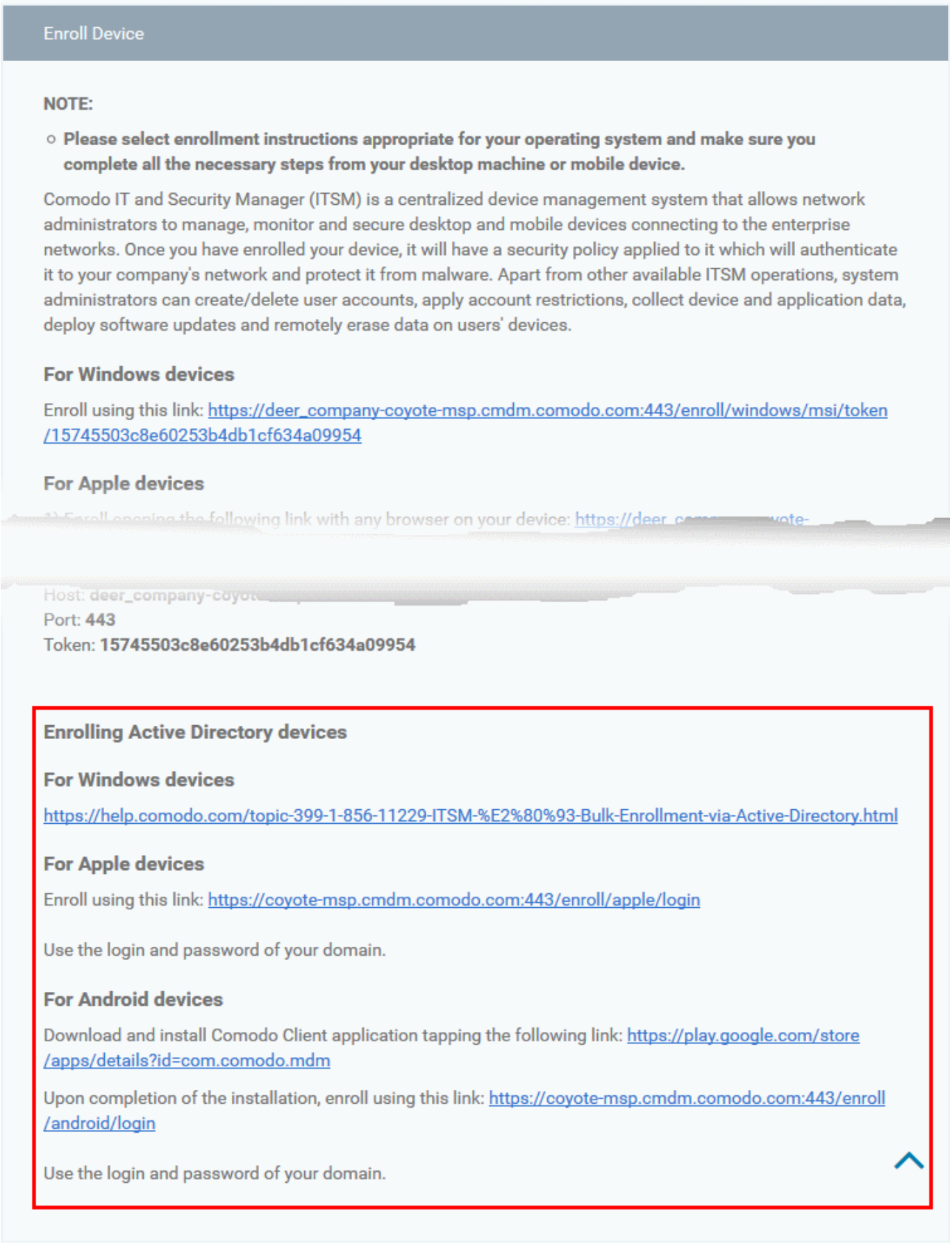


The 'Enroll Devices' dialog will open for the currently logged-in user:



- Click 'Show Enrollment Instructions'

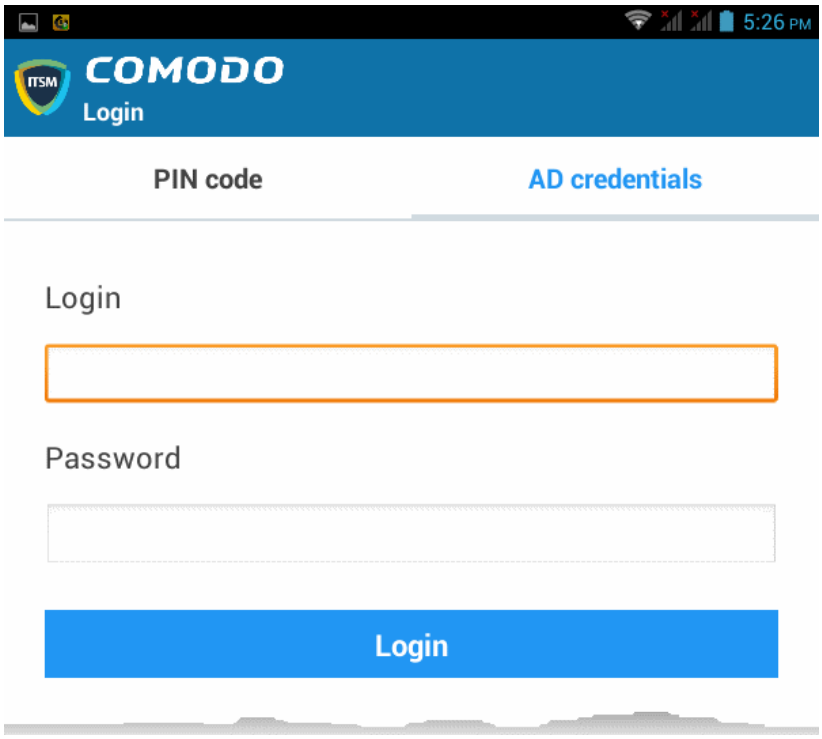
The 'Enroll Device' page will appear with enrollment instructions for Windows, Mac OS, Android and iOS devices.



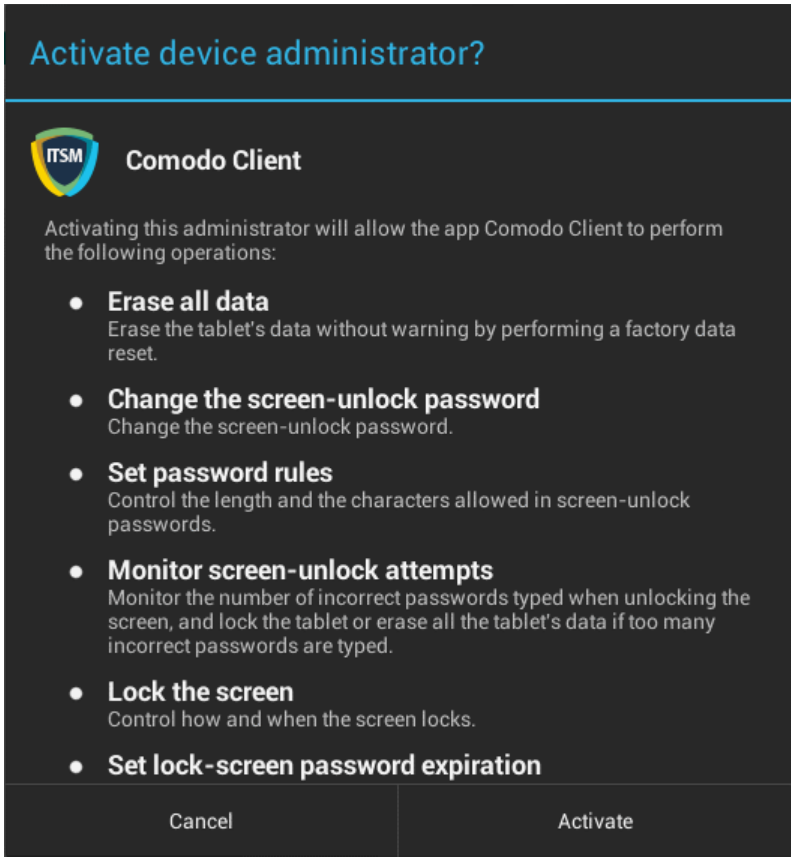
- Scroll down the page to the section 'Enrolling Active Directory devices'
- From this point, see either Import Android devices or Import iOS devices

Android Devices:

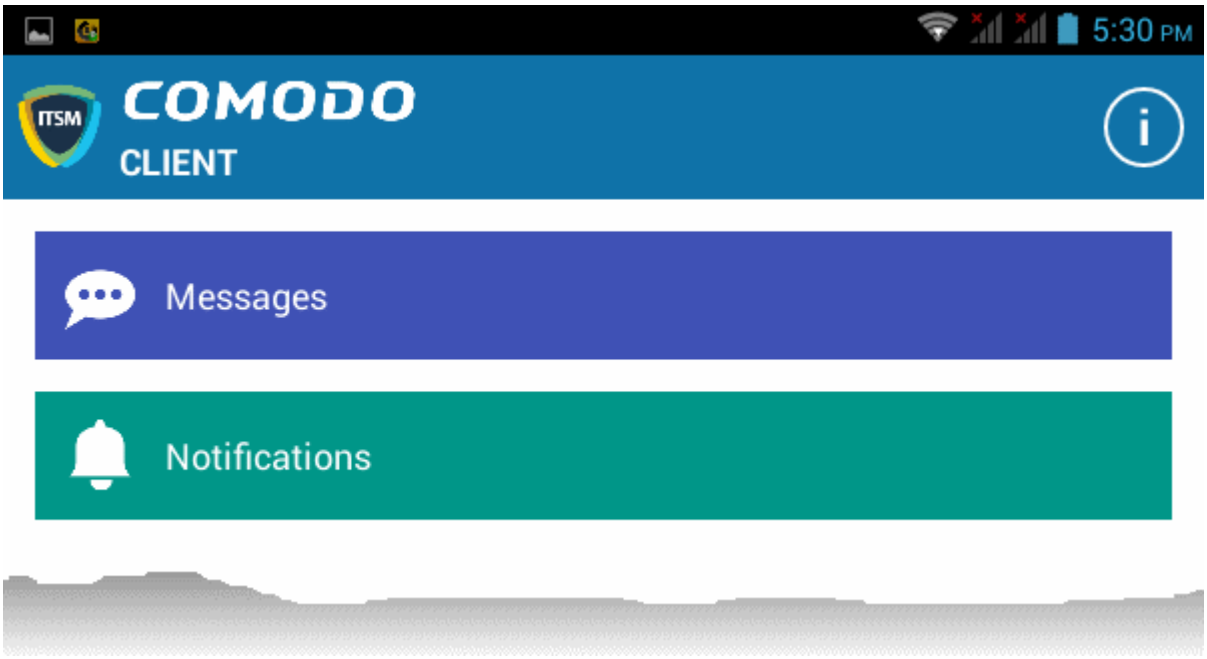
- Email the Android client download and enrollment links to all users
- Users should open the mail on the device you wish to enroll then open the agent download link
- The agent will be downloaded and installed on the device
- After installation is complete, the user should next tap the enrollment link.
- This will open a login page where they should enter the username and password they use to log into their domain:



- After agreeing to the EULA, the user should hit 'Activate' to grant the ITSM client admin privileges:



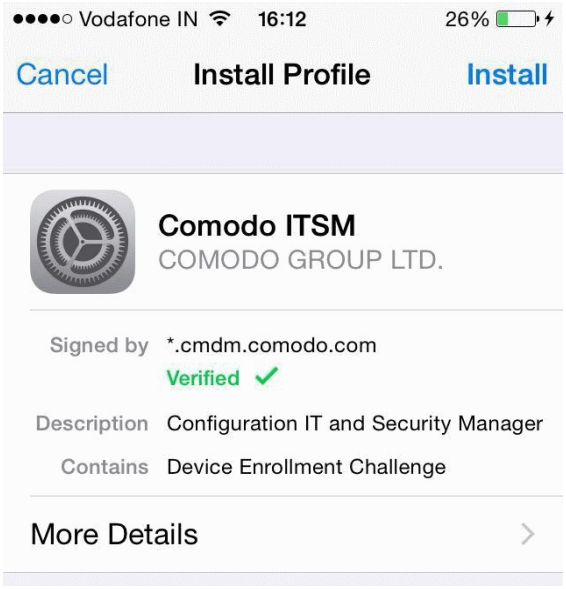
- After activating, the ITSM agent home screen will appear:



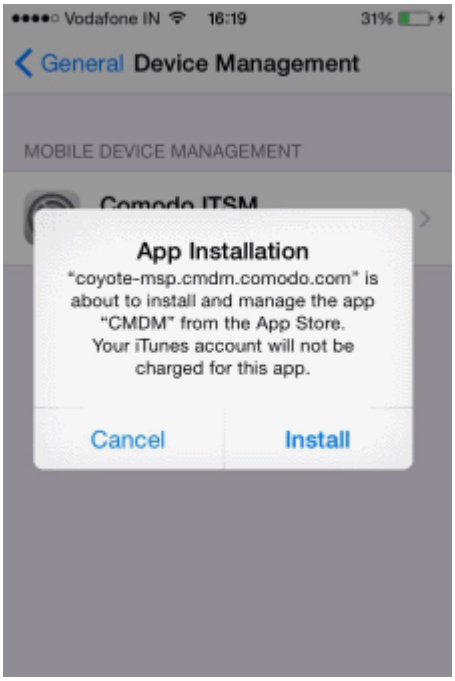
- The device is enrolled to ITSM and can be remotely managed from the ITSM console.

iOS Devices:

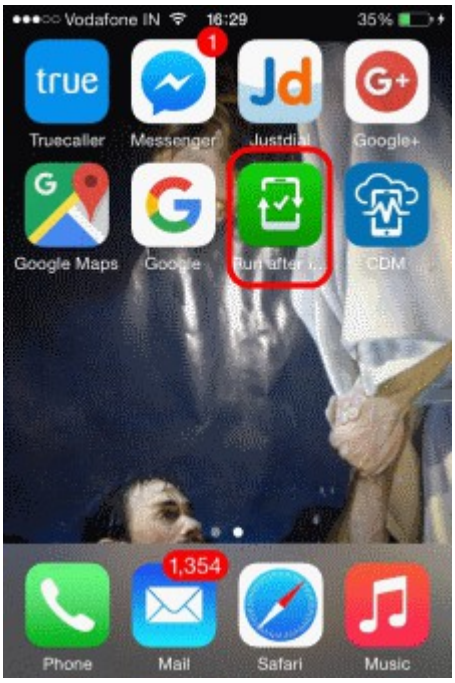
- Email the Apple enrollment link to all users
- Users should open the mail on the device you wish to enroll then tap the enrollment link
- After tapping the link, a configuration profile will be downloaded and the installation wizard will start.



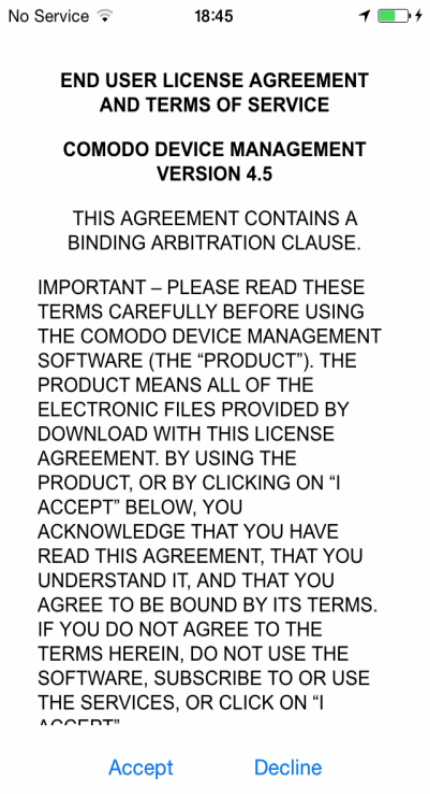
- The user needs to follow the wizard to complete the profile installation.
- After installing the profile, a login page will appear.
- The user needs to enter the username and password they use to log into their domain.
- The device will communicate with ITSM to begin enrollment.
- After the profile has been installed and the device enrolled, the client app installation will begin. The app is essential for app management, GPS location and messaging from the ITSM console.

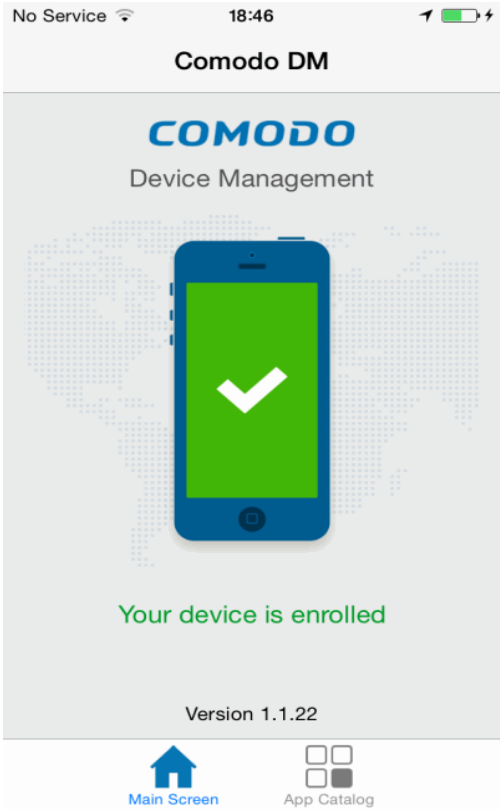


- The user should tap 'Install'. The app will be downloaded for free from the iTunes store using the user's iTunes account. Users may need to login with their Apple ID for the download to commence.
- After installation, users should tap the green 'Run After Install' icon on the home screen:

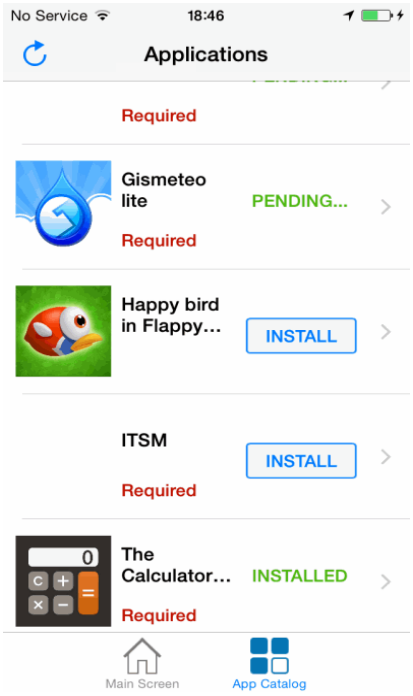


-
- The user should next accept the EULA to successfully complete device enrollment:





Tapping 'App Catalog' will display apps that are installed, required to be installed and available for installation:

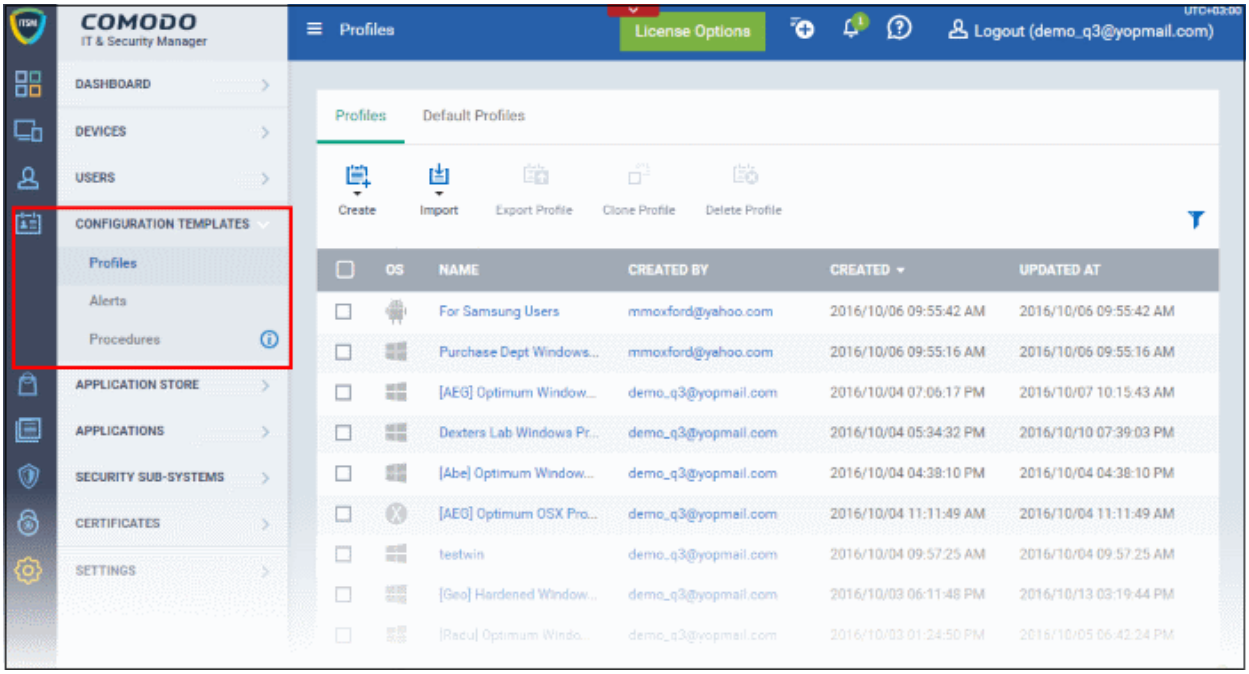


6.Configuration Templates

The 'Configuration Templates' section allows administrators to create and manage profiles for Android, iOS, OS X

and Windows operating systems. Profiles can can be applied to enrolled devices using the ITSM console. Each profile allows the administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and other general system settings.

You can also manage procedures, which include Windows patches deployment and instruction scripts for performing routine tasks such as disk cleaning, disk fragmentation and more. Procedures can be deployed as stand-alone instructions and run on enrolled devices and can also be scheduled as part of a profile. You can configure alerts to open tickets in Service Desk and also to create a notification in the interface. You can create multiple alerts and associate them with the monitoring feature in a profile according to your requirements.



The 'Configuration Templates' tab contains three sub sections:

- **Profiles** - Contains a list of every iOS, Android, Mac OS and Windows profile added to ITSM. Profiles listed here can be applied to individual devices, device groups, users and user groups. A profile can also be designated as a 'Default' profile. You can add new profiles, export profiles in .cfg format and import profiles from a saved or exported configuration file. The 'Default Profiles' tab contains profiles that ship with ITSM. Each default profile is pre-configured to provide optimum protection for devices at enrollment. The screen also lists profiles that have been created and marked as default by an administrator.
- **Alerts** - Allows you to configure alerts and raise tickets in Service Desk for any breach of monitoring setting in a profile. Alerts can also be configured to send notifications when a procedure fails to execute. Multiple alerts can be configured and these can be associated with monitoring settings and procedures in different profiles. Refer to the section '**Managing Alerts**' for more details.
- **Procedures** - Contains a list of predefined procedures that can be executed on enrolled devices. You can also create procedures according to your requirements and deploy them as a part of a profile. Refer to the section '**Managing Procedures**' for more details.

The interface allows the administrator to:

- Create/Import Configuration Profiles
- View the Profiles
- Edit Configuration Profiles
- Manage Default Profiles
- Manage Procedures
- Manage Alerts

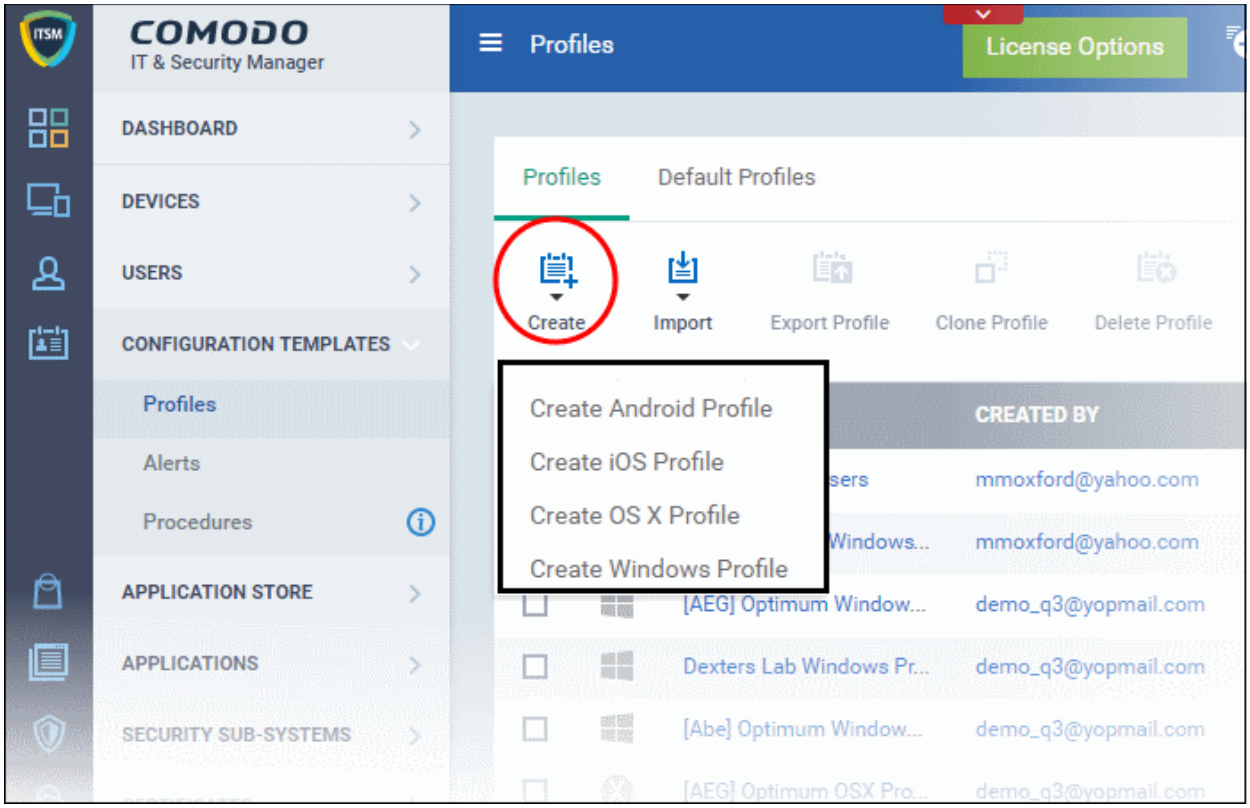
6.1. Creating Configuration Profiles

A configuration profile is a collection of settings which can be applied to devices that have been enrolled into Comodo IT and Security Manager. Each profile allows the administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and other general system settings. Profiles can be created and managed separately for iOS, Android, Mac OS and Windows devices. Once created, a profile can be applied to an individual device, to a group of devices, to a user, to a user group or designated as a 'default' profile.

The 'Profiles' interface allows you to create new profiles as well as to edit or delete existing profiles in the list. You can also create new profiles by cloning an existing profile or by importing a profile.

To create a configuration profile

- Click the 'Configuration Templates' tab from the left and choose 'Profiles'
- Click 'Create' from the options at the top



The 'Create' drop-down allows you to create new profiles for Android, iOS Mac OS and Windows devices. You can create any number of profiles with different parameters and settings for different devices. A single device can be have any number of profiles. If multiple profiles are associated with the device, the most restrictive policy will be applied. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera.

You can create a new Windows profile by defining security settings for each component of Comodo Client Security (CCS). In addition, you can import the current CCS configuration from an endpoint to use as a profile for other endpoints.

The interface also allows you to export an existing Windows profile in .cfg format. You can import the profile at a later time for re-use or modification.

The following sections explain more about:

- **Creating an Android Profile** - You can define parameters and configure various settings for Android devices and save them as a profile. Refer to the section **Profiles for Android Devices** for more details.
- **Creating an iOS Profile** - You can define parameters and configure various settings for iOS devices and save them as a profile. Refer to the section **Profiles for iOS Devices** for more details.

- Creating an OS X Profile - You can define parameters and configure various settings for the Antivirus component of the Comodo Antivirus for Mac installed on the Mac OS Endpoints and save them as a profile. Refer to the section Profiles for Mac OS Devices for more details.
- Creating a Windows Profile - You can define parameters and configure various settings for the Antivirus, Firewall, Containment components of the Comodo Client Security (CCS) installed on the Windows Endpoints and save them as a profile. Refer to the section Profiles for Windows Devices for more details.
- Importing a Windows Profile - You can import a profile from a stored configuration file or import the configuration of CCS with the current security settings of individual CCS components at an endpoint as a profile. Refer to the section Importing Windows Profiles for more details.

6.1.1. Profiles for Android Devices

Android profiles allow you to configure a device's network access rights, restrictions, antivirus scan schedules, user and device authentication certificates and other general settings.

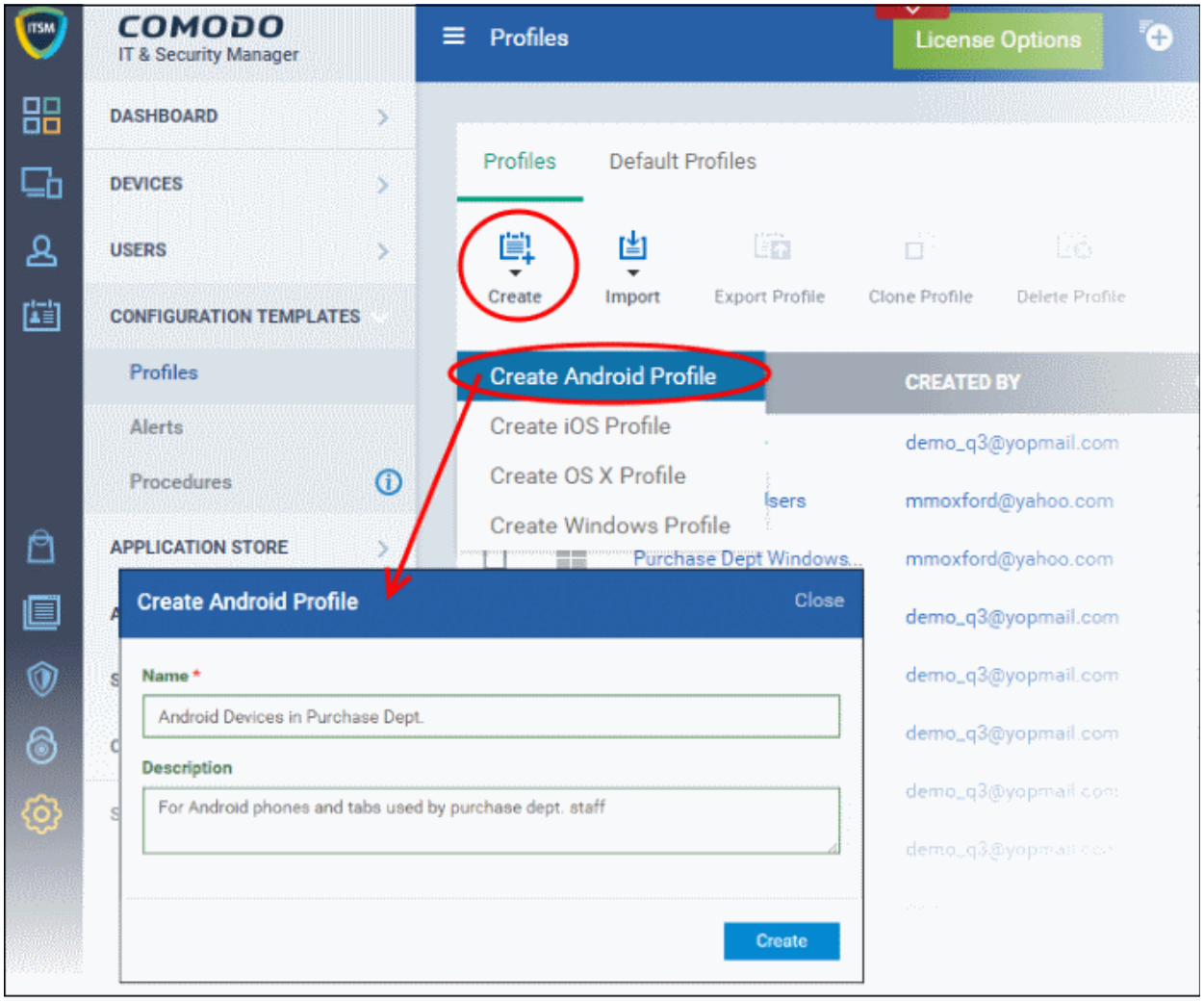
To create an Android profile

- Click 'Configuration Templates' on the left then choose 'Profiles'
- Click 'Create' then select 'Create Android Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profiles'.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Profile Section' drop-down. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices, device groups users and user groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.

To create an Android profile

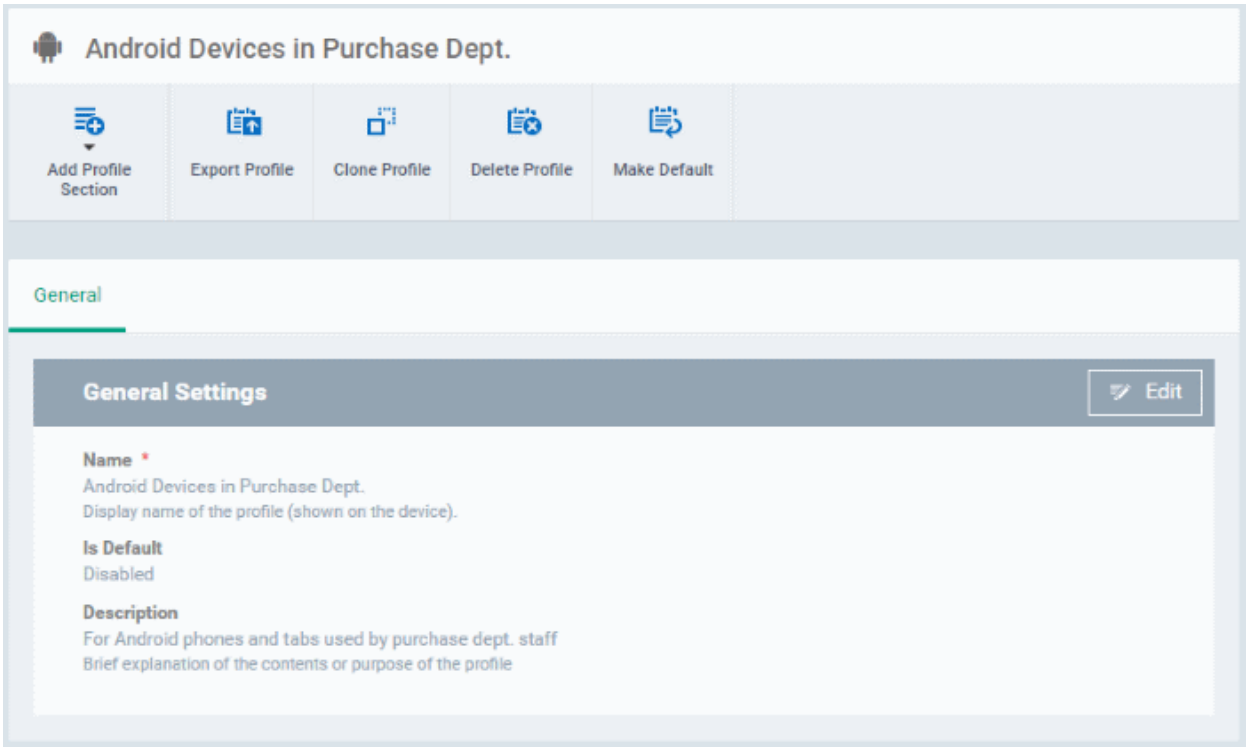
- Open the 'Profiles' interface by clicking 'Configuration Templates' on the left then 'Profiles'
- Click the 'Create' button above the table under 'Profiles' and choose 'Create Android Profile' from the options



In the 'Create Android Profile' dialog:

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

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

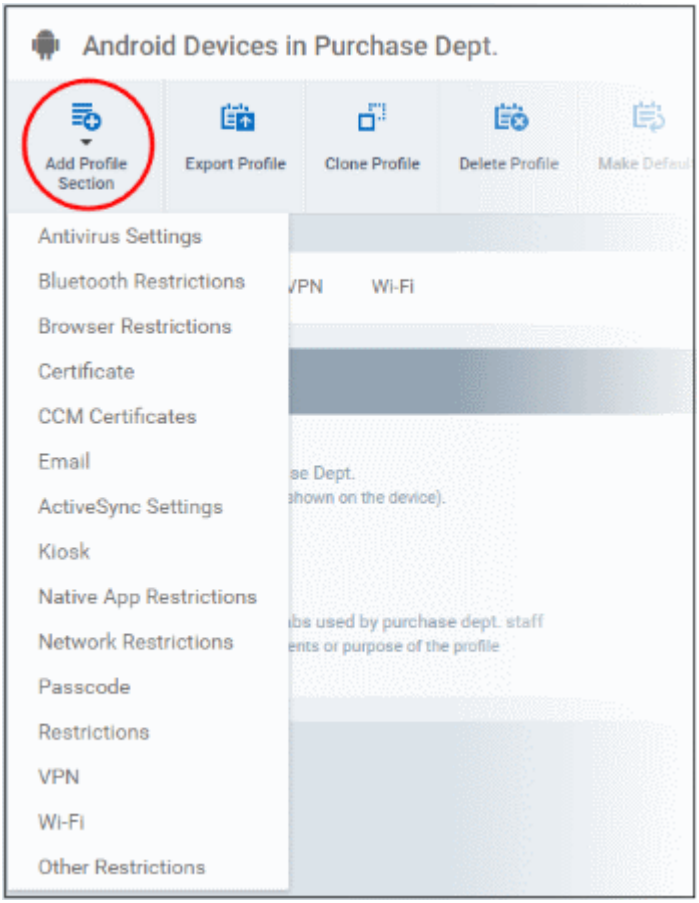


- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

Tip: You can set any profile as default profile from the Profiles screen. Refer to the section Editing Configuration Profiles for more details.

The next step is to add components for the profile.

- Click 'Add Profile Section' and select the security component from the list that you want to include in the profile

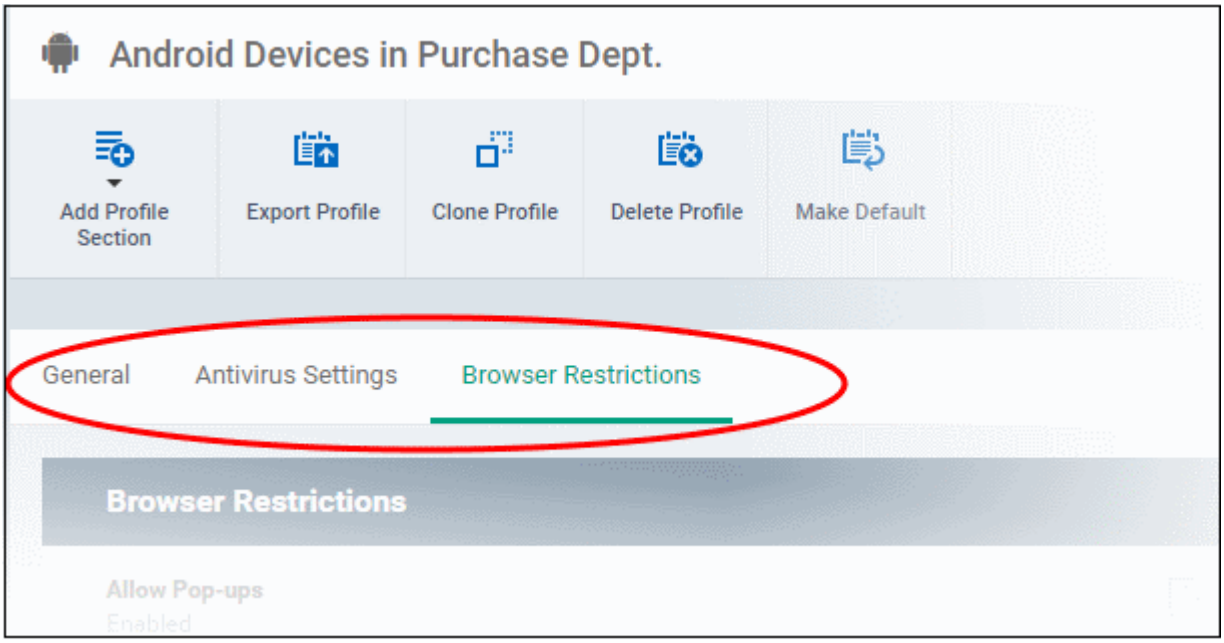


Note: Many Android profile settings have small information boxes next to them which indicate the OS and/or device required for the setting to work correctly.

For example, the following box indicates that the setting supports Android 4+ devices and SAFE 1.0+ (Samsung For Enterprises) devices:

Android 4.0+/SAFE 1.0+

The settings screen for the selected component will be displayed. After saving it will become available as a link at the top.



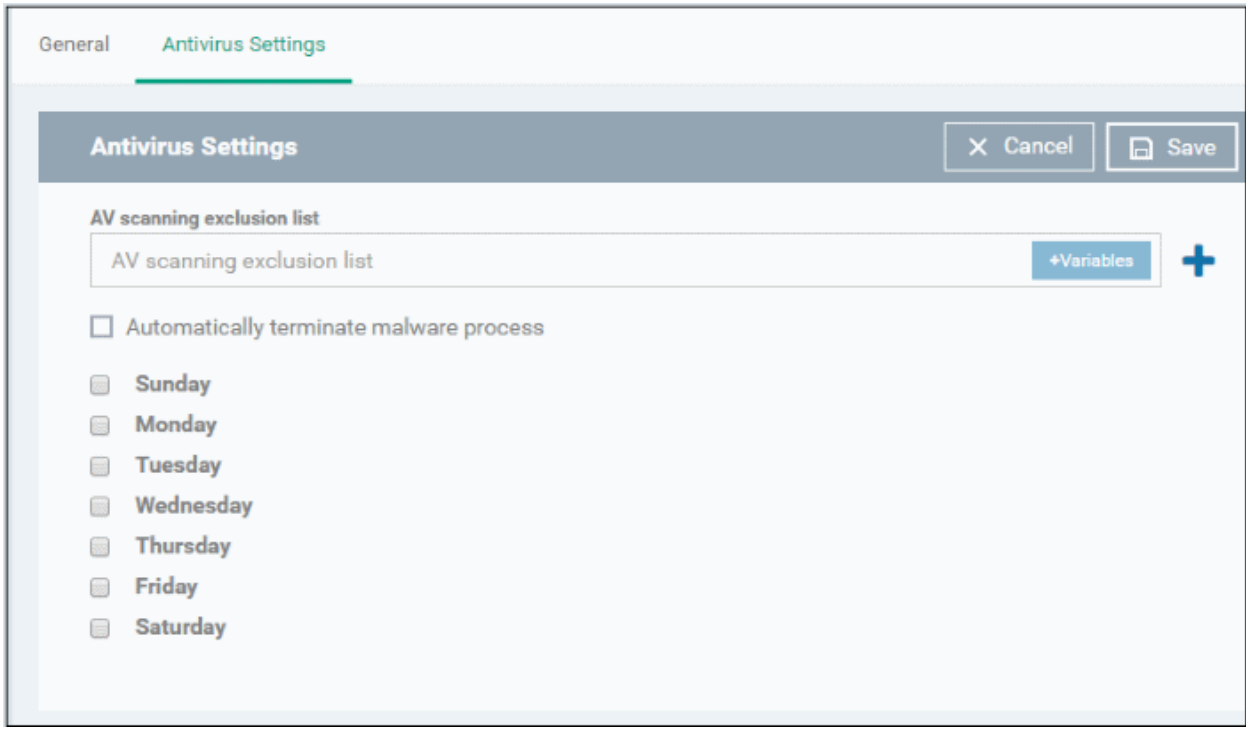
The following sections explain more about each of the settings:

- Antivirus
- Bluetooth Restrictions
- Browser Restrictions
- Certificate
- CCM Certificates
- Email
- Active Sync
- Kiosk
- Native App Restrictions
- Network Restrictions
- Passcode
- Restrictions
- VPN
- Wi-Fi
- Other Restrictions

To configure Antivirus settings

- Click 'Antivirus Settings' from the 'Add Profile Section' drop-down

The 'Antivirus Settings' screen will be displayed.



Antivirus Settings - Table of Parameters		
Form Element	**Type**	**Description**
AV scanning exclusion list	Text Field	Allows administrators to add trusted Apps. Trusted apps will be excluded from real-time, on-demand and scheduled Antivirus scans run on the devices. You can add apps installed from the Google Play Store and apps installed through the ITSM App store. • Enter the bundle identifier of the app that you want to exclude from antivirus scanning. For more details on getting the bundle identifier for an app, refer to the explanation given below this table. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Click + to add more 'AV scanning exclusions list' fields. To remove an item from the 'AV scanning exclusion list ' field, click the − button beside it.
Automatically terminate malware process	Checkbox	If enabled, any malware process detected during scanning will be terminated immediately on the devices.
Schedule scan	Checkbox	Select if you want to automate the process of antivirus scanning. Select the checkbox beside the day(s) that you want the scheduled scan to run.

- Click the 'Save' button.

The settings will be saved and displayed under the 'Antivirus Settings' tab. You can edit settings or remove the 'Antivirus Settings' section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

Obtaining Bundle/Package Identifier

The bundle identifier is a string that identifies the .apk package used to install the app.

For Google Play Apps:

The bundle identifier can be found at the end of the app's Google Play download URL.

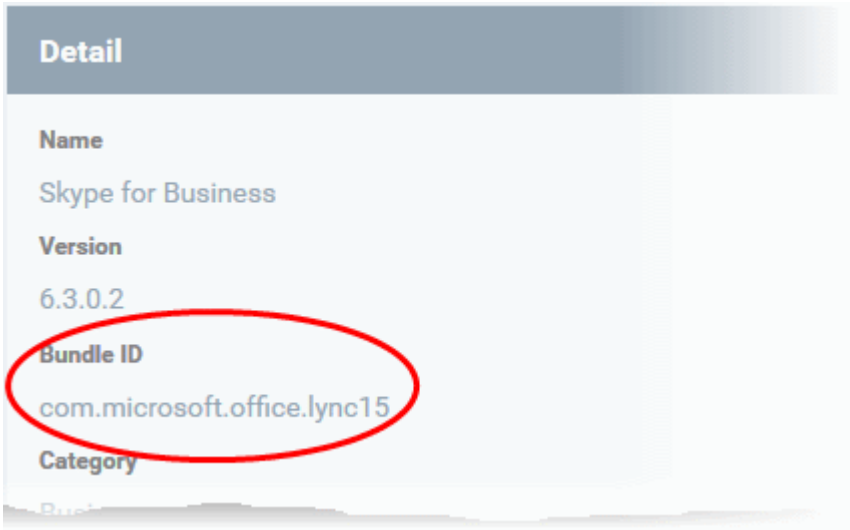
For example, 'com.comodo.batterysaver' is the Comodo Battery Saver app id in the URL

https://play.google.com/store/apps/details?id=com.comodo.batterysaver

For Enterprise Apps installed through ITSM App Store:

The bundle identifier can be viewed from the App Details screen of the App.

- Click 'App Store' from the left and choose Android
- Click on the app from the list displayed at the right



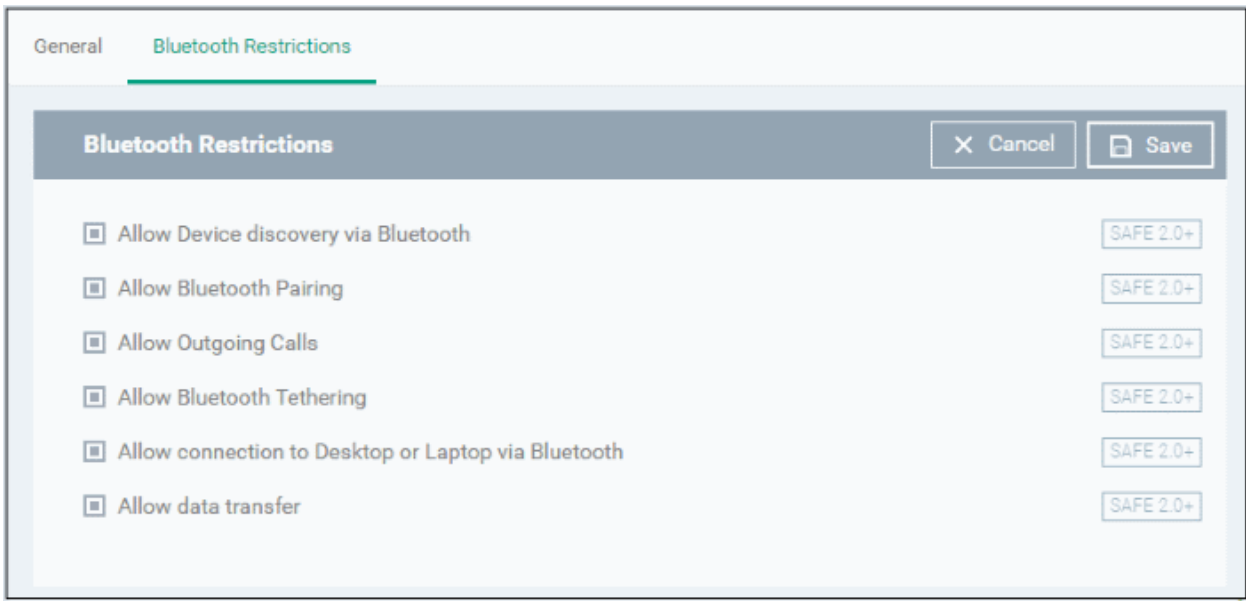
The bundle identifier is displayed in the 'Bundle ID' field.

To configure Bluetooth Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Bluetooth Restrictions' from the 'Add Profile Section' drop-down

The 'Bluetooth Restrictions' settings screen will be displayed.



Bluetooth Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Device discovery via Bluetooth	Checkbox	Allows discovery of other devices via Bluetooth.
Allow Bluetooth Pairing	Checkbox	Allows users' devices to pair with other their devices via Bluetooth.
Allow Outgoing Calls	Checkbox	Allows users to make calls using Bluetooth enabled devices (eg. hands-free devices)
Allow Bluetooth Tethering	Checkbox	Allows users to enable/disable Bluetooth tethering option.
Allow connection to Desktop or Laptop via Bluetooth	Checkbox	Allow users to enable/disable Bluetooth connection with Desktop or Laptop.
Allow data transfer	Checkbox	Allows data transfer between devices via Bluetooth.

- Click the 'Save' button.

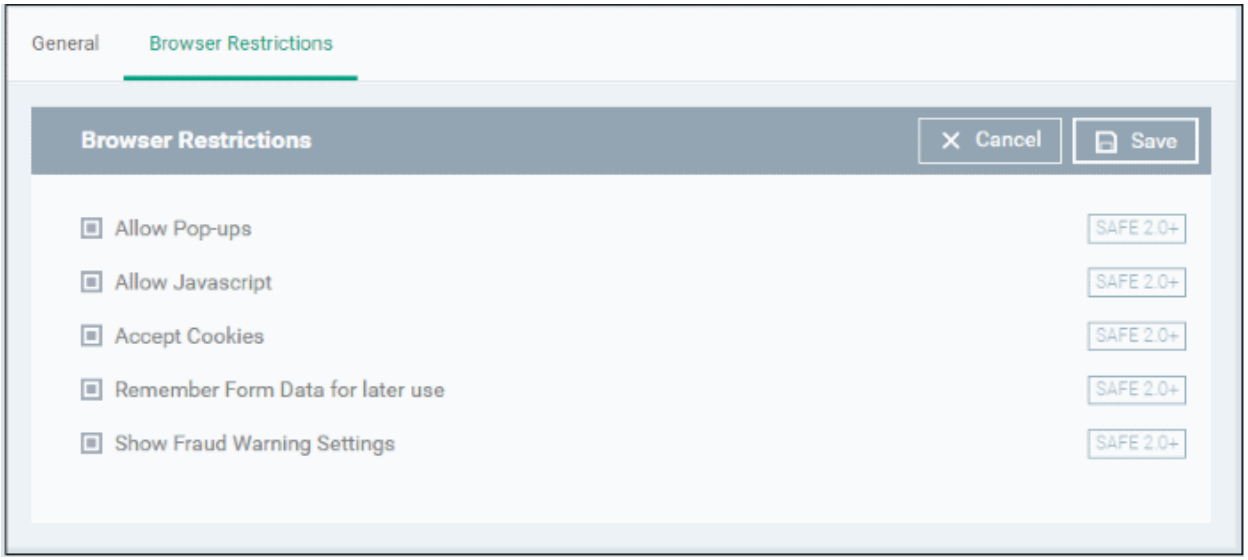
The settings will be saved and displayed under the 'Bluetooth Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Browser Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Browser Restrictions' from the 'Add Profile Section' drop-down

The 'Browser Restrictions' settings screen will be displayed.



Browser Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Pop-ups	Checkbox	Pop-ups in browsers will be allowed on user devices.
Allow Javascript	Checkbox	Java scripts will be allowed on user devices
Accept Cookies	Checkbox	Users will be allowed to modify Cookies settings on their devices.

Browser Restrictions Settings - Table of Parameters		
Remember Form Data for later use	Checkbox	Users will be allowed to use Auto Fill settings on their devices.
Show Fraud Warning Settings	Checkbox	Users will be allowed to view Fraud Warning Settings on their devices.

- Click the 'Save' button.

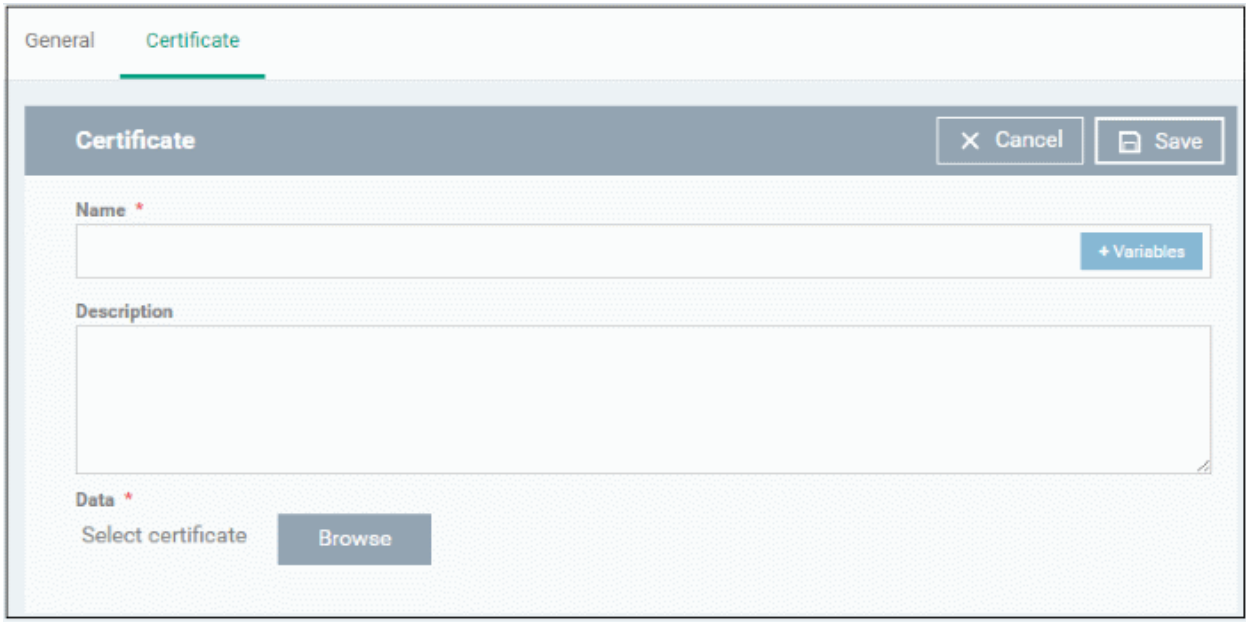
The settings will be saved and displayed under the 'Browser Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Certificate settings

The 'Certificate' settings section is used to upload certificates and will act as a repository from which certificates can be selected for use in other areas like 'Wi-Fi, 'Exchange Active Sync' and 'VPN'. You can also enroll user or device certificates from Comodo Certificate Manager (CCM) after activating your CCM account under Settings > Portal Set-Up > Certificates Activation.

- Click 'Certificate' from the 'Add Profile Section' drop-down

The 'Certificate' settings screen will be displayed.



Certificate Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name of the certificate. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Description	Text Field	Enter an appropriate description for the certificate.
Data	Browse button	Browse to the location of the stored certificate and select the certificate. Note: Only certificate files with extensions 'pub', 'crt' or 'key' can be uploaded.

- Click the 'Save' button.

The certificate will be added to the certificate store.

- To add more certificates, click 'Add Certificate' and repeat the process.
- To view the certificate key and edit the name, click on the name of the certificate
- To remove an unwanted certificate, select it and click 'Delete Certificate'

You can add any number of certificates to the profile and remove certificates at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To add CCM Certificates section

The Certificates Settings section of a profile allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Once the profile is applied to a device, a certificate request is automatically generated and forwarded to CCM. After issuance, the certificate will be sent to ITSM which in turn pushes it to the agent on the device for installation. You can add any number of certificates to a single profile. Appropriate certificate requests will be generated on each device to which the profile is applied.

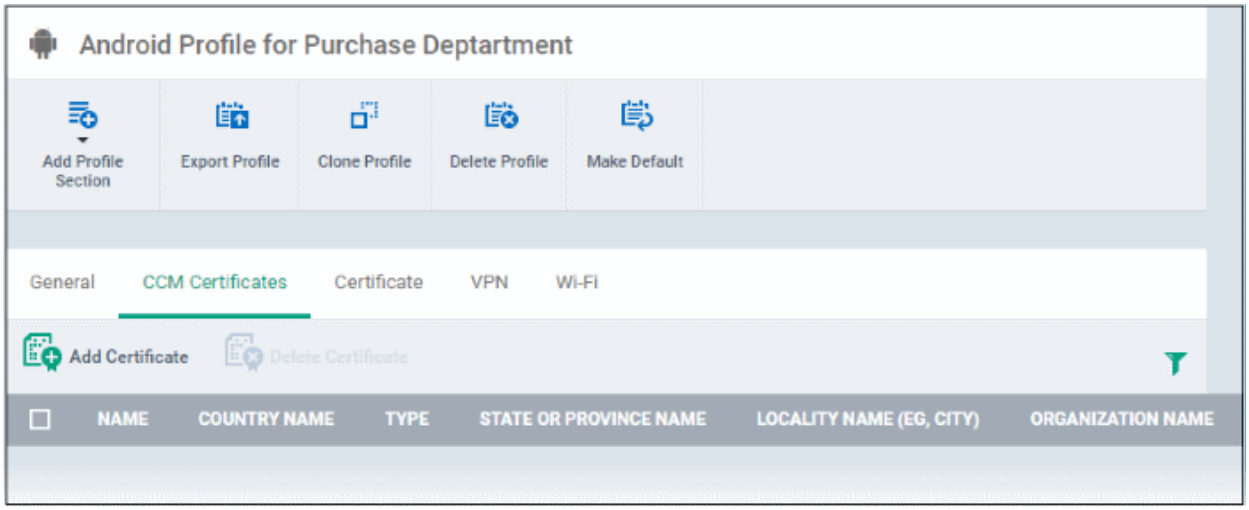
In addition to user authentication, client certificates can be used for email signing and encryption.

Prerequisite: Your CCM account should have been integrated to your ITSM server in order for ITSM to forward requests to CCM. For more details, refer to the section **Integrating with Comodo Certificate Manager.**

To configure CCM Certificate settings

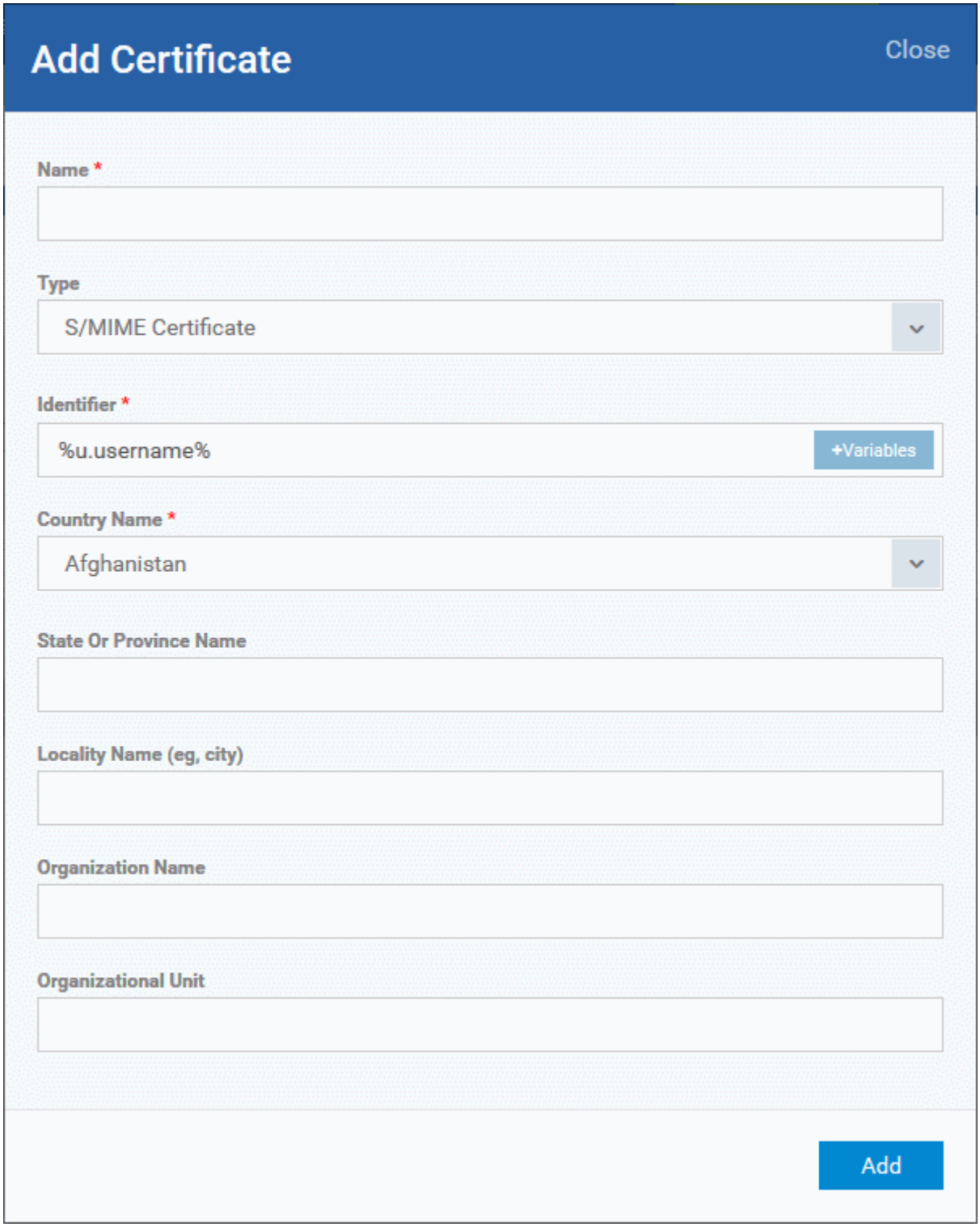
- Choose 'Certificates' from the 'Add Profile Section' drop-down

The settings screen for adding certificate requests to the profile will be displayed.



- Click 'Add Certificate' at the top to add a certificate request to the profile

The 'Add Certificate' form will appear.



Add Certificate - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter a name for the certificate to be requested, shortly describing its purpose.
Type	Drop-down	Select the type of certificate to be added. The available options are: • S/MIME Certificate (Client Certificate)

Add Certificate - Table of Parameters		
		• Device Certificate
Identifier	Text Field	The Identifier field will be auto-populated with mandatory variables depending on the chosen certificate type. • For client certificate, %username% will be added for fetching the username to be included as subject in the certificate request. • For device certificate, %d.uuid% will be added for fetching the device name to be included as subject in the certificate request. You can add more variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Country Name	Text Field	Enter the address details of the user/organization in appropriate fields.
State or Province Name		
Locality Name (eg. City)		
Organization Name	Text Field	Enter the name of the organization to which the user/device pertains. **Prerequisite**: The organization should have been added to your CCM account.
Organizational Unit	Text Field	Enter the name of the department to which the user/device pertains. **Prerequisite**: The department should have been defined under the organization in your CCM account.

- Click 'Add' once you have completed the form.
- Repeat the process to add more certificate requests.

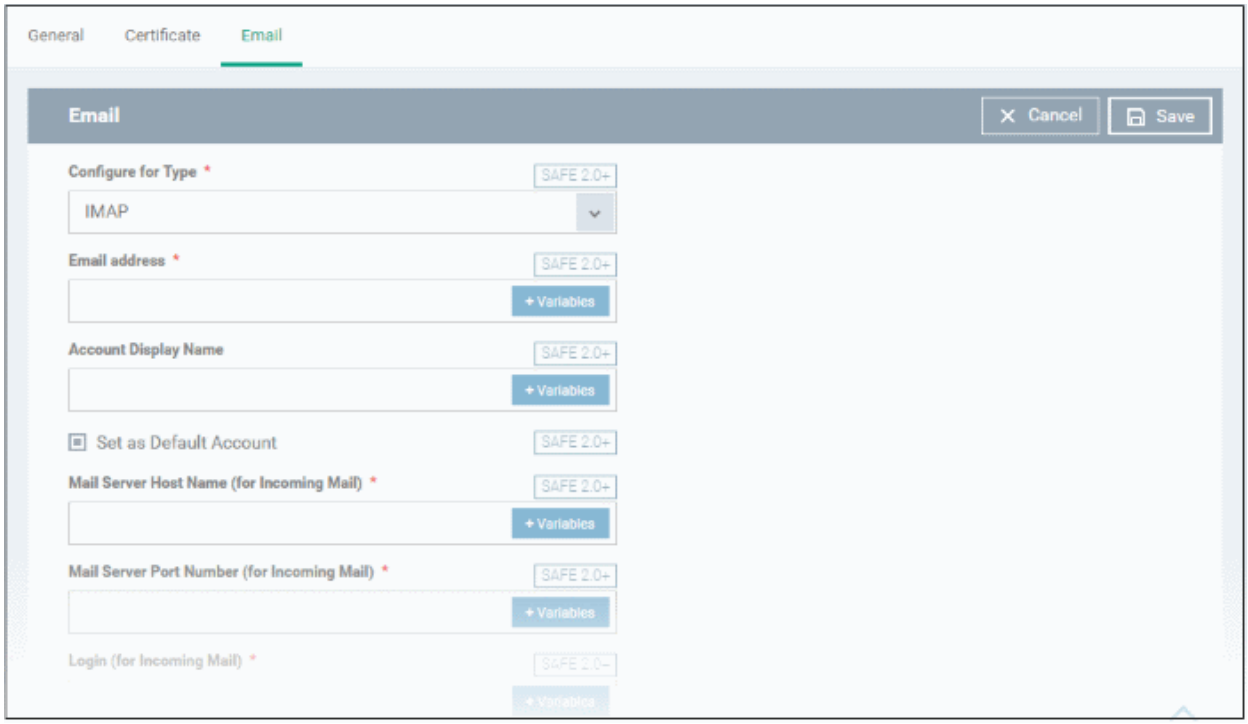
The certificate requests will be generated from the devices once the profile is applied to them.

To configure Email settings

Note: The feature is supported for Samsung for Enterprise (SAFE) devices only. This area allows administrators to configure email settings on devices.

- Click 'Email' from the 'Add Profile Section' drop-down

The settings screen for Email configuration will be displayed.



Email Settings - Table of Parameters		
Form Element	**Type**	**Description**
Configure for Type*	Drop-down	Choose the protocol for incoming mail server from IMAP and POP.
Email address*	Text Field	If the profile is for a single user, enter the email address of the user at the incoming mail server. If the profile is for several users, click the 'Variables' button + Variables, and click + beside '%u.mail%' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Account Display Name	Text Field	If the profile is for a single user, enter the name to identify the user's email account at the incoming mail server. If the profile is for several users, click the 'Variables' button + Variables, and click + beside '%u.login%' from the 'User Variables list'. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Set as Default Account	Checkbox	If enabled, the email account will be set as default for the users.
Mail Server Host Name (for Incoming Mail) *	Text Field	For a single user, enter the host name or IP address of the incoming mail server. For several users, add the variable to fetch the incoming mail server hostname/IP address by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section Configuring Custom Variables.
Mail Server Port Number (for Incoming Mail) *	Text Field	For a single user, enter the server port number used for incoming mail service. For POP3, it is usually 110 and if SSL is enabled it is

Email Settings - Table of Parameters		
		995. For IMAP, it is usually 143 and if SSL is enabled it is 993. For several users, add a variable to fetch the incoming mail server port number by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section Configuring Custom Variables.
Login (for Incoming Mail)*	Text Field	If the profile is for a single user, enter the username for the email account of the user at the incoming mail server. If the profile is for several users, click the 'Variables' button + Variables, select '%u.mail %' from the 'User Variables' list and click +. The email usernames of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Password (for Incoming Mail)*	Text Field	If the profile is for a single user, enter the password for the email account of the user at the incoming mail server. If the profile is for several users, click the 'Variables' button + Variables and click + beside the variable from the list. The email passwords of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Use SSL Incoming	Checkbox	If enabled, communication between incoming mail server and devices is encrypted using SSL (Secure Socket Layer Protocol).
Accept All Certificates (for Incoming Mail)	Checkbox	If enabled, the device automatically accepts all SSL certificates.
Accept TLS Certificates (for Incoming Mail)	Checkbox	If enabled, the device automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol).
Mail Server Host Name (for Outgoing mail)*	Text box	For a single user, enter the host name or IP address of the outgoing (SMTP) mail server. For several users, include the variable to fetch the outgoing mail server hostname/IP address by clicking the 'Variables' button + Variables and click + beside the variable from the list. For more details on variables, refer to the section Configuring Custom Variables.
Mail Server Port Number (for Outgoing Mail) *	Text box	For a single user, enter the server port number used for outgoing (SMTP) mail service. If no port number is specified then ports 25, 587 and 465 are used in the given order. For several users, include the variable to fetch the outgoing mail server port number by clicking the 'Variables' button + Variables and clicking + beside the variable from the list. For more details on variables, refer to the section Configuring Custom Variables.
Login (for outgoing Mail)*	Text Field	If the profile is for a single user, enter the username for the email account of the user at the outgoing (SMTP) mail server. If the profile is for several users, click the 'Variables' button + Variables, and click + beside '%u.login%' from the 'User Variables' list. The email usernames of the users to whom the profile is associated will be

Email Settings - Table of Parameters		
		automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Password (for outgoing Mail)*	Text Field	If the profile is for a single user, enter the password for the email account of the user at the outgoing (SMTP) mail server. If the profile is for several users, click the 'Variables' button + Variables and click + beside the variable created to fetch the email password of the user from the 'User Variables' list. The email passwords of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Use SSL (for Outgoing Mail)	Checkbox	If enabled, communication between outgoing mail server and devices is encrypted using SSL.
Accept All Certificates (for Outgoing Mail)	Checkbox	If enabled, the device automatically accepts all SSL certificates.
Accept TLS Certificates (for Outgoing Mail)	Checkbox	If enabled, automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol).
Sender Name	Text Field	For a single user, enter the name that should appear in the 'From' field of the sent emails from the device. For several users, add the variable to fetch the sender name by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section Configuring Custom Variables.
Set Signature	Text Field	Enter the signature and other details that will appear at the end of the mails sent from the device. You can add variables to the text by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section CConfiguring Custom Variables.
Prevent Moving Mail to other Accounts	Checkbox	If enabled, the user cannot move sent or received mails to another account.
Always Vibrate on New Email Notification	Checkbox	If enabled, the device will vibrate in addition to sound alert when a new email is received.
Vibrate on New Email Notification if device is silent	Checkbox	If enabled, the device will vibrate when a new email is received, when the device is in silent mode.

- Click the 'Save' button.

The settings will be saved and displayed under the 'Email' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

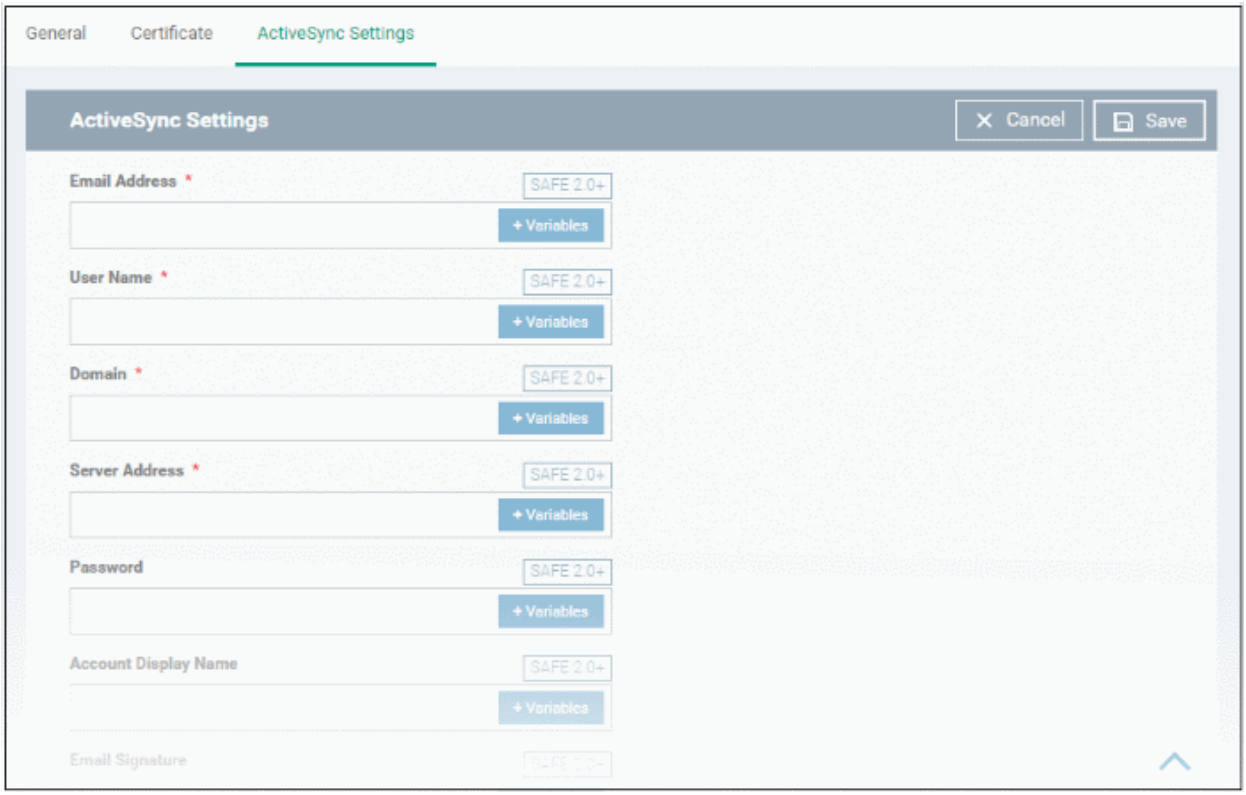
To configure ActiveSync settings

ActiveSync settings allows you to configure user access to Exchange Server mail accounts.

Note: Please make sure users are not blocked from using the email client on their devices in **Native App Restrictions**

- Click 'ActiveSync Settings' from the 'Add Profile Section' drop-down

The 'ActiveSync Settings' screen will be displayed.



ActiveSync Settings - Table of Parameters		
Form Element	**Type**	**Description**
Email Address *	Text Field	Click the 'Variables' button + Variables and click + beside '%u.mail' from the User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section **Configuring Custom Variables**.
User Name *	Text Field	Click the 'Variables' button + Variables and click + beside '%u.login' from the User Variables' list. The username of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section **Configuring Custom Variables**.
Domain *	Text Field	Enter the domain name in the field. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**.
Server Address *	Text Field	Enter the server address of the ActiveSync. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**.
Password	Text Field	Leave the field blank. The user will be prompted to enter the password

ActiveSync Settings - Table of Parameters		
		while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Account Display Name	Text Field	If the profile is for a single user, enter the name to identify the user's email account at the exchange server. If the profile is for several users, click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables list'. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Email Signature	Text Field	Enter the signature and other details that will appear at the end of the mails sent from the device. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Maximum Email Size	Comobo Box	The maximum size of email that the user can download from the server. Use the controls or enter the value in the field. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Sync Emails	Drop-down	Choose the period for which the emails are to be kept synchronized between the device and the exchange server from the recent past, from the drop-down.
Sync Calendar	Drop-down	Select the period for which the calendar events are to be synchronized between the device and the exchange server, from the drop-down.
Use SSL	Checkbox	If enabled, communication between the device and the exchange server is encrypted using SSL (Secure Socket Layer Protocol).
As Default Account	Checkbox	If enabled, the email address will be used as default for sending out emails.
Accept All Certificates	Checkbox	If enabled, the device automatically accepts all SSL certificates.
Can Sync Contacts	Checkbox	Select this option if you wish to allow synchronization of user contacts between device and exchange server.
Can Sync Calendar	Checkbox	Select this option if you wish to allow the synchronization of the calendar events set by the user at the device and the exchange server.
Can Sync Tasks	Checkbox	Select this option if you wish to allow the synchronization of Tasks scheduled by the user at the device and the email server.
Manual Roaming Sync	Checkbox	If enabled, the user can use the sync feature manually while away from the home network.
Always Vibro on New Email	Checkbox	If enabled, the device will vibrate when a new email is received.

Fields with * are mandatory.

- Click the 'Save' button.

The settings will be saved and displayed under the 'ActiveSync Settings' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

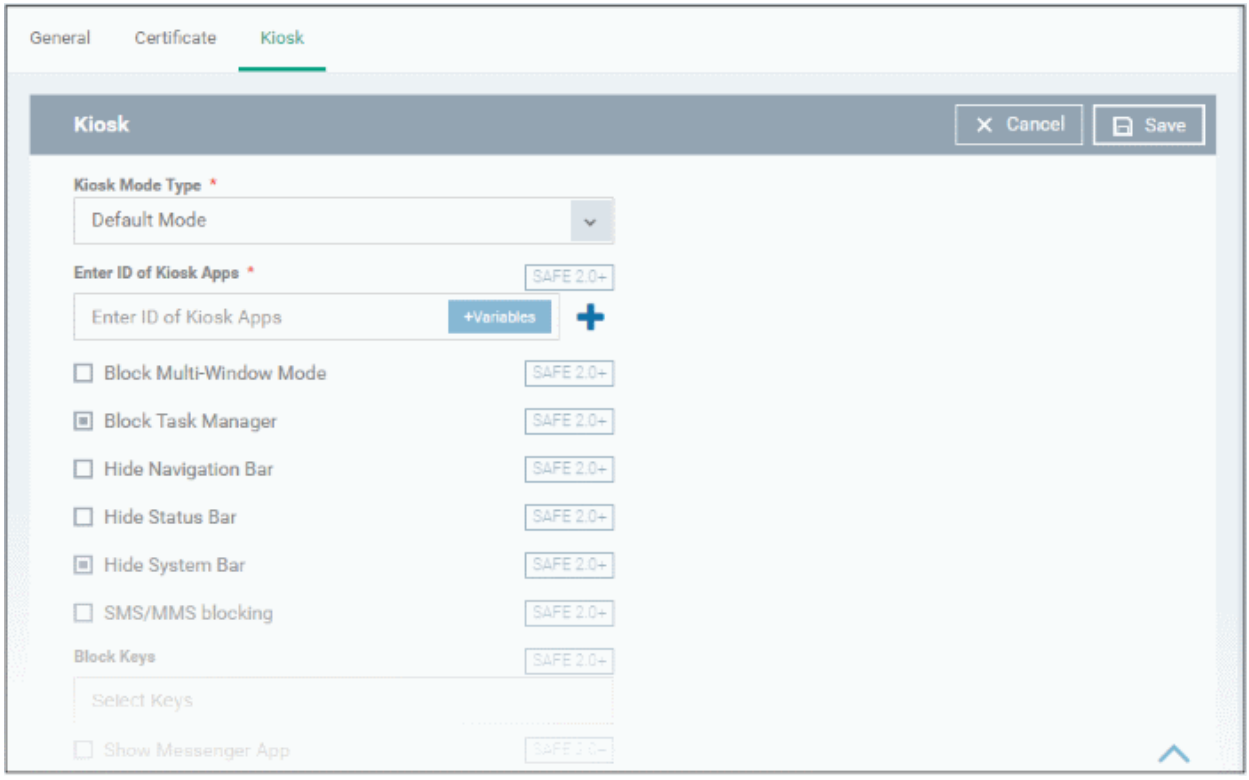
To configure Kiosk settings

Note: This feature is only supported by Samsung for Enterprise (SAFE) devices.

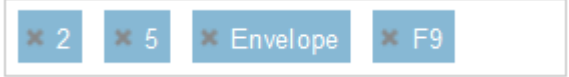
Background: Kiosk mode is a feature intended to help administrators lock-down mobile devices by limiting the applications that are able to run on a device. 'Locking' a device to particular applications can prevent users from opening other applications or straying into important device configuration areas. You can also block aspects of the OS should you wish. An example is a retail or school environment where only certain apps should be used on the device.

- Click 'Kiosk' from the 'Add Profile Section' drop-down

The 'Kiosk' settings screen will be displayed.



Kiosk Settings - Table of Parameters		
Form Element	**Type**	**Description**
Kiosk Mode Type	Drop-down	The two Kiosk modes are: • Default mode - Run multiple apps in Kiosk mode. Users will not be able to run non-kiosk applications. Kiosk mode can only be exited by entering the admin bypass password. • Single App mode - Users can only run the single application that you specify. Users will not be able to run non-kiosk applications. Kiosk mode can only be exited if the admin disables it in the ITSM console. Restrictions on access to other device functions, such as task manager

Kiosk Settings - Table of Parameters		
		and the status bar, can also be configured for either mode.
If 'Single App' is selected as Kiosk Mode Type:		
Enter ID of Kiosk Apps	Text Field	Enter the Package ID of the app that will run in Kiosk mode. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**. For more details on Package ID, refer to the explanation under **Obtaining Bundle/Package Identifier**.
If 'Default mode' is selected as Kiosk Mode Type:		
Enter ID of Kiosk Apps	Text Field	Enter the package IDs of the apps that will run in Kiosk mode. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**. For more details on Package ID, refer to the explanation under **Obtaining Bundle/Package Identifier**. Click + to add more 'App IDs for allowed Apps om Kiosk Mode' fields. To remove a field, click the − button beside it.
Block Multi-Window Mode	Checkbox	If selected, users cannot open multiple windows.
Block Task Manager	Checkbox	If selected, users cannot access task manager screen.
Hide Navigation Bar	Checkbox	If selected, the navigation bar will be hidden on the devices.
Hide System Bar	Checkbox	If selected, the system bar will not be displayed.
SMS/MMS blocking	Checkbox	If selected, the all the SMSs and MMSs to the device will be blocked.
Block Keys	Drop-down	This feature allows to selectively block touch keys and icons available on device screen. For example, if you do not want the device owners to use Caps Lock key and so on, then these can be blocked. To select the key to be blocked, click in the 'Block Keys' field:  The keys will be displayed from the drop-down. Scroll down to view the full list and select the required key to be blocked. Add more keys to be blocked similarly. 

Kiosk Settings - Table of Parameters		
The following features will be visible if 'Default mode' is selected as Kiosk Mode Type:		
Show messenger App	Checkbox	If selected, the messenger app will be available.
Show email App	Checkbox	If selected, email app will be available.
Show dialer App	Checkbox	If selected, dialer app will be available.
Show admin bypass button	Checkbox	If selected, the 'Admin bypass button' will be available, which an admin can tap, enter the password to exit from the Kiosk mode.
Admin bypass password	Text Field	Enter the password required to exit the Kiosk mode. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

- Click the 'Save' button.

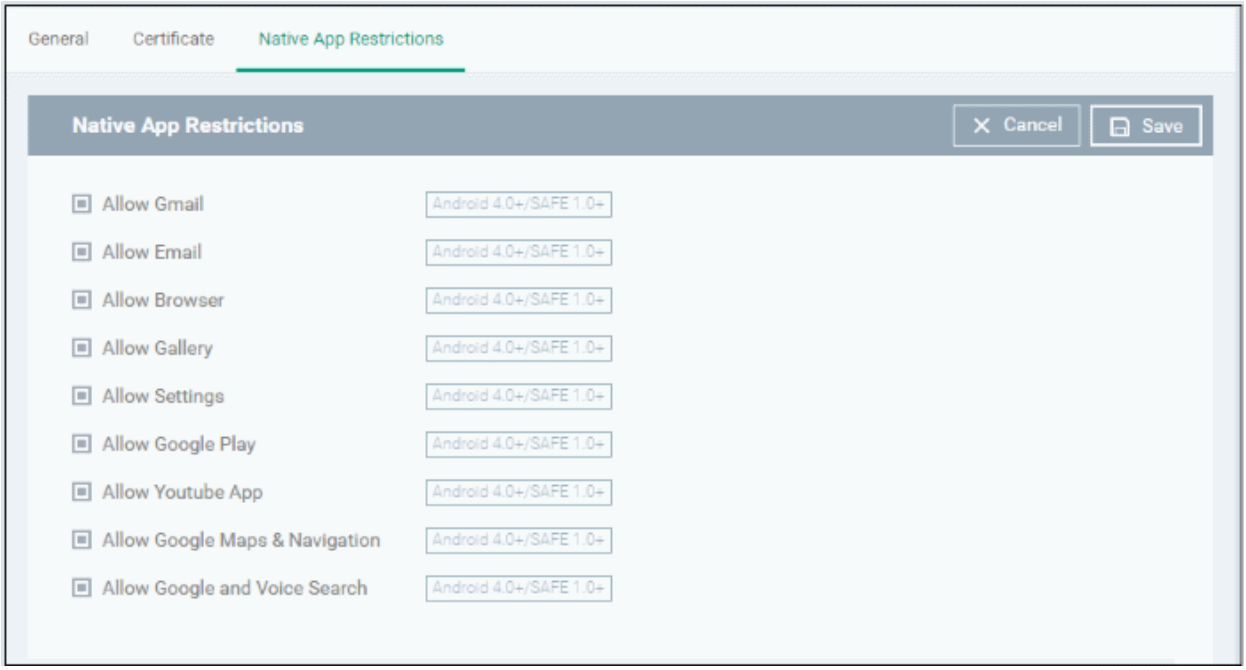
The settings will be saved and displayed under the 'Kiosk' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Native App Restriction settings

Applications that are included with the device operating system, such as the email and gallery apps, are called 'native applications'. Administrators can choose to allow or deny access to these native applications. The feature is available for Android version 4.0 + and Samsung for Enterprise devices SAFE 1.0 + version.

- Click 'Native App Restrictions' from the 'Add Profile Section' drop-down

The 'Native App Restriction' settings screen will be displayed.



Native Application Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Gmail	Checkbox	Select this to allow users to access Gmail app.

Native Application Restrictions Settings - Table of Parameters		
Allow Email	Checkbox	Select this to allow users to access the default Email app.
Allow Browser	Checkbox	If enabled, users can access the default Android browser on their devices.
Allow Gallery	Checkbox	If enabled, users can access Gallery on their devices.
Allow Settings	Checkbox	Select this to enable users to change their device settings.
Allow Google Play	Checkbox	If enabled, users can access Google Play on their mobile devices.
Allow YouTube App	Checkbox	If enabled, users can access the YouTube app.
Allow Google Maps & Navigation	Checkbox	If enabled, users can access Google Maps and Navigation app on their devices.
Allow Google and Voice Search	Checkbox	If enabled, users can use Google and Voice Search services.

- Click the 'Save' button.

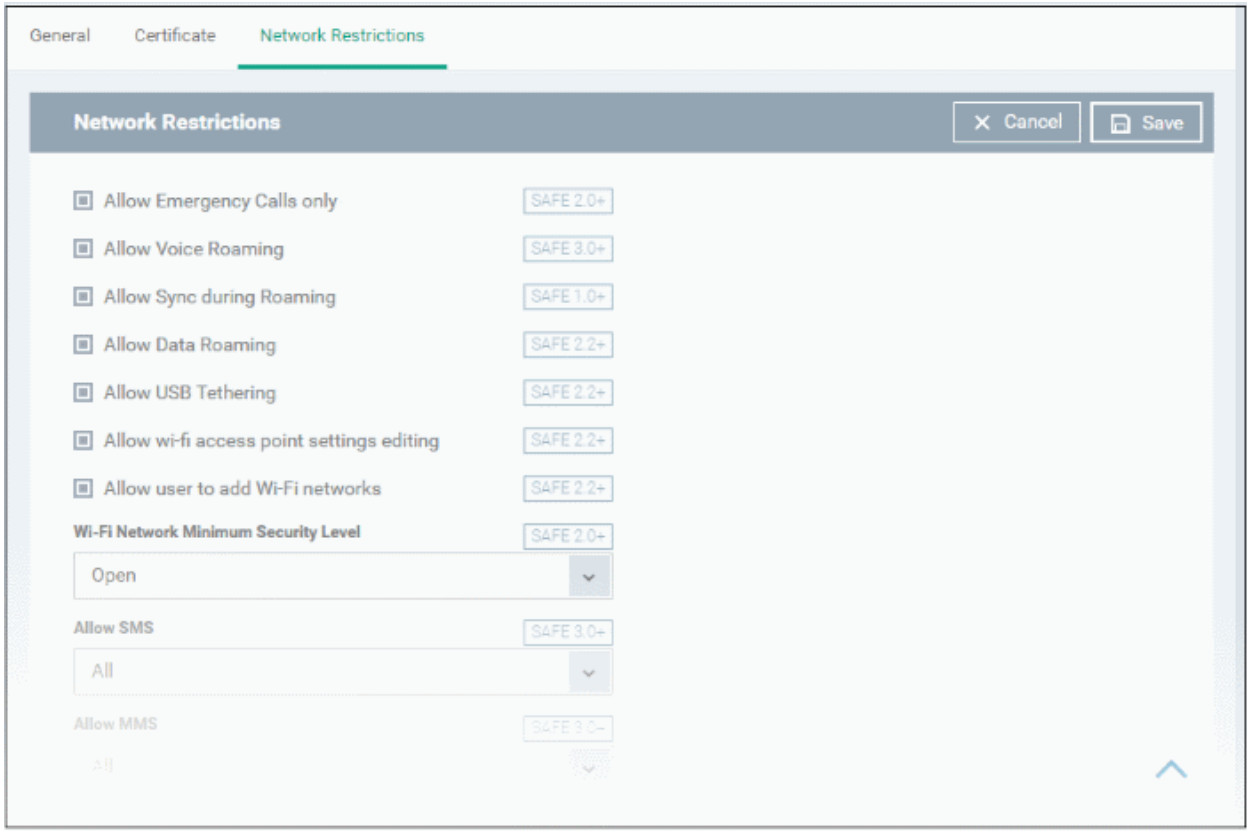
The settings will be saved and displayed under the 'Native App Restriction' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Network Restriction settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Network Restrictions' from the 'Add Profile Section' drop-down

The 'Network Restrictions' settings screen will be displayed.



Network Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Emergency Calls only	Checkbox	Allows users to make only emergency calls.
Allow Voice Roaming	Checkbox	Allows users to make/receive voice call during roaming.
Allow Sync during Roaming	Checkbox	Allows the use of Sync feature while roaming.
Allow Data Roaming	Checkbox	Allows users to enable 'Data Roaming' option on their devices to access data services during roaming.
Allow USB Tethering	Checkbox	Allows users to enable 'USB Tethering' option for sharing their data connection through USB tethering.
Allow Wi-Fi access point settings editing	Checkbox	Allows users to edit the Wi-Fi access point settings to create a Wi-Fi hotspot for sharing their data connection.
Allow user to add Wi-Fi networks	Checkbox	Allows users to add additional Wi-Fi networks.
Wi-Fi Network Minimum Security Level	Drop-down	Select the minimum security level required for the user to access the Wi-Fi network. The options available are: • Open • WEP • WPA • 802.1x EAP (LEAP) • 802.1x EAP (FAST) • 802.1x EAP (PEAP) • 802.1x EAP (TTLS) • 802.1x EAP (TLS)
Allow SMS	Drop-down	Allows text messages as per the option selected: • All - Allows both incoming and outgoing text messages. • Incoming Only - Allows incoming text messages only. • Outgoing Only - Allows outgoing text messages only. • None - Both incoming and outgoing text messages are blocked.
Allow MMS	Drop-down	Allows multimedia messages as per the option selected: • All - Allows both incoming and outgoing multimedia messages. • Incoming Only - Allows incoming multimedia messages only. • Outgoing Only - Allows outgoing multimedia messages only. • None - Both incoming and outgoing multimedia messages are blocked.
Blacklisted SSIDs	Text Field	Specify the name (SSID) of the wireless network that should be blacklisted. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

Network Restrictions Settings - Table of Parameters		
		Click the + button to add more 'Blacklisted SSID' fields. To remove a Blacklisted SSID field from the screen, click the minus button beside it.

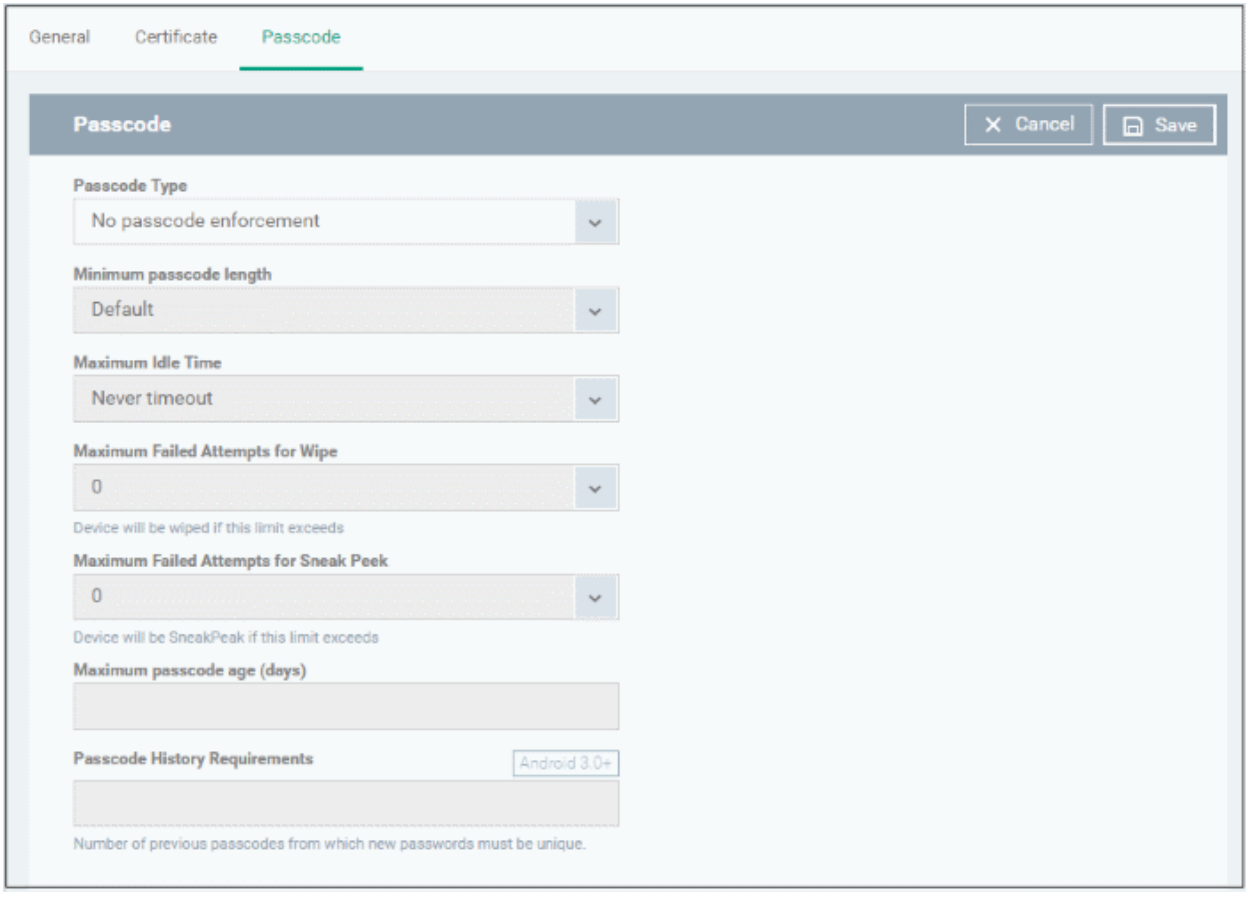
- Click the 'Save' button.

The settings will be saved and displayed under the 'Network Restrictions' tab. You can edit the settings or remove the section from the profile at anytime Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Passcode settings

- Click 'Passcode' from the 'Add Profile Section' drop-down

The Passcode settings screens will be displayed.



Passcode Settings - Table of Parameters		
Form Element	**Type**	**Description**
Passcode Type	Drop-down	Select the type of passcode from the drop-down that the user should configure for unlocking screen lock. The options available are: • No passcode enforcement • Only letters • Letters and numbers • Only numbers

Passcode Settings - Table of Parameters		
Form Element	**Type**	**Description**
		• Letters, numbers and a special symbol • Requires some kind of password
Minimum Passcode Length	Drop-down	Select the minimum number of passcode characters that can be configured by the user. (4-16 characters).
Maximum Idle Time	Drop-down	Select the maximum time period that can be set as idle time out period for device screen lock, from the drop-down.
Maximum Failed Attempts for Wipe	Drop-down	Select the maximum number of allowed unsuccessful login attempts for device wipe (4-16). Set the value as '0' for unlimited. If the number of failed attempts crosses this value, the data in the device will be automatically wiped off. This is useful to prevent the data from the device being stolen, if somebody, other than the user, tries to login to the device by entering guessed passcodes.
Maximum Failed Attempts for Sneak Peak	Drop-down	Select the maximum number of allowed unsuccessful login attempts for 'Sneak Peak' feature (4-16). Set the value as '0' for unlimited. The 'Sneak Peak' feature makes the device take a photograph with the front-facing camera if the wrong passcode is entered a certain number of times - hopefully getting a picture of the person holding a lost/stolen device. Photographs are forwarded to the ITSM server. The photograph(s) sent by the device can be viewed from the 'Device Details' interface that can be accessed by clicking 'Devices' > 'Device List' > the device name > 'Sneak Peak' tab. Refer to the section Viewing Sneak Peak Pictures to Locate Lost Devices for more details. Note: If the device does not have a front camera, the rear camera will capture a photograph and forward to the ITSM server.
Maximum Passcode Age (days)	Text Field	Enter the maximum period in days for which a passcode can be valid. After the number of days specified in this field, the passcode will expire. The user needs to change the passcode before the current one expires.
Passcode History Requirements	Text Field	Set how many unique, new passcodes must be created before the user can re-use an old password. This feature is available for Android 3.0 and later versions only.

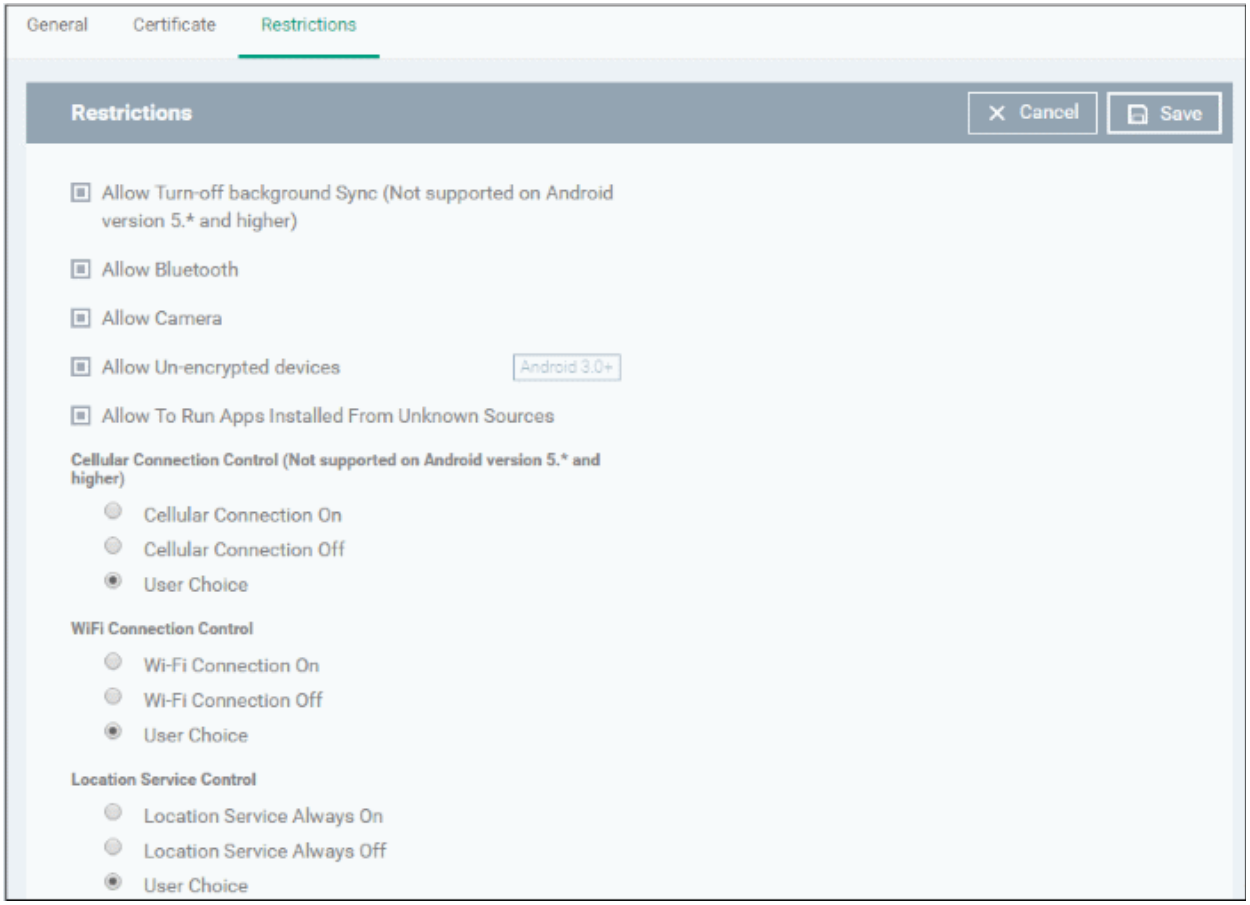
- Click the 'Save' button.

The settings will be saved and displayed under the 'Passcode' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Restriction settings

- Click 'Restrictions' from the 'Add Profile Section' drop-down

The 'Restrictions' settings screen will be displayed.



Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Turn-off background Sync	Checkbox	Select this to allow users to disable background synchronization setting on their devices.
Allow Bluetooth	Checkbox	Select this to allow users to enable/disable Bluetooth on their devices.
Allow Camera	Checkbox	Select this to allow users to use the camera
Allow Un-encrypted devices	Checkbox	Select this to enable users to use device without turning on the storage encryption feature. This feature is available for Android 3.0 and later versions only.
Allow to run Apps installed from unknown sources	Checkbox	Select this to allow users to run installed applications that were download from unknown sources
Cellular Connection Control	Radio Buttons	Choose whether or not to allow the device to connect to the internet through a cellular network (2G/3G/4G): • Cellular Connection on - Maintains the data connection through cellular network enabled, irrespective of user settings under 'Settings' > 'Wireless and Network settings' in the device. • Cellular Connection off - Maintains the data connection through cellular network disabled, irrespective of user settings under 'Settings' > 'Wireless and Network settings' in the device. • User Choice - The connection is enabled or disabled as per the user's setting under 'Settings' > 'Wireless and Network settings'

Restrictions Settings - Table of Parameters		
		in the device.
WiFi Connection Control	Radio Buttons	Choose whether or not to allow the device to connect to WiFi networks and hotspots from the options. • WiFi Connection on - Always maintains the WiFi connection enabled, irrespective of user's setting under 'Settings' > 'Wireless and Network settings' in the device. • WiFi Connection off - Always maintains the WiFi connection disabled, irrespective of user's setting under 'Settings' > 'Wireless and Network settings' in the device. • User Choice - The connection is enabled or disabled as per the user's setting under 'Settings' > 'Wireless and Network settings' in the device.
Location Service Control	Radio Buttons	Choose whether or not to allow the location services on the device from the options: • Location Service Always On - Always maintains the location services enabled, irrespective of the user's setting on the device. • Location Service Always Off - Always maintains the location services disabled, irrespective of the user's setting on the device. • User Choice - The location service is enabled or disabled as per the user's setting on the device.

- Click the 'Save' button.

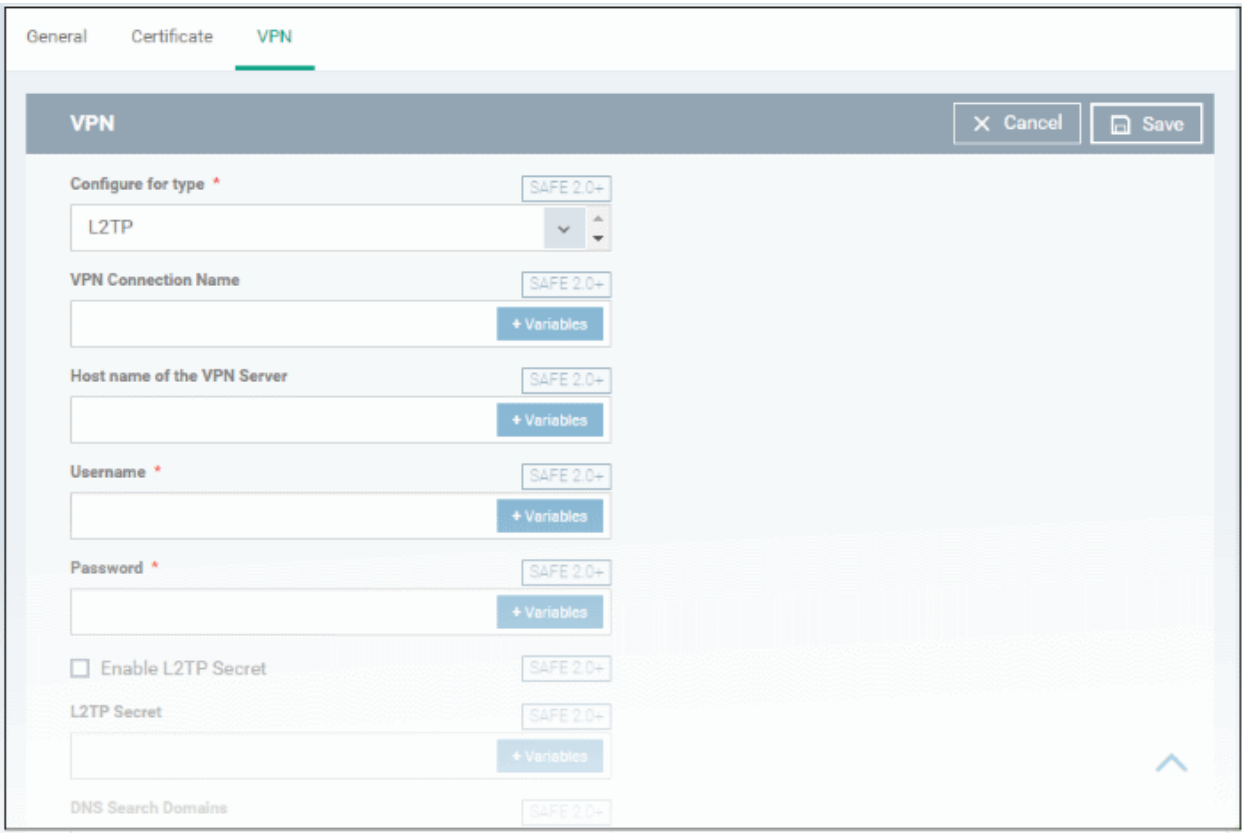
The settings will be saved and displayed under the 'Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure VPN settings

Note: The feature is supported for only Samsung for Enterprise (SAFE) devices.

- Click 'VPN' from the 'Add Profile Section' drop-down

The settings screen for VPN will be displayed.



VPN Settings - Table of Parameters		
Form Element	**Type**	**Description**
Configure for type	Drop-down	Choose the VPN connection type from drop-down. The options available are: L2TP, PPTP, L2TP/IPSec PSK, IPSec, XAuth PSK and IPSec XAuth RSA.
VPN Connection Name	Text Field	Enter the name of the connection, which will be displayed on the device. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**.
Host name of the VPN Server	Text Field	Enter the IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**.
Username	Text Field	For a single user account for VPN connection, enter the username for connection to the network. For several users, click the 'Variables' button , + Variables select the variable for fetching the VPN username from the 'Variables list' and click ' + . The usernames of the users to whom the profile is associated will be automatically included in the profile while rolling out the profile to respective devices. For more details on variables, refer to the section **Configuring Custom Variables**.

VPN Settings - Table of Parameters		
Password	Text Field	If the profile is for a single user account for VPN connection, enter the password for the account. If the profile is for several users, click the 'Variables' button + Variables, select the variable created to fetch the password of the user from the 'User Variables' list and click +. The VPN connection passwords for the accounts of the users to whom the profile is associated will be automatically added to the profile while rolling out to respective devices. For more details on variables, refer to the section Configuring Custom Variables.
DNS Search Domains	Text Field	Enter the IP address or hostname of the DNS server that devices will use for searching domain names. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
If L2TP is selected:		
• Enable L2TP Secret	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
• L2TP Secret	Text Field	If L2TP Secret is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables'
If PPTP is selected:		
• Enable Encryption	Checkbox	If selected, the connection is encrypted between the devices and the VPN server.
If L2TP/IPSec PSK is selected:		
• Enable L2TP Secret	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
• L2TP Secret	Text Field	If L2TP Secret is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables'
• IPSec Pre-Shared Key	Text Field	If IP Sec Identifier is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables'
If IPSec Xauth PSK is selected:		
• IP Sec Identifier	Text Field	Enter the IPSec identifier in the field. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
• IPSec Pre-Shared Key	Text Field	If IP Sec Identifier is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables'

VPN Settings - Table of Parameters		
Use for persistent connect	Checkbox	Forcibly maintains the VPN connection always at the enabled state, irrespective of user's settings through 'Settings' > 'Wireless and Networks' in the device. In order to enable this feature, the following conditions are to be satisfied: • The profile should have been created already and rolled out to the devices. Hence the administrator will be able to enable this feature after rolling out the profile and then by editing the profile. Refer to the section Editing Configuration Profiles. • Suits to all VPN connections types, except PPTP • The VPN server and the DNS server should have been specified by their IP addresses in IPv4.

- Click the 'Save' button after entering or selecting the parameters.

The VPN settings will be added to the profile.

You can add multiple VPN connection settings for the profile.

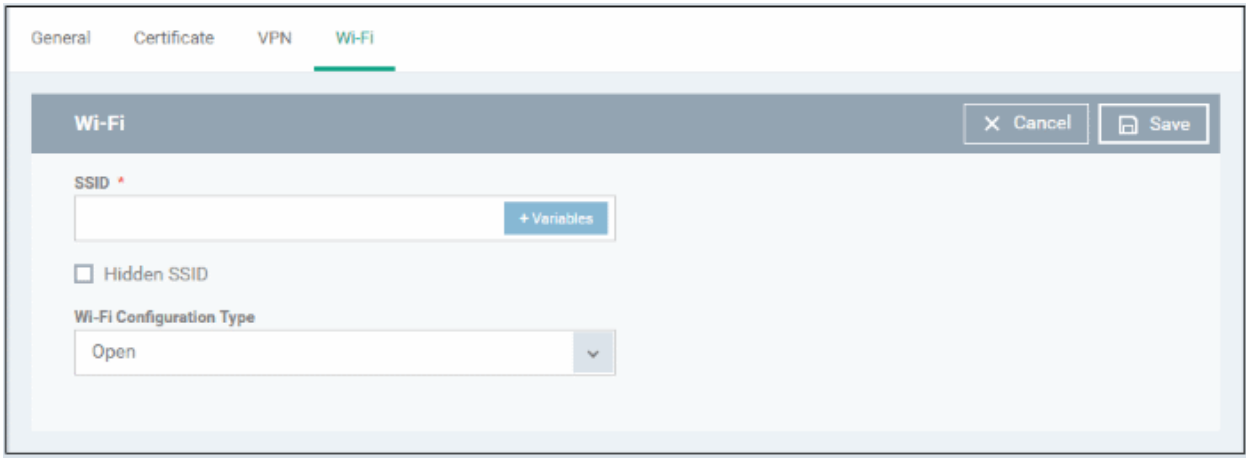
- To add another VPN connection, click 'Add VPN' and repeat the process
- To view and edit the VPN settings of a connection, click the name of the connection
- To remove a VPN connection, select VPN then click 'Delete VPN'

You can add any number of VPN connection settings to the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Profile Section' drop-down

The settings screen for Wi-Fi will be displayed.



Wi-Fi Settings - Table of Parameters		
Form Element	**Type**	**Description**
SSID	Text Field	Enter the Service Set Identifier (SSID), the name of the wireless network that a device should connect to. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Hidden SSID	Checkbox	If enabled, users will be able to access the hidden wireless network too. Users must know the hidden SSID details and the required credentials.
Wi-Fi Configuration Type	Drop-down	Select the type of encryption used by the wireless network from the drop-down. The options available are: • Open • WEP • WPA / WPA2 - PSK • 802.1x EAP The settings for each type is explained in the next table Wi-Fi configuration type settings.

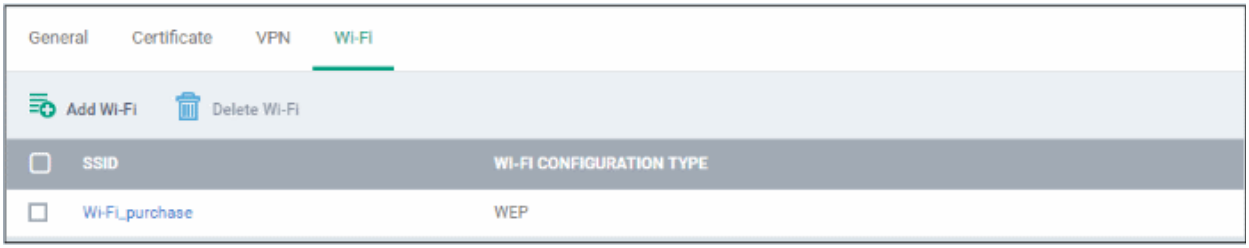
Wi-Fi Configuration Type settings

Wi-Fi Configuration Type Settings - Table of Parameters	
Security Configuration Type	**Description**
Open	No password is required for accessing the Wi-Fi network by the user.
WEP	Authentication Password - Enter the password to access the Wi-Fi network. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
WPA / WPA2 - PSK	Authentication Password - Enter the password to access the Wi-Fi network. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
802.1x EAP	**1. EAP Authentication Protocol** - Select the EAP authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version. • PEAP • TLS • TTLS **2. Phase 2 Authentication Protocol** - Select the Phase 2 authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.

Wi-Fi Configuration Type Settings - Table of Parameters	
	• None • PAP • MSCHAP • MSCHAPV2 • GTC **3. Certificate -** Select the user certificate from the drop-down or upload it using the 'Add New' button. 4. **CA Certificate** - Select the CA certificate from the drop-down or upload it using the 'Add New' button. 5. **Authentication Username** - Enter the username for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version. 6. **Authentiation Password** - Enter the password for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version. 7. **Authentication Domain** - Enter the details for RADIUS Server authentication. pplicable for Samsung for Enterprise devices SAFE 1.0 + version. 8. **Anonymous Identity** - Enter the username that can be used for anonymous access. Applicable for Samsung for Enterprise devices SAFE 1.0 + version. 9. **Encryption Key** - Enter the encryption key to access the Wi-Fi network. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. For items in the list from 5 to 8, you can also include a variable to the field by clicking the 'Variables' button + Variables and clicking + beside the variable from the list. For more details on variables, refer to the section Configuring Custom Variables.

- Click the 'Save' button after entering or selecting the parameters.

The 'Wi-Fi' network settings' will be saved for the profile.



You can add multiple Wi-Fi networks for a profile.

- To add another Wi-Fi SSID, click 'Add Wi-Fi' and repeat the process
- To view and edit the Wi-Fi network settings, click the SSID of the network
- To remove a Wi-Fi network, select it from the list and click 'Delete Wi-Fi'

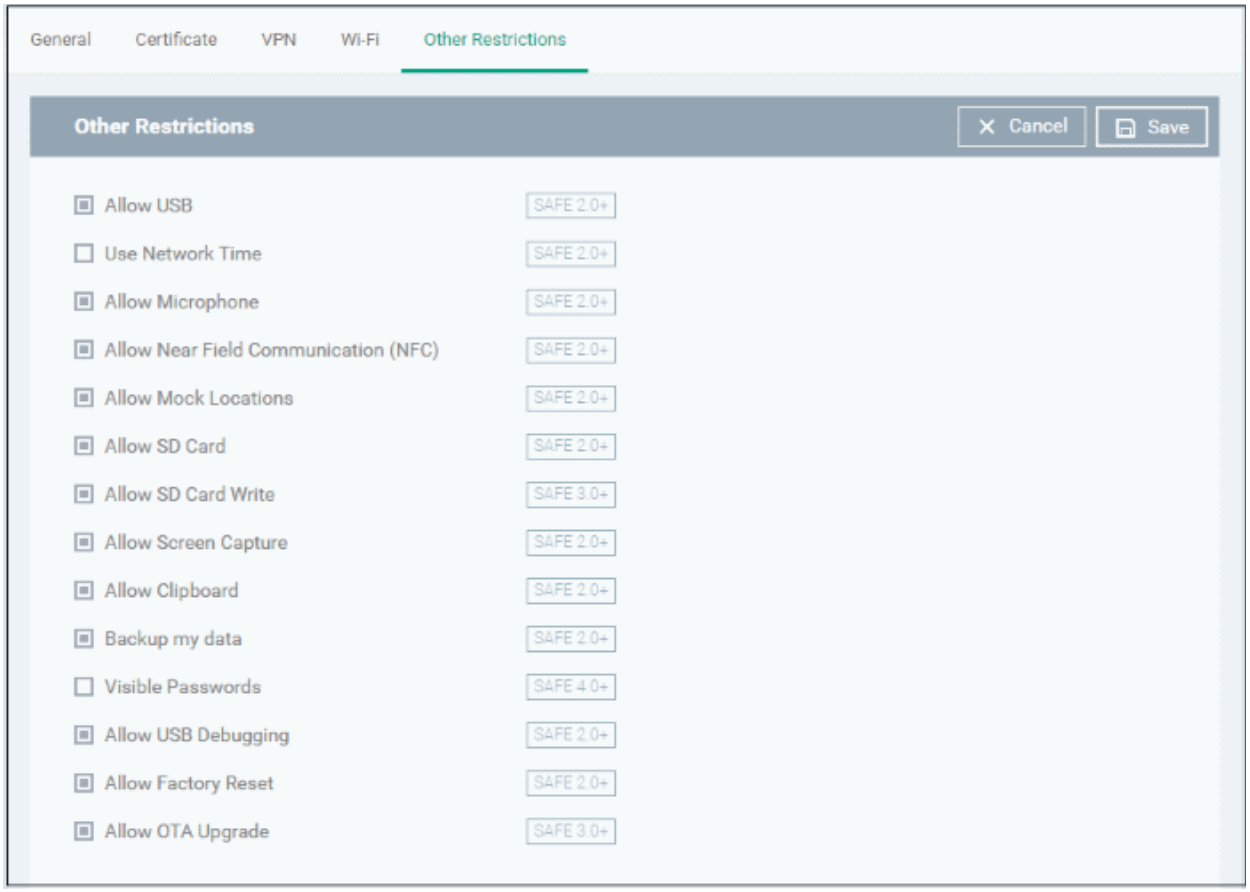
You can add or remove Wi-Fi networks at any time. Refer to the section 'Editing Configuration Profiles' for more details.

To configure 'Other Restrictions' settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Other Restrictions' from the 'Add Profile Section' drop-down

The 'Other Restrictions' settings screen will be displayed.



Other Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow USB	Checkbox	Allows users to establish connections via USB ports.
Use Network Time	Checkbox	Allows users to enable/disable network provided values in Date & Time settings.
Allow Microphone	Checkbox	Allows users to use microphone. If this is disabled, users can use microphone for receiving and making calls only.
Allow Near Field Communication (NFC)	Checkbox	Allows devices to establish connection via NFC
Allow Mock Locations	Checkbox	Allows users to enable/disable 'Mock Location' in developer mode settings.
Allow SD Card	Checkbox	Users can use SD card on their devices.
Allow SD Card Write	Checkbox	Users can store data on the SD card.

Other Restrictions Settings - Table of Parameters		
Allow Screen Capture	Checkbox	Users can take screenshot of the device screen.
Allow Clipboard	Checkbox	Users will be allowed to use clipboard memory.
Backup my data	Checkbox	Users will be allowed to take a backup of data in their devices.
Visible Passwords	Checkbox	Allows users to enable/disable show password feature.
Allow USB Debugging	Checkbox	Allows users to enable/disable 'USB Debugging' option in developer mode settings.
Allow Factory Reset	Checkbox	Allows users to reset the device to factory settings.
Allow OTA Upgrade	Checkbox	Allows devices to receive Over-the-air (OTA) upgrade for software updates.

- Click the 'Save' button.

The settings will be saved and displayed under 'Other Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.2. Profiles for iOS Devices

iOS Profiles allow you to specify a device's network access rights, restrictions and other general settings.

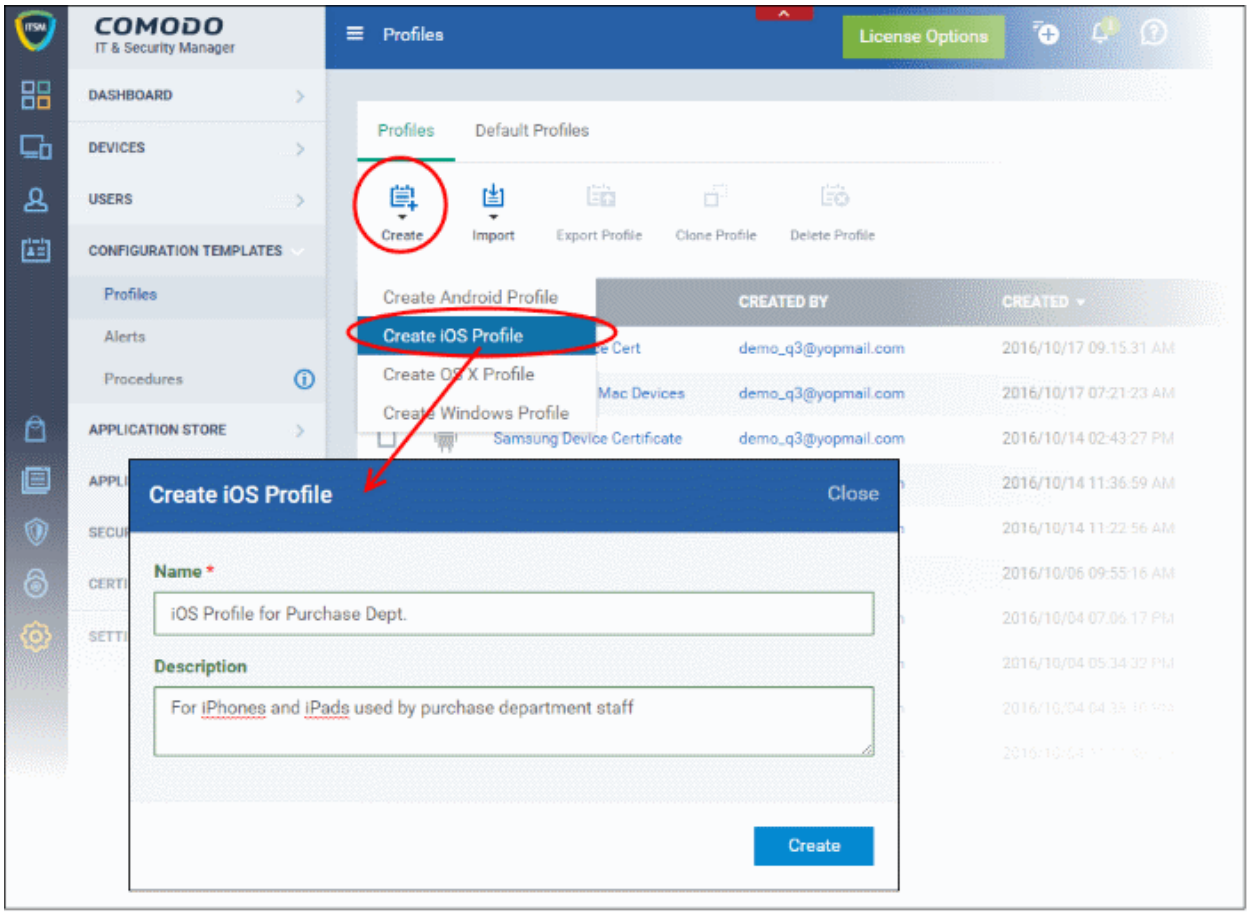
To create an iOS profile

- Click 'Configuration Templates' from the left then choose 'Profiles'
- Click 'Create' then select 'Create iOS Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profiles'.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Profile Section' button. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices, device groups, users and user groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.

To create an iOS profile

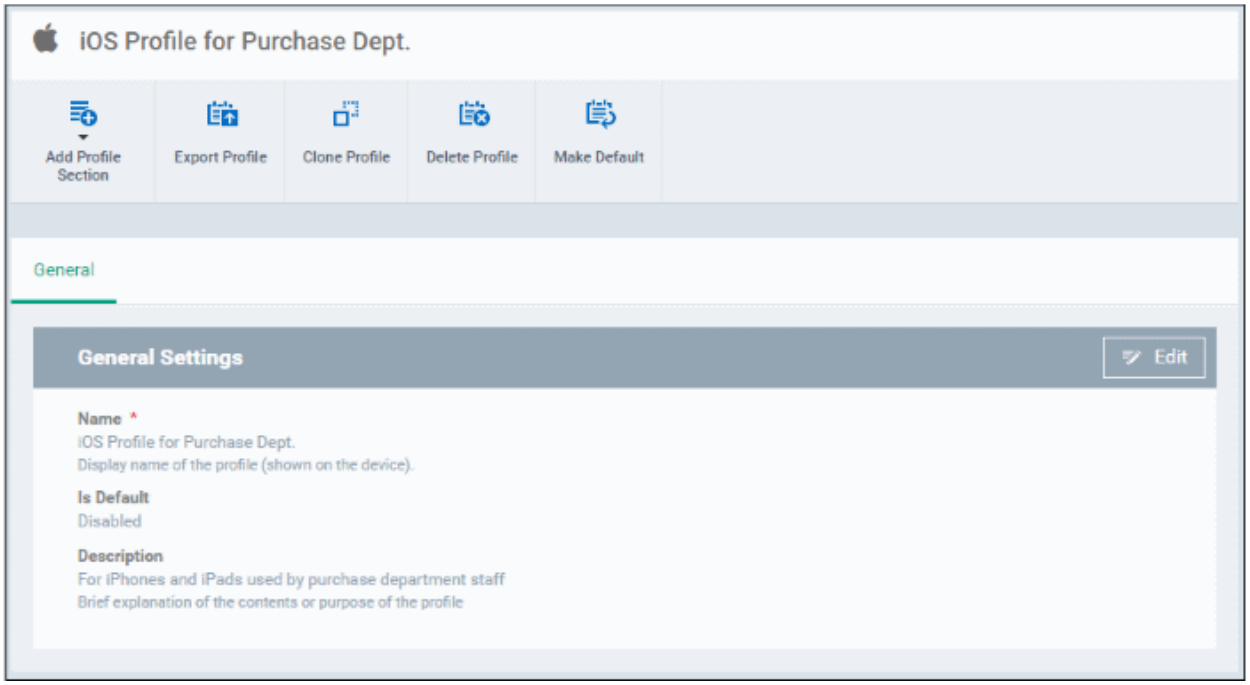
- Open the 'Profiles' interface by clicking 'Configuration Templates' from the left and choosing 'Profiles'
- Click the 'Create' button above the table under 'Profiles' and and choose 'Create iOS Profile' from the options



The 'Create iOS Profile' screen will be displayed.

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

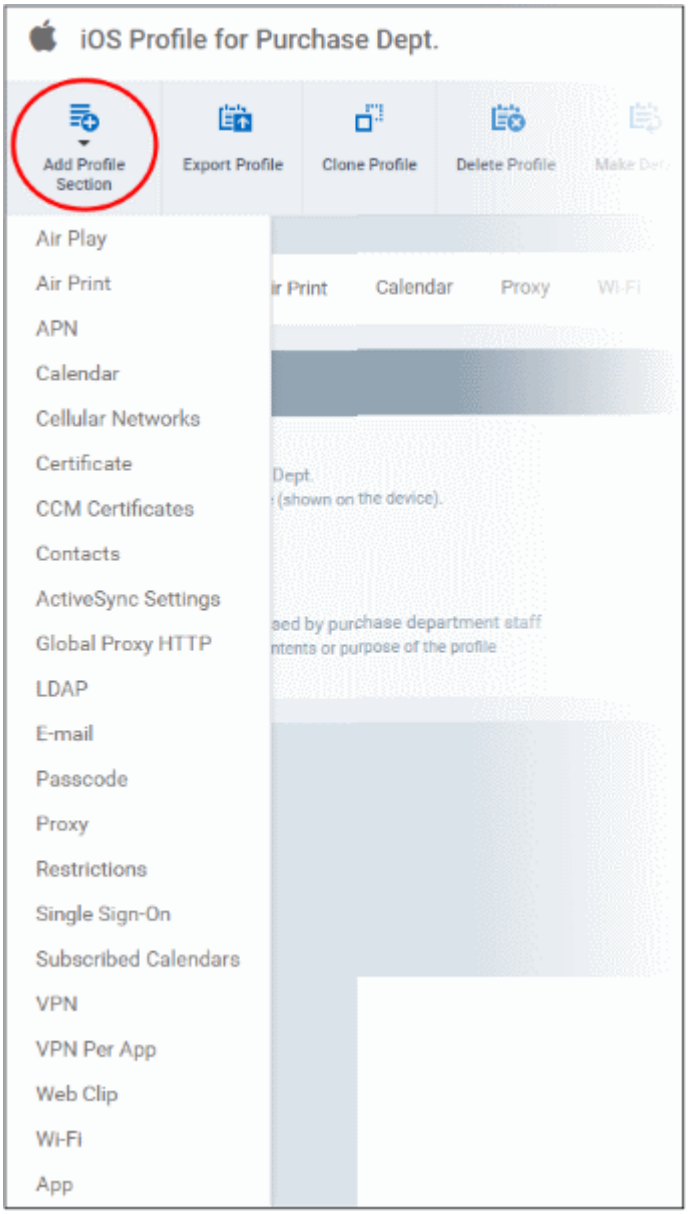
The iOS profile will be created and the 'General Settings' section will be displayed. The new profile is not a 'Default Profile' by default.



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

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

- Click the 'Add Profile Section' button and select components from the list that you want to include in the profile

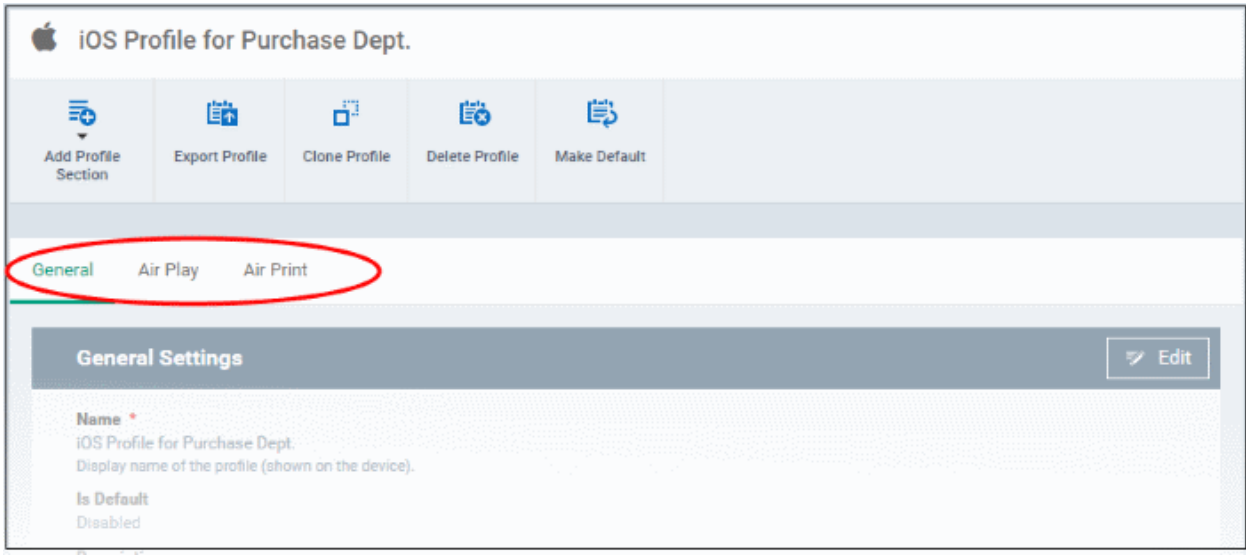


Note: Many iOS profile settings have small information boxes next to them which indicate the iOS version required for the setting to work correctly.

For example, the following box indicates that the setting supports Apple devices with iOS version 7 and above only:

iOS 7+

The settings screen for the selected component will be displayed. After configuring the component and saving the settings, it will be available as a tab at the top.



Following sections explain more about each of the settings:

- Air Play
- Air Print
- APN
- Calendar
- Cellular Networks
- Certificate
- CCM Certificates
- Contacts
- Active Sync
- Global Proxy HTTP
- LDAP
- E-Mail
- Passcode
- Proxy
- Restrictions
- Single Sign-On
- Subscribed Calendars
- VPN
- VPN Per App
- Web Clip
- Wi-Fi
- App Lock

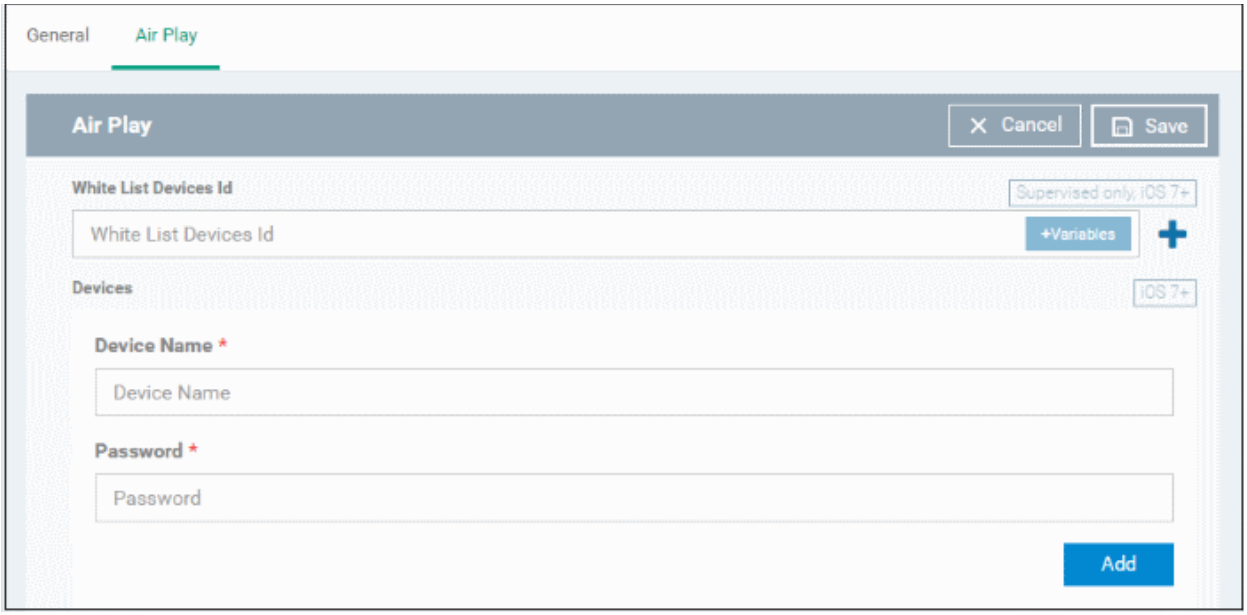
To configure AirPlay settings

These settings allow you to whitelist devices (televisions, stereo systems etc) which can be used to play content from managed iOS devices via Apple's Airplay system.

Note: If you do not create a whitelist then managed mobile devices will be able to broadcast to any Airplay capable device.

- Click 'Air Play' from the 'Add Profile Section' drop-down

The 'Air Play' settings screen will be displayed.



AirPlay Settings Configuration - Table of Parameters		
Form Element	**Type**	**Description**
White List Devices ID	Text Field	Enter the ID of the output device that you want to whitelist for Airplay. The ID numbers of the devices should be entered in the format as given below: XX:XX:XX:XX:XX:XX Note: The whitelist is applicable for supervised iOS 7+ devices and will not apply for all other devices. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Click + button to add more 'Device ID' fields. To remove an AirPlay destination device, click the − button beside it.
Device Name	Text Field	Enter the name of the AirPlay output device that you entered above. You can also add a variable to the field by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Click the 'Add' button to add more 'Device name' and 'Password' fields. To remove an AirPlay device, click the ✖ button beside it.
Password	Text Field	Enter the password for the AirPlay destination that you entered above.
Add	Button	Click this button to add another 'Devices' section.

- Click the 'Save' button.

The 'Air Play' device will be added to the list.

You can add multiple Air Play devices for the profile.

- To add more devices, click 'Add Air Play' at the top and repeat the process.
- To view and edit the settings for a device, click on its name
- To remove an Air Play device, select it and click 'Delete Air Play'

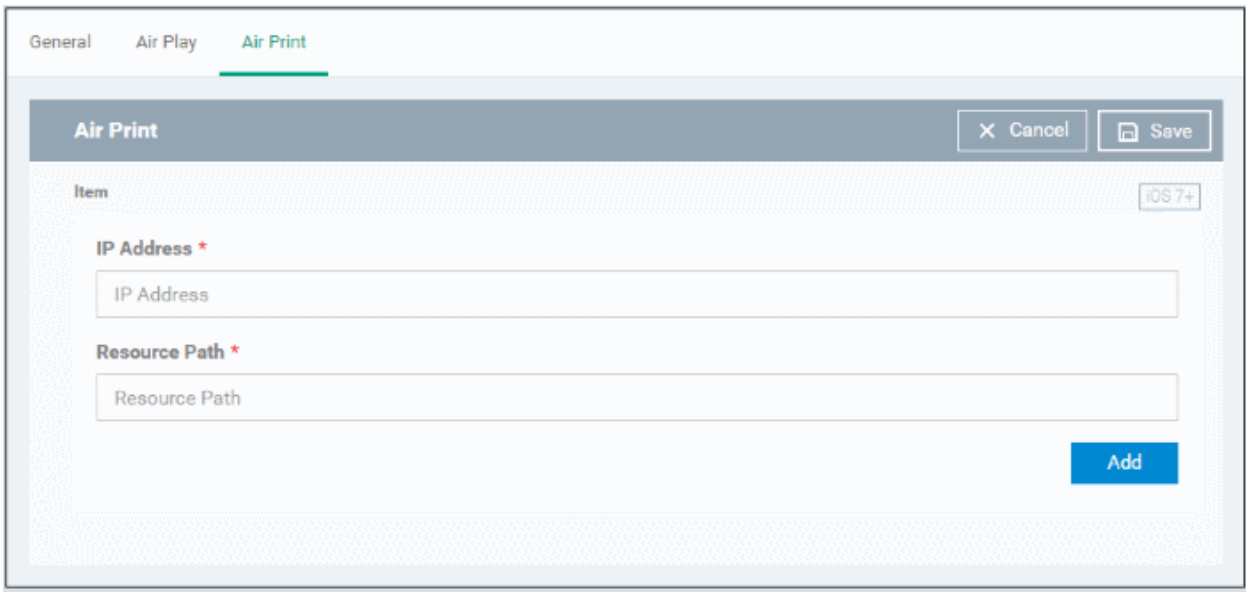
The settings will be saved and displayed under 'Air Play' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure AirPrint settings

These settings allow you to specify the default AirPrint printer to be used by devices on this profile.

- Click 'Air Print' from the 'Add Profile Section' drop-down

The 'Air Print' settings screen will be displayed.



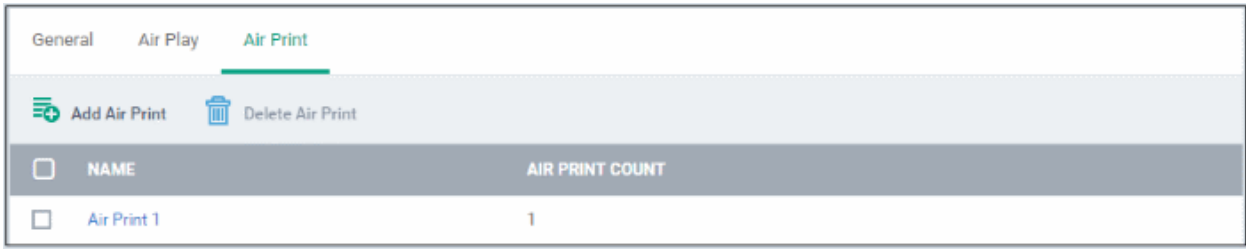
AirPrint Settings - Table of Parameters		
Form Element	**Type**	**Description**
IP Address	Text Field	Enter the device ID of the AirPrint printer you wish to use. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**.
Resource Path	Text Field	Enter the resource path of the printer, for example, printers/ HP_LaserJetPro_M1136_series. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the

AirPrint Settings - Table of Parameters		
		variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Add	Button	Click this button to add another AirPrint section.

You can add more printers by repeating the process. To remove a printer, click the 'X' button beside the printer.

- Click the 'Save' button.

The printer will be added to the list.



- To add another printer, click 'Add Air Print' and repeat the process
- To view and edit the settings of a printer, click the name of the printer
- To remove a printer, select it and click 'Delete Air Print'

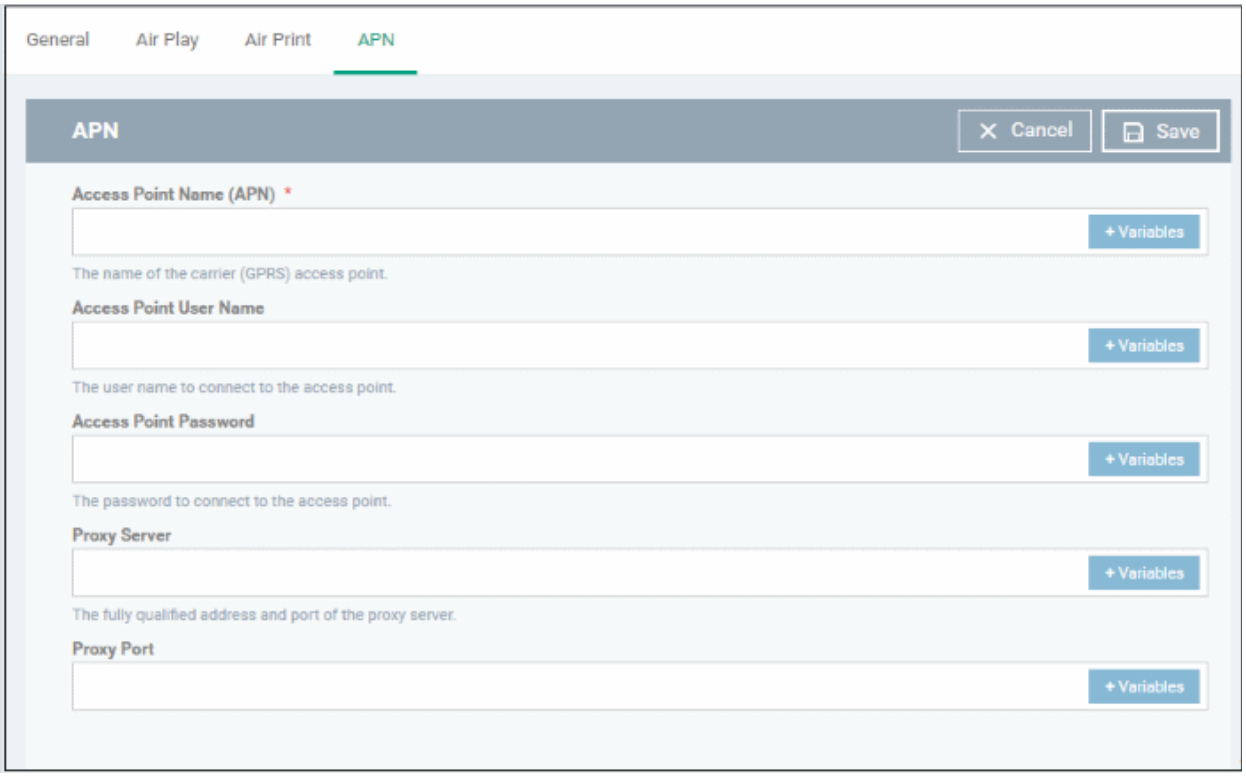
The settings will be saved and displayed under the 'Air Print' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure APN settings

Note: APN settings have been deprecated in favor of Cellular settings in iOS 7 and above.

- Click 'APN' from the 'Add Profile Section' drop-down

The 'APN' settings screen will be displayed.



APN Settings - Table of Parameters		
Form Element	**Type**	**Description**
Access Point Name (APN)*	Text Field	Enter the name of the GPRS access point provided by the carrier. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Access Point User Name	Text Field	Enter the username to connect to the access point. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Access Point Password	Text Field	The password to connect to the access point. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Proxy Server	Text Field	Enter the proxy host settings provided by the carrier. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Proxy Port	Text Field	Enter the port number of the proxy host provided by the carrier. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

Fields marked * are mandatory.

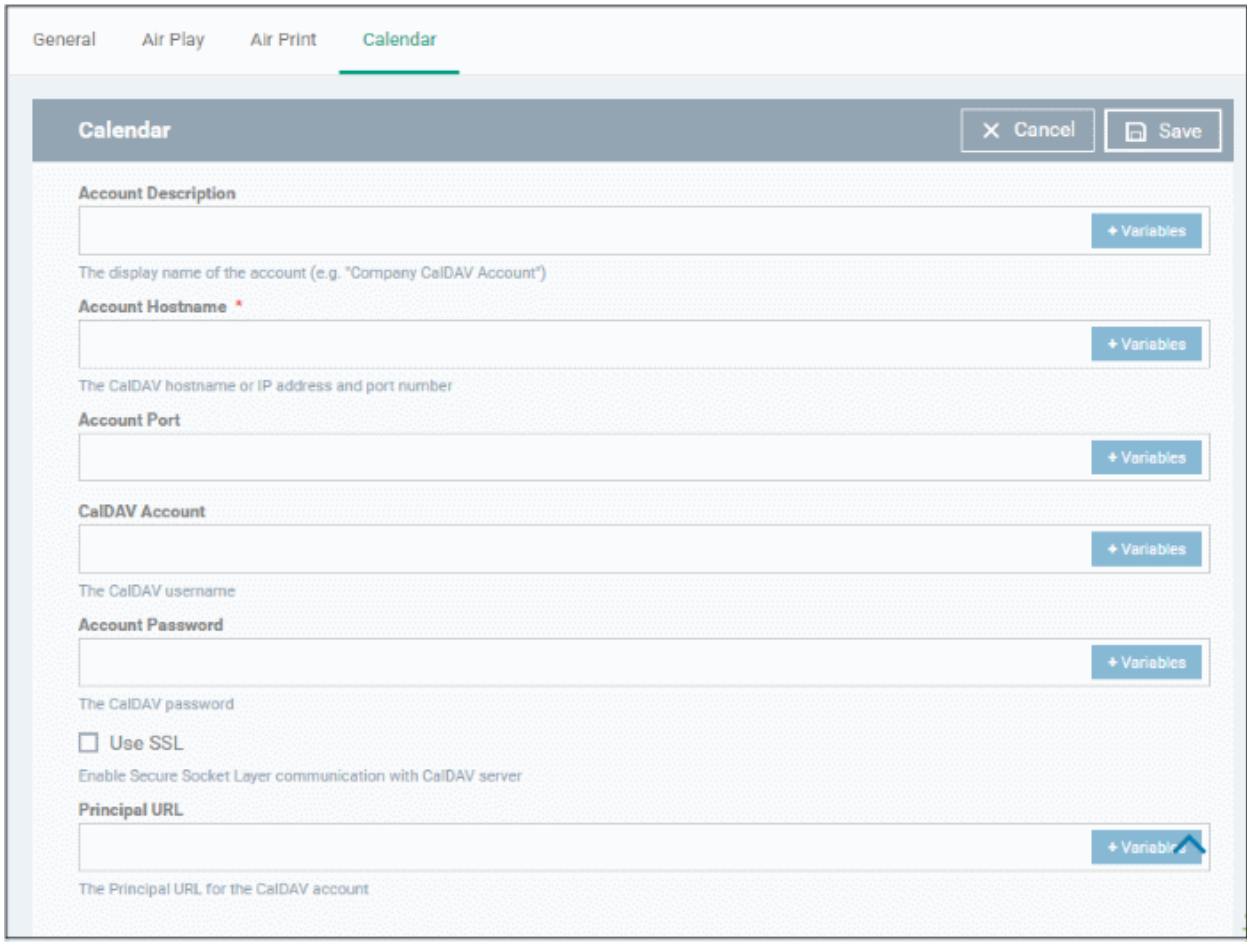
- Click the 'Save' button.

The settings will be saved and displayed under the 'APN' tab. You can edit these settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Calendar settings

- Click 'Calendar' from the 'Add Profile Section' drop-down

The 'Calendar' settings screen will be displayed.



Calendar Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Description	Text Field	Enter the display name of the CalDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Host Name*	Text Field	Enter the CalDav host name or IP address. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Port	Text Field	Enter the port number on which to connect to the server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables,

Calendar Settings - Table of Parameters		
		refer to the section Configuring Custom Variables.
CalDav Account	Text Field	The user name of the CalDav user. Click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Account Password	Text Field	The password for the CalDav account. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, the users can access the account without entering the credentials.
Use SSL	Checkbox	If enabled, SSL connection will be established with the CalDav server.
Principal URL	Text Field	Enter the Principal URL of the CalDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

Fields marked * are mandatory.

- Click the 'Save' button after entering or selecting the parameters.

The calendar account host will be added to the list.

- To add another Calendar server, click 'Add Calendar' and repeat the process
- To view and edit the calendar server settings, click on the hostname in the list
- To remove Calendar server, select it and click 'Delete Calendar'

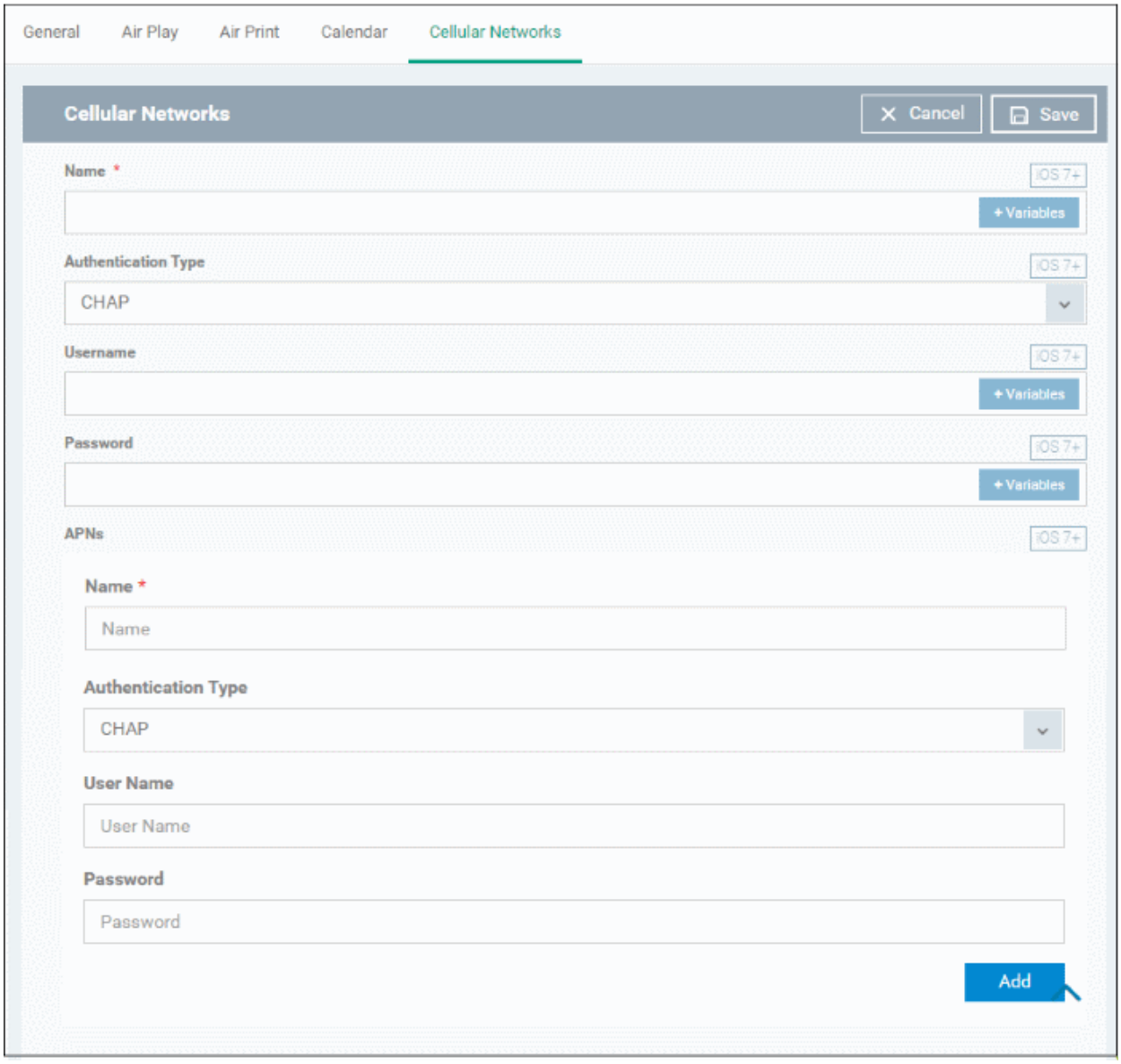
The settings will be saved and displayed under 'Calendar' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Cellular Network settings

Note: A cellular network setting cannot be applied if an APN setting is already installed. This feature is available for iOS 7 and later versions only.

- Click 'Cellular Networks' from the 'Add Profile Section' drop-down

The 'Cellular Networks' settings screen will be displayed.



Cellular Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name for this configuration, specifying the cellular service provider. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Authentication Type	Drop-down	Select the authentication type from the drop-down. The options are CHAP or PAP.
Username	Text Field	Enter the user name used for authentication. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Password	Text Field	Enter the password used for authentication. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the

Cellular Settings - Table of Parameters		
		variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
APNs Note: You can add more APN accounts for a single service provider by clicking the Add button at the bottom left.		
Name	Text Field	Enter a name for specifying the APN configuration. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Authentication Type	Drop-down	Select the authentication type from the drop-down. The options are CHAP or PAP.
User Name	Text Field	Enter the user name used for authentication. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Password	Text Field	Enter the password used for authentication. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

- Click the 'Save' button.

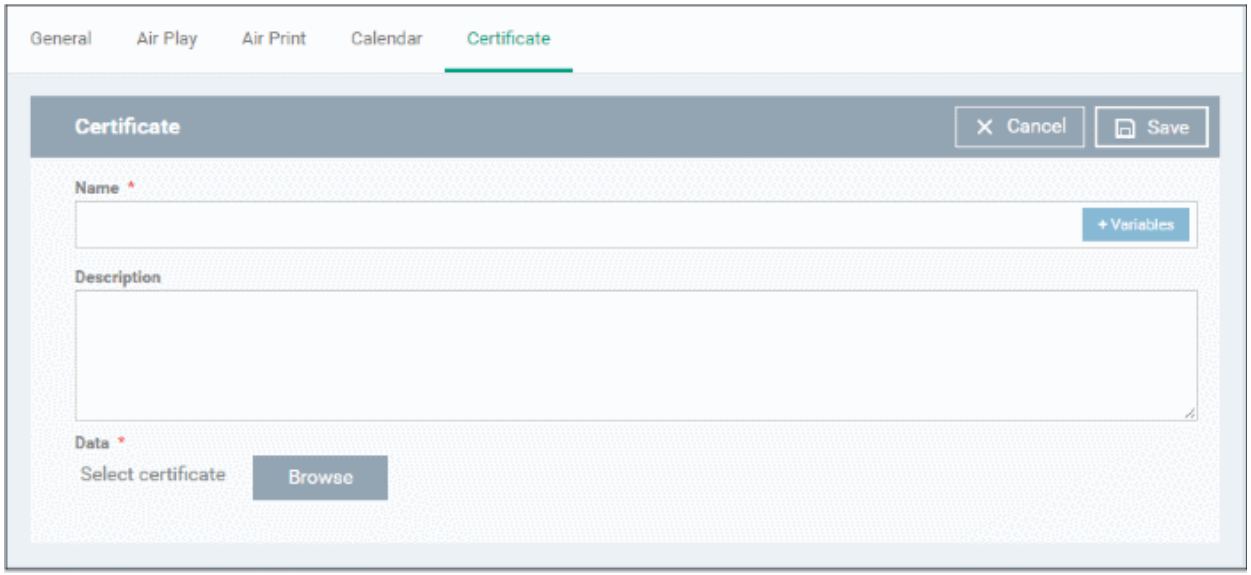
The settings will be saved and displayed under the 'Cellular Networks' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Certificate settings

Note: The 'Certificate Settings' section is used to upload certificates that can be selected for use in other settings such as 'Wi-Fi, 'Exchange Active Sync', 'VPN' and so on. You can also enroll user or device certificates from Comodo Certificate Manager (CCM) after activating your CCM account under Settings > Portal Set-Up > Certificates Activation.

- Click 'Certificate' from the 'Add Profile Section' drop-down

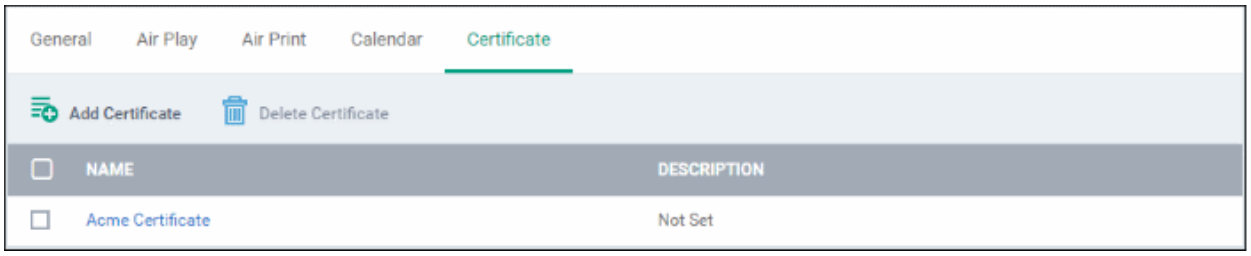
The 'Certificate' settings screen will be displayed.



Certificate Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name of the certificate. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Description	Text Field	Enter an appropriate description for the certificate.
Data	Browse button	Browse and upload the required certificate. Only certificate files with extensions 'pub', 'crt' or 'key' can be uploaded.

- Click the 'Save' button.

The certificate will be added to the certificate store.



- To add more certificates, click 'Add Certificate' and repeat the process.
- To view the certificate key and edit the name, click on the name of the certificate
- To remove an unwanted certificate, select it and click 'Delete Certificate'

You can add any number of certificates to the profile and remove certificates at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To add CCM Certificates

The Certificates Settings section of a profile allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Once the profile is applied to a device, a certificate request is automatically generated and forwarded to CCM. After issuance, the certificate will be sent to ITSM which in turn pushes it to the agent on the device for installation. You can add any number of certificates to a single profile. Appropriate certificate requests will be generated on each device to which the profile is applied.

In addition to user authentication, client certificates can be used for email signing and encryption.

Prerequisite: Your CCM account should have been integrated to your ITSM server in order for ITSM to forward requests to CCM. For more details, refer to the section **Integrating with Comodo Certificate Manager.**

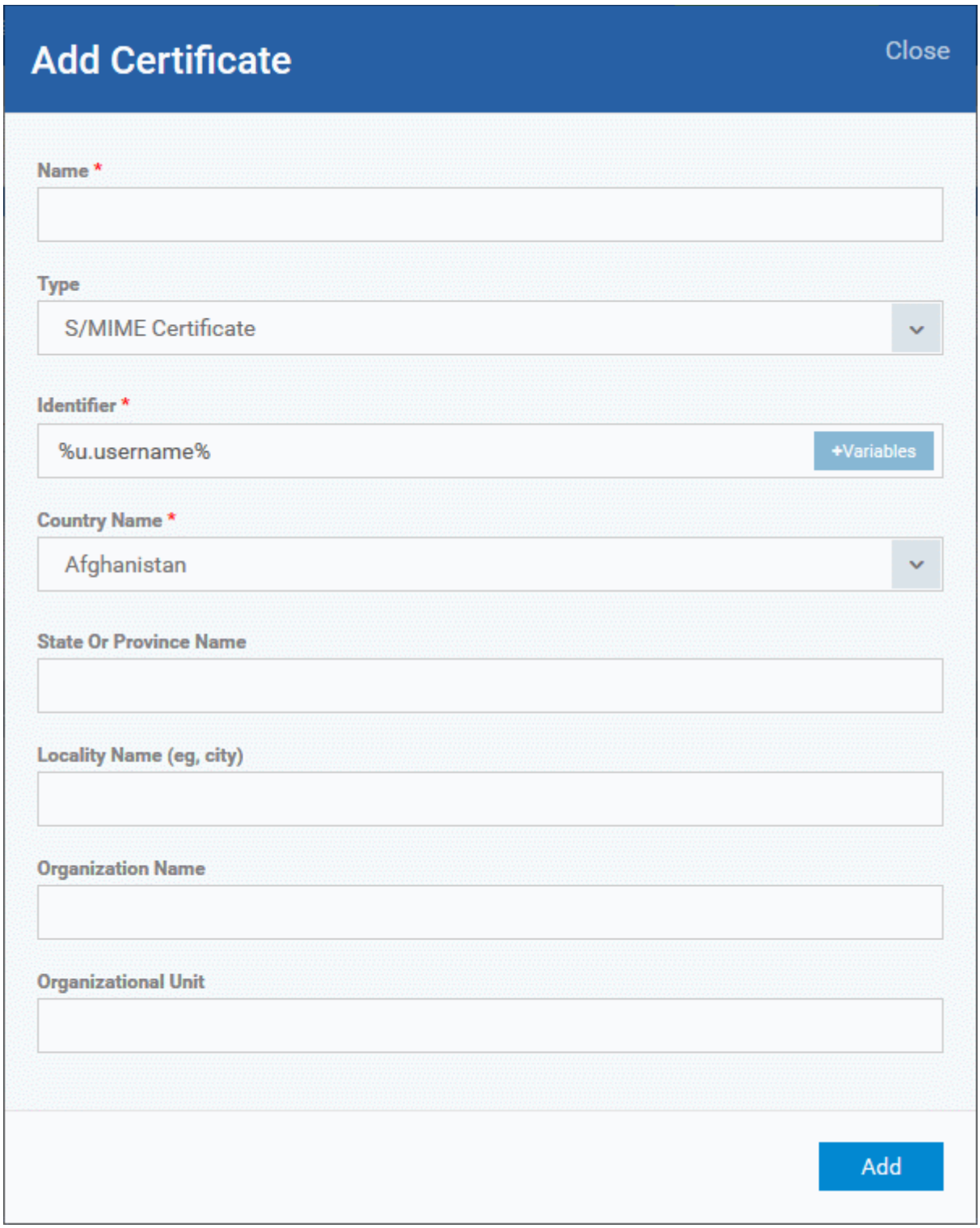
To configure CCM Certificate settings

- Choose 'Certificates' from the 'Add Profile Section' drop-down

The settings screen for adding certificate requests to the profile will be displayed.

- Click 'Add Certificate' at the top to add a certificate request to the profile

The 'Add Certificate' form will appear.



Add Certificate - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter a name for the certificate to be requested, shortly describing its purpose.
Type	Drop-down	Select the type of certificate to be added. The available options are: • S/MIME Certificate (Client Certificate) • Device Certificate

Add Certificate - Table of Parameters		
Identifier	Text Field	The Identifier field will be auto-populated with mandatory variables depending on the chosen certificate type. • For client certificate, %username% will be added for fetching the username to be included as subject in the certificate request. • For device certificate, %d.uuid% will be added for fetching the device name to be included as subject in the certificate request. You can add more variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Country Name	Text Field	Enter the address details of the user/organization in appropriate fields.
State or Province Name		
Locality Name (eg. City)		
Organization Name	Text Field	Enter the name of the organization to which the user/device pertains. **Prerequisite**: The organization should have been added to your CCM account.
Organizational Unit	Text Field	Enter the name of the department to which the user/device pertains. **Prerequisite**: The department should have been defined under the organization in your CCM account.

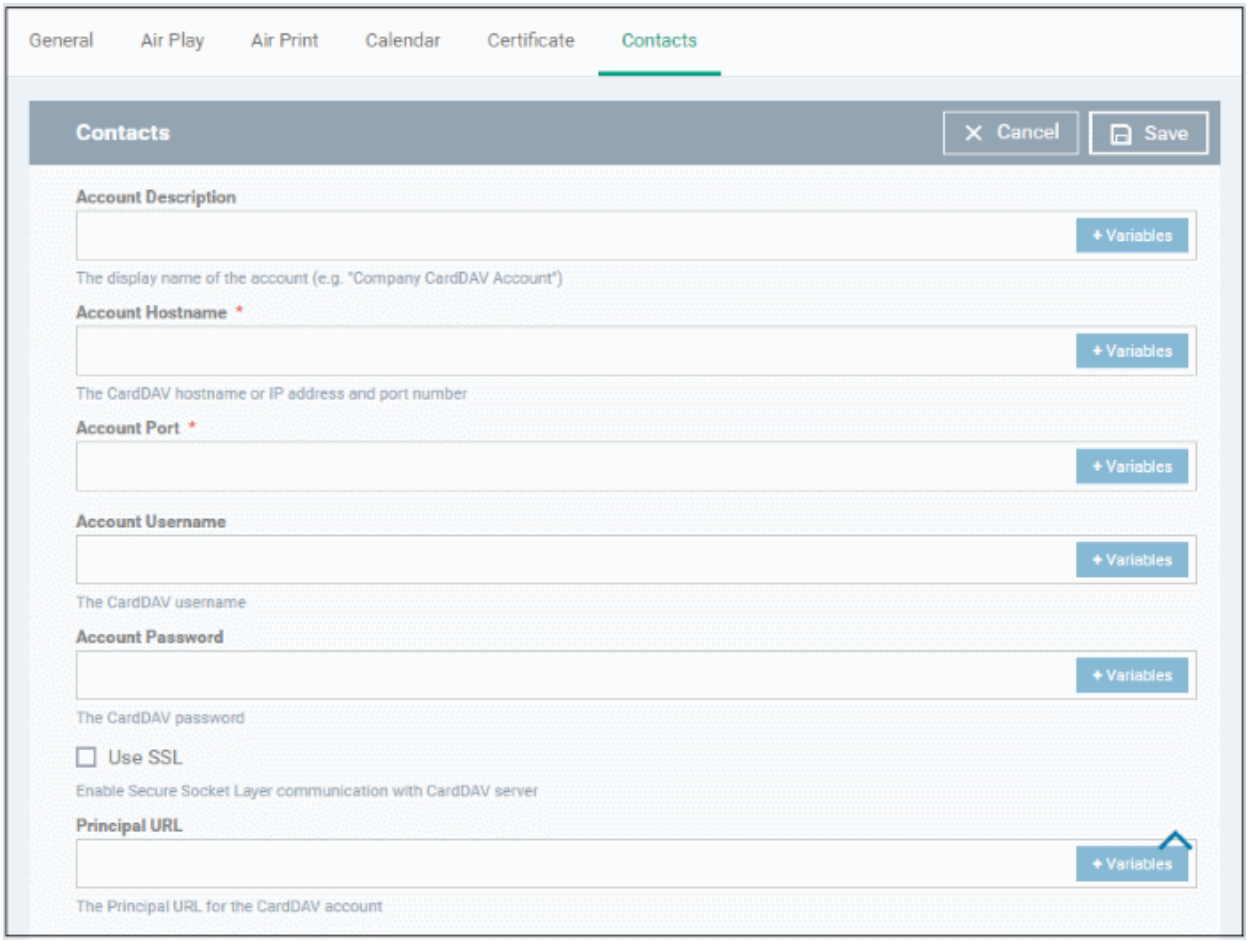
- Click 'Add' once you have completed the form.
- Repeat the process to add more certificate requests.

The certificate requests will be generated from the devices once the profile is applied to them.

To configure Contacts settings

- Click 'Contacts' from the 'Add Profile Section' drop-down

The 'Contacts' settings screen will be displayed.



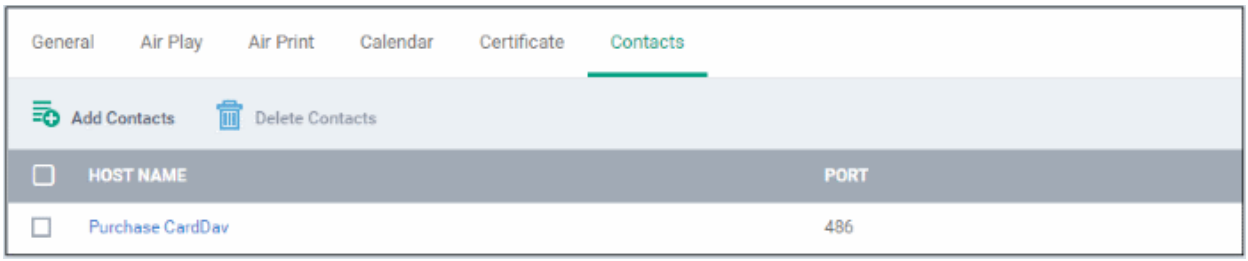
Contacts Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Description	Text Field	Enter the display name of the CardDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Host Name*	Text Field	Enter the CardDav host name or IP address. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Port*	Text Field	Enter the port number on which to connect to the server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Username	Text Field	The user name of the CardDav user. Click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.

Contacts Settings - Table of Parameters		
Account Password	Text Field	The password for the CardDav account. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, users will be able to access the account without entering a password.
Use SSL	Checkbox	If enabled, a secure SSL connection will be used for communications with the CardDav server.
Principal URL	Text Field	Enter the Principal URL of the CardDav account.

Fields marked * are mandatory.

- Click the 'Save' button after entering or selecting the parameters.

The CardDav account will be added to the list.



You can add multiple CardDav accounts to the profile.

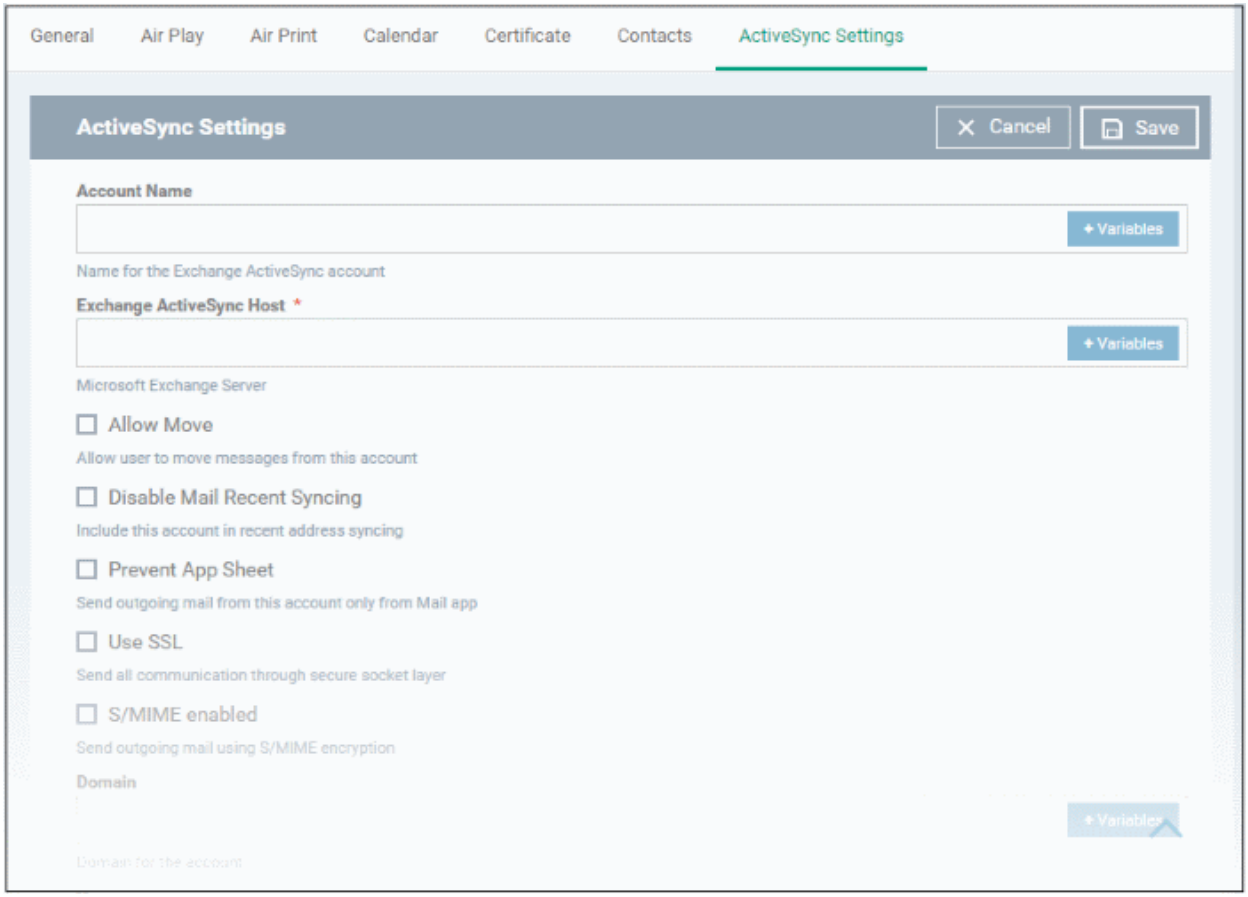
- To add another account, click 'Add Contacts' and repeat the process
- To view or edit a contact account, click on the Hostname of the contact account
- To remove a contact account, select it and click 'Delete Contacts'

The settings will be saved and displayed under 'Contacts' tab. You can edit the contacts or remove the section from the profile at anytime.Refer to the section '**Editing Configuration Profiles**' for more details.

To configure ActiveSync settings

- Click 'ActiveSync Settings' from the 'Add Profile Section' drop-down

The 'ActiveSync Settings' settings screen will be displayed:



ActiveSync Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Name	Text Field	Enter the Exchange ActiveSync account name. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Exchange ActiveSync host*	Text Field	Enter the Exchange host name (Microsoft Exchange Server). You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Allow Move	Checkbox	If enabled, the user can move sent or received mails to another account.
Disable Mail Recent Syncing	Checkbox	If enabled, recently used emailed addresses are not synced with other devices via iCloud.
Prevent App Sheet	Checkbox	If enabled, mails cannot be sent using third-party applications.
Use SSL	Checkbox	If enabled, communication between Exchange server and devices will be encrypted using SSL.
S/MIME Enabled	Checkbox	If enabled, users can sign and encrypt email messages from their devices. Please note that certificates have to be installed in users' devices before this feature can be used.
Domain	Text Field	Address of the account. Click the 'Variables' button + Variables and click

ActiveSync Settings - Table of Parameters		
		the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
User Name	Text Field	User name for the account. Click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Email Address	Text Field	Address of the account. Click the 'Variables' button + Variables and click + beside '%u.mail' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Password	Text Field	Leave the field blank. The user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Past days of mail to sync	Drop-down	Choose the period for which the emails are to be kept synchronized between the device and the exchange server from the recent past, from the drop-down.
User Certificate	Drop-down	Select the user client authentication certificate from the drop-down or upload it using the 'Add New' button.

- Click the 'Save' button.

The settings will be saved and displayed under 'ActiveSync Settings' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Global HTTP proxy settings

- Click 'Global Proxy HTTP' from the 'Add Profile Profile Section' drop-down

The 'Global Proxy HTTP' settings screen will be displayed.

Global HTTP Proxy Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name of the HTTP proxy to be displayed on devices to which the profile is applied. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Proxy	Drop-down	Select the proxy type from the drop-down. The options available are: • None • Manual • Auto If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. If you select 'Auto', enter the URL of the Proxy Pac, select whether or not the device can directly connect to the destination if Pac server is not reachable and whether or not the device can bypass the proxy server to display the login page for captive networks from the respective check box options. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

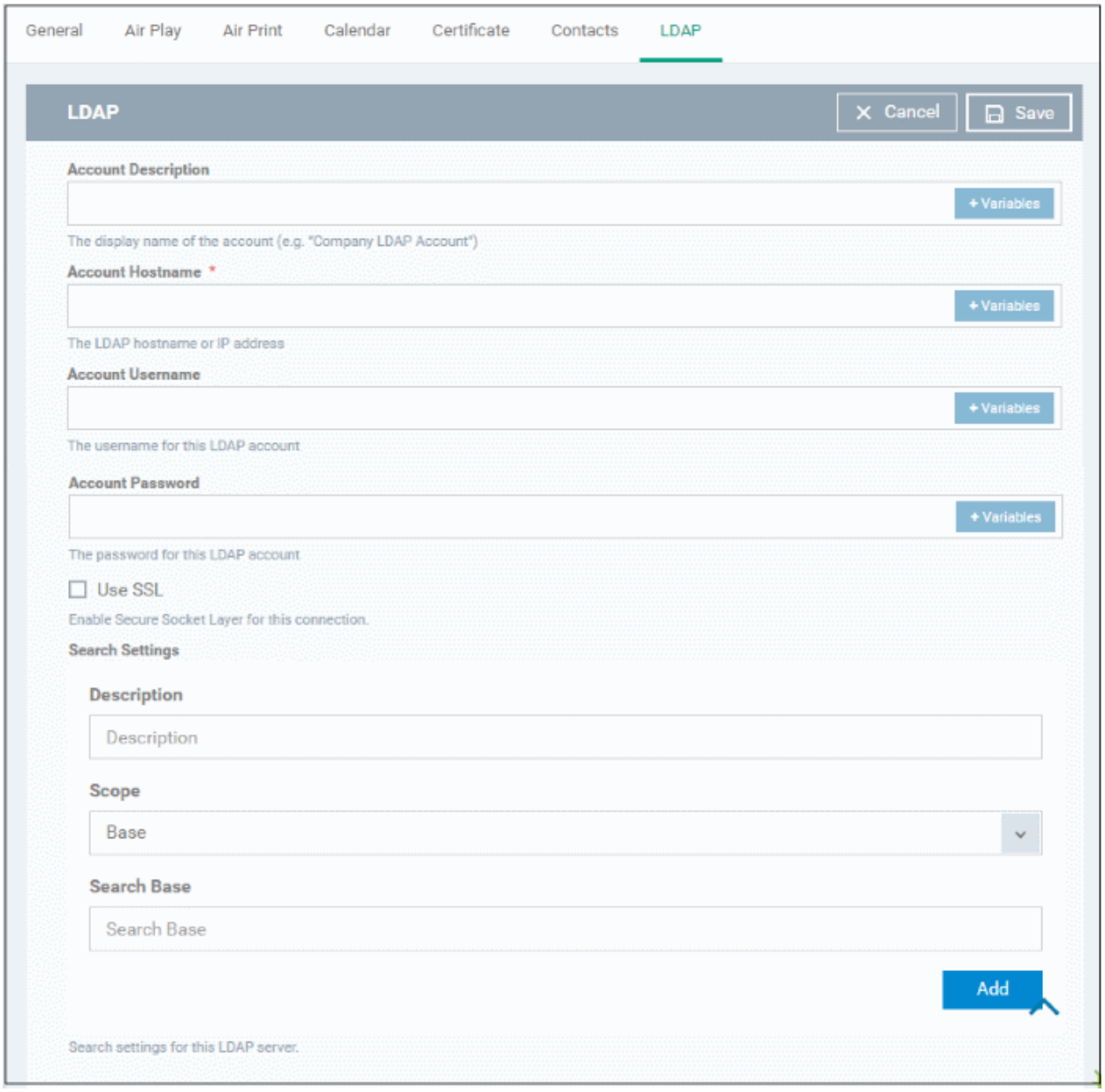
- Click the 'Save' button.

The settings will be saved and displayed under 'Global Proxy HTTP' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure LDAP settings

- Click 'LDAP' from the 'Add Profile Section' drop-down

The 'LDAP' settings screen will be displayed.

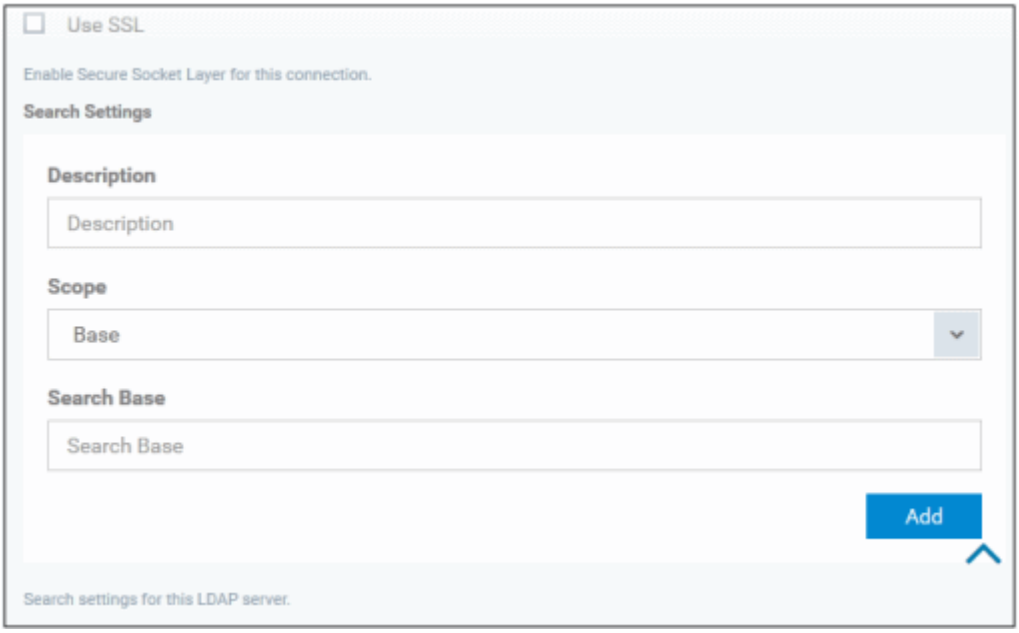


LDAP Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Description	Text Field	Enter the display name of the LDAP account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Hostname	Text Field	Enter the LDAP hostname or IP address. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Username	Text Field	The username for the LDAP account. You can also add variables by

LDAP Settings - Table of Parameters		
		clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Account Password	Text Field	The password for the LDAP account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Use SSL	Checkbox	If enabled, the communication will be encrypted.
Search Settings		Configure the settings for searching email contacts from the LDAP server. Refer to the section 'Searching the LDAP directory' below for more details.

Searching the LDAP directory

Admins can search for email contacts in the domain using the search feature.

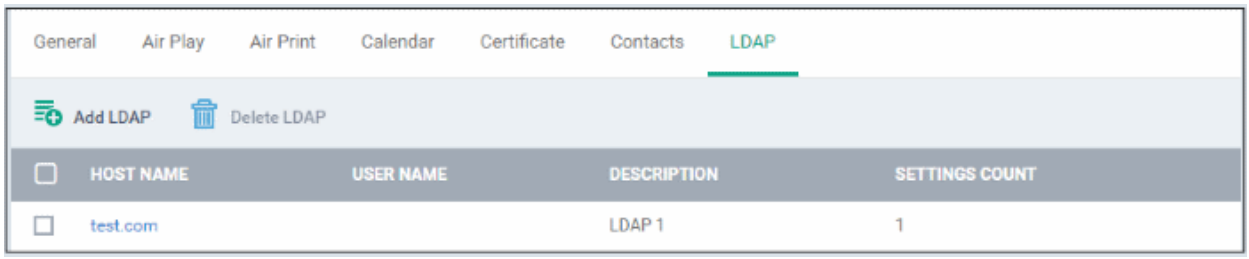


LDAP Search Settings - Table of Parameters		
Form Element	**Type**	**Description**
Description	Text Field	Enter the name of the search
Scope	Drop-down	Select from the drop-down to what level in the LDAP tree structure the search should run. • Base - Searches only the defined search base. • One level - Searches the base and the first level below it. • Subtree - Searches the base and all the levels below it.
Search base	Text Field	Enter the search base for which the search will be restricted. For example, you might want to allow users to search only for other email users via LDAP.

- You can add more 'Search Settings' by clicking the Add button below.
- To remove an item, click the ✖ button.

- Click the 'Save' button.

The LDAP account will be added to the list.



You can add multiple LDAP accounts.

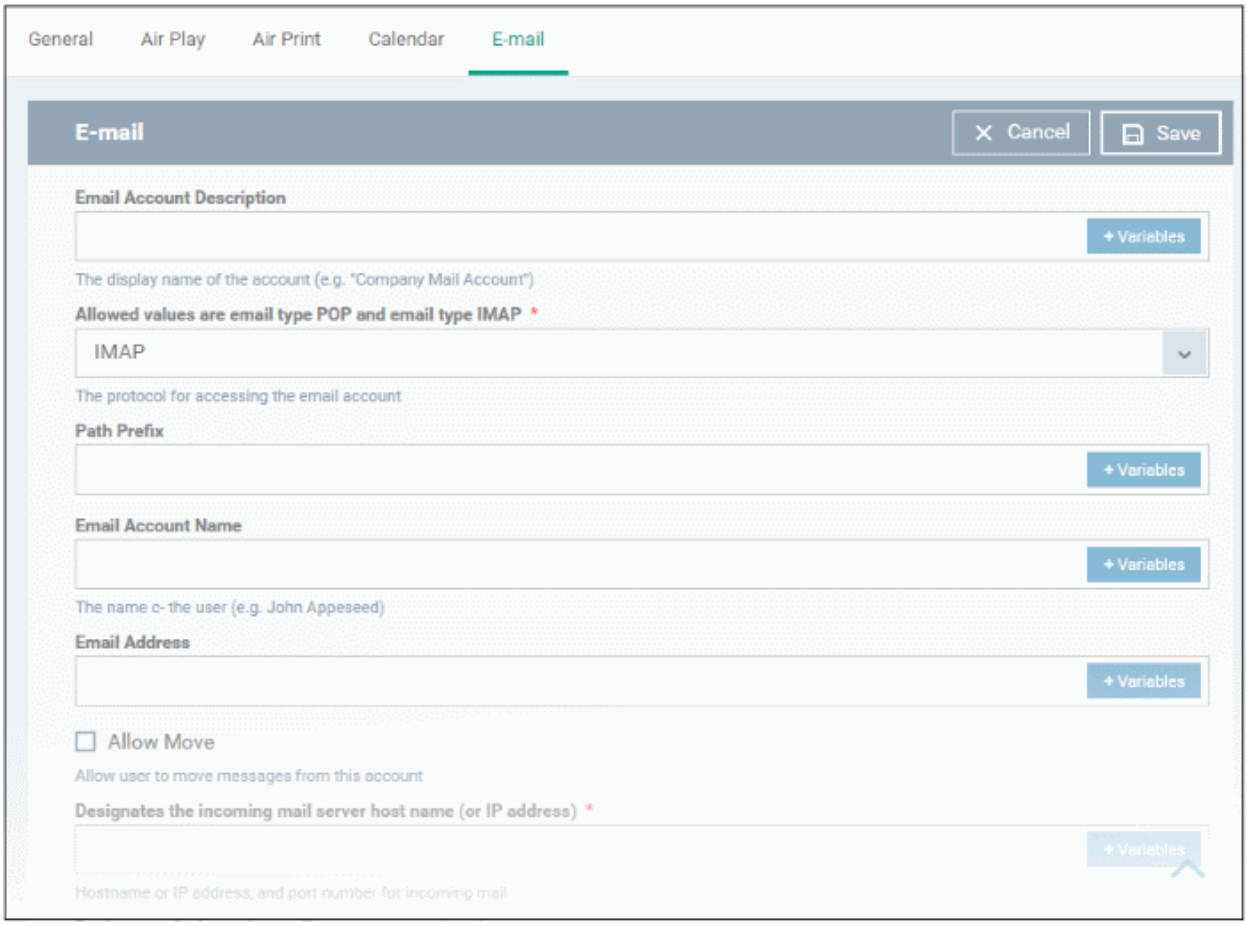
- To add another LDAP server, click 'Add LDAP' and repeat the process
- To view and edit the settings of an LDAP account, click the hostname of it
- To remove an LDAP account, select it and click 'Delete LDAP'

The settings will be saved and displayed under 'LDAP' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure E-Mail settings

- Click 'E-mail' from the 'Add Profile Section' drop-down

The 'E-mail' settings screen will be displayed.



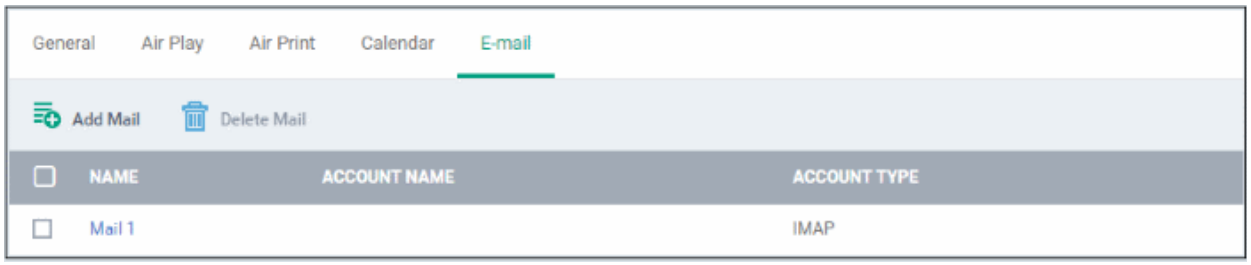
Mail Account Settings - Table of Parameters		
Form Element	**Type**	**Description**
Email Account Description	Text Field	Enter a description for the email account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Allowed values are email type POP and email type IMAP *	Drop-down	Select IMAP or POP from the email type for the profile.
Path Prefix	Text Field	This will be visible if IMAP is chosen as Email Type in the previous step. Enter the path of the inbox in the field. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Email Account Name	Text Field	If the profile is for a single user, enter the name to identify the user's email account. If the profile is for several users, click the 'Variables' button + Variables, and click + beside '%u.login%' from the 'User Variables list'. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Email Address	Text Field	If the profile is for a single user, enter the email address of the user. If the

Mail Account Settings - Table of Parameters		
		profile is for several users, click the 'Variables' button + Variables, and click + beside '%u.mail%' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables.
Allow Move	Checkbox	If enabled, the user can move sent or received mails to another account.
Designates the incoming mail server host name (or IP address)*	Text Field	Enter the host name of the incoming mail server or its IP address. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Designates the incoming mail server port number*	Text Field	Enter the server port number used for incoming mail service. For POP3, it is usually 110 and if SSL is enabled it is 995. For IMAP, it is usually 143 and if SSL is enabled it is 993. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Incoming Mail Server Username	Text Field	If the profile is for a single user, enter their username for the incoming mail server. If the profile is for several users, click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Allowed values are email auth password and email auth none *	Drop-down	Select the type of authentication method for the mail account from the drop-down. The options available are: • None • Password • CRAM MD5 • NTLM • HTTP MD5
Incoming Password	Text Field	Leave the field blank. If authentication is chosen in the previous step, then user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Incoming Mail Server use SSL	Checkbox	If enabled, communication between incoming mail server and devices is encrypted using SSL.
Outgoing Mails Server Host Name*	Text Field	Enter the host name or IP address for the outgoing mail server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

Mail Account Settings - Table of Parameters		
Designates the outgoing mail server port number*	Text Field	Enter the server port number used for outgoing mail service. If no port number is specified then ports 25, 587 and 465 are used in the given order. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Outgoing Mail Server Username	Text Field	If the profile is for a single user, enter the username of the user to login to outgoing mail server. If the profile is for several users, click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Outgoing Mail Server Authentication*	Drop-down	Select the type of authentication method for outgoing mail server from the drop-down. The options available are: • None • Password • CRAM MD5 • NTLM • HTTP MD5
Outgoing Password	Text Field	Leave the field blank. If authentication is chosen in the previous step, then user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Outgoing Password Same as Incoming Password	Checkbox	If enabled, the password for incoming mail server will be used for outgoing mail server too.
Disable Mail Recents Syncing	Checkbox	If enabled, recently used emailed addresses are not synced with other devices via iCloud.
Signing and encryption per-message	Checkbox	If enabled, the device digitally signs and encrypts your mail per-message.
Prevent App Sheet	Checkbox	If enabled, outgoing mails can be sent from this account only via mail app.
Outgoing Mail Server Use SSL	Checkbox	If enabled, communication between outgoing mail server and devices is encrypted using SSL.
SMIME enabled	Checkbox	If enabled, users can sign and encrypt email messages from their devices. Please note that certificates have to be installed in users' devices before this feature can be used.

- Click the 'Save' button.

The e-mail account will be added to the profile.



You can add several email accounts to the same profile.

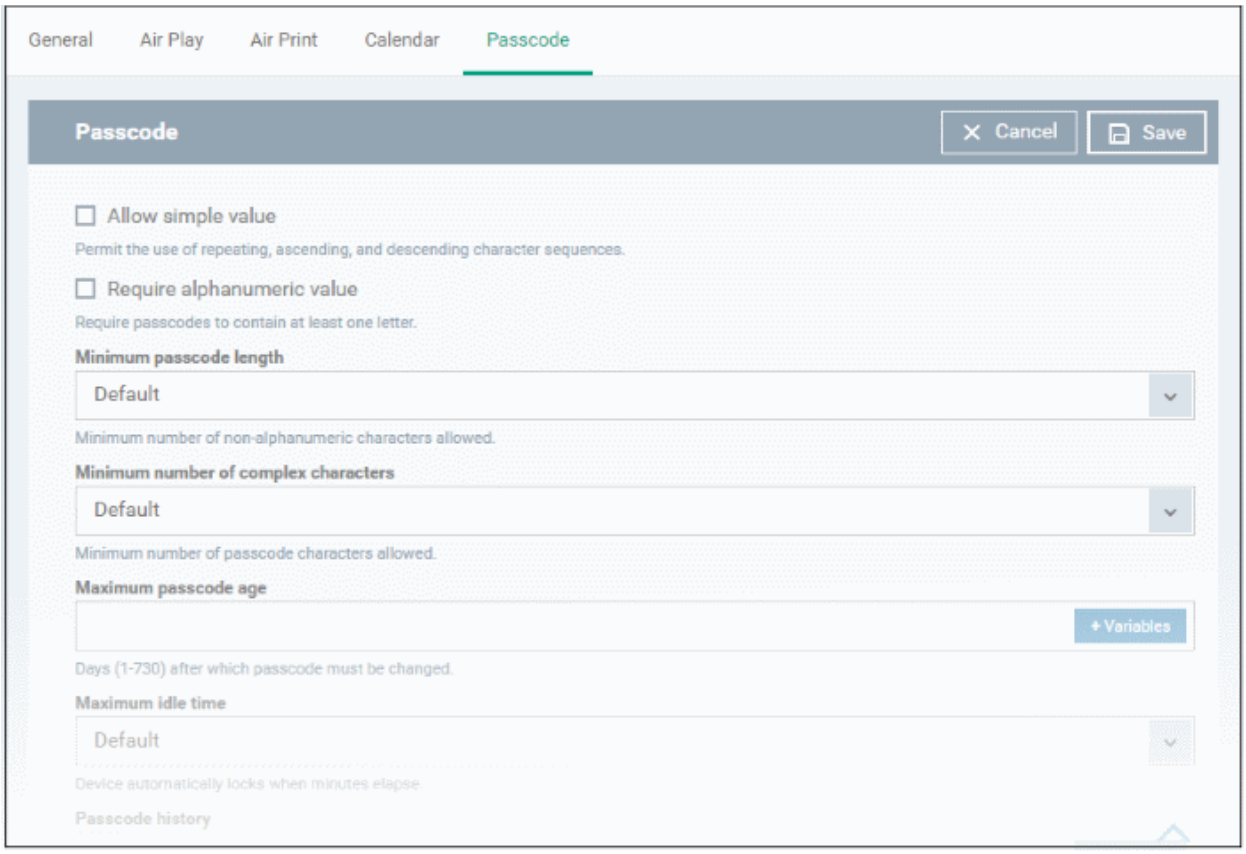
- To add another email account, click 'Add Mail' and repeat the process
- To view and edit the settings for an email account, click on its name
- To remove an email account, select it and click 'Delete Mail'

The settings will be saved and displayed under the 'Email' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Passcode settings

- Click 'Passcode' from the 'Add Profile Section' drop-down

The 'Passcode Settings' screen will be displayed.



Passcode Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Simple Value	Checkbox	Selecting this will allow the users to configure repeated or sequential characters in their passwords. For example, '9999' or ABCD.
Require Alphanumeric Value	Checkbox	Selecting this will compel the user to configure at least one number or letter in their passwords.
Minimum Passcode Length	Drop-down	The minimum number of characters that a password should contain. The option is available to set from 1 to 16.
Minimum Number of Complex Characters	Drop-down	The minimum number of symbols (non alphanumeric characters such as *, %, @) that a password should contain. The option is available to set from 1 to 4.
Maximum Passcode Age	Text Field	Enter the maximum number of days that a password can be valid. The option is available from 1 day to 730 days. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Maximum Idle Time	Drop-down	Select the period of time in minutes that a device can be idle before it's screen is automatically locked.
Passcode History	Text Field	New passwords should not match previously used passwords. Specify the number of last used passwords that should be stored for comparison. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Maximum Grace Period for Device Lock	Drop-down	Select the period from the drop-down how soon the device can be unlocked since last used without prompting the user to enter the password. The option is available from 'Immediately' to '4 Hours' If 'Immediately' is selected, the user has to enter the password each time the device is unlocked.
Maximum Number of Failed Attempts	Drop-down	Select the number of unsuccessful login attempts that can be tried by a user before the device is wiped clean of all its data and settings. The option is available to set from 4 to 10. After 6 unsuccessful login attempts, there will be a time delay before a password can be entered again and the time delay period increases with each failed login attempt. This time delay begins only after the sixth attempt, so if you select the period as 6 or lower, there will be no time delay and data will be erased after the final attempt.
Allows the user to modify Touch ID	Check box	If enabled, allows user you to modify the biometric authentication to unlock your device, make purchases and so on.

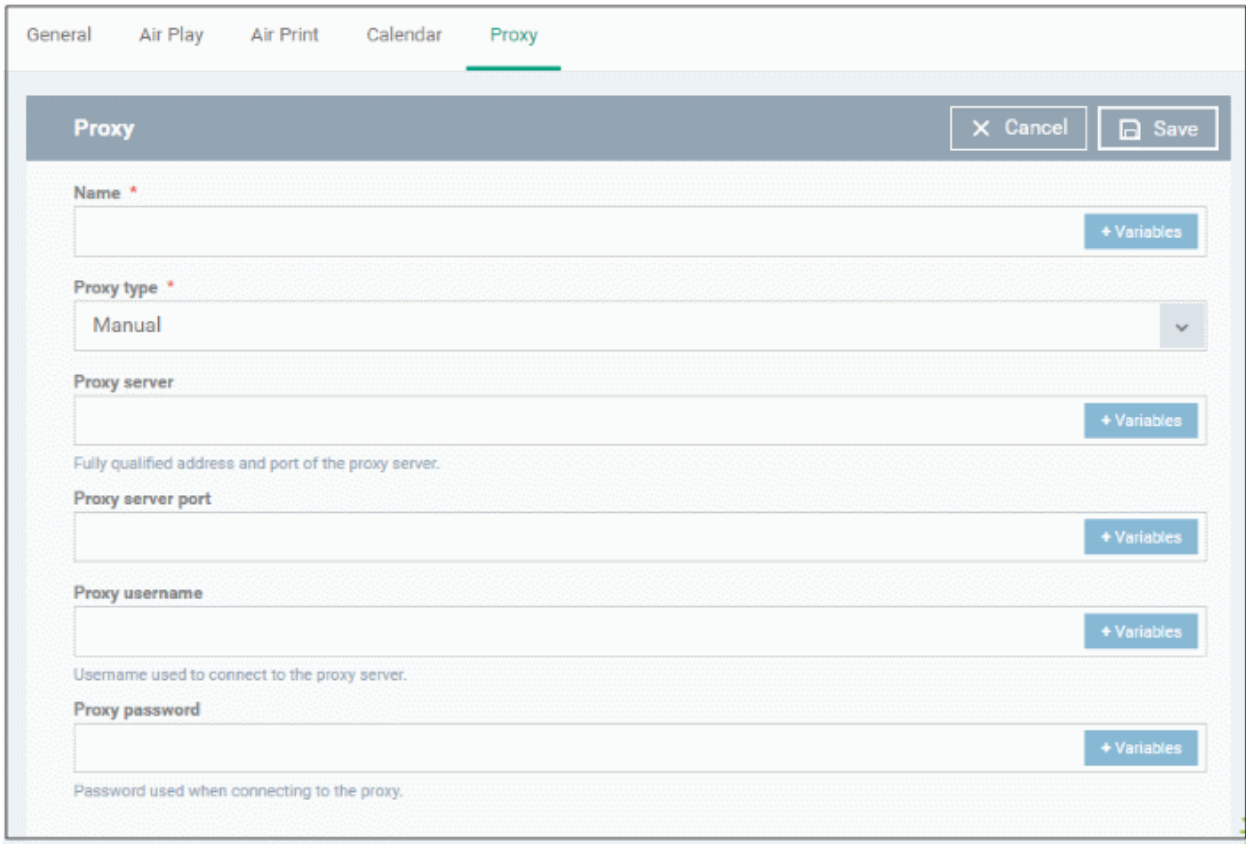
- Click the 'Save' button.

The settings will be saved and displayed under the 'Passcode' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Proxy settings

- Click 'Proxy' from the 'Add Profile Section' drop-down

The 'Proxy' settings screen will be displayed.



Proxy Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name of the that will be displayed to the users for the policy. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Proxy	Drop-down	Select the proxy type from the drop-down. The options available are: • None • Manual • Auto If you select 'Manual', enter the details for IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. If you select 'Auto', enter the URL of the Proxy Pac. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.

- Click the 'Save' button.

The proxy server configuration will be added to the profile.

You can add more proxy server accounts to the profile.

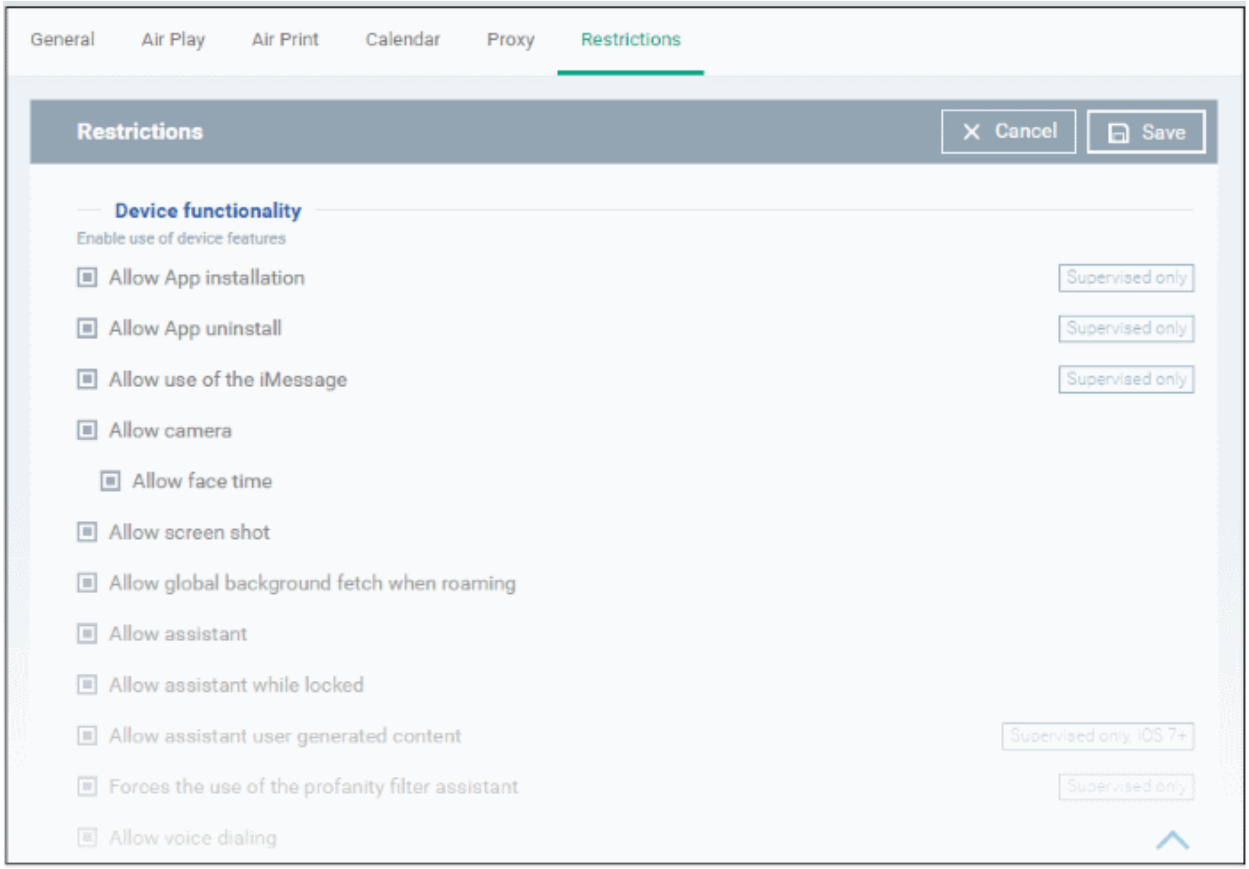
- To add another proxy server account, click 'Add Proxy' and repeat the process
- To view or edit a proxy server account, click on its name
- To remove a proxy server account, select it then click 'Delete Proxy'

The settings will be saved and displayed under the 'Proxy' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Restrictions settings

- Click 'Restrictions' from the 'Add Profile Section' drop-down

The 'Restrictions' settings screen will be displayed.



Restrictions Settings - Table of Parameters		
Device Functionality		
Form Element	Type	Description

Restrictions Settings - Table of Parameters		
Allow App Installation	Checkbox	Allows the user to install or update apps from the Apple App Store. If left unchecked, the App Store icon is removed from the device's home screen.
Allow App uninstall	Checkbox	Allows the user to uninstall applications.
Allow use of iMessage	Checkbox	Allows the user to quickly and easily chat over iMessage or SMS/MMS.
Allow camera	Checkbox	Allows the user to take photos, videos or use FaceTime (if enabled). If left unchecked, the camera icon is removed from the device and camera is disabled.
Allow face time	Checkbox	Allows the user to use FaceTime. Please note the 'Allow face time' can be enabled only if 'Allow Camera' is enabled.
Allow screen shot	Checkbox	Select this to allow the user to take screenshots.
Allow global background fetch when roaming	Checkbox	Select this to allow the device to sync data when in roaming mode abroad.
Allow assistant	Checkbox	If enabled, users can use Siri voice commands and dictation.
Allow assistant while Locked	Checkbox	If enabled, users can use Siri even when the device is locked. The checkbox will be active only when 'Allow Assistant' is enabled.
Allow assistant user generated content	Checkbox	If enabled, users can use Siri to query user-generated content from the Internet or device. (Supervised mode only.)
Forces the use of the profanity filter assistant	Checkbox	If enabled, enforces profanity filter for Siri.
Allow voice dialing	Checkbox	Select this to allow the user to dial their phone using voice commands.
Allow passbook while locked	Checkbox	If enabled, Passbook notifications will be displayed even when the device is locked.
Allow in app purchases	Checkbox	Select this to allow the user to make in-app purchases from the device.
Force iTunes store password entry	Checkbox	If enabled, users have to enter their Apple ID to enter the iTunes store.
Allow multiplayer gaming	Checkbox	Select this to allow the user to play multiplayer games in Game Center.
Allow adding game center friends	Checkbox	If enabled, users can add friends in Game Center.
Allow account modification	Checkbox	Select this to allow user account modifications on devices. Note: This feature is available for iOS 7+ and supervised devices only.
Allow air drop	Checkbox	Select this to allow Air Drop on devices. Note: This feature is available for iOS 7+ and supervised devices only.
Allow find my friends modification	Checkbox	Select this to enable Find My Friends feature on devices. Note: This feature is available for iOS 7+ and supervised devices only.
Allow fingerprint for unlock	Checkbox	Select this to enable Touch ID to unlock devices. Note: This feature is available for iOS 7+ and supervised devices only.

Restrictions Settings - Table of Parameters		
Allow game center	Checkbox	If enable, users can access Game Center, an online multiplayer social gaming network. Note: This option is available for supervised devices only.
Allow host pairing	Checkbox	Select this to allow host pairing on devices. Note: This feature is available for iOS 7+ and supervised devices only.
Allow lock screen control center	Checkbox	Select this option to allow Control Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow lock screen notifications view	Checkbox	Select this option to allow Notification Center to be displayed on the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow lock screen today view	Checkbox	Select this option to allow the Today View from Notification Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow OTAPKI updates	Checkbox	Select this option to allow over-the-air public key infrastructure (OTAPKI) updates on the device. Note: This feature is available for iOS 7 and later versions.
Allow UI configuration profile installation	Checkbox	Select this option to allow users to install UI configuration profiles. Note: This option is available for supervised devices only.
Force limit ad tracking	Checkbox	Select this to limit ad tracking on devices. Note: This feature is available for iOS 7 and later versions.
Forces all devices receiving AirPlay requests from this device to use a pairing password	Checkbox	If enabled, forces the use of pairing password for all other devices sending AirPlay requests to the device.
Allow managed applications from using cloud sync	Checkbox	If enabled, users can restrict managed apps backing up any data to iCloud, while still allowing it for user downloaded apps.
Allow the "Erase All Content And Settings" option in the Reset UI	Checkbox	If enabled, users can remove his/her personal information: credit or debit card, photos, contacts, music, or apps. Note: This feature is available for supervised devices only.
Spotlight will return Internet search results	Checkbox	If enabled, the spotlight features will provide suggestions from the Internet, iTunes, and the App Store for the user to quickly find any file, documents, emails, apps contacts and more on the device. (For supervised devices only.)
Allow the "Enable Restrictions" option in the Restrictions UI in Settings	Checkbox	If enabled, users can enable or disable 'Enable Restrictions' option in the 'Restrictions' user interface on the device. (For supervised devices only.)
Allow Activity Continuation	Checkbox	If enabled, user can control data flow through iCloud.
Allow backed up Enterprise books	Checkbox	If enabled, users can backup iBooks and restrict synchronization to iCloud.

Restrictions Settings - Table of Parameters		
Enterprise books notes and highlights will be synced	Checkbox	If enabled, allows the user to to sync Enterprise books, notes and highlights to iCloud.
Allow podcasts	Checkbox	If enabled users can receive their favorite podcasts. Note: This feature is available only for supervised devices with iOS 8 and later versions.
Allow definition lookup	Checkbox	If enabled, allows the user to enable or disable spell check and definition features on the device. Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions.
Allow predictive keyboard	Checkbox	If enabled, users can enable or disable the predictive keyboard feature. Note: This feature is available only for supervised devices only with iOS 8.1.3 and later versions.
Allow keyboard auto-correction	Checkbox	If enabled, allows user to enable/disable keyboard auto-correct feature. Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions.
Allow keyboard spell-check	Checkbox	If enabled, allows user to enable/disable keyboard spell check feature. Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions.
Paired Apple Watch will be forced to use Wrist Detection	Checkbox	If an Apple Watch is paired with the device, the device forces the Apple Watch to enable Wrist Detection. Note: This feature is available for iOS 8.2 and later versions.
Allow Music service and Music	Checkbox	If enabled, it allows third-party apps to add music to user's iCloud music library. Note: This feature is available for iOS 9.0 and later versions.
Allow iCloud Photo Library	Checkbox	If enabled, allows the user to upload photos and videos to iCloud photo library.
Allow News	Checkbox	If enabled, users can subscribe to news services. Note: This feature is available only for supervised devices with iOS 9.0 and later versions.
Causes AirDrop to be considered an unmanaged drop target	Checkbox	If enabled, all targets specified for the AirDrop feature will be considered as unmanaged drop targets. Note: This feature is available for iOS 9.0 and later versions.
Enable the App Store on the Home screen	Checkbox	If enabled, displays the AppStore icon on the home screen of the device.
Allow keyboard shortcuts	Checkbox	If enabled, allows the user to create and use keyboard shortcuts for typing snippets. Note: This feature is available only for Supervised devices with iOS 9.0 and later versions.
Allow pairing with an Apple Watch	Checkbox	If enabled, allows the user to pair the device with an Apple Watch. Note: This feature is available only for Supervised devices with iOS 9.0 and later versions.

Restrictions Settings - Table of Parameters		
Allow device passcode from being added, changed, or removed	Checkbox	If enabled, users can create and modify screenlock passcodes for the device. Note: This feature is available only for supervised devices with iOS 9.0 and later versions.
Allow device name modification	Checkbox	If enabled, allows users to change the device name. Note: This feature is available for only Supervised devices with iOS 9.0 and later versions.
Allow wallpaper modification	Checkbox	If enabled, allows user to change wallpaper displayed on the device. Note: This feature is available only for supervised devices with iOS 9.0 and later versions.
Allow automatic download applications	Checkbox	If enabled, allows applications in the device to automatically download and install apps and updates. Note: This feature is available only for supervised devices with iOS 9.0 and later versions.
Allow enterprise application trust	Checkbox	If enabled, 'Trusted' status is automatically applied to enterprise applications. Note: This feature is available for iOS 9.0 and later versions.
Allow enterprise application trust modification	Checkbox	If enabled, users can manually change the Trust status of enterprise applications. Note: This feature is available only for Supervised devices with iOS 9.0 and later versions.
Allow radio service	Checkbox	If enabled, users can use Radio services on their device. Note: This feature is available only for Supervised devices with iOS 9.3 and later versions.
Allow notifications modification	Checkbox	If enabled, user can modify 'Apple Push Notifications' settings on the device. Note: This feature is available only for Supervised devices with iOS 9.3 and later versions.
Whitelisted application bundles	Text box	Allows you to add applications to the app whitelist. The applications in the whitelist will be skipped from security checks during installation and usage. • Enter the App IP of the application to be added to the whitelist. For more details on obtaining the App ID, refer to the explanation at the end of this section. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. • To add more Whitelisted application bundles, click + button. • To remove an app, click the − beside it. Note: This feature is available only for supervised devices with iOS 9.3 and later versions.

Restrictions Settings - Table of Parameters		
Blacklisted application bundles	Text box	Allows you to add applications to the app blacklist. The applications in the blacklist will not be allowed to be installed or used. • Enter the App IP of the application to be added to the blacklist. For more details on obtaining the App ID, refer to the **explanation** at the end of this section. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**. • To add more Blacklisted application bundles, click + button. • To remove an app, click the − beside it. Note: This feature is available only for Supervised devices with iOS 9.3 and later versions.
Security and privacy		
Allow diagnostic submission	Checkbox	If enabled, the device will be enabled to submit its iOS diagnostic information to Apple.
Allow untrusted TLS prompt	Checkbox	If enabled, users will be prompted if they want to trust unverified certificates. This setting applies to Calendar accounts, Contacts, Safari and to Mail.
Force encrypted backup	Checkbox	If left unchecked, users can select whether or not to encrypt backups from the device to iTunes in a local computer. If this option is enabled, the backup data from the device to iTunes in local computer will be automatically encrypted.
Content ratings		
Allow explicit content	Checkbox	Content providers of iTunes flag their explicit content for easy identification. If enabled, explicit content including music and video will be displayed in iTunes store instead being hidden, in the device.
Allow iBookstore	Checkbox	If enabled, users can access iBookstore, an online bookstore from Apple. Note: This option is available only for supervised devices.
Allow iBookstore erotica	Checkbox	If enabled, users can download media tagged as erotica from iBooks. Note: This feature is available only for Supervised devices with versions prior to iOS 6.1.
Rating region	Drop-down	Select the region whose content ratings are to be followed, from the drop-down.
Rating movies	Drop-down	Choose the content rating to be allowed for watching movies.
Rating TV Shows	Drop-down	Choose the content rating to be allowed for watching the TV shows.
Rating apps	Drop-down	Choose the rating to be allowed for using apps.
Applications		

Restrictions Settings - Table of Parameters		
Allow i Tunes	Checkbox	If enabled, users can access iTunes store. If left unchecked, iTune store is disabled and its icon will be removed from the home screen.
Allow Safari	Checkbox	If enabled, users can use Safari for browsing internet. If left unchecked, the Safari browser app will be disabled and its icon will be removed from the home screen.
Safari allow auto fill	Checkbox	If enabled, the 'auto-fill' feature will be enabled for Safari, to automatically fill details such as user name, password, credit card details and so on in web forms.
Safari allow java script	Checkbox	If enabled, java script features will be supported by Safari.
Safari allow popups	Checkbox	If enabled, popups will be allowed in Safari.
Safari force fraud warning	Checkbox	If enabled, Safari displays alerts to users when visiting websites that are identified as compromised or fraudulent.
Safari accept cookies	Drop-down	Select the option on when Safari can accept cookies, from the drop-down. The available options: • Always • Never • From visited site
Allow app cellular data modification	Checkbox	If enabled, user can modify cellular data usage settings for individual apps on the device. Note: This feature is available only for Supervised devices with iOS 7 or later versions.
Allow open from Managed to Unmanaged	Checkbox	If enabled, users can send data from managed apps to unmanaged apps. Note: This feature is available for iOS 7 and later versions.
Allow open from Unmanaged to Managed	Checkbox	If enabled, users can send data from unmanaged apps to managed apps. Note: This feature is available for iOS 7 and later versions.
Autonomous single app mode permitted app IDs	Text Field	iOS apps built with the functionality of single App Lock, can provoke App Lock for them under certain scenarios in Autonomous single app mode. Administrators can specify the apps for which the mode can be enabled, by entering their App Ids. • Enter the App IP of the application to be permitted for autonomous single app mode. For more details on obtaining the App ID, refer to the explanation at the end of this section. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. • To add more apps, click + button. • To remove an app, click the − beside it. Note: This feature is applicable only for Supervised devices with iOS 7 or

Restrictions Settings - Table of Parameters		
		later versions.
iCloud		
Allow cloud keychain sync	Checkbox	If enabled, the Apple Keychain data on the device will be synced to iCloud. Note: This feature is applicable only for iOS 7 and later versions.
Allow cloud backup	Checkbox	If enabled, users can backup their device data to iCloud. Note: This feature is applicable only for iOS 7 and later versions.
Allow cloud document sync	Checkbox	If enabled, users can synchronize documents on their device with iCloud. Note: This feature is applicable only for iOS 7 and later versions.
Allow photo stream	Checkbox	Allows users to use Photo Stream. Note: This feature is applicable only for iOS 7 and later versions.
Allow shared stream	Checkbox	If enabled, users can share and view photos in Photo Stream. Note: This feature is applicable only for iOS 7 and later versions.

- Click the 'Save' button.

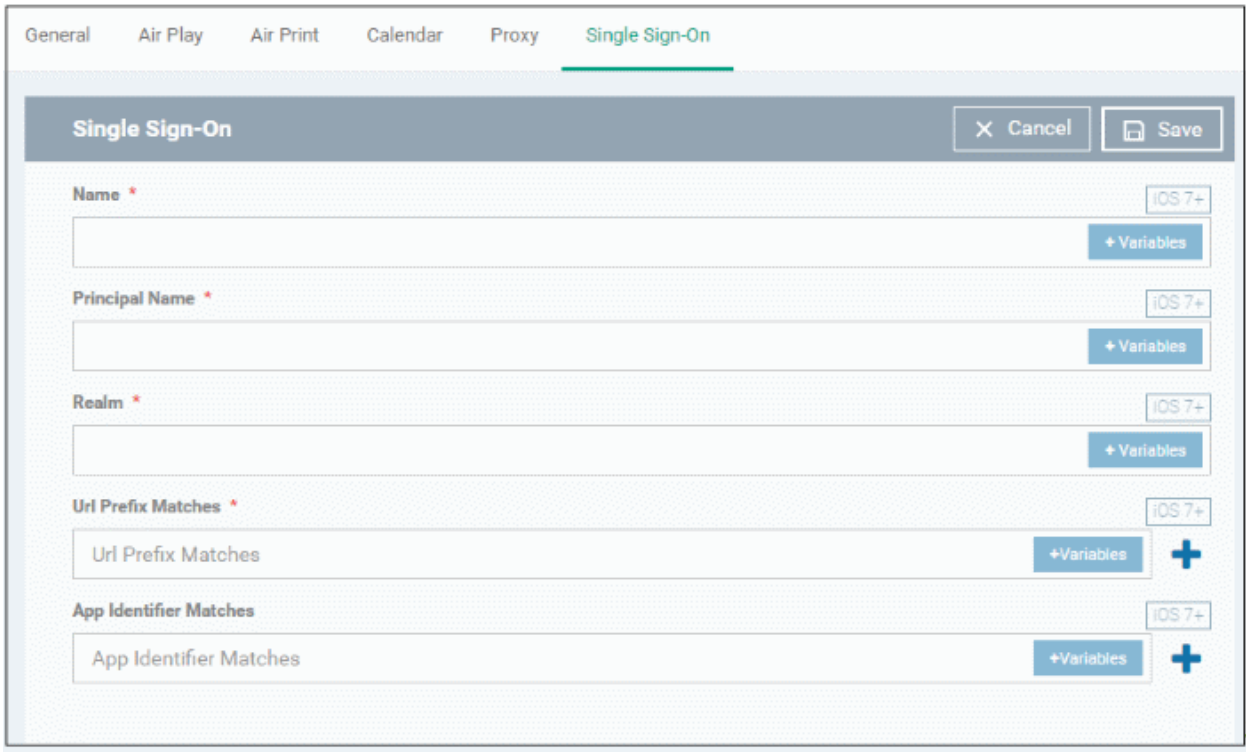
The saved 'Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Single Sign-On settings

These settings are used to configure Kerberos authentication and are applicable for iOS 7 or later versions only. You can add several Single Sign On accounts to a profile.

- Click 'Single Sign-On' from the 'Add Profile Section' drop-down

The 'Single Sign On' settings screen will be displayed.

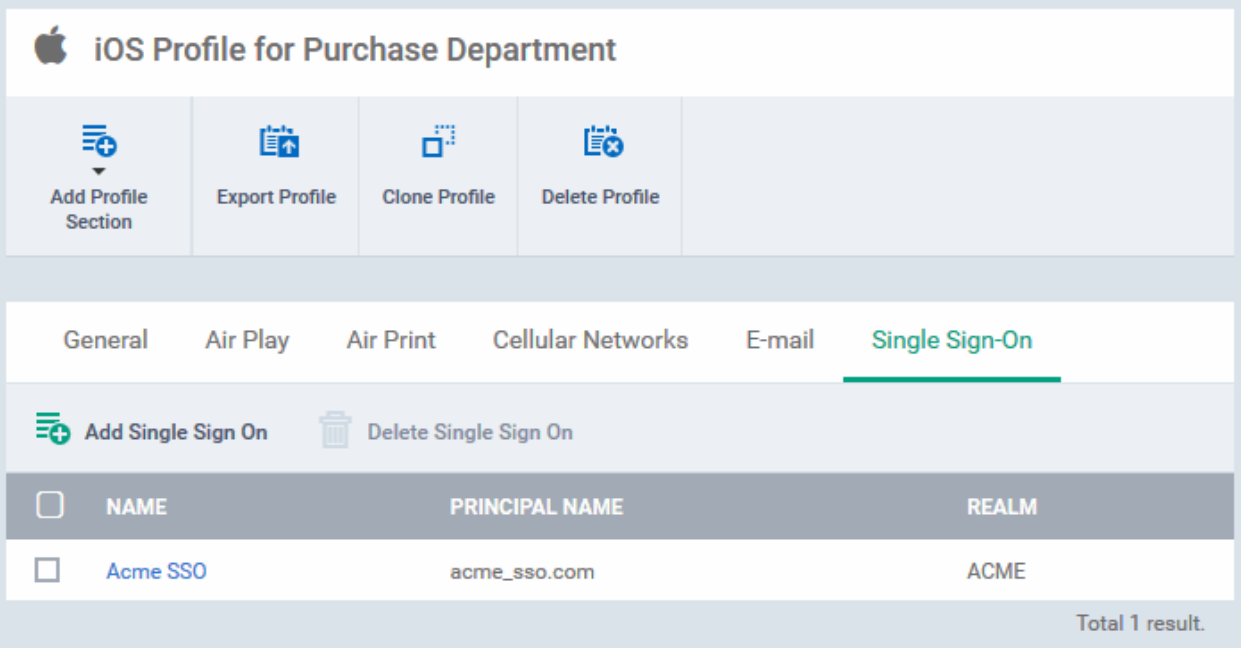


Single Sign-On Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name*	Text Field	Enter the name for the account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Principal Name*	Text Field	Enter the Kerberos principal name. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Realm*	Text Field	Enter the Kerberos realm name with upper-case characters. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
URL prefix matches*	Text Field	Enter the URL prefix, which must be matched in order to use this account for Kerberos authentication over HTTP. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Click + button to add more 'URL prefix matches' fields. To remove a URL prefix, click the minus button beside it.
App identifier matches	Text Field	Enter the bundle IDs of apps that are allowed to use this Single Sign-On account for logging-in to respective account. If this field is left blank, this login matches all app IDs.

Single Sign-On Settings - Table of Parameters		
		You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Click + button to add more 'App identifier matches' fields. To remove an App identifier match, click the minus button beside it.

- Click the 'Save' button.

The account will be added to the Single Sign-On section of the profile.



You can add several SSO accounts to the profile.

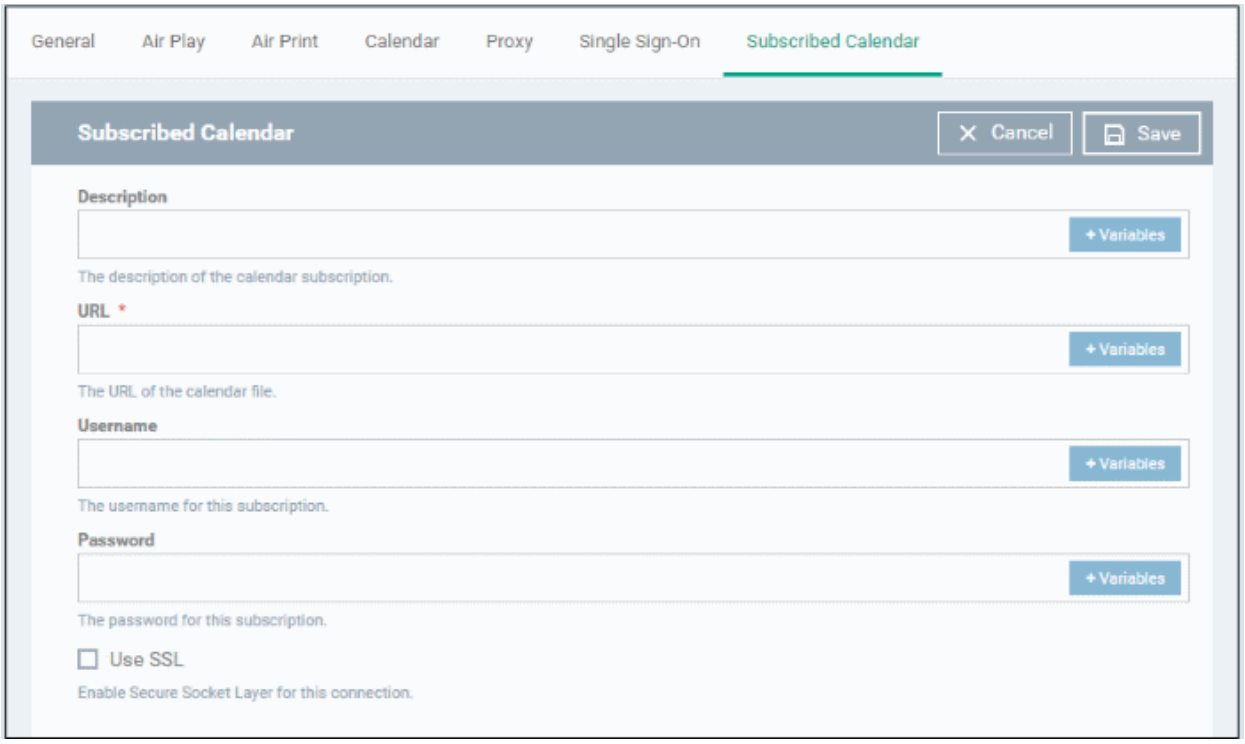
- To add another SSO account, click 'Add Single Sign-On' and repeat the process
- To view and edit an SSO account, click the name of it
- To remove an SSO account, select it then click 'Delete Single Sign-On'

The settings will be saved and displayed under the Single Sign-On tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Subscribed Calendar settings

- Click 'Subscribed Calendars' from the 'Add Profile Section' drop-down

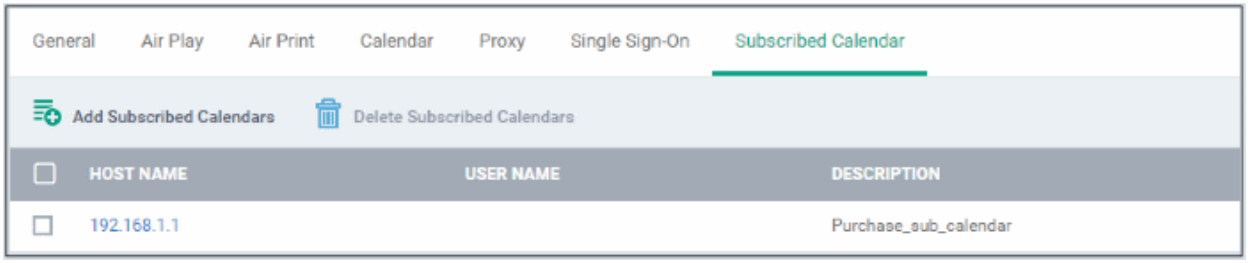
The 'Subscribed Calendar' settings screen will be displayed.



Subscribed Calendars Settings - Table of Parameters		
Form Element	**Type**	**Description**
Description	Text Field	Enter a description of the calendar subscription. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
URL*	Text Field	Enter the URL of the calendar account to be subscribed. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Username	Text Field	The user name for the subscription. If the profile is for several users, you can add variables for setting up subscription to respective user's calendar account. Click the 'Variables' button + Variables and click + beside '%u.login%' from the 'User Variables' list. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables.
Password	Text Field	The password for the subscription. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, the users can access the account without entering the credentials.
Use SSL	Checkbox	If enabled, SSL connection will be established with the calendar server, if available.

- Click the 'Save' button.

The calendar account will be added.



You can add several calendar accounts for a profile.

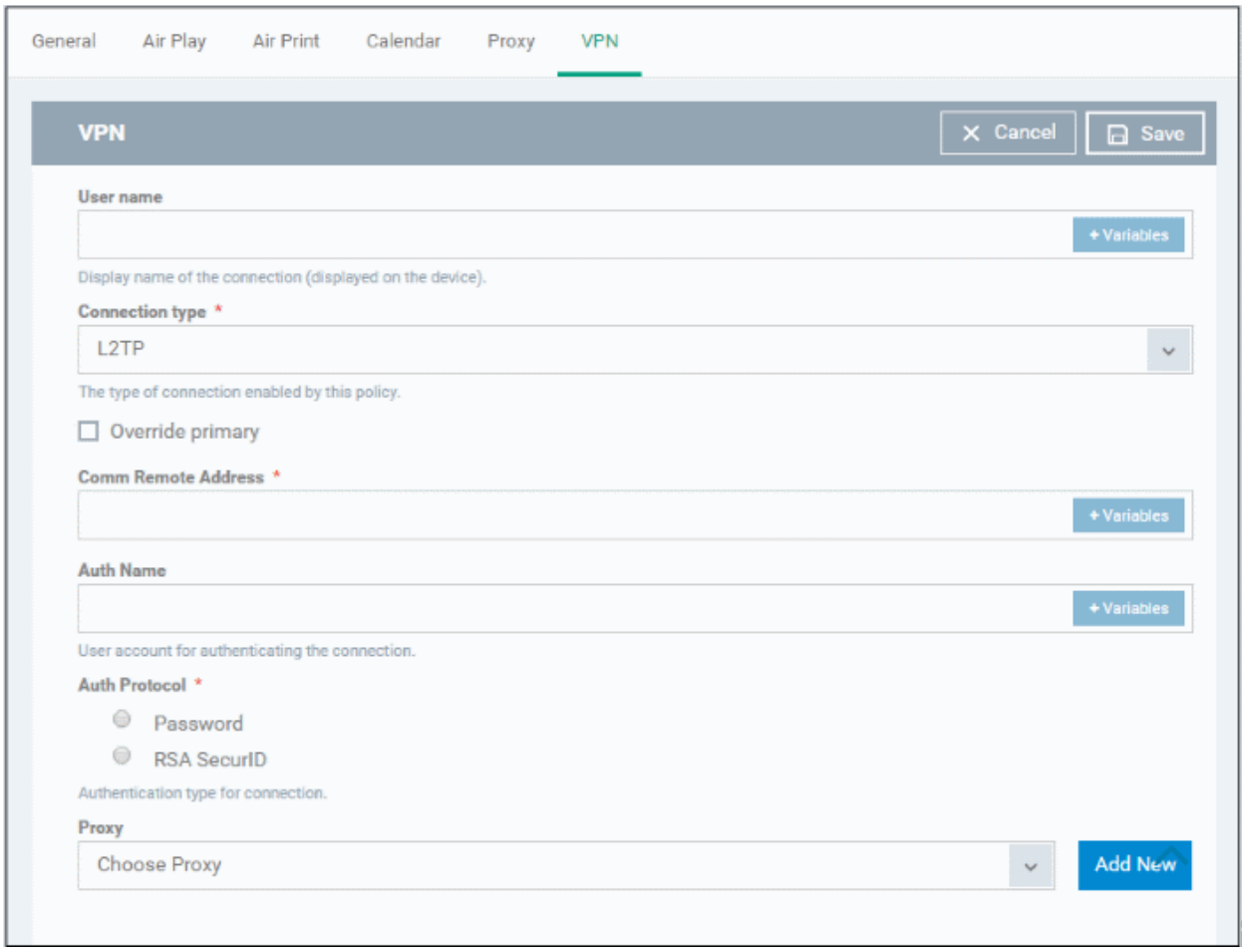
- To add another Subscribed Calendar account, click 'Add Subscribed Calendar' and repeat the process
- To view and edit a calendar account, click the Hostname of it
- To remove a calendar account, select it and click 'Delete Subscribed Calendar'

The settings will be saved and displayed under the Subscribed Calendars tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure VPN settings

- Click 'VPN' from the 'Add Profile Section' drop-down

The settings screen for VPN will be displayed.



VPN Settings - Table of Parameters		
Form Element	**Type**	**Description**
User name	Text Field	Enter the name of the connection, to be displayed on the device. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Connection type*	Drop-down	Choose the VPN connection type from the drop-down. The options available are: • L2TP • PPTP • IPSec • Cisco Any Connection • Juniper SSL • F5 SSL • Open VPN The connection parameters differ for each type. The parameters to be configured for each connection type are explained in the table below.
Proxy	Drop-down	Select the proxy settings for the VPN from the drop-down. You can create a new proxy by clicking the 'Add New' button beside it. The options available are: • None • Manual • Auto If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields. If you select 'Auto', enter the URL of the Proxy Pac.

VPN Connection Type settings

VPN Connection Type Settings - Table of Parameters	
Connection Type	**Description**
L2TP	• Override Primary - Make this connection override the primary server. • Comm Remote Address - Enter IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Auth Name - Enter the VPN account user name. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Auth Protocol - Select the authentication method. The available options are 'Password' and 'RSA SecurID'. • Auth Password - If 'Password' is selected in 'Auth Protocol', enter

VPN Connection Type Settings - Table of Parameters	
	the VPN account password. Also, you can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Token Card - Select this if you have chosen 'RSA SecurID' in 'Auth Protocol'. • Auth EAP Plugins - Applicable only if RSA SecurID is being used. Enter the 'EAP-RSA' value or add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Shared secret - Applicable only if RSA SecurID is being used. Enter the shared secret or add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section Configuring Custom Variables.
PPTP	• Override Primary - Make this connection override the primary server. • Comm Remote Address - Enter the IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Auth Name - Enter the VPN account user name. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Auth Protocol - Select the authentication method. The available options are 'Password' and 'RSA SecurID' • Auth Password - If 'Password' is selected in 'Auth Protocol', enter the VPN account password. Also, you can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Token Card - Select this if you have chosen 'RSA SecurID' in 'Auth Protocol'. • Auth EAP Plugins - Applicable only if RSA SecurID is being used. Enter the 'EAP-RSA' value. You can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Encryption Level - Choose the encryption level to be used for the VPN connection. The available options are: • None • Automatic • Maximum 128 bit encryption • Shared secret - Applicable only if RSA SecurID is being used. Enter the shared secret string. You can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable. For more details on variables, refer to the section Configuring Custom Variables.
IP SEC	• Override Primary - Make this connection override the primary server. • Server - Enter the IP address or host name of the VPN server. You can add variables by clicking the 'Variables' button + Variables and clicking +

VPN Connection Type Settings - Table of Parameters	

beside the variable you want to add.

- Account - Enter the VPN account name. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
- Password - Enter the password for the account . You can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable.
- Authentication Method - Select the authentication method from the drop-down. The available options are:
    - Shared secret / Group name - If selected, enter the shared secret string and group name in the 'Shared secret' and 'Local identifier' fields.
        - Hybrid Authentication - If you want use server side certificate for authentication in combination with the Shared secret/Group name authentication for a more secure connection, then select the 'Hybrid authentication' option..
    - Certificate - If you want client certificate type authentication, choose this option and configure the parameters as given below:
        - Password encryption - select this option if you want communications to be encrypted using the password as the key.
        - Prompt for VPN PIN - If selected, the user will be prompted to enter the VPN Pin while connecting.
        - On demand enabled - If selected, you can create rules for automatic establishment of the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.
        - Choose Certificate - The drop-down displays the certificates uploaded for the profile. Select the client certificate to be used for authentication. Refer to the explanation of adding certificates to the profile for more details. If a new certificate is to be added, click 'Add New' and upload the certificate.
        - Domain and Type fields - Allows you to add a list of domains and specify VPN connection type for each domain, if 'On demand enabled' is selected.
        - Enter a domain name in the domain field and choose the establishment type from the 'Type' drop-down.
            - Always establish - Initiates a VPN connection for the domain.
            - Never establish - No VPN connection will be established while accessing the domain.
            - Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails.
        - Click 'Add' to add the domain to the list

VPN Connection Type Settings - Table of Parameters	
	• Repeat the process to add more domains for On Demand VPN connection establishment rules. • To remove a domain, click 'X' beside it. For more details on variables, refer to the section Configuring Custom Variables.

Cisco AnyConnection, F5 SSL and Open VPN	• Override Primary - Make this connection override the primary server.
	• Remote Address - Enter the IP address or host name of the VPN server. You can add variables too, by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Auth Name - Enter the VPN account user name. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Authentication Method - Select the authentication method from the drop-down. The available options are:
	  • Shared secret / Group name - If selected, enter the shared secret string and group name in the 'Shared secret' and 'Local identifier' fields.
	  • Certificate - If you want client certificate type authentication, choose this option and specify the certificate to be used:
	  • Id Certificate - The drop-down displays the certificates uploaded for the profile. Select the client certificate to be used for authentication. Refer to the explanation of adding certificates to the profile for more details. If a new certificate is to be added, click 'Add New' and upload the certificate.
	• On demand enabled - If selected, you can create rules for automatic establishment of the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.
	  • Domain and Type fields - Allow you to add list of domains and specify VPN connection establishment type for each domain, if 'On demand enabled' option is selected.
	  • Enter a domain name in the domain field and choose the establishment type from the 'Type' drop-down.
	  • Always establish - Initiates a VPN connection for the domain.
	  • Never establish - No VPN connection will be established while accessing the domain.
	  • Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails.
	  • Click 'Add' to add the domain to the list
	  • Repeat the process to add more domains for On Demand VPN connection establishment rules.
	  • To remove a domain, click 'X' beside it.
	For more details on variables, refer to the section Configuring Custom Variables.

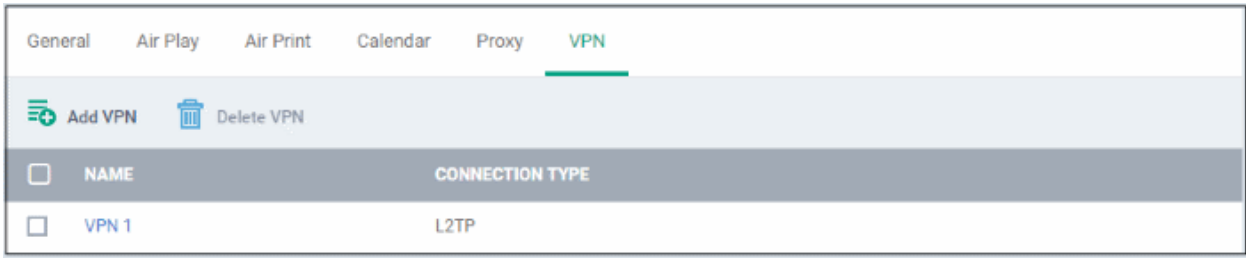
Juniper SSL	• Override Primary - Make this connection override the primary server.

VPN Connection Type Settings - Table of Parameters	

	• Remote Address - Enter the IP address or host name of the VPN server. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Auth Name - Enter the VPN account user name. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Realm - Enter the name of the authentication server. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Role - Enter the role of the user. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
	• Authentication Method - Select the authentication method from the drop-down. The available options are:
	  • Shared secret / Group name - If selected, enter the shared secret string and group name in the 'Shared secret' and 'Local identifier' fields.
	  • Certificate - If you want client certificate type authentication, choose this option and specify the certificate to be used:
	• Id Certificate - The drop-down displays the certificates uploaded for the profile. Select the client certificate to be used for authentication. Refer to the explanation of adding certificates to the profile for more details. If a new certificate is to be added, click 'Add New' and upload the certificate.
	• On demand enabled - If selected, you can create rules for automatic establishment of the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.
	  • Domain and Type fields - Allow you to add list of domains and specify VPN connection establishment type for each domain, if 'On demand enabled' option is selected.
	  • Enter a domain name in the domain field and choose the establishment type from the 'Type' drop-down.
	  • Always establish - Initiates a VPN connection for the domain.
	  • Never establish - No VPN connection will be established while accessing the domain.
	  • Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails.
	  • Click 'Add' to add the domain to the list
	  • Repeat the process to add more domains for On Demand VPN connection establishment rules.
	  • To remove a domain, click 'X' beside it.
	For more details on variables, refer to the section Configuring Custom Variables.

- Click the 'Save' button.

The VPN connection will be added to the profile.



You can add several VPN connection accounts to the profile.

- To add another VPN connection, click 'Add VPN' and repeat the process
- To view and edit the settings of a VPN connection, click its name
- To remove VPN connection, select it and click 'Delete VPN'

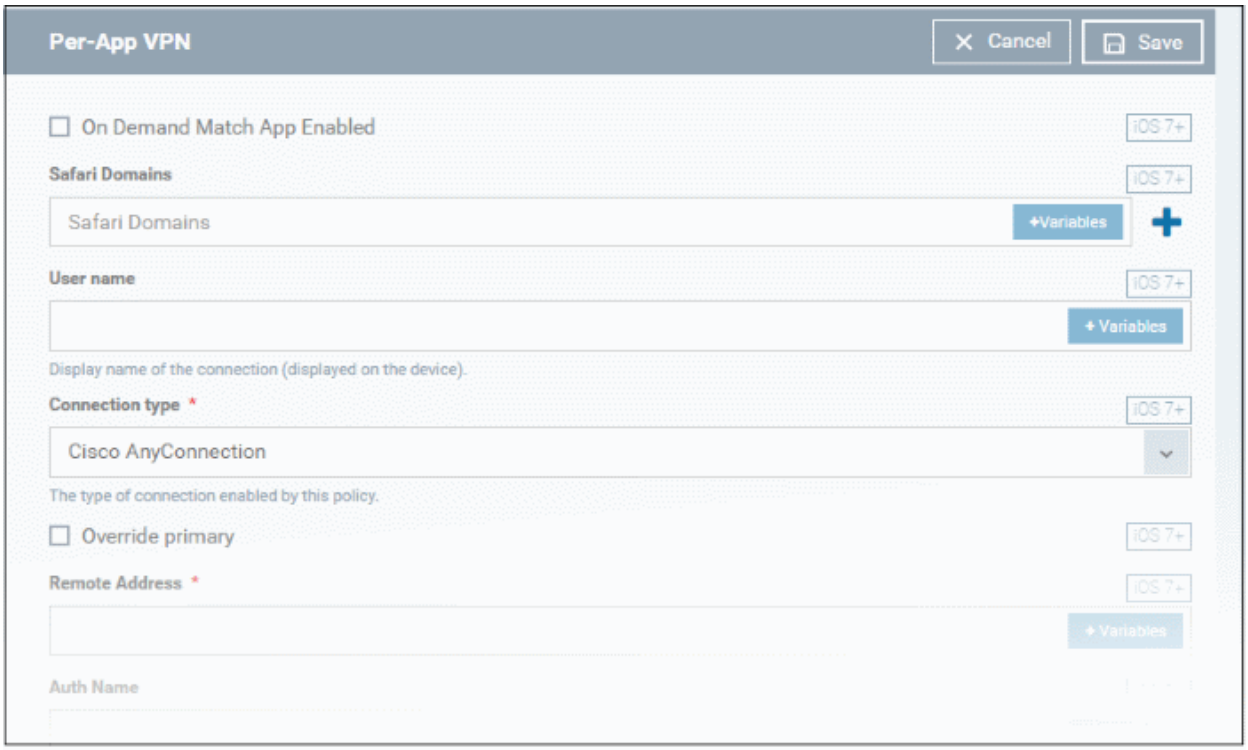
The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Per-App VPN settings

Note: If you would like to connect only certain apps to VPN, then this feature allows you to configure the settings. This feature is available for iOS 7 and later versions.

- Click 'VPN Per App' from the 'Add Profile Section' drop-down

The settings screen for VPN will appear.



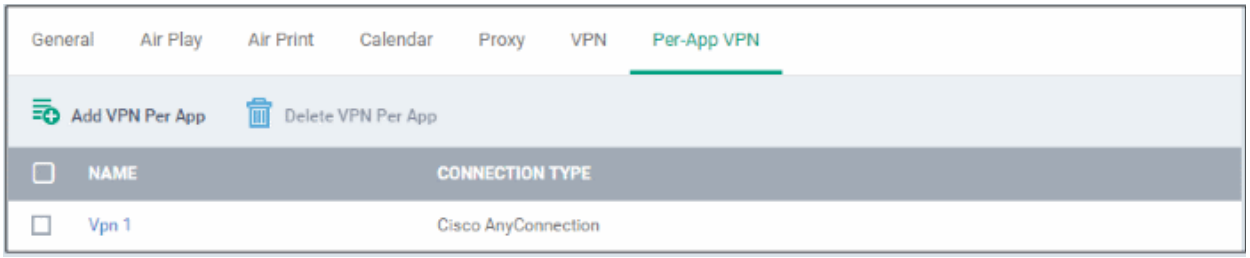
- **On Demand Match App Enabled** - Select this checkbox to enable per-app VPN connection.
- **Safari domains** - Allows you to add domains for which VPN connection has to be established, when visited through Safari browser. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom**

Variables. Click the button to add more domains in the field. If you want to remove a domain from the list, click the button beside it.

For details on other settings please refer to the section 'To configure VPN settings'.

- Click the 'Save' button.

The VPN per App settings for the specified VPN server will be saved and added to the list.



You can add multiple VPN servers for the profile.

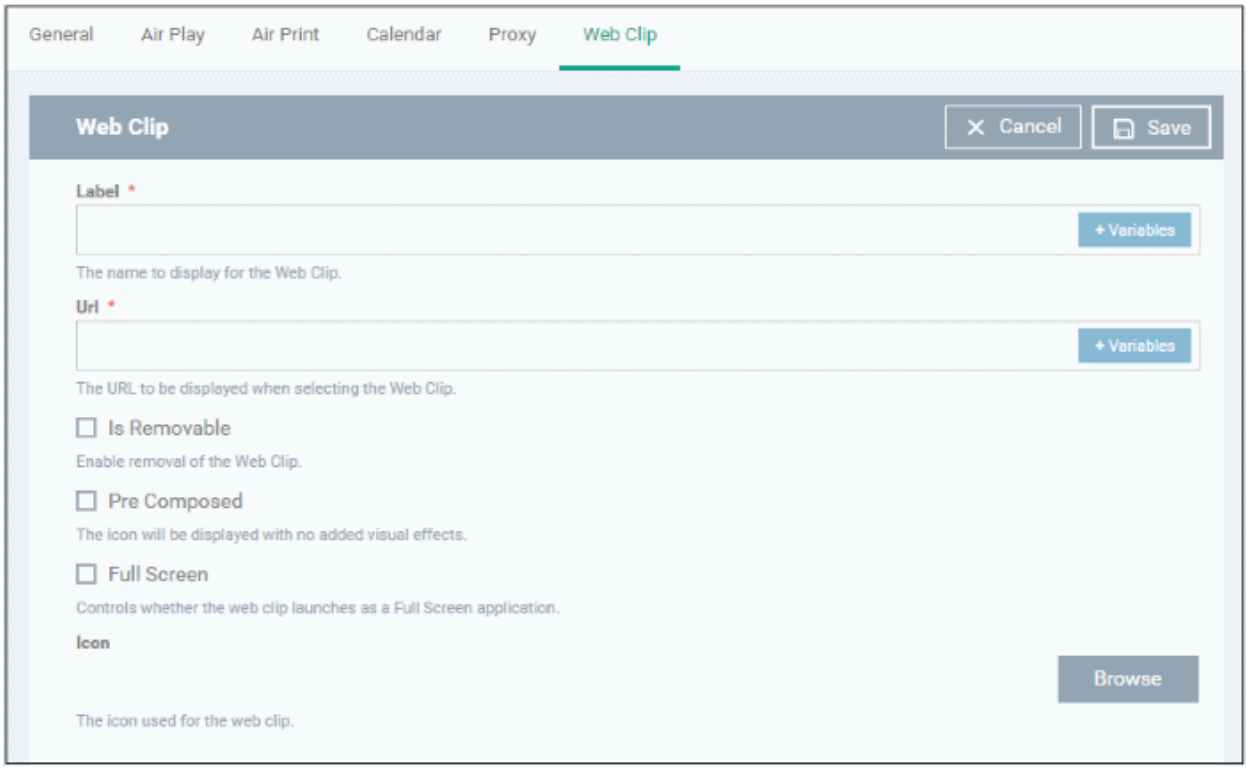
- To add another VPN server per App, click 'Add VPN Per App' and repeat the process
- To view and edit the settings of a VPN connection, click its name
- To remove VPN connection, select it and click 'Delete VPN Per App'

The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Web Clip settings

- Click 'Web Clip' from the 'Add Profile Section' drop-down

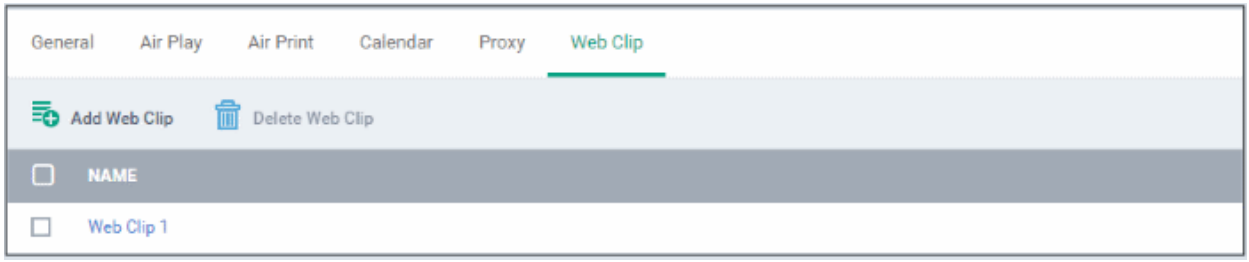
The 'Web Clip' settings screen will be displayed.



Web Clip Settings - Table of Parameters		
Form Element	**Type**	**Description**
Label*	Text Field	Enter the display name of the Web Clip. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
URL*	Text Field	Enter the URL to be displayed when Web Clip is opened. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Is Removable	Checkbox	If enabled, users can remove the Web Clip from their devices.
Pre Composed	Checkbox	If enabled, the Web Clip icon will be displayed with no added visual effects.
Full Screen	Checkbox	If enabled, the user can choose to view the Web Clip full screen mode.
Icon	Button	Upload the image to be used as icon for the Web Clip.

- Click the 'Save' button.

The WebClip will be added to the list.



You can add multiple web clips for a profile.

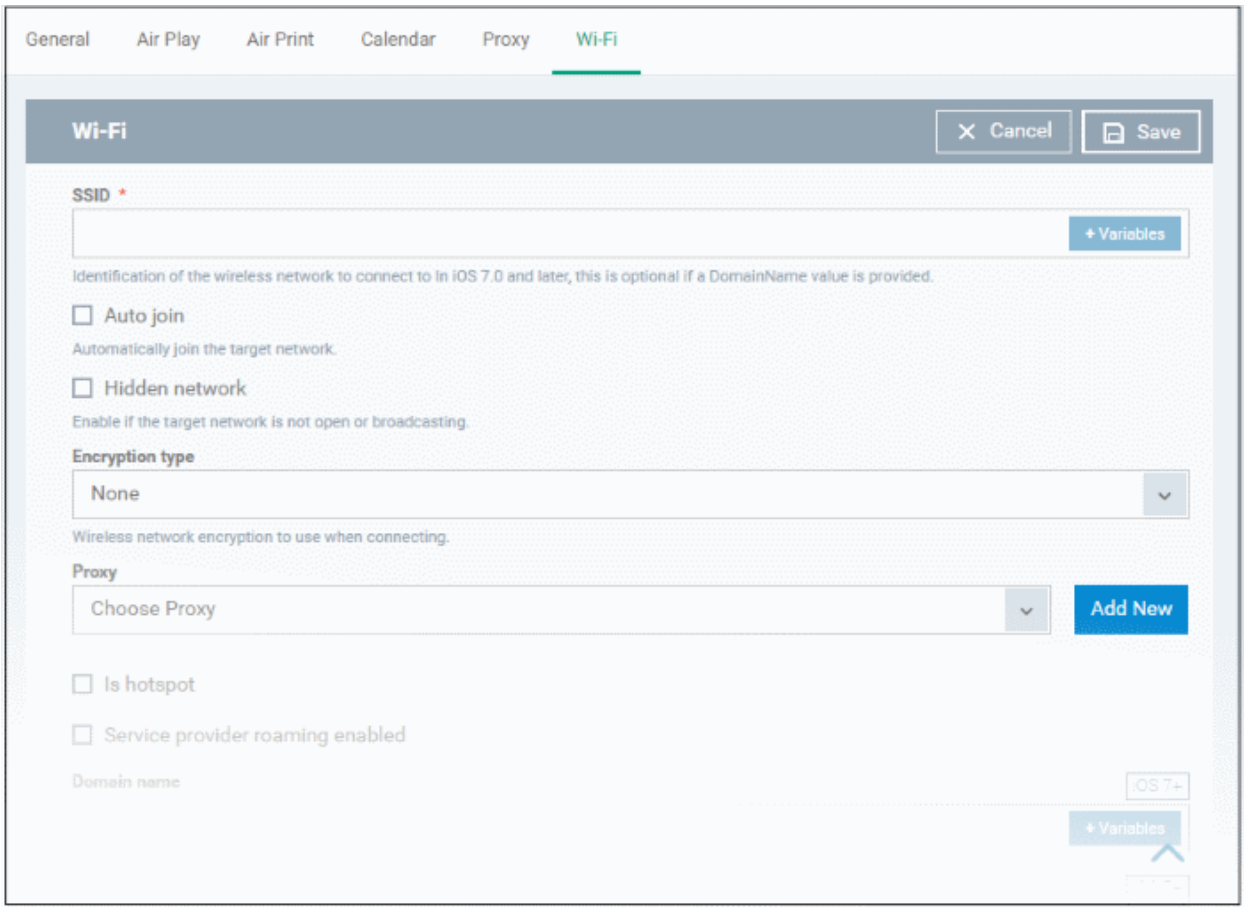
- To add another Web Clip, click 'Add Web Clip' and repeat the process
- To view and edit the settings for a web clip, click the name of it
- To remove a web clip, select it and click 'Delete Web Clip'

The settings will be saved and displayed under the 'Web Clip' tab. You can add more web clips and edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Profile Section' drop-down

The 'Wi-Fi' settings screen will be displayed.



Wi-Fi Settings - Table of Parameters		
Form Element	**Type**	**Description**
SSID*	Text Field	Enter a unique identifier (Service Set Identifier) of a wireless network that the device should connect to. Note: In iOS 7 and later versions, this is optional if Domain Name value is provided.
Auto Join	Checkbox	If enabled, devices will automatically connect to the configured wireless network.
Hidden Network	Checkbox	Select this option if the specified wireless network is hidden and not visible to Wi-Fi scans.
Encryption Type	Drop-down	Select the type of encryption used by the wireless network from the drop-down. The options available are: • None • WEP • WPA / WPA2 • Any • WEP Enterprise

		• WPA / WPA2 Enterprise • Any (Enterprise) The Password field will appear if any of the options, WEP, WPA / WPA2 and Any (Personal) are chosen. If any of the Enterprise encryption type is chosen, then select the supported protocols and configure authentication. The options available are: TLS, LEAP, TTLS, PEAP, EAP-FAST, Use Pac, Provision pac and Provision Pac Anonymously, PAP, CHAP, MS CHAP ans MS CHAP V2
Password	Text Field	Enter the password to connect to the Wi-Fi network. If left blank, the user will be prompted to enter the password when the device attempts to connect to the network.
Proxy	Drop-down	Select the proxy settings for the wireless network from the drop-down. To include more proxies, click the 'Add New' beside the field. The 'Create New Proxy' dialog will be displayed. Enter the proxy name in the 'Name' field. 'The options available for proxy type are: • None • Manual • Auto If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields and click the 'Create' button. If you select 'Auto', enter the URL of the Proxy Pac and click the 'Create' button.
Is Hotspot	Checkbox	If enabled, the network is treated as a hotspot.
Service Provider Roaming Enabled	Checkbox	If enabled, devices can connect to roaming service providers.
Domain Name	Text Field	Enter the domain name used for Wi-Fi hotspot to which the devices have to connect. This is optional and can be provided instead of Service Set Identifier. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Note: This feature is available for iOS 7 and later versions.
Displayed Operator Name	Text Field	Enter the network operator name that will be displayed in the devices. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. Note: This feature is available for iOS 7 and later versions.
Roaming Consortium OIs	Text Field	Enter the Roaming Consortium Organization Identifier of the service provider to which the devices will connect to. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. To removed the field, click the button beside it. Click the button to add Roaming Consortium OIs fields.

		Note: This feature is available for iOS 7 and later versions.
NAI Realm Names	Text Field	Enter the Network Access Identifier (NAI) realm names used for Wi-Fi hotspot 2.0. You can add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables. To remove the field, click the beside it. Click the button to add more NAI Realm Names. Note: This feature is available for iOS 7 and later versions.

- Click the 'Save' button.

The Wi-Fi network will be added to the list.

You can add multiple Wi-Fi networks to the profile.

- To add another Wi-Fi network, click 'Add Wi-Fi' and repeat the process
- To view and edit the settings of a Wi-Fi network, click on the SSID of it
- To remove a Wi-Fi network, select it and click 'Delete Wi-Fi'

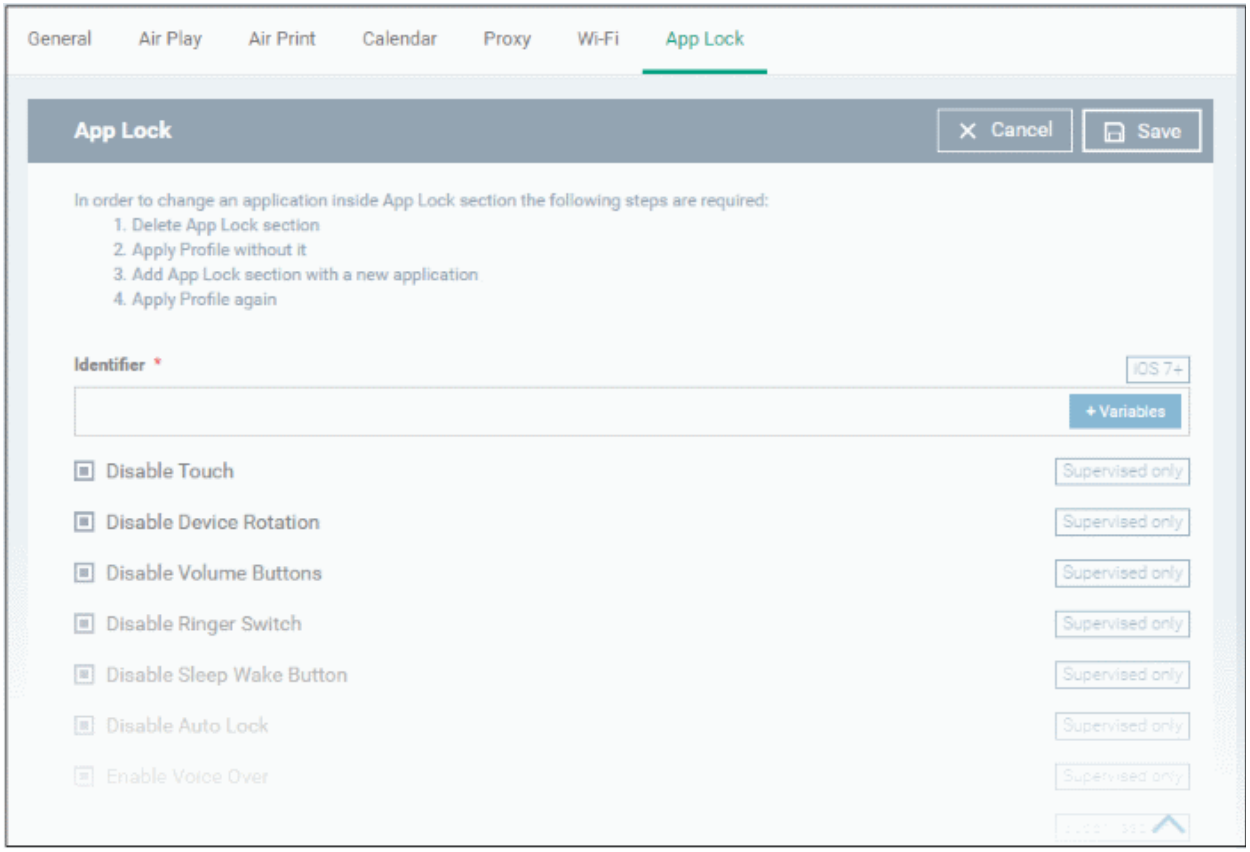
The settings will be saved and displayed under the Wi-Fi tab. You can edit the settings, add or remove Wi-Fi networks or remove the Wi-Fi networks at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

To configure App Lock settings

Tip: The 'App Lock' section allows you to restrict the ability of specific applications to use device resources. You can add only one application with app restriction settings for a profile. To have impose restrictions on several applications, create a profile for each and apply those profiles to the managed devices, as required.

- Click 'App' from the 'Add Profile Section' drop-down

The 'App Lock' settings screen will be displayed.



App Lock Settings - Table of Parameters		
Form Element	**Type**	**Description**
Identifier	Text field	Allows administrators to specify the app to be included in the App Lock section of the profile. You can specify an Apple iTunes Store App or Enterprise App. • Enter the App ID of the application to be included in the profile, with the app restrictions. For more details on getting the App ID of an application, refer to the **explanation** given below this table. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section **Configuring Custom Variables**. **Note**: This feature is available for iOS 7 and later versions only.
Disable Touch	Checkbox	Touch screen inputs will be disabled for the app.
Disable Device Rotation	Checkbox	The app will not be able to change display orientation.
Disable Volume Buttons	Checkbox	The app will not be able to modify device volume.
Disable Ringer Switch	Checkbox	Inputs through the ringer switch will be disabled for the app.
Disable Sleep Wake Button	Checkbox	Inputs through the power/lock/wake button will be disabled for the app.
Disable Auto Lock	Checkbox	The device will not auto-lock when this app is running.

App Lock Settings - Table of Parameters		
Enable Voice Over	Checkbox	Allows the user to use the voice over feature on the device for this app.
Enable Zoom	Checkbox	Allows the user to zoom-in/zoom-out the display for this app
Enable Invert Colors	Checkbox	Allows the user to invert the colors for the display screens of this app.
Enable Assistive Touch	Checkbox	Allows the user to use the 'Assistive Touch' feature on the device for this app.
Enable Speak Selection	Checkbox	Allows the user to use the 'Speak Selection' feature on the device for this app.
Enable Mono Audio	Checkbox	Allows the user to choose mono mode for audio output of this app.
Voice Over	Checkbox	Automatically switches ON the 'Voice Over' feature for the app.
Zoom	Checkbox	Automatically switches ON the 'zoom-in' feature for the app.
Invert Colors	Checkbox	Automatically switches ON the 'Invert Colors' feature when the app is used.
Assistive Touch	Checkbox	Automatically switches ON the 'Voice Over' feature when the app is used.

- Click Save after configuring the parameters and options

The settings will be saved and displayed under 'App Lock' tab. You can edit the settings or remove the 'App Lock' section from the profile at anytime Refer to the section '**Editing Configuration Profiles**' for more details.

Obtaining App Identifier

For App Store Application:

The App ID can be obtained from the iTunes Store download URL of the app. The general format of the download URL is:

http://itunes.apple.com/<country>/app/<name of the app>/id<**App ID**>?mt=8.

The number string that follows 'id' in the URL gives the App ID.

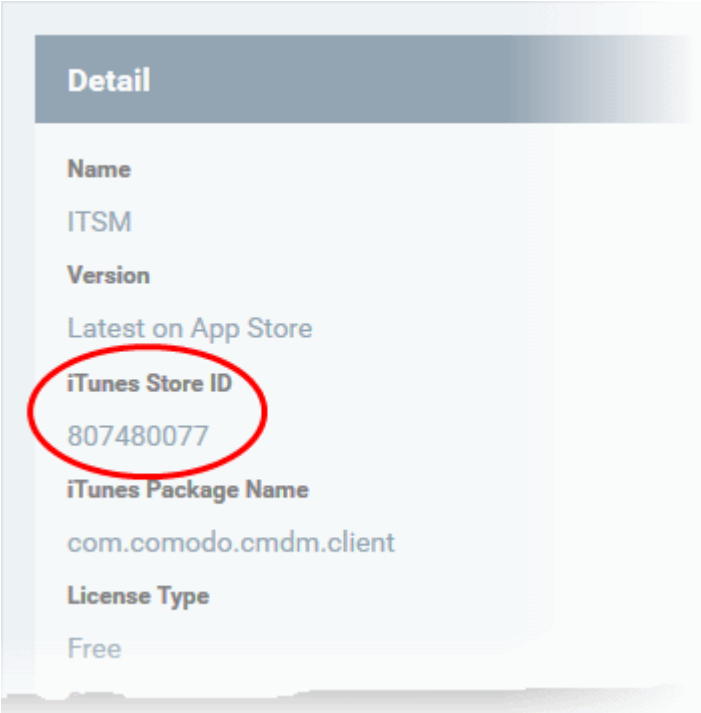
Example:

The download URL of the ITSM client from the iTunes store is https://itunes.apple.com/us/app/cmdm/id**807480077**?mt=8. The App ID of the application is 807480077.

For Enterprise Application:

The App ID can be viewed from the App Details screen of the App.

- Click 'App Store' from the left and choose 'iOS'
- Click on the app from the list displayed at the right



The App ID is displayed in the 'iTunes Store ID' field.

6.1.3. Profiles for Windows Devices

Windows profiles allow you to specify security settings for Comodo Client Security (CCS) installed on managed Windows devices.

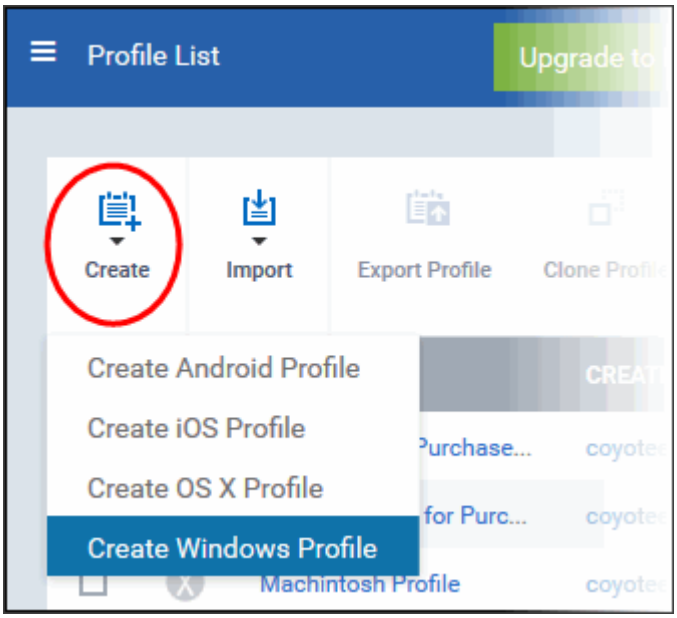
Security profiles for Windows endpoints can be added to ITSM in two ways:

- Create a profile by configuring CCS settings in the ITSM interface. Refer to **Creating Windows Profiles** for more details.
- Import a profile from a managed endpoint which is already running CCS, or import from a stored configuration profile (.cfg file). Refer to the section **Importing Windows Profiles** for more details.

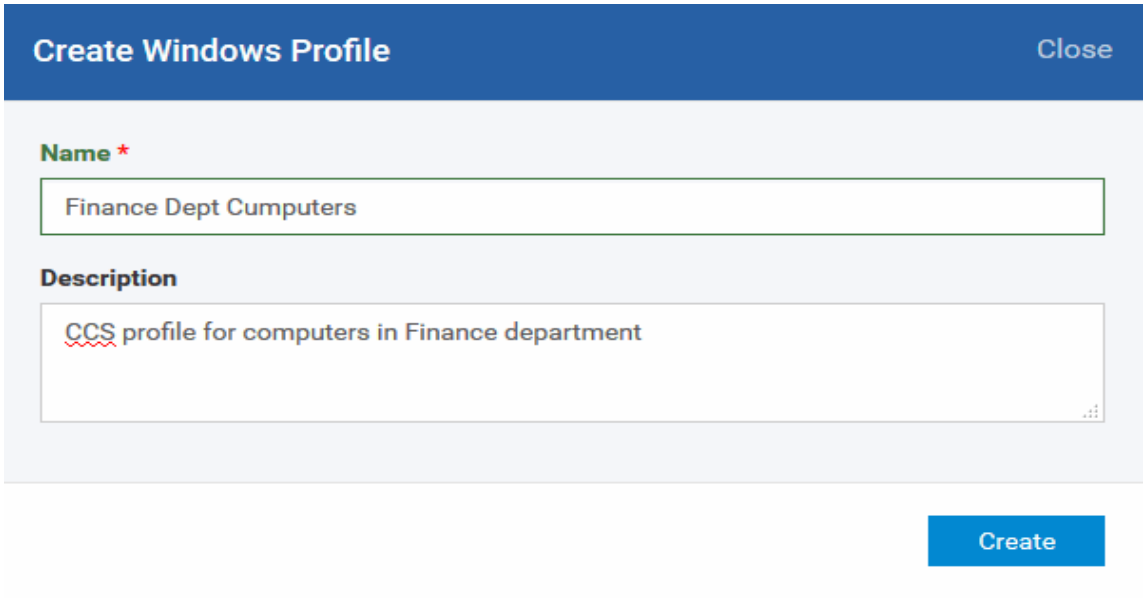
6.1.3.1. Creating Windows Profiles

To create a new Windows profile

- Click 'Configuration Templates' on the left then 'Profiles'
- Click 'Create' then select 'Create Windows Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profiles' screen.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Profile Section' button. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices and device groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.
- This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.
- To create a new profile, click 'Configuration Templates > Profiles > Create':

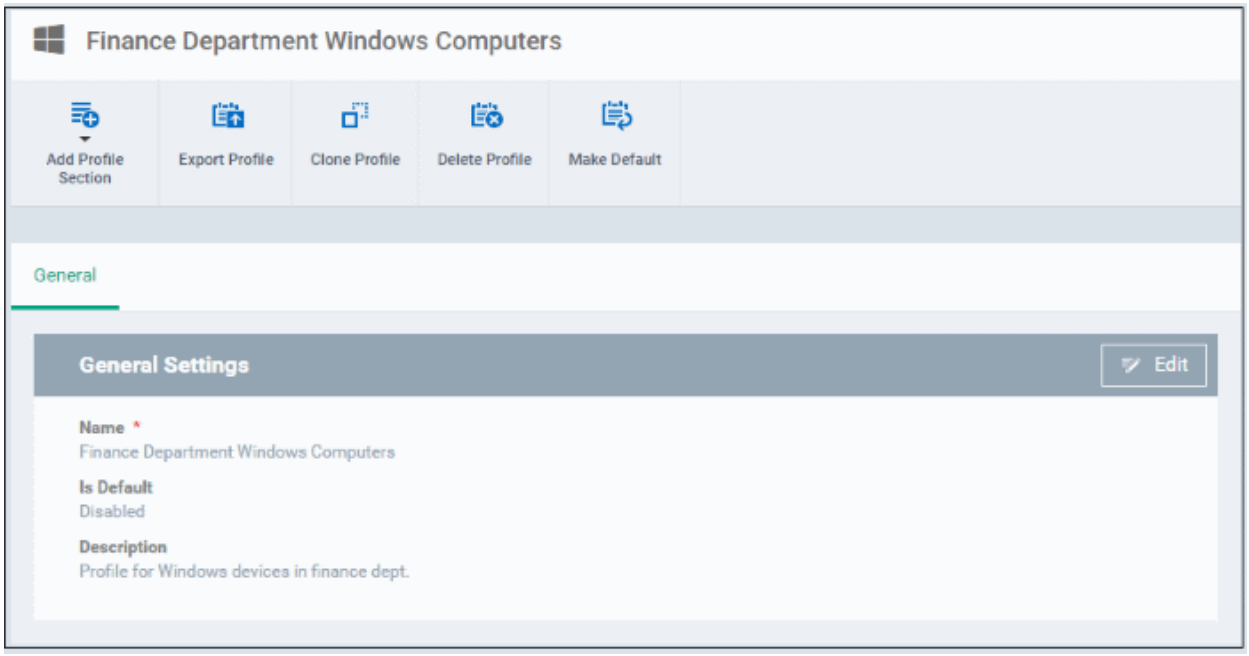


The 'Create Windows Profile' screen will be displayed.



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

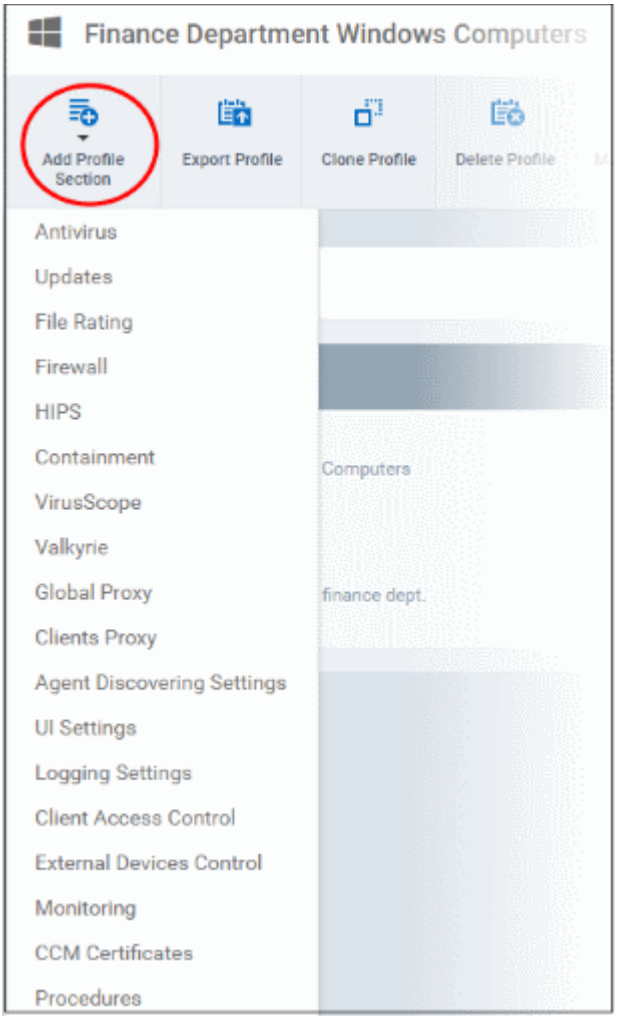
The Windows profile will be created and the 'General Settings' section will be displayed. The new profile is not a 'Default Profile' by default.



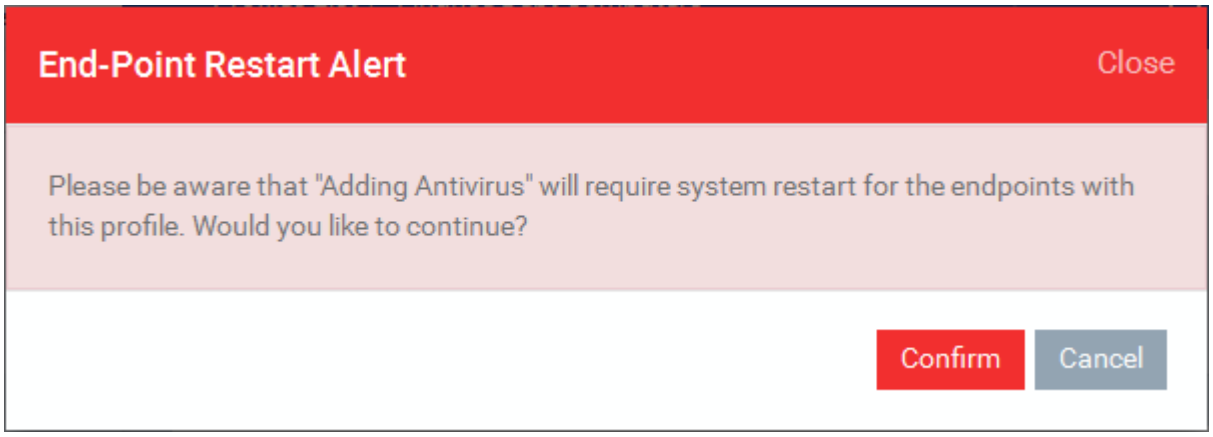
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

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

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

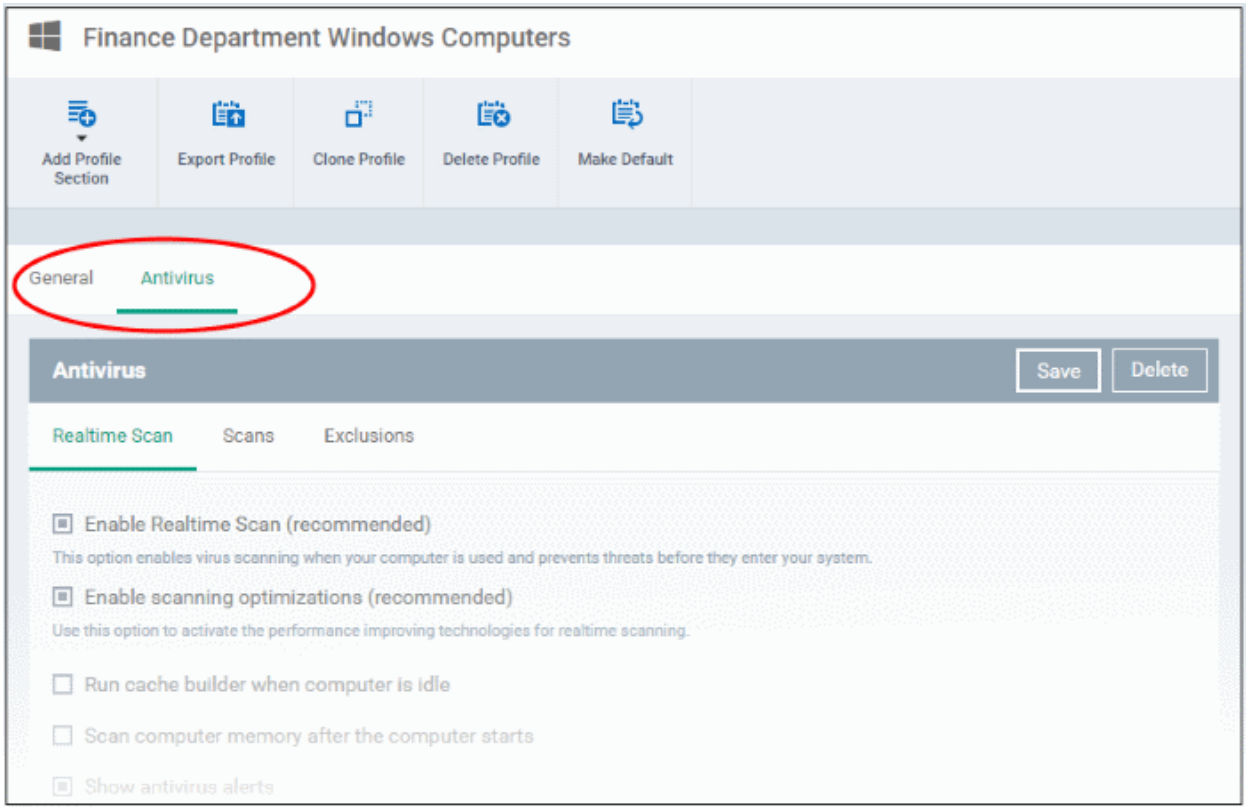


If the changes in the configuration of the component requires the restart of the endpoint to which the profile is applied, an alert dialog will be displayed.



- Click 'Confirm' to continue.

The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top.



Following sections explain more about each of the settings:

- Antivirus
- Update Settings
- File Rating
- Firewall
- HIPS
- Containment
- VirusScope
- Valkyrie
- Global Proxy
- Clients Proxy
- Agent Discovery Settings
- UI Settings
- Logging Settings
- Client Access Control
- External Devices Control
- Monitoring
- CCM Certificates
- Procedures

6.1.3.1.1. Antivirus Settings

The Antivirus setting screen has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe) for the profile.

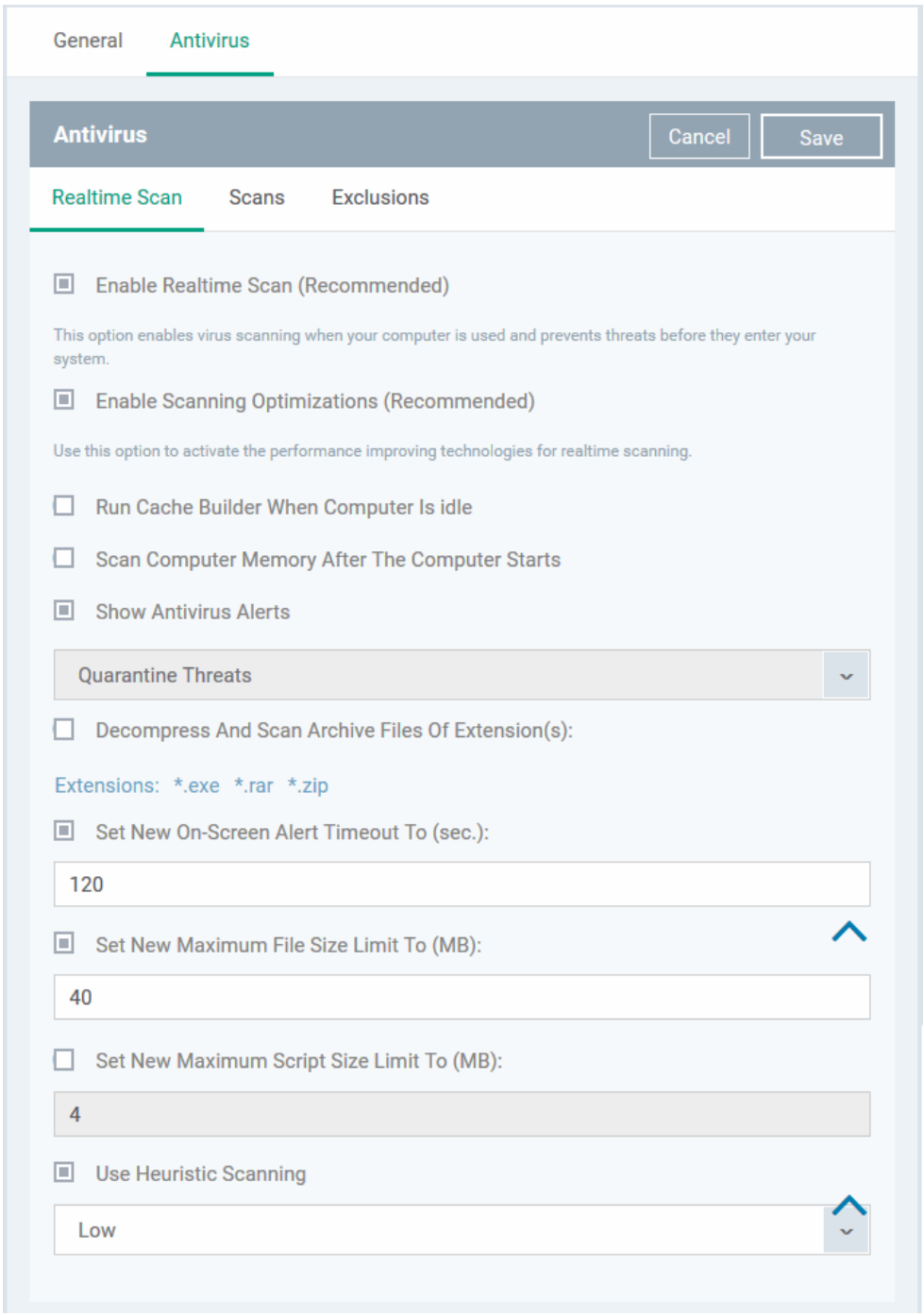
To configure Antivirus settings

- Choose 'Antivirus' from the 'Add Profile Section' drop-down

The settings screen for Antivirus will be displayed.

- **Real Time Scan** - To set the parameters for on-access scanning
- **Scans** - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans
- **Exclusions** - To add items to be skipped on Antivirus scans at the devices, to which the profile is applied.

Realtime Scan Settings



Realtime Scan Settings - Table of Parameters	
Form Element	**Description**
Enable Realtime Scan	The Real time Scanning (aka 'On-Access Scanning') is always ON protection for checking files in real time when they are created, opened or copied. (as soon as a user interacts with a file, CCS checks it). This instant detection of viruses assures the user, that the system is perpetually monitored for malware and enjoys the highest level of protection. • Choose whether of not to enable real time scanning.
Enable Scanning Optimizations	CCS will employ various optimization techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process. • Choose whether of not to enable scanning optimizations.
Run cache builder when computer is idle	The CCS installation at the device runs the Antivirus Cache Builder whenever the computer is idle to boost real-time scanning
Scan computer memory after the computer start	Select this option to run the antivirus scan on the system memory during system start-up of the endpoint
Show antivirus alerts	Allows you to configure whether or not to show antivirus alerts at the endpoints, when malware is encountered. Deselecting 'Show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CCS should automatically take - either 'Block Threats' or 'Quarantine Threats'. • Quarantine threats - Moves the detected threat(s) to quarantine for your later assessment and action. • Block threats - Stops the application or file from execution, if a threat is detected in it.
Decompress and scan archive files of extensions	CCS can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is selected. CCS generates an alert even on the presence of viruses in compressed files before the end-user opens them. On selecting the option, you can add the archive file types that should be decompressed and scanned by clicking file types that are displayed below it and adding the new file types from the 'Extensions' dialog.
Set new on-screen alert timeout to (secs)	Select the option to set the time period (in seconds) for which the alert message should stay on the screen at the endpoint. (Default = 120 seconds)
Set new maximum file size to (MB)	Select the option to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here will not be not scanned. (Default = 40 MB)
Set new maximum script size limit to (MB)	Select the option to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here are not scanned. (Default = 4 MB)
Use heuristics scanning	Allows you to enable or disable Heuristics scanning and define scanning level. If enabled, you can select the level of Heuristic scanning from the drop-down: • Low - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo

	recommends this setting for most users. (Default) • Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives. • High- Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too. **Background Note**: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or moves it to quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. It allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

- Click the 'Save' button at the bottom.

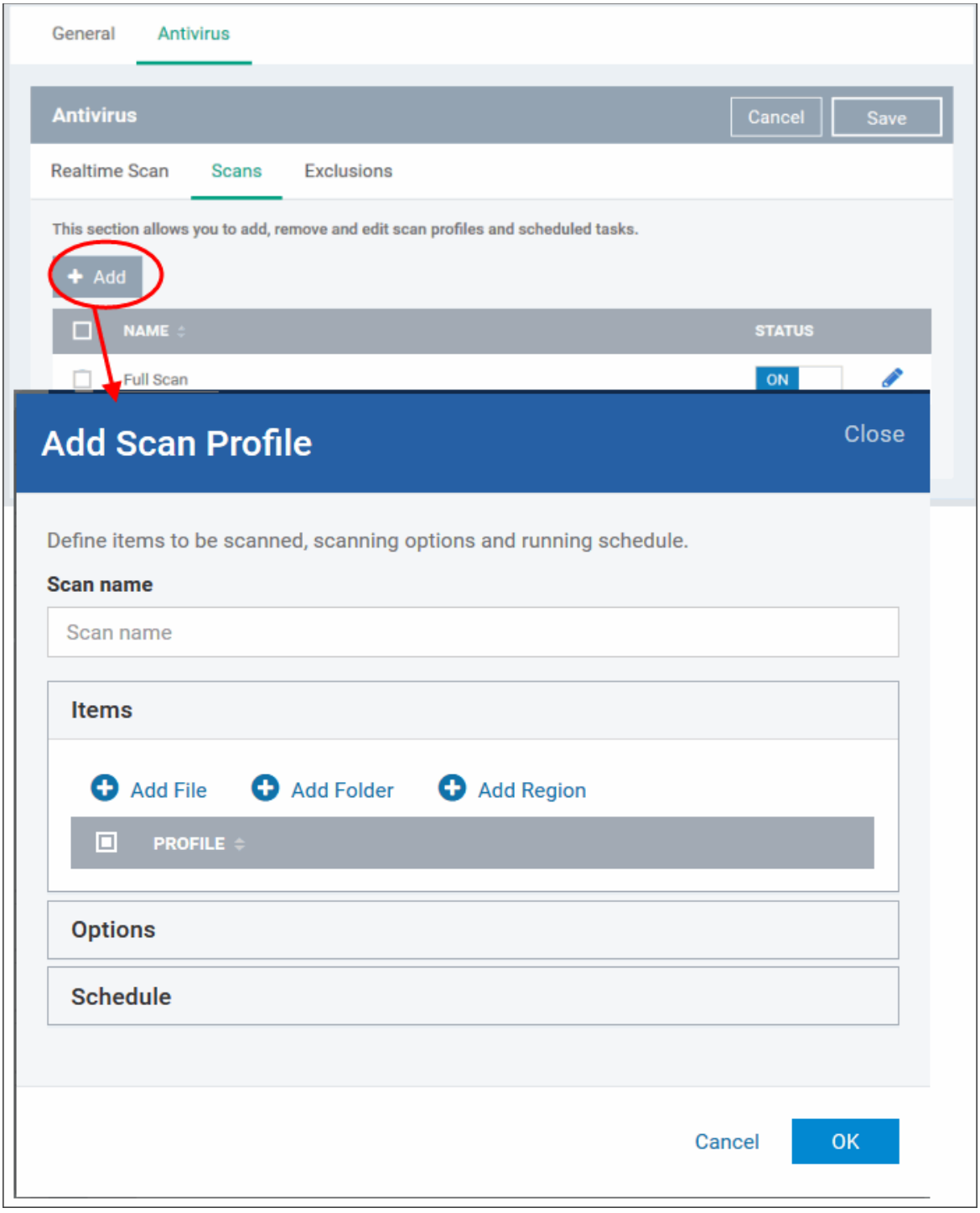
Custom Scans

The 'Scans' pane allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CCS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To create a custom scan profile

- Click the 'Add' button in the Scans screen



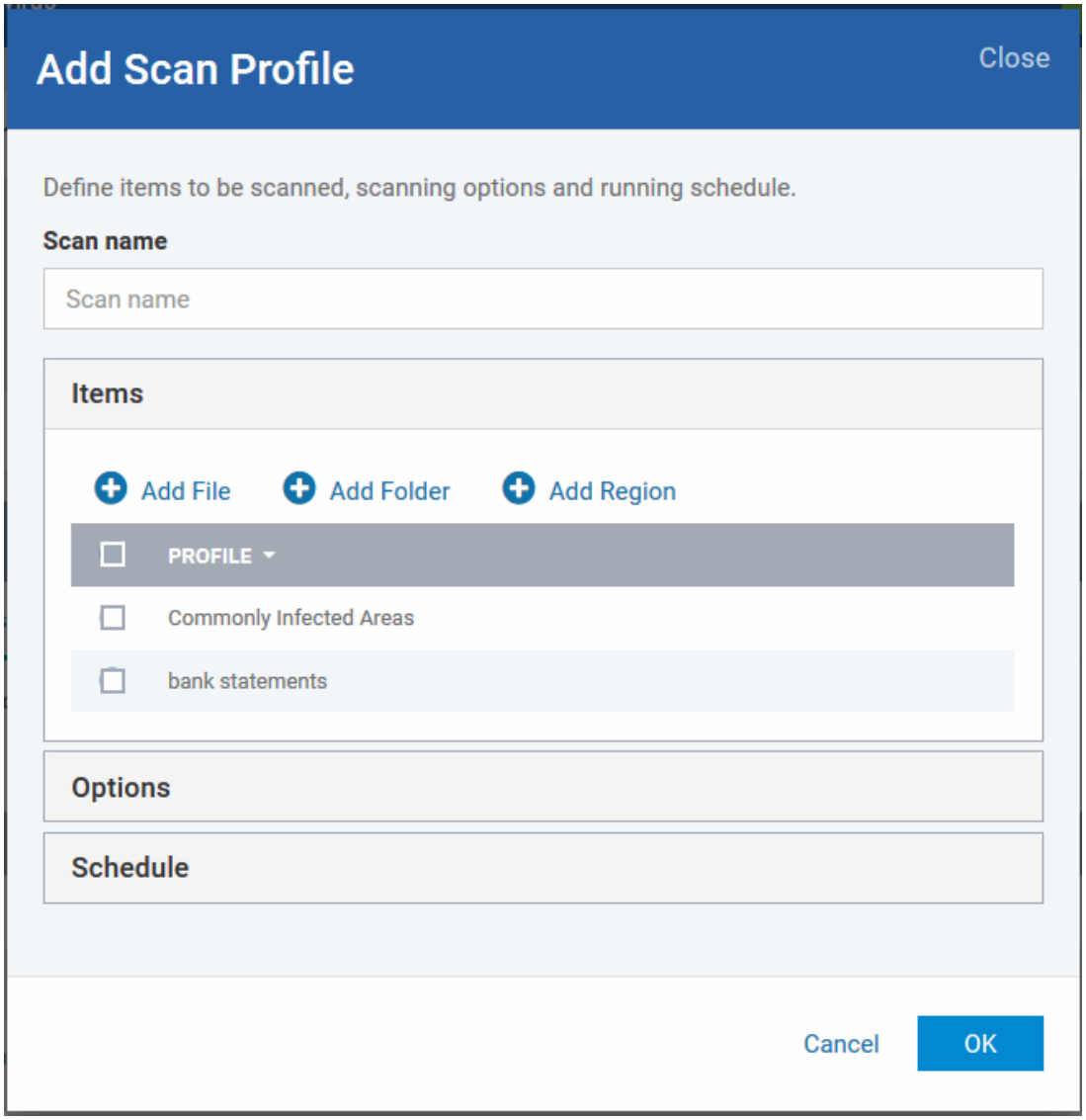
The 'Add Scan Profile' dialog will be displayed.

- Enter the name of the custom scan in the 'Scan name' field

By default, the 'Items' section will be displayed allowing you to specify the file name, folder and region to be included in the custom scan profile.

- Add File - Allows you to add a specific file or you can also choose to add files with the same extension using the wildcard character
- Add Folder - Allows you to add a folder name
- Add Region - Allows you to add predefined regions to the profile. For example, 'Entire Computer', 'Commonly Infected Areas' and 'Memory'.

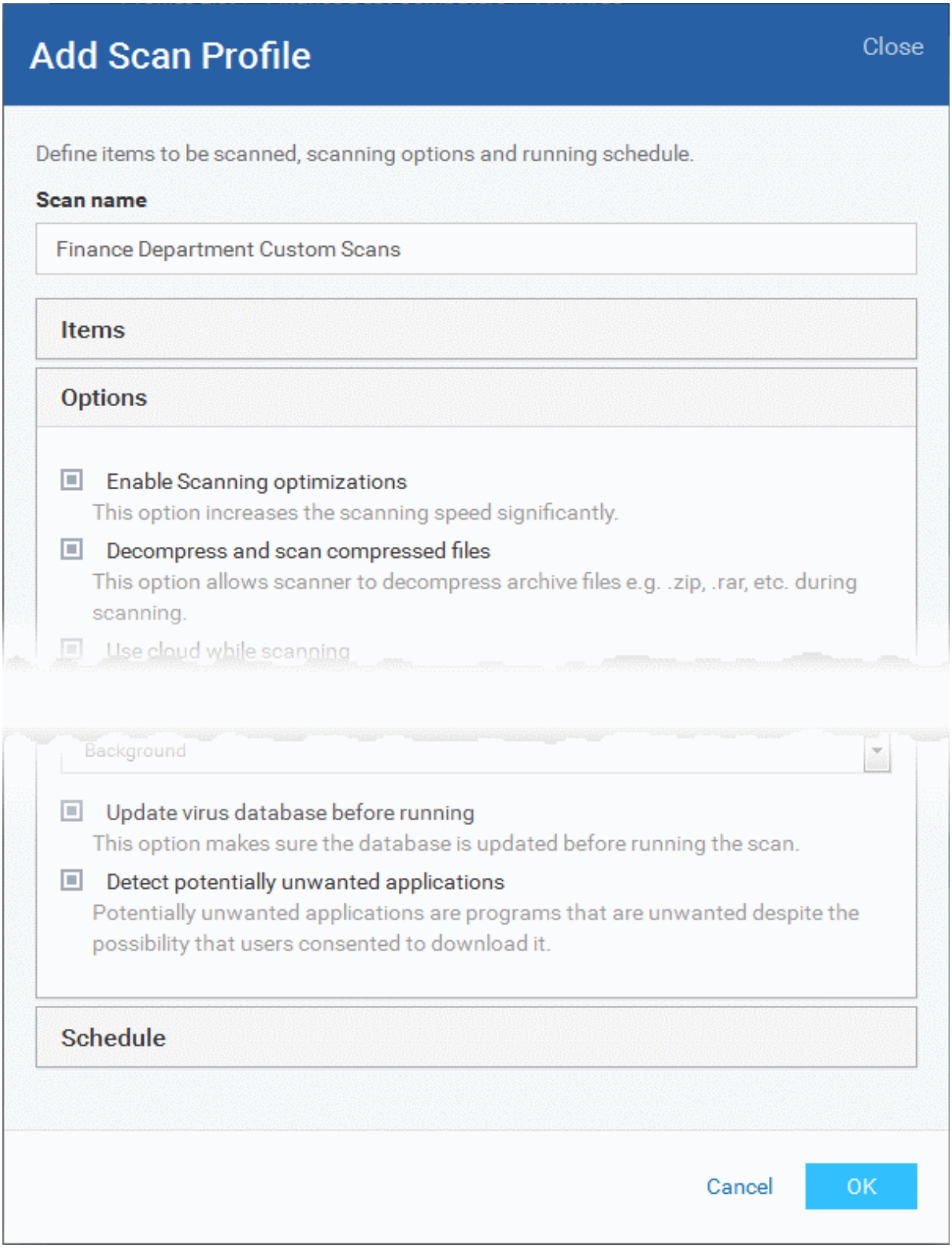
The entered/selected items will be displayed.



- To remove an item from the list, select it and click 'Remove'.

The next step is to define how the selected items should be scanned.

- Click 'Options'


Add Scan Profile
Close
Define items to be scanned, scanning options and running schedule.
Scan name
Finance Department Custom Scans
Items
Options
Enable Scanning optimizations
This option increases the scanning speed significantly.
Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning.
Use cloud while scanning
Background
Update virus database before running
This option makes sure the database is updated before running the scan.
Detect potentially unwanted applications
Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download it.
Schedule
Cancel
OK

Options Configuration - Table of Parameters	
Form Element	**Description**
Enable scanning optimizations	On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (***Default = Enabled***) .
Decompress and scan compressed files	When this option is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***).
Use cloud while scanning	Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is out-dated. (***Default = Disabled***).
Automatically clean threats	On selecting this option, CCS will automatically take action against the threats detected at the end of the scan, instead of showing the results screen with a list of threats identified. You can choose the action to be taken from the drop-down. The available options are: • Disinfect • Quarantine (***Default = Enabled with Disinfect Threats option***)
Show scan results window	If enabled, the results window for AV scans that are run automatically from schedule as well as for on-demand scans that are executed from ITSM will be displayed. ***(Default = Disabled)***
Use heuristics scanning	Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. (Default = Disabled). Background Info: Comodo Client Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This allows CCS to 'predict' the existence of new viruses - even if it is not contained in the current virus database. • **Low** - Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. • **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives. • **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
Limit maximum file size to	Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected (Default = 40 MB).

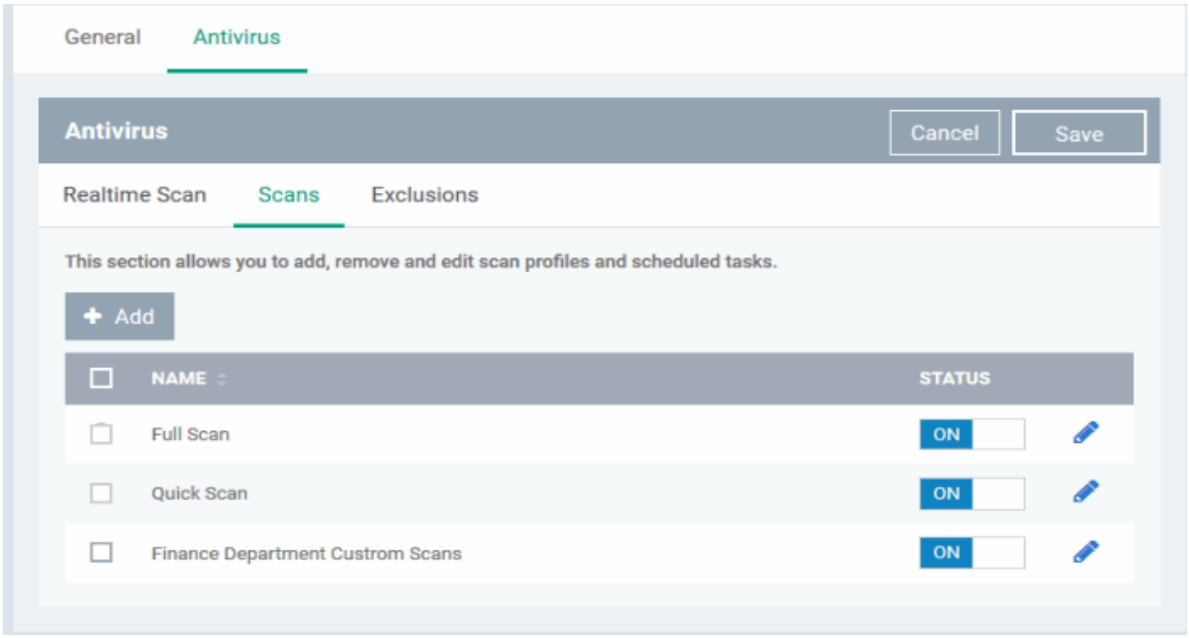
Options Configuration - Table of Parameters	
Run this scan with	Enables you to set the priority of the scanning from High to Low and to run at background. (Default = Enabled)
Update virus database before running	Selecting this option makes CCS to check for virus database updates and if available, update the database before commencing the scan. (Default = Enabled).
Detect potentially unwanted applications	When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (Default = Disabled).

The next step is to schedule when the custom scan should be run.

- Click 'Schedule'

Schedule Settings - Table of Parameters	
Form Element	**Description**
Frequency	• **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning • **Every Day** - Runs the scan every day at the time specified • **Every Week** - Scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them. • **Every Month** - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
Run only when computer is not running on battery	This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
Run only when computer is IDLE	Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
Turn off computer if no threats are found at the end of the scan	Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.

- Click 'OK' to save the custom scan settings



The added will be listed in the screen.

- Click the toggle switch under the 'Status' column beside the respective profile row to toggle between on and off status. The scan will be run only if it is enabled for the profile.
- To change the settings for the custom scan, click the edit button , edit the parameters and click 'OK'
- To remove a custom scan from the list, select it and click 'Remove'

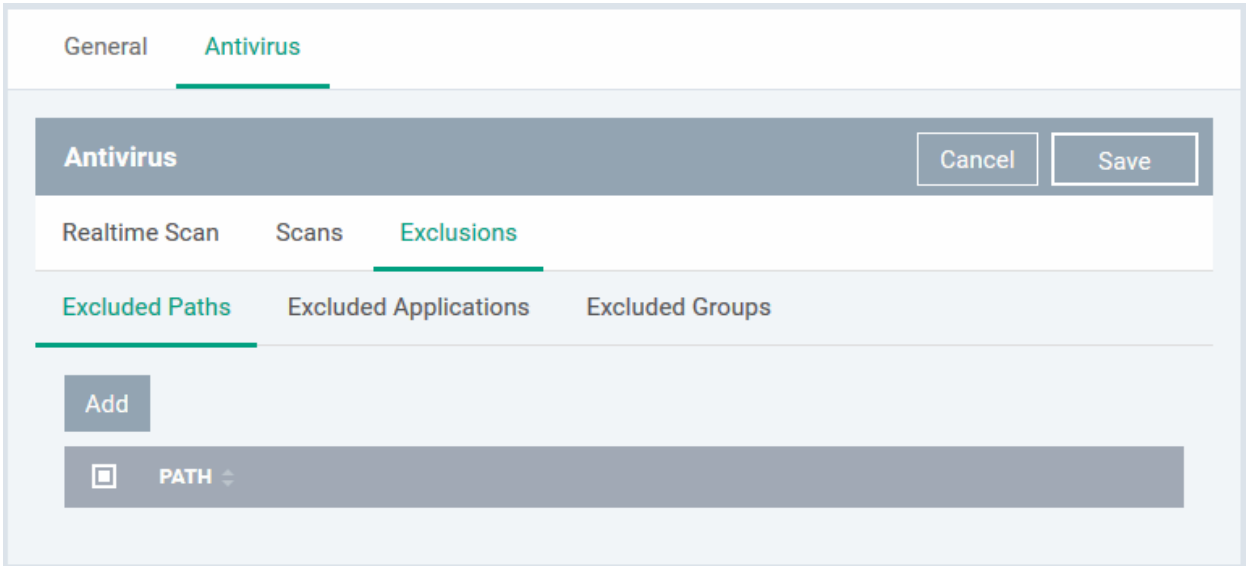
Exclusions

The 'Exclusions' screen under the Antivirus setting has three sub sections that allow you to add a list of paths, list of applications/files and 'File Groups' which should be excluded from the antivirus scan.

- Click 'Exclusions'

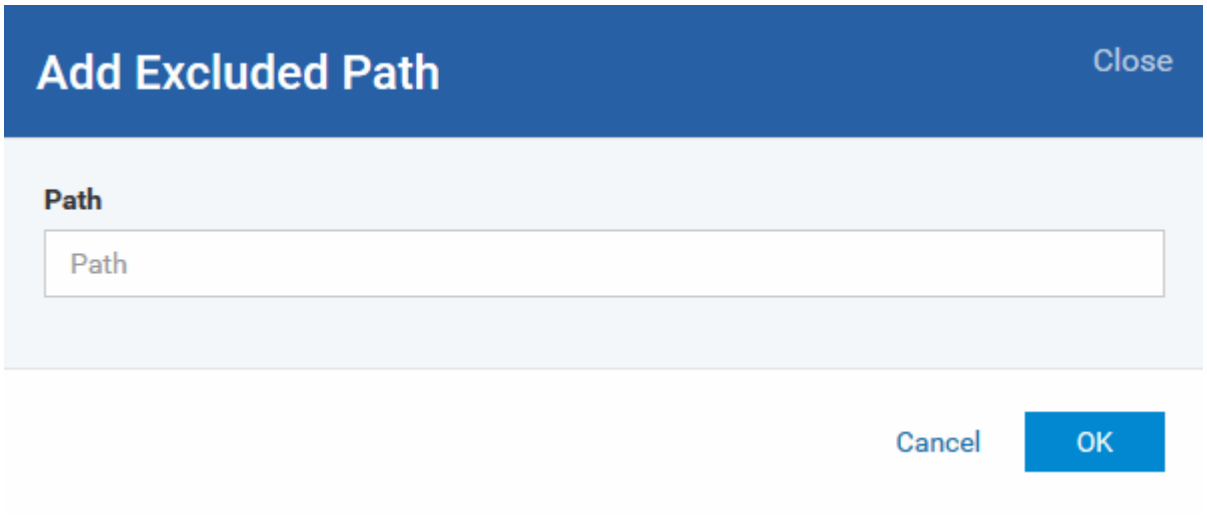
To add excluded paths

By default the 'Excluded Paths' screen will be displayed:



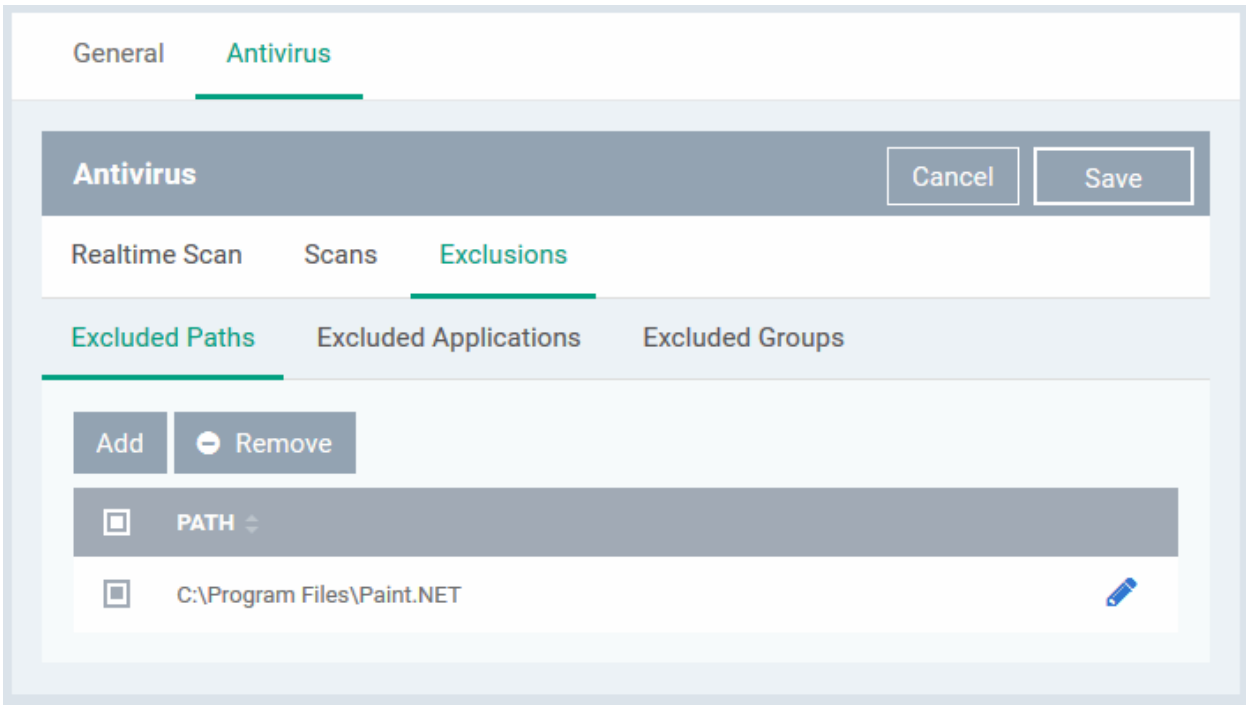
- Click 'Add'

The 'Add' dialog will be displayed:



- Enter the full path that should be excluded from scanning and click 'OK'.

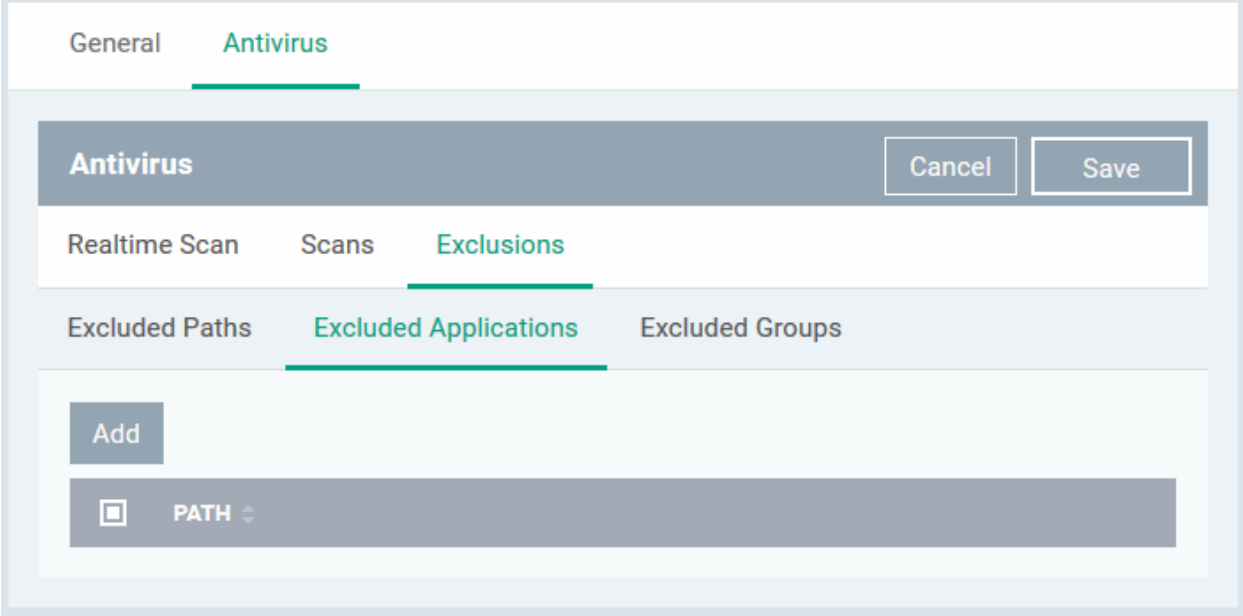
The added excluded path will be added to the list.



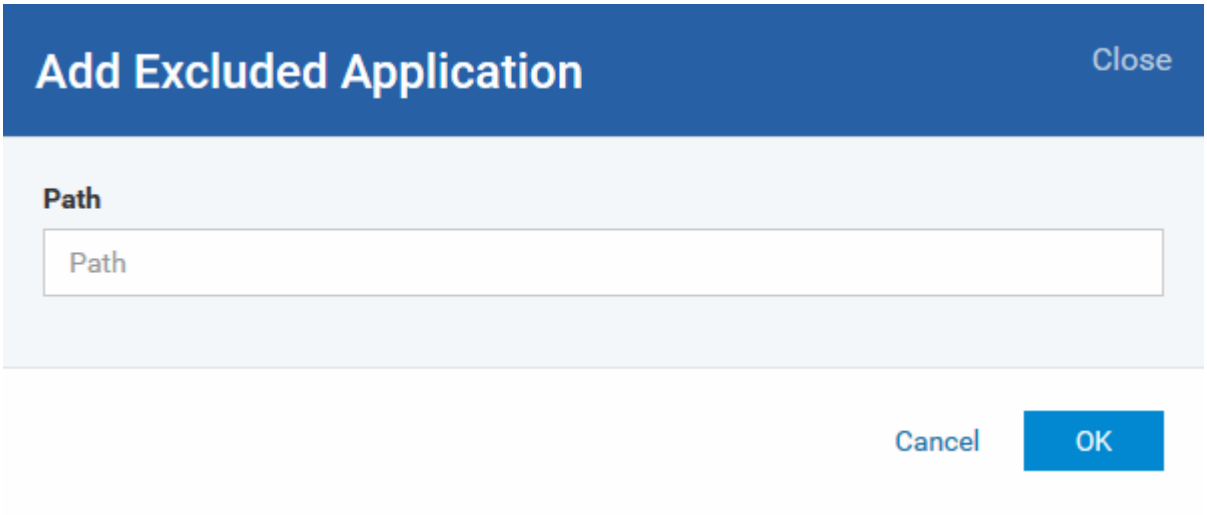
- Repeat the process to include more paths
- To change the path, click the edit button , edit the parameters and click 'OK'
- To remove a path from the list, select it and click 'Remove'

To add excluded applications

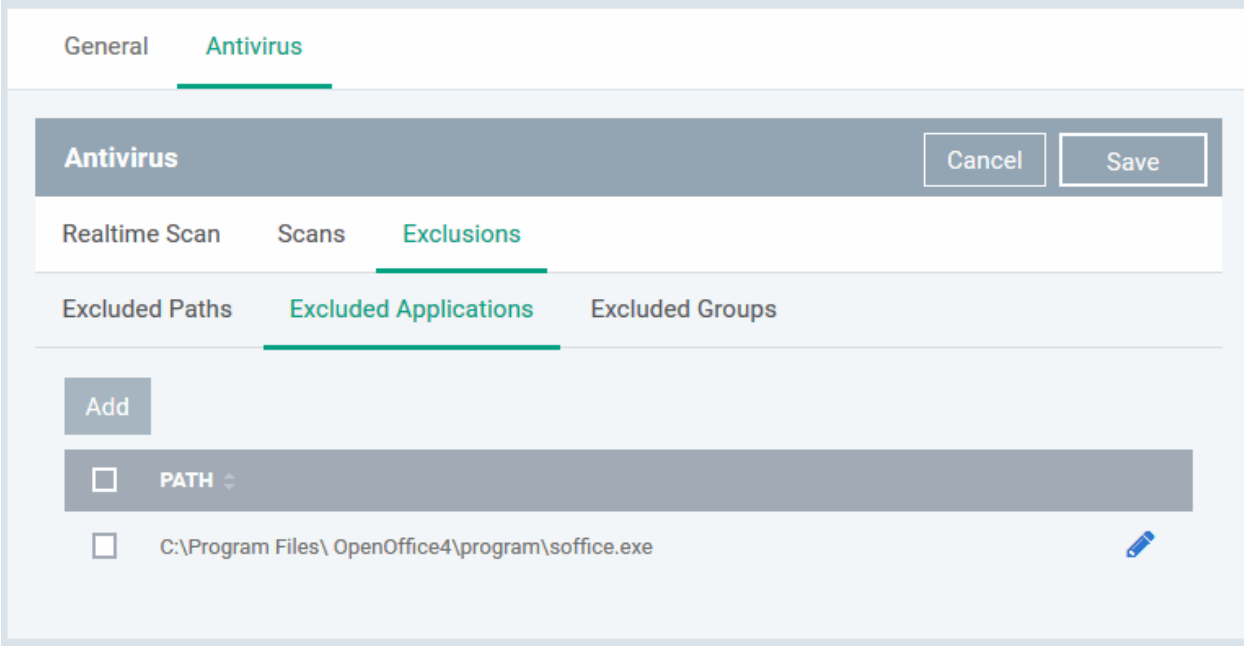
- Click 'Excluded Applications'



- Click 'Add'



- Enter the full path including the application that should be excluded from scanning and click 'OK'
- Repeat the process to include more applications

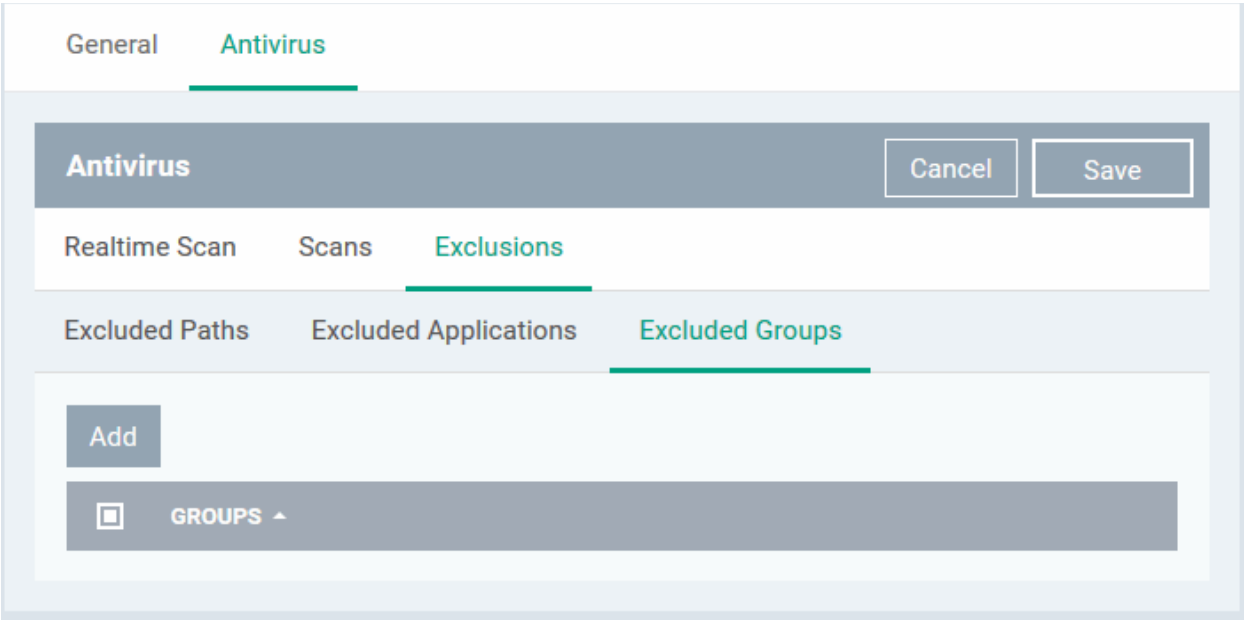


- To change the application path, click the edit button , edit the parameters and click 'OK'
- To remove an application from the list, select it and click 'Remove'

To add Excluded Groups

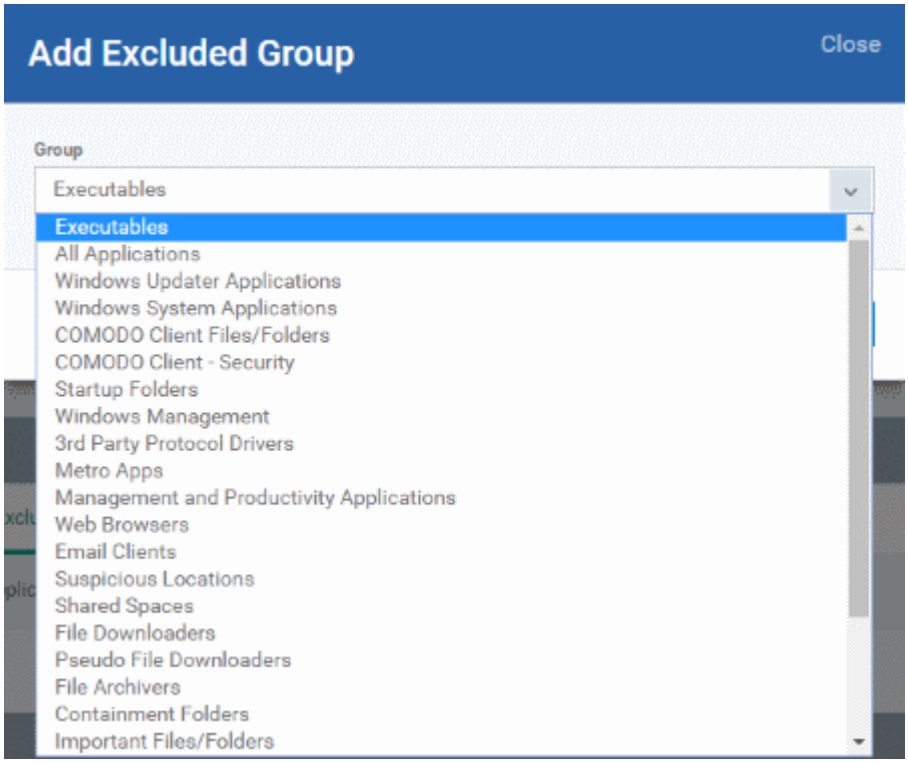
File Groups are handy, predefined groupings of one or more file types which make it easy to add an entire class of file types to Exclusions. ITSM ships with a set of predefined 'File Groups' and, if required users, can add new File Groups and edit existing groups. Refer to the portion explaining '**File Groups**' under 'Settings' > 'System Templates' > 'File Groups Variables'.

- Click 'Excluded Groups'



- Click 'Add'.

The 'Add Group' dialog will appear.



- Choose the group from the 'Group' drop-down and click 'OK'.

The group will be added to the exclusions.

- Repeat the process to add more file groups
- Click the 'Save' button at the bottom to save the antivirus settings.
- Click 'Delete' to remove the antivirus settings section. Refer to the section 'Editing Configuration Profiles' for more details about editing the parameters.

6.1.3.1.2. CCS and Virus Database Update Settings

Comodo Client Security (CCS) on managed computers automatically downloads virus database and program updates.

The 'Updates' component of a Windows profile allows you to schedule when managed computers should check for

and download updates from Comodo servers. This section contains two tabs: Schedule and Servers. The Schedule tab allows you to configure the update frequency and the Servers tab lets you configure the download location.

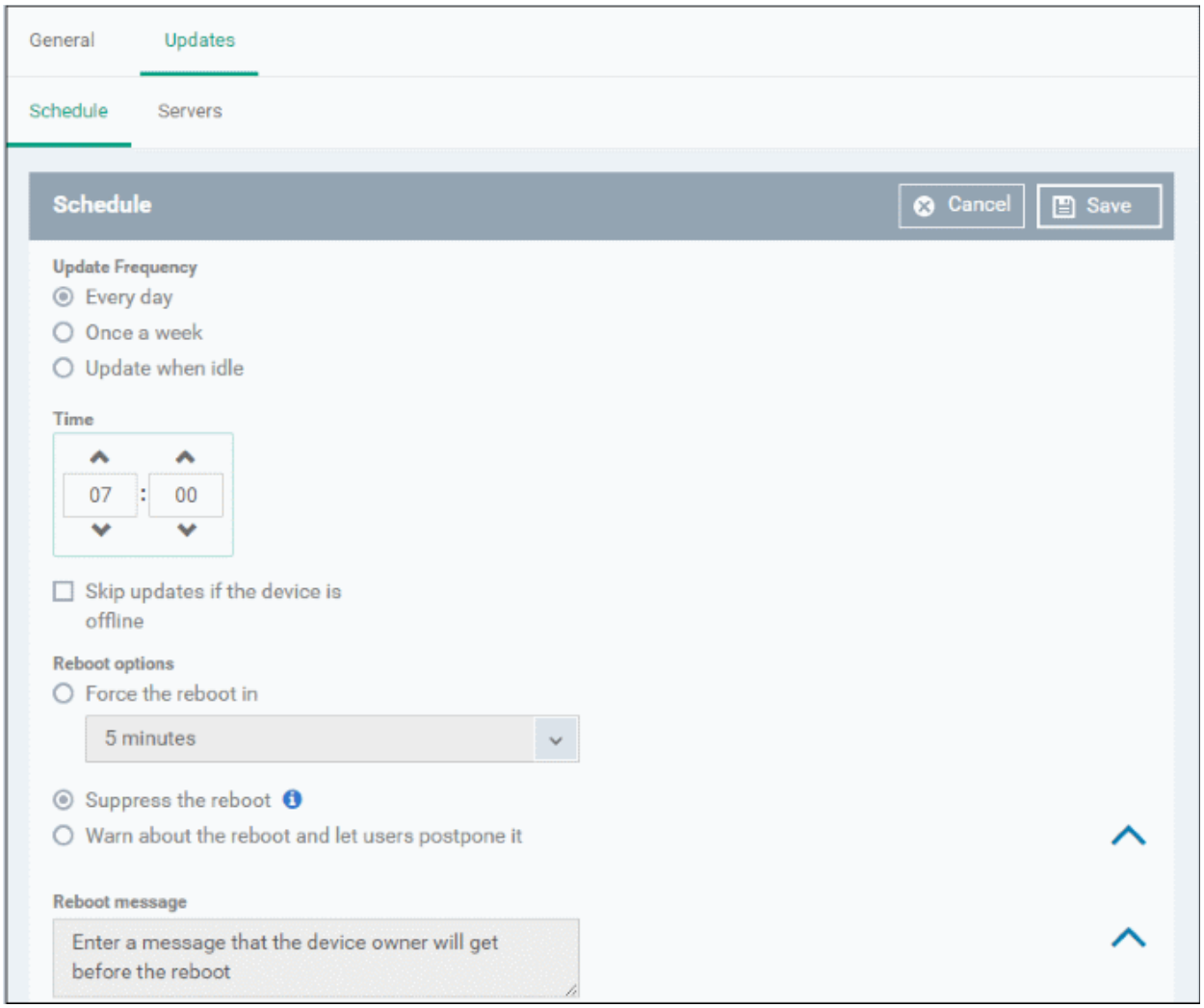
- Configure update frequency
- Configure download location

To configure Update frequency Settings

- Click 'Updates' from the 'Add Profile Section' drop-down in the Windows Profile interface

The 'Updates' settings screen will be displayed.

- Click the 'Schedule' tab



Update Frequency

- 'Every Day' will check daily for updates at a specific time. Select 'Every Day' and set the time in the Time combo boxes, in HH:MM format.
- 'Once a Week' allows you check for updates on a certain day of the week at a specific time. Choose the day from the 'Day of Week' drop-down and set the time in the 'Time' combo boxes.
- Update when idle - Devices check for and download updates when the device goes idle.
- Skip updates if the device is offline - If enabled, updates will not be applied to devices that are in offline mode. The updates will be applied to devices on next scheduled time.

Reboot Options

- Force the reboot in - If enabled, devices will be automatically rebooted per the time selected from the drop-down. You can also enter an appropriate message in the 'Reboot message' field that will be displayed on the endpoints to warn users about the upcoming forced reboot.

- Suppress the reboot - If enabled, reboot command will not be applied. Please note some updates require device reboot to become fully functional.
- Warn about the reboot and let users postpone it - If enabled, users will be alerted about the required device restart and allows them to choose the time when to reboot. You can also enter an appropriate message in the 'Reboot message' field that will be displayed on the endpoints to warn users about the required reboot.

- Click 'Save'.

To configure download server settings

The 'Servers' tab allows you to add and select the proxy servers from which updates are downloaded. By default, the download is directly from Comodo at http://download.comodo.com/. However, admins may wish to first download updates to a proxy/staging server and have the endpoints collect the updates from there. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

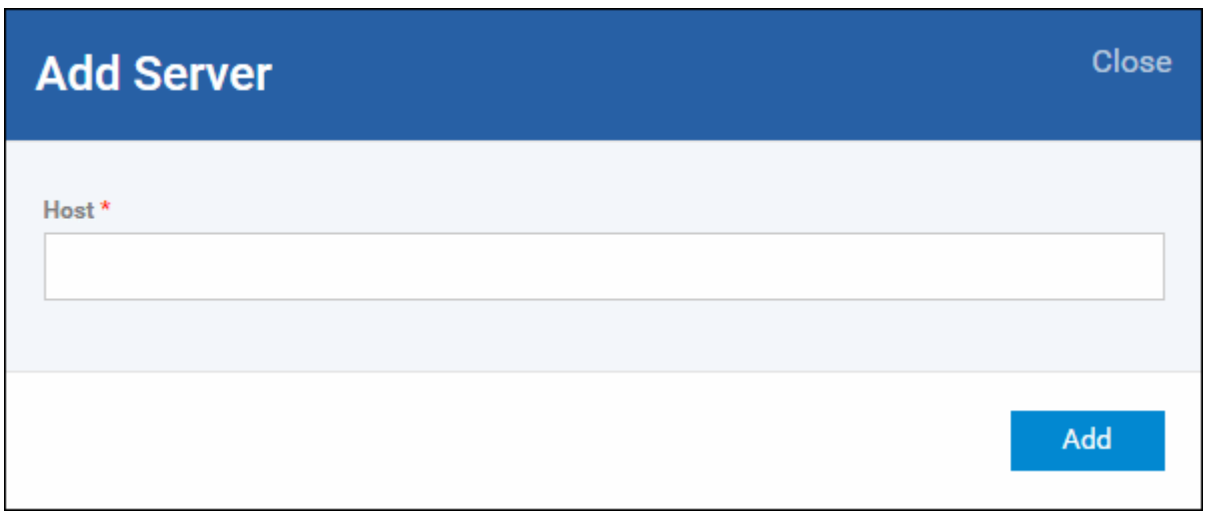
Note: You need to install an offline update utility on the local cache servers in order to get regular updates from Comodo. Contact your Comodo account manager or Comodo support for the same.

- Click the 'Servers' tab

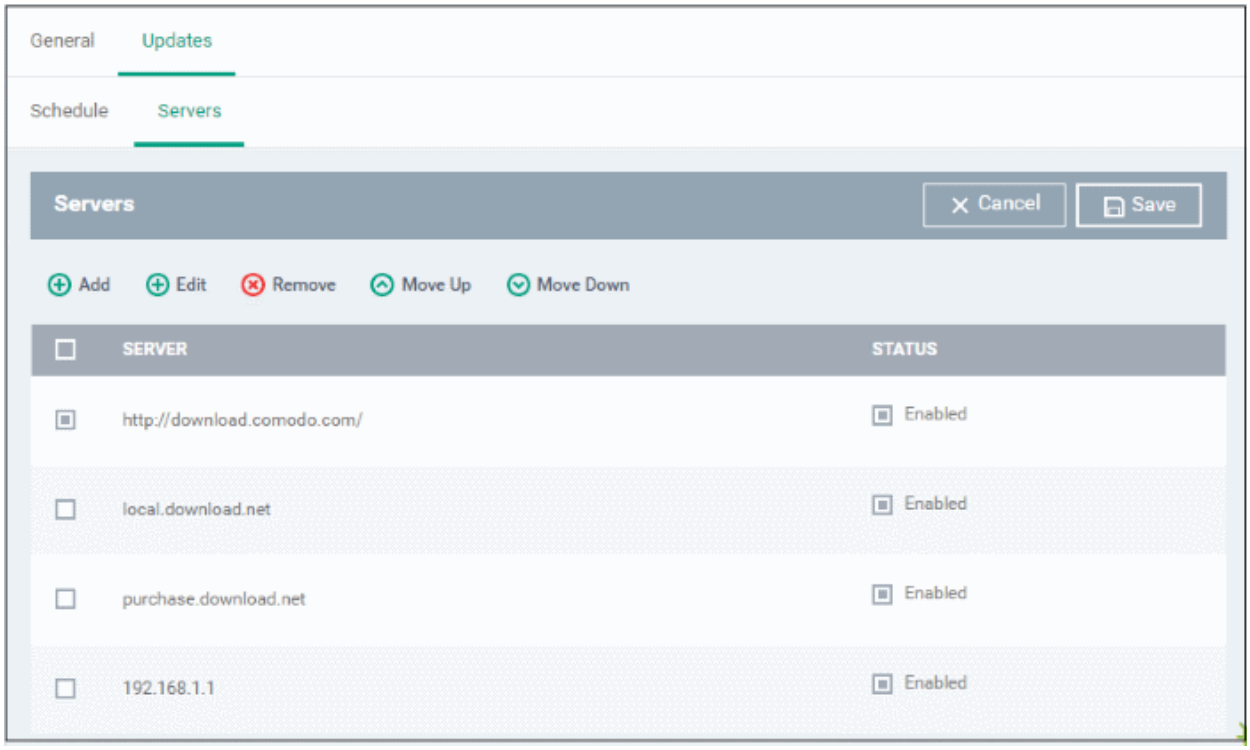
By default, ITSM is set to download from the Comodo servers. You can add your local servers here, edit, reorder the list of servers and remove servers if required.

- To add a server, click 'Add'

The 'Add Server' dialog will be displayed.



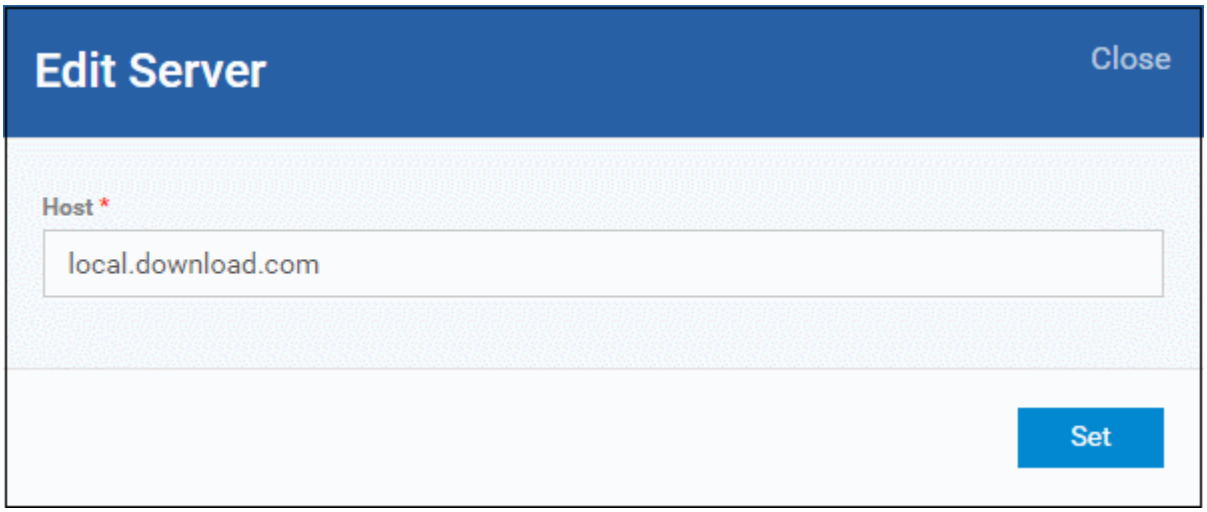
- Enter the server details in the Host field, either IP or the host name and click 'Add'. Repeat the process to add more servers.



- Server - Details of the update server
- Status - Indicates whether the server should be included for update checking. If this is selected, the endpoints will check the server for any updates.

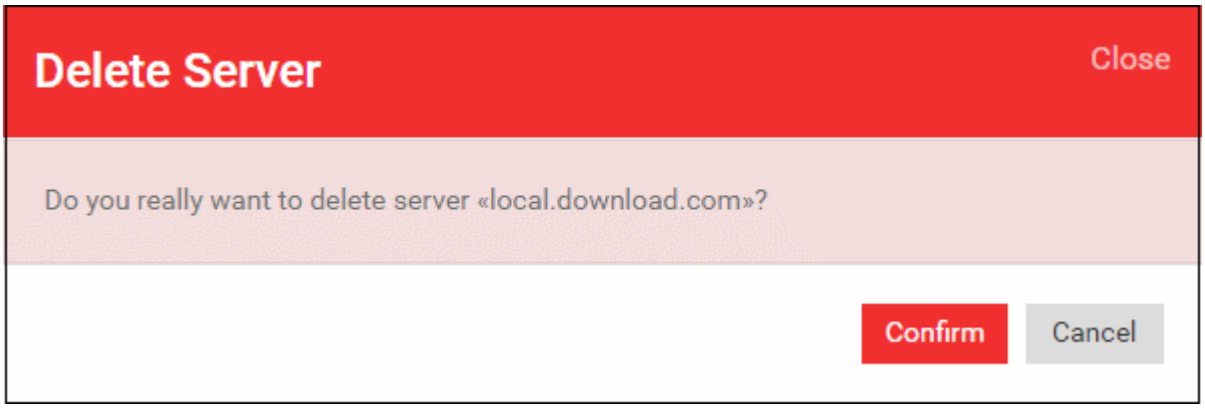
You can edit, remove or reorder the list of servers.

- To edit a server details, select it and click the 'Edit' button at the top.



Update the details as required and click the 'Set' button

- To remove a server, select it and click 'Remove' at the top



- Click 'Confirm' to remove the server from the list.

The updates are checked from the server at the top and moves down the list. You can reorder the list of servers.

- To reorder the server list, select the server(s) and click 'Move Up' or 'Move Down'
- Click 'Save' for the changes to updated in the profile.

6.1.3.1.3. File Rating Settings

The CCS rating system is a cloud-based file lookup service (FLS) that ascertains the reputation of files on the computer. Whenever a file is first accessed, CCS will check the file against Comodo's master whitelist and blacklists and will award it trusted status if:

- The application is from a vendor included in the Trusted Software Vendors list;
- The application is included in the extensive and constantly updated Comodo safelist;
- The application/file is awarded 'Trusted' status in the local File List.

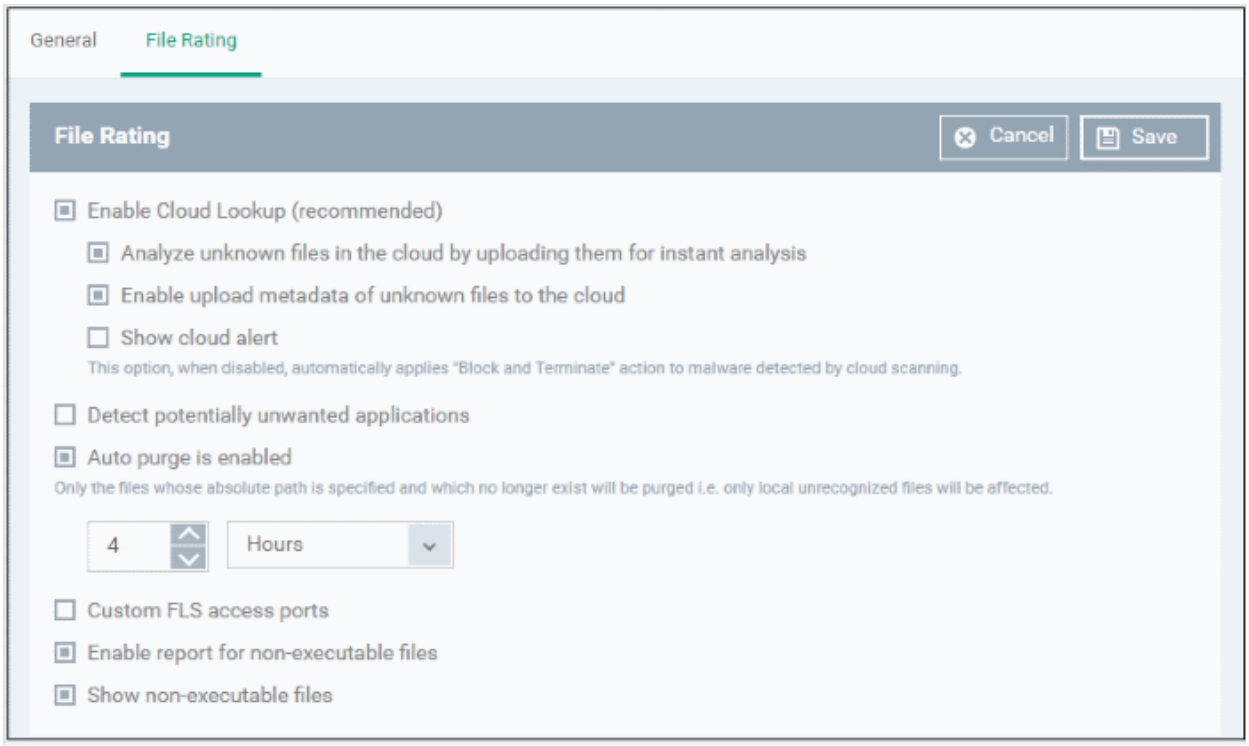
Note: CCS uses Ports 4446 and 4447 of the endpoint computers for TCP and UDP connections to the cloud. If this option is enabled, we advise you keep these ports free and do not assign them to other applications.

The File Rating setting interface allows you to configure the overall behavior of 'File Rating' of CCS installation at the Windows devices to which the profile is applied.

To configure File rating settings

- Click 'File Ratings' from the 'Add Profile Section' drop-down

The settings screen for 'File Ratings' will be displayed.



File Rating Configuration - Table of Parameters	
Form Element	**Description**
Enable Cloud Lookup	Allows you to enable or disable cloud based File Rating.
Analyze unknown files in the cloud by uploading them for instant analysis	When this option is enabled CCS instructs to upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the the whitelist or blacklist according to the analysis.
Enable upload metadata of unknown files to the cloud	If enabled, information about the unknown files will be uploaded to Comodo servers.
Show Cloud Alert	This option allows you to configure whether or not to show alerts when malware is encountered. If this option is not selected, then CCS will automatically apply 'Block and Terminate' action to malware detected by cloud scanning.
Detect potentially unwanted applications	When this option is selected, CCS identifies the applications that: • A user may or may not be aware is installed on their computer, and/or • May have functionality and objectives that are not clear to the user. Example: Potentially Unwanted Applications (PUAs) include adware and browser toolbars. PUAs are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. On detecting a PUA, the CCS installation at the endpoint raises an alert for the user to decide whether or not to run it and add it to the logs.

File Rating Configuration - Table of Parameters	
Auto Purge is enabled	When this option is selected, CCS refreshes the file list and removes invalid and obsolete entries in the file list corresponding to the endpoint, at the time interval specified in the 'Auto Purge' Period field.
Auto Purge Period	The time interval at which the auto purge operations are performed. Enter the time interval in hours.
Custom FLS access ports	This option allows you to define the ports through which the FLS will be connected. Select this option and enter the port details for UDP or TCP connections.
Enable report for non-executable files	If enabled, information about non-executable files will be reported to ITSM.
Show non-executable files	If selected, non-executable files will also be shown in the File List interface of the CCS installation on the endpoints ('Tasks' > 'Advanced Tasks' > 'Advanced settings' > 'Security settings' > 'File Rating' > 'File list'.

- Click the 'Save' button

The saved 'File Rating' settings screen will be displayed with options to edit the settings or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.3.1.4. Firewall Settings

The Firewall Settings area allows you to configure the behavior of the CCS firewall on endpoints to which the profile is applied. You can also configure network zones, portsets and traffic filtering rules.

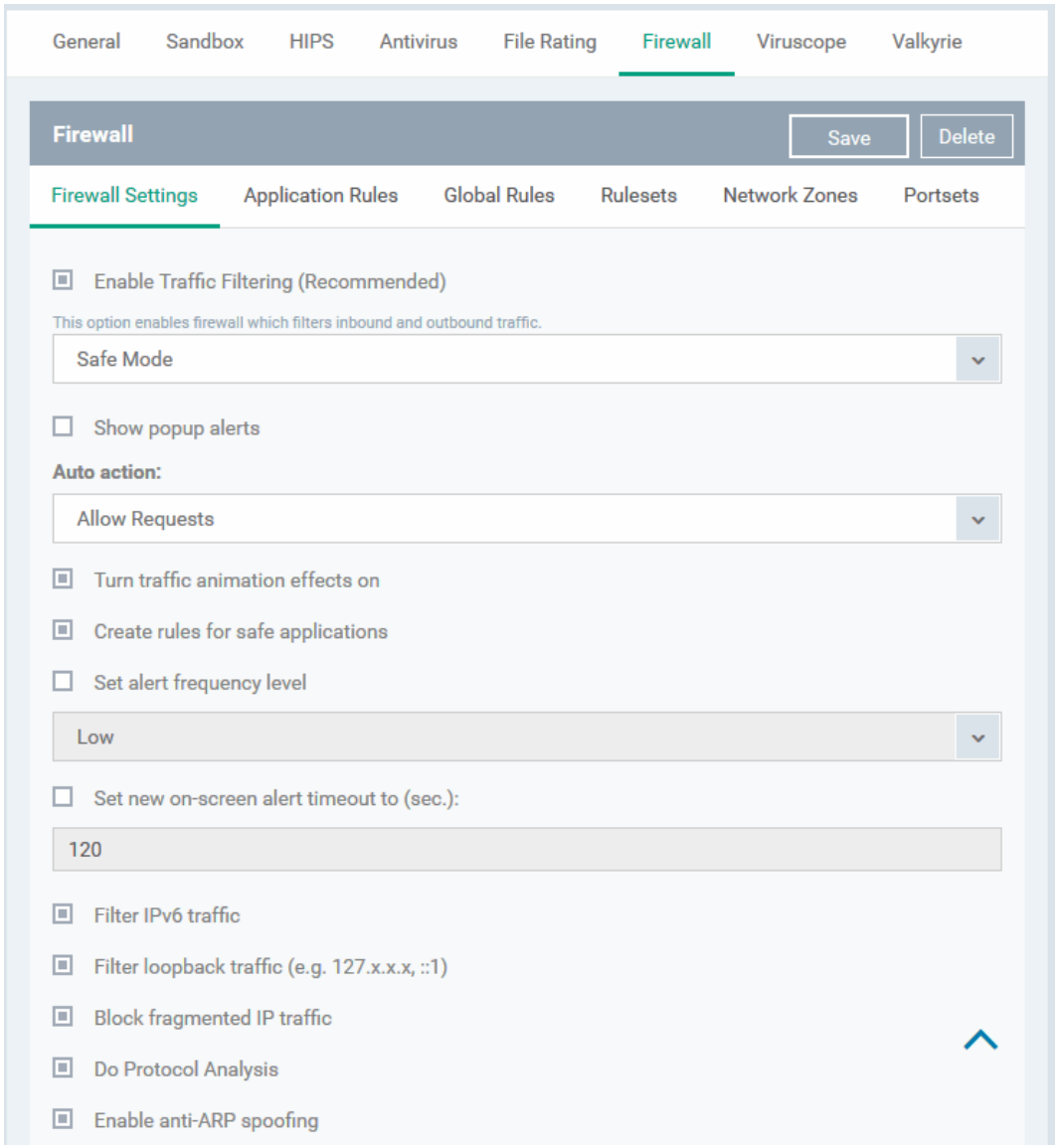
To configure Firewall Settings and Traffic Filtering Rules

- Click 'Firewall' from the 'Add Profile Section' drop-down

The Firewall settings screen will be displayed. It contains six tabs:

- **Firewall Settings** - Allows you to configure the general firewall behavior
- **Application Rules** - Allows you to define rules that determine the network access privileges of individual applications or specific types of applications at the endpoint
- **Global Rules** - Allows you to define rules that apply to all traffic flowing in and out of the endpoint
- **Rulesets** - Allows you create predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - Allows you to create named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Allows you to define groups of regularly used ports that can used and reused when creating traffic filtering rules.

Firewall Settings



Firewall Configuration - Table of Parameters	
Form Element	**Description**
Enable Traffic Filtering	Allows you to enable or disable Firewall protection at the endpoint. If enabled the following options are available: • **Custom Ruleset** - The firewall applies ONLY the custom security configurations and network traffic policies specified by the administrator. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. The user will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, the administrator has specified rules and policies that instruct the firewall to trust the application's connection attempt). If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their

Firewall Configuration - Table of Parameters	
	computer. • **Safe Mode** - While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo, if the checkbox Create rules for safe applications is selected. For non-certified new applications, the user will receive an alert whenever that application attempts to access the network. The administrator can choose to grant that application Internet access by selecting 'Treat this application as a Trusted Application' at the alert. This deploys the predefined firewall policy 'Trusted Application' onto the application. 'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts. • **Training Mode** - The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. The user will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on endpoints are assigned the correct network access rights. For more details on the Firewall Settings, see the of CCS - Firewall Settings online help page at http://help.comodo.com/topic-399-1-790-10358-Firewall-Settings.html .
Show popup alerts	You can enable the alerts to be displayed at the endpoint whenever the firewall encounters a request for network access, for the user to respond. If you choose not to show the alerts, you can select the default responses from the 'Auto Action' drop-down. The available options are: • Block Requests • Allow Requests
Turn traffic animation effects on	The CCS tray icon can display a small animation whenever traffic moves to or from your computer.  You can enable or disable the animation to be displayed at the endpoint.
Create rules for safe applications	Comodo Firewall trusts the applications if: • The application/file is included in the Trusted Files list under File Rating Settings; • The application is from a vendor included in the Trusted Software Vendors list • The application is included in the extensive and constantly updated Comodo safelist. By default, CCS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules. Enabling this option instructs CCS at endpoints to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules

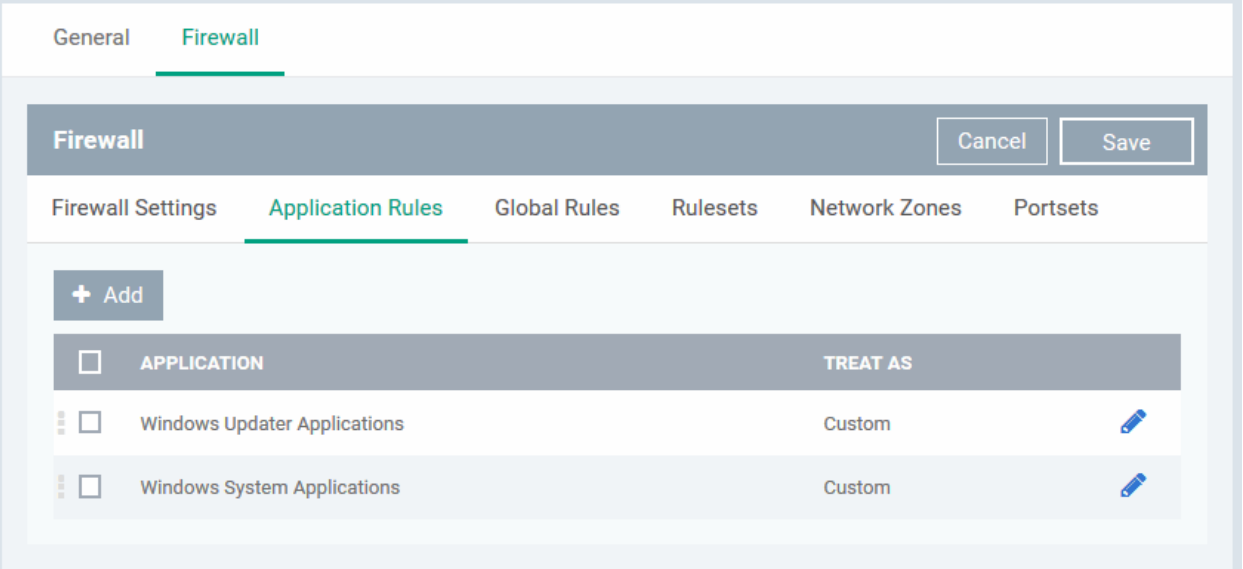
Firewall Configuration - Table of Parameters	
	are listed in the 'Advanced Settings' > 'Firewall Settings' > 'Application Rules' interface of the local CCS installation. Advanced users can edit/modify the rules as they wish. (Default = Disabled)
Set alert frequency level	Enabling this option allows you to configure the amount of alerts that Comodo Firewall generates, from the drop-down at the endpoint. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. (***Default=Disabled***) The options available are: • **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone. • **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application. • **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application. • **Low**: The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users. • **Very Low**: The firewall shows only one alert for an application. The Alert Frequency settings refer only to connection attempts by applications or from IP addresses that you have not (yet) decided to trust.
Set new on-screen alert timeout to:	Determines how long the Firewall shows an alert for, without any user intervention at the endpoint. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference by selecting this option and choosing the period from the drop-down combo-box.
Filter IPv6 traffic	If enabled, the firewall component of CCS at the endpoint will filter IPv6 network traffic in addition to IPv4 traffic. **Background Note**: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available. This hard limit has already led to the development of 'work-around' solutions such as Network Address Translation (NAT), which enable multiple hosts on private networks to access the Internet using a single IP address. IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique

Firewall Configuration - Table of Parameters	
	addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.
Filter loopback traffic	Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the Internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to, under its domain name of 'http://localhost', i.e. the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this option enabled means the firewall will filter traffic sent through this channel at the endpoints. (***Default = Enabled***).
Block fragmented IP traffic	When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time. If you want the firewall component of CCS at the endpoint to block the fragmented datagrams, enable this option. (***Default = Enabled***).
Do Protocol Analysis	Protocol Analysis is key to the detection of fake packets used in denial of service (DOS) attacks. If you want firewall at the endpoint to check whether every packet conforms to that protocols standards, select this option. If not, then the packets are blocked (***Default = Enabled***).
Enable anti-ARP spoofing	A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update the machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in another machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update its ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in a small network. Enabling this setting helps to block such requests at the endpoints to which the profile is applied - protecting the ARP cache from potentially malicious updates (***Default = Enabled***).

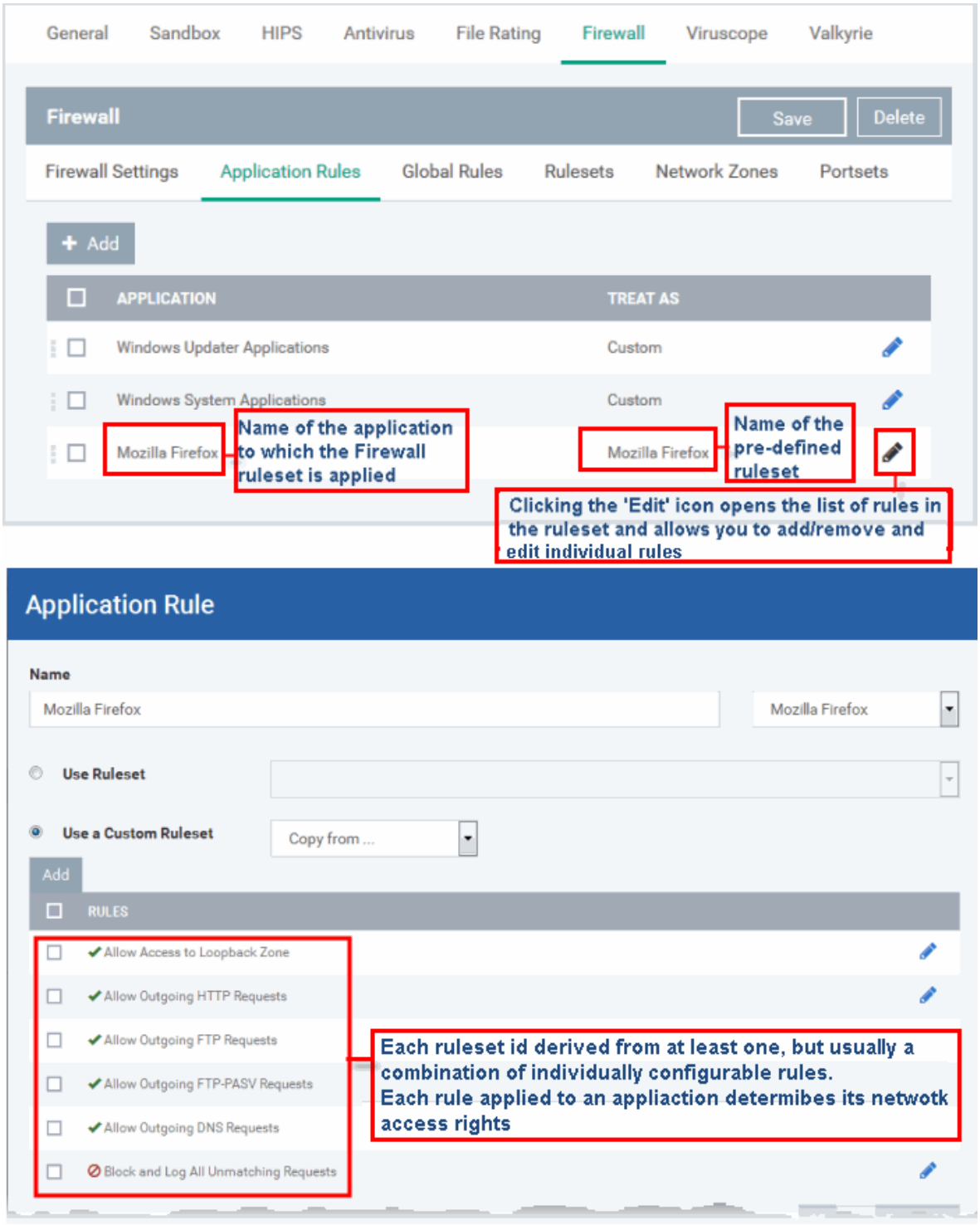
Application Rules

Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this

request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network access rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.



The 'Application Rules' interface allows you to create and manage application rules for regulating network access to individual applications at the endpoints to which the profile is applied.



Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Administrators can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see Predefined Rule Sets.

- See Application Rule interface for an introduction to the rule setting interface
- See Creating and Modifying Firewall Rulesets to learn how to create and edit Firewall rulesets
- See Understanding Firewall Rules for an overview of the meaning, construction and importance of

individual rules

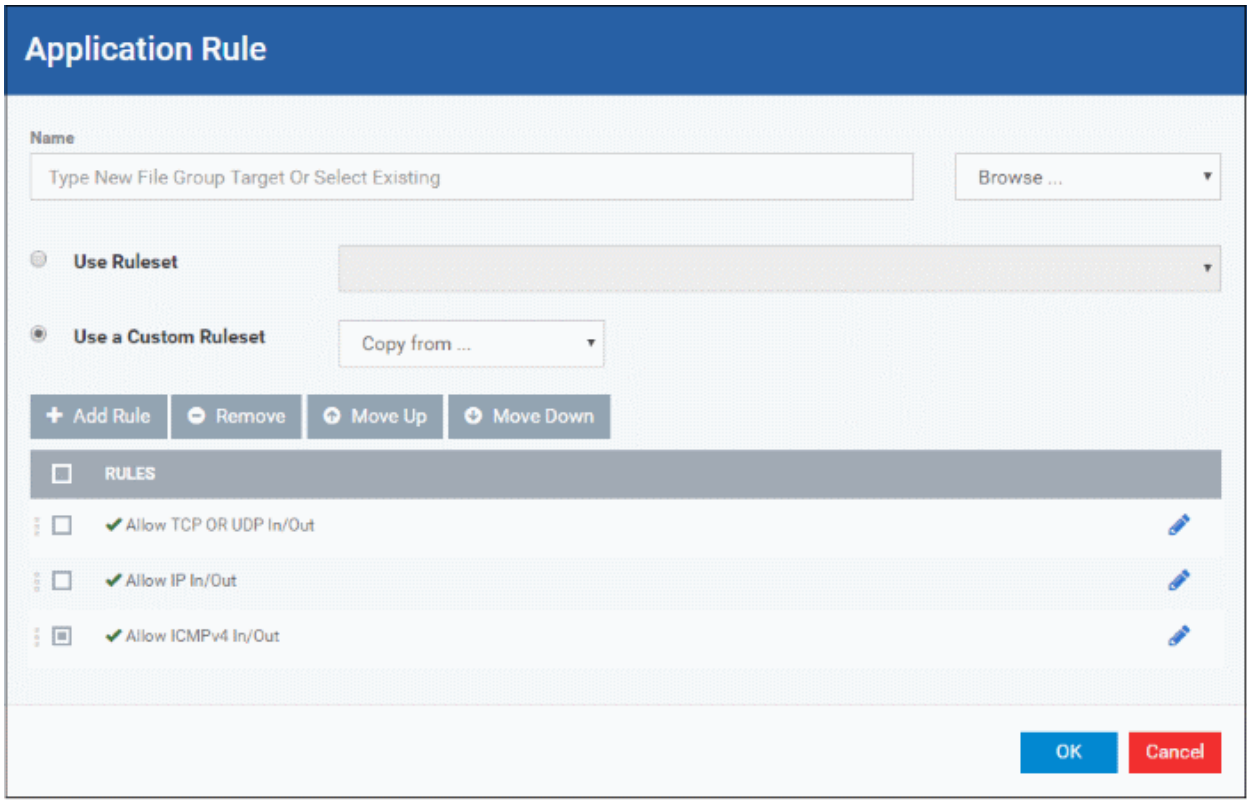
- See Adding and Editing a Firewall Rule for an explanation of individual rule configuration

Application Rule interface

The rules in a Firewall ruleset can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using Adding and Editing a Firewall Rule is displayed in this list.

The Application Rule interface is displayed when you click the 'Add' button 

or 'Edit' icon beside a ruleset, from the options in 'Application Rules' interface.



Comodo Firewall applies rules on a per packet basis and applies the first rule that matches that packet type to be filtered (see Understanding Firewall Rules for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied. Administrators can re-prioritize rules by uisng the 'Move Up' or 'Move Down' buttons.

Creating and Modifying Firewall Rulesets

To begin defining an application's Firewall ruleset, you need take two basic steps.

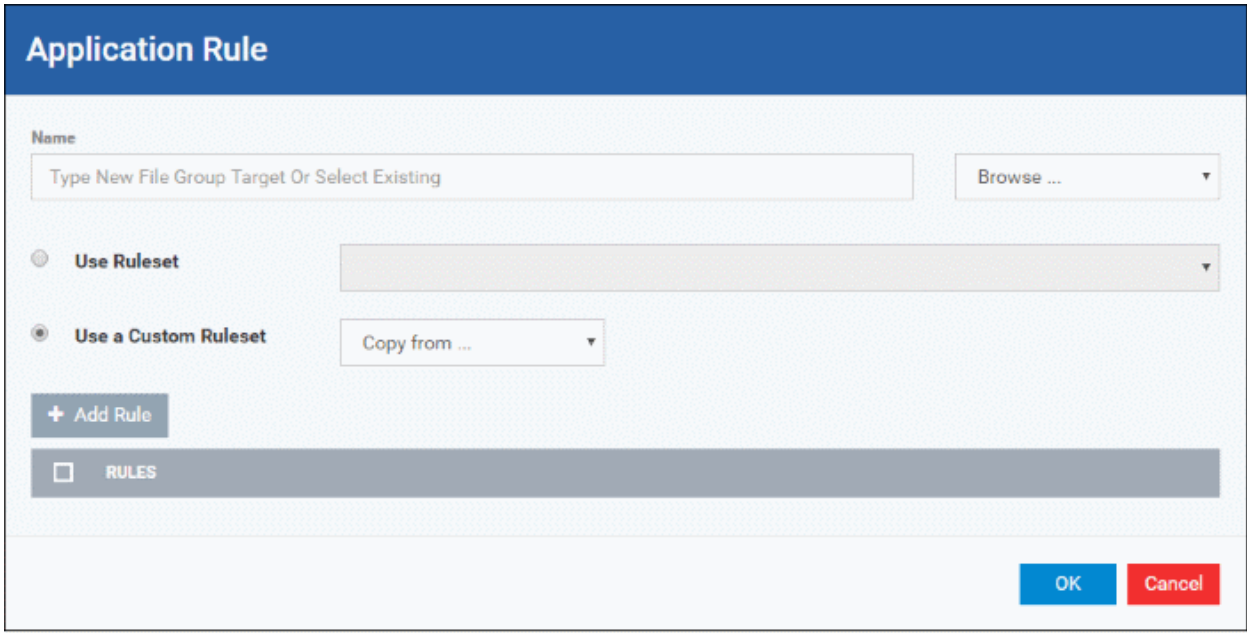
- Step 1 - Select the application that you wish the ruleset is to be applied.
- Step 2 - Configure the rules for this application's ruleset.

Step 1 - Select the application that you wish the ruleset is to be applied

- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add' button 

at the top of the list in the 'Application Rules' interface.

The 'Application Rule' interface will open as shown below:



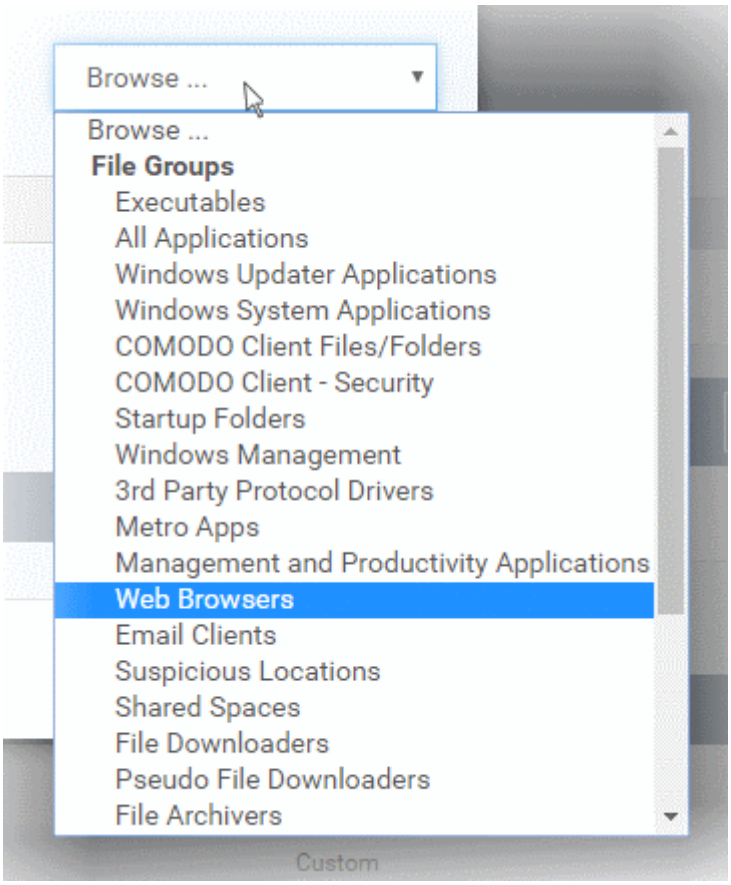
Because this is a new application, the 'Name' field is blank. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

You can enter the application(s) to which the rule set is to be applied in two ways:

- Enter the installation path of the application with the application file name in the Name field (For example, 'C:\Program Files\Mozilla Firefox\firefox.exe').

  Or

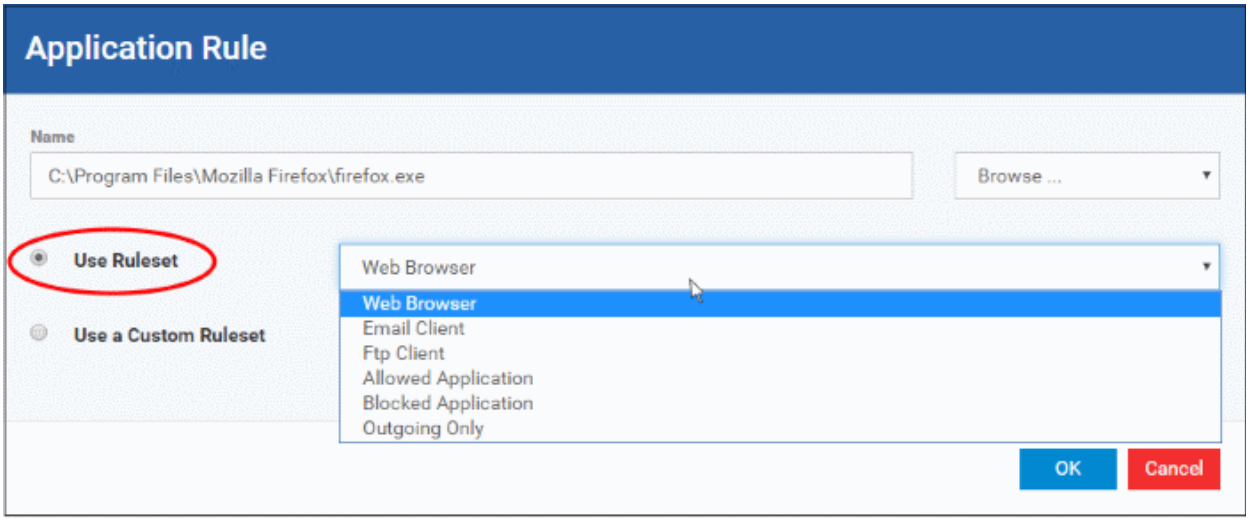
- Open the drop-down beside the 'Name' field and choose the Application Group to which the ruleset is to be applied. Choosing a 'File Group' allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders. ITSM ships with a set of predefined 'File Groups' and, if required users, can add new File Groups and edit existing groups. Refer to the portion explaining '**File Groups**' under 'Settings' > 'System Templates' > 'File Groups Variables'



Step 2 - Configure the rules for this application's ruleset

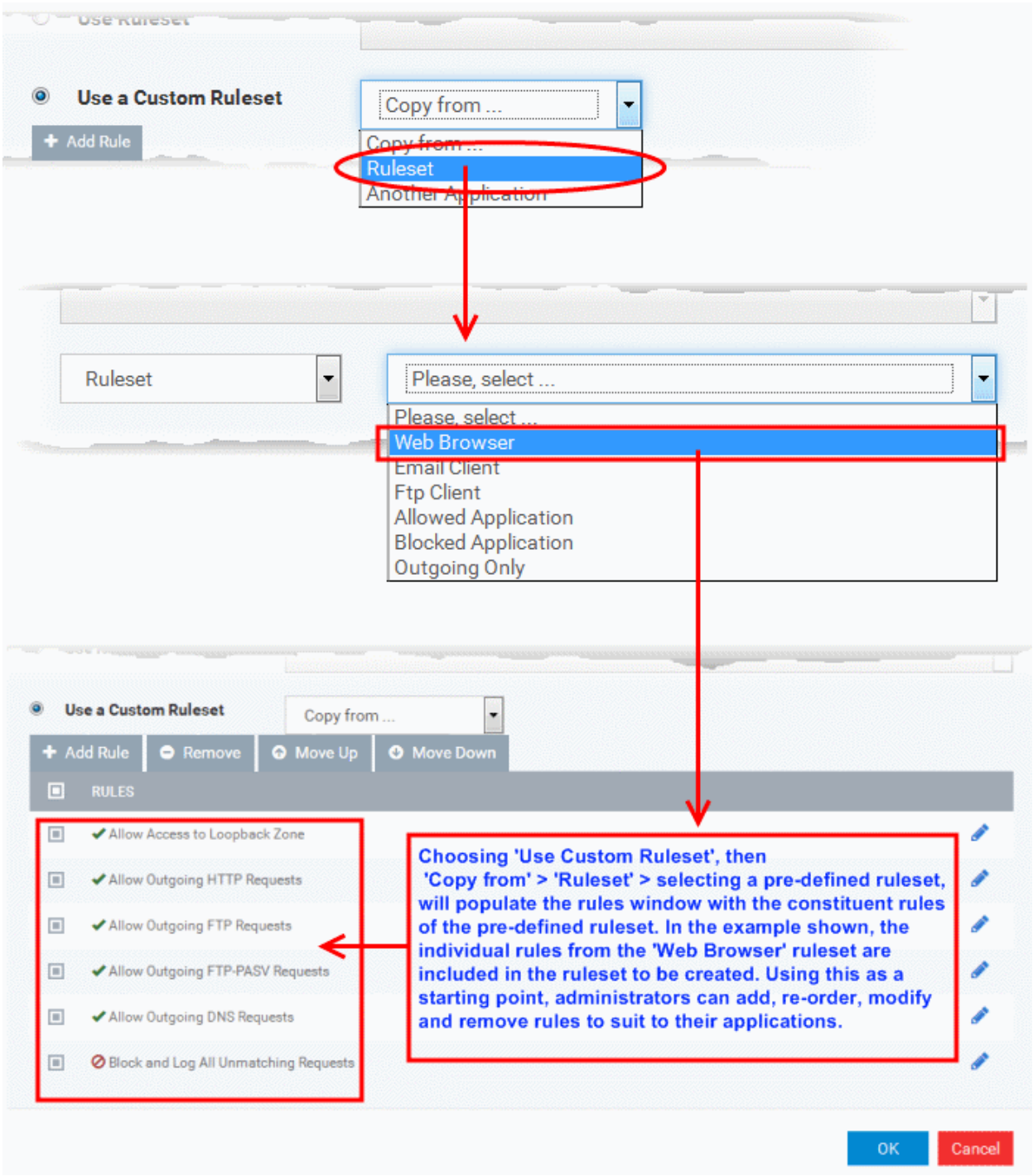
There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Allows you to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Firefox' browser. The name of the predefined ruleset you choose is displayed in the '**Treat As** ' column for that application in the '**Application Rules**' interface *(Default = Disabled).*



Note: Predefined Rulesets, once chosen, cannot be modified *directly* from this interface - they can only be modified and defined using the **Application Rule** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - Designed for more experienced administrators, the Custom Ruleset option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset (*Default = Enabled*).



You can create an entirely new ruleset or use a predefined ruleset as a starting point by:

- Clicking 'Add' from the top to add individual Firewall rules. See '**Adding and Editing a Firewall Rule**' for an overview of the process.

- Use the 'Copy From' button to populate the list with the Firewall rules of a Predefined Firewall Rule.
- Use the 'Copy From' button to populate the list with the Firewall rules of another application's ruleset.

General Tips:

- If you wish to create a reusable ruleset for deployment on multiple applications, we advise you add a new Predefined Firewall Rules (or modify one of the existing ones to suit your needs) - then come back to this section and use the 'Ruleset' option to roll it out.
- If you want to build a bespoke ruleset for maybe one or two specific applications, then we advise you choose the '**Use a Custom Ruleset**' option and create your ruleset either from scratch by adding individual rules or by using one of the built-in rulesets as a starting point.

Understanding Firewall Rules

At their core, each Firewall rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** it that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave the computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.

The actual **conditions** (attributes) you see * on a particular Firewall Rule are determined by the protocol chosen in **Adding and Editing a Firewall Rule**

If you chose 'TCP' , 'UDP' or 'TCP and 'UDP', then the rule has the form: **Action** |**Protocol** | **Direction** |**Source Address** | **Destination Address** | **Source Port** | **Destination Port**

If you chose 'ICMP', then the rule has the form: **Action** |**Protocol** | **Direction** | **Source Address** | **Destination Address** | **ICMP Details**

If you chose 'IP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **IP Details**

- **Action**: The action the firewall takes when the conditions of the rule are met. The rule shows '**Allow**', '**Block**' or '**Ask**'.**
- **Protocol**: States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows '**TCP**', '**UDP**', '**TCP** or **UDP**', '**ICMP**' or '**IP**'
- **Direction**: States the direction of traffic that the data packet must be attempting to negotiate. The rule shows '**In**', '**Out**' or '**In/Out**'
- **Source Address**: States the source address of the connection attempt. The rule shows '**From**' followed by one of the following: **IP** , **IP range**, **IP Mask** , **Network Zone**, **Host Name** or **Mac Address**
- **Destination Address**: States the address of the connection attempt. The rule shows '**To**' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Source Port**: States the port(s) that the application must be attempting to send packets of data through. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **Destination Port**: States the port(s) on the remote entity that the application must be attempting to send to. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **ICMP Details**: States the ICMP message that must be detected to trigger the action. See **Adding and Editing a Firewall Rule** for details of available messages that can be displayed.
- **IP Details**: States the type of IP protocol that must be detected to trigger the action: See **Adding and Editing a Firewall Rule** to see the list of available IP protocols that can be displayed here.

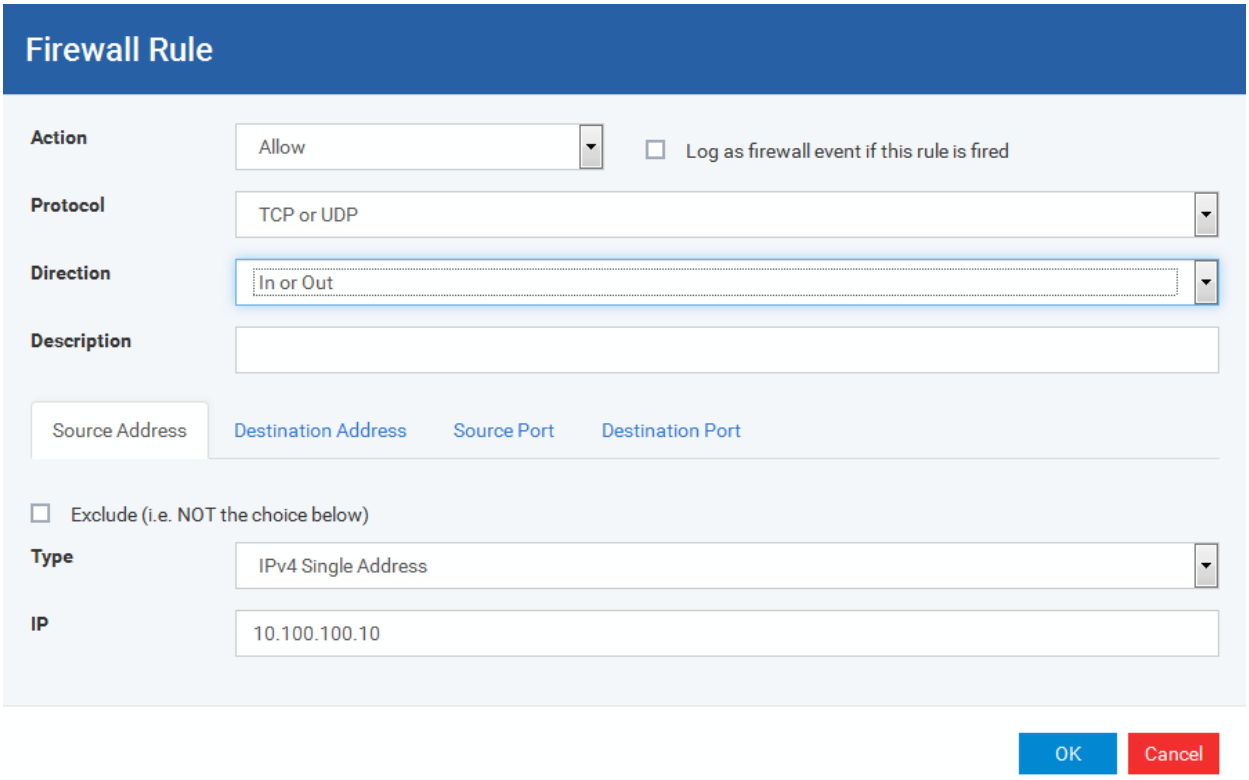
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section 'Global Rules' to understand the interaction between Application Rules and Global Rules.

* *If you chose to add a descriptive name when creating the rule then this name is displayed here rather than it's full parameters. See the next section, 'Adding and Editing a Firewall Rule', for more details.*

** *If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)*

Adding and Editing a Firewall Rule

The Firewall Rule Interface is used to configure the actions and conditions of an individual Firewall rule. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading the sections 'Understanding Firewall Rules', 'Overview of Rules and Policies' and 'Creating and Modifying Firewall Rulesets'.



General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are **'Allow'** ***(Default)***, **'Block'** or **'Ask'**.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are **'TCP'**, **'UDP'**, **'TCP or UDP'** ***(Default)***, **'ICMP'** or **'IP'** .

Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

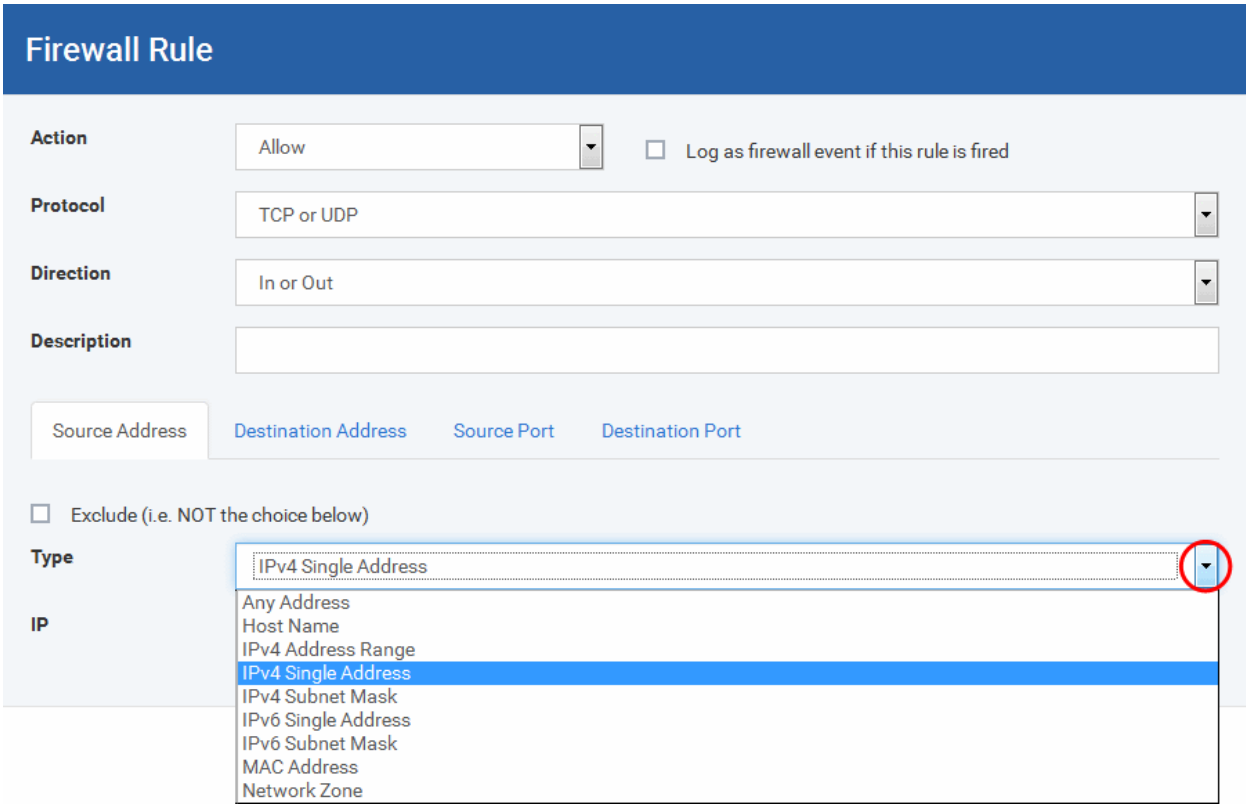
- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the firewall event log viewer whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is

displayed to represent instead of the full actions/conditions in the main Application Rules interface and the Application Rule interface.

Protocol

i. **TCP', 'UPD' or 'TCP or UDP'**

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information



Source Address and Destination Address:

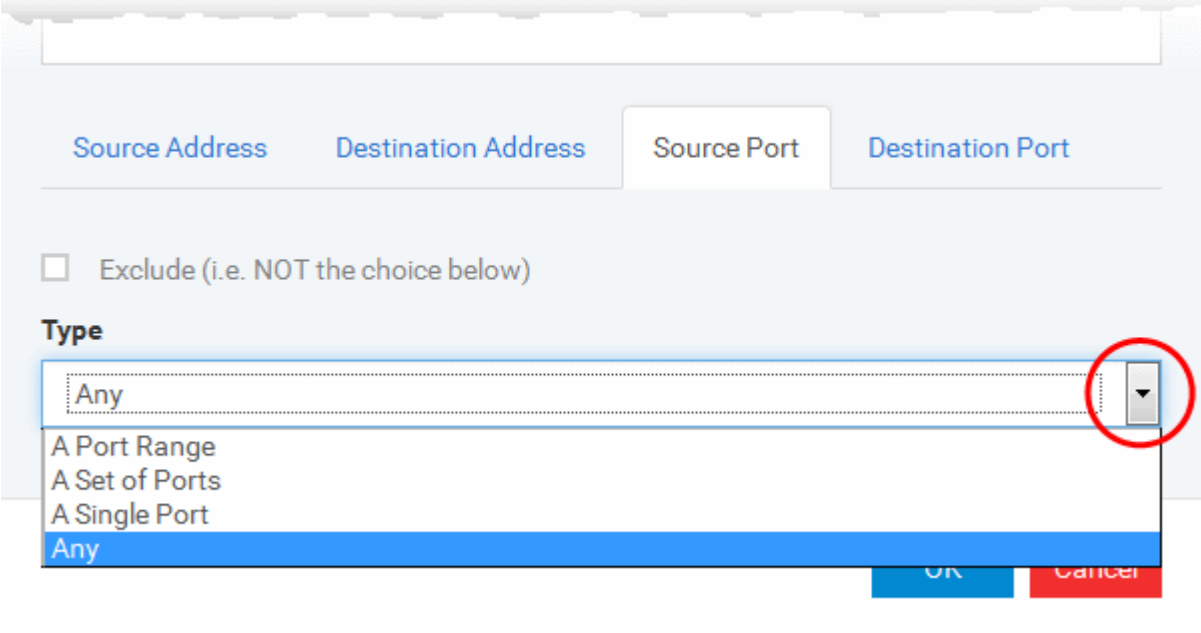
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area

Network. But you can also define your own zone by first creating a Zone through the 'Network Zones' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.



1. You can choose any port number by selecting Any - set by default , 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined Port Set by choosing A Set of Ports. If you wish to create a custom port set then please see the section 'Port Sets'.

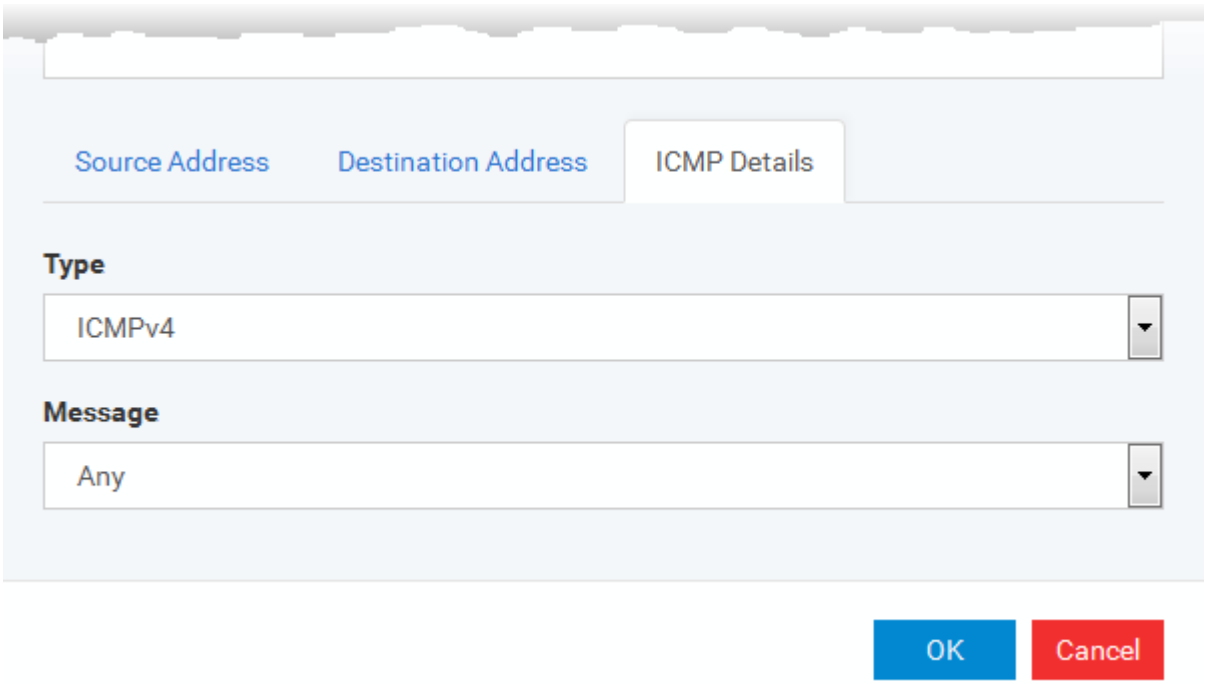
ii. **ICMP**

When you select ICMP as the protocol in General Settings, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the Destination Address tabs. The last two tabs are configured identically to the explanation above. You cannot see the source and destination port tabs.

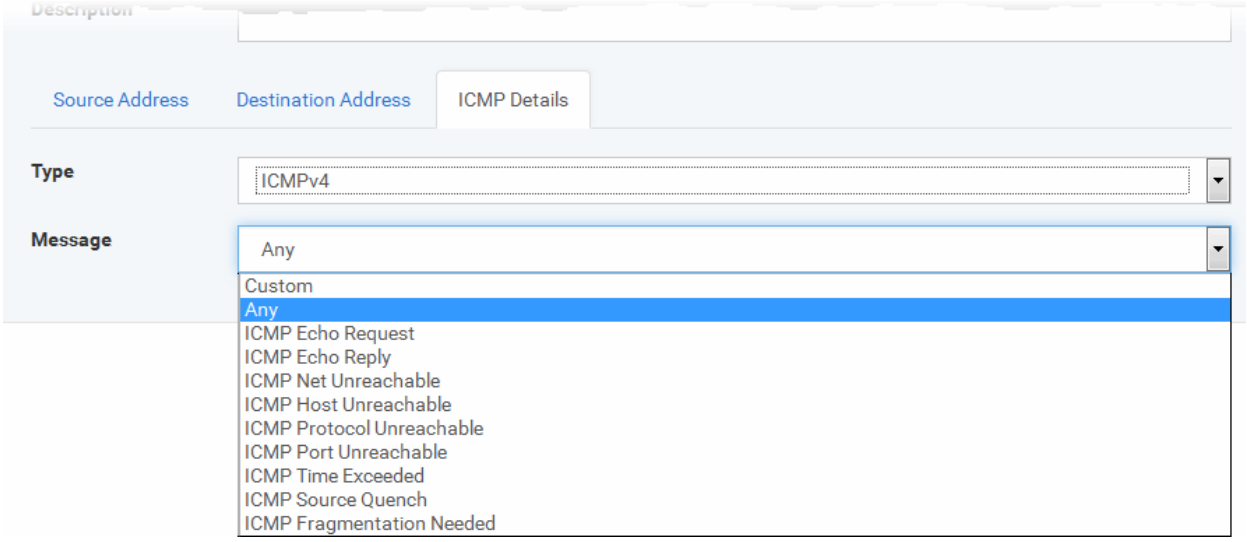
- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.



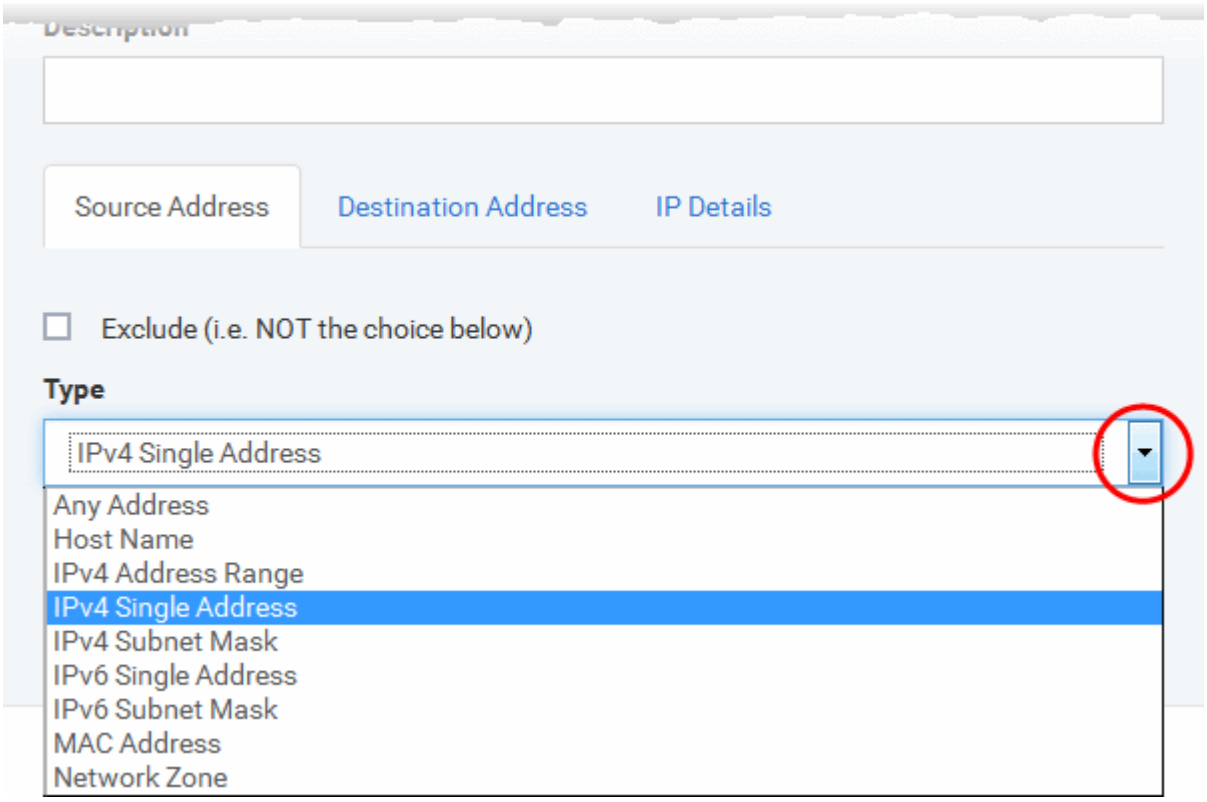
2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.
3. Specify ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.



When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

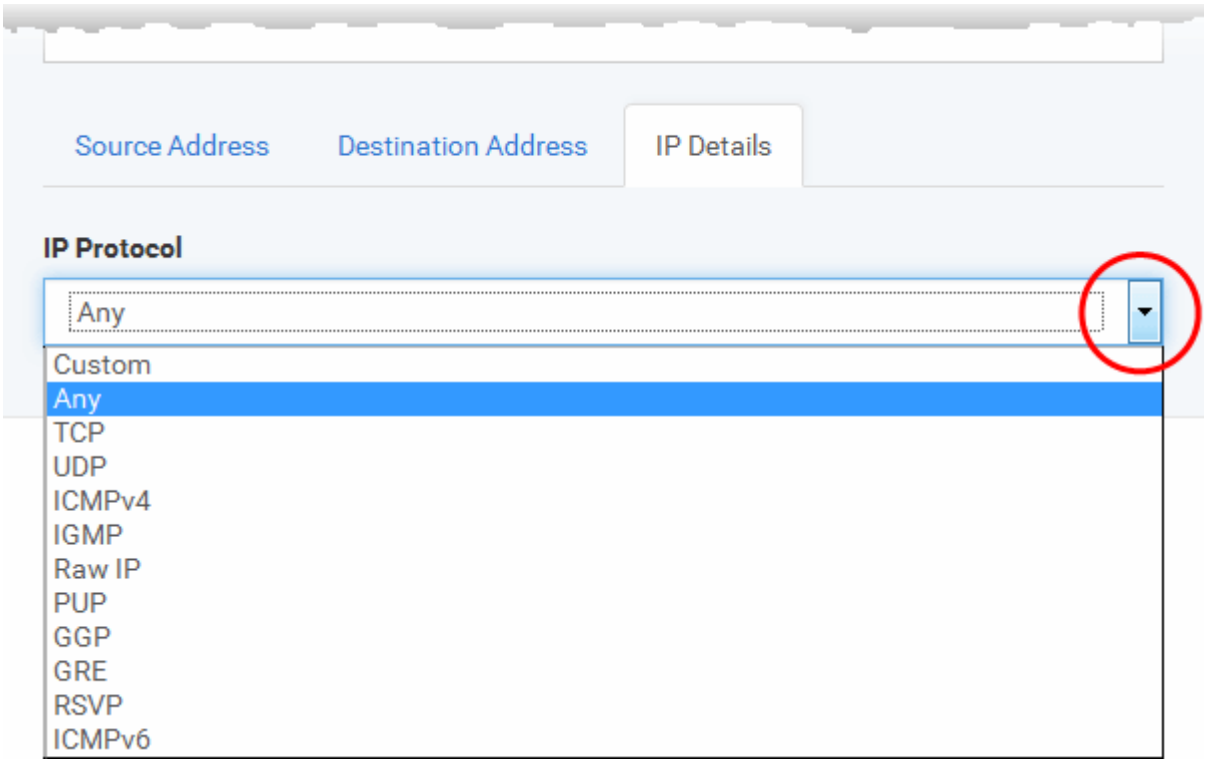
iii. **IP**

When you select IP as the protocol in General Settings, you are shown a list of IP message type in the 'IP Details' tab alongside the Source Address and Destination Address tabs. The last two tabs are configured identically to the explanation above. You cannot see the source and destination port tabs.



- **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.



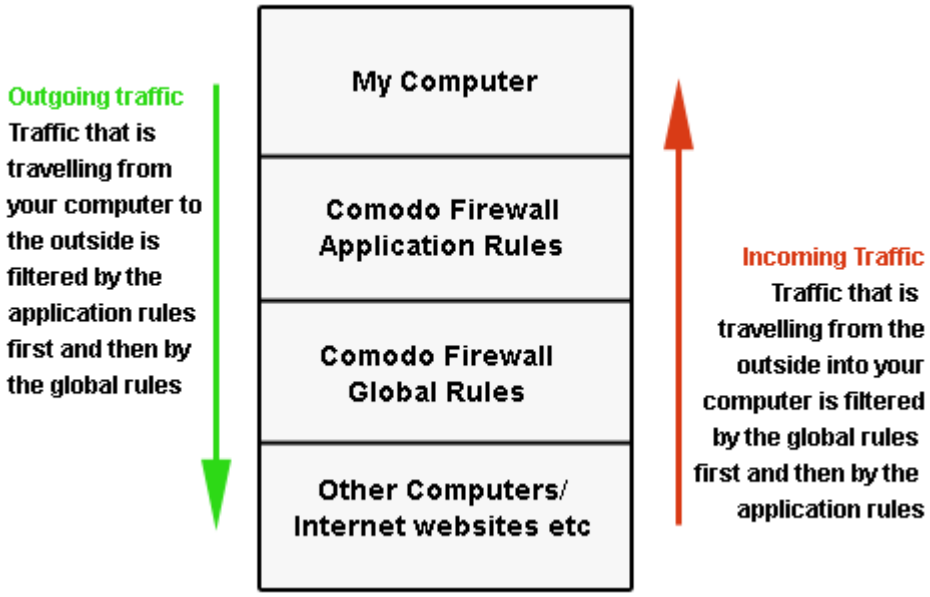
- Click 'OK' to save the firewall rule.

Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied to all traffic traveling in and out of the computers applied with this profile.

Comodo Firewall analyzes every packet of data in and out of the computer using combination of Application and Global Rules.

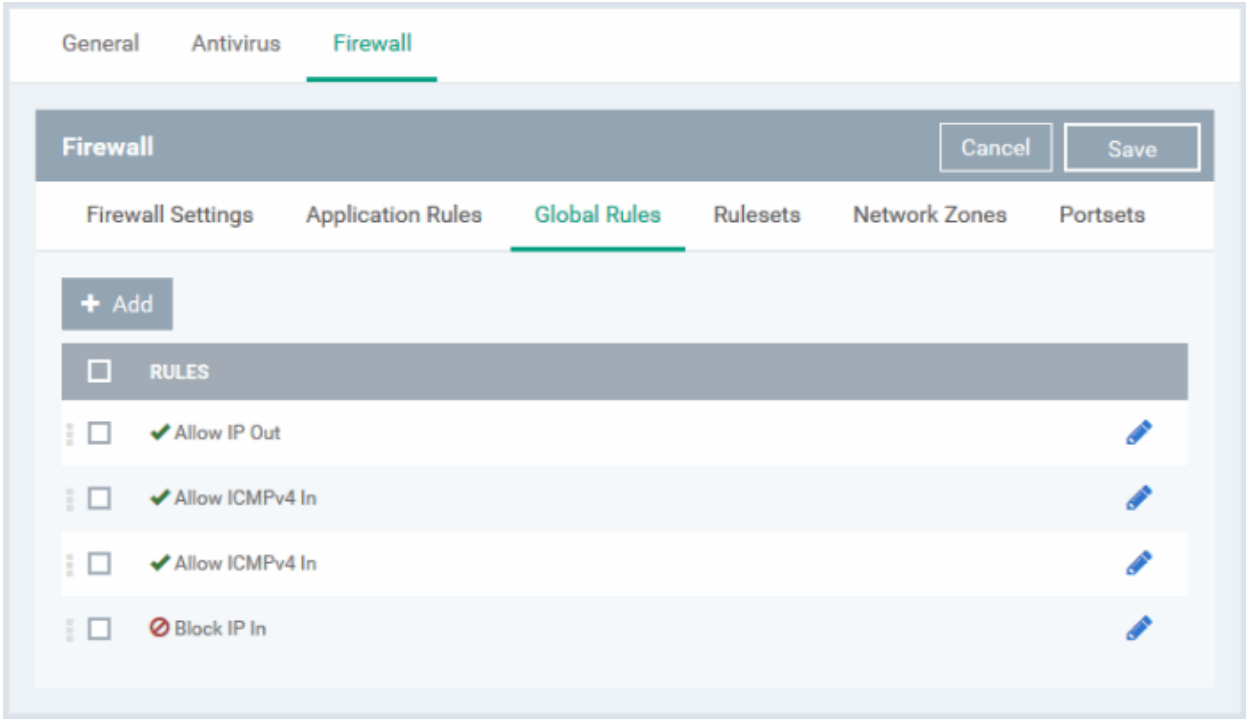
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

The 'Global Rules' panel in the under 'Firewall' tab allows you to view create and manage the global firewall rules.



The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add' button + Add on the top. To edit an existing global rule, click the edit icon beside it.

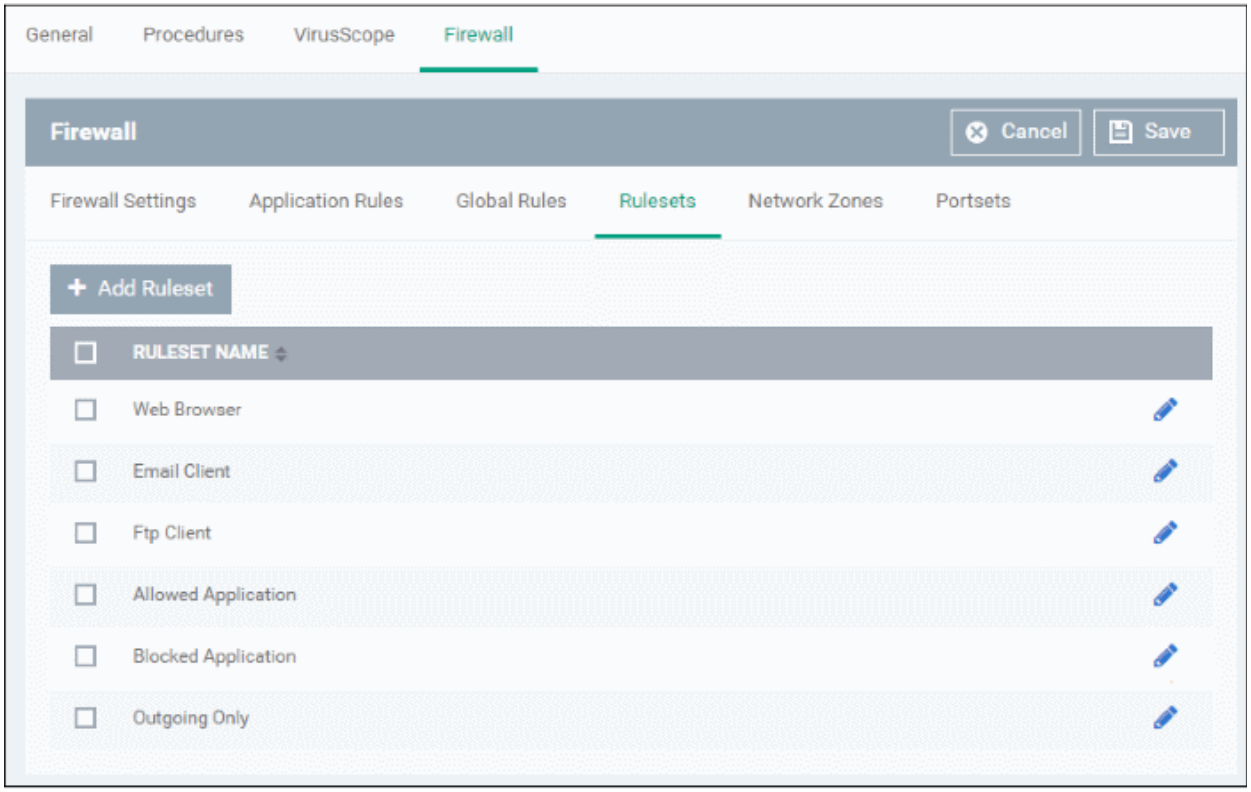
- See Application Rules for an introduction to the rule setting interface.
- See Understanding Firewall Rules for an overview of the meaning, construction and importance of individual rules.
- See Adding and Editing a Firewall Rule for an explanation of individual rule configuration.

Rulesets

As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. ITSM ships with six predefined rulesets and allows you to create and manage custom rulesets as required. This section contains advice on the following:

- Predefined Rulesets
- Creating a new ruleset

The 'Rulesets' panel under the 'Firewall' tab allows you to view, create and manage the firewall rulesets.



The Rulesets panel displays a list of pre-defined and custom Firewall Rulesets.

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined policies to suit their environment and requirements. (for example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of it rules).

ITSM ships with six predefined firewall rulesets for different categories of applications:

- Web Browser
- Email Client
- FTP Client
- Allowed Application
- Blocked Application
- Outgoing Only

These rulesets can be edited by adding new rules or reconfiguring the existing rules. For more details refer to the explanation of **Adding and Editing Firewall Rules** in the section 'Application Rules'.

Creating a new ruleset

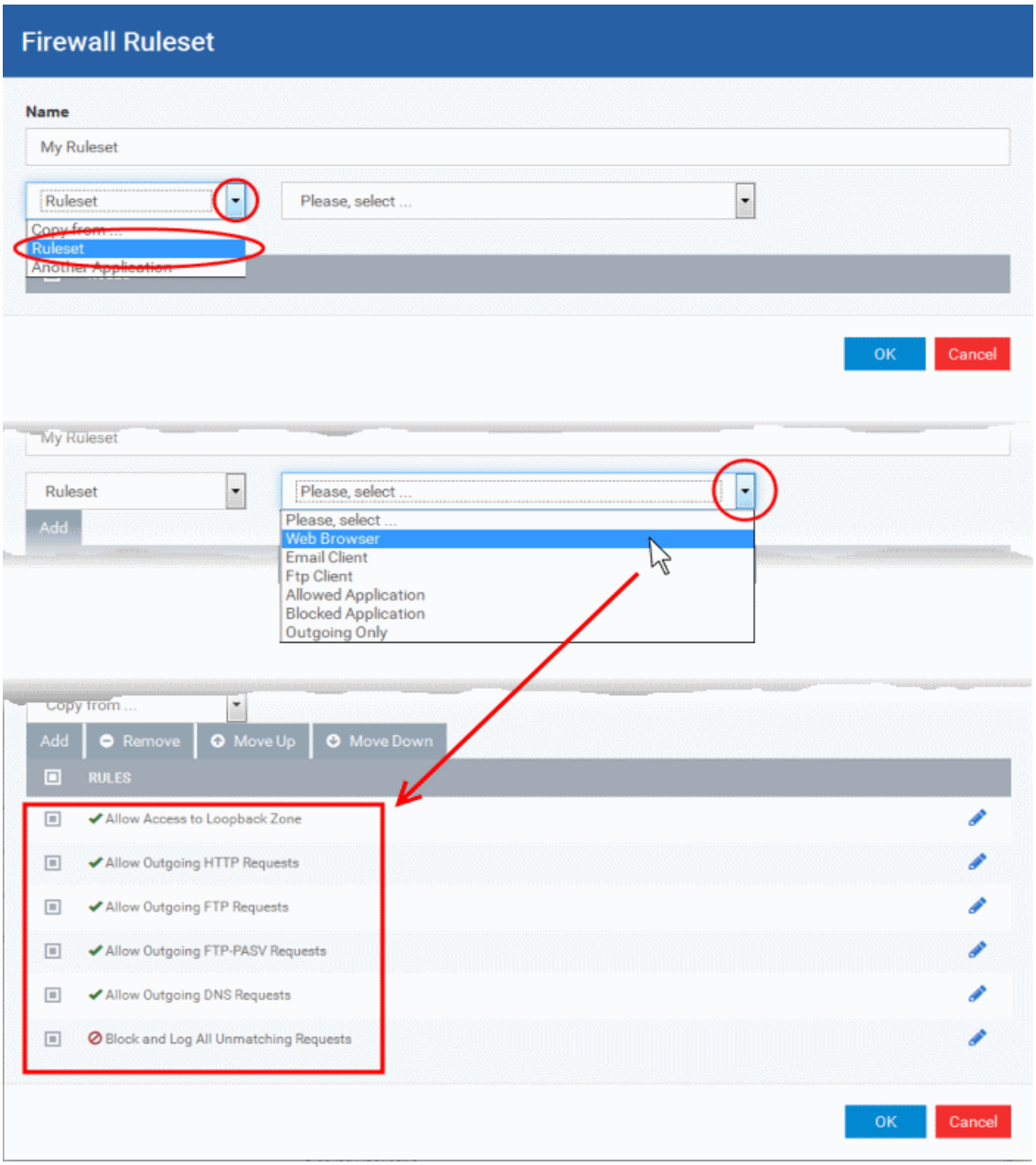
You can create new rulesets with network access control rules customized as per your requirements and can roll out them to required applications while **creating Firewall ruleset** for the applications individually.

To add a new Ruleset

- Click the 'Add Ruleset' button 

from the top of the list of rulesets in the 'Rulesets' panel

The 'Firewall Ruleset' interface will open.



- As this is a new ruleset, you need to name it in the 'Name' field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for. Next you should add and configure the individual rules for this ruleset. See 'Adding and Editing a Firewall Rule' for more advice on this.

Once created, this ruleset can be quickly called from 'Use Ruleset' when creating or modifying a Firewall ruleset.

To view or edit an existing predefined Ruleset

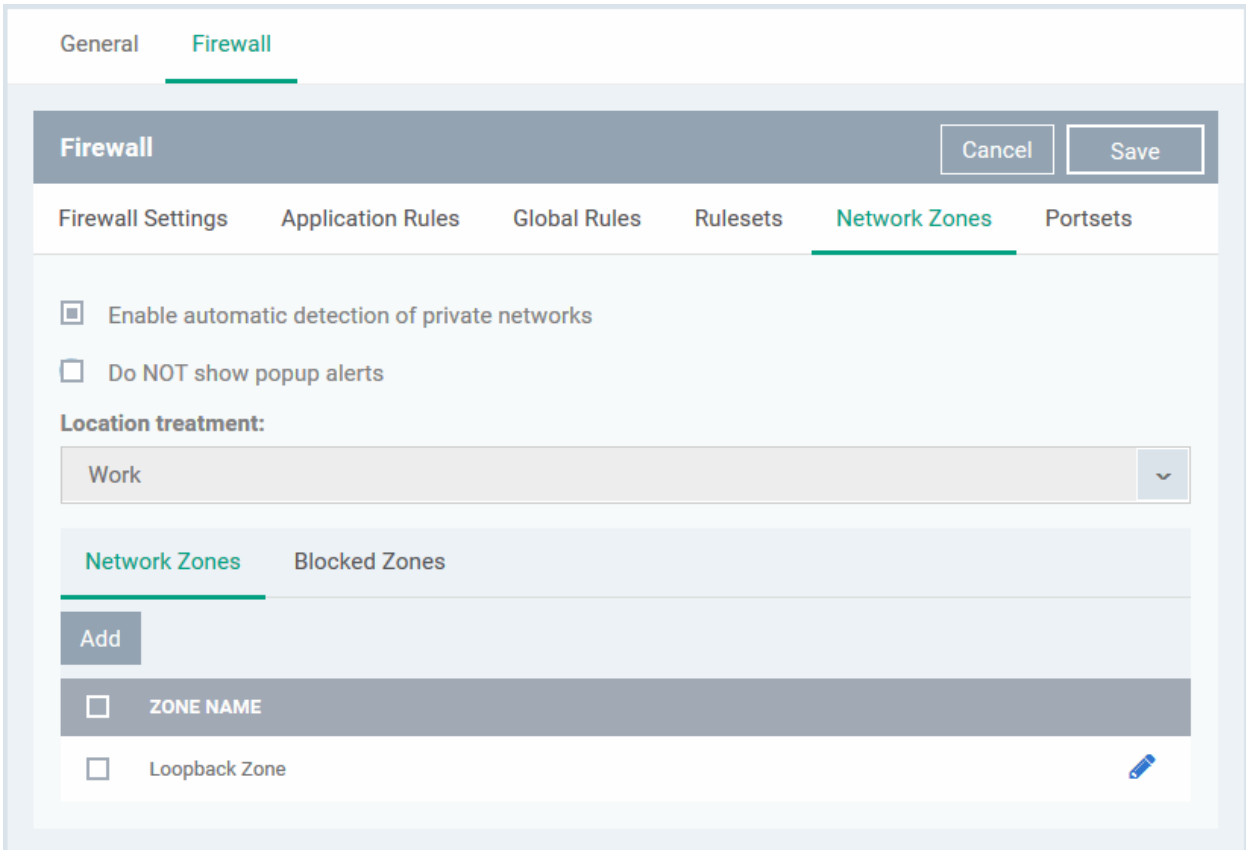
- Click on the 'Edit' icon beside Ruleset Name in the list.
- Details of the process from this point on can be found under 'Use Custom Rule Set.'.

Network Zones

The 'Network Zones' panel under the 'Firewall' tab allows you to:

- Configure to detect any new network (wired or wireless) that the computer applied with this profile is trying to connect and provide alerts for the same
- Define network zones that are trusted, and to specify access privileges to them

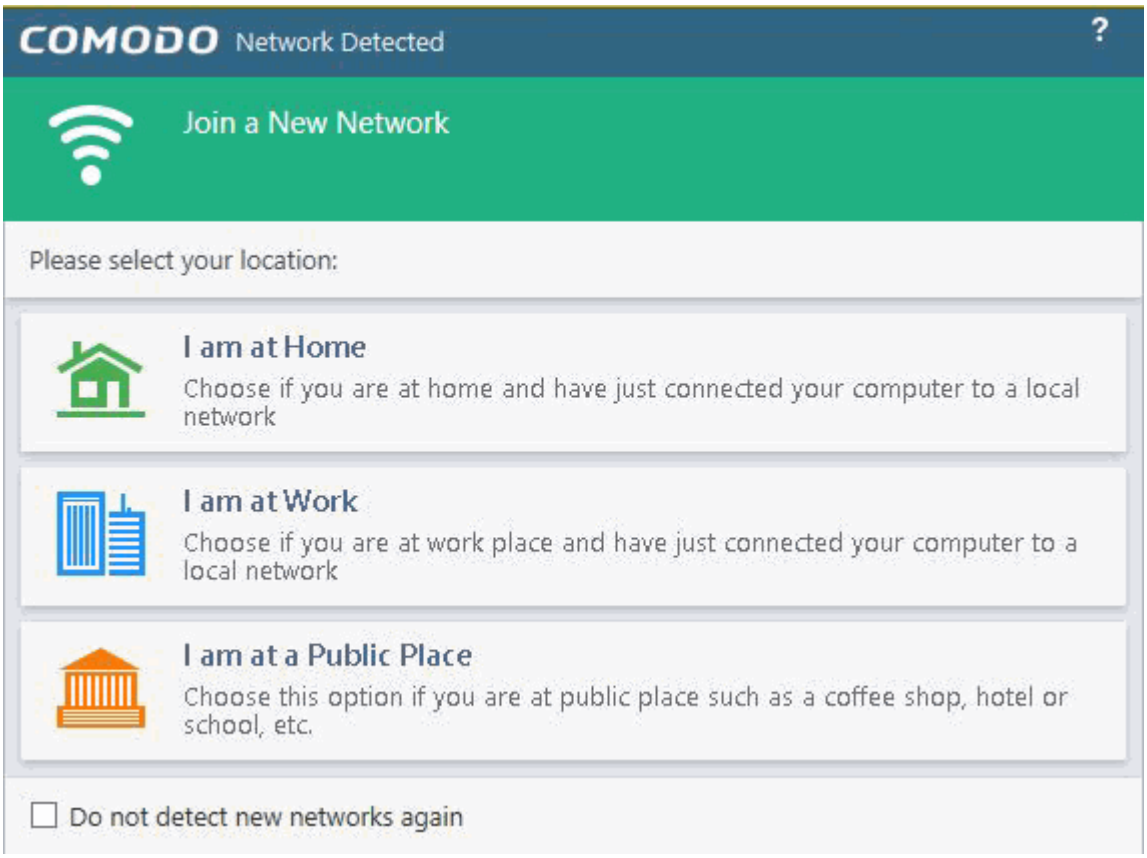
- Define network zones that are untrusted, and to block access to them



The 'Network Zones' panel contains options for configuring the general network monitoring settings and lists of 'Allowed Network Zones' and 'Blocked Network Zones' under respective tabs. You can add and manage network zones to be allowed and blocked from this interface.

Network Monitoring Settings:

- **Enable automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether the computer applied with this security profile is connected to any new wired or wireless network ***(Default = Enabled).*** Deselect this option if you do not want the new connection attempts is to be detected and/or wish to manually set-up their own trusted networks (this can be done in **'Network Zones**'.
- **Do Not show popup alerts** - By default, an alert will be displayed at the computer, if the computer attempts to connect to a new network, for the end-user to select the type of network. CCS will optimize its firewall settings for the new network, based on the selection. An example is shown below.



If you do not want the alert to be displayed to the end-user and wish the CCS at the computer to decide on the type of network by default, deselect this option and choose the network type from the drop-down under Location Treatment. The available options are:

- Home
- Work
- Public

The panel has two tabs:

- Network Zones - Allows you to define network zones and to allow access to them for applications, with the access privileges specified through Application Rule interface. Refer to 'Creating or Modifying Firewall Rules' for more details.
- Blocked Zones - Allows you to define trusted networks that are not trustworthy and to block access to them.

Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a

network of thousands of machines to which access can be granted or denied.

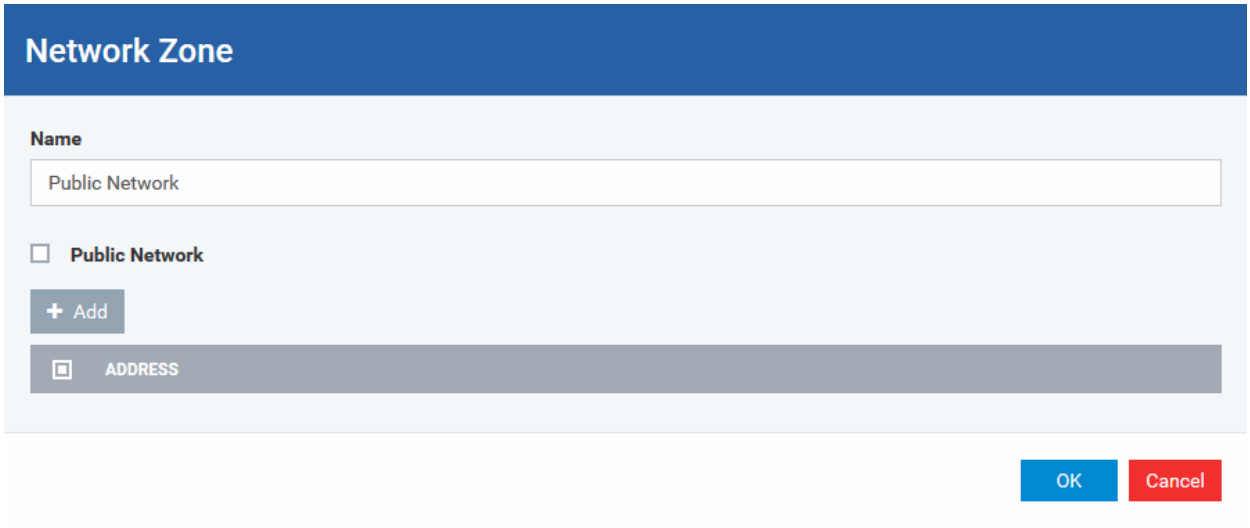
The 'Network Zones' tab in the 'Network Zones' panel displays a list of defined network zones and allows you to define network zones, to which the computer applied with this profile can connect, with access rights as defined by the firewall rules or blocked access to.

To define a new Network Zone

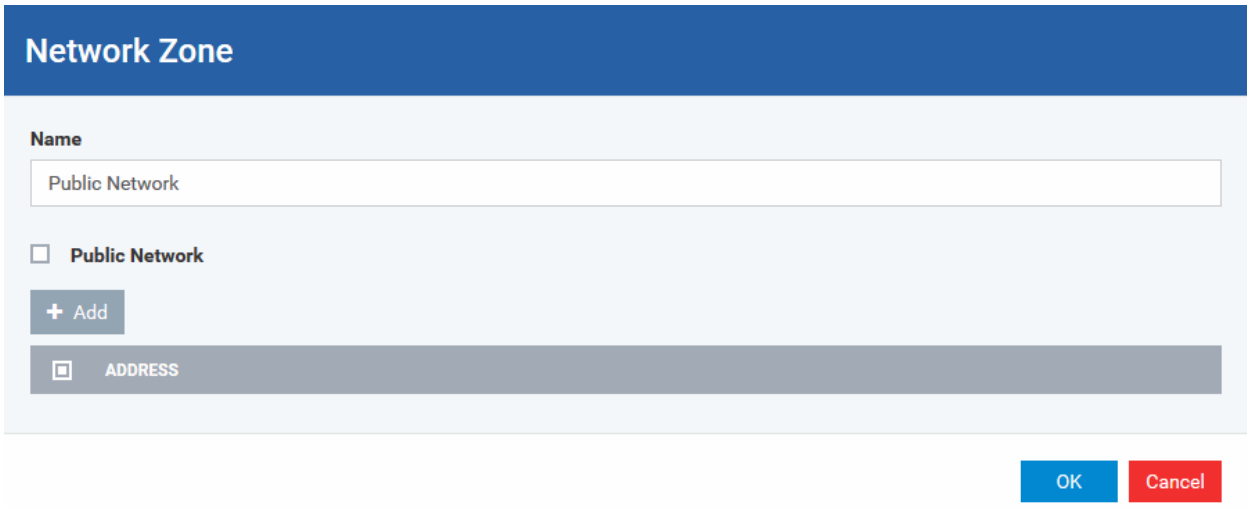
- Click the 'Add' 

button at the top of the list.

The 'Network Zone' dialog will open.



- Enter a name for the new network zone in the 'Name' field.
- Select the checkbox 'Public Network' if you are defining a network zone for a network in a public place, for example, when you are connecting to a Wi-Fi network at an airport, restaurant etc., so that Comodo Firewall will optimize the configuration accordingly.
- Click 'Add' to add the computers in the new network zone



The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below ***(Default = Any Address)***. The 'Exclude' check box will be enabled only if any other choice is selected from the drop-down box.

Address Types:

i. Any Address - Adds all the IP addresses (0.0.0.0- 255.255.255.255) to the zone.

ii. Host Name- Enter a named host which denotes an address on your network.

iii. IPv4 Range - Will include all the IPv4 addresses between the values you specify in the 'Start Range' and 'End Range' text boxes.

iv. IPv4 Single Address - Enter a single IP address to be added to the zone - e.g. 192.168.200.113.

v. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to add to the defined zone.

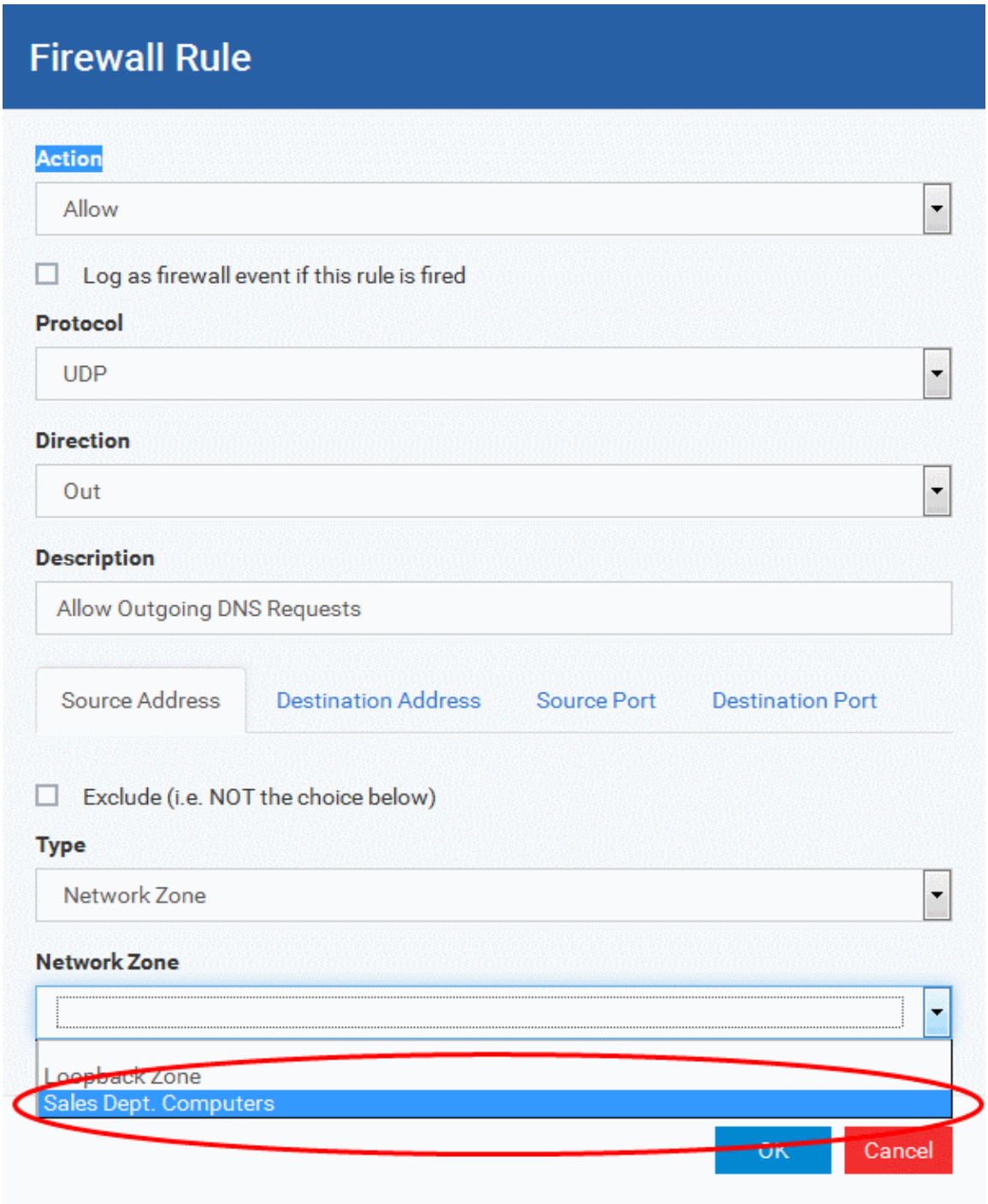
vi. IPv6 Single Address -Enter a single address to be added to the zone - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

vii. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

viii. MAC Address - Enter a specific MAC address to be added to the zone.

- Select/enter the Addresses to be included in the new network zone
- If you want to select all the other addresses to be included in the network zone, excluding those selected under the Type drop-down, select the 'Exclude' option.
- Click 'OK' in the 'Address' dialog.
- Click 'OK' in the 'Network Zone' dialog

The network zone will be added under Network Zones list and will be available to be quickly called as 'Zone' when creating or modifying a Firewall Ruleset. Or when defining a Blocked Zone.



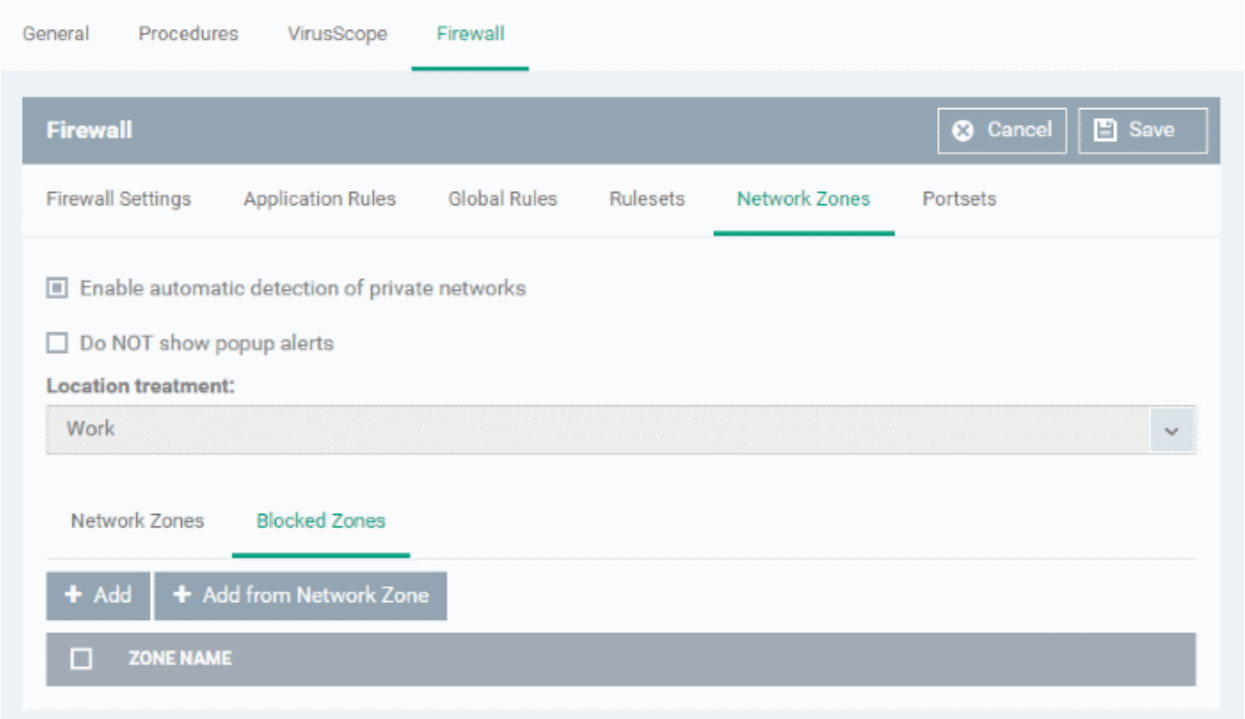
To edit a network zone, click the 'Edit' icon beside the network zone name. The 'Network Zone' dialog will appear populated with the name and the addresses of the network zone. Edit the details as required. The process is similar to defining a new network zone as explained above.

Blocked Zones

A computer network enables users to share information and devices between computers and other users within the network. There are certain networks that you'll want to 'trust' and grant access to - for example your work network. Conversely, there may be other networks that you do not trust and want to restrict communication with - or even block entirely.

The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not wish to trust and the computers applied with this profile will be blocked access to them.

The 'Blocked Zones' tab allows you to view the list of blocked network zones and add new blocked zones.



The 'Blocked Zones' tab displays a list of zones that are currently blocked and allows you to:

- Deny access to an existing network zone
- Deny access to a network by manually defining a new blocked zone

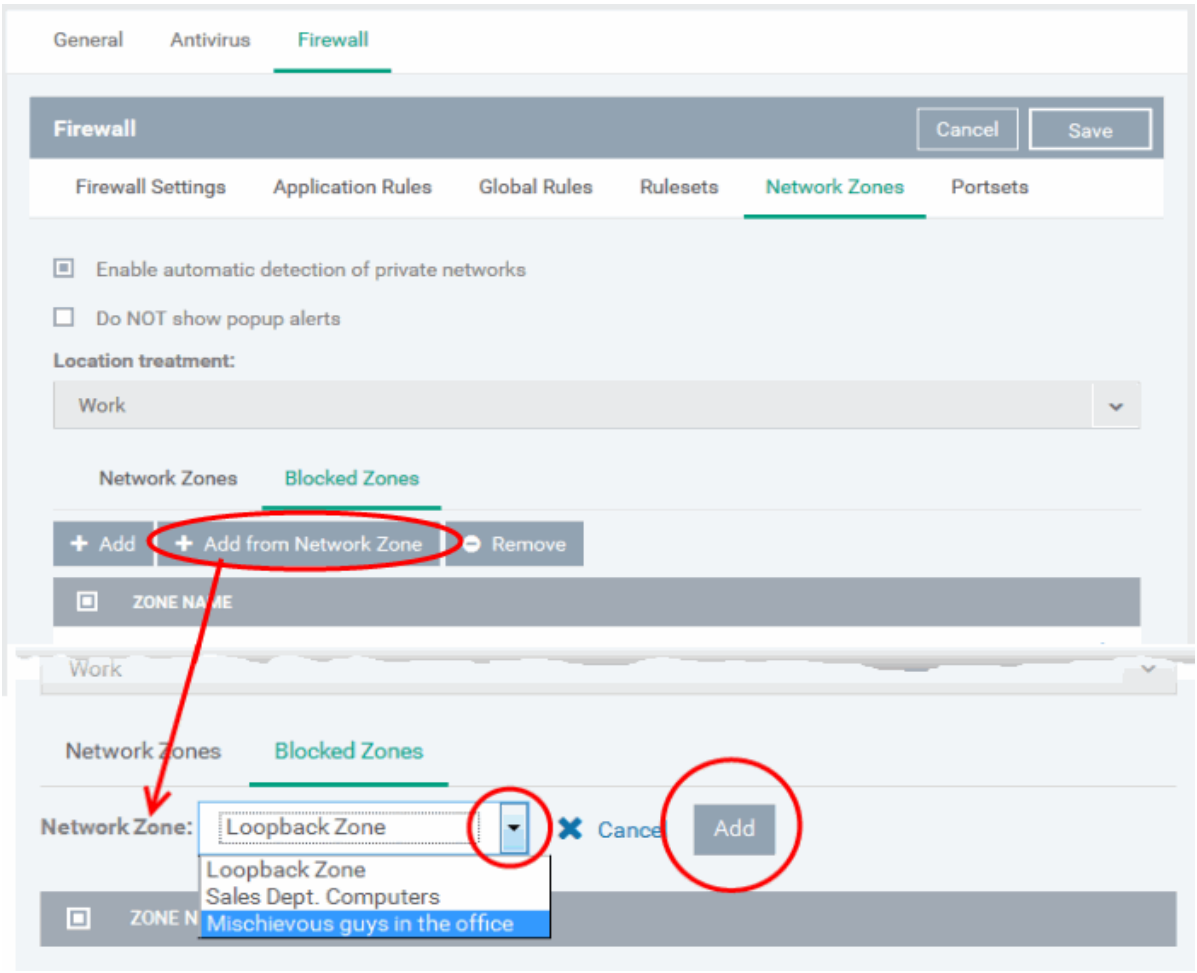
Note 1: You must create a zone before you can block it. There are two ways to do this;

1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *existing* zones from this interface (e.g. to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

To deny access to an existing network zone

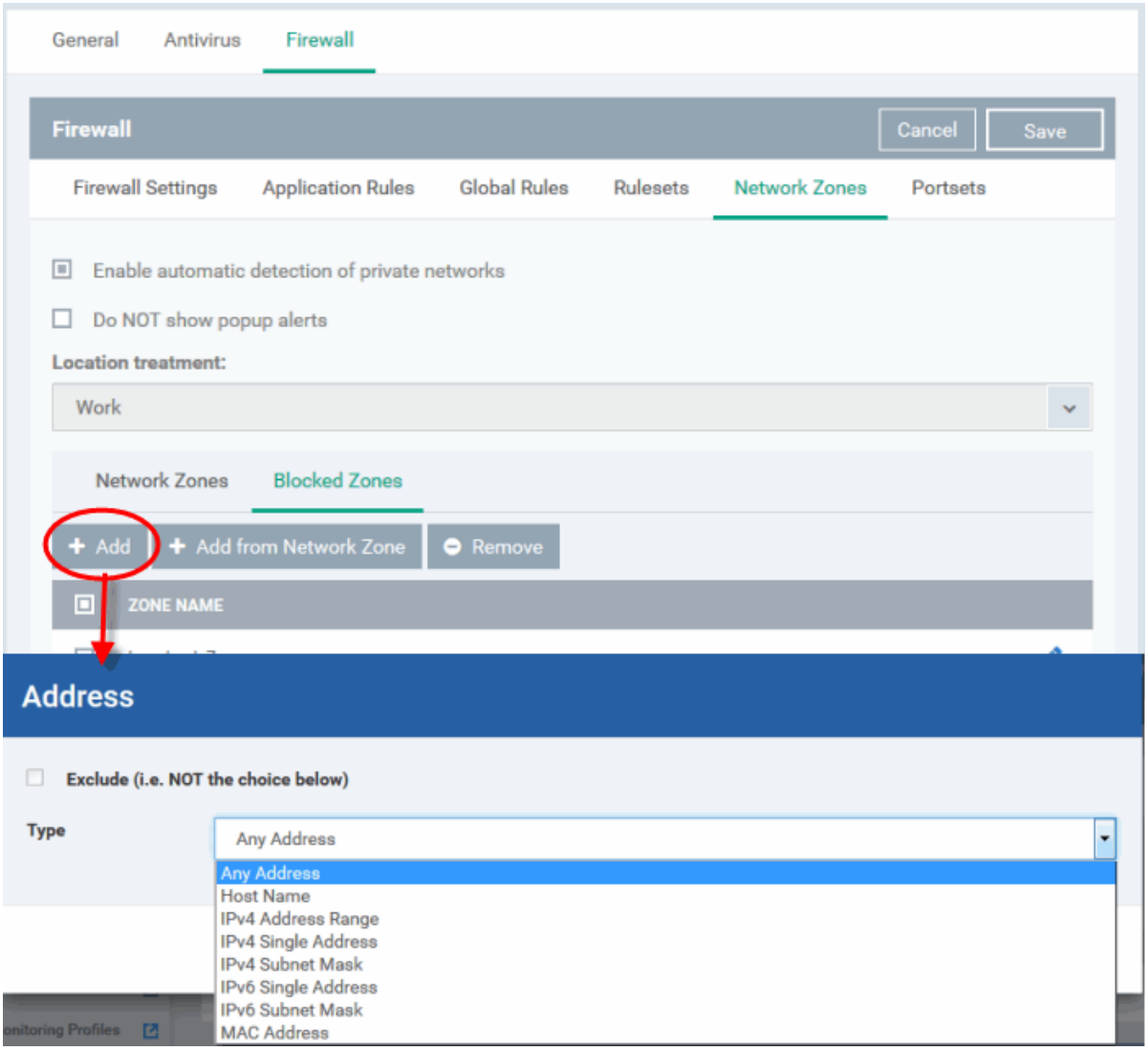
- Click 'Add from Network Zone' button from the top
- Choose the particular zone you wish to block from the 'Network Zone' drop-down.



- Click 'Add'
- Repeat the process to add more blocked network zones for the profile

To deny access to a network by manually defining a new blocked zone

- Click the 'Add' button from the top.



- Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

  Address Types:

  i. Any Address - Will block connections from all IP addresses (0.0.0.0- 255.255.255.255)

  ii. Host Name- Enter a named host which denotes an address on your network.

  iii. IPv4 Range - Will block access to the IPv4 addresses you specify in the 'Start Range' and 'End Range' text boxes.

  iv. IPv4 Single Address - Block access to a single address - e.g. 192.168.200.113.

  v. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to block.

  vi. IPv6 Single Address -Block access to a single address - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

  vii. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

  viii. MAC Address - Block access to a specific MAC address.

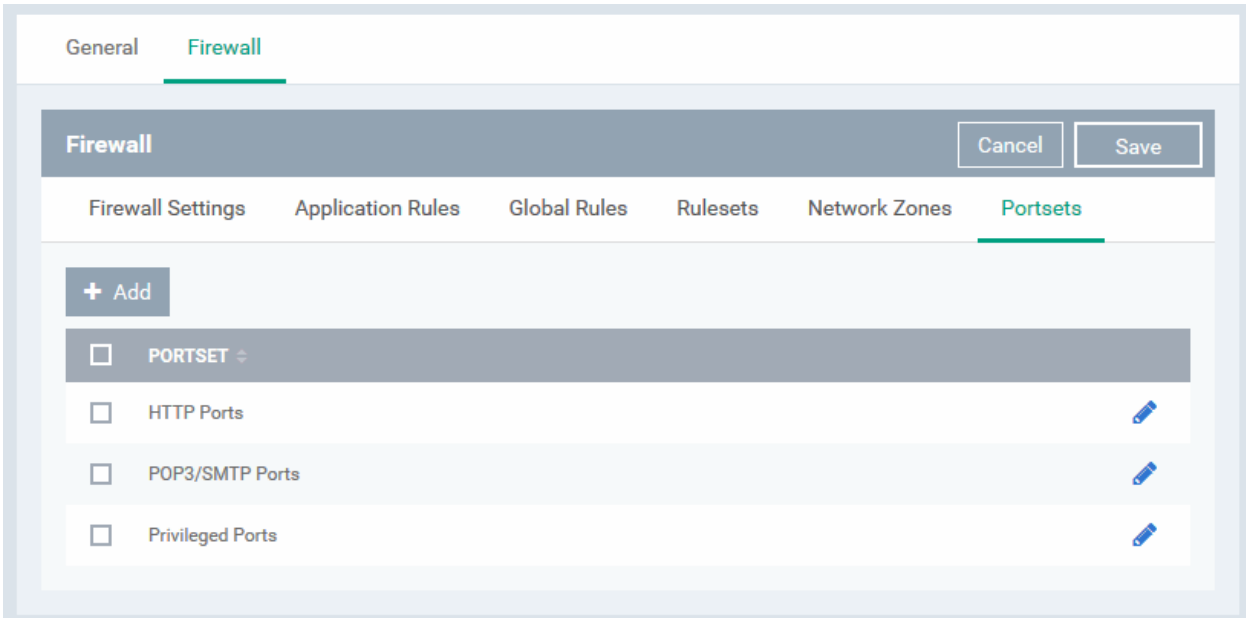
2. Select the address to be blocked and click 'OK'

The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

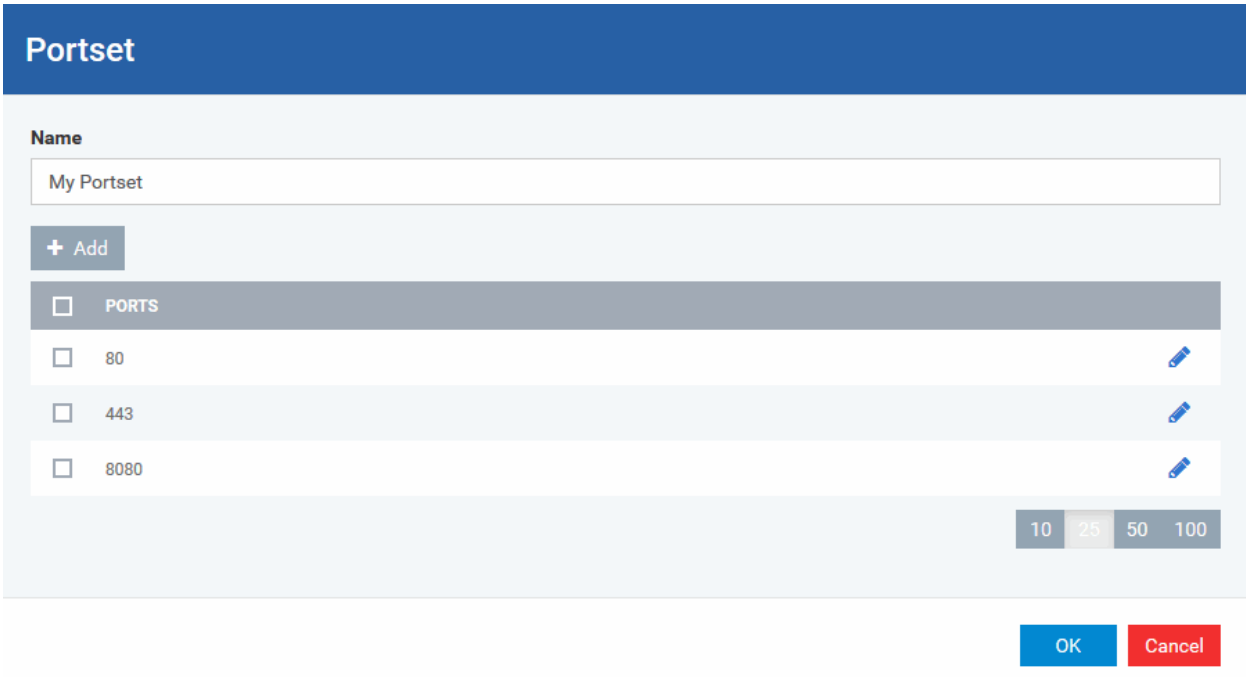
3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

Portsets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple Application Rules and Global Rules. The 'Port Sets' panel under the 'Firewall' tab allows you to view and manage pre-defined port sets and to add new port sets for the profile. The name of the port set is listed above the actual port numbers that belong to that set.



The panel lists all portsets that are defined for the profile. Clicking the 'Edit' icon beside a name reveals the ports included in the set.



ITSM ships with three default portsets:

- **HTTP Ports**: 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.
- **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
- **Privileged Ports:** 0-1023**.** This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

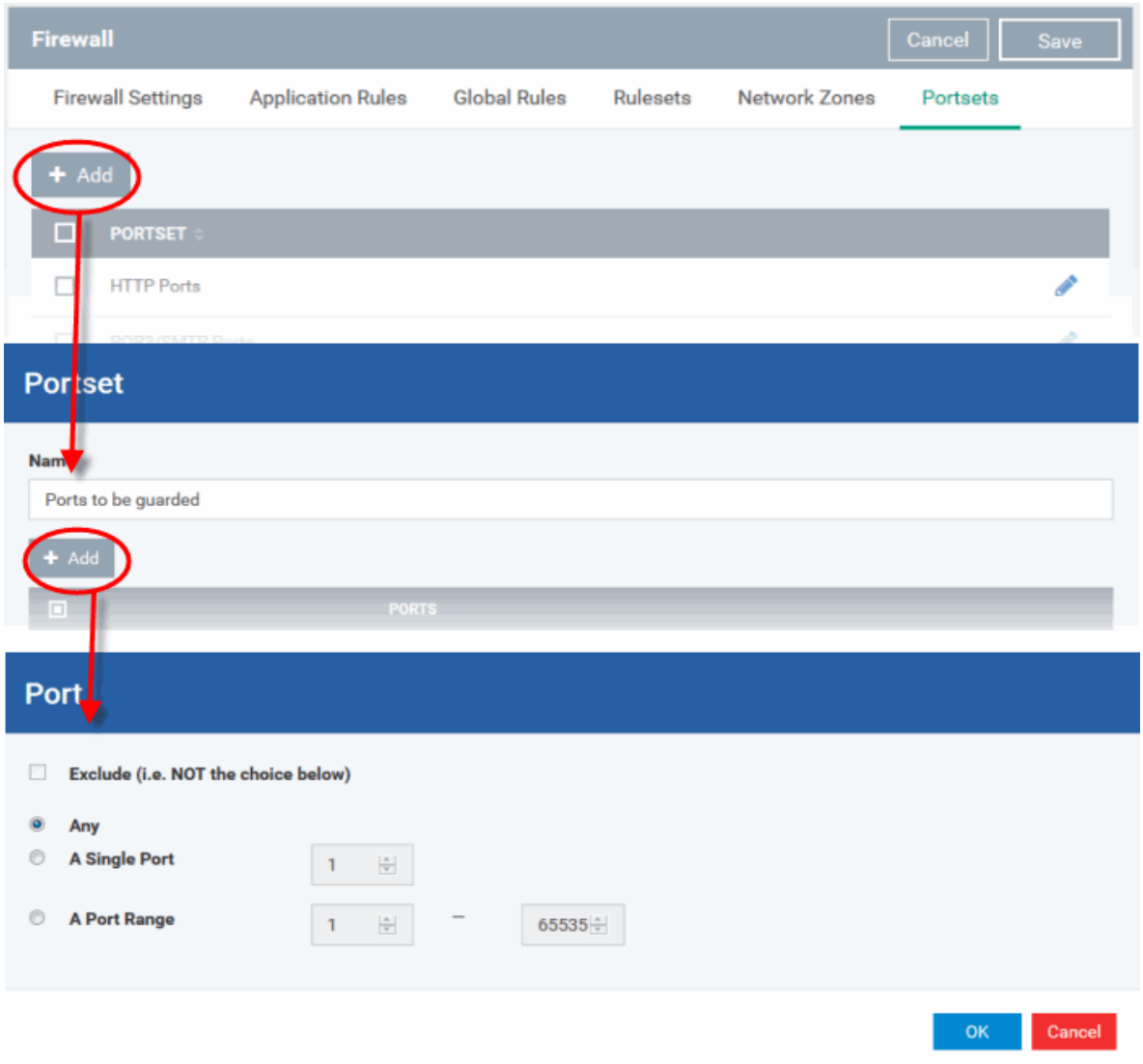
Defining a new Port Set

You can create new portsets and allow access to them for applications, with the access privileges specified through Application Rule interface. Refer to 'Creating or Modifying Firewall Rules' for more details.

To add a new portset

- Click the 'Add' button from the top.

The 'Portset' dialog will open.

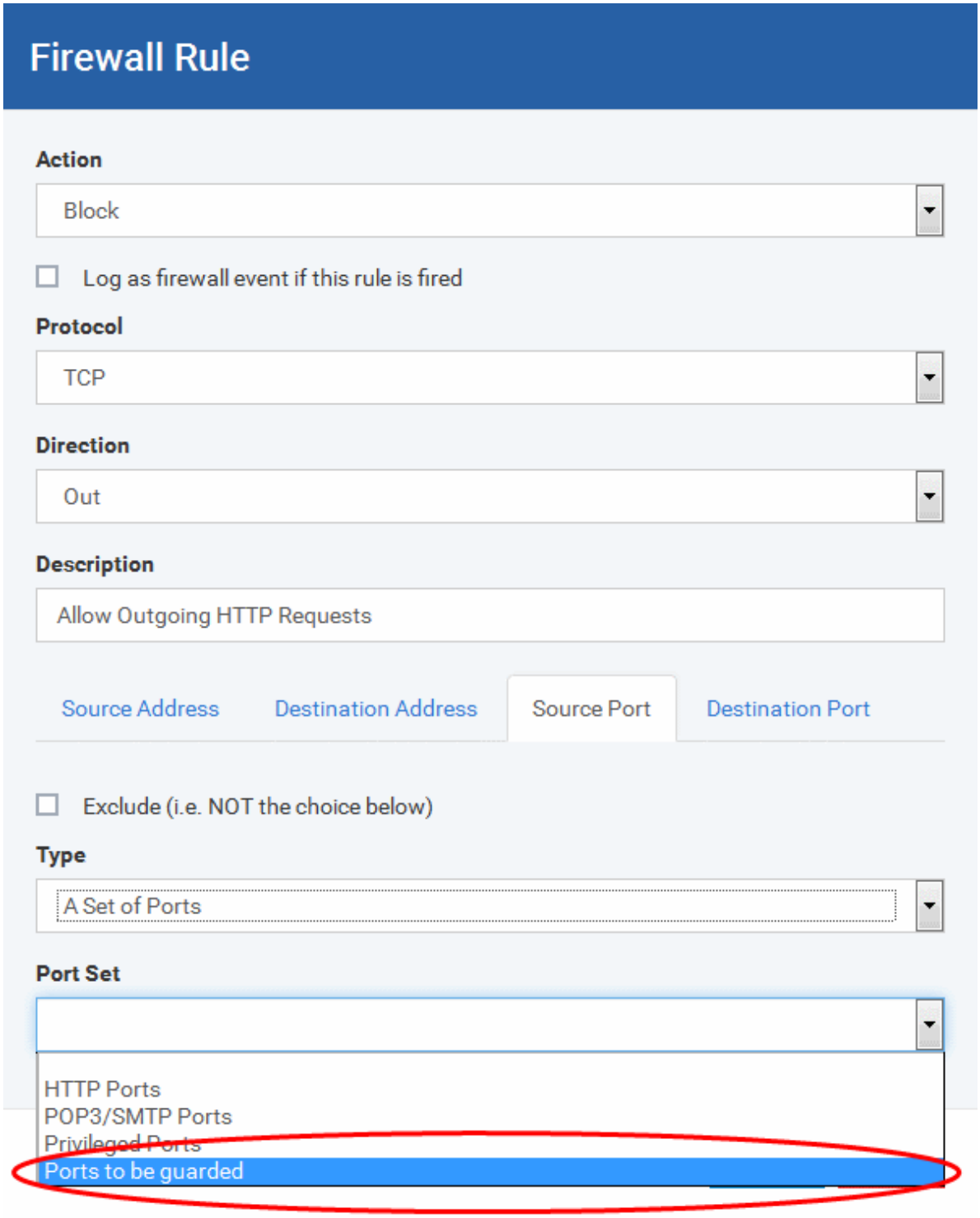


- Enter a name for the new portset in the 'Name' field.
- To add ports to the new portset, click the 'Add' button above the list of ports.

- Specify the ports to be included in the new portset:
  - **Any** - to choose all ports;
  - **A single port** - Define the port number in the combo box beside;
  - **A port range** - Enter the start and end port numbers in the respective combo boxes.
  - Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.
- Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
- Click 'OK' in the 'Portset' dialog to create the new portset.

Once created, a Portset can be:

- Quickly called as 'A Set of Ports' when creating or modifying a Firewall Ruleset



To edit an existing port set

- Click the 'Edit' icon beside the name of the portset. The 'Portset' dialog will appear with a list of port numbers in the port set.
- The editing procedure is similar to adding the portset explained above.

- Click the 'Save' button at the top of 'Firewall' interface to sane your settings for the profile.

The saved 'Firewall' settings screen will be displayed with options to edit the settings or delete the section. Refer to the section 'Editing Configuration Profiles' for more details.

6.1.3.1.5. HIPS Settings

The Host Intrusion Prevention System (HIPS) constantly monitors system activity and only allows executables and processes to run if they comply with security rules that have been enforced by the Windows profile applied to the managed computer. Comodo Client Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Administrators looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface and roll it out through the Windows profile.

To configure HIPS Settings and Rules

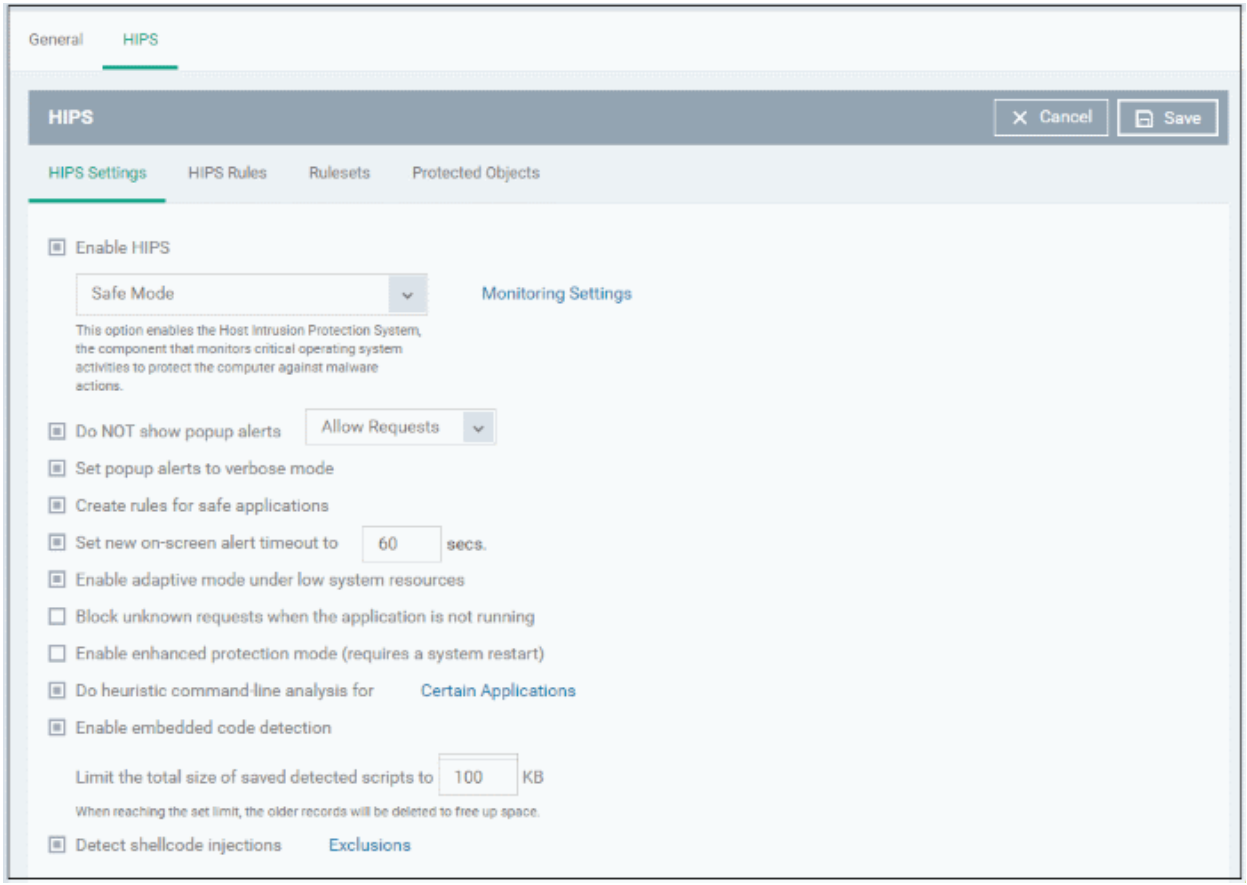
- Click 'HIPS' from the 'Add Profile Section' drop-down

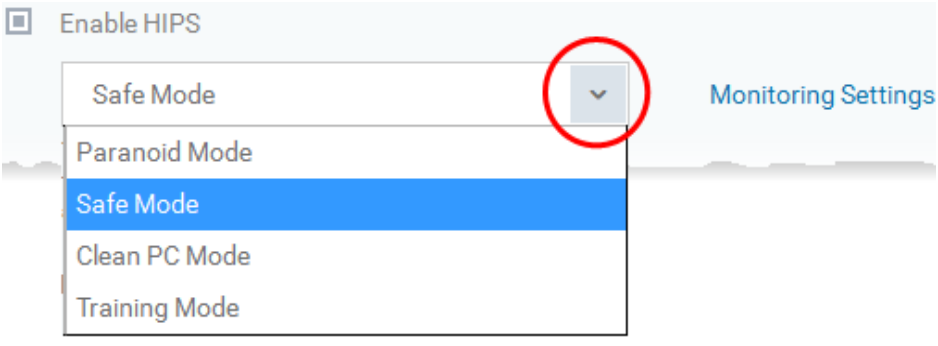
The HIPS settings screen will be displayed. It contains six tabs:

- HIPS Settings - Allows you to configure the settings that govern the overall behavior of the HIPS component.
- HIPS Rules - Allows you to view, create and modify rules that determine how the applications in the managed computer have to be protected
- Rulesets - Allows you view predefined rulesets and create new rulesets that can be applied to the applications on the managed computer.
- Protected Objects - Allows you to view and edit predefined 'Registry Groups' and 'COM Groups', create new groups so as to add them to Protected Objects.

HIPS Settings

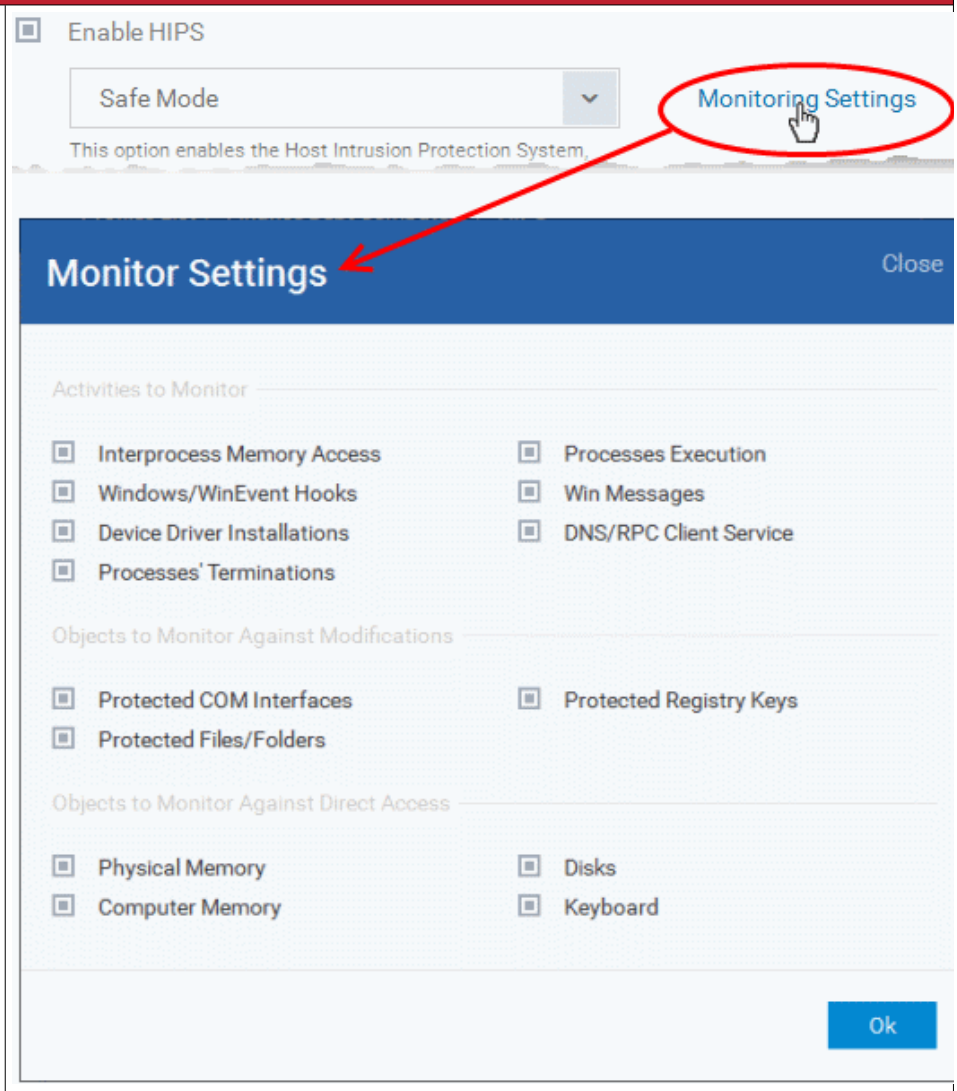
The HIPS settings panel under the HIPS tab allows you to enable/disable HIPS, set HIPS security level and configure HIPS' general behavior.



HIPS Settings - Table of Parameters	
Form Element	**Description**
Enable HIPS	Allows you to enable or disable HIPS protection for the managed computers to which the profile is applied. (***Default=Enabled***) If enabled, you can configure the HIPS security level and monitoring settings.
Hips Security Level	If HIPS is enabled, you can choose the security level for the HIPS to provide at the managed computer from the drop-down below 'Enable HIPS'.  The available options are: • **Paranoid Mode**: This is the highest security level setting and means that HIPS monitors and controls all executable files apart from those that you have deemed safe. Comodo Client Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Client Security does automatically create 'Allow' rules for any

HIPS Settings - Table of Parameters	
	executables - although the end user still has the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system. • **Safe Mode**: While monitoring critical system activity, HIPS automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules for these activities, if the option '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, the end-user will receive an alert whenever that application attempts to run. Should you choose, the end-user can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the HIPS not to generate an alert the next time it runs. If the endpoint is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts. • **Clean PC Mode:** From the time you set the setting to 'Clean PC Mode', HIPS learns the activities of the applications currently installed on the server while all new executables introduced to the server are monitored and controlled. This patent-pending mode of operation is the recommended option on a new server or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files with 'Unrecognized' rating in the '**File List** ' are excluded from being considered as clean and are monitored and controlled. • **Training Mode**: HIPS monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. The end-user will not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on the endpoints are safe to run.
Monitoring Settings	If HIPS is enabled, you can configure the activities, entities and objects that should monitored by it at the managed endpoint by clicking the 'Monitoring Settings' link.

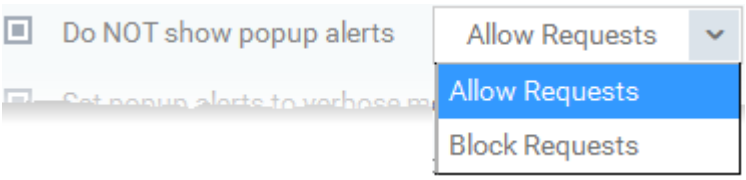
HIPS Settings - Table of Parameters	



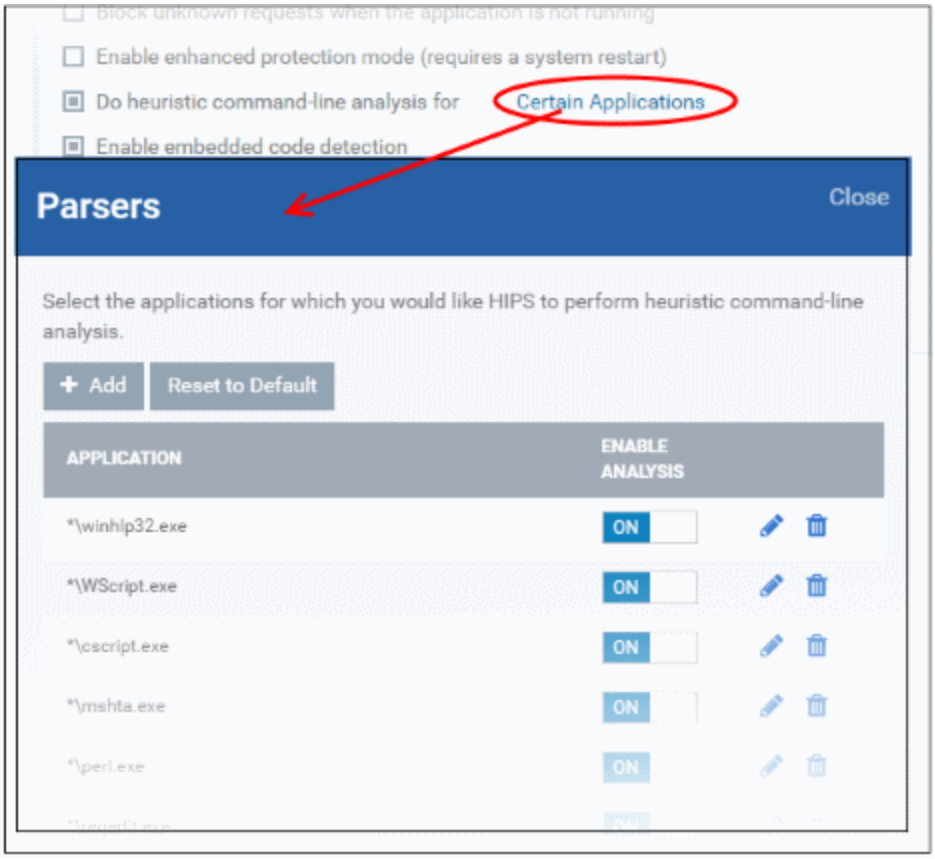
Activities To Monitor:

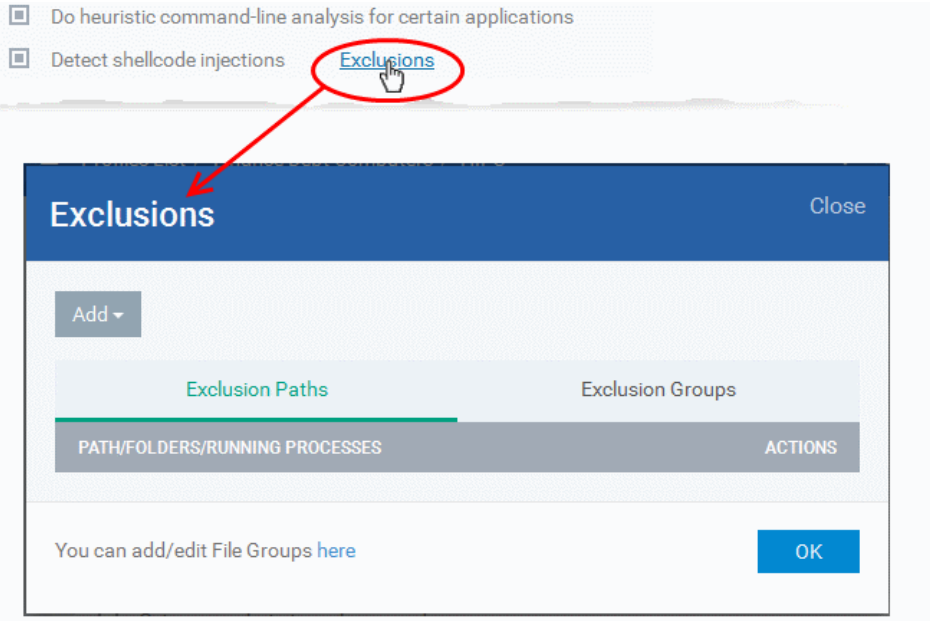
- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks. These include recording your keyboard strokes; modifying the behavior of applications and stealing data by sending confidential information from one process to another. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of a compromised process to 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this option selected, and HIPS generates alerts when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks -** In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events before they reach an application. Example intercepted events include messages, mouse actions and keystrokes. Hooks can react to these events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer and take remote control of your computer. Leaving this option selected means that

HIPS Settings - Table of Parameters	
	an alert is generated every time a hook is executed by an untrusted application *(Default = Enabled)*. • **Device Driver Installations -** Device drivers are small programs that allow applications and/or operating systems to interact with hardware devices on the managed computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on the system. The installation of a malicious driver could, obviously, cause irreparable damage to the computer or even pass control of that device to a hacker. Leaving this option selected means HIPS generates alerts every time a device driver is installed on the computer by an untrusted application *(Default = Enabled)*. • **Processes' Terminations -** A process is a running instance of a program. Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, HIPS monitors and generates alerts for all attempts by an untrusted application to close down another application *(Default = Enabled)*. • **Process Execution** - Malware such as rootkits and key-loggers often execute as background processes. With this setting enabled, HIPS monitors and generates alerts whenever a process is invoked by an untrusted application. *(Default = Enabled)*. • **Windows Messages -** This setting means Comodo Client Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) *(Default = Enabled)*. • **DNS/RPC Client Service -** This setting generates alerts if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' computers which send out the requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack *(Default = Enabled)*. **Objects To Monitor Against Modifications:** • **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. *(Default = Enabled)* • **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. *(Default = Enabled)*. • **Protected Files/Folders** enables monitoring of files and folders you specified from the **File Protection** pane. *(Default = Enabled)*. **Objects To Monitor Against Direct Access:** Determines whether or not Comodo Client Security should monitor access to system critical objects on the managed computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave

HIPS Settings - Table of Parameters	
	these settings enabled: • **Physical Memory:** Monitors your computer's memory for direct access by an applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code ***(Default = Enabled)***. • **Computer Monitor:** Comodo Client Security raises an alert every time a process tries to directly access the computer monitor. Although legitimate applications sometimes require this access, spyware can also use such access to take screen shots of the current desktop, record browsing activities of the user and more ***(Default = Enabled).*** • **Disks:** Monitors the local disk drives at the managed computer, for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***. • **Keyboard:** Monitors the keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke made on keyboard and can be used to steal passwords, credit card numbers and other personal data typed through the keyboard. With this setting is enabled, Comodo Client Security generates alerts every time an application attempts to establish direct access to the keyboard ***(Default = Enabled)***. **Note**: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a global basis - effectively creating a universal 'Allow' rule for that activity . This 'Allow' setting over-rules any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface.
Do NOT show popup alerts	Configure whether or not the HIPS alerts are to be displayed at the managed computer for the end-user to respond. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness (***Default = Enabled***). If you choose not to show alerts then you have a choice of default responses that CCS should automatically take - either 'Block Requests' or 'Allow Requests'. 
Set popup alerts to verbose mode	Enabling this option instructs CCS to display HIPS alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests ***(Default = Enabled).***
Create rules for safe applications	Automatically creates rules for safe applications in HIPS Ruleset ***(Default = Enabled)*** **Note:** HIPS trusts the applications if: • The application/file is rated as 'Trusted' in the **File List** • The application is from a vendor included in the **Trusted Software Vendors** list

HIPS Settings - Table of Parameters	
	• The application is included in the extensive and constantly updated Comodo safelist.
Set new on-screen alert timeout to	Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 60 seconds. You may adjust this setting to your own preference.
Enable adaptive mode under low system resources	Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems ***(Default = Enabled)***.
Block unknown requests when the application is not running	Selecting this option blocks all unknown execution requests if Comodo Client Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know the managed computer machine is already 'clean' and are looking just to enable the highest CCS security settings then it is OK to leave this option disabled. ***(Default = Disabled)***
Enable enhanced protection mode (Requires a system restart)	On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to counteract extremely sophisticated malware that tries to bypass regular HIPS protection. Because of limitations in Windows 7/8 x64 systems, some HIPS functions in previous versions of CCS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. ITSM requires a system restart for enabling enhanced protection mode. (***Default = Disabled***)
Do heuristic command-line analysis for certain applications	Selecting this option instructs Comodo Client Security to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscipt.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CCS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the Internet, for example, the alert will state 'test.vbs' is attempting to connect to the Internet (***Default = Enabled***). • If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'. The list of programs that are included by default can be viewed by clicking the 'Certain Applications' link.

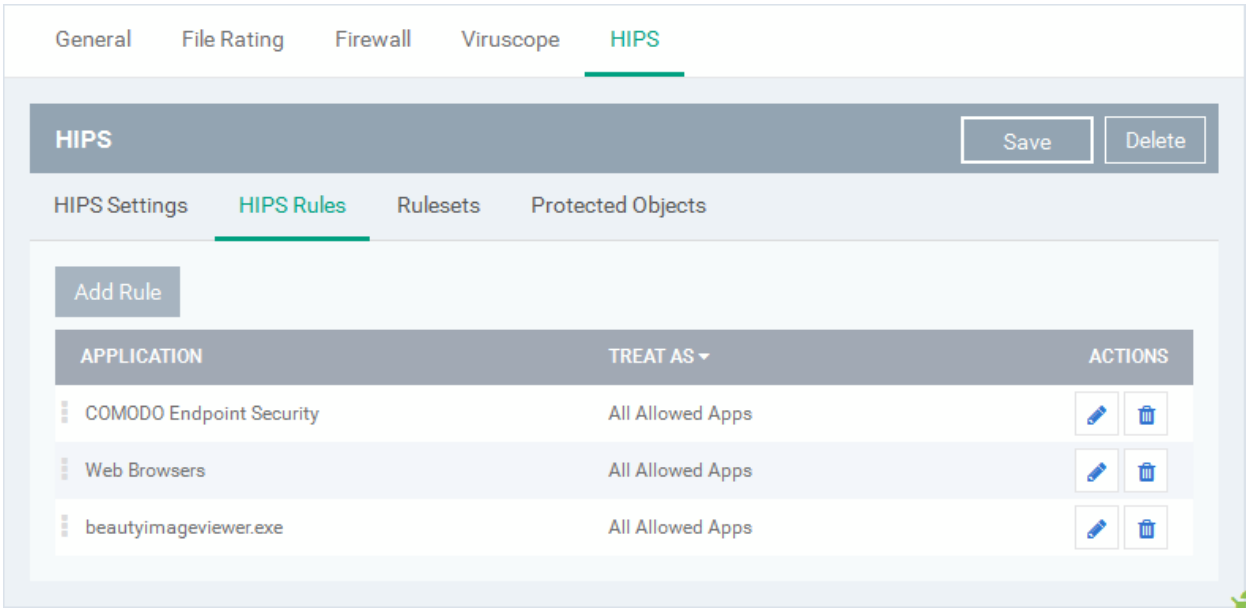
HIPS Settings - Table of Parameters	
	 • Use the slider beside the applications to enable/disable them for analysis. • Click the edit button to update the details of an application. • Click the trash can icon to remove an application from the list. • To include a new application to the list for analysis, click 'Add' at the top, provide the details and click 'Add' in the 'Add Parser' dialog. • To reset to default applications for analysis, click 'Reset to Default' at the top. • Click 'OK' at the bottom to apply your changes. Background note: 'Heuristics' describes the method of analyzing a file to ascertain whether it contains codes typical of a virus. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This helps to identify previously unknown (new) viruses.
Enable embedded code detection	If enabled, CCS will detect embedded codes (scripts) for "Fileless Malware" protection.
Detect shellcode injections	Enabling this setting turns-on the Buffer over flow protection. Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Turning-on buffer overflow protection instructs the Comodo Client Security to raise pop-

HIPS Settings - Table of Parameters	
	up alerts in every event of a possible buffer overflow attack. The end-user can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor. Comodo recommends this setting is left enabled *(Default = Enabled)*. You can also add files/folders and/or file groups to be excluded from Shellcode injections. To add exclusions, click the 'Exclusions' link after enabling this option.  The process of adding exclusions is similar to adding exclusions for containing in Containment Settings. Refer to the explanation of adding files / folders to be excluded in the previous section Containment Settings.

HIPS Rules

The 'HIPS Rules' screen allows you to view the list of active HIPS rulesets applied to different groups of or individual applications and to create and manage rules for the profile. You can change the ruleset applied to a selected application or application group.

Note: HIPS Rulesets are to be created before applying them to an individual application or an application group. Refer to the next section Rulesets for details on creating new rulesets.



HIPS Rules - Column Descriptions	
Column Header	**Description**
Application	Name of the individual application or the application to which the ruleset is applied
Treat As	The ruleset applied. For more details on the rulesets, refer to the next section Rulesets.
Actions	Contains control buttons to edit or remove the rule

Creating and Modifying Hips Rules

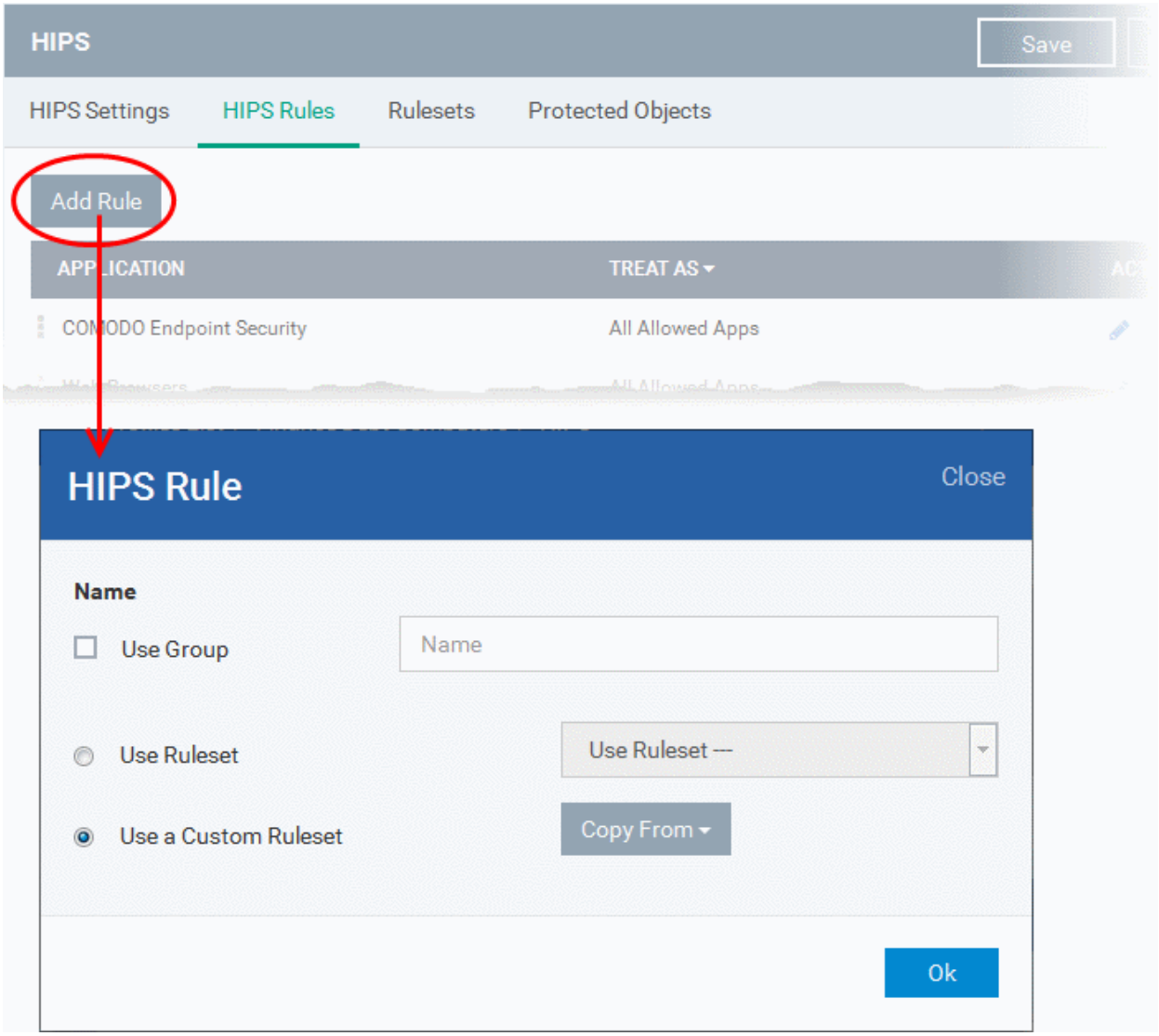
To begin defining an application's HIPS rule, you need take two basic steps.

- Step 1 - Select the application that you wish the ruleset is to be applied.
- Step2 - Configure the rules for this application's ruleset.

Step 1 - Select the application that you wish the ruleset is to be applied

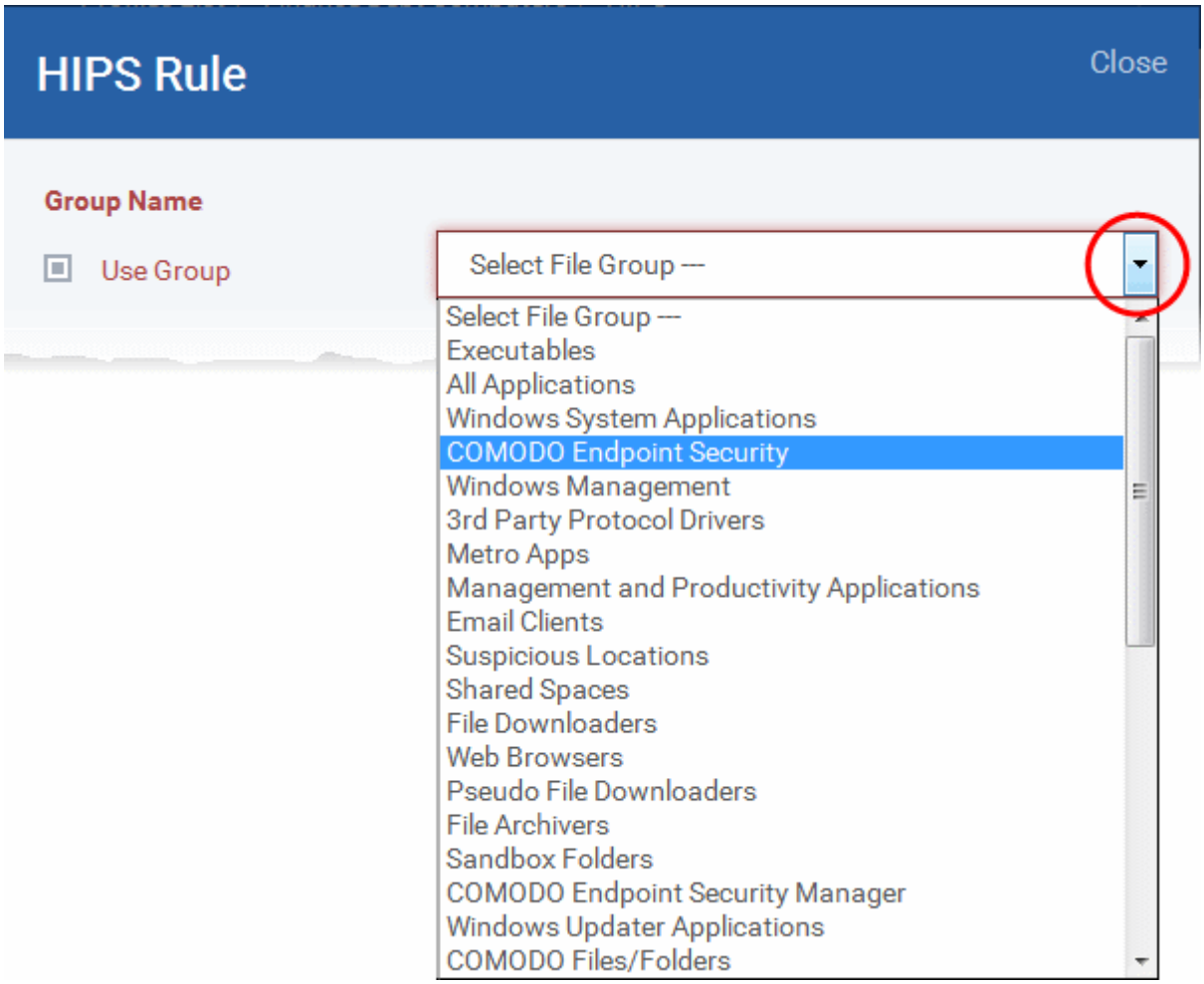
- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add Rule' button at the top of the list in the 'HIPS Rules' interface.

The 'HIPS Rule' interface will open as shown below:



Because this is a new application, the 'Name' field is blank. (If you are modifying an existing rule, then this interface shows the individual rules for that application's ruleset).

- To create a rule for a single application enter the file name of it in the 'Name' field
- To create a rule for an application group, select 'Use Group' and choose the file group from the drop-down

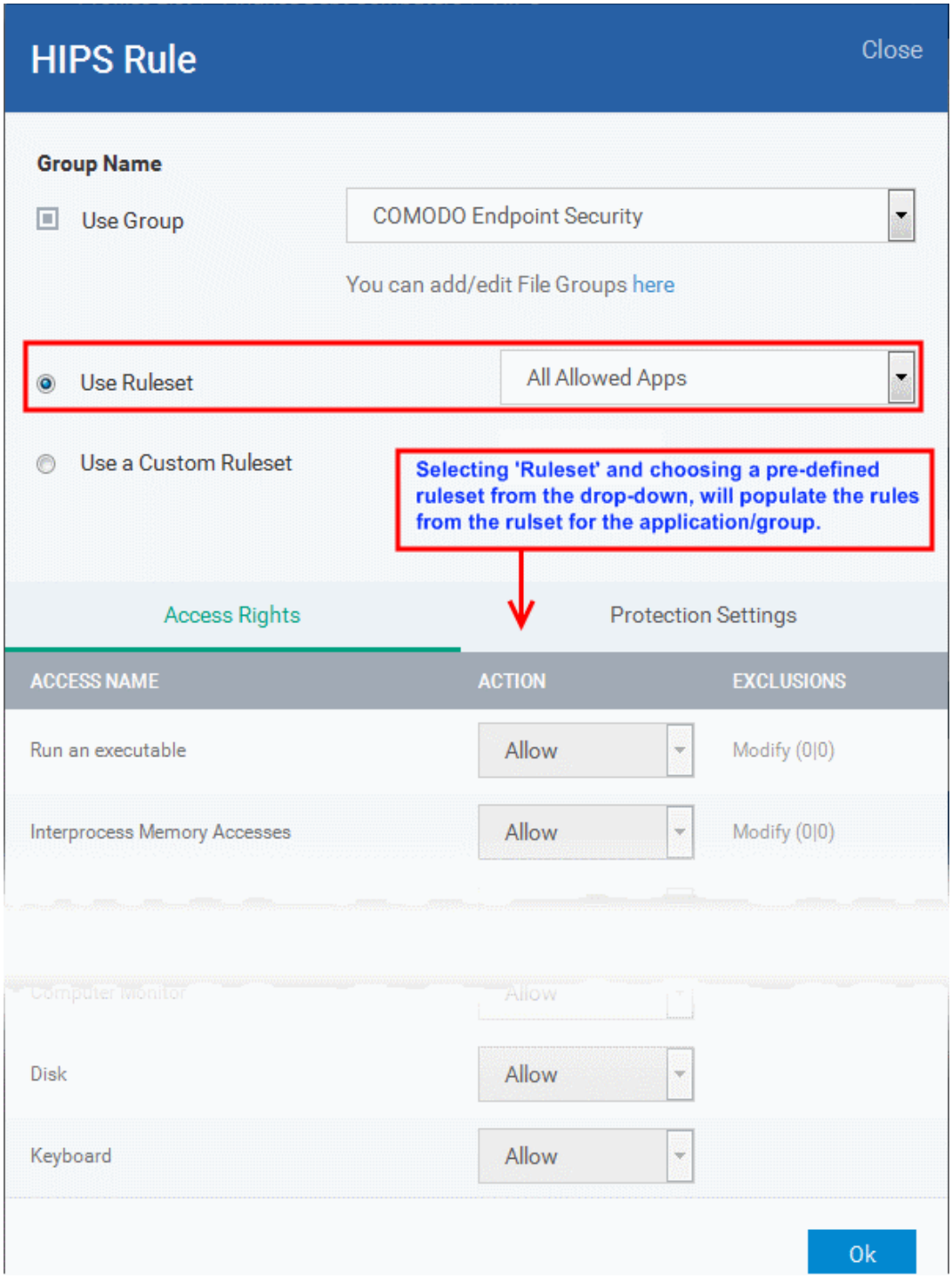


Note: ITSM ships with a set of predefined file groups containing collections of files under respective categories. Administrators can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can be created under 'Settings' > 'System Templates' > 'File Groups Variables' interface. Refer to the section File Groups for more details.

Step 2 - Configure the rules for this application's ruleset

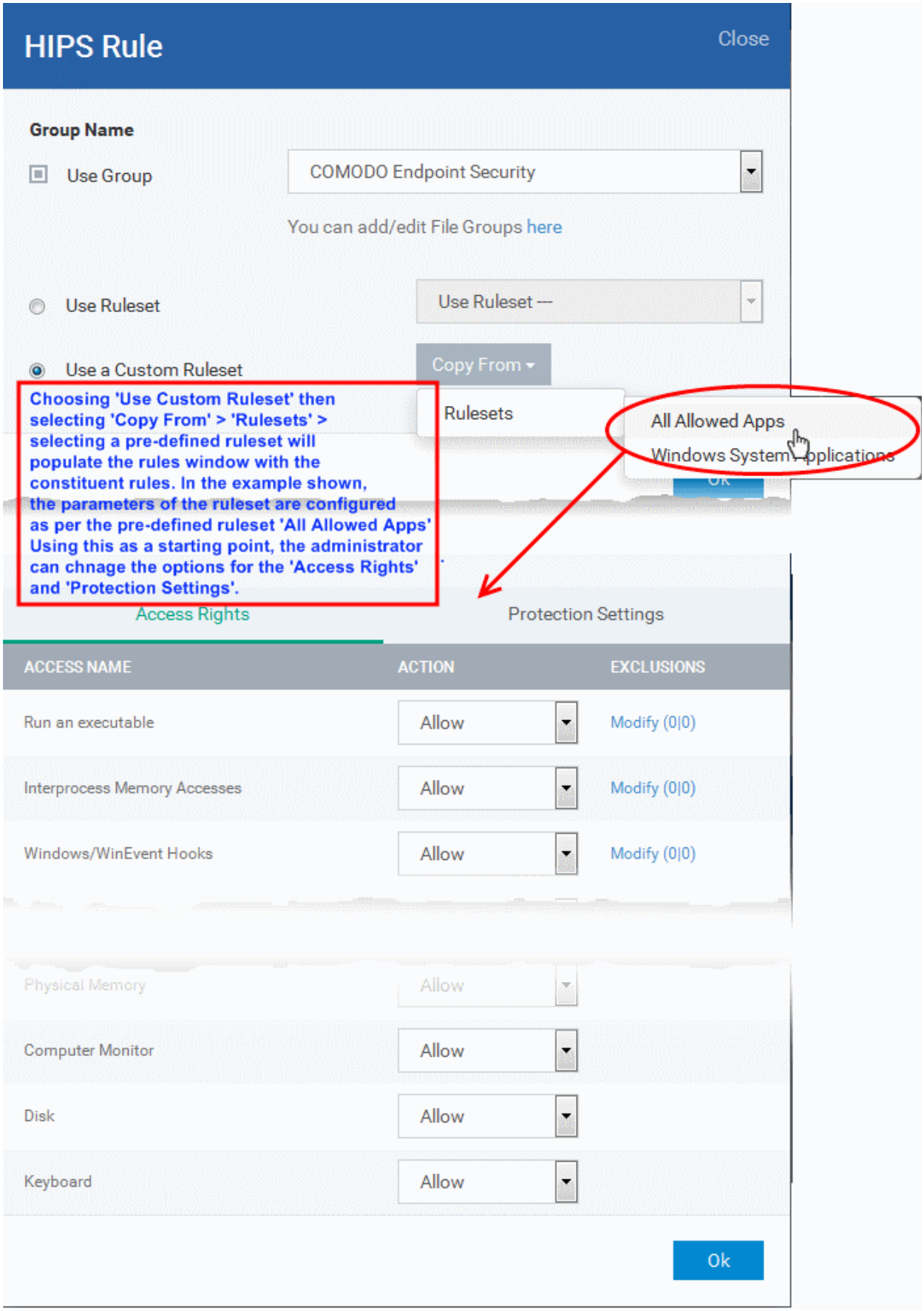
There are two broad options available for creating a ruleset that applies to an application - Use a Predefined Ruleset or Use a Custom Ruleset.

- **Use a Predefined Ruleset** - Allows you to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. The name of the predefined ruleset you choose is displayed in the '**Treat As** ' column for that application in the 'HIPS Rules' interface.



Note: Predefined Rulesets, once chosen, cannot be modified *directly* from this interface - they can only be modified and defined using the Ruleset interface. If you require the ability to modify components of the rule set, then you are effectively creating a new, custom ruleset and should choose the more flexible Use Custom Ruleset option instead.

- **Use a Custom Ruleset** - Designed for more experienced administrators, the 'Custom Ruleset' option grants full control over the configuration of each rule within that ruleset. The custom ruleset has two main configuration areas - Access Rights and Protection Settings. *(Default = Enabled)*



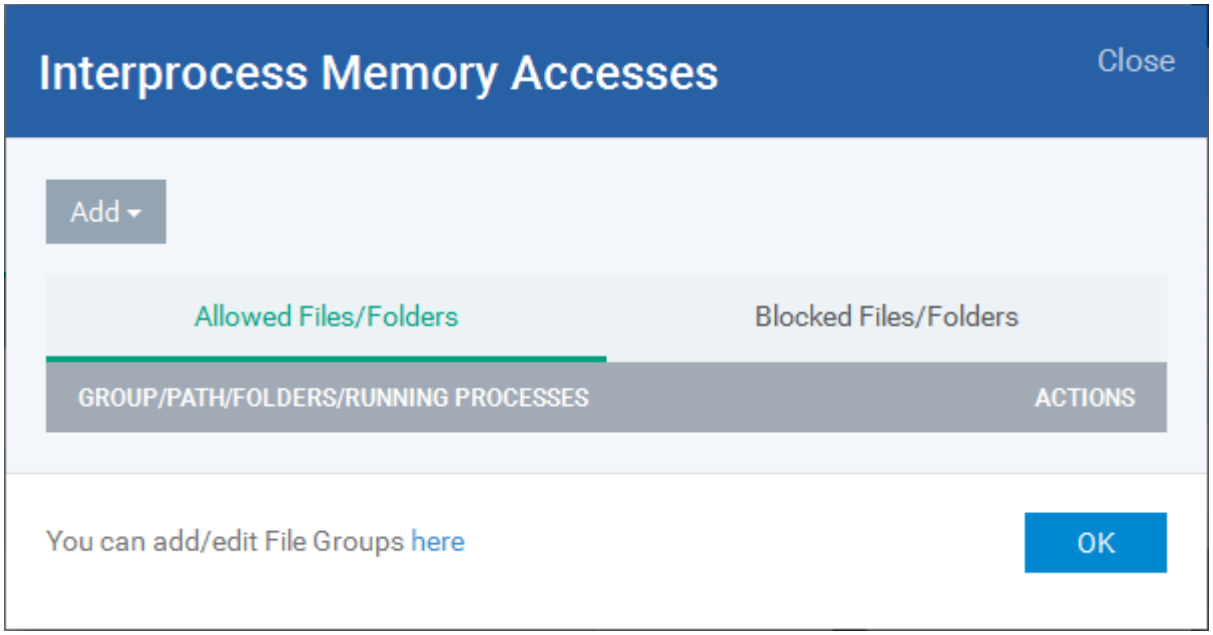
In simplistic terms 'Access Rights' determine what the application *can do to other processes and objects* whereas 'Protection Settings' determine what the application *can have done to it by other processes*.

i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be

performed by the applications in your custom ruleset.

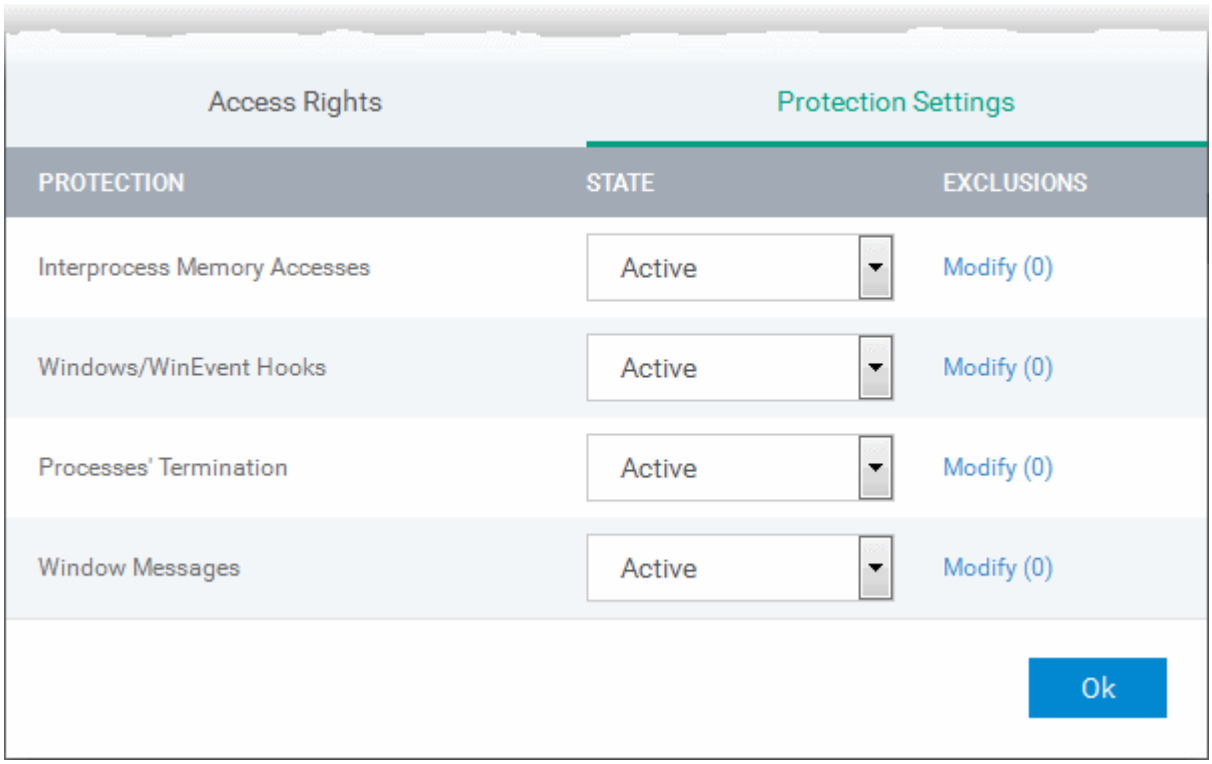
Refer to the section **HIPS Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:

- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.



- Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection State' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

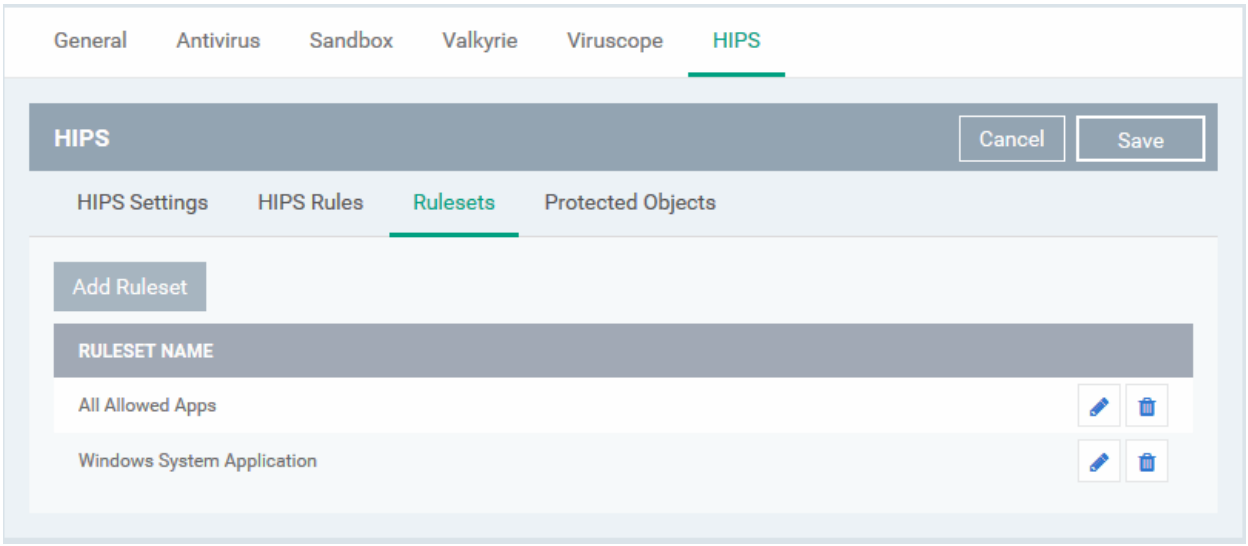
Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

7. Click 'OK' to confirm your settings.

Rulesets

A Pre-defined ruleset is a set of access rights and protection settings that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of rules and each of these rules is defined by a set of conditions/settings/parameters. Rulesets concern an application's access rights to memory, other programs, the registry etc.

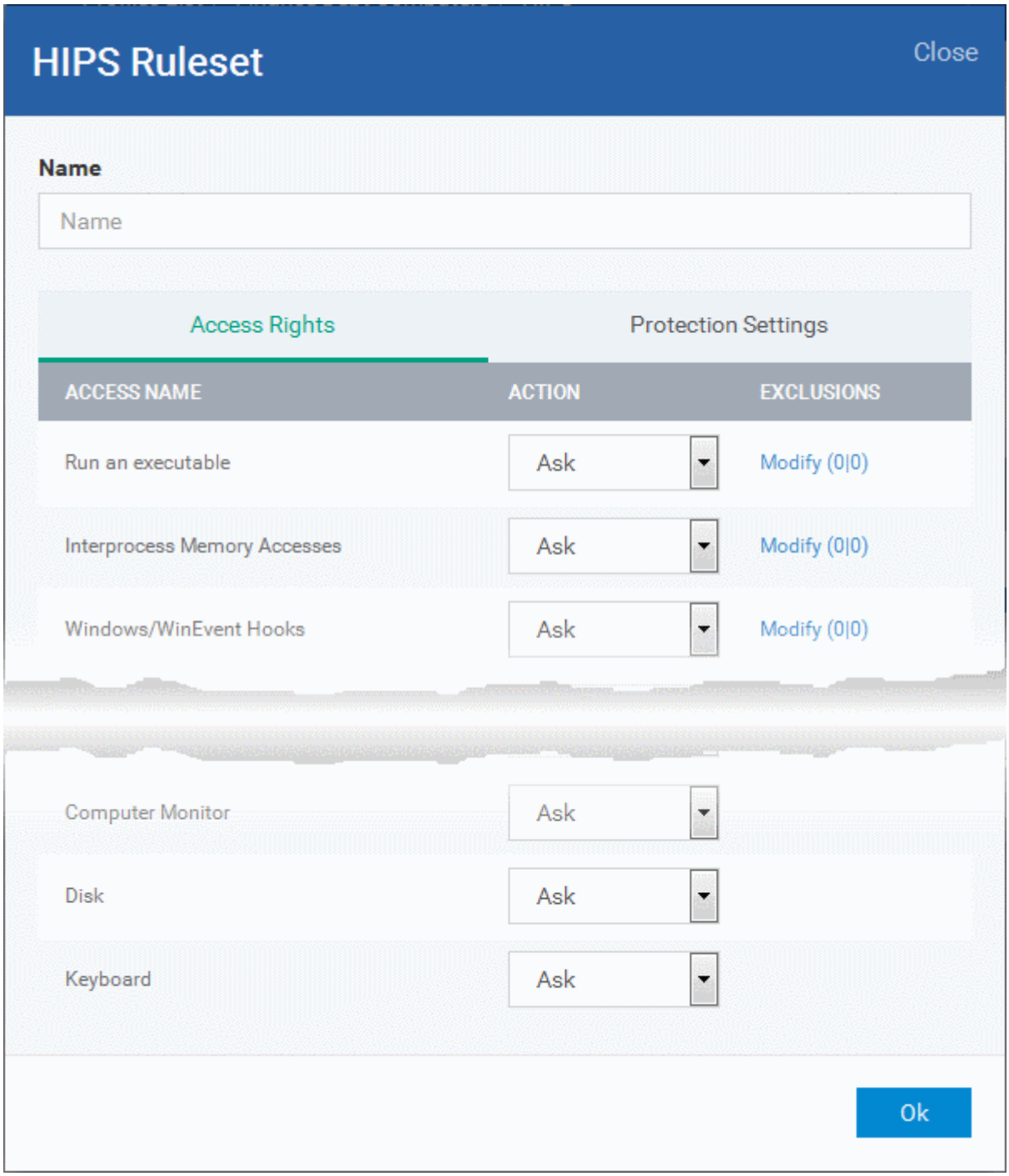
The Rulesets screen under the the 'HIPS' tab displays the list of rulesets and allows you to add and manage new rulesets.



To add a new ruleset

- Click the 'Add Ruleset' button  above the list of rulesets.

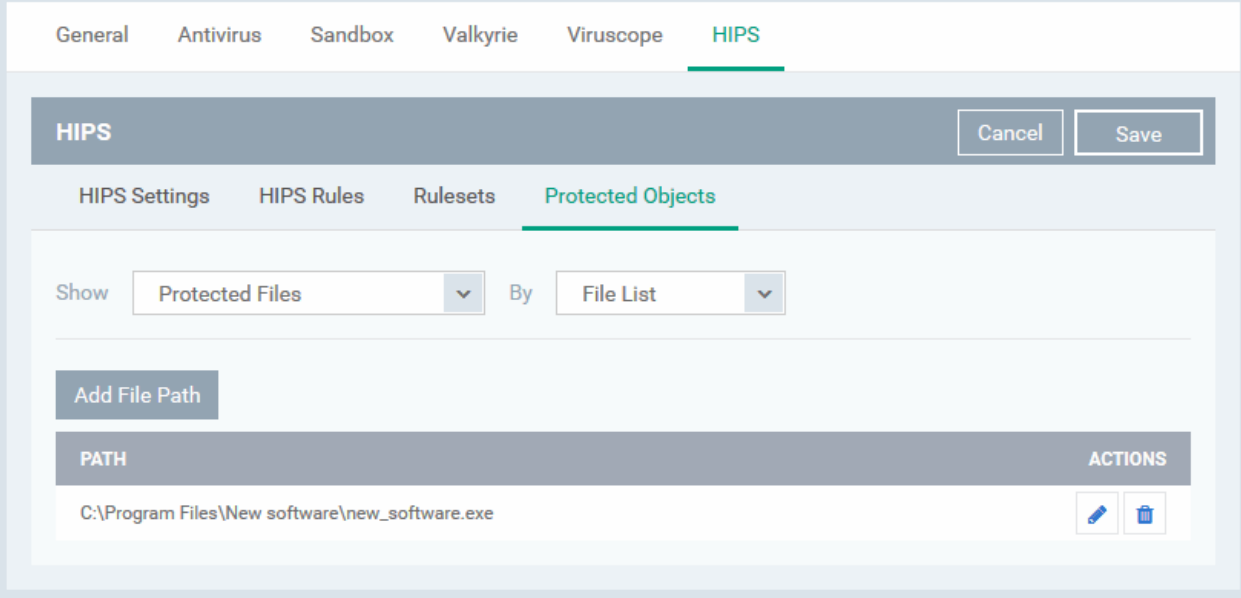
The 'HIPS Ruleset' dialog will appear.



- Enter a name for the ruleset
- Configure the Actions, states and exclusions for **'Access Rights' and 'Protection Settings'** as explained above. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset. The new ruleset will be available for deployment to HIPS rule for applications/application groups from the HIPS Rules interface.
- To edit a ruleset, click the Edit button under the Actions in the Rulesets interface. The Editing process is similar to the Ruleset creation process explained above.

Protected Objects

The 'Protected Objects' panel under 'HIPS' tab allows you to protect specific files and folders, system critical registry keys and COM interfaces at the managed computers, against access or modification by unauthorized processes and services. You can also add files in 'Protected Data Folders', so that 'Contained' programs will be blocked from accessing them.



The 'Show' drop-down allows you to choose the category of protected objects to be displayed in the list and add and manage the protected objects of that category. You can add following categories of protected objects:

- **Protected Files** - Allows you to view and specify programs, applications, files an file groups that are to be protected from changes
- **Registry Keys** - Allows you to view and specify registry keys that are to be protected from changes
- **COM Interfaces** - Allows you to view and specify COM interfaces that are to be protected from changes
- **Protected Data Folders** - Allows you to view and specify folders containing data files that are to be protected from changes by 'Contained' programs

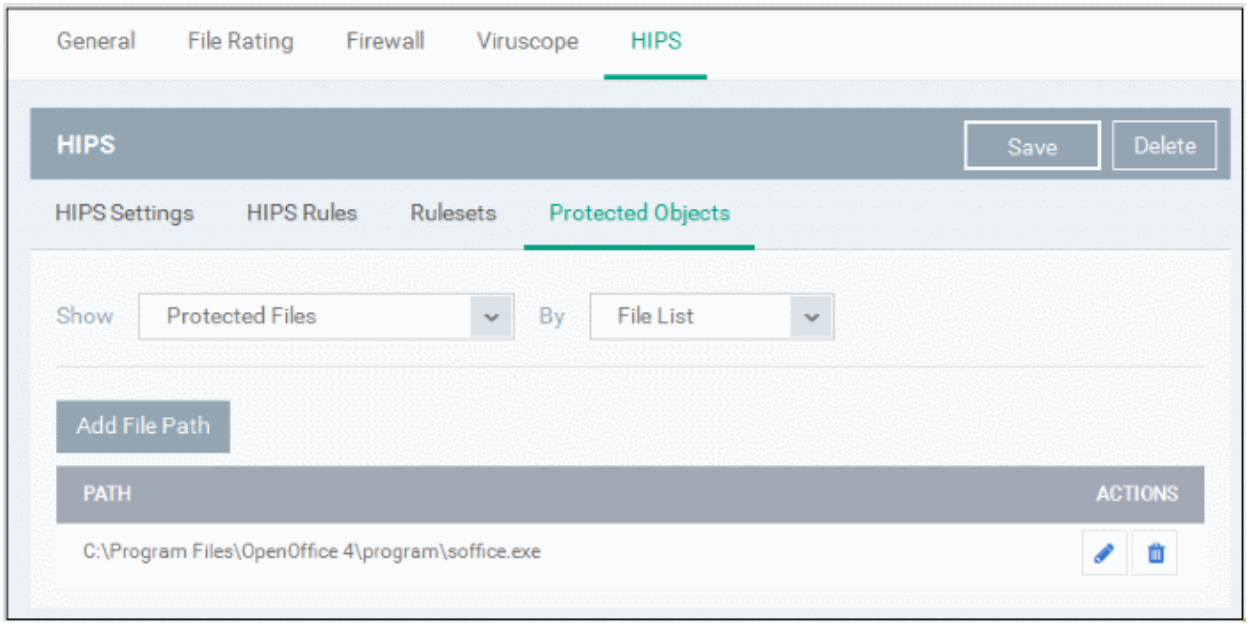
Protected Files

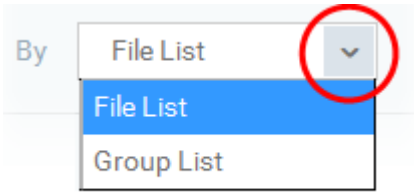
The 'Protected Files' list under 'Protected Objects' interface allows you to view and manage list of files and file groups that are to be protected from access by other programs, especially malicious programs such as virus, Trojans and spyware at the managed computer. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Client Security blocks this attempt and produces a 'Protected File Access' pop-up alert.

If you add a file to 'Protected Files', but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. Refer to the explanation of **adding 'Exceptions' at the end of this section** for more details about how to allow access to files placed in Protected Files.

- To view the list of Protected Files, choose 'Protected Files' from the 'Show' drop-down in the 'Protected Objects' interface

The Protected File list is displayed under two categories, which can be selected from the drop-down at the right.



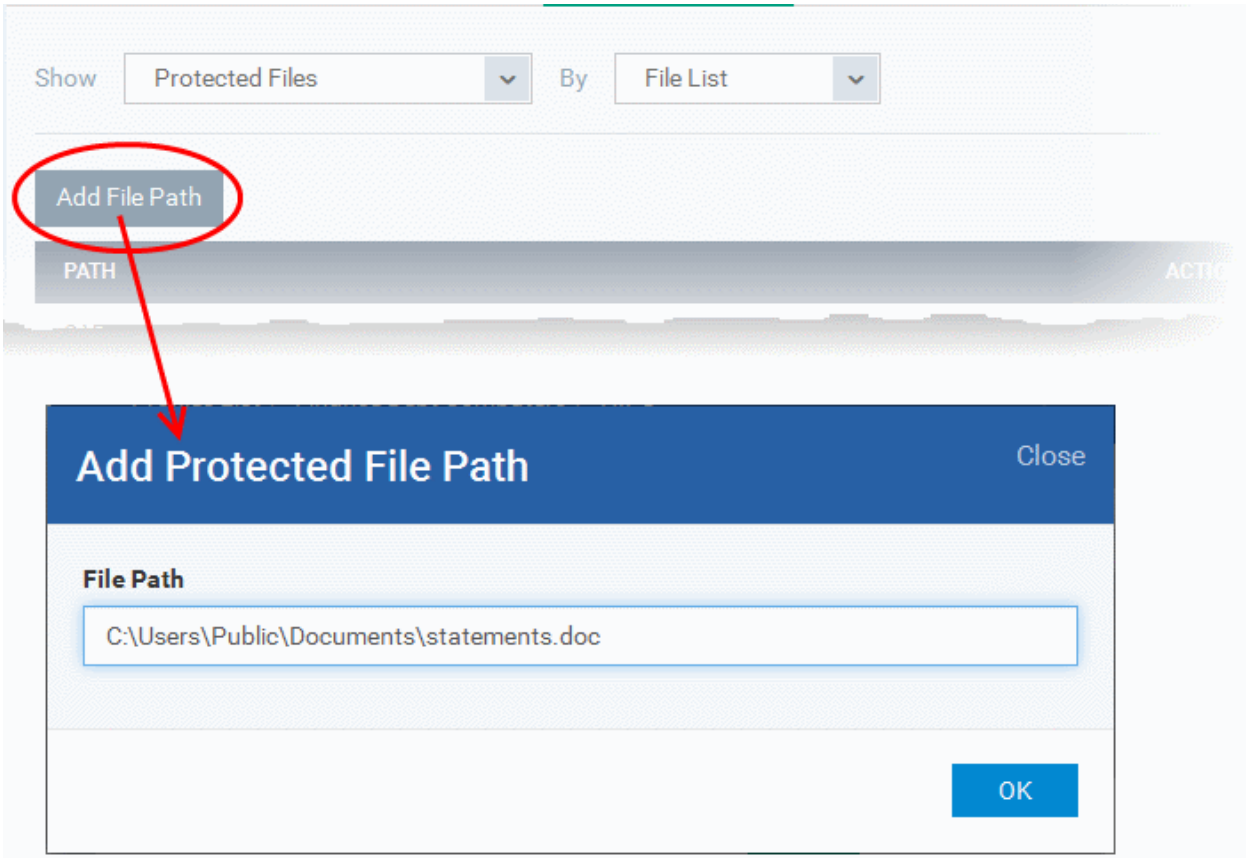


- To view the list of individual files, programs, applications added to the Protected Files list and manage them, choose 'File List'
- To view the File Groups added to the Protected File list, choose 'Group List'

You can add individual files, programs, applications or file/groups to 'Protected Files'.

To add an individual file, program or an application

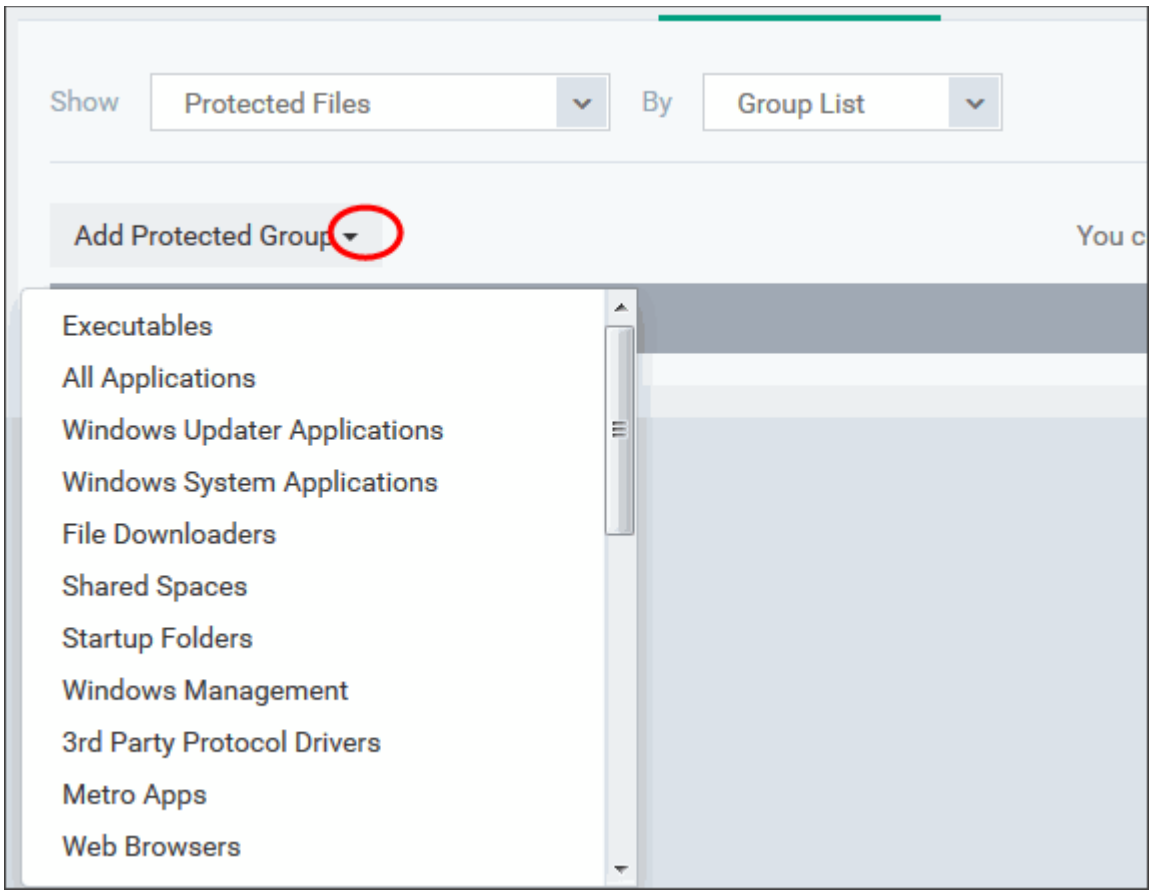
- Choose 'File List' from the drop-down at the right and click the 'Add File Path' button.



- Enter the installation/storage path with file name of the file to be protected, in the managed computers, in the 'Add Protected File Path' dialog and click 'OK'.
- Repeat the process to add more files.
- To edit the path of an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add an application/file group to the Protected Files list

- Choose 'Group List' from the drop-down at the right and click the 'Add Protected Group' button



- Choose the file group from the drop-down and click 'OK'.

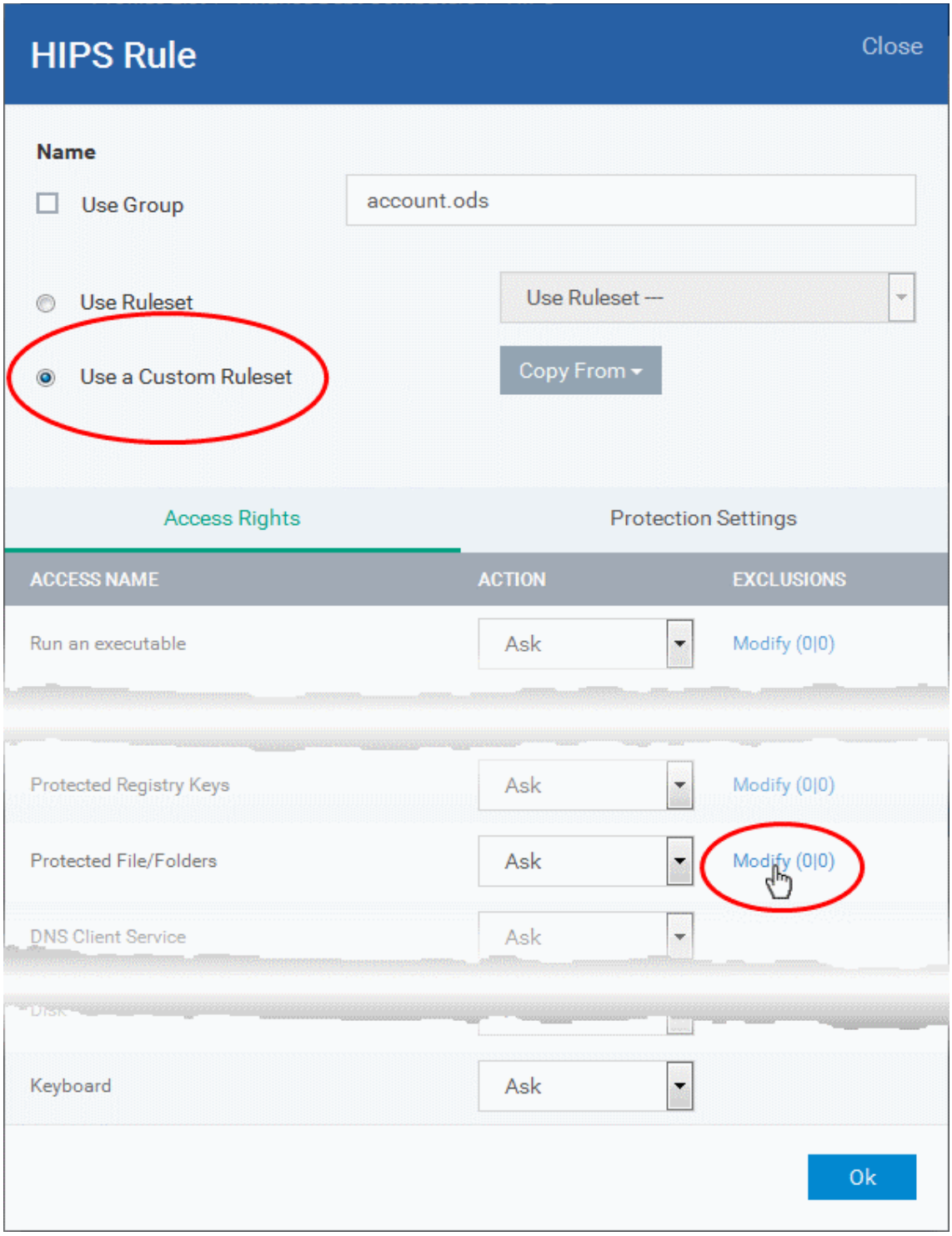
Note: ITSM ships with a set of predefined file groups containing collections of files under respective categories. Administrators can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can be created under 'Settings' > 'System Templates' > 'File Groups Variables' interface. Refer to the section File Groups for more details.

- Repeat the process to add more file groups.
- To edit the path of an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

Exceptions

You can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in 'HIPS Rules' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the 'Open Office Calc' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first add the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into 'HIPS Rules' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

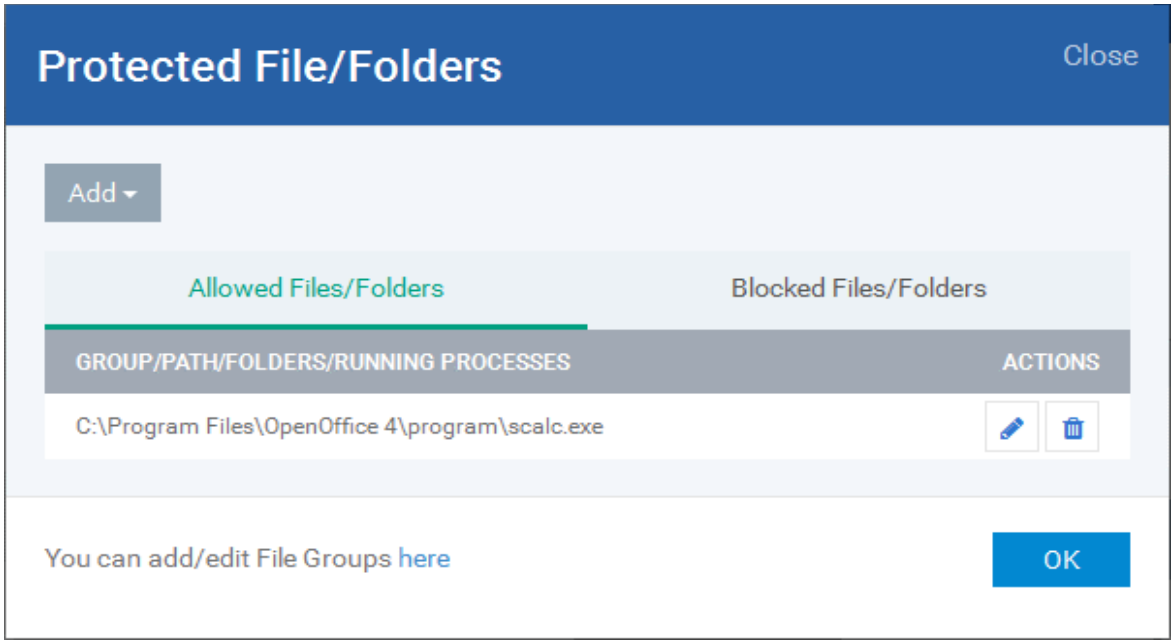
- First add Accounts.ods to 'Protected Files' area as explained above.
- Then go to 'HIPS Rules' interface and add it to the list of applications.
- In the 'HIPS Rule' interface, enter the file name as account.ods, choose 'Use a Custom Ruleset' and select a ruleset from the 'Copy From' drop-down.
- Under 'Access Rights' tab, set all the rules to 'Ask'



- Click the 'Modify' beside 'Protected File/Folders'
- Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'.

The 'Protected Files/Folders' interface will appear.

- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.

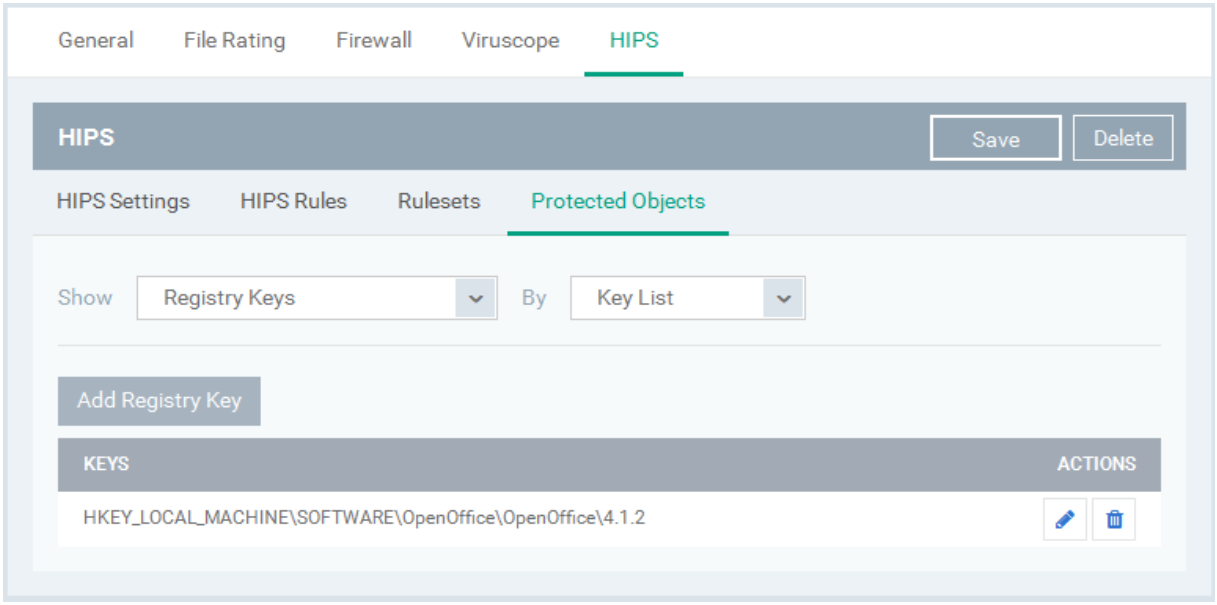


Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to 'HIPS Rules', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

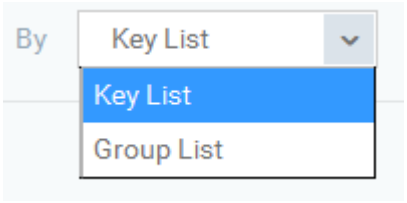
Registry Keys

The 'Registry Keys' list under 'Protected Objects' interface allows you to view and manage list of critical registry keys and registry groups to be protected against modification. Irreversible damage can be caused to the managed endpoint if important registry keys are corrupted or modified in any way. It is essential that the registry keys are protected against any type of attack.

To view the list of Protected Registry Keys, choose 'Registry Keys' from the 'Show' drop-down in the 'Protected Objects' interface



The Protected Registry Keys list is displayed under two categories, which can be selected from the drop-down at the right.

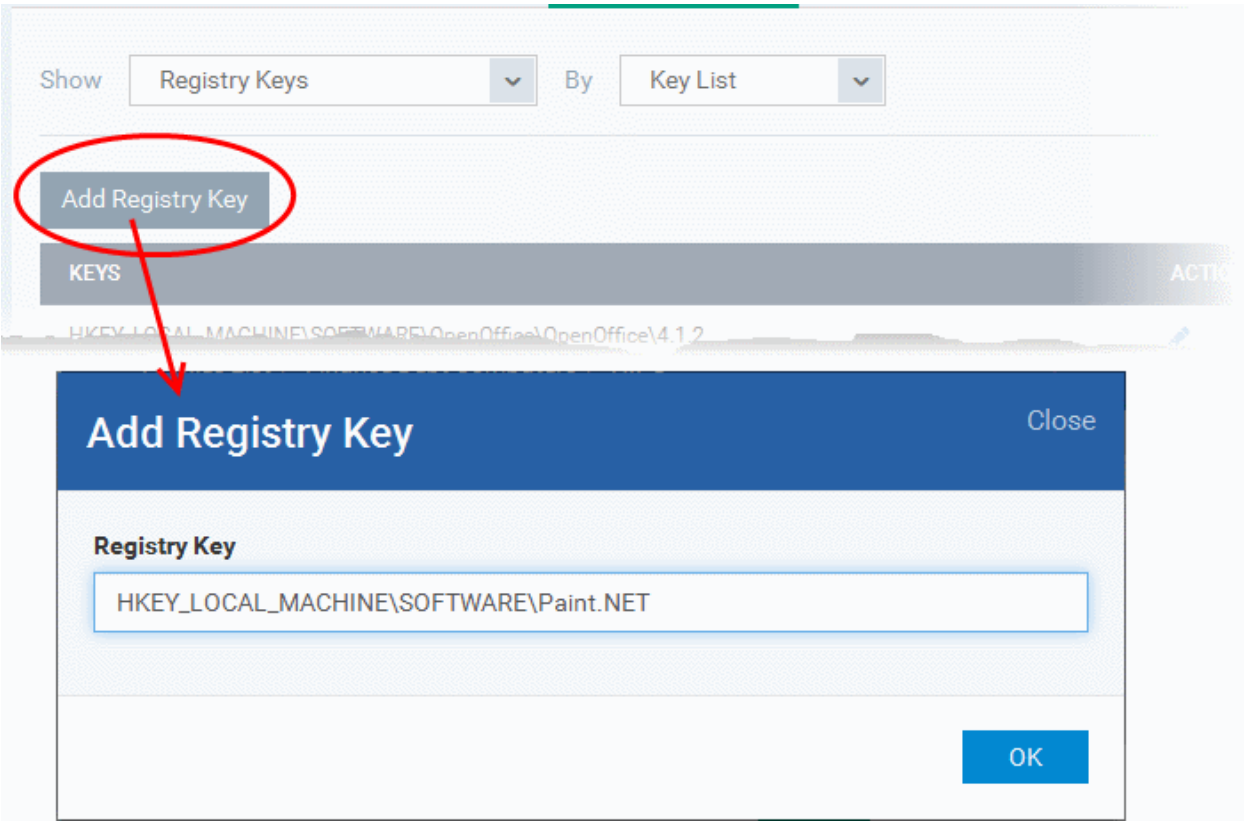


- To view the list of individual keys and values, and manage them, choose 'Key List'
- To view the Registry Groups, choose 'Group List'

You can add individual registry keys and Registry groups to Protected Registry Keys list.

To add an individual key

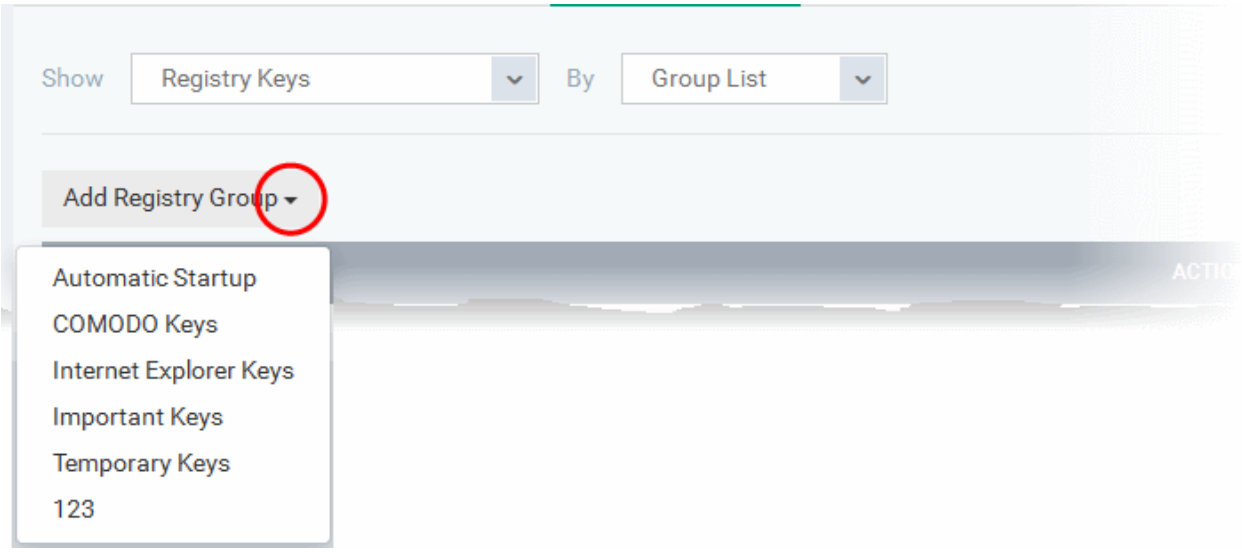
- Choose 'Key List' from the drop-down at the right and click the 'Add Registry Key' button.



- Enter the key name to be protected in the 'Add Registry Key' dialog and click 'OK'.
- Repeat the process to add more keys.
- To edit an item in the list, click the 'Edit' icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add an Registry group to the Protected Registry Keys list

- Choose 'Group List' from the drop-down at the right and click the 'Add Protected Files' button



- Choose the Registry group from the drop-down and click 'OK'.

Note: ITSM ships with a set of predefined Registry groups containing collections of registry keys under respective categories. Administrators can also create custom Registry groups with required key values. All the pre-defined and the custom Registry groups will be available in the drop-down. The custom Registry groups can be created under 'Settings' > 'System Templates' > 'Registry Variables' interface. Refer to the section **Registry Groups** for more details.

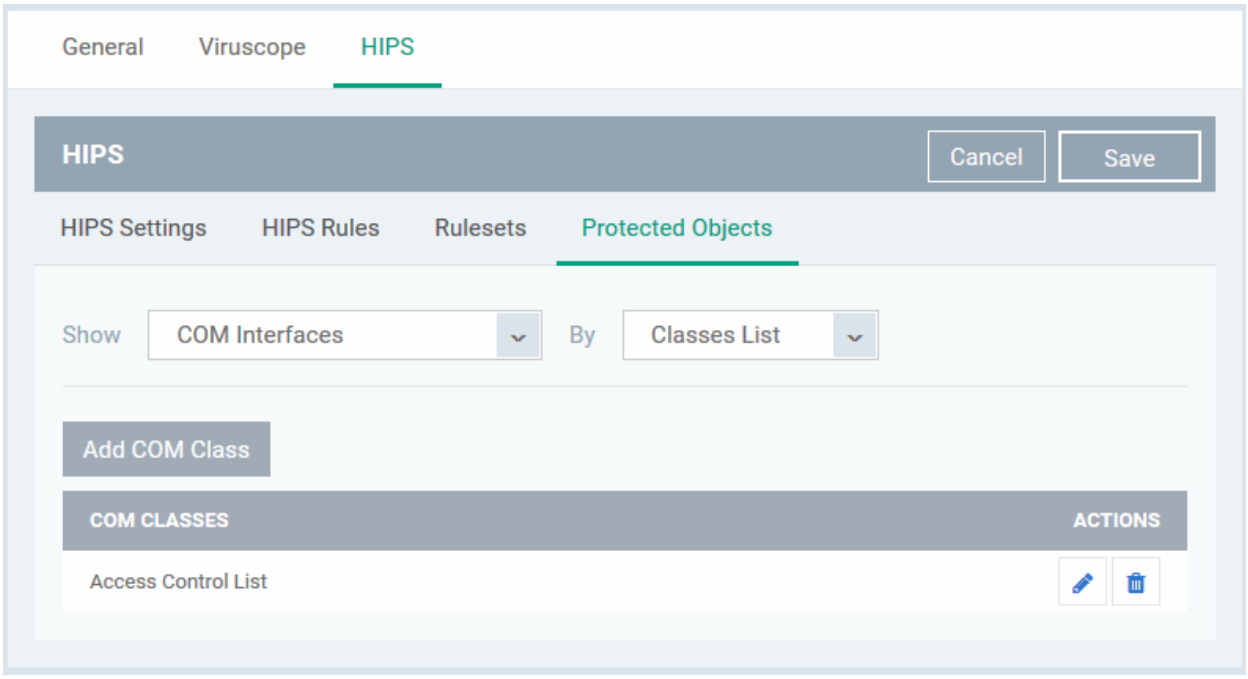
- Repeat the process to add more Registry groups.
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

COM Interfaces

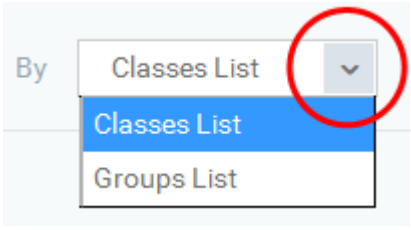
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

The 'COM Interfaces' list under 'Protected Objects' interface allows you to view and manage list of individual COM classes and COM groups that are to be protected by the Comodo Client Security at the managed computer against modification, corruption and manipulation by malicious processes.

- To view the list of Protected COM interfaces, choose 'COM Interfaces' from the 'Show' drop-down in the 'Protected Objects' interface



The Protected COM Interfaces list is displayed under two categories, which can be selected from the drop-down at the right.

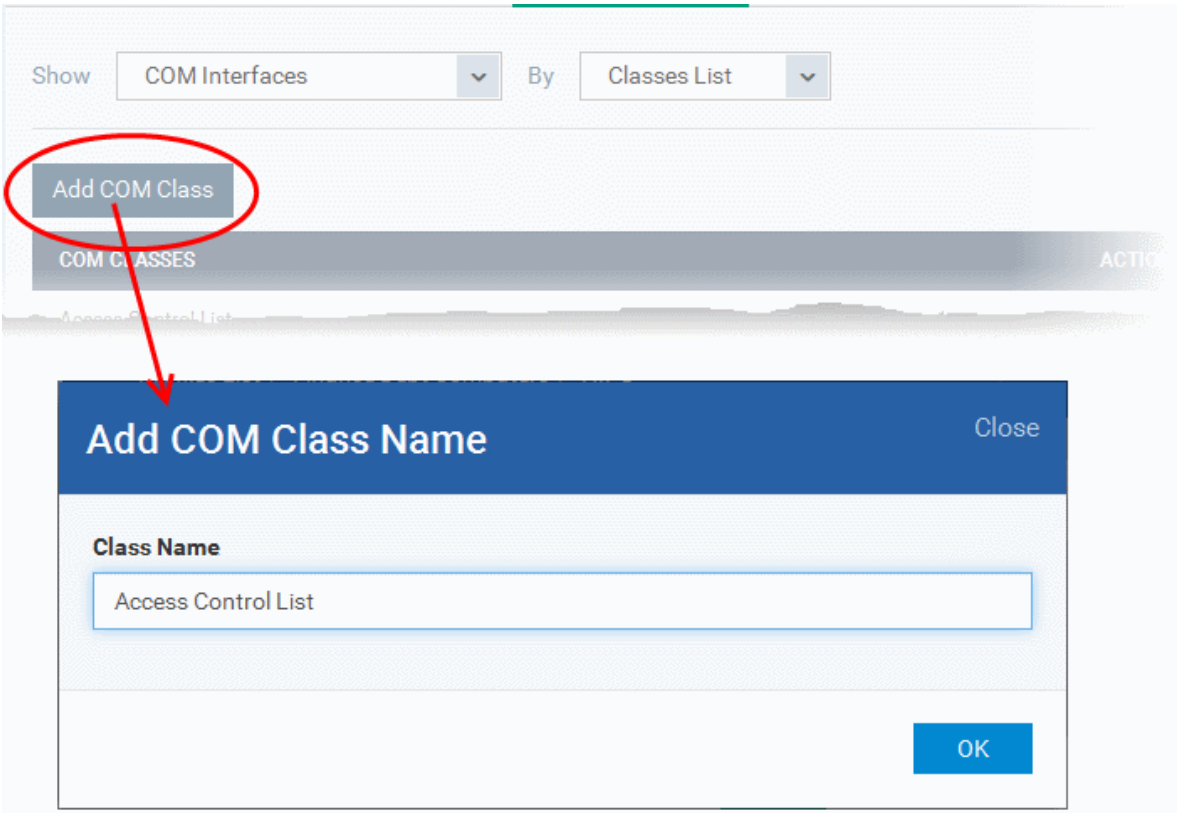


- To view the list of individual COM Interfaces/Classes and manage them, choose 'Classes List'
- To view the COM Groups and manage them, choose 'Group List'

You can add individual COM Interfaces/Classes and/or pre-defined COM groups to 'Protected COM Objects' list.

To add an individual COM object

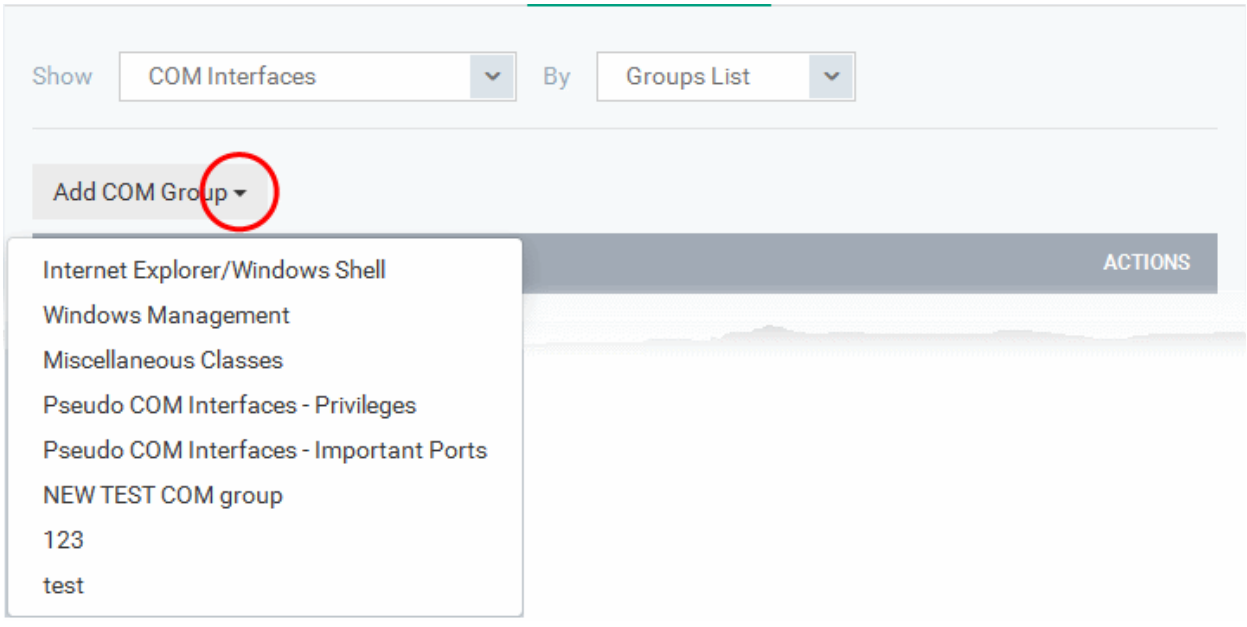
- Choose 'Classes List' from the drop-down at the right and click the 'Add COM Class' button



- Enter the name of the COM object to be protected at the managed computer, in the 'Add COM Class Name' dialog and click 'OK'.
- Repeat the process to add more COM objects.
- To edit an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add a predefined COM Group to the Protected COM objects list

- Choose 'Group List' from the drop-down at the right and click the 'Add COM Group' button



- Choose the file group from the drop-down and click 'OK'.

Note: ITSM ships with a set of predefined COM groups containing collections of COM interfaces under respective categories. Administrators can also create custom COM groups with required COM objects. All the pre-defined and the custom file groups will be available in the drop-down. The custom COM groups can be created under 'Settings' > 'System Templates' > 'COM Variables' interface. Refer to the section **COM Groups** for more details.

- Repeat the process to add more COM groups.
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

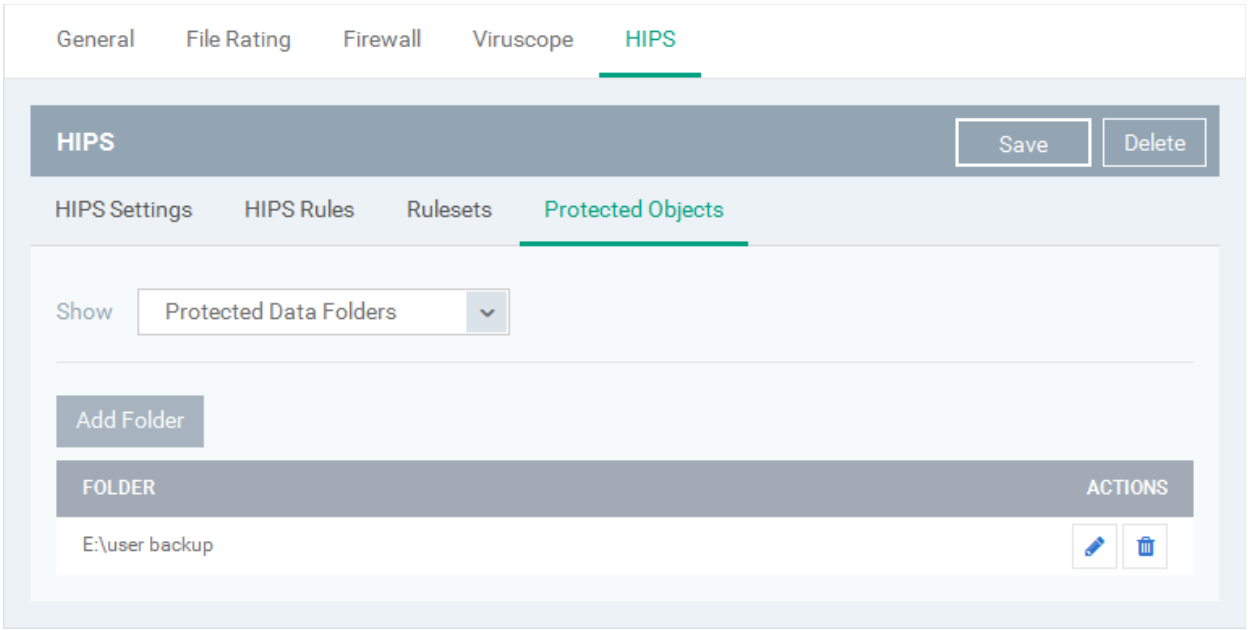
Protected Data Folders

The data files in the folders listed under the 'Protected Data Folders' area cannot be seen, accessed or modified by any known or unknown application that is running inside the container.

Tip: Files and folders that are added to '**Protected Files**' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to contained programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the contained programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

The Protected Data Folders list under Protected Objects allows you define protected data folders at the managed computers and to manage them.

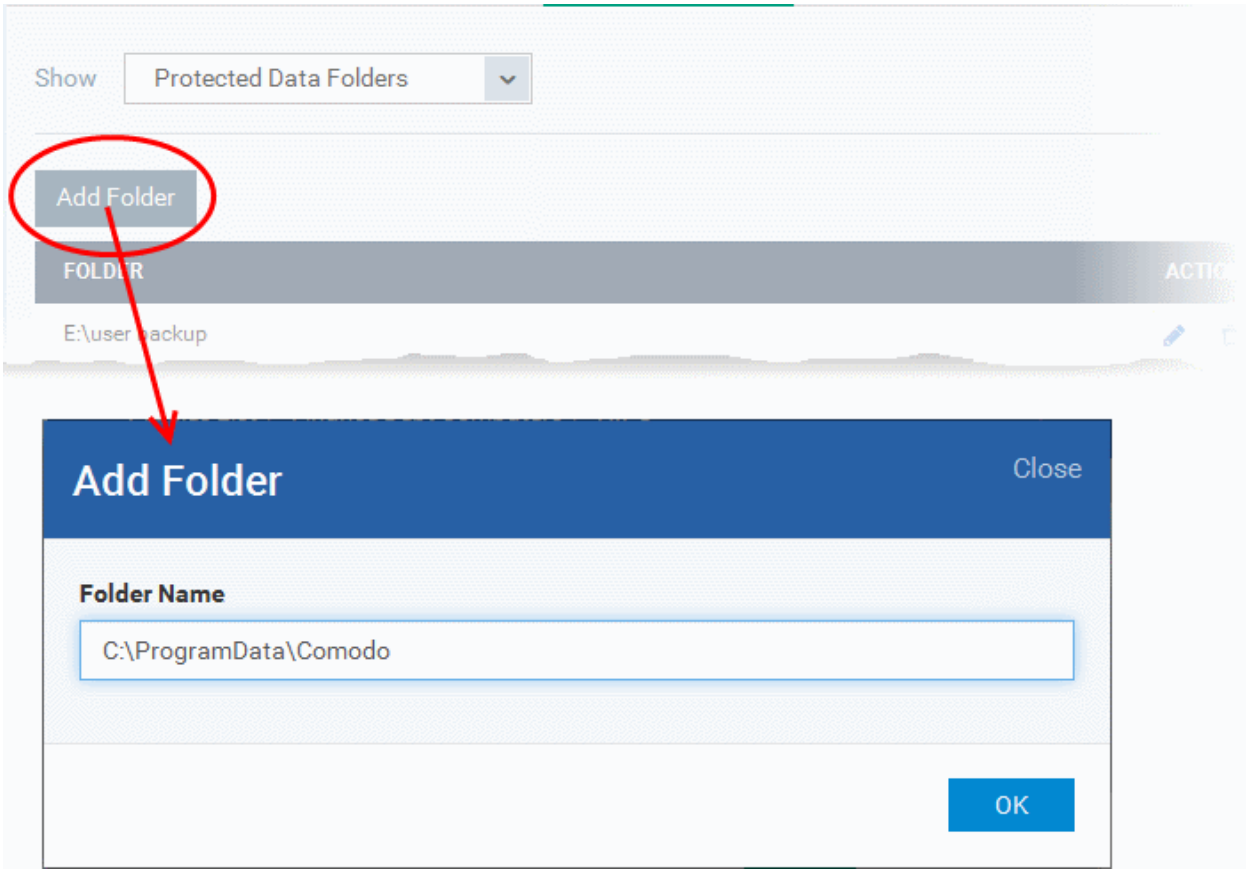
- To open the Protected Data Folders list, choose 'Protected Data Folders' from the Show drop-down in the Protected Objects interface.



You can add standard folders at the managed computers as Protected Data Folders. Data files to be protected from contained programs, can be saved inside the folders at the managed computers.

To add the path of protected data folder

- Click the 'Add Folder' button at the top of the list



- Enter the folder path in the Add Folder dialog and click 'OK'
- Repeat the process to add more folders
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

6.1.3.1.6. Containment Settings

Comodo Client Security (CCS) on managed computers can be configured to automatically run all unknown files in a security hardened environment known as the 'container'. Files running in the container are isolated from the computer's operating system and all user data to prevent them causing damage.

The 'Containment' settings area allows you to configure the overall behavior of the containment component. It also allows you to manage rules which define what types of files should be contained and at what restriction level. Restriction levels include:

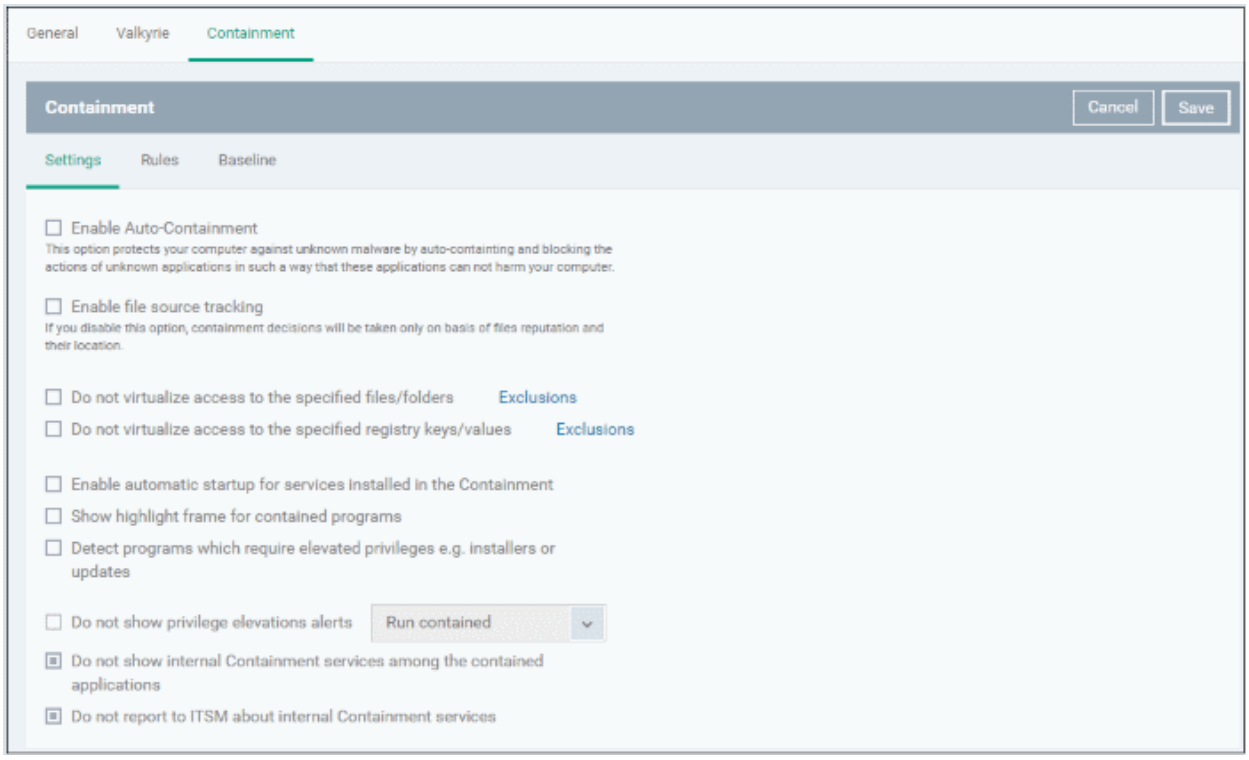
- Run completely isolated from your operating system and files on your computer
- Run with restricted access to operating system resources
- Completely block from running
- Allow to run outside the container without restriction

For more information about defining rules, refer to the section Auto-Containment Rules.

To configure Containment settings

- Choose 'Containment' from the 'Add Profile Section' drop-down

The settings screen for Containment will be displayed.

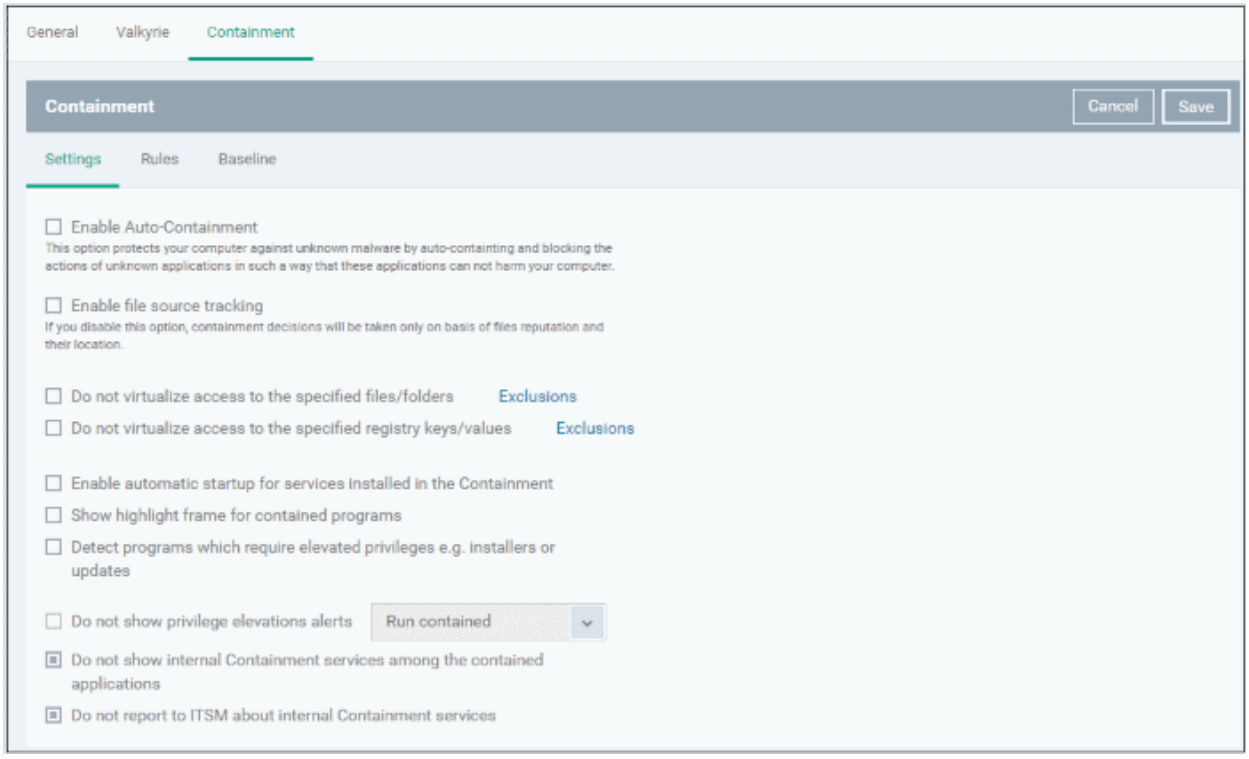


It contains three tabs.

- Containment Settings
- Auto-Containment Rules
- Baseline Settings (This tab will be available only after Vakyrie is added to the profile)

Containment Settings

The 'Settings' pane under the 'Containment' tab allows you to configure the parameters that determine how proactive the containment should be and which types of files it should check.

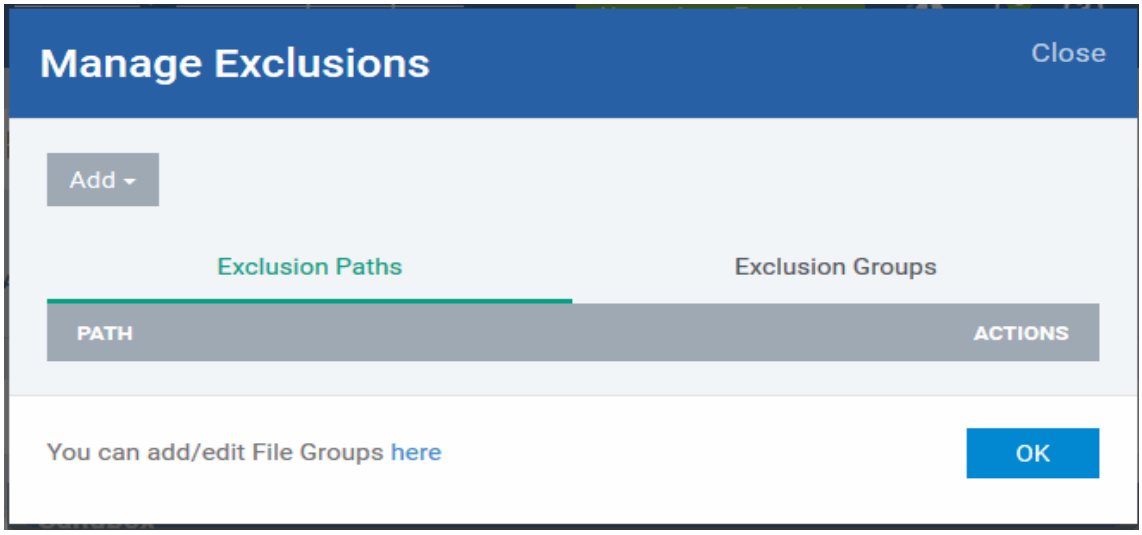


Containment Settings - Table of Parameters	
Form Element	**Description**
Enable Auto-Containment	Allows you to enable or disable Auto-Containment on the endpoint. If enabled, the CCS at the endpoint will automatically run applications inside the container as per the rules defined. For more details on creating the rules, refer to the section 'Configuring Rules for Auto-Containment'.
Enable file source tracking	If enabled, the source parameter of a containment rule will be considered. Specifying a source in a rule allows you to create granular custom rules. For example, if you wanted to only auto-contain all files downloaded from the internet, then the 'internet' is your source. If this setting is disabled then the source parameter will be disregarded and only the reputation and location parameters will be considered.
Do not virtualize access to the specified files/folders	Contained applications can access folders and files on the 'real' system but cannot save any changes to them. However, you can define exclusions to this rule. To add files and folders in which contained files can make changes, select this option and click the 'Exclusions' link. Refer to the explanation of defining exclusions for Files/Folders, below this table to find out how to add exclusions.
Do not virtualize access to the specified registry keys/values	Contained applications can access Windows Registry Keys and Values on the 'real' system but cannot save any changes to them. However, you can define exclusions to this rule. To add registry keys and values in which contained files can make changes, select this option and click the 'Exclusions' link. Refer to the explanation of defining exclusions for registry keys/values, below this table to find out how to add exclusions.
Enable automatic startup for services installed in the Containment	By default, CCS does not permit contained services to run at Windows startup. Select this check-box to allow them to do so on target endpoints.
Show highlight frame for contained programs	If enabled, CCS will display a green border around the windows of programs that are running inside the container on the endpoint.
Detect programs which require elevated privileges e.g. installers or updates	If enabled, CCS displays an alert when an installer or updater requires administrator or elevated privileges to run on an endpoint. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry.
Do not show privilege elevation alerts	If 'Detect...' (see the setting above) is enabled then privilege elevation alerts are shown to the user when a new or unrecognized program requires admin or elevated privileges to run. If you do not want these alerts to be displayed at the endpoint, select this option and choose the action to be taken for unrecognized programs: 
Do not show internal Containment services among the contained	If enabled, the processes invoked by CCC/CCS will not be displayed in the Active Process List interface of CCS on the endpoint.

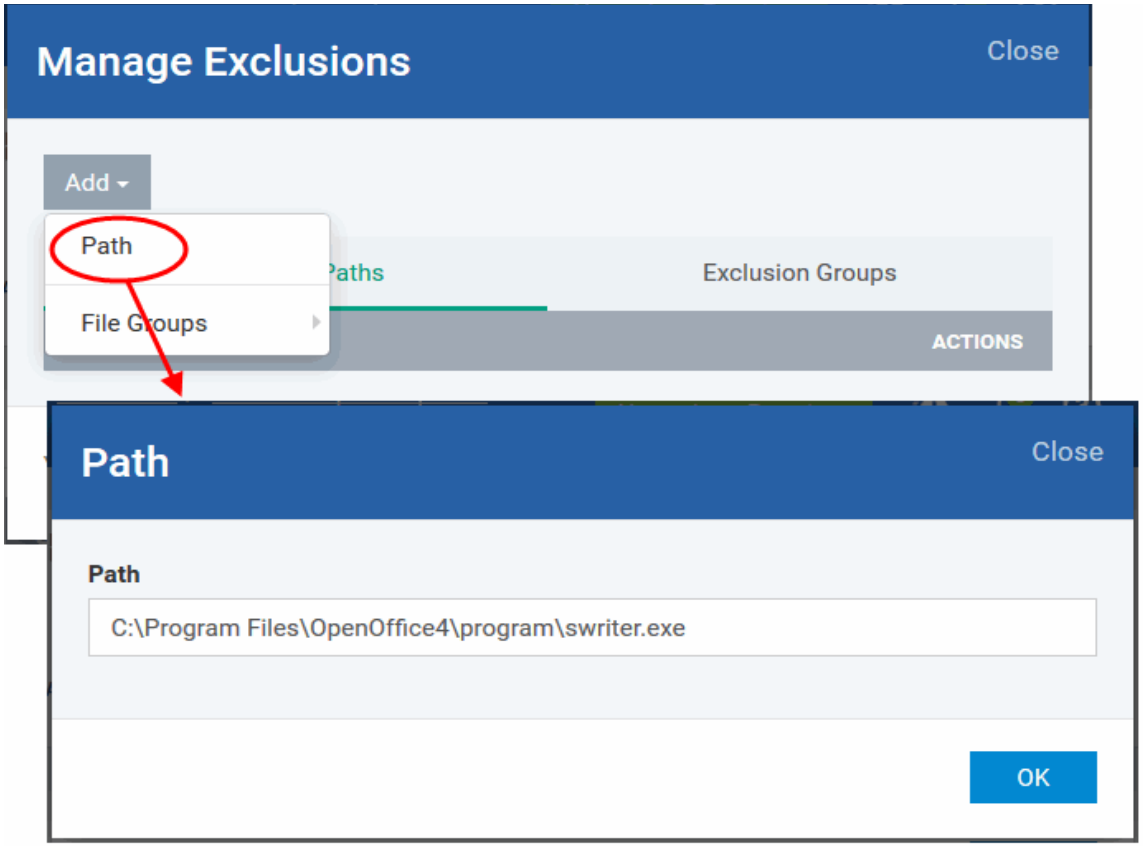
Containment Settings - Table of Parameters	
applications	You can view the list of contained process list in CCS from 'Tasks' > 'General Tasks' > 'View Active Processes' > right click and select 'Show Contained Applications only'
Do not report to ITSM about internal Containment services	If enabled, no information about contained processes invoked by CCC/CCS from the endpoints will be sent to ITSM. You can view the history of contained applications and processes in ITSM by clicking 'Security Sub-Systems' > 'Containment' on the left.

To define exclusions for files and folders

- Enable the 'Do not virtualize access to the specified files/folders' option and then click on the link 'Exclusions'.

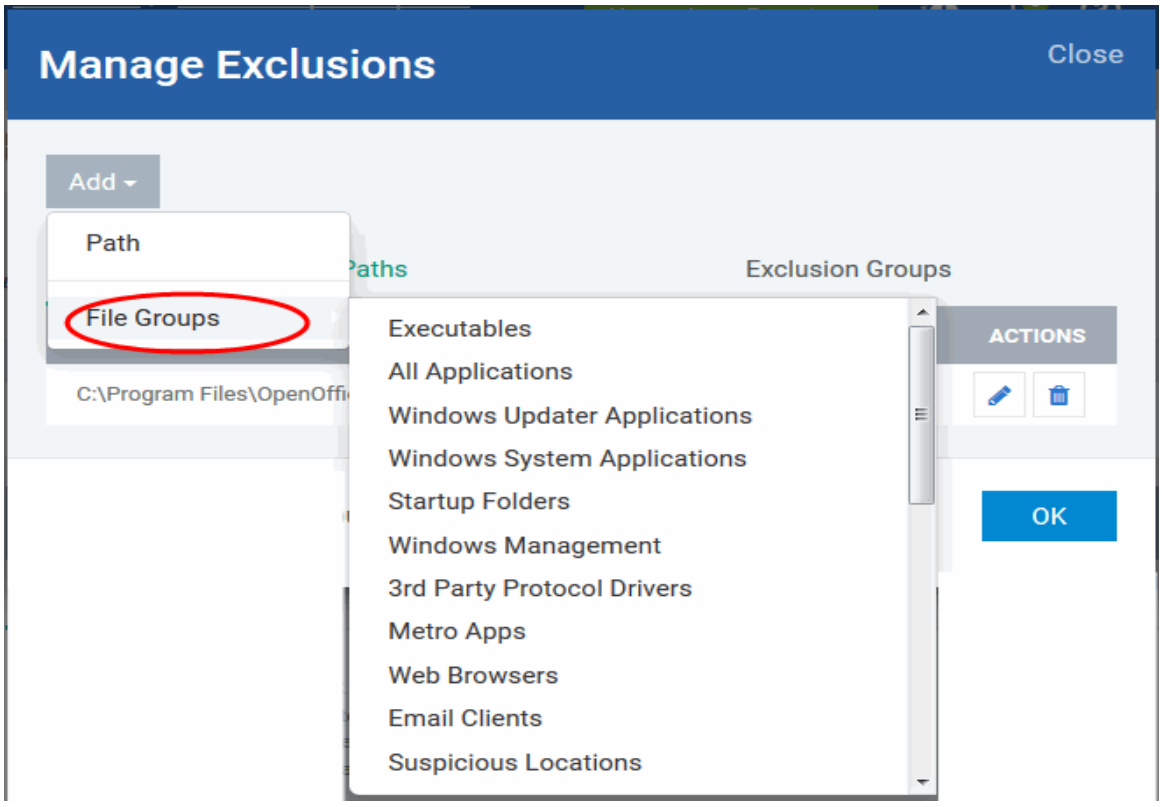


- The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:
  - **Exclusion Paths** - The individual files that are added to the list, with their installation path
  - **Exclusion Groups** - The file groups that are added to the list. A file group is a group of executable files of certain category. ITSM ships with a set of file groups. The administrator can create custom file groups from the 'Settings' > 'System Templates' > 'File Groups Variables' interface. Refer to the portion explaining '**File Groups**'.
- To add a file path, choose File Path from the 'Add' Drop-down



- Enter the storage/installation path of the file to be added to the exclusions list

- To add a File Group to exclusions, choose File Groups from the Add drop-down and choose the File Group.

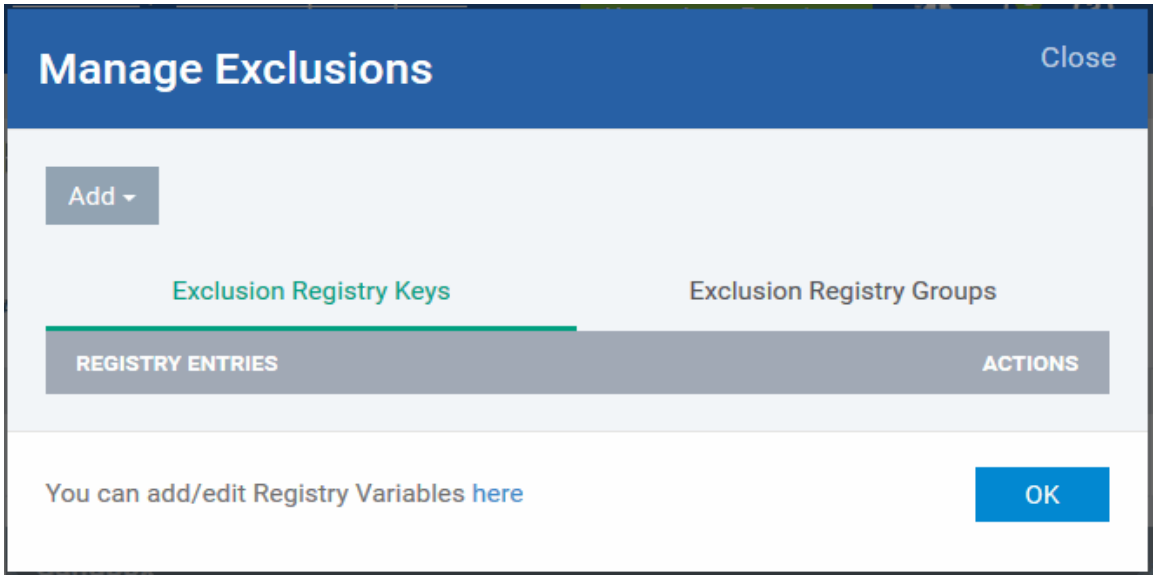


- Click 'OK' to save your settings.

- You can edit or remove the exclusions using the respective buttons in the 'Action' column in the File/Folders interface.

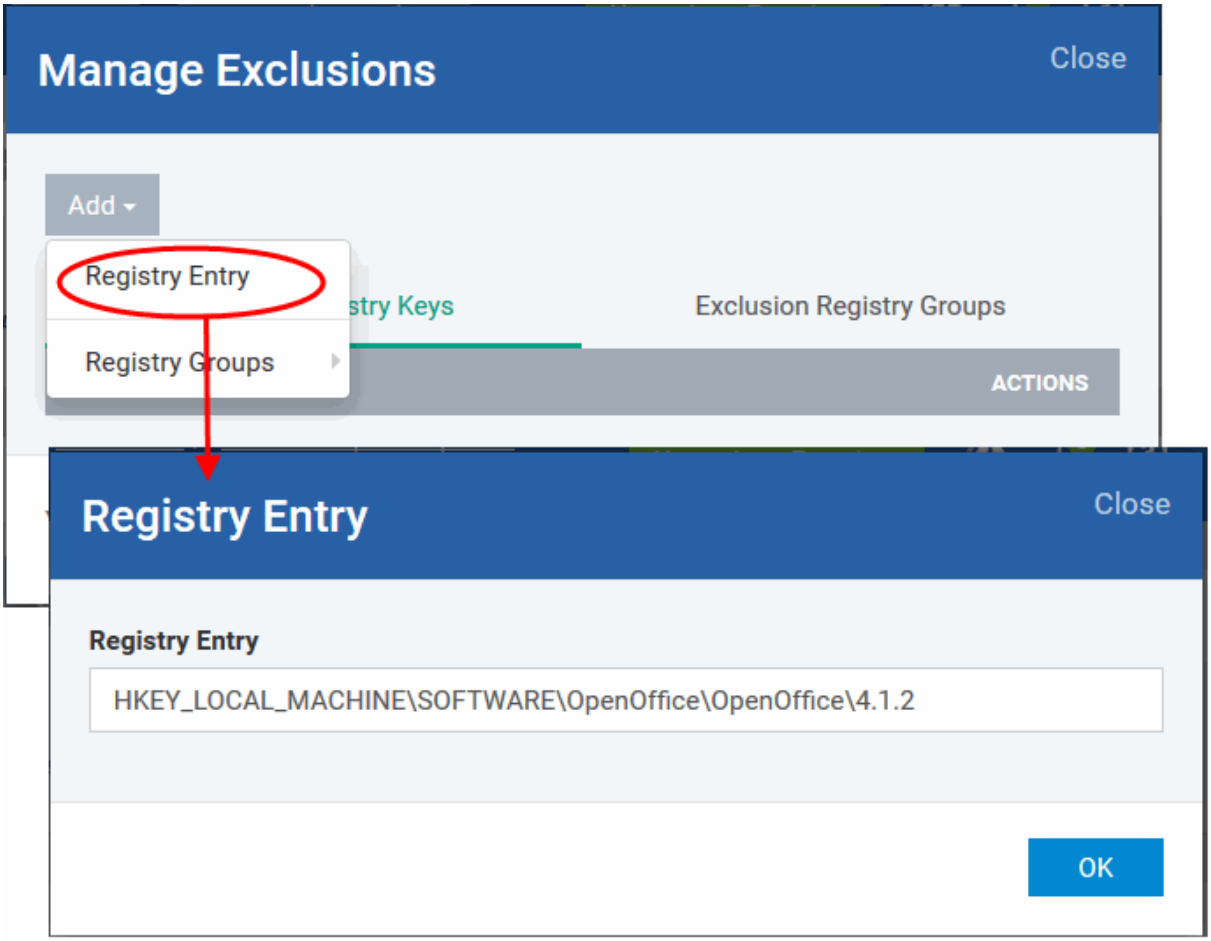
To define exclusions for specific Registry keys and values

- Click 'Exclusions' beside 'Do not virtualize access to specified registry keys/values'.



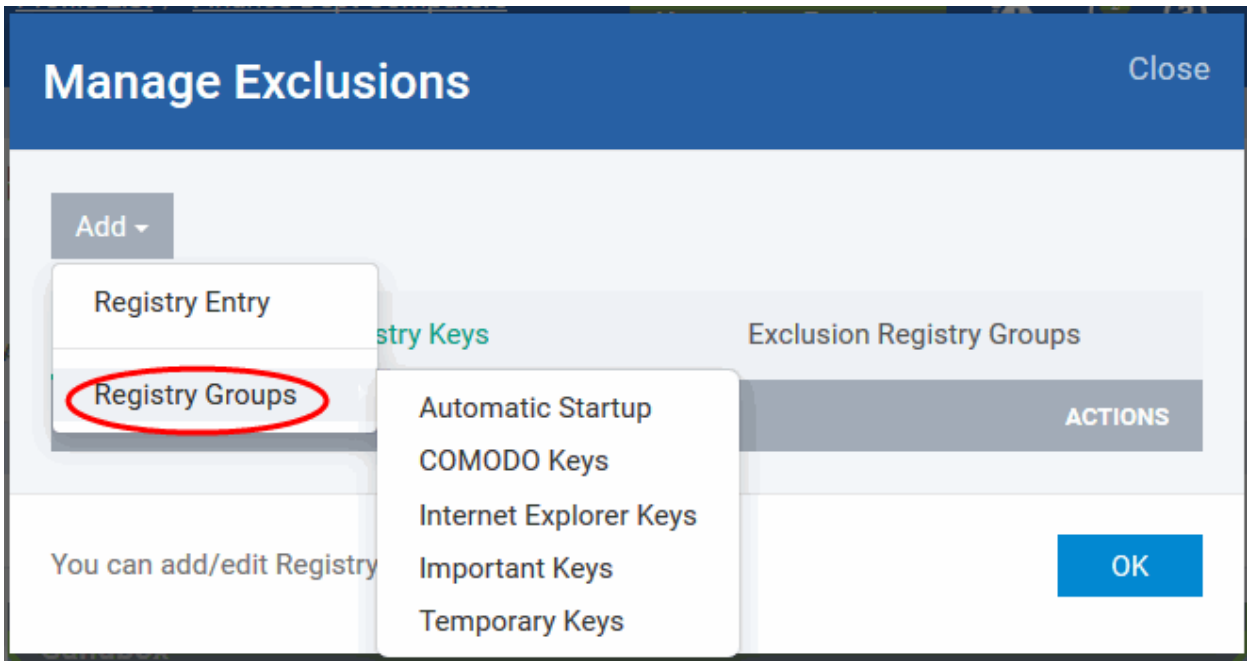
The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:

- **Exclusion Registry Keys** - The Registry Keys /Values that are added to the list
- **Exclusion Registry Groups** - The Registry Groups that are added to the list. A Registry Group is a collection of Windows registry keys and values of certain category. ITSM ships with a set of registry groups. The administrator can create custom registry groups from the 'Settings' > 'System Templates' > Registry Variables' interface. Refer to the portion explaining '**Registry Groups**'.
- To add a registry key or value, choose 'File Path' from the 'Add' drop-down.



- Enter the registry key to be added to the list in the File Path dialog an click 'OK'

- To add a pre-defined 'Registry Group' to exclusions, choose 'Registry Groups' from the 'Add' drop-down and choose the Group.



- Click 'OK' to save your settings.

You can edit or remove the exclusions using the respective buttons in the 'Action' column in the Registry Keys /

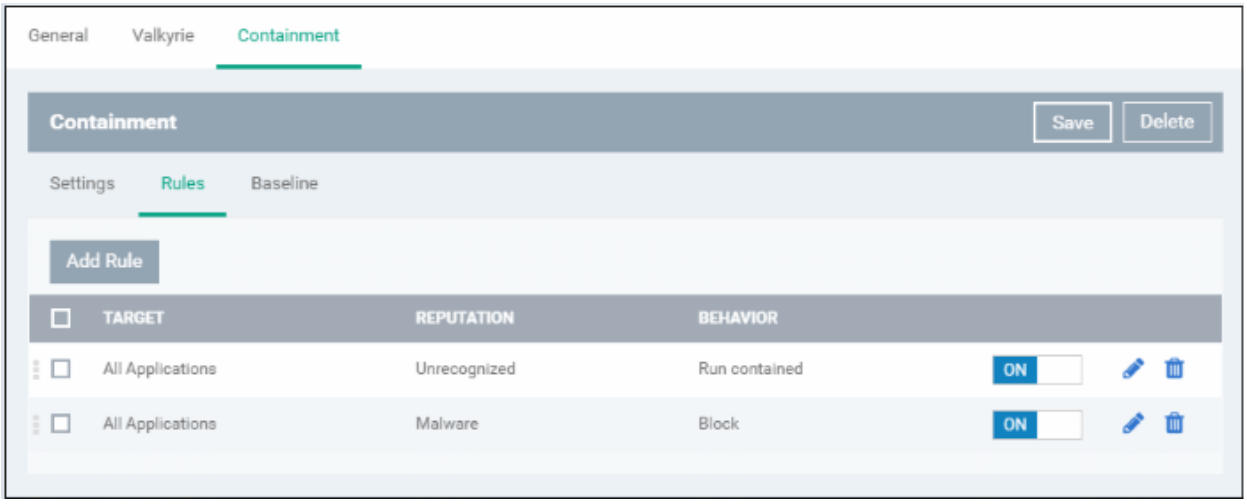
Values interface.

- Click the 'Save' button.

Configuring Rules for Auto-Containment

Containment rules determine whether a program should be allowed to run with full privileges, ignored, run restricted or run in fully contained environment. For easy identification, CCS will show a green border around programs that are running in the container on an endpoint.

The table in the rules screen displays a list of rules configured for the profile. Rules at the top of the table have a higher priority than those at the bottom. In the event of a conflict between rules, the setting in the rule nearer to the top of the table will be applied.



Containment Rules - Column Descriptions	
Column Heading	**Description**
Target	The files, file groups or specified locations on which the rule will be executed.
Reputation	The trust status of the files to which the rule should apply. The possible values are: • 'Any' • 'Malware' • 'Trusted' • 'Unrecognized'.
Behavior	Displays how the containment should act for the rule. The possible actions are: • Run contained • Run restricted • Block • Ignore

- Use the slider to enable/disable a rule
- To remove a rule, click the trash icon next to it.
- To edit a rule, click the edit icon next to it.

Sorting and filtering options

- Clicking on 'Target', 'Reputation' and 'Behavior' column headers will sort the rules in ascending/descending

order

You can add new rules for automatically running specified programs inside the container at the endpoints to which the profile is applied.

An auto-containment rule can be created for:

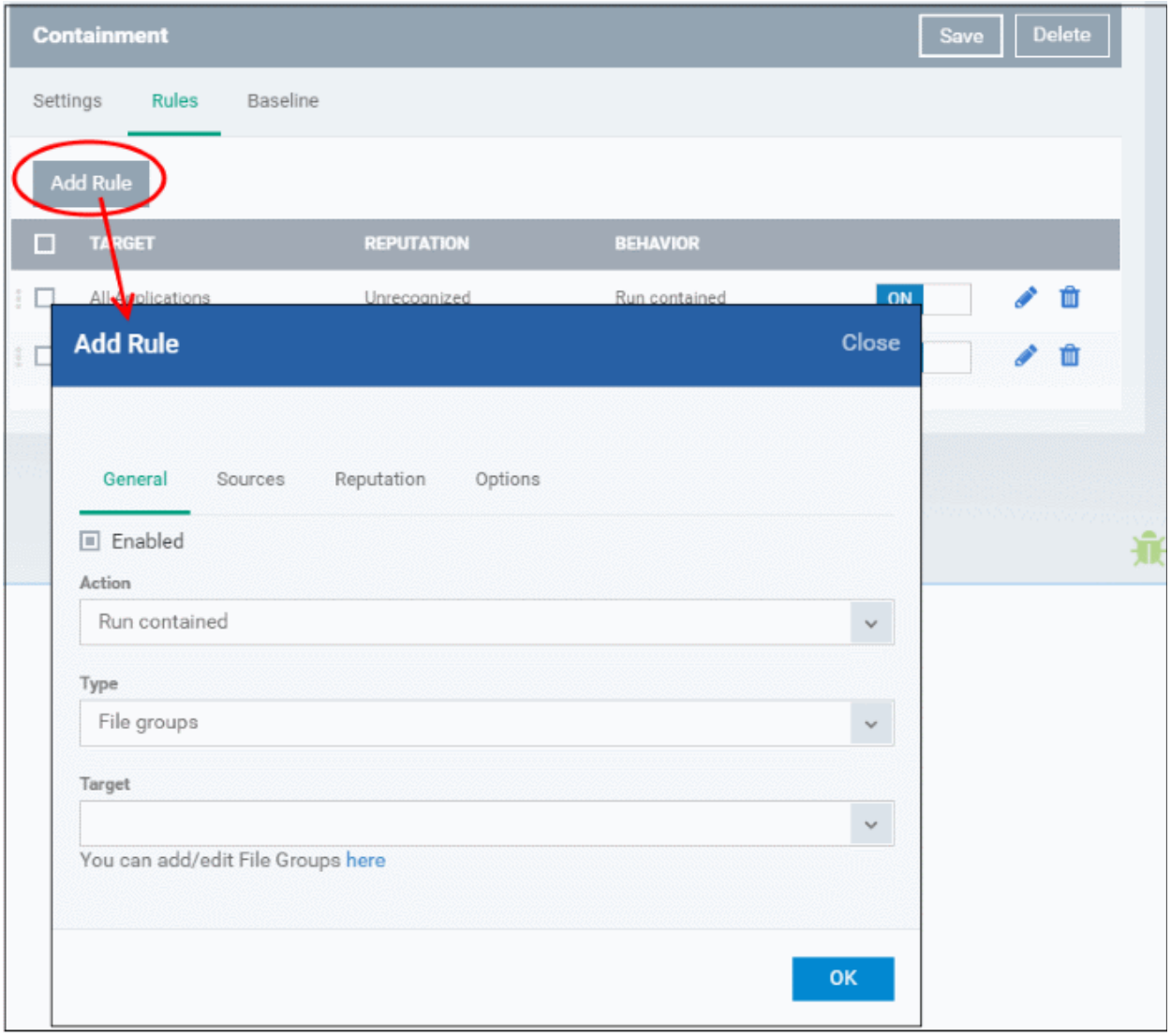
- An individual target application at a specific endpoint by specifying the file path of the executable file;
- An individual target application at several endpoints by specifying its common file path or the Hash value of the executable file;
- All applications in a File Group.

The target(s) can be filtered by specifying 'Source', 'Reputation' and 'Options'. They are, however, optional, so the administrator can create a very simple rule to run an application in the container just by specifying the action and the target application.

To add a new rule

- Click the 'Add Rule' button 

from the 'Containment > Rules' interface.



The 'Add Rule' dialog will displayed.

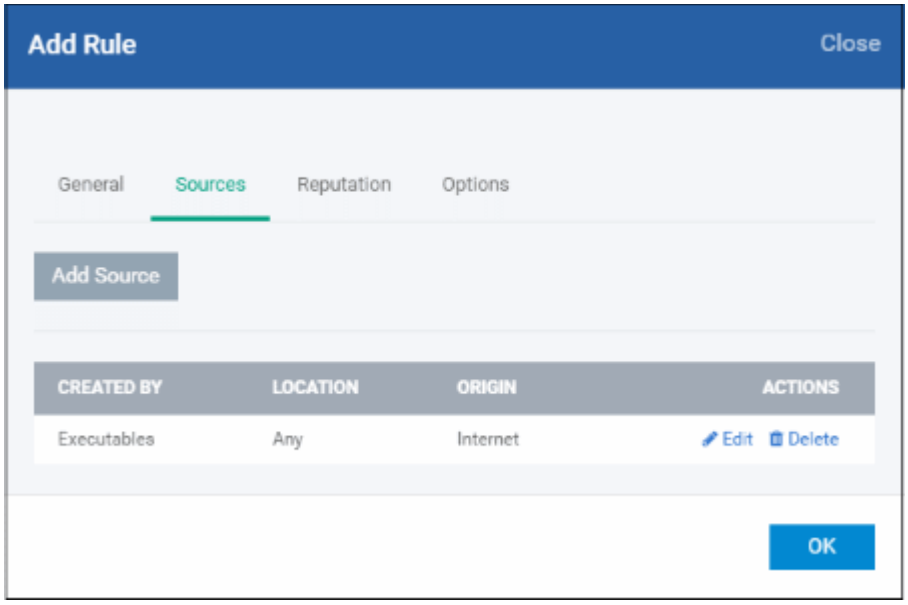
- Click the 'General' tab in the 'Add Rule' dialog

'Add Rule' dialog - General tab - Table of Parameters	
Form Element	**Description**
Enabled	Allows you to enable or disable the rule.
Action	Allows you to choose whether or not the target applications should be contained and the restriction level to be applied. The restriction level determines the ability of the contained application to access other software and hardware resources on the endpoint. The options available are: • **Run restricted** - The application is allowed to run and access operating system files and resources as per the restriction level set in the '**Restriction Level**' drop-down. • **Run contained** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of the endpoint. • **Block** - The application is not allowed to run at all. • **Ignore** - The application will not be contained and is allowed to run with all privileges.
Type	Allows you to select the target type from the drop-down. The options available are: • File Groups • File Path • File Hash Depending on the option selected here, the next field, '**Target**' will allow you to select/enter the target details.
Target	Select the target application to which the auto-containment rule is to be applied. • If 'File groups' is selected in '**Type**', the predefined file group will be available for selection from the 'Target' drop-down. **File Groups** - File groups are handy, predefined groupings of one or more file types. Choosing File Groups allows the administrator to add a category of pre-set files or folders. For example, selecting 'Executables' would include all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such predefined categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. ITSM ships with a set of File Groups. Administrators can also create custom file groups in 'Settings' > 'System Templates' > 'File Groups Variables'. Refer to the section '**Creating and Managing File Groups**' for more details. • If 'File path' is selected in '**Type**', enter the path of the file in the 'Target' field. **File Path** - Allows you to add executable files as the target by entering the entire common path. • If 'File hash' is selected in '**Type**', enter the SHA1 hash value of the file in the 'Target' field. **File Hash** - Allows you to add a program as a target by specifying the SHA1 Hash value of the executable file. CCS monitors the files at the endpoint applied with the policy and if the executable file with the same hash value attempts to execute, the rule will be triggered and the program will be auto-contained as per the rule.

The next step is to define the source for the rule.

Please note that 'Enable file source tracking' check box should be enabled in 'Settings' for the source parameter to be taken account for the rule. If this is not enabled, then this source parameter will be ignored and the rule will apply based on other parameters.

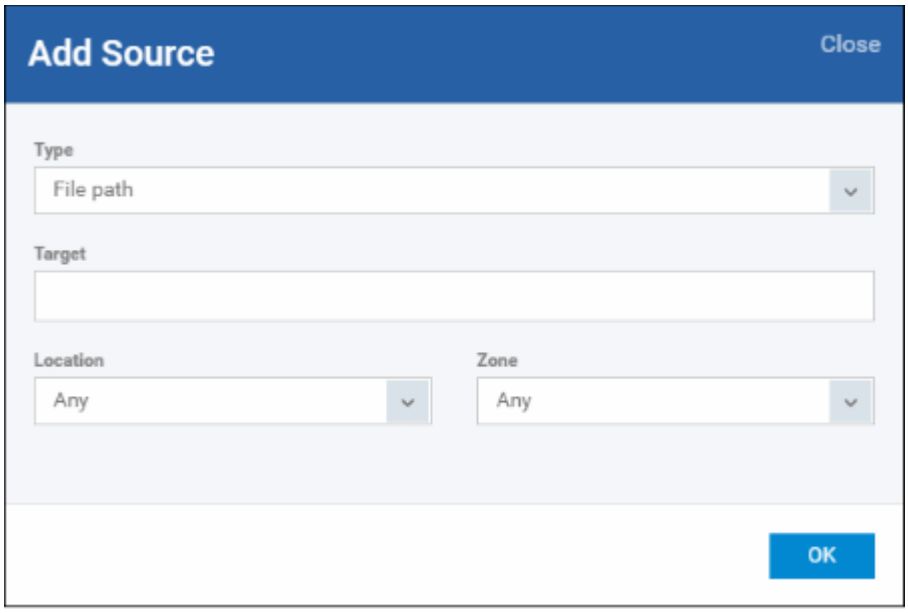
- Click the 'Sources' tab in the 'Add Rule' dialog



If you include a number of items for a rule but want the rule to be applied only for items from certain sources, you can specify the sources by clicking the 'Add Source' button.

For example, if you include all executables in the 'Target' but want the rule to be applied only to executables that were downloaded from the Internet, then the filter can be applied in the 'Sources'. Another example is if you want to run unrecognized files from a network share, you have to create an ignore rule with All Applications as target and source located on network drives.

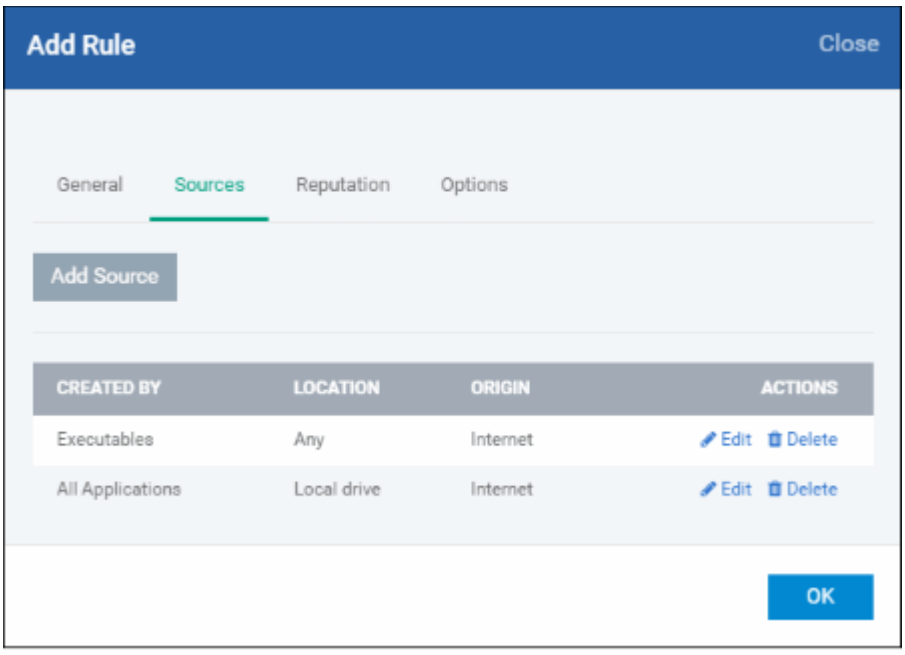
On clicking the 'Add Source' button, a new 'Add Source' dialog will be displayed.



'Add Source' dialog - Table of Parameters	
Form Element	**Description**
Type	Allows you to select the target type from the drop-down. The options available are: • File groups • File path • File hash

'Add Source' dialog - Table of Parameters	
	Depending on the option selected here, the next field, 'Target' will allow you to select/enter the target details.
Target	Choose the source file that has created the application set as target in the Target field. The process of adding the source file is similar to adding a file for target. Refer to the description above for more details. • For example, if the file was downloaded from the internet using a web browser, you can choose the file group 'Web Browsers'. • If you are unsure of the source, choose 'All Applications' file group.
Location	Choose the location where the application is stored from the drop-down. The options available are: • Any - The rule will apply to the target application located on the local drive or on a removable drive of the endpoint or on a network drive. • Local Drive - The rule will apply only to the target application located on the local drive of the endpoint. • Removable Drive - The rule will apply only to the target application located on the removable drive connected to the endpoint. • Network Drive - The rule will apply only to the target application located on a network drive but executed at the endpoint.
Zone	Choose the origin of the executable. The available options are: • Any - The rule will apply to the target application downloaded, copied or moved from anywhere. • Internet - The rule will apply only to target applications downloaded from the internet. • Intranet - The rule will apply only to target applications downloaded from the local network.

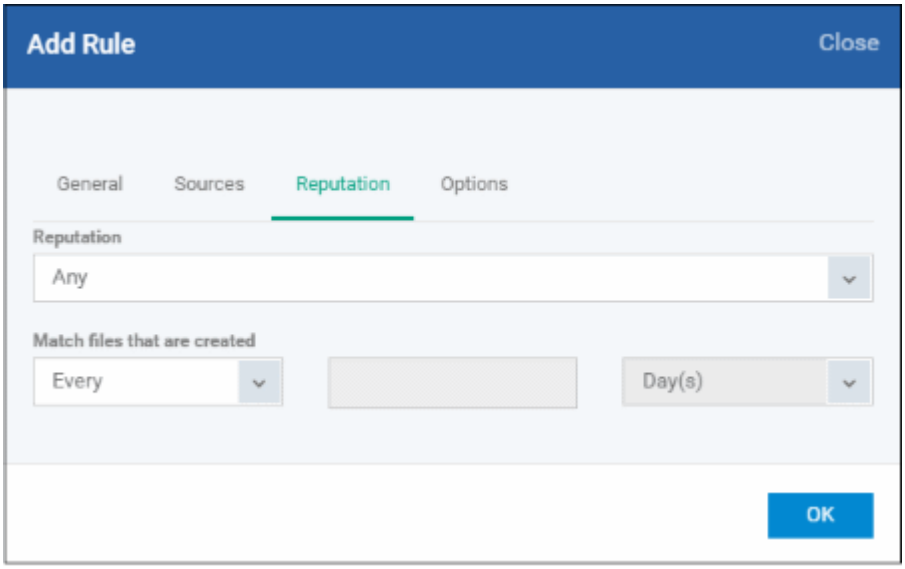
- Click 'OK'
- Repeat the process to add more sources. The source list will be displayed:



- Clicking on 'Target', 'Location' and 'Origin' column headers will sort the rules in ascending/descending order
- Click 'Edit' to change the source parameters
- Click 'Delete' to remove the source from the list

The next step is to define the reputation for the rule.

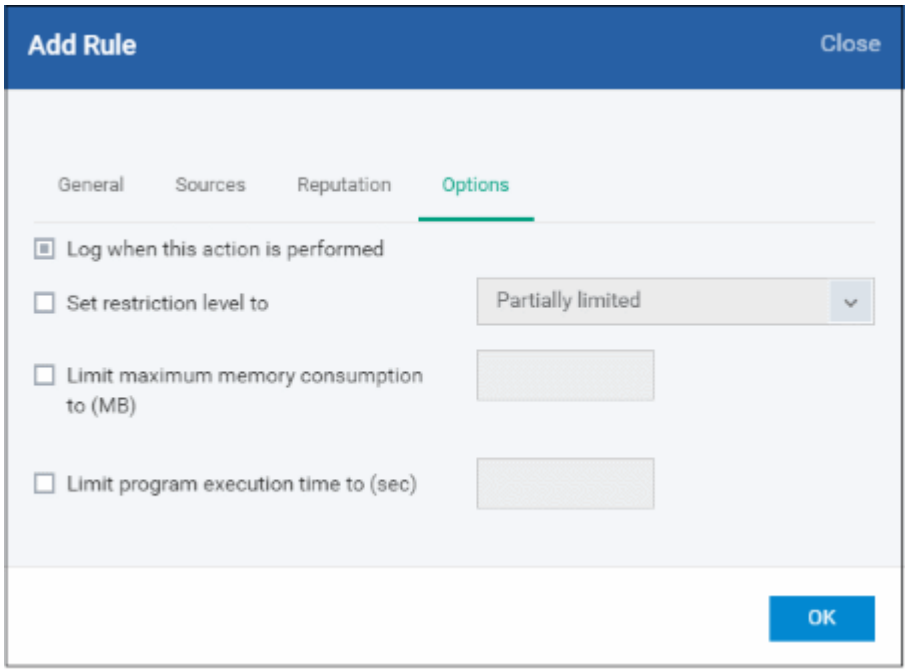
- Click the 'Reputation' tab in the 'Add Rule' dialog



'Add Rule' dialog - Reputation tab - Table of Parameters	
Form Element	**Description**
Reputation	Allows you to narrow down the scope of applications to which the rule needs to be applied by choosing the File Rating from the 'Reputation' drop-down. The available options are: • **Any -** Application of any file rating • **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files as configured under File Rating configuration of the profile. Refer to the section explaining **File Rating configuration**. • **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. • **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions.
Match files that are created	Allows you to narrow down the scope of applications to which the rule needs to be applied by specifying the age of the target files. The available options are: • **Every** - Includes all the files that match the conditions set from the Target and Reputation fields. • **More than** - Includes the files whose age is more than the specified time period. Specify the time period using the next two drop-downs. • **Less than** - Includes the files whose age is less than the specified time period. Specify the time period using the next two drop-downs

The next step is to define the options for the rule.

- Click the 'Options' tab in the 'Add Rule' dialog



'Add Rule' dialog - Options tab - Table of Parameters	
Form Element	**Description**
Log when this action is performed	Allows you choose whether or not to add the event to the CCS logs at the endpoint, whenever this rule is triggered.
Set Restriction Level to	You can choose whether or not the restriction level is to be applied to the programs run inside the container by selecting or deselecting this option. This option is available only if you have chosen 'Run restricted' or 'Run contained' as the 'Action' for the rule. For 'Run Restricted' action, the option is selected by default. If this option is selected, you should choose the restriction level to be applied from the drop-down. The available options are: • **Partially Limited** - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. • **Limited** - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges. • **Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting. • **Untrusted** - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
Limit maximum memory consumption to (MB)	Allows you to choose whether or not you wish to set an upper limit for the size of system memory that the processes run by the target application can use. This option is available only if you have chosen 'Run restricted' or 'Run contained' as the 'Action' for the rule.

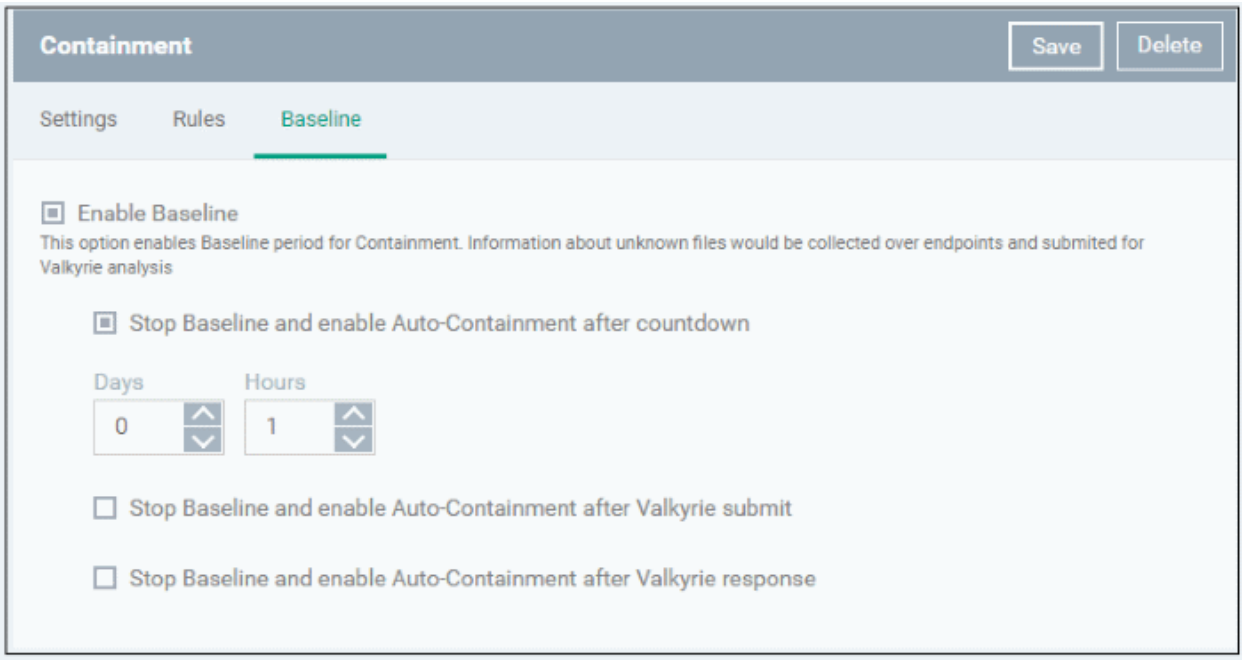
'Add Rule' dialog - Options tab - Table of Parameters	
	• If selected, enter the upper limit of size of system memory (in MB) that the process(es) can use.
Limit program execution time to (secs)	Allows you to choose whether or not you wish to specify an upper limit for the time for which the target application can continuously be run. This option is available only if you have chosen 'Run restricted' or 'Run contained' as the 'Action' for the rule. • Enter the maximum time in seconds for which the program can be allowed to run. On lapse of the time, the program will be automatically terminated.

- Click 'OK' to save the rule

Baseline Settings

Note: This tab will be available only after the Valkyrie component is added to the profile.

The 'Baseline' feature allows you set a period of time during which unknown files will be submitted to Valkyrie for analysis. Unknown files will not be auto-contained for the duration of the baseline. This feature is best used during the initial setup period when, typically, many unknown files are discovered.



Baseline Settings - Table of Parameters	
Form Element	Description
Enable Baseline	Enables you to choose one of the three options underneath.
Stop Baseline and Enable Auto-Containment after countdown	Allows you to define a baseline period in days and hours. If you choose this option alone, all unknown files discovered on your network will be sent to Valkyrie but will not be contained during the time

Baseline Settings - Table of Parameters	
	period you specify. CCS will resume containment after the time-period expires. You can use this option in conjunction with the two options underneath. The timer begins after you apply the profile.
Stop Baseline and Enable Auto-Containment after Valkyrie submit	CCS will only contain an individual unknown file after the file has been submitted to Valkyrie. If you do not set a baseline period above, then this setting will always apply.
Stop Baseline and Enable Auto-Containment after Valkyrie response	CCS will only contain an individual unknown file once Valkyrie has returned a verdict on the file. If you do not set a baseline period above, then this setting will always apply.

- Click 'Save' to apply your changes.

6.1.3.1.7. VirusScope Settings

The 'VirusScope' component of CCS monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten privacy and/or security of the end-user. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the CCS by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

VirusScope alerts give the end-user, the opportunity to quarantine the process & reverse its changes or to let the process go ahead.

The VirusScope settings screen allows you to configure the behavior of VirusScope component of CCS at the endpoint computer, to which the profile is applied.

To configure VirusScope settings

- Choose 'VirusScope' from the 'Add Profile Section' drop-down

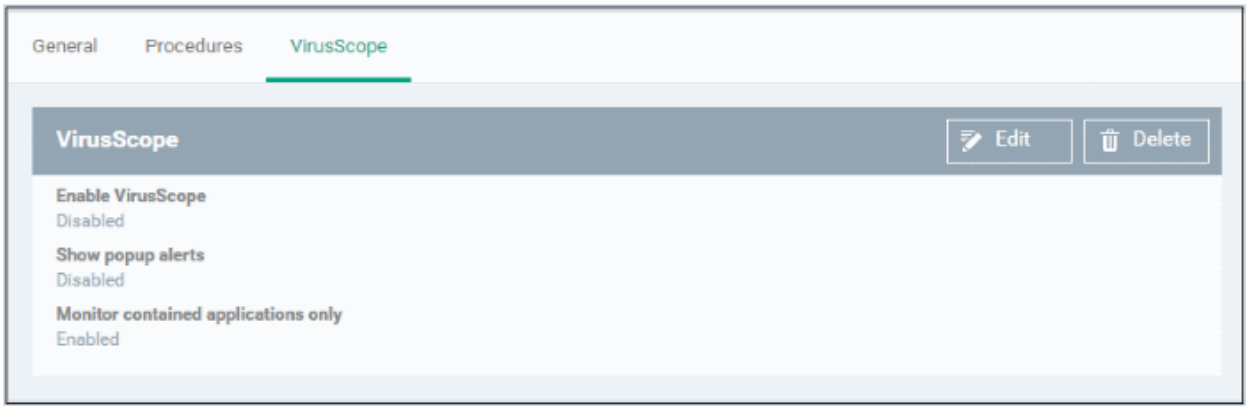
The VirusScope settings screen will be displayed.

VirusScope Configuration - Table of Parameters	
Form Element	**Description**
Enable Viruscope	Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities

VirusScope Configuration - Table of Parameters	
	of all the running processes and generates alerts on suspicious activities
Show popup alerts	Allows you to configure whether or not to show Viruscope alerts when a suspicious activity is recognized at the endpoint. Choosing to disable 'Show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.
Monitor contained applications only	VirusScope can monitor all the processes running at the endpoint. If you want it only to monitor the processes pertaining to auto-contained applications or applications manually added to run inside the sandbox, select this option.

- Click the 'Save' button.

The VirusScope component will be added to the Windows profile.



The saved 'VirusScope' settings screen will be displayed with options to edit the settings or delete the section. Refer to the section 'Editing Configuration Profiles' for more details.

6.1.3.1.8. Valkyrie Settings

Valkyrie is a cloud-based file verdicting service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Comodo Client Security on managed Windows computers can automatically submit unknown files to Valkyrie for analysis. The results of these tests produce a trust verdict on the file which can be viewed in the 'Valkyrie Processed Files' tab in the 'Windows File List' interface. See Viewing list of Valkyrie Analyzed Files for more details.

A summary of Valkyries results is all displayed in the The Dashboard.

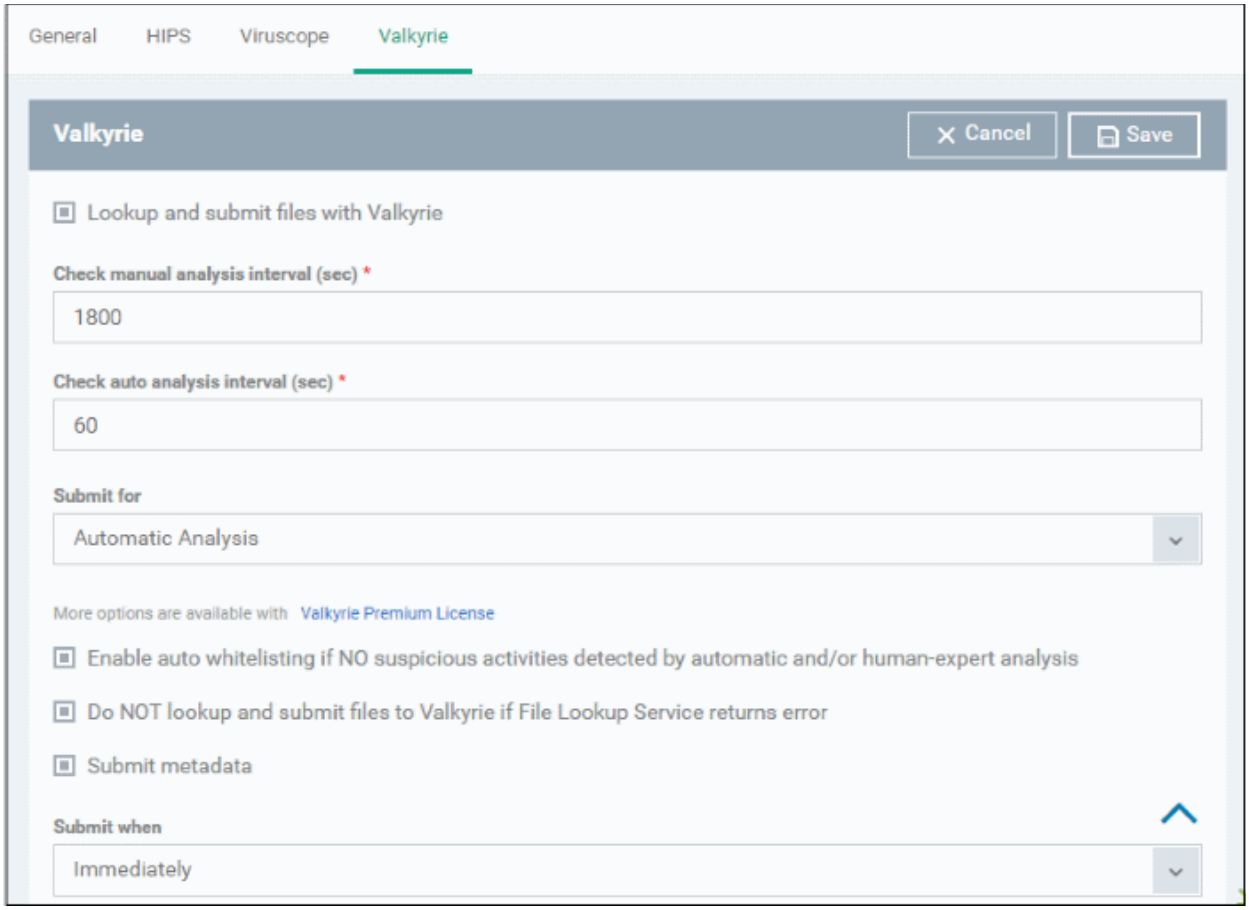
Note: The version of Valkyrie that comes with the free version of ITSM is limited to the online testing service. The Premium version of ITSM also includes manual testing of files by Comodo research labs, helping enterprises quickly create definitive whitelists of trusted files. Valkyrie is also available as a standalone service. Contact your Comodo Account manager for further details.

You can configure general Valkyrie settings and create an analysis schedule in the Valkyrie component of a Windows profile.

To configure Valkyrie Settings

- Click 'Valkyrie' from the 'Add Profile Section' drop-down in the Windows Profile interface

The 'Valkyrie' settings screen will be displayed.



Valkyrie Settings - Table of Parameters	
Form Element	**Description**
Lookup and Submit Files with Valkyrie	Choose this option if you want the files to be submitted to the cloud file lookup service
Check Manual Analysis Interval (sec)*	Set the interval for manual analysis (Default=1800)
Check Auto Analysis Interval (sec)*	Set the interval for auto analysis (Default=60)
Submit for	Choose the type of Valkyrie analysis, e.g, automatic online analysis or manual analysis. The options available depend on your type of subscription.
Enable Auto Auto-Whitelisting if NO suspicious activities detected by Automatic and/or Human-Expert analysis	Choose this option if you wish the files identified as harmless by Valkyrie to be added to your local whitelist.
Do NOT lookup and submit files to Valkyrie if File Lookup Service returns error	Choose this option,if you with files haven't been submitted to the cloud file lookup service if File Lookup Service returns error.
Submit Metadata	Choose this option if you wish the unknown file is to be submitted to Valkyrie, along with

Valkyrie Settings - Table of Parameters	
	their metadata. Metadata gives information about the file source, author, date of creation and so forth.
Submit When	Choose when the unknown files are to be submitted. The options available are: Immediately - CCS uploads the file to Valkyrie as soon as it encounters an Unknown file Schedule Analysis - CCS accumulates the unknown files and uploads them as per the set schedule. Refer to Valkyrie Analysis Schedule about how to set analysis schedule.

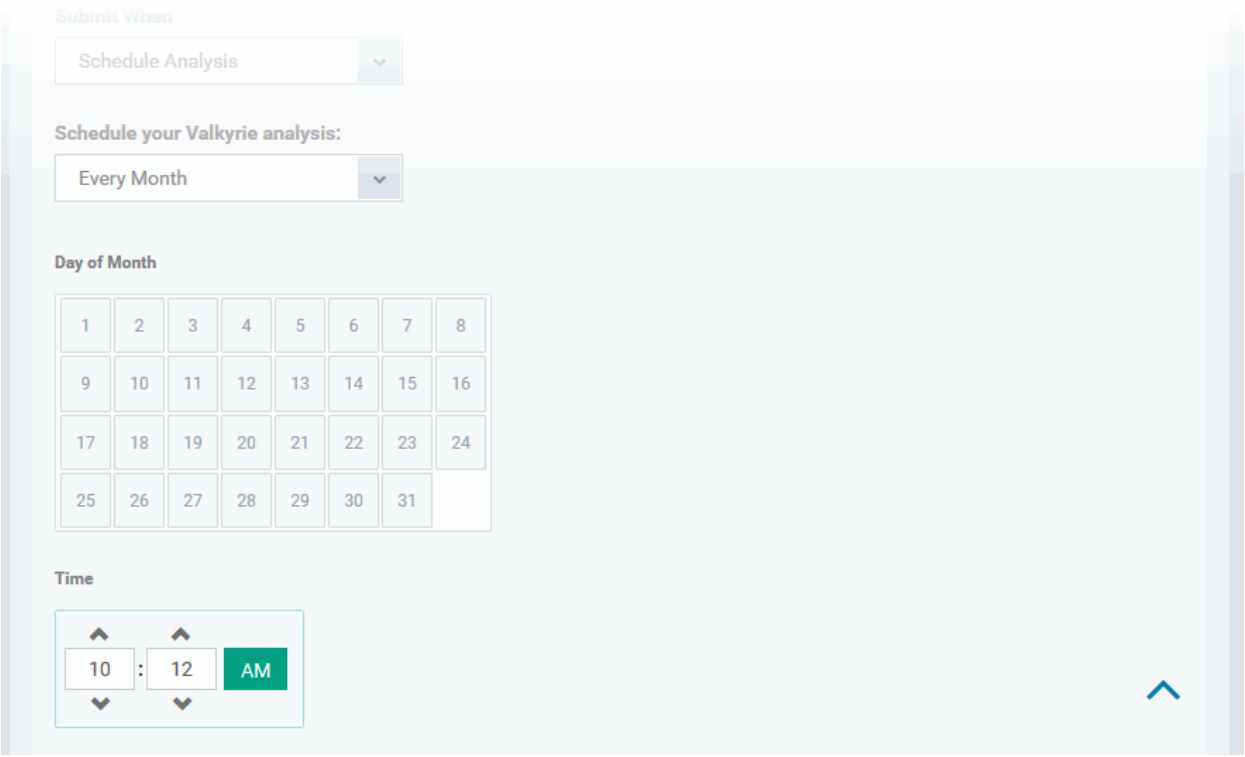
Fields marked * are mandatory.

- The 'Valkyrie Premium License' link takes to Valkyrie signup page for a full subscription.

Valkyrie Analysis Schedule

The Valkyrie allows you to create a schedule for CCS to upload unknown files.

- Select 'Schedule Analysis' from the 'Submit When' drop-down.



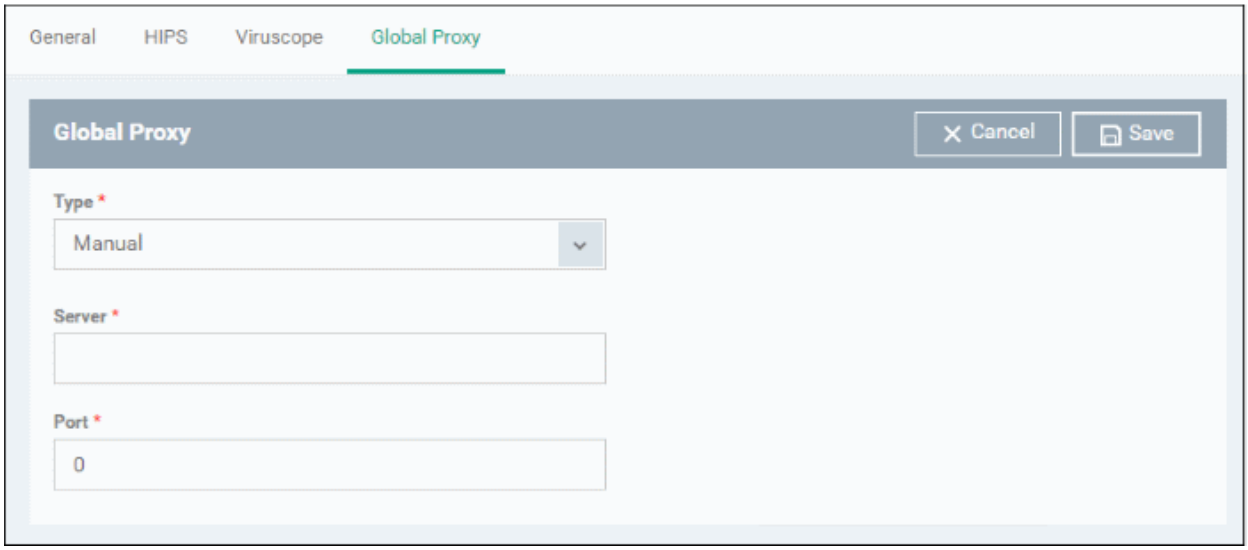
- To upload the unknown files daily choose 'Daily' from the drop-down at the top and set the time for upload in HH:MM format in the combo boxes under 'Time'.
- To upload the unknown files once per week, choose 'Every Week' from the drop-down at the top. Choose the day of the week from the 'Day of Week' options and set the time for upload in HH:MM format in the combo boxes under 'Time'.
- To upload the unknown files monthly, choose 'Every Month' from the drop-down at the top, choose the day of the month from the 'Day of month' options and set the time for upload in HH:MM format in the combo boxes under 'Time'.

6.1.3.1.9. Global Proxy Settings

The Global Proxy settings allows you to specify a proxy server through which applications in endpoints using this profile should connect to external network such as the Internet. Please note the setting done here will not affect how Comodo Client Security (CCS) and Comodo Client Communication (CCC) in the endpoints connect to ITSM and Comodo servers. The proxy setting for CCS and CCC is done in the Client Proxy section.

To configure Global Proxy Settings

- Click 'Global Proxy' from the 'Add Profile Section' drop-down in the Windows Profile interface



Global Proxy Settings - Table of Parameters	
Form Element	**Description**
Type *	Select the type of the proxy. e.g, automatic or manual.
Pac Url*	This filed will be displayed when 'Auto' is selected in the first field. Enter the URL where your proxy auto-config file is located.
Server *	This filed will be displayed when 'Manual' is selected in the first field. Enter the address or domain of your proxy server.
Port *	This filed will be displayed when 'Manual' is selected in the first field. Type the port number of the proxy. If you do not have a set port number, port 8080 will work in many cases.

* - options are mandatory.

- Click 'Save' in the title bar to save your update settings to the profile.

6.1.3.1.10. Clients Proxy Settings

The Clients Proxy settings allows you to specify a proxy server through which Comodo Client Security (CCS) and Comodo Client Communication (CCC) in the endpoints using this profile should connect to ITSM management portal and Comodo servers. If you choose not to set these, then CCS and CCC will connect directly as per the network settings.

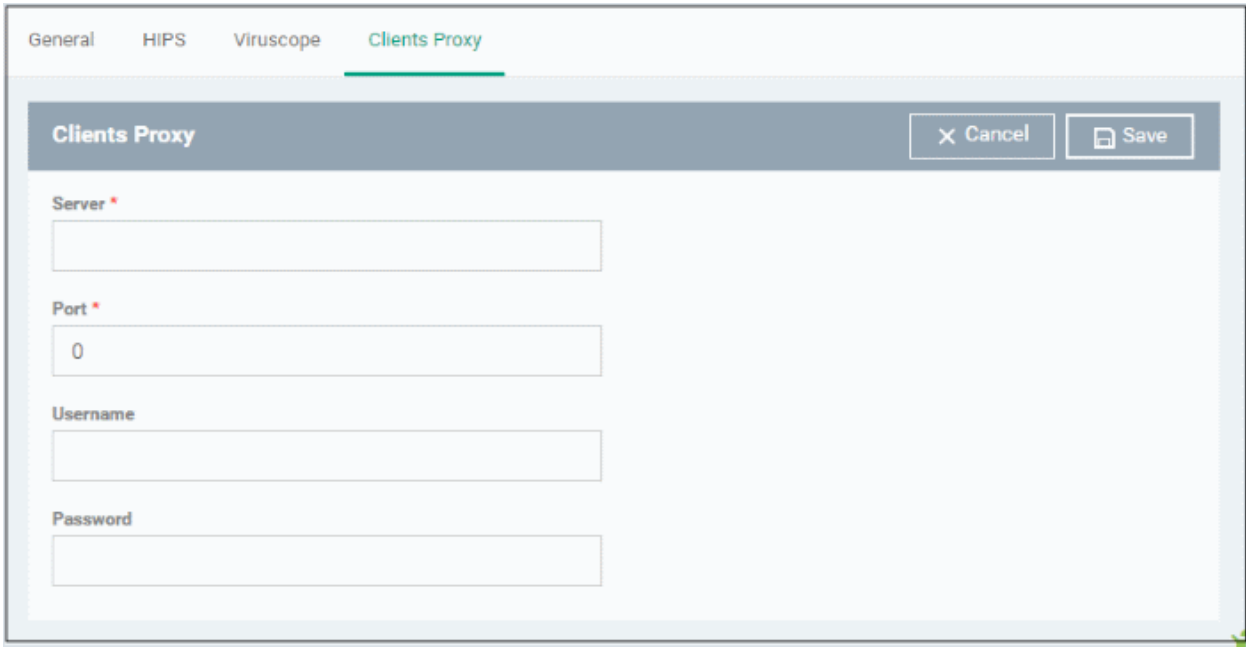
During bulk enrollment of endpoints, make sure the proxy settings in the bulk enrollment form and the client proxy settings in the device group profile that is automatically applied to enrolled endpoints are the same. If the settings vary, then the connection to ITSM will be lost after first successful connection, since the device group profile will be deployed that has different proxy settings. Also make sure the profiles that are applied to the enrolled devices later on has the same proxy settings. Please note if no proxy settings is provided in the applied profiles then the

connection to ITSM will be lost.

Please note the proxy setting done here will not affect how other applications in the endpoints connect to other networks such as the internet. The proxy setting for applications other than CCS and CCC is done in the Global Proxy section.

To configure Clients Proxy Settings

- Click 'Clients Proxy' from the 'Add Profile Section' drop-down in the Windows Profile interface

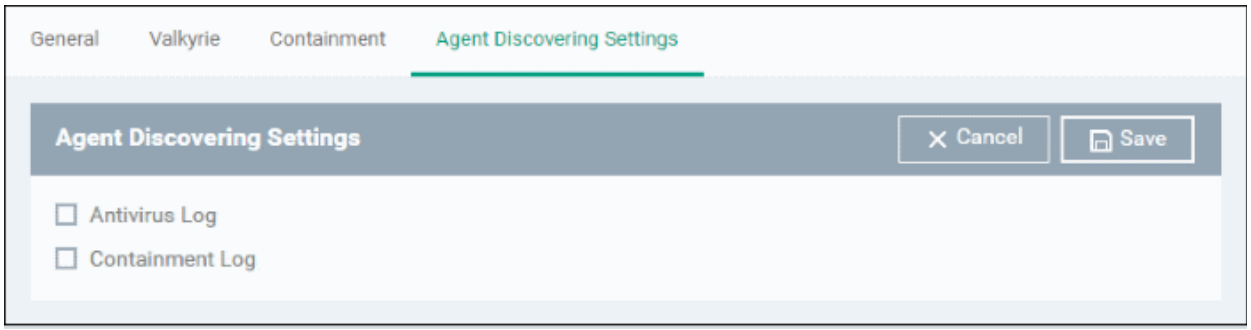


Clients Proxy Settings - Table of Parameters	
Form Element	**Description**
Server *	Enter the address or domain of your proxy server.
Port *	Type the port number of the proxy. If you do not have a set port number, port 8080 will work in many cases.
Username	If required, enter a username for the proxy.
Password	If required, enter a username for the proxy.

- Click 'Save' to apply your changes to the profile.

6.1.3.1.11. Agent Discovery Settings

The Agent Discovery Settings allows you to specify whether or not CCS should log antivirus and contained events on the endpoint.



- Antivirus Log - Select this option if antivirus log is to be enabled
- Containment Log - Select this option if containment log is to be enabled

- Click 'Save' to apply your changes.

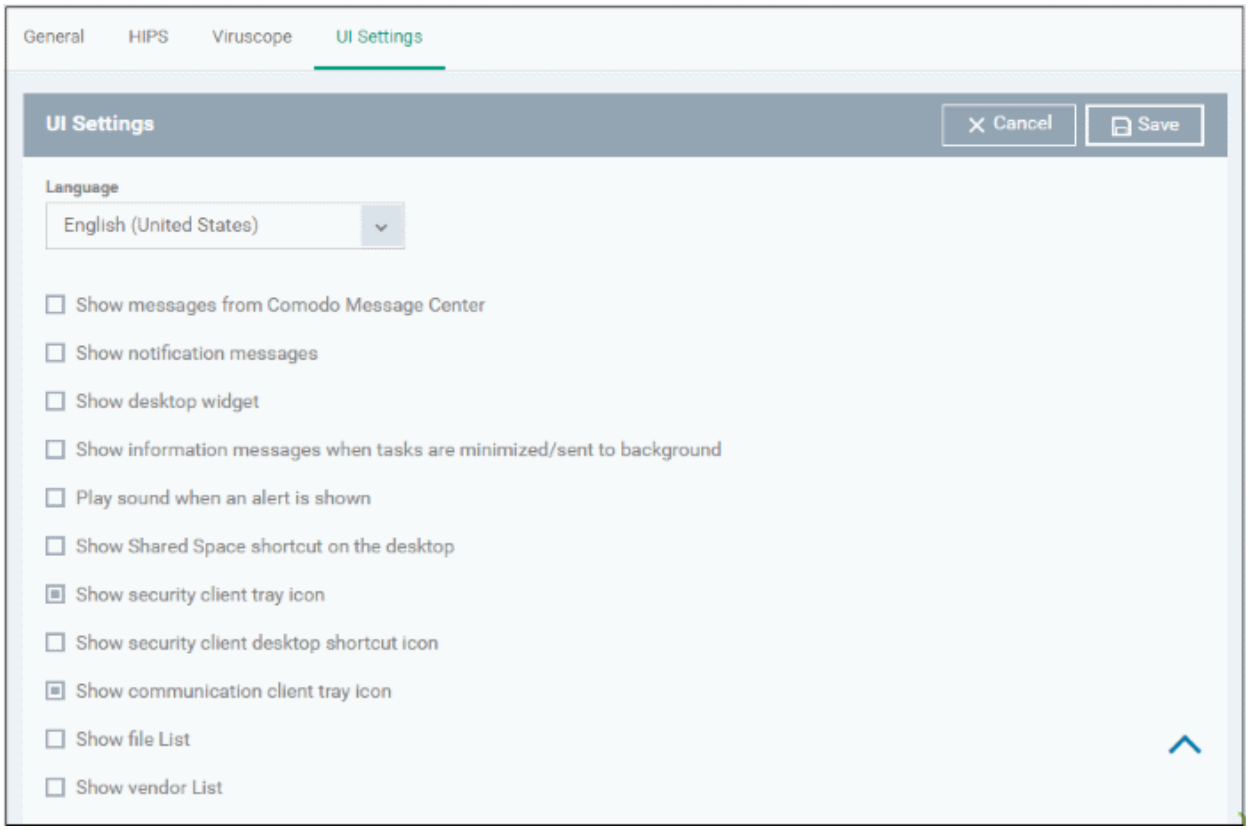
6.1.3.1.12. UI Settings

The Comodo Client - Security (CCS) UI settings screen allows you to configure how CCS should appear on endpoints to which the profile is applied.

To configure CCS UI settings

- Choose 'UI Settings' from the 'Add Profile Section' drop-down

The 'UI Settings' screen will be displayed.



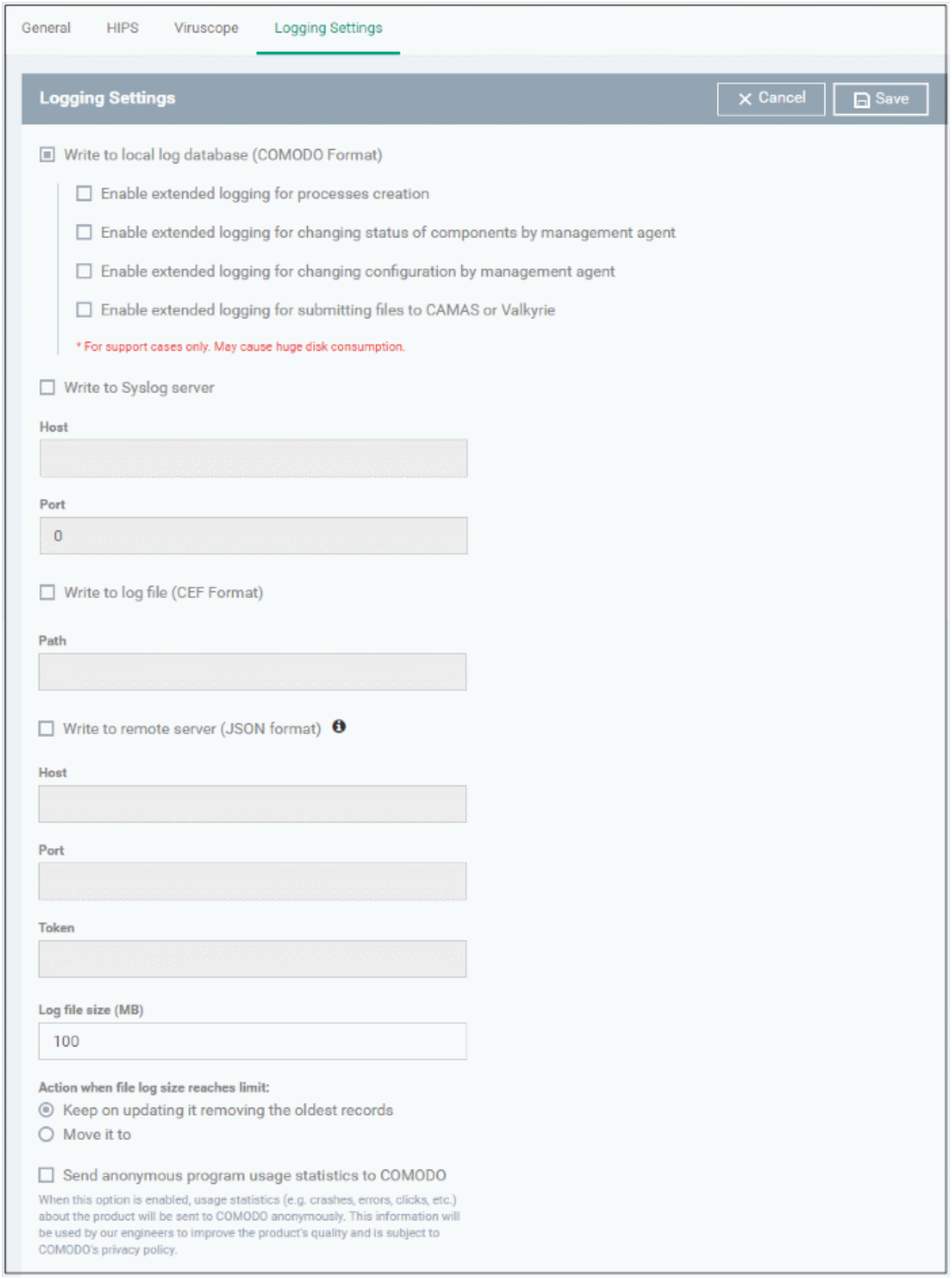
UI Settings Configuration - Table of Parameters	
Form Element	**Description**
Language	Allows you to view or modify the language used in the CCS interface.
Show messages from Comodo Message Center	If selected, Comodo Message Center messages will periodically appear to keep end-users abreast of news in the Comodo world.
Show notification messages	If selected, CCS informs end-users about its actions and status updates. CCS notices appear in the bottom right hand corner of the screen (just above the tray icons).
Show desktop widget	If enabled, the desktop widget will display at-a-glance information about security status, speed of outgoing and incoming traffic, number of background tasks and shortcuts to various areas of the CCS interface.
Show information messages when tasks are minimized/sent to background	If selected, CCS will display messages explaining the effects of minimizing or moving a running task to the background. For example, this message would be shown if a virus scan task was moved to the background.
Play sound when an alert is shown	If selected, CCS generates a chime whenever it raises a security alert.
Show Shared Space shortcut on the desktop	Provides quick access to the dedicated area for files downloaded or generated by contained applications.
Show security client tray icon	If selected, the CCS icon will be available in the system tray.
Show security client desktop shortcut icon	If selected, the CCS shortcut icon will be available on the endpoint desktop.
Show communication client tray icon	If selected, the C1 communication client icon will be available in the system tray.
Show file list	If selected, users will be able to view list of trusted, unrecognized and malicious files in the CCS interface under Advanced Settings > Security Settings > File Rating > File List. For more details click the link https://help.comodo.com/topic-399-1-790-10397-File-List.html
Show vendor list	If selected, users will be able to view list of trusted vendors in the CCS interface under Advanced Settings > Security Settings > File Rating > Trusted Vendors List. For more details click the link https://help.comodo.com/topic-399-1-790-10401-Trusted-Vendors-List.html

- Click the 'Save' button.

The UI settings will be added to the Windows profile. To edit or delete the component, click 'Edit or 'Delete' in the title bar. Refer to the section '**Editing Configuration Profiles**' for more details about editing the parameters

6.1.3.1.13. Logging Settings

The Logging Settings allows you to specify whether you want to enable logging, the maximum size of the log file and configure behavior once log file reaches the maximum file size.



Logging Settings Configuration - Table of Parameters		
Form Element	**Type**	**Description**
Write to Local Log Database (COMODO Format)	Checkbox	ITSM logs events in Comodo format and the log storage depends on settings done in Log File Management section below.

Logging Settings Configuration - Table of Parameters		
Enable extended logging for processes creation	Checkbox	Select this option to enable extended logging for processes creation
Enable extended logging for changing status of components by Management Agent	Checkbox	Select this option to enable extended logging for changing status of components by Management Agent.
Enable extended logging for changing configuration by Management Agent	Checkbox	Select this option to enable extended logging for changing configuration by Management Agent.
Enable extended logging for submitting files to CAMAS or Valkyrie	Checkbox	Select this option to enable extended logging for submitting files to CAMAS or Valkyrie.
Write to Syslog Server	Checkbox	ITSM log events are written to Syslog Event Logs.
Host *	Text box	Enter the host name or IP address of the Syslog server.
Port *	Text box	Type the port number used to connect to the Syslog server.
Write to Log File (CEF Format)	Checkbox	ITSM log events are written to Log File (CEF Format) Logs.
Path	Text box	Enter the path of the log in the field.
Write to remote server (JSON format)	Checkbox	ITSM log events are written to HTTPS in JSON format on a remote server.
Host *	Text box	Enter the host name or IP address of the remote server.
Port *	Text box	Type the port number used to connect to the remote server.
Token*	Text box	Enter the security token to access the remote server.
Log file size (MB)	Text box	Specify the maximum limit for the log file size *(Default = 100 MB).*
Action when file log size reaches limit:	Checkbox	Enables you to specify behavior when the log file reaches a certain size.
Keep on updating it removing the oldest records		Discard the log file if it reaches the maximum size . Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant
Move it to		Choose this option if you wish to move and save the log file when it reaches the maximum size.
The path to the folder for old log files *	Text box	If 'Move it to' is enabled, type a destination path for the log file.
Send anonymous program usage statistics to COMODO	Checkbox	Comodo collects the usage details from ITSM users to analyze their usage patterns for the continual enhancement of the product; collects details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best product. (Default =

Logging Settings Configuration - Table of Parameters		
		Disabled)

Fields marked * are mandatory.

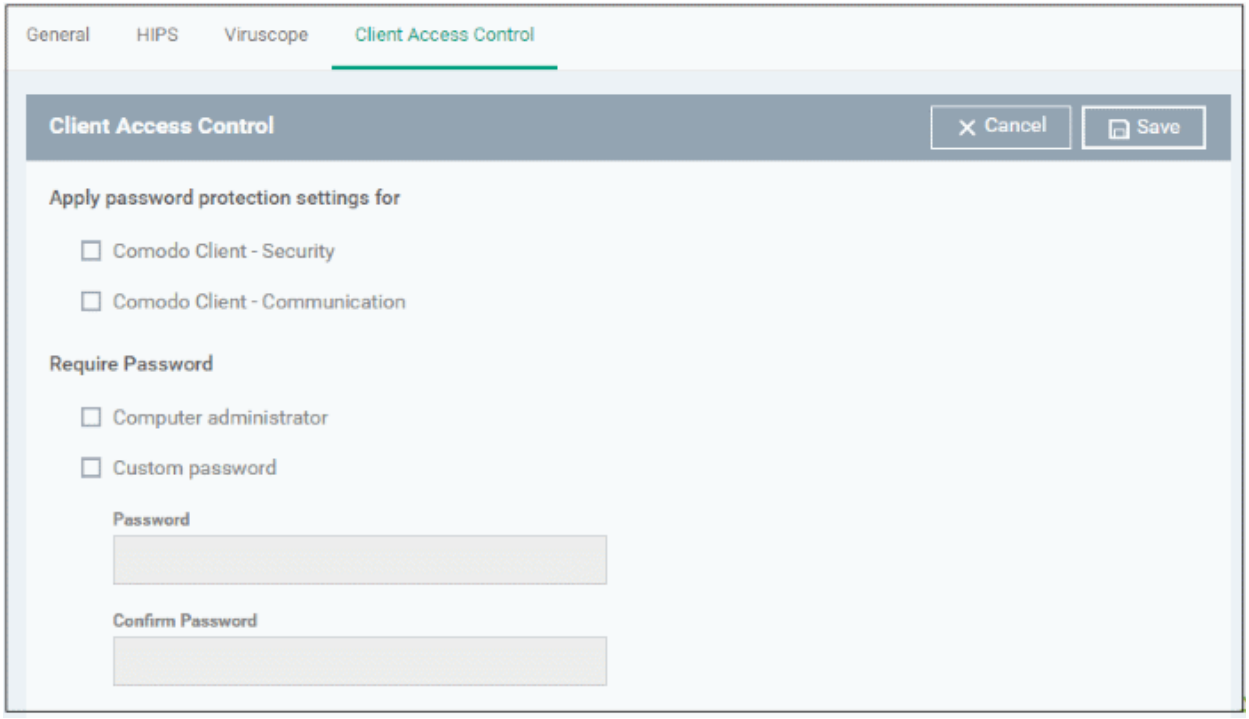
- Click the 'Save' button to apply your changes.
- Click 'Delete' or 'Edit' to remove / edit the logging settings section. Refer to the section 'Editing Configuration Profiles' for more details about editing the parameters

6.1.3.1.14. Client Access Control

ITSM admins can restrict access to Comodo Client Security (CCS) and Comodo Client Communication (CCC) on the endpoints with password protection.

To configure Client Access Control Settings

- Click 'Client Access Control' from the 'Add Profile Section' drop-down



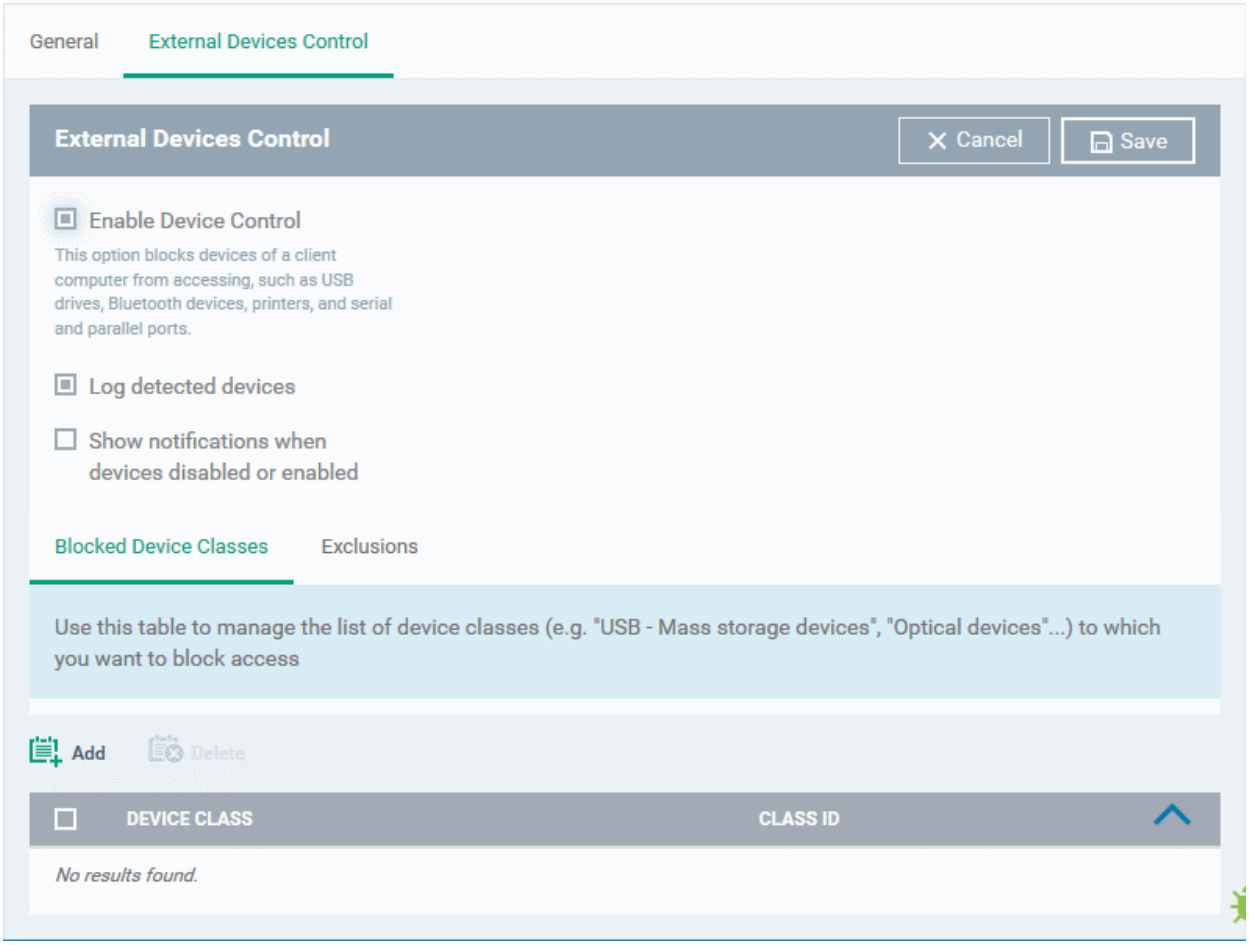
- Apply password protection settings for - Select the component(s), CCS and CCC to apply password protection.
  - Comodo Client - Security - If enabled, CCS can be accessed only after providing password.
  - Comodo Client - Communication - If enabled, CCC can be accessed only after providing password.
- Require Password - If enabled, CCS and CCC can be accessed only after entering password.
  - Computer administrator - If selected, CCS and CCC can be accessed after entering the computer administrator password.
  - Custom password - Select this to configure custom password. Enter the password and confirm it in the respective fields.
- Click Save to apply your changes to the profile.

6.1.3.1.15. External Devices Control Settings

External Device Control Settings allows administrators to define a list of devices that should be blocked on endpoints using this profile. For example, USB storage devices, human interface devices, Bluetooth devices, infrared devices, IDE ATA/ATAPI controllers and so on. ITSM blocks access to specified devices connected through both serial and parallel ports and creates a log of their connection activities. You can also define exclusions for certain devices by specifying their Device ID, so that only those devices will be allowed access.

To configure External Devices Control Settings

- Click 'External Devices Control' from the 'Add Profile Section' drop-down



The settings screen allows you to configure the general settings and to define lists of blocked device types and exclusions.

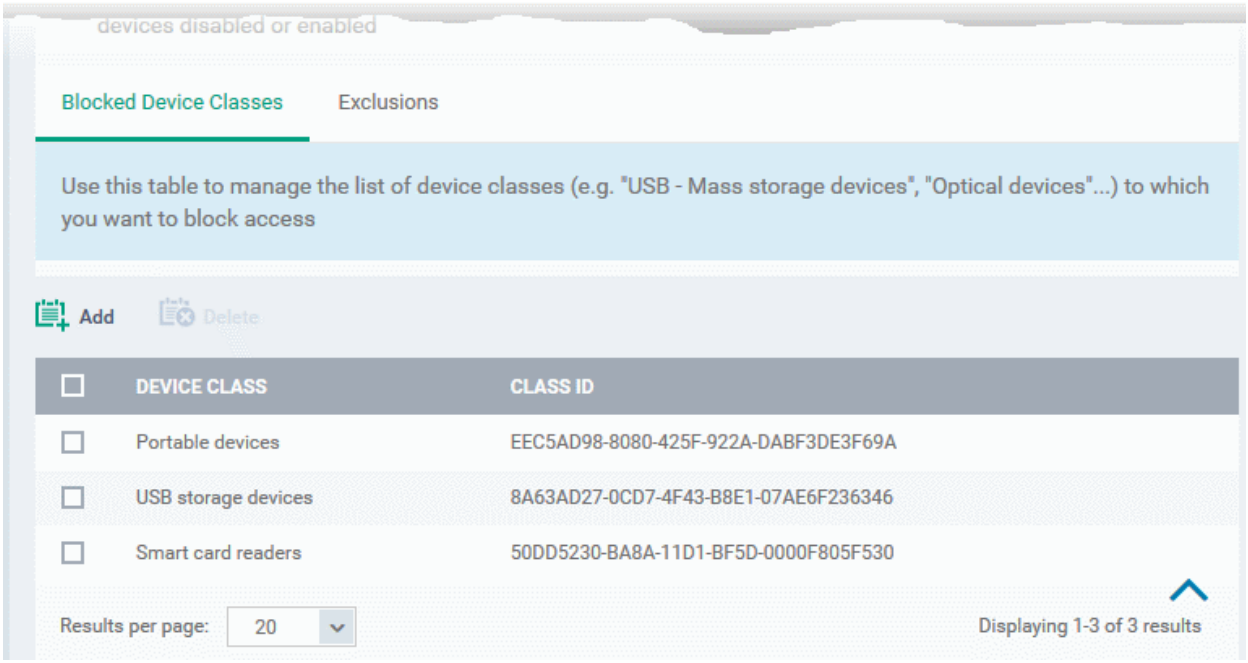
- **Enable Device Control** - Allows you to enable or disable the external device control feature. This is useful if you want to configure external device control settings for a profile during its creation and enable it at a later time
- **Log detected devices** - Allows you to enable or disable logging of external device connection attempts on endpoints that use this profile. The logs can be viewed from Security Sub Systems > Device Control interface. Refer to the section **Viewing History of External Device Connection Attempts** for more details.
- **Show notifications when devices disabled or enabled** - Allows you select whether or not a notification is to be shown to end-user when a connected device is blocked or allowed.

The 'External Devices Control' settings interface contains two tabs:

- Blocked Device Classes - Allows you to define the list of types of external devices to be blocked at the endpoints
- Exclusions - Allows you to specify the devices that should be excluded from blocking and allowed access at the endpoints

Blocked Device Classes

The 'Blocked Device Classes' tab displays a list of types of device that are blocked as per the profile and allows you to add/remove new device types.

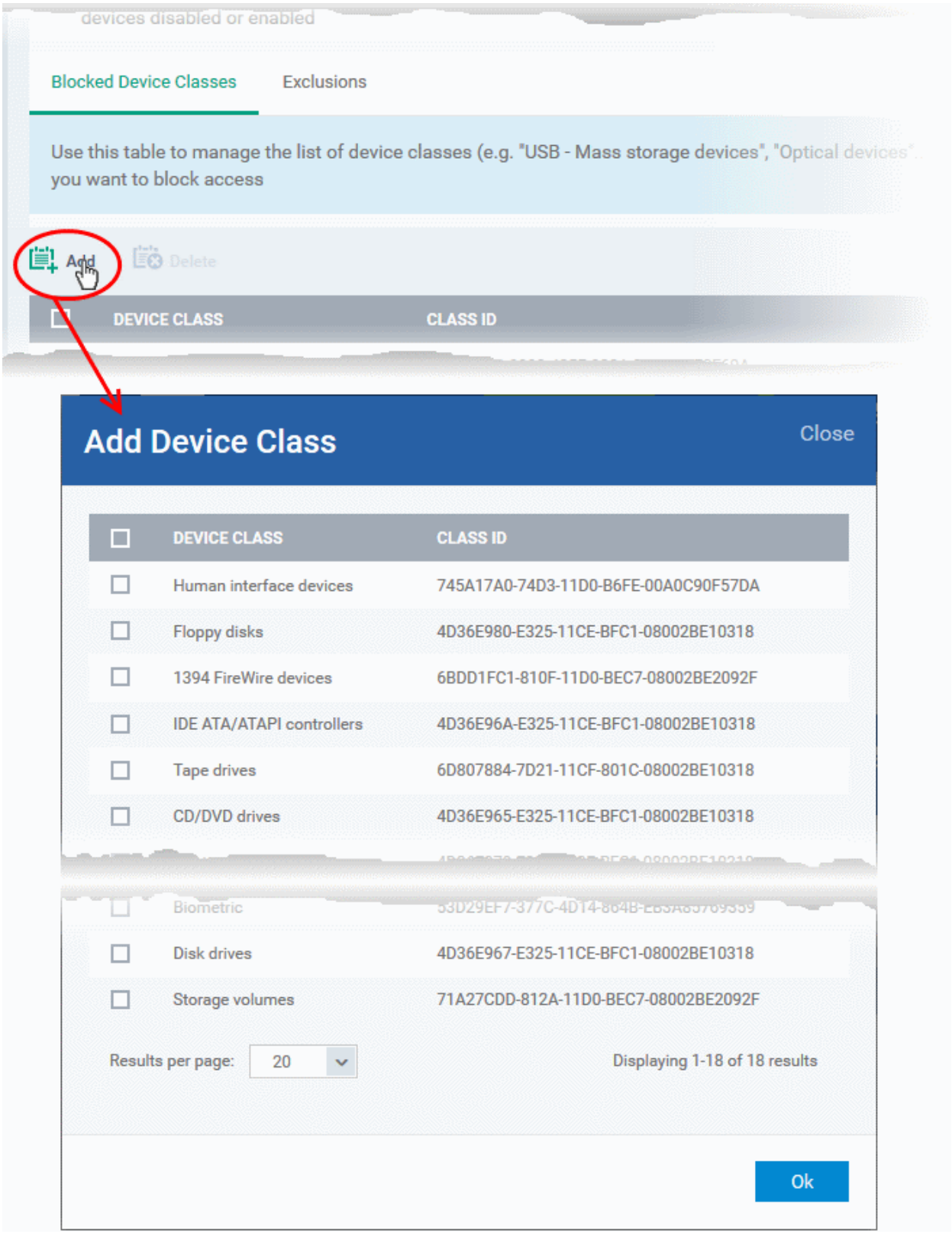


Blocked Device Classes - Column Descriptions	
Column Header	**Description**
Device Class	Displays the device type as per global hardware classification
Class ID	Displays the Globally Unique Identifier (GUID) of the device class

To add device types to be blocked

- Click 'Add' at the top of the list

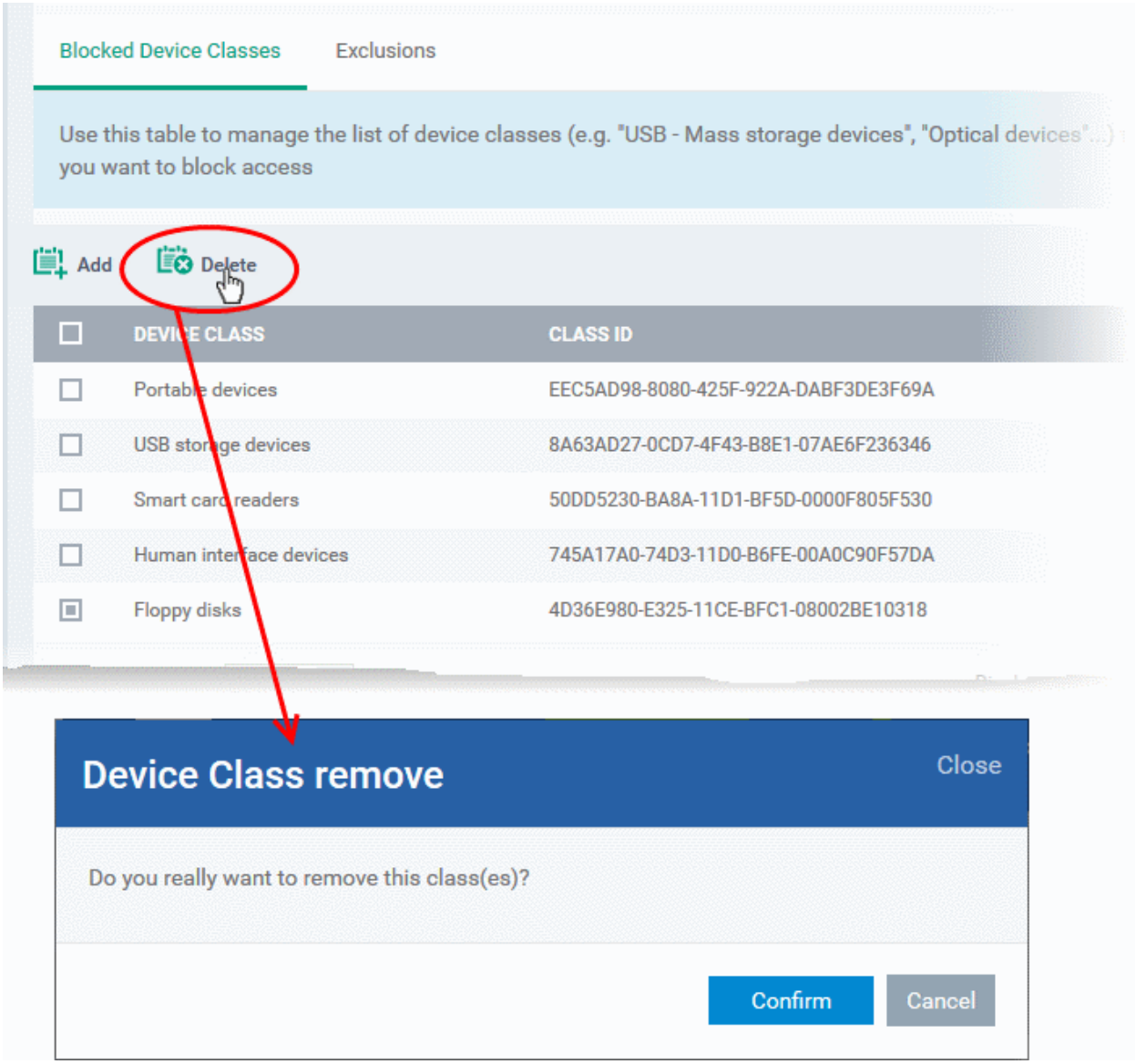
The 'Add Device Class' dialog will appear with a list of device types.



- Select the device types to be added to the block list and click 'Ok'.
- Repeat the process to add more device types.

To remove a device type from the list

- Select the device type from the list and click 'Delete'

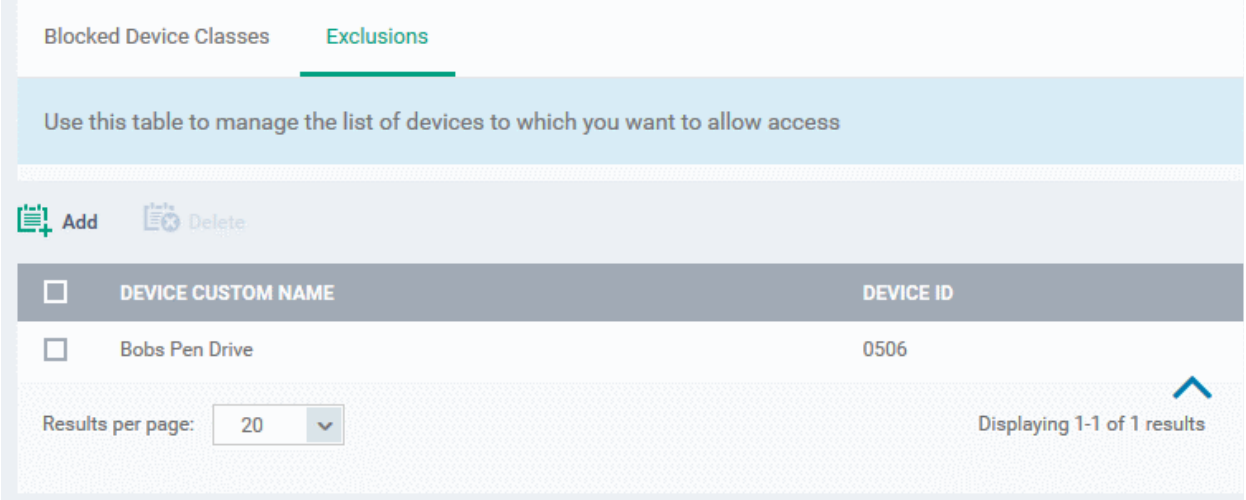


A confirmation dialog will appear.

- Click 'Confirm' to remove the device type from the blocked list.

Exclusions

The 'Exclusions' tab displays a list of external devices that are exempt from the block rule and so allowed access to the endpoint(s).

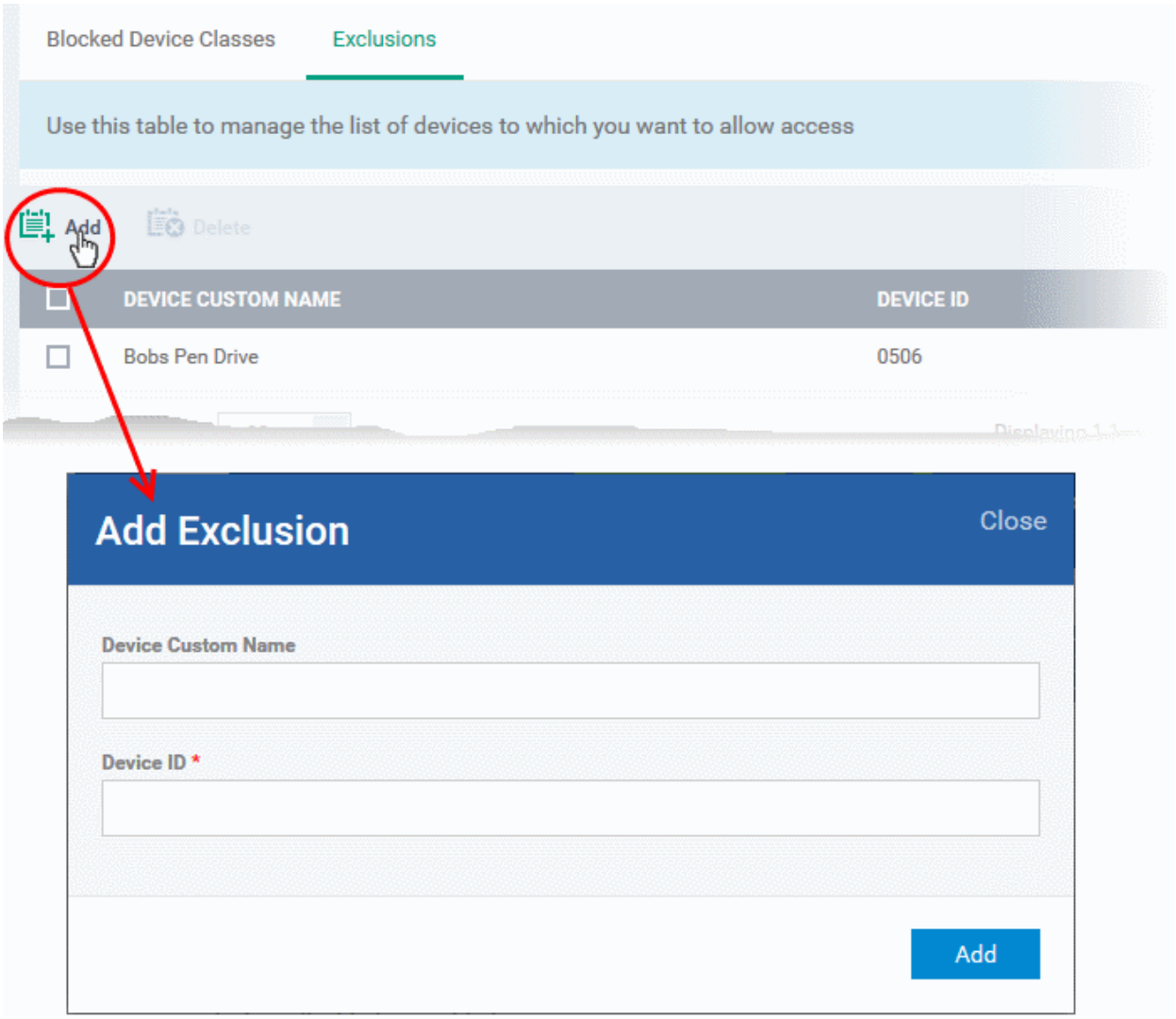


Exclusions - Column Descriptions	
Column Header	**Description**
Device Custom Name	Displays the name of the device.
Device ID	Displays the unique device identifier of the device.

To add a device to be excluded

- Click 'Add' at the top of the list

The 'Add Device Class' dialog will appear with a list of device types.

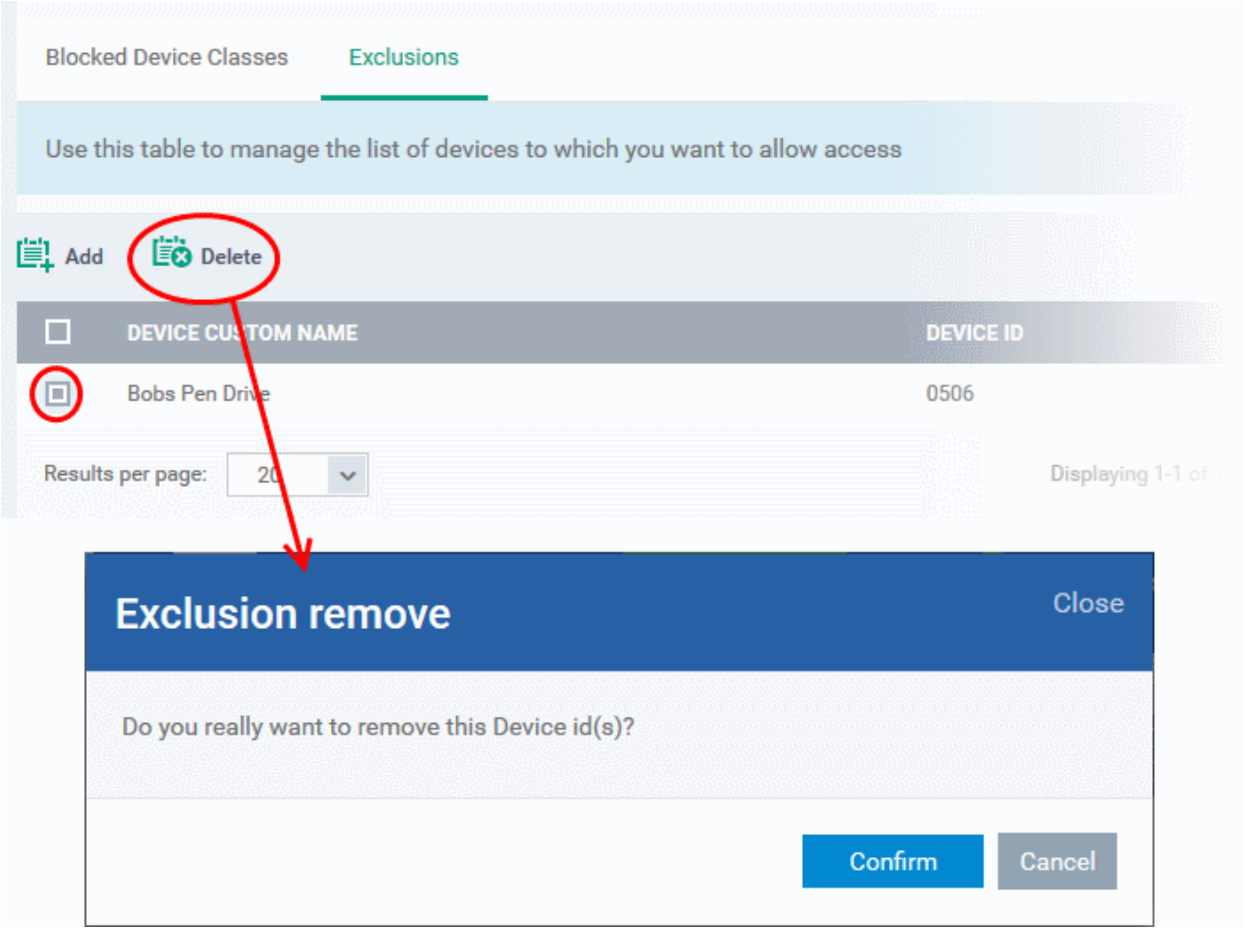


- Enter the custom name of the device in the 'Device Custom Name' field and the unique device identifier in the 'Device ID' field
- Click 'Add'

The device will be added to the exclusions list and will be allowed access to the endpoint(s).

To remove a device from exclusions

- Select the device and click 'Delete'



A confirmation dialog will appear.

- Click 'Confirm' to remove the item from the list
- Click the 'Save' button save the 'External Devices Control' settings.
- Click 'Delete' to remove the 'External Devices Control' section from the profile. Refer to the section '**Editing Configuration Profiles**' for more details about editing the parameters.

6.1.3.1.16. Monitoring Settings

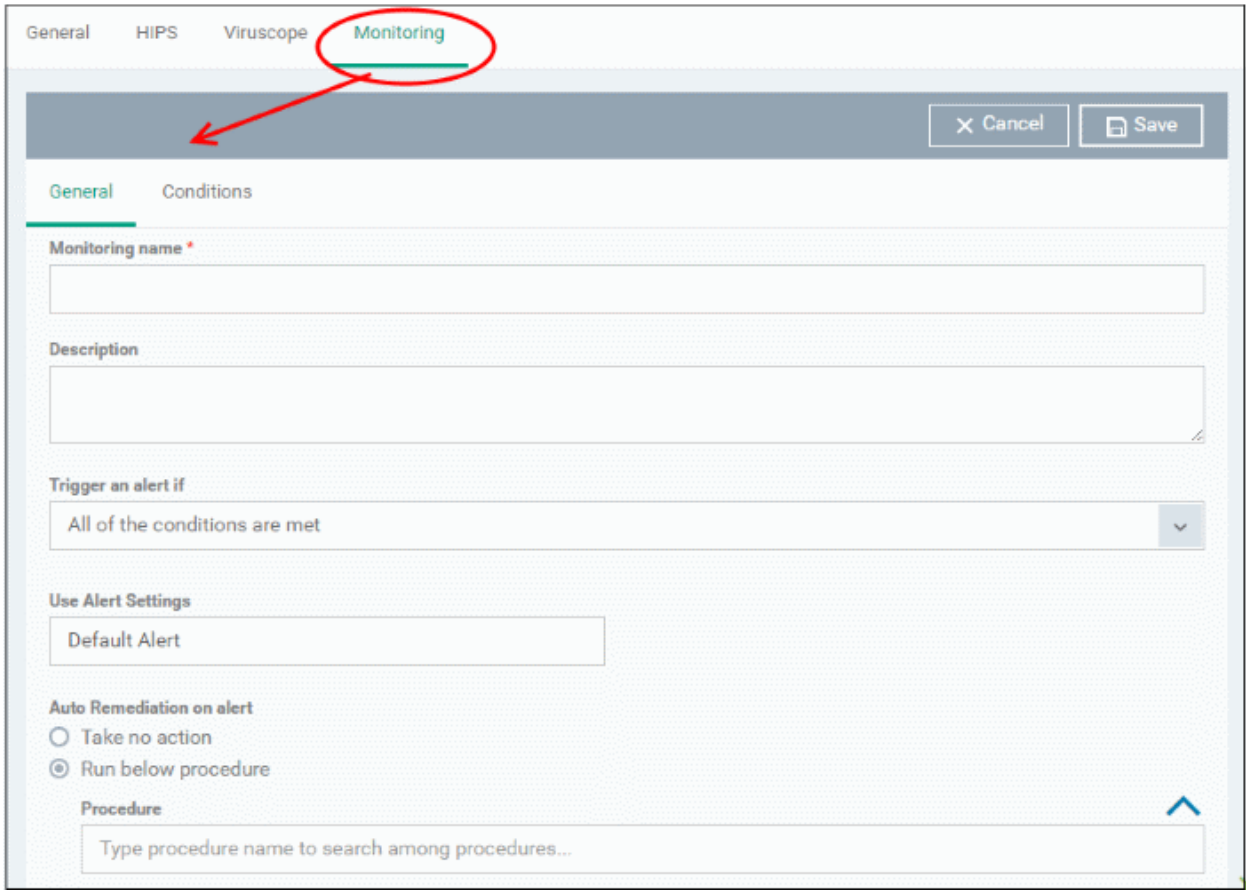
Monitoring settings allow administrators to define performance and availability conditions for various events and services. An alert will be triggered if the conditions are breached. For example, you can monitor free disk space, service and web page availability, CPU/RAM usage and more. You can also configure automatic procedures to run if an alert is generated.

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

To configure monitoring settings

- Choose 'Monitoring' from the 'Add Profile Section' drop-down

The 'Monitoring' screen will be displayed.



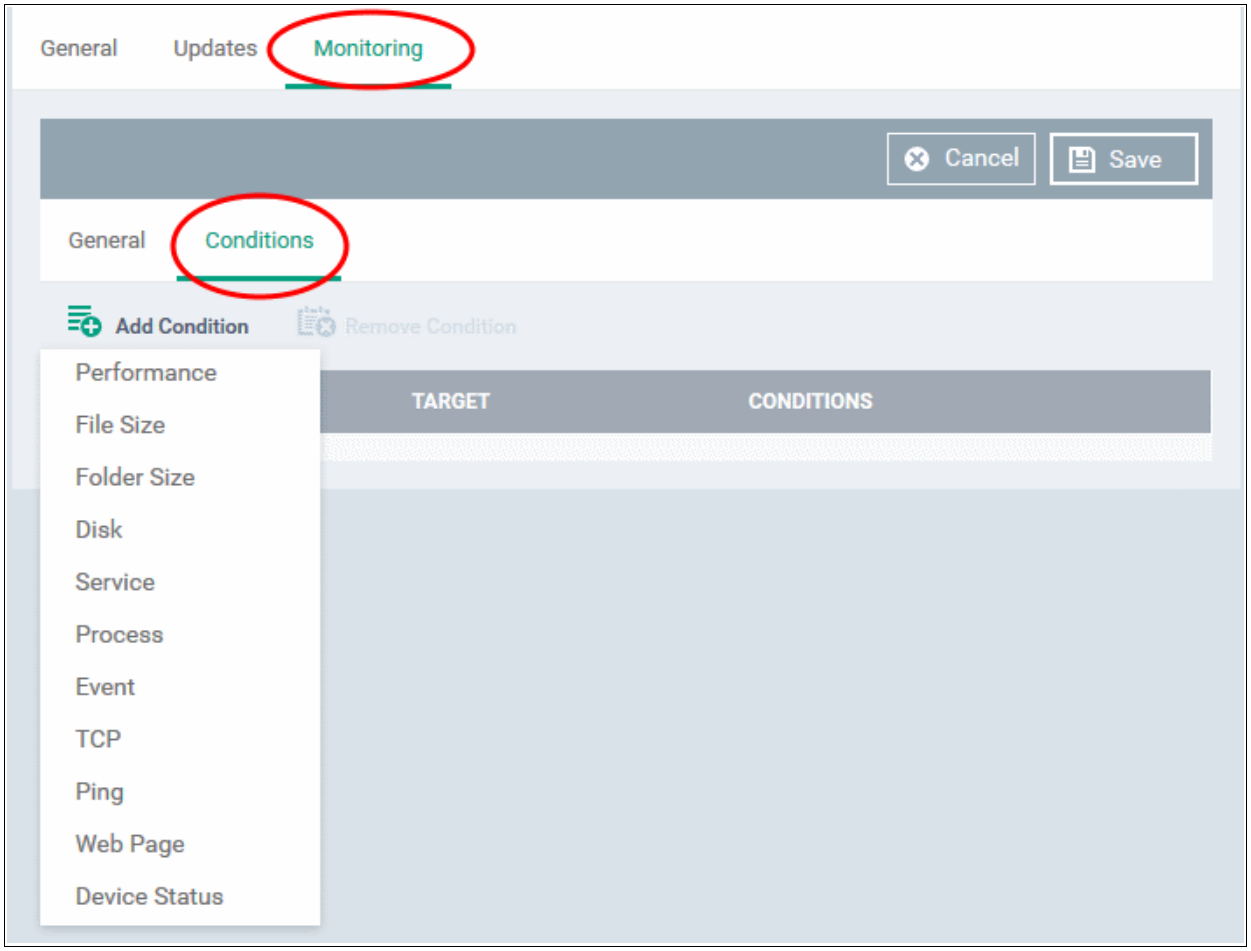
General Tab

- Monitoring Name - Provide a name for the monitoring setting
- Description - Enter appropriate comments for the monitoring setting
- Trigger an alert if - Allows you to select when the alert should be sent. The options are to send alert when all conditions are met and any of the conditions are met.
- Use Alert Settings - Allows you to select the alert that should be generated. The alert types that are listed here are predefined in the 'Alerts' section. Refer to the section '**Managing Alerts**' for more details.
- Auto Remediation on alert - Allows you the choice whether to take automatic remedial action for the alert or not.
    - Taken no action - No remedial action will be taken automatically. You can, of course, manually take appropriate action for the generated alert.
    - Run below procedure - If selected, the 'Procedure' field allows you to select the procedure that should be run automatically for the alert on the affected endpoints. The procedures listed here are predefined in the **Procedures** interface. Type first few characters of the procedure and select an appropriate procedure from the list.

Conditions Tab

The conditions tab allows you to define thresholds for various monitoring parameters that when breached will trigger alerts per the setting.

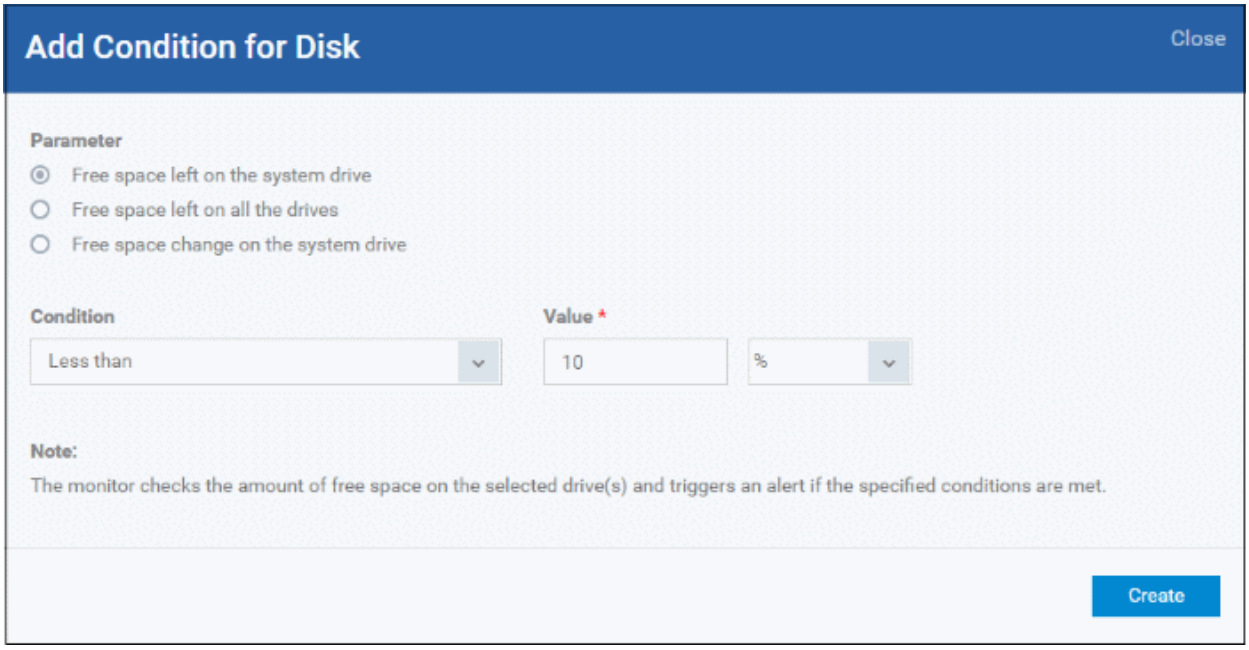
- Click 'Add Condition'



Monitoring Conditions	
Name of the Condition	**Description**
Performance	Checks the usage of CPU, RAM and Network on devices and triggers an alert if the specified conditions are met.
File Size	Checks the disk space used by a specified file on target computers and triggers an alert when the specified conditions are met.
Folder Size	Checks the disk space used by a directory/folder on target computers and triggers an alert when the specified conditions are met.
Disk	Checks for free disk space and free space change and triggers an alert whenever the specified conditions are met.
Service	Checks periodically if the specified services are matching the required status, for example, running, stopped, not started.
Process	Checks if the specified processes are running or not running and triggers an alert if the conditions are met.
Event	Checks Windows Event logs on devices. Alerts are generated when a Windows event with the specified Event Sources, Event IDs or Event level occurs.
TCP	Periodically attempts to connect to a specified host name / IP:port. The monitor can be configured to trigger alerts based on connection status. This allows to check for services that should be running and trigger alerts when ports that should be closed become open.

Ping	Pings a device using its hostname, fully qualified domain name or an IP Address to check the connectivity and triggers an alert depending on the selected option.
Web Page	Checks periodically the web page content of the specified URL and triggers an alert if the specified conditions are met.
Device Status	Checks that the device has sent a message to confirm that it is online and connected. Each device sends its online status message to the ITSM server every minute and monitoring period is set as 3 minutes. If ITSM does not receive the online status from a device continuously for 3 minutes, the device's state is set to 'Offline'.

You can add as many monitoring parameters as required for the profile. The conditions depend on the type of monitor selected. For example, if you select 'Disk' monitor, you have the option to specify conditions for three parameters. See example image below.

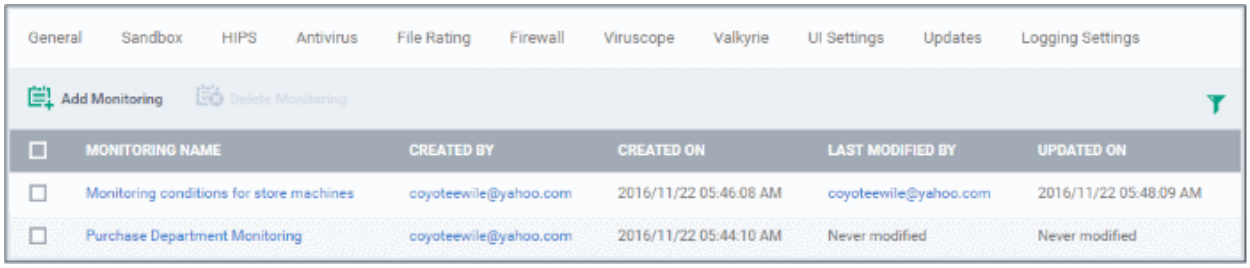


- Click 'Create' after specifying the conditions.

The monitoring parameters added for the profile will be listed.

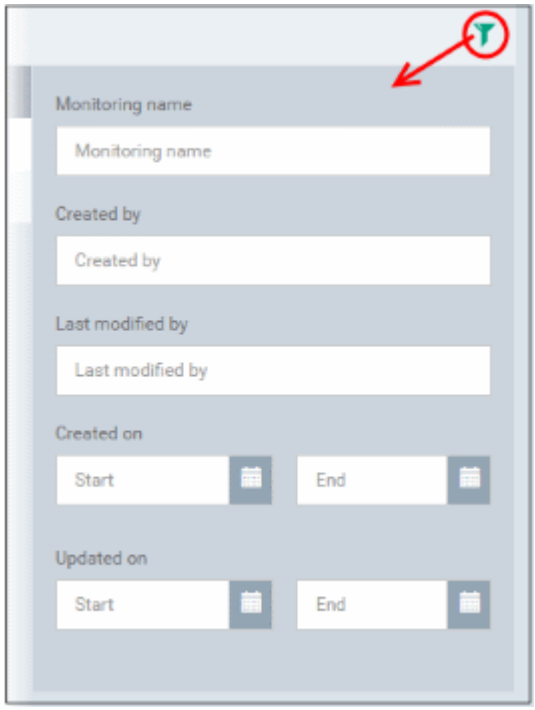
- To remove a monitoring condition, select the check box beside it and click 'Remove Condition' at the top.
- Click 'Save' to apply your changes.

- Repeat the process to add more monitors. The added monitors will be listed under the 'Monitoring ' tab in the profile.

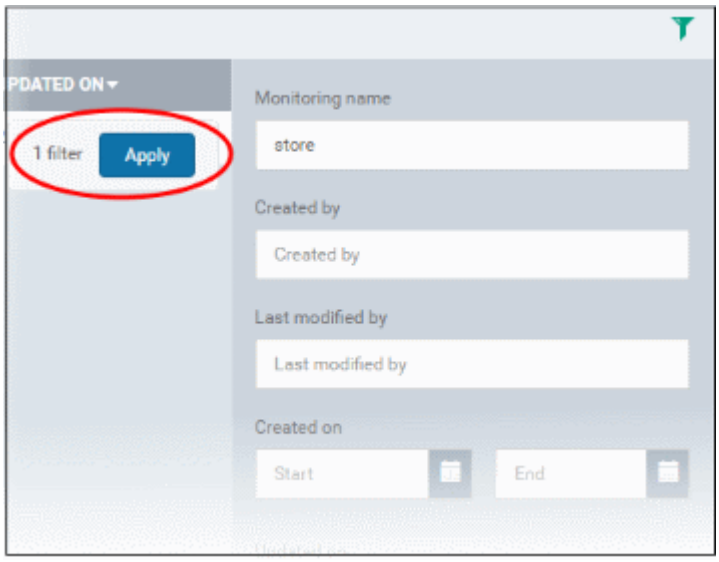


Sorting, Search and Filter Options

- Clicking on the column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific monitor, enter the search criteria in part or full in the 'Monitoring name', 'Created by' and / or 'Last modified by' fields and click 'Apply'

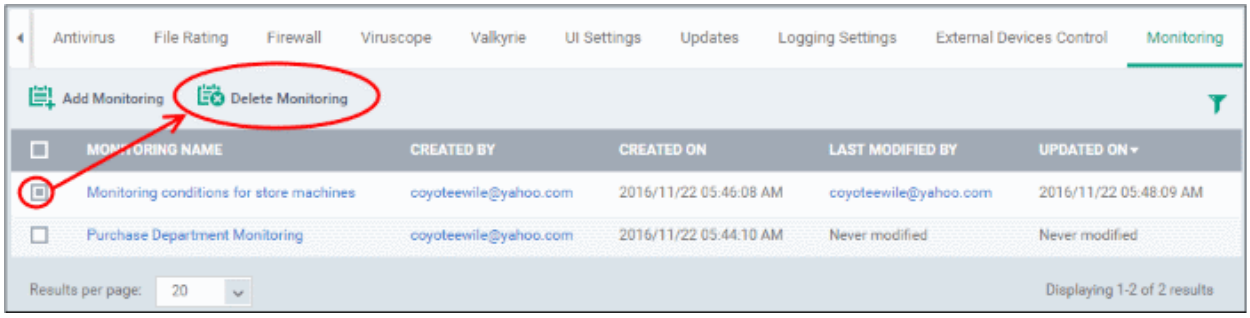


- To filter the monitors by 'Created on' and / or 'Updated on' dates, enter or select from the calendar the start and end dates of the period in the respective 'Start' and 'End' fields and click 'Apply'.

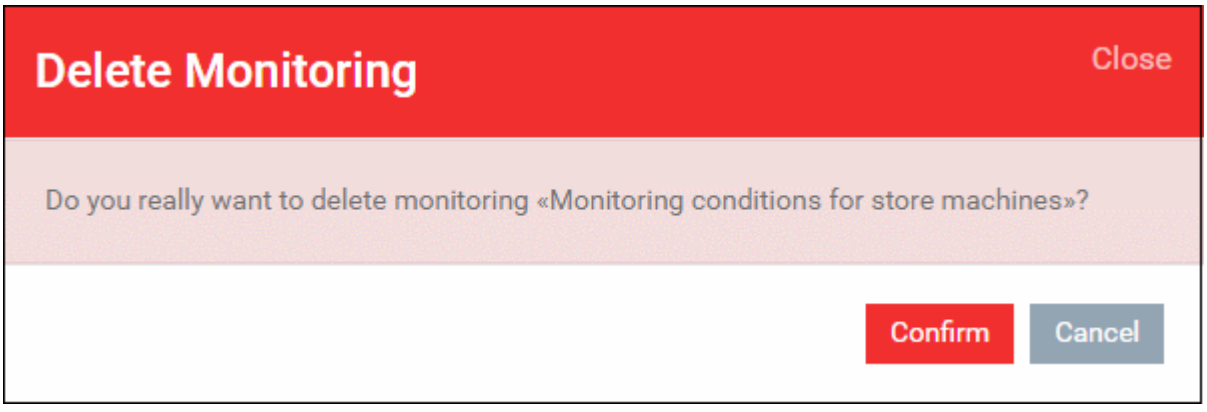
You can use any combination of filters at-a-time to search for specific monitors.

- To display all the items again, remove the search key from filter(s) and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

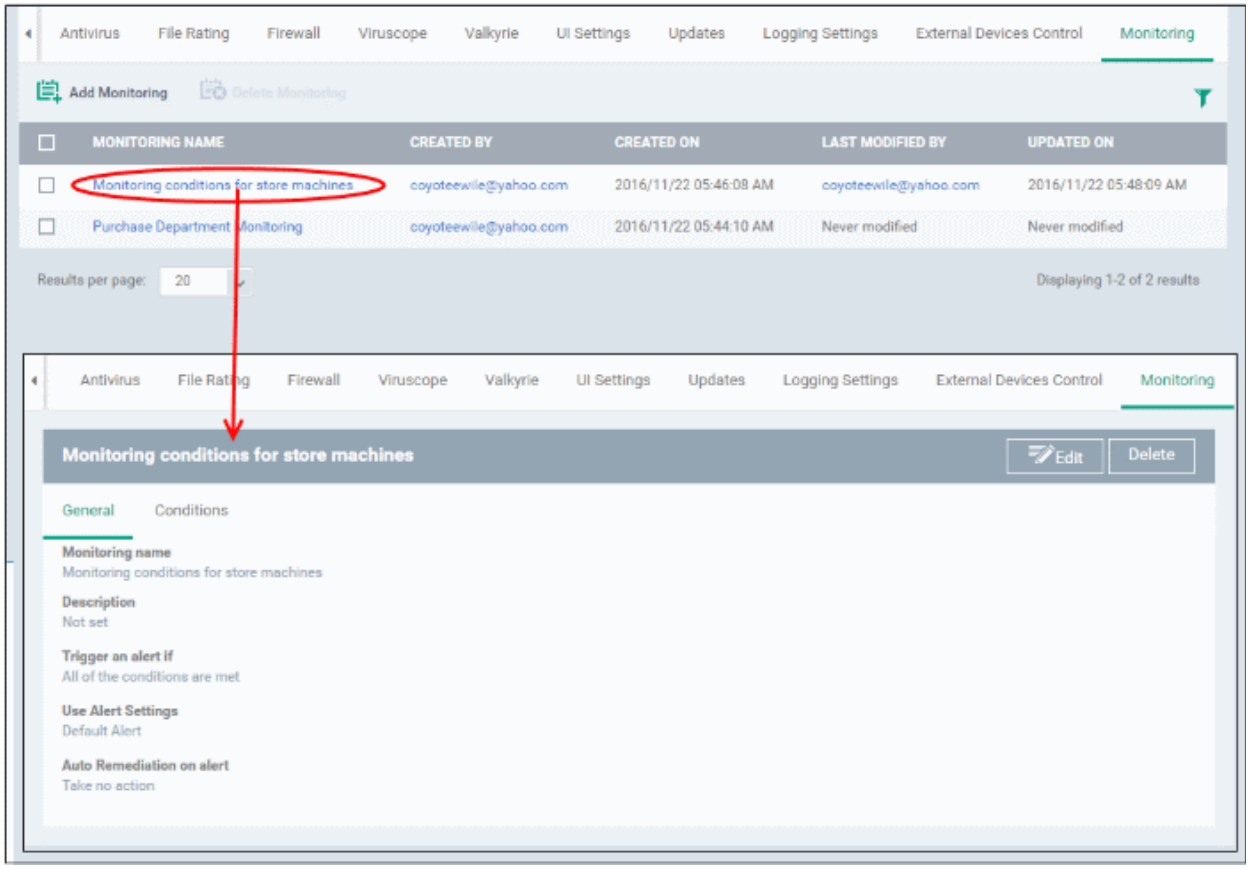
To remove a monitor from the profile, select it and click 'Delete Monitoring' at the top.



A confirmation message will be displayed.



- Click 'Confirm' to remove the selected monitor.
- To edit a monitor, click the name and then the 'Edit' button on the right.



The editing procedure is similar to adding a new monitor as explained above. Click 'Save' after editing the name, description, alert and / or the monitoring conditions.

6.1.3.1.17. CCM Certificate Settings

The Certificates Settings section of a profile allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Once the profile is applied to a device, a certificate request is automatically generated and forwarded to CCM. After issuance, the certificate will be sent to ITSM which in turn pushes it to the agent on the device for installation. You can add any number of certificates to a single profile. Appropriate certificate requests will be generated on each device to which the profile is applied.

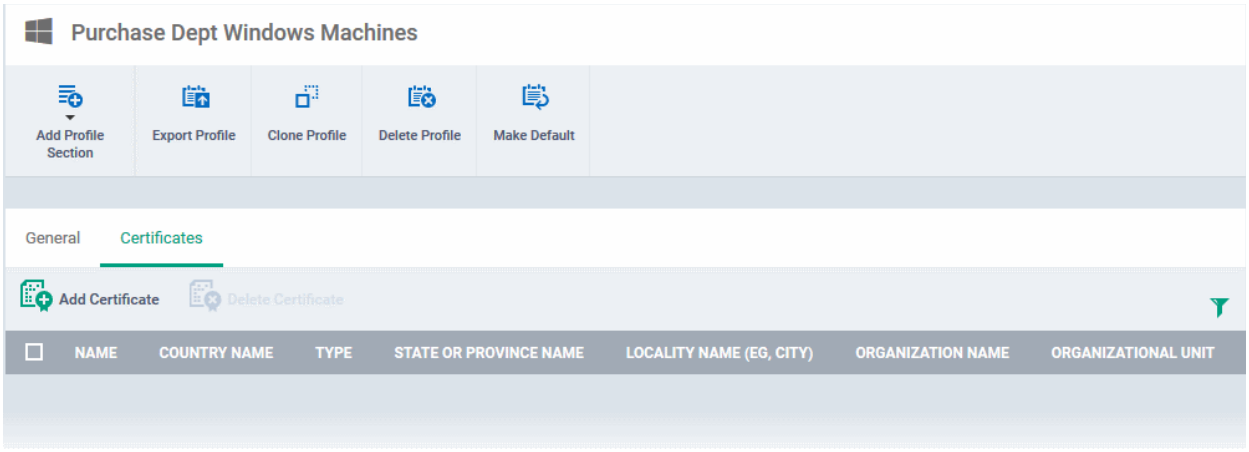
In addition to user authentication, client certificates can be used for email signing and encryption.

Prerequisite: Your CCM account should have been integrated to your ITSM server in order for ITSM to forward requests to CCM. For more details, refer to the section **Integrating with Comodo Certificate Manager.**

To configure CCM Certificate settings

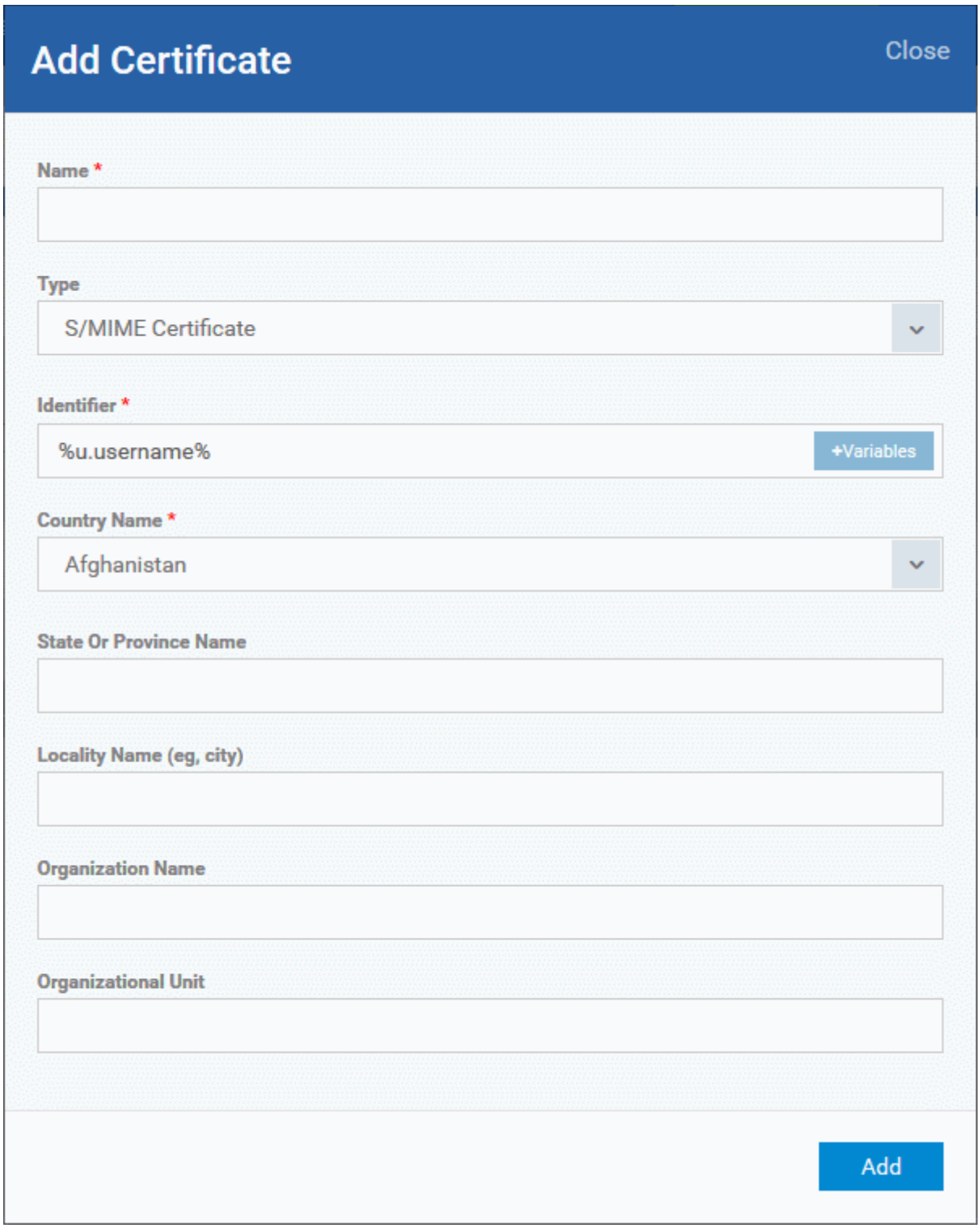
- Choose 'Certificates' from the 'Add Profile Section' drop-down

The settings screen for adding certificate requests to the profile will be displayed.



- Click 'Add Certificate' at the top to add a certificate request to the profile

The 'Add Certificate' form will appear.



Add Certificate - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter a name for the certificate to be requested, shortly describing its purpose.
Type	Drop-down	Select the type of certificate to be added. The available options are: • S/MIME Certificate (Client Certificate) • Device Certificate

Add Certificate - Table of Parameters		
Identifier	Text Field	The Identifier field will be auto-populated with mandatory variables depending on the chosen certificate type. • For client certificate, %username% will be added for fetching the username to be included as subject in the certificate request. • For device certificate, %d.uuid% will be added for fetching the device name to be included as subject in the certificate request. You can add more variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Country Name	Text Field	Enter the address details of the user/organization in appropriate fields.
State or Province Name		
Locality Name (eg. City)		
Organization Name	Text Field	Enter the name of the organization to which the user/device pertains. Prerequisite: The organization should have been added to your CCM account.
Organizational Unit	Text Field	Enter the name of the department to which the user/device pertains. Prerequisite: The department should have been defined under the organization in your CCM account.

- Click 'Add' once you have completed the form.
- Repeat the process to add more certificate requests.

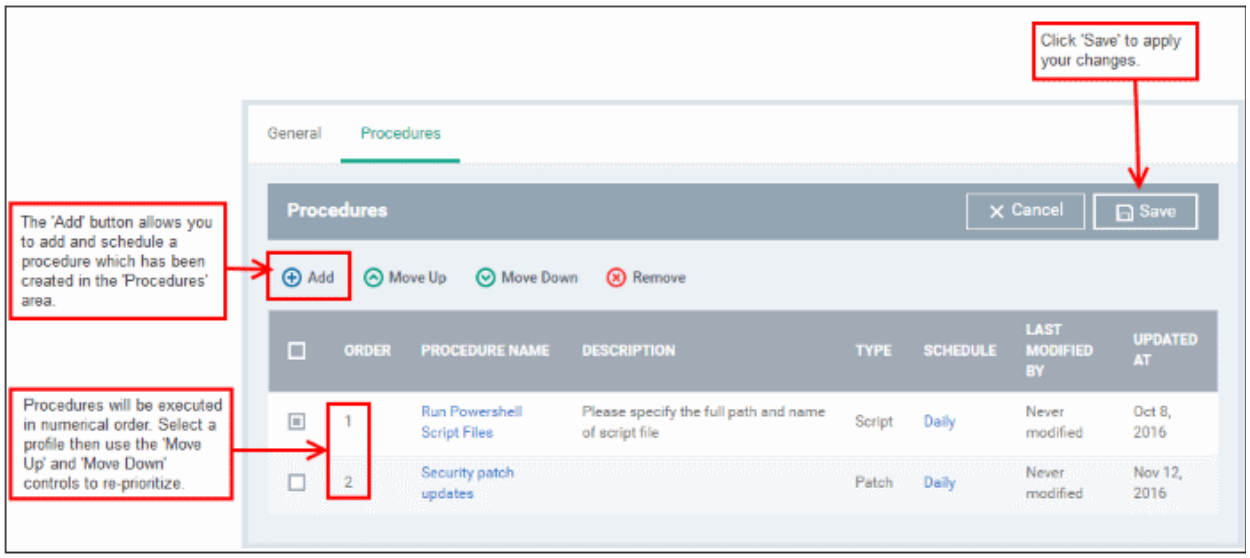
The certificate requests will be generated from the devices once the profile is applied to them.

6.1.3.1.18. Procedures Settings

ITSM allows you to add scripts and patches as procedures to run on Windows devices. You can also automate the process by adding procedures to a profile and scheduling for deployment as required. The procedures area of a profile allows you to add, view, delete and prioritize procedures which have been added to a profile.

To add procedures to a profile

- Click 'Configuration Templates' > 'Profiles'
- Open a Windows profile from the list
- Click 'Add Profile Section' > 'Procedures'



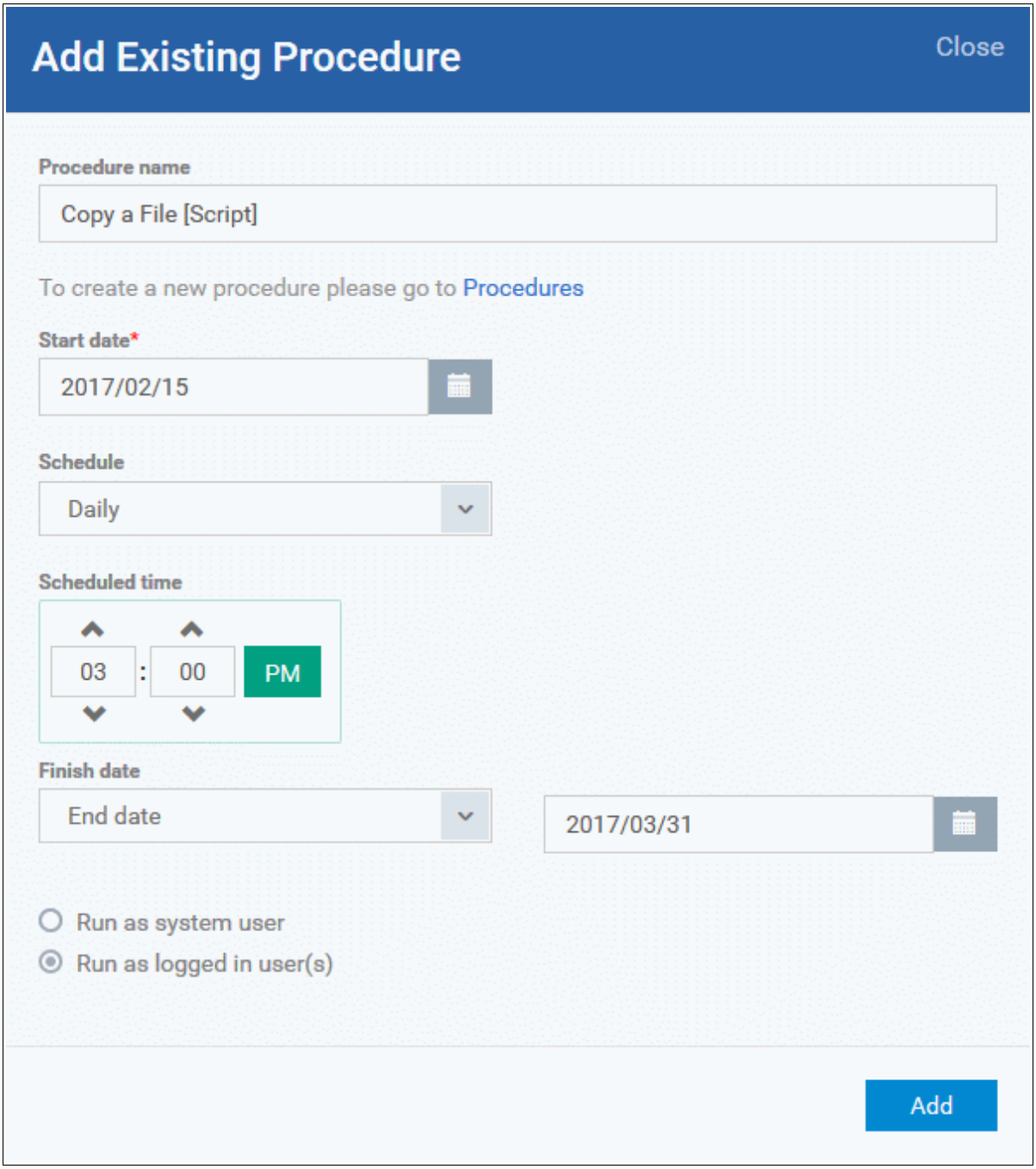
Procedures are created and configured in the 'Procedures' area ('Configuration Templates' > 'Procedures').

Managing Procedures contains help about configuring a procedure and adding a procedure to a profile:

- Create a Custom Procedure
- Combine procedures to build broader procedures
- Review / Approve / Decline new procedures
- Add a Procedure to a Profile / Procedure Schedules
- Import / Export / Clone Procedures
- Change Alert Settings
- Directly Apply Procedures to Devices
- Edit / Delete Procedures
- View Procedure Results

To add a procedure

- Choose 'Procedures' from the 'Add Profile Section drop down' and click 'Add'.



- Choose a procedure to run by entering the first few characters of the existing procedure name and selecting it from the options. For more details on procedures configured in ITSM refer to the section Viewing and Managing Procedures.
- The next step is to create a schedule for the procedure to run periodically on the devices applied with this profile
    - Select the 'Start date' for the procedure by clicking the calendar icon beside 'Start Date' and choosing a date.
    - Select the period fro the schedule from the Schedule drop-down. The available options are:
        - Never
        - Daily
        - Weekly - If chosen you need to select the days of the week on which the procedure is to be run
        - Monthly - If chosen you need to select the dates of a month on which the procedure is to be run

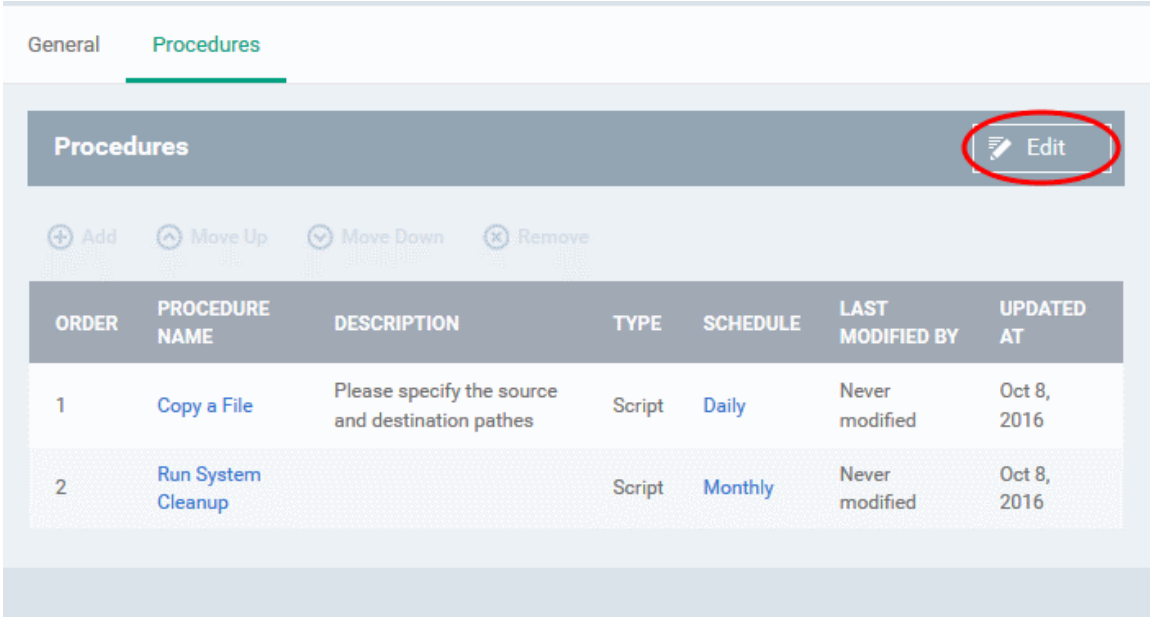
- Set the time at which the procedure is to be run on the scheduled days from the Scheduled Time field
- Then select the 'Finish date'. If you select 'End date', from the drop down, then specify the end date for the procedure from the calendar.

- If you have chosen a 'Script' type procedure, Then select the user account with which the procedure has to be run. The available options are:
  - Run as System User - The procedure will run with administrative privileges
  - Run as logged-in user(s) - The procedure will run with privileges of the user currently logged-on to the endpoint
- Repeat this process to add multiple procedures.
- Click 'Save'.

Administrators can add or edit procedure by clicking 'Edit' button present on the top right corner of the profile section tab.

To edit a procedure:

- Click 'Edit' and select the procedure that needs to be modified.
- Then click either 'Add', 'Move Up', 'Move down', or 'Remove' based on the changes that need to take effect.
  - Click 'Add' to add another procedure to the existing list
  - Click 'Move Up' to increase the priority of the procedure.
  - Click 'Move Down' to decrease the priority of the procedure.
  - Click 'Remove' to delete the procedure.



- Click 'Save'.

6.1.3.2. Importing Windows Profiles

In addition to creating a new Windows profile from the ITSM interface, you can create new profiles for rolling out to endpoints or endpoint group(s) in the following ways:

- Import the security configuration of CCS from a managed endpoint and save it as a new profile
- Export a profile from ITSM in .cfg format then import it as a new profile
- Clone an existing profile and edit it to create a new profile

This section explains more about **Importing CCS configuration from a selected endpoint**.

- For more details on Importing configurtion from an exported profile, refer to the section Exporting and Importing Configuration Profiles.
- For more details on creating a new profile by Cloning a profile, refer to the section Cloning a Profile.

Importing CCS Configuration from a Managed Device

By importing the configuration of Comodo Client Security from an existing endpoint, you can create a Windows profile which can be deployed to similar machines on your network.

- Step 1 - Export the current configuration from the selected device as an .xml file
- Step 2 - Import the .xml file as a profile to required endpoints or endpoint group(s).

Step 1 - Export the current configuration from the selected device as an .xml file

You can export the CCS configuration from a managed Windows device in two ways:

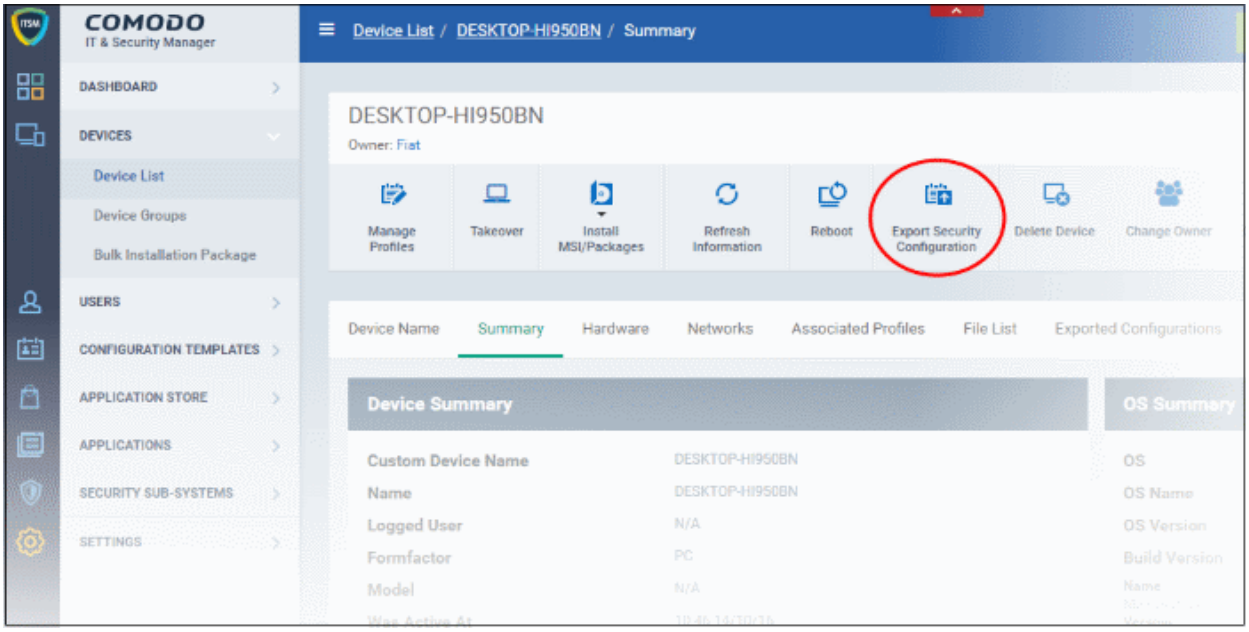
- Export configuration of a selected device from ITSM interface
- Manually export the CCS configuration from the selected device

Export Configuration from ITSM interface

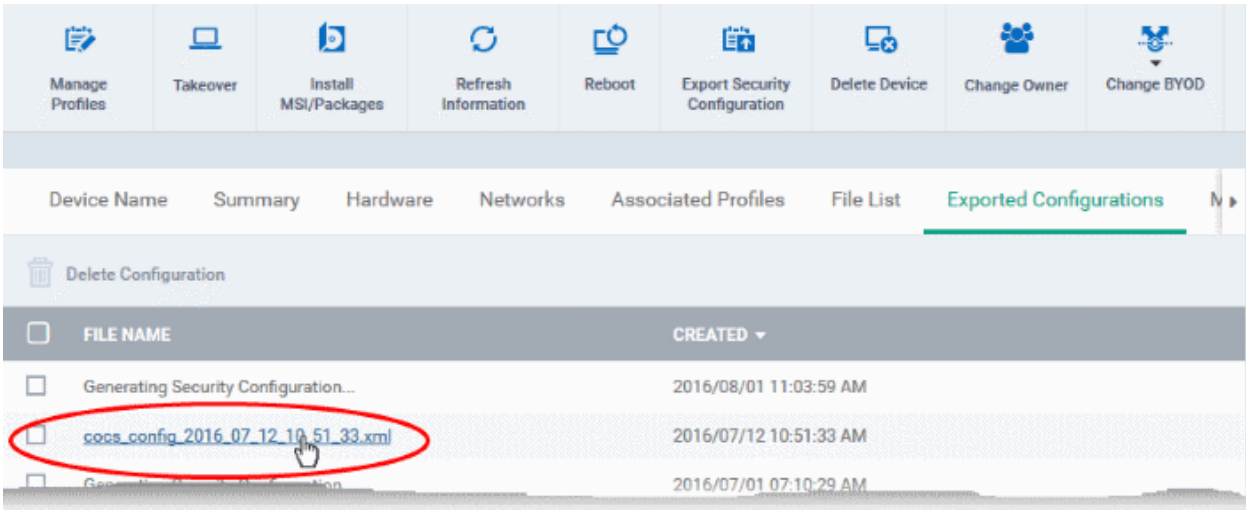
You can export the current configuration of CCS as per profiles applied to a selected device and the manual configuration of the security components of the CCS installation, as a new configuration file and import it as a new profile.

To export the configuration from a device

- Open the 'Device List' interface from the ITSM console by clicking 'Devices' > 'Device List' on the left
- Click the name of the device whose configuration you wish to export to open its 'Device Details'
- Click the 'Export Security Configuration' button:



- The CCS configuration will be exported as a .xml file and saved in ITSM.
- You can view all configuration files exported from this device under the 'Exported Configurations' tab in 'Device Details':



- Click the name of the file that you want to import as a profile and save it in a safe location.
- Then move on to **Step 2 - Import the .xml file as a profile to required endpoints or endpoint group(s)**.

Manually exporting CCS configuration from a selected device

- If you haven't done so already, configure the security settings of CCS at an endpoint to your requirements. Refer to 'Advanced Settings' in the CCS guide if you need help with this - **https://help.comodo.com/topic-399-1-790-10272-Introduction-to-Comodo-Client-Security.html**
- To export the current configuration as an xml file, the following command locally on the endpoint:

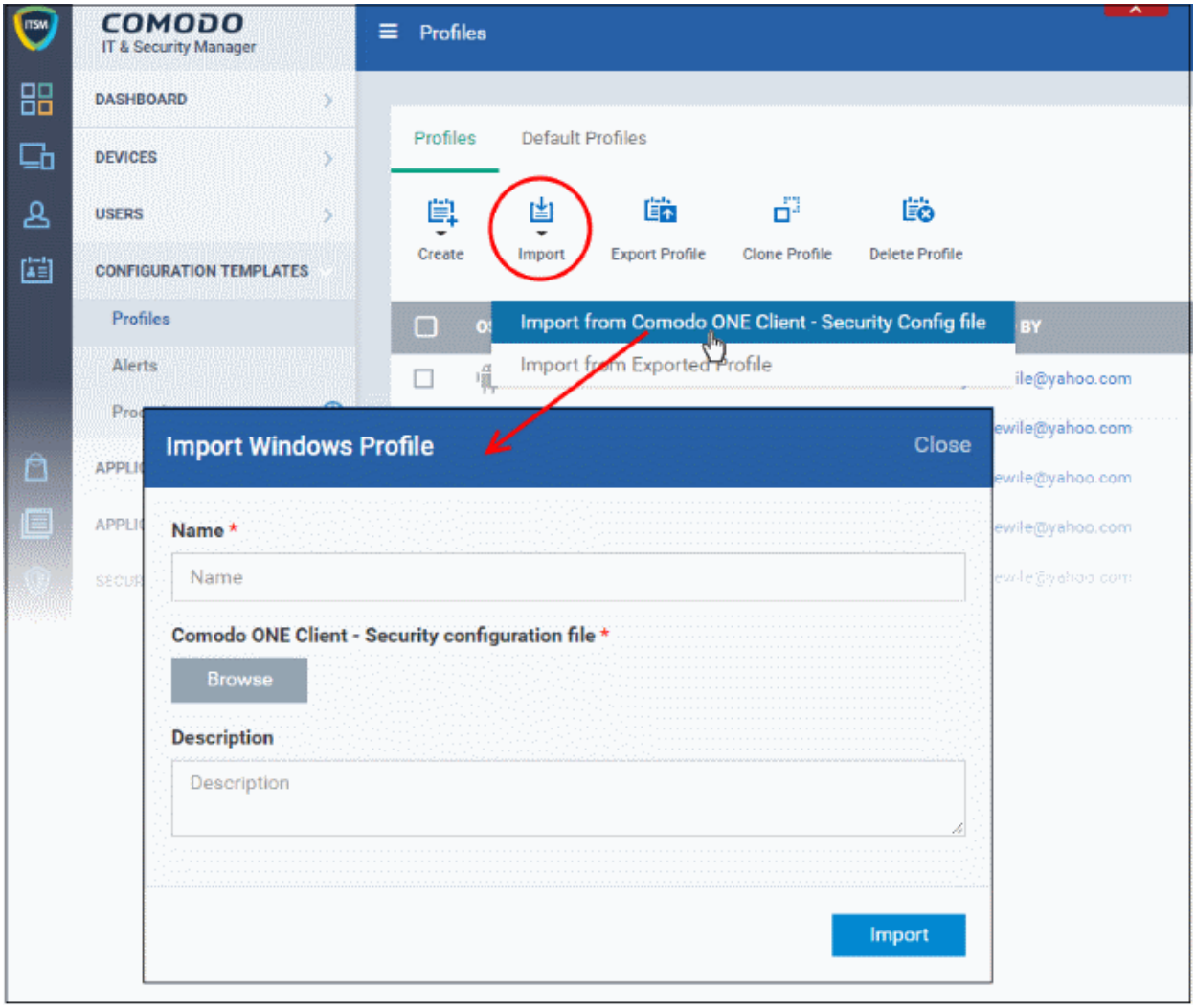
  C:\[installation folder of CCS]\cfpconfg.exe --xcfgExport="C:\<filename>.xml" --filter=""

  For example, C:\Program Files\COMODO\COMODO Internet Security\cfpconfg.exe --xcfgExport="C:\winconfigprofile.xml" --filter=""

- Copy the .xml file from the endpoint to the computer from which the ITSM console is accessed.
- Then move on to **Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)**.

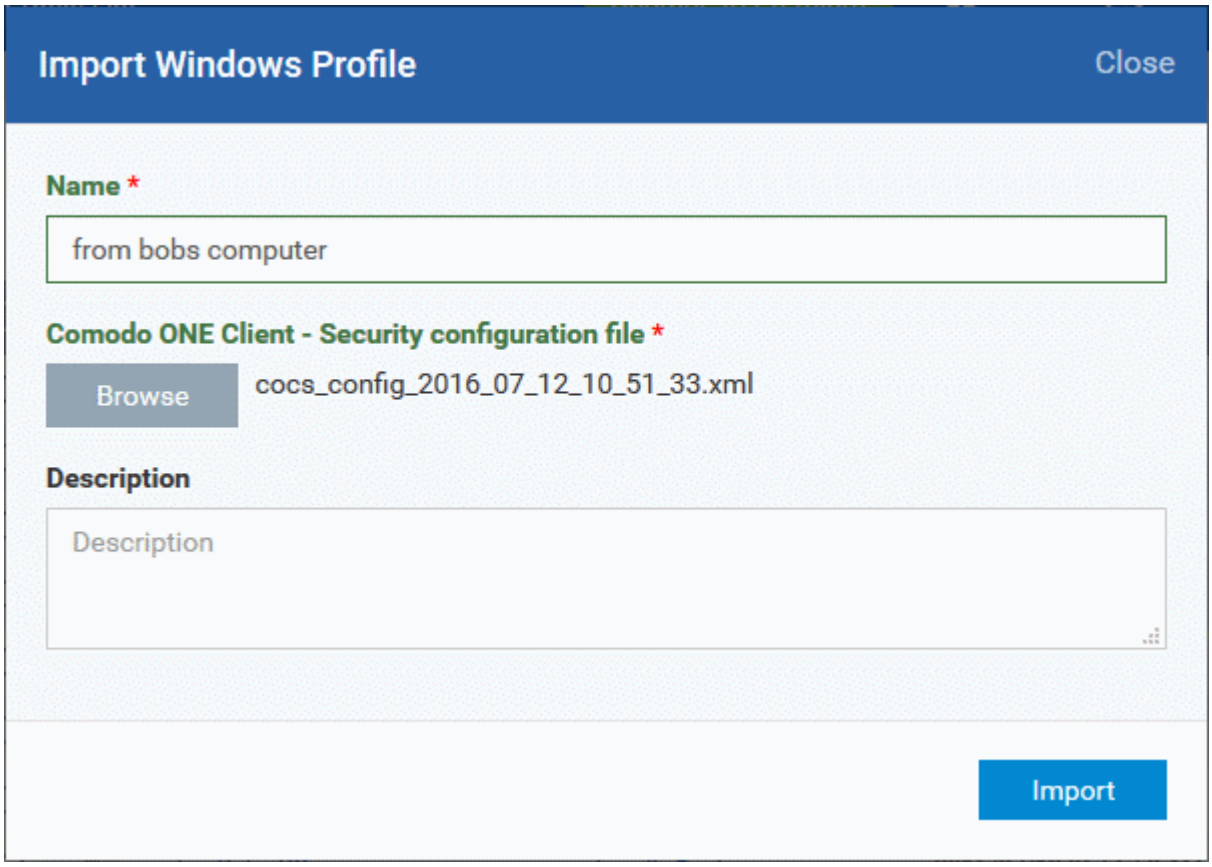
Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)

- Open the 'Profiles' screen in ITSM by clicking 'Configuration Templates' > 'Profiles' from the left hand navigation
- Click 'Import' from the top of the list and choose 'Import from 'Comodo Client Security Config file'



The 'Import Windows Profile' dialog will appear.

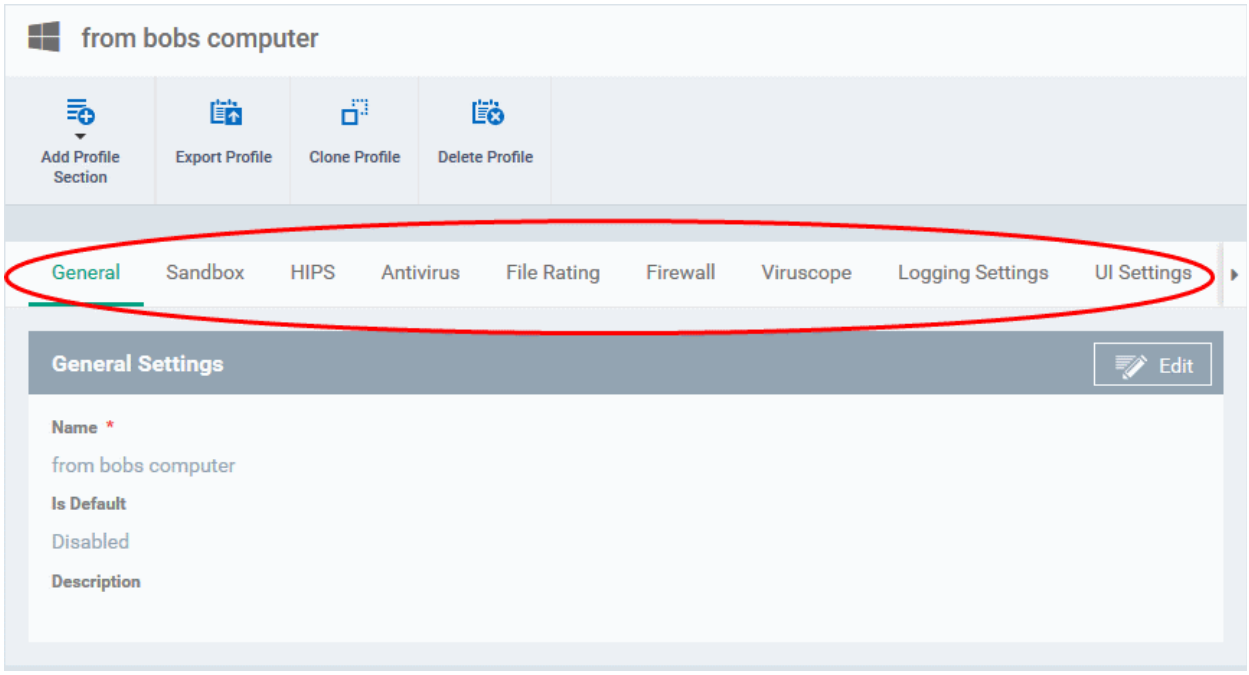
- Enter a name and description for the profile.
- Click 'Browse', navigate to the location in your computer where the .xml file is saved, select the file and click 'Open'.



The selected file will be displayed beside the 'Browse' button.

- Click the 'Import' button.

The Windows Profile interface will open, with the security components pre-configured as per the settings in the configuration file.



- The imported profile will not be set as 'Default Profile' by default.
- To change the name of the profile and/or to enable it as a default profile, click on the 'Edit' button

Edit at the top right of the 'General' settings screen, edit the settings and click the 'Save' button.

- You can now deploy this profile to endpoints and endpoint groups. You can add new profile components by clicking 'Add Profile Section' and can edit the settings for any security component by clicking the relevant tab. For more details on the options available under each component, refer to the explanation of the component settings in the previous section Creating Windows Profiles.

6.1.4. Profiles for Mac OS Devices

Mac OS profiles allow you to specify the general settings and configuration of Comodo Antivirus for Mac (CAVM) installed on managed Mac OS devices.

Security profiles for Mac OS endpoints can be added to ITSM in two ways:

- Create a CAVM profile using the ITSM interface. Refer to Creating Mac OS Profiles for more details.
- Clone an existing profile and modify its settings as per your requirements. For more details on creating a new profile by Cloning a profile, refer to the section Cloning a Profile.

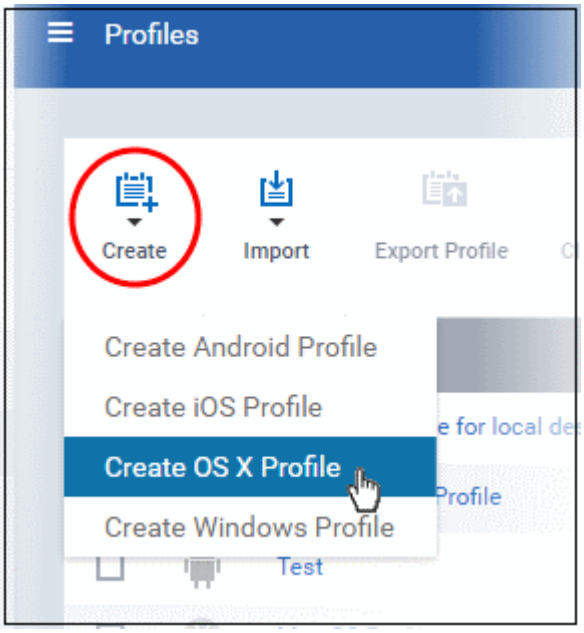
6.1.4.1. Creating Mac OS X Profiles

Creating a Mac OS Profile involves the following steps:

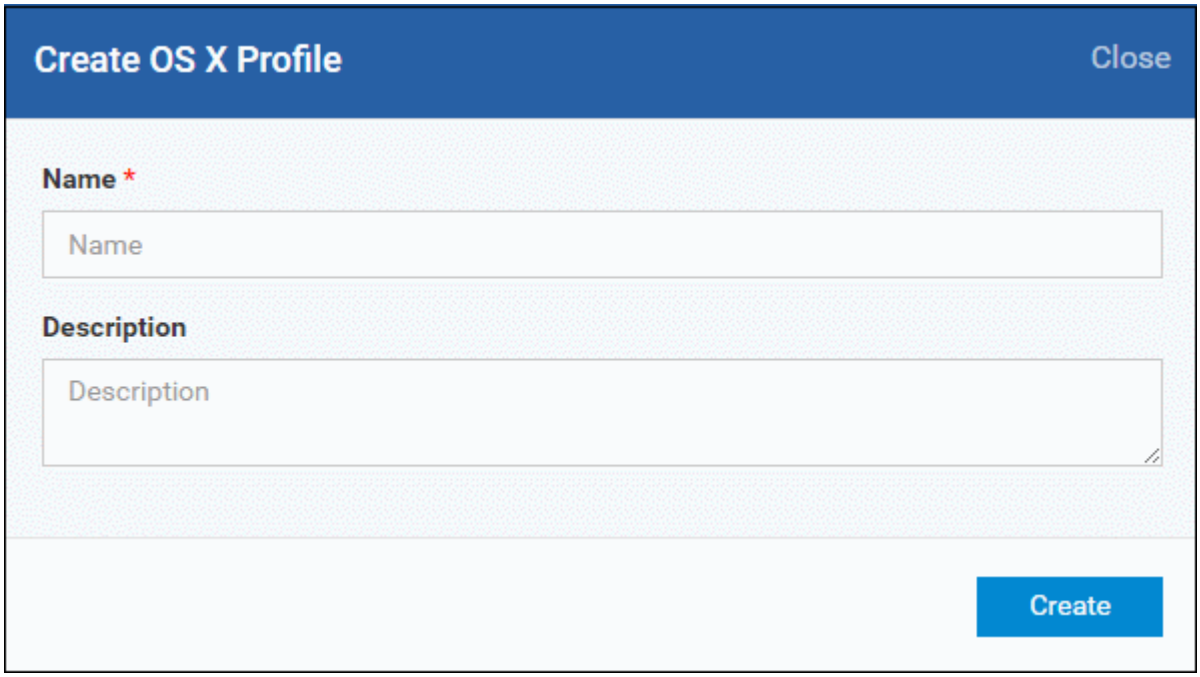
- Click 'Configuration Templates' from the left then choose 'Profiles'
- Click 'Create' then select 'Create OSX Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profiles' screen.
- New profiles have only one tab - 'General'. You can configure permissions and settings for CAVM by clicking the 'Add Profile Section' button.
- Once you have fully configured your profile you can apply it to devices and device groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.
- This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.

To create a new profile

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

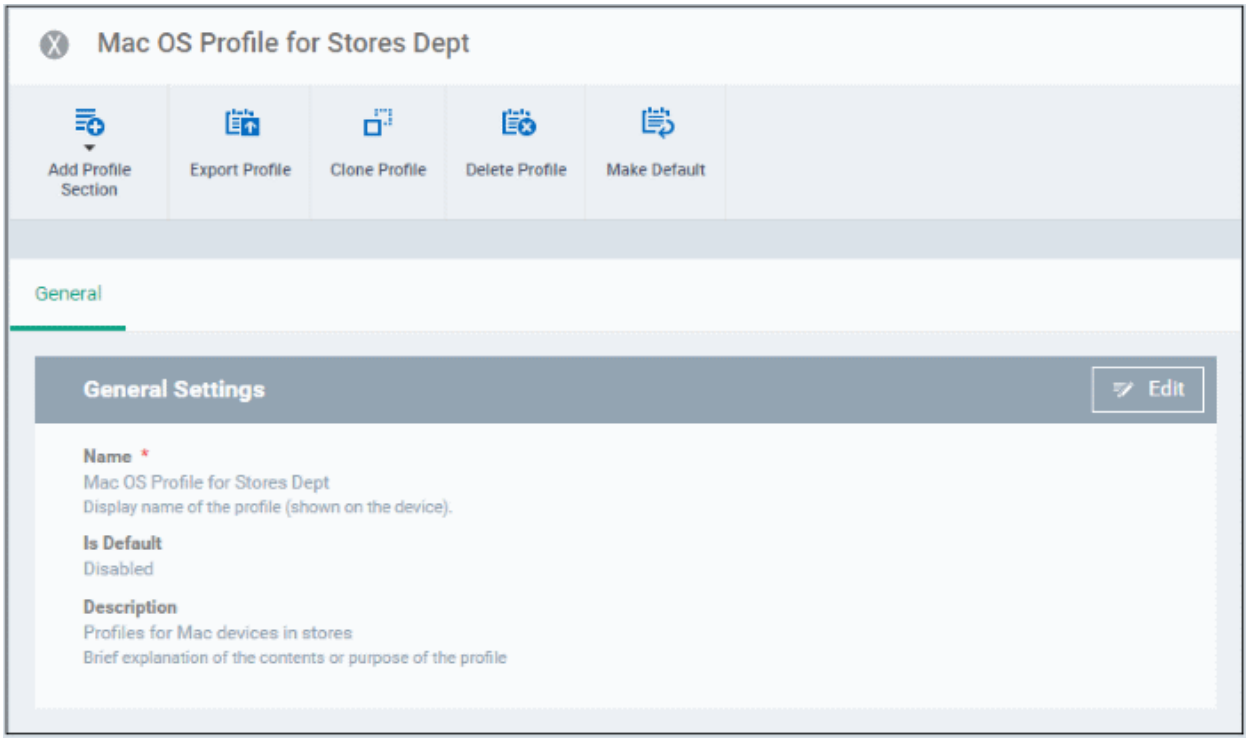


The 'Create OSX Profile' dialog will appear.



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

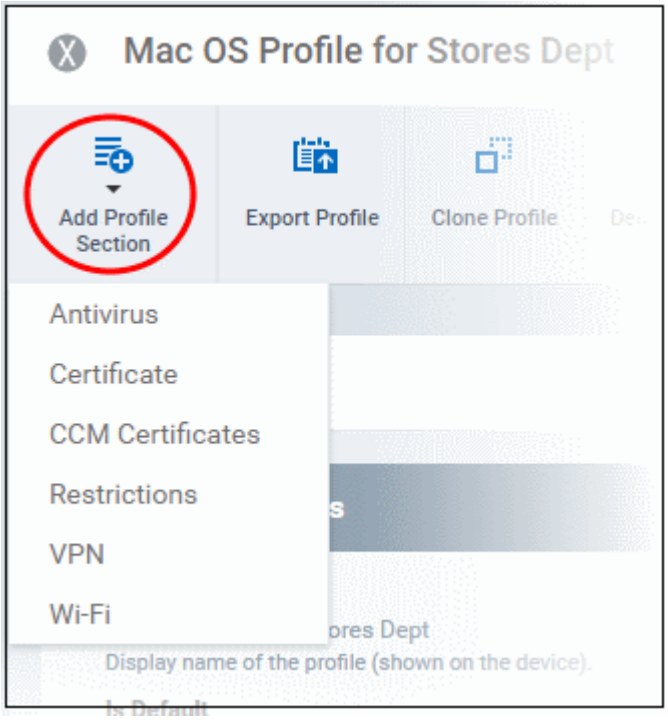
The Mac OS profile will be created and the 'General Settings' section will be displayed. The new profile is not a 'Default Profile' by default.



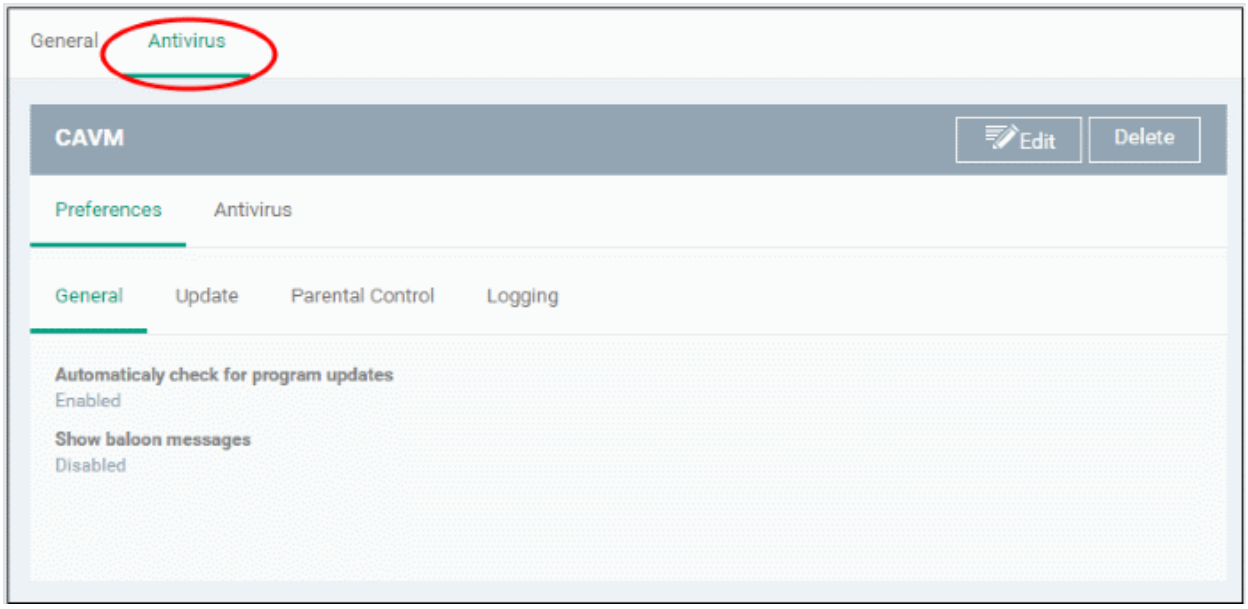
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

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

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



The settings screen for the selected component will be displayed and after saving the settings, it will be available as tabs at the top.



Following sections explain more about each of the settings:

- Antivirus
- Certificate
- CCM Certificates
- Restrictions
- VPN
- Wi-Fi

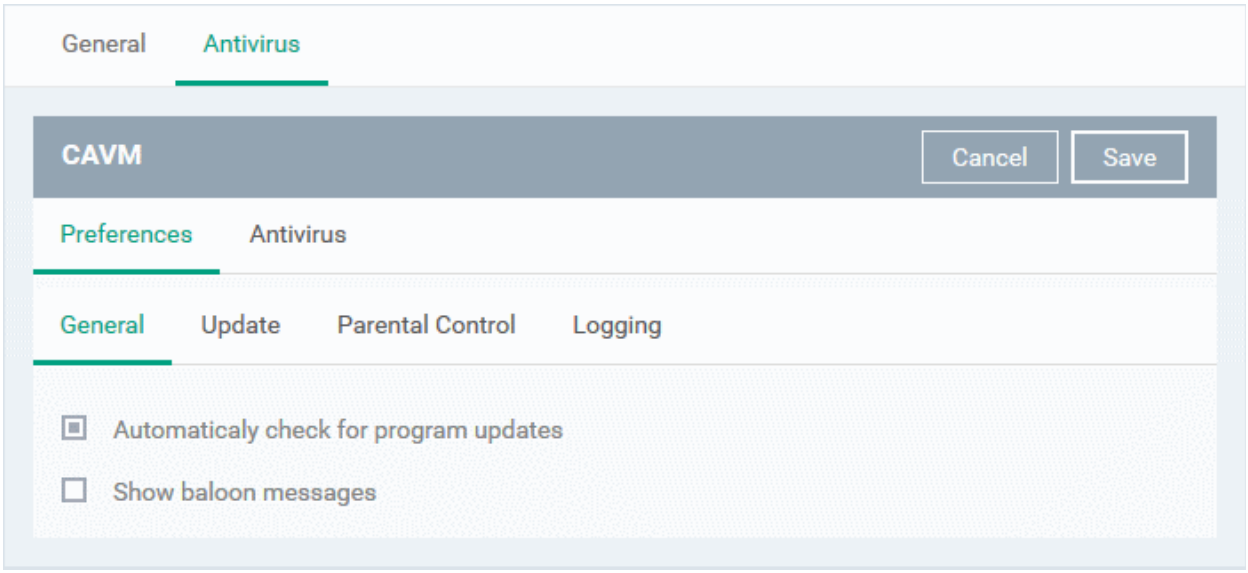
6.1.4.1.1. Antivirus Settings for OS X Profile

The Antivirus setting screen has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, Exclusions and more for the profile.

To configure Antivirus settings for OS X profile

- Choose 'Antivirus' from the 'Add Profile Section' drop-down

The settings screen for CAVM will be displayed.



It contains two tabs:

- **Preferences** - Allows you to configure general behavior, updates, parental control and log settings for CAVM.
- **Antivirus** - Allows you to configure AV scan parameters, scan profiles ans schedule AV scans.

Configuring Preferences for CAVM

The 'Preferences' tab allows you to configure the general behavior of CAVM, the server from which updates should be downloaded, parental controls and log storage settings.

You can configure for the following from the The 'Preferences' interface:

- General
- Update
- Parental Control
- Logging

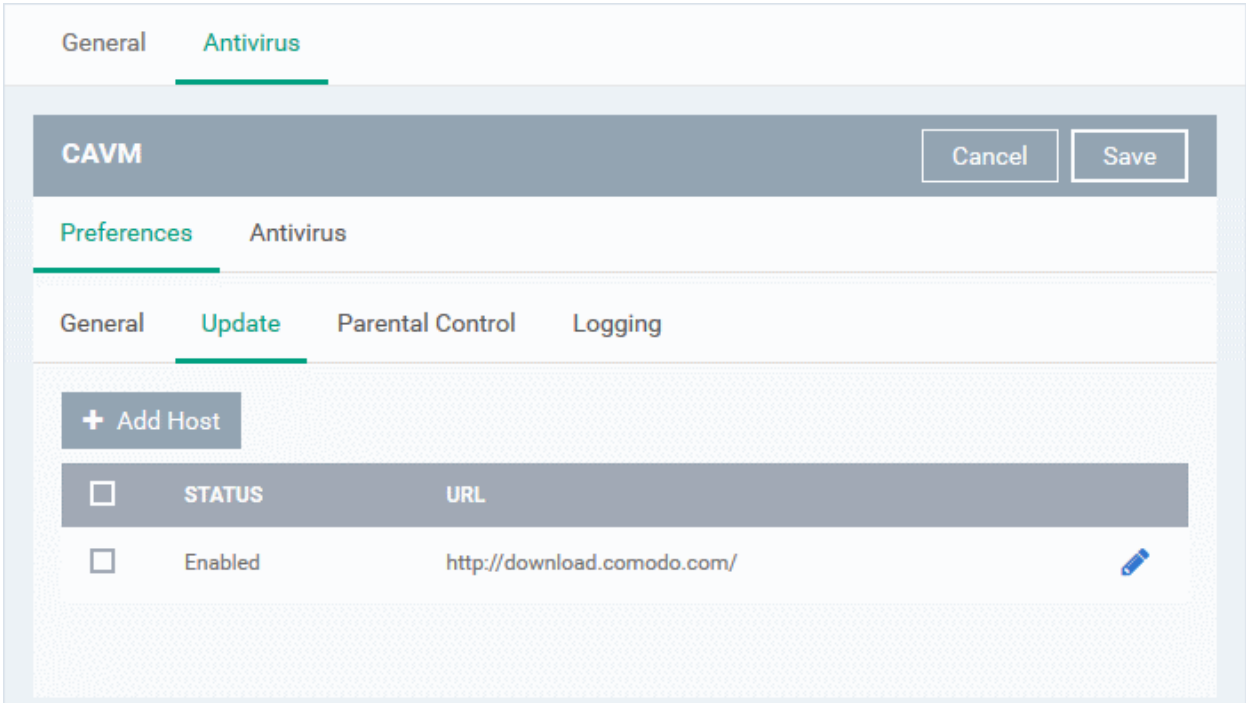
To configure general behavior settings

- Click the 'Preferences' tab under 'Antivirus' and choose 'General'
  - **Automatically check for program updates** - Choose whether or not CAVM should automatically contact Comodo servers for updates. With this option selected, CAVM automatically checks for updates every 24 hours AND every time the users start their computers. If updates are found, they are automatically downloaded and installed. (***Default = Enabled***).
  - **Show balloon messages** - If enabled, notifications from CAVM will appear in the bottom right hand corner of the computer screen - just above the tray icons. Usually these messages are generated when these modules are learning the activity of previously unknown components of trusted applications. (***Default = Disabled***).

To configure update settings

Tip: The Update tab allows you enable/disable CAV program updates and to select the host from which updates should be downloaded. By default, updates are downloaded from http://download.comodo.com

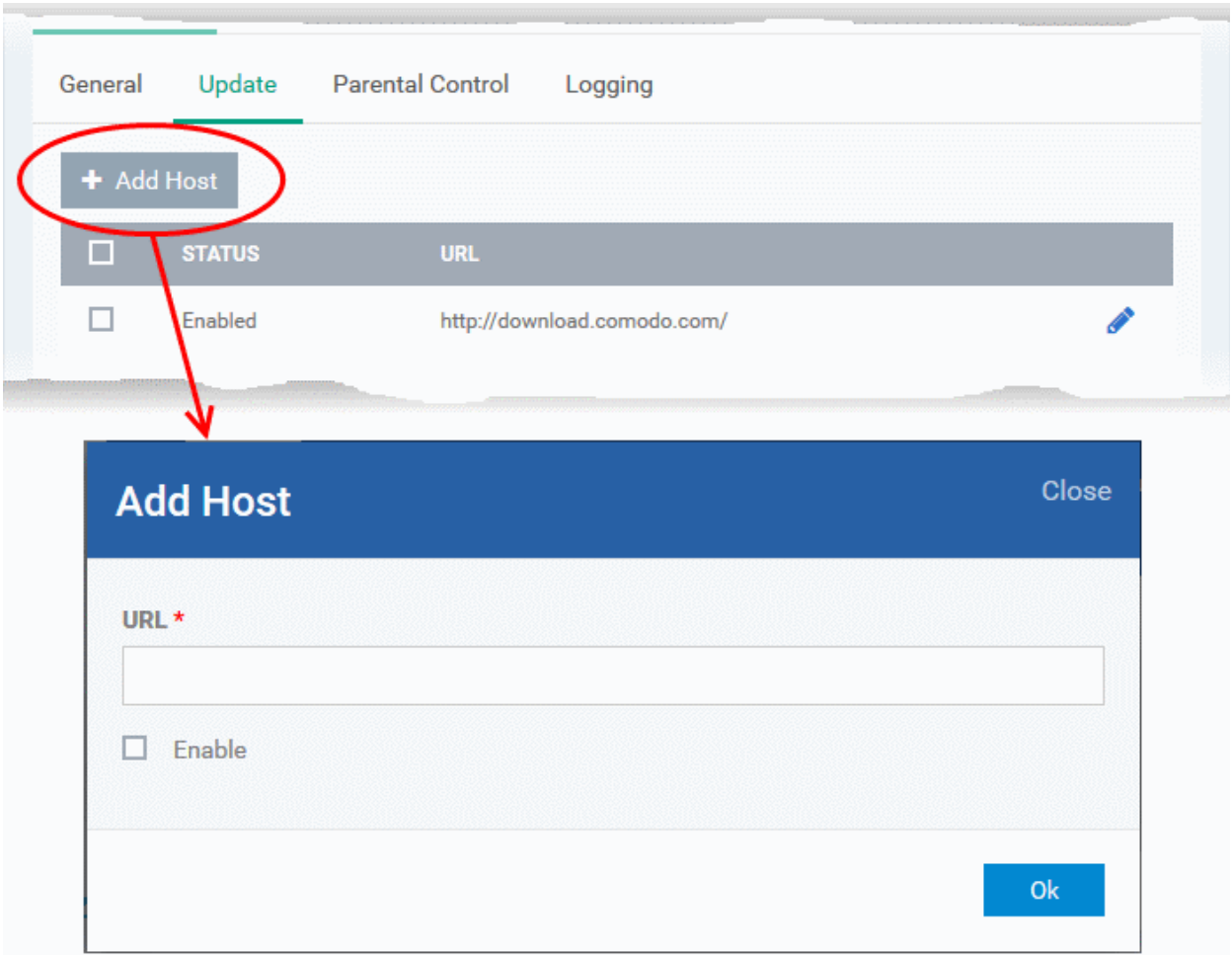
- Choose the 'Update' tab under 'Preferences'



- Leave this setting enabled if you want the devices to download the updates from Comodo servers

You can add the URL of an alternative download host if required. For example, if CAV updates are available on a server on the local network to which the device is connected.

- To add a host in the local network, click 'Add Host'

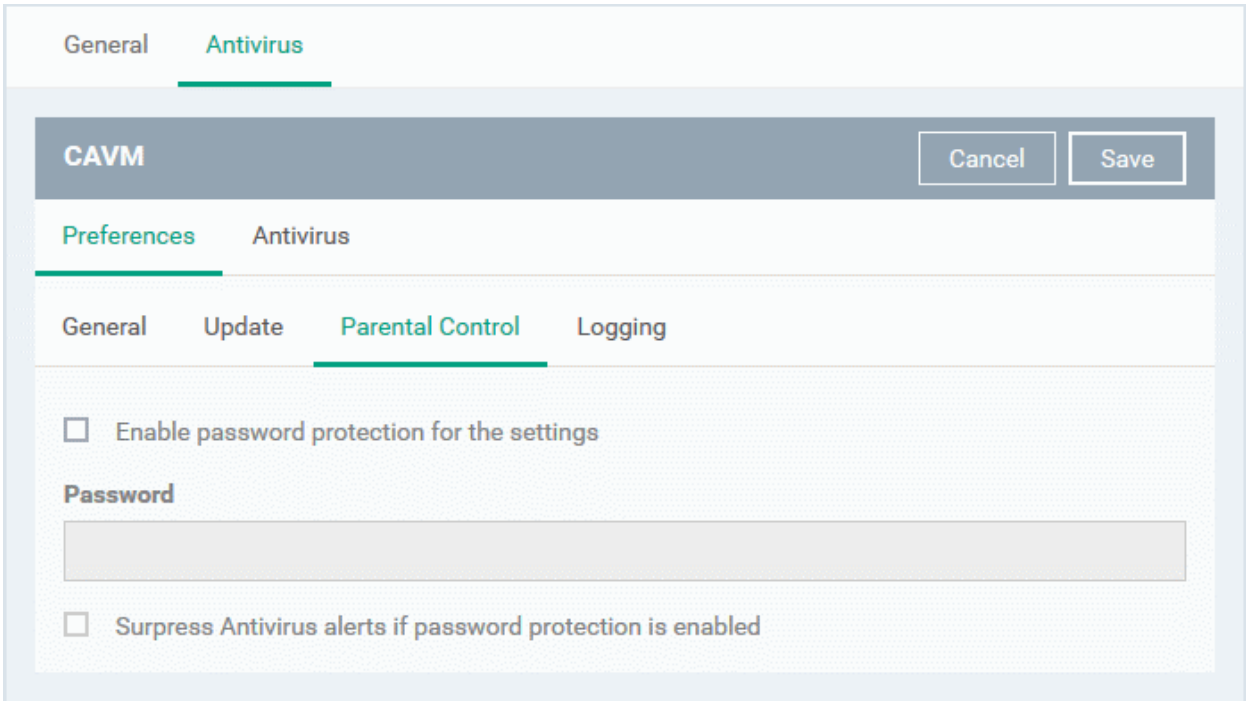


The 'Add Host' dialog will appear.

- Enter the URL or IP of the host from which updates should be downloaded in the 'URL' field
- Select the 'Enable' to activate the host
- Click 'Ok' to apply your changes
- Repeat the process to add multiple hosts.
- To edit a host, click the pencil icon beside the host name in the list

To configure Parental Control settings

- Click the 'Parental Control' tab under 'Preferences'

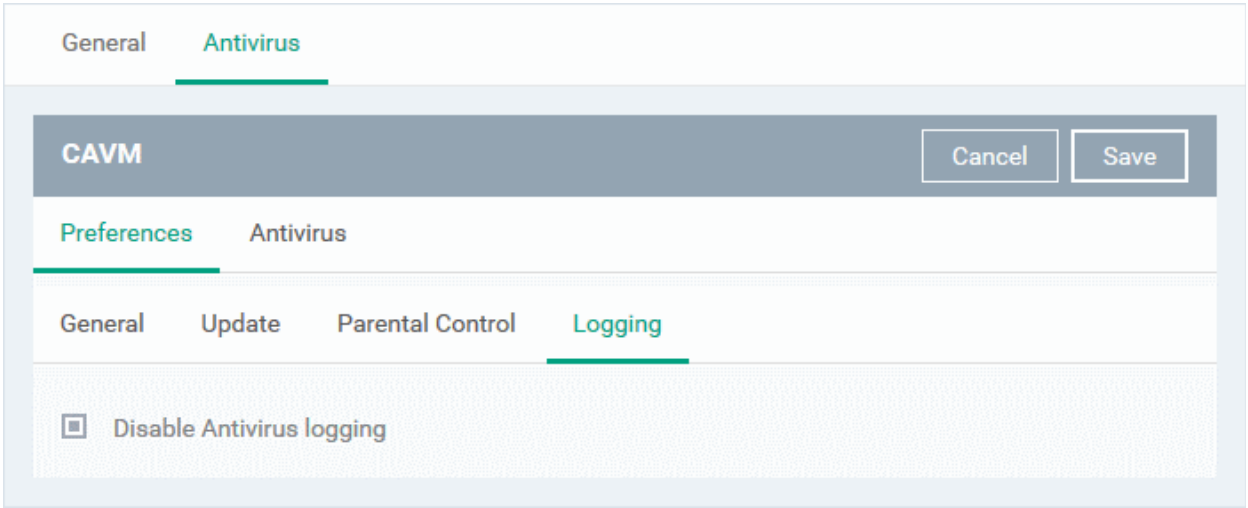


- **Enable password protection for the settings** - Activates password protection for all important CAVM settings against unauthorized changes by the user. If the user attempts to change a setting using the CAVM interface at the endpoint, he/she will be prompted to enter the password. If selected, enter the password in the 'Password' field.
- **Suppress Antivirus alerts if password protection is enabled** - If selected, any threat detected at the device will be automatically blocked but no Antivirus Alerts will be displayed. Select this option if you do not want users to be made aware when an Antivirus alert has been triggered.

  For example, a virus program may be attempting to copy itself and infect user's computer without permission or knowledge of the user. Usually, the Antivirus would generate an alert and ask the user how to proceed. If the user is inexperienced then they may click 'allow' just to get rid of the alert and/or gain access to the website in question - thus exposing the machine to attack

To configure 'Log' settings

- Click the 'Logging' tab under 'Preferences'



Comodo Antivirus can maintain a log of all antivirus (AV) events locally in the device. Users can view the logs by clicking 'View Antivirus Events' from the Antivirus Tasks interface of the CAVM interface.

- If you want the CAVM installation to not to maintain the logs locally, select 'Disable Antivirus

Logging'.

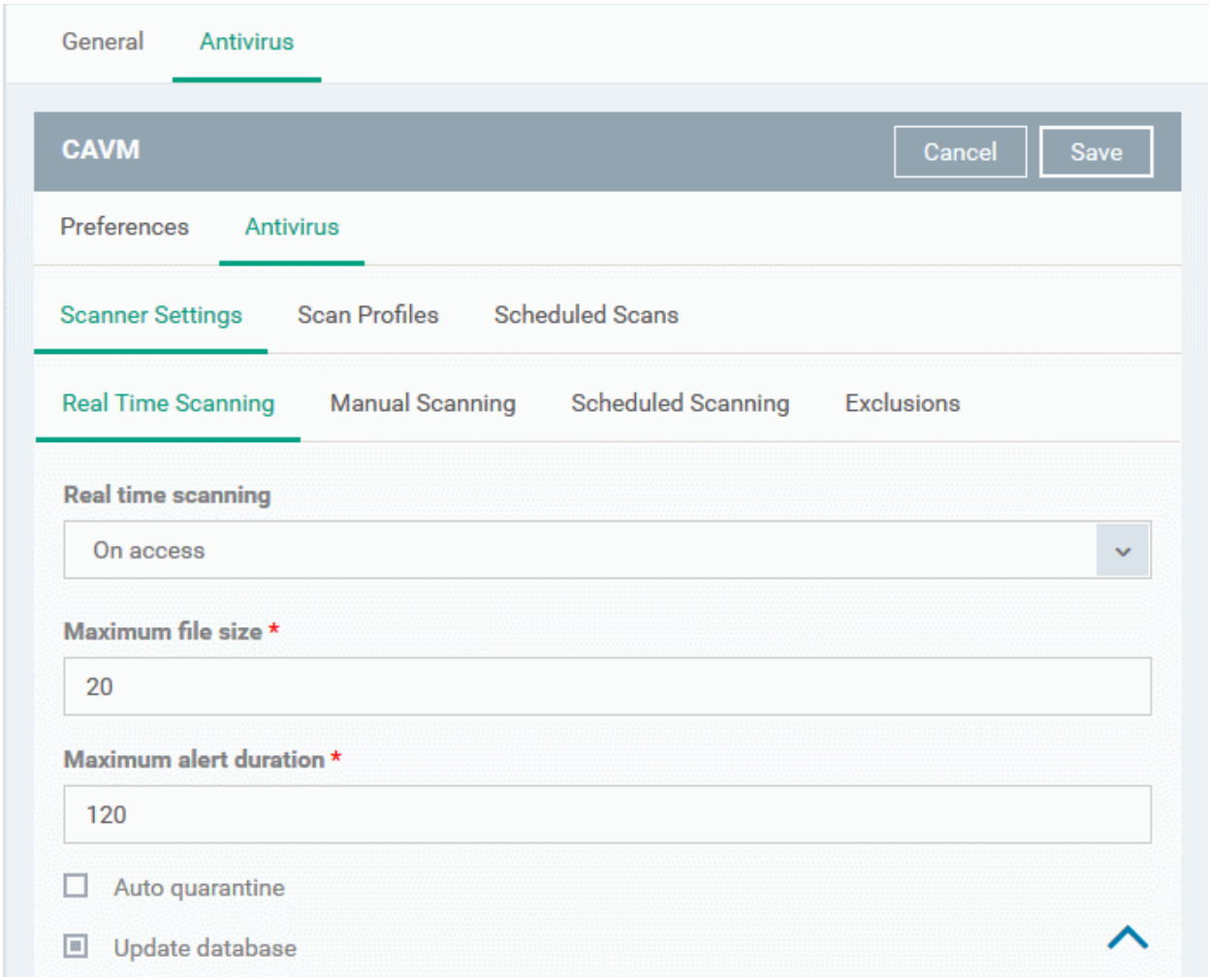
Configuring Antivirus Settings

The 'Antivirus' tab under the 'Antivirus' section allows you to configure the general settings for the AV scanner, scan profiles and create schedules to periodically run AV scans on selected areas of the device..

The 'Antivirus' interface contains three sub-tabs:

- Scanner Settings
- Scan Profiles
- Scheduled Scans

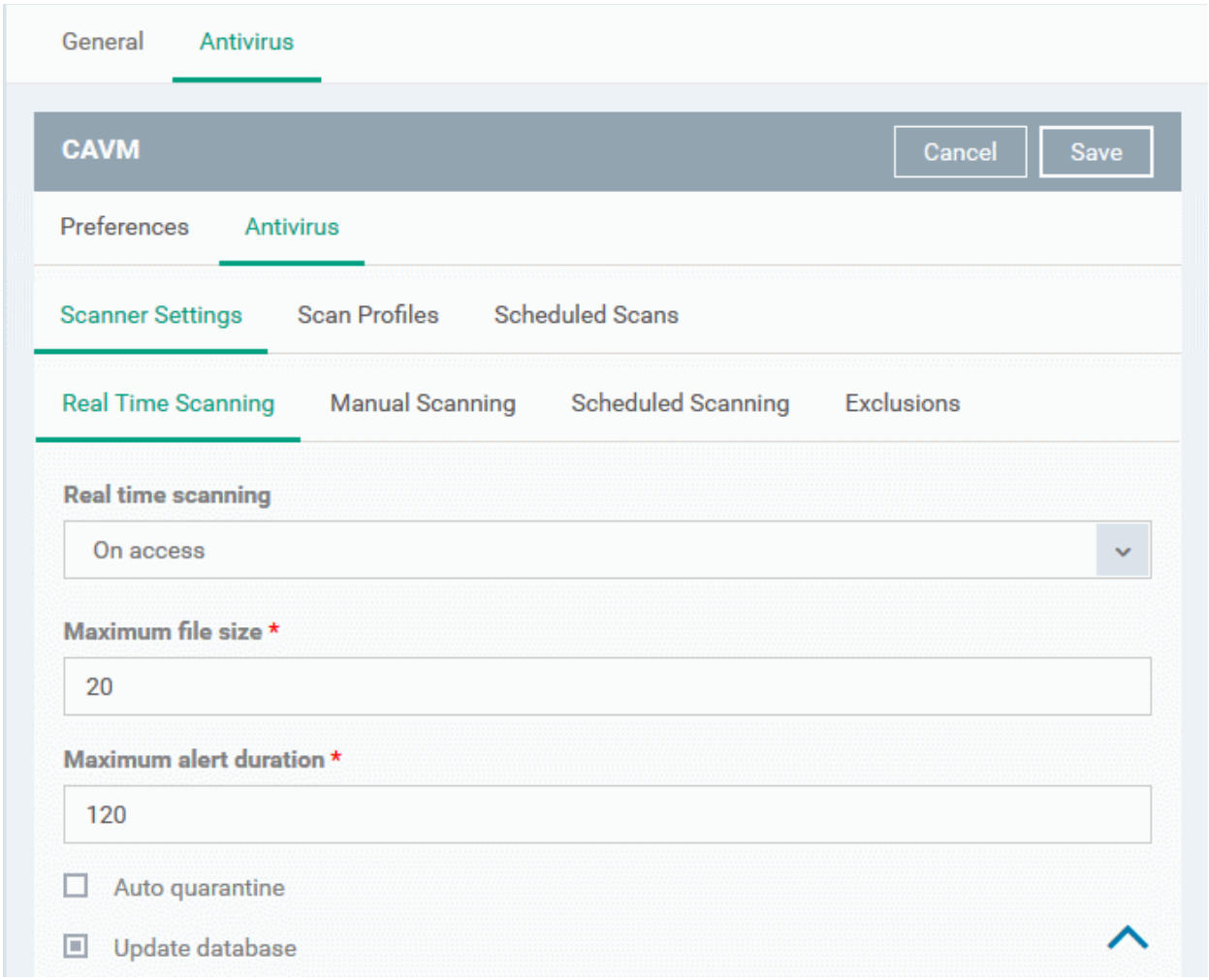
To configure Scanner Settings click the 'Scanner Settings' tab under Antivirus



You can configure the following from the Scanner Settings interface:

- Realtime Scanning
- Manual Scanning
- Scheduled Scanning
- Exclusions

- To configure Realtime Scanning Settings, click the 'Realtime Scanning' tab.

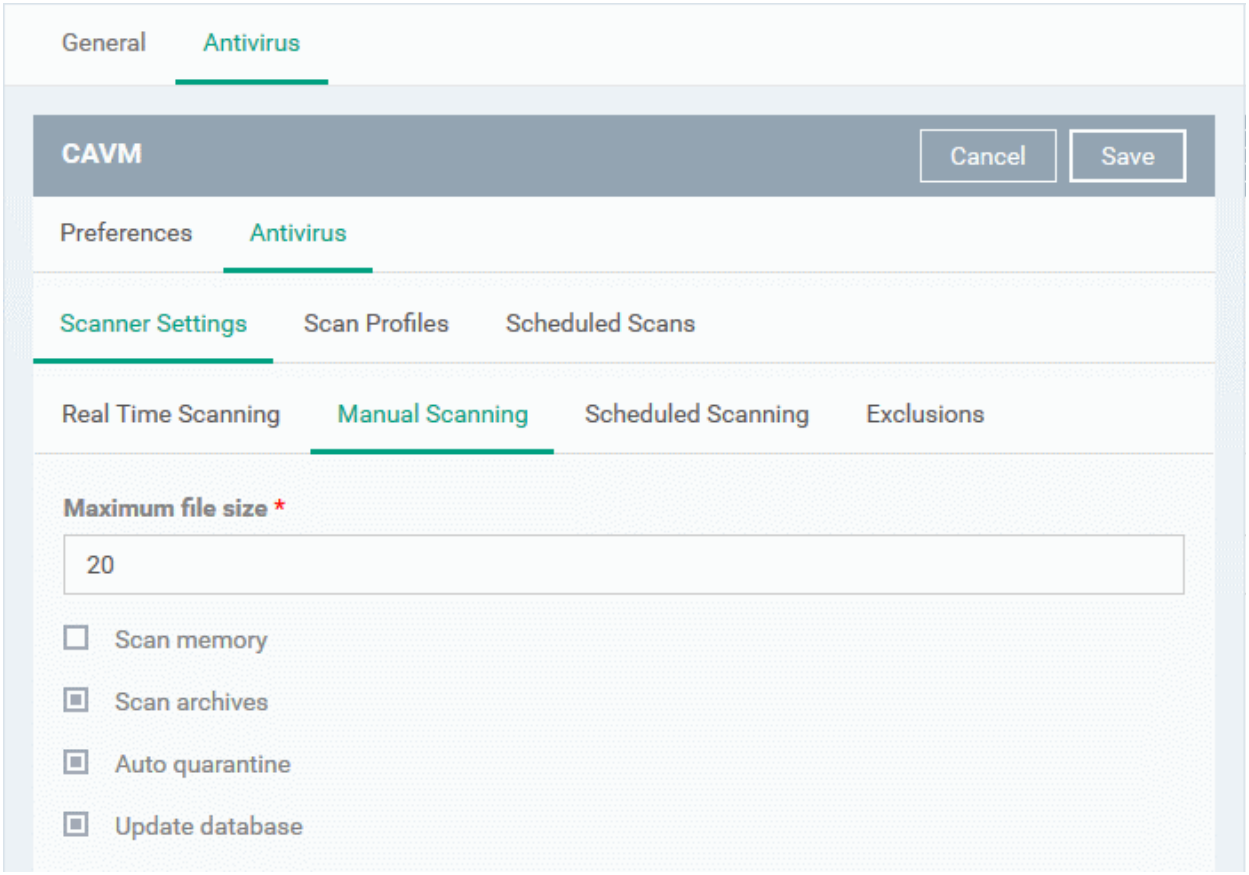


Real Time Scanning Settings - Table of Parameters		
Form Element	**Type**	**Description**
Real time scanning	Drop-down	Allows you to enable or disable realtime scanning. The available options are: • On Access - Provides the highest level of On Access Scanning and protection. Any file opened at the device is scanned before it is run and the threats are detected before they get a chance to be executed. • Disabled - The Real time scanning is disabled. Antivirus does not perform any scanning and the threats cannot be detected before they impart any harm to the system.
Maximum file size	Text box	Allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be scanned (***Default =20MB***).
Maximum alert duration	Text box	Allows you to set the time period (in seconds) for which the alert message should be displayed to the user. (***Default = 120 seconds***)

Real Time Scanning Settings - Table of Parameters		
Auto quarantine	Checkbox	When enabled, all detected threats will be moved to quarantine at the device for your later analysis. (*Default = Disabled*)
Update database	Checkbox	When enabled, Comodo Antivirus will check for and download the latest virus database updates on system start-up and subsequently at regular intervals. (*Default = Enabled*).

- To configure Manual Scanning Settings, click the 'Manual Scanning' tab.

Tip: The Manual Scanning Settings interface allows you to set the parameters that will be implemented when you run an 'On Demand' scan on selected devices from the Protection > Device List interface. For more details on running on-demand scans on selected devices, refer to the section **Running On-Demand Antivirus Scans on Devices**.

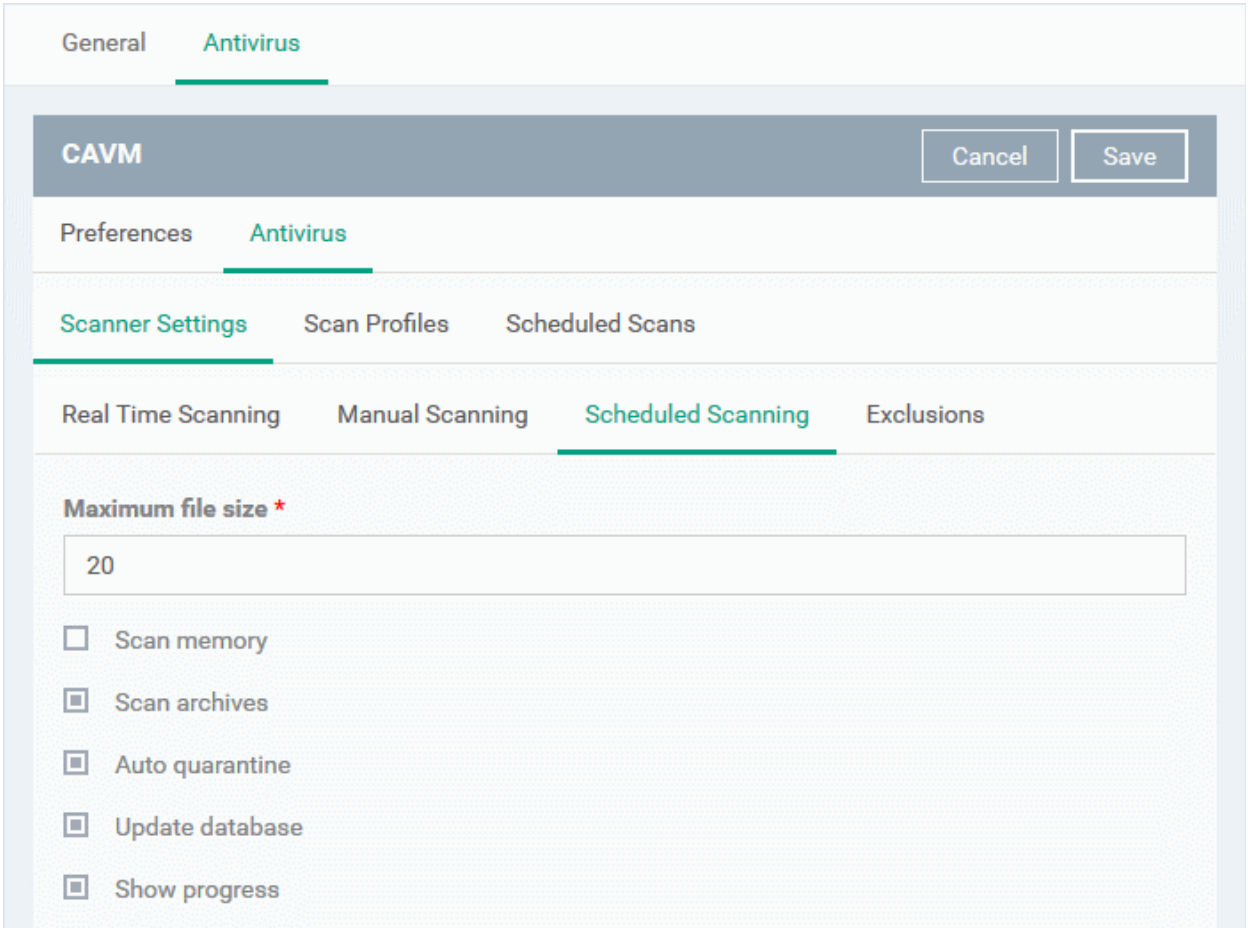


Manual Scanning Settings - Table of Parameters		
Form Element	**Type**	**Description**
Maximum file size	Text box	Allows you to set a maximum size (in MB) for the individual files to be scanned during on-demand scanning. Files larger than the size specified here, will not be scanned (*Default =20MB*).
Scan memory	Checkbox	When this check box is selected, CAVM scans the system memory at the start of each manual scan (*Default = Disabled*).
Scan archives	Checkbox	When this check box is selected, CAVM scans archive files such as .ZIP and .RAR files. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (*Default =*

Manual Scanning Settings - Table of Parameters		
		Enabled).
Auto quarantine	Checkbox	When enabled, all detected threats will be moved to quarantine at the device for your later analysis. (*Default = Enabled*)
Update database	Checkbox	Instructs CAVM to check for latest virus database updates and download the updates automatically before starting each on-demand scan (*Default = Enabled*).

- To configure Scheduled Scanning Settings, click the 'Scheduled Scanning' tab under 'Scanner Settings'

Tip: The 'Scheduled Scanning' Settings interface allows you to set the parameters that will be implemented when CAVM runs AV scans as per schedules set under the 'Scheduled Scans' tab. For more details on creating periodical scan schedules, refer to the explanation under 'To create Scheduled Scans'.

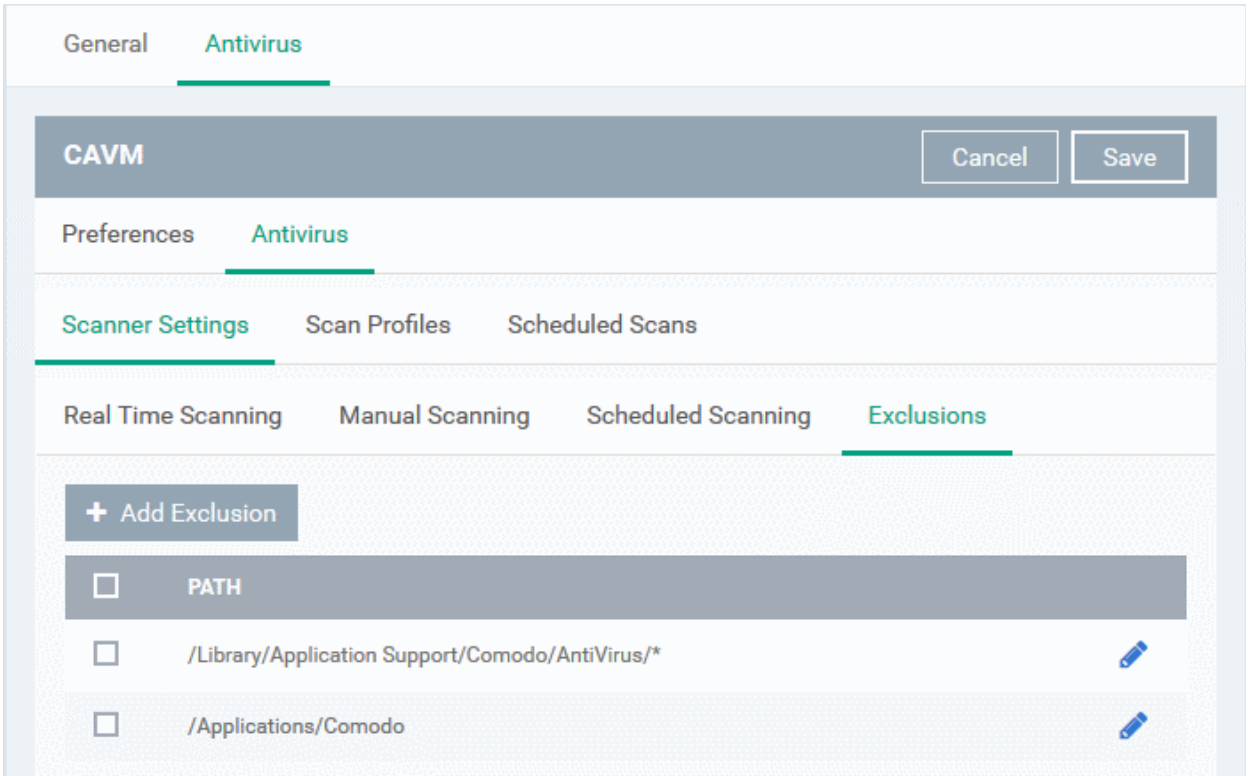


Scheduled Scanning Settings - Table of Parameters		
Form Element	**Type**	**Description**
Maximum file size	Text box	Allows you to set a maximum size (in MB) for the individual files to be scanned during scheduled scanning. Files larger than the size specified here, will not be scanned (*Default =20MB*).

Scheduled Scanning Settings - Table of Parameters		
Scan memory	Checkbox	When this check box is selected, CAVM scans the system memory at the start of each scheduled scan (***Default = Disabled***).
Scan archives	Checkbox	When this check box is selected, CAVM scans archive files such as .ZIP and .RAR files. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***).
Auto quarantine	Checkbox	When enabled, all detected threats will be moved to quarantine at the device for your later analysis. (***Default = Enabled***)
Update database	Checkbox	Instructs CAVM to check for latest virus database updates and download the updates automatically before starting each on-demand scan (***Default = Enabled***).
Show Progress	Checkbox	When enabled, a progress bar is displayed whenever a scheduled scan is run at the device. (***Default = Enabled***)

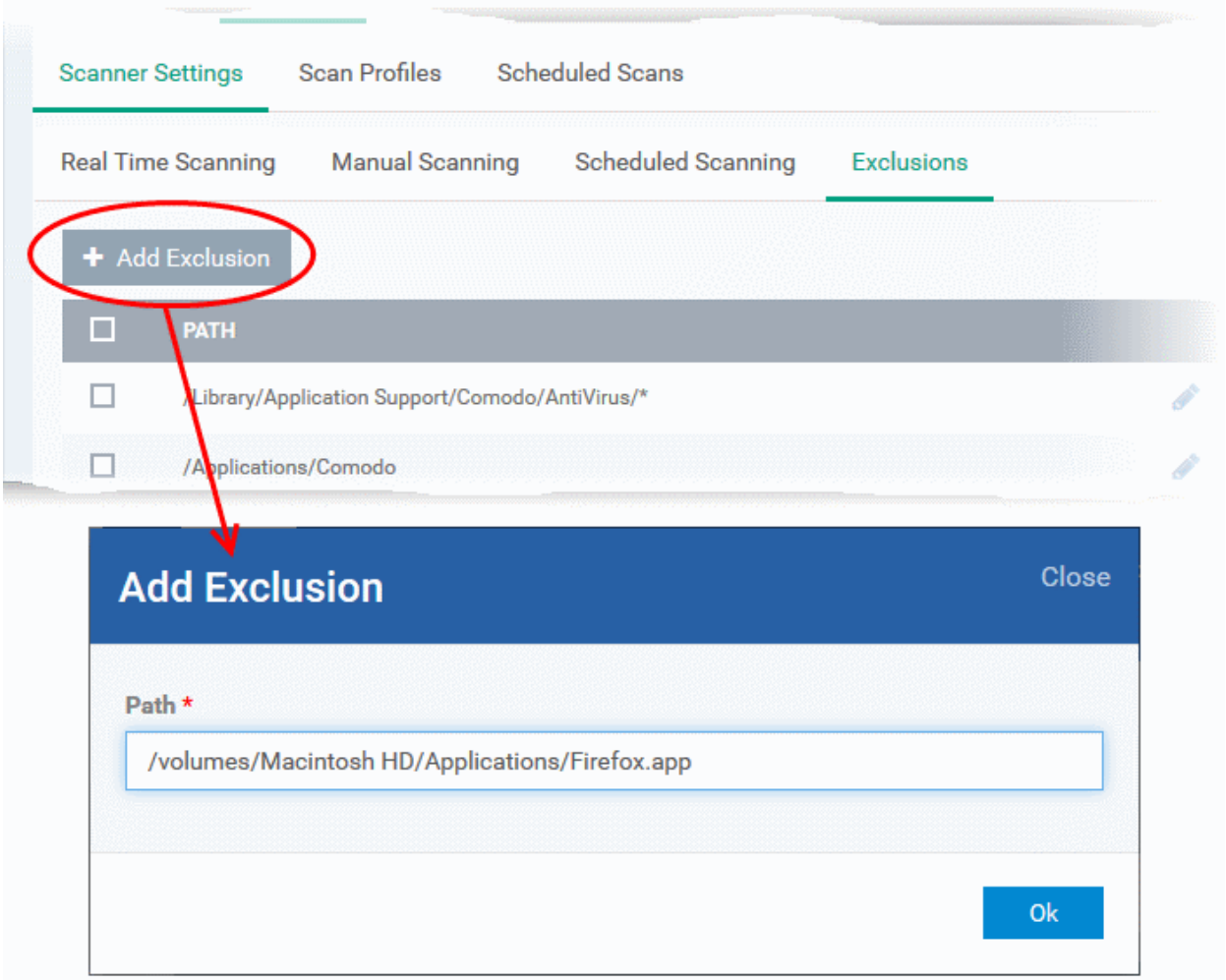
- To add items to be excluded from scanning, click 'Exclusions' under 'Scanner Settings'

Tip: The 'Exclusions' Settings interface allows you to specify the items that should be excluded by the AV scanner. These files will be skipped during realtime, on-demand and scheduled scans.



A list of excluded items will be displayed.

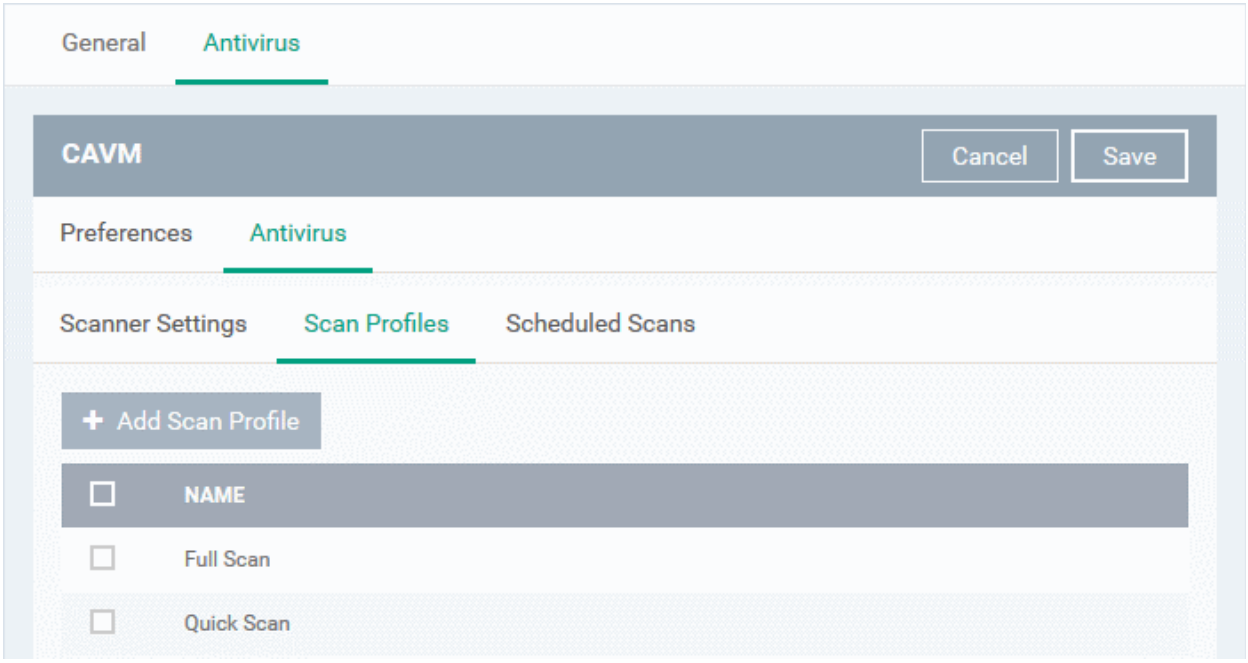
- Click 'Add Exclusion'



- Enter the location of the item to be excluded in the 'Path' field and click 'Ok'
- Repeat the process to add more items
- To edit the path of an item, click the pencil icon beside it

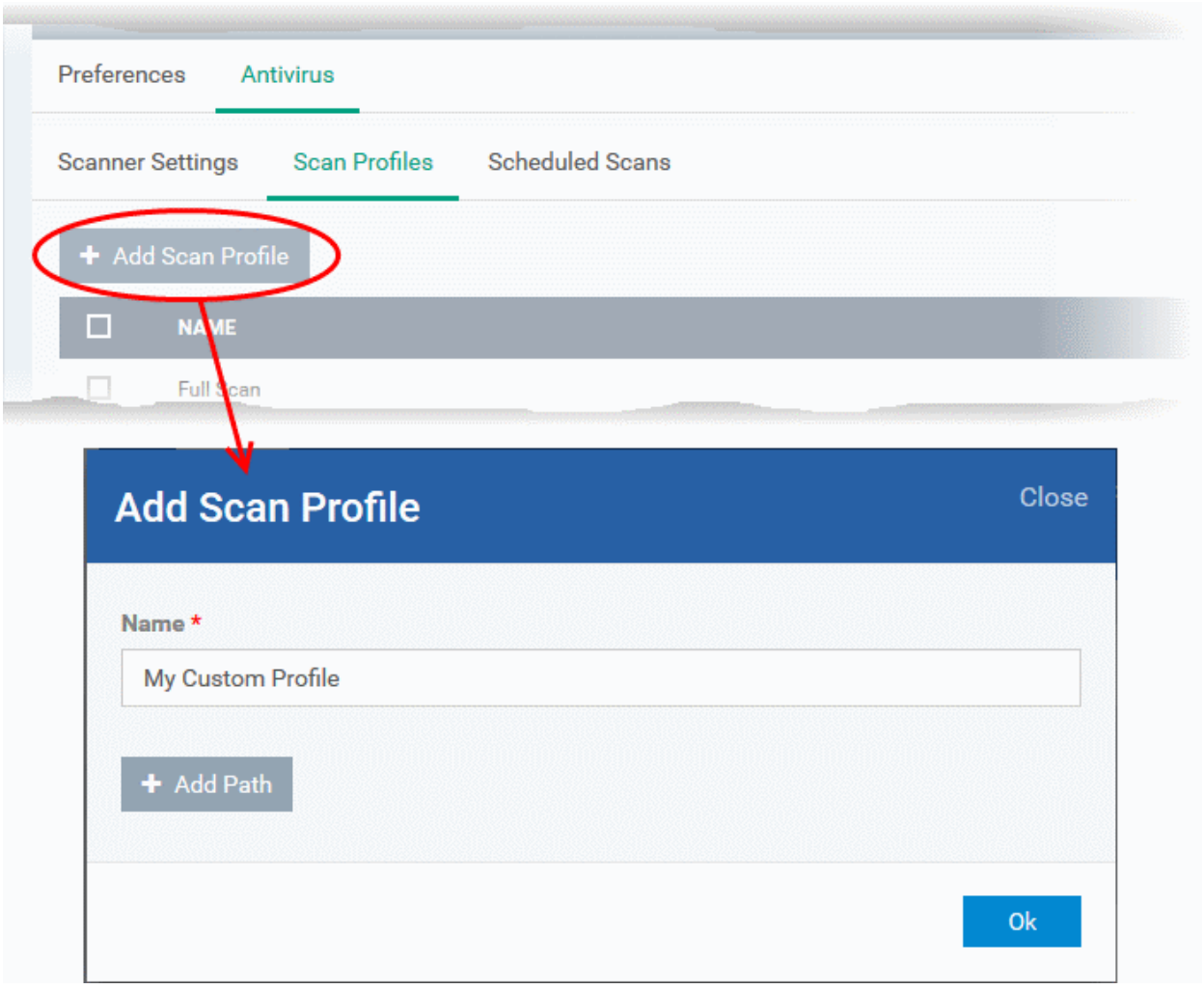
To create Scan Profiles click the 'Scan Profiles' tab under 'Antivirus'

Tip: Creating a Scan Profile allows you to instruct CAVM to scan selected areas, folders or selected drives of the device to which the profile is applied. You can select the scan profiles while creating scan scheduled scans and while running on-demand scans on the device applied with the profile.



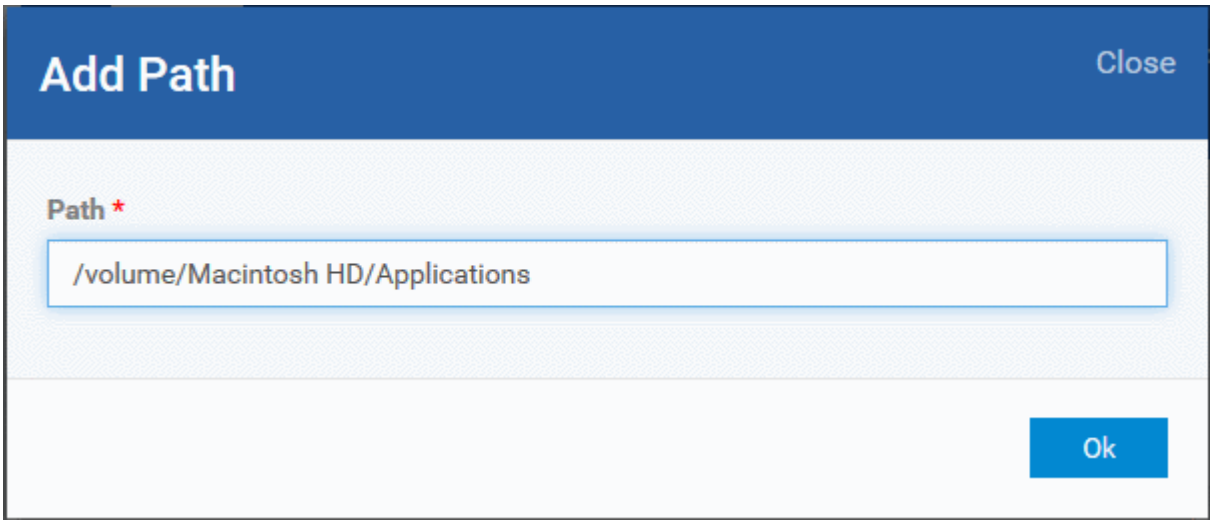
The list of pre-defined scan profiles will be displayed.

- Click 'Add Scan Profile'



The 'Add Scan Profile' dialog will appear.

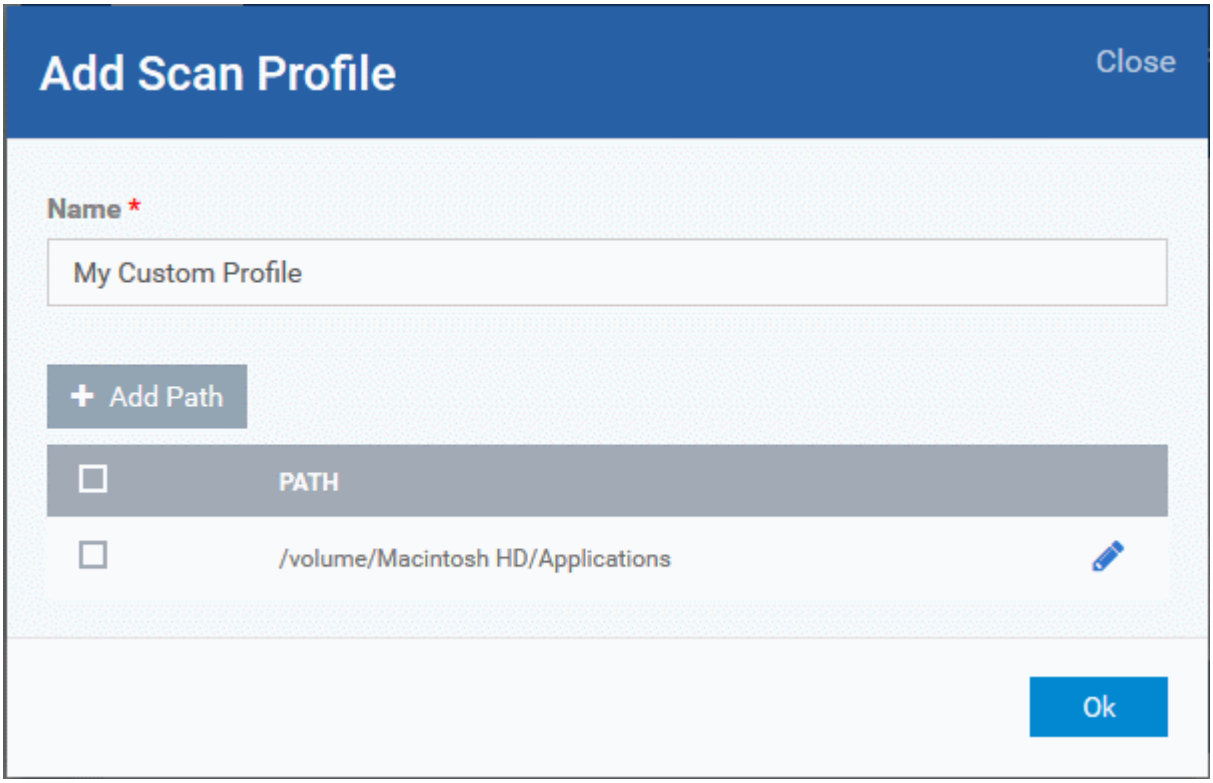
- Enter a name for the scan profile
- Click 'Add Path' to add the locations to be scanned as per the custom profile



The 'Add Path' dialog will appear.

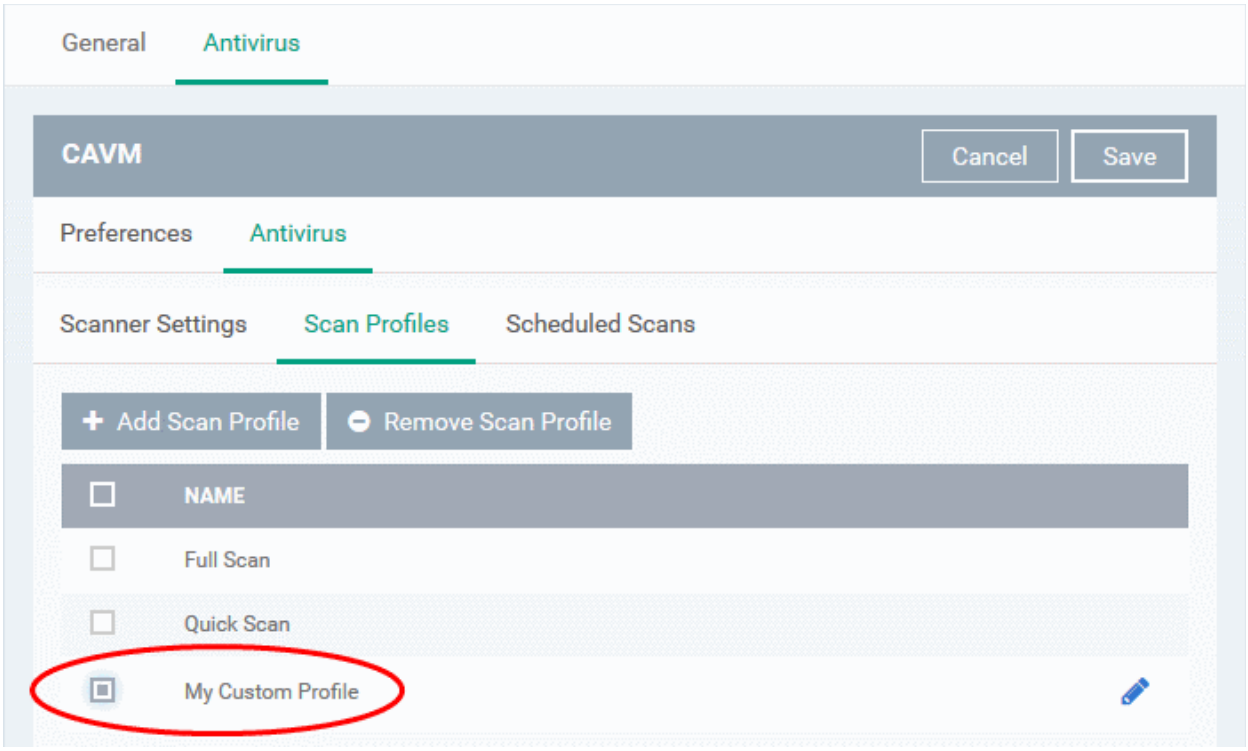
- Enter the path of the location to be scanned as per the custom profile and click 'Ok'

The path will be added to the profile.



- To add more paths, click 'Add Path' and repeat the process
- To edit the path, click the pencil icon beside it
- Click 'Ok' in the 'Add Scan Profile' dialog.

- The profile will be added to the list of 'Scan Profiles'.



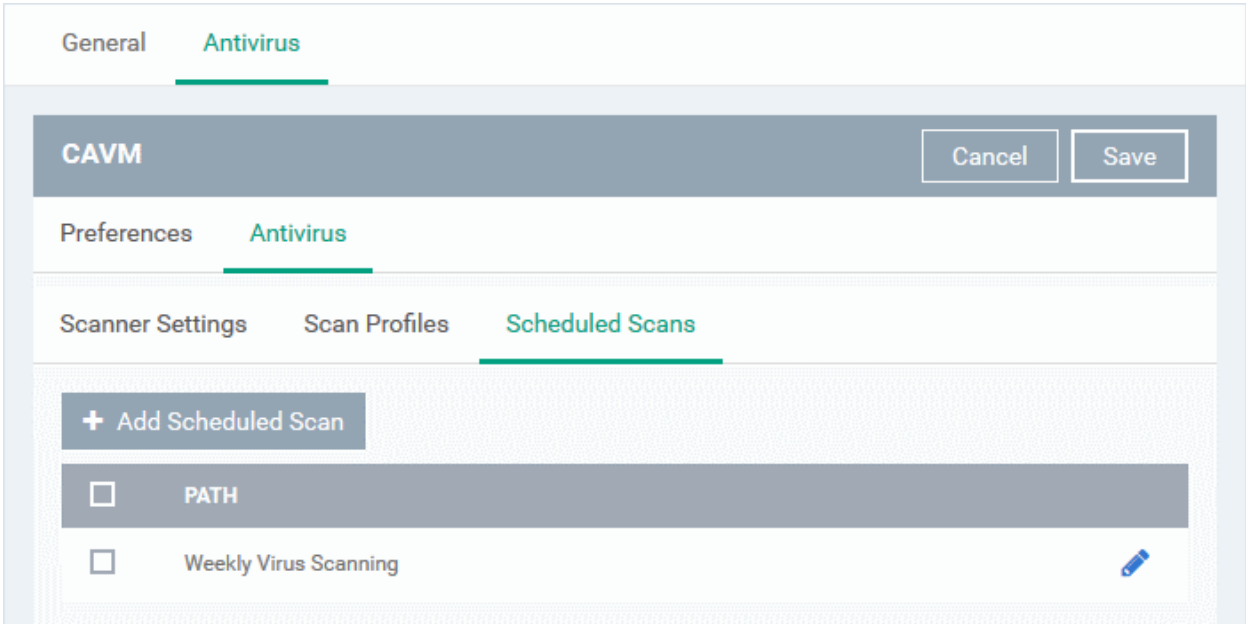
The custom profile will be added to the list.

- To add more custom scan profiles, click 'Add Scan Profile' and repeat the process
- To edit a custom scan profile, click the pencil icon beside it
- To remove a custom scan profile, select it and click 'Remove Scan Profile'.

To create Scheduled Scans, click the 'Scheduled Scans' tab under 'Antivirus'

Tip: The highly customizable scan scheduler that lets you timetable scans to be run on managed devices according to your preferences. CAVM automatically starts scanning the entire system or the disks or folders contained in the profile selected for that scan.

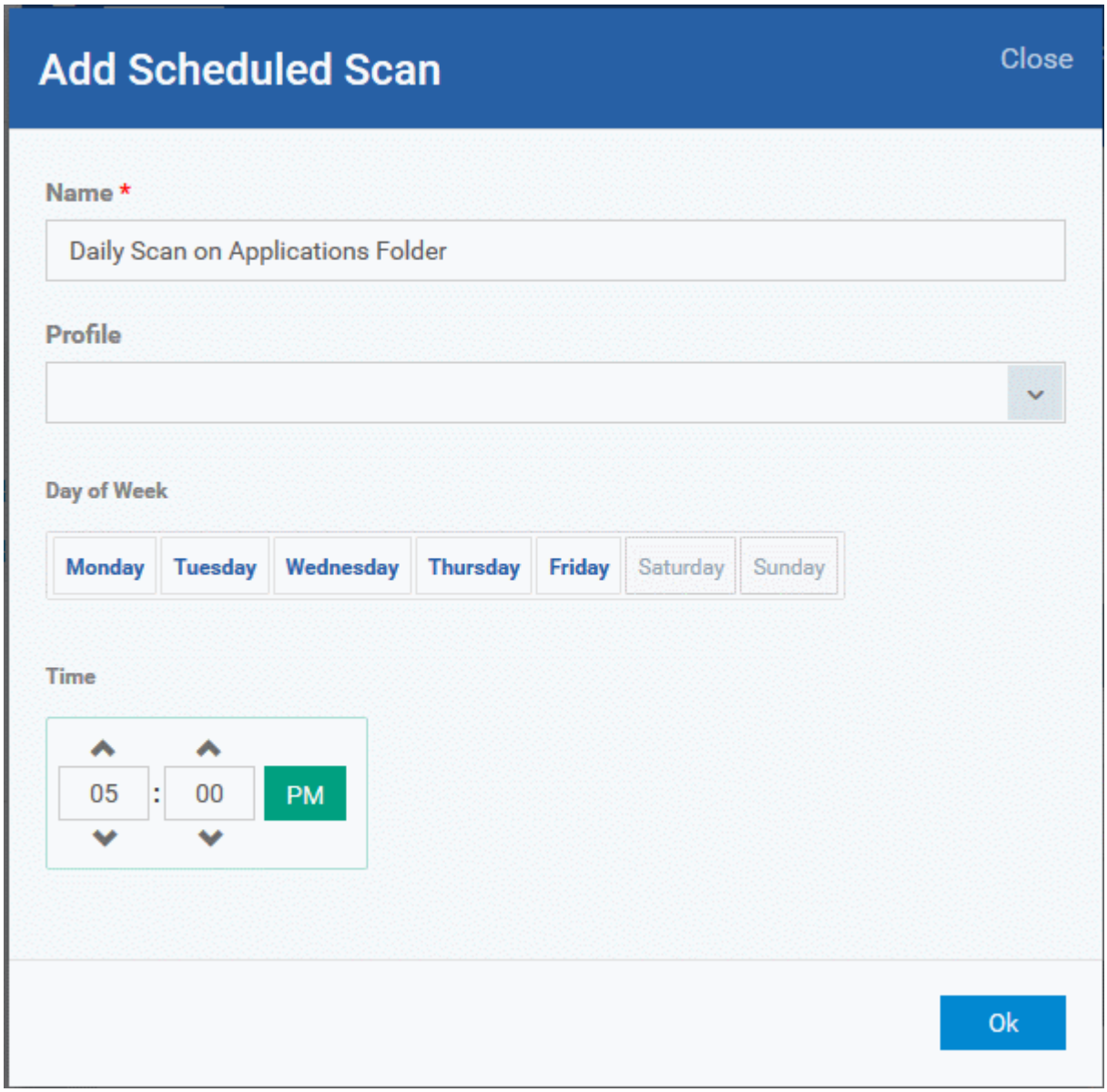
You can add any number of scheduled scans for a profile to run at a time that suits your preference. A scheduled scan may contain any profile of your choice.



A list of pre-configured scheduled scans will be displayed.

- To add a new scheduled scan click Add 'Scheduled Scan'

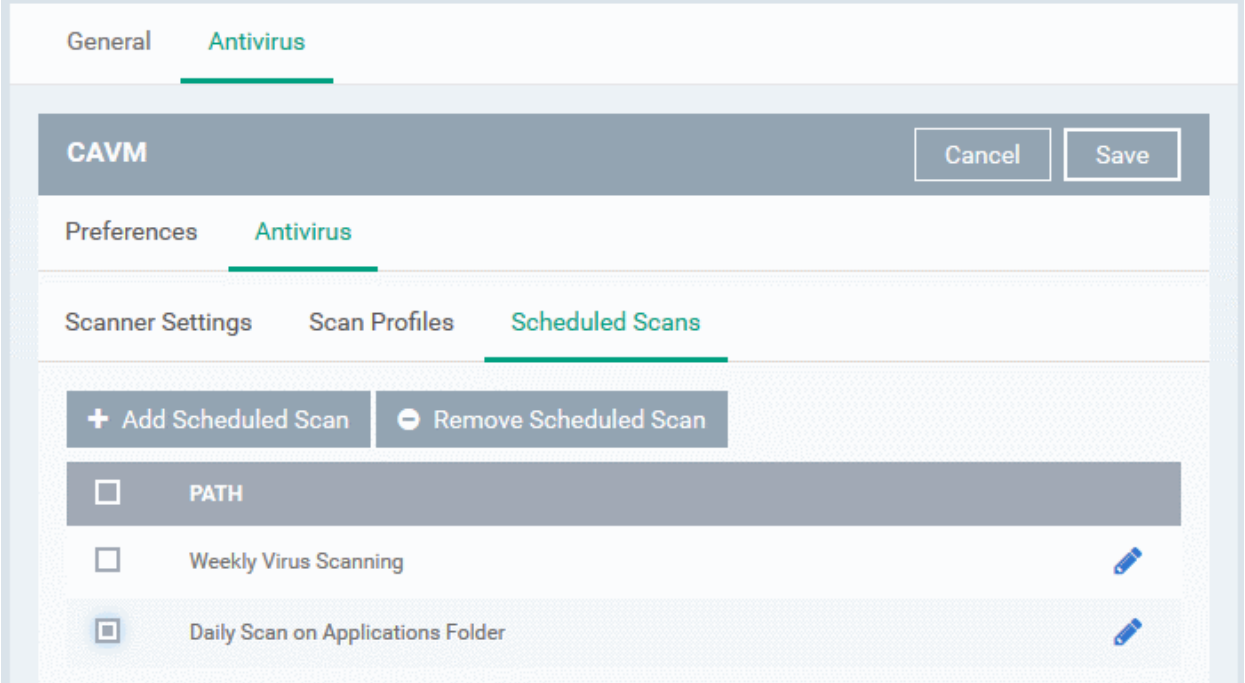
The 'Add Scheduled Scan' dialog will appear.



Add Scheduled Scan - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text box	Enter a name for the scheduled scan
Profile	Drop-down	Choose the pre-defined or custom scan profile to be applied for the scheduled scan. The scan profiles included under the 'Scan Profiles' tab will be available in the drop-down.
Day of the Week	Buttons	Select the day(s) of the week on which the scan has to run
Time	HH:MM drop-down combo boxes	Set the time at which the scans are to run on the selected days.

- Click 'Ok'

The scheduled scan will be added to the list.



- To add more scheduled scans to the configuration profile, click 'Add Scheduled Scan' and repeat the process
- To edit the settings of a scheduled scan, click the pencil icon beside it
- To remove a scheduled scan, select it and click 'Remove Scheduled Scan'

- Click 'Save' for your settings to take effect for the profile.

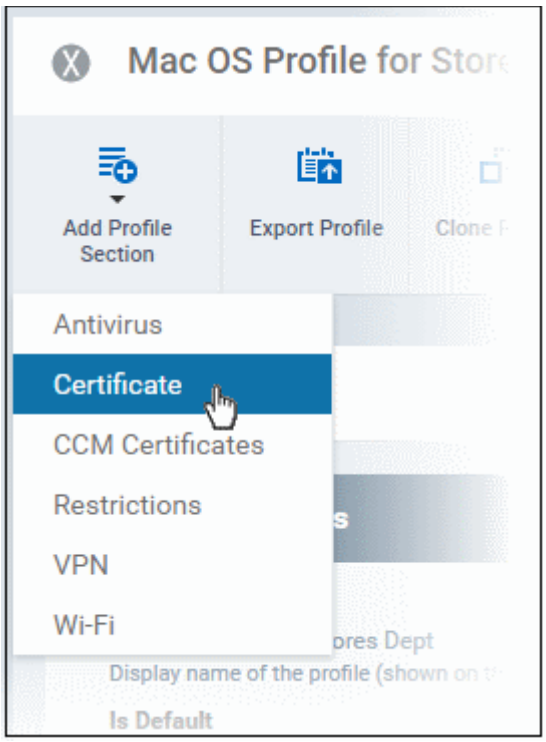
The settings will be saved and displayed under the 'Antivirus' tab. You can edit the settings or remove the section at anytime. Refer to the section Editing Configuration Profiles for more details.

6.1.4.1.2. Certificate Settings for OS X Profile

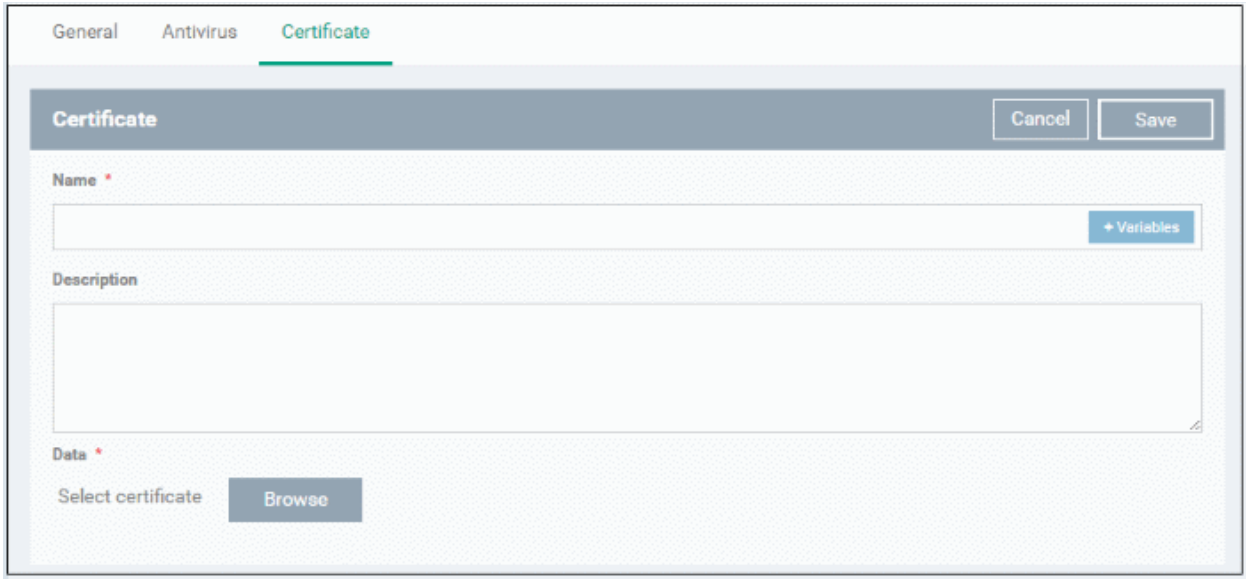
The 'Certificate Settings' section is used to upload certificates that can be selected for use in other settings such as 'Wi-Fi, 'Exchange Active Sync', 'VPN' and so on. You can also enroll user or device certificates from Comodo Certificate Manager (CCM) after activating your CCM account under Settings > Portal Set-Up > Certificates Activation.

To configure Certificate settings for OS X profile

- Choose 'Certificate' from the 'Add Profile Section' drop-down



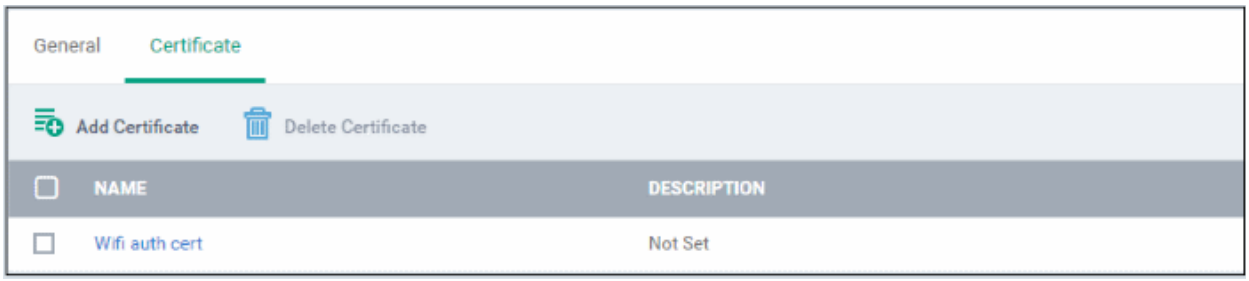
The 'Certificate' settings screen will be displayed.



Certificate Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter the name of the certificate. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Description	Text Field	Enter an appropriate description for the certificate.
Data	Browse button	Browse and upload the required certificate. Only certificate files with extensions 'pub', 'crt' or 'key' can be uploaded.

- Click the 'Save' button.

The certificate will be added to the certificate store.



- To add more certificates, click 'Add Certificate' and repeat the process.
- To view the certificate key and edit the name, click on the name of the certificate
- To remove an unwanted certificate, select it and click 'Delete Certificate'

You can add any number of certificates to the profile and remove certificates at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.4.1.3. CCM Certificate Settings for OS X Profile

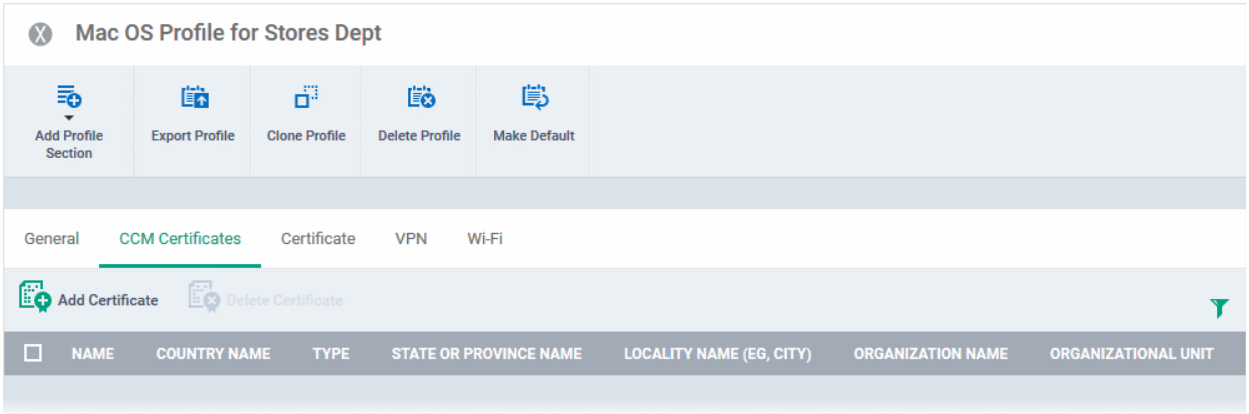
The Certificates Settings section of a profile allows you to create requests for client and device authentication certificates. Both types of certificate are issued by Comodo Certificate Manager (CCM). Once the profile is applied to a device, a certificate request is generated and forwarded by the client to CCM. After issuance, CCM will send the certificate to ITSM which in turn pushes it to the device for installation by the agent. You can add any number of certificates to a single profile.

In addition to user authentication, client certificates can also be used for email signing and encryption (users will need to import the certificate to their email client).

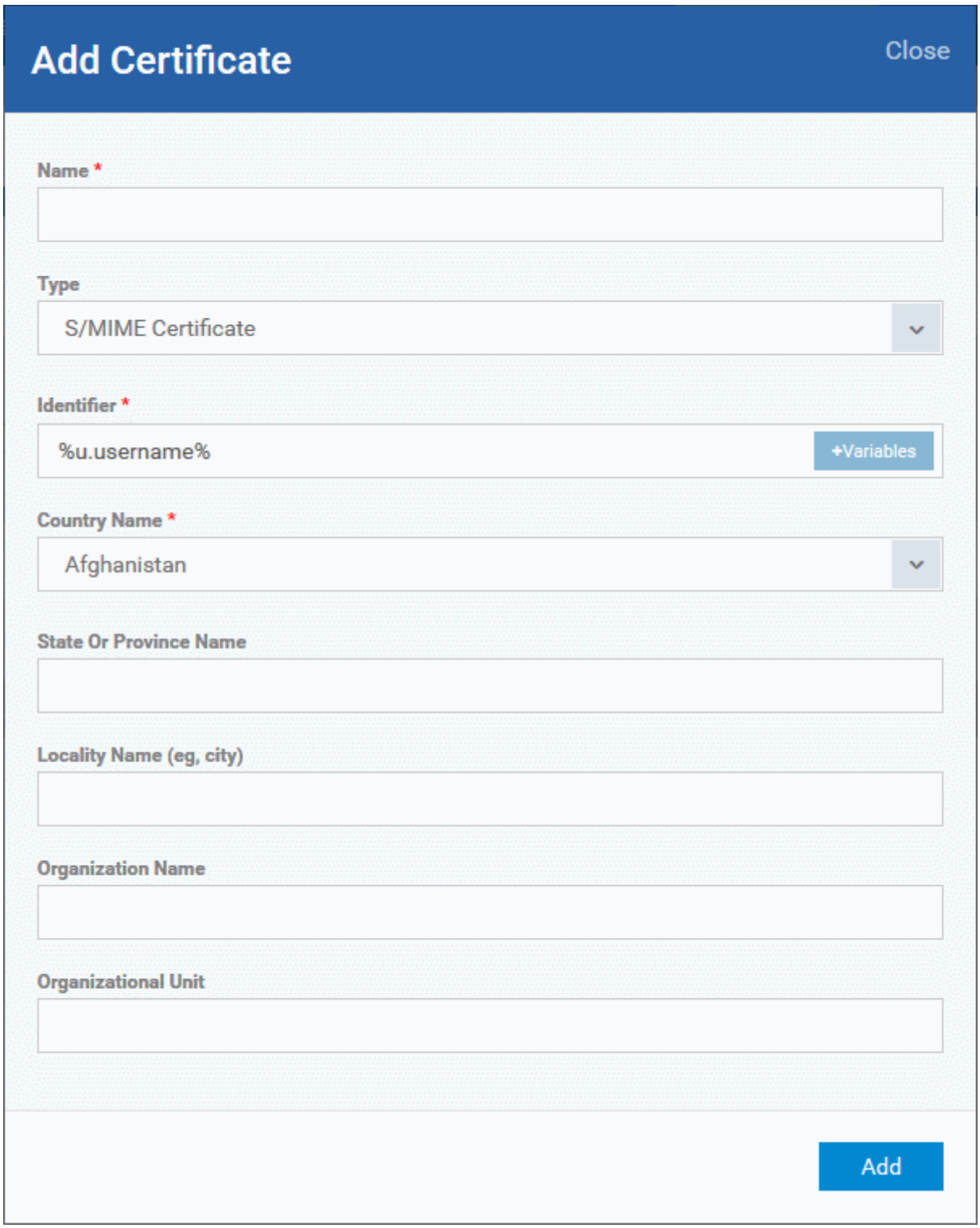
Prerequisite: Your CCM account should have been integrated to your ITSM server in order for ITSM to forward requests to CCM. For more details, refer to the section **Integrating with Comodo Certificate Manager.**

To add a client or device certificate

- Choose 'CCM Certificates' from the 'Add Profile Section' drop-down
- Click 'Add Certificate' to add a certificate request to the profile



The 'Add Certificate' form will appear:



Add Certificate - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Enter a name for the certificate to be requested, shortly describing its purpose.
Type	Drop-down	Select the type of certificate to be added. The available options are: • S/MIME Certificate (Client Certificate)

Add Certificate - Table of Parameters		
		• Device Certificate
Identifier	Text Field	The identifier field will be auto-populated with the variables depending on the chosen certificate type. • For client certificates, %username% will be added for fetching the username to be included as subject in the certificate request. • For device certificates, %d.uuid% will be added for fetching the device name to be included as subject in the certificate request. Also, you can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.
Country Name	Text Field	Enter the address details of the user/organization in appropriate fields.
State or Province Name		
Locality Name (eg. City)		
Organization Name	Text Field	Enter the name of the organization to which the user/device pertains. Prerequisite: The organization should have been added to your CCM account.
Organizational Unit	Text Field	Enter the name of the department to which the user/device pertains. Prerequisite: The department should have been defined under the organization in your CCM account.

- After completing the form, click 'Add' to include the certificate request in the profile.
- Repeat the process to add more certificate requests

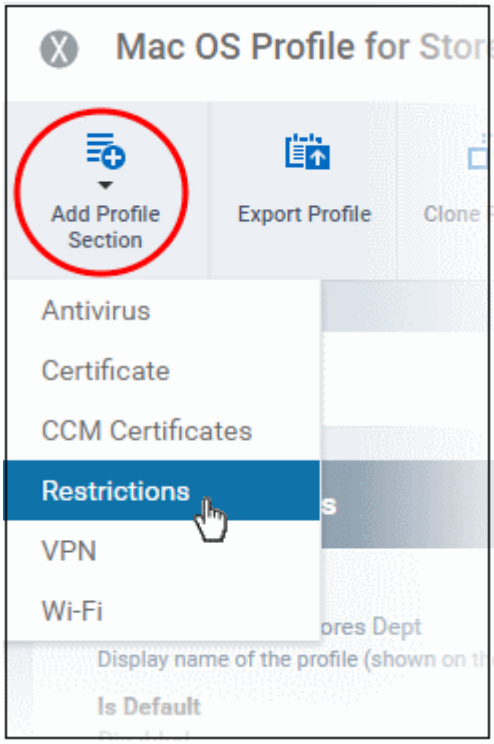
Certificate requests will be generated on the devices once the profile is applied to them.

6.1.4.1.4. Restrictions Settings for OS X Profile

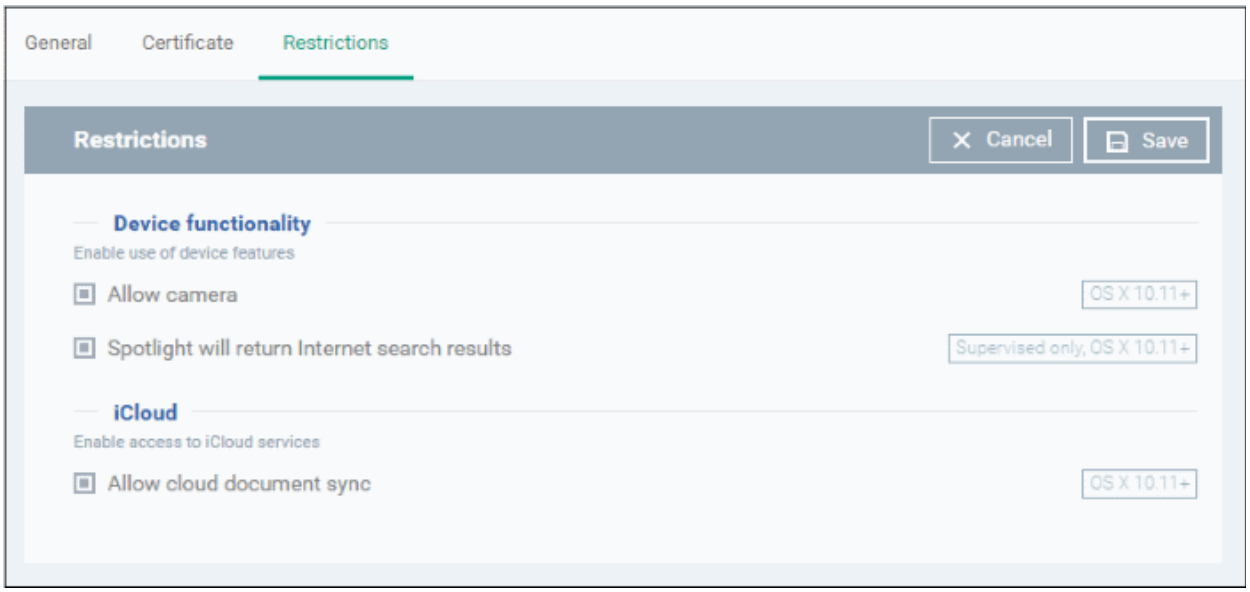
The 'Restrictions' section allows you to modify the profile to enable or disable selected device features:

To configure Restrictions settings

- Click 'Restrictions' from the 'Add Profile Section' drop-down



The 'Restrictions' settings screen will be displayed.



Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Device Functionality		
Allow Camera	Checkbox	Allows the user to take photos or videos (if enabled). If left unchecked, the camera icon is removed from the device and camera is disabled. Note: This feature is applicable only for OS X 10.11 and later versions.
Spotlight will return Internet search results	Checkbox	If enabled, the spotlight features will provide suggestions from the Internet, iTunes, and the App Store for the user to quickly find any file,

Restrictions Settings - Table of Parameters		
		documents, emails, apps contacts and more on the device. Note: This feature is applicable only for Supervised devices with OS X 10.11 and later versions.
iCloud		
Allow cloud document sync	Checkbox	If enabled, users can synchronize documents on their device with iCloud. Note: This feature is applicable only for OS X 10.11 and later versions.

- Click the 'Save' button.

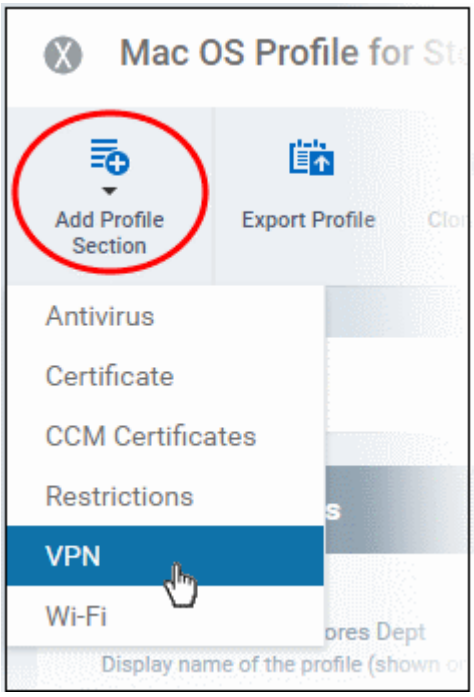
The saved 'Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.4.1.5. VPN Settings for OS X Profile

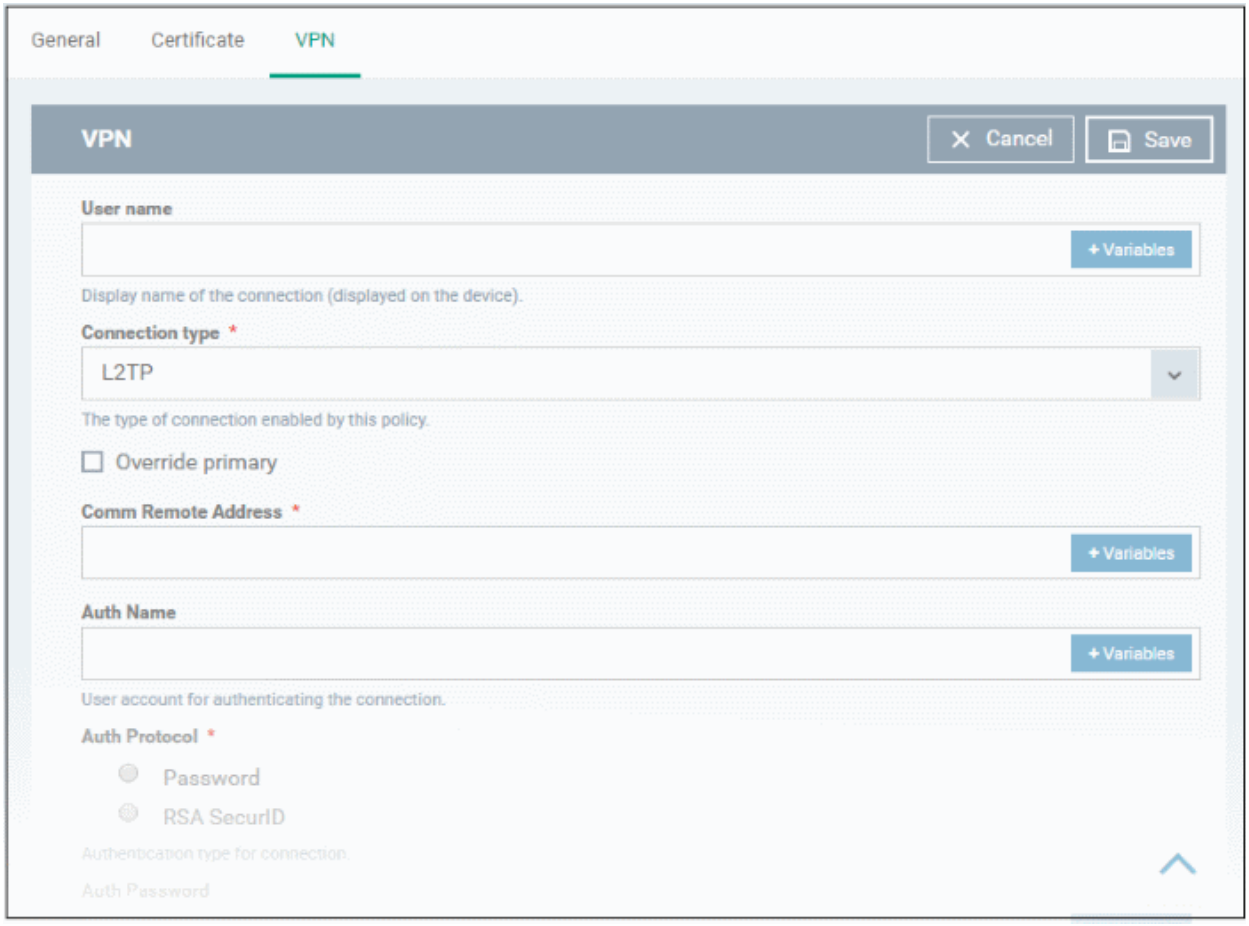
The 'VPN' section allows you to configure the VPN connection settings for the profile.

To configure VPN settings

- Click 'VPN' from the 'Add Profile Section' drop-down



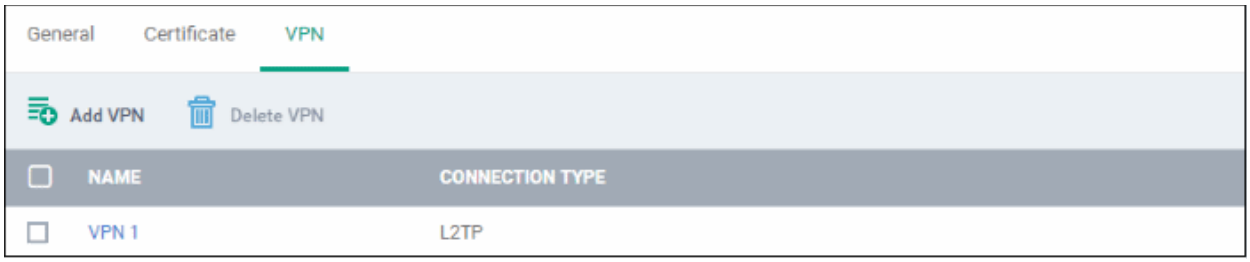
The settings screen for VPN will be displayed.



The connection setting parameters are similar to the VPN settings for an iOS profile. Refer to the VPN settings section for an iOS profile for details.

- Click the 'Save' button after configuring the settings.

The VPN connection will be added to the profile.



You can add several VPN connection accounts to the profile.

- To add another VPN connection, click 'Add VPN' and repeat the process
- To view and edit the settings of a VPN connection, click its name
- To remove VPN connection, select it and click 'Delete VPN'

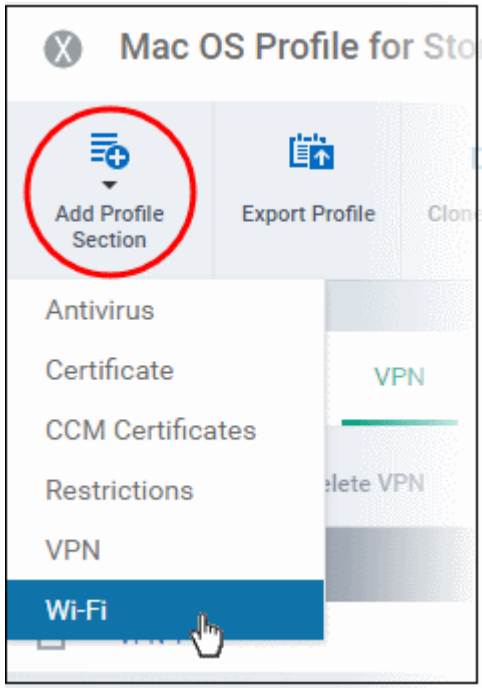
The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

6.1.4.1.6. Wi-Fi Settings for OS X Profile

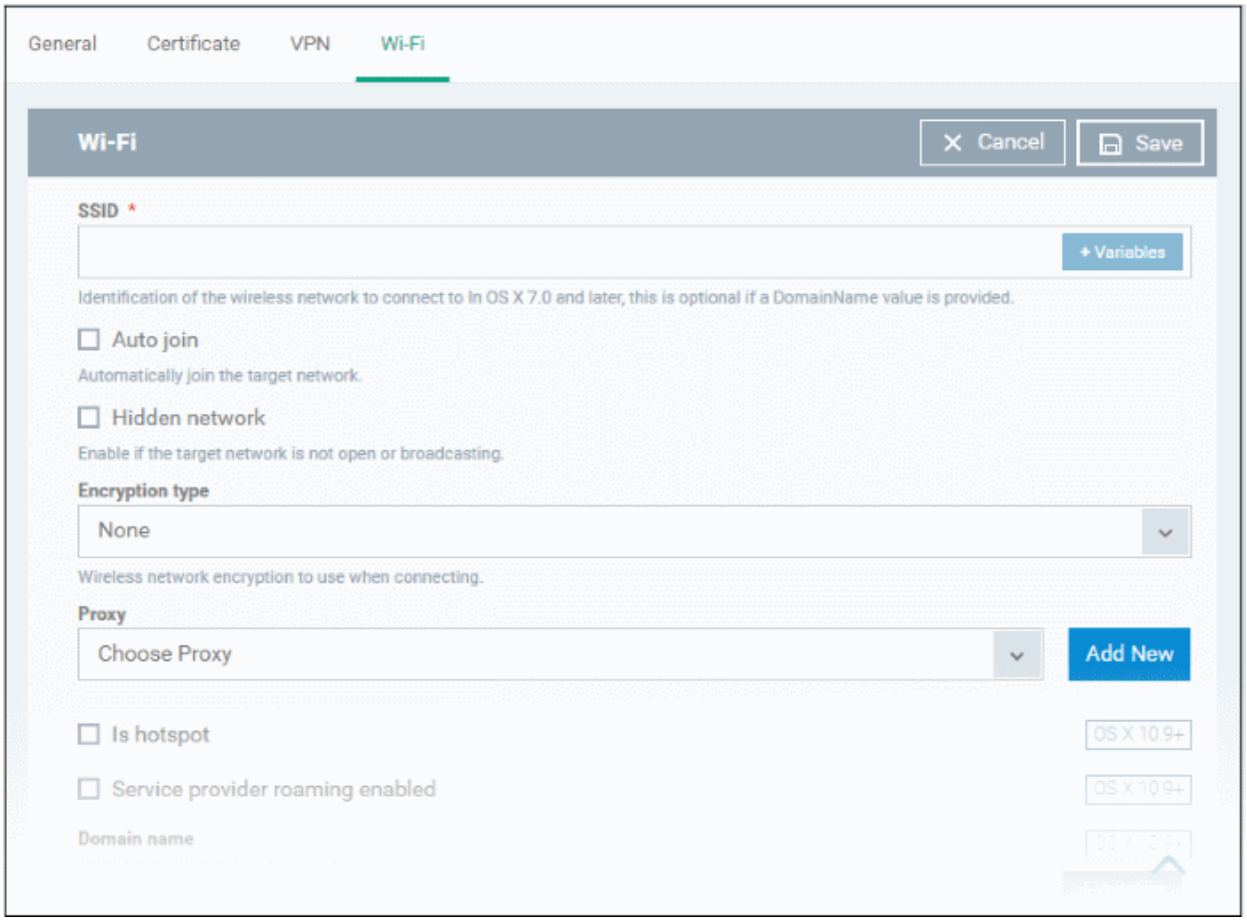
The 'Wi-Fi' section allows you to configure Wi-Fi connection settings for the profile.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Profile Section' drop-down



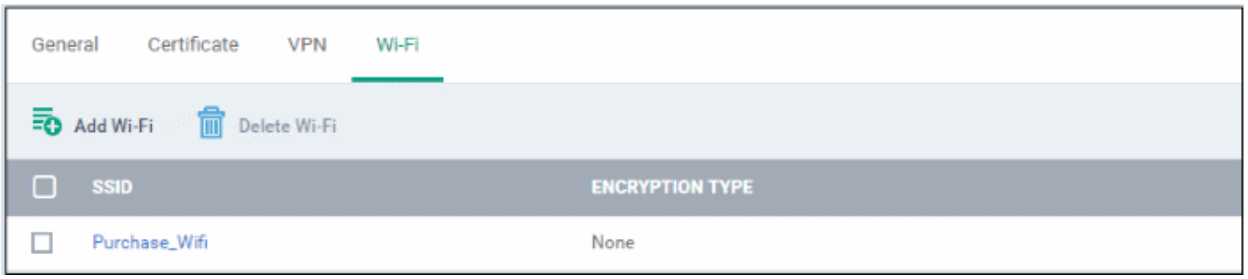
The 'Wi-Fi' settings screen will be displayed.



The connection setting parameters are similar to the Wi-Fi settings for an iOS profile. Refer to the Wi-Fi settings section for an iOS profile for details.

- Click the 'Save' button after configuring the settings.

The Wi-Fi network will be added to the list.



You can add multiple Wi-Fi networks to the profile.

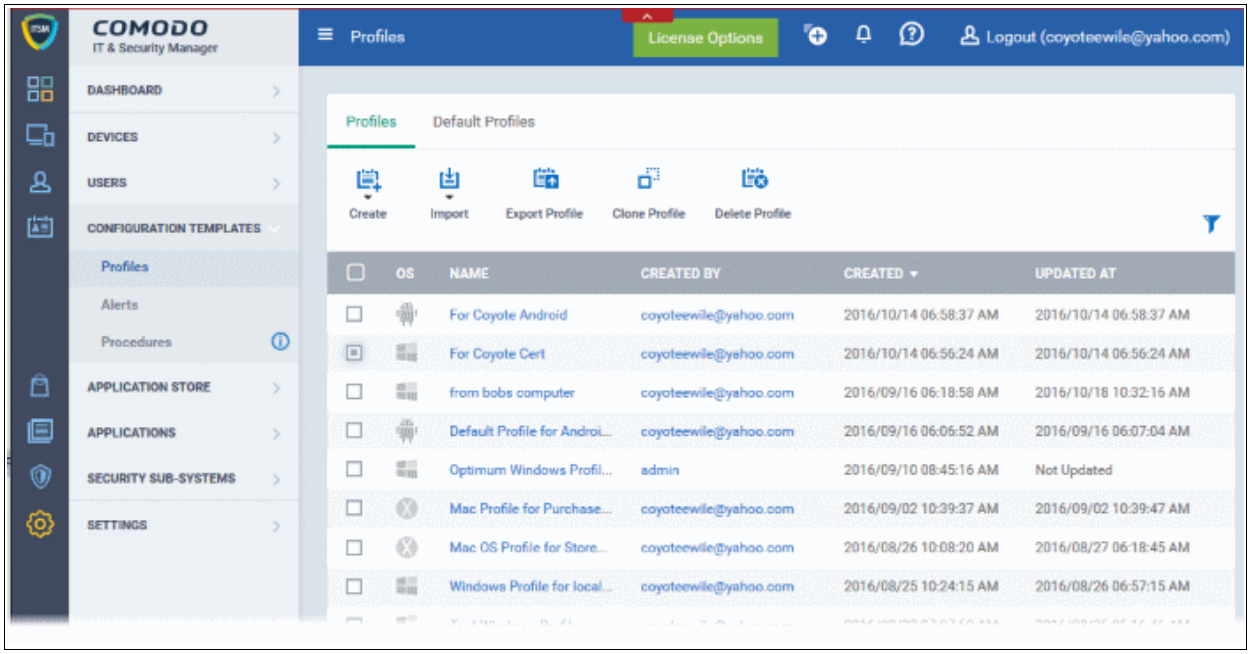
- To add another Wi-Fi network, click 'Add Wi-Fi' and repeat the process
- To view and edit the settings of a Wi-Fi network, click on the SSID of it
- To remove a Wi-Fi network, select it and click 'Delete Wi-Fi'

The settings will be saved and displayed under the Wi-Fi tab. You can edit the settings, add or remove Wi-Fi networks or remove the Wi-Fi networks at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

6.2. Viewing and Managing Profiles

The 'Profiles' screen displays all profiles available for Android, iOS, Mac OS and Windows devices. The screen also allows administrators to create new profiles, export profiles, clone profiles, import profiles from an exported file and remove profiles.

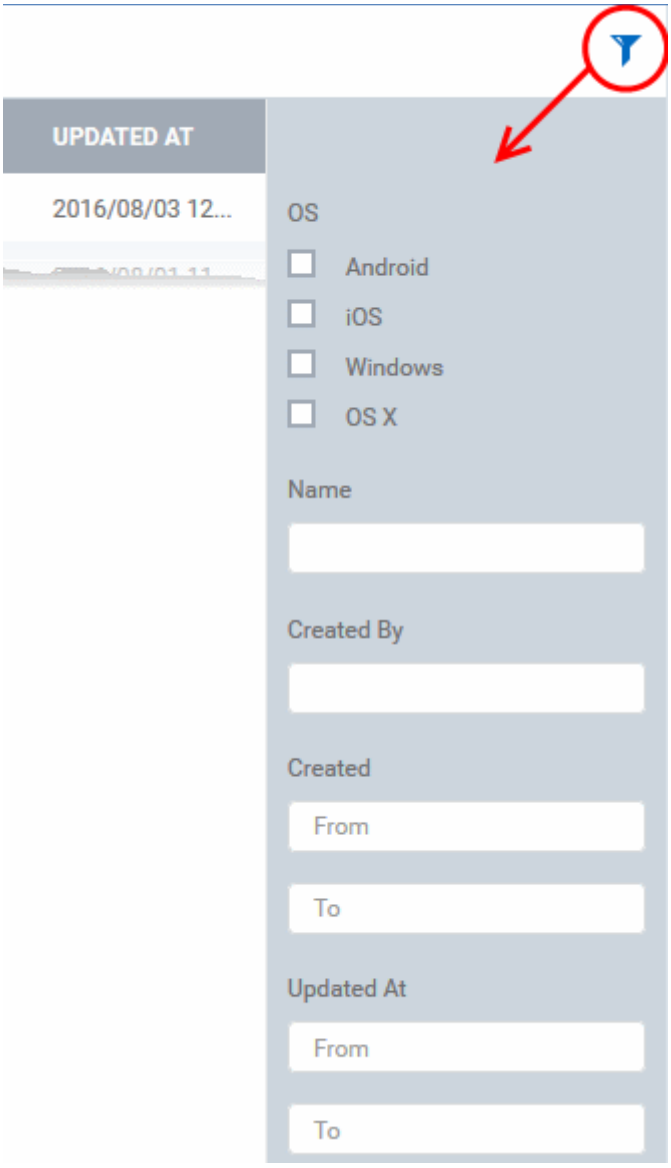
- To open the 'Profiles' interface, click 'Configuration Templates' on the left and choose 'Profiles' from the options on the top.



Profiles - Column Descriptions		
Column Heading		**Description**
OS		Indicates the operating system that the profile supports.
Name		The name assigned to the profile. Clicking the profile name will open the profile settings and configuration interface. Refer to the section **Editing Configuration Profiles** for more details.
Created by		Displays the name of the administrator who created the profile. Clicking the name of the administrator will open the 'Personal' pane, displaying the details of the Administrator. Refer to the section **Viewing the details of the User** for more details.
Created		The date and time at which the profile was created.
Updated at		The date and time at which the profile was last updated.
Controls		
Create	Create Android profile	Allows administrators to create a new Android profile. Refer to the section '**Profiles for Android Devices**' for more details.
	Create iOS profile	Allows administrators to create a new iOS profile. Refer to the section '**Profiles for iOS Devices**' for more details.
	Create OS X profile	Allows administrators to create a new Mac OS profile. Refer to the section '**Profiles for Mac OS Devices**' for more details.
	Create Windows profile	Allows administrators to create a new Windows profile. Refer to the section '**Creating Windows Profiles**' for more details.
Import	Import from Comodo Client Security Config file	Allows administrators to import the security configuration of CCS from a .cfg configuration file as a Windows profile. The configuration file will usually have been exported from a managed endpoint with CCS installed. Refer to the section '**Importing Windows Profiles**' for more details.
	Import from Exported Profile	Allows administrators to import a configuration profile from a previously exported and saved profile. Refer to the section **Exporting and Importing Configuration Profiles** for more details.
Clone Profile		Allows administrators to create a new profile by cloning an existing profile and modifying its settings as required. Refer to the section **Cloning a Profile** for more details.
Export profile		Allows administrators to export the selected configuration as a .cfg file and save it for future implementation. Refer to the section **Exporting and Importing Configuration Profiles** for more details. The control will appear only if a single profile is selected from the list.
Delete profile		Allows administrators to delete profile(s). The control will appear only if one or more profiles are selected.

Sorting, Search and Filter Options

- Clicking on any of the column headers will sort the items in ascending/descending order of entries in that column.
- Clicking the funnel icon enables you to search for profiles based on the filter parameters



- To filter the profiles based on 'OS' type, select the check box and click the 'Apply' button.
- To filter the profiles based on name and author, enter the text partially or fully in the respective fields and click the 'Apply' button.
- To filter the profiles based on the period at which they were created or last modified, enter the date range in the specified fields, and click the 'Apply' button.
- You can use these filters in combination to search for specific profile.

Profiles which match the search parameters will be displayed in the screen.

- To display all profiles again, clear all filters and click the 'Apply' button.
- Click the funnel icon again to close filter options

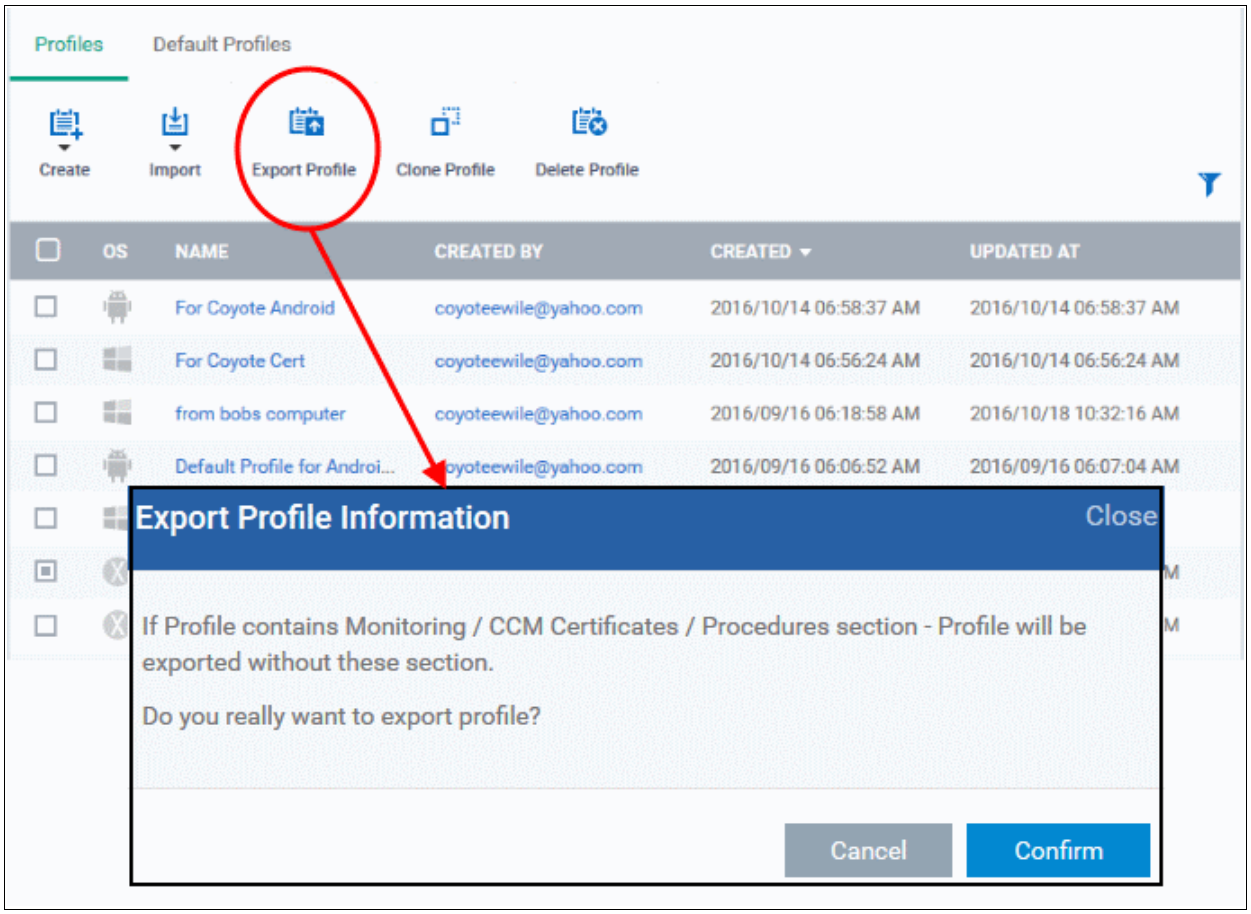
6.2.1. Exporting and Importing Configuration Profiles

ITSM allows you to export and import existing Android, iOS, Mac OS and Windows profiles for re-deployment to other endpoints and endpoint groups.

Note: 'Monitoring Settings', 'CCM Certificate Settings' and 'Procedure Settings' will be excluded from exported profiles. You will need to reconfigure these sections before deploying if they are required in a new profile.

To export a profile

- Open the 'Profile' interface by clicking 'Configuration Template' on the left then click 'Profiles' tab.
- Select the profile you want to export and click the 'Export profile' button:

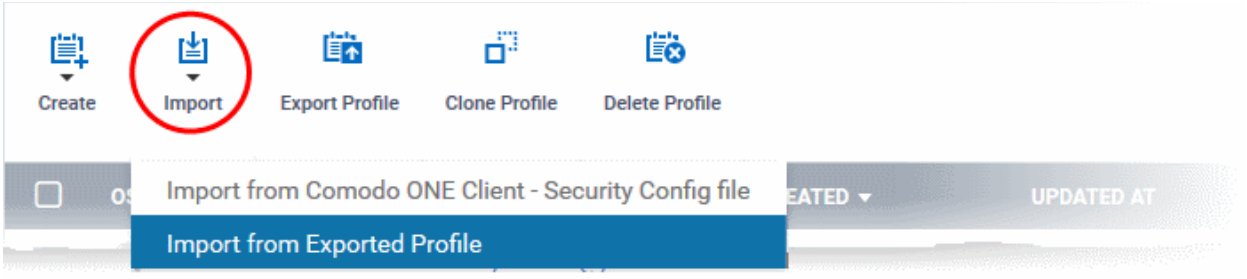


The application will prompt with a dialog stating that all profiles except the Monitoring or CCM Certificates or Procedure sections that contain confidential information will be exported.

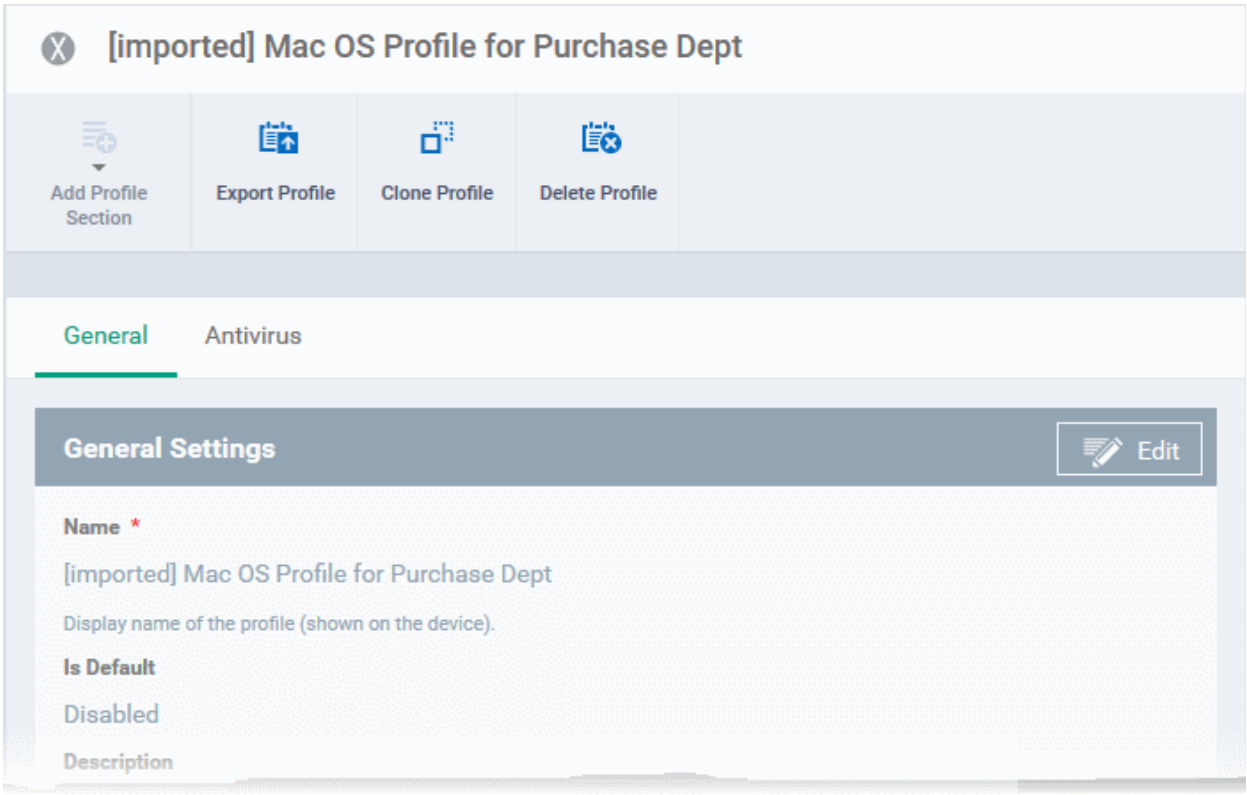
- Click 'Confirm' on the dialog to export profiles and save the file in a safe location in .cfg format.
- This file can now be imported back to ITSM as a profile.

To import a profile from a saved .cfg file

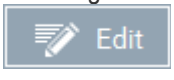
- Open the 'Profiles' interface by clicking 'Configuration Template' from the left and choosing 'Profiles' from the options.



- Click 'Import' and choose 'Import from Exported Profile' from the drop-down
- Navigate to the location in your computer where the .cfg file is stored, select the file and click 'Open'.
- The 'Profile' interface will open, with the prefix [Imported] in the file name and security components pre-configured as per the source profile.



The profile details interface of the imported profile will be displayed. The imported profile will not be enabled as a 'Default Profile' by default.

- To change the name of the profile and/or to enable it as a default profile, click the 'Edit' button 

at the top right of the 'General' settings screen.
- You can add new components by clicking the 'Add Profile Section' button. You can view and edit the settings of existing components by clicking the component name. For more details on the options available under each component, refer to the sections Profiles for Android Devices, Profiles for iOS Devices, Profiles for Mac OS Devices and Profiles for Windows Devices.

6.2.2. Cloning a Profile

ITSM allows you to create a new configuration profile using an existing profile as a template. You can then edit the cloned profile according to the requirements of your target devices or group.

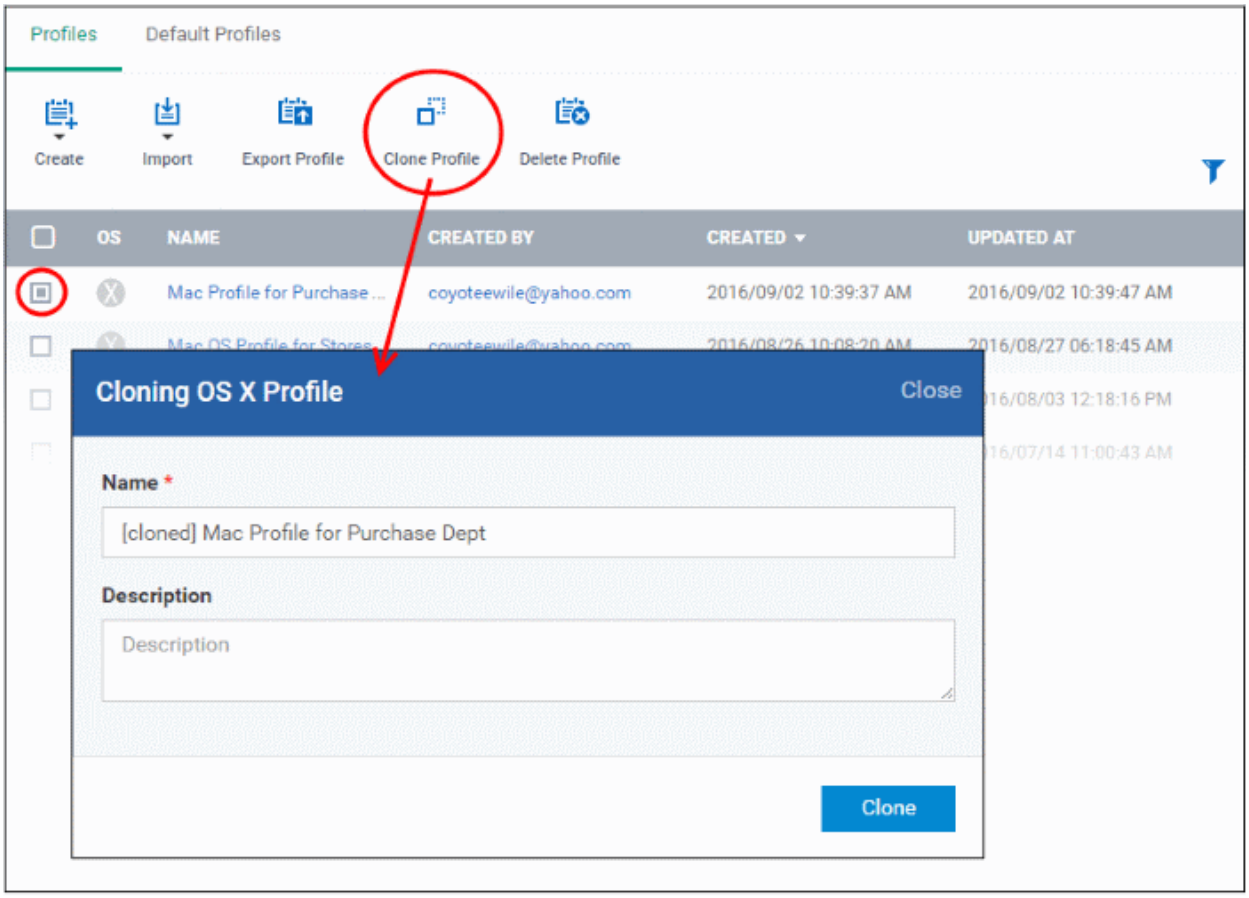
To create a clone of a profile

- Open the 'Profiles' interface by clicking 'Configuration Template' on the left then click 'Profiles' Tab.
- Click on the name of the profile you want to clone.

The profile details interface will open with the components configured in the profile

- Click 'Clone Profile' from the top

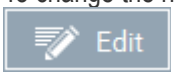
Alternatively, select the profile from the 'Profiles' interface and click 'Clone Profile' at the top.



The 'Cloning OS X Profile' dialog will open for the OS type of the chosen profile. The name of the new profile will be the same as the source profile with the prefix [cloned].

- If required, enter a new name for the profile and a short description
- Click 'Clone'.

A new profile will be created with configuration parameters identical to the source profile. The profile details interface will be displayed. The cloned profile will not be enabled as a 'Default Profile' by default.

- To change the name of the profile and/or to enable it as a default profile, click the 'Edit' button 

at the top right of the 'General' settings screen, edit the settings and click the 'Save' button.
- To edit component settings, click the name of the component you wish to modify, click 'Edit' and change the parameters.
- You can add new profile components by clicking the 'Add Profile Section' button

For more details on the options available under each component, refer to the sections Profiles for Android Devices, Profiles for iOS Devices, Profiles for Mac OS Devices and Profiles for Windows Devices..

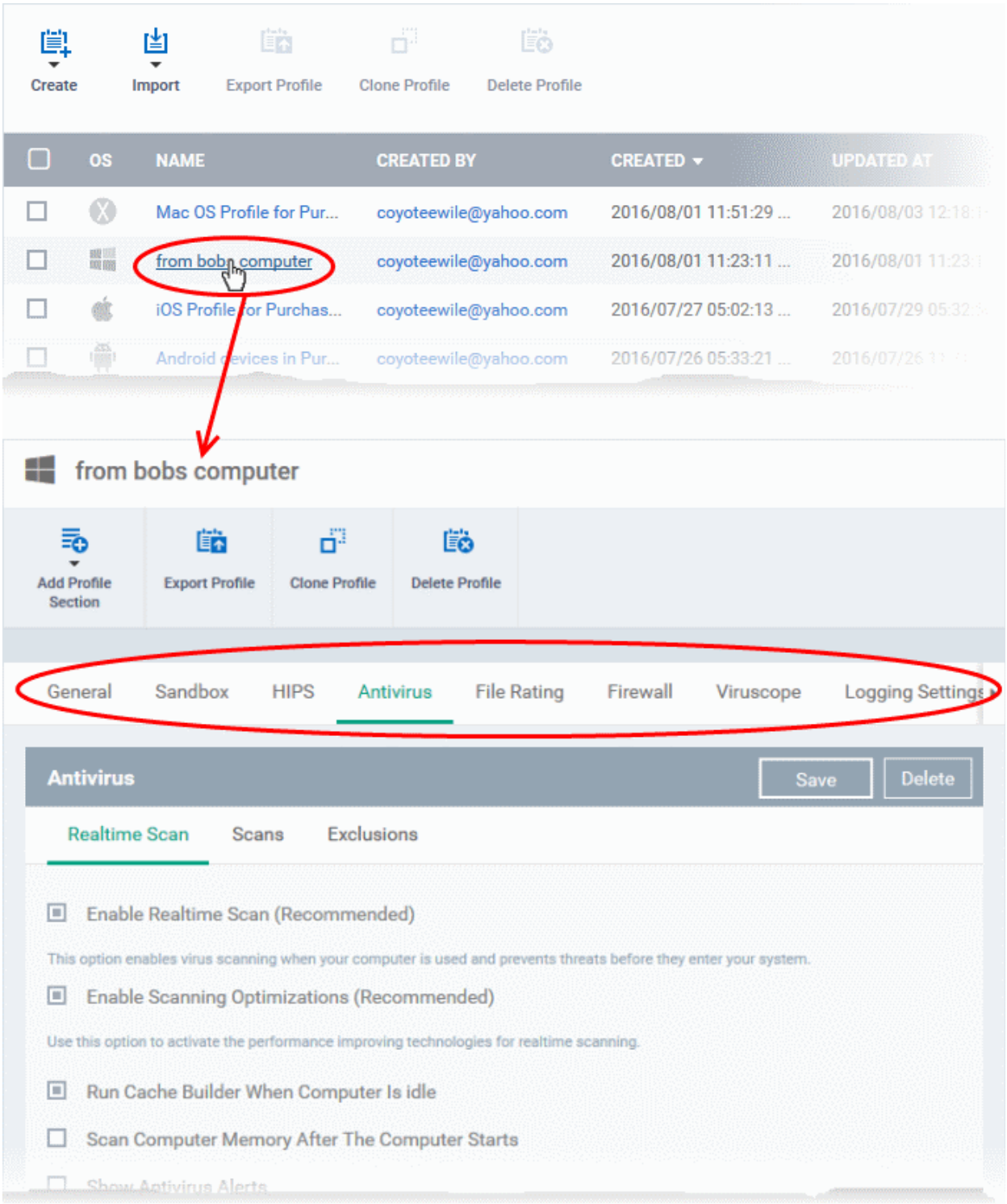
6.3. Editing Configuration Profiles

An existing configuration profile in ITSM can be edited according to the requirements of the organization, for

example, for adding or removing security components and changing configuration parameters.

To edit a profile

- Click the 'Configuration Templates' tab from the left and choose 'Profiles' from the options and choose 'Profiles' tab
- Click on the name of the profile that you want edit, from the list.



The profile details will appear. The parameters and settings configured for each security component added as a profile section, will be displayed under respective tab.

- To edit the settings of a profile section, click the respective tab.
- Depending on the components that can be configured, you can directly edit the parameters or click the

'Edit' button  and then edit the parameters.

The editing steps are similar to creating a new profile. Refer to the sections Profiles for Android Devices, Profiles for iOS Devices, Profiles for Mac OS Devices and Profiles for Windows Devices..

- Click 'Save' for your changes to take effect for the profile
- To delete a profile section from the profile, click 'Delete' from the edit options
- To delete the profile itself, click the  button at the top

6.4. Managing Default Profiles

Default profiles are automatically assigned to devices at enrollment and implement a strong, baseline level of security. Comodo supplies default profiles for each OS type - each pre-configured to provide optimum protection to newly enrolled devices. These 'Optimum' profiles can be used in isolation or in conjunction with any custom profiles that you create. The default profiles supplied by Comodo cannot be modified or deleted from ITSM, but may be removed from devices (or replaced), if you wish.

In addition to built-in 'Optimum' default profiles, ITSM also ships with two more Windows profiles, Standard Windows Profile for ITSM and Hardened Windows Profile for ITSM, each configured with different settings. These two profiles also cannot be edited or removed.

You can turn any profile you create into a default profile and you can also clone a default profile to use as a template. You can create as many default profiles as you want, but please make sure the settings in them do not conflict. If the settings conflict then the most restrictive policy will be applied. For example, if the camera is enabled in a policy and disabled in another, then it will be disabled on the devices.

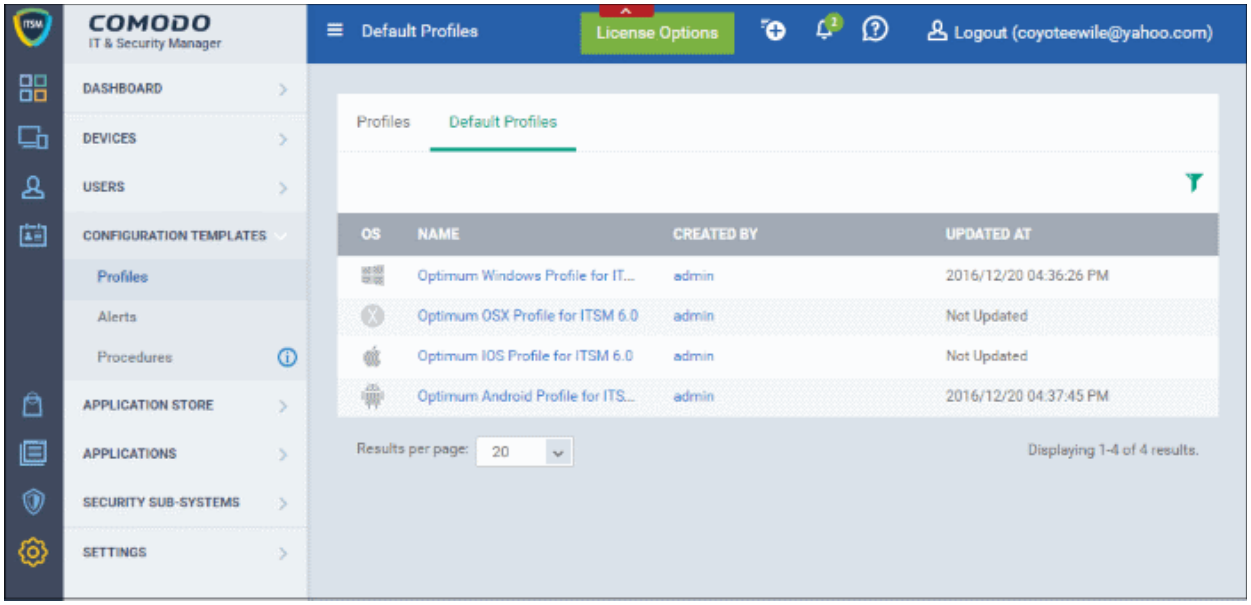
Please note that you can cancel any default profiles including built-in 'Optimum' profiles, meaning devices that are enrolled will not be applied any profile during enrollment. The behavior of default profiles is as follows:

- When a profile is set as default, it will be applied to new devices during enrollment
- When a profile is set as default, it will be applied to already enrolled devices that has no assigned profiles
- When a default profile is set as not default, the profile will be unassigned from enrolled devices

For devices with no profiles applied, you can carry out on-demand functions such as run antivirus scans, run a procedure and so on. For Windows devices with CCS installed, when there are no profiles applied, the default CCS settings will apply.

The 'Profiles' tab from the left hand side navigation allows the administrator to view and manage default profiles.

- To open the default profiles screen, click 'Configuration Templates' on the left.
- Choose 'Default Profiles' tab on the top.



The image above displays the default profiles that are shipped with ITSM. You can edit a default profile or remove its default status, edit a created custom profile and make it is as default.

Click the following links for more details:

- Creating a default profile
- View and manage default profiles
- Assigning default profiles to devices
- Removing default profiles
- Canceling default profiles

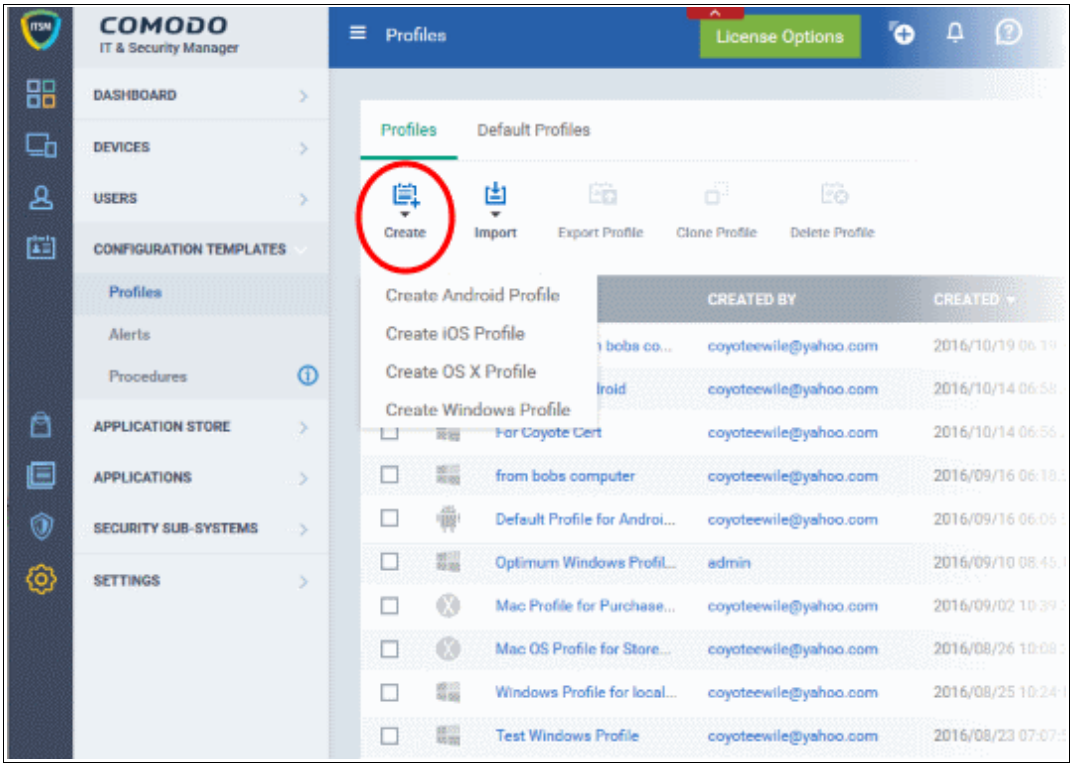
Creating a default profile

A profile can be made as a default profile while creating it or edit the existing profiles and make as default. Click the following links to know more about creating default profiles.

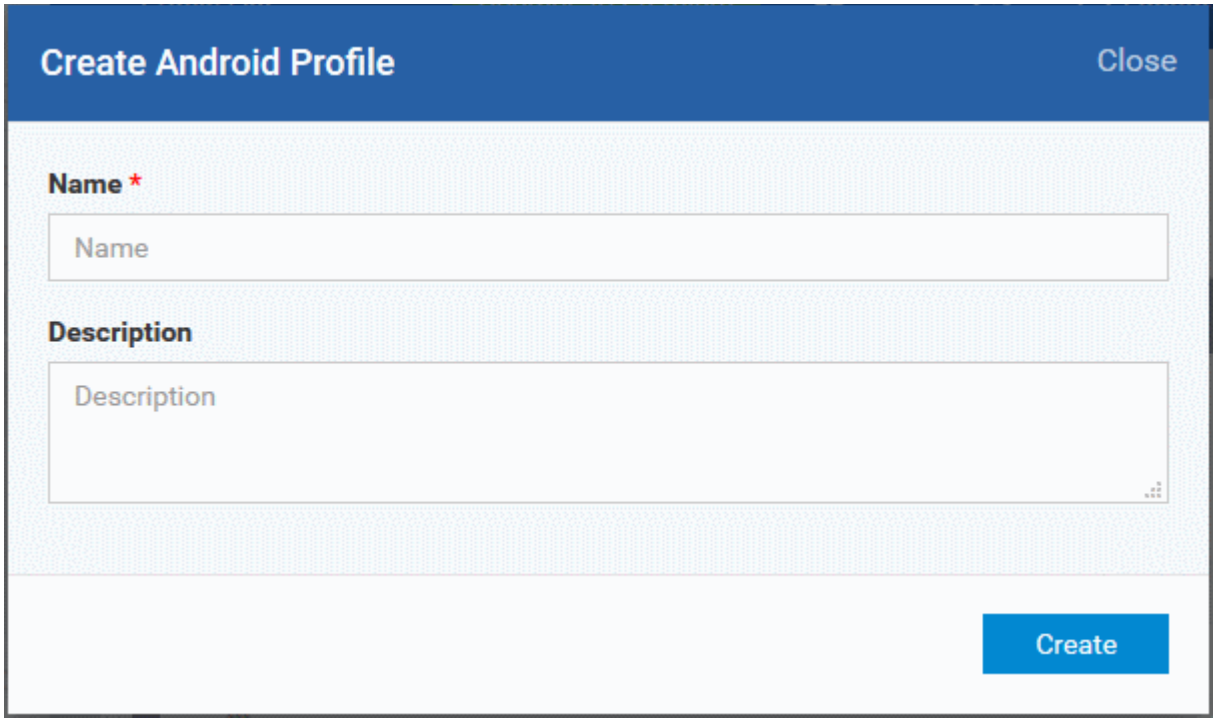
- Creating a default profile from the create profiles screen
- Creating a default profile from the edit screen of existing profiles

To create a default profile from the create profile screen

- Click 'Configuration Templates' on the left and then choose 'Profiles' from the options
- Choose the type of profile that you want to create from the 'Create' drop-down

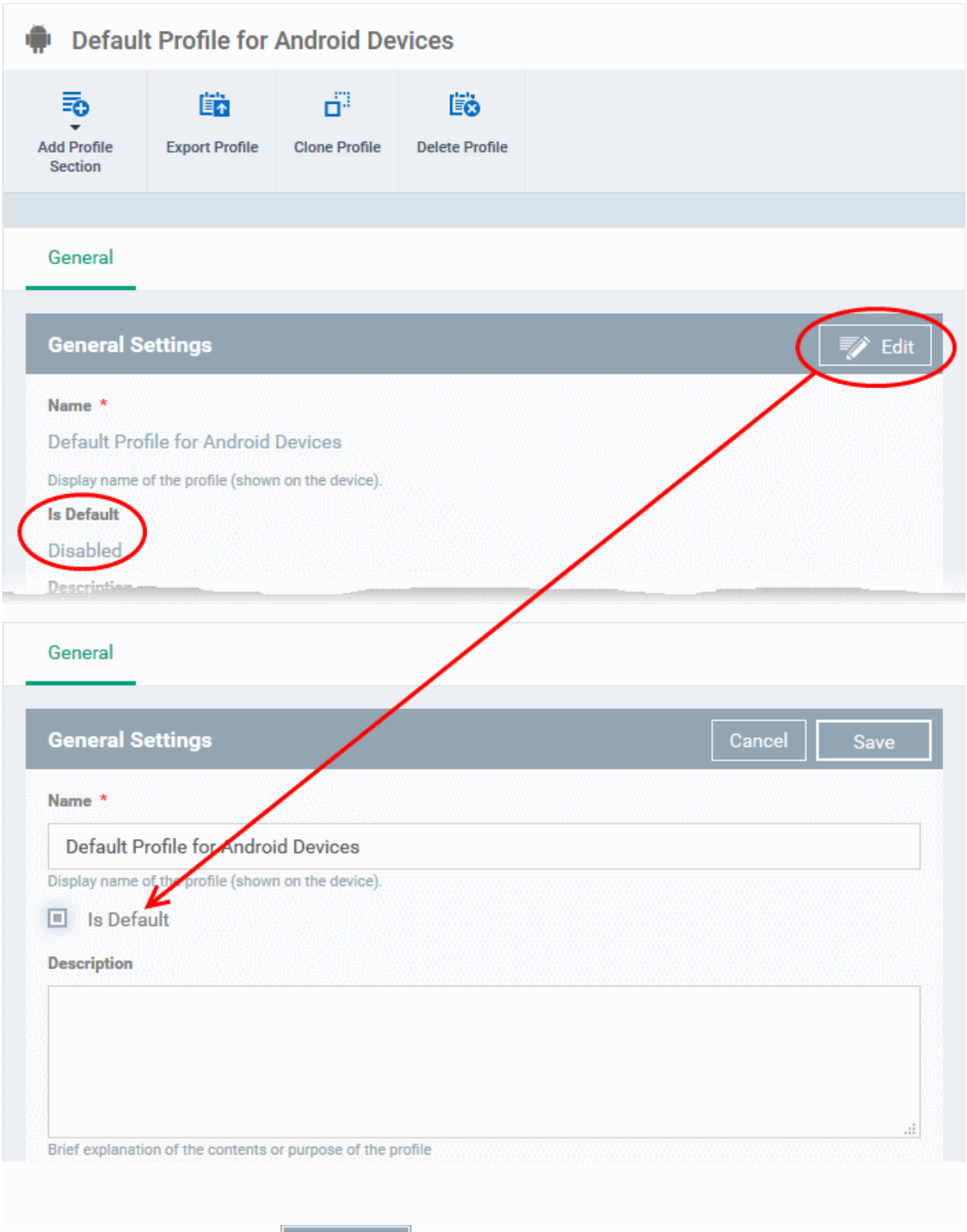


The 'Create OS Profile' screen will be displayed.



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

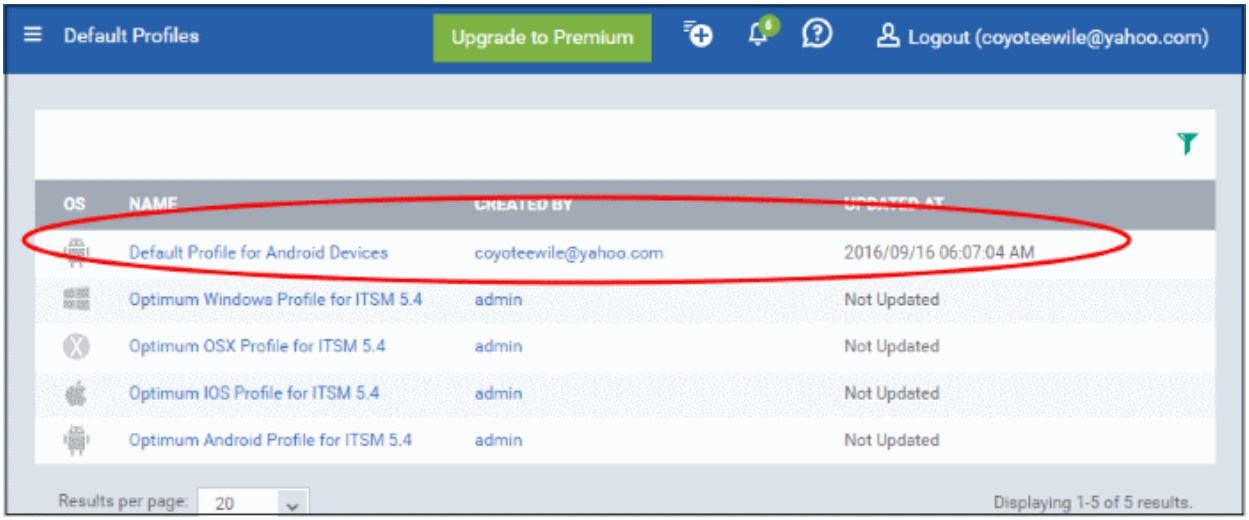
The profile for the selected OS type will be created and the 'General Settings' section will be displayed. The new profile is not enabled as a 'Default Profile' by default.



- Click on the 'Edit' button 

at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- Click the 'Save' button.

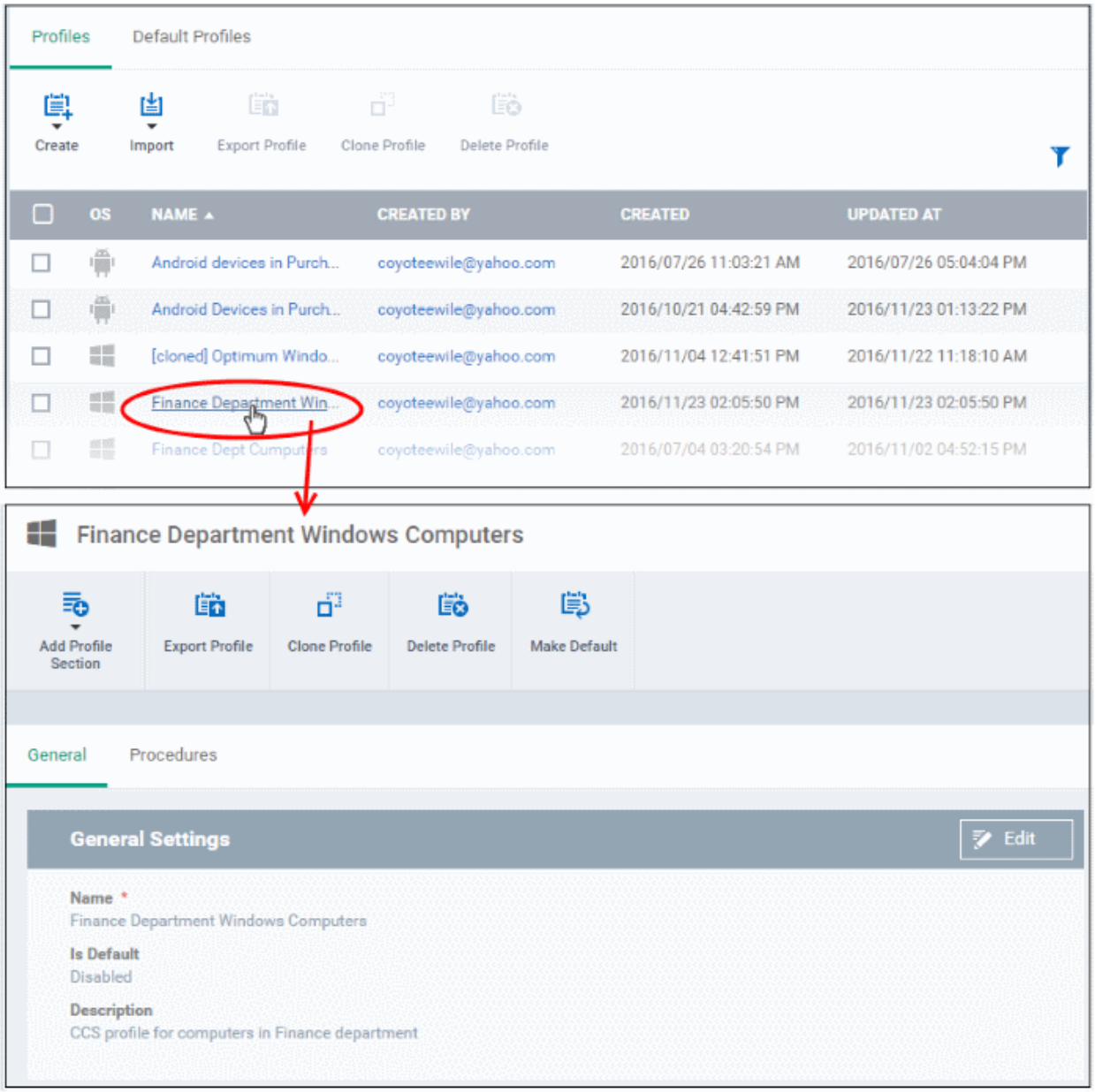
The profile will be saved as a 'Default Profile' and listed in the 'Default Profiles' screen.



You can edit the profile and add profile sections as required. Refer to the section **Editing Configuration Profiles** for more details.

To create a default profile from the existing profiles screen

- Click 'Configuration Templates' on the left and choose 'Profiles' from the options.
- Click Profiles tab on the top.
- Click the profile name that you want the ITSM to display as a default profile



The profile details screen of the selected profile will be displayed.

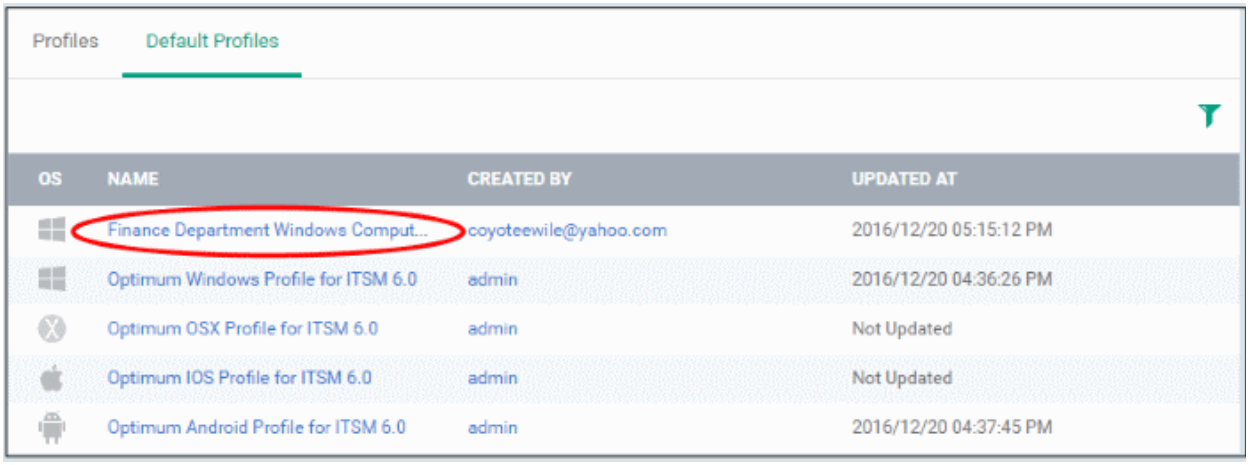
- Click the 'Edit' button 

at the top right of the 'General' settings screen and select 'Is Default' check box and click 'Save'.

Or

- Click 'Make Default' at the top.

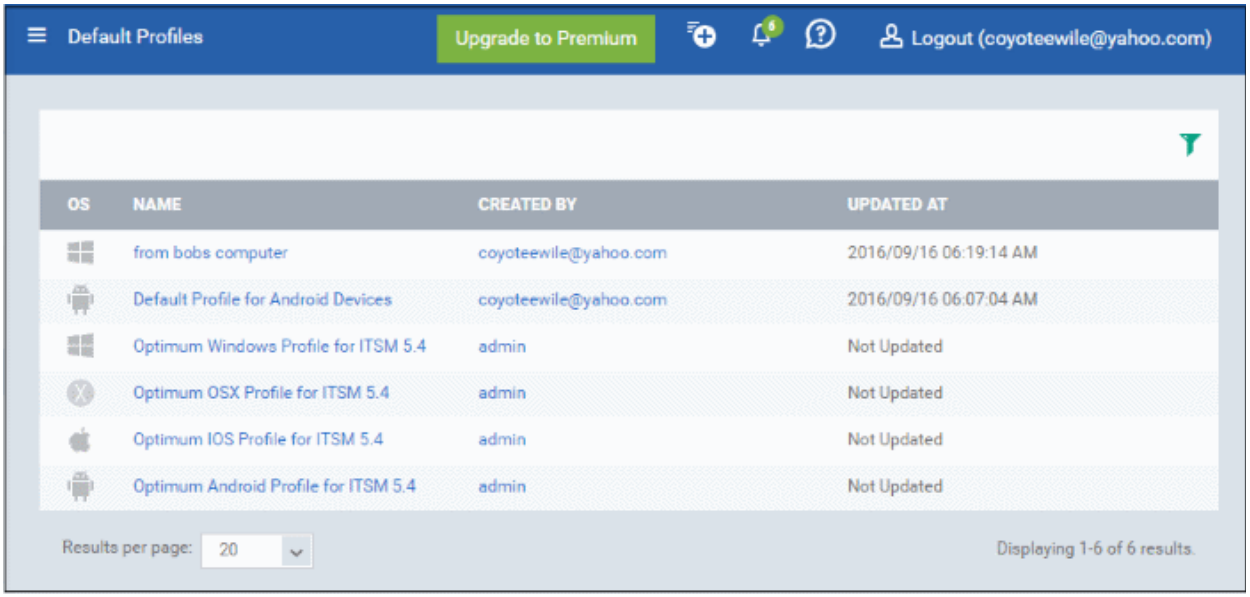
The profile will be saved as a 'Default Profile' and listed in the 'Default Profiles' screen.



To view and manage default profiles

- Click 'Profiles' from the left and choose 'Default Profiles' tab on the top.

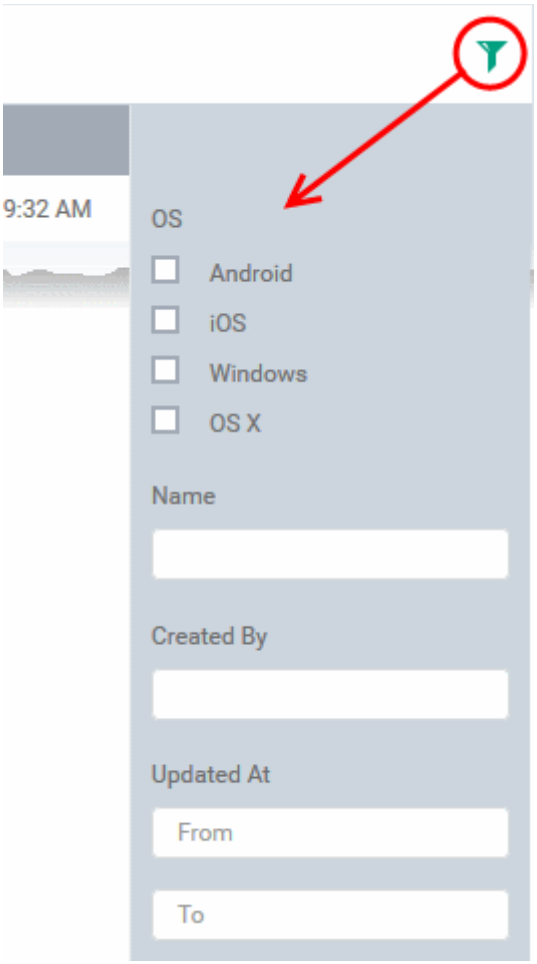
The list of default profiles will be displayed.



Profiles - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system that the profile is applied for.
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Profile' interface. Refer to the section Editing Configuration Profiles for more details.
Created by	Displays the name of the administrator who created the profile. Clicking the name of the administrator will open the 'Personal' pane, displaying the details of the Administrator. Refer to the section Viewing the details of the User for more details.
Updated at	The date and time at which the profile was last updated.

Sorting, Search and Filter Options

- Clicking on any of the column headers will sort the profiles in ascending/descending order of entries under that column.
- Clicking the funnel icon enables you to search for profiles based on the filter parameters.



- To filter the profiles based on 'OS' type, select the check box and click the 'Apply' button.
- To filter the profiles based on name and/or name of the administrator that created the profile, enter the text partially or fully in the respective fields and click the 'Apply' button.
- To filter the profiles based on the period at which they were last modified, enter the date range in the specified fields, and click the 'Apply' button.
- You can use these filters in combination to search for specific profile.

The profiles that matches the entered/selected parameters will be displayed in the screen.

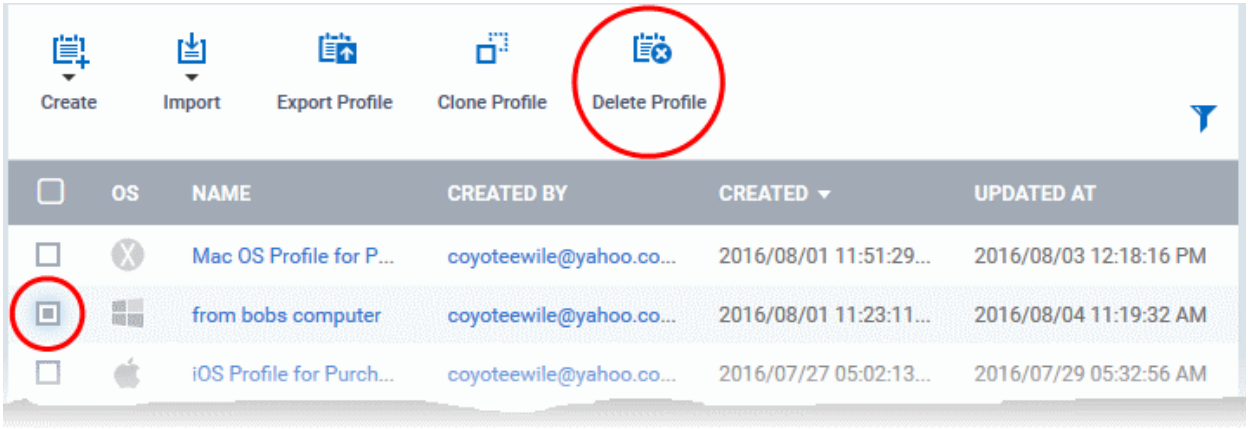
- To display all the profiles again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the filter options

Assigning default profiles to devices

Devices that are enrolled for the first time will automatically be assigned the default profiles according to their operating system. These default profiles will be automatically overridden by the profiles that are assigned to the devices by the administrator according the organizational requirements. Please note the default profiles that were installed initially will become active again in the devices when the applied profiles are removed from them.

Removing default profiles

You can remove a default profile from the 'Configuration Templates' > 'Profiles' screen. Please note that default profiles that are shipped with ITSM cannot be removed.



- Select the default profile from 'Profiles' screen and click the 'Delete Profile' button at the top of the screen.

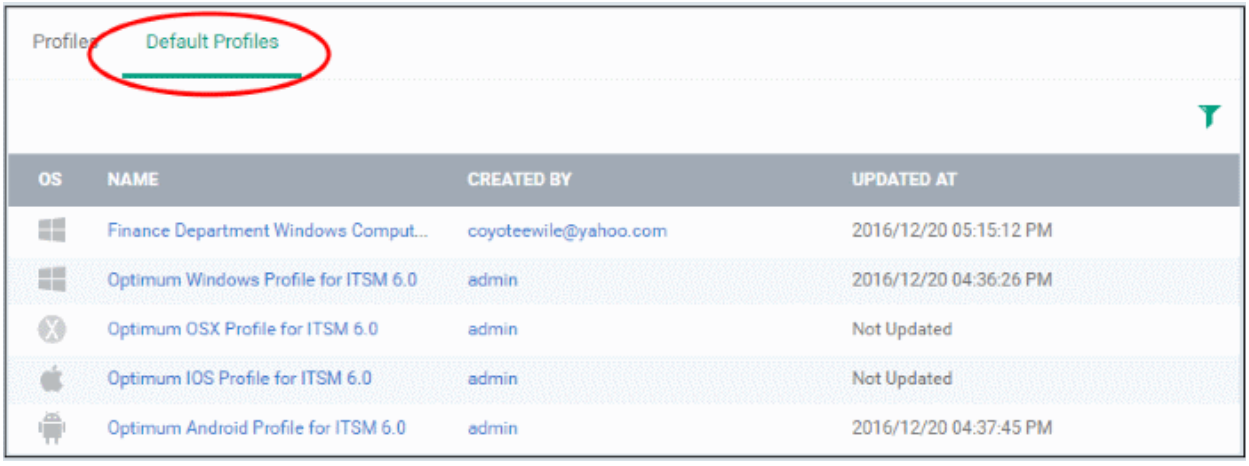
The default profile will be removed from the list and it will also be removed as a regular profile from the 'Profiles' screen. Please note that even if default profile(s) are removed from the list, the device(s) will still retain the configured settings from the profiles till a new profile(s) are assigned to them.

To cancel default profiles

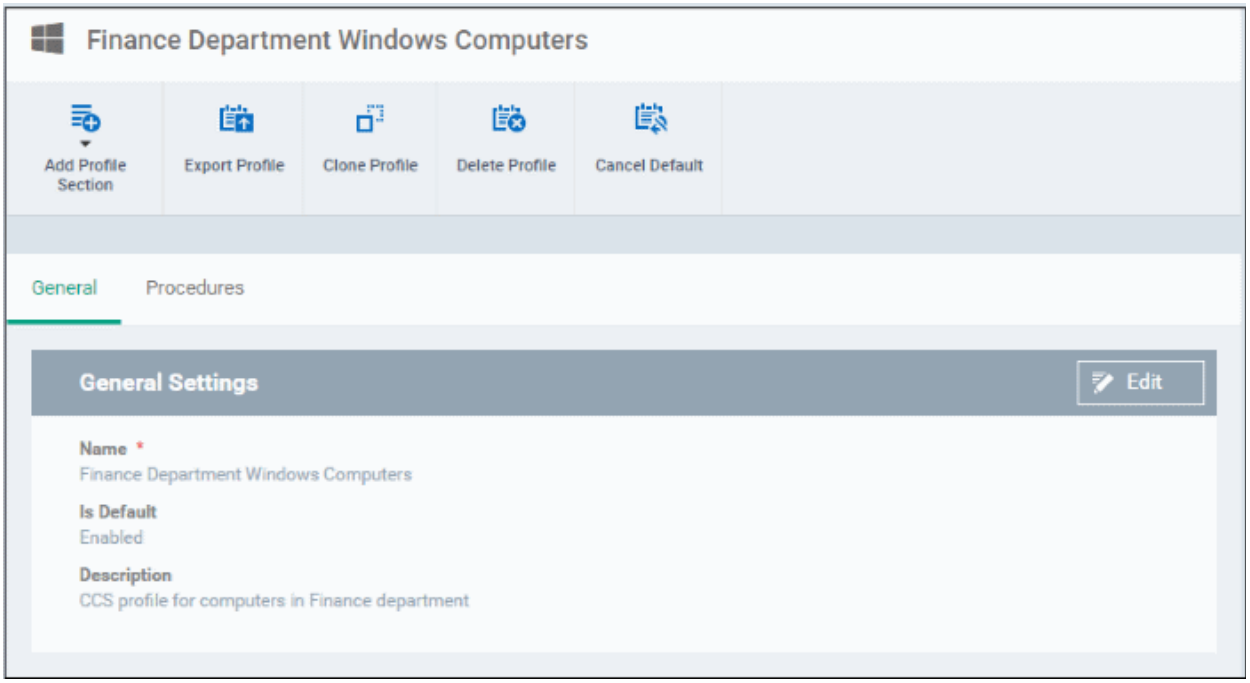
You can cancel custom default profiles as well as built-in default profiles, meaning no default profiles will be applied to devices on enrollment. These canceled default profiles will also be unassigned from already enrolled devices.

For devices with no profiles applied, you can carry out on-demand functions such as run antivirus scans, run a procedure and so on. For Windows devices with CCS installed, when there are no profiles applied, the default CCS settings will apply.

- To open the default profiles screen, click 'Configuration Templates' on the left.
- Choose 'Default Profiles' tab on the top.



- Click the name of the default profile from the list



- Click 'Edit' on the right, deselect 'Is Default' check box and click 'Save'

Or

- Click 'Cancel Default' button at the top

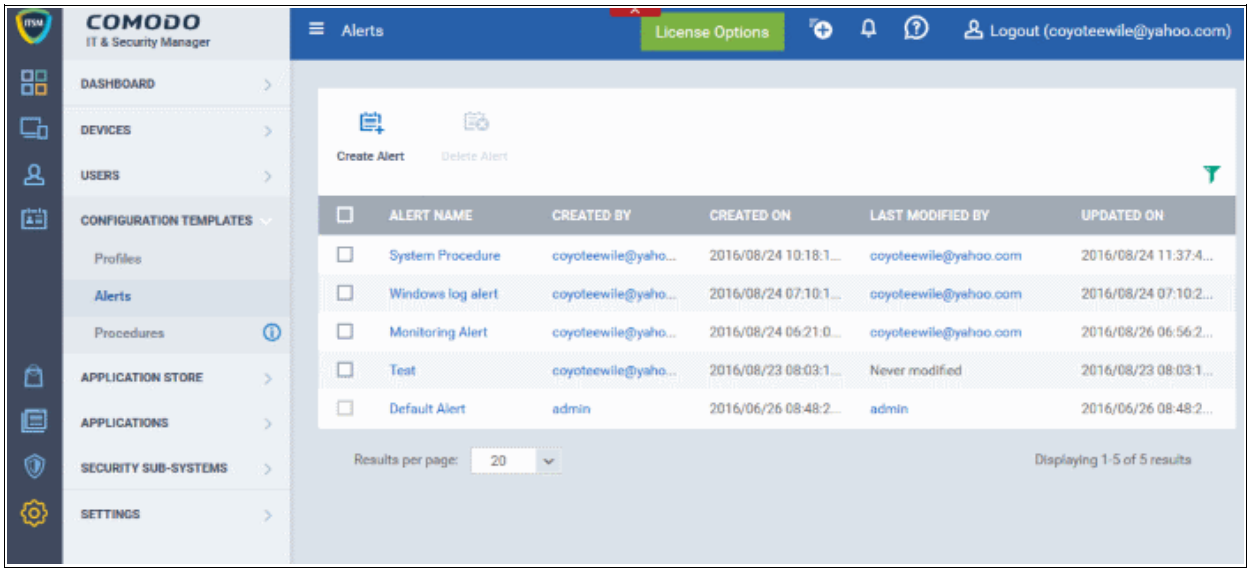
Please note that for built-in default profiles, the 'Edit' button will not available and you can cancel its default status only by clicking the 'Cancel Default' button at the top.

6.5. Managing Alerts

You can configure alerts to be generated upon events such as procedures not running on devices or any breach of monitoring feature setting in profiles. Alerts can be configured to notify administrators in multiple ways:

- Service Desk Ticket - Alerts and notifications are created on Service Desk application
- Notification - Shown as notification on portal
- Email - Sent to administrators when a check fails for a consecutive number of times

The alerts that are created here will be available for selection in the **Procedure** section and while configuring **Monitoring Settings** for a Windows profile.



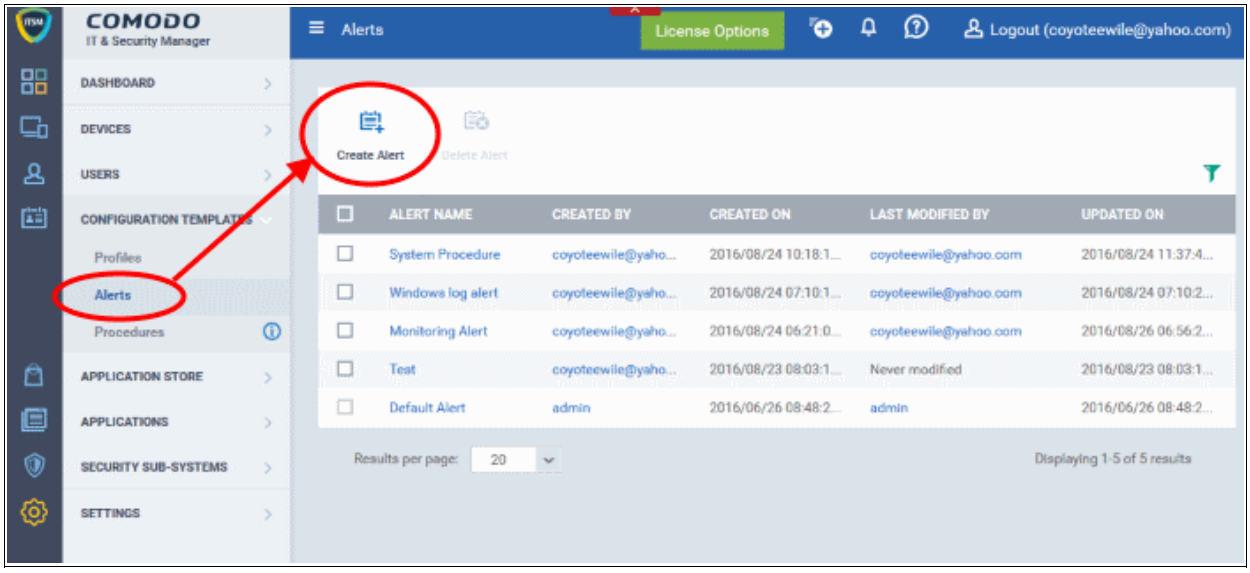
Note - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit files for analysis, monitor Windows events and provide alerts and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports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

Click the following links for more details:

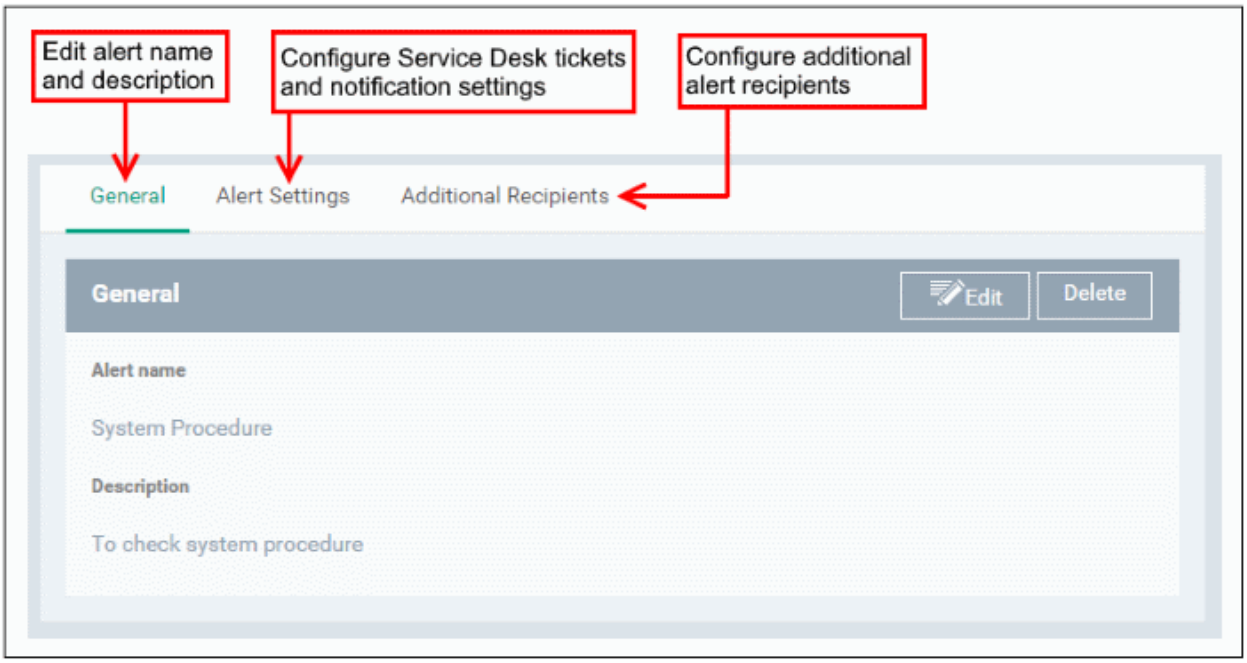
- **Create a new alert**
- **Edit / delete an alert**

6.5.1. Create a New Alert

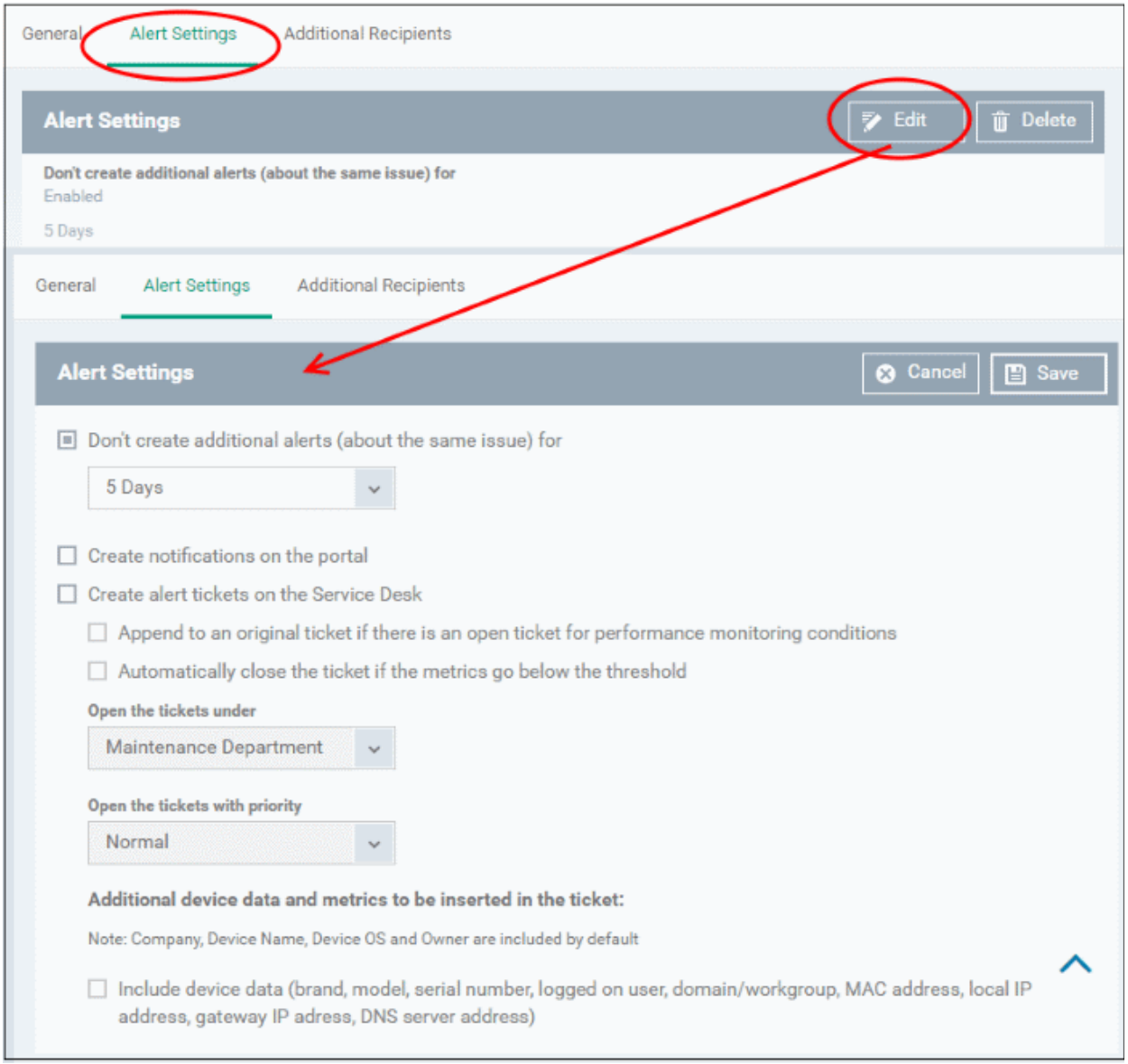
- To create a new alert, click 'Configuration Templates' > 'Alerts'
- Click 'Create Alert'



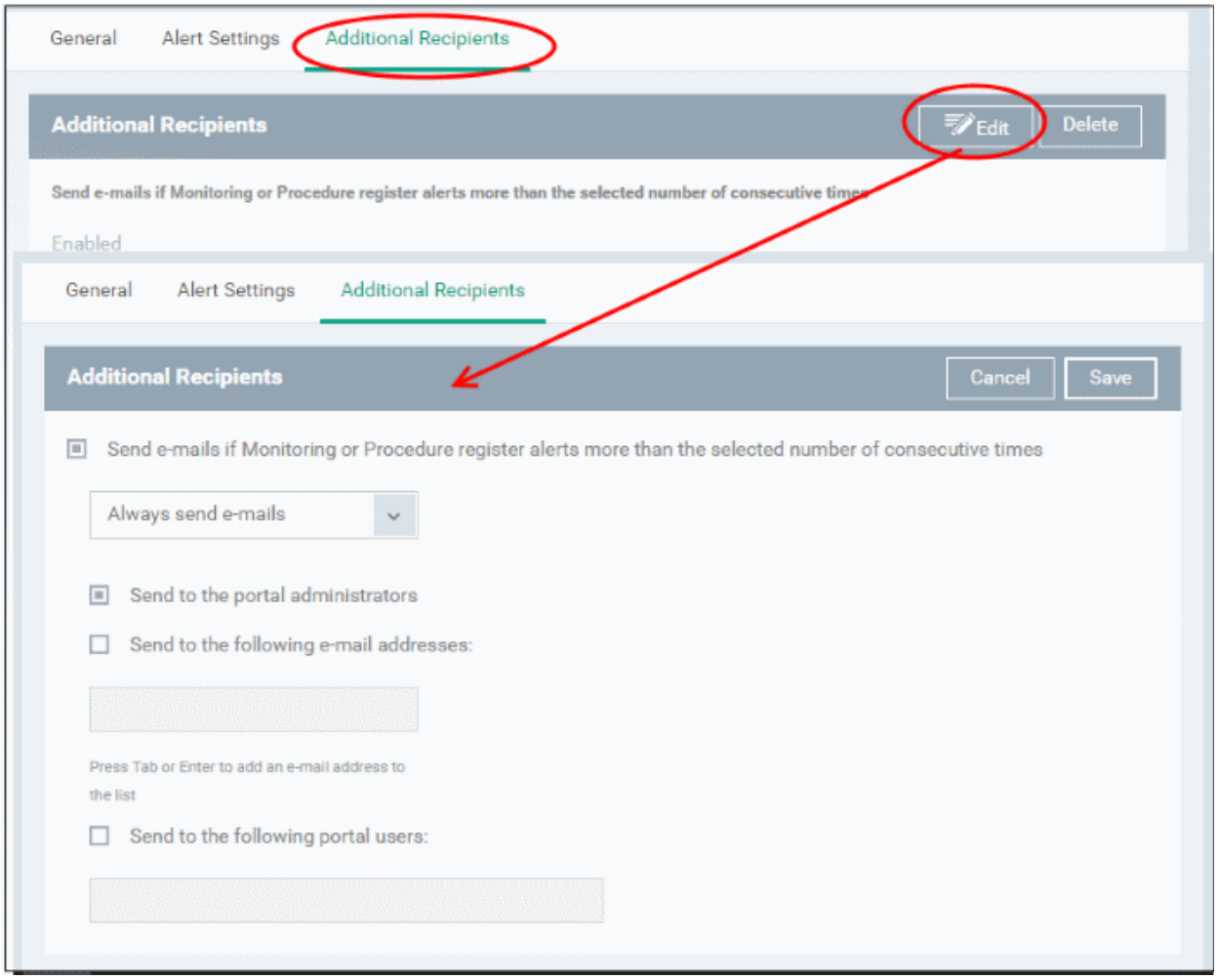
- Create a name and description for your alert. After saving, you will be taken to the alert configuration screen. The 'General' section allows you to modify basic settings:



- To configure alert settings, click 'Alert Settings' tab and then 'Edit'



- **Don't create additional alerts (about the same issue) for** - Determines whether additional alerts should be generated if same issue occurs within the specified period. The field below this allows you to select the period which ranges from 5 minutes to 5 days. By default, this is selected with a specified period of 5 days.
- **Create notifications on the portal** - Alerts will be generated and displayed on the **Notifications** screen.
- **Create alert tickets on the Service Desk** - If enabled, tickets will be raised automatically on Service Desk application and allotted to specified departments.
  - **Append to an original ticket if there is an open ticket for performance monitoring conditions** - Determines whether a new ticket should be raised for an issue even if a ticket is open for the same issue in Service Desk.
  - **Automatically close the ticket if the metrics go below the threshold** - Determines whether the open tickets for an issue should be closed automatically if the monitoring parameter goes below the set threshold.
  - **Open the tickets under** - Select the the department from the drop-down to which the tickets should be allotted.
  - **Open the tickets with priority** - Select the ticket priority, whether normal, high or critical from the drop-down.
  - **Additional device data and metrics to be inserted in the ticket** - By default, the name of the company, device, device OS and owner are included in the ticket. Select the option to include other data such as brand, model and so on.
- To configure 'Additional Recipients' settings, click 'Additional Recipients' tab and then 'Edit'



- **Send e-mails if Monitoring or Procedure register alerts more than the selected number of consecutive times** - Determines when email alerts should be sent for an issue. For example, if you select 5 from the drop-

down, email alert will be sent only if the same issue is generated 5 consecutive times.

- **Send to the portal administrators** - Emails alerts will be sent to users with 'Administrative' roles.
- **Send to the following e-mail addresses** - Allows you to add external recipients. Enter the email address and press either 'Tab' or 'Enter' button. You can add multiple recipients. To remove a recipient, click the 'X' beside the recipient.
- **Send to the following portal users** - Allows you to add users with 'User' roles. Type the username fully or partly and select from the list. You can add multiple users. To remove a user, click the 'X' beside the name.

Click 'Save' to apply your changes. The alert will be created and displayed in the list. The alerts will be available for selection in the Procedure section and while configuring Monitoring Settings for a Windows profile.

6.5.2. Edit / Delete an Alert

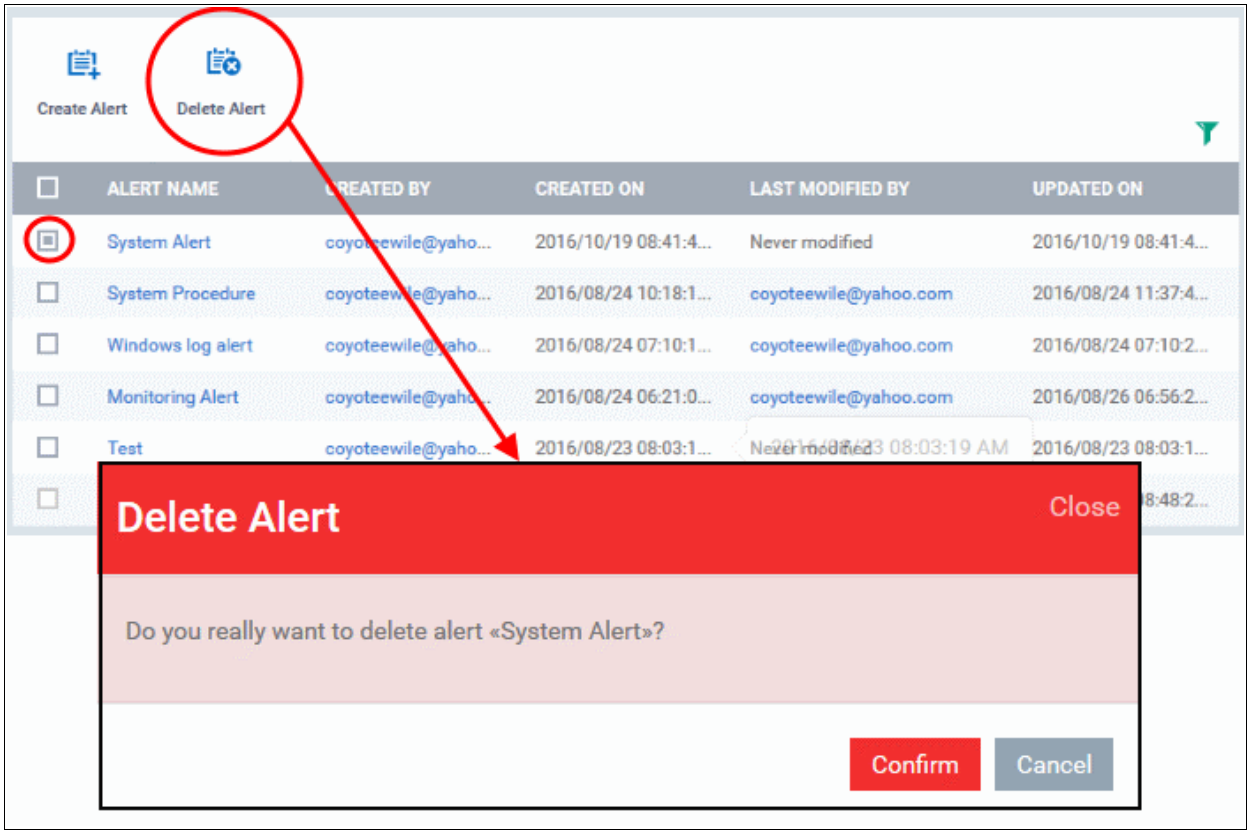
To edit an alert:

- Click 'Configuration Templates' > 'Alerts'
- Click the name of the alert you wish to modify
- Click the 'Edit' button on the right
- You can edit settings in the 'General', 'Alert Settings' and 'Additional Recipients' areas
- See 'Create a New Alert' for more information on the settings in these areas
- Click 'Save' to apply your changes

Before deleting an alert, please consider whether it is currently being used on any Procedures or Monitoring Settings for a Windows profile. Please also investigate whether the alert could be edited rather than deleted.

To delete an alert:

- Click 'Configuration Templates' > 'Alerts'
- Click the name of the alert you wish to delete
- Click the 'Delete' button on the right.
- Click 'Confirm' in the confirmation dialog:



6.6. Managing Procedures

Procedures are standalone instruction scripts and patches for Windows devices. Procedures can be run on an ad-hoc basis or added to a profile. Admins can create procedures to quickly pinpoint and resolve issues and run patches. Features include:

- Select a predefined procedure to be executed on endpoints
- Create custom procedures to be executed on endpoints
- Compose script instructions in Python
- Select Microsoft software updates for a patch procedure
- Associate a defined alert with a specific procedure.
- Combine procedures to build broader procedures.
- Show procedure results in the Execution Log as well as inside particular device
- Import procedures from JSON.
- Export and clone procedures.
- Run procedures on demand by selecting 'Run Over Device'. Can be applied to single devices, multiple devices or all devices.
- Add predefined procedures to Windows device profiles and create schedules for them.

Please use the following links to learn more about procedures:

- Viewing and Managing Procedures
- Create a Custom Procedure
- Combine Procedures to Build Broader Procedures
- Review / Approve / Decline New procedures

- Add a Procedure to a Profile / Procedure Schedules
- Import / Export / Clone Procedures
- Change Alert Settings
- Directly Apply Procedures to Devices
- Edit / Delete Procedures
- View Procedure Results

6.6.1. Viewing and Managing Procedures

- Click 'Configuration Templates' > 'Procedures' to open the procedures interface.

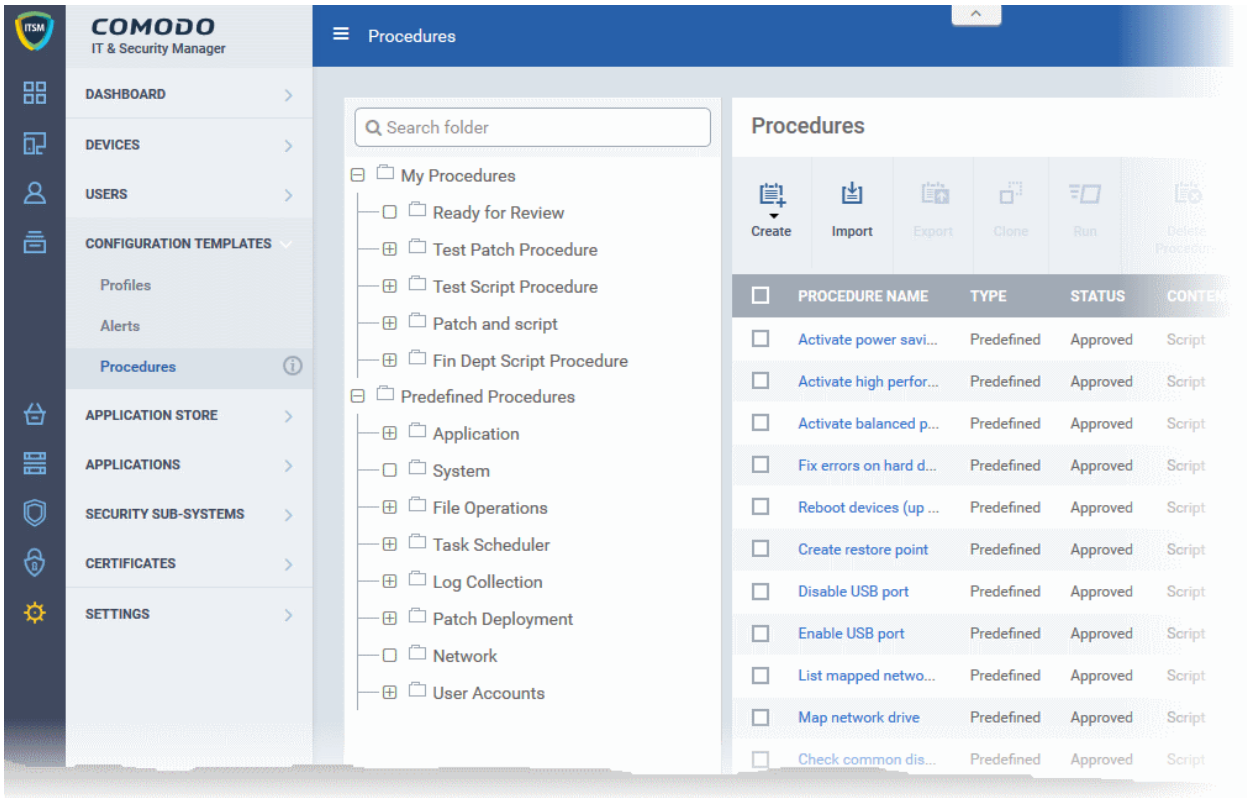
'Procedures' are available in two categories which are shown in folders on the left - predefined procedures and custom procedures ('My Procedures').

ITSM ships with two types of predefined procedures - Script and Patch.

- The folders 'Application', 'System', 'File Operations', 'Task Scheduler', 'Log Collection', 'Network' and 'User Accounts' contain scripts to execute many useful tasks.
- The 'Patch Deployment' folder contains procedures to install Windows OS patches onto Windows endpoints.

Predefined procedures cannot be edited. Guidance on creating a custom procedure can be found in Create a Custom Procedure.

The procedures interface lists all existing custom and predefined procedures. Click the funnel icon on the right to filter procedures by various criteria.



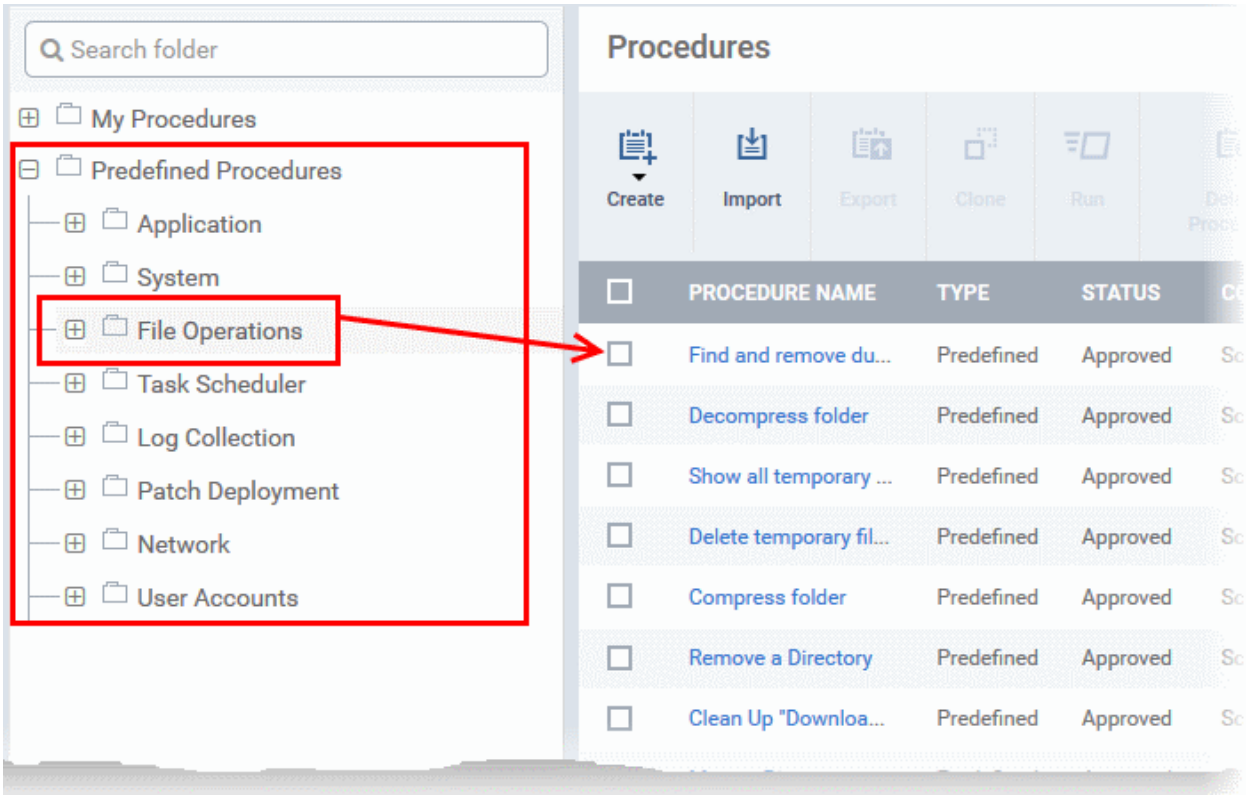
Procedures - Column Descriptions	
Column Heading	**Description**
Procedure Name	The name of the procedure

Type	Indicates whether the procedure is a custom or a predefined procedure.
Status	Indicates the status of the procedure. The statuses are: • Created • Edited • Ready to review • Approved • Declined
Content Type	Indicates whether the procedure is script or patch.
Created by	Displays the name of the administrator who created the custom procedure. Clicking the name of the administrator will open the 'Personal' pane, displaying the details of the Administrator. Refer to the section Viewing the details of the User for more details.
Created On	The date and time at which the procedure was created.
Last Modified By	The details of the administrator that modified by the procedure last.
Updated On	The date and time at which the procedure was last updated.
Controls	
Create	Allows to create custom script and patch procedures. Refer to the section 'Create a Custom Procedure' for more details
Import / Export / Clone	Allows administrators to import a saved procedure, export a procedure and clone an existing procedure. Refer to the section 'Import / Export / Clone Procedure' for more details.
Run	Allows administrators to run a procedure on Windows device(s) instantly. Refer to the section 'Directly Apply Procedures to Devices' for more details.
Delete Procedure	Allows administrators to delete procedure(s).

To view the sub-categories of 'Predefined Procedures':

- Click 'Predefined Procedures' in the folder pane on the left
- Click a category folder to view procedures related to the category.

Procedures are shown on the right:



The following table lists all predefined categories and procedures:

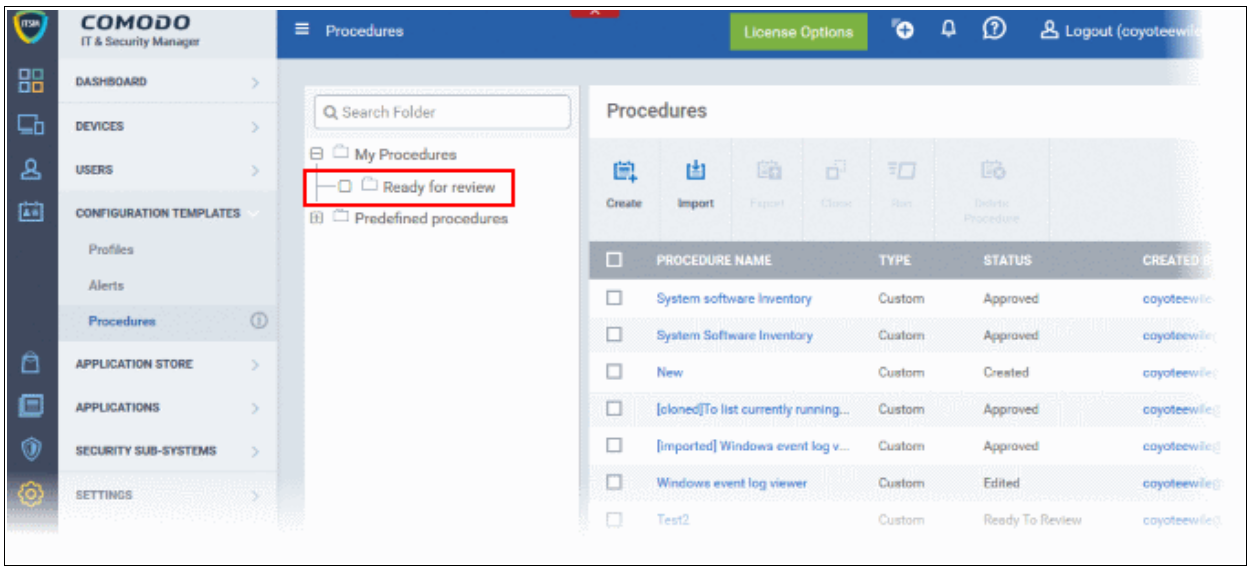
Category	Procedures
Application	Installing/uninstalling applications, kill running applications, get details on running applications, processes, servers and more.
System	Rebooting devices, create restore point, enable/disable USB ports, mapping network drives, running disk defragmentation, fixing disk errors and more.
File Operations	Copy, move/delete files/folders, find and remove duplicate files, compress/decompress folders, clean up temporary files and downloaded files and more.
Task Scheduler	Creating new tasks and schedule them, run tasks and more.
Log Collection	Contains procedures for obtaining various system logs.
Patch Deployment	Installation and update of OS patches of different categories.
Network	View TCP/IP settings, save/restore network configurations, clear DNS cache and more
• User Accounts	Add/remove domain user to a group, enable/disable user access control (UAC), get UAC status and more

Any predefined procedure can be cloned and edited to create a custom procedure. Refer to the following sections for more details.

- Import / Export / Clone Procedures
- Editing Procedures
- Add a Procedure to a Profile / Procedure Schedules

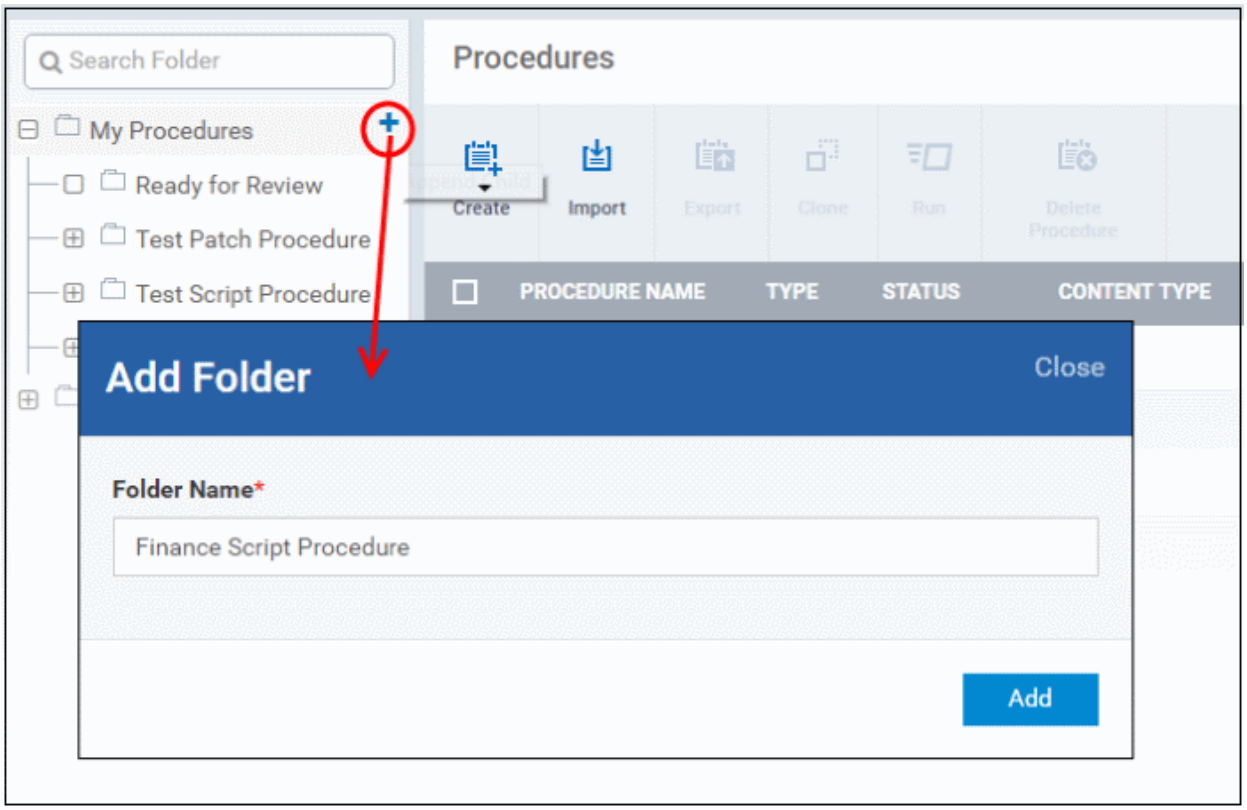
To view 'My Procedures':

- Click 'Configuration Templates' > 'Procedures'. Expand the 'My Procedures' folder. Each folder has sub-folders which display procedures under specific categories (for example, 'Ready for review').



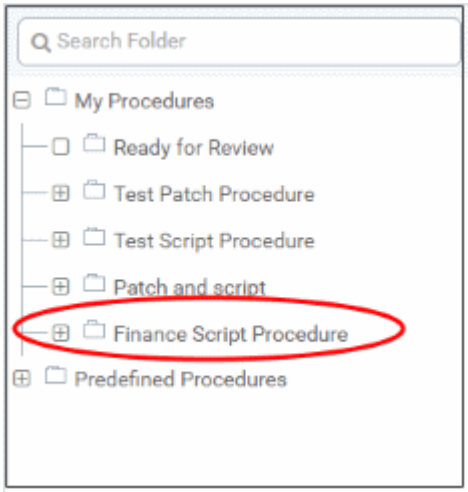
To add a sub folder to the My Procedures folder:

- Place your mouse on the 'My Procedures' folder and click '+' beside it



- Enter a name for the sub-folder to be created in the 'Add Folder' dialog and click 'Add'

The sub-folder will be created and displayed under 'My Procedures'



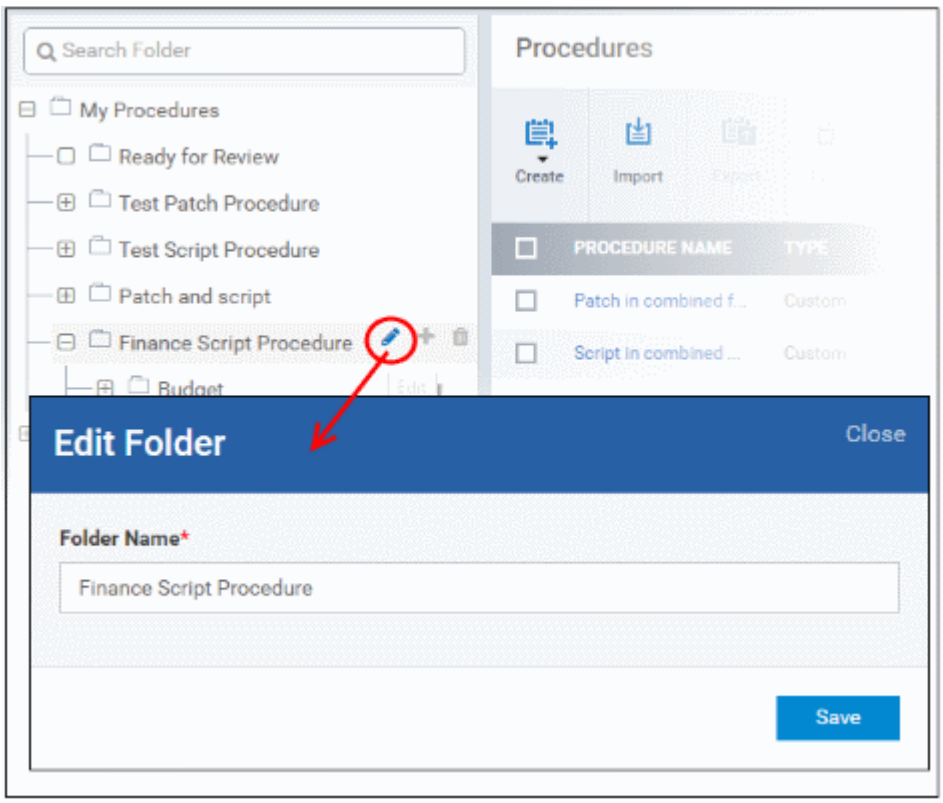
You can also add sub-folders of a sub-folder. Once sub folders are created, you can create new procedures inside them or import/clone predefined procedures.

These section explain more about these processes:

- Creating a new procedure
- Importing/Exporrting/Cloning a procedure
- Editing Procedures

To edit the name of a sub folder under 'My Procedures'

- Place your mouse on the sub folder and click the pencil symbol beside it
- Enter a new name for the sub folder in the Edit Folder dialog and click 'Save'

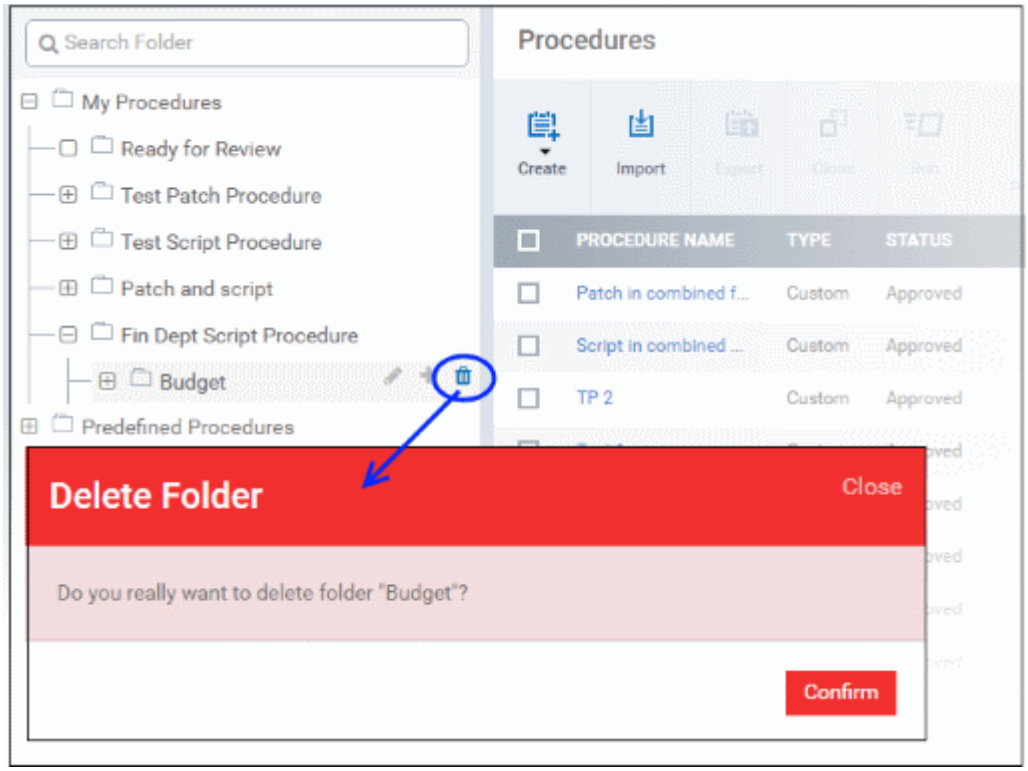


The folder name will be updated in folder tree.

Note: You cannot edit or delete the 'Ready for Review' folder.

To delete a sub folder under 'My Procedures' folder:

- Place your mouse on the sub folder and click the trash can symbol beside it



- Click 'Confirm' to update the tree.

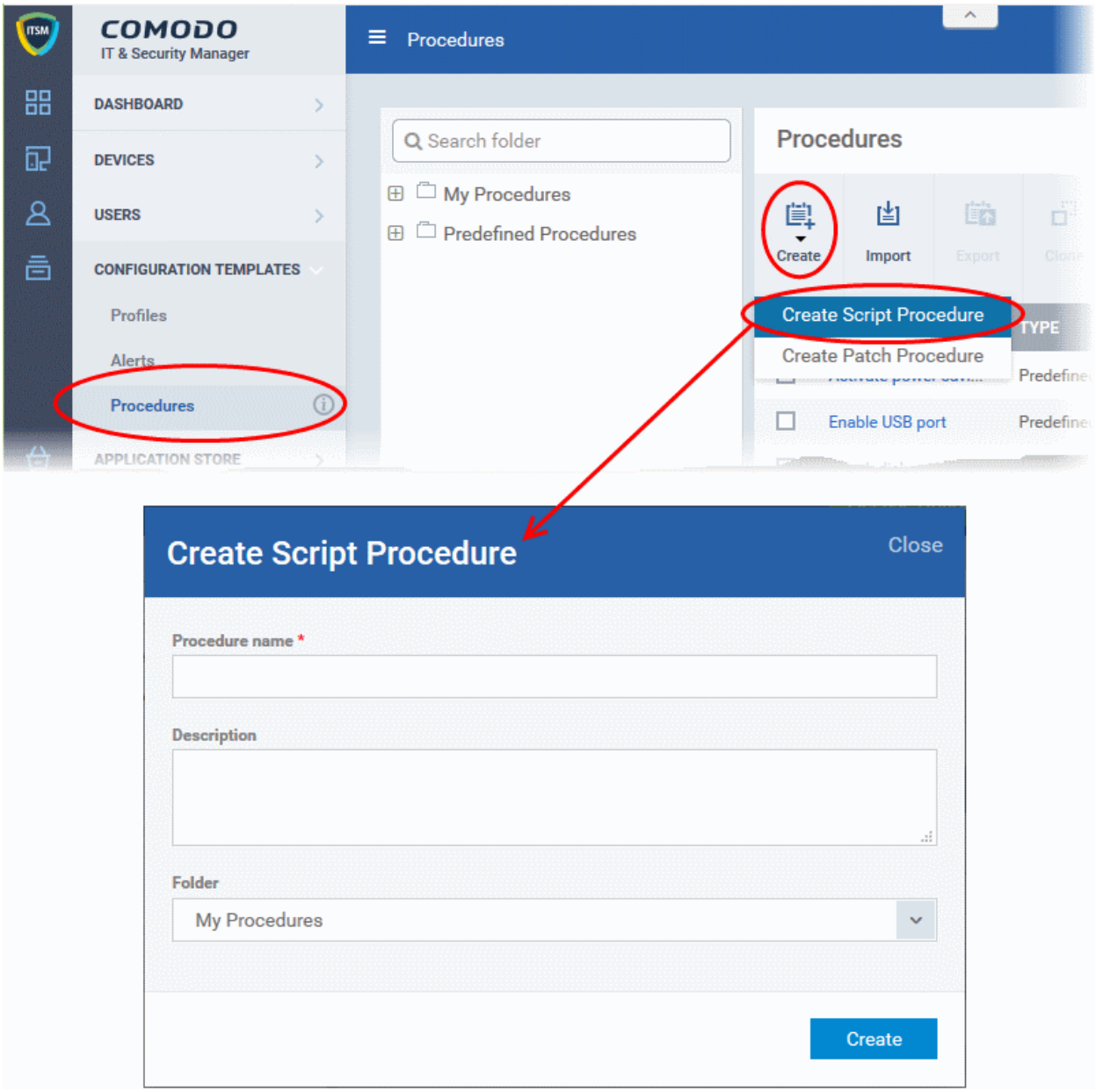
6.6.2. Create a Custom Procedure

ITSM allows you to create custom script / patch procedures according to your requirements. Click the following links to find out more:

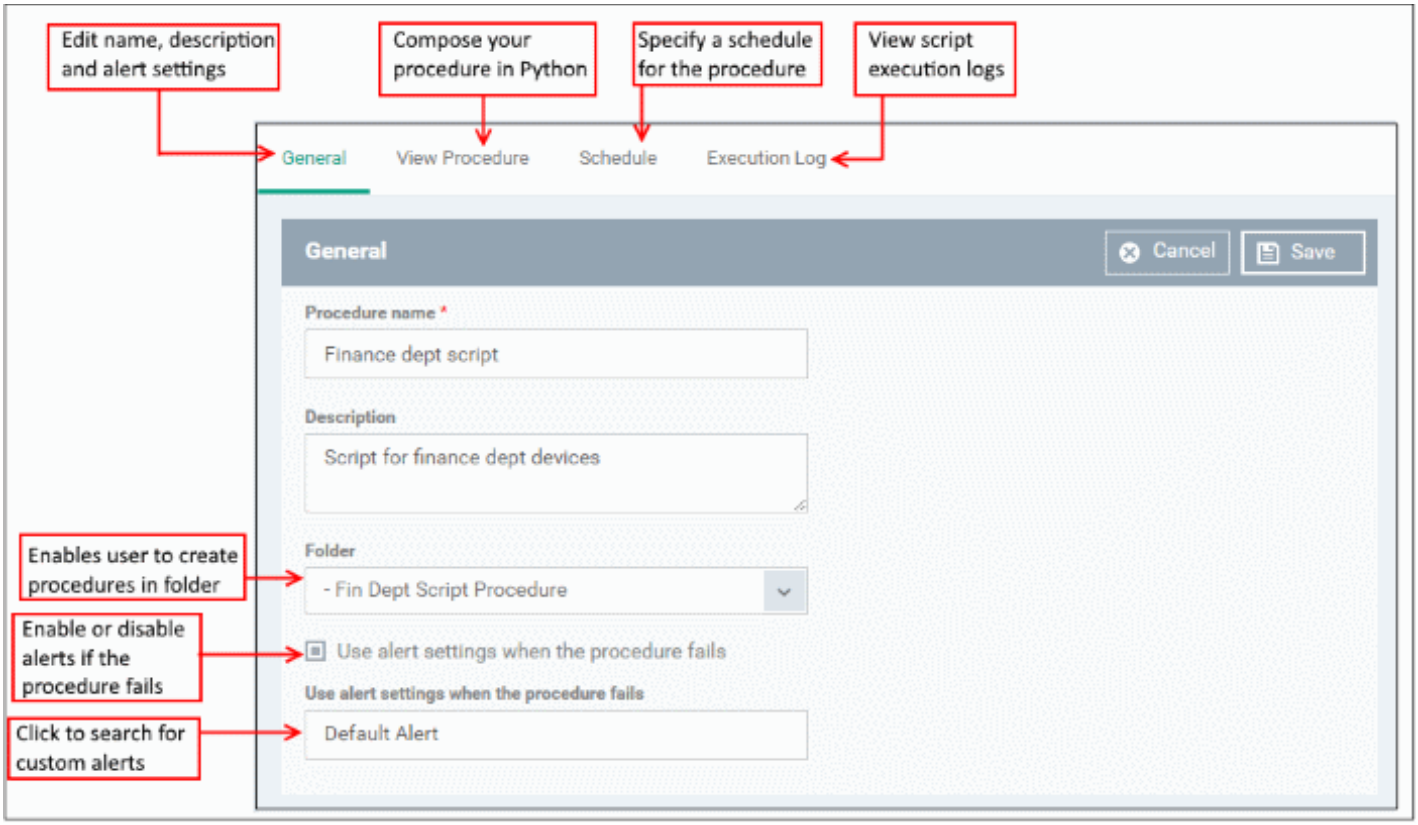
- Creating a custom script procedure
- Creating a custom patch procedure

To create a custom script procedure

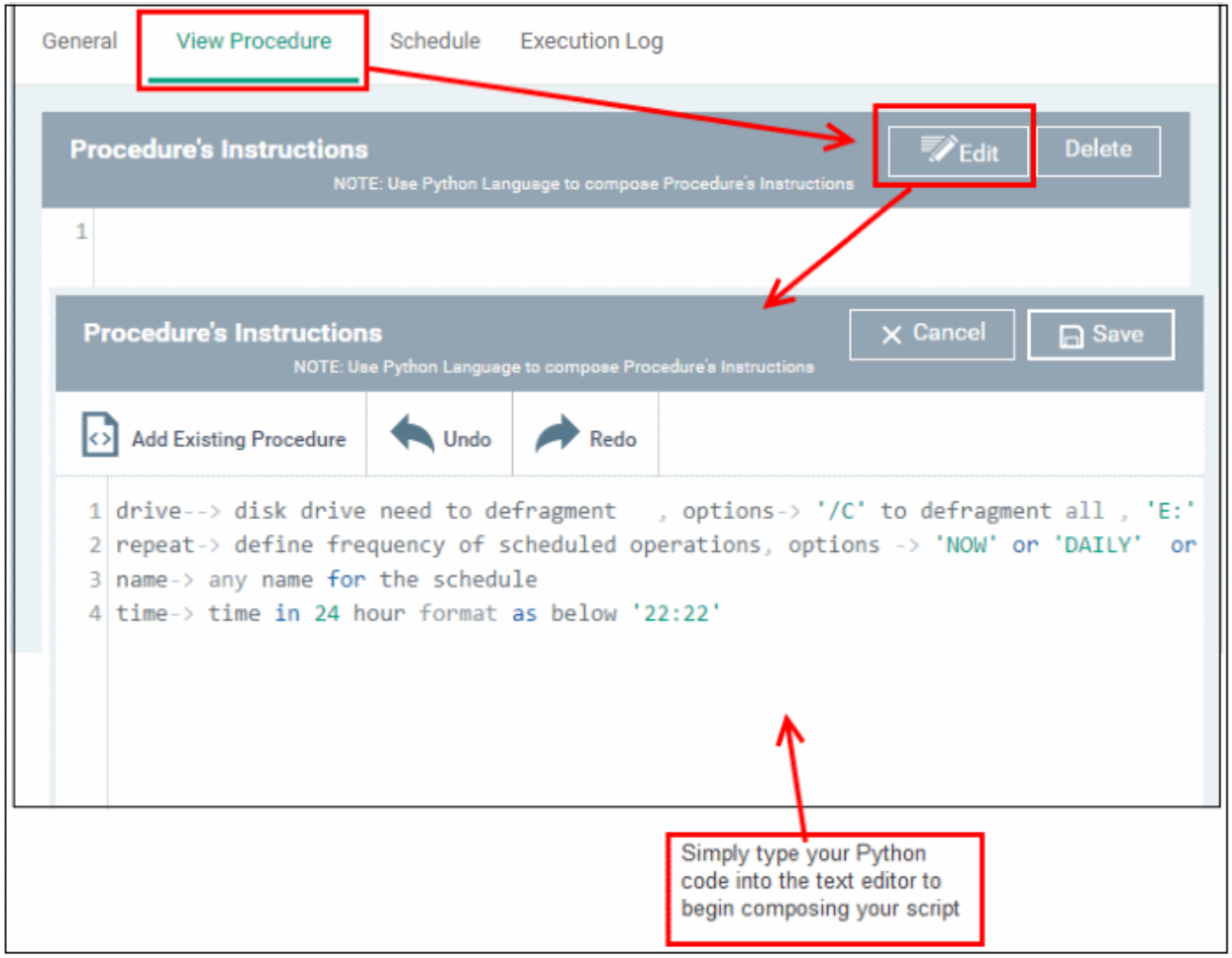
- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create Script Procedure'



- Enter a name and description for your script procedure and specify the folder in which you want it to be saved. After saving, you will be taken to the procedure configuration screen. The 'General' section allows you to modify basic settings:



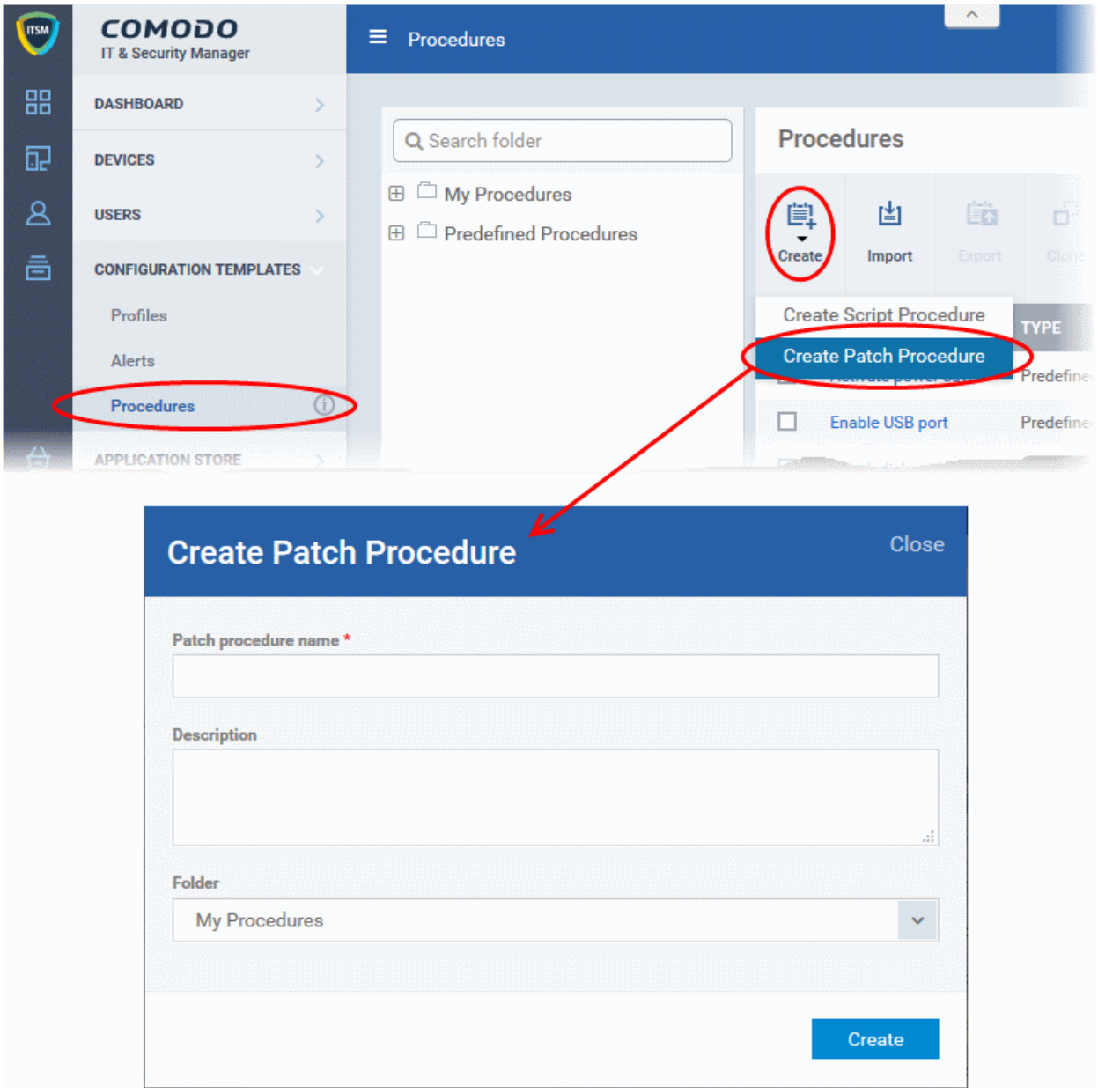
- To define a Python script for your procedure, click the 'View Procedure' tab followed by the 'Edit' button. You can create a custom script using the built-in text editor:



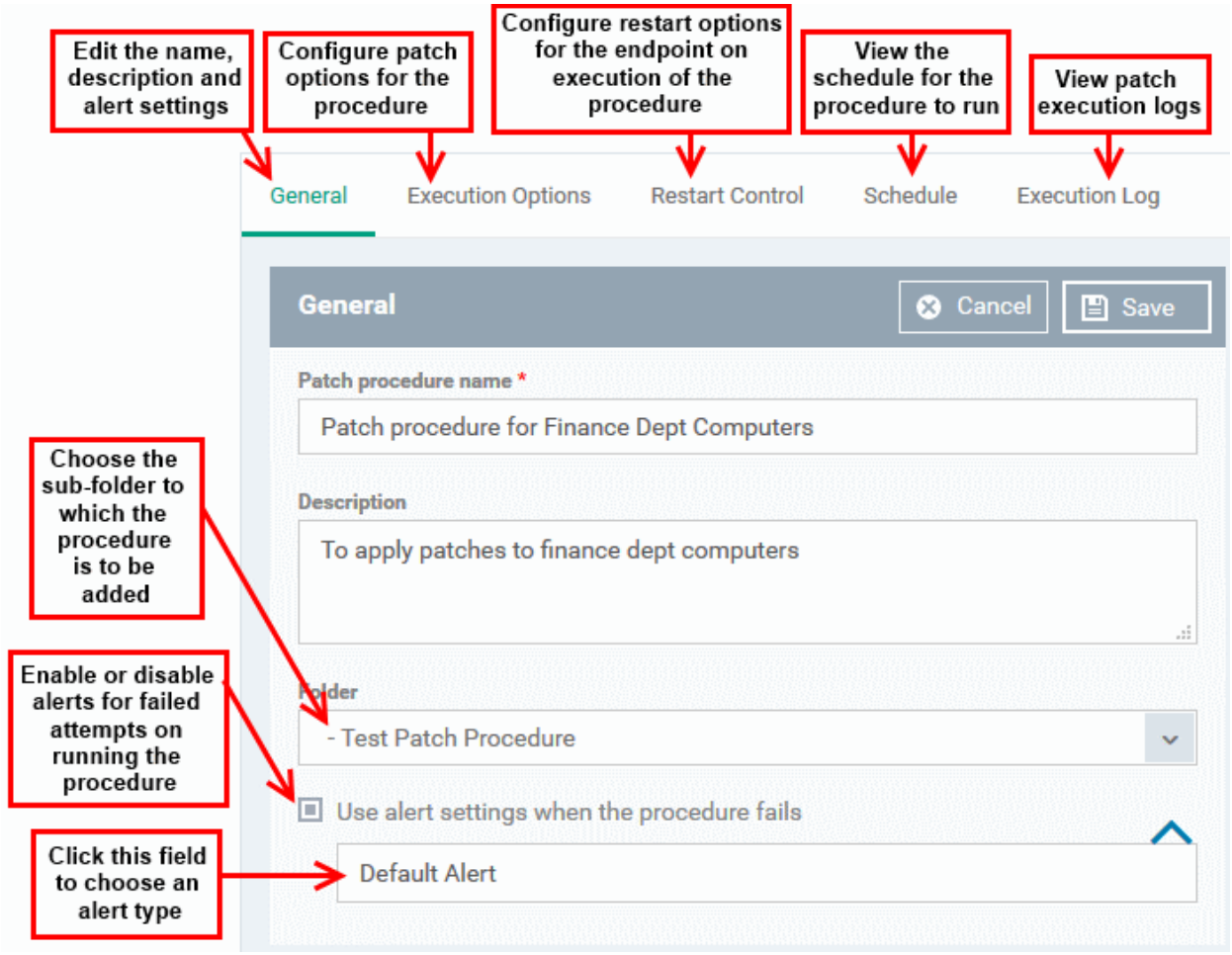
- After saving your script you need to approve it before it can be deployed in a profile.
- The 'Schedule' tab will be auto-populated once you deploy the procedure to a configuration profile and create a schedule for the procedure to run in the profile. Refer to the section Add a Procedure to a Profile / Procedure Schedules for more details.
- The 'Execution Log' tab will be auto-populated upon successive execution of the procedure on the end-points to which the configuration profile with this procedure component. You can view the history of execution of this procedure at anytime by selecting this procedure from the Procedures interface and clicking the 'Execution Log' tab.
- Note 1. The MSP forum has a free script library which contains Python scripts submitted by community members and the Comodo development team - https://forum.mspconsortium.com/forum/script-library. Feel free to try any script that fits your needs, or submit your own scripts for other members to use.
- Note 2. You can also use the Import and Clone features if you wish to create a new procedure using an existing procedure as a starting point

To create a custom patch procedure

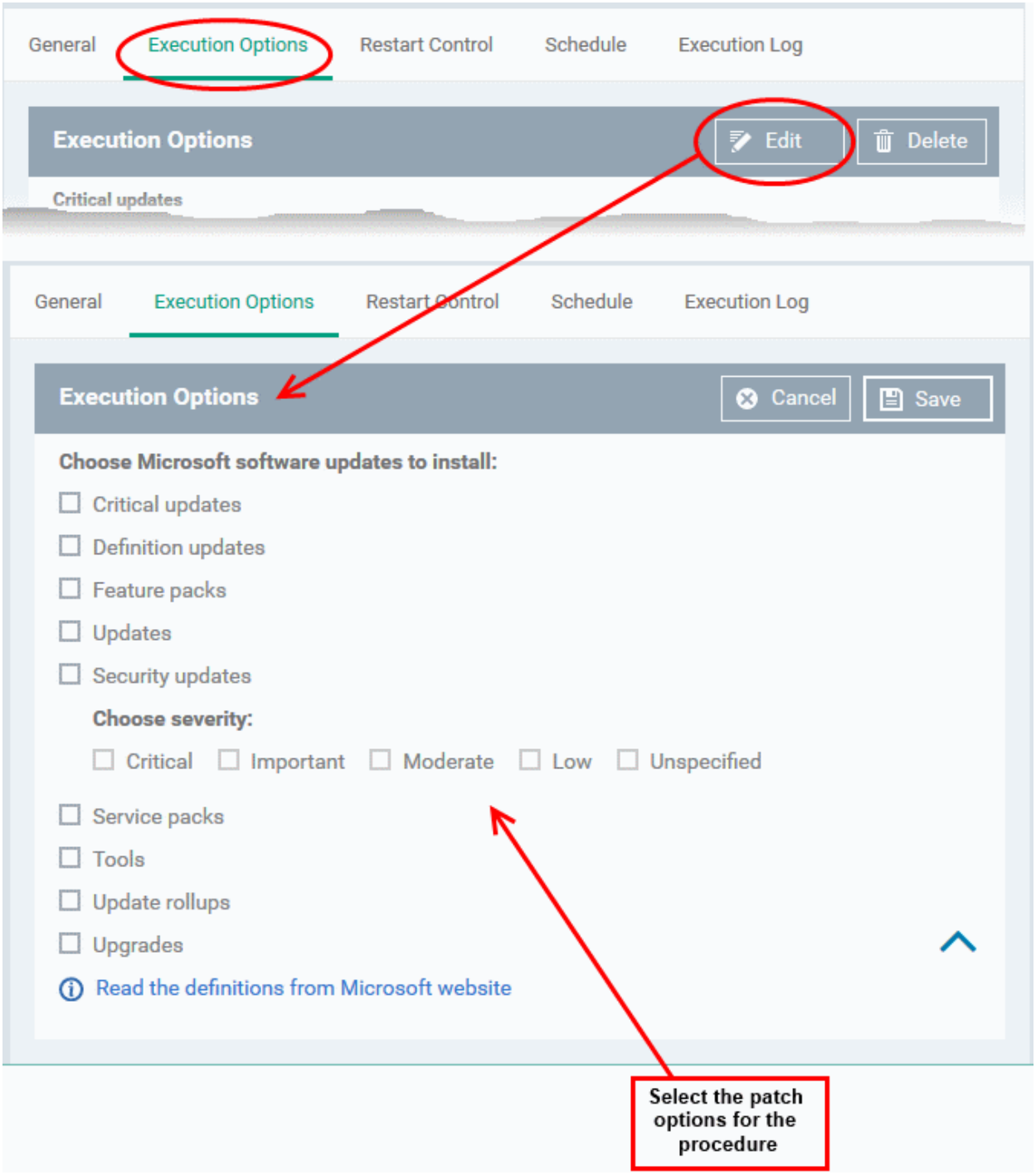
- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create Patch Procedure'



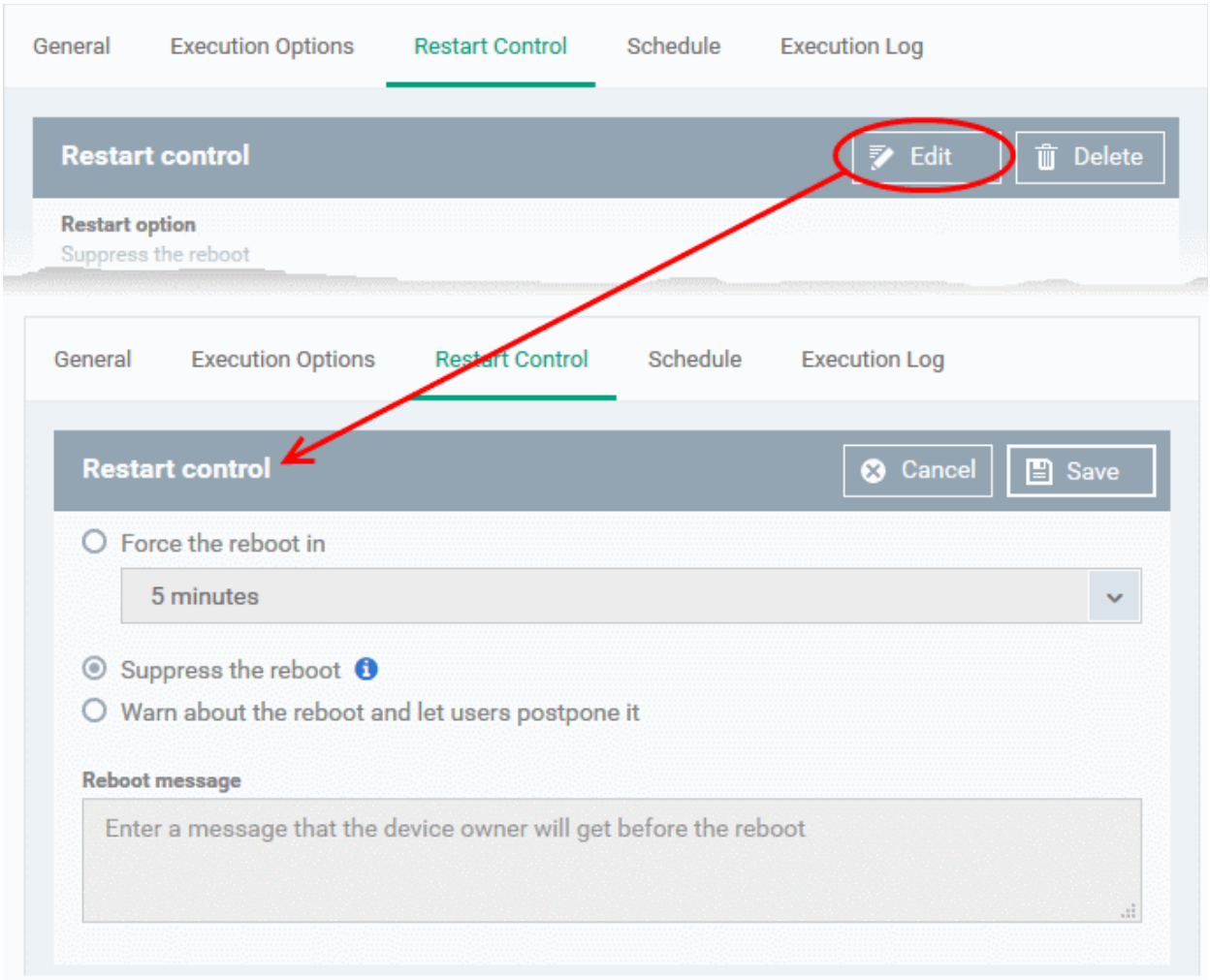
- Enter a name and description for your patch procedure and specify the folder in which you want to save it. After saving, you will be taken to the procedure configuration screen with the 'General' section open:



- To configure patch options for your procedure, click the 'Execution Options' tab followed by the 'Edit' button. You can select the Microsoft software updates required for the procedure from the options.



- Click the link 'Read the definitions from Microsoft website' link to view patch details.
- Choose which types of patch the procedure should install and click 'Save'
- Click the 'Restart Control' tab followed by the 'Edit' button to configure restart options for the endpoint after the procedure has run successfully.



- You can choose to:
  - Continue the operation of the endpoint without restart by selecting 'Suppress the reboot'
  - Force restart the endpoint a certain period of time after the procedure has completed.

    OR
  - Display a warning to the user and let them postpone the restart. Type a message for the user if you choose this option.
- The 'Schedule' tab will be auto-populated once you add the procedure to a configuration profile and schedule its execution. See Add a Procedure to a Profile / Procedure Schedules for more details.
- The 'Execution Log' will be auto-populated after the procedure has been successful executed as part of a profile. You can view a history of executions at anytime by selecting this procedure in the 'Procedures' interface and clicking the 'Execution Log' tab.
- After saving your patch procedure you need to approve it before it can be deployed in a profile.

Important Note: Patches that are hidden by administrators will not be executed. Refer to the section ' Installing OS Patches on Windows Endpoints' for more details.

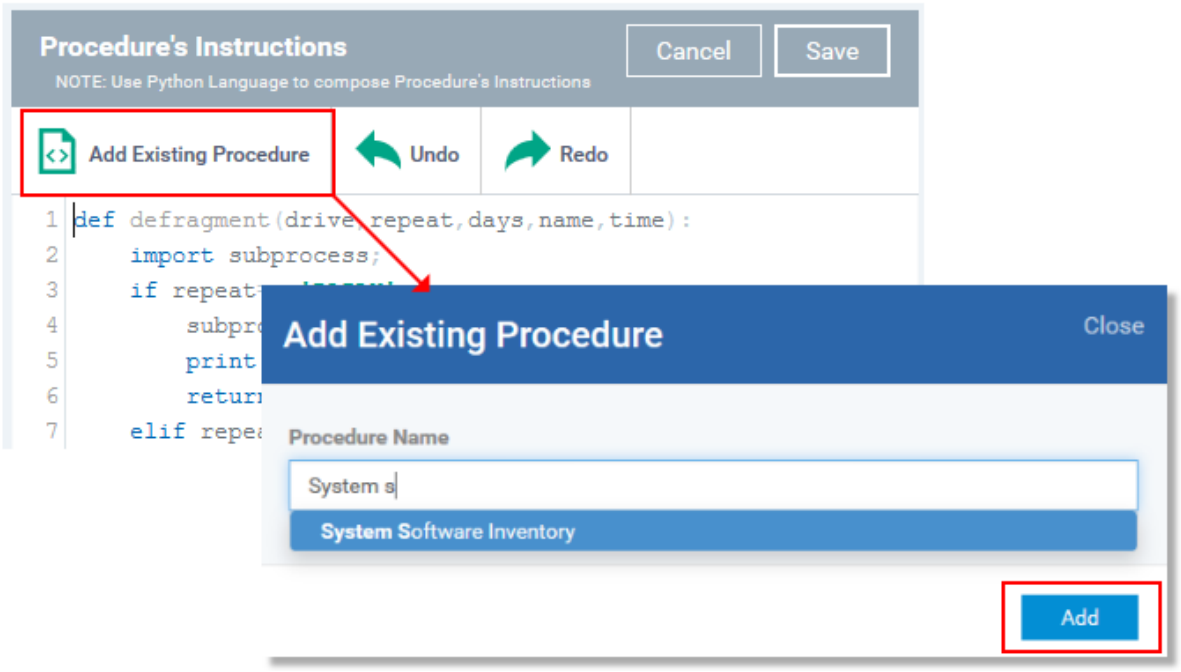
6.6.3. Combine Procedures to Build Broader Procedures

Please note this is applicable only for script procedures - not patch procedures.

To incorporate a script from another procedure:

- Open your custom procedure and click the 'View Procedure' tab, then click 'Edit' on the right

- Position your mouse cursor at the place in your script where you wish to add the new code
- Click 'Add Existing Procedure'
- Type the name of the procedure whose script you want to import
- Click 'Add'. The code will be added to your existing script at the place you specified.
- You can, of course, subsequently modify the script as required.



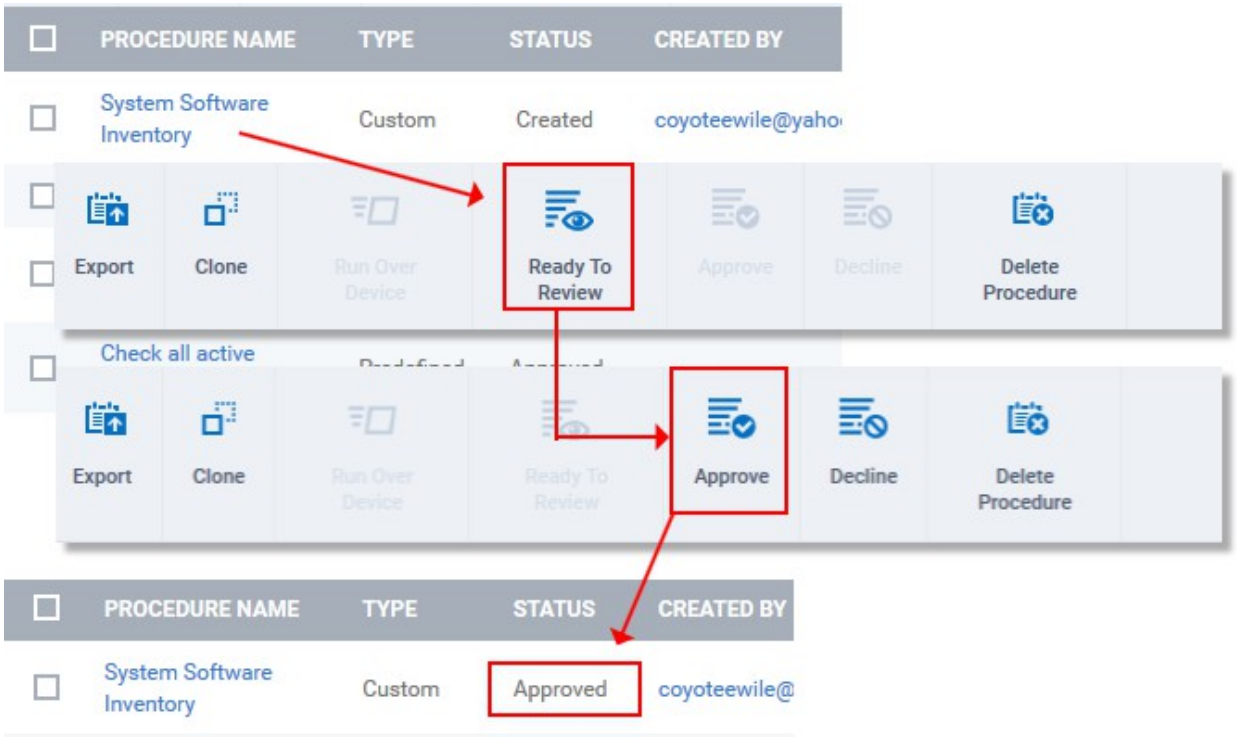
- Click 'Save' for your changes to take effect.

6.6.4. Review / Approve / Decline New Procedures

New custom script procedures are given an initial status of 'Created'. Custom script procedures must be approved for them to become available for inclusion in a profile. New custom patch procedures do not require any approval and are automatically approved after creation.

To access the review features:

- Open a custom script procedure
- Click 'Ready to Review'.
  - This will notify *authorized* administrators that a procedure requires approval
  - If you are an *authorized* administrator, it will also activate the 'Approve' and 'Decline' buttons
- Click 'Approve' if you wish to commit this script and make it available for selection in profiles
- Click 'Decline' if you do not wish to commit this script.



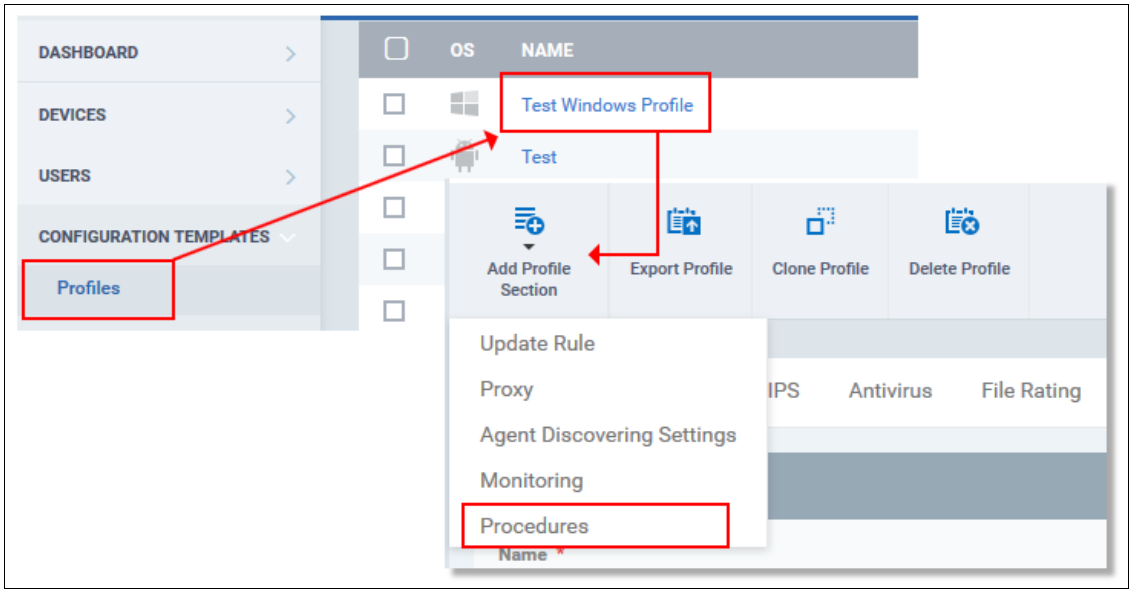
- Approved procedures can be selected and added to a profile.

6.6.5. Add a Procedure to a Profile / Procedure Schedules

Note. Procedure schedules for both script and patch procedures are actually configured in the 'Profiles' area. You set a schedule for a procedure when you add a procedure to a profile. The 'Schedule' tab in the procedures area essentially allows you to view profiles which are scheduled to use the procedure.

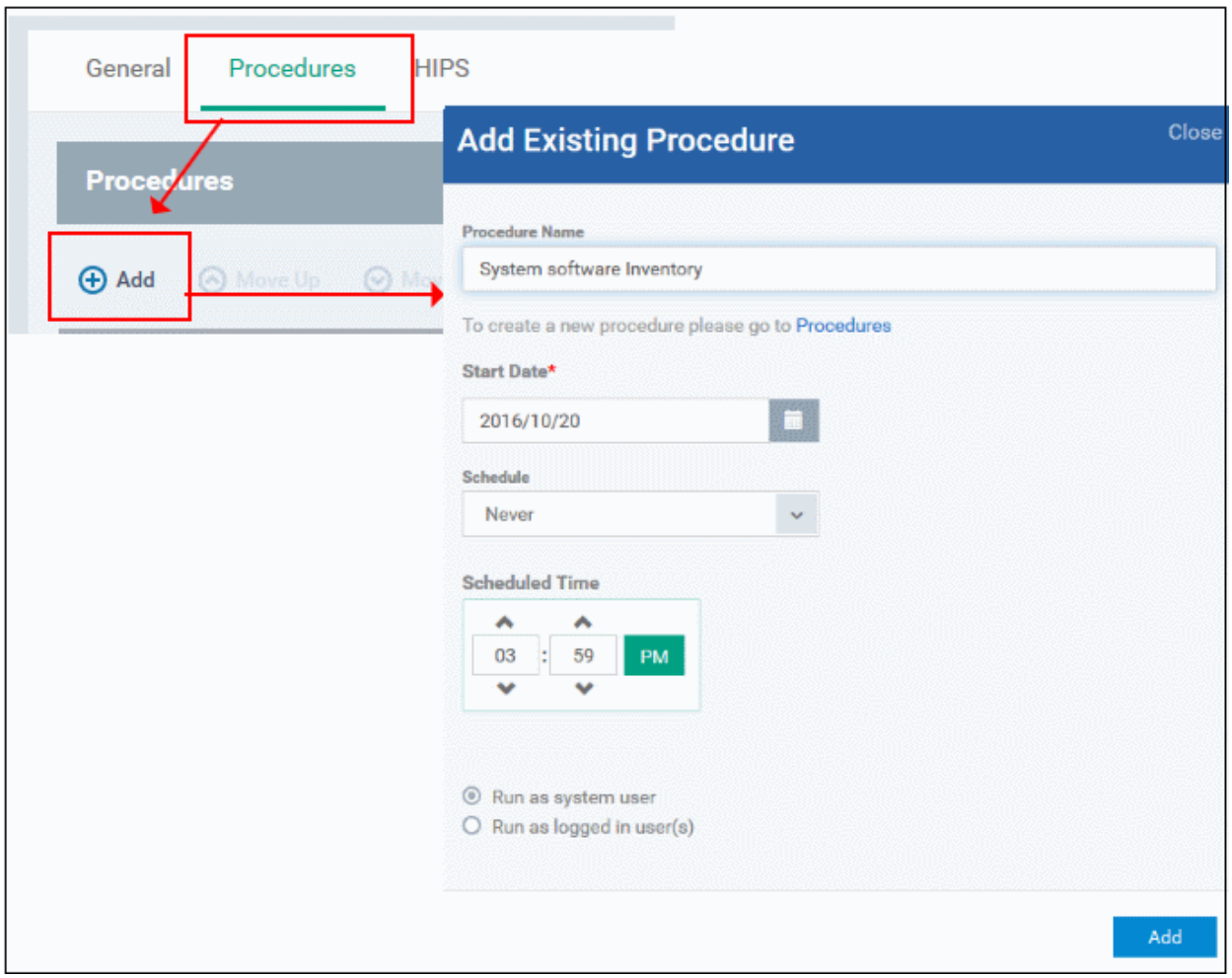
To add and schedule a procedure:

- Click 'Configuration Templates' > 'Profiles'
- Click the profile to which you want to add a procedure
- Click 'Add Profile Section' > 'Procedures':

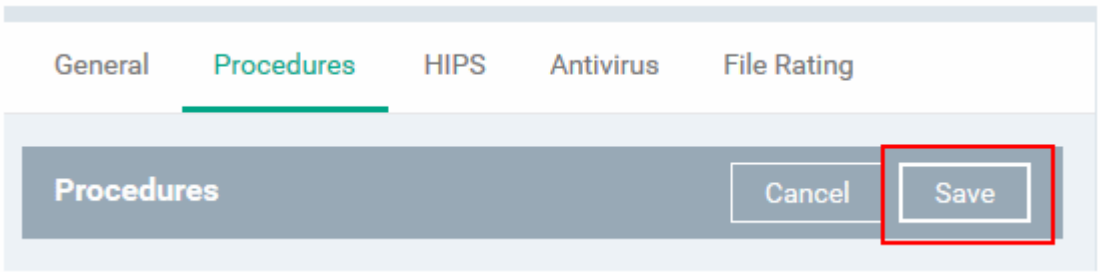


- This will add a 'Procedures' tab to the profile.

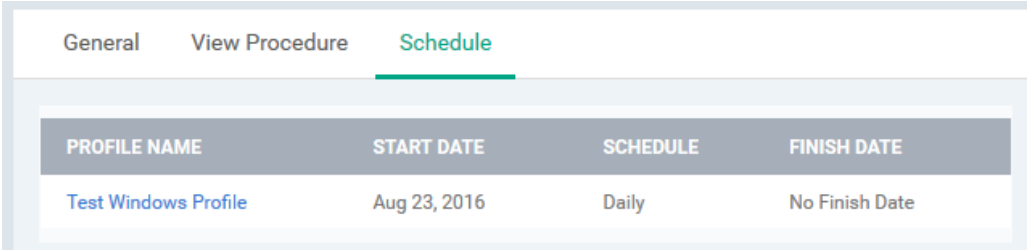
- Click the 'Add button' to open the procedure configuration screen



- Type the name of the procedure that you want to add to the profile (make sure you have approved the procedure)
- Set the date and time on which you want the procedure to start running.
- Set whether you want the procedure to run daily, weekly or monthly (or never)
- For weekly and monthly schedules, set the day of the week on which you want the procedure to run.
- Choose 'Run as system user' or 'Run as logged in user' based on the access rights required for the procedure to run at the endpoint.
- Click 'Add'.
- Finally, click 'Save' to apply the procedure and the schedule to the profile:



- The 'Schedule' tab of the procedure interface will list all profiles which have this procedure scheduled:



Important Note: Patches that are hidden by administrators will not be executed. Refer to the section '**Installing OS Patches on Windows Endpoints**' for more details.

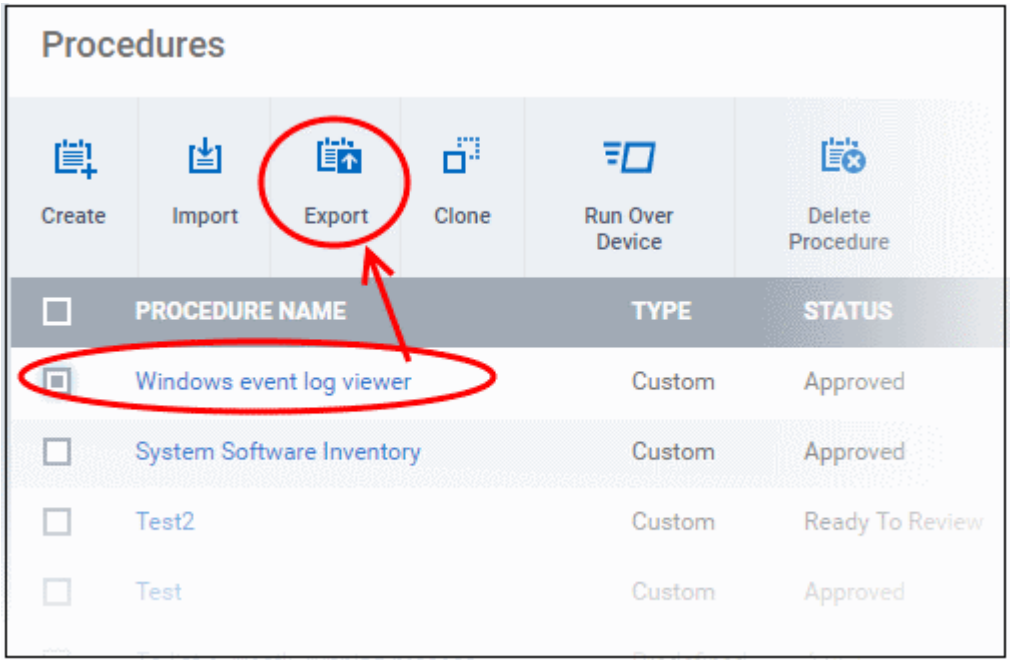
6.6.6. Import / Export / Clone Procedures

ITSM allows you to export or import procedures in order to use them in profiles. The procedure files are saved in .json format. You can also clone a procedure and use it as a starting point to create a new procedure according to your requirements. Click the following links to find out more:

- **Export a procedure**
- **Import a procedure**
- **Clone a procedure**

To export a procedure

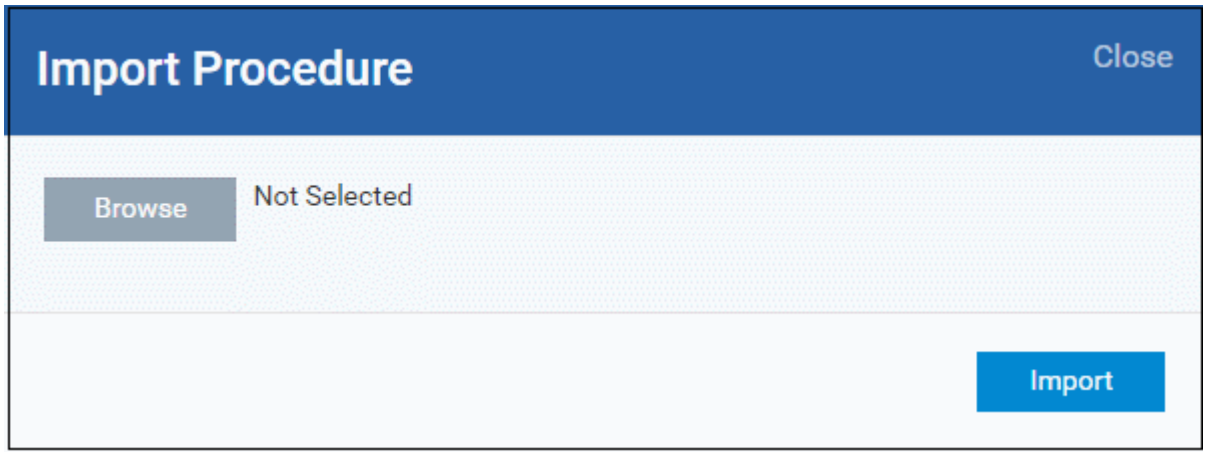
- Click 'Configuration Templates' > 'Procedures'
- Select the procedure and click 'Export' at the top. Please note you can export only custom procedures.



The selected procedure file will be saved in your default download location.

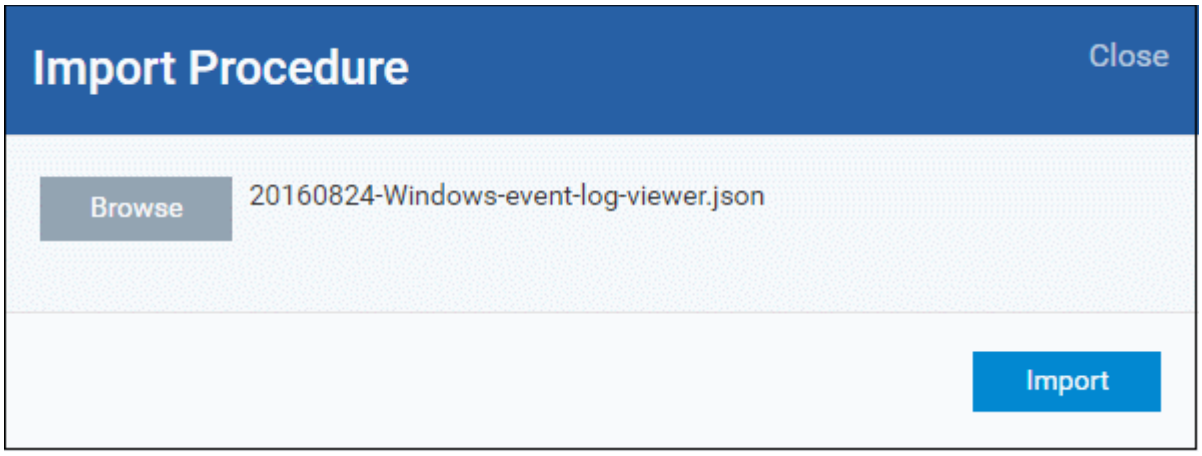
To import a procedure

- Click 'Configuration Templates' > 'Procedures'
- Click 'Import' at the top



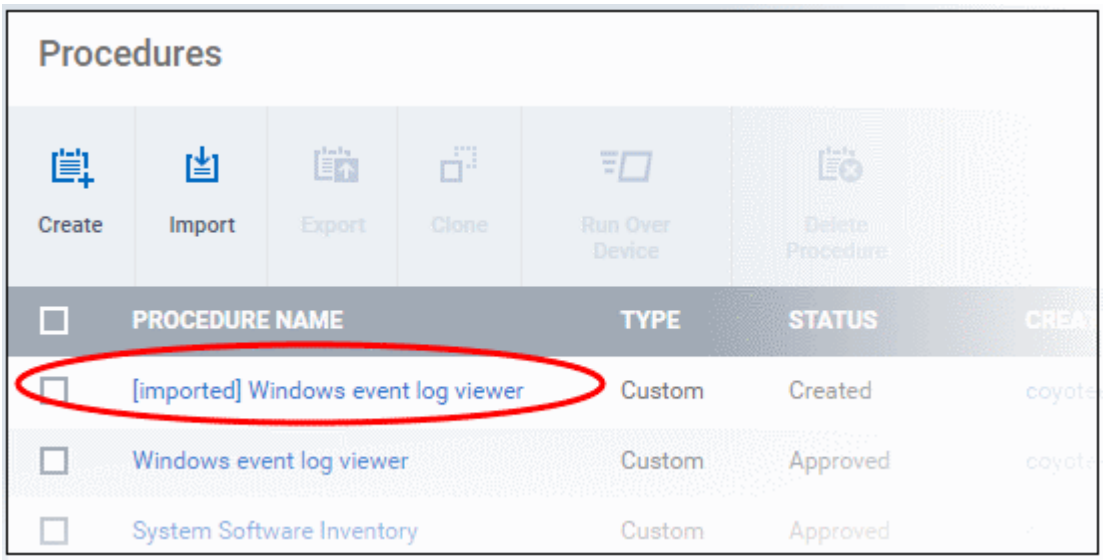
- Click 'Browse', navigate to the location where the procedure file is saved and click 'Open'

The selected file will be displayed on the 'Import Procedure' dialog.



- Click 'Import'

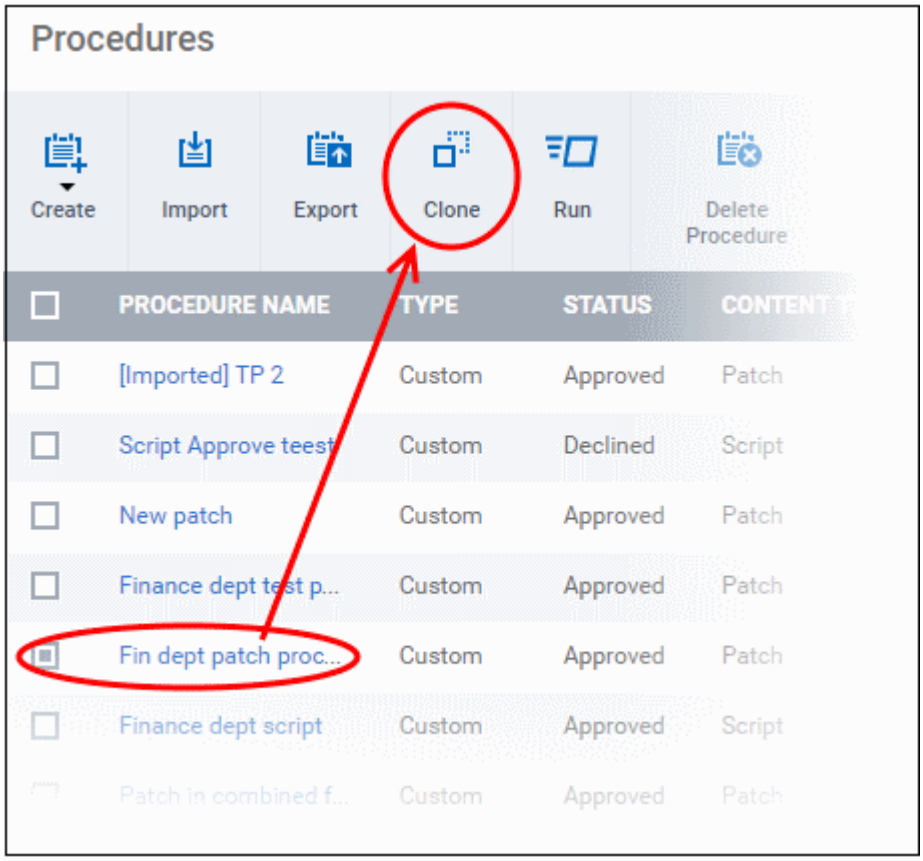
The procedure will be added to the list with the word 'Imported' to distinguish it from other procedures.



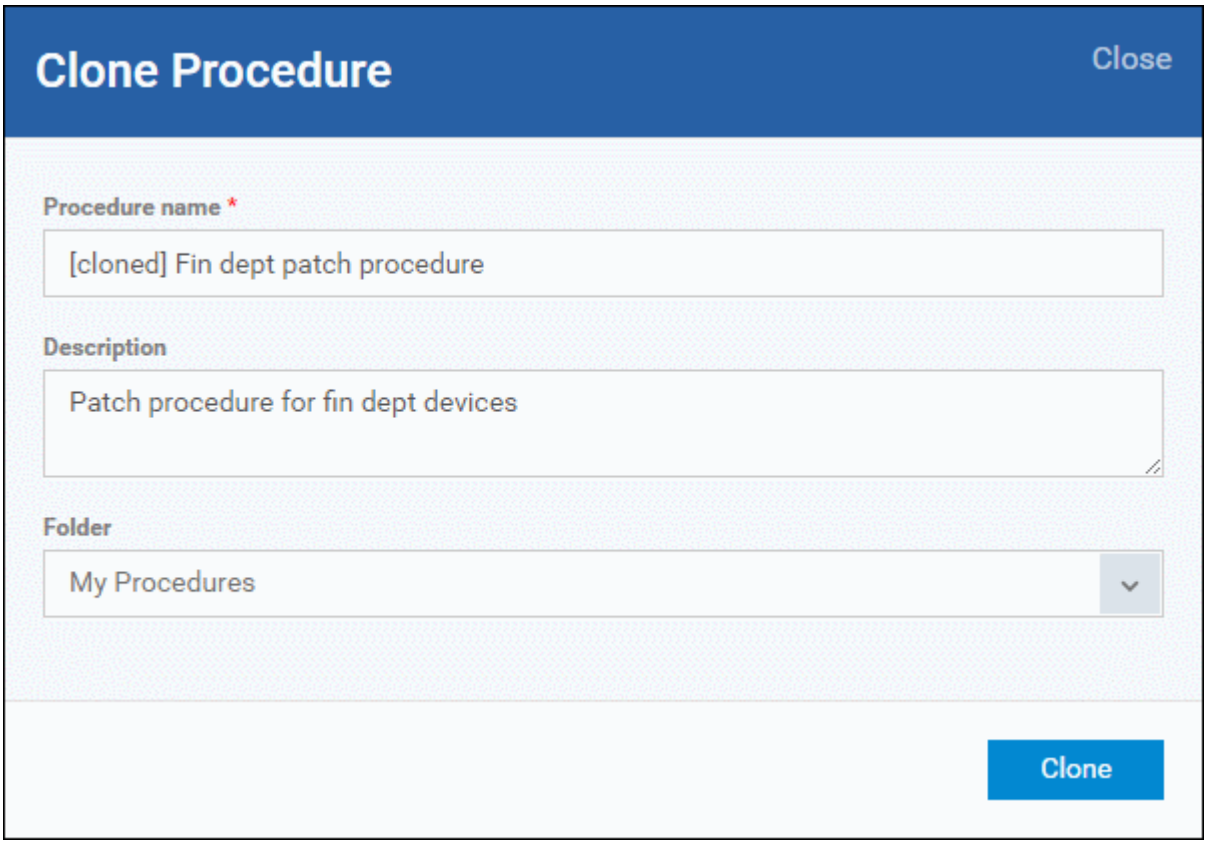
Please note you have to approve the imported procedure in order to deploy it in profiles. To change the name and/or edit the script, click on the procedure and then click 'Edit' button on the right. Refer to the section 'Edit / Delete Procedures' for more details.

To clone a procedure

- Click 'Configuration Templates' > 'Procedures'
- Select the procedure and click 'Clone' at the top.

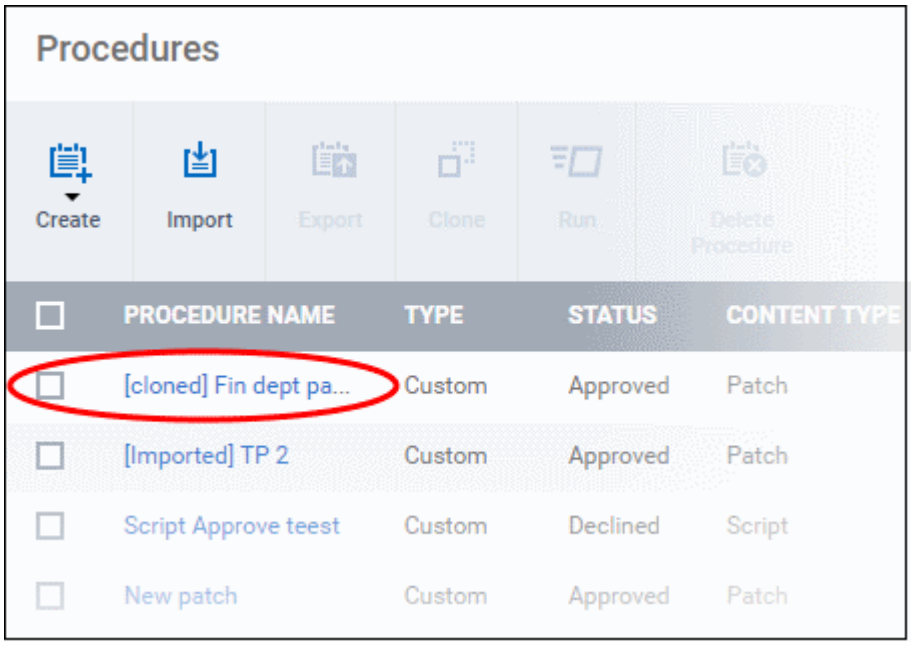


The 'Clone Procedure' dialog will be displayed with name of the selected procedure auto filled in the name field.



- Change the name, if required, and provide an appropriate description of the profile
- Select the folder in which the cloned procedure is to be placed
- Click 'Clone'

The procedure will be added to the list:



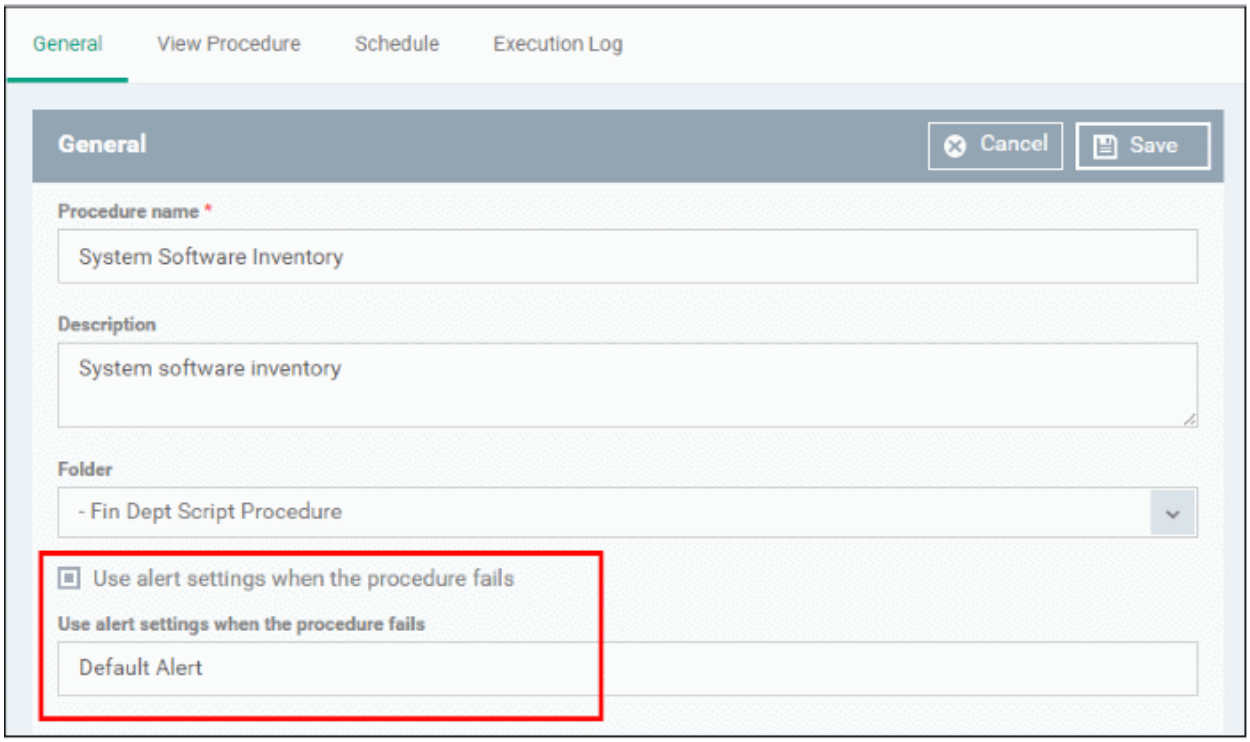
Please note the status of the cloned procedure will be same as that of the procedure that was cloned. For example, if the status was approved then the cloned procedure will also be of the same status. Please note the procedure has to be approved in order to deploy it in profiles.

6.6.7. Change Alert Settings

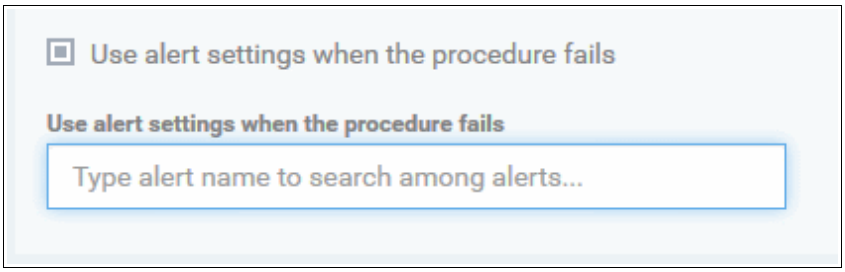
ITSM is capable of issuing alerts when procedures fail to execute as intended. You can set the type of alert shown while you are creating a new procedure, or by editing an existing procedure. Please note you can only select alerts that are already created in the 'Alerts' section. Refer to the section 'Managing Alerts' for more details.

To change alert settings

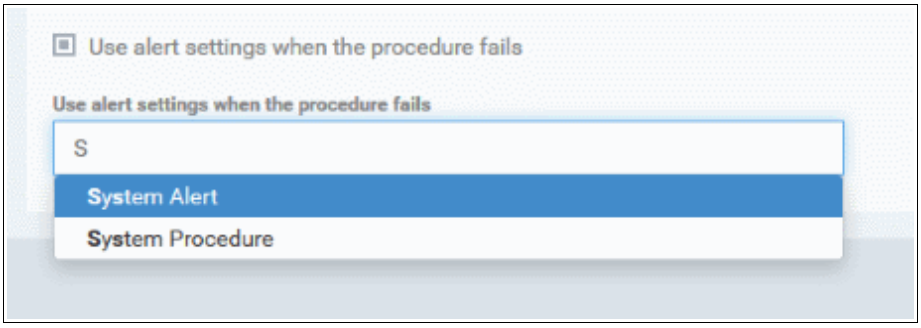
- Click 'Configuration Templates' > 'Procedures'
- Open the procedure whose alert you wish to modify and click 'Edit' on the right. The alert settings will be available under the 'General' tab.



- Make sure the 'Use alert settings when the procedure fails' check box is selected.
- The current alert name will be displayed in the field. Click on the field and type the name of alert that you want to add here. You can create and view alerts in 'Configuration Templates' > 'Alerts'. See 'Managing Alerts' for help with this.



- Enter fully or partly the name of the predefined alert in the field. Matching alerts will be displayed.



- Select the alert and click 'Save' at the top right.

The alert changes will be applied to the profiles also that are using this procedure.

6.6.8. Directly Apply Procedures to Devices

Procedures can be run on devices in three ways:

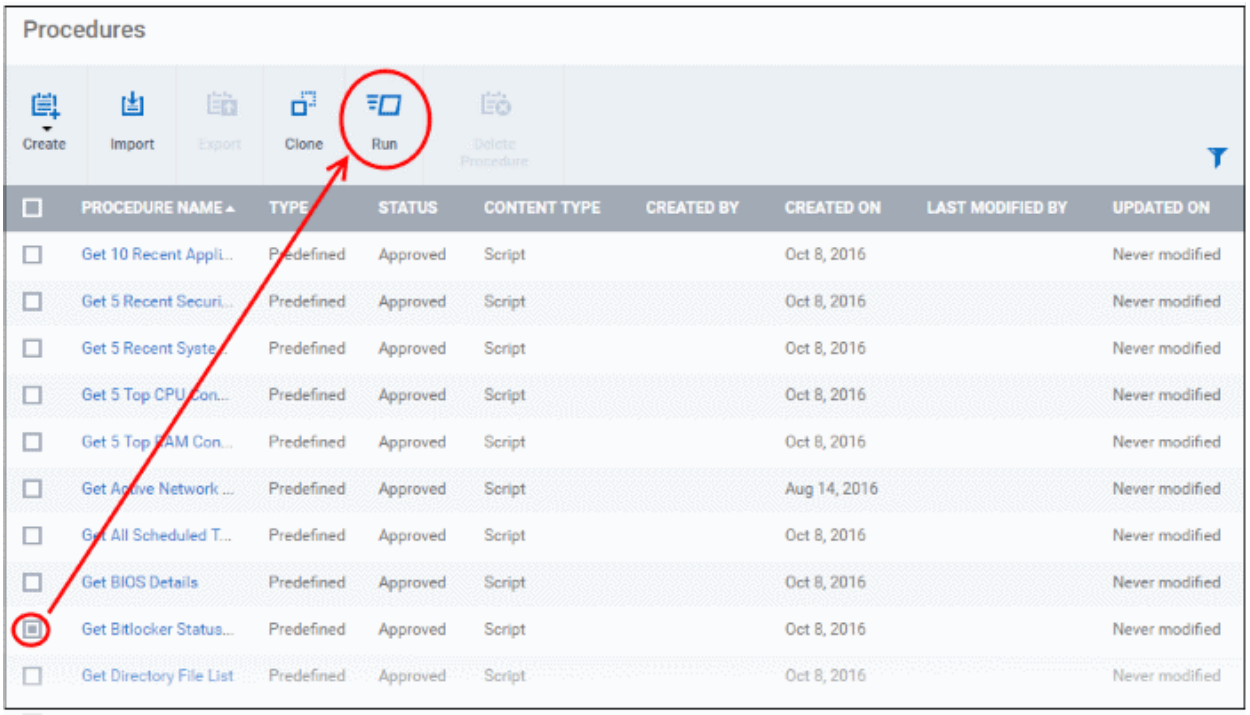
- From the procedures interface

- From the device list interface
- Via profiles according to a schedule

The following section describes how to apply procedures to devices from the procedures interface.

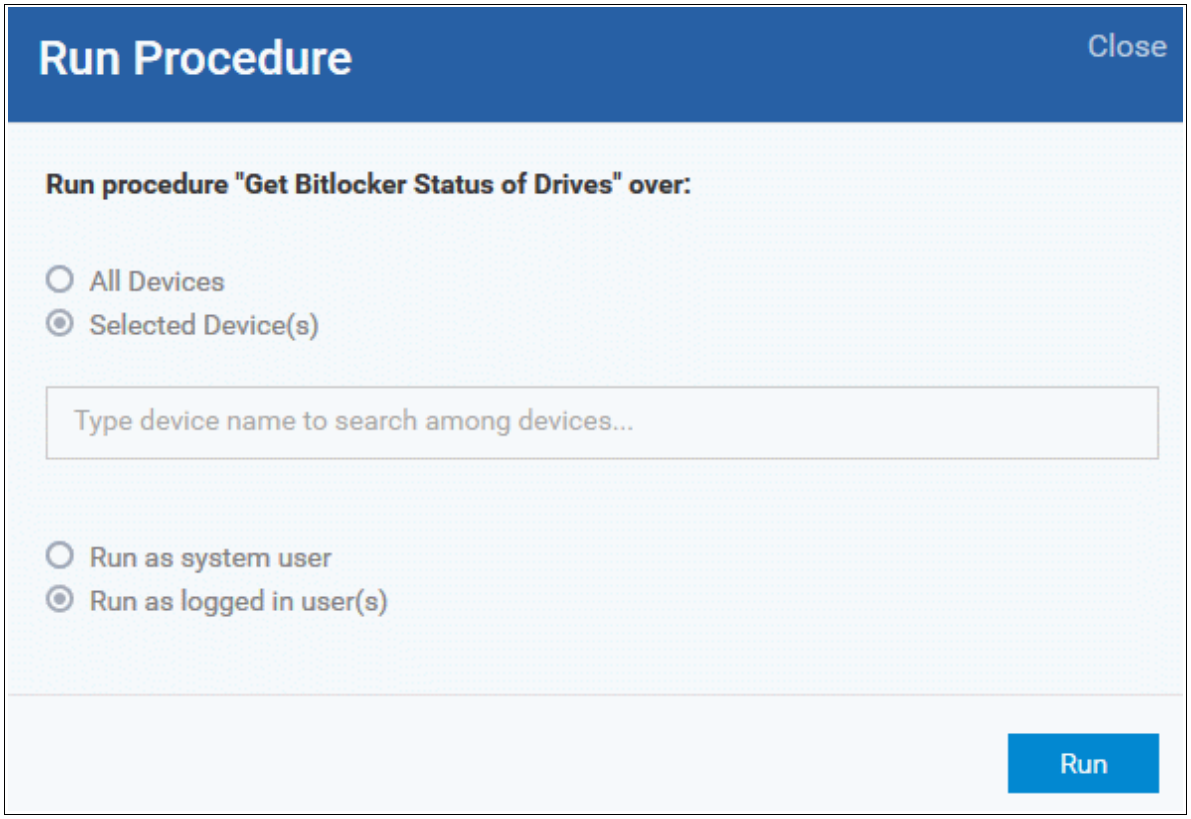
To run a procedure

- Click 'Configuration Templates' > 'Procedures'
- Select the check box beside the procedure that you want to apply. Please note only approved procedures can be applied. You can also run only one procedure at a time.

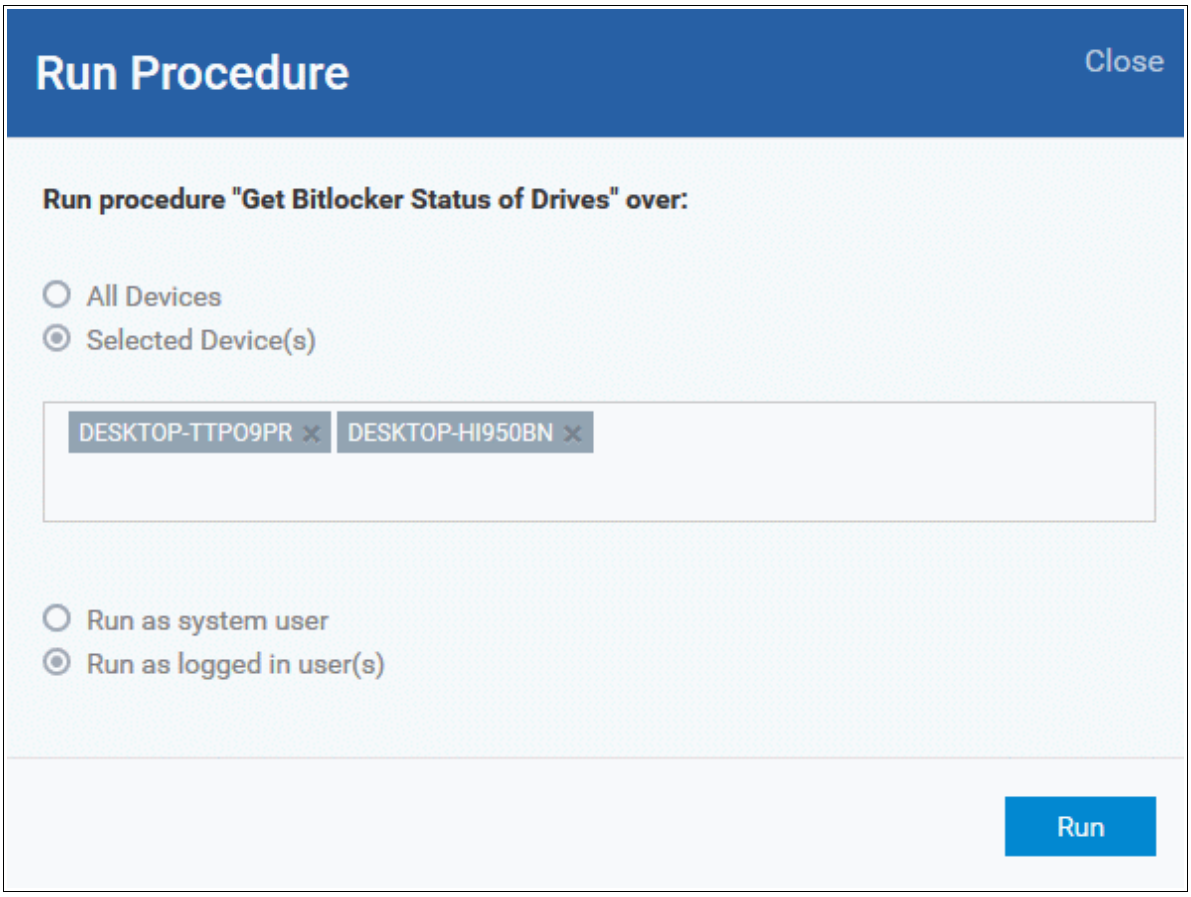


- Click 'Run' at the top

The 'Run' dialog will be displayed:



- All Devices - The procedure will be applied to all Windows devices.
- Selected Device(s) - Enter the name of the Windows device partly or fully and select the device from the list. You can also add multiple devices in the field.



- Choose 'Run as system user' or 'Run as logged in user' based on the access rights required for the procedure to run at the endpoint. Please note this option will not be available for a patch procedure.
- To remove a device from the list, click 'X' beside it.
- Click the 'Run' button

The procedure will be applied to the selected devices. A confirmation dialog will be displayed and the process will be logged. You can view the details in the Procedure Logs screen for script procedures. Patch procedure logs will be available in the respective patch procedure itself.

Important Note: Patches that are hidden by administrators will not be executed. Refer to the section 'Installing OS Patches on Windows Endpoints' for more details.

6.6.9. Edit / Delete Procedures

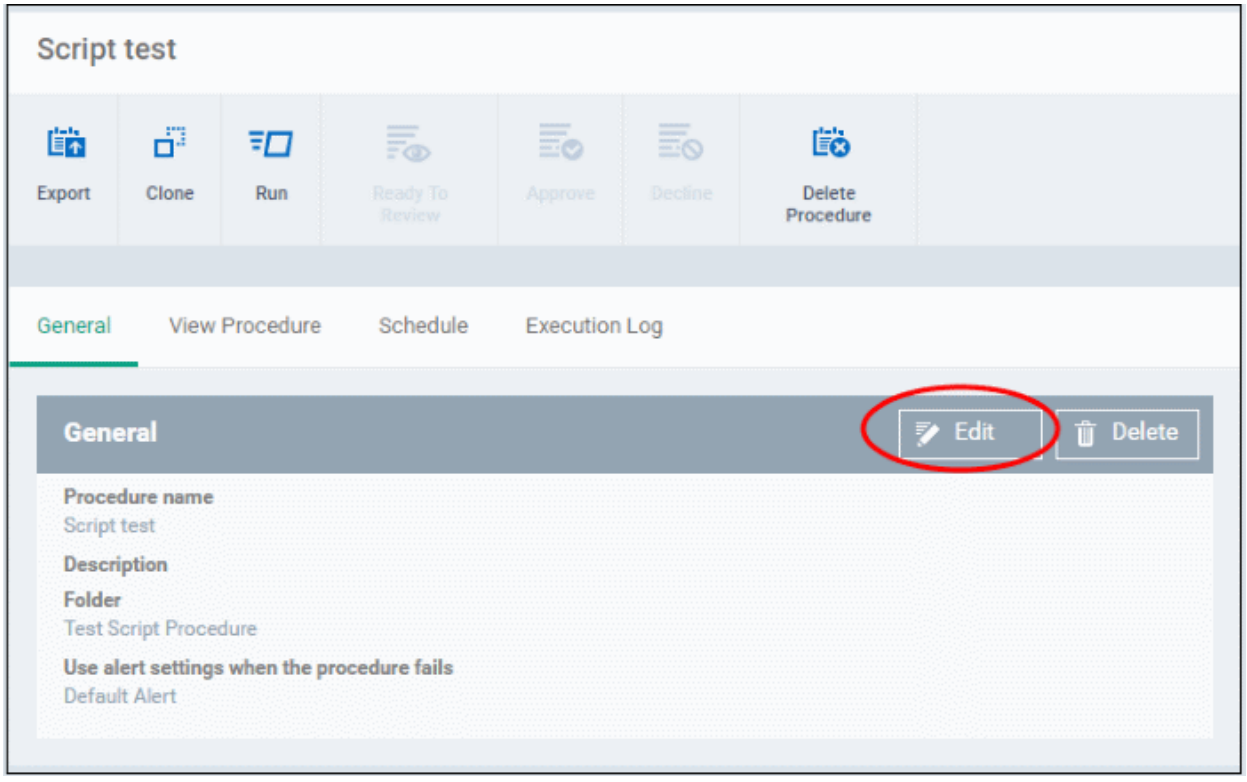
Custom procedures can be edited or deleted according to your requirements. Please note that if you edit a script procedure, it has to be approved again. Predefined procedures cannot be edited or deleted. Click the following links for more details:

- Editing / deleting a script procedure
- Editing / deleting a patch procedure

Editing a Script Procedure

To edit a script procedure

- Click 'Configuration Templates' > 'Procedures'
- Click on the script procedure that you want to modify and click 'Edit' at the top right



General

- Modify the procedure name, description and / or alert settings

View Procedure

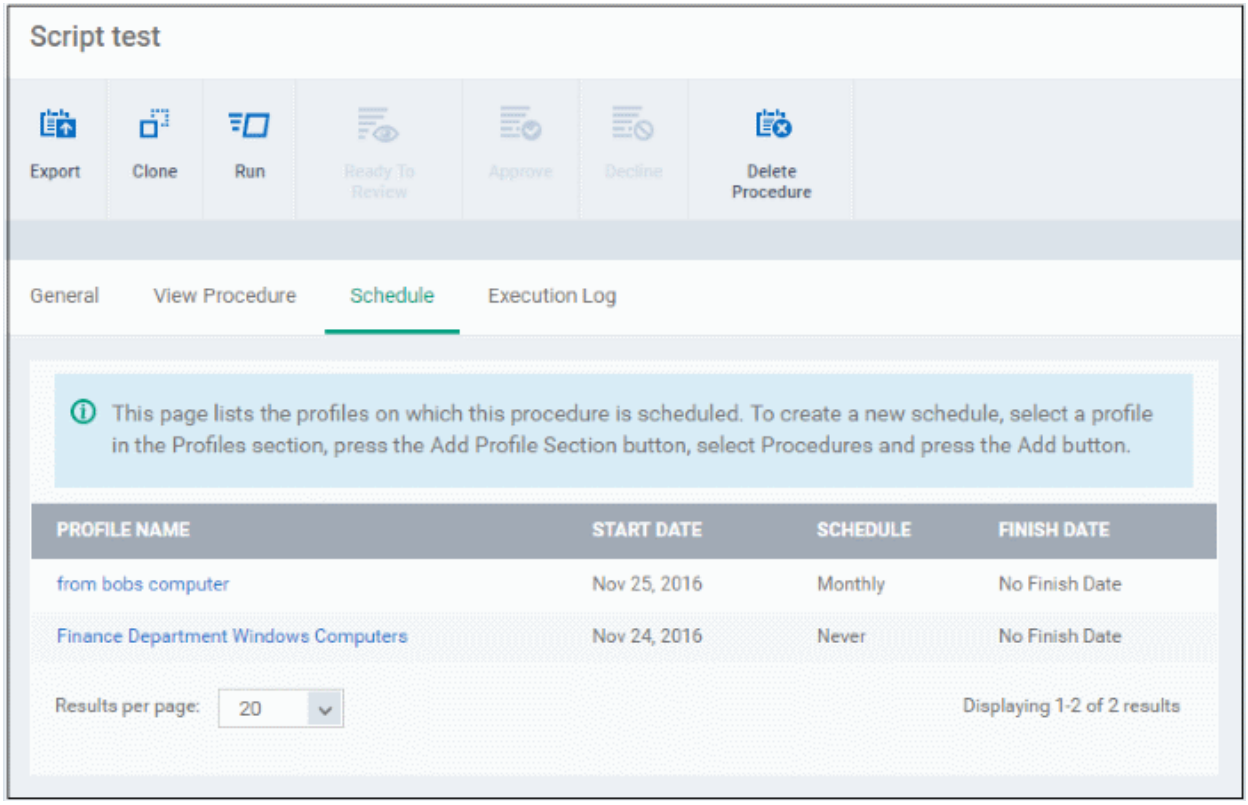
- Click 'Edit'
- Modify the script and / or add another existing procedure

Execution Log

- Displays the results of the script procedure that was executed, both manually and scheduled on Windows profiles.

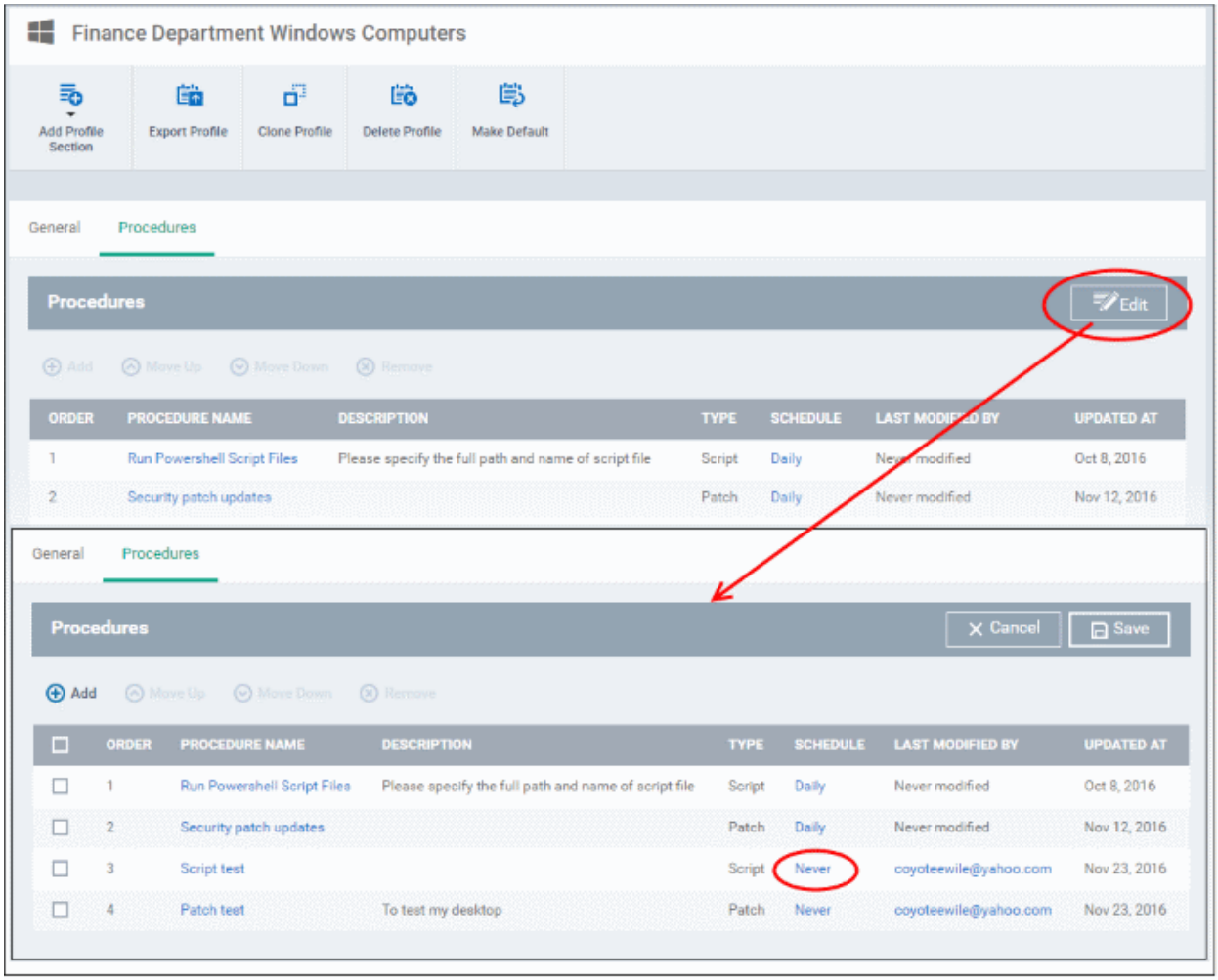
Schedule

The schedule can be edited only in the profile(s) that the procedure is deployed. Clicking the 'Schedule' tab will display the profile(s) name that the procedure is being used.



- Click on the profile name for which you want to edit the procedure schedule.

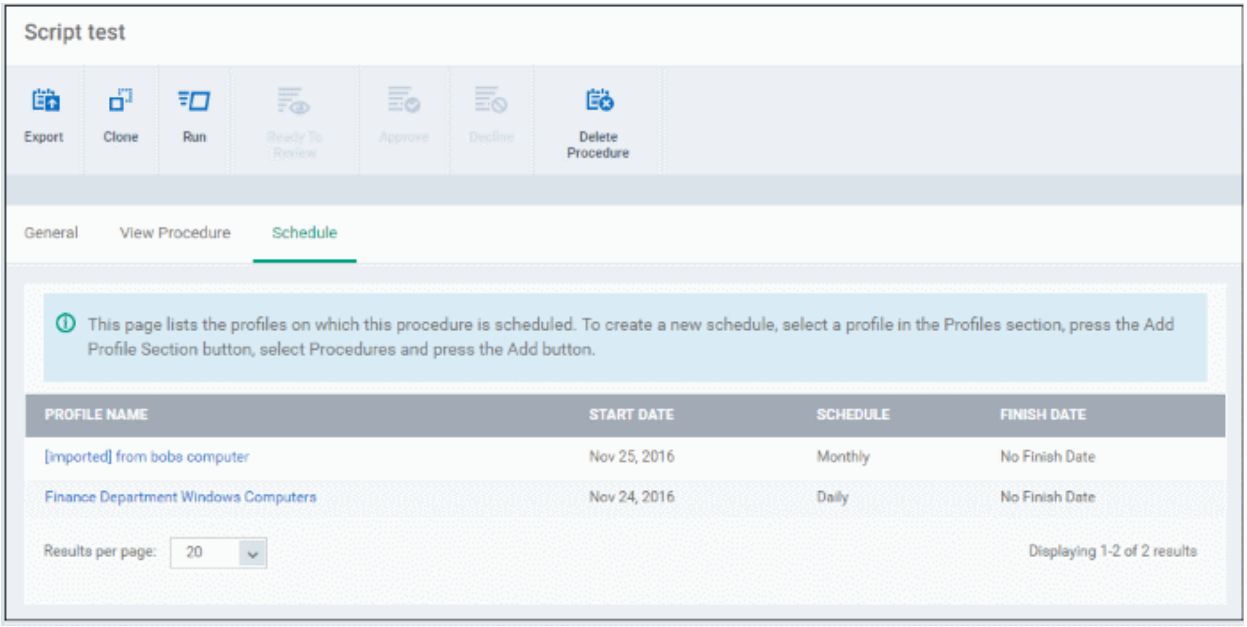
The selected profile will be displayed with the 'Procedure' tab opened. Click 'Edit' at the top right.



You can find the procedure type, whether script or patch, under the 'Type' column.

- Click the schedule parameter under 'Schedule' column beside the procedure.
- The 'Procedure Schedule' dialog will be displayed. Modify the schedule per your requirement and click 'Set'.
- The schedule will be modified for the profile. Please note the procedure schedule will impact only the profile that you modify. The schedule for the same procedure deployed onto other profiles will not be affected.
- Click 'Save'

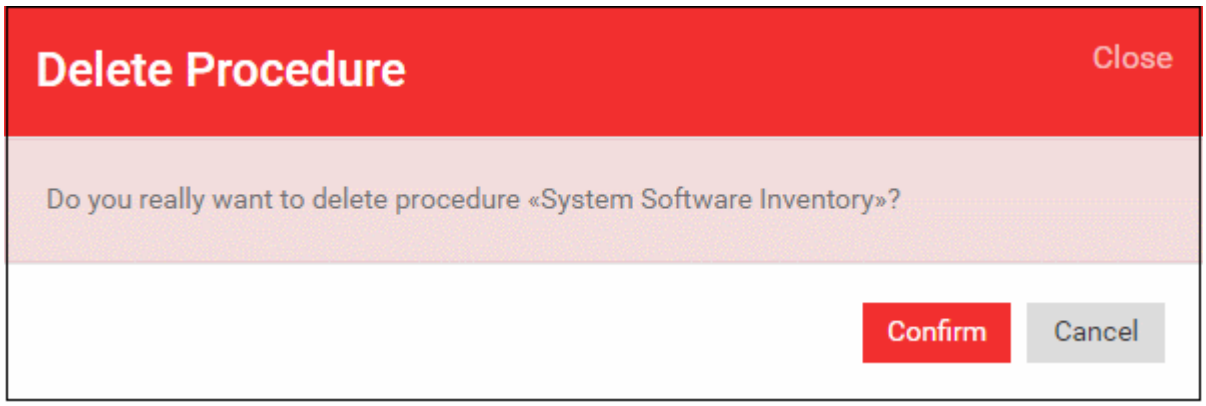
The changes for the procedure will be saved. The following image shows the same procedure having different schedule for different profiles.



To delete a script procedure

- Click 'Configuration Templates' > 'Procedures'
- Select the check box beside the procedure and click 'Delete Procedure' at the top.
- Alternatively, click on the procedure that you want to delete and click 'Delete' on the top right

A confirmation dialog will be displayed.



- Click 'Confirm'. The procedure will be removed from the list as well as from the profiles on which it is deployed.

Editing a patch procedure

- Click 'Configuration Templates' > 'Procedures'
- Click on the patch procedure that you want to modify and click 'Edit' on the top right

General

- Modify the procedure name, description and / or alert settings

Execution Options

- Click 'Edit'
- Modify the patch options
- Click 'Save' when done

The changes for the patch procedure will be saved.

Execution Log

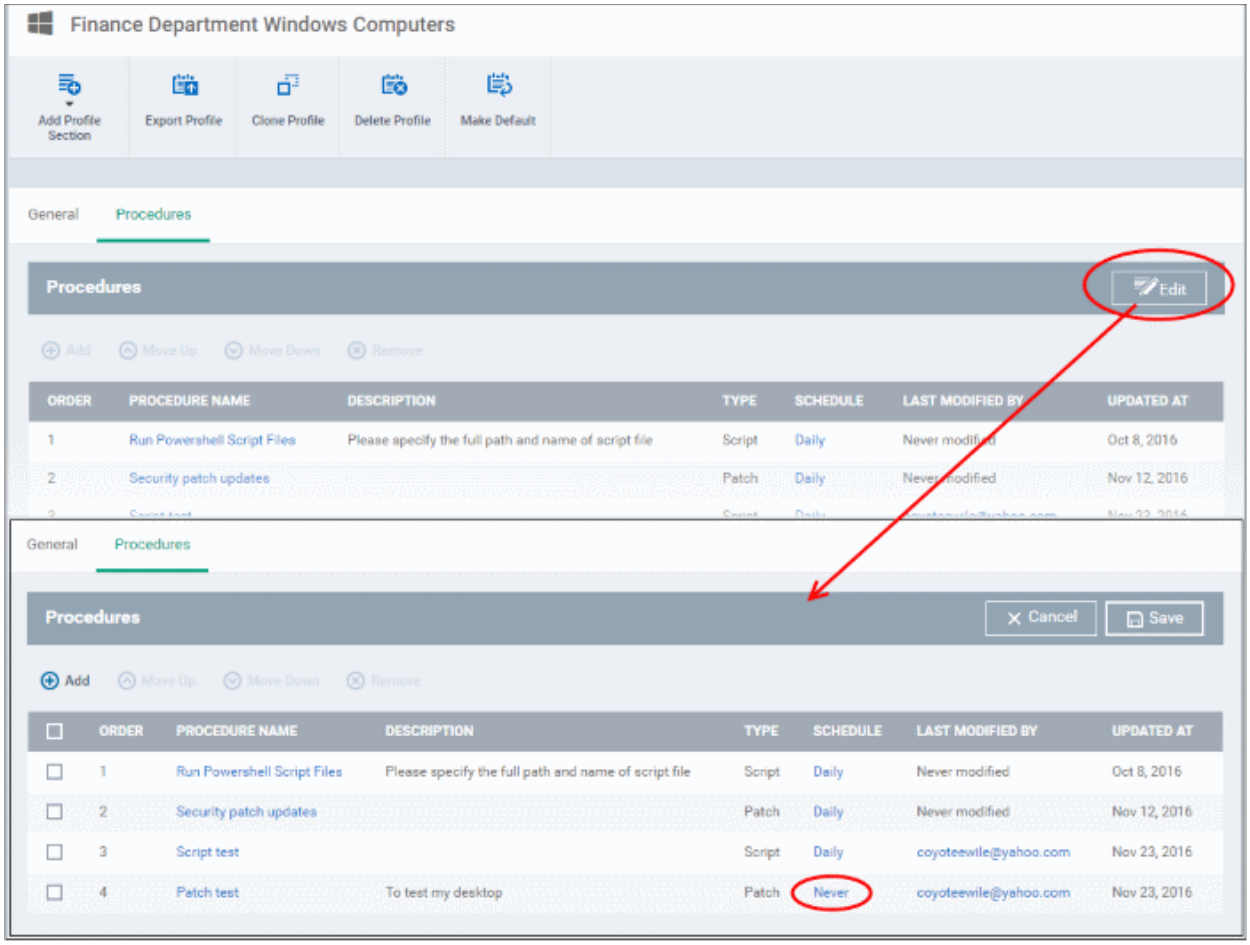
- Displays the results of the patch procedure that was executed, both manually and scheduled on Windows profiles.

Schedule

To modify the patch procedure schedule, you have to edit it in the profile(s) that the procedure is deployed.

- Click 'Configuration Templates' > 'Profiles'
- Click on the profile name that you want to modify the patch procedure

The selected profile will be displayed. Click the 'Procedure' tab and click 'Edit' at the top right.



You can find the procedure type, whether script or patch, under the 'Type' column.

- Click the schedule parameter under 'Schedule' column beside the patch procedure.
- The 'Procedure Schedule' dialog will be displayed. Modify the schedule per your requirement and click 'Set'.
- The schedule will be modified for the profile. Please note the procedure schedule will be impacted for only the profile that you modify. The schedule for the same procedure deployed onto other profiles will not be affected.
- Click 'Save'

The changes for the patch procedure will be saved.

Important Note: Patches that are hidden by administrators will not be executed. Refer to the section '**Installing OS Patches on Windows Endpoints**' for more details.

6.6.10. View Procedure Results

The results of any script procedure can be viewed in the '**Procedure Logs**' section of a device as well as from the script procedure. The results of patch procedures can be viewed in the patch procedure itself. Click the following links for more details:

- **Viewing script procedure results**
- **Viewing patch procedure results**

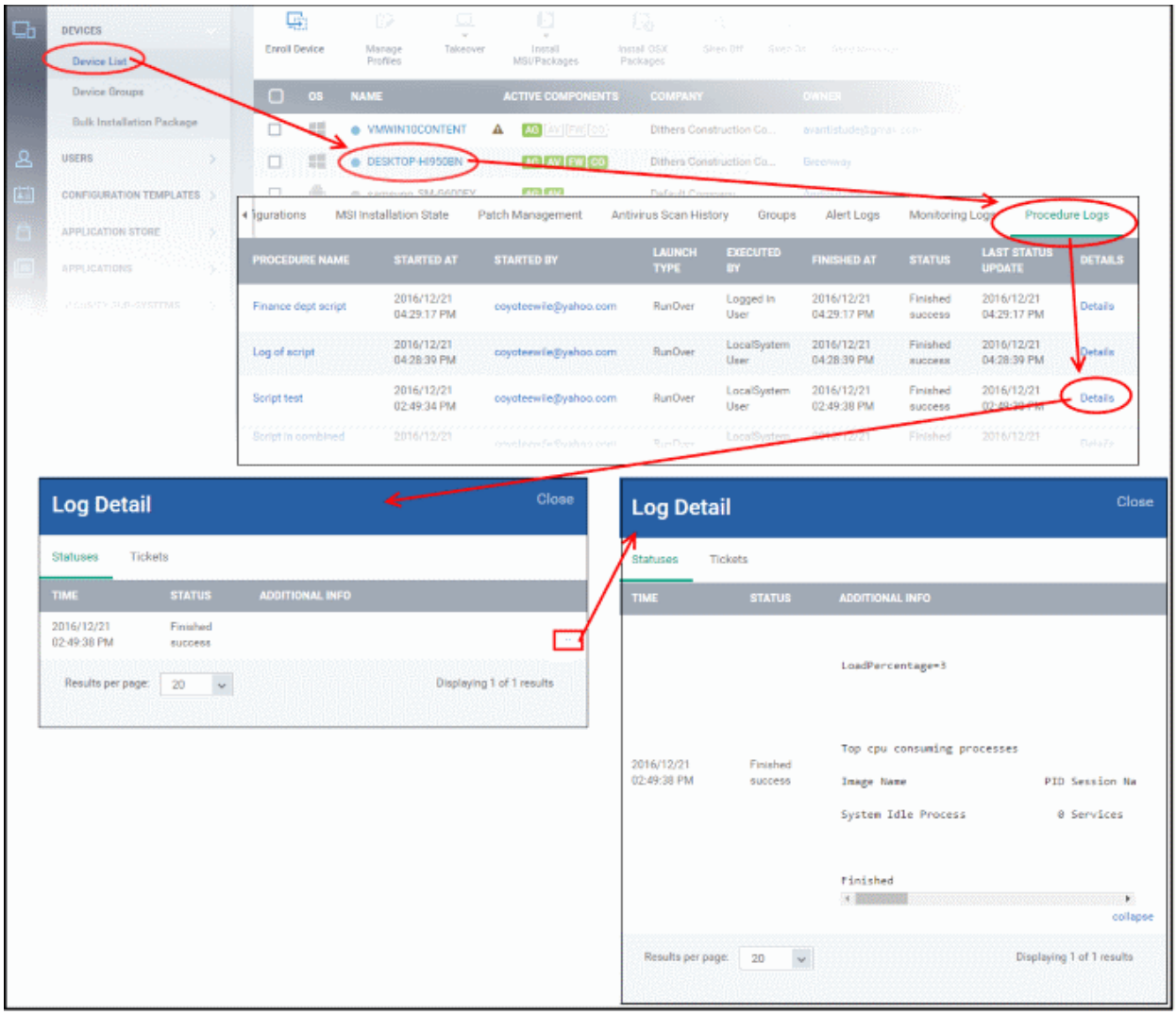
Viewing Script Procedure Results

To view script procedure results

The script procedure logs can be viewed from two interfaces - Device List and Script Procedure. While the 'Procedure Logs' screen from the Device List interface displays results for all the script procedures run on a device, the 'Execution Log' tab on a script procedure displays all the devices that was run the selected script procedure.

Script procedures results run on a particular device

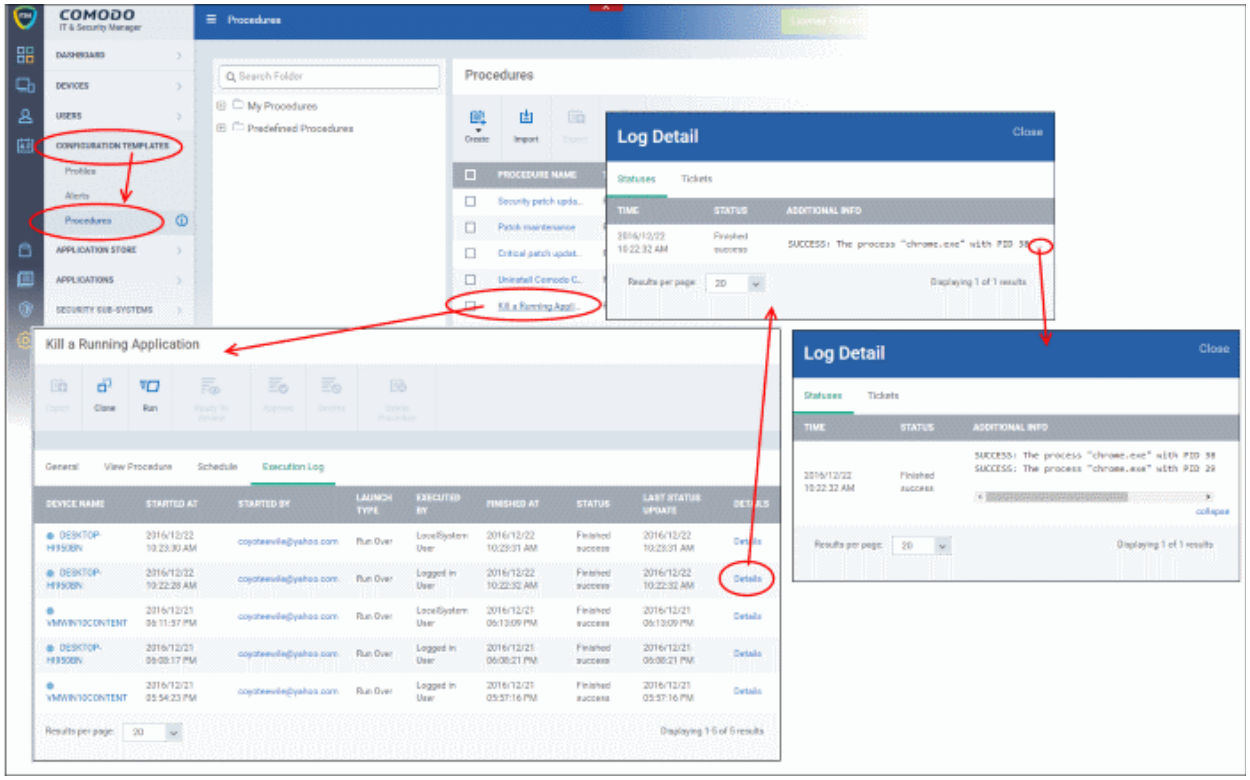
- Click 'Devices' > 'Device List'.
- Click the name of the Windows device to which the procedure was applied.
- Click the 'Procedure Logs' link on the right.
- This will open a list of all procedures run on the device along with their status (success/failure), their start/finish time and time of last status update.
- To view the results of a particular procedure, click 'Details' then the ellipsis (...) link on the left of the 'Log Detail' dialog.
- The details dialog will display the specific results of the procedure. For example, the 'Check all running services' results will show a list of all services found running on the device:



- The 'Tickets' section lists tickets which were created as a result of a failed procedure. Clicking the ticket link will open the ticket in service desk.

Results of a script procedure run on all the devices

- Click 'Configuration Templates' > 'Procedures'.
- Click the name of the script procedure under 'My Procedures' or 'Predefined Procedures' for which you want to view results, then click 'Execution Log'.
- This will open a list of all devices on which the script procedure was run along with their status (success/failure), their start/finish time and time of last status update.
- To view the results of the procedure on a particular device, click 'Details' then the ellipsis (...) link on the left of the 'Log Detail' dialog.
- The details dialog will display the specific results of the procedure. For example, the 'Kill a Running Application' results will show a list of all applications and processes that were stopped on a device by the script.

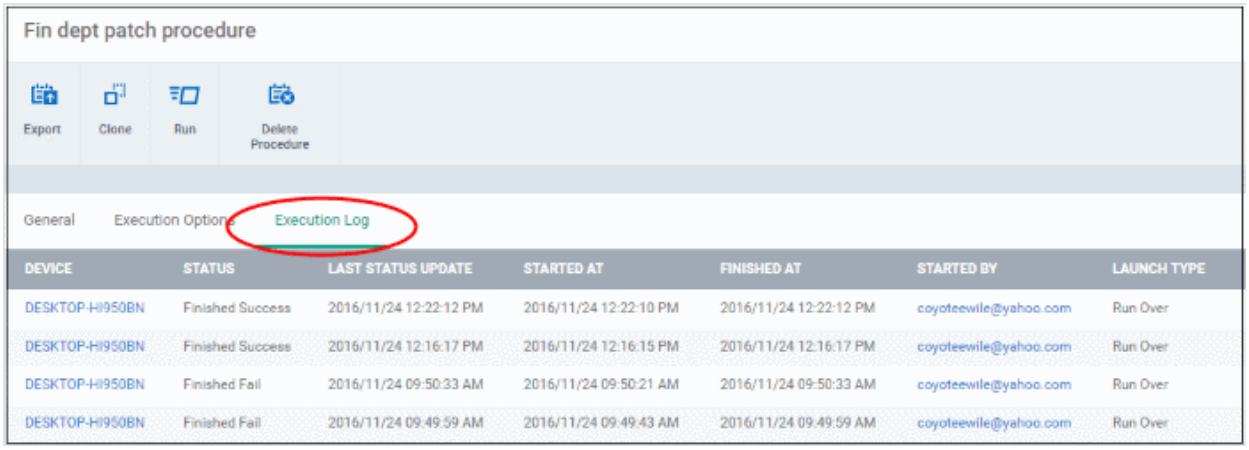


- The 'Tickets' section lists tickets which were created as a result of a failed procedure. Clicking the ticket link will open the ticket in service desk.

Viewing Patch Procedure Results

To view patch procedure results

- Click 'Configuration Templates' > 'Procedures'
- Click the name of the patch procedure under 'My Procedures' or 'Predefined Procedures'
- Click 'Execution Log' tab



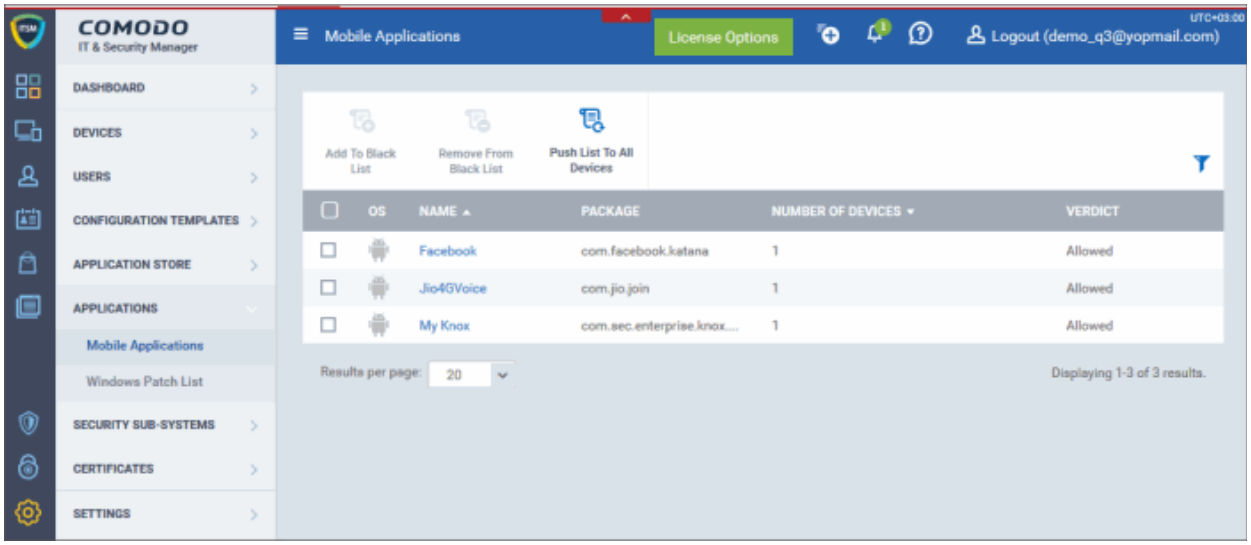
- This will open a list of devices that the patch procedure was executed along with their status (success/failure), their start/finish time, started by and how it was initiated whether manually or scheduled.
- A Service Desk ticket will also be created for failed patch procedures if the alerts are configured appropriately.

7. Applications

ITSM provides visibility and control to administrators over applications installed on user devices.

The 'Applications' tab allows the administrator to:

- View all applications installed on enrolled Android and iOS devices and block any malicious applications that are identified. Once blacklisted, the application will not be allowed to run on any device(s) on which it is installed.
- View a constantly updated list of patches available for managed Windows devices and install selected patches on to the devices.



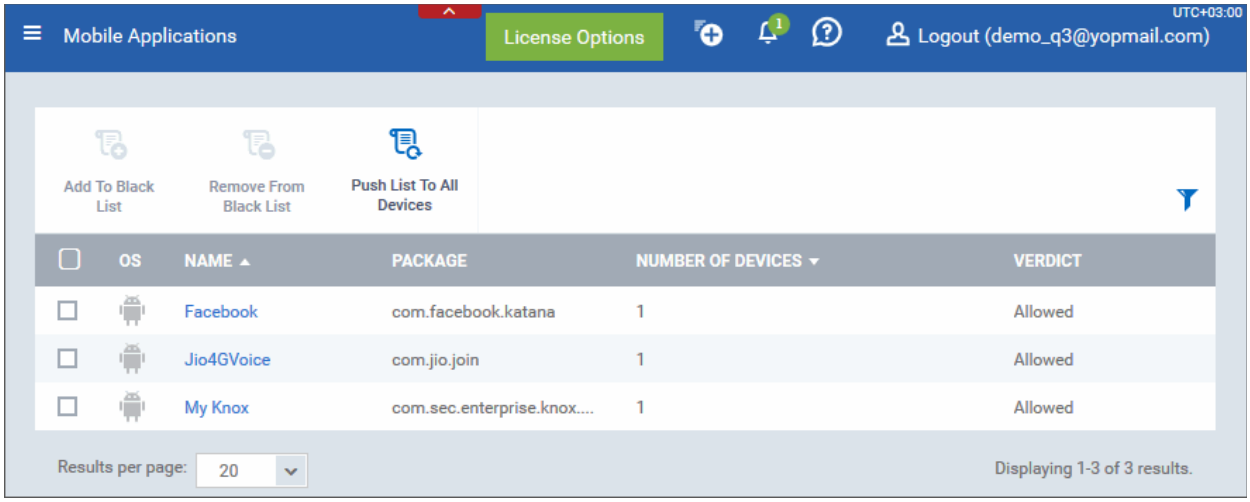
The following sections explain in more detail on:

- Viewing Applications Installed on Android and iOS Devices
  - Blacklisting and Whitelisting Applications
- Installing OS Patches On Windows Endpoints

7.1. Viewing Applications Installed on Android and iOS Devices

The 'Mobile Applications' interface displays a list of all applications identified from all enrolled Android and iOS devices with details like their package name and number of devices on which the app is found. Administrators can determine authenticity of the applications and blacklist the applications deemed to be malicious, suspicious or not trustworthy. The blacklisted apps can be immediately blocked in the devices upon which they are installed and prevented from being installed on to other devices in future.

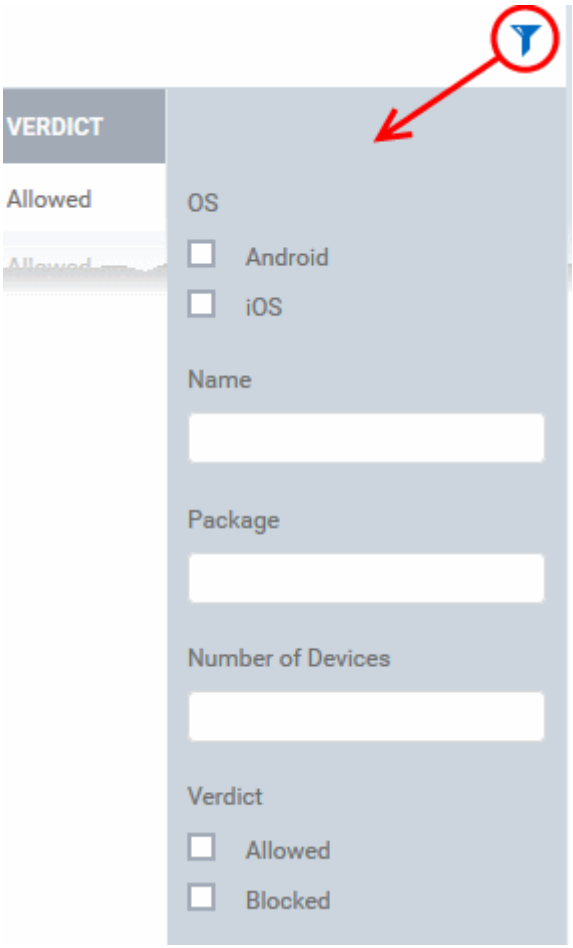
- To access the 'Mobile Applications' interface, click the 'Applications' link on the left and choose 'Mobile Applications' from the options.



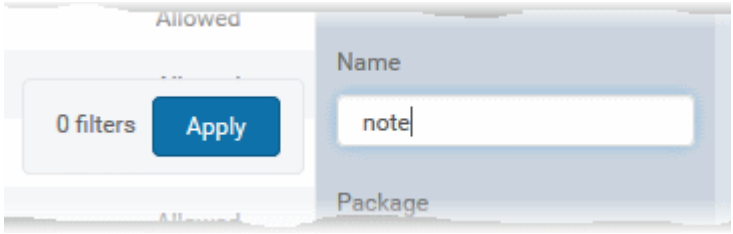
Mobile Applications interface - Column Descriptions	
Column Heading	**Description**
OS	Indicates OS type of the app.
Name	Name of the application. Clicking the name of an application opens the 'Devices' interface with a list of only those devices on which the app is installed, enabling the administrator to identify the devices using the application.
Package	The package name or identifier of the package from which the app was installed.
Number of Devices	Indicates the number of devices on which the app is installed currently.
Verdict	Indicates whether the application is allowed or blacklisted.

Sorting, Search and Filter Options

- Clicking on any of the column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific app based on the app name and/or its package name, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- To filter the items based on OS types, select the OS types.
- To filter items based on number of devices on which it is installed, enter the number in the 'Number of Devices' field and click 'Apply'.
- To filter the items based on their blacklist status, select the state under Verdict'

You can use any combination of filters at-a-time to search for specific apps.

- To display all items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Refer to the next section **Blacklisting and Whitelisting Applications** for explanation on moving malicious or unwanted apps to blacklist.

7.1.1. Blacklisting and Whitelisting Applications

ITSM allows administrators to view a list of applications identified on all enrolled mobile devices and to review their trustworthiness. If a suspicious or malicious application is identified then it can be moved to the blacklist. This will block the application on all devices and prevent other devices from installing the application in future.

Blacklisted files that are subsequently found to be trustworthy can be moved to the whitelist.

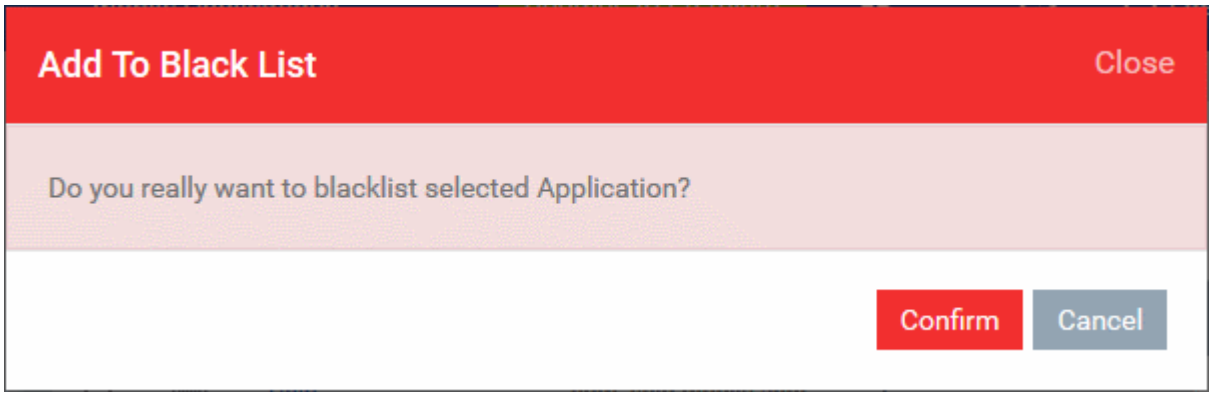
To move selected apps to blacklist

- Click 'Applications' tab from left and choose 'Mobile Applications' from the options.
- Select the apps to be black listed.

Tip: You can filter the list or search for a specific app by using the filter options that appear on clicking the funnel icon at the top right.

- Click the 'Add to Black List' from the top.

A confirmation dialog will appear.



- Click 'Confirm'.

The selected apps will be added to the 'Black List' and their status will change to 'Blocked'

- To block the apps immediately in the devices on which they are currently installed, click 'Push List to All Devices' from the top.

Unblocking Blacklisted Apps

If an application is moved to blacklist by mistake or if an application previously blacklisted appears to be a genuine or trustworthy, the administrator can remove it from the blacklist and allow the application to be installed or run on the devices.

To remove trustworthy apps from blacklist

- Click 'Applications' from the left and choose 'Mobile Applications' from the options.

- Select the apps with 'Blocked' status, to be whitelisted.

- Click 'Remove From Black List' at the top.

The status of the apps will change to 'Allowed'.

- If you want the changes to take effect immediately, click 'Push List to All Devices'.

7.2. Installing OS Patches on Windows Endpoints

ITSM allows administrators to install patches on selected Windows devices from the 'Device List' interface. Alternatively, the 'Applications' interface allows you to deploy patches to all managed devices. Refer to the section 'Viewing and Installing Windows Patches' to learn more about installing patches to individual Windows devices.

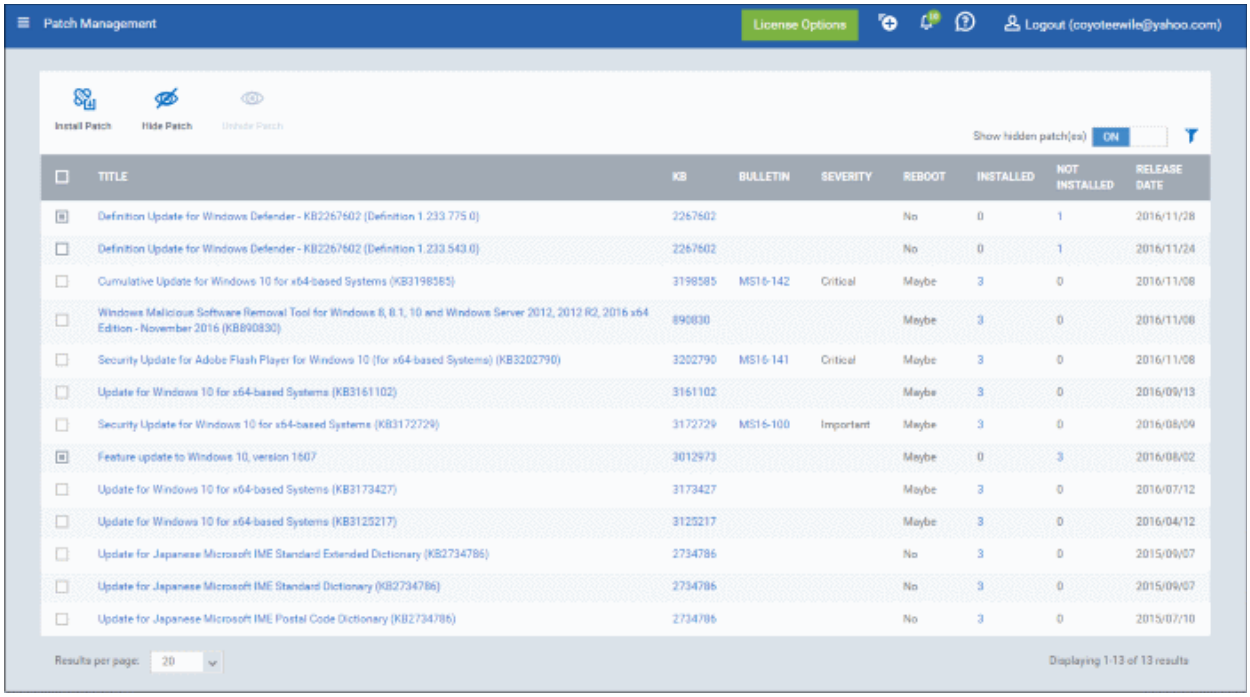
The 'Patch Management' feature allows admins to deploy patches to all managed Windows devices. ITSM checks Microsoft update servers for Windows patches, software and security updates and lists these in the interface.

ITSM will display available patches along with the number of endpoints they are installed/not installed on, the patch release date and its severity. You can choose to hide patches in the screen if you do not want them to be deployed onto the endpoints. Hidden patches will not be available for deployment on the 'Device List' screen and will not be executed as well if added to a patch procedure.

To view and install patches on Windows endpoints

- Click 'Applications' on the left and select 'Patch Management' from the options

The list of all the OS patches and update packages that are applicable to the managed Windows endpoints will be displayed.

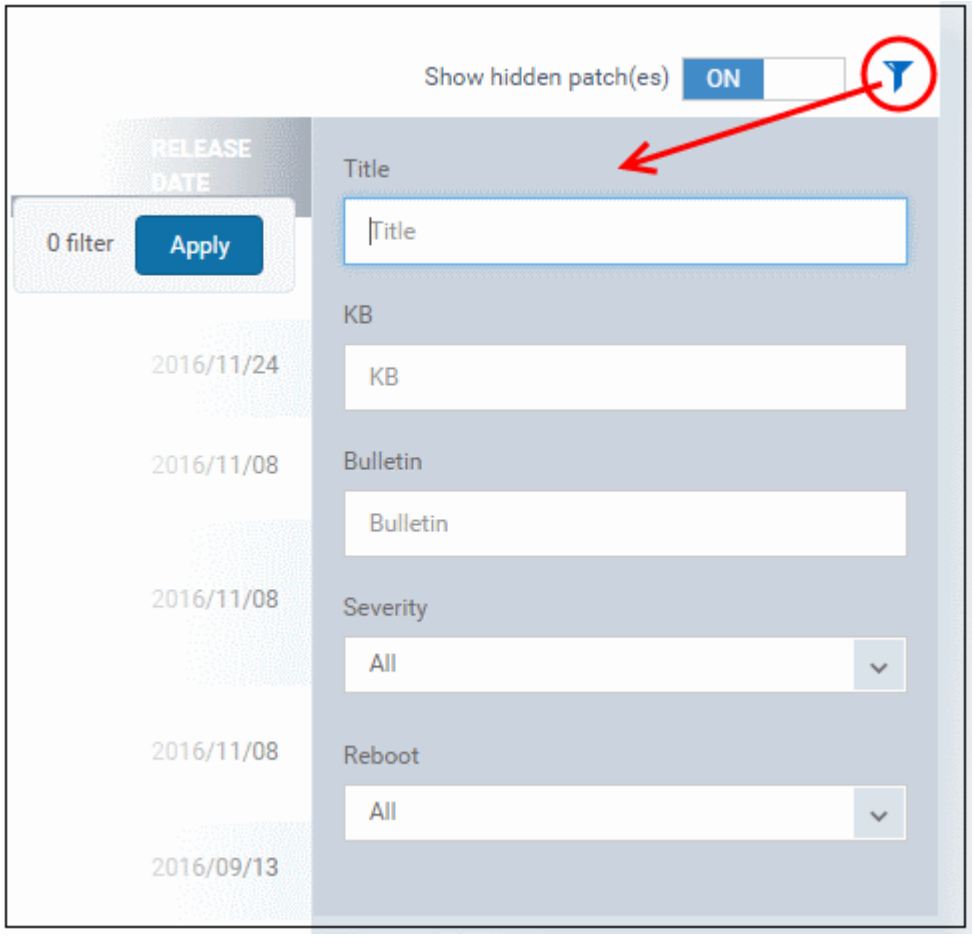


Patch Management Table - Column Descriptions	
Column Heading	**Description**
Title	The name of the patch.
KB	Displays the knowledgebase article number that describes the patch. • Clicking the number will take you to the Microsoft Knowledgebase article web page.
Bulletin	Displays the Microsoft Bulletin number that contains the details about the patch release. • Clicking the number will take you to the respective 'Microsoft Security Bulletin' page.
Severity	Indicates the level of severity for the patch. The severity levels are: • Unknown • Critical • Important • Low • Moderate • None
Reboot	Indicates whether the endpoint requires a reboot for the patch installation to take effect.
Installed	Indicates the number of managed endpoints on which the patch is already installed. Clicking the number will take you to the 'Device List' screen displaying the list of devices onto which the patches/updates are installed.
Not Installed	Indicates the number of managed endpoints to which the patch is yet to be installed. Clicking the number will take you to the 'Device List' screen displaying the list of devices onto which the patches/updates are yet to be installed.

Release Date	The date on which the patch was released by Microsoft.
Controls	
Install Patch	Allows you to install the patches/updates.
Hide Patch	Allows you to hide selected patches that you do not want to be deployed onto enrolled endpoints. Hidden patches will not be available for deployment on the 'Device List' screen and will not be executed as well if added to a patch procedure.
Unhide Patch	Allows you to unlock hidden patches.
Show hidden patch(es)	Allows you to view the hidden patches and if required you can install these hidden patches onto endpoints. Use the toggle button to hide / view hidden patches.

Sorting, Search and Filter Options

- Clicking on any column header sorts the items based on alphabetical or ascending/descending order of entries in the respective column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the patches or search for a specific patch, enter the details in part or full and /or select from the drop-downs and click 'Apply'.
  - Title - Filters the items based on the name of the patch

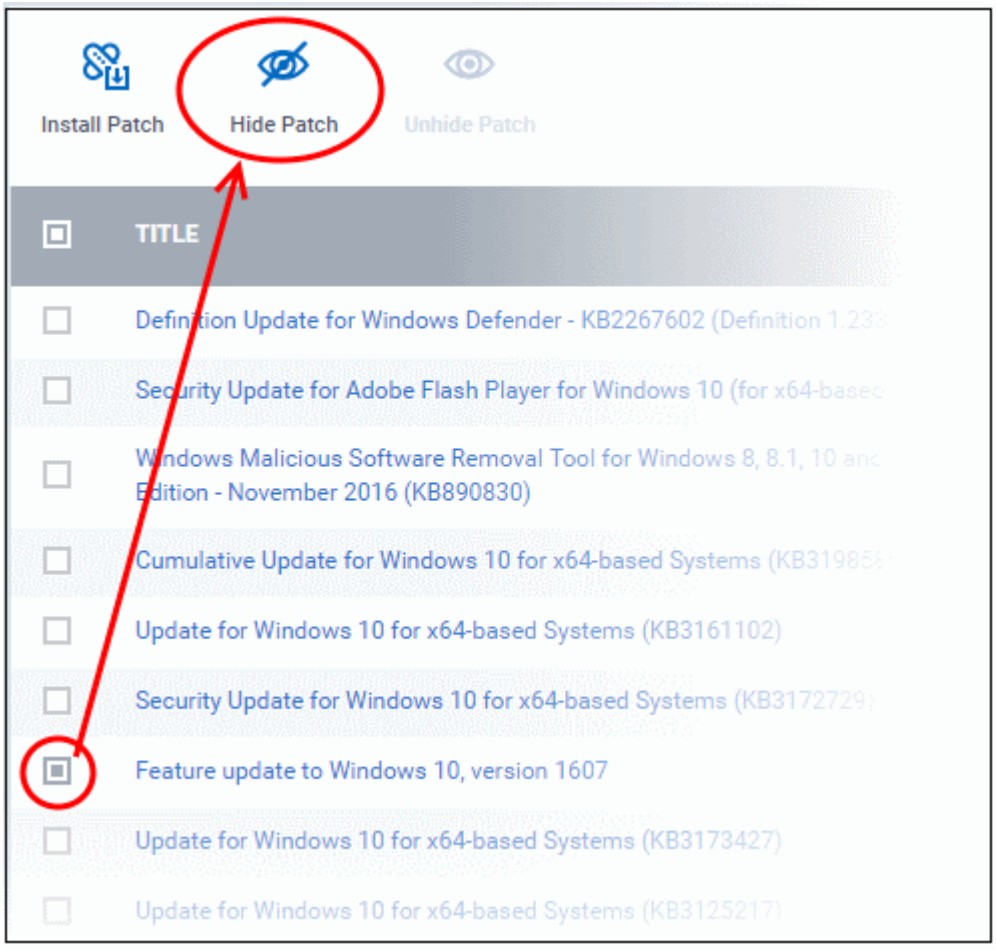
- KB - Filters the items based on the KB number
- Bulletin - Filters the items based on the entered bulletin details
- Severity - Filters the items based on the selected severity level
- Reboot - Filters the items based on the selected reboot option
- Release Date - Filters the items based on the entered release date

You can use any combination of filters at-a-time to search for a specific patch.

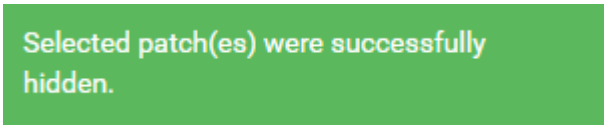
- To display all the items again, remove / deselect the search key from the filters and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

To hide patch(es)

- Select the patch(es) to be hidden from the list and click 'Hide Patch'



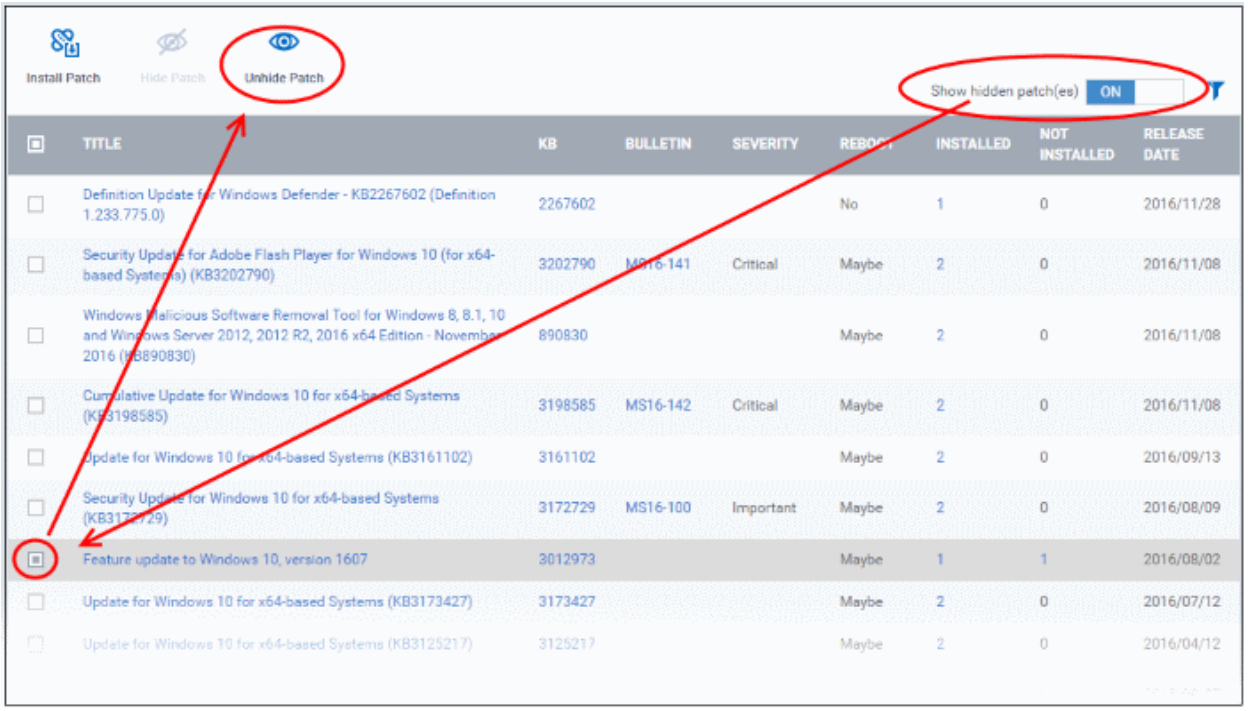
A confirmation message will be displayed.



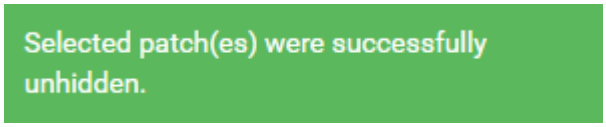
Please note hidden patches will not be available for deployment on the 'Device List' screen and will not be executed if added to a patch procedure. However, you can view the hidden patches by using the 'Show hidden patch(es) toggle button and install these patches onto endpoints.

To view and unhide patch(es)

- Click the 'Show hidden patch(es)' toggle button to 'On' position
- Select the hidden patch(es) from the list and click 'Unhide Patch'



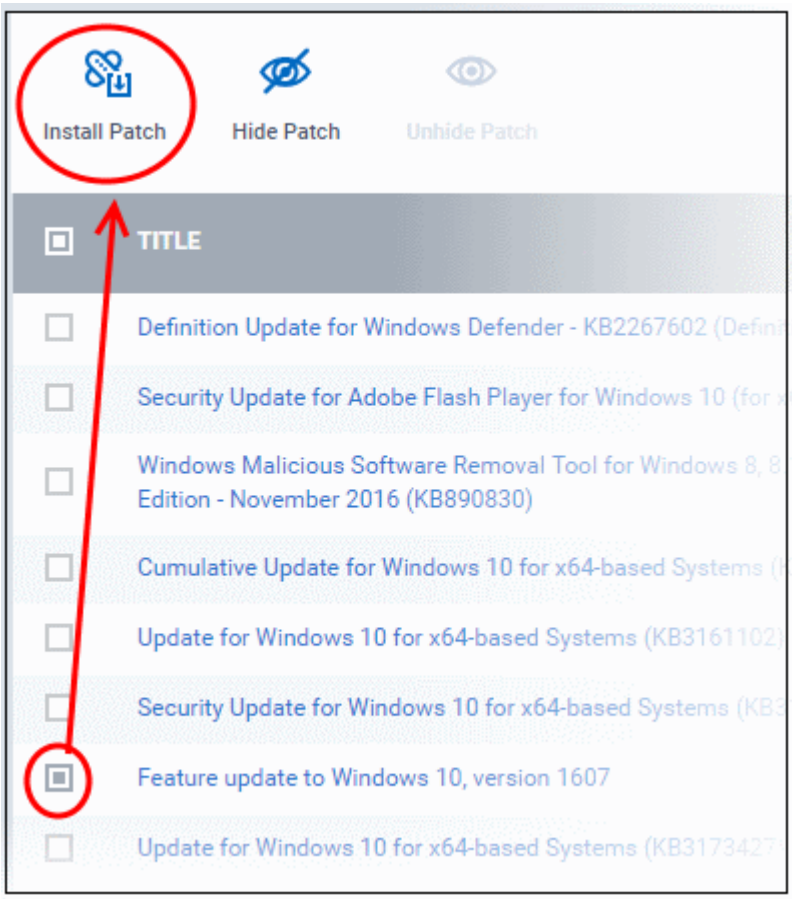
A confirmation message will be displayed.



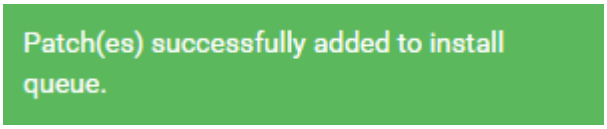
These unlocked patches will now be available for deployment on the 'Device List' screen and will be executed if added to a patch procedure.

To install patch(es) on managed endpoints

- Select the patch(es) to be installed from the list and click 'Install Selected Patch'



A confirmation message will be displayed.



The command will be sent and the selected patch(es) will be installed on the endpoint(s).

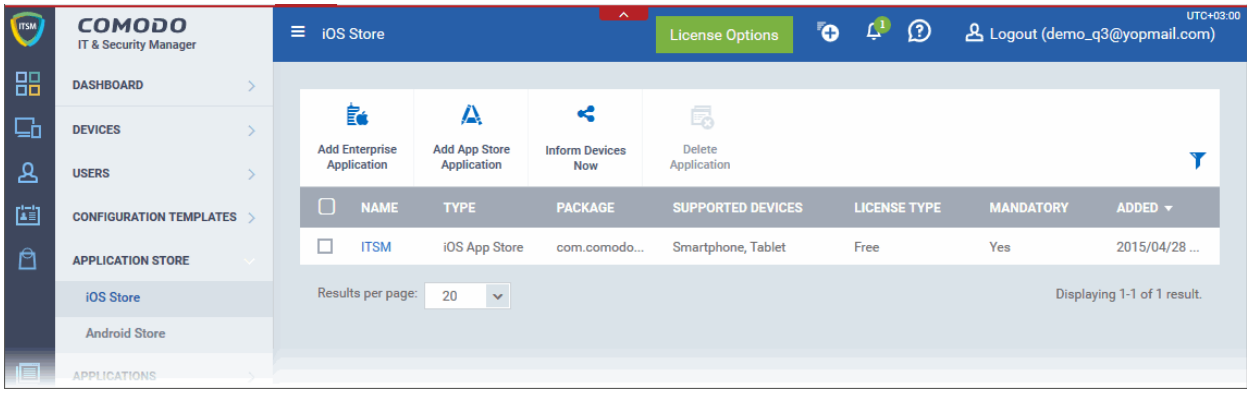
8. App Store

The Application Store interface allows administrators to add and manage Android and iOS applications and push them to managed devices. ITSM maintains a repository of custom and enterprise apps from apps from Google Play and the App Store. You can add both mandatory and optional apps to the repository and can update all devices with one click using the 'Inform Devices Now' button.

- For applications from the Google Play and App Store, you can specify the app name or bundle identifier. ITSM will automatically fetch the details and download URL of the app. During installation on the device, the end-user will be taken to the respective Google Play page or App Store page to download and install the app.
- For custom and enterprise applications, you can upload the .apk file (for Android) and .ipa file (for iOS) to ITSM directly. The device agent will download the app from the ITSM repository and install it.

Apps in the repository are automatically synchronized with enrolled devices every 24 hours and notifications are sent to devices if new apps are ready to be installed. In addition, you can manually sync apps between the repository and devices from the 'App Store' interface. The list of new apps that are waiting to be installed can be viewed from the App Store interface of the ITSM agent interface.

The 'Application Store' tab contains two sub tabs for adding and managing Android and iOS applications.



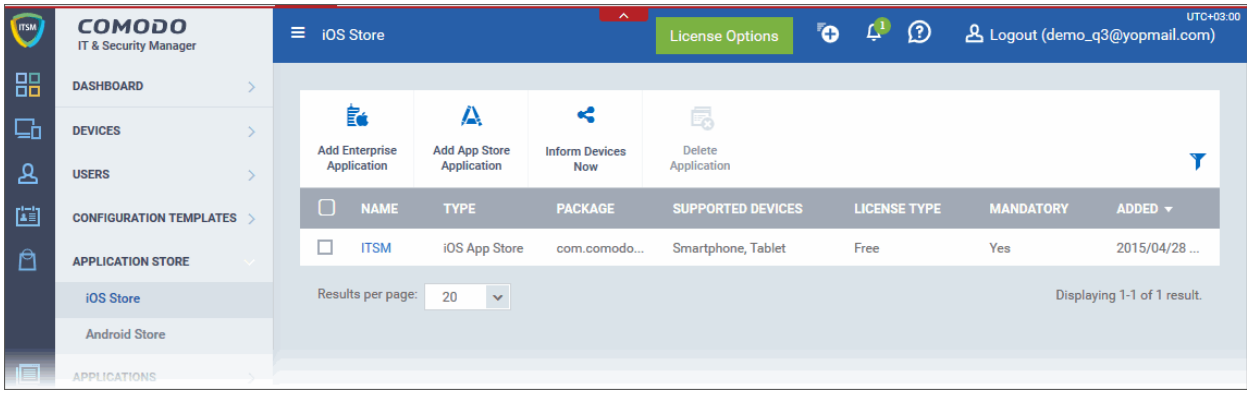
The following sections contain more details on each app type:

- iOS Apps
  - Adding iOS Apps and Installing them on Devices
  - Managing iOS Apps
- Android Apps
  - Adding Android Apps and Installing them on Devices
  - Managing Android Apps

8.1. iOS Apps

The 'iOS Store' interface displays a list of all available iOS apps and allows you to add new apps from the Apple store. You can also upload custom enterprise apps and synchronize the app list to managed iOS devices. You can edit existing app parameters and remove any unwanted apps from the repository.

- To open the 'iOS Store' interface, click 'Application Store' from the left and choose 'iOS Store' from the options.

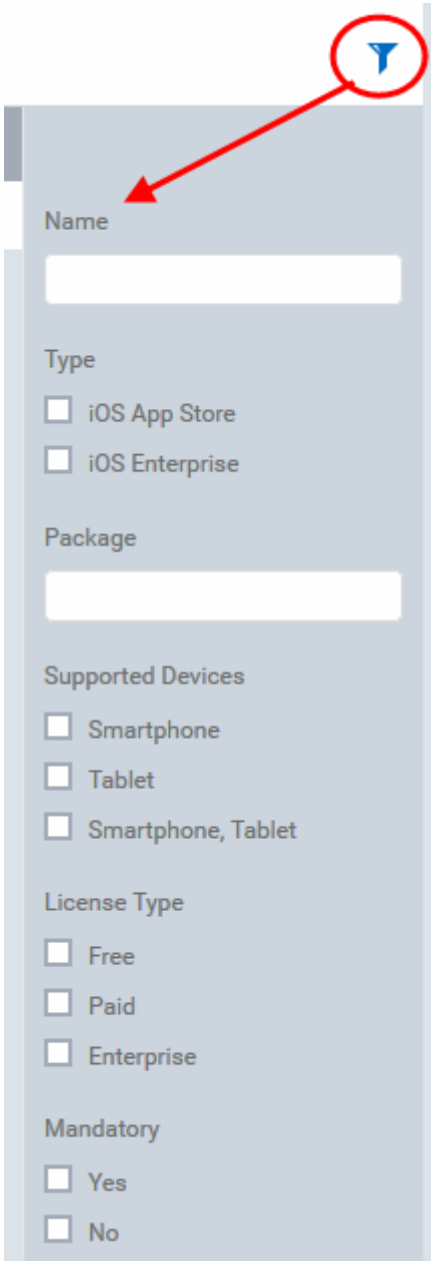


'iOS App Catalog' - Column Descriptions	
Column Heading	**Description**
Name	Displays the name of the application. Clicking on the name of an app opens the 'Detail' screen that displays the details like description, version number, Bundle ID, category, supported devices, whether the app is mandatory or optional, download URL. The Details screen also allows you to edit the app details . Refer to the section Managing iOS Apps for more details.
Type	Indicates the source type of the app. Possible types are: • iOS App Store

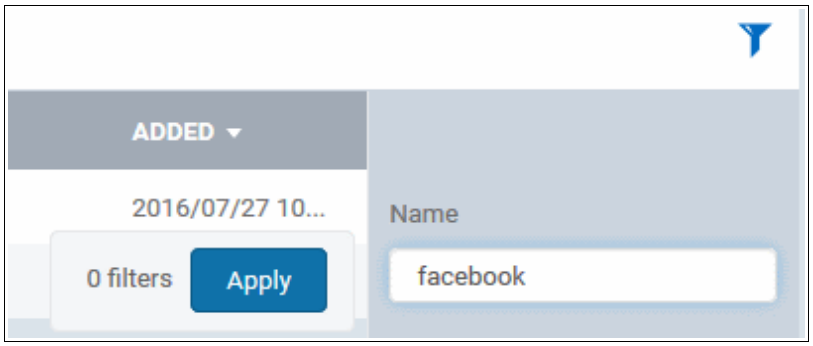
	• iOS Enterprise uploaded by the administrator
Package	Displays the Bundle Identifier of the app.
Supported Devices	Displays the type of devices for which the application is compatible.
License Type	Indicates whether the app is a free, paid or enterprise version.
Mandatory	Indicates whether the app has been marked to be installed compulsorily on the devices. Refer to the section '**Adding iOS Apps and Installing them on Devices**' for more details.
Added	Displays the date and time at which the app was added to repository.

Sorting, Search and Filter Options

- Clicking on any of the column headers sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific app based on the app name and/or its package name, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- To filter the items based on their application type, select the criteria under 'Type'
- To filter the items based on type of devices on which they can be installed, select the device type from 'Supported Devices'
- To filter the items based on license type, select the criteria from 'License Type'
- To view only mandatory or only optional apps, select the respective type from 'Mandatory' options.

You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The following sections explain in detail on:

- Adding iOS Apps and Installing them on Devices
- Managing iOS Apps

8.1.1. Adding iOS Apps and Installing them on Devices

You can add iOS apps to the repository both from App Store and by uploading custom/enterprise apps for installation on to managed iOS smart phones and tablets.

The following sections provide more details on:

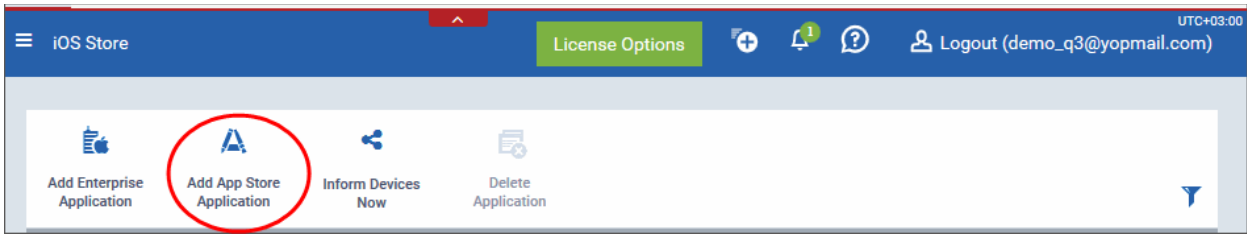
- Adding iOS Apps from App Store
- Adding Custom/Enterprise iOS Apps

Adding iOS Apps from App Store

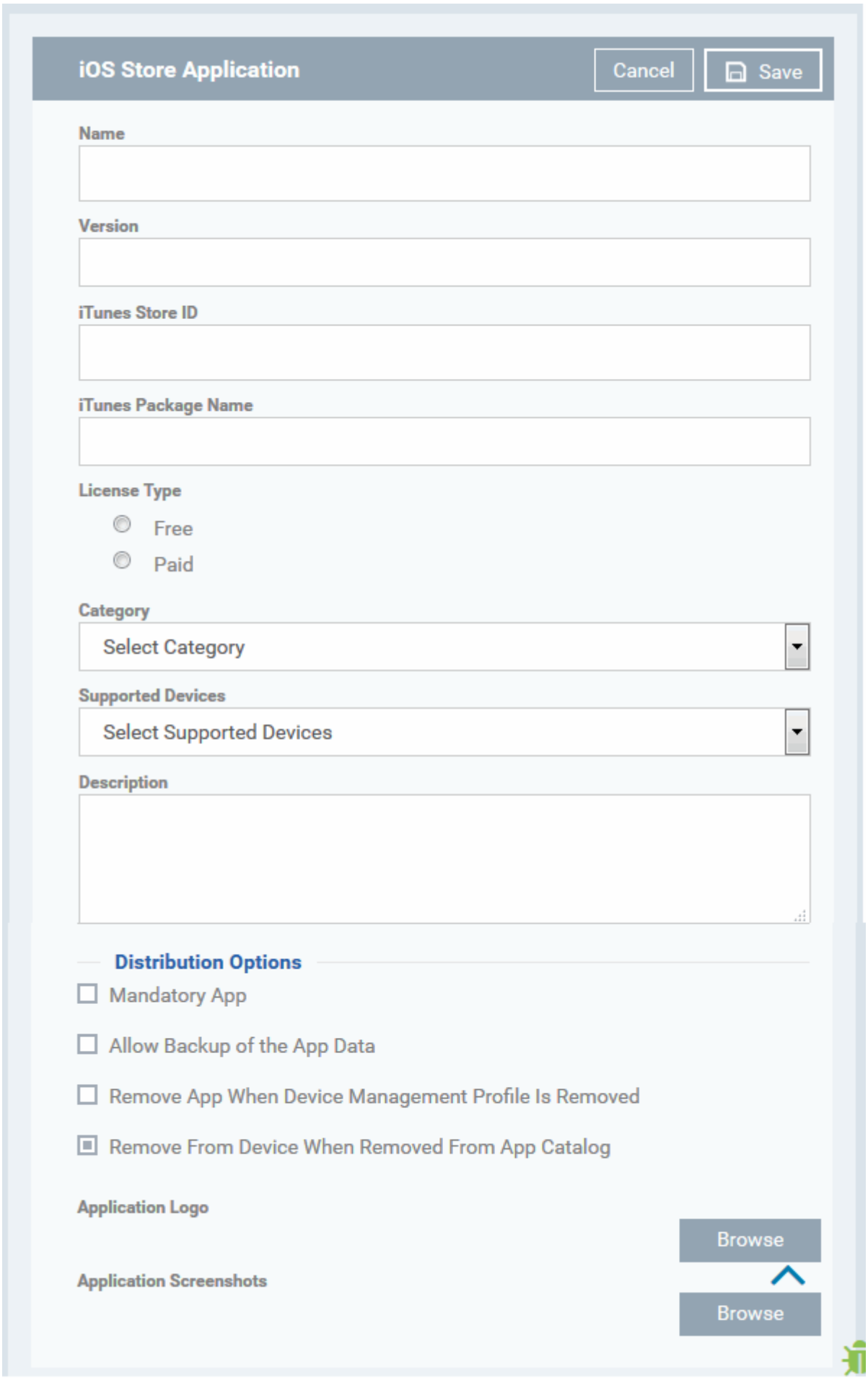
The iOS Apps from the App Store can be added by simply specifying the name of the application as it is available in the App Store page. All the other details including the version, iTunes Store ID, iTunes Package name, and so on, will be automatically fetched from the App Store page and will be populated in the 'Add iOS App Store Application' screen. You can just enter first few letters in the name of the App, ITSM will search for the matching apps from App Store for you to select the intended one.

To add an iOS App from App Store

- Click 'Application Store' from the left and choose 'iOS Store' to open the 'iOS Store' interface
- Click on 'Add App Store Application' from the options at the top.



The 'iOS Store Application' screen will open:


iOS Store Application
Cancel
Save
Name
Version
iTunes Store ID
iTunes Package Name
License Type
Free
Paid
Category
Select Category
Supported Devices
Select Supported Devices
Description
Distribution Options
Mandatory App
Allow Backup of the App Data
Remove App When Device Management Profile Is Removed
Remove From Device When Removed From App Catalog
Application Logo
Browse
Application Screenshots
Browse

Apple Store Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Allows you to enter the name of the application. • Start entering the first few letters of the name of the application. ITSM will search for Apps from the App Store using the letters entered as search criteria and display the matching results as a drop-down • Choose the App to the added from the drop-down On choosing the App all the other fields excluding the last few options will be auto-populated.
Version	Text Field	The version of the application. This field will be auto-populated on entering the correct App name in the 'Name' field.
iTunes Store ID	Text Field	The iTunes Store ID number of the App. This field will be auto-populated on entering the correct App name in the 'Name' field. Usually, this number will appear after ID in the download URL of the app. For example, in the URL https://itunes.apple.com/us/app/ITSM/id807480077, the numbers after ID is the iTunes Store ID for this app.
iTunes Package name	Text Field	The package name of the app. This field will be auto-populated on entering the correct App name in the 'Name' field. For example, the Package name for ITSM client is com.comodo.ITSM.client
License Type	Radio Button	Allows you to specify whether the app is free or a paid version. This option will be pre-chosen depending on the App chosen in the 'Name' field.
Category	Drop-down	The category will be auto-selected depending on the App chosen in the 'Name' field The drop-down also enables you to choose the category to which the App belongs.
Supported devices	Drop-down	The device type will be auto-selected depending on the App chosen in the 'Name' field The drop-down also enables you to choose the device types to which the App is compatible.
Description	Text Field	The 'Description' filed will be auto-populated with the description of the selected App, from the App Store page. The text field also enables you to enter your description or edit the existing description.
Mandatory App	Checkbox	Allows you to specify whether the app should compulsorily be installed at the devices. If enabled, all enrolled devices will get alerts automatically to install the mandatory apps. Refer to the section Installing Apps on Devices for more details.
Allow Backup of the App Data	Checkbox	If enabled, the user will be allowed to backup the application along with its user data to iTunes.

Apple Store Application - Table of Parameters		
Form Element	**Type**	**Description**
Remove App When Device Management Profile Is Removed	Checkbox	If enabled, the app will be automatically uninstalled from the device when the ITSM profile applied to the device is removed.
Remove From Device When Removed from App Catalog	Checkbox	If enabled, the app will be automatically uninstalled from the device, if it is removed from the 'App Catalog' in future for any reasons.
Application Logo	'Browse' Button	The Application logo will be automatically fetched from the App Store for the App chosen in the Name field. If you want to change the logo, upload a new logo from the local computer by clicking 'Browse'.
Application Screenshots	'Browse' Button	The Application sreenshots will be automatically fetched from the App Store for the App chosen in the Name field. If you want to add new screenshots from the local computer, upload them by clicking 'Browse'.

- Click 'Save' after entering the details.

The App will be added to the App repository and will be listed in the 'App Catalog' interface and will be synched to the devices during their next poll.

- If you want the devices to be notified to install the app, click 'Inform Devices Now' from the options above the table in the 'iOS App Catalog' interface.

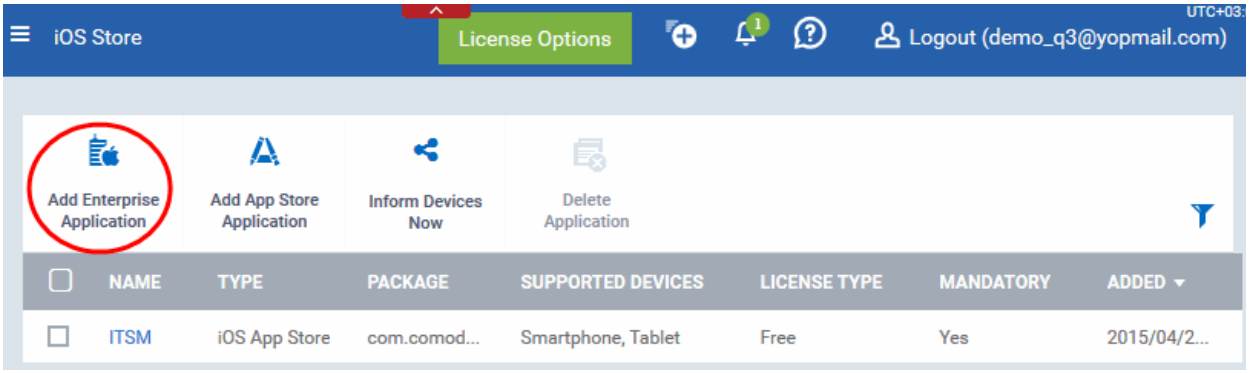
Adding Custom/Enterprise iOS Apps

Custom and Enterprise applications to be installed on the managed iOS devices can be added to the ITSM App repository by simply uploading the .ipa file for the App. The details of the file like name, version, bundle ID and so on, will be automatically fetched by parsing the file and saved. You just need to manually enter only some of the details, which could not be fetched from the .ipa file.

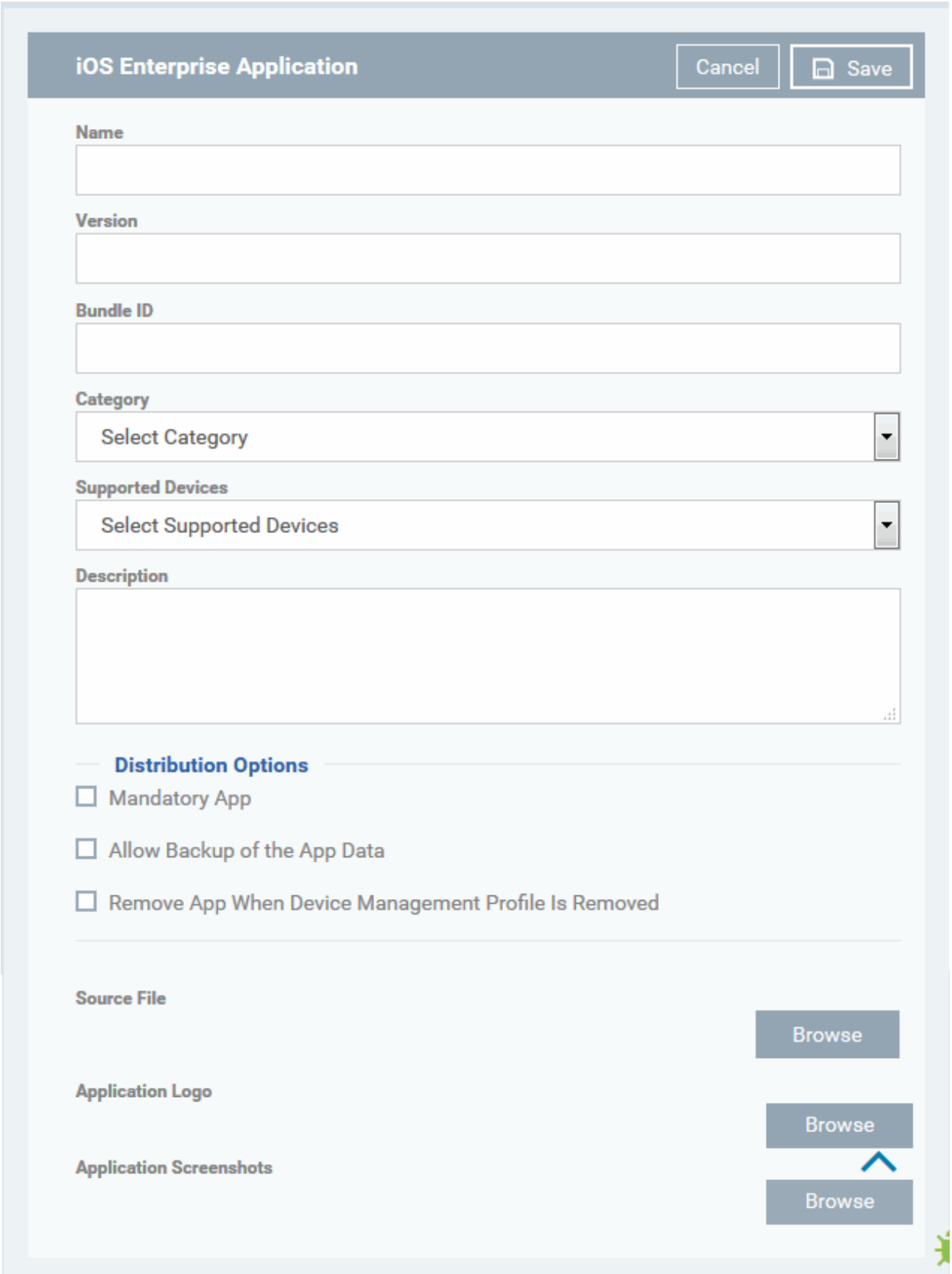
Prerequisite: The .ipa file of the app should have been saved in the computer or in the network storage accessible through the computer, from which the ITSM console is accessed.

To add Custom/Enterprise iOS Apps

- Click 'Application Store' from the left and choose 'iOS Store' to open the 'iOS Store' interface
- Click on 'Add Enterprise Application' from the options at the top.



The 'iOS Enterprise Application' screen will open.



- Click 'Browse' under 'Source File', navigate to the location of the .ipa file to be uploaded, select the file and click 'Open'

The file will be uploaded and the details will be auto-populated.

Add iOS Enterprise Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	The name of the application as obtained from the .ipa file and auto-populated. If not auto-populated, enter the name of the app.
Version	Text Field	The version of the application as obtained from the .ipa file. If it is not auto-populated, enter the version number of the app.
Bundle ID	Text Field	The bundle identifier of the app as obtained from the .ipa file. If it is not auto-populated, enter the bundle identifier of the app. Usually, this number will appear after ID in the download URL of the app. For example, in the URL https://itunes.apple.com/us/app/ITSM/id807480077, the numbers after ID is the iTunes Store ID for this app.
Category	Drop-down	The drop-down enables you to choose the category to which the App belongs.
Supported devices	Drop-down	The drop-down enables you to choose the device types to which the App is compatible.
Description	Text Field	Allows you to enter a description for the App.
Mandatory App	Checkbox	Allows you to specify whether the app should compulsorily be installed at the devices. If enabled, all enrolled devices will get alerts automatically to install the mandatory apps. Refer to the section Installing Apps on Devices for more details.
Allow Backup of the App Data	Checkbox	If enabled, the user will be allowed to backup the application along with its user data to iTunes.
Remove App When Device Management Profile Is Removed	Checkbox	If enabled, the app will be automatically uninstalled from the device, if the ITSM profile applied to the device is removed.
Source File	Browse button	Enables you to navigate and select the source file for the app to be uploaded.
Application Logo	Browse button	Enables you to upload the logo image for the App.
Application Screenshots	Browse button	Allows you to upload screenshots of the app, if required.

- Click 'Save' after entering the details.

The App will be added to the App repository and will be listed in the 'App Catalog' interface and will be synched to the devices during their next poll.

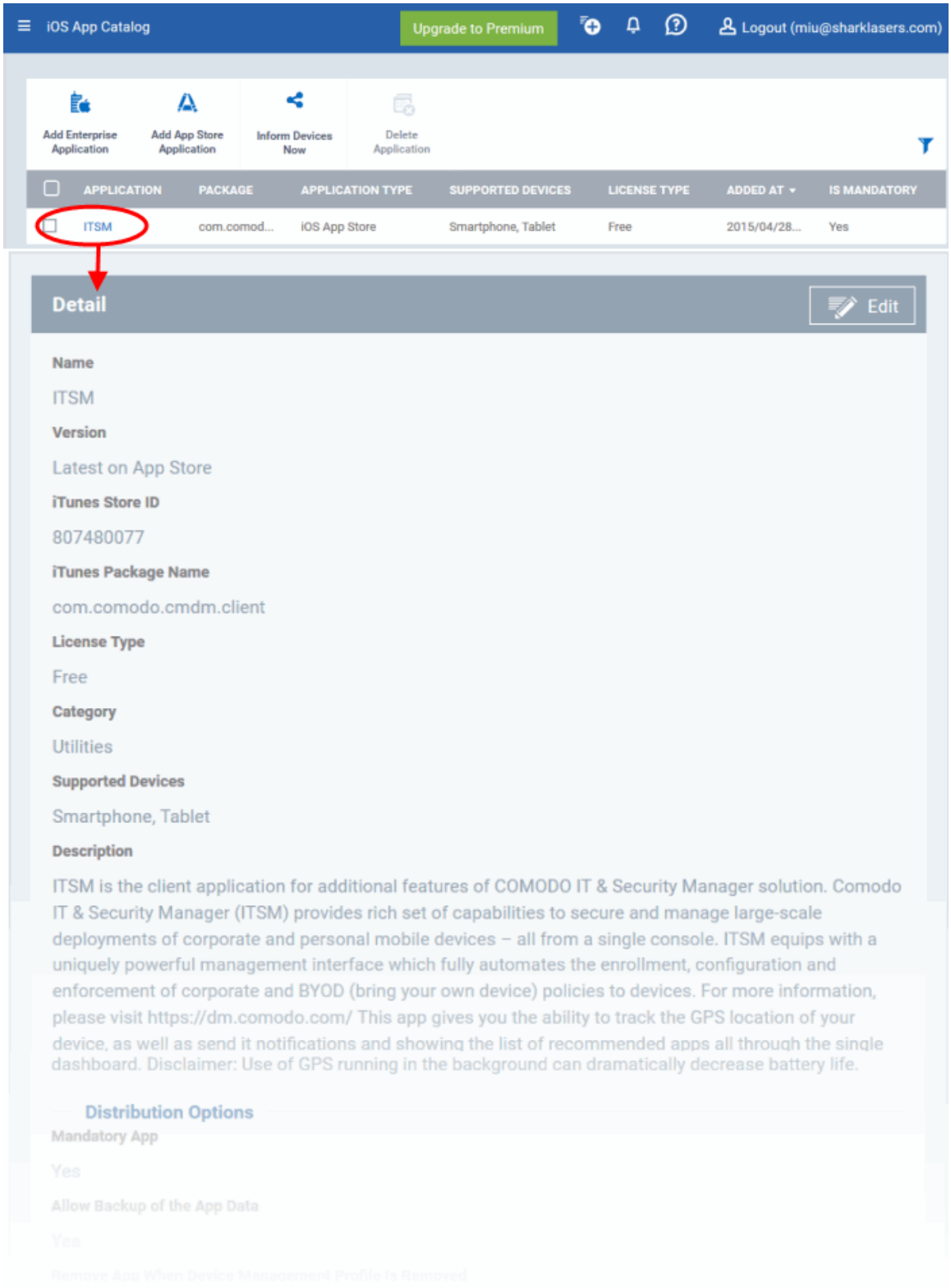
- If you want the devices to be notified to install the app, click 'Inform Devices Now' from the options above the table in the 'App Catalog' interface.

8.1.2. Managing iOS Apps

The 'Application Details' page for a selected application from the list in iOS App Catalog, displays complete details of the 'App' and allows you to edit the details.

To open the 'App Details' page

- Click 'Application Store' from the left and choose 'iOS Store' to open the 'iOS Store' interface
- Click on the name of the App.



The 'Application Details' page displays the details of the App, including the logo, screenshots and the download URL, depending on whether it is iOS App Store App or Custom/Enterprise App. The details page also allows you to edit the details of the App.

To edit the details of an application

- Click on the 'Edit' button  at the top right .

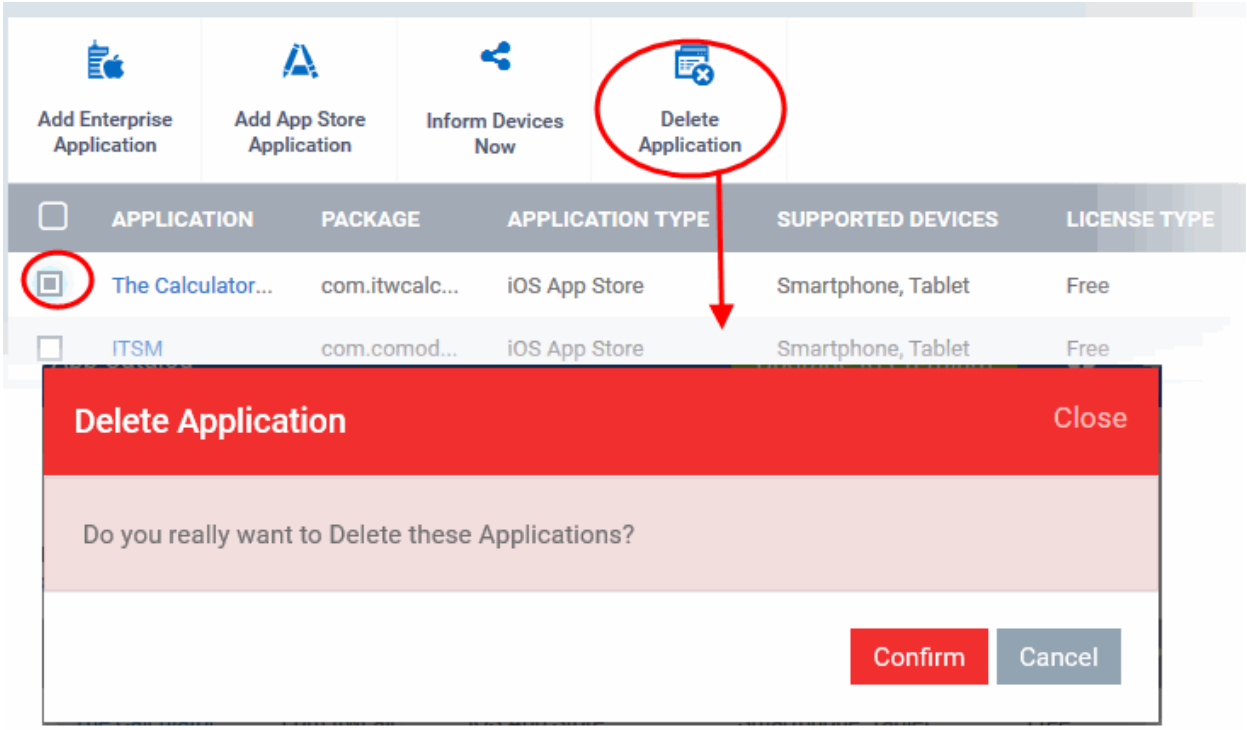
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section **Adding iOS Apps and Installing them on Devices**.

Removing Apps from the iOS App Catalog

You can remove unwanted applications from the App Repository at any time. If the option 'Remove from device when removed from app catalog' is selected while adding/editing an App, the App will also be removed from the devices at which it is installed.

To remove selected Apps

- Click 'Application Store' from the left and choose 'iOS Store' to open the 'iOS Store' interface
- Select the App(s) to be removed and click 'Delete Application' from the options above the table.

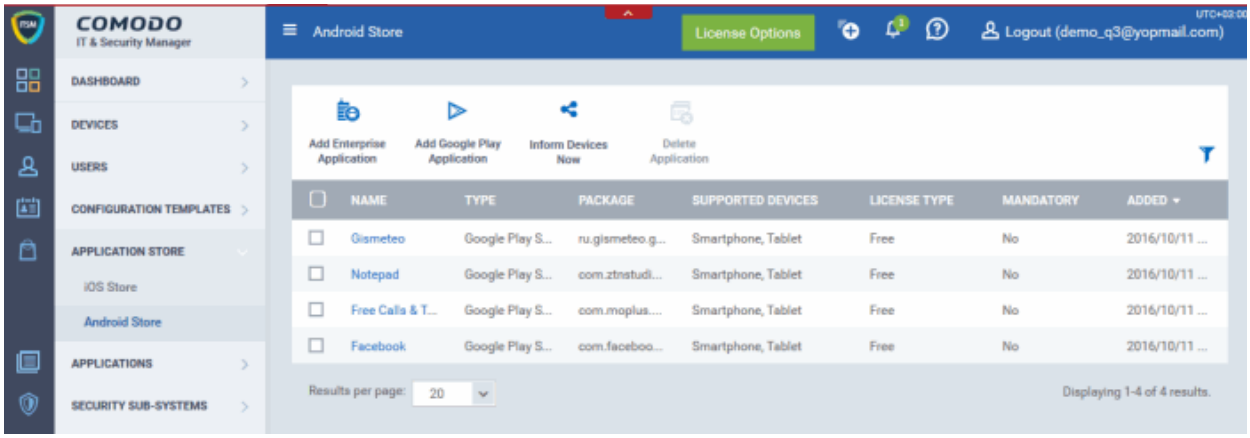


- Click 'Confirm' in the confirmation dialog to remove the app(s)

8.2. Android Apps

The 'Android Store' interface displays a list of all available Android apps and allows you to add new apps from the Google Play Store. You can also upload custom enterprise apps and synchronize the app list to the managed Android devices. You can edit existing app parameters and remove any unwanted apps from the repository.

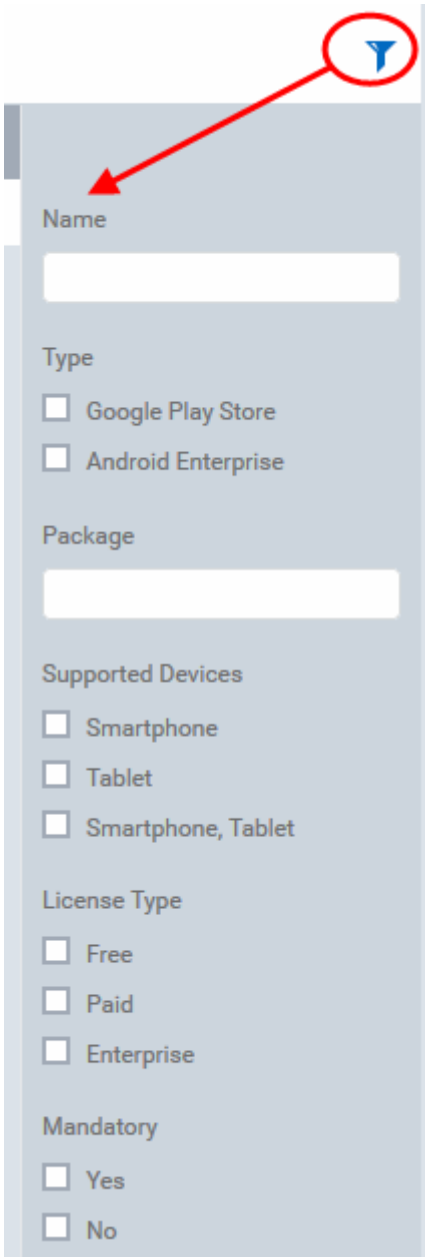
- To open the 'Android Store' interface, click 'Application Store' from the left and choose 'Android Store' from the options.



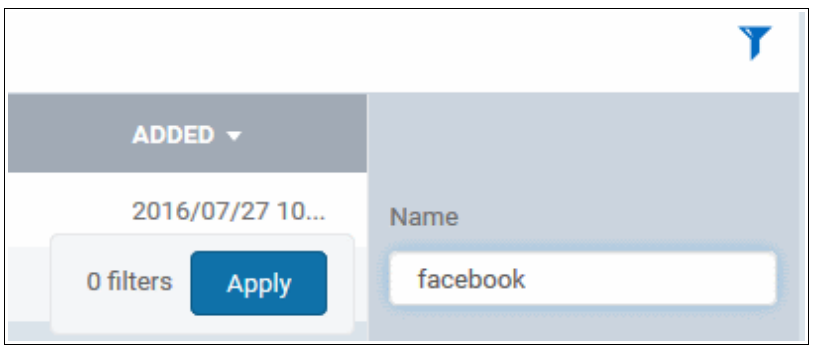
'Android Store' - Column Descriptions	
Column Heading	**Description**
Name	Displays the name of the application. Clicking on the name of an app opens the 'Detail' screen that displays the details like description, version number, Bundle ID, category, supported devices, whether the app is mandatory or optional, whether this application can be installed or Uninstalled silently when possible and details of source file. The Details screen also allows you to edit the app details. Refer to the section **Managing Android Apps** for more details.
Package	Displays the Bundle Identifier of the app.
Type	Indicates the source type of the app. Possible types are: • Google Play Store Application • Android Enterprise Application uploaded by the administrator
Supported Devices	Displays the type of devices for which the application is compatible.
License Type	Indicates whether the app is a free, paid or enterprise version.
Mandatory	Indicates whether the app has been marked to be installed compulsorily on the devices. Refer to the section '**Adding Android Apps and Installing them on Devices**' for more details
Added	Displays the date and time at which the app was added to repository.

Sorting, Search and Filter Options

- Clicking on any of the column headers sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific app based on the app name and/or its package name, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- To filter the items based on their application name, select the criteria under 'Name'.
- To filter the items based on their application type, select the criteria under 'Type'
- To filter the items based on type of devices on which they can be installed, select the device type from 'Supported Devices'

- To filter the items based on license type, select the criteria from 'License Type'
- To view only mandatory or only optional apps, select the respective type from 'Mandatory' options.

You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The following sections explain in detail on:

- Adding Android Apps and Installing them on Devices
- Managing Android Apps

8.2.1. Adding Android Apps and Installing them on Devices

You can add Android apps to the repository both from Google Play Store and by uploading custom/enterprise apps for installation on to managed Android smart phones and tablets.

The following sections provide more details on:

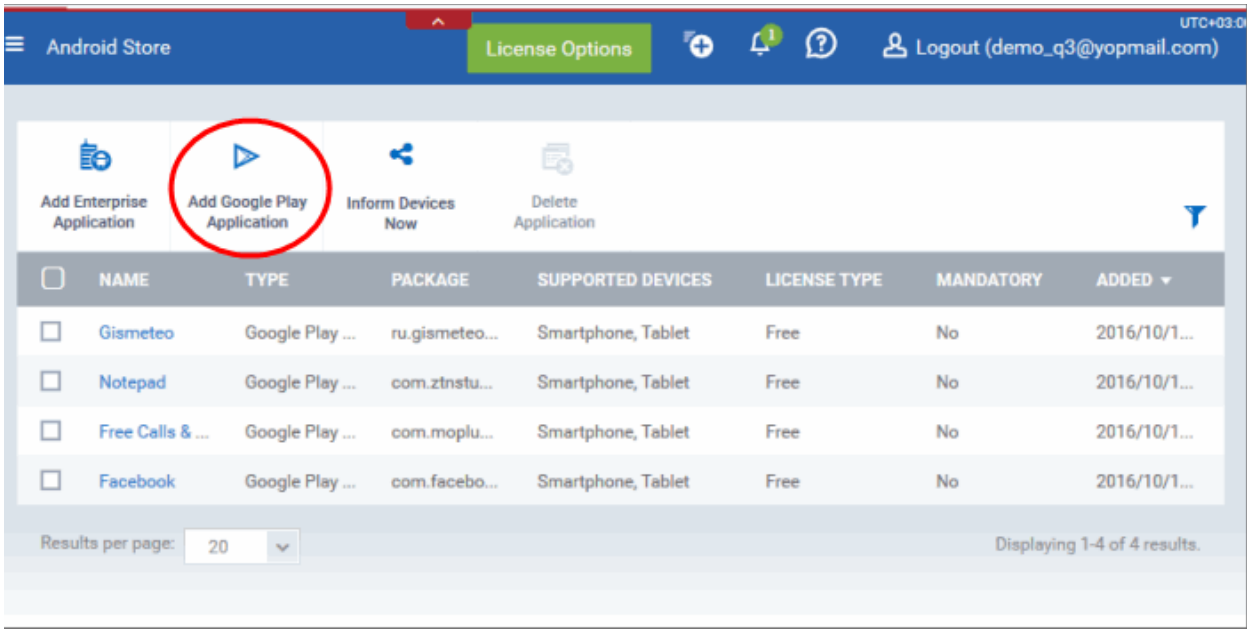
- Adding Android Apps from App Store
- Adding Custom/Enterprise Android Apps

Adding Android Apps from Google Play Store

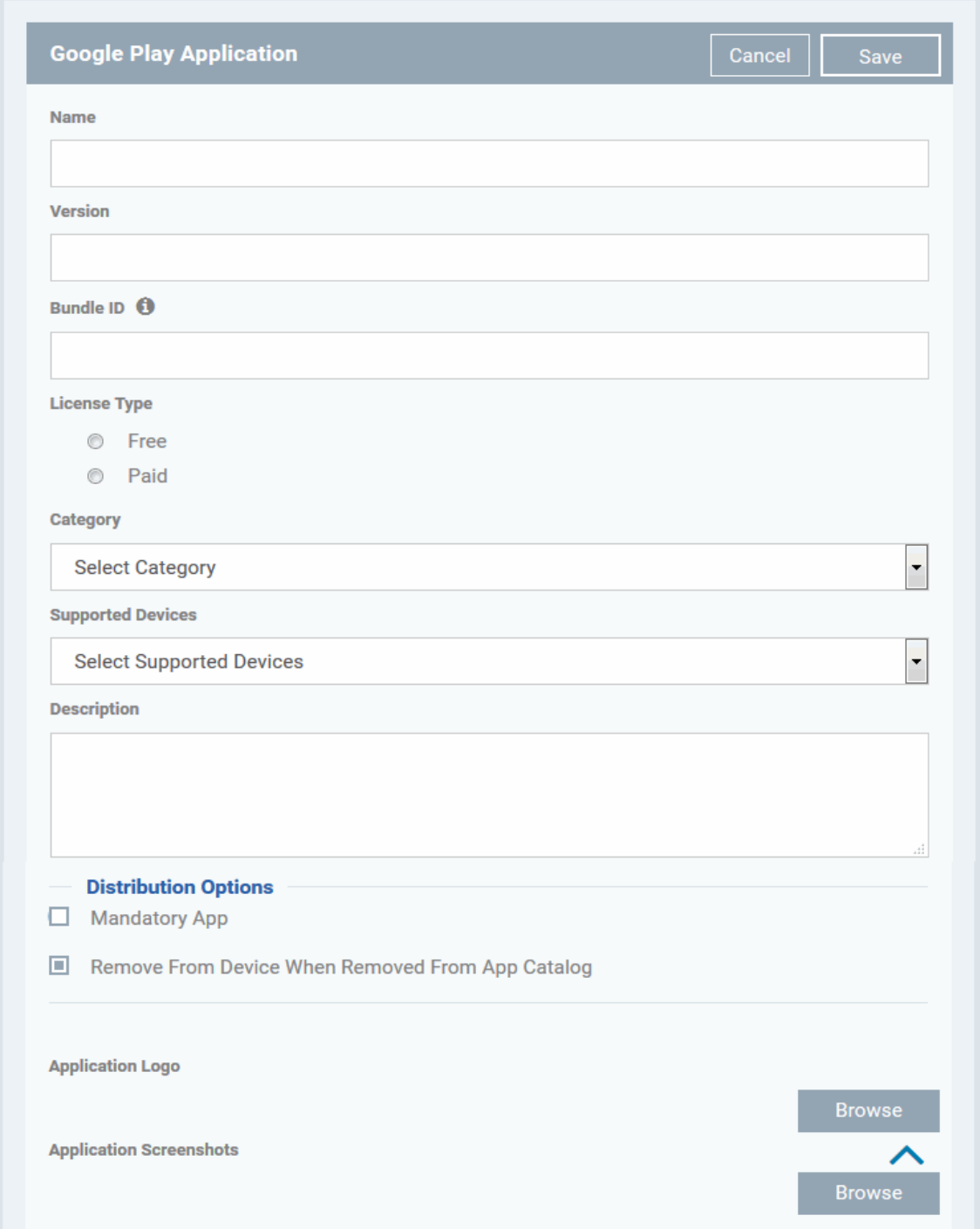
The Android Apps from the Google Play Store can be added by simply specifying the name of the application as it is available in the Play Store page. All the other details including the version, bundle ID, app logo and so on, will be automatically fetched from the Google Play Store page and will be populated in the 'Google Play Application' screen. You can just enter first few letters in the name of the App, ITSM will search for the matching apps from Google Play Store for you to select the intended one.

To add an Android App from Google Play Store

- Click 'Application Store' from the left and choose 'Android Store' to open the 'Android Store' interface
- Click on 'Add Google Play Application' from the options at the top.



The 'Google Play Application' screen will open.



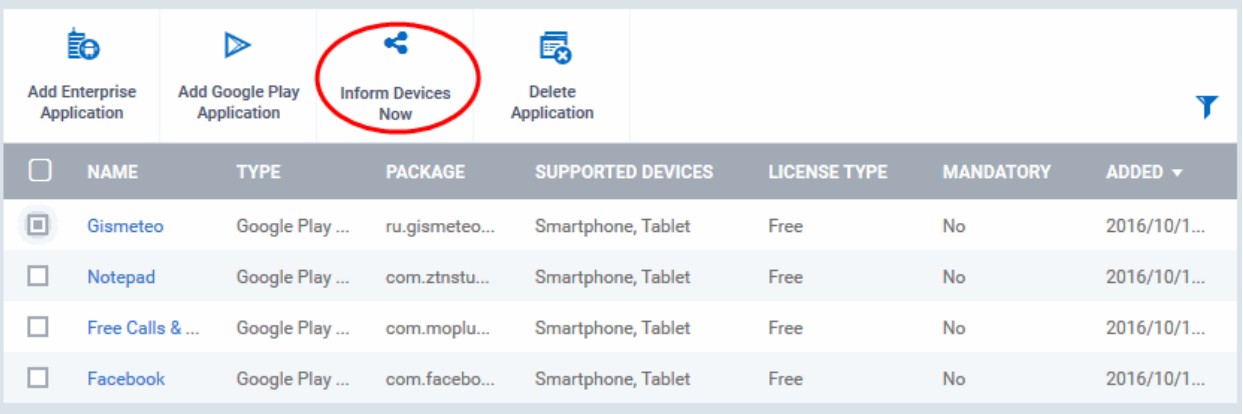
Google Play Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Allows you to enter the name of the application. • Start entering the first few letters of the name of the application. ITSM will search for Apps from the Google Play Store using the letters entered as search criteria and display the matching results as a drop-down • Choose the App to the added from the drop-down On choosing the App all the other fields excluding the last few options will be auto-populated.

Google Play Application - Table of Parameters		
Version	Text Field	The version of the application. This field will be auto-populated on entering the correct App name in the 'Name' field.
Bundle ID	Text Field	The bundle identifier of the app. Usually this is must be in the reverse DNS format, for example, 'com.comodo.mobile.comodoantitheft'. In the Google Play store, the identifier is located between '=' and '&' in the URL. An example is shown below: https://play.google.com/store/apps/details?id=com.comodo.pimsecure&hl=en The identifier, com.comodo.pimsecure, identifies this as Comodo Antivirus Free app. Clicking the help icon beside the field displays how to retrieve the bundle identifier for the Play Store Apps. This field will be auto-populated on entering the correct App name in the 'Name' field.
License Type	Radio Button	Allows you to specify whether the app is free or a paid version. This option will be pre-chosen depending on the App chosen in the 'Name' field.
Category	Drop-down	The category will be auto-selected depending on the App chosen in the 'Name' field. The drop-down also enables you to choose the category to which the App belongs.
Supported Devices	Drop-down	The device type will be auto-selected depending on the App chosen in the 'Name' field. The drop-down also enables you to choose the device types to which the App is compatible.
Description	Text Field	Allows you to enter a description for the App. The 'Description' filed will be auto-populated with the description of the selected App, from the Google Play Store page. The text field also enables you to edit the description or enter your own description of the app.
Mandatory App	Checkbox	Allows you to specify whether the app should compulsorily be installed at the devices. If enabled, all enrolled devices will get alerts automatically to install the mandatory apps. Refer to the section Installing Apps on Devices for more details.
Remove From Device When Removed From App Catalog	Checkbox	If enabled, the app will be automatically uninstalled from the device, if it is removed from the 'App Catalog' in future for any reasons.
Application Logo	Button	The Application logo will be automatically fetched from the Google Play Store for the App chosen in the Name field. If you want to change the logo, upload a new logo from the local computer by clicking 'Browse'.
Application Screenshots	Button	The Application screenshots will be automatically fetched from the Google Play Store for the App chosen in the Name field. If you want to add new screenshots from the local computer, upload them by clicking 'Browse'.

- Click 'Save' after entering the details.

The App will be added to the App repository and will be listed in the 'Android Store' interface and will be synced to the devices during their next poll.

- If you want the devices to be notified to install the app, click 'Inform Devices Now' from the options above the table in the 'Android Store' interface.



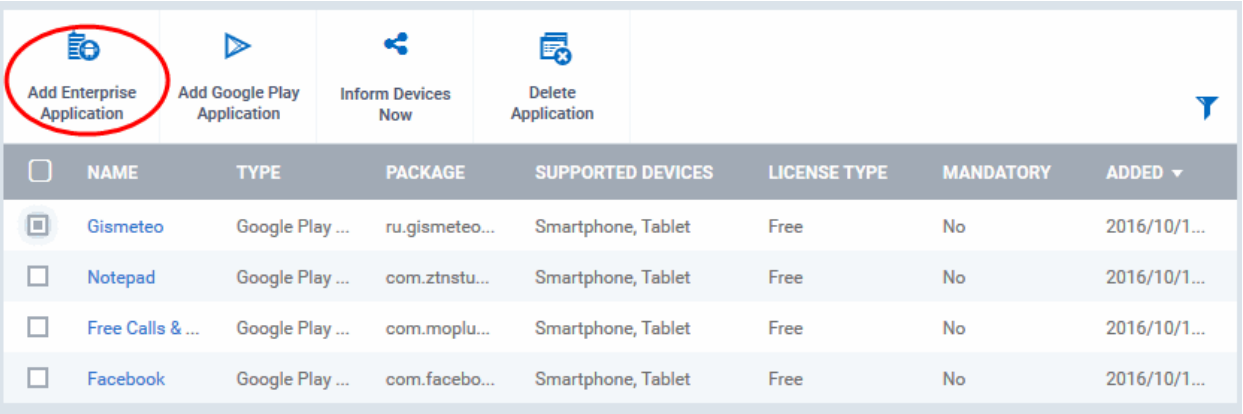
Adding Custom/Enterprise Android Apps

Custom and Enterprise applications to be installed on the managed Android devices can be added to the ITSM App repository by uploading the .apk file for the App. The details of the file like name, version, bundle ID and so on, will be automatically fetched by parsing the file and saved. You need to manually enter the details, which could not be fetched from the .apk file.

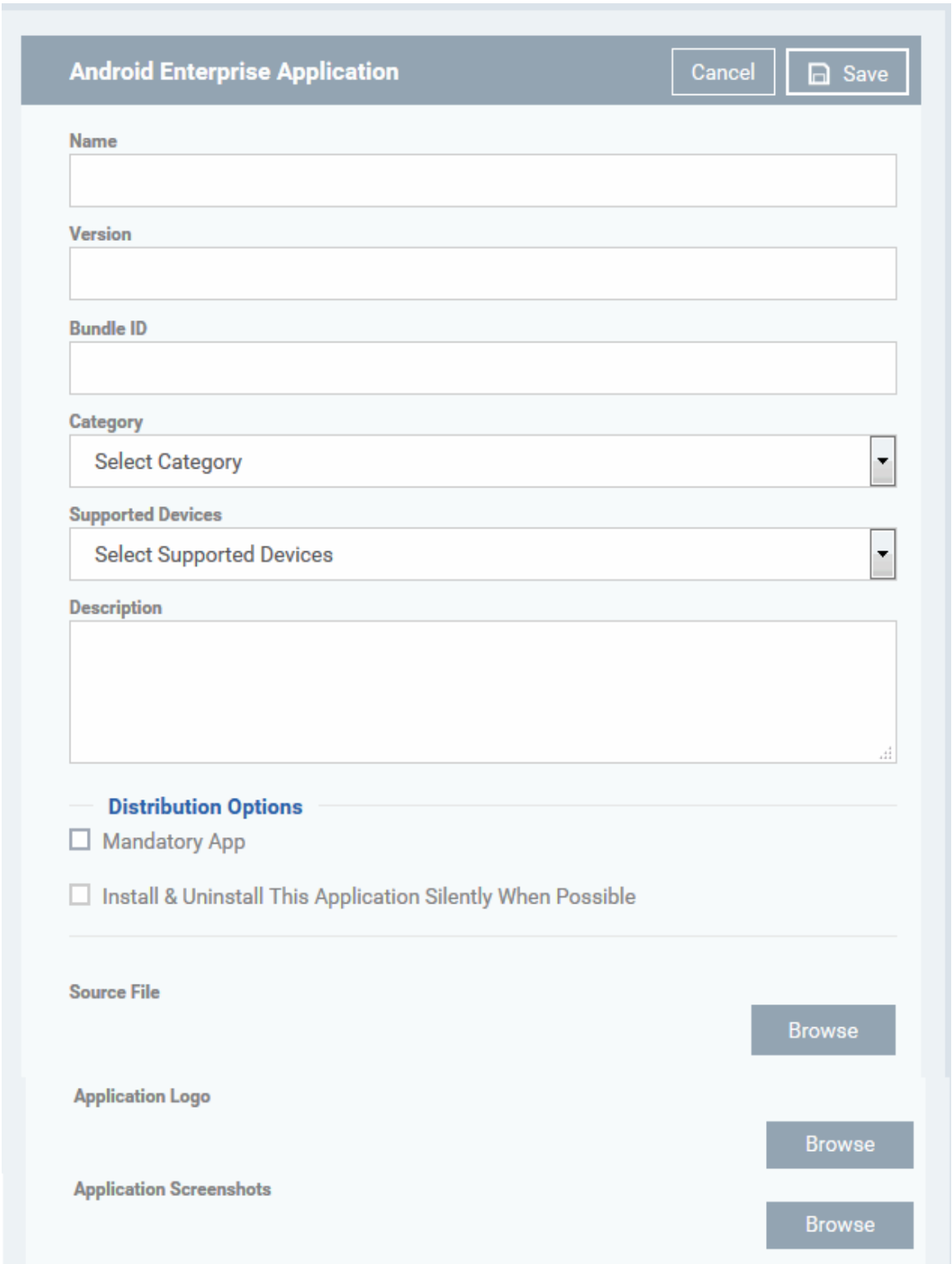
Prerequisite: The .apk file of the app should have been saved in the computer or in the network storage accessible through the computer, from which the ITSM console is accessed.

To add Custom/Enterprise Android Apps

- Click 'Application Store' from the left and choose 'Android Store' to open the 'Android Store' interface
- Click on 'Add Enterprise Application' from the options at the top.



The 'Android Enterprise Application' screen will open.



- Click 'Browse' under 'Source File', navigate to the location of the .apk file to be uploaded, select the file and click 'Open'

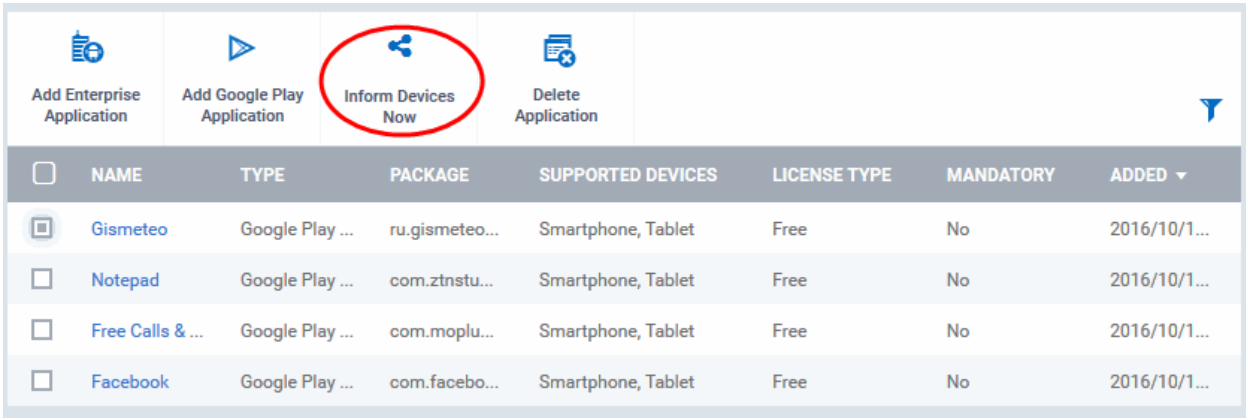
The file will be uploaded and the details will be auto-populated.

Add Enterprise Android Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	The name of the application as obtained from the .apk file. If the name is not auto-populated, enter the name of the app.
Version	Text Field	The version of the application as obtained from the .apk file. If it is not auto-populated, enter the version number of the app.
Bundle ID	Text Field	The bundle identifier of the app as obtained from the .apk file.
Category	Drop-down	The category to which the app belongs. If not automatically chosen, you can select the category from the drop-down.
Supported Devices	Drop-down	The type(s) of device(s) to which the app is compatible. Choose the device type from the drop-down.
Description	Text Field	Enter an appropriate description for the app.
Mandatory App	Checkbox	Allows you to specify whether the app should compulsorily be installed at the devices. If enabled, all enrolled devices will get alerts automatically to install the mandatory apps. Refer to the section **Installing Apps on Devices** for more details.
Install & Uninstall This Application Silently When Possible	Checkbox	This can be enabled only when the 'Mandatory app' checkbox is selected. Enabling this option, the mandatory apps are installed silently without user interaction. On removing the app from the App Repository, it will also be uninstalled from the device. This feature will work only for rooted and Samsung KNOX devices.
Source File	'Browse' button	Enables you to navigate and select the source file for the app to be uploaded.
Application Logo	'Browse' button	The application logo will be automatically fetched from the .apk file. If the logo is not auto-fetched, click the 'Browse' button and upload the logo.
Application Screenshots	'Browse' button	Allows you to upload screenshots of the app, if required.

- Click 'Save' after entering the details.

The App will be added to the App repository and will be listed in the 'Android Store' interface and will be synched to the devices during their next poll.

- If you want the devices to be notified to install the app, click 'Inform Devices Now' from the options above the table in the 'Android Store' interface.

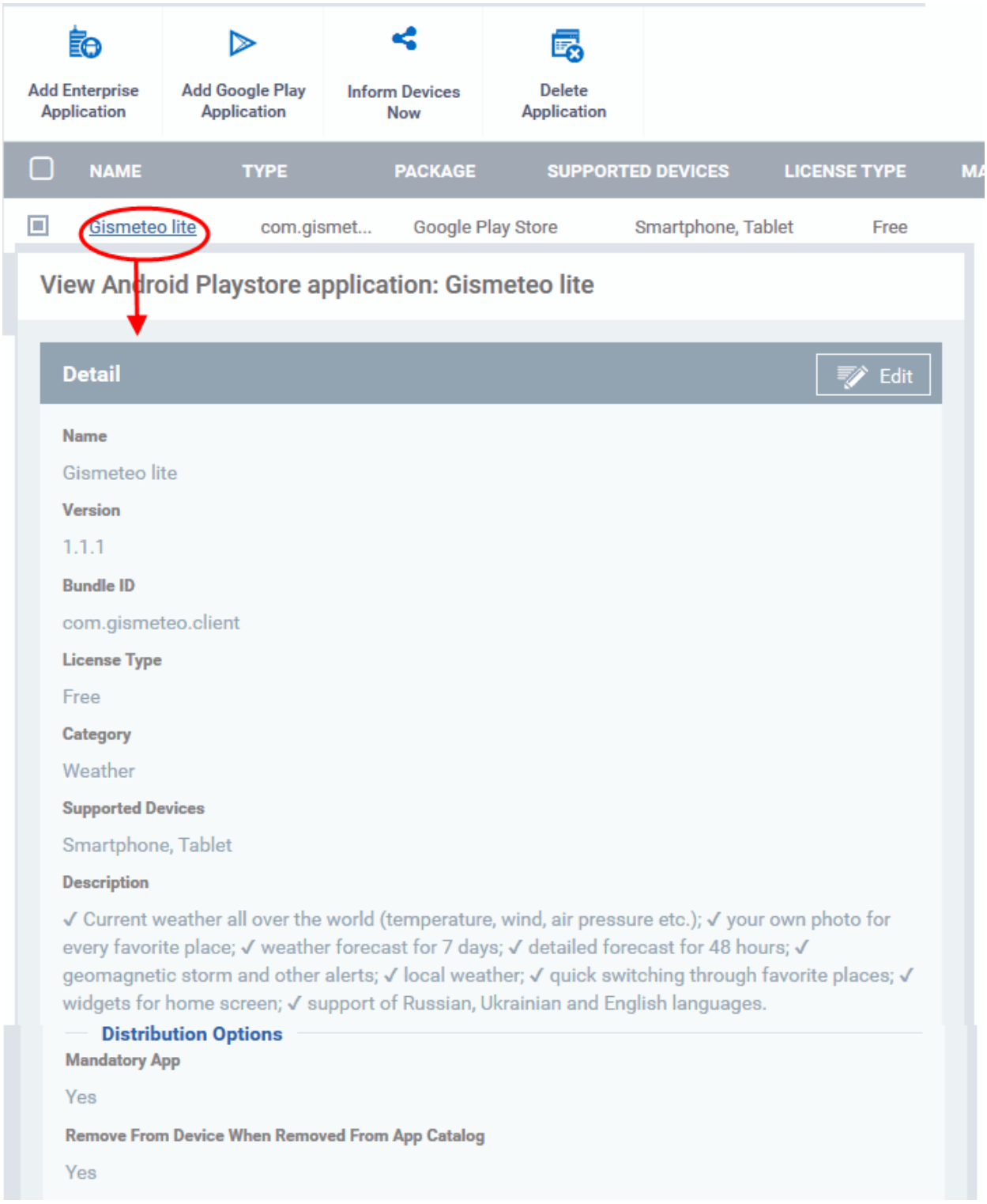


8.2.2. Managing Android Apps

The 'Application Details' page for a selected application from the list in Android Store, displays complete details of the 'App' and allows you to edit the details.

To open the 'App Details' page

- Click 'Application Store' from the left and choose 'Android Store' to open the 'Android Store' interface
- Click on the name of the App.



The 'Application Details' page displays the details of the App, including the logo, screenshots and the download URL, depending on whether it is Google Play Store App or Custom/Enterprise App. The details page also allows you to edit the details of the App.

To edit the details of an application

- Click on the 'Edit' button  at the top right .

The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section Adding Android Apps and Installing them on

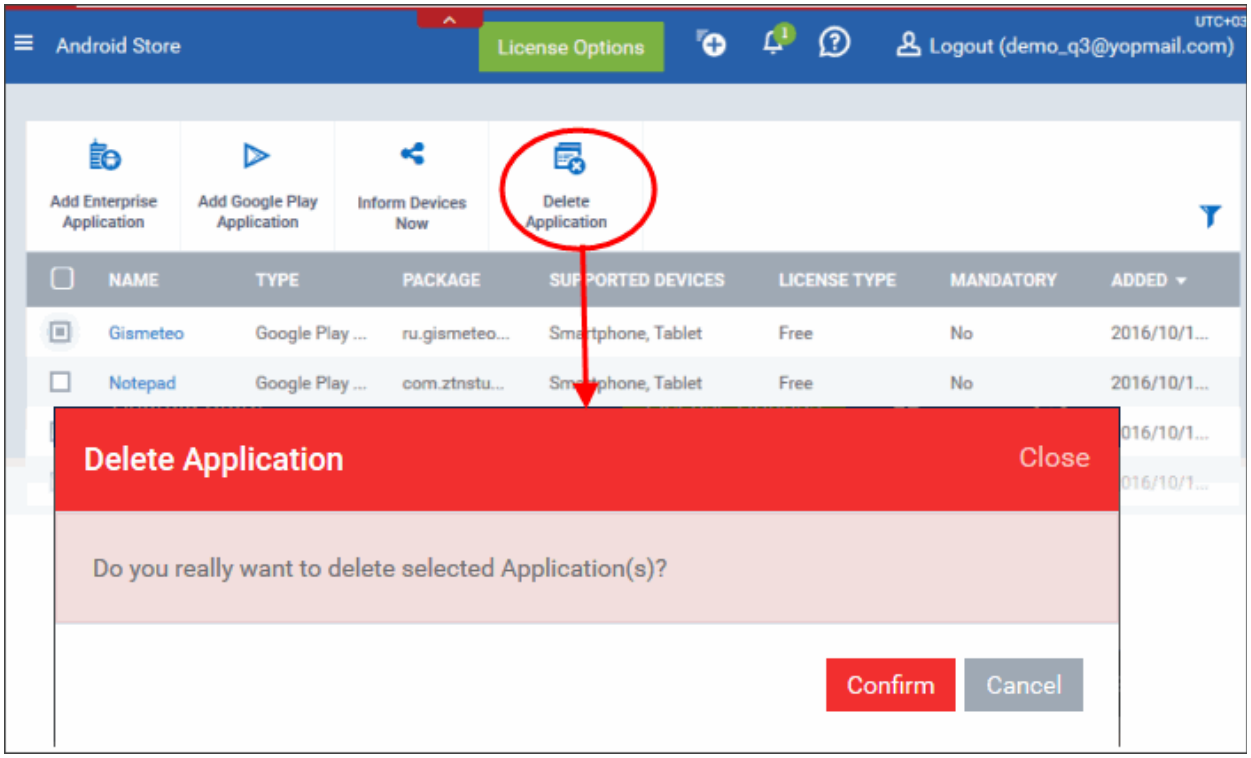
Devices.

Removing Apps from the Android App Catalog

You can remove unwanted applications from the Android App Repository at any time. If the option 'Remove from device when removed from app catalog' is selected while adding/editing an App, the App will also be removed from the devices at which it is installed.

To remove selected Apps

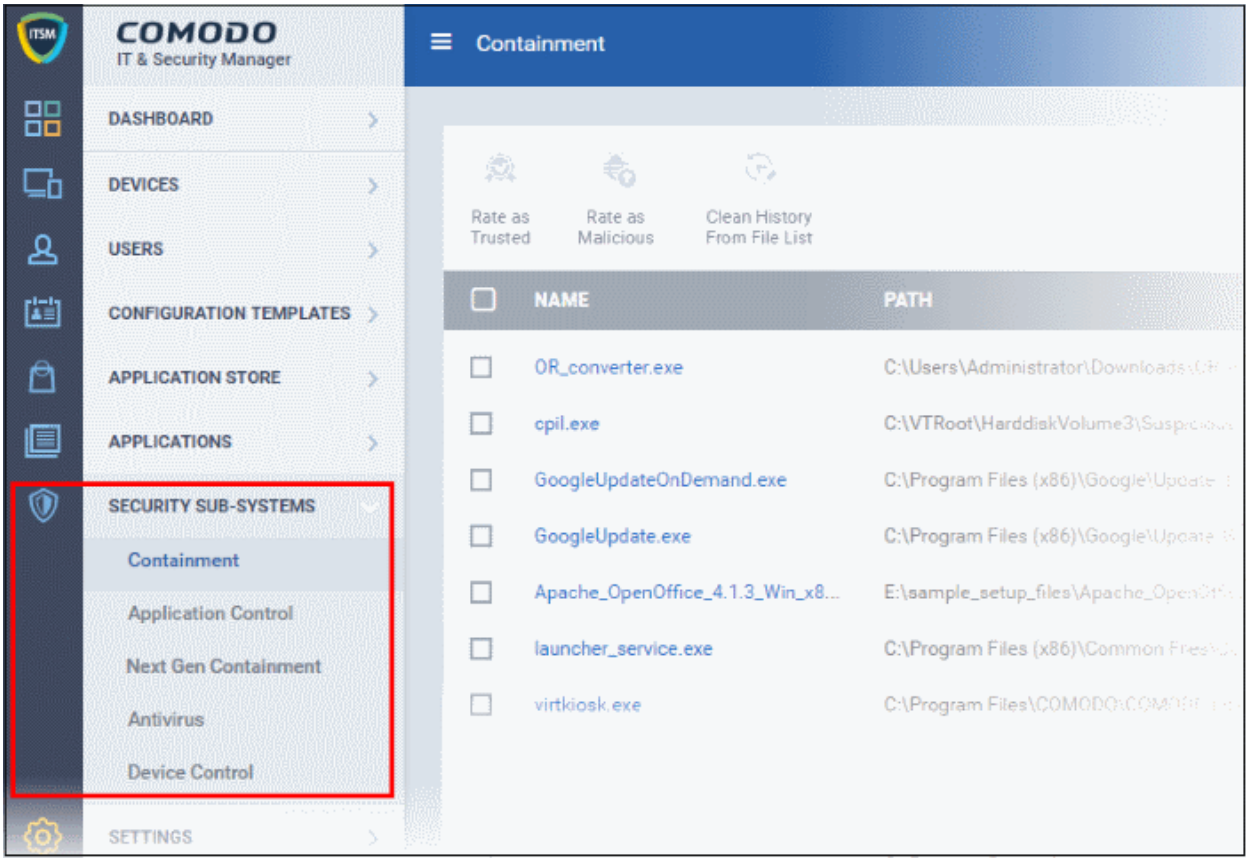
- Click 'App Store' from the left and choose 'Android' to open the 'Android App Catalog' interface
- Select the App(s) to be removed and click 'Delete Application' from the options.



9.Security Sub Systems

The 'Security Sub systems' interface allows administrators to view the infection status of managed Android, Mac OS and Windows devices, initiate on-demand AV and file rating scans and to initiate virus database updates. Administrators can view the list of malware found on the devices from various real-time, on-demand and scheduled scans, take actions against them and to view a history of threats identified on all devices. The section also allows administrators to:

- View a list of applications and files discovered on managed Windows devices under 'Unrecognized', 'Trusted' and 'Malicious' categories. Administrators can move the files between the categories based on their analysis.
- View files that were run inside the container on managed Windows endpoints.
- View and manage files that were moved to quarantine by CCS on Windows endpoints and by CAVM on Mac OS endpoints.



The following sections contain more details on each area:

- Viewing Contained Applications
- Viewing applications installed on Windows Devices
  - Viewing and Managing Unrecognized files
  - Viewing and Managing Trusted Files
  - Viewing and Managing Malicious Files
  - Viewing and Managing Quarantined Items
- Viewing and Managing Quarantined Items on Mac OS Devices
- Viewing List of Valkyrie Analyzed Files
- Antivirus and File Rating scans
  - Running On-Demand Antivirus Scans on Devices
  - Running Rating Scans on Windows Devices
  - Handling Malware on Scanned Devices
  - Updating Virus Signature Database on Windows Devices
  - Updating Virus Signature Database on Mac OS Devices
- Viewing and Managing Identified Malware
- Viewing Threats History
- Viewing History of External Device Connection Attempts

9.1. Viewing Contained Applications

The Containment component of CCS on each endpoint provides an isolated environment in which unknown/unrecognized are run. Contained applications are not permitted to access files or user data on the host machine.

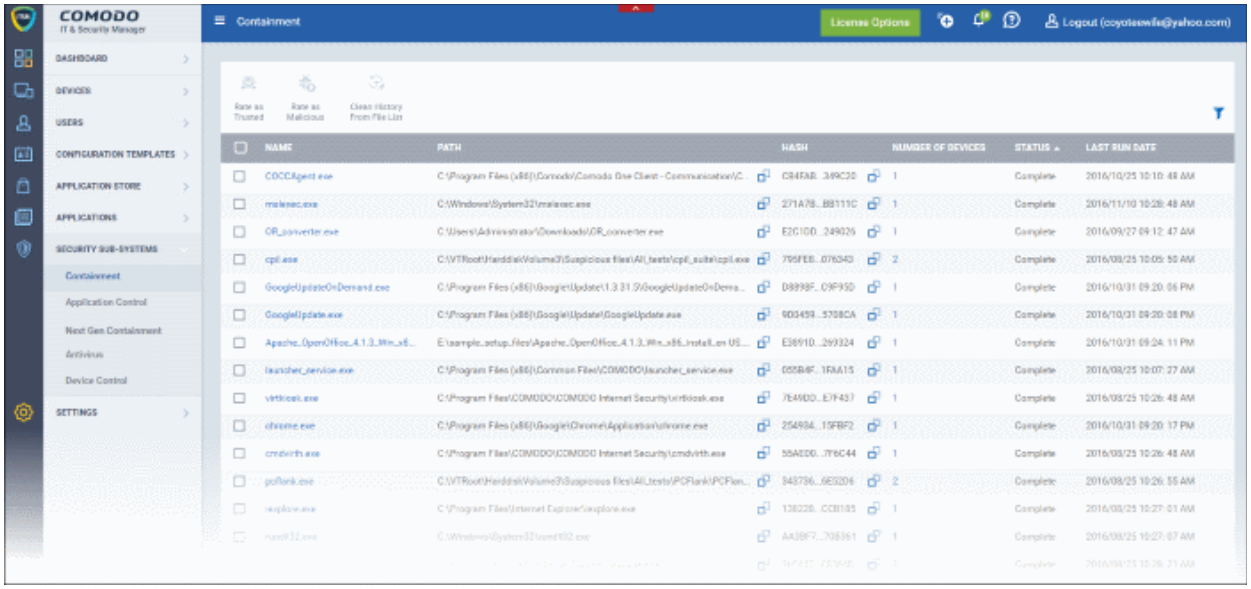
An application is run inside the container when:

- The application is auto-contained based on rules defined in the configuration profile applied to the endpoint. Refer to the description under 'Containment Settings' in the section Creating Windows Profiles for more details on setting the Containment Rules for a profile.
- The application is auto-contained based on rules defined in CCS on the endpoint
- The user at the endpoint runs a program inside the container on a 'one-off' basis. This is helpful to test the behavior of new executables that have they downloaded or for applications that they are not sure that you trust.

Administrators can view a list of all programs that have been executed inside the container from the 'Containment' interface. The administrator can also view the activities of the processes executed by the contained applications. The interface also allows administrators to rate a contained file as trusted or malicious.

To open the 'Containment' Files List interface

- Click the 'Security Sub-System' from the left and choose 'Containment' from the options

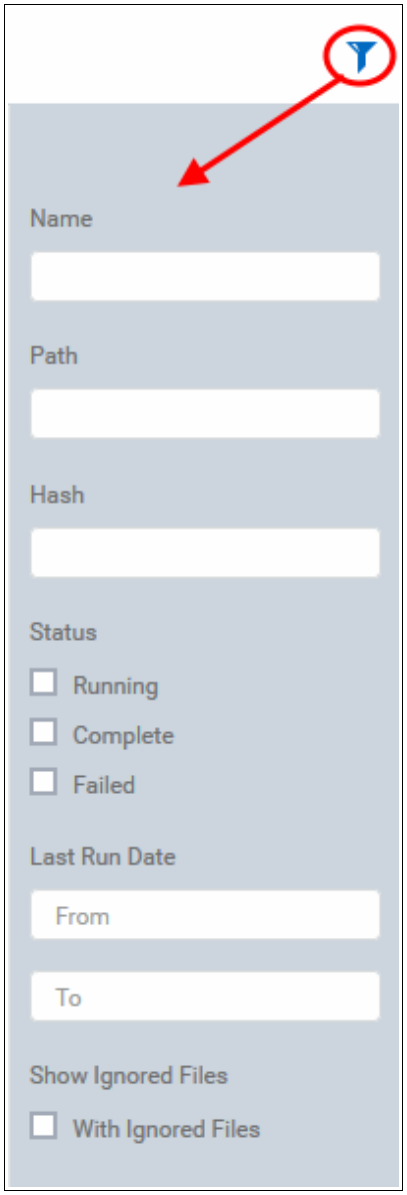


Containment - Column Descriptions	
Column Heading	**Description**
Name	Displays the file name of the 'Contained' executable.
Path	The endpoint location of the file which was run inside the container.
Hash	Displays the hash value of the file derived using SHA1 hash algorithm.
Number of Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device List' interface with a list of endpoints from which the item was identified and allow the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device List Screen below.
Status	Indicates whether the executable is currently running inside the container at the endpoint, completed execution or failed to execute.
Last Run Date	The date and time at which the file was started executing inside the container.
Controls	

Rate as Trusted	Allows administrators to rate contained files as trusted. Trusted files are allowed to run outside the container. The changed file verdict is sent to the endpoints.
Rate as Malicious	Allows administrators to rate the contained files as malicious. Malicious files will be moved to quarantine. The changed file verdict is sent to the endpoints.
Clean History From File List	Allows administrators to remove unwanted files from the list.

Sorting and Filtering Options

- Clicking on 'Name', 'Path', 'Status', 'Start Date' and/or 'Number of Devices' column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter items or search for a specific file, enter the search criteria in part or full in the respective text boxes and click 'Apply'.
- To display results with files ignored by containment, select 'With Ignored Files'

You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Contained Items

The 'Containment' interface allows you to:

- View the details of the contained applications
- Rate the files
- Remove files from list

Viewing the details of contained items

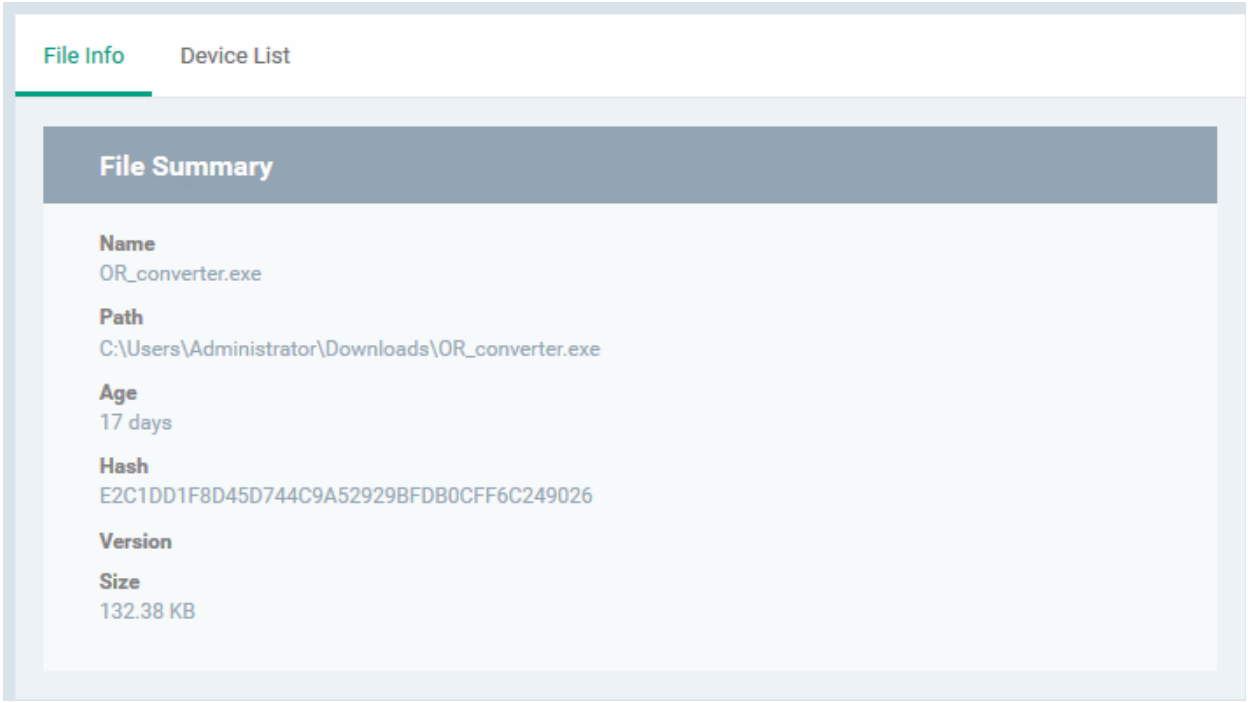
- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- File Info - Displays the general information on the selected item.
- Device List- Displays the list of endpoints up on which the item was identified with its activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Containment' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.



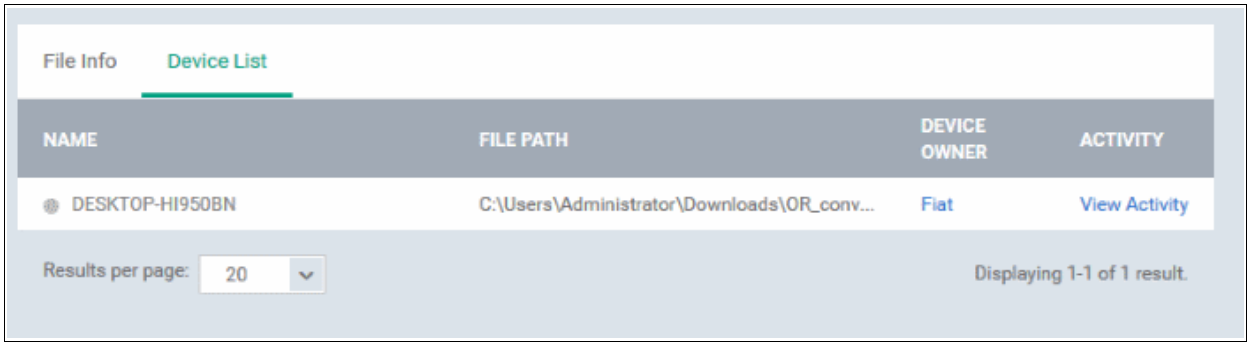
The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, and its age.

Device List Screen

The 'Device List' screen can be opened by clicking the 'Device List' tab in the 'File Info' interface.

The 'Device List' displays the list of endpoints on which the item was identified and its activities at each endpoint.

The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.



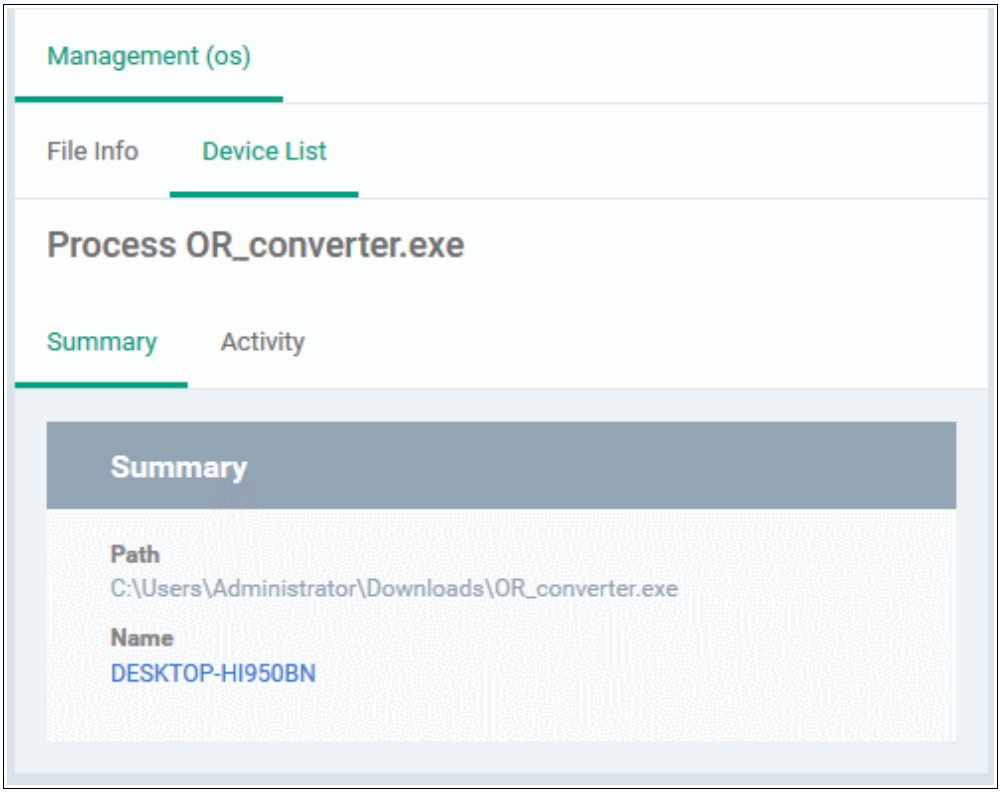
Viewing Process Activities of the File

Note: In order for ITSM to fetch the data on activities of the files from an endpoint and display them, VirusScope should have been enabled in the profile in effect on the endpoint. Refer to the explanation of **Configuring VirusScope Settings** in the section **Creating Windows Profiles** for more details.

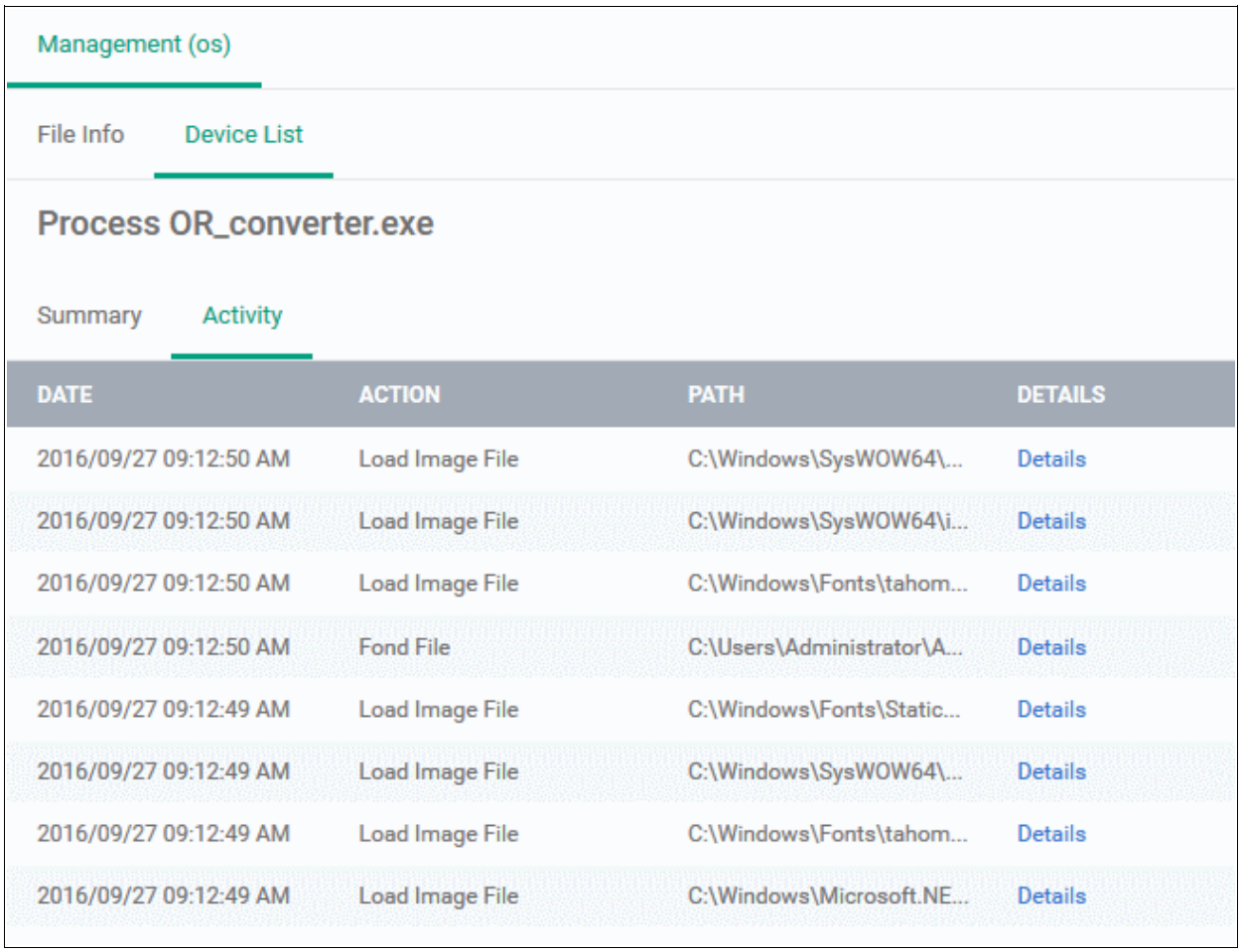
- To view the activities of the file at an endpoint, click the 'View Activity' link in the 'Activity' column

The 'Process Activity' interface will open. It has two tabs.

- **Summary** - Displays the details of the process(es) executed by the contained file at the endpoint.



- **Activity** - Displays a chronological order of process activities with details of files modified by the process.



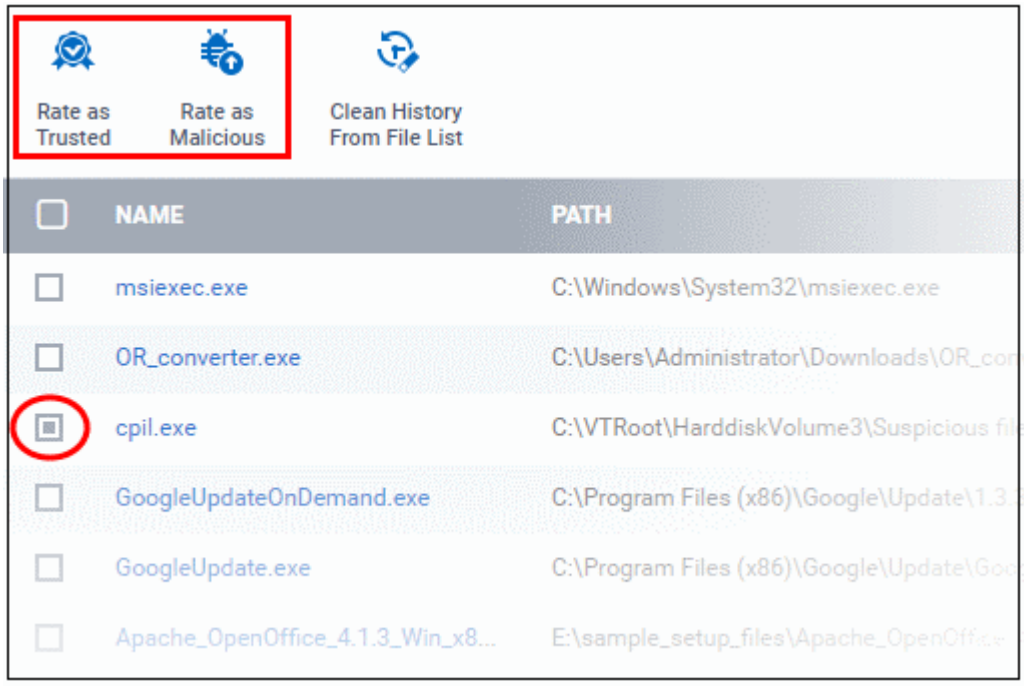
The 'Activity' - Table of Column Descriptions	
Column Heading	**Description**
Date	Indicates the date and time of process execution
Action	Indicates the action executed by the process on the target file
Name	Indicates the target file affected by the process
Details	Contains link to view the details of the action

- To view the details of an activity, click the 'Details' link under the 'Details' column.

Rate files as trusted / malicious

Administrators can rate unrecognized, contained files as trusted or malicious as required. Please make sure before marking a file as trusted. The changed file rating will be sent to the endpoints.

- To rate a file, select it and click 'Rate as Trusted' or 'Rate as Malicious' at the top.

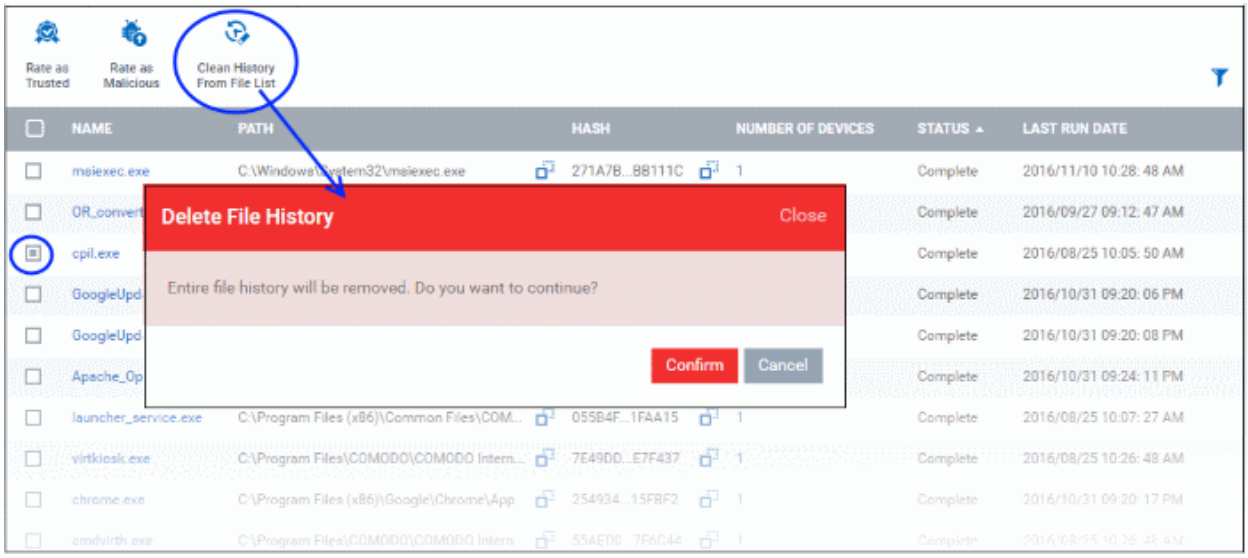


The changed file rating will be propagated to the endpoints.

Removing files from the list

The administrator can remove unwanted items from the 'Containment' interface.

- To delete an item, select it from the list and click 'Clean History From File List' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Containment' interface.

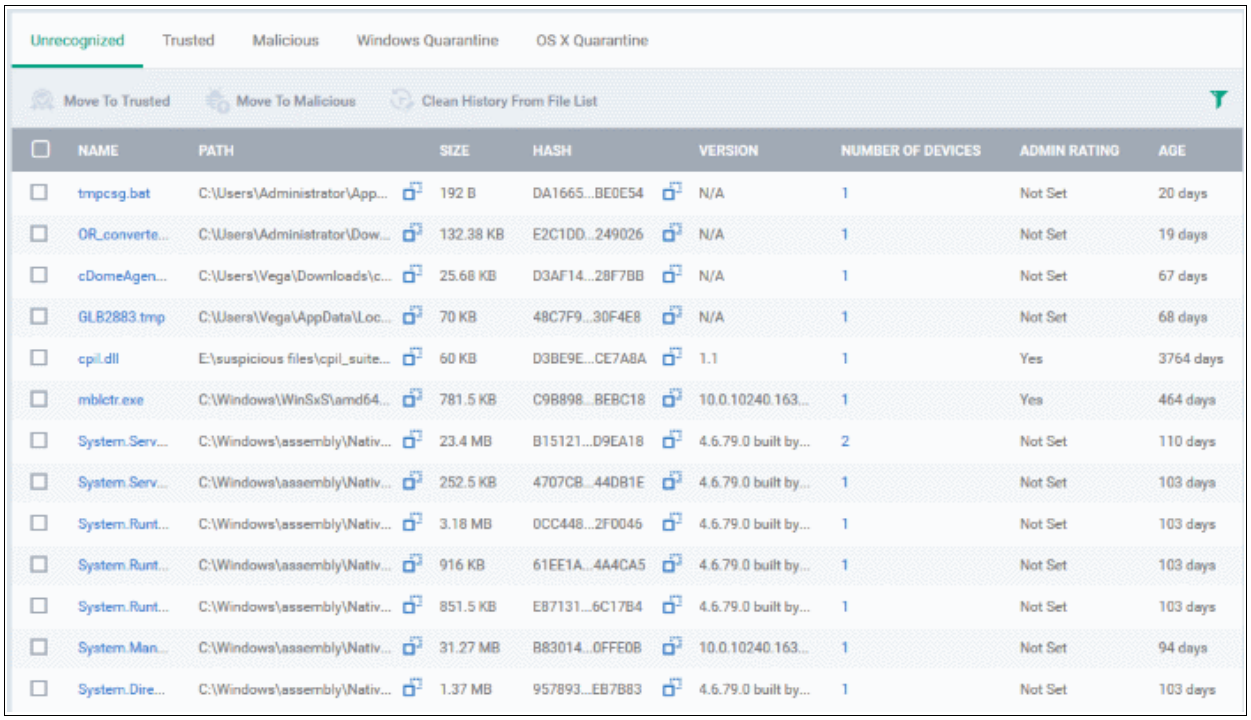
9.2. Viewing Applications Installed on Windows Devices

The CCS installation on each enrolled Windows device will monitor all file system activities. Every new executable is first scanned against the Comodo whitelist and blacklists and rated as 'Unrecognized', 'Trusted' or 'Malicious' (as configured in 'File Rating settings' in the configuration profile active at the endpoint). Refer to the explanation of File Rating settings in section Creating a Windows Profile for more details.

The 'Application Control' interface allows admins to view items that are rated as 'Unrecognized', 'Trusted' or 'Malicious' by CCS on the endpoints. Administrators can analyze the trustworthiness of the items and move files to

lists depending on their nature. Files added to the 'Trusted Files' list are allowed to run. Files added to the 'Malicious Files' list are quarantined and not allowed to run. 'Unknown' files are run in the container. The rating set by the administrator is propagated to all the enrolled endpoints.

- To access the 'File List' interface, click 'Security Sub-Systems' from the left and choose 'Application Control' from the options.



The interface contains five tabs:

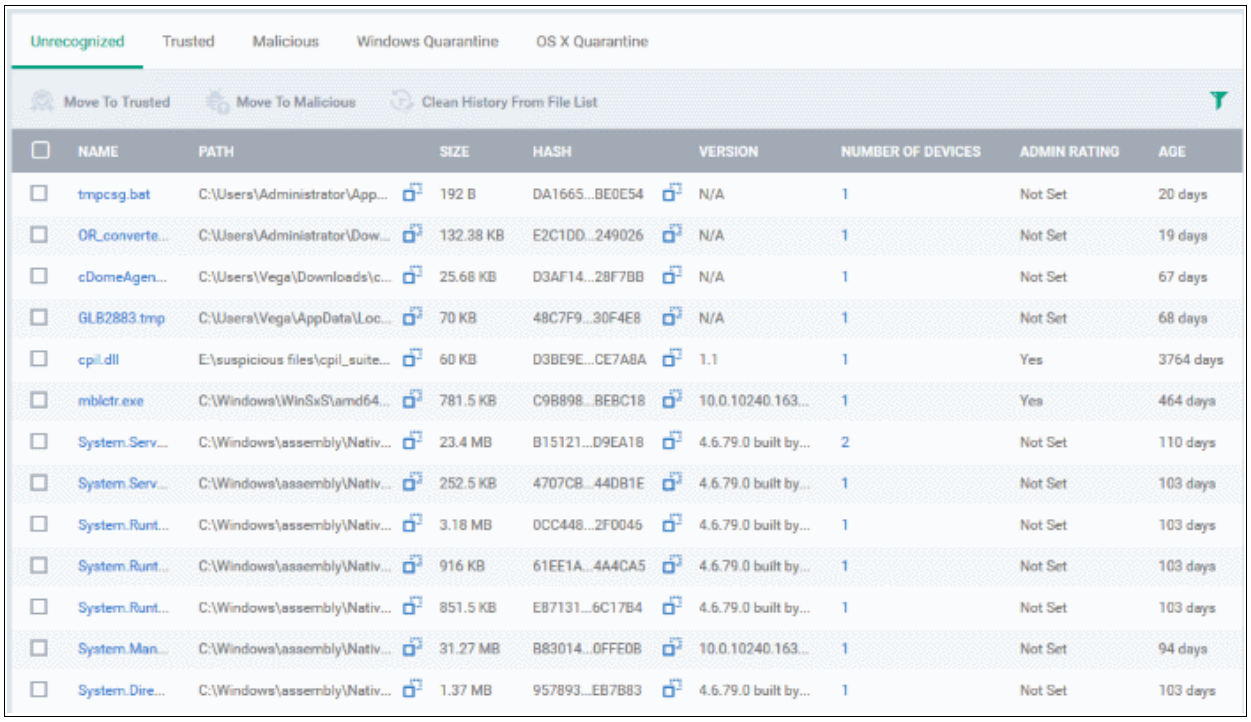
- **Unrecognized** - Displays the list of files reported as 'Unrecognized' by the CCS installations at the Windows endpoints. Administrators can move items to the 'Trusted Files' list or 'Malicious Files' list should they wish. Refer to the section **Viewing and Managing Unrecognized Files** for more details.
- **Trusted** - Displays the global 'Trusted Files' list .Administrators can move items to this list from 'Unrecognized Files' or 'Malicious Files' lists. Refer to the section **Viewing and Managing Trusted Files** fro more details.
- **Malicious** - Displays the global 'Malicious Files' list . Administrators can manually add files or move items to this list from Unrecognized Files or Trusted Files lists. False positives can also be moved to 'Unrecognized Files' or 'Trusted Files' lists. Refer to the section **Viewing and Managing Malicious Files**
- **Windows Quarantine** - Displays a list of files on Windows devices that were moved to quarantine (those file which were identified as potential threats). Administrators can delete the files from the device, restore files to their original locations, rate them as unrecognized or rate them as trusted. Refer to the section **Viewing and Managing Quarantined Items** for more details.
- **OS X Quarantine** - Displays a list of files on Mac OS devices that hat were moved to quarantine (those files which were identified as potential threats). Administrators can delete files from the device, restore files to their original locations, rate them as unrecognized or rate them as trusted. Refer to the section **Viewing and Managing Quarantined Items on Mac OS Devices** for more details.

9.2.1. Viewing and Managing Unrecognized Files

The 'Unrecognized' interface displays a consolidated list of all unrecognized files reported by Comodo Client Security software on all managed Windows endpoints. The list also contains files that were marked as 'Unrecognized' by an administrator via the 'Trusted', 'Malicious', 'Windows Quarantine' and 'OS X Quarantine' interfaces.

To open the Unrecognized Files interface

- Click 'Secure Sub-systems' on the left and choose 'Application Control' from the options
- Click the 'Unrecognized' tab at the top.

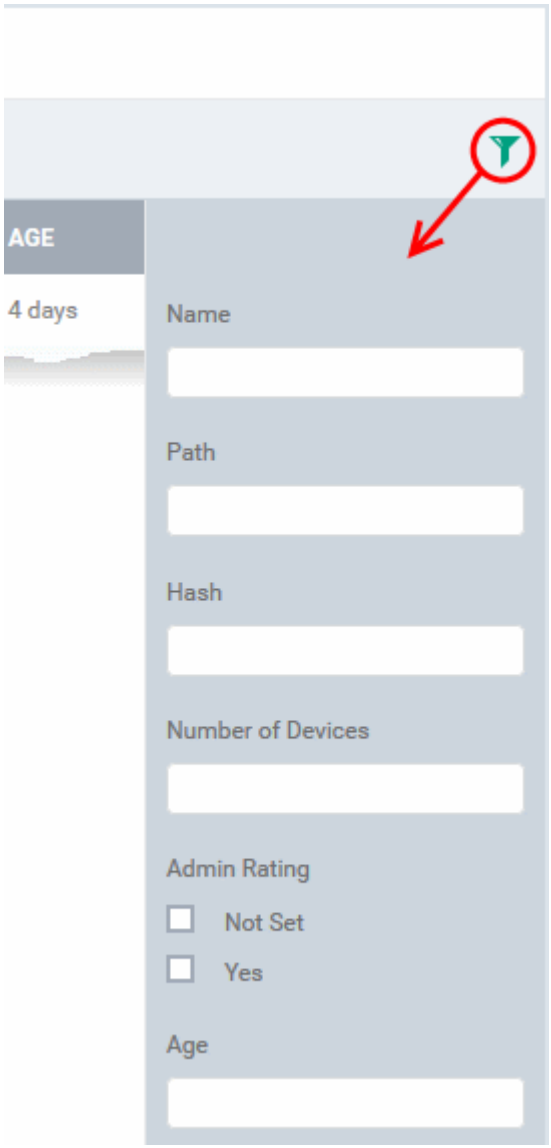


The 'Unrecognized' Files List - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the file name of the unrecognized item.
Path	The installation location of the file at the endpoint. • Clicking the icon copies the path to the clipboard.
Size	The size of the file.
Hash	Displays the SHA1 hash value of the file. • Clicking the icon copies the hash value to the clipboard.
Version	Displays the version number of the executable file.
Number of Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device List' interface with a list of endpoints containing the item. You can also view the activities of the item from here. For more details, refer to the description under Device List Screen below.
Admin Rating	Indicates whether the file was manually moved to the 'Unrecognized Files' list by the administrator. 'Not Set' indicates the rating was not changed by the administrator and 'Yes' means the file rating was changed.
Age	The number of days since the item was created on the first endpoint on which it was discovered or re-rated by the administrators.

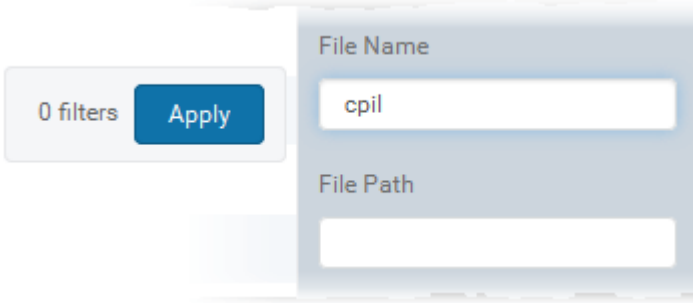
Sorting, Search and Filter Options

- Clicking on 'Name', 'Path', 'Number of Devices' and/or 'Admin Rating' column header sorts the items based on alphabetical order of entries in that column.

- Clicking the funnel button at the right end opens the filter options.



- To filter items or search for a specific file, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Unrecognized Files

The 'Unrecognized Files' interface allow you to:

- View the details of files in the list
- Move selected files to global 'Trusted Files' or 'Malicious Files' list
- Remove files from the list

View the details of files in the list

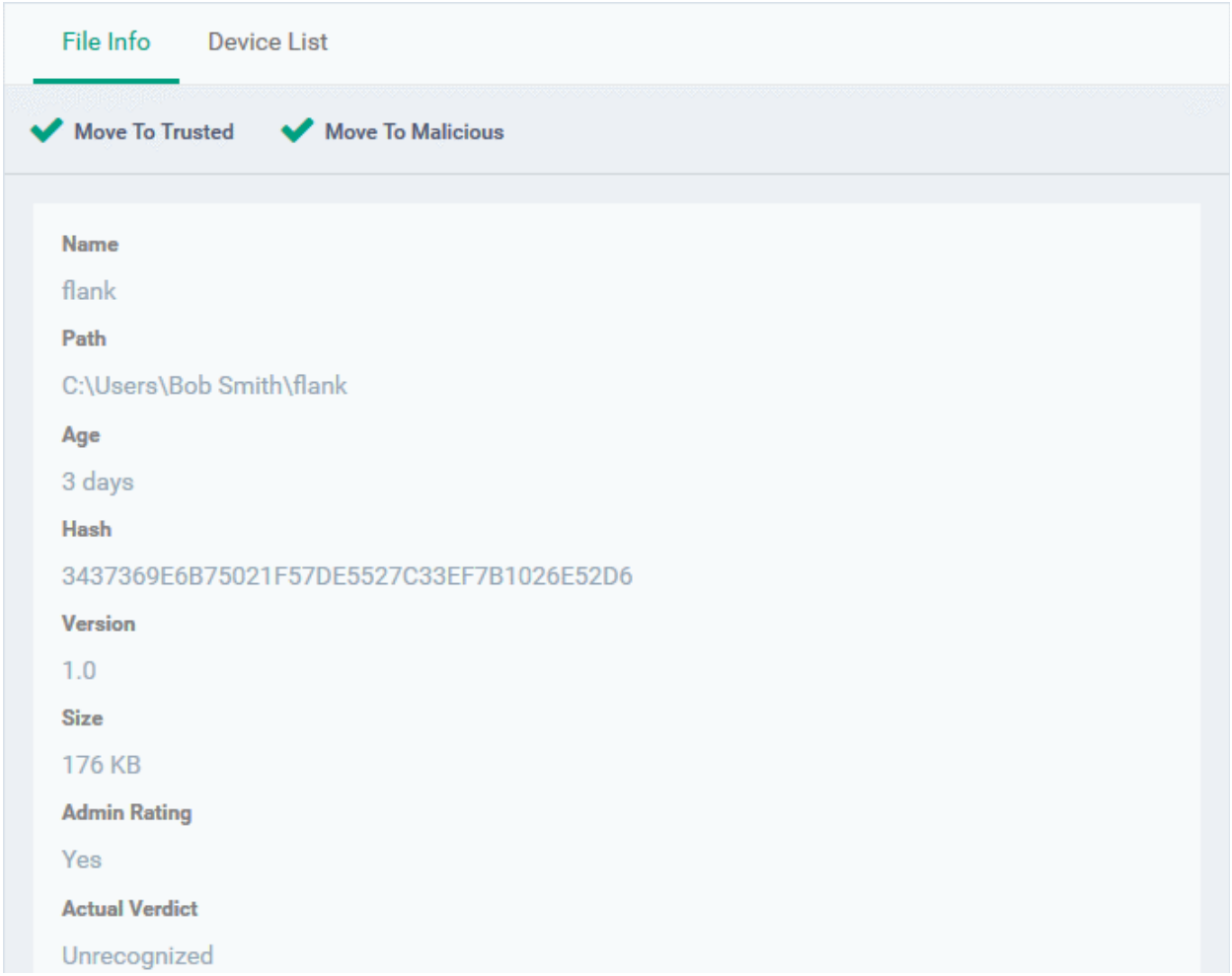
- Click a file name to view file details, the endpoints on which it was identified and its activities.

The file information interface will be displayed. The interface contains two tabs:

- File Info - Displays general information about the selected item.
- Device List - Displays a list of endpoints upon which the item was found and its activities on each endpoint.

File Information Screen

The 'File Info' screen is displayed when you click the name of an item in the 'Unrecognized Files' interface. To return to the 'File Info' screen from 'Device List' screen, click the 'File Info' tab at the top:



The screen shows summary file details like file name, installation path, version, size, hash value, age, if it was manually moved to Unrecognized files list and the file rating from Comodo Client software.

- If the item is found to be trustworthy you can move it to 'Trusted Files' by clicking 'Move to Trusted'
- If the item is found to be malicious you can move it to the malicious files list (and block the item on all enrolled endpoints) by clicking 'Move to Malicious'

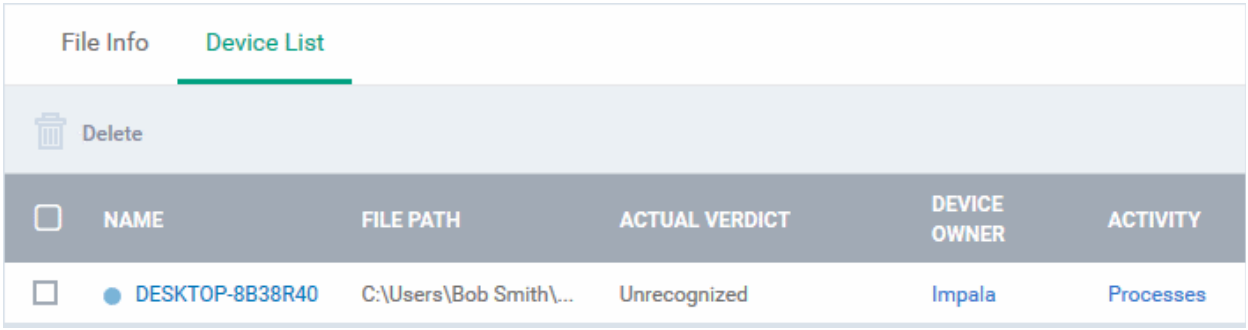
The changed file verdict will be sent to the endpoints.

Device List Screen

The 'Device List' screen can be opened by clicking the 'Device List' tab in the 'File Info' interface.

Tip: The 'Device List' Screen can also be opened by clicking on the number displayed in the 'Number of Devices' column in the 'Unrecognized Files' list table.

The 'Device List' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. Administrators can view the processes executed by the file at each endpoint with the details on data handled by each process.



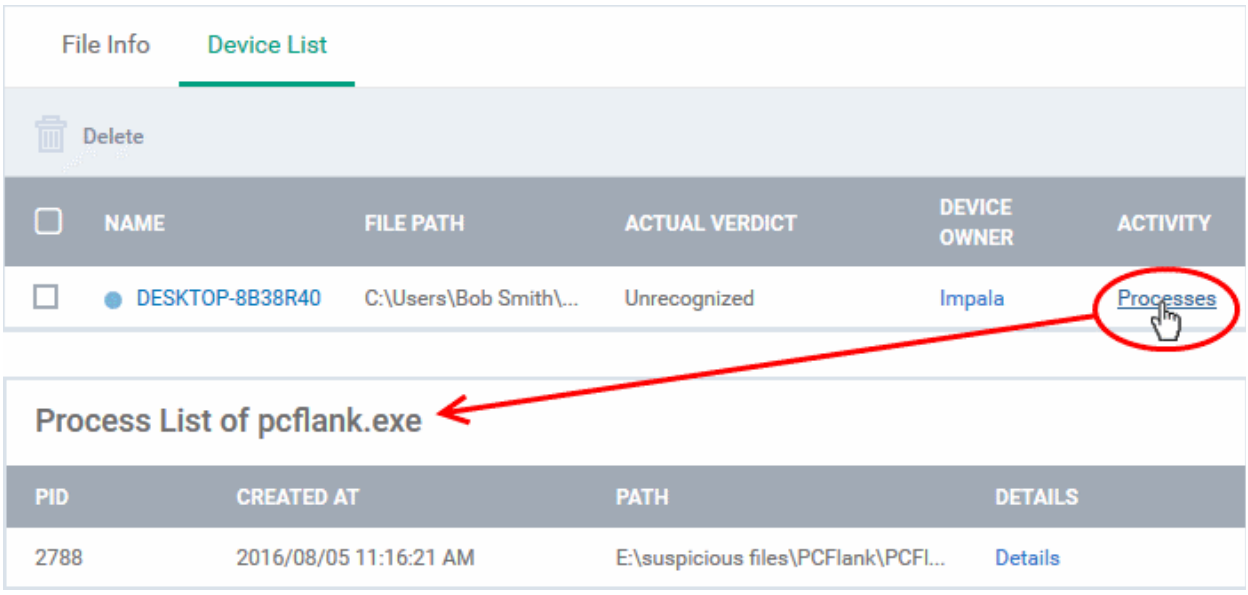
- If you want to delete the file from selected devices, select the devices from the list and click 'Delete'.

Viewing Process Activities of the File

Note: In order to fetch file activity data from an endpoint, VirusScope should have been enabled in the profile in effect on the endpoint. Refer to the explanation of **Configuring Viruscope Settings** in the section **Creating a Windows Profile** for more details.

To view the activities of the file on an endpoint

- Click the number link in the 'Number of Devices' column
- Click the 'Processes' link in the 'Activity' column:

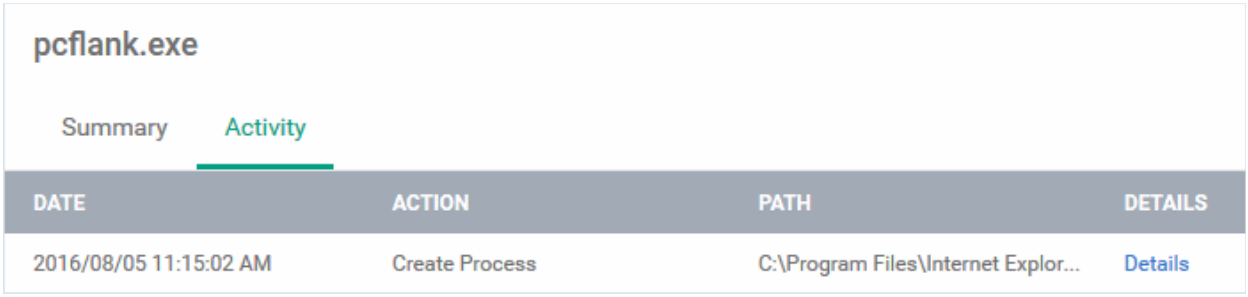


The list of processes executed by the file on the selected endpoint will be displayed.

- Click 'Details' to view detailed information about the activities of a selected process

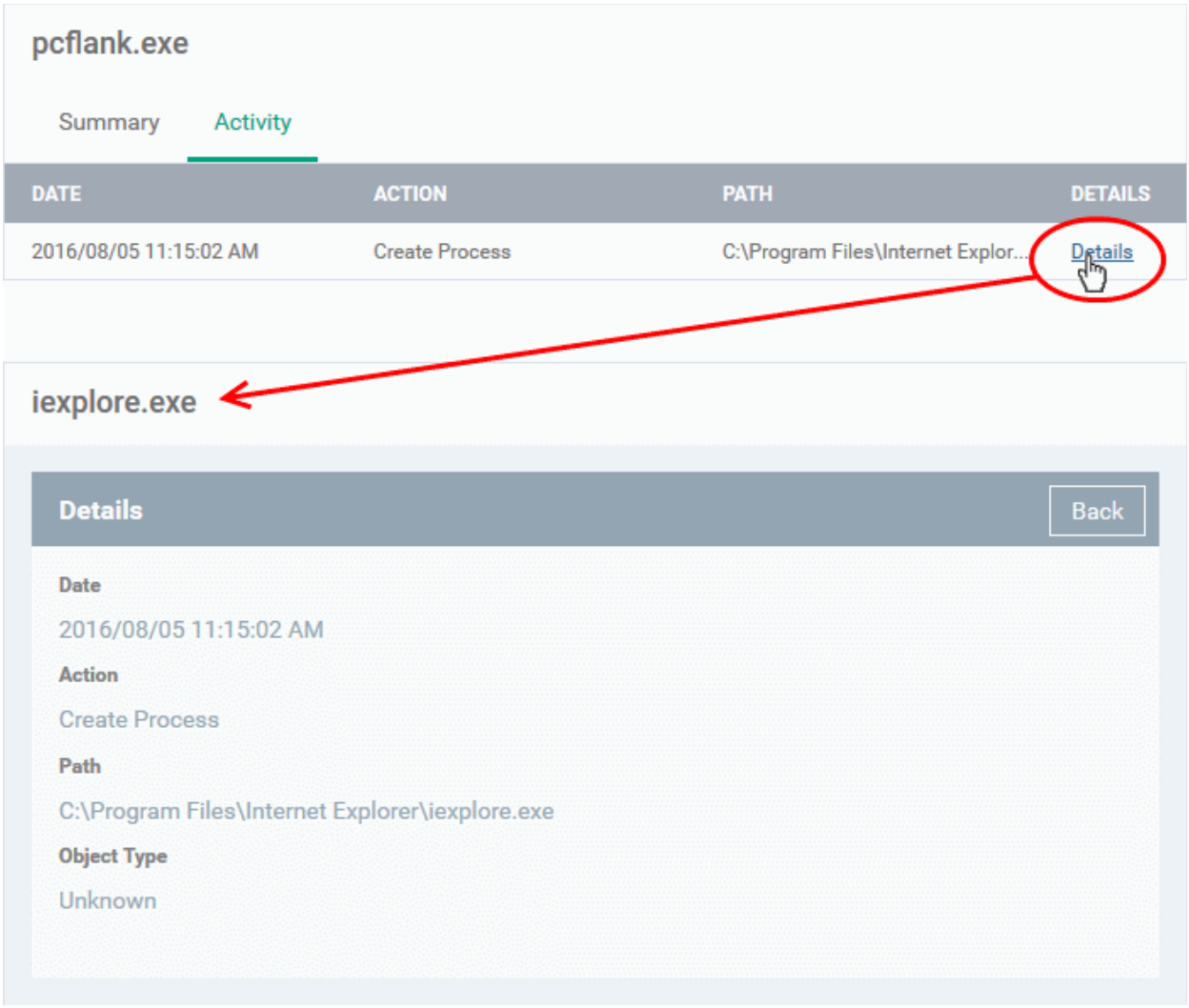
The 'Process Activity' interface will open. It has two tabs.

- **Summary** - Displays the name of the device and the installation path of the executable
- **Activity** - Displays a chronological list of activities by the selected process, including details of files modified by the process.



The 'Activity' - Table of Column Descriptions	
Column Heading	**Description**
Date	Indicates the date and time of process execution
Action	Indicates the action executed by the process on the target file
Path	Indicates the path of the target file
Details	Contains a link to view details of the action

- To view the details of an activity, click the 'Details' link under the 'Details' column.



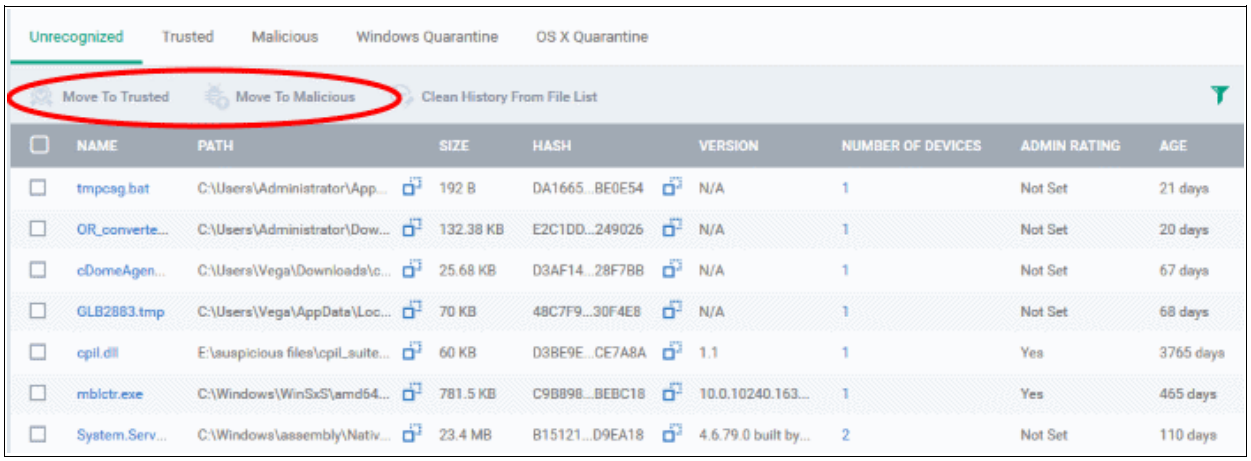
Move Selected Files to 'Trusted Files' or 'Malicious Files'

If an unrecognized item is identified as trustworthy by the administrator, they can add the file to the global 'Trusted Files' list. Files added to trusted file list will be skipped during all types of antivirus scans until the next AV database update.

Tip: If a file is to be excluded from all types of AV scans in future, the administrator can add the file to the Exclusions list in the configuration profile applied to the endpoint. Refer to the explanation of adding Exclusions to Antivirus Component in the section Creating a Windows Profile for more details.

If an unrecognized item is identified as malware by the administrator, the file can be added to the global 'Malicious Files' list and the new file rating will be sent to the endpoints. Files added to malicious files list will not be allowed to run at the endpoints.

- To move item(s) to the 'Trusted Files' list, select the items and click 'Move to Trusted' from the options at the top.



- To move item(s) to the 'Malicious Files' list, select the item, click 'Move to Malicious' from the options at the top.

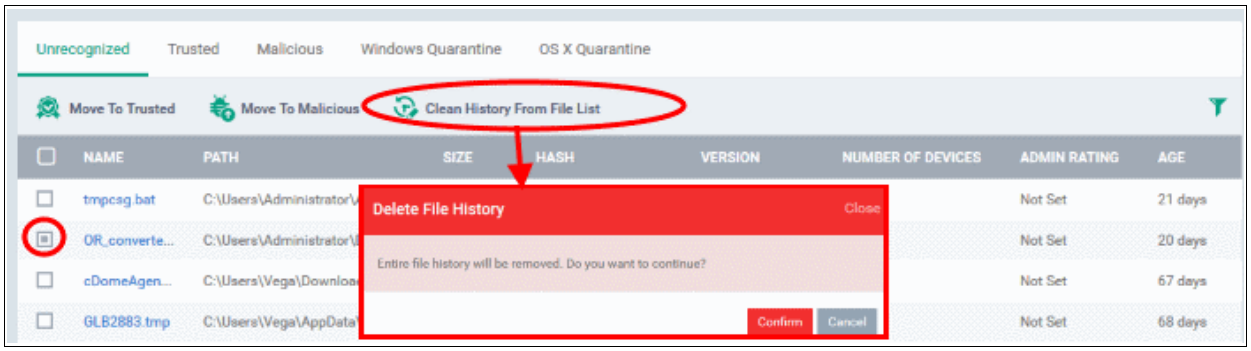
The changed file verdict will be sent to the endpoints.

Tip: You can filter or search for specific files using the filter options that appear on clicking the funnel icon at the top right.

Remove files from the list

If an unrecognized item is identified as a false-positive, the administrator can remove it from the 'Unrecognized Files' list.

- To remove or delete an item, select the item from the list and click 'Clean History For This File' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Unrecognized Files' list.

The file will only be removed from the Unrecognized Files list. If the same file is identified from the same of a different endpoint, it will be again be added to the list unless the file is moved to 'Trusted Files' list or 'Malicious Files' list.

9.2.2. Viewing and Managing Trusted Files

Files included in the 'Trusted Files' list are automatically given CCS trusted status. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, the Comodo Client security (CCS) software on an endpoint will check the file against our master whitelist and blacklists. It will award it trusted status if:

- The application is from a vendor included in the Trusted Software Vendors list;
- The application is included in the extensive and constantly updated Comodo safelist.

- Administrator rating - The Administrator moves files identified as trustworthy from the 'Unrecognized Files' list or 'Malicious Files' list.
- User Rating - Users can assign 'Trusted' status to files at the local CCS installation in two ways:
  - If an executable is unknown to the 'Advanced Protection' safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, the user could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted'.
  - The user can assign 'Trusted' rating to any desired file from the 'File List' interface.

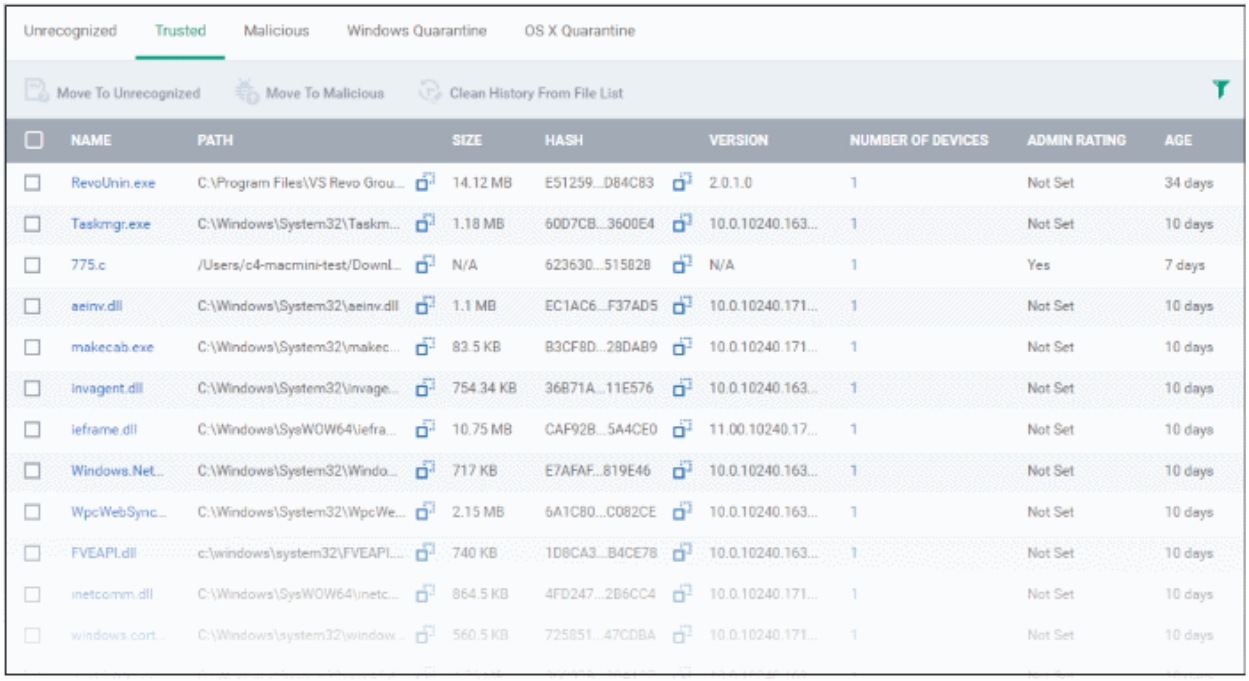
For the files assigned with 'Trusted' status by the user, CCS generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. In this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same. This is particularly useful for developers who are creating new applications that, by nature, are unknown to Comodo safe list.

The 'Trusted' tab under 'File List' interface displays a consolidated list of Trusted files reported by CCS on endpoints. The list also contains files that were marked as 'Trusted' by administrators from the 'Unrecognized', 'Malicious', 'Windows Quarantine' and 'OS X Quarantine' interfaces.

Note - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, rate unknown files, submit files for analysis, monitor Windows events and provide alerts 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**.

To open the Trusted Files interface

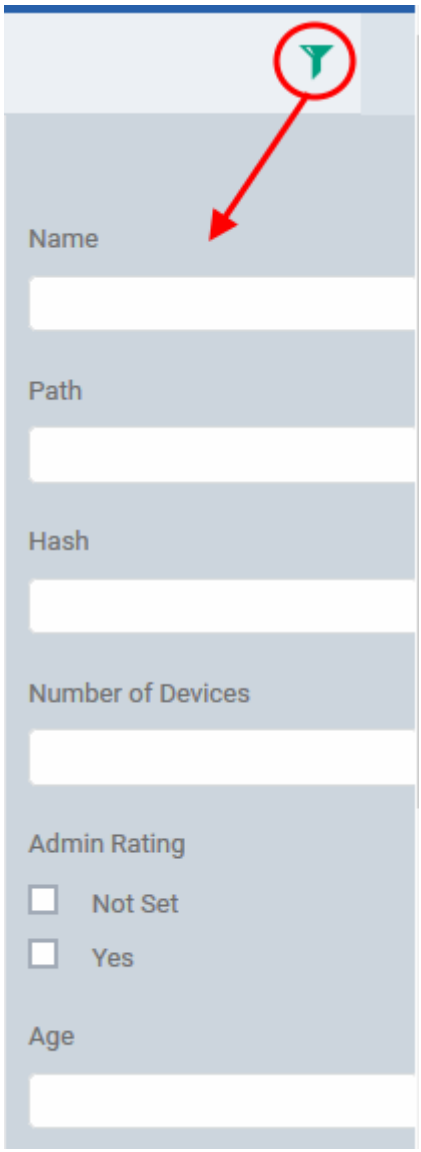
- Click 'Secure Sub -Systems' on the left and choose 'Application control' from the options.
- Click the 'Trusted' tab at the top.



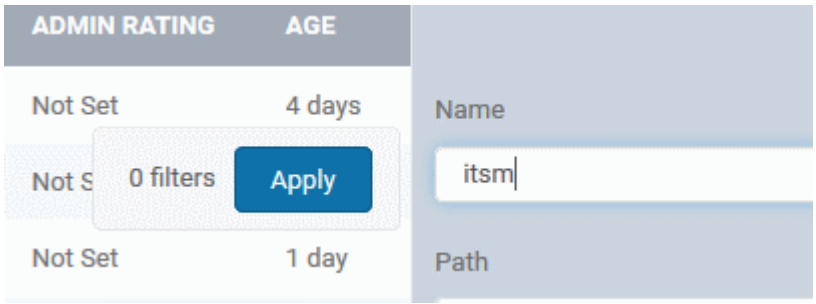
The 'Trusted ' List - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the file name of the unrecognized item.
Path	The installation location of the file at the endpoint. • Clicking the icon copies the path to the clipboard.
Size	The size of the file.
Hash	Displays the hash value of the file derived using SHA1 hash algorithm. • Clicking the icon copies the hash value to the clipboard.
Version	Displays the version number of the executable file.
Number of Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device List' interface with a list of endpoints containing the item and allows the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device List Screen below.
Admin Rating	Indicates whether the file was manually moved to the Trusted files list by the administrator.
Age	The length of time since the item was created on the first endpoint on which it was discovered

Sorting, Search and Filter Options

- Clicking on the 'Name', 'Path', 'Number of Devices' or 'Admin Rating' column headers will sort the table in alphabetical or numerical order according to the items in the selected column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific file, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Trusted Files

The 'Trusted' Files interface allows you to:

- View the details of files in the list
- Move selected files to 'Unrecognized Files' or 'Malicious Files' list
- Removing files from the list

View the details of files in the list

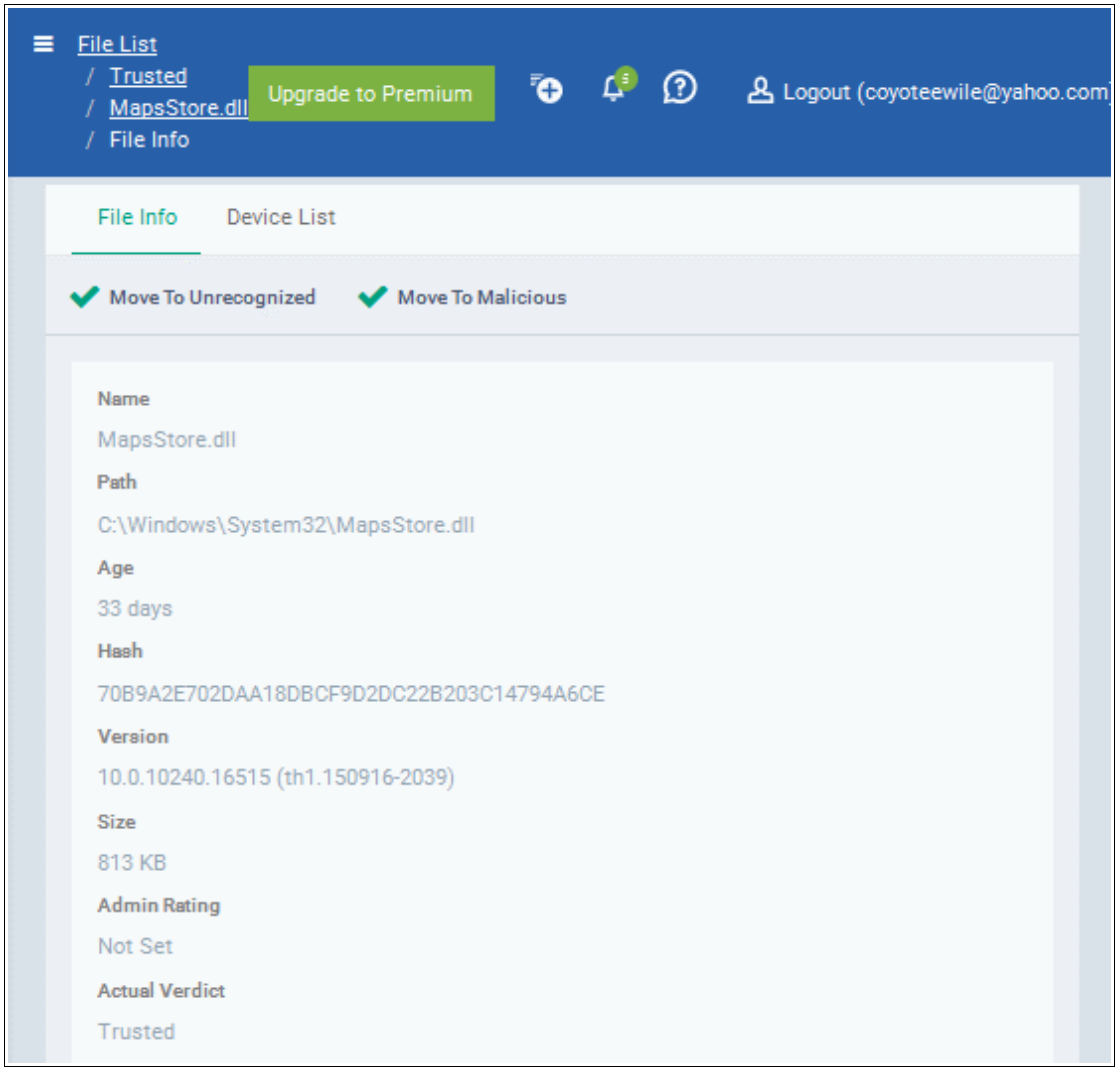
- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- File Info - Displays the general information on the selected item.
- Device List - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Trusted' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.



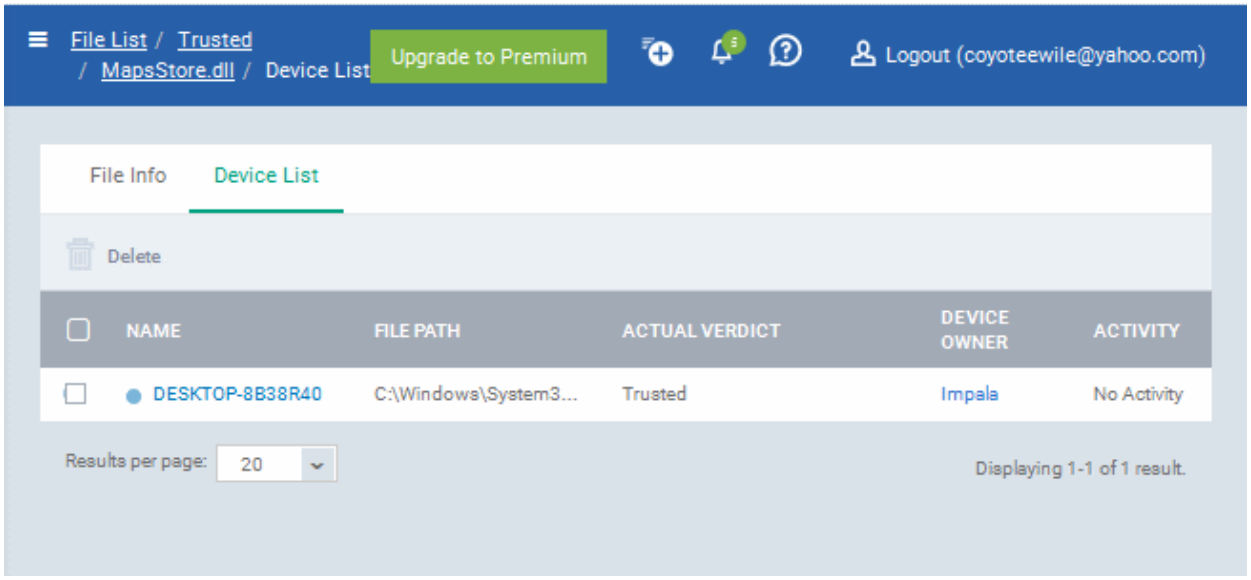
The 'File Info' screen displays a summary of the file details like (file)name, (file installation)path, version, size, hash(value), age, whether manually moved to Trusted files list and the actual file rating result by the local CCS installation at the endpoint.

- If the item is found to be suspicious, you can move it to the Unrecognized Files list by clicking 'Move to Unrecognized' from the options at the top
- If the item is found to be malicious you can move it to malicious files list and block it at all the enrolled endpoints by clicking 'Move to Malicious' from the options at the top

Devices List Screen

The 'Device List' screen can be opened by clicking the 'Device List' tab in the 'File Info' interface.

The 'Device List' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.

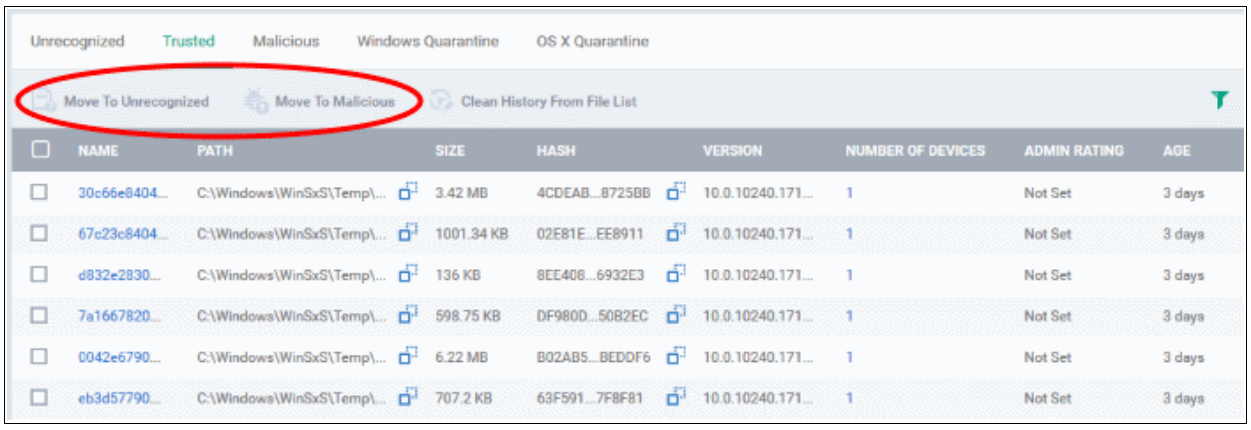


The Device interface allows the administrator to view the activities of the file at the selected endpoint. Refer to the explanation of Viewing Process Activities of the File in the previous section for more explanation.

Moving Selected Files to 'Unrecognized Files' or 'Malicious Files' list

Items that are added to the 'Trusted Files' list by mistake can be moved to 'Unrecognized Files' list or global 'Malicious Files' list.

- To move item(s) to the 'Unrecognized Files' list, select the items and click 'Move to Unrecognized' from the options at the top.



- To move item(s) to the 'Malicious Files' list, select the item, click 'Move to Malicious' from the options at the top.

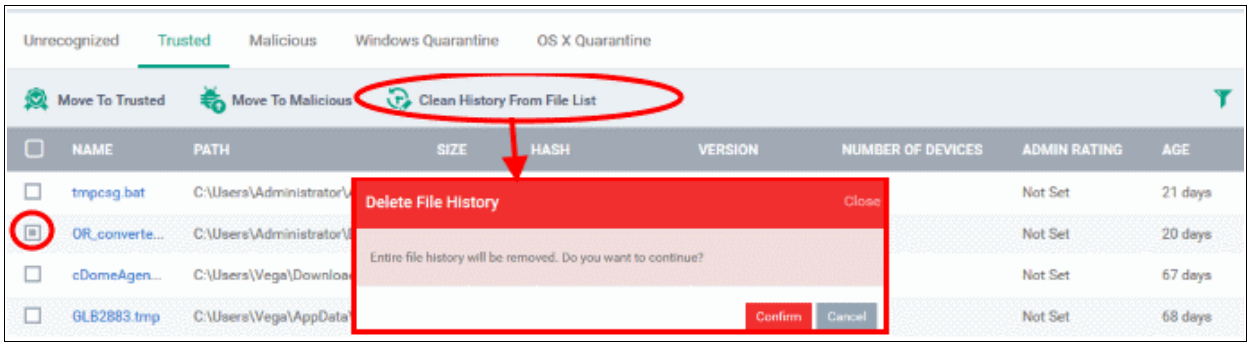
The changed file verdict will be sent to the endpoints.

Tip: You can filter or search for specific files using the filter options that appear on clicking the funnel icon at the top right.

Removing files from the list

If an item in 'Trusted Files' list is identified as not trustworthy, the administrator can remove it from the 'Trusted Files' list.

- To remove or delete an item, select the item from the list and click 'Clean History From File List' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Trusted Files' list.

The file will only be removed from the 'Trusted' Files list and not from the endpoints.

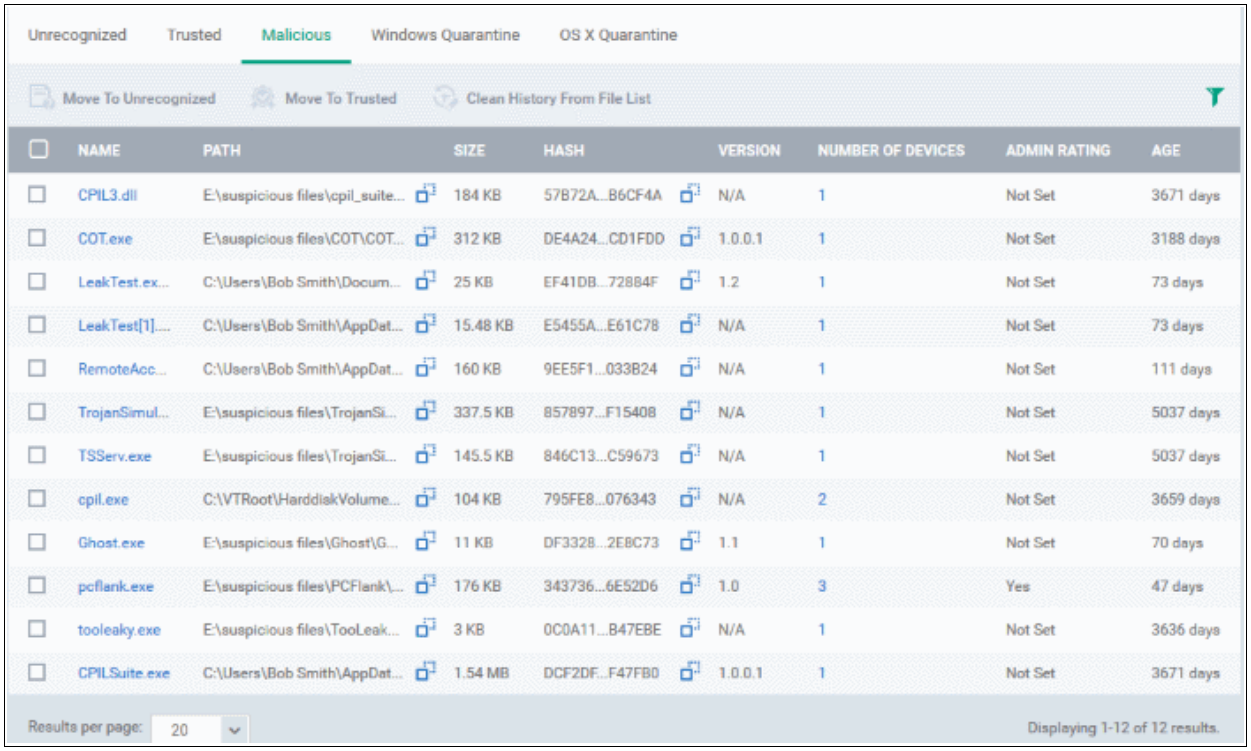
9.2.3. Viewing and Managing Malicious Files

Files that are identified as malicious from the File Look up Service (FLS) by the local CCS installations will be given 'Malicious' rating and will not be allowed to run by default.

The 'Malicious' tab under 'Application Control' displays a consolidated list of all malicious files reported by Comodo Client security software on all managed endpoints. The list also contains files that were marked as 'Malicious' by an administrator via the 'Trusted', 'Unrecognized', 'Windows Quarantine' and 'OS X Quarantine' interfaces.

To open the Malicious Files List interface

- Click 'Secure Sub-System' on the left and choose 'Application Control' from the options
- Click the 'Malicious' tab at the top.

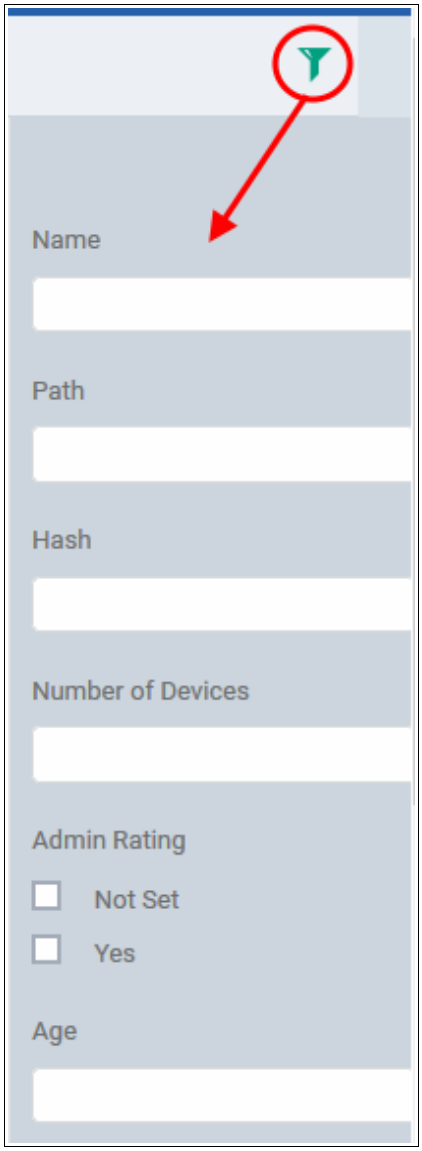


The 'Malicious ' List - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the file name of the 'Unrecognized' item.
Path	The installation location of the file at the endpoint. • Clicking the icon copies the path to the clipboard.
Size	The size of the file.
Hash	Displays the hash value of the file derived using SHA1 hash algorithm. • Clicking the icon copies the hash value to the clipboard.
Version	Displays the version number of the executable file.
Number of Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device List' interface with a list of endpoints containing item and allows the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device List Screen below.
Admin Rating	Indicates whether the file was manually moved to the Malicious file list by an administrator.
Age	The number of days since the item was created on the first endpoint on which it was discovered. This can also mean the number of days since it was re-rated by an administrator.

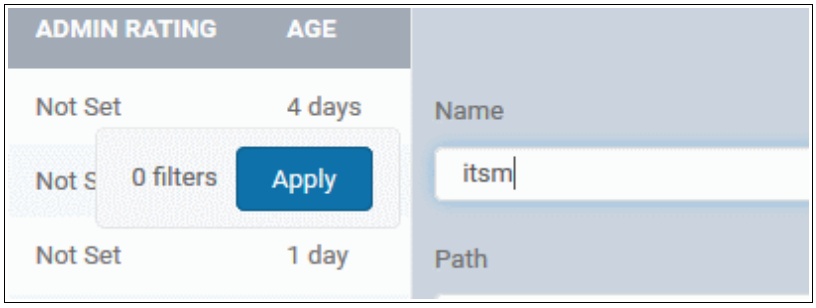
Sorting, Search and Filter Options

- Clicking on Name, Path, Number of Devices and/or Admin Rating column header sorts the items based on alphabetical order of entries in that column.

- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific file, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



You can use any combination of filters at-a-time to search for specific apps.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Malicious Items

The Malicious Files interface allow you to:

- View the details of files in the list
- Move selected files to 'Unrecognized Files' or 'Trusted Files' list
- Removing files from the list

View the details of files in the list

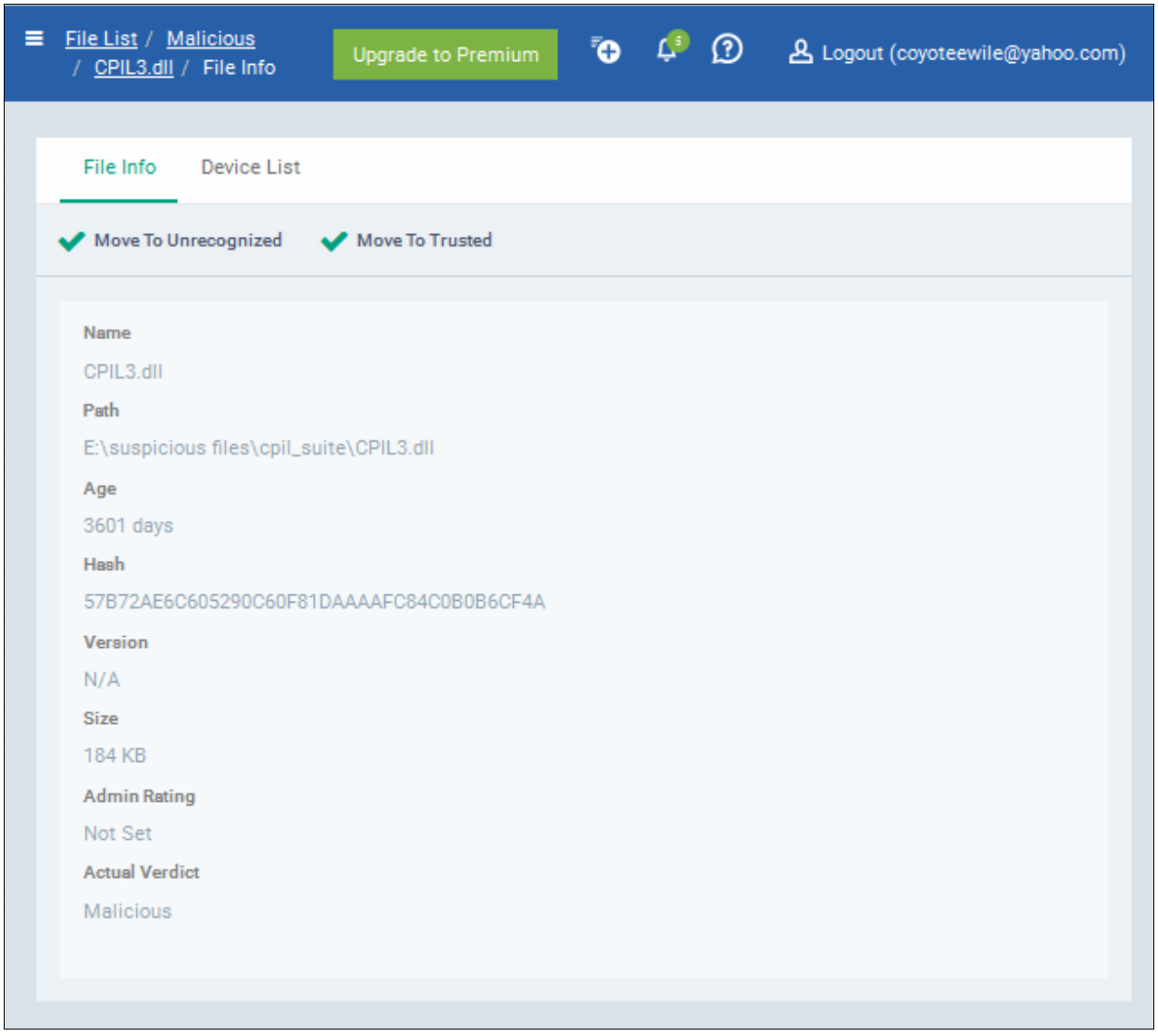
- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- File Info - Displays the general information on the selected item.
- Device List - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Malicious' interface. To return to the 'File Info' screen from 'Device List' screen, click the 'File Info' tab from the top.



The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, age, whether manually moved to Trusted files list and the actual file rating result by the local CCS installation at the endpoint.

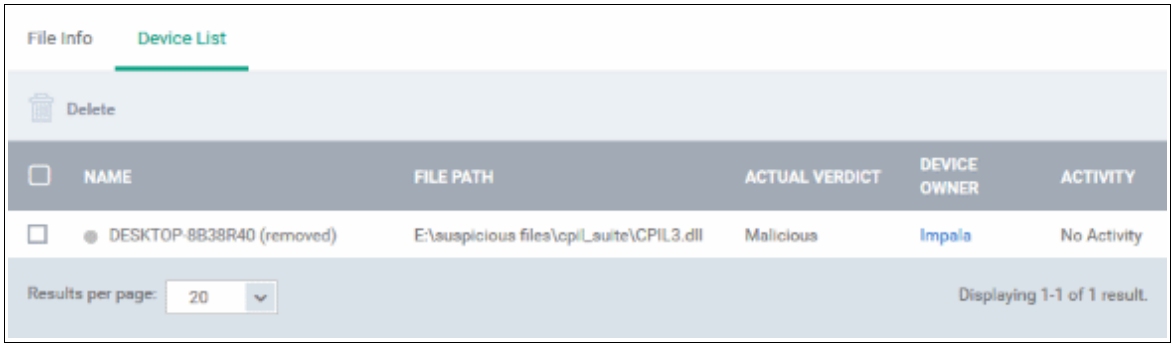
- If the item is found to be suspicious, you can move it to the Unrecognized Files list by clicking 'Move to Unrecognized' from the options at the top
- If the item is found to be trustworthy, you can move it to Trusted files list by clicking 'Move to Trusted' from the options at the top

The changed file verdict will be sent to the endpoints.

Device List Screen

The 'Device List' screen can be opened by clicking the 'Device List' tab in the 'File Info' interface.

The 'Device List' screen displays a list of endpoints on which the item was identified and its activities at each endpoint. Administrators can view the processes executed by the file on each endpoint and the details of data handled by each process.

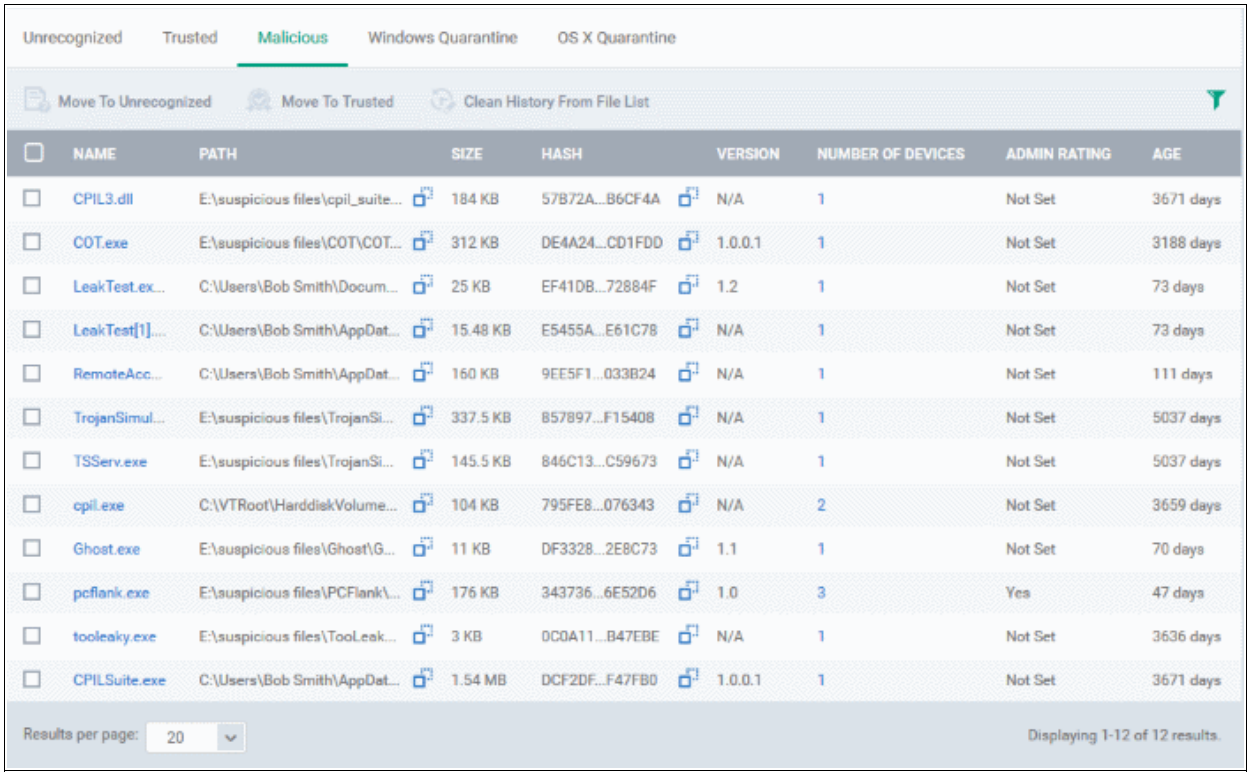


The Device interface allows administrators to view the activities of the file at the selected endpoint. Refer to the explanation of Viewing Process Activities of the File in the previous section for more explanation.

Moving Selected Files to 'Unrecognized Files' or 'Trusted Files' list

Items that are added to the 'Malicious Files' list by mistake or found trustworthy can be moved to 'Unrecognized Files' list or global 'Trusted Files' list.

- To move item(s) to the 'Unrecognized Files' list, select the items and click 'Move to Unrecognized' from the options at the top.



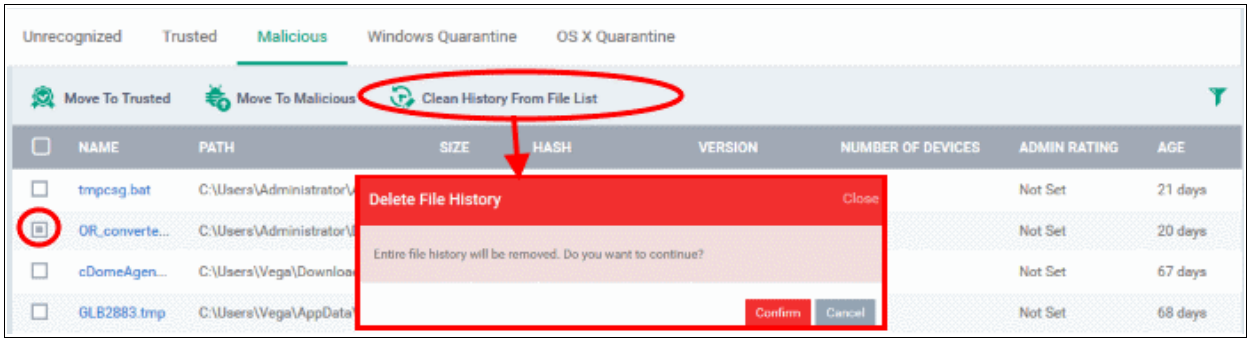
- To move item(s) to the 'Trusted Files' list, select the item, click 'Move to Trusted' from the options at the top.

The changed file verdict will be sent to the endpoints.

Tip: You can filter or search for specific files using the filter options that appear on clicking the funnel icon at the top right.

Removing files from the list

- To remove or delete an item, select the item from the list and click 'Clean History From File List' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item.

The file will only be removed from the Malicious Files list and not from the endpoints.

9.2.4. Viewing and Managing Quarantined Items

Threats will be placed in quarantine by Comodo Client Security (CCS) on managed endpoints if:

- 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action in the profile active on the device. This setting can be found in the 'Realtime Scan Settings' section of the profile's antivirus

component.

- 'Show antivirus alerts' is enabled in 'Realtime Scan Settings' and the end user chose to quarantine the threat at the alert.
- An administrator moved a threat to quarantine from the 'Current Malware List' interface
- An end-user moved a file to quarantine on the endpoint

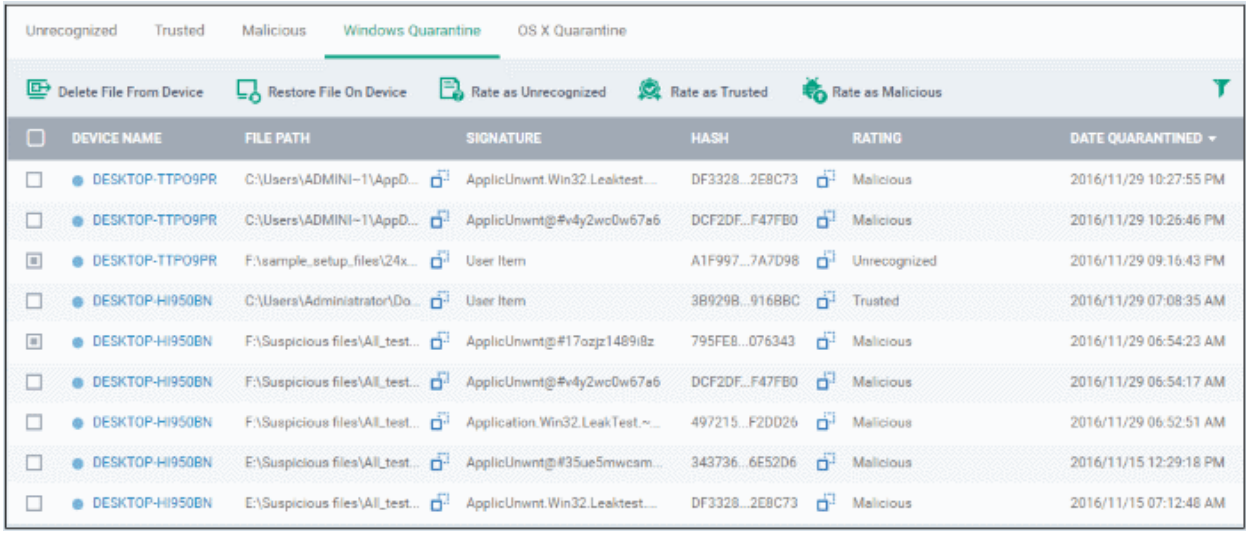
Items moved to quarantine are saved in an encrypted format and not allowed to run at the endpoint.

Refer to the explanation of **Realtime Scan settings** in the section **Antivirus Settings** under **Creating Windows Profile** and the section **Viewing and Managing Identified Malware** for more details.

The 'Windows Quarantine' interface lists all items quarantined by CCS on all enrolled endpoints. Administrators can analyze the trustworthiness of the items,rate them as unrecognized or trusted, delete them permanently or restore them to their original location from this interface.

To open the Quarantine Files interface

- Click 'Secure Sub-system' on the left and choose 'Application Control' from the options
- Click the 'Windows Quarantine' tab

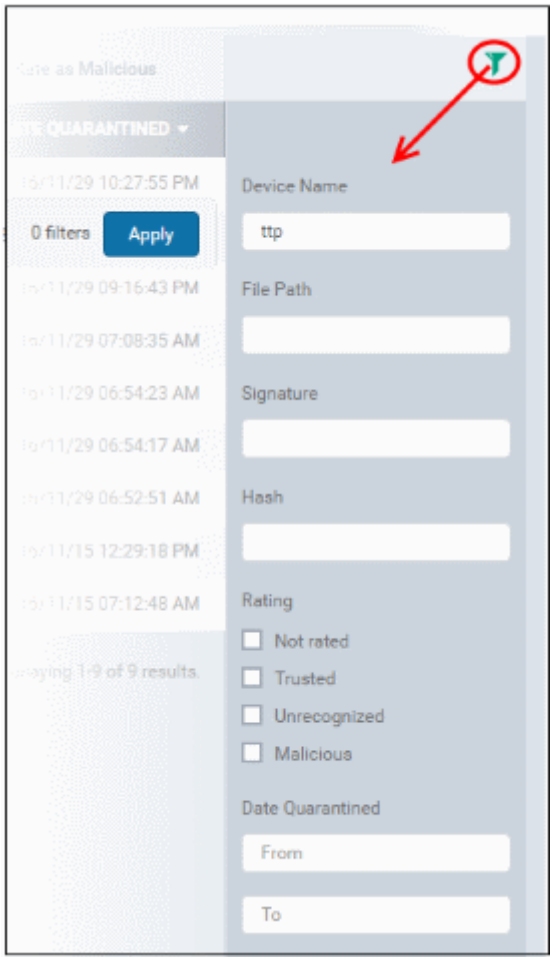


The 'Windows Quarantine' List - Table of Column Descriptions	
Column Heading	**Description**
Device Name	The name assigned to the device by the user. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to manage the device and to apply configuration profiles. Refer to the section **Managing Windows Devices** for more details.
File Path	The installation path of the infected application. • Clicking the icon copies the path to the clipboard.
Signature	The name of the identified malware. 'User Item' indicates the file was moved to quarantine manually by the user on the endpoint.
Hash	Displays the SHA1 hash value of the quarantined file • Clicking the icon copies the hash value to the clipboard.
Rating	Indicates the file's trust level as rated by CCS.
Date Quarantined	Indicates the precise date and time at which the malware was quarantined on the

	device.

Sorting, Search and Filter Options

- Clicking on any of the column headers sorts the table in ascending or descending order of the entries in the selected column.
- Clicking the funnel  on the top right opens the filter options.



- To filter the items based on device details, file path, signature and / or hash value, enter the search criteria in part or full in the respective text boxes and click 'Apply'.
- To filter the items based on file rating, select the required check box(es) under 'Rating' and click 'Apply'
- To filter the items based on the quarantined dates, enter or select from the calendar the dates in the 'From' and 'To' fields under 'Date Quarantined' and click 'Apply'

You can use any combination of filters at-a-time to search for specific items.

- To display all the items again, remove / deselect the search key from the filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Quarantine Items

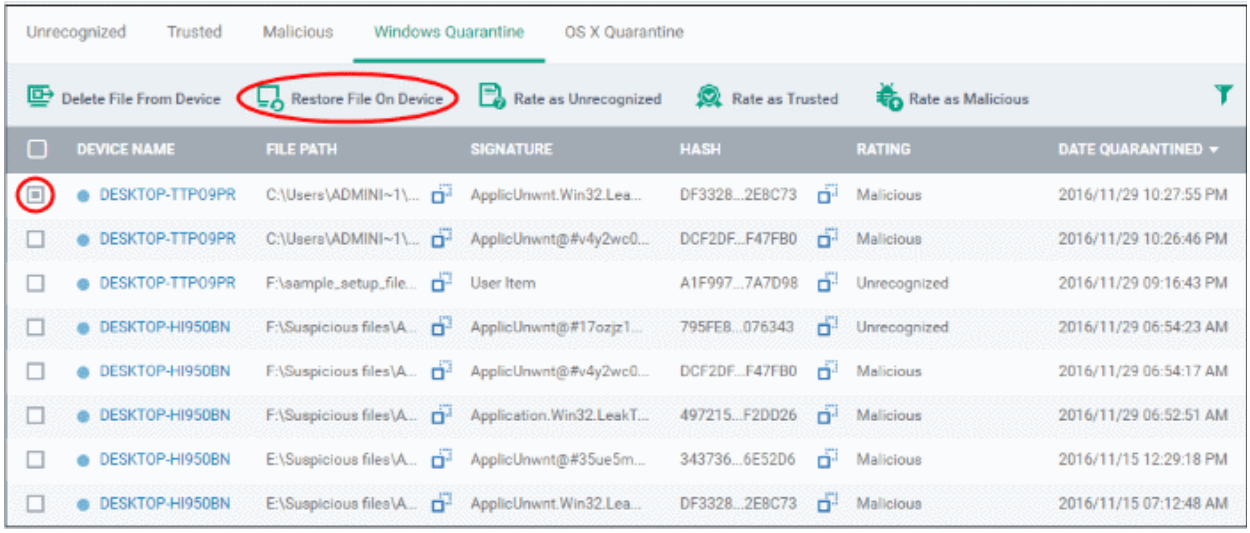
If the item identified as malware is found to be a genuine threat then administrators can delete it from the endpoints on which it was found. If an item is is found to be a false positive, administrators can restore the item to its original

location on the endpoint. You can also rate a file from the list as unrecognized or trusted based on your assessment. The changed file verdict will be reflected in the 'Unrecognized' and 'Trusted' interfaces and updated information will be sent to the endpoints.

Restoring False Positives from Quarantine

- If the identified item is a false positive, select the item from the list and click 'Restore File On Device' from the options at the top.

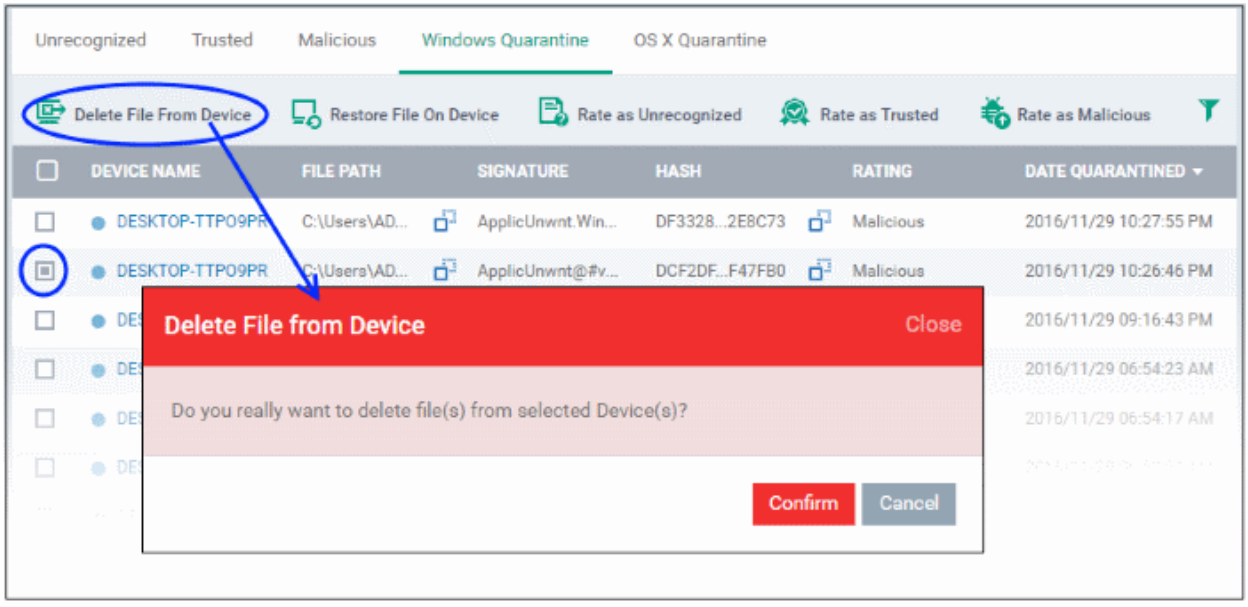
The item will be restored to its original location from the quarantine and removed from the list.



Removing Malware files from the devices

Administrators can remove malicious items from the devices through the 'Windows Quarantine' interface.

- To delete an item, select it from the list and click 'Delete File From Device' from the options at the top.



- Click 'Confirm' in the confirmation dialog.

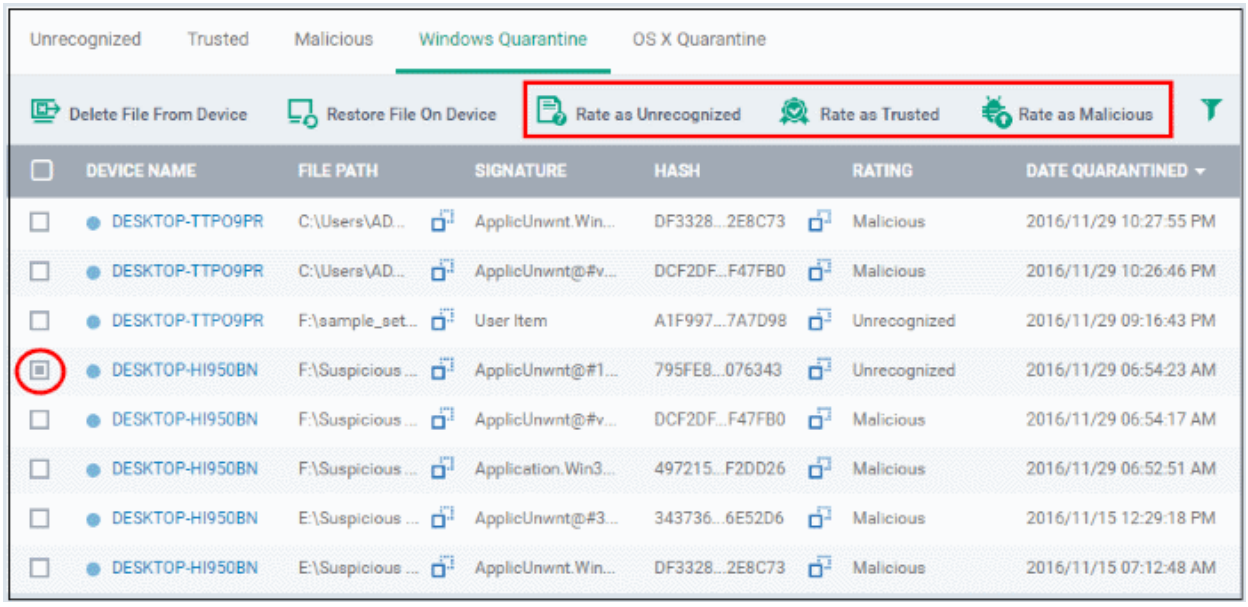
The file will be deleted from the device at which it was quarantined and from the list.

Rating files as 'Unrecognized', 'Trusted' or 'Malicious'

ITSM allows administrators to change the file rating of a quarantined file from this interface. If the file rating of a malicious file is changed to 'Trusted' or 'Unrecognized', the quarantined file is restored on the endpoints and the

'Trusted' / 'Unrecognized' interfaces are also updated.

- To change the file rating of an quarantined file, select it and click the respective rating button at the top



A confirmation will be displayed and the information will also be sent to the endpoints.

9.3. Viewing and Managing Quarantined Items on Mac OS Devices

Threats will be moved to quarantine in Comodo Antivirus for Mac (CAVM) on managed Mac OS X endpoints if:

- 'Auto quarantine' is enabled in the 'Realtime Scanning', 'Manual Scanning' and/or 'Scheduled Scans' area of the antivirus component of the profile active on the device (recommended)
- The end user chooses to quarantine the threat from a displayed alert
- An administrator moved a threat to quarantine from the 'Current Malware List' interface
- An end-user moved a file to quarantine on the endpoint

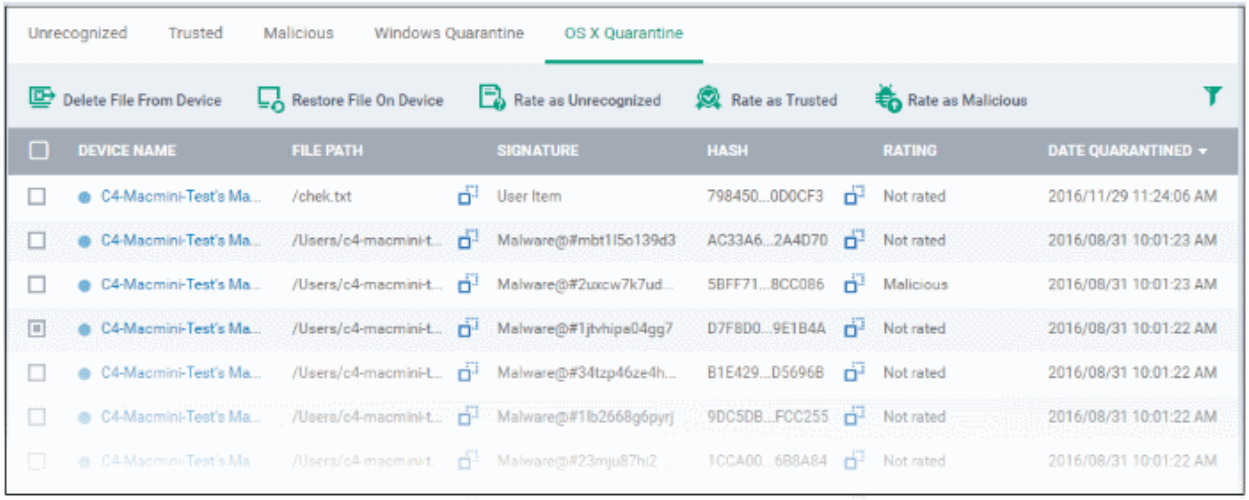
Items moved to quarantine are saved in an encrypted format and are not allowed to run on endpoints.

Refer to the explanation of **Scanner Settings** in the section **Antivirus Settings for OS X Profile** under **Creating Mac OS X Profiles** and the section **Viewing and Managing Identified Malware** for more details.

The 'OS X Quarantine' interface lists all items quarantined by CAVM on managed Mac OS X endpoints. The administrator can analyze the trustworthiness of the items, rate them as unrecognized or trusted, delete them permanently or restore them to their original location from this interface.

To open the Quarantine Files interface

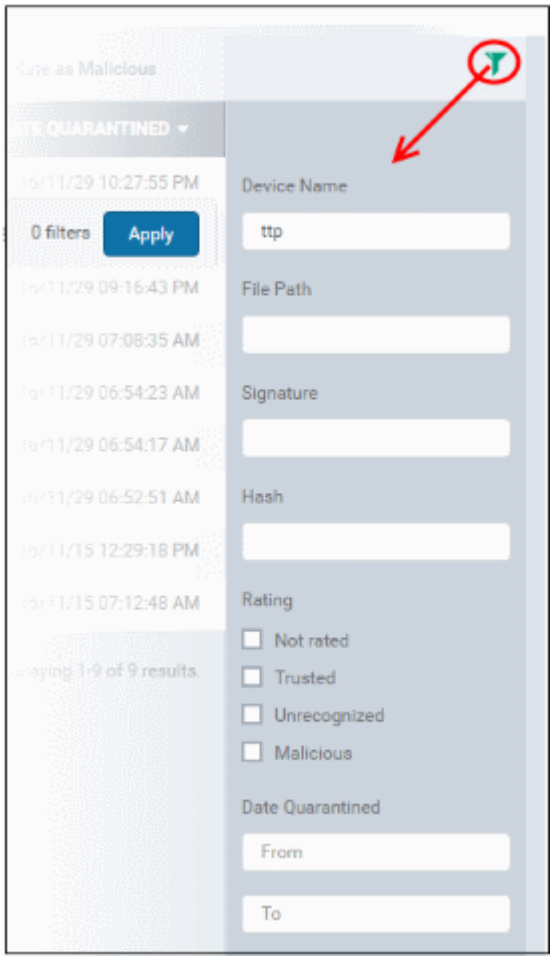
- Click 'Secure Sub-system' on the left and choose 'Application Control' from the options
- Click the 'OS X Quarantine' tab



The 'OS Quarantine' List - Table of Column Descriptions	
Column Heading	**Description**
Device Name	The name assigned to the device by the user. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to manage the device and to apply configuration profiles. Refer to the section **Managing Mac OS Devices** for more details.
File Path	The installation path of the infected application. • Clicking the icon copies the path to the clipboard.
Signature	The name of the malware. 'User Item' indicates the file was moved to quarantine manually by the user on the endpoint.
Hash	Displays the SHA1 hash value of the quarantined file • Clicking the icon copies the hash value to the clipboard.
Rating	Since CAVM does not have file rating functionality, the column will show 'Not Rated'. Administrators can manually change the rating from the options above and this change will be reflected in the interface.
Date Quarantined	Indicates the precise date and time at which the malware was first identified from the device.

Sorting, Search and Filter Options

- Clicking on any of the column headers sorts the table in ascending or descending order according to the items in the selected column.
- Clicking the funnel on the top right opens the filter options.



- To filter the items based on device details, file path, signature and / or hash value, enter the search criteria in part or full in the respective text boxes and click 'Apply'.
- To filter the items based on file rating, select the required check box(es) under 'Rating' and click 'Apply'
- To filter the items based on the quarantined dates, enter or select from the calendar the dates in the 'From' and 'To' fields under 'Date Quarantined' and click 'Apply'

You can use any combination of filters at-a-time to search for specific items.

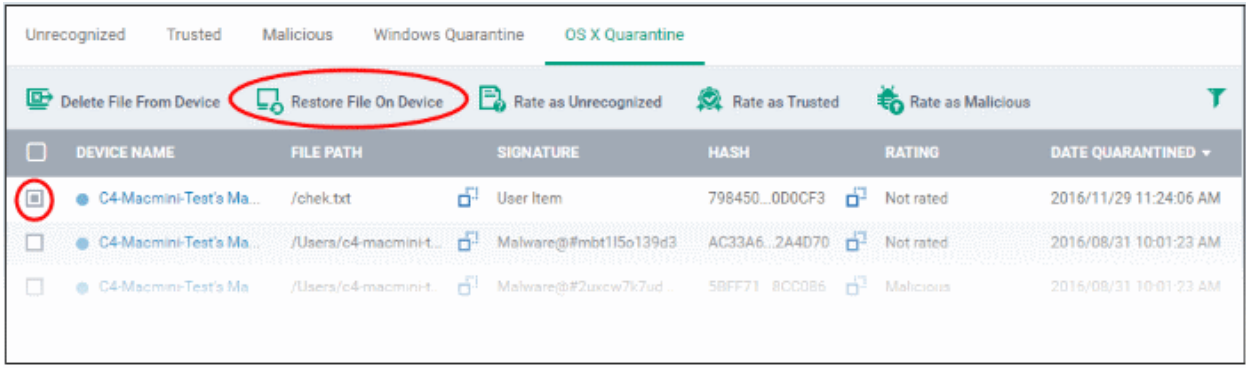
- To display all the items again, remove / deselect the search key from the filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Quarantined Items

Quarantined items that are confirmed as malicious can be deleted from the endpoints on which they were found. If an item is found to be a false positive, administrators can choose to restore the item to its original location. You can also rate a file from the list as unrecognized or trusted based on your assessment. The changed file verdict will be reflected in the 'Unrecognized' and 'Trusted' interfaces and the updated information will be sent to the endpoints.

Restoring False Positives from Quarantine

- If the identified item is a false positive, select the item from the list and click 'Restore File On Device' from the options at the top.

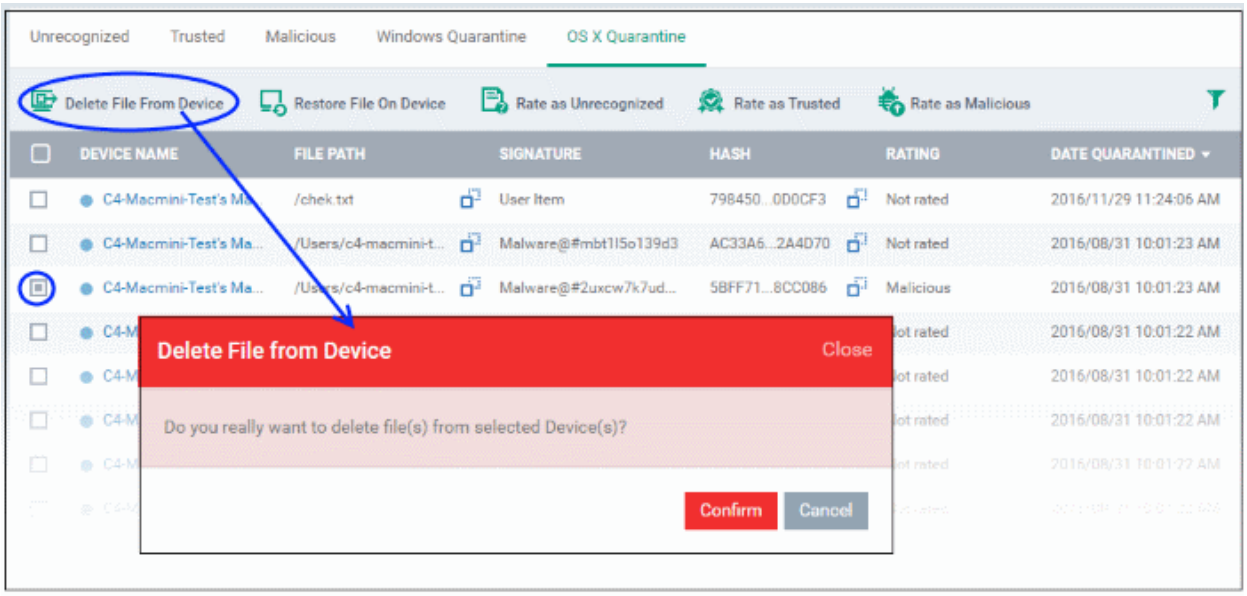


The item will be restored to its original location from the quarantine and removed from the list.

Removing Malware files from the devices

Administrators can remove malicious items from the devices through the 'OS X Quarantine' interface.

- To delete an item, select it from the list and click 'Delete File From Device' from the options at the top.



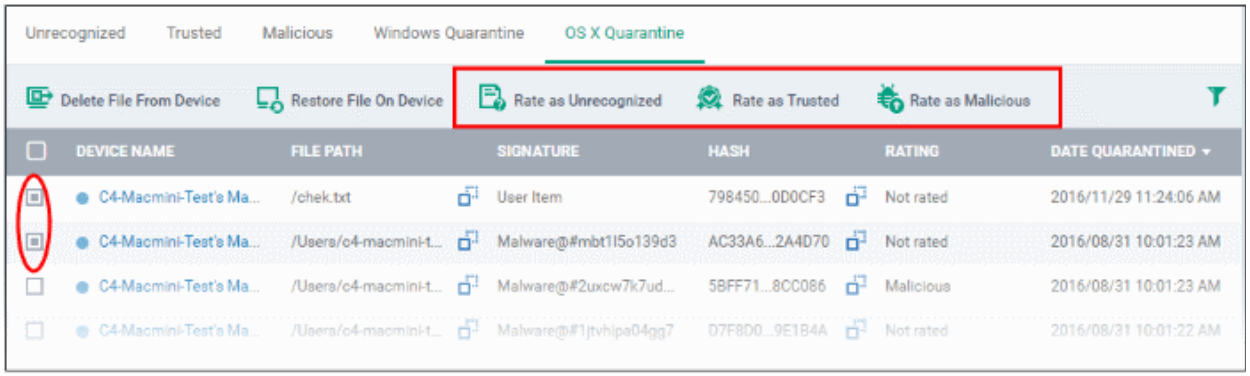
- Click 'Confirm' in the confirmation dialog.

The file will be deleted from the device at which it was quarantined and from the list.

Rating files as 'Unrecognized', 'Trusted' or 'Malicious'

ITSM allows administrators to change the file rating of a quarantined file from this interface. If the file rating of a malicious file is changed to 'Trusted' or 'Unrecognized', the quarantined file is restored on the endpoints and the 'Trusted' / 'Unrecognized' interfaces are also updated.

- To change the file rating of an quarantined file, select it and click the respective rating button at the top



A confirmation will be displayed and the information will also be sent to the endpoints.

9.4. Viewing list of Valkyrie Analyzed Files

Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Each CCS installation on a managed Windows Device is capable of uploading unknown files to Valkyrie for analysis.

- You can view all unknown files along with Valkyrie ratings by clicking 'Security Sub-Systems' > 'Next Gen Containment'
- You can view Valkyrie statistics in the ITSM Dashboard by clicking 'Dashboard' > 'Valkyrie'.
- You can schedule unknown files for upload by configuring the Valkyrie component of the Windows Profile applied to the device. For more details on configuring Valkyrie refer to the section **Valkyrie Settings** under **Creating Windows Profiles**.

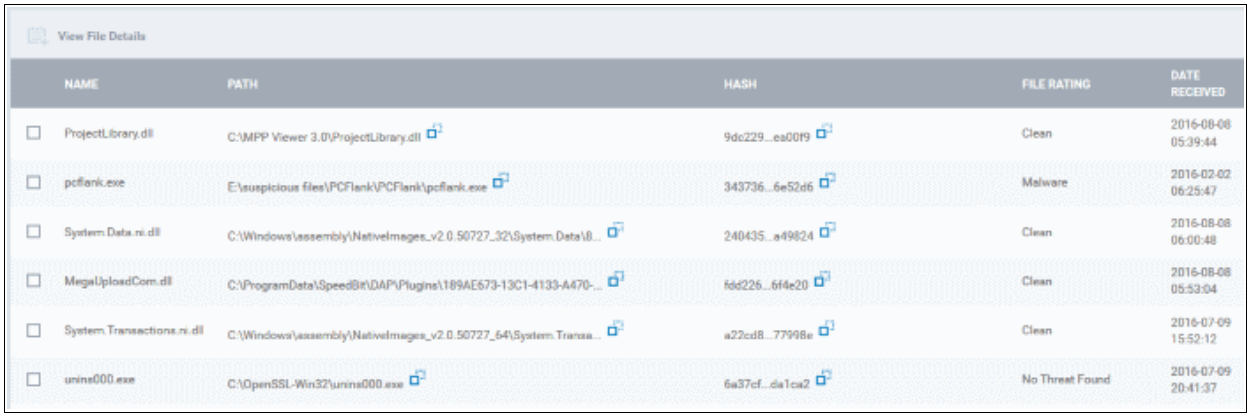
Note 1: The version of Valkyrie that comes with the free version of ITSM is limited to the online testing service. The Premium version of ITSM also includes manual testing of files by Comodo research labs. This helps enterprises quickly create definitive whitelists of trusted files. Valkyrie is also available as a standalone service. Contact your Comodo account manager for further details.

Note 2: ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit unknown files for analysis, monitor Windows events, provide alerts 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**.

The 'Next Gen Containment' screen displays a list of Valkyrie ratings for every unknown file uploaded from managed Windows devices. It also displays details about the unknown file.

To open the 'Next Gen Containment' interface

- Click 'Security Sub-Systems' on the left and choose 'Next Gen Containment' from the options

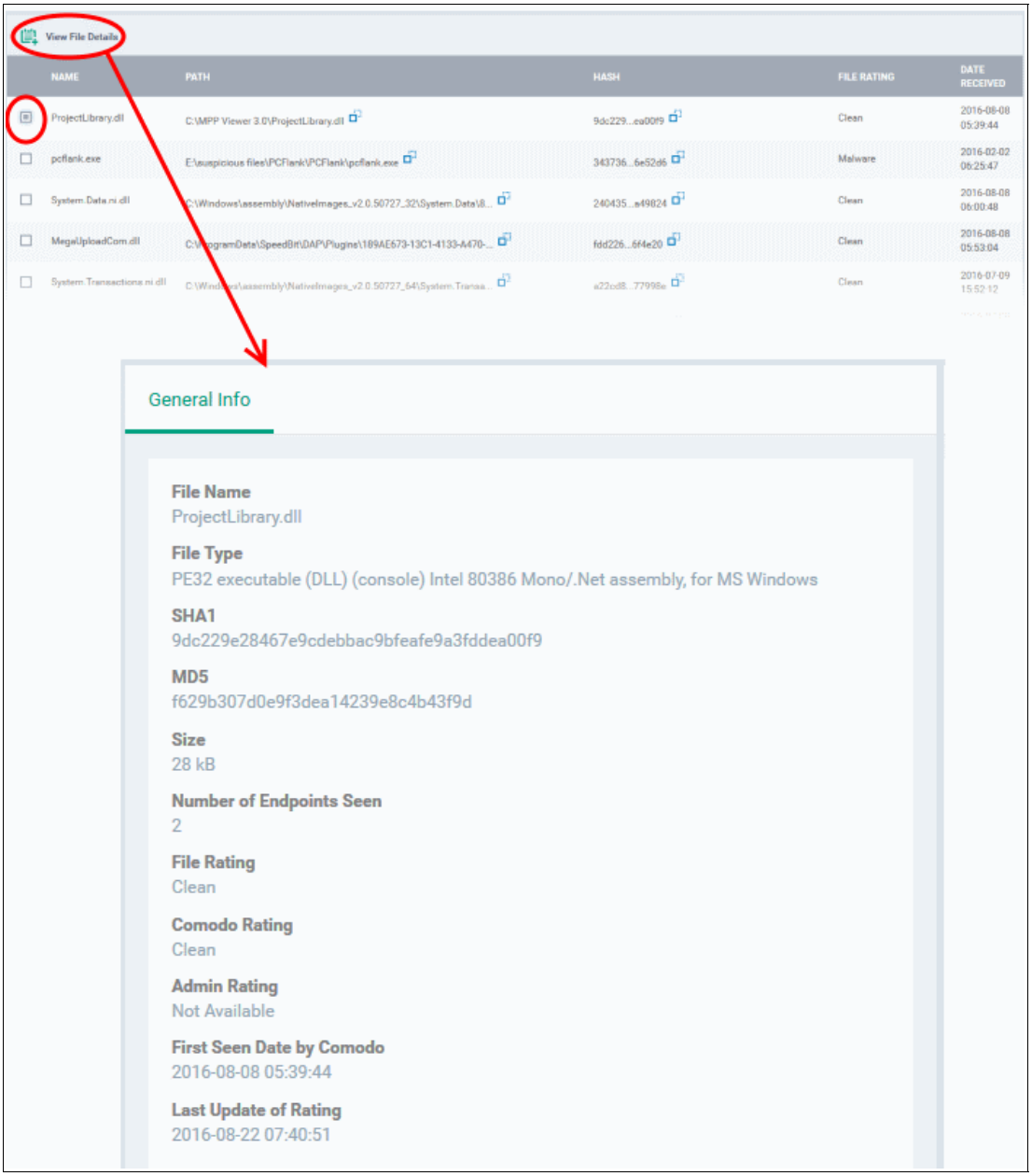


The 'Next Gen Containment' List - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the file name of the unknown item
Path	The installation location of the file at the endpoint
Hash	Displays the SHA1 hash value of the unknown file • Clicking the icon copies the hash value to the clipboard.
File Rating	Displays the verdict for the file from Valkyrie. The possible values are: • Clean - The file is safe to run • No Threat Found - No malware found in the file, but cannot say it is safe to run • Malware - The file is malicious and should not be allowed to run. • Potentially Unwanted Application - Applications such as Adware, browser toolbars and so on. These applications may be installed while installing an unrelated piece of software. Users may or may not be aware they are installed or may not be aware of their full functionality. For example, a browser toolbar may also contain code that tracks a user's activity on the internet.
Date Received	Indicates date and time at which the file was received by Valkyrie from the endpoint.

View the details of files in the list

Administrators can view complete details of files identified as 'Unknown' and uploaded to Valkyrie for analysis.

- To view the details of a file, select it and click 'View File Details' from the top.



The 'General Info' screen displays file details like file name, installation path, file version, size, hash value and file ratings assigned by Comodo and by the Administrator.

9.5. Antivirus and File Rating Scans

The 'Antivirus Device List' interface displays the infection status of Android, Mac OS and Windows devices and allows you to:

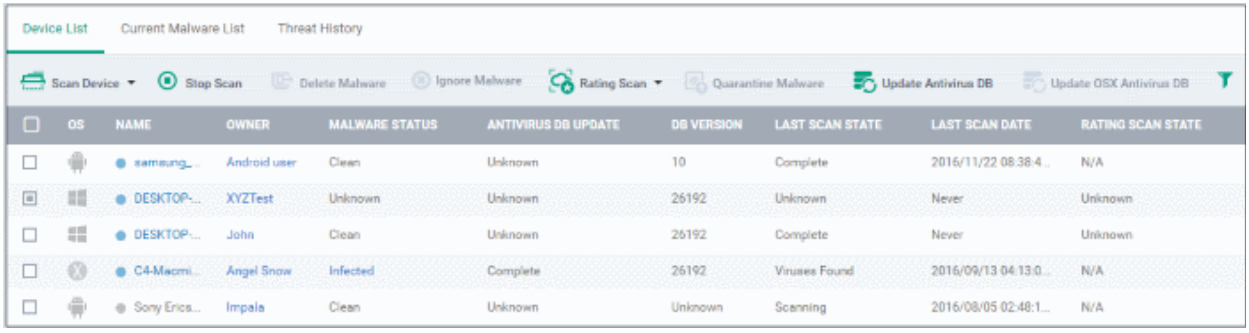
- Run on-demand antivirus scans on selected devices
- Run file rating scans on Windows devices

It also allows you to choose the action to be taken on malware discovered by scans.

Note: Comodo security software on Windows and Mac endpoints is capable of scanning specific areas and running scheduled antivirus scans. You can define these items in the 'Antivirus' component of Windows and Mac OS configuration profiles. For more details on creating custom scan profiles, refer to:

- The explanation of Custom Scans in the section Antivirus Settings under Creating a Windows Profile.
- The explanation of Scan Profiles in the section Antivirus Settings under Creating Mac OS X Profiles.

- To open the 'Antivirus Device List' interface, click 'Secure Sub-Systems' > 'Antivirus' on the left and choose 'Device List' from the options.

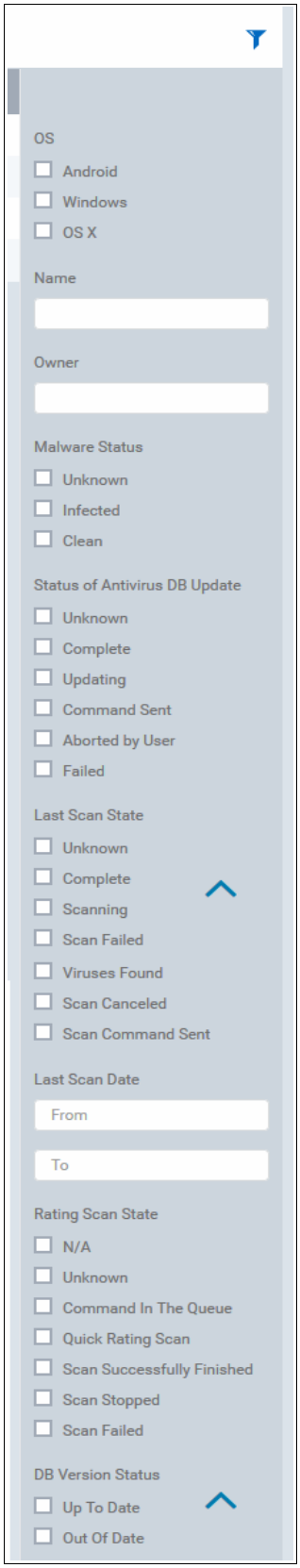


The list displays all Android, Mac OS and Windows devices along with the device owner, date of the last virus scan, infection status and the progress of the most recent scan.

Antivirus Device List - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system of the device.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used. A gray text color indicates the device has been offline for the past 24 hours. Clicking the device name will open the granular device details interface. Refer to the sections Managing Windows Devices, Managing Mac OS Devices and Managing Android / iOS Devices for more details.
Owner	Indicates the device user. Clicking the user name will open the 'View User' interface. Refer to Viewing the User Information for more details.
Malware Status	Indicates the infection status of the device based on the results from the real-time, on-demand and/or scheduled scans. The devices identified with malware will be indicated as 'Infected'. Clicking on 'Infected' will open the 'Current Malware List' interface that displays the list of malware identified from all managed devices. Refer to the section Handling Malware on Scanned Devices for more details.
Antivirus Database Update	Indicates the update status of virus signature database at the device.
DB Version	Indicates the database version at the device
Last Scan State	Indicates whether the device is found infected or not, from the results of the last run on-demand/scheduled scan.
Last Scan Date	Indicates the date and time at which the last antivirus scan was run.
Rating Scan State	Indicates the status of last run file rating scan or currently running scan.

Sorting, Search and Filter Options

- Clicking on any column header sorts the table in order of the entries in the selected column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific device based on device name and/or owner, enter the search criteria in part or full in the respective text boxes and click 'Apply'.
- To filter the items based on OS types, select the OS types of the devices to be displayed in the list
- To filter the devices last scanned within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under 'Last Scan Date', using the calendars that appear on clicking inside the respective field and click 'Apply'.

- To filter the devices based on their Malware Status, AV database update status, last scan state and/or last file rating scan state, select the status and click 'Apply'.

You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Following sections explain more about:

- Running On-Demand Antivirus Scans on Devices
- Running Rating Scans on Windows Devices
- Handling Malware identified from Scanned Devices
- Updating virus signature database at selected Devices

9.5.1. Running On-Demand Antivirus Scans on Devices

The 'Antivirus > Device List' interface allows Administrators to initiate on-demand virus scans on Android, Mac OS and Windows devices.

Note: The scans interface allows you to manage on-demand scans only. For automatic or scheduled AV scans, administrators should specify the scan schedule in a configuration profile then push it to the selected devices/group. Refer to the section Creating Configuration Profiles for more details.

To launch an on-demand AV scan

- Click 'Security Sub-Systems' at the left and select 'Antivirus' from the options.
- Click the 'Device List' tab
- Select the Android, Mac OS or Windows device(s) you wish to scan.
- Click 'Scan Device' and choose Quick Scan, Full Scan or SD Card Scan.

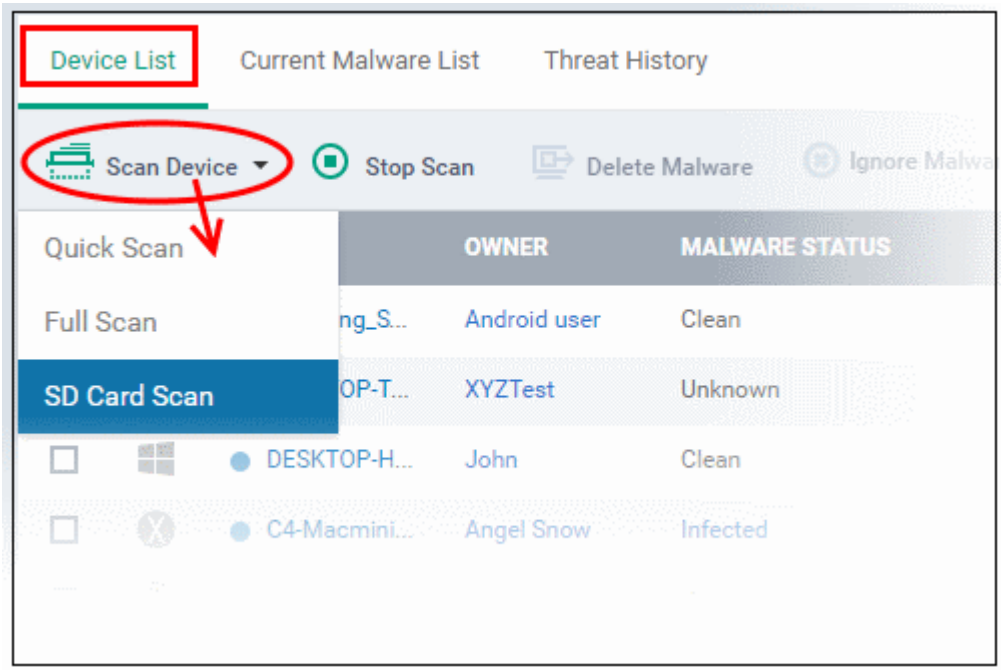
Tip: You can filter or search for specific devices using the filter options that appear on clicking the funnel icon at the top right. For example, you may want to display only devices with Last Scan States of 'Unknown', 'Scan Failed' and 'Scan Canceled'.

The next step is to choose the scan profile that defines the areas to be scanned in the selected device(s). The profiles differ depending on the OS type of the chosen devices. The following sections explain the scan process for:

- Android Devices
- Windows Devices
- Mac OS Devices

Android Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Quick Scan** - Scans the critical areas of the device, which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include RAM, hidden services and other significant areas like system files. These areas are of great importance to the health of the device so it is essential to keep them free of infection.
- **Full scan** - Scans all the folders/files in both the system internal memory and the SD card.
- **SD Card Scan** - Scans all folders/files in the Secure Digital (SD) memory card mounted on the device.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

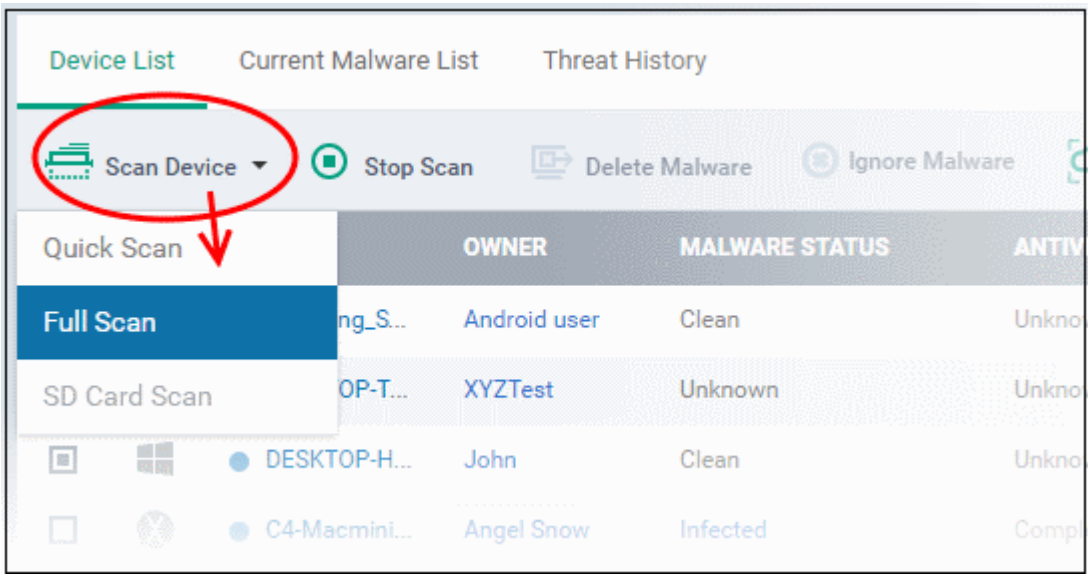
- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found after the scan then the 'Last Scan State' will say 'Infected'. The infections identified after the scan will be treated according the settings in 'Settings' > 'Portal Set-Up' >Android Client Configuration' > 'Antivirus'. Refer to the section **Configuring Android Client Antivirus Settings** for more details. If 'Manual control' is chosen, then administrators have the option to uninstall or ignore from the results displayed in the Current Malware List interface. Refer to the section **Viewing and Managing Identified Malware** for more details.

Administrators can also choose to uninstall or ignore the identified malware by clicking the respective buttons at the top. Refer to the **Handling Malware Identified from Scanned devices** section for more details.

Windows Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Quick Scan** - The 'Quick Scan' scans critical areas of the computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of each computer so it is essential to keep them free of infection.
- **Full Scan** - The 'Full Scan' scans every local drive, folder and file on each computer. Any external devices like USB drives, digital camera and so on are also scanned.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

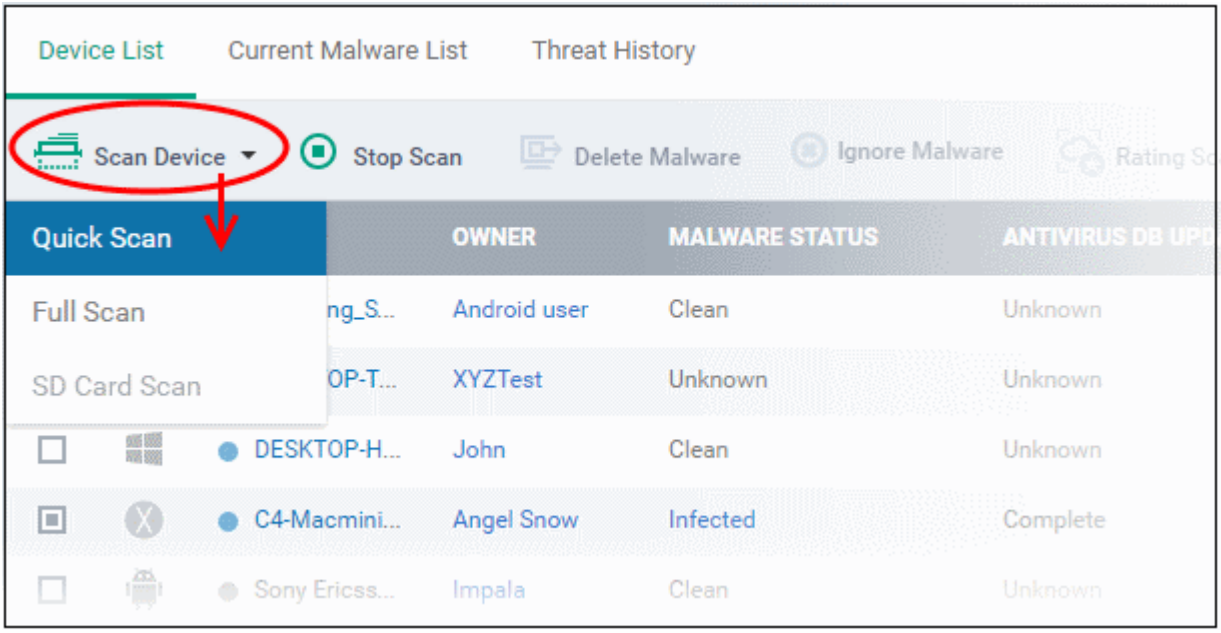
- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found on completion of scan the Last Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. Refer to the next section **Handling Malware Identified from Scanned devices** for more details.

Items moved to quarantine are encrypted and saved in the endpoint itself, so that they are isolated from the rest of the system. You view the quarantined items from the 'Quarantine' interface and have the option to delete the file, if the item is identified as malicious or restore it at the endpoint if the item is a false-positive. Refer to the section **Viewing and Managing Quarantined Items** for more details.

Mac OS Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Quick Scan** - When this profile is selected, Comodo Antivirus scans every local drive, folder and file on your system including external devices, storage drives, digital cameras.
- **Full Scan** - When this profile is selected, Comodo Antivirus runs a scan of important operating system files and folders including system memory, auto-run entries, hidden services.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found on completion of scan the Last Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. Refer to the next section **Handling Malware Identified from Scanned devices** for more details.

Items moved to quarantine are encrypted and saved in the endpoint itself, so that they are isolated from the rest of the system. You view the quarantined items from the 'Quarantine' interface and have the option to delete the file, if the item is identified as malicious or restore it at the endpoint if the item is a false-positive. Refer to the section **Viewing and Managing Quarantined Items on Mac OS Devices** for more details.

9.5.2. Running Rating Scans on Windows Devices

The 'Rating Scan' feature runs a cloud-based assessment on files on the Windows devices to assess how trustworthy they are. The Quick rating scan checks commonly infected areas and memory in the the cloud for file reputation.

Based on the trustworthiness, the files are rated as:

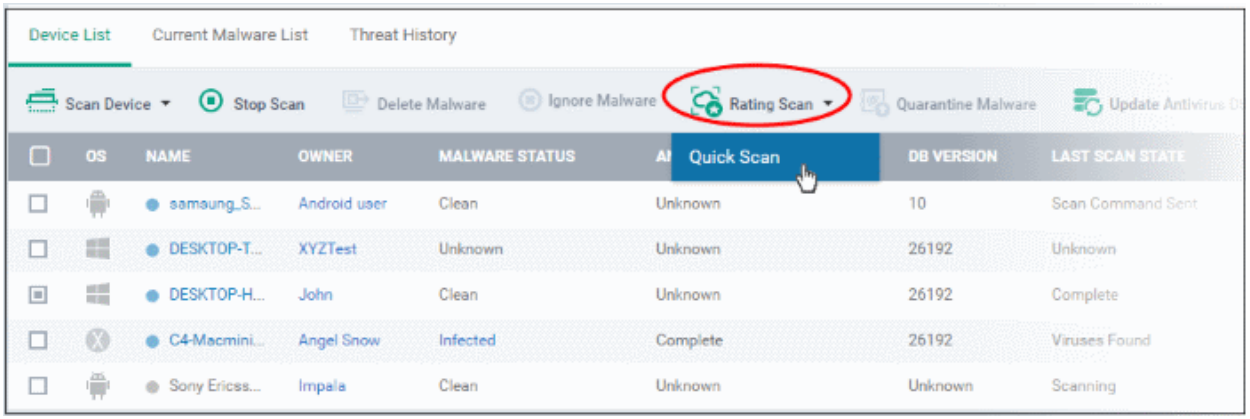
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code

To run a rating scan on Windows devices

- Click 'Security Sub-Systems' at the left and select 'Anti-Virus' from the options.
- Click the 'Device List' tab
- Select the Windows device(s) you wish to scan.

- Click 'Rating Scan' > 'Quick Scan'

Tip: You can filter or search for specific devices using the filter options that appear on clicking the funnel icon at the top right. For example, you may want to display only devices with Last Scan States of 'Unknown', 'Scan Failed' and 'Scan Canceled'.



The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Rating Scan State' column for each device.

- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found on completion of scan the Last Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. Refer to the next section **Handling Malware Identified from Scanned devices** for more details.

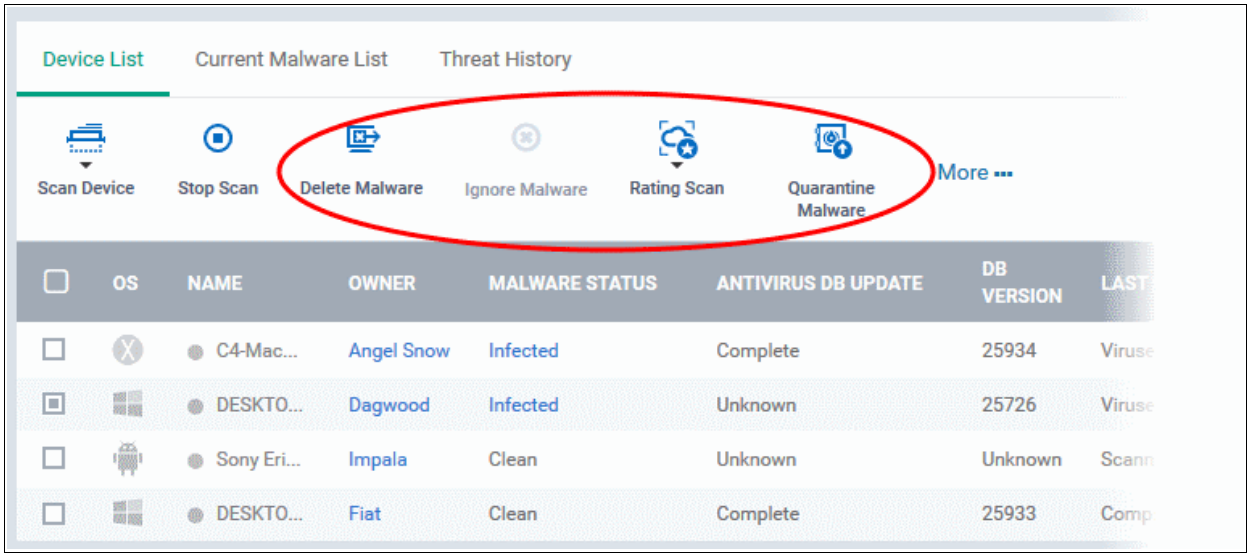
9.5.3. Handling Malware on Scanned Devices

If malware is detected on a managed Android, Windows or Mac OS device, the 'Malware Status' column will display 'Infected' or 'Virus Found'. You can choose to remove, ignore or quarantine detected malware using the buttons above the table.

Tip: The 'Security Sub-Systems' > 'Anti-Virus' interface allows you apply actions to all malware identified on a particular device. If you want to review and apply actions to individual pieces of a malware on a device, please use the 'Current Malware List' instead. Refer to the section **Viewing and Managing Identified Malware** for more details.

To choose the action to be taken on the detected malware

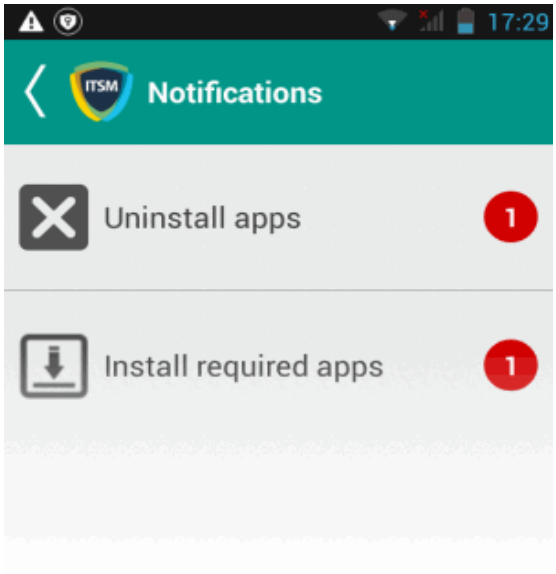
- Click 'Security Sub-systems' from the left then select 'Antivirus'.
- Click the 'Current Malware List' tab
- Select an infected Android, Windows or Mac OS device(s) using the check-boxes on the left.
- Choose an action from the top row:



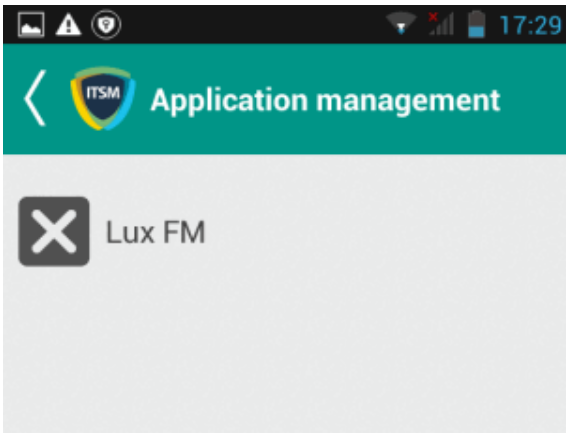
For Android Devices:

- Delete Malware - Removes the malicious app
- Ignore Malware - Ignores the malware for the current scan. On the next scan, the item will again be identified as malware

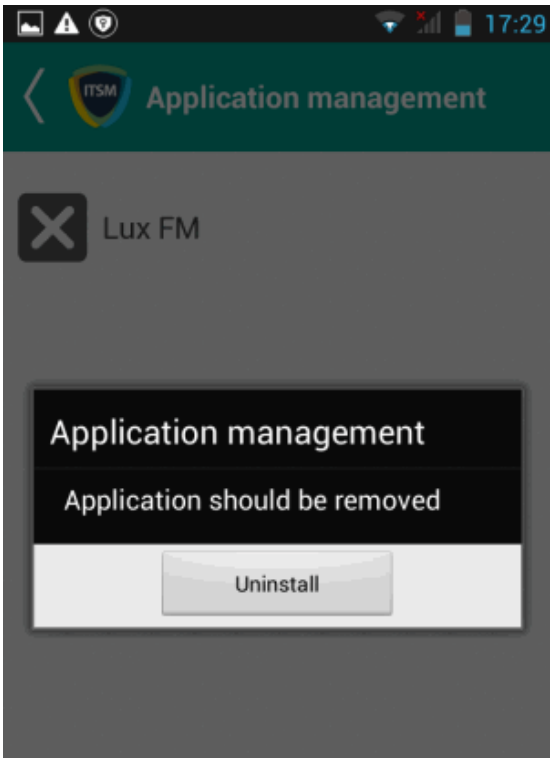
For the uninstall operation, a notification will be sent to all affected devices:



The notification will indicate the number of threats to be removed from the device. On touching the alert, a list of items to be removed will be displayed.



The user needs to tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



For Windows Devices

- Delete Malware - ITSM instructs the CCS application at the endpoint to clean the malware. If a disinfection routine is available for the selected infection(s), CCS will disinfect the application and retain the application. If a disinfection routine is not available, CCS will remove the application.
- Quarantine Malware - Moves the detected malware to the Quarantine in the device for later analysis. You can view quarantined files from the 'Quarantine' interface. Based on their trustworthiness, you can remove them from the device or restore them to their original locations. Refer to the section Viewing and Managing Quarantined Items for more details.

For Mac OS Devices

- Delete Malware - ITSM instructs the CAVM application at the endpoint to clean the malware. If a disinfection routine is available for the selected infection(s), CAVM will disinfect the application and retain the application. If a disinfection routine is not available, CAVM will remove the application.
- Quarantine Malware - Moves the detected malware to the Quarantine in the device for later

analysis. You can view quarantined files from the 'Quarantine' interface. Based on their trustworthiness, you can remove them from the device or restore them to their original locations. Refer to the section Viewing and Managing Quarantined Items for more details.

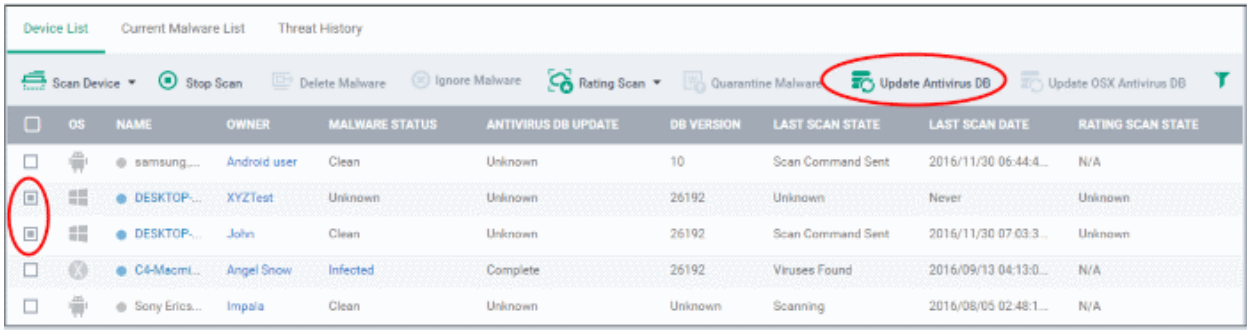
9.5.4. Updating Virus Signature Database on Windows Devices

In order to guarantee continued and effective antivirus protection on managed Windows devices, it is imperative that their virus databases are updated as regularly as possible. ITSM allows you to automate the periodical virus database updates at the managed Windows devices by the configuring a schedule in the Client Security Update Rule component in the Windows profile applied to the device. Refer to the explanation of configuring the Client Security Update Rule component under the section Creating Windows Profiles for more details.

You can also manually update the virus signature database at the managed Windows devices as and when required. The 'Anti-Virus' interface under 'Secure Sub-Systems' allows you to remotely update the virus databases at selected devices.

To update virus signature database on selected endpoints

- Choose 'Security Sub-Systems' from the left then select 'Anti-Virus'.
- Click the 'Device List' tab
- Select the Windows device(s) on which you wish to update the virus database.



Tip: You can filter the list or search for specific device(s) by clicking the funnel icon at the top right of the table.

- Click 'Update Antivirus DB' from the options at the top.

A command will be sent to the ITSM agent at the selected endpoints to start download the updates from the Comodo's update servers.

9.5.5. Updating Virus Signature Database on Mac OS Devices

In order to guarantee continued and effective antivirus protection on managed Mac devices, it is imperative that their virus databases are updated as regularly as possible. ITSM allows you to automate the periodical virus database updates at the managed Mac OS devices by the configuring a schedule in the OS X profile applied to the device. Refer to the update section in Creating Mac OS X Profiles for more details.

You can also manually update the virus signature database at the managed Mac OS devices as and when required. The 'Anti-Virus' interface under 'Secure Sub-System' allows you to remotely update the virus databases at selected devices.

To update virus signature database on selected endpoints

- Click 'Security Sub-Systems' on the left then select 'Antivirus'.
- Click the 'Device List' tab
- Select the Mac OS device(s) on which you wish to update the virus database.

Tip: You can filter the list or search for specific device(s) by clicking the funnel icon at the top right of the table.

- Click 'Update OSX Antivirus DB' from the options at the top.

A command will be sent to the ITSM agent at the selected endpoints to start download the updates from the Comodo's update servers.

9.6. Viewing and Managing Identified Malware

The 'Current Malware List' interface displays malicious items identified on enrolled devices for which no action has yet been taken. Administrators can choose to uninstall the malicious items from the devices or quarantine the item from this interface. You have the option to ignore the item and remove it from the malware list if you feel the item is trustworthy.

Note:

For Android Devices:

If AV settings in the configuration profile active on a device is configured to automatically uninstall or ignore, the identified malicious item will be cleaned accordingly and will not be displayed in the Current Malware List interface. Refer to the section **Android Client Antivirus Settings** for more details.

For Windows Devices:

If 'Show antivirus alerts' is disabled and Quarantine Threats is chosen as default action in the 'Realtime Scan Settings' of the Antivirus component in the configuration profile active on the device, the identified threats will be moved to Quarantine automatically and will not be listed in this interface. If 'Show antivirus alerts' is enabled, and if the end user chooses to quarantine the threat from the displayed alert, the threat will be moved to Quarantine at the device and will not be displayed in this interface. Only if 'Block Threats' is chosen in both the cases, the threats will be displayed in this interface. Refer to the explanation of **Realtime Scan settings** in the section **Antivirus Settings** under **Creating Windows Profiles** for more details.

For Mac OS X Devices:

Threats will only appear in this interface if 'Block Threats' is enabled rather than 'Auto-Quarantine' in the profile in effect on the device.

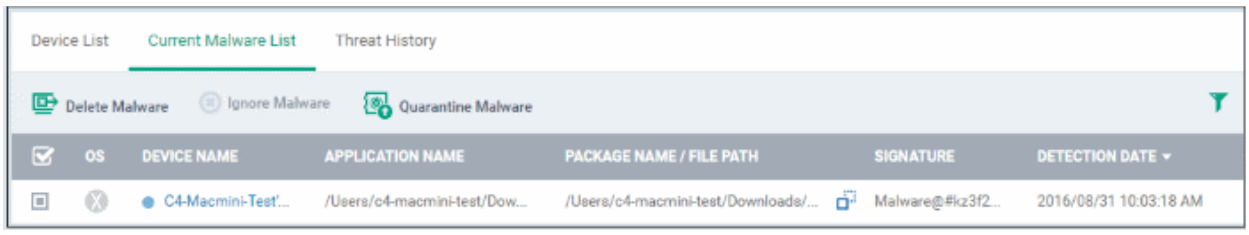
If 'Auto quarantine' is enabled in 'Real-time Scan Settings' , 'Manual Scanning' and 'Scheduled Scanning' then the threats will be moved to quarantine automatically and not shown in this interface.

If 'Auto quarantine' is disabled but the end user chooses to quarantine the item from the alert, then it will be moved to quarantine and not listed in this interface.

Refer to the explanation in the section **Antivirus Settings** under **Creating Mac OS X Profiles** for more details.

To view the malware list

- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Current Malware List' tab.

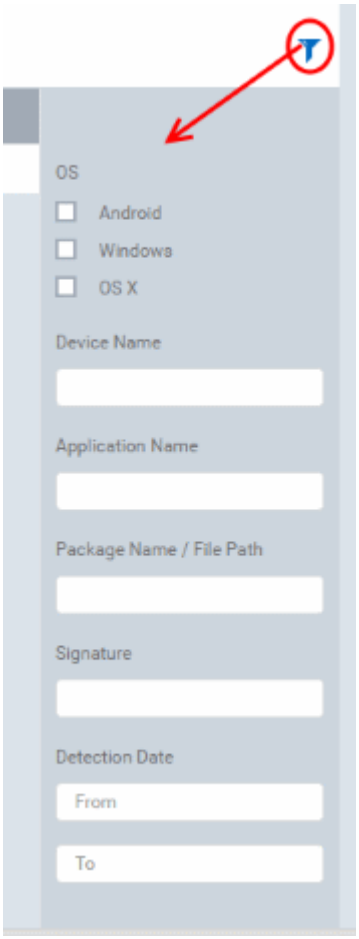


A list of malware identified from all the enrolled Android, Windows and Mac OS X devices will be displayed.

Current Malware List - Column Descriptions	
Column Heading	**Description**
OS	Indicates operating system of the device from which the malware was identified.
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the section **Managing an Individual Device** for more details.
Application Name	The name of the infected application.
Package Name / File Path	The installation location of the file at the endpoint. For malware on Android devices, the package name or identifier of the package from which the app was installed will be displayed.
Signature	The name of the identified malware.
Detection Date	The precise date and time at which the malware was identified.

Sorting, Search and Filter Options

- Clicking on any of the column headers sorts the items based on alphabetical / numerical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific malware based on device name, signature name, infected application name, and/or package name/file path, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

- To filter the items based on OS types, select the OS types of the infected devices for respective items to be displayed in the list
- To filter the threats identified within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under 'Detection Date', using the calendars that appear on clicking inside the respective field and click 'Apply'.
- To filter the devices based on their last or current scan status, select the status under 'Last Scan State' and click 'Apply'.

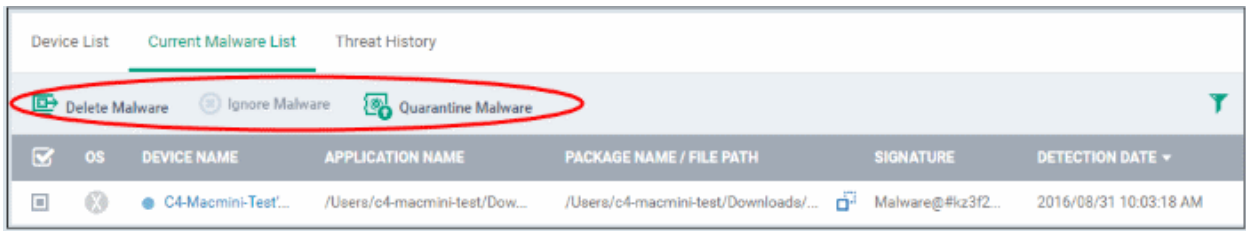
You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

Handling the Threats

If the item identified as malware is found to be a genuinely malicious, the administrator can uninstall/delete it from the devices on which it was found. If an item is found to be a false positive, the administrator can choose to ignore the item. The item will not be uninstalled from the device but will be removed from the 'Current Malware List' interface. If an item is found to be suspicious, the administrator can choose to move it to quarantine for later analysis and removal.

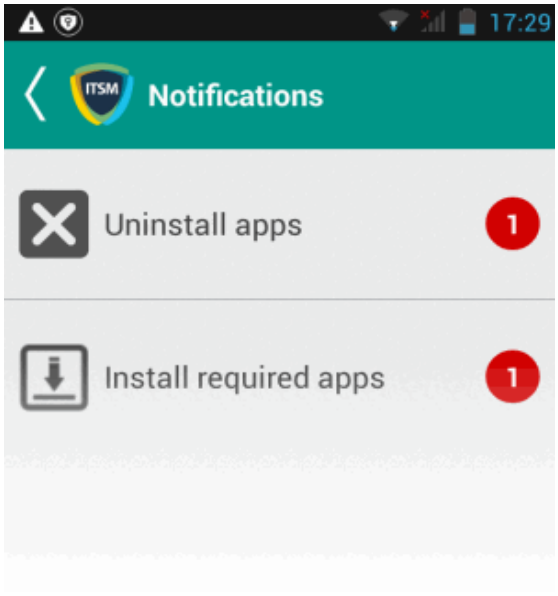
The options at the top of the table allow you to choose the action to be taken on selected items.



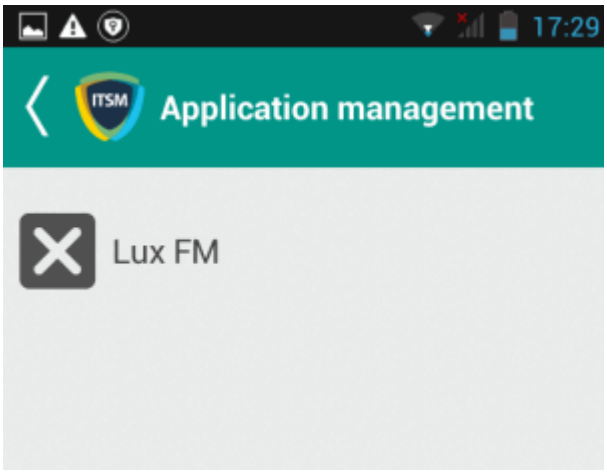
For threats identified from Android Devices

- If the identified item is a false positive, select the app from the list and click 'Ignore Malware' from the options at the top.
- To remove malware package(s), select the packages from the list and click 'Uninstall Malware' from the options at the top.

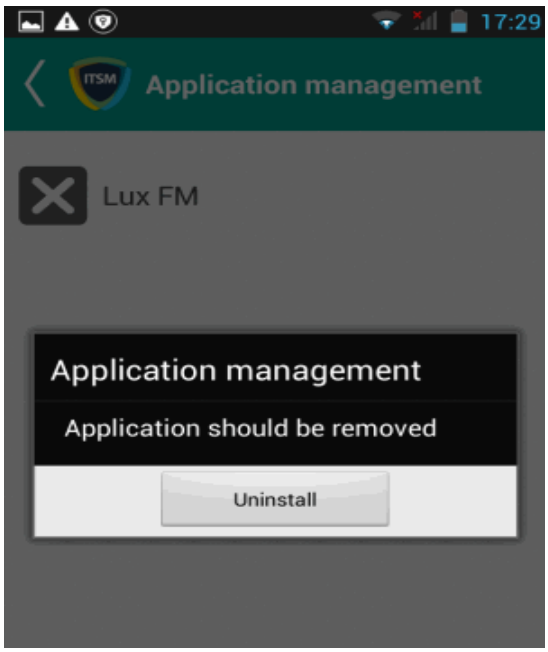
For the uninstall operation, a notification will be sent to all affected devices.



A notification will indicate the number of threats to be removed from the device. On touching the alert, a list of items to be removed will be displayed.



You needs to tap on the malware that needs to be removed, confirm the removal in the next dialog. and follow the uninstall wizard.



For threats identified from Windows Devices:

- If the identified item is a virus, select the app from the list and choose 'Delete Malware'. If a disinfection routine is available in the CCS for removing the malware, only the threat will be removed from the applications. Else, the infected application will be removed from the device.
- If the identified item is suspicious, select the item(s) and click 'Quarantine Malware'. The item(s) will be moved to quarantine in the respective device(s). You can analyze the quarantined files and if they are found trustworthy, you can restore them to their original locations, else remove them from the devices. Refer to the section Viewing and Managing Quarantined Items for more details.

For threats identified from Mac OS X Devices:

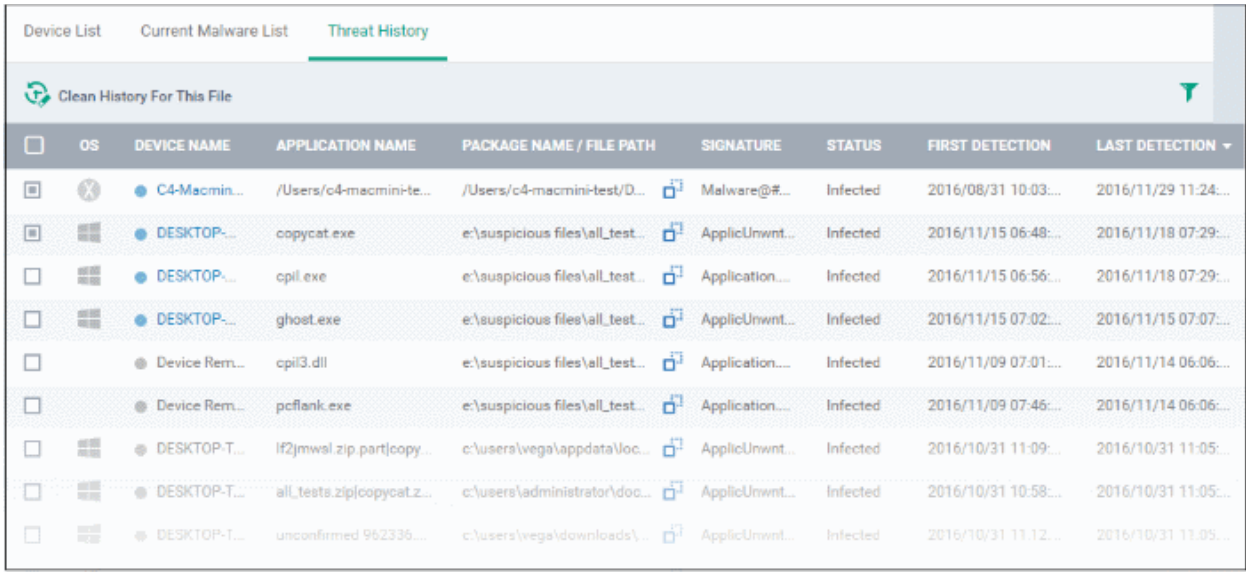
- If the identified item is a virus, select the app from the list and choose 'Delete Malware'. If a disinfection routine is available in CAVM for removing the malware, only the threat will be removed from the applications. Else, the infected application will be removed from the device.
- If the identified item is suspicious, select the item(s) and click 'Quarantine Malware'. The item(s) will be moved to quarantine in the respective device(s). You can analyze the quarantined files and if they are found trustworthy, you can restore them to their original locations, else remove them from the devices. Refer to the section Viewing and Managing Quarantined Items for more details.

9.7. Viewing Threats History

The 'Threat History' interface displays all threats identified on Android, Windows and Mac OS X devices over time. The list includes both the items that are removed from the devices and those yet to be removed.

To view the history of threats identified

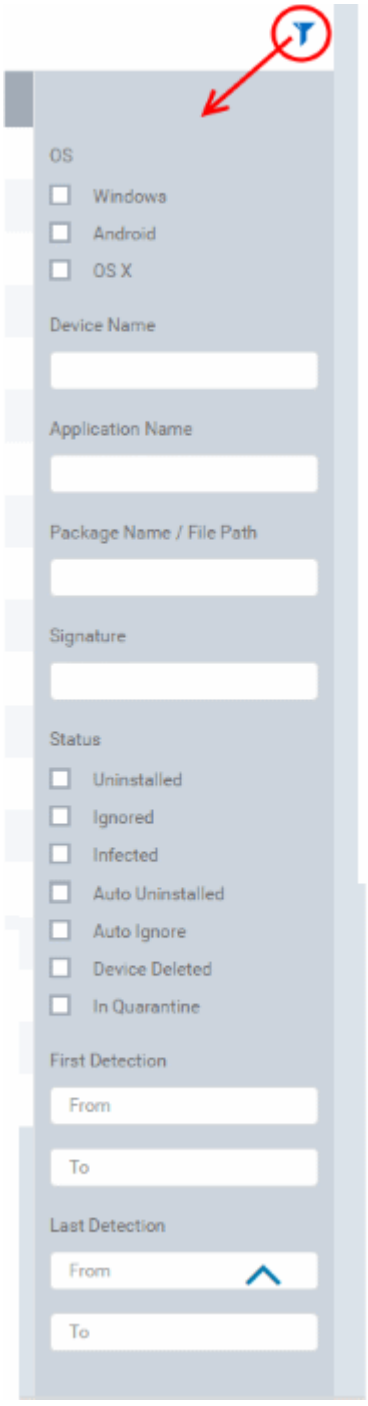
- Choose 'Security Sub-systems' from the left and click 'Antivirus'.
- Select the 'Threat History' tab.



Antivirus Threat History - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system type
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the sections 'Managing Windows Devices' and 'Managing Mac OS Devices' for more details.
Application Name	The name of the infected application.
Package Name / File Path	The Android package name or identifier of the package from which the app was installed. For Windows and Mac OS X devices, the file path of the detected malware will be displayed.
Signature	The name of the identified malware.
Status	Indicates whether the malware was uninstalled or yet to be uninstalled
First Detection	Indicates the precise date and time of the scan at which the malware was first identified from the device.
Last Detection	Indicates the precise date and time of the scan at which the malware was last identified from the device.

Sorting, Search and Filter Options

- Clicking any column header will sort items in alphabetical/numerical order
- Clicking the funnel button at the right end, opens the filter options.



- To filter the items or search for a specific malware based on OS type, select the check box beside the type and click 'Apply'.
- To filter the items or search for a specific malware based on device name, signature name, infected application name, and/or package name/file path, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

- To filter the items based on their infection status(es), select the status(es)
- To filter the threats based on time at which they were first identified or last identified within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under respective categories, using the calendars that appear on clicking inside the respective field and click 'Apply'.

You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

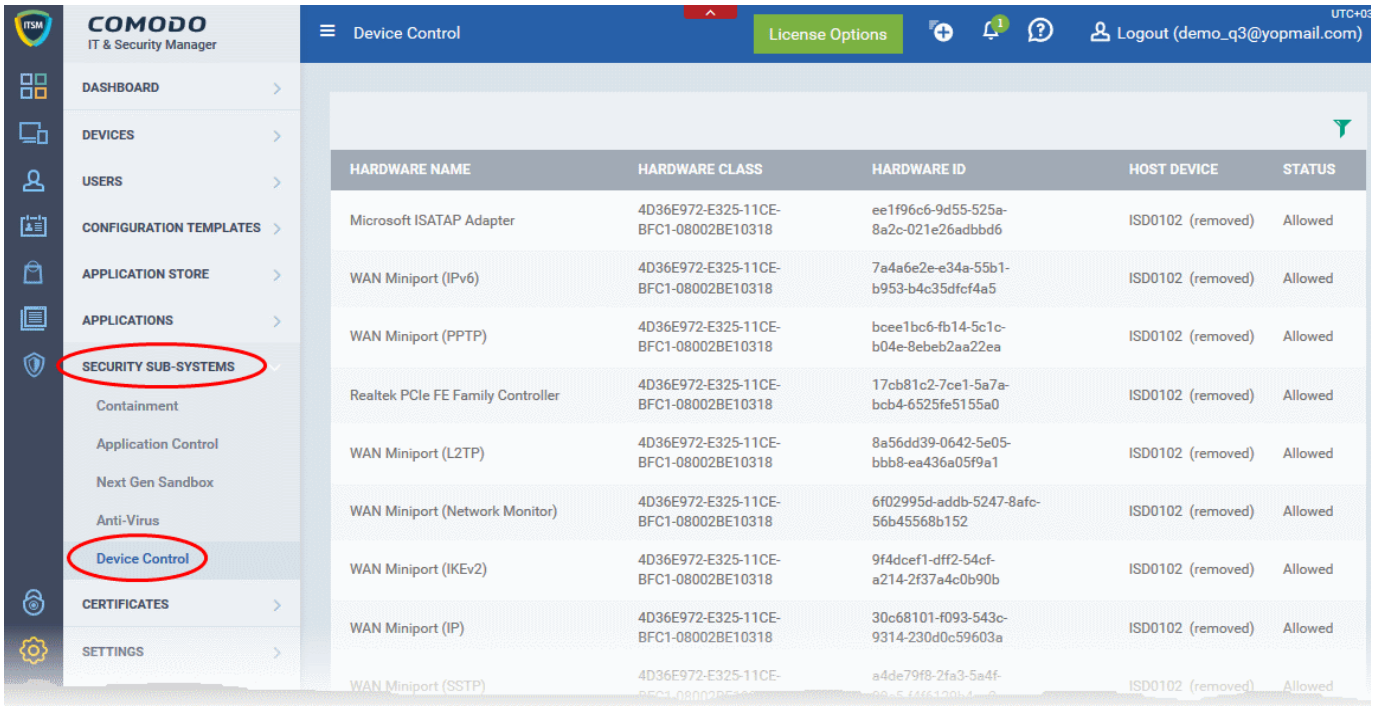
9.8. Viewing History of External Device Connection Attempts

ITSM can maintain a log of connection attempts to managed Windows endpoints by external devices such as USB storage devices, human interface devices, printers and Bluetooth devices. These logs are created when the Windows profile contains the 'External Devices Control' section. Refer to the section External Devices Control Settings for more details.

Administrators can view a list of external devices that were connected/removed to/from managed Windows devices, from the 'Device Control' interface.

To view a history of device connections:

- Click 'Security Sub-Systems' on the left and the select 'Device Control'

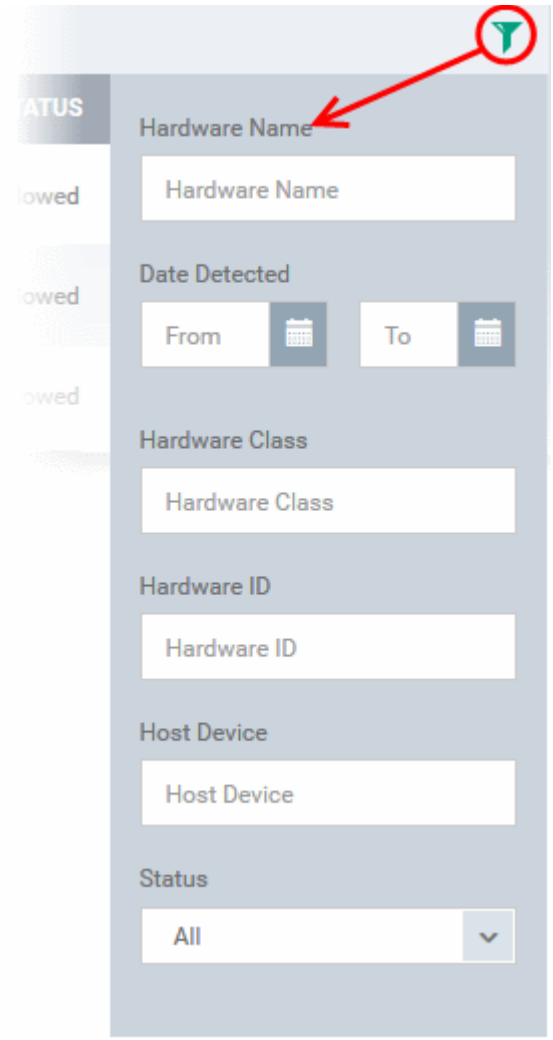


Device Control - Column Descriptions	
Column Header	**Description**

Hardware Name	Displays the name of the external device connected to a managed Windows device
Hardware Class	Displays the Globally Unique Identifier (GUID) of the device class of the device
Hardware ID	Displays the Device Identifier of the external device
Host Device	Indicates the managed Windows device, to which the device was connected and the current connection status (connected or removed)
Status	Indicates whether the connection was allowed or blocked, depending on the configuration of 'External Devices Control' section of the profile, active on the device.

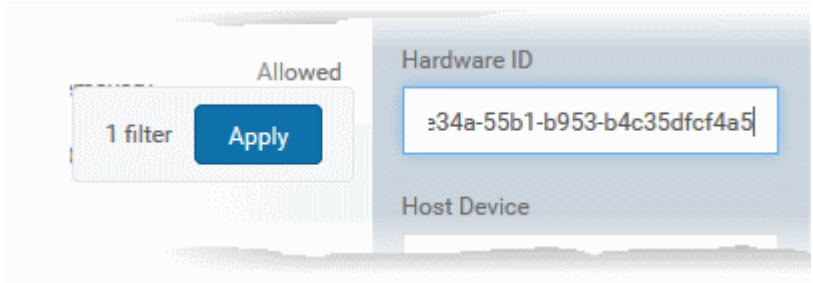
Sorting, Search and Filter Options

- Clicking on any of the 'Hardware Name', 'Hardware Class', 'Host Device' or 'Status' column headers sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific item based on the device name, GUID, Device ID and/or connected endpoint, enter the search criteria in the respective field and click 'Apply'.
- To filter the items based on the time at which connection attempt was made, enter the start and end dates of the period in the 'From' and 'To' fields under respective categories, using the calendars that appear on clicking inside the respective field and click 'Apply'.
- To filter the items or search for a specific item based on the allow/block status, choose the status from the

Status drop-down and click 'Apply'.



You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

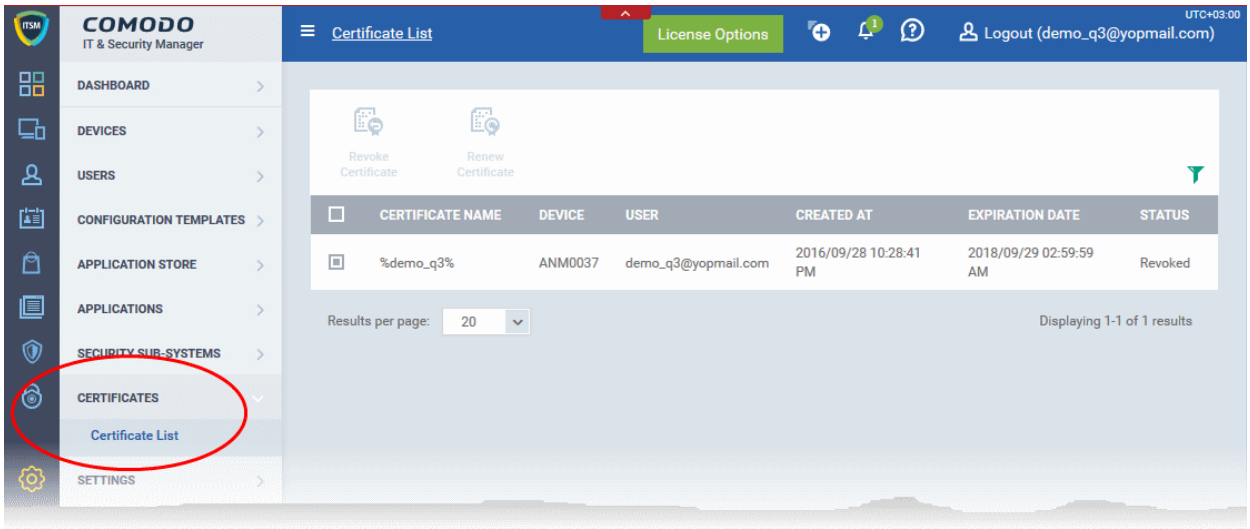
10. Managing Certificates Installed on Devices

The 'Certificate List' interface allows administrators to view client and device certificates acquired from Comodo Certificate Manager and installed on devices by ITSM. Administrators can also revoke certificates that are no longer required and renew certificates that are nearing expiry.

The Certificate List interface will be available only if you have integrated ITSM with your CCM account. For more details, refer to the section Integrating ITSM with Comodo Certificate Manager.

To open the 'Certificate List' interface

- Click 'Certificates' on the left and choose 'Certificate List'



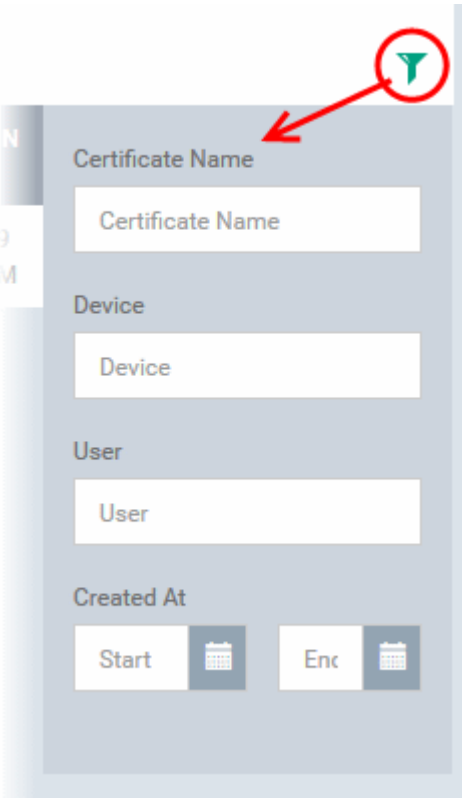
The list of certificates issued by CCM for users and devices through ITSM will be displayed.

Certificate List - Column Descriptions	
Column Header	**Description**
Certificate Name	The name for identifying the certificate

Device	The name of the device on which the certificate was installed
User	The name or email address of the user for whom the certificate was issued.
Created At	Displays the precise date and time at which the certificate request was created.
Expiration Date	The date and time at which the validity of the certificate expires
Status	Indicates whether the certificate is active, revoked or expired.

Sorting, Search and Filter Options

- Clicking on any of the 'Certificate Name', 'Device', 'User' or 'Created At' column headers sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button at the right end opens the filter options.



- To filter the items or search for a specific item based on the certificate name, device name or username, enter the search criteria in the respective field and click 'Apply'.
- To filter the items based on the period at which the certificate request was made, enter the start and end dates of the period in the 'From' and 'To' fields under respective categories, using the calendars that appear on clicking inside the respective field and click 'Apply'.

You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

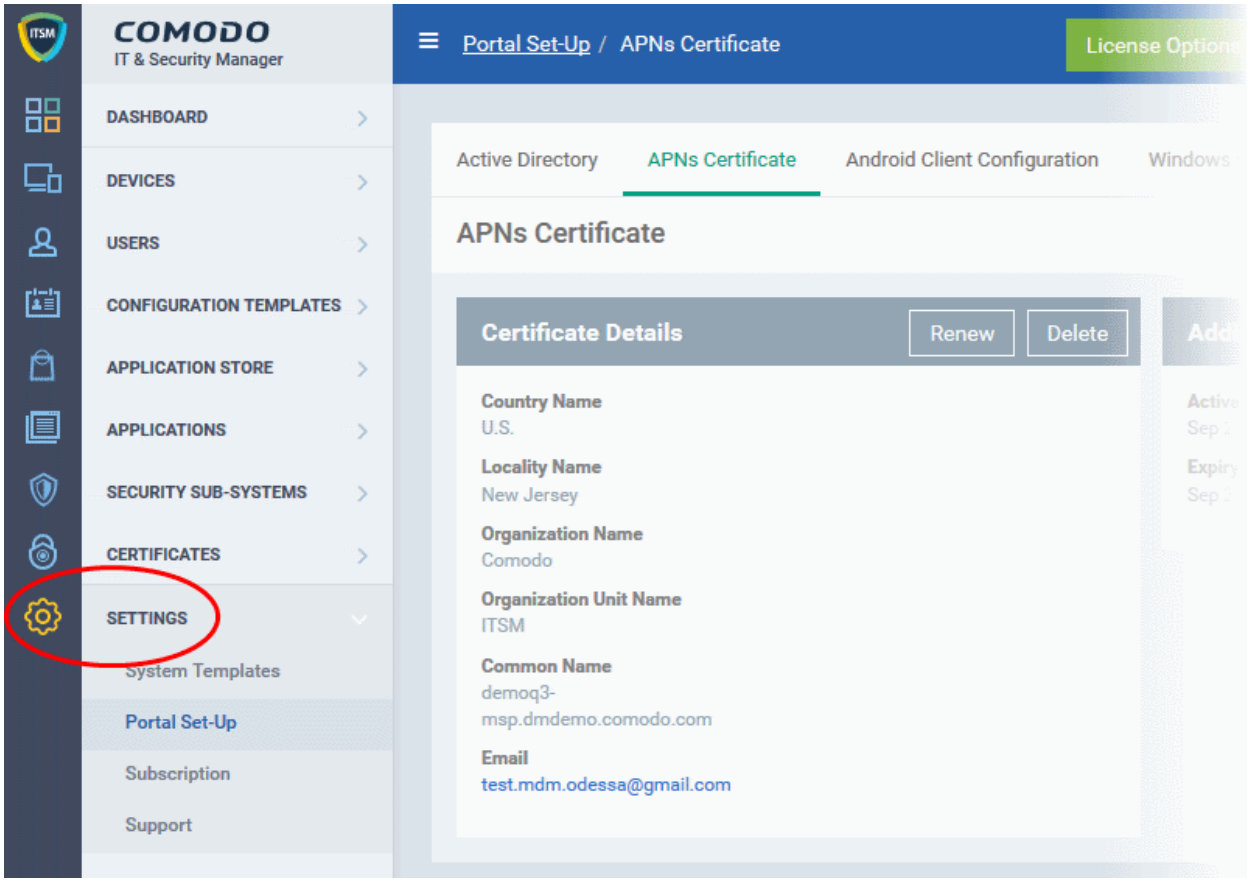
Managing Certificates

- To revoke an unwanted certificate, select it and click Revoke Certificate

- To renew an expired certificate, select it and click Renew Certificate.

11. Configuring Comodo IT and Security Manager

The 'Settings' tab allows administrators to configure email notifications, active directory, Google Cloud Messaging (GCM) and Apple Push Notification (APN) certificates, integration with Comodo Certificate Manager and more. Administrators can also manage subscriptions, renew/upgrade licenses and view support information from this interface.

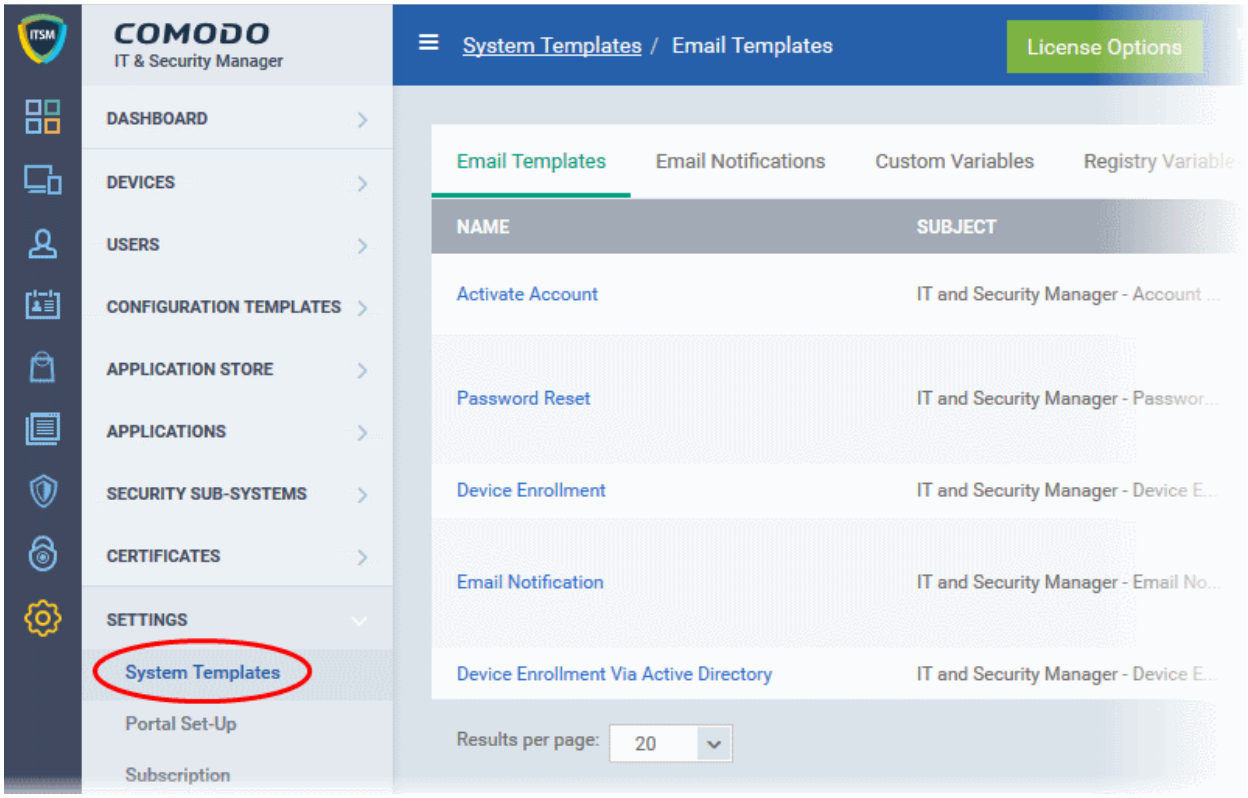


The following sections provide more details on each area:

- Email Notifications, Templates and Custom Variables
  - Configuring Email Templates
  - Configuring Email Notifications
  - Creating and Managing Custom Variables
  - Creating and Managing Registry Groups
  - Creating and Managing COM Groups
  - Creating and Managing File Groups
- ITSM Portal Configuration
  - Importing User Groups from LDAP
  - Adding Apple Push Notification Certificate
  - Configuring the ITSM Android Agent
    - Configuring General Settings

11.1. Email Notifications, Templates and Custom Variables

The 'System Templates' tab under 'Settings' allows administrators to manage email notifications, notification templates and to specify variables and file groups that can be used in various profile settings.



The following sections explain more about:

- Configuring Email Templates
- Configuring Email Notifications
- Creating and Managing Custom Variables
- Creating and Managing Registry Groups
- Creating and Managing COM Groups
- Creating and Managing File Groups

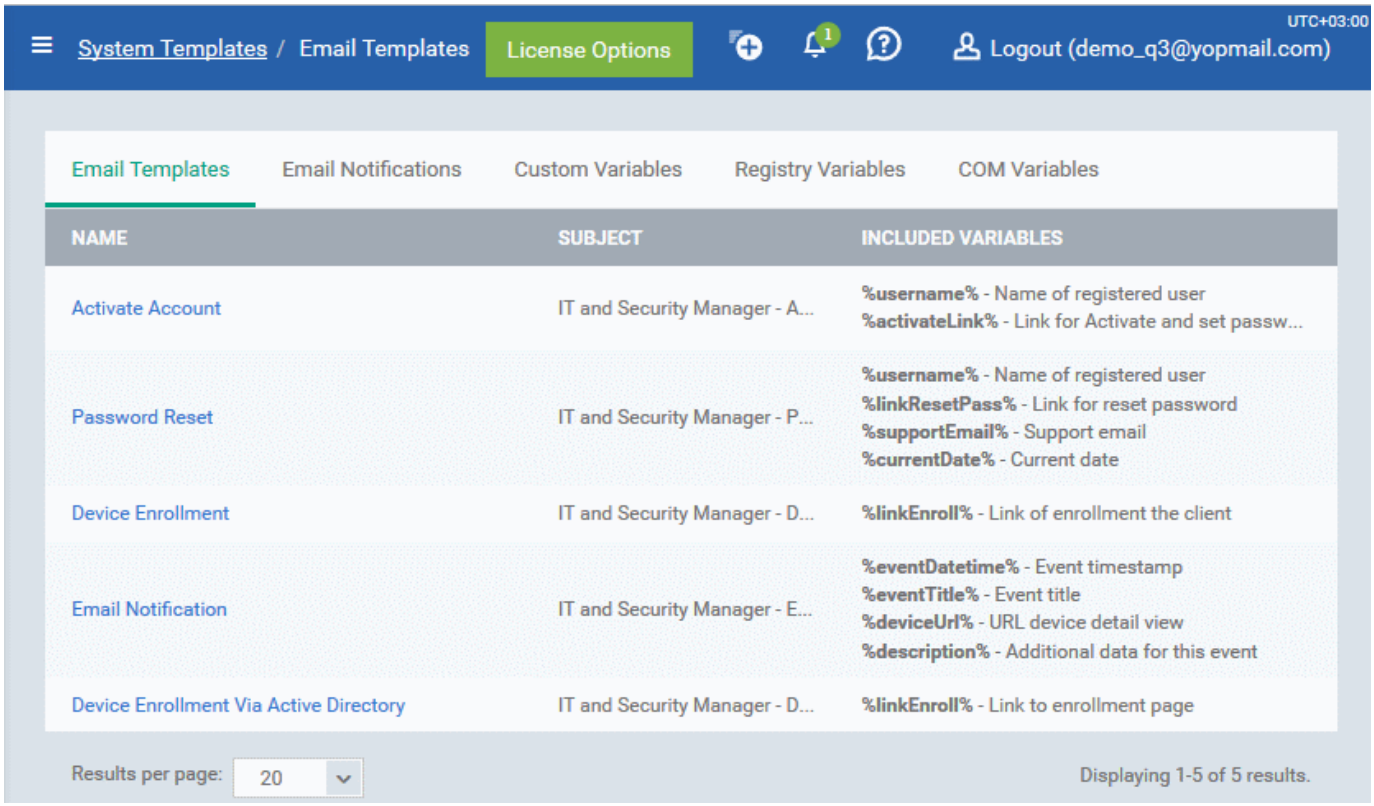
11.1.1. Configuring Email Templates

ITSM uses predefined templates to send automated mails to end-users for account activation, device enrollment,

password reset and so on. Administrators can customize these templates according to their requirements. For example, you can edit email subject and content, insert custom variables and more.

To view and manage email templates

- Click 'Settings' on the left and select 'System Templates'.
- Click the 'Email Templates' tab

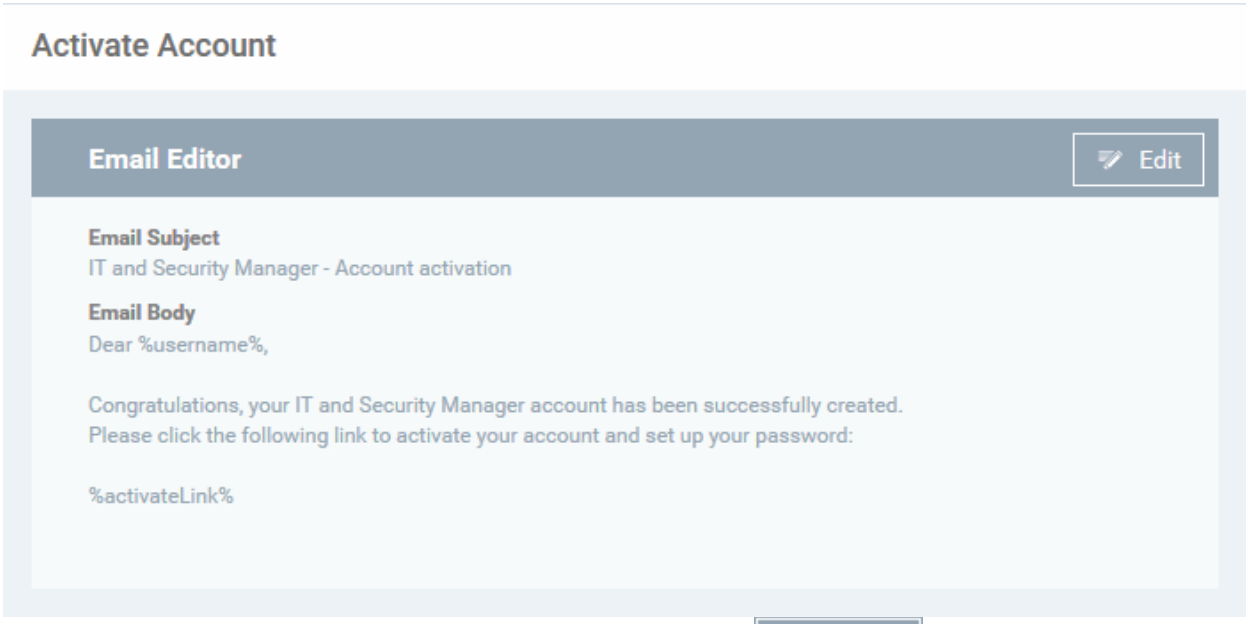


Email Templates- Column Descriptions	
Column Heading	**Description**
Name	Indicates the name of email template. This cannot be edited.
Subject	Displays the subject line of the email.
Included Variables	Displays the variables contained in the email, with their values. These cannot be edited.

To edit an email template

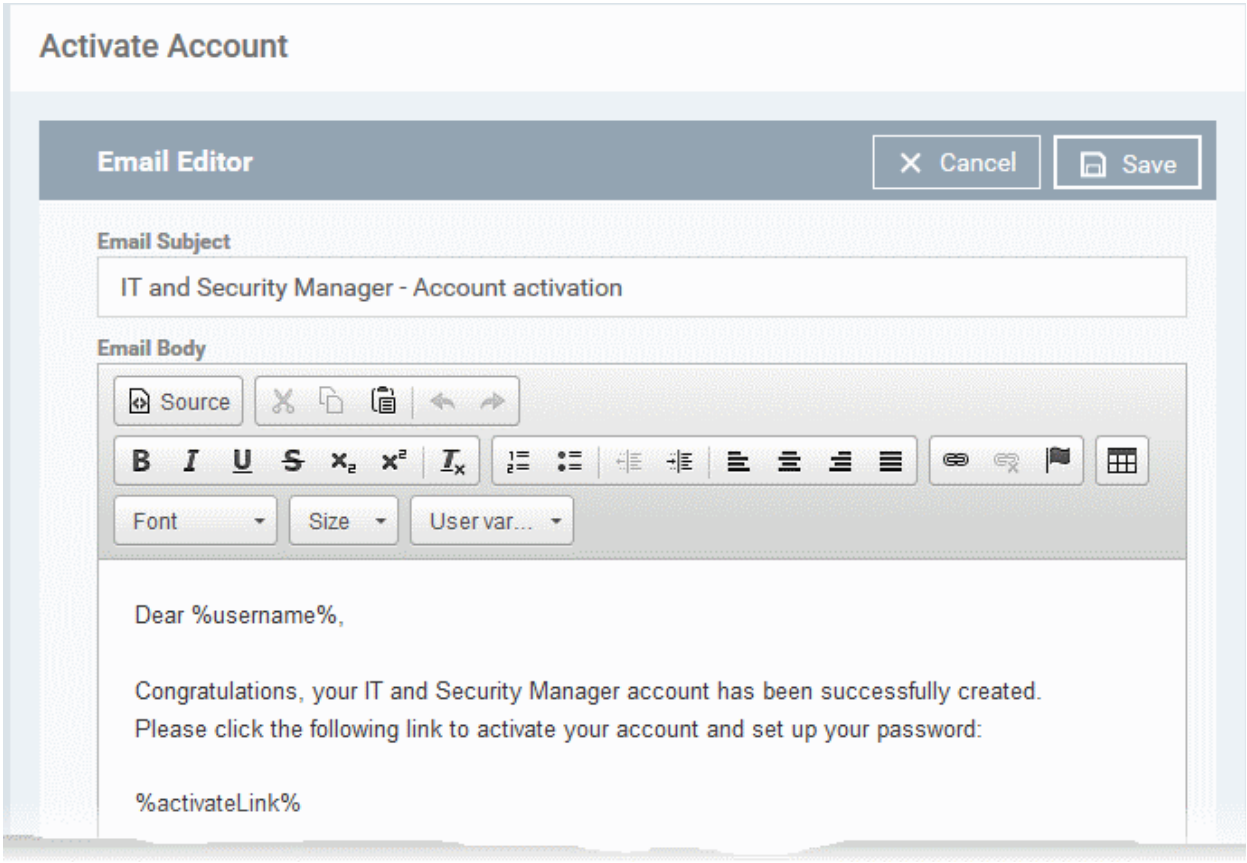
- Click 'Settings' on the left and select 'System Templates'.
- Click the 'Email Templates' tab
- Click on the type of email template under the 'Name' column that you want to edit.

The template editor of the respective email type will be displayed. For example, if you click the 'Activate Account' link, the following template editor will be displayed:



- To edit the subject line and the message, click the edit button  on the top right.

The 'Email Editor' window will open.



- Edit the subject line and email content of the template per your requirements and insert the variables available in the toolbar wherever required.

Note: For each type of email template, appropriate variables will be available in the toolbar. Make sure not to change the variable name as these will not work at all or fetch wrong values.

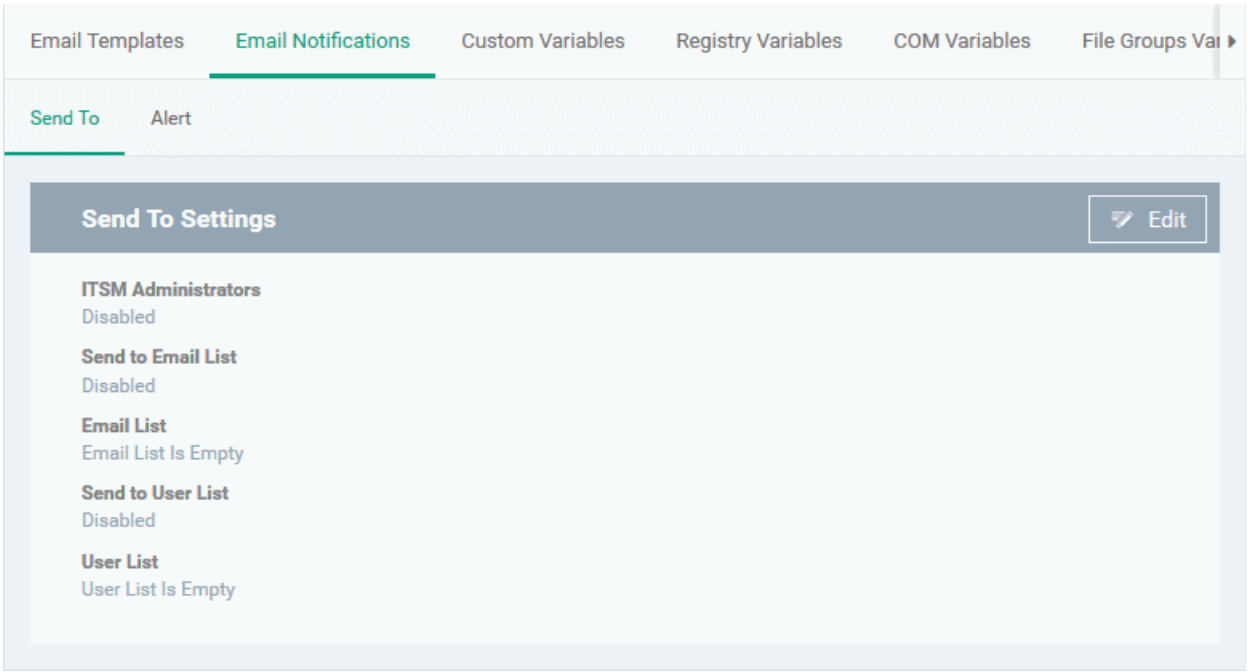
- Click the 'Save' button for your changes to take effect.

11.1.2. Configuring Email Notifications

ITSM can be configured to send alert emails to selected administrators and users on events like detection of a new infection and removal of iOS and Mac OS devices.

To configure email notifications

- Click 'Settings' on the left and select 'System Templates'.
- Click 'Email Notifications' at the top



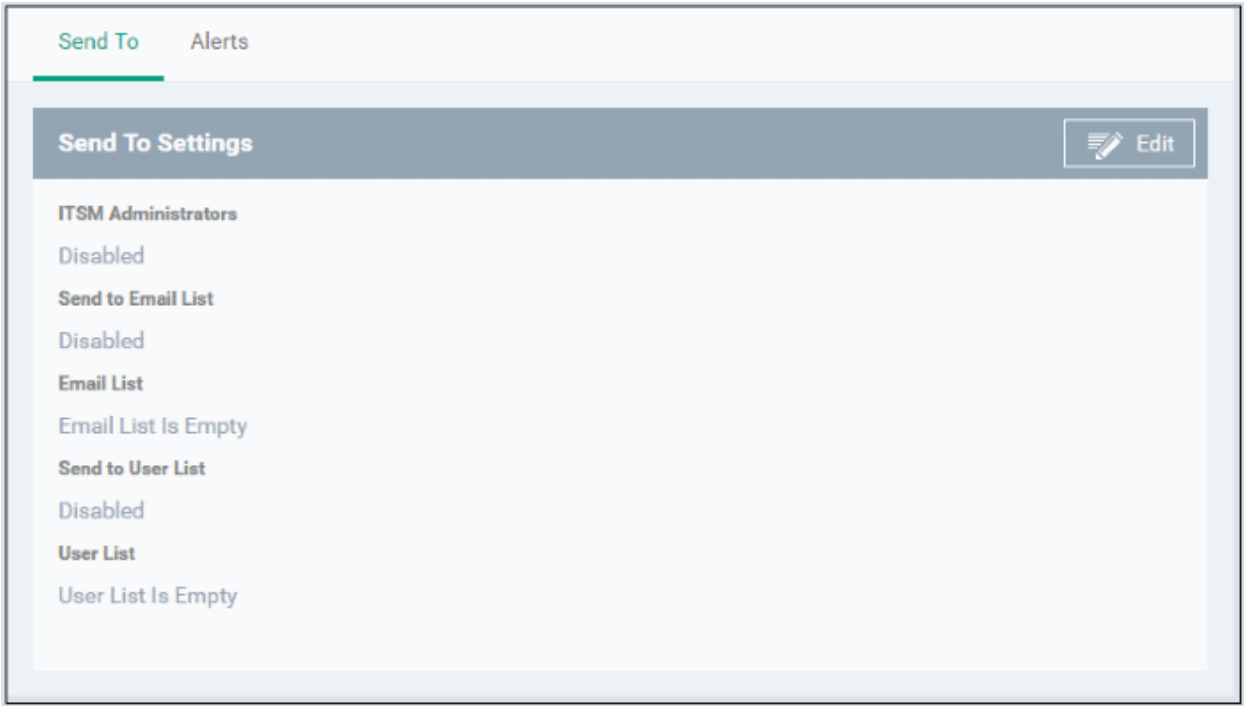
The interface contains two tabs.

- Send To - Allows to configure the alert recipients email addresses
- Alerts - Allows to configure the type of alert for which the email notifications will be sent

To configure email alert recipients

- Click 'Send To'

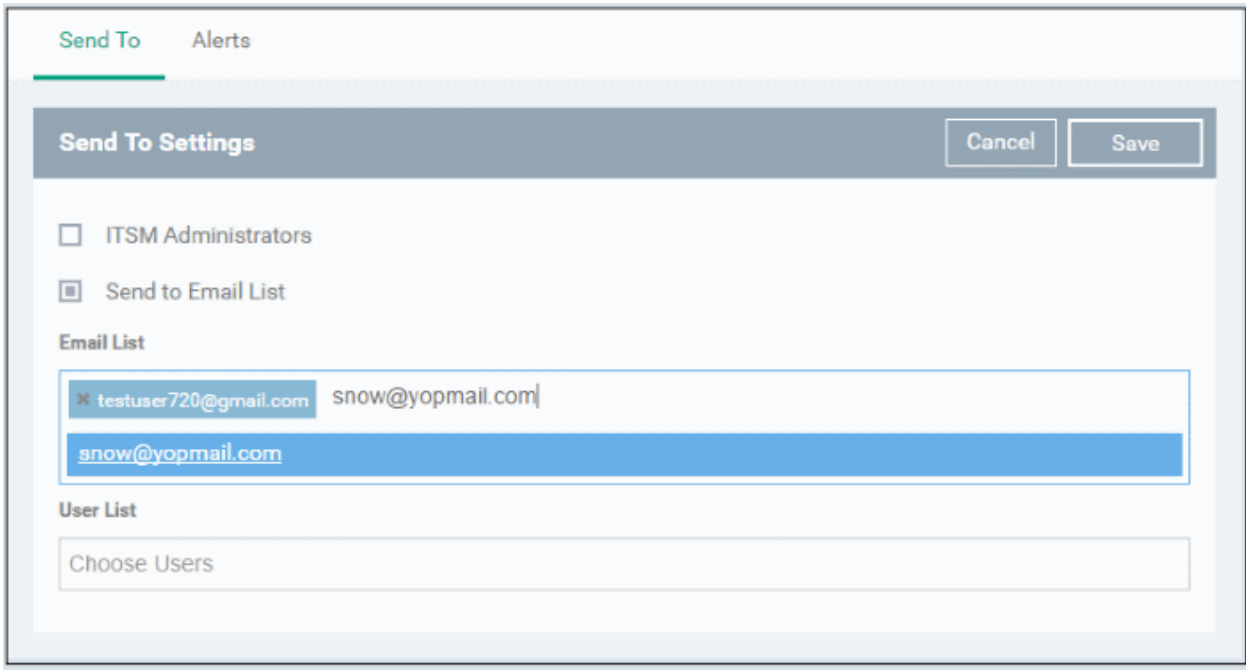
The 'Send to Settings' screen will be displayed.



- **ITSM Administrators** - If enabled, the alerts will be sent to all ITSM administrators
- **Send to Email List** - If enabled, the alerts will be sent to selected recipients whose addresses are added to the 'Emails List'
- **Emails List** - Displays the list of email addresses of recipients added to the 'Email List'.
- **Send to User List** - If enabled, the alerts will be sent the ITSM users that are added to the 'Users List'
- **User List** - Displays the list of users added to the 'User List'.

- Click the 'Edit' button at the top right to add new recipients and / or edit the current details

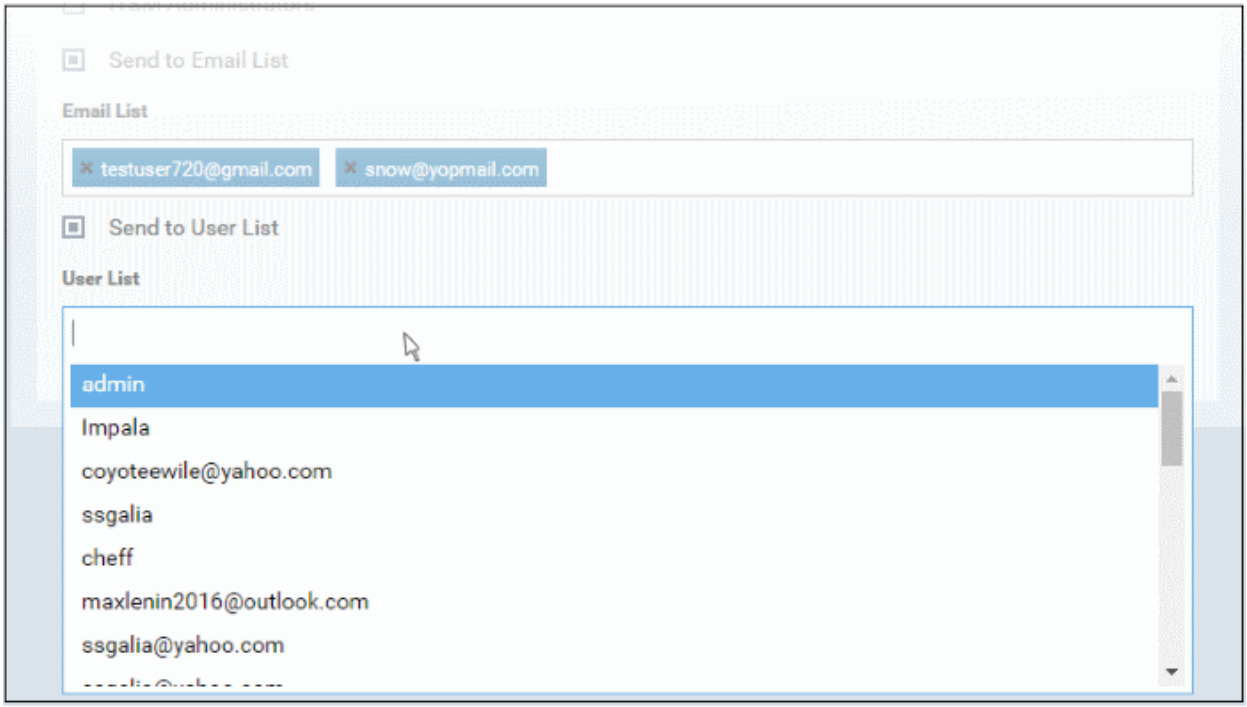
- To add recipients under 'Emails List', type the email address in the field and click the 'Enter' key or click the address that appear below the field.



Please note the check box(es) should be enabled for the alerts to be sent.

- To add ITSM users as recipients, click in the 'Users List' field

The available ITSM users will be listed.



- Select the users from the list

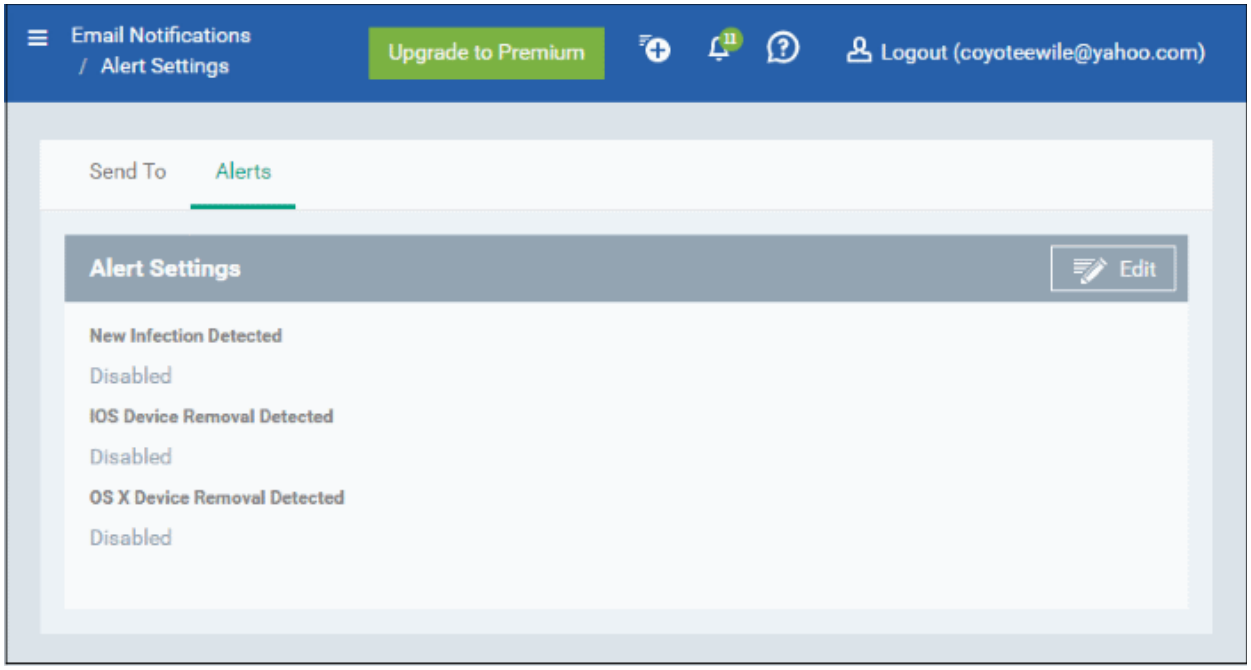
Please note the 'Send to Users List' check box should be enabled for the alerts to be sent to the users.

- Click the 'Save' button at the top right for your changes to take effect.

To configure alert settings

- Click 'Alerts'

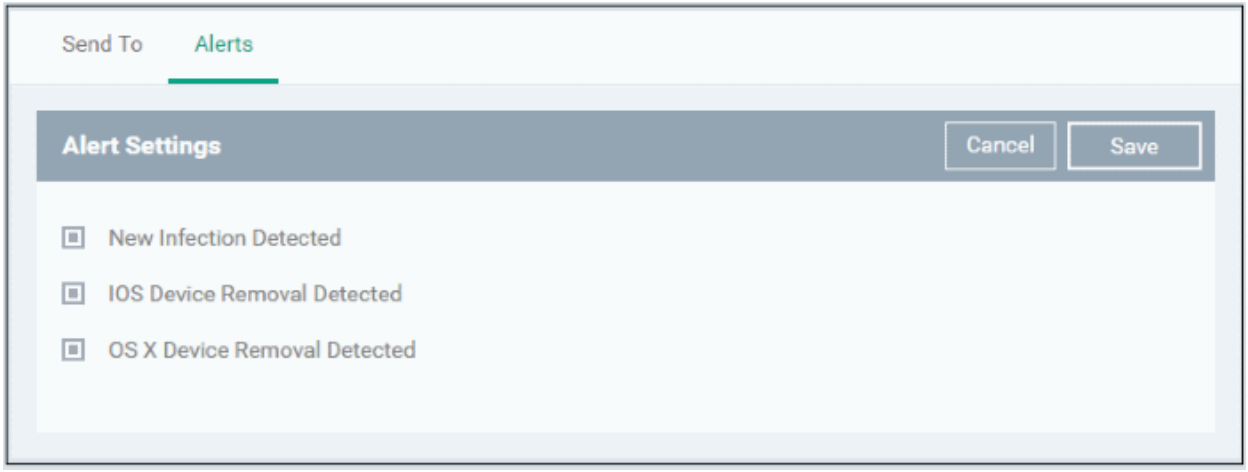
The 'Alert Settings' screen will be displayed.



The alerts interface allows you to select the events for which the alerts are sent.

- **New Infection Detected** - If enabled, an alert will be sent if a new malware is detected at an endpoint.
- **iOS Device Removal Detected** - If enabled, an alert will be sent if an iOS device is removed from ITSM
- **OS X Device Removal Detected** - If enabled, an alert will be sent if a Mac OS X device is removed from ITSM.

Click the 'Edit' button at the top right to enable/disable the type of alert.



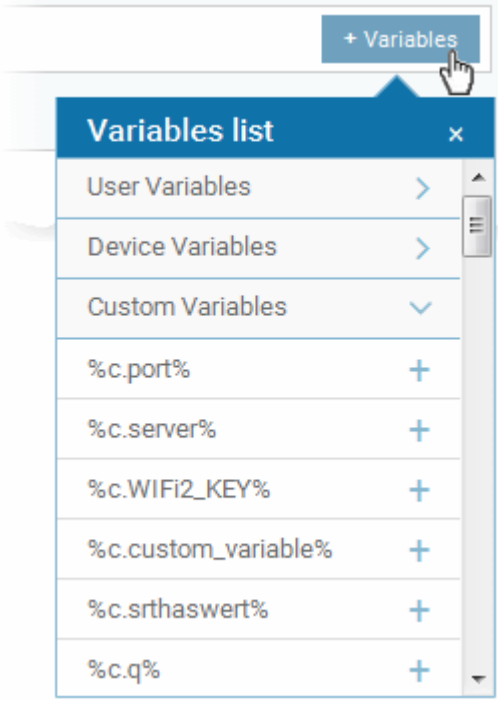
- Select / deselect the check boxes besides the alerts to enable / disable them
- Click the 'Save' button for the changes to take effect

11.1.3. Creating and Managing Custom Variables

ITSM is capable of fetching values for variables which have been defined for various settings and configuration profiles. There are three types of variables, ('User', 'Device' and 'Custom' variables), that can be used by the administrator to configure various settings.

When configuring various settings for a profile, the 'Variables' button 

will appear in fields which can have variables added. On clicking this button, a list of variables added to ITSM will appear. Choose the variable you wish to add:

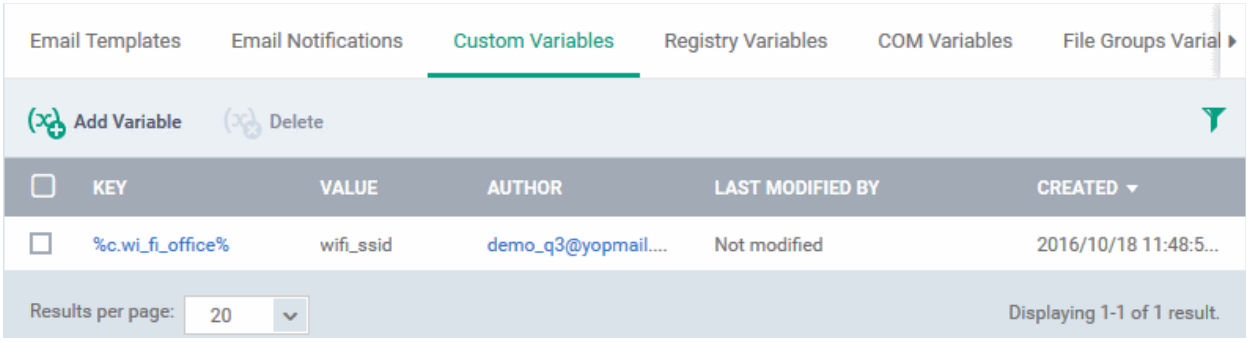


The first two, 'User Variables' and 'Device Variables', are hard coded and cannot be altered. These are useful for fetching the values of user and devices, for example user login details, email details from 'Users' > 'User List'. The last one, 'Custom Variables', can be created by administrators used in the configuration of various settings.

The custom variables can be added to ITSM from the 'Custom Variables' interface. These are useful for rolling changes across all profiles that have custom variables inserted. For example, if an administrator has provided a variable for an app in the AV scanning exclusion list in the Anti-virus settings of a profile and wants to change the app, he can just change the value in the custom variable screen. The changes will be rolled out to all profiles that has this custom variable.

To view the list of custom variables, add new variables and manage them

- Choose 'Settings' on the left and select 'System Templates'
- Click the 'Custom Variables' tab from the top of the interface

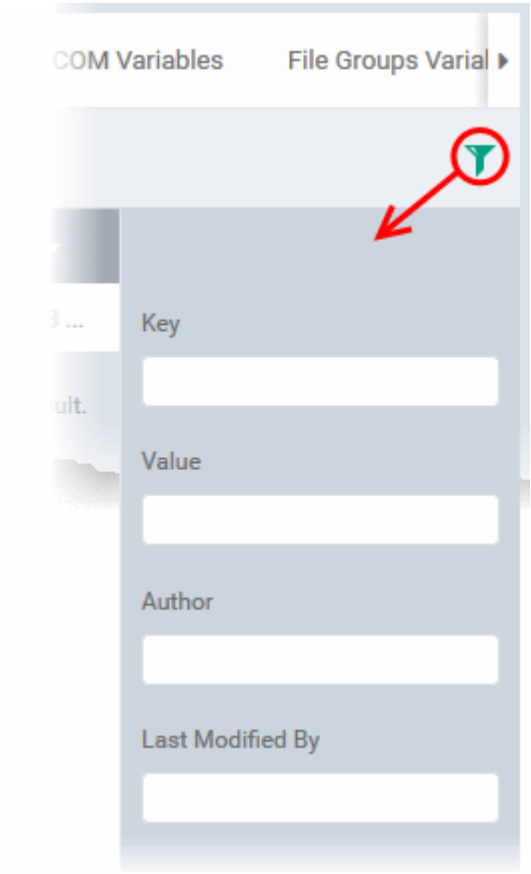


Custom Variables - Column Descriptions	
Column Heading	**Description**
Key	Displays the name of key for the value in the next column. Clicking the key will open the 'Update Custom Variable' interface that allows you to edit the value for the key.
Value	Displays the value for the key

Author	Displays the name of administrator that created the custom variable. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the user. Refer to the section Viewing the details of a User for more details.
Last Modified By	Displays the name of the user that last modified the custom variable.
Created	Displays the date and time at which the custom variable was created.

Sorting, Search and Filter Options

- Clicking on any of the column headers will sort the items in ascending/descending order of entries in that column
- Click the funnel icon to search for custom variables based on filter parameters



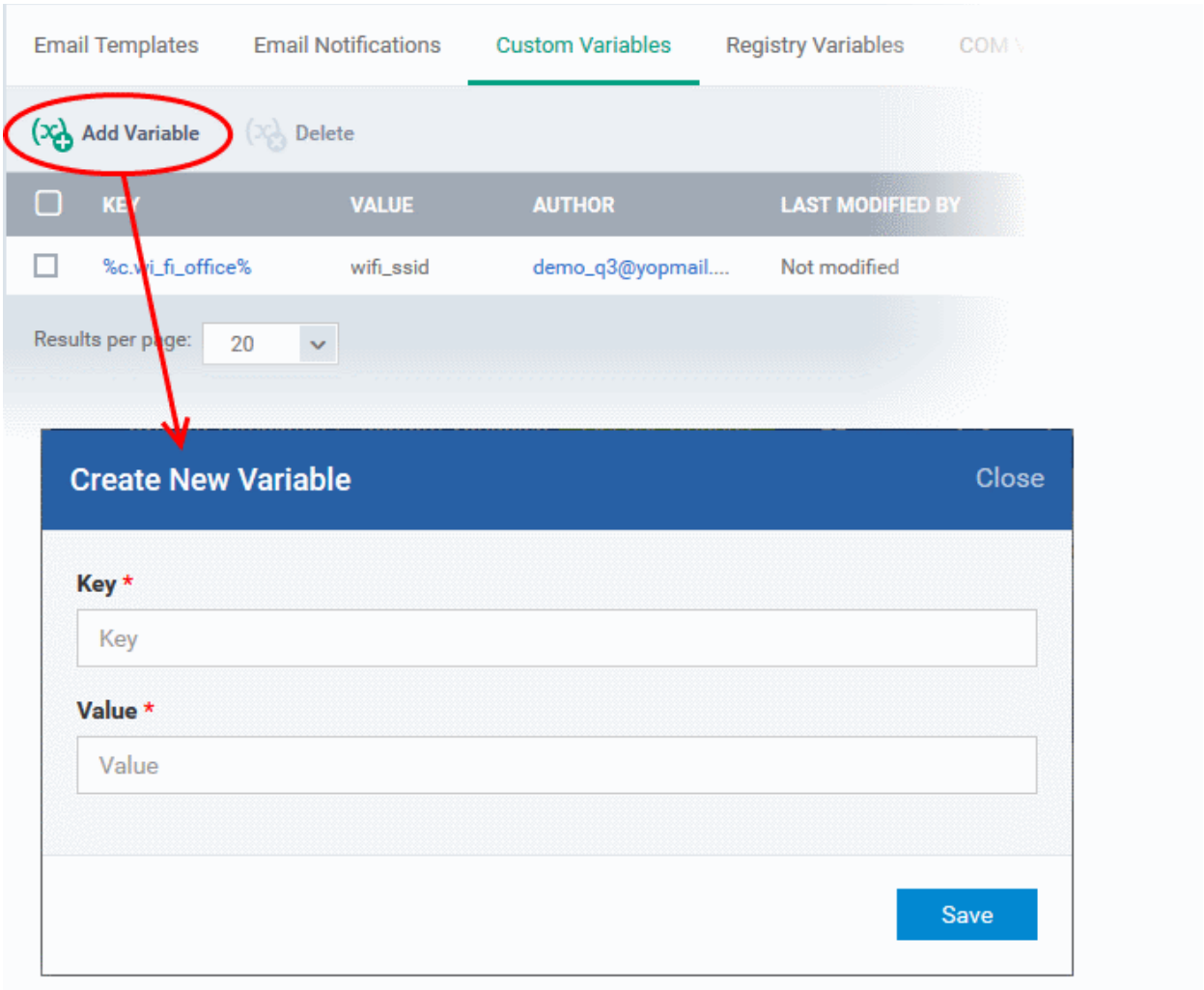
- To display variables which are based on 'Key', 'Value', 'Author' and 'Last Modified By', enter the text partially or fully in the respective fields and click the 'Apply' button.

The custom variables that matches the entered parameters will be displayed in the screen.

- To display all the variables again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the filter option

To create a new Custom Variable

- Click the 'Settings' from the left, choose 'System Templates' and click on 'Custom Variables' tab
- Click 'Add Variable'



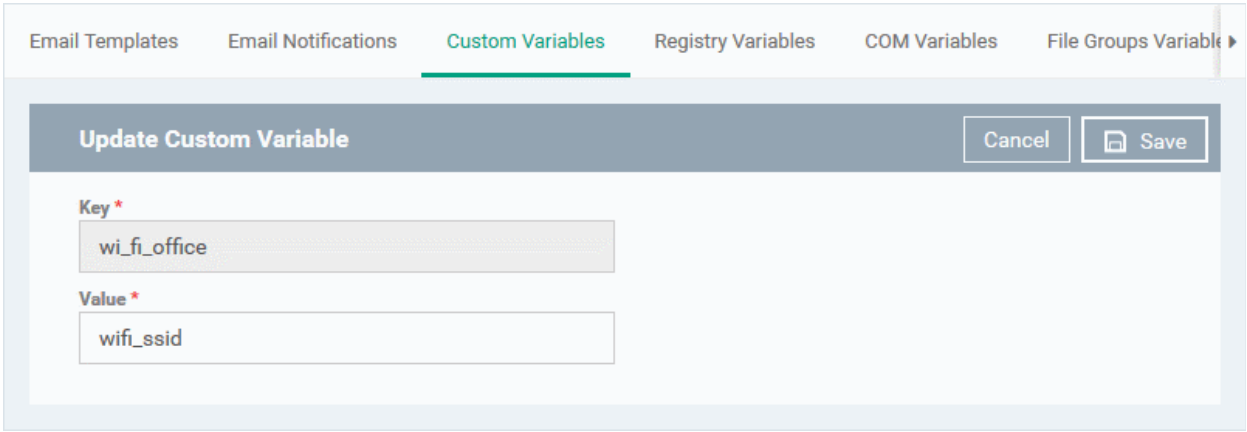
- In the 'Create New Variable' dialog enter a variable name in the 'Key' text box.
- In the 'Value' text field, enter the value for the variable.
- Click 'Save' to add the variable to ITSM.

The variable will be added and listed in the screen.

To edit a Custom Variable

- Click on the name of the 'Custom Variable' to be edited.

The 'Update Custom Variable' screen will appear.



- Edit the 'Key' and 'Value' as required and click the 'Save' button.

To remove a Custom Variable

- Select the custom variable to be removed from the list and click the 'Delete' button at the top

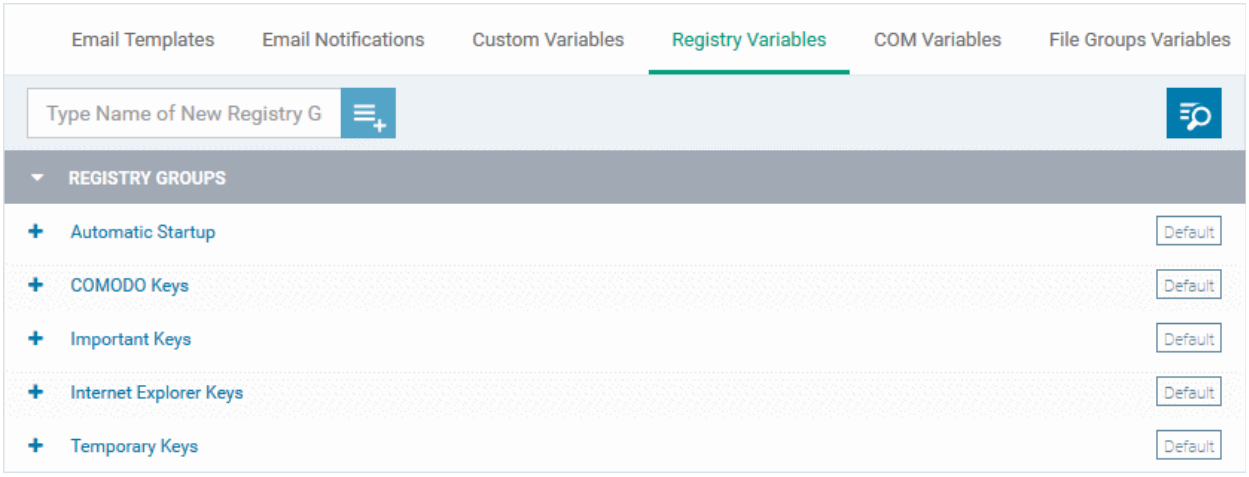
11.1.4. Creating and Managing Registry Groups

Each Registry group is a predefined batch of one or more registry keys and values that fall under a specific category. ITSM ships with a set of predefined Registry Groups that are available for use in configuration profiles, for example. to specify a group as an exclusion to containment rules when configuring 'Containment Settings' in a Windows profile. If required, administrators can add new groups and edit existing groups.

The 'Registry Variables' tab in the 'System Templates' interface allows administrators to view, create and manage pre-defined and custom Registry groups. The groups added to this interface will be available for selection while configuring Windows Profiles from the 'Profiles' interface.

To open the 'Registry Groups' interface

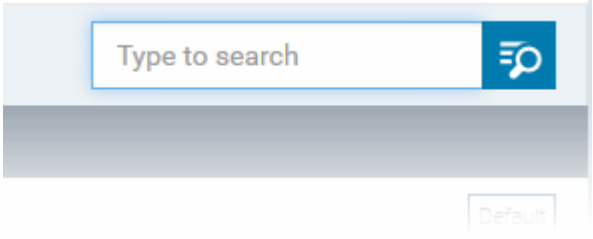
- Click 'Settings' from the left and select 'System Templates'
- Click 'Registry Variables' from the top



The list of default and user-defined Registry groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

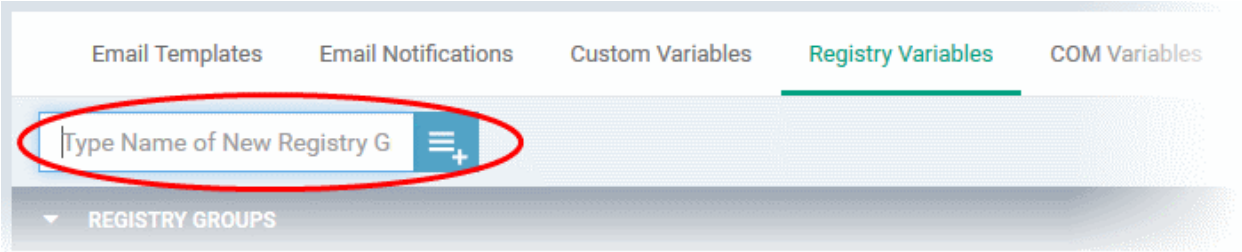
Sorting, Search and Filter Options

- Clicking on the 'Registry Groups' column header will sort the items in ascending/descending order of the names of the Registry groups.
- To filter or search for a specific Registry group, click the search icon at the top right and enter the name of the group on part or full



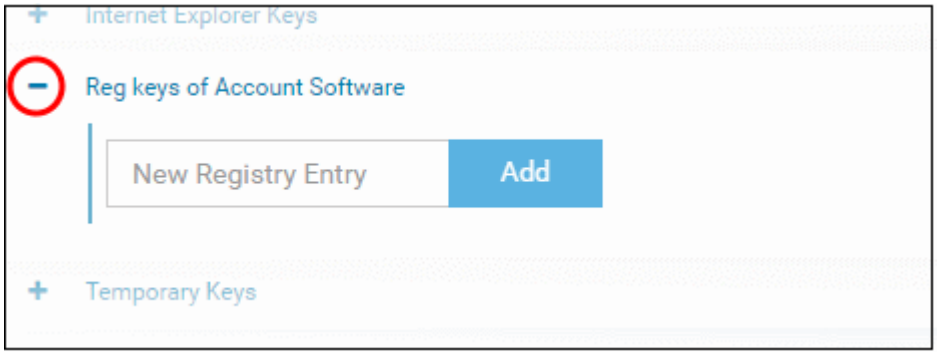
To add a new Registry group

- Enter the name of the new Registry Group in the New Registry Group field and click the '+' button.

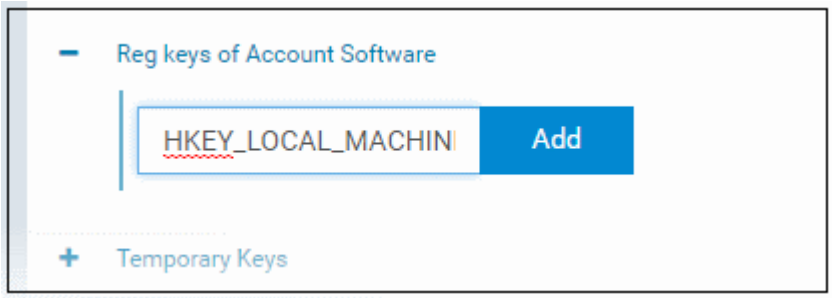


The new group will be added to the list. The next step is to add the Registry keys to the group.

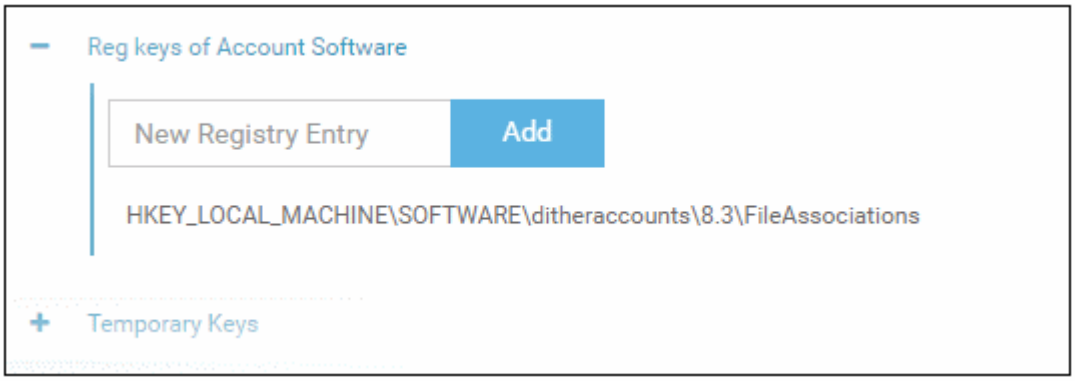
- Click the '+' at the left of the group name



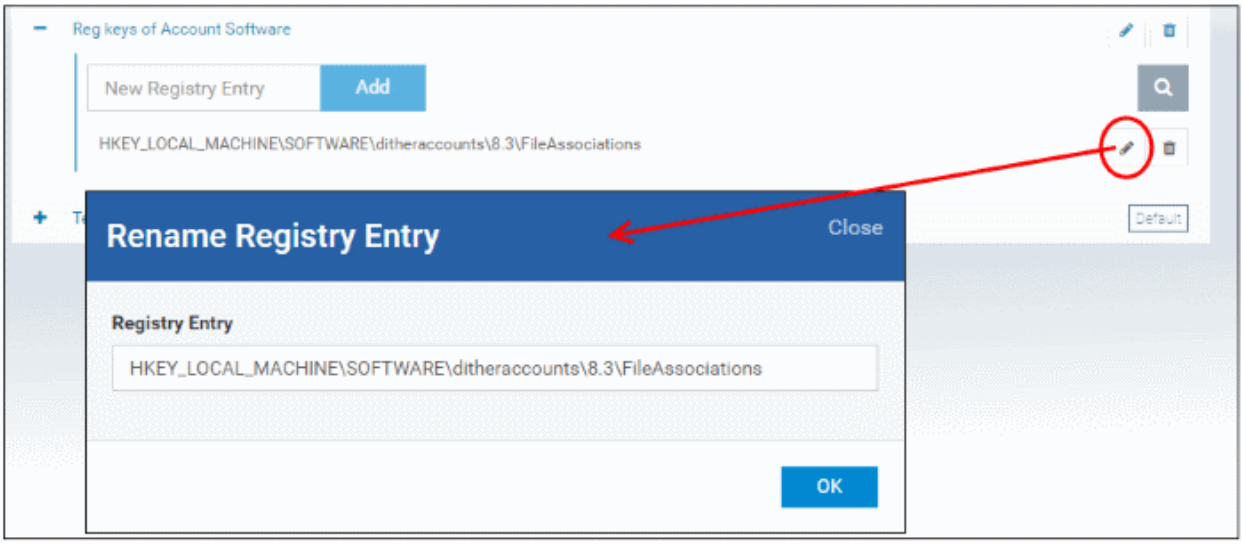
- Enter the path of the registry key/value in the New Registry Entry field and click 'Add'



The key will be added to the group.



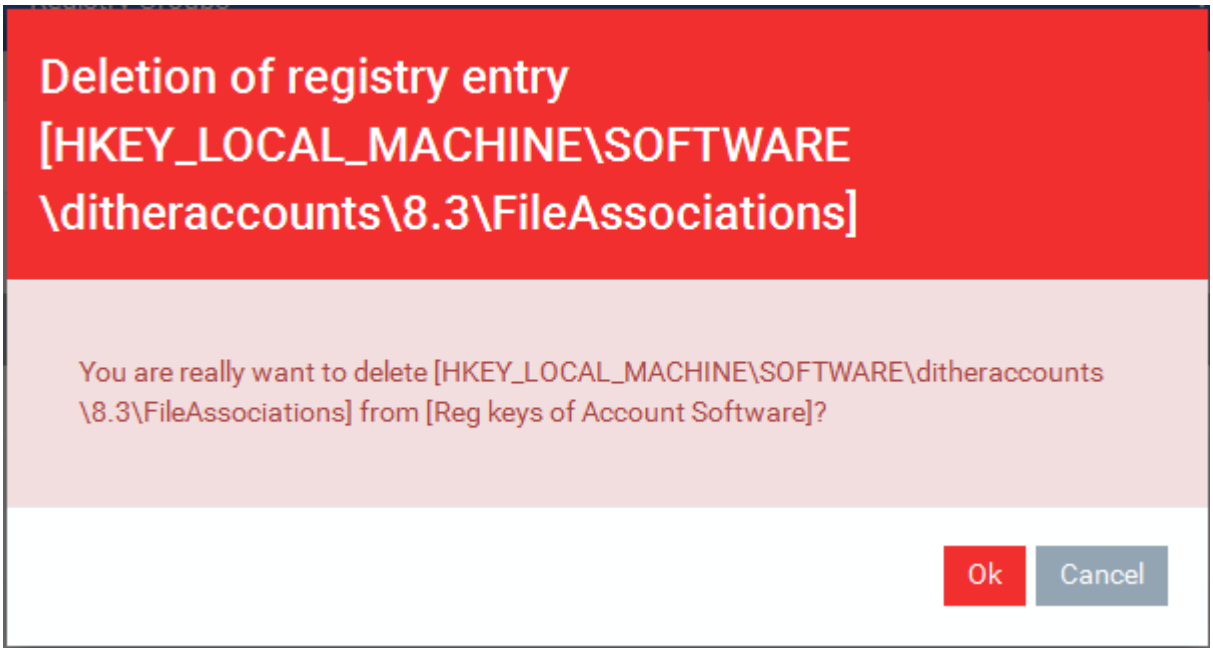
- Repeat the process to add more Registry keys and values to the group.
- To edit the key/value in the group, click the 'Edit' icon beside the key name.



- Edit the entry and click 'OK' to save your changes

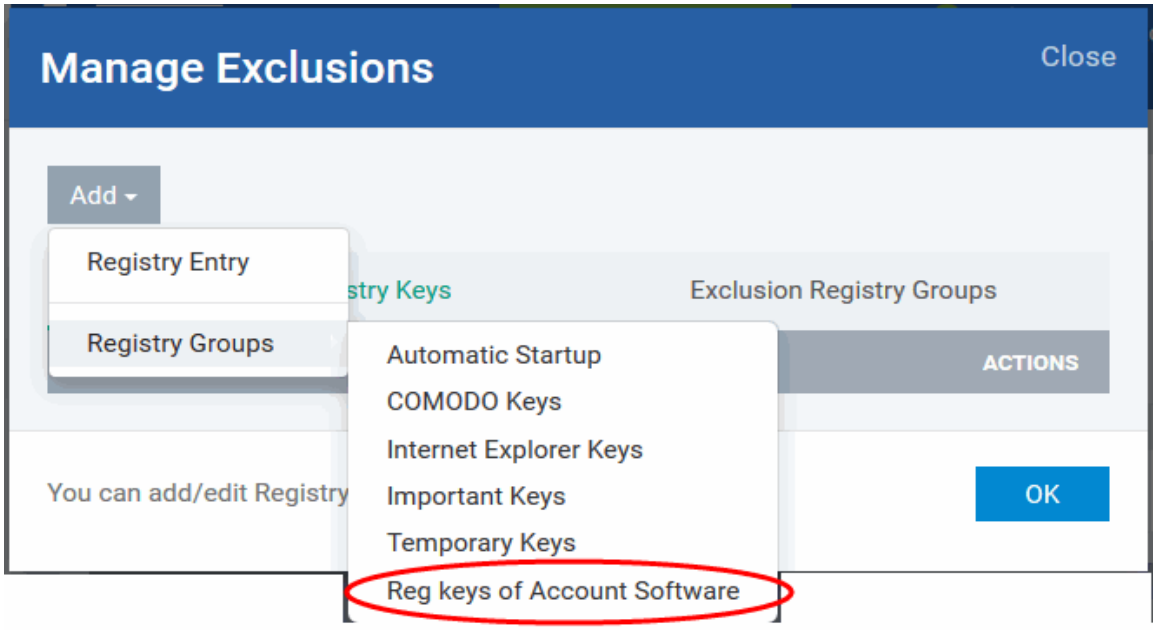
- To remove the key added by mistake or an unwanted key from the group, click the trash can icon beside the key name.

A confirmation dialog will appear.



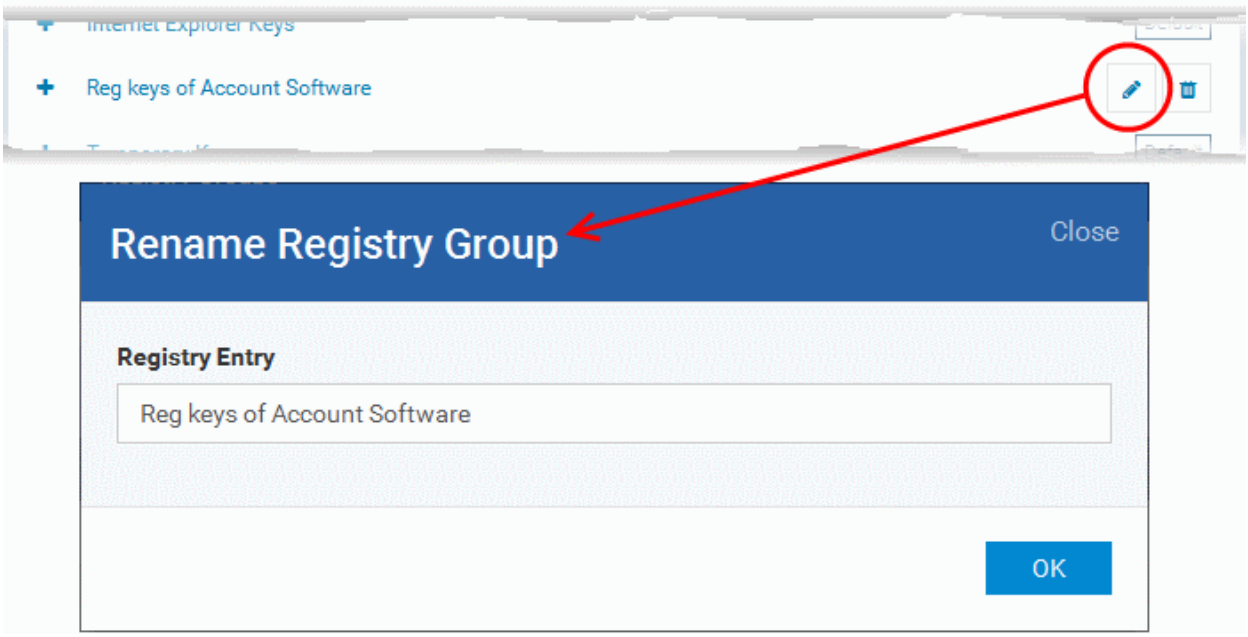
- Click 'OK' in the confirmation dialog.

Once a registry group is added, it will be available for selection while configuring Windows Profiles, for example in the 'Containment' > 'Registry Key Exclusions' .



To edit the name of a Registry Group

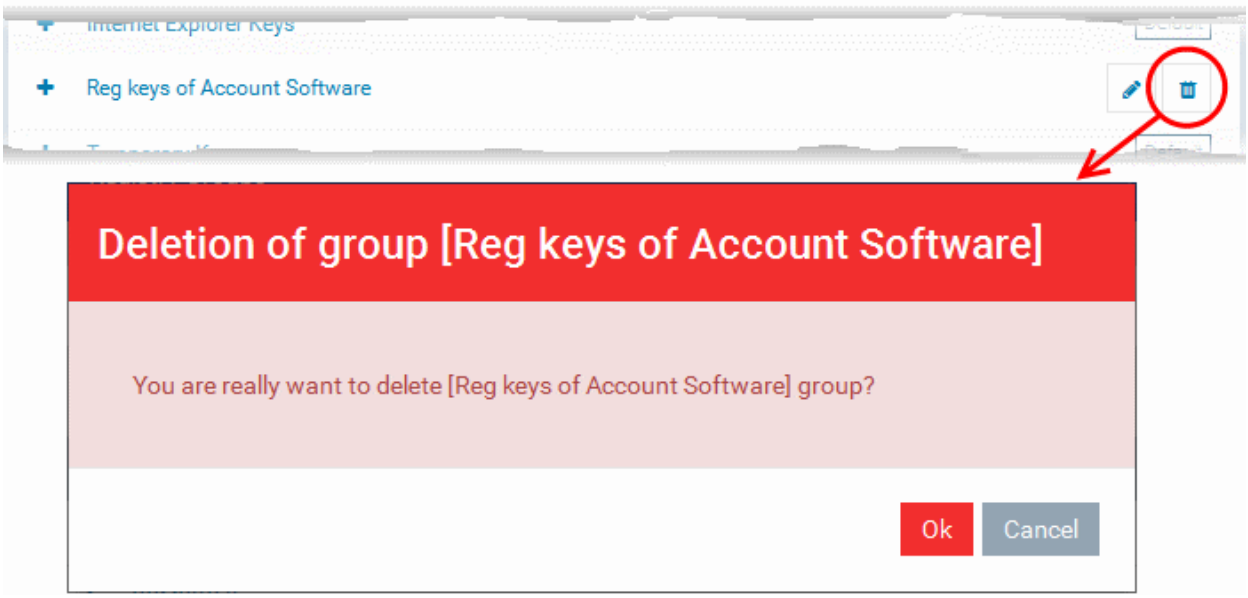
- Click the 'Edit' icon beside the Registry Group



- Enter the new name for the group in the Rename Registry Group dialog and click 'OK'

To remove a Registry Group

- Click the Trash can icon beside the Registry Group



A confirmation dialog will appear.

- Click OK in the confirmation dialog.

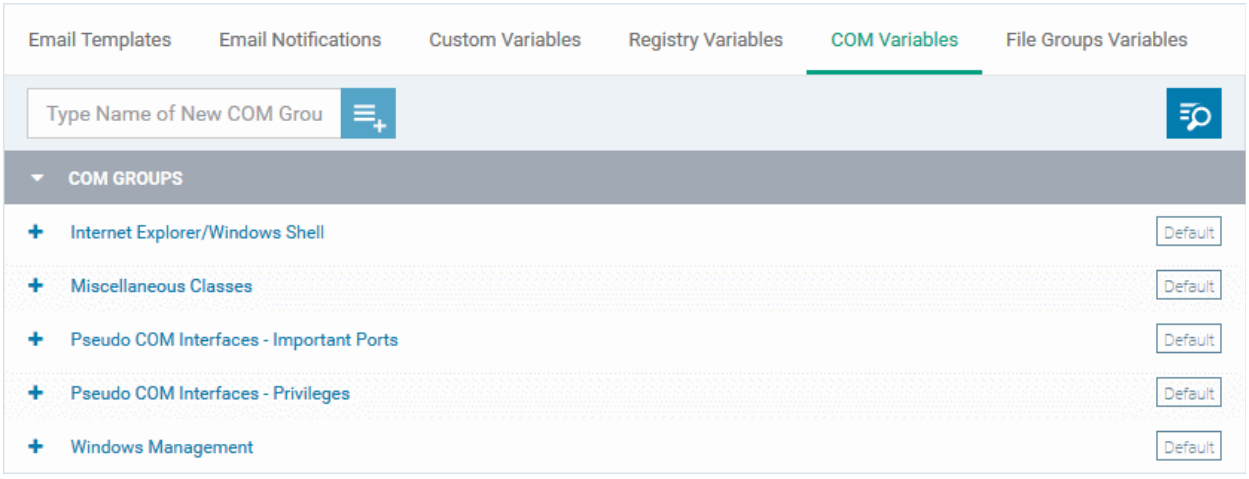
11.1.5. Creating and Managing COM Groups

Each COM group is a handy collection of COM interfaces falling under a certain category. ITSM ships with a set of predefined COM Groups that are available for use in configuration profiles, for example to add a COM group to the 'Protected Objects' list in the HIPS settings of a Windows profile. If required, administrators can add new COM Groups, edit and manage them.

The COM Variables tab in the 'System Templates' interface allows administrators to view and manage pre-defined and custom COM groups. The groups added to this interface will be available for selection while configuring Windows Profiles from the 'Profiles' interface.

To open the 'COM Groups' interface

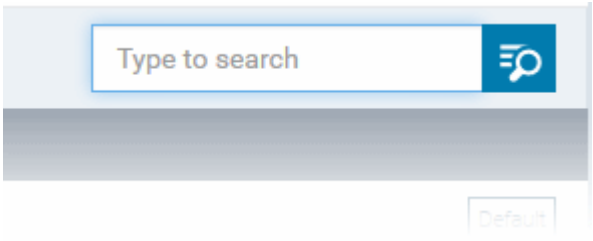
- Click 'Settings' on the left and select 'System Templates'
- Click 'COM Variables' from the top



The list of pre-defined and user-defined COM groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

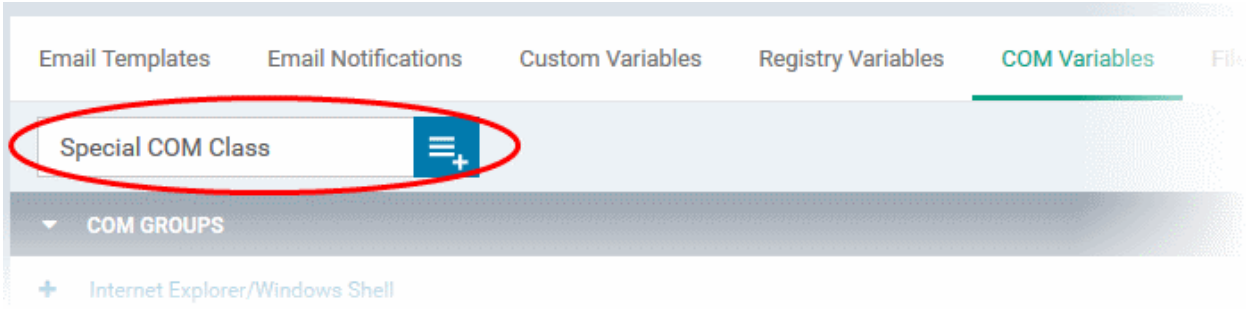
Sorting, Search and Filter Options

- Clicking on the 'COM Groups' column header will sort the items in ascending/descending order of the names of the groups.
- To filter or search for a specific COM group, click the search icon at the top right and enter the name of the group on part or full



To add a new COM group

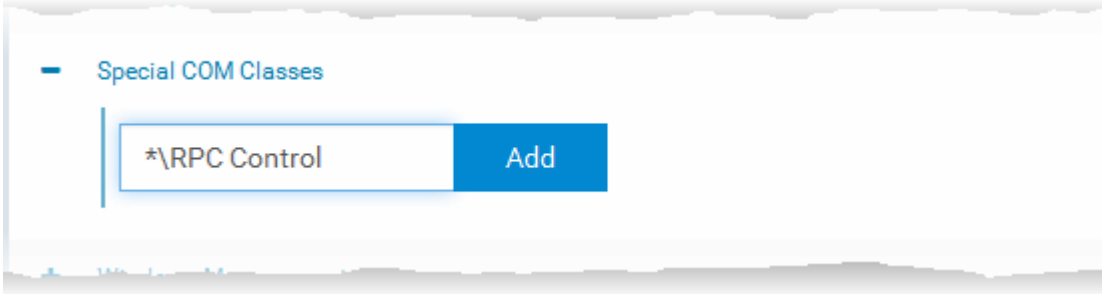
- Enter the name of the new COM Group in the 'Type Name of New COM Group' field and click the '+ ' button.



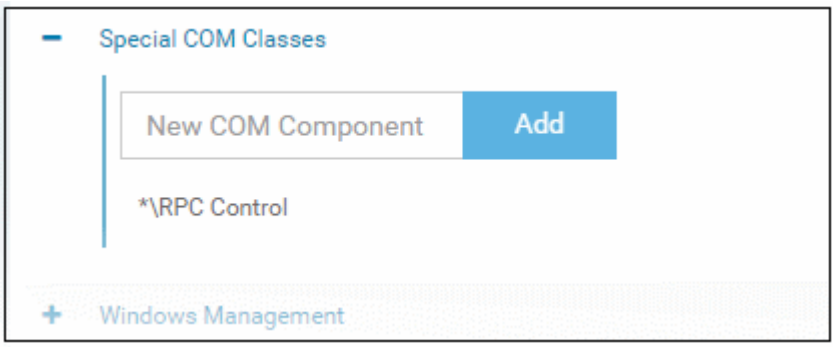
The new group will be added to the list. The next step is to add COM classes to the group.

- Click the '+' at the left of the group name

- Enter the COM classes to be added to the group, in the 'New COM Component' field and click 'Add'

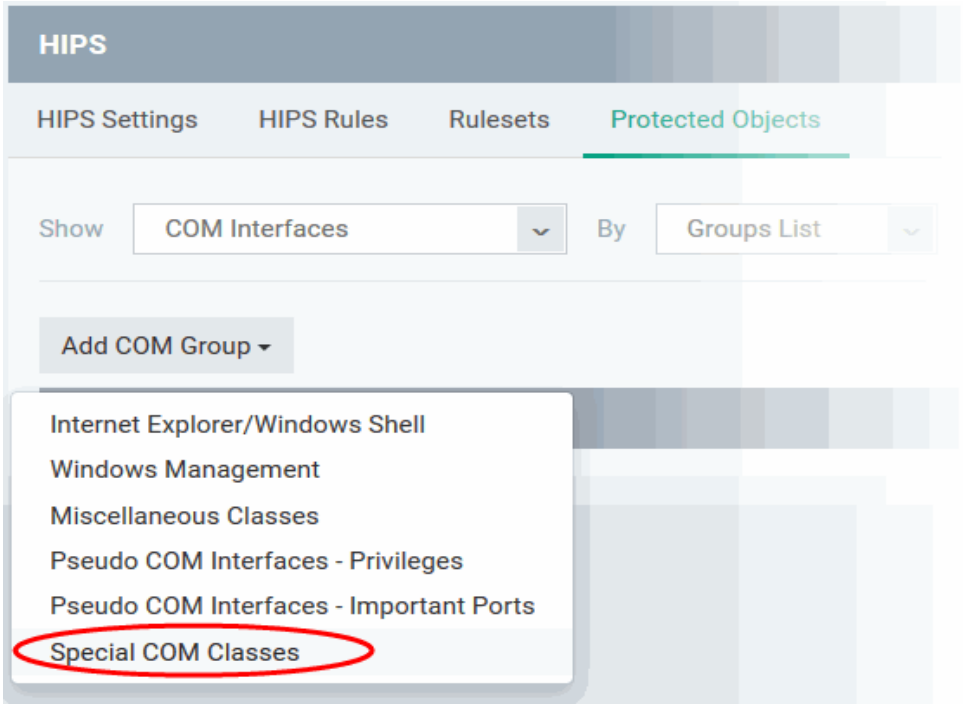


The COM class will be added to the group.

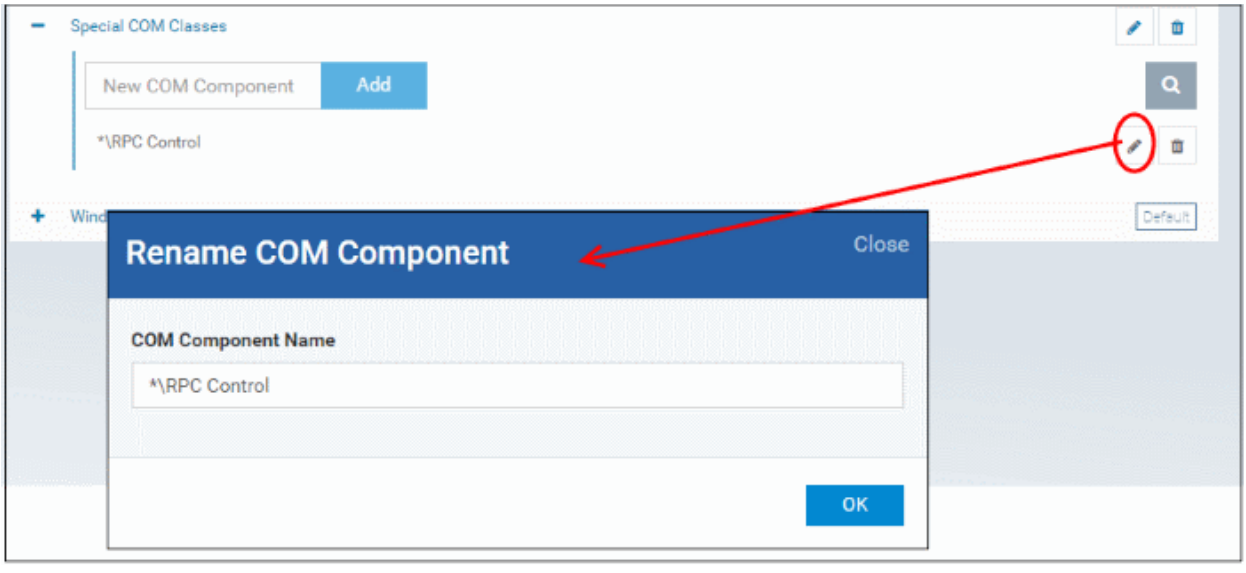


- Repeat the process to add more COM classes to the group.

Once a COM group is added, it will be available for selection while configuring a Windows Profile, for example in the 'HIPS' > 'Protected Objects' > 'Groups List' interface.



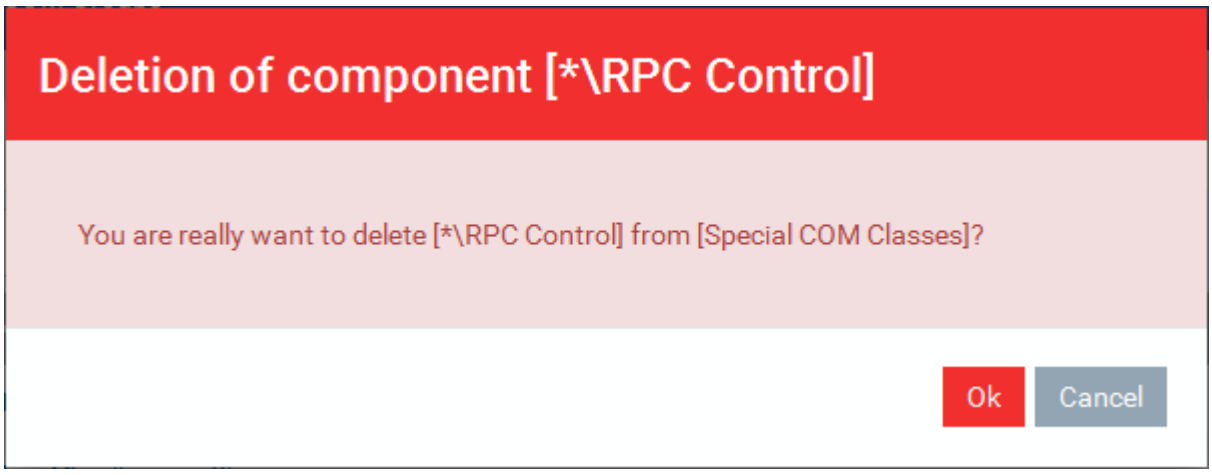
- To edit ta class in the group, click the 'Edit' icon beside the class name.



- Edit the entry and click 'OK' to save your changes

- To remove the COM class added by mistake or an unwanted class from the group, click the trash can icon beside the COM component name.

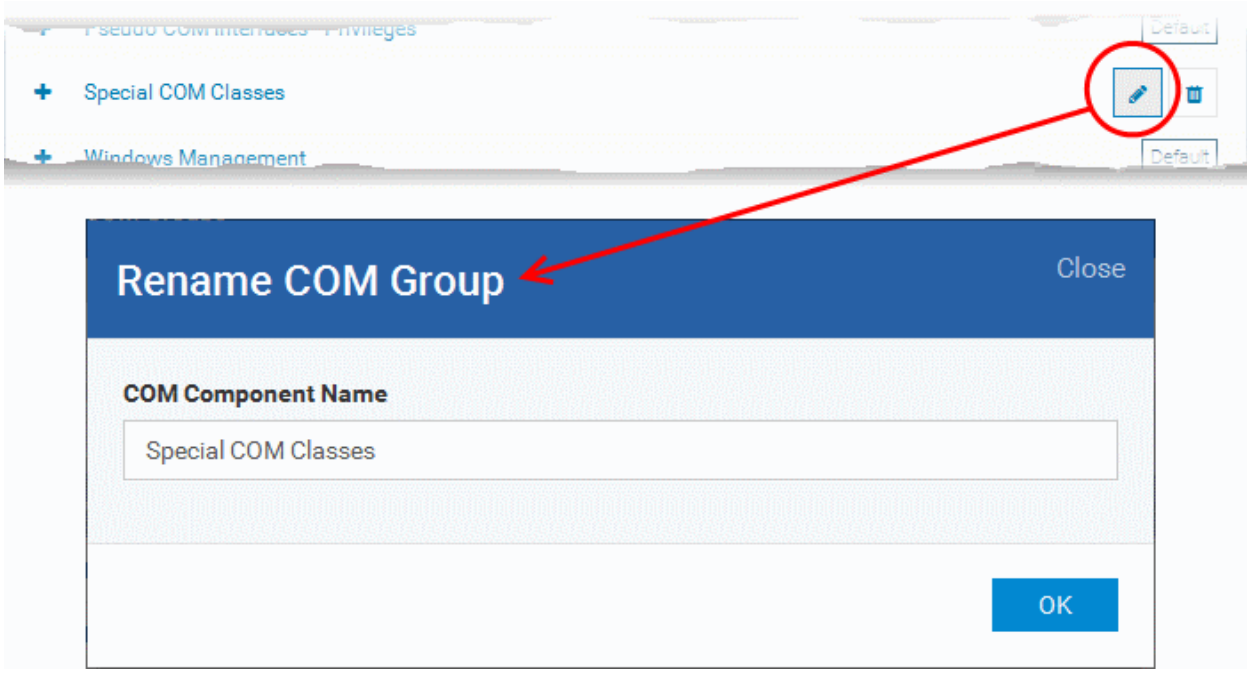
A confirmation dialog will appear.



- Click 'OK' in the confirmation dialog.

To edit the name of a COM Group

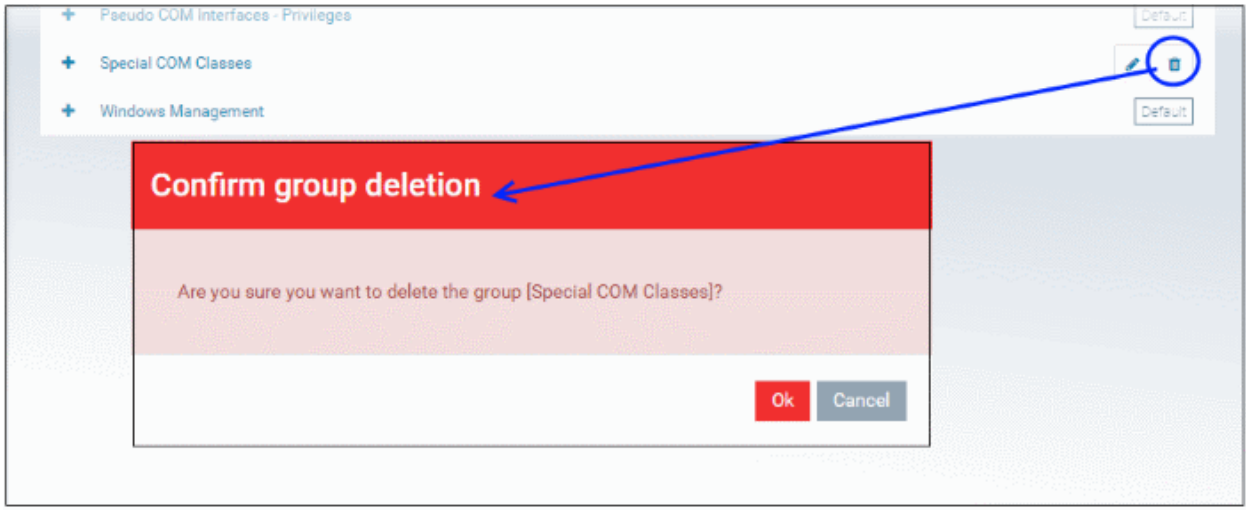
- Click the 'Edit' icon beside the COM Group



- Enter the new name for the group in the Rename COM Group dialog and click 'OK'

To remove a COM Group

- Click the Trash can icon beside the COM Group



A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

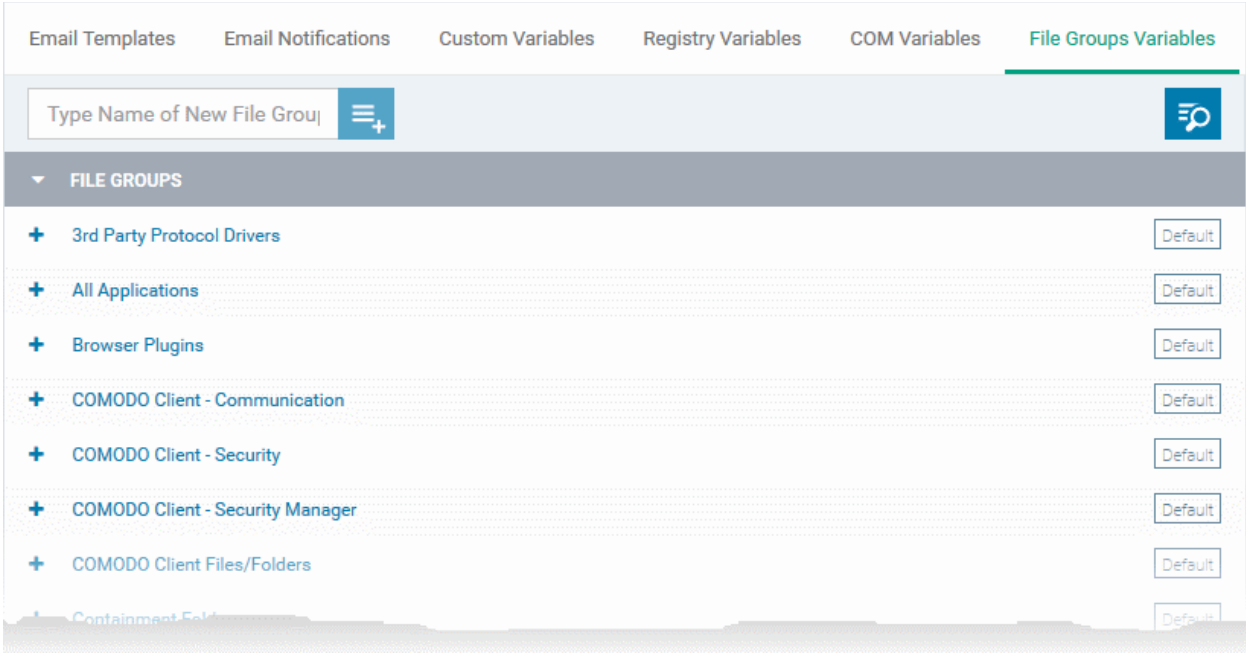
11.1.6. Creating and Managing File Groups

File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various functions such as adding them to Exclusions for AV scans, HIPS monitoring, auto-containment rules and so on in Windows Profiles. ITSM ships with a set of predefined File Groups and if required administrators can add new File Groups, edit and manage them.

The 'File Group Variables' tab in the 'System Templates' interface allows administrators to view, create and manage pre-defined and custom file groups. The groups added to this interface will be available for selection while configuring Windows Profiles from the 'Profiles' interface.

To open the 'File Groups ' interface

- Click 'Settings' on the left and select 'System Templates'
- Click 'File Groups Variables' from the top

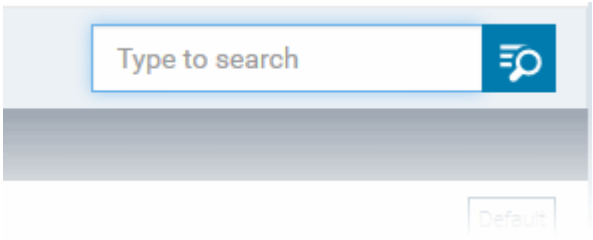


The list of default and user-defined File groups will be displayed. The default groups are indicated by 'Default' at their

right and cannot be edited or deleted.

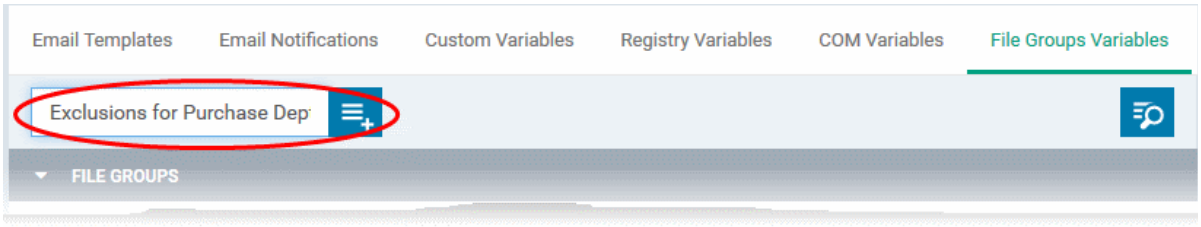
Sorting, Search and Filter Options

- Clicking on the 'File Groups' column header will sort the items in ascending/descending order of the names of the groups.
- To filter or search for a specific File group, click the search icon at the top right and enter the name of the group on part or full



To add a new File group

- Enter the name shortly describing the group in the 'New File Group' field and click the '+'.button



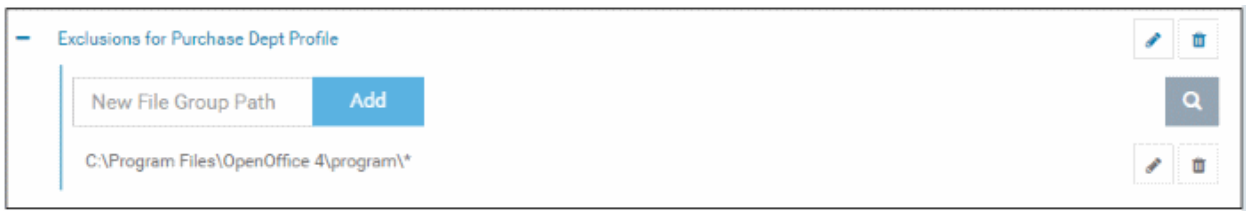
The new group will be added to the list. The next step is to add files to the group.

- Click the '+' at the left of the group name

- Enter the full standard folder/file path of the file to be added to the group in the 'New File Group Path' field and click 'Add'

Tip: To include all the files in a folder, place the wildcard character in the place of file name in the folder path. For example: " C:\My Files* "

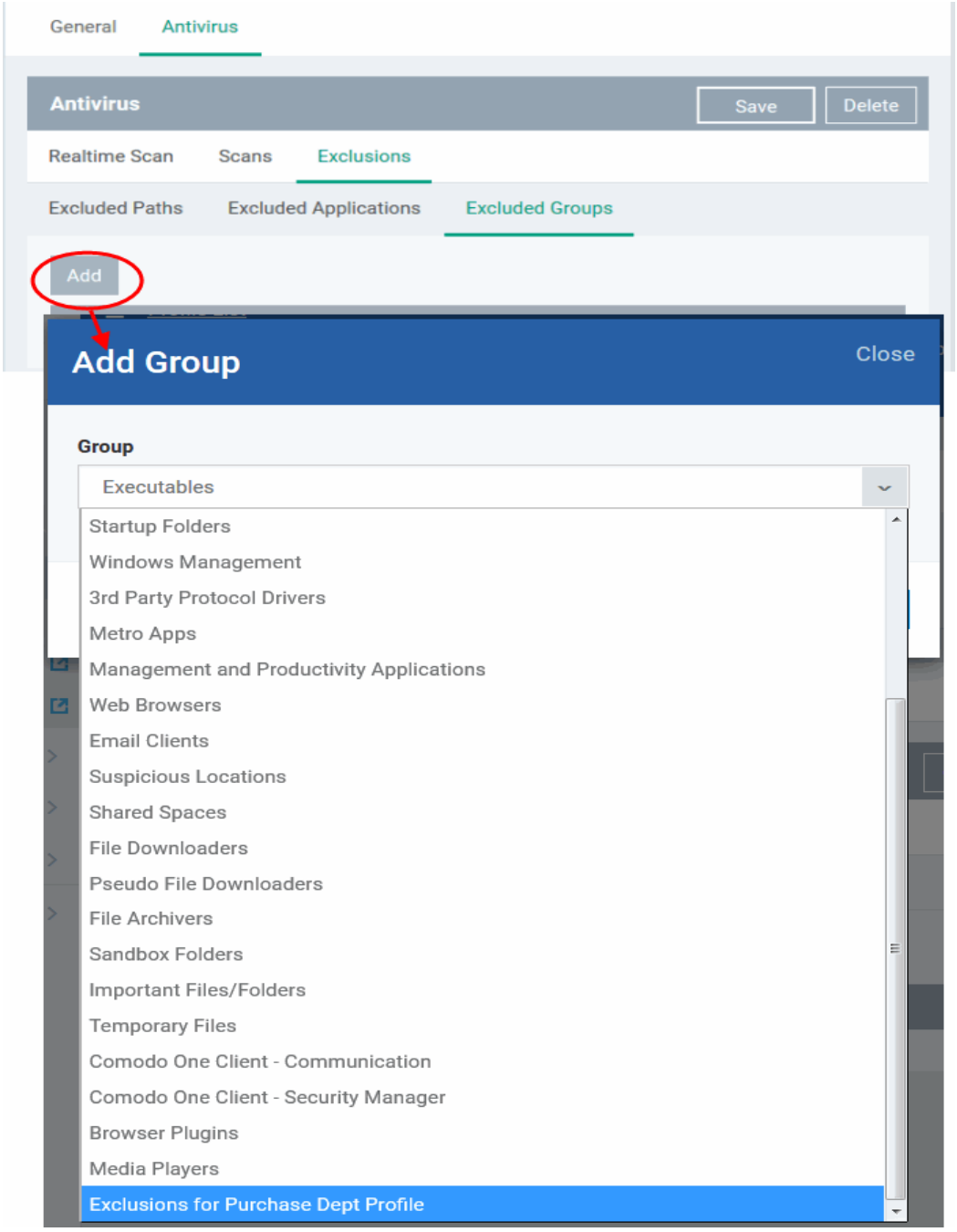
The file(s) will be added to the group.



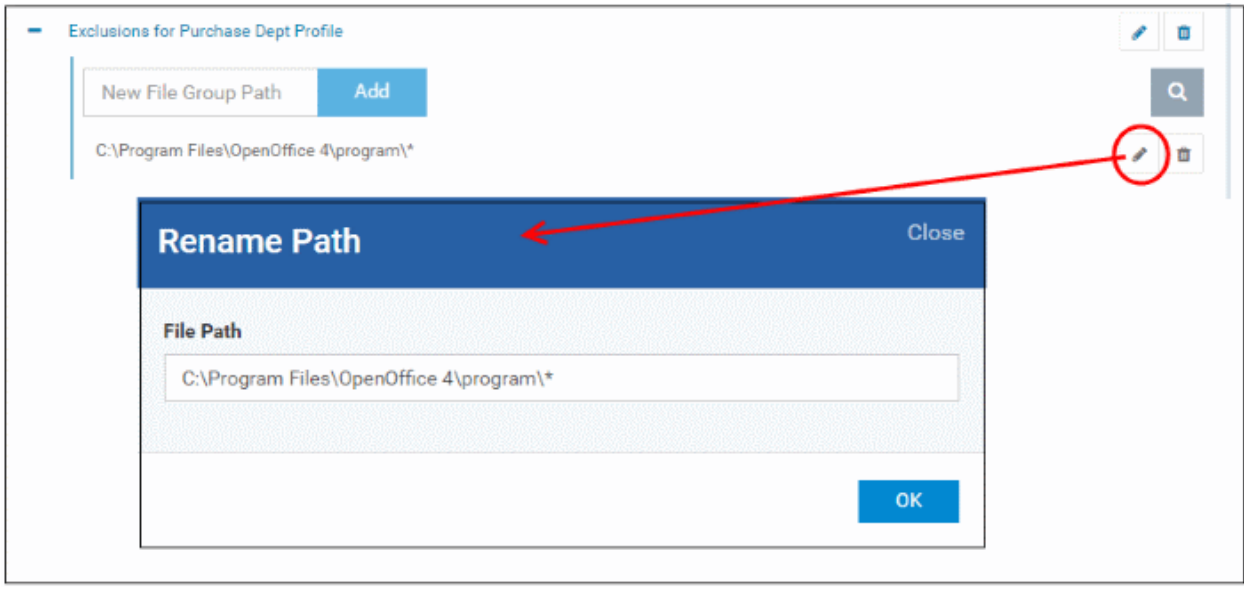
- Repeat the process to add more files to the group.

Once a File Group is added, it will be available for selection in applicable settings interfaces for defining the File

Groups, example, for adding to 'Exclusions' list in 'Antivirus Settings' panel , in the 'Windows Profile' interface.

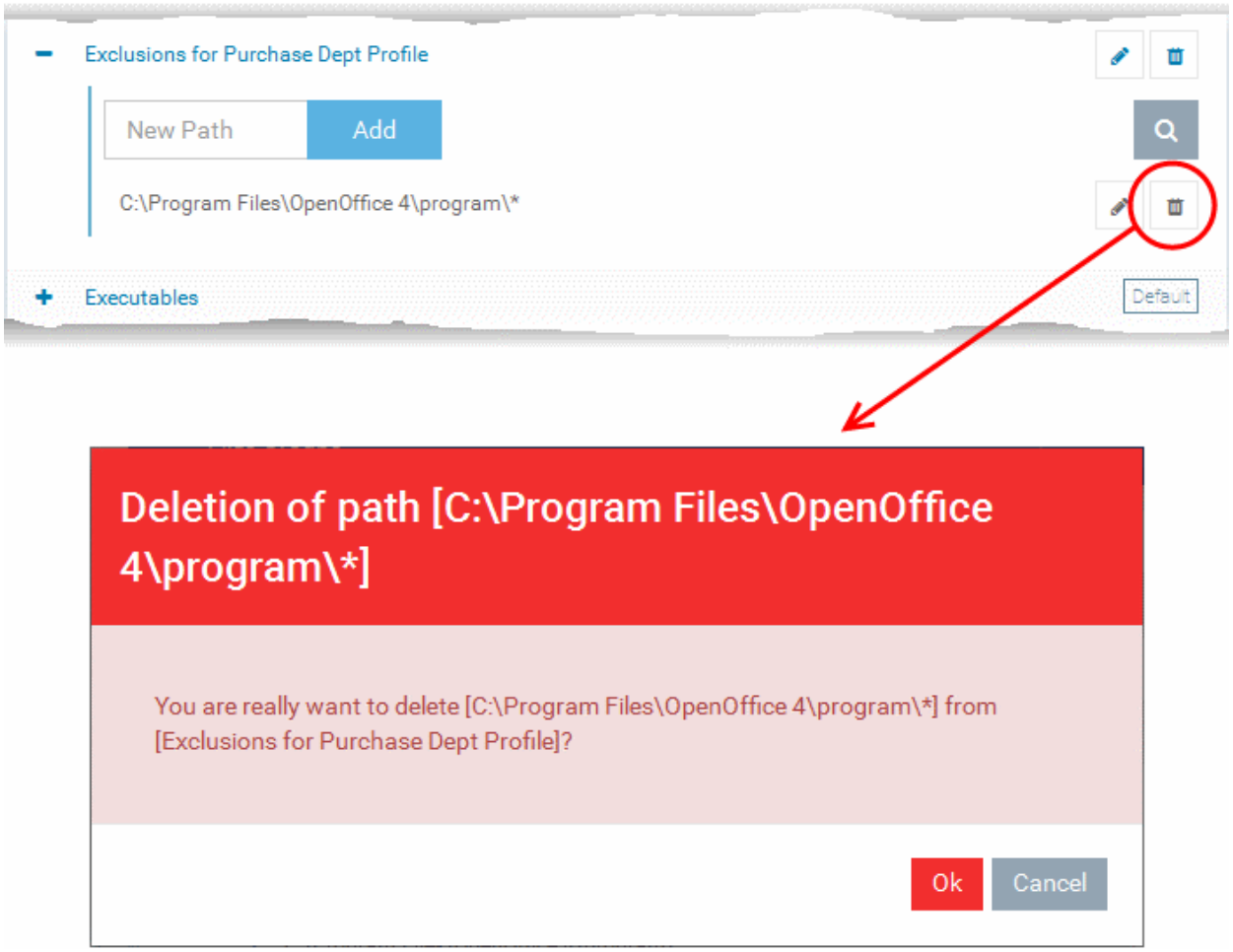


- To edit the files in the group, click the 'Edit' icon beside the file name.



- Edit the file path in the Rename Path dialog and click 'OK'.

- To remove ta file added by mistake or an unwanted file from the group, click the trash can icon beside the file name.

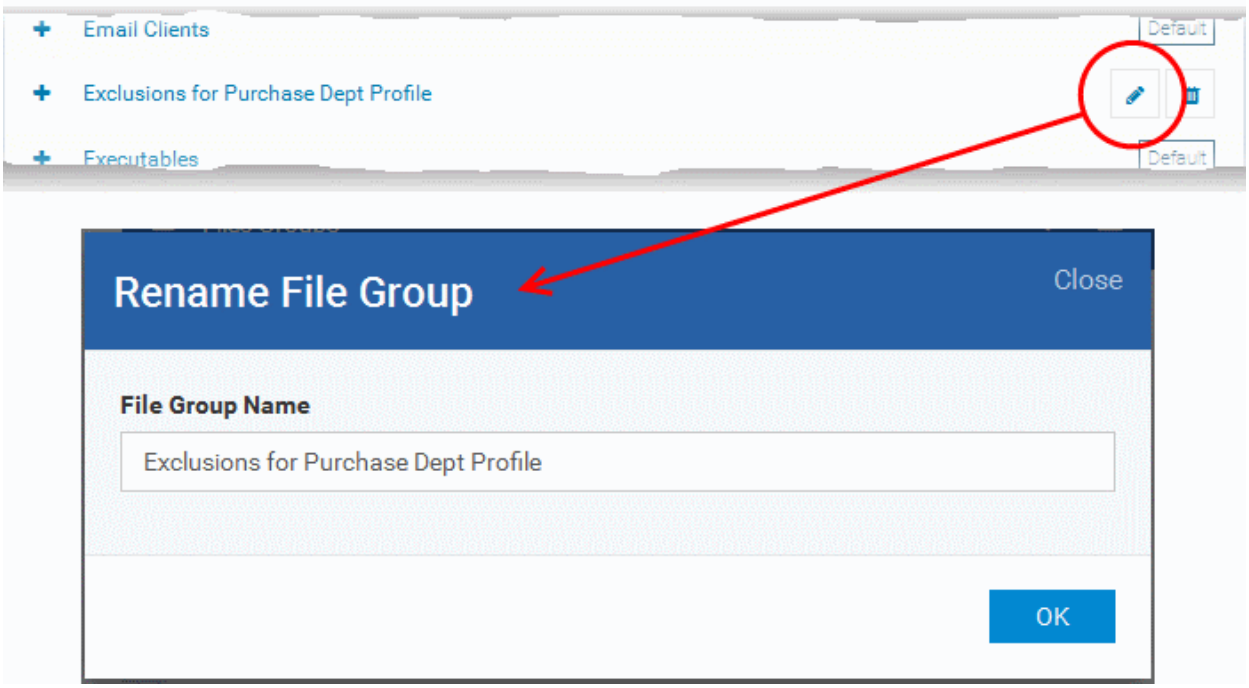


A confirmation dialog will appear.

- Click OK in the confirmation dialog

To edit the name of a File Group

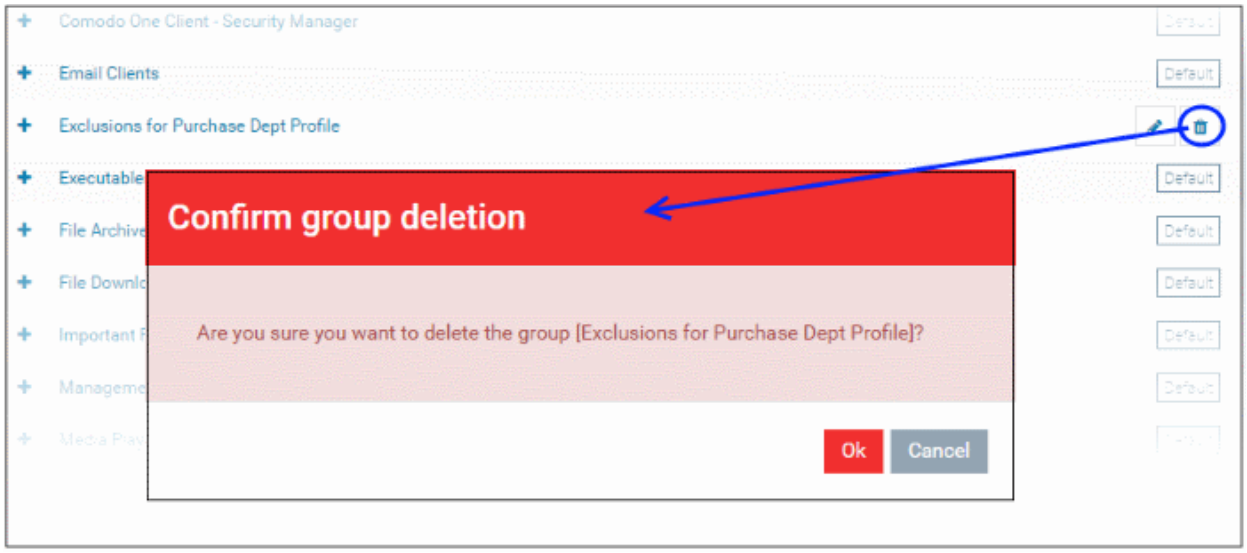
- Click the 'Edit' icon beside the File Group



- Enter the new name for the group in the 'Rename File Group' dialog and click 'OK'

To remove a File Group

- Click the Trash can icon beside the File Group



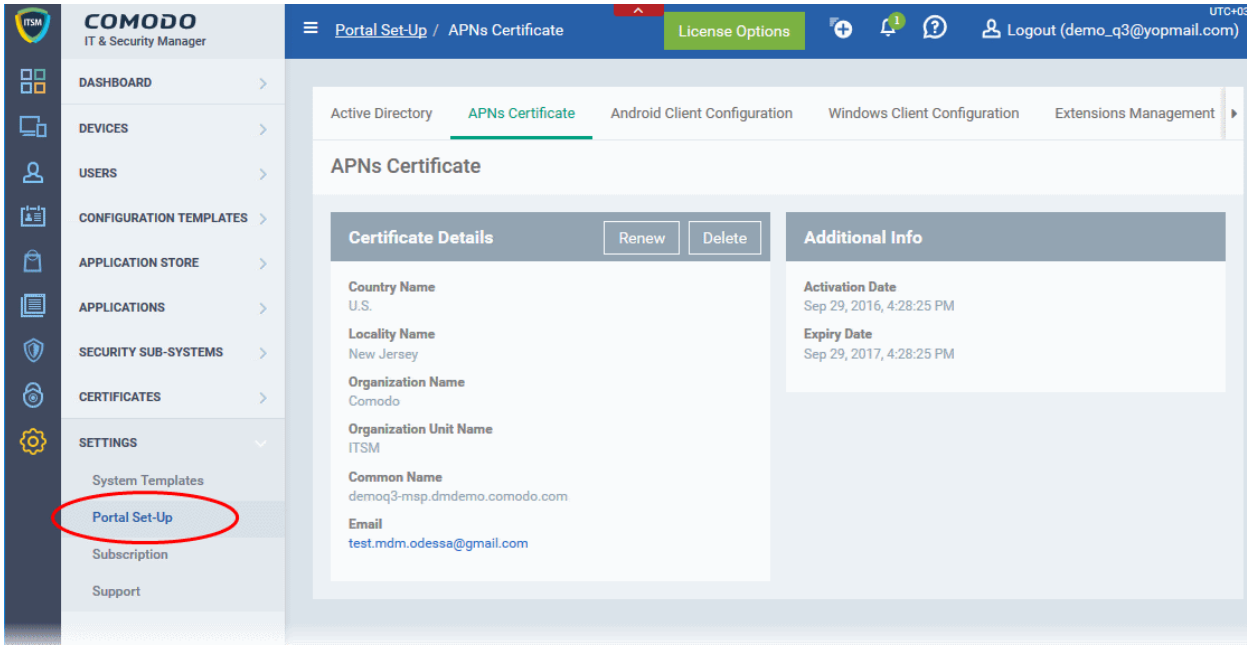
A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

11.2. ITSM Portal Configuration

The 'Portal Set-up' tab under 'Settings' tab allows administrators to set-up and configure the ITSM portal as per their requirements. Administrators can integrate AD server(s) in their network for importing the users and devices, integrate their Apple Push Notification (APN) certificate for communication with managed iOS and Mac OS devices, Google Cloud Messaging (GCM) token for communication with managed Android devices, choose ITSM extensions like RMM and Patch Management, integration with Comodo Certificate Manager (CCM) for issuance of client and

device certificates and so on.



Following sections explain more about:

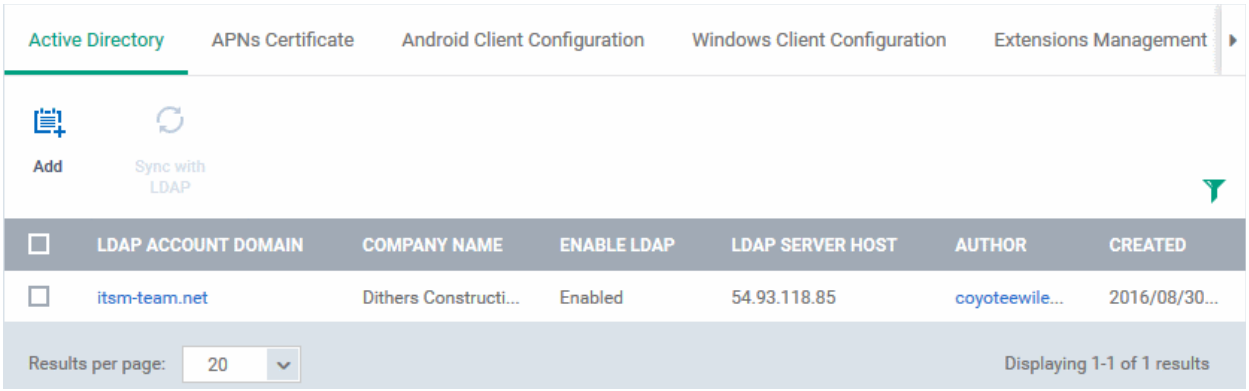
- Importing User Groups from LDAP
- Adding Apple Push Notification Certificate
- Configuring the ITSM Android Agent
  - Configuring General Settings
  - Configuring Android Client Antivirus Settings
  - Adding Google Cloud Messaging (GCM) Token
- Configuring ITSM Windows Client
- Managing ITSM Extensions
- Configuring ITSM Reports
- Integrating with Comodo Certificate Manager
- Setting-up Administrators Time Zone

11.2.1. Importing User Groups from LDAP

In addition to adding user groups manually, ITSM enables administrators to import user groups from Active Directory (AD). You can configure ITSM to access your AD server through the Lightweight Directory Access Protocol (LDAP). You can add multiple LDAP accounts.

To open the Active Directory interface

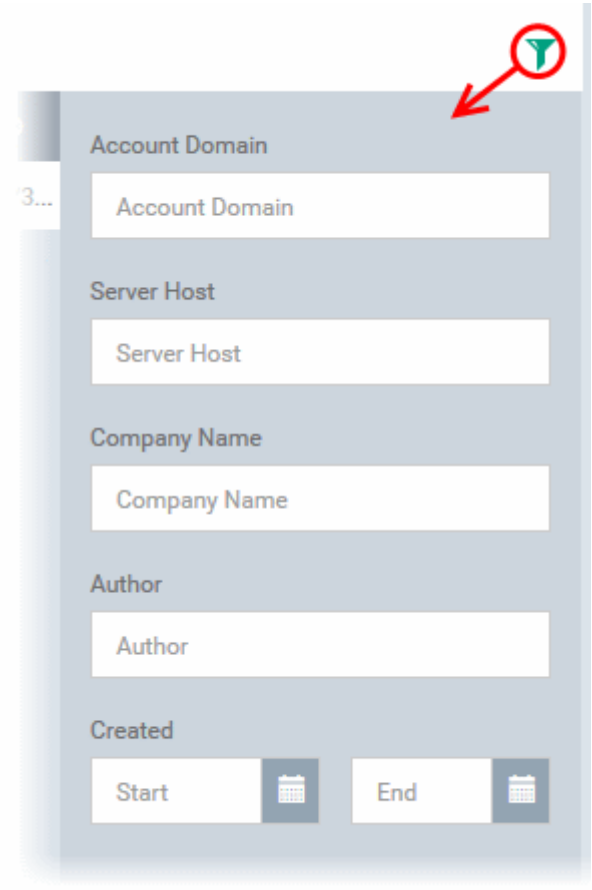
- Click 'Settings' on the left and select 'Portal Set-Up'
- Click 'Active Directory' from the top



LDAP Accounts - Column Description	
Column Heading	**Description**
LDAP Account Domain	Displays the LDAP account domain name. Clicking the AD domain name allows administrators to view the AD details, user groups in the AD, instantly import selected user groups from the AD, configure device enrollment for the imported users, configure connection between AD server and ITSM. Refer to the explanations under **Managing LDAP Accounts** for more details.
Company Name	The name of the company associated with the LDAP account
Enable LDAP	Indicates whether or not the LDAP account is active
LDAP Server Host	Displays the LDAP server host name or IP
Author	Name of the administrator who added the LDAP account
Created	Displays the date and time when the LDAP account was added

Sorting, Search and Filter Options

- Clicking on the column headers sorts items in alphabetical, ascending/descending order
- Clicking the funnel button on the right to open filter options:



- To search for a specific LDAP account based on domain name, host, company and/or author, enter your search criteria in part or full in the respective text boxes and click 'Apply'.
- To filter items based on date created, select the date from the calendar beside Start and End and click 'Apply.

You can use any combination of filters to search for specific LDAP accounts.

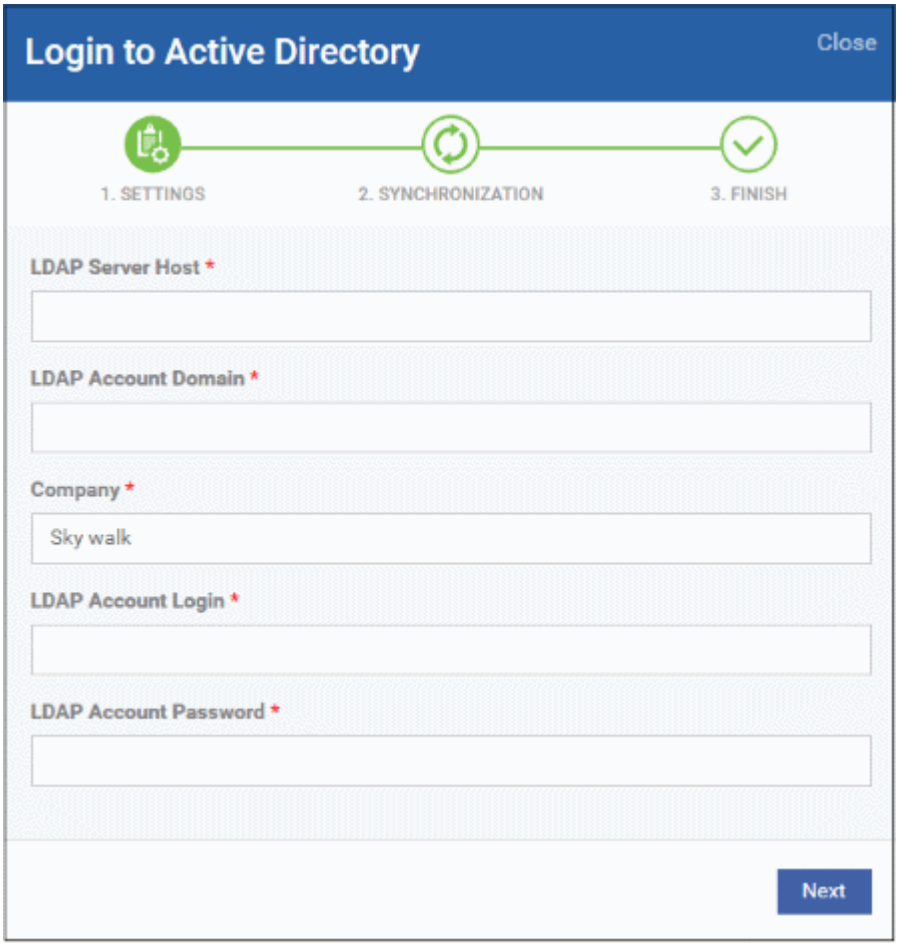
Note: ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, synchronize LDAP server via devices and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in Appendix 1.

To add LDAP accounts

- Click 'Add' at the top

The 'Login to Active Directory' dialog will be displayed.

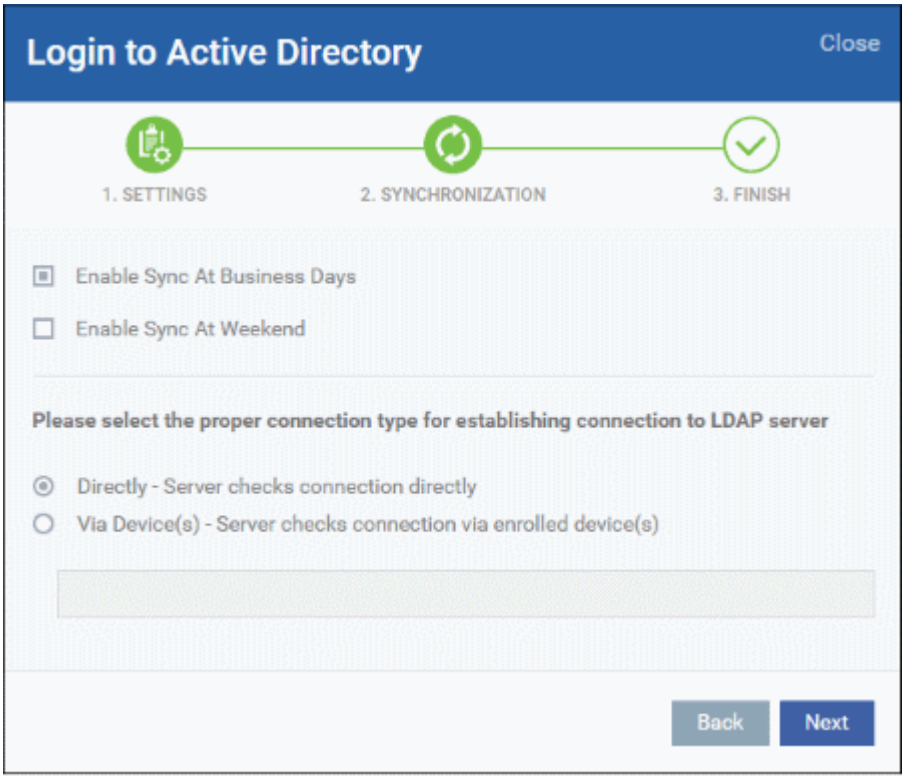
Step 1 - Enter LDAP account details



- **LDAP Server Host** - Enter the IP or host name of LDAP server
- **LDAP Account Domain** - Enter the LDAP account domain that should be used for importing the user groups
- **Company:**
  - Comodo One (C1) customers - Enter the first few characters of the company and select it from the drop-down.
  - Stand-alone ITSM customers - Select 'Default Company' from the drop-down
- **LDAP Account Login -** Enter the username for the LDAP account
- **LDAP Account Password** - Enter the password for the LDAP account

- Click 'Next' after completing the settings form.

Step 2 - Configure Synchronization Settings



Sync Settings

- Enable Sync at Business Days - ITSM will automatically sync with the LDAP server once per day Monday through Friday to check for and import new users
- Enable Sync At Weekend - ITSM will automatically sync with the LDAP server once a day on Saturdays and Sundays to check for and import new users on weekends.

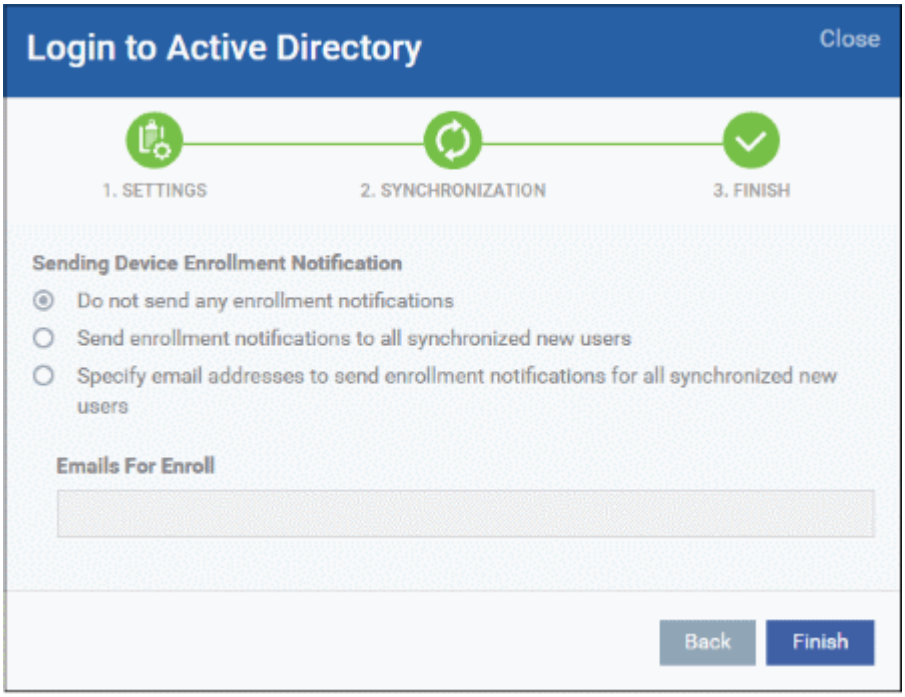
Note - you can manually sync at any time by clicking the 'Sync with LDAP' button.

Connection Type

This settings determines how ITSM will connect to the LDAP server, whether from the ITSM server directly or via the enrolled devices. If you choose the second option, then you can add multiple enrolled Windows devices. The second option is used to connect ITSM SaaS portal to AD server placed in the local network in which the enrolled endpoints are available.

- Click 'Next'

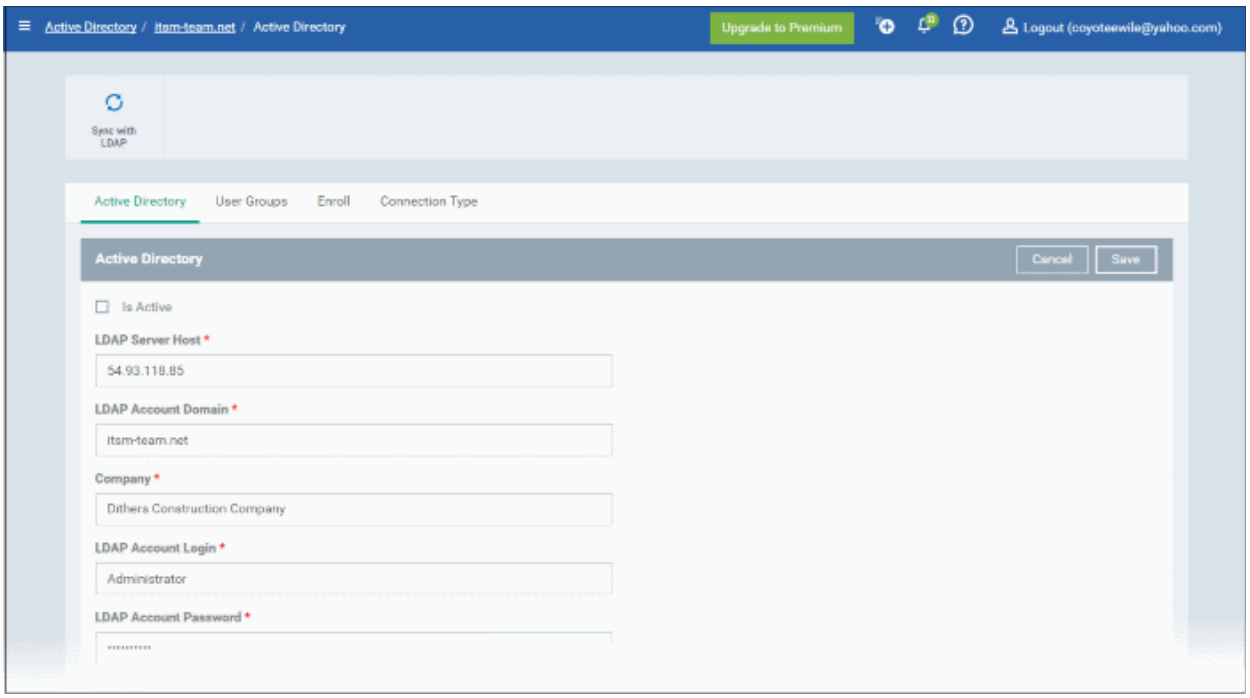
Step 3 - Finish



- Do not send any enrollment notifications - No enrollment mails will be sent to users imported via LDAP
- Send enrollment notifications to all synchronized new users - Device enrollment emails will be sent to new users enrolled via LDAP
- Specify email address to send enrollment notifications for all synchronized new users - Specify email recipients who should receive a notification mail when new users have been added. Usually sent to an administrator, the mail will contain instructions on how to enroll devices for the new users. You can add multiple email addresses here.

- Click 'Finish'

ITSM will connect to the LDAP server per the configuration and if successful, a summary of account settings will be displayed:



- Click 'Save' to complete the set up process.

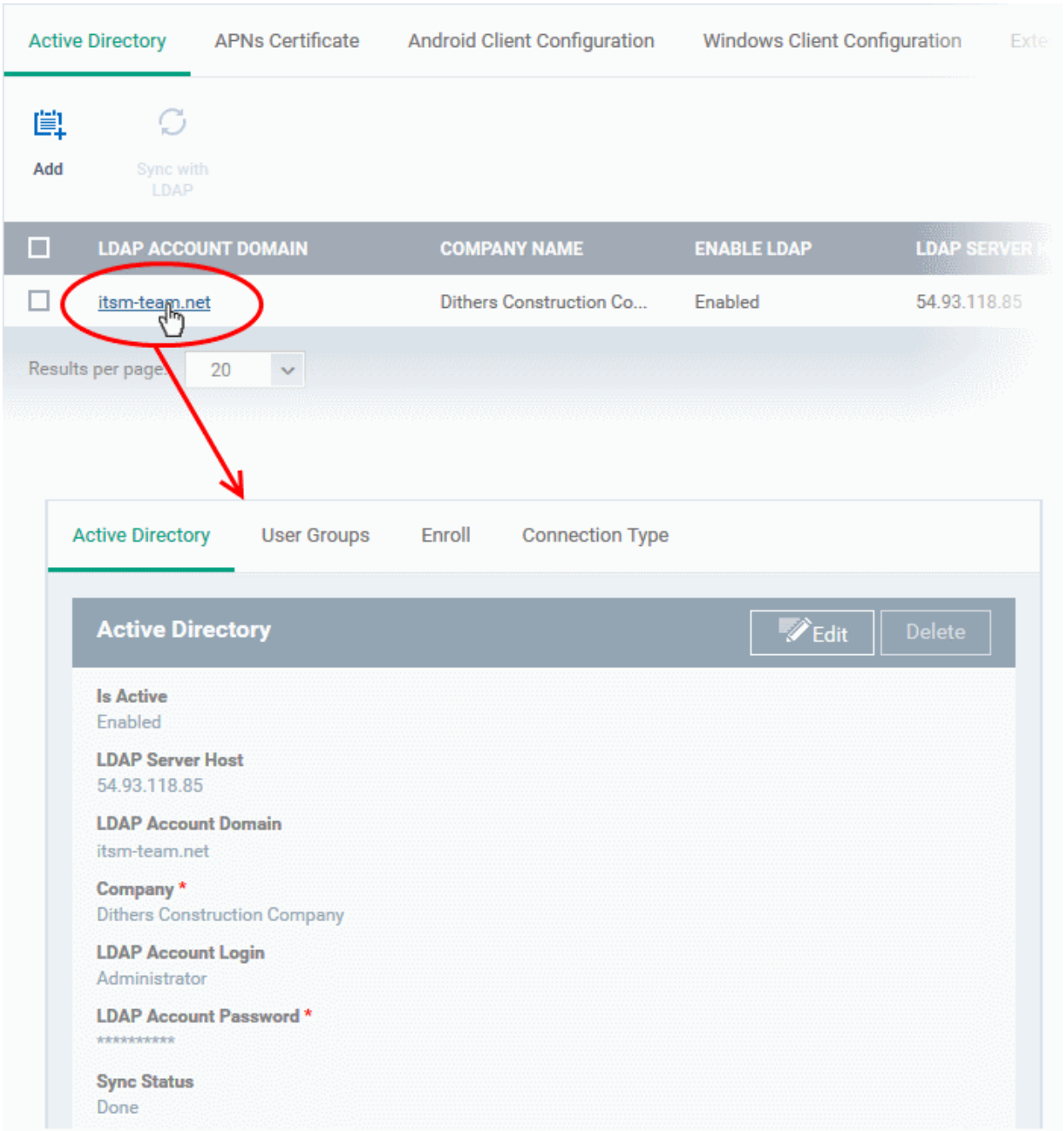
- Next, sync user groups with the LDAP server by clicking the 'Sync with LDAP' button at the top.

The synchronization task will run and user groups will be added. You have to select the group and enable sync to import users into their respective groups.

Managing LDAP Accounts

Administrators can view and edit the details of integrated AD servers, synchronize the users in selected group between AD server and ITSM and more, from the 'Active Directory' interface.

- To manage an AD server click the AD domain name from the list of LDAP accounts in the Active Directory interface.



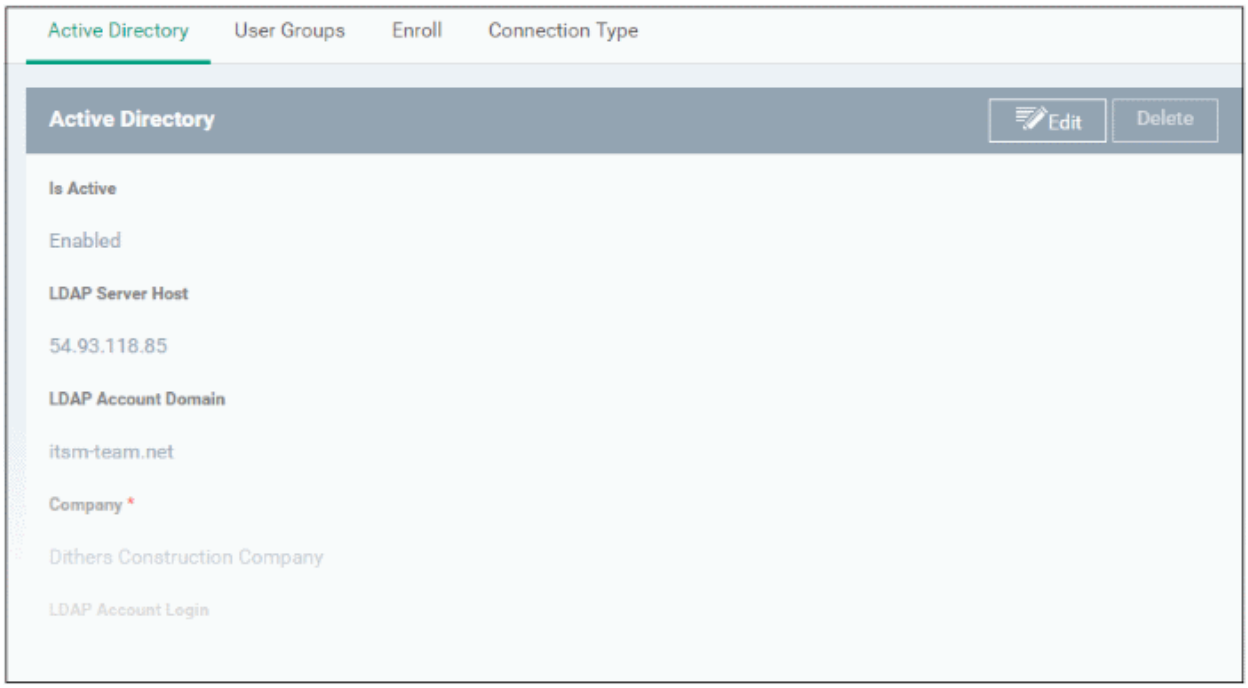
The Active Directory details will be displayed under four tabs:

- Active Directory

- User Groups
- Enroll
- Connection Type

Active Directory tab

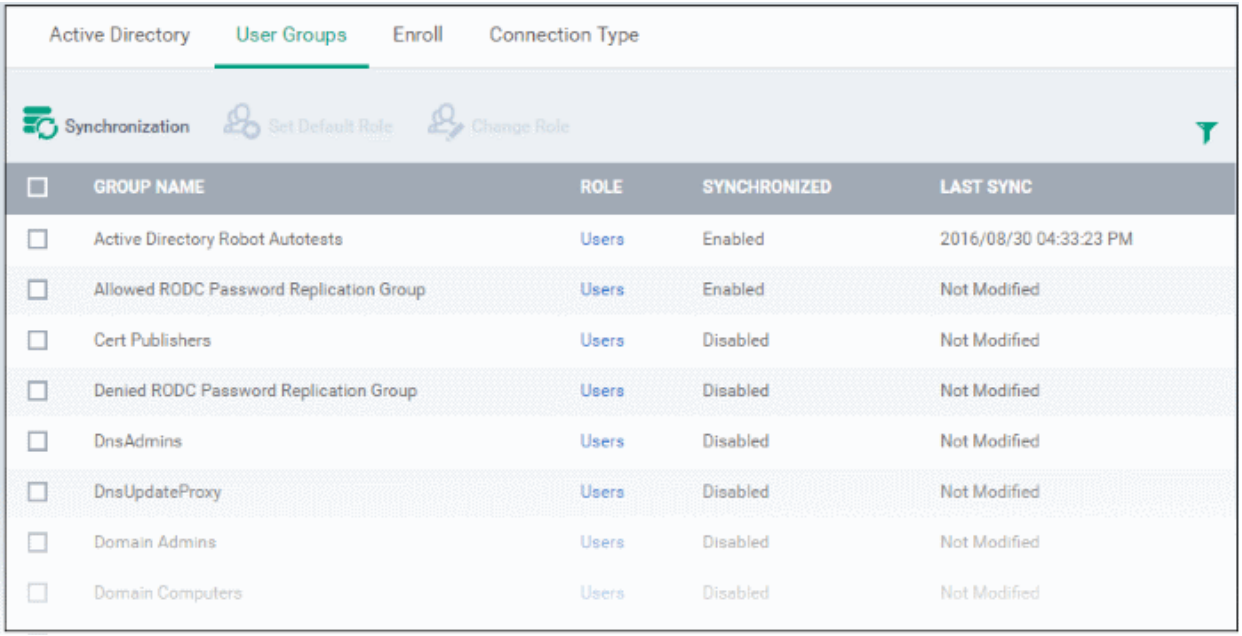
The 'Active Directory' tab displays AD configuration details.



- Click 'Edit' to update any LDAP details and click the 'Save' button

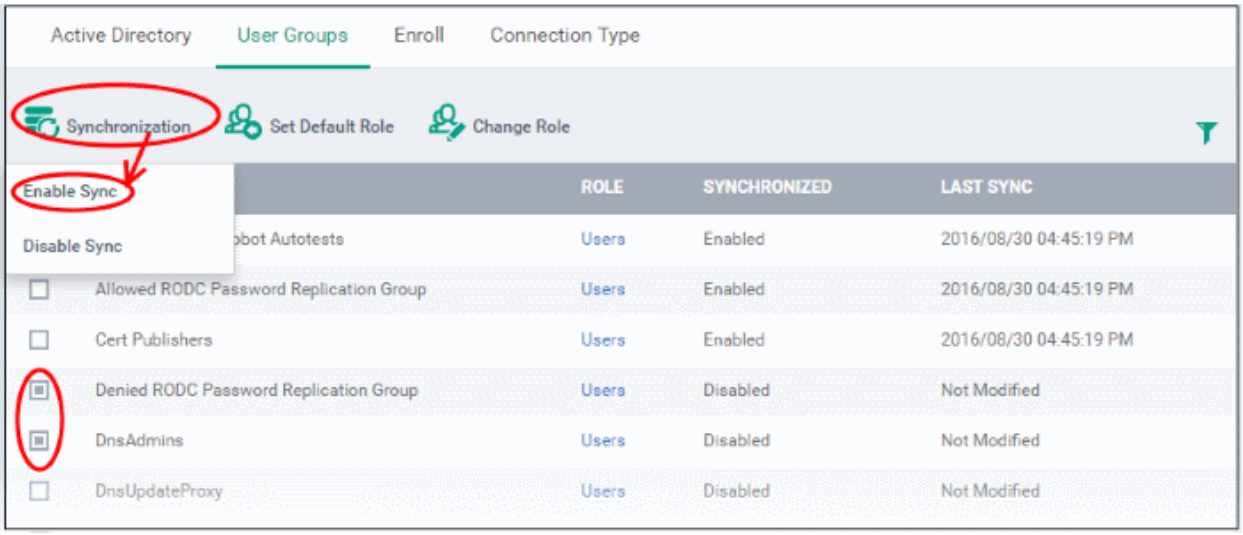
User Groups tab

The 'User Groups' tab displays the list of user groups that were imported to ITSM from the AD server. It also allows you to synchronize the users in selected user groups, so as to import the newly added users to the group and to remove users removed from the group.



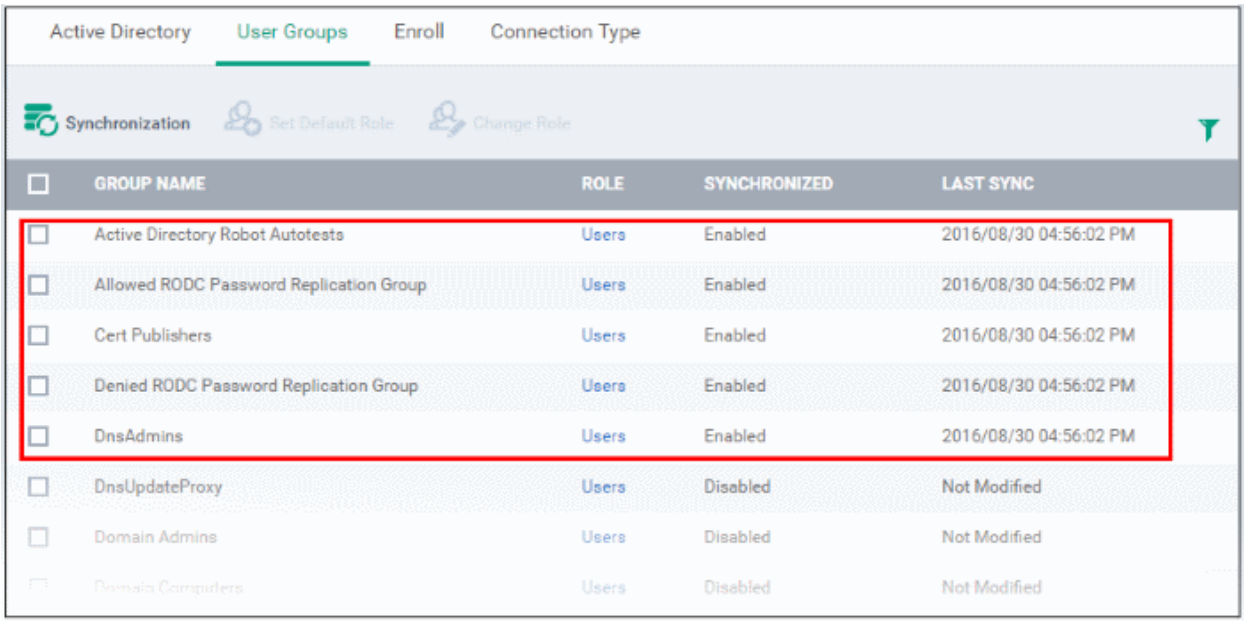
Once the user groups are imported, you have to enable sync for the groups to import users in a group. Please note the role for the users will be assigned the default role that is set in ITSM.

- Select user group(s) from the list and click 'Synchronization' at the top

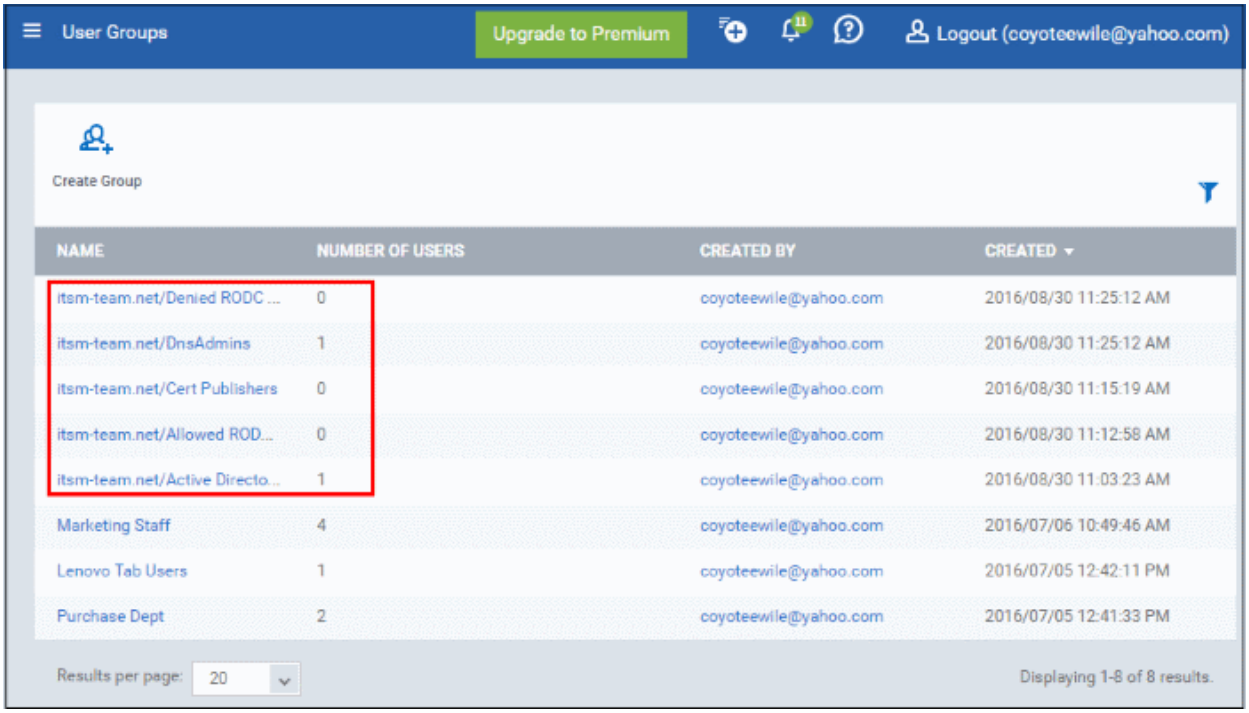


- Click 'Enable Sync'. The status of the group in the 'Synchronized' column will display as 'Enabled'.
- To import users for an enabled group from LDAP instantly, click 'Sync with LDAP'

The 'Last Sync"status for the sync-enabled groups will be updated and displayed.

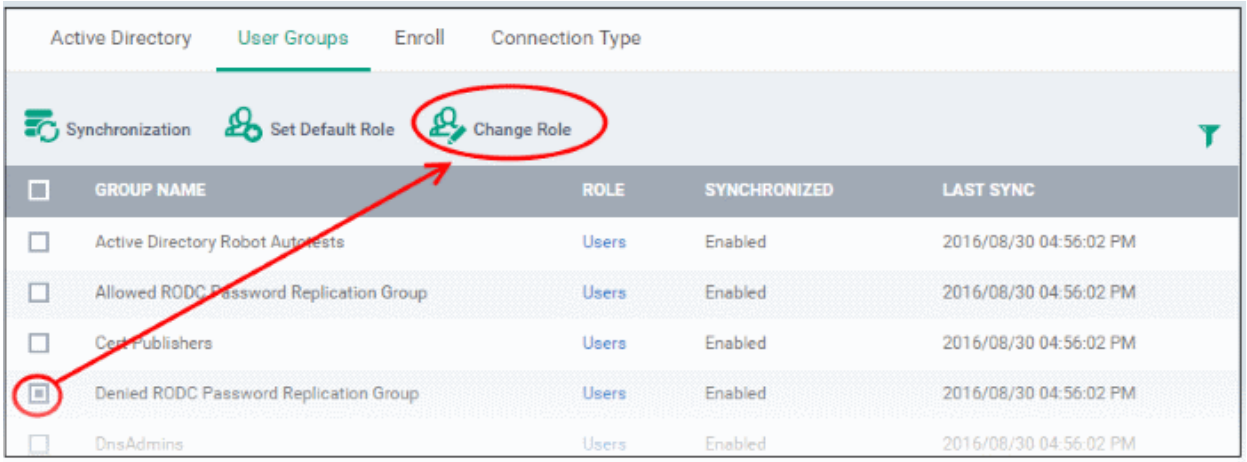


You can view the imported user groups in 'Users' > 'User Groups':

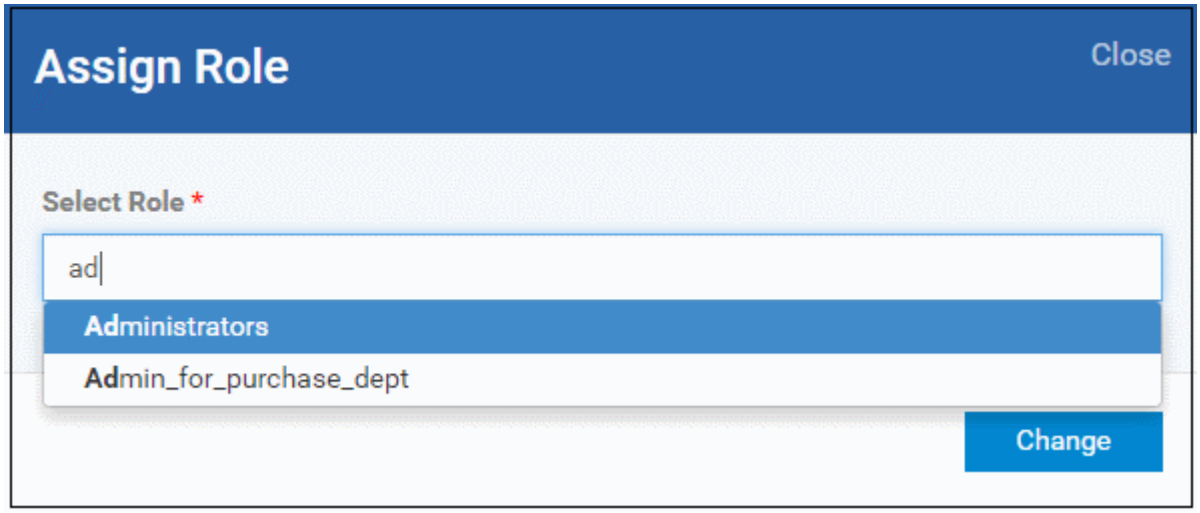


Refer to the section '**Managing User Groups**' for more details.

- To set roles for the users in a group, select the group and click 'Set Default Role'.
- To set different role other than default role, click 'Change Role'



The 'Assign Role' dialog will be displayed:



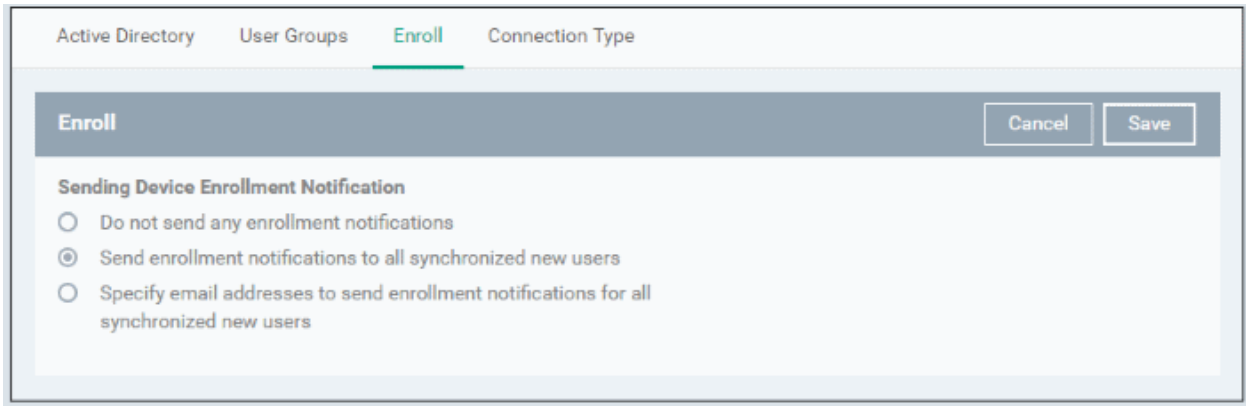
- Type the first few characters of the role, select it from the drop-down and click 'Change'.

The new role will be assigned for the users in the user group. Refer to the section '**Managing Roles Assigned to a User**' for more details.

Enroll tab

The 'Enroll' tab displays the current setting of enrollment notification sent to imported users.

- Click 'Edit' to change the enrollment notification type



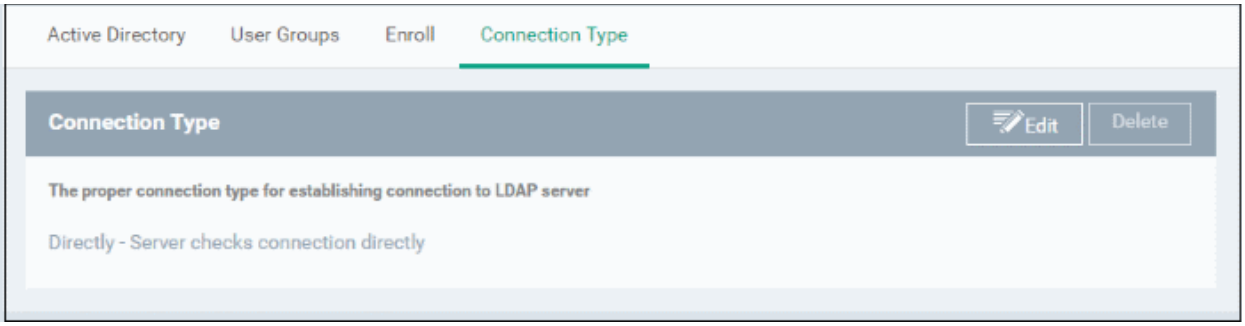
- Do not send any enrollment notifications - No enrollment mails will be sent to users imported via LDAP
- Send enrollment notifications to all synchronized new users - Device enrollment emails will be sent to new users enrolled via LDAP.
- Specify email address to send enrollment notifications for all synchronized new users - Specify email recipients who should receive a notification mail when new users have been added. Usually sent to an administrator, the mail will contain instructions on how to enroll devices for the new users. You can add

multiple email addresses here.

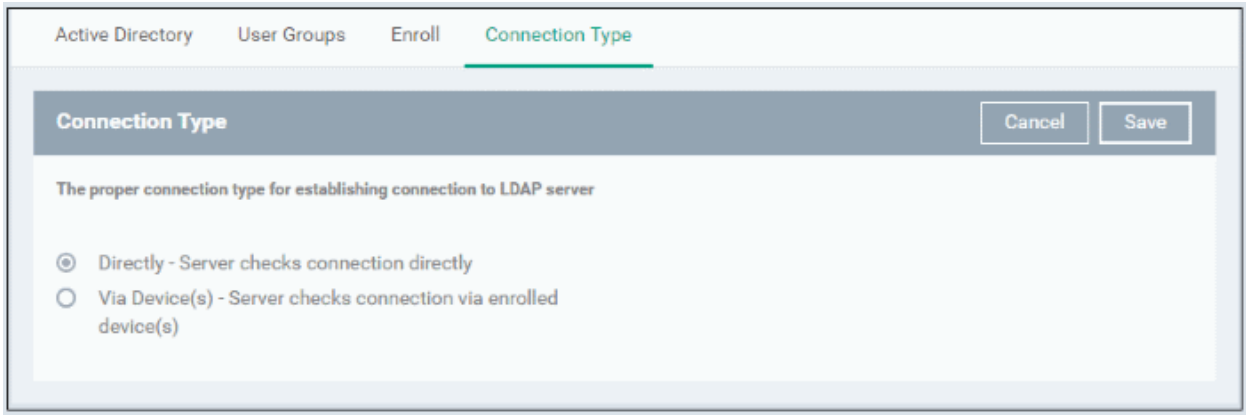
- Update the notification type from the options and click 'Save'

Connection Type Tab

The Connection Type tab displays how the AD server currently connects to ITSM.



- Click the 'Edit' button to change the connection type.



If the first option is selected, ITSM will connect to the configured LDAP server directly. The second option enables the ITSM server to connect to the LDAP server via enrolled devices. Multiple devices can be configured for the second option.

- Click 'Save' after selecting the option.

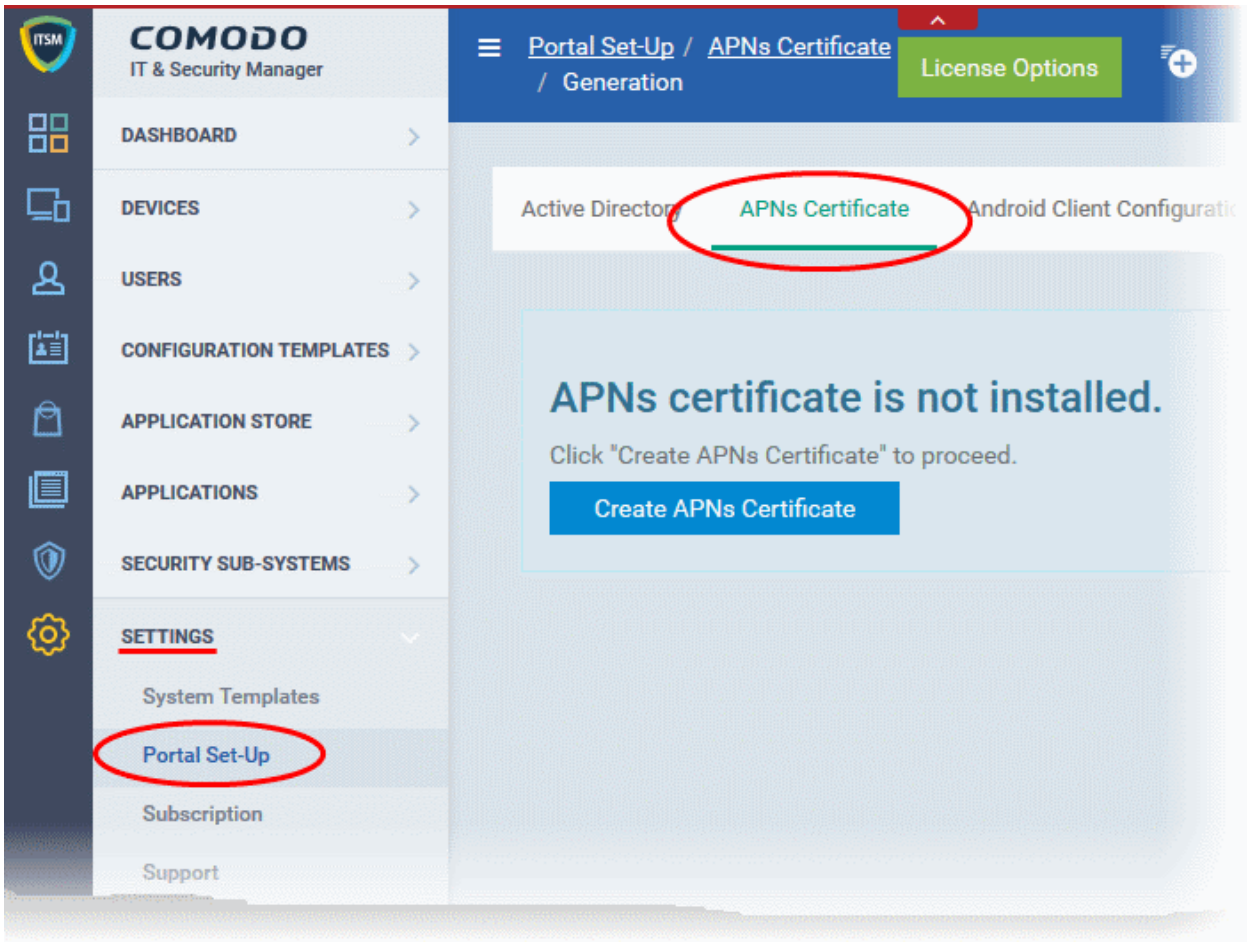
You can add multiple LDAP servers for the account from the Active Directory interface. Click 'Add' and follow the same procedure explained above.

11.2.2. 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:

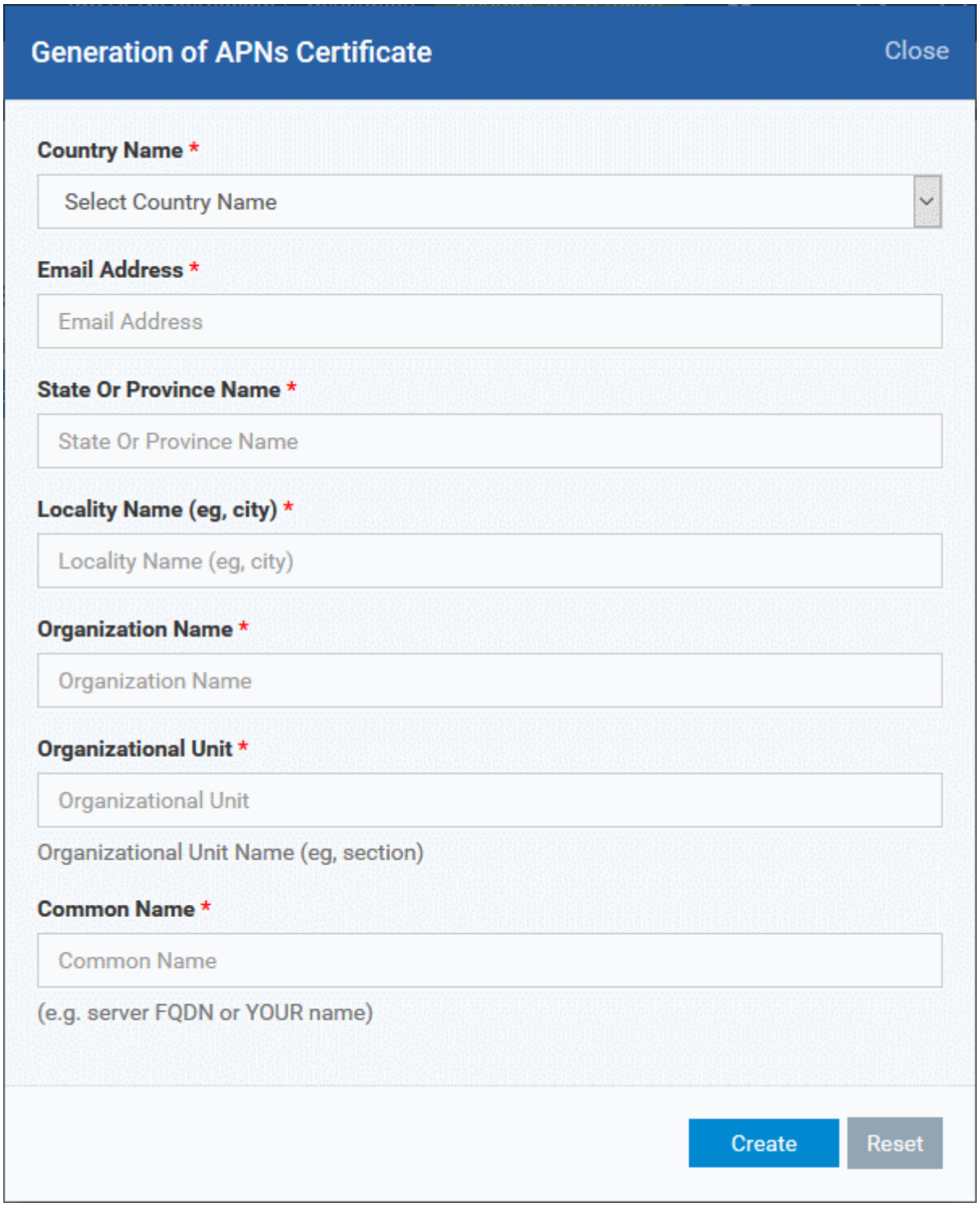
Step 1- Generate your PLIST

- Click 'Settings' on the left and select 'Portal Set-Up'
- Click APN Certificate from the top.

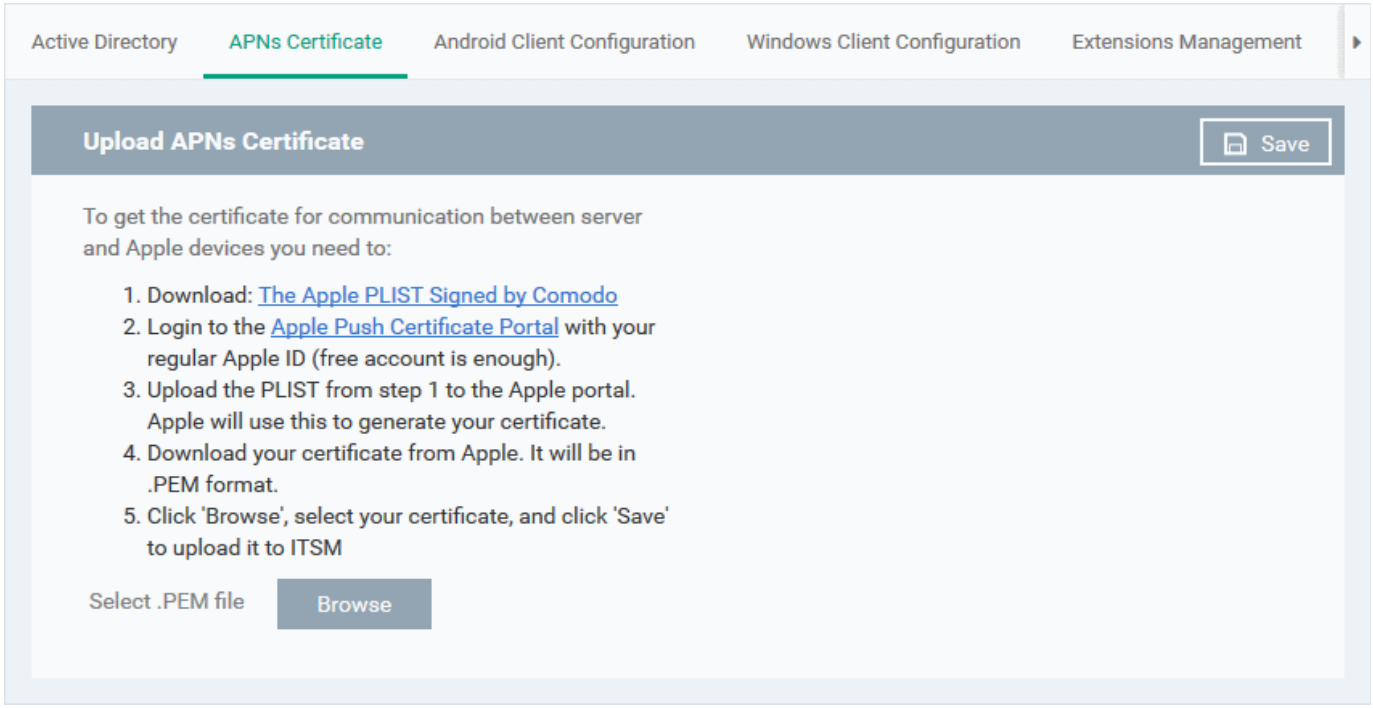


- Click the 'Create APNs Certificate' button to open the APNs application form.

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:



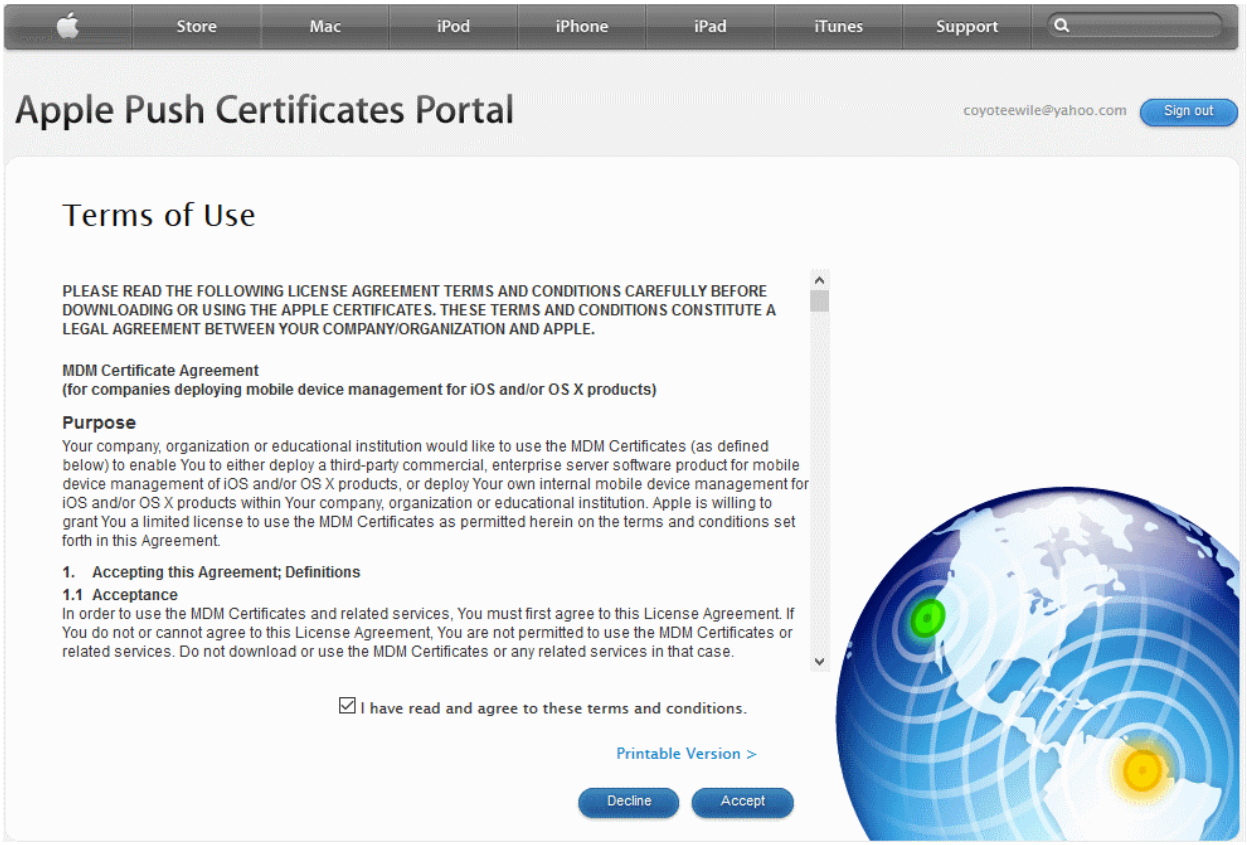
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.

Step 2 -Obtain Your Certificate From Apple

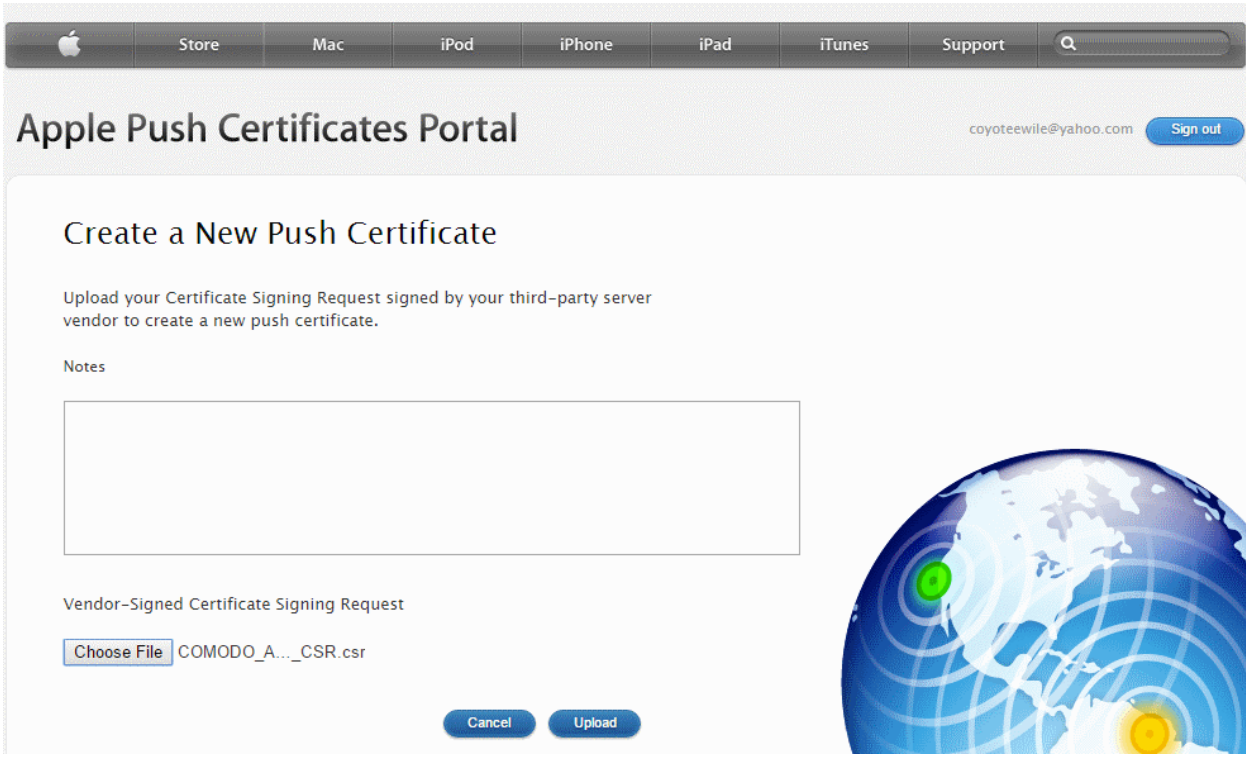
- Login to the 'Apple Push Certificates Portal' with your Apple ID at https://identity.apple.com/pushcert/.

  If you do not have an Apple account then please create one at https://appleid.apple.com.
- Once logged in, click 'Create a Certificate'.

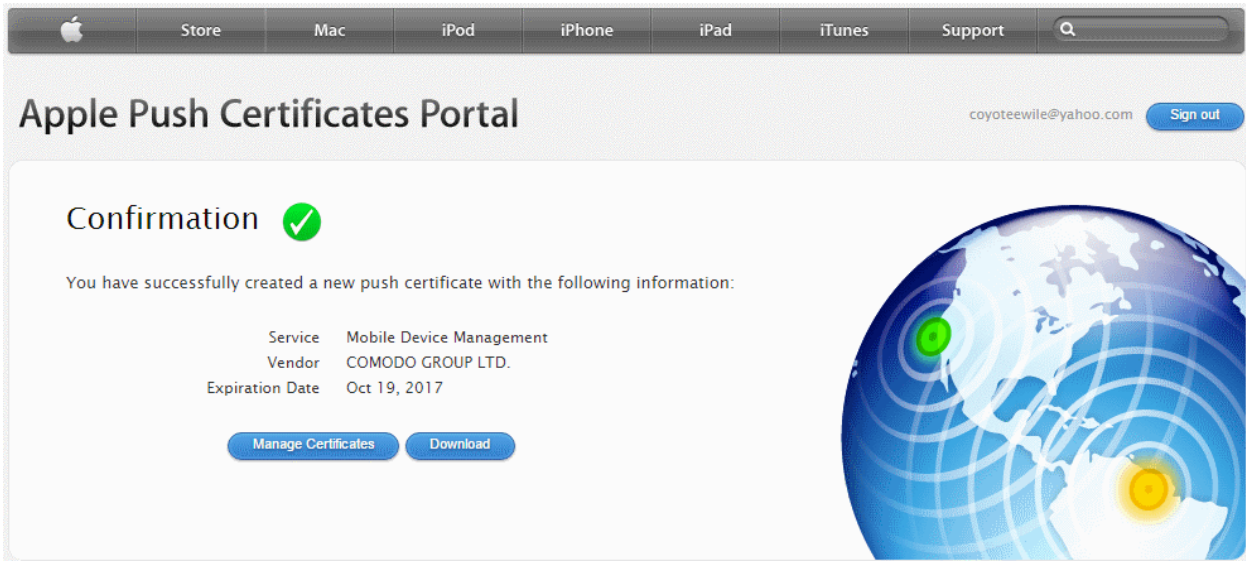
You will need to agree to Apple's EULA to proceed.



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



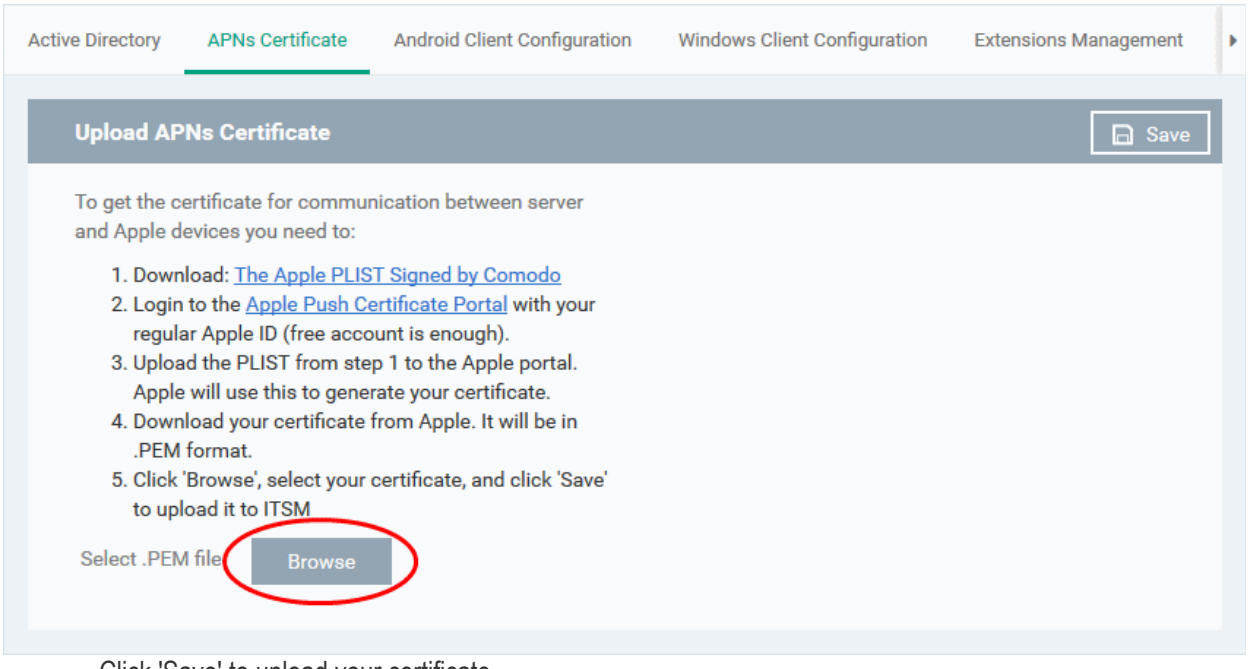
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



- 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'

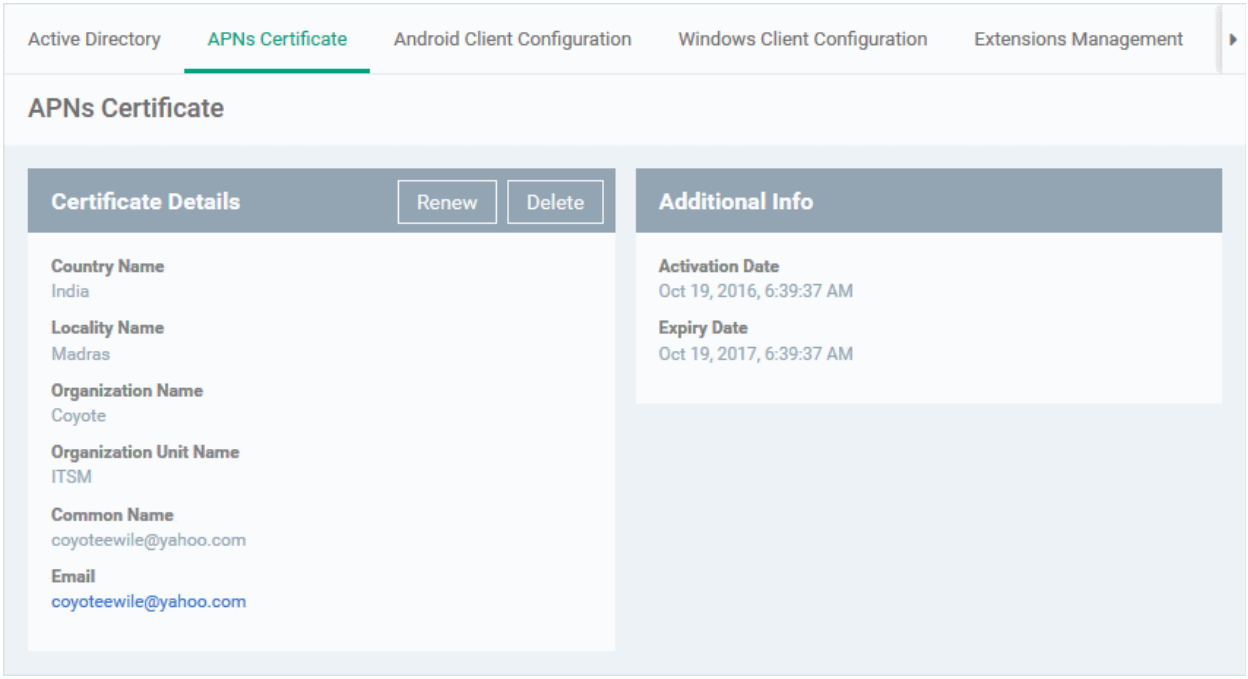
Step 3 - Upload your certificate to ITSM

- 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.

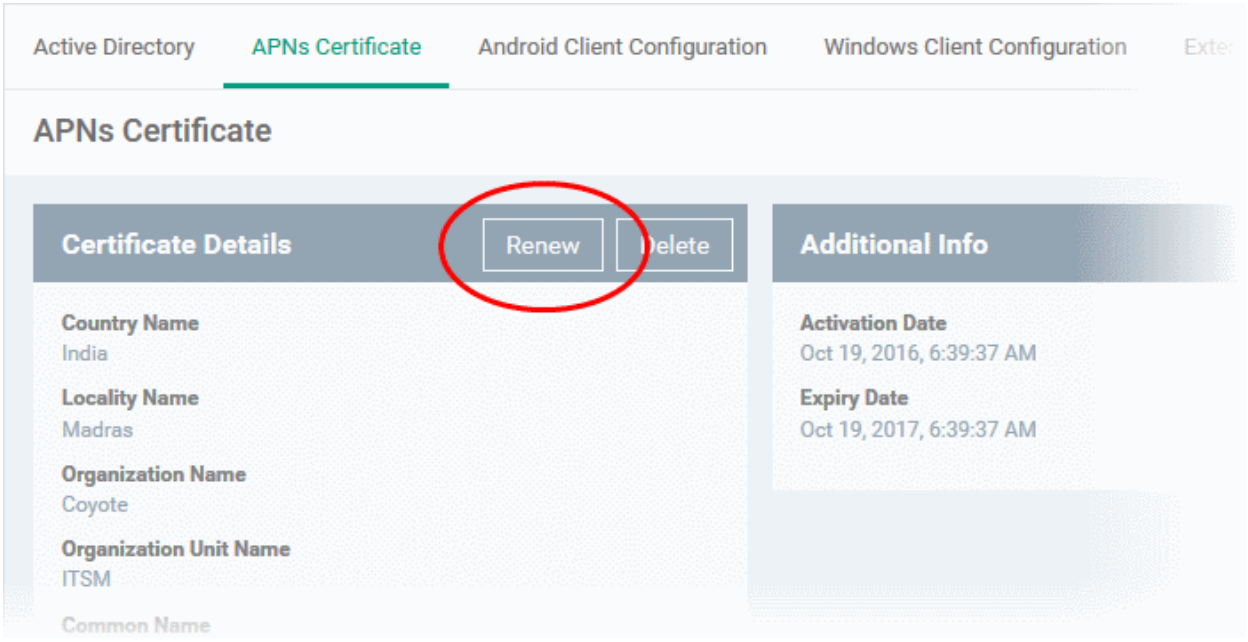
The APNs Certificate details interface will open:



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.



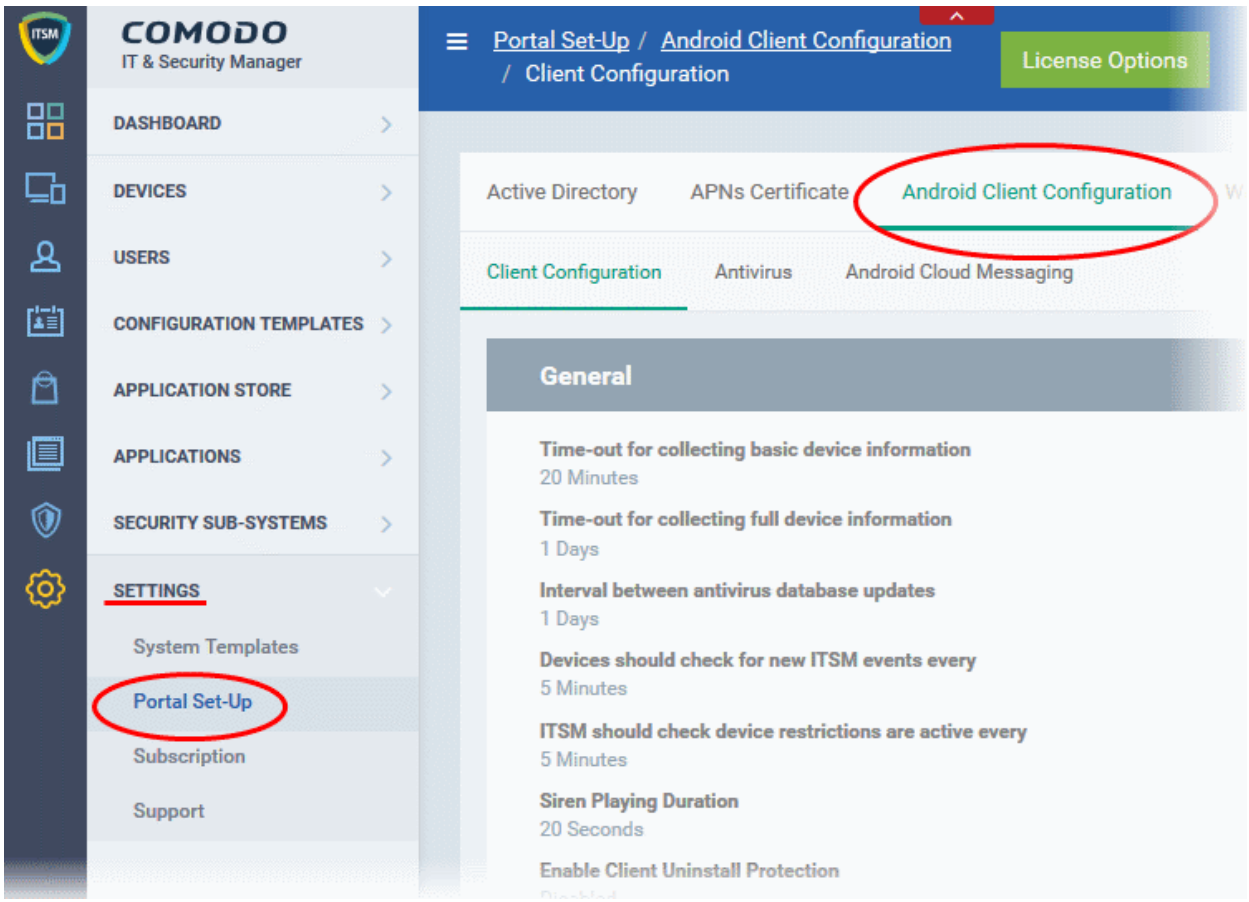
- Click 'Delete' only if you wish to remove the certificate so you can generate a new APNs certificate.

11.2.3. Configuring the ITSM Android Agent

ITSM uses an agent installed on enrolled Android devices for communication with the server and for running antivirus functionality. The 'Android Client Configuration' area allows admins to add a Google Cloud Messaging token for agent communication, and to configure general agent behavior and antivirus settings.

To open the 'Android Client Configuration' interface

- Click 'Settings' on the left and select 'Portal Set-Up'
- Click Android Client Configuration from the top



The interface contains three tabs:

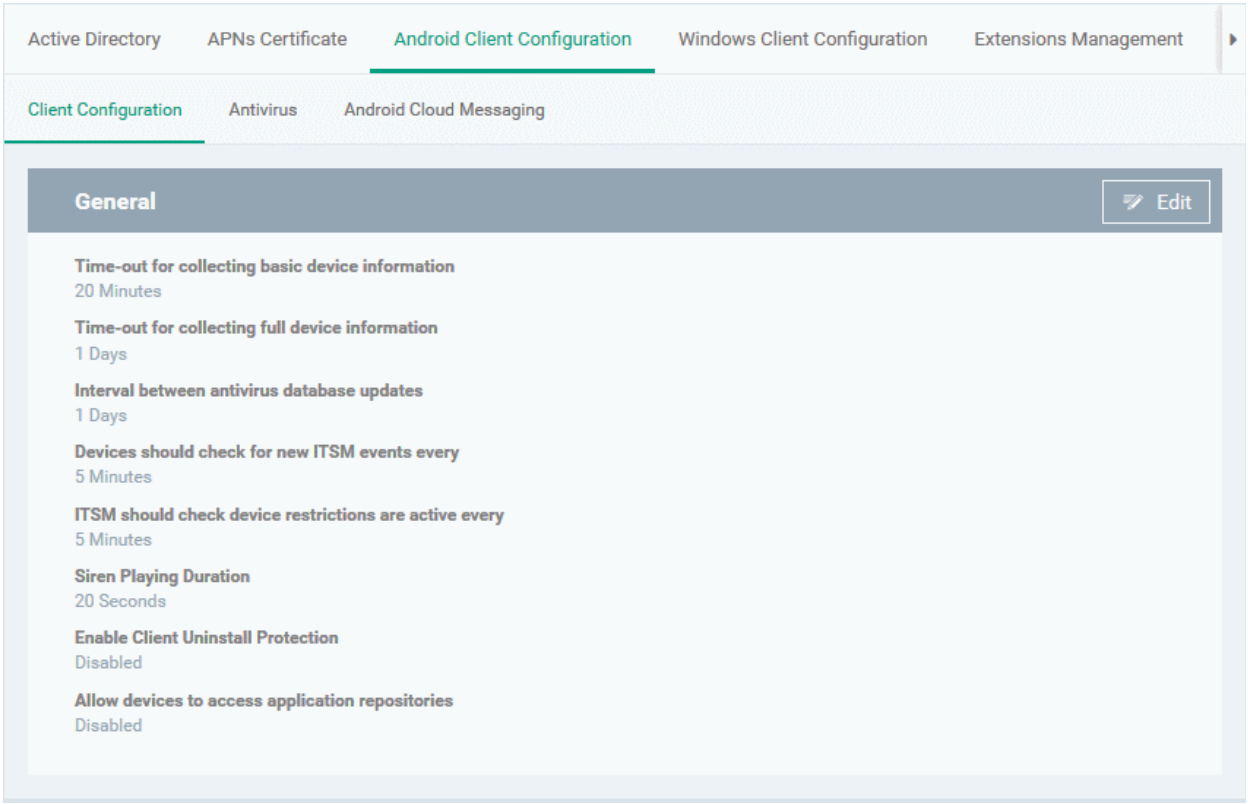
- **Client Configuration** - Allows you to configure general settings like agent and AV virus updates, polling intervals, client uninstall protection and so on. Refer to **Configuring General Settings** for more details.
- **Antivirus** - Allows you to specify whether Android viruses should be dealt with automatically or manually. If 'Automatic' is chosen' you can also specify whether the AV should remove the threat or ignore it. Refer to **Configuring Android Client Antivirus Settings** for more details.
- **Android Cloud Messaging** - Allows you to create a Google Cloud Messaging (GCM) token to facilitate communications between ITSM and Android devices. Refer to the section **Adding Google Cloud Messaging (GCM) Token** for more details.

11.2.3.1. Configuring General Settings

The Android 'Client Configuration' area allows you to configure various settings related to update periods, device alarms, uninstall protection and the visibility of application repositories on the device.

To open the Android 'Client Configuration' interface:

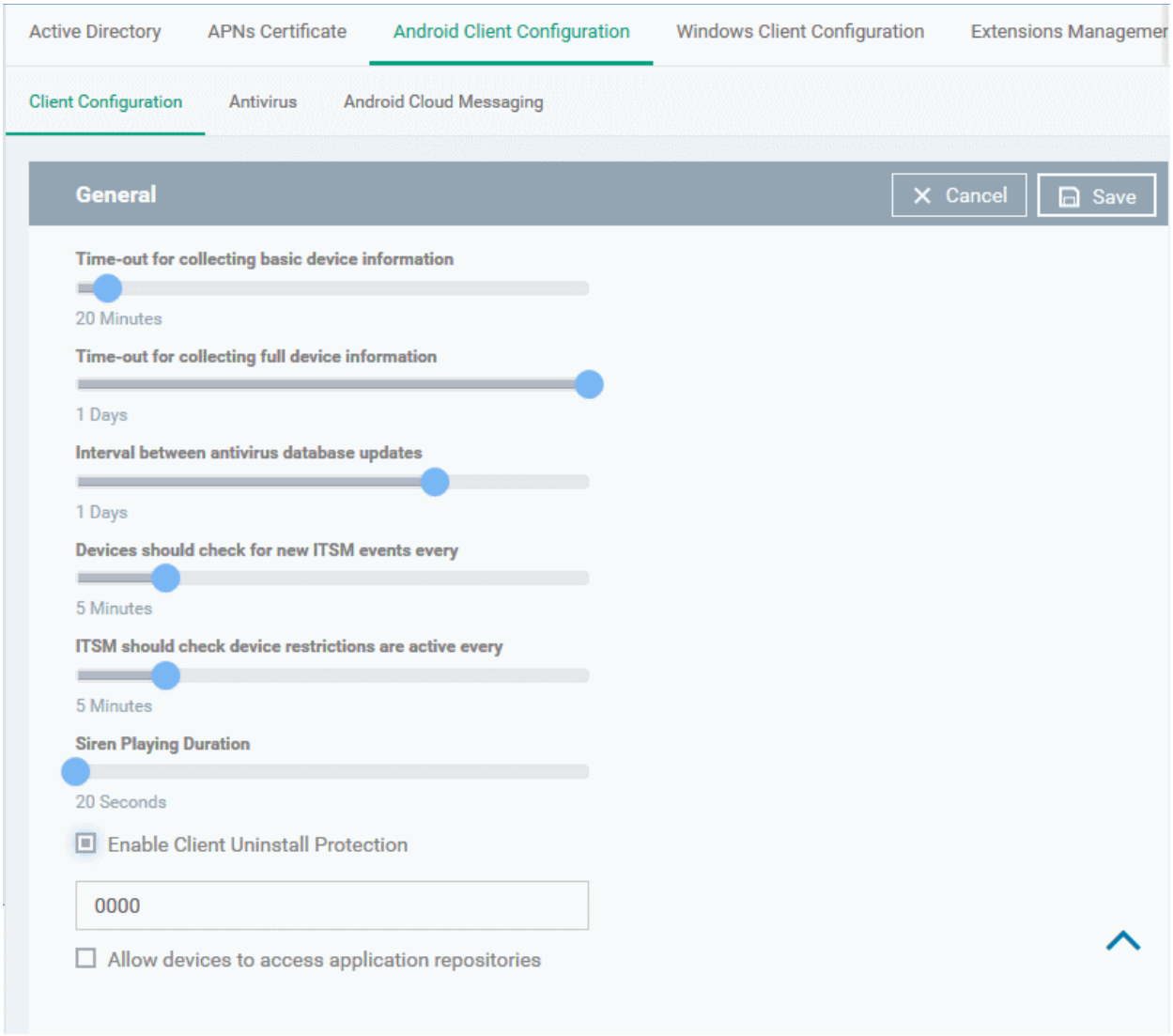
- Click 'Settings' on the left and select 'Portal Set-Up'.
- Click 'Android Client Configuration' at the top.
- Click the 'Client Configuration' tab in the 'Android Client Configuration' interface



-

The current settings for various parameters of Client Configuration will be displayed.

- To change the settings, click the edit button  on the top.



Android Client Configuration Settings	
Parameter	**Description**
Time-out for collecting basic device information	The update time interval for device information such as battery level, CPU usage, location of the device (GPS) and current WiFI SSID.
Time-out for collecting full device information	The update time interval for complete device information such as memory status, name of the device, IMEI number, roaming state, MAC address of bluetooth and MAC address of WiFi.
Interval between antivirus database update	The time intervals at which the antivirus database should be updated on the device.
Devices should check for new ITSM events every	The time interval at which the device should check ITSM for new push notifications.
ITSM should check device restrictions are active every	The time interval at which the client checks that its device restrictions are in place.
Siren Playing Duration	Length of time that the siren will sound for when administrators remotely activate a

	device alarm.
Enable client uninstall protection	Specify whether or not a password is required in order to remove the agent from a device. • Select the 'Enable client uninstall protection' check box and specify a password in the text box. The ITSM agent can be uninstalled from any enrolled device only after entering the password.
Allow devices to access application repositories	If enabled, an 'Applications' bar will be visible on Android devices which will open a list of Android apps in the 'App Catalog'.

- Click 'Save' to apply your changes.

11.2.3.2. Configuring Android Client Antivirus Settings

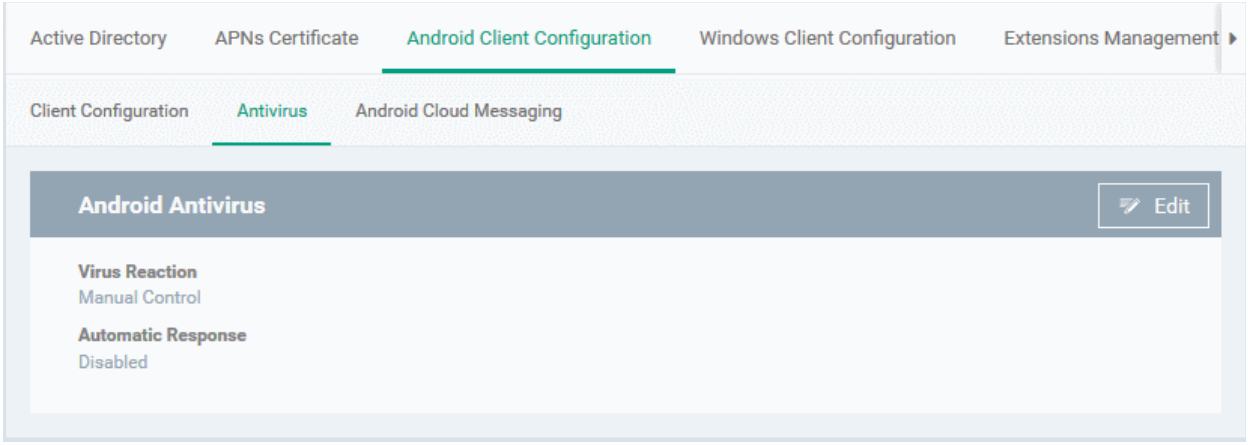
The Android Client Antivirus provides real-time protection against malware and malicious apps on Android devices. Administrators can also launch 'on-demand' scans from the ITSM administrative console on selected devices.

The antivirus settings area allows administrators to configure whether threats identified by the antivirus should be automatically removed or handled manually .

- If 'Automatic Control' is chosen, you should next choose your 'Automatic Action'. You have the choice to automatically uninstall the threat, or ignore it.
- If 'Manual Control' is chosen, the device status will change to 'Infected' in the console if a virus is found. A notification will also be shown on the device. The user can respond to the notification to manually remove the virus. Refer to the section **Running On-demand AV Scan on Android Devices** for more details.

To configure antivirus settings

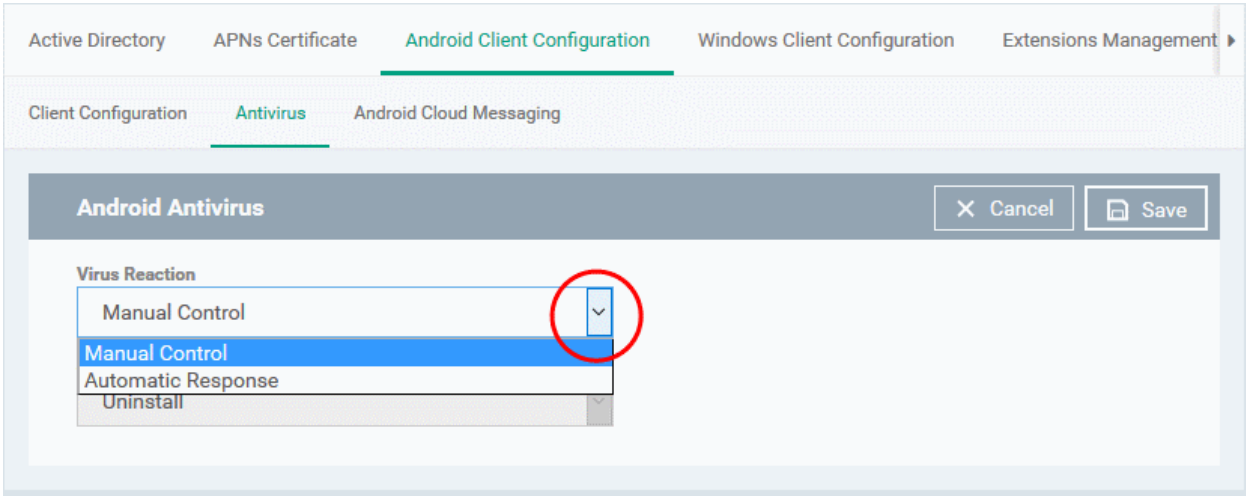
- Click 'Settings' on the left and select 'Portal Set-Up'.
- Click 'Android Client Configuration' at the top.
- Click the 'Antivirus' tab:



The current antivirus settings will be displayed.

- To change the settings, click the edit button 

at the top.



Android Client Antivirus Settings - Table of Parameters	
Parameter	**Description**
Virus Reaction	Choose the type of action to be taken if malware is discovered on the device. The options are: • Manual control • Automatic response If Manual Control is chosen, the administrators can take appropriate action on threats detected, from the AV Scan interface. Refer to the section Running On-demand AV Scan on Android Devices for more details.
Automatic Response	If 'Automatic Response' is chosen from the 'Virus Reaction' drop-down, select the action to be taken on the app identified as infected by ITSM. The options available are: • Uninstall • Ignore

- Click 'Save' for your settings to take effect.

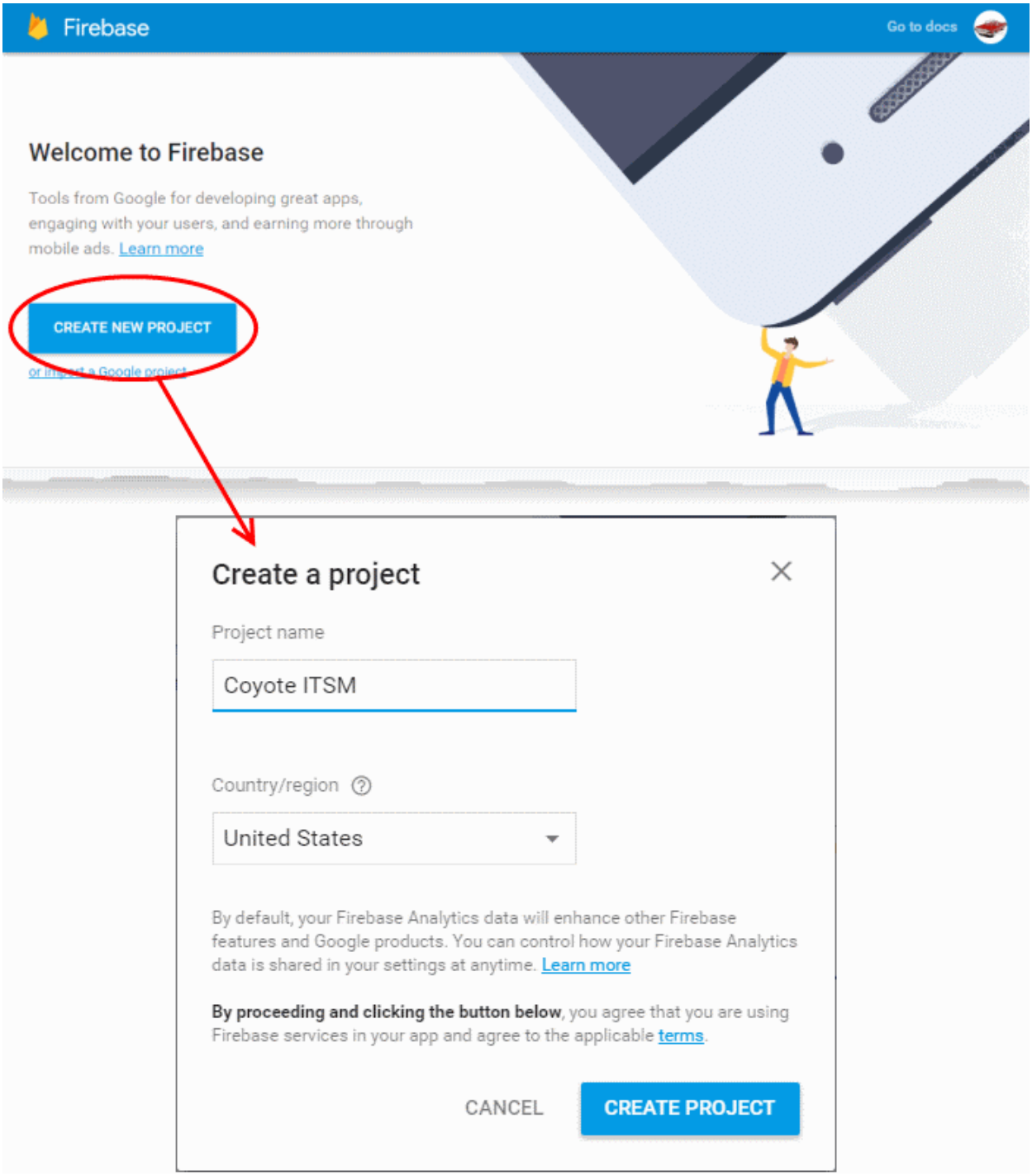
11.2.3.3. Adding Google Cloud Messaging (GCM) Token

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.

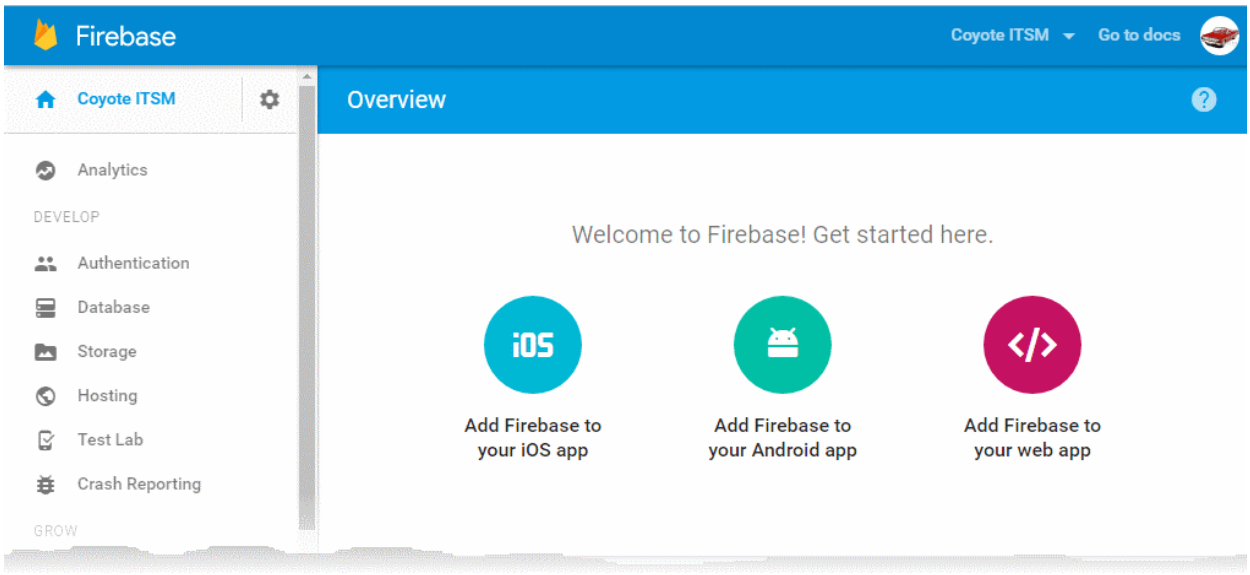
Step 1 - Create a New Project

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



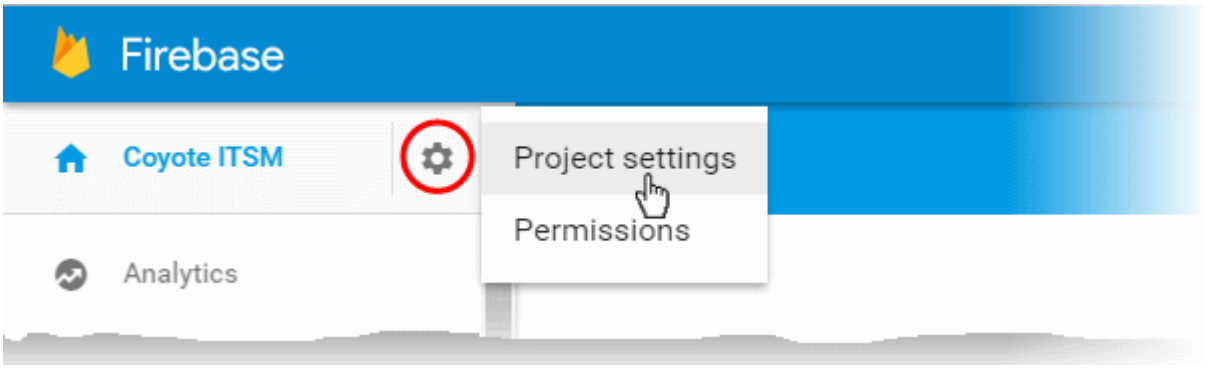
- Click 'Create Project'
- Type a name for the new project in the 'Project Name' field
- Select your country from the 'Country/region' drop-down
- Click 'Create Project'.

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



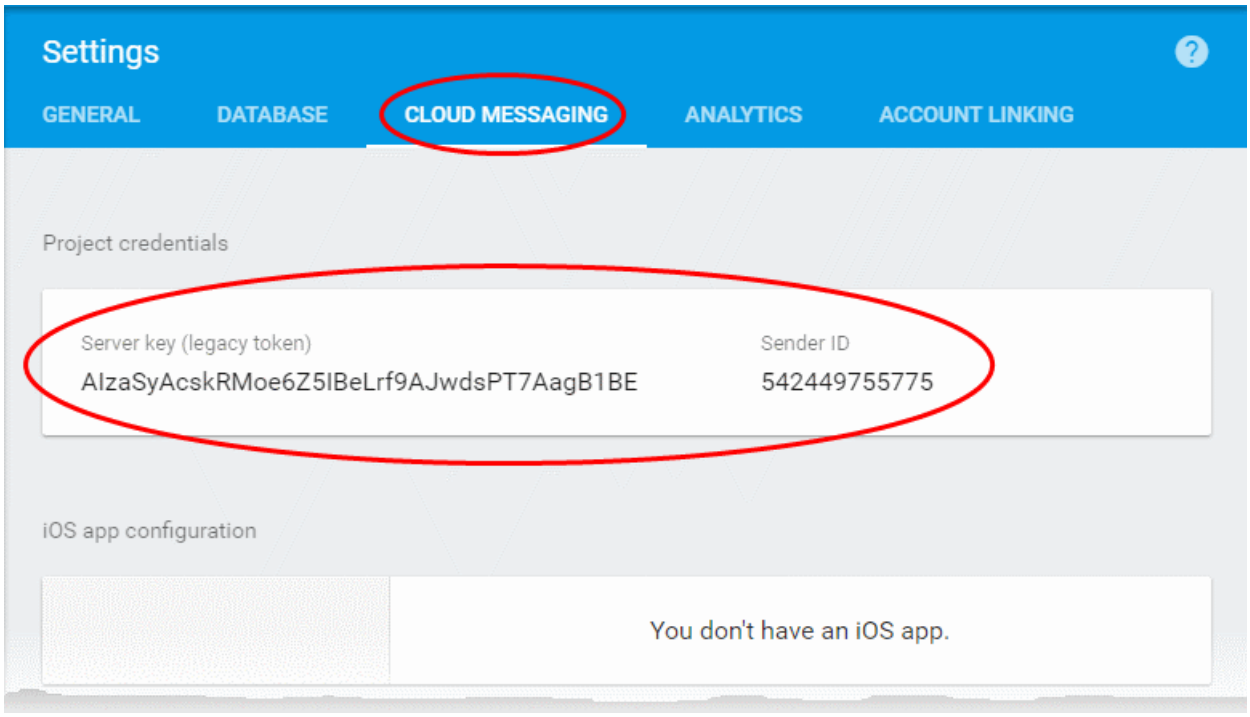
Step 2 - Obtain GCM Token and Project number

- 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.

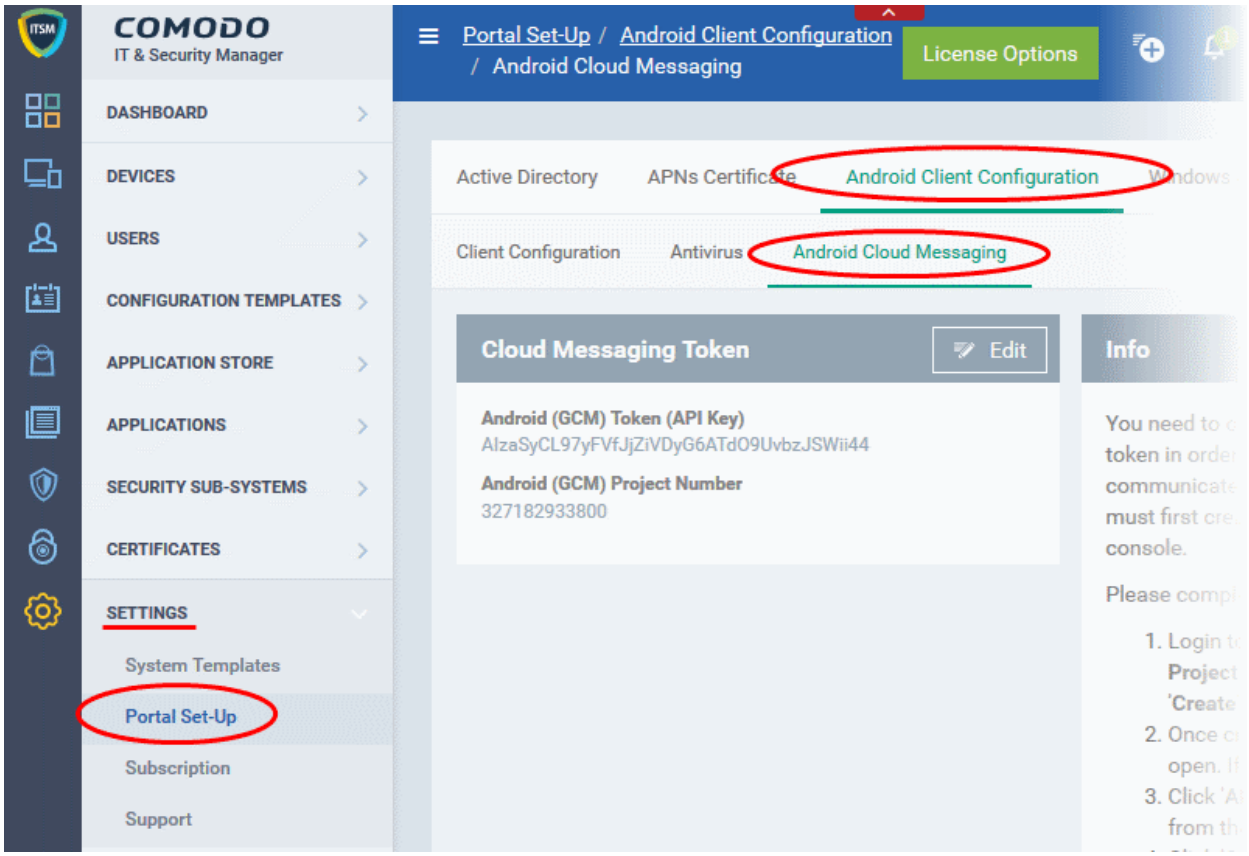
- Click the 'Cloud Messaging' tab from the top.



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

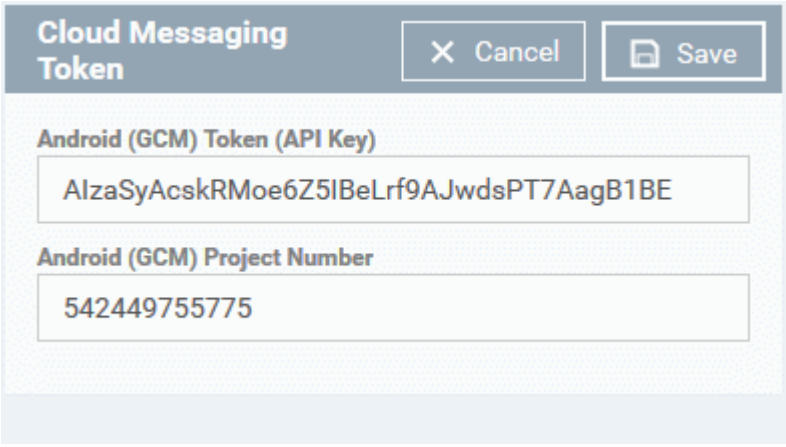
Step 3 - Enter GCM Token and Project number

- 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.

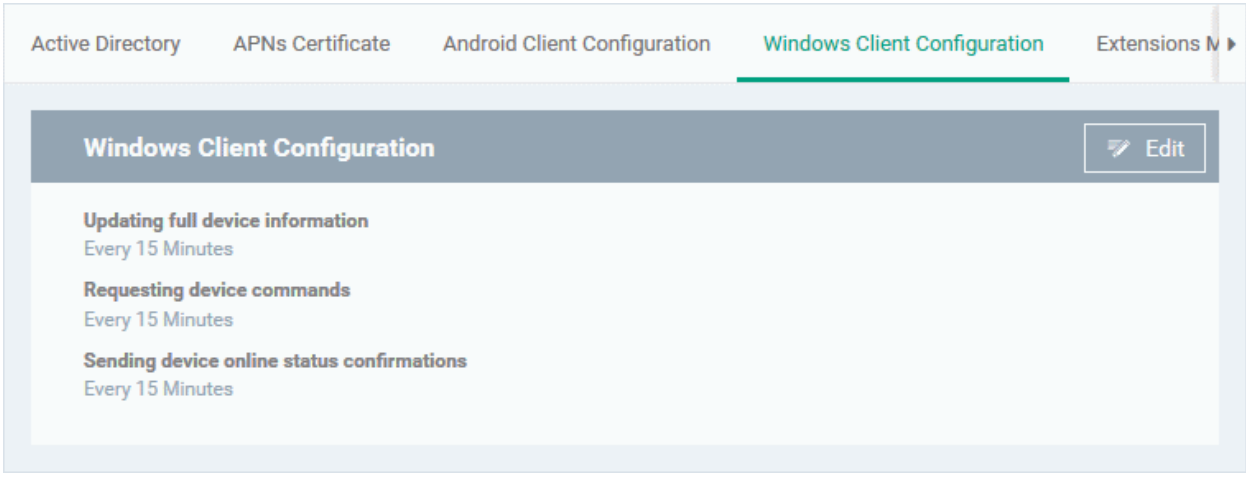
Your ITSM Portal will be now be able to communicate with Android devices using the unique token generated for your ITSM portal.

11.2.4. Configuring ITSM Windows Client

The 'Windows Agent Configuration' area allows you to configure time intervals for device information updates, and polling intervals for the agent to obtain commands from ITSM.

To configure the windows agent

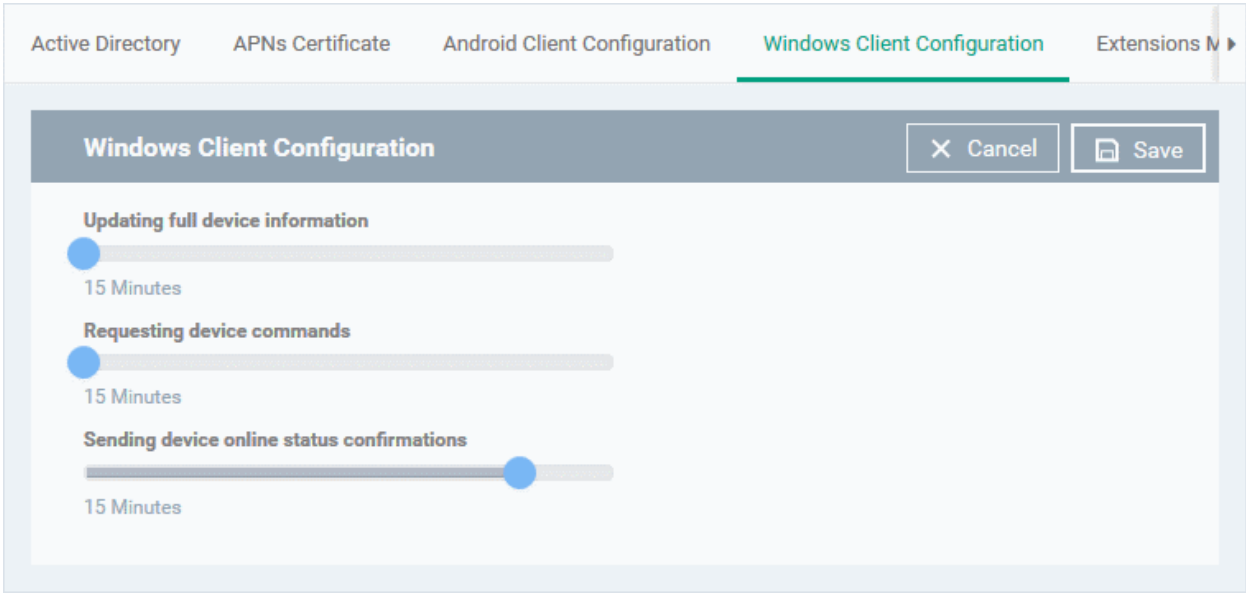
- Click 'Settings' on the left and select 'Portal Set-Up'
- Click 'Windows Client Configuration' at the top



The default values of the update intervals are displayed.

- Click the edit button  on the top right to modify these settings

The settings screen will be displayed.



Windows Agent Configuration Settings	
Parameter	**Description**
Updating full device information	Determines how often the device should provide ITSM with updates about its status. This includes, for example, memory status, name of the device, OS summary, security information from the CCS installation and network information. Use the slider to set the update interval. (Default = 15 minutes)
Request device commands	The time interval at which the agent on the device should poll the ITSM server to receive commands about, for example, updating configuration profiles, refreshing device information and so on. Use the slider to set the update interval. (Default = 15 minutes)
Sending device online status confirmations	The time period during which the agent on the device should send a message confirming that it is online and connected. If ITSM does not receive such a message for more than the set time period, it changes the device status to 'Offline'.

	Use the slider to set the update interval. (Default = 15 minutes)

- Click 'Save' to apply your changes.

11.2.5. Managing ITSM Extensions

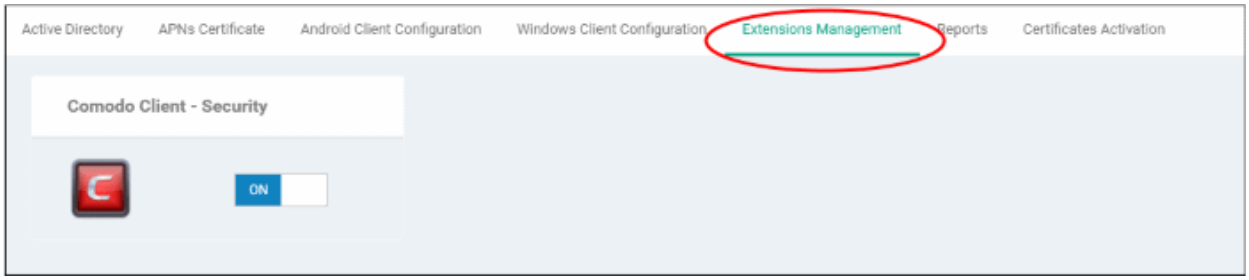
ITSM Extensions are additional software modules which administrators can add to ITSM to expand its functionality. Once added, each extension can be controlled and managed from the ITSM interface. The 'Extensions Management' interface allows administrators to enable or disable modules.

The extension currently available is:

- **Comodo Client Security** - Comodo Client Security is the remotely managed Client Security software installed on managed Windows devices. It offers complete protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, an advanced host intrusion prevention system (HIPS) and Containment feature that runs unknown and unrecognized applications in an isolated environment at the endpoints. CCS can be installed on the endpoints from the Devices interface. Refer to the section **Remotely Installing Packages onto Windows Devices** for more details. Once installed, CCS can be configured for optimal security by applying configuration profiles. Refer to the section **Profiles for Windows Devices** for more details.

To access the 'Extensions Management' interface

- Click 'Settings' on the left and select 'Portal Set-Up'
- Click 'Extensions Management' at the top



- Use the toggle switch in the respective tile to enable or disable the extensions. Please note only if the extension is enabled, this will available for deployment onto the selected endpoints from the Device List interface. Refer to the section '**Remotely Installing Packages onto Windows Devices**' for more details.

11.2.6. Configuring ITSM Reports

ITSM undergoes rigorous Quality Assurance testing before release to ensure that the software is as stable and reliable as possible. However, in rare situations, ITSM may run into an exception which needs to be addressed. If the report setting is enabled, an exception report will automatically be sent to Comodo if ITSM encounters a problem.

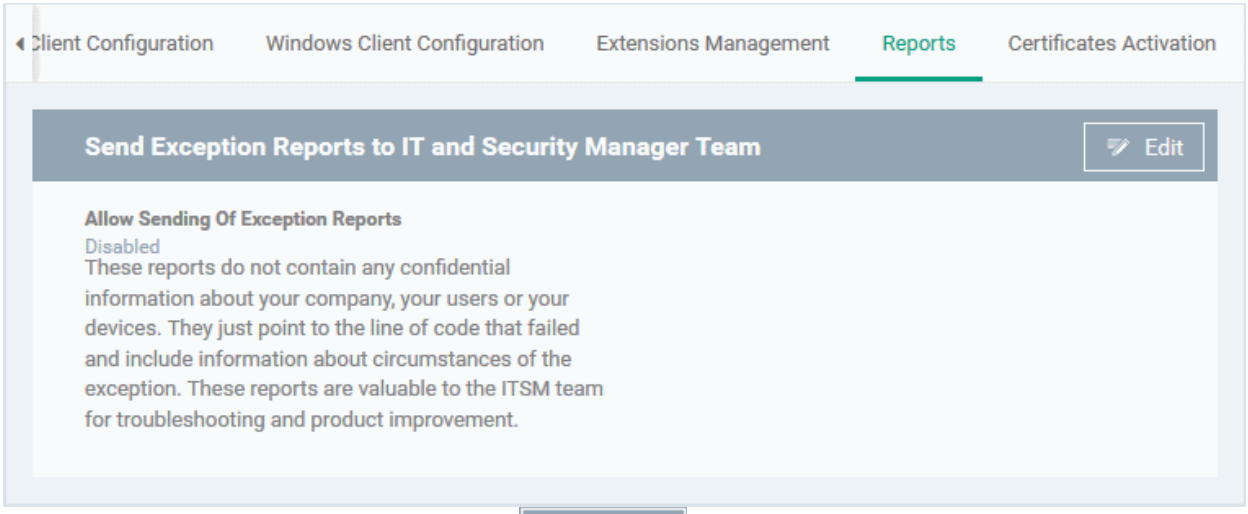
Exception reports are a valuable and constructive means of feedback that help Comodo to debug our products and improve the service we provide to our customers.

These reports contain only the line of code that failed with additional information about the circumstances of the exception. They do not contain any private information about your company or your users.

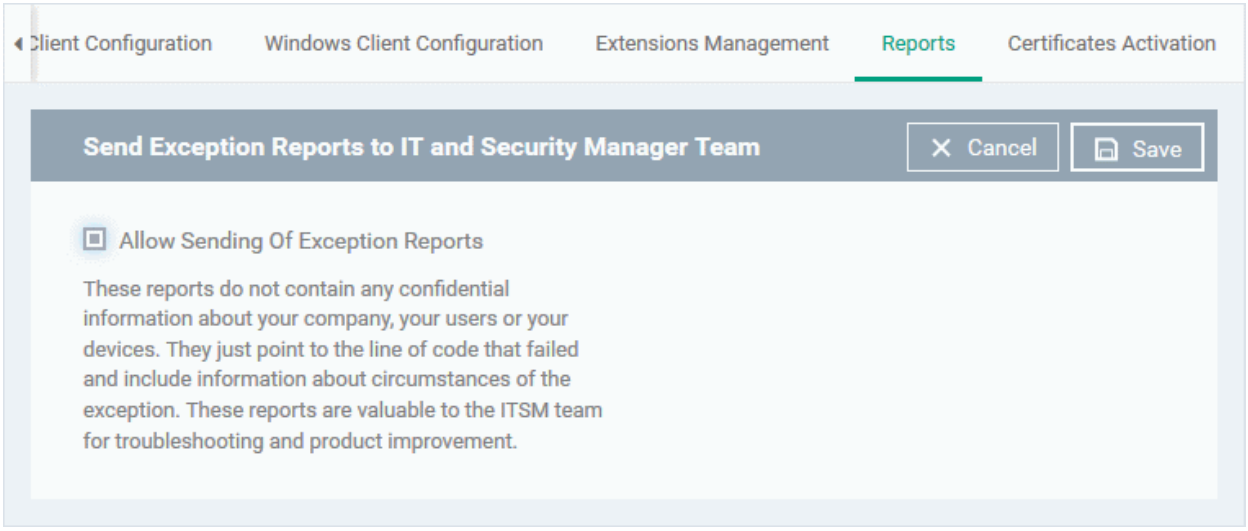
The 'Reports' interface allows you to enable or disable automated sending of exception reports. Automatic report submission is disabled by default.

To configure exception reporting

- Click 'Settings' on the left and select 'Portal Set-Up'.
- Click the 'Reports' tab



- To edit the settings click the edit button  at the top right.



- Select the 'Allow sending of exception reports' to allow the ITSM to send the error reports to 'Comodo'.
- Click 'Save' for your settings to take effect.

11.2.7. Integrating with Comodo Certificate Manager

ITSM allows administrators to integrate their Comodo Certificate Manager (CCM) account with ITSM to issue client certificates to end-users and device certificates to managed devices. These certificates can also be used for authentication for secure connection applications like VPN connections.

Administrators can add any number of CCM accounts from different CCM servers for different organizations. Certificates will be issued to end-users/devices by the CCM server with which the organization is associated.

Note 1: Please contact your Comodo Account Manager should you need a CCM account.

Note 2:: ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, issue client certificates, submit unknown files for analysis to Valkyrie, monitor Windows events and provide alerts. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in Appendix 1.

Once a CCM account is added, a new component will be added to your profiles called 'CCM Certificates'.

Administrators can configure client and device certificate requests in a profile which can be applied to enrolled devices. Once the profile is applied, a corresponding certificate request will be sent to CCM. CCM obtains the

certificate and sends it to ITSM which in turn pushes it to the agent on the device. The agent installs the certificate to the certificate store in the respective device.

The client certificate can also be used for email signing and encryption if it is imported into a user's mail client.

The rest of this section explains how to integrate your CCM account to ITSM.

Prerequisites:

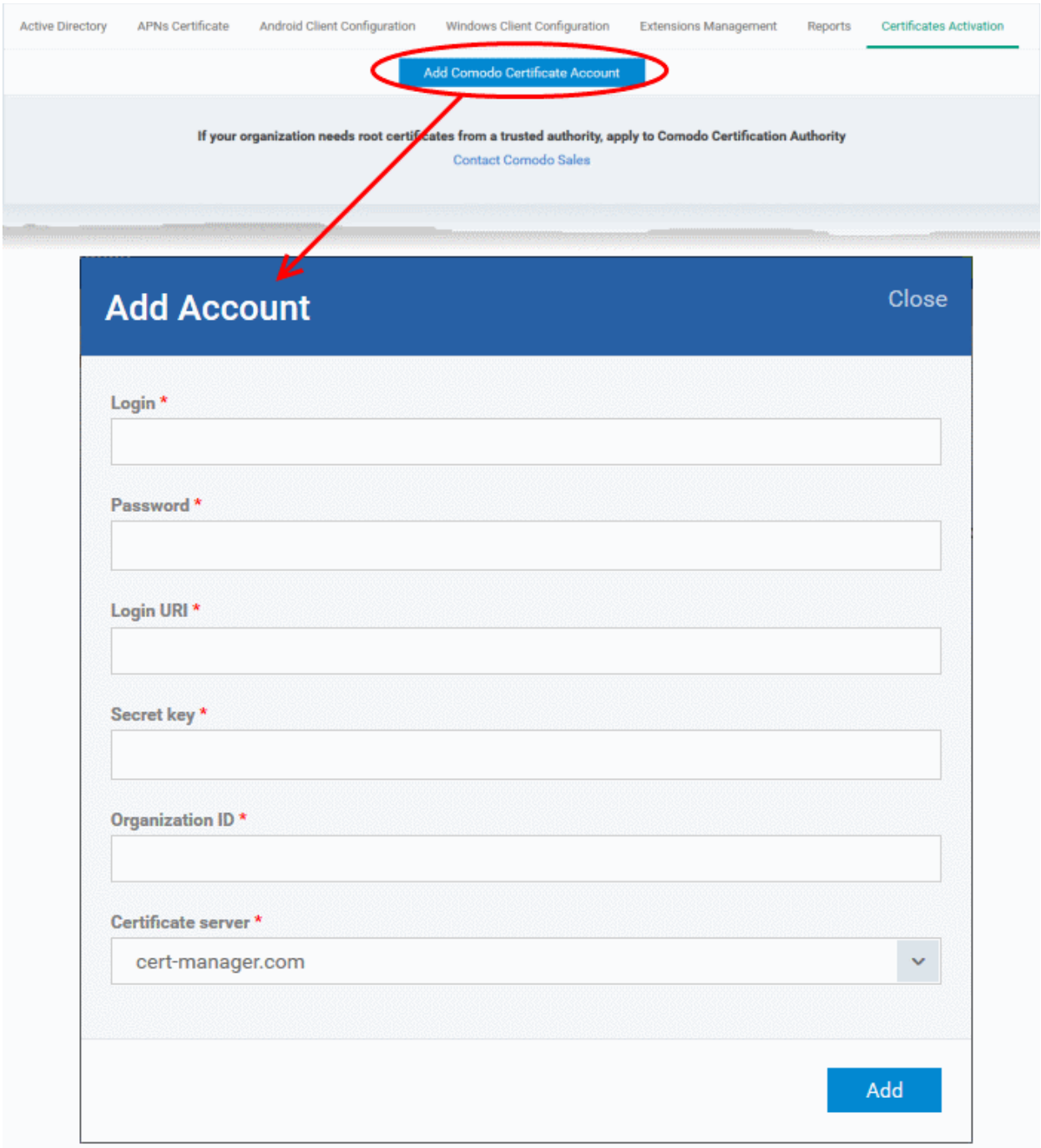
- The organization whose end-users/devices require certificates is added as an organization in CCM.
- The email domains used by end-users have been delegated to the organization in CCM.
- SMIME certificate enrollment through Web API has been enabled for the CCM organization, and a secret key has been set for Web API enrollment.

For help to add an organization to CCM and configure it for enrollment of client certificates through Web API, please see the following section in the CCM admin guide: https://help.comodo.com/topic-286-1-606-7511-Comodo-Certificate-Manager-MRAO.html.

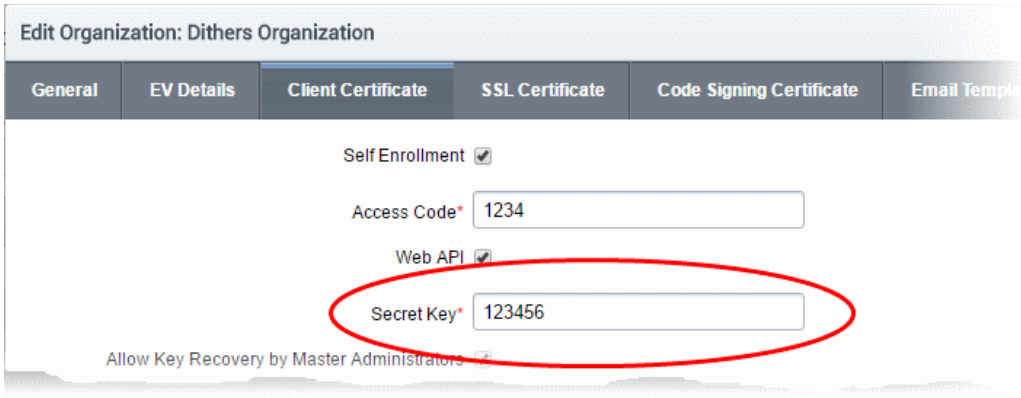
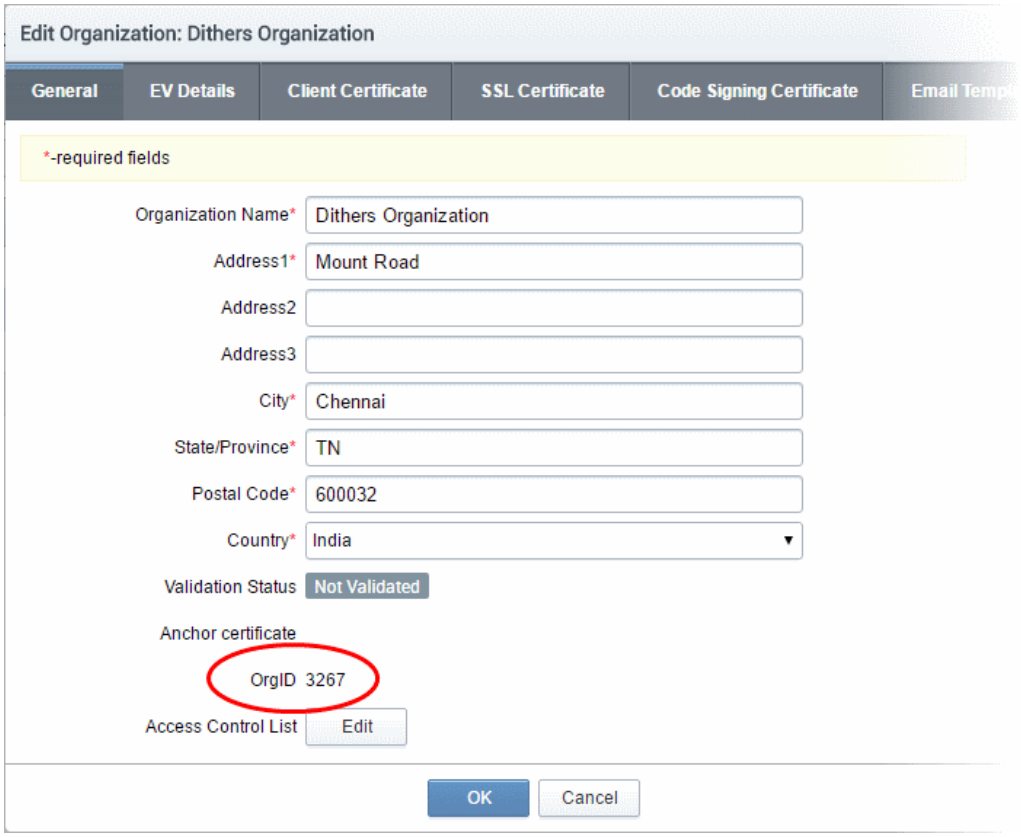
To add a CCM Account

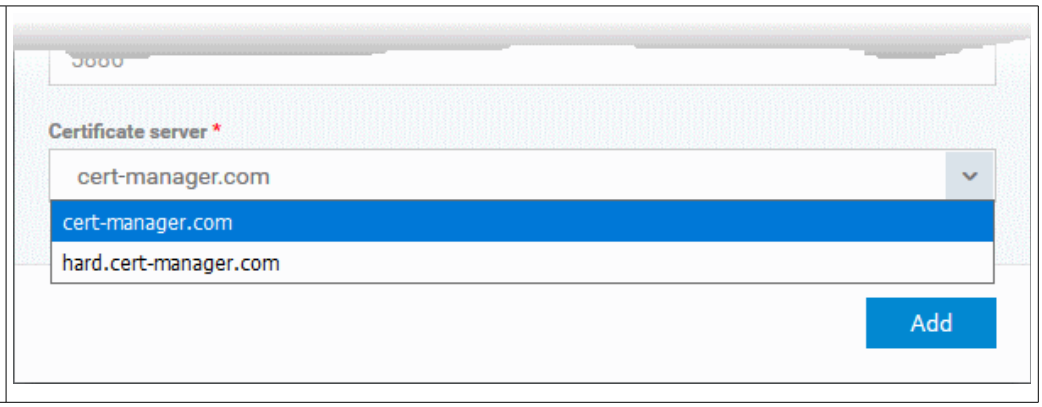
- Click 'Settings' on the left and select 'Portal Set-Up'
- Click the 'Certificate Activation' tab at the top
- Click 'Add Comodo Certificate Account'

The 'Add Account' dialog will open.



Add Account Dialog - Description of form parameters	
Field	**Description**
Login/Password	Enter the login credentials for the CCM MRAO Administrator account. This will allow ITSM to access CCM.
Login URI	Enter the customer URI of the CCM account which you wish to add to ITSM. Tip: The customer URI is the suffix of the URL used to access CCM. CCM URLs use the following format: https://cert-manager.com/customer/<customer URI> So if your URL is https://cert-manager.com/customer/examplecompany , then you would enter

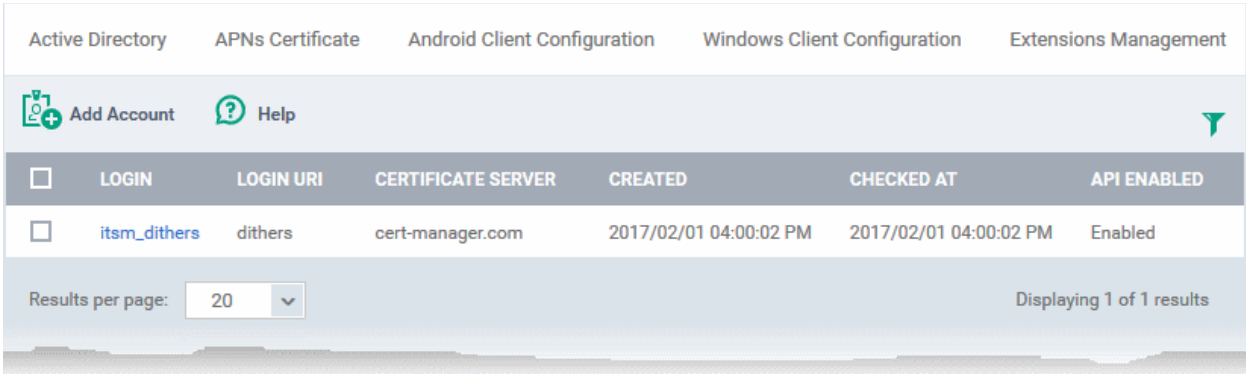
	'examplecompany' in this field.
Secret Key	Enter the secret key which has been set for the organization for Web API enrollment of client certificates. Tip: You can find the secret identifier in CCM from the 'Client Cert' tab of the Add/Edit organization dialog:  For more details, see the following section of the CCM admin guide: https://help.comodo.com/topic-286-1-606-7511-Comodo-Certificate-Manager-MRAO.html.
Organization ID	Enter the ID of the organization to which certificates are to be issued from this CCM account. Tip: You can identify the organization id in CCM from the 'General' tab of the 'Edit Organization' dialog of the organization:  For more details, see https://help.comodo.com/topic-286-1-606-7511-Comodo-Certificate-Manager-MRAO.html.
Certificate Server	Choose the CCM server at which you have your CCM account subscription:



- Click 'Add' after completing the form.

The CCM account will be added to ITSM. ITSM will now be able to issue client certificates to users of Windows devices. You can also issue device certificates by applying a suitably enabled profile to the device.

The CCM account will be listed in the interface as follows:



Certificates Activation - Column Descriptions	
Column Heading	**Description**
Login	The username of the MRAO Administrator account for ITSM to login to CCM. Clicking the username displays the account details like the login URI and the Organization ID of the organization to which certificates are issued from this account.
Login URI	The real customer URI of the CCM account.
Certificate Server	The CCM server from which the account is subscribed. The certificates will be issued only from this server,
Created	The precise date and time at which the CCM account was added to ITSM by the administrator.
Checked at	The precise date and time at which the ITSM logged-in to the CCM account.
API Enabled	Indicates whether the organization is enabled for procuring client and device certificates from CCM through API integration

- To add more CCM accounts, click Add Account at the top left and repeat the process as explained above.

11.2.8. Setting-up Administrator's Time Zone

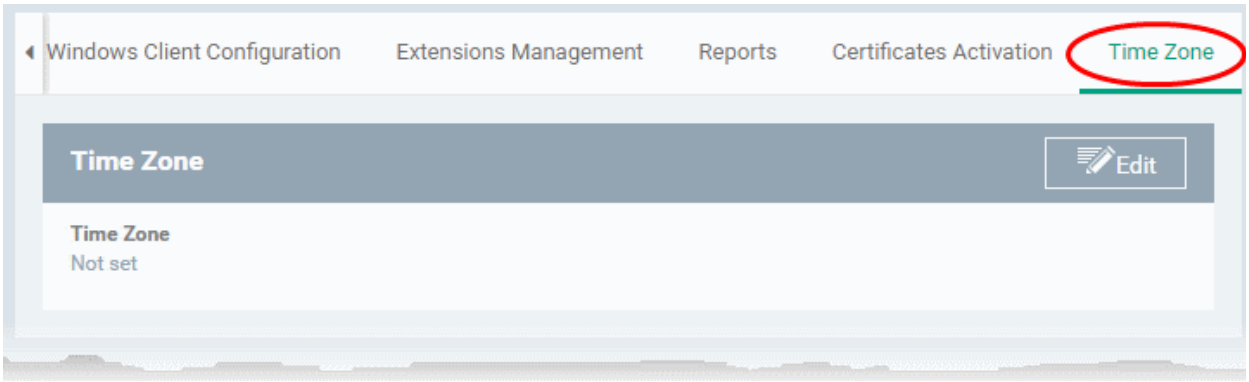
Administrators can set their time zone so that ITSM interfaces and logs will be displayed to each administrator using their local time.

Note. Administrators added through Comodo One must set their time zone in the C1 console. Only administrators added through the ITSM console and who login using the dedicated ITSM URL can set their time zone in the ITSM console.

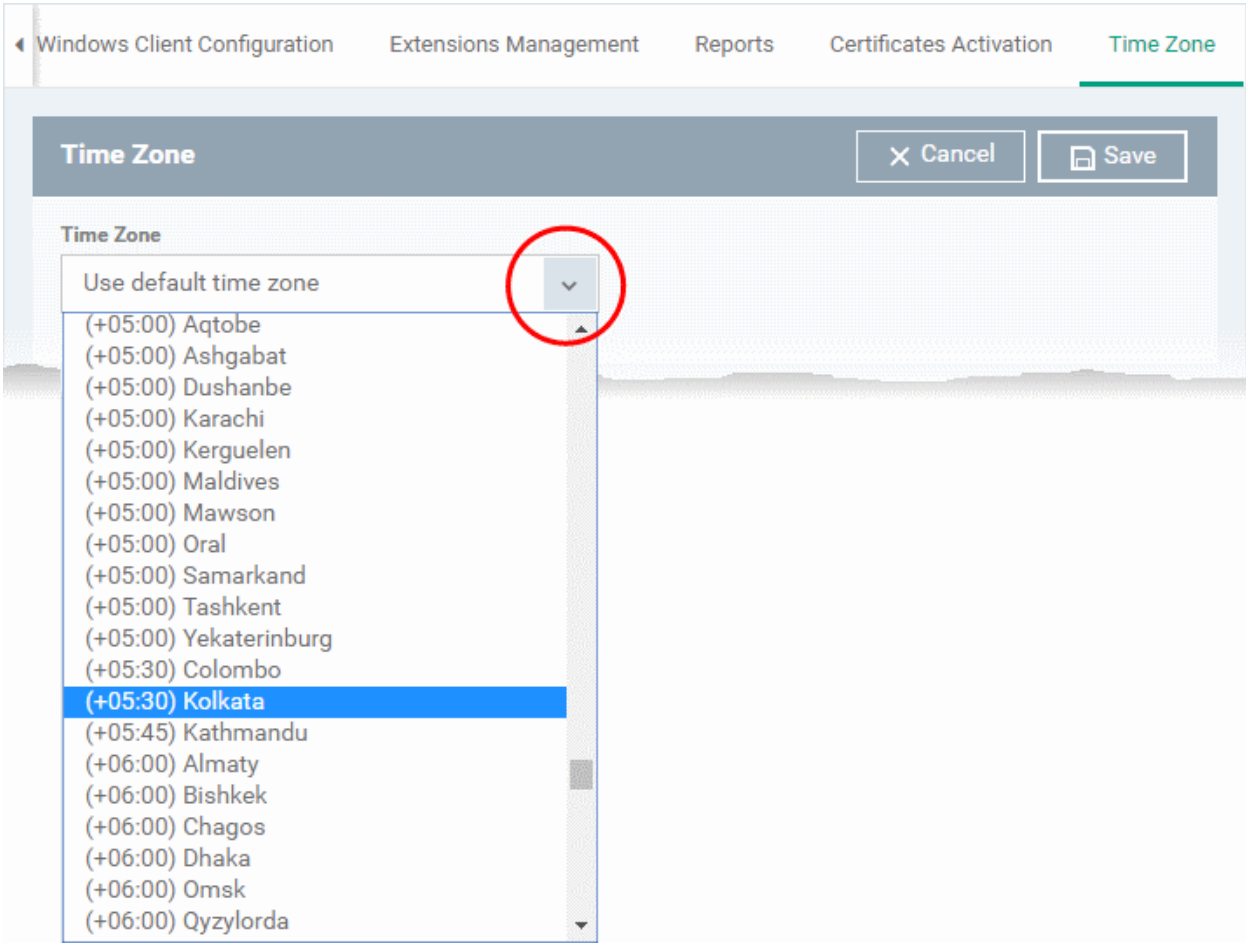
To set your time zone

- Click 'Settings' on the left and select 'Portal Set-Up'
- Click the 'Time Zone' tab at the top

Note: The 'Time Zone' tab will be available only if you have logged-in to ITSM through the dedicated URL for the ITSM console and will not be available if you have logged-in through the Comodo One console.



- Click 'Edit' at the top right



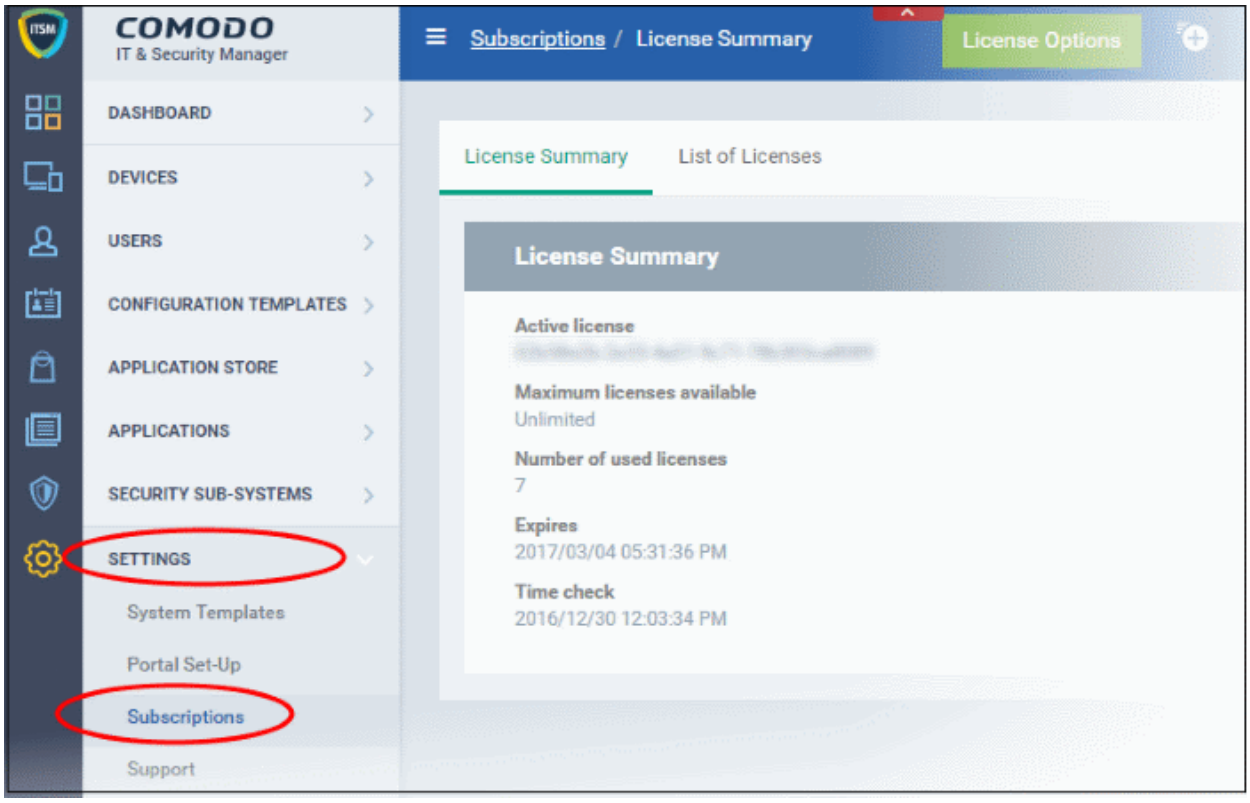
- Choose your time zone from the 'Time Zone' drop-down and click 'Save'.

Your time zone will be updated. All logs and time indications in the ITSM interface will be displayed based on the set time zone. You can change the time zone settings at anytime following the same process.

11.3. Viewing and Managing Licenses

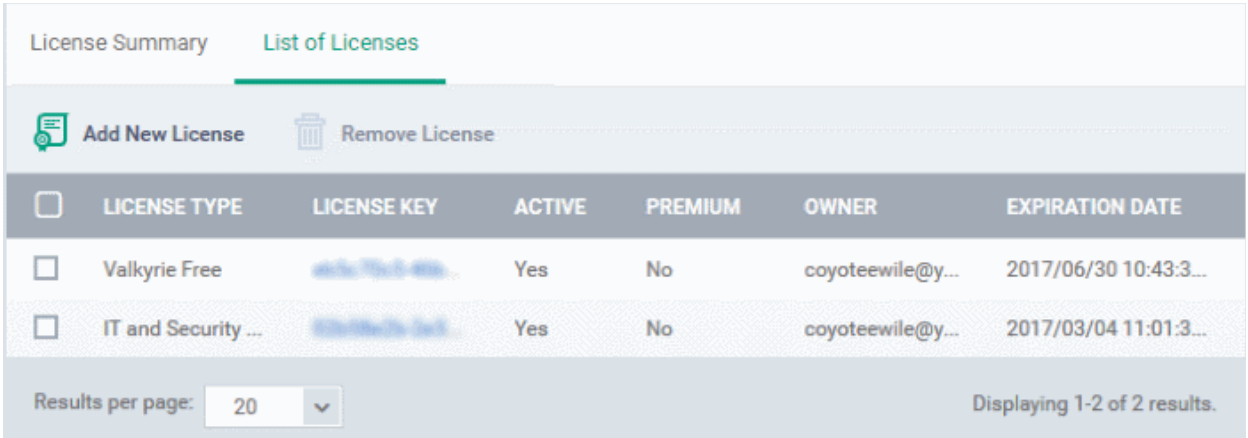
The 'Subscriptions' interface displays details about licenses purchased, their type and validity status and the number of users and devices allowed on each. The 'Subscriptions' screen also allows the administrator to add new licenses.

- To open the 'Subscription' interface, choose 'Settings' from the left and select 'Subscription'.

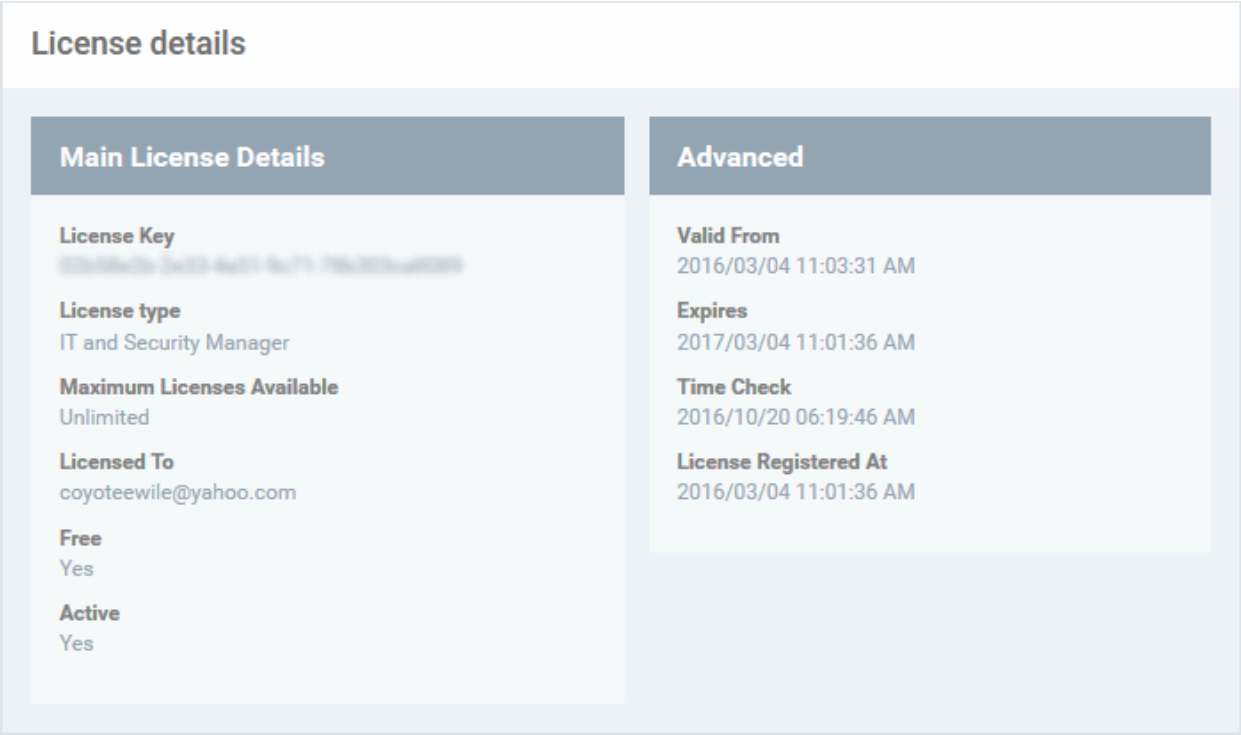


It contains two tabs:

- **License Summary** - Displays a summary of details of your currently active license(s). An example is shown above.
- **List of Licenses** - Displays a list of licenses purchased so far with their details.



- Clicking on the license key will display the details of the license.



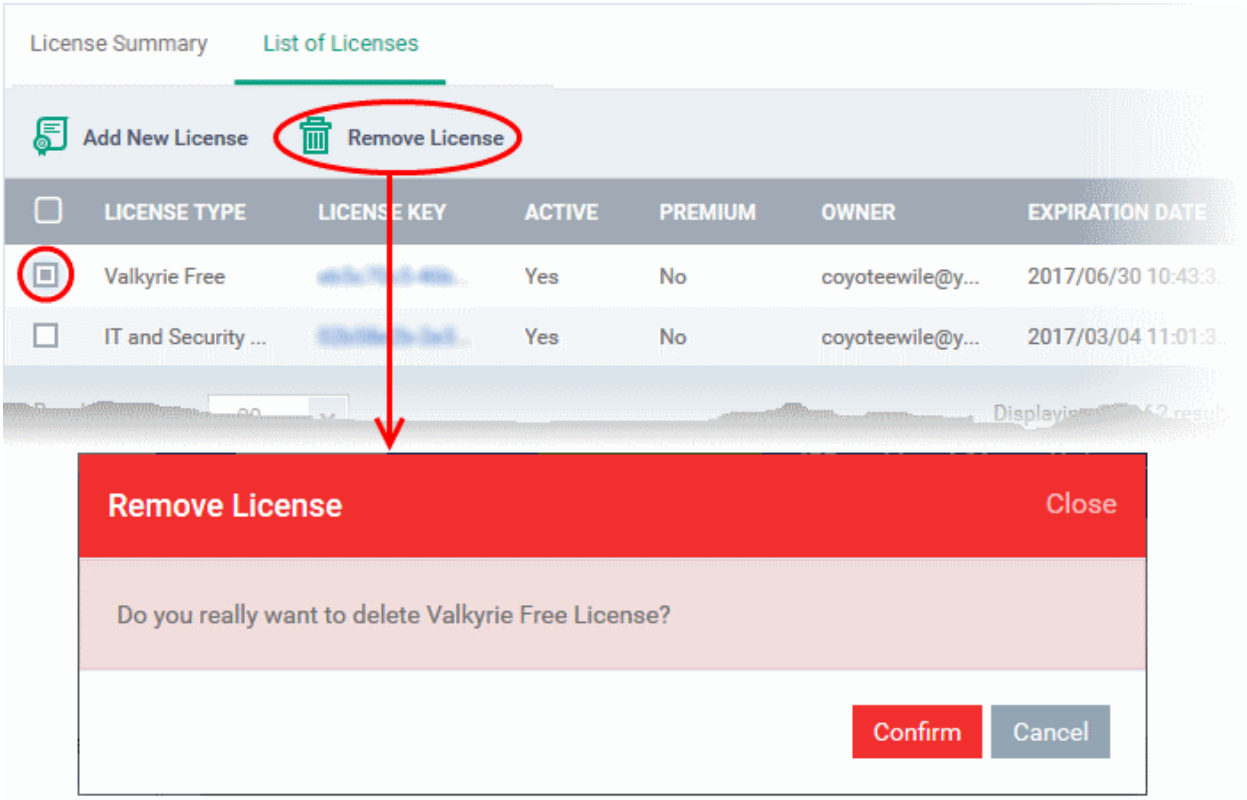
The next section **Upgrading or Adding the License** provides more details on upgrading your license for adding more number of users and renewing your license.

Removing Licenses

You can remove expired or the licenses that you do not want to use, from the list

To remove a license

- Select 'Settings' from the left and select 'Subscriptions'
- Click on 'List Of Licenses' tab to open the 'Subscriptions/List of Licenses interface
- Select the license to be removed
- Click 'Remove License' from the top of the 'List of Licenses' interface



- Click 'Confirm' that appears in the Remove License dialog.

The license will be removed from the list.

11.3.1. Upgrading or Adding a License

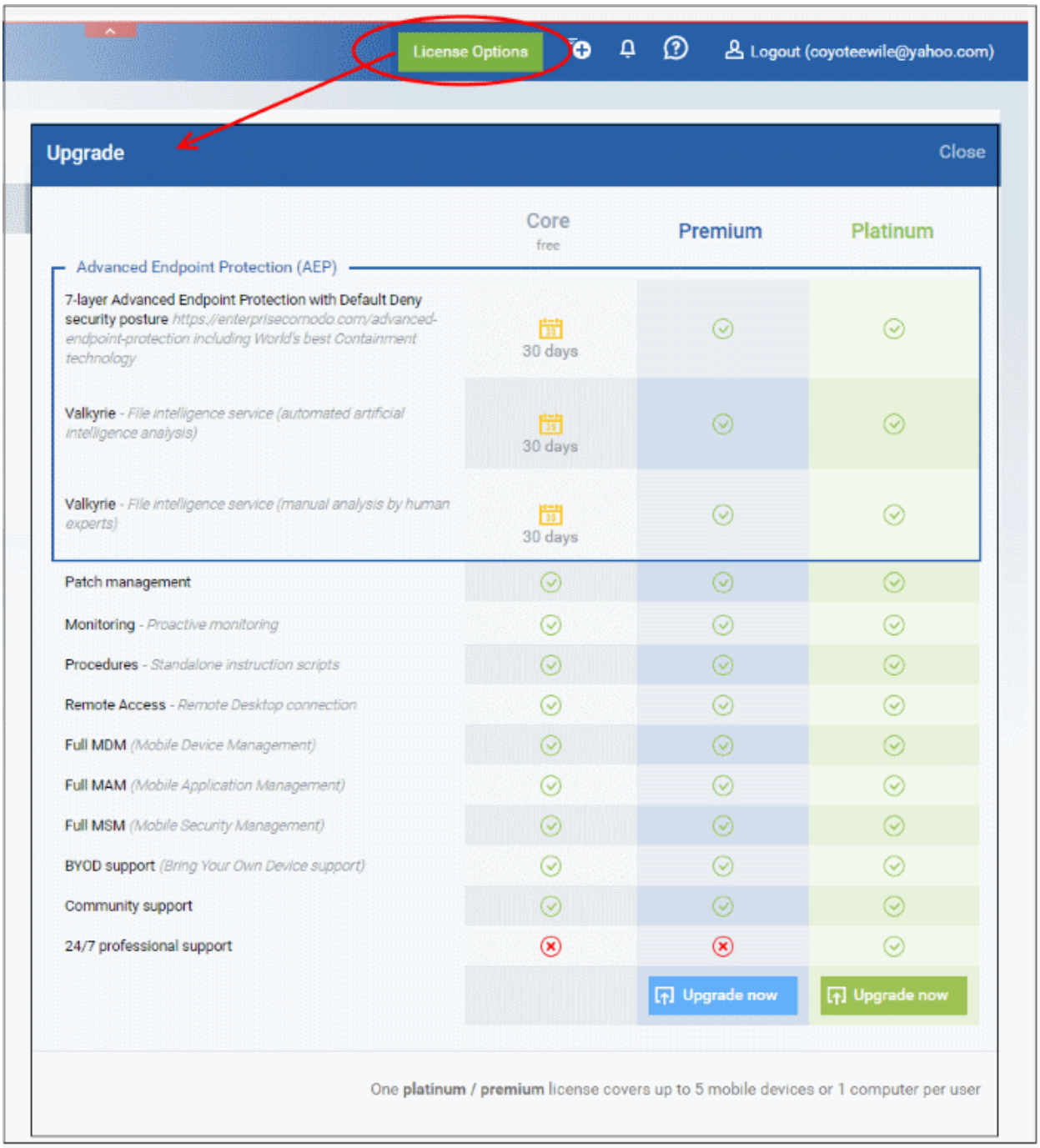
Administrators can add more users to their account by upgrading their license in the Comodo account management portal.

To upgrade a license

- Log in at https://accounts.comodo.com with your Comodo username and password
- Select 'IT and Security Manager' and complete the purchase process.

Your license key will be sent via email to your registered email address.

Alternatively, click 'License Options' at the top of the ITSM interface



The 'Upgrade' screen will be displayed which lists the features of 'Premium' and 'Platinum' licenses.

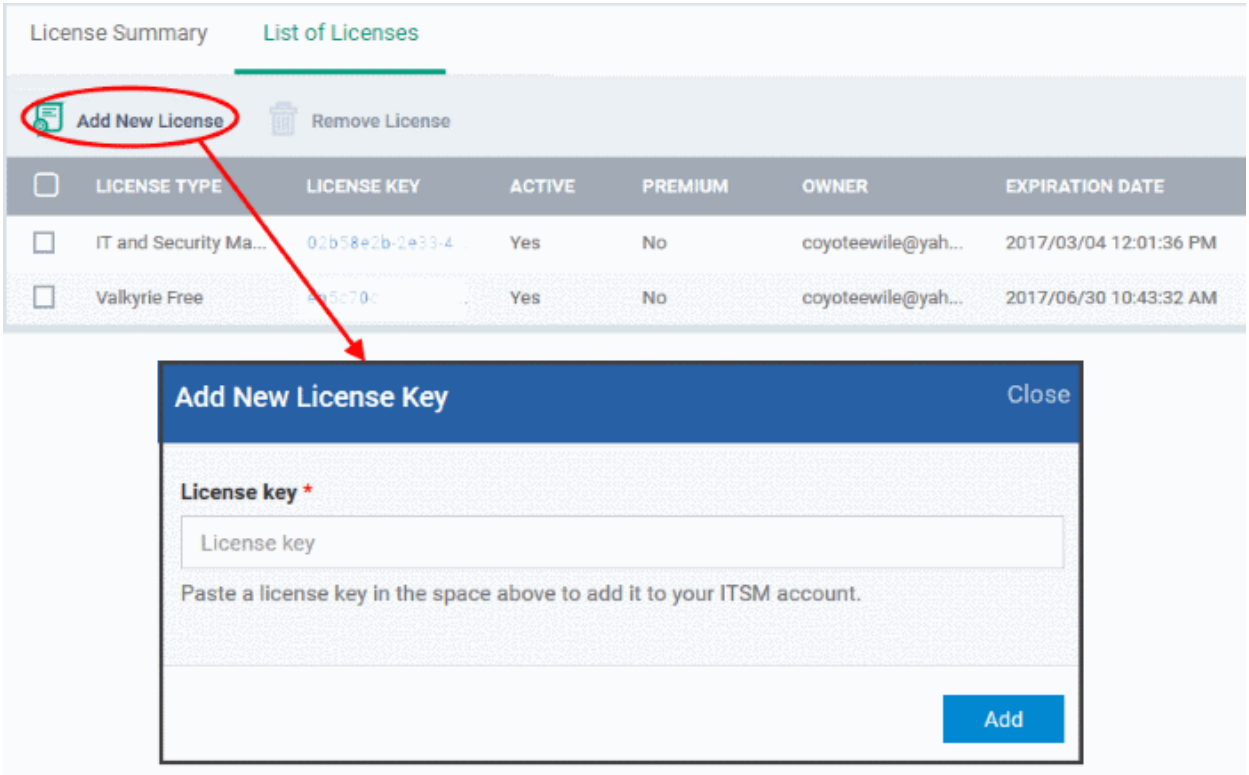
- Click 'Upgrade Now'

You will be directed to the C1 management portal to complete the purchase process.

Once you have obtained a new license, you need to register it in the interface.

To add a new license

- Select 'Settings' from the left and select 'Subscriptions'
- Click the 'List of Licenses' tab to open the 'Subscriptions/List of Licenses' interface
- Click 'Add New License' at the top left.



- Enter the license key from your license confirmation email.
- Click 'Add'.

Your new license will be activated. The license key will be displayed under the 'License Key' column.

- To view the license details and activation status, click on the license key.

New License

Please ensure to validate your license within 10 days of registration and to start using ITSM. Otherwise, access to ITSM may be blocked.

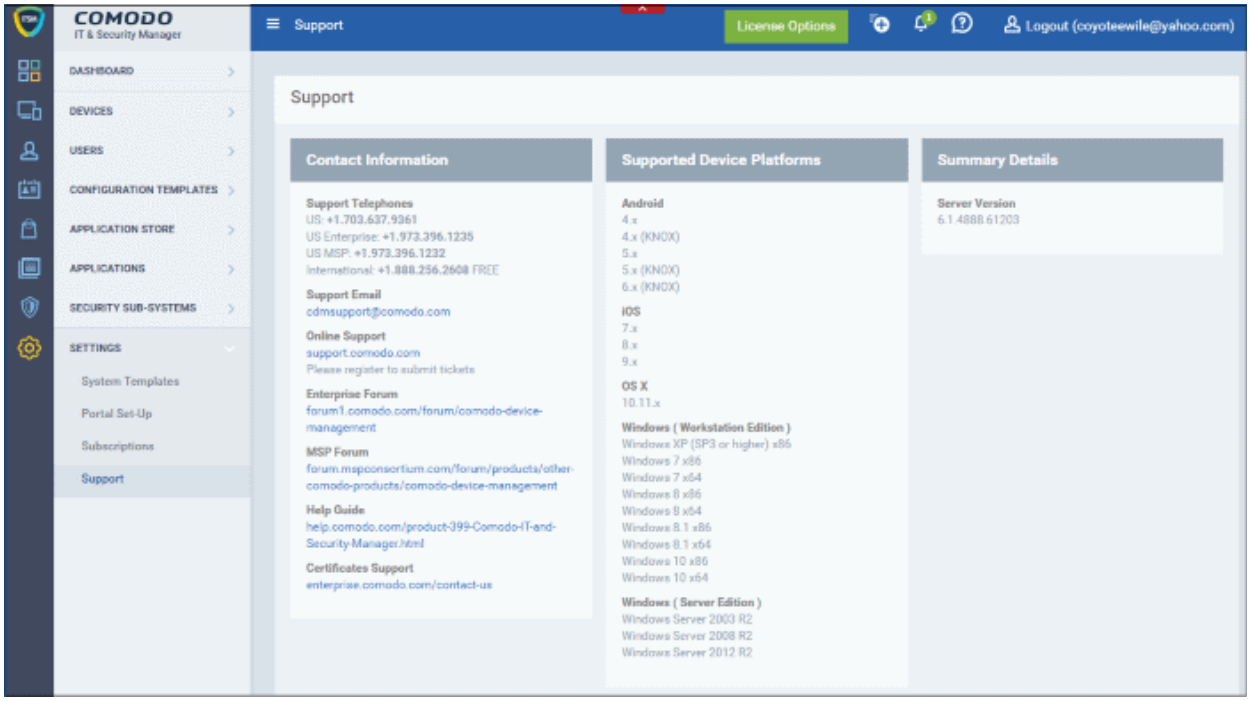
Renewal

Make sure to renew your license before expiry and activate it. If the license is not renewed, admins will have access to the ITSM management portal for 30 days only after the expiry of the license. After this grace period, access to the ITSM will be blocked.

11.4. Viewing Version and Support Information

The 'Support' panel displays support contact information, the current product version number, and contains a list of platforms supported by this version of ITSM.

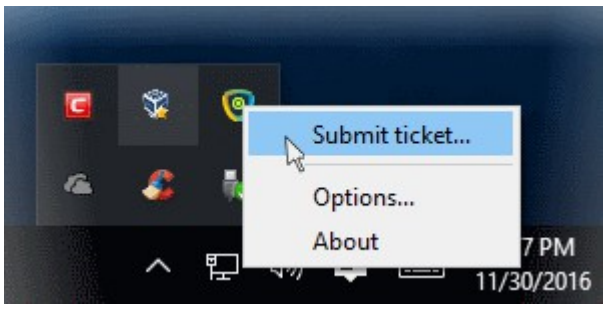
- To open the 'Support' pane, click 'Settings' at the left and select 'Support'.



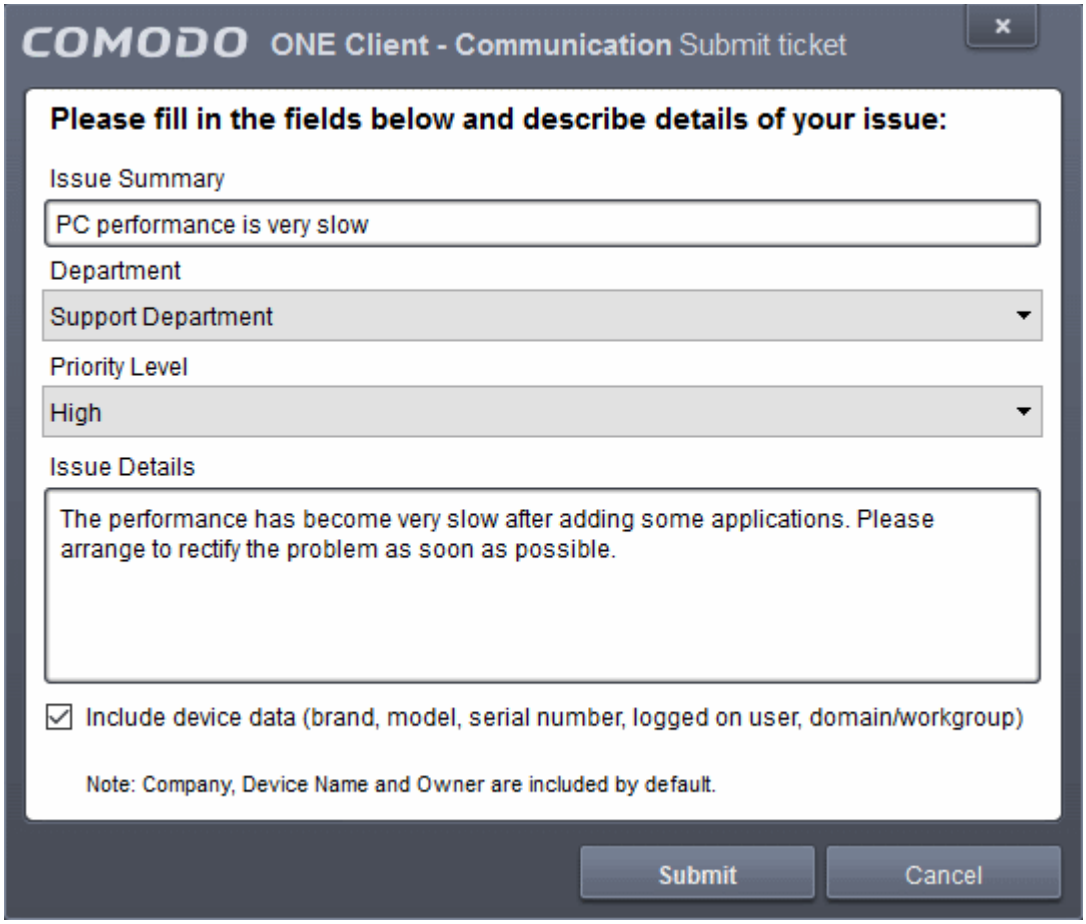
- **Contact Information** - Displays the telephone numbers and email addresses for contacting Comodo for purchasing new licenses and product support.
- **Supported Device Platforms** - Displays the list of types of devices that can be managed by ITSM, with their supported OS versions.
- **Summary Details** - Displays the version number of ITSM server.

Users also can create a support ticket from the Comodo Client - Communication (ITSM agent) tray icon on Windows and Mac OS X devices. A ticket will be created in Service Desk and assigned to the selected department.

- To submit a support ticket, right click the ITSM agent tray icon and click 'Submit ticket...'



The 'Submit ticket' dialog will be displayed



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

- Click 'Submit'.

A support ticket will be created in the Service Desk module of the C1 account and assigned to the selected department.

Appendix 1: ITSM Services - IP Nos, Host Names and Port Details

ITSM communicates with Comodo servers, agents installed on devices, Comodo Client - Security and Comodo Antivirus for Mac (CAVM) in order to update data, submit files for analysis and so on. You need to configure your firewall accordingly to allow these connections. The following table provides details for Comodo Client - Communication, ITSM Server (on premise installation) and Comodo Client - Security.

Comodo Client - Communication (CCC)

Comodo Client - Communication (CCC)				
Service	**Purpose**	**Hostname**	**IP**	**Port**
CCC	Communication between device and ITSM server	*subdomain*.cmdm.comodo.com	Dynamic (Amazon load balancing)	443
Enrollment	To get client certificates	mdmsupport.comodo.com	54.93.214.133	443
Monitoring and alerts	Access to Monitoring and alerts server	plugins.cmdm.comodo.com	Dynamic (Amazon load balancing)	443
File rating management	Access to Local Verdict Server	*subdomain*.cmdm.comodo.com	Dynamic (Amazon load balancing)	444
Windows push service (XMPP)	Device communication (push messages)	*subdomain*.cmdm.comodo.com	Dynamic (Amazon load balancing)	5222
LDAP synchronization	Synchronization with LDAP via device	User's LDAP server host	User's LDAP server IP	389 636 (LDAPS)
SSO	Single Sign On	one.comodo.com	69.4.89.244	443

Comodo Client - Security (CCS)

Comodo Client - Security (CCS)					
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Protocol**
FLS	FLS lookup	fls.security.comodo.com	91.209.196.27 91.209.196.28 199.66.201.20 199.66.201.21 199.66.201.22 199.66.201.25 199.66.201.26	4447	UDP
	FLS lookup	fls.security.como	91.209.196.27	4448	TCP

		do.com	91.209.196.28 199.66.201.20 199.66.201.21 199.66.201.22 199.66.201.25 199.66.201.26		
	FLS TCP keep alive	fls.security.comodo.com	91.209.196.27 91.209.196.28 199.66.201.20 199.66.201.21 199.66.201.22 199.66.201.25 199.66.201.26	4442	TCP
Valkyrie	Valkyrie lookup	valkyrie.comodo.com	178.255.87.4	443	HTTPS
	Submit to Valkyrie	valkyrie.comodo.com	178.255.87.4	443	HTTPS
CAMAS	Submit to CAMAS	usfftp.security.comodo.com	199.66.200.132 199.66.201.19 91.212.12.70	21 2118 2116 217 2117	FTP
		cima.security.comodo.com	199.66.201.27	80	HTTP
cdn.download.comodo.com	Update / upgrade mirror	cdn.download.comodo.com	104.16.61.31 104.16.60.31	80	HTTP
		cdn.download.comodo.com	104.16.61.31 104.16.60.31	443	HTTPS
download.comodo.com	Update/ upgrade (Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by the CDN provider, and those IP addresses do change)	download.comodo.com	178.255.82.5	80	HTTP
		download.comodo.com	178.255.82.5	443	HTTPS

ITSM Server (on premise installation)

ITSM Server (on premise)				
Service	**Purpose**	**Hostname**	**IP**	**Port**
E-mail	Connection to the configured SMTP server for e-mail sending	SMTP server hostname	SMTP server IP	25
LDAP synchronization	Direct synchronization with LDAP	User's LDAP server host	User's LDAP server IP	389 636 (LDAPS)
Connection to Comodo Accounts Manager	License verification	https://accounts.comodo.com	91.199.212.166	443
Google Cloud Messaging	To push messages	https://android.googleapis.com/gcm/send	Dynamic	443
Connection to Apple Push Notification Server	To push messages	https://gateway.push.apple.com	Dynamic	2195 2196 80 443
Local Verdict Server	File rating management	ITSM server hostname	ITSM server IP	444

If you require more details about firewall configuration, please contact mdmsupport@comodo.com.

Appendix 2: Pre-configured Profiles

ITSM ships with the following pre-configured configuration profiles:

- Optimum Windows Profile for ITSM (default profile)
- Standard Windows Profile for ITSM
- Hardened Windows Profile for ITSM
- Optimum OSX Profile for ITSM (default profile)
- Optimum IOS Profile for ITSM (default profile)
- Optimum Android Profile for ITSM (default profile)

Important Settings in preconfigured Windows profiles are given in the table below.

Section	Optimum	Standard	Hardened
Containment Rule	• Will contain all unknown executables	Internet born threats: • standard policy (Rules from Recommended Windows Profile for ITSM) • contain all unknowns with file age - less than 2 days • as a last rule of that policy ignore all unknowns with logging)	• Will contain all unknown executables
HIPS	Disabled	Disabled	Enabled (Safe mode, Block - default action, Enabled Enhanced Protection Mode)
Firewall	Enabled (Safe mode, Block - default action)	Enabled (Safe mode, Allow - default action)	Enabled (Safe mode, Block by default)
VirusScope	Enabled (Contained applications only)	Enabled (Contained applications only)	Enabled (All applications)
File Rating	Enabled Detect potentially unwanted applications	Enabled Detect potentially unwanted applications	Enabled Detect potentially unwanted applications

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.