Comodo

IT and Security Manager

Software Version 6.17

Administrator Guide

Guide Version 6.17.041318

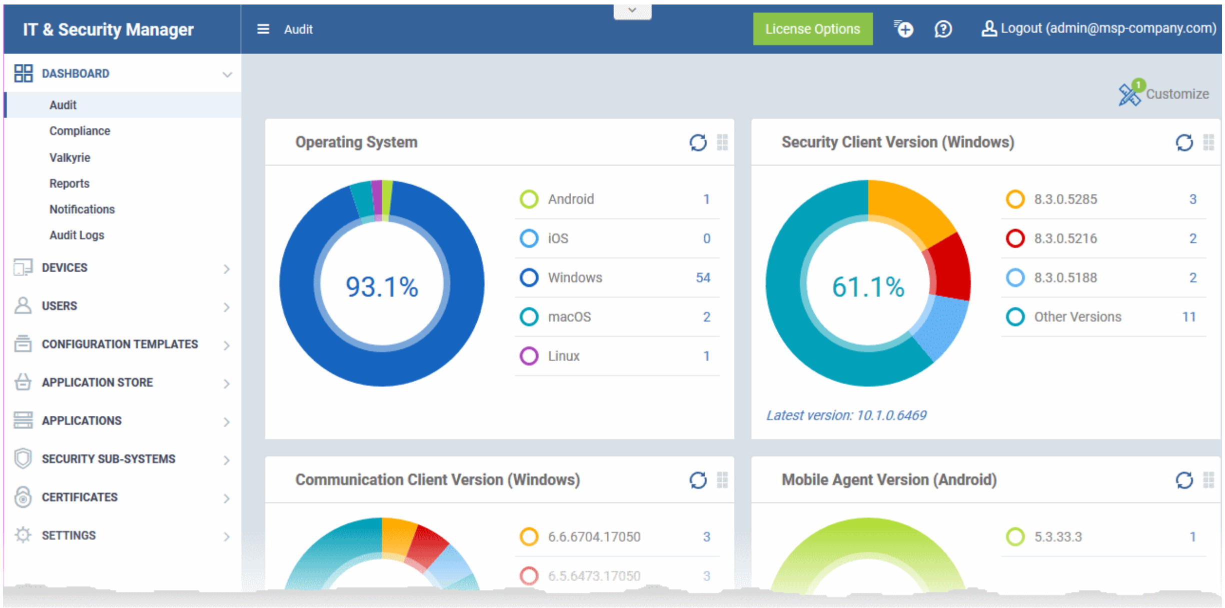
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

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/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 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.



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 used.

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 and Device Groups - 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.

- Managing Device Groups
    - Creating Device Groups
    - Editing a Device Group
    - Assign Configuration Profiles to a Device Group
    - Remove a Device Group
- Managing Devices
    - Managing Windows Devices
    - Managing Mac OS Devices
    - Managing Android/iOS Devices
    - Viewing User Information
    - Removing a Device
    - Remote Management of Windows Devices
    - Applying Procedures to Windows Devices
    - Remotely Installing and Updating Packages on Windows Devices
    - Remotely Installing Packages on Mac OS Devices
    - Installing Apps on Android/iOS Devices
    - Generating an Alarm on Devices
    - 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
    - Changing the ownership status of a Device
- Bulk Enrollment of Devices

- 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
- Enroll Android and iOS Devices of AD Users

Configuration Templates - Covers creation and management of configuration profiles to be applied to enrolled iOS and Android Smartphones and Tablets and Windows endpoints.

- Creating Configuration Profiles
  - Profiles for Android Devices
  - Profiles for iOS Devices
  - Profiles for Windows Device
  - Profiles for Mac OS Devices
- Viewing and Managing Profiles
  - Exporting and Importing Configuration Profiles
  - Cloning a Profile
- Editing Configuration Profiles
- Managing Default Profiles
- Managing Alerts
  - Create a New Alert
  - Edit / Delete an Alert
- Managing 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

Applications - Covers the management of applications installed on the managed devices, blacklist and whitelist application and OS update patches that can be pushed to Windows devices from the ITSM console.

- Viewing Applications Installed on Android and iOS Devices
  - Blacklisting and Whitelisting Applications
- Patch Management
    - Installing OS Patches on Windows Endpoints
    - Installing 3rd Party Application Patches on Windows Endpoints

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
- Manage File Trust Ratings on Windows Devices
- Viewing list of Valkyrie Analyzed Files
- Antivirus and File Rating Scans
  - Running Antivirus and/or File Rating Scans on Devices
  - Handling Malware on Scanned Devices
  - Updating Virus Signature Database on Windows and Mac OS Devices
- Viewing and Managing Identified Malware
- Viewing and Managing Quarantined Items on Windows Devices
- Viewing and Managing Quarantined Items on Mac OS Devices
- Viewing Threat 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
  - Managing ITSM Extensions
  - Configuring ITSM Reports
  - Integrating with Comodo Certificate Manager
  - Setting-up Administrator's Time Zone
- Viewing and Managing Licenses
  - Upgrading or Adding a License

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. 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 - For purpose of this guide, Mac OS 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.

- CCS can be white-labelledwith your own company branding and UI texts. You can customize the company name, company logo, product logo and more.

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 default profiles, Android default profiles and Windows default profiles. Multiple default profiles can be created and applied to a device or group of devices.

Comodo Client Communication (a.k.a ITSM Agent) - Comodo Client Communication (CCC) is an agent which needs to be installed on all enrolled devices to facilitate communication with the ITSM server. The agent is responsible for receiving and executing tasks. Tasks include implementing configuration profiles, fetching device details, running antivirus scans, adding or removing apps and wiping the device.

- CCC can be white-labeled with your own company branding and UI texts. You can customize the company name, company logo, product logo and more. You can also specify your support email, support website and support email in the CCC 'About' dialog.

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.

    See **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.

    See **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.

See **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.

   See **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. See **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. See **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

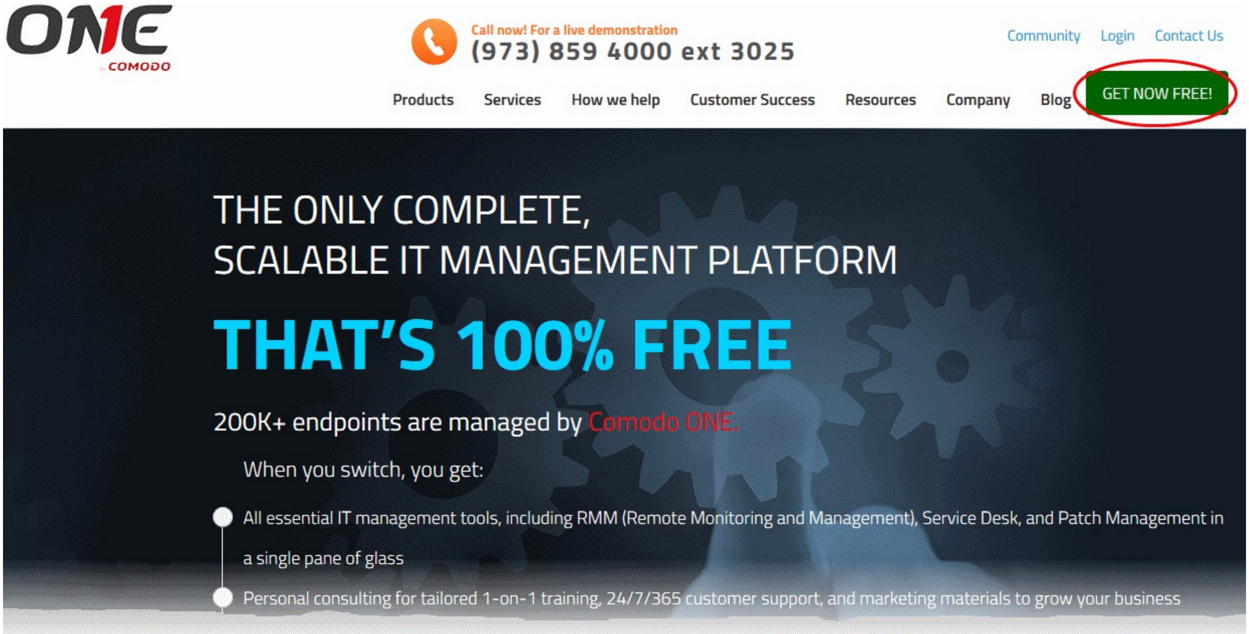
Note - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit files for analysis and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in **Appendix 1**.

Step 1 - Enrollment and Configuration

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

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

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



THE ONLY COMPLETE,
SCALABLE IT MANAGEMENT PLATFORM

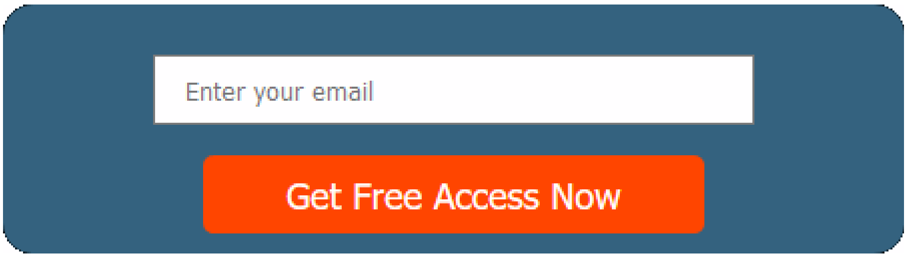
THAT'S 100% FREE

200K+ endpoints are managed by Comodo ONE.

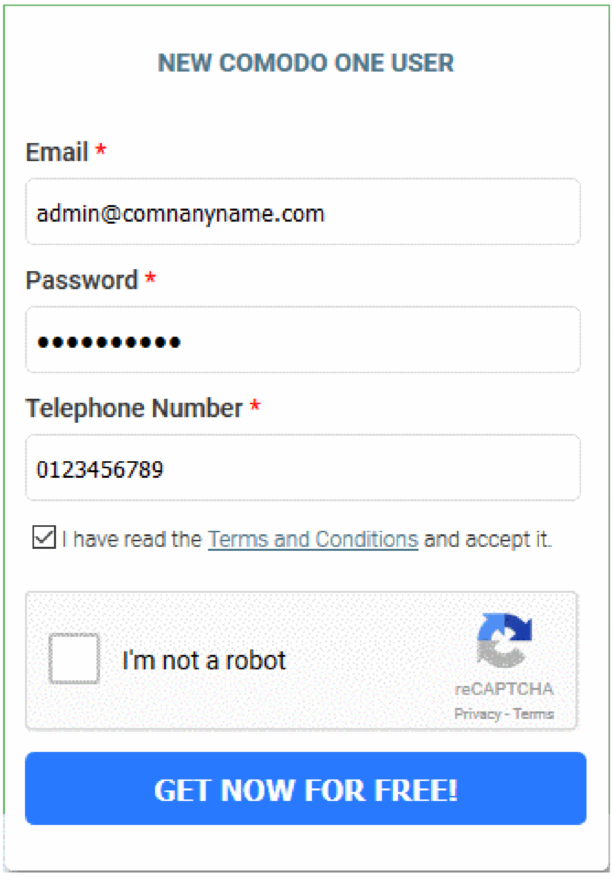
When you switch, you get:

- All essential IT management tools, including RMM (Remote Monitoring and Management), Service Desk, and Patch Management in a single pane of glass
- Personal consulting for tailored 1-on-1 training, 24/7/365 customer support, and marketing materials to grow your business

You will be taken to the Comodo One enrollment wizard:



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



NEW COMODO ONE USER

Email *

admin@comnanyname.com

Password *

•••••••••••

Telephone Number *

0123456789

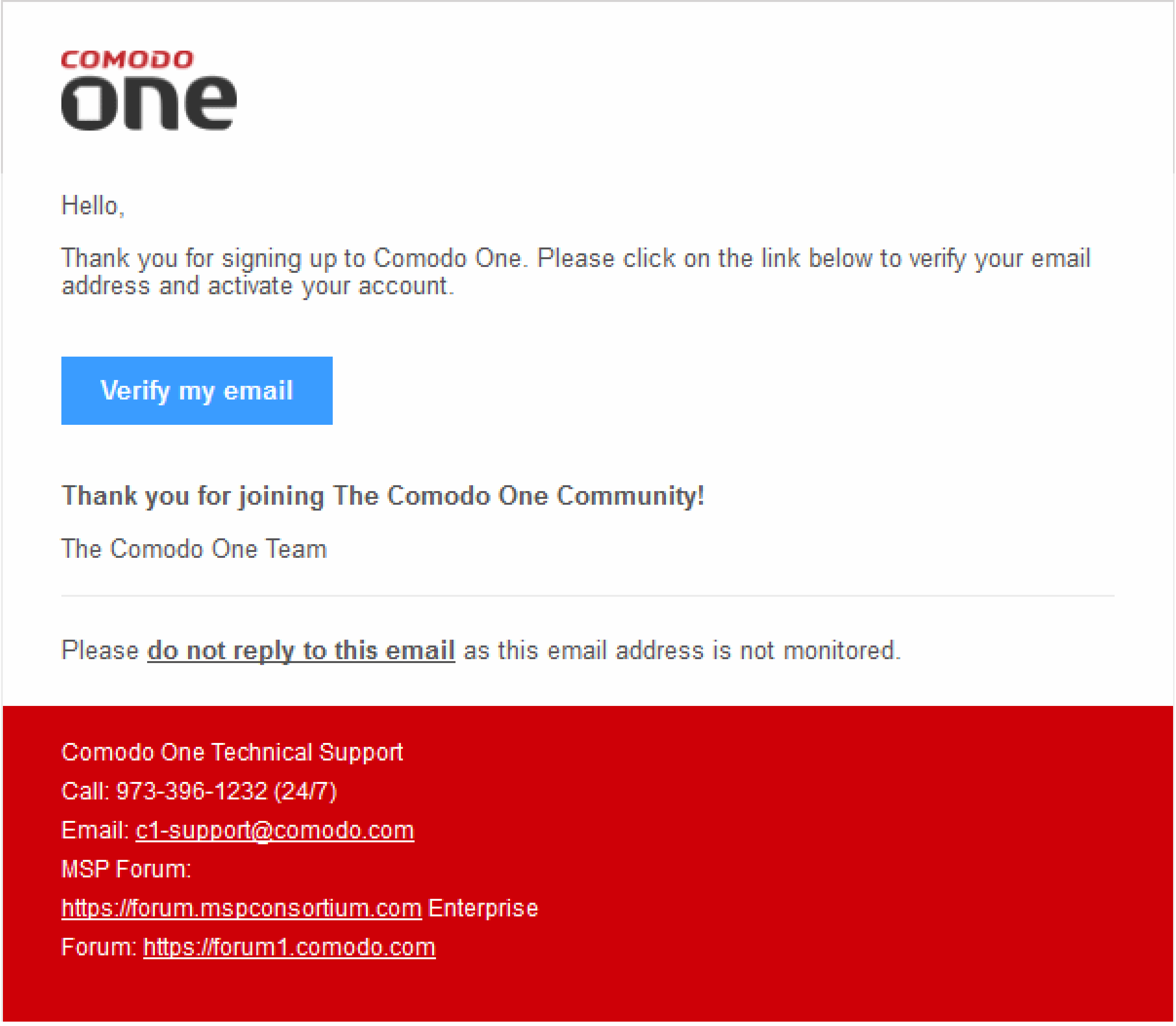
☑ I have read the Terms and Conditions and accept it.

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

  - At least eight characters long
  - Contain a mix off lower case and upper case letters
  - Contain at least one numeral
  - Contain at least one of the following special characters - '("!#$%^&*")'
- **Telephone Number** - Primary contact number
- **End User License Agreement**: Read the EULA fully by clicking the 'EULA' link and select the 'I have read EULA and accept it' check box.
- **Captcha**: Select I'm not a robot and complete the verification.

Click 'Get Now for Free'.

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



Hello,

Thank you for signing up to Comodo One. Please click on the link below to verify your email address and activate your account.

Thank you for joining The Comodo One Community!

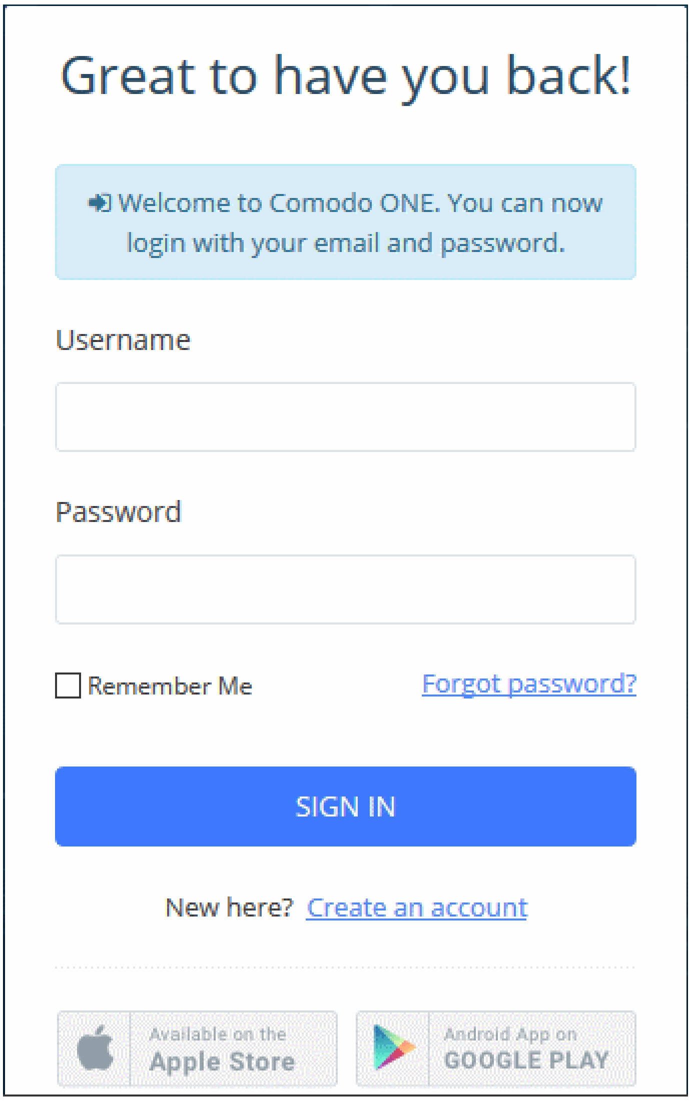
The Comodo One Team

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

Comodo One Technical Support
Call: 973-396-1232 (24/7)
Email: c1-support@comodo.com
MSP Forum:
https://forum.mspconsortium.com Enterprise
Forum: https://forum1.comodo.com

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

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

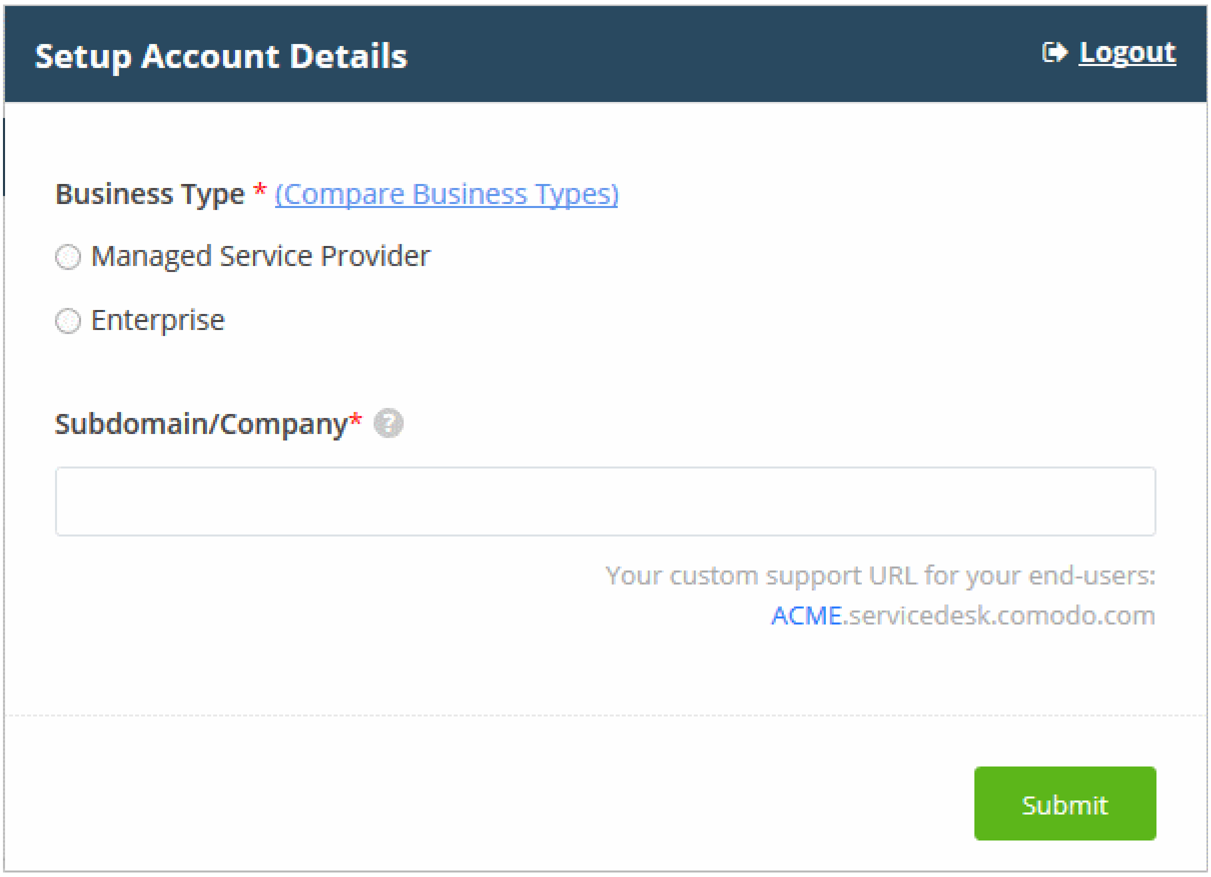


Great to have you back!

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

Username
Password
□ Remember Me
Forgot password?
SIGN IN
New here? Create an account
Available on the Apple Store
Android App on GOOGLE PLAY

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



Setup Account Details

Business Type * (Compare Business Types)

○ Managed Service Provider

○ Enterprise

Subdomain/Company* ?

Your custom support URL for your end-users:
ACME.servicedesk.comodo.com

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

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

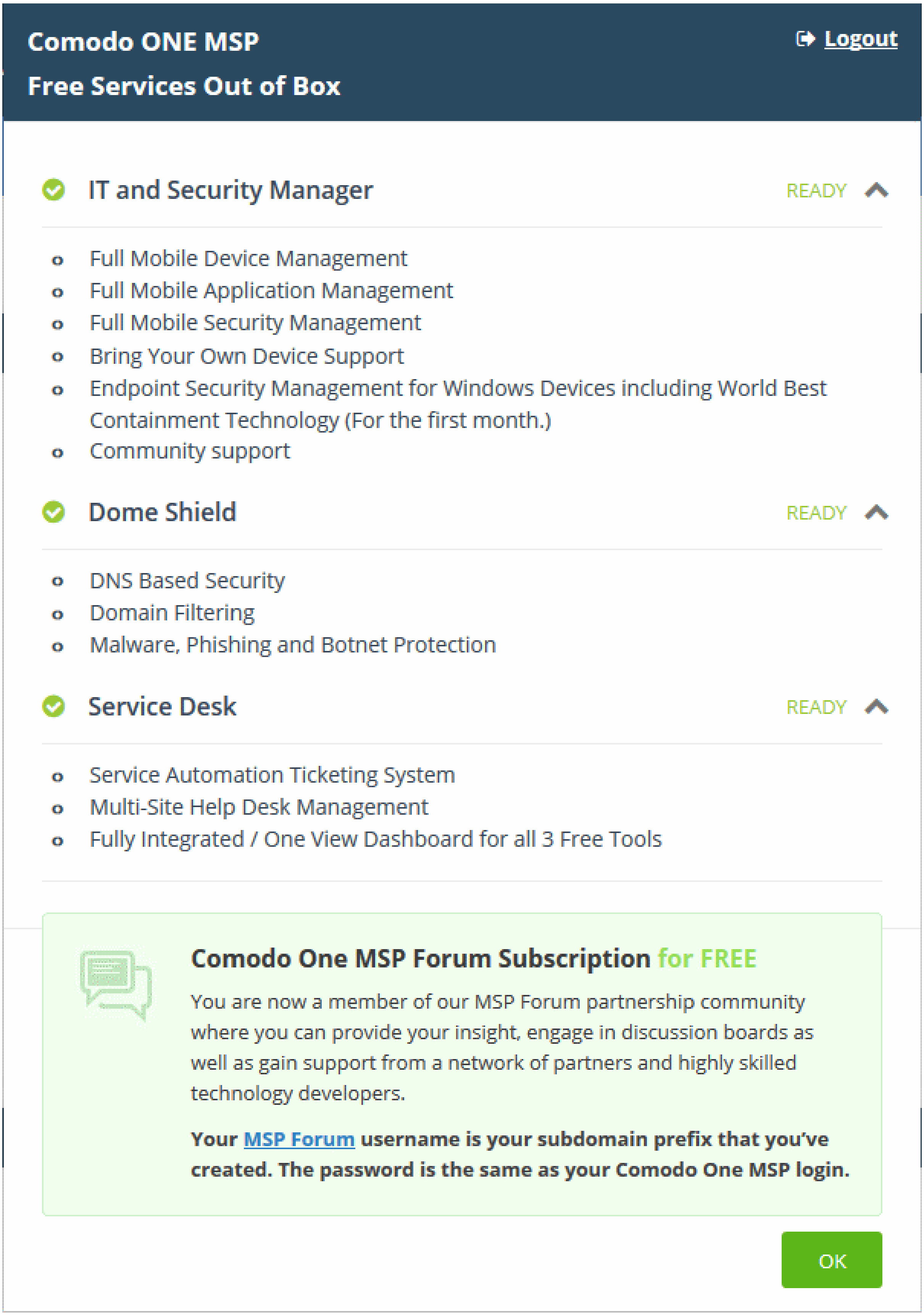
For more details on C1 modules, see **https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html**.

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

For example, if you enter the sub-domain 'dithers' then you will access ITSM at **https://dithers.cmdm.comodo.com**

- Click 'Submit'

The next screen shows a summary of your active services:



Comodo ONE MSP

Free Services Out of Box

✓ IT and Security Manager READY

- Full Mobile Device Management
- Full Mobile Application Management
- Full Mobile Security Management
- Bring Your Own Device Support
- Endpoint Security Management for Windows Devices including World Best Containment Technology (For the first month.)
- Community support

✓ Dome Shield READY

- DNS Based Security
- Domain Filtering
- Malware, Phishing and Botnet Protection

✓ Service Desk READY

- Service Automation Ticketing System
- Multi-Site Help Desk Management
- Fully Integrated / One View Dashboard for all 3 Free Tools

Comodo One MSP Forum Subscription for FREE

You are now a member of our MSP Forum partnership community where you can provide your insight, engage in discussion boards as well as gain support from a network of partners and highly skilled technology developers.

Your MSP Forum username is your subdomain prefix that you've created. The password is the same as your Comodo One MSP login.

- Click 'OK' to finish setup. You will be taken to the Comodo One Dashboard
- Click 'Licensed Applications' > 'ITSM' to open the ITSM console
- This account will be given master 'Account Admin' privileges and cannot be deleted. You will be able to create administrators and staff under this account
- Admins/users who enrolled via C1 can login at **https://one.comodo.com/app/login**
- Admins/users created in ITSM can login at https://<*company name*>.cmdm.comodo.com/

Step 2 - Configure ITSM Communications

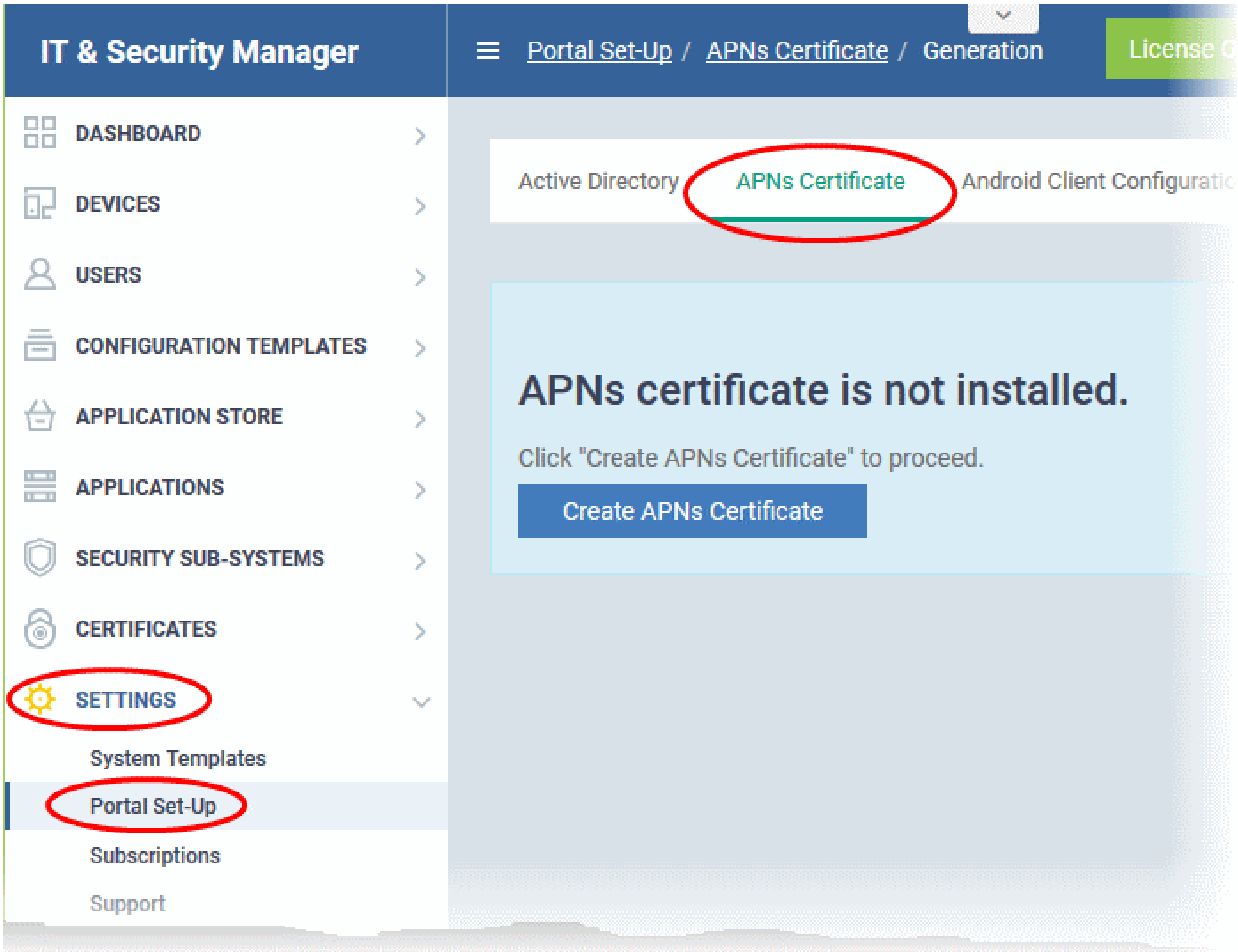
In order for your ITSM server to communicate with enrolled devices, you need to install an Apple Push Notification (APN) certificate and/or a Google Cloud Messaging (GSM) Token on your portal. The following sections explain more about:

- **Adding APN Certificate**
- **Adding GCM Token**

Adding Apple Push Notification Certificate

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

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

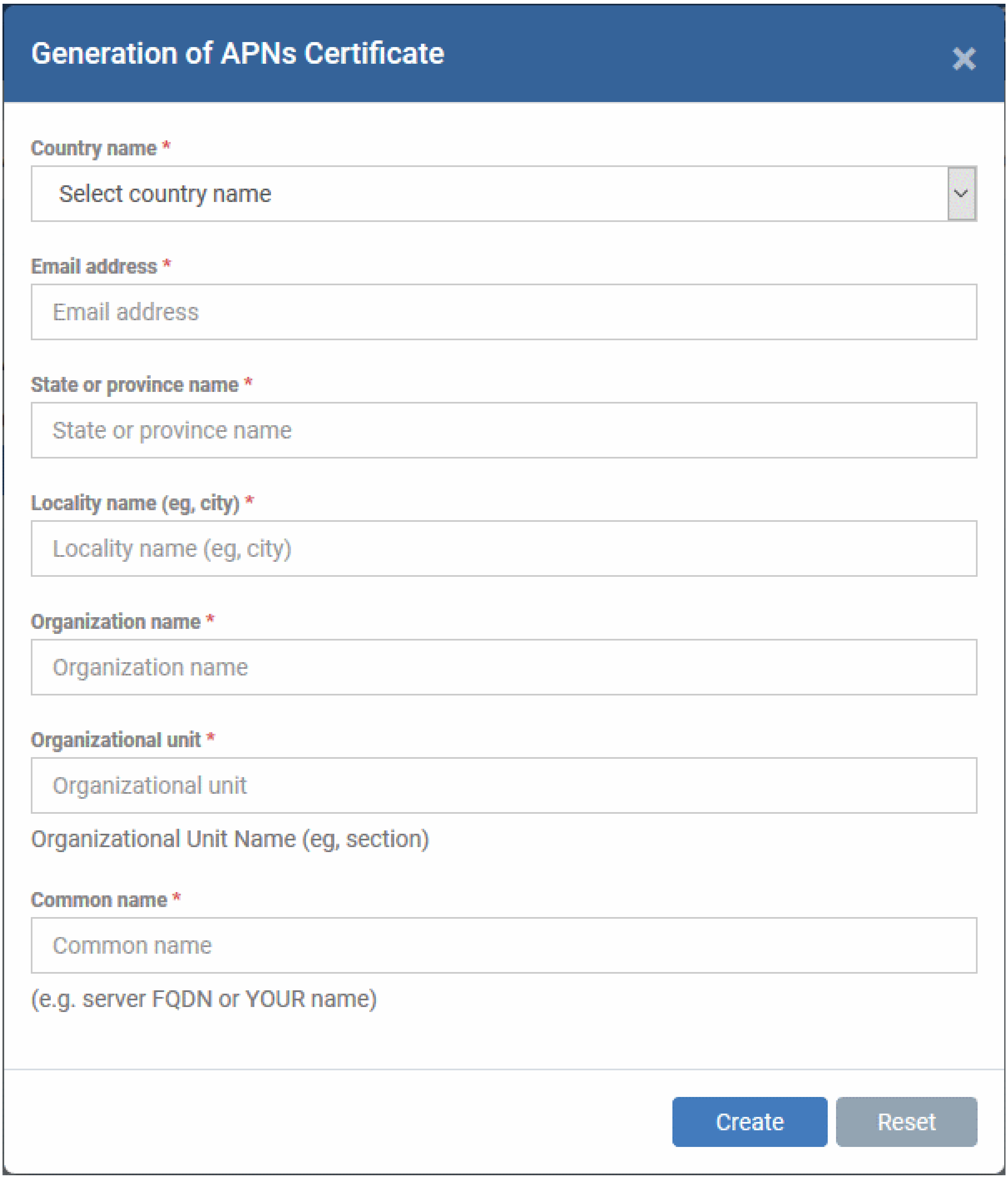


APNs certificate is not installed.

Click "Create APNs Certificate" to proceed.

  - 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):



Generation of APNs Certificate

Country name *

Select country name

Email address *

Email address

State or province name *

State or province name

Locality name (eg, city) *

Locality name (eg, city)

Organization name *

Organization name

Organizational unit *

Organizational unit

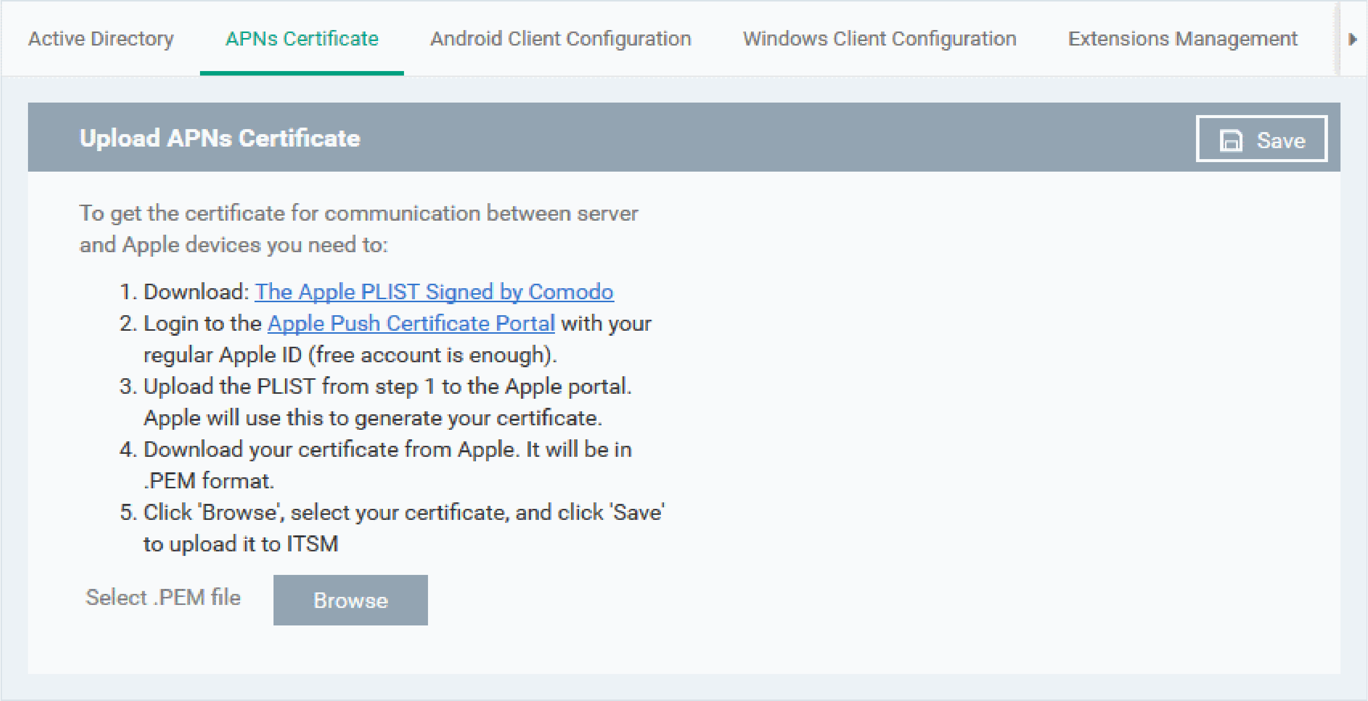
Organizational Unit Name (eg, section)

Common name *

Common name

(e.g. server FQDN or YOUR name)

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



Upload APNs Certificate

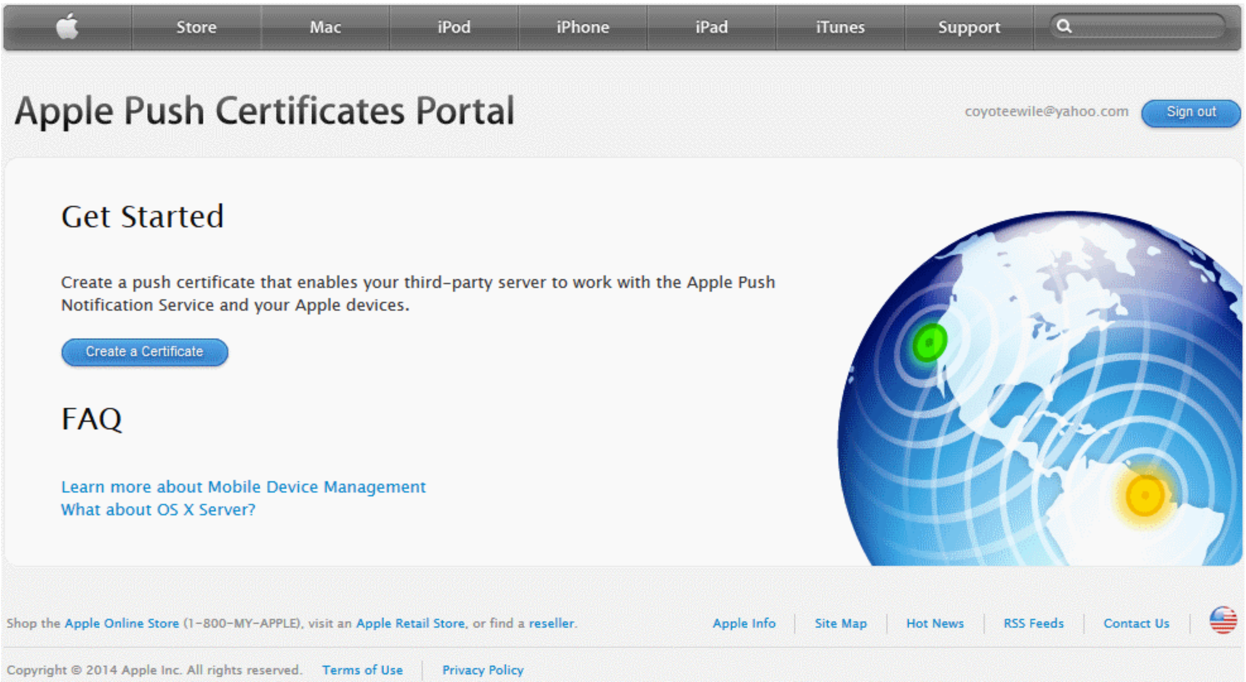
To get the certificate for communication between server and Apple devices you need to:

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

Select .PEM file

- Download 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'.



Apple Push Certificates Portal

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

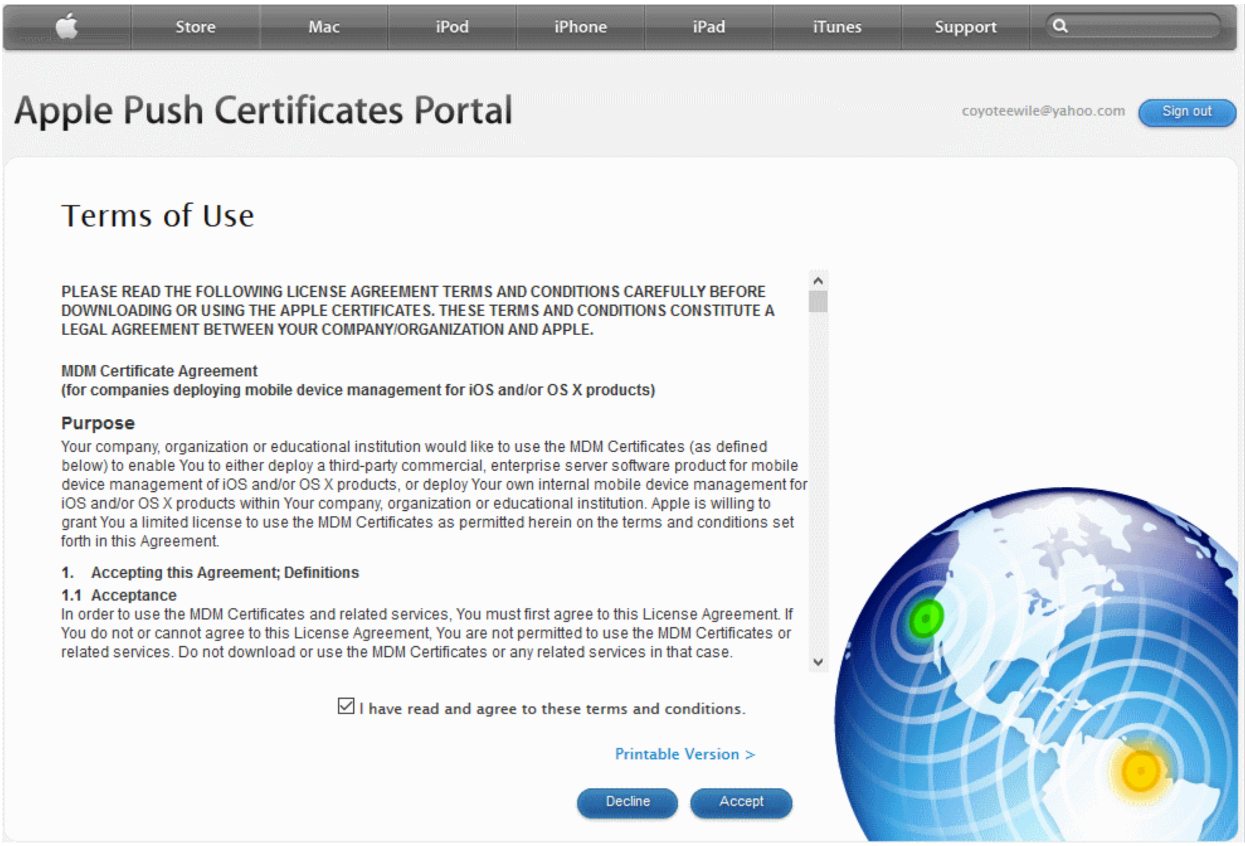
FAQ

Learn more about Mobile Device Management
What about OS X Server?

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

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



Apple Push Certificates Portal

Terms of Use

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

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

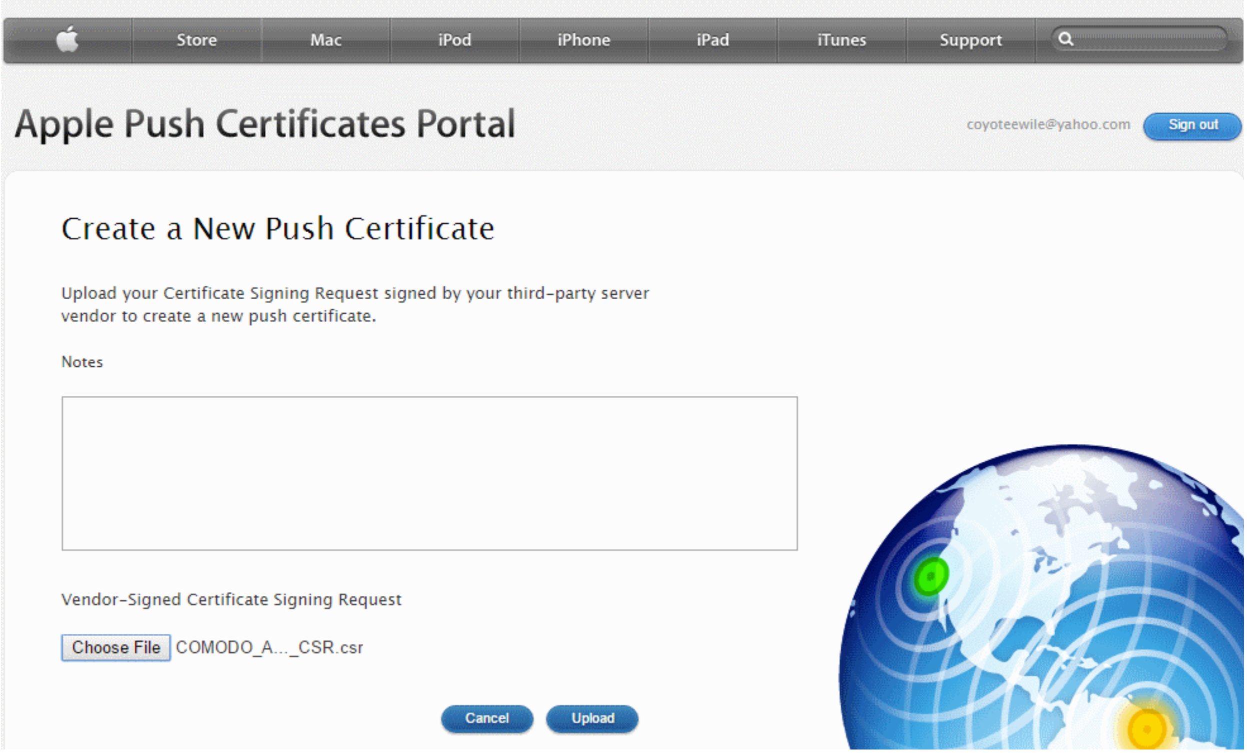
Purpose
Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile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

1. Accepting this Agreement; Definitions

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

☑ I have read and agree to these terms and conditions.

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



Apple Push Certificates Portal

Create a New Push Certificate

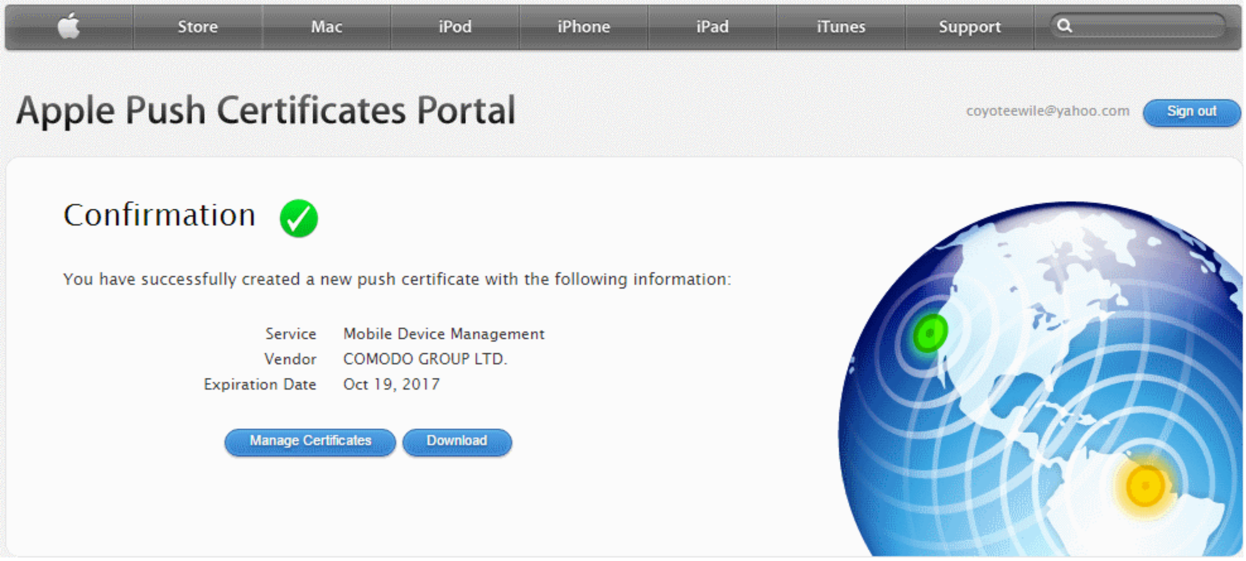
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

Choose File COMODO_A..._CSR.csr

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



Apple Push Certificates Portal

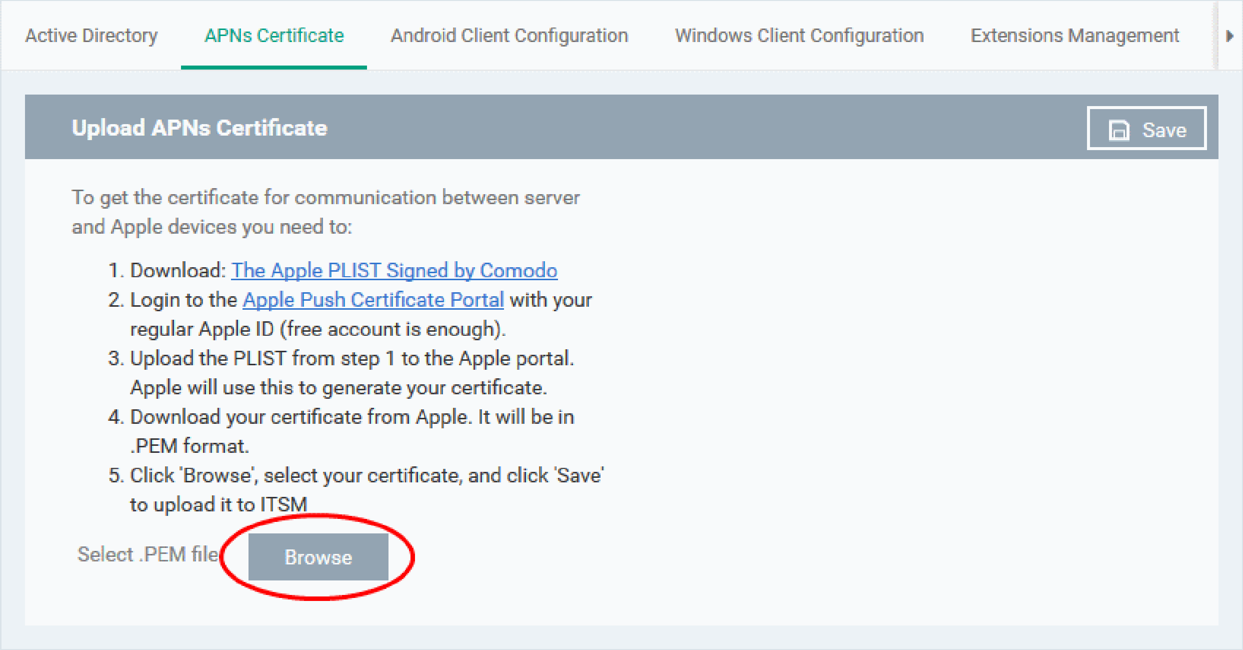
Confirmation

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	COMODO GROUP LTD.
Expiration Date	Oct 19, 2017

   - 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.



Upload APNs Certificate

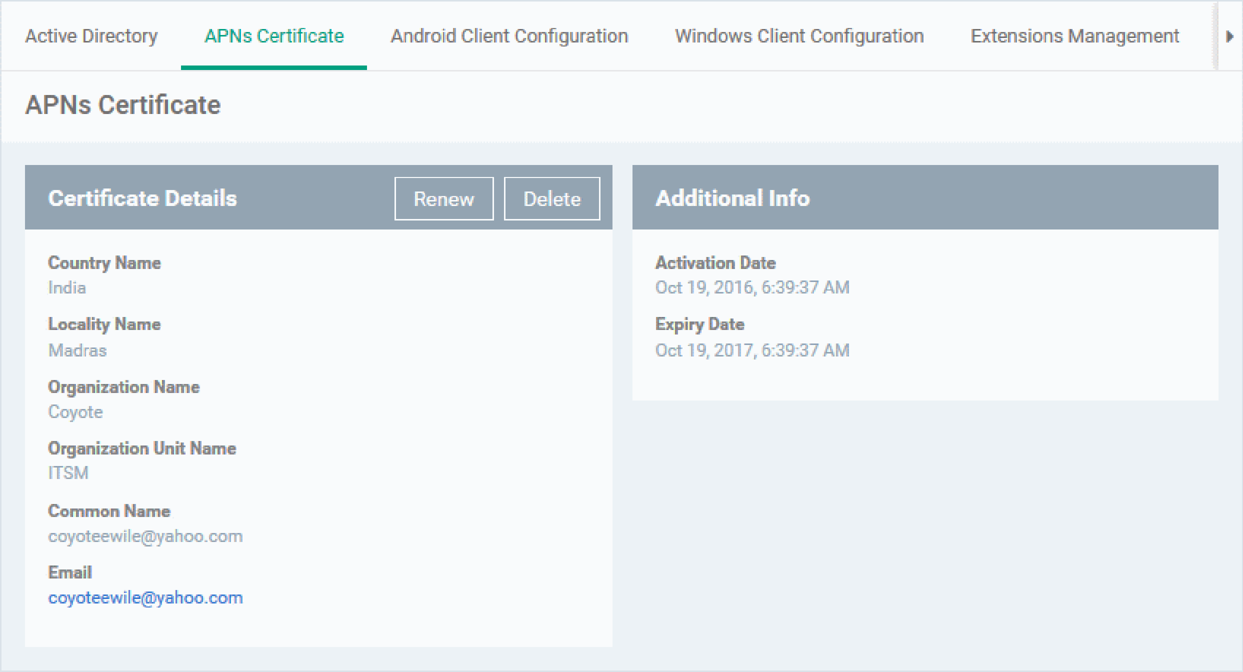
To get the certificate for communication between server and Apple devices you need to:

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

Select .PEM file

   - Click 'Save' to upload your certificate.

The APNs Certificate details interface will open:



APNs Certificate

Certificate Details

Country Name
India

Locality Name
Madras

Organization Name
Coyote

Organization Unit Name
ITSM

Common Name
coyoteewile@yahoo.com

Email
coyoteewile@yahoo.com

Additional Info

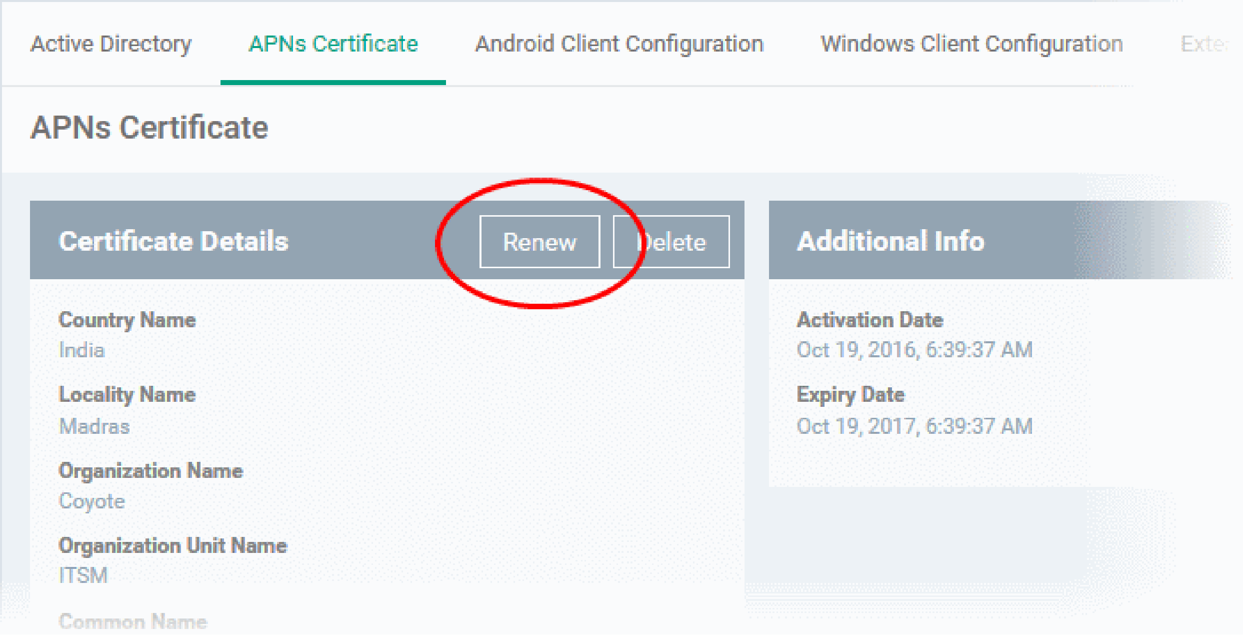
Activation Date
Oct 19, 2016, 6:39:37 AM

Expiry Date
Oct 19, 2017, 6:39:37 AM

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.



APNs Certificate

Certificate Details

Country Name
India

Locality Name
Madras

Organization Name
Coyote

Organization Unit Name
ITSM

Common Name

Additional Info

Activation Date
Oct 19, 2016, 6:39:37 AM

Expiry Date
Oct 19, 2017, 6:39:37 AM

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

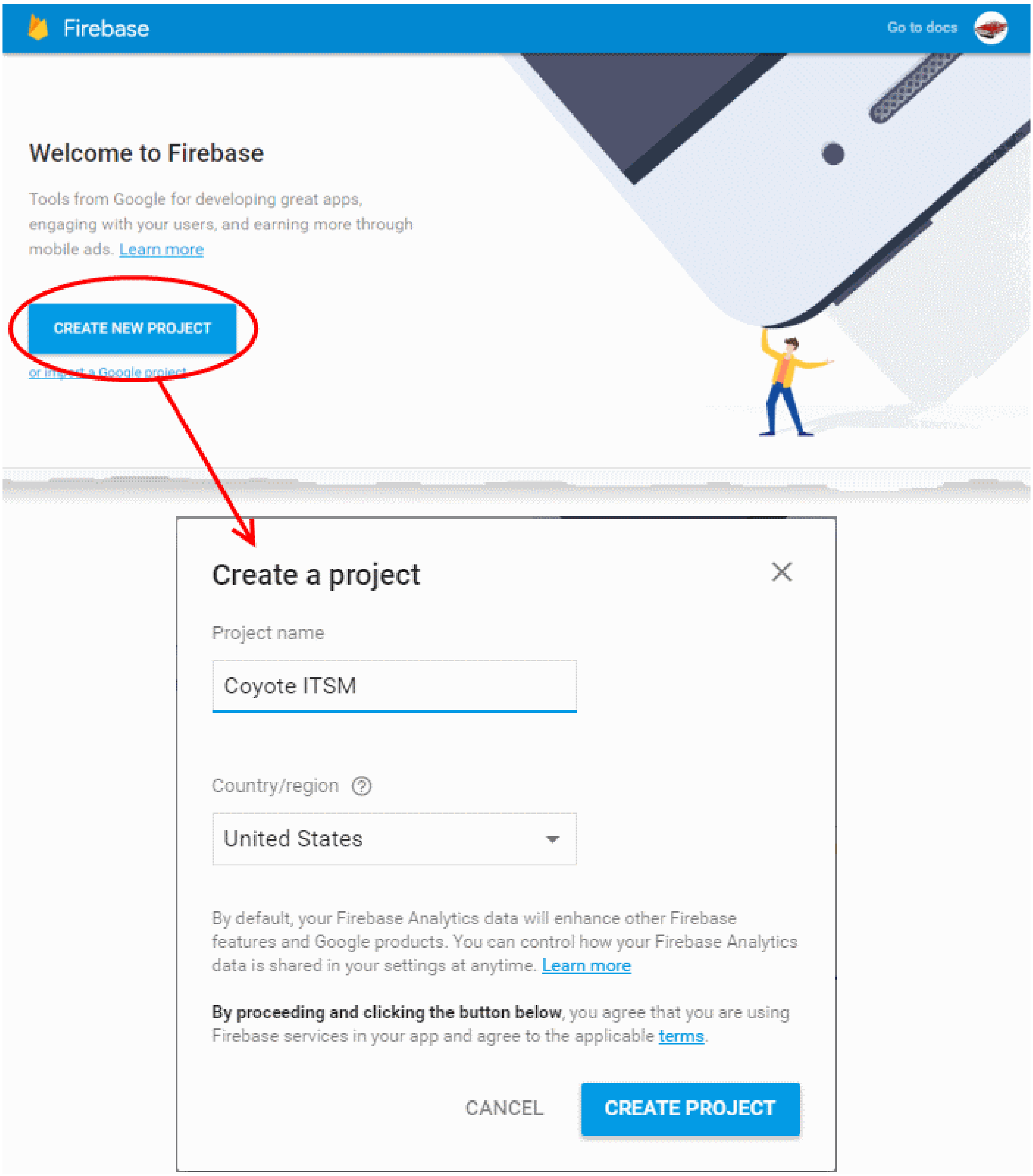
Adding Google Cloud Messaging (GCM) Token

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**

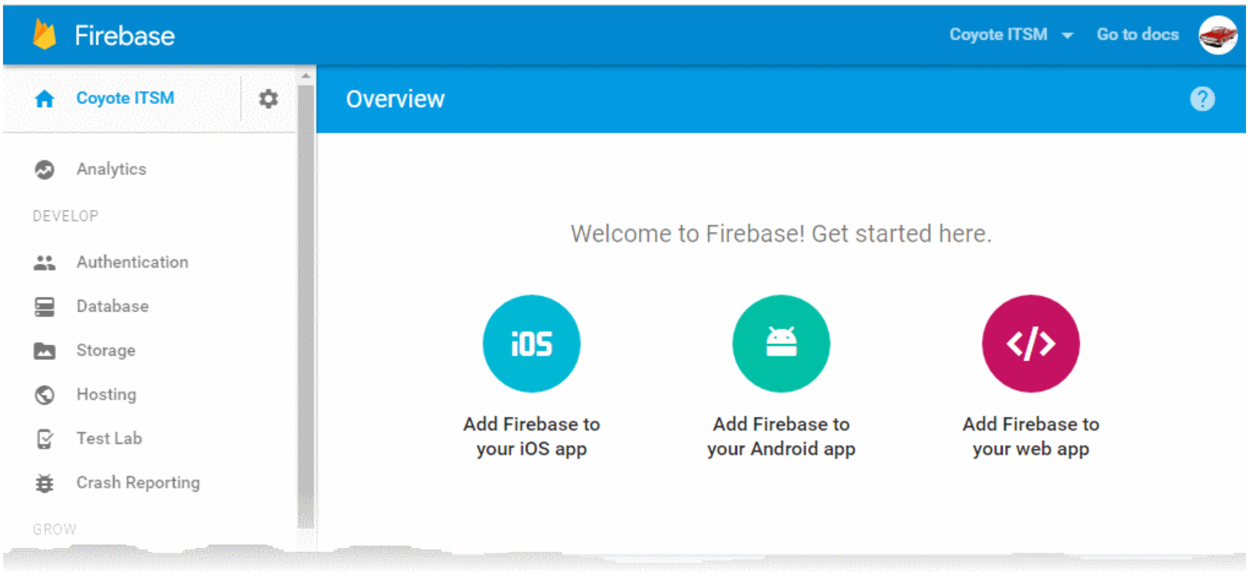
- Login to the Google Firebase API Console at **https://console.firebase.google.com**, using your Google account.



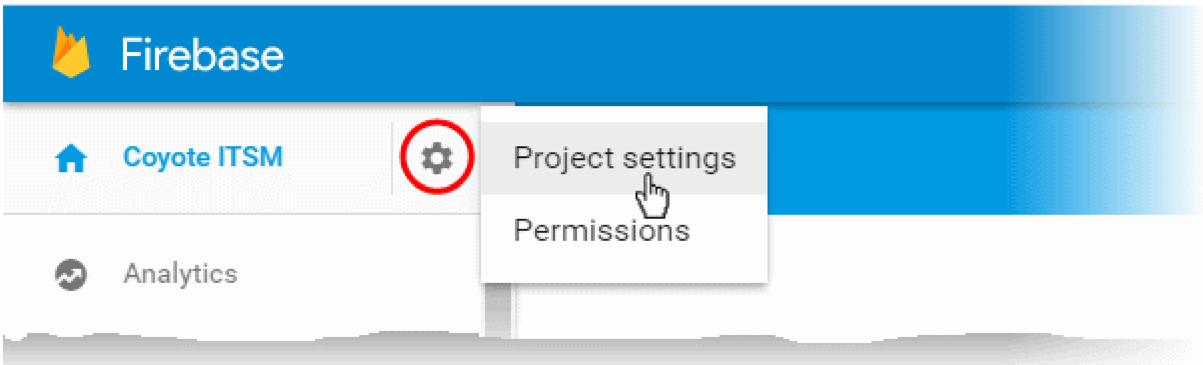
Firebase
Go to docs
Welcome to Firebase
Tools from Google for developing great apps, engaging with your users, and earning more through mobile ads. Learn more
CREATE NEW PROJECT
or import a Google project
Create a project
Project name
Coyote ITSM
Country/region
United States
By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at anytime. Learn more
By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable terms.
CANCEL
CREATE PROJECT

- 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.

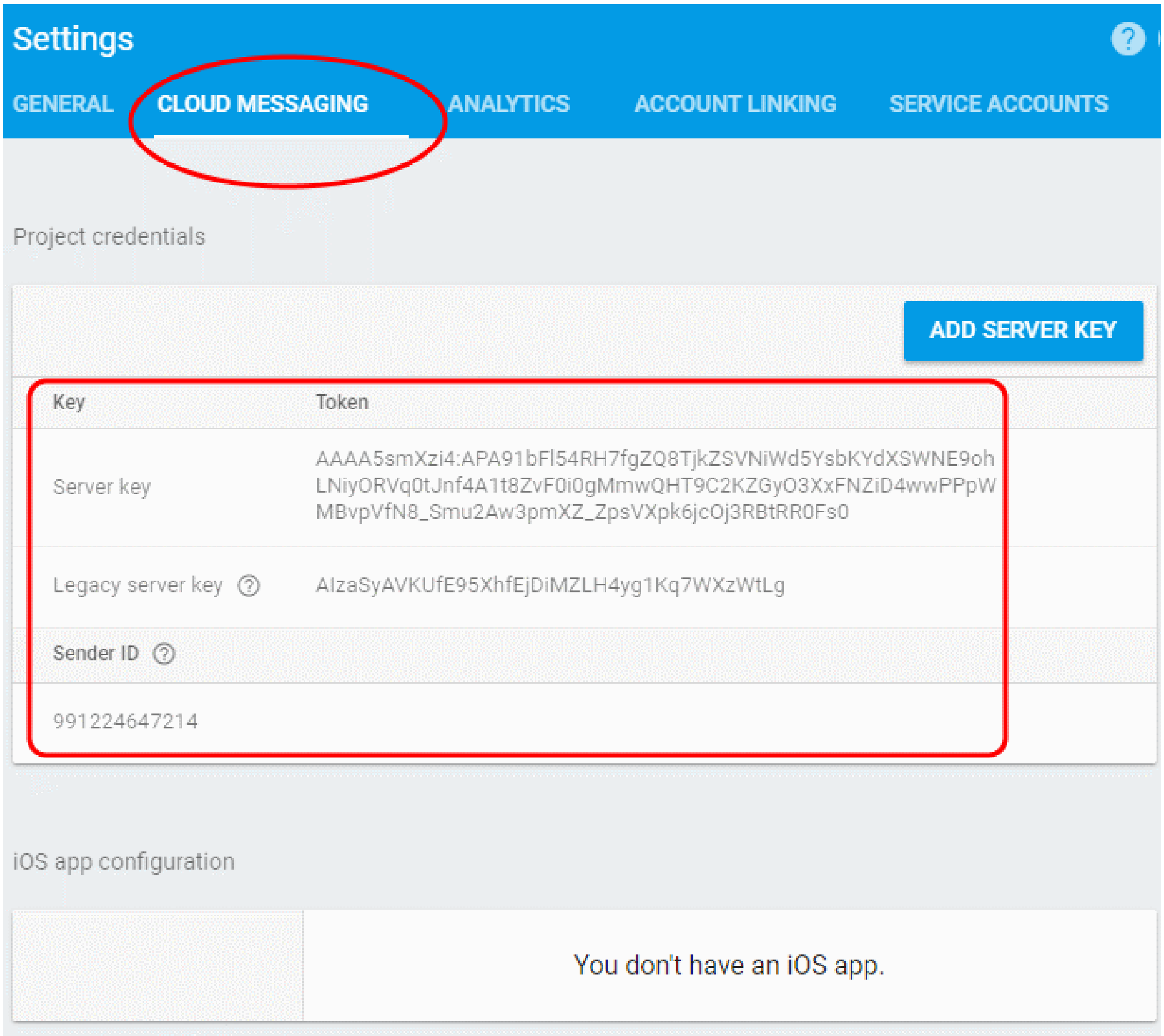


- **Step 2 - Obtain GCM Token and Project number**
  - Click the gear icon beside the project name at the left and choose Project Settings from the options.



The 'Settings' screen for the project will appear.

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



Project credentials

Key	Token
Server key	AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0
Legacy server key	AIzaSyAVKUfE95XhfEjDiMZLH4yg1Kq7WXzWtLg

Sender ID

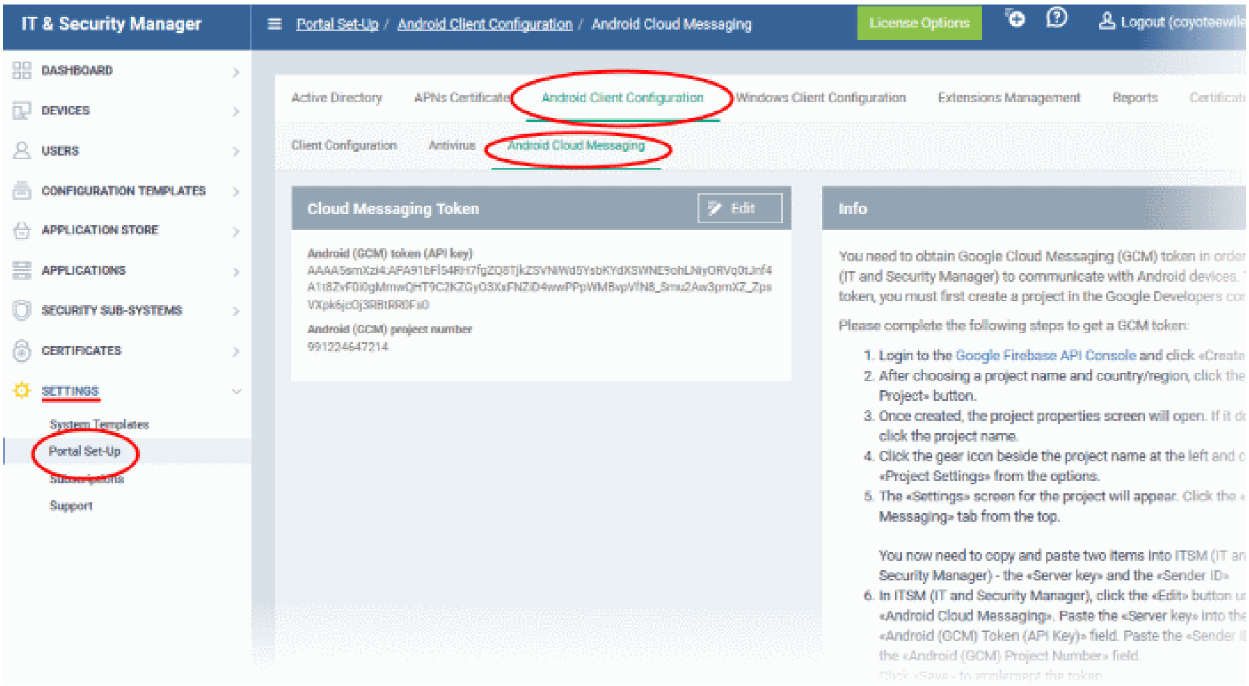
991224647214

iOS app configuration

You don't have an iOS app.

- 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



Cloud Messaging Token

Android (GCM) token (API key)
AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number
991224647214

Info

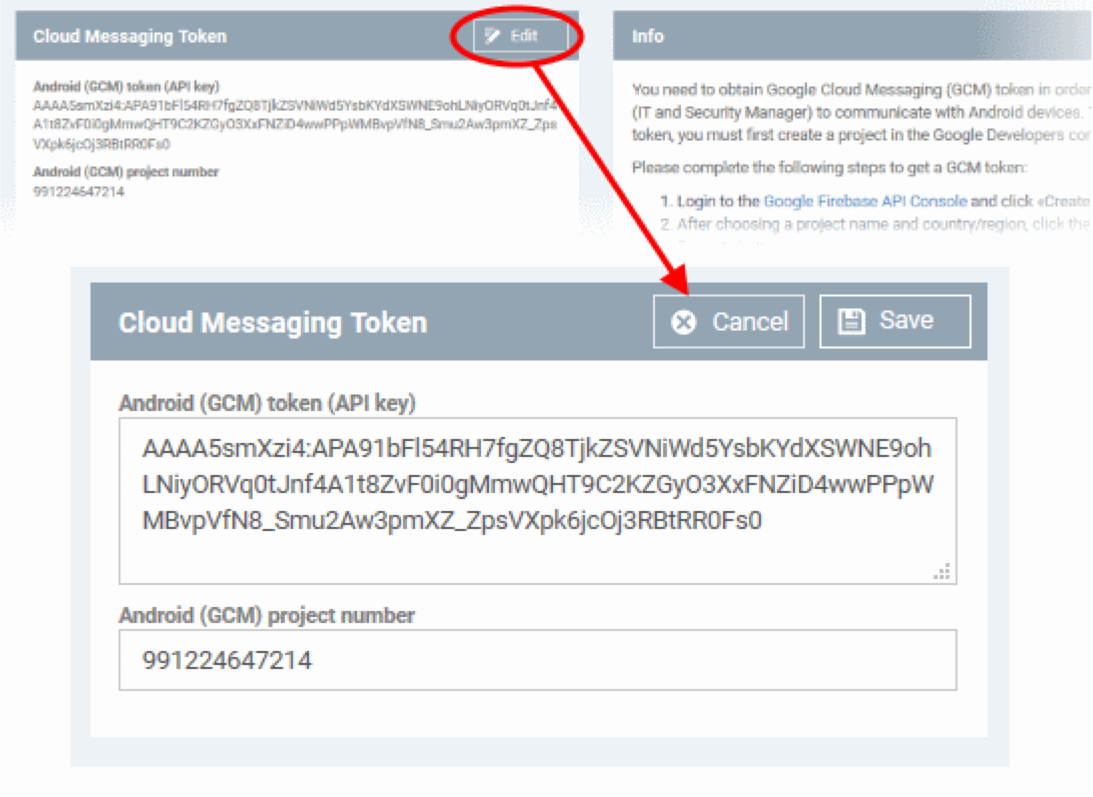
You need to obtain Google Cloud Messaging (GCM) token in order (IT and Security Manager) to communicate with Android devices. token, you must first create a project in the Google Developers con

Please complete the following steps to get a GCM token:

1. Login to the Google Firebase API Console and click «Create
2. After choosing a project name and country/region, click the Project» button.
3. Once created, the project properties screen will open. If it d click the project name.
4. Click the gear icon beside the project name at the left and c «Project Settings» from the options.
5. The «Settings» screen for the project will appear. Click the « Messaging» tab from the top.

   You now need to copy and paste two items into ITSM (IT an Security Manager) - the «Server key» and the «Sender ID»
6. In ITSM (IT and Security Manager), click the «Edit» button u «Android Cloud Messaging». Paste the «Server key» into the «Android (GCM) Token (API Key)» field. Paste the «Sender I the «Android (GCM) Project Number» field.
   Click «Save» to implement the token.

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



Android (GCM) token (API key)
AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number
991224647214

You need to obtain Google Cloud Messaging (GCM) token in order (IT and Security Manager) to communicate with Android devices. token, you must first create a project in the Google Developers cor

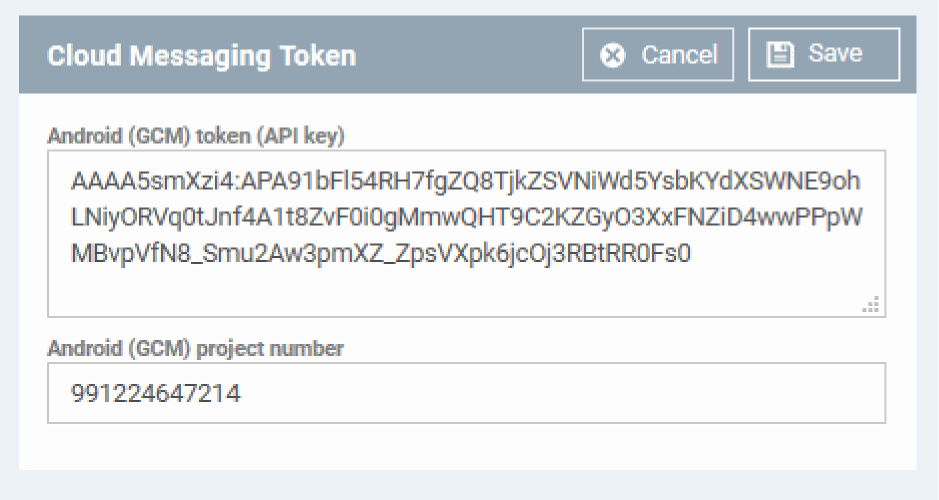
Please complete the following steps to get a GCM token:

1. Login to the Google Firebase API Console and click «Create
2. After choosing a project name and country/region, click the

- 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.



Cloud Messaging Token

Android (GCM) token (API key)

AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number

991224647214

Step 3 - Add Users

Users and staff can be added via the C1 console or directly through the ITSM interface.

- **Comodo One Staff**
  - C1 Enterprise - Staff created in C1 will be automatically added as users in ITSM.
  - C1 MSP - Staff created in C1 will be automatically added as users in ITSM and will be available for all companies.
- **ITSM Users**
  - C1 enterprise and ITSM 'stand-alone' customers can add users for a single company via ITSM.
  - C1 MSP customers can create multiple companies and add users/staff to them accordingly. You can group users/devices under different companies (for C1 MSP customers) as explained in **Step 5 - Create Groups of Devices**.

Staff added via Comodo One will be available in ITSM and other C1 applications like Service Desk. Users added via ITSM will only be available in ITSM.

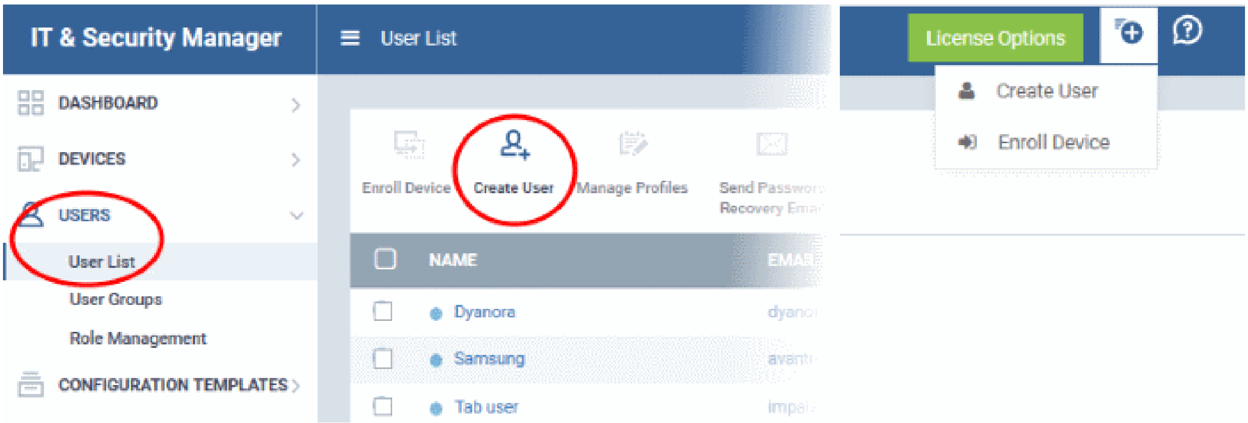
The following section explains how to add users via the ITSM interface:

To add a user

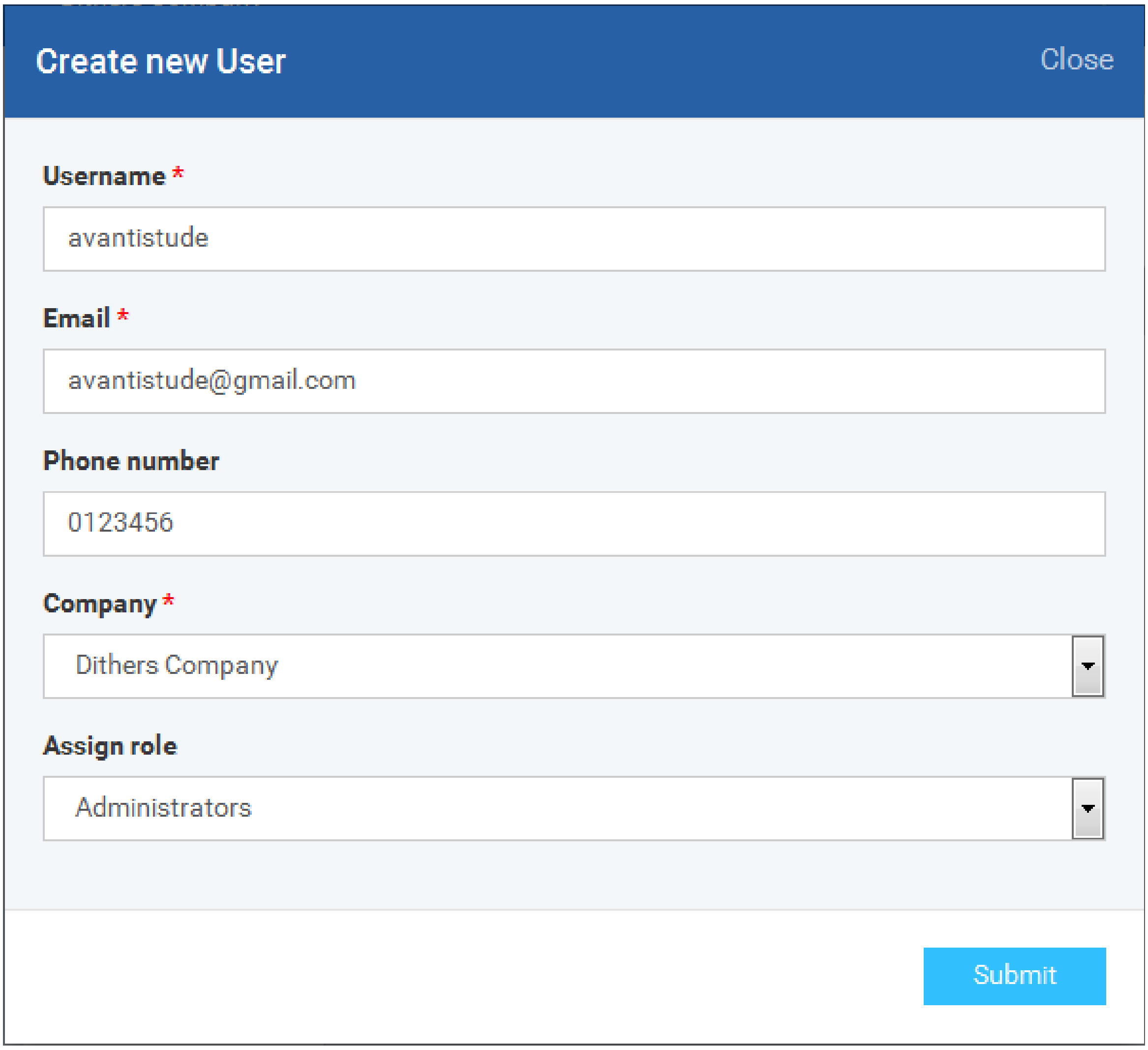
- Click 'Users' on the left then 'User List', then click the 'Create User' button

  or

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



The 'Create new user' form will open.



Create new User

Username *

avantistude

Email *

avantistude@gmail.com

Phone number

0123456

Company *

Dithers Company

Assign role

Administrators

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Choose user's company (mandatory)
    - Comodo One MSP Users - The drop-down will list companies added to C1. Choose which company the user should be enrolled under.
    - Comodo One Enterprise and 'stand-alone' ITSM users - Leave the selection as 'Default Company'.
- Choose user role. A 'role' determines user permissions within the ITSM console itself. ITSM ships with four default roles:
    - Account Admin - Can login to the ITSM administrative interface and access all management interfaces. This will not be listed here since it will be automatically assigned only to the person who opens a C1 account. This role is not editable.
    - Administrators - Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
    - Technician - Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
    - Users - Can login to the ITSM interface and view only the dashboard part of the application. This role can be edited according to your requirements.

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

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

Tip: **Importing User Groups from LDAP** for more details.

Step 4 - Enroll Users' devices

The next step is to enroll user devices for management.

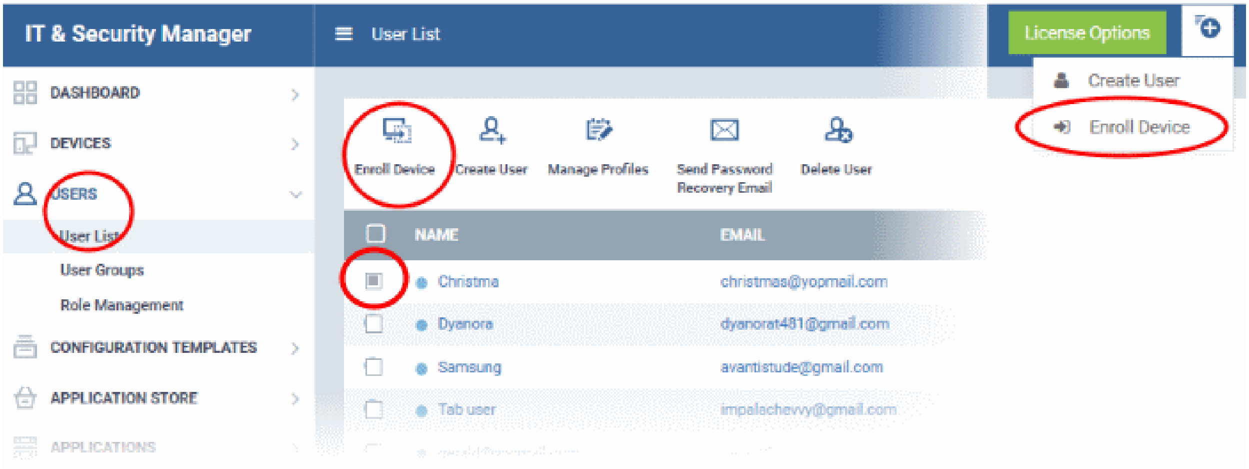
- Each license allows you to enroll up to five mobile devices or one Windows endpoint per user. So 1 user license will be consumed by 5 mobile devices and 1 license will be consumed by a single Windows endpoint.
- If more than 5 devices or 1 endpoint are added for the same user then an additional user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

To enroll devices

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

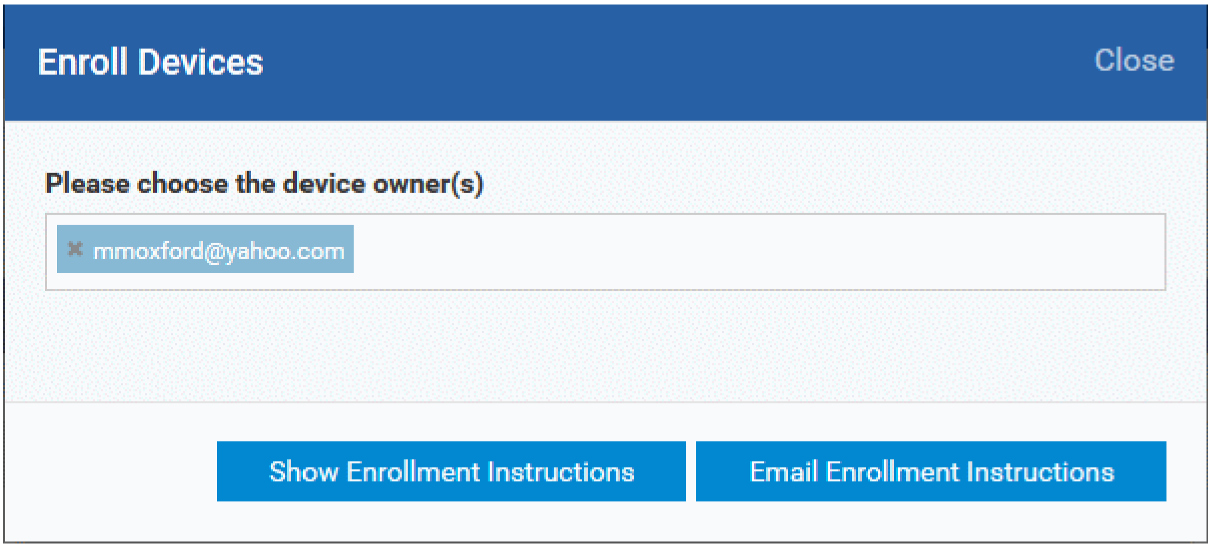
Or

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



	NAME	EMAIL
▣	Christma	christmas@yopmail.com
□	Dyanora	dyanorat481@gmail.com
□	Samsung	avantistude@gmail.com
□	Tab user	impalachevvy@gmail.com

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



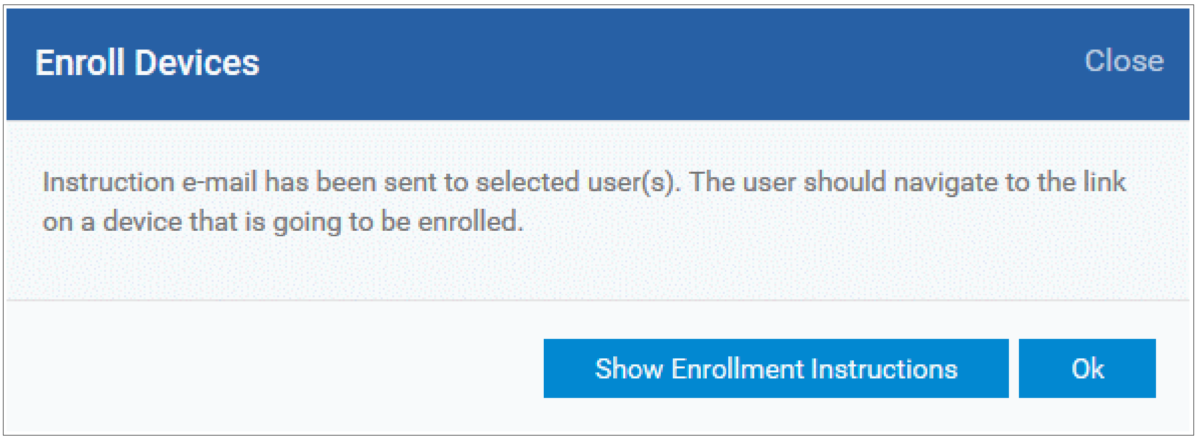
Enroll Devices

Please choose the device owner(s)

mmoxford@yahoo.com

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

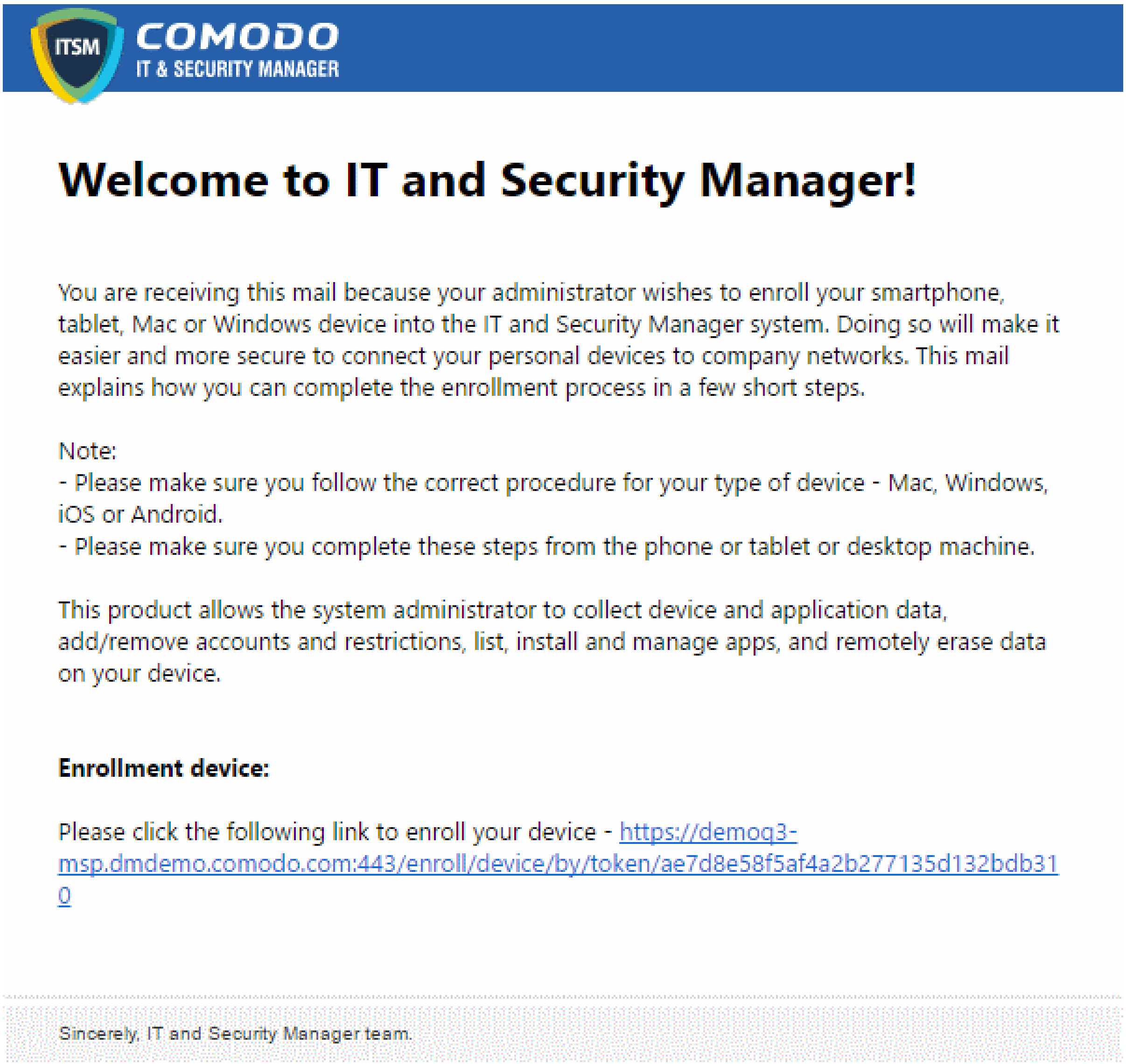
- To add more users, start typing first few letters of the username and choose from the results
- If you want enrollment instructions to be displayed in the ITSM interface, click 'Show Enrollment Instructions'. This is useful for administrators attempting to enroll their own devices.
- If you want the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



Enroll Devices

Instruction e-mail has been sent to selected user(s). The user should navigate to the link on a device that is going to be enrolled.

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



Welcome to IT and Security Manager!

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

Note:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

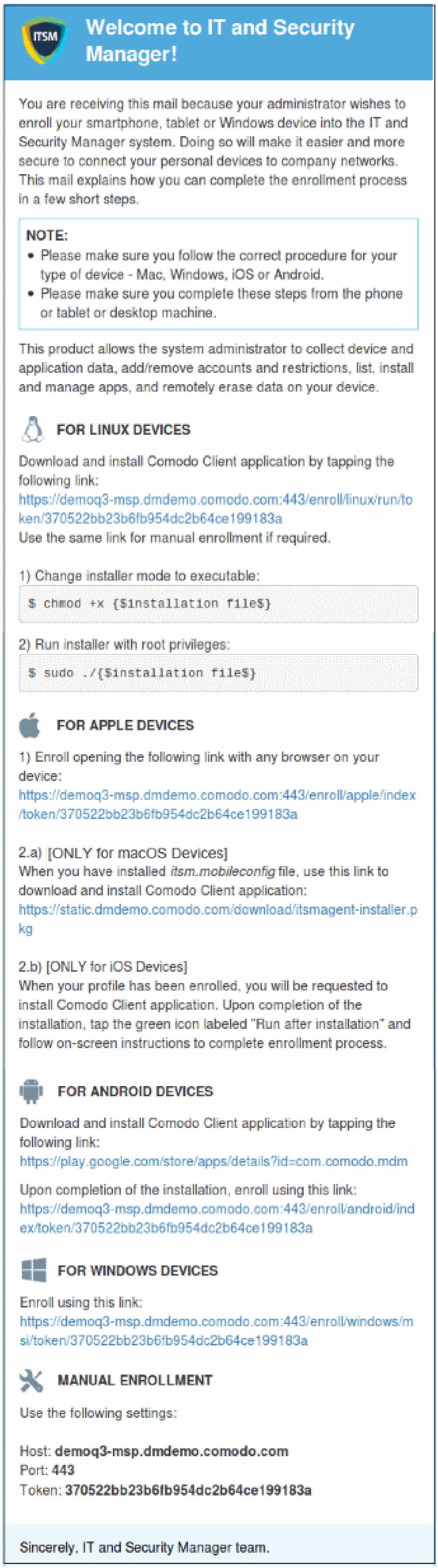
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Enrollment device:

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

Sincerely, IT and Security Manager team.

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



Welcome to IT and Security Manager!

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

NOTE:

- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

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

FOR LINUX DEVICES

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

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

FOR APPLE DEVICES

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

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

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

FOR ANDROID DEVICES

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

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

FOR WINDOWS DEVICES

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

MANUAL ENROLLMENT

Use the following settings:

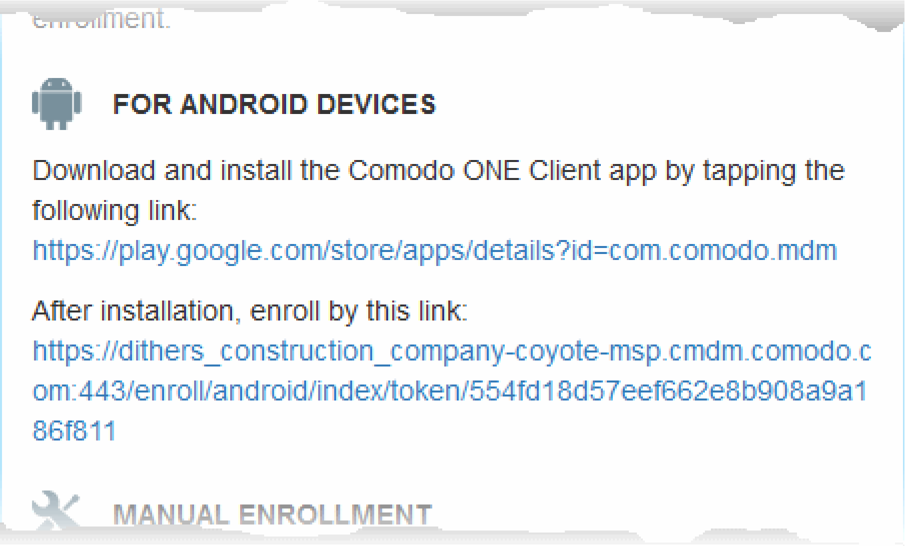
Host: **demoq3-msp.dmdemo.comodo.com**
Port: **443**
Token: **370522bb23b6fb954dc2b64ce199183a**

Sincerely, IT and Security Manager team.

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

Enroll Android Devices

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



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://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/android/index/token/554fd18d57eef662e8b908a9a186f811

MANUAL ENROLLMENT

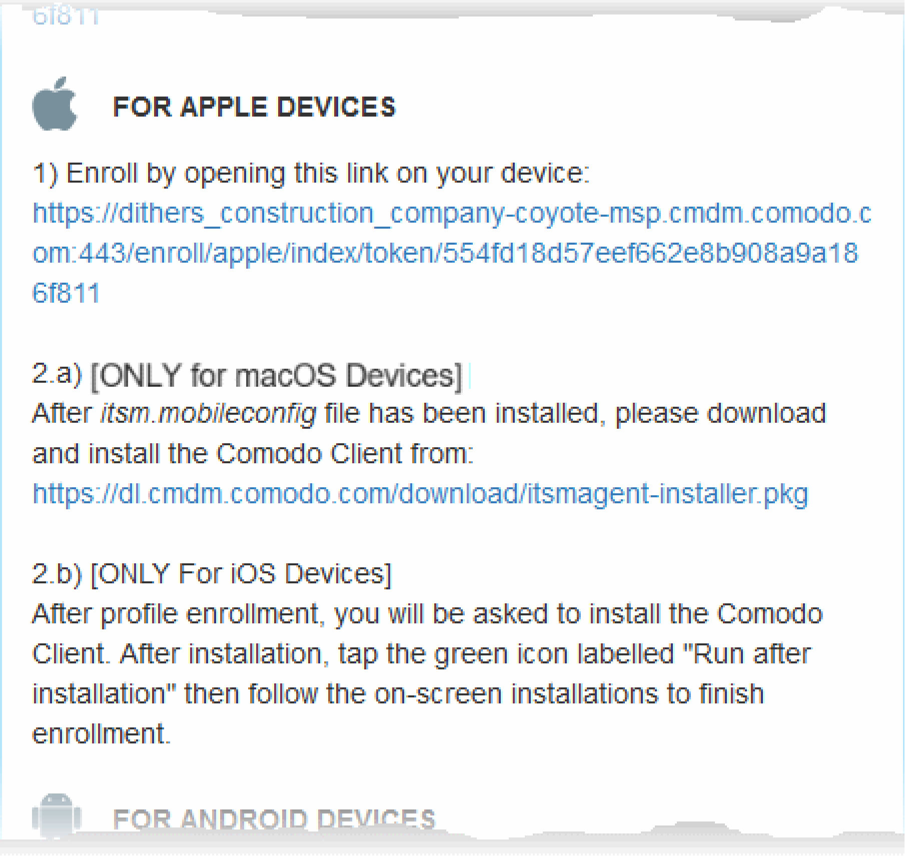
1. User opens the enrollment page on the target device and taps the 1st link to install the ITSM app.
2. After the app has been installed, the user clicks the 2nd link to enroll their device to ITSM. The app will connect to ITSM then request the user to tap 'Activate' to enroll the device.

Enroll iPhones, iPods and iPads

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

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

- After the profile has been installed, the client app installation will begin.



6f811

FOR APPLE DEVICES

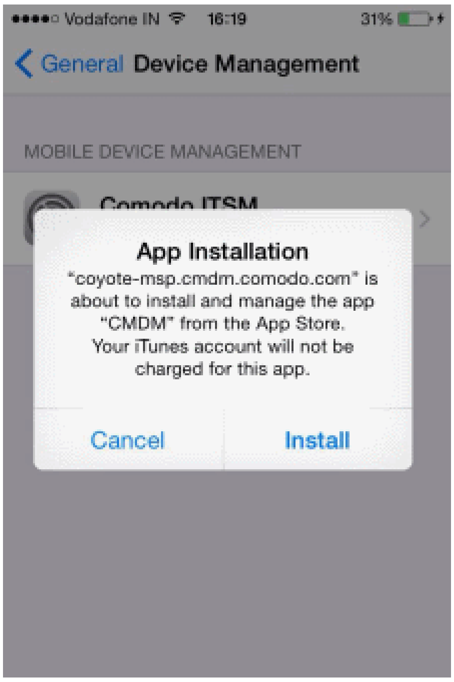
1) Enroll by opening this link on your device:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/apple/index/token/554fd18d57eef662e8b908a9a186f811

2.a) [ONLY for macOS Devices]
After *itsm.mobileconfig* file has been installed, please download and install the Comodo Client from:
https://dl.cmdm.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.

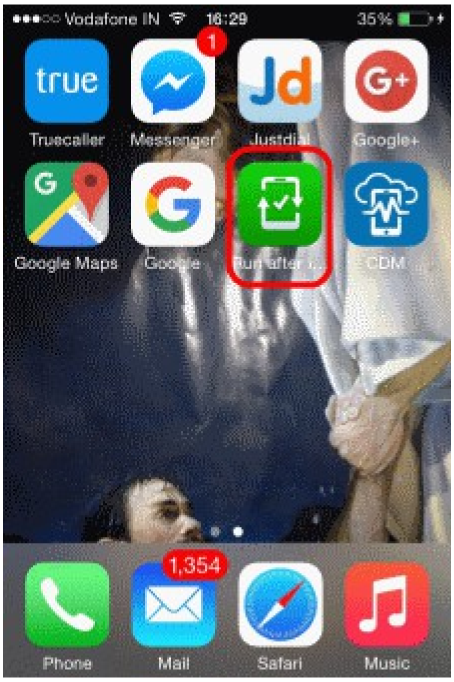
FOR ANDROID DEVICES

- The app is required so that ITSM can manage the remote device:



App Installation
"coyote-msp.cmdm.comodo.com" is about to install and manage the app "CMDM" from the App Store. Your iTunes account will not be charged for this app.

- The app will be downloaded and installed from the iTunes store. End-users may need to login with their Apple ID.
- After installation, users should tap the green 'Run After Install' icon on the home screen to complete registration:

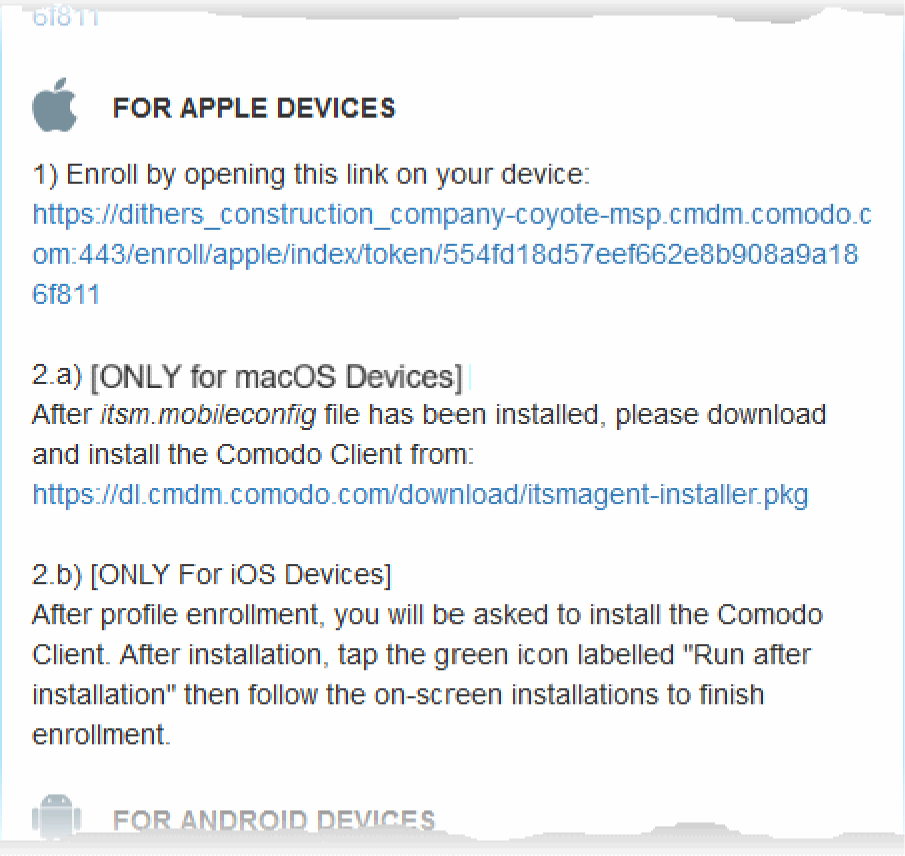


The device will be enrolled and connected to ITSM.

Enroll Mac OS Devices

Step 1 - Install the ITSM Configuration Profile

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



6f811

FOR APPLE DEVICES

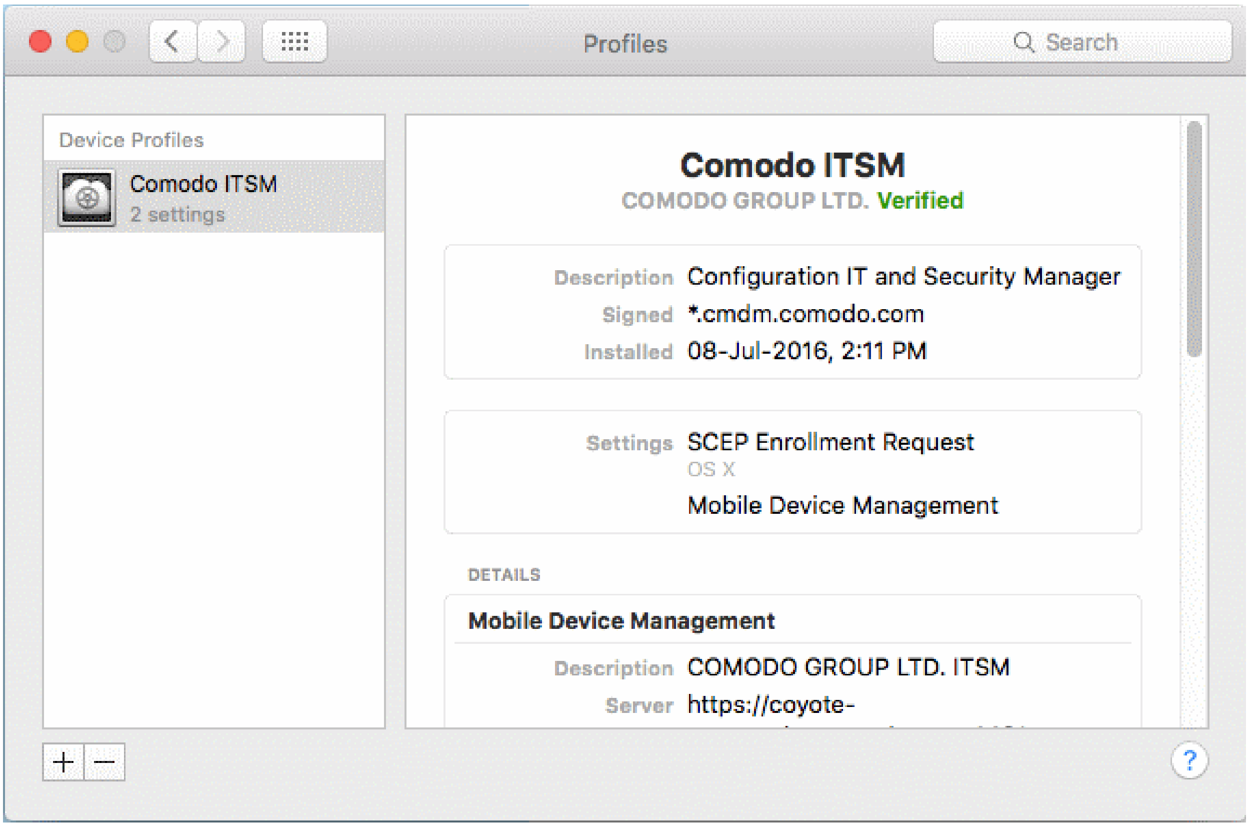
1) Enroll by opening this link on your device:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/apple/index/token/554fd18d57eef662e8b908a9a186f811

2.a) [ONLY for macOS Devices]
After *itsm.mobileconfig* file has been installed, please download and install the Comodo Client from:
https://dl.cmdm.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

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



Comodo ITSM
2 settings

Comodo ITSM
COMODO GROUP LTD. Verified

Description Configuration IT and Security Manager
Signed *.cmdm.comodo.com
Installed 08-Jul-2016, 2:11 PM

Settings SCEP Enrollment Request
OS X
Mobile Device Management

DETAILS

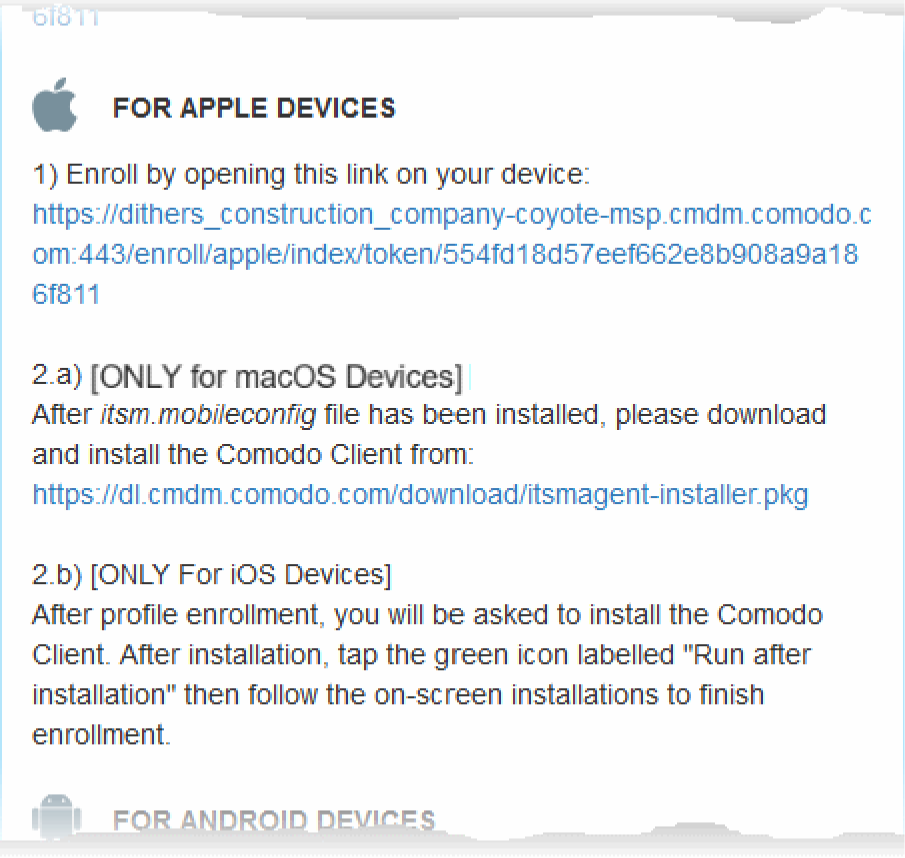
Mobile Device Management

Description COMODO GROUP LTD. ITSM
Server https://coyote-

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 Devices' to download the ITSM agent for Mac.



6f811

FOR APPLE DEVICES

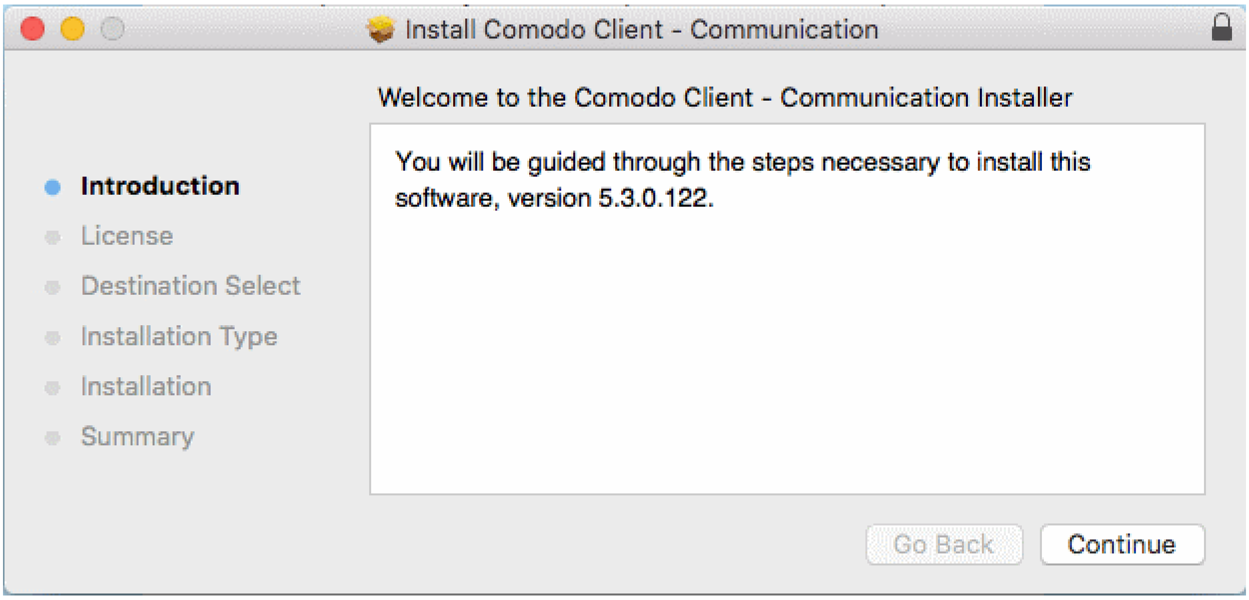
1) Enroll by opening this link on your device:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/apple/index/token/554fd18d57eef662e8b908a9a186f811

2.a) [ONLY for macOS Devices]
After *itsm.mobileconfig* file has been installed, please download and install the Comodo Client from:
https://dl.cmdm.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

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

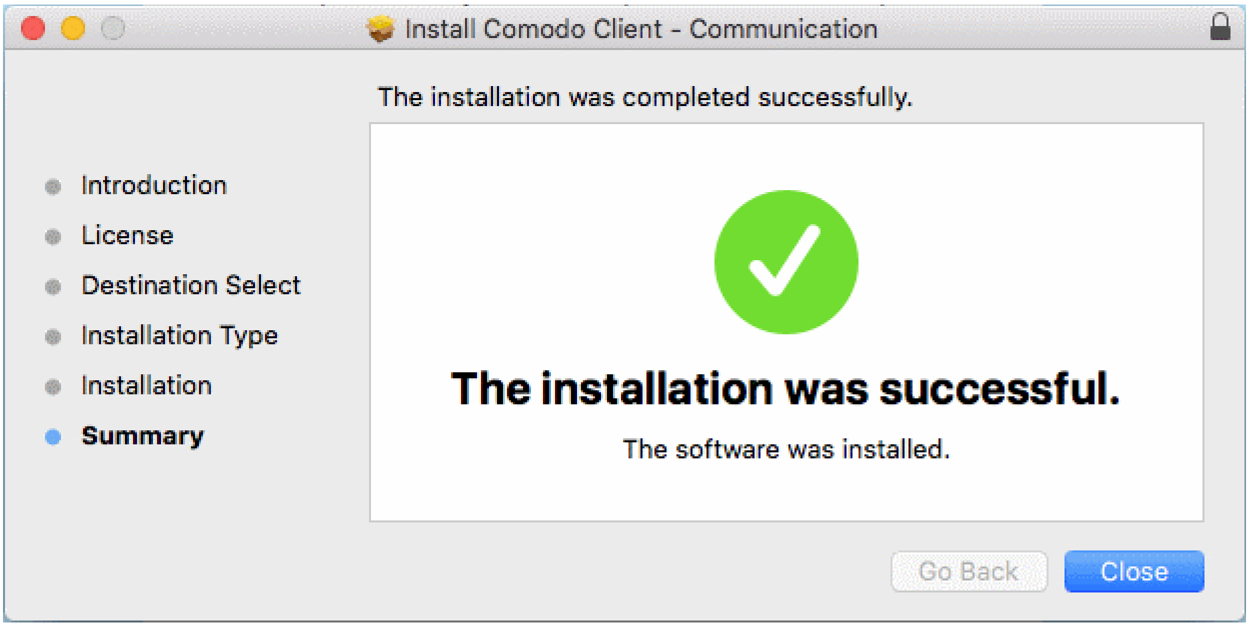


Welcome to the Comodo Client - Communication Installer

You will be guided through the steps necessary to install this software, version 5.3.0.122.

- The user follows the wizard and completes the installation.

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



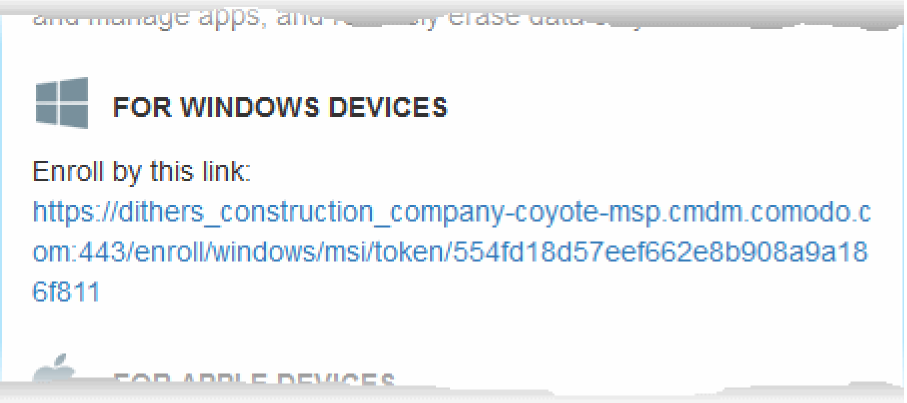
The installation was completed successfully.

The installation was successful.

The software was installed.

Enroll Windows PCs

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



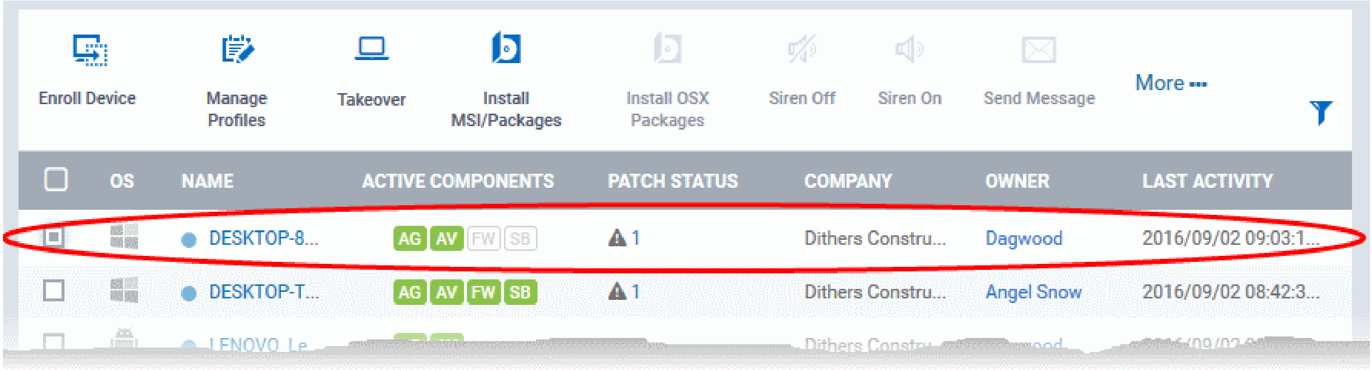
FOR WINDOWS DEVICES

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

FOR APPLE DEVICES

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

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

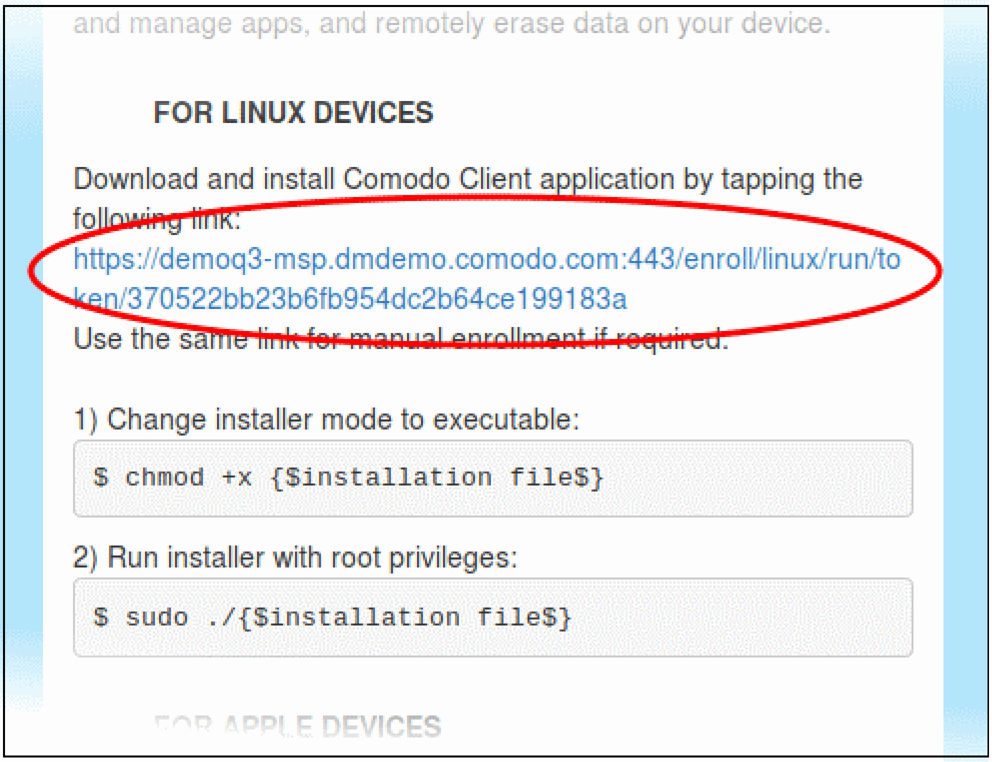


□	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
☒		● DESKTOP-8...	AG AV FW SB	⚠ 1	Dithers Constru...	Dagwood	2016/09/02 09:03:1...
□		● DESKTOP-T...	AG AV FW SB	⚠ 1	Dithers Constru...	Angel Snow	2016/09/02 08:42:3...

The 'Device List' interface contains a list of all enrolled devices with columns that indicate the device IMEI, owner, platform and more. The interface allows you to quickly perform remote tasks on selected devices, including device wipe/lock/unlock/shutdown, siren on/off, install apps, password set/reset and more.

Enroll Linux Devices

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



and manage apps, and remotely erase data on your device.

FOR LINUX DEVICES

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

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

FOR APPLE DEVICES

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

The ITSM agent setup file will be downloaded.

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

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

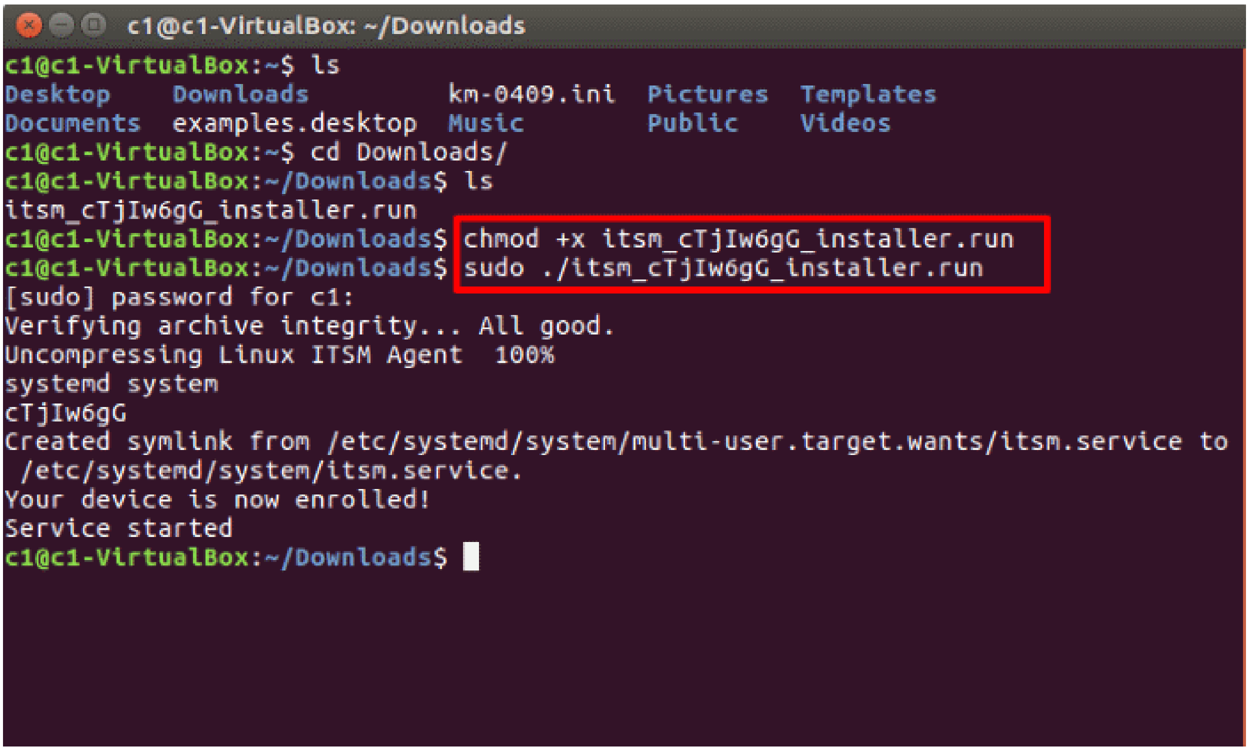
   $ chmod +x {$installation file$}

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

   $ sudo ./{$installation file$}

For example:

```
chmod +x itsm_cTjIw6gG_installer.run
sudo./itsm_cTjIw6gG_installer.run
```



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

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

See **Devices** for more details.

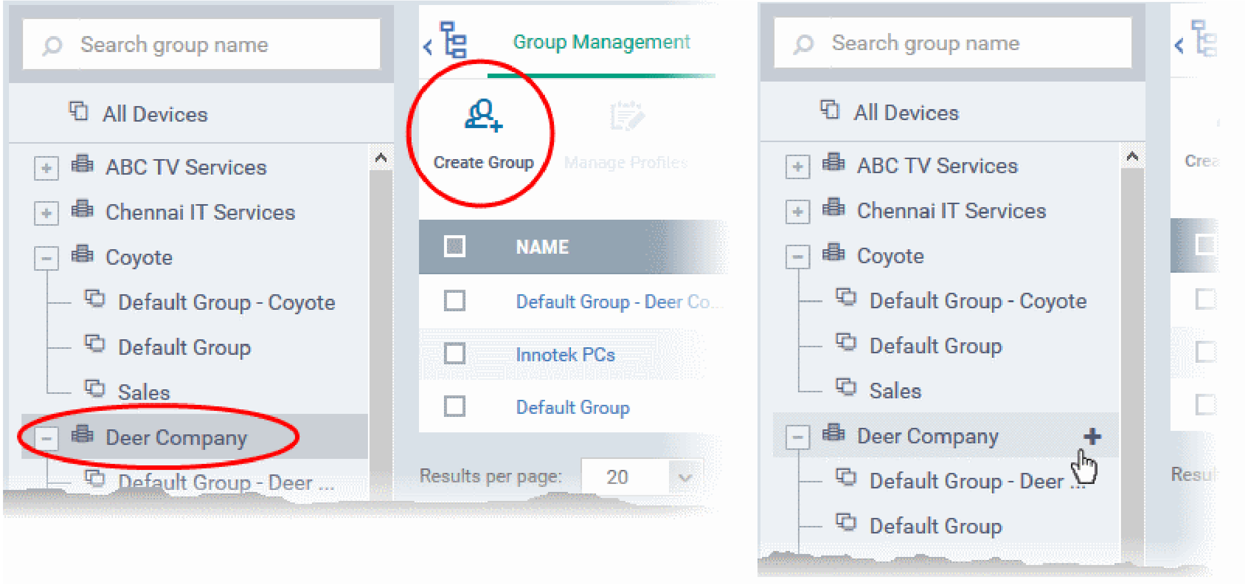
Step 5 - Create Groups of Devices (optional)

- You can create groups of Android, iOS and Windows devices to view, manage and apply policies to large numbers of devices. Dedicated configuration profiles can be created for each group.
- Each group can contain devices of different OS types. OS specific profiles which are applied to a group will be deployed appropriately.
  - C1 MSP customers can create separate device groups for each Company/Organization in their account.
  - C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.

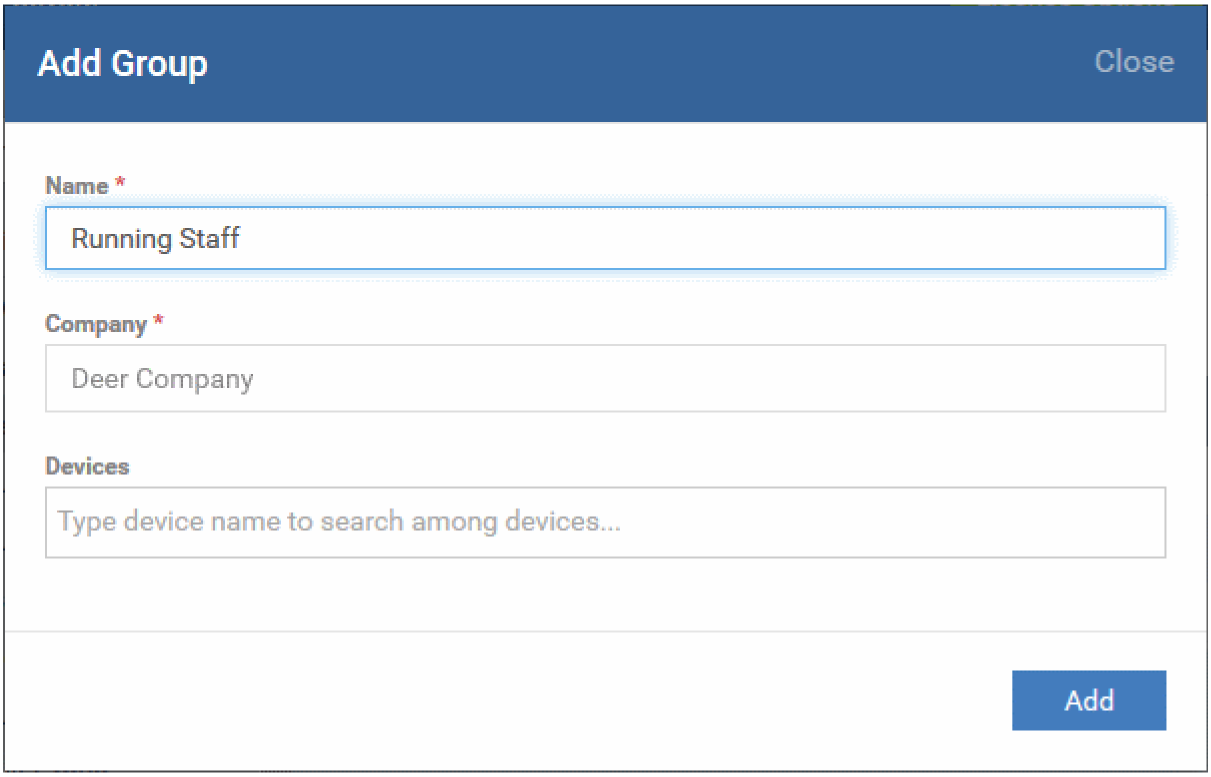
See **Managing Companies** if you need more help with this.

To create a device group

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



The 'Add Group' interface will open:



Name *

Running Staff

Company *

Deer Company

Devices

Type device name to search among devices...

- You now have to name the group and choose the device(s). Enter a name in the 'Name' field. Type the first few letters of the device name in the Devices field and choose the device from the drop-down that appears. Repeat the process to add more devices.
  - You can also add devices after the group is created. Click on the group name then click the 'Add to Group' button. You can then select devices from the list.
- Click 'OK'. Repeat the process to create more groups. See **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 iOS, Android, Windows or Mac OS devices.
- Devices must have been enrolled to ITSM before a profile can be applied to them.

- Each profile allows you to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.
- You can designate a profile as 'Default'. Default profiles are automatically applied to newly enrolled devices. There are default profiles for all supported operating systems (Windows, Mac, iOS, Android).
- You can also create custom profiles for users and user groups. Any custom user profiles you create will be applied to devices instead of the default profile.
- If no custom profiles exist then the default profile will be automatically applied. This ensures all devices have a working profile installed. If you remove a custom profile then the default profile will be automatically installed to take its place.

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

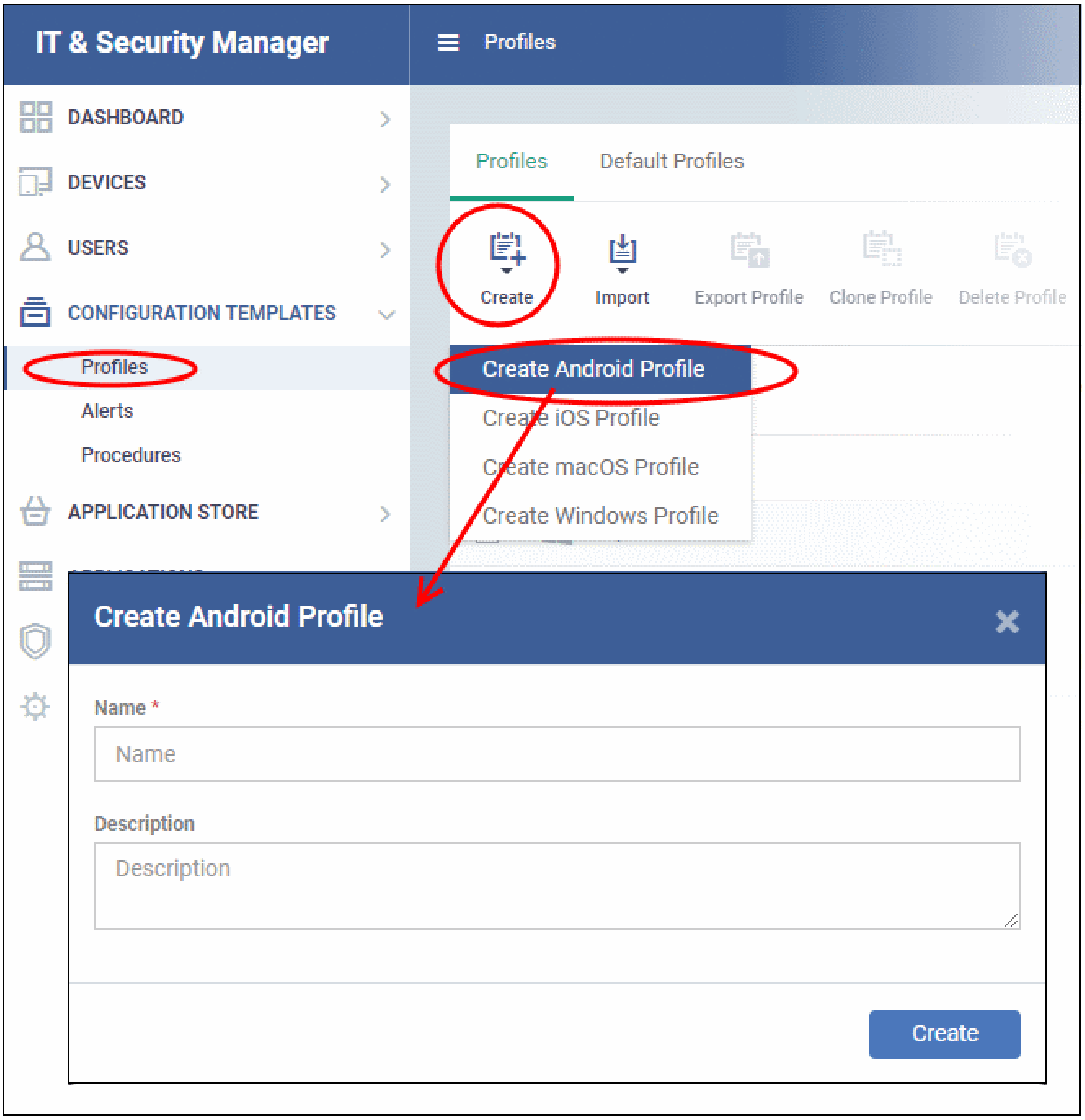
Profiles are applied at the time a device connects to the network. Profile settings will remain in effect until such time as the ITSM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

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

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

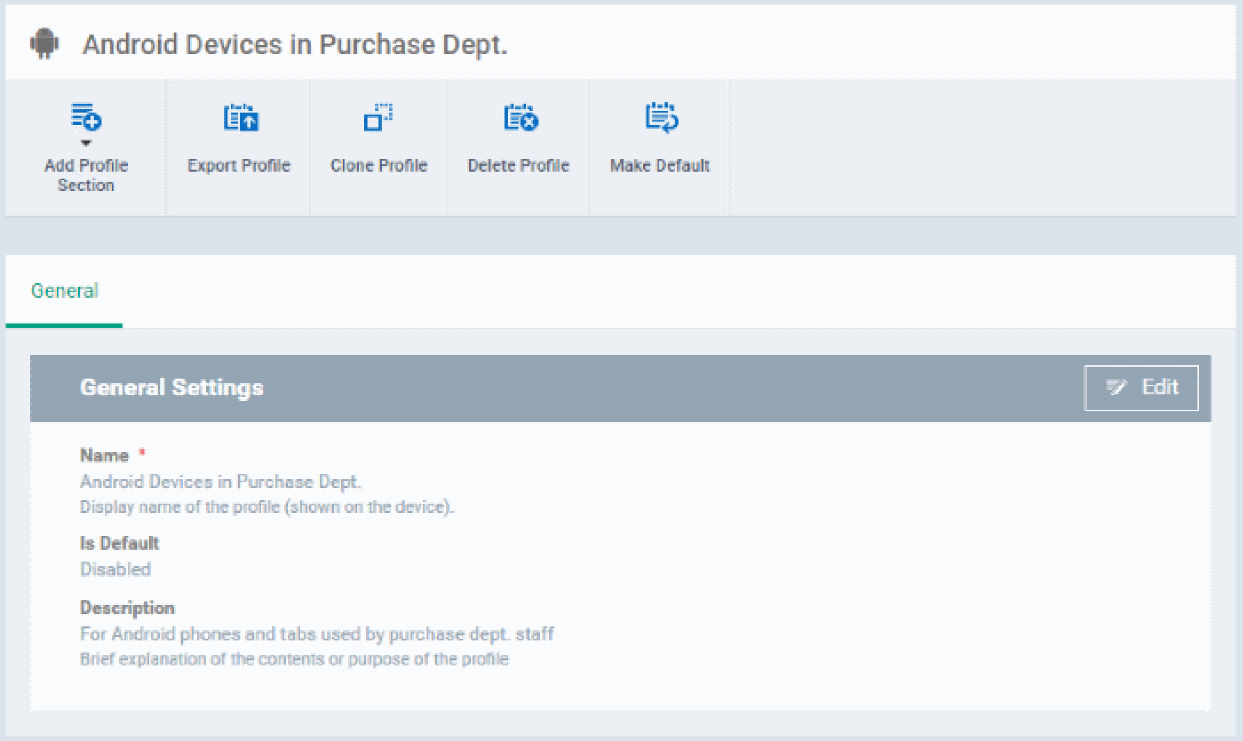
To create an Android Profile

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



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

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



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

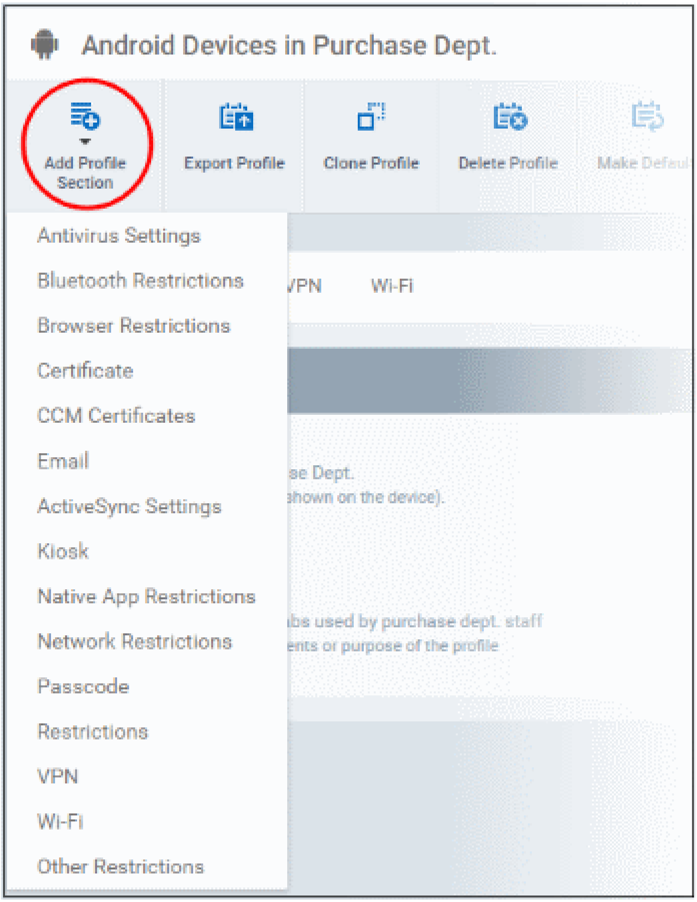
Is Default
Disabled

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

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

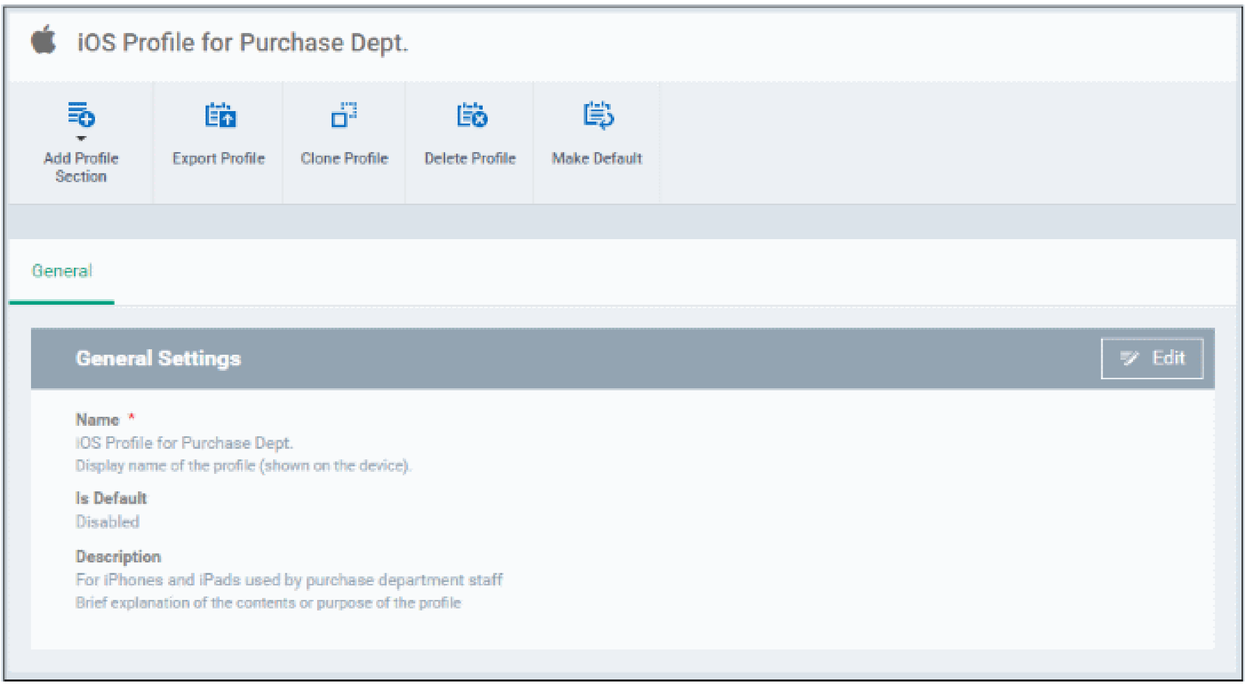
- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied upon device enrollment.
- **Antivirus Settings** - Schedule antivirus scans on the device and specify trusted Apps to be excluded 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). Note - The CCM Certificates section will appear only if you have integrated your ITSM server with your CCM account. For more details, refer to the section **Integrating with Comodo Certificate Manager.**
- **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.



Name *
iOS Profile for Purchase Dept.
Display name of the profile (shown on the device).

Is Default
Disabled

Description
For iPhones and iPads used by purchase department staff
Brief explanation of the contents or purpose of the 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 Edit on the right of the 'General' settings screen and enable the 'Is Default' check box.
- Click 'Save'.

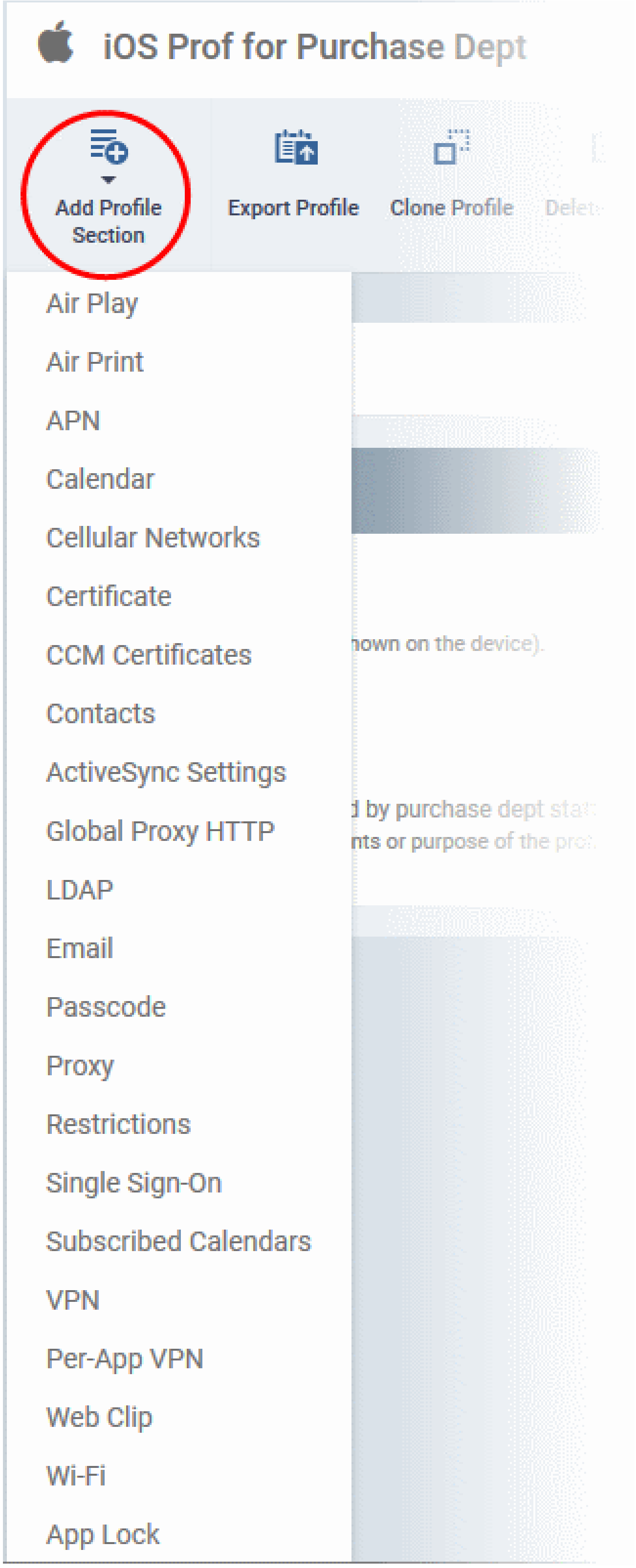
The next step is to add components for the profile.

- 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),

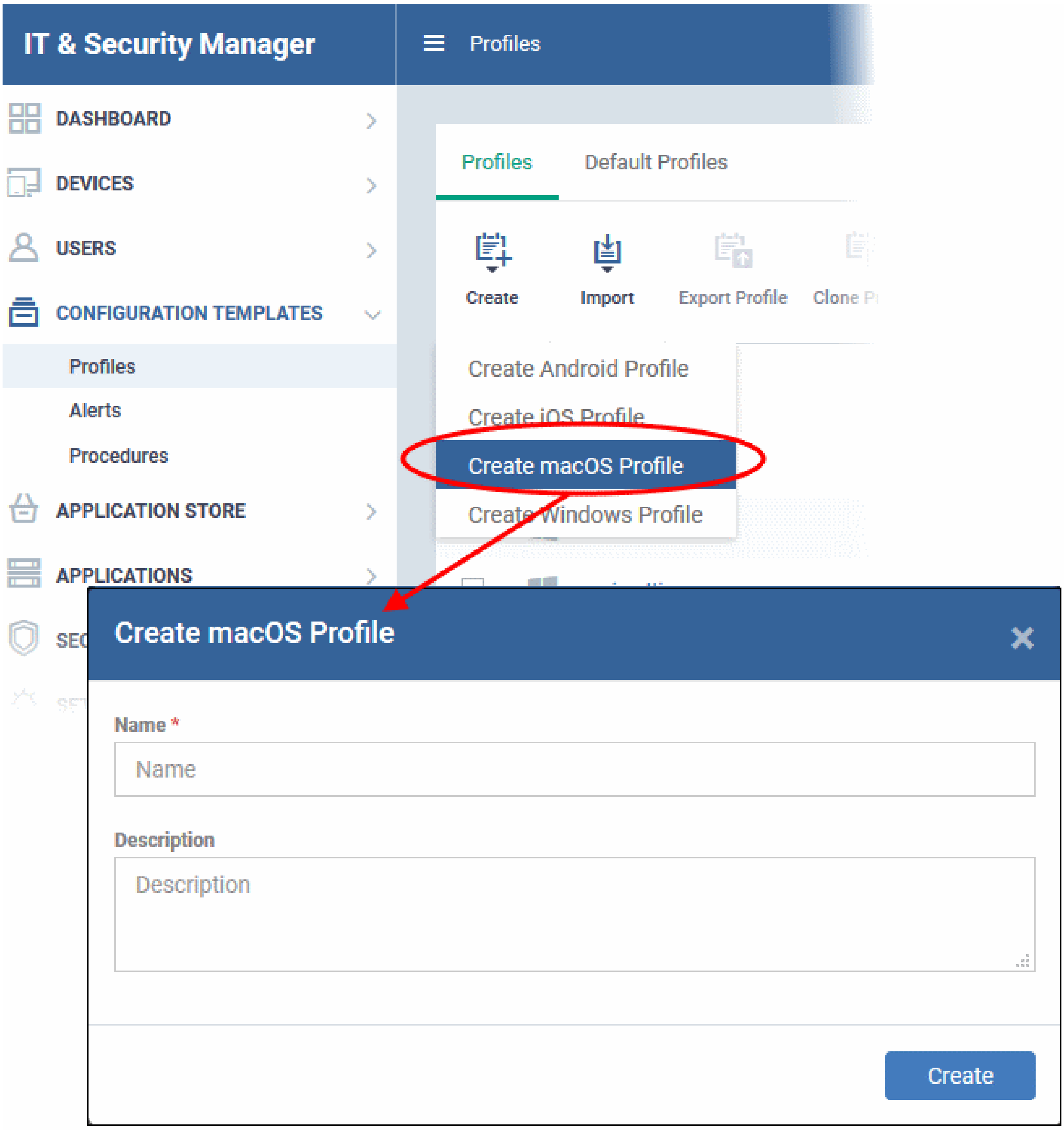
username/password and the address/port of the poxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.

- **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). Note - The CCM Certificates section will appear only if you have integrated your ITSM server with your CCM account. For more details, refer to the section **Integrating with Comodo Certificate Manager.**
- **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.

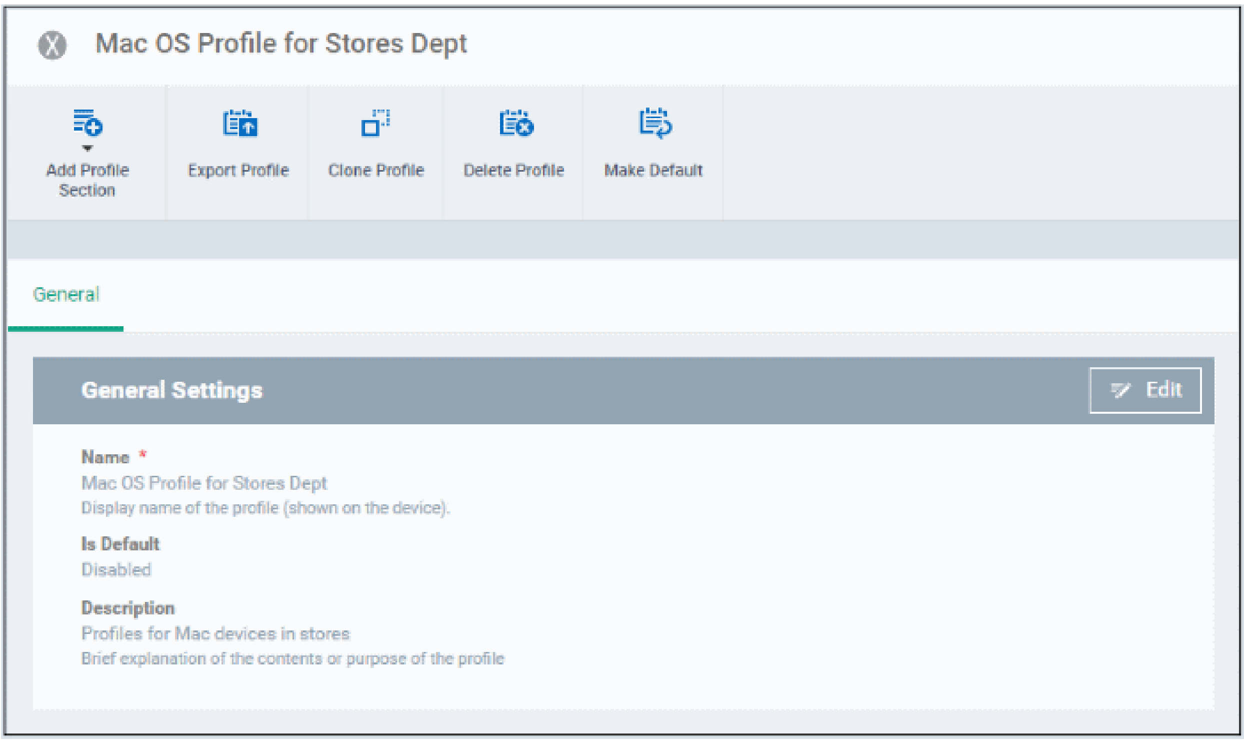
- **App Lock** - Configure restrictions on usage of device resources for selected applications.

To create Mac OS Profile

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



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



Name *
Mac OS Profile for Stores Dept
Display name of the profile (shown on the device).

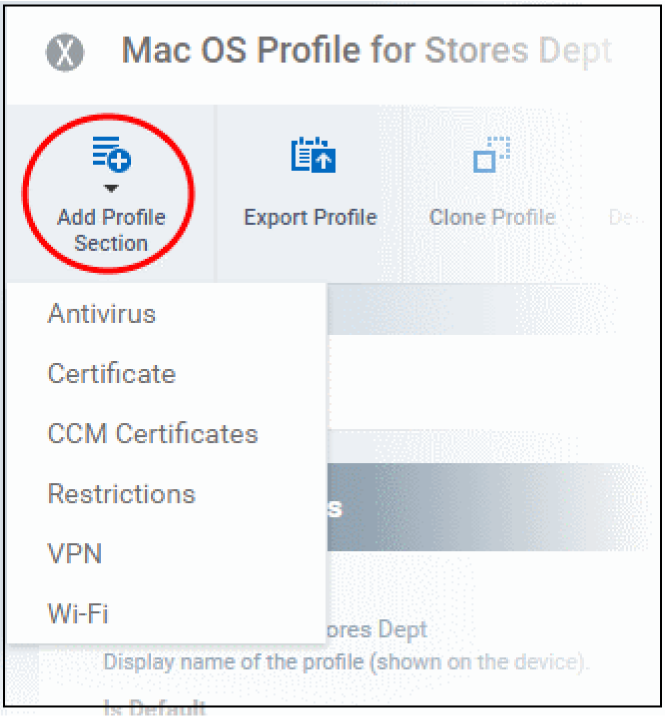
Is Default
Disabled

Description
Profiles for Mac devices in stores
Brief explanation of the contents or purpose of the profile

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

The next step is to add components for the profile.

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

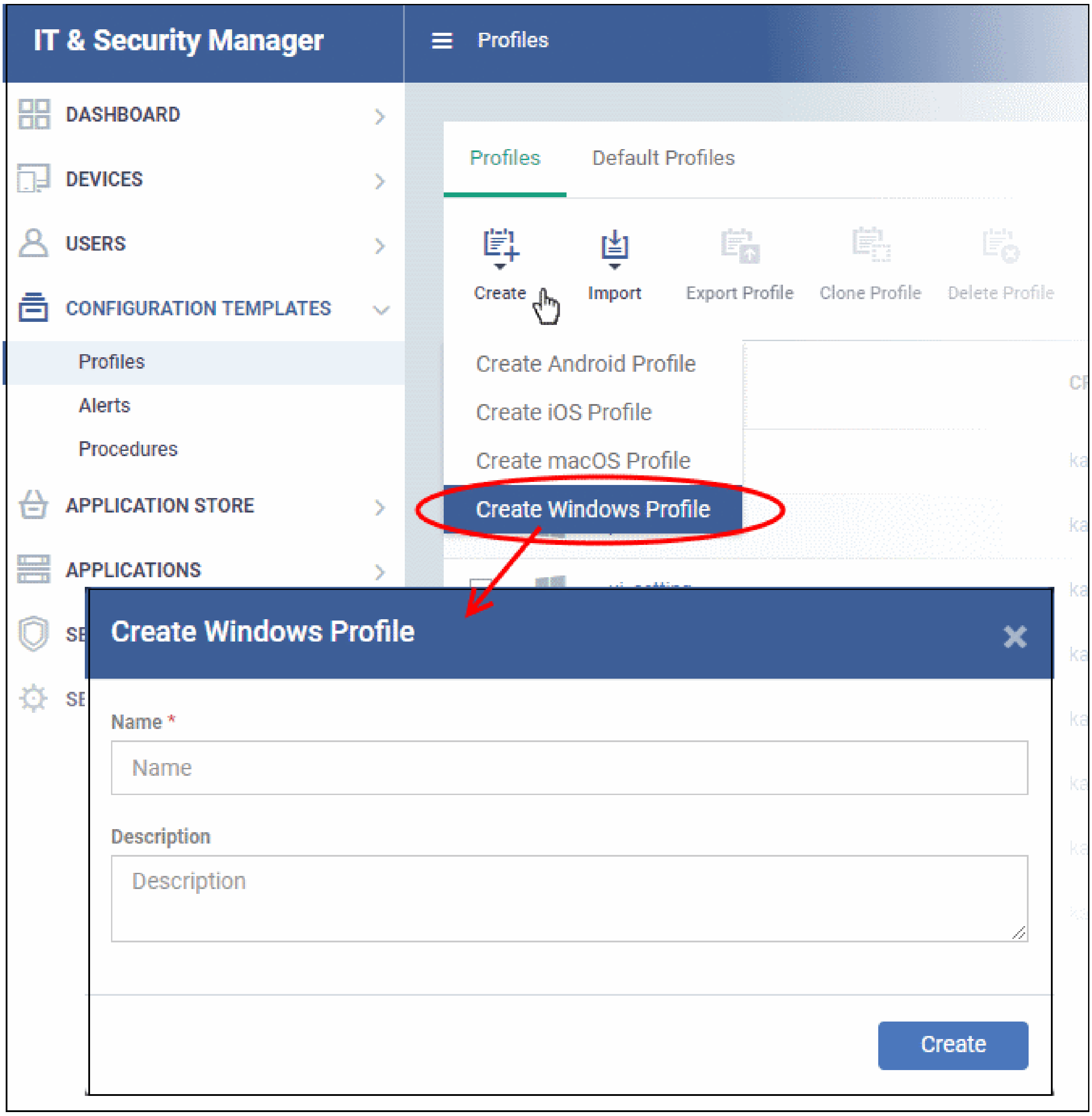


- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.

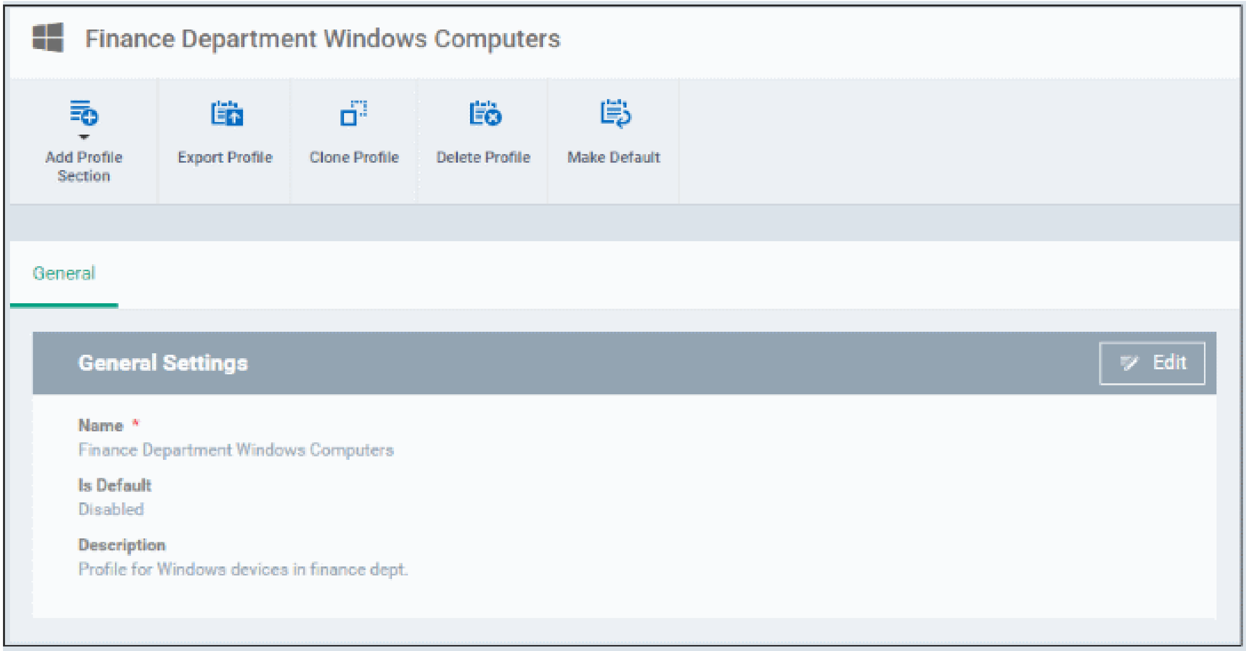
- **Certificates** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings like 'Wi-Fi and 'VPN'.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The CCM Certificates section will appear only if you have integrated your ITSM server with your CCM account. For more details, refer to the section **Integrating with Comodo Certificate Manager.**
- **Restrictions** - Configure restrictions on device functionality and features, iCloud access and so on.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location and more.
- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected.
- **Remote Control** - Allows you to configure settings for remote takeover and notifications which are shown to end-users before and during a remote control session.

To create a Windows profile

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



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



Finance Department Windows Computers

Name *
Finance Department Windows Computers

Is Default
Disabled

Description
Profile for Windows devices in finance dept.

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

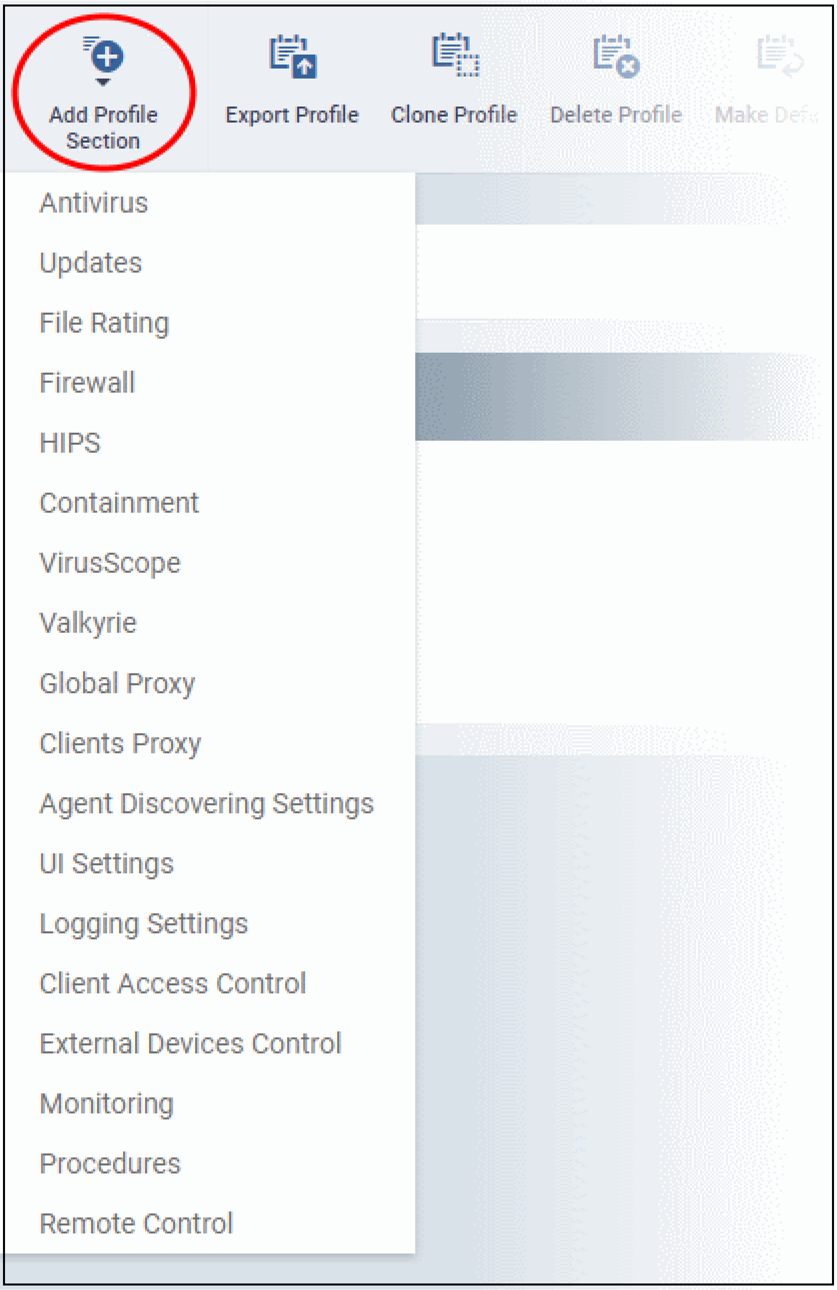
The next step is to add components for the profile.

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

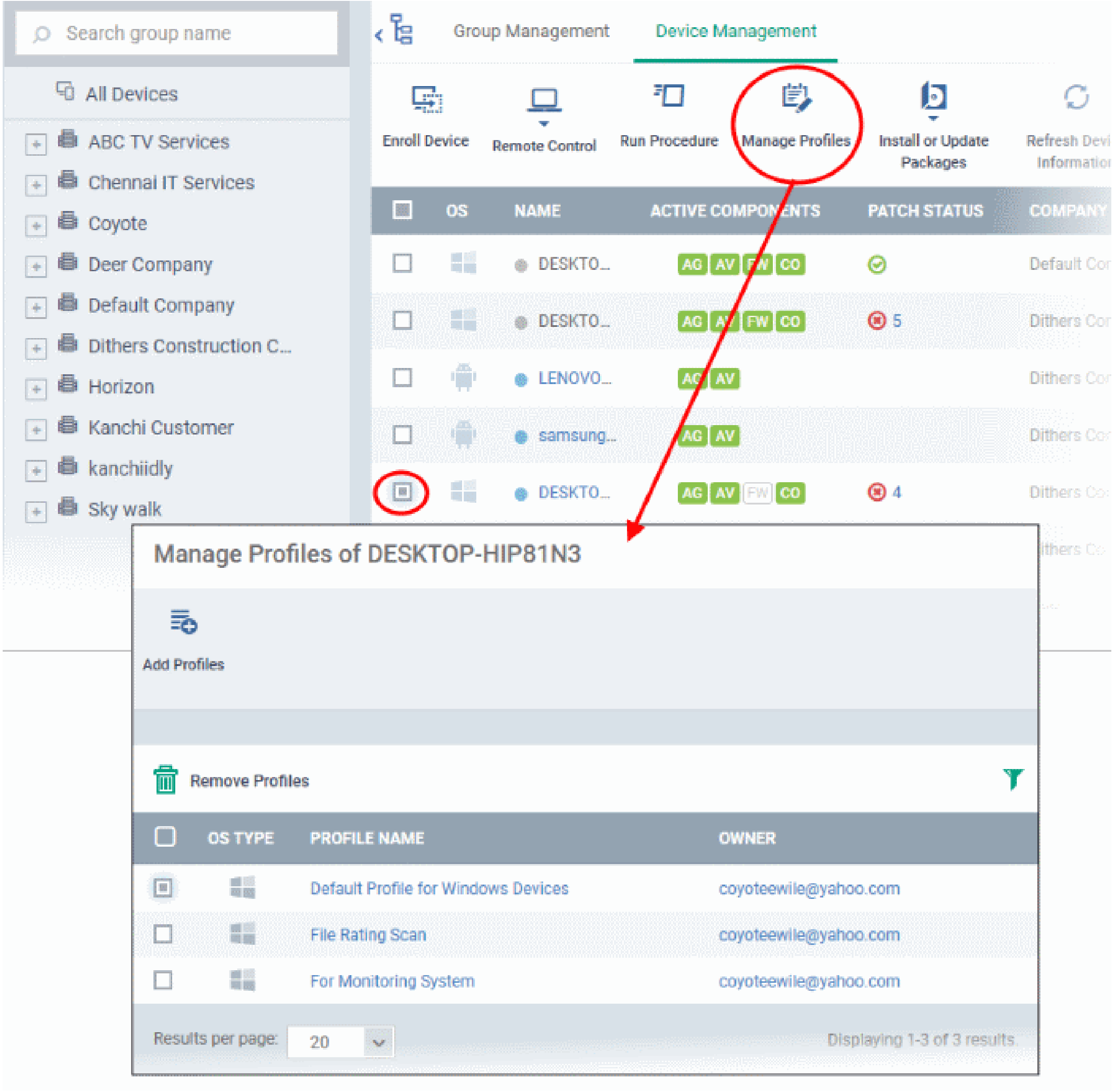
behavior and alert options and view and manage Containment Rules for auto-containing applications. See help page explaining **Containment** in **CCS online help guide**, for more details on Containment in CCS.

- **VirusScope** - Enable VirusScope that monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten your privacy and/or security and configure options for alert generation. See **help page explaining VirusScope**, for more details on VirusScope in CCS online help guide.
- **Valkyrie** - Valkyrie is a cloud based file analysis system. look-up system. It uses a range of static and dynamic detectors including heuristics, file look-up, real-time behavior analysis and human expert to analyze the submitted files and determine if the file is good or bad (malicious). You can enable Valkyrie and its components and set a schedule for submitting unknown files identified from the endpoints.
- **Proxy** - Allows you to specify a proxy server to be used by the device for network connections.
- **Agent Discovery Settings** - Allows you to specify whether or not Comodo Client should send logs to ITSM above antivirus and containment events.
- **UI Settings** - Configure the appearance of Comodo Client Communication (CCC) and Comodo Client Security (CCS). You can re-brand CCC and CCS with your own company name, logo, product name and product logo and select which components of CCS should be visible to end-users.
- **Logging Settings** - Allows you to enable logging events from CCS, the maximum size of the log file and configure behavior once log file reaches the maximum file size.
- **Monitoring Settings** - Allows you to configure performance and availability conditions for various events and services. An alert will be triggered if the conditions are breached. For example, you can monitor free disk space, service and web page availability, CPU/RAM usage, device online status and more.
- **CCM Certificates** - Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The CCM Certificates section will appear only if you have integrated your ITSM server with your CCM account. See **Integrating with Comodo Certificate Manager**, for more details.
- **Procedures** - Allows you to add, view, delete and prioritize procedures which have been added to a profile.
- **Remote Control** - Allows you to configure settings for remote takeover and notifications which are shown to end-users before and during a remote control session.

Step 7 - Apply profiles to devices or device groups

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

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



☐	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY
☐		DESKTO...	AG AV FW CO	✓	Default Cor
☐		DESKTO...	AG AV FW CO	⊗ 5	Dithers Cor
☐		LENOVO...	AG AV		Dithers Cor
☐		samsung...	AG AV		Dithers Cor
☒		DESKTO...	AG AV FW CO	⊗ 4	Dithers Co

Manage Profiles of DESKTOP-HIP81N3

☐	OS TYPE	PROFILE NAME	OWNER
☒		Default Profile for Windows Devices	coyoteewile@yahoo.com
☐		File Rating Scan	coyoteewile@yahoo.com
☐		For Monitoring System	coyoteewile@yahoo.com

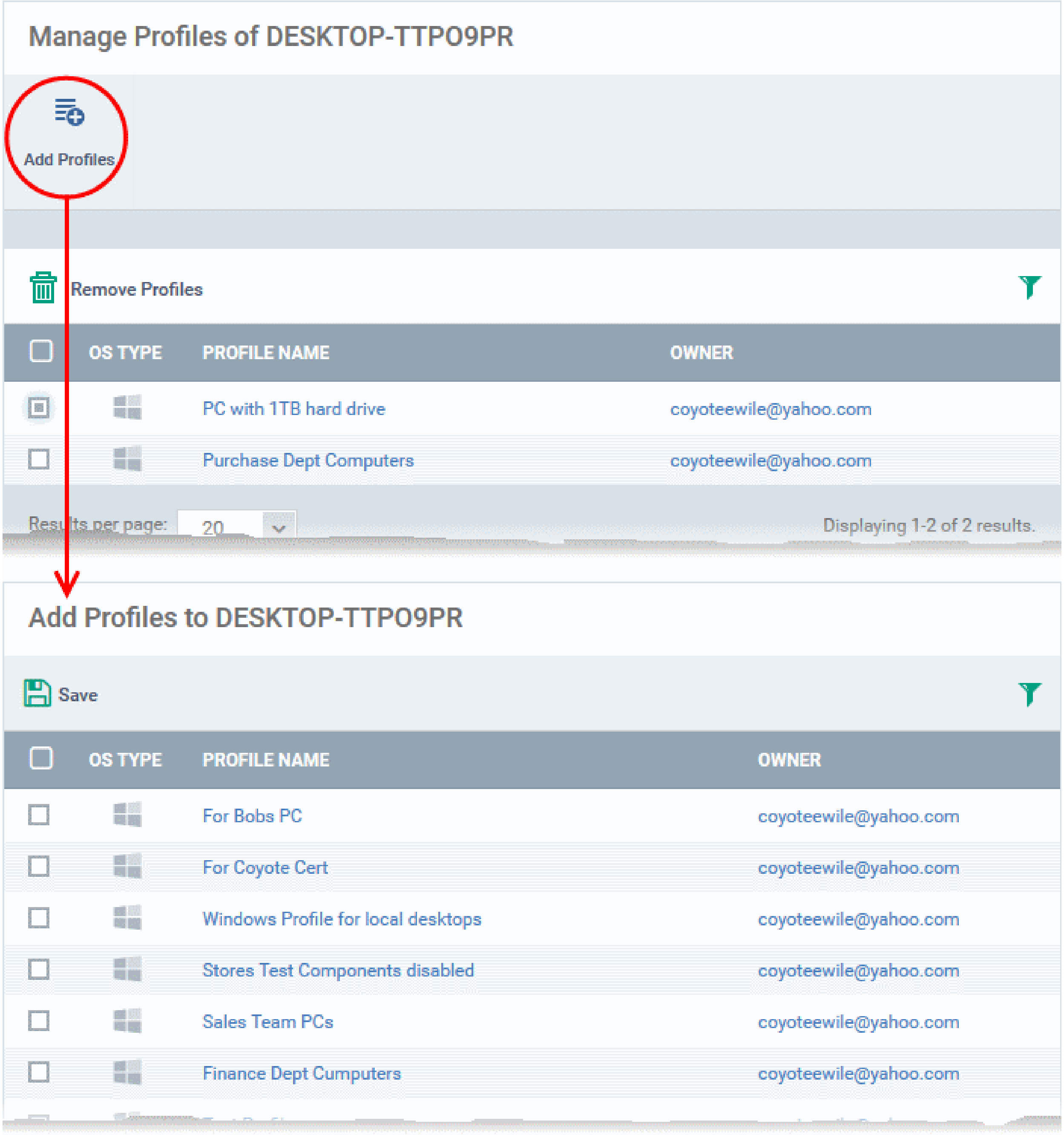
Results per page: 20

Displaying 1-3 of 3 results

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

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

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



Manage Profiles of DESKTOP-TTPO9PR

□	OS TYPE	PROFILE NAME	OWNER
▣		PC with 1TB hard drive	coyoteewile@yahoo.com
□		Purchase Dept Computers	coyoteewile@yahoo.com

Results per page: 20 Displaying 1-2 of 2 results.

Add Profiles to DESKTOP-TTPO9PR

□	OS TYPE	PROFILE NAME	OWNER
□		For Bobs PC	coyoteewile@yahoo.com
□		For Coyote Cert	coyoteewile@yahoo.com
□		Windows Profile for local desktops	coyoteewile@yahoo.com
□		Stores Test Components disabled	coyoteewile@yahoo.com
□		Sales Team PCs	coyoteewile@yahoo.com
□		Finance Dept Cumputers	coyoteewile@yahoo.com

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

To apply profiles to a *group* of devices

The procedure is similar to adding profile(s) to a device except for the second step.

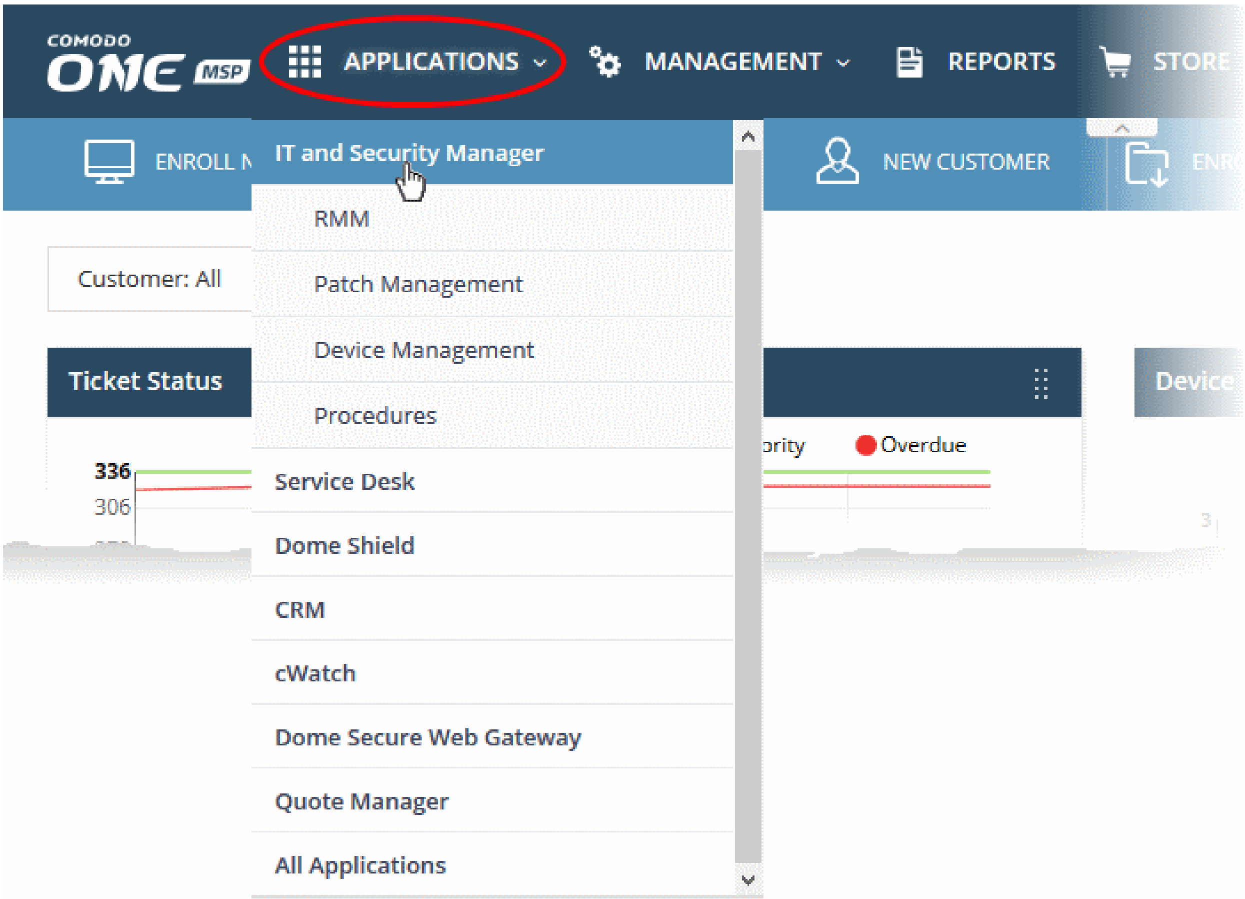
1. Click the 'Devices' tab on the left and choose 'Device List ' from the options.
2. Click the 'Group Management' tab
3. Choose the Company to view the list of groups in the right pane (for C1 MSP customers)
4. Click the name of the device group
5. Click 'Manage Profiles'
6. Select the profile(s) to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

If you have successfully followed all 7 steps of this quick start guide then you should have a created a basic working environment from which more detailed strategies can be developed. Should you need further assistance, each topic is covered in more granular detail in the full administrator guide. If you have problems that you feel have not been addressed, then please contact mdmsupport@comodo.com.

1.4. Login into the Admin Console

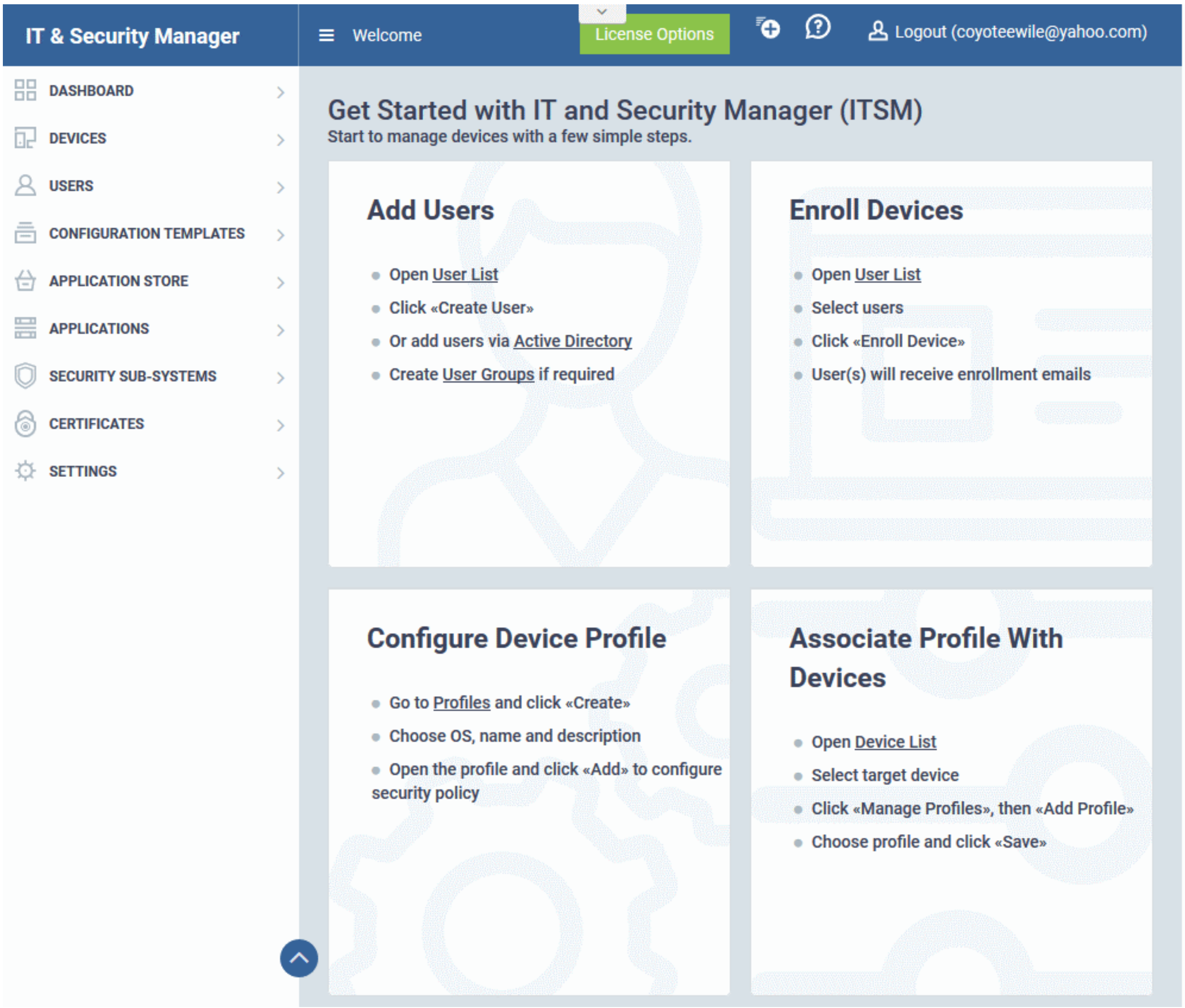
After sign-up, you will receive an email containing your username and an account activation link. Click the link to activate your account and set your password. Once activated, you can login to ITSM using any internet browser.

- C1 customers:
  - Login at **https://one.comodo.com/app/login**
  - Click 'Applications' > 'IT and Security Manager'.
- ITSM standalone customers:
  - Login at: https://<*your company name*>.cmdm.comodo.com/user/site/login - where <your company name> is your ITSM company name.
  - You will have received a confirmation email with this URL.
- Username and password are case sensitive. Please make sure that you use the correct case and caps lock is OFF.
- Click the 'I forgot my password' if you can't remember your password. A mail will be sent to your registered email with a link which will allow you to reset your password.



Tip: The shortcuts below 'IT and Security Manager' in the drop-down allow you to open the respective interface in ITSM.

The ITSM welcome screen will be displayed.



Get Started with IT and Security Manager (ITSM)

Start to manage devices with a few simple steps.

Add Users

- Open User List
- Click «Create User»
- Or add users via Active Directory
- Create User Groups if required

Enroll Devices

- Open User List
- Select users
- Click «Enroll Device»
- User(s) will receive enrollment emails

Configure Device Profile

- Go to Profiles and click «Create»
- Choose OS, name and description
- Open the profile and click «Add» to configure security policy

Associate Profile With Devices

- Open Device List
- Select target device
- Click «Manage Profiles», then «Add Profile»
- Choose profile and click «Save»

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. See '**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. See '**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. See **Enrolling User Devices for Management** for more details.

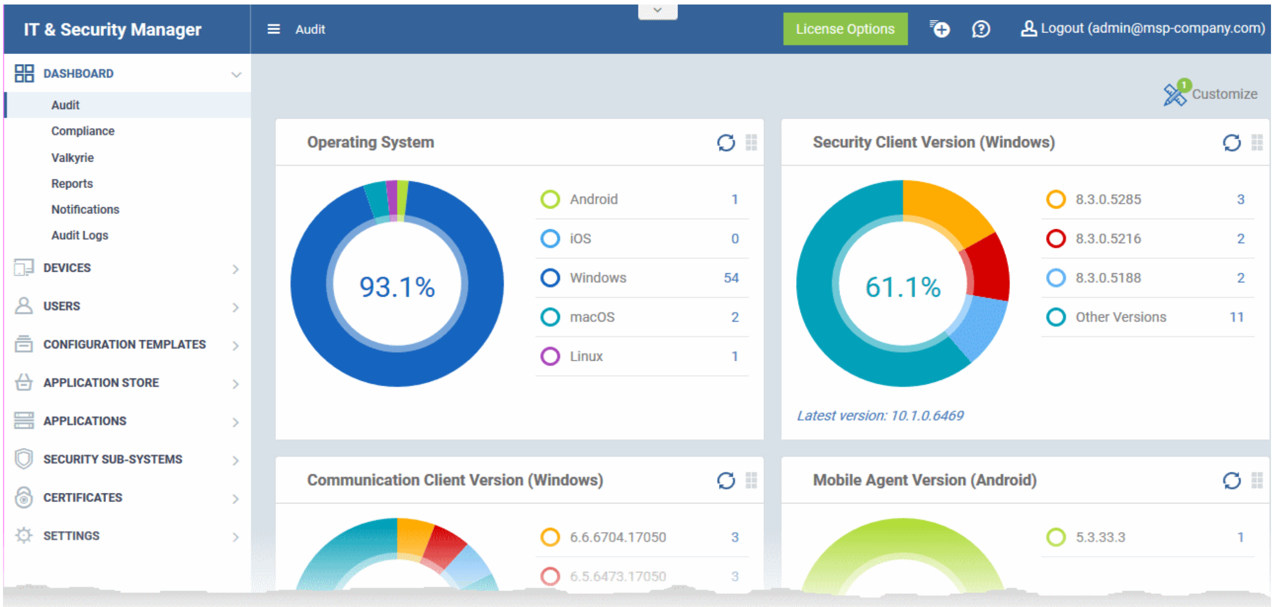
- **Configure Device Profile** - Allows you to create and manage configuration profiles for Android, iOS and Windows devices by clicking the ⚙ icon. See **Configuration Profiles** for more details.

- **Associate Profile With Devices** - Allows you to deploy and manage configuration profiles on devices by clicking the ☰ icon. See **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 Admin Console

The admin console is the nerve center of Comodo IT and Security Manager (ITSM), allowing you to add and import users, enroll devices, apply configuration profiles, run virus 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 - Contains charts and graphs which show the structure and security status of devices in your network. 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. See **Devices and Device Groups** for more details.

Users - Allows administrators to create and manage users and user groups, enroll of their devices and assign configuration profiles to devices. See **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 endpoints. See **Configuration Templates** for more details.

Application Store - Allows administrators to add apps to be pushed to managed iOS and Android devices. See **App Store** for more details.

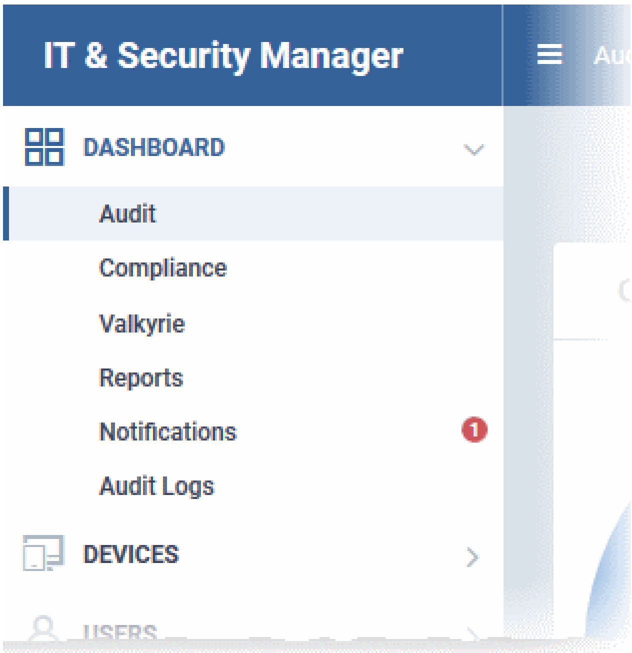
Applications - Allows administrators to view and manage applications installed on enrolled Android and iOS devices, view files installed on managed Windows devices, contained programs, view and manage software vendors list and manage OS patch installation on to managed Windows devices. See **Applications** 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. See **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. See **Manage Certificates Installed on Devices** for more details.

Settings - Allows admins to create admin and user roles with different privileges, configure the behavior of various ITSM components and agents, renew/upgrade licenses and more. See **Configuring Comodo 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. See '**Creating New User Accounts**' and '**Enrolling Users' Devices for Management**' 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.  IT & Security Manager DASHBOARD Audit Compliance Valkyrie Reports Notifications 1 Audit Logs DEVICES USERS
IT & Security Manager	Clicking the logo will open the 'Welcome' screen. See '**Logging into your Administrative Console**' for more details.
Logout (coyoteewile@yahoo.com)	Displays the username of the person currently logged in. Click this to log out of ITSM interface.
License Options	Allows you to upgrade to the Premium or Platinum version of ITSM.

3. The Dashboard

The dashboard displays real-time statistics about the operating system, connection status and security posture of all devices enrolled into 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' link in the left menu.

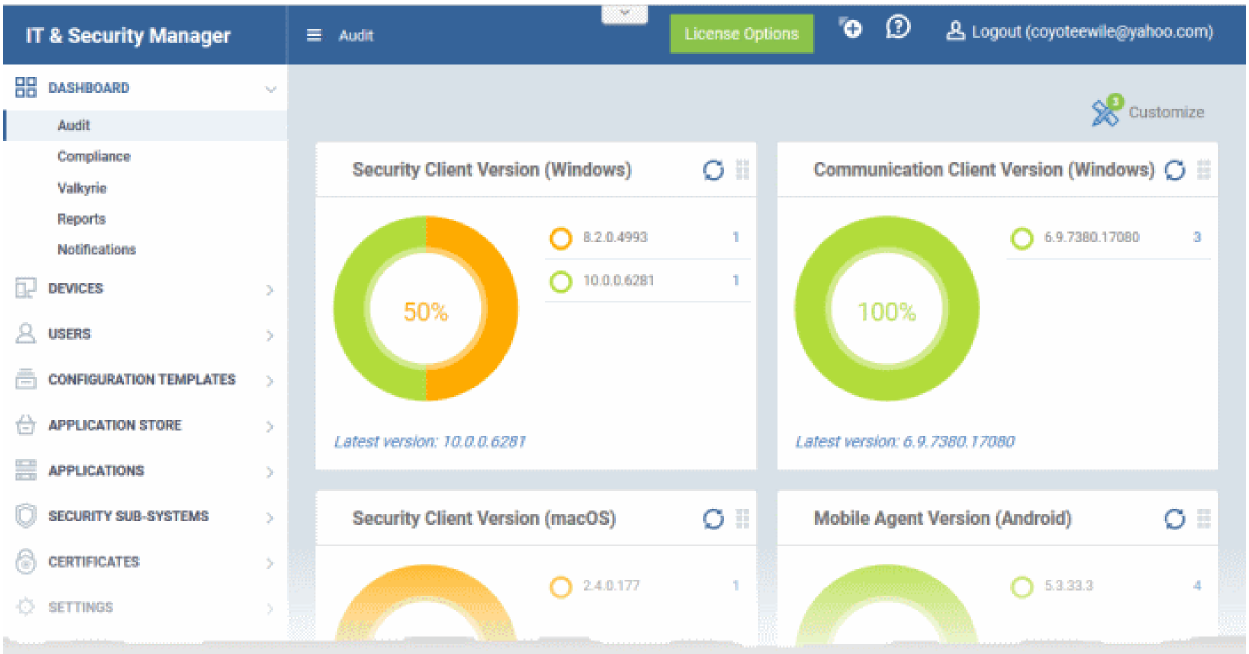
The dashboard is divided into five sections:

- **Audit** - Charts which show the operating systems and client versions installed on devices on your network. Also contains charts which show the types of devices in your network, and whether the devices are personal or corporate. See the **Audit** section for more details.

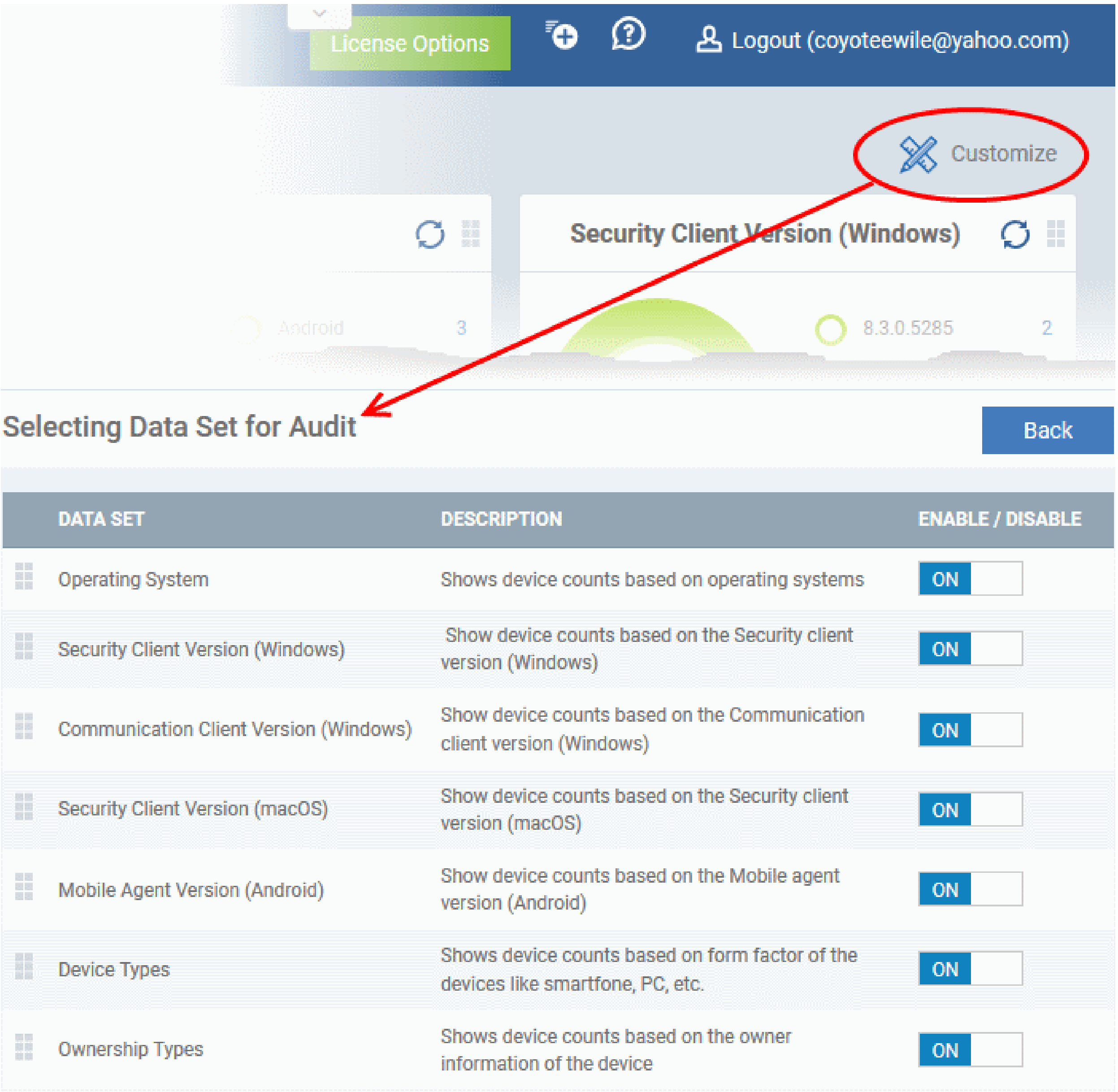
- **Compliance** - Statistics which detail how compliant your devices are with ITSM security policies. For example, device connection status, devices with viruses, devices with blacklisted applications, rooted and jailbroken devices, and device scan status. See **Compliance** for more details.
- **Valkyrie** - A summary of verdicts on unknown files submitted to the Valkyrie file analysis system. See **Valkyrie** for more details.
- **Reports** - A list of all reports generated by ITSM. You can also create new reports from here. See **Reports** section for more information.
- **Notifications** - A list of notifications sent to the administrator by ITSM. See **Notifications** for more details.
- **Audit Logs** - A list of actions taken on managed devices by admins and staff. Example actions include applying profiles, remote installation of packages and more. See **Audit Logs** for more details.

Audit

- Click 'Dashboard' on the left then 'Audit'



- Click 'Customize' at top-right if you want to change which charts are shown on the page


License Options
Logout (coyoteewile@yahoo.com)
Customize
Security Client Version (Windows)
Android
3
8.3.0.5285
2
Back

Selecting Data Set for Audit

DATA SET	DESCRIPTION	ENABLE / DISABLE
Operating System	Shows device counts based on operating systems	ON
Security Client Version (Windows)	Show device counts based on the Security client version (Windows)	ON
Communication Client Version (Windows)	Show device counts based on the Communication client version (Windows)	ON
Security Client Version (macOS)	Show device counts based on the Security client version (macOS)	ON
Mobile Agent Version (Android)	Show device counts based on the Mobile agent version (Android)	ON
Device Types	Shows device counts based on form factor of the devices like smartfone, PC, etc.	ON
Ownership Types	Shows device counts based on the owner information of the device	ON

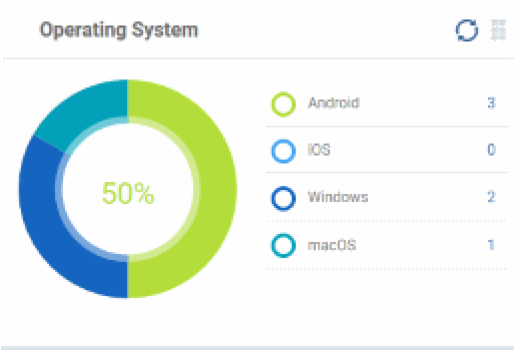
- Use the 'On/Off' switches to add or remove charts from the dashboard
- The 'Customize' icon shows the number of charts removed from the default view

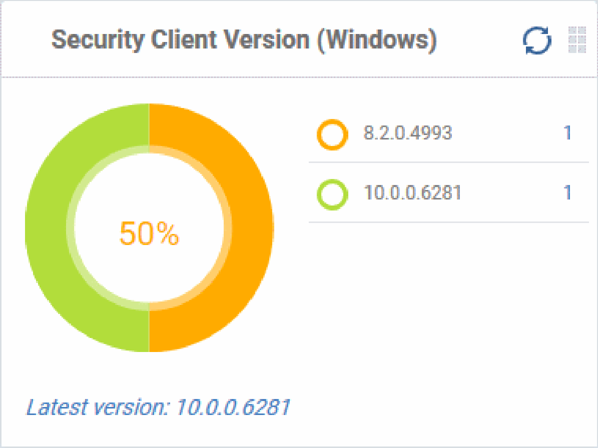
- Click and hold the icon at top right of a tile to move it around the page

Operating System

Shows enrolled devices by operating system. Place your mouse cursor over a sector or the legend to see further details.

Clicking on an item in 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. See '**Devices**' for more details.




Security Client Version (Windows)
8.2.0.4993 1
10.0.0.6281 1
50%
Latest version: 10.0.0.6281

Security Client Version (Windows)

The versions of Comodo Client Security installed on Windows devices on your network. Comodo Client Security is the antivirus/security software on an endpoint.

The number of devices with each version is also shown. Click the number to view all devices which have that version installed. To update to the latest version, click the number, select the target devices then click 'Install or Update Packages'.

The latest available version of the client is shown underneath the chart.

See **Remotely Installing and Updating Packages on Windows Devices** for more details.

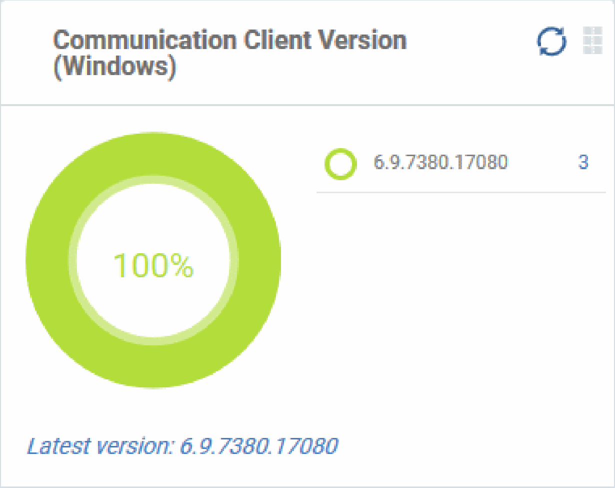
Communication Client Version (Windows)

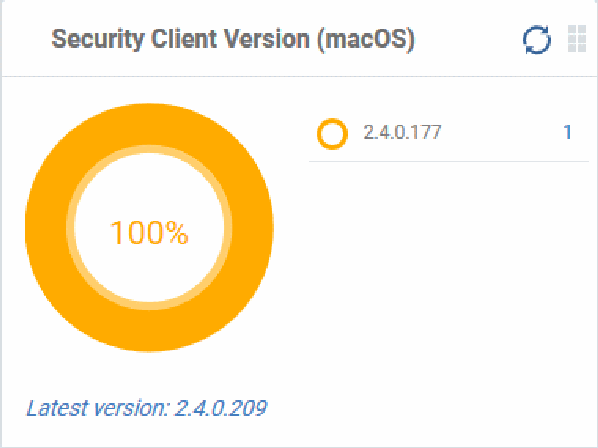
The versions of Comodo Communication Client installed on Windows devices on your network. This is the agent which sends updates to the ITSM console.

The number of devices with each version is also shown. Click the number to view all devices which have that version installed. To update to the latest version, click the number, select the target devices then click 'Install or Update Packages'.

The latest available version of the client is shown underneath the chart.

See **Remotely Installing and Updating Packages on Windows Devices** for more details.


Communication Client Version (Windows)
6.9.7380.17080 3
100%
Latest version: 6.9.7380.17080



Security Client Version (MacOS)

The versions of the security client installed on MAC OS devices on your network. The security client is the Comodo antivirus for MAC software on an endpoint.

The number of devices with each version is also shown. Click the number to view all devices which have that version installed. To update to the latest version, click the number, select the target devices then click 'Install or Update Packages'.

The latest available version of the client is shown underneath the chart.

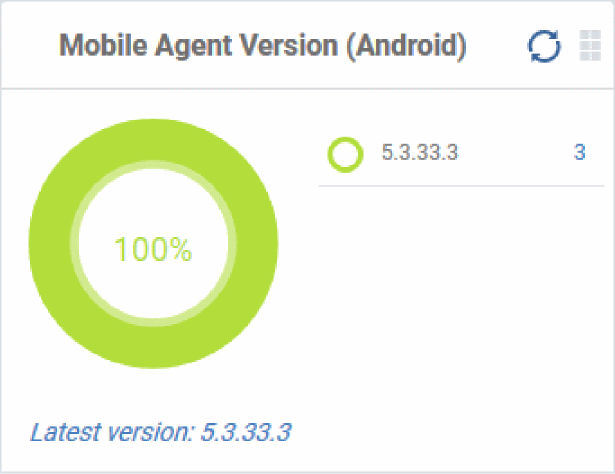
See **Remotely Installing Packages on Mac OS Devices** for more details.

Mobile Agent Version (Android)

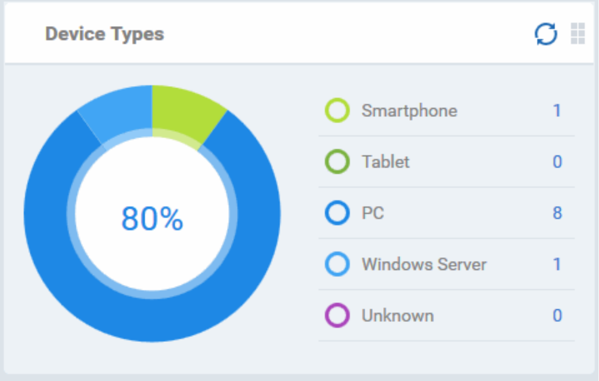
The versions of the mobile agent installed on Android device in your network.

The number of devices with each version is also shown. Click the number to view all devices which have that version installed. To update to the latest version, click the number, select the target devices then click 'Install or Update Packages'.

The latest available version of the client is shown underneath the chart.



Device Types



Shows the composition of your device fleet by device type. Place your mouse cursor over a sector or the legend to see further details.

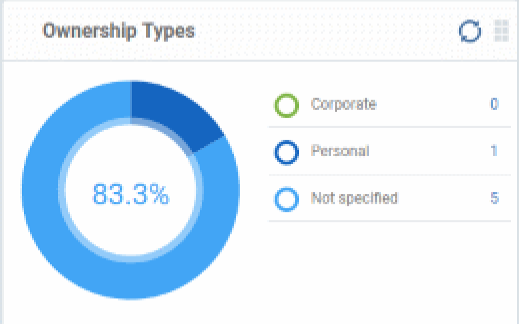
Clicking on an item in the legend will open the respective 'Device List' page. For example, clicking on 'Tablet' in the legend will open the 'Device List' page displaying the list of tablet devices. See '**Devices**' for more details.

Ownership Types

Shows devices by ownership type. This can be 'Corporate', 'Personal' or 'Not Specified'. Place your mouse cursor over a sector or the legend to see further details.

Clicking on an item in 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. See '**Devices**' for more details.

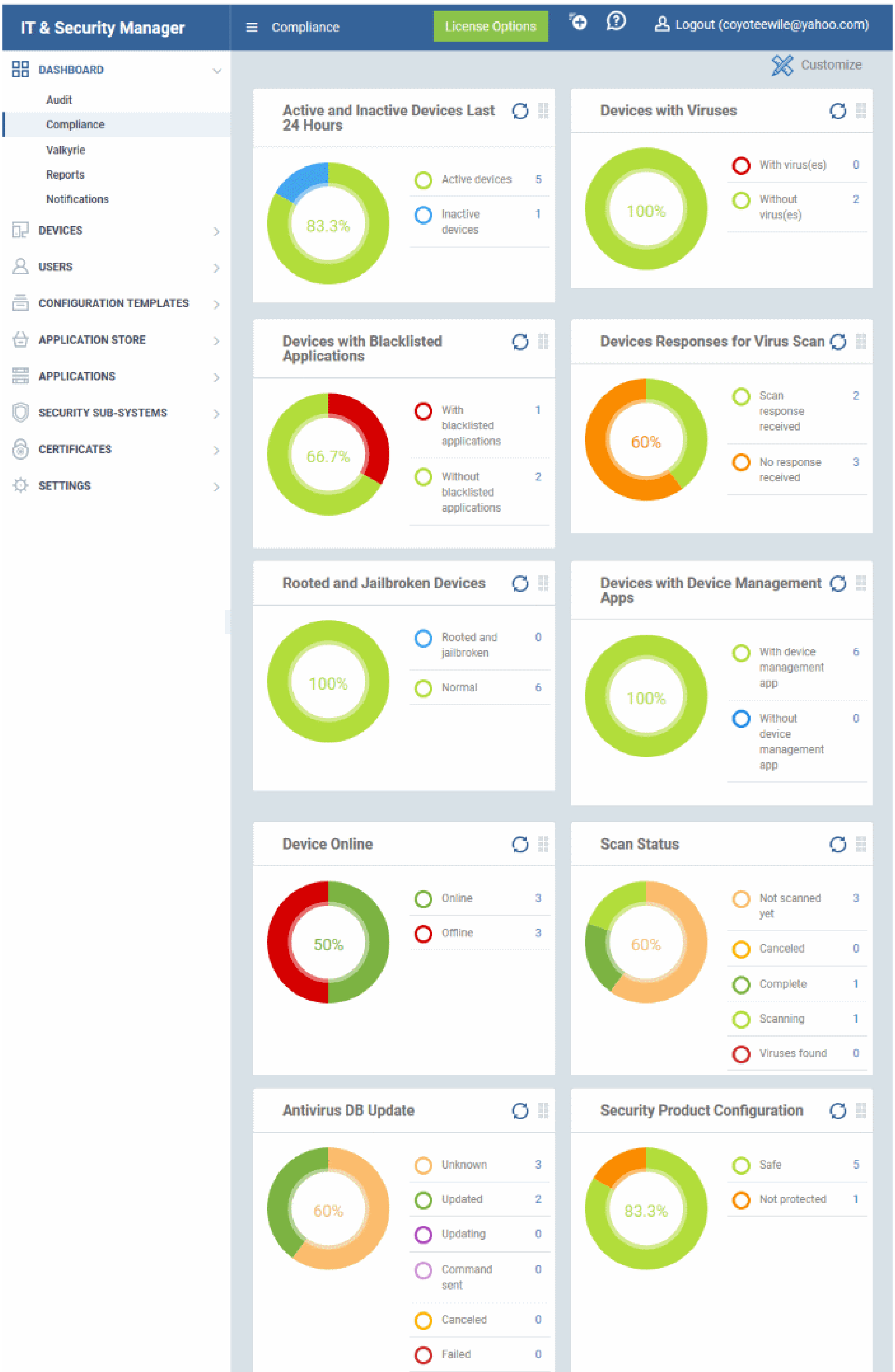
Note: The device ownership type can be changed by administrators from the device details screen > Change ownership and then selecting the ownership type from the options.



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.

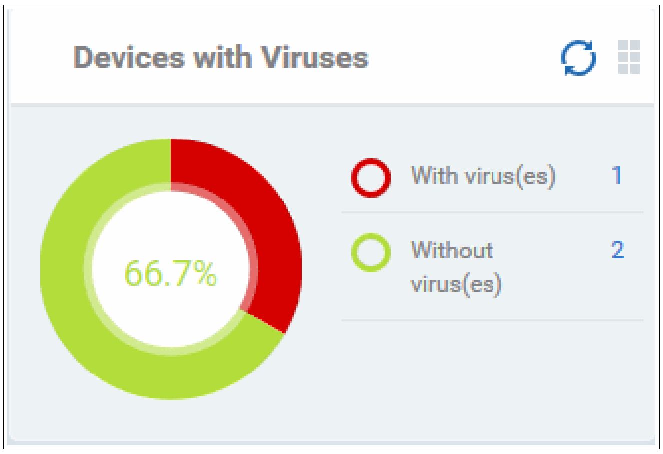
- To view the compliance status of devices, click 'Dashboard' in the left navigation then 'Compliance'.



- 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

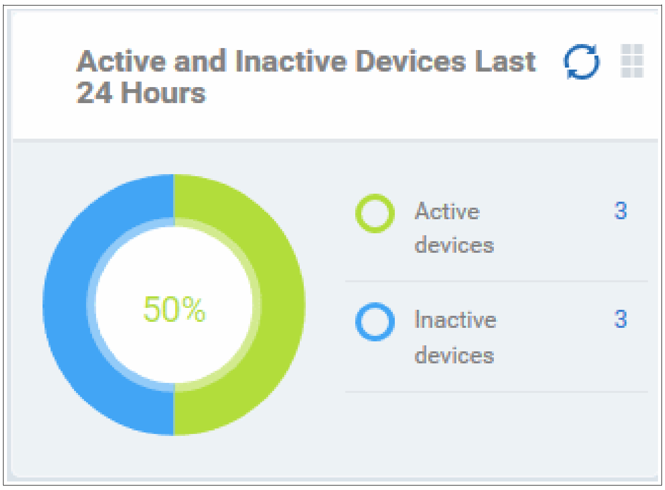
Shows how many enrolled devices are affected by viruses and how many are clean. Placing the mouse cursor over a sector or the legend displays further details. See **Antivirus Scans** for details about scanning for viruses on enrolled devices.



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. See '**Devices**' for more details.

Active and Inactive Devices Last 24 Hours

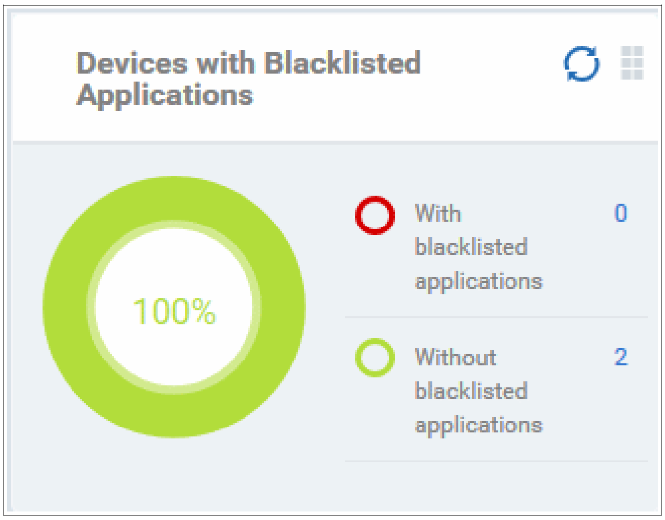
Shows the connectivity status of enrolled devices. Devices which have not contacted ITSM for more than 24 hours are marked as 'inactive'. Placing the mouse cursor over a sector or the legend displays the further details.



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. See '**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. See **Applications** for details about adding and removing apps from blacklist.



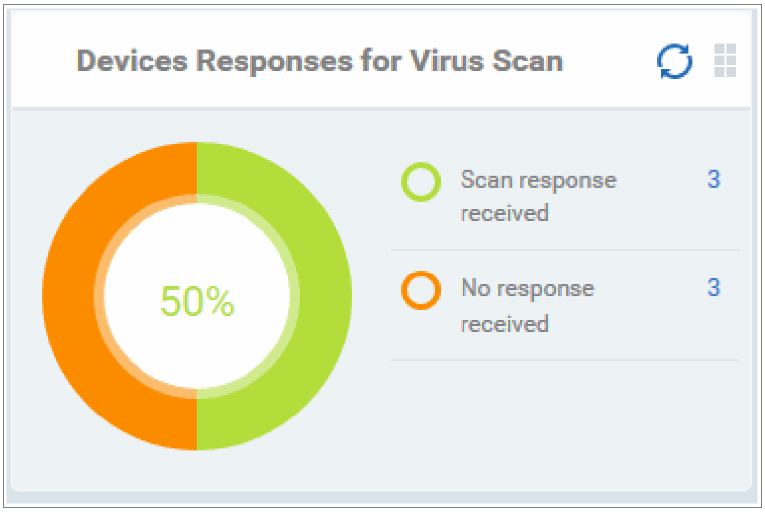
Devices with Blacklisted Applications

100%
With blacklisted applications 0
Without blacklisted applications 2

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. See '**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. See **Antivirus Scans** for details about scanning for viruses on enrolled devices.



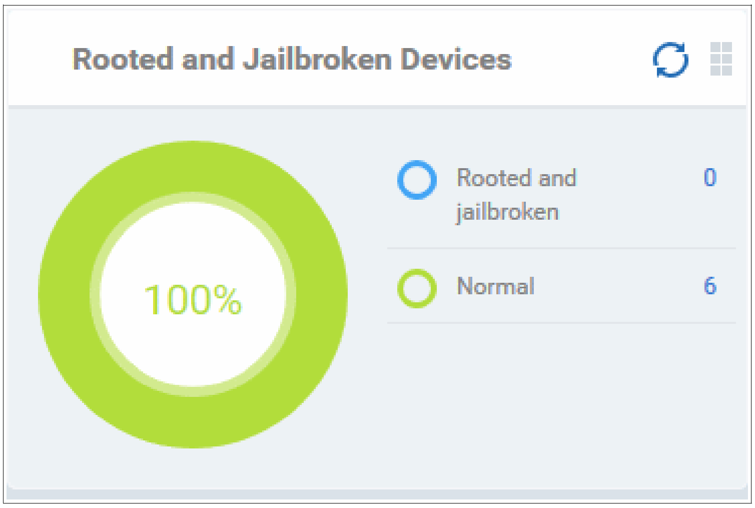
Devices Responses for Virus Scan

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. See **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.



Rooted and Jailbroken Devices

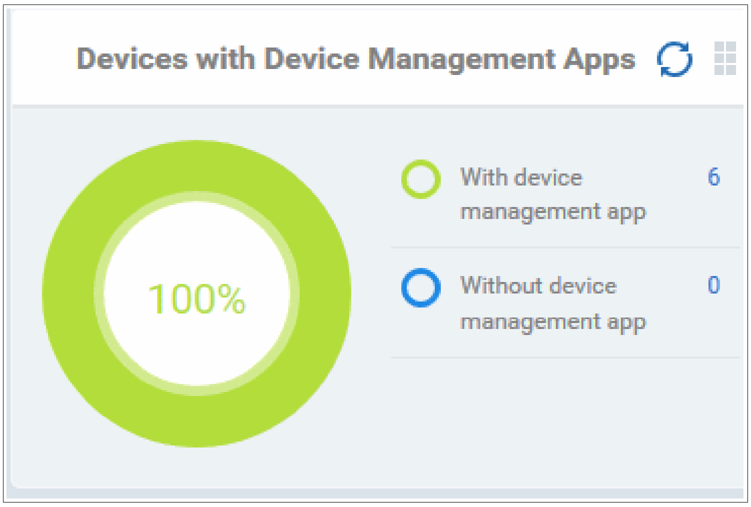
○ Rooted and jailbroken	0
○ Normal	6

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. See '**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.



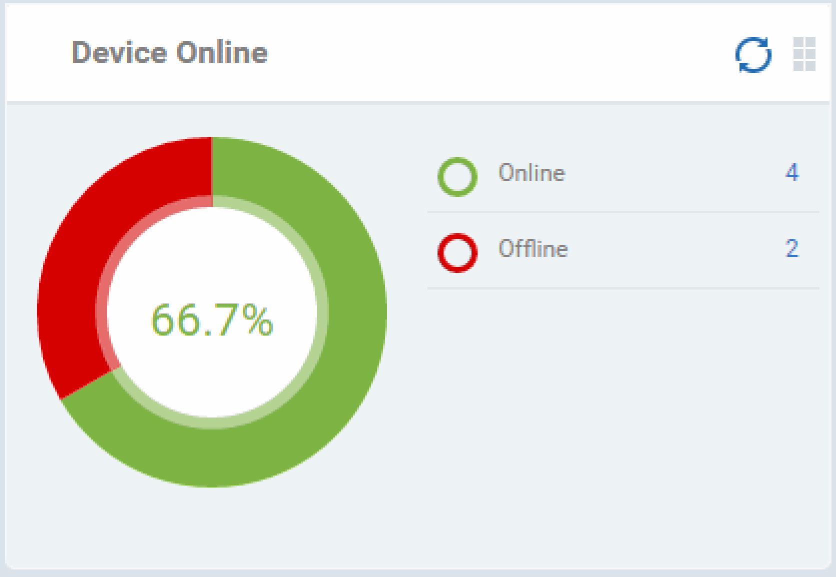
Devices with Device Management Apps

○ With device management app	6
○ Without device management app	0

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. See '**Devices**' for more details.

Device Online

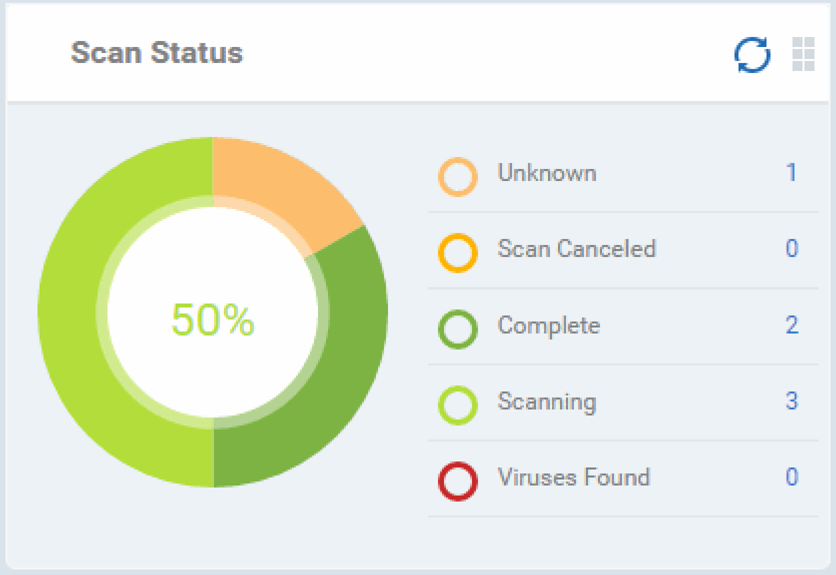
Shows enrolled devices by online/offline status. Devices will shown as offline if they are turned-off, are not communicating with ITSM for other reasons, or if Comodo Client Security is not running. Placing the mouse cursor over a sector or the legend displays the further details.



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. See '**Devices**' for more details.

Scan Status

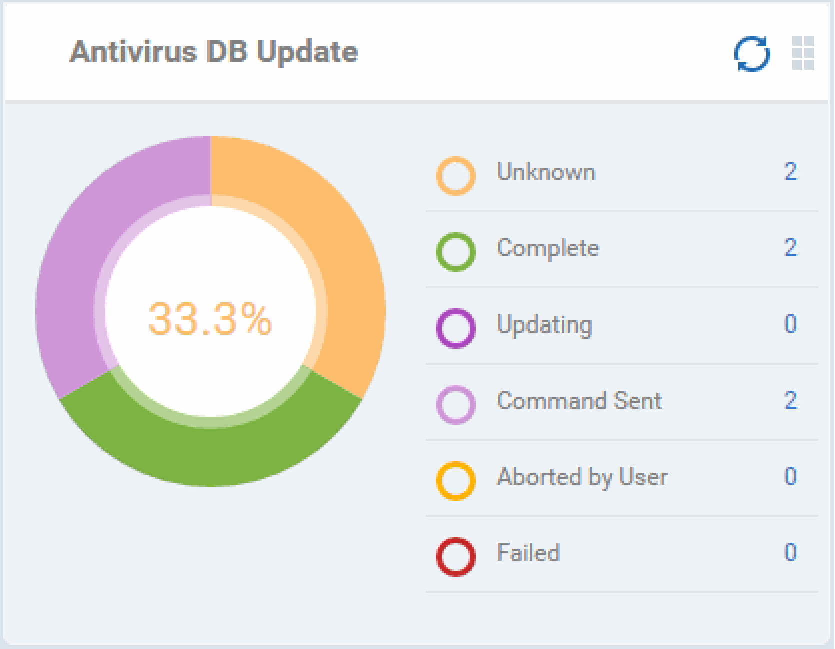
Shows the progress and results of antivirus scans on enrolled devices. Placing the mouse cursor over a sector or the legend displays the further details.



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. See '**Antivirus Scans**' for more details.

Antivirus DB Update

Shows the progress and results of AV database updates on enrolled devices. Place your mouse cursor over a sector to view extra details.



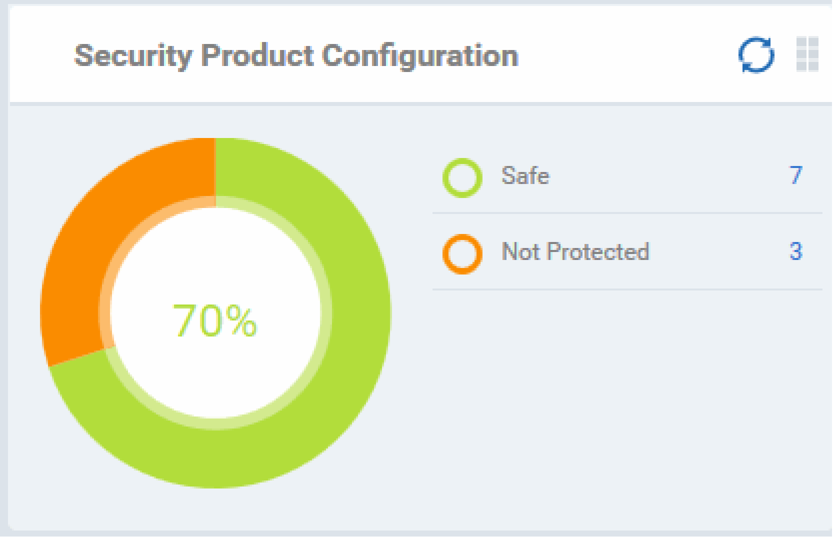
Click any legend item to view all devices in that category. For example, clicking on 'Complete' in the legend will show devices which have the latest virus database. See **Antivirus Scans**' for more details.

Security Product Configuration

Shows 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.

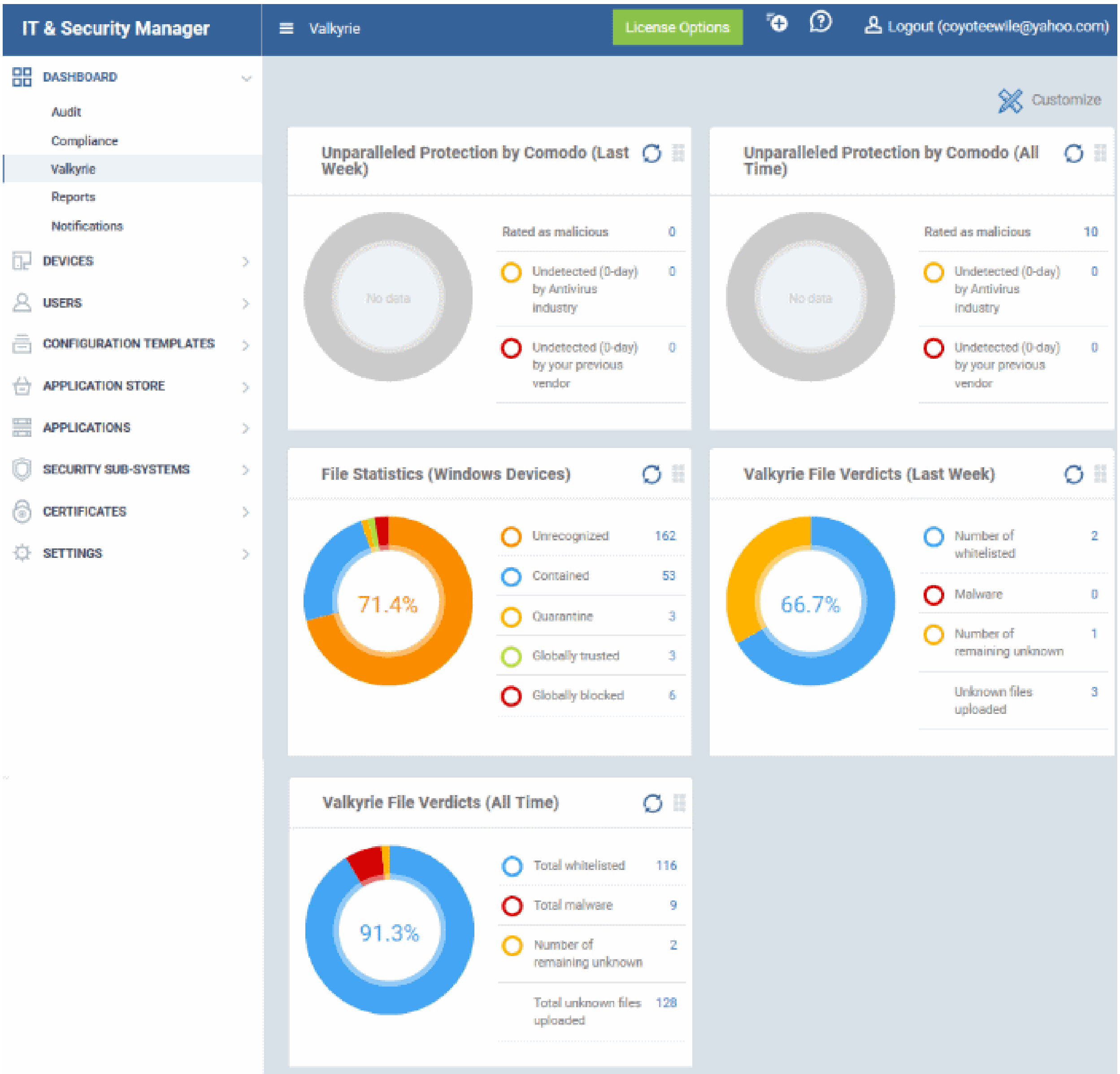


Clicking on any item in the legend will open the respective 'Device List' page. For example, clicking on 'Safe' will open the 'Device List' page displaying the list of devices that have Antivirus installed. See '**Devices**' for more details.

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. To use the service, apply a profile to Comodo Client Security which automatically uploads unknown files to Valkyrie. All results will be displayed in the Valkyrie dashboard. See **Valkyrie Settings** in **Creating Windows Profile** for more details.

Note: The version of Valkyrie that comes with the free version of ITSM is limited to the online testing service. The Premium version also includes manual file testing 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)

Rated as malicious	0
Undetected (0-day) by Antivirus industry	0
Undetected (0-day) by your previous vendor	0

Unparalleled Protection by Comodo (All Time)

Rated as malicious	10
Undetected (0-day) by Antivirus industry	0
Undetected (0-day) by your previous vendor	0

File Statistics (Windows Devices)

Unrecognized	162
Contained	53
Quarantine	3
Globally trusted	3
Globally blocked	6

Valkyrie File Verdicts (Last Week)

Number of whitelisted	2
Malware	0
Number of remaining unknown	1
Unknown files uploaded	3

Valkyrie File Verdicts (All Time)

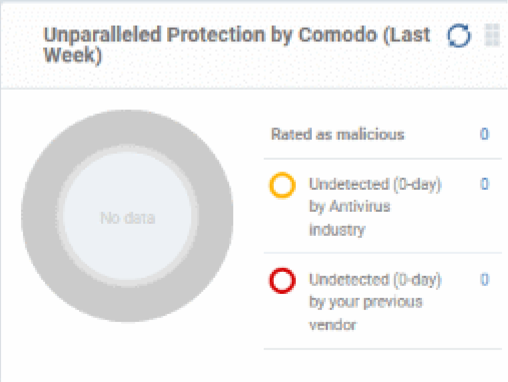
Total whitelisted	116
Total malware	9
Number of remaining unknown	2
Total unknown files uploaded	128

Unparalleled Protection by Comodo (Last Week)

Shows the number of threats identified by Valkyrie over the past week versus the user's previous vendor and the antivirus industry as a whole.

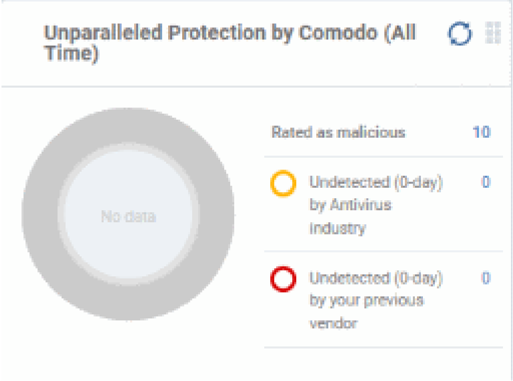
Place the mouse cursor over a sector or the legend to see the percentage of number of files in a particular category.

See **Manage File Trust Ratings on Windows Devices** for more details on Windows File List screen.



Unparalleled Protection by Comodo (Last Week)

Rated as malicious	0
○ Undetected (0-day) by Antivirus industry	0
○ Undetected (0-day) by your previous vendor	0



Unparalleled Protection by Comodo (All Time)

Rated as malicious	10
○ Undetected (0-day) by Antivirus industry	0
○ Undetected (0-day) by your previous vendor	0

Unparalleled Protection By Comodo (All Time)

Shows the number of threats identified by Valkyrie since installation versus the user's previous vendor and the antivirus industry as a whole.

Place the mouse cursor over a sector or the legend to see the percentage of number of files in a particular category.

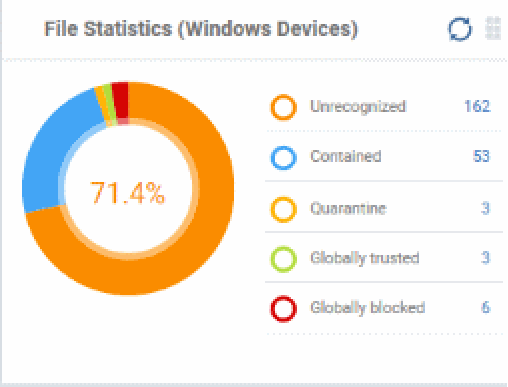
See **Manage File Trust Ratings on Windows Devices** for more details on Windows File List screen.

File Statistics (Windows Devices)

Shows the trust rating and status of files on your network.

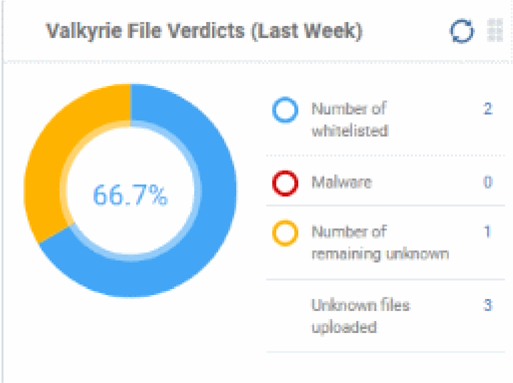
See **Manage File Trust Ratings on Windows Devices**, for more details on Windows File List screen

Click any item in the legend will to 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. See '**Manage File Trust Ratings on Windows Devices**.' for more details.



File Statistics (Windows Devices)

○ Unrecognized	162
○ Contained	53
○ Quarantine	3
○ Globally trusted	3
○ Globally blocked	6



Valkyrie File Verdicts (Last Week)

○ Number of whitelisted	2
○ Malware	0
○ Number of remaining unknown	1
Unknown files uploaded	3

Valkyrie File Verdicts (Last Week)

Displays Valkyrie trust verdicts on unknown files for the previous 7 days. This includes the number of unknown files identified as malicious, those that remain unknown, and those that were white-listed (trusted). The total amount of unknown files analyzed is shown at the bottom.

Place your mouse cursor over a sector or the legend to view the percentage of files in that category.

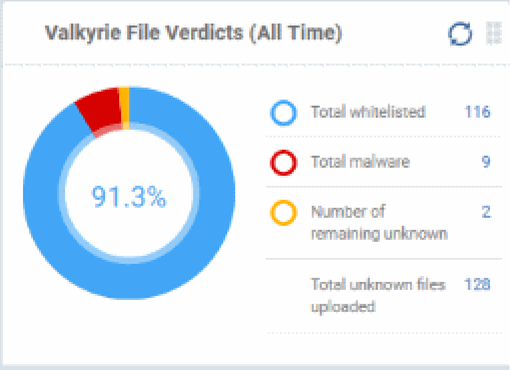
See **Manage File Trust Ratings on Windows Devices**, for more details on Windows File List screen.

Valkyrie File Verdicts (All Time)

Displays Valkyrie trust verdicts on unknown files for the lifetime of your account. This includes the number of unknown files identified as malicious, those that remain unknown, and those that were white-listed (trusted). The total amount of unknown files analyzed is shown at the bottom.

Place your mouse cursor over a sector or the legend to view the percentage of files in that category.

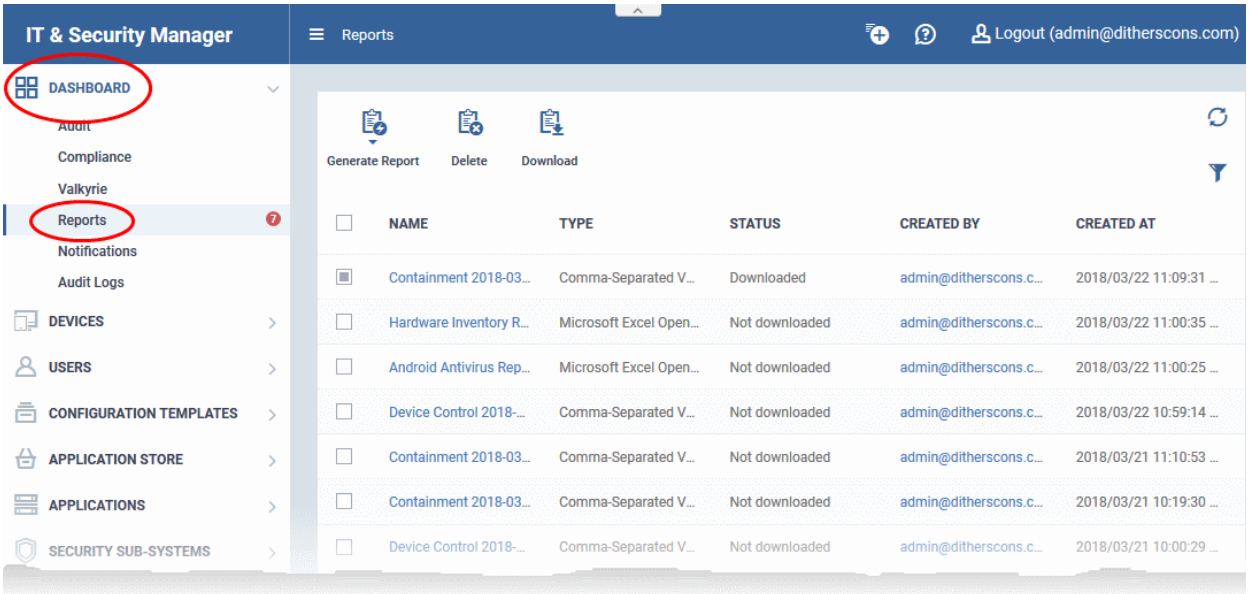
See **Manage File Trust Ratings on Windows Devices**, for more details on Windows File List screen.



Reports

ITSM is capable of generating a wide variety of reports covering system and malware activity across your entire fleet of devices.

- Click 'Dashboard' on the left then select 'Reports' to open the 'Reports' interface.
- The interface allows you to generate and view/download different types of reports.



□	NAME	TYPE	STATUS	CREATED BY	CREATED AT
▣	Containment 2018-03...	Comma-Separated V...	Downloaded	admin@ditherscons.c...	2018/03/22 11:09:31 ...
□	Hardware Inventory R...	Microsoft Excel Open...	Not downloaded	admin@ditherscons.c...	2018/03/22 11:00:35 ...
□	Android Antivirus Rep...	Microsoft Excel Open...	Not downloaded	admin@ditherscons.c...	2018/03/22 11:00:25 ...
□	Device Control 2018-...	Comma-Separated V...	Not downloaded	admin@ditherscons.c...	2018/03/22 10:59:14 ...
□	Containment 2018-03...	Comma-Separated V...	Not downloaded	admin@ditherscons.c...	2018/03/21 11:10:53 ...
□	Containment 2018-03...	Comma-Separated V...	Not downloaded	admin@ditherscons.c...	2018/03/21 10:19:30 ...
□	Device Control 2018-...	Comma-Separated V...	Not downloaded	admin@ditherscons.c...	2018/03/21 10:00:29 ...

Reports - Column Descriptions	
Column Header	**Description**
Name	The subject of the report. • Click the name to view details of the report and to download it. See **the explanation of viewing report details**' for more details.
Type	The file format of the report.
Status	Whether or not the report has been downloaded by any user.
Created By	The name or email address of the admin/staff who generated the report.
Created At	The date and time the report was generate

- Click any column header to sort items in ascending/descending order of items in that column.
- Click the funnel icon at the top right to filter reports and search for reports

Reports can be generated in two ways:

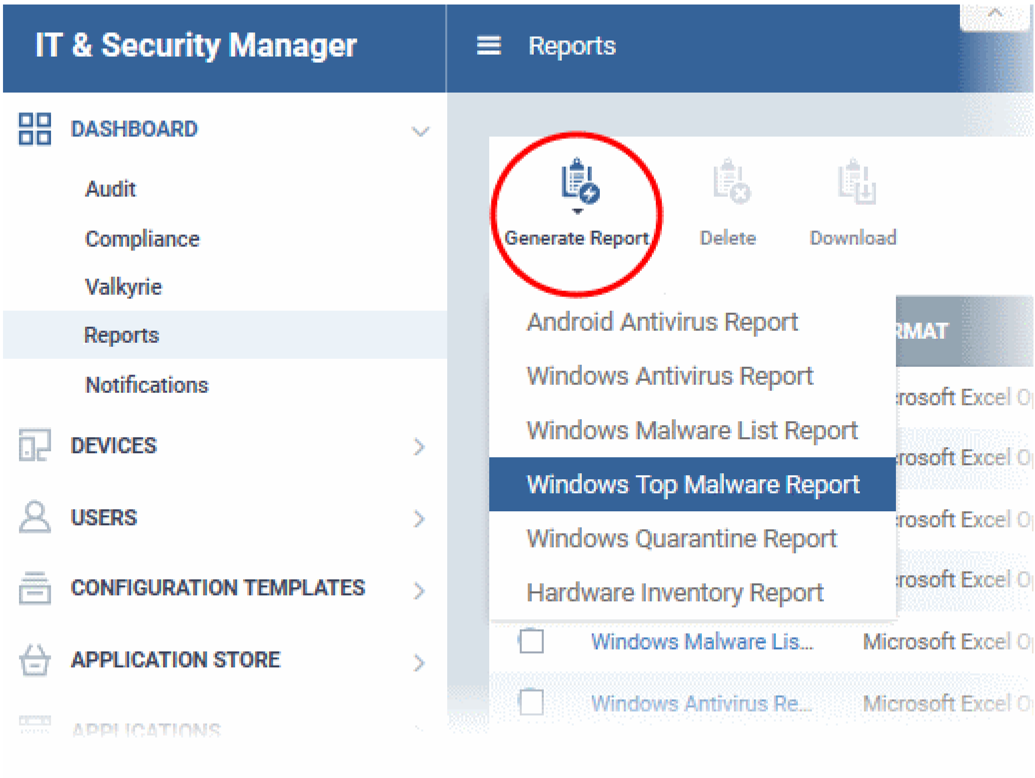
1. From the 'Dashboard' > 'Reports' interface - You can generate following types of reports from the 'Reports' interface
    - Android Antivirus
    - Windows Antivirus
    - Windows Malware List
    - Windows Top Malware
    - Windows Quarantine
    - Hardware Inventory

   These reports are generated in spreadsheet (.xls) file format. See **generating reports** for more details.
2. From the 'Security Subsystems' menu - You can generate the following reports from here:
    - Contained Applications. See **Viewing Contained Applications** for more details
    - File Rating applied to applications identified on managed Windows devices. See **Manage File Trust Ratings on Windows Devices** for more details
    - History of External Device Connection Attempts. See **View History of External Device Connection Attempts** for more details

   These reports are generated in comma separated values (.csv) format.

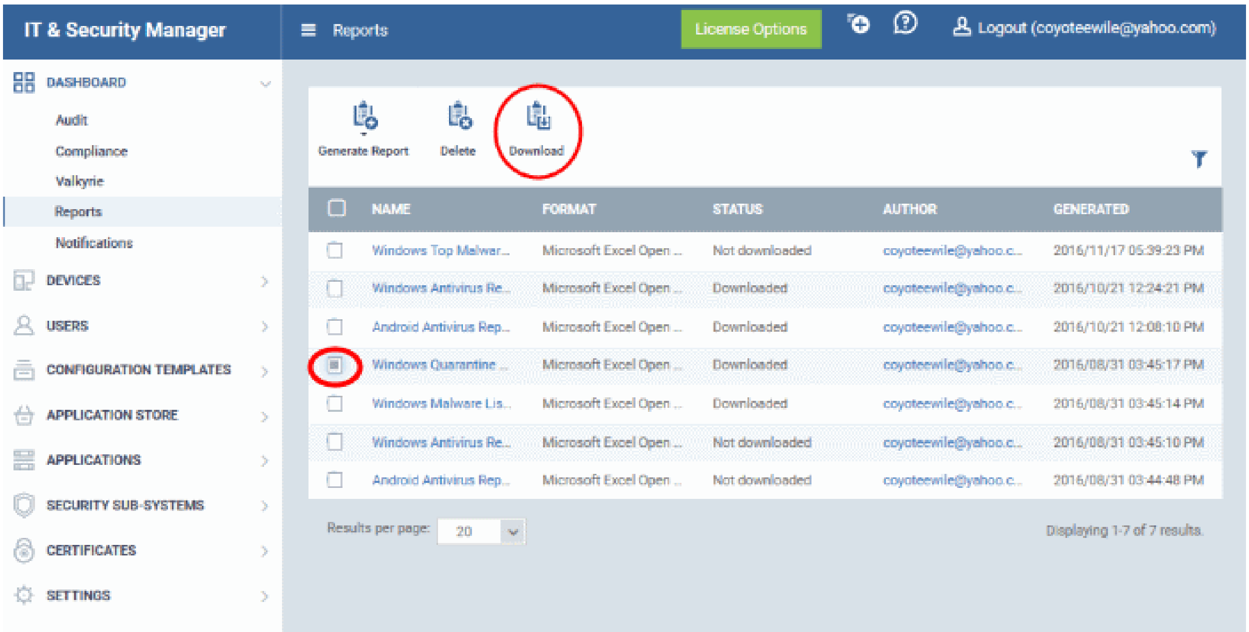
Generate a report from the 'Reports' interface

- 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 a report, select it and click 'Download' at the top

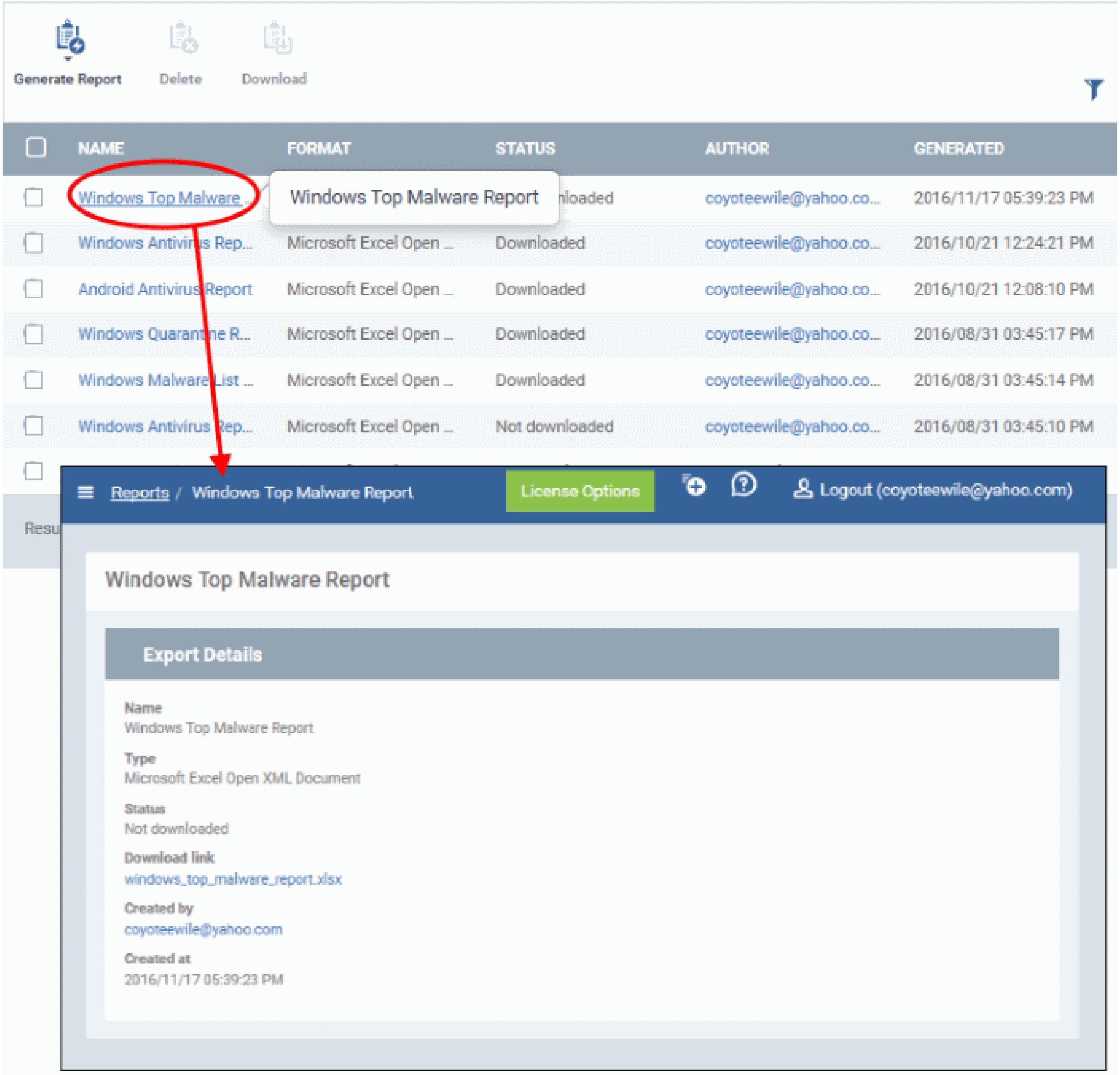


☐	NAME	FORMAT	STATUS	AUTHOR	GENERATED
☐	Windows Top Malwar...	Microsoft Excel Open ...	Not downloaded	coyoteewile@yahoo.c...	2016/11/17 05:39:23 PM
☐	Windows Antivirus Re...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.c...	2016/10/21 12:24:21 PM
☐	Android Antivirus Rep...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.c...	2016/10/21 12:08:10 PM
■	Windows Quarantine ...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.c...	2016/08/31 03:45:17 PM
☐	Windows Malware Lis...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.c...	2016/08/31 03:45:14 PM
☐	Windows Antivirus Re...	Microsoft Excel Open ...	Not downloaded	coyoteewile@yahoo.c...	2016/08/31 03:45:10 PM
☐	Android Antivirus Rep...	Microsoft Excel Open ...	Not downloaded	coyoteewile@yahoo.c...	2016/08/31 03:44:48 PM

Results per page: 20

Displaying 1-7 of 7 results.

- To download the report, select it and click 'Download' at the top. The report will be exported to .xls or .csv format.
- Click a report name to view report details.



□	NAME	FORMAT	STATUS	AUTHOR	GENERATED
□	Windows Top Malware ...	Windows Top Malware Report	...nloaded	coyoteewile@yahoo.co...	2016/11/17 05:39:23 PM
□	Windows Antivirus Rep...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.co...	2016/10/21 12:24:21 PM
□	Android Antivirus Report	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.co...	2016/10/21 12:08:10 PM
□	Windows Quarantine R...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.co...	2016/08/31 03:45:17 PM
□	Windows Malware List ...	Microsoft Excel Open ...	Downloaded	coyoteewile@yahoo.co...	2016/08/31 03:45:14 PM
□	Windows Antivirus Rep...	Microsoft Excel Open ...	Not downloaded	coyoteewile@yahoo.co...	2016/08/31 03:45:10 PM

Reports / Windows Top Malware Report
License Options
Logout (coyoteewile@yahoo.com)
Resu

Windows Top Malware Report

Export Details

Name
Windows Top Malware Report

Type
Microsoft Excel Open XML Document

Status
Not downloaded

Download link
windows_top_malware_report.xlsx

Created by
coyoteewile@yahoo.com

Created at
2016/11/17 05:39:23 PM

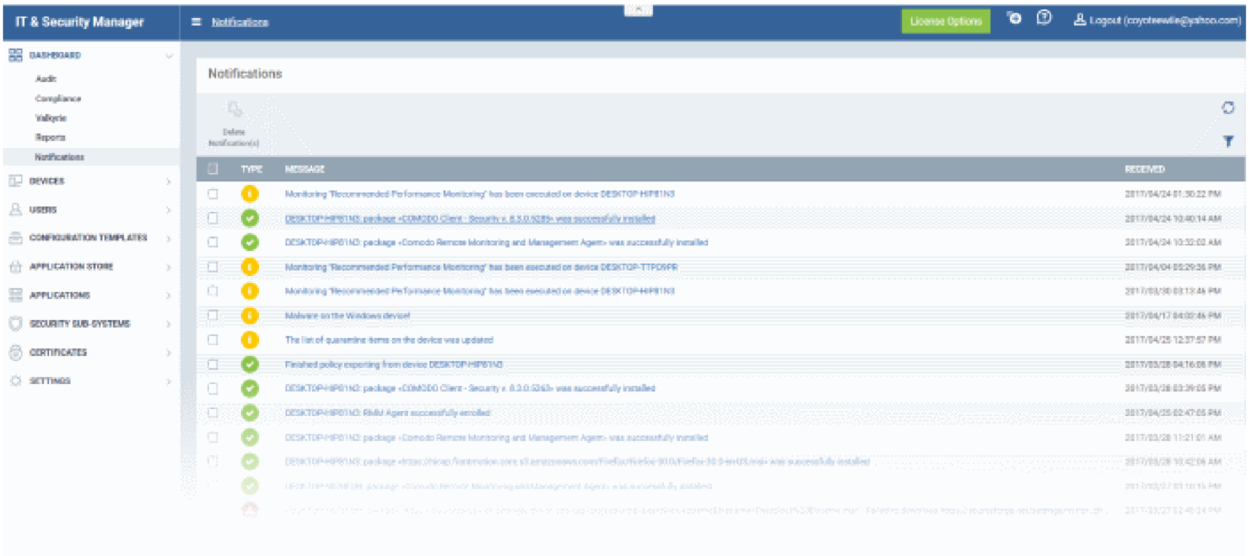
- To remove a report from the list,select it and click 'Delete'.

Notifications

Whenever there is a new notification in the C1 title bar, the notification symbol is incremented. Clicking the notification icon will take you to the respective C1 interface.

Tip: ITSM can send notifications as emails. Click 'Settings' > 'Email Notifications' to configure them. See **Configuring Email Notifications** if you need help with this.

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

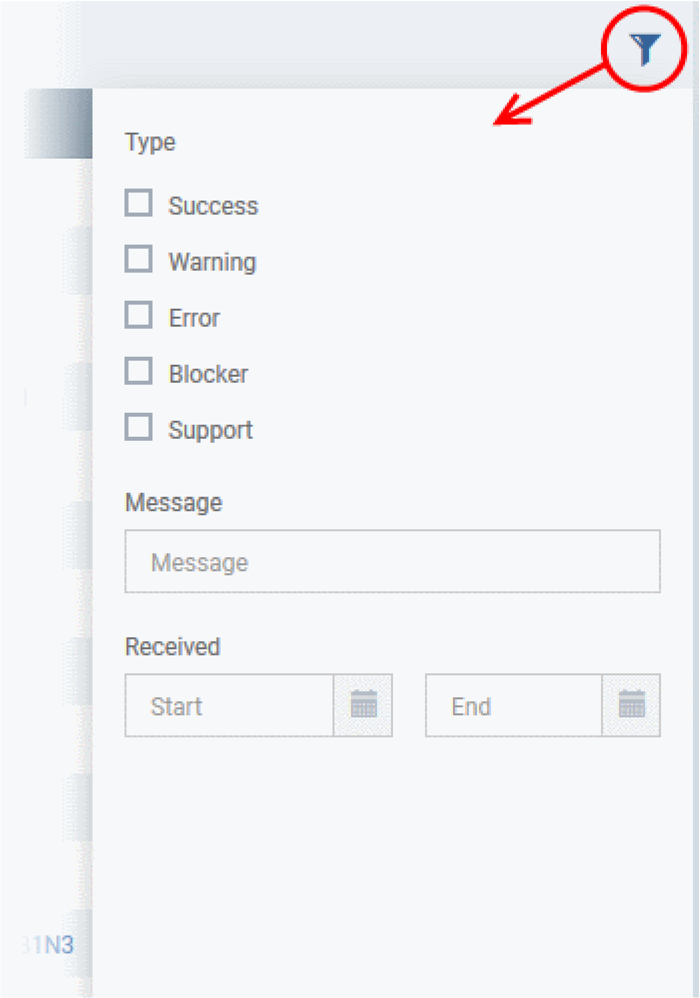


Notifications

	TYPE	MESSAGE	RECEIVED
□	!	Monitoring 'Recommended Performance Monitoring' has been executed on device DESKTOP-HIP81N3	2017/04/24 01:30:22 PM
□	✓	DESKTOP-HIP81N3: package «COMODO Client - Security v. 8.3.0.5285» was successfully installed	2017/04/24 10:40:14 AM
□	✓	DESKTOP-HIP81N3: package «Comodo Remote Monitoring and Management Agent» was successfully installed	2017/04/24 10:32:02 AM
□	!	Monitoring 'Recommended Performance Monitoring' has been executed on device DESKTOP-TTPD9PR	2017/04/04 05:29:36 PM
□	!	Monitoring 'Recommended Performance Monitoring' has been executed on device DESKTOP-HIP81N3	2017/03/30 03:13:46 PM
□	!	Malware on the Windows device!	2017/04/17 04:02:46 PM
□	!	The list of quarantine items on the device was updated	2017/04/25 12:37:57 PM
□	✓	Finished policy exporting from device DESKTOP-HIP81N3	2017/03/28 04:16:08 PM
□	✓	DESKTOP-HIP81N3: package «COMODO Client - Security v. 8.3.0.5263» was successfully installed	2017/03/28 03:39:05 PM
□	✓	DESKTOP-HIP81N3: RMM Agent successfully enrolled	2017/04/25 02:47:05 PM
□	✓	DESKTOP-HIP81N3: package «Comodo Remote Monitoring and Management Agent» was successfully installed	2017/03/28 11:21:01 AM
□	✓	DESKTOP-HIP81N3: package «https://hicap.frontmotion.com.s3.amazonaws.com/Firefox/Firefox-30.0/Firefox-30.0-en-US.msi» was successfully installed	2017/03/28 10:42:08 AM
	✓	[illegible] package «Comodo Remote Monitoring and Management Agent» was successfully installed	2017/03/27 [illegible] PM
		[illegible]	2017/03/27 [illegible] PM

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.



Type

□ Success

□ Warning

□ Error

□ Blocker

□ Support

Message

Message

Received

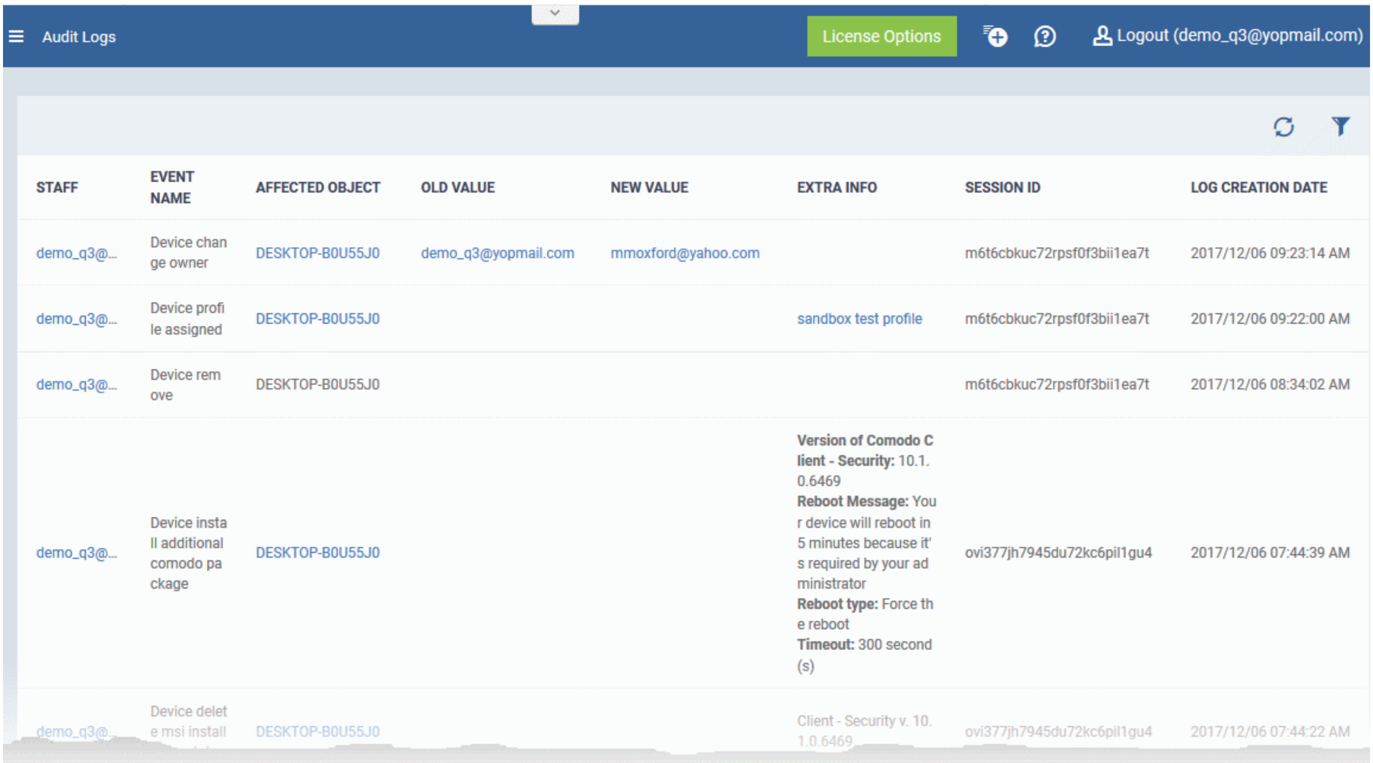
Start

End

- To remove notification(s), select them in the list and click 'Delete Notifications' above the table.

Audit Logs

- ITSM keeps a log of actions implemented on managed devices by administrators and staff members. These logs can be useful when troubleshooting issues.
- Logged actions include device enrollment, applying a security profile, package installations, remote take-overs sessions, restarting a device, removing a device and more.
- The 'Audit Logs' interface shows all log entries with details such as the name of the staff member who applied the action, the affected device, the action taken and more.
- Click 'Dashboard' > 'Audit Logs' on the left-menu to open the log interface:



STAFF	EVENT NAME	AFFECTED OBJECT	OLD VALUE	NEW VALUE	EXTRA INFO	SESSION ID	LOG CREATION DATE
demo_q3@...	Device change owner	DESKTOP-B0U55J0	demo_q3@yopmail.com	mmoxford@yahoo.com		m6t6cbkuc72rpsf0f3bii1ea7t	2017/12/06 09:23:14 AM
demo_q3@...	Device profile assigned	DESKTOP-B0U55J0			sandbox test profile	m6t6cbkuc72rpsf0f3bii1ea7t	2017/12/06 09:22:00 AM
demo_q3@...	Device remove	DESKTOP-B0U55J0				m6t6cbkuc72rpsf0f3bii1ea7t	2017/12/06 08:34:02 AM
demo_q3@...	Device install additional comodo package	DESKTOP-B0U55J0			**Version of Comodo Client - Security:** 10.1.0.6469 **Reboot Message:** Your device will reboot in 5 minutes because it's required by your administrator **Reboot type:** Force the reboot **Timeout:** 300 second(s)	ovi377jh7945du72kc6pil1gu4	2017/12/06 07:44:39 AM
demo_q3@...	Device delete msi install	DESKTOP-B0U55J0			Client - Security v. 10.1.0.6469	ovi377jh7945du72kc6pil1gu4	2017/12/06 07:44:22 AM

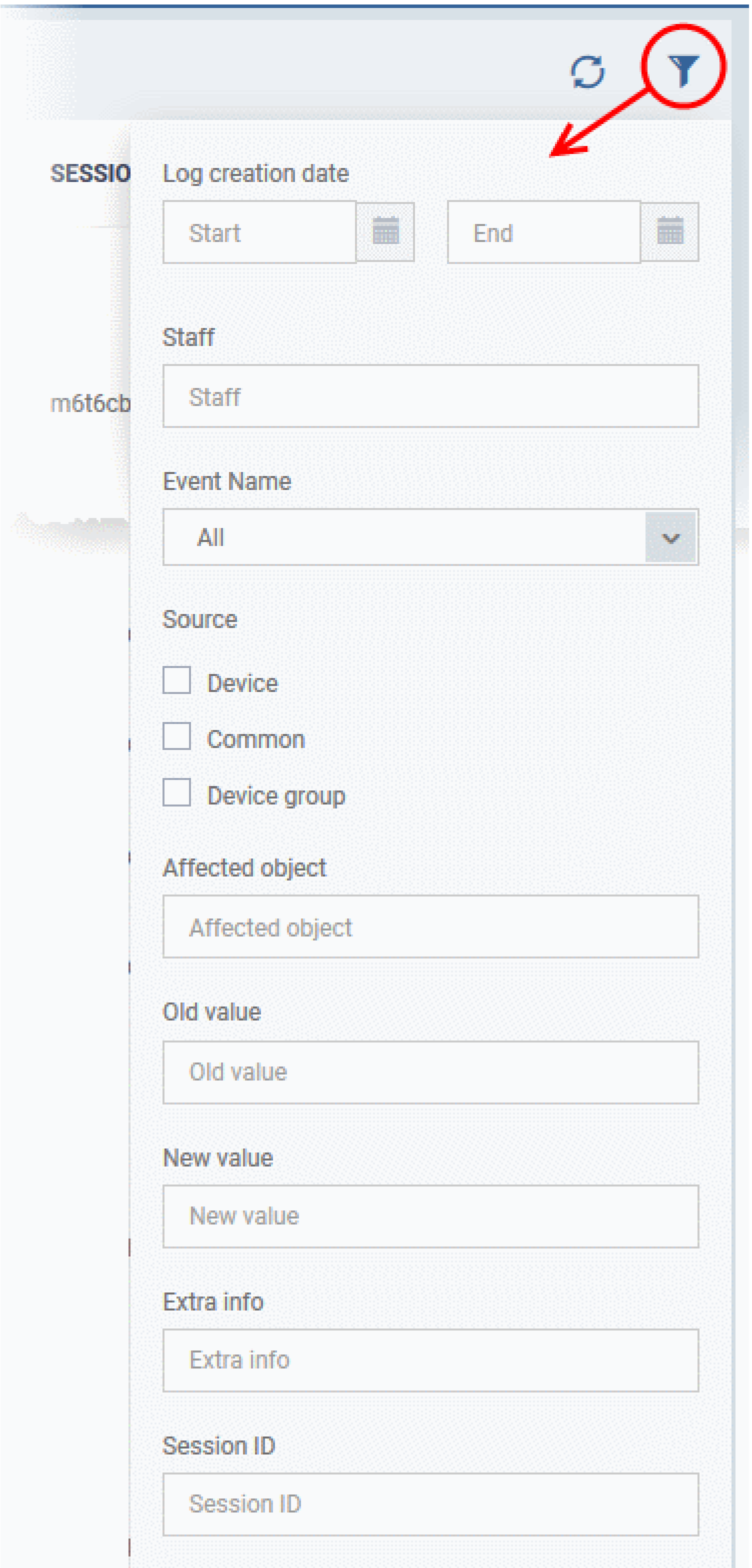
Audit Logs - Column Descriptions	
Column Heading	**Description**
Staff	Username of the admin or staff member who executed the action. • Click the staff name to view their details. See **Viewi the details of the User** if you need help with the details interface.
Event Name	The action executed on the device. Examples include enrollment of devices, remote installation of Comodo and third party MSI packages, remote take-overs and device removals.
Affected Object	The device, device group, profile or procedure on which the action was executed. • Click the name to view more details about the item • The details interface allows you to view and manage the respective item.
Old Value	The previous setting or value before the action was implemented. For example, if a Comodo package is remotely updated, the old version number of the package will be shown here.
New Value	The new setting or value after the action was implemented. For example, if a Comodo package is remotely updated, the version number of the new package will be shown here.
Extra Info	Additional details about the action. Additional details include devices on which the procedure was run, package installation parameters, profiles applied/removed and so on. • Script or patch procedures - Click the 'Selected Devices' link to view devices on which the procedure was run.

	• Click a device name in the list to view its 'Device Details' interface
Session ID	String used to identify the connection session between the device and the ITSM server during the action.
Log Creation Date	Date and time of the event.

- Click the 'Refresh' icon to load the latest events.

Search and filtering option

- Click any of the column header (except 'Event Name') to sort the items in alphabetical order of items in that column
- To filter or search for a specific event, click the funnel icon at the top right.



SESSIO

m6t6cb

Log creation date

Start

End

Staff

Staff

Event Name

All

Source

□ Device

□ Common

□ Device group

Affected object

Affected object

Old value

Old value

New value

New value

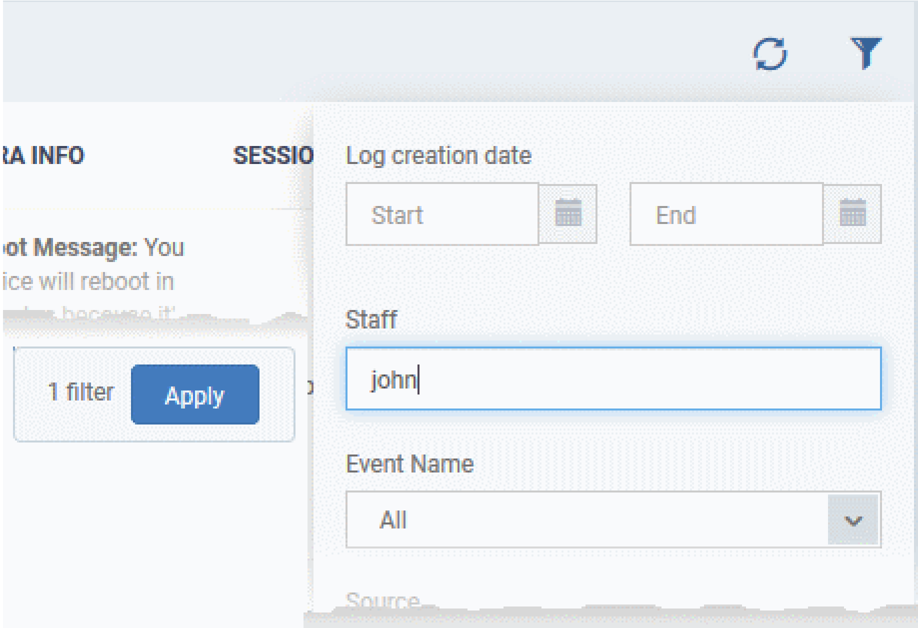
Extra info

Extra info

Session ID

Session ID

- To filter the items or search for a specific event based on log creation period, staff, event type, device affected, values changed, and session ID, enter the search criteria in part or full and click 'Apply'



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.

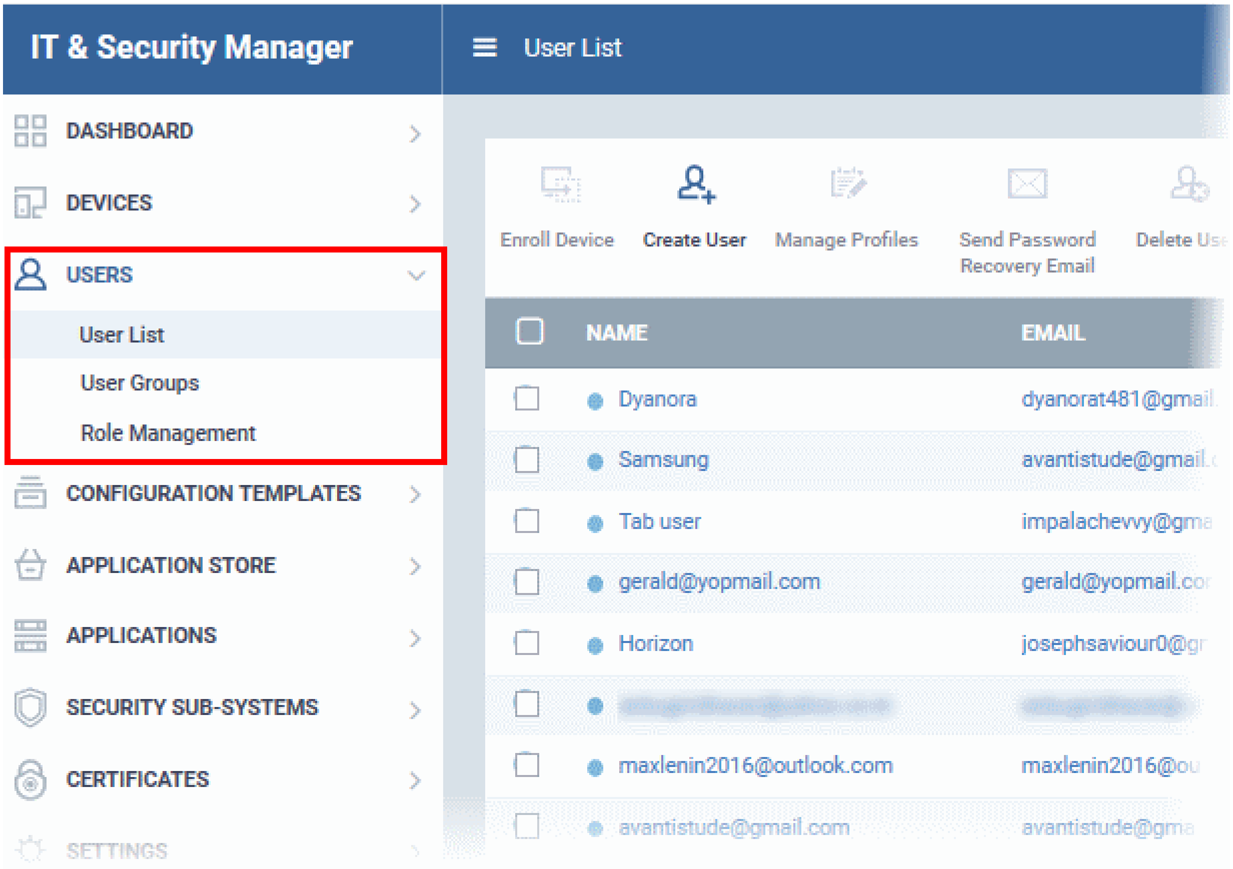
Users can access the ITSM interface according to the privileges assigned to them. Privilege levels are assigned by applying a 'role' to a user.

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:



□	NAME	EMAIL
□	Dyanora	dyanorat481@gmail.
□	Samsung	avantistude@gmail.c
□	Tab user	impalachevvy@gma
□	gerald@yopmail.com	gerald@yopmail.co
□	Horizon	josephsaviour0@gr
□	[redacted]	[redacted]
□	maxlenin2016@outlook.com	maxlenin2016@ou
□	avantistude@gmail.com	avantistude@gma

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

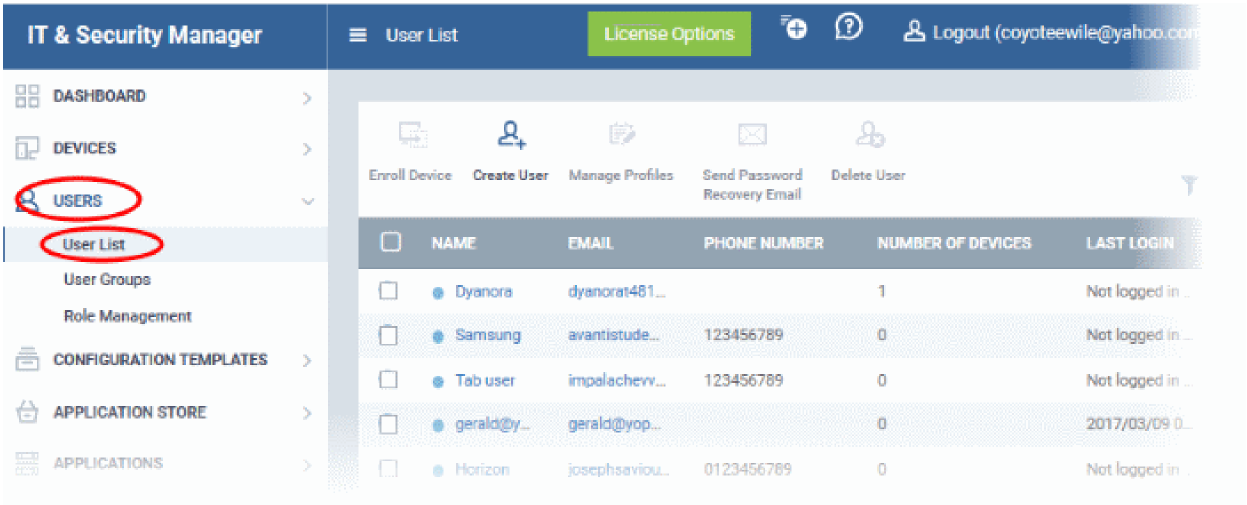
4.1. Manage Users

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'

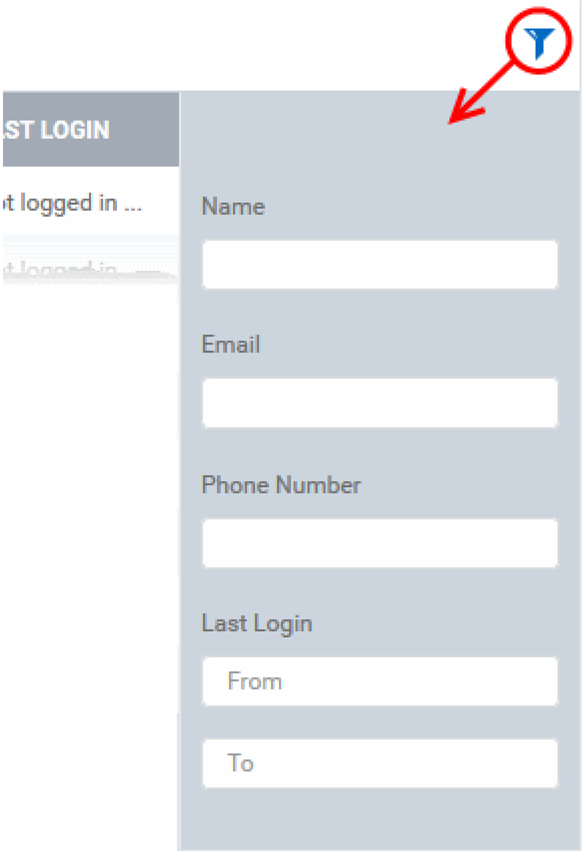


	NAME	EMAIL	PHONE NUMBER	NUMBER OF DEVICES	LAST LOGIN
□	Dyanora	dyanorat481...		1	Not logged in ...
□	Samsung	avantistude...	123456789	0	Not logged in ...
□	Tab user	impalachevv...	123456789	0	Not logged in ...
□	gerald@y...	gerald@yop...		0	2017/03/09 0...
□	Horizon	josephsaviou...	0123456789	0	Not logged in ...

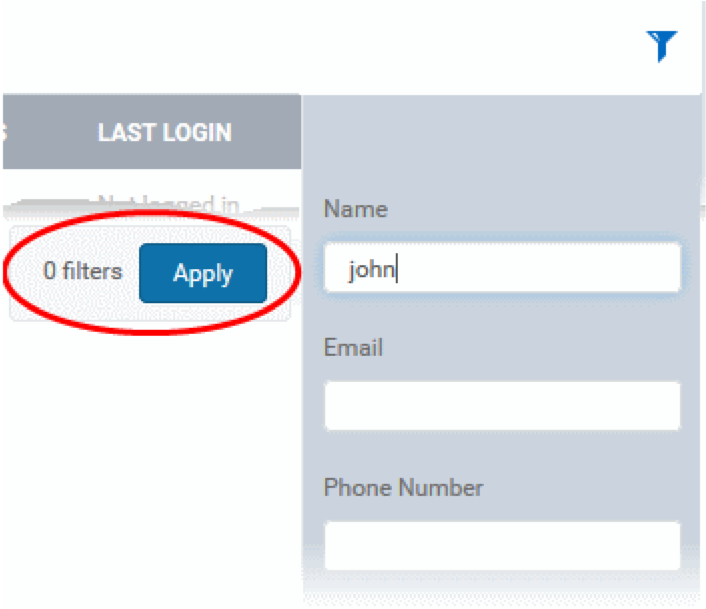
User List Table - Column Descriptions	
Column Heading	**Description**
Name	The login username of the user. Clicking the username will open the user details screen where you can edit user details. See '**Viewing the Details of a User**' for more details.
Email	The registered email address of the user. 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. Create 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.

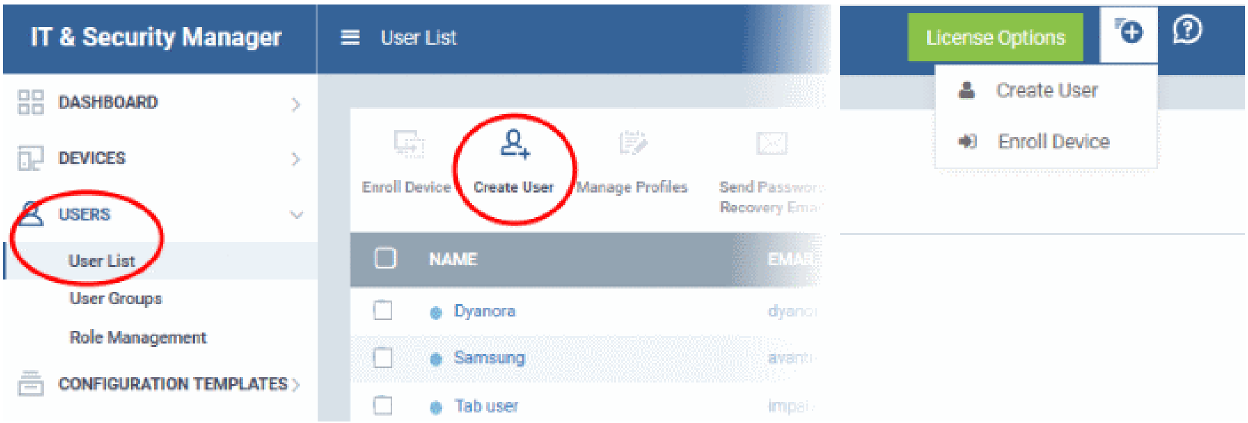
> **Important Note**: User device(s) can only be enrolled after the user has been added to the system.
>
> Each user license covers up to five mobile devices or one Windows/Mac OS endpoint for a single user (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single 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

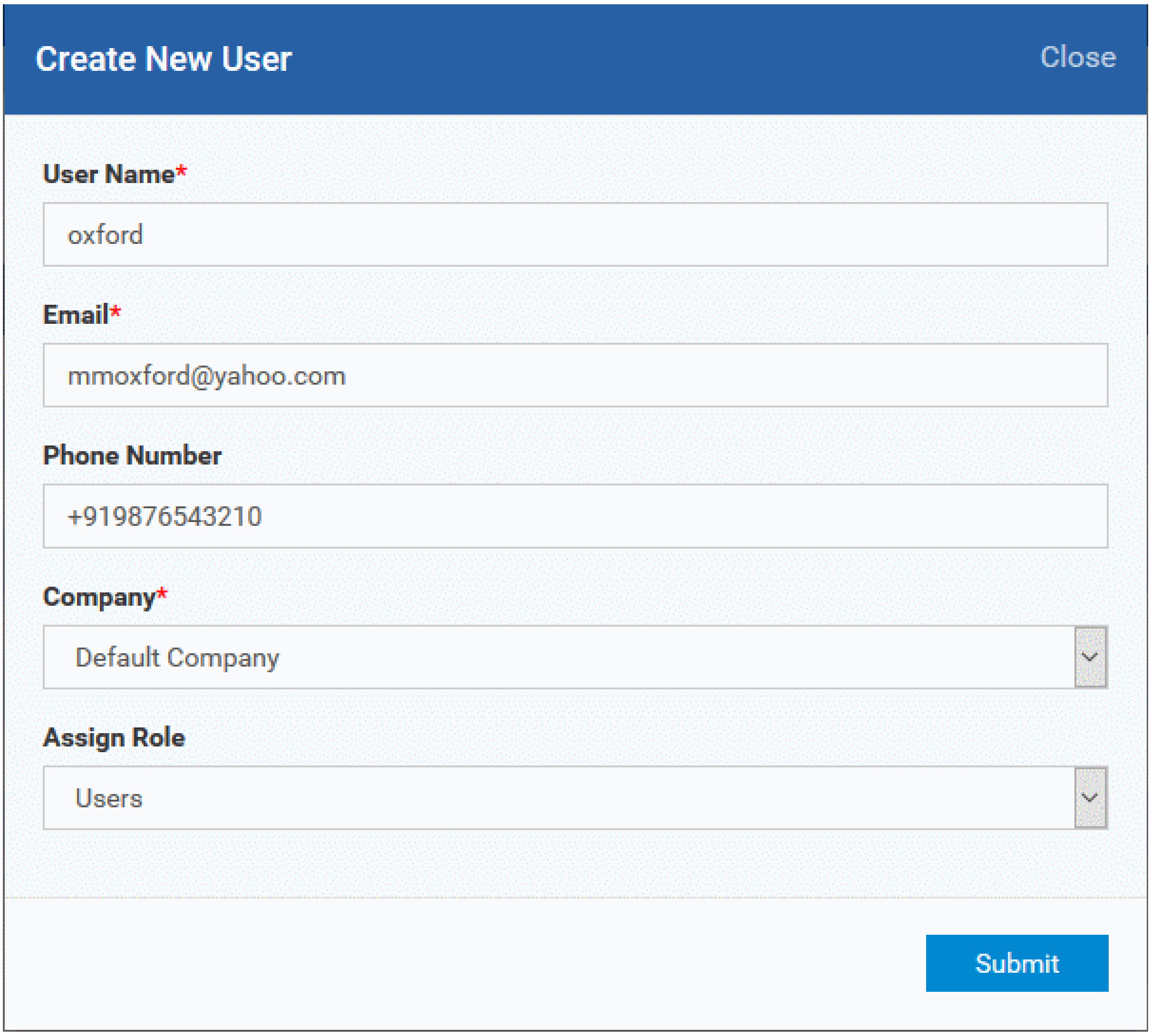
- Click 'Users' > 'User List' from the left then click the 'Create User' button

  or

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



The 'Create New User' form will open:


Create New User

Close

User Name*

oxford

Email*

mmoxford@yahoo.com

Phone Number

+919876543210

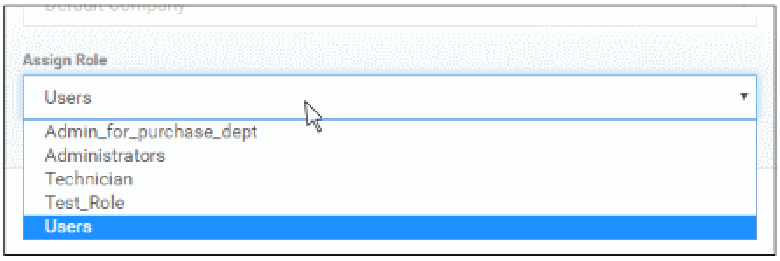
Company*

Default Company

Assign Role

Users

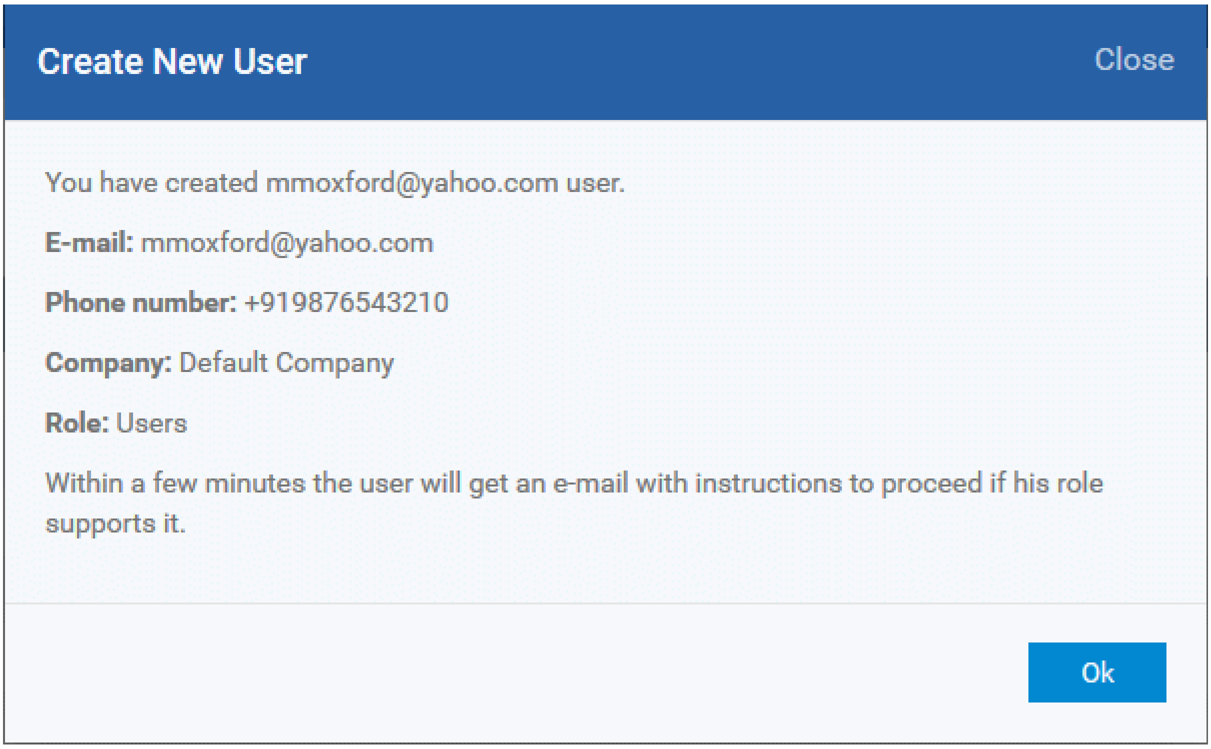
Submit

'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.  Assign Role: Users Admin_for_purchase_dept Administrators Technician Test_Role Users 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,



Create New User

You have created mmoxford@yahoo.com user.

E-mail: mmoxford@yahoo.com

Phone number: +919876543210

Company: Default Company

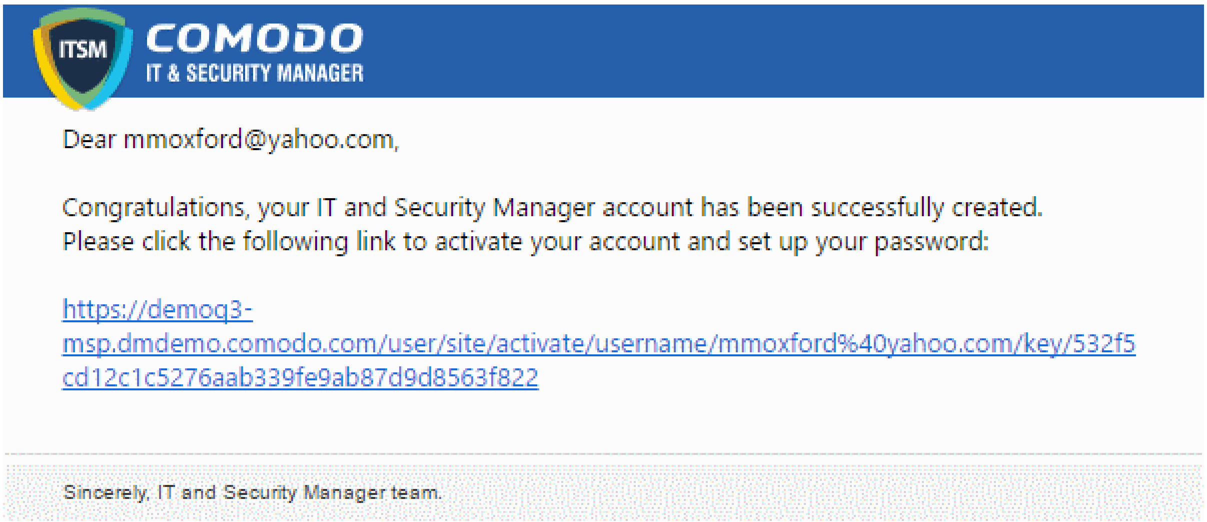
Role: Users

Within a few minutes the user will get an e-mail with instructions to proceed if his role supports it.

- 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:



Dear mmoxford@yahoo.com,

Congratulations, your IT and Security Manager account has been successfully created.
Please click the following link to activate your account and set up your password:

https://demoq3-msp.dmdemo.comodo.com/user/site/activate/username/mmoxford%40yahoo.com/key/532f5cd12c1c5276aab339fe9ab87d9d8563f822

Sincerely, IT and Security Manager team.

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. Enroll 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/Linux 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.

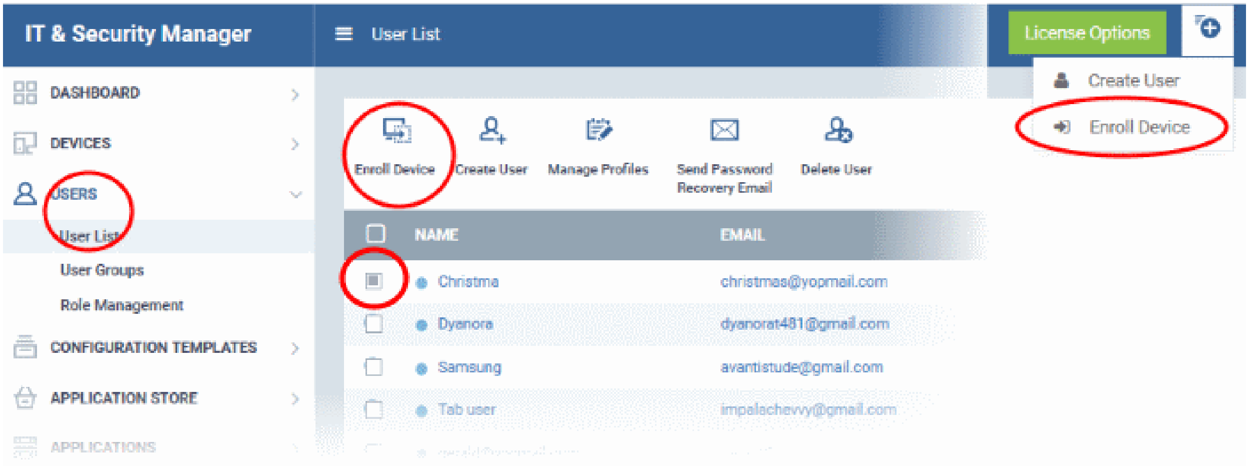
Refer to the section **Viewing and Managing Licenses** for more details.

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

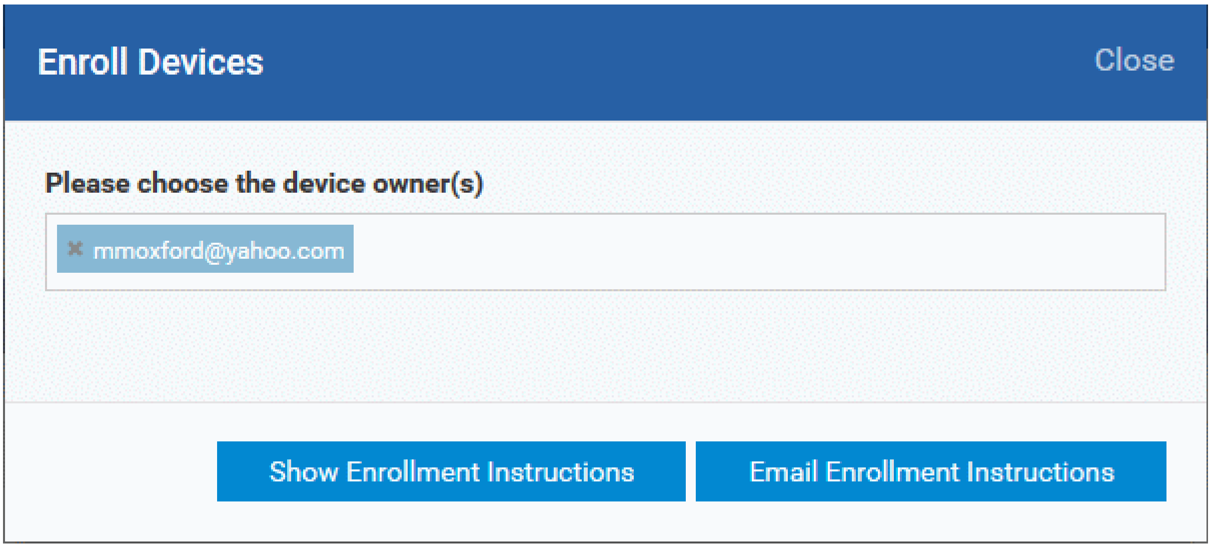
  Or

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



	NAME	EMAIL
☒	Christma	christmas@yopmail.com
□	Dyanora	dyanorat481@gmail.com
□	Samsung	avantistude@gmail.com
□	Tab user	impalachevvy@gmail.com

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



Enroll Devices

Close

Please choose the device owner(s)

✖ mmoxford@yahoo.com

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

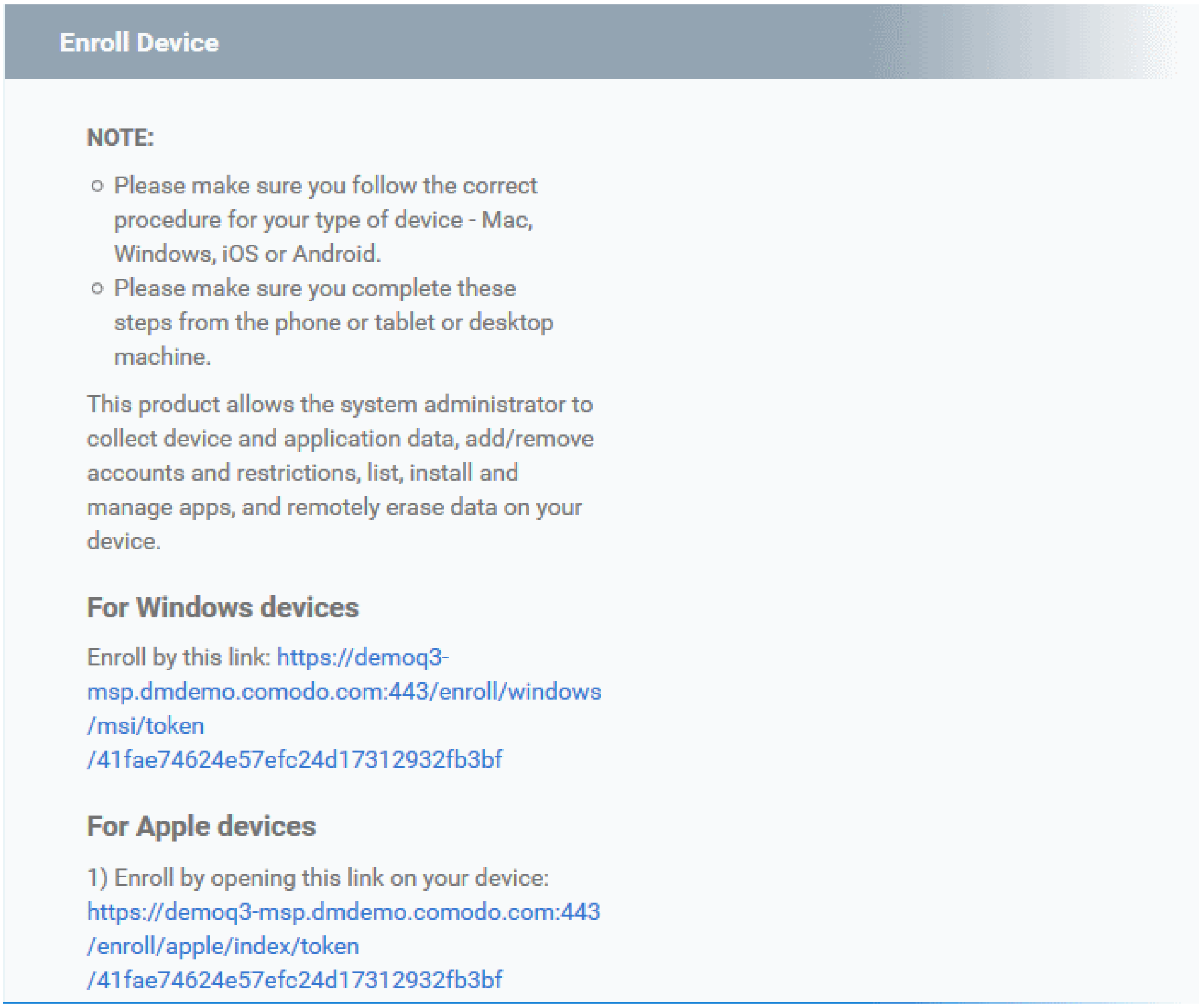
- Opening the 'User Info' screen of a user by clicking on the username and selecting 'Enroll Device' at the top
- Opening the 'Device List' interface by clicking 'Devices' > 'Device List' from the left and selecting 'Enroll Device'

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.



Enroll Device

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

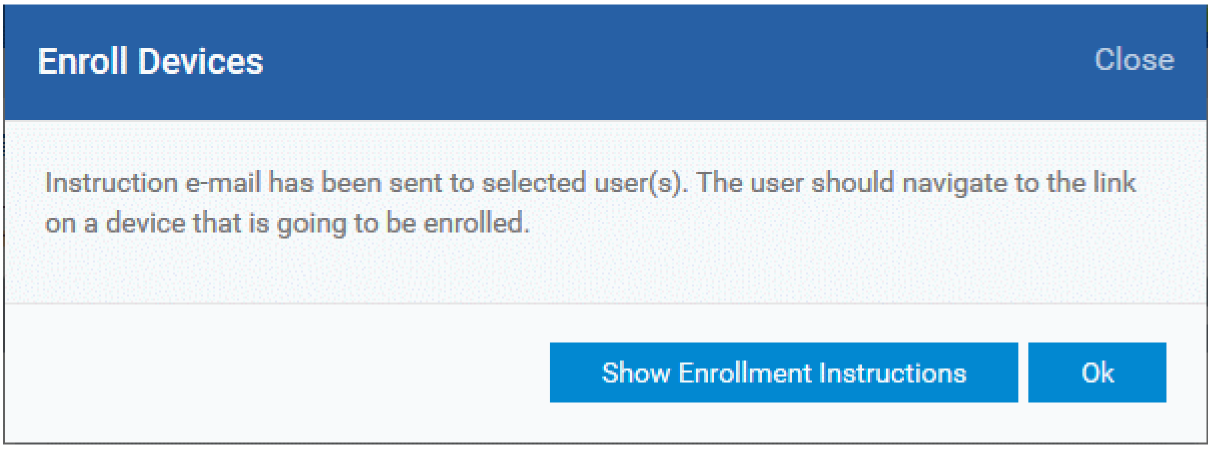
Enroll by this link: https://demoq3-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/41fae74624e57efc24d17312932fb3bf

For Apple devices

1) Enroll by opening this link on your device: https://demoq3-msp.dmdemo.comodo.com:443/enroll/apple/index/token/41fae74624e57efc24d17312932fb3bf

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

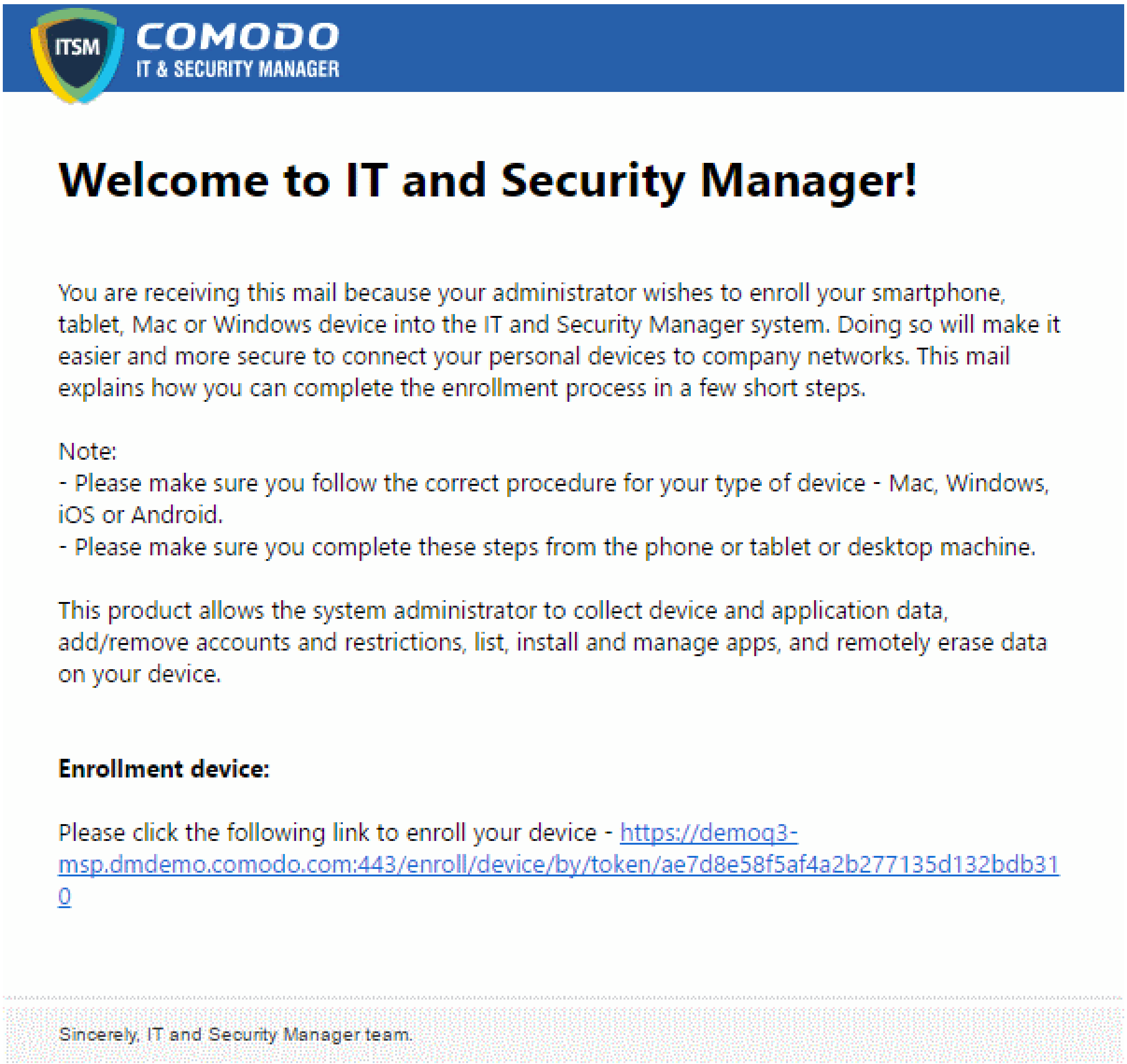
A confirmation dialog will be displayed.



Enroll Devices

Instruction e-mail has been sent to selected user(s). The user should navigate to the link on a device that is going to be enrolled.

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.



Welcome to IT and Security Manager!

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

Note:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

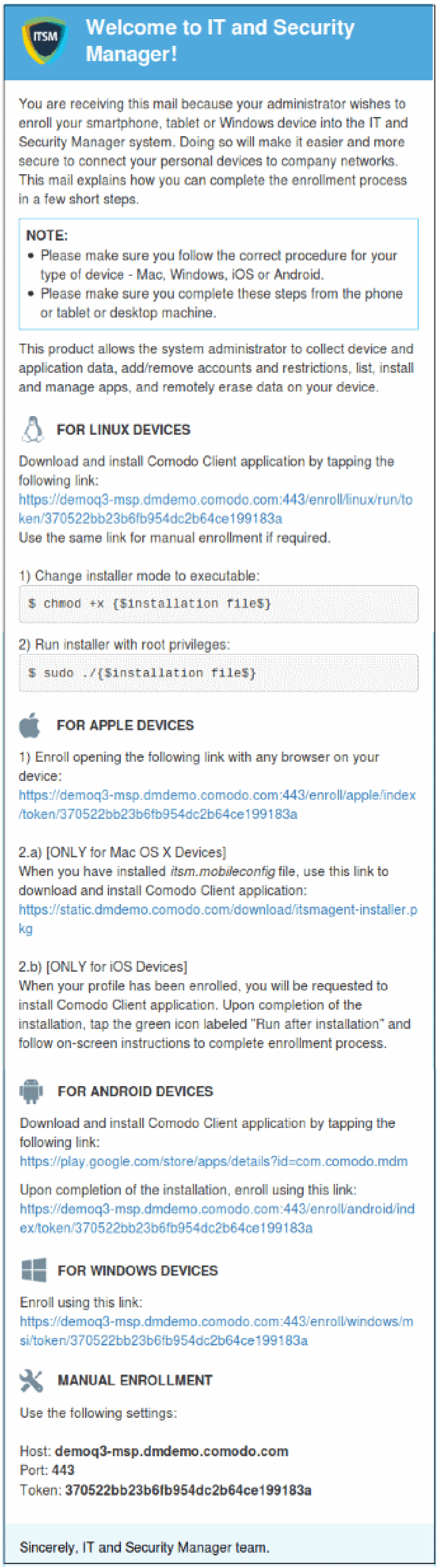
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Enrollment device:

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

Sincerely, IT and Security Manager team.

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



Welcome to IT and Security Manager!

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

NOTE:

- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

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

FOR LINUX DEVICES

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

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

FOR APPLE DEVICES

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

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

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

FOR ANDROID DEVICES

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

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

FOR WINDOWS DEVICES

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

MANUAL ENROLLMENT

Use the following settings:

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

Sincerely, IT and Security Manager team.

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:

- **Enroll Android Devices**
- **Enroll iOS Devices**
- **Enroll Windows Endpoints**
- **Enroll Mac OS Endpoints**
- **Enroll Linux OS Endpoints**

4.1.2.1. Enroll Android Devices

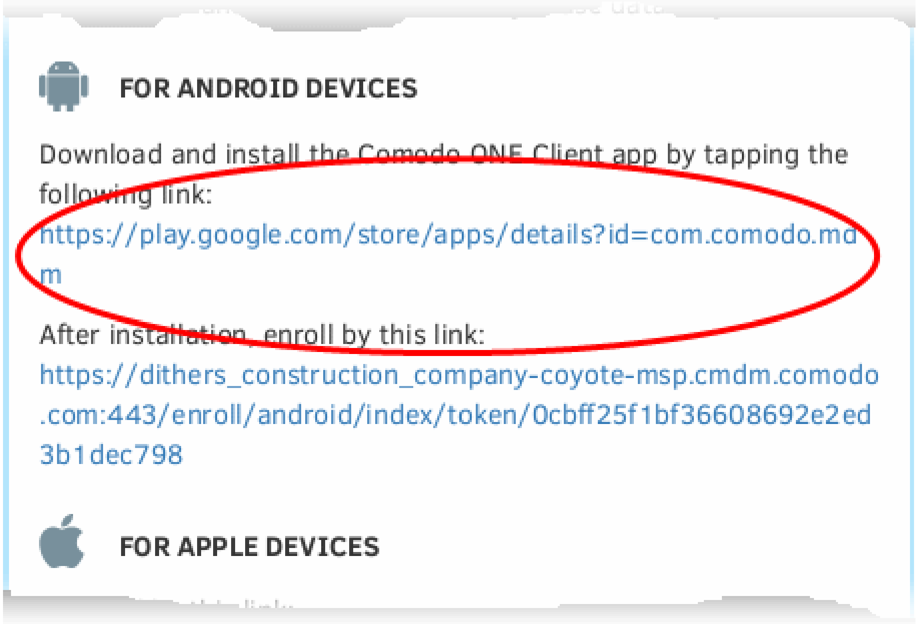
After adding a user's devices, the user will receive an email containing enrollment instructions and links to download the android ITSM agent. Users should open the mail on the device you want to enroll and follow the setup instructions.

Android device enrollment involves two steps:

- **Step 1 - Download and Install the agent**
- **Step 2 - Configure the agent**

Step 1 - Download and Install the agent

- Open the mail on the device itself then tap the Android enrollment link to open the device setup page
- On the setup page, click the install link for Android devices:



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://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/android/index/token/0cbff25f1bf36608692e2ed3b1dec798

FOR APPLE DEVICES

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

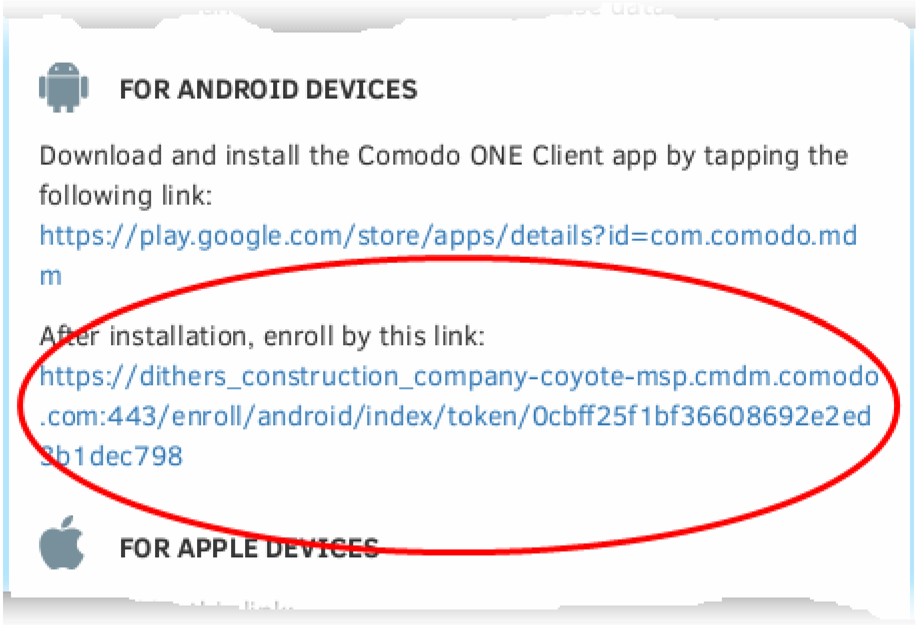
Step 2 - Configure the agent

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

- **Automatic Configuration**
- **Manual Configuration**

Automatic Configuration

- After installation in step 1, go back to the setup page and tap the enrollment link as shown below:



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

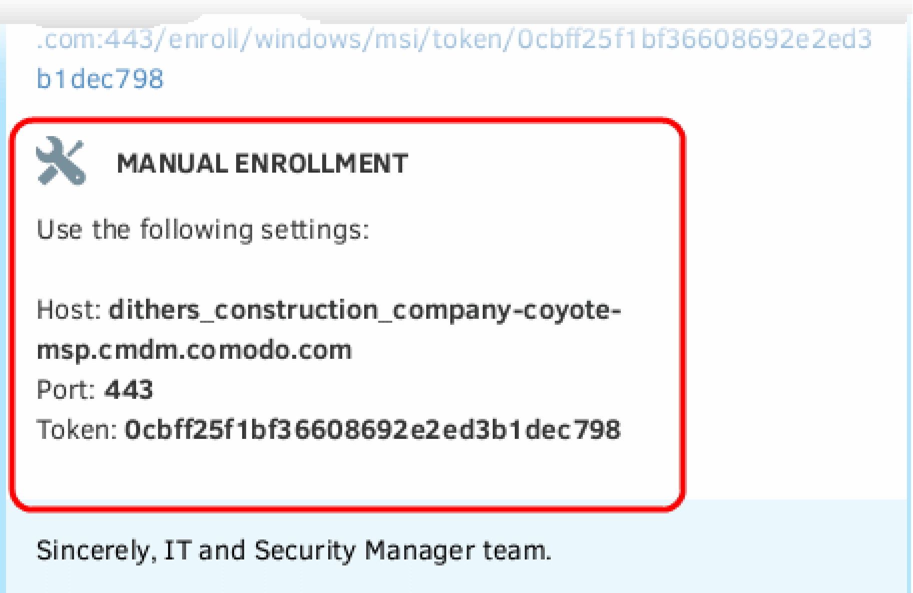
After installation, enroll by this link:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/android/index/token/0cbff25f1bf36608692e2ed3b1dec798

FOR APPLE DEVICES

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

Manual Configuration

Users can manually configure the agent to connect to ITSM by entering the server settings and the token ID. You can find these items on the setup page:



.com:443/enroll/windows/msi/token/0cbff25f1bf36608692e2ed3b1dec798

MANUAL ENROLLMENT

Use the following settings:

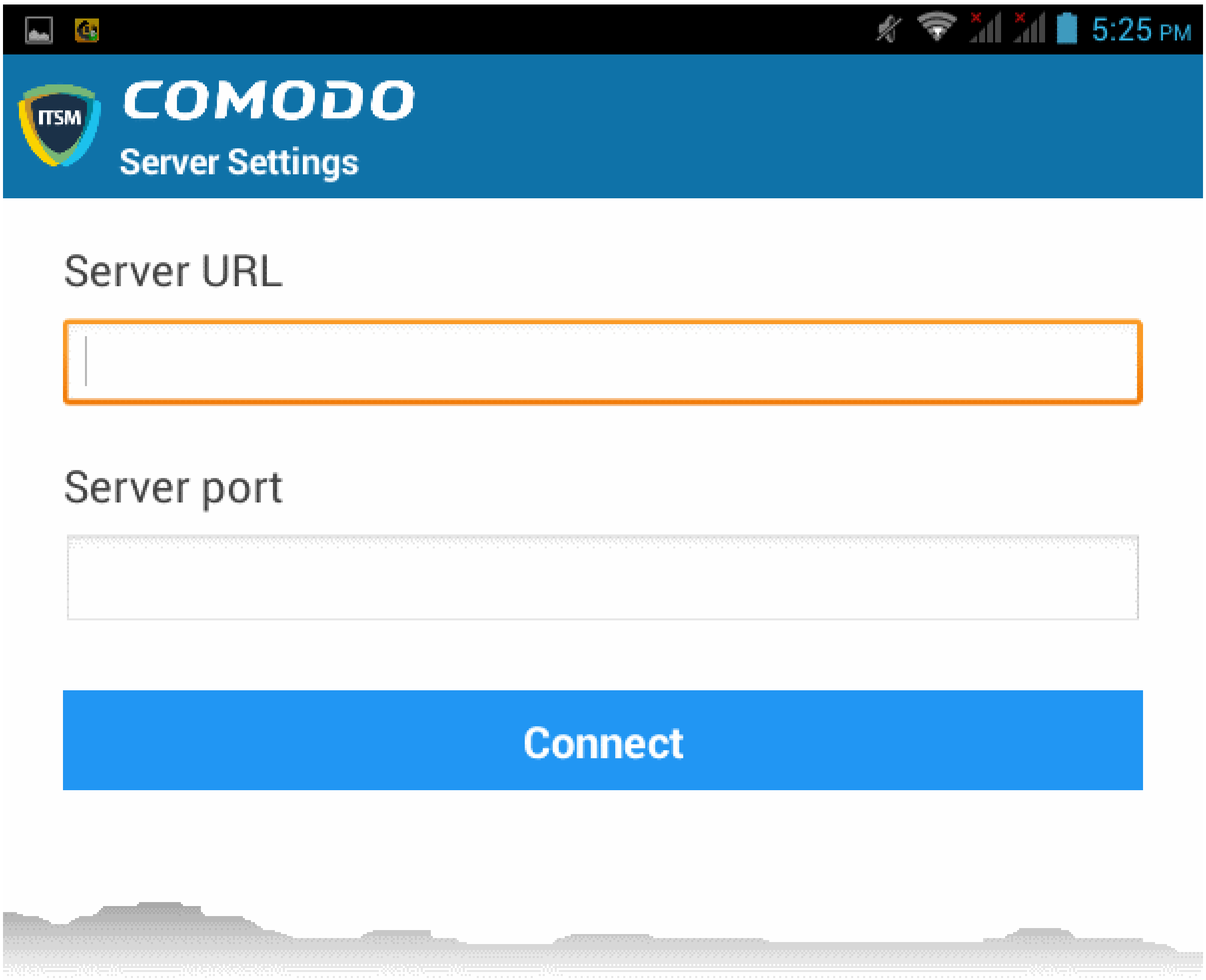
Host: **dithers_construction_company-coyote-msp.cmdm.comodo.com**
Port: **443**
Token: **0cbff25f1bf36608692e2ed3b1dec798**

Sincerely, IT and Security Manager team.

To manually configure the agent

- Open the agent by tapping the agent icon on your device. This will start the agent configuration wizard where you can enroll the device by entering the server settings and unique token.

Server Settings



Server URL

Server port

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

Login to the Console

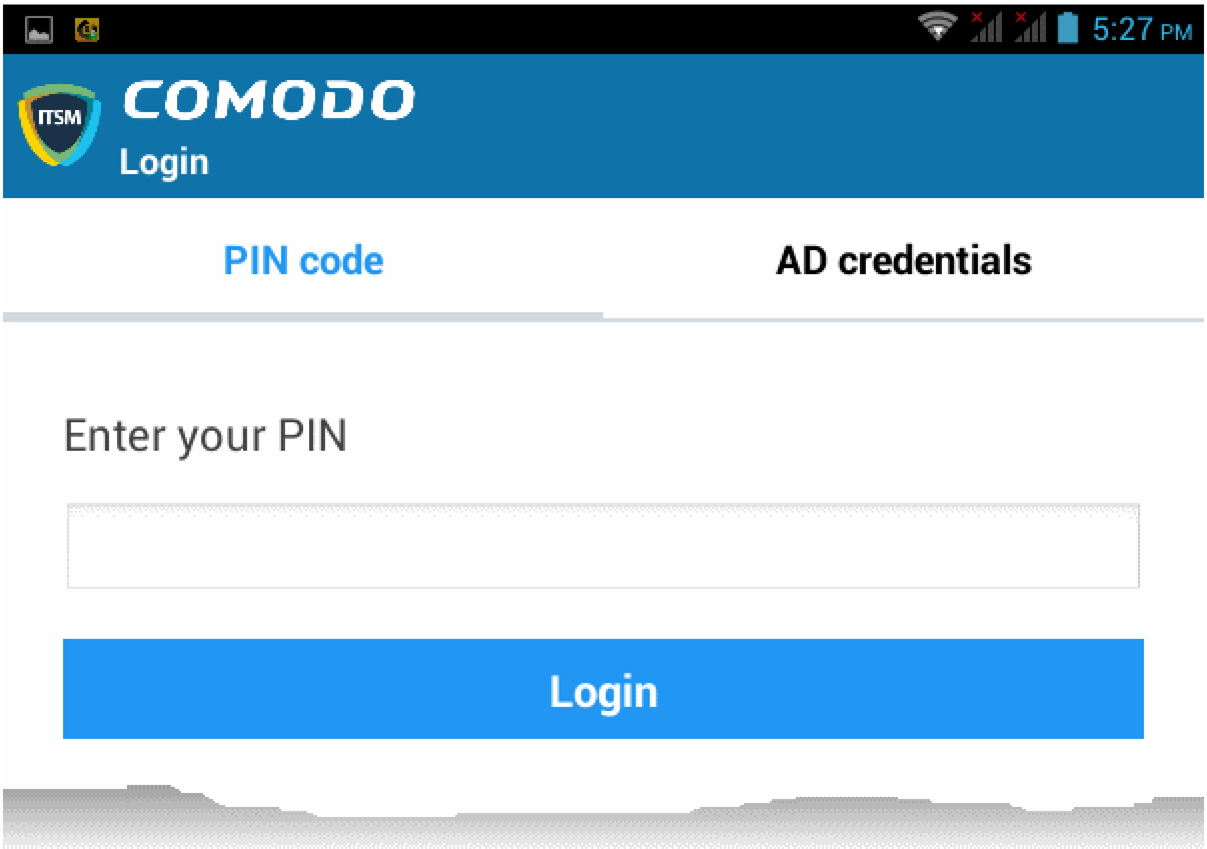
You can login to the ITSM console via the Android app in two ways:

- **Enter the personal identification number (PIN) contained in the email**

  OR
- **Enter your username and password**

Enter your PIN

- Open the ITSM Android app
- Open the '**Pin Code**' tab on the login screen:



- Enter the PIN (aka 'Token' code) from the enrollment email
- Tap 'Login'. The **End User License Agreement** screen will appear.

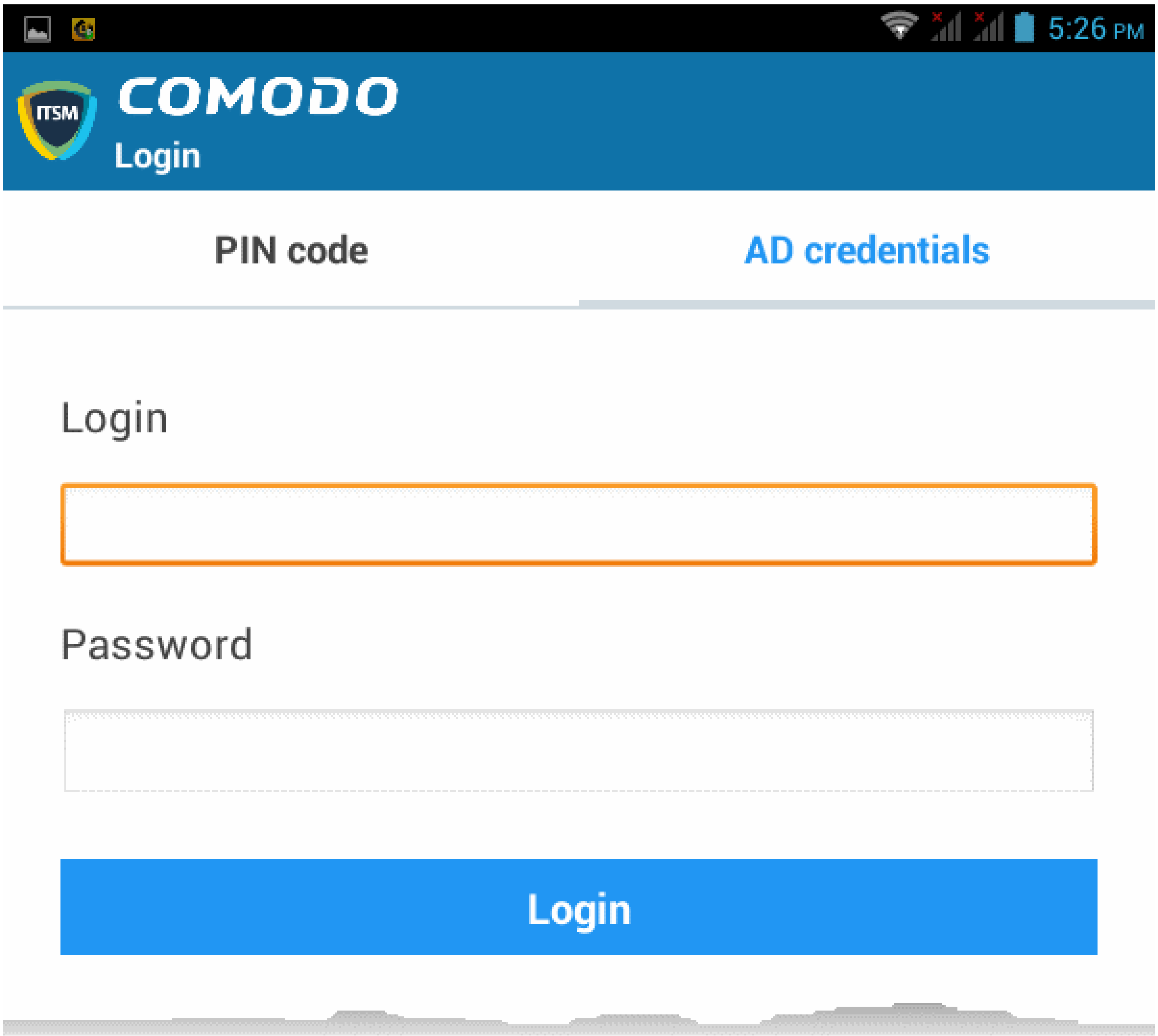
Enter your username and password

- Tap the '**AD Credentials**' tab on 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.

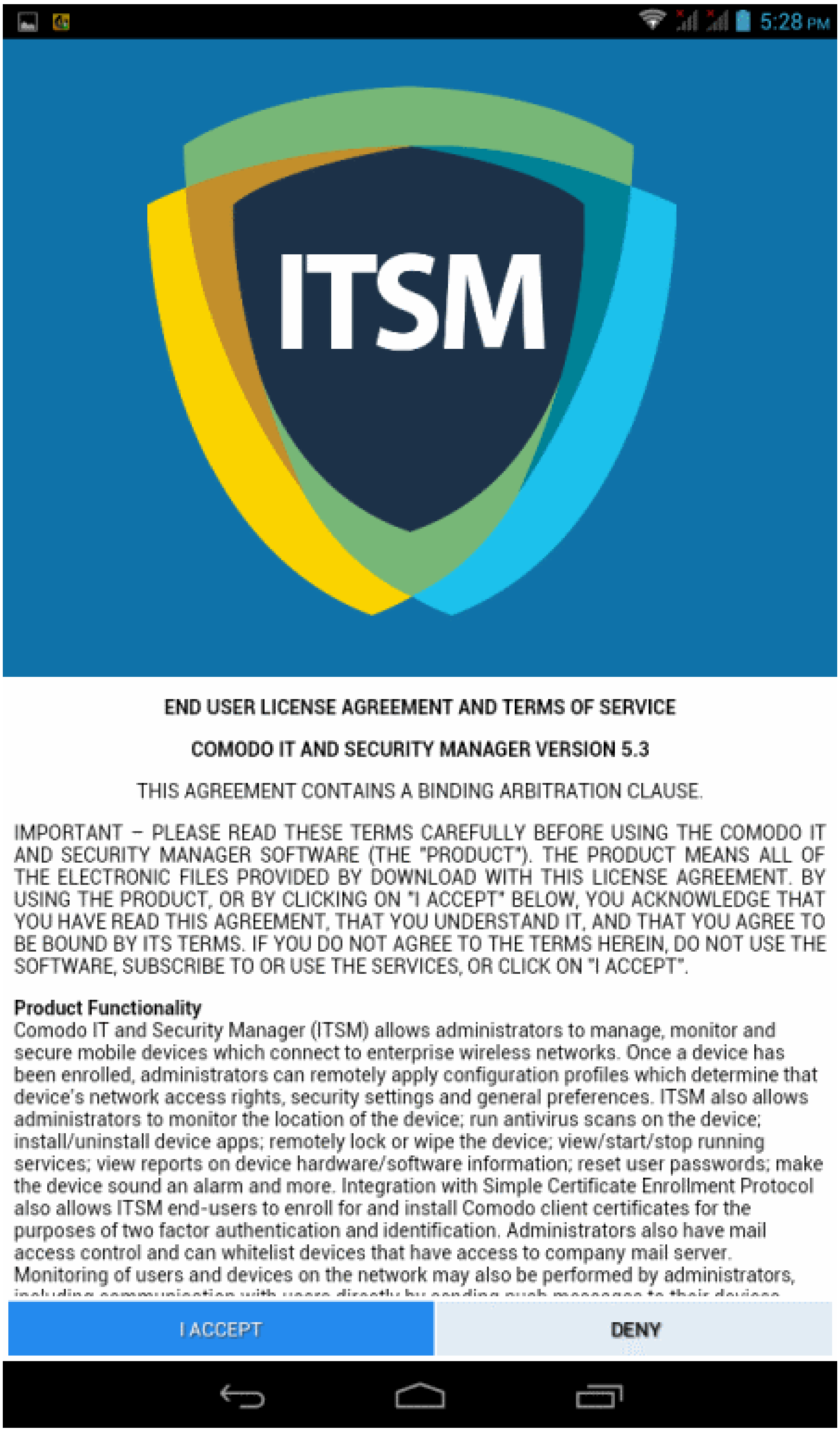
See **Importing User Groups from LDAP** for more details on this process.



- Enter the username and password you use to login to your network domain.
- Tap the 'Login' button

End User License Agreement

The EULA screen will appear.



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

COMODO IT AND SECURITY MANAGER VERSION 5.3

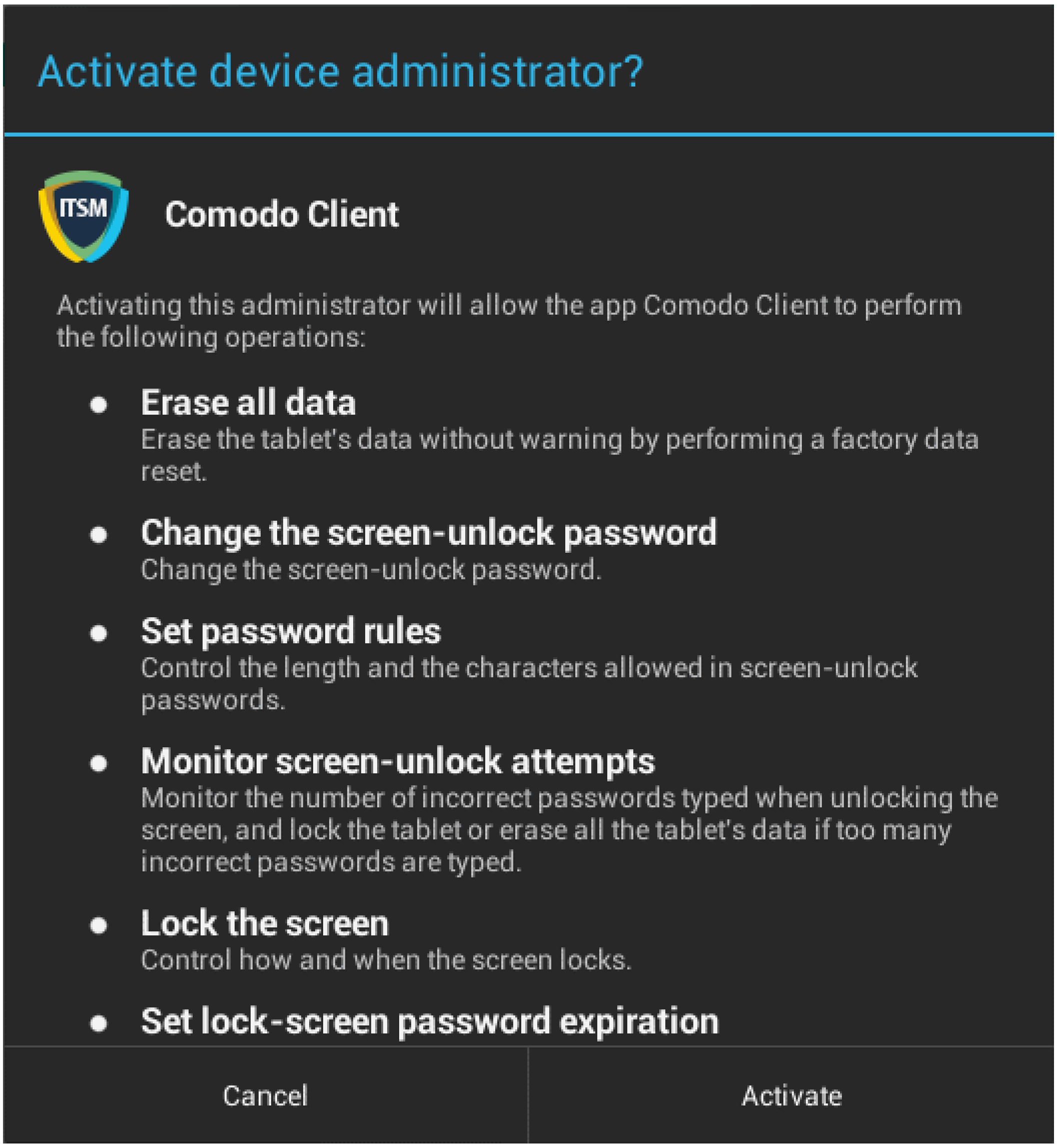
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO IT AND SECURITY MANAGER SOFTWARE (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

Product Functionality
Comodo IT and Security Manager (ITSM) allows administrators to manage, monitor and secure mobile devices which connect to enterprise wireless networks. 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 administrators to monitor the location of the device; run antivirus scans on the device; install/uninstall device apps; remotely lock or wipe the device; view/start/stop running services; view reports on device hardware/software information; reset user passwords; make the device sound an alarm and more. Integration with Simple Certificate Enrollment Protocol also allows ITSM end-users to enroll for and install Comodo client certificates for the purposes of two factor authentication and identification. Administrators also have mail access control and can whitelist devices that have access to company mail server. Monitoring of users and devices on the network may also be performed by administrators, including communication with users directly by sending push messages to their devices

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

This will open the app activation screen. Activation requires the app is given some admin privileges:



Activate device administrator?

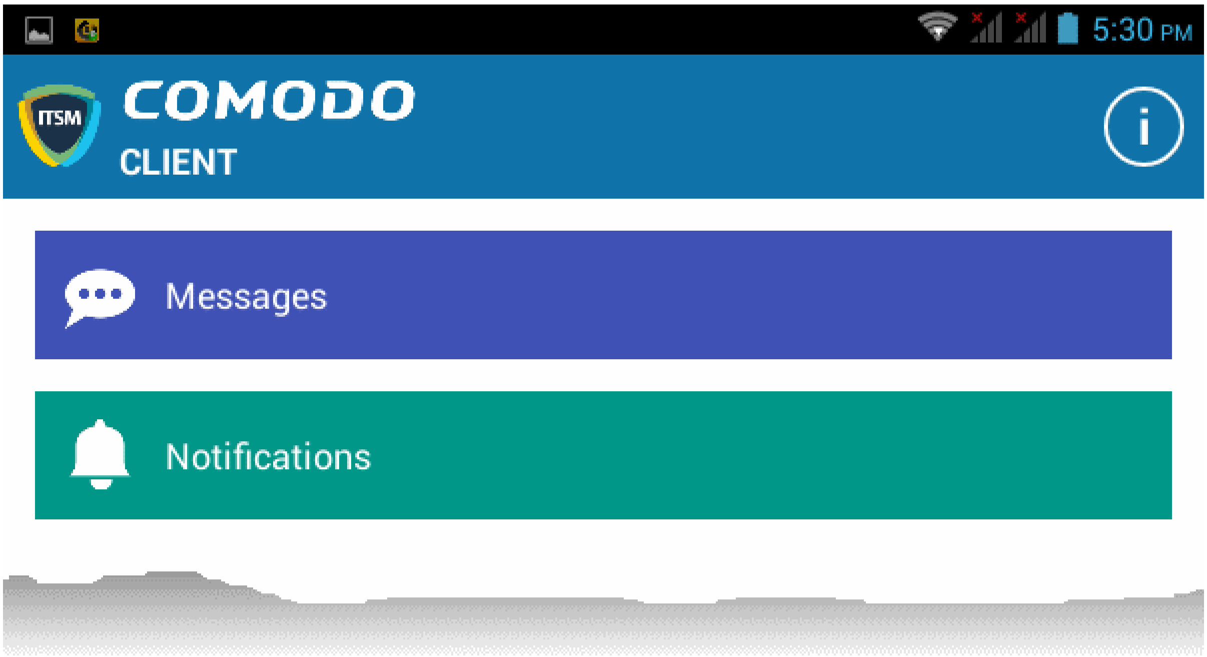
Comodo Client

Activating this administrator will allow the app Comodo Client to perform the following operations:

- **Erase all data**
  Erase the tablet's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set lock-screen password expiration**

- Tap 'Activate'.

The ITSM agent home screen will open:



The device is now enrolled to ITSM. A security profile will be applied to the device as follows:

- If the user is already associated with a configuration profile in ITSM then those profiles will be applied to the device. See **Assign Configuration Profile(s) to User Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default Android profile(s) will be applied to the device. See **Managing Default Profiles** for more details.

The device can now be remotely managed from the ITSM console.

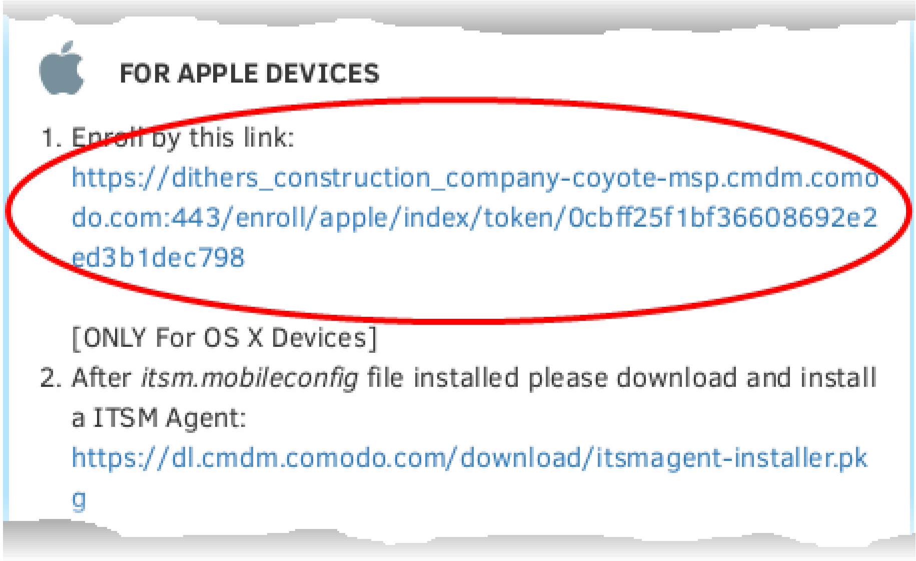
4.1.2.2. Enroll iOS Devices

After the administrator has added devices for a user, the user will receive an enrollment email with a link to a page containing enrollment instructions and links to download the ITSM profile and the server certificate. Users should open the mail on the device you want to enroll and follow the setup 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 on the device itself then tap the Apple enrollment link to open the device setup page
- On the setup page, click the install link for Apple devices:

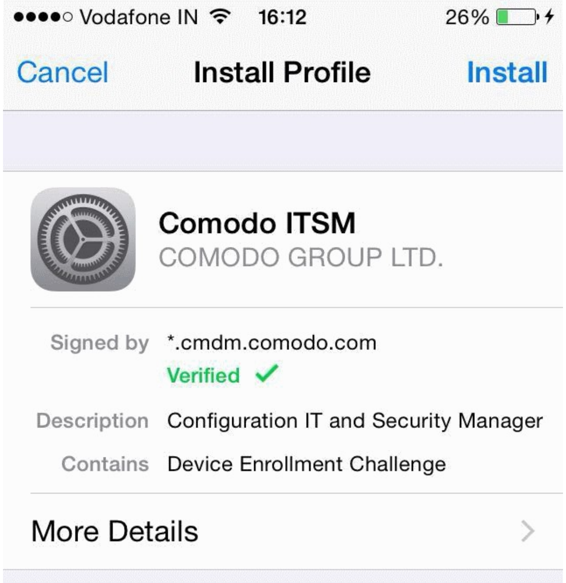


FOR APPLE DEVICES

1. Enroll by this link:
   https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/apple/index/token/0cbff25f1bf36608692e2ed3b1dec798

   [ONLY For OS X Devices]
2. After *itsm.mobileconfig* file installed please download and install a ITSM Agent:
   https://dl.cmdm.comodo.com/download/itsmagent-installer.pkg

The 'Install Profile' wizard will start.



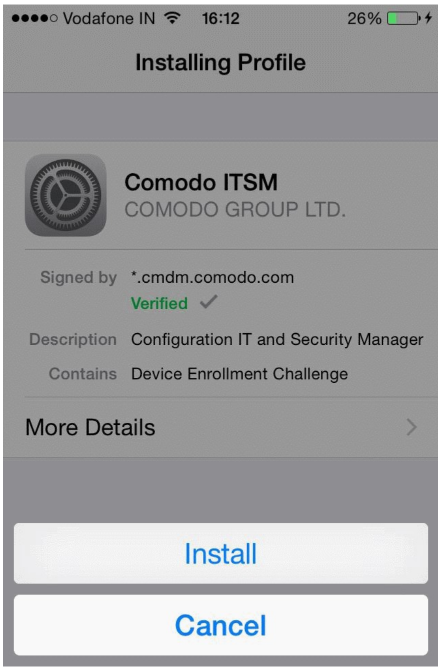
Comodo ITSM
COMODO GROUP LTD.

Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

Contains Device Enrollment Challenge

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



Comodo ITSM
COMODO GROUP LTD.

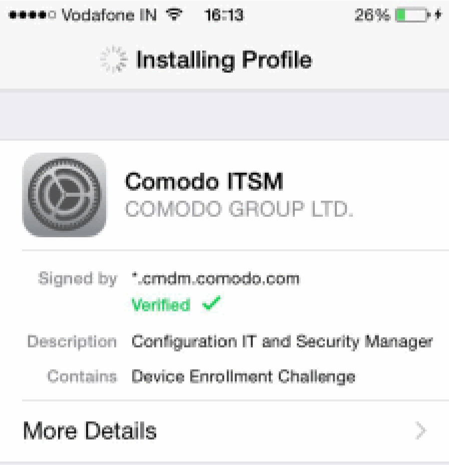
Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

Contains Device Enrollment Challenge

- Tap 'Install'.

The ITSM Profile installation progress will be displayed.

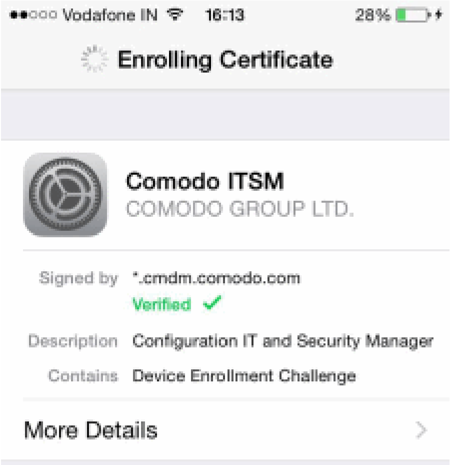


Comodo ITSM
COMODO GROUP LTD.

Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

Contains Device Enrollment Challenge



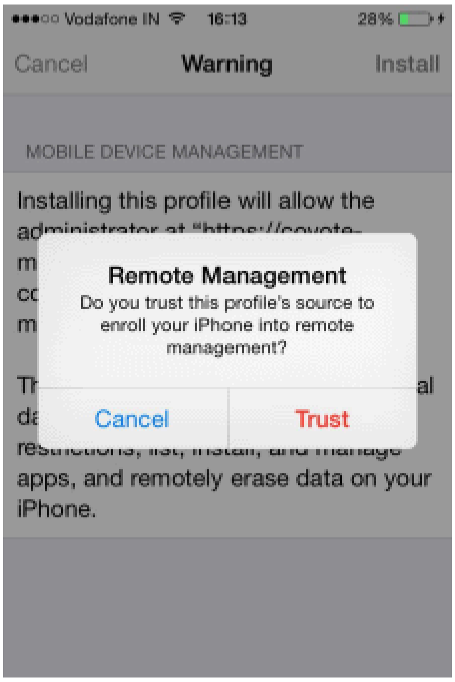
Comodo ITSM
COMODO GROUP LTD.

Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

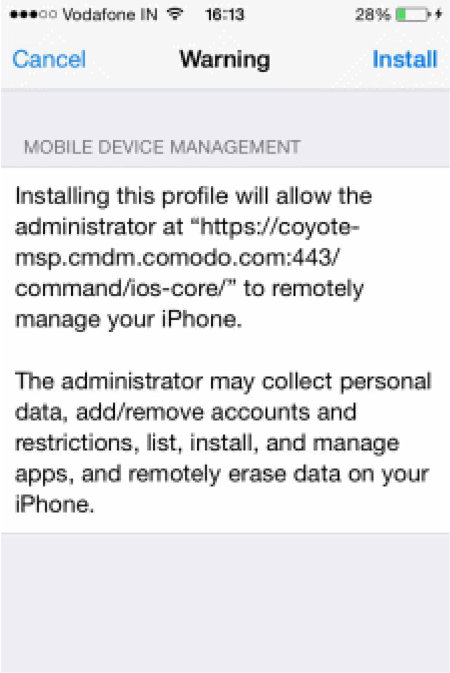
Contains Device Enrollment Challenge

- 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.



Remote Management

Do you trust this profile's source to enroll your iPhone into remote management?

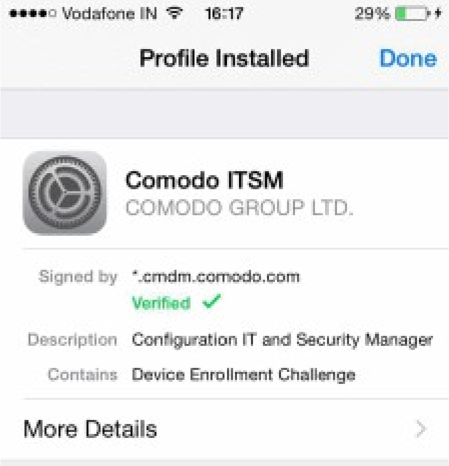


Installing this profile will allow the administrator at "https://coyote-msp.cmdm.comodo.com:443/command/ios-core/" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.

- Click Install in the 'Warning' screen

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



Comodo ITSM
COMODO GROUP LTD.

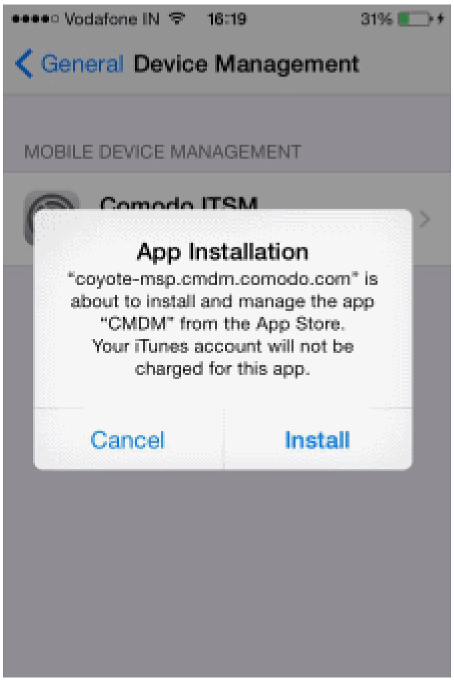
Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

Contains Device Enrollment Challenge

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

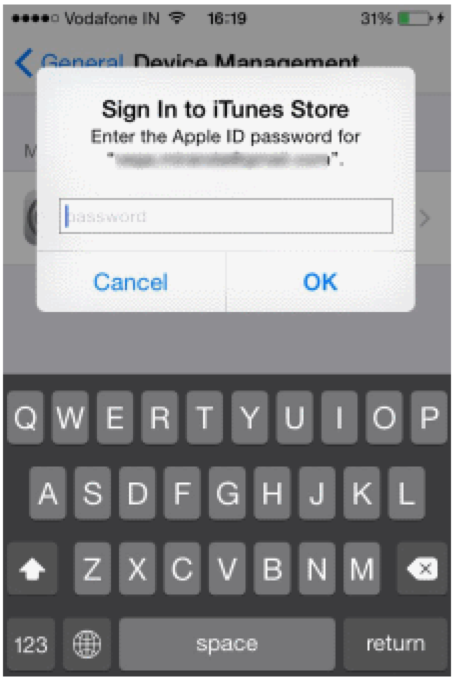
After installing the profile, the ITSM client app installation will begin. The app is essential for features such as app management, GPS location and ITSM messaging.



App Installation

"coyote-msp.cmdm.comodo.com" is about to install and manage the app "CMDM" from the App Store. Your iTunes account will not be charged for this app.

The app will be downloaded from the iTunes store using the user's iTunes account. The user needs to enter their Apple account password to access the iTunes store:

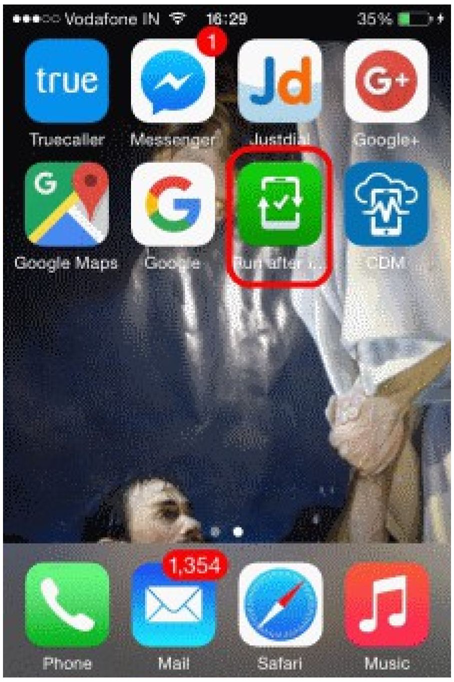


Sign In to iTunes Store

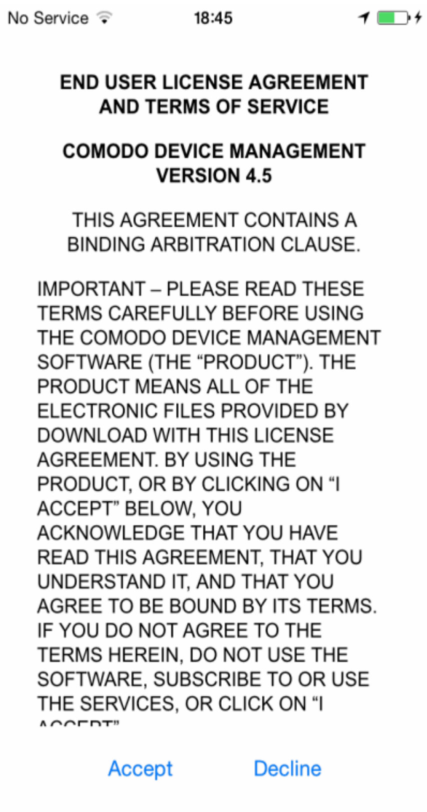
Enter the Apple ID password for "[redacted]".

password

- After installation, tap the green 'Run After Install' icon on the home screen:



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



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

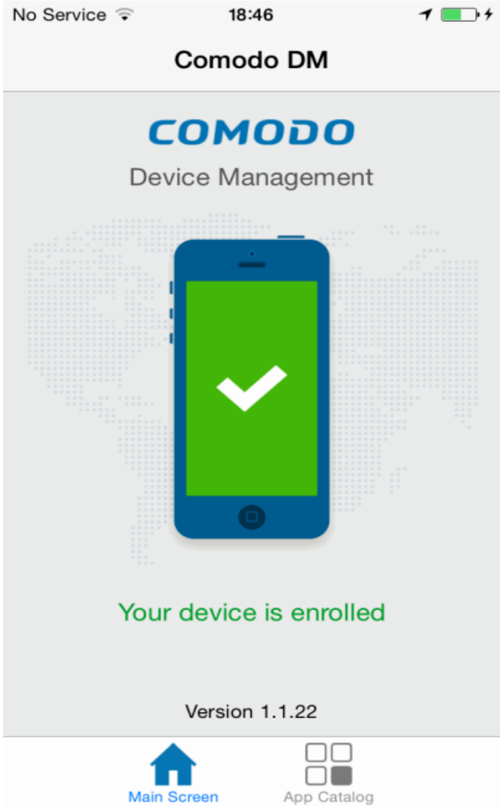
COMODO DEVICE MANAGEMENT VERSION 4.5

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

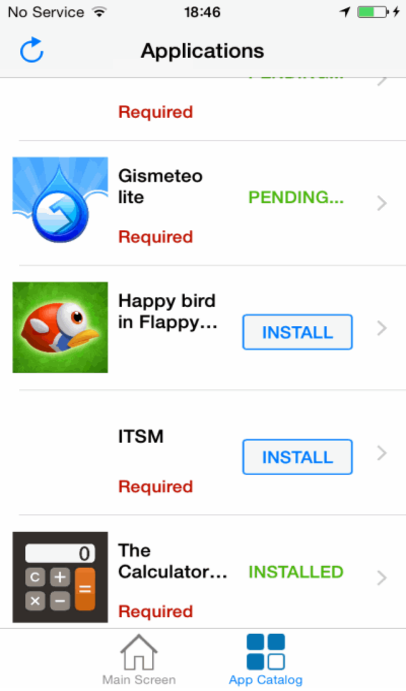
IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO DEVICE MANAGEMENT SOFTWARE (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT"

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

The device will be successfully enrolled.



Tap 'App Catalog' to view iOS apps that are installed, apps that are required to be installed and available apps:



The device is now enrolled to ITSM. A security profile will be applied to the device as follows:

- If the user is already associated with a configuration profile in ITSM then those profiles will be applied to the device. See **Assig Configuration Profile(s) to User Device** and **Assig Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default iOS profile(s) will be applied to the device. See **Managing Default Profiles** for more details.

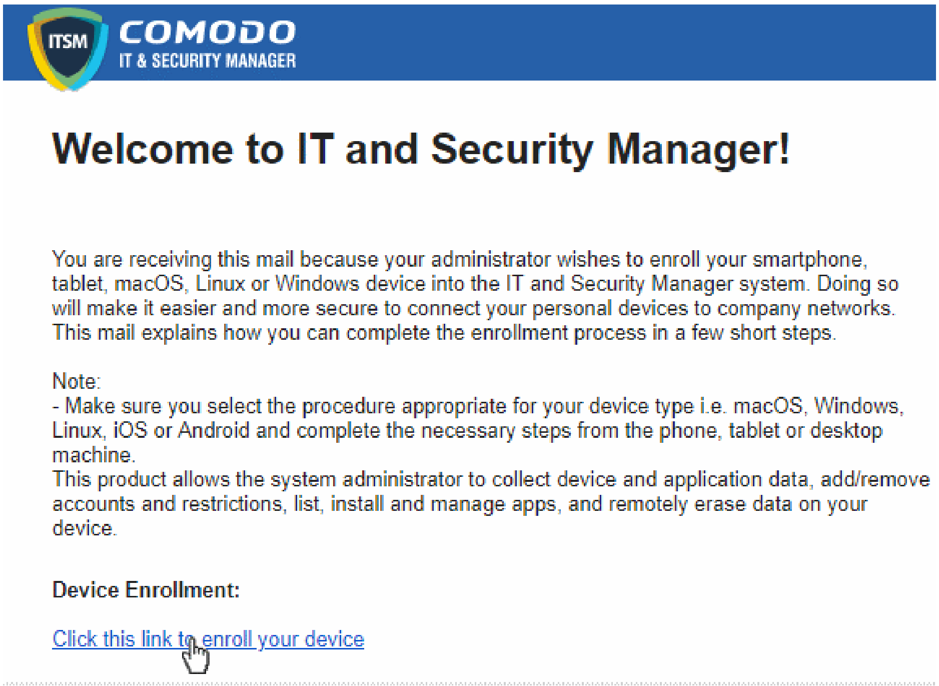
The device can now be remotely managed from the ITSM console.

4.1.2.3. Enroll Windows Endpoints

- After an administrator has added devices for a user, the user will receive an enrollment email with a link to the setup page.
- The setup page contains device enrollment instructions and a link to install the ITSM communication agent for Windows endpoints.
- Users should open the email on the Windows endpoint you want to enroll. After installation, the ITSM agent will automatically connect to the ITSM server.

To auto enroll a Windows device

- Open the email on the device you want to enroll.



Welcome to IT and Security Manager!

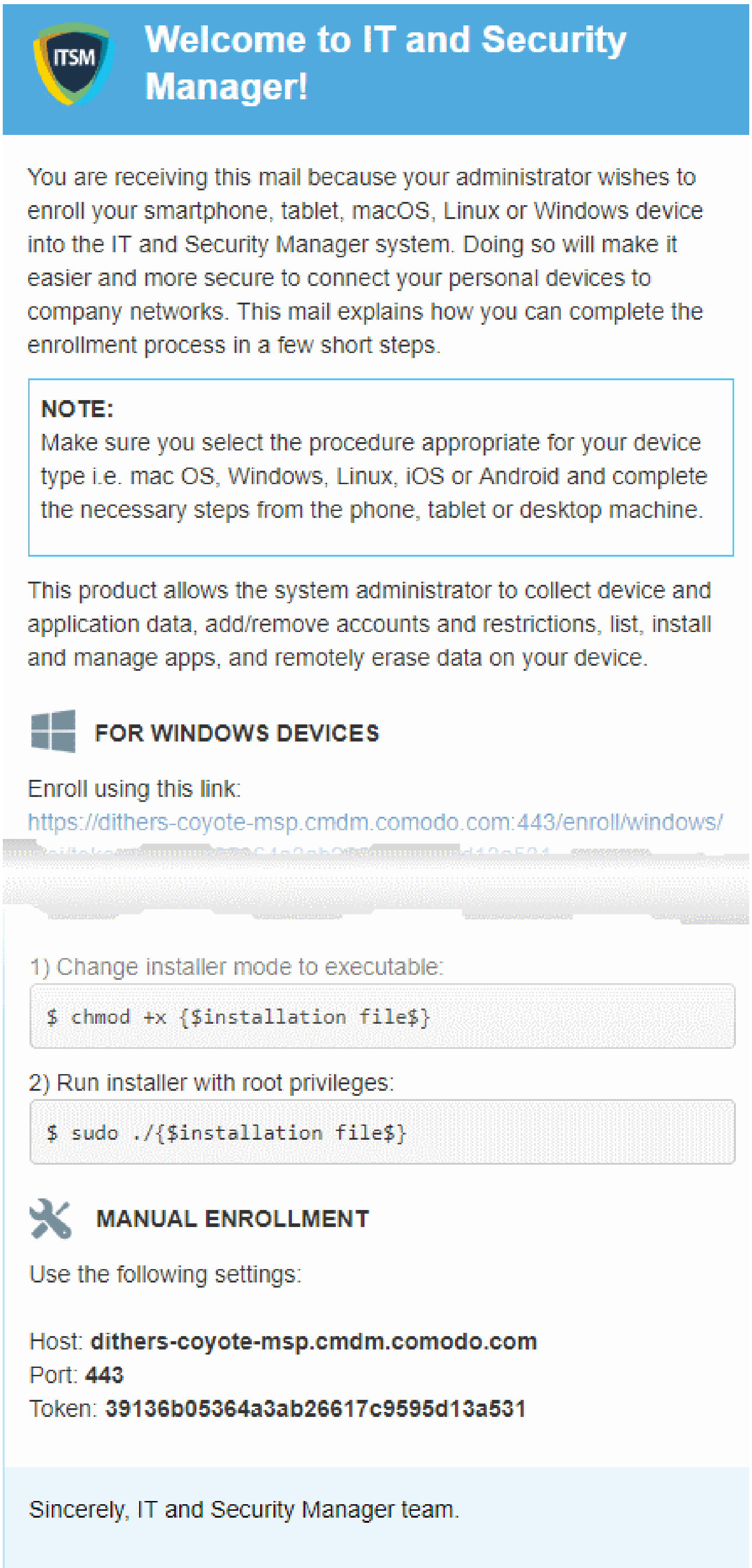
You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux or Windows device into the IT and Security Manager system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete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

Note:
- Make sure you select the procedure appropriate for your device type i.e. macOS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, 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.

Device Enrollment:

Click this link to enroll your device

- Click the enrollment link in the email.
- The 'Device Enrollment' page will open.



Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux 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:
Make sure you select the procedure appropriate for your device type i.e. mac OS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, 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 using this link:
https://dithers-coyote-msp.cmdm.comodo.com:443/enroll/windows/

[redacted]

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

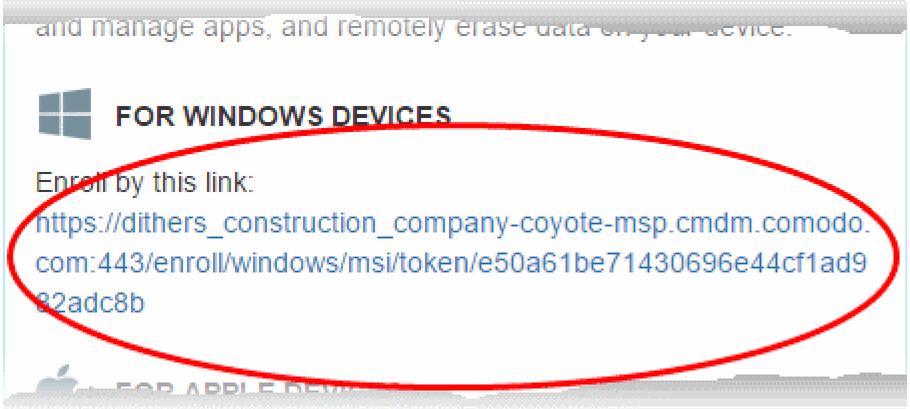
MANUAL ENROLLMENT

Use the following settings:

Host: **dithers-coyote-msp.cmdm.comodo.com**
Port: **443**
Token: **39136b05364a3ab26617c9595d13a531**

Sincerely, IT and Security Manager team.

- On the Device Enrollment page, click the install link for Windows devices:



and manage apps, and remotely erase data on your device.

FOR WINDOWS DEVICES

Enroll by this link:
https://dithers_construction_company-coyote-msp.cmdm.comodo.com:443/enroll/windows/msi/token/e50a61be71430696e44cf1ad982adc8b

FOR APPLE DEVICES

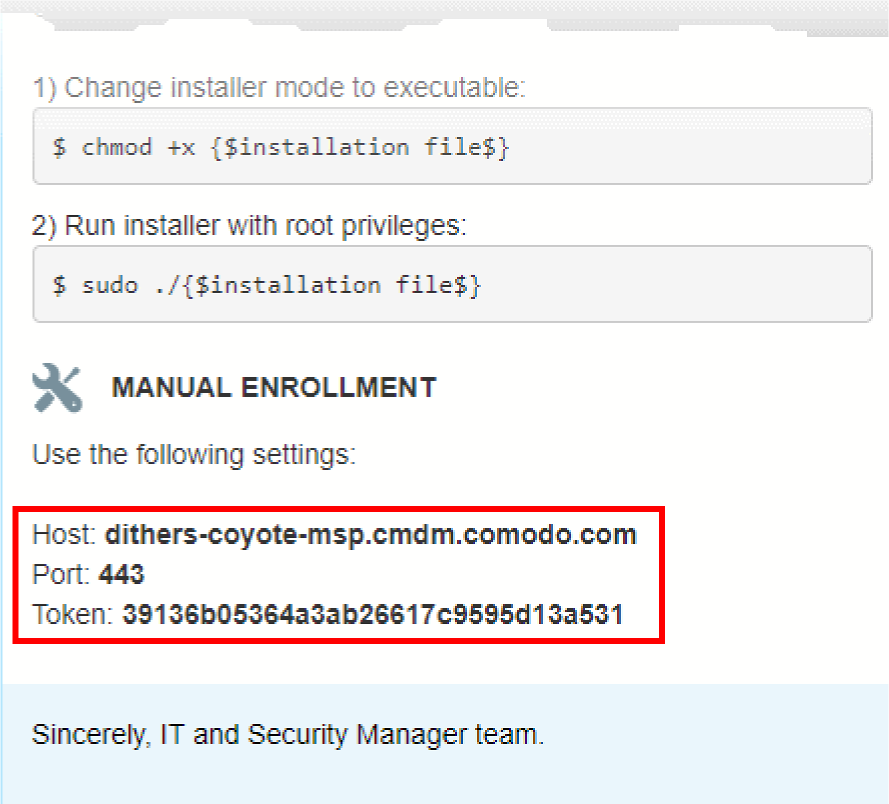
The ITSM agent setup file will download.

- Double-click on the file to install the agent.

The device will be automatically enrolled to ITSM once installation is complete. The following icon will appear at the bottom-right of the endpoint screen.

If the ITSM communication agent is not automatically enrolled at the time of installation, for example, due to internet connectivity issues, you can manually enroll the device at a later time.

For manual enrollment you will need to enter the host, port and token ID. You can find these items on the end of the device enrollment page.



1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

MANUAL ENROLLMENT

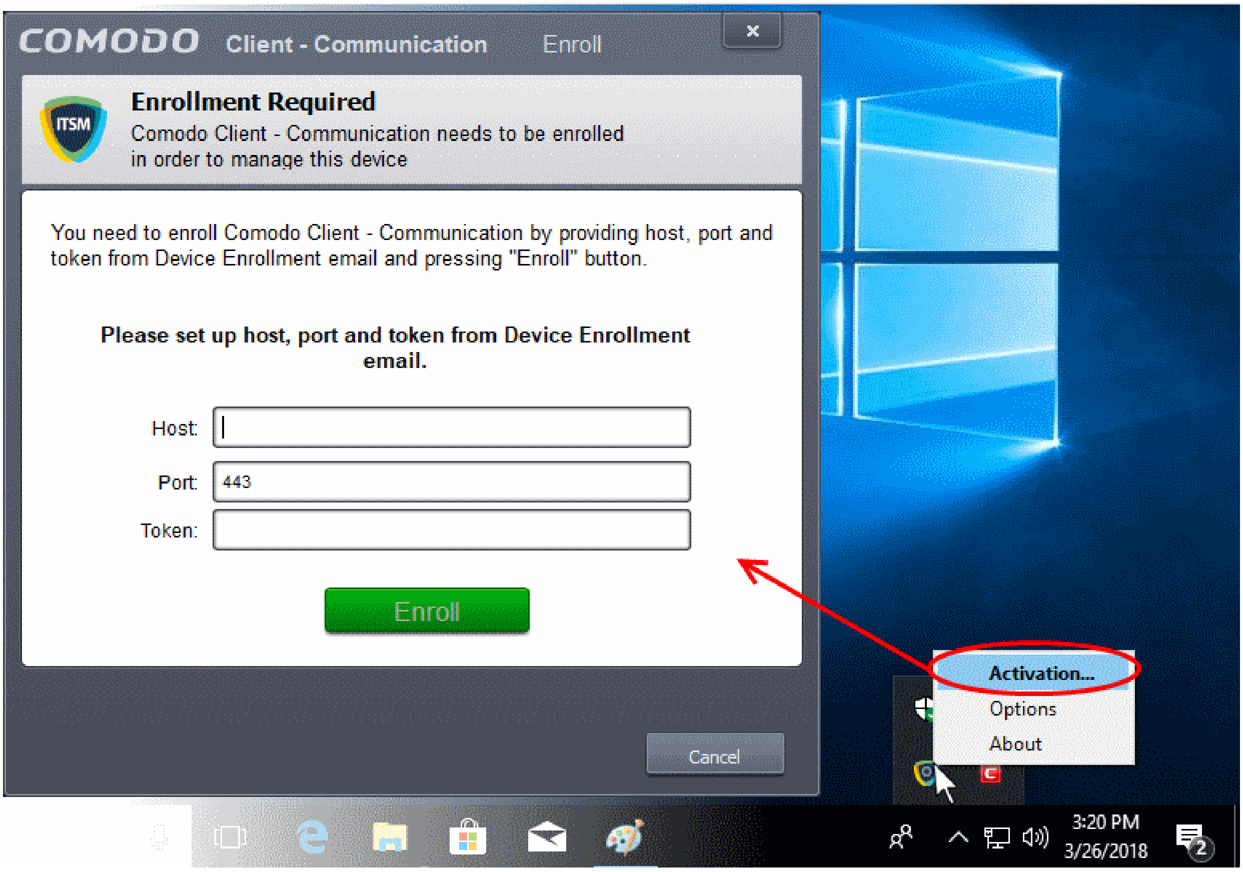
Use the following settings:

Host: **dithers-coyote-msp.cmdm.comodo.com**
Port: **443**
Token: **39136b05364a3ab26617c9595d13a531**

Sincerely, IT and Security Manager team.

To manually enroll your device

- Right-click on the ITSM system tray icon and select 'Activation'



COMODO Client - Communication Enroll

Enrollment Required

Comodo Client - Communication needs to be enrolled in order to manage this device

You need to enroll Comodo Client - Communication by providing host, port and token from Device Enrollment email and pressing "Enroll" button.

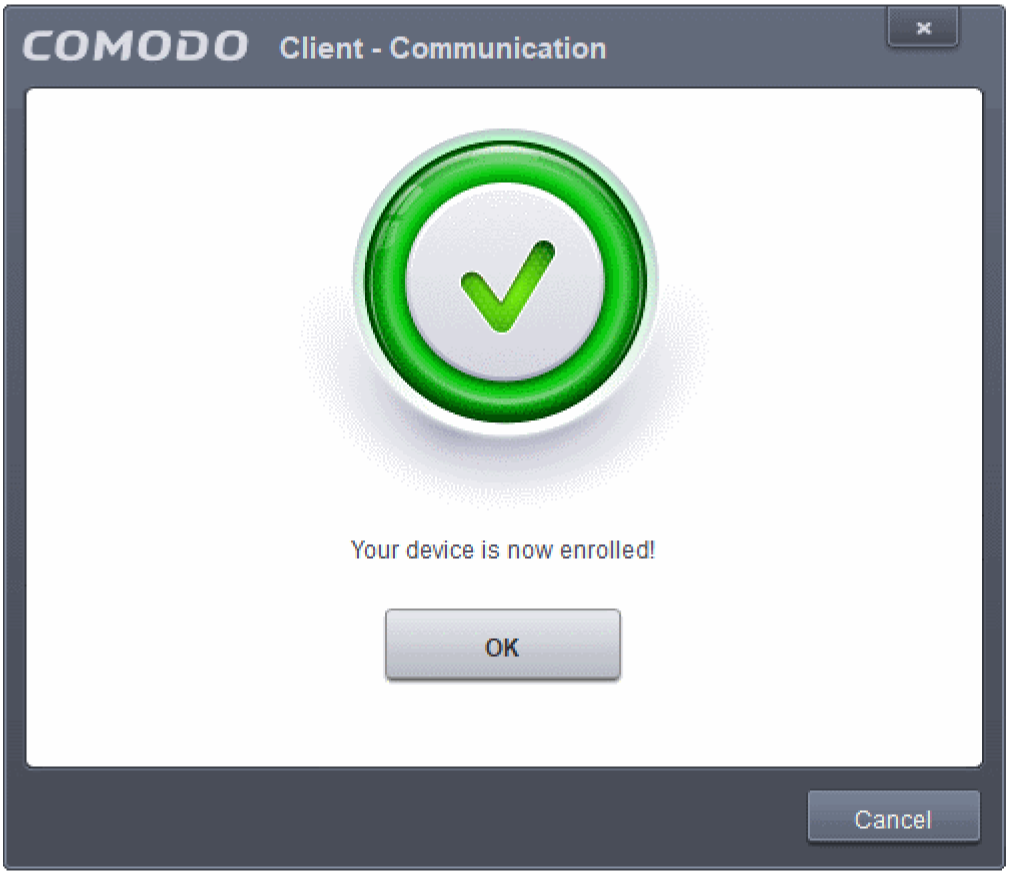
Please set up host, port and token from Device Enrollment email.

Host:

Port: 443

Token:

- Enter the 'host', 'port' and the 'Token' contained in the device enrollment page and click 'Enroll'.
- CCC (the endpoint software) will communicate with the ITSM server and enroll the device.



COMODO Client - Communication

Your device is now enrolled!

After device enrollment, the next step is to install Comodo Client Security (CCS) onto the endpoint. See **Remotely Installing Packages onto Windows Devices** for help with this.

A security profile will be applied to the device when CCS is installed. Profile deployment is as follows:

- If the user is already associated with a configuration profile in ITSM then those profiles will be applied to the device. See **Assign Configuration Profile(s) to User Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default Windows profile(s) will be applied to the device. See. See **Managing Default Profiles** for more details.

The device can now be remotely managed from the ITSM console.

ITSM allows you to rebrand the CCC and CCS applications to change the appearance and interface texts in their GUI. This is especially useful for customers who wish to white-label the CCC/CCS interfaces for their clients.

- The 'UI Settings' component of a configuration profile applied to the device can be configured to:
    - Show your company name, support website, phone number and email.
    - Display your company logo, header logo, product icons and product logo in various interfaces of the applications.
    - See **CCC and CCS Application UI Settings** under **Creating Windows Profiles** for more details.

4.1.2.4. Enroll 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.

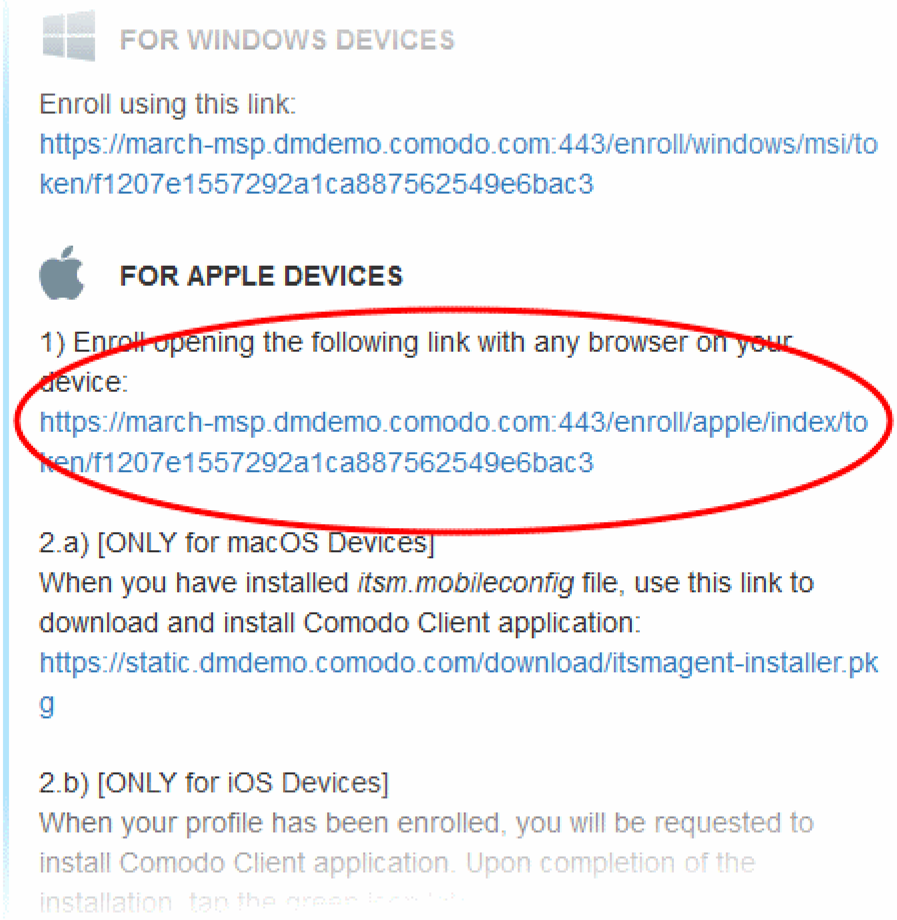
Enrolling a Mac OS device involves two steps:

- **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":



FOR WINDOWS DEVICES

Enroll using this link:
https://march-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/f1207e1557292a1ca887562549e6bac3

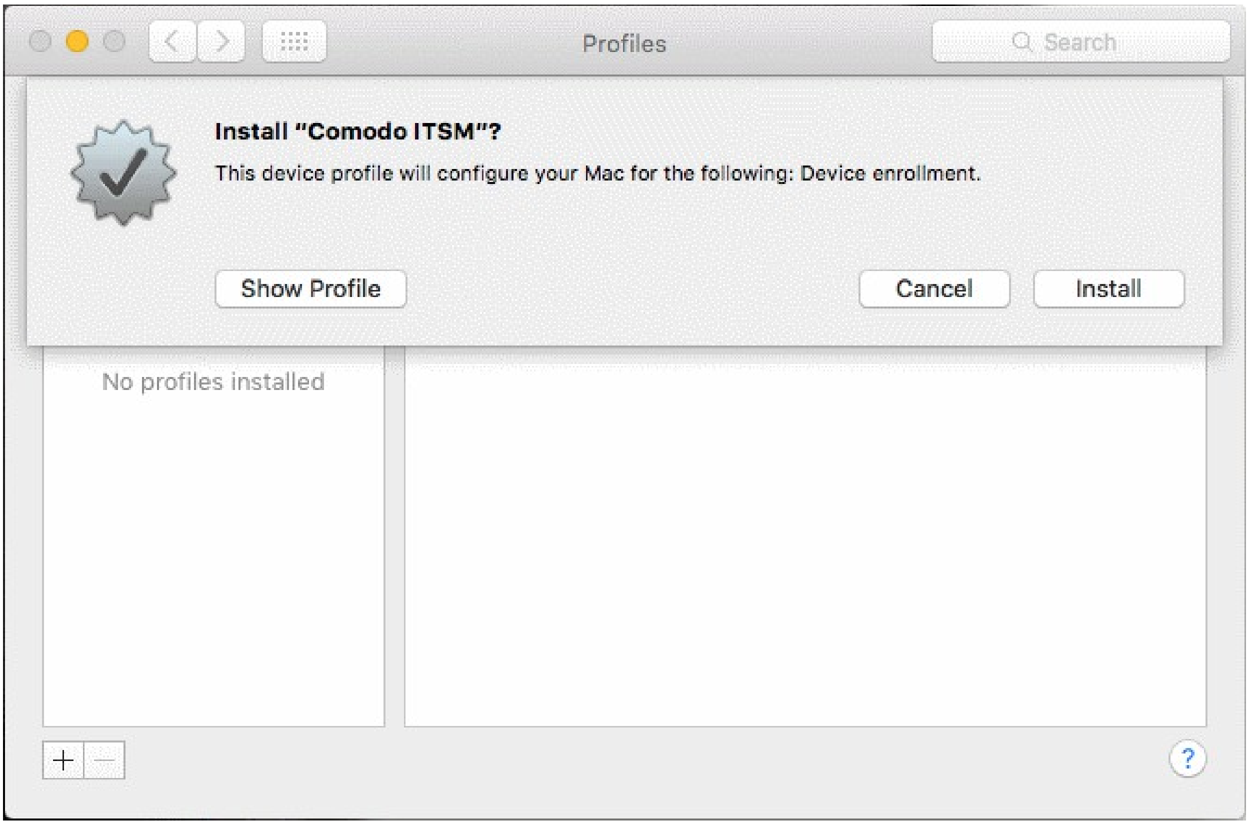
FOR APPLE DEVICES

1) Enroll opening the following link with any browser on your device:
https://march-msp.dmdemo.comodo.com:443/enroll/apple/index/token/f1207e1557292a1ca887562549e6bac3

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

2.b) [ONLY for iOS Devices]
When your profile has been enrolled, you will be requested to install Comodo Client application. Upon completion of the installation, tap the green icon ...

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

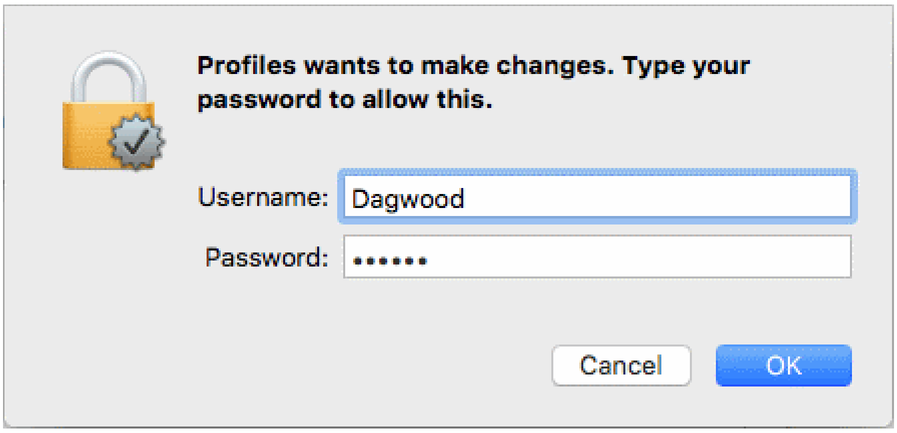


Install "Comodo ITSM"?

This device profile will configure your Mac for the following: Device enrollment.

- Tap 'Install'.

You need to enter your password to install the profile.



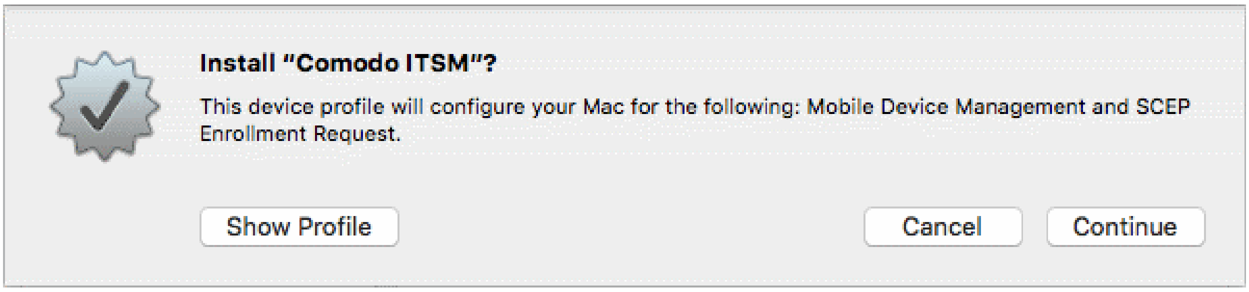
Profiles wants to make changes. Type your password to allow this.

Username: Dagwood

Password: ••••••

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

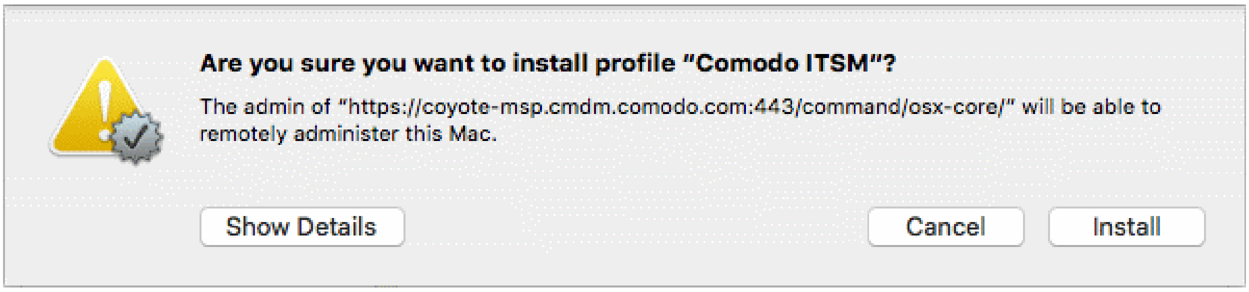
Confirmation dialogs will appear for profile installation.



Install "Comodo ITSM"?

This device profile will configure your Mac for the following: Mobile Device Management and SCEP Enrollment Request.

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

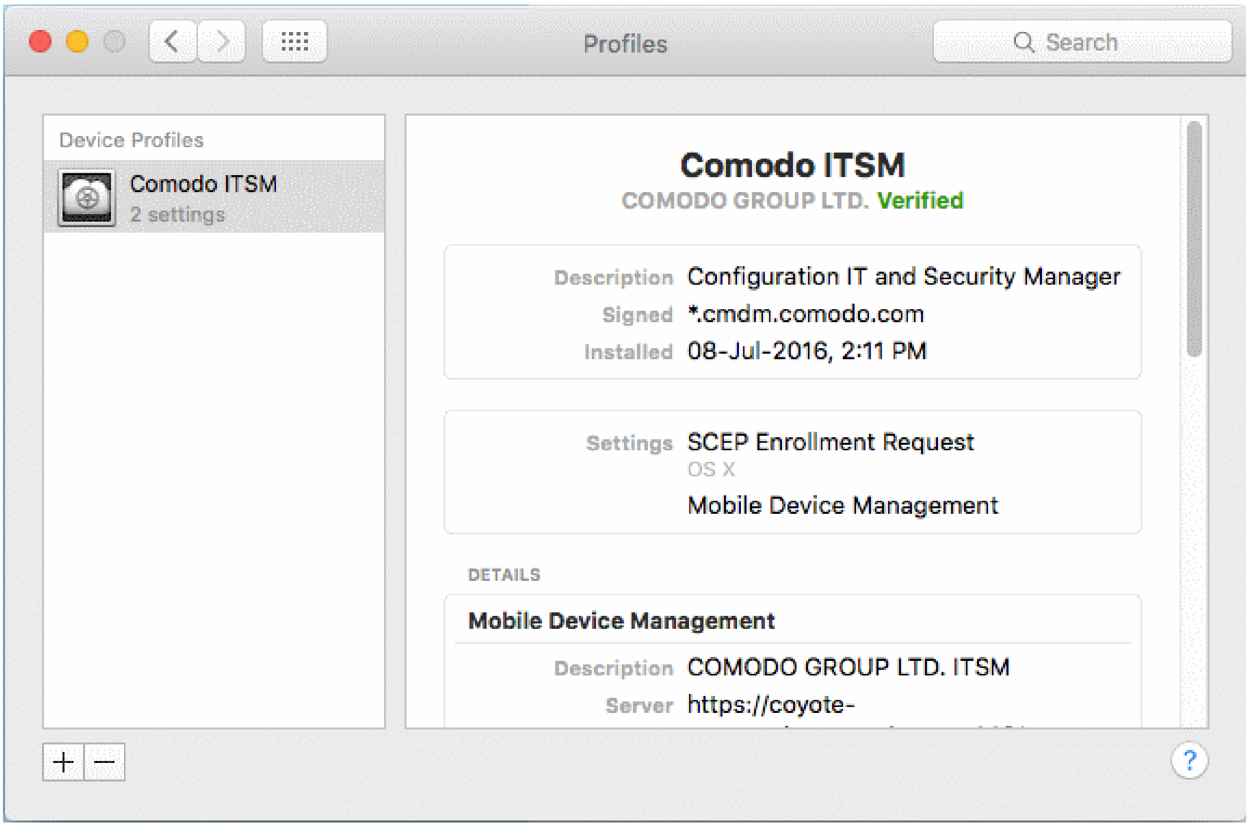


Are you sure you want to install profile "Comodo ITSM"?

The admin of "https://coyote-msp.cmdm.comodo.com:443/command/osx-core/" will be able to remotely administer this Mac.

- Click 'Install'

The profile will be installed.



Comodo ITSM
COMODO GROUP LTD. Verified

Description Configuration IT and Security Manager
Signed *.cmdm.comodo.com
Installed 08-Jul-2016, 2:11 PM

Settings SCEP Enrollment Request
OS X
Mobile Device Management

DETAILS

Mobile Device Management

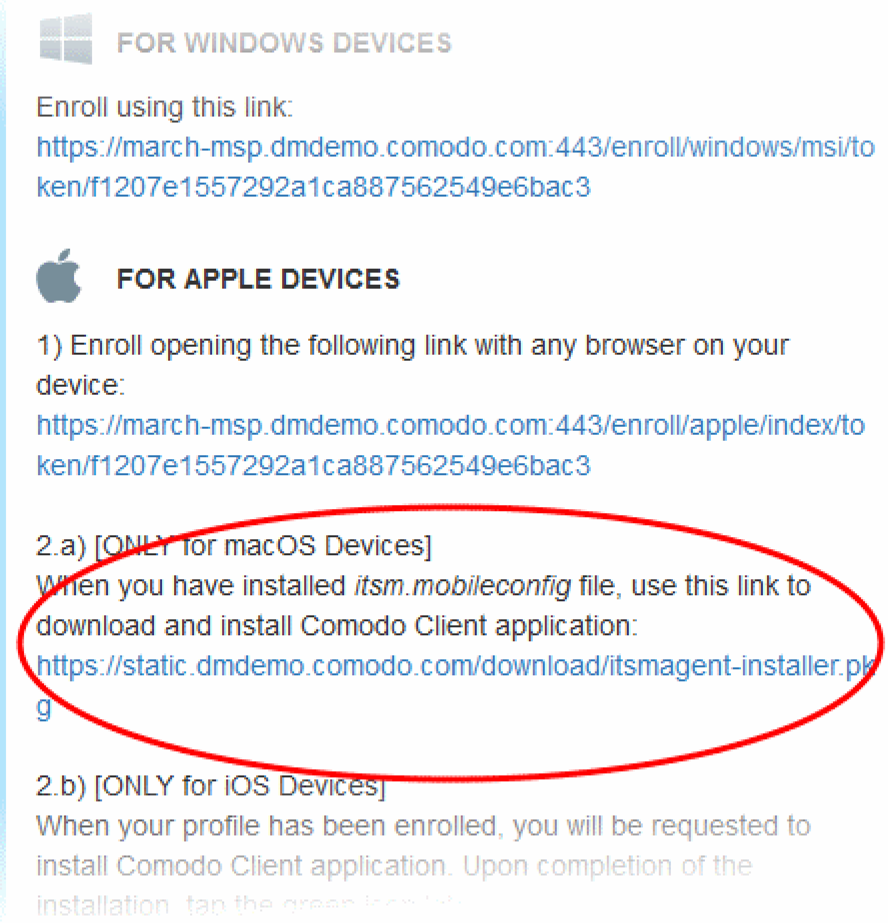
Description COMODO GROUP LTD. ITSM
Server https://coyote-

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:



FOR WINDOWS DEVICES

Enroll using this link:
https://march-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/f1207e1557292a1ca887562549e6bac3

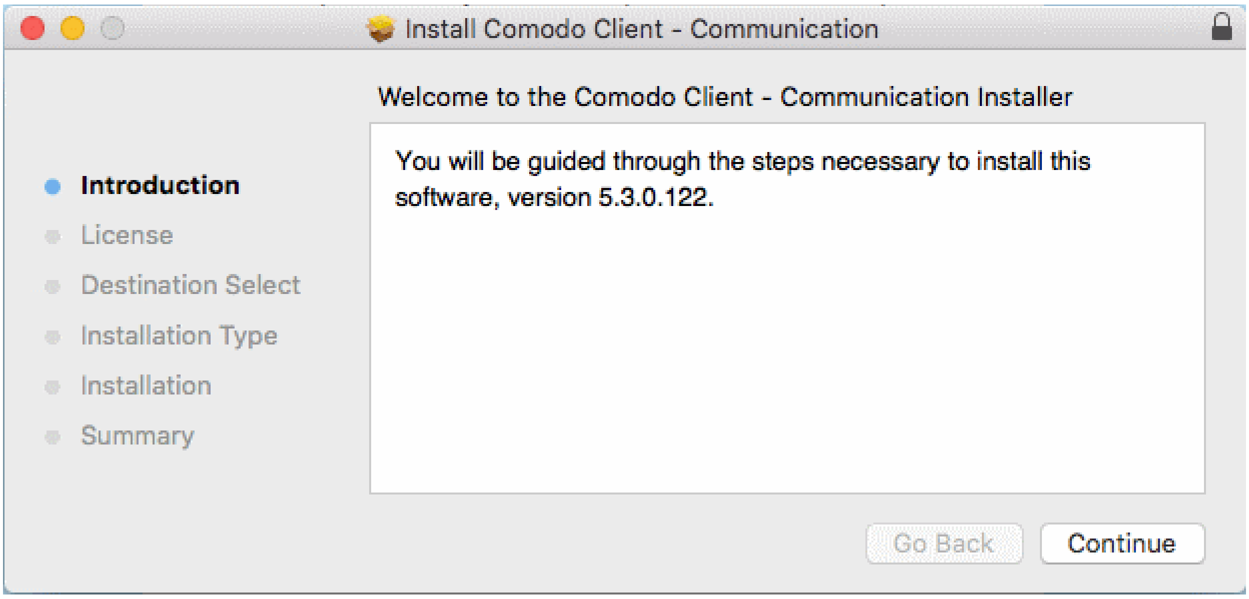
FOR APPLE DEVICES

1) Enroll opening the following link with any browser on your device:
https://march-msp.dmdemo.comodo.com:443/enroll/apple/index/token/f1207e1557292a1ca887562549e6bac3

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

2.b) [ONLY for iOS Devices]
When your profile has been enrolled, you will be requested to install Comodo Client application. Upon completion of the installation, tap the green icon...

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



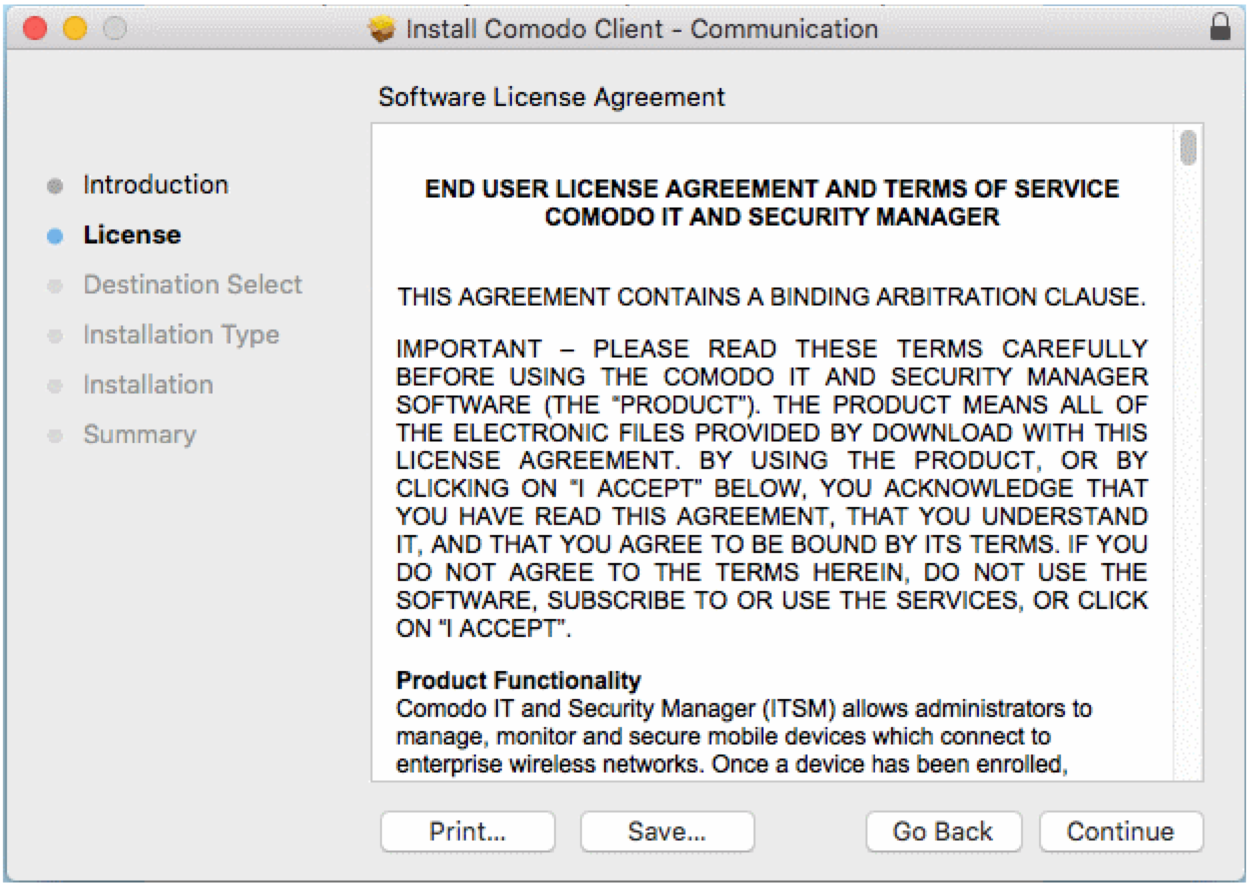
Install Comodo Client - Communication

Welcome to the Comodo Client - Communication Installer

You will be guided through the steps necessary to install this software, version 5.3.0.122.

- Click 'Continue'

The End User License Agreement will be displayed.



Software License Agreement

END USER LICENSE AGREEMENT AND TERMS OF SERVICE COMODO IT AND SECURITY MANAGER

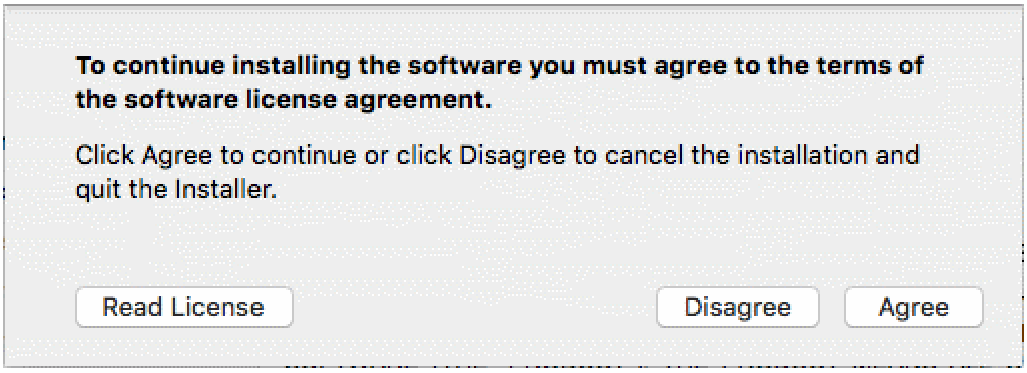
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO IT AND SECURITY MANAGER SOFTWARE (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

Product Functionality
Comodo IT and Security Manager (ITSM) allows administrators to manage, monitor and secure mobile devices which connect to enterprise wireless networks. Once a device has been enrolled,

- Read the EULA and click 'Continue'.

A confirmation dialog will appear.

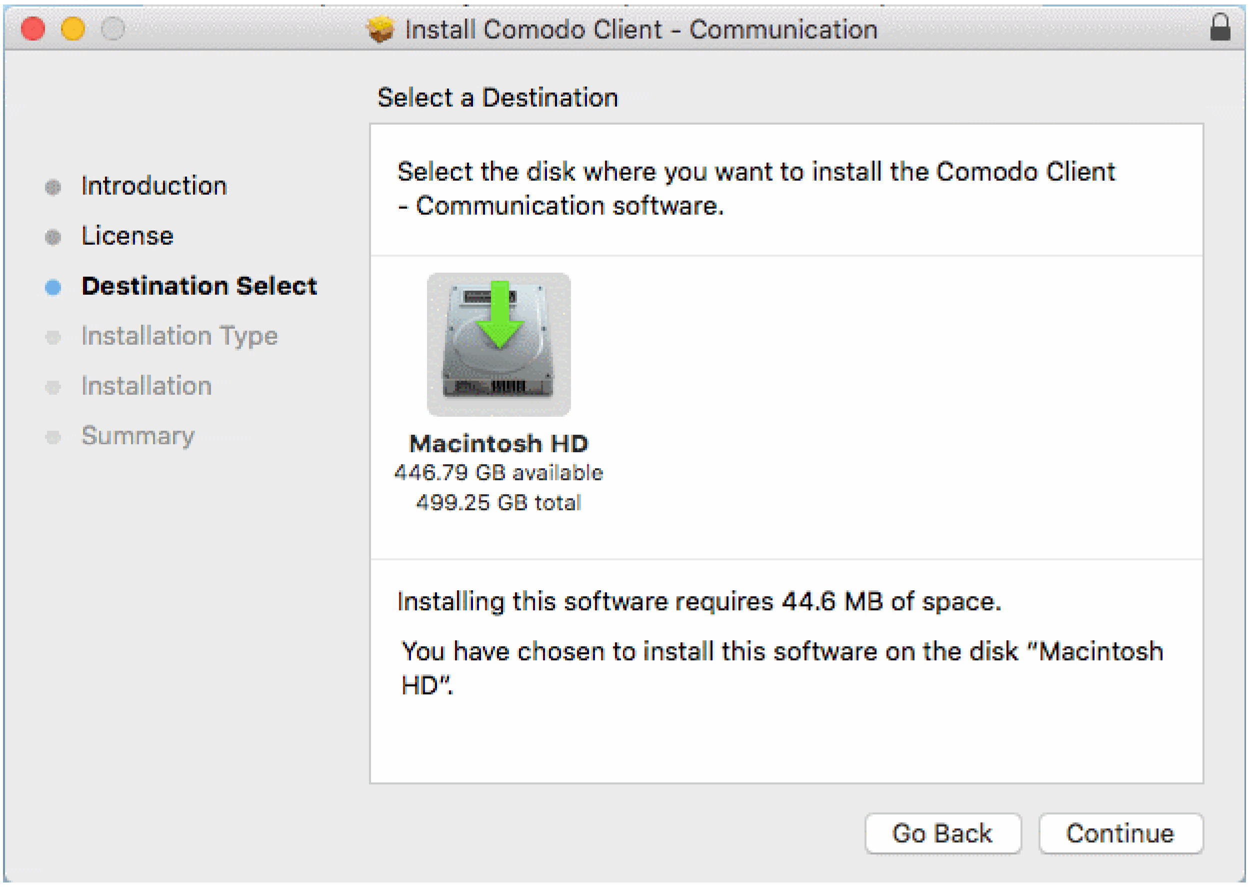


To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

- Click 'Agree'

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



Select a Destination

Select the disk where you want to install the Comodo Client - Communication software.

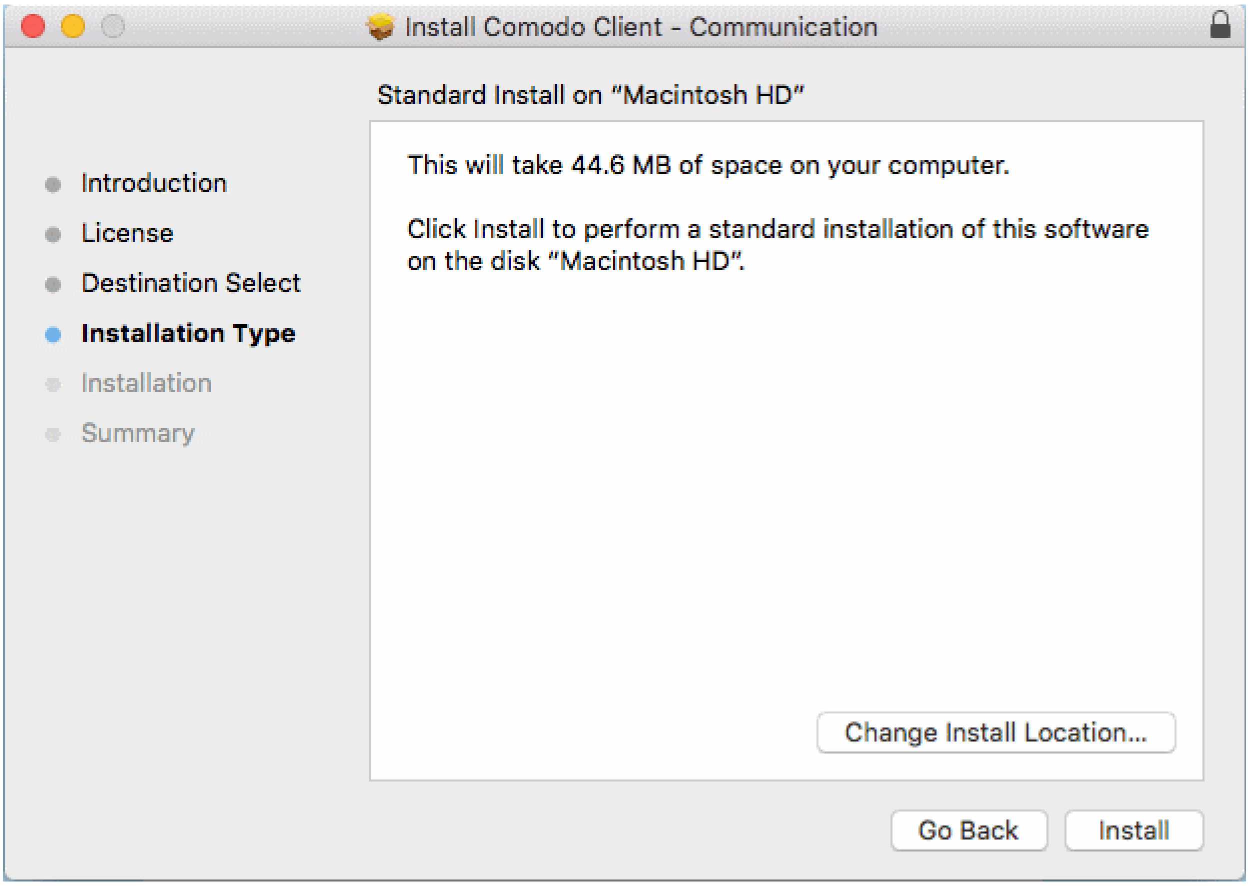
Macintosh HD
446.79 GB available
499.25 GB total

Installing this software requires 44.6 MB of space.

You have chosen to install this software on the disk "Macintosh HD".

- 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.



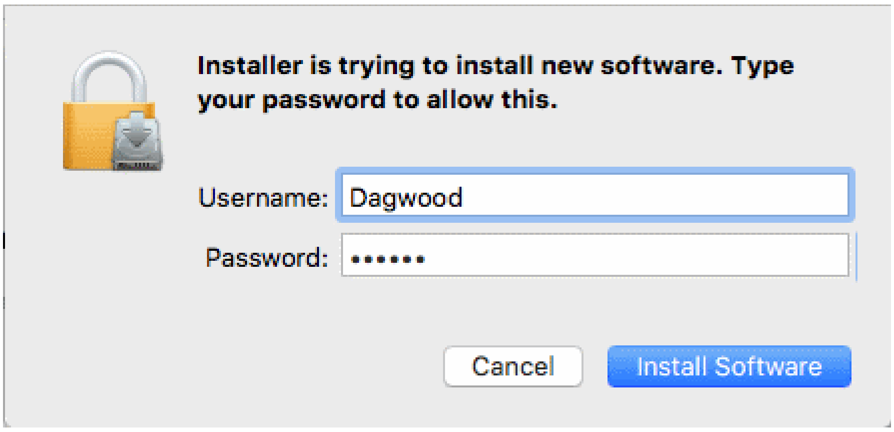
Standard Install on "Macintosh HD"

This will take 44.6 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

- Click 'Install'

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

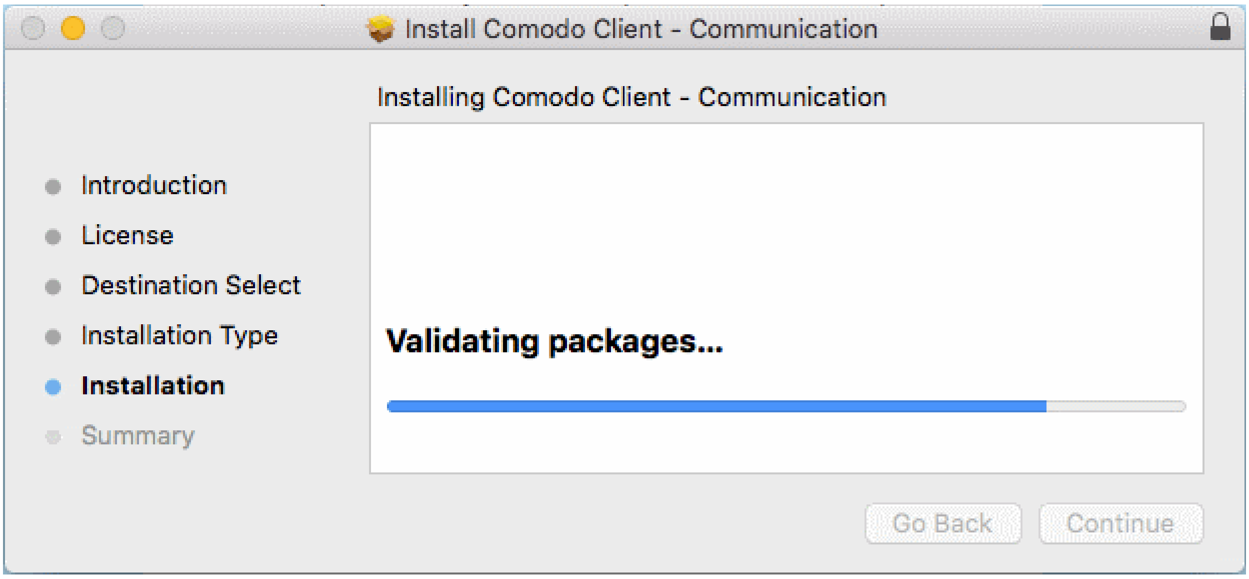


Installer is trying to install new software. Type your password to allow this.

Username: Dagwood

Password: ••••••

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

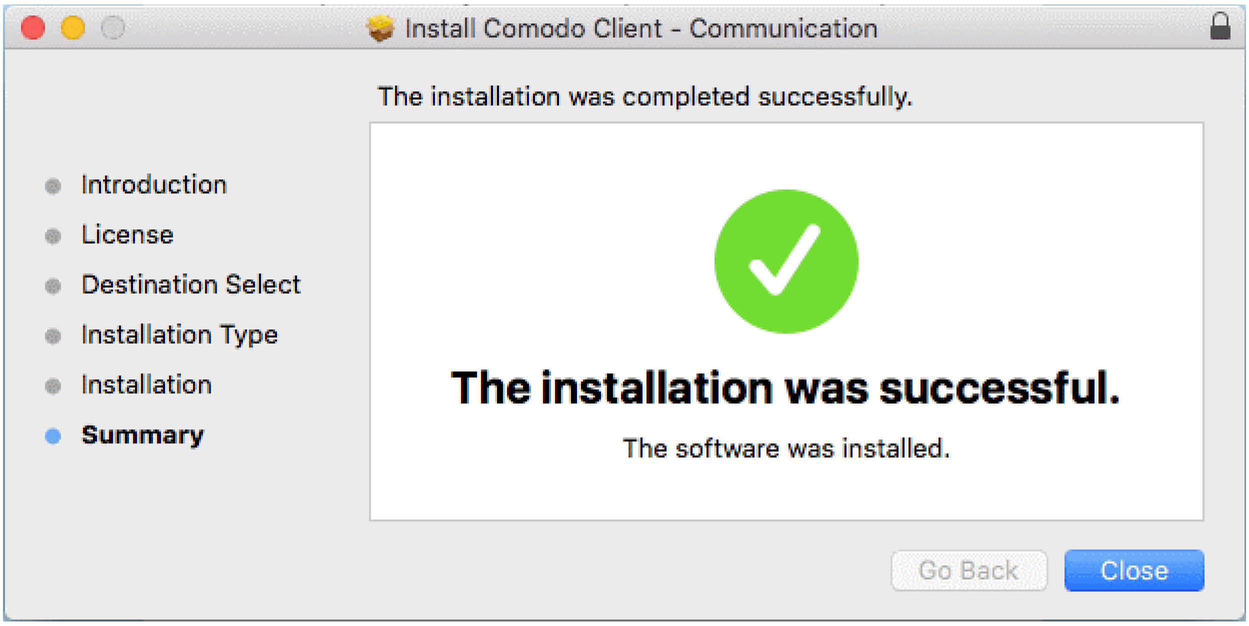


Install Comodo Client - Communication

Installing Comodo Client - Communication

Validating packages...

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



Install Comodo Client - Communication

The installation was completed successfully.

The installation was successful.

The software was installed.

Once the device is enrolled, the next step is to install Comodo Antivirus for Mac (CAVM) onto the endpoint in order for the default or assigned Mac profiles to take effect. Refer to the section **Remotely Installing Packages on Mac OS Devices** for more details.

- If the user/user group to which the user belongs is pre-associated with configuration profiles, then those Mac OS profiles will be applied to the device. See **Assigning Configuration Profile(s) to a Users' Devices** and **Assigning Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user/user group, the default profile(s) for Mac OS will be applied to the device. See **Managing Default Profiles** for more details.

The device can now be remotely managed from the ITSM console.

4.1.2.5. Enroll Linux OS Endpoints

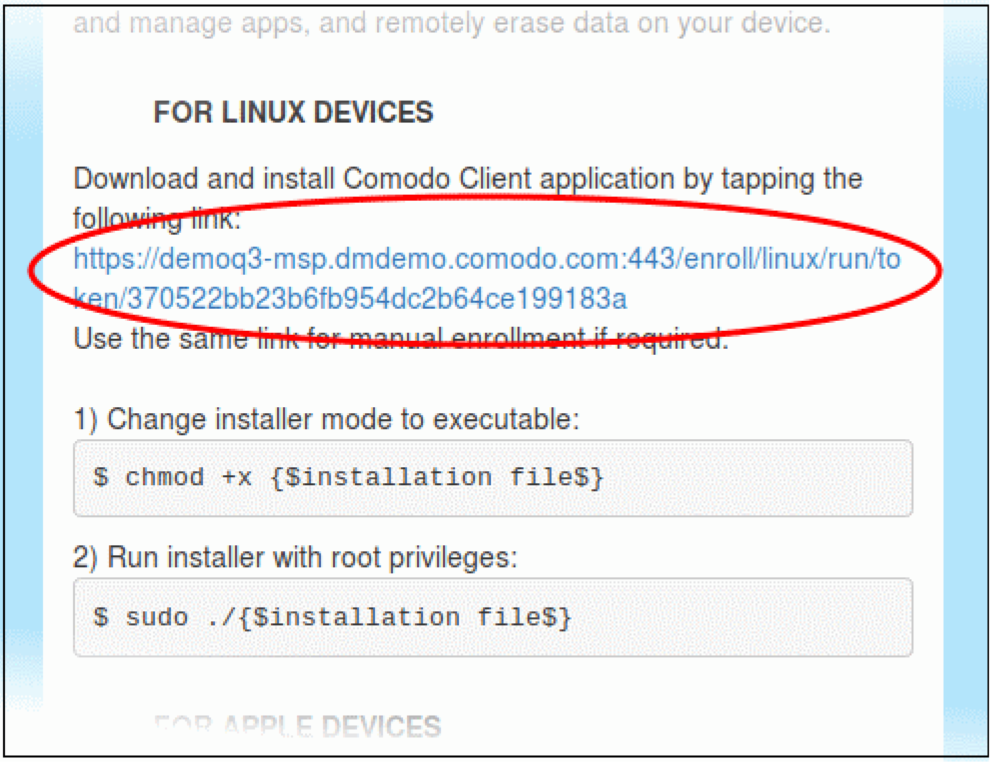
- End-users will receive an enrollment email after an admin has added their device to ITSM.
- The email contains instructions and a link to download the Linux ITSM agent.
- Users should open the email/complete the installation process on the Linux endpoint that is being enrolled.
- After installing the agent, the endpoint will automatically to connect to the ITSM server.

Supported Linux OS

- Ubuntu 16.04.2
- Debian 8.8
- Red Hat Enterprise 7

To auto enroll a Linux 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.



and manage apps, and remotely erase data on your device.

FOR LINUX DEVICES

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

1) Change installer mode to executable:

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

2) Run installer with root privileges:

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

FOR APPLE DEVICES

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

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

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

   $ chmod +x {$installation file$}

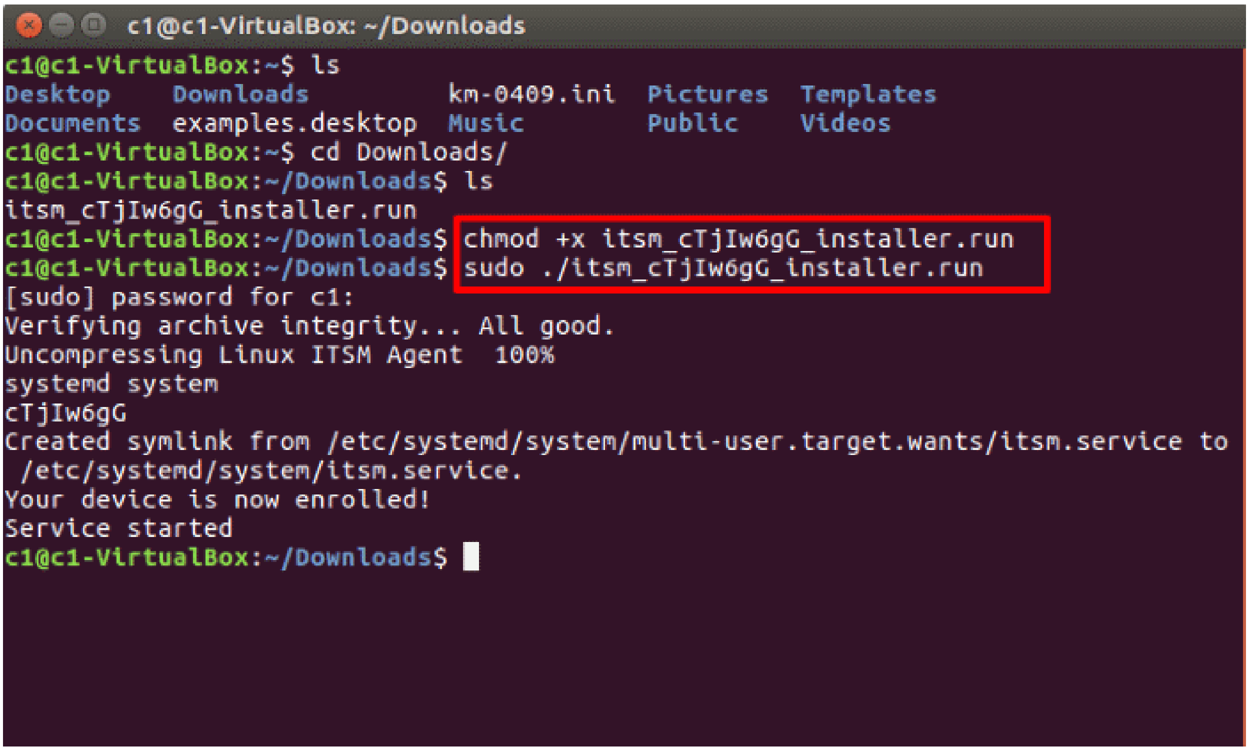
2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjIw6gG_installer.run

sudo./itsm_cTjIw6gG_installer.run



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

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

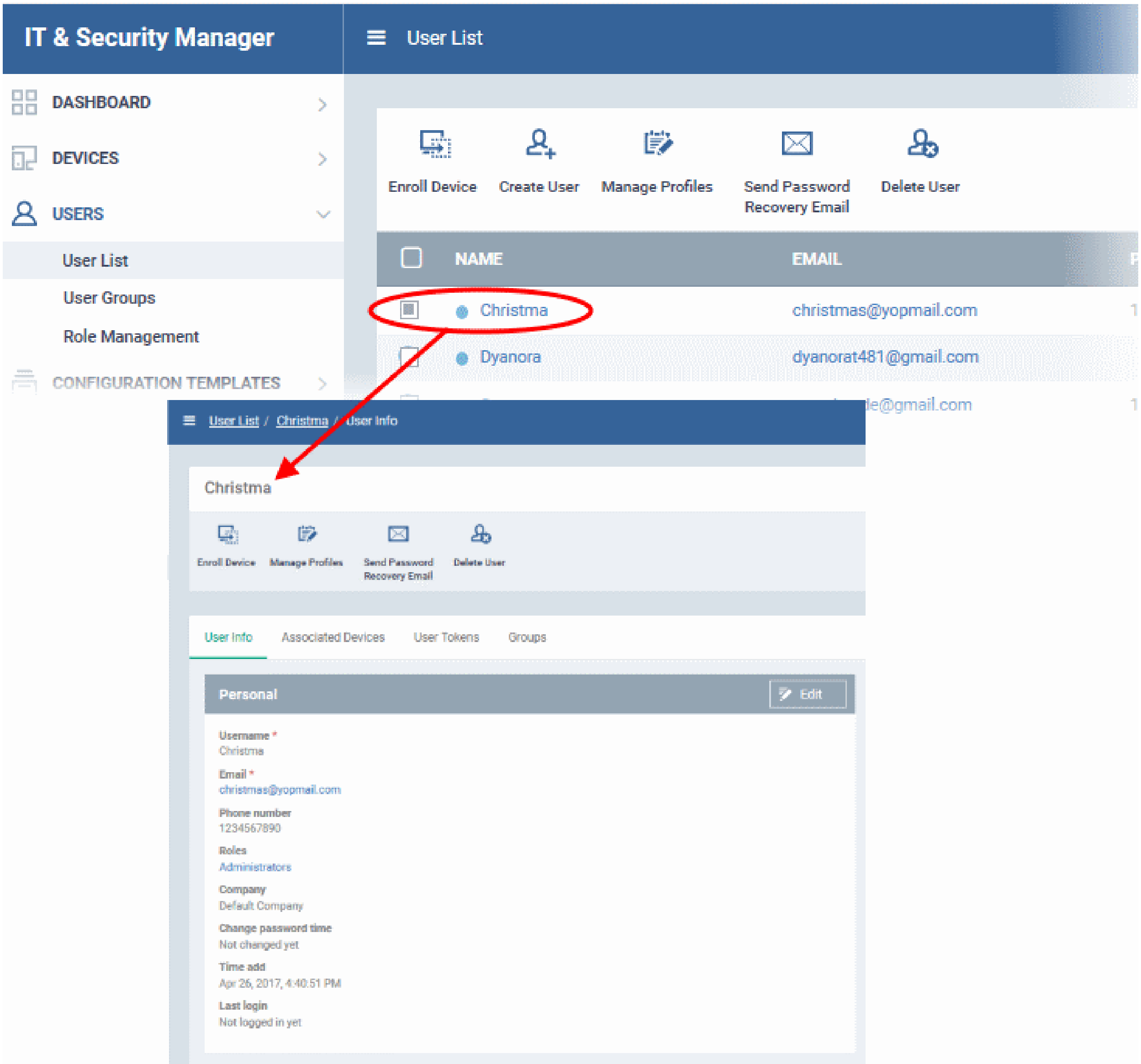
4.1.3. View User Details

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:



Username *
Christma

Email *
christmas@yopmail.com

Phone number
1234567890

Roles
Administrators

Company
Default Company

Change password time
Not changed yet

Time add
Apr 26, 2017, 4:40:51 PM

Last login
Not logged in yet

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

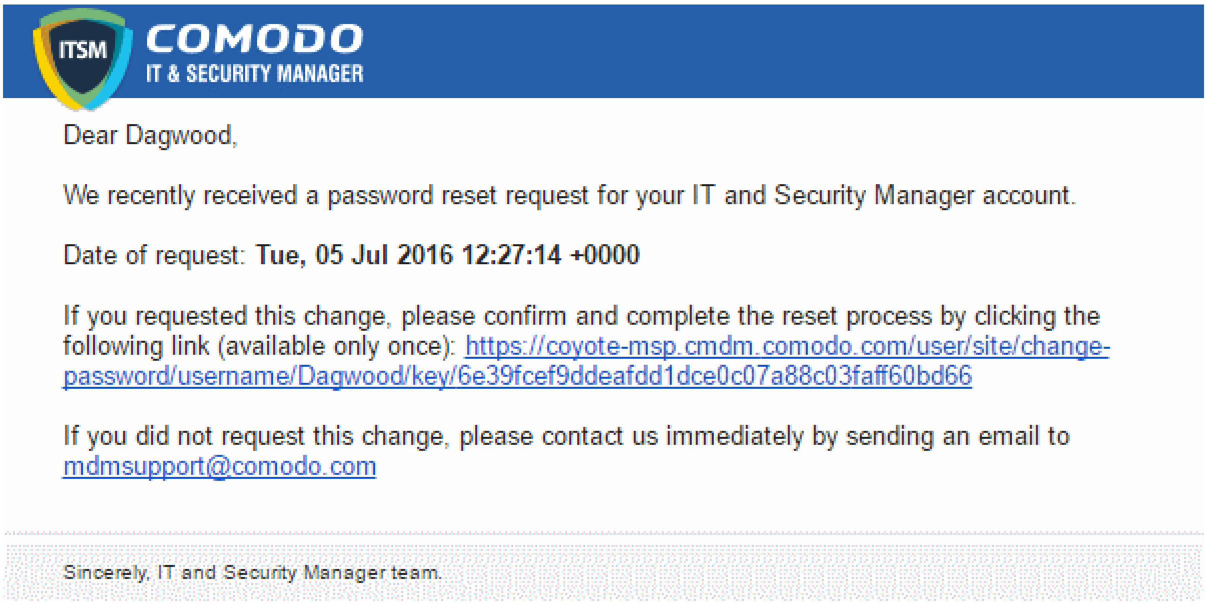
- Click 'Manage Profiles' at the top of the User Details interface

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:



Dear Dagwood,

We recently received a password reset request for your IT and Security Manager account.

Date of request: **Tue, 05 Jul 2016 12:27:14 +0000**

If you requested this change, please confirm and complete the reset process by clicking the following link (available only once): https://coyote-msp.cmdm.comodo.com/user/site/change-password/username/Dagwood/key/6e39fcef9ddeafdd1dce0c07a88c03faff60bd66

If you did not request this change, please contact us immediately by sending an email to mdmsupport@comodo.com

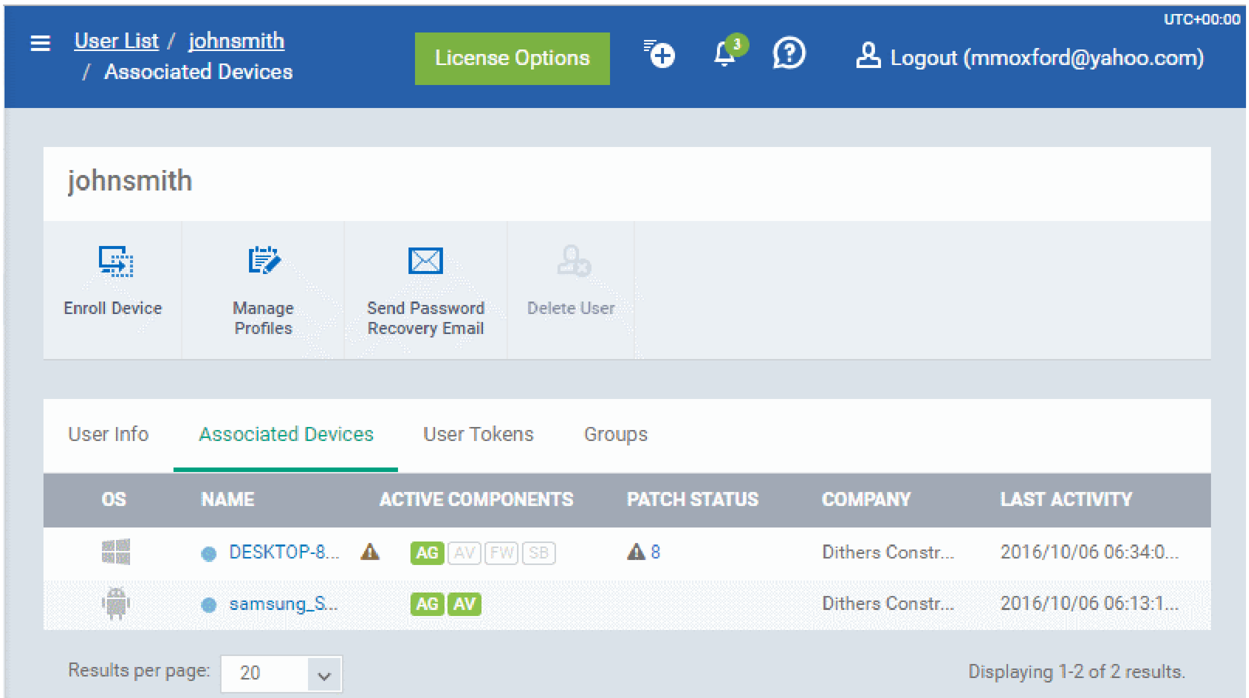
Sincerely, IT and Security Manager team.

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:



UTC+00:00

User List / johnsmith / Associated Devices

License Options

Logout (mmoxford@yahoo.com)

johnsmith

Enroll Device | Manage Profiles | Send Password Recovery Email | Delete User

User Info | Associated Devices | User Tokens | Groups

OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	LAST ACTIVITY
	DESKTOP-8... ⚠	AG AV FW SB	⚠ 8	Dithers Constr...	2016/10/06 06:34:0...
	samsung_S...	AG AV		Dithers Constr...	2016/10/06 06:13:1...

Results per page: 20

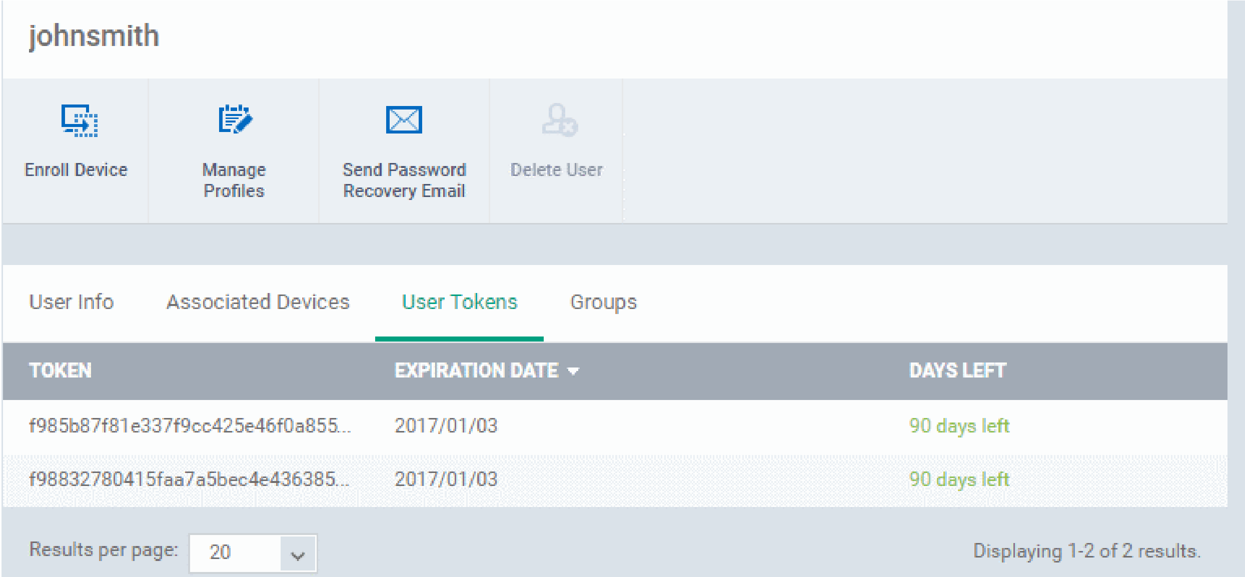
Displaying 1-2 of 2 results.

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:



johnsmith

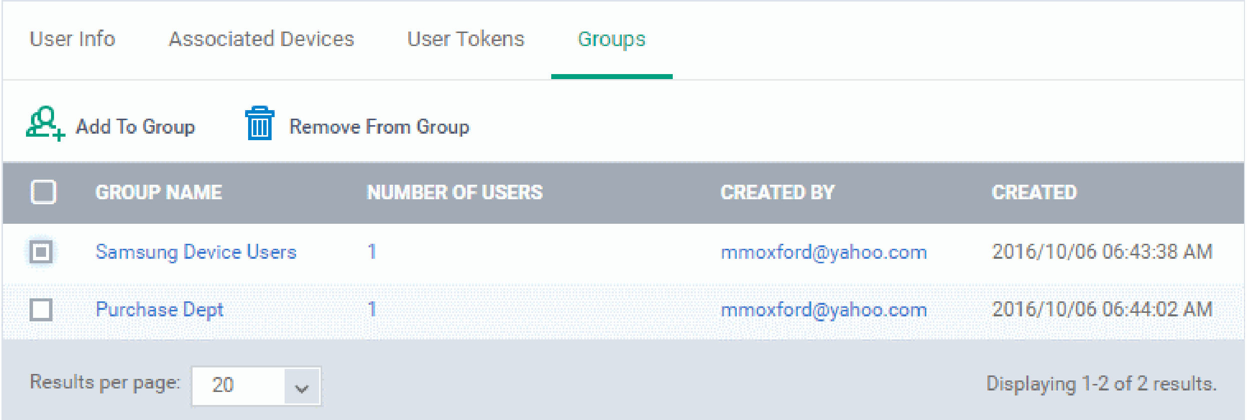
TOKEN	EXPIRATION DATE	DAYS LEFT
f985b87f81e337f9cc425e46f0a855...	2017/01/03	90 days left
f98832780415faa7a5bec4e436385...	2017/01/03	90 days left

Results per page: 20 Displaying 1-2 of 2 results.

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:



□	GROUP NAME	NUMBER OF USERS	CREATED BY	CREATED
▣	Samsung Device Users	1	mmoxford@yahoo.com	2016/10/06 06:43:38 AM
□	Purchase Dept	1	mmoxford@yahoo.com	2016/10/06 06:44:02 AM

Results per page: 20 Displaying 1-2 of 2 results.

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. Update 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.

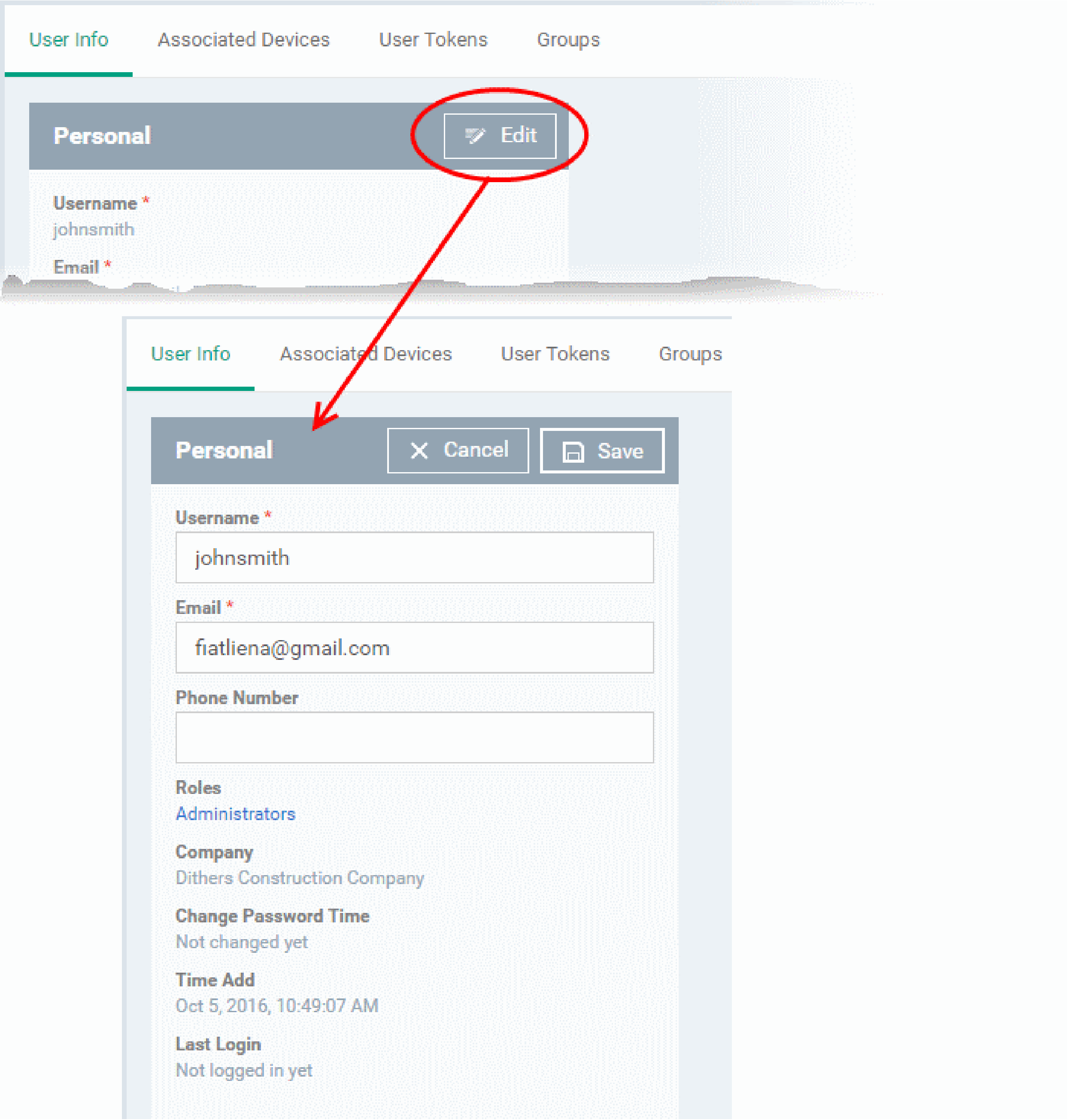
Note: The 'Edit' option is not available for users that were added via the C1 management portal. Those users must be edited in the C1 interface. All changes will be reflected in the ITSM interface.

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 Edit at the top right



Username *
johnsmith

Email *
fiatliena@gmail.com

Phone Number

Roles
Administrators

Company
Dithers Construction Company

Change Password Time
Not changed yet

Time Add
Oct 5, 2016, 10:49:07 AM

Last Login
Not logged in yet

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

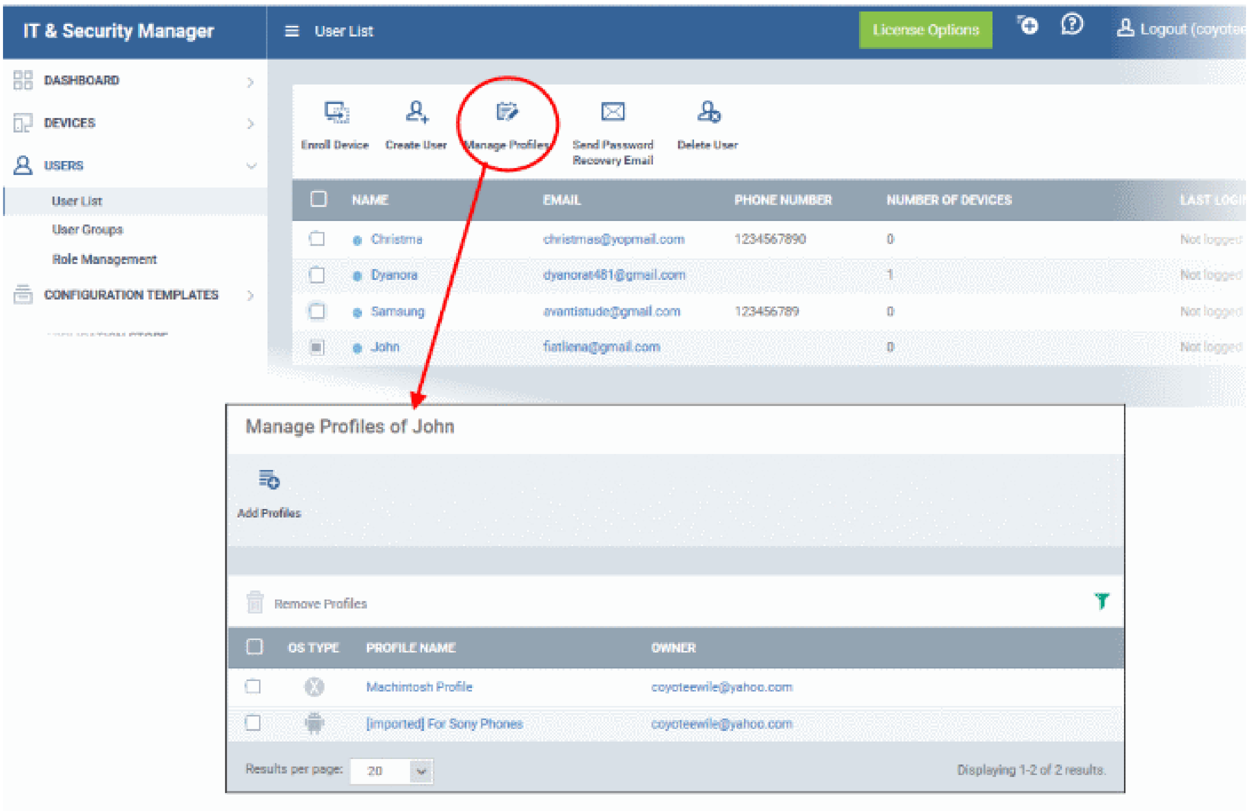
The role assigned to the user is displayed under 'Roles'. Clicking the role name allows you to change the role if required. Refer to the section '**Managing Roles Assigned to a User**' for more details.

4.1.4. Assign 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)



☐	NAME	EMAIL	PHONE NUMBER	NUMBER OF DEVICES	LAST LOGI
☐	Christma	christmas@yopmail.com	1234567890	0	Not logged
☐	Dyanora	dyanora481@gmail.com		1	Not logged
☐	Samsung	avantistude@gmail.com	123456789	0	Not logged
☑	John	fiatliena@gmail.com		0	Not logged

☐	OS TYPE	PROFILE NAME	OWNER
☐		Machintosh Profile	coyoteewile@yahoo.com
☐		[imported] For Sony Phones	coyoteewile@yahoo.com

Results per page: 20

Displaying 1-2 of 2 results.

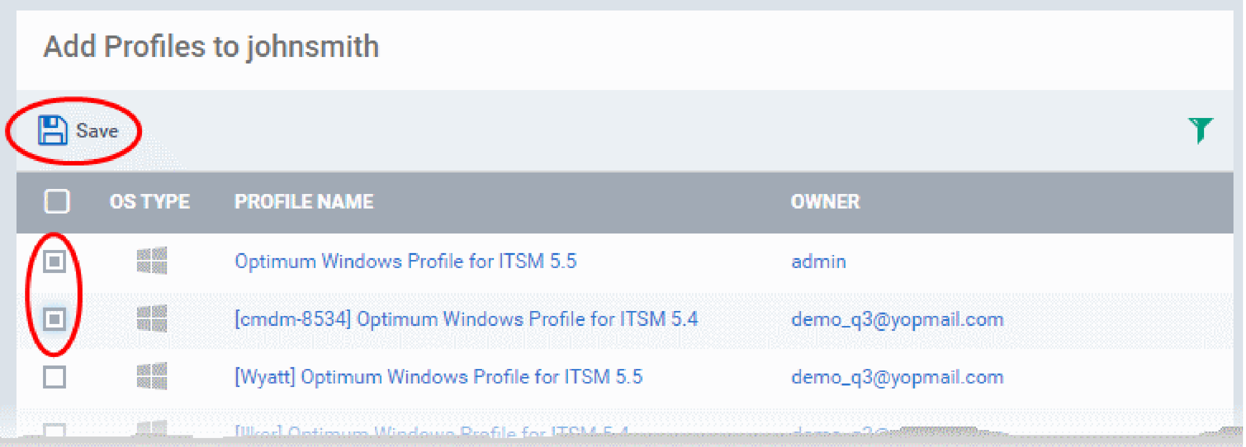
- Click 'Manage Profiles'.

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'



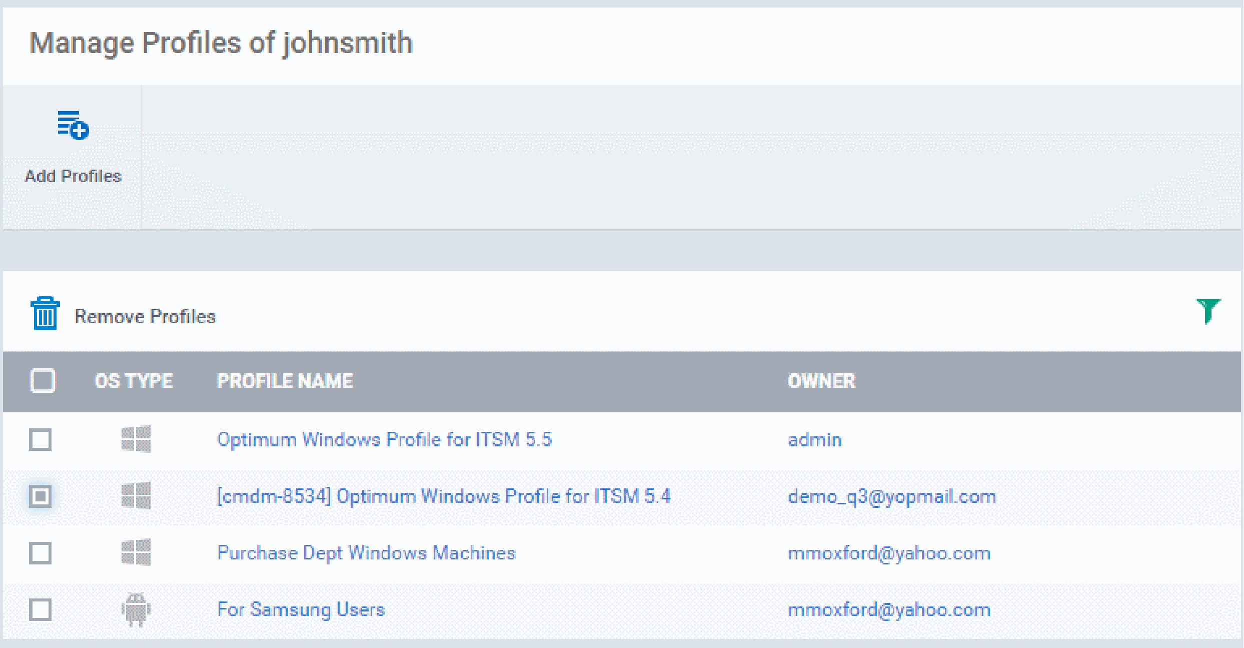
Add Profiles to johnsmith

□	OS TYPE	PROFILE NAME	OWNER
☑		Optimum Windows Profile for ITSM 5.5	admin
☑		[cmdm-8534] Optimum Windows Profile for ITSM 5.4	demo_q3@yopmail.com
□		[Wyatt] Optimum Windows Profile for ITSM 5.5	demo_q3@yopmail.com
□		[Ilker] Optimum Windows Profile for ITSM 5.4	demo_q3@

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.

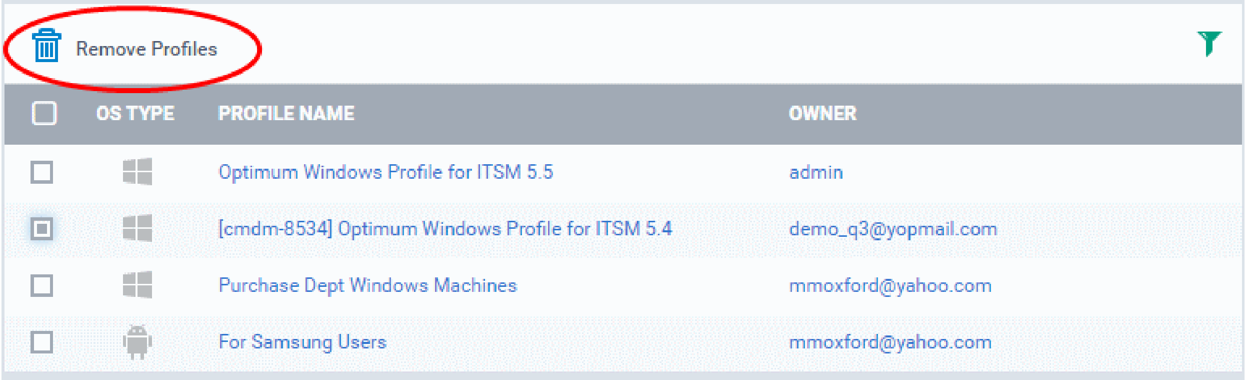


Manage Profiles of johnsmith

□	OS TYPE	PROFILE NAME	OWNER
□		Optimum Windows Profile for ITSM 5.5	admin
☑		[cmdm-8534] Optimum Windows Profile for ITSM 5.4	demo_q3@yopmail.com
□		Purchase Dept Windows Machines	mmoxford@yahoo.com
□		For Samsung Users	mmoxford@yahoo.com

To remove a profile

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



□	OS TYPE	PROFILE NAME	OWNER
□		Optimum Windows Profile for ITSM 5.5	admin
☒		[cmdm-8534] Optimum Windows Profile for ITSM 5.4	demo_q3@yopmail.com
□		Purchase Dept Windows Machines	mmoxford@yahoo.com
□		For Samsung Users	mmoxford@yahoo.com

The selected profile(s) will be removed.

4.1.5. Remove 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.

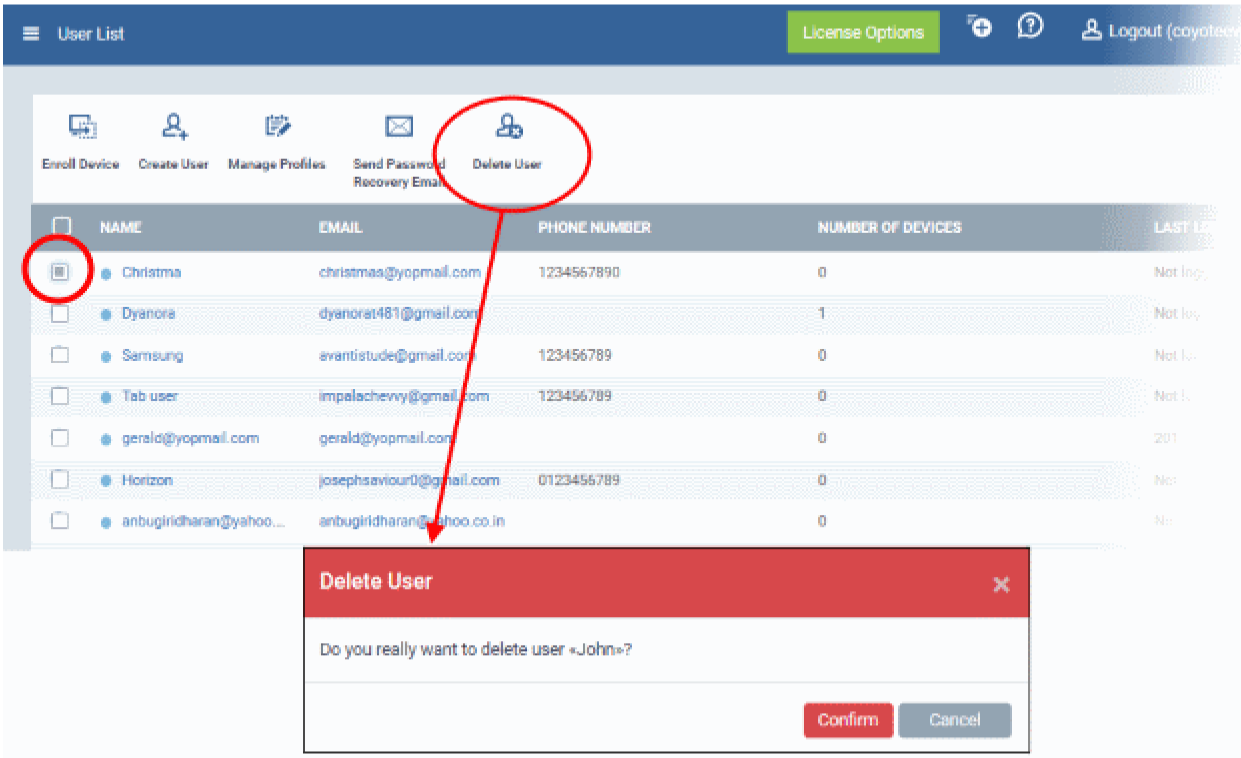
Note 1: Users added via the C1 management portal cannot be removed via the ITSM interface. They can be removed only from C1 and once removed they will be automatically deleted from the user list in ITSM.

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.



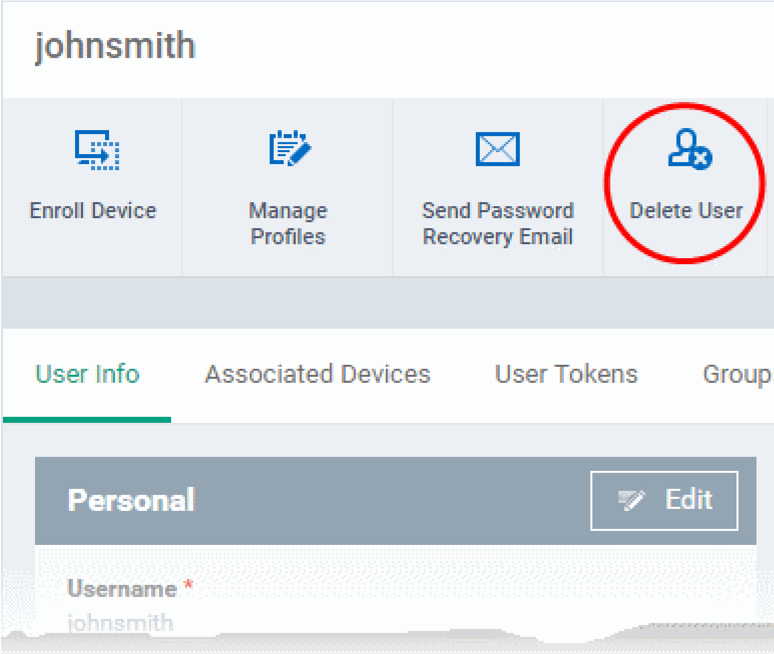
□	NAME	EMAIL	PHONE NUMBER	NUMBER OF DEVICES	LAST L
☒	Christma	christmas@yopmail.com	1234567890	0	Not log
□	Dyanora	dyanorat481@gmail.com		1	Not log
□	Samsung	avantistude@gmail.com	123456789	0	Not l...
□	Tab user	impalachevvy@gmail.com	123456789	0	Not l...
□	gerald@yopmail.com	gerald@yopmail.com		0	201
□	Horizon	josephsaviour0@gmail.com	0123456789	0	No
□	anbugiridharan@yahoo...	anbugiridharan@yahoo.co.in		0	No

Delete User ×

Do you really want to delete user «John»?

Confirm | Cancel

- Click 'Delete User' at the top



Username *
johnsmith

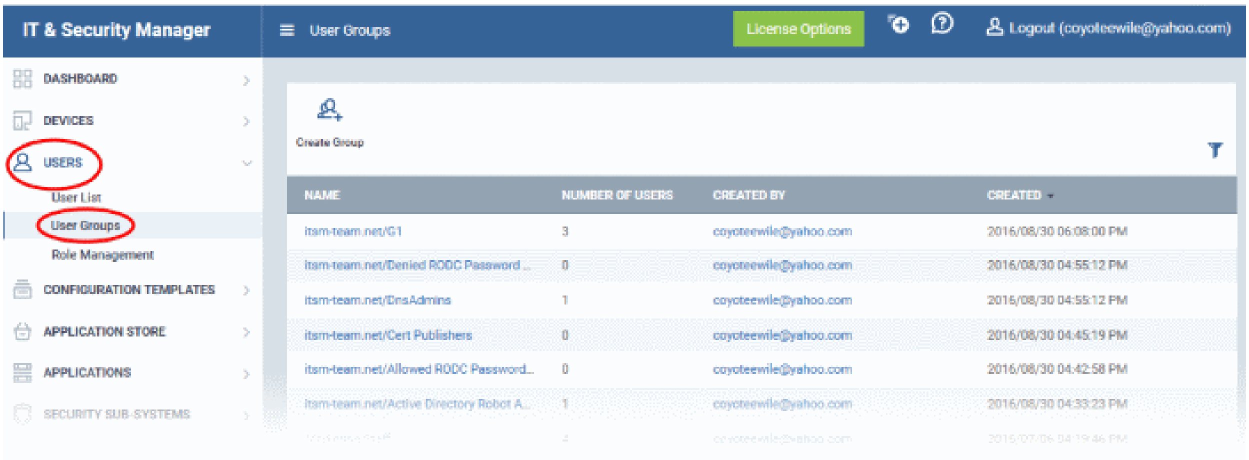
The user will be removed from ITSM.

4.2. Manage User Groups

- Comodo ITSM allows you to create logical groups of users to simplify and streamline user management. For example, users could be grouped according to existing corporate units ('Sales Dept.', 'Accounts Dept.') and/or by type of user.
- Once created, dedicated configuration profiles can be applied to each user group as required. See **Configuration Profiles** for more help with profiles.
- You can also import users/user groups from Active Directory using LDAP. Imported users will be placed into ITSM with the same group structure. ITSM will periodically synchronize with AD to ensure any changes to AD users are mirrored in the ITSM database. See **Import User Groups from LDAP** for more details.

The 'User Groups' interface lists all existing groups and allows you to add new groups and edit groups. You can also assign profiles to groups from this interface.

- Click 'Users' > 'User Groups' to open the groups interface.

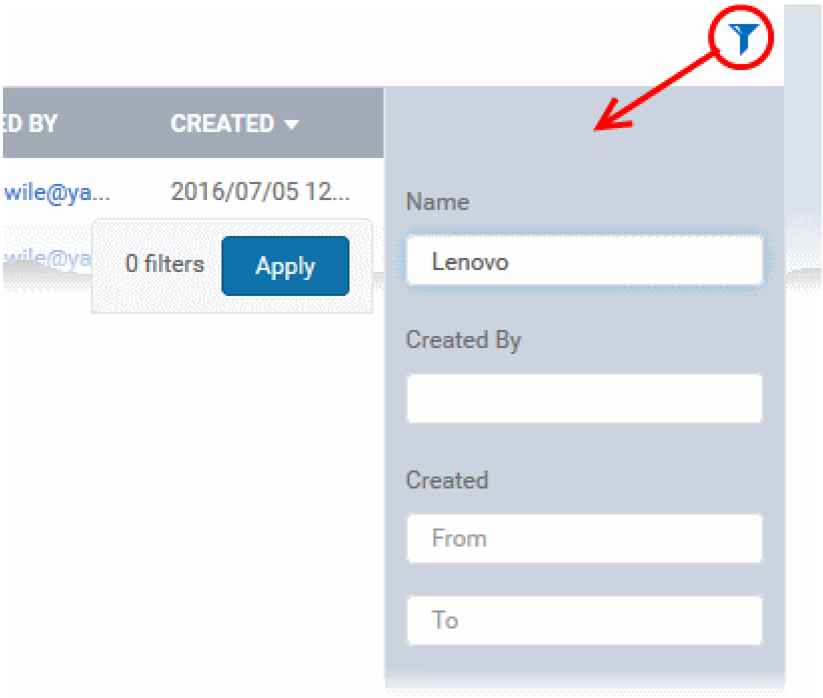


NAME	NUMBER OF USERS	CREATED BY	CREATED
itsm-team.net/G1	3	coyoteewile@yahoo.com	2016/08/30 06:08:00 PM
itsm-team.net/Denied RODC Password ...	0	coyoteewile@yahoo.com	2016/08/30 04:55:12 PM
itsm-team.net/DnsAdmins	1	coyoteewile@yahoo.com	2016/08/30 04:55:12 PM
itsm-team.net/Cert Publishers	0	coyoteewile@yahoo.com	2016/08/30 04:45:19 PM
itsm-team.net/Allowed RODC Password...	0	coyoteewile@yahoo.com	2016/08/30 04:42:58 PM
itsm-team.net/Active Directory Robot A...	1	coyoteewile@yahoo.com	2016/08/30 04:33:23 PM
[illegible]	4	coyoteewile@yahoo.com	2016/07/06 04:19:46 PM

User Groups - Column Descriptions	
Column Heading	**Description**
Name	The name assigned to the user group by the administrator. Click the name of a group to view members. The group details interface allows you to add and manage group members. See **Editing a User Group** for more details.
Number of Users	Shows how many users are in the group.
Created By	Name of the administrator that created the group. Click the administrator name to view full admin details. See **Viewing the details of a User** for more information.
Created	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

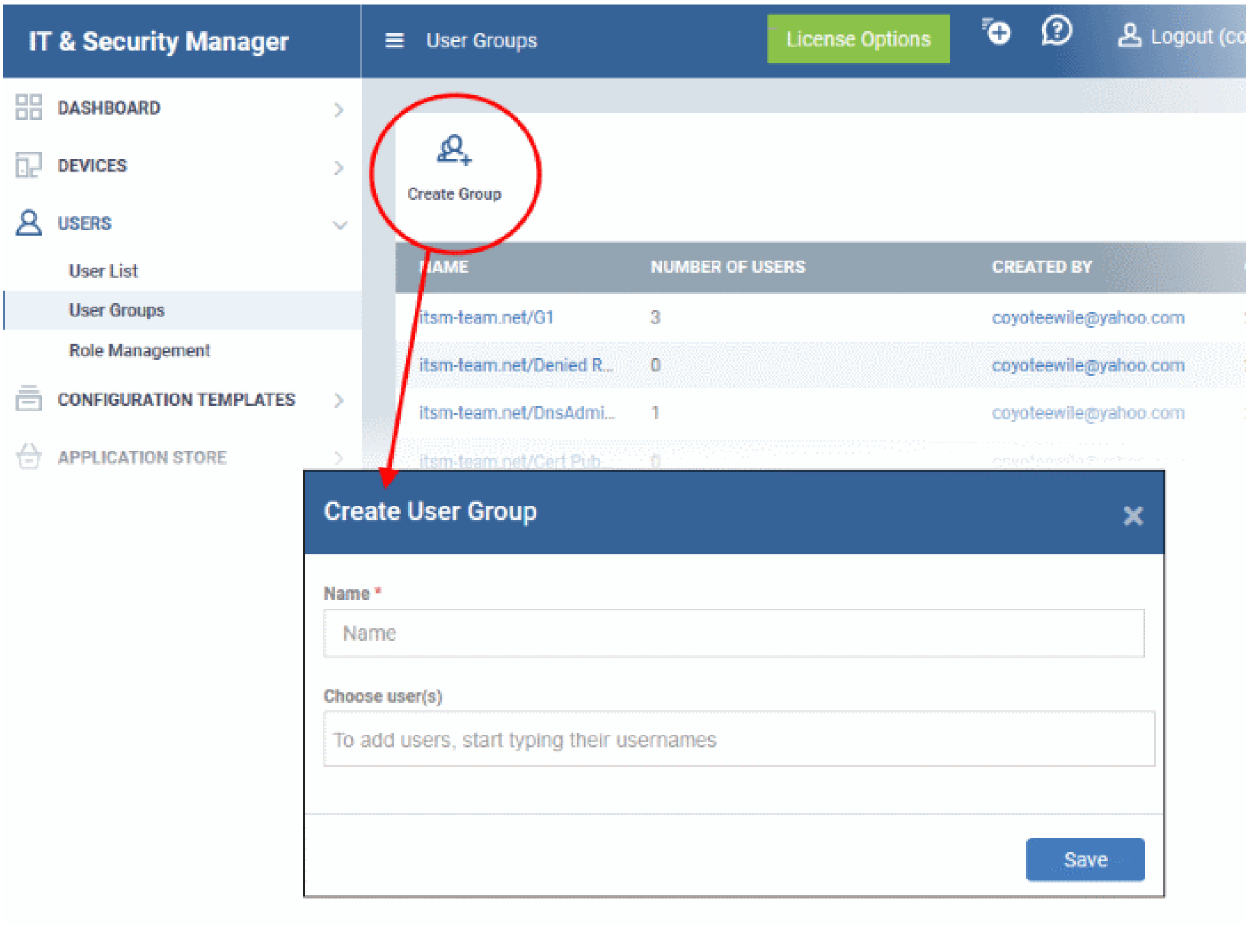
4.2.1. Create a New User Group

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.



NAME	NUMBER OF USERS	CREATED BY
itsm-team.net/G1	3	coyoteewile@yahoo.com
itsm-team.net/Denied R...	0	coyoteewile@yahoo.com
itsm-team.net/DnsAdmi...	1	coyoteewile@yahoo.com
itsm-team.net/Cert Pub...	0	coyoteewile@yahoo.com

'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

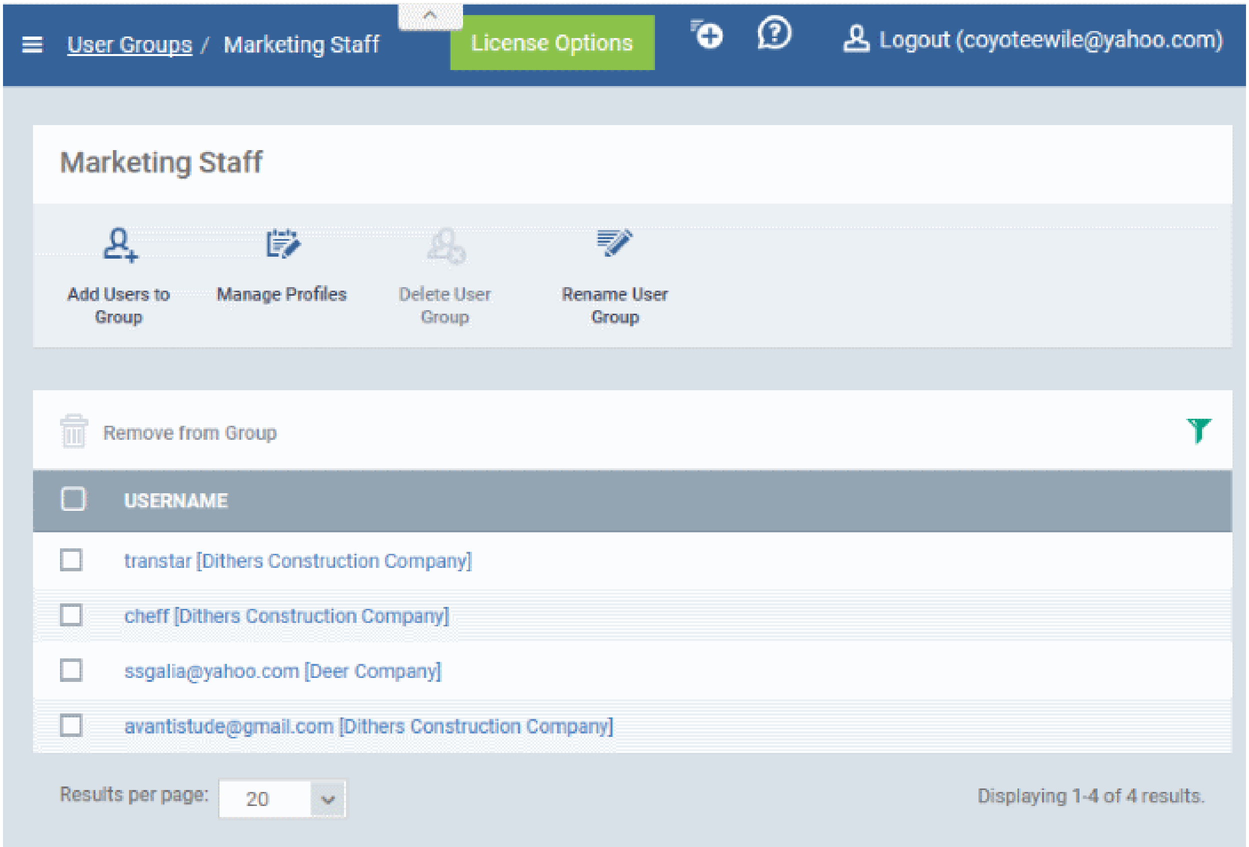
'Create User Group' dialog - Table of Parameters		
		drop-down. Repeat the process for adding more number of users. • Note: You can add users at a later stage too. See the following section **Editing a User Group** for more details.

- 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.



□	USERNAME
□	transtar [Dithers Construction Company]
□	cheff [Dithers Construction Company]
□	ssgalia@yahoo.com [Deer Company]
□	avantistude@gmail.com [Dithers Construction Company]

Results per page: 20

Displaying 1-4 of 4 results.

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.

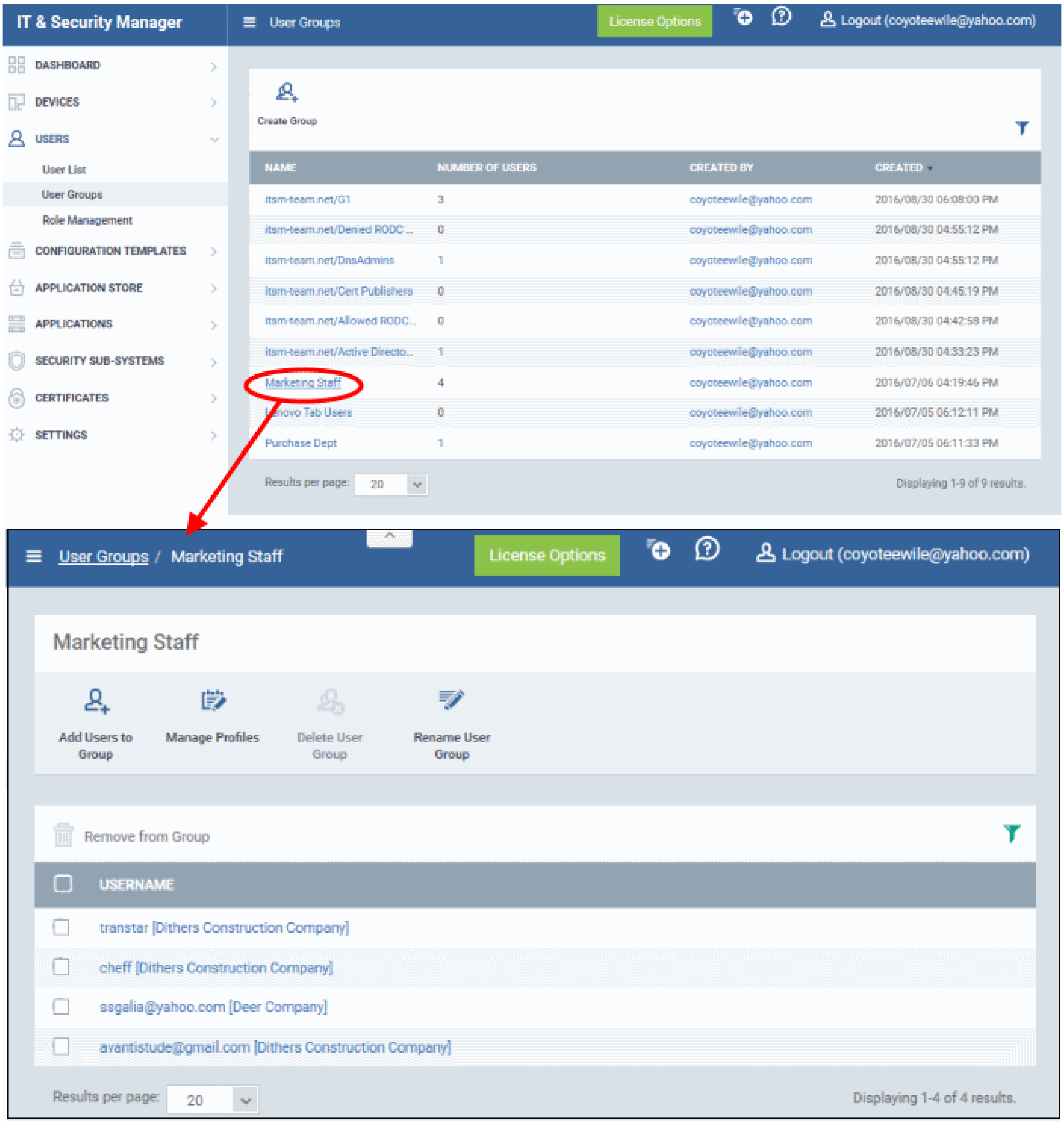
4.2.2. Edit a User Group

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.



NAME	NUMBER OF USERS	CREATED BY	CREATED
itsm-team.net/G1	3	coyoteewile@yahoo.com	2016/08/30 06:08:00 PM
itsm-team.net/Denied RODC ...	0	coyoteewile@yahoo.com	2016/08/30 04:55:12 PM
itsm-team.net/DnsAdmins	1	coyoteewile@yahoo.com	2016/08/30 04:55:12 PM
itsm-team.net/Cert Publishers	0	coyoteewile@yahoo.com	2016/08/30 04:45:19 PM
itsm-team.net/Allowed RODC...	0	coyoteewile@yahoo.com	2016/08/30 04:42:58 PM
itsm-team.net/Active Directo...	1	coyoteewile@yahoo.com	2016/08/30 04:33:23 PM
Marketing Staff	4	coyoteewile@yahoo.com	2016/07/06 04:19:46 PM
Lenovo Tab Users	0	coyoteewile@yahoo.com	2016/07/05 06:12:11 PM
Purchase Dept	1	coyoteewile@yahoo.com	2016/07/05 06:11:33 PM

Results per page: 20 Displaying 1-9 of 9 results.

□	USERNAME
□	transtar [Dithers Construction Company]
□	cheff [Dithers Construction Company]
□	ssgalia@yahoo.com [Deer Company]
□	avantistude@gmail.com [Dithers Construction Company]

Results per page: 20 Displaying 1-4 of 4 results.

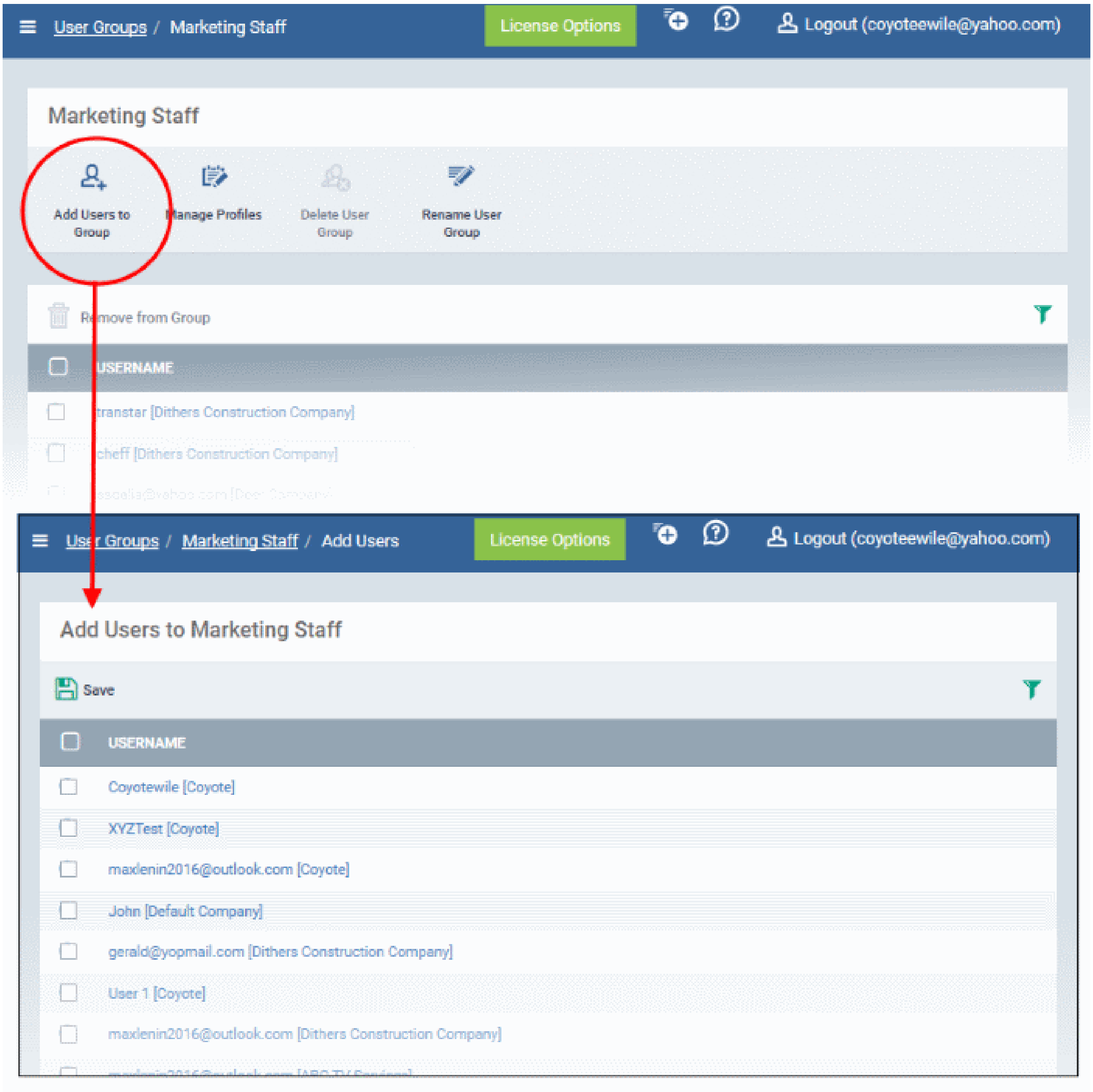
The user group details interface will open with the list of users in the group and allows you to:.

- 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.



User Groups / Marketing Staff

License Options

Logout (coyoteewile@yahoo.com)

Marketing Staff

Add Users to Group | Manage Profiles | Delete User Group | Rename User Group

Remove from Group

□	USERNAME
□	transtar [Dithers Construction Company]
□	cheff [Dithers Construction Company]

User Groups / Marketing Staff / Add Users

License Options

Logout (coyoteewile@yahoo.com)

Add Users to Marketing Staff

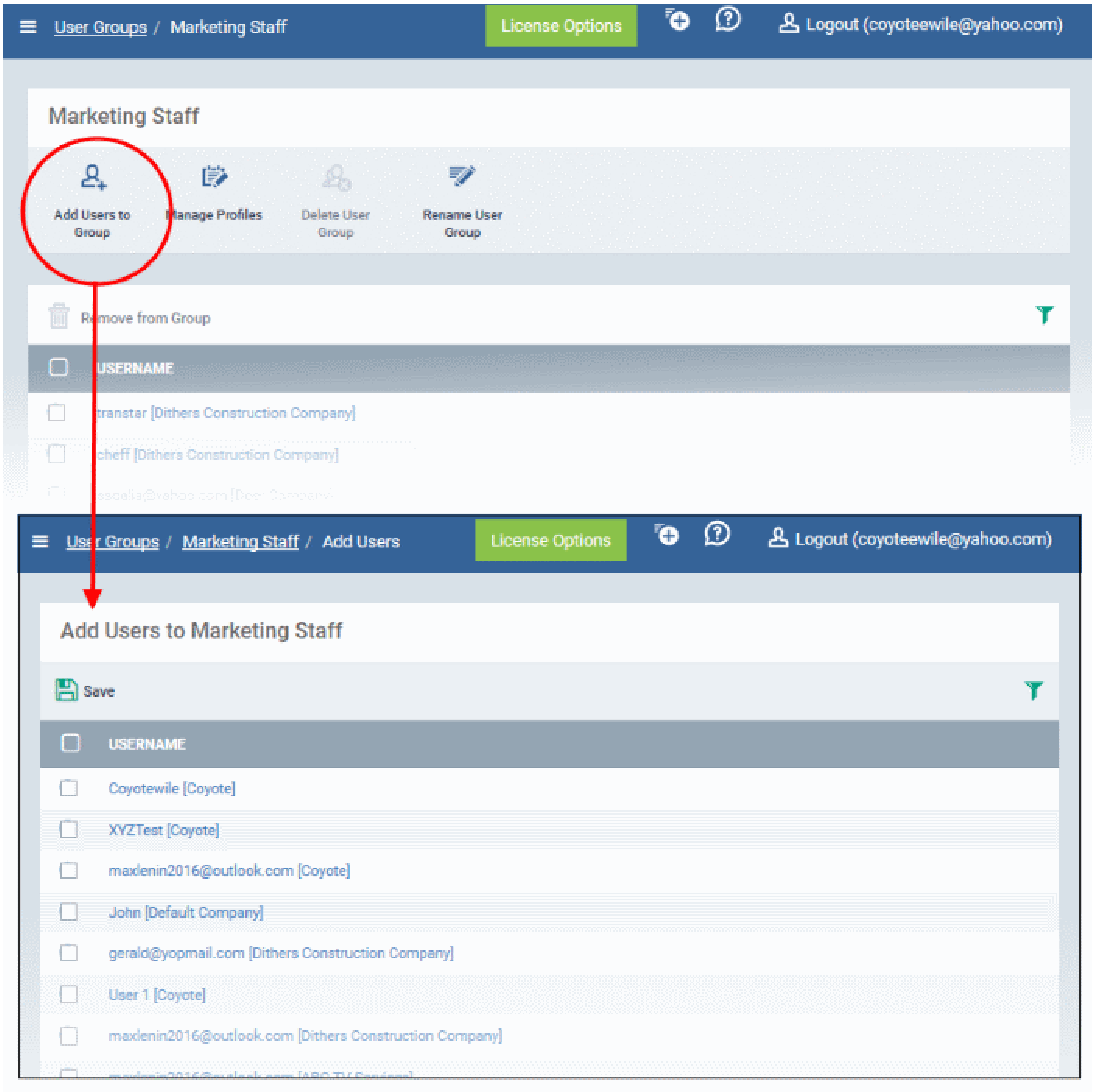
Save

□	USERNAME
□	Coyotewile [Coyote]
□	XYZTest [Coyote]
□	maxlenin2016@outlook.com [Coyote]
□	John [Default Company]
□	gerald@yopmail.com [Dithers Construction Company]
□	User 1 [Coyote]
□	maxlenin2016@outlook.com [Dithers Construction Company]

- 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).

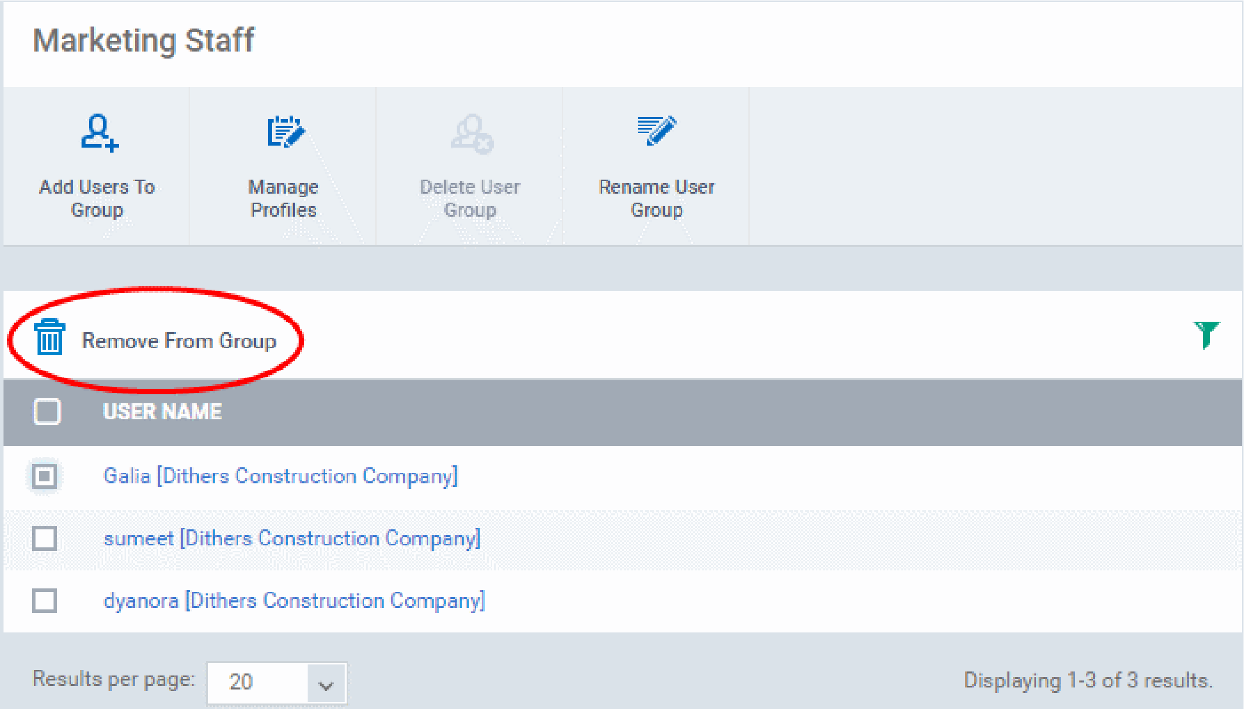
To remove a user from the group


User Groups / Marketing Staff
License Options
Logout (coyoteewile@yahoo.com)
Marketing Staff
Add Users to Group
Manage Profiles
Delete User Group
Rename User Group
Remove from Group
User Groups / Marketing Staff / Add Users
License Options
Logout (coyoteewile@yahoo.com)
Add Users to Marketing Staff
Save

☐	USERNAME
☐	transtar [Dithers Construction Company]
☐	cheff [Dithers Construction Company]

☐	USERNAME
☐	Coyotewile [Coyote]
☐	XYZTest [Coyote]
☐	maxlenin2016@outlook.com [Coyote]
☐	John [Default Company]
☐	gerald@yopmail.com [Dithers Construction Company]
☐	User 1 [Coyote]
☐	maxlenin2016@outlook.com [Dithers Construction Company]

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



☐	USER NAME
▣	Galia [Dithers Construction Company]
☐	sumeet [Dithers Construction Company]
☐	dyanora [Dithers Construction Company]

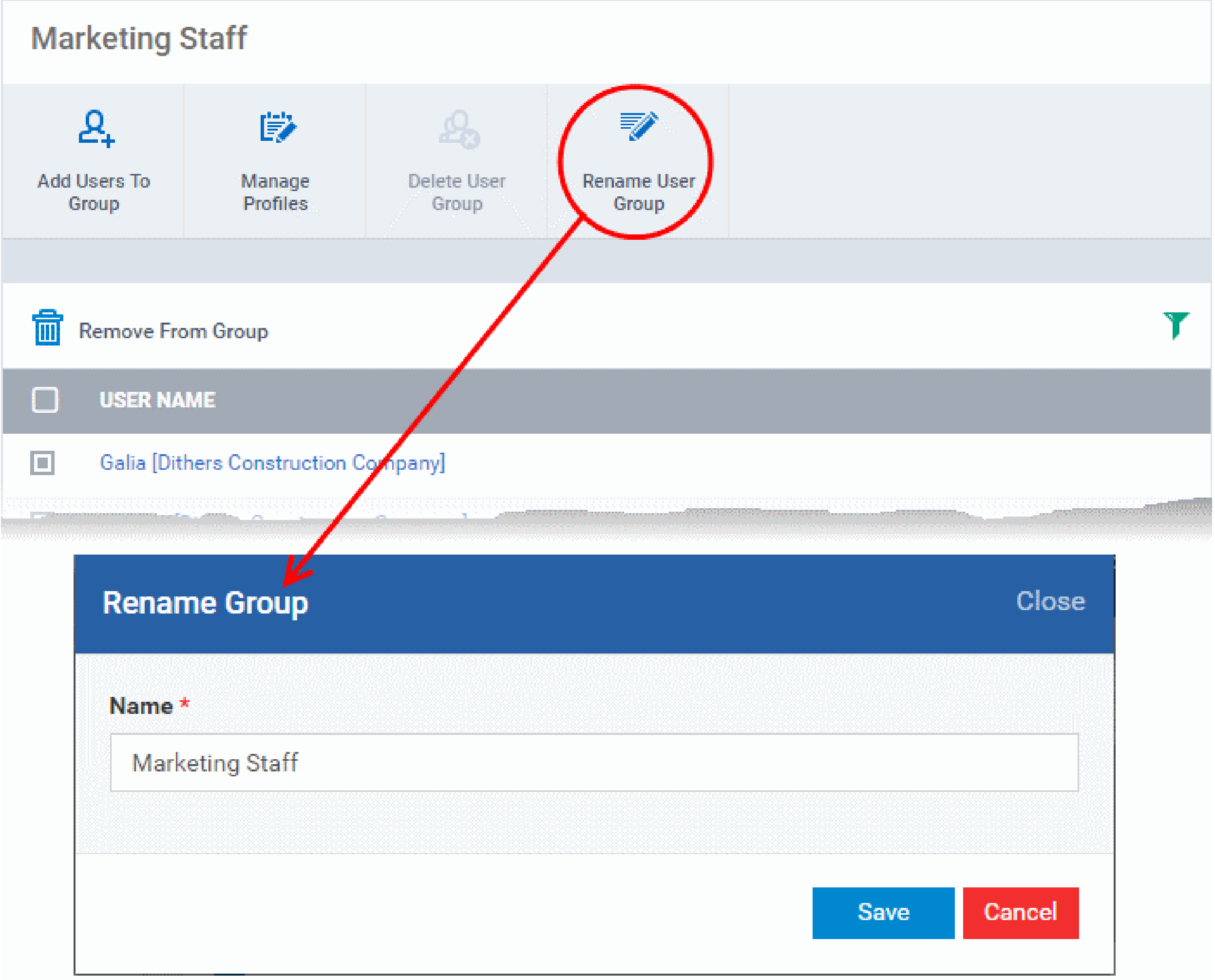
Displaying 1-3 of 3 results.

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. Assign 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.

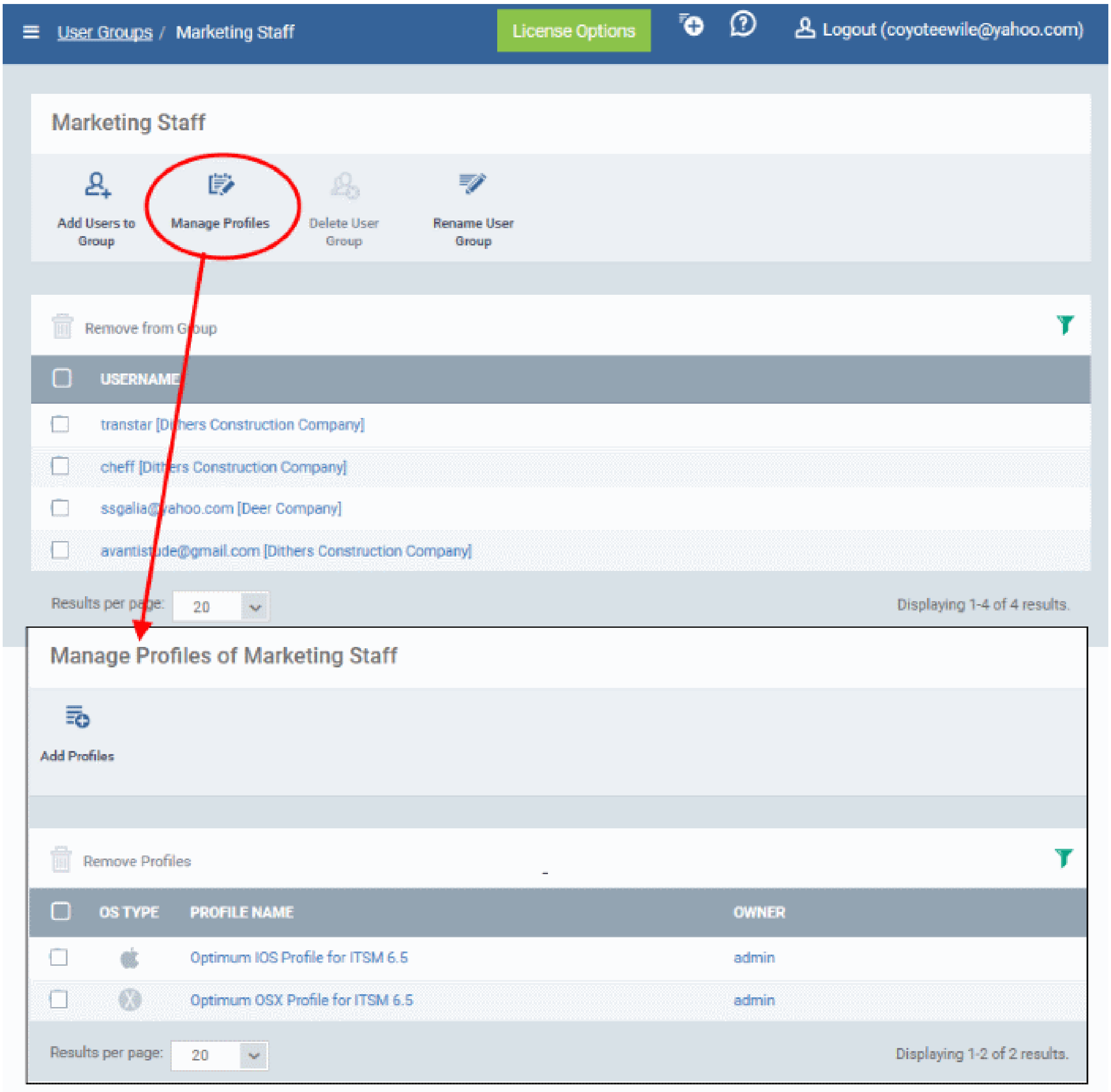
For more details on profiles, refer to the chapter **Configuration Profiles**.

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.



Marketing Staff

☐	USERNAME
☐	transtar [Dithers Construction Company]
☐	cheff [Dithers Construction Company]
☐	ssgalia@yahoo.com [Deer Company]
☐	avantistude@gmail.com [Dithers Construction Company]

Results per page: 20 Displaying 1-4 of 4 results.

Manage Profiles of Marketing Staff

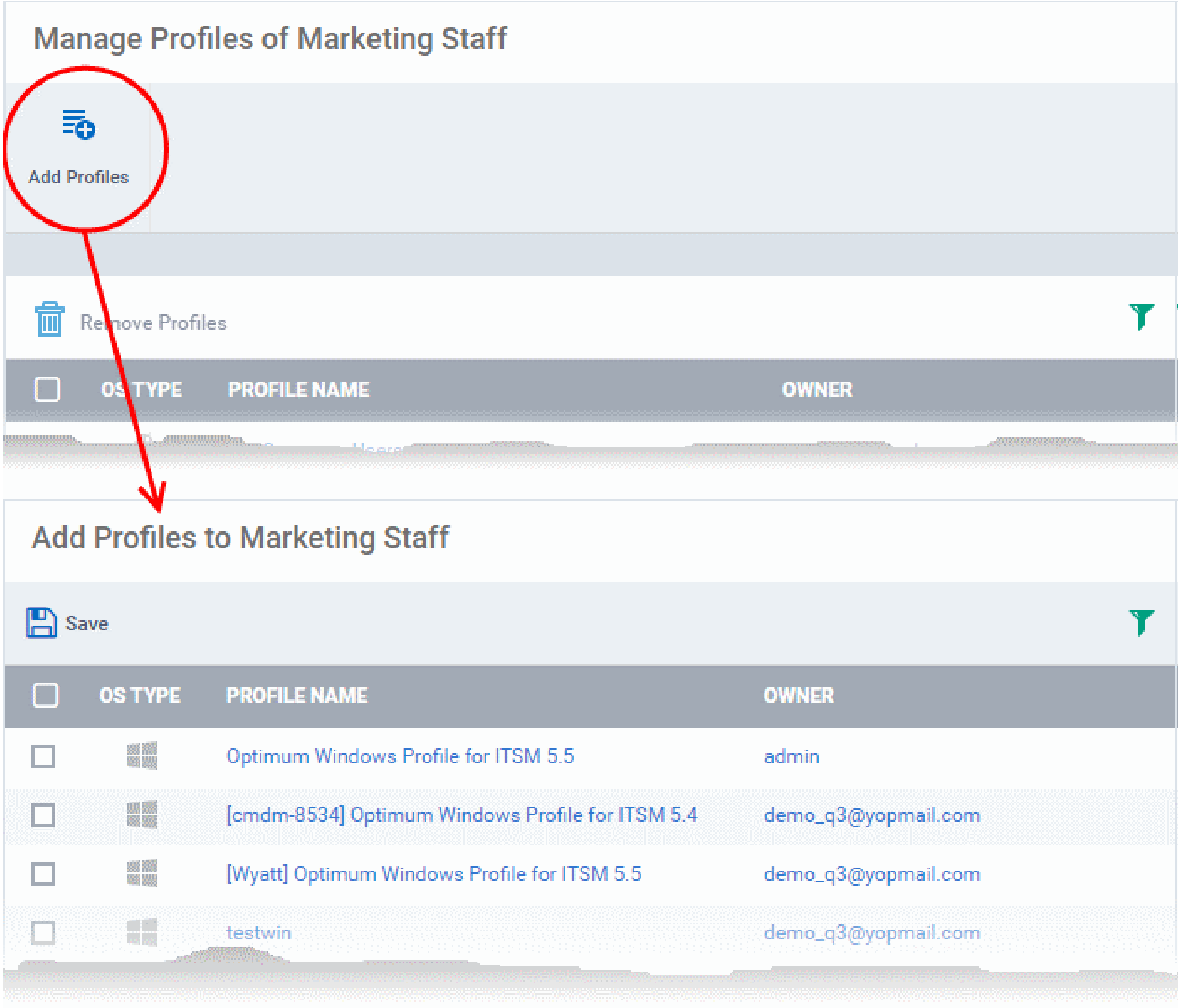
☐	OS TYPE	PROFILE NAME	OWNER
☐		Optimum IOS Profile for ITSM 6.5	admin
☐	X	Optimum OSX Profile for ITSM 6.5	admin

Results per page: 20 Displaying 1-2 of 2 results.

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

To add a new profile

- Click 'Add Profiles'



Manage Profiles of Marketing Staff

□	OS TYPE	PROFILE NAME	OWNER

Add Profiles to Marketing Staff

□	OS TYPE	PROFILE NAME	OWNER
□	⊞	Optimum Windows Profile for ITSM 5.5	admin
□	⊞	[cmdm-8534] Optimum Windows Profile for ITSM 5.4	demo_q3@yopmail.com
□	⊞	[Wyatt] Optimum Windows Profile for ITSM 5.5	demo_q3@yopmail.com
□	⊞	testwin	demo_q3@yopmail.com

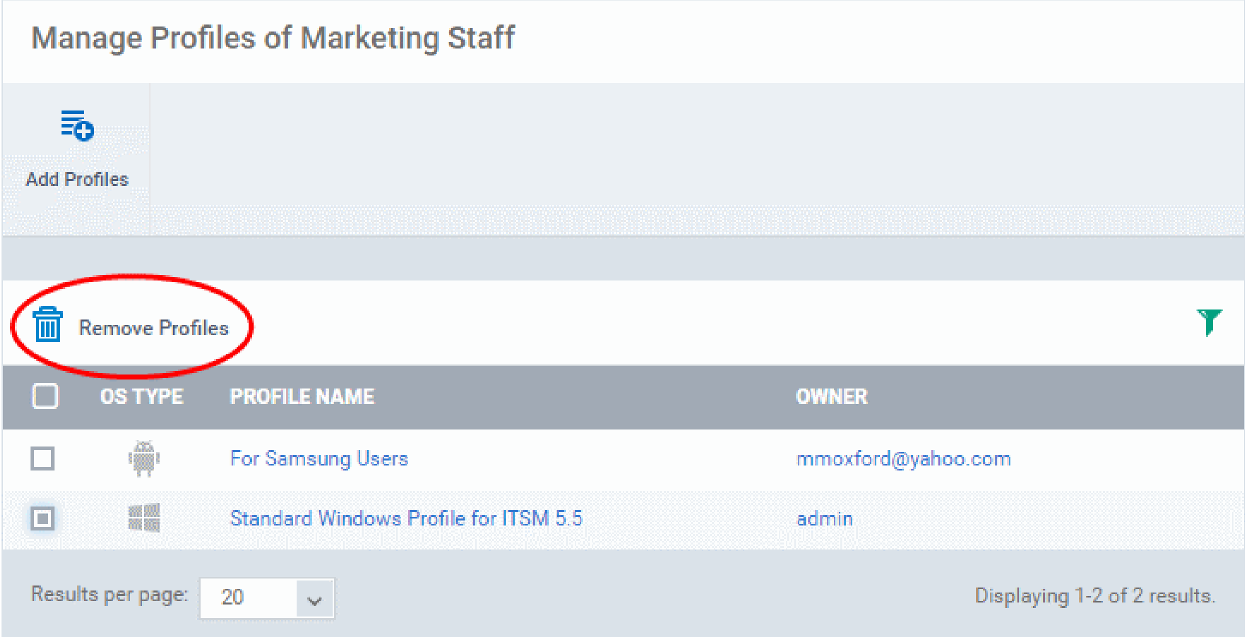
A list of all configuration profiles, available in ITSM, excluding those already applied to the group will be displayed.

- 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'


Manage Profiles of Marketing Staff
Add Profiles
Remove Profiles

□	OS TYPE	PROFILE NAME	OWNER
□		For Samsung Users	mmoxford@yahoo.com
☒		Standard Windows Profile for ITSM 5.5	admin

Results per page: 20
Displaying 1-2 of 2 results.

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

4.2.4. Remove 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.

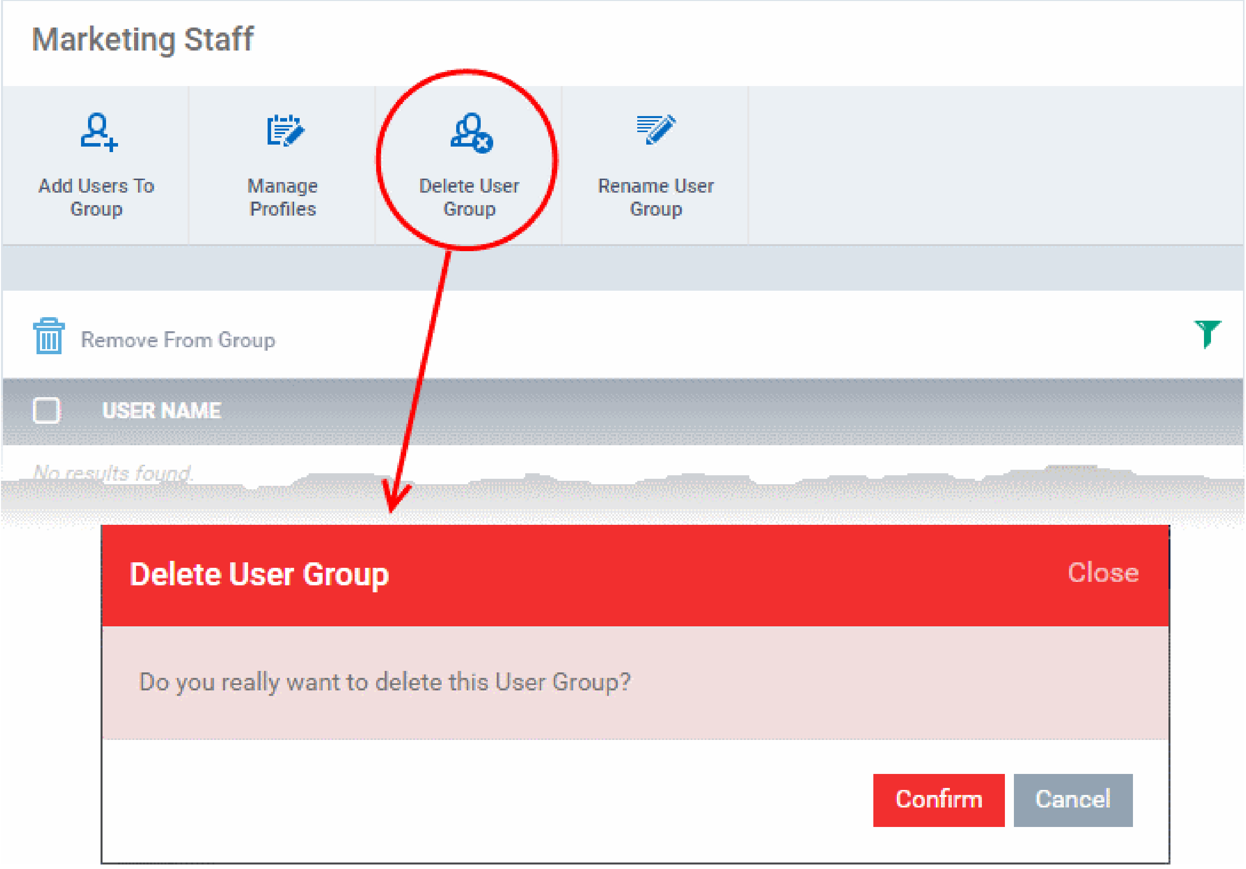
Note: Only Groups that do not contain any members in it can be removed. Ensure that all users are removed from the group before removing it. Refer to the **explanation of removing users from a group** in the section **Editing a User Group** for more details.

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.



Delete User Group

Close

Do you really want to delete this User Group?

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

4.3. Configure Role Based Access Control for Users

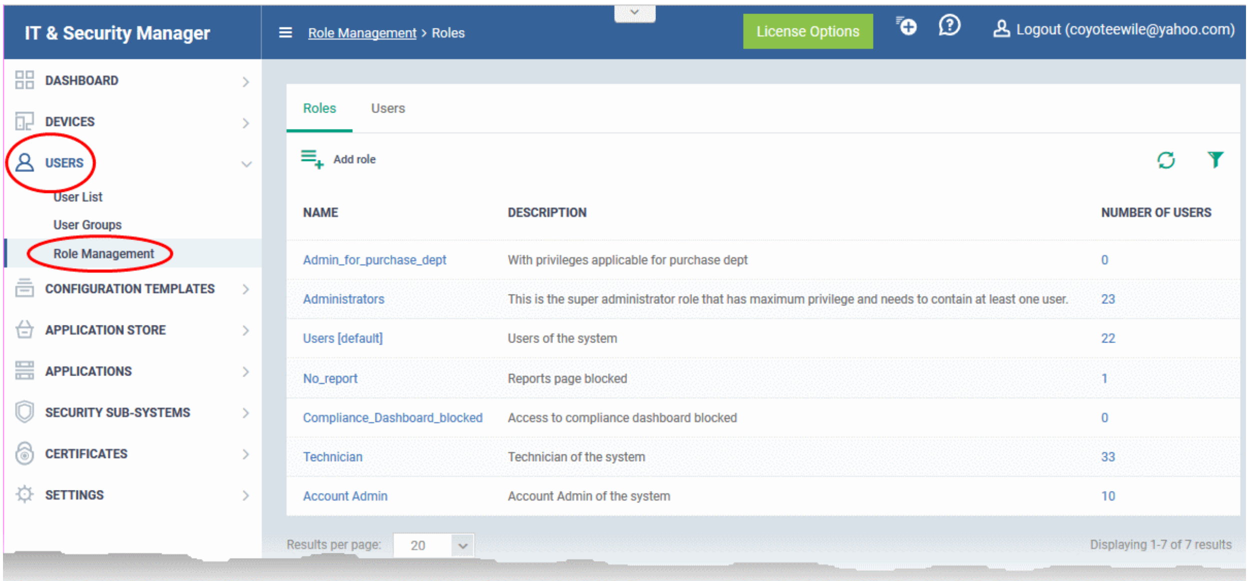
- Click 'Users' > 'Role Management' to open the 'Role Management' interface
- User privileges depend on the roles assigned to them. Administrators can create different roles with different access privileges and assign them to users as required. A single user can be assigned to any number of roles.
- All staff created in the C1 interface will be available for selection for 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 restrict access to selected companies and device groups for a role by defining the access scope. Staff members can manage devices belonging only to the companies/device groups allowed as per their role.

There are two tabs in the role management interface:

- 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 you to create and manage user roles.
- Each role defines a staff member's rights to access ITSM modules and to manage users/devices belonging to different companies. You can restrict a role to manage specific companies and specific device groups.
- ITSM ships with four roles, 'Account Admin', 'Administrators', 'Technician' and 'Users'.
- The 'Account Admin' role can be viewed but not edited. The permissions in the other three roles can be modified. You can also create custom roles according to your requirements.



NAME	DESCRIPTION	NUMBER OF USERS
Admin_for_purchase_dept	With privileges applicable for purchase dept	0
Administrators	This is the super administrator role that has maximum privilege and needs to contain at least one user.	23
Users [default]	Users of the system	22
No_report	Reports page blocked	1
Compliance_Dashboard_blocked	Access to compliance dashboard blocked	0
Technician	Technician of the system	33
Account Admin	Account Admin of the system	10

Results per page: 20 Displaying 1-7 of 7 results

- 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. You can also change the role of any user at any time.
- New users are assigned the 'User' role by default. However, you have the option to make any role the default.

Roles - Column Descriptions	
Column Heading	**Description**
Name	The name of the role. Click on the name to open the 'Role Management > Permissions screen. This allows you to view and manage the permissions assigned to the role. See '**Managing Permissions and Assigned Users of a Role**' for more details.
Description	Short description of the role.
Number of Users	Number of users to whom the role is assigned. Click the number to open the 'Assign Users' screen, which allows you to assign or remove the role from users. See '**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.

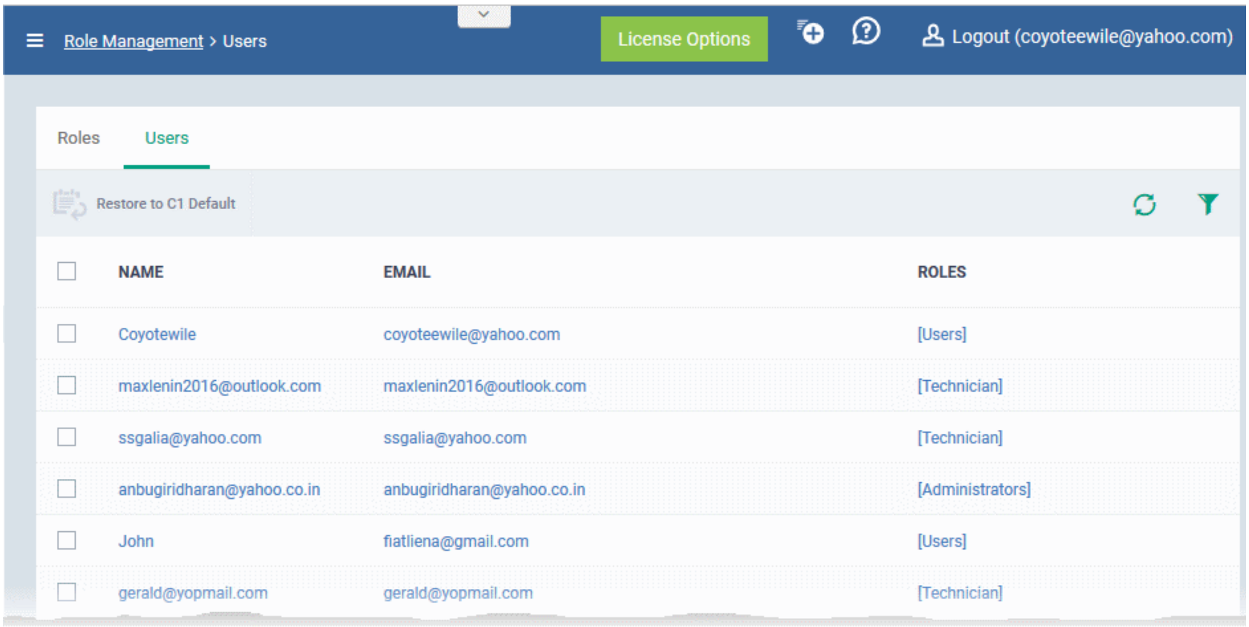
The roles interface allows admins to:

- **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.



□	NAME	EMAIL	ROLES
□	Coyotewile	coyoteewile@yahoo.com	[Users]
□	maxlenin2016@outlook.com	maxlenin2016@outlook.com	[Technician]
□	ssgalia@yahoo.com	ssgalia@yahoo.com	[Technician]
□	anbugiridharan@yahoo.co.in	anbugiridharan@yahoo.co.in	[Administrators]
□	John	fiatliena@gmail.com	[Users]
□	gerald@yopmail.com	gerald@yopmail.com	[Technician]

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:

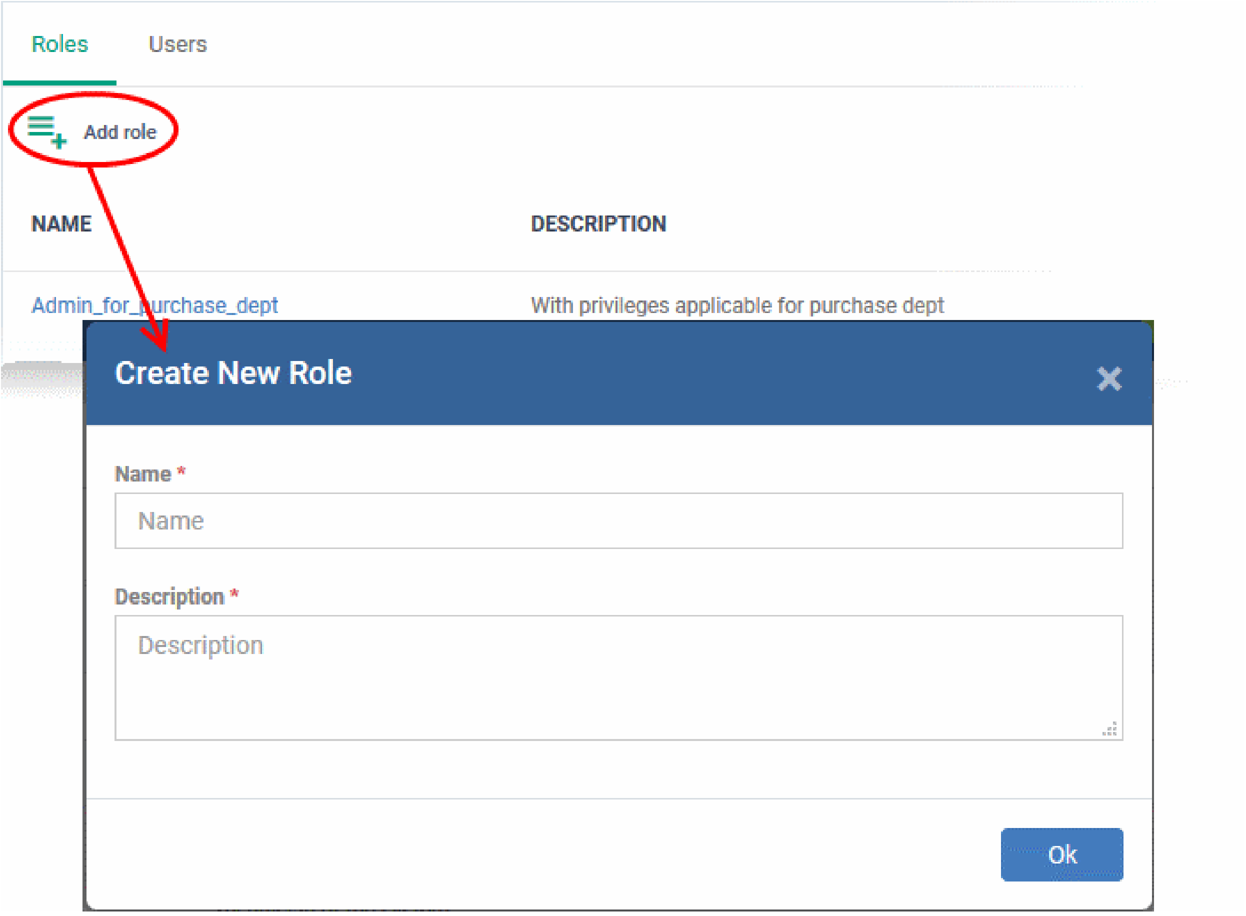
- **Manage Roles Assigned to a User**

4.3.1. Create 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.



Admin_for_purchase_dept — With privileges applicable for purchase dept

Name *

Name

Description *

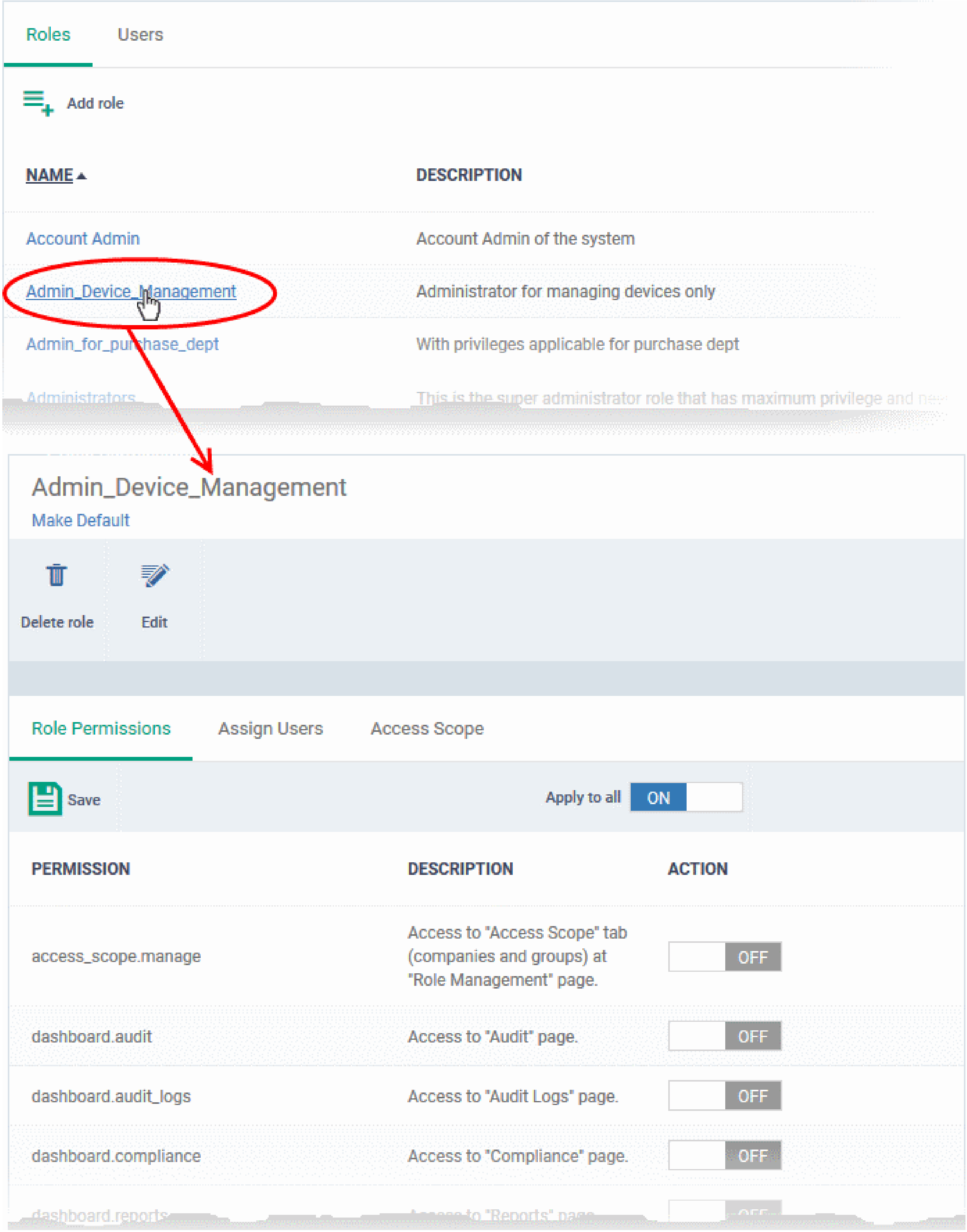
Description

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 edit its permissions, to assign users to the role, and to specify which companies and device groups the role is allowed to manage.



NAME ▲	DESCRIPTION
Account Admin	Account Admin of the system
Admin_Device_Management	Administrator for managing devices only
Admin_for_purchase_dept	With privileges applicable for purchase dept
Administrators	This is the super administrator role that has maximum privilege and ne

PERMISSION	DESCRIPTION	ACTION
access_scope.manage	Access to "Access Scope" tab (companies and groups) at "Role Management" page.	OFF
dashboard.audit	Access to "Audit" page.	OFF
dashboard.audit_logs	Access to "Audit Logs" page.	OFF
dashboard.compliance	Access to "Compliance" page.	OFF
dashboard.reports	Access to "Reports" page.	OFF

The 'Role Details' interface contains three tabs:

- **Role Permissions** - Define access rights and privileges for the role
- **Assign Users** - Select users who should have the role.
- **Access Scope** - Select which companies and device groups can be accessed by staff assigned to the role

To select access rights and privileges for the role

- Click the 'Role Permissions' tab if it is not open

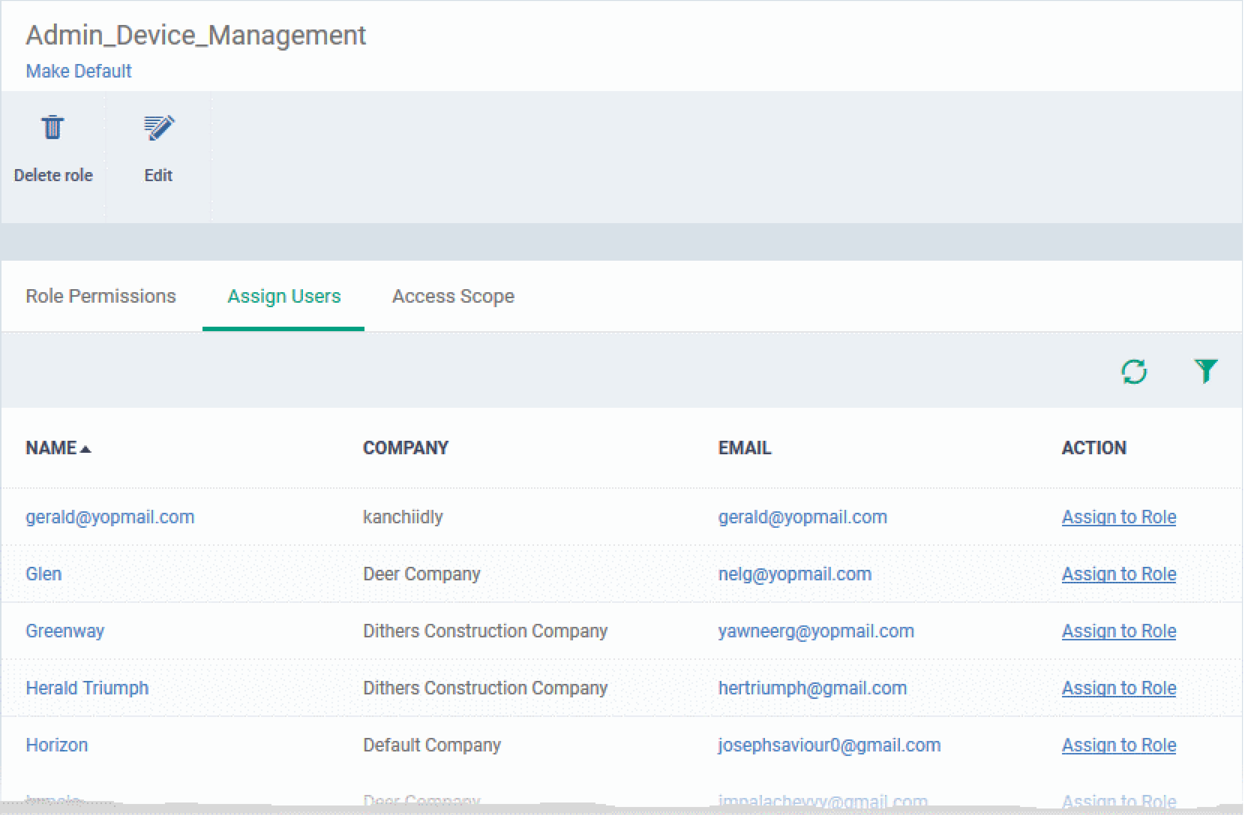
The tab shows a list of all available permissions along with a description of each.

- Use the switches on the right of each item to enable or disable a permission
- Use the 'Apply to all' switch to enable all permissions or disable all permissions
- Click 'Save' for your settings to take effect

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.



Admin_Device_Management

Make Default

NAME ▲	COMPANY	EMAIL	ACTION
gerald@yopmail.com	kanchiidly	gerald@yopmail.com	Assign to Role
Glen	Deer Company	nelg@yopmail.com	Assign to Role
Greenway	Dithers Construction Company	yawneerg@yopmail.com	Assign to Role
Herald Triumph	Dithers Construction Company	hertriumph@gmail.com	Assign to Role
Horizon	Default Company	josephsaviour0@gmail.com	Assign to Role
Impala	Deer Company	impalachevy@gmail.com	Assign to Role

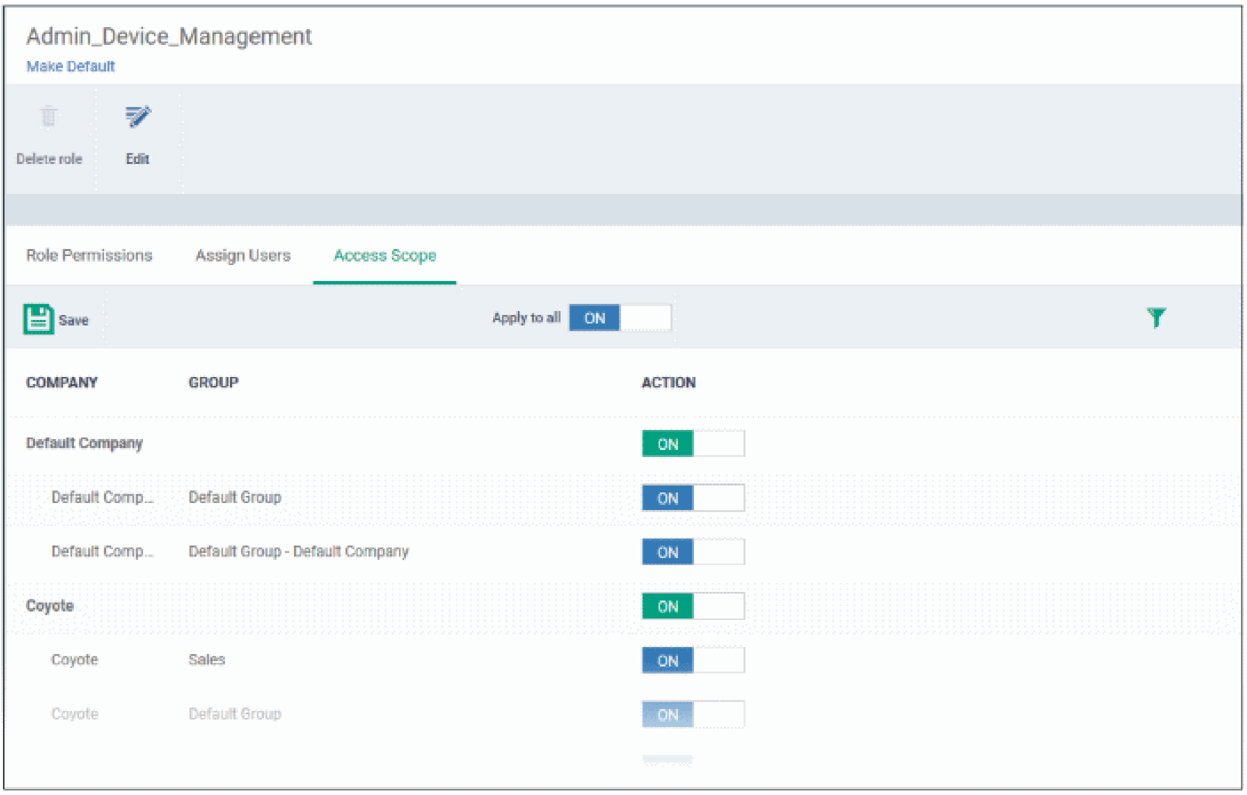
- Click the 'Assign to Role' links to place a user in the role.
- Click the 'Remove from Role' link to unassign a user from the role.

Tip: You can search for specific user(s) by clicking the funnel icon at the top right.

Select which companies and device groups can be accessed by the role

- Click the 'Access Scope' tab.

This will open a list of all companies added to ITSM so far. **Device groups** belonging to each company will be listed below the company name.



Admin_Device_Management

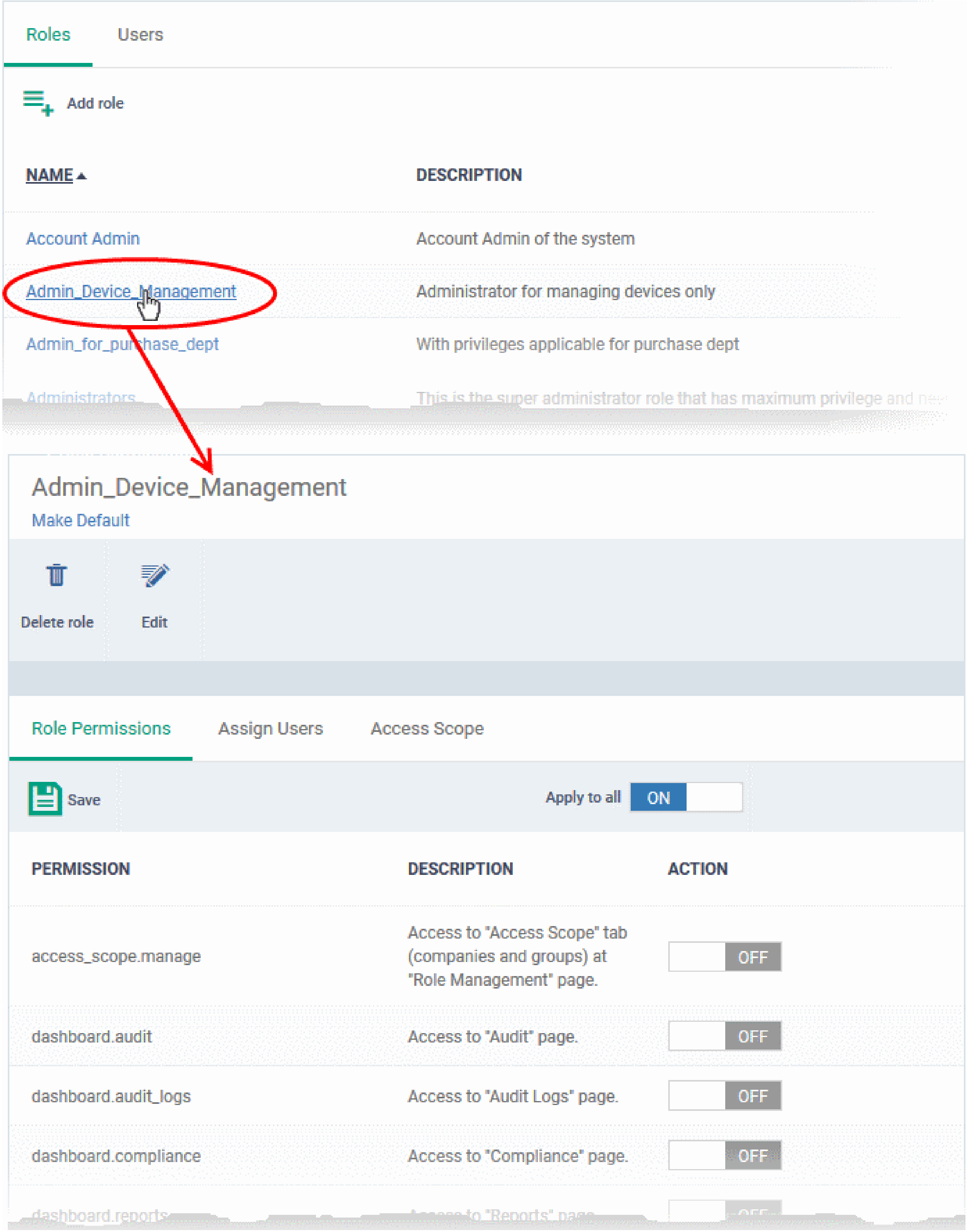
Make Default

COMPANY	GROUP	ACTION
Default Company		ON
Default Comp...	Default Group	ON
Default Comp...	Default Group - Default Company	ON
Coyote		ON
Coyote	Sales	ON
Coyote	Default Group	ON

- Use the green 'master' switch beside a company name to enable or disable the ability to manage groups belonging to the company. Please note you should have provided appropriate devices management **role permissions**.
- Use the switches beside a device group to enable or disable access to specific company groups.
- Use the 'Apply to All' switch to enable or disable access to all companies and groups on the page.
- Click 'Save' for your settings to take effect
- 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.

4.3.2. Manage Permissions and Users Assigned to a Role

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



NAME ▲	DESCRIPTION
Account Admin	Account Admin of the system
Admin_Device_Management	Administrator for managing devices only
Admin_for_purchase_dept	With privileges applicable for purchase dept
Administrators	This is the super administrator role that has maximum privilege and ne

Admin_Device_Management

PERMISSION	DESCRIPTION	ACTION
access_scope.manage	Access to "Access Scope" tab (companies and groups) at "Role Management" page.	OFF
dashboard.audit	Access to "Audit" page.	OFF
dashboard.audit_logs	Access to "Audit Logs" page.	OFF
dashboard.compliance	Access to "Compliance" page.	OFF
dashboard.reports	Access to "Reports" page.	OFF

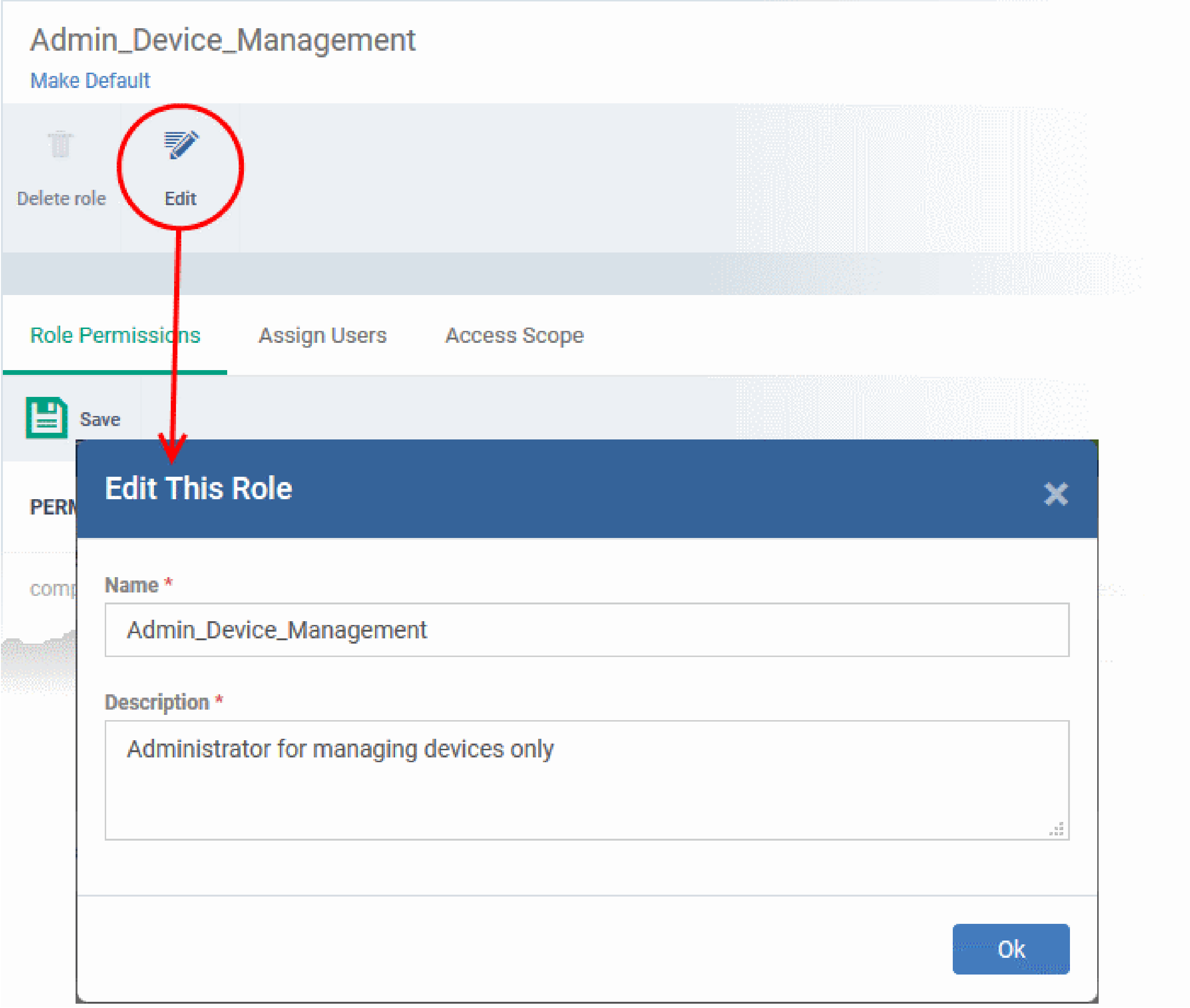
The 'Role Management' interface allows you to:

- 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
- Select companies and device groups accessible to a role

- Set a role as the default role

To edit the name and description of the role

- Click the 'Edit' button Edit at the top



Name *

Admin_Device_Management

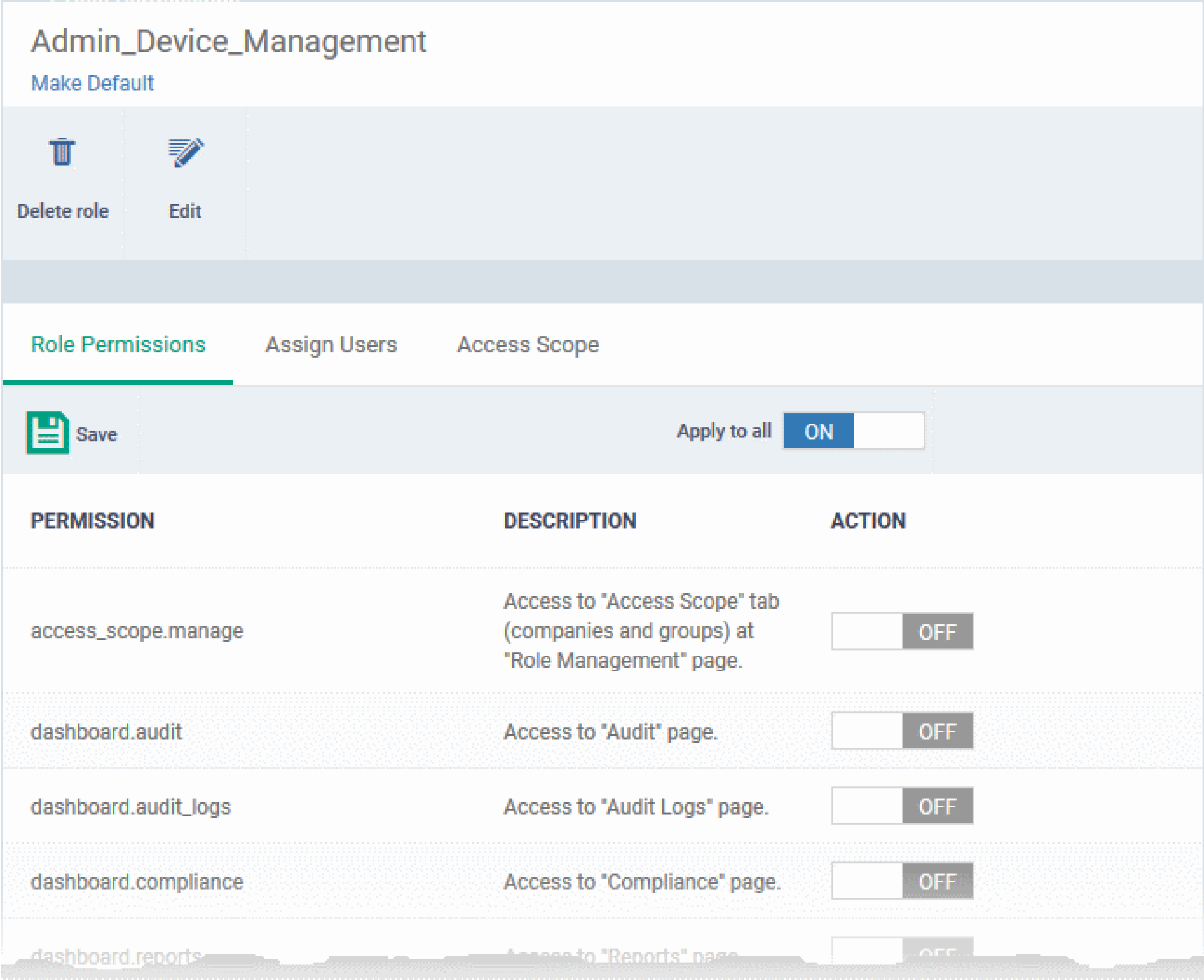
Description *

Administrator for managing devices only

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

To manage the permissions assigned to a role

- Click the name of the role to open the 'Role Details' interface
- Click the 'Role Permissions' tab if it is not open



Admin_Device_Management

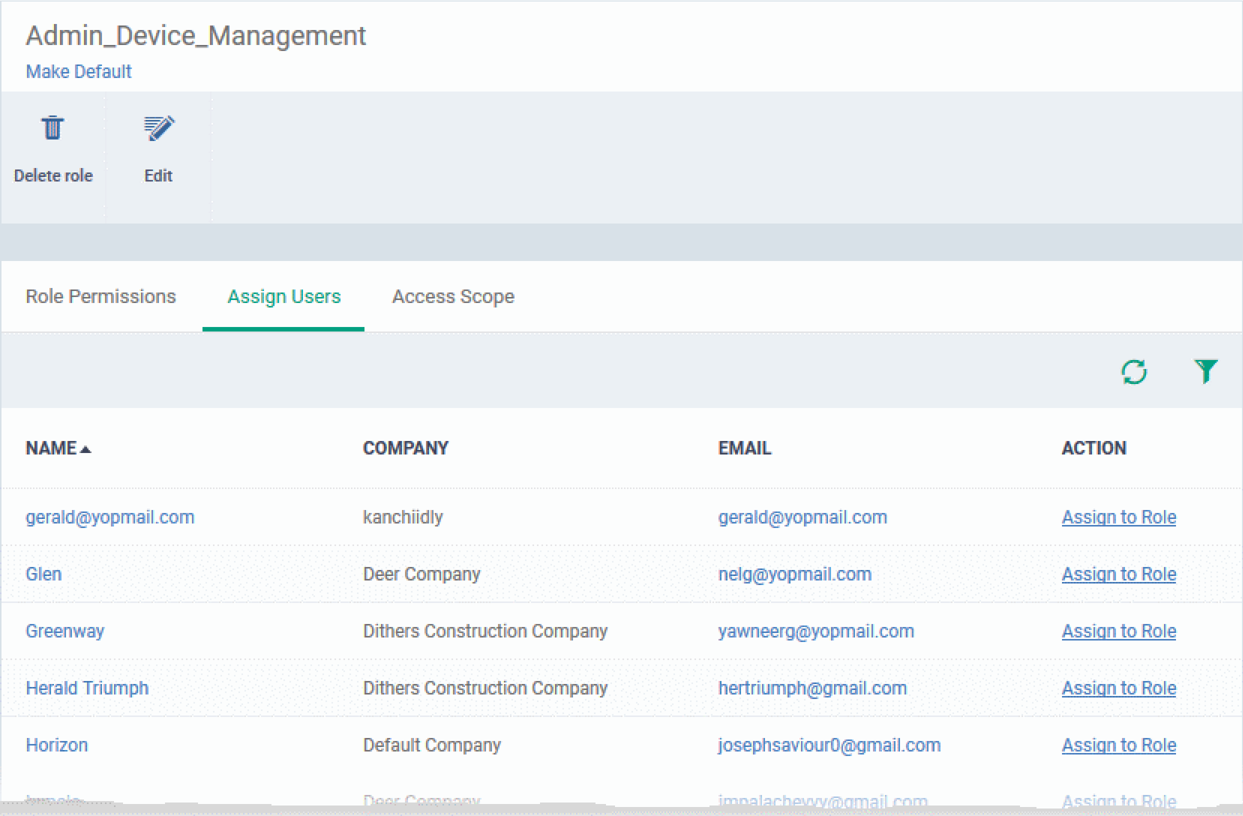
PERMISSION	DESCRIPTION	ACTION
access_scope.manage	Access to "Access Scope" tab (companies and groups) at "Role Management" page.	OFF
dashboard.audit	Access to "Audit" page.	OFF
dashboard.audit_logs	Access to "Audit Logs" page.	OFF
dashboard.compliance	Access to "Compliance" page.	OFF
dashboard.reports	Access to "Reports" page.	OFF

The tab shows a list of all available permissions along with a description of each.

- Use the switches on the right of each item to enable or disable a permission
- Use the 'Apply to all' switch to enable all permissions or disable all permissions
- Click 'Save' for your settings to take effect

To view users assigned to a role

- Click the name of the role to open the 'Role Details' interface
- Click the 'Assign Users' tab



Admin_Device_Management

Make Default

NAME ▲	COMPANY	EMAIL	ACTION
gerald@yopmail.com	kanchiidly	gerald@yopmail.com	Assign to Role
Glen	Deer Company	nelg@yopmail.com	Assign to Role
Greenway	Dithers Construction Company	yawneerg@yopmail.com	Assign to Role
Herald Triumph	Dithers Construction Company	hertriumph@gmail.com	Assign to Role
Horizon	Default Company	josephsaviour0@gmail.com	Assign to Role
Impala	Deer Company	impalachevvy@gmail.com	Assign to Role

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

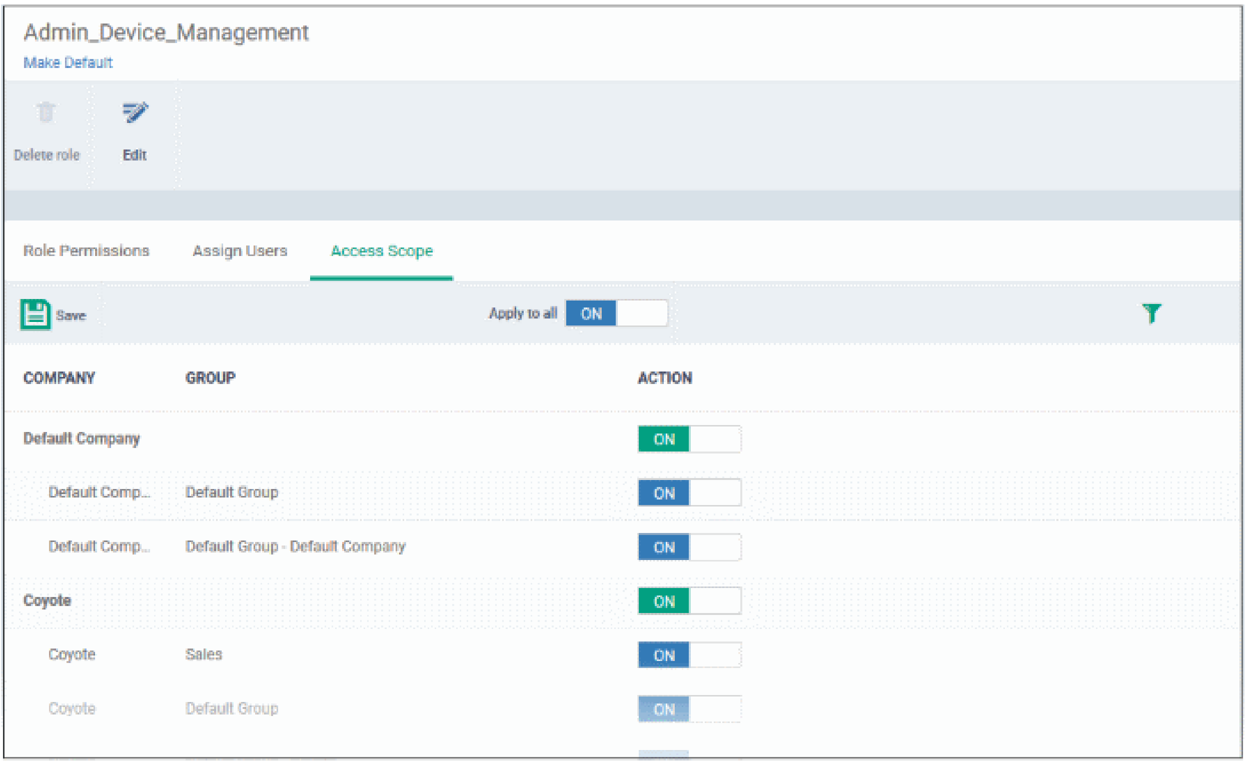
- Click the 'Assign to Role' links to place a user in the role.
- Click the 'Remove from Role' link to unassign a user from the role.

Tip: You can search for specific user(s) by clicking the funnel icon at the top right.

- Click a username to open 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 select which companies and device groups can be accessed by the role

- Click the name of the role to open the 'Role Details' interface
- Click the 'Access Scope' tab



COMPANY	GROUP	ACTION
Default Company		ON
Default Comp...	Default Group	ON
Default Comp...	Default Group - Default Company	ON
Coyote		ON
Coyote	Sales	ON
Coyote	Default Group	ON

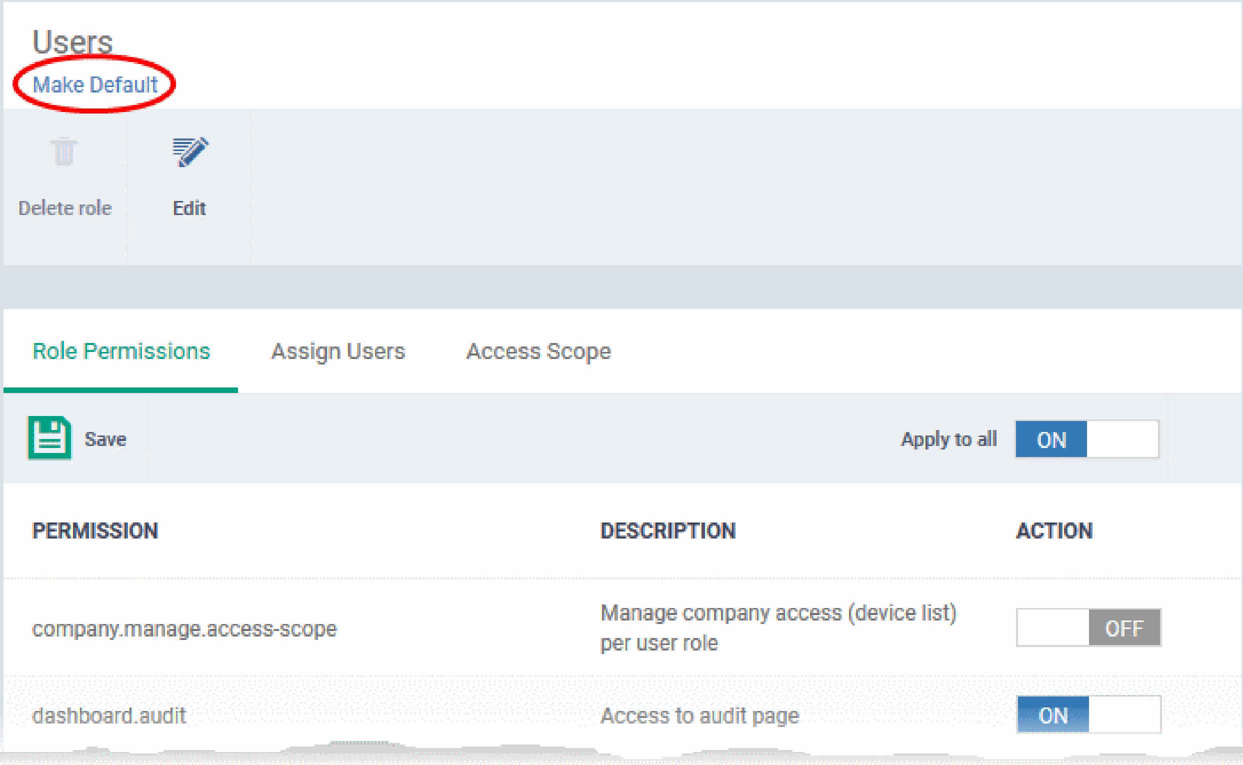
- Use the green 'master' switch beside a company name to enable or disable the ability to manage groups belonging to the company. Please note you should have provided appropriate devices **role permission**.
- Use the switches beside a device group to enable or disable access to specific company groups.
- Use the 'Apply to All' switch to enable or disable access to all companies and groups on the page.
- Click 'Save' for your settings to take effect

Set a role as the default role

- The default role is automatically applied to any new user unless the admin specifies a different role when adding the user
- The default role is automatically applied to users if their current role is removed

To set the default role:

- Click 'Users' > 'Role Management' > 'Roles'
- Click the name of the role you wish to make default. To open the 'Role Details' interface
- Click 'Make Default' under the name of the role:

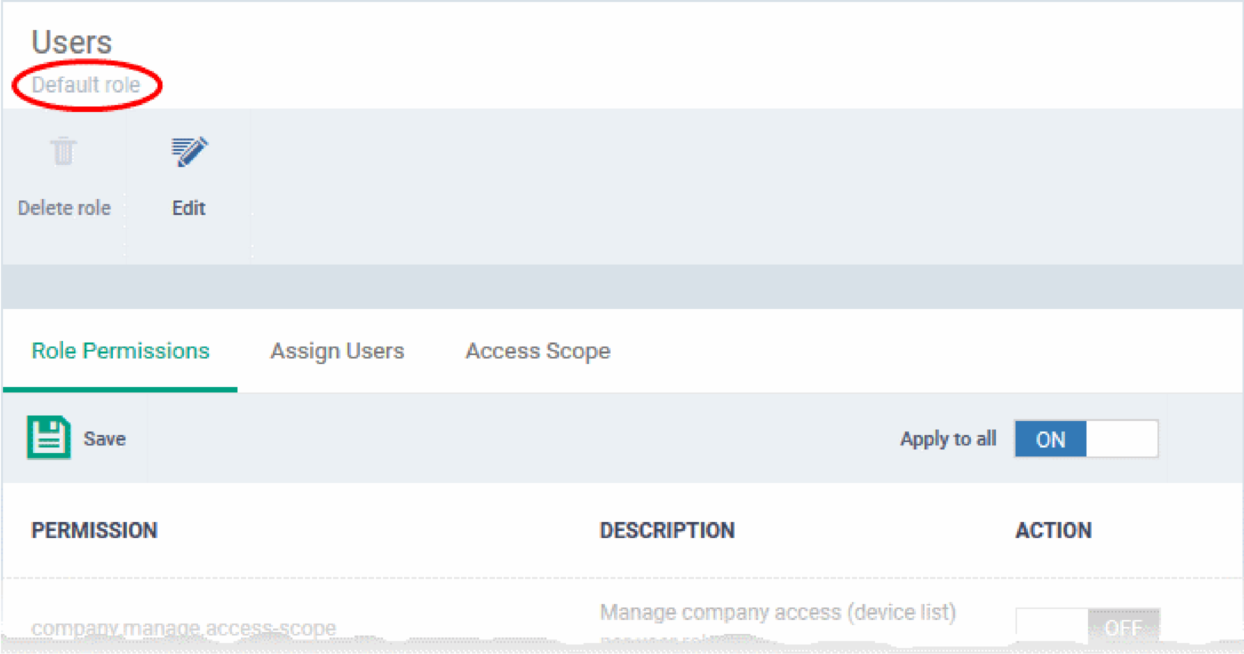


Users

Make Default

PERMISSION	DESCRIPTION	ACTION
company.manage.access-scope	Manage company access (device list) per user role	OFF
dashboard.audit	Access to audit page	ON

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



Users

Default role

PERMISSION	DESCRIPTION	ACTION
company.manage.access-scope	Manage company access (device list)	OFF

4.3.3. Remove a Role

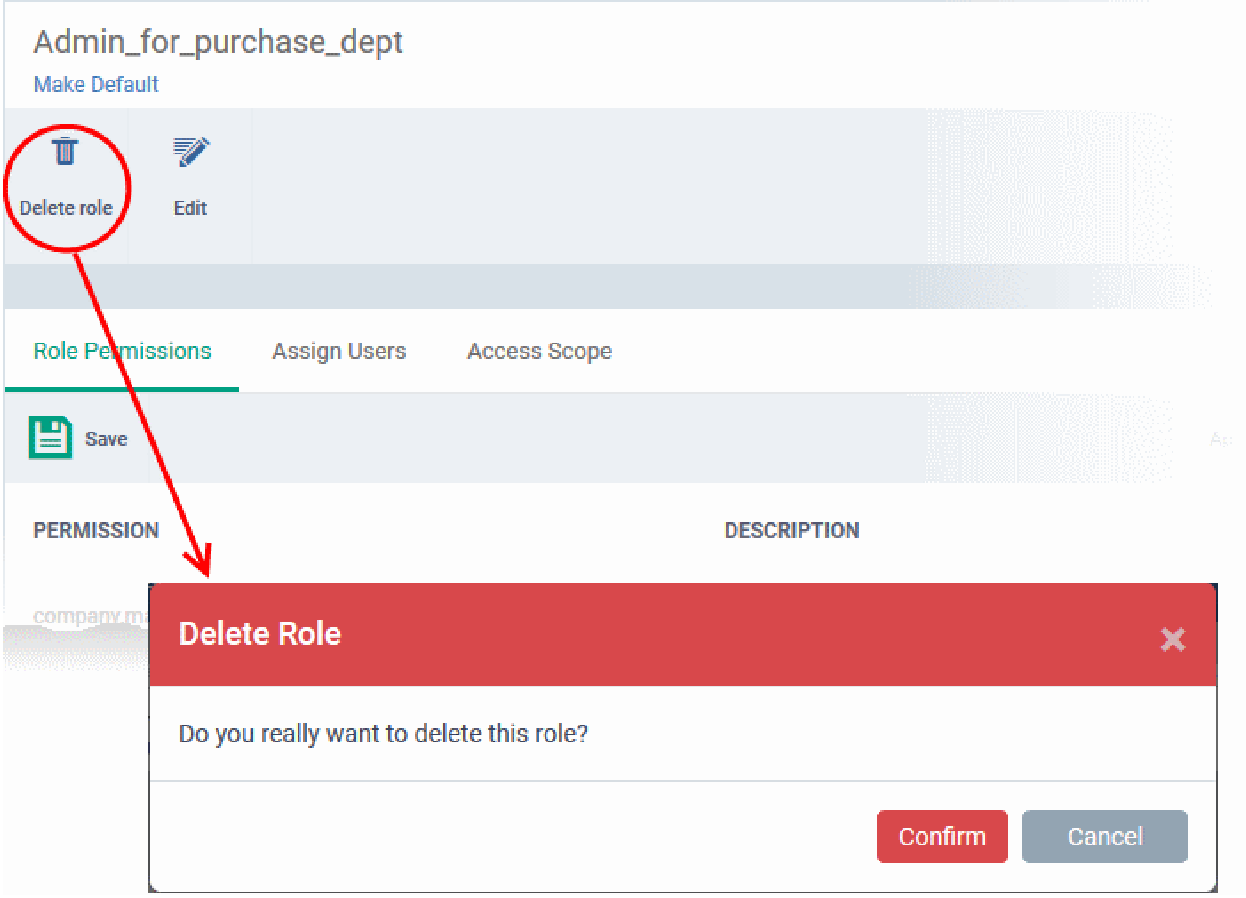
Administrators can delete roles that are no longer deemed necessary.

- Roles that are currently assigned to users cannot be removed. You should first 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



Do you really want to delete this role?

A confirmation dialog will appear.

- Click 'Confirm' to remove the role.

4.3.4. Manage Roles Assigned to a User

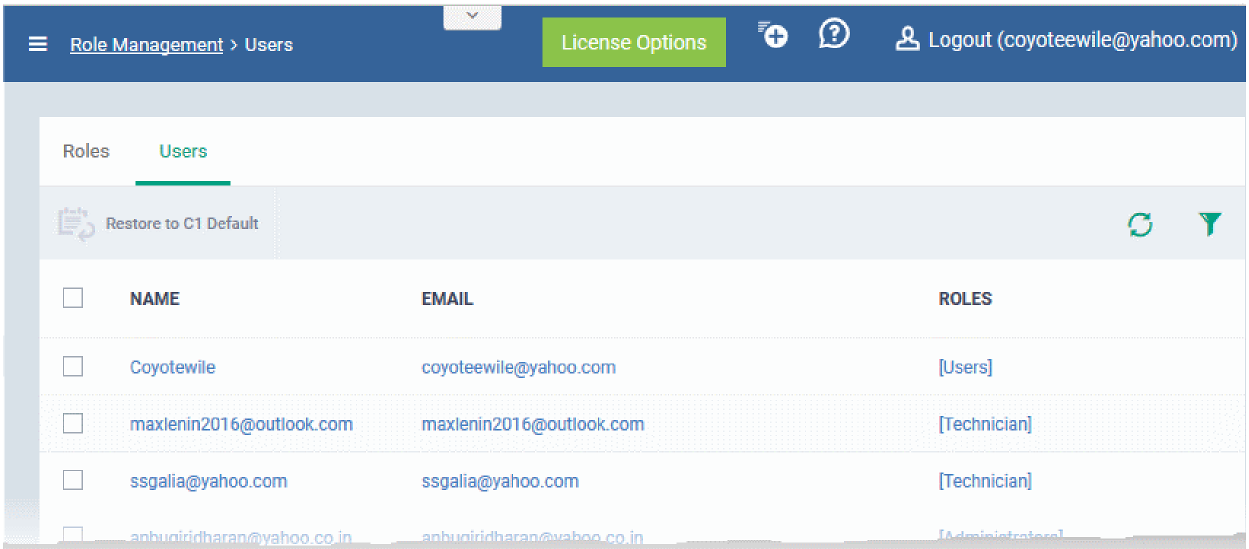
The 'Users' interface lets administrators add and remove roles from a user. Please note you cannot assign or remove the 'Account Admin' role. This role is automatically assigned to the person that created the C1 account.

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. You can restrict access to different companies by defining the access scope in the role assigned to a staff member.

To open the Users interface

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

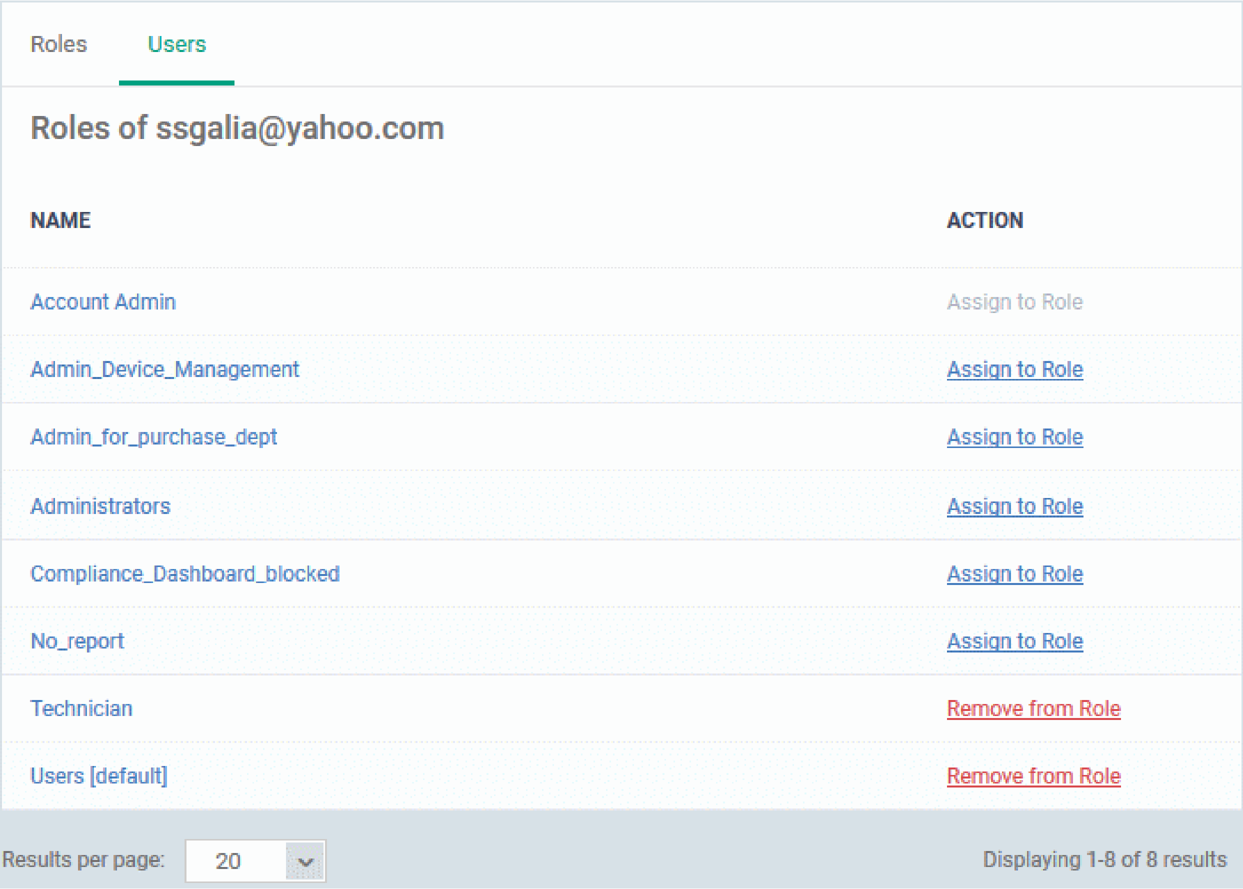
This will display a list of users and the roles assigned to them:



☐	NAME	EMAIL	ROLES
☐	Coyotewile	coyoteewile@yahoo.com	[Users]
☐	maxlenin2016@outlook.com	maxlenin2016@outlook.com	[Technician]
☐	ssgalia@yahoo.com	ssgalia@yahoo.com	[Technician]
☐	anbugiridharan@yahoo.co.in	anbugiridharan@yahoo.co.in	[Administrators]

To manage roles assigned to a user

- Click on the name of a user whose roles you want to manage.
- The interface will show all roles you can assign to the user.
- Click 'Assign to Role' to delegate a new role to the user .
- Click 'Remove from Role' to withdraw membership of a role from a user.



Roles of ssgalia@yahoo.com

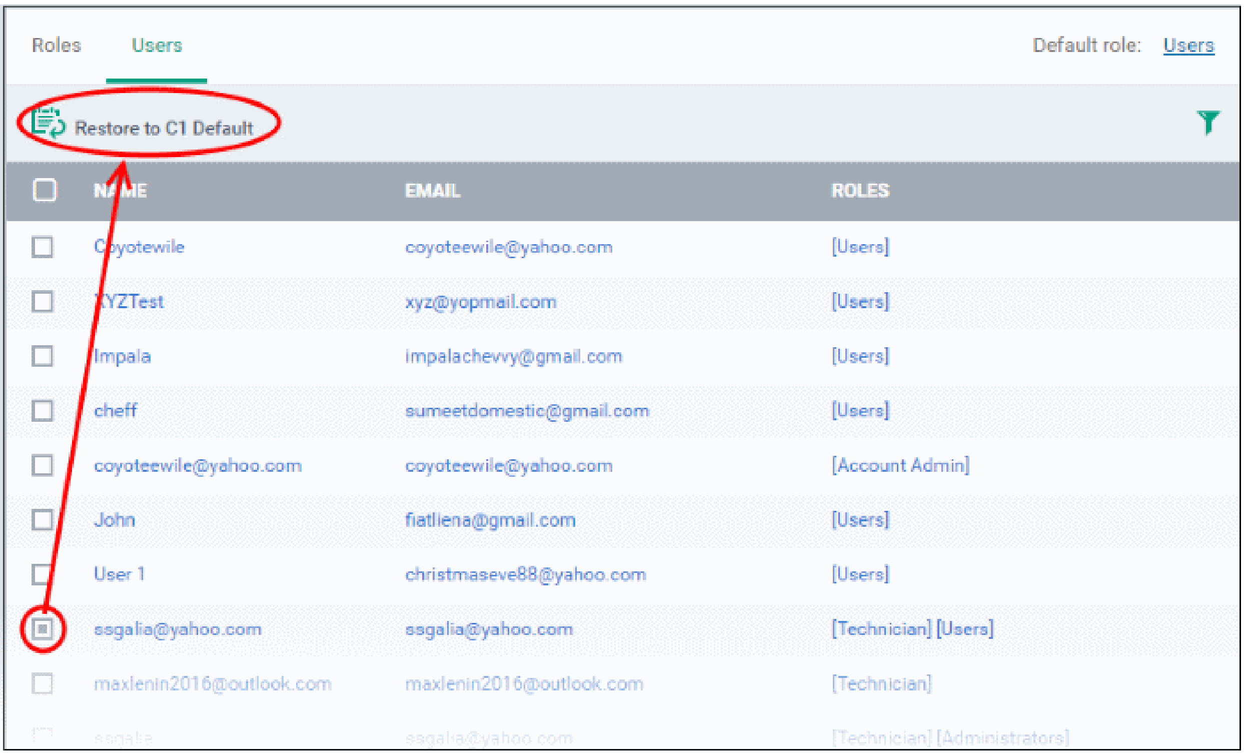
NAME	ACTION
Account Admin	Assign to Role
Admin_Device_Management	Assign to Role
Admin_for_purchase_dept	Assign to Role
Administrators	Assign to Role
Compliance_Dashboard_blocked	Assign to Role
No_report	Assign to Role
Technician	Remove from Role
Users [default]	Remove from Role

Results per page: 20 Displaying 1-8 of 8 results

To reset the roles to C1 default

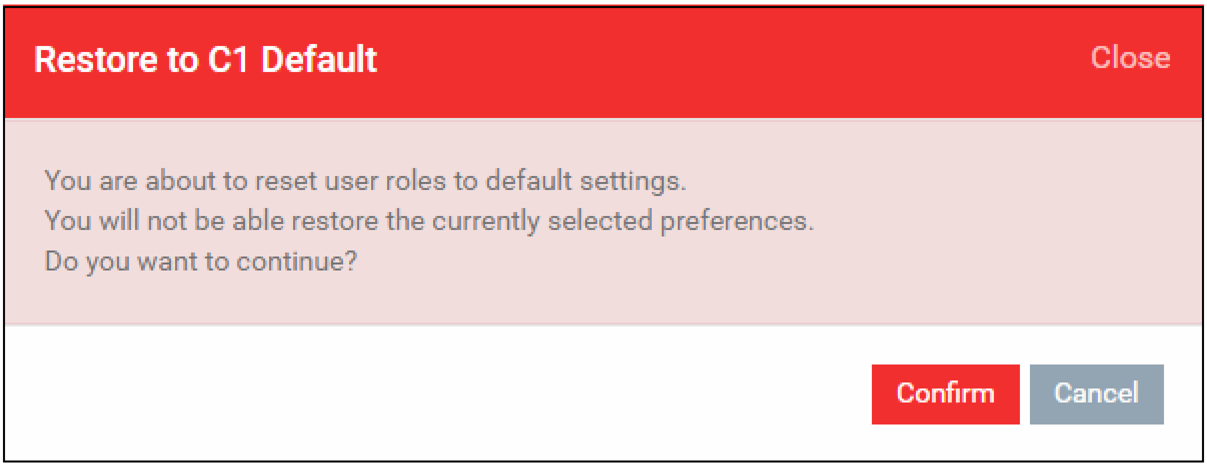
The following only applies to users added via the C1 interface. It does not apply to users added via the ITSM interface.

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



□	NAME	EMAIL	ROLES
□	Coyotewile	coyoteewile@yahoo.com	[Users]
□	XYZTest	xyz@yopmail.com	[Users]
□	Impala	impalachevvy@gmail.com	[Users]
□	cheff	sumeetdomestic@gmail.com	[Users]
□	coyoteewile@yahoo.com	coyoteewile@yahoo.com	[Account Admin]
□	John	fiatliena@gmail.com	[Users]
□	User 1	christmaseve88@yahoo.com	[Users]
☑	ssgalia@yahoo.com	ssgalia@yahoo.com	[Technician] [Users]
□	maxlenin2016@outlook.com	maxlenin2016@outlook.com	[Technician]
□	ssgalia	ssgalia@yahoo.com	[Technician] [Administrators]

- Select the user and click the 'Restore to C1 Default' button. Use the filter option at top-right if you need to search for users.



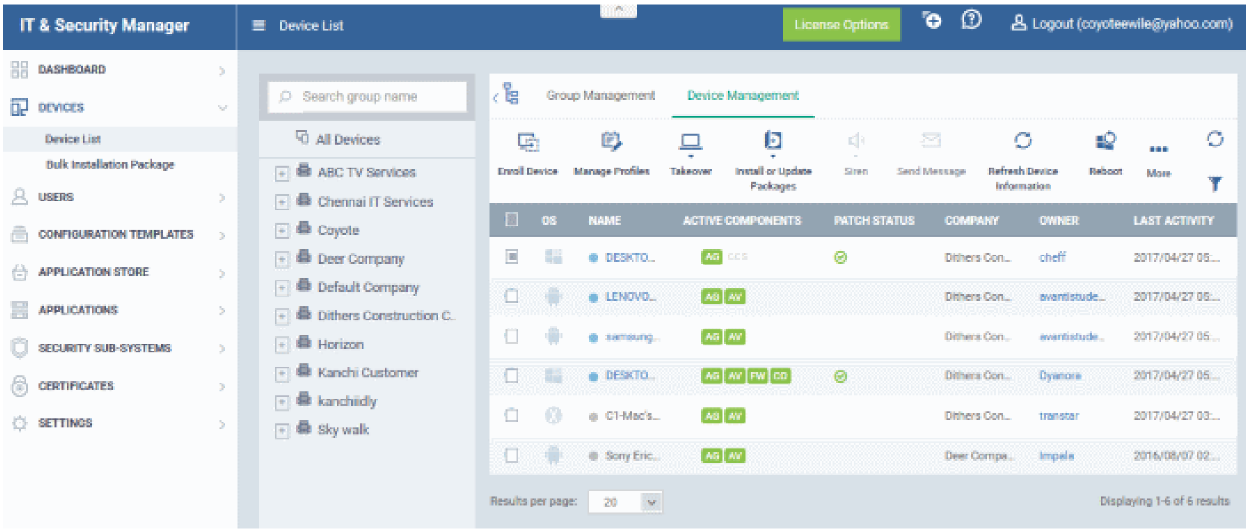
You are about to reset user roles to default settings.
You will not be able restore the currently selected preferences.
Do you want to continue?

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

5. Devices and Device Groups

The 'Devices' area allows admins to:

- View, manage and take actions upon enrolled devices and device groups.
- Download agent packages required for offline enrollment of endpoints and for enrollment of devices through Active Directory.
- Download the Comodo Remote Control tool which allows staff to remotely access Windows and Mac OS endpoints.



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
	DESKTO...	AG CCS	✓	Dithers Con...	cheff	2017/04/27 05:...
	LENOVO...	AG AV		Dithers Con...	avantistude...	2017/04/27 05:...
	samsung...	AG AV		Dithers Con...	avantistude...	2017/04/27 05:...
	DESKTO...	AG AV FW CD	✓	Dithers Con...	Dyanora	2017/04/27 05:...
	C1-Mac's...	AG AV		Dithers Con...	transtar	2017/04/27 03:...
	Sony Eric...	AG AV		Deer Compa...	impala	2016/08/07 02:...

Results per page: 20

Displaying 1-6 of 6 results

The device list area is split into two sections - Device Management and Group Management. A list of all companies, and groups under those companies, is shown to the left of the main information pane.

- **Device Management** - Displays all enrolled devices in the selected group. All available groups are listed under their company name on the left of the main information pane.

  The device management area allows you to enroll new devices for management, add or remove device profiles, install Comodo Client Security, take remote control of Windows devices, remotely lock devices and more. See '**Managing Devices**' for more details.
- **Group Management** - Allows admins to create new device groups, view and manage membership of existing groups, apply profiles to groups and more. You can choose the group you wish to manage from the list on the left. See '**Managing Device Groups**' for more details.
- **Bulk Installation Package** - Download the agent required to manually enroll devices and/or bulk-enroll devices from Active Directory. You can also download the Comodo Remote Control tool which allows you to interact with remote Windows and Mac OS endpoints. See **Bulk Enrollment of Devices** for more details.

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). See **step 2** of the quick start guide if you have not yet added an APN certificate and/or GCM token.

Process in short:

- Step 1 - **Enroll users** (if you haven't done so already)
- Step 2 - **Enroll devices** (if you haven't done so already). Note - you also can use **bulk enrollment** to import Windows and MAC devices en masse.
- Step 3 - **Create Device Groups**.
- Step 4 - **Import Devices into Groups**.
- Step 5 - **Apply Configuration Profiles to Groups**.
- Step 6 - **View Details of and Manage Individual Devices.**

Please use the following links to learn more:

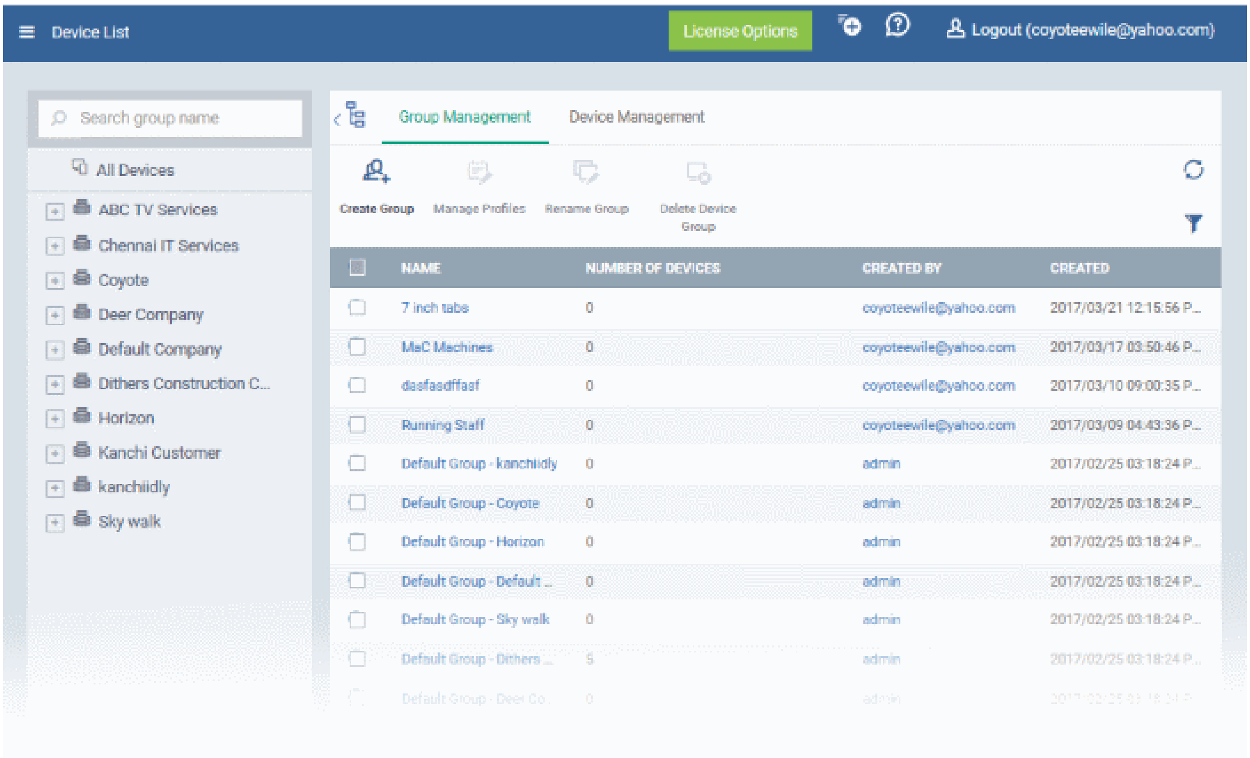
- **Managing Device Groups**
  - **Creating Device Groups**
  - **Editing Device Groups**
  - **Assigning Configuration Profile to Groups**

5.1. Manage Device Groups

ITSM allows you to create logical groups of Android, iOS, Mac and Windows devices in order to conveniently manage large numbers of 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. All companies and groups can be selected from the list to the left of the main pane.	C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.



	NAME	NUMBER OF DEVICES	CREATED BY	CREATED
□	7 inch tabs	0	coyoteewile@yahoo.com	2017/03/21 12:15:56 P...
□	MaC Machines	0	coyoteewile@yahoo.com	2017/03/17 03:50:46 P...
□	dasfasdffasf	0	coyoteewile@yahoo.com	2017/03/10 09:00:35 P...
□	Running Staff	0	coyoteewile@yahoo.com	2017/03/09 04:43:36 P...
□	Default Group - kanchiidly	0	admin	2017/02/25 03:18:24 P...
□	Default Group - Coyote	0	admin	2017/02/25 03:18:24 P...
□	Default Group - Horizon	0	admin	2017/02/25 03:18:24 P...
□	Default Group - Default ...	0	admin	2017/02/25 03:18:24 P...
□	Default Group - Sky walk	0	admin	2017/02/25 03:18:24 P...
□	Default Group - Dithers ...	5	admin	2017/02/25 03:18:24 P...
□	Default Group - Deer Co...	0	admin	2017/02/25 03:18:24 P...

The 'Device List' interface displays all device groups under each company as a tree structure. The 'Group Management' tab allows administrators to create new groups, import devices into groups, assign configuration profiles to groups and more.

- To open the 'Group Management' interface:
- Click 'Devices' on the left and choose 'Device Groups'
- Click the 'Group Management' tab
- To view all devices enrolled to ITSM, select 'All Devices' on the menu to the left
- Click on a company name, then a group name, to view all devices in a particular group

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 Management' 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 Management' 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 User Details** for more details.
Created	Indicates the date and time at which the group was created.

Sorting, Search and Filter Options

- Clicking any column header sorts the items in alphabetical or numerical order
- Clicking the funnel button on the right opens the filter options.
- Use the search box to find a specific group

Profiles

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**.

Refer to the following sections for more details about:

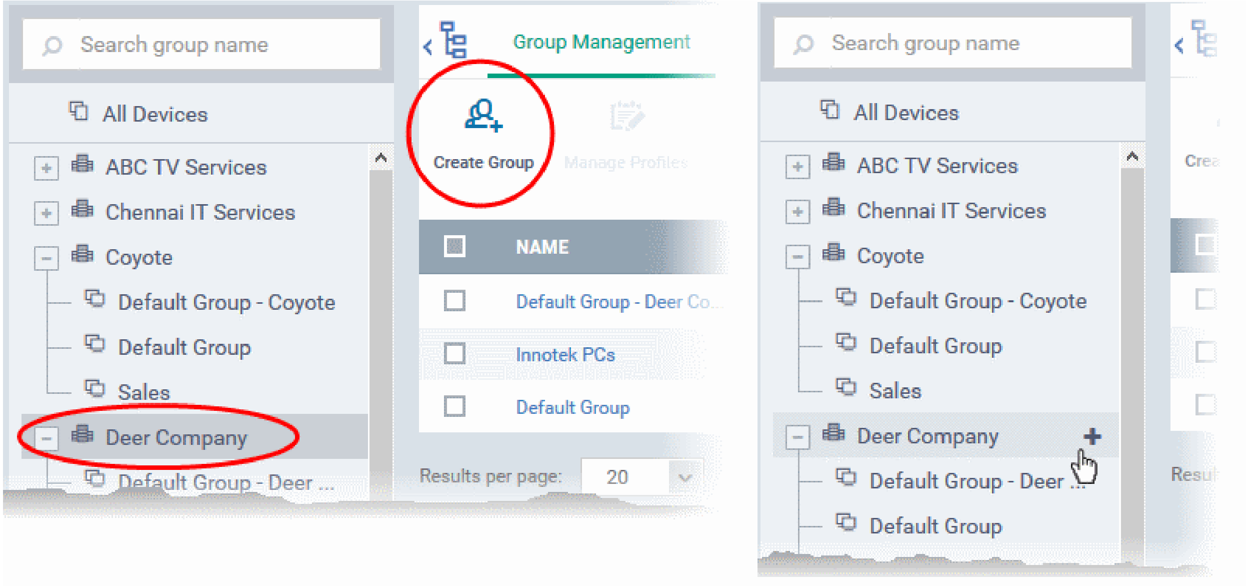
- **Creating Device Groups**
- **Editing a Device Group**
- **Assigning Configuration Profiles to a Device Group**
- **Removing a Device Group**

5.1.1. Create Device Groups

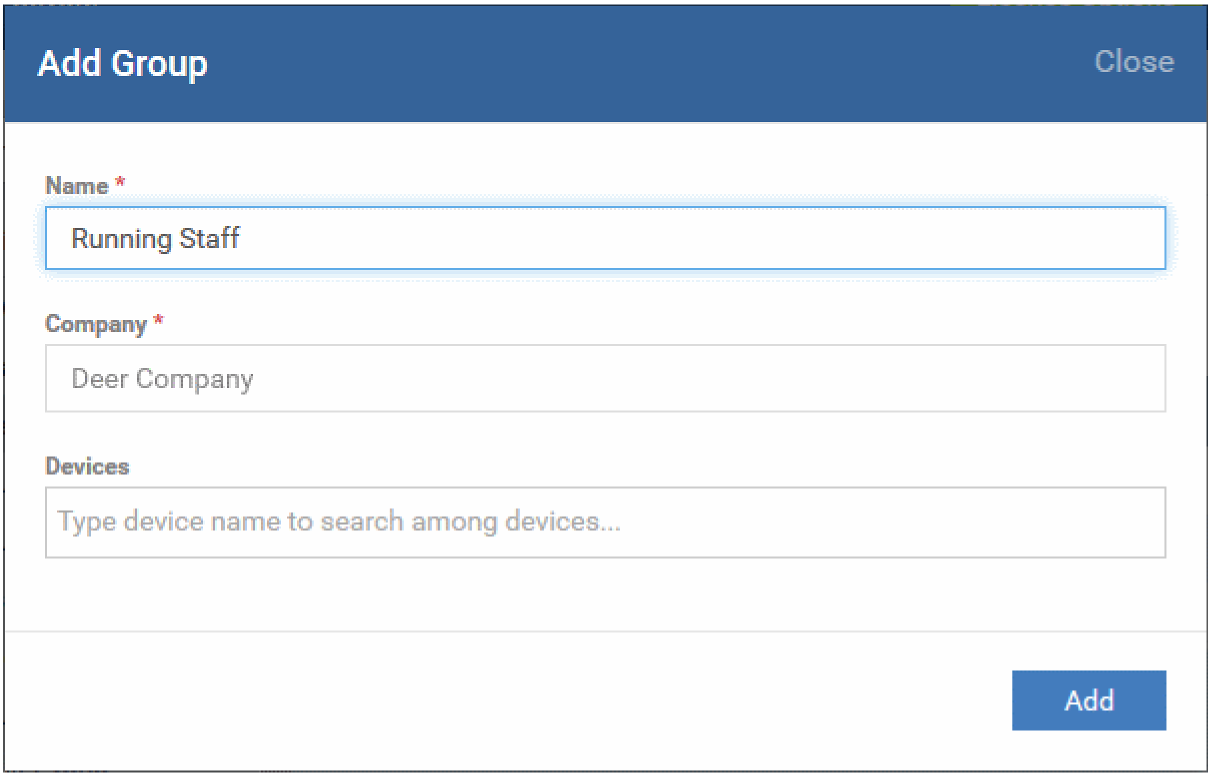
Placing devices into a group allows administrators to push configuration profiles to multiple devices simultaneously. OS-specific profiles will be automatically applied to the relevant devices.

To create a device group

- Click the 'Devices' tab from the left and choose 'Device List'
- C1 MSP customers should choose the company/department under which to create the group from the left
- Click 'Create Group' from the top left
- Alternatively move the mouse over the company name and click the '+' sign that appears at the right



The 'Add Group' interface will open.



Add Group

Close

Name *

Running Staff

Company *

Deer Company

Devices

Type device name to search among devices...

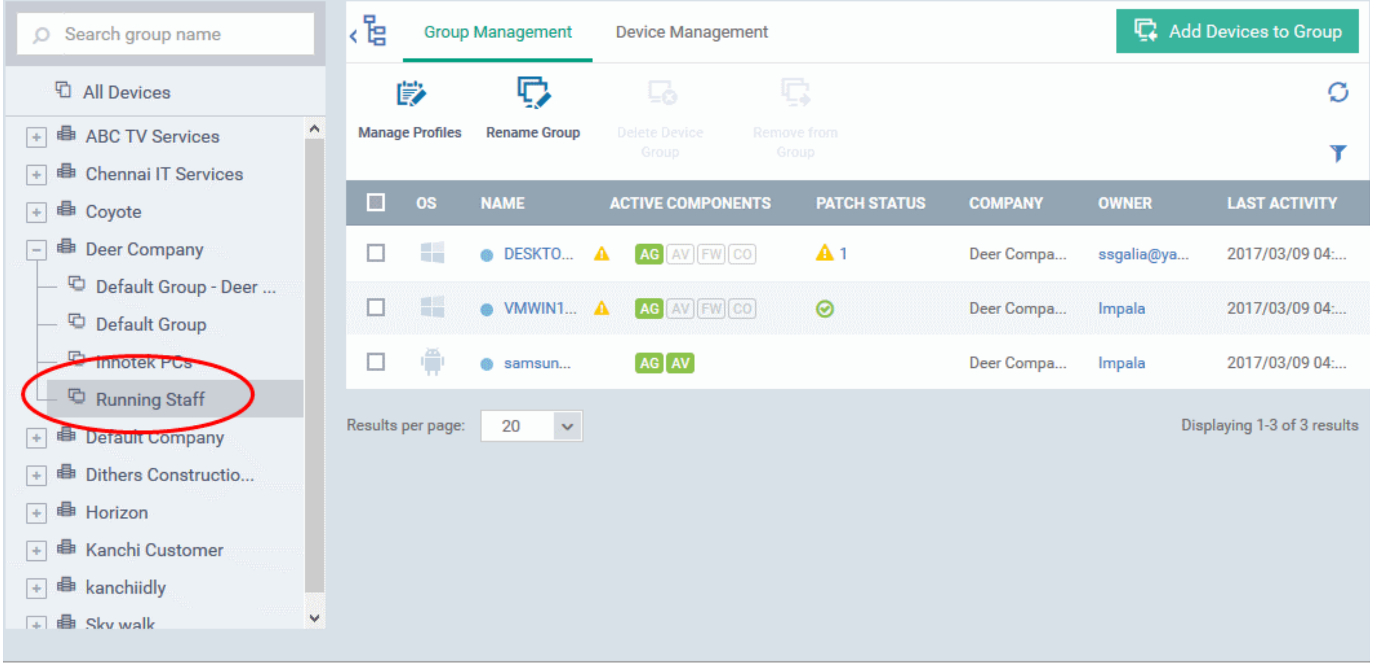
Add

'Add Group' dialog - Table of Parameters	
Form Element	**Description**
Name	Enter a descriptive name for the group.
Company	The company for which the group is to be created. This field will be pre-populated with the company chosen. You cannot edit this field.
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. Please note that you will be able to add only the devices enrolled for the chosen company.

'Add Group' dialog - Table of Parameters	
	Tip: You can add devices at a later stage too.

- Fill the details and click 'Add'.

The new group will be created under the company. You can add or remove devices and manage profiles applied to the devices in the group at any time. See **Editing a Device Group** for more details.



☐	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
☐		● DESKTO... ⚠	AG AV FW CO	⚠ 1	Deer Compa...	ssgalia@ya...	2017/03/09 04:...
☐		● VMWIN1... ⚠	AG AV FW CO	✓	Deer Compa...	Impala	2017/03/09 04:...
☐		● samsun...	AG AV		Deer Compa...	Impala	2017/03/09 04:...

- 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. See **Assigning Configuration Profiles to a Device Group** for more details.

5.1.2. Edit a Device Group

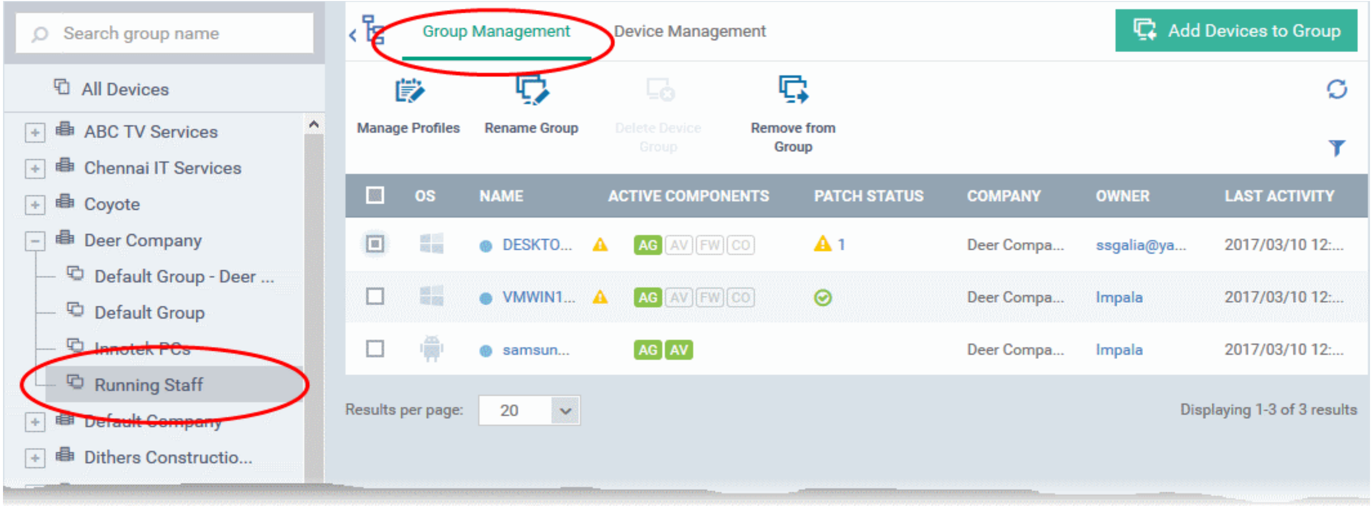
The Group Management interface allows admins to view devices in the selected group, add or remove devices, rename the group and manage policies applied to each device in the group.

- **View or edit a device group**
- **Add new devices to a group**
- **Remove devices from a group**
- **Rename a group**
- **Assign Configuration profiles to a device group**
- **Remove a group**

To view or edit a device group

- Click the 'Devices' link on the left and choose 'Device List'
- C1 MSP customers should choose the company/department whose group is to be edited
- Click the name of the group to be edited on the left
- Click the 'Group Management' tab on the right

The group management interface for the selected group will open.



□	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
□		● DESKTO... ⚠	AG AV FW CO	⚠ 1	Deer Compa...	ssgalia@ya...	2017/03/10 12:...
□		● VMWIN1... ⚠	AG AV FW CO	✓	Deer Compa...	Impala	2017/03/10 12:...
□		● samsun...	AG AV		Deer Compa...	Impala	2017/03/10 12:...

Results per page: 20

Displaying 1-3 of 3 results

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 has been offline for the past 24 hours. Clicking the device name will open the granular device details interface. See **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 with the 'Patch Management' tab open.
Company	Indicates the name of the company to which the device is enrolled.
Owner	Indicates the device user. Clicking the user name will open the 'View User' interface. See **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

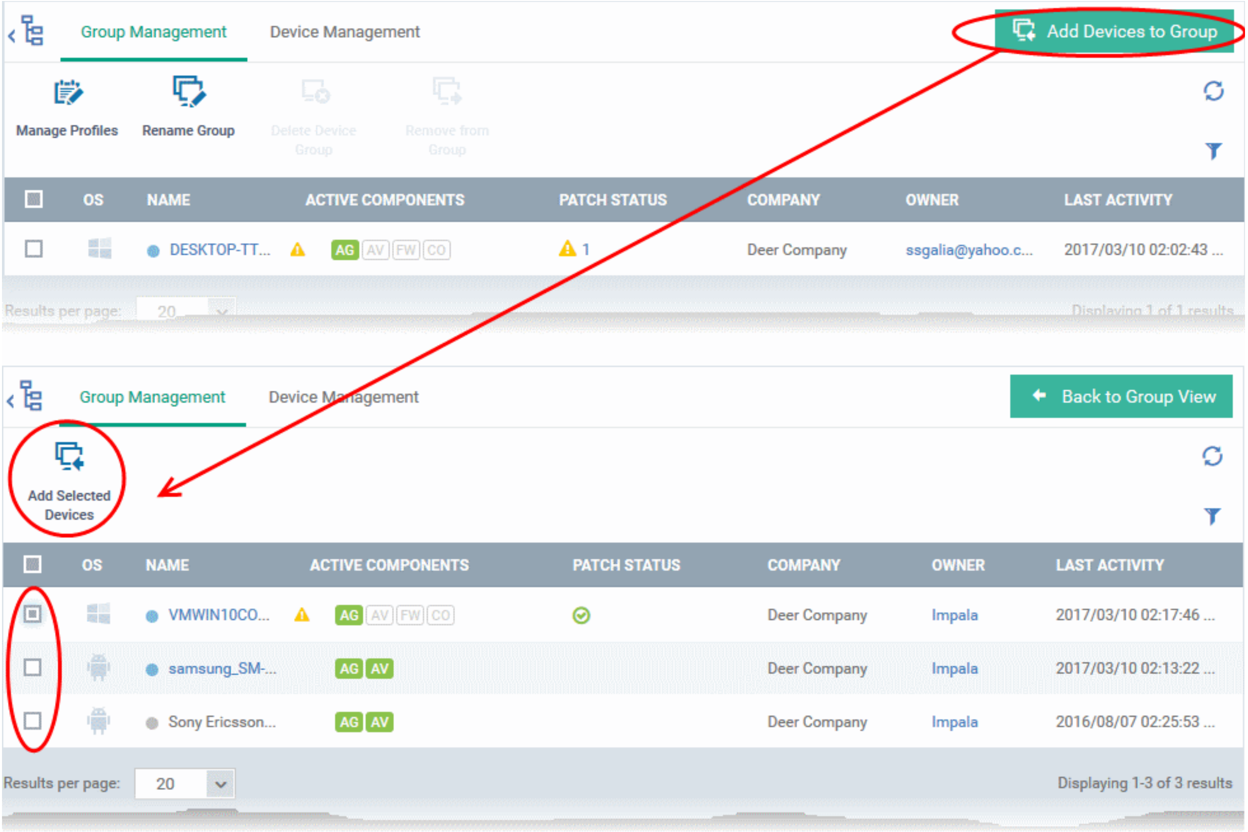
- Clicking on any of the 'OS', 'Name', 'Patch Status', 'Company', 'Owner' and 'Last Activity' column header sorts the items based on alphabetical or ascending/descending order of entries in that column.
- Clicking the funnel button at the right end opens the filter options that allows to search for a particular device.
- To filter the items or search for a device based on its OS, online status, name, patch status, company. Owner and/or a period of last activity, 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.

To add new devices to a group

- Click the 'Devices' link on the left and choose 'Device List'
- C1 MSP customers should choose the company/department whose group is to be edited
- Click the name of the group to be edited on the left
- Click the 'Group Management' tab on the right
- Click 'Add Devices to Group' at the top right.

Note: You can only add devices which belong to the same company as the group.

The interface will list all devices enrolled to the company that are not already in the target group:



□	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
□		● DESKTOP-TT... ⚠	AG AV FW CO	⚠ 1	Deer Company	ssgalia@yahoo.c...	2017/03/10 02:02:43 ...

Results per page: 20 Displaying 1 of 1 results

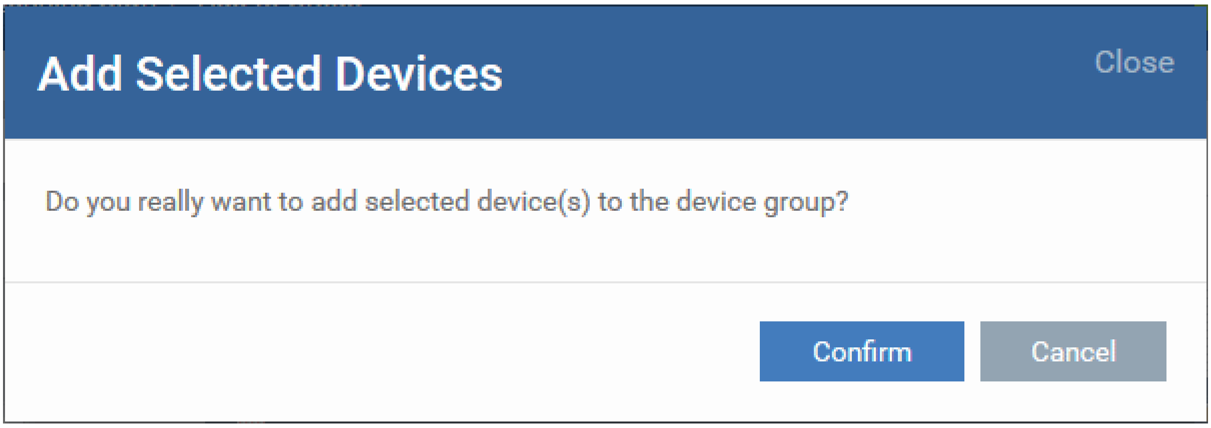
□	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
☒		● VMWIN10CO... ⚠	AG AV FW CO	✓	Deer Company	Impala	2017/03/10 02:17:46 ...
□		● samsung_SM-...	AG AV		Deer Company	Impala	2017/03/10 02:13:22 ...
□		● Sony Ericsson...	AG AV		Deer Company	Impala	2016/08/07 02:25:53 ...

Results per page: 20 Displaying 1-3 of 3 results

- Select the devices to be added to the group and click 'Add Selected Devices'.

Tip: You can filter or search for specific devices using the filter options that appear on clicking the funnel icon at the top right.

A confirmation dialog will appear.



Add Selected Devices

Close

Do you really want to add selected device(s) to the device group?

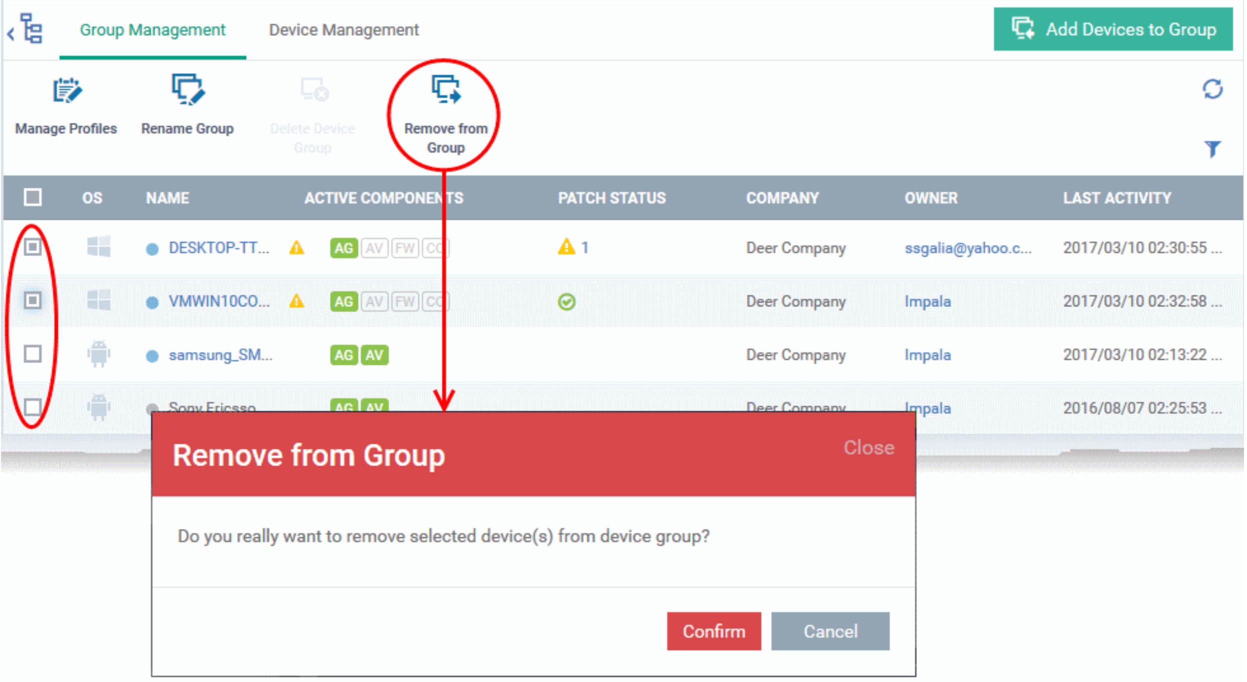
- Click 'Confirm'. The devices will be added to the group.

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, see **Viewing and Managing Device Group Membership**.

To remove devices from a group

- Choose the devices to be removed from the device group details interface
- Click 'Remove from Group'



☐	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
▣		DESKTOP-TT... ⚠	AG AV FW CO	⚠ 1	Deer Company	ssgalia@yahoo.c...	2017/03/10 02:30:55 ...
▣		VMWIN10CO... ⚠	AG AV FW CO	✓	Deer Company	Impala	2017/03/10 02:32:58 ...
☐		samsung_SM...	AG AV		Deer Company	Impala	2017/03/10 02:13:22 ...
☐		Sony Ericsso	AG AV		Deer Company	Impala	2016/08/07 02:25:53 ...

Remove from Group

Close

Do you really want to remove selected device(s) from device group?

- Click 'Confirm' in the confirmation dialog.

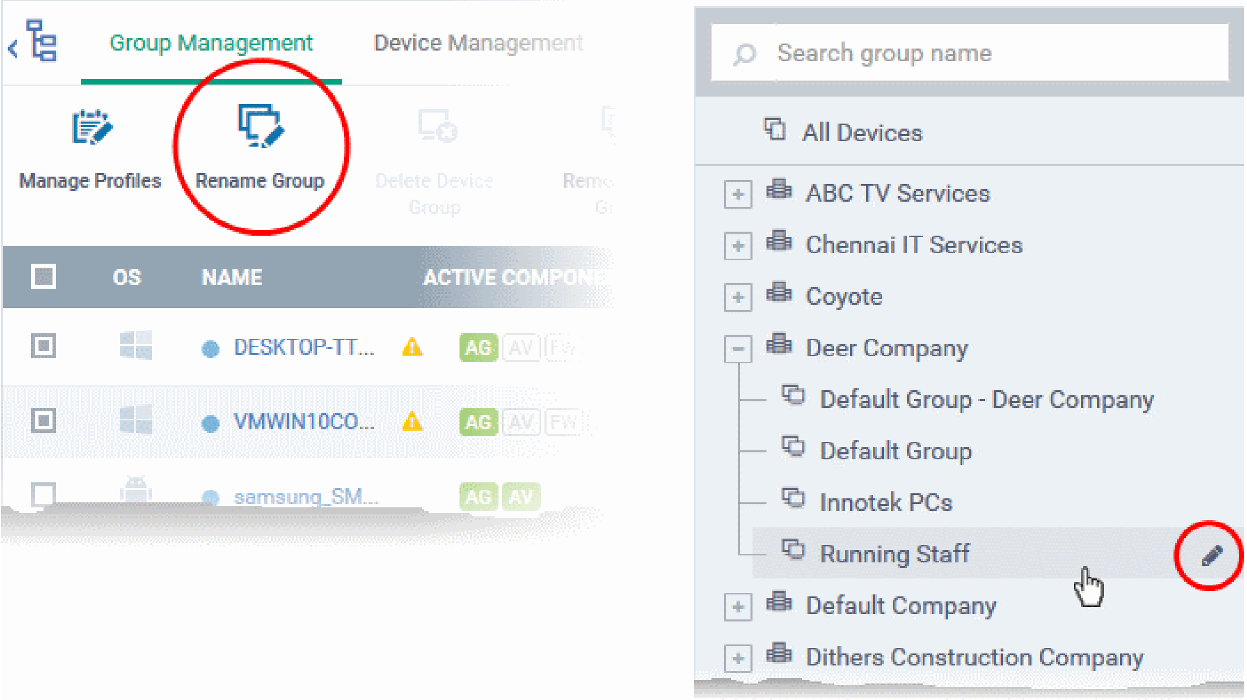
If a device is removed from a group, any group profiles will also be removed from the device.

Tip: You can remove the membership of a device to a group, from the 'Device Details' interface too. See **Viewing**

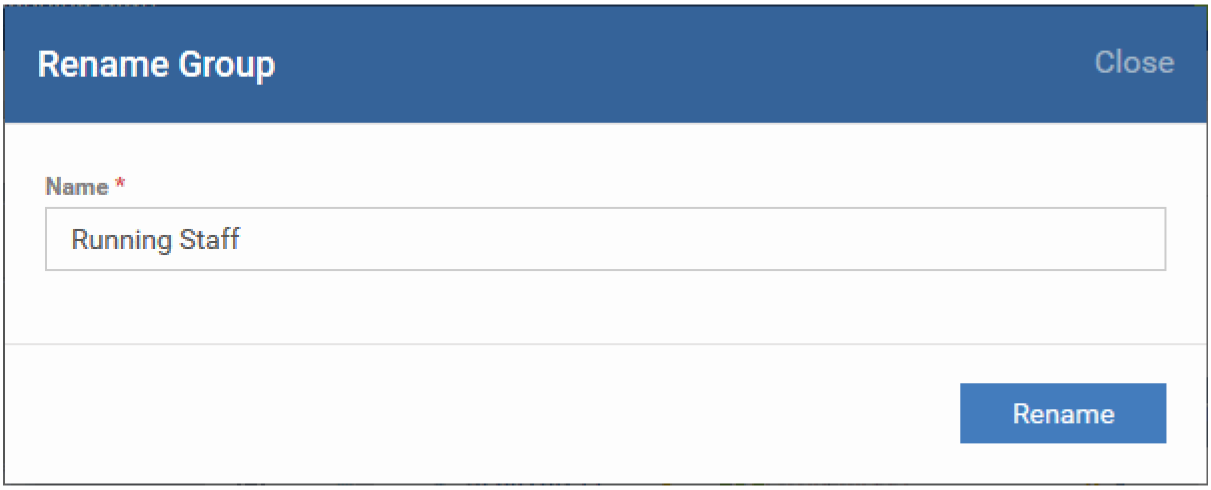
and Managing Device Group Membership, for more details.

To rename a group

- Click on the 'Rename' button at the top.
- Alternatively, move your mouse over the group name in the left pane and click the pencil icon.



The 'Rename Group' dialog will open.



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

The group will be updated with the new name.

5.1.3. Assign Configuration Profiles to a Device Group

Administrators can view configuration profiles currently assigned to the device group, add new profiles or remove existing profiles.

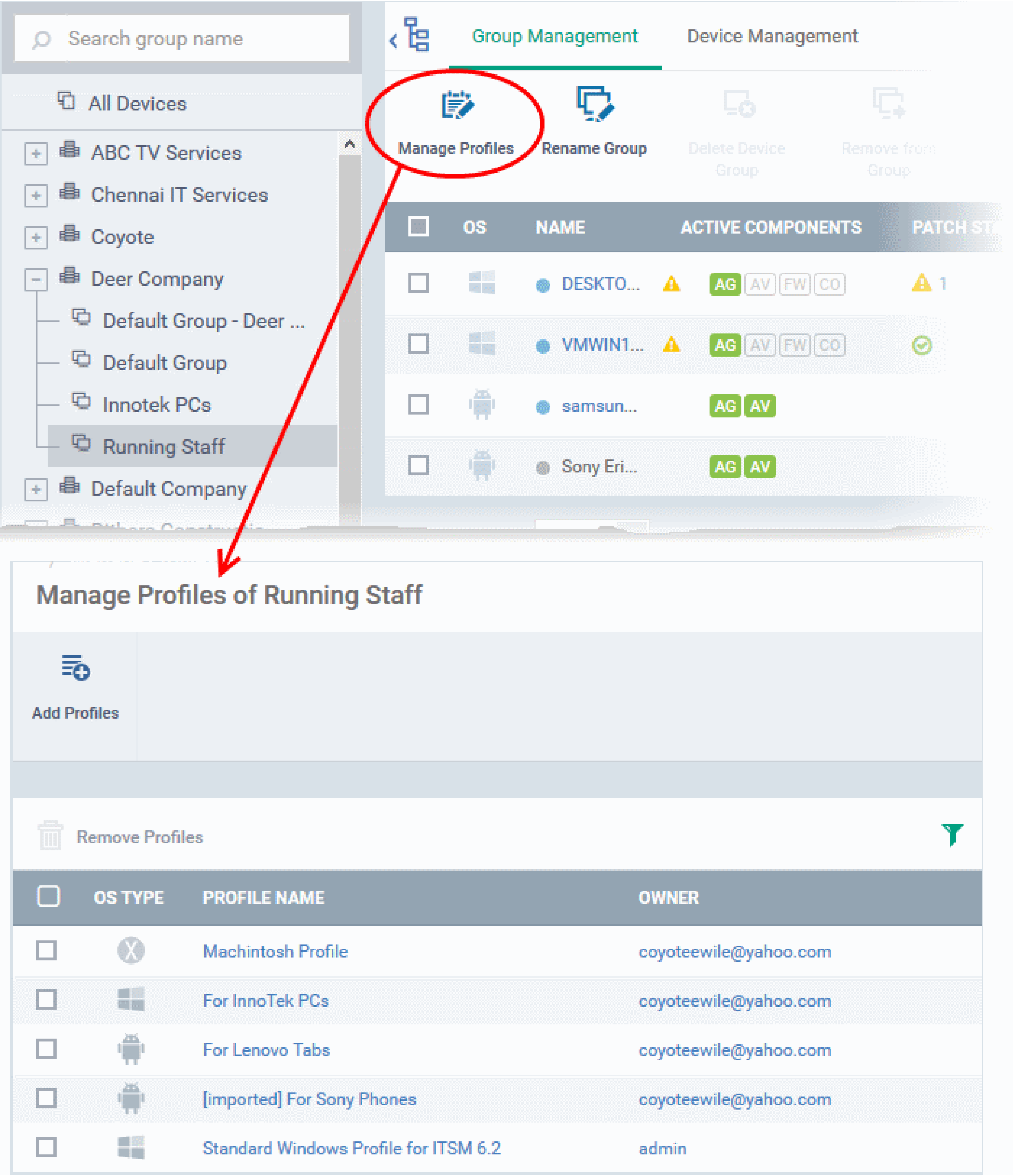
- See **Configuration Profiles**, for more details on setting up profiles.

To view and manage the profiles applied to a group

- Click the 'Devices' tab on the left and choose 'Device List'
- C1 MSP customers should choose the company/department whose group is to be edited
- Click the name of the group to be edited from the tree on the left
- Click the 'Group Management' tab on the right

The 'Group Management' interface for the selected group will open.

- Click 'Manage Profiles' from the options at the top.



□	OS	NAME	ACTIVE COMPONENTS	PATCH ST
□		DESKTO... ⚠	AG AV FW CO	⚠ 1
□		VMWIN1... ⚠	AG AV FW CO	✓
□		samsun...	AG AV	
□		Sony Eri...	AG AV	

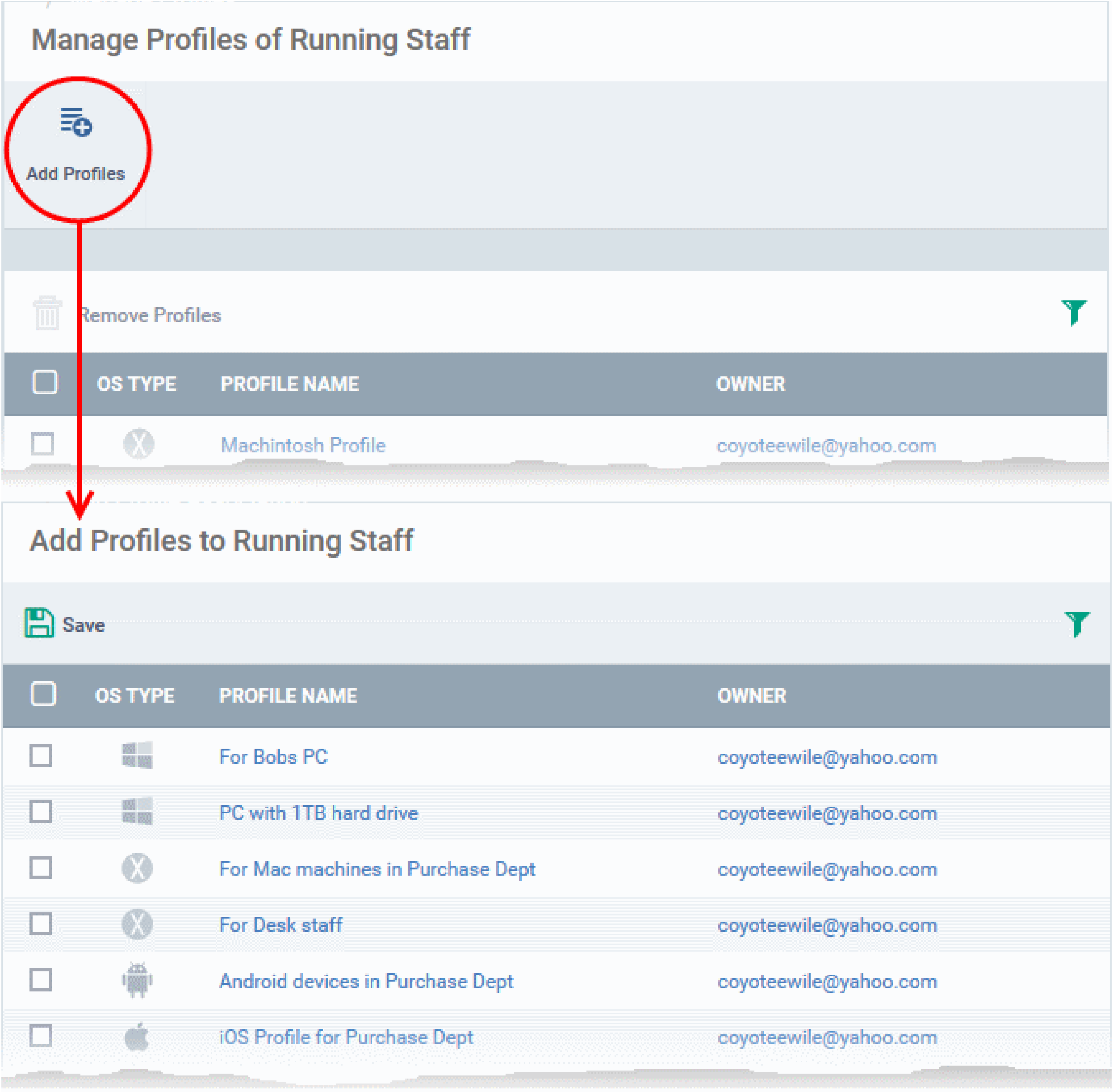
Manage Profiles of Running Staff

□	OS TYPE	PROFILE NAME	OWNER
□		Machintosh Profile	coyoteewile@yahoo.com
□		For InnoTek PCs	coyoteewile@yahoo.com
□		For Lenovo Tabs	coyoteewile@yahoo.com
□		[imported] For Sony Phones	coyoteewile@yahoo.com
□		Standard Windows Profile for ITSM 6.2	admin

The list of profiles in effect on the device group will be displayed.

To add a new profile

- Click 'Add Profiles' from the top.



Manage Profiles of Running Staff

□	OS TYPE	PROFILE NAME	OWNER
□	X	Machintosh Profile	coyoteewile@yahoo.com

Add Profiles to Running Staff

□	OS TYPE	PROFILE NAME	OWNER
□	⊞	For Bobs PC	coyoteewile@yahoo.com
□	⊞	PC with 1TB hard drive	coyoteewile@yahoo.com
□	X	For Mac machines in Purchase Dept	coyoteewile@yahoo.com
□	X	For Desk staff	coyoteewile@yahoo.com
□	🤖	Android devices in Purchase Dept	coyoteewile@yahoo.com
□		iOS Profile for Purchase Dept	coyoteewile@yahoo.com

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

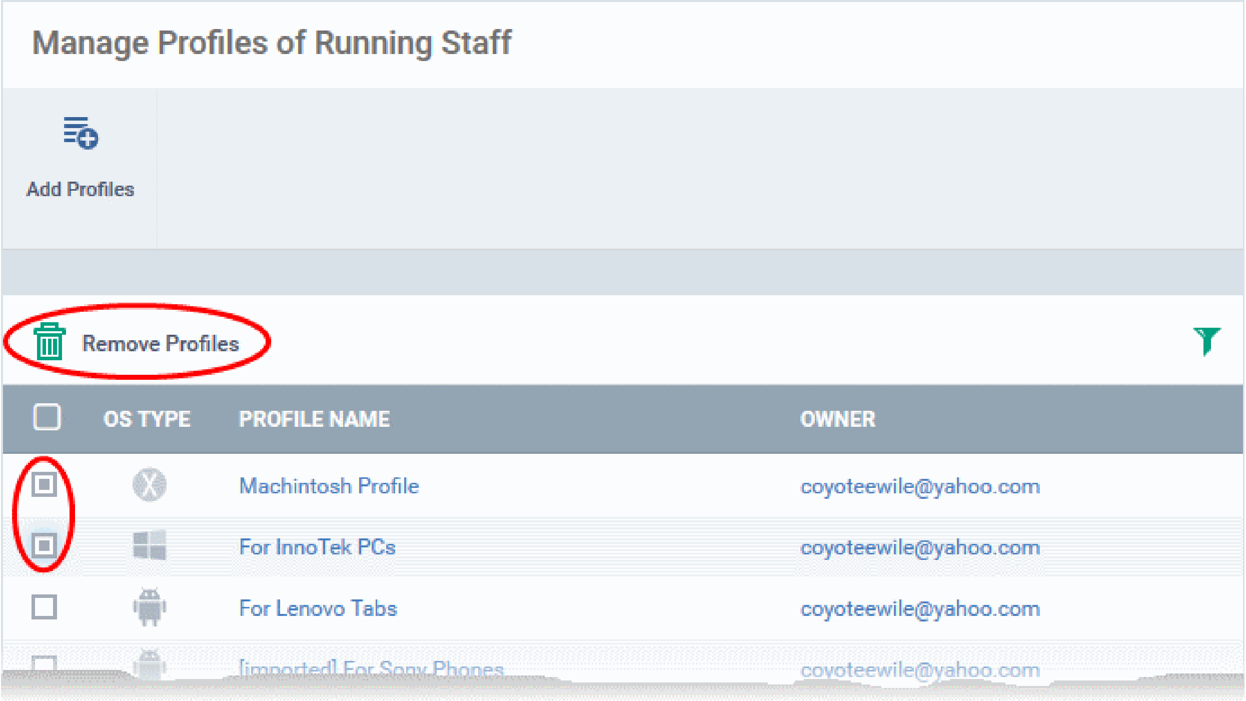
- Select the profiles to be applied to the devices in the group and click 'Save'.

> 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'



Manage Profiles of Running Staff

□	OS TYPE	PROFILE NAME	OWNER
☒		Machintosh Profile	coyoteewile@yahoo.com
☒		For InnoTek PCs	coyoteewile@yahoo.com
□		For Lenovo Tabs	coyoteewile@yahoo.com
□		[imported] For Sony Phones	coyoteewile@yahoo.com

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.

5.1.4. Remove a Device Group

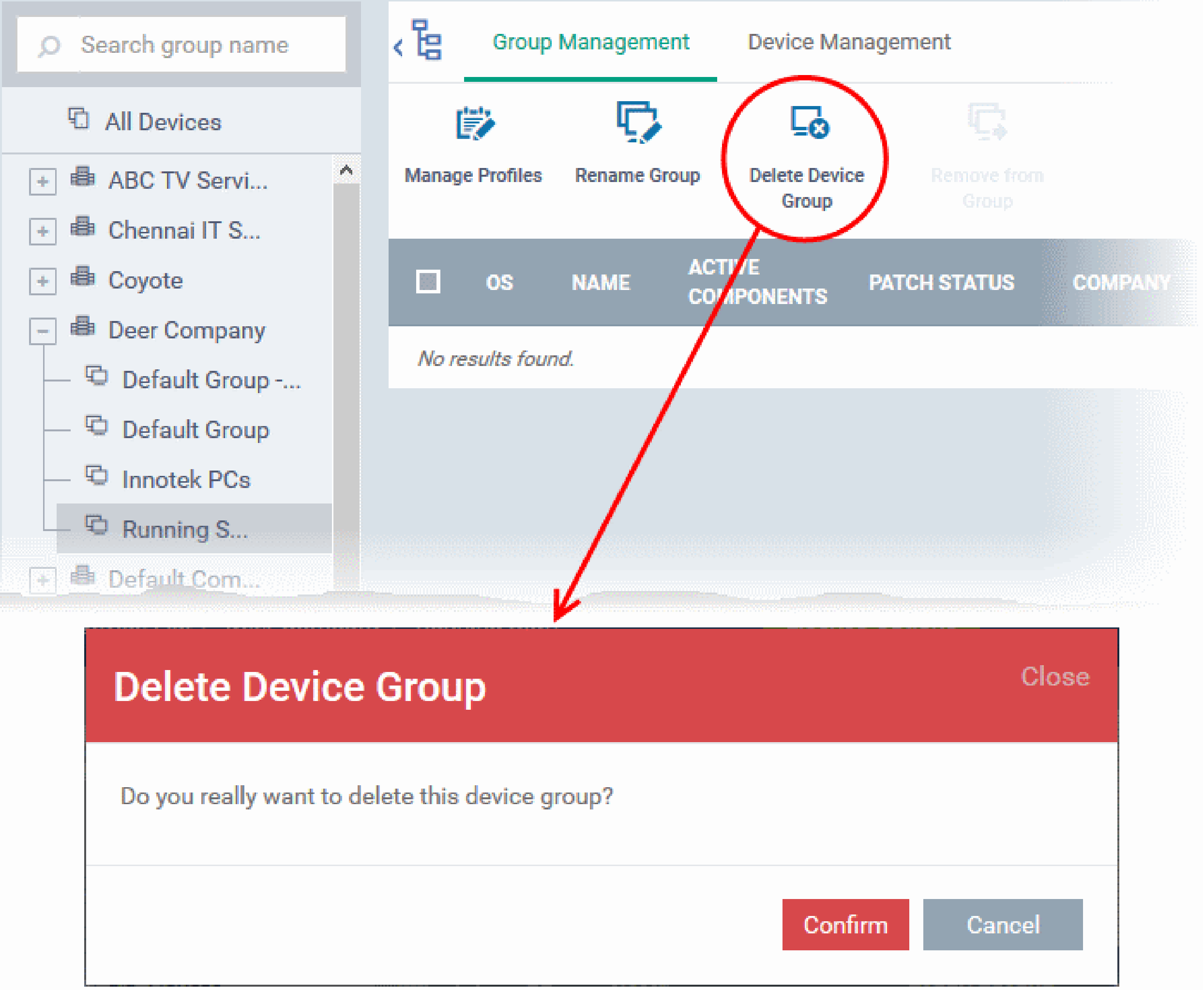
Admins can quickly remove unwanted device group(s) from ITSM. Note - you cannot delete a device group unless it is empty, so remove all member devices first.

To remove a device group

- Click the 'Devices' tab on the left and choose 'Device List'
- C1 MSP customers should choose the company/department whose group is to be edited
- Click the name of the group to be deleted from the tree structure at the left
- Click the 'Group Management' tab on the right

The 'Group Management' interface for the selected group will open.

- Ensure that there are no devices included in the group. See **removing devices from a group** in **Editing a Device Group** for more details.
- Click 'Delete Device Group' at the top.
- Alternatively, move your mouse over the group name and click the trash can icon.



No results found.

Delete Device Group

Close

Do you really want to delete this device group?

- Click 'Confirm' to apply your changes

The device group will be removed from ITSM.

5.2. Manage Devices

Note: If you haven't done so already, you should first **enroll users** then **enroll their devices**.

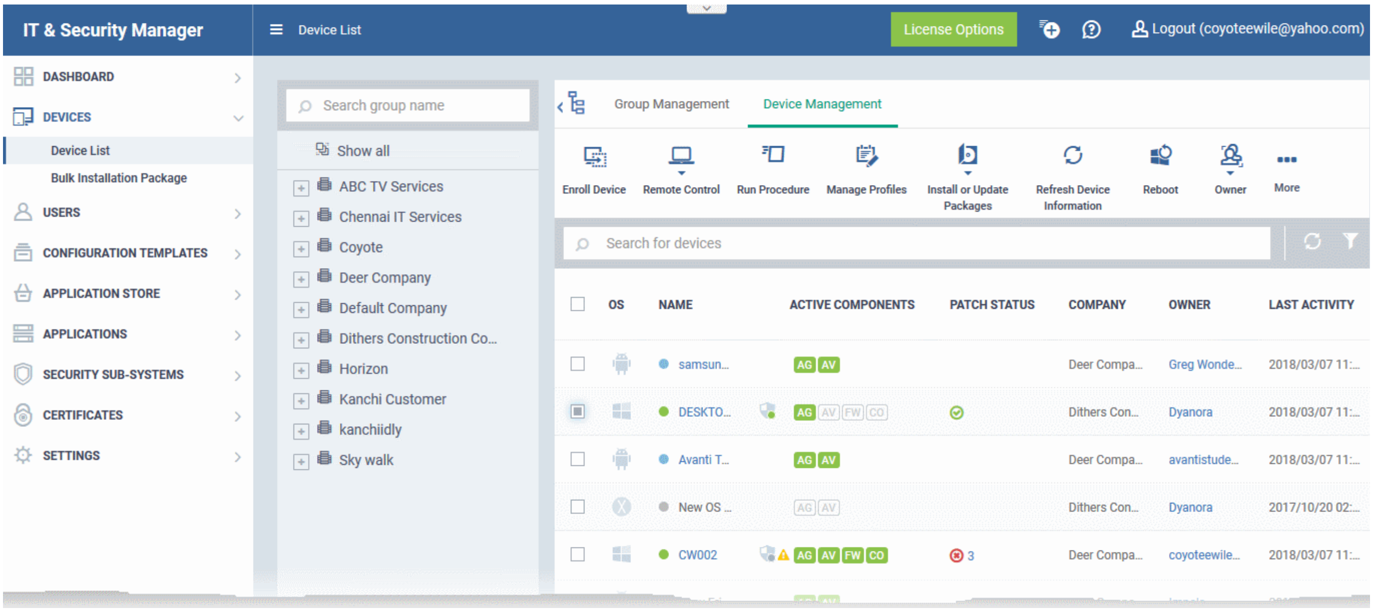
The 'Device Management' screen contains a full inventory of all mobile devices, Windows and Mac OS endpoints for a selected company/group. The screen also shows the device's connection and patch status, which security components are enabled, last activity and more. From this area you can:

- 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 and Mac OS 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 Management' interface

- Click the 'Devices' tab on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

The interface shows devices belonging to the company or group selected on the left. Select 'Show All' to view every device enrolled to ITSM.



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
	samsun...	AG AV		Deer Compa...	Greg Wonde...	2018/03/07 11:...
	DESKTO...	AG AV FW CO	✓	Dithers Con...	Dyanora	2018/03/07 11:...
	Avanti T...	AG AV		Deer Compa...	avantistude...	2018/03/07 11:...
	New OS ...	AG AV		Dithers Con...	Dyanora	2017/10/20 02:...
	CW002	AG AV FW CO	⊗ 3	Deer Compa...	coyoteewile...	2018/03/07 11:...

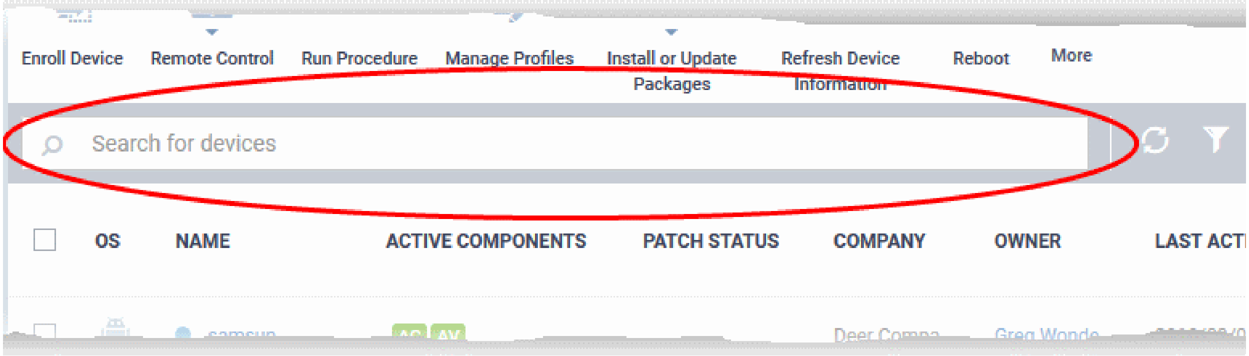
Devices - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system of the device.
Name	The label assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name. The circle to the left of the name shows the device's connection status: Gray - Device is not reachable. The connection maybe down or the endpoint is switched off. Blue - Slow connection. The device is connected but commands and messages may take some time to execute since the endpoint is busy. Green - Good connection. Commands should be executed in real time. Windows endpoints also have a shield icon to the right of their name. The shield has a colored circle on it which indicates the status of Comodo Client Security (CCS): White - CCS is not installed on the endpoint Gray - Outdated clients. Comodo Client Communication (CCS) and/or Comodo Client Security (CCS) on the endpoint require updates. Note. This status will only be shown on endpoints that have CCC 6.16 or higher and CCS 10.0 or higher installed. Red - The endpoint is at risk. A security component (AV, FW or Containment) may have been disabled by the user. Amber - The endpoint needs attention. The virus signature database might be out-dated or the endpoint needs to be re-started after installation of CCS. Green - The endpoint is secure. All installed components are up and running. Blue - CCS is running in 'Silent Mode'.

	Note: CCS allows users to switch it o 'Silent Mode' if they do not want to be disturbed while carrying out important tasks or when playing games. Alerts and notifications are suppressed and operations that could interfere with their work are postponed. ⚠ - Communication with CCS on the endpoint has been lost. • Click the device name to open the device details interface. See **Manage Windows Devices**, **Manage Mac OS Devices** and **Manage 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. These components are installed automatically when a profile featuring the components is installed. • Mac OS endpoints - Available components are - Agent and AV
Patch status	• Indicates the number of patches available for Windows endpoints. Patch status icons are as follows: ✓ - No patches required. All patches are up-to-date. ✖ - Critical patches are available. The number to the right shows how many are pending. Click the number to view and manage the patches. See **View and Install Windows and 3rd Party Application Patches** for more details. ⚠ - Optional patches are available. Click the number to the right to view and manage the patches.
Company	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	The device user. Click the user name to open the 'View User' interface. See **View User Information** for more details.
Last Activity	The date and time at which the device last communicated with the ITSM agent.

- Click a column header to sort the table in ascending/descending order of items in that column.

Search and Filter Options

- The search box at the top allows you filter devices based on any parameter in the table.
- Alternatively, you can click the funnel button ▼ on the right to open filter options.



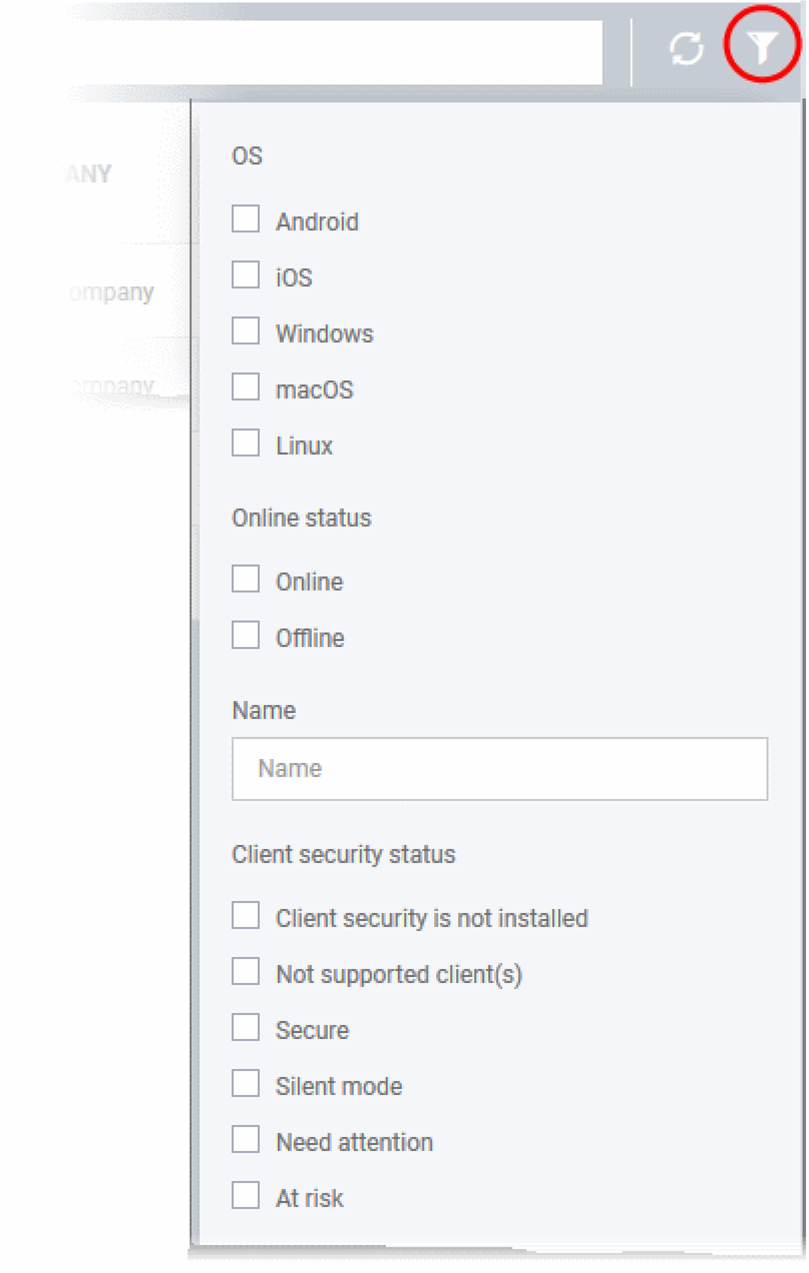
- Enter your search criteria and click the magnifying glass to view devices matching the criteria.

You can search using the following criteria:

- OS - Enter the operating system of the devices you wish to view.
- Online/Offline status - Type 'Online' or 'Offline'
- Name - Enter the name of the device in part or full
- CSS Status - Type one of the following values as required:
  - Not installed
  - Not supported
  - Secure
  - Silent mode
  - Need attention
  - At risk
- Company - Enter the customer company name in part or full
- Owner - Enter the name/email address of the device owner in part or full
- Last Activity - Enter a date in YYYY/MM/DD format to filter devices by the time of their last connection with ITSM.
  - You can use operators such as '<, '>', '<=' and '>=' to view devices before or after the date.
  - To view devices within a range, enter start and end dates as follows: YYYY/MM/DD - YYYY/MM/DD

- Clear any search terms and click the magnifying glass to view all devices again.

You can also access filters by clicking the funnel button ▼ on the right:



OS

□ Android

□ iOS

□ Windows

□ macOS

□ Linux

Online status

□ Online

□ Offline

Name

Name

Client security status

□ Client security is not installed

□ Not supported client(s)

□ Secure

□ Silent mode

□ Need attention

□ At risk

- 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 Device Logs
- Managing Mac OS Devices
  - Viewing and Editing Mac OS Device Name
  - Viewing Summary Information
  - Managing Installed Applications
  - Viewing and Managing Profiles Associated with the Device
  - Viewing Mac OS Packages Installed on the Device through ITSM
  - Viewing and Managing Device Group Memberships
- Managing Android / iOS Devices
  - Viewing and Editing Device Name
  - Viewing Summary Information
  - Managing Installed Applications
  - Viewing and Managing Profiles Associated with the Device
  - Viewing Sneak Peak Pictures to Locate Lost Device
  - Viewing the Location of the Device
  - Viewing and Managing Device Group Memberships

5.2.1. Manage Windows Devices

The Windows device details page allows you to view device hardware and software details, installed components and network connection details. You can also manage the configuration profiles in effect on the endpoint, deploy Windows patches, and manage the device's group membership.

View details and manage a Windows device

- Click 'Devices' > 'Device List' on the left
- Click the 'Device Management' tab above the main configuration pane

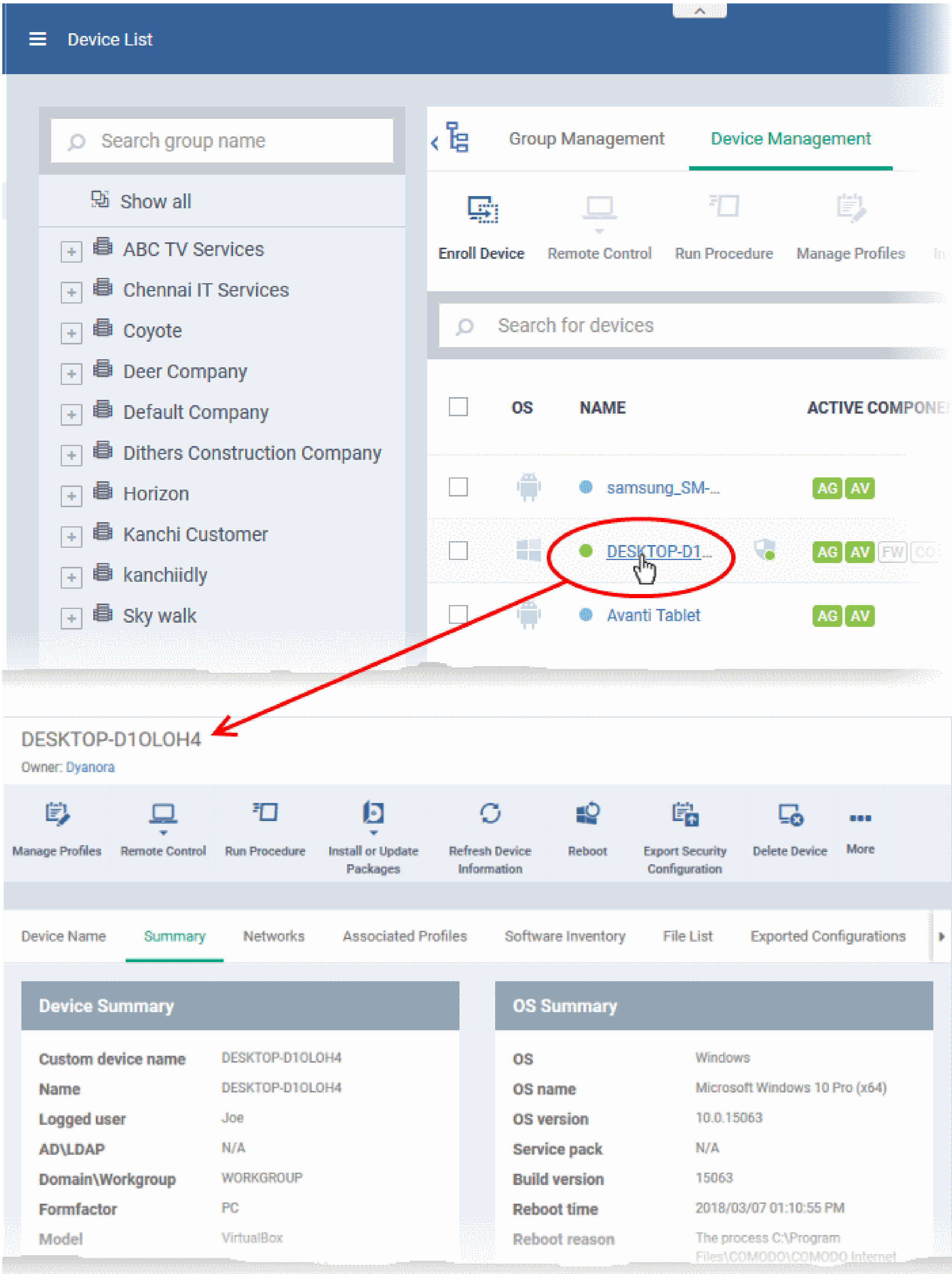
The interface shows devices belonging to the company or group selected on the left.

  - Select a company and choose a group under it to view devices in that group

  Or

  - Select 'All Devices' to view every device enrolled to ITSM

- Click on the name of any Windows device to open the 'Windows device details' pane:



☐	OS	NAME	ACTIVE COMPONE
☐		samsung_SM-...	AG AV
☐		DESKTOP-D1...	AG AV FW CO
☐		Avanti Tablet	AG AV

DESKTOP-D1OLOH4

Owner: Dyanora

Device Summary

Custom device name	DESKTOP-D1OLOH4
Name	DESKTOP-D1OLOH4
Logged user	Joe
AD\LDAP	N/A
Domain\Workgroup	WORKGROUP
Formfactor	PC
Model	VirtualBox

OS Summary

OS	Windows
OS name	Microsoft Windows 10 Pro (x64)
OS version	10.0.15063
Service pack	N/A
Build version	15063
Reboot time	2018/03/07 01:10:55 PM
Reboot reason	The process C:\Program Files\COMODO\COMODO Internet

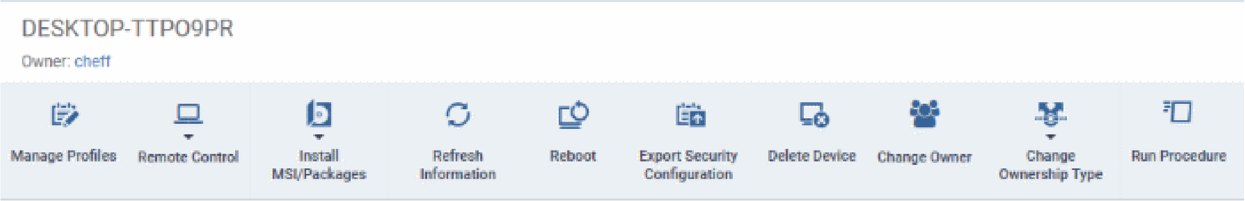
The details screen of the selected device contains a maximum of thirteen tabs. The 'Summary' tab is open by default.

- **Device Name** - The device label. You can change this as per your preference. See **Viewing and Editing Device Name** for more details.
- **Summary** - General details about the device, including device and OS information and performance

metrics like CPU, RAM, network and disk usage. See **Viewing Summary Information** for more details.

- **Hardware** - Hardware configuration of the selected device. See **Viewing Hardware Information** for more details. Note - the 'Hardware' tab will be available only if Comodo RMM agent is installed on the device. See **Remotely Installing and Updating Packages on Windows Devices** for more details.
- **Networks** - The device's network details. This includes its MAC address, its IP address, currently connected networks and more. See **Viewing Network Information** for more details.
- **Associated Profiles** - Details of the profiles deployed on the device. See **Viewing and Managing Profiles Associated with the Device** for more details.
- **Software Inventory** - Applications installed on the device. See **Viewing Applications Installed on the Device** for more details.
- **File List** - Inventory of files on the device along with their file rating ('Unrecognized', 'Trusted' or 'Malicious'). See **Viewing List of Files in the Device** for more details. Note - the 'File List' tab will be available only if Comodo Client Security is installed on the device. See **Remotely Installing and Updating Packages on Windows Devices** for more details.
- **Exported Configurations** - Saved Comodo Client Security configuration files. See **Viewing CCS Configurations Exported from the Device** for more details. Note - the 'Exported Configurations' tab will be available only for devices with Comodo Client Security installed. See **Remotely Installing and Updating Packages on Windows Devices** for more details.
- **MSI Installation State** - .MSI executables that have been installed on the device via ITSM. See **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. See **Viewing and Installing Windows Patches** for more details.
- **Antivirus Scan History** - A history of threats identified on all devices and the actions taken by ITSM in response. See **Viewing Antivirus Scan History** for more details. Note - the 'Antivirus Scan History' tab will be available only if Comodo Client Security is installed on the device. See **Remotely Installing and Updating Packages on Windows Devices** for more details.
- **Groups** - A list of device groups to which the endpoint belongs. You can also manage group membership from here. See **Viewing and Managing Device Group Memberships** for more details.
- **Logs** - View event logs from activities recorded on the device. See **Viewing Device Logs** for more details.
    - **Alert Logs** - Alerts generated because of a breach of monitoring conditions or because of a procedure deployment.
    - **Monitoring Logs** - Monitoring breaches that occurred fin the past 24 hours on the endpoint.
    - **Script Logs** - Script procedures that were run on the Windows device manually and/or automatically via scheduling in a profile.
    - **Patch Logs** -Patch procedures that were run on the Windows device manually and/or automatically via scheduling in a profile.

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 security configuration profiles to/from the device. These profiles will be in addition to any group profiles applied to the device. See **Assigning Configuration Profiles to Selected Devices** for more details.
- **Remote Control** - Access the endpoint over a remote desktop connection. There are two ways to do this:

- **Comodo Remote Control Viewer**: Click 'Remote Control' > 'With Comodo Remote Control' to download and install the app. After installation, selecting 'With Comodo Remote Control' will open the desktop of the endpoint, allowing you to take remote control. Refer to '**Remote Management of Windows Devices**' for more details.
- **Remote Monitoring and Management (RMM) Console**: The RMM Console allows you to 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.

- **Install MSI Packages** - Remotely install Comodo endpoint security software and third party Windows packages. See **Remotely Installing Packages onto Windows Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. See **Updating Device Information** for more details.
- **Reboot** - Remotely restart the device. See **Rebooting a Selected Device** for more details.
- **Export Configurations** - Export the device's 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. See **Importing Windows Profiles** for more details.
- **Delete Device** - Removes the device from ITSM. See **Removing a Device** for more details.
- **Change Owner** - Change the user with whom the device is associated. See **Changing a Device's Owner** for more details.
- **Change Ownership Type** - Changes the 'Bring Your Own Device' (BYOD) status of the device. See '**Changing the ownership status of a Device**' for more details.
- **Run Procedure** - Apply procedures on a Windows device. See '**Applying Procedures for Windows Devices** for more details.

5.2.1.1. View and Edit Device Name

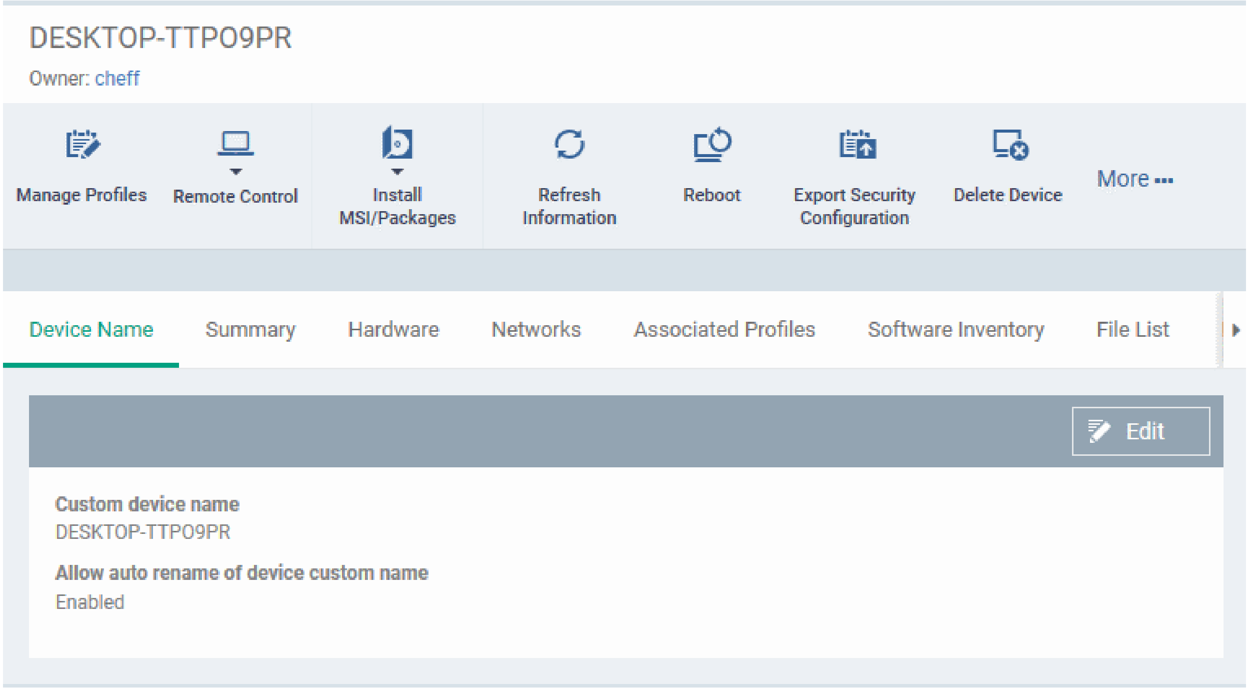
- Enrolled devices are listed by the name assigned to them by their owner.
- If no name was assigned then the actual device name or model number will be used.
- Admins can change the device name according to their preferences. If you change a device name, the name will apply in ITSM but will not change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

To change a device name

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

  Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Device Name' tab

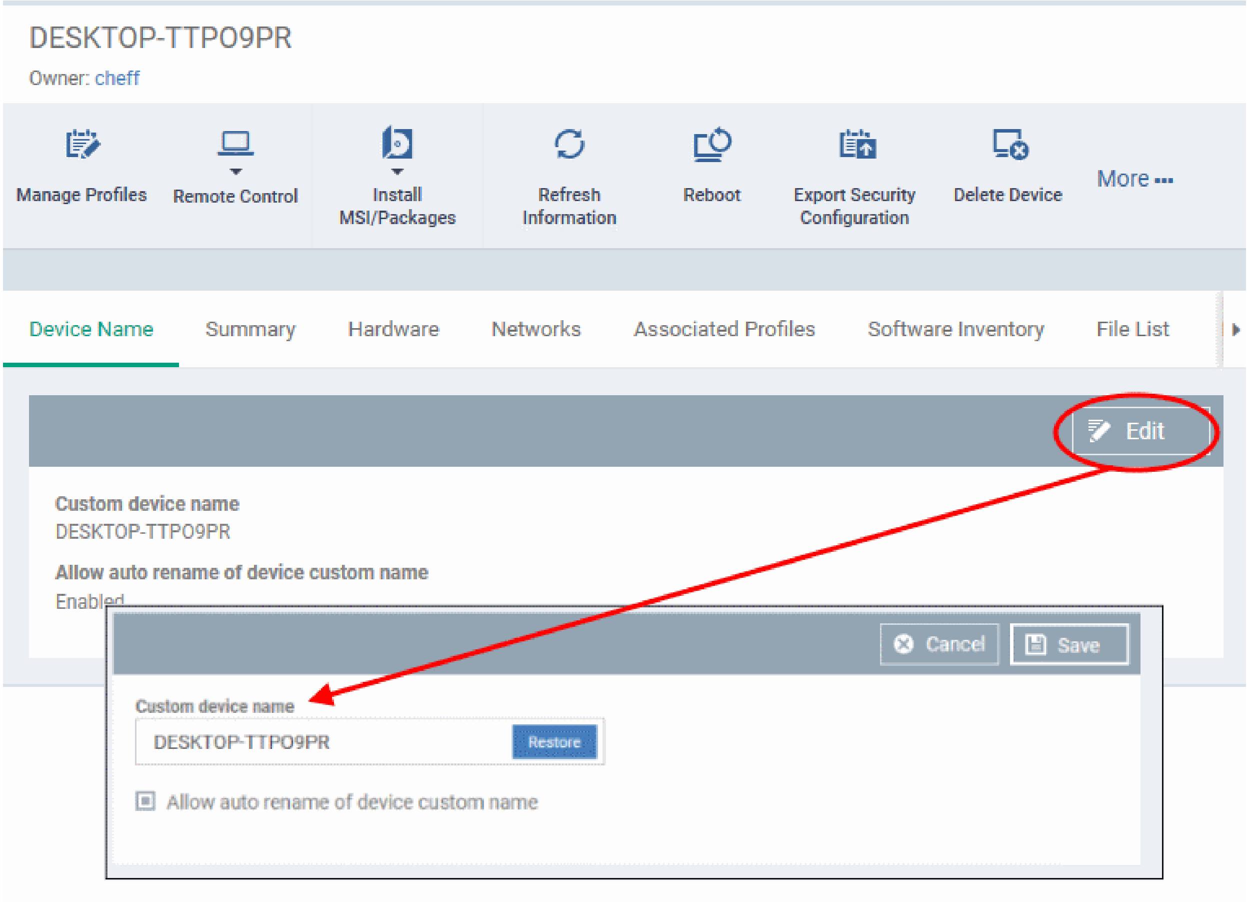


Custom device name
DESKTOP-TTPO9PR

Allow auto rename of device custom name
Enabled

- 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.



Custom device name
DESKTOP-TTPO9PR

Allow auto rename of device custom name
Enabled

Custom device name
DESKTOP-TTPO9PR

□ Allow auto rename of device custom name

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'.

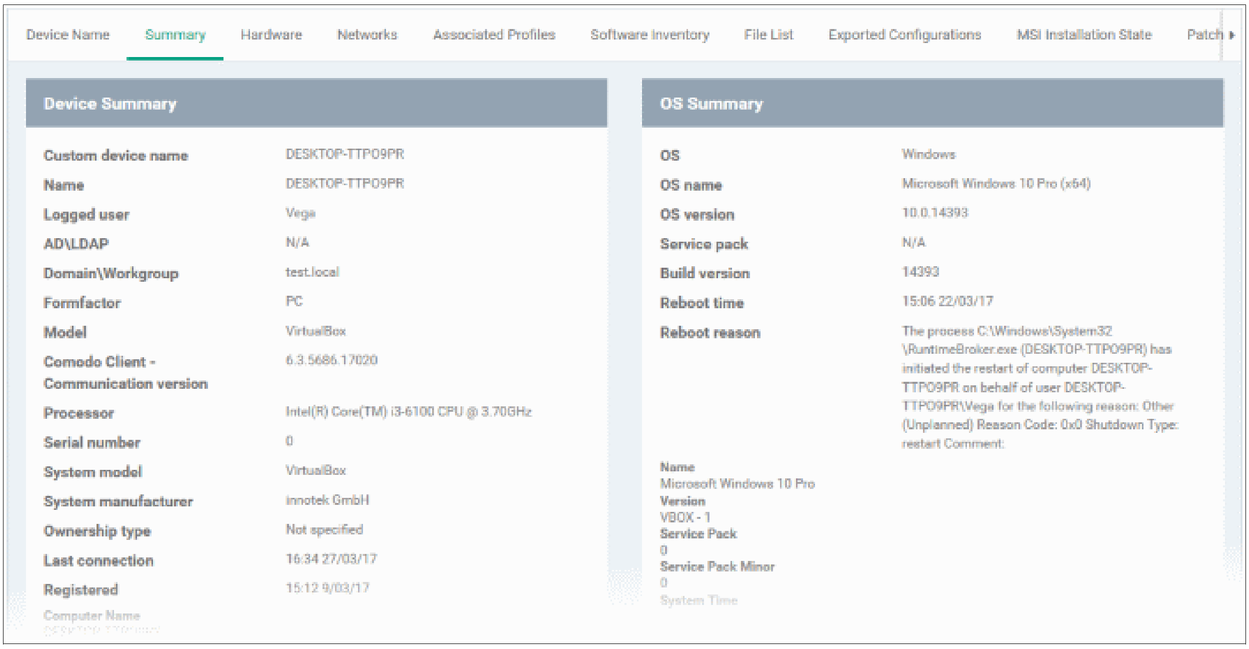
5.2.1.2. View Summary Information

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then open the 'Summary' tab (if it is not already open).



Device Summary

Custom device name	DESKTOP-TTPO9PR
Name	DESKTOP-TTPO9PR
Logged user	Vega
AD\LDAP	N/A
Domain\Workgroup	test.local
Formfactor	PC
Model	VirtualBox
Comodo Client - Communication version	6.3.5686.17020
Processor	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
Serial number	0
System model	VirtualBox
System manufacturer	innotek GmbH
Ownership type	Not specified
Last connection	16:34 27/03/17
Registered	15:12 9/03/17

Computer Name

OS Summary

OS	Windows
OS name	Microsoft Windows 10 Pro (x64)
OS version	10.0.14393
Service pack	N/A
Build version	14393
Reboot time	15:06 22/03/17
Reboot reason	The process C:\Windows\System32 \RuntimeBroker.exe (DESKTOP-TTPO9PR) has initiated the restart of computer DESKTOP-TTPO9PR on behalf of user DESKTOP-TTPO9PR\Vega for the following reason: Other (Unplanned) Reason Code: 0x0 Shutdown Type: restart Comment:

Name
Microsoft Windows 10 Pro
Version
VBOX - 1
Service Pack
0
Service Pack Minor
0
System Time

- **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, numbers of 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.

5.2.1.3. View Hardware Information

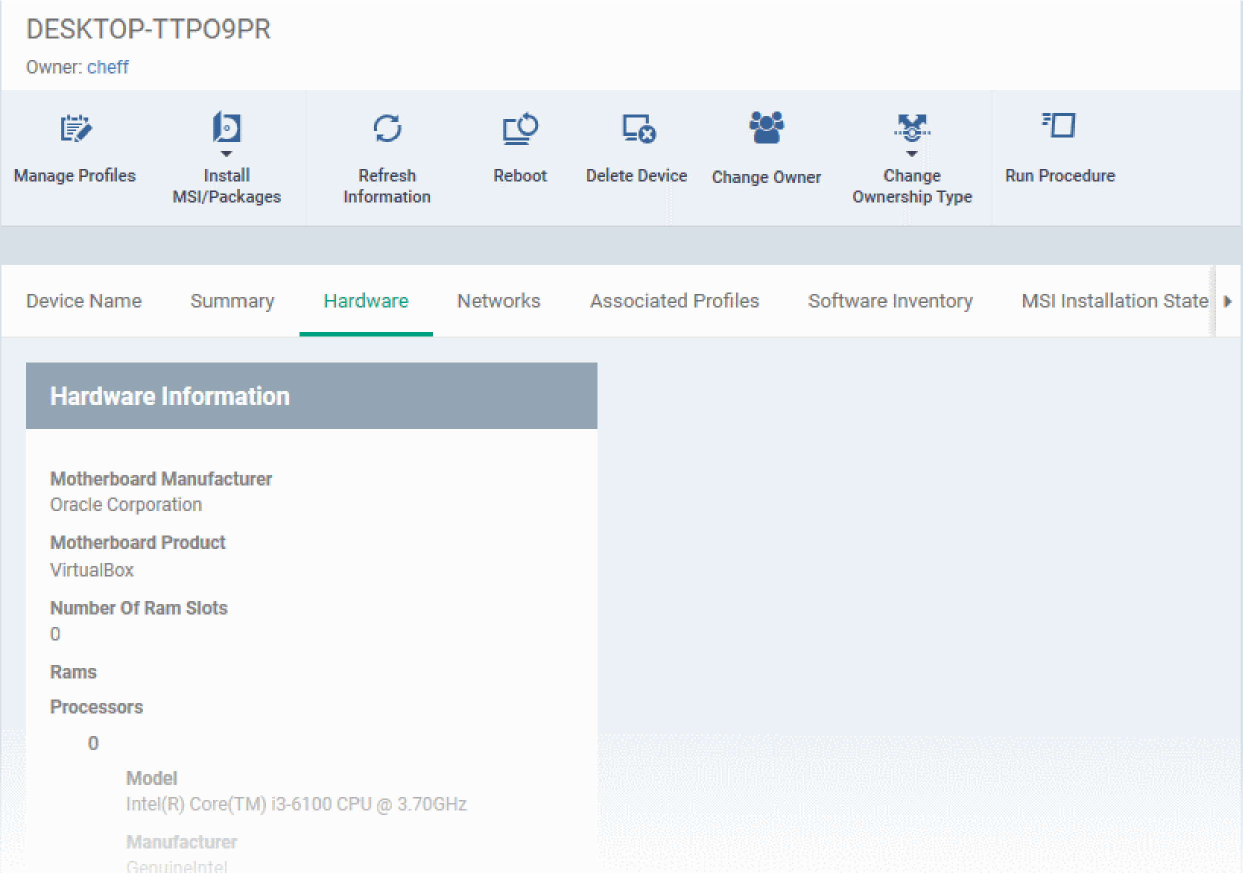
This screen contains basic details about the hardware component of the Windows endpoint.

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

To view a device's hardware details

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

    Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Hardware' tab


DESKTOP-TTPO9PR

Owner: cheff

Hardware Information

Motherboard Manufacturer
Oracle Corporation

Motherboard Product
VirtualBox

Number Of Ram Slots
0

Rams

Processors

0

Model
Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz

Manufacturer
GenuineIntel

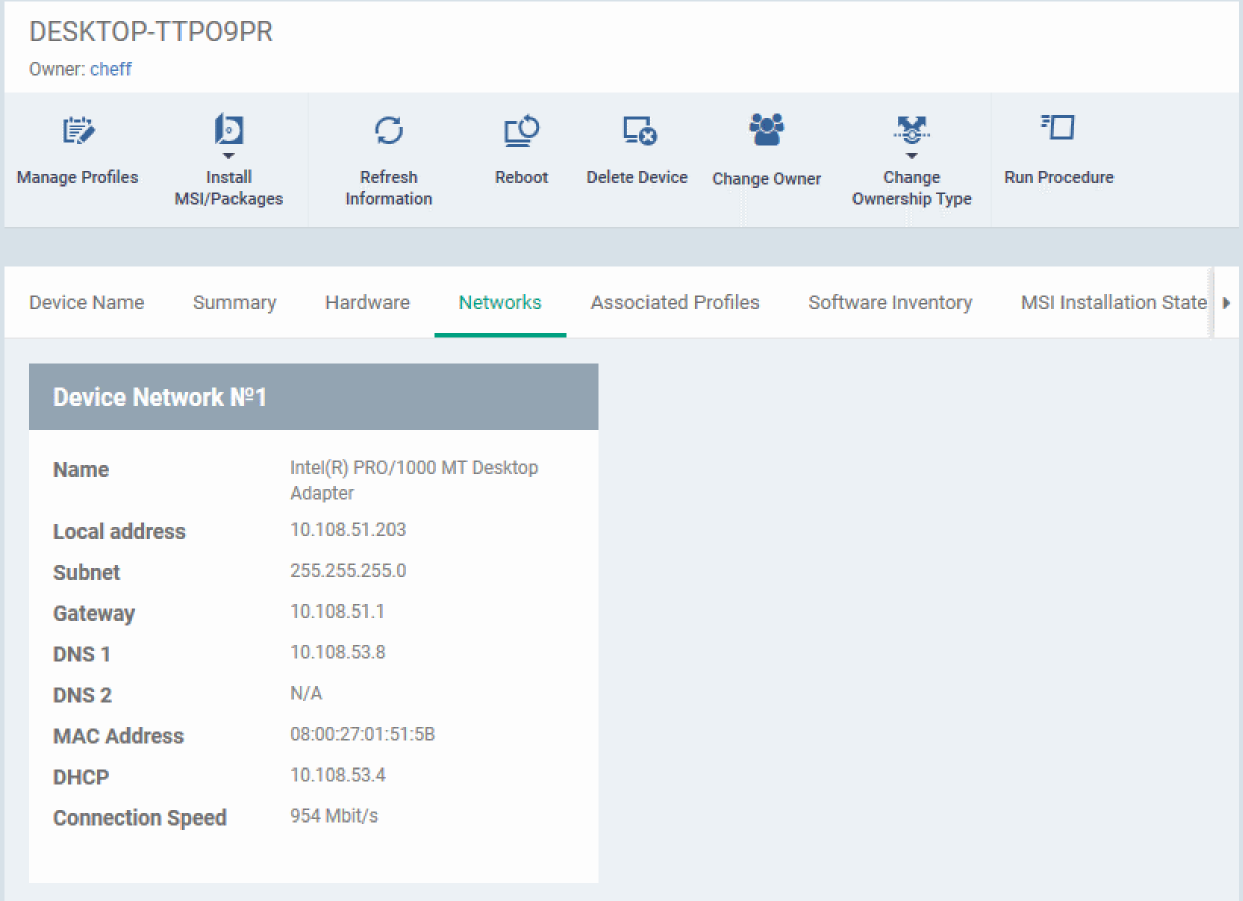
5.2.1.4. View Network Information

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

To view a device's network details

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

  Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Networks' tab



Device Network №1

Name	Intel(R) PRO/1000 MT Desktop Adapter
Local address	10.108.51.203
Subnet	255.255.255.0
Gateway	10.108.51.1
DNS 1	10.108.53.8
DNS 2	N/A
MAC Address	08:00:27:01:51:5B
DHCP	10.108.53.4
Connection Speed	954 Mbit/s

5.2.1.5. View and Manage 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:

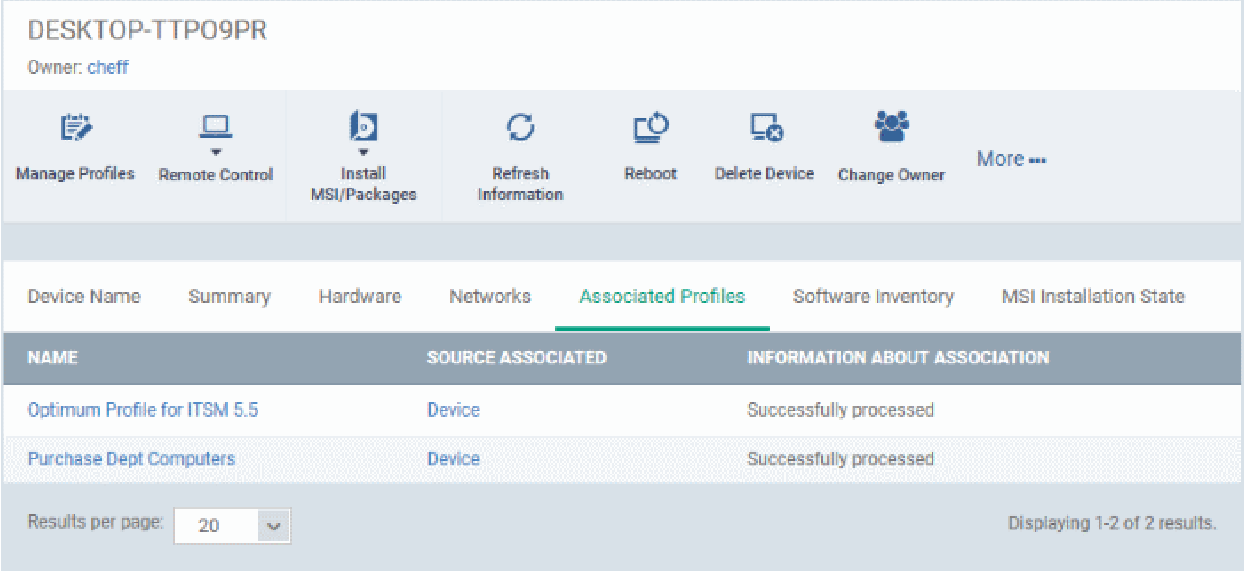
- Because it is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- Because the device belongs to a device group
- Because the user belongs to a user group

For more details on profiles and groups of profiles, see **Configuration Profiles**.

To view and manage the profiles associated with a device

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Associated Profiles' tab



NAME	SOURCE ASSOCIATED	INFORMATION ABOUT ASSOCIATION
Optimum Profile for ITSM 5.5	Device	Successfully processed
Purchase Dept Computers	Device	Successfully processed

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. See **Editing Configuration Profiles** for more details.
Source Associated	Indicates the source through which the profile was applied to the device. Configuration profiles can be applied to a device in different ways: • Profiles can be directly applied to the device. See **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. See **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. See **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. See **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. See **Assigning Configuration Profile to Selected Devices** for more details.

5.2.1.6. View Applications Installed on a Device

The 'Software Inventory' tab displays a list of applications and programs installed on an endpoint.

To view the applications installed on a device

- Click the 'Devices' link on the left and choose 'Device List'

- Click the 'Device Management' tab at the top of the main configuration pane

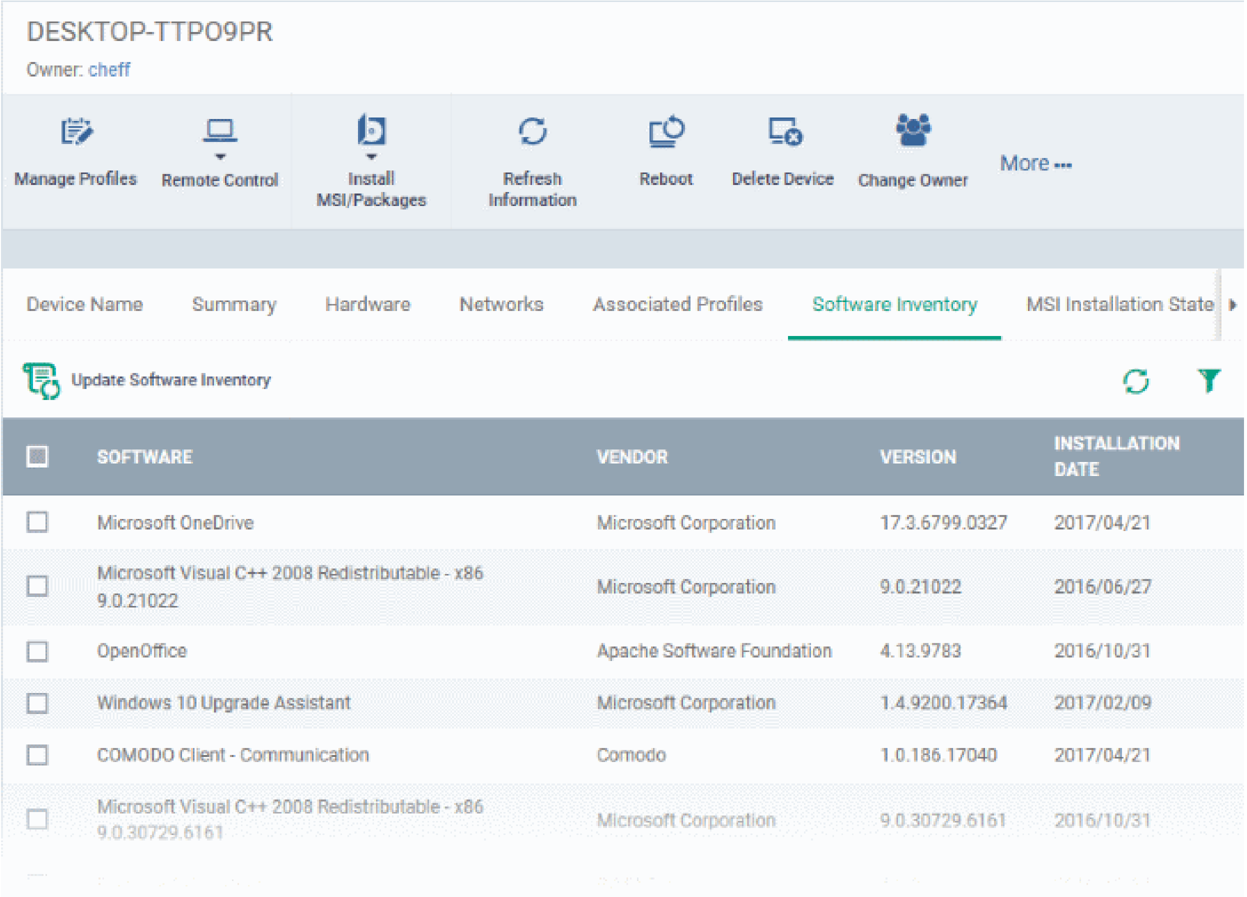
The interface displays devices belonging to the company or group selected on the left.

- Select a company and choose a group under it to view devices in the group

  Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click the name of any Windows device then select the 'Software Inventory' tab:



☐	SOFTWARE	VENDOR	VERSION	INSTALLATION DATE
☐	Microsoft OneDrive	Microsoft Corporation	17.3.6799.0327	2017/04/21
☐	Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022	Microsoft Corporation	9.0.21022	2016/06/27
☐	OpenOffice	Apache Software Foundation	4.13.9783	2016/10/31
☐	Windows 10 Upgrade Assistant	Microsoft Corporation	1.4.9200.17364	2017/02/09
☐	COMODO Client - Communication	Comodo	1.0.186.17040	2017/04/21
☐	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161	2016/10/31

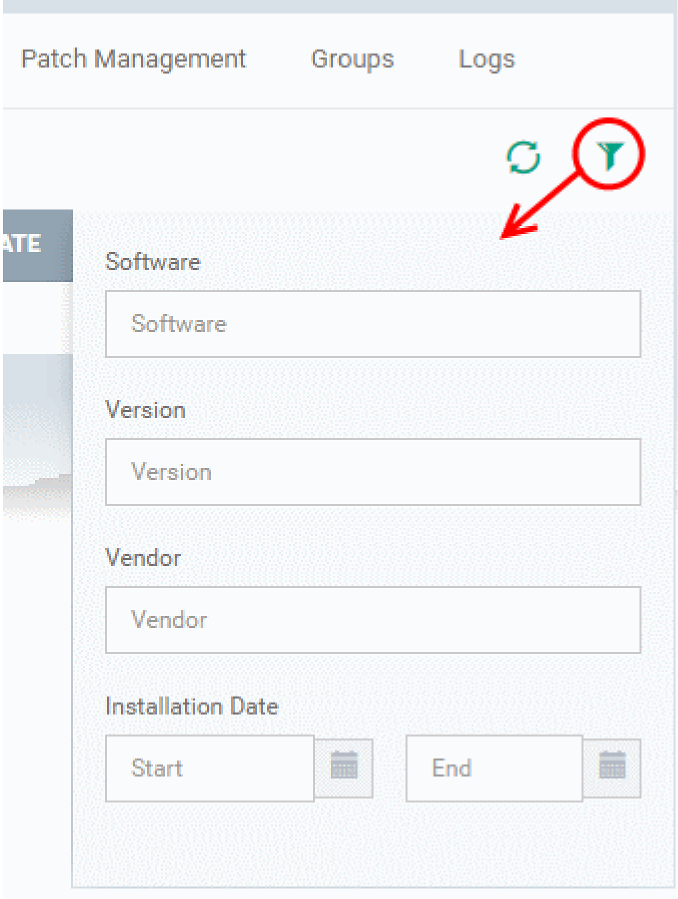
Installed Apps - Column Descriptions	
Column Heading	**Description**
Software	The name of the application. Click the application name to see a list of all devices on which the application is installed.
Vendor	The publisher of the application.
Version	The version number of the application.
Installation Date	The date at which the application was installed.

- Click 'Update Software Inventory' to retrieve the latest list of applications from the endpoint

Sorting, Search and Filter Options

- Click the 'Software', 'Vendor' and 'Version' column headers to sort items in alphabetical or ascending/descending order

- Click the funnel button on the right to open filter options



- Type search criteria in the search fields to find an application based on name, version and/or vendor.
- Enter 'Start' and 'End' dates to search for applications installed during a certain period of time.
- Click 'Apply' to run your filter
- To display all items again, remove all search terms and click 'Apply'.
- By default, 20 results are shown per page. Click the arrow next to 'Results per page' to increase the number up to 200.

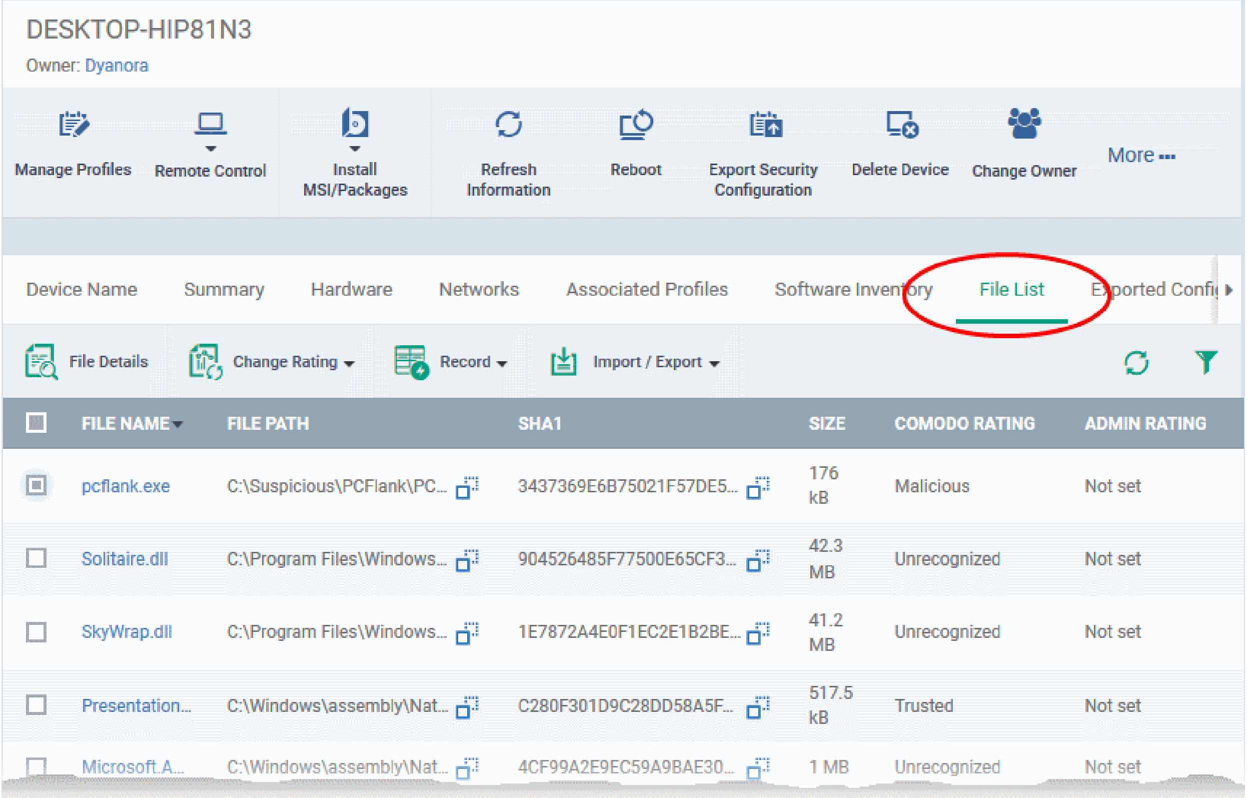
5.2.1.7. View the Files on a Device

The 'File List' tab displays executable files found on a Windows device along with their trust rating.

To view files on a Windows device:

- Click the 'Devices' tab on the left and choose 'Device List'
- Click the 'Device Management' tab
    - Select the Company and choose the group under it to view the list of devices in that group

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'File List' tab:



☐	FILE NAME	FILE PATH	SHA1	SIZE	COMODO RATING	ADMIN RATING
☐	pcflank.exe	C:\Suspicious\PCFlank\PC... ⧉	3437369E6B75021F57DE5... ⧉	176 kB	Malicious	Not set
☐	Solitaire.dll	C:\Program Files\Windows... ⧉	904526485F77500E65CF3... ⧉	42.3 MB	Unrecognized	Not set
☐	SkyWrap.dll	C:\Program Files\Windows... ⧉	1E7872A4E0F1EC2E1B2BE... ⧉	41.2 MB	Unrecognized	Not set
☐	Presentation...	C:\Windows\assembly\Nat... ⧉	C280F301D9C28DD58A5F... ⧉	517.5 kB	Trusted	Not set
☐	Microsoft.A...	C:\Windows\assembly\Nat... ⧉	4CF99A2E9EC59A9BAE30... ⧉	1 MB	Unrecognized	Not set

File List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the application/executable file.
File Path	The installation location of the application at the endpoint. • Clicking the ⧉ icon copies the path to the clipboard.
SHA1	Displays the SHA1 hash value of the executable file. • Clicking the ⧉ icon copies the hash value to the clipboard.
Size	The size of the executable file.
Comodo Rating	Indicates the rating of the file as per the Comodo File Look-up service, reported by the CCS installations at the endpoints
Admin Rating	Indicates the rating of the file as manually set by the administrator, if any.

Comodo Client Security monitors all file activity on a Windows endpoint. New executables are scanned against the Comodo files database and rated as 'Unrecognized', 'Trusted' or 'Malicious'. You can configure this behavior in the 'File Rating settings' section of the configuration profile applied to the device. See **File Rating settings** in **Creating a Windows Profile** for more details.

Unrecognized Files

Files that could not be identified as 'Trusted' or 'Malicious' by Comodo Client Security (CCS) are reported as 'Unrecognized' to ITSM . Administrators can review these files and can manually rate them as 'Trusted' or 'Malicious' as required.

Trusted Files

Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, Comodo Client security (CCS) on an endpoint will check the file against Comodo's master whitelist and blacklists. The file will be awarded 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 - Admins can assign a 'Trusted' rating to files from the Application Control interface
- User Rating - Users can assign a 'Trusted' rating to files at the local CCS installation in two ways:
  - In response to an alert. If an executable is unknown then it may generate a HIPS alert on the local endpoint. Users could choose 'Treat this as a Trusted Application' at the alert
  - The user can assign 'Trusted' rating to any file from the 'File List' interface.

  CCS creates a hash of all files assigned 'Trusted' status by the user. In this way, even if the file name is changed later, the file will retain its trusted status as the hash remains same. This is particularly useful for developers who are creating new applications that, by their nature, are unknown to the Comodo safe list.

Malicious Files

Files identified as malicious by the File Look-Up Service (FLS) will not be allowed to run by default. These files are reported as malware to ITSM.

The File List screen

Possible file ratings are 'Unrecognized', 'Trusted' or 'Malicious'. Administrators can manually set the file rating at their discretion.

- Files rated as 'Trusted' are allowed to run.
- Files rated as 'Malicious' are quarantined and not allowed to run.
- Files rated as 'Unrecognized' are run inside the container - an isolated operating environment. Contained applications are not permitted to access files or user data on the host machine.

Any ratings set by the administrator are propagated to all enrolled endpoints.

Admins can also view a history of purged files. Purged files are those which existed on devices at one point in time, but are not currently present on any device. To view these files, apply the filter named 'Show Purged Files'. See the explanation of **Filter Options** given below.

> **Tip**: if you wish to see all files across all managed devices, please view the '**Applications**' and '**Application Control**' interfaces. See '**Applications** > **Mobile Applications**' to view applications in mobile devices.

Sorting, Search and Filter Options

- Click any column header to sort items in alphabetical order
- Click the funnel icon to open more filter options:
- Use the check-boxes to show or hide purged, non-executable, hidden or unrecognized files.
- Use the search fields to filter by file name, file path or SHA1 hash value. You can also filter by file size and the number of devices on which the file is present.
- Use the drop-down boxes to filter items by Comodo and/or Admin rating
- To display all items again, clear any search filters and click 'OK'.

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

Managing Applications

The 'File List' interface allows you to:

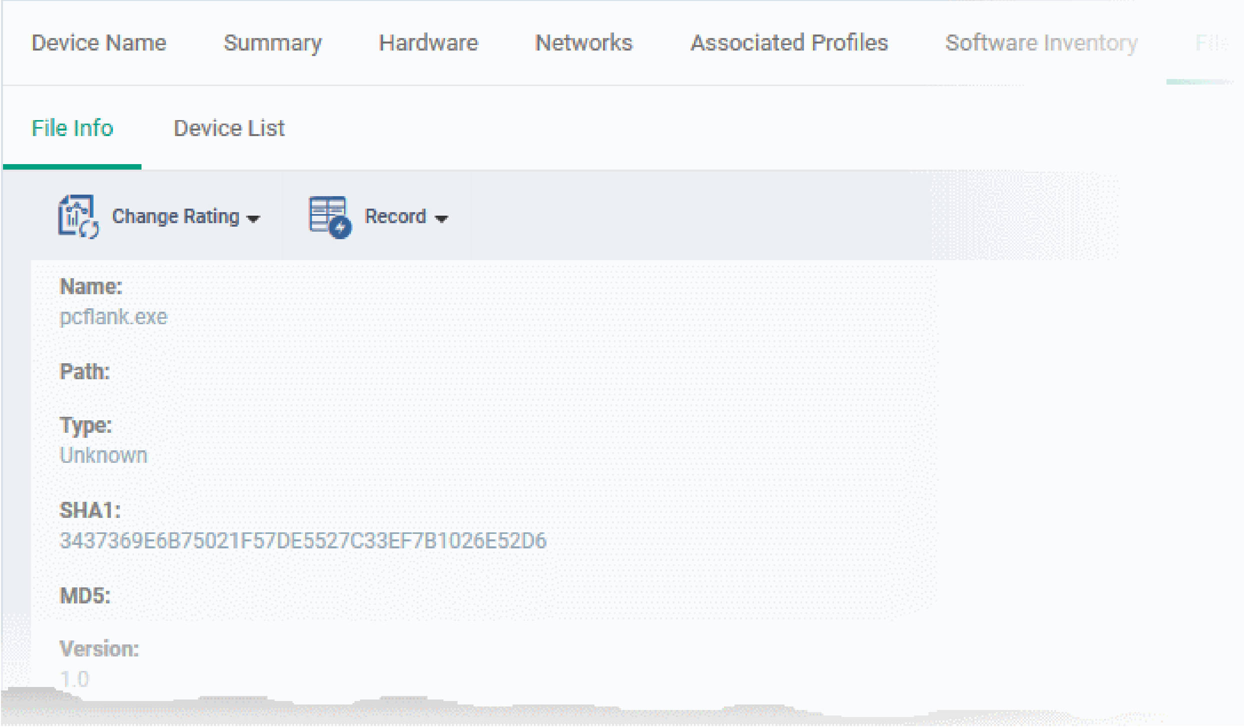
- View the details of files in the list
- View Process Activities of a File
- Assign Admin rating to a file
- Hide/Display selected files in the list
- Export the list of selected files to a CSV file
- Remove files from the list

View file details

- Simply click on a file in the list or select a file and click 'File Details' at the top.
- The File Details screen contains two tabs:
    - **File info** - Shows basic file details and the devices on which the file is present. You can also change the trust rating of the file in this area.
    - **Device List** - Displays the list of managed Windows devices on which the file is discovered. The 'Device List' interface also allows you to view the process activities of the file in respective devices.

File info

- The file info screen shows file name, installation path, file type, version, size, hash values and the date the file was first encountered. The screen also shows the file's trust rating and the number of endpoints on which the file is present.



Name:
pcflank.exe

Path:

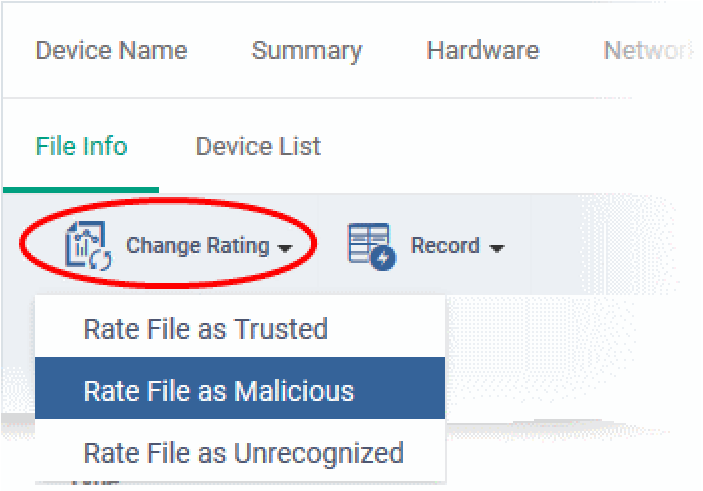
Type:
Unknown

SHA1:
3437369E6B75021F57DE5527C33EF7B1026E52D6

MD5:

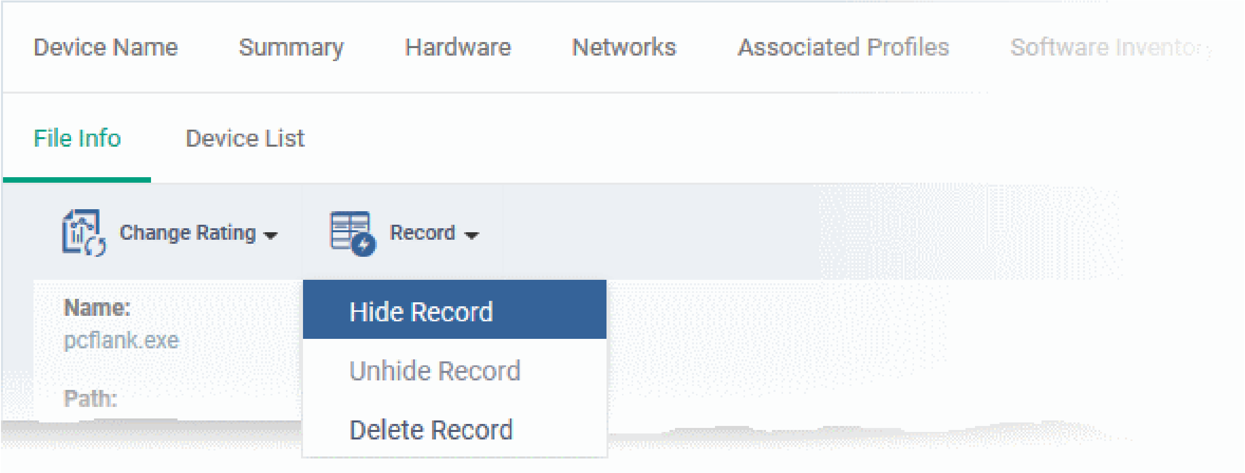
Version:
1.0

- The 'Change Rating' button allows you to manually set the file's rating as 'Trusted', 'Malicious' or 'Unrecognized':



The new rating will be sent to all endpoints.

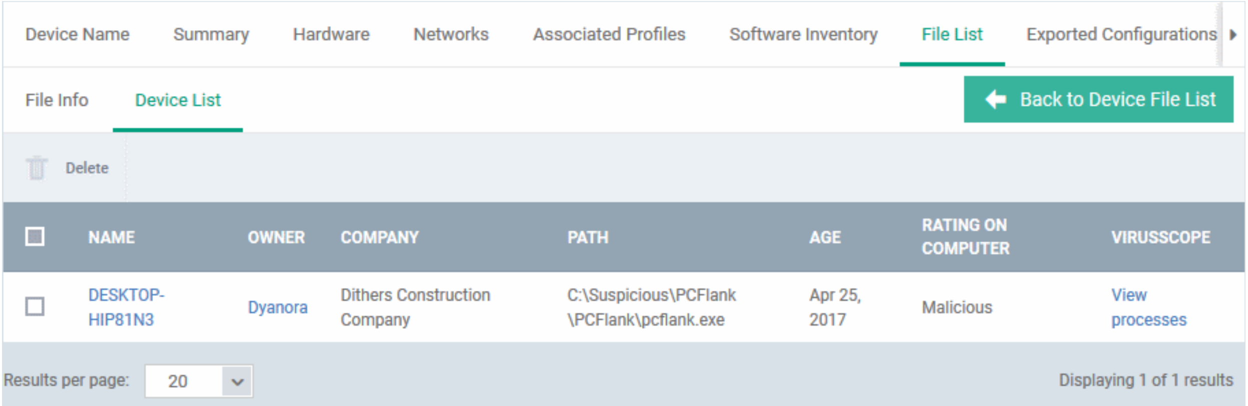
- The 'Record' button lets you hide, display or remove the file from the 'File List' screen.



Name:
pcflank.exe
Path:

Device List Screen

- The device list screen shows the list of endpoints on which the item was discovered. The screen also shows the installation path, the installation date and the file rating assigned by Comodo Client Security. The Viruscope column shows detailed info on processes started by the file. See the explanation under View **Process Activities of a File** for more details.



□	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSSCOPE
□	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious\PCFlank \PCFlank\pcflank.exe	Apr 25, 2017	Malicious	View processes

Results per page: 20

Displaying 1 of 1 results

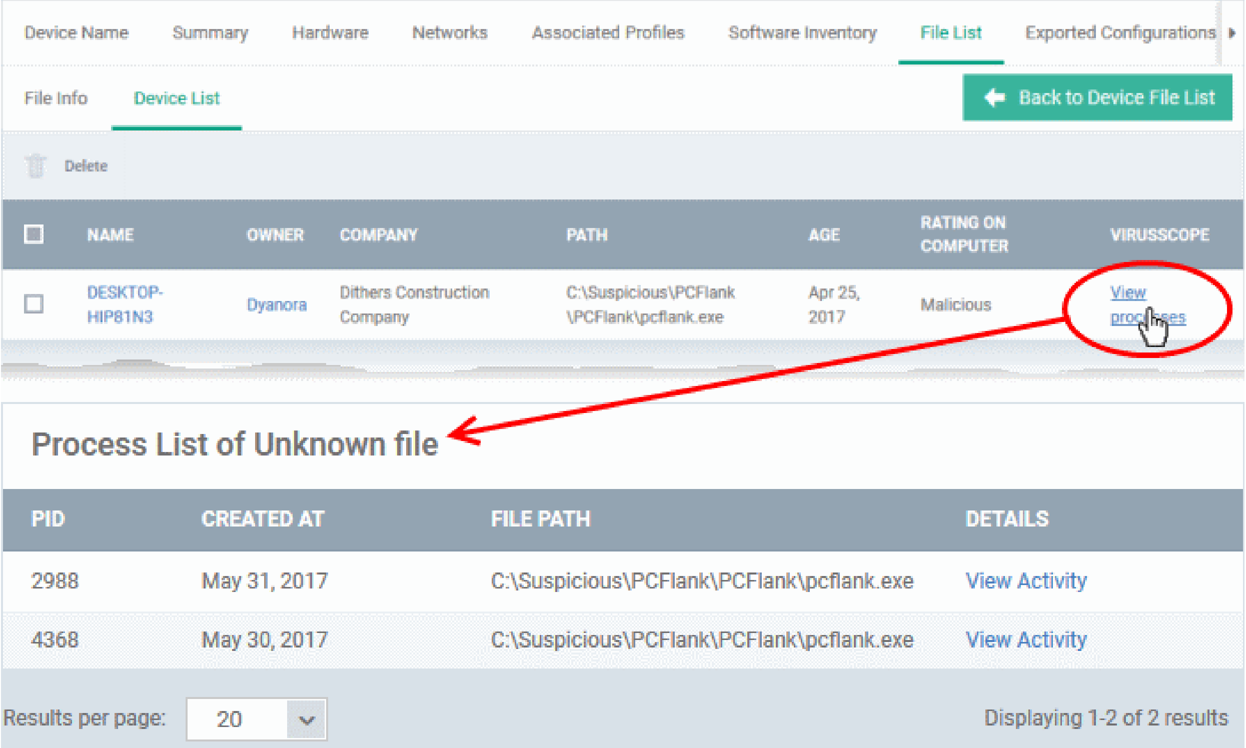
- You can remove the file from device(s) by selecting a device then clicking 'Delete'

View Process Activities of a File

Note: In order to fetch process activity data, VirusScope should be enabled in the profile in effect on the endpoint. See **Configuring Viruscope Settings** in **Creating a Windows Profile** for more details.

To view the activities of a file on the endpoint

- Click the file name from the 'File List' screen to open the 'File Details' screen
- Click the 'Device List' tab
- Click the 'View Processes' link in the 'Viruscope' column in the row of the device name.
- This will open a list of processes executed by the file on the selected endpoint in chronological order:



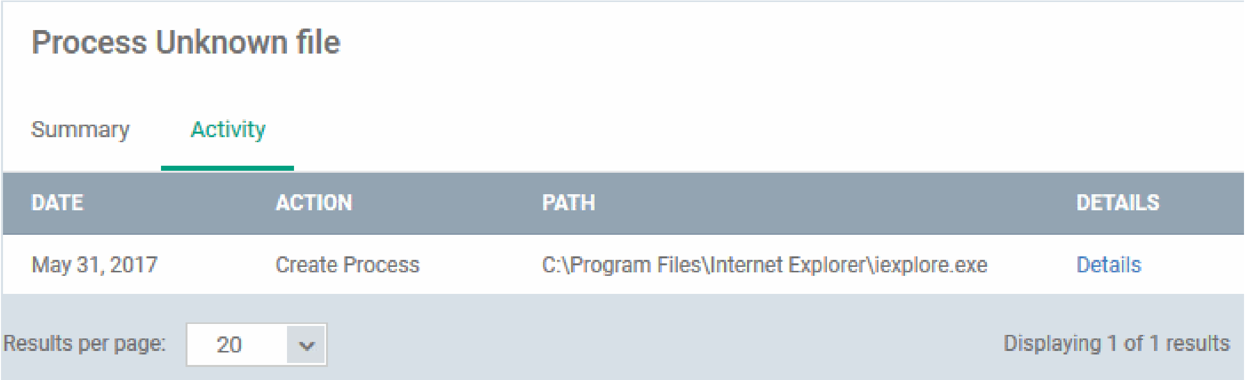
□	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSSCOPE
□	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious\PCFlank \PCFlank\pcflank.exe	Apr 25, 2017	Malicious	View processes

Process List of Unknown file

PID	CREATED AT	FILE PATH	DETAILS
2988	May 31, 2017	C:\Suspicious\PCFlank\PCFlank\pcflank.exe	View Activity
4368	May 30, 2017	C:\Suspicious\PCFlank\PCFlank\pcflank.exe	View Activity

Results per page: 20 Displaying 1-2 of 2 results

- Click 'View Activity' to see detailed information about each process. The 'Process Activity' interface 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.



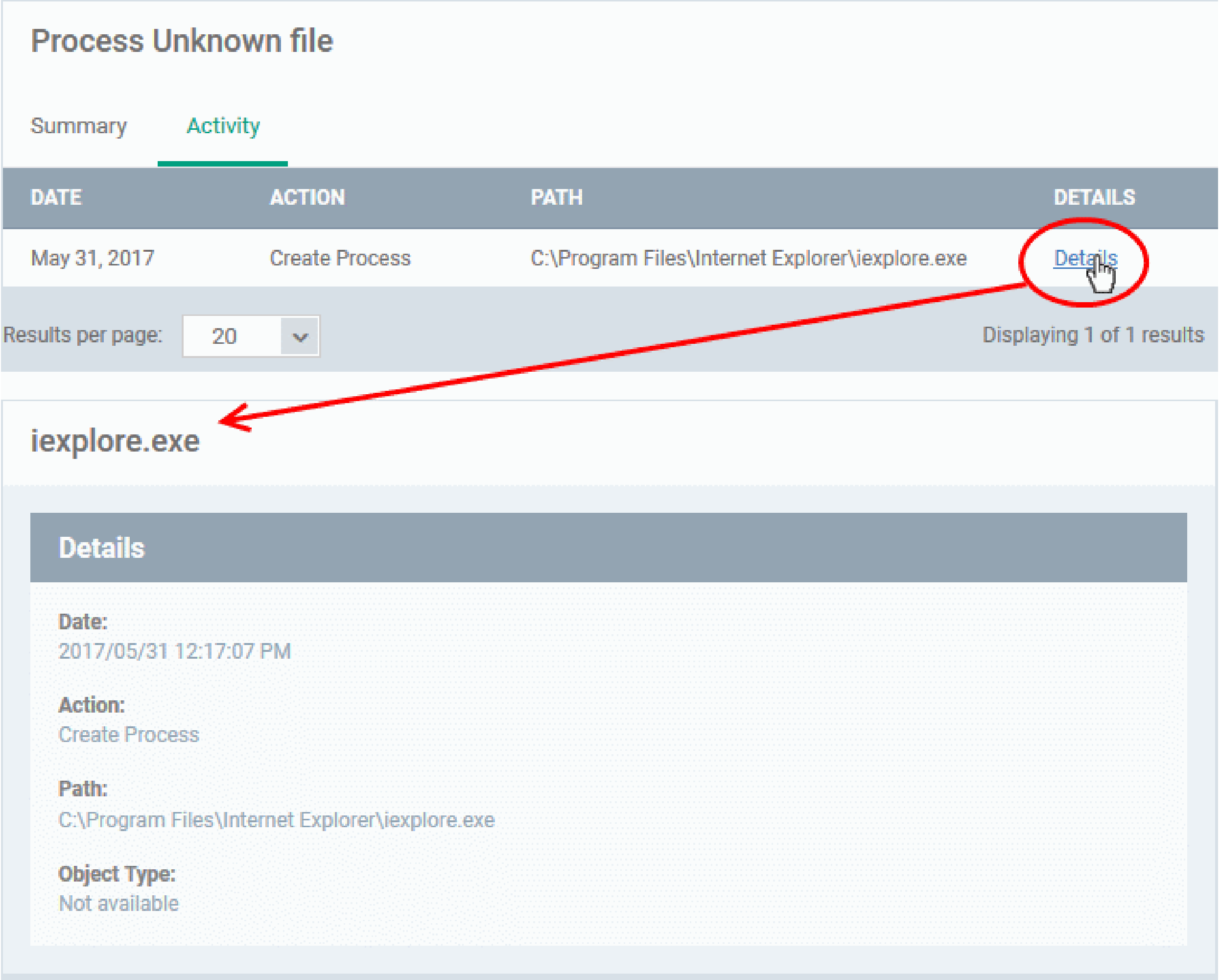
Process Unknown file

DATE	ACTION	PATH	DETAILS
May 31, 2017	Create Process	C:\Program Files\Internet Explorer\iexplore.exe	Details

Results per page: 20 Displaying 1 of 1 results

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

- You can inspect a particular activity by clicking the 'Details' link:



DATE	ACTION	PATH	DETAILS
May 31, 2017	Create Process	C:\Program Files\Internet Explorer\iexplore.exe	Details

Date:
2017/05/31 12:17:07 PM

Action:
Create Process

Path:
C:\Program Files\Internet Explorer\iexplore.exe

Object Type:
Not available

Assign Admin Rating to a File

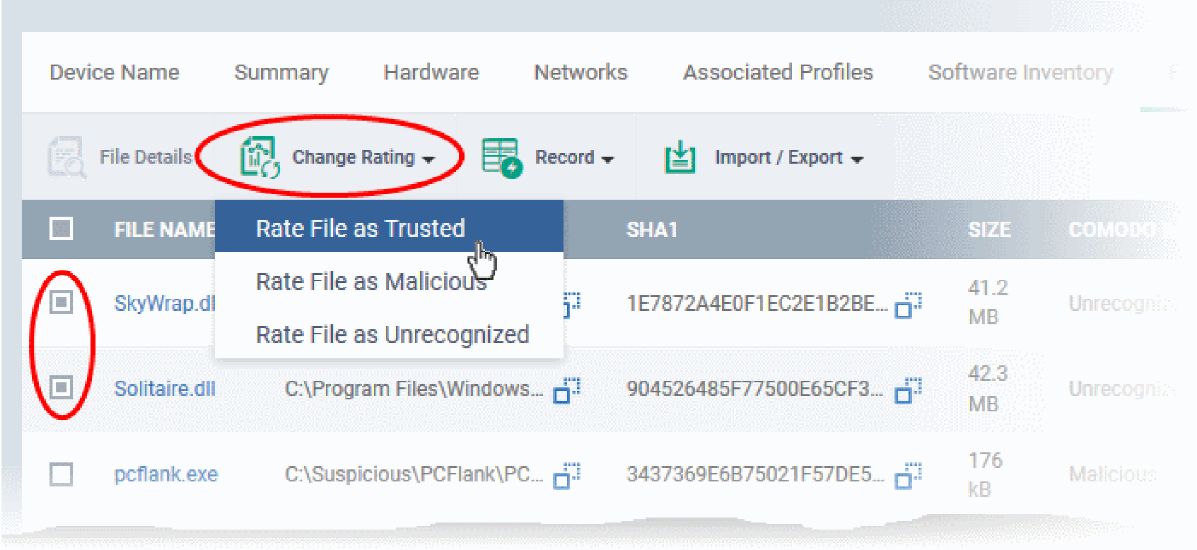
- Each file on an endpoint is automatically scanned and assigned a trust rating by Comodo Client Security.
- These ratings can be either '**Unrecognized**', '**Trusted**' or '**Malicious**'. The rating for each file is shown in the 'Comodo Rating' column of the 'File List' screen.
- The file rating determines whether or how the file is allowed to run:
  - **Trusted** - The file will be allowed to run normally. It will, of course, still be subject to the standard protection mechanisms of Comodo Client Security (behavior monitoring, host intrusion prevention etc).
  - **Malicious** - The file will not be allowed to run. It will be automatically quarantined or deleted depending on admin preferences.

- ◦ **Unknown** - The file will be run inside the container. The container is a virtual operating environment which is isolated from the rest of the endpoint. Files in the container write to a virtual file system, use a virtual registry and cannot access user or operating system data.

- Automatic file rating can be configured in the 'File Rating' section of the configuration profile active on the endpoint. See **File Rating settings** in **Creating a Windows Profile** for more details.
- Click 'Change Rating' in the 'File List' interface to manually set a rating for a selected file or files. The new rating will be propagated to all endpoints and will determine the file's run-time privileges. Admin assigned ratings will be shown in the 'Admin Rating' column of the interface:

To assign a file rating to a file

- Select the file(s) whose rating you want to change and click the 'Change Rating' button.
- Choose the rating you want to from the drop-down:

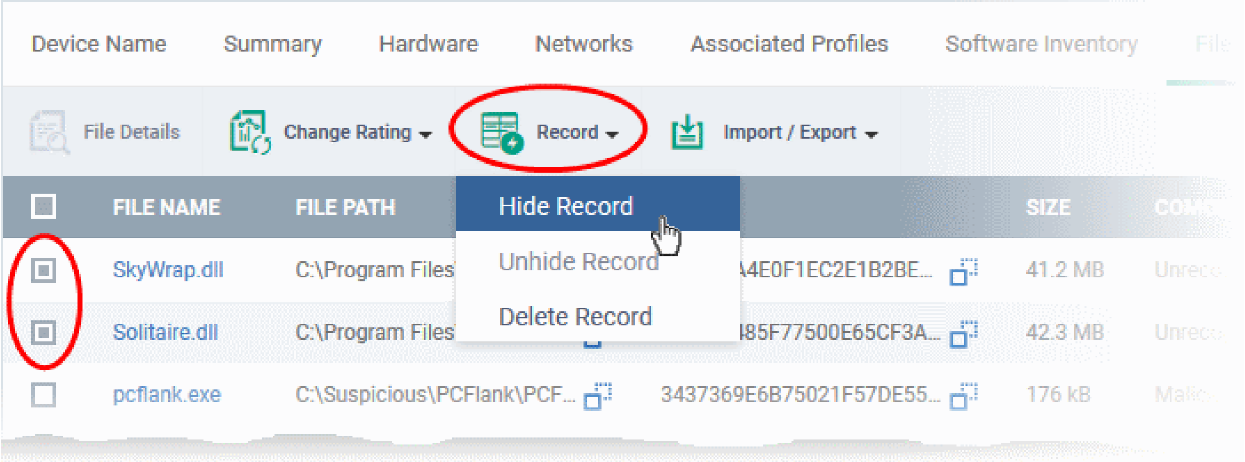


FILE NAME		SHA1	SIZE	COMODO
☐ SkyWrap.dl		1E7872A4E0F1EC2E1B2BE...	41.2 MB	Unrecogni
☐ Solitaire.dll	C:\Program Files\Windows...	904526485F77500E65CF3...	42.3 MB	Unrecogni
☐ pcflank.exe	C:\Suspicious\PCFlank\PC...	3437369E6B75021F57DE5...	176 kB	Malicious

As mentioned, the new admin rating will be set and sent to all endpoints. The Admin Rating will determine the file's run-time privileges.

Hide/Display Selected Files

- Select the file(s) you want to hide and click 'Record' at the top

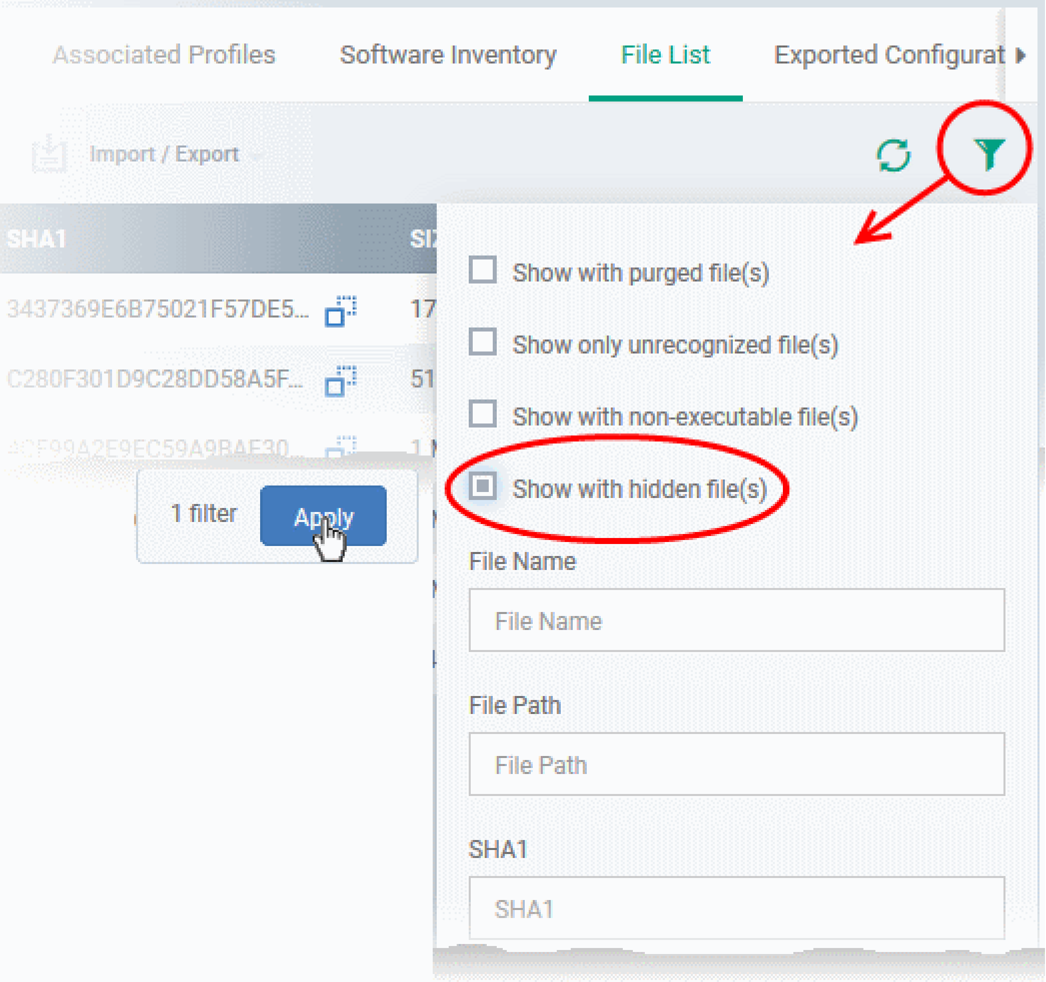


FILE NAME	FILE PATH		SIZE	COMO
☐ SkyWrap.dll	C:\Program Files	4E0F1EC2E1B2BE...	41.2 MB	Unreco
☐ Solitaire.dll	C:\Program Files	85F77500E65CF3A...	42.3 MB	Unreco
☐ pcflank.exe	C:\Suspicious\PCFlank\PCF...	3437369E6B75021F57DE55...	176 kB	Malic

- Select 'Hide / Unhide / Delete Record' as required.

To view hidden files

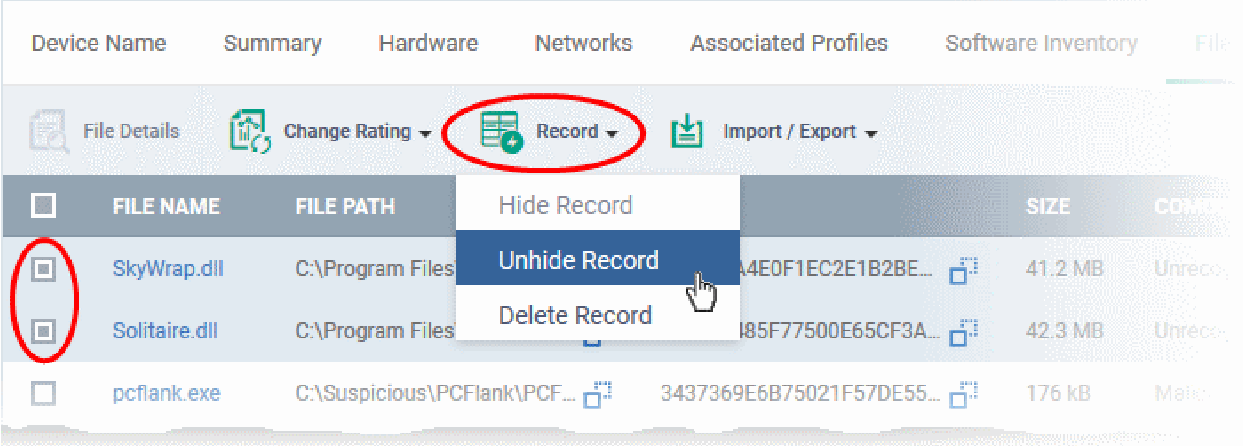
- Click the funnel icon at the top-right to open the filter options
- Select 'Show with hidden file(s)' and click 'Apply'



The hidden files will be added to the list in the 'File List' screen. The files will be highlighted with a gray stripe.

To restore hidden files

- Click the funnel icon at the top-right to open the filter options
- Enable 'Show with hidden file(s)'
- Select the hidden files you want to restore and click 'Unhide Record' from the drop-down


Device Name
Summary
Hardware
Networks
Associated Profiles
Software Inventory
File Details
Change Rating
Record
Import / Export
Hide Record
Unhide Record
Delete Record
FILE NAME
FILE PATH
SIZE
▣ SkyWrap.dll C:\Program Files 4E0F1EC2E1B2BE... 41.2 MB
▣ Solitaire.dll C:\Program Files 85F77500E65CF3A... 42.3 MB
□ pcflank.exe C:\Suspicious\PCFlank\PCF... 3437369E6B75021F57DE55... 176 kB

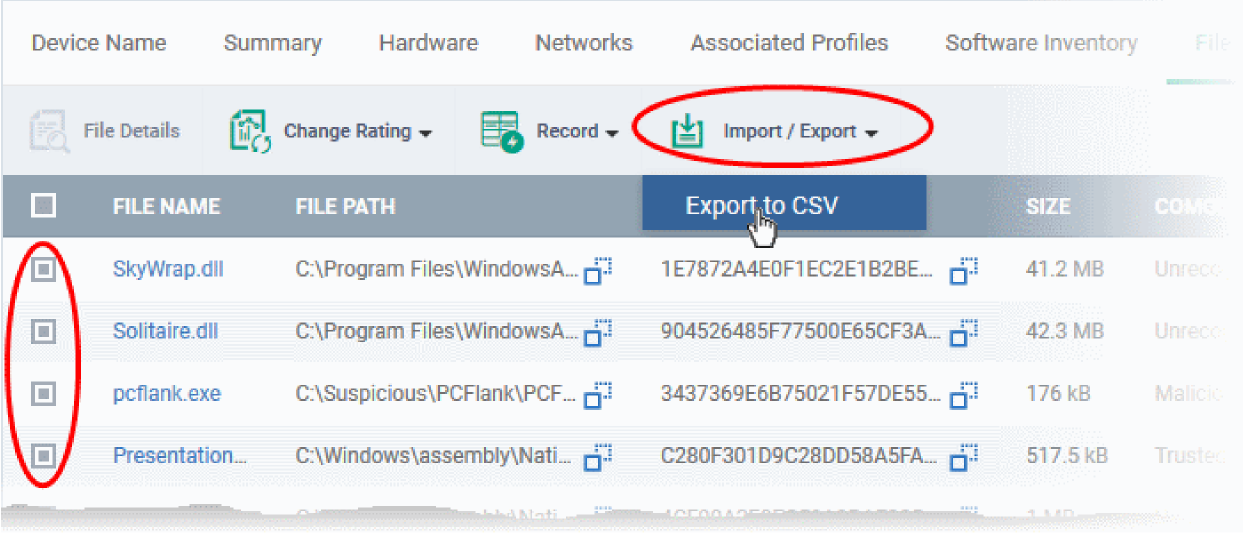
The files will be displayed in the permanently.

Export the List of Files

The 'File List' screen allows administrators to save a local copy of a list of files selected from the interface, with their details by exporting the list and saving it as a Comma Separated Values (CSV) file.

To export a list of files

- Select the files to be included in the list and click 'Import / Export' at the top



☐	FILE NAME	FILE PATH		SIZE	COMO
☐	SkyWrap.dll	C:\Program Files\WindowsA...	1E7872A4E0F1EC2E1B2BE...	41.2 MB	Unreco
☐	Solitaire.dll	C:\Program Files\WindowsA...	904526485F77500E65CF3A...	42.3 MB	Unreco
☐	pcflank.exe	C:\Suspicious\PCFlank\PCF...	3437369E6B75021F57DE55...	176 kB	Malicio
☐	Presentation...	C:\Windows\assembly\Nati...	C280F301D9C28DD58A5FA...	517.5 kB	Truste

- Choose 'Export to CSV' from the drop-down

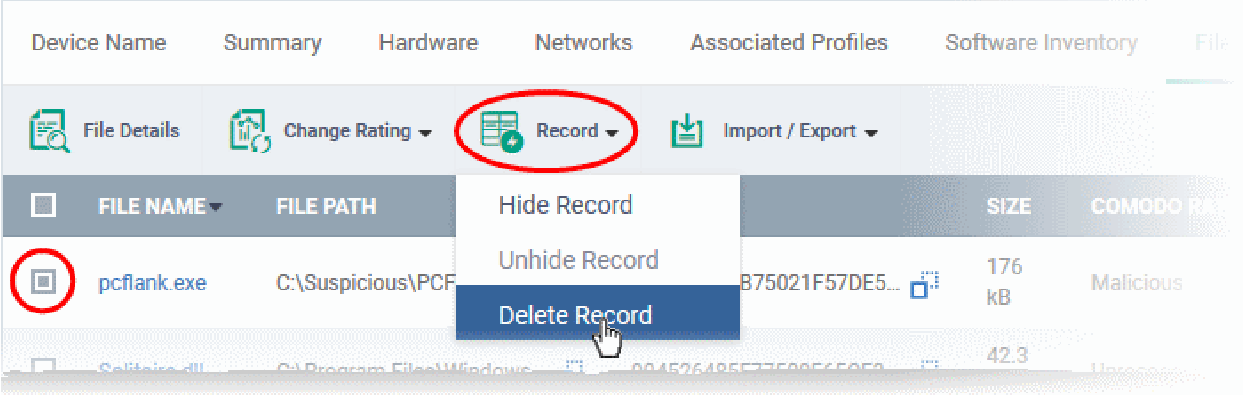
The CSV file containing the list of selected files with their details will be downloaded.

Remove files from the list

Items that no longer need to be displayed, can be removed from the 'File List' screen. These files will only be removed from the list and not from the endpoints.

To remove unwanted items from the 'File List' screen

- Select the files you want to remove and click 'Record' at the top
- Choose 'Delete Record' from the drop-down



☐	FILE NAME	FILE PATH		SIZE	COMODO R
☐	pcflank.exe	C:\Suspicious\PCF	B75021F57DE5...	176 kB	Malicious

5.2.1.8. View Exported Configurations and Import Profiles

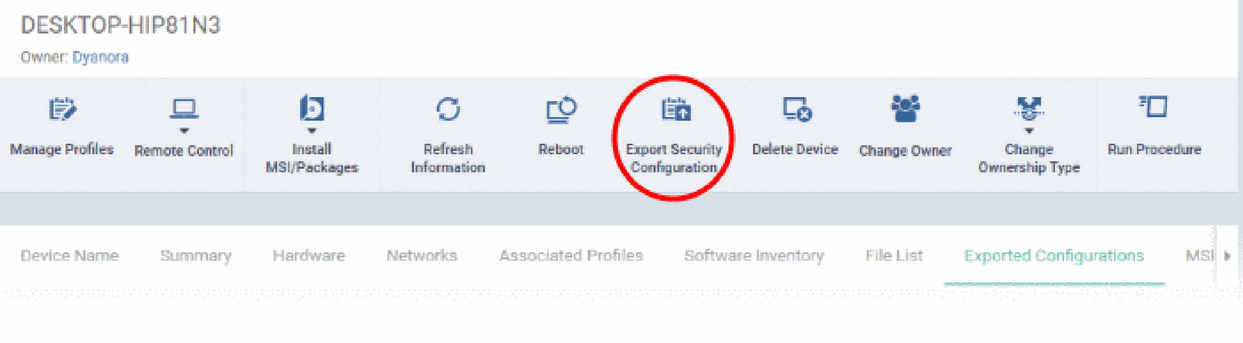
ITSM allows you to create a new Windows profile using the existing CCS configuration on an endpoint. This is useful if you want the current configuration on an endpoint to be rolled out to a number of endpoints.

To export a CCS configuration

- Click the 'Devices' tab on the left and choose 'Device List'

- Click the 'Device Management' tab at the top of the main configuration pane
  - Select the Company and choose the group under it to view the list of devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- 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.

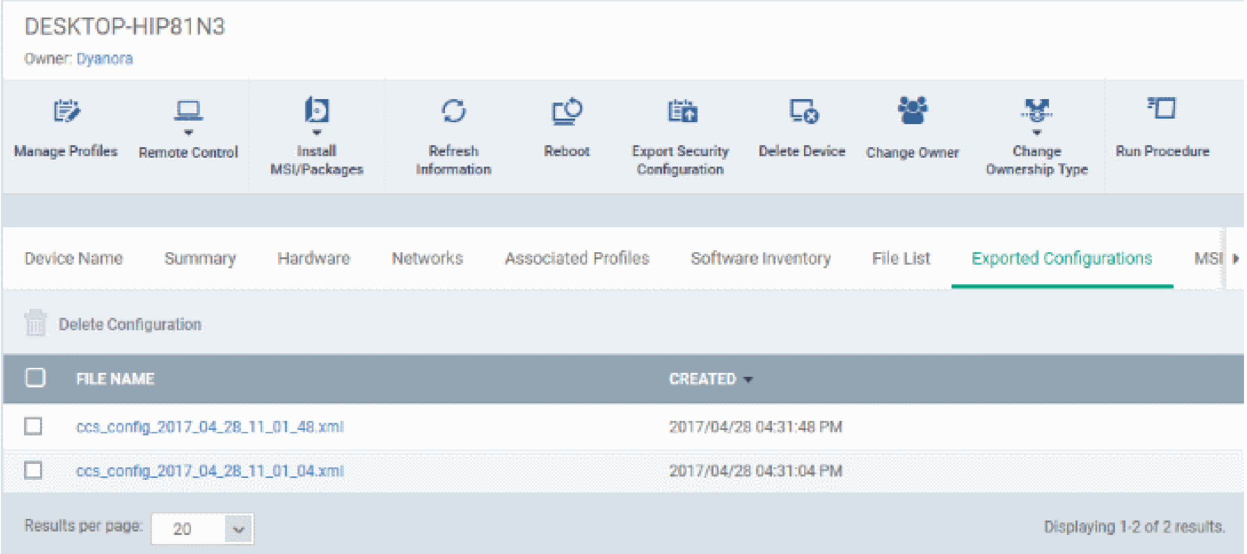


The CCS configuration will be exported as an .xml file with date/time stamp suffix in the file name. The profile will be saved on the ITSM server and can be viewed by clicking the 'Exported Configurations' tab of the device details interface of the same device.

To view and manage exported profiles

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on the Windows device,then select the 'Exported Configurations' tab



☐	FILE NAME	CREATED ▾
☐	ccs_config_2017_04_28_11_01_48.xml	2017/04/28 04:31:48 PM
☐	ccs_config_2017_04_28_11_01_04.xml	2017/04/28 04:31:04 PM

Results per page: 20 Displaying 1-2 of 2 results.

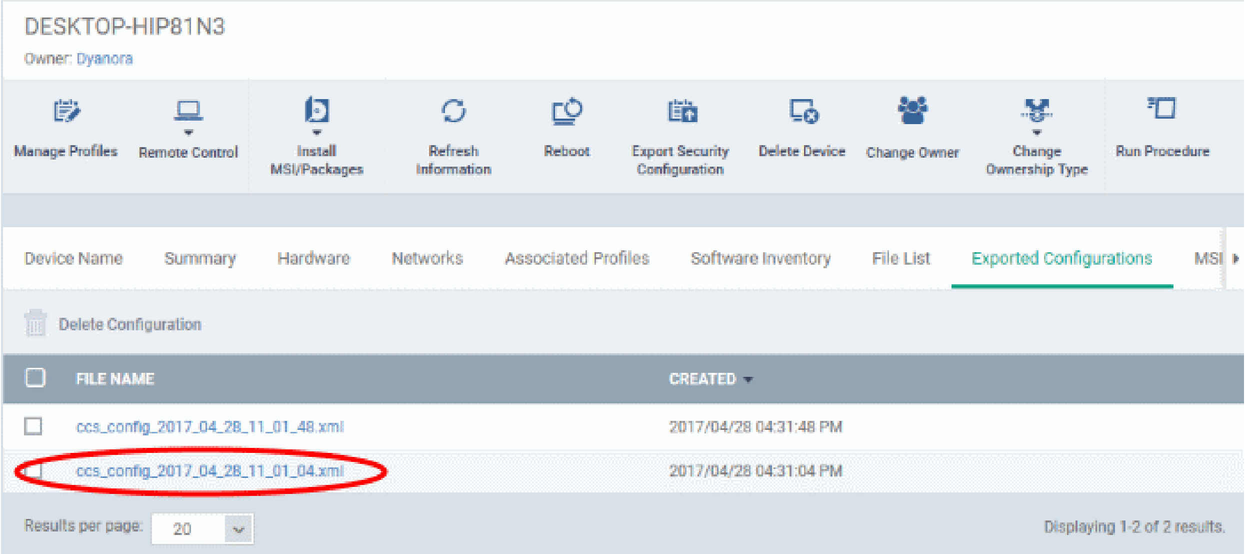
The 'Exported Security Configuration' List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the file name of the exported file.

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

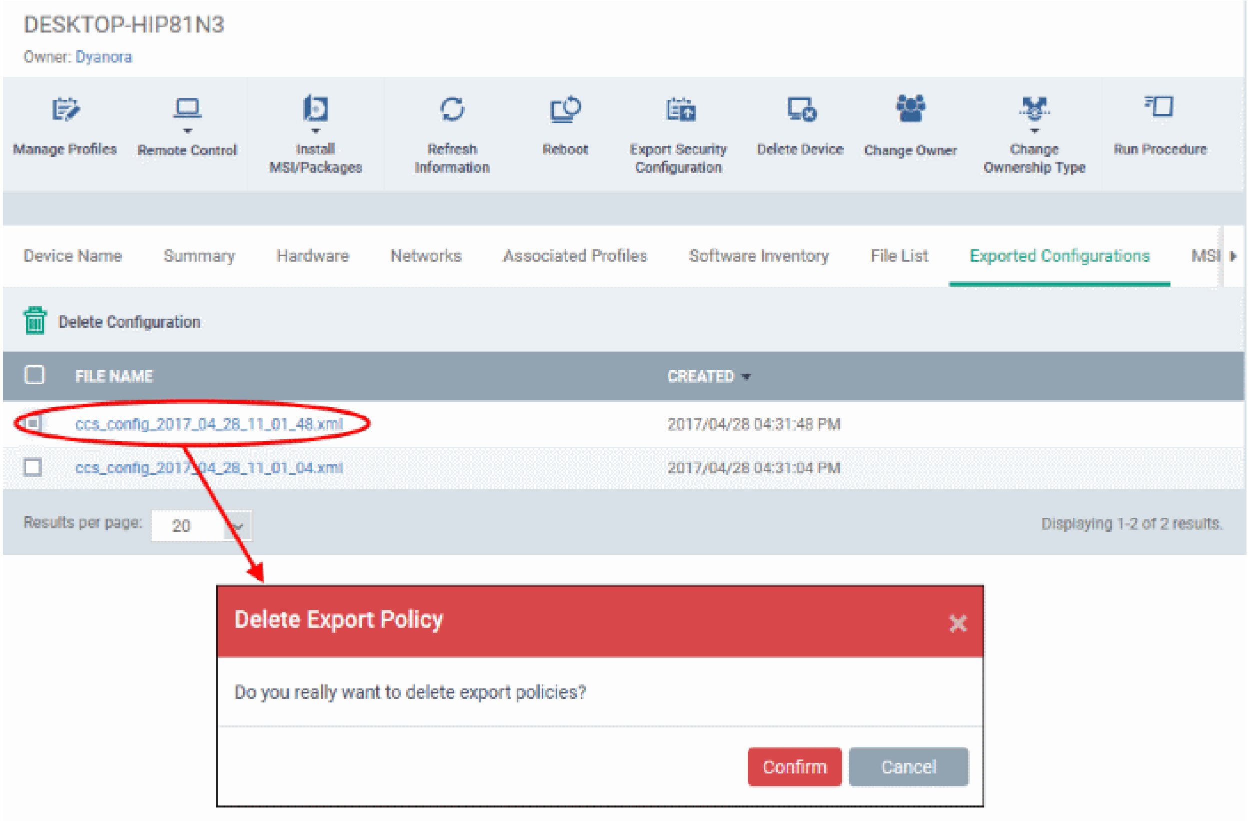


□	FILE NAME	CREATED
□	ccs_config_2017_04_28_11_01_48.xml	2017/04/28 04:31:48 PM
□	ccs_config_2017_04_28_11_01_04.xml	2017/04/28 04:31:04 PM

The file will be imported as a .xml file.

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

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



□	FILE NAME	CREATED
☑	ccs_config_2017_04_28_11_01_48.xml	2017/04/28 04:31:48 PM
□	ccs_config_2017_04_28_11_01_04.xml	2017/04/28 04:31:04 PM

Delete Export Policy

Do you really want to delete export policies?

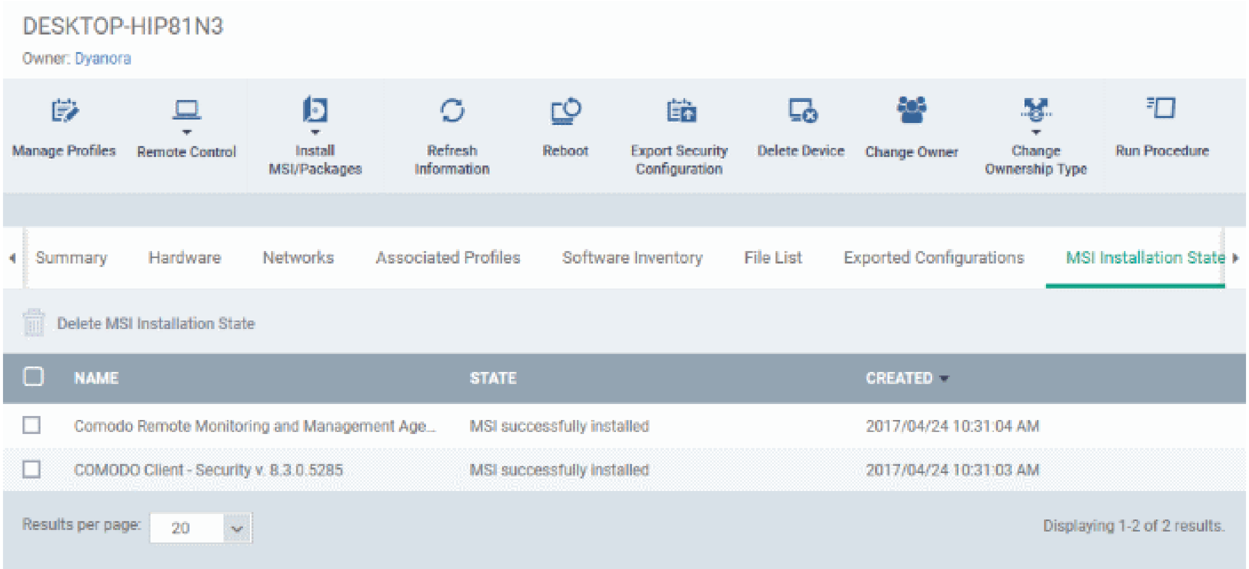
5.2.1.9. View MSI Files Installed on the Device through ITSM

You can remotely install ITSM packages on to managed endpoints. These may be Comodo applications or third-party MSI packages. See **Remotely Installing Packages onto Windows Devices**, for more information on remote deployment of MSI packages.

To view MSI file installation list on the device

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

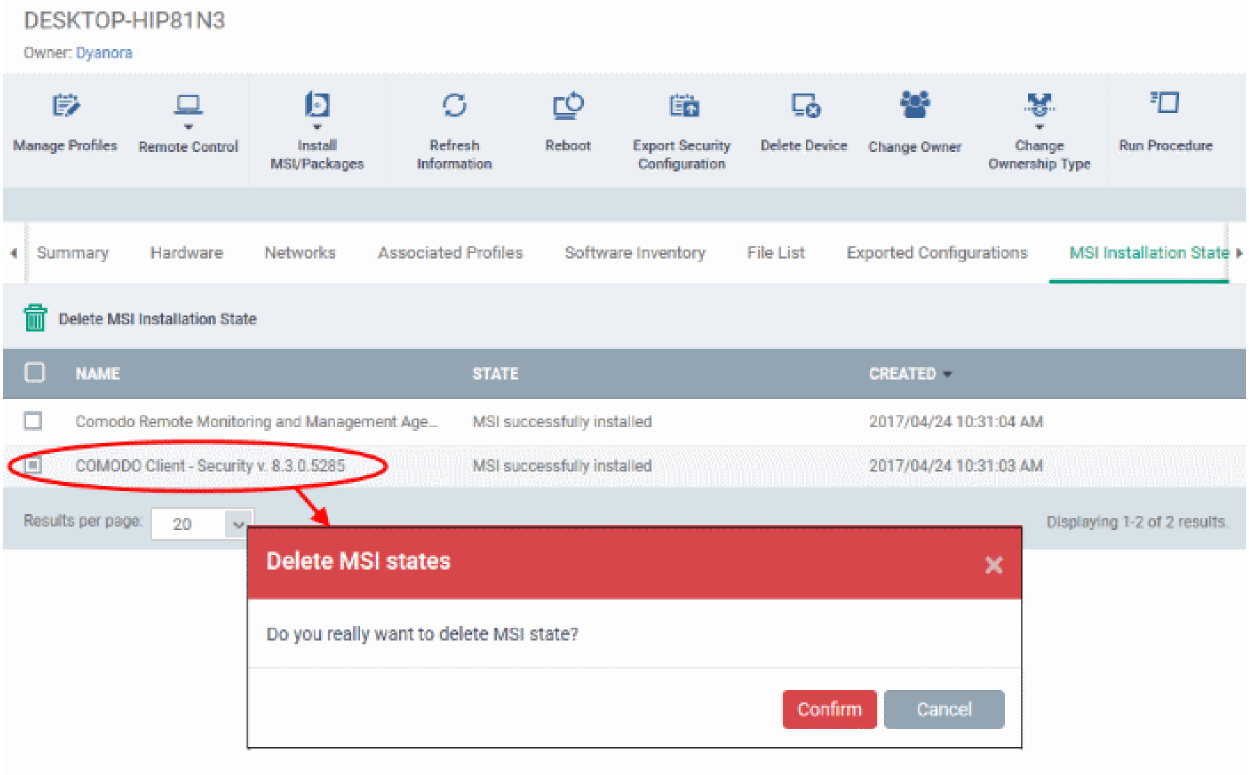
      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of any Windows device then select the 'MSI Installation State' tab



□	NAME	STATE	CREATED
□	Comodo Remote Monitoring and Management Age...	MSI successfully installed	2017/04/24 10:31:04 AM
□	COMODO Client - Security v. 8.3.0.5285	MSI successfully installed	2017/04/24 10:31:03 AM

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'.



□	NAME	STATE	CREATED
□	Comodo Remote Monitoring and Management Age...	MSI successfully installed	2017/04/24 10:31:04 AM
☑	COMODO Client - Security v. 8.3.0.5285	MSI successfully installed	2017/04/24 10:31:03 AM

Do you really want to delete MSI state?

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

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

5.2.1.10. View and Install Windows and 3rd Party Application Patches

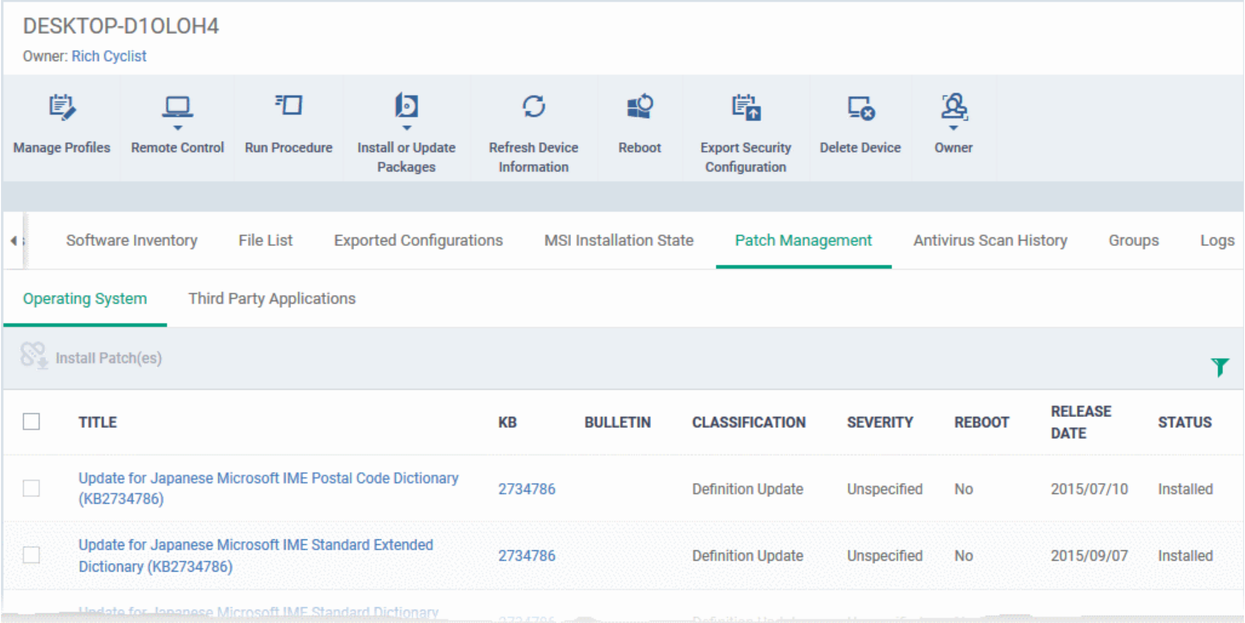
- Windows OS and 3rd party applications have to be kept up-to-date to protect them from vulnerabilities and malicious attacks.
- The 'Patch Management' feature allows administrators to view available patches and deploy patches remotely. Administrators can install multiple patches on a device simultaneously.
  - This section tells you how to patch *individual* devices via the 'Device Details' screen.
  - If you want to install patches on multiple devices instead then go to 'Applications' > 'Patch Management'. See '**Patch Management**' for help with this.

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

To view and install patches and updates on Windows endpoints

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of any Windows device then select the 'Patch Management' tab



□	TITLE	KB	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
□	Update for Japanese Microsoft IME Postal Code Dictionary (KB2734786)	2734786		Definition Update	Unspecified	No	2015/07/10	Installed
□	Update for Japanese Microsoft IME Standard Extended Dictionary (KB2734786)	2734786		Definition Update	Unspecified	No	2015/09/07	Installed
	Update for Japanese Microsoft IME Standard Dictionary	2734786		Definition Update				

The interface contains two tabs:

- **Operating System** - Shows all previously installed patches and patches that are awaiting installation on the device. Each patch contains additional details such as classification, severity, release date, installation status and links to knowledgebase articles. You can remotely install selected patches on the endpoint from this interface. See **View and Install Windows Patches** for more details.
- **Third Party Applications** - Shows applications on the device for which updates are available. The version numbers of the currently installed version and the latest available version are shown. The 'severity' column tells you the importance of the update. You can remotely update selected applications on the device from this interface. See **View and Install 3rrdParty Application Patches** for more details.

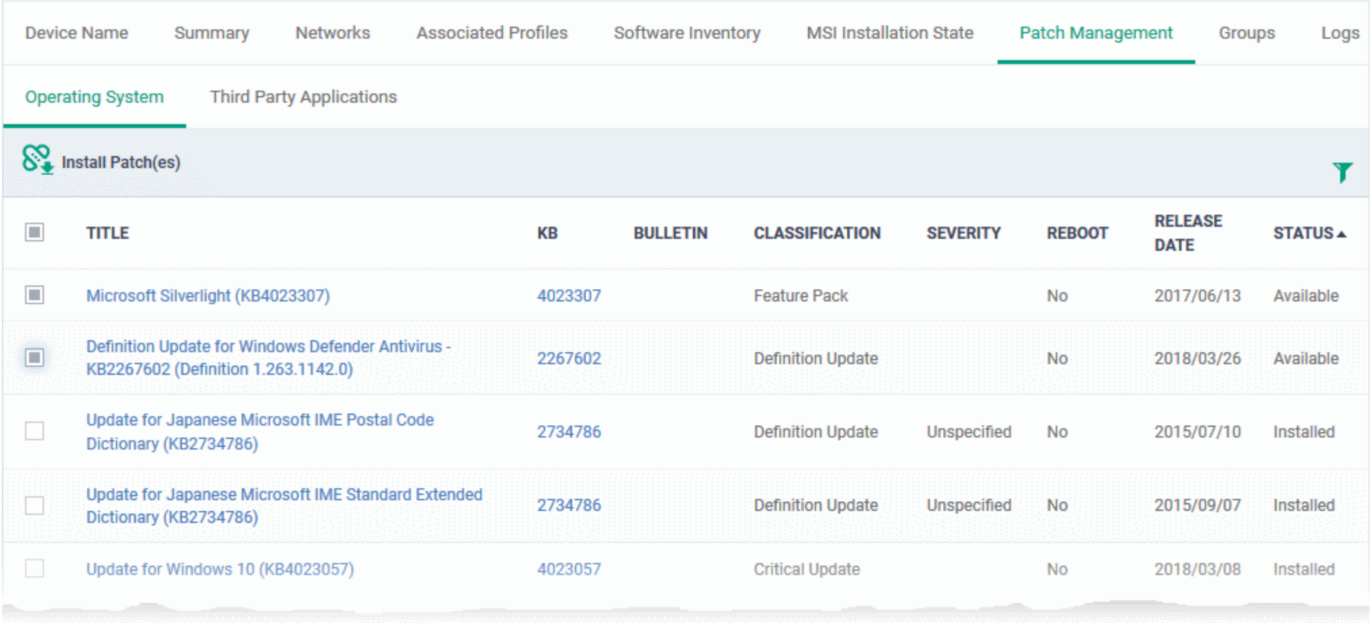
View and Install Windows Patches

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of any Windows device then select the 'Patch Management' tab
- Click the 'Operating System' tab:

Note:

- The 'Operating System' tab only shows Windows patches which are relevant to a device.
- Any hidden patches are not shown. Hidden patches can be configured in 'Application' > 'Patch Management'.
- For more details, see **hiding patches** in **Install OS Patches on Windows Endpoints**.



☐	TITLE	KB	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS ▲
☑	Microsoft Silverlight (KB4023307)	4023307		Feature Pack		No	2017/06/13	Available
☑	Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.1142.0)	2267602		Definition Update		No	2018/03/26	Available
☐	Update for Japanese Microsoft IME Postal Code Dictionary (KB2734786)	2734786		Definition Update	Unspecified	No	2015/07/10	Installed
☐	Update for Japanese Microsoft IME Standard Extended Dictionary (KB2734786)	2734786		Definition Update	Unspecified	No	2015/09/07	Installed
☐	Update for Windows 10 (KB4023057)	4023057		Critical Update		No	2018/03/08	Installed

Operating System Patches - Column Descriptions	
Column Heading	**Description**
Title	The descriptive name of the patch. • Click the name to view patch details. See **View Details of a Patch** for more details.
KB	The knowledgebase article number that describes the patch. • Click the number to view the Microsoft Knowledgebase article web page.
Bulletin	The Microsoft Bulletin number that contains details about the patch release.

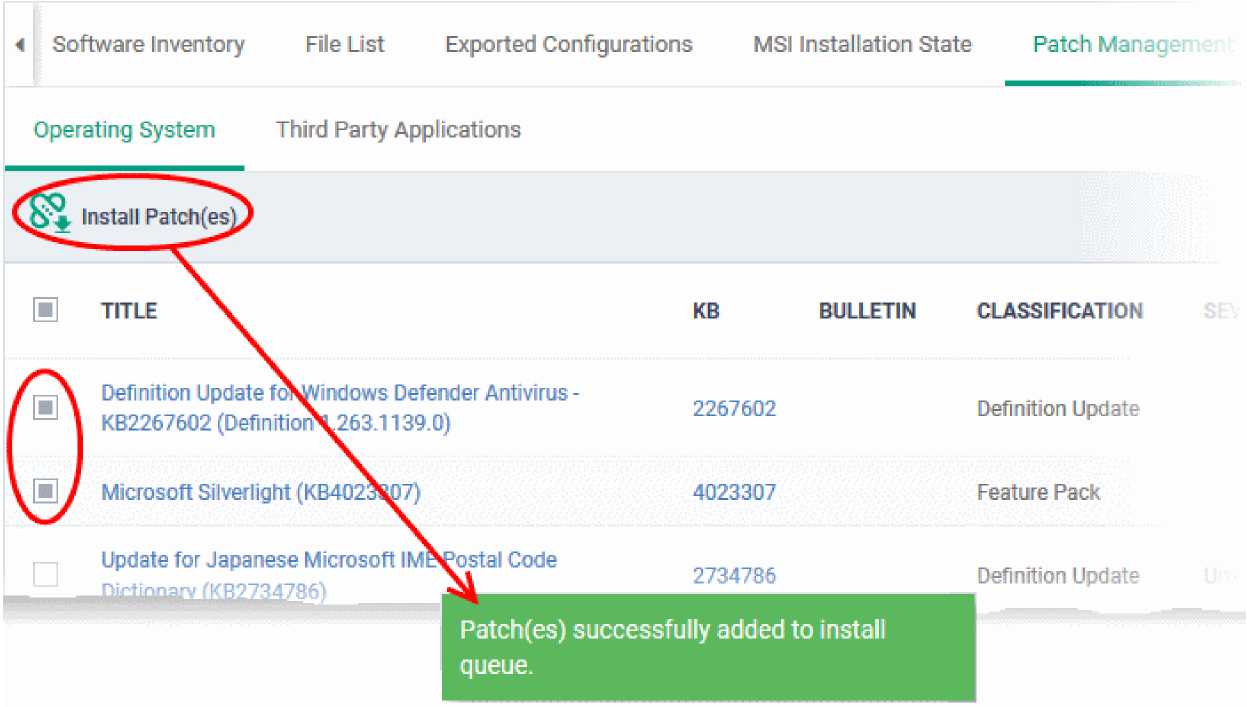
	- Click the number to view the respective 'Microsoft Security Bulletin' page.

Classification	The category of the patch. The possible values are: • Update - Fixes a specific non-critical problem but not a security-related bug. • Definition update - Contains updates to a product's definition database. For example, an update to the virus signature database for Windows Defender. • Critical Update - Fixes a specific critical problem but not a security-related bug. • Security update - Fixes a version specific, security related vulnerability • Update rollup - A collection of updates, hotfixes, security updates and critical updates packaged together for easy deployment. These updates generally target a specific Windows component. • Driver - Adds software for controlling peripherals or add-on devices that could be connected to the endpoint • Feature pack - Adds new functionality distributed after an OS release. • Service pack - Contains a collection of updates, hotfixes, security updates, critical updates and additional fixes. • Tool - Installs a utility or feature for a specific task or a set of tasks. • Upgrades - Updates the Windows OS version on the endpoint to the latest build.
Severity	The criticality of the patch. The severity levels are: • Critical • Important • Low • Moderate • Unspecified
Reboot	Whether or not the endpoint requires a restart to complete the patch installation.
Release Date	The date on which the patch was released by Microsoft
Status	Indicates whether the patch has been installed on the device or not.

- Click any column header to sort the items in ascending/descending order of entries in that column
- Click the funnel icon on the right to filter patches by various criteria, including by severity, by whether a patch is available, or by patch installation status.
  - Start typing the name of a patch in the search field to find a particular patch. Select the patch from the search suggestions and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.

To install missing patch(es) on the device

- 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 patches you wish to install
- Click 'Install Patch(es)'



	TITLE	KB	BULLETIN	CLASSIFICATION
☒	Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.1139.0)	2267602		Definition Update
☒	Microsoft Silverlight (KB4023307)	4023307		Feature Pack
□	Update for Japanese Microsoft IME Postal Code Dictionary (KB2734786)	2734786		Definition Update

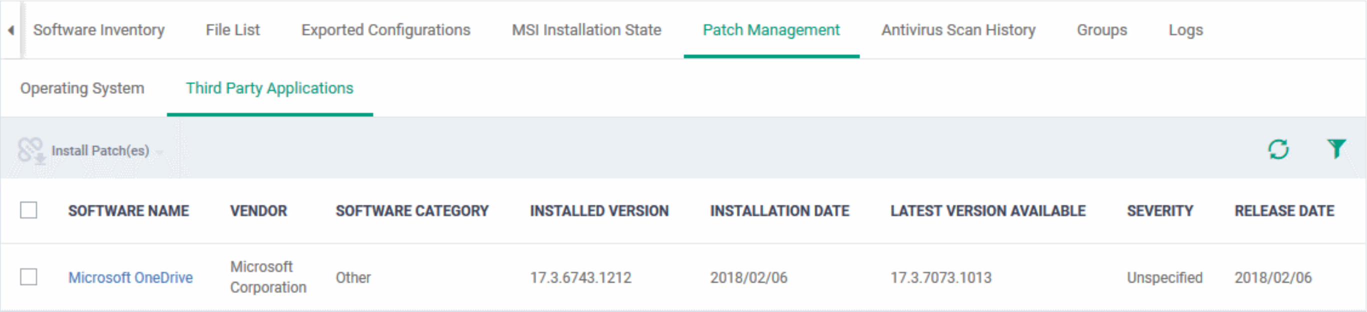
Patch(es) successfully added to install queue.

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.

View and Install 3rd Party Application Patches

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of any Windows device then select the 'Patch Management' tab
- Click the 'Third Party Applications' tab:



□	SOFTWARE NAME	VENDOR	SOFTWARE CATEGORY	INSTALLED VERSION	INSTALLATION DATE	LATEST VERSION AVAILABLE	SEVERITY	RELEASE DATE
□	Microsoft OneDrive	Microsoft Corporation	Other	17.3.6743.1212	2018/02/06	17.3.7073.1013	Unspecified	2018/02/06

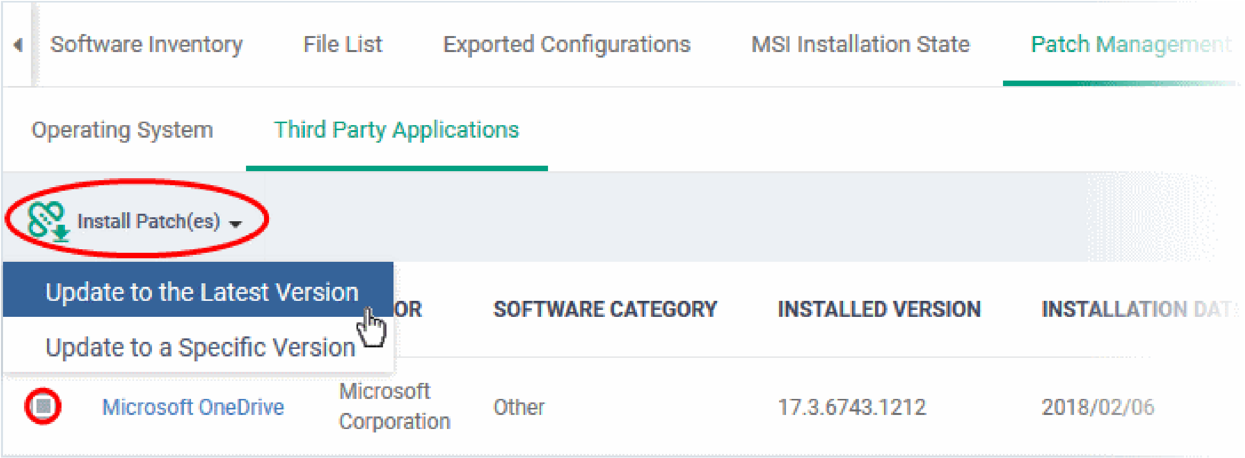
Third Party Applications - Column Descriptions	
Column Heading	**Description**
Software Name	The name of the application. • Click the name to view general application details and a list of devices on which the (outdated) application is installed. See **View Details of an Application** in **Install 3rd Party Application Patches on Windows Endpoints** for more details.

Vendor	The software publisher.
Software Category	The type of the application. Possible values include: • Comodo Products • Runtime applications • Web Browsers • Utilities • Messaging • File Compression utilities • Developer Tools • Documents • Online Storage • Other
Installed Version	The version number of the application currently installed on the endpoint.
Installation Date	The date on which the application was installed on the endpoint.
Latest Version Available	The version number of the latest version of the application that is available from the publisher
Severity	Indicates the level of severity of the update as determined by Microsoft. The severity levels are: • Unspecified • Critical • Important • Low • Moderate
Release Date	The date at which the latest version of the application was released.

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Click the funnel icon on the right to filter patches by various criteria, including by software/vendor name, by whether a patch is available, or by patch severity.
    - Start typing the name of a patch in the search field to find a particular patch. Select the patch from the search suggestions and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.

To update 3rd party applications

- Select the application(s) to be updated and click 'Install Patches'



- To update the application to the latest available version, choose 'Update to Latest Version' from the options.
- To update the application to a particular version, choose 'Update to a Specific Version' from the options. The 'Update to a Specific Version' dialog will appear. Select the version you wish to install from the drop-down and click 'Send'.
- A command will be sent to the endpoint to schedule installation of the patch.
- Once the command is received, Comodo Client Communication (CCC) on the endpoint will check whether the update is available on any other devices in the local network.
    - If the update is available, CCC establishes a peer-to-peer network with the device on which the update is available and downloads the patch. This reduces bandwidth usage as the update is downloaded from the local network.
    - If the update is not available on any devices in the local network, CCC downloads the update from the ITSM patch portal.

See '**ITSM Supported 3rd Party Applications**' to view a full list of applications that can be updated.

5.2.1.11. View Antivirus Scan History

The 'Antivirus Scan History' tab of 'Device Details' displays items identified as malware on an endpoint. You can also see the malware's installation path and the action taken against the file.

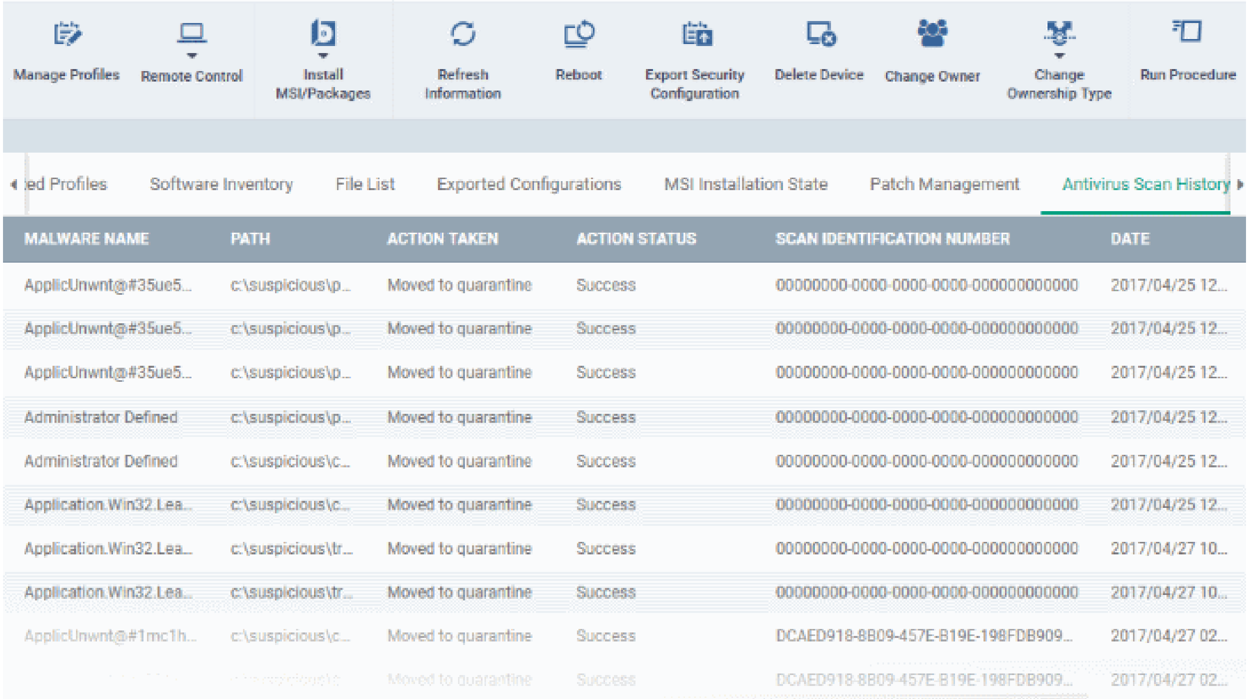
You only can view virus scan history on endpoints that have Comodo Client Security installed. The scan history covers manual scans and automatic scans run as part of a configuration profile.

To view Antivirus Scan history of the device

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of any Windows device then select the 'Antivirus Scan History' tab

Note: The 'Antivirus Scan History' tab will be available only for endpoints with Comodo Client Security installed.



MALWARE NAME	PATH	ACTION TAKEN	ACTION STATUS	SCAN IDENTIFICATION NUMBER	DATE
ApplicUnwnt@#35ue5...	c:\suspicious\p...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
ApplicUnwnt@#35ue5...	c:\suspicious\p...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
ApplicUnwnt@#35ue5...	c:\suspicious\p...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
Administrator Defined	c:\suspicious\p...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
Administrator Defined	c:\suspicious\c...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
Application.Win32.Lea...	c:\suspicious\c...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/25 12...
Application.Win32.Lea...	c:\suspicious\tr...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/27 10...
Application.Win32.Lea...	c:\suspicious\tr...	Moved to quarantine	Success	00000000-0000-0000-0000-000000000000	2017/04/27 10...
ApplicUnwnt@#1mc1h...	c:\suspicious\c...	Moved to quarantine	Success	DCAED918-8B09-457E-B19E-198FDB909...	2017/04/27 02...
[illegible]	c:\suspicious\c	Moved to quarantine	Success	DCAED918-8B09-457E-B19E-198FDB909...	2017/04/27 02...

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.

5.2.1.12. View and Manage Device Group Membership

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

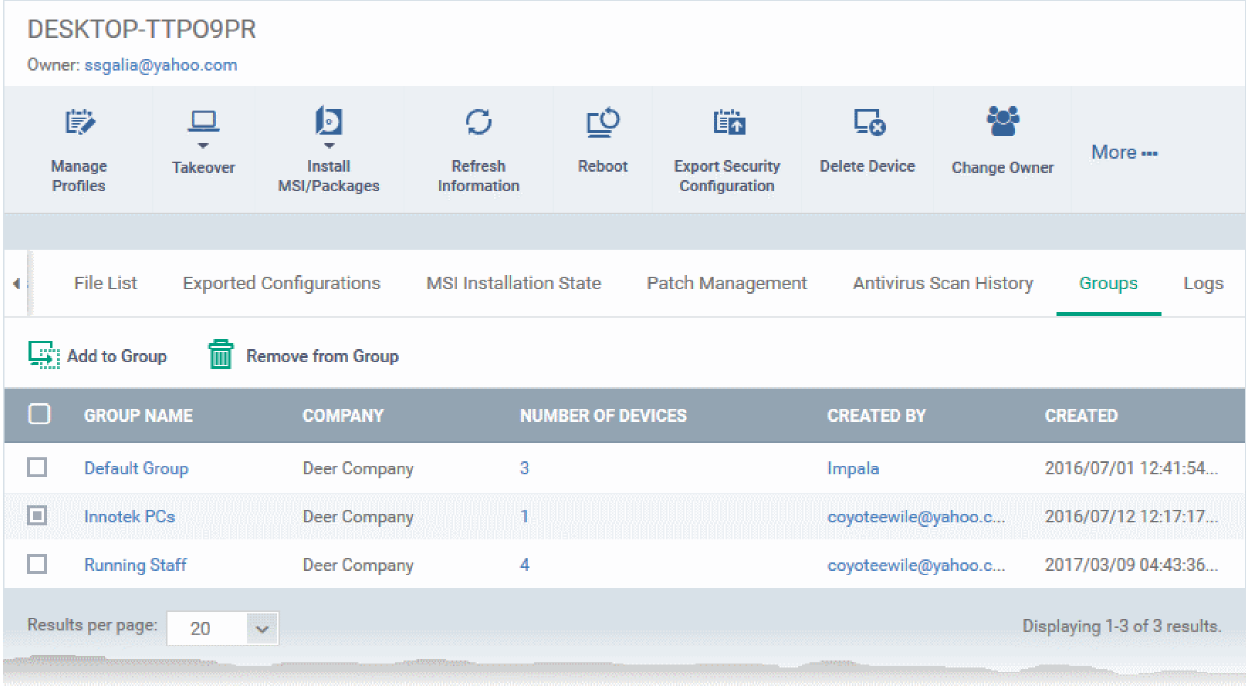
To view and manage device group membership

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

    Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click the name of any Windows device then select the 'the 'Groups' tab



□	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY	CREATED
□	Default Group	Deer Company	3	Impala	2016/07/01 12:41:54...
▣	Innotek PCs	Deer Company	1	coyoteewile@yahoo.c...	2016/07/12 12:17:17...
□	Running Staff	Deer Company	4	coyoteewile@yahoo.c...	2017/03/09 04:43:36...

Results per page: 20 Displaying 1-3 of 3 results.

- The interface lists all groups of which the device is a member.

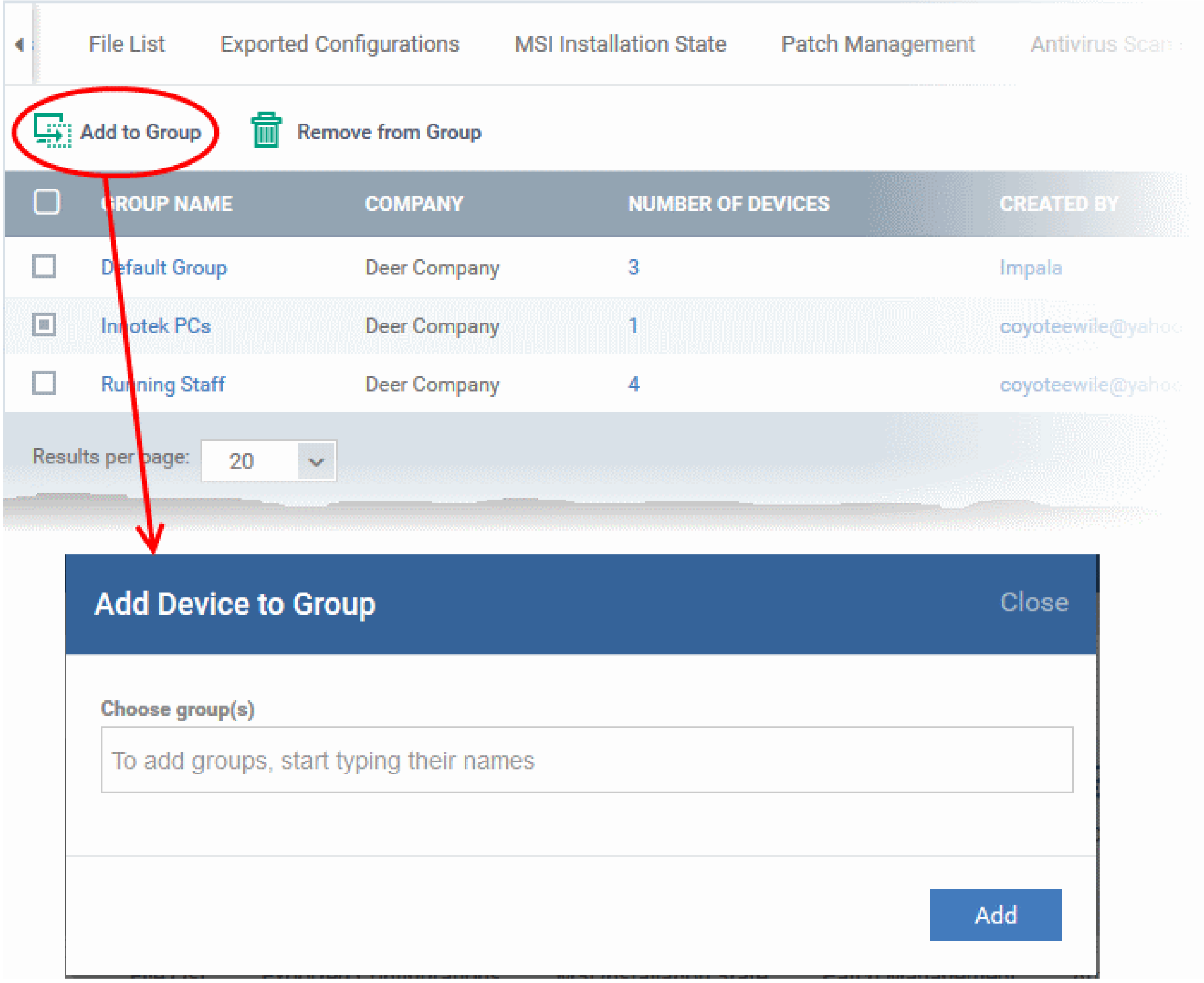
- All group profiles will also be applied to the endpoint.

See **Assigning Configuration Profiles to a Device Group**, for more details about applying configuration profiles to device groups.

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. See **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. See **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. See **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'



☐	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY
☐	Default Group	Deer Company	3	Impala
▣	Innotek PCs	Deer Company	1	coyoteewile@yahoo
☐	Running Staff	Deer Company	4	coyoteewile@yahoo

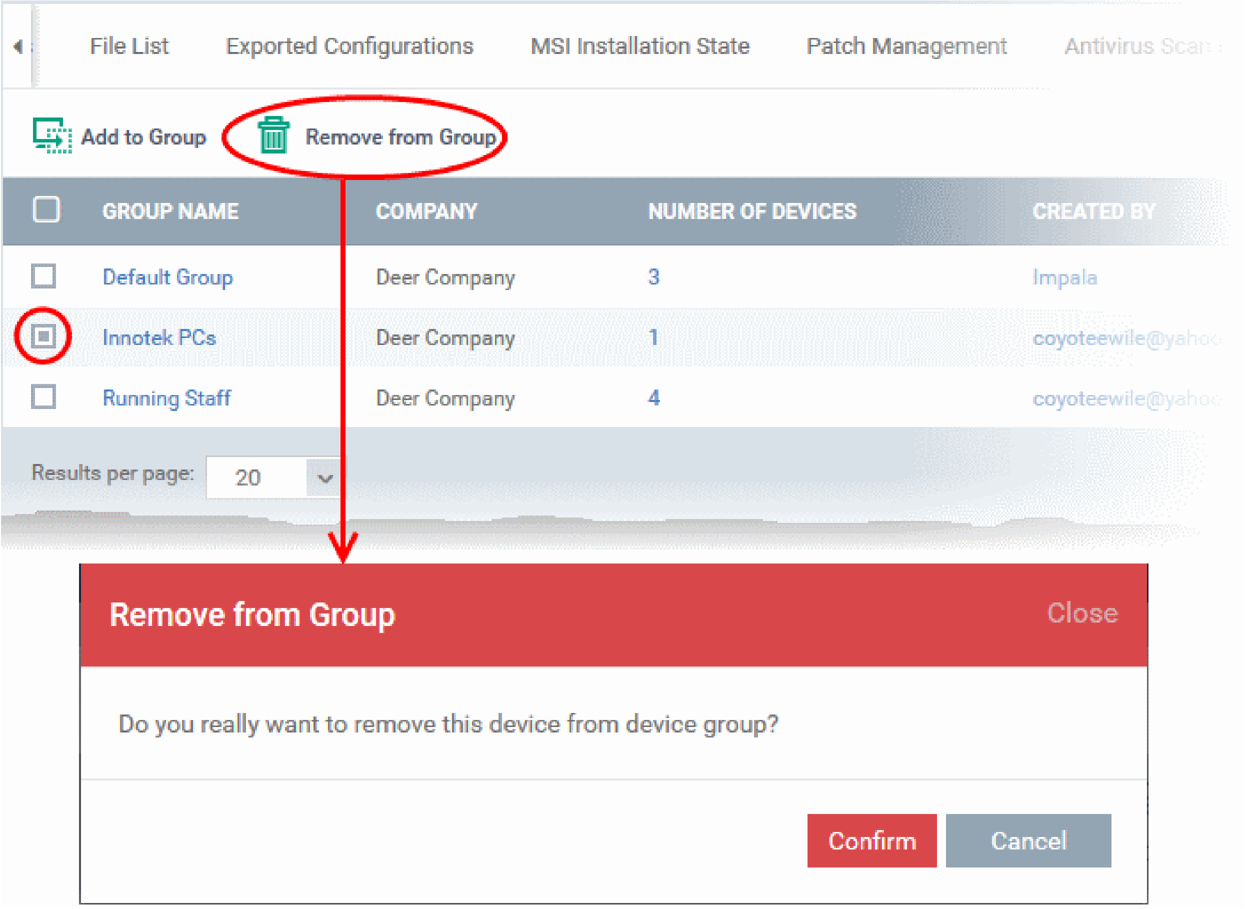
The 'Add Device to Group' dialog will appear.

- 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'.



□	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY
□	Default Group	Deer Company	3	Impala
☒	Innotek PCs	Deer Company	1	coyoteewile@yahoo
□	Running Staff	Deer Company	4	coyoteewile@yahoo

Remove from Group

Do you really want to remove this device from device 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.

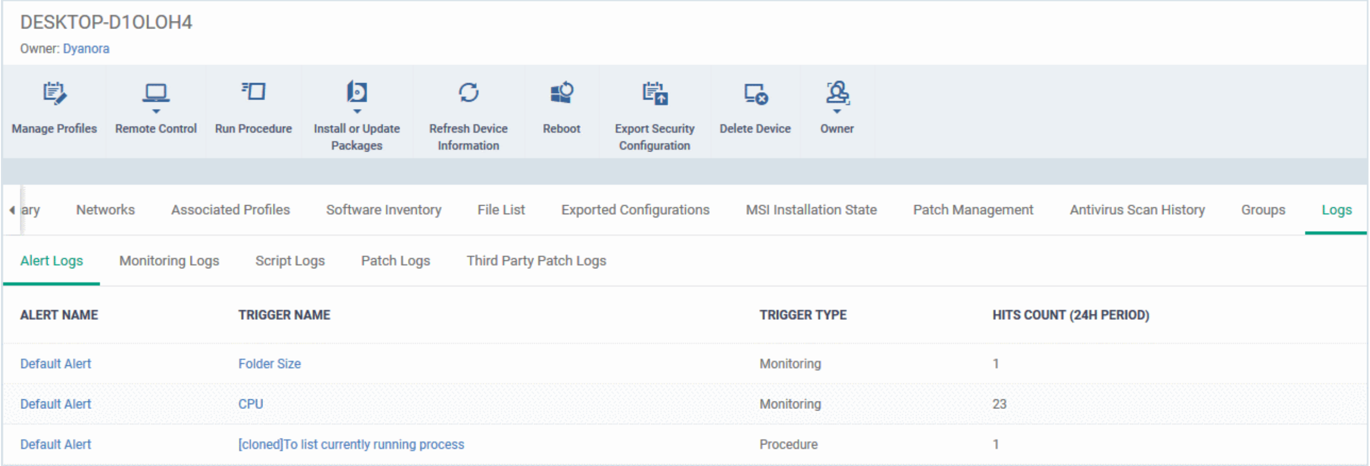
5.2.1.13. View Device Logs

ITSM collects logs from managed Windows devices for various events. Logs are created, for example, when there is a breach of monitoring conditions, when an alert is generated on the device and when a script or patch procedure is executed.

To view logs from a device

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Logs' tab



ALERT NAME	TRIGGER NAME	TRIGGER TYPE	HITS COUNT (24H PERIOD)
Default Alert	Folder Size	Monitoring	1
Default Alert	CPU	Monitoring	23
Default Alert	[cloned]To list currently running process	Procedure	1

The interface has five sub-tabs:

- Alert Logs
- Monitoring Logs
- Script Logs
- OS Patch Logs
- Third Party Patch Logs

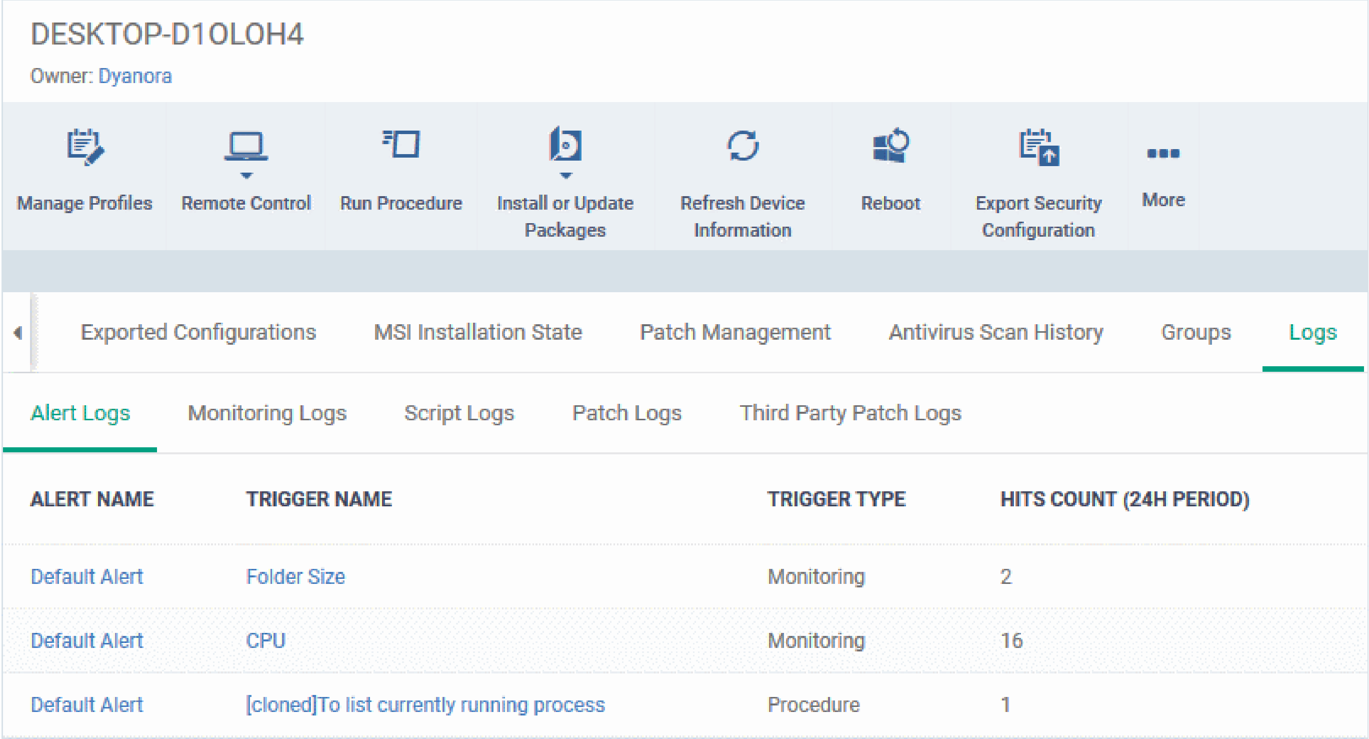
View Alert Logs

'Alerts Logs' logs are generated after a failed procedure deployment or a breach of monitoring conditions.

To view alert logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the Windows device you want to view
- Click the 'Logs' tab then 'Alert Logs'



ALERT NAME	TRIGGER NAME	TRIGGER TYPE	HITS COUNT (24H PERIOD)
Default Alert	Folder Size	Monitoring	2
Default Alert	CPU	Monitoring	16
Default Alert	[cloned]To list currently running process	Procedure	1

Alert Logs - Table of Column Descriptions	
Column Heading	**Description**
Alert Name	The name of the alert that generated the log. Different alerts can be configured for specific events. • Click the alert name to view and manage the configuration parameters of the alert • See '**Manage Alerts**' for more details.
Trigger Name	The name of the monitoring component, procedure or condition that failed. • Click the trigger name to view the configuration parameters of the monitoring settings or the procedure that raised the alert. • See **Monitoring Settings** and **Manage Procedures** for more details.
Trigger Type	The category of trigger, either 'Monitoring' or 'Procedure'.
Hits Count (24 H Period)	The number of instances of this alert in the past 24 hours.

View 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, see **Monitoring Settings** under **Profiles for Windows Devices**.

To view monitoring logs

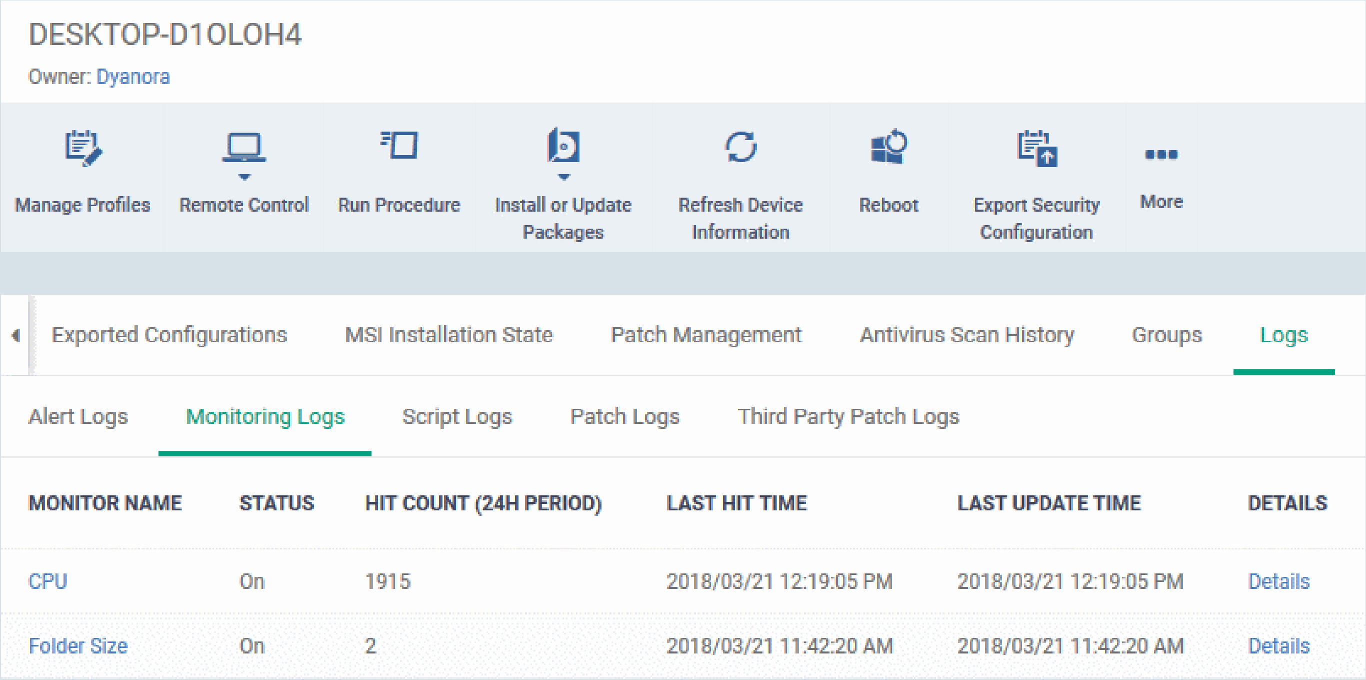
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab

- Select a company or a group to view devices in that group

  Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click the name of the Windows device you want to view
- Click the 'Logs' tab then 'Monitoring Logs'

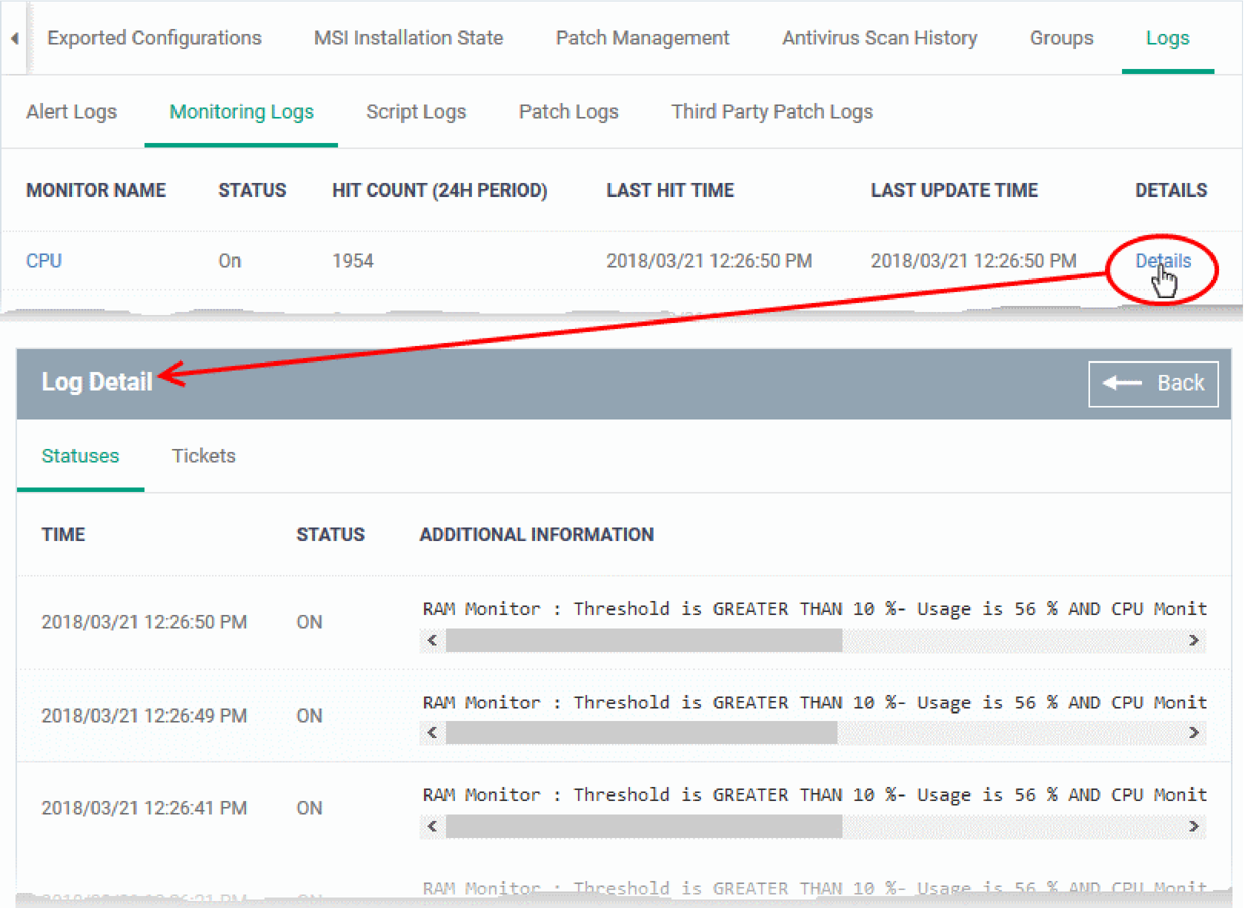


MONITOR NAME	STATUS	HIT COUNT (24H PERIOD)	LAST HIT TIME	LAST UPDATE TIME	DETAILS
CPU	On	1915	2018/03/21 12:19:05 PM	2018/03/21 12:19:05 PM	Details
Folder Size	On	2	2018/03/21 11:42:20 AM	2018/03/21 11:42:20 AM	Details

Monitoring Logs - Table of Column Descriptions	
Column Heading	**Description**
Monitor Name	The name of the monitoring condition in the Windows profile that was violated. • Click the name to view and manage the parameters of the monitoring condition. • See 'Monitoring Settings' for more details.
Status	The status of the device at the time of last monitoring
Hit Count	The number of times the monitoring condition was breached during the last 24 hours.
Last Hit Time	The date and time the monitoring rule was last broken.
Last Update Time	Indicates the date and time when the information was last updated.
Details	• Click the 'Details' link to view a log of the breach events. • See View Details of Monitoring Logs (given below) for more information.

View Details of Monitoring Logs

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



MONITOR NAME	STATUS	HIT COUNT (24H PERIOD)	LAST HIT TIME	LAST UPDATE TIME	DETAILS
CPU	On	1954	2018/03/21 12:26:50 PM	2018/03/21 12:26:50 PM	Details

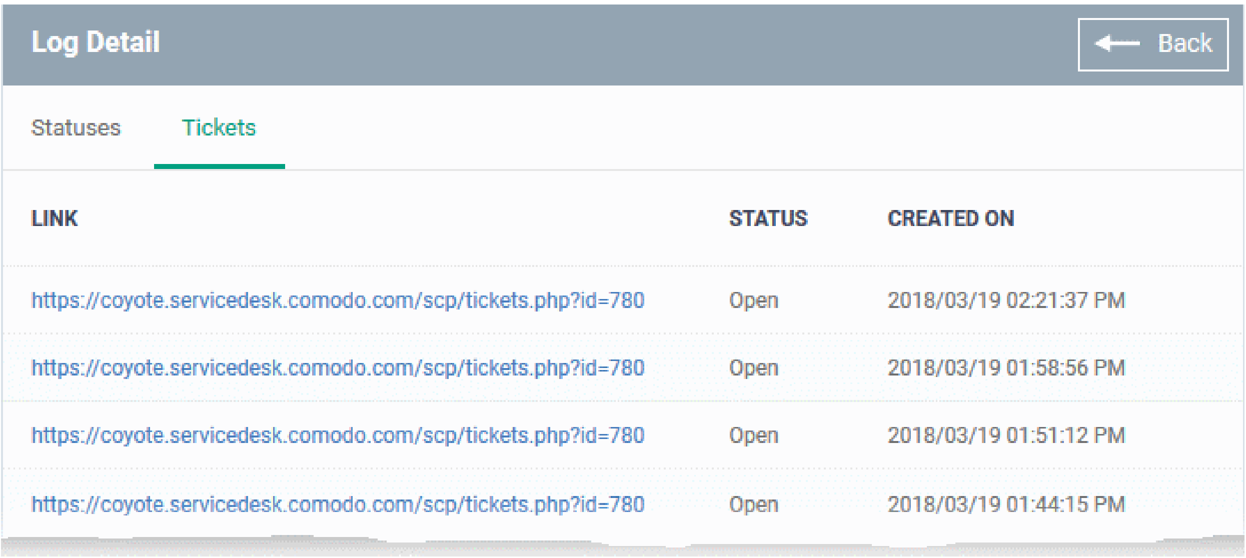
TIME	STATUS	ADDITIONAL INFORMATION
2018/03/21 12:26:50 PM	ON	RAM Monitor : Threshold is GREATER THAN 10 %- Usage is 56 % AND CPU Monit
2018/03/21 12:26:49 PM	ON	RAM Monitor : Threshold is GREATER THAN 10 %- Usage is 56 % AND CPU Monit
2018/03/21 12:26:41 PM	ON	RAM Monitor : Threshold is GREATER THAN 10 %- Usage is 56 % AND CPU Monit
2018/03/21 12:26:21 PM	ON	RAM Monitor : Threshold is GREATER THAN 10 %- Usage is 56 % AND CPU Monit

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	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 - Shows any service desk tickets raised for the alert.



LINK	STATUS	CREATED ON
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 02:21:37 PM
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 01:58:56 PM
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 01:51:12 PM
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 01:44:15 PM

Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions

Column Heading	Description
Link	A link to the support ticket created for the breach event. • Click the link to open the ticket in service desk.
Status	Indicates whether the ticket is open or closed
Created On	The date and time at which the ticket was created.

.

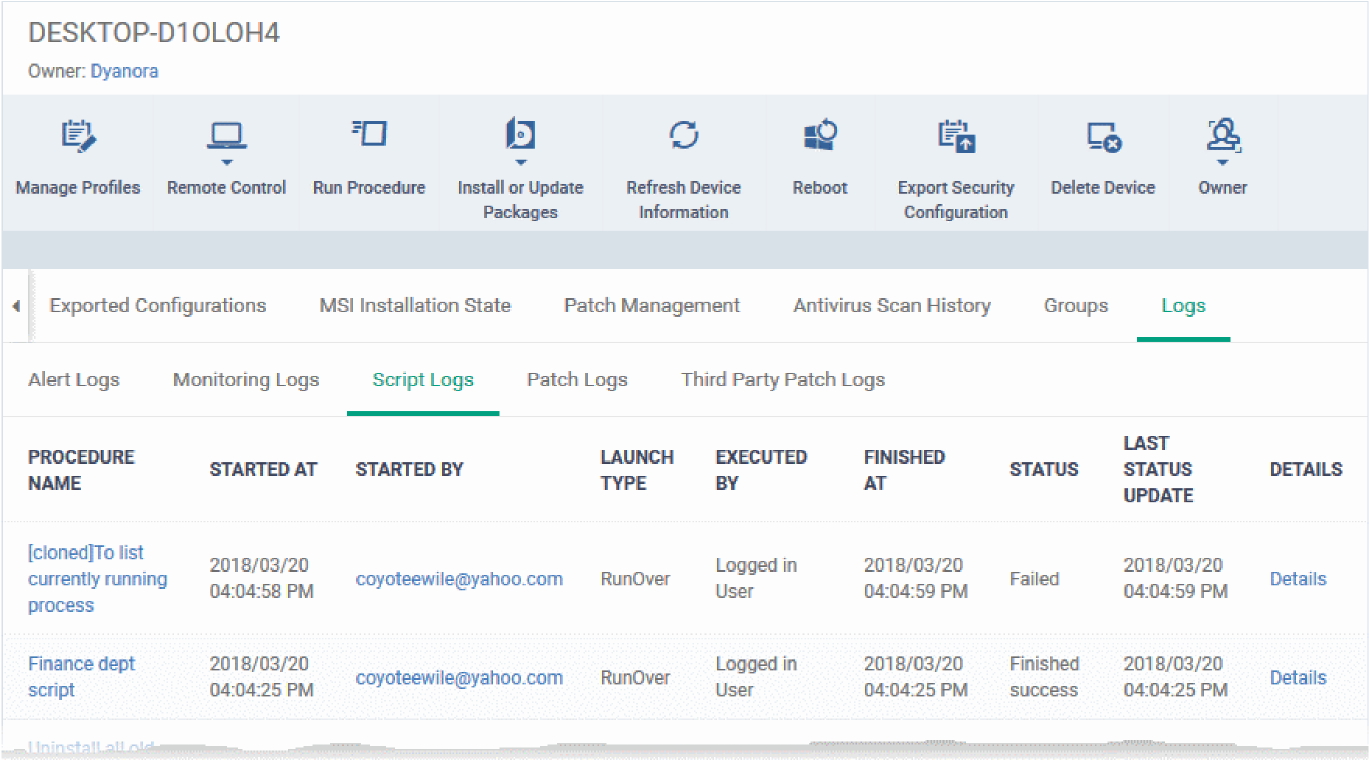
View Script Procedure Logs

- The 'Script Logs' tab shows script procedures that were manually run on Windows devices as well as those run automatically via a profile.
- For more details on creating and running script procedures, see **Manage Procedures**.

To view script procedures logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
    - Select a company or a group to view devices in that group

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the Windows device you want to view
- Click the 'Logs' tab then 'Script Logs'



DESKTOP-D1OLOH4

Owner: Dyanora

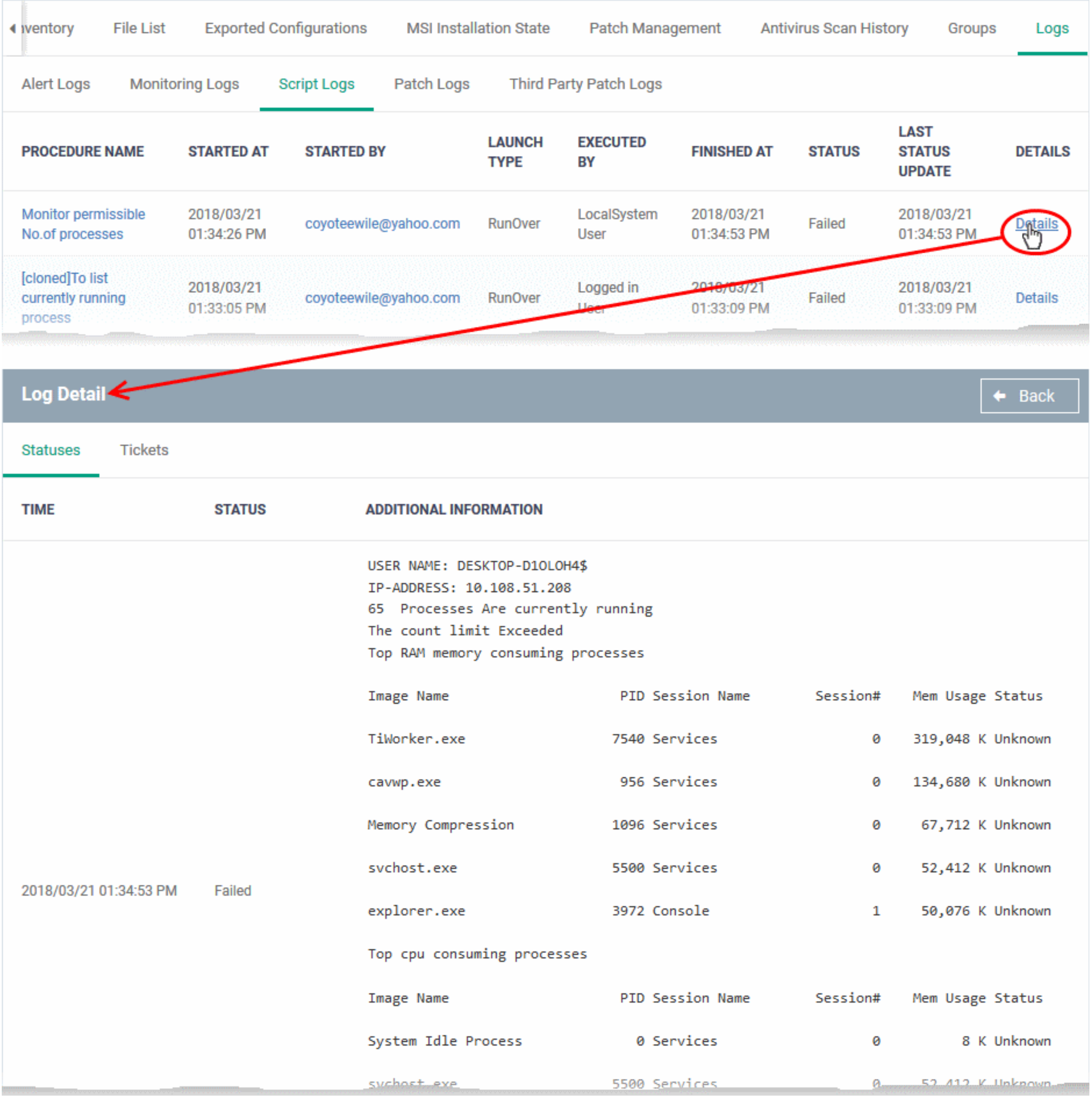
PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	EXECUTED BY	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
[cloned]To list currently running process	2018/03/20 04:04:58 PM	coyoteewile@yahoo.com	RunOver	Logged in User	2018/03/20 04:04:59 PM	Failed	2018/03/20 04:04:59 PM	Details
Finance dept script	2018/03/20 04:04:25 PM	coyoteewile@yahoo.com	RunOver	Logged in User	2018/03/20 04:04:25 PM	Finished success	2018/03/20 04:04:25 PM	Details
Uninstall all old								

Script Procedure Logs - Table of Column Descriptions

Column Heading	Description
Procedure Name	The name of the script procedure that was run on the device. • Click the procedure name to view the configuration parameters of the script procedure. • See **Manage Procedures** for more details.
Started At	The date and time when the procedure commenced.
Started By	Indicates who or what launched the procedure. • The profile name will be shown here if the procedure was run as scheduled in a configuration profile active on the device. • The admins email address will be shown if the procedure was manually initiated.
Launch Type	Indicates whether the procedure was scheduled or run manually.
Executed By	The user account type used by ITSM to execute the procedure.
Finished At	The date and time when the procedure was completed.
Status	Whether the script successfully executed or not. You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details.
Last Status Update	The date and time when the information was last updated.
Details	• Click the 'Details' link to view a log of the procedure's execution. • See the explanation of **View Details of Script Procedure Logs** given below.

View Script Procedure Log details

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



PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	EXECUTED BY	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
Monitor permissible No.of processes	2018/03/21 01:34:26 PM	coyoteewile@yahoo.com	RunOver	LocalSystem User	2018/03/21 01:34:53 PM	Failed	2018/03/21 01:34:53 PM	Details
[cloned]To list currently running process	2018/03/21 01:33:05 PM	coyoteewile@yahoo.com	RunOver	Logged in User	2018/03/21 01:33:09 PM	Failed	2018/03/21 01:33:09 PM	Details

TIME	STATUS	ADDITIONAL INFORMATION
2018/03/21 01:34:53 PM	Failed	(see below)

```
USER NAME: DESKTOP-D1OLOH4$
IP-ADDRESS: 10.108.51.208
65  Processes Are currently running
The count limit Exceeded
Top RAM memory consuming processes

Image Name                     PID Session Name        Session#    Mem Usage Status

TiWorker.exe                  7540 Services                   0    319,048 K Unknown

cavwp.exe                      956 Services                   0    134,680 K Unknown

Memory Compression            1096 Services                   0     67,712 K Unknown

svchost.exe                   5500 Services                   0     52,412 K Unknown

explorer.exe                  3972 Console                    1     50,076 K Unknown

Top cpu consuming processes

Image Name                     PID Session Name        Session#    Mem Usage Status

System Idle Process              0 Services                   0          8 K Unknown

svchost.exe                   5500 Services                   0     52,412 K Unknown
```

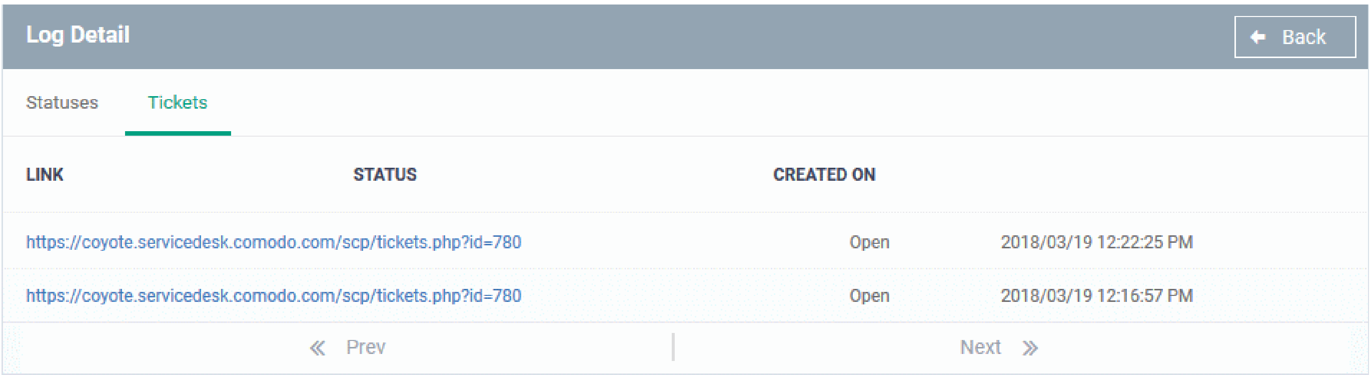
The details are displayed under two tabs:

Statuses - The date and time at which successive stages in the procedure were run, their success status and results.

Script Procedure Log Details - 'Statuses' tab - Table of Column Descriptions	
Column Heading	**Description**
Time	The date and time of the procedure execution.
Status	Whether the execution was successful or not.
Additional Information	Provides details on the execution:

	• If successful, displays the results of the procedure execution • If failed, displays the reason for not running the procedure

Tickets - Displays tickets raised for any failed procedures.



LINK	STATUS	CREATED ON
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 12:22:25 PM
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 12:16:57 PM

Script Procedure Log Details - 'Tickets' tab - Table of Column Descriptions	
Column Heading	**Description**
Link	A link to the support ticket created for the breach event. • Click the link to open the ticket in service desk.
Status	Indicates whether the ticket is open or closed
Created On	The date and time at which the ticket was created.

View OS Patch Procedure Logs

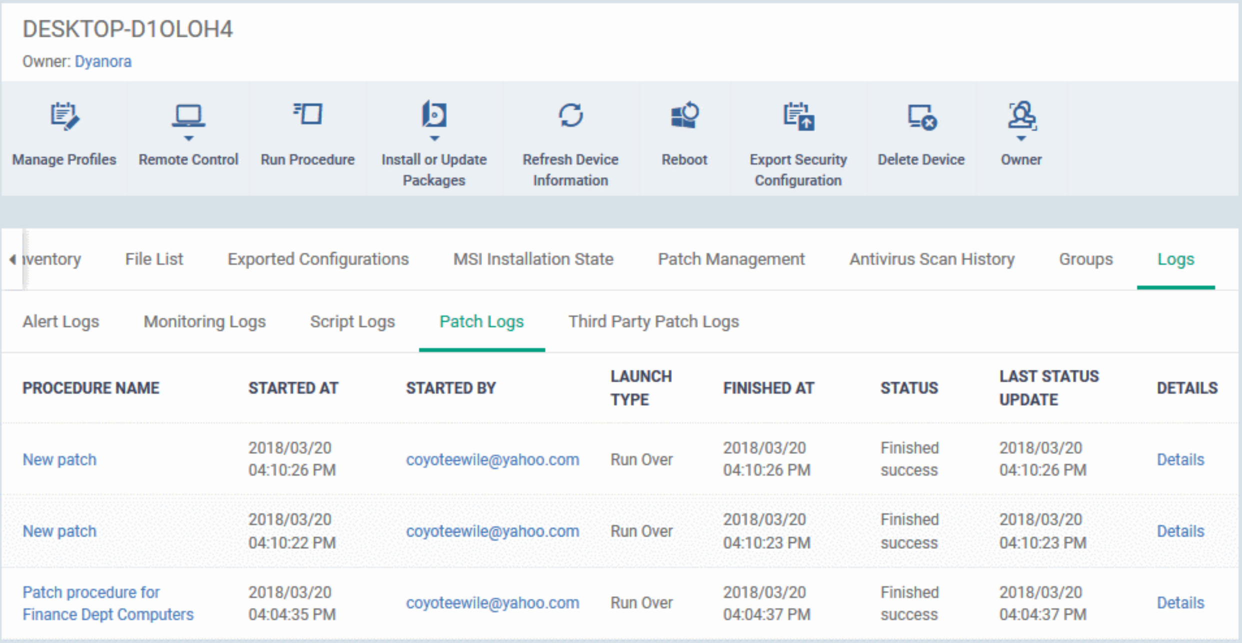
- The 'Patch Logs' tab shows OS patch procedures that were manually run on Windows devices as well as those run automatically via a profile.
- For more details on creating and running patch procedures, see **Manage Procedures**.

To view patch procedures logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view devices in that group

  Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the Windows device you want to view
- Click the 'Logs' tab then 'Patch Logs'


DESKTOP-D1OLOH4

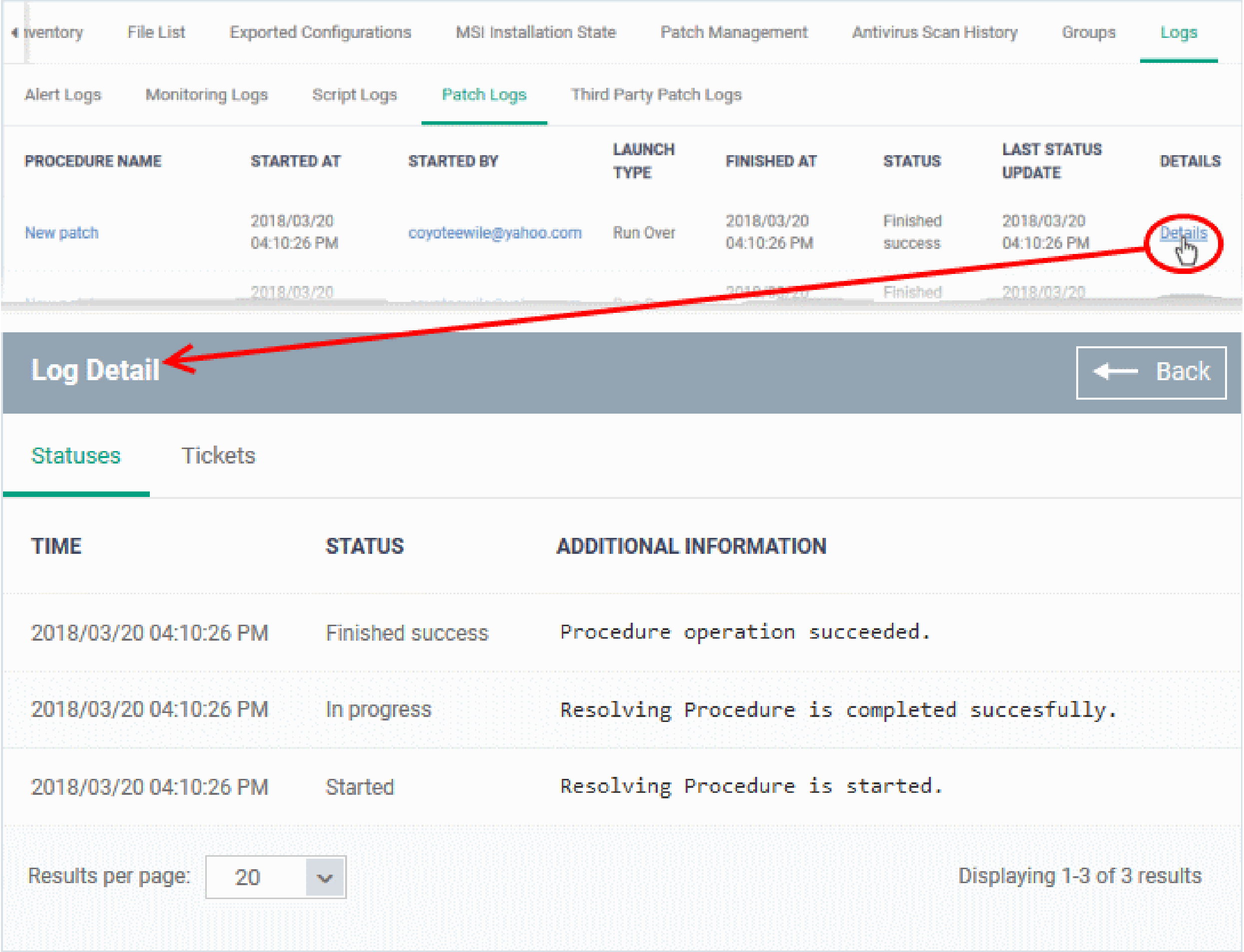
Owner: Dyanora

PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
New patch	2018/03/20 04:10:26 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:10:26 PM	Finished success	2018/03/20 04:10:26 PM	Details
New patch	2018/03/20 04:10:22 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:10:23 PM	Finished success	2018/03/20 04:10:23 PM	Details
Patch procedure for Finance Dept Computers	2018/03/20 04:04:35 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:04:37 PM	Finished success	2018/03/20 04:04:37 PM	Details

Patch Procedure Logs - Table of Column Descriptions	
Column Heading	**Description**
Procedure Name	The name of the patch procedure that was run on the device. • Click the procedure name to view and manage the configuration parameters of it. • See '**Manage Procedures**' for more details.
Started At	The date and time when the procedure commenced.
Started By	Indicates who or what launched the procedure. • The profile name will be shown here if the procedure was run as scheduled in a configuration profile active on the device. • The admins email address will be shown if the procedure was manually initiated.
Launch Type	Whether the procedure was scheduled or run manually.
Finished At	The date and time when the procedure was completed.
Status	Whether the OS patch procedure was successfully executed or not. You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details.
Last Status Update	The date and time when the information was last updated.
Details	• Click the 'Details' link to view a log of the procedure's execution. • See the explanation of **View Details of OS Patch Procedure Logs** given below.

View OS Patch Procedure Log details

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



PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
New patch	2018/03/20 04:10:26 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:10:26 PM	Finished success	2018/03/20 04:10:26 PM	Details

TIME	STATUS	ADDITIONAL INFORMATION
2018/03/20 04:10:26 PM	Finished success	Procedure operation succeeded.
2018/03/20 04:10:26 PM	In progress	Resolving Procedure is completed succesfully.
2018/03/20 04:10:26 PM	Started	Resolving Procedure is started.

Results per page: 20

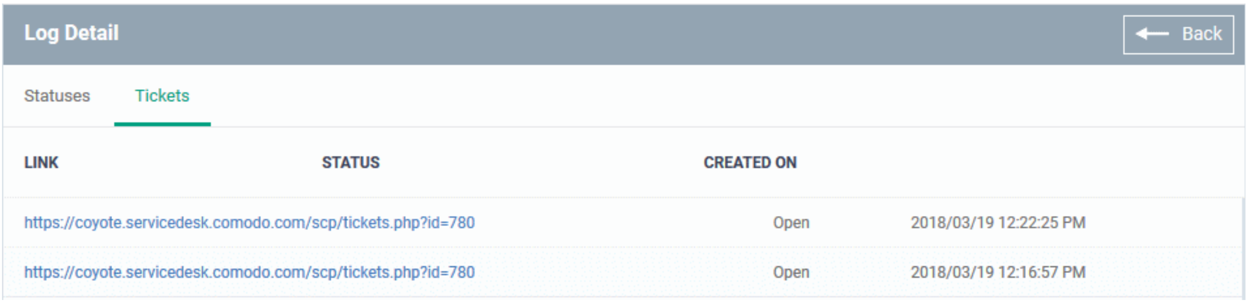
Displaying 1-3 of 3 results

The details are displayed under two tabs:

Statuses - The date and time at which successive stages in the procedure were run, their success status and results.

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

Tickets - Displays tickets raised for any failed procedures.



LINK	STATUS	CREATED ON
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 12:22:25 PM
https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780	Open	2018/03/19 12:16:57 PM

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

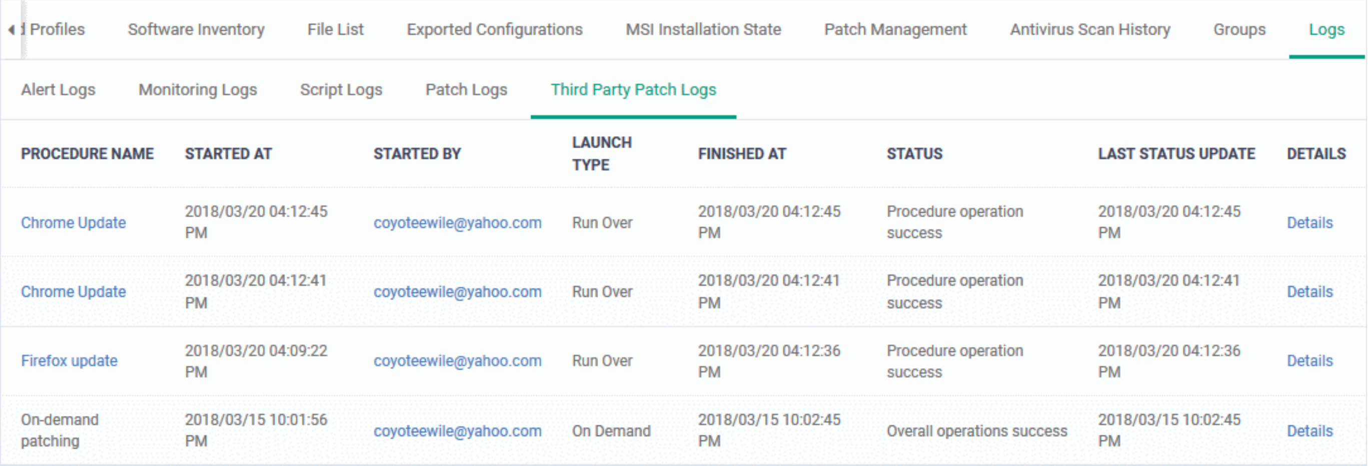
View Third Party Patch Procedure Logs

- The 'Third Party Patch Logs' tab shows procedures for updating third party applications.
- This includes procedures that were manually run on Windows devices and those run automatically via a profile.
- For more details on creating and running patch procedures, see **Manage Procedures**.

To view patch procedures logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the Windows device you want to view
- Click the 'Logs' tab then "Third Patch Logs'



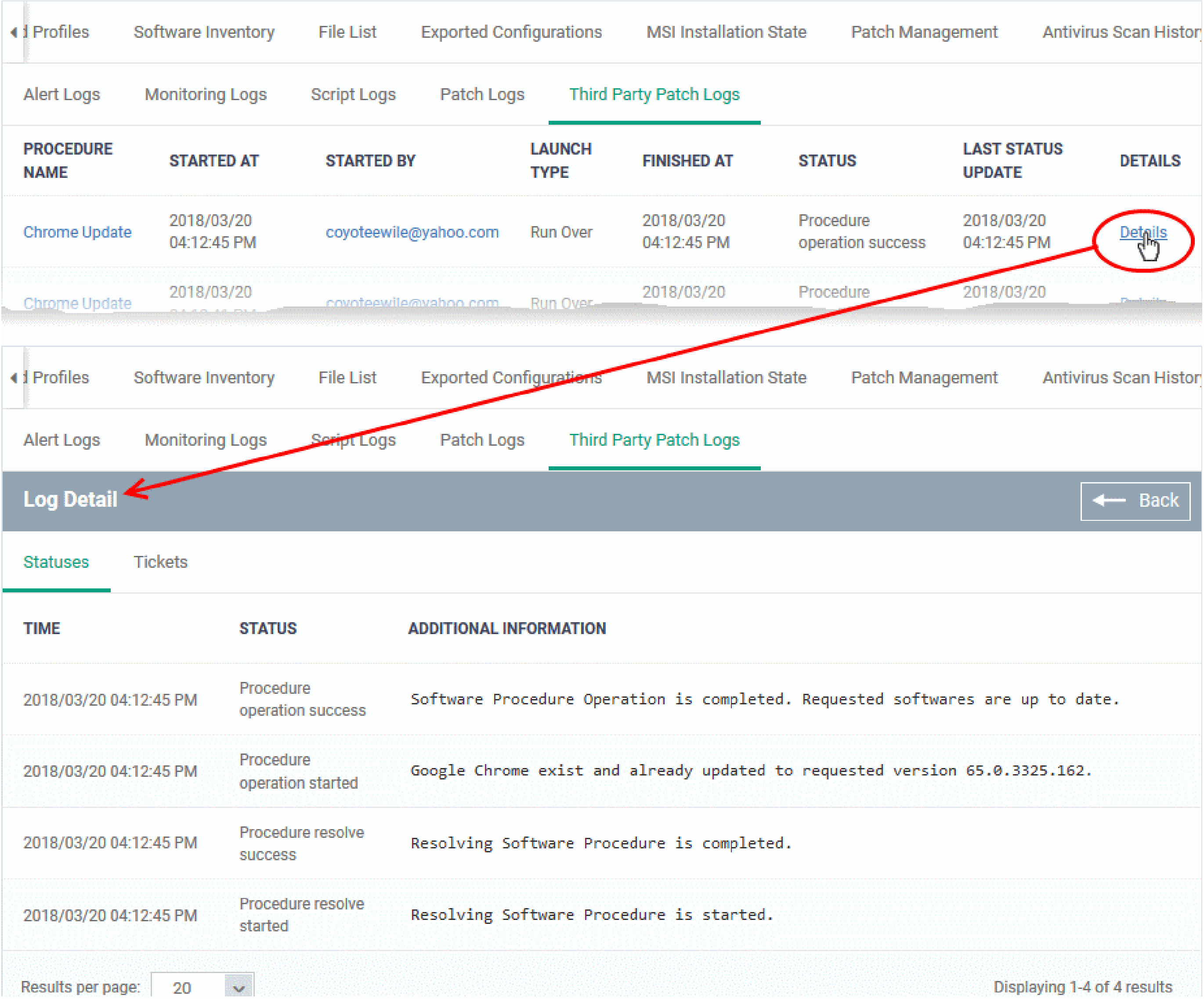
PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
Chrome Update	2018/03/20 04:12:45 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:12:45 PM	Procedure operation success	2018/03/20 04:12:45 PM	Details
Chrome Update	2018/03/20 04:12:41 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:12:41 PM	Procedure operation success	2018/03/20 04:12:41 PM	Details
Firefox update	2018/03/20 04:09:22 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:12:36 PM	Procedure operation success	2018/03/20 04:12:36 PM	Details
On-demand patching	2018/03/15 10:01:56 PM	coyoteewile@yahoo.com	On Demand	2018/03/15 10:02:45 PM	Overall operations success	2018/03/15 10:02:45 PM	Details

Third Party Patch Logs - Table of Column Descriptions	
Column Heading	**Description**
Procedure Name	The name of the procedure that was run on the device. • Click the procedure name to view and manage the configuration parameters of the third party patch procedure.

	• See '**Manage Procedures**' for more details.
Started At	The date and time when the procedure commenced.
Started By	Indicates who or what launched the procedure. • The profile name will be shown here if the procedure was run as scheduled in a configuration profile active on the device. • The admins email address will be shown if the procedure was manually initiated.
Launch Type	Indicates whether the procedure was scheduled or run manually.
Finished At	The date and time when the procedure was completed.
Status	Indicates whether the third party patch procedure was successfully executed or not. • You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details.
Last Status Update	The date and time when the information was last updated.
Details	• Click the 'Details' link to view a log of the procedure's execution. • See explanation of **View Details of Third Party Patch Procedure Logs** given below.

View Third Party Patch Procedure Log details

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



PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
Chrome Update	2018/03/20 04:12:45 PM	coyoteewile@yahoo.com	Run Over	2018/03/20 04:12:45 PM	Procedure operation success	2018/03/20 04:12:45 PM	Details

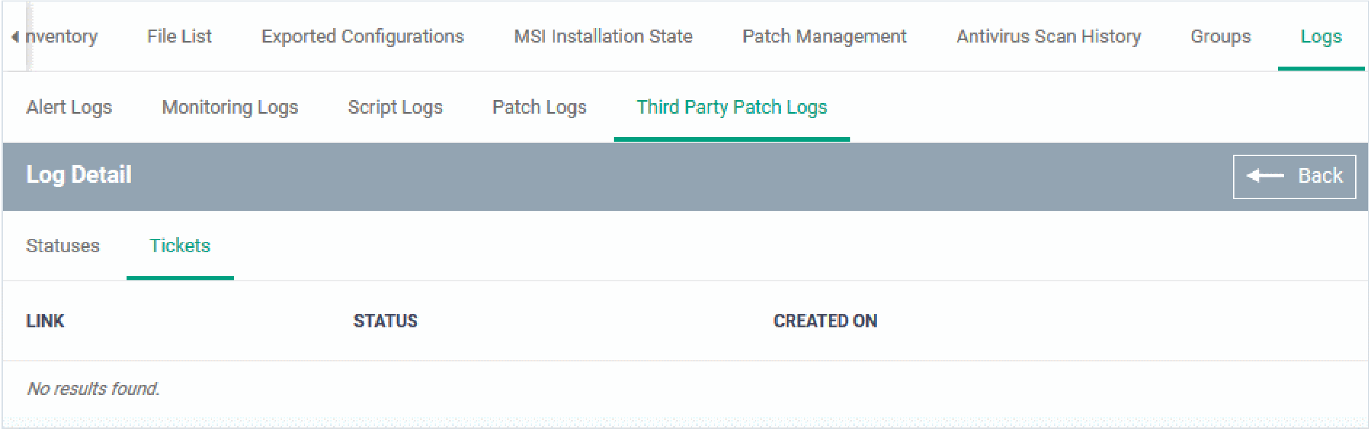
TIME	STATUS	ADDITIONAL INFORMATION
2018/03/20 04:12:45 PM	Procedure operation success	Software Procedure Operation is completed. Requested softwares are up to date.
2018/03/20 04:12:45 PM	Procedure operation started	Google Chrome exist and already updated to requested version 65.0.3325.162.
2018/03/20 04:12:45 PM	Procedure resolve success	Resolving Software Procedure is completed.
2018/03/20 04:12:45 PM	Procedure resolve started	Resolving Software Procedure is started.

The details are displayed under two tabs:

Statuses - The date and time at which successive stages in the procedure were run, their success status and results.

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

Tickets - Displays tickets raised for any failed procedures.



LINK	STATUS	CREATED ON
No results found.		

Third Party Patch Log Details - 'Tickets' tab - Table of Column Descriptions	
Column Heading	**Description**
Link	A link to the support ticket created for the breach event. • Click the link to open the ticket in service desk.
Status	Indicates whether the ticket is open or closed
Created On	The date and time at which the ticket was created.

5.2.2. Manage Mac OS Devices

The Mac OS device details page shows OS and software details, installed applications, security information from Comodo Antivirus, network connections and more. Administrators can also manage configuration profiles for the endpoint, remotely install Mac OS packages and manage group membership.

To view and manage a Mac OS device

- Click the 'Devices' tab on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

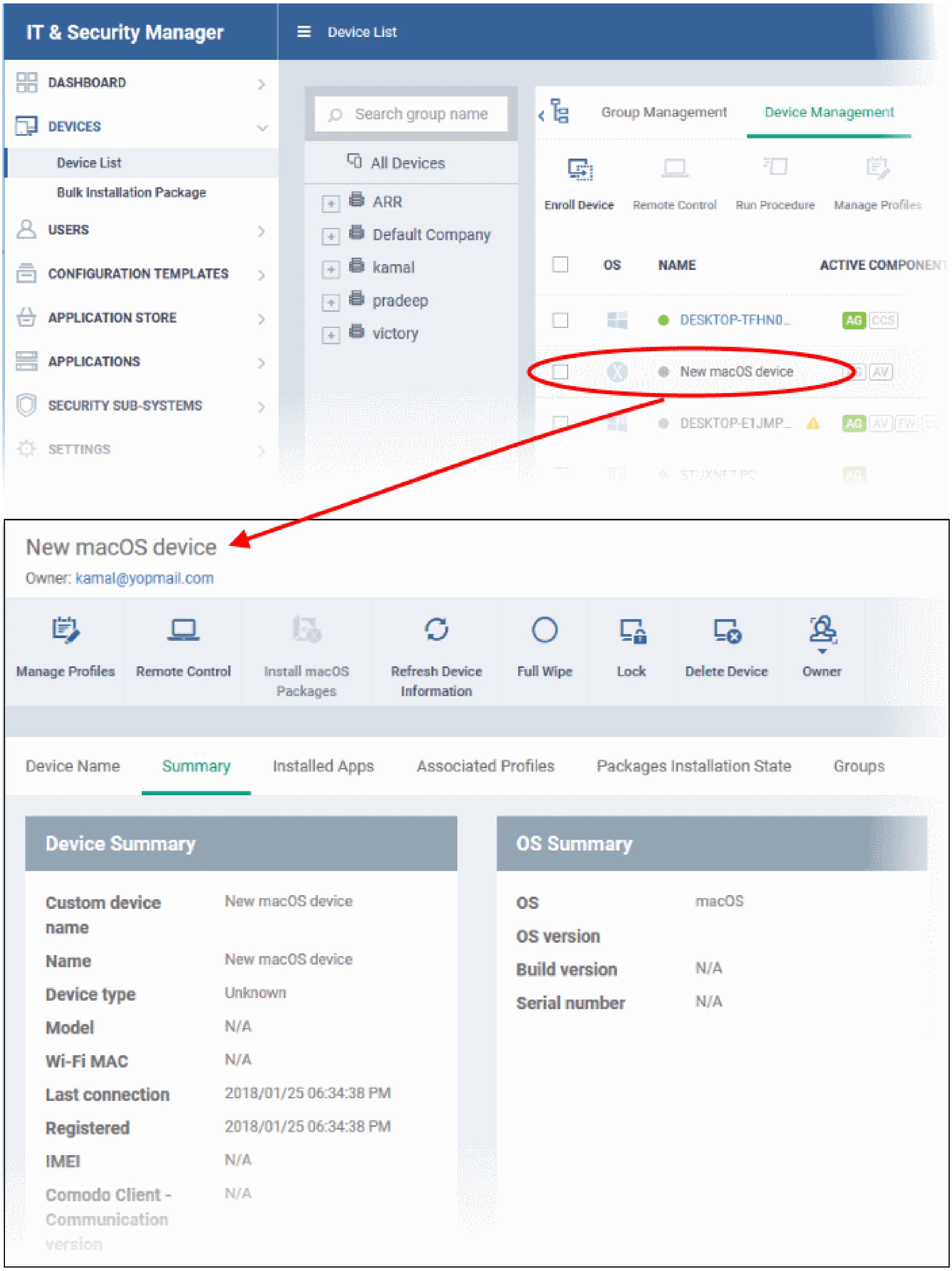
The interface displays devices belonging to the company or group selected on the left.

  - Select the Company and choose the group under it to view the list of devices in that group

    Or

  - Select 'All Devices' to view every device enrolled to ITSM

- Click the name of any Mac OS device to open its 'Device Details' pane:



New macOS device

Owner: kamal@yopmail.com

Device Summary

Custom device name	New macOS device
Name	New macOS device
Device type	Unknown
Model	N/A
Wi-Fi MAC	N/A
Last connection	2018/01/25 06:34:38 PM
Registered	2018/01/25 06:34:38 PM
IMEI	N/A
Comodo Client - Communication version	N/A

OS Summary

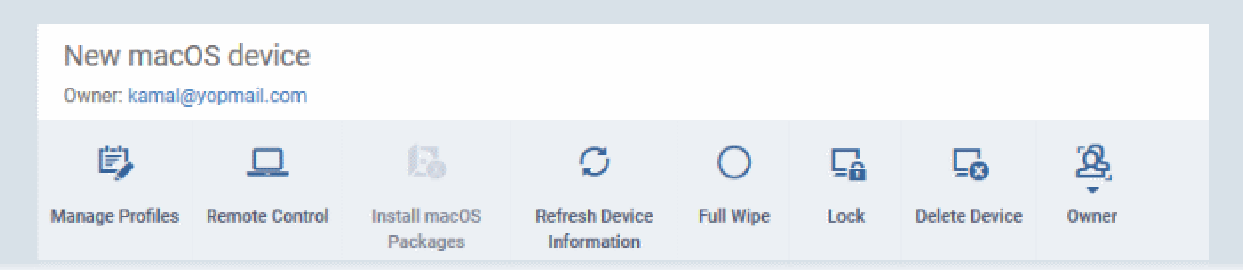
OS	macOS
OS version	
Build version	N/A
Serial number	N/A

This displays details of the selected device under six tabs. The 'Summary' tab will be displayed by default.

- **Device Name** - The device label. You can change this as per your preferences. See **Viewing and Editing Mac OS Device Name** for more details.
- **Summary** - General details of the device, including device information, OS details, Network details and security configuration. See **Viewing Summary Information** for more details.

- **Installed Apps** - A list of applications currently installed on the device, along with their versions. See **Viewing Installed Applications** for more details.
- **Associated Profiles** - Details of profiles deployed on the device. See **Viewing and Managing Profiles Associated with the Device** for more details.
- **Package Installation State** - Mac OS packages that have been installed on the device via ITSM. See **Viewing Mac OS Packages Installed on the Device through ITSM** for more details.
- **Groups** - Device groups to which the endpoint belongs. You can manage group membership from here. See **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.



New macOS device

Owner: kamal@yopmail.com

- **Manage Profiles** - Add or remove device profiles. See **Assigning Configuration Profiles to Selected Devices** for more details.
- **Remote Control** - Establish a remote desktop connection to an endpoint. See **Remote Management of Windows and Mac OS Devices** for more details
- **Install Mac OS Packages** - Remotely install Comodo Antivirus for Mac and other Mac OS packages. See **Remotely Installing Packages onto Mac OS Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. See **Updating Device Information** for more details.
- **Wipe / Corporate** - Delete data stored on the device if it is lost or stolen. See **Wiping Data from Devices** for more details
- **Lock/Unlock Mac OS** - Remotely lock or unlock the device if it is lost, misplaced or stolen. See **Locking/Unlocking Devices** for more details
- **Delete Device** - Removes the device from ITSM. See **Removing a Device** for more details.
- **Change Owner** - Change the user with whom the device is associated. See **Changing a Device's Owner** for more details.
- **Change Ownership Type** - Changes the 'Bring Your Own Device' (BYOD) status of the device. See '**Changing the ownership status of a Device**' for more details.

5.2.2.1. View and Edit Mac OS Device Name

- Enrolled devices are listed by the name assigned to them by their owner.
- If no name was assigned then the actual device name or model number will be used.
- 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.
- If 'Allow Auto Rename of Device Custom Name' is enabled then the custom name will be replaced automatically by the device name/model number during the next sync. To retain the custom name for the device, make sure to disable this option.

To change a device name

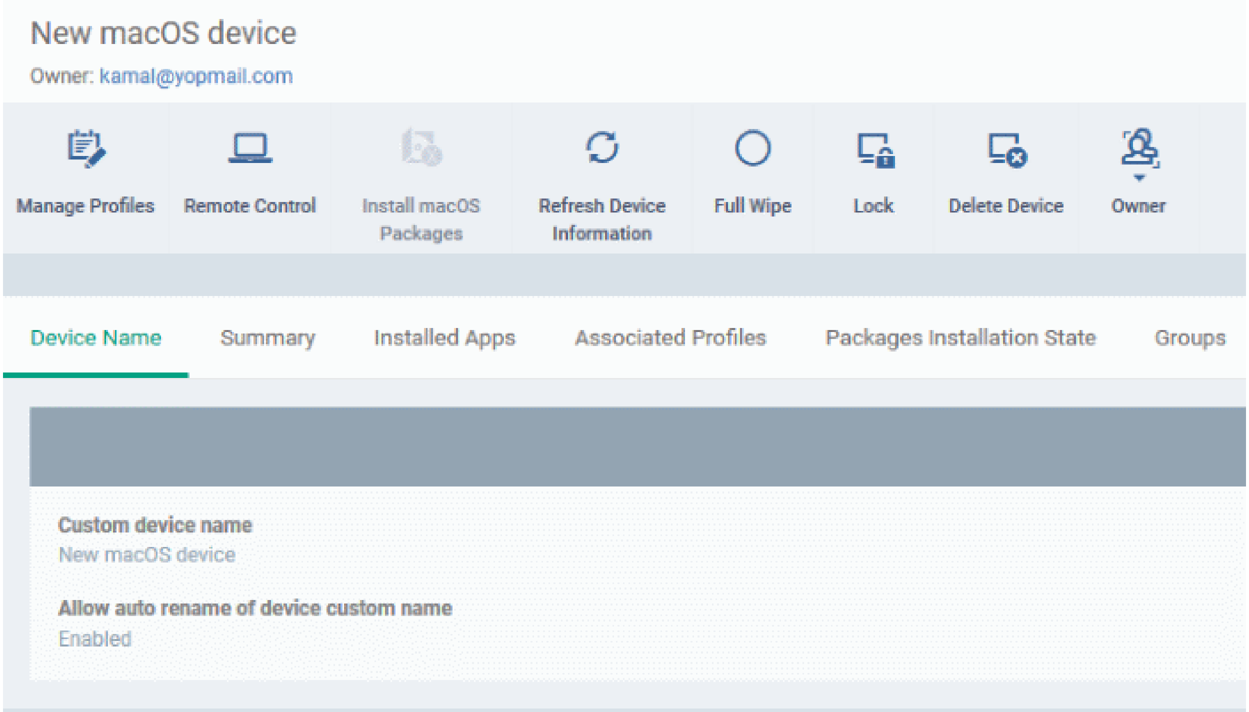
- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

- Select a company or a group to view the list of devices in that group

  Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click on any Mac OS device then select the 'Device Name' tab



New macOS device

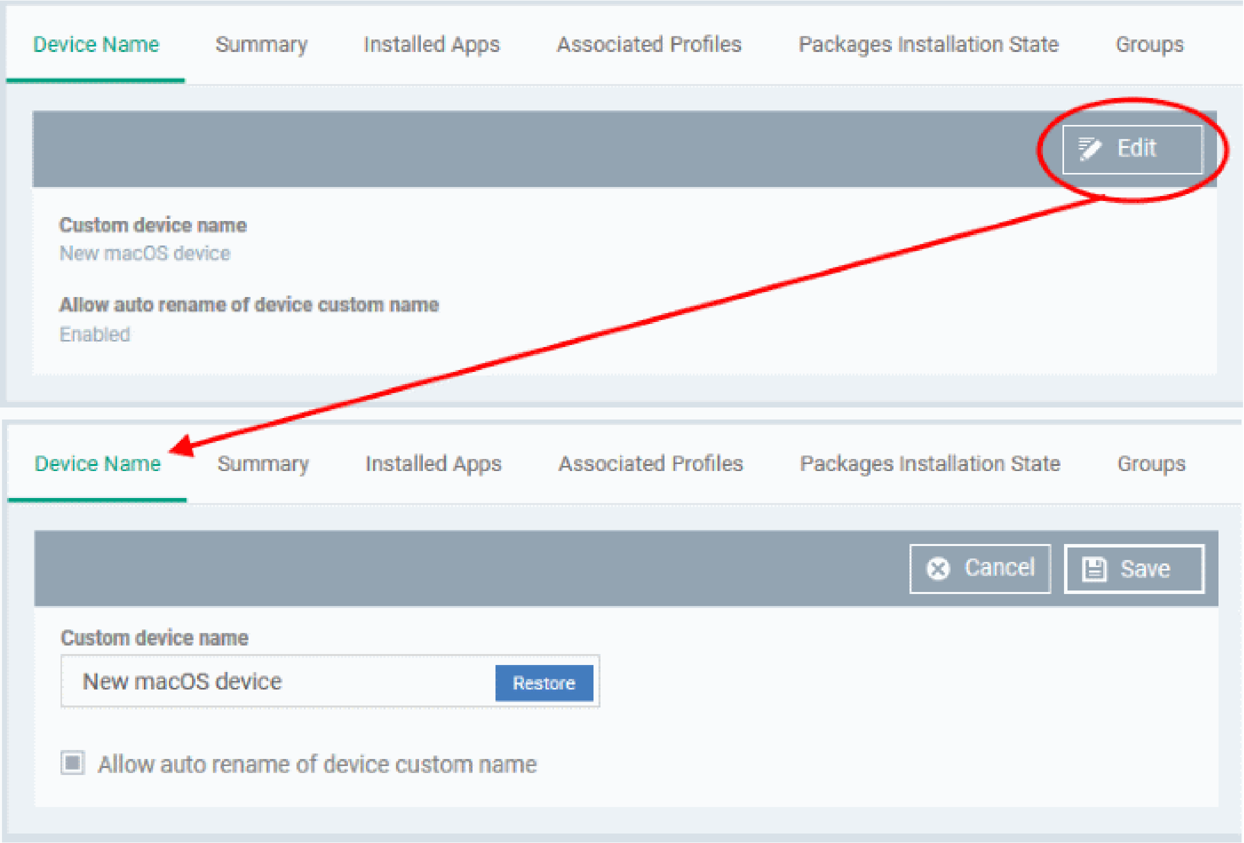
Owner: kamal@yopmail.com

Custom device name
New macOS device

Allow auto rename of device custom name
Enabled

- 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.



Custom device name
New macOS device

Allow auto rename of device custom name
Enabled

Custom device name
New macOS device

■ Allow auto rename of device custom name

- 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'.

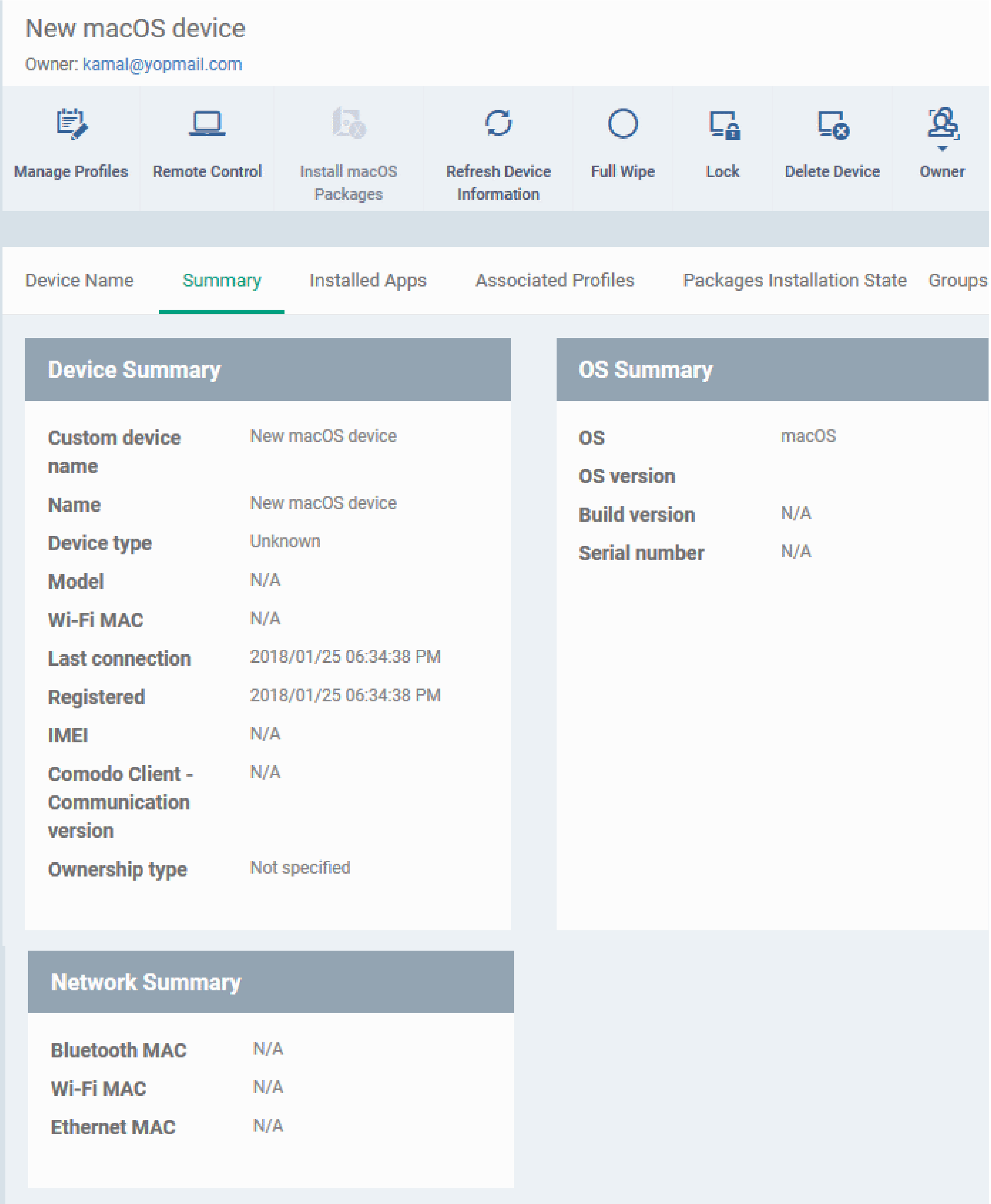
5.2.2.2. View Summary Information

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

To view the device information summary

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Mac OS device then select the 'Summary' tab (if it is not already open).



Device Summary

Custom device name	New macOS device
Name	New macOS device
Device type	Unknown
Model	N/A
Wi-Fi MAC	N/A
Last connection	2018/01/25 06:34:38 PM
Registered	2018/01/25 06:34:38 PM
IMEI	N/A
Comodo Client - Communication version	N/A
Ownership type	Not specified

OS Summary

OS	macOS
OS version	
Build version	N/A
Serial number	N/A

Network Summary

Bluetooth MAC	N/A
Wi-Fi MAC	N/A
Ethernet MAC	N/A

- **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 version number, virus database version and its update status.

5.2.2.3. View Installed Applications

The 'Device Details' interface allows you to view all applications on a managed Mac OS device.

To view the list of applications

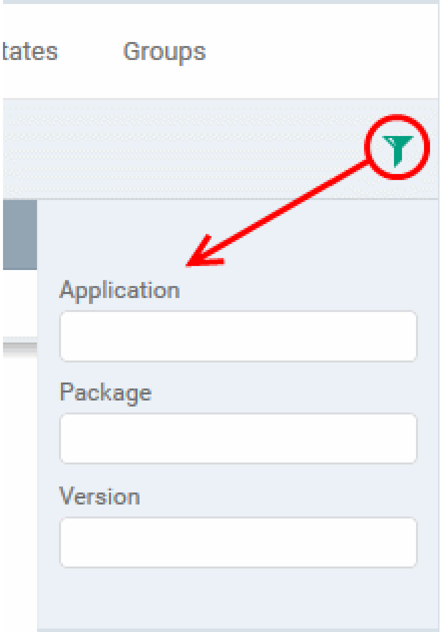
- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
    - Select a company or a group on the left to view a list of devices in that group

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any 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 Management**' interface, listing only the devices in which the same application is installed.
Package	Indicates the source of the application, i.e downloaded Mac OS package, from which the application was installed.
Version	Indicates the version number of the application.

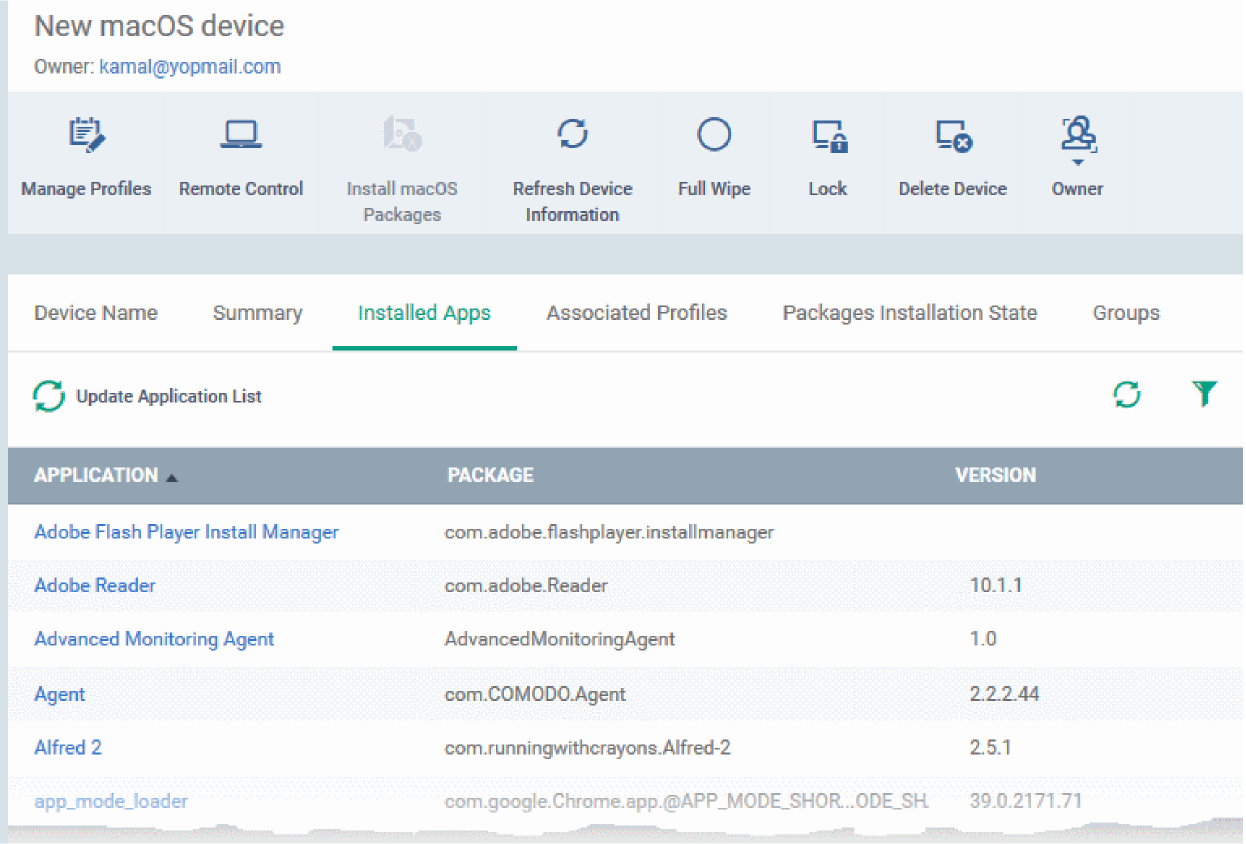
Sorting and Filtering Options

- 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.



APPLICATION	PACKAGE	VERSION
Adobe Flash Player Install Manager	com.adobe.flashplayer.installmanager	
Adobe Reader	com.adobe.Reader	10.1.1
Advanced Monitoring Agent	AdvancedMonitoringAgent	1.0
Agent	com.COMODO.Agent	2.2.2.44
Alfred 2	com.runningwithcrayons.Alfred-2	2.5.1
app_mode_loader	com.google.Chrome.app.@APP_MODE_SHOR...ODE_SH	39.0.2171.71

- 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'

5.2.2.4. View and Manage Profiles Associated with a Device

The 'Associated Profiles' tab lists 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 of the device
- Because the device belongs to a device group
- Because the user of the device belongs to a user group

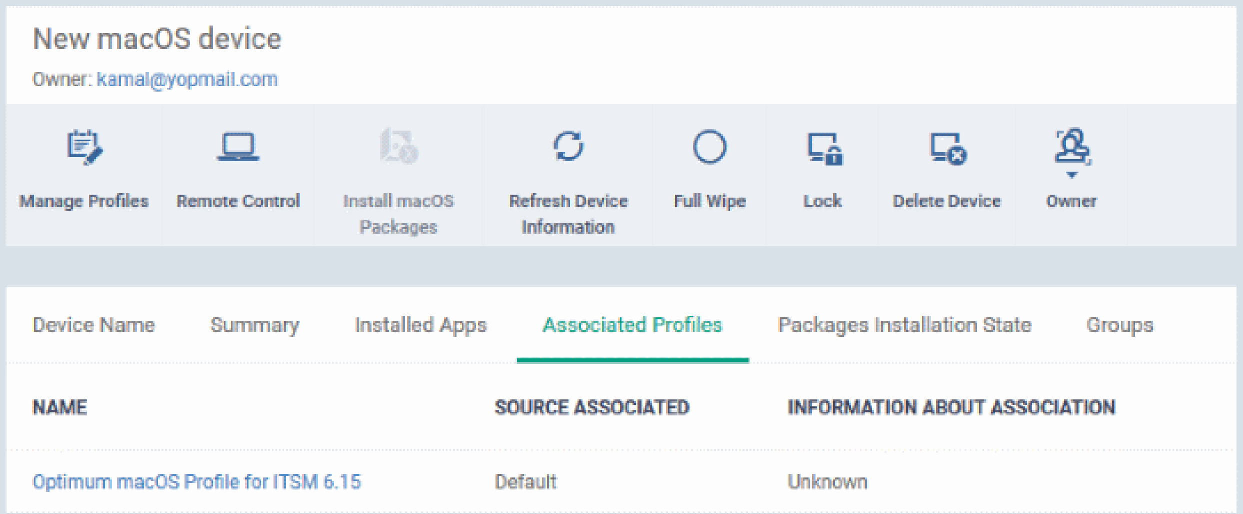
For more details on profiles and groups of profiles, see **Configuration Profiles**.

To view and manage the profiles associated with a device

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

    Or

    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Mac OS device then select the 'Associated Profiles' tab



New macOS device
Owner: kamal@yopmail.com

NAME	SOURCE ASSOCIATED	INFORMATION ABOUT ASSOCIATION
Optimum macOS Profile for ITSM 6.15	Default	Unknown

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. See **Editing Configuration Profiles** for more details.
Source Associated	Indicates the source through which the profile was applied to the device. Configuration profiles can be applied to a device in different ways: • Profiles can be directly applied to the device. See **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. See **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. See **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. See **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.

5.2.2.5. View Mac OS Packages Installed on a Device through ITSM

- ITSM allows you to remotely install packages on to managed MAC OS endpoints.

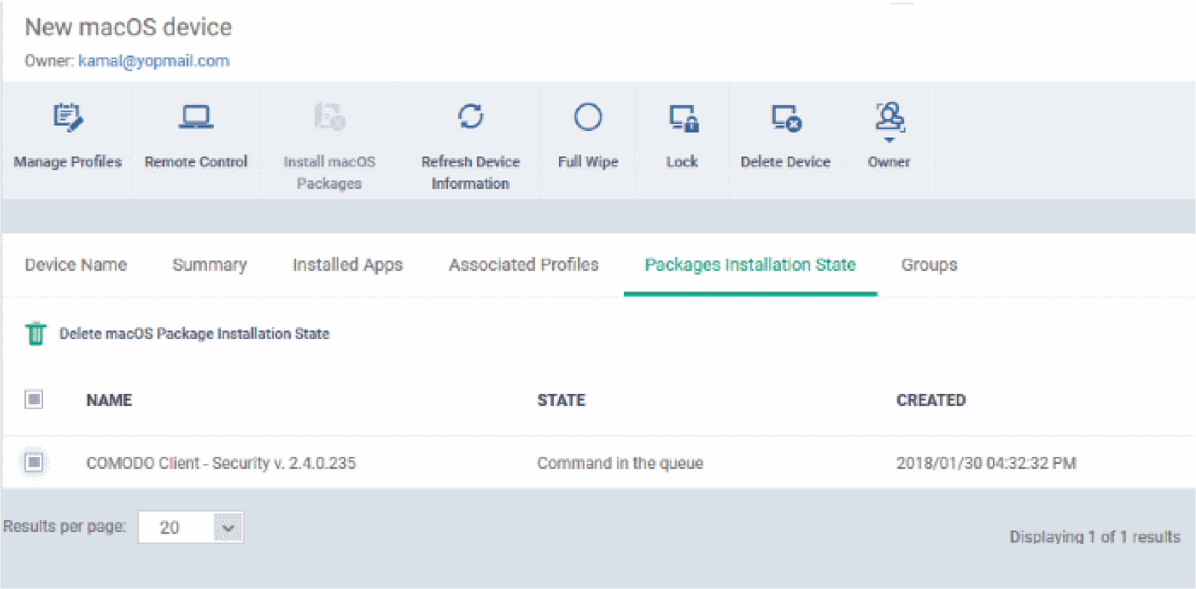
- These can be Comodo applications like Comodo Antivirus for Mac (CAVM), or third-party Mac OS packages.
- For more information, see **Remotely Installing Packages on Mac OS Devices**.

Note: Currently only CAVM can be remotely installed on Mac OS devices from ITSM. Support for other ITSM packages and third party Mac OS packages will be available in the future versions.

To view list of Mac OS packages installed on an endpoint through ITSM

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Mac OS device then select the 'Packages Installation States' tab


New macOS device

Owner: kamal@yopmail.com

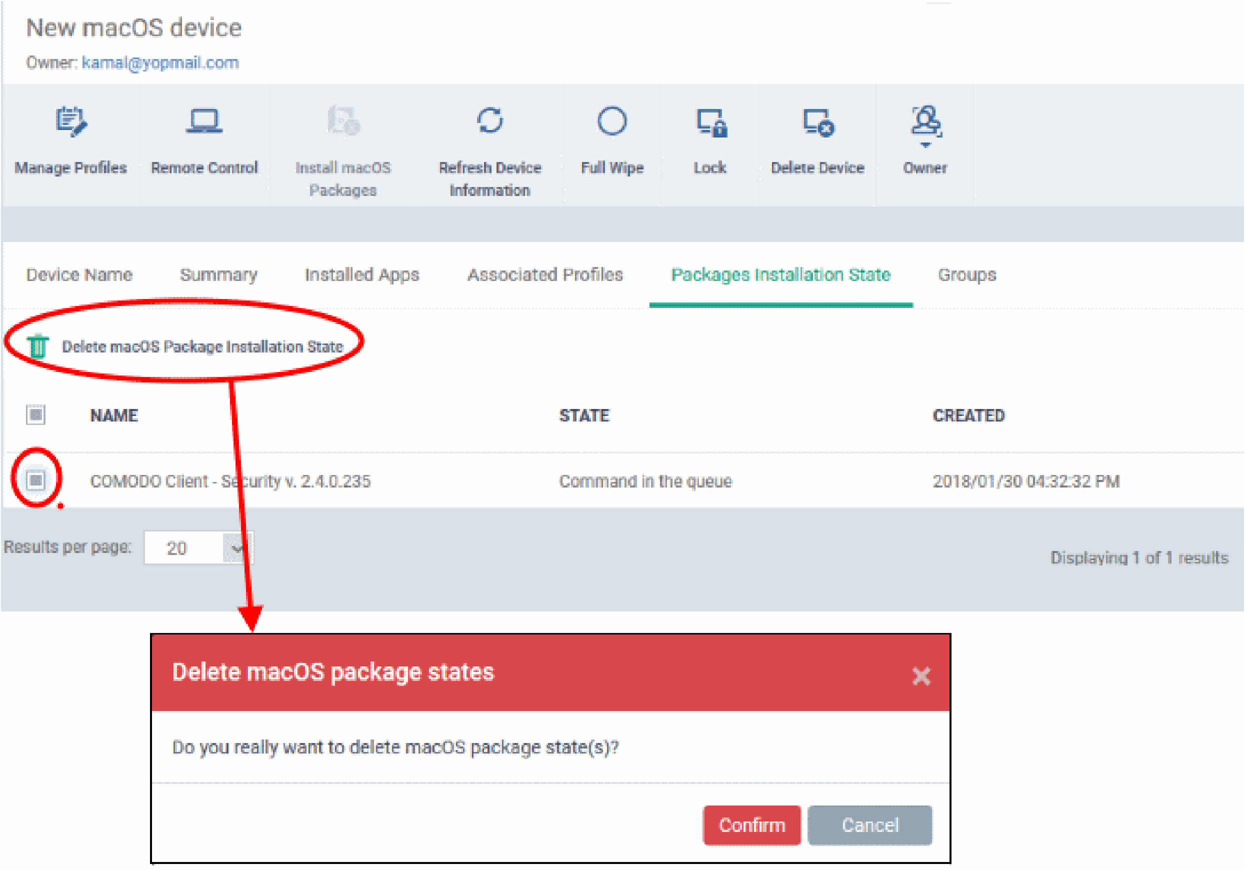
NAME	STATE	CREATED
COMODO Client - Security v. 2.4.0.235	Command in the queue	2018/01/30 04:32:32 PM

Results per page: 20

Displaying 1 of 1 results

MSI Installation State - Table of Column Descriptions	
Column Heading	**Description**
Name	Displays the URL/file name of the Mac OS 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 macOS Package Installation State'.


New macOS device

Owner: kamal@yopmail.com

□	NAME	STATE	CREATED
□	COMODO Client - Security v. 2.4.0.235	Command in the queue	2018/01/30 04:32:32 PM

Results per page: 20

Displaying 1 of 1 results

Delete macOS package states

Do you really want to delete macOS package state(s)?

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

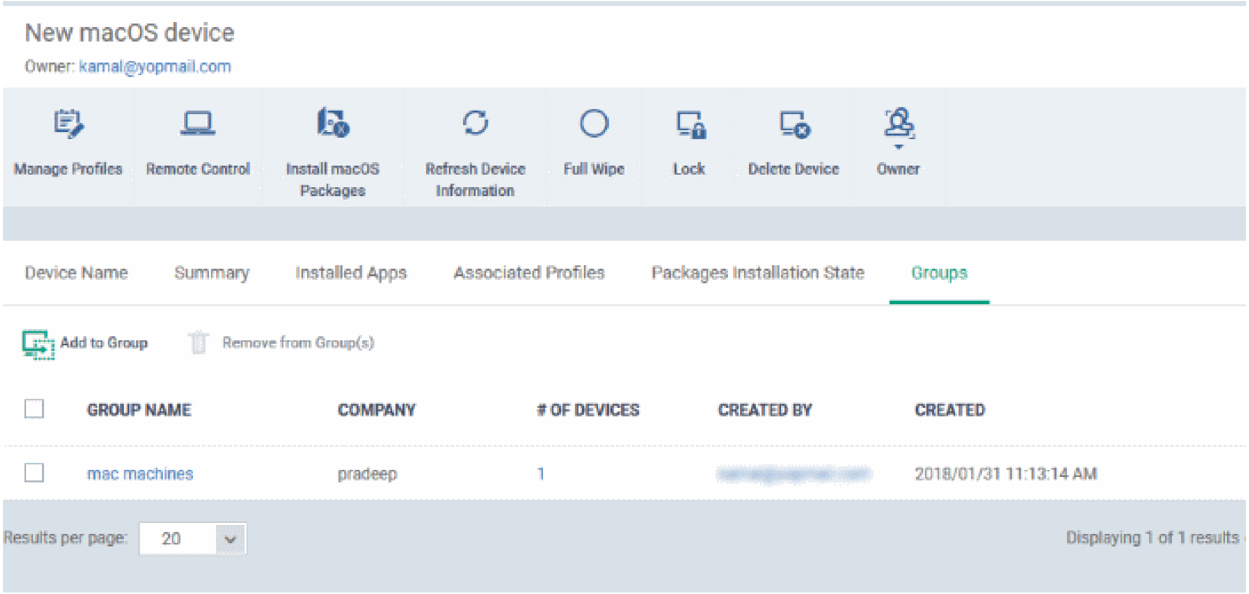
- Click 'Confirm' to remove the file from the list

5.2.2.6. View and Manage Device Group Memberships

To view and manage the device group membership

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of a Mac OS device then select the 'the 'Groups' tab



New macOS device

Owner: kamal@yopmail.com

□	GROUP NAME	COMPANY	# OF DEVICES	CREATED BY	CREATED
□	mac machines	pradeep	1	[redacted]	2018/01/31 11:13:14 AM

Results per page: 20

Displaying 1 of 1 results

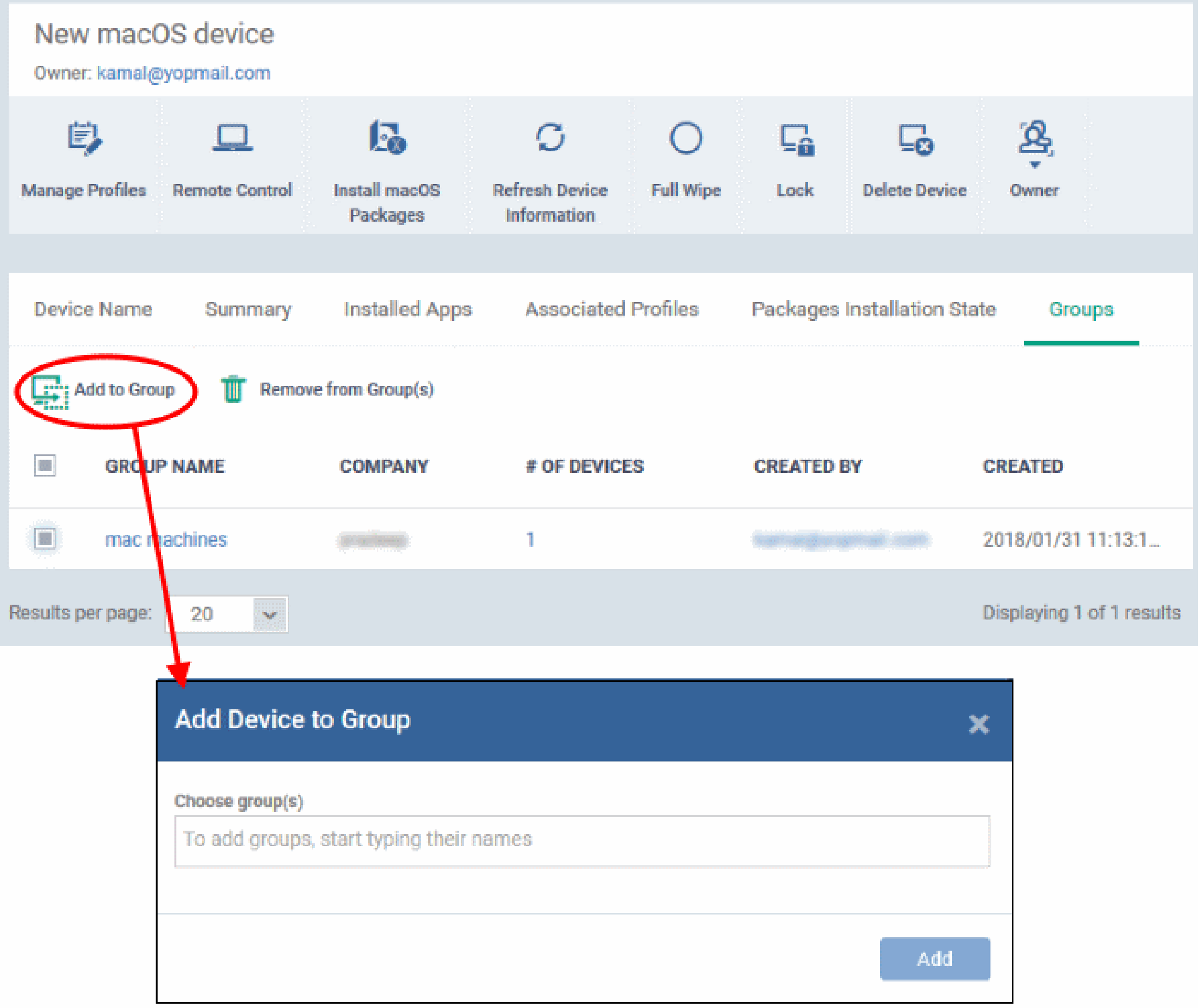
- The interface lists all groups of which the device is a member.
- All group profiles will also be applied to the endpoint.

See **Assign Configuration Profiles to a Device Group**, for more details about applying configuration profiles to device groups.

Device Groups - Table of Column Descriptions	
Column Heading	**Description**
Group Name	The label of the group. Click the group name to view group details and edit the group. See **Edit a Device Group** for more details.
Company	The company for which the group was created.
Number of Devices	The total number of devices in the group. Click the number to view group details and edit the group. See **Editing a Device Group** for more details.
Created By	The administrator that created the group. Click the name to open the user details interface. See **Viewing the Details of a User** for more details.
Created	Date and time at which the group was created

To add the device to a new group

- Click 'Add to Group'



New macOS device

Owner: kamal@yopmail.com

□	GROUP NAME	COMPANY	# OF DEVICES	CREATED BY	CREATED
□	mac machines	[redacted]	1	[redacted]	2018/01/31 11:13:1...

Results per page: 20

Displaying 1 of 1 results

Add Device to Group

Choose group(s)

To add groups, start typing their names

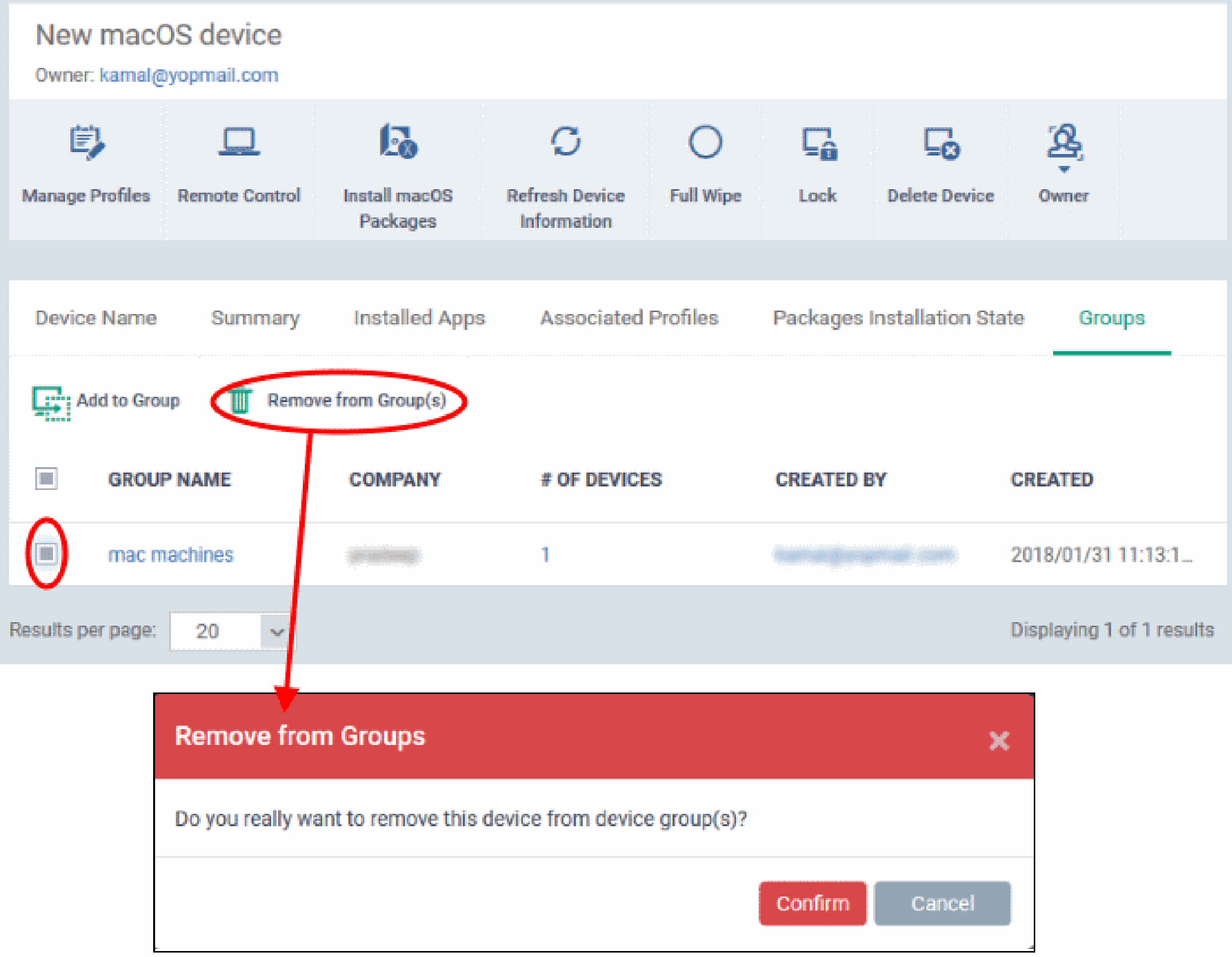
The 'Add Device to Group' dialog will appear.

- 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'.



New macOS device

Owner: kamal@yopmail.com

□	GROUP NAME	COMPANY	# OF DEVICES	CREATED BY	CREATED
□	mac machines	[redacted]	1	[redacted]	2018/01/31 11:13:1...

Results per page: 20

Displaying 1 of 1 results

Remove from Groups

Do you really want to remove this device from device group(s)?

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.

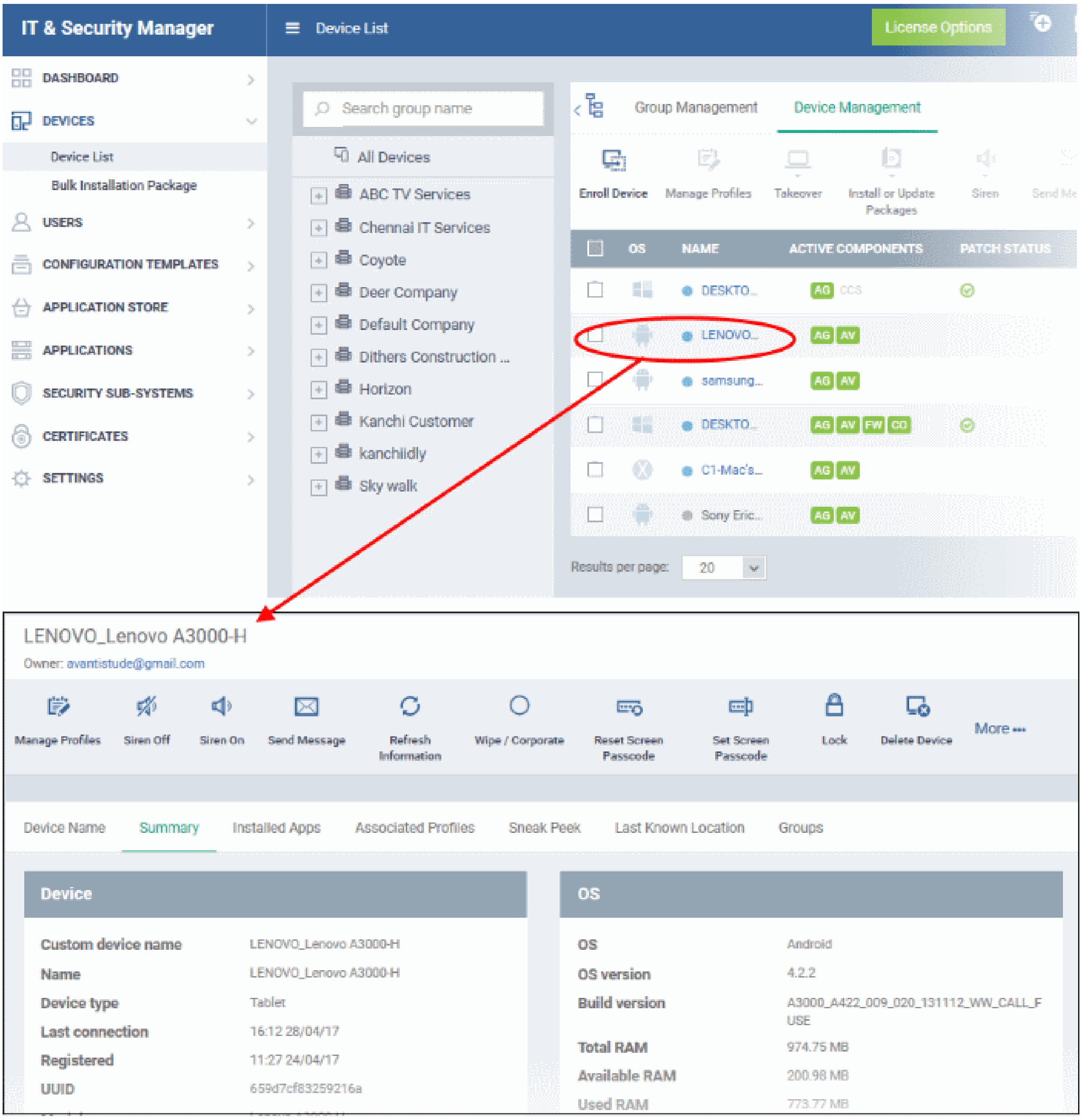
5.2.3. Manage Android/iOS Devices

- Admins can view hardware and software details of enrolled mobile devices, and manage profiles and applications on the device.
- Admins can also send messages to the device, sound an alarm on the device, remotely lock the device, view device location and view 'Sneak Peek' photographs.

To view details of and manage an individual device

- Click the 'Devices' tab on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
- The interface shows devices belonging to the company or group selected on the left.
  - Select a company and/or group to view devices that belong to that entity.

    Or
  - Select 'All Devices' to view every device added to ITSM
- Click the name of any Android or iOS device to open the 'Device Details' pane:



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS
	DESKTO...	AG CCS	✓
	LENOVO...	AG AV	
	samsung...	AG AV	
	DESKTO...	AG AV FW CO	✓
	C1-Mac's...	AG AV	
	Sony Eric...	AG AV	

Results per page: 20

LENOVO_Lenovo A3000-H

Owner: avantistude@gmail.com

Device	
Custom device name	LENOVO_Lenovo A3000-H
Name	LENOVO_Lenovo A3000-H
Device type	Tablet
Last connection	16:12 28/04/17
Registered	11:27 24/04/17
UUID	659d7cf83259216a

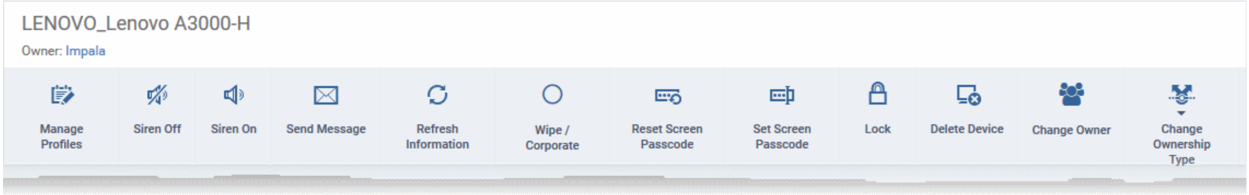
OS	
OS	Android
OS version	4.2.2
Build version	A3000_A422_009_020_131112_WW_CALL_FUSE
Total RAM	974.75 MB
Available RAM	200.98 MB
Used RAM	773.77 MB

The device details screen has seven tabs:

- **Device Name** - Device label. Click the 'Edit' button if you wish to change the device name. See **Viewing and Editing Device Name** for more details.
- **Summary** - General information about the device. Includes basic device information, operating system details, network details and security configuration. See **Viewing Summary Information** for more details.
- **Installed apps** - Details of applications installed on the device. You can remotely block/release apps or uninstall applications. See **Managing Apps Installed on a Device** for more details.
- **Associated Profiles** - Lists profiles which have been deployed to the device. Enables you to add new profiles or remove existing profiles. See **Managing Profiles associated with the Device** for more details.
- **Sneak Peek** - Pictures captured by the 'Sneak Peek' feature of ITSM. The 'Sneak Peek' feature photographs the person holding the device if they enter the wrong passcode too many times. You must enable sneak peek on a profile to use the feature. See **Viewing Sneak Peek Pictures to Locate Lost Devices** for more details.
- **Last Known Location** - The map location of the device when it last connected to ITSM. See **Viewing the Location of the Device** for more details.

- **Groups** - Shows all groups of which the Android/iOS device is a member. You can manage group membership from this tab. See **Viewing and Managing Device Group Memberships** for more details

Device tasks are shown along the top of the interface:



LENOVO_Lenovo A3000-H

Owner: Impala

- **Manage Profiles** - Add or remove device profiles. See **Assigning Configuration Profiles to Selected Devices** for more details.
- **Siren Off/Siren On** - Sound an alarm on the device to locate it. See **Generating Alarm on Devices** for more details.
- **Send Message** - Send a text message to the user. See **Sending Text Message to Devices** for more details
- **Refresh Information** - Obtain updated details from the device. See **Updating Device Information** for more details.
- **Wipe/Corporate** - Delete all data stored in the device if it is lost or stolen. See **Wiping Data from Devices** for more details
- **Reset Screen Passcode** - Reset the device's screen lock passcode. See **Setting / Reseting Screen Lock Password for Devices** for more details
- **Set Screen Passcode** - Create a new screen lock passcode for the device. See **Setting / Resetting Screen Lock Password for Devices** for more details
- **Lock/Unlock** - Remotely lock or unlock the device. See **Locking/Unlocking Devices** for more details
- **Delete Device** - Remove the device from ITSM. See **Removing a Device** for more details.
- **Change Owner** - Change the user with whom the device is associated in ITSM. See **Changing a Device's Owner** for more details.
- **Change Ownership Type** - Changes the 'Bring Your Own Device' (BYOD) status of the device. See '**Changing Ownership status of a Device**' for more details.

5.2.3.1. View and Edit Device Name

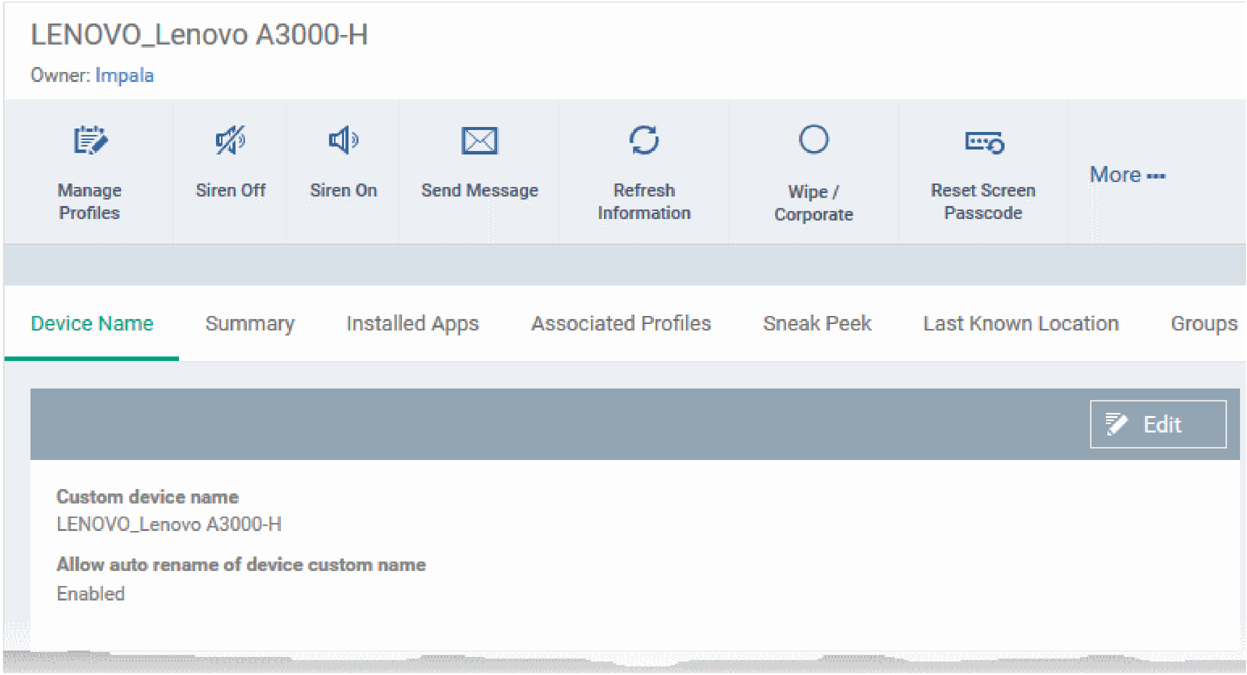
- Enrolled devices are listed by the name assigned to them by their owner.
- If no name was assigned then the actual device name or model number will be used.
- Admins can change the device name according to their preferences. If you change a device name, the name will apply in ITSM but will not change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

To change the device's name

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM

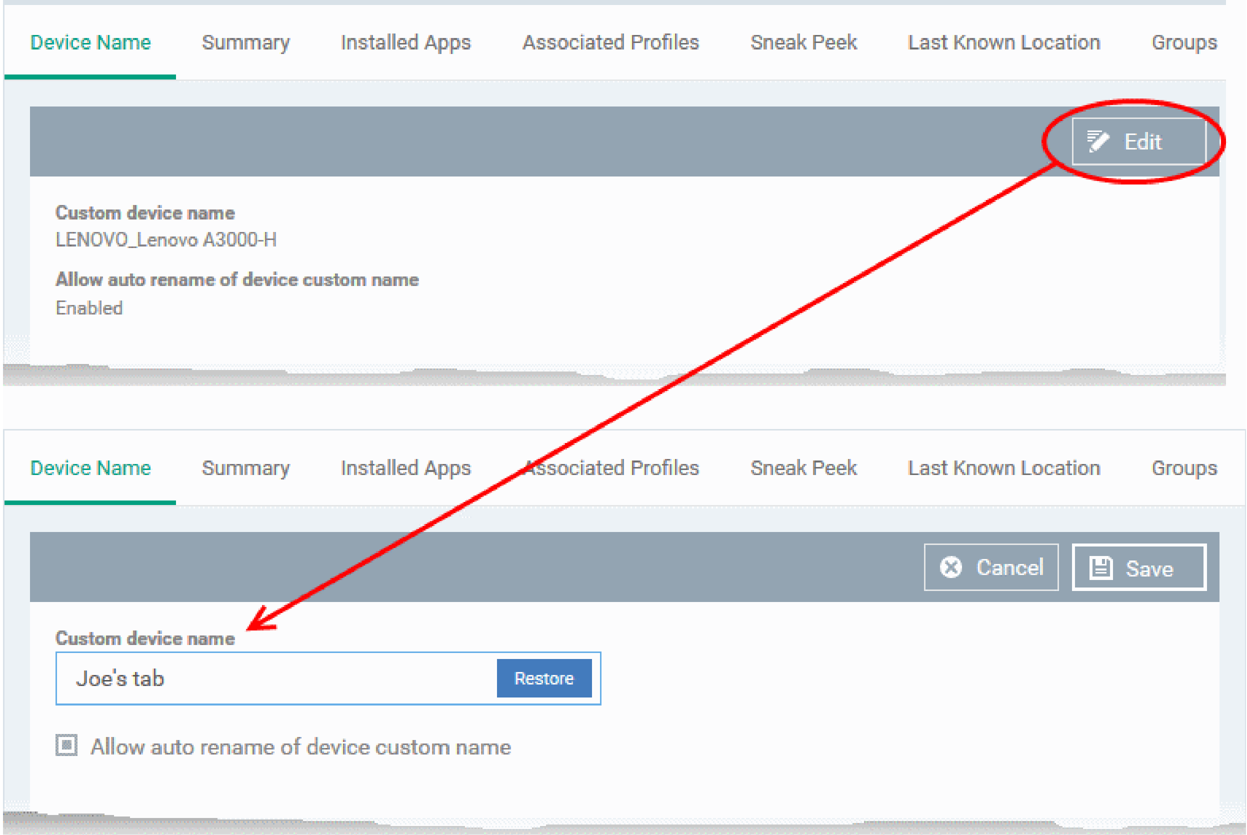
- Click on any Android or iOS device then select the 'Device Name' tab



Custom device name
LENOVO_Lenovo A3000-H

Allow auto rename of device custom name
Enabled

- 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.



Custom device name
LENOVO_Lenovo A3000-H

Allow auto rename of device custom name
Enabled

Custom device name
Joe's tab

□ Allow auto rename of device custom name

- 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'.

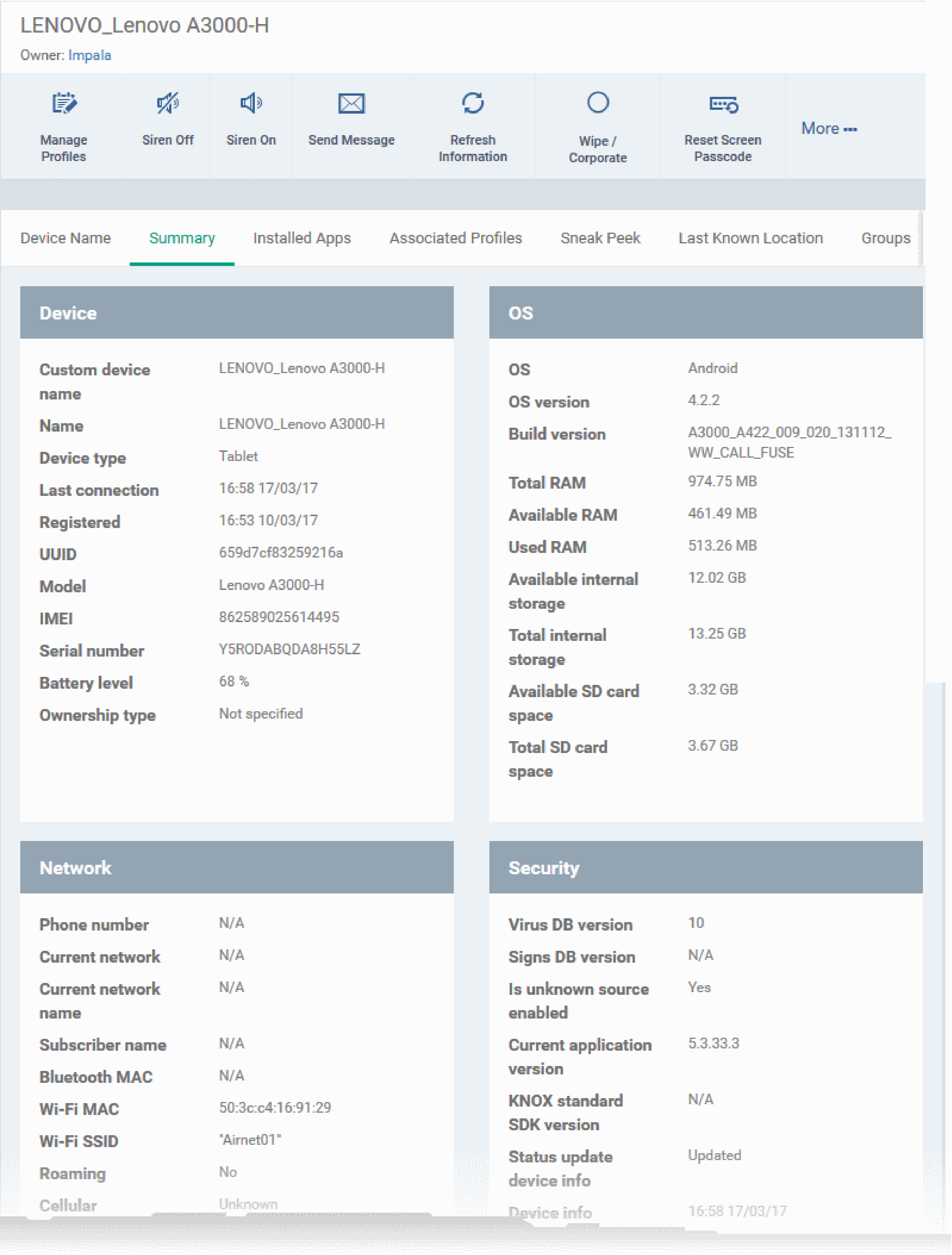
5.2.3.2. View Summary Information

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

To view the device information summary

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Android or iOS device then open the 'Summary' tab (if it is not already open).



LENOVO_Lenovo A3000-H

Owner: Impala

Device

Custom device name	LENOVO_Lenovo A3000-H
Name	LENOVO_Lenovo A3000-H
Device type	Tablet
Last connection	16:58 17/03/17
Registered	16:53 10/03/17
UUID	659d7cf83259216a
Model	Lenovo A3000-H
IMEI	862589025614495
Serial number	Y5RODABQDA8H55LZ
Battery level	68 %
Ownership type	Not specified

OS

OS	Android
OS version	4.2.2
Build version	A3000_A422_009_020_131112_WW_CALL_FUSE
Total RAM	974.75 MB
Available RAM	461.49 MB
Used RAM	513.26 MB
Available internal storage	12.02 GB
Total internal storage	13.25 GB
Available SD card space	3.32 GB
Total SD card space	3.67 GB

Network

Phone number	N/A
Current network	N/A
Current network name	N/A
Subscriber name	N/A
Bluetooth MAC	N/A
Wi-Fi MAC	50:3c:c4:16:91:29
Wi-Fi SSID	"Airnet01"
Roaming	No
Cellular	Unknown

Security

Virus DB version	10
Signs DB version	N/A
Is unknown source enabled	Yes
Current application version	5.3.33.3
KNOX standard SDK version	N/A
Status update device info	Updated
Device info	16:58 17/03/17

- **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 Ownership 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.

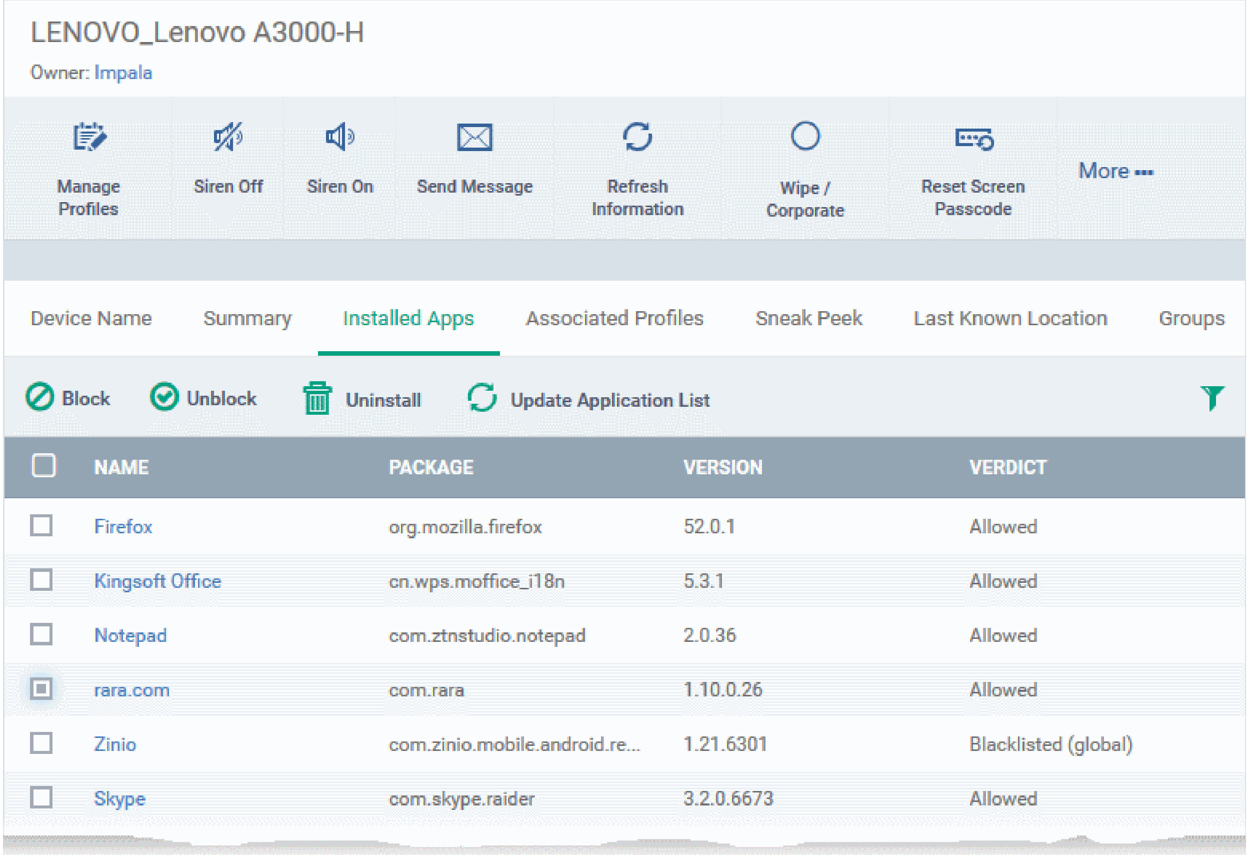
5.2.3.3. Manage Installed Applications

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Android or iOS device then open the 'Installed Apps' tab



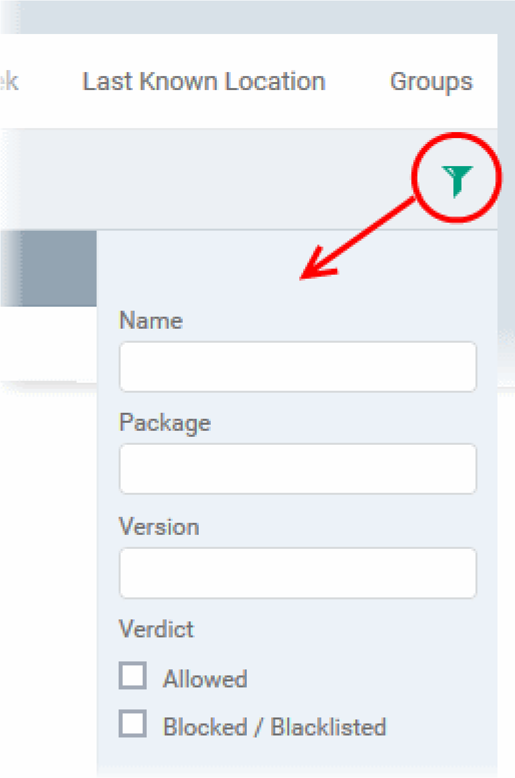
	NAME	PACKAGE	VERSION	VERDICT
□	Firefox	org.mozilla.firefox	52.0.1	Allowed
□	Kingsoft Office	cn.wps.moffice_i18n	5.3.1	Allowed
□	Notepad	com.ztnstudio.notepad	2.0.36	Allowed
▣	rara.com	com.rara	1.10.0.26	Allowed
□	Zinio	com.zinio.mobile.android.re...	1.21.6301	Blacklisted (global)
□	Skype	com.skype.raider	3.2.0.6673	Allowed

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'

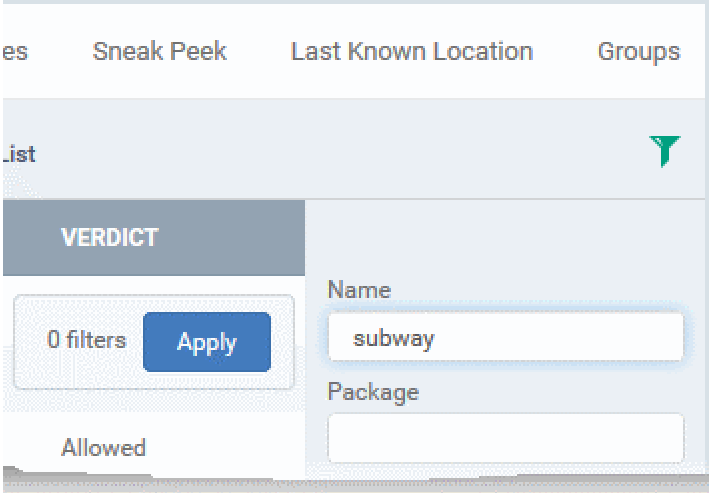
	can be found at **https://play.google.com/store/apps/details?id=cn.wps.moffice_i18n**
Version	Indicates the version of the application.
Verdict	Indicates whether the application is allowed, blocked or blacklisted.

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'



Name: subway

- 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

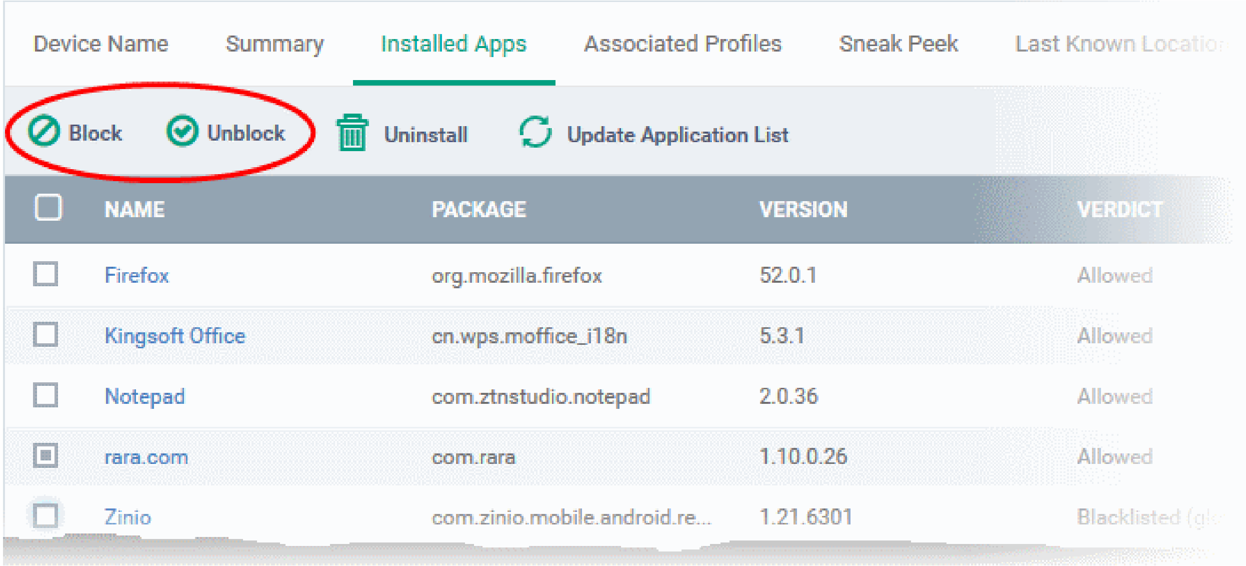
- Choose the app(s) that you wish to block and simply click the 'Block' button.

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'.

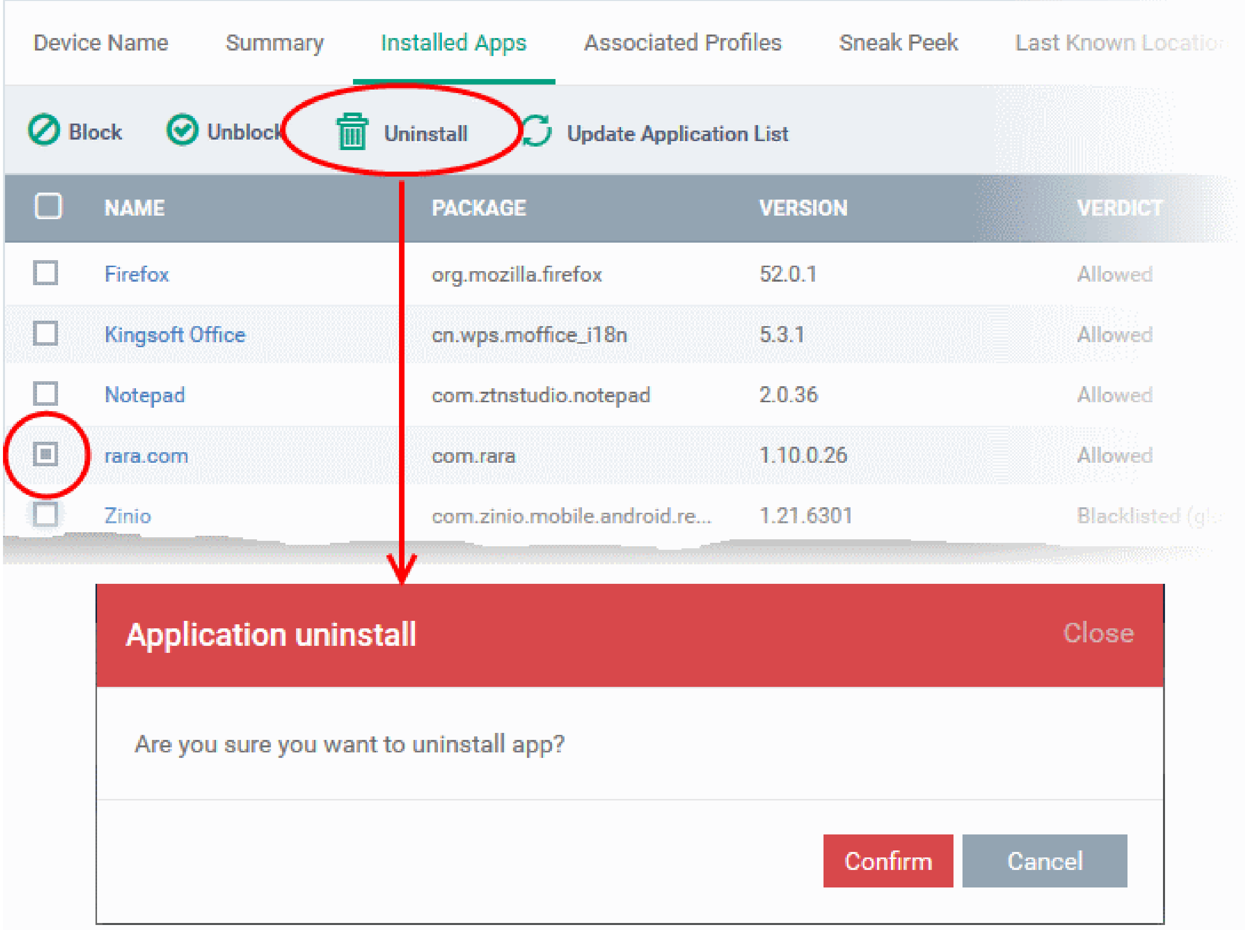
The verdict of the app(s) will change to 'Allowed' and they will be allowed to run on the device.



□	NAME	PACKAGE	VERSION	VERDICT
□	Firefox	org.mozilla.firefox	52.0.1	Allowed
□	Kingsoft Office	cn.wps.moffice_i18n	5.3.1	Allowed
□	Notepad	com.ztnstudio.notepad	2.0.36	Allowed
☑	rara.com	com.rara	1.10.0.26	Allowed
□	Zinio	com.zinio.mobile.android.re...	1.21.6301	Blacklisted (gl

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'.



☐	NAME	PACKAGE	VERSION	VERDICT
☐	Firefox	org.mozilla.firefox	52.0.1	Allowed
☐	Kingsoft Office	cn.wps.moffice_i18n	5.3.1	Allowed
☐	Notepad	com.ztnstudio.notepad	2.0.36	Allowed
☑	rara.com	com.rara	1.10.0.26	Allowed
☐	Zinio	com.zinio.mobile.android.re...	1.21.6301	Blacklisted (gl

Application uninstall

Are you sure you want to uninstall app?

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'.

5.2.3.4. View and Manage 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

See '**Profiles for Android Devices**', '**Profiles for iOS Devices**', '**Viewing and Managing Profiles**' and '**Managing Default Profiles**', for more details on profiles and default profiles.

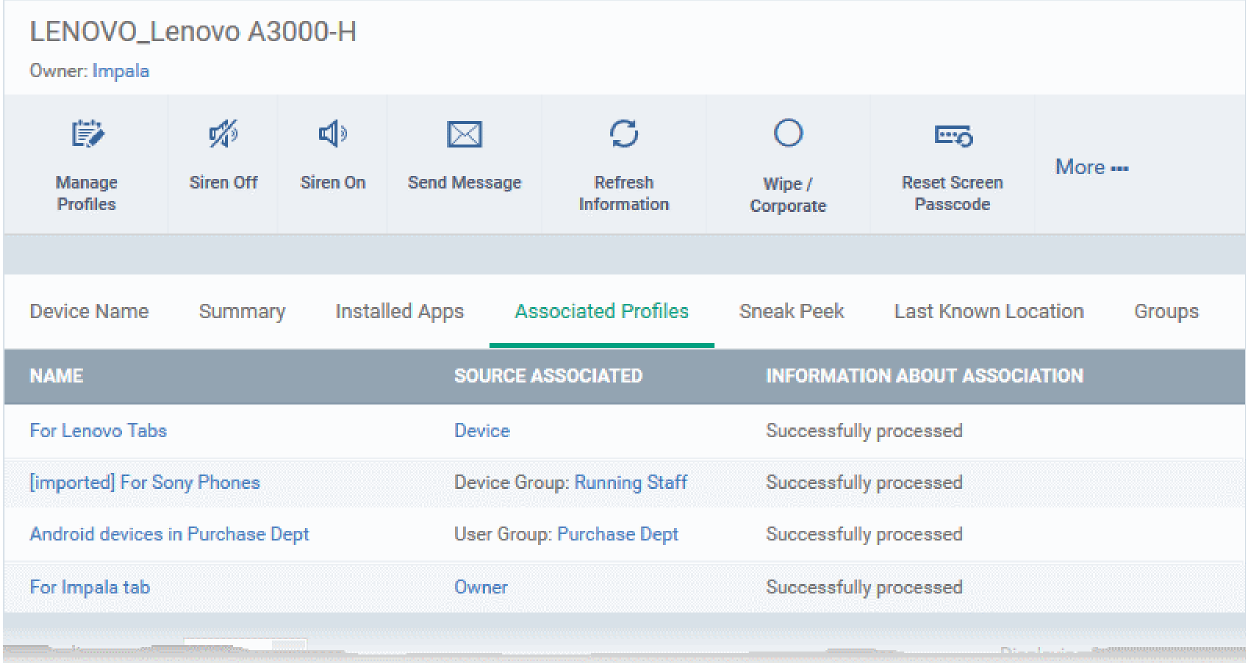
To view and manage associated profiles

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

    Or

  - Select 'All Devices' to view every device enrolled to ITSM

- Click on any Android or iOS device then open the 'Associated Profiles' tab



LENOVO_Lenovo A3000-H

Owner: Impala

NAME	SOURCE ASSOCIATED	INFORMATION ABOUT ASSOCIATION
For Lenovo Tabs	Device	Successfully processed
[imported] For Sony Phones	Device Group: Running Staff	Successfully processed
Android devices in Purchase Dept	User Group: Purchase Dept	Successfully processed
For Impala tab	Owner	Successfully processed

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 channel through which the profile was applied to the device. Configuration profiles can be applied to a device in different ways: • Profiles can be directly applied to the device. See **Assigning Configuration Profiles to Selected Devices** for more details • Profiles applied to a user are deployed to all devices belonging to them. See **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. See **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. See **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.

5.2.3.5. View Sneak Peek Pictures to Locate Lost Devices

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

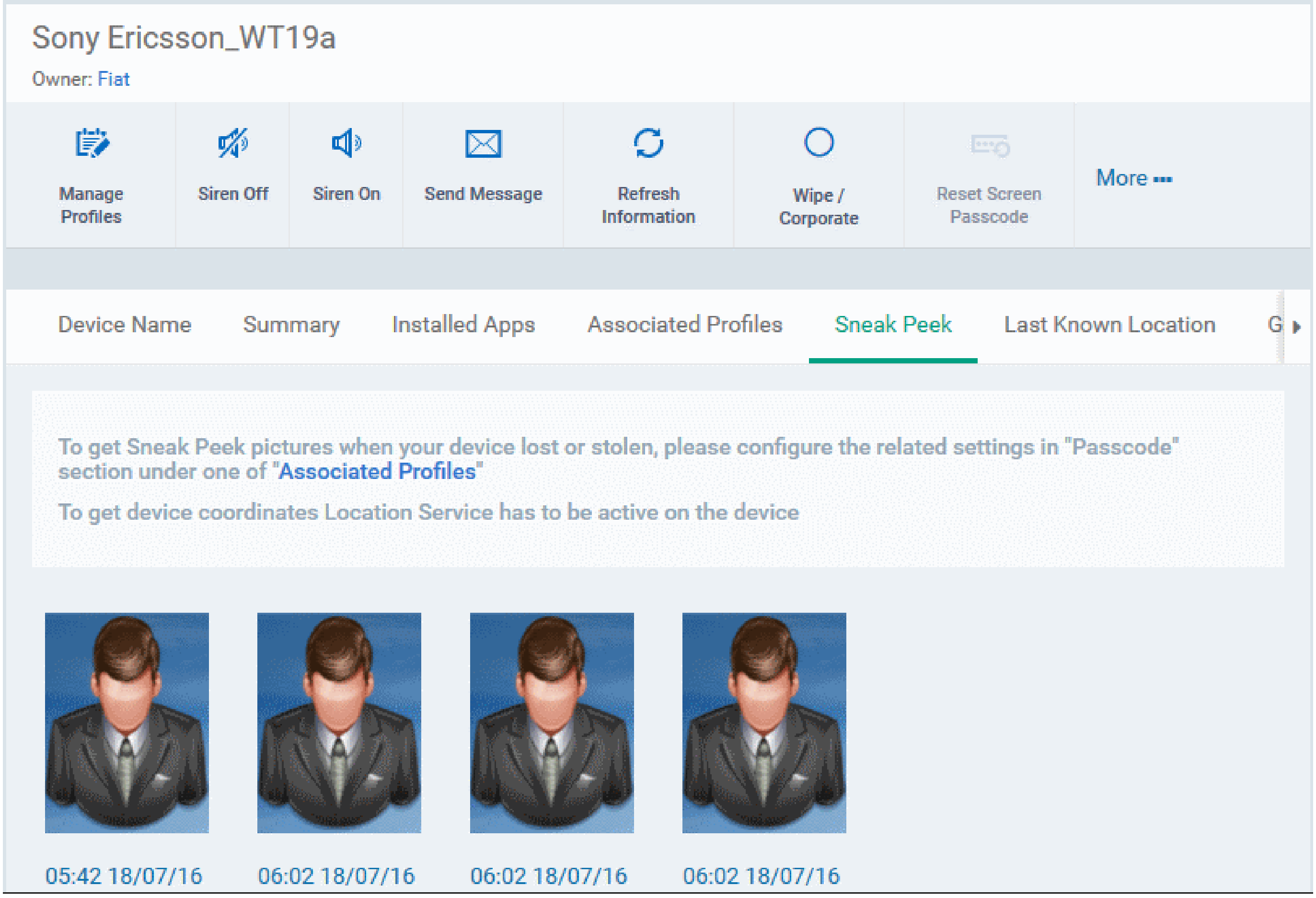
The 'Sneak Peek' feature can help administrators to recover mislaid Android phones and tablets. If somebody enters the wrong password on a lost or stolen device, the device will automatically take a photo of the device holder and save it to the server with their picture and location. The Sneak Peek feature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

To view Sneak Peak pictures

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any 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:


Sony Ericsson_WT19a

Owner: Fiat

To get Sneak Peek pictures when your device lost or stolen, please configure the related settings in "Passcode" section under one of "Associated Profiles"

To get device coordinates Location Service has to be active on the device

05:42 18/07/16

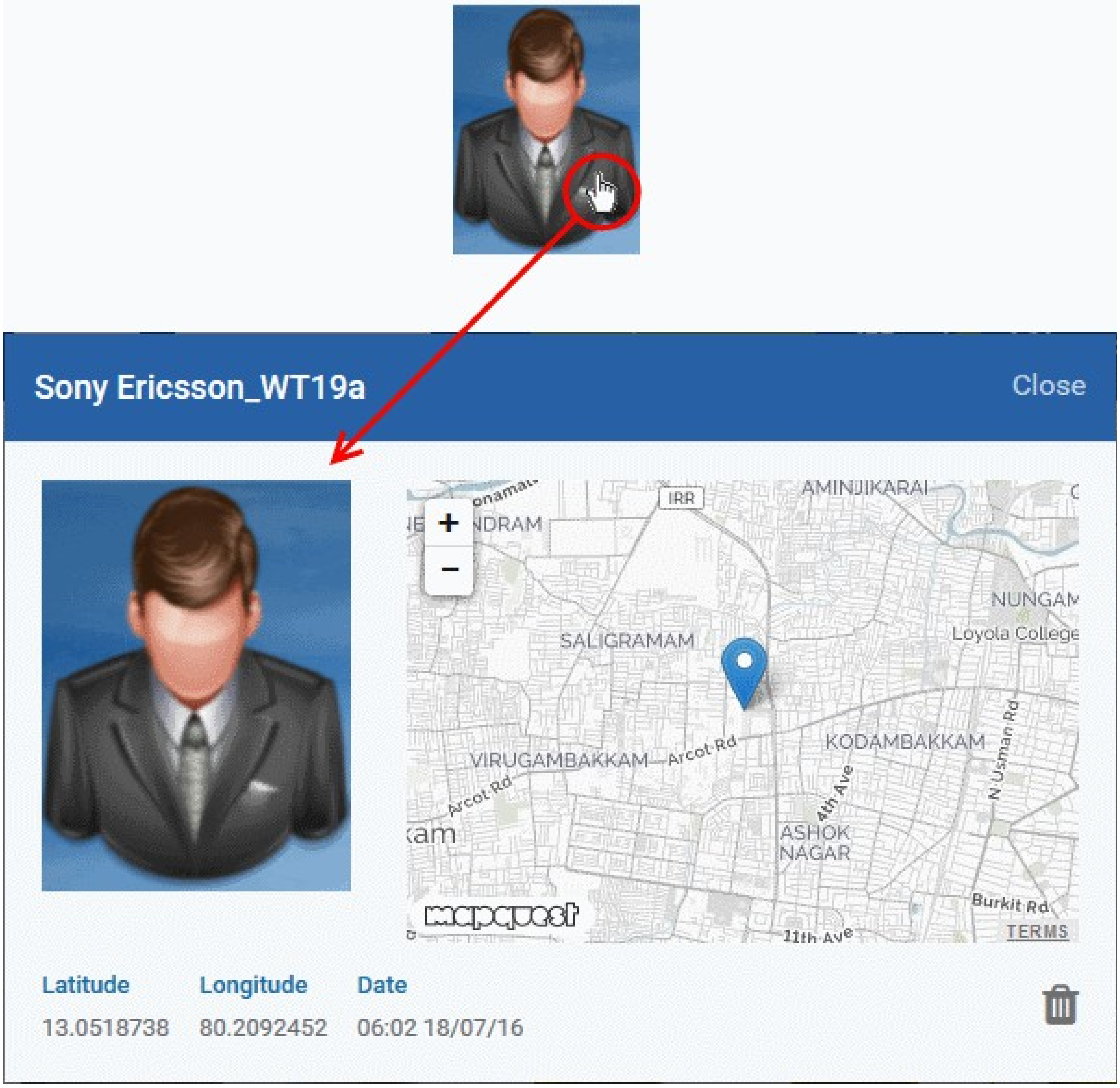
06:02 18/07/16

06:02 18/07/16

06:02 18/07/16

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.



Sony Ericsson_WT19a

Close

Latitude	Longitude	Date
13.0518738	80.2092452	06:02 18/07/16

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

5.2.3.6. View 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 the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

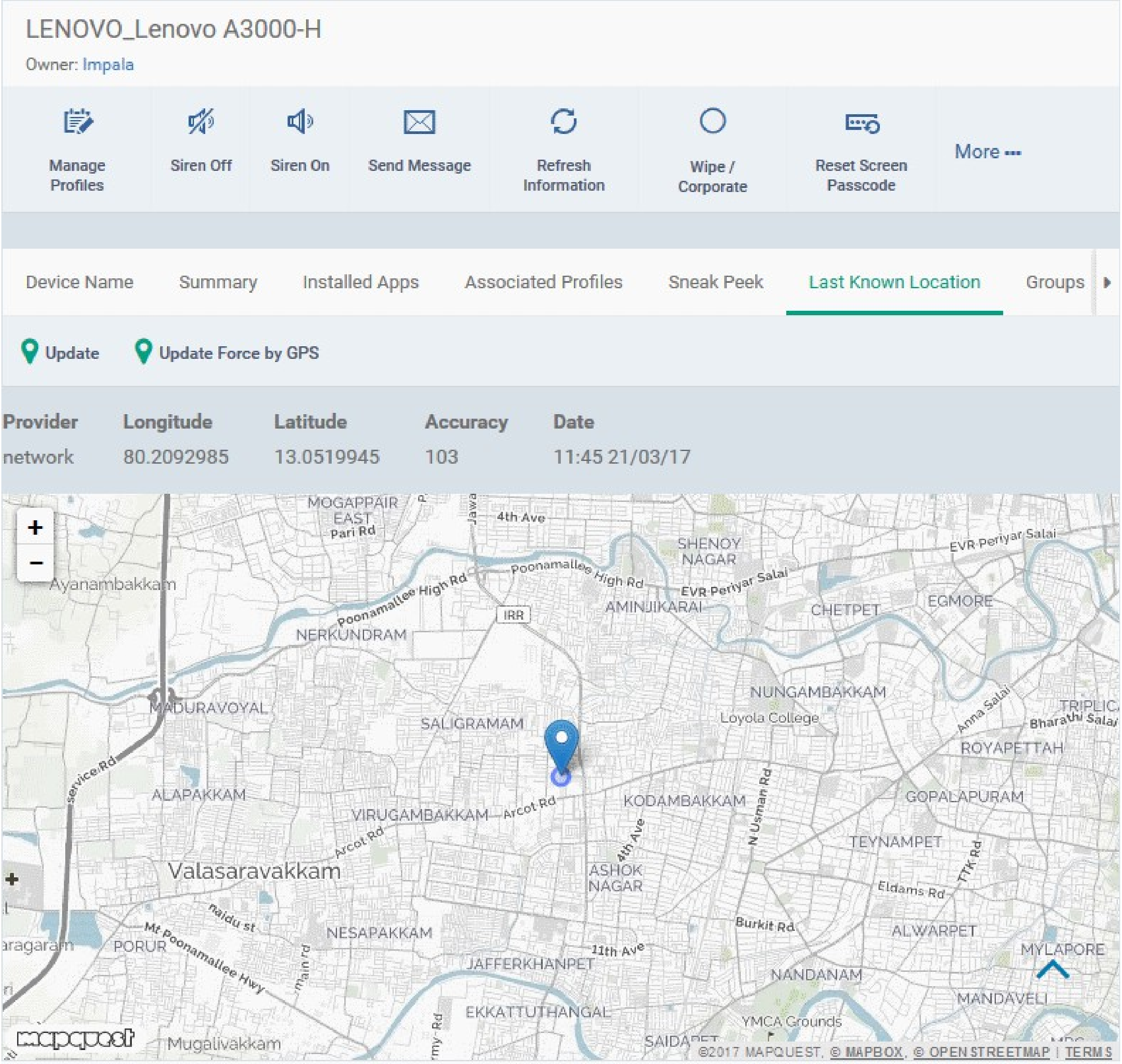
- Select a company or a group to view the list of devices in that group

  Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click on any Android or iOS device then select the 'Last Known Location' tab

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



LENOVO_Lenovo A3000-H

Owner: Impala

Provider	Longitude	Latitude	Accuracy	Date
network	80.2092985	13.0519945	103	11:45 21/03/17

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

5.2.3.7. View and Manage Device Group Memberships

The 'Groups' tab in 'Device Details' shows all groups of which the device is a member. Admins can remove the device from a group or add it to a new group.

To view and manage device group membership

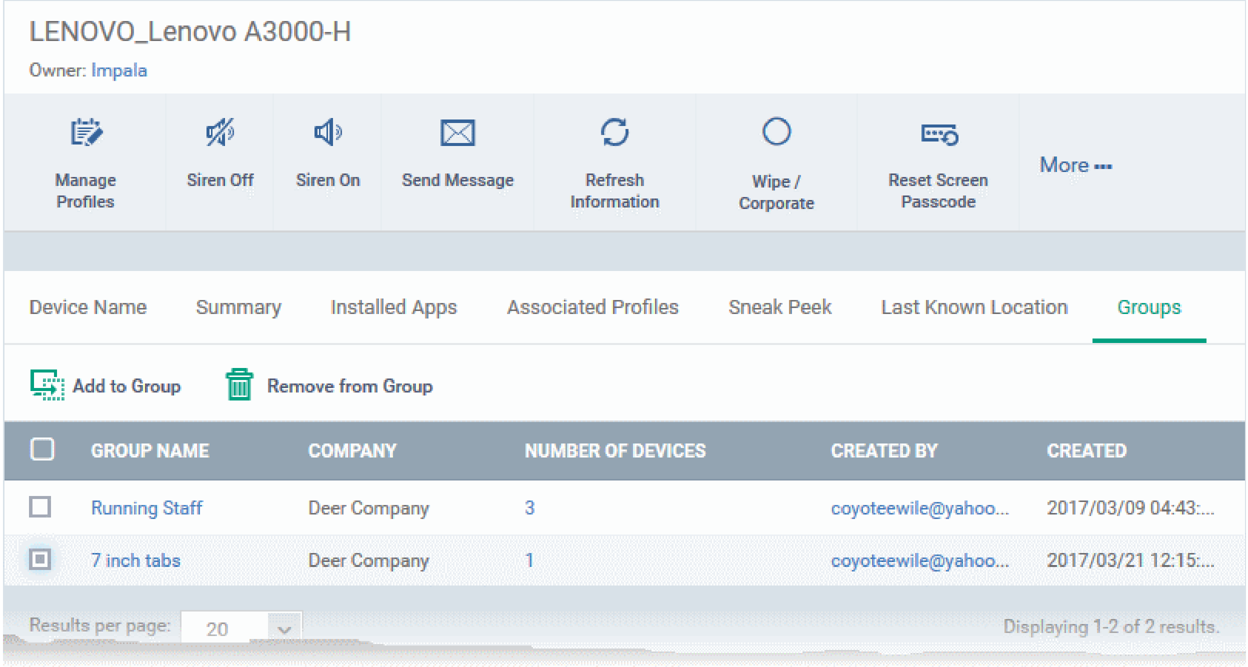
- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

- Select a company or a group to view the list of devices in that group

  Or

- Select 'All Devices' to view every device enrolled to ITSM

- Click the name of any Android or iOS device then select the 'Groups' tab


LENOVO_Lenovo A3000-H

Owner: Impala

□	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY	CREATED
□	Running Staff	Deer Company	3	coyoteewile@yahoo...	2017/03/09 04:43:...
▣	7 inch tabs	Deer Company	1	coyoteewile@yahoo...	2017/03/21 12:15:...

Results per page: 20

Displaying 1-2 of 2 results.

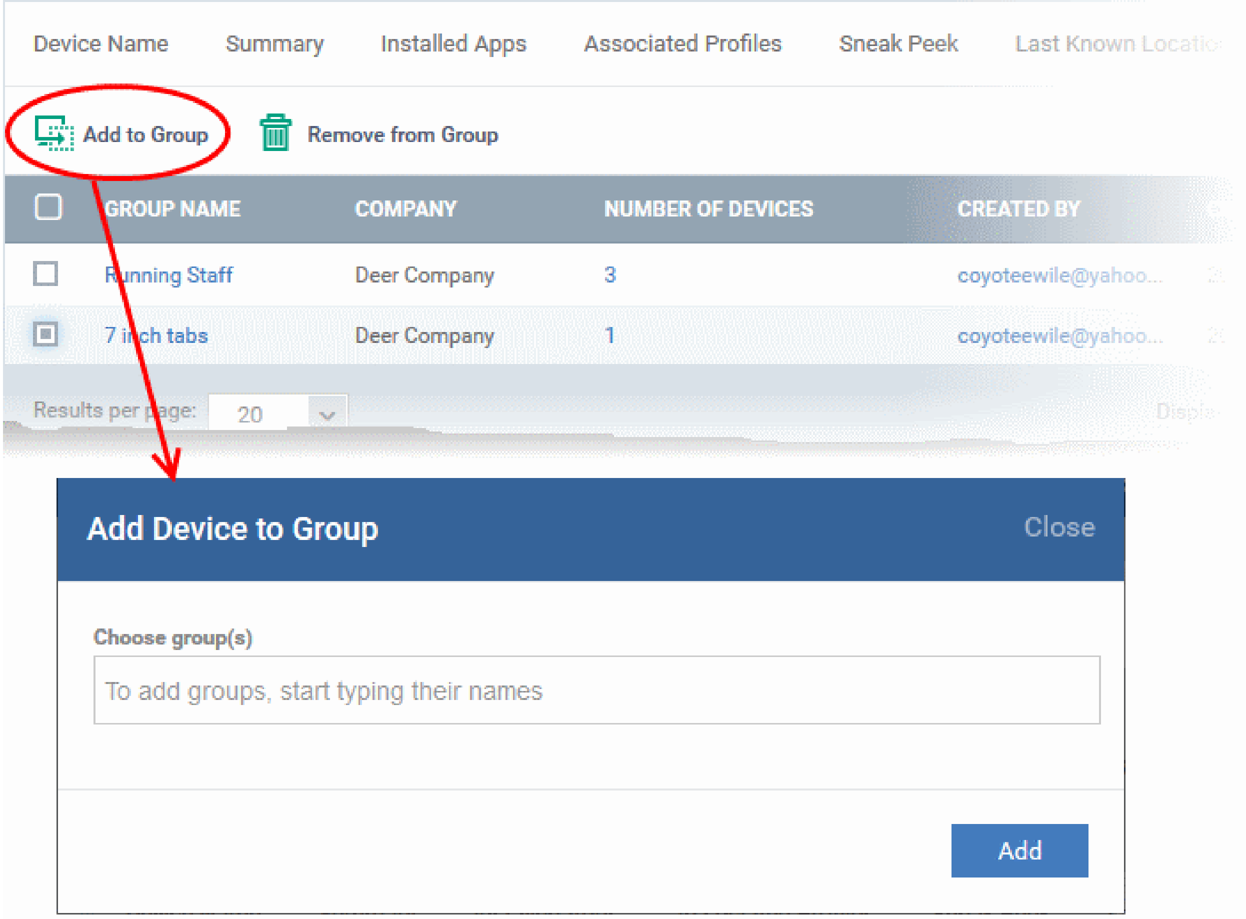
- The interface lists all groups of which the device is a member.
- Any device group profiles will also be applied to the endpoint.

For more details about applying configuration profiles to device groups, see **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 settings. See **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. See **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. See **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'



□	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY
□	Running Staff	Deer Company	3	coyoteewile@yahoo...
□	7 inch tabs	Deer Company	1	coyoteewile@yahoo...

Results per page: 20

Add Device to Group

Choose group(s)

To add groups, start typing their names

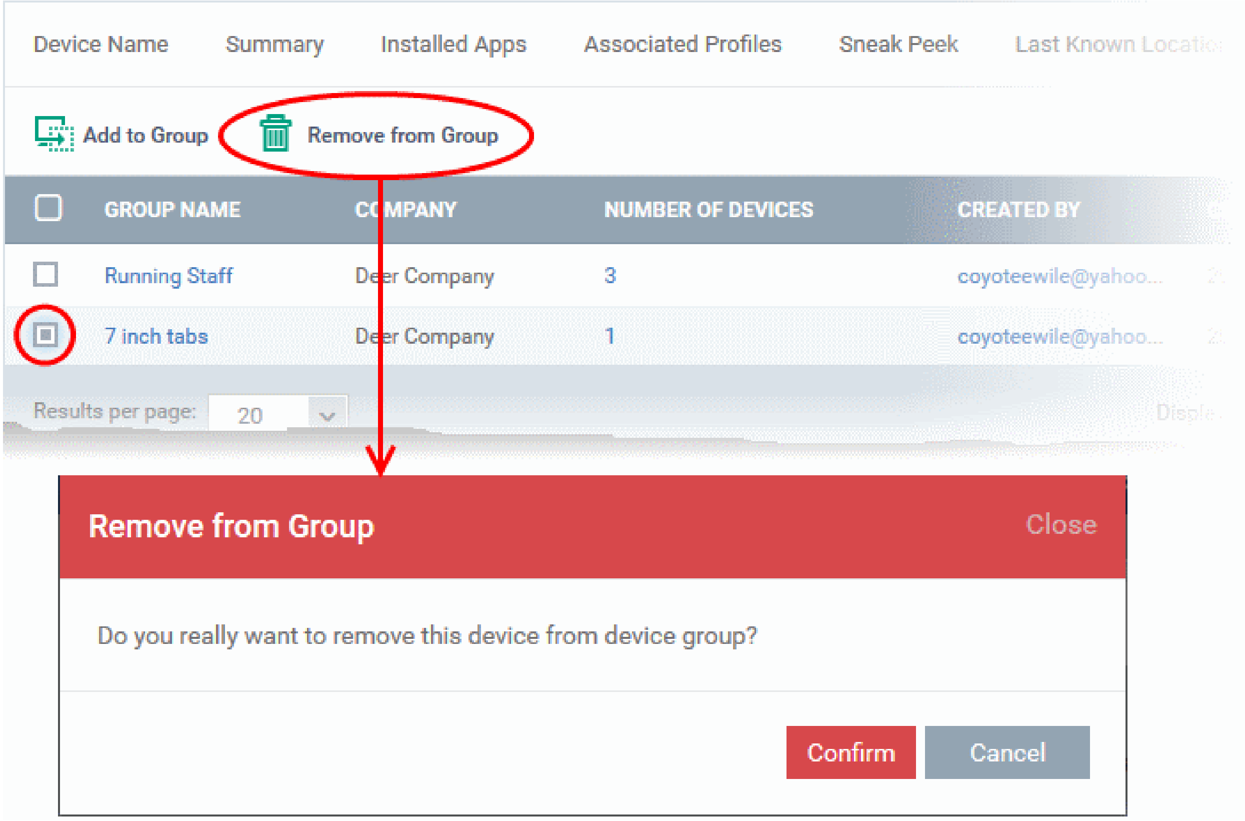
The 'Add Device to Group' dialog will appear.

- 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'.



□	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY
□	Running Staff	Deer Company	3	coyoteewile@yahoo...
☒	7 inch tabs	Deer Company	1	coyoteewile@yahoo...

Remove from Group

Do you really want to remove this device from device 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.

5.2.4. View User Information

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

To view the user information of a device

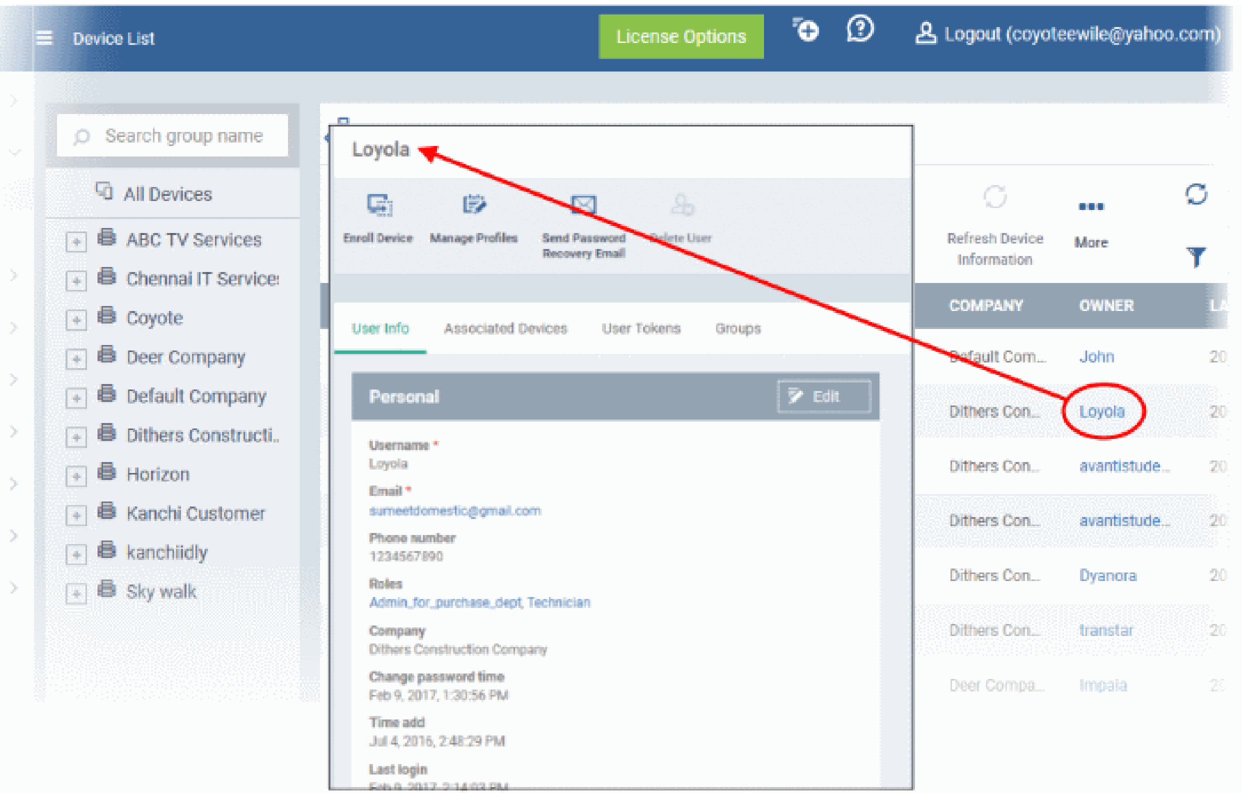
- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select a company or a group to view the list of devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM

The users of each device are listed in the 'Owner' column.

- Click the 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.



Username *
Loyola

Email *
sumeetdomestic@gmail.com

Phone number
1234567890

Roles
Admin_for_purchase_dept, Technician

Company
Dithers Construction Company

Change password time
Feb 9, 2017, 1:30:56 PM

Time add
Jul 4, 2016, 2:48:29 PM

Last login

5.2.5. Remove 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.

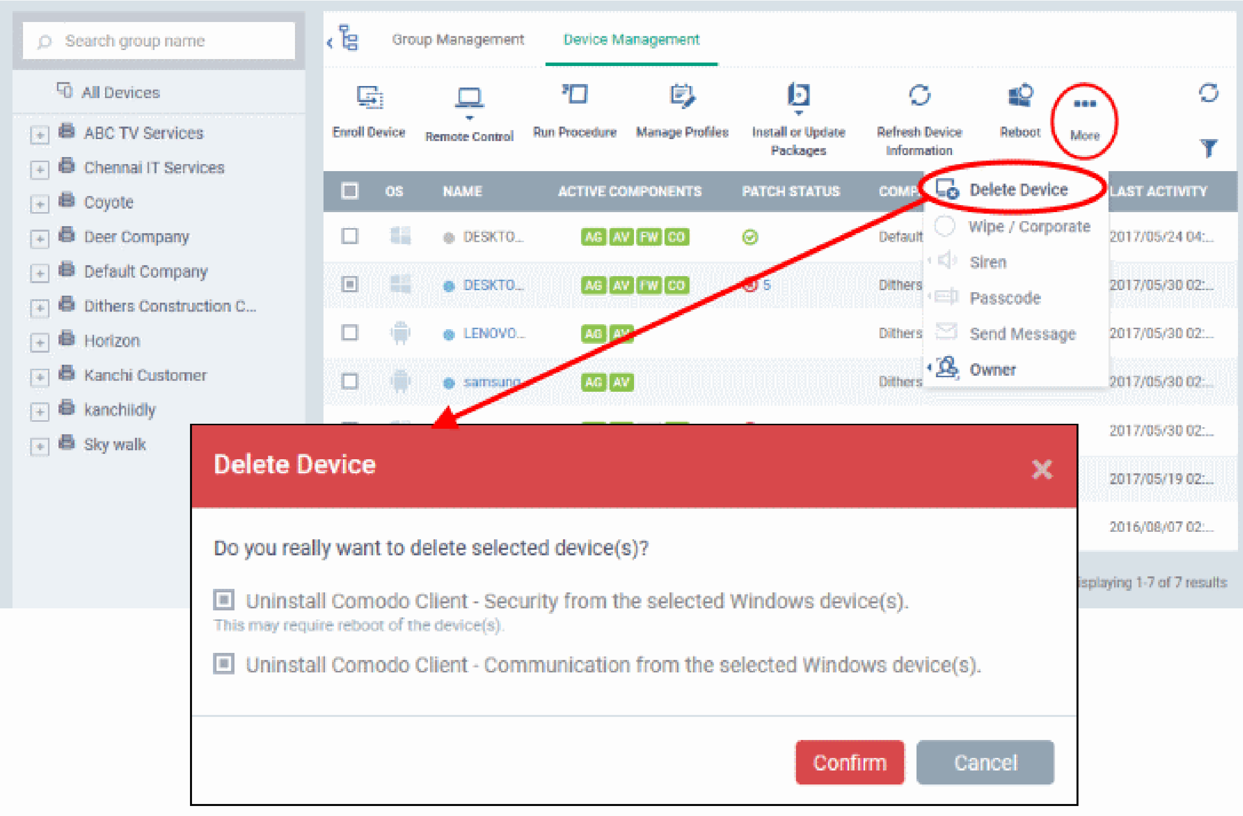
Android, iOS and Mac OS devices - End users can manually uninstall the communication client and security software or the iOS profile from their devices. **Instructions for uninstalling the agent/software** are available at the end of this section.

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- 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.



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMP...	LAST ACTIVITY
	DESKTO...	AG AV FW CO	✓	Default	2017/05/24 04:...
	DESKTO...	AG AV FW CO	5	Dithers	2017/05/30 02:...
	LENOVO...	AG AV		Dithers	2017/05/30 02:...
	samsung...	AG AV		Dithers	2017/05/30 02:...
					2017/05/30 02:...
					2017/05/19 02:...
					2016/08/07 02:...

isplaying 1-7 of 7 results

Delete Device ×

Do you really want to delete selected device(s)?

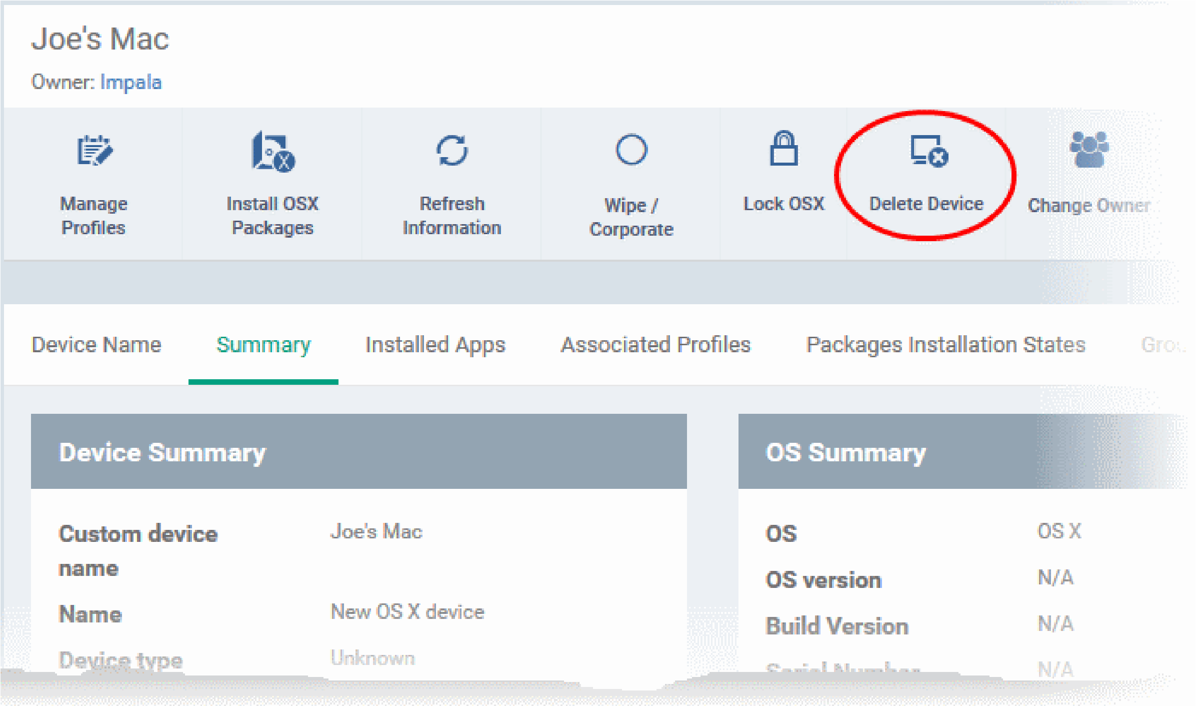
☐ Uninstall Comodo Client - Security from the selected Windows device(s).
This may require reboot of the device(s).

☐ Uninstall Comodo Client - Communication from the selected Windows device(s).

Confirm Cancel

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.



Joe's Mac

Owner: Impala

Device Summary

Custom device name	Joe's Mac
Name	New OS X device
Device type	Unknown

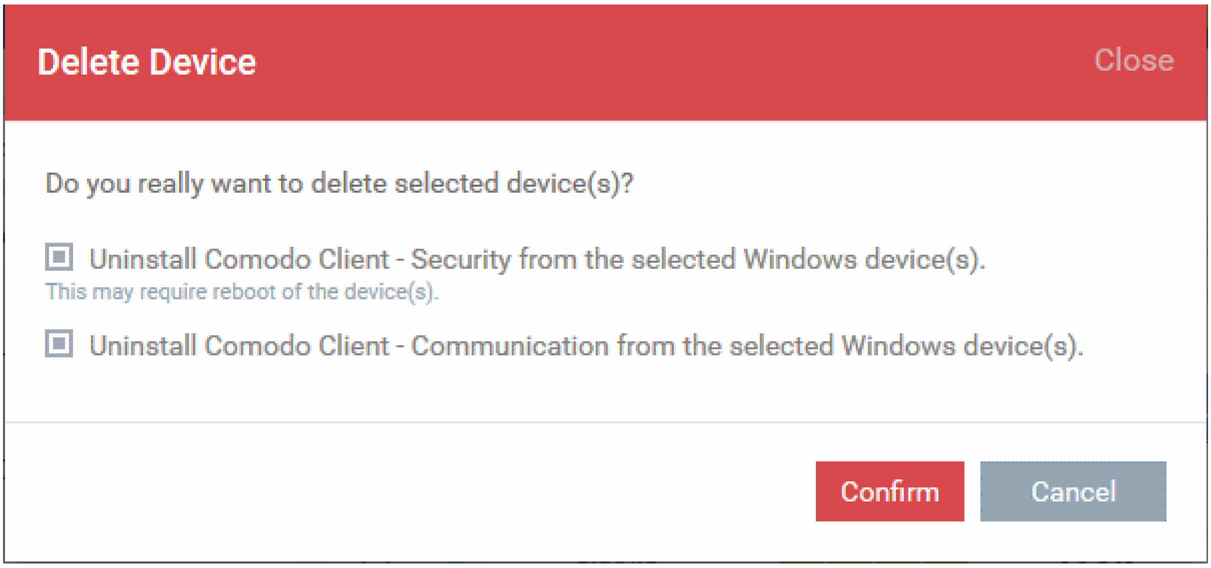
OS Summary

OS	OS X
OS version	N/A
Build Version	N/A
Serial Number	N/A

- 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.



Delete Device

Do you really want to delete selected device(s)?

▣ Uninstall Comodo Client - Security from the selected Windows device(s).
This may require reboot of the device(s).

▣ Uninstall Comodo Client - Communication from the selected Windows device(s).

- 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 device
- 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 Mac OS devices

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

The ITSM profile will be removed from the device.

5.2.6. Remote Management of Windows and Mac OS Devices

- Click 'Settings' > 'Portal Setup' > 'Extensions Management' to enable Comodo Remote Control for your account.

The 'Remote Control' feature allows you to remotely access Windows and Mac OS devices to solve issues, install third party software and run system maintenance.

You can takeover Windows and Mac devices using the following tools:

- **Comodo Remote Control** (Windows and Mac OS devices - recommended for most users)
- **Comodo Remote Monitoring and Management (RMM)** (Windows devices only - legacy tool for Comodo RMM users)

Comodo Remote Control

- You first need to install Comodo Remote Control (CRC) on your admin computer:
  - Click 'Devices' > 'Bulk Installation Package'
  - Select the 'Comodo Remote Control' tab
  - Choose the operating system of your admin machine
  - Click 'Download'
- Once installed, you can takeover devices:
  - By using the desktop application, or
  - From the ITSM console: 'Devices' > 'Device List' > 'Device Management' > select a device > click 'Remote Control').
- You can select the location of the C1 server nearest to your location for the CRC for faster connection
- For an additional security, you can assign custom ports for use by remote connection protocols on the device. These can be configured in the 'Remote Control' component of the policy active on the device. For more details, see **Remote Control Settings** for Windows devices and **Remote control Settings for Mac OS Profile**.
- The viewer supports clip-board sharing between your computer and the managed device.
- You can also use key combinations such as 'Ctrl+Alt+Del', 'Alt+F4', Ctrl+C on the remote machine (Windows devices only).
- If the managed endpoint has a multi-monitor setup, the viewer allows you to view individual monitors or all monitors at once.

See the following sections for more help:

- **Download and install the Comodo Remote Control Viewer**
- **Use the Desktop Application for Remote Control**

Download and install 'Comodo Remote Control' application

- Click 'Devices' > 'Bulk Installation Package' > Select the 'Comodo Remote Control' tab > Choose the operating system of your admin machine > Click 'Download'.

Tip: You can also download the 'Comodo Remote Control' application from the Comodo One portal.

- Click 'Tools' on the menu bar
- Locate the 'Comodo Remote Control' tile.
- Click 'Download'
- Choose the operating system of your admin machine and click 'Download'.

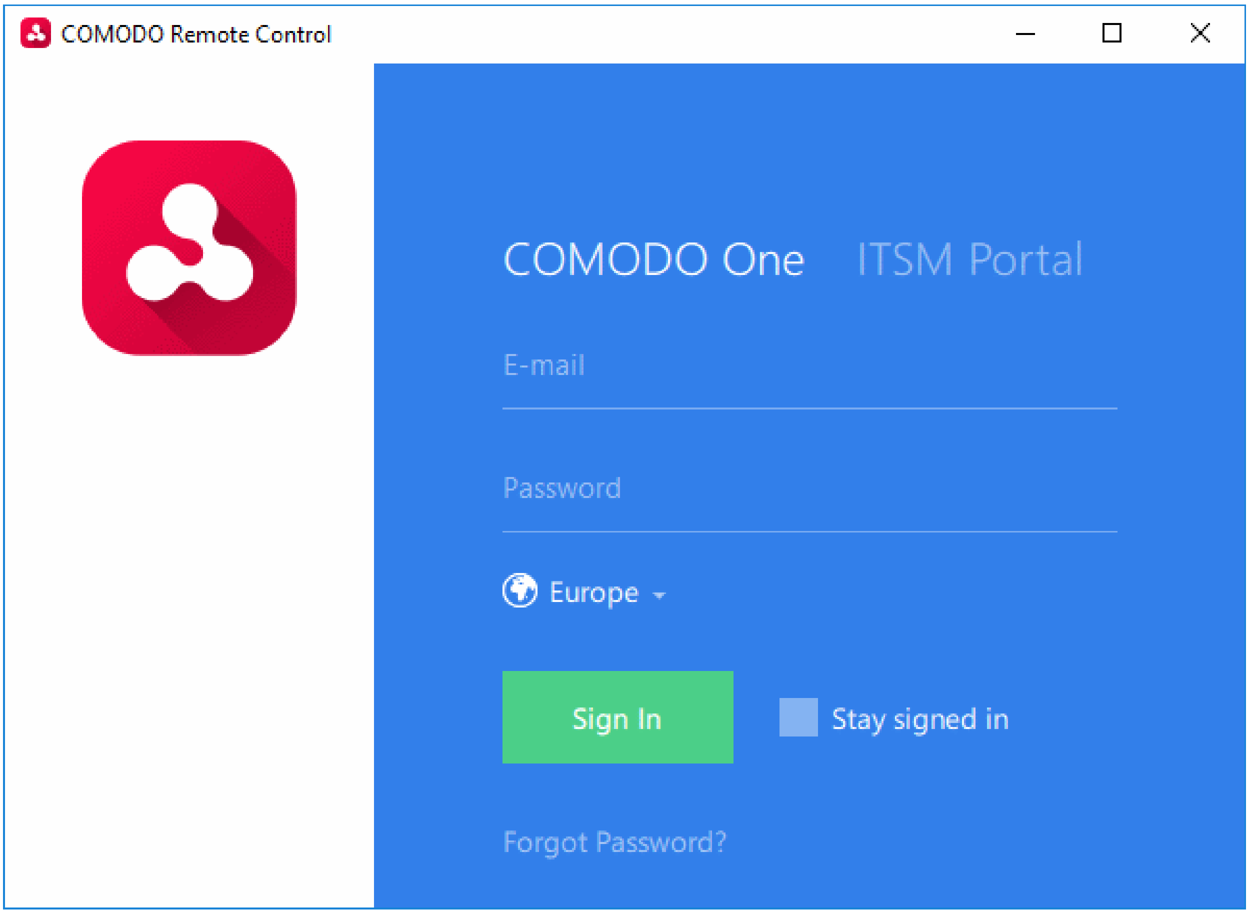
- See **Download Remote Control Tool** if you need any more help with this.

Use the Desktop Application for Remote Control

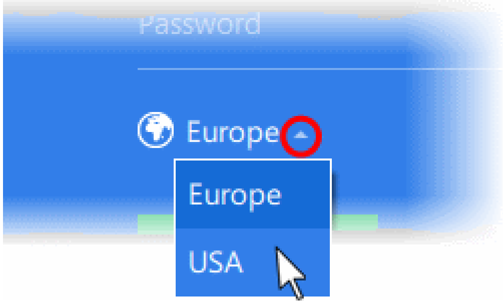
- Once installed, the Comodo Remote Control viewer can be launched from your desktop
- You can also take control direct from the ITSM interface:
  - Click 'Devices' > 'Device List' > 'Device Management' > select a Windows / Mac OS device > Click the 'Remote Control' button.

To access the remote control viewer

- Double click the desktop shortcut or the system tray icon to open the login screen:

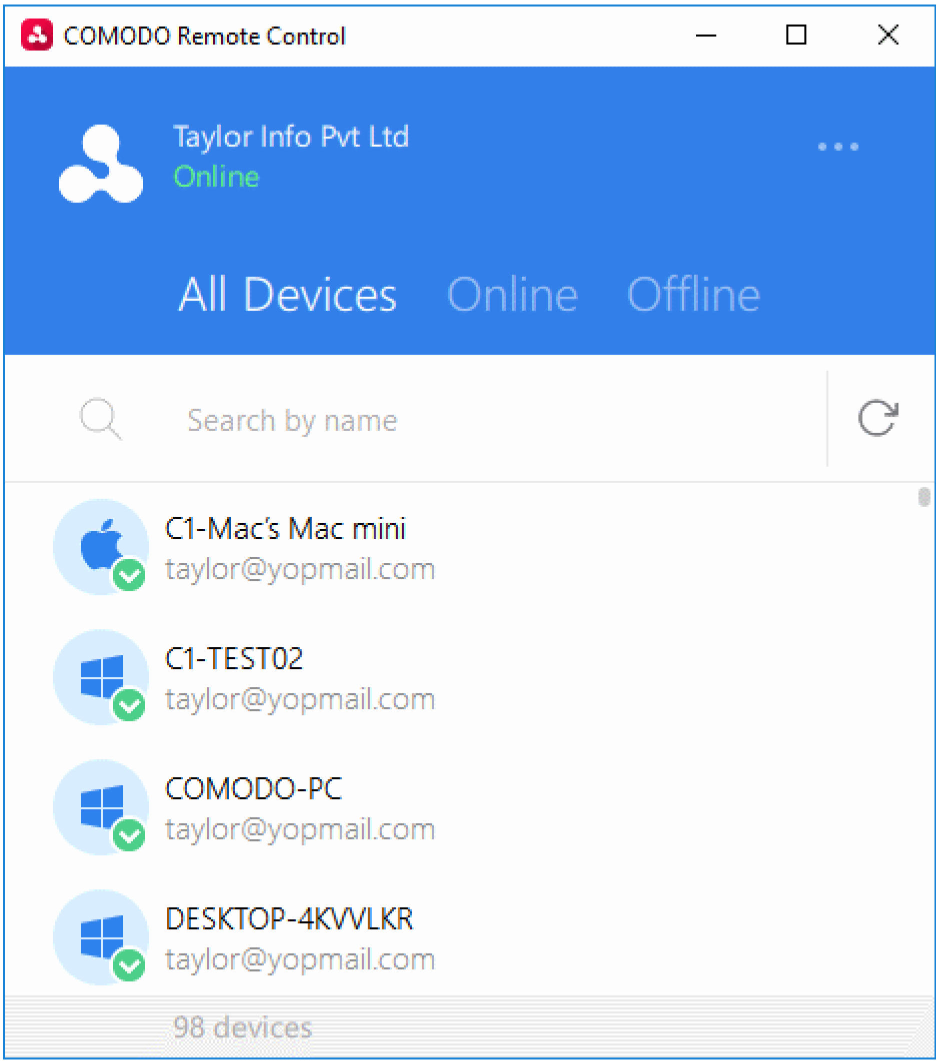


- **C1 users** - Click the 'Comodo One' tab then login with your C1 username and password
- **ITSM users** - Click the 'ITSM Portal' tab then enter your ITSM URL + your login credentials. Your ITSM URL will use the format https://<your company name>.cmdm.comodo.com, where <your company name> is your ITSM company name.
- The region selector allows you to choose the C1 hosted service closest to your location. Select the location nearest to you for the best performance / fastest connection.



- Select 'Stay Signed in' if you want the CRC application to store your login credentials. The application will not ask for your credentials to login in future.
- Click 'Sign In'

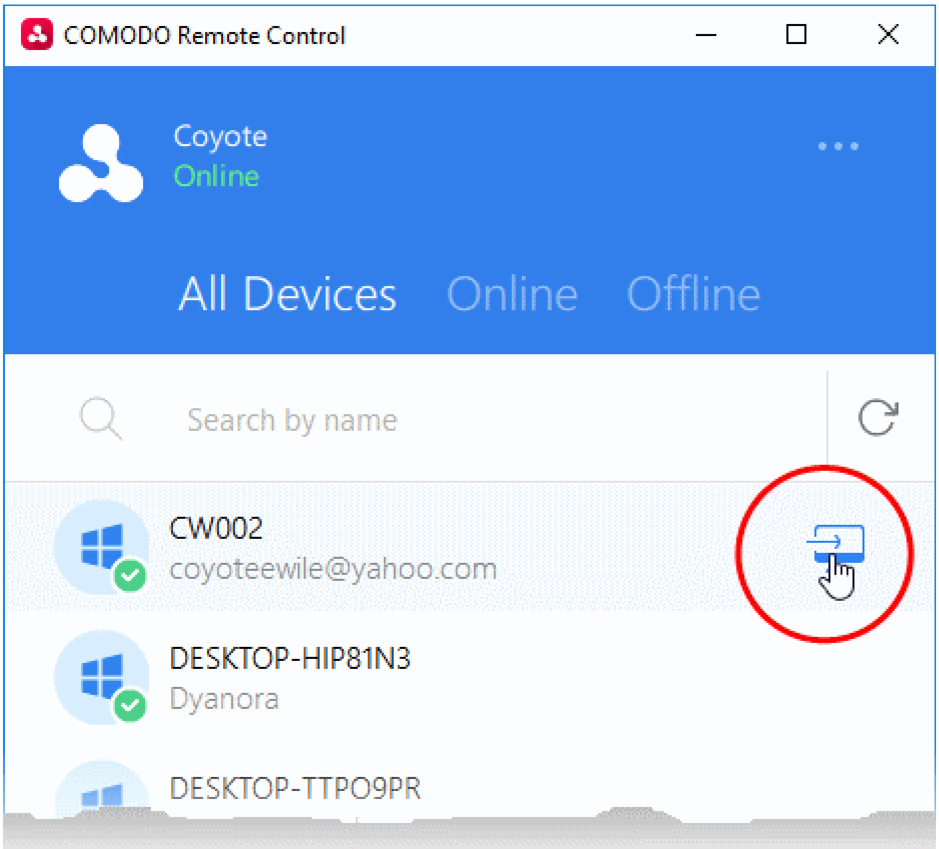
The viewer application will open with a list of enrolled Windows / Mac OS endpoints:



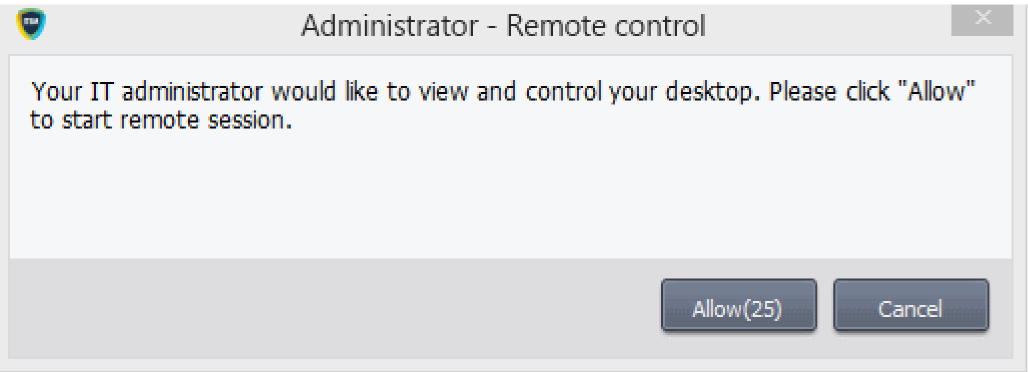
- To search for an endpoint, start typing its name in the search field and select from the suggestions
- To view an updated list of endpoints including those recently added, click the refresh icon ⟳
- Use the 'Online' and 'Offline' tabs to filter the list based on endpoint connection status

To remotely manage an endpoint

- Move your mouse over an endpoint and click the icon on the right:



A request message will be shown to end-users if configured appropriately:

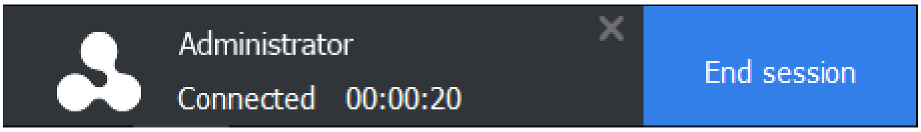


Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

You have the following configuration options:

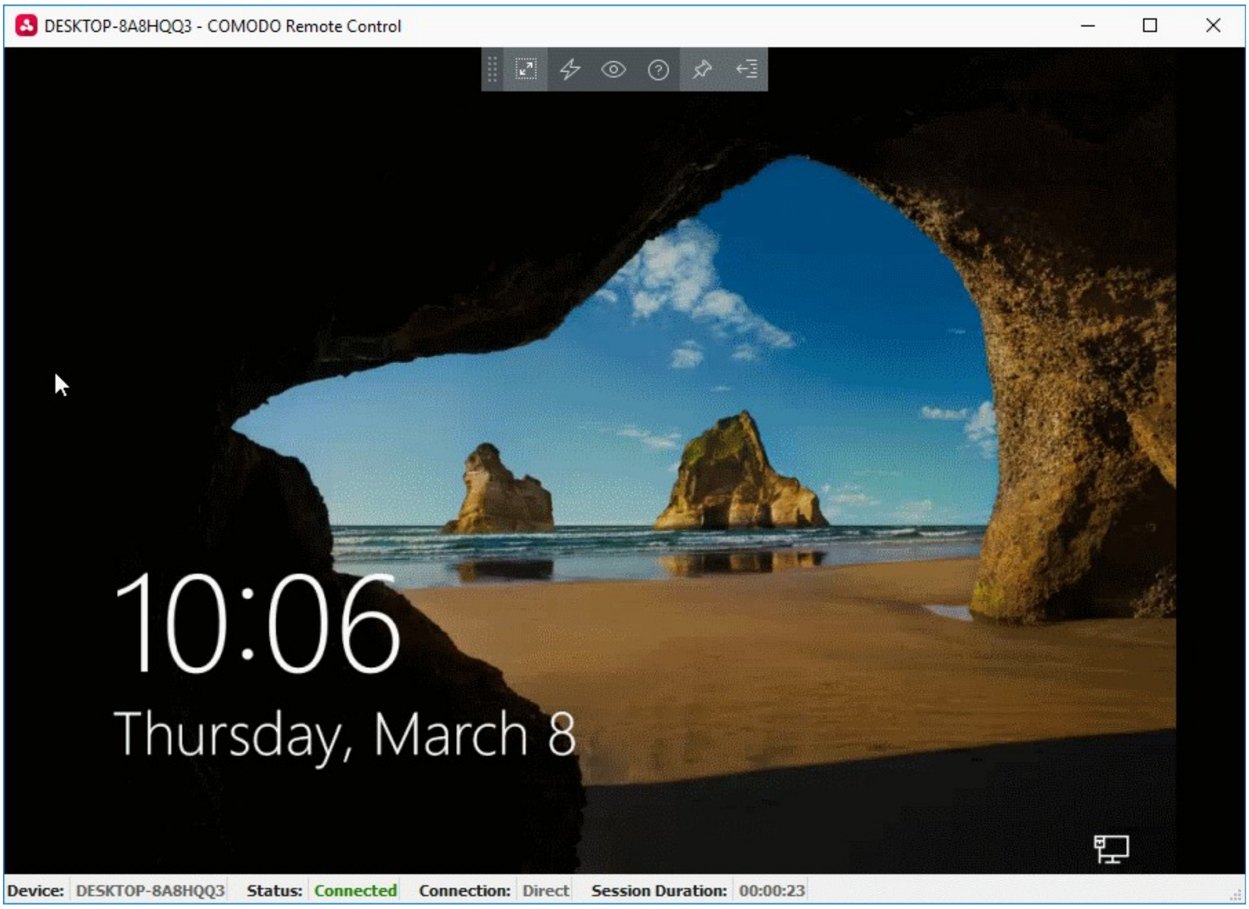
- You can take remote control of device without permission from the user
- You can ask for permission and take control if the user allows, or if the user does not respond within a certain time
- Disable remote control entirely
- See **Remote Control Settings** for more details.

Once the connection is established, a notification will appear on the endpoint stating that an administrator has taken control:



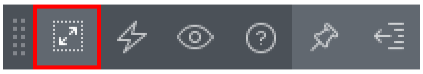
  - The end-user can allow the session to continue or terminate it by clicking 'End session'.
- The message will be shown if the endpoint's profile is set to show the notification (in the 'Remote Control' section). See **Remote Control Settings** for more details.

The remote control application will show the desktop of the remote computer:



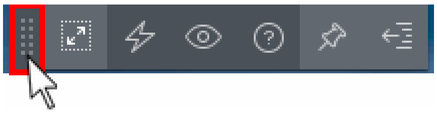
Device: DESKTOP-8A8HQQ3 Status: Connected Connection: Direct Session Duration: 00:00:23

- Administrators can now interact with the target device to perform tasks as required.
- The tool bar at the top of the client interface contains the following menus and settings:

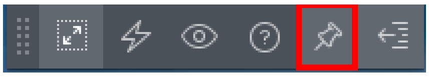


Full Screen - The remote desktop will cover your entire display, without the operating system's window-framing interface.

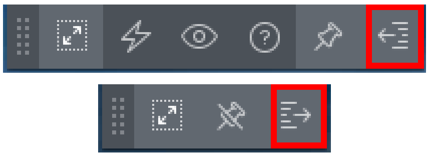
  - Click the same icon to exit full screen mode



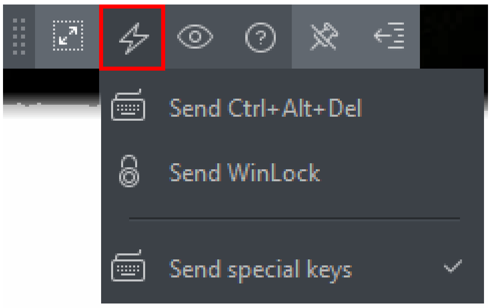
Position - Click and drag the tool bar to your preferred location.



Pin - Pin or unpin the tool bar to the title bar in full screen view.

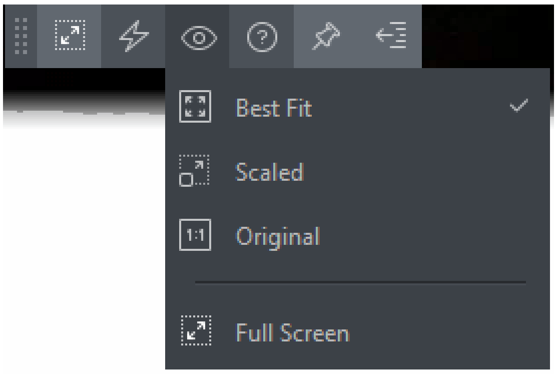


Minimize/Maximize - Show/hide tool bar options.



Actions - (Applies to Windows devices only) Send control commands to the endpoint.

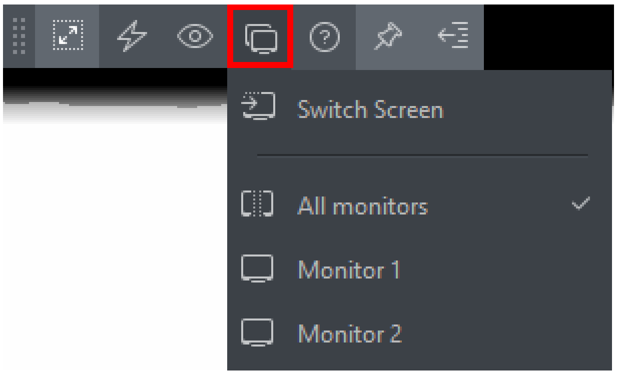
- **Send Ctrl + Alt + Del** - Opens the Windows security screen. This allows you to lock the computer, log the current user out of the remote machine, change passwords, view the local task manager or shut down/restart/hibernate the machine.
- **Send WinLock** - Locks the managed endpoint. A password will be required to unlock the endpoint.
- **Send special Keys** - If enabled, allows you to send key combination commands such as Ctrl+C, Windows + R and so on.



View - Change the display size of the remote desktop. The available options are:

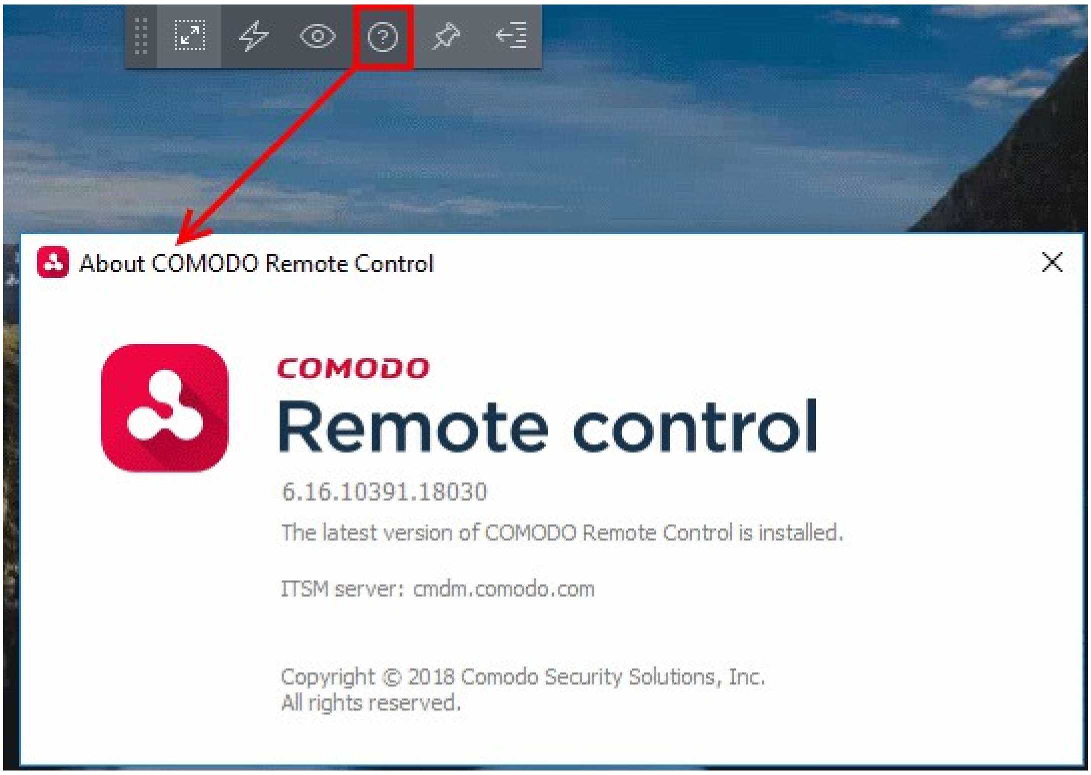
- **Best Fit** - Automatically adjusts the screen resolution for the best visual experience.
- **Scaled** - Displays the target desktop with the resolution of the admin computer
- **Original** - Displays the target desktop at its own resolution
- **Full screen** - Displays the remote desktop in full screen view

Multi-Screen - The multi-screen icon only appears if the target point endpoint has a multi-monitor setup. The drop-down shows all monitors connected to the endpoint and allows you to choose which to view.



- Select 'Switch Screen' to move to the next screen on the list
- Select 'All Monitors' to view all connected screens simultaneously
- Select an individual monitor to view it in stand-alone mode

Help - Shows the 'About Comodo Remote Control' dialog which shows version number and copyright information.



About COMODO Remote Control

COMODO Remote control

6.16.10391.18030

The latest version of COMODO Remote Control is installed.

ITSM server: cmdm.comodo.com

Copyright © 2018 Comodo Security Solutions, Inc.
All rights reserved.

Using the RMM Console for Remote Control

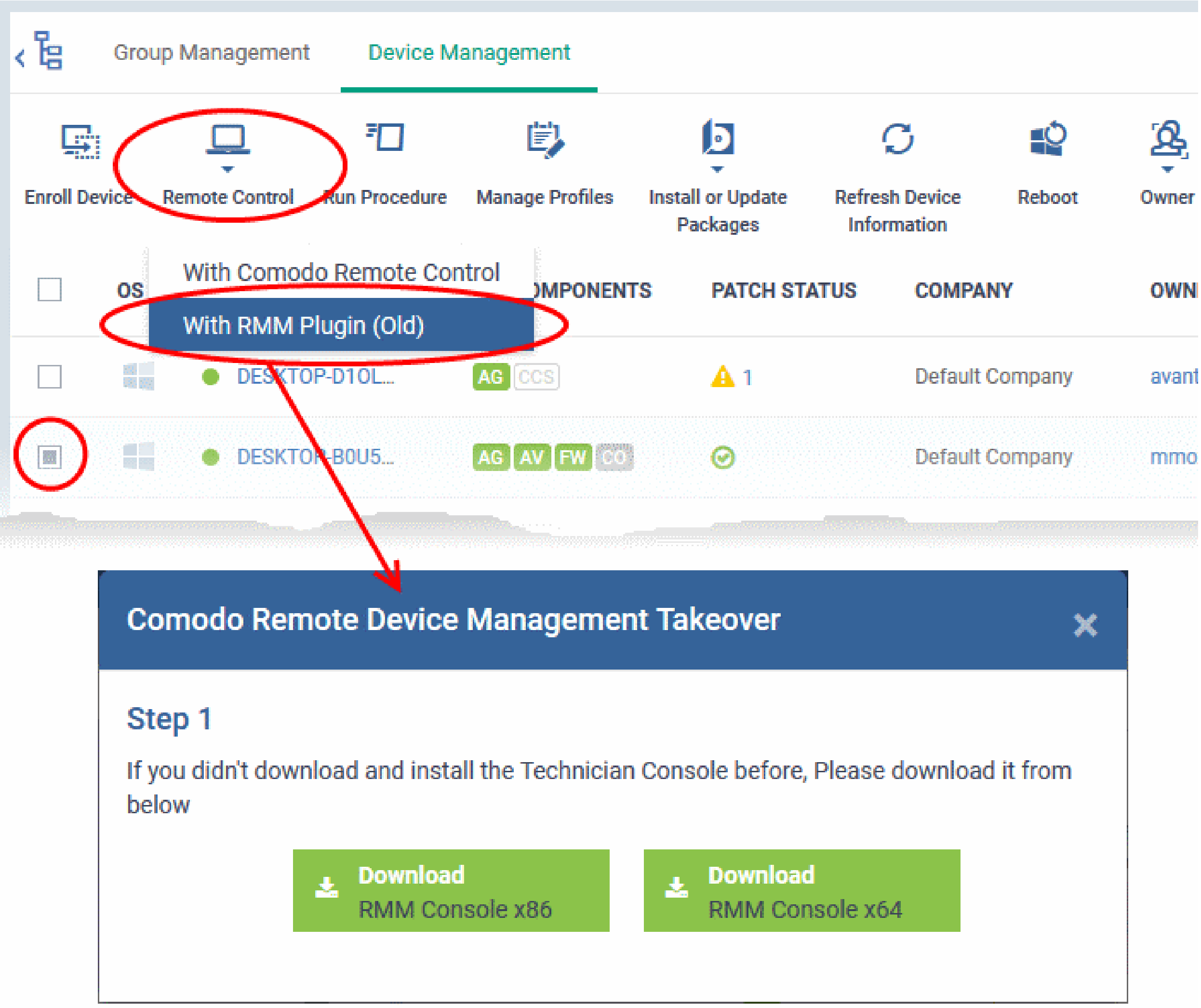
Comodo's Remote Monitoring and Management (RMM) grants MSPs complete visibility and control over the systems they manage. C1 customers can use RMM to takeover Windows devices. In order to do that, administrators should:

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

To download the RMM admin console

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Choose a 'Windows' device, click 'Remote Control' on the top then select 'With RMM Plugin'



Comodo Remote Device Management Takeover

Step 1

If you didn't download and install the Technician Console before, Please download it from below

Download RMM Console x86

Download RMM Console x64

The 'Remote Device Management Takeover Wizard' will appear.

- 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**.

5.2.7. Apply Procedures to 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 Management' interface.
  - See **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 Management' interface.

- **Applying procedures on a single device**
- **Applying procedures on multiple devices at once**

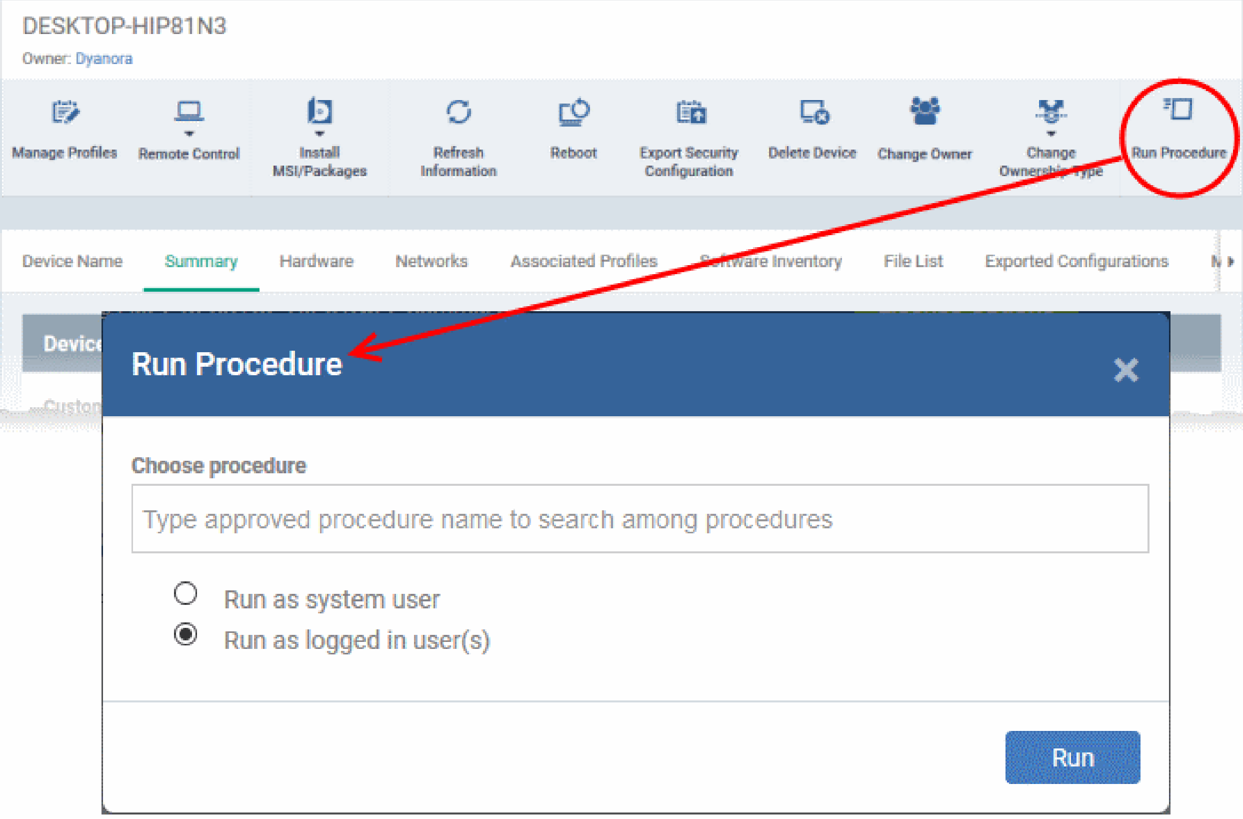
To run a procedure on a single device

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of a 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



- Type the first few characters of the name of the procedure in the 'Choose Procedure' text box. Select the procedure you want to apply from the search suggestions. Only one procedure can be run at a time. Please note only **approved** procedures will be listed.
- Choose the endpoint user account which should be used to run the procedure. The available options are:
    - Run as system user
    - Run as logged in user(s) (default)
- Click 'Run'

The command will sent to the device and the selected procedure will be run on the device. An alert will be generated if the procedure fails (presuming alerts have been configured). The process will be logged and can be viewed in the 'Procedure Logs' screen.

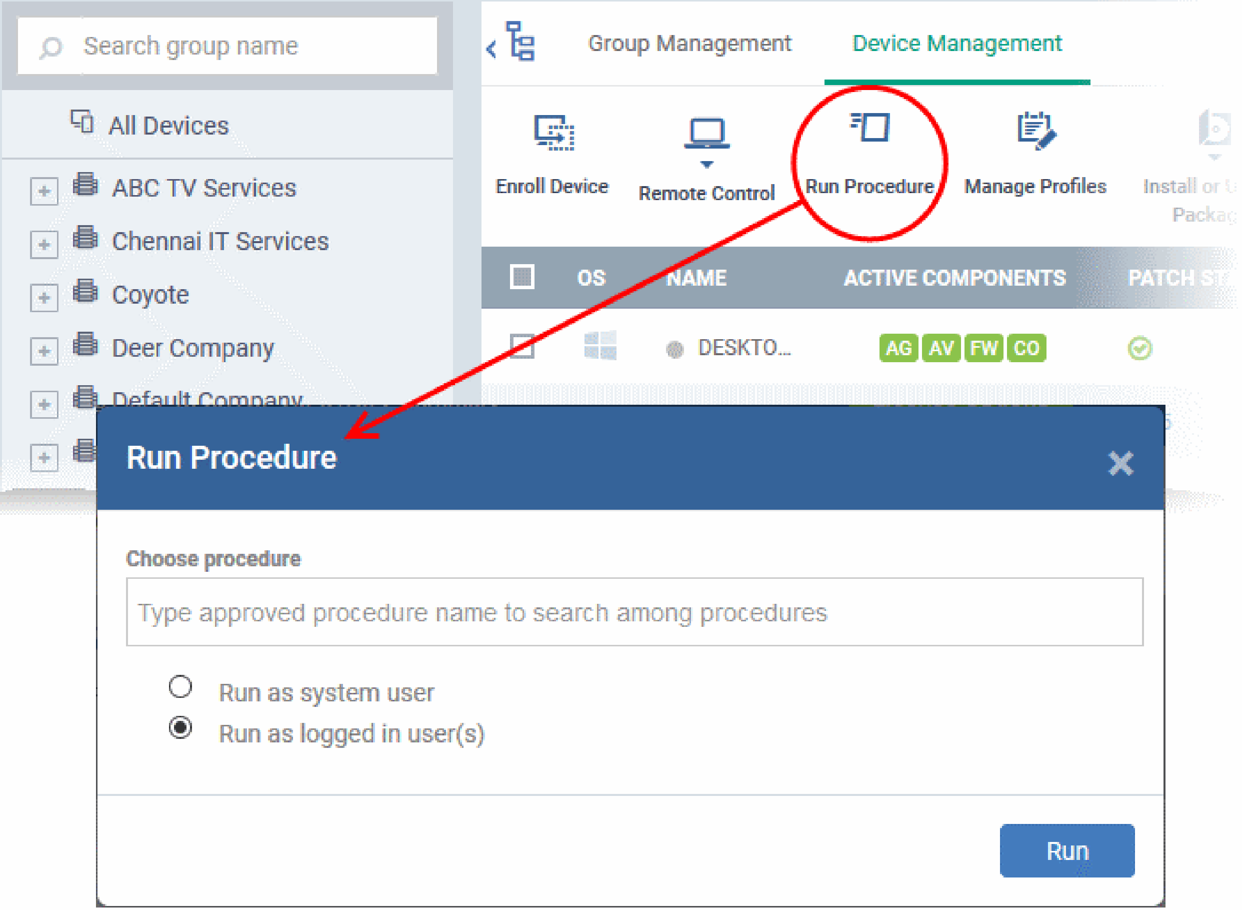
To run procedures on multiple devices at once

- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

- Select the Company and choose the group under it to view the list of devices in that group

  Or
- Select 'All Devices' to view every device enrolled to ITSM

- Select the devices on which 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



Run Procedure

Choose procedure

Type approved procedure name to search among procedures

○ Run as system user

● Run as logged in user(s)

Run

- Type the first few characters of the name of the procedure in the 'Choose Procedure' text box. Select the procedure you want to apply from the search suggestions. Only one procedure can be run at a time. Please note only **approved** procedures will be listed.
- Choose the endpoint user account which should be used to run the procedure. The available options are:
  - Run as system user
  - Run as logged in user(s) (default)
- 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.

5.2.8. Remotely Install and Update Packages on Windows Devices

The 'Device Management' interface lets you install Comodo applications and third-party MSI packages on to managed Windows endpoints. Admins can also update ITSM packages which are already installed on endpoints.

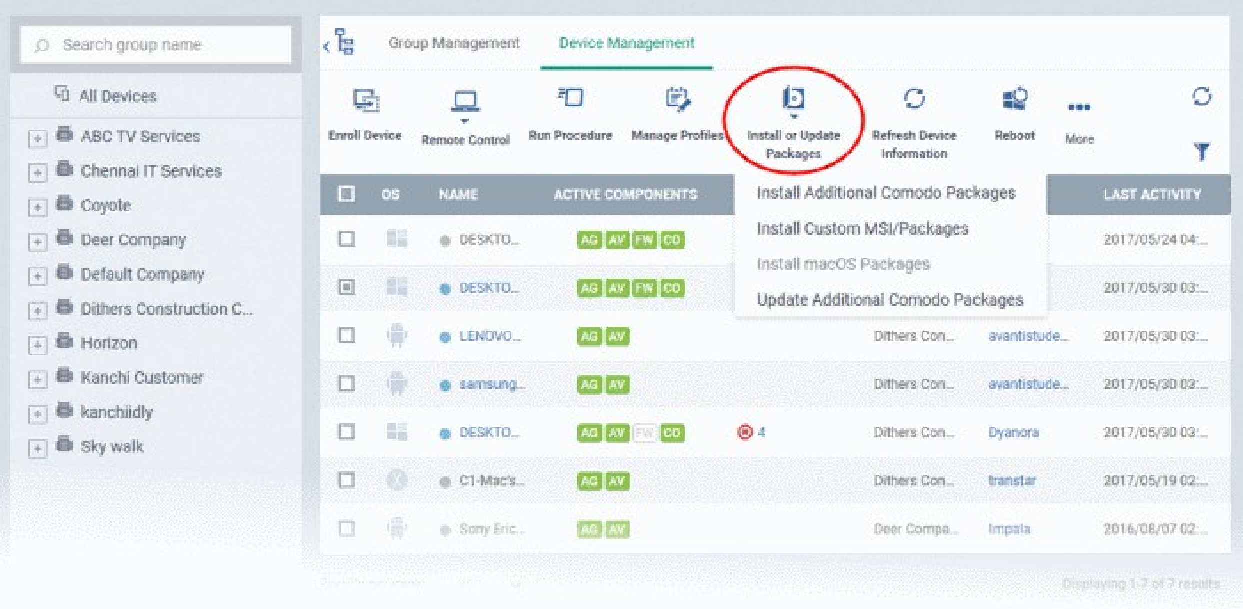
Note for RMM Users: The option to install the RMM agent onto Windows endpoints is available if you logged into

ITSM via the Comodo One interface.

To install MSI / ITSM packages

- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
    - Select a company or a group from the left pane to view the list of devices in that company/group

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Select the Windows device(s) on which you want install or update the packages
- Click 'Install or Update Packages'



☐	OS	NAME	ACTIVE COMPONENTS				LAST ACTIVITY
☐		DESKTO...	AG AV FW CO				2017/05/24 04:...
☒		DESKTO...	AG AV FW CO				2017/05/30 03:...
☐		LENOVO...	AG AV		Dithers Con...	avantistude...	2017/05/30 03:...
☐		samsung...	AG AV		Dithers Con...	avantistude...	2017/05/30 03:...
☐		DESKTO...	AG AV FW CO	4	Dithers Con...	Dyanora	2017/05/30 03:...
☐		C1-Mac's...	AG AV		Dithers Con...	transtar	2017/05/19 02:...
☐		Sony Eric...	AG AV		Deer Compa...	Impala	2016/08/07 02:...

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

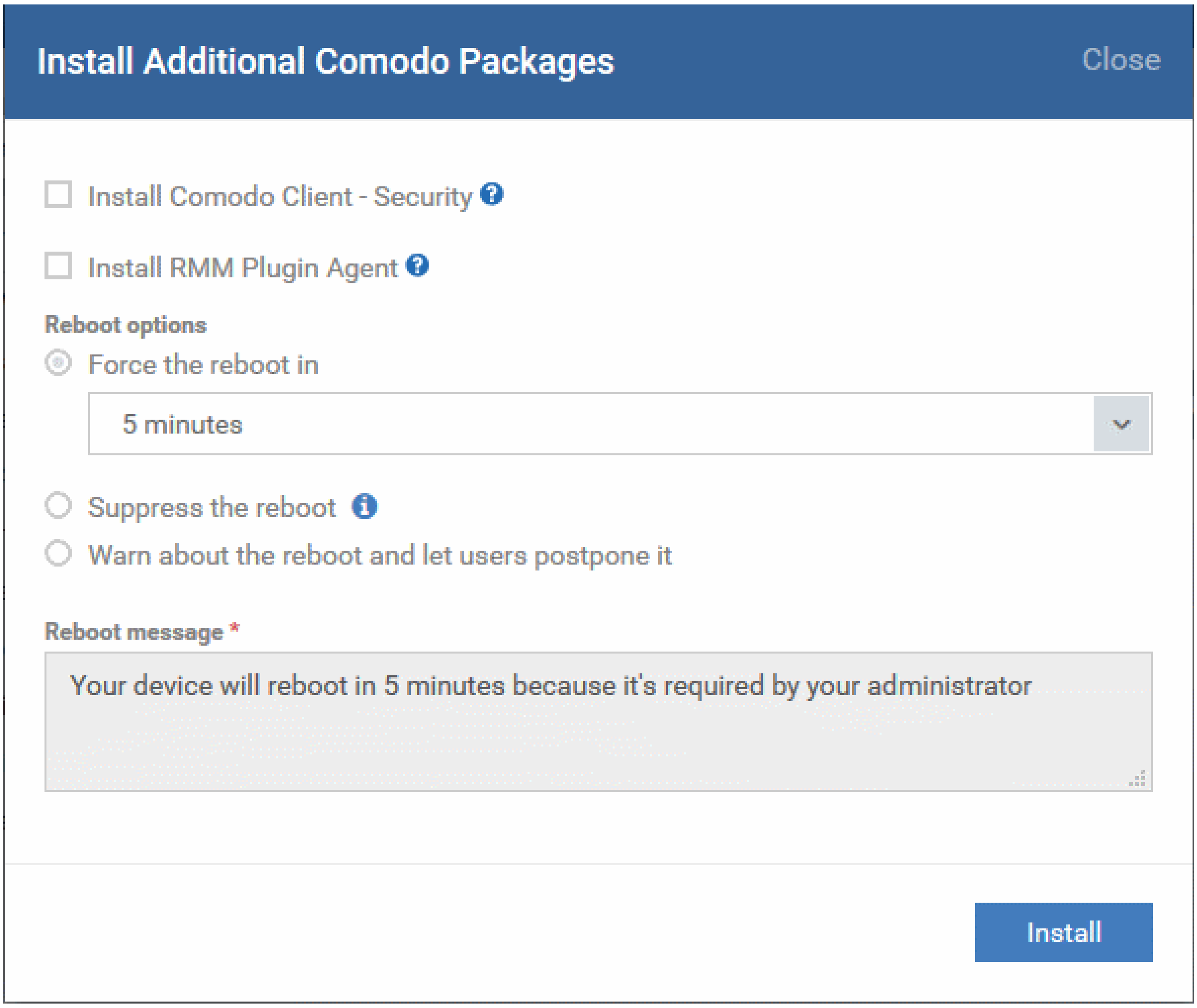
The drop-down displays options for:

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

To install ITSM packages

- Select 'Install Additional Comodo packages' from the 'Install or Update 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.



Install Additional Comodo Packages

□ Install Comodo Client - Security

□ Install RMM Plugin Agent

Reboot options

● Force the reboot in

5 minutes

○ Suppress the 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

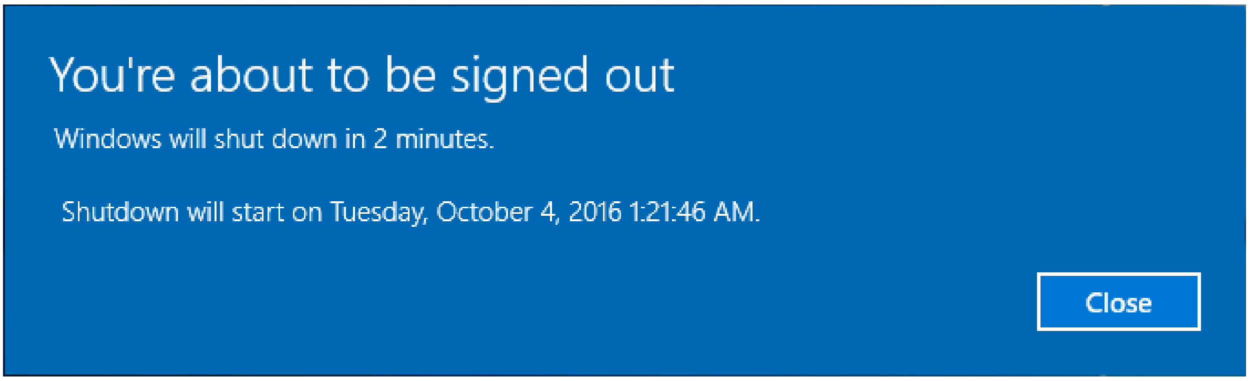
The list of available additional packages will be displayed. The available packages are:

- **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. Note: This option is only available for endpoints that do not have CCS installed.
- **Install RMM Plug-in Agent** - Select this option only if you want to use the older, standalone RMM module. RMM functionality has now been incorporated into the main ITSM application, so most users should not need to install this agent on endpoints.

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:



You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

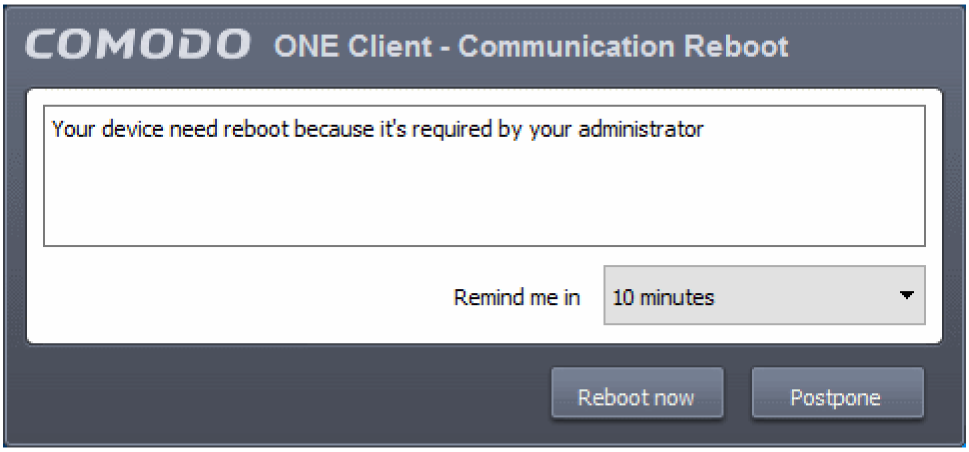
The device will be restarted automatically when the time period elapses.

- 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:



COMODO ONE Client - Communication Reboot

Your device need reboot because it's required by your administrator

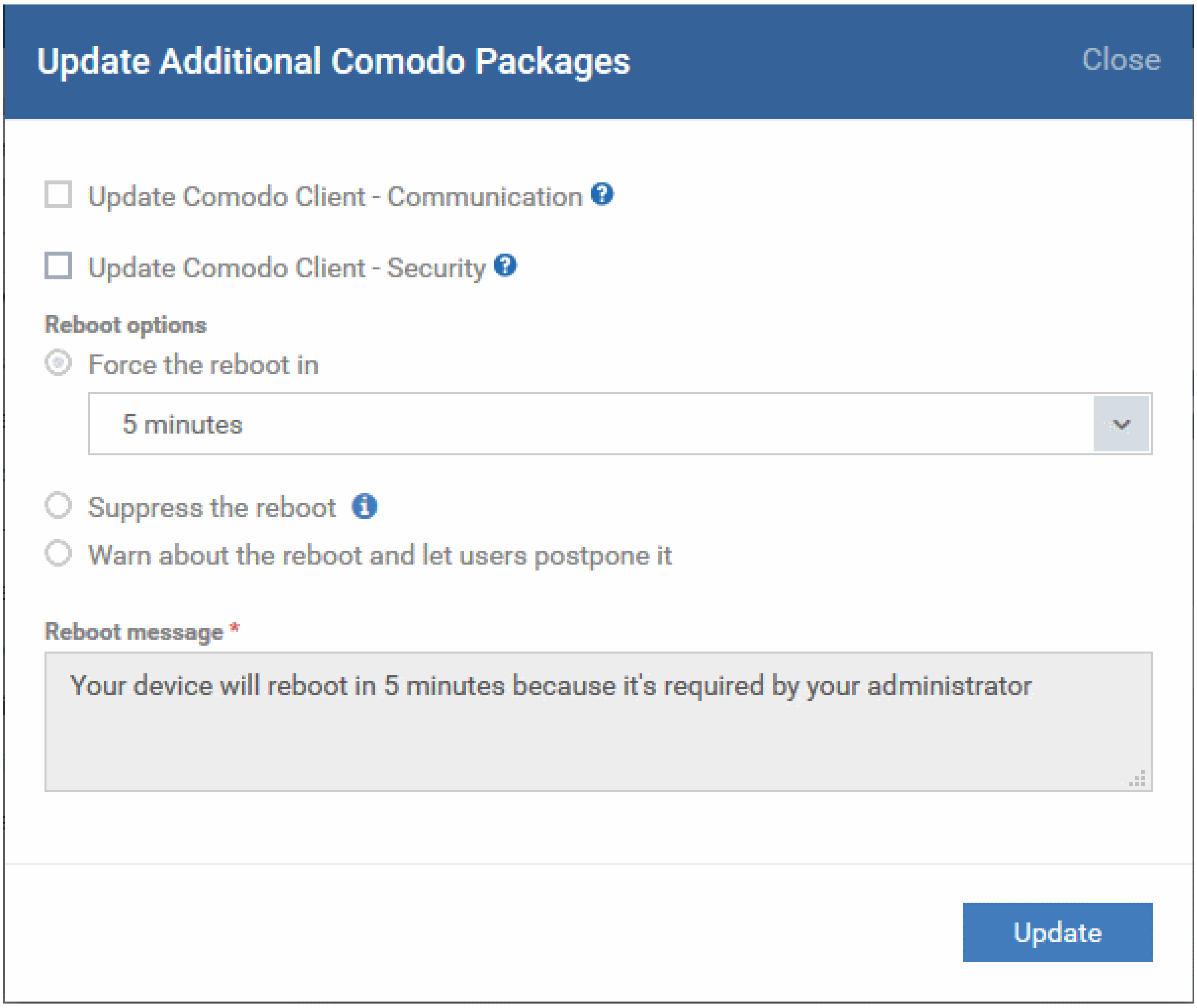
Remind me in: 10 minutes

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. See **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 update ITSM Packages

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



Update Additional Comodo Packages

□ Update Comodo Client - Communication

□ Update Comodo Client - Security

Reboot options

● Force the reboot in

5 minutes

○ Suppress the 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

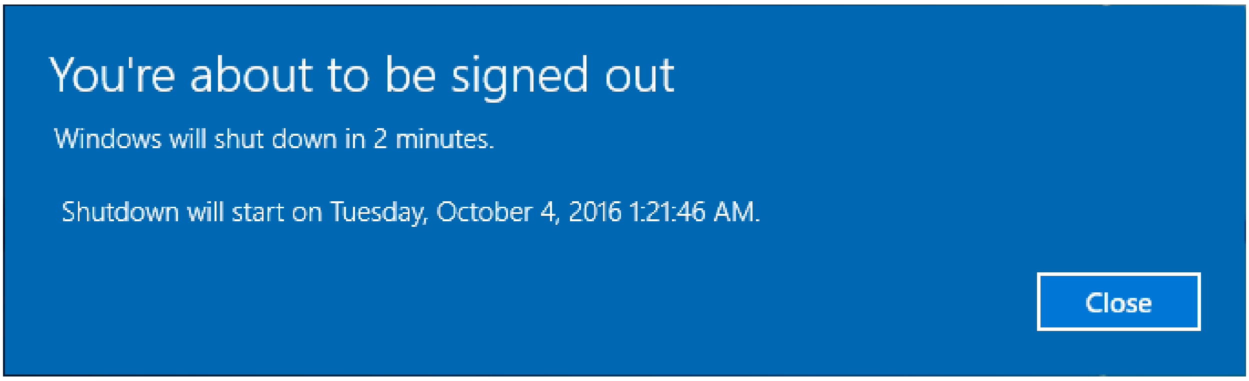
A list of additional packages that can be updated will be displayed. The available options are:

- **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.
- **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.

CCS requires the endpoint to be restarted in order for the update 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:



You're about to be signed out

Windows will shut down in 2 minutes.

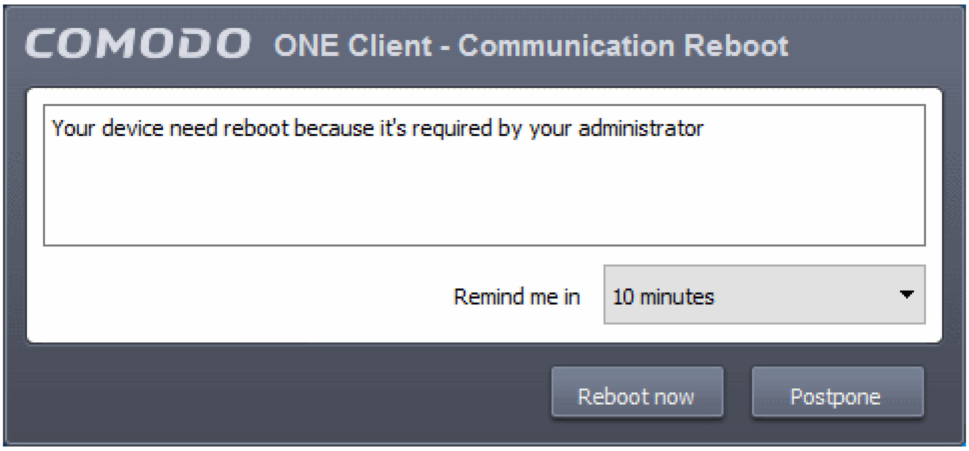
Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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 'Update'.

The endpoint will not restart after the update. However, the update will not take effect until the endpoint is next restarted.

- To let end-users restart the machine at their convenience, choose 'Warn about the reboot and let users postpone it'. Enter a message to be shown to the user and click 'Update':



Your device need reboot because it's required by your administrator

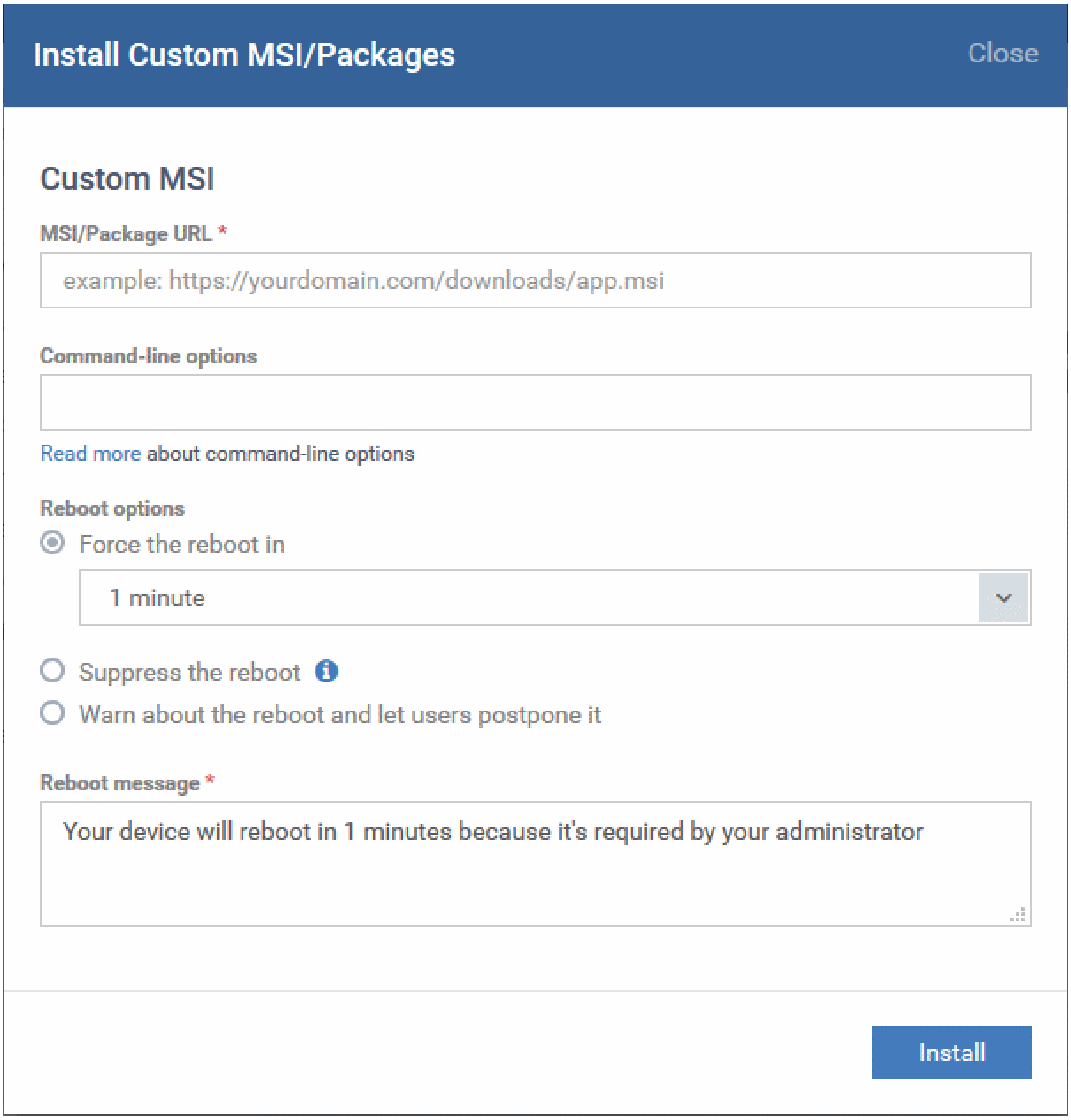
Remind me in: 10 minutes

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.

To install third-party MSI packages

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

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



Custom MSI

MSI/Package URL *

example: https://yourdomain.com/downloads/app.msi

Command-line options

Read more about command-line options

Reboot options

● Force the reboot in

1 minute

○ Suppress the reboot

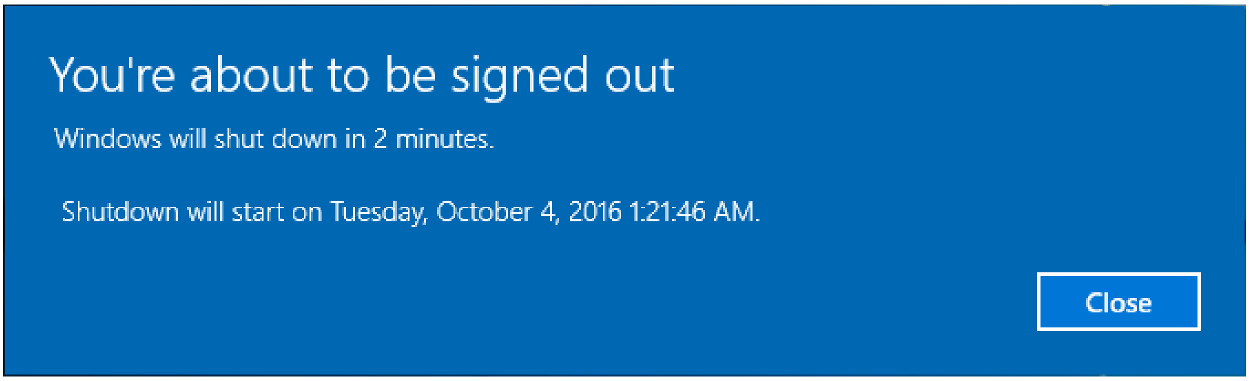
○ Warn about the reboot and let users postpone it

Reboot message *

Your device will reboot in 1 minutes because it's required by your administrator

- 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:



You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

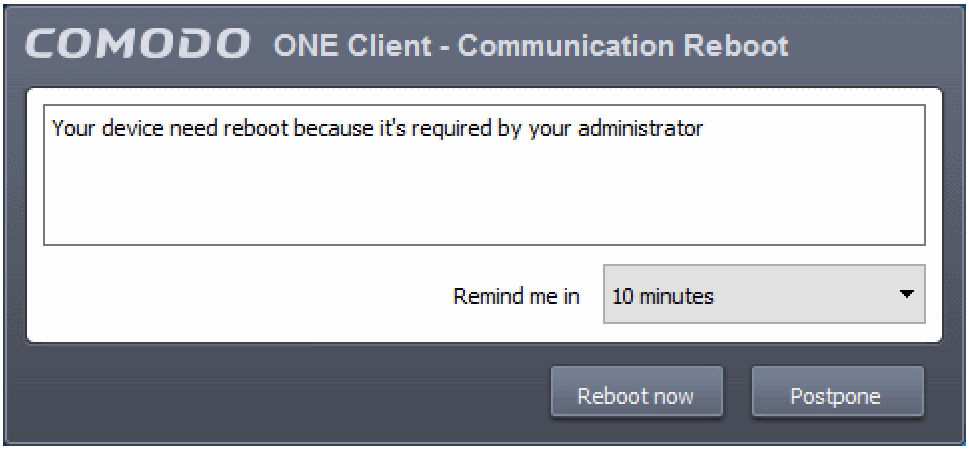
The device will be restarted automatically when the time period elapses.

- 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:



Your device need reboot because it's required by your administrator

Remind me in: 10 minutes

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.

5.2.9. Remotely Install Packages on Mac OS Devices

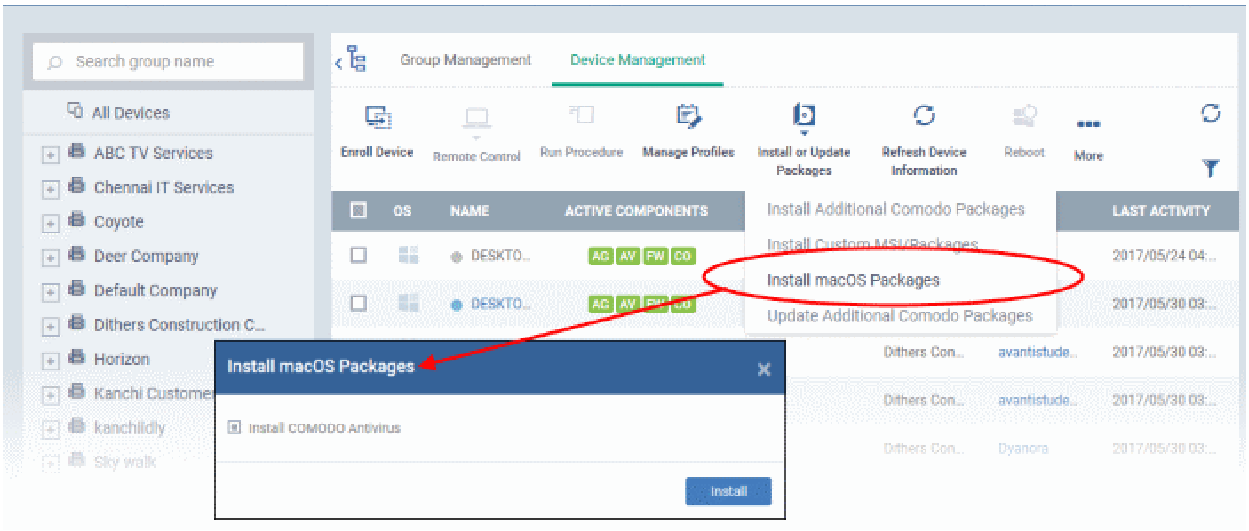
Administrators can remotely install Comodo Antivirus for Mac (CAVM) onto Mac OS devices from the 'Device Management' interface.

To install Mac OS packages

- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
    - Select a company and group to view all devices in the group

  Or

    - Select 'All Devices' to view every device enrolled to ITSM
- Select the Mac OS device(s) on which you want install packages
- Click 'Install or Update Packages' from the options at the top and choose 'Install macOS Packages'



- Alternatively, click the name of the device to open the 'Device Details' interface. Click 'Install Mac OS Packages' from the options at the top.

The 'Install Mac OS 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

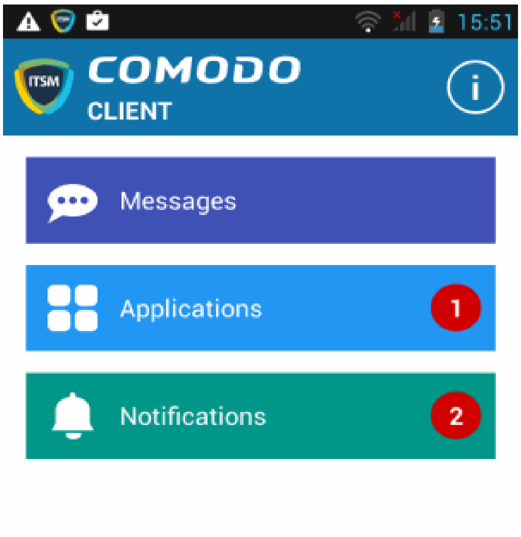
The installation command will be sent to the device. The security components that are active once CAVM is installed depends on the security profile applied.

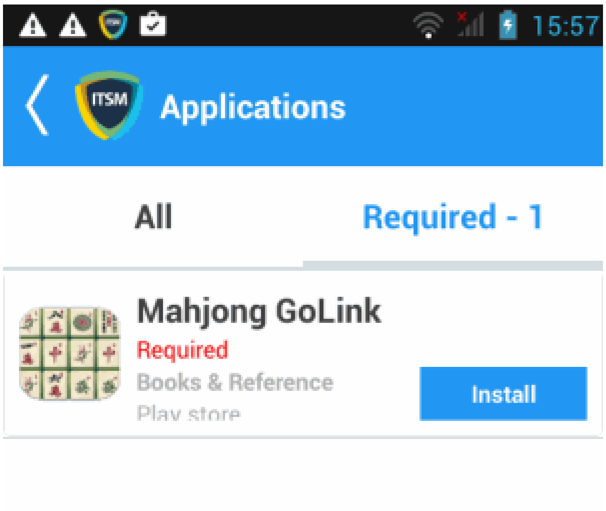
See **Assigning Configuration Profile to Selected Devices**, **Assigning Configuration Profile(s) to Users' Devices**, **Assigning Configuration Profile to a User Group** and **Assigning Configuration Profile to a Device Group** for help with profiles.

5.2.10. Install 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:

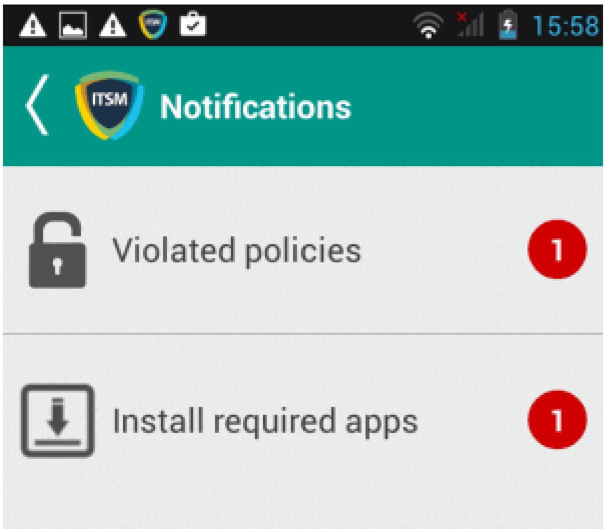




- **All** - Displays all apps available for installation, including mandatory and optional apps.
- **Required** - Displays apps that must be installed on the device to comply with the ITSM profile applied to the device.

- 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.

5.2.11. Generate 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.

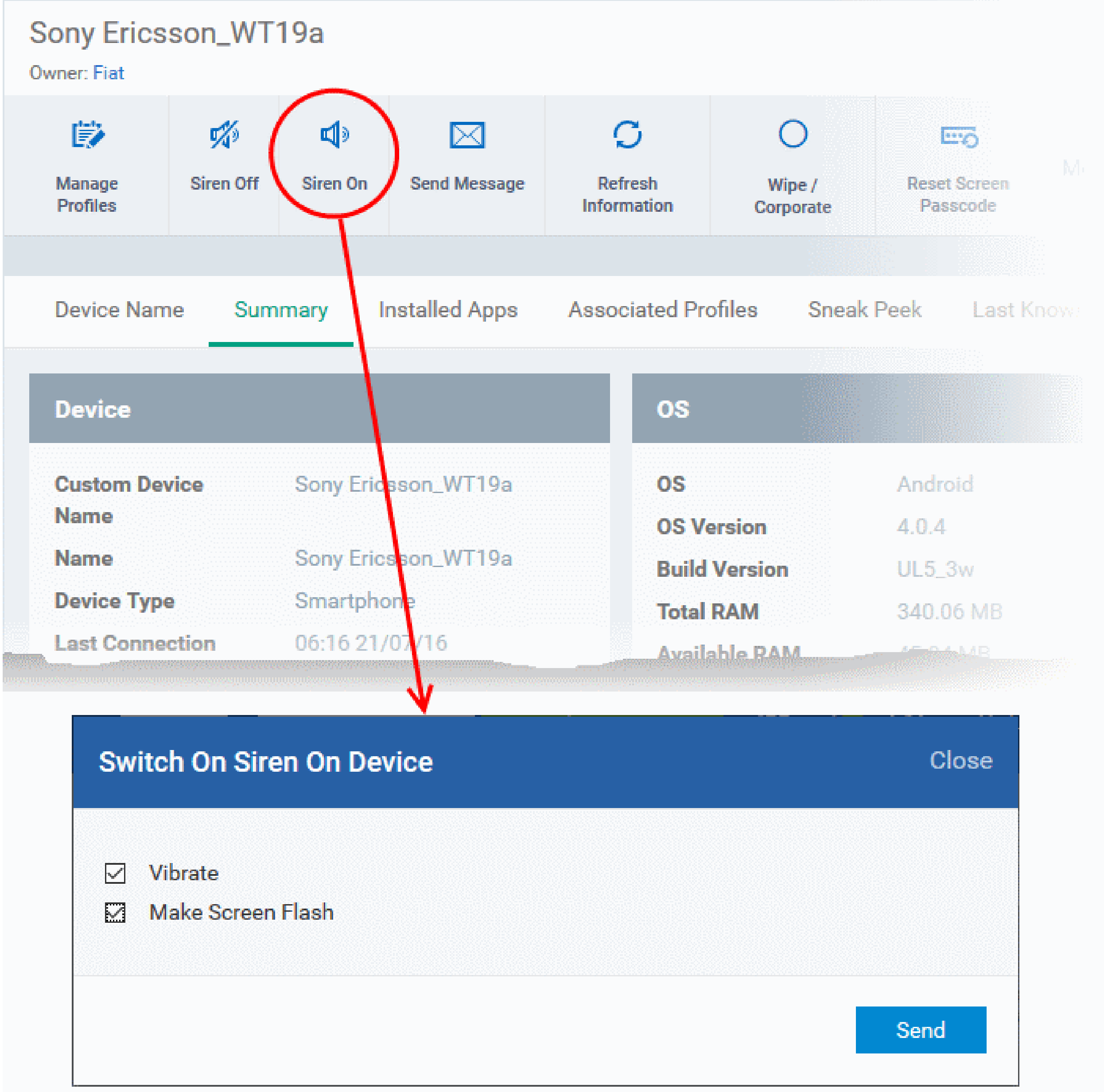
The following sections contain more information on:

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

To generate alarm on a single device

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the device on which you want to sound an alarm
- Click the 'Siren On' option in the 'Device Details' interface



Device	
Custom Device Name	Sony Ericsson_WT19a
Name	Sony Ericsson_WT19a
Device Type	Smartphone
Last Connection	06:16 21/07/16

OS	
OS	Android
OS Version	4.0.4
Build Version	UL5_3w
Total RAM	340.06 MB
Available RAM	

☑ Vibrate
☑ Make Screen Flash

You can choose from the following options:

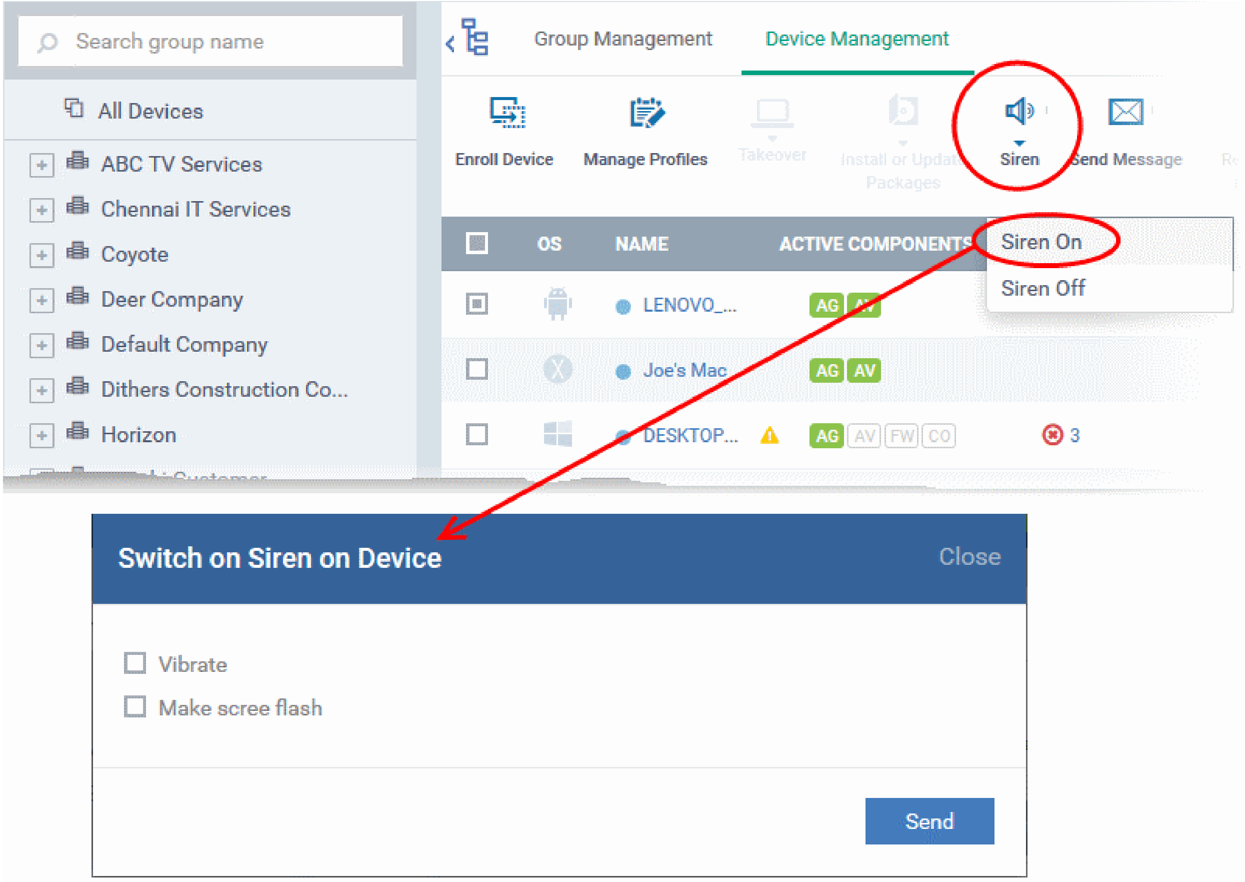
  - Vibrate - The device will vibrate along with the siren
  - Make screen flash - The device screen will flash intermittently along with the siren
- Click the 'Send' button to issue the alarm.
- To switch off the alarm, click 'Siren Off' from the same interface.

To generate alarm on several devices

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

  Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices on which you want to sound an alarm
- Click 'Siren' at the top and choose Siren On'



Switch on Siren on Device

Close

□ Vibrate

□ Make scree flash

Send

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 s top sounding an alarm, from the 'Device Management' interface.
- Click 'Siren' at the top and choose 'Siren Off'

5.2.12. Lock/Unlock 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**

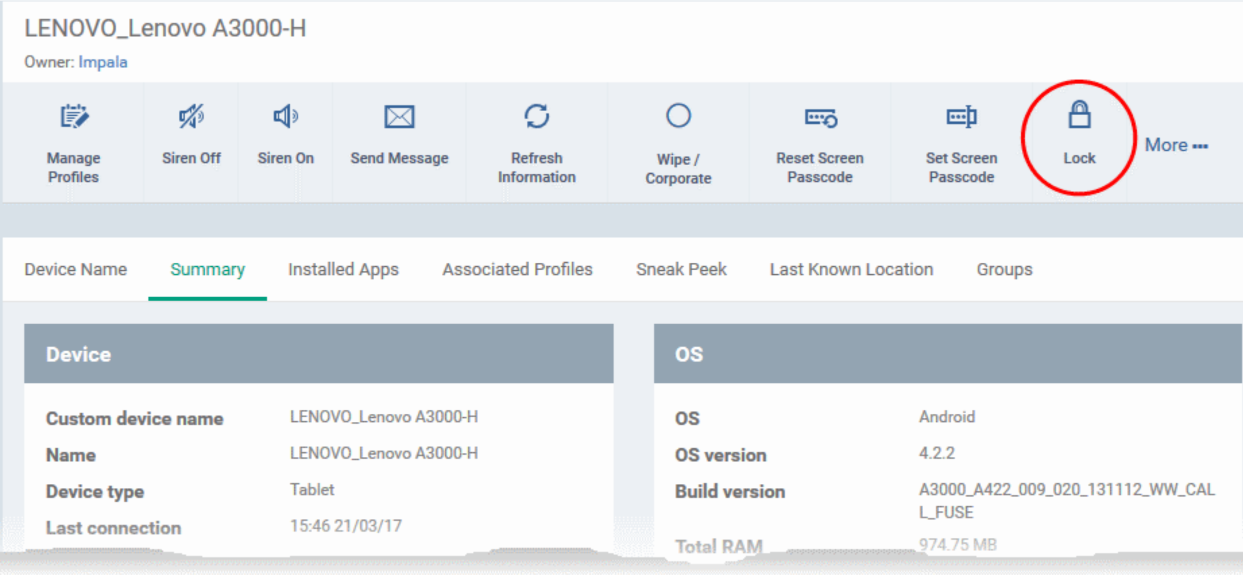
To remotely lock a single device

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

  Or

  - Select 'All Devices' to view every device enrolled to ITSM

- 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



LENOVO_Lenovo A3000-H

Owner: Impala

Device	
Custom device name	LENOVO_Lenovo A3000-H
Name	LENOVO_Lenovo A3000-H
Device type	Tablet
Last connection	15:46 21/03/17

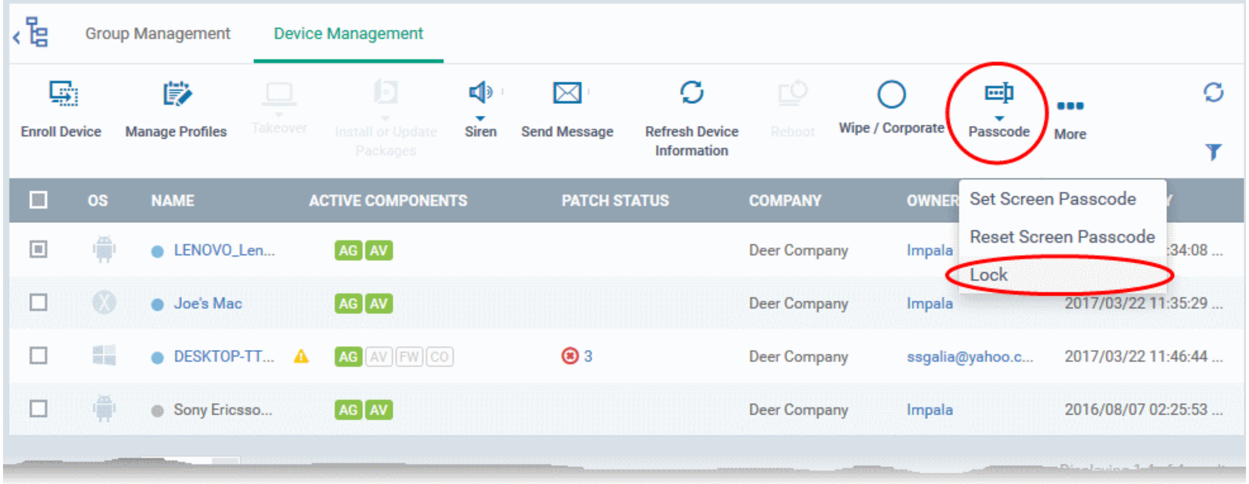
OS	
OS	Android
OS version	4.2.2
Build version	A3000_A422_009_020_131112_WW_CALL_FUSE
Total RAM	974.75 MB

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices to be locked
- Click 'Passcode' from the options at the top or click 'More...' and select 'Passcode' from the drop-down.
- Choose 'Lock' from the options



☐	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	
☑		LENOVO_Len...	AG AV		Deer Company	Impala	:34:08 ...
☐		Joe's Mac	AG AV		Deer Company	Impala	2017/03/22 11:35:29 ...
☐		DESKTOP-TT... ⚠	AG AV FW CO	3	Deer Company	ssgalia@yahoo.c...	2017/03/22 11:46:44 ...
☐		Sony Ericsso...	AG AV		Deer Company	Impala	2016/08/07 02:25:53 ...

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.

5.2.13. Wipe 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 Management' 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).

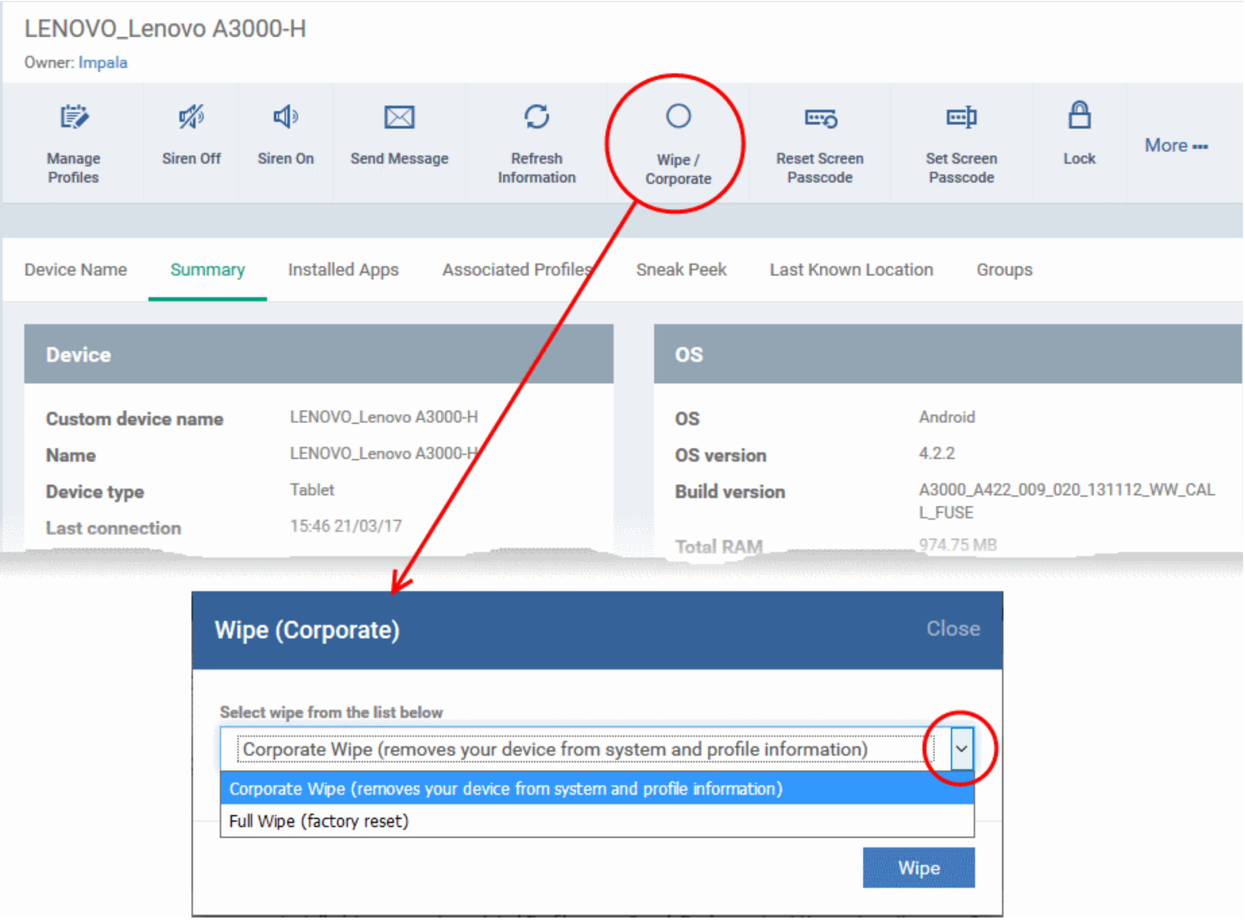
The following sections explain more about:

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

To erase the contents stored in a selected device

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click 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



LENOVO_Lenovo A3000-H

Owner: Impala

Device

Custom device name	LENOVO_Lenovo A3000-H
Name	LENOVO_Lenovo A3000-H
Device type	Tablet
Last connection	15:46 21/03/17

OS

OS	Android
OS version	4.2.2
Build version	A3000_A422_009_020_131112_WW_CAL L_FUSE
Total RAM	974.75 MB

Wipe (Corporate)

Select wipe from the list below

Corporate Wipe (removes your device from system and profile information)

- Corporate Wipe (removes your device from system and profile information)
- Full Wipe (factory reset)

The 'Wipe (Corporate)' dialog will open.

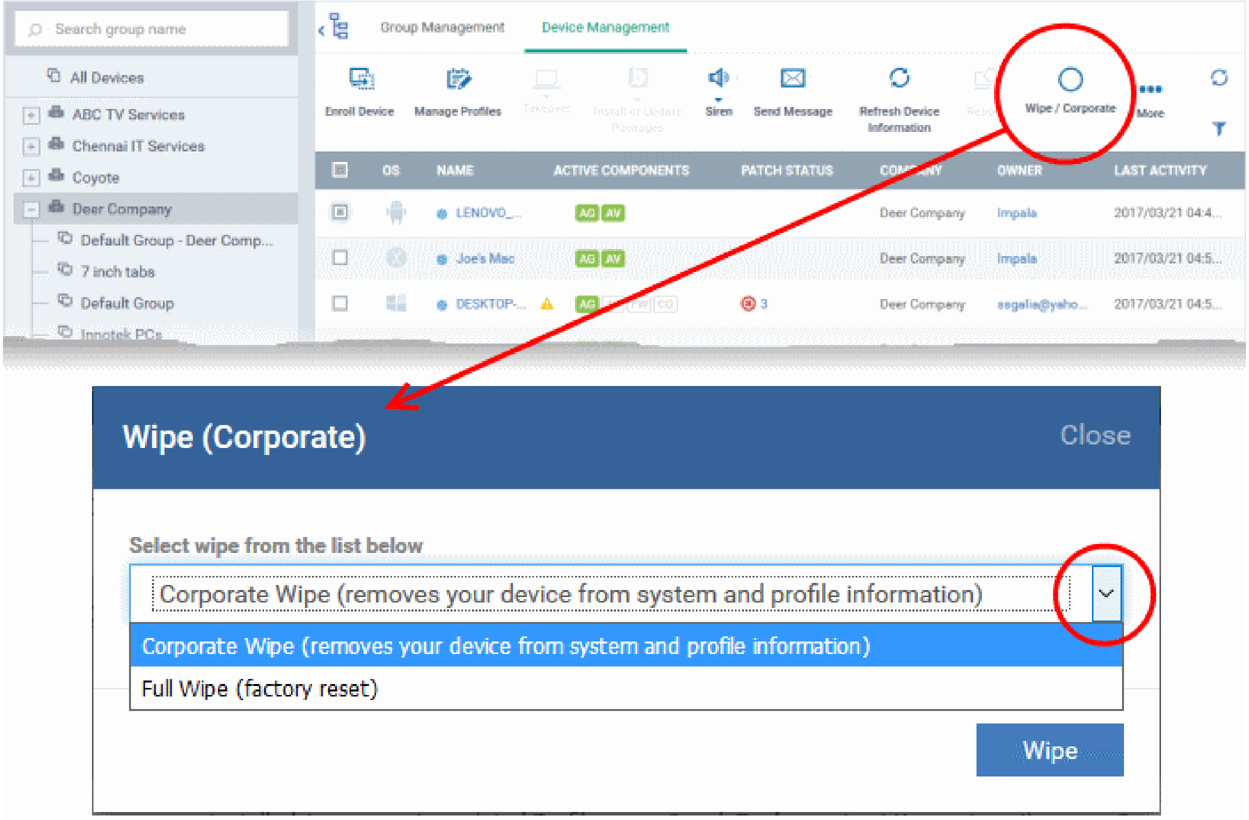
- Select the content to be erased.
  - To remove only ITSM agent and configuration profiles, select 'Corporate Wipe' from the drop-down
  - To erase all the data from the device and the SD card, select 'Full Wipe' from the drop-down. The device will be returned to default factory settings after the wipe 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 the 'Devices' tab on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select the Company and choose the group under it to view the list of devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices to be wiped
- Click 'Wipe / Corporate' from the options at the top or click 'More...' and choose 'Wipe / Corporate' from the options.



Wipe (Corporate)

Close

Select wipe from the list below

Corporate Wipe (removes your device from system and profile information)

Corporate Wipe (removes your device from system and profile information)

Full Wipe (factory reset)

Wipe

The 'Wipe (Corporate)' 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.

5.2.14. Assign Configuration Profiles to Selected Devices

- The 'Device Management' interface lets you view the 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).
- If 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.

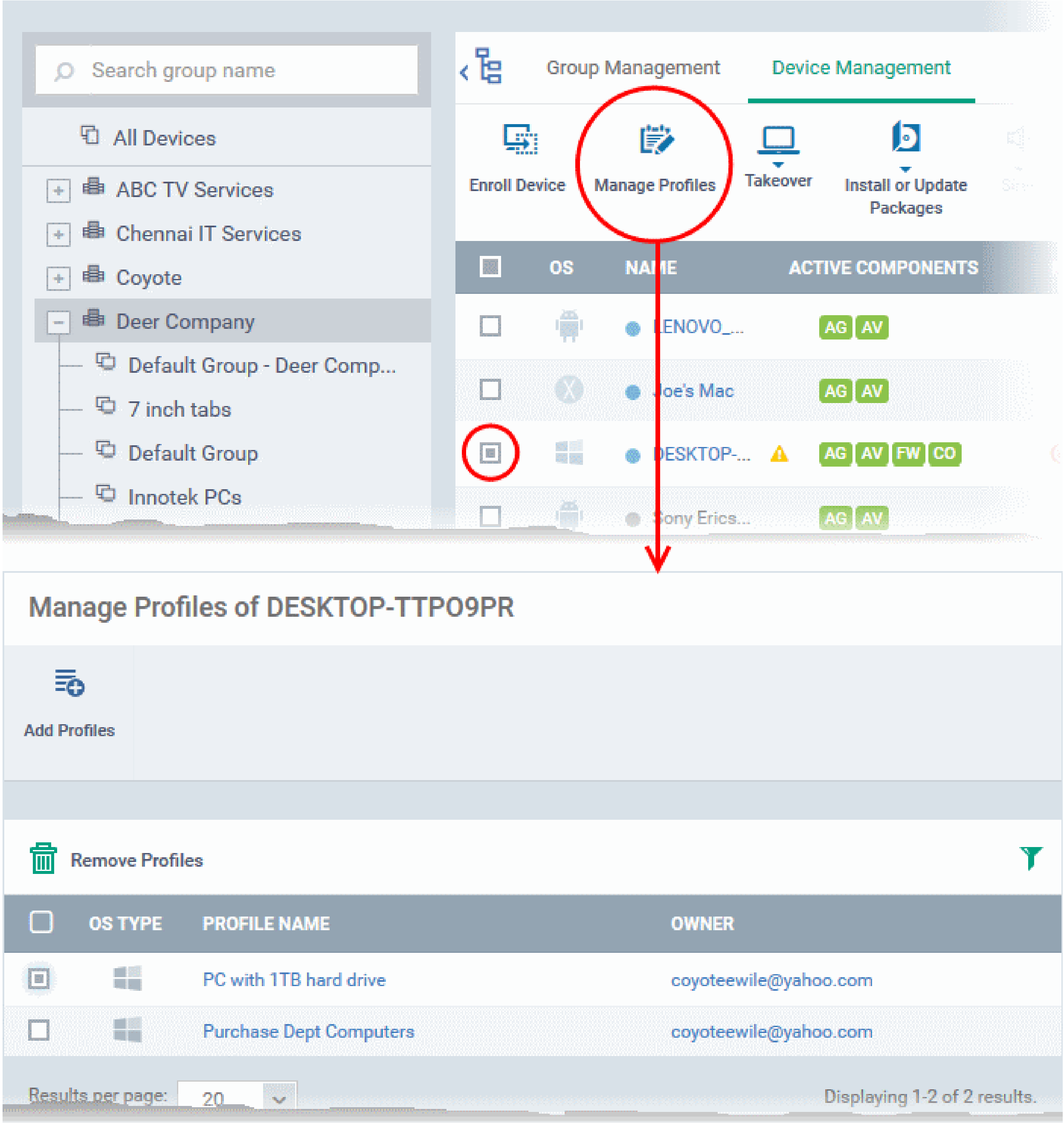
See **Configuration Profiles**, for more details on profiles.

To manage profiles applied to a device

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM

- Select the device to be managed and click 'Manage Profiles' from the options at the top



☐	OS TYPE	PROFILE NAME	OWNER
▣		PC with 1TB hard drive	coyoteewile@yahoo.com
☐		Purchase Dept Computers	coyoteewile@yahoo.com

Results per page: 20

Displaying 1-2 of 2 results.

- Alternatively, click the name of the device to be managed to open its 'Device Details' interface and choose 'Manage Profiles' from the options at the top

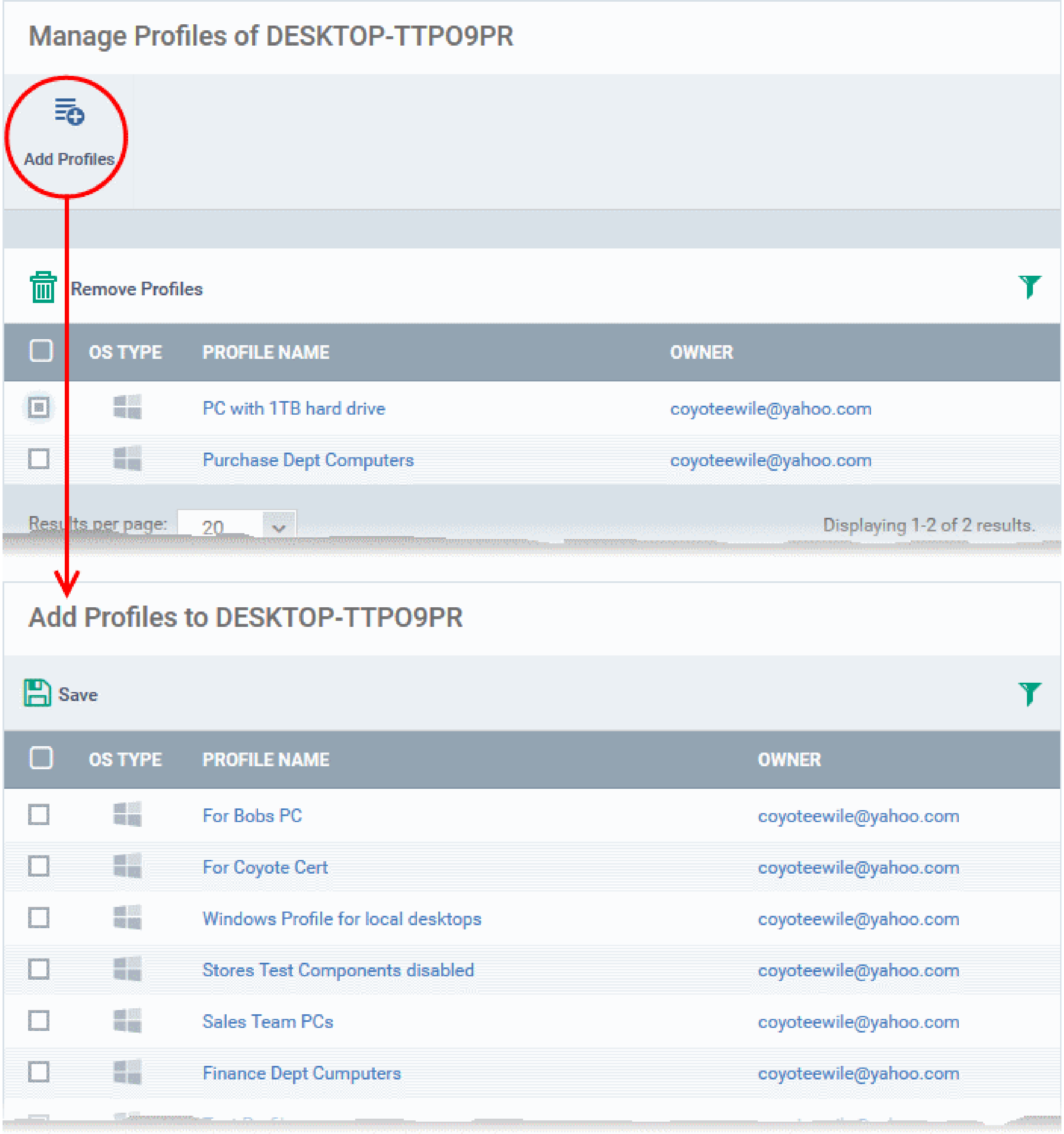
The list of profiles currently active on the device will be displayed.

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. Profiles applied to a device through different channels can be viewed from the respective 'Device Details' interface. Refer to the section **Viewing and Managing Profiles Associated with a Device** for more details.

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



Manage Profiles of DESKTOP-TTPO9PR

□	OS TYPE	PROFILE NAME	OWNER
☒	⊞	PC with 1TB hard drive	coyoteewile@yahoo.com
□	⊞	Purchase Dept Computers	coyoteewile@yahoo.com

Results per page: 20 Displaying 1-2 of 2 results.

Add Profiles to DESKTOP-TTPO9PR

□	OS TYPE	PROFILE NAME	OWNER
□	⊞	For Bobs PC	coyoteewile@yahoo.com
□	⊞	For Coyote Cert	coyoteewile@yahoo.com
□	⊞	Windows Profile for local desktops	coyoteewile@yahoo.com
□	⊞	Stores Test Components disabled	coyoteewile@yahoo.com
□	⊞	Sales Team PCs	coyoteewile@yahoo.com
□	⊞	Finance Dept Cumputers	coyoteewile@yahoo.com

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

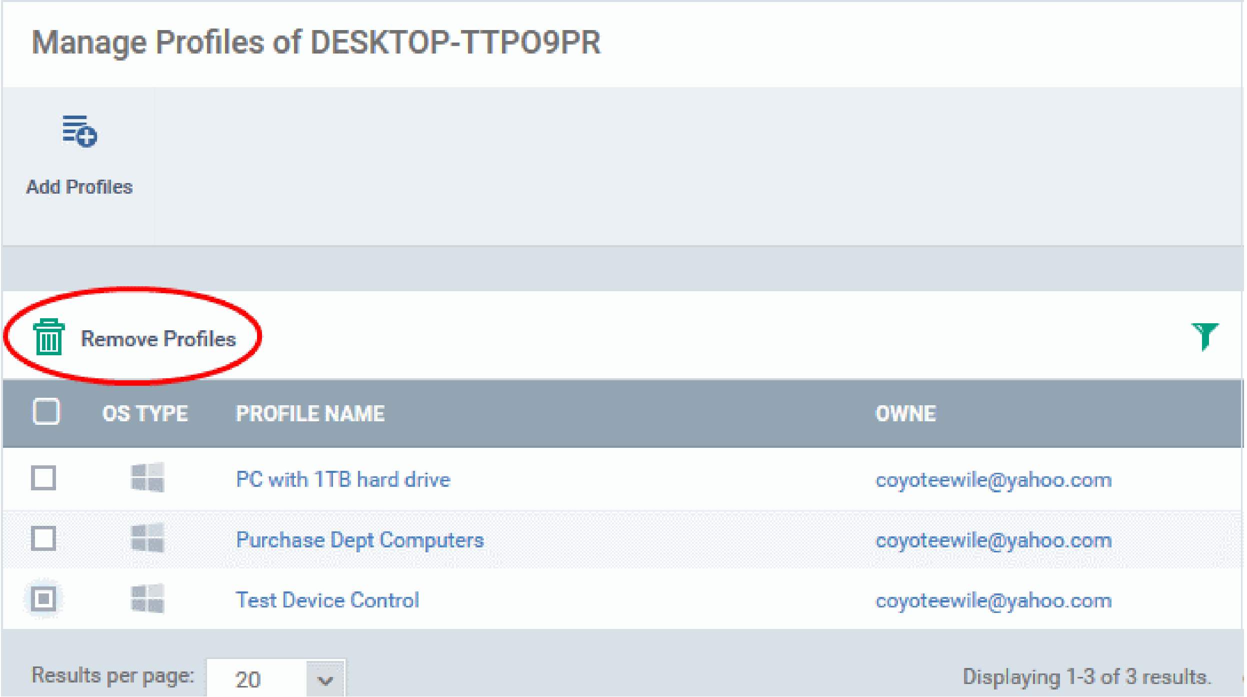
- Select the profile(s) to be applied to the device

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.



Manage Profiles of DESKTOP-TTPO9PR

☐	OS TYPE	PROFILE NAME	OWNE
☐		PC with 1TB hard drive	coyoteewile@yahoo.com
☐		Purchase Dept Computers	coyoteewile@yahoo.com
☒		Test Device Control	coyoteewile@yahoo.com

Results per page: 20

Displaying 1-3 of 3 results.

The selected profile(s) will be removed from the device immediately.

5.2.15. Set / Reset Screen Lock Password for Selected Devices

Administrators can remotely set a new screen lock passcode (or reset the existing code) for enrolled Android devices from the 'Device Management' interface.

Note: Setting new passcode from ITSM is not supported for iOS devices.

The following sections explain more about:

- **Setting and resetting password for a single device**
- **Setting and resetting password for several devices at-once**

To set a new screen lock password or remove password for a single device

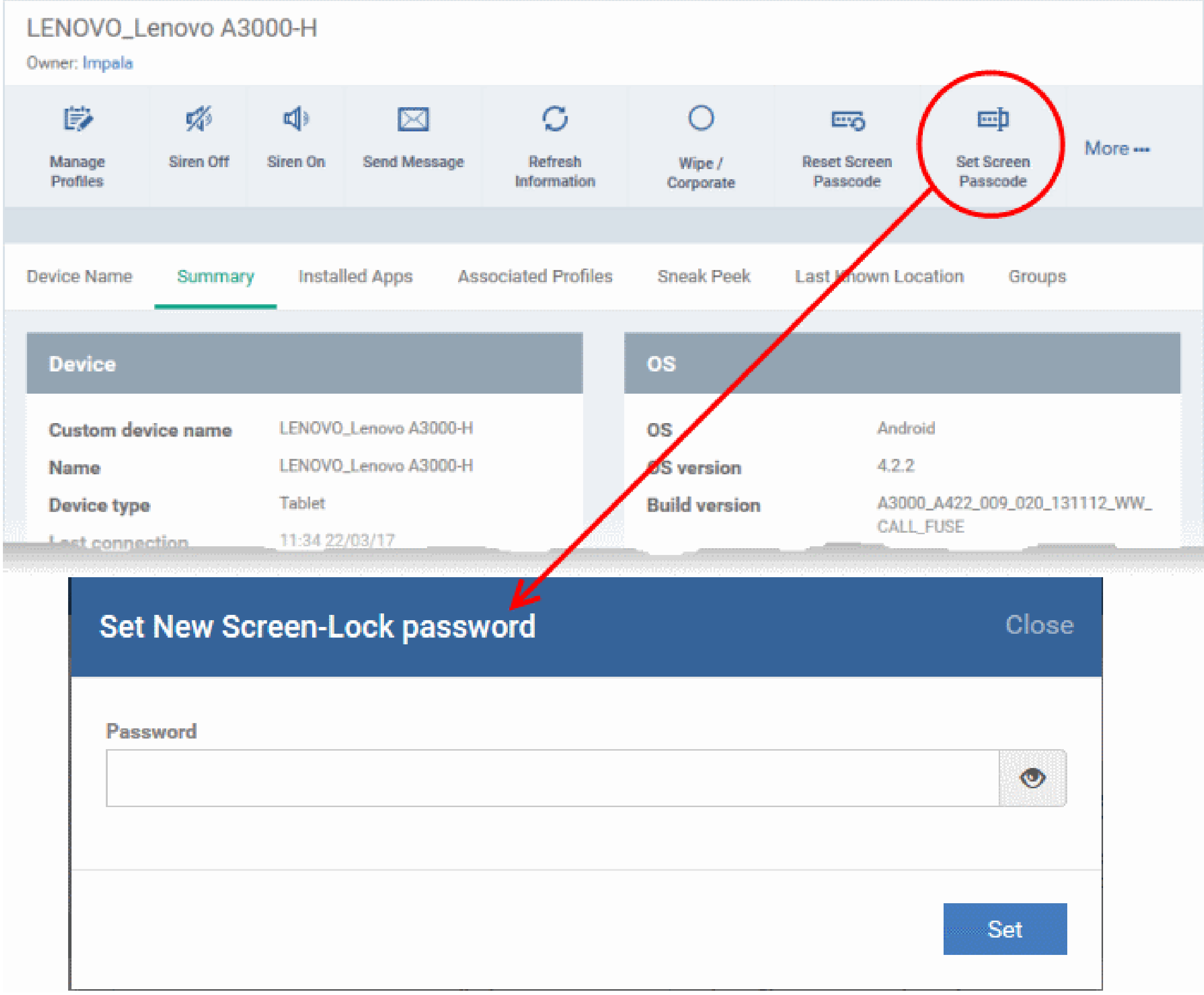
- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select the Company and choose the group under it to view the list of devices in that group

    Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Click 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 drop-down


LENOVO_Lenovo A3000-H

Owner: Impala

Device

Custom device name: LENOVO_Lenovo A3000-H
Name: LENOVO_Lenovo A3000-H
Device type: Tablet
Last connection: 11:34 22/03/17

OS

OS: Android
OS version: 4.2.2
Build version: A3000_A422_009_020_131112_WW_CALL_FUSE

Set New Screen-Lock password

Password

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.

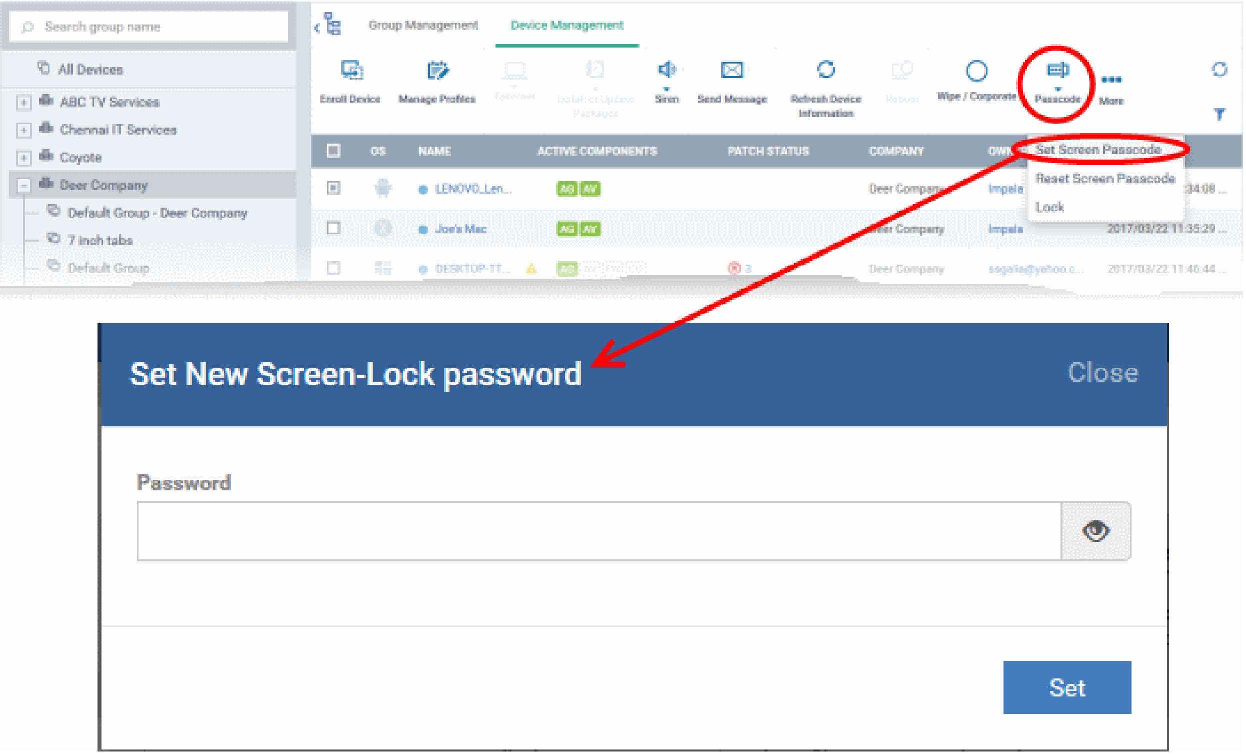
The command will be sent to the device and the current screen lock password will be cleared. A message will also be sent to the device regarding the password change. If a password profile is applied the device, the user will be required to enter a new password that complies with the profile.

To set a new screen lock password or remove password for several devices

- Click the 'Devices' link on the left then choose 'Device List'

- Click the 'Device Management' tab at the top of the main configuration pane
    - Select the Company and choose the group under it to view the list of devices in that group

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices to set/reset password.
- To set a new password, choose 'Passcode' from the options at the top or click 'More...' and select 'Passcode' from the drop-down
- Choose 'Set Screen Passcode' from the options



□	OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWN	
▣		LENOVO_Len...	AG AV		Deer Compan	Impala	34:08 ...
□		Joe's Mac	AG AV		er Company	Impala	2017/03/22 11:35:29 ...
□		DESKTOP-TT... ⚠	AG	3	Deer Company	sagalia@yahoo.c...	2017/03/22 11:46:44 ...

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 and choose 'Passcode' from the options at the top or click 'More...' and select 'Passcode' from the options.
    - 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.

5.2.16. Update 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 Management' interface.

The following sections explain more about:

- **Getting updated information from a single device**
- **Getting updated information from several devices at once**

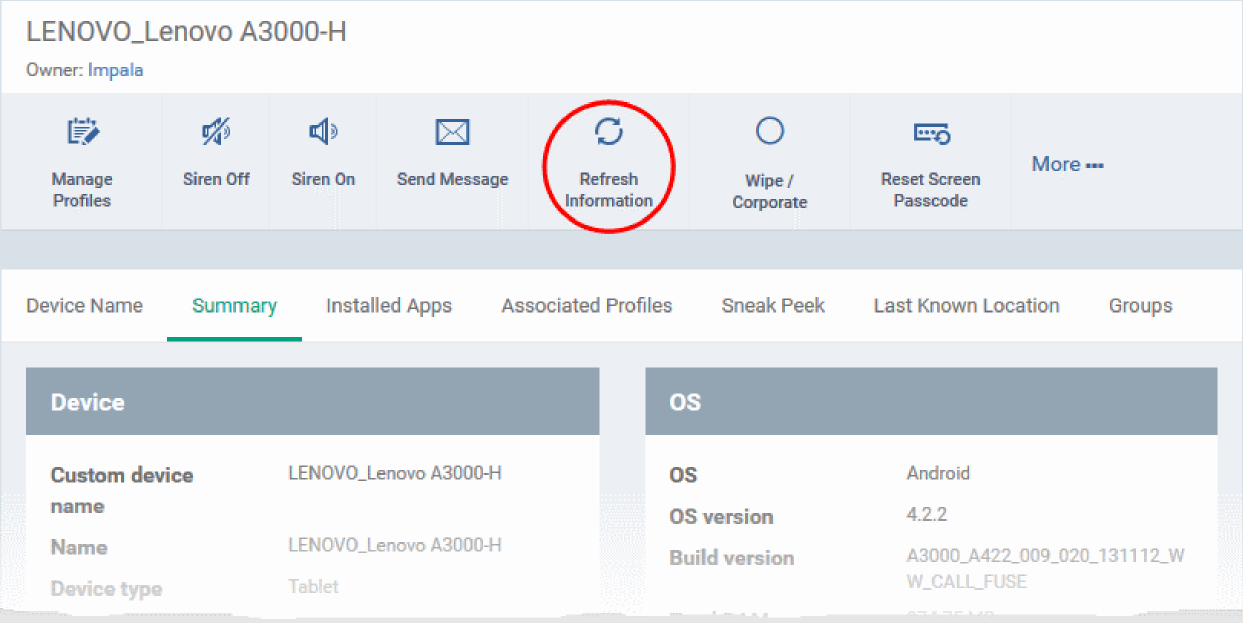
To get updated information from a single device

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the device to refresh the information from

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



LENOVO_Lenovo A3000-H

Owner: Impala

Device

Custom device name	LENOVO_Lenovo A3000-H
Name	LENOVO_Lenovo A3000-H
Device type	Tablet

OS

OS	Android
OS version	4.2.2
Build version	A3000_A422_009_020_131112_WW_CALL_FUSE

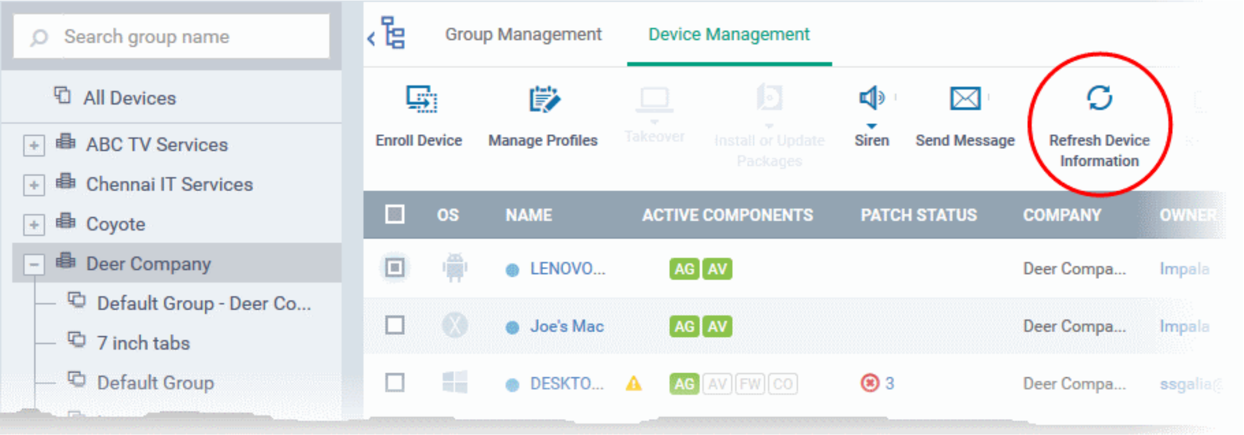
To get updated information from several devices

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

    Or

- Select 'All Devices' to view every device enrolled to ITSM

- Select the 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.



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER
	LENOVO...	AG AV		Deer Compa...	Impala
	Joe's Mac	AG AV		Deer Compa...	Impala
	DESKTO...	AG AV FW CO	3	Deer Compa...	ssgalia(

5.2.17. Send 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

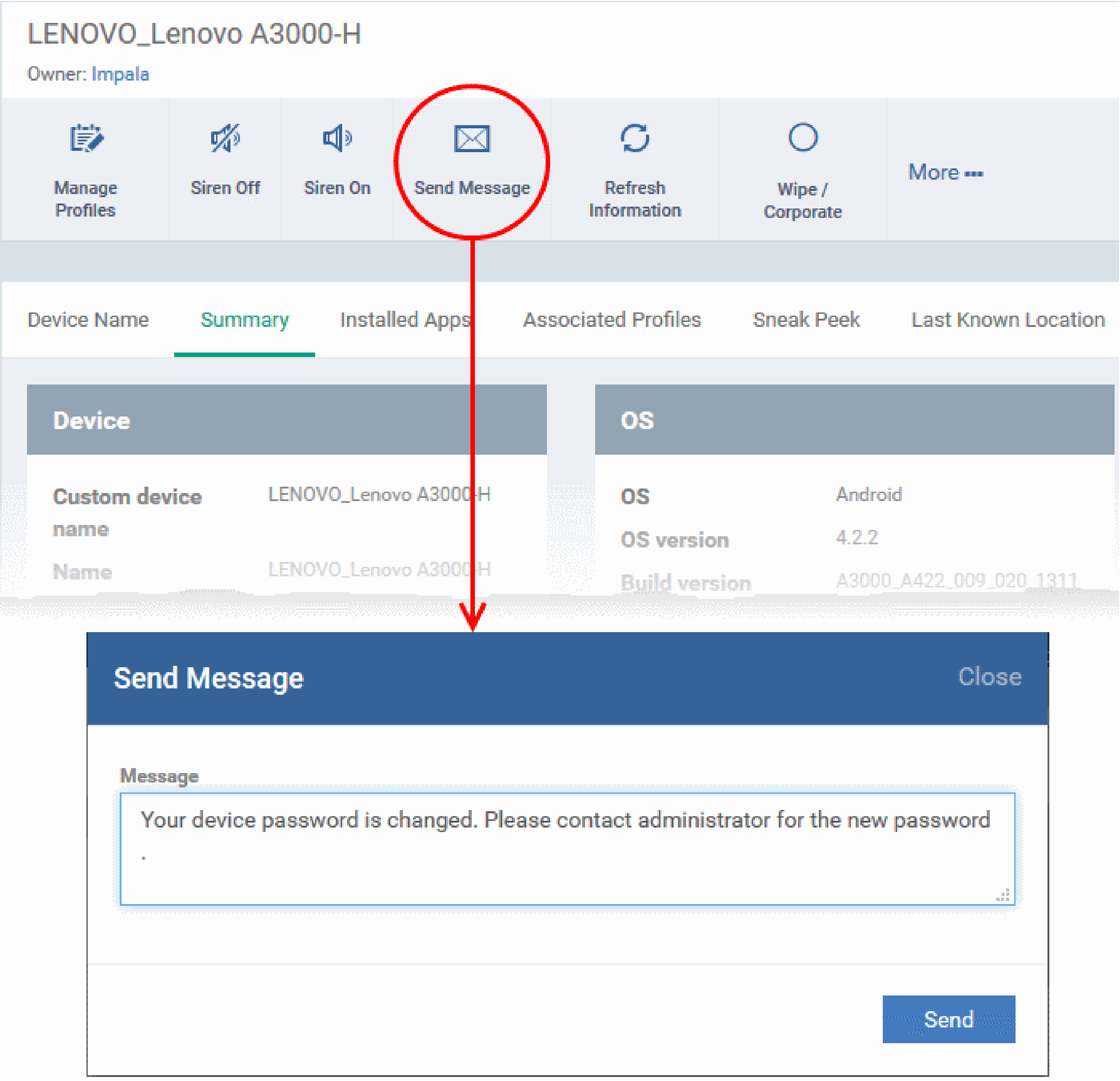
- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select the Company and choose the group under it to view the list of devices in that group

  Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the device to which a message should be sent

The 'Device Details' interface will open.

- Click 'Send Message' from the options at the top.



Message

Your device password is changed. Please contact administrator for the new password .

The 'Send Message' dialog will open.

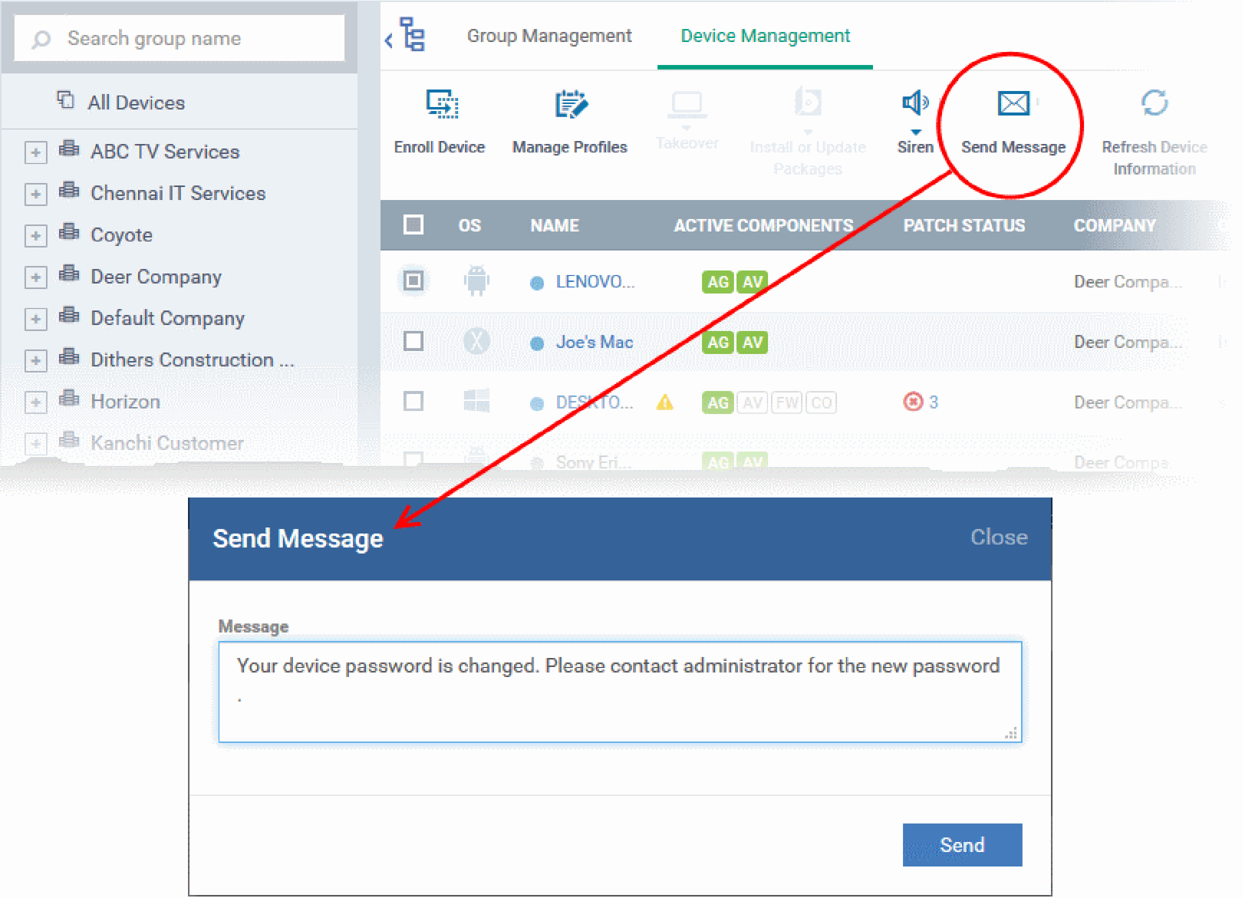
- Enter the text message in the 'Message' field.
- Click on the 'Send' button.

The message will be sent to the device for the user's attention.

To send a text message to several devices at-once

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

  Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices to which you wish to send messages
- Click 'Send Message' from the options at the top or click 'More...' and choose 'Send Message' from the drop-down



Send Message

Message

Your device password is changed. Please contact administrator for the new password .

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.

5.2.18. Restart 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

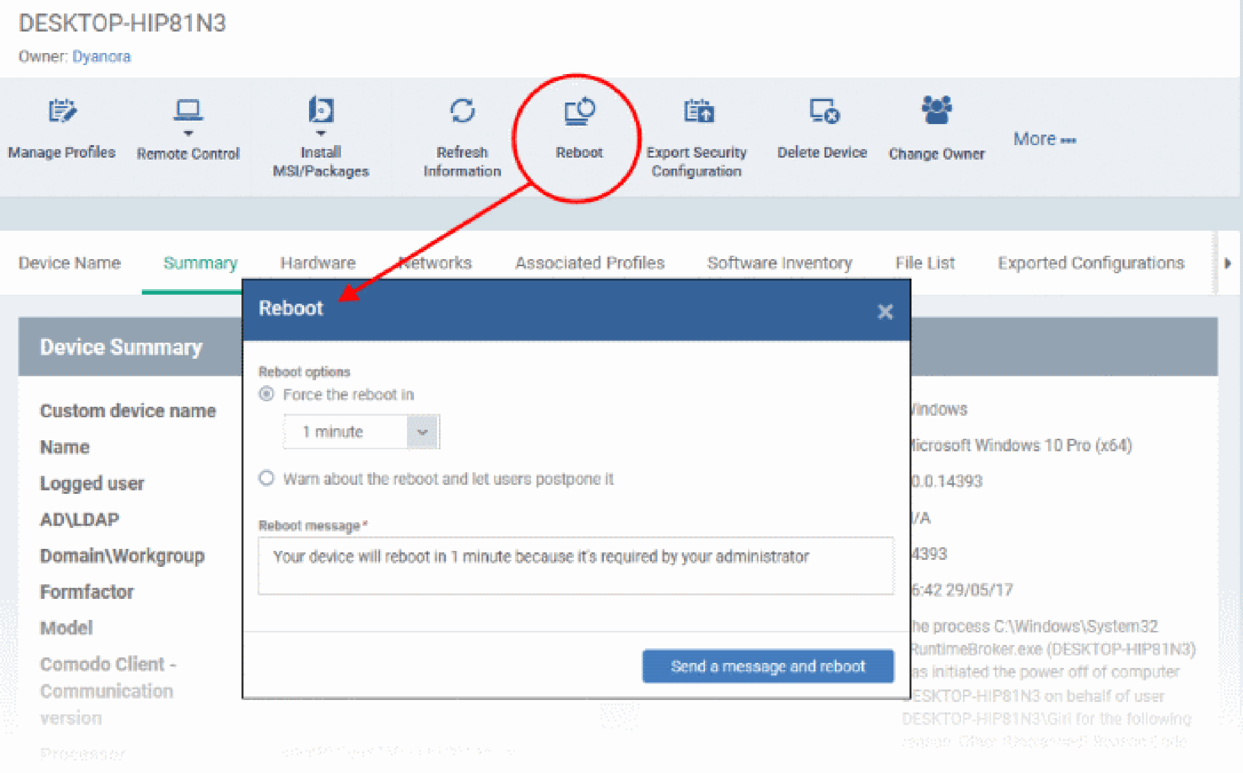
- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
    - Select the Company and choose the group under it to view the list of devices in that group

    Or

    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of the Windows device to be restarted

The device details interface will open.

- Click the 'Reboot' option at the top.



Reboot

Reboot options

● Force the reboot in

1 minute

○ Warn about the reboot and let users postpone it

Reboot message *

Your device will reboot in 1 minute because it's required by your administrator

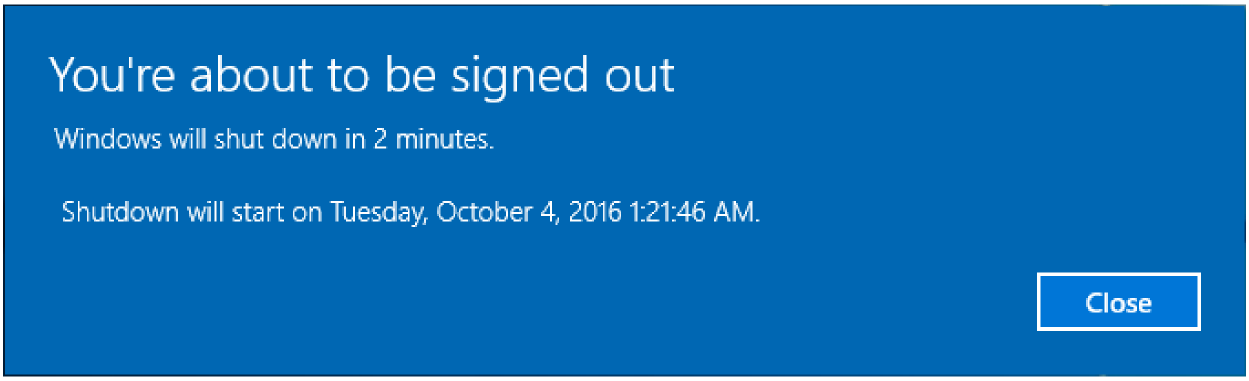
Send a message and reboot

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:



You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

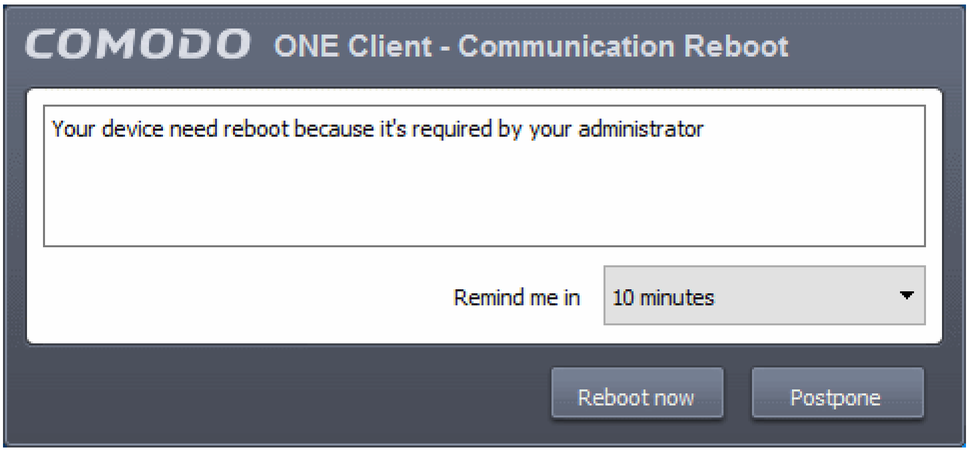
Close

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:



Your device need reboot because it's required by your administrator

Remind me in: 10 minutes

- 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'.

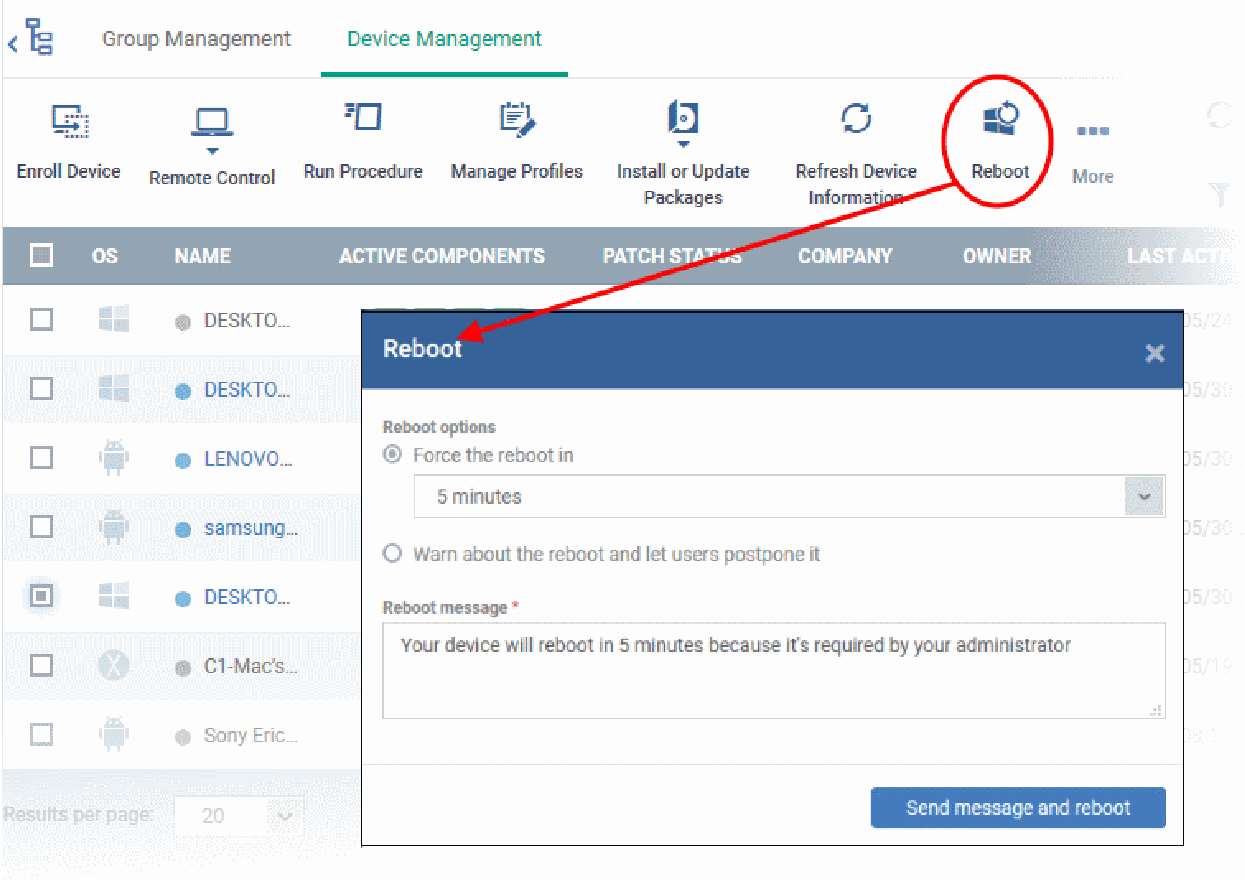
To restart several devices at once

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

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Select the Windows 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



Reboot

Reboot options

● Force the reboot in

5 minutes

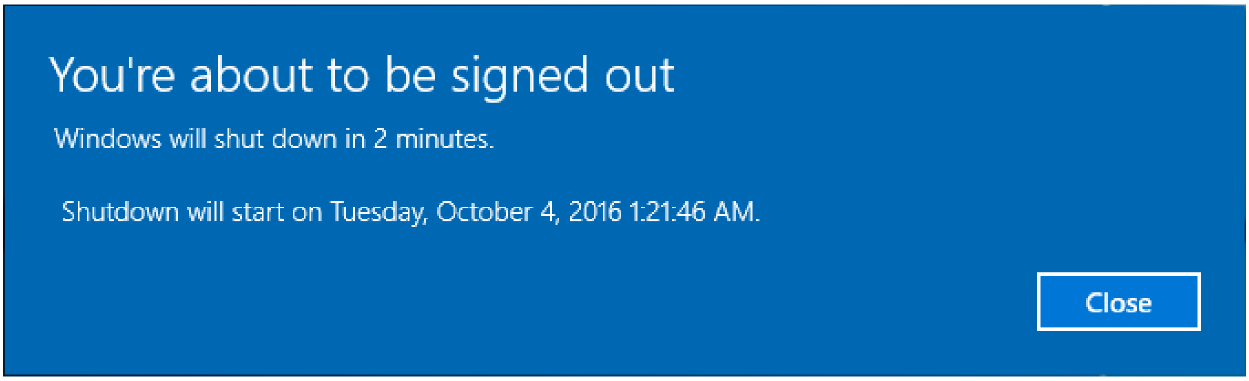
○ Warn about the reboot and let users postpone it

Reboot message *

Your device will reboot in 5 minutes because it's required by your administrator

- 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:



You're about to be signed out

Windows will shut down in 2 minutes.

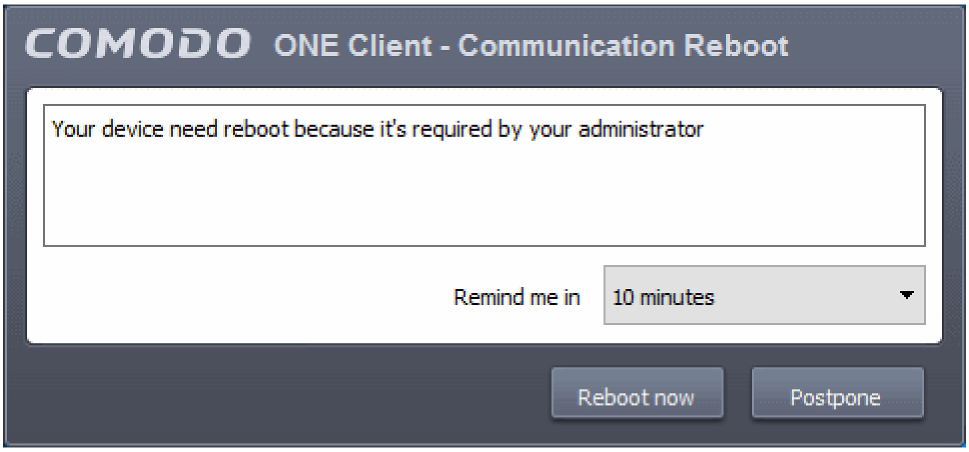
Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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:



COMODO ONE Client - Communication Reboot

Your device need reboot because it's required by your administrator

Remind me in: 10 minutes

- 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'.

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

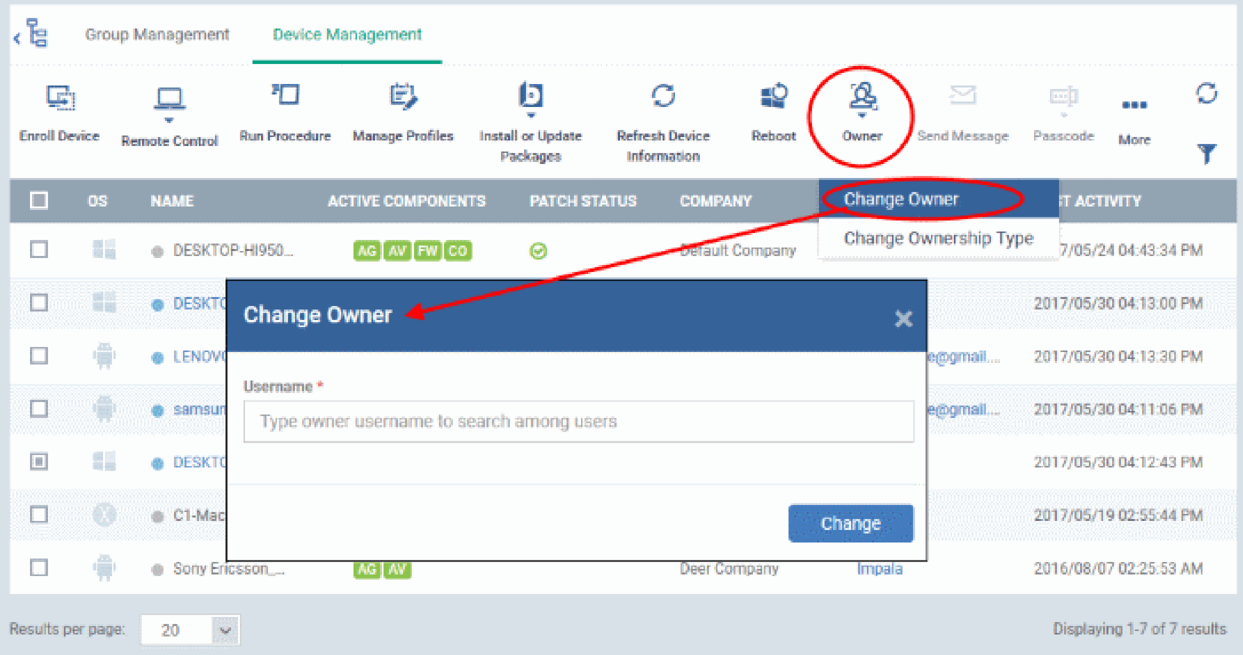
Or

- Select 'All Devices' to view every device enrolled to ITSM

- 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

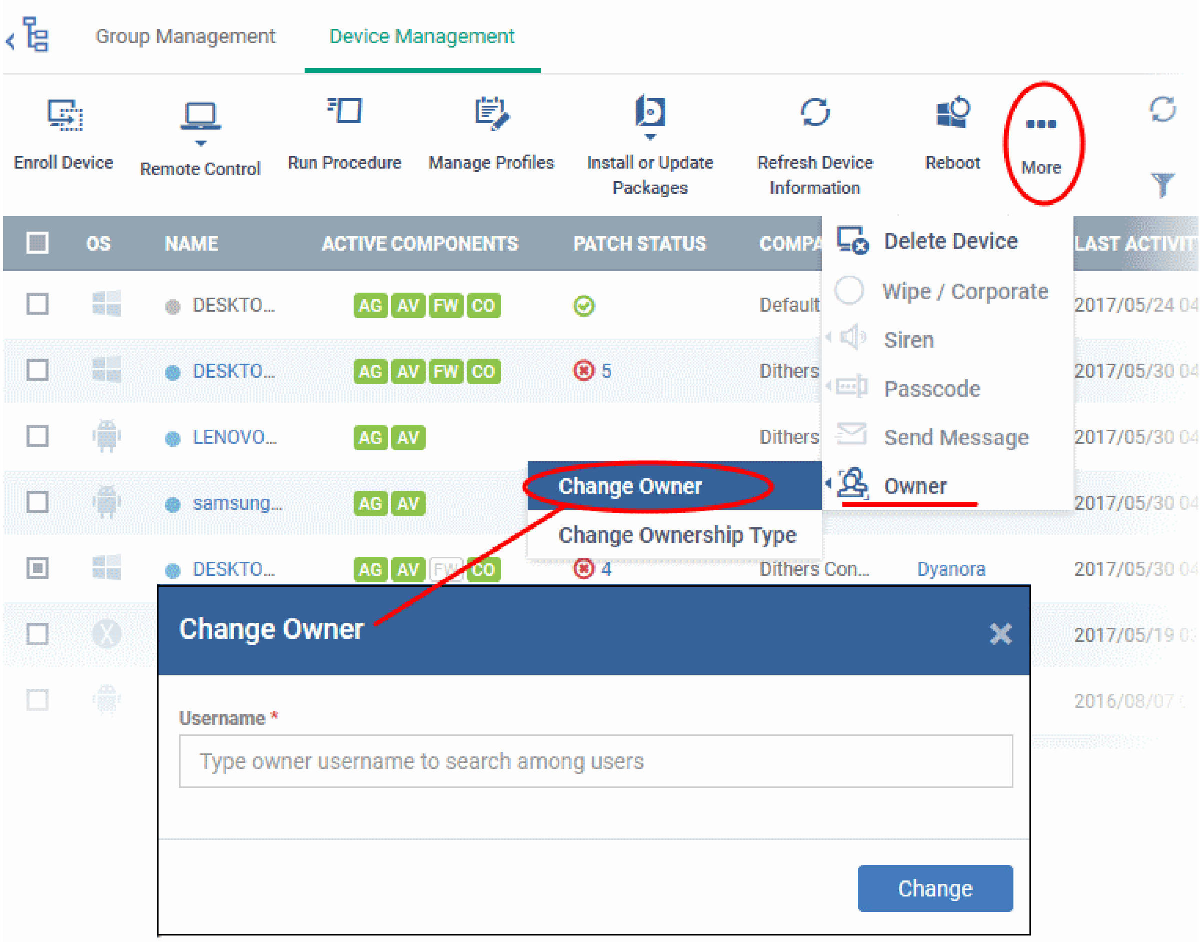
- Click the 'Devices' link on the left then choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select the Company and choose the group under it to view the list of devices in that group

  Or

  - Select 'All Devices' to view every device enrolled to ITSM
- Select the 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 'Owner' from the options at the top or click 'More' and choose 'Owner' from the drop-down
- Select '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.

5.2.20. Change the Ownership Status of a Device

- Administrators can set the ownership status of a device depending on whether it belongs to a user or to the company.
- There are three ownership types - 'Personal', 'Corporate' and 'Not Specified'. The ownership type is listed in the 'Summary' tab of the device configuration area.
- By default, any new device enrolled to ITSM will have an ownership status of 'Not Specified'.
- Ownership types do not have any impact on device security policy or how the device is treated by ITSM. It is a just a descriptive label which allows admins to more easily identify and group devices.

The following sections explain more about:

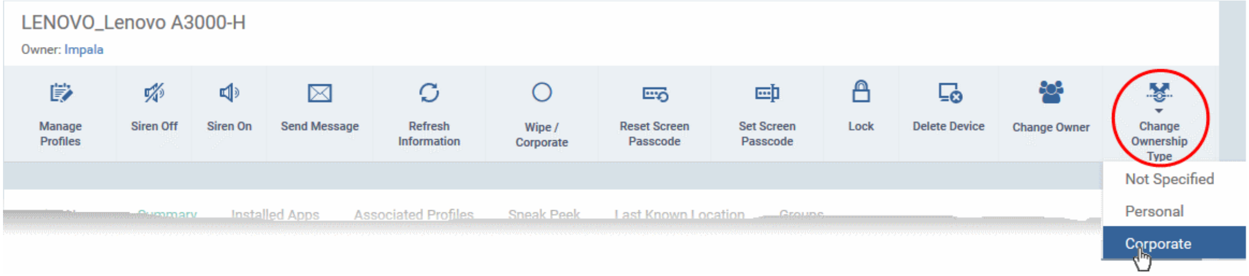
- **Changing ownership status of a single device**
- **Changing ownership status of several devices at-once**

To set the ownership status of a single device

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click the name of a device whose ownership status you wish to change.

The device details interface will open.



LENOVO_Lenovo A3000-H

Owner: Impala

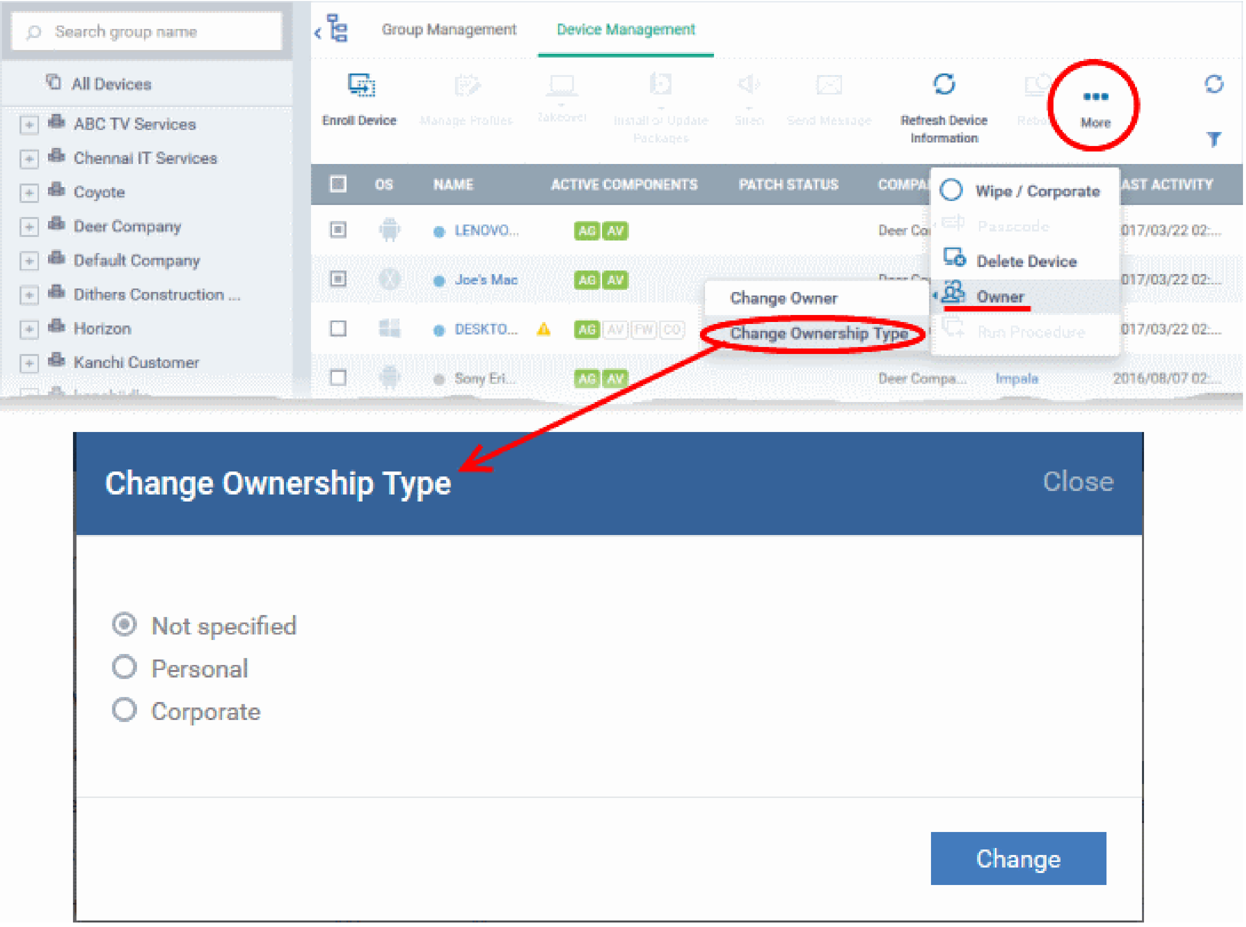
- Click 'Change Ownership Type' from the options at the top and choose from the following options:
    - Personal
    - Corporate
    - Not Specified

To set the ownership status of several devices at-once

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

      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Select the devices whose ownership status you wish to change.
- Click 'Owner' from the options at the top or click 'More...' and choose 'Owner' from the drop-down
- Select 'Change Ownership Type' from the options

The 'Change Ownership Type' dialog will appear:



Change Ownership Type Close

● Not specified
○ Personal
○ Corporate

Change

- Choose the ownership type to be assigned to the selected devices and click 'Change'. The available options are:
    - Personal
    - Corporate
    - Not Specified

5.3. Bulk Enrollment of Devices

- The 'Bulk Enrollment Package' interface allows you to:
    - Download the agent which lets you bulk-enroll Windows and Mac devices from Active Directory. You can also manually install the agent on devices if you wish to enroll them offline.
    - Download the Comodo Remote Control (CRC) tool for remote desktop management of Windows and Mac OS devices For help to download and install the CRC tool, see **Download Remote Control Tool**.
- Click 'Devices' on the left then choose 'Bulk Enrollment Package'

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**.

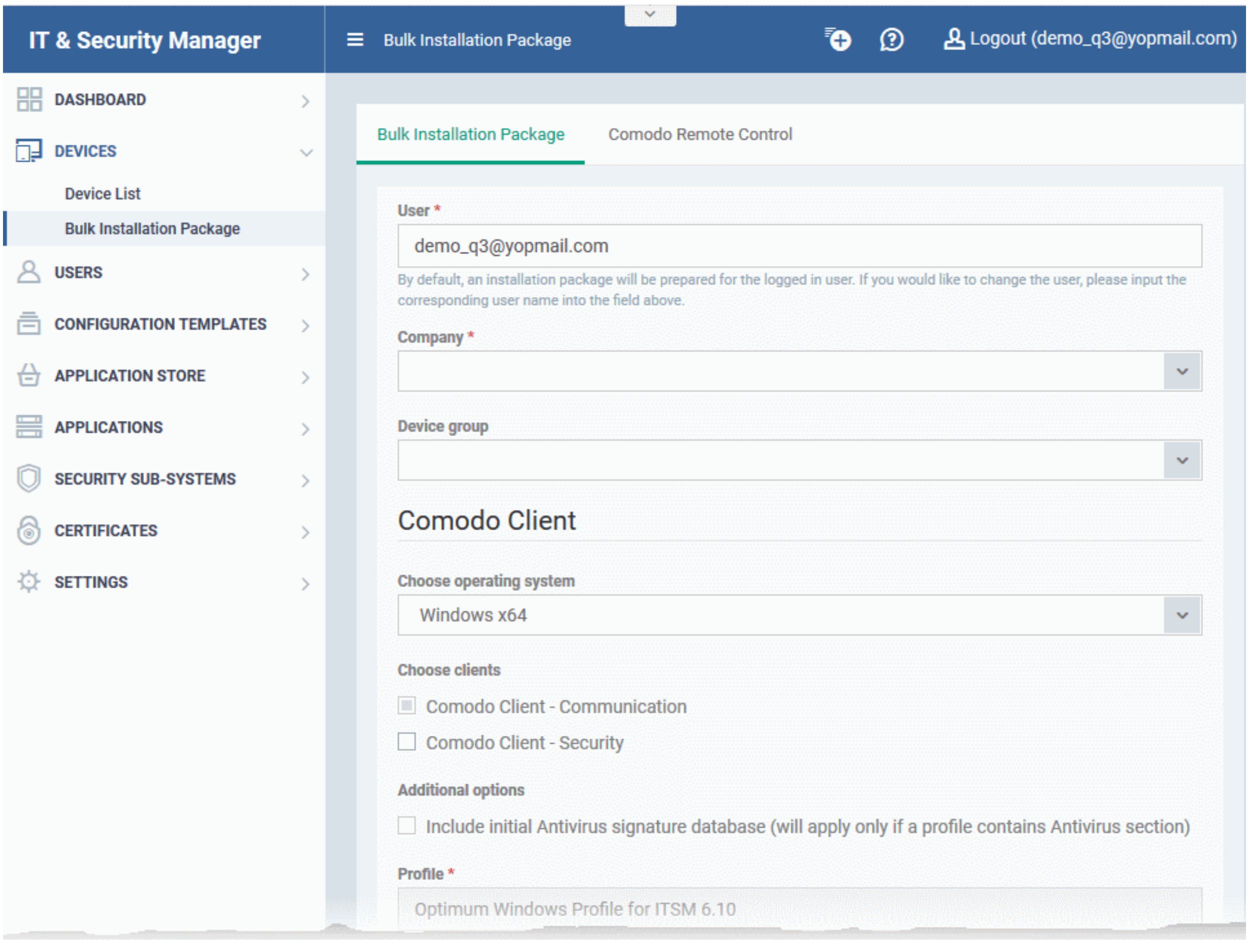
5.3.1. Enroll Windows and Mac OS Devices by Installing the ITSM Agent Package

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. See **Enrolling Windows Endpoints** and **Enrolling Mac OS Endpoints** for more details
- Administrators can manually enroll devices by downloading the installation package from ITSM and installing it on a target device.
- 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.
- Alternatively, admins can bulk enroll devices using the 'Comodo Auto Discovery and Deployment Tool'. Click 'Tools' in the Comodo One file-menu to access and download the tool. See **Enroll Windows Devices using Comodo Auto Discovery and Deployment Tool** for help to configure the too.

The 'Bulk Installation Package' interface allows you 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.

- Click 'Devices' on the left then select 'Bulk Installation Package'.
- Select the 'Bulk Installation Package' tab.



User *

demo_q3@yopmail.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 *

Device group

Comodo Client

Choose operating system

Windows x64

Choose clients

☑ 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 6.10

You can download MSI/MST packages for deployment via AD server and a .EXE package for offline installation to individual endpoints. See 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

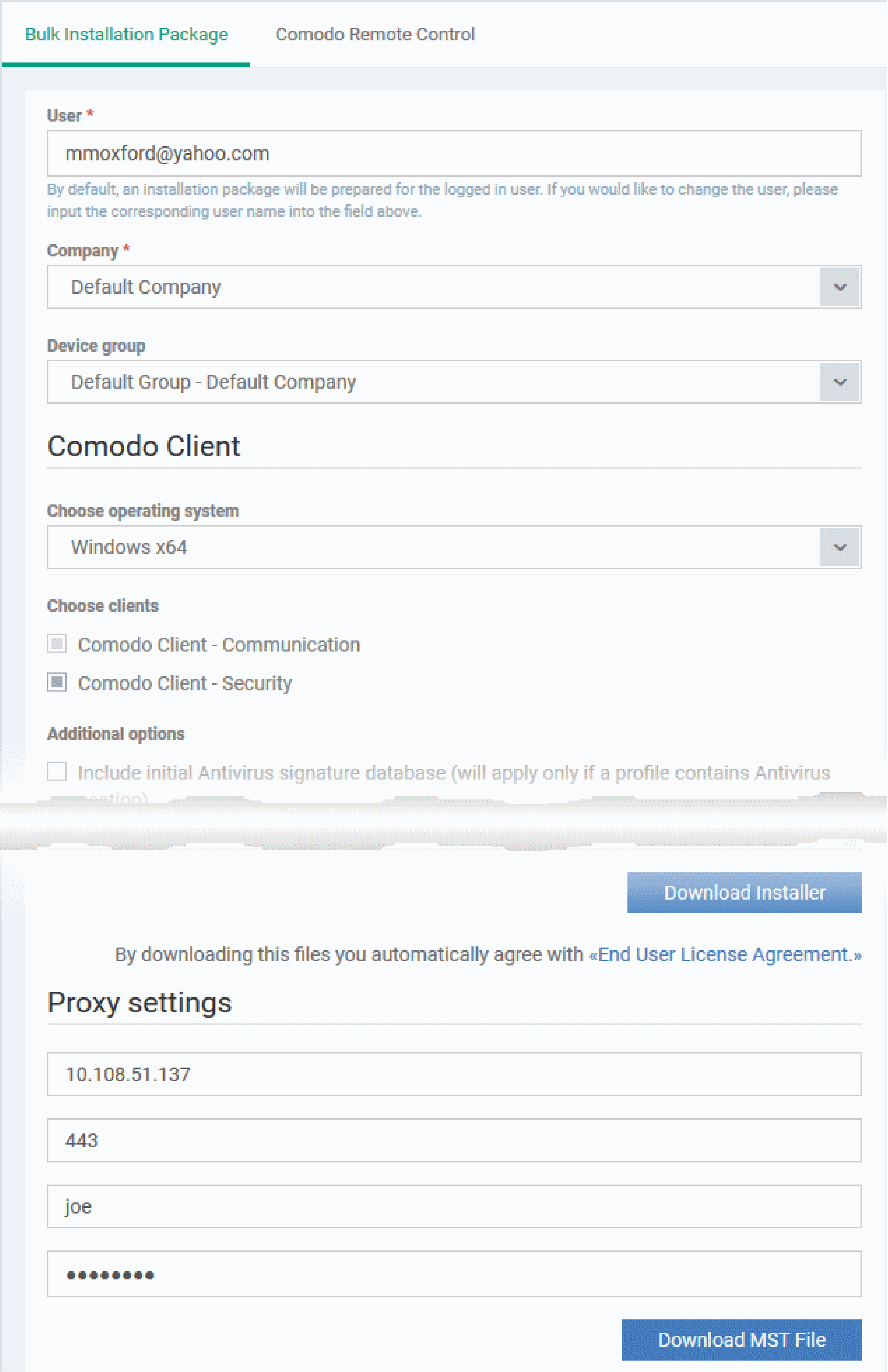
5.3.1.1. Enroll Windows Devices Via AD Group Policy

- Enrollment via Active Directory (AD) group policy lets you add devices in bulk
- You need to download and install the ITSM agent package and, if required, the transformed MST installation file. You then need to add these items to the GPO.
- The MST file includes details of the proxy that the 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. See Changing a Device's Owner for more details.

Note: The AD method only allows you to install ITSM agent (CCC) on target endpoints. You can remotely install the endpoint security software, Comodo Client - Security (CCS), at a later time from the ITSM interface. See Remotely Installing Packages onto Windows Devices for more details.

To download the installation package

- Click 'Devices' on the left then choose 'Bulk Installation Package'
- Select the 'Bulk Installation Package' tab



User *

mmoxford@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 *

Default Company

Device group

Default Group - Default Company

Comodo Client

Choose operating system

Windows x64

Choose clients

☐ Comodo Client - Communication

☒ Comodo Client - Security

Additional options

☐ Include initial Antivirus signature database (will apply only if a profile contains Antivirus section)

By downloading this files you automatically agree with «End User License Agreement.»

Proxy settings

10.108.51.137

443

joe

••••••••

Bulk Installation 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. See **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

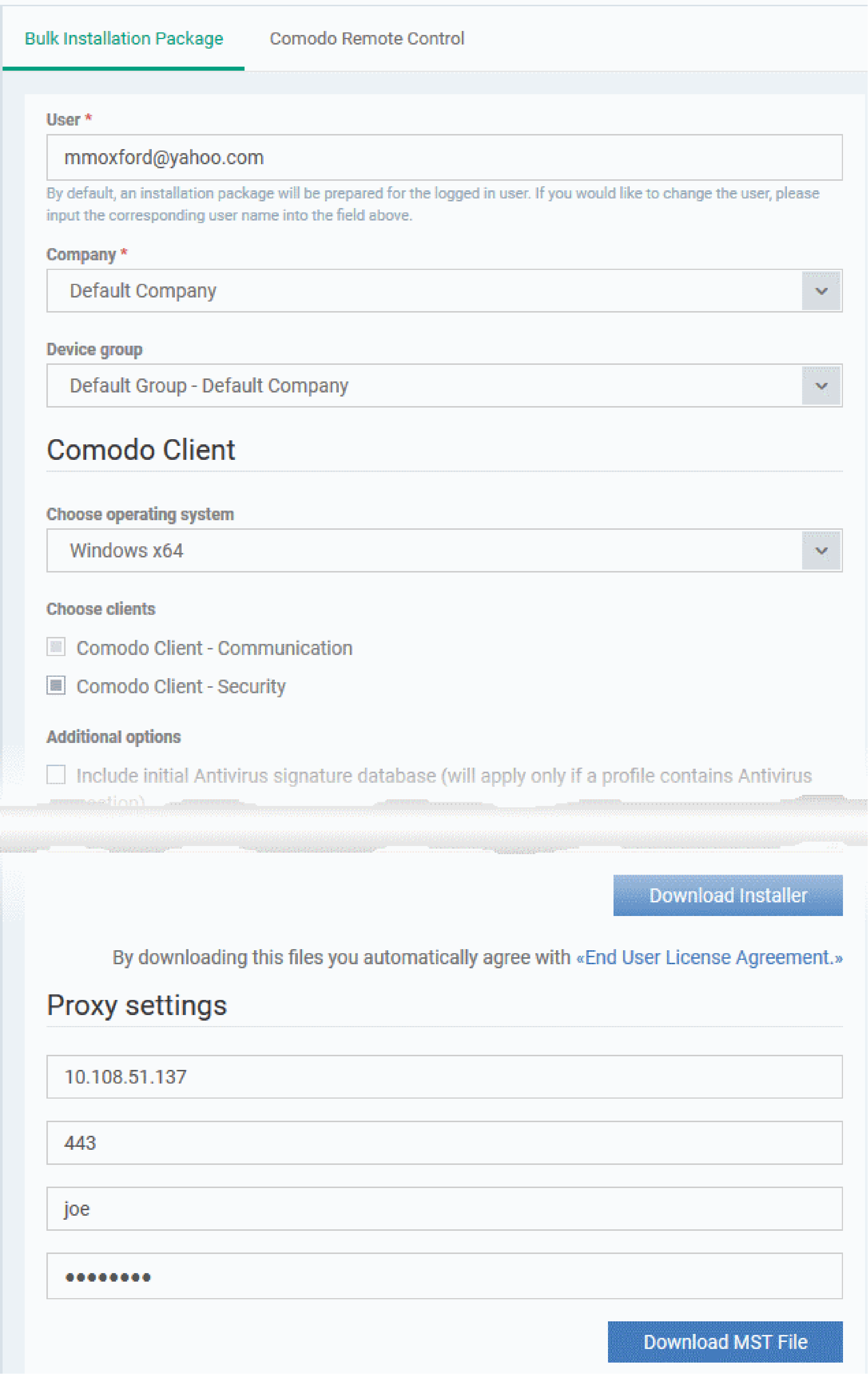
Administrators can download an installation package containing the agent and the Comodo Client - Security (CCS) software for offline installation. This is useful for endpoints which could not be reached by ITSM for auto-installation of the agent during enrollment.

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 then choose 'Bulk Installation Package'
- Select the 'Bulk Installation Package' tab



User *

mmoxford@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 *

Default Company

Device group

Default Group - Default Company

Comodo Client

Choose operating system

Windows x64

Choose clients

☐ Comodo Client - Communication

☒ Comodo Client - Security

Additional options

☐ Include initial Antivirus signature database (will apply only if a profile contains Antivirus section)

By downloading this files you automatically agree with «End User License Agreement.»

Proxy settings

10.108.51.137

443

joe

••••••••

Bulk Installation 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 Devices

ITSM will create a custom installation file in .pkg format for installation on to the user's Mac OS 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 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

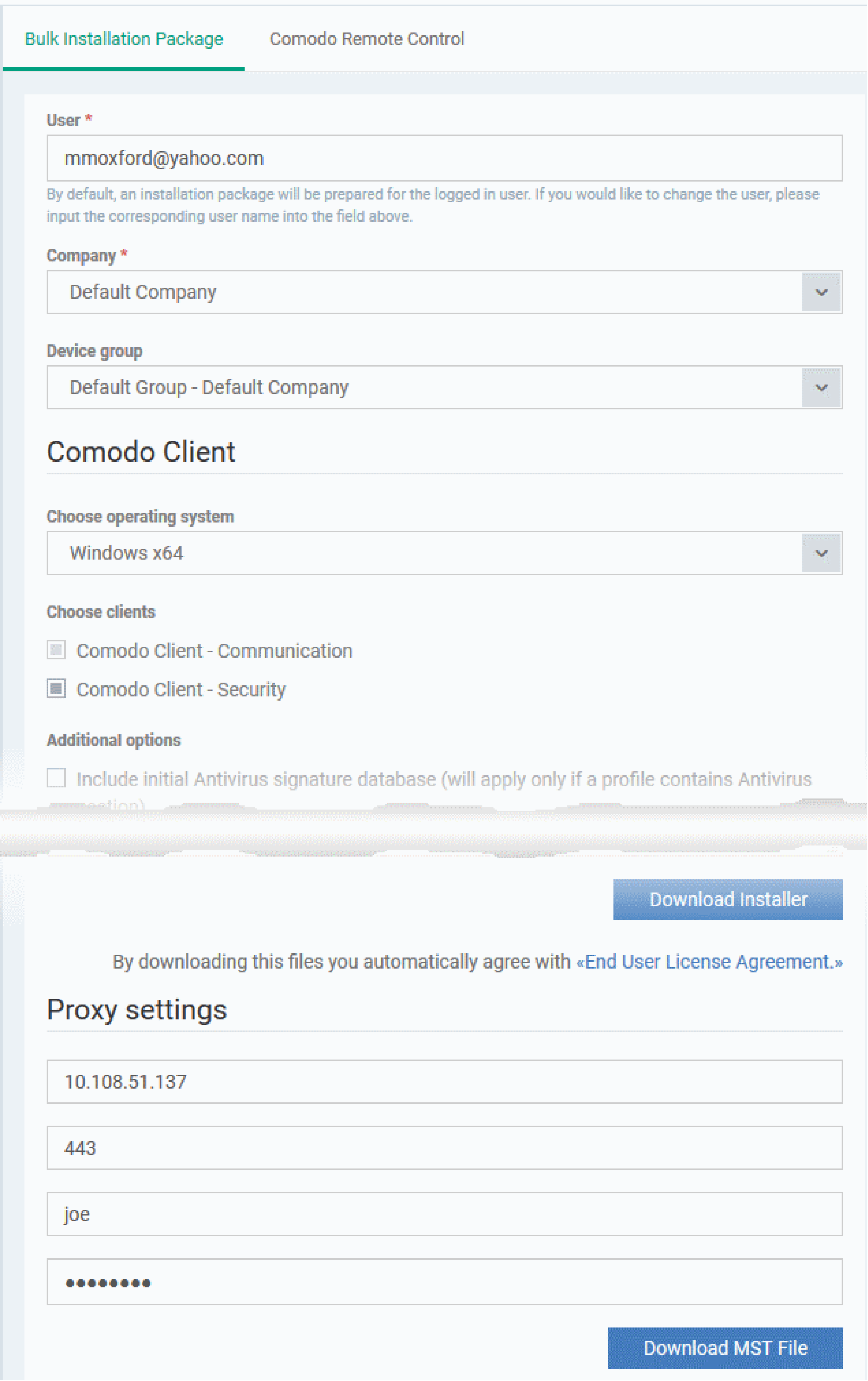
Comodo Auto Discovery and Deployment Tool (CADDT) allows network admins to remotely deploy the ITSM agent and client security application to multiple endpoints. You can install via Active Directory, Workgroup, IP address/range or host-name.

- 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'



User *

mmoxford@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 *

Default Company

Device group

Default Group - Default Company

Comodo Client

Choose operating system

Windows x64

Choose clients

☑ Comodo Client - Communication

☑ Comodo Client - Security

Additional options

□ Include initial Antivirus signature database (will apply only if a profile contains Antivirus section)

By downloading this files you automatically agree with «End User License Agreement.»

Proxy settings

10.108.51.137

443

joe

••••••••

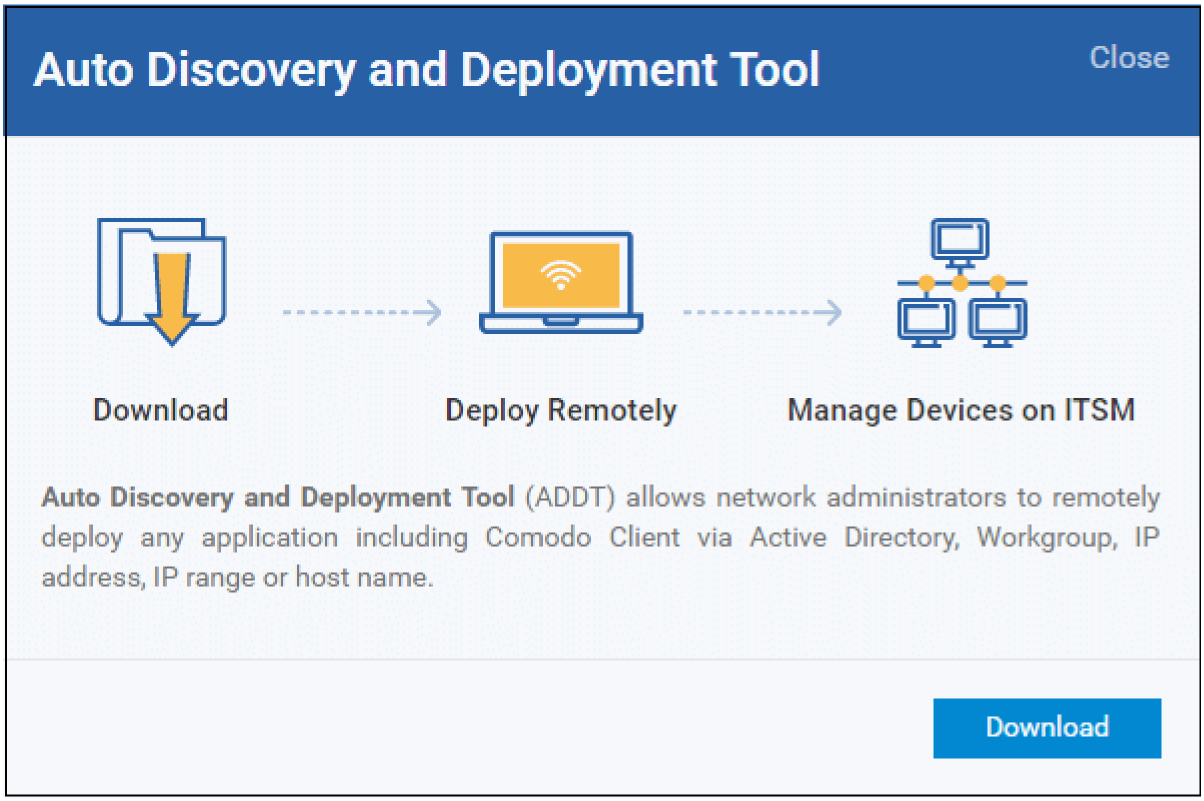
Bulk Installation Package - Form Parameters	
Parameter	**Description**
User	Allows you to specify the user to whom the endpoint(s) should be assigned upon enrollment. By default, the 'User' field is pre-populated with the currently logged-in administrator. • Start typing the first few characters of the 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 Mac OS. • 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):



Auto Discovery and Deployment Tool

Auto Discovery and Deployment Tool (ADDT) allows network administrators to remotely deploy any application including Comodo Client via Active Directory, Workgroup, IP address, IP range or host name.

- 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

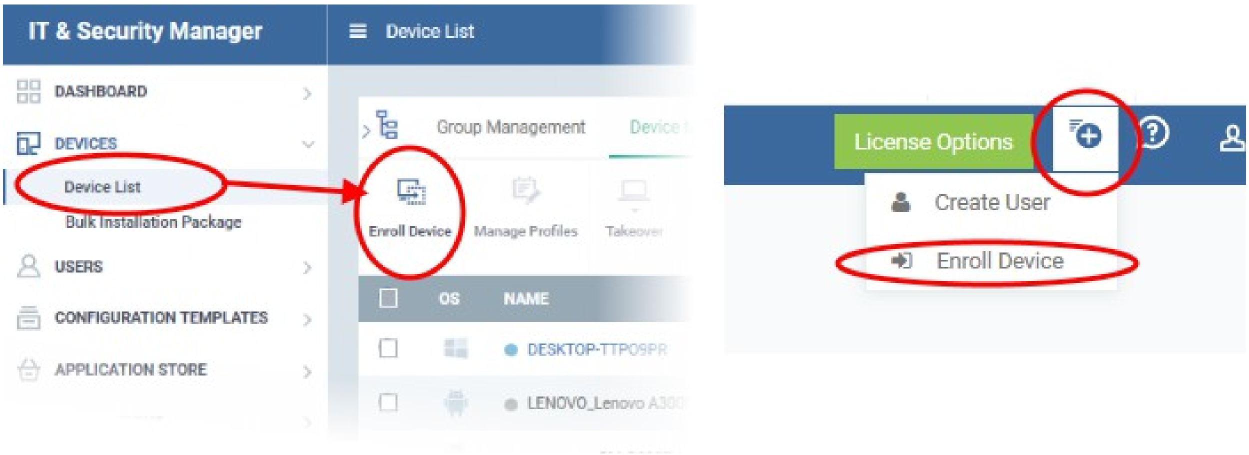
Import iOS devices

To view enrollment instructions

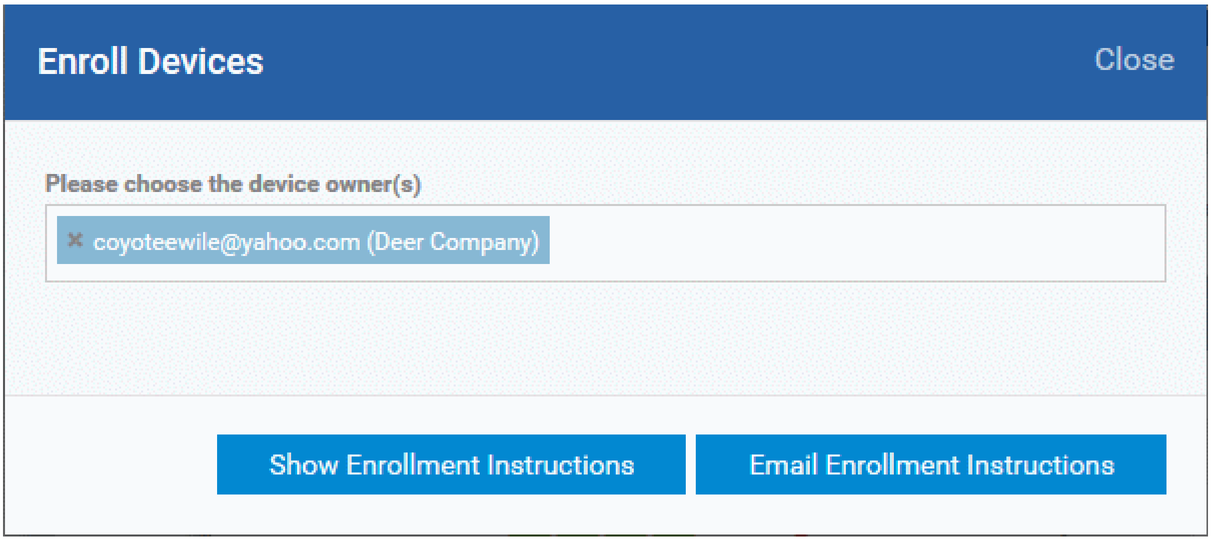
- Click 'Devices' > 'Device List' on the left
- Click the 'Enroll Device' button above the table

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:

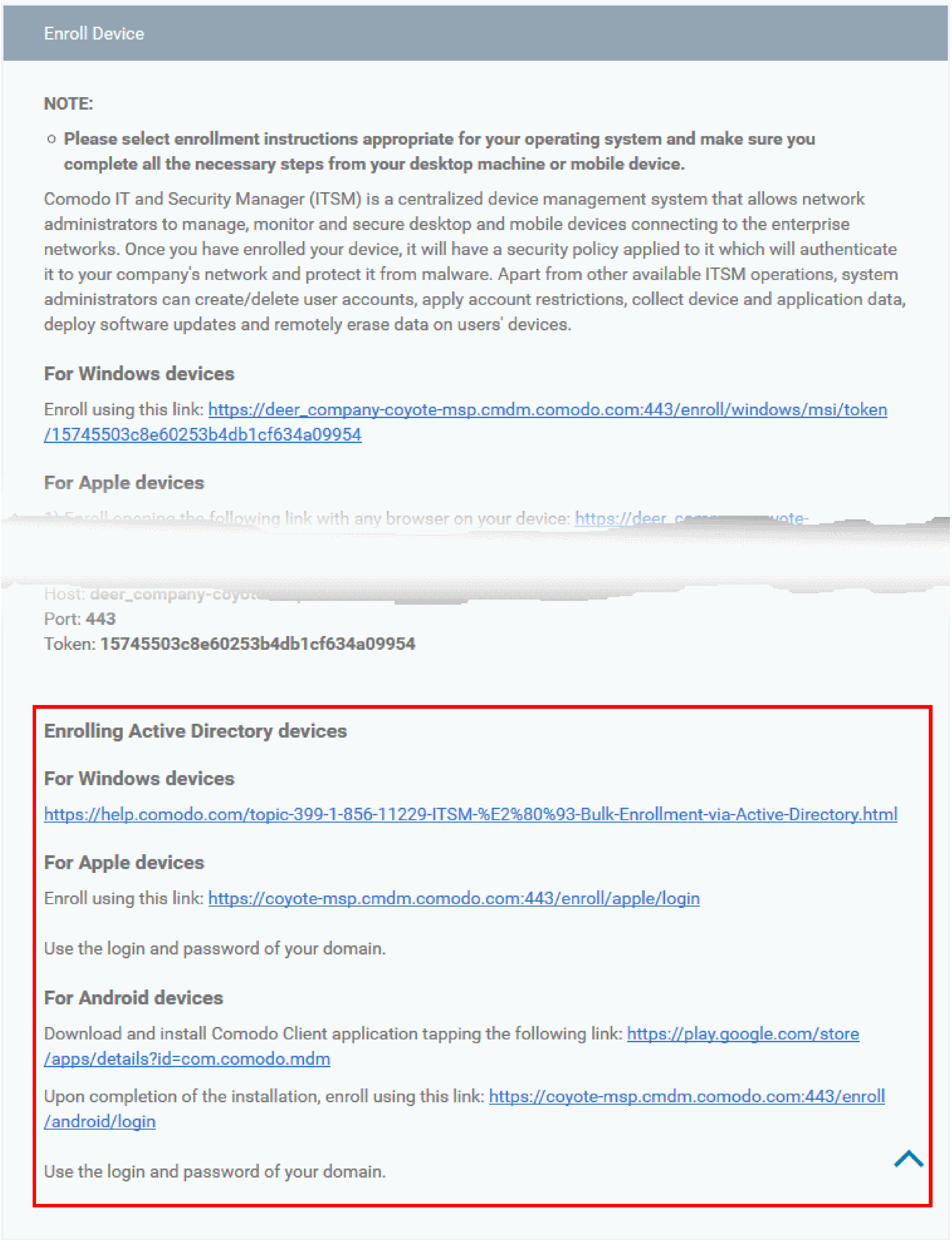


Please choose the device owner(s)

× coyoteewile@yahoo.com (Deer Company)

- Click 'Show Enrollment Instructions'

The 'Enroll Device' page will appear with enrollment instructions for Windows, Mac OS, Android and iOS devices.



Enroll Device

NOTE:

- **Please select enrollment instructions appropriate for your operating system and make sure you complete all the necessary steps from your desktop machine or mobile device.**

Comodo IT and Security Manager (ITSM) is a centralized device management system that allows network administrators to manage, monitor and secure desktop and mobile devices connecting to the enterprise networks. Once you have enrolled your device, it will have a security policy applied to it which will authenticate it to your company's network and protect it from malware. Apart from other available ITSM operations, system administrators can create/delete user accounts, apply account restrictions, collect device and application data, deploy software updates and remotely erase data on users' devices.

For Windows devices

Enroll using this link: https://deer_company-coyote-msp.cmdm.comodo.com:443/enroll/windows/msi/token/15745503c8e60253b4db1cf634a09954

For Apple devices

1) Enroll opening the following link with any browser on your device: https://deer_com ... yote-

Host: **deer_company-coyote**

Port: **443**

Token: **15745503c8e60253b4db1cf634a09954**

Enrolling Active Directory devices

For Windows devices

https://help.comodo.com/topic-399-1-856-11229-ITSM-%E2%80%93-Bulk-Enrollment-via-Active-Directory.html

For Apple devices

Enroll using this link: https://coyote-msp.cmdm.comodo.com:443/enroll/apple/login

Use the login and password of your domain.

For Android devices

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

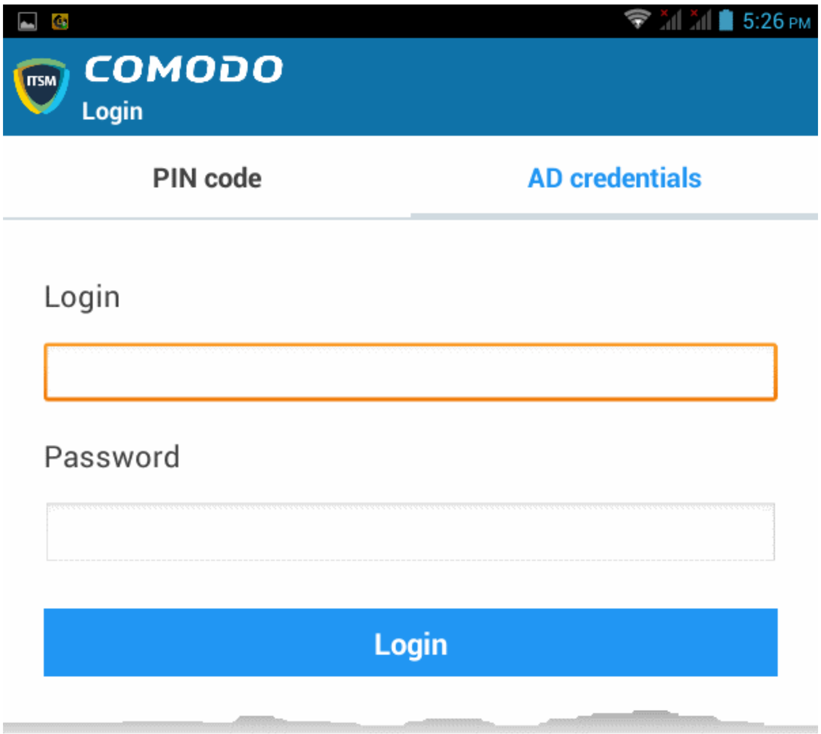
Upon completion of the installation, enroll using this link: https://coyote-msp.cmdm.comodo.com:443/enroll/android/login

Use the login and password of your domain.

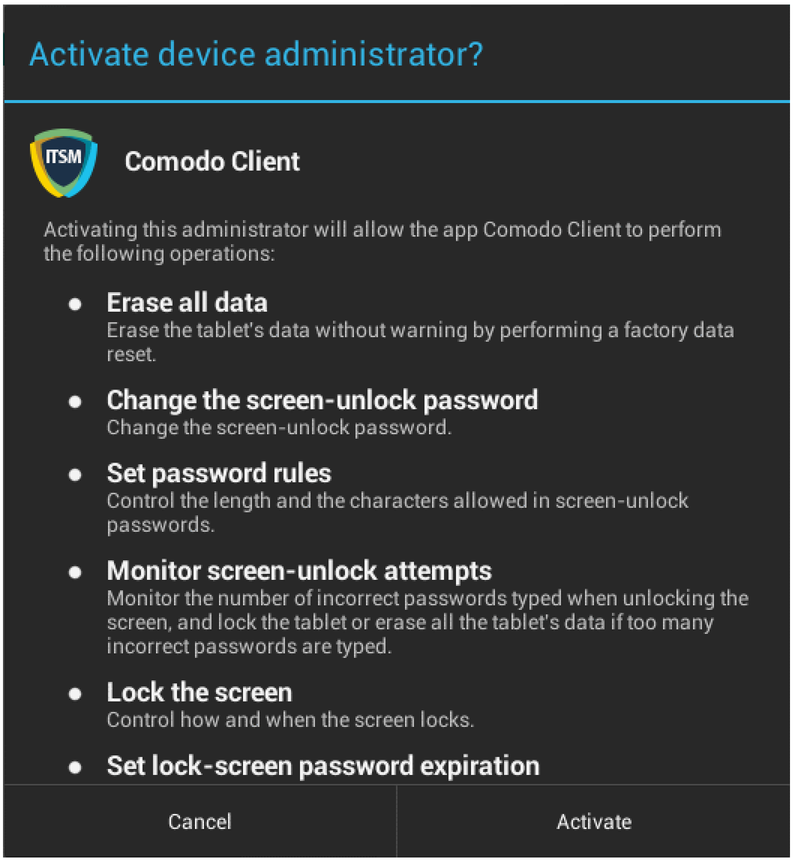
- Scroll down the page to the section 'Enrolling Active Directory devices'
- From this point, see either **Import Android devices** or **Import iOS devices**

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:



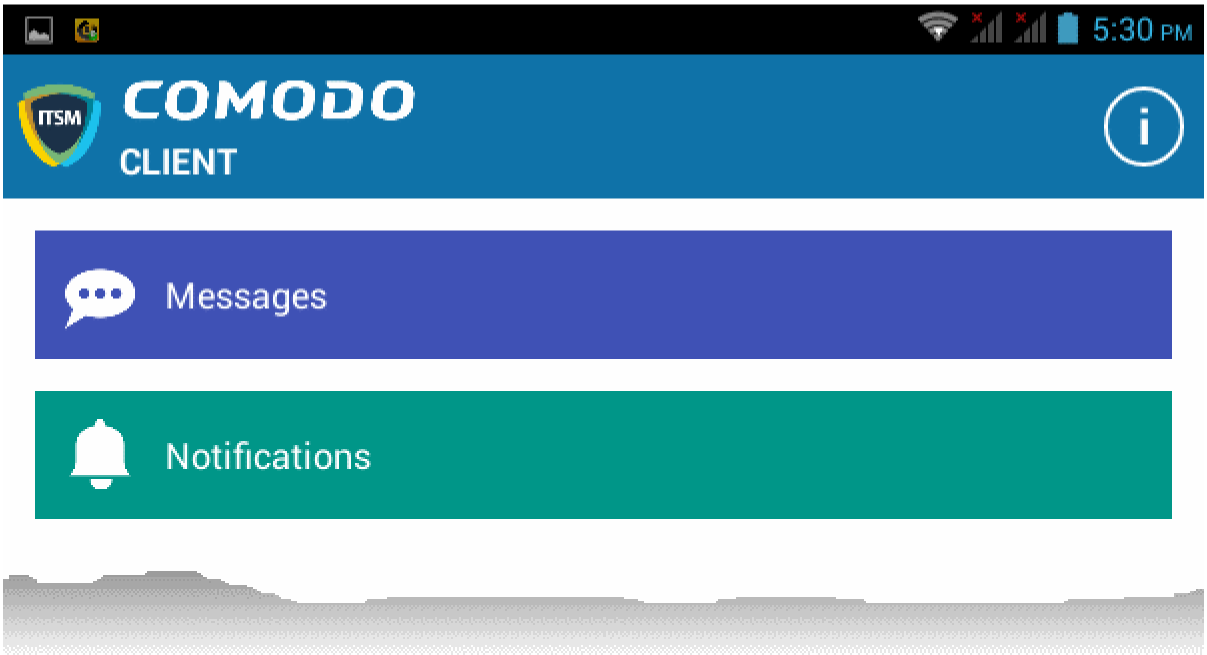
Activate device administrator?

Comodo Client

Activating this administrator will allow the app Comodo Client to perform the following operations:

- **Erase all data**
  Erase the tablet's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set lock-screen password expiration**

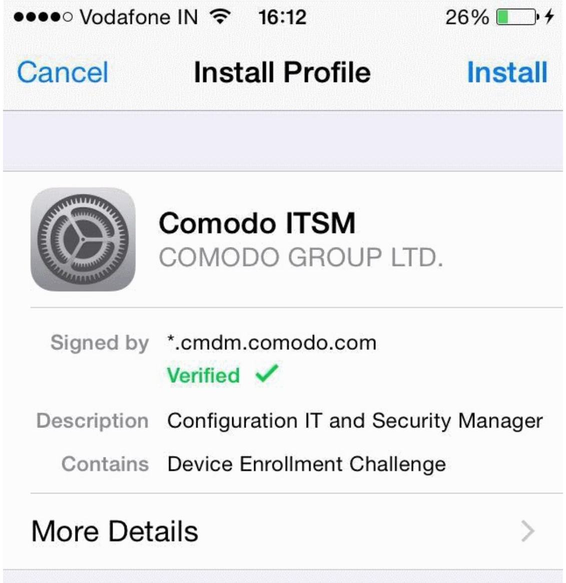
- After activating, the ITSM agent home screen will appear:



- 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.



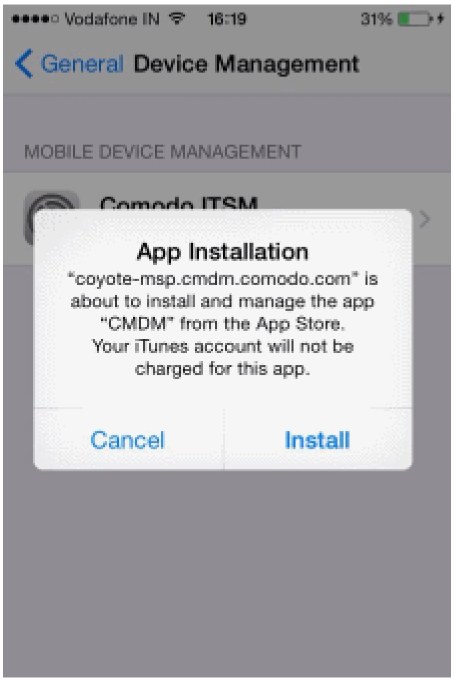
Comodo ITSM
COMODO GROUP LTD.

Signed by *.cmdm.comodo.com
Verified ✓

Description Configuration IT and Security Manager

Contains Device Enrollment Challenge

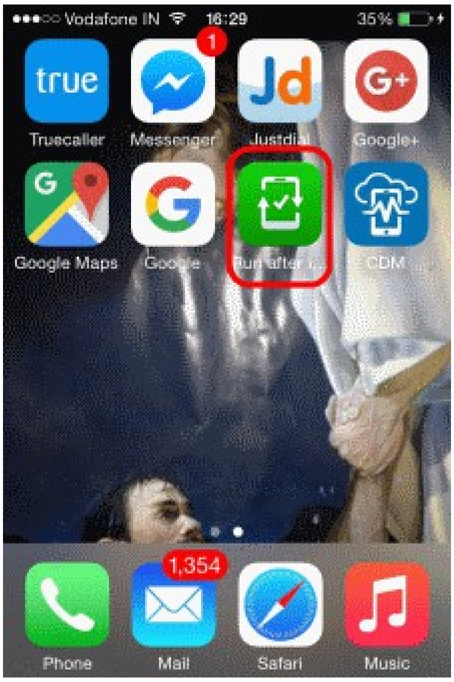
- The user needs to follow the wizard to complete the profile installation.
- After installing the profile, a login page will appear.
- The user needs to enter the username and password they use to log into their domain.
- The device will communicate with ITSM to begin enrollment.
- After the profile 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.



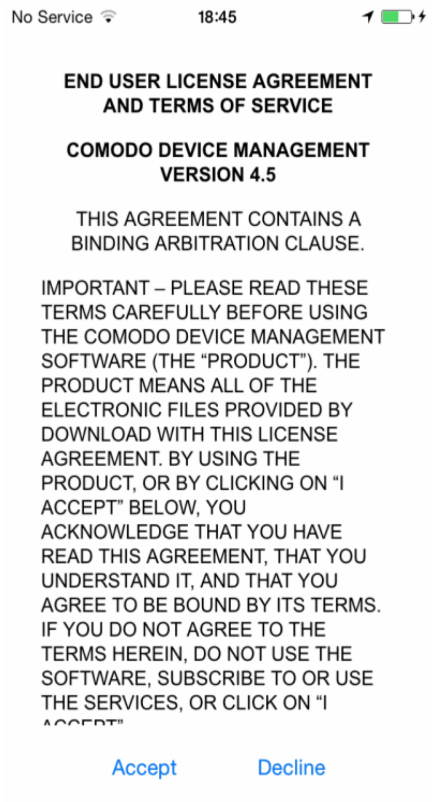
App Installation

"coyote-msp.cmdm.comodo.com" is about to install and manage the app "CMDM" from the App Store. Your iTunes account will not be charged for this app.

- 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:

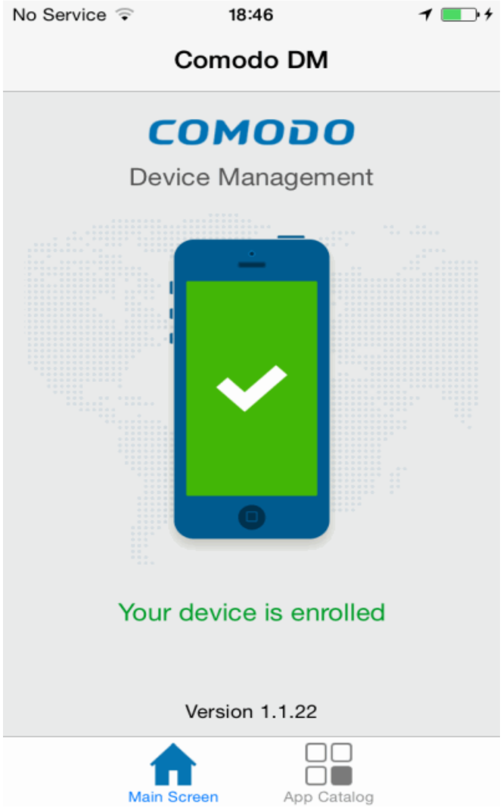


END USER LICENSE AGREEMENT AND TERMS OF SERVICE

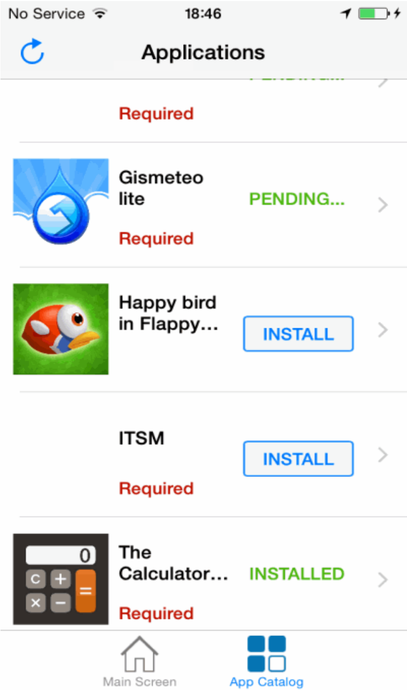
COMODO DEVICE MANAGEMENT VERSION 4.5

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO DEVICE MANAGEMENT SOFTWARE (THE “PRODUCT”). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON “I ACCEPT” BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON “I ACCEPT”



Tapping 'App Catalog' will display apps that are installed, required to be installed and available for installation:



5.3.3. Download and Install the Remote Control Tool

- The Comodo Remote Control (CRC) tool allows admins and staff to remotely take control of managed Windows and Mac OS endpoints.
- This is useful in a number of circumstances, but especially for troubleshooting issues, running system

maintenance tasks and providing training to users.

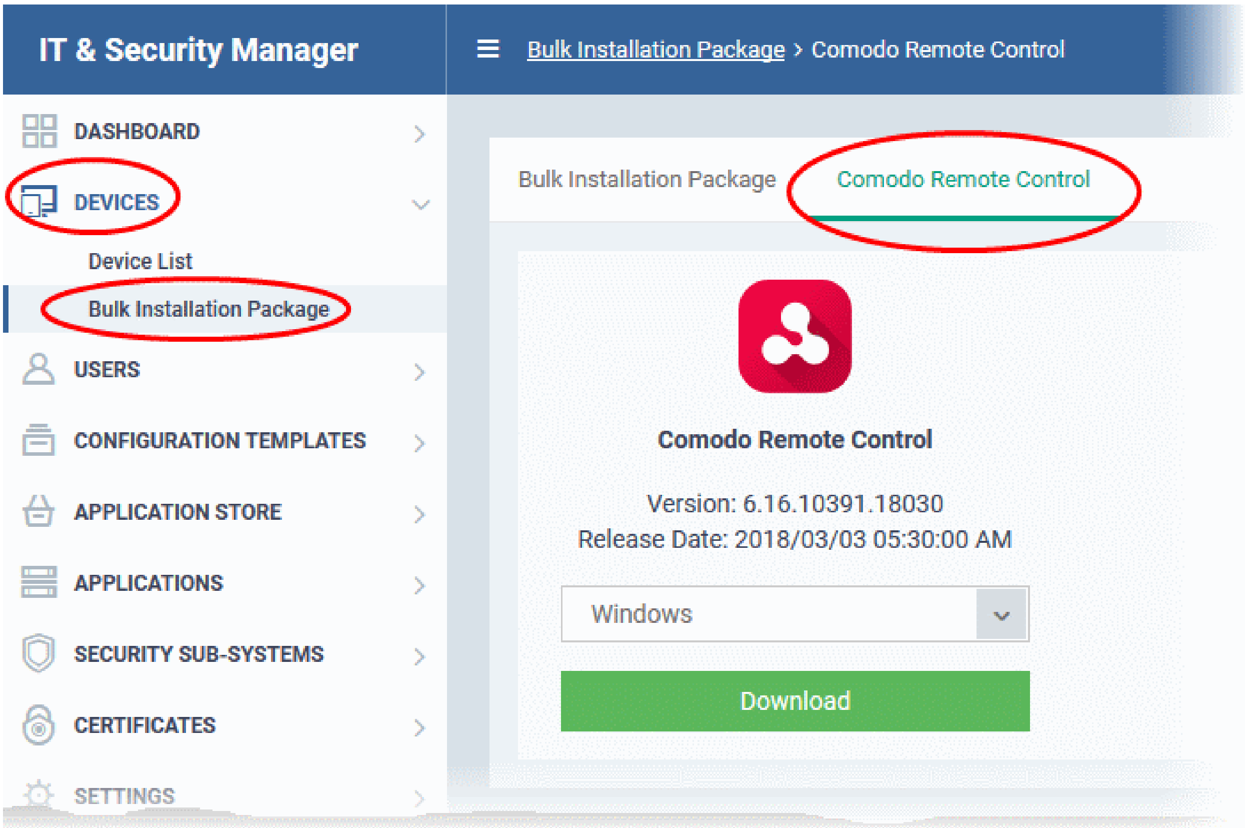
- You can download the tool from two places:
  - **ITSM interface** - Click 'Devices' > 'Bulk Enrollment Package' > Comodo Remote Control.
  - **C1 Console** - Click 'Tools' > Click 'Download' in the 'Comodo Remote Control' tile.
- The tool should be installed on your admin computer (the computer from which you want to control the remote endpoints).
- Once installed, the tool can be started from the desktop application or from the ITSM admin console.
- See **Remote Management of Windows and Mac OS Devices** for more help to takeover Windows and Mac OS devices

Limitations:

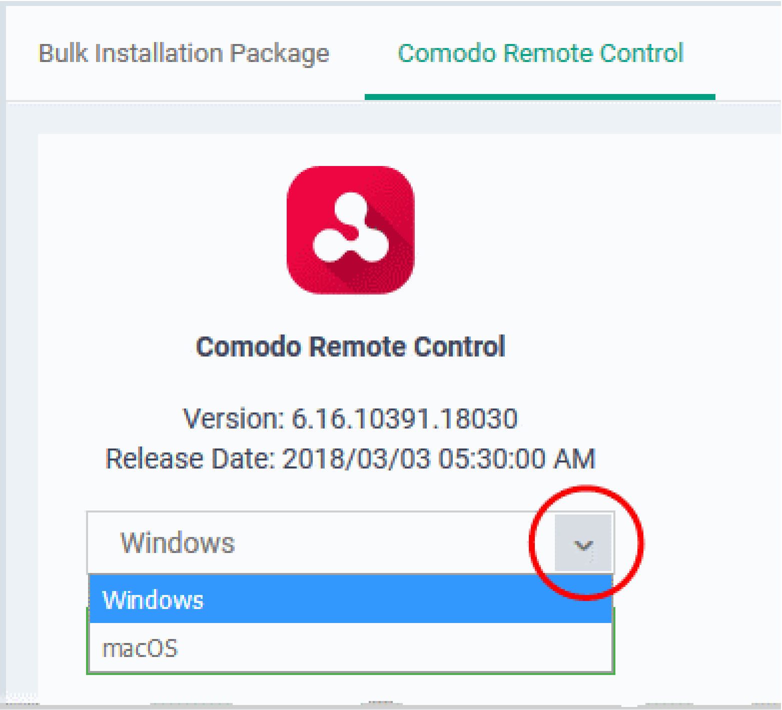
- Comodo Remote Control uses WebRTC and Chromodo protocols to connect to Windows devices and Chromodo protocol to connect to Mac OS devices.
- Chromoro is supported only by Windows 7 and later and Mac OS.
- WebRTC is not supported by Mac OS
- Chromodo is not supported by Windows XP
- You will not be able to take remote control of:
  - A Mac OS device from CRC installed on a Windows XP computer
  - A Windows device from CRC installed on a Mac OS machine

Download CRC from ITSM interface

- Click 'Devices' on the left then choose 'Bulk Installation Package'.
- Select the 'Comodo Remote Control' tab



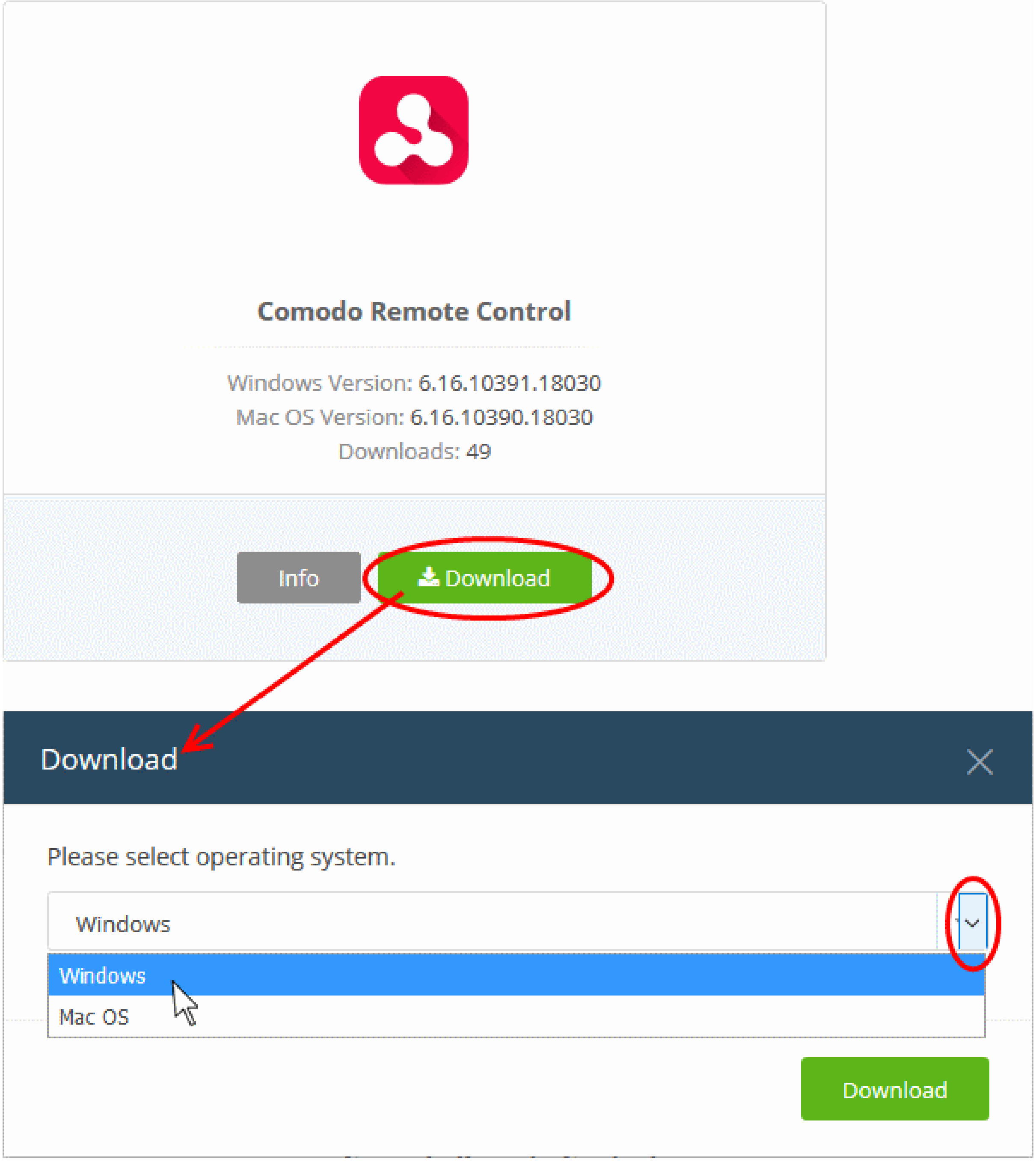
- Select the OS of the computer on which you want to install the tool.


Bulk Installation Package
Comodo Remote Control
Comodo Remote Control
Version: 6.16.10391.18030
Release Date: 2018/03/03 05:30:00 AM
Windows
Windows
macOS

- Click 'Download' and save the setup file.

Download CRC from Comodo One Console

- Login to your Comodo One account and click 'Tools' from the top
- The 'Tools' interface displays a list of productivity and security tools available for download from C1 as tiles
- Click the 'Download' button in the 'Comodo Remote Control' tile



Comodo Remote Control

Windows Version: 6.16.10391.18030

Mac OS Version: 6.16.10390.18030

Downloads: 49

Download

Please select operating system.

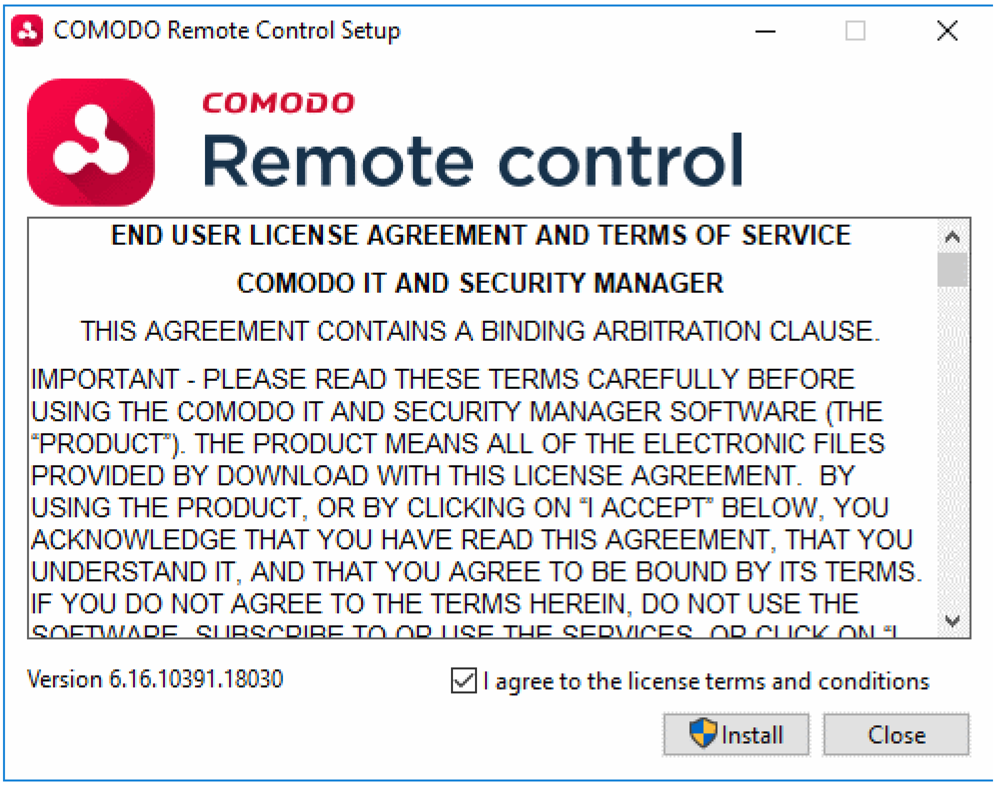
Windows

The 'Download' dialog will appear.

- Select the operating system of your admin machine, click 'Download' and save the setup file.

To install the tool

- Launch the set up file to start the installation wizard:



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

COMODO IT AND SECURITY MANAGER

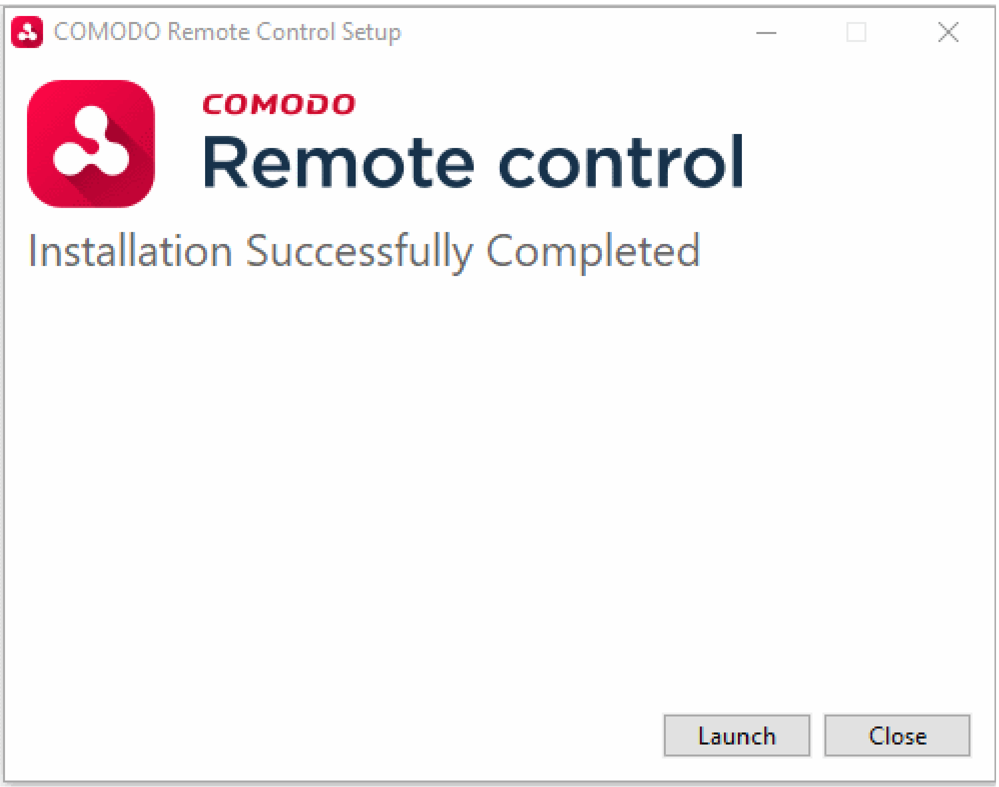
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO IT AND SECURITY MANAGER SOFTWARE (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I

Version 6.16.10391.18030

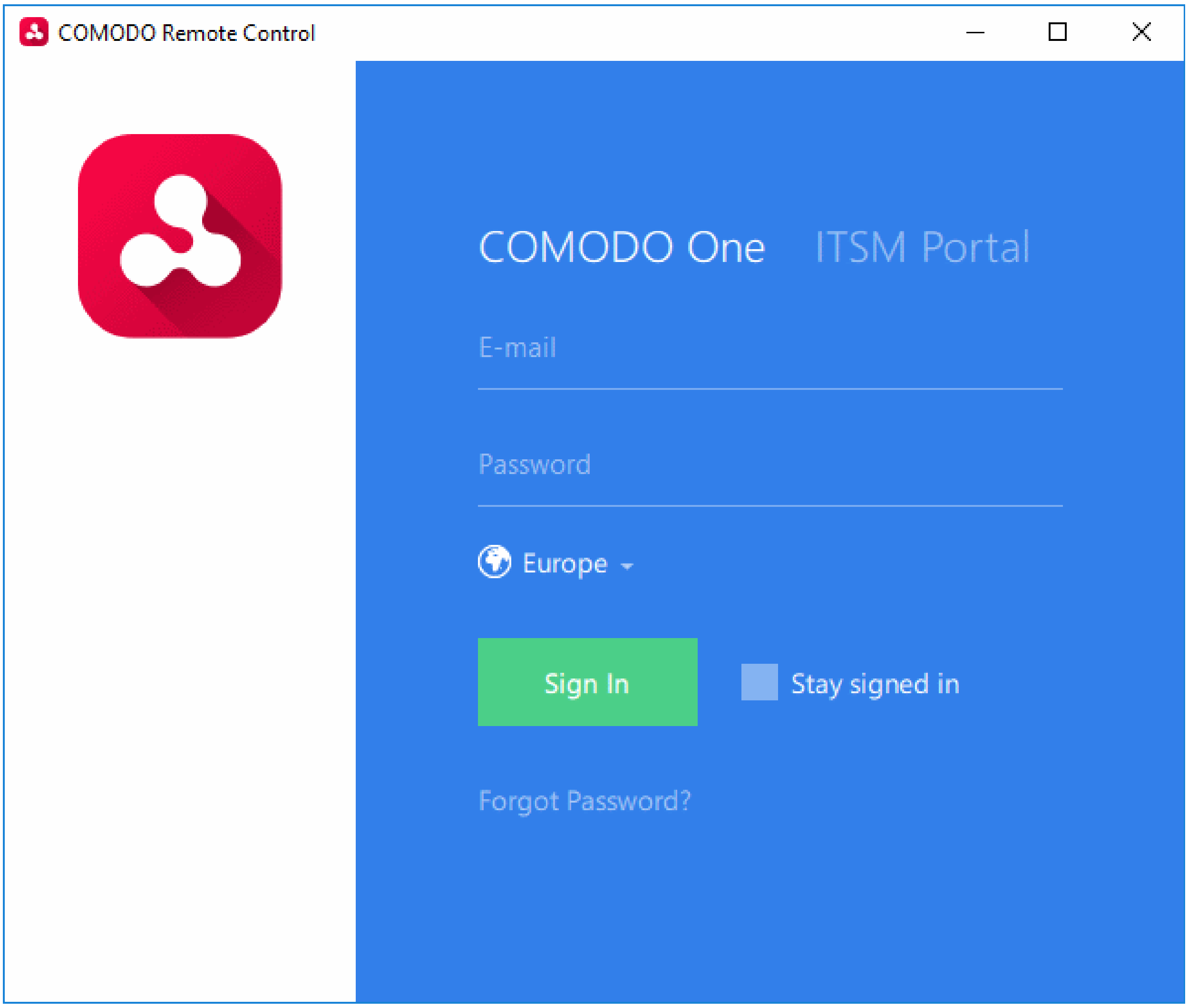
☑ I agree to the license terms and conditions

- You must read and accept the End User License Agreement before continuing. After doing so, click 'Install' to start the installation.



Installation Successfully Completed

- After installation is complete, click 'Launch' to start the application.

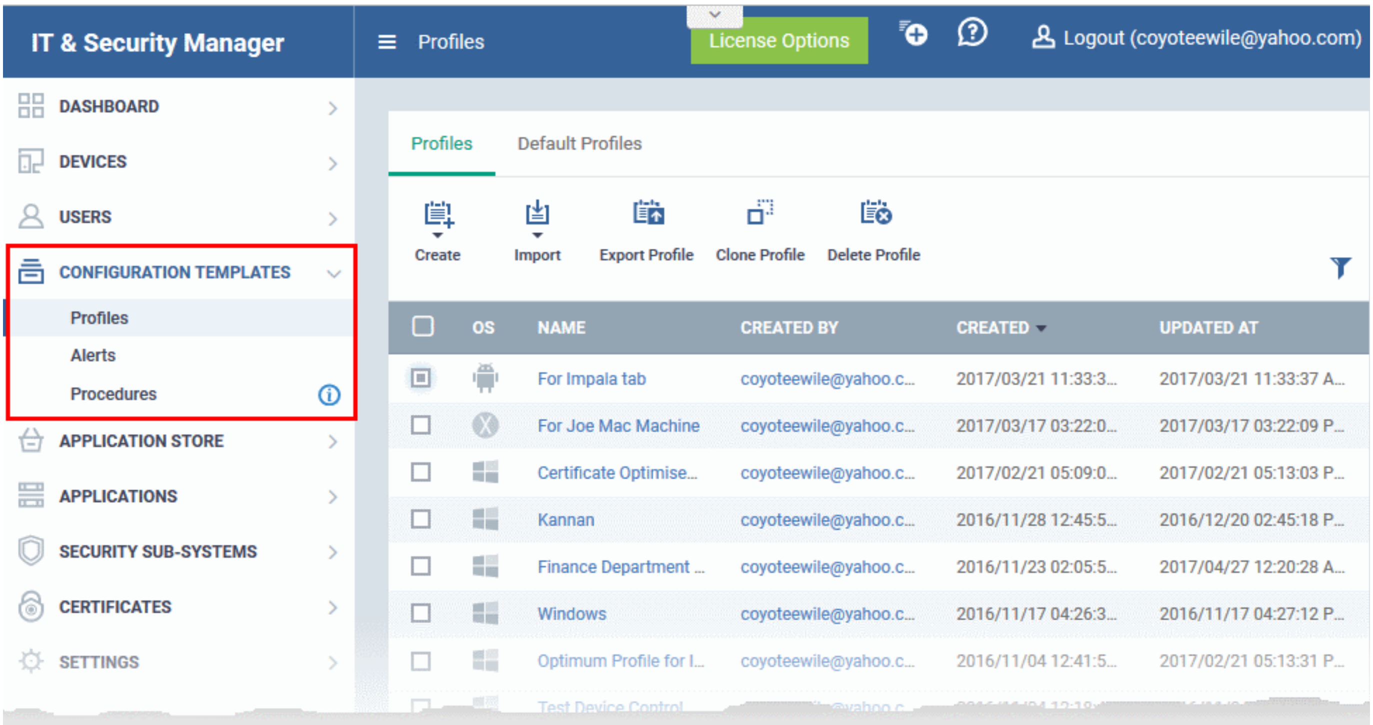


- Login to the application using your Comodo One username and password to start managing Windows or Mac OS endpoints. See **Remote Management of Windows and Mac OS Devices** for more details on using the desktop application.

6. Configuration Templates

The 'Configuration Templates' section lets you create and manage profiles for Android, iOS, Mac OS and Windows operating systems.

- Each profile allows you to specify a device's network access rights, overall security policy, antivirus scan schedule and other general system settings.
- Once created, profiles can be applied to devices/device groups and users/user groups.
- You can also add procedures to a profile. Procedures allow you to automate the execution of various tasks (for example, patch installation, disk fragmentation and so on). Procedures can also be deployed as stand-alone instructions.
- You can configure alerts to open tickets in Service Desk and also to create notifications in the interface. You can create multiple alerts and associate them with the monitoring feature in a profile according to your requirements.



OS	NAME	CREATED BY	CREATED	UPDATED AT
	For Impala tab	coyoteewile@yahoo.c...	2017/03/21 11:33:3...	2017/03/21 11:33:37 A...
	For Joe Mac Machine	coyoteewile@yahoo.c...	2017/03/17 03:22:0...	2017/03/17 03:22:09 P...
	Certificate Optimise...	coyoteewile@yahoo.c...	2017/02/21 05:09:0...	2017/02/21 05:13:03 P...
	Kannan	coyoteewile@yahoo.c...	2016/11/28 12:45:5...	2016/12/20 02:45:18 P...
	Finance Department ...	coyoteewile@yahoo.c...	2016/11/23 02:05:5...	2017/04/27 12:20:28 A...
	Windows	coyoteewile@yahoo.c...	2016/11/17 04:26:3...	2016/11/17 04:27:12 P...
	Optimum Profile for I...	coyoteewile@yahoo.c...	2016/11/04 12:41:5...	2017/02/21 05:13:31 P...
	Test Device Control	...@yahoo.c...		

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. See '**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. See '**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**

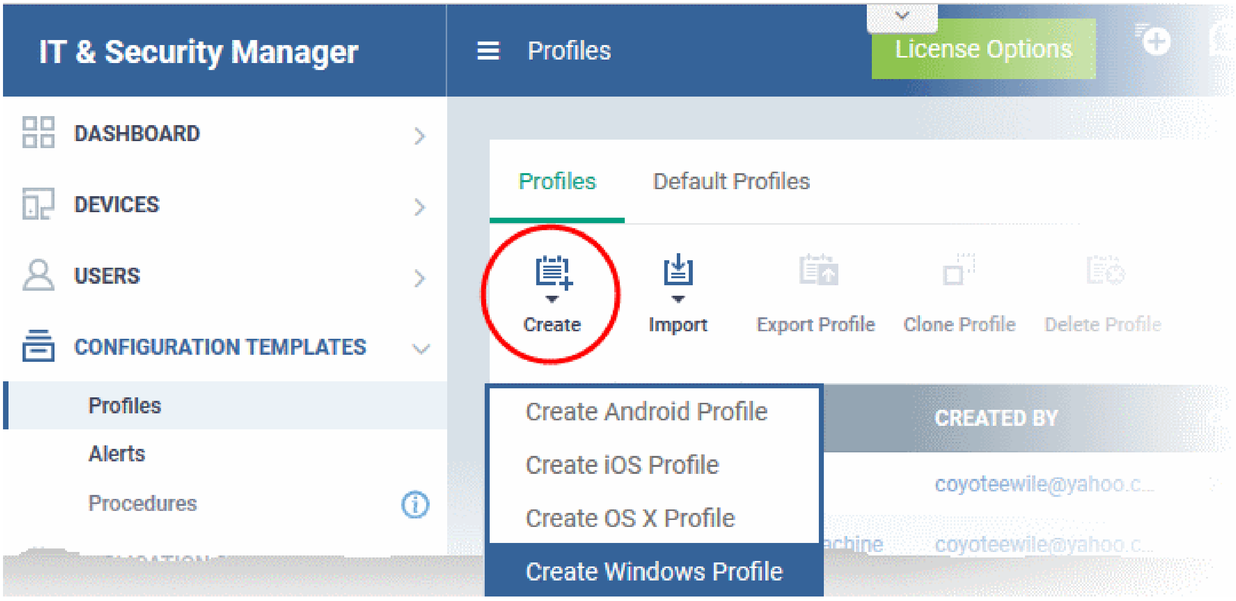
6.1. Create Configuration Profiles

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 on the left then 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 one 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 Mac OS 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 let you configure a device's network access rights, restrictions, scan schedule, authentication certificates, and other general settings.

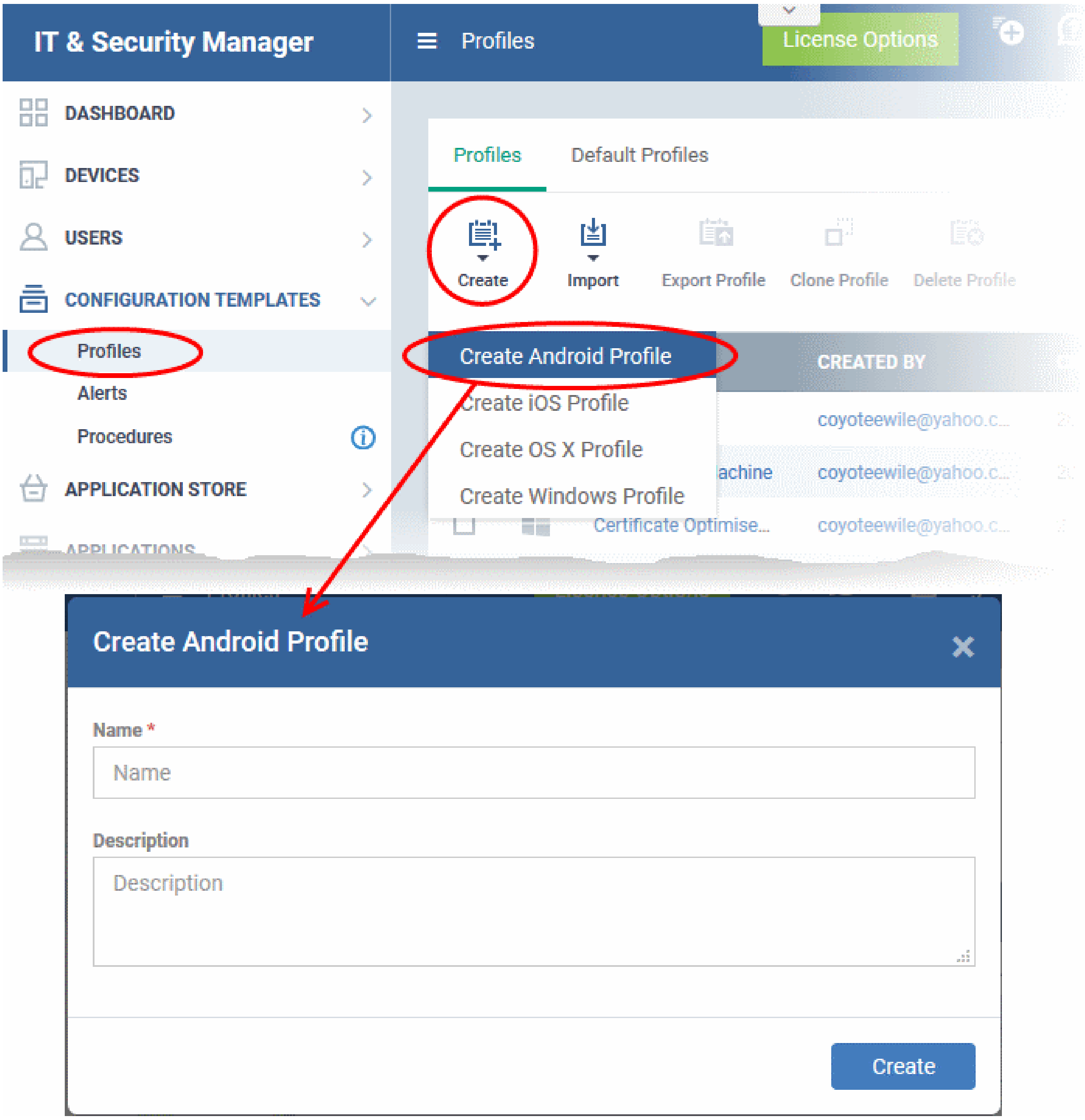
To create an Android profile

- 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. The profile will now appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - '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

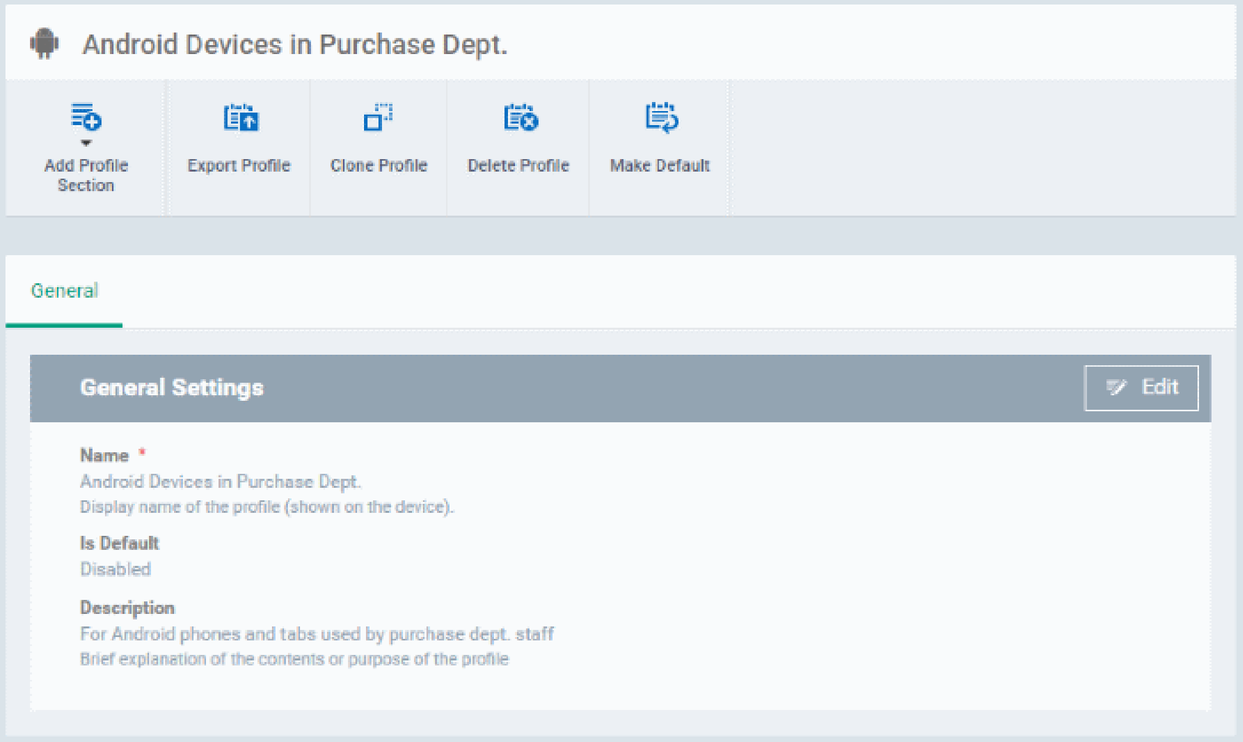
- Open the 'Profiles' interface by clicking 'Configuration Templates' on the left then 'Profiles'
- Click the 'Create' button above the table under 'Profiles' and choose 'Create Android Profile' from the options



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.



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

Is Default
Disabled

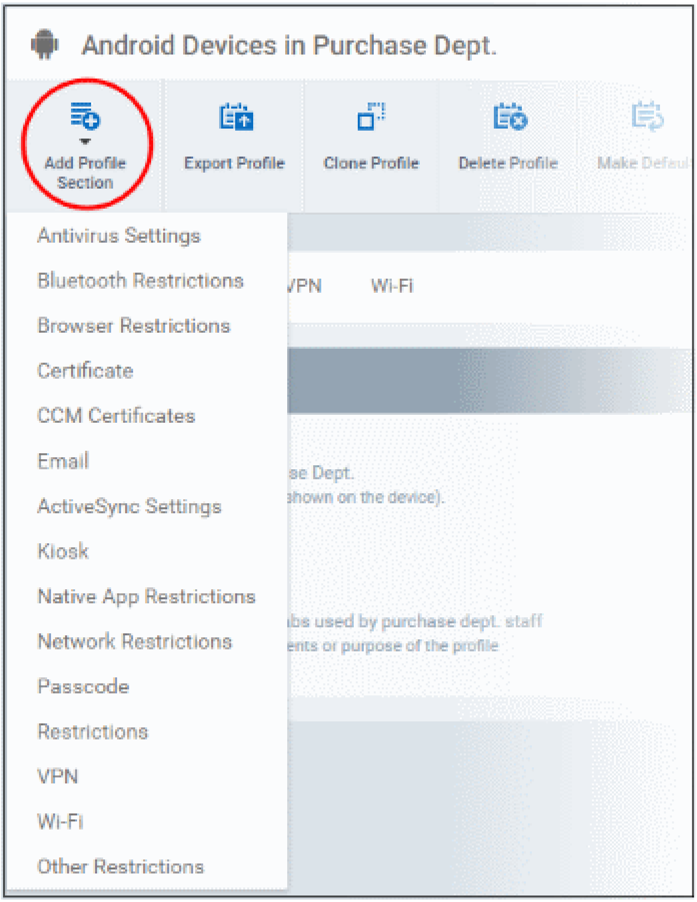
Description
For Android phones and tabs used by purchase dept. staff
Brief explanation of the contents or purpose of the profile

- If you want this profile to be a default policy, click 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. See **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

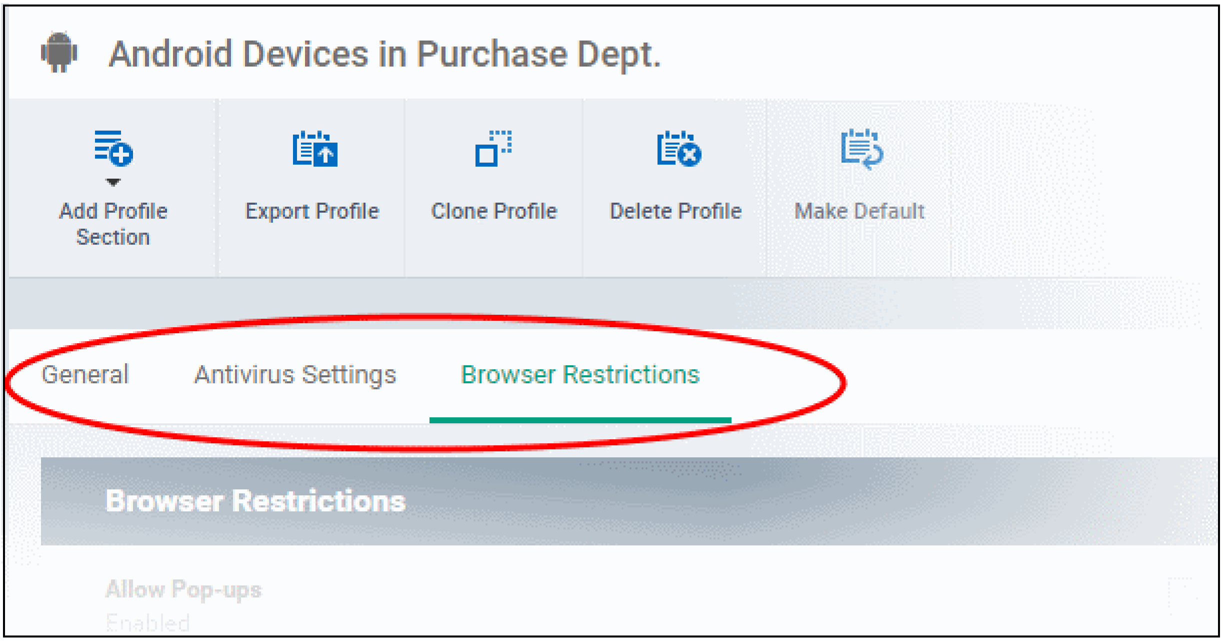


Note: Many Android profile settings have small information boxes next to them which indicate the OS and/or device required for the setting to work correctly.

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.



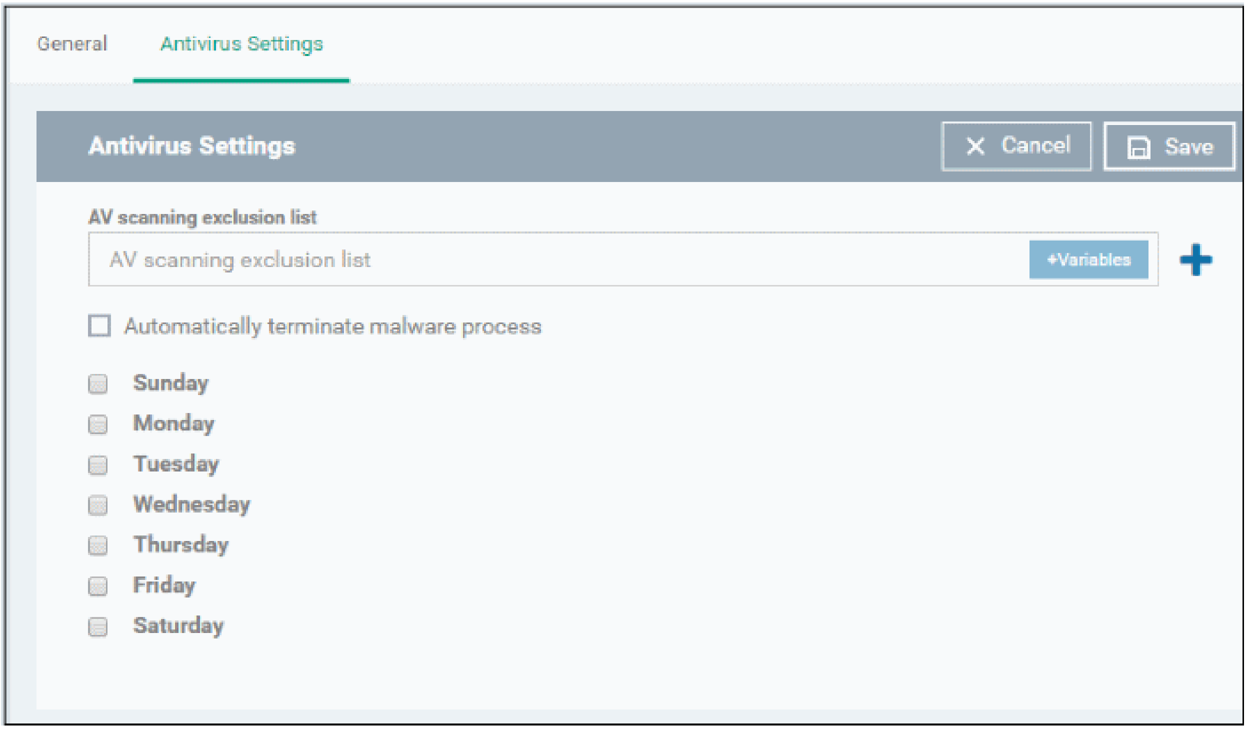
The following sections explain more about each of the settings:

- 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.



General | Antivirus Settings

Antivirus Settings

AV scanning exclusion list

AV scanning exclusion list

□ Automatically terminate malware process

- □ Sunday
- □ Monday
- □ Tuesday
- □ Wednesday
- □ Thursday
- □ Friday
- □ Saturday

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, see **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. See '**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.

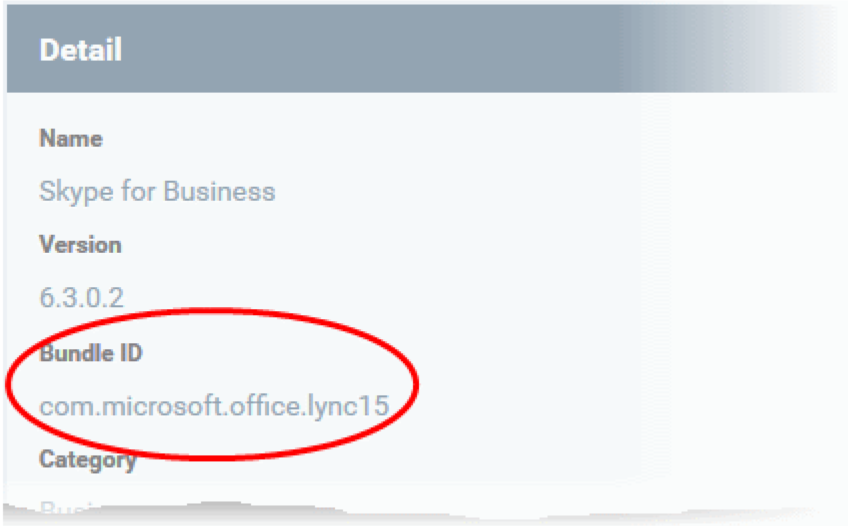
For example, 'com.comodo.batterysaver' is the Comodo Battery Saver app id in the URL

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



Detail

Name

Skype for Business

Version

6.3.0.2

Bundle ID

com.microsoft.office.lync15

Category

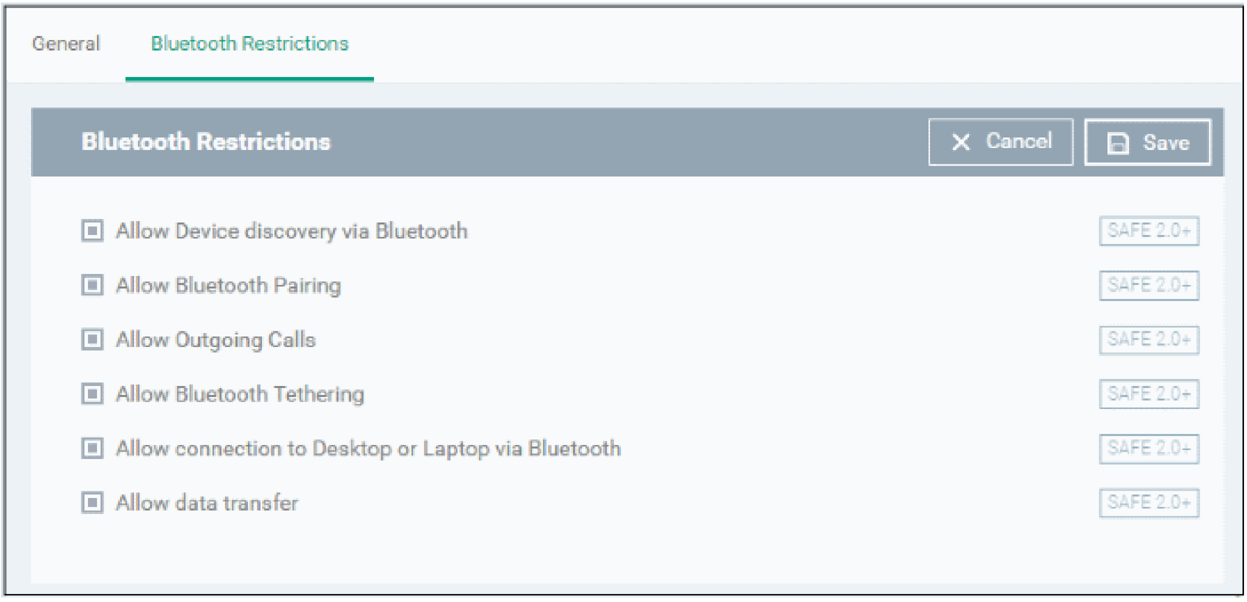
The bundle identifier is displayed in the 'Bundle ID' field.

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

☑ Allow Device discovery via Bluetooth SAFE 2.0+

☑ Allow Bluetooth Pairing SAFE 2.0+

☑ Allow Outgoing Calls SAFE 2.0+

☑ Allow Bluetooth Tethering SAFE 2.0+

☑ Allow connection to Desktop or Laptop via Bluetooth SAFE 2.0+

☑ Allow data transfer SAFE 2.0+

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.

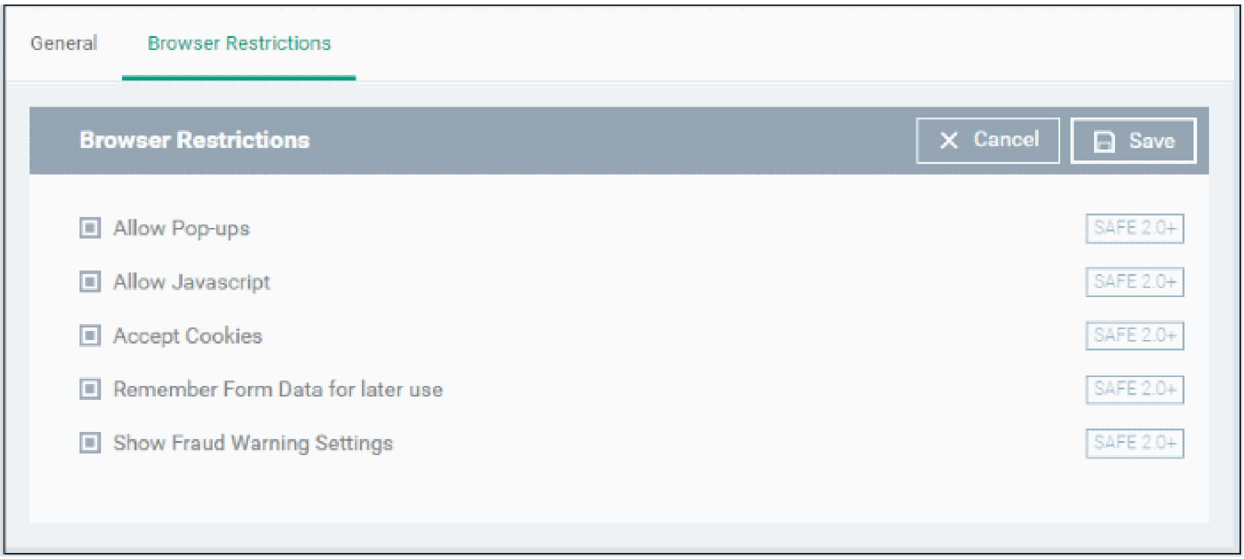
The settings will be saved and displayed under the 'Bluetooth Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See '**Editing Configuration Profiles**' for more details.

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.



□ Allow Pop-ups SAFE 2.0+

□ Allow Javascript SAFE 2.0+

□ Accept Cookies SAFE 2.0+

□ Remember Form Data for later use SAFE 2.0+

□ Show Fraud Warning Settings SAFE 2.0+

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.

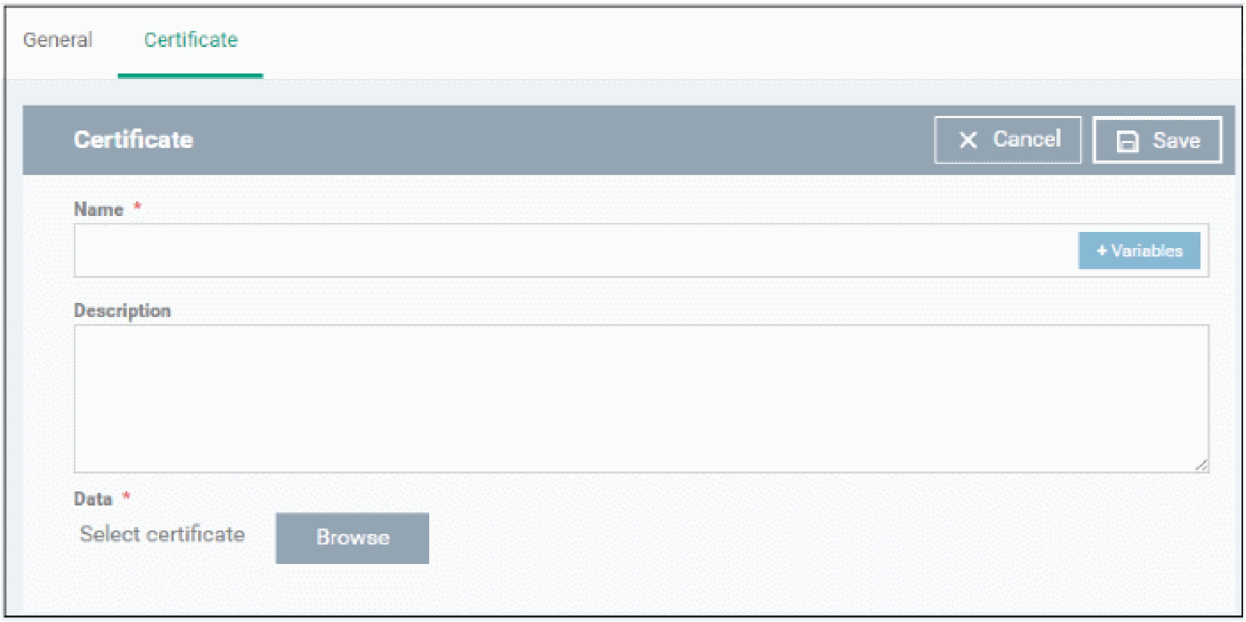
The settings will be saved and displayed under the 'Browser Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See '**Editing Configuration Profiles**' for more details.

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

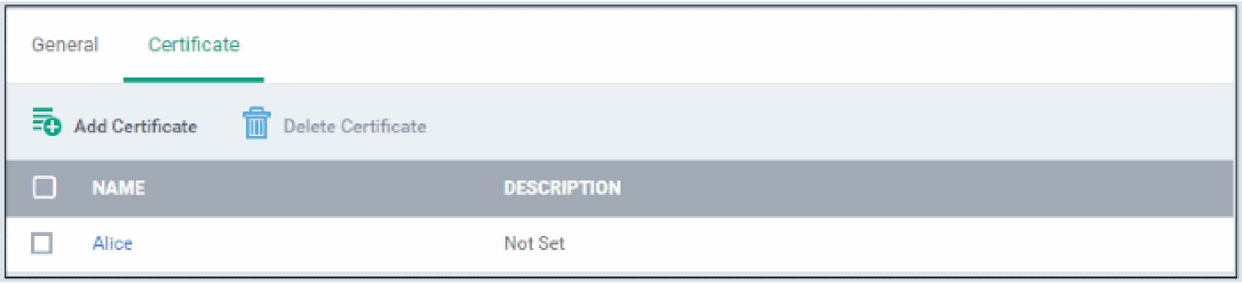
The 'Certificate' settings screen will be displayed.



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.



☐	NAME	DESCRIPTION
☐	Alice	Not Set

- 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.

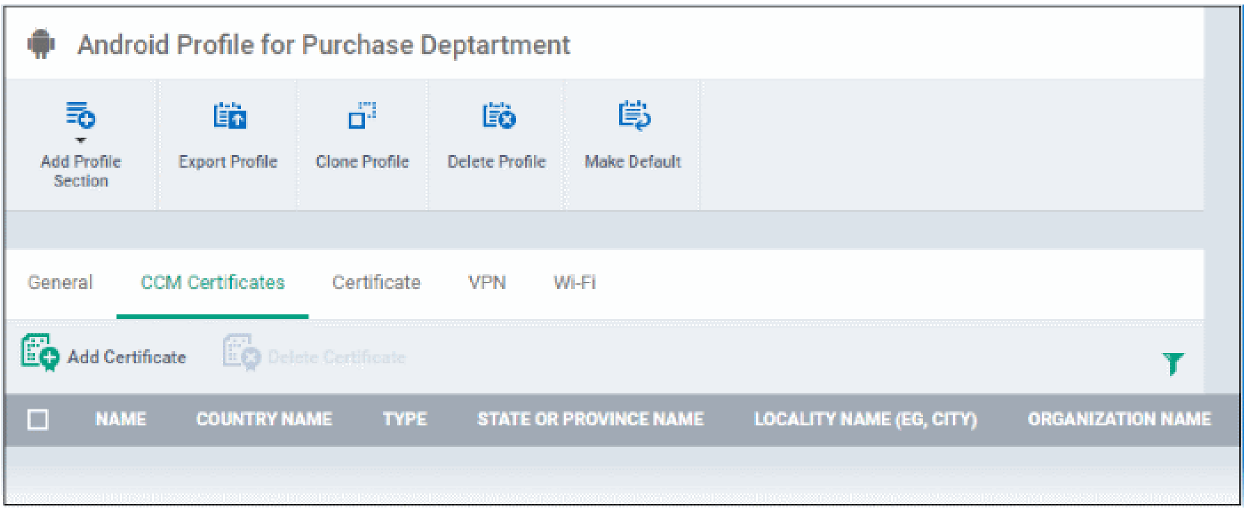
In addition to user authentication, client certificates can be used for email signing and encryption.

Prerequisite: Your CCM account should have been integrated to your ITSM server in order for ITSM to forward requests to CCM. For more details, see **Integrating with Comodo Certificate Manager.**

To configure CCM Certificate settings

- Choose 'Certificates' from the 'Add Profile Section' drop-down

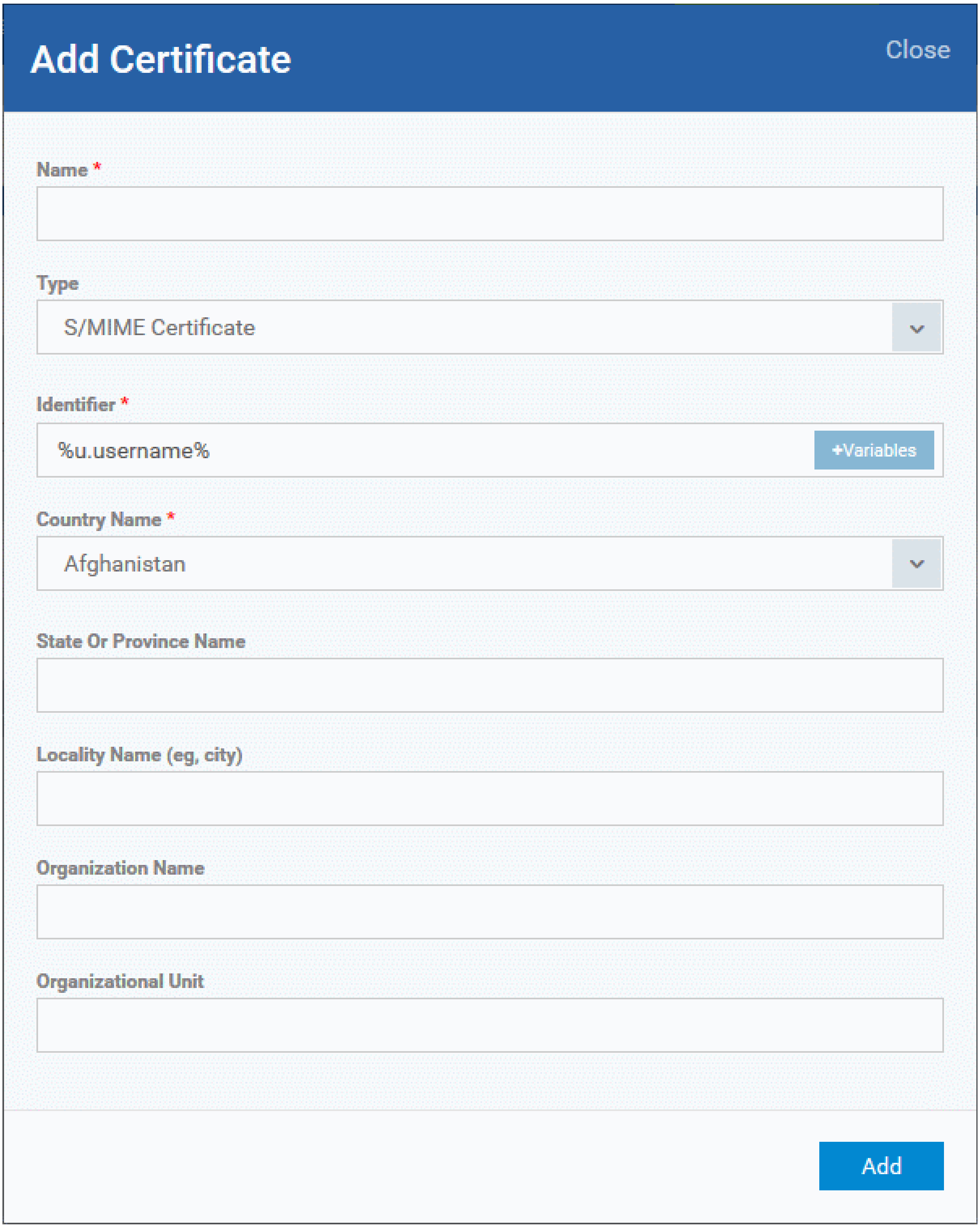
The settings screen for adding certificate requests to the profile will be displayed.



☐	NAME	COUNTRY NAME	TYPE	STATE OR PROVINCE NAME	LOCALITY NAME (EG, CITY)	ORGANIZATION NAME

- 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, see **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.

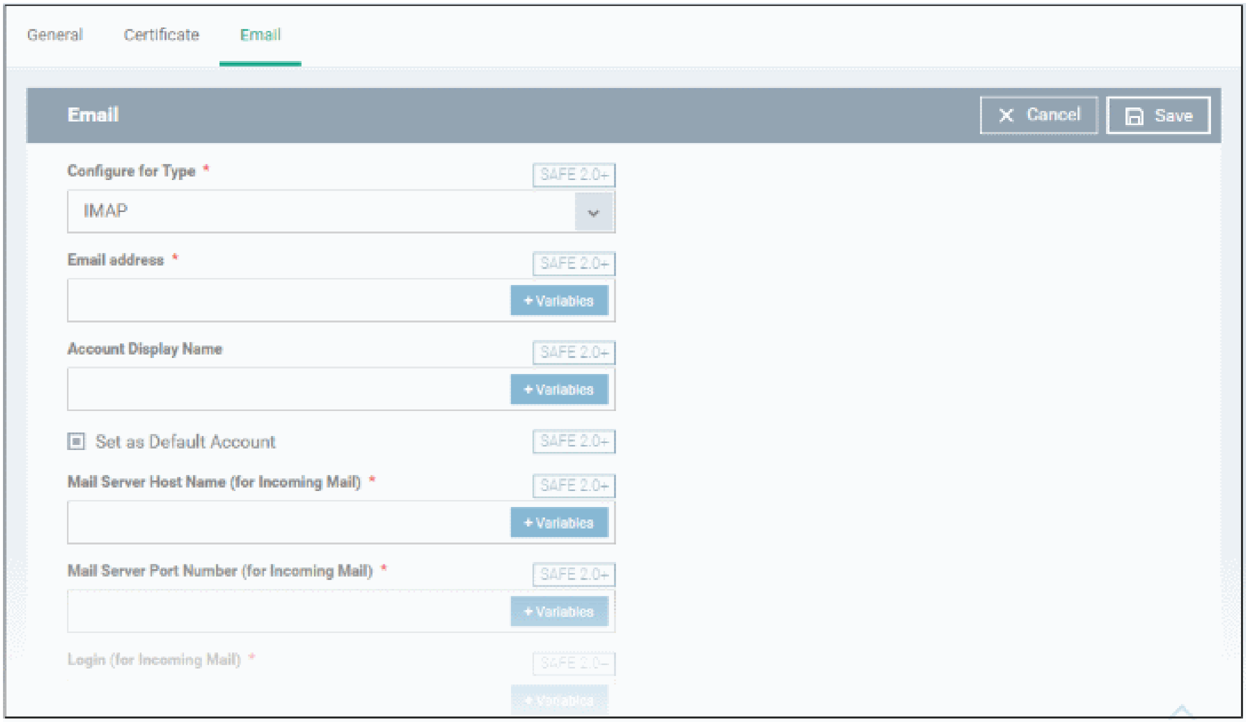
The certificate requests will be generated from the devices once the profile is applied to them.

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, see **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, see **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, see **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, see **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, see **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, see **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, see **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, see **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 automatically added to the profile while rolling out to the devices. For

Email Settings - Table of Parameters		
		more details on variables, see **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, see **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, see **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, see **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. See '**Editing Configuration Profiles**' for more details.

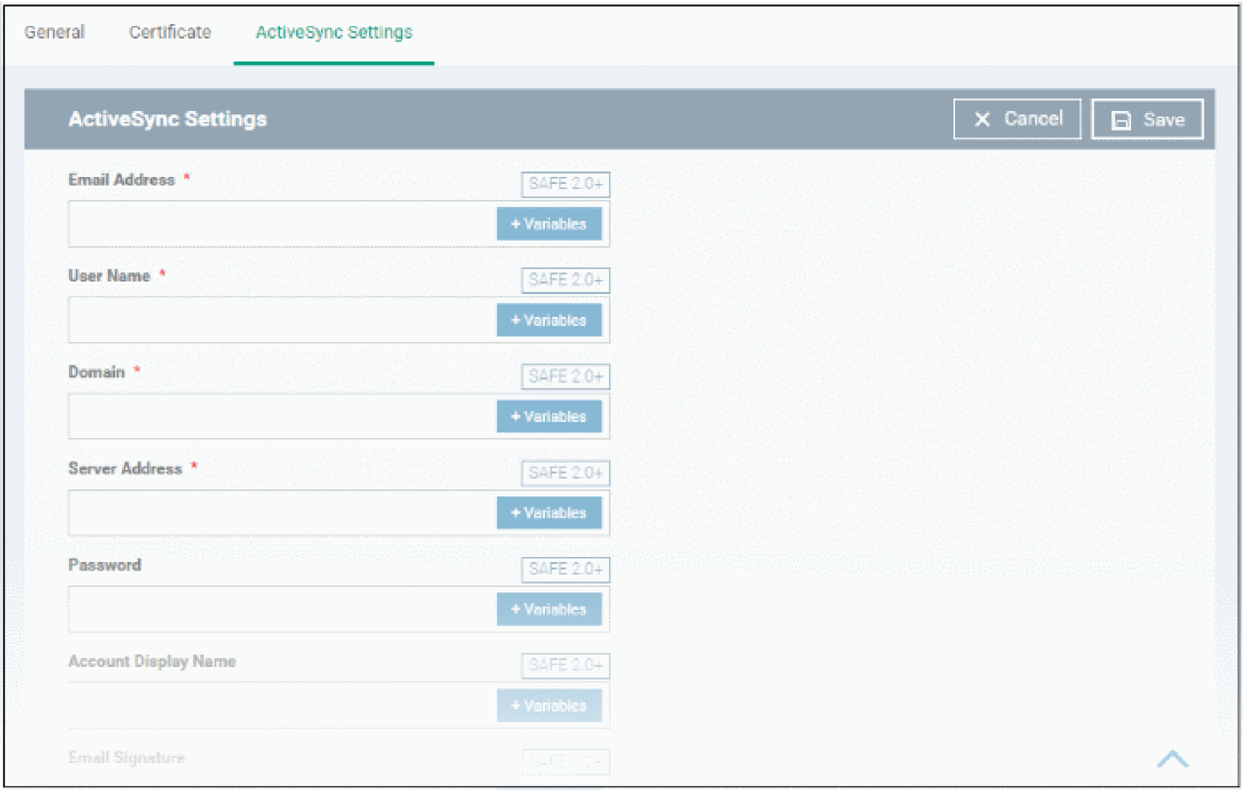
To configure ActiveSync settings

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, see **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, see **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, see **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, see **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.

ActiveSync Settings - Table of Parameters		
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, see **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, see **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, see **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.

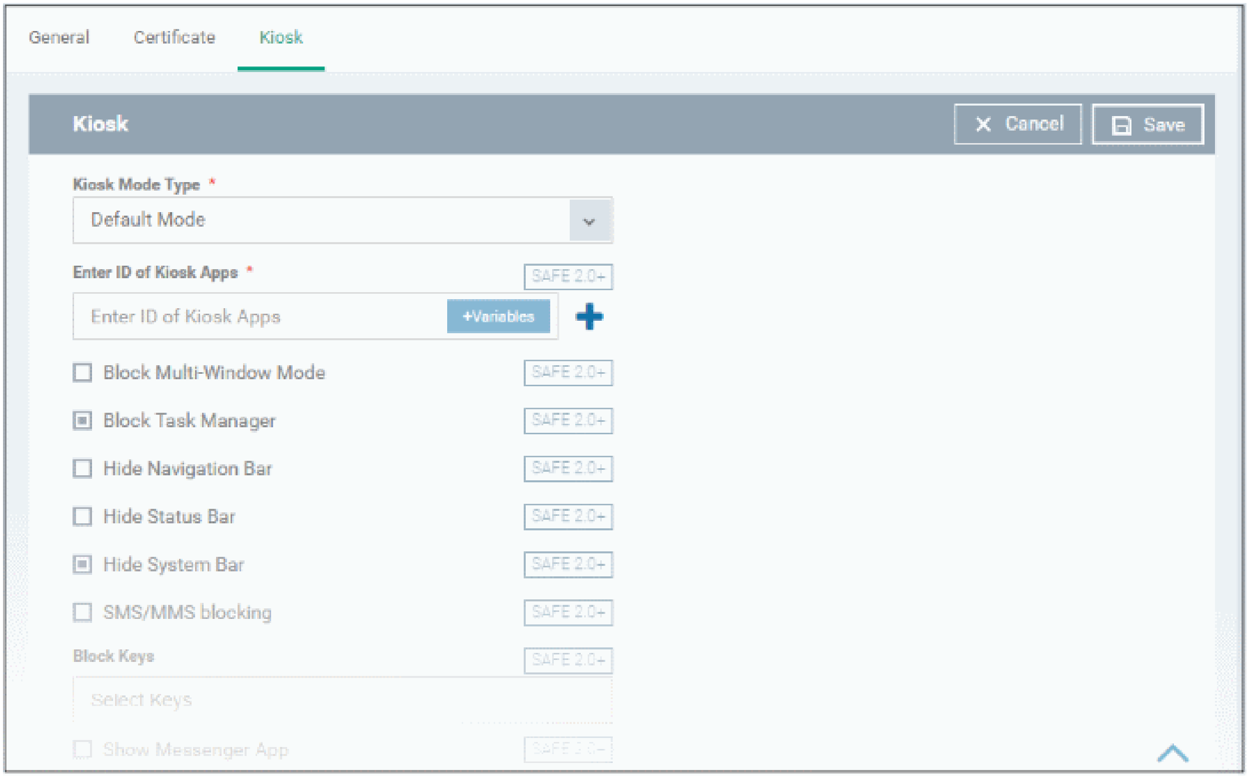
To configure Kiosk settings

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 Mode Type *
Default Mode

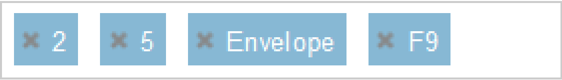
Enter ID of Kiosk Apps * SAFE 2.0+
Enter ID of Kiosk Apps +Variables

□ Block Multi-Window Mode SAFE 2.0+
☑ Block Task Manager SAFE 2.0+
□ Hide Navigation Bar SAFE 2.0+
□ Hide Status Bar SAFE 2.0+
☑ Hide System Bar SAFE 2.0+
□ SMS/MMS blocking SAFE 2.0+

Block Keys SAFE 2.0+
Select Keys

□ Show Messenger App SAFE 2.0+

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 and the status bar, can also be configured for either mode.
If 'Single App' is selected as Kiosk Mode Type:		

Kiosk Settings - Table of Parameters		
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, see **Configuring Custom Variables**. For more details on Package ID, see **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, see **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: Select Keys 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.  ✖ 2 ✖ 5 ✖ Envelope ✖ F9
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.

Kiosk Settings - Table of Parameters		
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.

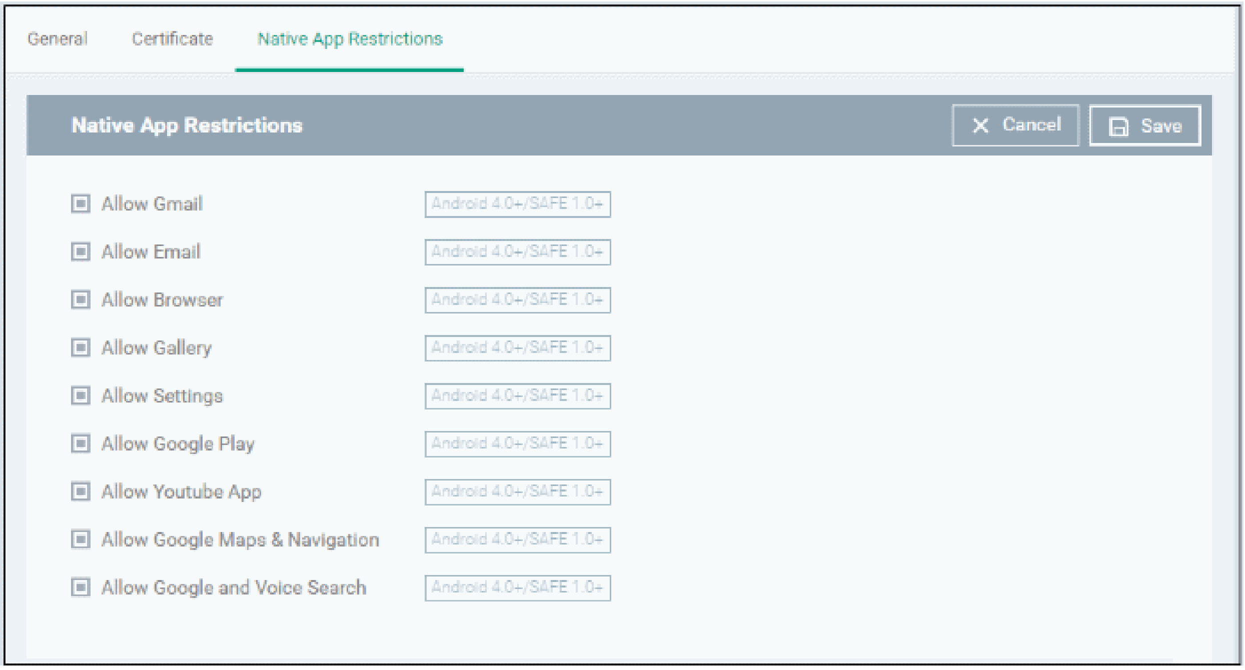
The settings will be saved and displayed under the 'Kiosk' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



□ Allow Gmail — Android 4.0+/SAFE 1.0+
□ Allow Email — Android 4.0+/SAFE 1.0+
□ Allow Browser — Android 4.0+/SAFE 1.0+
□ Allow Gallery — Android 4.0+/SAFE 1.0+
□ Allow Settings — Android 4.0+/SAFE 1.0+
□ Allow Google Play — Android 4.0+/SAFE 1.0+
□ Allow Youtube App — Android 4.0+/SAFE 1.0+
□ Allow Google Maps & Navigation — Android 4.0+/SAFE 1.0+
□ Allow Google and Voice Search — Android 4.0+/SAFE 1.0+

Native Application Restrictions Settings - Table of Parameters		
Form Element	**Type**	**Description**
Allow Gmail	Checkbox	Select this to allow users to access Gmail app.
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

Native Application Restrictions Settings - Table of Parameters		
		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.

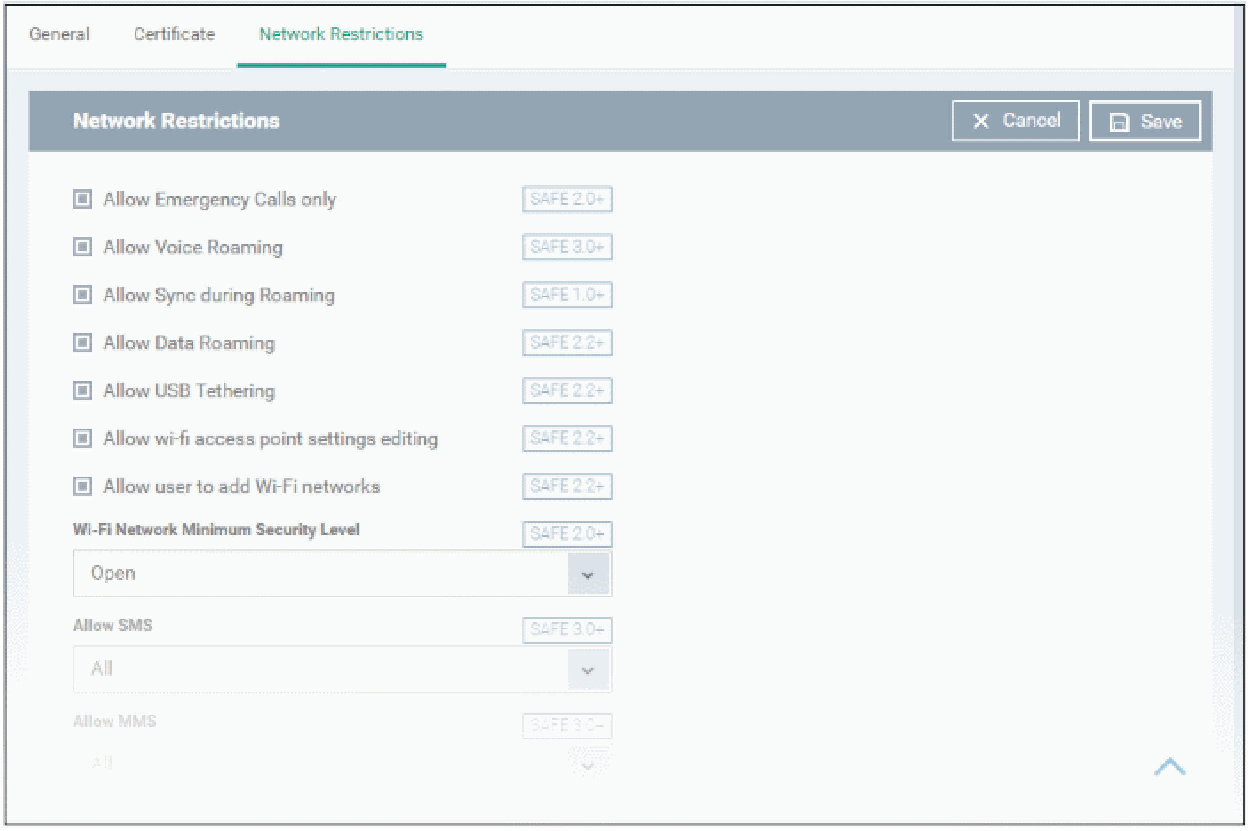
The settings will be saved and displayed under the 'Native App Restriction' tab. You can edit the settings or remove the section from the profile at anytime. See '**Editing Configuration Profiles**' for more details.

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

☐ Allow Emergency Calls only SAFE 2.0+

☐ Allow Voice Roaming SAFE 3.0+

☐ Allow Sync during Roaming SAFE 1.0+

☐ Allow Data Roaming SAFE 2.2+

☐ Allow USB Tethering SAFE 2.2+

☐ Allow wi-fi access point settings editing SAFE 2.2+

☐ Allow user to add Wi-Fi networks SAFE 2.2+

Wi-Fi Network Minimum Security Level SAFE 2.0+

Open

Allow SMS SAFE 3.0+

All

Allow MMS SAFE 3.0+

All

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**. Click the + button to add more 'Blacklisted SSID' fields. To remove a

Network Restrictions Settings - Table of Parameters		
		Blacklisted SSID field from the screen, click the minus ▬ button beside it.

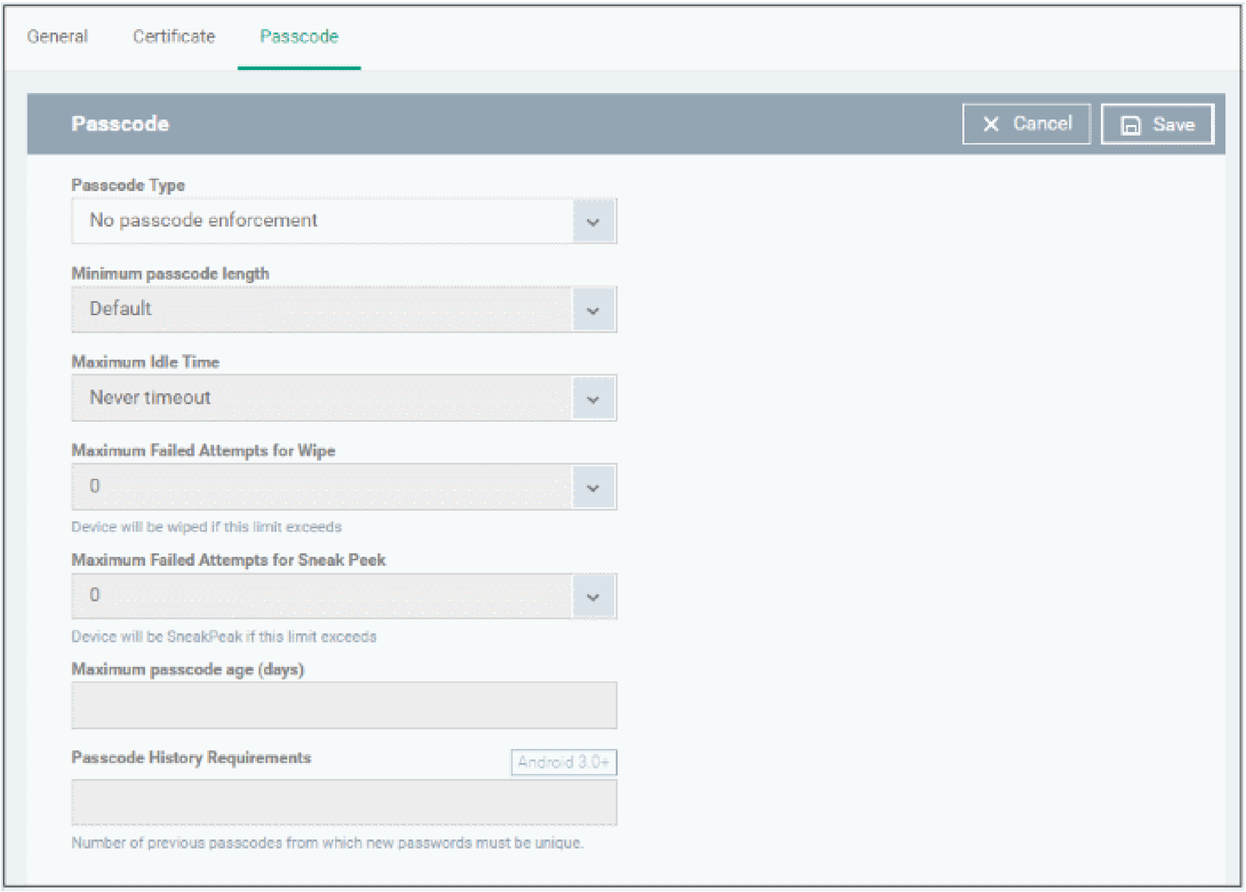
- Click the 'Save' button.

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 Type: No passcode enforcement

Minimum passcode length: Default

Maximum Idle Time: Never timeout

Maximum Failed Attempts for Wipe: 0

Device will be wiped if this limit exceeds

Maximum Failed Attempts for Sneak Peek: 0

Device will be SneakPeak if this limit exceeds

Maximum passcode age (days)

Passcode History Requirements Android 3.0+

Number of previous passcodes from which new passwords must be unique.

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.

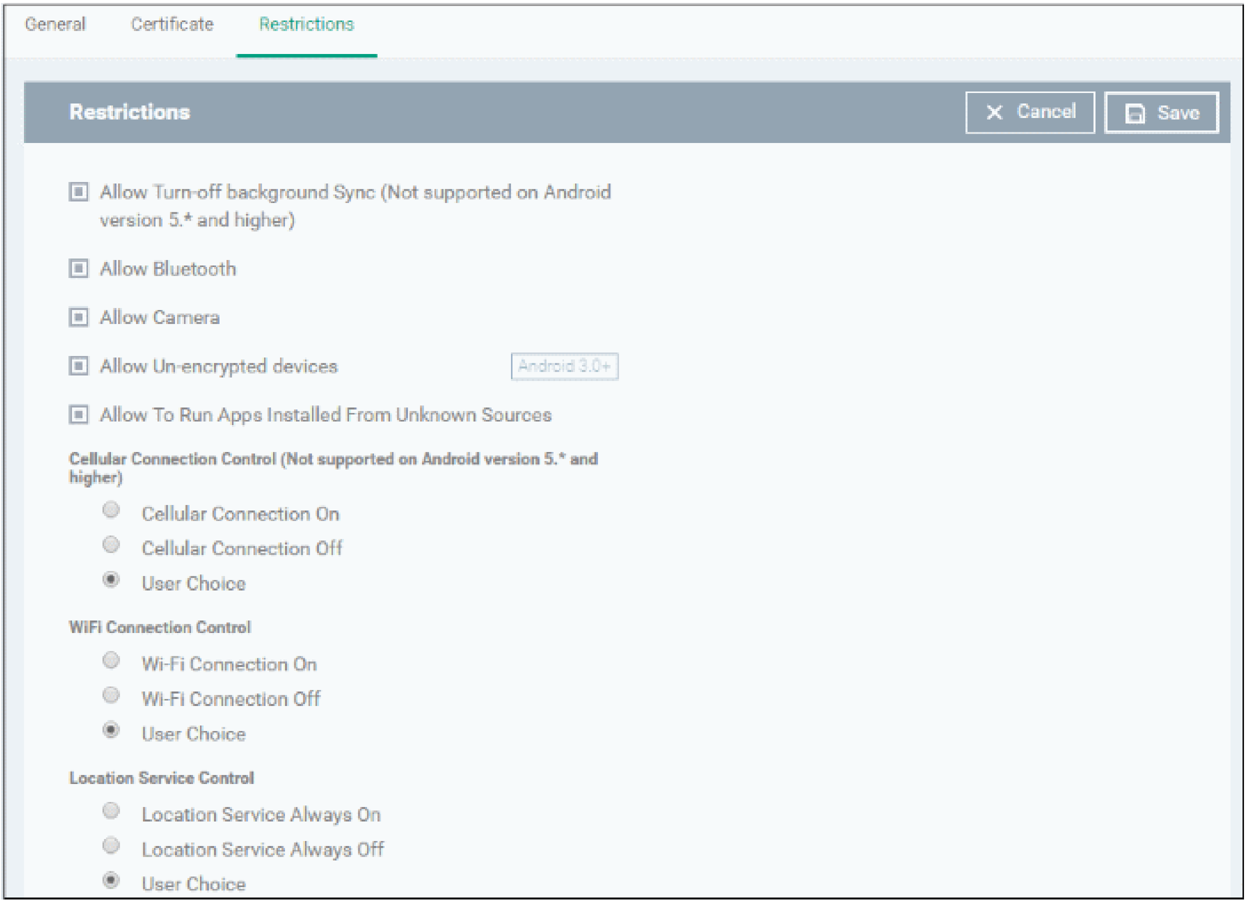
- Click the 'Save' button.

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.



☑ Allow Turn-off background Sync (Not supported on Android version 5.* and higher)

☑ Allow Bluetooth

☑ Allow Camera

☑ Allow Un-encrypted devices Android 3.0+

☑ Allow To Run Apps Installed From Unknown Sources

Cellular Connection Control (Not supported on Android version 5.* and higher)

○ Cellular Connection On
○ Cellular Connection Off
● User Choice

WiFi Connection Control

○ Wi-Fi Connection On
○ Wi-Fi Connection Off
● User Choice

Location Service Control

○ Location Service Always On
○ Location Service Always Off
● User Choice

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.

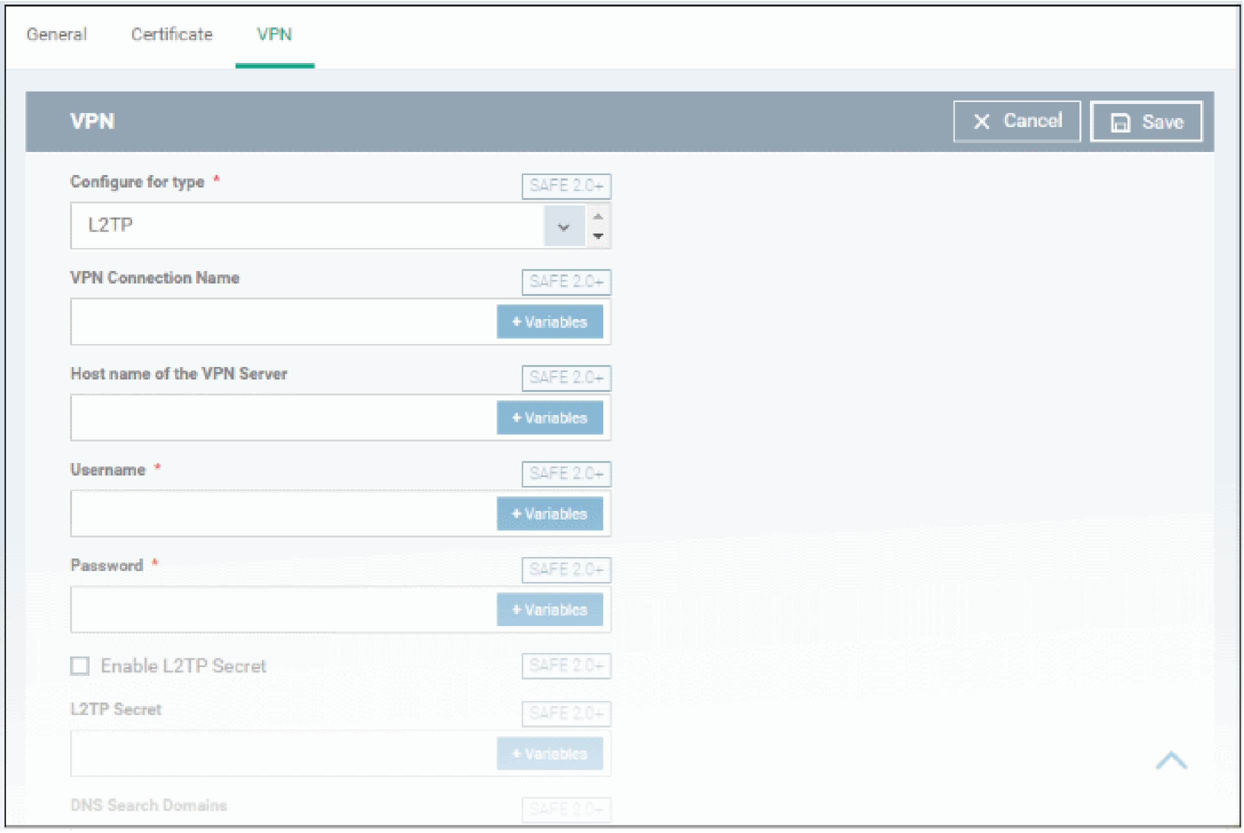
The settings will be saved and displayed under the 'Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



Configure for type *: L2TP

VPN Connection Name

Host name of the VPN Server

Username *

Password *

□ Enable L2TP Secret

L2TP Secret

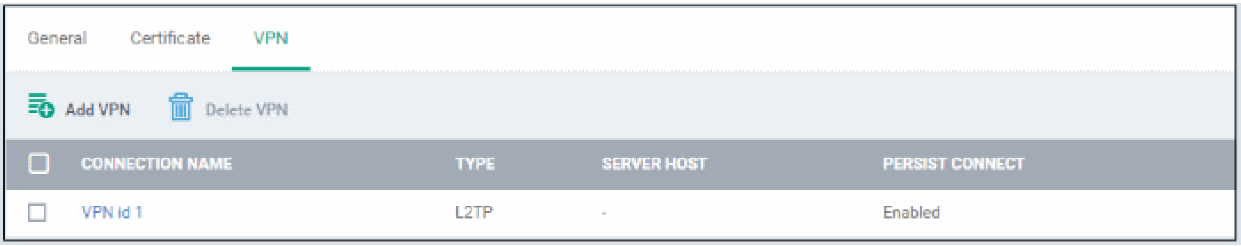
VPN Settings - Table of Parameters		
Form Element	**Type**	**Description**
Configure for type	Drop-down	Choose the VPN connection type from drop-down. The options available are: L2TP, PPTP, L2TP/IPSec PSK, IPSec, XAuth PSK and IPSec XAuth RSA.
VPN Connection Name	Text Field	Enter the name of the connection, 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.



☐	CONNECTION NAME	TYPE	SERVER HOST	PERSIST CONNECT
☐	VPN id 1	L2TP	-	Enabled

You can add multiple VPN connection settings for the profile.

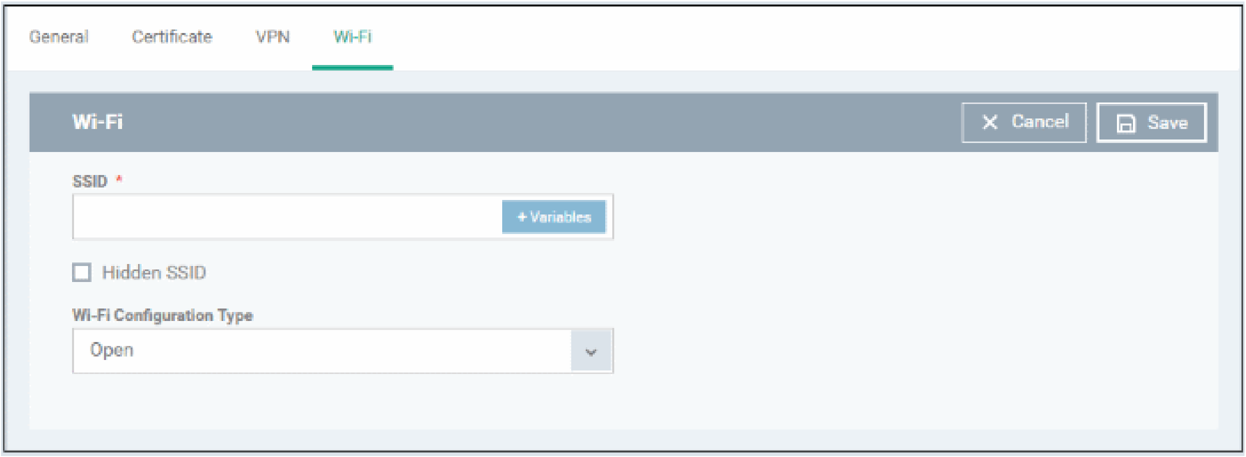
- To add another VPN connection, click 'Add VPN' and repeat the process
- To view and edit the VPN settings of a connection, click the name of the connection
- To remove a VPN connection, select VPN then click 'Delete VPN'

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**.

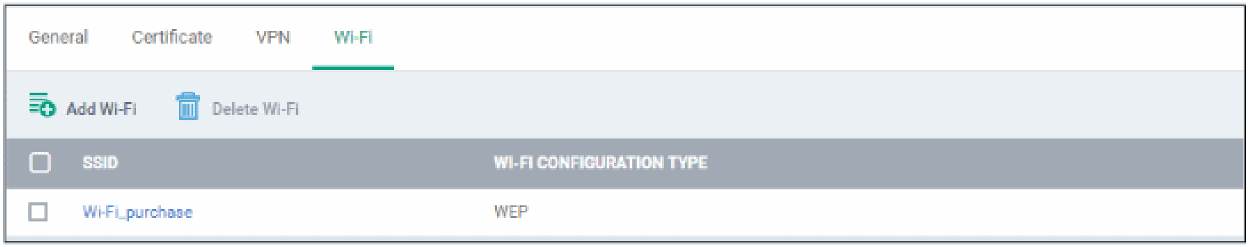
Wi-Fi Configuration Type settings

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. • None • PAP • MSCHAP

Wi-Fi Configuration Type Settings - Table of Parameters	
	• 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.



□ SSID	WI-FI CONFIGURATION TYPE
□ Wi-Fi_purchase	WEP

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'

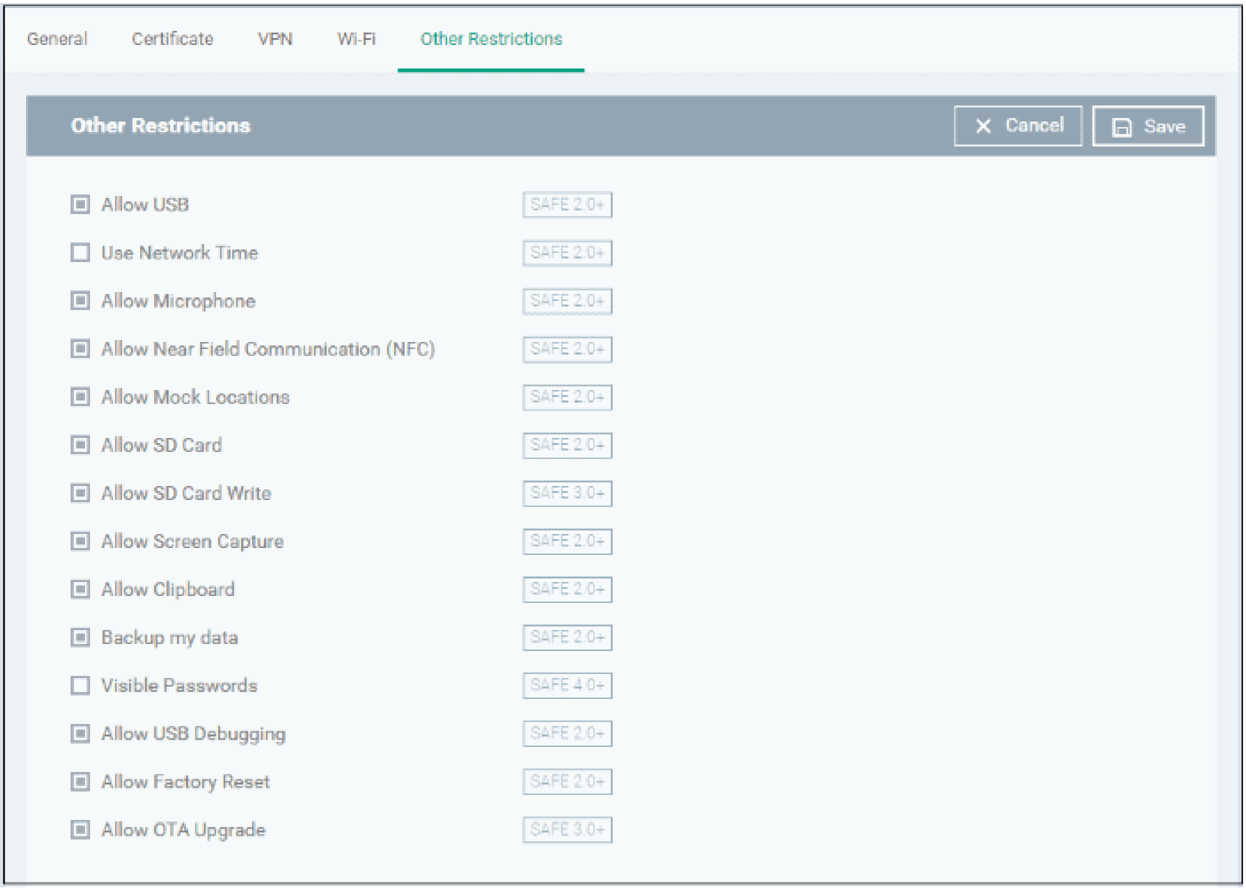
You can add or remove Wi-Fi networks at any time. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



☑ Allow USB SAFE 2.0+
□ Use Network Time SAFE 2.0+
☑ Allow Microphone SAFE 2.0+
☑ Allow Near Field Communication (NFC) SAFE 2.0+
☑ Allow Mock Locations SAFE 2.0+
☑ Allow SD Card SAFE 2.0+
☑ Allow SD Card Write SAFE 3.0+
☑ Allow Screen Capture SAFE 2.0+
☑ Allow Clipboard SAFE 2.0+
☑ Backup my data SAFE 2.0+
□ Visible Passwords SAFE 4.0+
☑ Allow USB Debugging SAFE 2.0+
☑ Allow Factory Reset SAFE 2.0+
☑ Allow OTA Upgrade SAFE 3.0+

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.
Allow Screen Capture	Checkbox	Users can take screenshot of the device screen.

Other Restrictions Settings - Table of Parameters		
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.

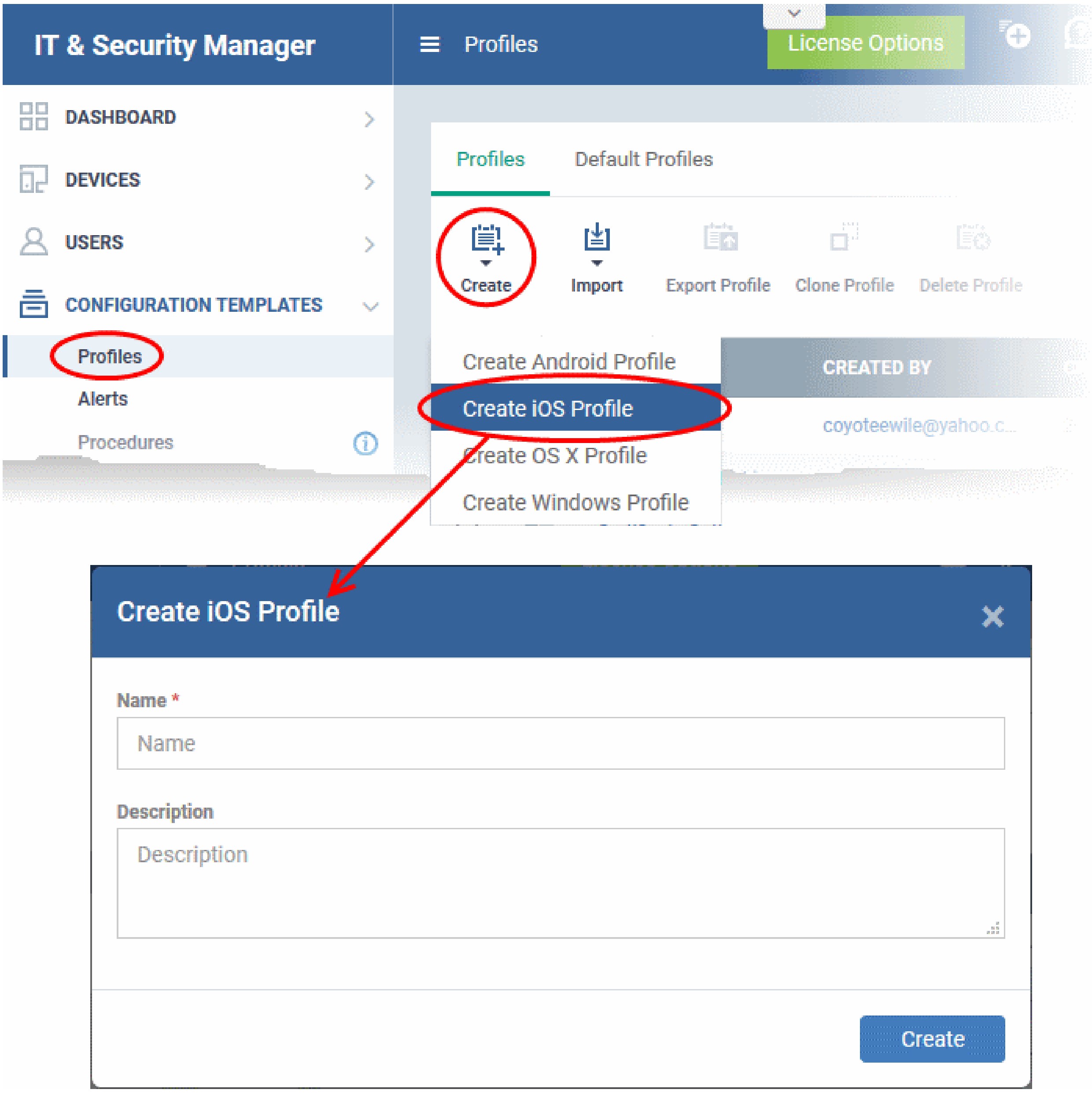
To create an iOS profile

- 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. The profile will now appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - '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 iOS profile

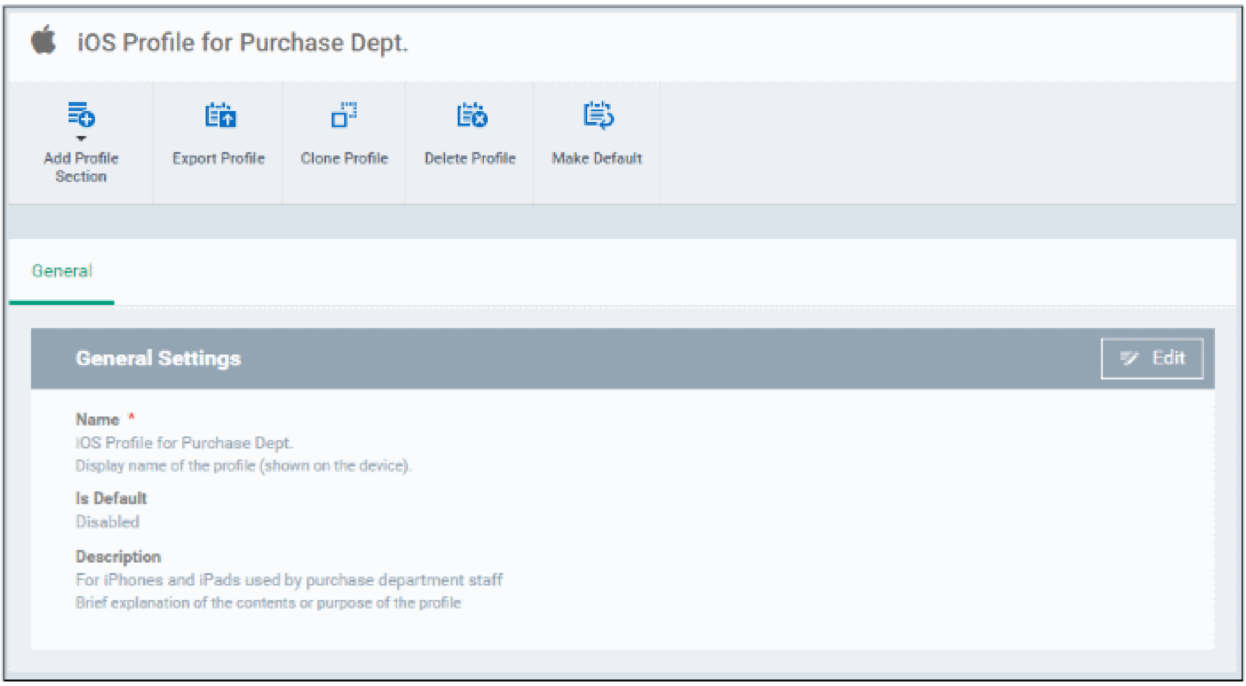
- Open the 'Profiles' interface by clicking 'Configuration Templates' from the left and choosing 'Profiles'
- Click the 'Create' button above the table under 'Profiles' and and choose 'Create iOS Profile' from the options



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.



Name *
iOS Profile for Purchase Dept.
Display name of the profile (shown on the device).

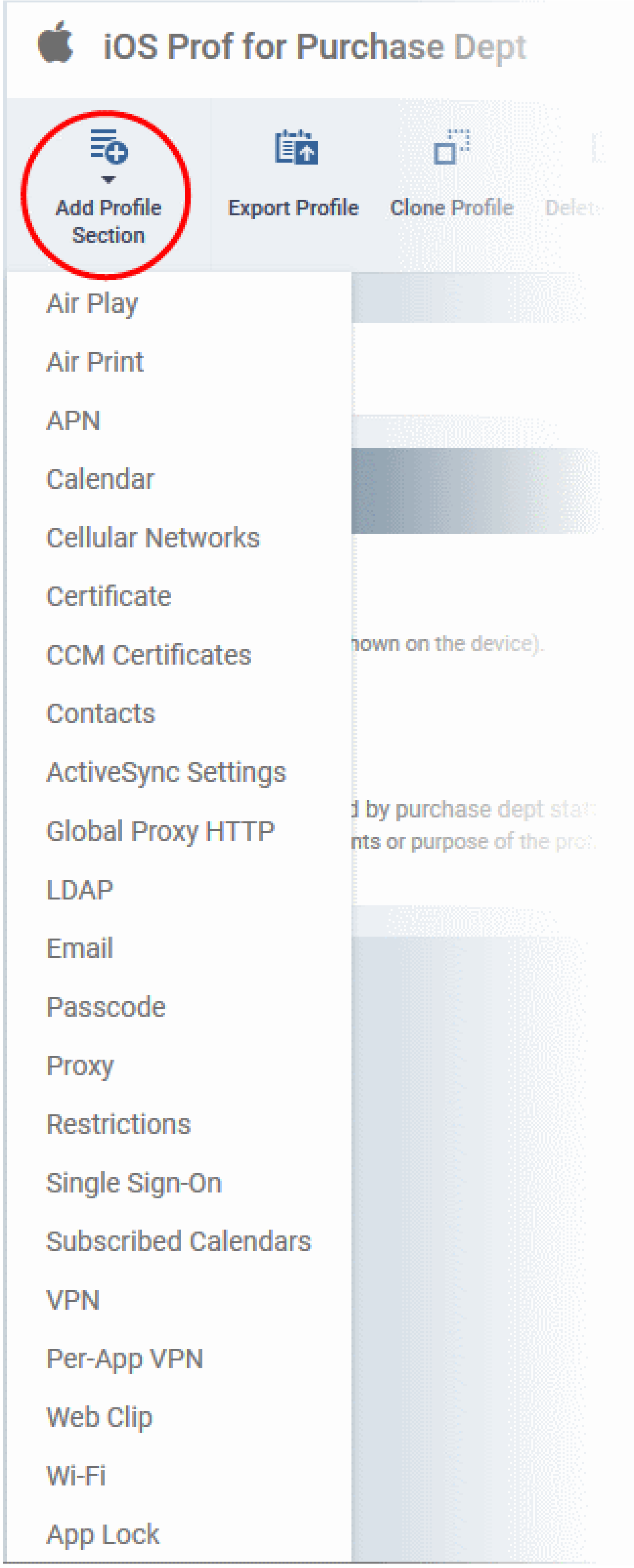
Is Default
Disabled

Description
For iPhones and iPads used by purchase department staff
Brief explanation of the contents or purpose of the profile

- 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

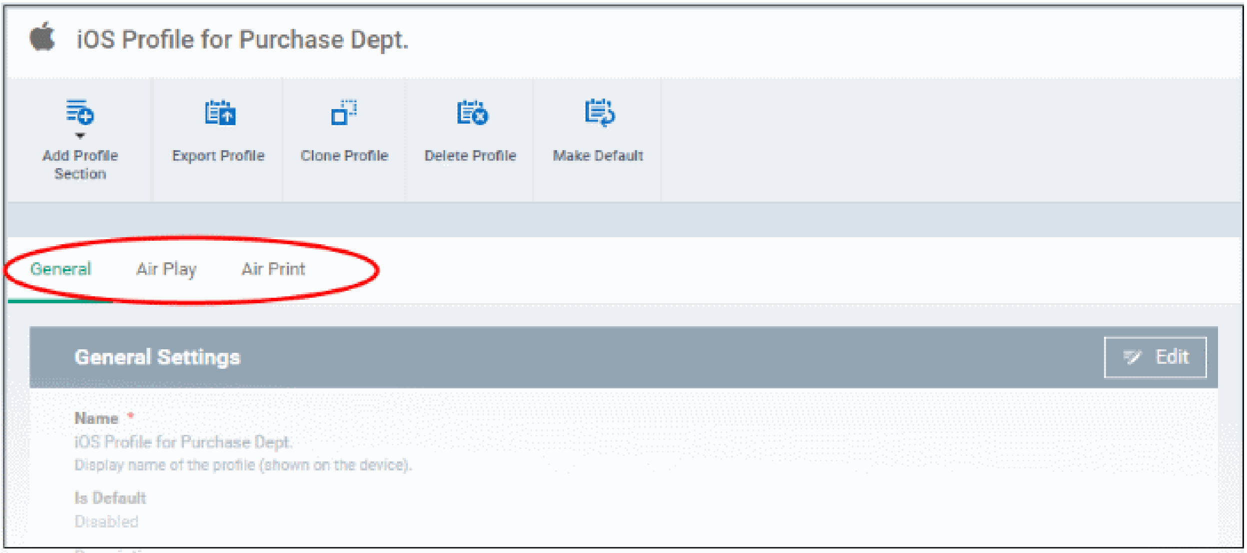


Note: Many iOS profile settings have small information boxes next to them which indicate the iOS version required for the setting to work correctly.

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.



Name *
iOS Profile for Purchase Dept.
Display name of the profile (shown on the device).

Is Default
Disabled

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
- Per -App VPN
- Web Clip
- Wi-Fi
- App Lock

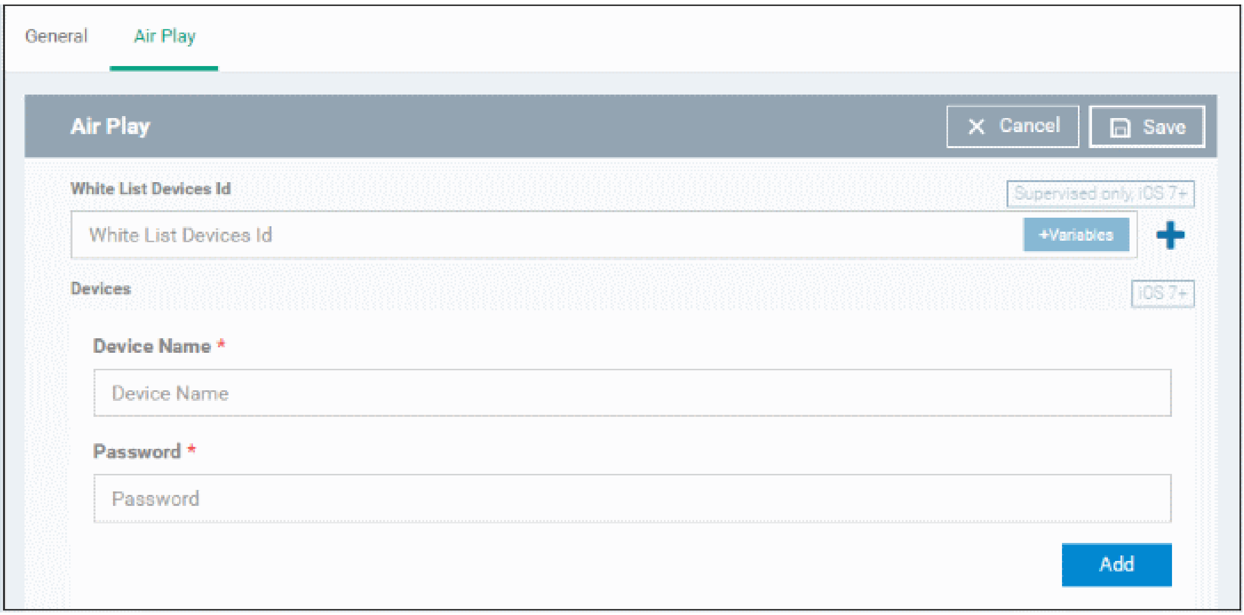
To configure AirPlay settings

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

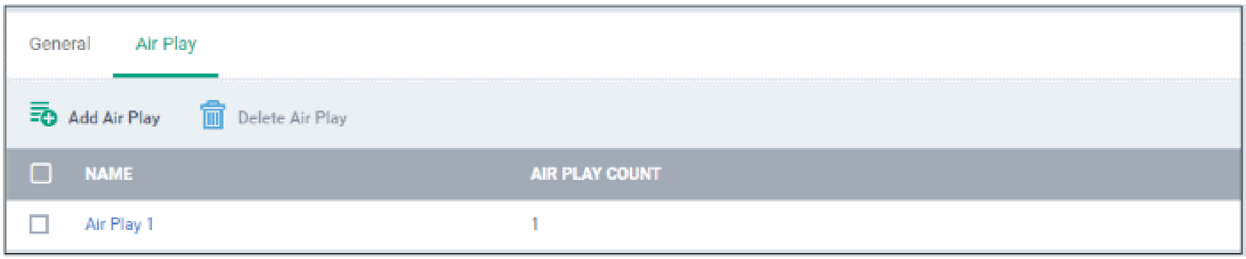
The 'Air Play' settings screen will be displayed.



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.



□	NAME	AIR PLAY COUNT
□	Air Play 1	1

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'

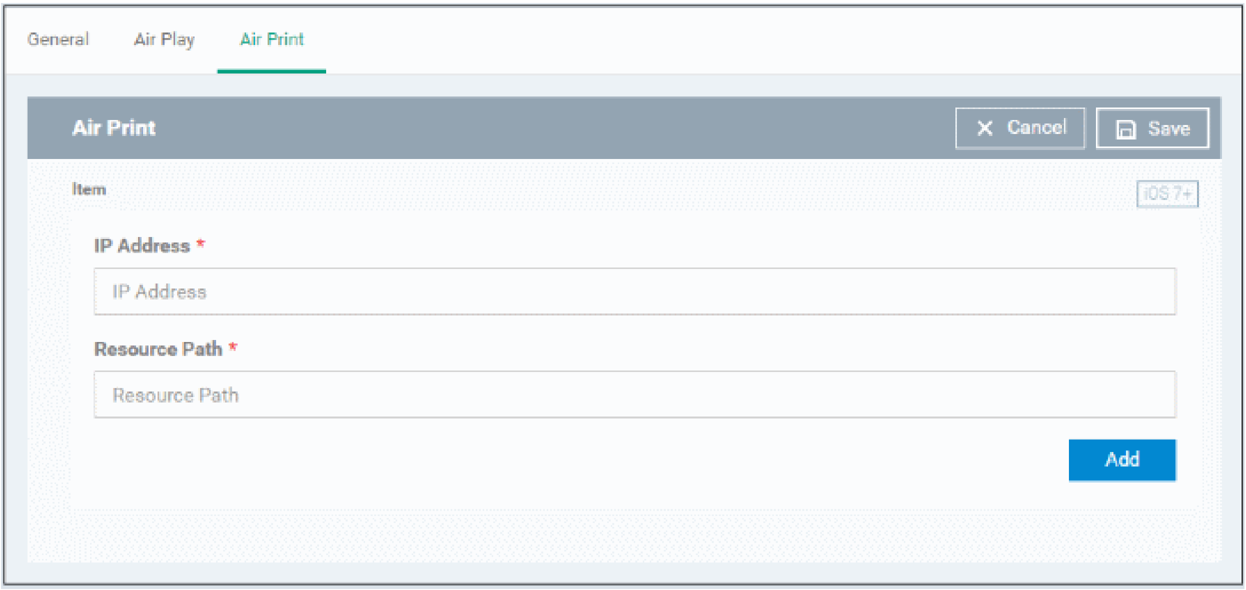
The settings will be saved and displayed under 'Air Play' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



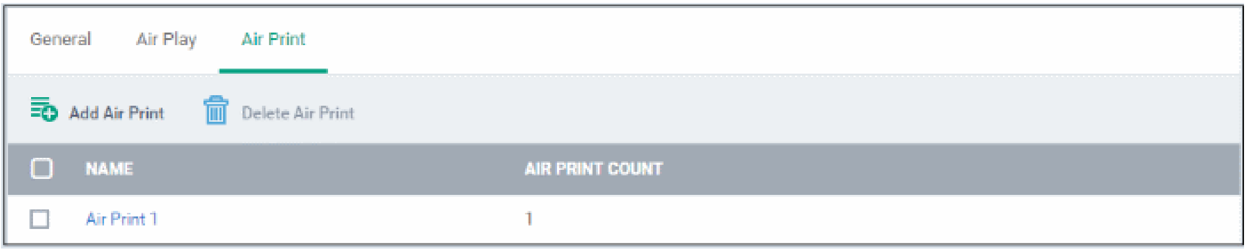
AirPrint Settings - Table of Parameters		
Form Element	**Type**	**Description**
IP Address	Text Field	Enter the IP Address of the AirPrint printer you wish to use.
Resource Path	Text Field	Enter the resource path of the printer, for example, printers/ HP_LaserJetPro_M1136_series.

AirPrint Settings - Table of Parameters		
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.



□	NAME	AIR PRINT COUNT
□	Air Print 1	1

- 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'

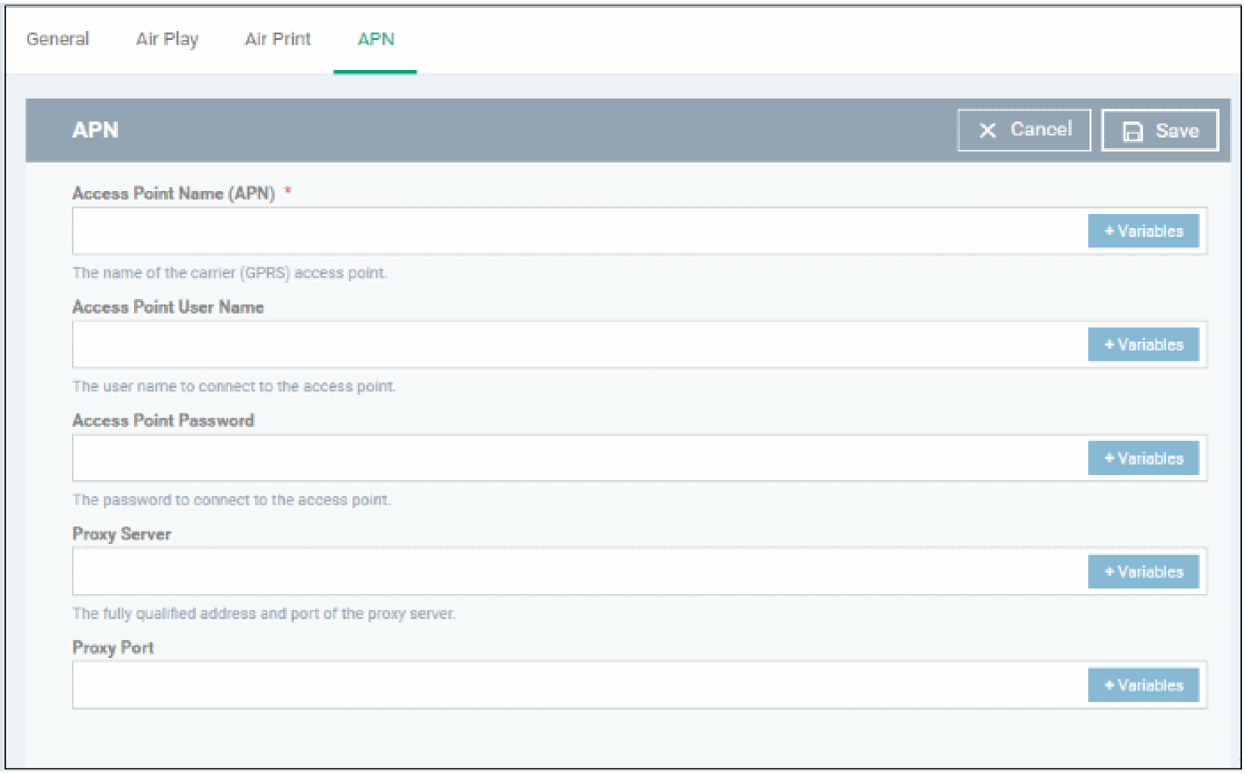
The settings will be saved and displayed under the 'Air Print' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



Access Point Name (APN) *

The name of the carrier (GPRS) access point.

Access Point User Name

The user name to connect to the access point.

Access Point Password

The password to connect to the access point.

Proxy Server

The fully qualified address and port of the proxy server.

Proxy Port

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.

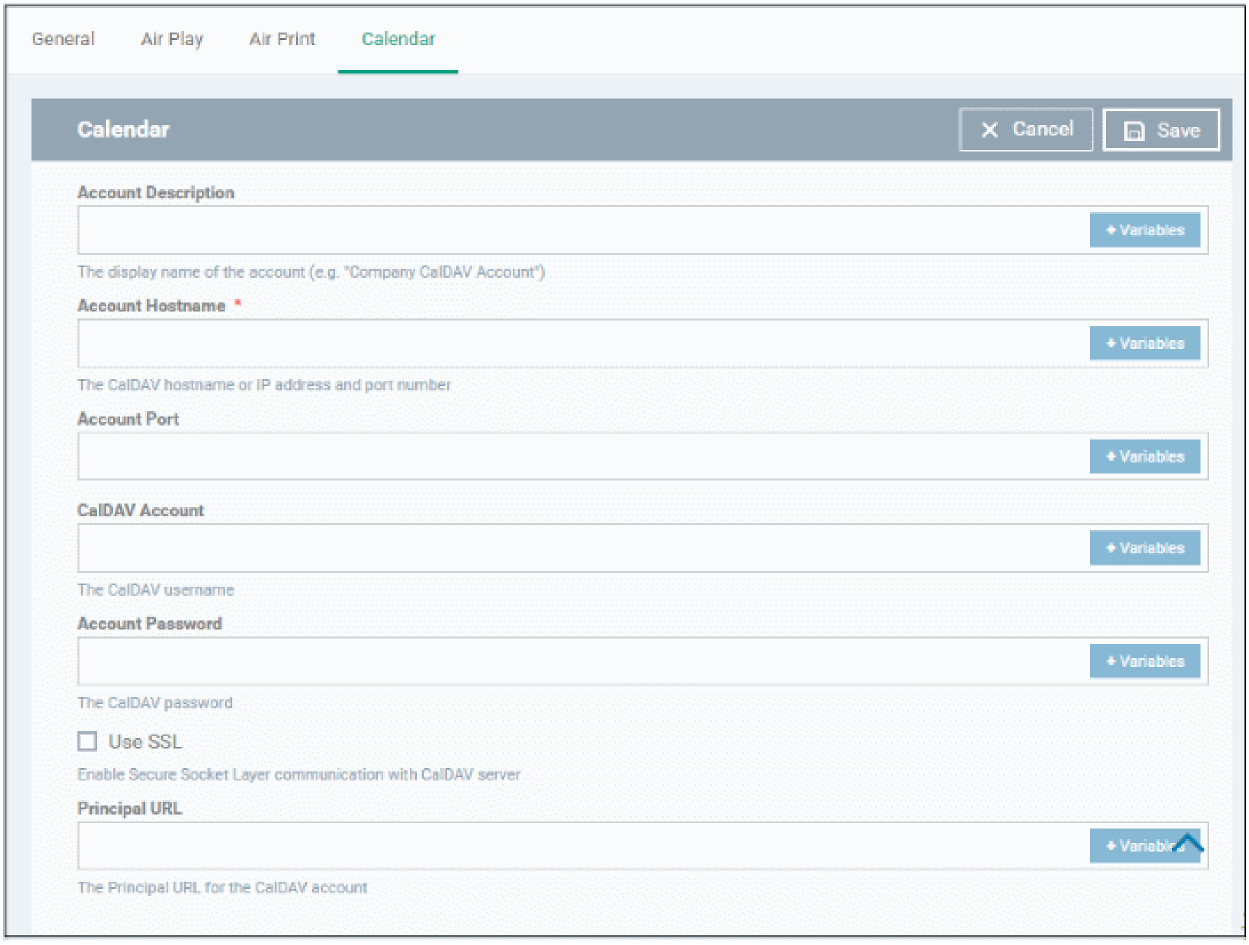
- Click the 'Save' button.

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.



Account Description

The display name of the account (e.g. "Company CalDAV Account")

Account Hostname *

The CalDAV hostname or IP address and port number

Account Port

CalDAV Account

The CalDAV username

Account Password

The CalDAV password

☐ Use SSL

Enable Secure Socket Layer communication with CalDAV server

Principal URL

The Principal URL for the CalDAV account

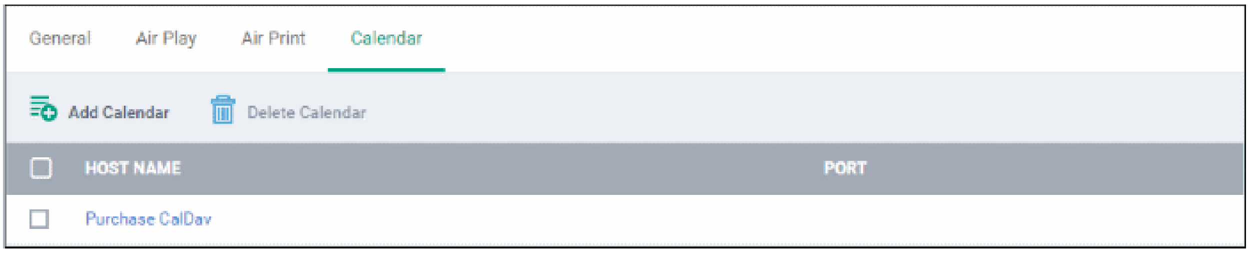
Calendar Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Description	Text Field	Enter the display name of the CalDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on 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.



□	HOST NAME	PORT
□	Purchase CalDav	

- 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'

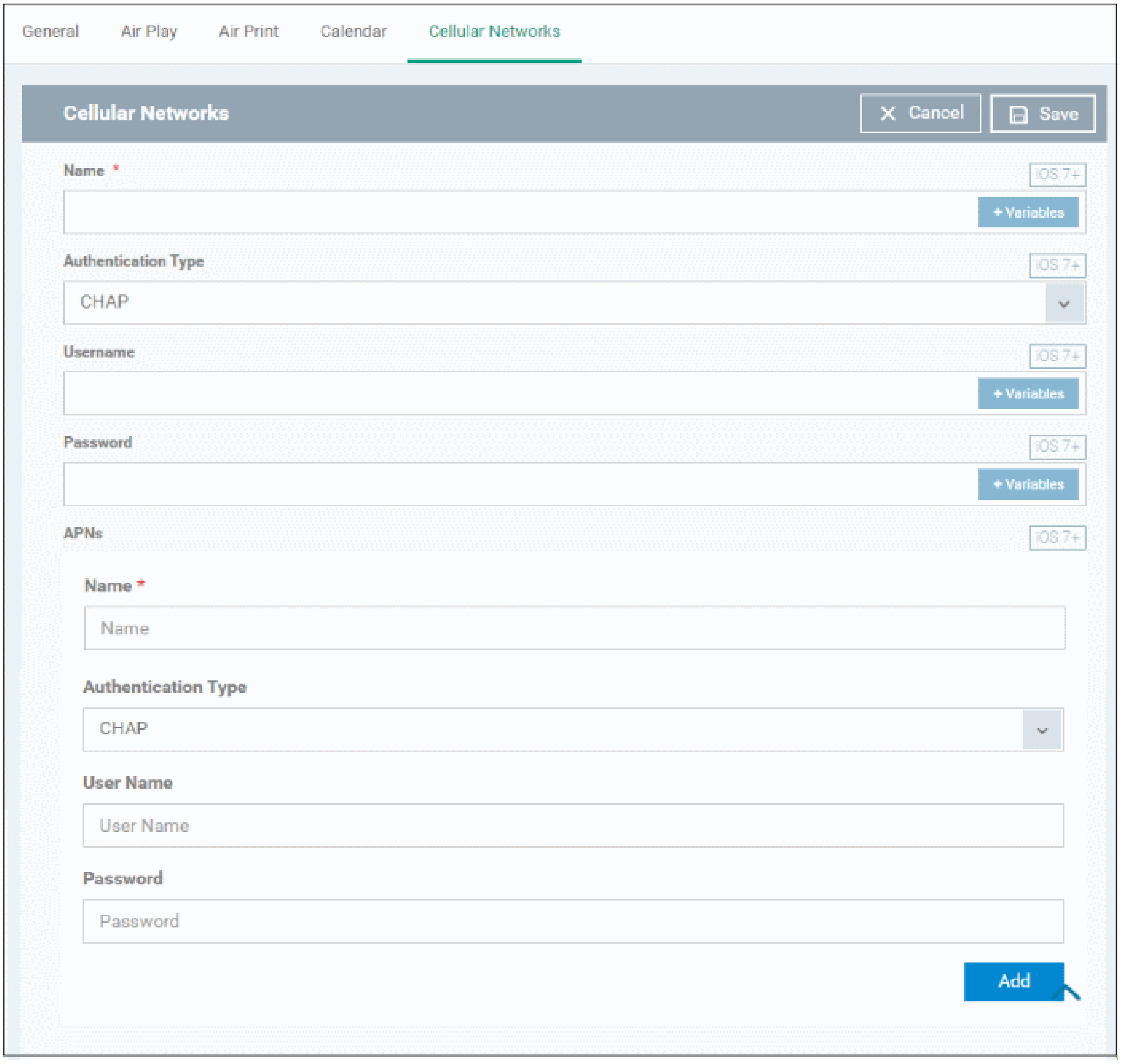
The settings will be saved and displayed under 'Calendar' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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.



General Air Play Air Print Calendar Cellular Networks

Cellular Networks ✕ Cancel Save

Name *

Authentication Type: CHAP

Username

Password

APNs

Name *

Authentication Type: CHAP

User Name

Password

Add

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.

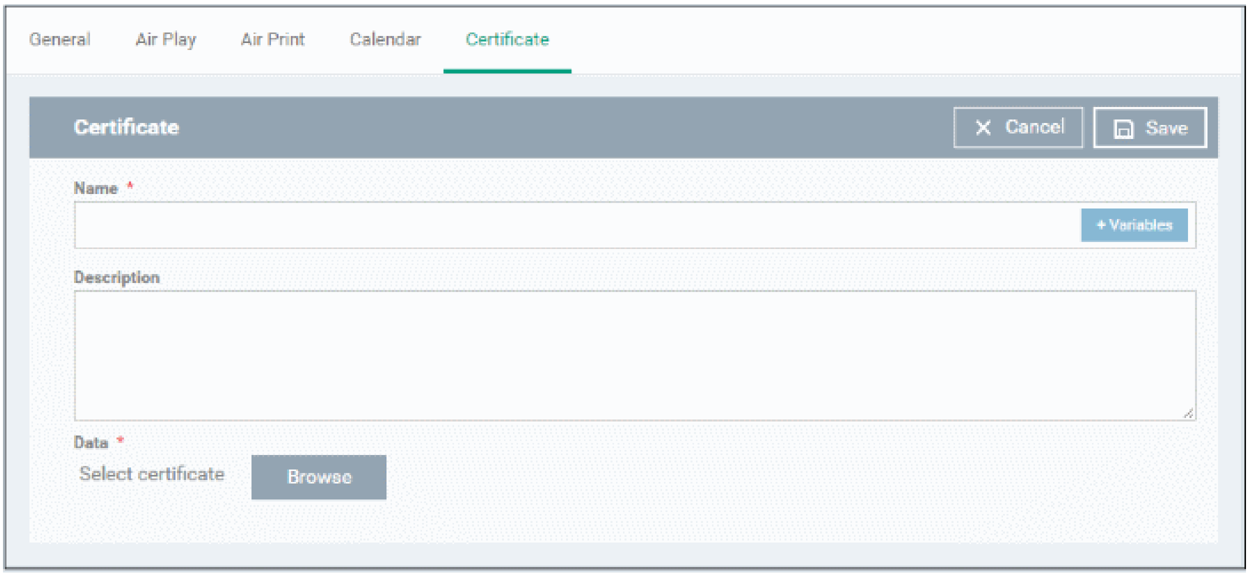
The settings will be saved and displayed under the 'Cellular Networks' tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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

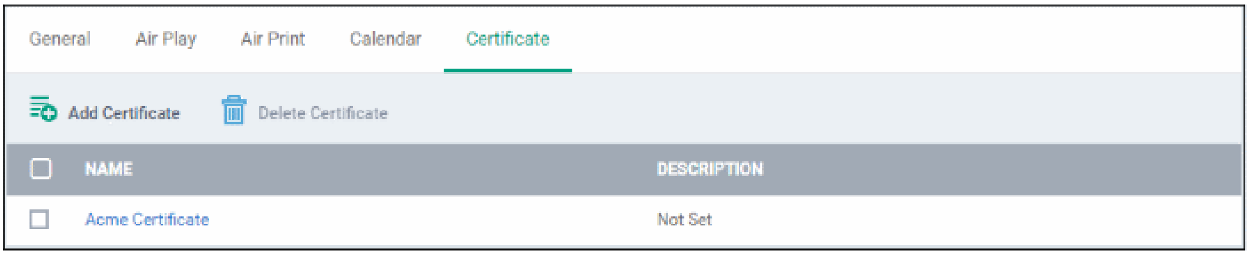
The 'Certificate' settings screen will be displayed.



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.



□	NAME	DESCRIPTION
□	Acme Certificate	Not Set

- 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.

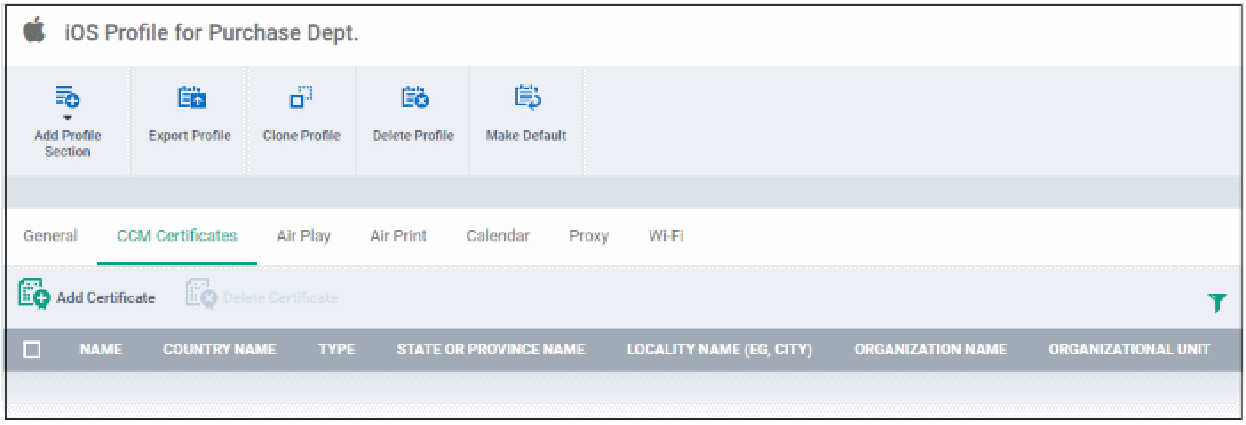
In addition to user authentication, client certificates can be used for email signing and encryption.

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

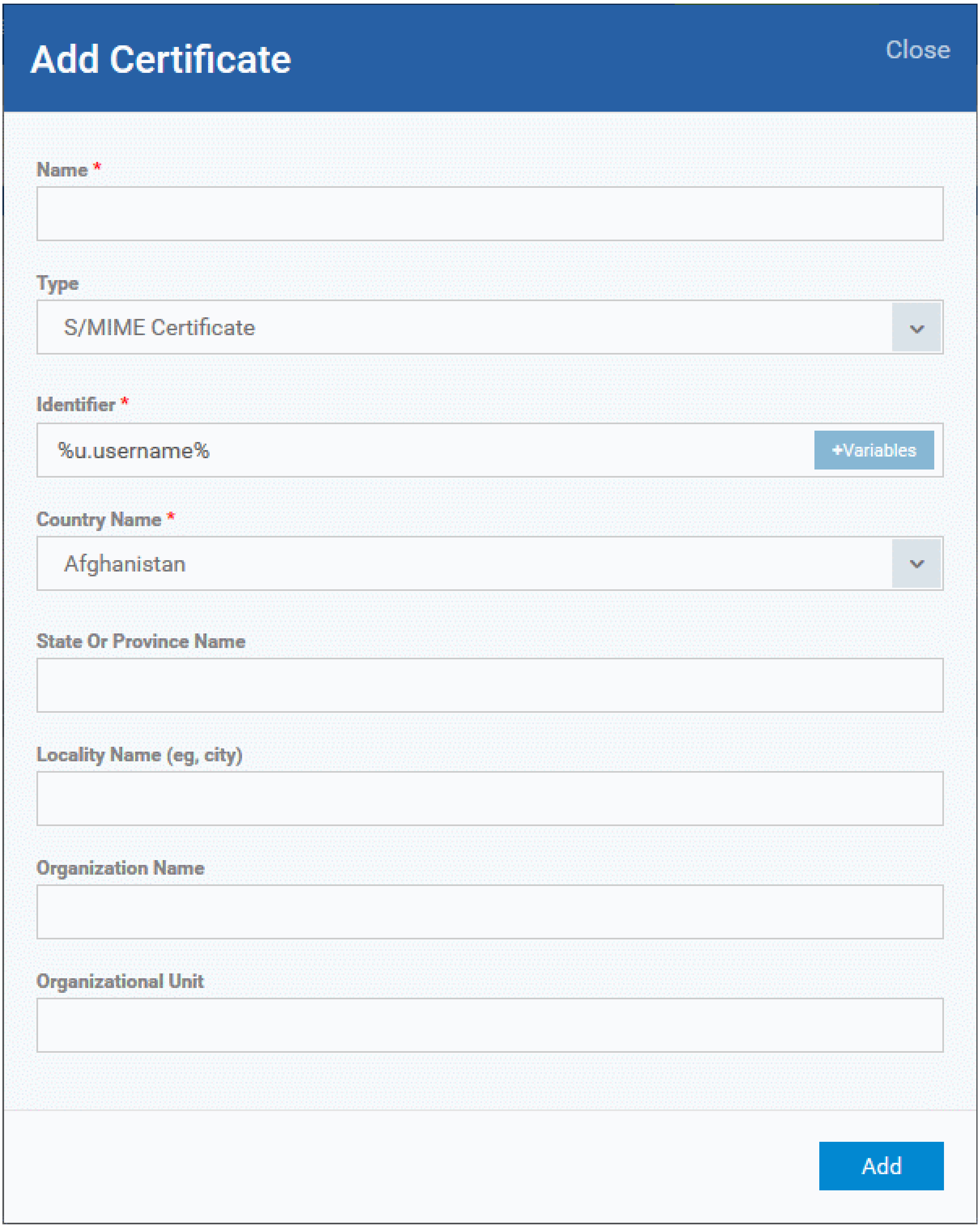
The settings screen for adding certificate requests to the profile will be displayed.



□	NAME	COUNTRY NAME	TYPE	STATE OR PROVINCE NAME	LOCALITY NAME (EG, CITY)	ORGANIZATION NAME	ORGANIZATIONAL UNIT

- Click 'Add Certificate' at the top to add a certificate request to the profile

The 'Add Certificate' form will appear.



Add Certificate

Close

Name *

Type: S/MIME Certificate

Identifier *: %u.username%

Country Name *: Afghanistan

State Or Province Name

Locality Name (eg, city)

Organization Name

Organizational Unit

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.

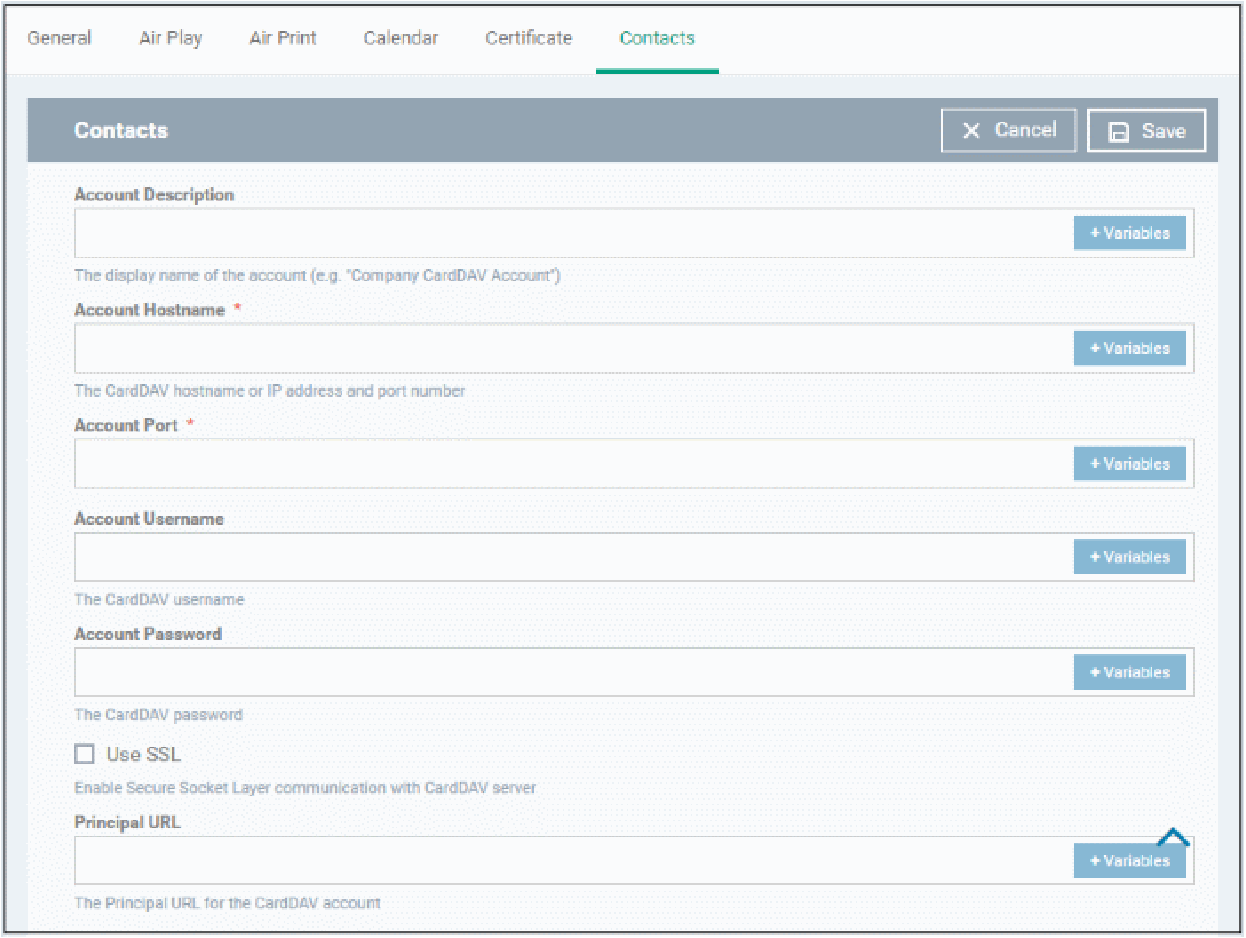
- Click 'Add' once you have completed the form.
- Repeat the process to add more certificate requests.

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.



Account Description

The display name of the account (e.g. "Company CardDAV Account")

Account Hostname *

The CardDAV hostname or IP address and port number

Account Port *

Account Username

The CardDAV username

Account Password

The CardDAV password

□ Use SSL

Enable Secure Socket Layer communication with CardDAV server

Principal URL

The Principal URL for the CardDAV account

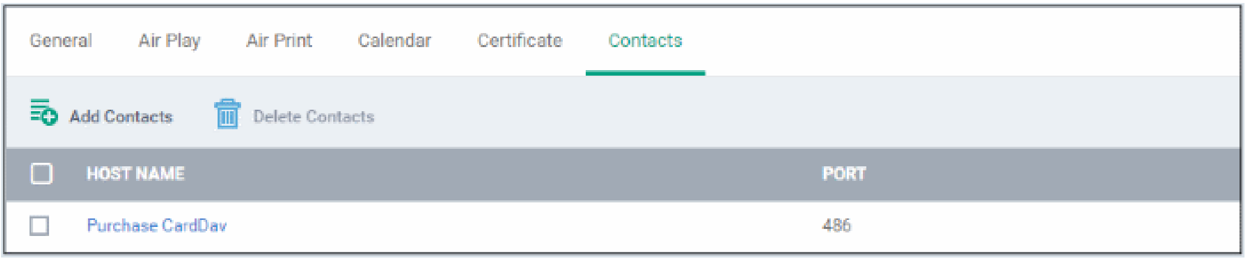
Contacts Settings - Table of Parameters		
Form Element	**Type**	**Description**
Account Description	Text Field	Enter the display name of the CardDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details 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.



□	HOST NAME	PORT
□	Purchase CardDav	486

You can add multiple CardDav accounts to the profile.

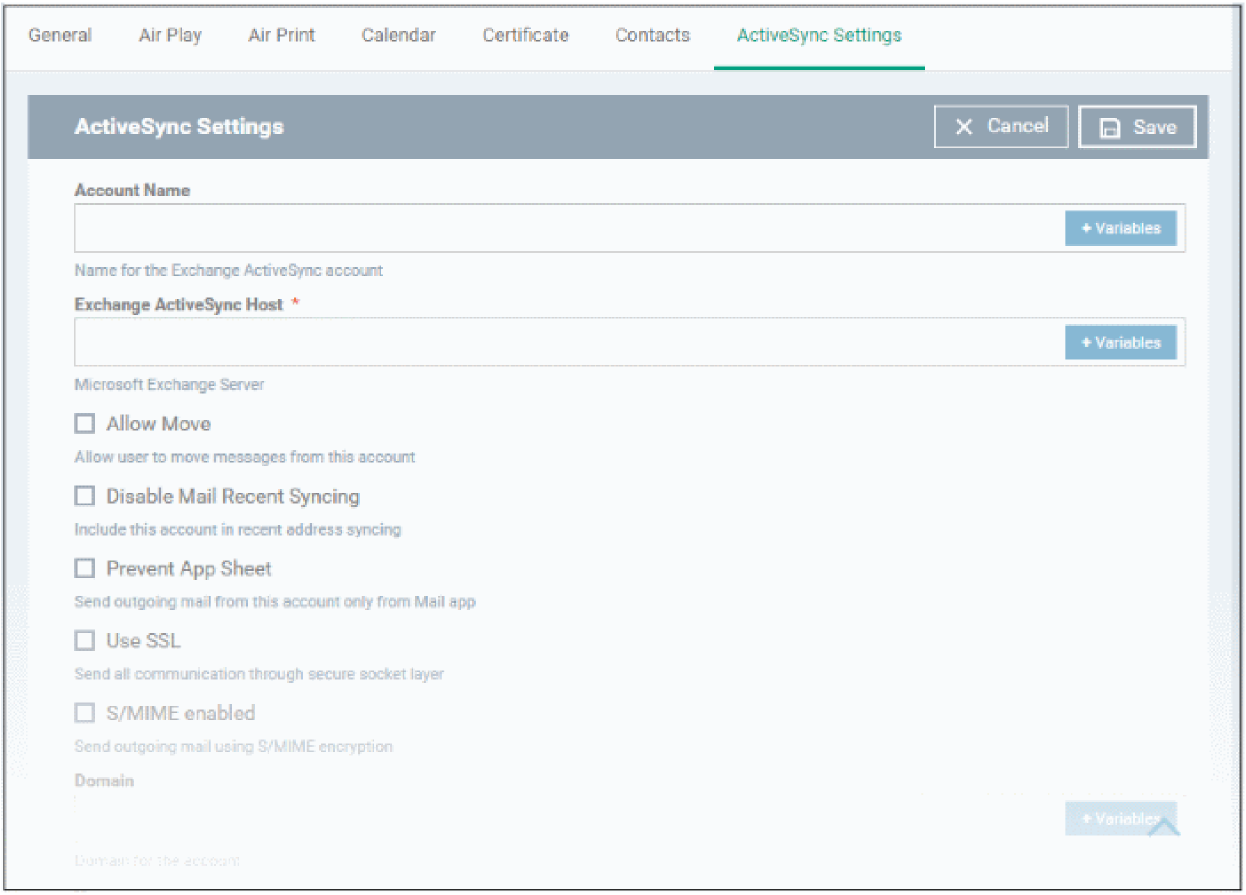
- To add another account, click 'Add Contacts' and repeat the process
- To view or edit a contact account, click on the Hostname of the contact account
- To remove a contact account, select it and click 'Delete Contacts'

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

Account Name

Name for the Exchange ActiveSync account

Exchange ActiveSync Host *

Microsoft Exchange Server

☐ Allow Move

Allow user to move messages from this account

☐ Disable Mail Recent Syncing

Include this account in recent address syncing

☐ Prevent App Sheet

Send outgoing mail from this account only from Mail app

☐ Use SSL

Send all communication through secure socket layer

☐ S/MIME enabled

Send outgoing mail using S/MIME encryption

Domain

Domain for the account

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.

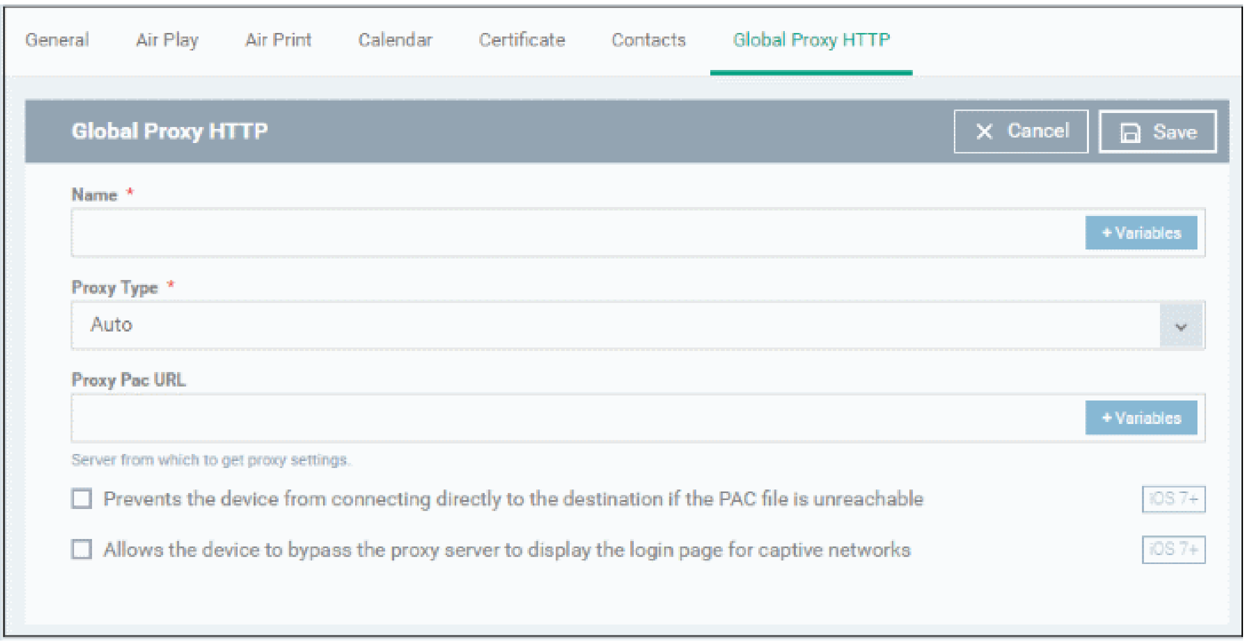
- Click the 'Save' button.

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.



General | Air Play | Air Print | Calendar | Certificate | Contacts | Global Proxy HTTP

Global Proxy HTTP

✕ Cancel | Save

Name *

+Variables

Proxy Type *

Auto

Proxy Pac URL

+Variables

Server from which to get proxy settings.

□ Prevents the device from connecting directly to the destination if the PAC file is unreachable iOS 7+

□ Allows the device to bypass the proxy server to display the login page for captive networks iOS 7+

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**.

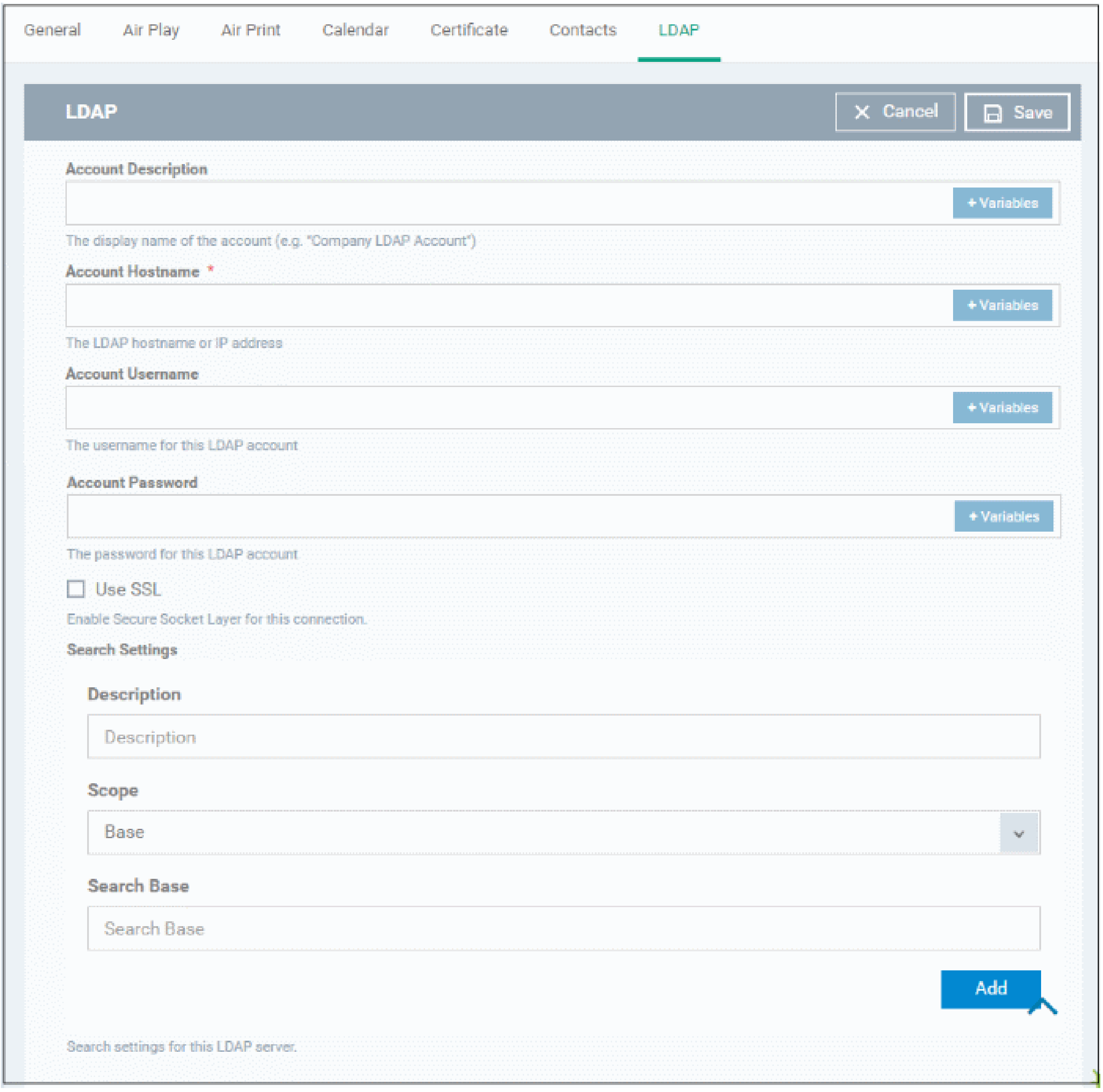
- Click the 'Save' button.

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.



Account Description

The display name of the account (e.g. "Company LDAP Account")

Account Hostname *

The LDAP hostname or IP address

Account Username

The username for this LDAP account

Account Password

The password for this LDAP account

□ Use SSL

Enable Secure Socket Layer for this connection.

Search Settings

Description: Description

Scope: Base

Search Base: Search Base

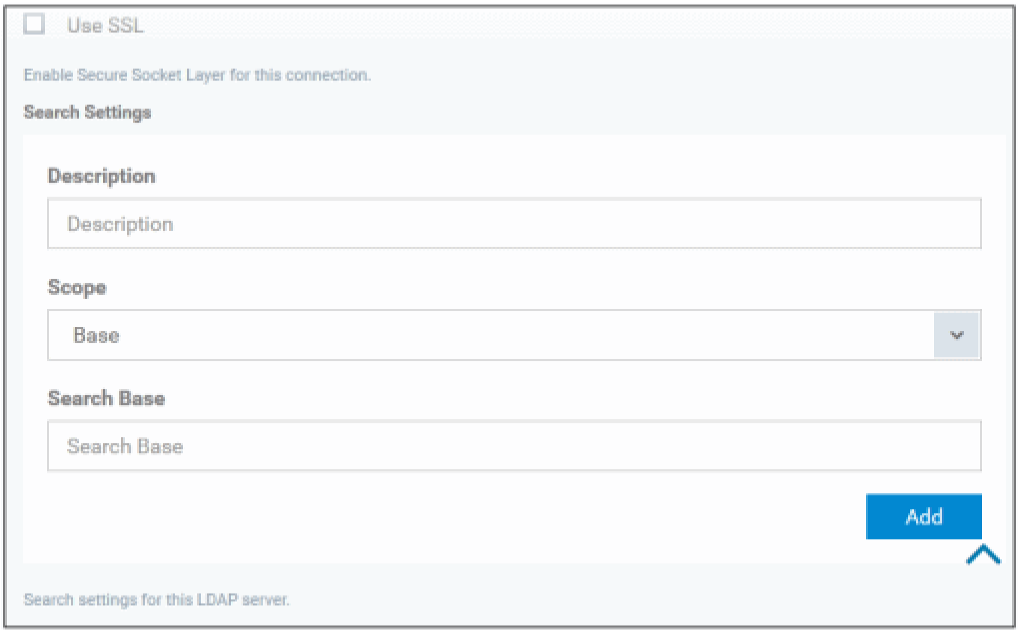
Search settings for this LDAP server.

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**.

LDAP Settings - Table of Parameters		
Account Username	Text Field	The username 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**.
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.



□ Use SSL

Enable Secure Socket Layer for this connection.

Search Settings

Description

Description

Scope

Base

Search Base

Search Base

Search settings for this LDAP server.

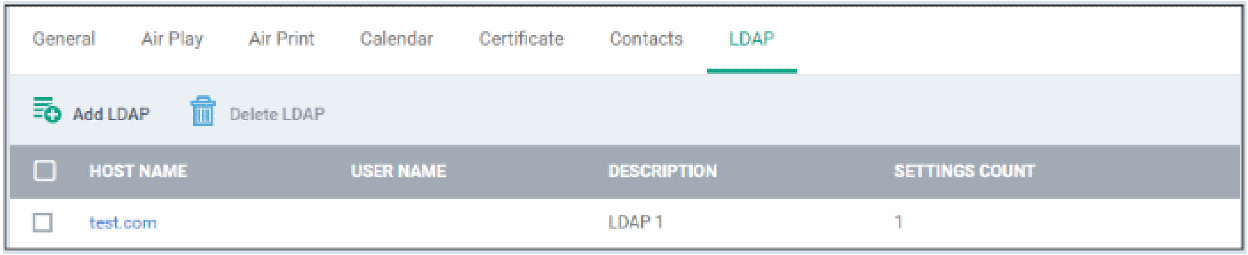
LDAP Search Settings - Table of Parameters		
Form Element	**Type**	**Description**
Description	Text Field	Enter the name of the search
Scope	Drop-down	Select from the drop-down to what level in the LDAP tree structure the search should run. • Base - Searches only the defined search base. • One level - 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

LDAP Search Settings - Table of Parameters		
		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.



□	HOST NAME	USER NAME	DESCRIPTION	SETTINGS COUNT
□	test.com		LDAP 1	1

You can add multiple LDAP accounts.

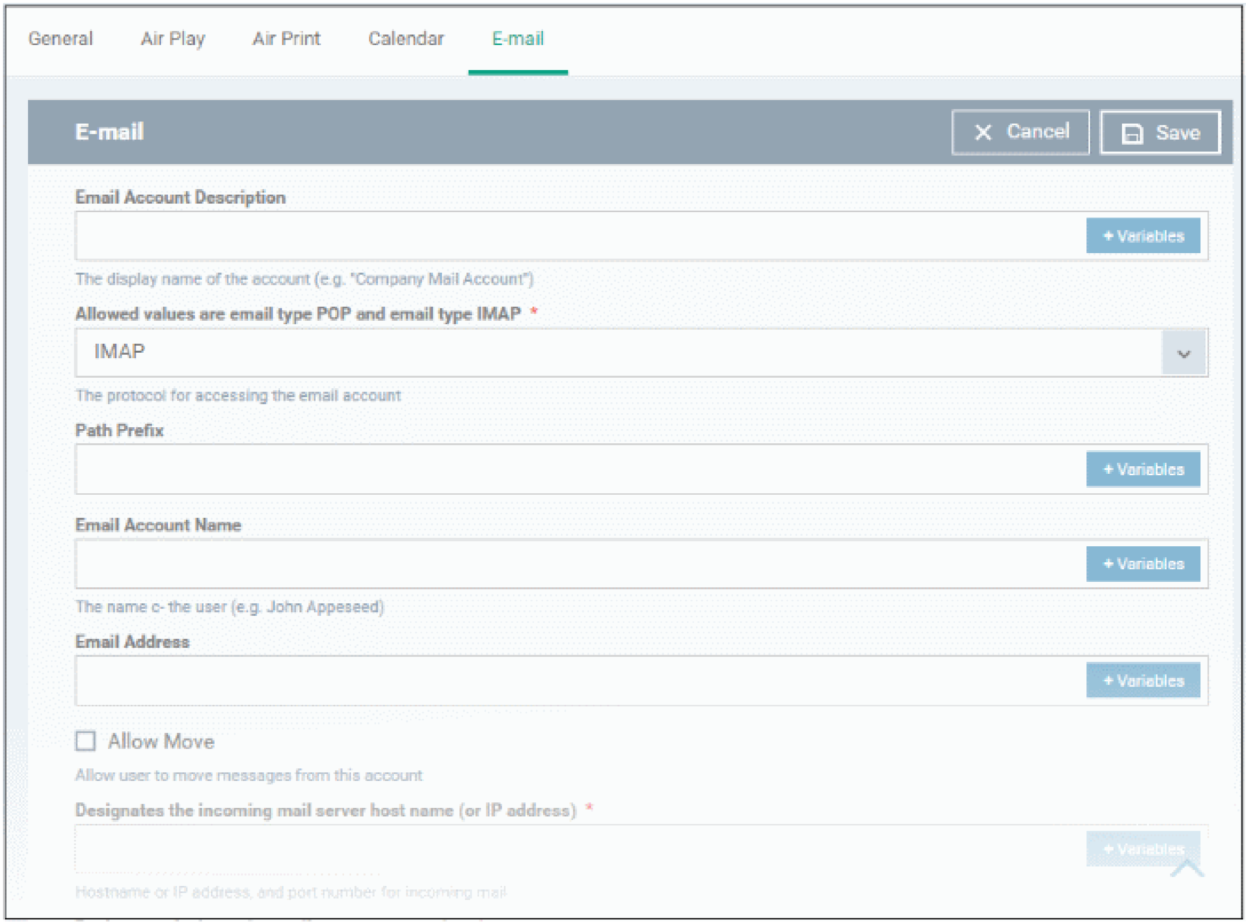
- To add another LDAP server, click 'Add LDAP' and repeat the process
- To view and edit the settings of an LDAP account, click the hostname of it
- To remove an LDAP account, select it and click 'Delete LDAP'

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.



Email Account Description

The display name of the account (e.g. "Company Mail Account")

Allowed values are email type POP and email type IMAP *

IMAP

The protocol for accessing the email account

Path Prefix

Email Account Name

The name c- the user (e.g. John Appeseed)

Email Address

□ Allow Move

Allow user to move messages from this account

Designates the incoming mail server host name (or IP address) *

Hostname or IP address, and port number for incoming mail

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

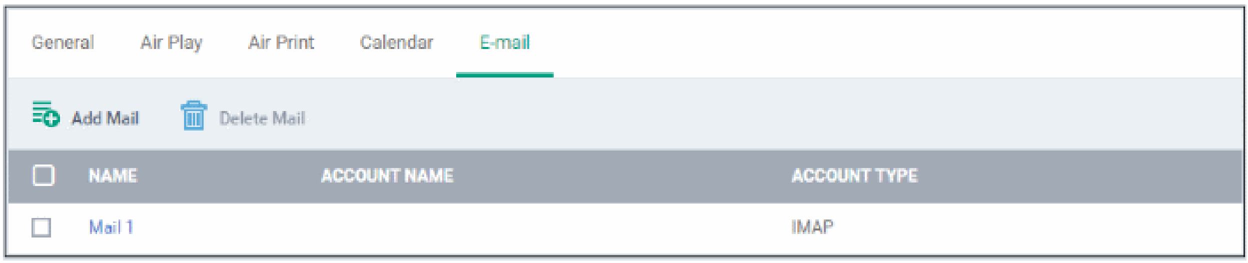
Mail Account Settings - Table of Parameters

		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.



□	NAME	ACCOUNT NAME	ACCOUNT TYPE
□	Mail 1		IMAP

You can add several email accounts to the same profile.

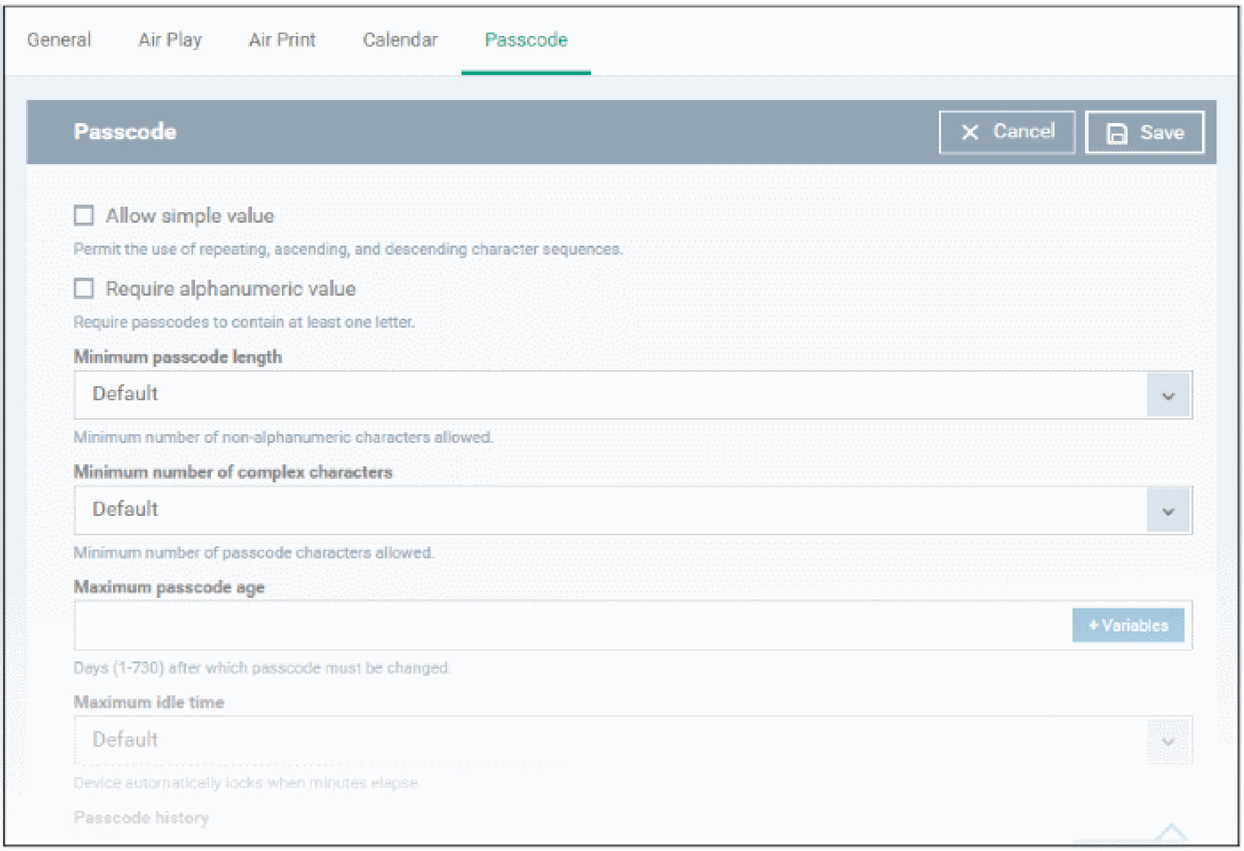
- To add another email account, click 'Add Mail' and repeat the process
- To view and edit the settings for an email account, click on its name
- To remove an email account, select it and click 'Delete Mail'

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.



□ Allow simple value

Permit the use of repeating, ascending, and descending character sequences.

□ Require alphanumeric value

Require passcodes to contain at least one letter.

Minimum passcode length: Default

Minimum number of non-alphanumeric characters allowed.

Minimum number of complex characters: Default

Minimum number of passcode characters allowed.

Maximum passcode age

Days (1-730) after which passcode must be changed.

Maximum idle time: Default

Device automatically locks when minutes elapse.

Passcode history

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.

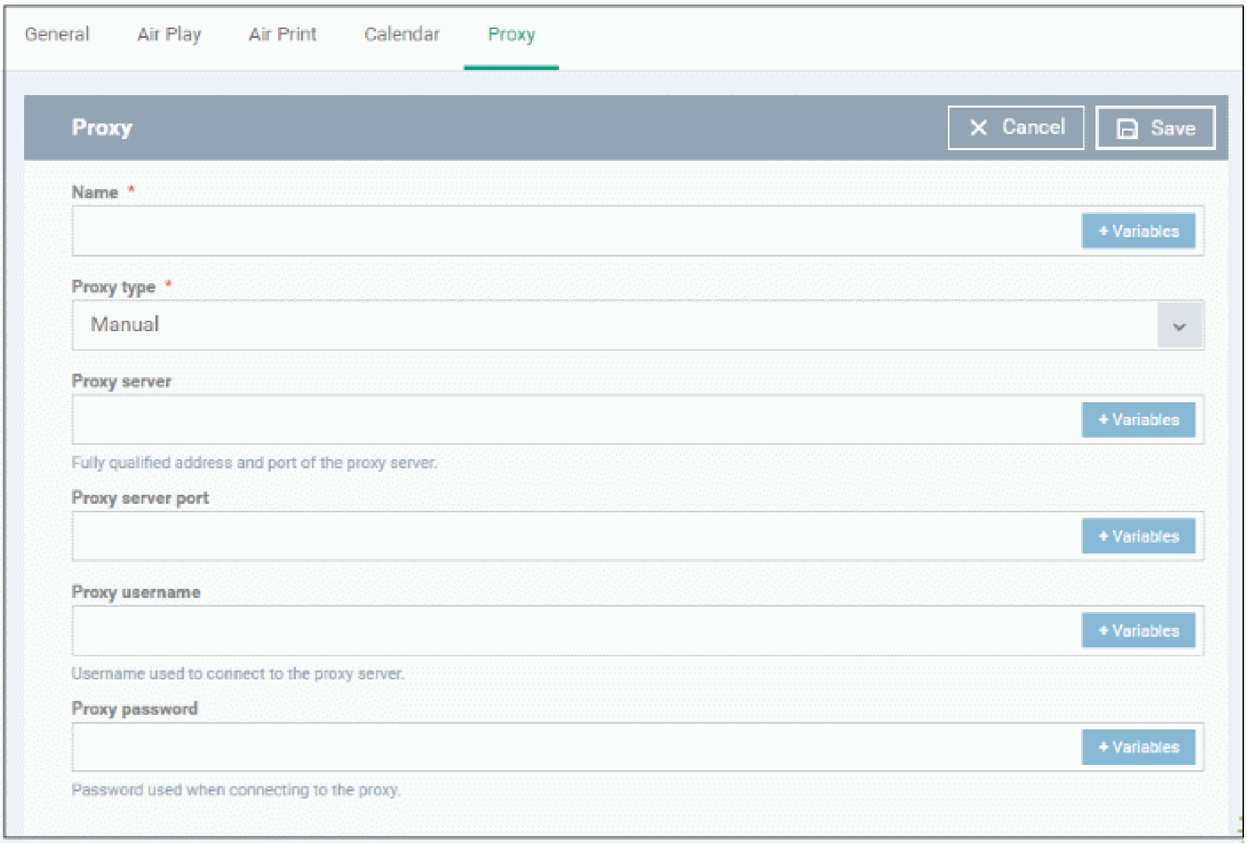
- Click the 'Save' button.

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

Name *

Proxy type *
Manual

Proxy server
Fully qualified address and port of the proxy server.

Proxy server port

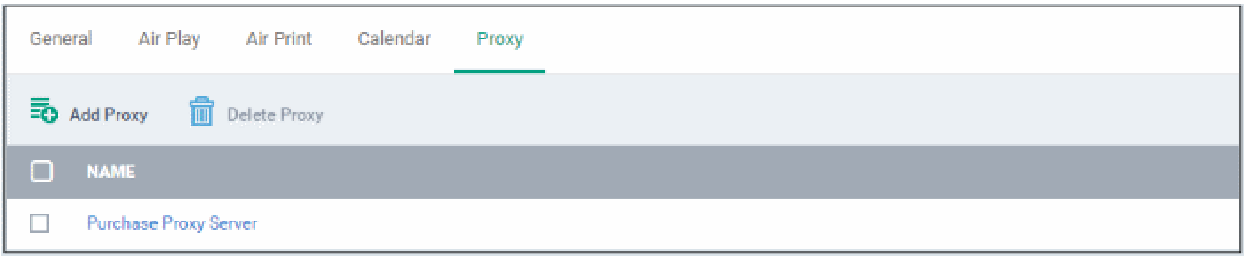
Proxy username
Username used to connect to the proxy server.

Proxy password
Password used when connecting to the proxy.

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.



□	NAME
□	Purchase Proxy Server

You can add more proxy server accounts to the profile.

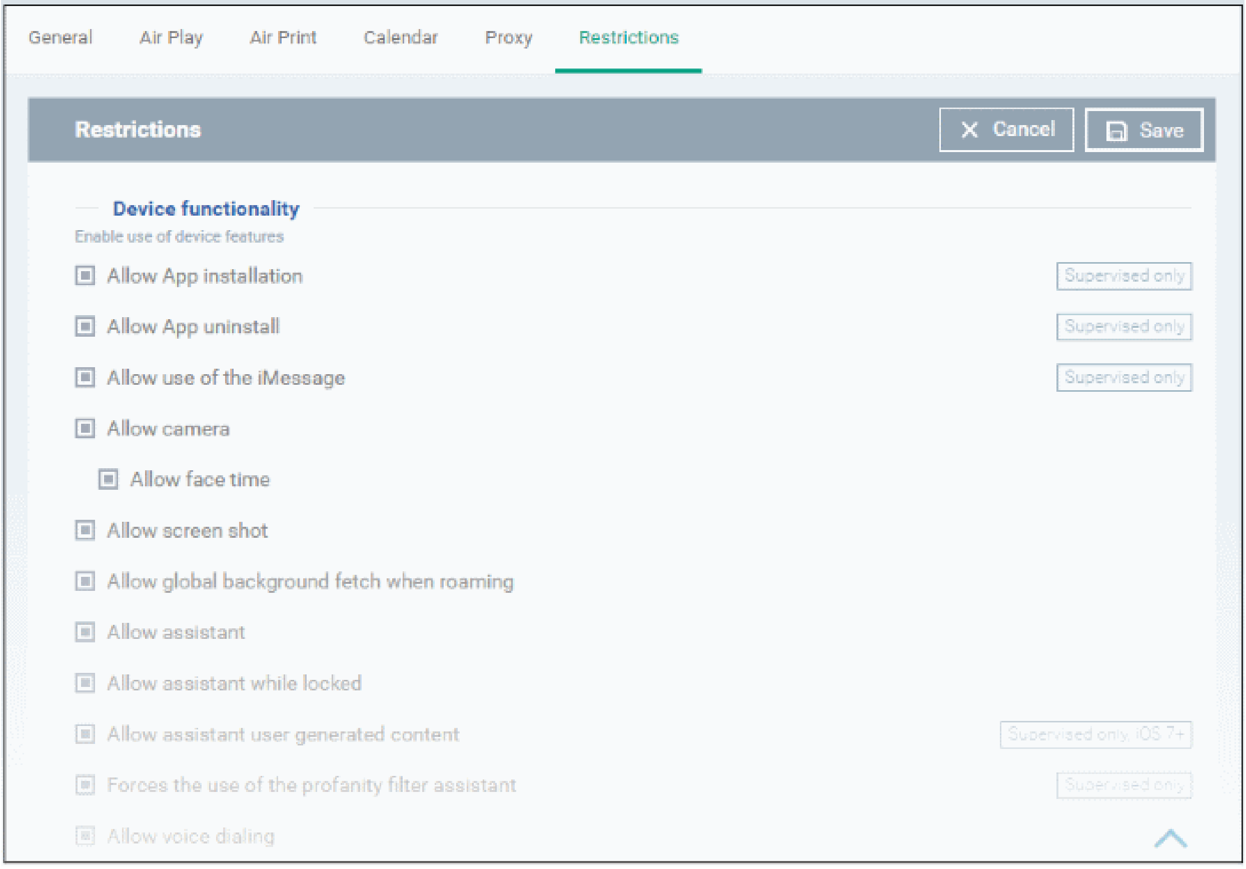
- To add another proxy server account, click 'Add Proxy' and repeat the process
- To view or edit a proxy server account, click on its name
- To remove a proxy server account, select it then click 'Delete Proxy'

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.



Device functionality

Enable use of device features

- ☒ Allow App installation — Supervised only
- ☒ Allow App uninstall — Supervised only
- ☒ Allow use of the iMessage — Supervised only
- ☒ Allow camera
  - ☒ Allow face time
- ☒ Allow screen shot
- ☒ Allow global background fetch when roaming
- ☒ Allow assistant
- ☒ Allow assistant while locked
- ☒ Allow assistant user generated content — Supervised only, iOS 7+
- ☒ Forces the use of the profanity filter assistant — Supervised only
- ☒ Allow voice dialing

Restrictions Settings - Table of Parameters		
Device Functionality		
Form Element	**Type**	**Description**
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.

Restrictions Settings - Table of Parameters		
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.
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.

Restrictions Settings - Table of Parameters		
Allow backed up Enterprise books	Checkbox	If enabled, users can backup iBooks and restrict synchronization to iCloud.
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	Checkbox	If enabled, allows the user to pair the device with an Apple Watch.

Restrictions Settings - Table of Parameters		
Watch		Note: This feature is available only for Supervised devices with iOS 9.0 and later versions.
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 bundle ID of the application to be added to the whitelist. For more details on obtaining the App bundle 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**.

Restrictions Settings - Table of Parameters		
		• 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.
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 bundle ID of the application to be added to the blacklist. For more details on obtaining the App bundle 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

Restrictions Settings - Table of Parameters		
		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		
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 bundle 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 bundle IDs. • Enter the App bundle ID of the application to be permitted for autonomous single app mode. For more details on obtaining the App bundle ID, refer to the **explanation** at the end of this section.

Restrictions 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**. • 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 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.

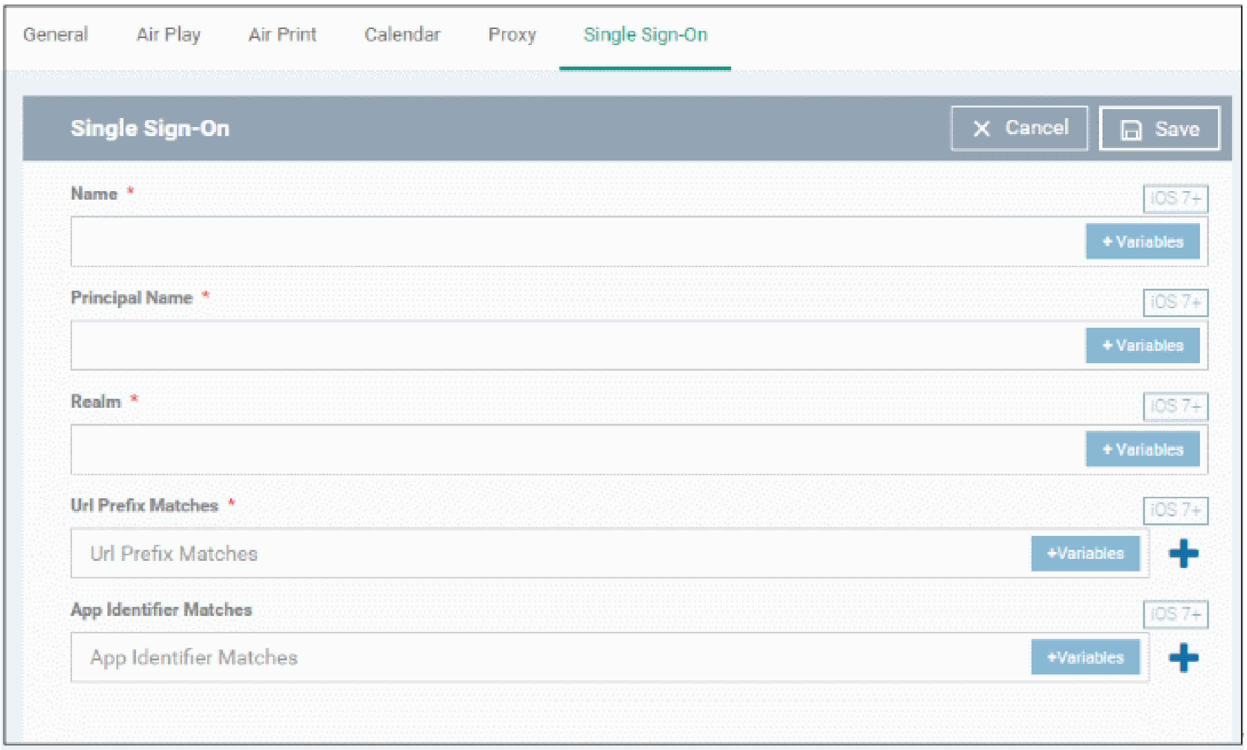
The saved 'Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

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.

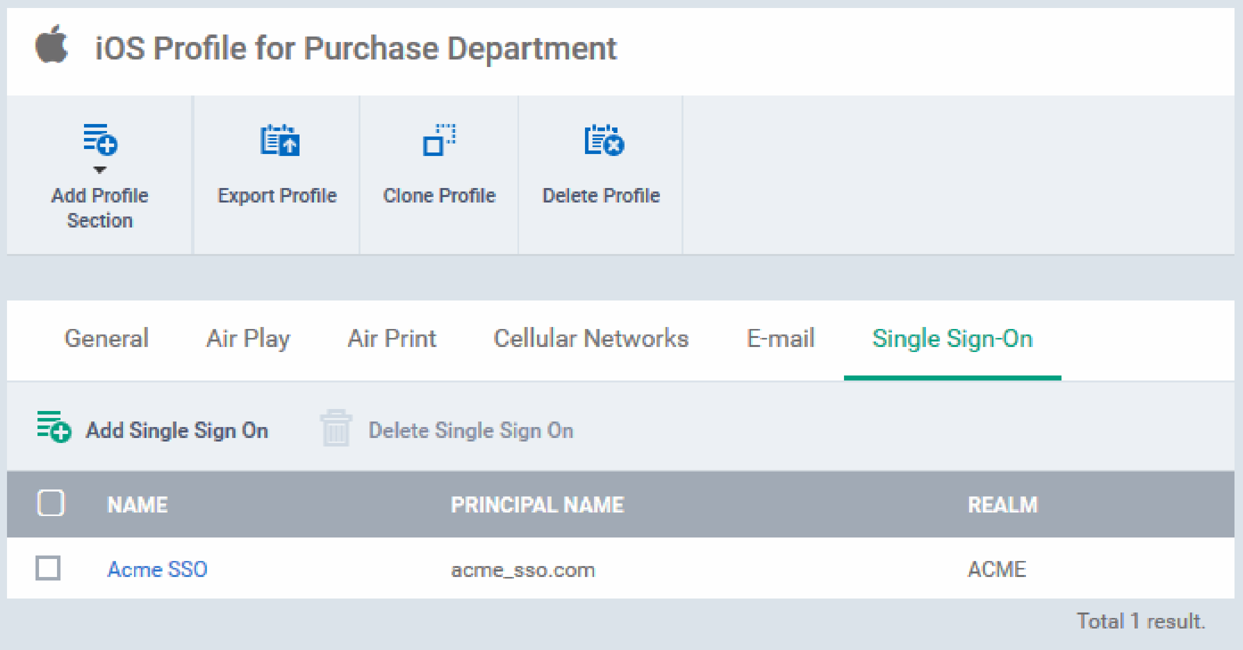


Single Sign-On Settings - Table of Parameters		
Form Element	**Type**	**Description**
Name*	Text Field	Enter the name for the account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to 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	Text Field	Enter the bundle IDs of apps that are allowed to use this Single Sign-On

Single Sign-On Settings - Table of Parameters		
matches		account for logging-in to respective account. If this field is left blank, this login matches all app bundle IDs. 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.


iOS Profile for Purchase Department

□	NAME	PRINCIPAL NAME	REALM
□	Acme SSO	acme_sso.com	ACME

Total 1 result.

You can add several SSO accounts to the profile.

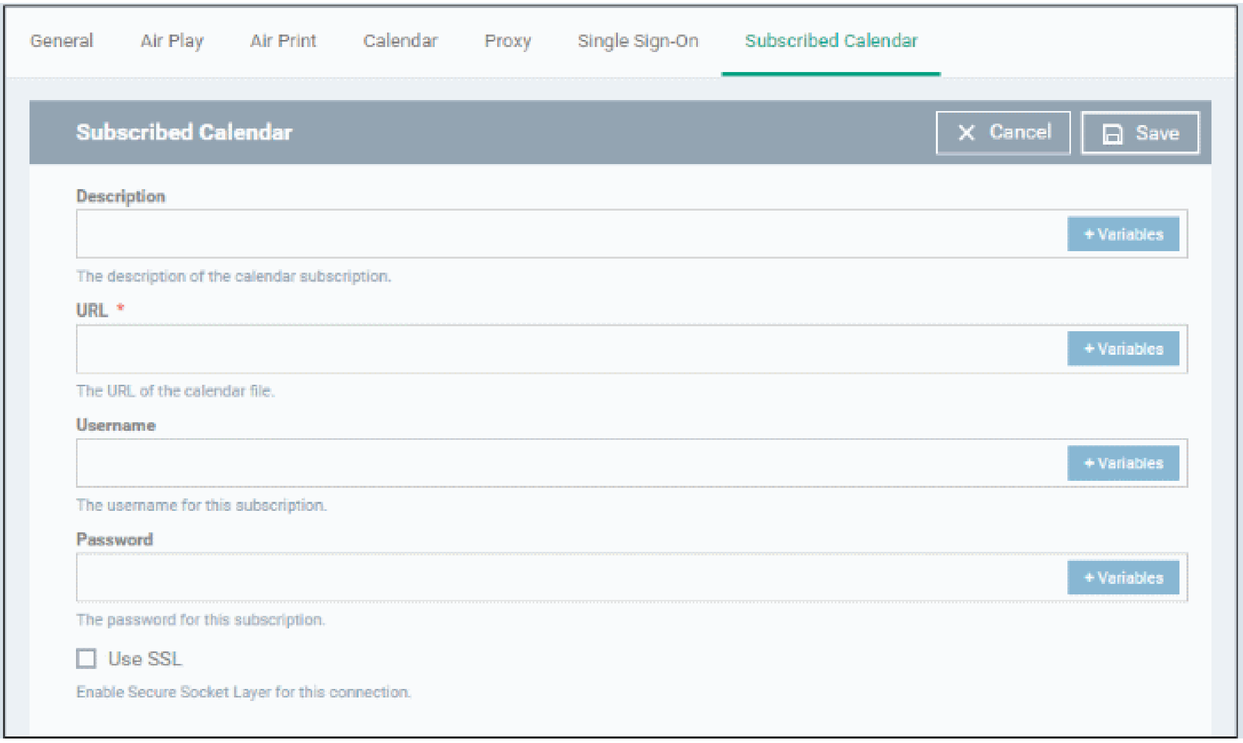
- To add another SSO account, click 'Add Single Sign-On' and repeat the process
- To view and edit an SSO account, click the name of it
- To remove an SSO account, select it then click 'Delete Single Sign-On'

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 Calendar

Description

The description of the calendar subscription.

URL *

The URL of the calendar file.

Username

The username for this subscription.

Password

The password for this subscription.

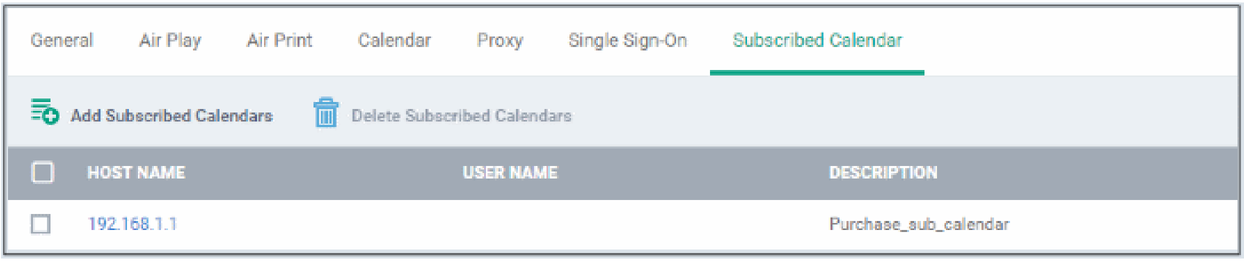
□ Use SSL

Enable Secure Socket Layer for this connection.

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.



□	HOST NAME	USER NAME	DESCRIPTION
□	192.168.1.1		Purchase_sub_calendar

You can add several calendar accounts for a profile.

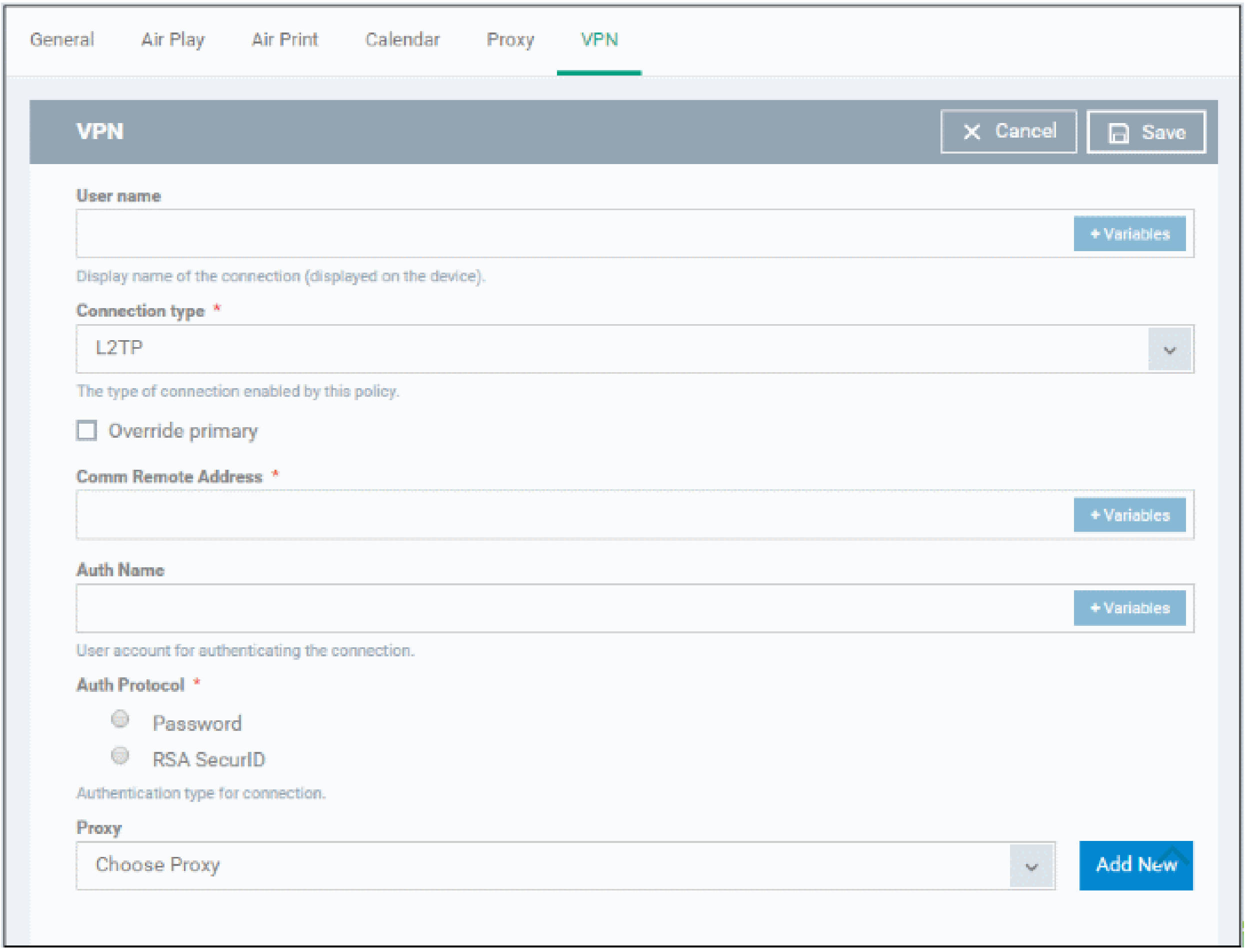
- To add another Subscribed Calendar account, click 'Add Subscribed Calendar' and repeat the process
- To view and edit a calendar account, click the Hostname of it
- To remove a calendar account, select it and click 'Delete Subscribed Calendar'

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.



User name

Display name of the connection (displayed on the device).

Connection type *

L2TP

The type of connection enabled by this policy.

□ Override primary

Comm Remote Address *

Auth Name

User account for authenticating the connection.

Auth Protocol *

○ Password

○ RSA SecurID

Authentication type for connection.

Proxy

Choose Proxy

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'.

VPN Connection Type Settings - Table of Parameters	
	• 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 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

<table>
<tr><th colspan="2">VPN Connection Type Settings - Table of Parameters</th></tr>
<tr><td></td><td>
variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add.
<ul>
<li>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.</li>
<li>Password - Enter the password for the account . You can add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable.</li>
<li>Authentication Method - Select the authentication method from the drop-down. The available options are:
<ul>
<li>Shared secret / Group name - If selected, enter the shared secret string and group name in the 'Shared secret' and 'Local identifier' fields.
<ul>
<li>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.</li>
</ul></li>
<li>Certificate - If you want client certificate type authentication, choose this option and configure the parameters as given below:
<ul>
<li>Password encryption - select this option if you want communications to be encrypted using the password as the key.</li>
<li>Prompt for VPN PIN - If selected, the user will be prompted to enter the VPN Pin while connecting.</li>
<li>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.</li>
<li>Choose Certificate - The drop-down displays the certificates uploaded for the profile. Select the client certificate to be used for authentication. Refer to the <b>explanation of adding certificates to the profile</b> for more details. If a new certificate is to be added, click 'Add New' and upload the certificate.</li>
<li>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.</li>
<li>Enter a domain name in the domain field and choose the establishment type from the 'Type' drop-down.
<ul>
<li>Always establish - Initiates a VPN connection for the domain.</li>
<li>Never establish - No VPN connection will be established while accessing the domain.</li>
<li>Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails.</li>
</ul></li>
</ul></li>
</ul></li>
</ul>
</td></tr>
</table>

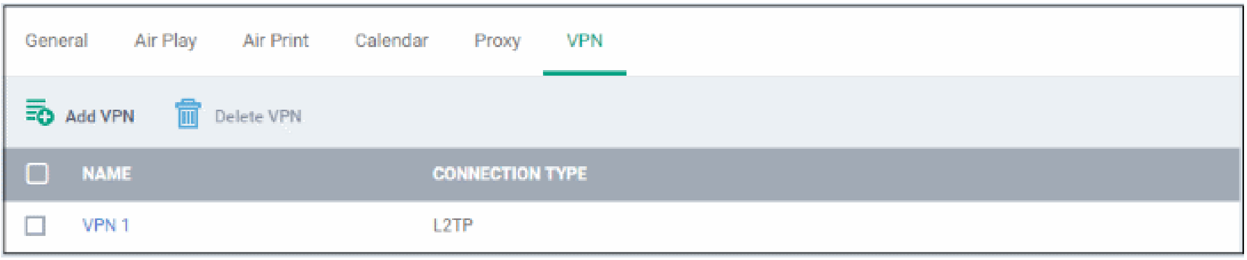
VPN Connection Type Settings - Table of Parameters	
	• Click 'Add' to add the domain to the list • Repeat the process to add more domains for On Demand VPN connection establishment rules. • To remove a domain, click 'X' beside it. For more details on variables, refer to the section **Configuring Custom Variables**.
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.

VPN Connection Type Settings - Table of Parameters	
	For more details on variables, refer to the section **Configuring Custom Variables**.
Juniper SSL	• 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 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.

VPN Connection Type Settings - Table of Parameters	
	- 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.



□	NAME	CONNECTION TYPE
□	VPN 1	L2TP

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'

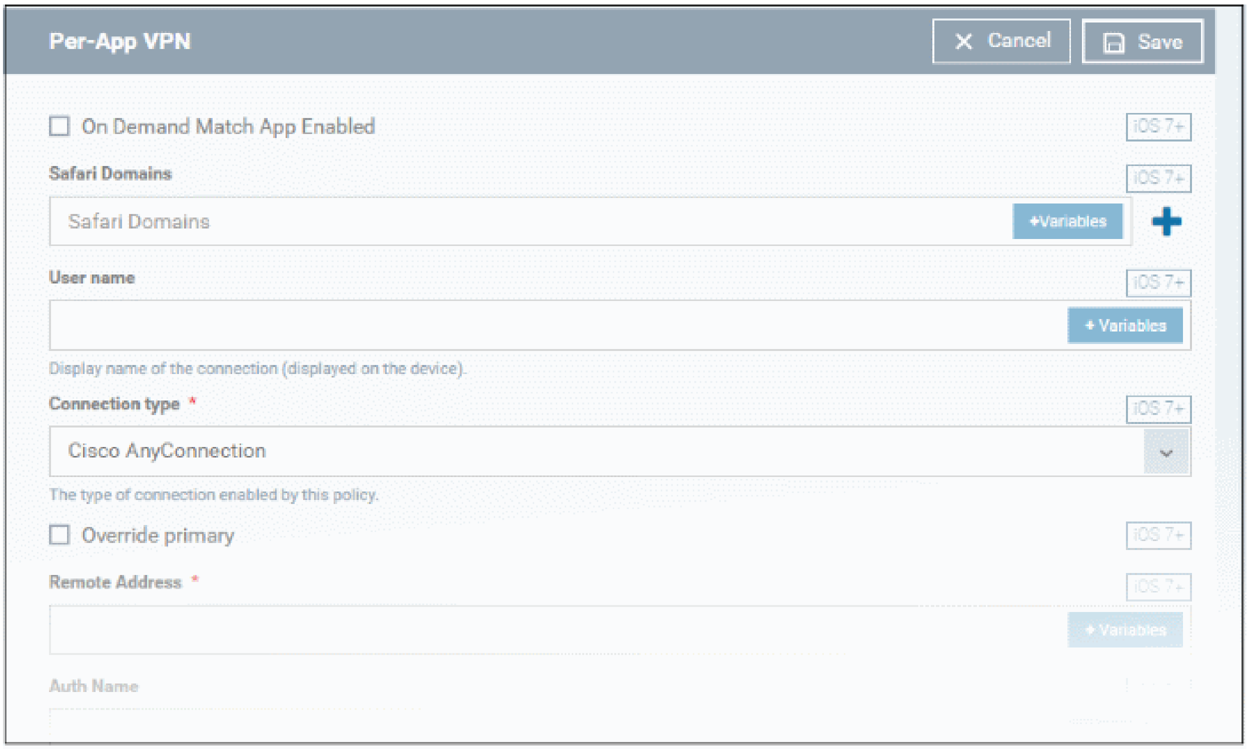
The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section 'Editing Configuration Profiles' for more details.

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

Safari Domains

Safari Domains

User name

Display name of the connection (displayed on the device).

Connection type *

Cisco AnyConnection

The type of connection enabled by this policy.

□ Override primary

Remote Address *

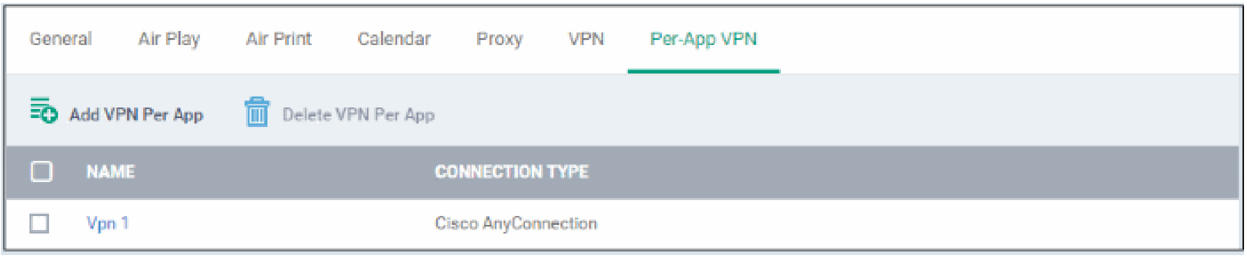
Auth Name

- **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.



□	NAME	CONNECTION TYPE
□	Vpn 1	Cisco AnyConnection

You can add multiple VPN servers for the profile.

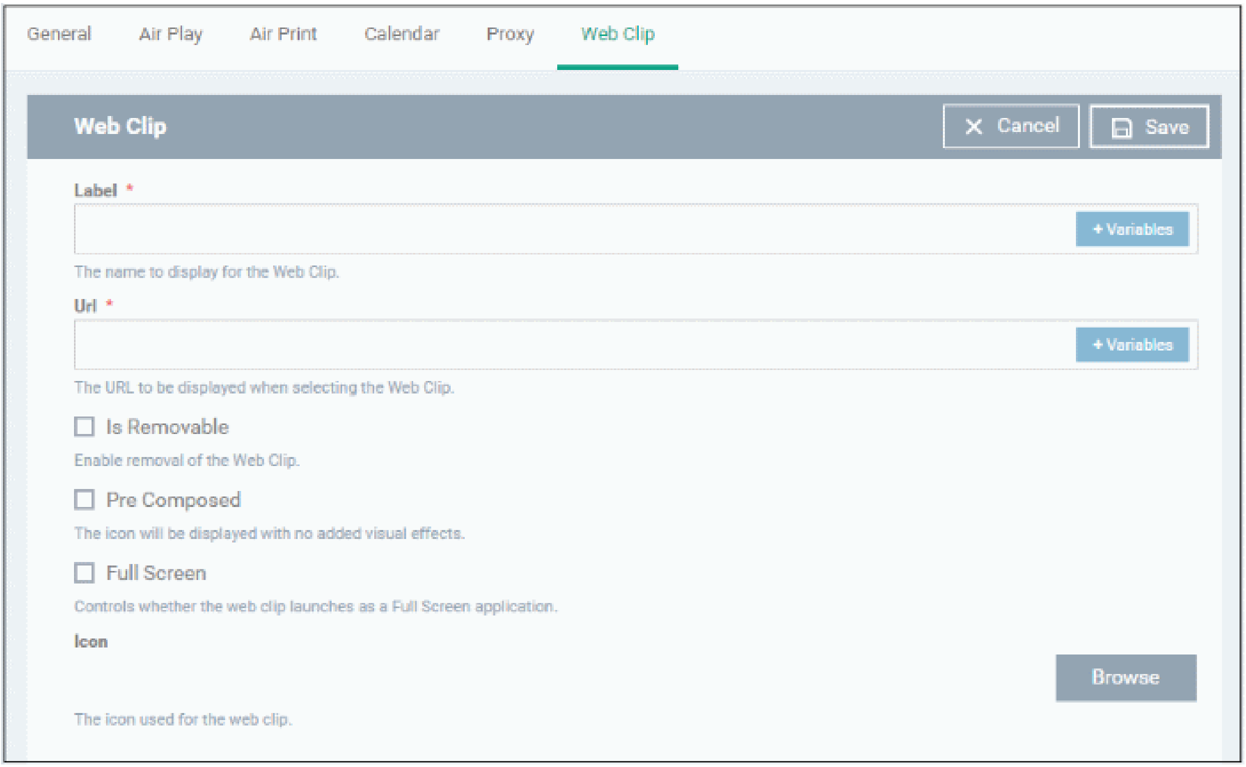
- To add another VPN server per App, click 'Add VPN Per App' and repeat the process
- To view and edit the settings of a VPN connection, click its name
- To remove VPN connection, select it and click 'Delete VPN Per App'

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.



Label *

The name to display for the Web Clip.

Url *

The URL to be displayed when selecting the Web Clip.

□ Is Removable

Enable removal of the Web Clip.

□ Pre Composed

The icon will be displayed with no added visual effects.

□ Full Screen

Controls whether the web clip launches as a Full Screen application.

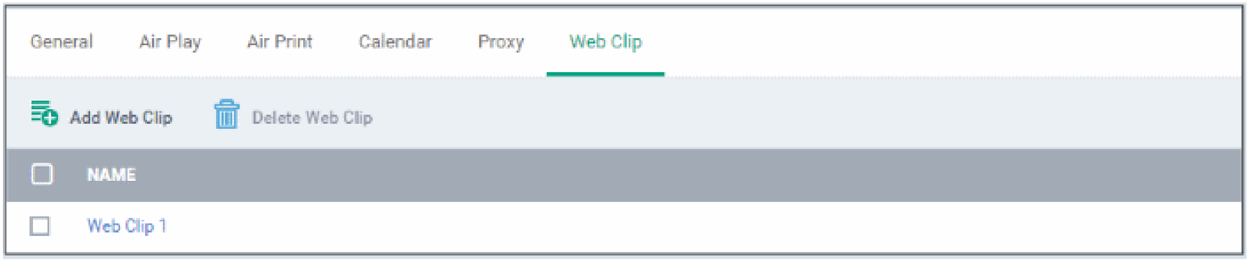
Icon

The icon used for the web clip.

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.

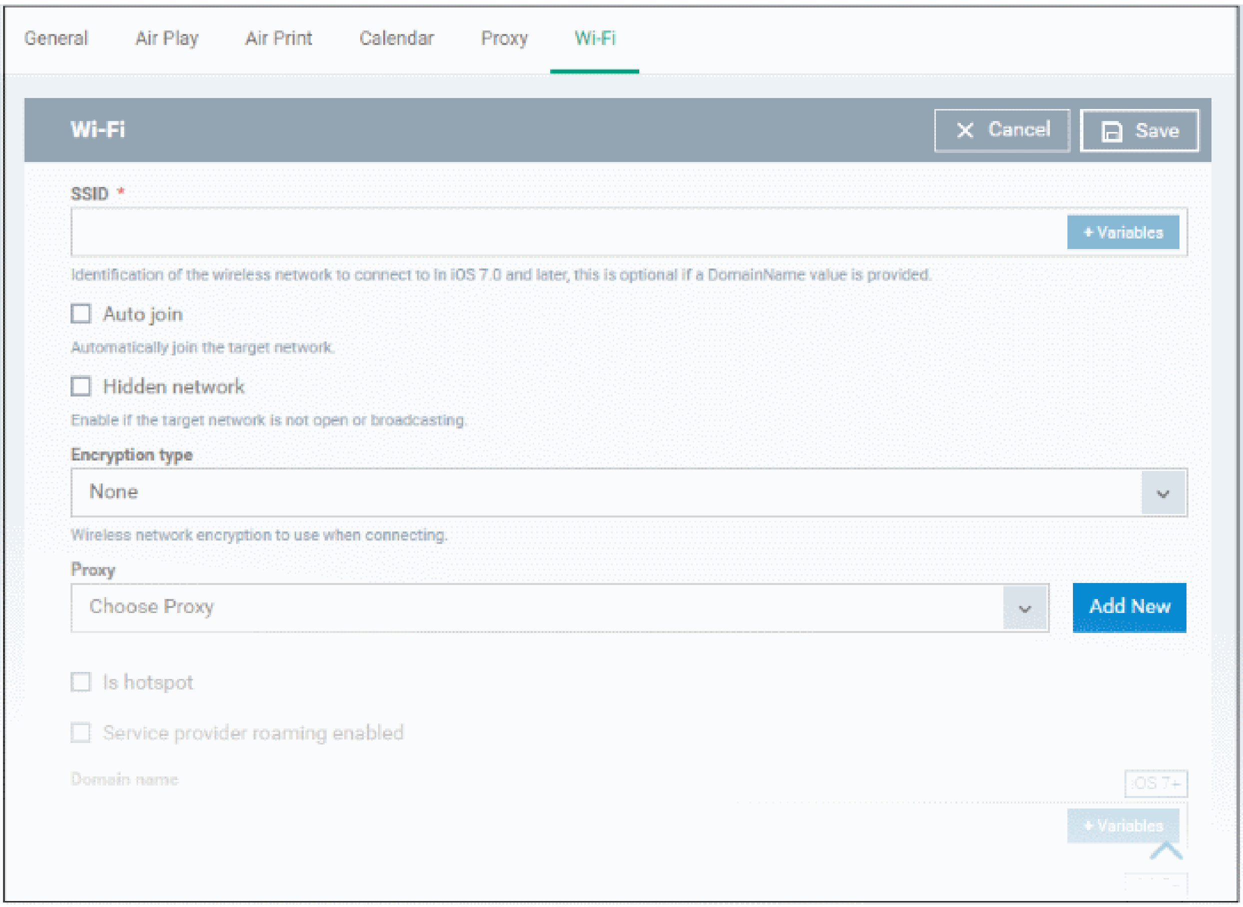
- To add another Web Clip, click 'Add Web Clip' and repeat the process
- To view and edit the settings for a web clip, click the name of it
- To remove a web clip, select it and click 'Delete Web Clip'

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.



SSID *

Identification of the wireless network to connect to In iOS 7.0 and later, this is optional if a DomainName value is provided.

□ Auto join

Automatically join the target network.

□ Hidden network

Enable if the target network is not open or broadcasting.

Encryption type

None

Wireless network encryption to use when connecting.

Proxy

Choose Proxy

□ Is hotspot

□ Service provider roaming enabled

Domain name

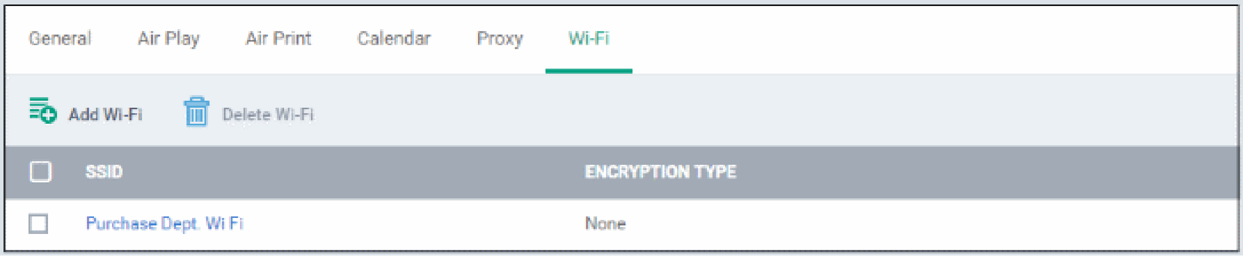
Wi-Fi Settings - Table of Parameters		
Form Element	**Type**	**Description**
SSID*	Text Field	Enter a unique identifier (Service Set Identifier) of a wireless network that

		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.



	SSID	ENCRYPTION TYPE
□	Purchase Dept. Wi Fi	None

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'

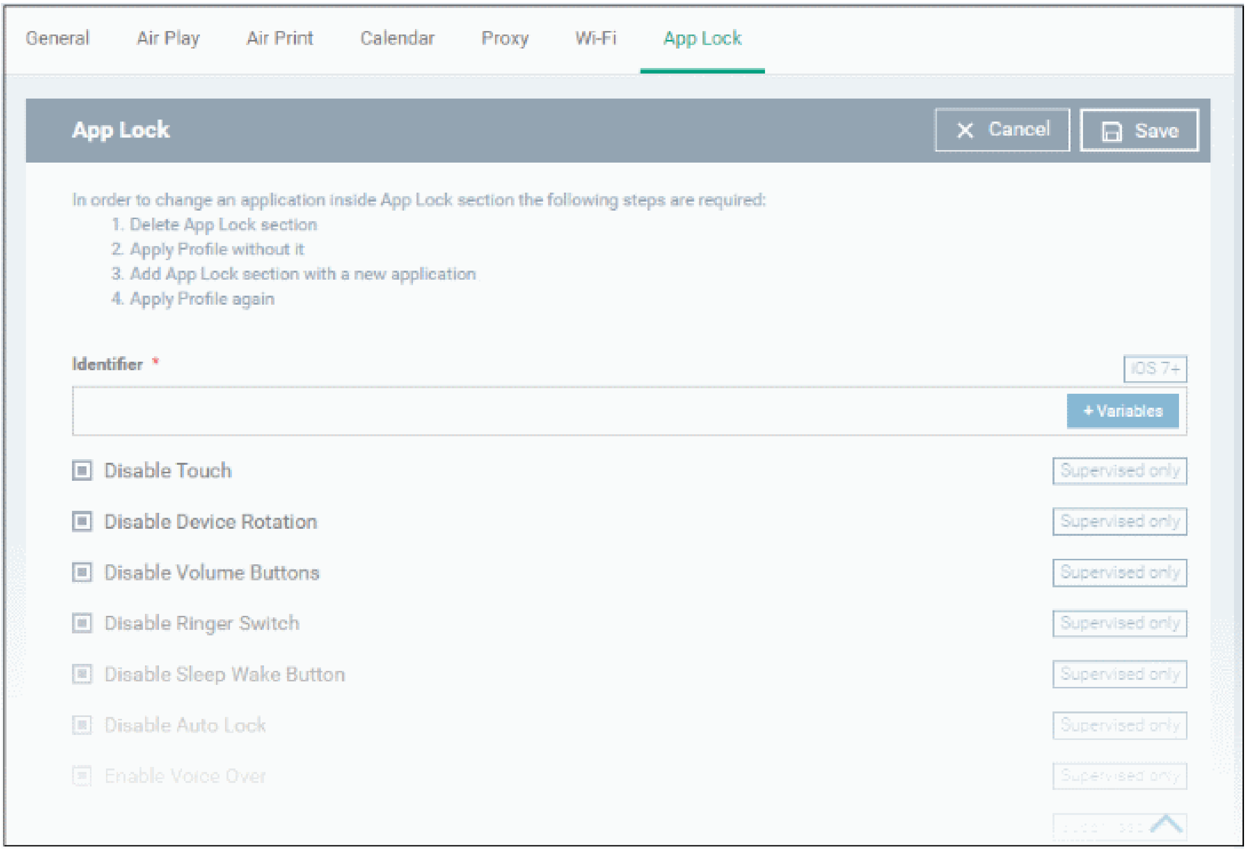
The settings will be saved and displayed under the Wi-Fi tab. You can edit the settings, add or remove Wi-Fi networks or remove the Wi-Fi networks at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

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 Lock' from the 'Add Profile Section' drop-down

The 'App Lock' settings screen will be displayed.



App Lock

In order to change an application inside App Lock section the following steps are required:

1. Delete App Lock section
2. Apply Profile without it
3. Add App Lock section with a new application
4. Apply Profile again

Identifier *

□ Disable Touch

□ Disable Device Rotation

□ Disable Volume Buttons

□ Disable Ringer Switch

□ Disable Sleep Wake Button

□ Disable Auto Lock

□ Enable Voice Over

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 bundle ID of the application to be included in the profile, with the app restrictions. For more details on getting the App bundle 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.

App Lock Settings - Table of Parameters		
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.
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

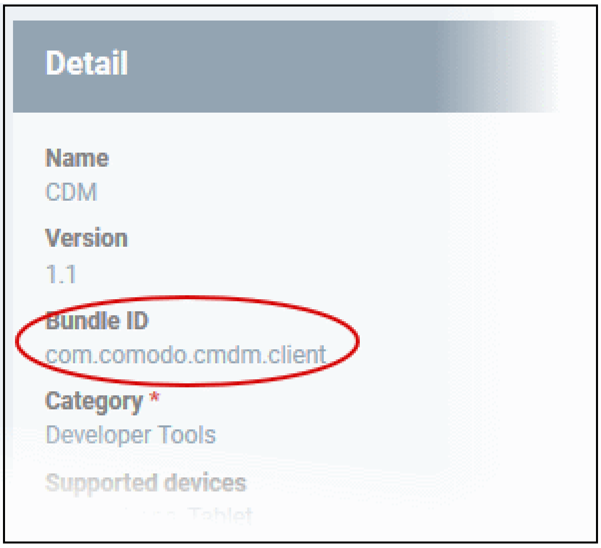
For App Store Application:

1. Find the iTunes Store download URL of the app. Example: **https://itunes.apple.com/us/app/cmdm/id807480077?mt=8**.
2. Copy the number after the id in the URL. (Here it is: 807480077).
3. Open https://itunes.apple.com/lookup?id=807480077 where you replace the ID with the one you looked up.
4. Search the output for "bundleID". In this example: "bundleId":"com.comodo.cmdm.client". So the Bundle ID is com.comodo.cmdm.client

For Enterprise Application:

The App bundle ID can be viewed from the App Details screen of the App.

- Click 'Application Store' from the left and choose 'iOS Store'
- Click on the app from the list displayed at the right



Detail

Name
CDM

Version
1.1

Bundle ID
com.comodo.cmdm.client

Category *
Developer Tools

Supported devices
Tablet

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.

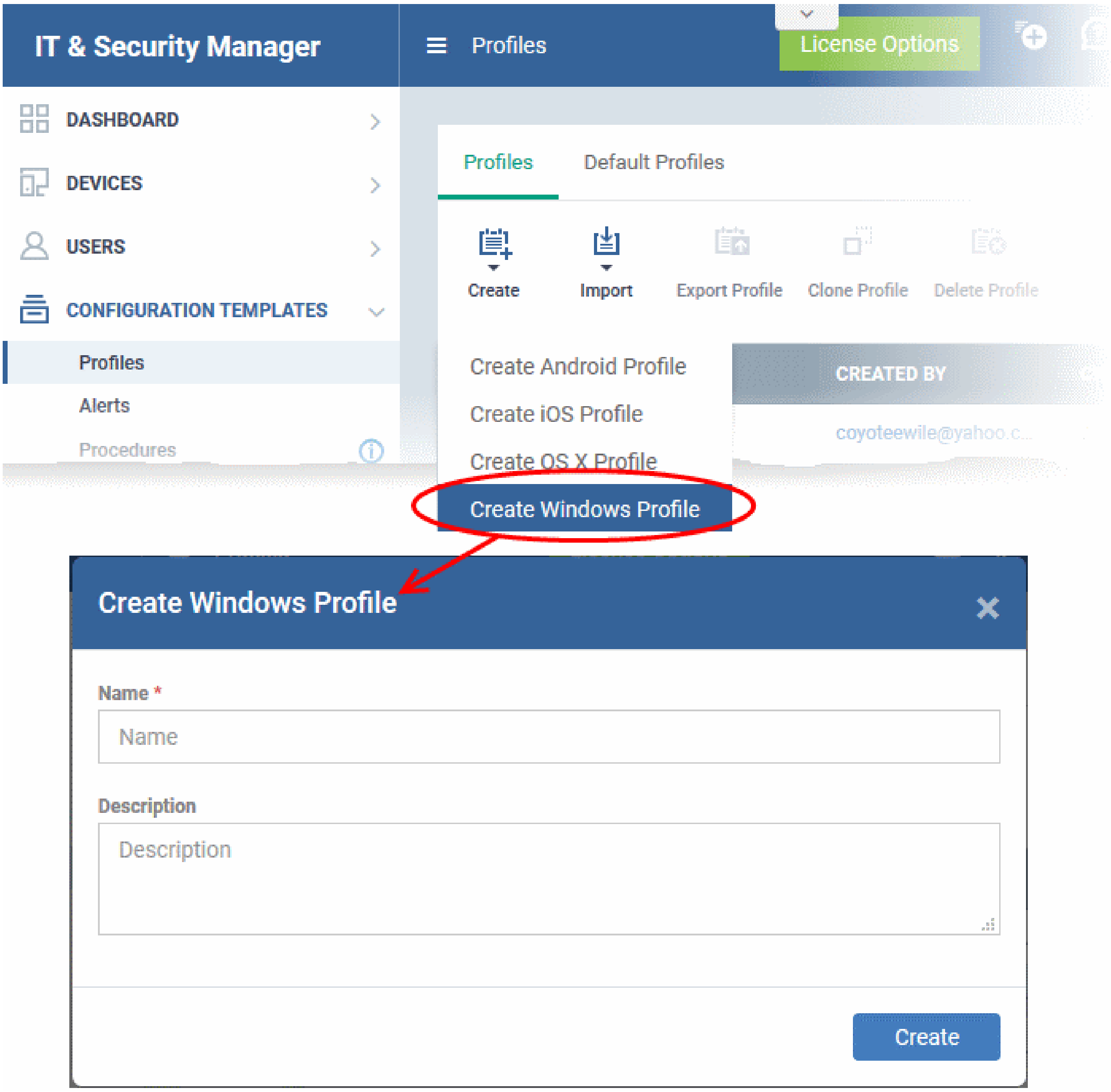
Security profiles for Windows endpoints can be added to ITSM in two ways:

- 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. Create Windows Profiles

To create a new Windows profile

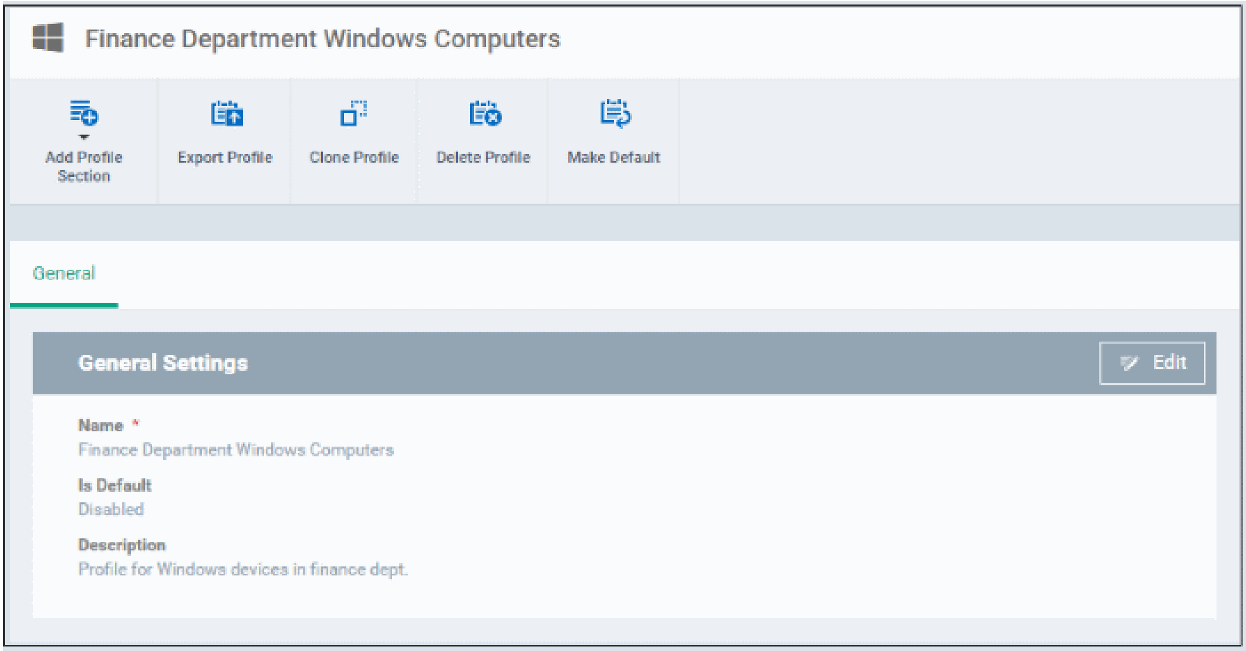
- Click 'Configuration Templates' on the left then 'Profiles'
- Click 'Create' then select 'Create Windows Profile'
- Specify a name and description for your profile then click the 'Create' button. The profile will now appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - '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 a new profile, click 'Configuration Templates > Profiles > Create' > 'Create Windows Profile':



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.



Name *
Finance Department Windows Computers

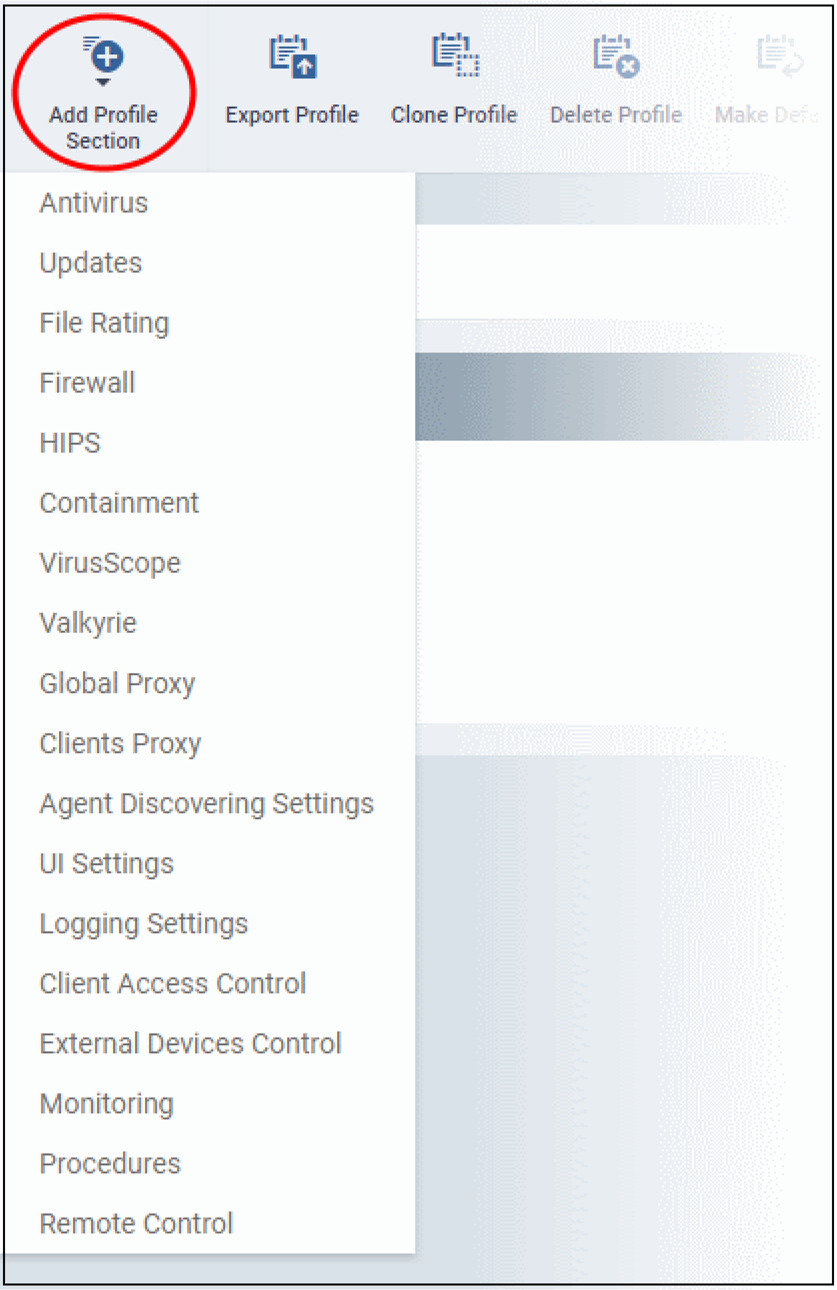
Is Default
Disabled

Description
Profile for Windows devices in finance dept.

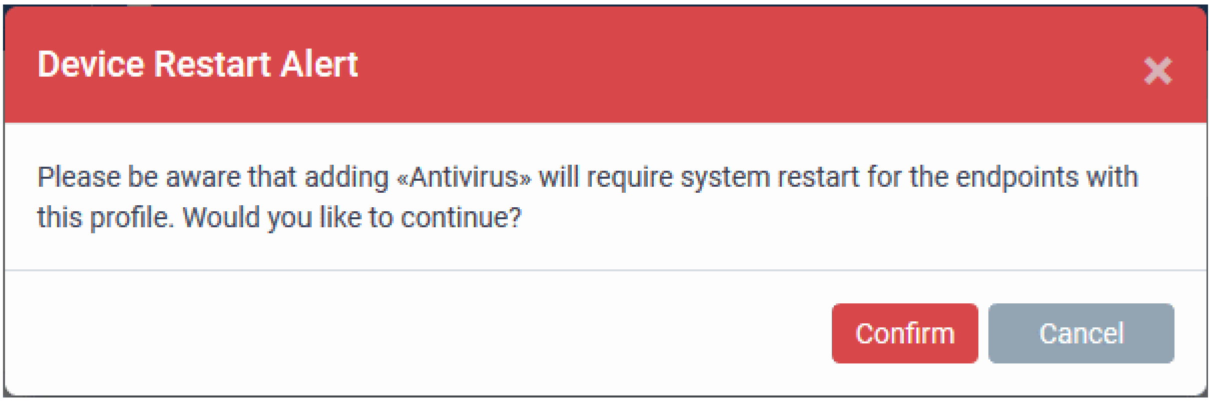
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

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.



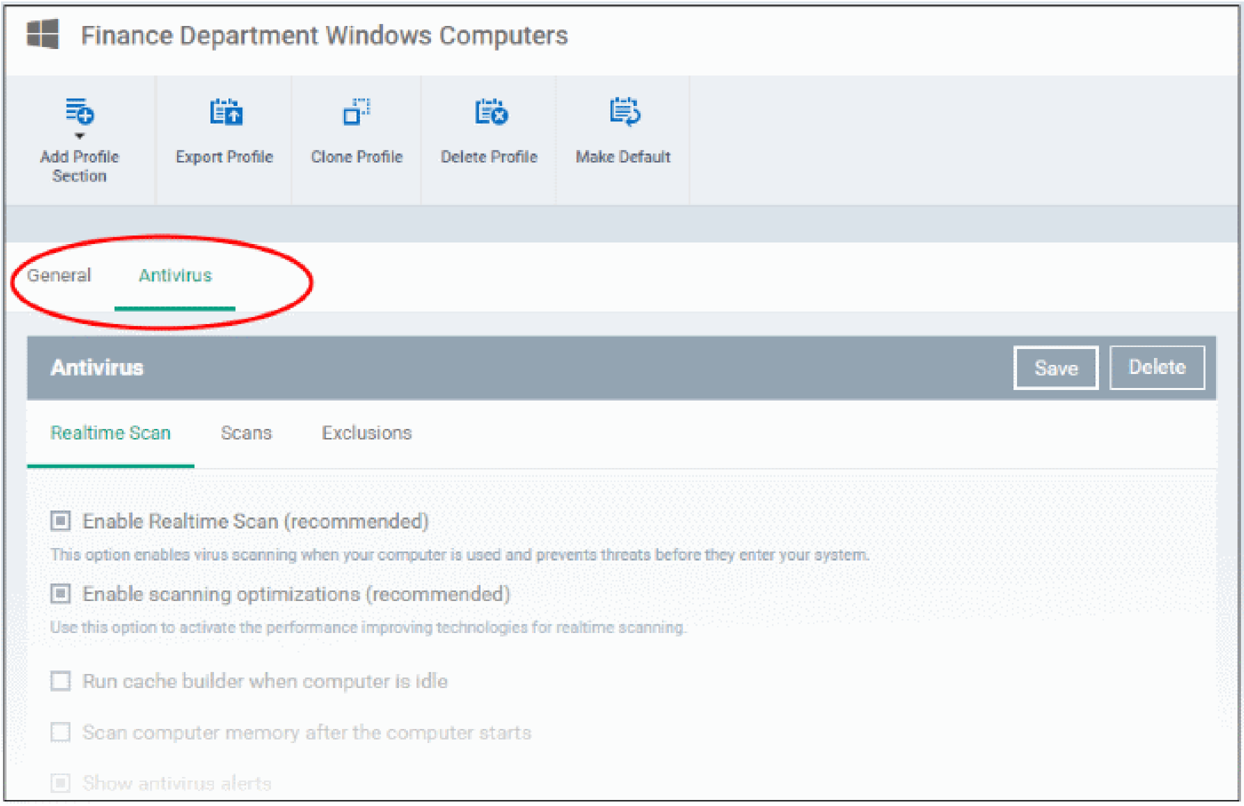
If the changes in the configuration of the component requires the restart of the endpoint to which the profile is applied, an alert dialog will be displayed.


Device Restart Alert

Please be aware that adding «Antivirus» will require system restart for the endpoints with this profile. Would you like to continue?

- 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.



☒ Enable Realtime Scan (recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☒ Enable scanning optimizations (recommended)

Use this option to activate the performance improving technologies for realtime scanning.

□ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☒ Show antivirus alerts

The 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**

- **Remote Control**

6.1.3.1.1. Antivirus Settings

The antivirus settings screen allows you to configure real-time monitoring, scan profiles and exclusions for the profile.

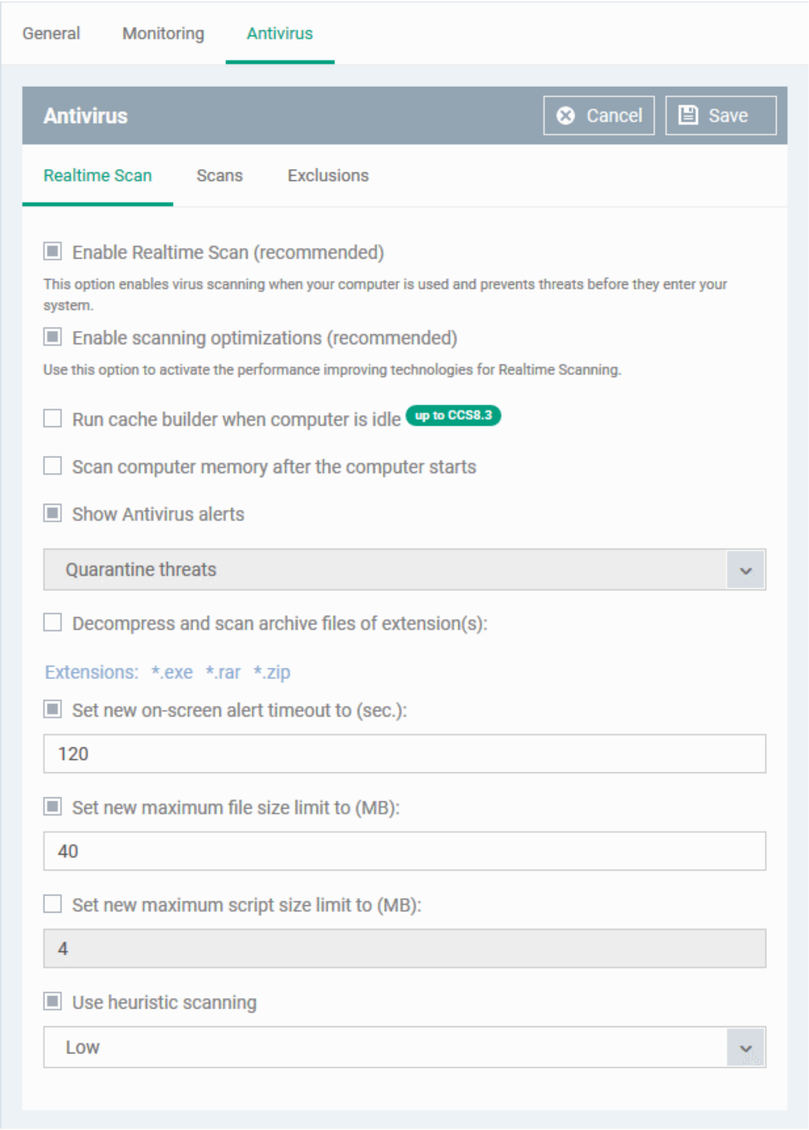
To configure Antivirus settings

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click 'Add Profile Section' > 'Antivirus'

The settings screen for Antivirus will open:

- **Real Time Scan** - Configure the 'always-on' virus monitor
- **Scans** - Create custom scan profiles. A scan profile lets you scan specific areas and configure custom scan options. You can also create a schedule for the scan profile. Multiple scan profiles can be added to a device profile.
- **Exclusions** - Items that should be skipped by virus scans on devices to which the profile is applied. Items you add here are excluded from real-time scans and any custom scan profiles.

Realtime Scan settings



☑ Enable Realtime Scan (recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (recommended)

Use this option to activate the performance improving technologies for Realtime Scanning.

□ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☑ Show Antivirus alerts

Quarantine threats

□ Decompress and scan archive files of extension(s):

Extensions: *.exe *.rar *.zip

☑ Set new on-screen alert timeout to (sec.):

120

☑ Set new maximum file size limit to (MB):

40

□ Set new maximum script size limit to (MB):

4

☑ Use heuristic scanning

Low

Realtime Scan Settings - Table of Parameters	
Form Element	**Description**
Enable Realtime Scan	The realtime scanner ensures your devices are constantly protected from malware. The scanner inspects files whenever they are created, opened or copied. • Choose whether of not to enable real time scanning. (***Default = Enabled***)
Enable Scanning Optimizations	Various techniques to improve antivirus scan performance and reduce system resource use. • Choose whether or not to enable scan optimization. (***Default = Enabled***)
Run cache builder when computer is idle	The antivirus cache builder runs whenever the computer is idle to boost the speed of real-time scans. (***Default = Disabled***) • Applies only to CCS versions 8.3 or lower.
Scan computer memory after the computer start	If enabled, CCS will scan system memory for threats after a re-boot. (***Default = Disabled***)
Show antivirus alerts	Configure whether or not to show alerts on the endpoints when malware is discovered. Disabling will minimize disturbance to the end-user 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: • Quarantine threats - Moves detected threat(s) to quarantine for assessment. • Block threats - Deletes the threat. (***Default = Enabled with 'Quarantine threats' option***)
Decompress and scan archive files of extensions	The antivirus will open and scan archive files such as .jar, RAR, ZIP, ARJ, WinARJ and CAB. If enabled, you can choose which types of archive should be decompressed and scanned. Click the 'Extensions' link to view existing extensions and add new extensions. (***Default = Disabled***)
Set new on-screen alert timeout to (secs)	Specify how long an alert should stay on the screen at an endpoint. (***Default = 120 seconds***)
Set new maximum file size to (MB)	Specify the maximum file size that the antivirus should attempt to scan. Files larger than the size specified here will not be not scanned. (***Default = 40 MB***)
Set new maximum script size limit to (MB)	Specify the maximum size of a script that the antivirus should attempt to scan. Files larger than the size specified here are not scanned. (***Default = 4 MB***)
Use heuristic scanning	Enable or disable heuristics scanning and define the scan level.

	The scan level determines how likely the scanner is to classify an unknown file as a threat. • Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' 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 / increased possibility of false positives. (***Default = Enabled with 'Low ' option***) **Background Note**: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing a file to ascertain whether it contains code typical of a virus. It is about detecting attributes which resemble a virus, rather than looking for a signature that matches a signature on the virus blacklist. This allows the engine to predict the existence of new viruses - even if they are not in the current virus database.

- Click the 'Save' button at the bottom.

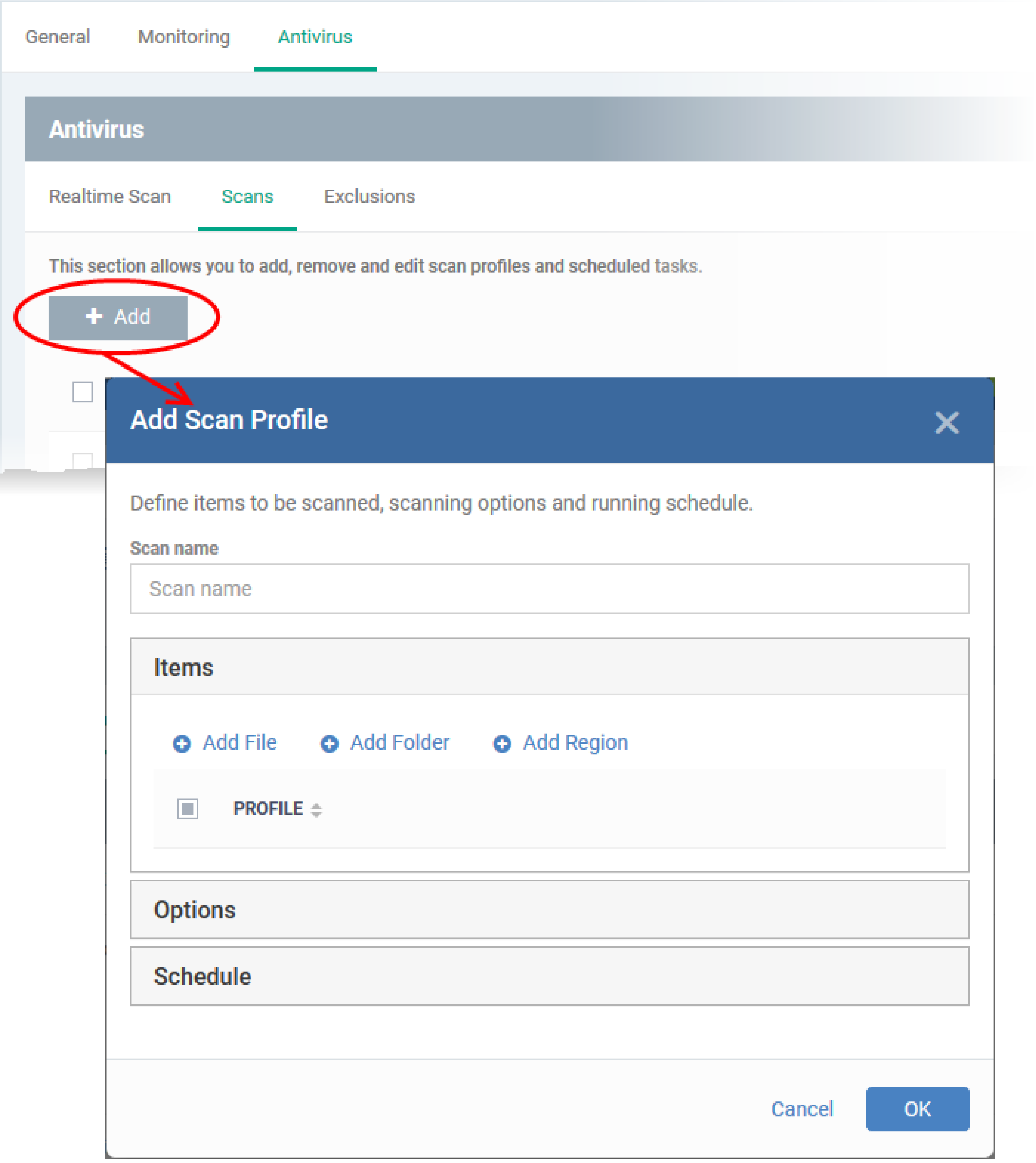
Custom Scans

The 'Scans' pane allows you to view, edit, create and run custom scan profiles. Each scan 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)
- You can add multiple scan-profiles to a device profile.

To create a custom scan profile

- Open the 'Antivirus' scan of a device profile ('Configuration Templates' > 'Profiles' > 'Antivirus' section)
- Click the 'Scans' tab.
- Click the 'Add' button in the 'Scans' tab



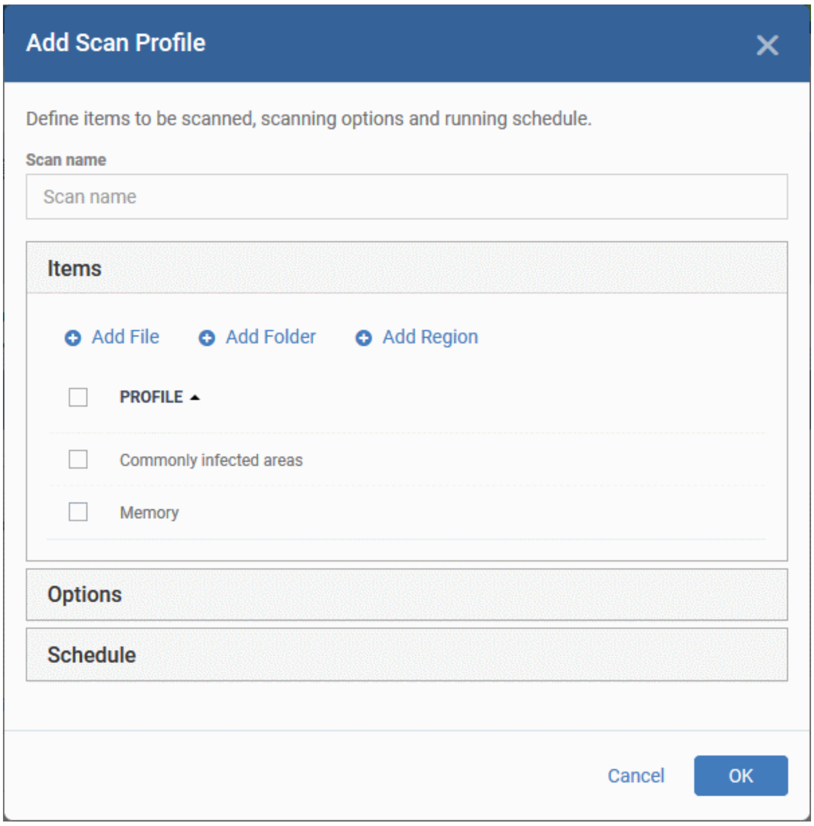
The 'Add Scan Profile' dialog will open:

- Enter the name of the custom scan in the 'Scan name' field

The 'Items' section lets you choose a specific file, folder or region to that should be scanned by the profile.

- Add File - A specific file that should be scanned. You can also add an entire extension by using the the wildcard character (e.g. *.exe).
- Add Folder - Allows you to scan a particular directory.
- Add Region - Scan a predefined region. For example, 'Entire Computer', 'Commonly Infected Areas' and 'Memory'.

The selected items will be displayed as follows:



Add Scan Profile

Define items to be scanned, scanning options and running schedule.

Scan name: Scan name

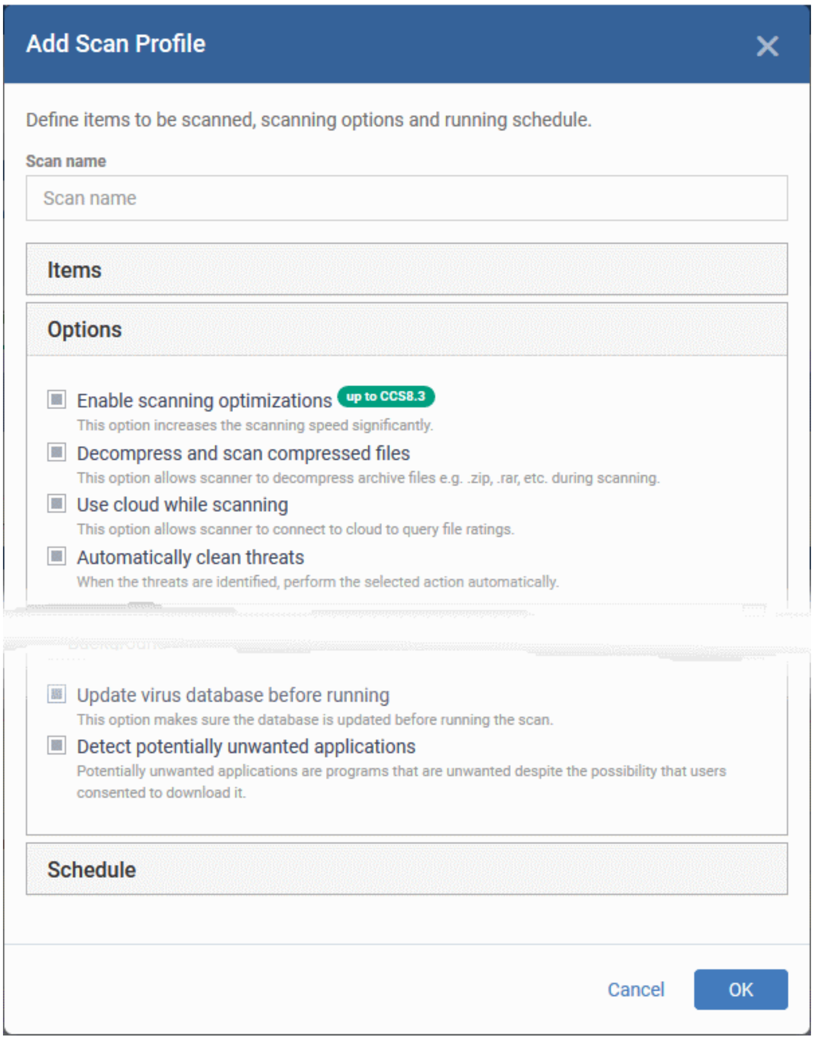
Items

□	PROFILE ▲
□	Commonly infected areas
□	Memory

- 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

Define items to be scanned, scanning options and running schedule.

Scan name

Scan name

Items

Options

☐ Enable scanning optimizations up to CCS8.3
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
This option allows scanner to connect to cloud to query file ratings.

☐ Automatically clean threats
When the threats are identified, perform the selected action automatically.

☐ 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.

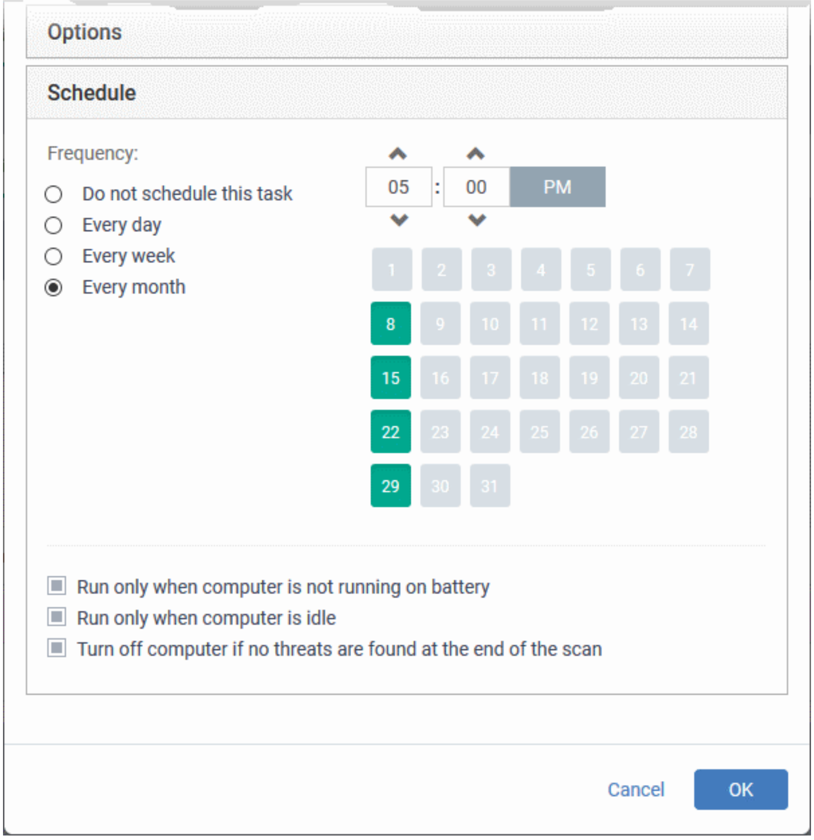
Schedule

Options Configuration - Table of Parameters	
Form Element	**Description**
Enable scanning optimizations	The antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (***Default = Enabled***) . - Applies only to CCS versions 8.3 or lower.
Decompress and scan compressed files	The antivirus will open and scan archive files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***).
Use cloud while scanning	Augments the local scan with a real-time look-up of Comodo's online signature database. The cloud database is the most up-to-date version of our virus database, so antivirus scans are more accurate. With 'Cloud Scanning' enabled, CCS is capable of detecting zero-day malware even if the local database is out-dated. (***Default = Enabled***).
Automatically clean threats	CCS will automatically take action against detected threats instead of showing the results screen with a list of threats. You can choose the action to be taken from the drop-down. The available options are: - Disinfect - Quarantine (***Default = Enabled with Disinfect option***)
Show scan results window	Displays a results window at the end of a virus scan. The results windows shows all threats identified by the scan. (***Default = Disabled***)
Use heuristic scanning	Enable or disable heuristics scanning and define the scan level. The scan level determines how likely the scanner is to classify an unknown file as a threat. - Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' 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 / increased

Options Configuration - Table of Parameters	
	possibility of false positives. (***Default = Enabled with 'Low ' option***) **Background Note**: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing a file to ascertain whether it contains code typical of a virus. It is about detecting attributes which resemble a virus, rather than looking for a signature that matches a signature on the virus blacklist. This allows the engine to predict the existence of new viruses - even if they are not in the current virus database.
Limit maximum file size to	Specify the maximum file size that the antivirus should attempt to scan.(***Default = 40 MB***).
Run this scan with	Set the Windows priority of the scan. Choices are high, medium, low and run in the background. (***Default = Enabled with Background option***)
Update virus database before running	Makes CCS to check for virus database updates before a scan. Available updates will be downloaded prior to the scan. (***Default = Enabled***).
Detect potentially unwanted applications	CCS 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 = Enabled***).

The next step is to schedule when the custom scan should be run.

- Click 'Schedule'



Options

Schedule

Frequency:

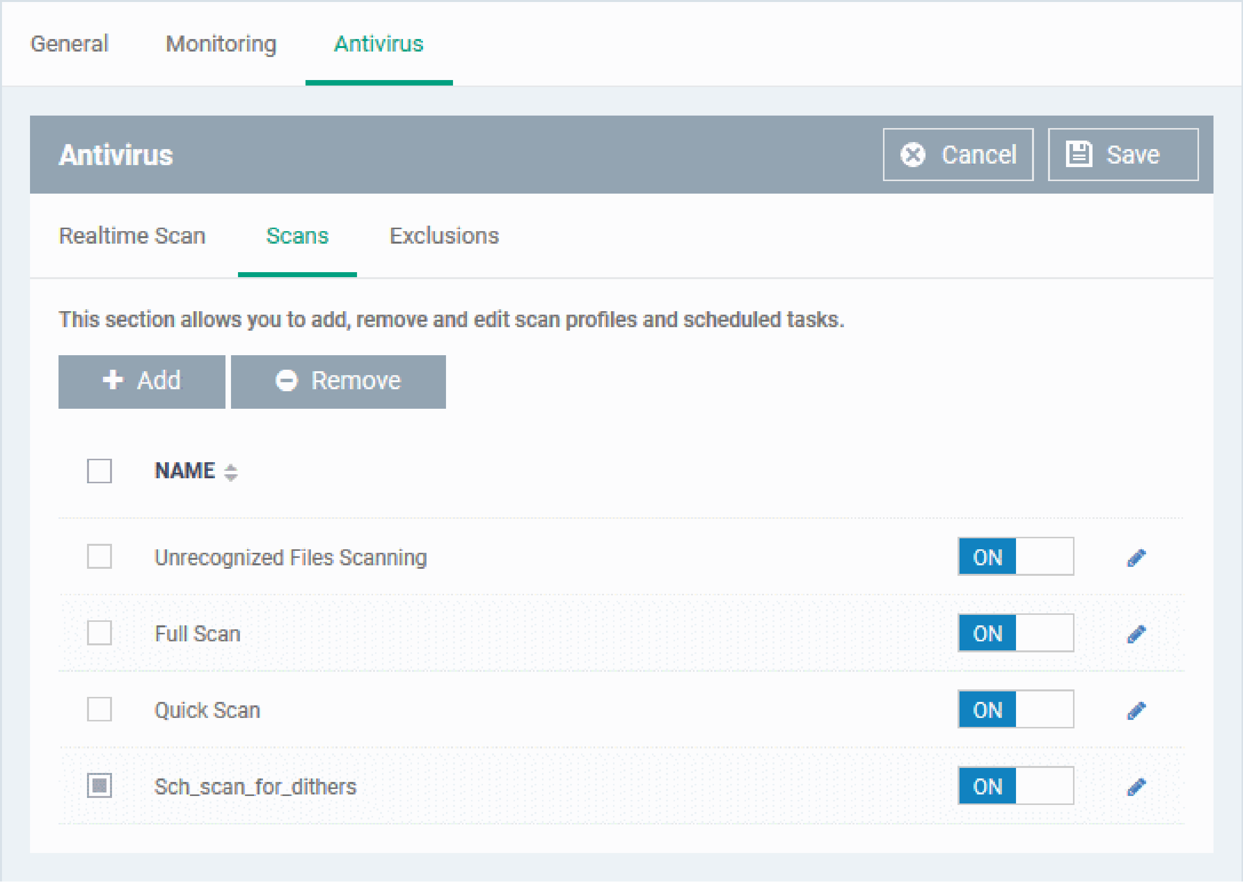
○ Do not schedule this task
○ Every day
○ Every week
● Every month

05 : 00 PM

□ Run only when computer is not running on battery
□ Run only when computer is idle
□ Turn off computer if no threats are found at the end of the scan

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	Runs the scan only if the computer is connected to the mains supply. This is useful if you are using a laptop or any other battery driven portable computer.
Run only when computer is idle	Scans will run only if the computer is in idle state. Select this if you do not want to be disturbed, or if you are running resource intensive programs and do not want the scan to take processing power.
Turn off computer if no threats are found at the end of the scan	Powers down your computer if no threats are found during the scan. For example, this is useful if you have scans which are scheduled to run at night.

- Click 'OK' to save the custom scan settings



This section allows you to add, remove and edit scan profiles and scheduled tasks.

	NAME		
□	Unrecognized Files Scanning	ON	
□	Full Scan	ON	
□	Quick Scan	ON	
☑	Sch_scan_for_dithers	ON	

The added scan profile will be listed in the screen.

- Use the switches to enable or disable a scan-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'

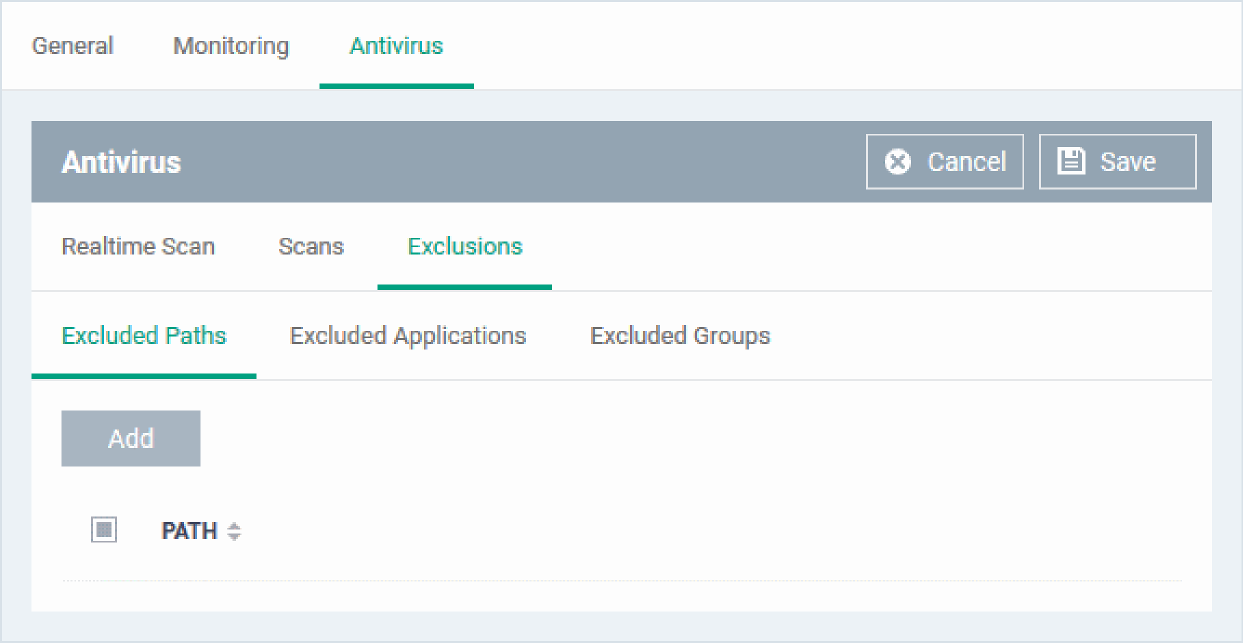
Exclusions

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'

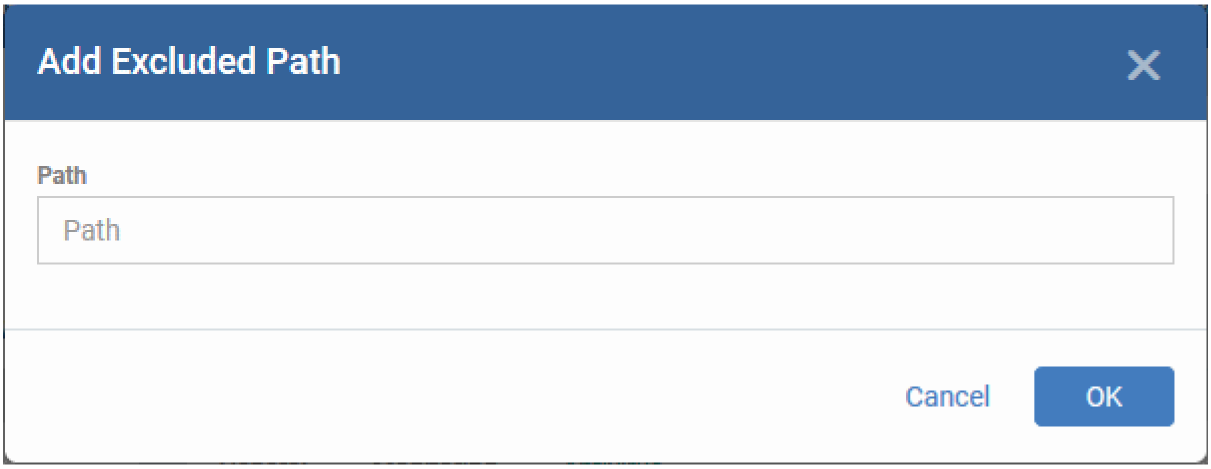
To add excluded paths

By default the 'Excluded Paths' screen will be displayed:



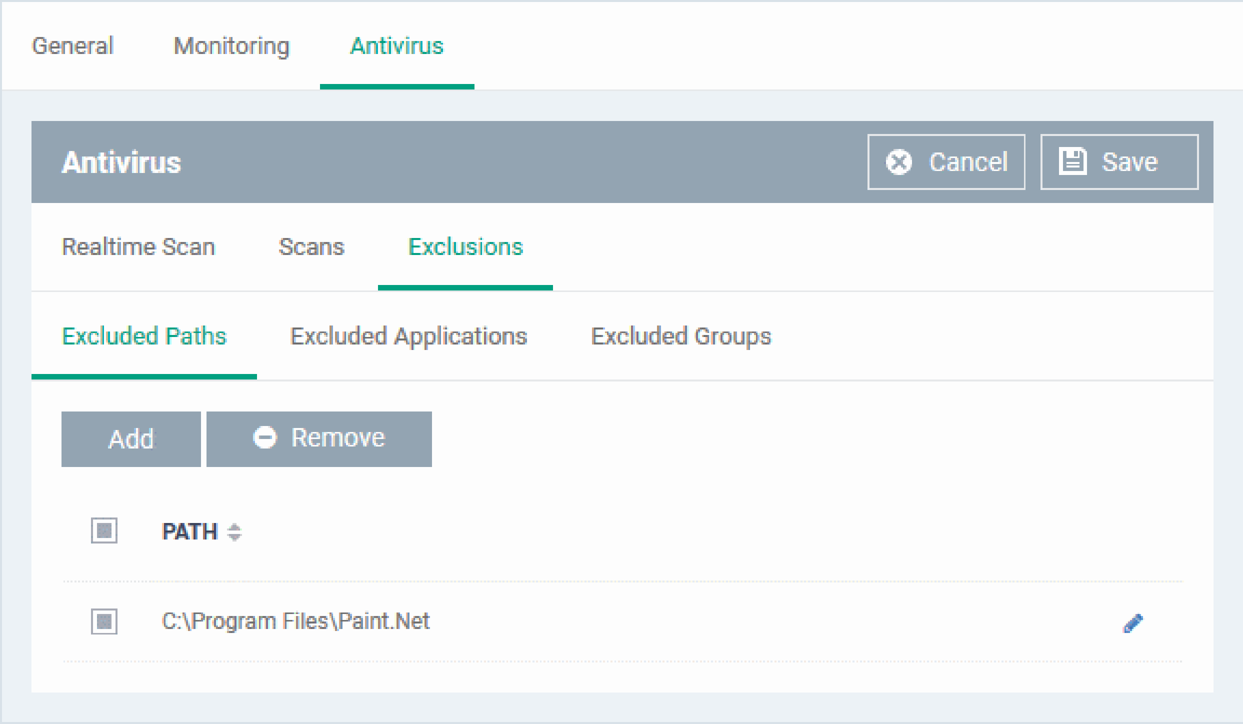
- Click 'Add'

The 'Add' dialog will appear:



- Enter the full path that should be excluded from scanning and click 'OK'.

The added excluded path will be added to the list.

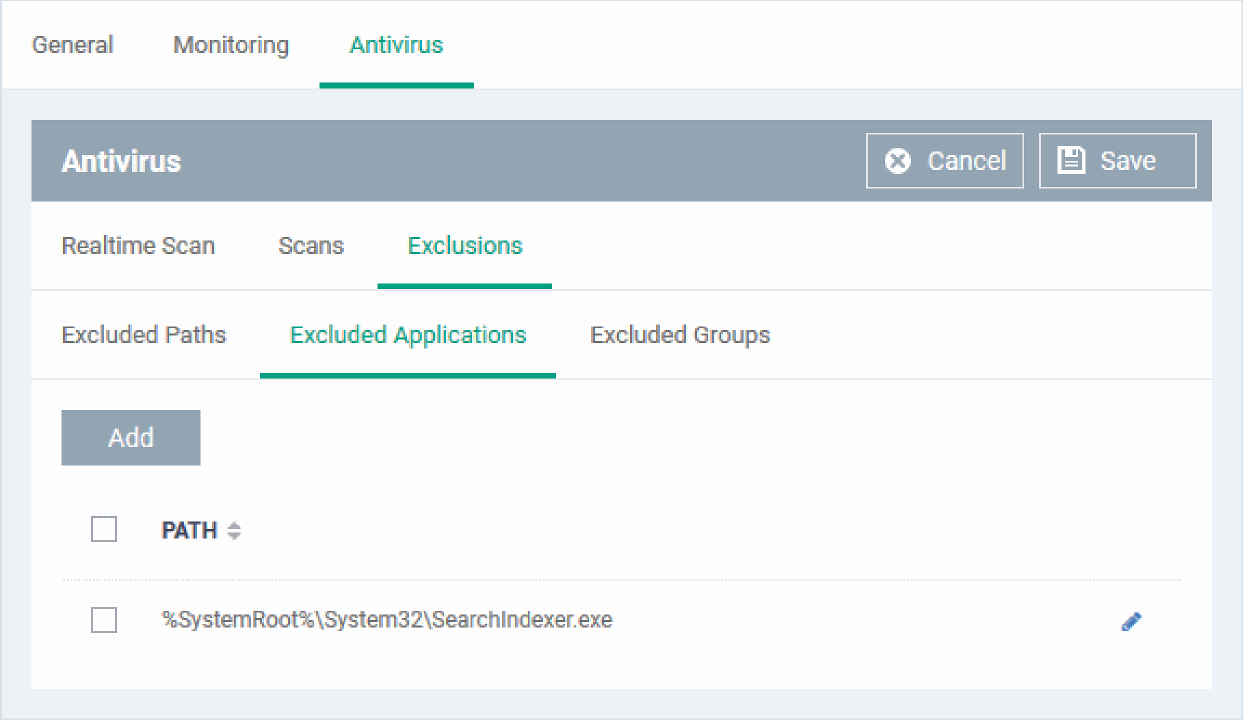


C:\Program Files\Paint.Net

- 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'

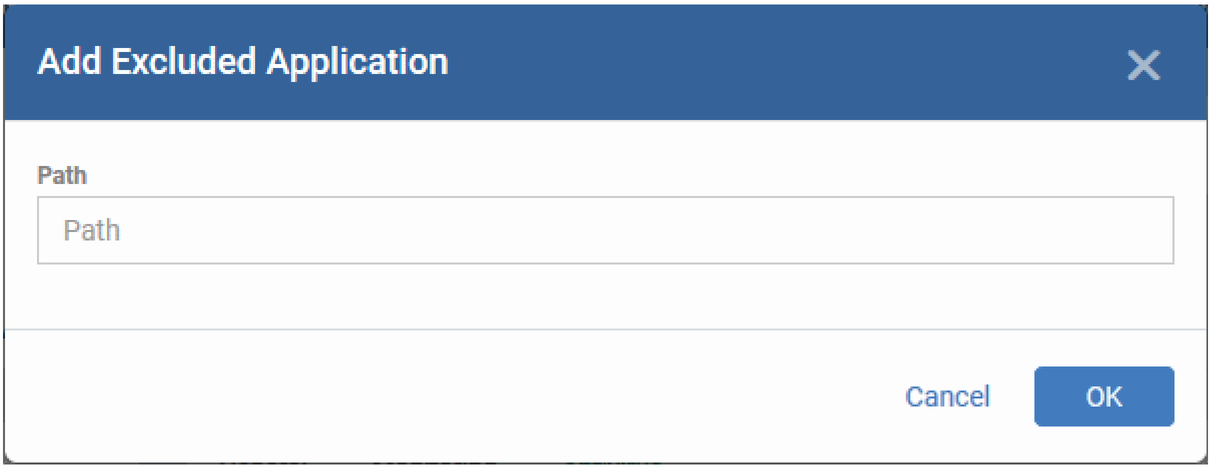
To add excluded applications

- Click 'Excluded Applications'

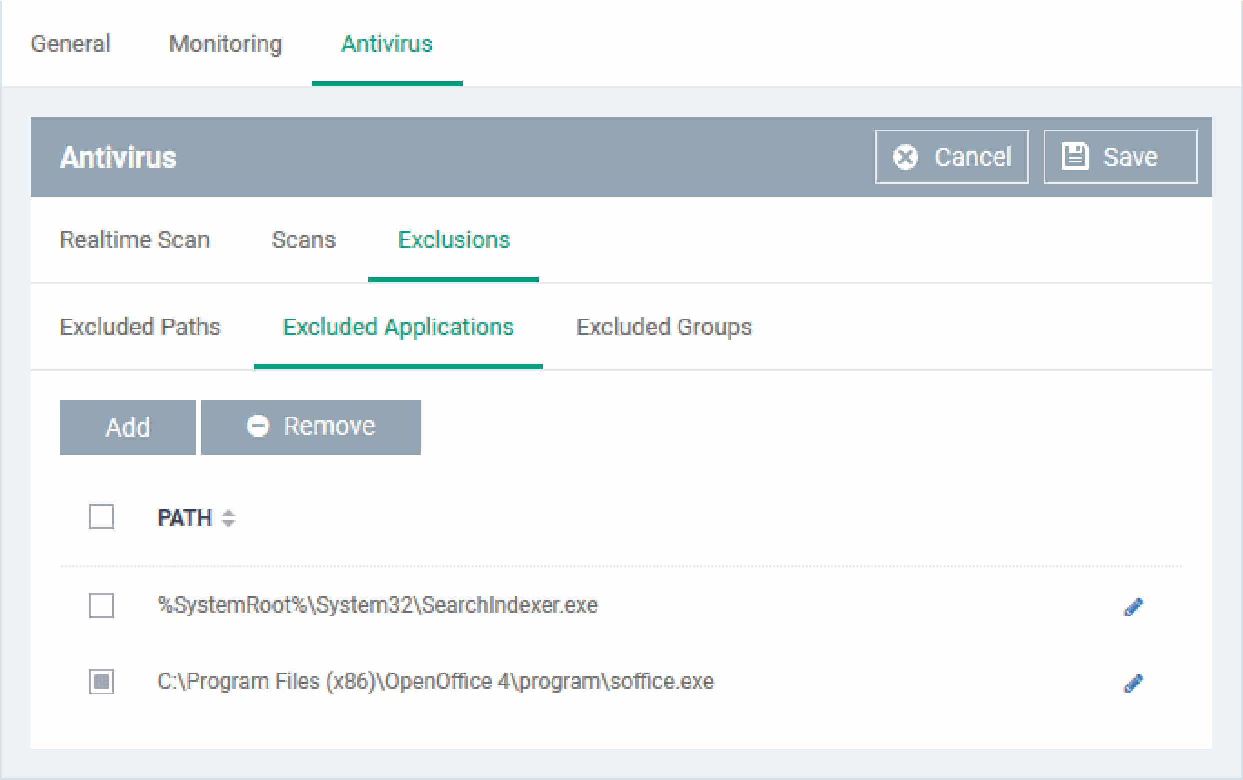


%SystemRoot%\System32\SearchIndexer.exe

- 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



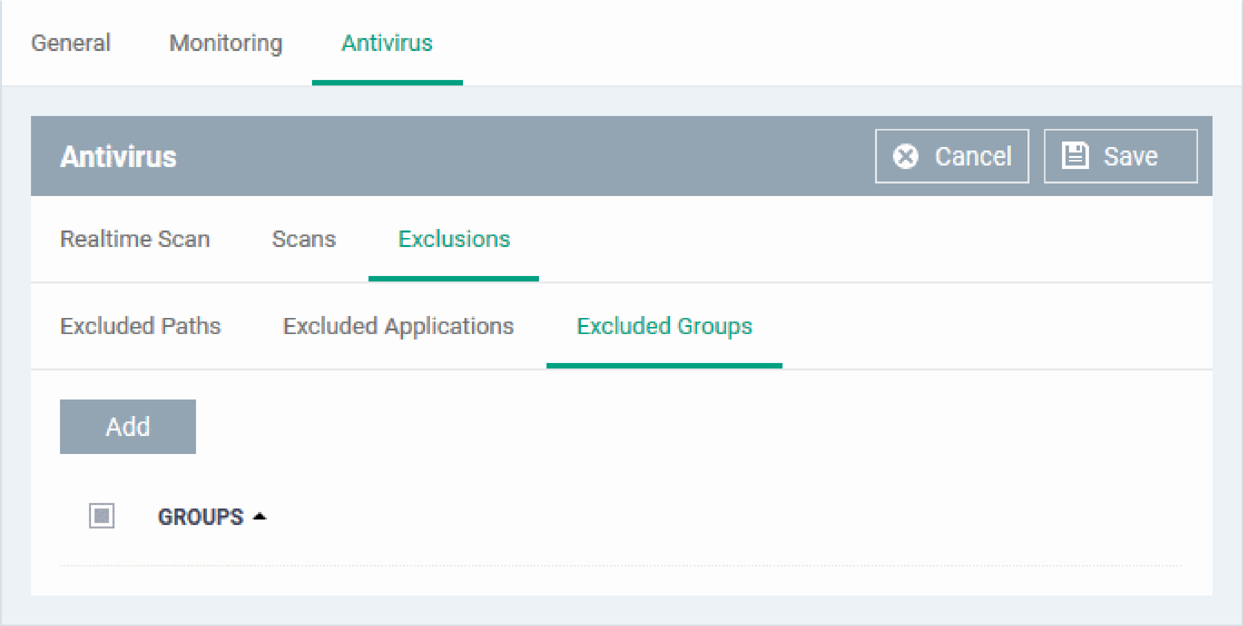
	PATH
□	%SystemRoot%\System32\SearchIndexer.exe
☒	C:\Program Files (x86)\OpenOffice 4\program\soffice.exe

- 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

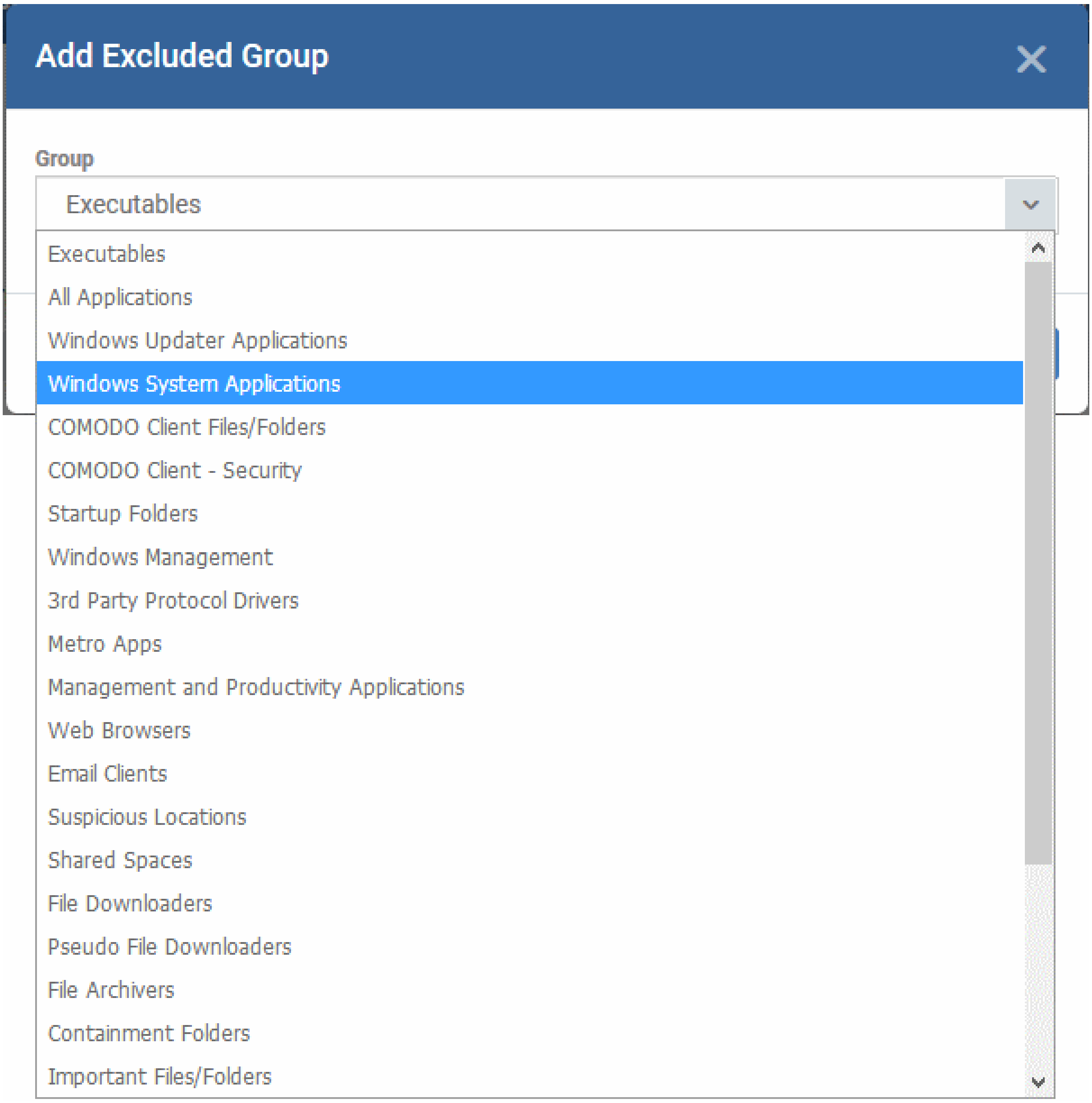
File groups are handy, predefined groupings of one or more file types. File groups make it easy to exclude an entire class of file types. ITSM ships with a set of predefined 'File Groups'. Users, can add new groups and edit existing groups. See '**File Groups**' under 'Settings' > 'System Templates' > 'File Groups Variables'.

- Click 'Excluded Groups'



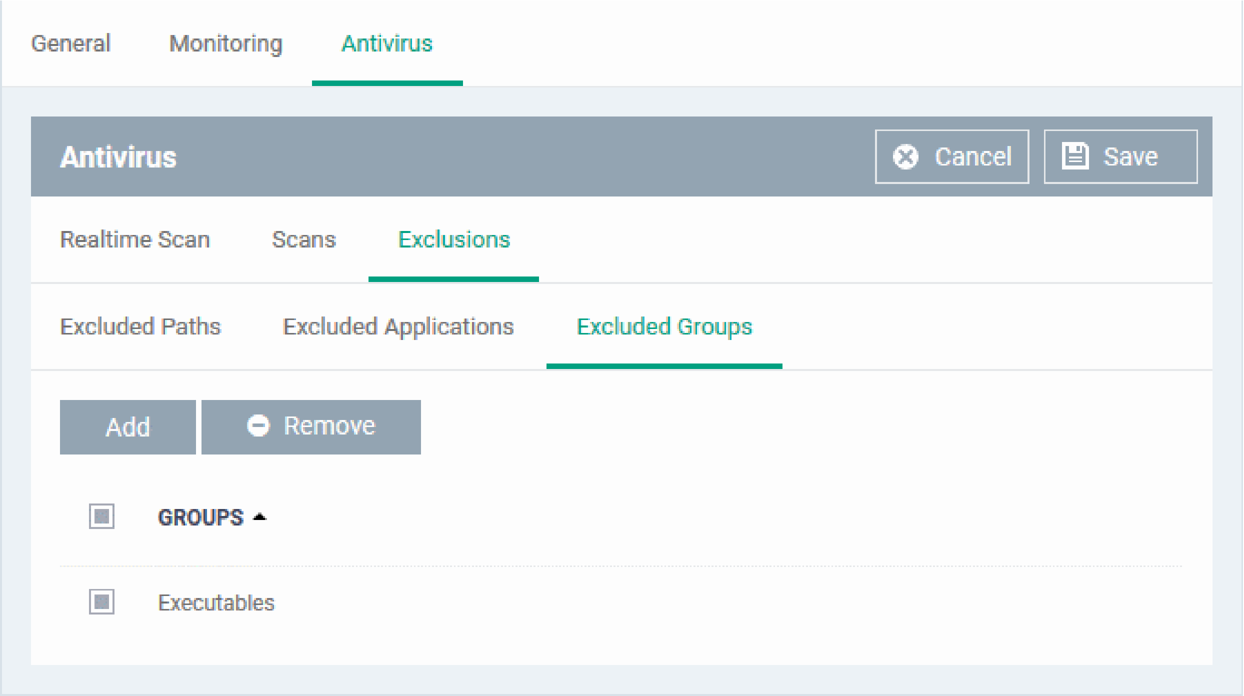
- Click 'Add'.

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. CCC and CCS Application Update Settings

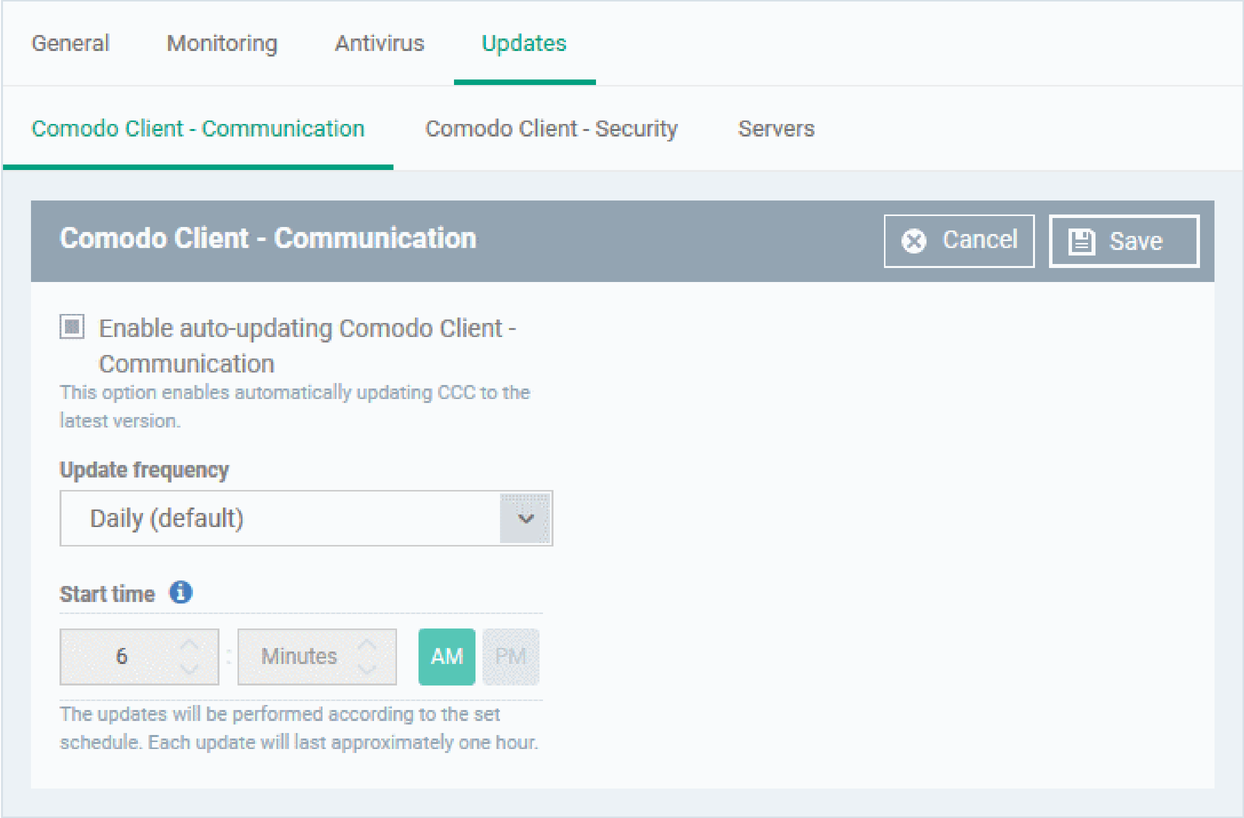
The 'Updates' component of a Windows profile lets you configure when managed computers should check for updates for Comodo Client - Communication (CCC) and Comodo Client - Security (CCS). You can also specify the location from where updates should be downloaded.

Tip: You can also manually update CCC and CCS on selected endpoints from the 'Device List' interface. See **Remotely Installing and Updating Packages on Windows Devices** for more details.

To configure Update Settings

- Click 'Updates' from the 'Add Profile Section' drop-down in the Windows Profile interface

The 'Updates' settings screen will be displayed.



□ Enable auto-updating Comodo Client - Communication

This option enables automatically updating CCC to the latest version.

Update frequency: Daily (default)

Start time: 6 : Minutes AM PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

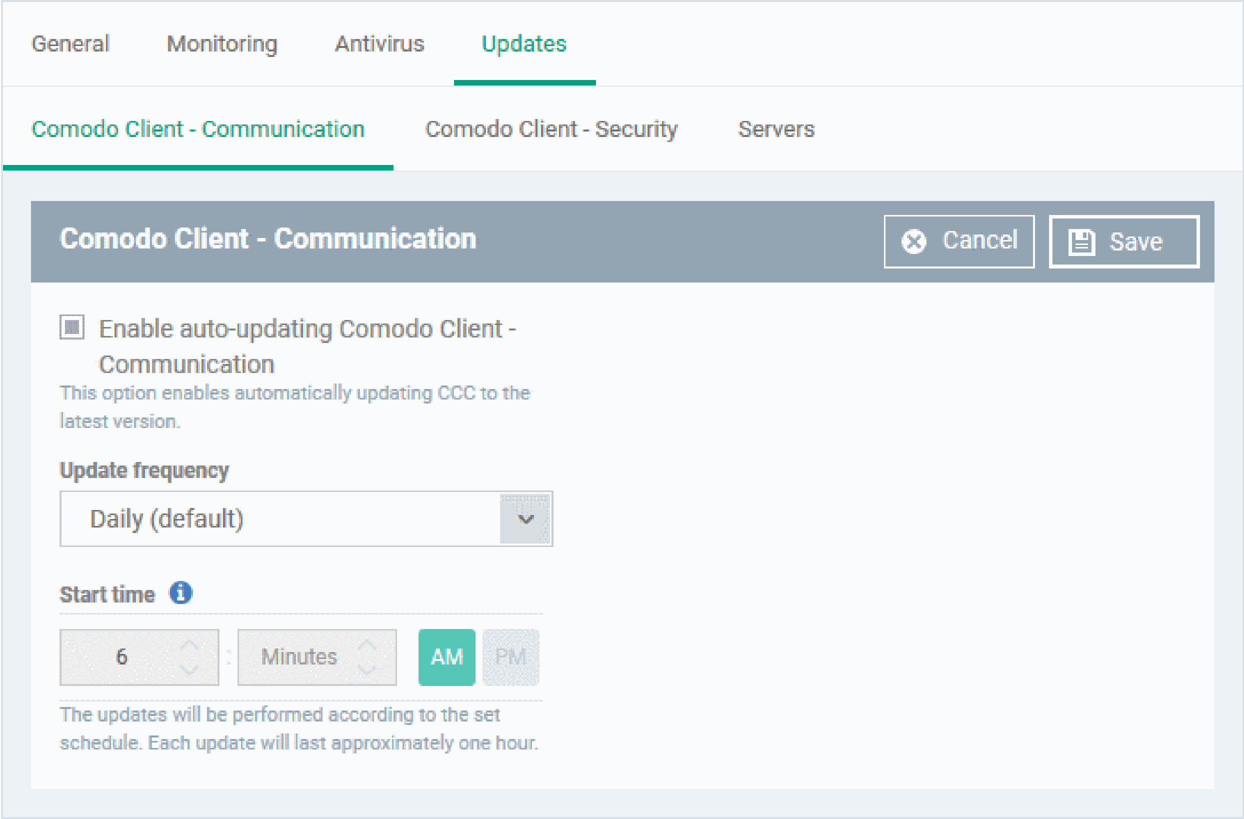
The settings screen for updates contains three tabs:

- **Comodo Client - Communication** - Enable automatic program updates for CCC and configure a schedule.
- **Comodo Client - Security** - Enable automatic program updates for CCS and configure a schedule.
- **Servers** - Configure the download server from which the managed endpoints should download the updates.

Comodo Client - Communication

- Click the 'Comodo Client - Communication' tab

The 'Comodo Client - Communication' tab allows you to enable or disable automatic program updates for the CCC application and set a schedule for the endpoints to check for availability and download the updates.



☐ Enable auto-updating Comodo Client - Communication

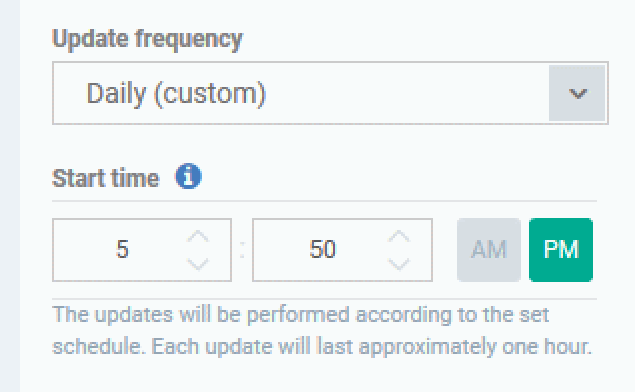
This option enables automatically updating CCC to the latest version.

Update frequency: Daily (default)

Start time: 6 : Minutes AM PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

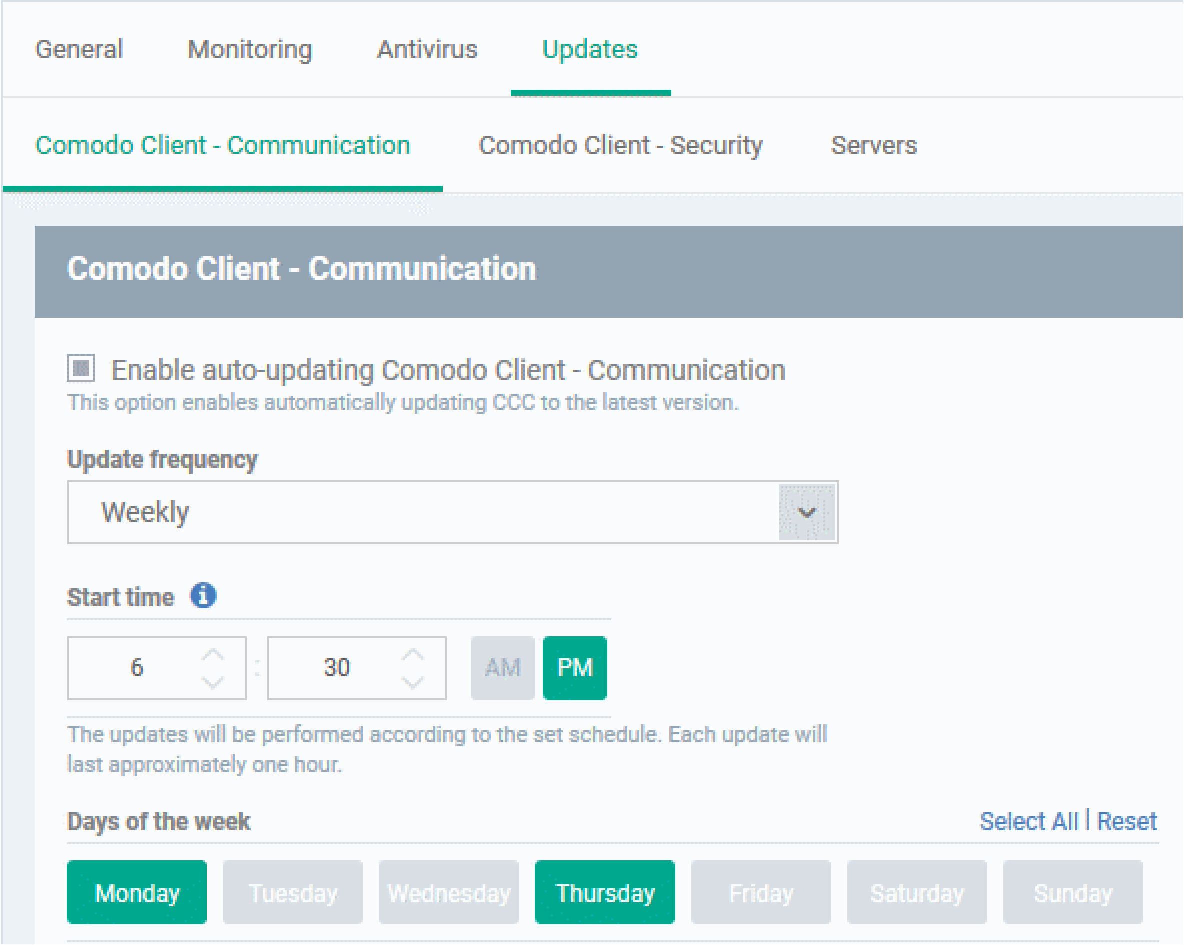
- **Enable auto-updating Comodo Client - Communication** - Makes the endpoint to check the availability of CCC program updates at the location specified under the '**Servers**' tab and if available, updates the application. De-select if you want to disable the auto updates for CCC application. If enabled, you can configure a schedule for the updates.
- **Update Frequency -** Choose the period for automatic updates. The available options are:
  - Daily (Default) - The application will check for updates everyday at 6:00 am everyday
  - Daily (custom) - Enter the time in hours and minutes and choose AM or PM for the auto-update.


Update frequency: Daily (custom)

Start time: 5 : 50 AM PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

  - Weekly - Select the days and specify the time for the updates to be checked every week



Comodo Client - Communication

☒ Enable auto-updating Comodo Client - Communication
This option enables automatically updating CCC to the latest version.

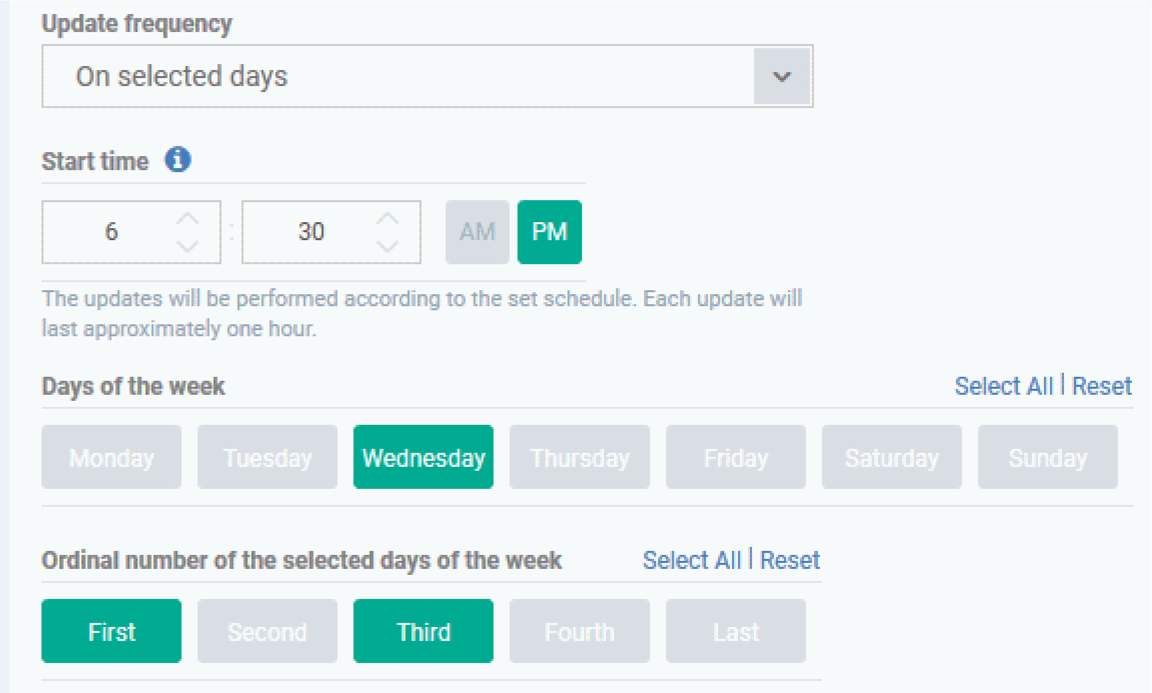
Update frequency: Weekly

Start time: 6 : 30 PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

Days of the week: Monday, Thursday

- On selected days - You can select the custom day(s) in a month for auto update. For example you may wish the auto update to be scheduled on every first and third Wednesdays of every month.


Update frequency: On selected days

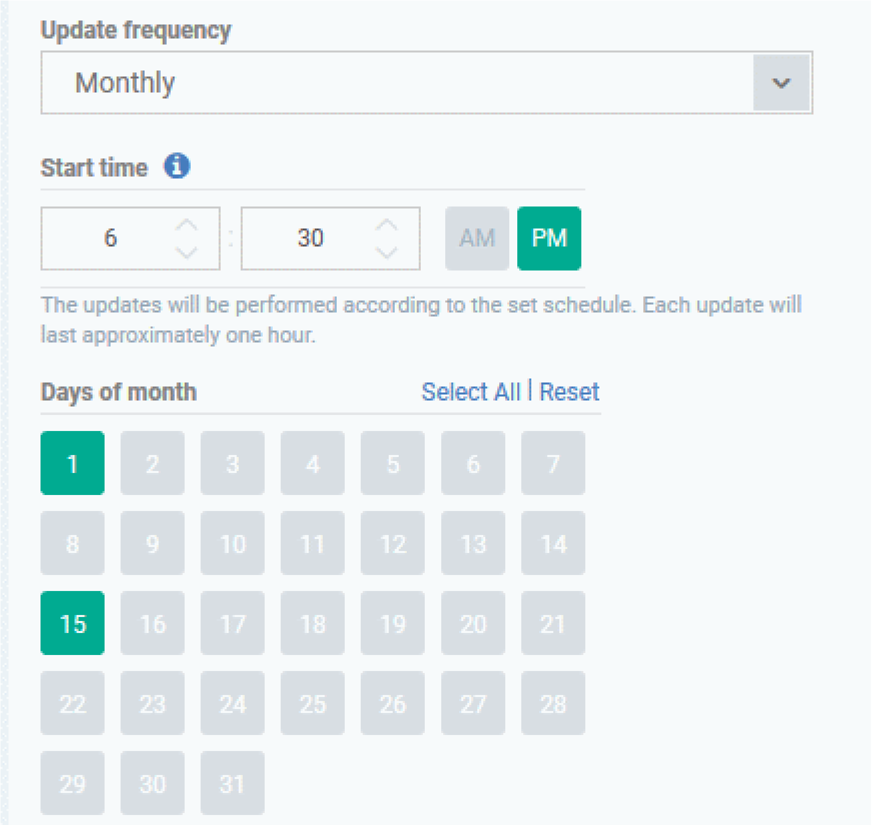
Start time: 6 : 30 PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

Days of the week: Wednesday

Ordinal number of the selected days of the week: First, Third

- Monthly - Select the date(s) and specify the time for the updates to be checked every month



Update frequency: Monthly

Start time: 6 : 30 PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

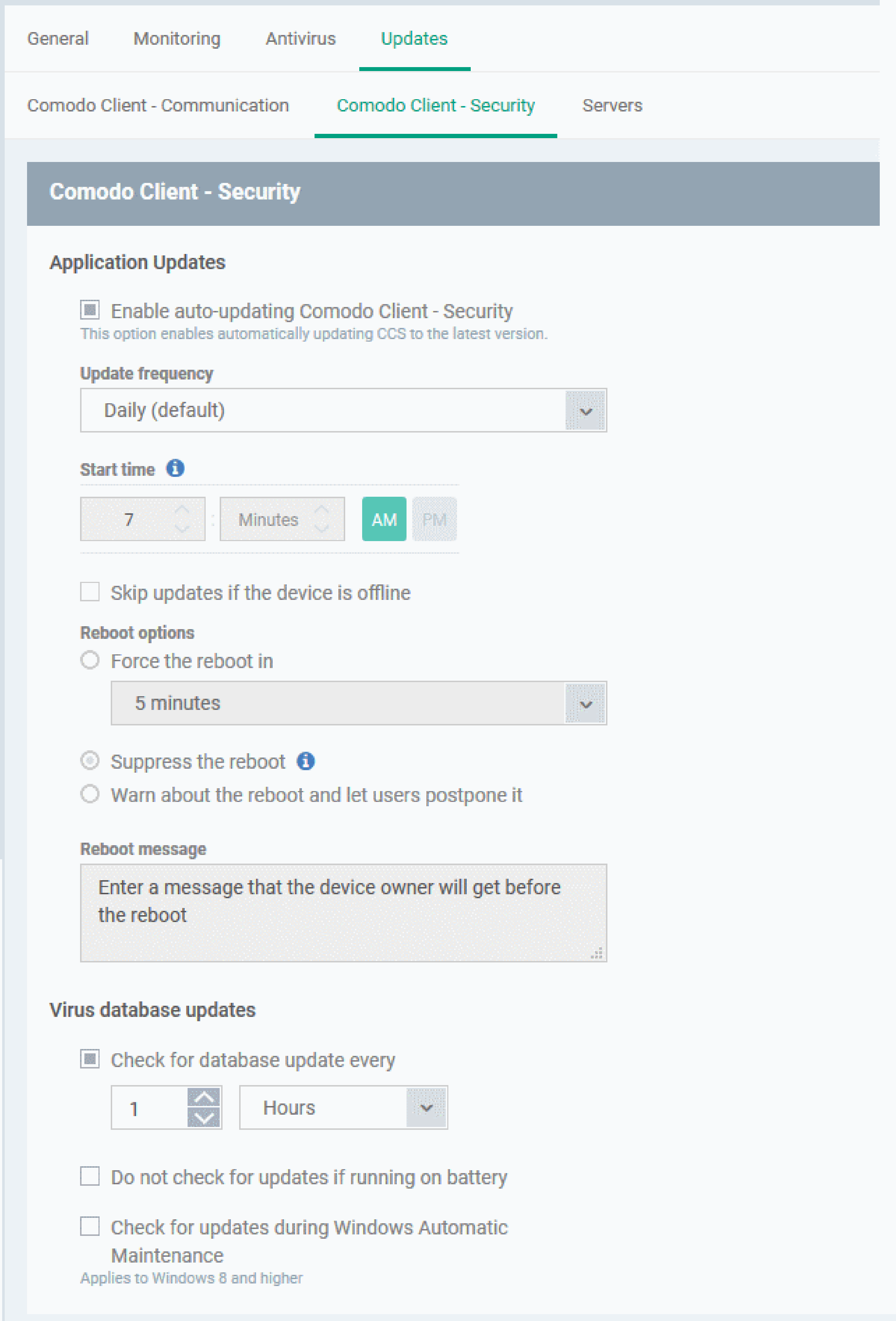
Days of month: 1, 15

- Click 'Save'.

Comodo Client - Security

- Click the 'Comodo Client - Security' tab

The 'Comodo Client - Security' tab allows you to enable or disable automatic program updates and virus signature database updates for the CCS application on the at the endpoints and set a schedule for auto-updates.



Comodo Client - Security

Application Updates

☑ Enable auto-updating Comodo Client - Security
This option enables automatically updating CCS to the latest version.

Update frequency: Daily (default)

Start time: 7 : Minutes AM PM

□ Skip updates if the device is offline

Reboot options

○ Force the reboot in 5 minutes

● Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message: Enter a message that the device owner will get before the reboot

Virus database updates

☑ Check for database update every 1 Hours

□ Do not check for updates if running on battery

□ Check for updates during Windows Automatic Maintenance
Applies to Windows 8 and higher

- **Enable auto-updating Comodo Client - Security** - Makes the endpoint to check the availability of CCS program updates at the location specified under the 'Servers' tab and if available, updates the application. De-select if you want to disable the auto updates for CCS application. If enabled, you can configure a schedule for the updates.

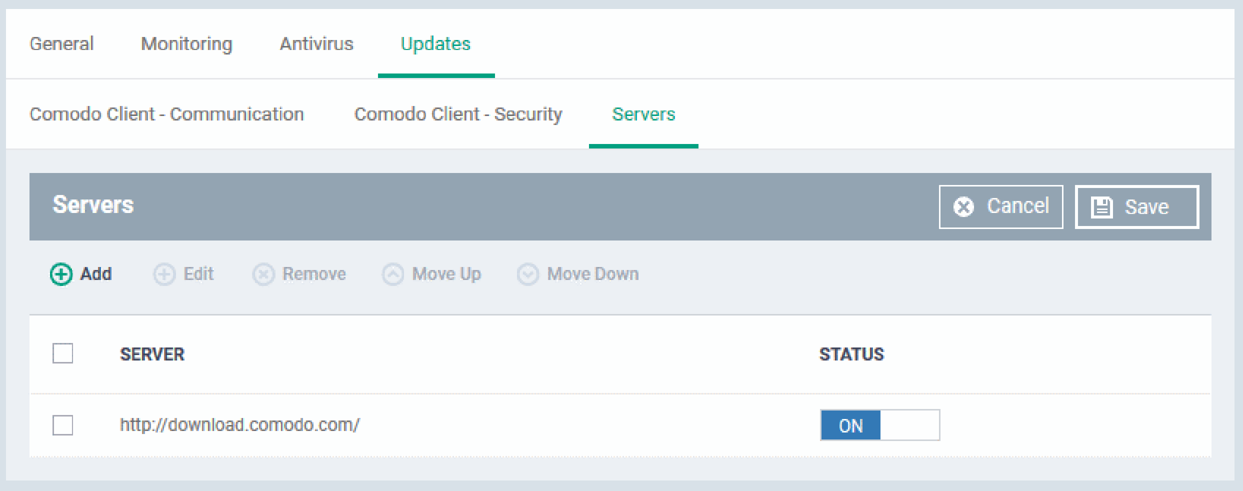
- **Update Frequency -** Choose the period for automatic updates. The available options are:
    - Daily (Default) - The application will check for updates everyday at 7:00 am everyday
    - Daily (custom) - Enter the time in hours and minutes and choose AM or PM for the auto-update.
    - Weekly - Select the days and specify the time for the updates to be checked every week
    - On Selected Days - You can select the custom day(s) in a month for auto update. For example you may wish the auto update to be scheduled on every first and third Wednesdays of every month.
    - Monthly - Select the date(s) and specify the time for the updates to be checked every month
- **Skip updates if the device is offline** - Select this option if you want the updates to be skipped if the endpoint is not connected to ITSM
- **Reboot Options -** Configure how the endpoint should restart after installation of an update
    - 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.
- **Virus database Updates** - Configure when the endpoint should automatically check for virus signature database updates and apply them
    - Check for database update every - If you want to enable automatic and periodical virus signature database updates for the endpoint, select this option and choose the frequency from the drop-down,
    - Do not check for updates if running on battery - This option is useful for devices like a laptop or any other battery driven portable computer. Selecting this option checks for updates only if the computer runs with the adopter connected to mains supply and not on battery.
    - Check for updates during Windows Automatic Maintenance - Applicable only for for Windows 8 and later. Select this option if you want CCS to check for virus database updates when Windows enters into automatic maintenance mode. The update will run at maintenance time in addition to the configured schedule.
- Click 'Save'.

Server

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

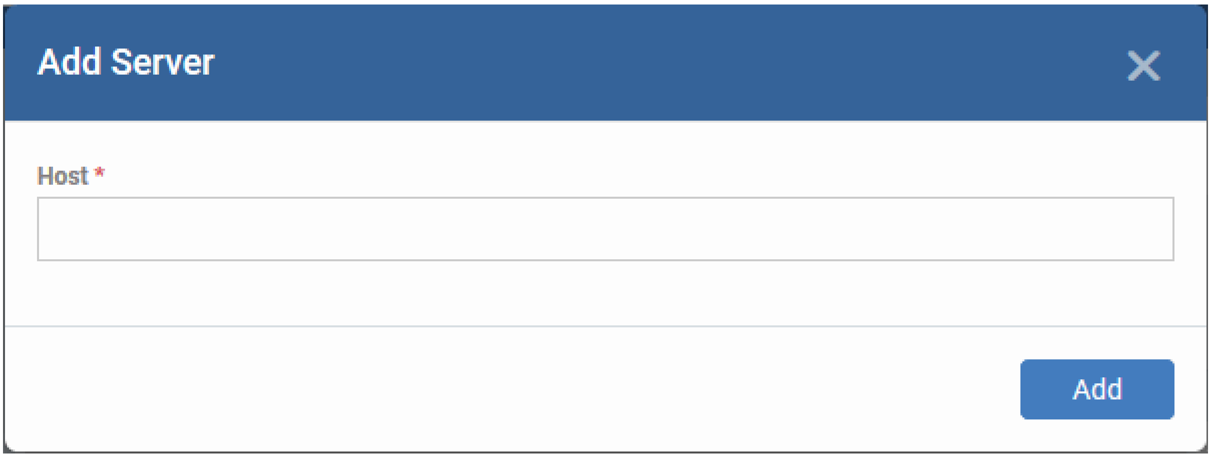


□	SERVER	STATUS
□	http://download.comodo.com/	ON

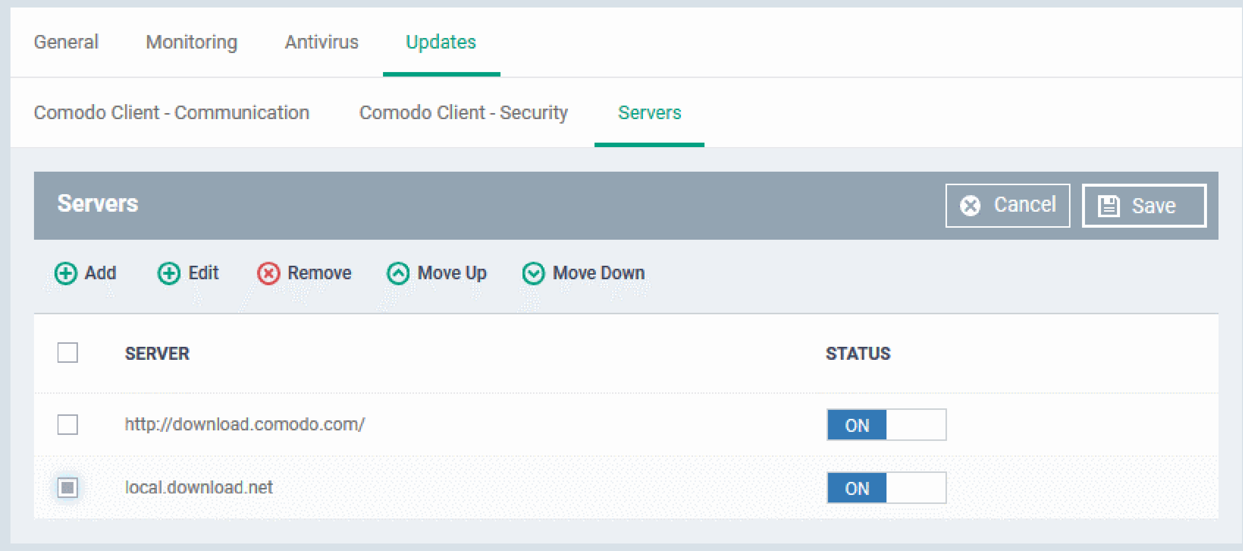
By default, ITSM is set to download from the Comodo servers. You can add your local servers here, edit, reorder the list of servers and remove servers if required.

- 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	STATUS
□	http://download.comodo.com/	ON
☒	local.download.net	ON

- Use the switch in the row of a server to toggle it between on and off status. The server will be checked only if it is enabled for the profile.

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

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 interface lets you configure the overall behavior of the file rating system on Windows devices to which the profile is applied. You can also choose whether or not local file ratings should be consulted.

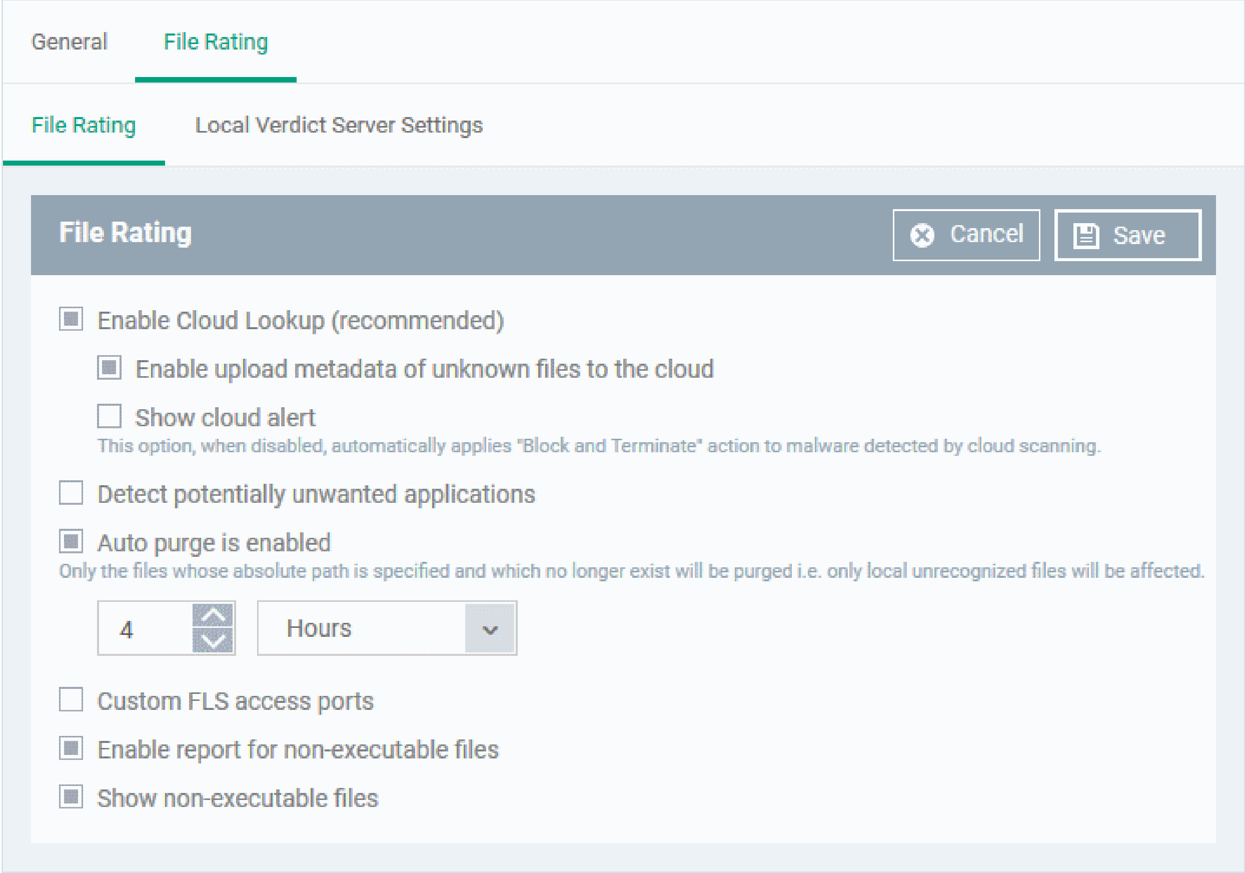
To configure File rating settings

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click 'Add Profile Section' > 'File Rating'

The file rating screen has two tabs:

- **File Rating** - Enable file rating and configure overall behavior.
- **Local Verdict Server Settings** - Choose whether ITSM should obey or ignore the trust rating of files saved by the local installation. If disabled, file rating scans will only consider the verdicts of the cloud server.

File Rating Settings



☒ Enable Cloud Lookup (recommended)

☒ Enable upload metadata of unknown files to the cloud

□ Show cloud alert

This option, when disabled, automatically applies "Block and Terminate" action to malware detected by cloud scanning.

□ Detect potentially unwanted applications

☒ Auto purge is enabled

Only the files whose absolute path is specified and which no longer exist will be purged i.e. only local unrecognized files will be affected.

4 Hours

□ Custom FLS access ports

☒ Enable report for non-executable files

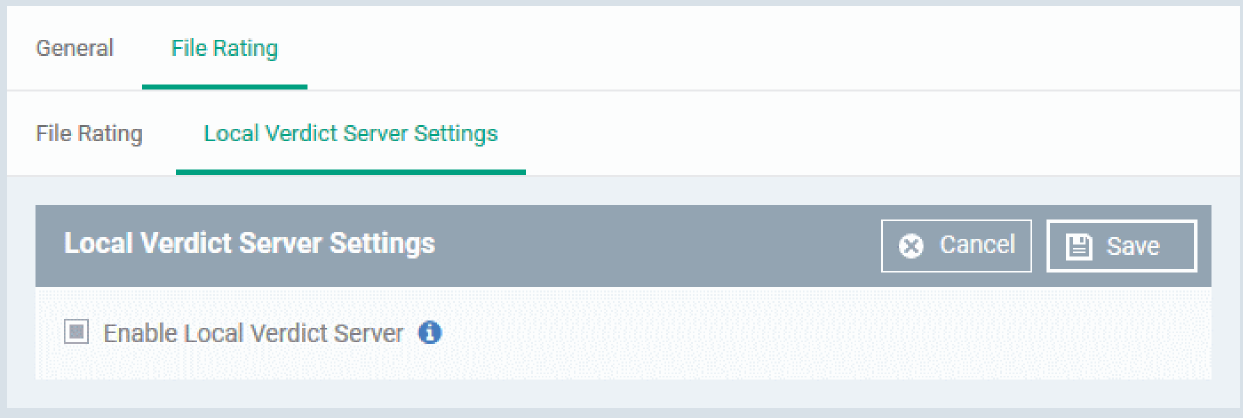
☒ Show non-executable files

File Rating Configuration - Table of Parameters	
Form Element	**Description**
Enable Cloud Lookup	Enable or disable cloud-based file rating. (***Default = Enabled***)
Enable upload metadata of unknown files to the cloud	If enabled, anonymized information about unknown files will be uploaded to Comodo servers. This allows us to analyze and whitelist/blacklist files more effectively. (***Default = Enabled***)
Show Cloud Alert	Choose whether to show an alert on the device when malware is found during a file rating scan. If disabled, CCS will automatically block and delete any discovered malware. (***Default = Disabled***)
Detect potentially unwanted applications	A potentially unwanted application (PUA) is an app that: • A user may or may not be aware is installed on their computer. • May have functionality and objectives that are not clear to the user. PUAs include adware and browser toolbars. They are often installed as an 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 may 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.

File Rating Configuration - Table of Parameters	
	CCS will show an alert on the endpoint if it detects a PUA and a log entry is created. (***Default = Disabled***)
Auto-Purge is enabled	CCS checks the file list and removes invalid and obsolete entries. You can specify the interval at which the check should take place. (***Default = Enabled***)
Auto Purge Period	The time interval at which auto-purge operations are performed. • Enter the time interval in hours. (***Default = Four hours***)
Custom FLS access ports	Define custom ports through which the file lookup service will connect. • Select the protocol(s) and enter the port details for UDP or TCP connections. (***Default = Disabled***)
Enable report for non-executable files	If enabled, information about non-executable files will be reported to ITSM. (***Default = Enabled***)
Show non-executable files	If enabled, non-executable files will also be shown in the 'File List' interface of CCS on the endpoint. To access the file list in CCS, click 'Tasks' > 'Advanced Tasks' > 'Advanced settings' > 'Security settings' > 'File Rating' > 'File list'. (***Default = Enabled***)

- Click 'Save' to apply your file rating settings.

Local Verdict Server Settings



□ Enable Local Verdict Server

- **Enable Local Verdict Server** - Local trust verdicts are those stored in the CCS installation on the endpoint. For example, a user can assign a trust level to a file when answering an alert. Users and admins can also manually assign a trust verdict to a file in CCS.
    - Enabled - CCS will obey the local trust verdict on a file in the event of a conflict with the cloud verdict.
    - Disabled - CCS will ignore local verdicts and only use cloud verdicts to determine the trust level of a file

      (***Default = Enabled***)
- Click 'Save' to apply your changes.

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.

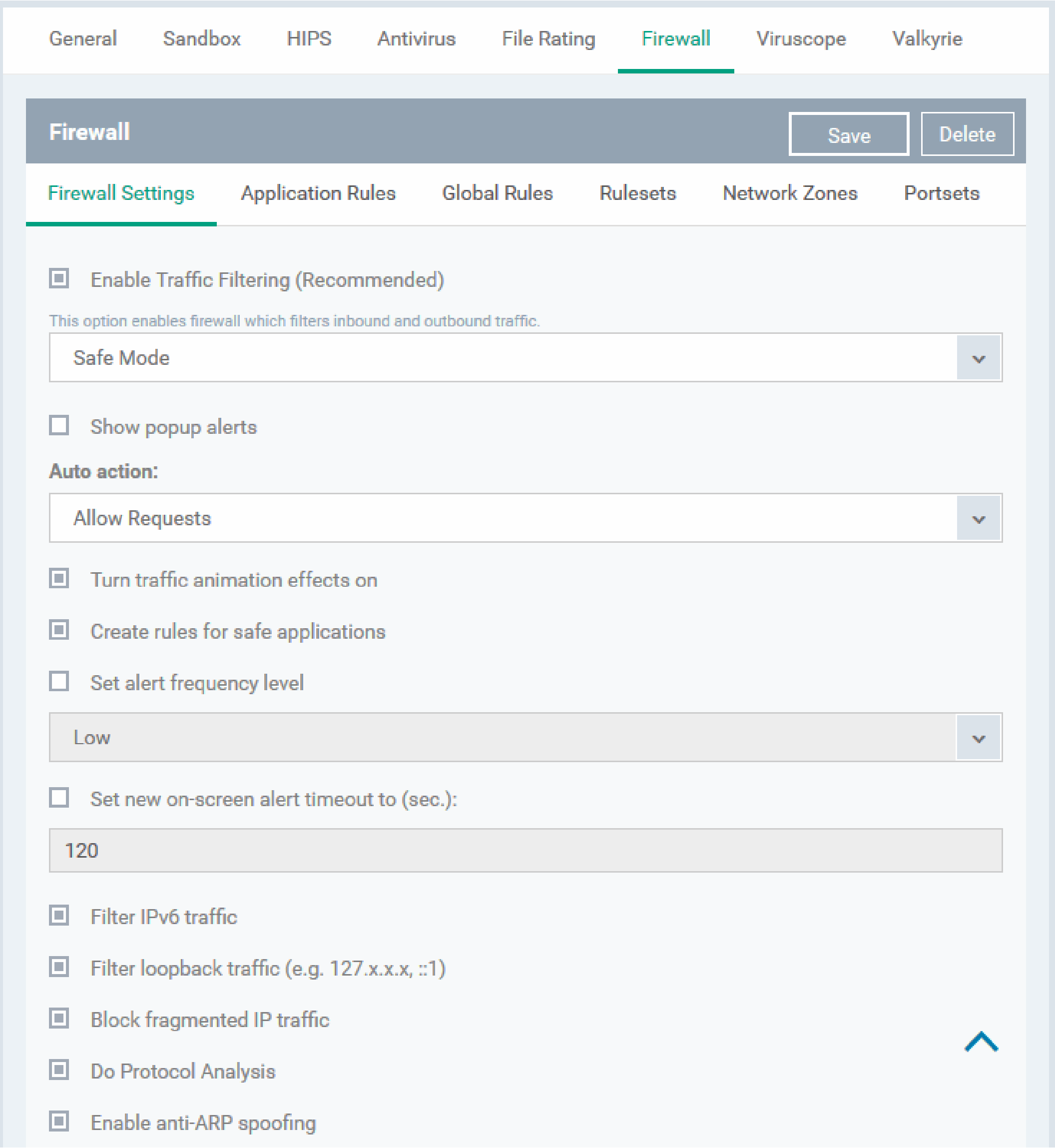
To configure Firewall Settings and Traffic Filtering Rules

- 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



☑ Enable Traffic Filtering (Recommended)

This option enables firewall which filters inbound and outbound traffic.

Safe Mode

☐ Show popup alerts

Auto action:

Allow Requests

☑ Turn traffic animation effects on

☑ Create rules for safe applications

☐ Set alert frequency level

Low

☐ Set new on-screen alert timeout to (sec.):

120

☑ Filter IPv6 traffic

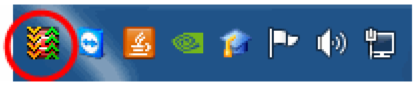
☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☑ Block fragmented IP traffic

☑ Do Protocol Analysis

☑ Enable anti-ARP spoofing

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 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.

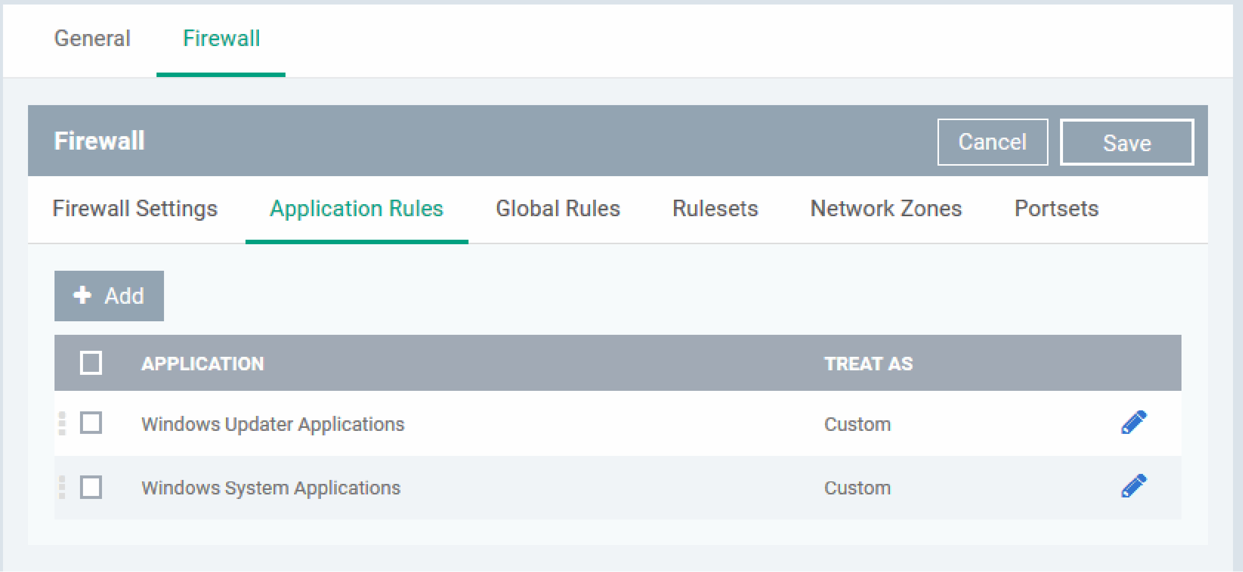
Firewall Configuration - Table of Parameters	
	 You can enable or disable the animation to be displayed at the endpoint.
Create rules for safe applications	Comodo Firewall trusts the applications if: • The application/file is included in the Trusted Files list under File Rating Settings; • The application 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 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	Determines how long the Firewall shows an alert for, without any user intervention

Firewall Configuration - Table of Parameters	
timeout to:	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 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***0.
Do Protocol Analysis	Protocol Analysis is key to the detection of fake packets used in denial of service (DOS) attacks.

Firewall Configuration - Table of Parameters	
	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***).

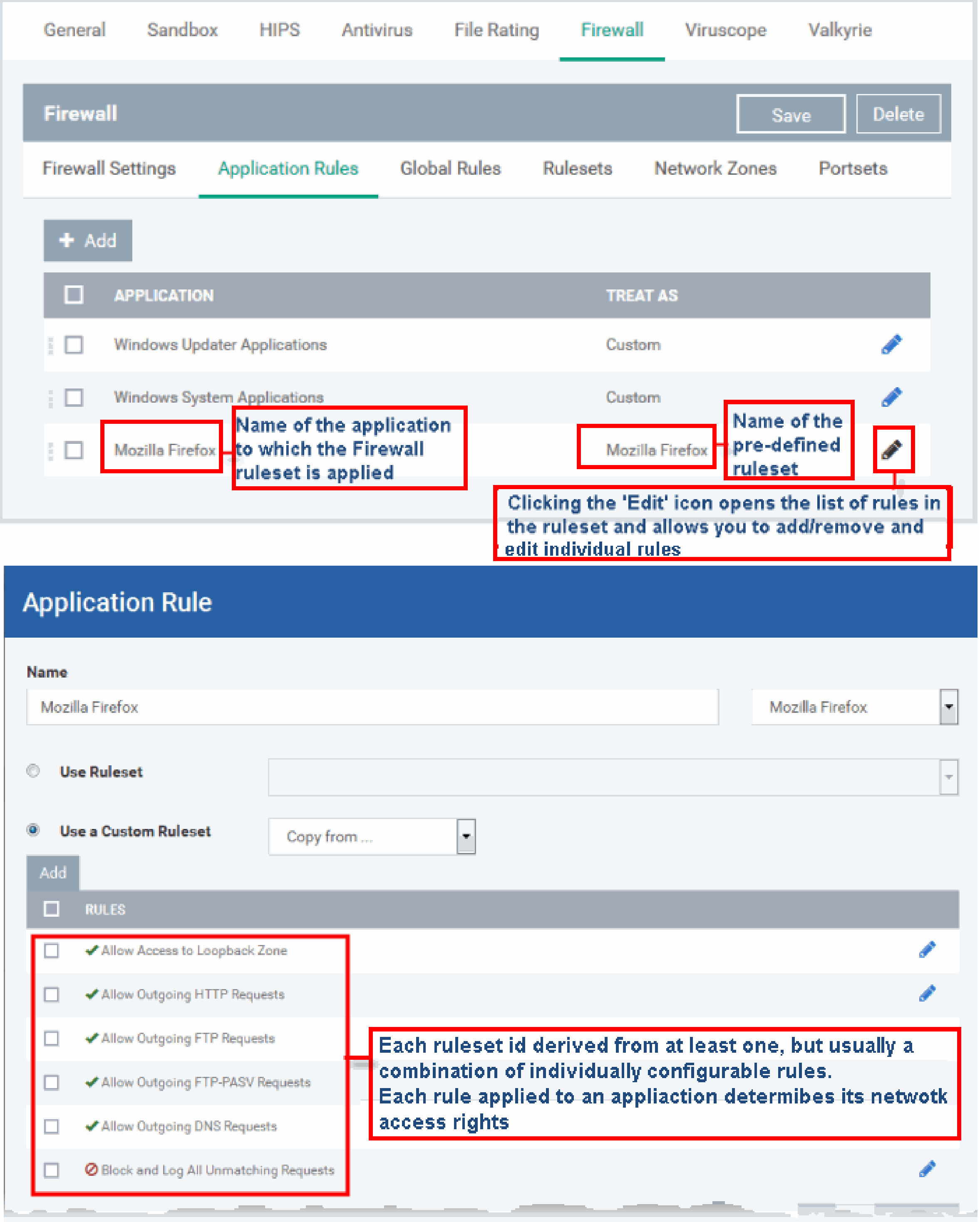
Application Rules

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.



□	APPLICATION	TREAT AS
□	Windows Updater Applications	Custom
□	Windows System Applications	Custom

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.



□ APPLICATION	TREAT AS
□ Windows Updater Applications	Custom
□ Windows System Applications	Custom
□ Mozilla Firefox	Mozilla Firefox

Name of the application to which the Firewall ruleset is applied

Name of the pre-defined ruleset

Clicking the 'Edit' icon opens the list of rules in the ruleset and allows you to add/remove and edit individual rules

Name: Mozilla Firefox | Mozilla Firefox

○ Use Ruleset

● Use a Custom Ruleset | Copy from ...

□ RULES
□ ✓ Allow Access to Loopback Zone
□ ✓ Allow Outgoing HTTP Requests
□ ✓ Allow Outgoing FTP Requests
□ ✓ Allow Outgoing FTP-PASV Requests
□ ✓ Allow Outgoing DNS Requests
□ ⊘ Block and Log All Unmatching Requests

Each ruleset id derived from at least one, but usually a combination of individually configurable rules.
Each rule applied to an appliaction determibes its netwotk access rights

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.**

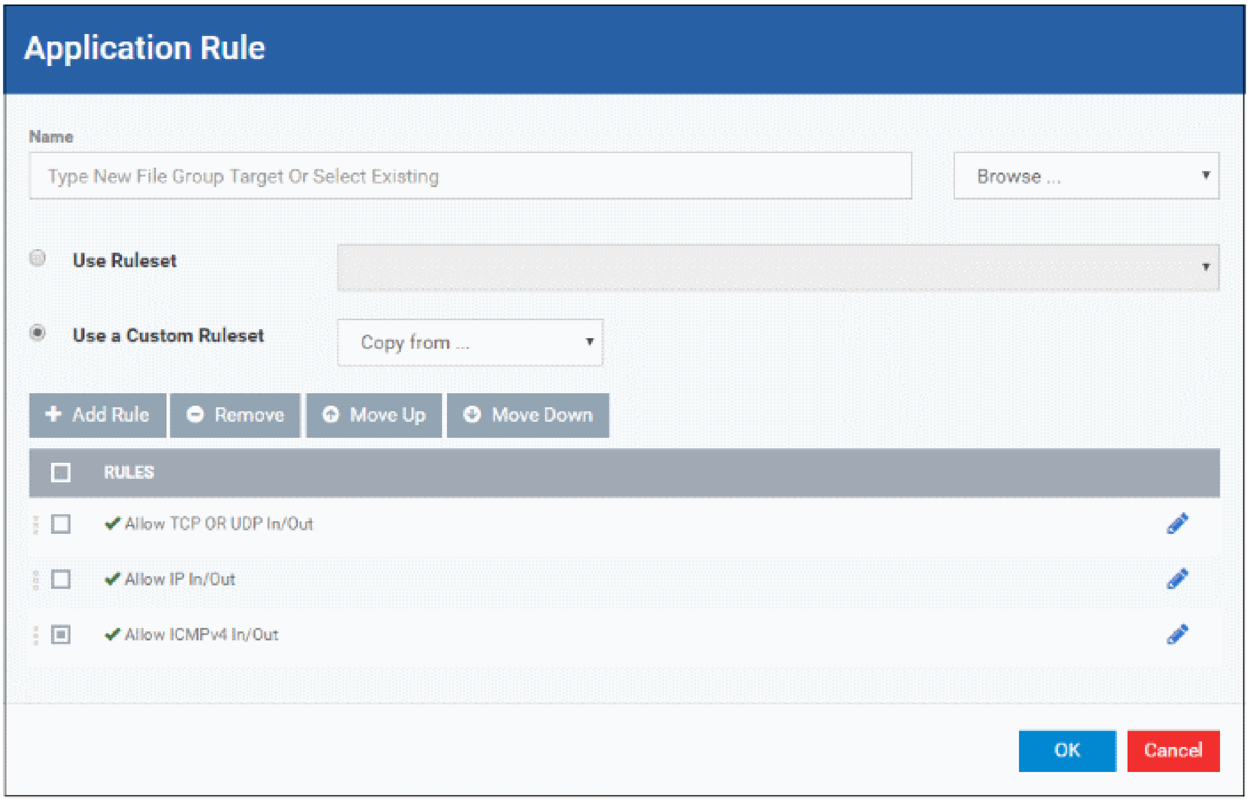
- See **Application Rule interface** for an introduction to the rule setting interface
- See **Creating and Modifying Firewall Rulesets** to learn how to create and edit Firewall rulesets
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual 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 + Add or 'Edit' icon beside a ruleset, from the options in 'Application Rules' interface.



Type New File Group Target Or Select Existing

○ Use Ruleset

● Use a Custom Ruleset   Copy from ...

□	RULES
□	✓ Allow TCP OR UDP In/Out
□	✓ Allow IP In/Out
□	✓ Allow ICMPv4 In/Out

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

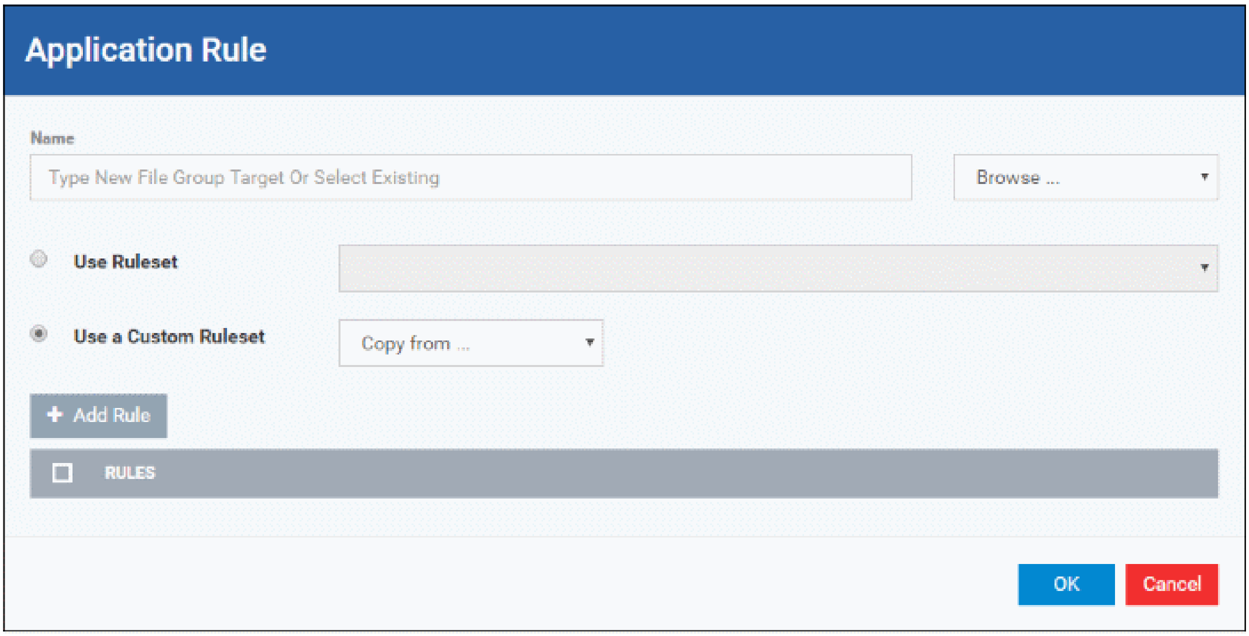
To begin defining an application's Firewall ruleset, you need take two basic steps.

- 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 + Add at the top of the list in the 'Application Rules' interface.

The 'Application Rule' interface will open as shown below:



Application Rule

Name

Type New File Group Target Or Select Existing

○ Use Ruleset

● Use a Custom Ruleset

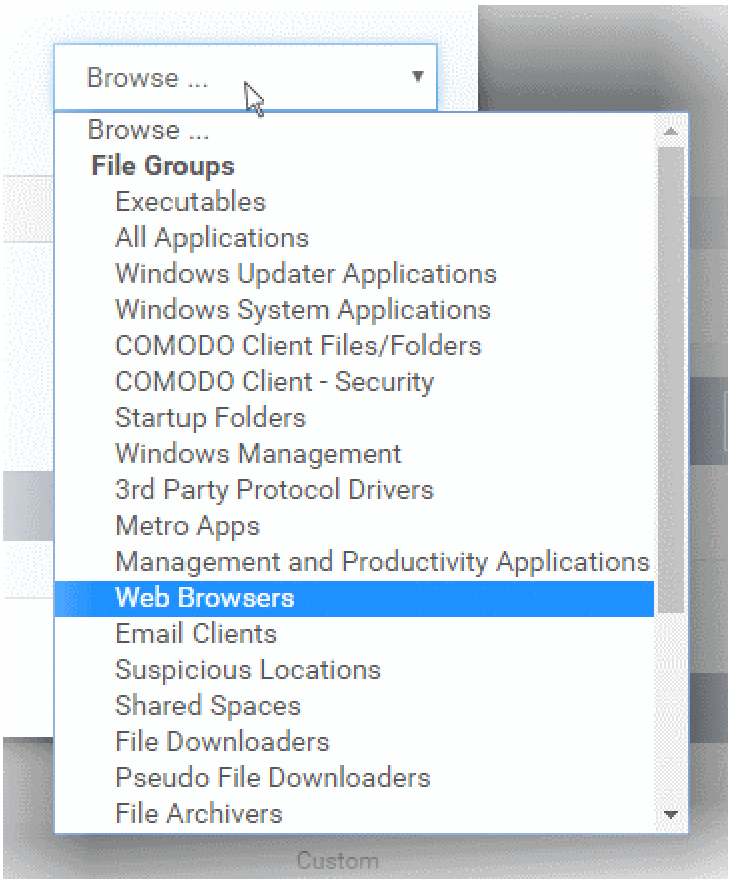
Because this is a new application, the 'Name' field is blank. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

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

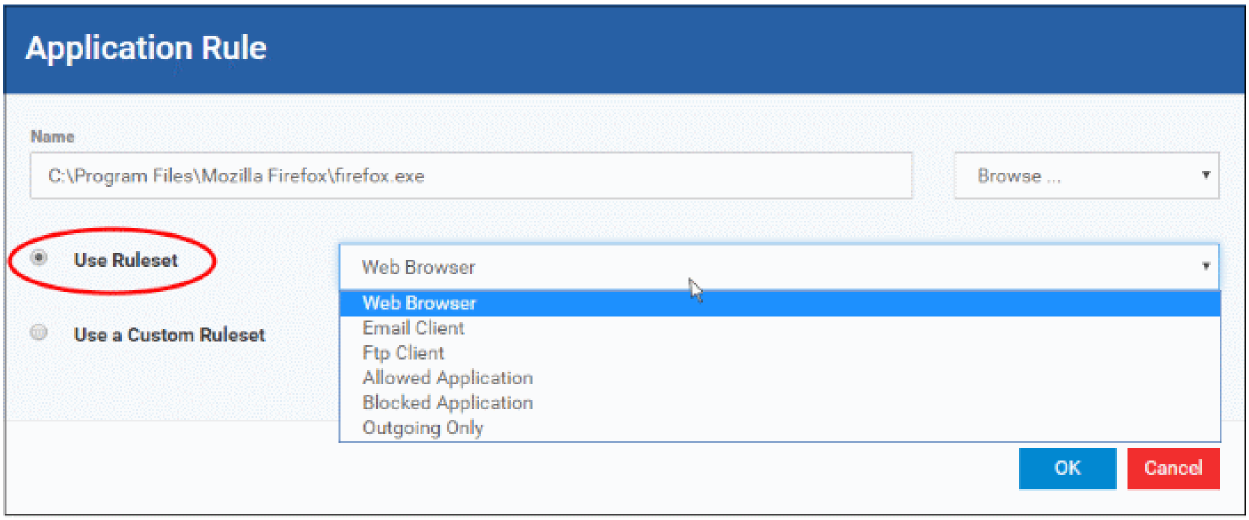
- Open the drop-down beside the 'Name' field and choose the Application Group to which the ruleset is to be applied. Choosing a 'File Group' allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset 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).***



Application Rule

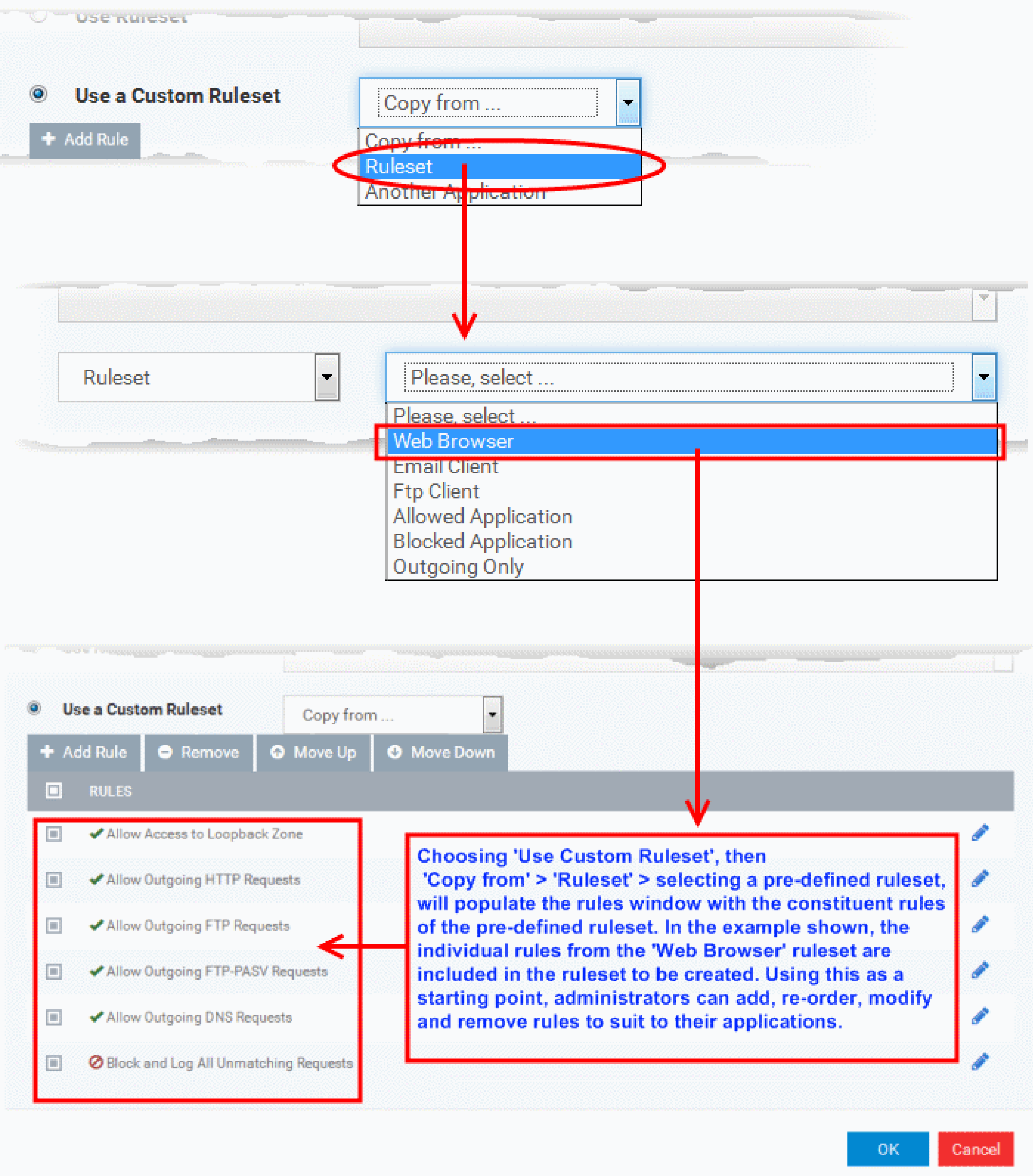
Name: C:\Program Files\Mozilla Firefox\firefox.exe

● Use Ruleset: Web Browser

○ Use a Custom Ruleset

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***).



Choosing 'Use Custom Ruleset', then 'Copy from' > 'Ruleset' > selecting a pre-defined ruleset, will populate the rules window with the constituent rules of the pre-defined ruleset. In the example shown, the individual rules from the 'Web Browser' ruleset are included in the ruleset to be created. Using this as a starting point, administrators can add, re-order, modify and remove rules to suit to their applications.

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.

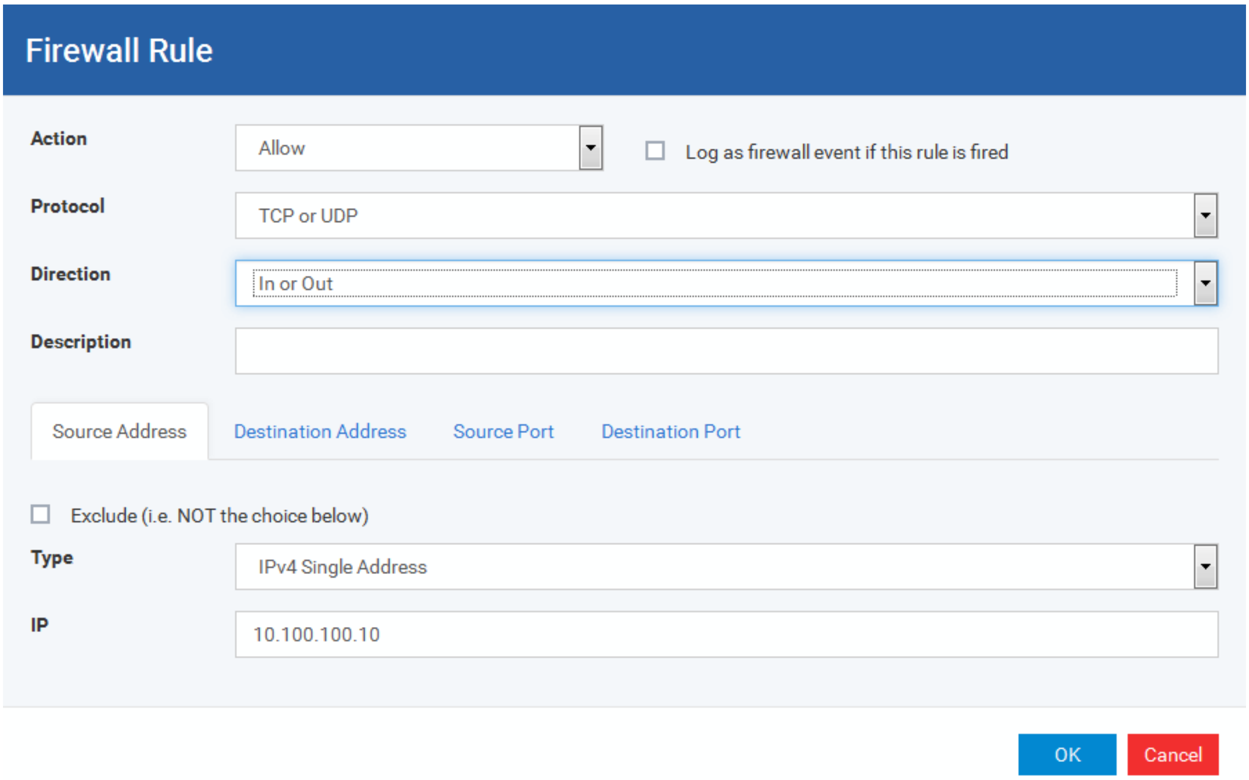
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

* 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**'.



Firewall Rule

Action: Allow □ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description:

□ Exclude (i.e. NOT the choice below)

Type: IPv4 Single Address

IP: 10.100.100.10

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.

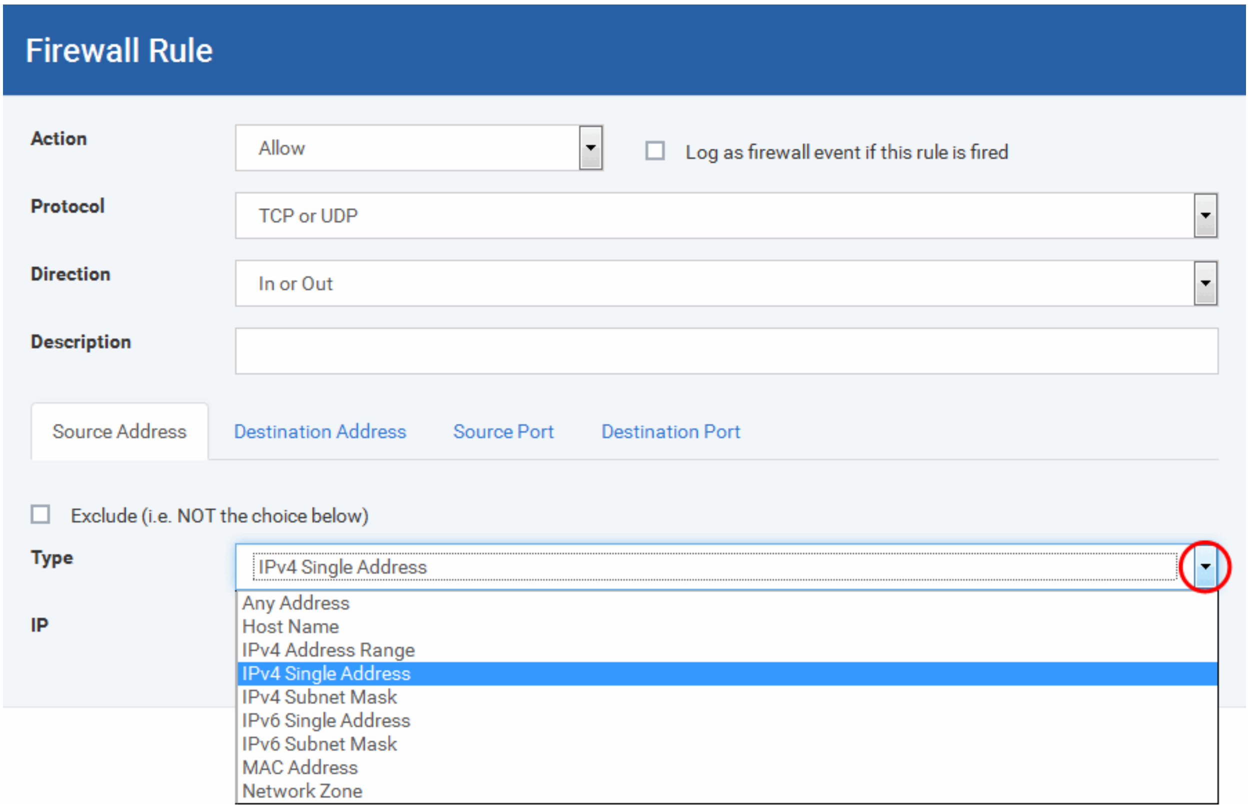
- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the firewall event log 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**,' '**UDP'** or '**TCP or UDP'**

If you select 'TCP', 'UDP' 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



Firewall Rule

Action: Allow
□ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description:

□ Exclude (i.e. NOT the choice below)

Type: IPv4 Single Address

IP

Source Address and Destination Address:

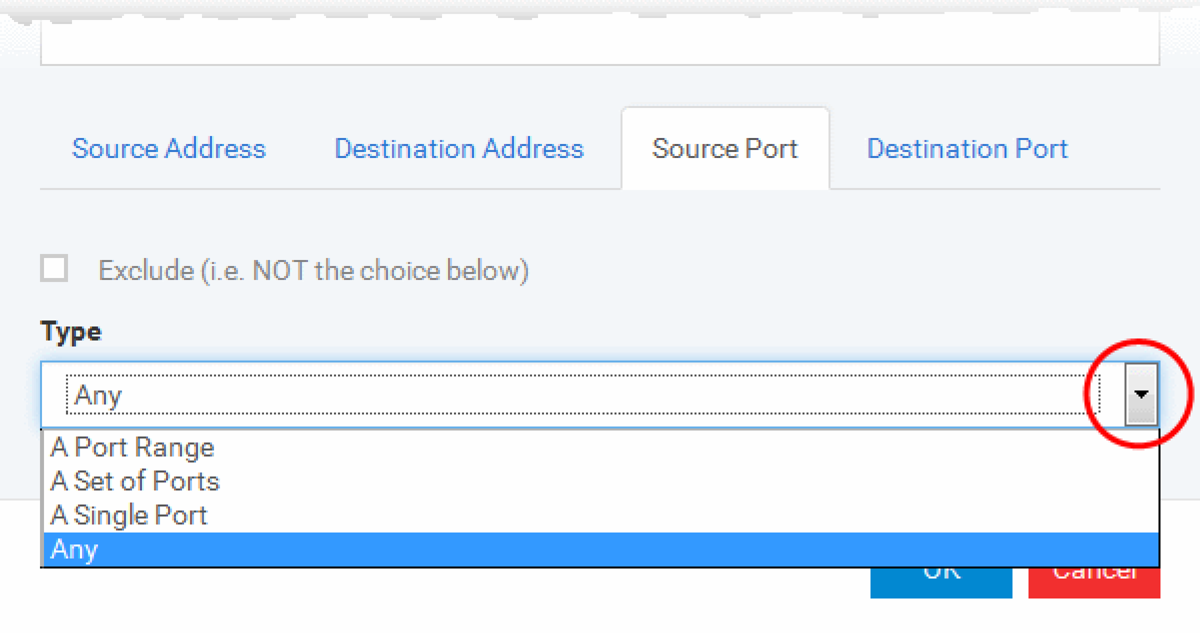
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 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**'.

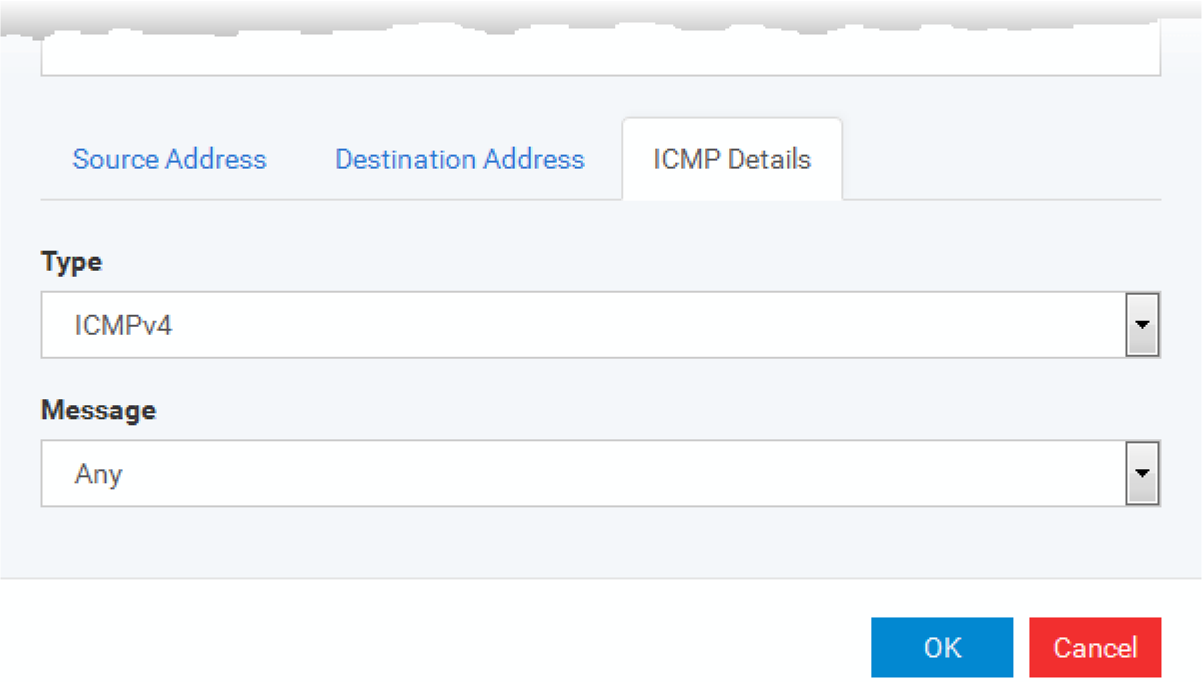
ii. **ICMP**

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.

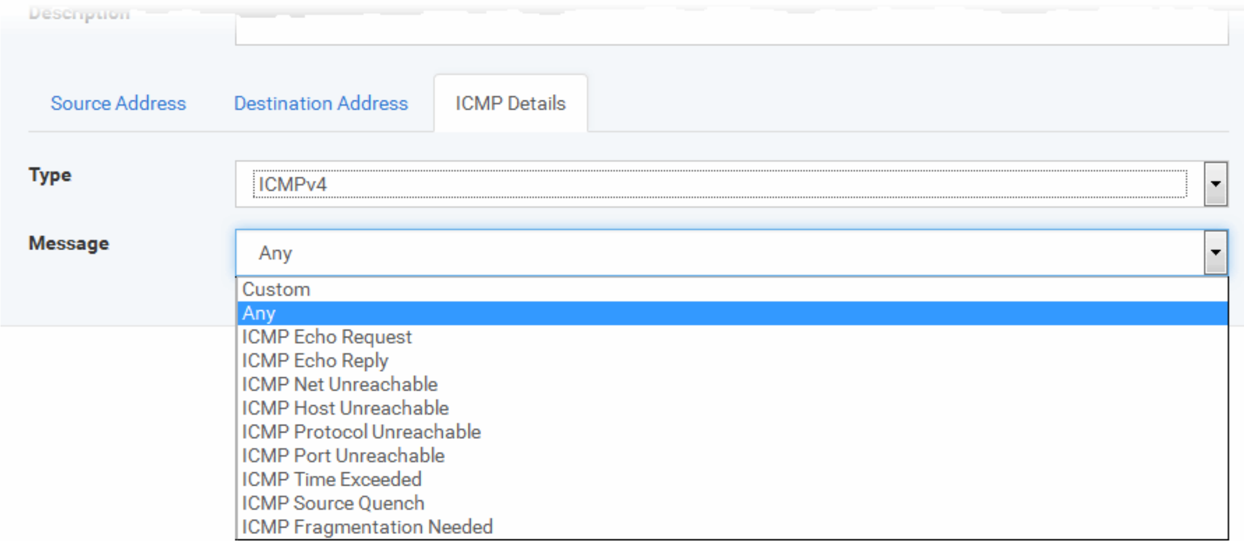
- **ICMP Details**

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.



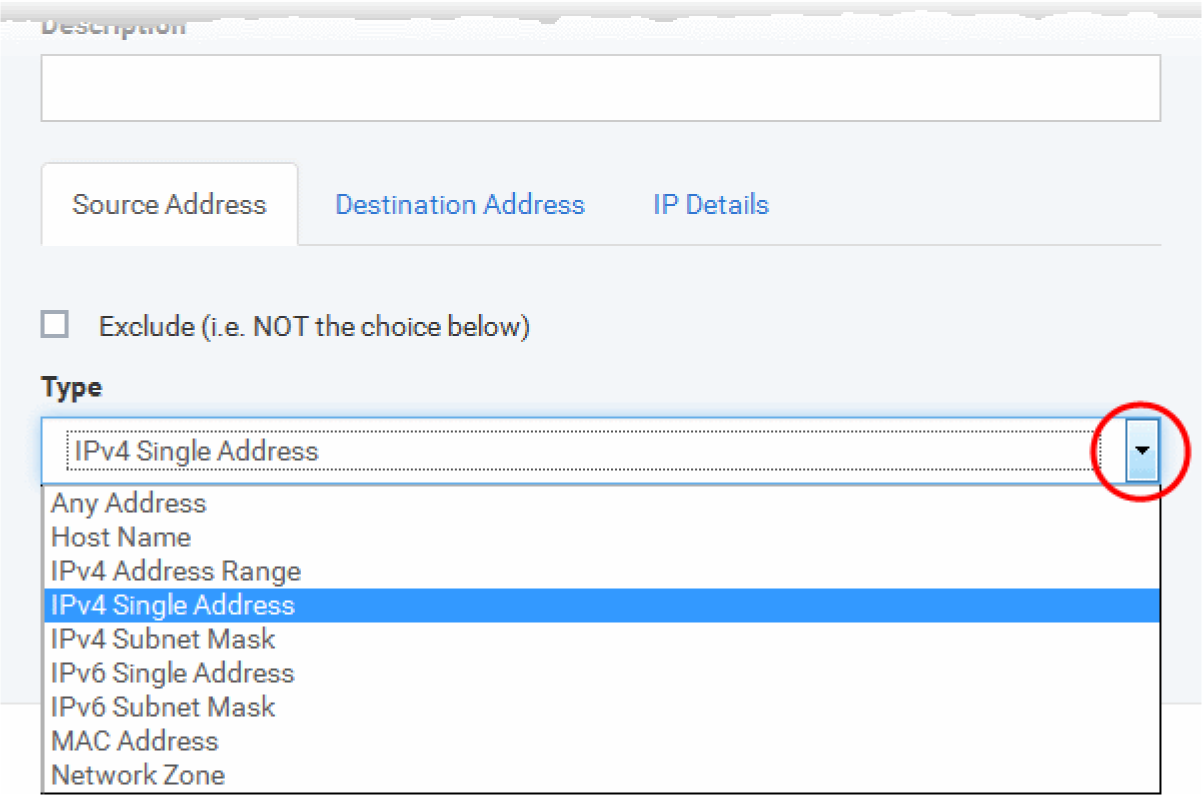
2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.
3. Specify ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.



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.


Description

Source Address | Destination Address | IP Details

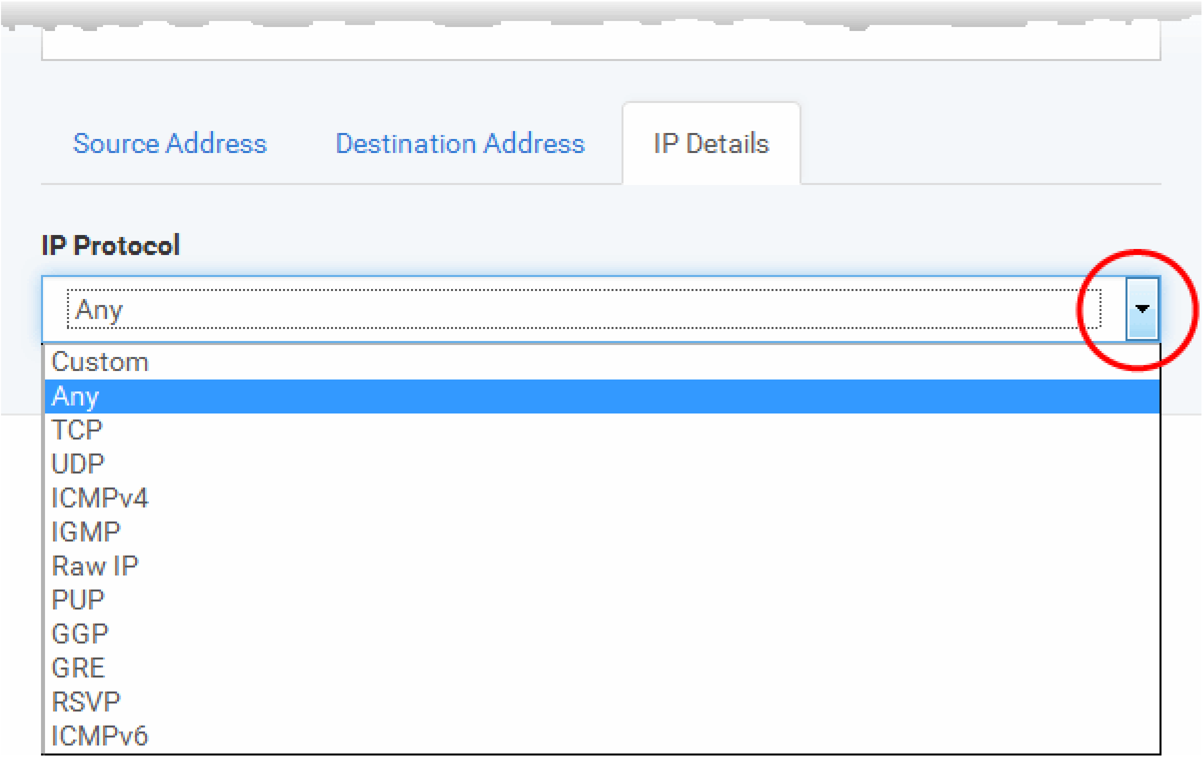
□ Exclude (i.e. NOT the choice below)

Type

IPv4 Single Address

- **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.


Source Address | Destination Address | IP Details

IP Protocol

Any

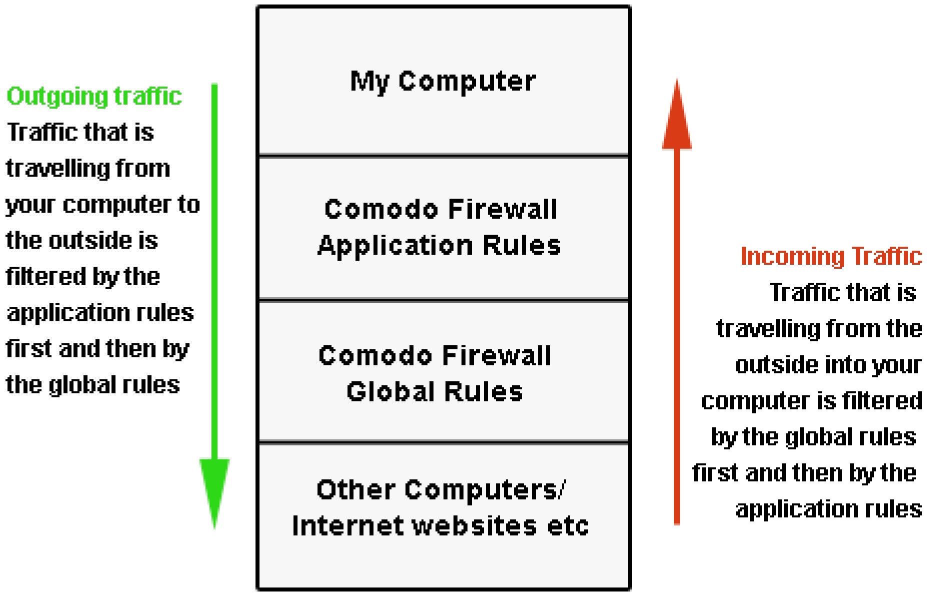
- Click 'OK' to save the firewall rule.

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.

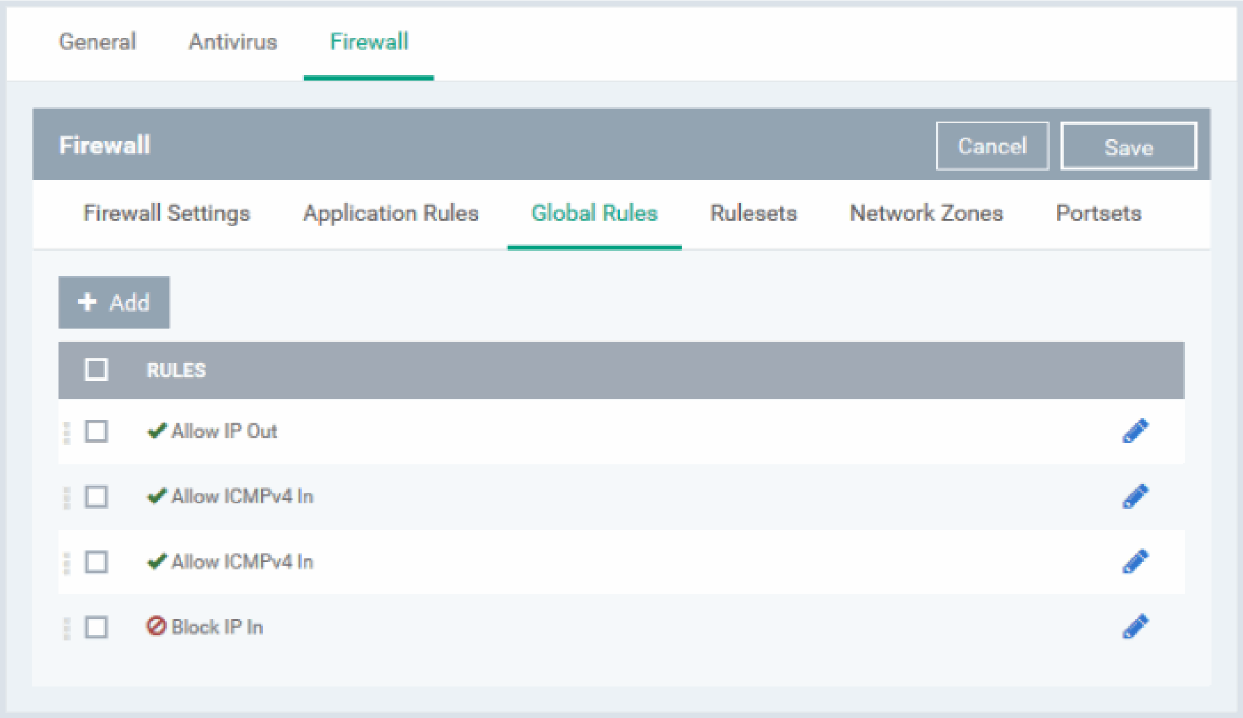
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.


Outgoing traffic
Traffic that is travelling from your computer to the outside is filtered by the application rules first and then by the global rules
My Computer
Comodo Firewall Application Rules
Comodo Firewall Global Rules
Other Computers/ Internet websites etc
Incoming Traffic
Traffic that is travelling from the outside into your computer is filtered by the global rules first and then by the application rules

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.



□	RULES
□	✓ Allow IP Out
□	✓ Allow ICMPv4 In
□	✓ Allow ICMPv4 In
□	⊘ Block IP In

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.

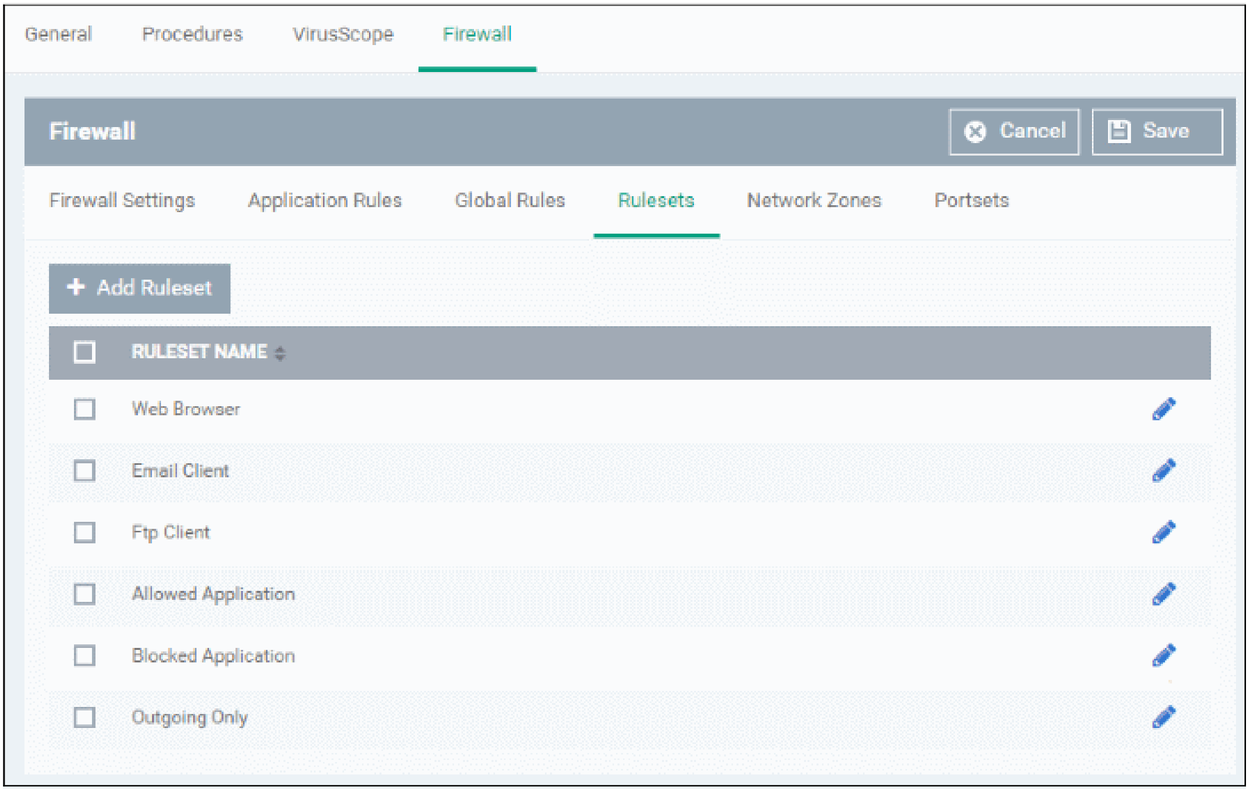
- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration.

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.



□	RULESET NAME	
□	Web Browser	✎
□	Email Client	✎
□	Ftp Client	✎
□	Allowed Application	✎
□	Blocked Application	✎
□	Outgoing Only	✎

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'.

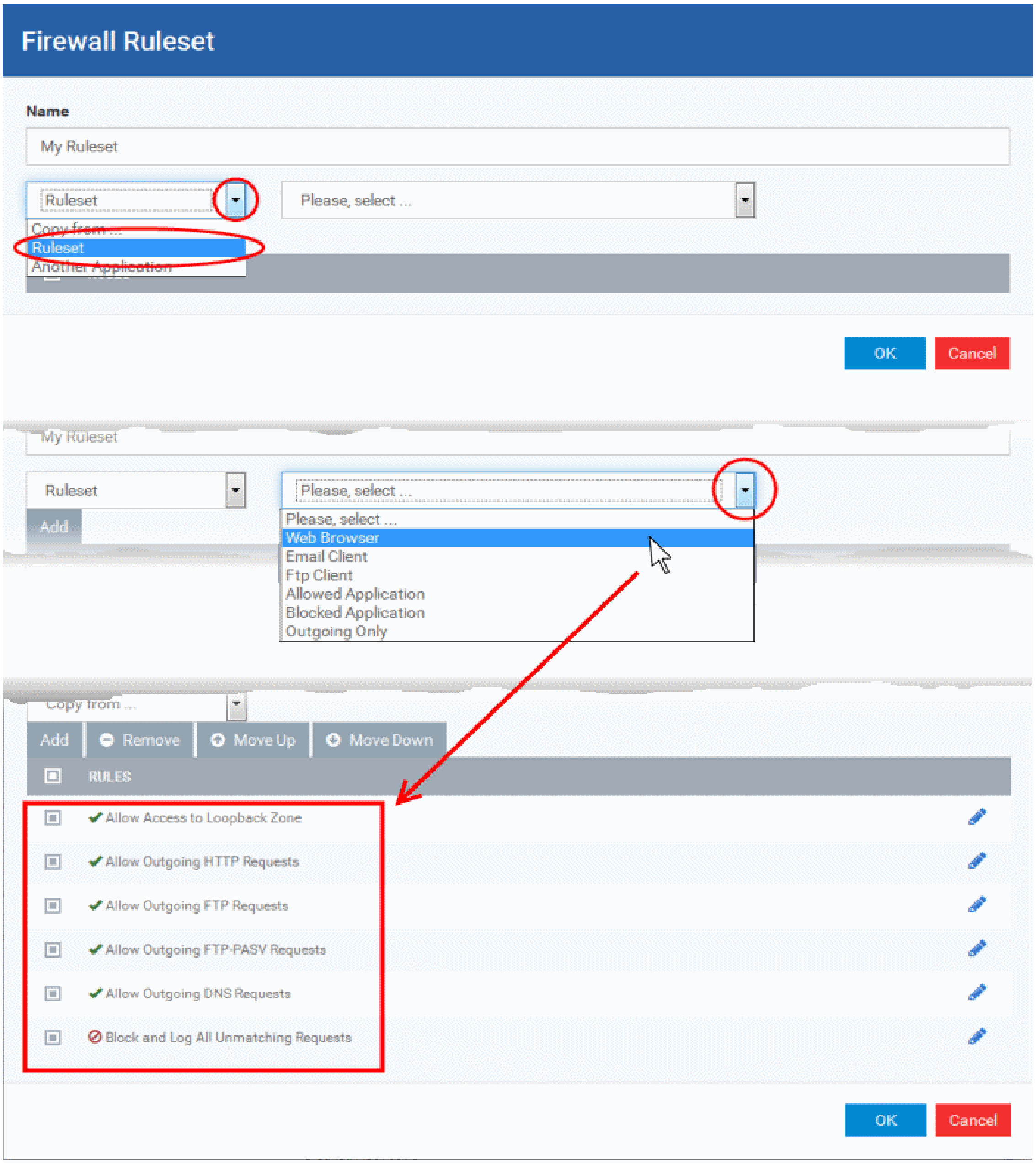
Creating a new ruleset

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.



Firewall Ruleset

Name: My Ruleset

RULES

- ✓ Allow Access to Loopback Zone
- ✓ Allow Outgoing HTTP Requests
- ✓ Allow Outgoing FTP Requests
- ✓ Allow Outgoing FTP-PASV Requests
- ✓ Allow Outgoing DNS Requests
- ⊘ Block and Log All Unmatching Requests

- 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

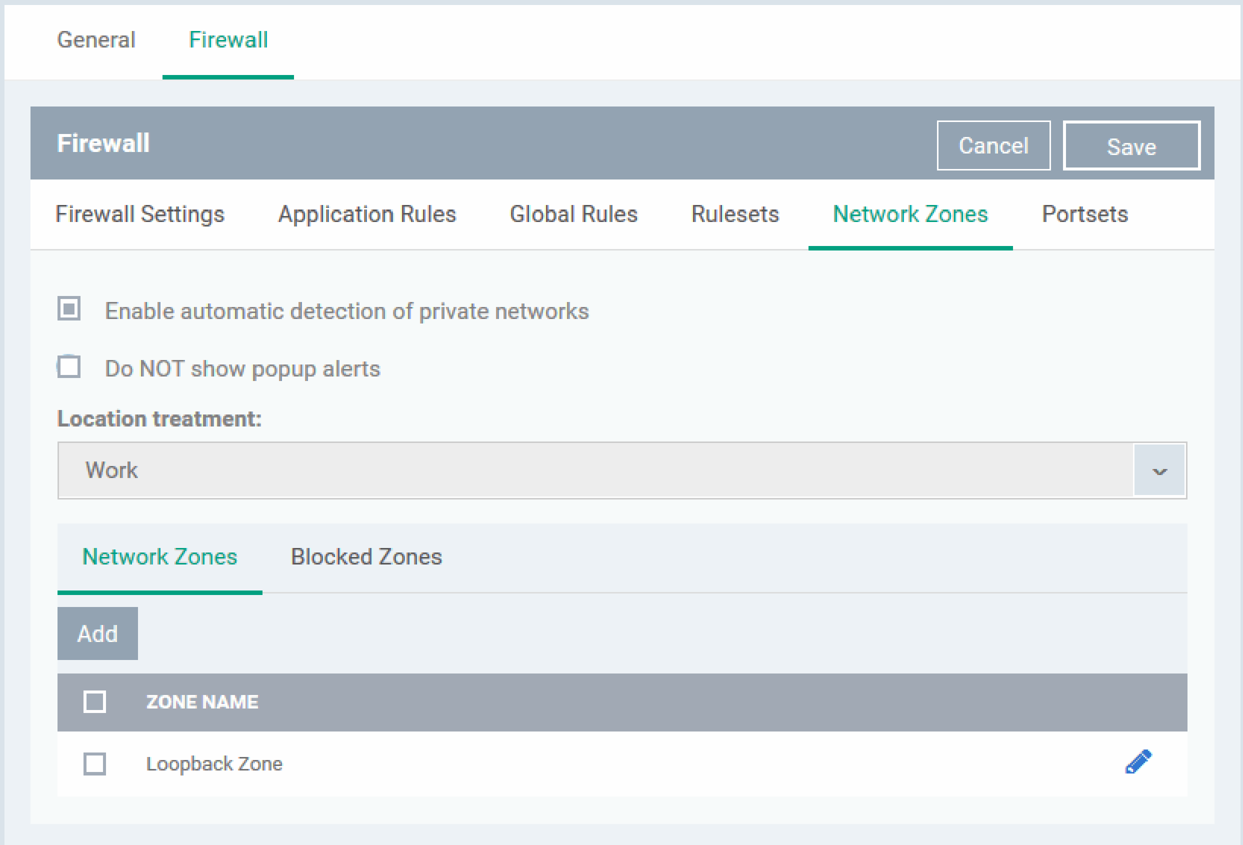
- Click on the 'Edit' icon ✎ beside Ruleset Name in the list.
- Details of the process from this point on can be found under '**Use Custom Rule Set.**'.

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



☑ Enable automatic detection of private networks

☐ Do NOT show popup alerts

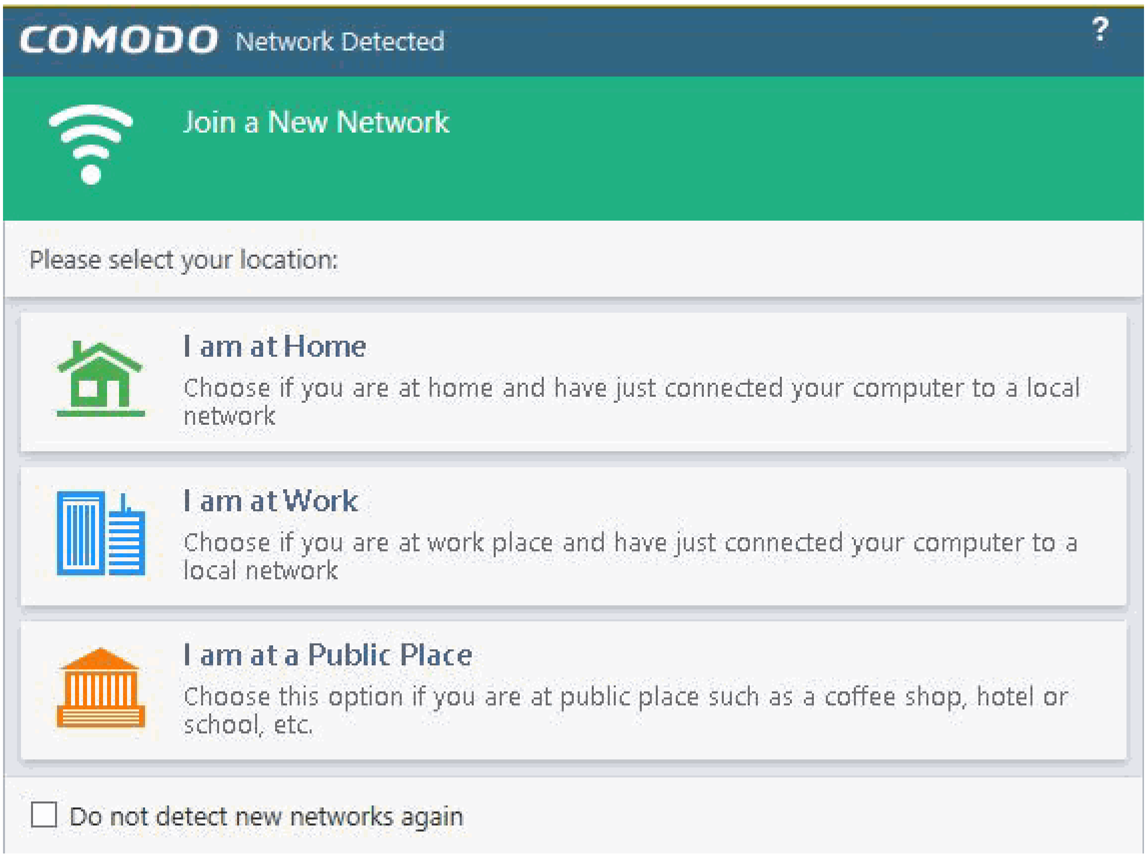
Location treatment: Work

☐	ZONE NAME
☐	Loopback Zone

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.



COMODO Network Detected ?

Join a New Network

Please select your location:

I am at Home
Choose if you are at home and have just connected your computer to a local network

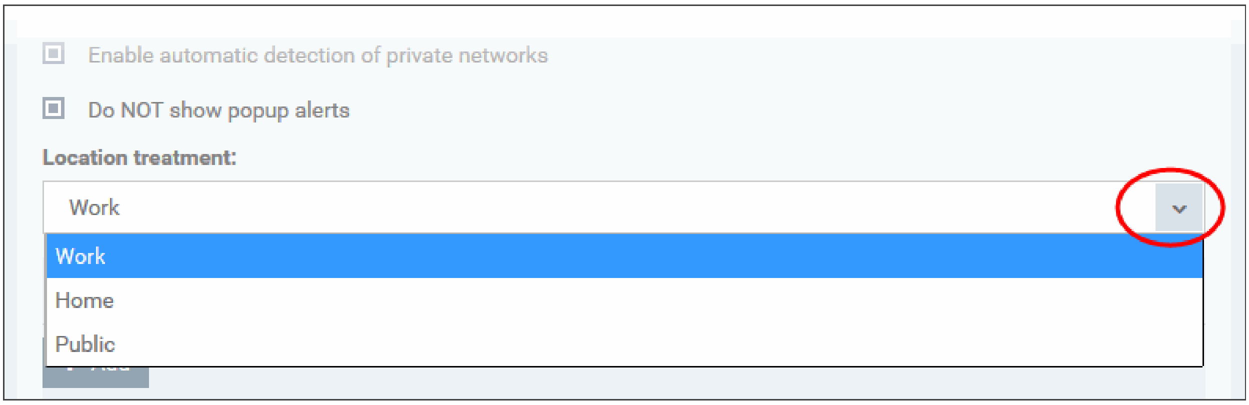
I am at Work
Choose if you are at work place and have just connected your computer to a local network

I am at a Public Place
Choose this option if you are at public place such as a coffee shop, hotel or school, etc.

☐ Do not detect new networks again

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



☐ Enable automatic detection of private networks

☒ Do NOT show popup alerts

Location treatment:

Work

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

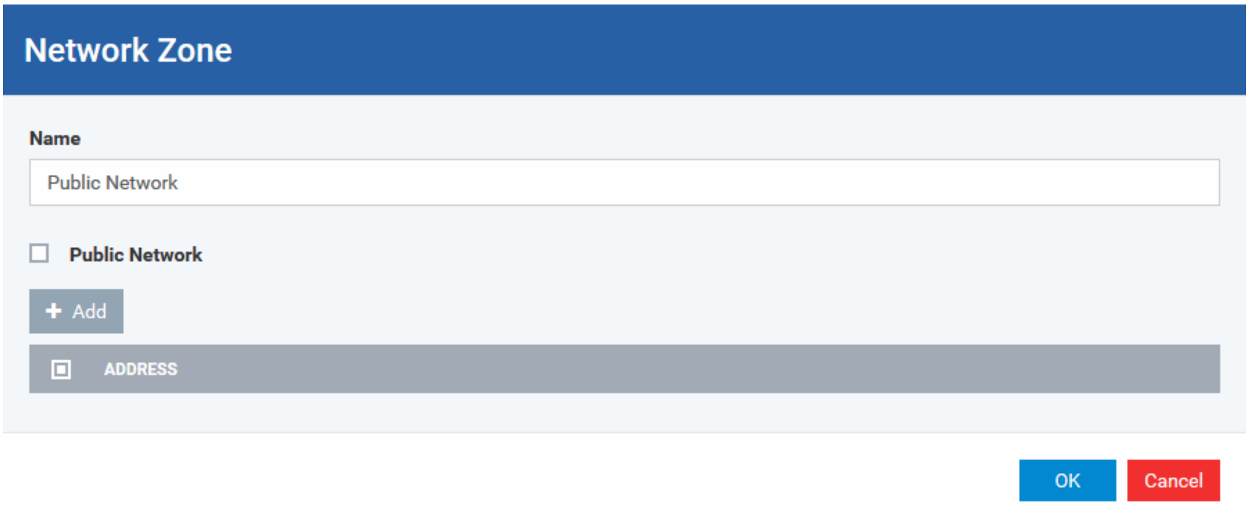
A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied.

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' + Add button at the top of the list.

The 'Network Zone' dialog will open.



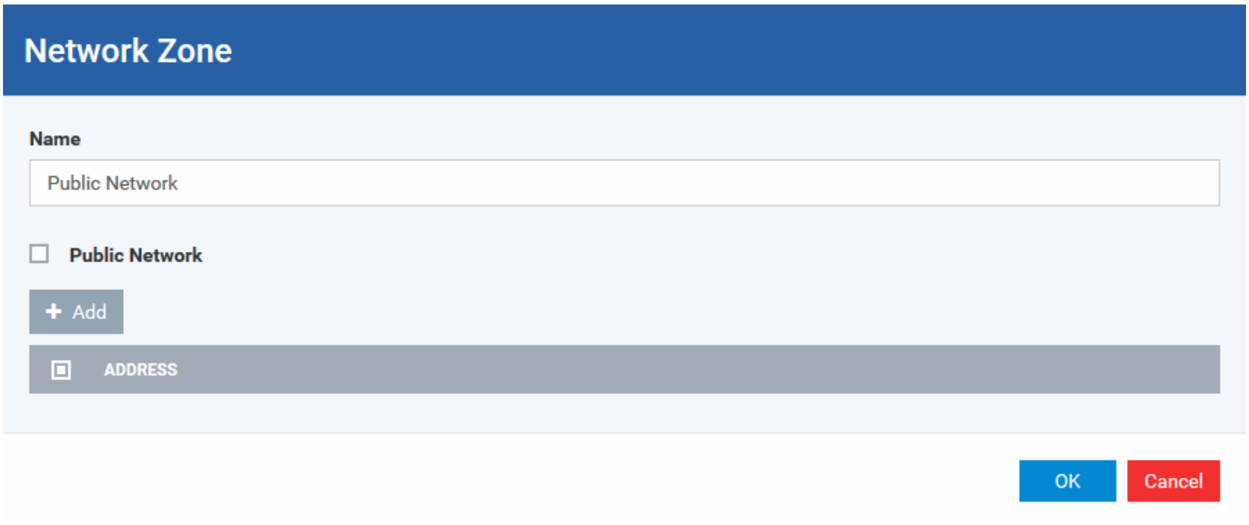
Network Zone

Name

Public Network

□ Public Network

- 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



Network Zone

Name

Public Network

□ Public Network

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.

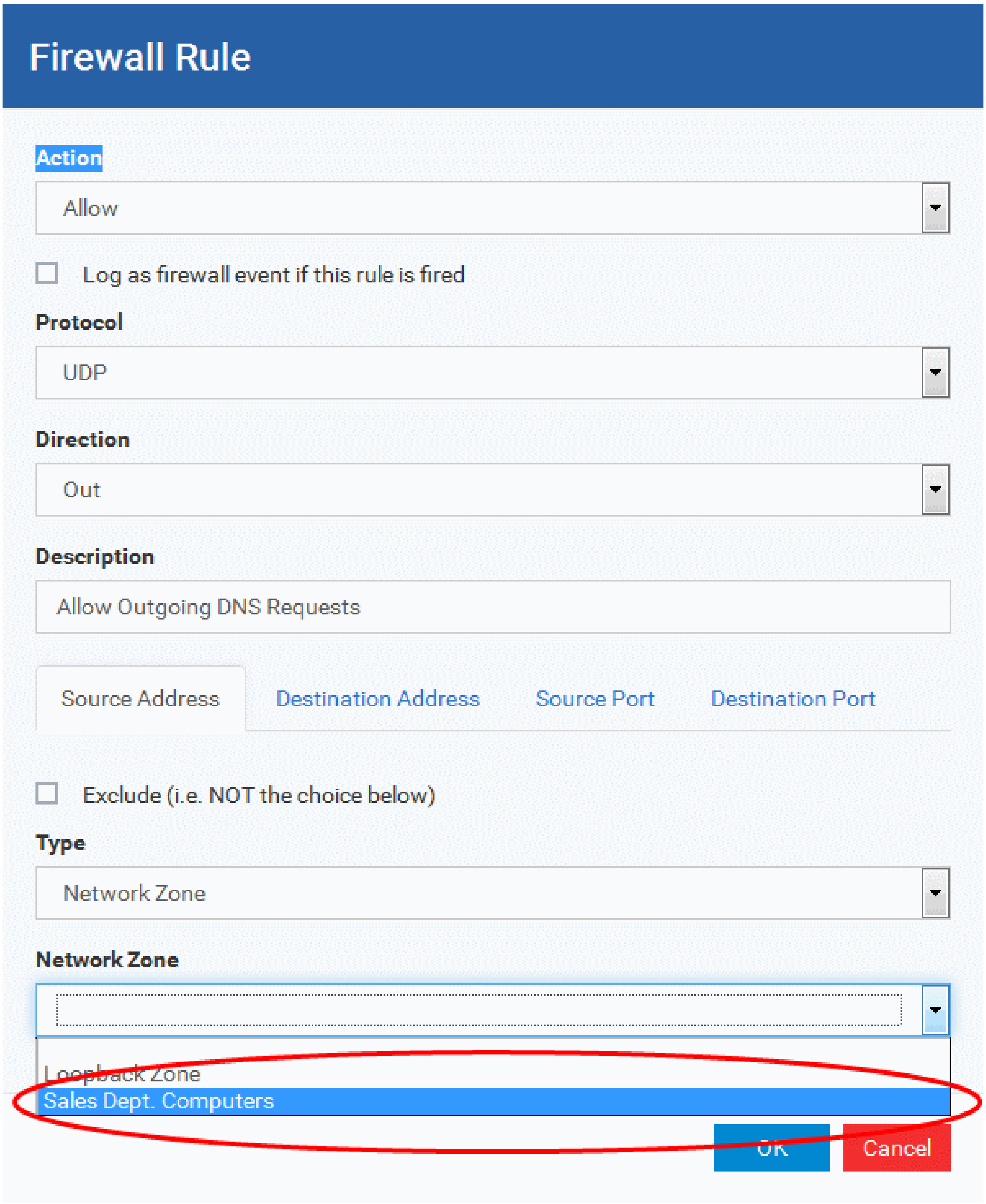
vi. IPv6 Single Address -Enter a single address to be added to the zone - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

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**.



Firewall Rule

Action

Allow

□ Log as firewall event if this rule is fired

Protocol

UDP

Direction

Out

Description

Allow Outgoing DNS Requests

□ Exclude (i.e. NOT the choice below)

Type

Network Zone

Network Zone

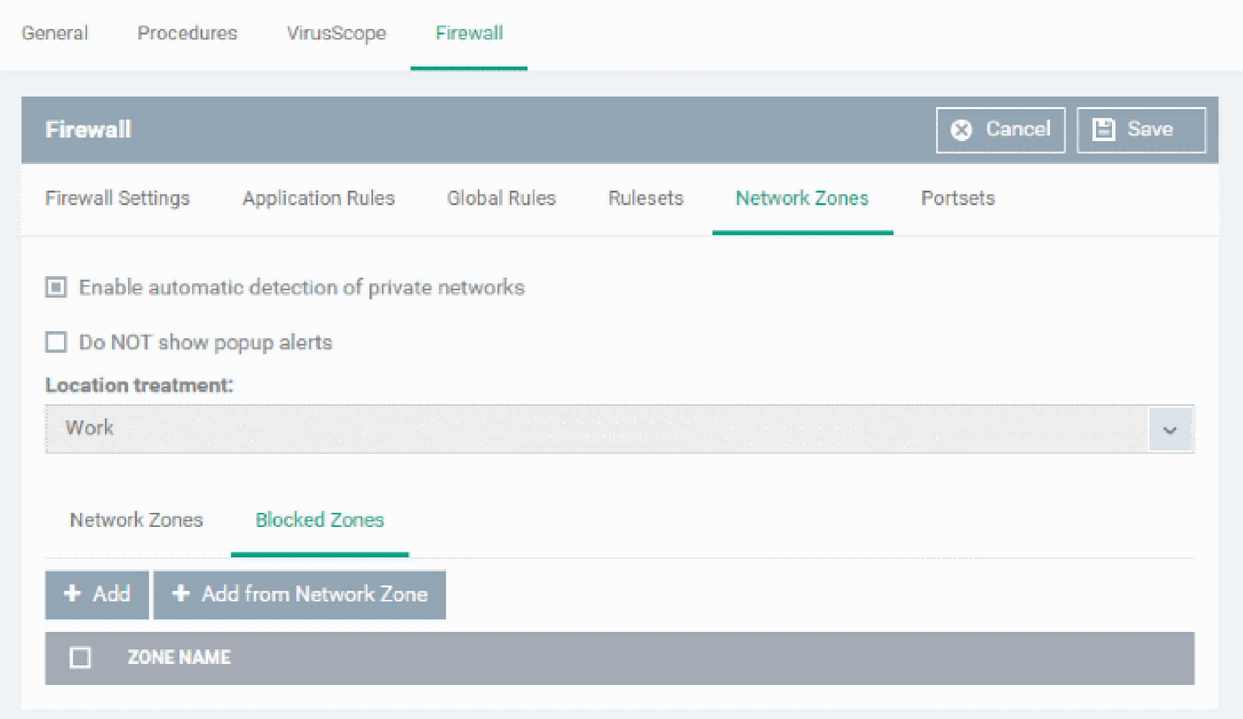
To edit a network zone, click the 'Edit' icon ✎ beside the network zone name. The 'Network Zone' dialog will appear populated with the name and the addresses of the network zone. Edit the details as required. The process is similar to **defining a new network zone** as explained above.

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.



☒ Enable automatic detection of private networks

□ Do NOT show popup alerts

Location treatment: Work

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**

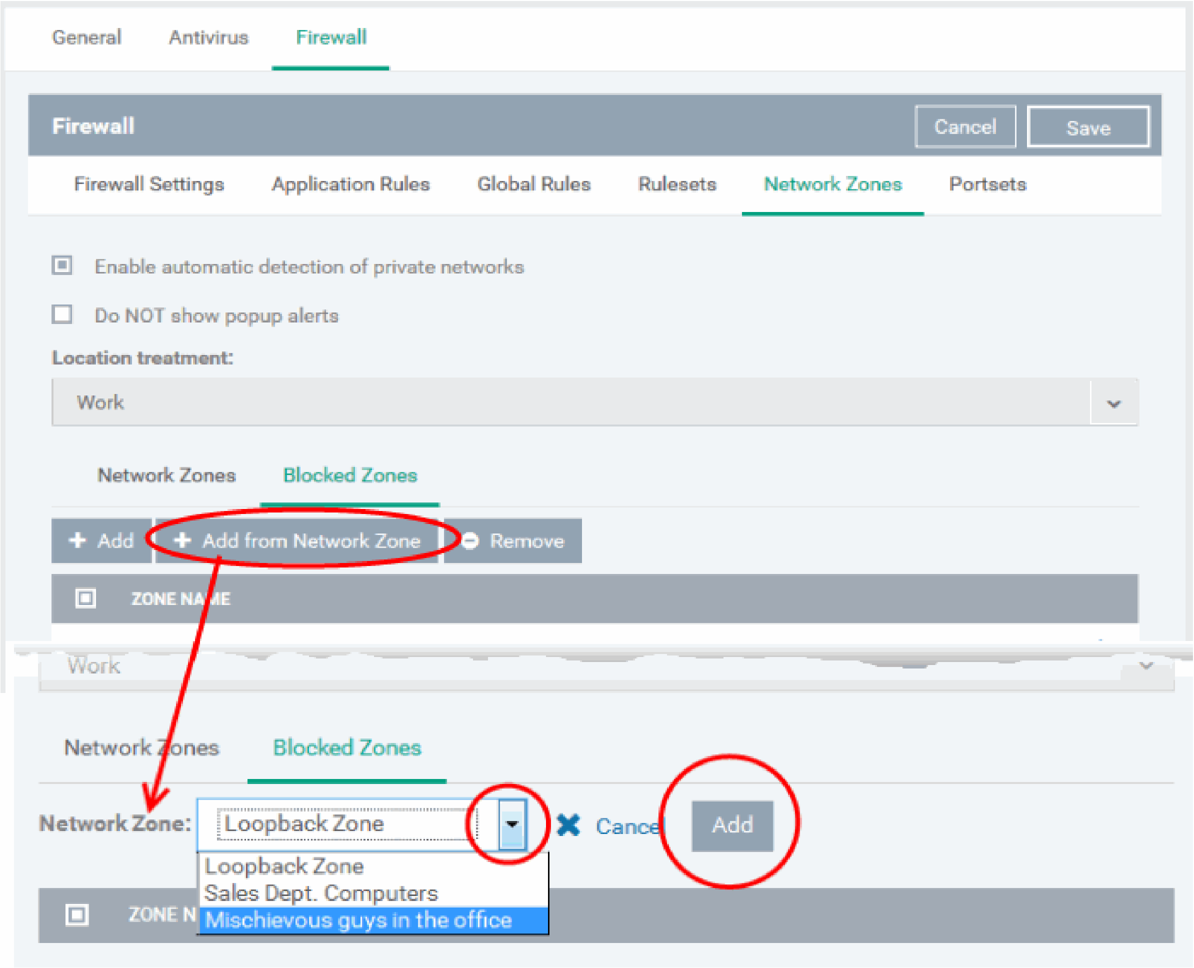
Note 1: You must create a zone before you can block it. There are two ways to do this;

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

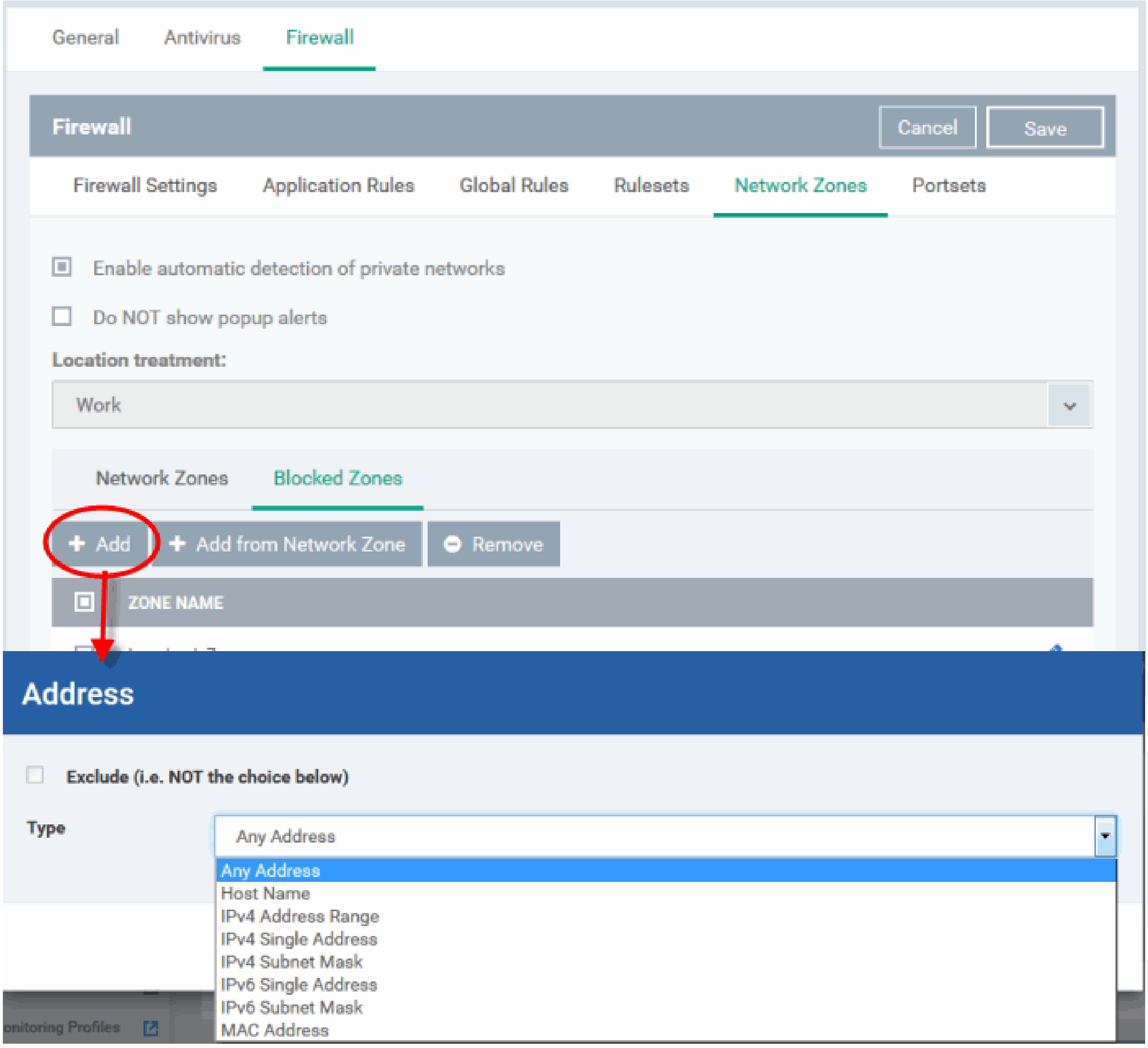
- Click 'Add from Network Zone' button from the top
- Choose the particular zone you wish to block from the 'Network Zone' drop-down.



- 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.

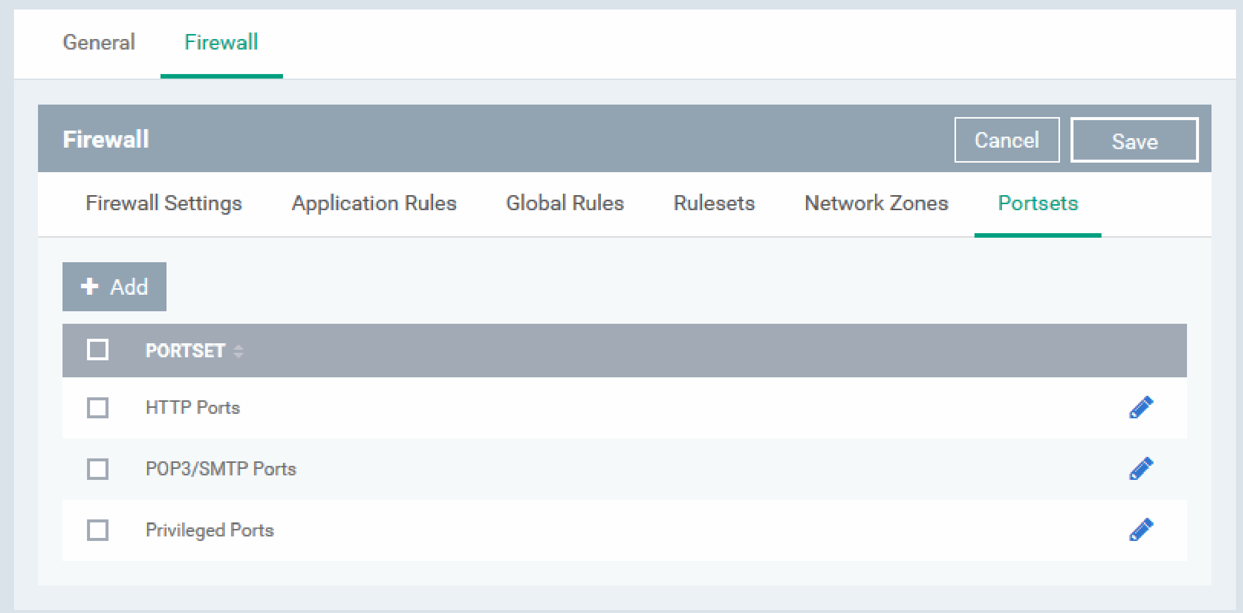
2. Select the address to be blocked and click 'OK'

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.

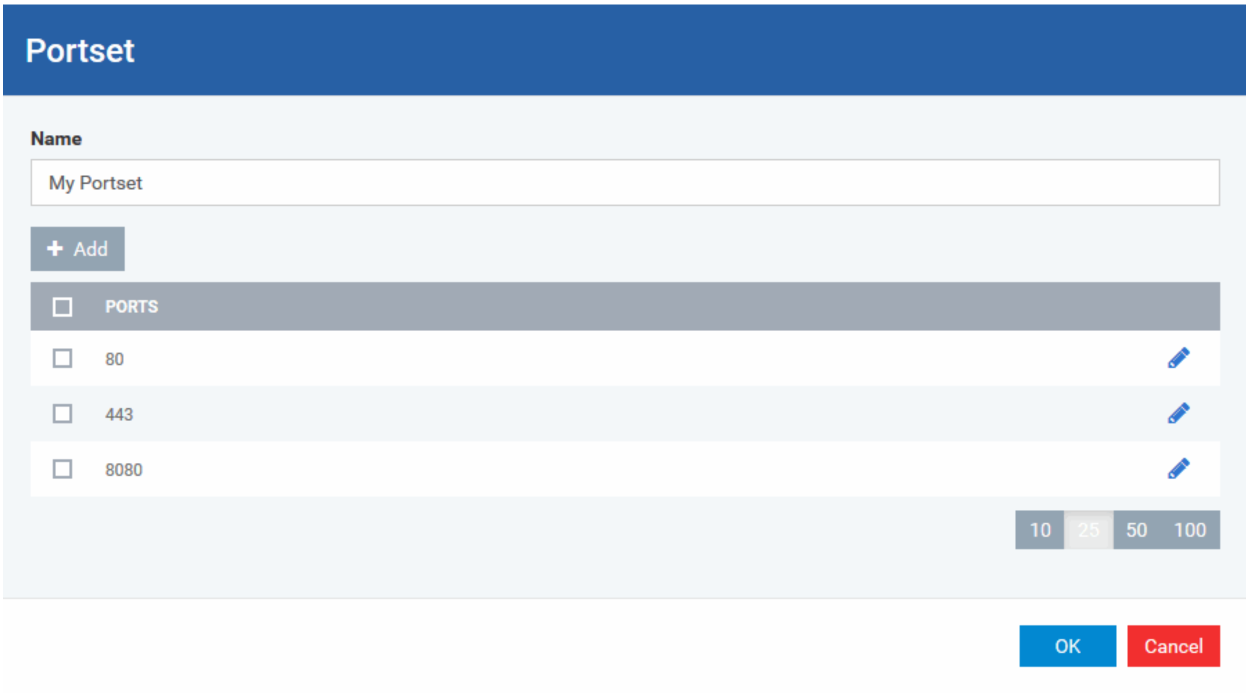
Portsets

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.



□	PORTSET
□	HTTP Ports
□	POP3/SMTP Ports
□	Privileged Ports

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.



Name: My Portset

□	PORTS
□	80
□	443
□	8080

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.

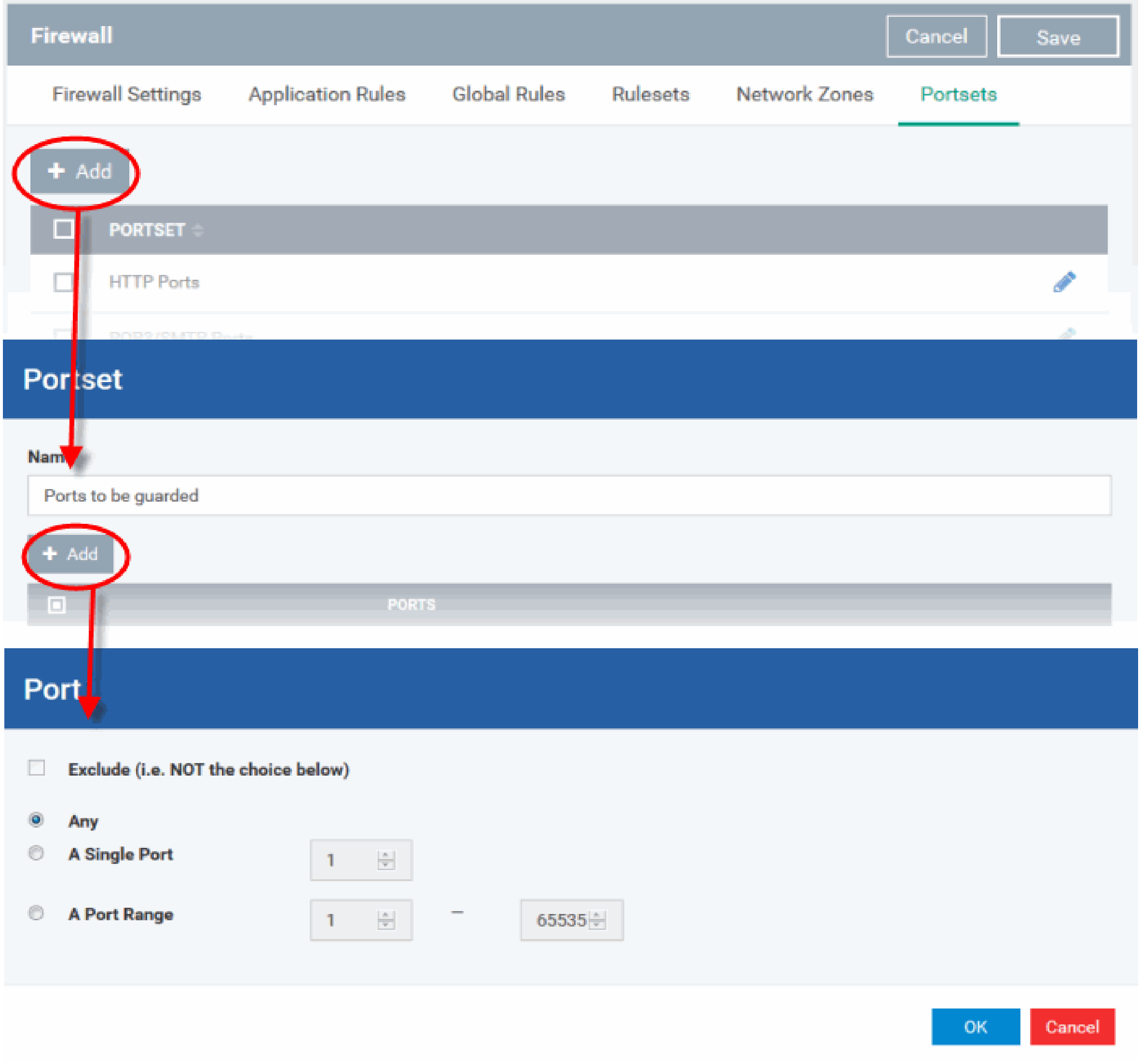
Defining a new Port Set

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.



Name: Ports to be guarded

☐ Exclude (i.e. NOT the choice below)

● Any

○ A Single Port 1

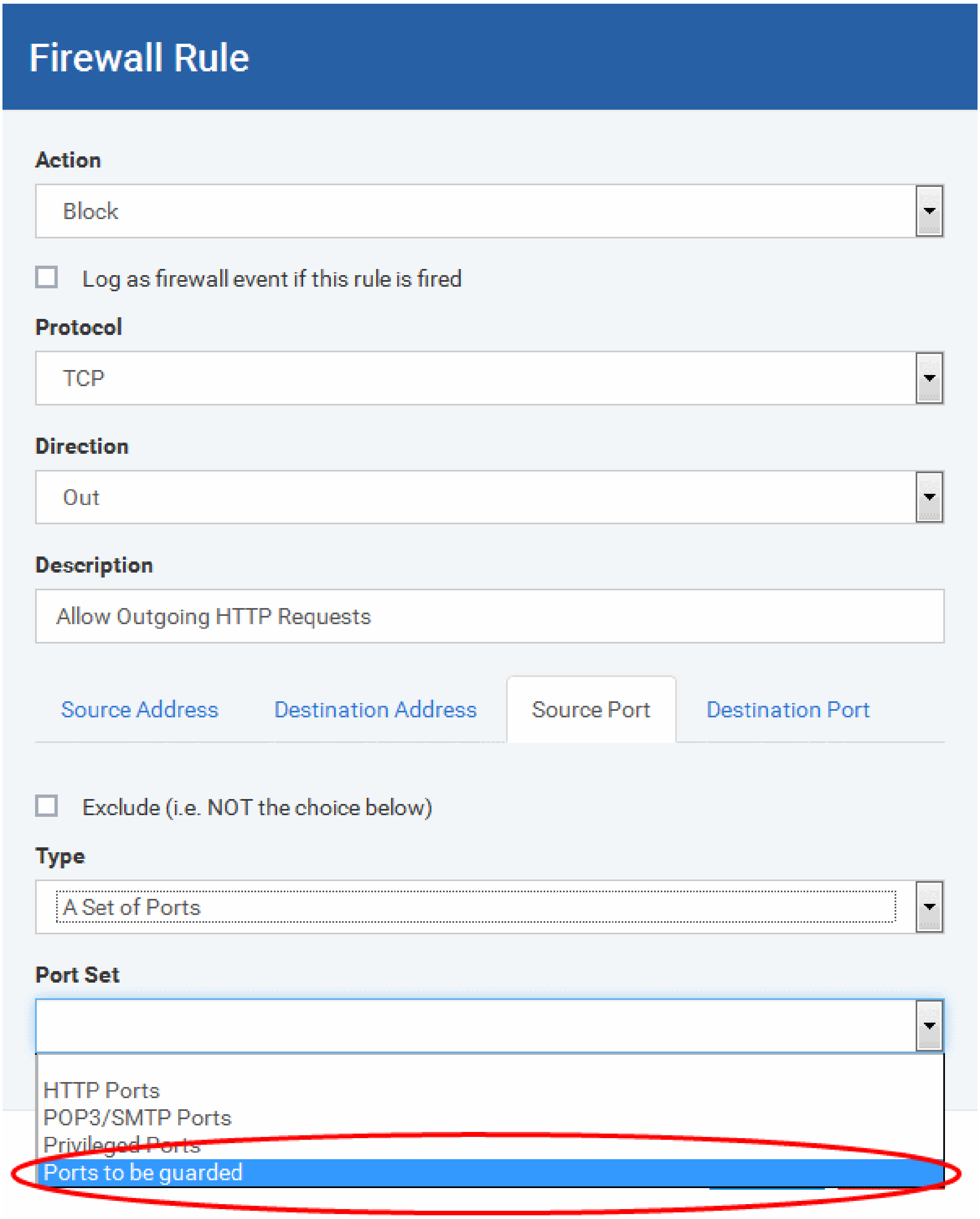
○ A Port Range 1 – 65535

- 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**



Firewall Rule

Action: Block

□ Log as firewall event if this rule is fired

Protocol: TCP

Direction: Out

Description: Allow Outgoing HTTP Requests

□ Exclude (i.e. NOT the choice below)

Type: A Set of Ports

Port Set:

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

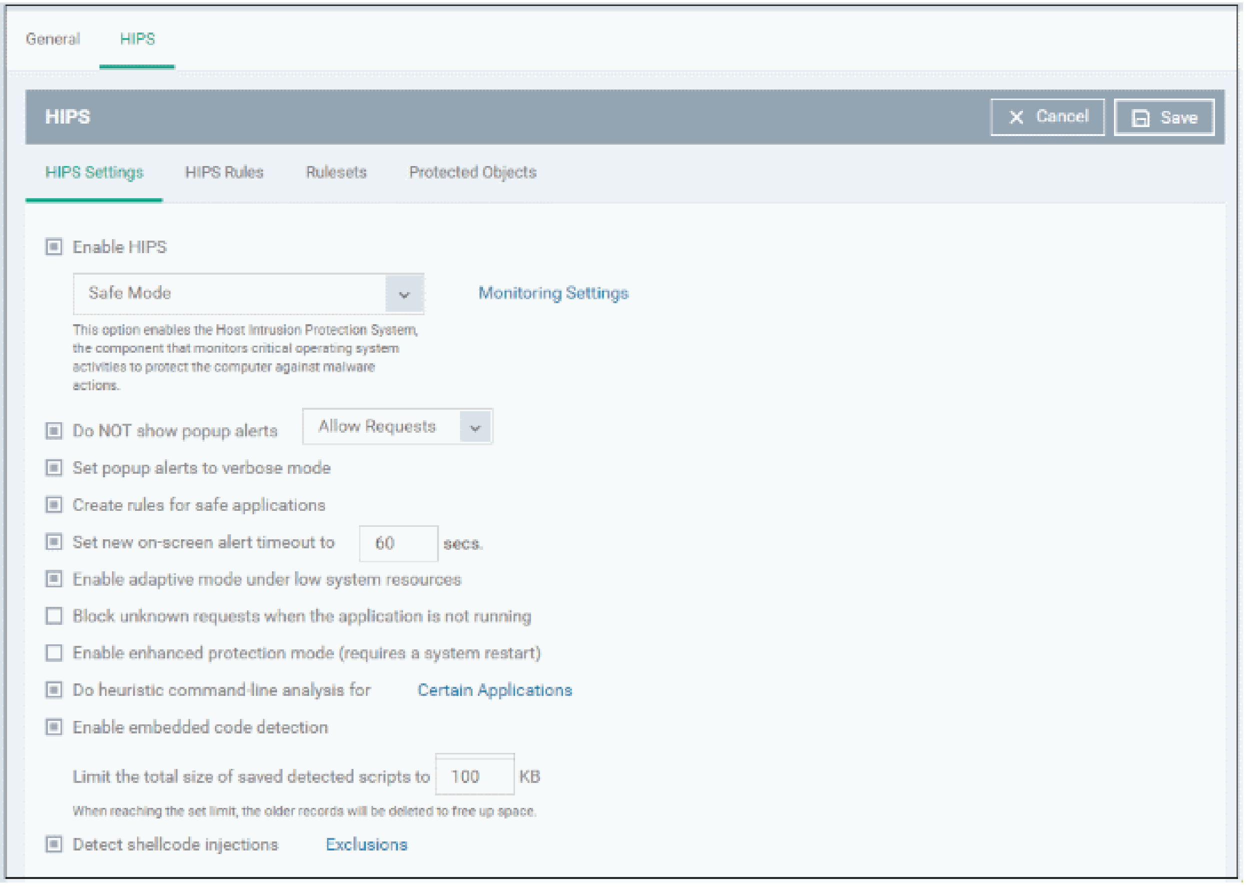
- Click 'HIPS' from the 'Add Profile Section' drop-down

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.



☑ Enable HIPS

Safe Mode

Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do NOT show popup alerts — Allow Requests

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs.

☑ Enable adaptive mode under low system resources

☐ Block unknown requests when the application is not running

☐ Enable enhanced protection mode (requires a system restart)

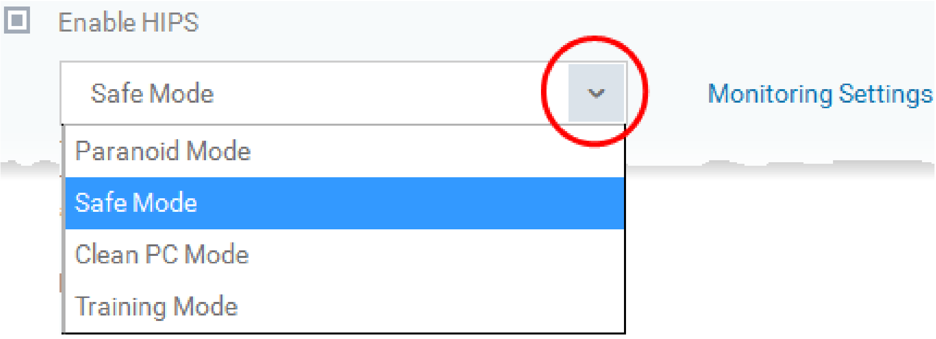
☑ Do heuristic command-line analysis for Certain Applications

☑ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

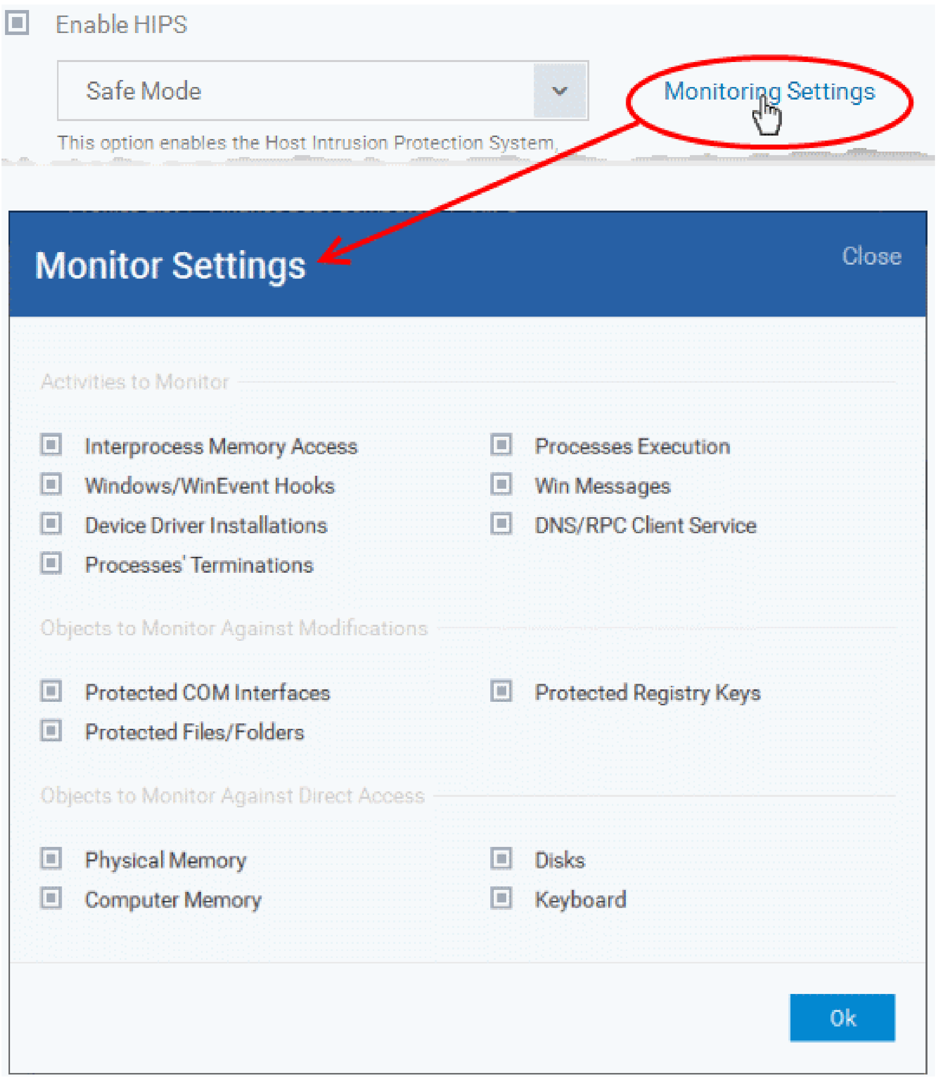
When reaching the set limit, the older records will be deleted to free up space.

☑ Detect shellcode injections Exclusions

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'.  ☑ Enable HIPS Safe Mode Monitoring Settings Paranoid Mode Safe Mode Clean PC Mode Training Mode 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



☑ Enable HIPS

Safe Mode

Monitoring Settings

This option enables the Host Intrusion Protection System.

Monitor Settings

Close

Activities to Monitor

☑ Interprocess Memory Access

☑ Windows/WinEvent Hooks

☑ Device Driver Installations

☑ Processes' Terminations

☑ Processes Execution

☑ Win Messages

☑ DNS/RPC Client Service

Objects to Monitor Against Modifications

☑ Protected COM Interfaces

☑ Protected Files/Folders

☑ Protected Registry Keys

Objects to Monitor Against Direct Access

☑ Physical Memory

☑ Computer Memory

☑ Disks

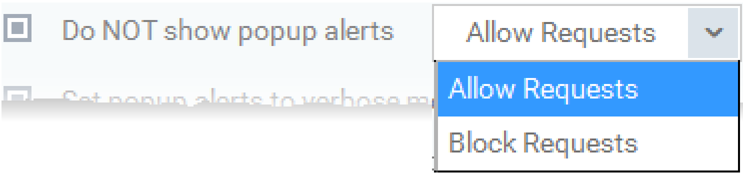
☑ Keyboard

Ok

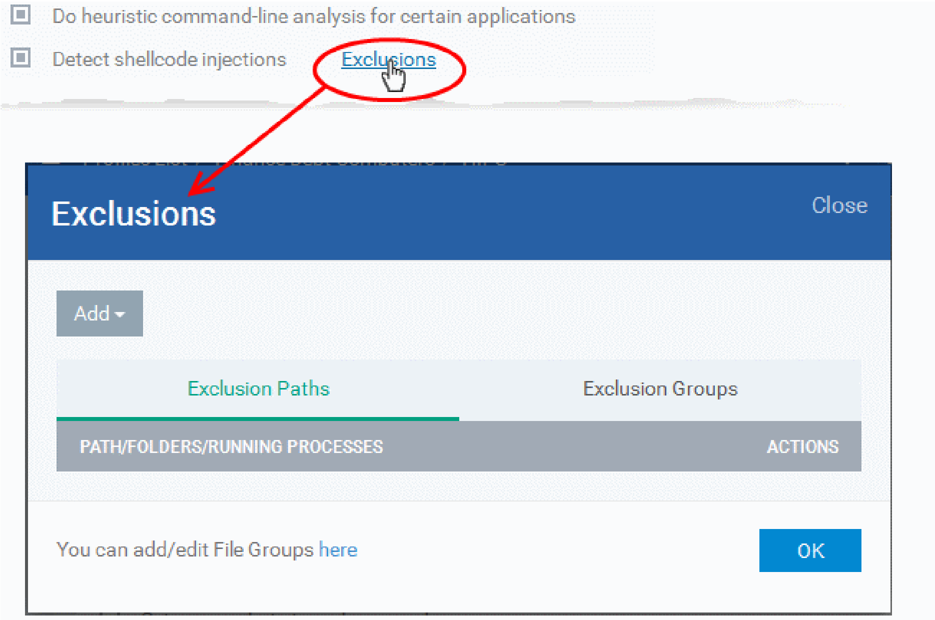
Activities To Monitor:

- **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 an

HIPS Settings - Table of Parameters	
	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 these settings enabled:

HIPS Settings - Table of Parameters	
	- **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'.  ☑ Do NOT show popup alerts — Allow Requests Allow Requests Block Requests Set popup alerts to verbose m
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

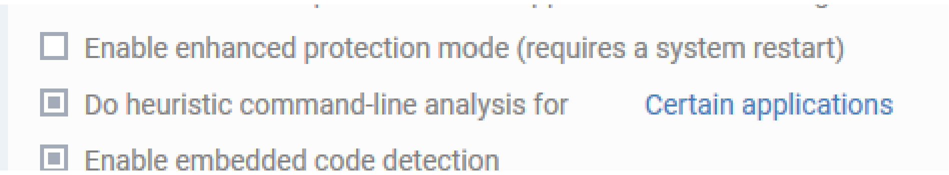
HIPS Settings - Table of Parameters	
	- The application is included in the extensive and constantly updated Comodo safelist.
Set new on-screen alert timeout to	Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 60 seconds. You may adjust this 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, java applications, python scripts and AutoIt scripts. 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'. You can view and select which applications are analyzed by clicking the 'Certain applications' link. See the explanation under **Selecting Applications for Heuristic Command Line Analysis** for more details. **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

HIPS Settings - Table of Parameters	
	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-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.  ☑ Do heuristic command-line analysis for certain applications ☑ Detect shellcode injections Exclusions Exclusions Close Add Exclusion Paths Exclusion Groups PATH/FOLDERS/RUNNING PROCESSES ACTIONS You can add/edit File Groups here OK 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**.

Selecting Applications for Heuristic Command Line Analysis

- Click 'Configuration Templates' > 'Profiles' > select a profile > Open the 'HIPS settings' tab.
- If it is not available, click 'Add Section' and add 'HIPS settings'.

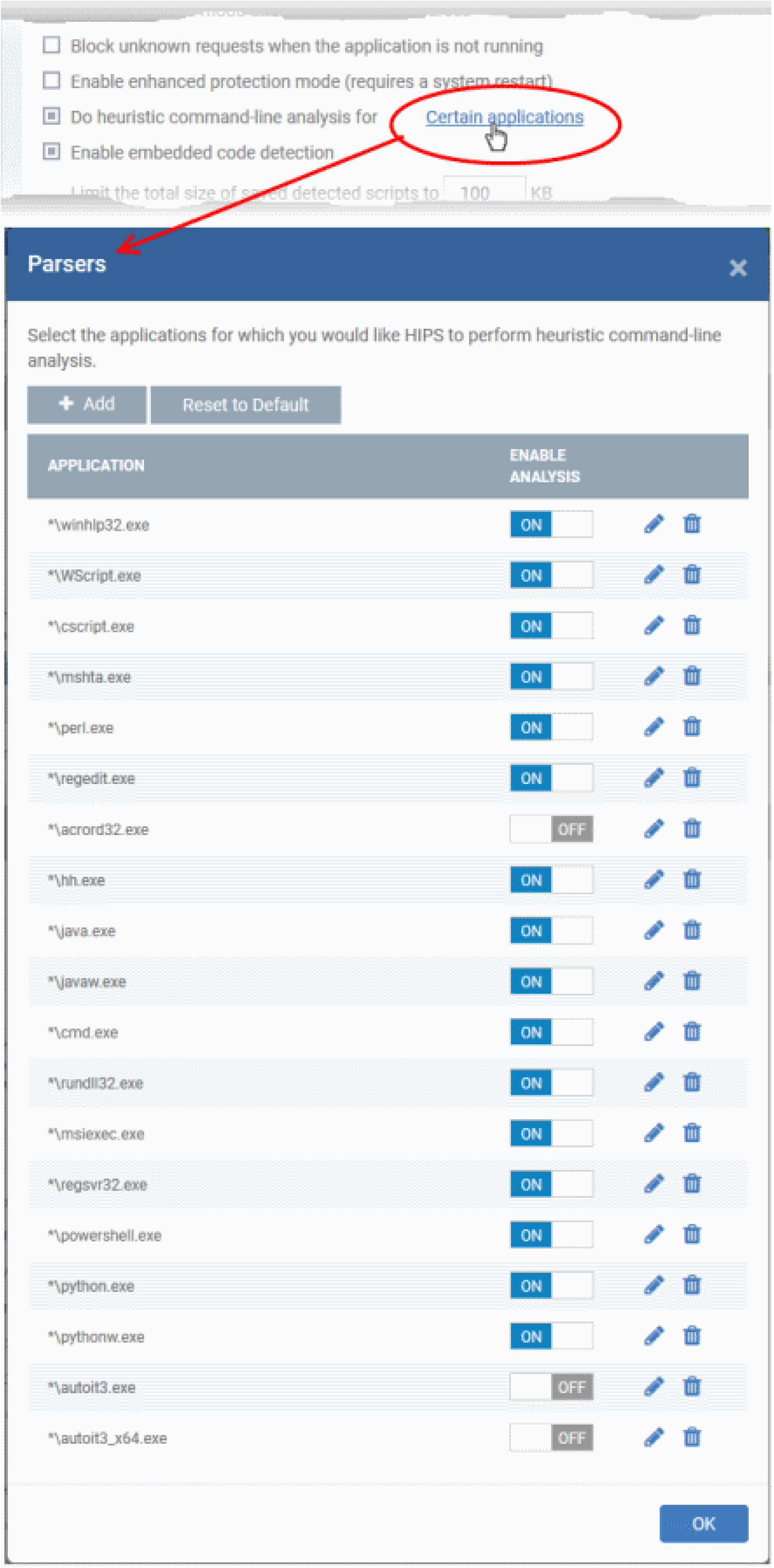
You can view and select which applications undergo Heuristics Command Line analysis by clicking 'Certain Applications' next to 'Do heuristic command-line analysis for ':



☐ Enable enhanced protection mode (requires a system restart)

☑ Do heuristic command-line analysis for Certain applications

☑ Enable embedded code detection



☐ Block unknown requests when the application is not running

☐ Enable enhanced protection mode (requires a system restart)

☒ Do heuristic command-line analysis for Certain applications

☒ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

Parsers

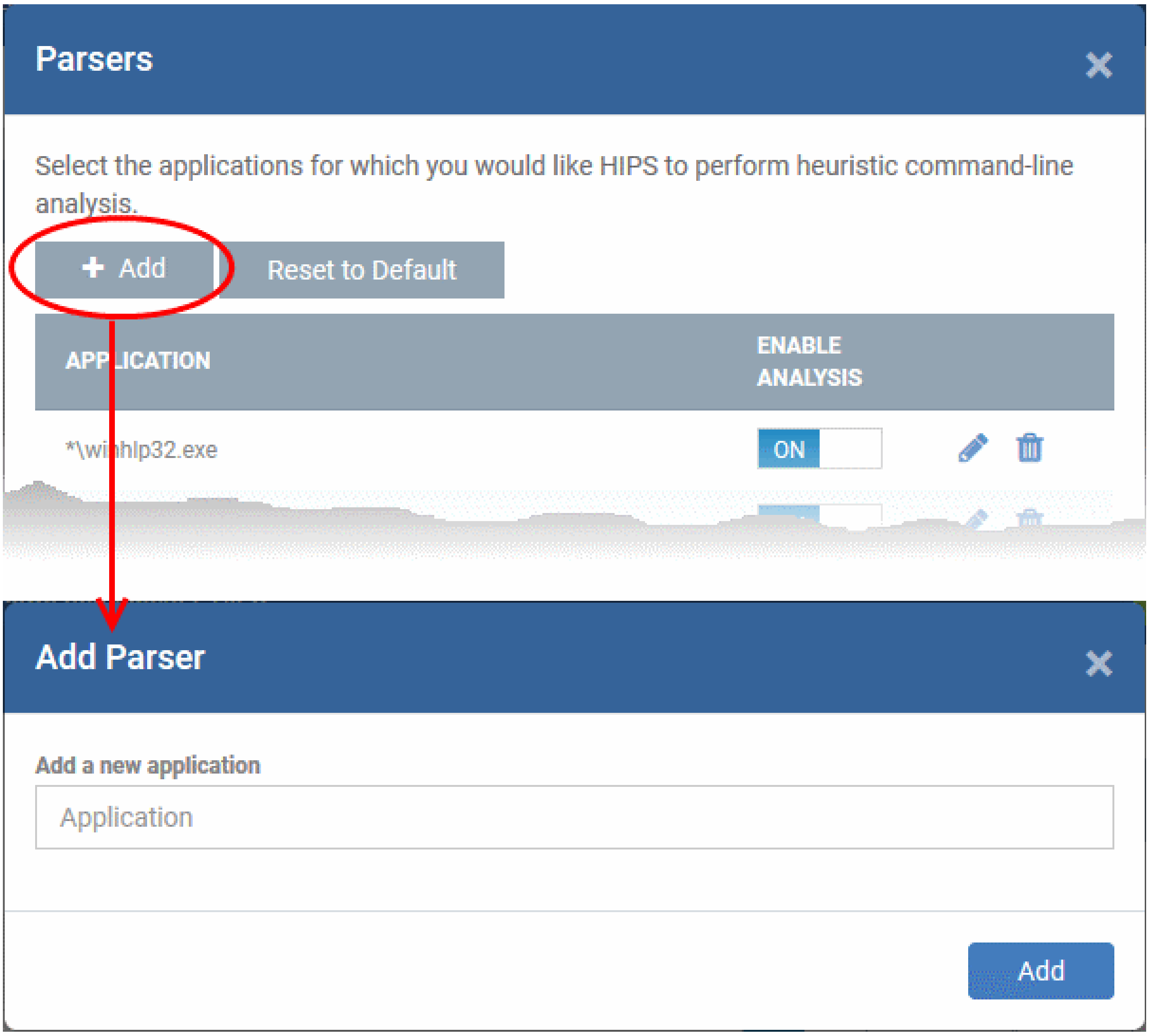
Select the applications for which you would like HIPS to perform heuristic command-line analysis.

APPLICATION	ENABLE ANALYSIS
*\winhlp32.exe	ON
*\WScript.exe	ON
*\cscript.exe	ON
*\mshta.exe	ON
*\perl.exe	ON
*\regedit.exe	ON
*\acrord32.exe	OFF
*\hh.exe	ON
*\java.exe	ON
*\javaw.exe	ON
*\cmd.exe	ON
*\rundll32.exe	ON
*\msiexec.exe	ON
*\regsvr32.exe	ON
*\powershell.exe	ON
*\python.exe	ON
*\pythonw.exe	ON
*\autoit3.exe	OFF
*\autoit3_x64.exe	OFF

The 'Parser' dialog displays the list of applications to choose from and also allows you to add custom applications.

- Use the toggle switch 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.
- Click 'Add' at the top to add a new application to the list.



Parsers

Select the applications for which you would like HIPS to perform heuristic command-line analysis.

APPLICATION	ENABLE ANALYSIS
*\winhlp32.exe	ON

Add Parser

Add a new application

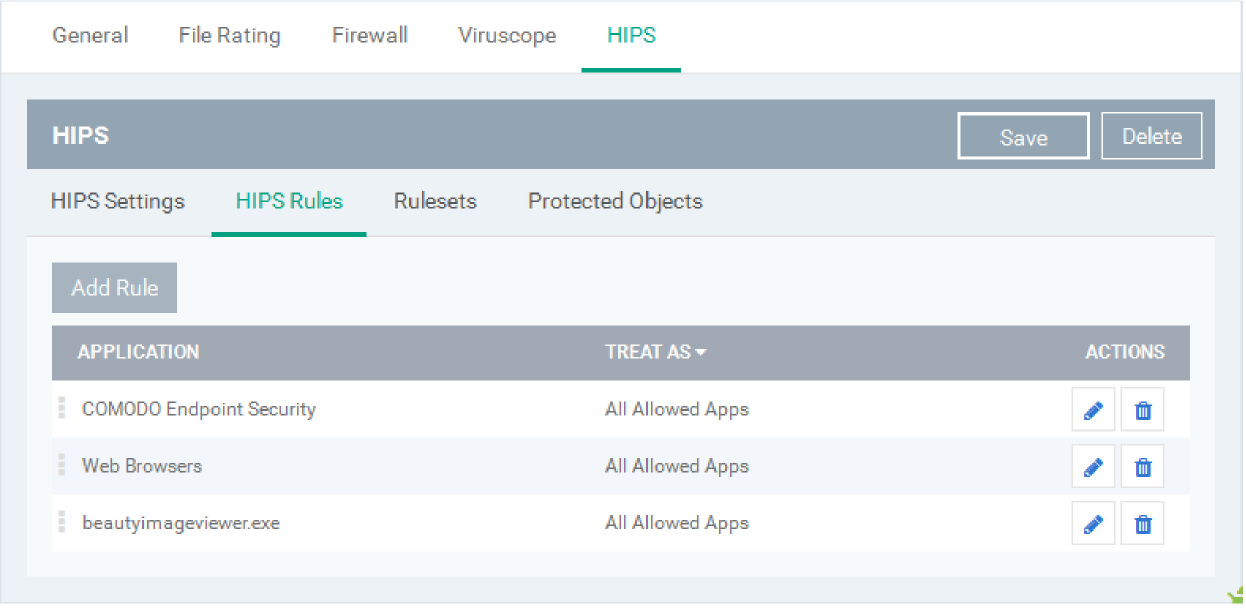
- Enter the name of the application in the 'Add Parser' dialog and click 'Add'.
- The new application will be added to the list and will be selected by default. You can use the toggle switch beside it to enable/disable it at any time.

- To reset the list to the default list of applications, click 'Reset to Default' at the top
- Click 'OK' to apply your changes.

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.



APPLICATION	TREAT AS	ACTIONS
COMODO Endpoint Security	All Allowed Apps	✎ 🗑
Web Browsers	All Allowed Apps	✎ 🗑
beautyimageviewer.exe	All Allowed Apps	✎ 🗑

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

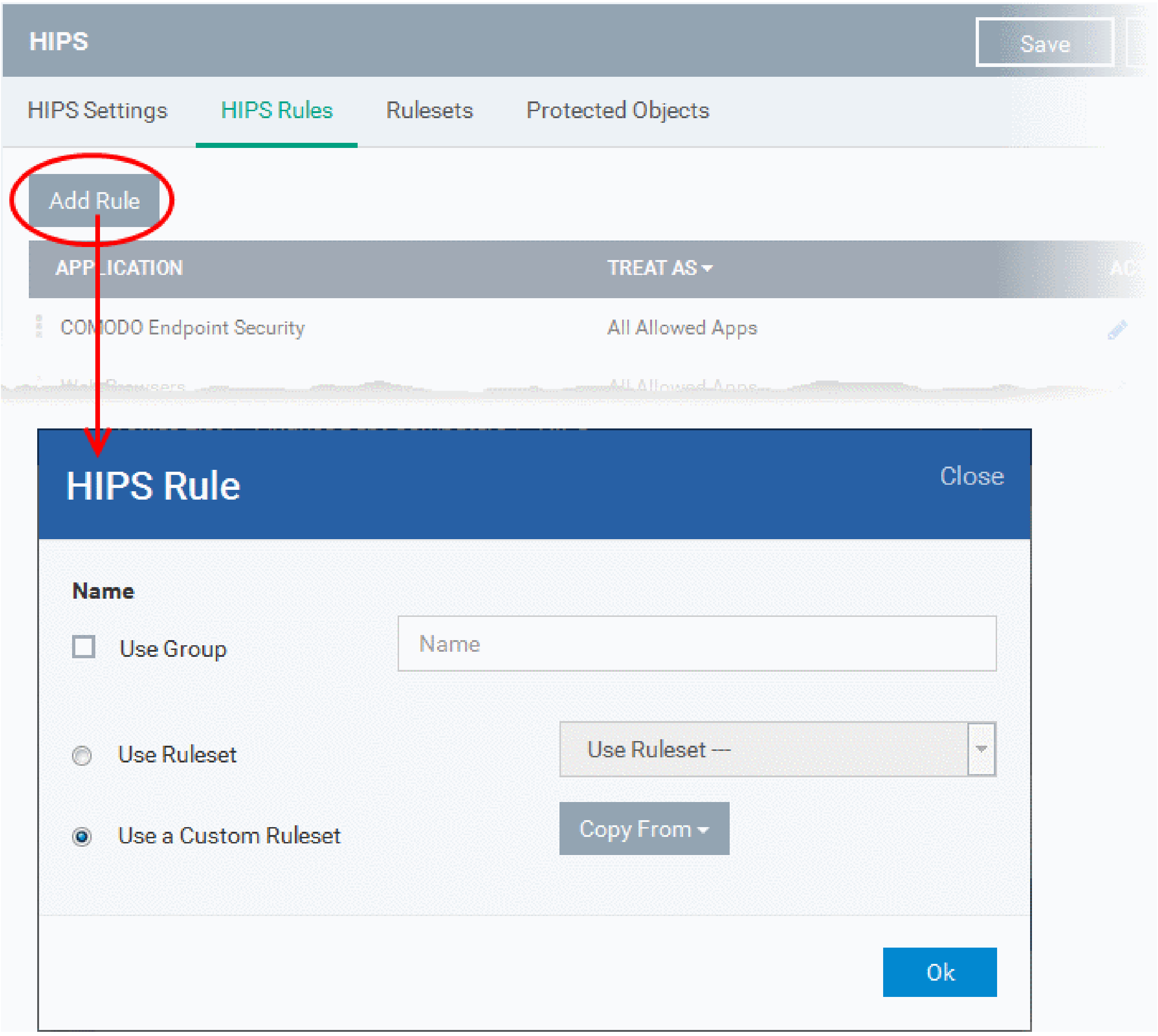
To begin defining an application's HIPS rule, you need take two basic steps.

- 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

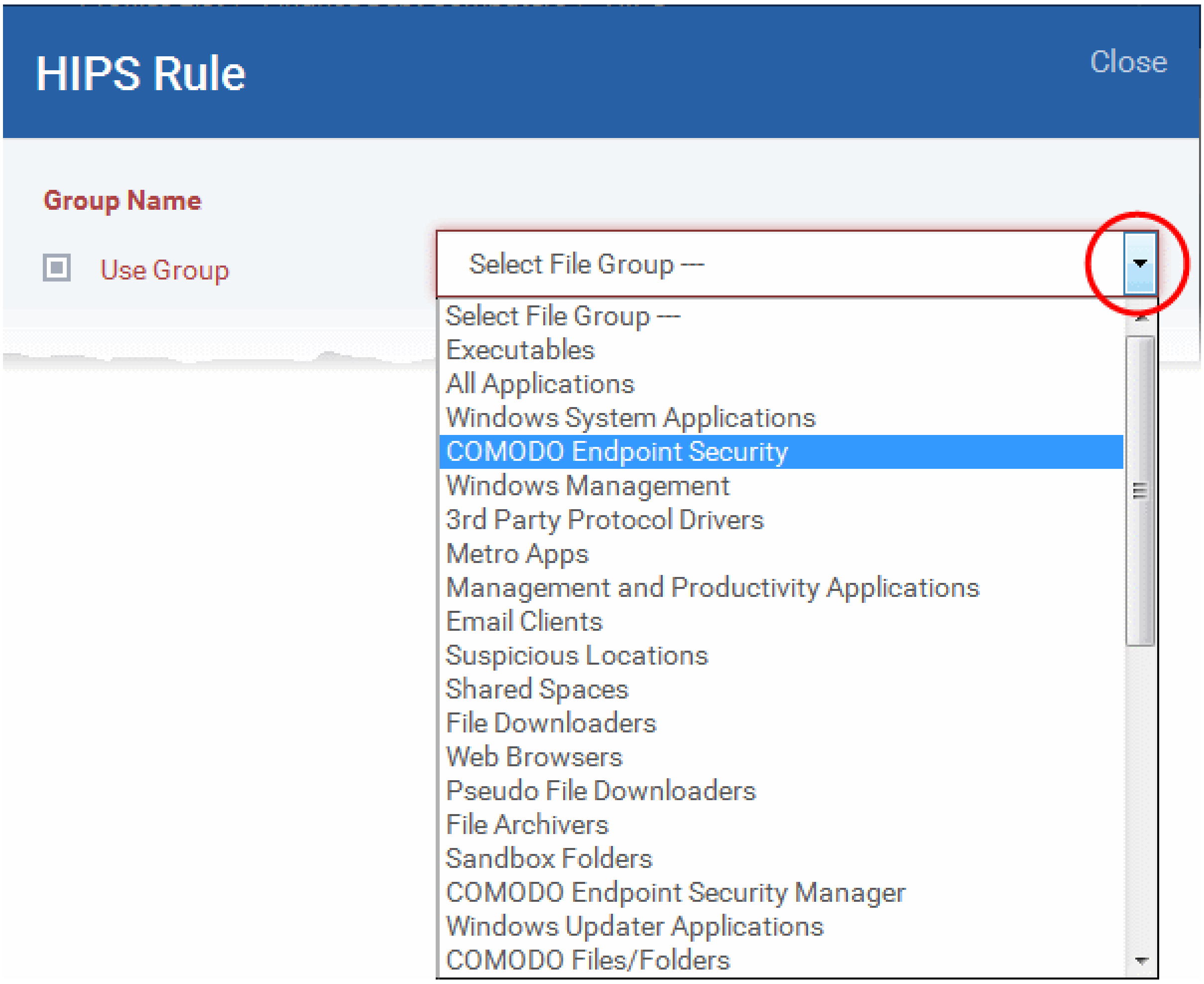
- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add Rule' button at the top of the list in the 'HIPS Rules' interface.

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

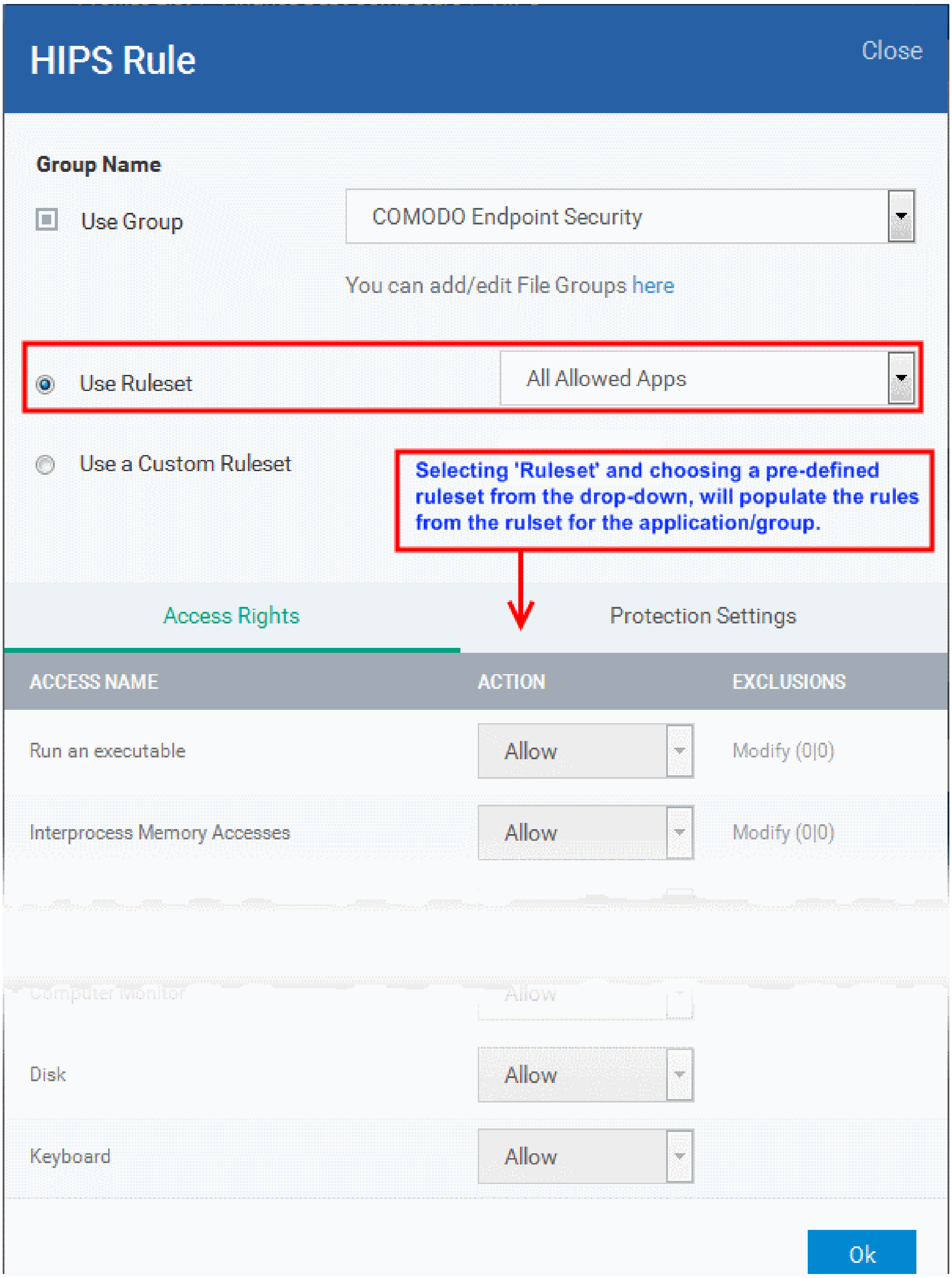


Note: ITSM ships with a set of predefined file groups containing collections of files under respective categories. Administrators can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can 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.



HIPS Rule

Group Name

□ Use Group: COMODO Endpoint Security

You can add/edit File Groups here

● Use Ruleset: All Allowed Apps

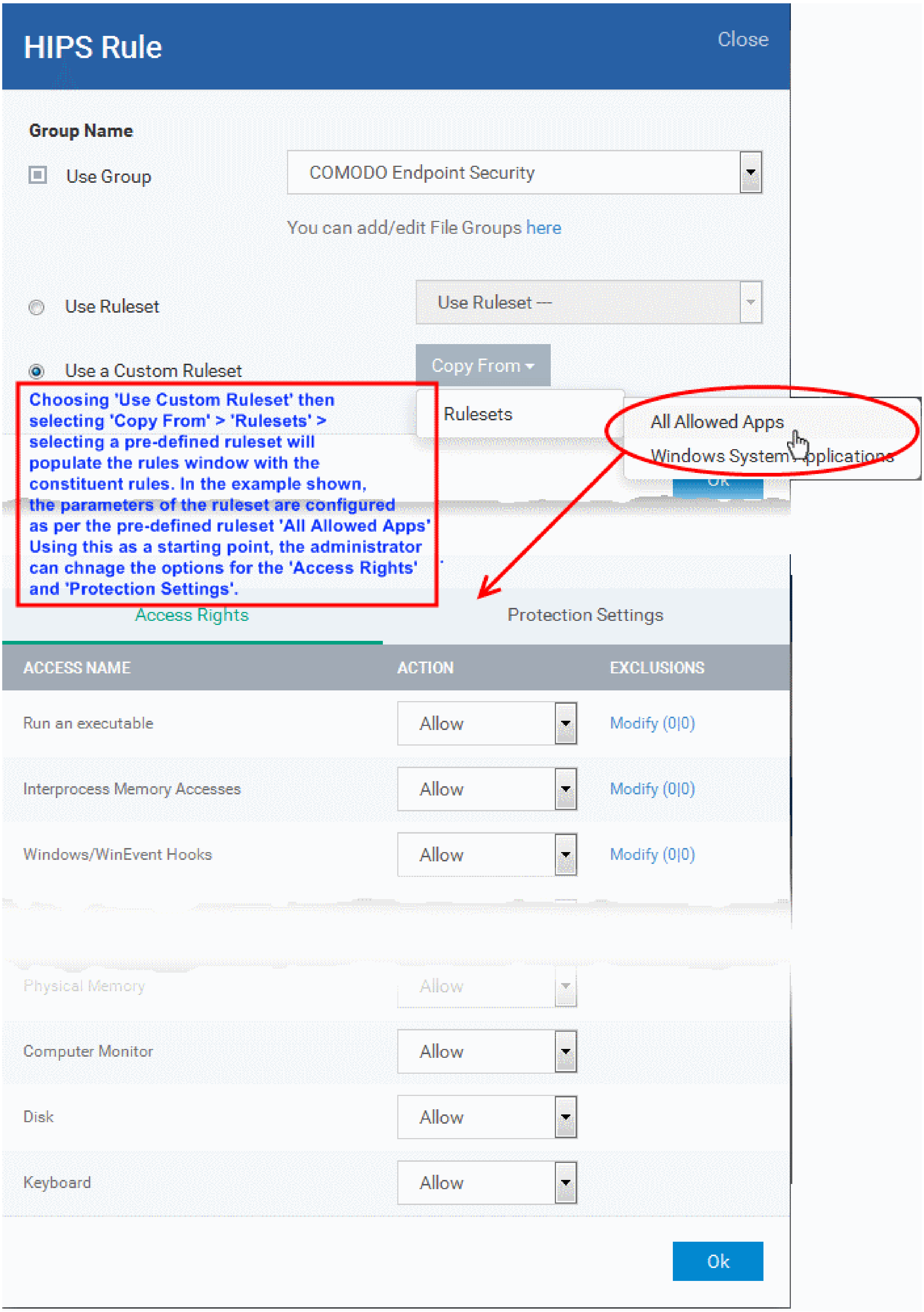
○ Use a Custom Ruleset

Selecting 'Ruleset' and choosing a pre-defined ruleset from the drop-down, will populate the rules from the rulset for the application/group.

ACCESS NAME	ACTION	EXCLUSIONS
Run an executable	Allow	Modify (0|0)
Interprocess Memory Accesses	Allow	Modify (0|0)
Computer Monitor	Allow	
Disk	Allow	
Keyboard	Allow	

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)***



HIPS Rule

Close

Group Name

□ Use Group — COMODO Endpoint Security

You can add/edit File Groups here

○ Use Ruleset — Use Ruleset ---

● Use a Custom Ruleset — Copy From ▾

Rulesets

All Allowed Apps

Windows System Applications

Choosing 'Use Custom Ruleset' then selecting 'Copy From' > 'Rulesets' > selecting a pre-defined ruleset will populate the rules window with the constituent rules. In the example shown, the parameters of the ruleset are configured as per the pre-defined ruleset 'All Allowed Apps' Using this as a starting point, the administrator can chnage the options for the 'Access Rights' and 'Protection Settings'.

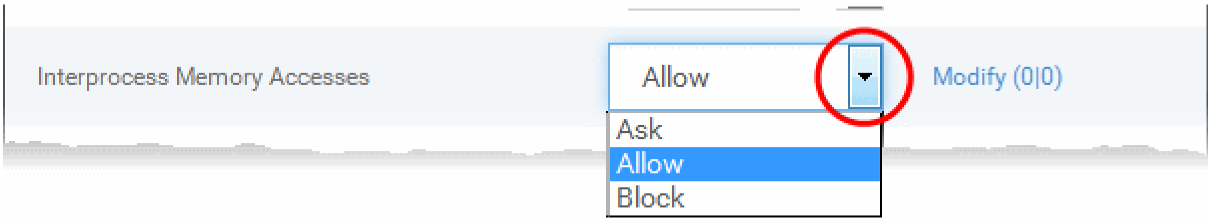
Access Rights | Protection Settings

ACCESS NAME	ACTION	EXCLUSIONS
Run an executable	Allow	Modify (0|0)
Interprocess Memory Accesses	Allow	Modify (0|0)
Windows/WinEvent Hooks	Allow	Modify (0|0)
Physical Memory	Allow	
Computer Monitor	Allow	
Disk	Allow	
Keyboard	Allow	

Ok

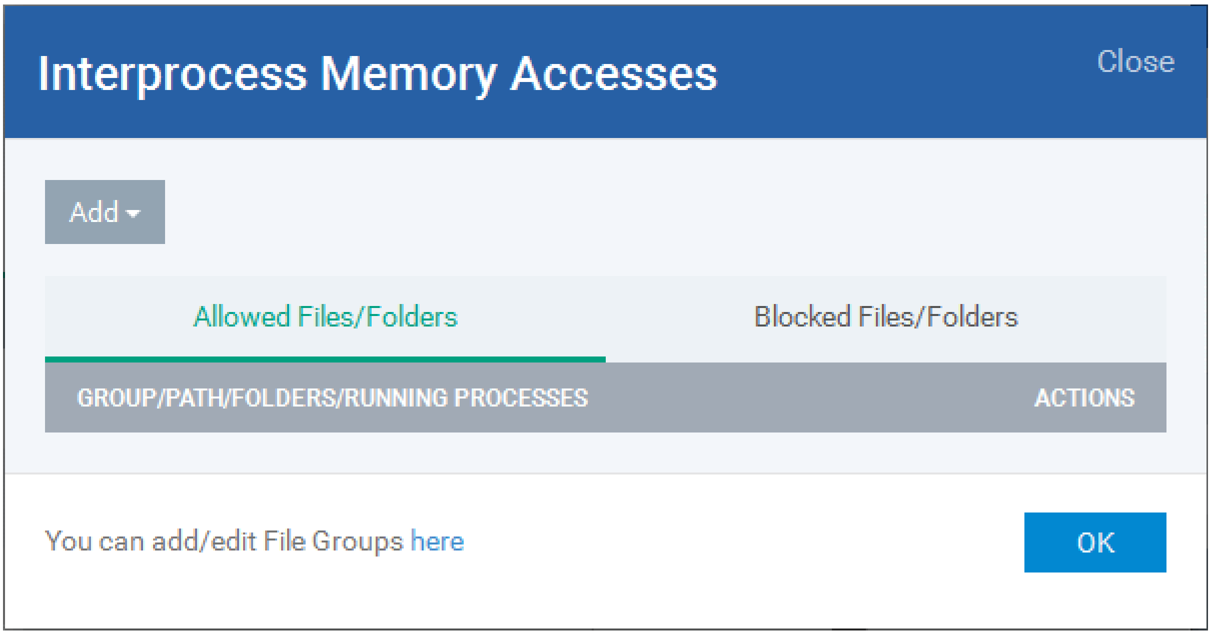
In simplistic terms 'Access Rights' determine what the application *can do to other processes and objects* whereas 'Protection Settings' determine what the application *can have done to it by other processes*.

i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset.



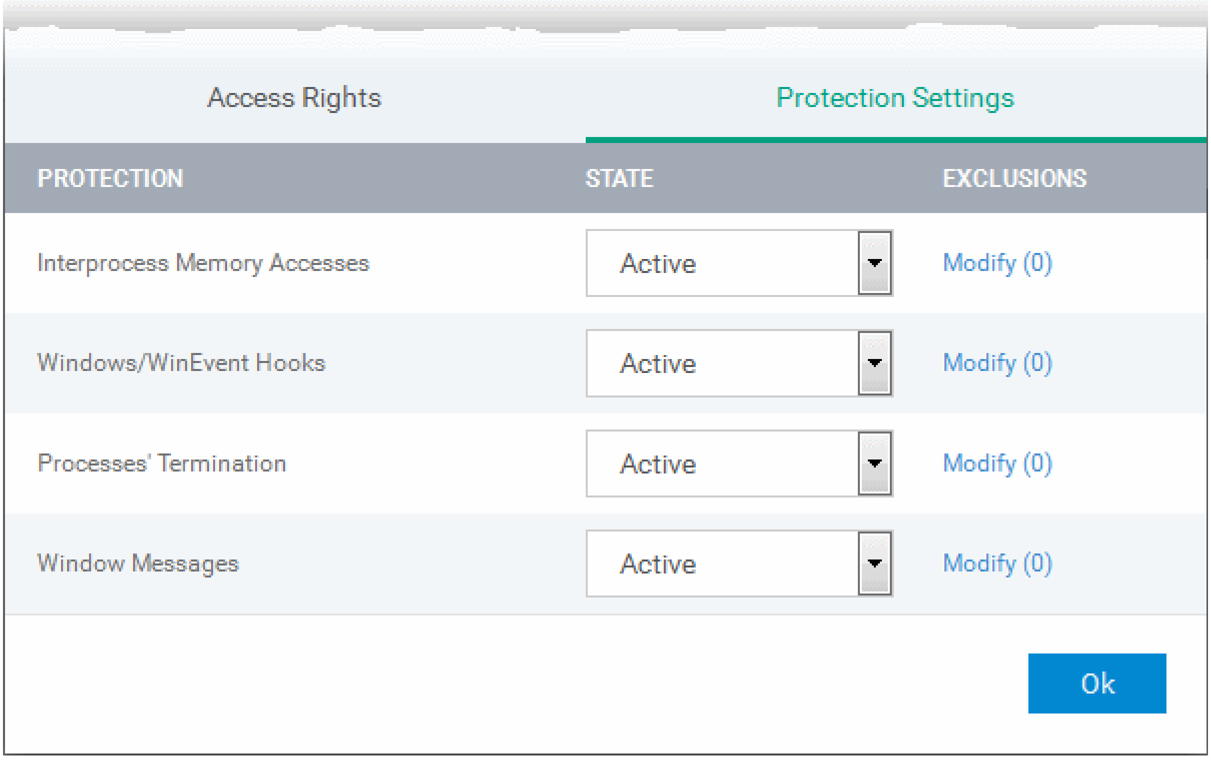
Refer to the section **HIPS Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:

- 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.


Interprocess Memory Accesses
Close
Add
Allowed Files/Folders
Blocked Files/Folders
GROUP/PATH/FOLDERS/RUNNING PROCESSES
ACTIONS
You can add/edit File Groups here
OK

- 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'.



PROTECTION	STATE	EXCLUSIONS
Interprocess Memory Accesses	Active	Modify (0)
Windows/WinEvent Hooks	Active	Modify (0)
Processes' Termination	Active	Modify (0)
Window Messages	Active	Modify (0)

- 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.

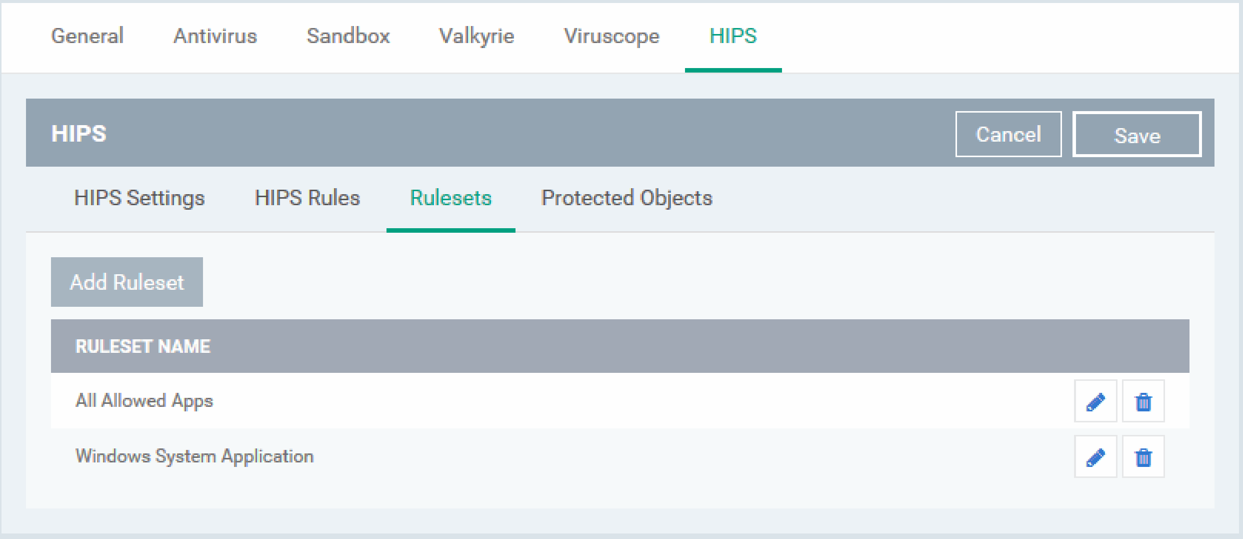
Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

5. 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.

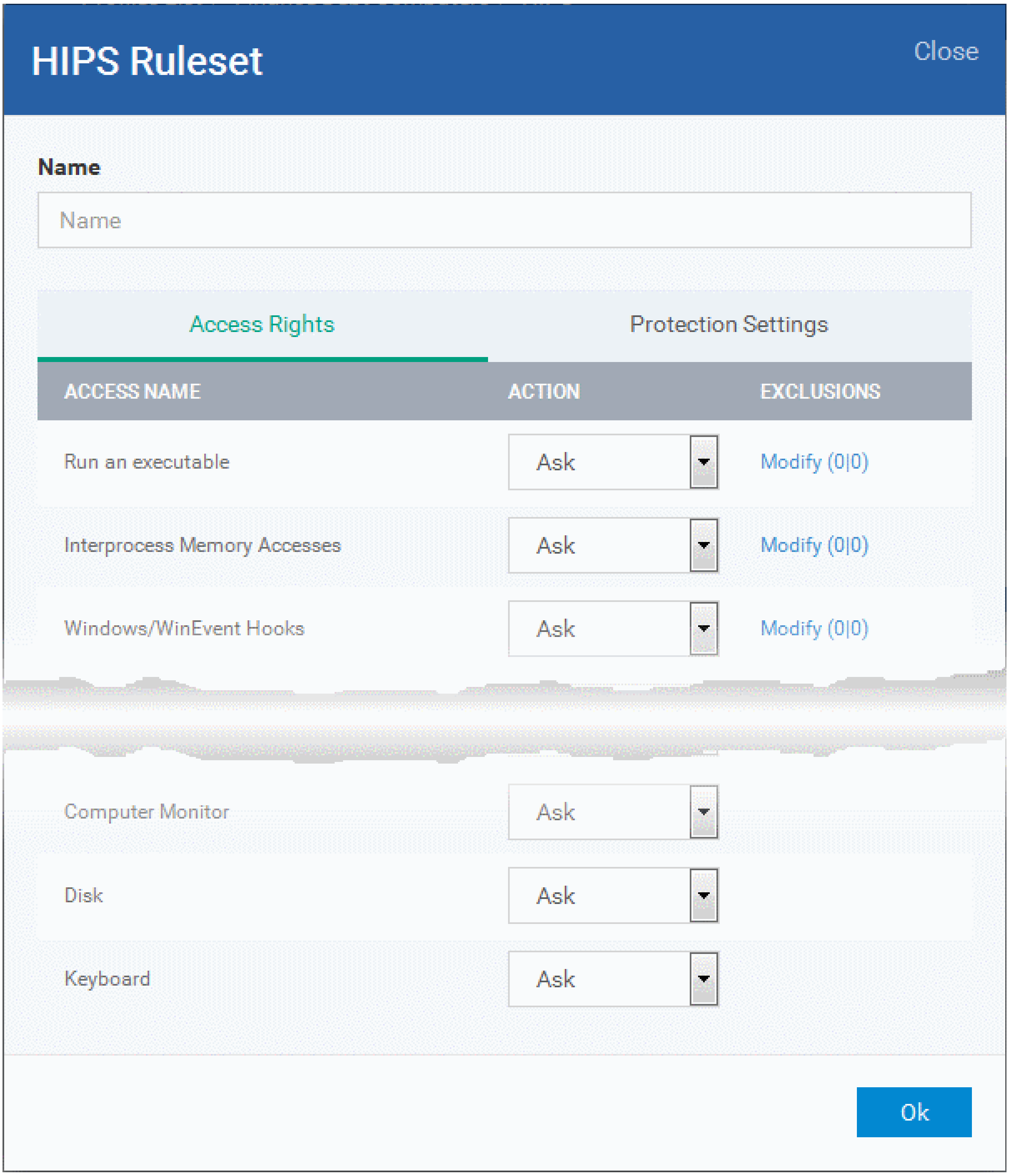


RULESET NAME
All Allowed Apps
Windows System Application

To add a new ruleset

- Click the 'Add Ruleset' button Add Ruleset above the list of rulesets.

The 'HIPS Ruleset' dialog will appear.



Name

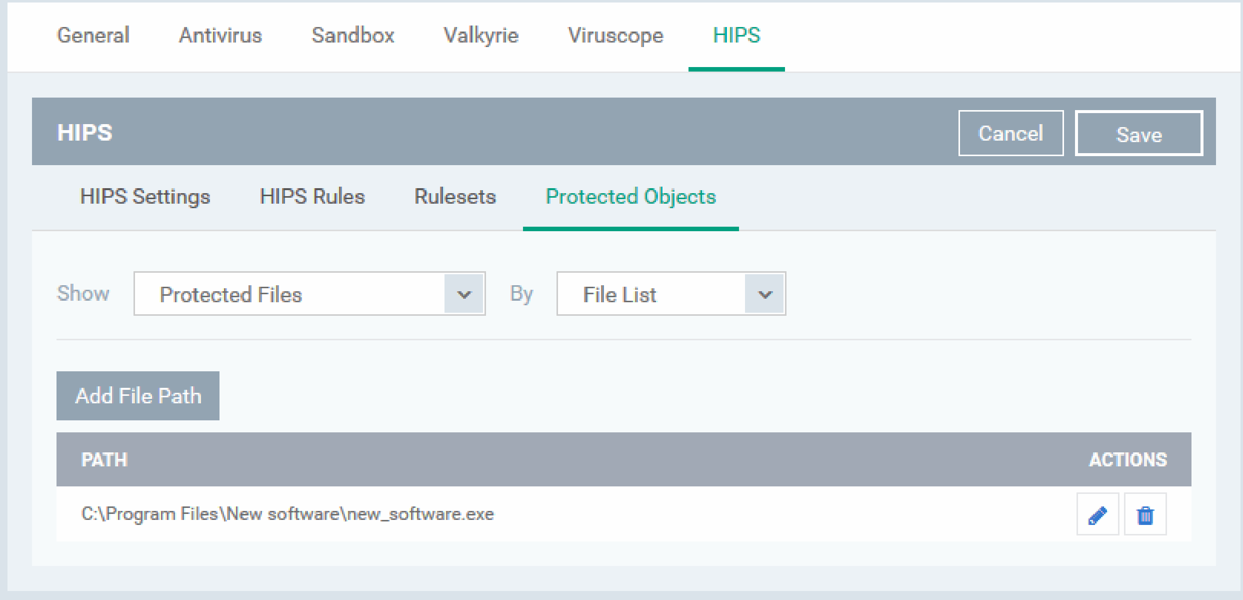
Name

ACCESS NAME	ACTION	EXCLUSIONS
Run an executable	Ask	Modify (0|0)
Interprocess Memory Accesses	Ask	Modify (0|0)
Windows/WinEvent Hooks	Ask	Modify (0|0)
Computer Monitor	Ask	
Disk	Ask	
Keyboard	Ask	

- 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.



Show: Protected Files By: File List

PATH	ACTIONS
C:\Program Files\New software\new_software.exe	

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

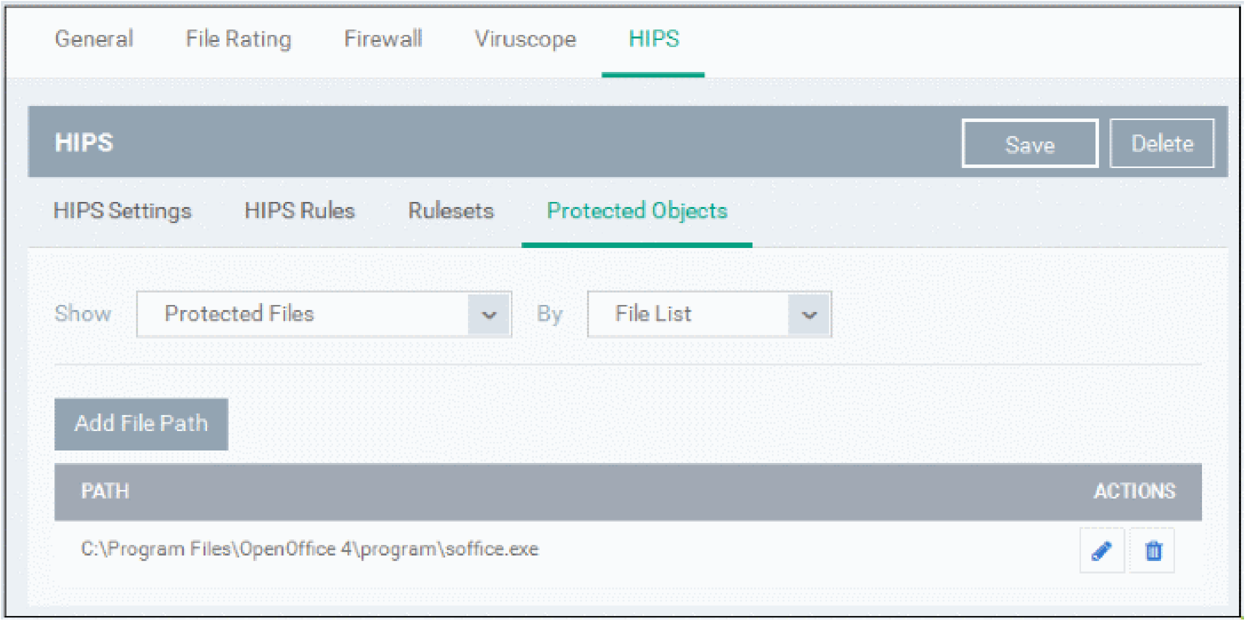
Protected Files

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.

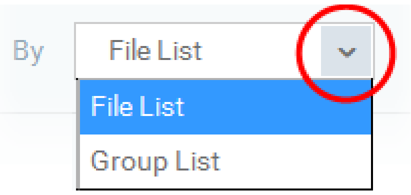
If you add a file to 'Protected Files', but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. Refer to the explanation of **adding 'Exceptions' at the end of this section** for more details about how to allow access to files placed in Protected Files.

- 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.



C:\Program Files\OpenOffice 4\program\soffice.exe

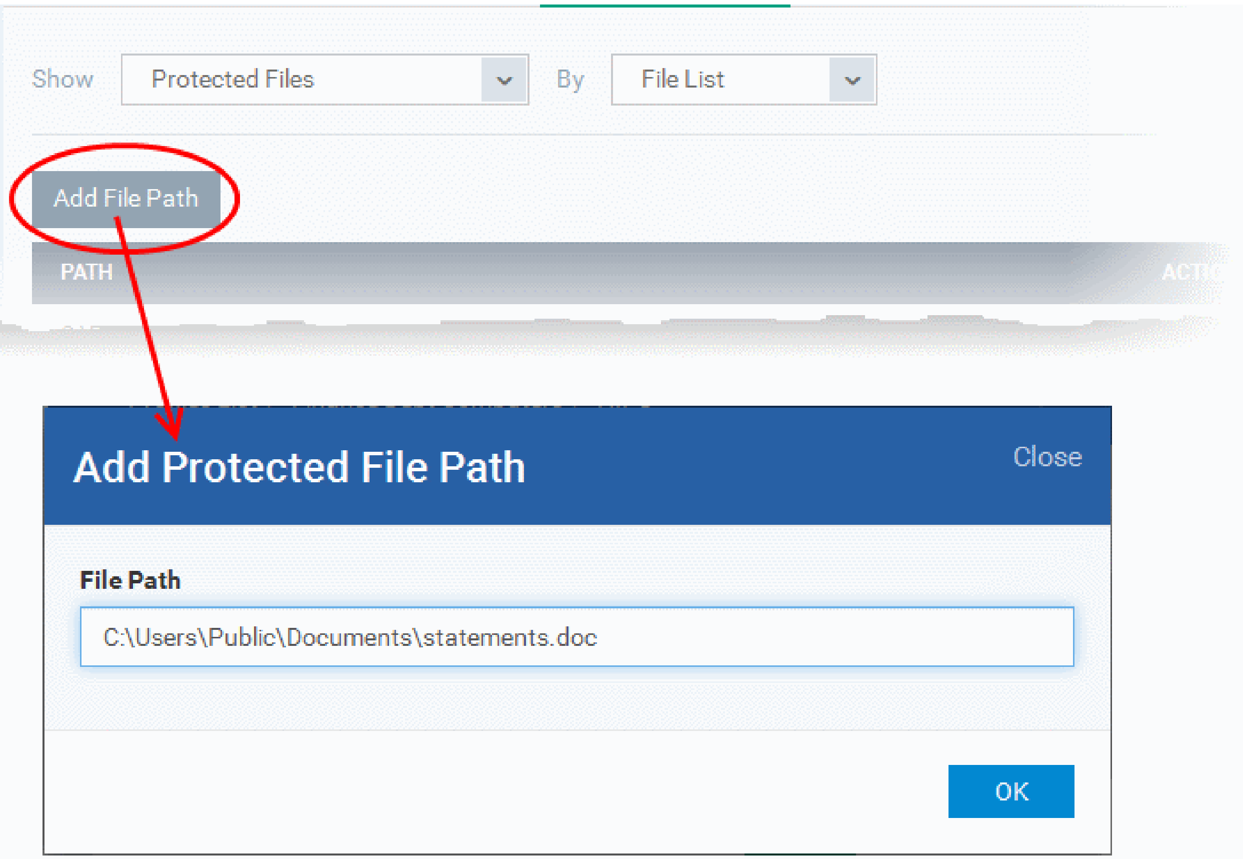


- To view the list of individual files, programs, applications added to the Protected Files list and manage them, choose 'File List'
- To view the File Groups added to the Protected File list, choose 'Group List'

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.



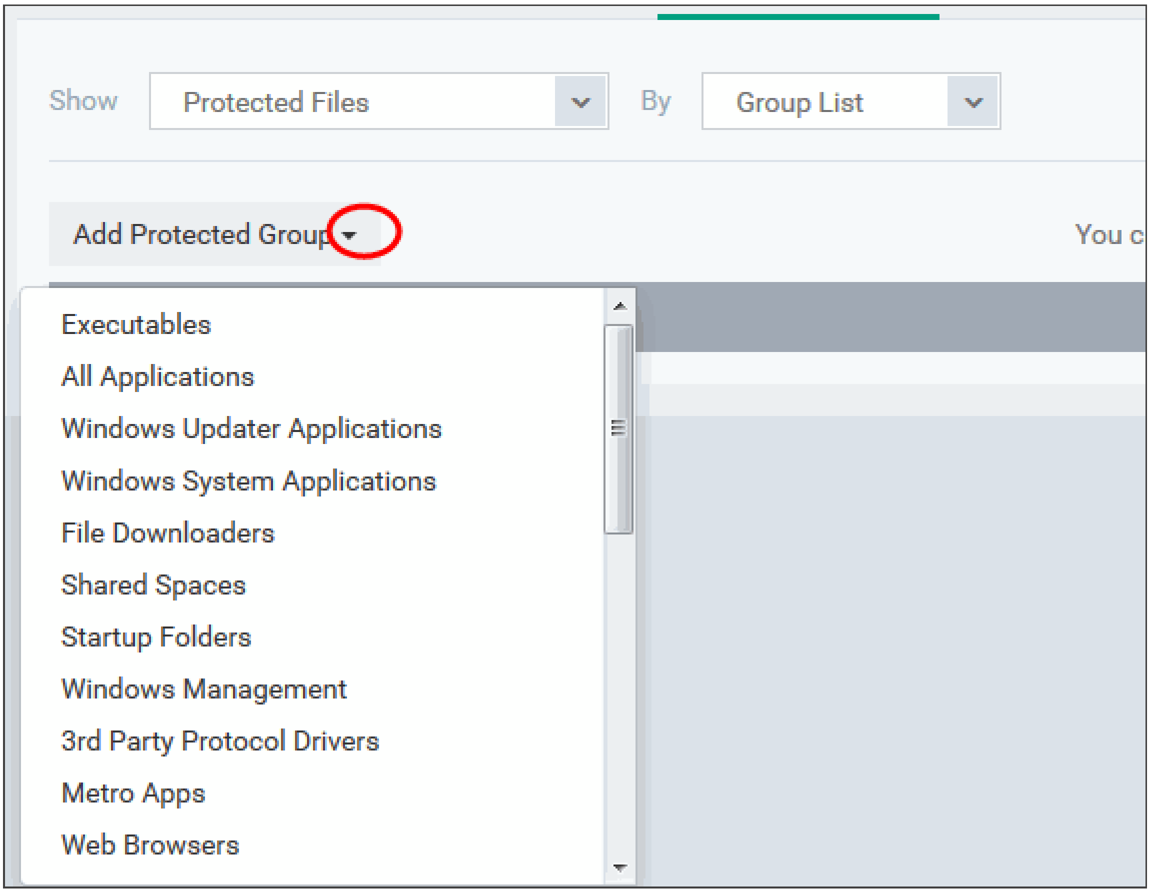
File Path

C:\Users\Public\Documents\statements.doc

- 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'.

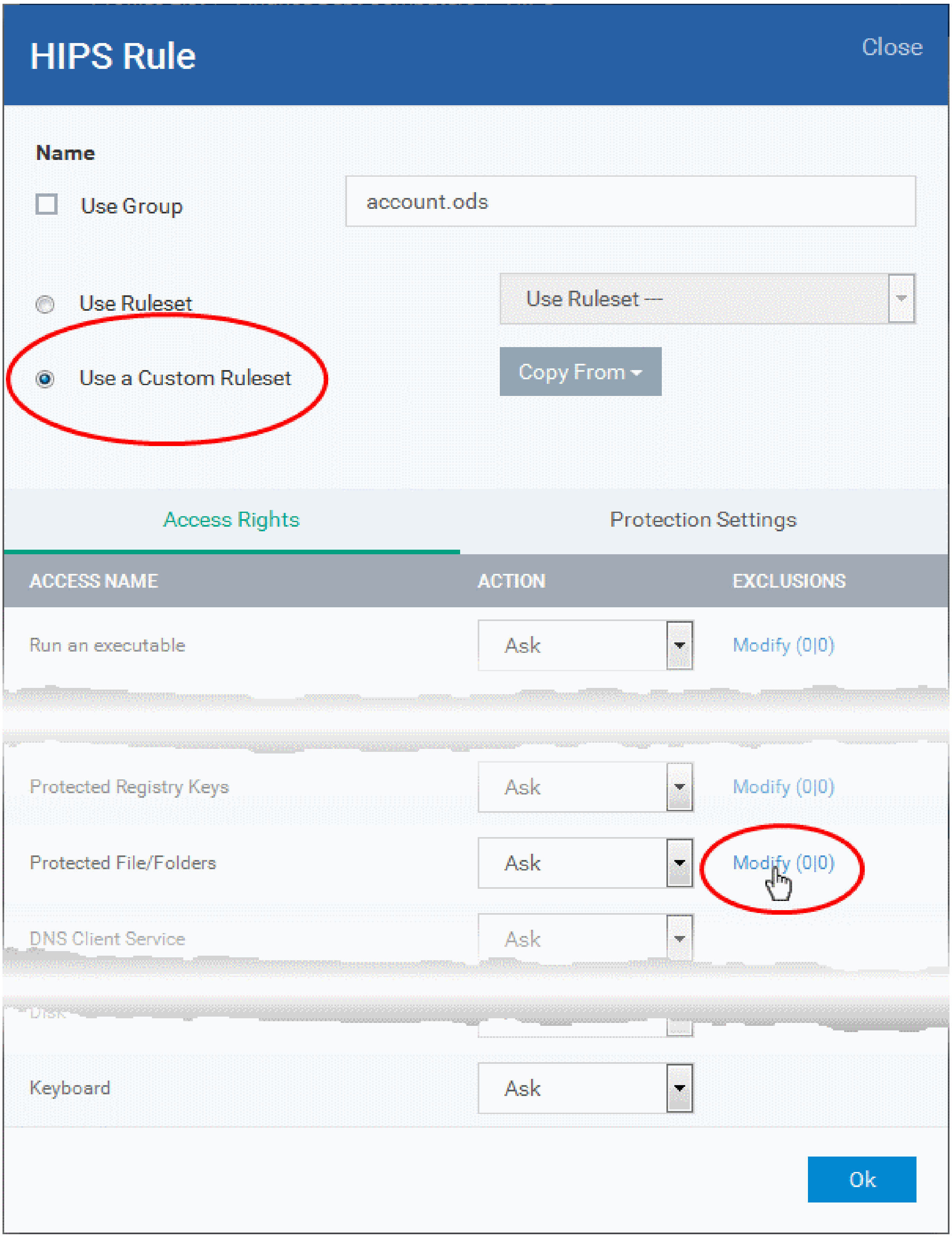
Note: ITSM ships with a set of predefined file groups containing collections of files under respective categories. Administrators can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can 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'
-



HIPS Rule

Name

□ Use Group — account.ods

○ Use Ruleset — Use Ruleset ---

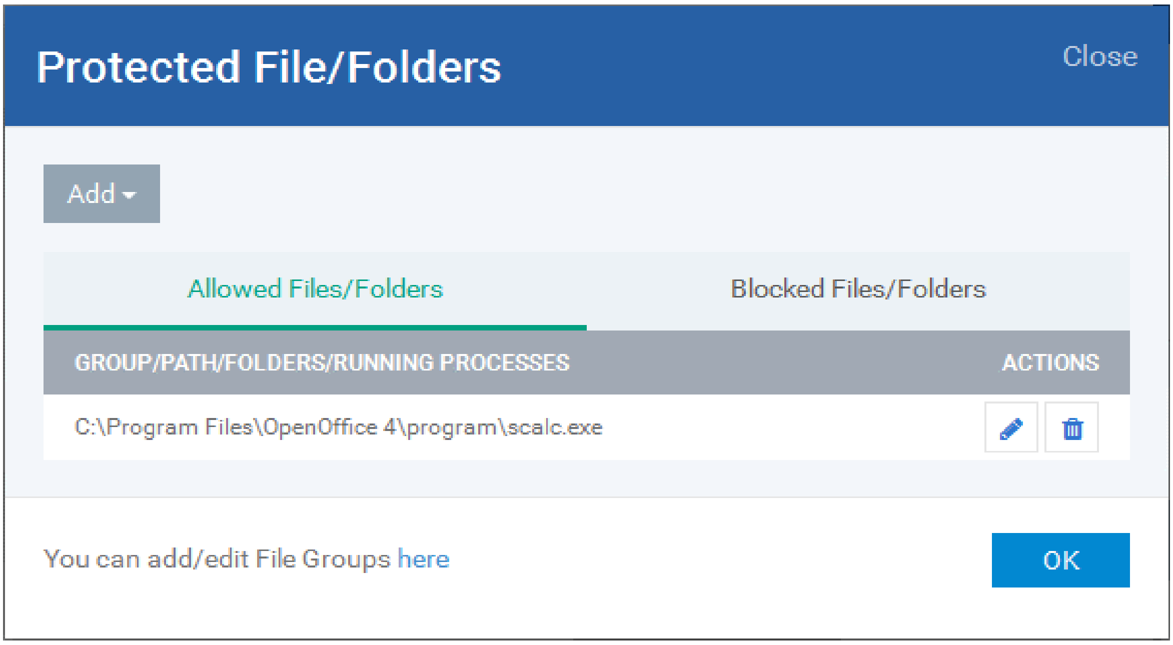
● Use a Custom Ruleset — Copy From

ACCESS NAME	ACTION	EXCLUSIONS
Run an executable	Ask	Modify (0|0)
Protected Registry Keys	Ask	Modify (0|0)
Protected File/Folders	Ask	Modify (0|0)
DNS Client Service	Ask	
Keyboard	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'.



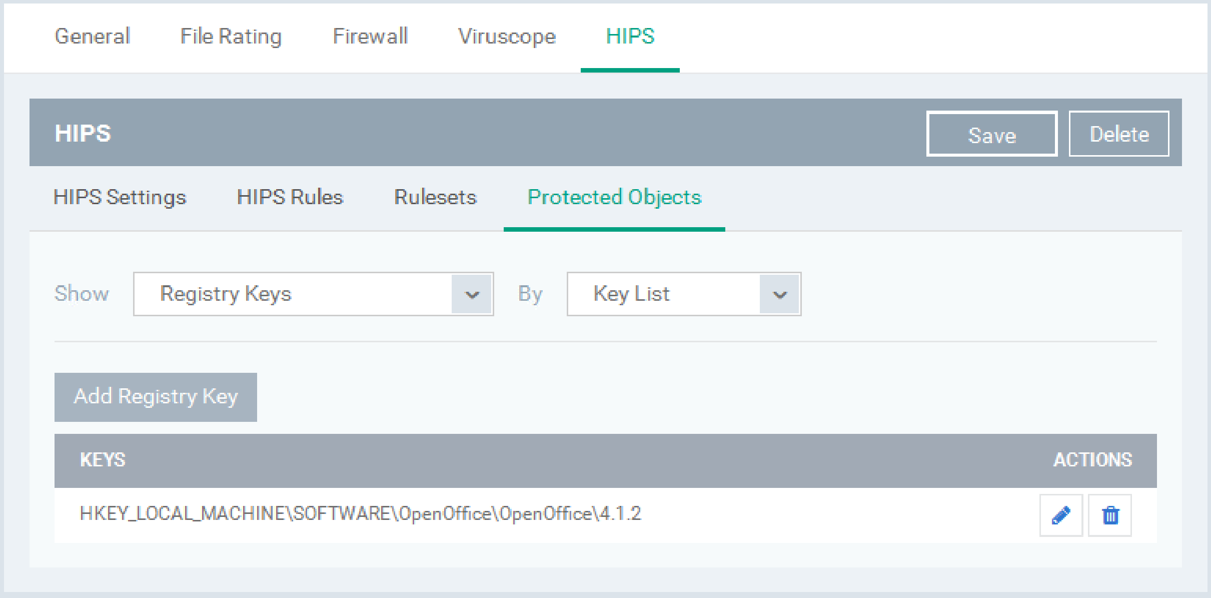
C:\Program Files\OpenOffice 4\program\scalc.exe

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.

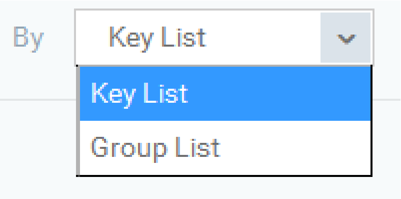
To view the list of Protected Registry Keys, choose 'Registry Keys' from the 'Show' drop-down in the 'Protected Objects' interface



Show: Registry Keys
By: Key List

HKEY_LOCAL_MACHINE\SOFTWARE\OpenOffice\OpenOffice\4.1.2

The Protected Registry Keys list is displayed under two categories, which can be selected from the drop-down at the right.

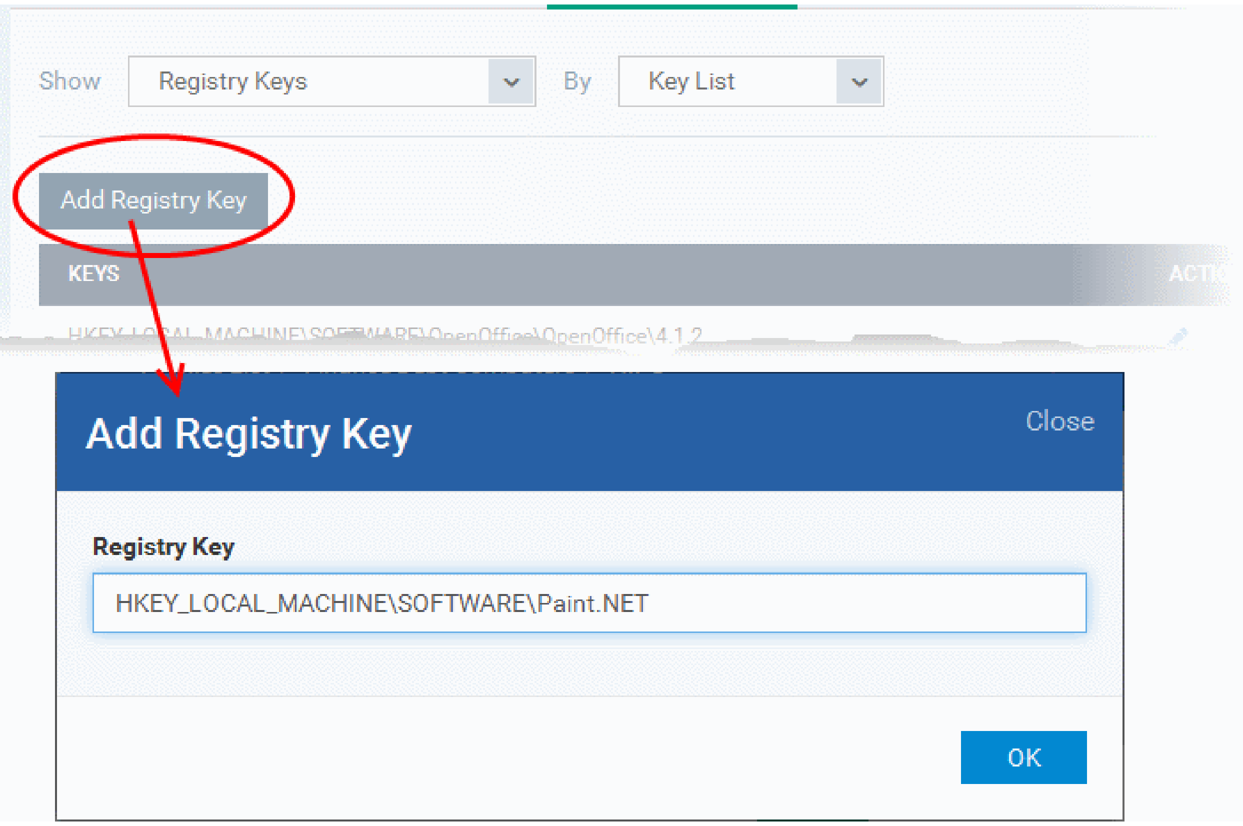


- To view the list of individual keys and values, and manage them, choose 'Key List'
- To view the Registry Groups, choose 'Group List'

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.

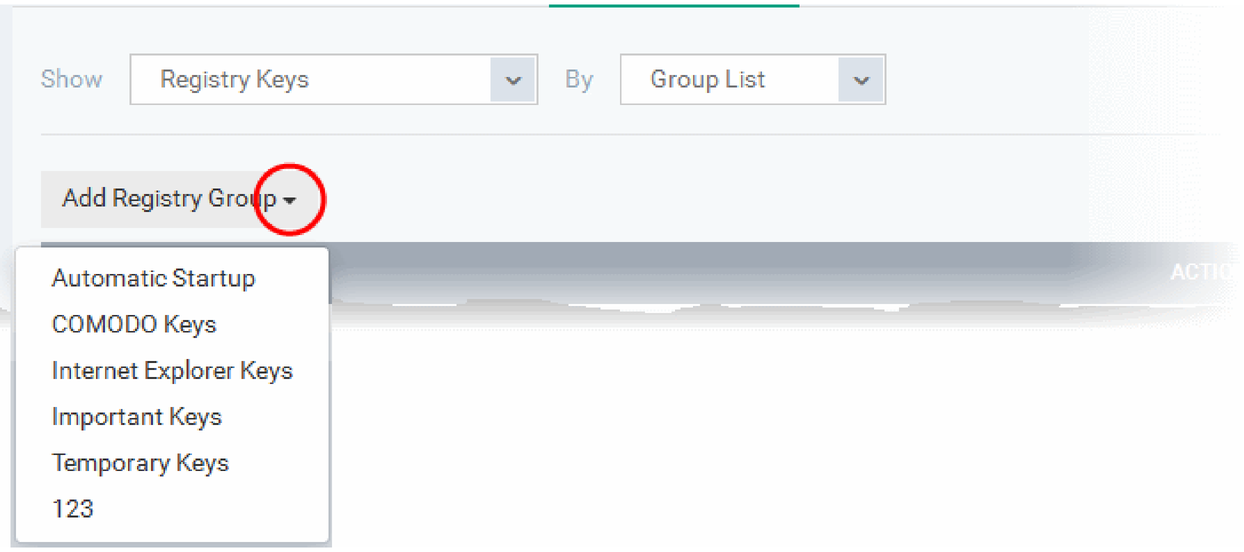


Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\Paint.NET

- 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.

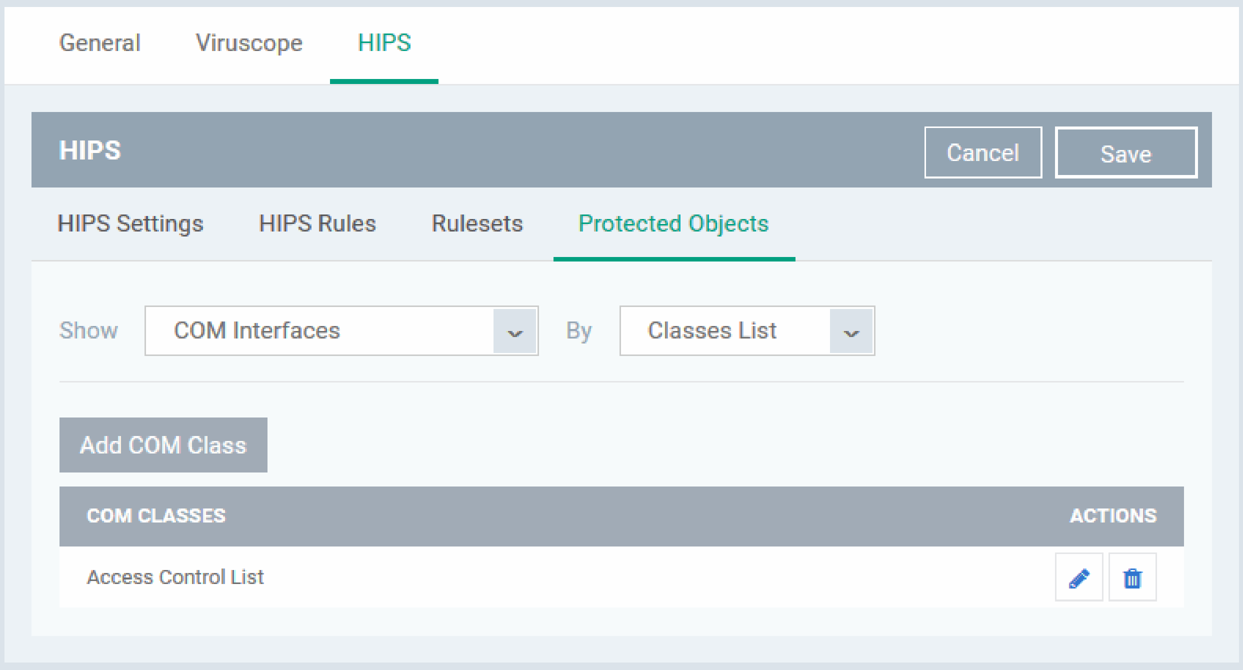
- Repeat the process to add more Registry groups.
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

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.

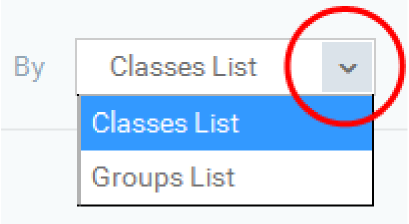
The 'COM Interfaces' list under 'Protected Objects' interface allows you to view and manage list of individual COM classes and COM groups that are to be protected by the Comodo Client Security at the managed computer against modification, corruption and manipulation by malicious processes.

- To view the list of Protected COM interfaces, choose 'COM Interfaces' from the 'Show' drop-down in the 'Protected Objects' interface



Access Control List

The Protected COM Interfaces list is displayed under two categories, which can be selected from the drop-down at the right.

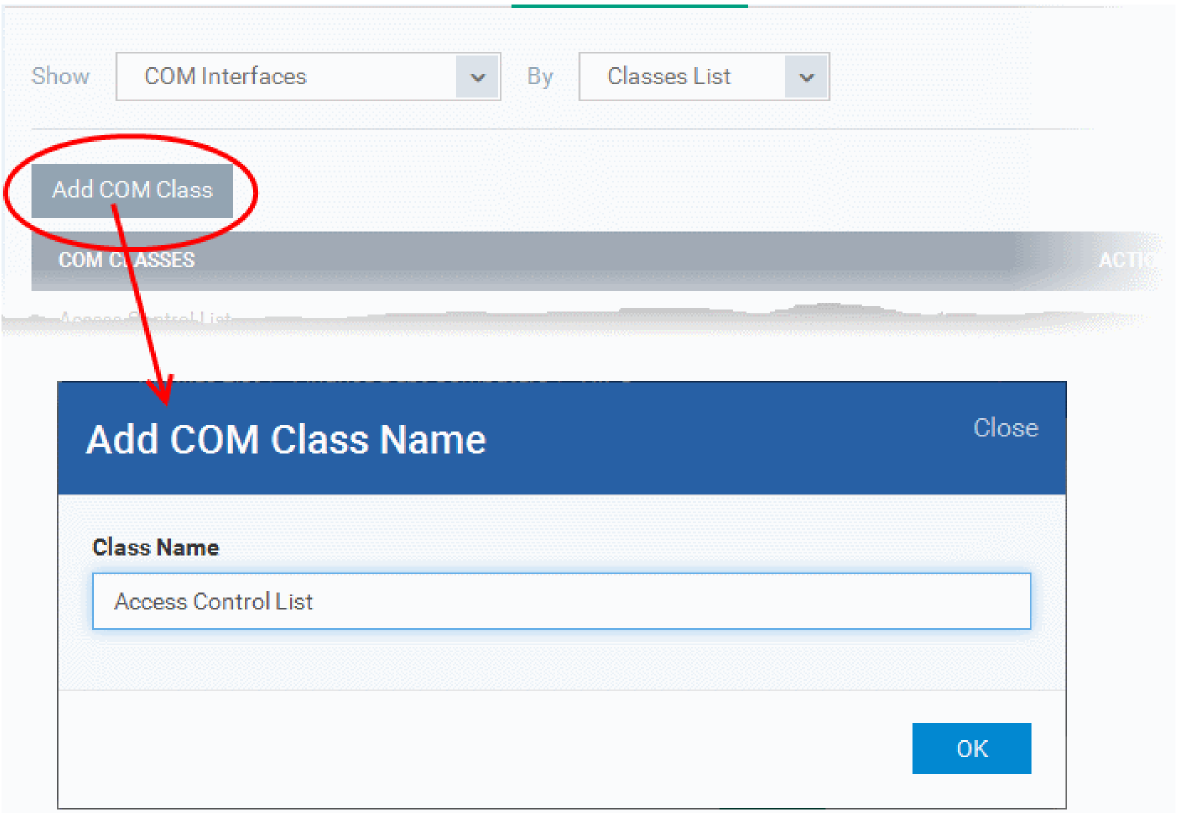


- To view the list of individual COM Interfaces/Classes and manage them, choose 'Classes List'
- To view the COM Groups and manage them, choose 'Group List'

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

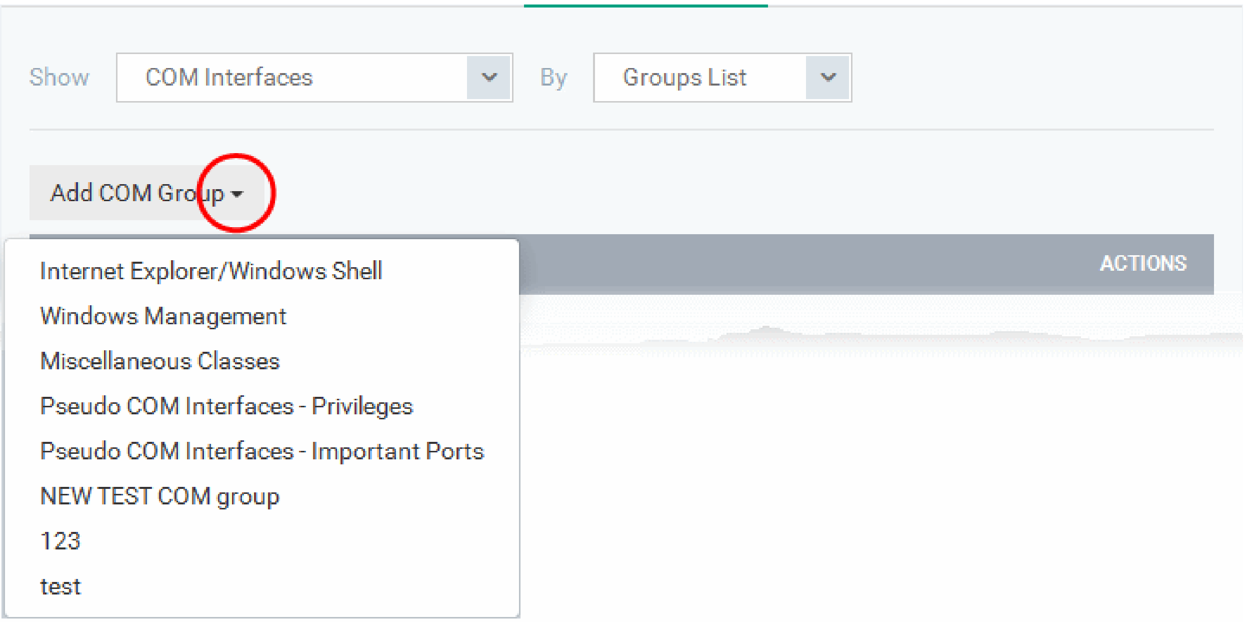


Access Control List

- 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

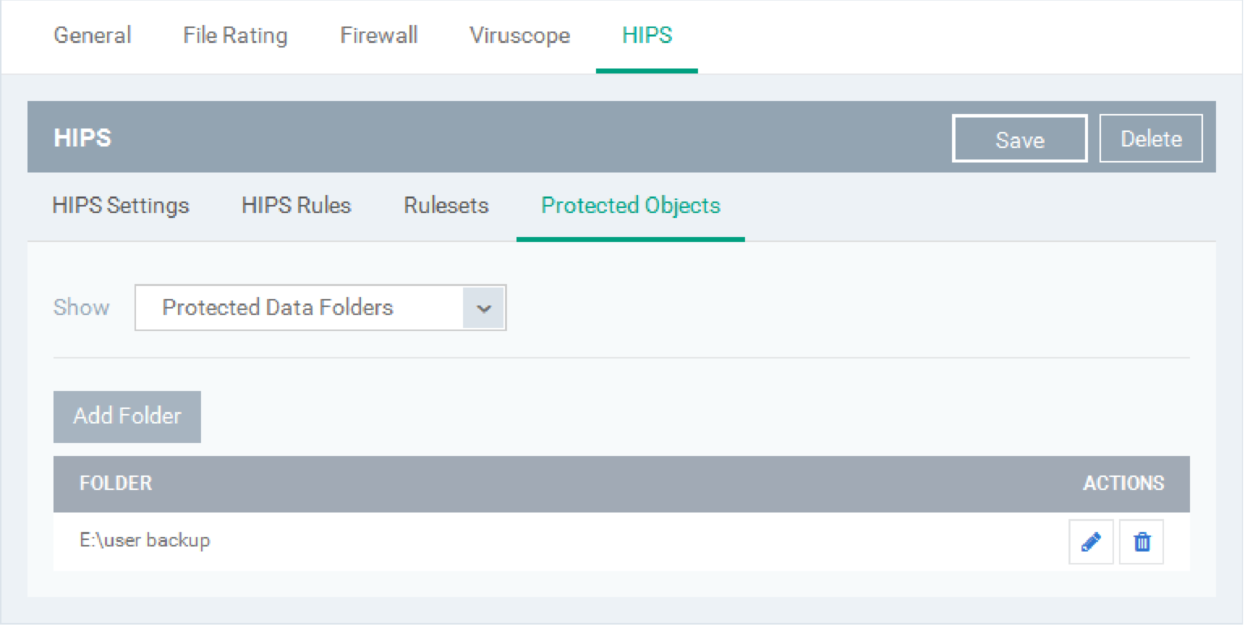
Protected Data Folders

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.



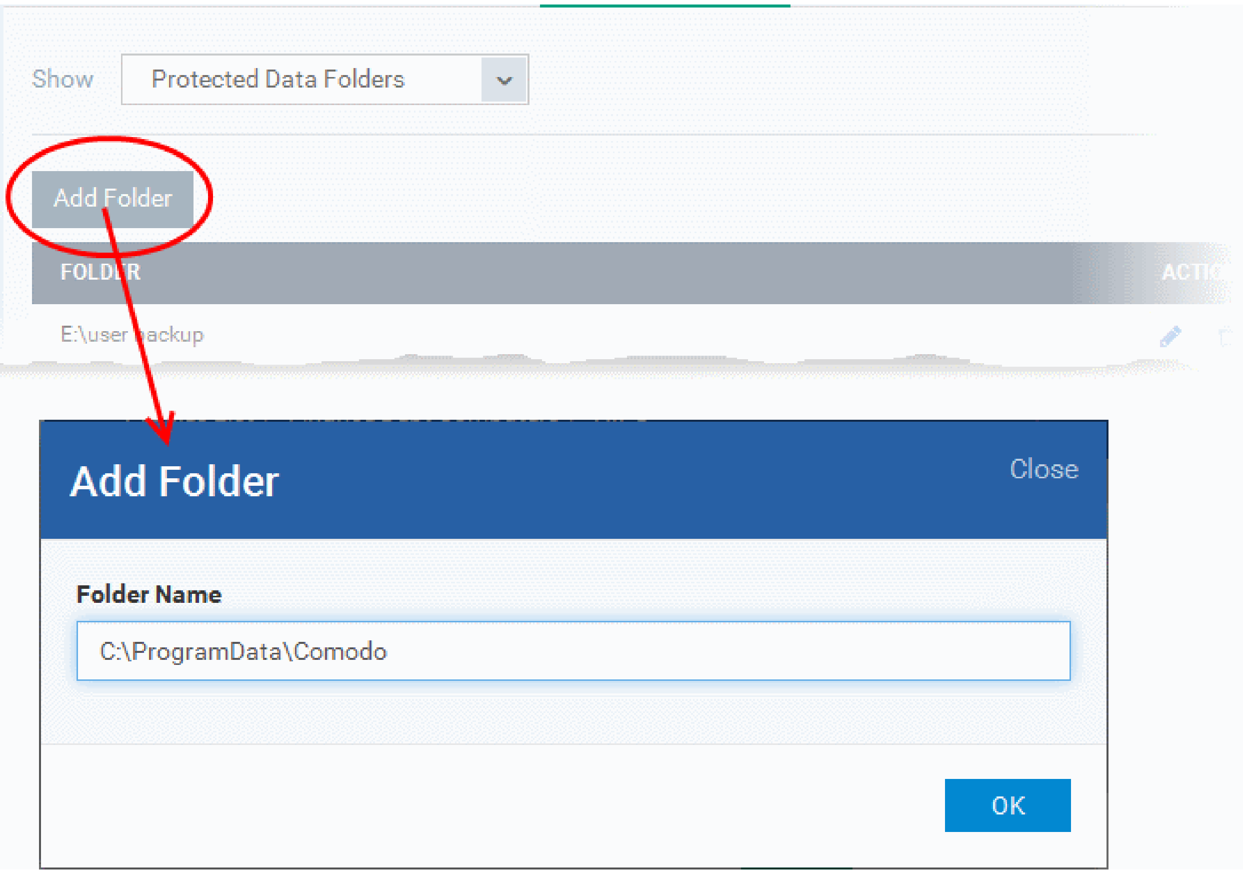
Show: Protected Data Folders

FOLDER	ACTIONS
E:\user backup	✎ 🗑

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) can be configured to run all unknown files in a security hardened environment known as the 'container'.
- Files in the container are prevented from causing damage because they are isolated from the OS, file system and user data.
- The 'Containment' settings area lets you configure the overall behavior of the containment component.
- You can also create rules to define what types of files should be contained and at what restriction level.

Restriction levels include:

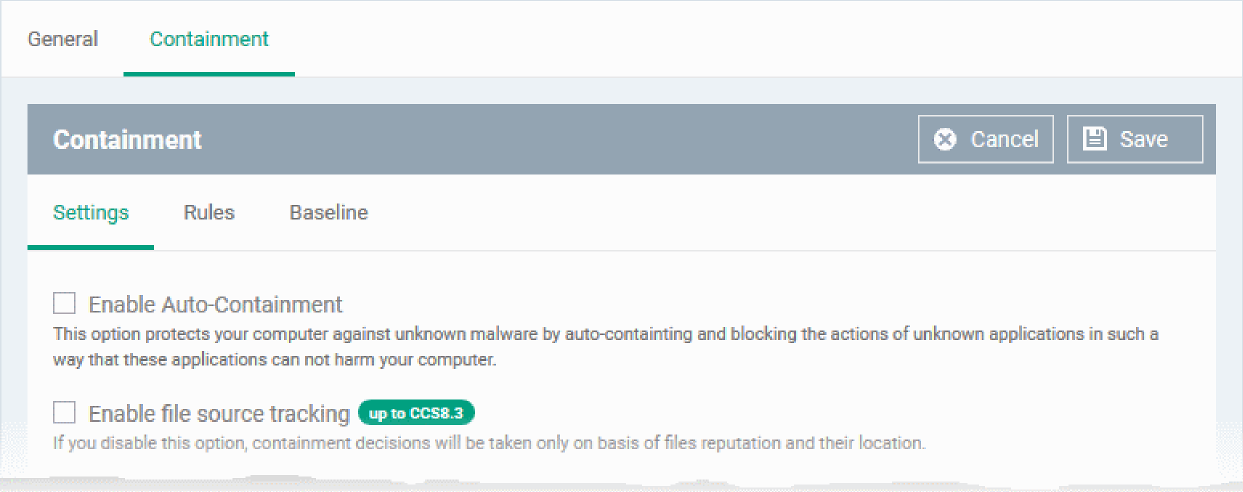
- **Run Virtually**. The file is completely isolated from your operating system and files on your computer
- **Run Restricted**. The file is contained but has limited access to operating system resources
- **Block**. The file is completely prevented from running
- **Ignore**. The file is run outside the container without restrictions

See Auto-Containment Rules for more information about rules.

To configure Containment settings

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click 'Add Profile Section' > 'Containment'

The containment settings screen will open:



□ Enable Auto-Containment

This option protects your computer against unknown malware by auto-containting and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

□ Enable file source tracking up to CCS8.3

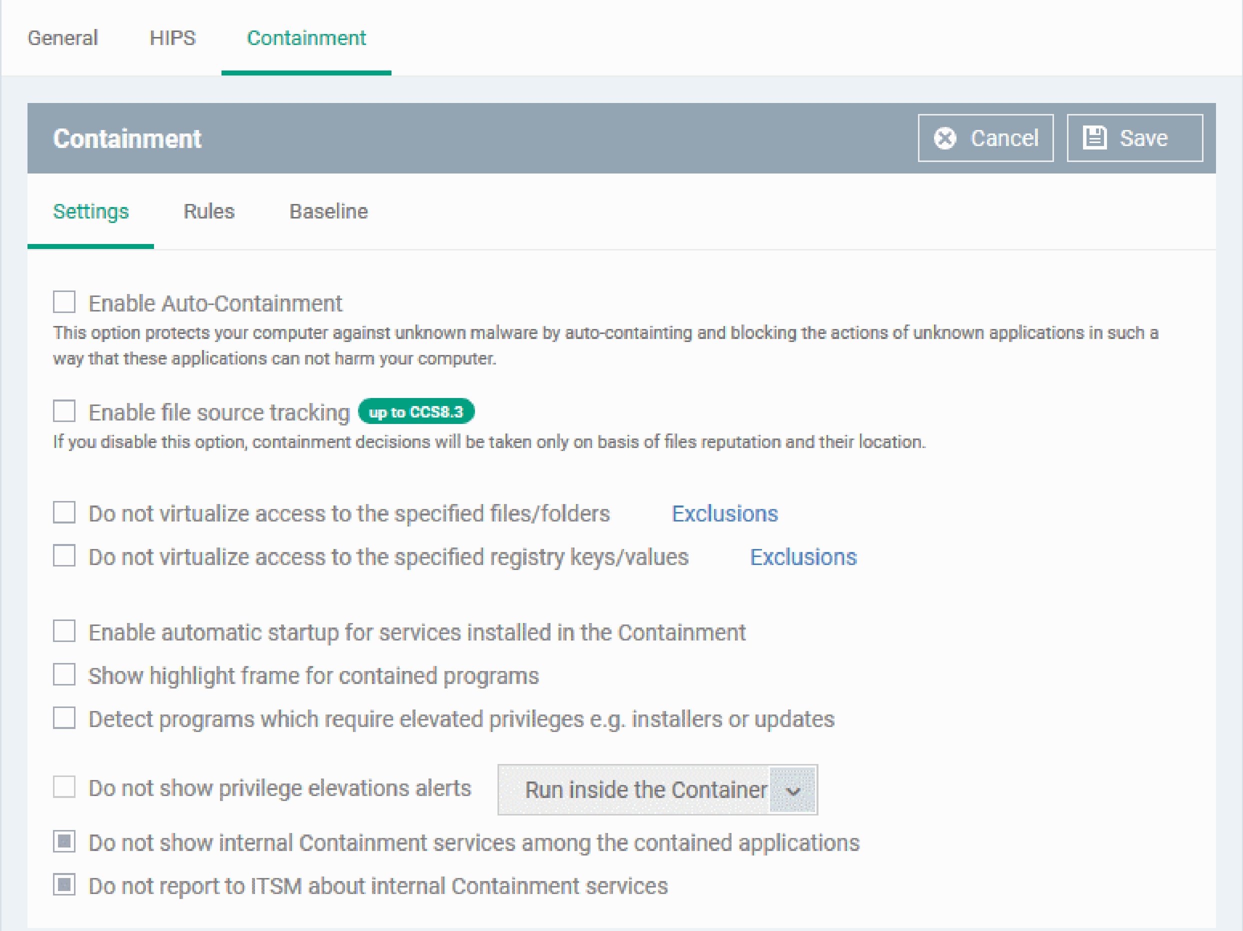
If you disable this option, containment decisions will be taken only on basis of files reputation and their location.

It contains three tabs.

- **Containment Settings**
- **Auto-Containment Rules**
- **Baseline Settings**

Containment Settings

- Enable or disable auto-containment
- Configure files/folders which contained applications are allowed to access
- Configure various settings related to the behavior of the auto-containment system



□ Enable Auto-Containment

This option protects your computer against unknown malware by auto-containting and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

□ Enable file source tracking up to CCS8.3

If you disable this option, containment decisions will be taken only on basis of files reputation and their location.

□ Do not virtualize access to the specified files/folders Exclusions

□ Do not virtualize access to the specified registry keys/values Exclusions

□ Enable automatic startup for services installed in the Containment

□ Show highlight frame for contained programs

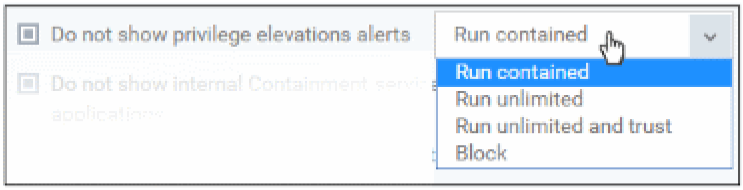
□ Detect programs which require elevated privileges e.g. installers or updates

□ Do not show privilege elevations alerts Run inside the Container

▣ Do not show internal Containment services among the contained applications

▣ Do not report to ITSM about internal Containment services

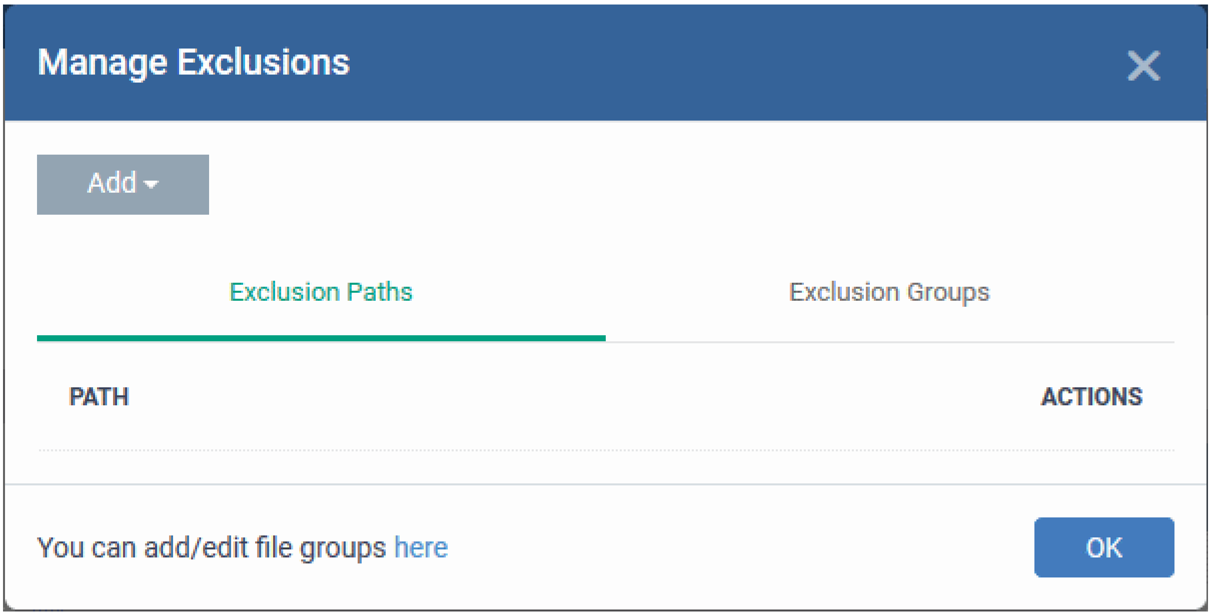
Containment Settings - Table of Parameters	
Form Element	**Description**
Enable Auto-Containment	Enable or disable auto-containment on the endpoint. If enabled, CCS will automatically run unknown applications inside the container. You can also create rules to fine-tune exactly which types of files are contained. For more details on rules, see '**Configuring Rules for Auto-Containment**'. (***Default = Disabled***)
Enable file source tracking	If enabled, the source parameter of a containment rule will be considered. For example, if you only want to auto-contain files downloaded from the internet, then 'internet' is your source. If this setting is disabled then the source will be disregarded and only the reputation and location parameters will be considered. • Applies only to CCS versions 8.3 or lower. (***Default = Disabled***)
Do not virtualize access to the specified files/folders	Contained applications can access folders and files on the local system but cannot save any changes to them. However, you can define exceptions to this rule. (***Default = Disabled***) See **exclusions for files/tolders** (below this table) to find out how to add exclusions. Note - This setting determines whether or not a contained application can access specific files/folders on your local system. It does not determine whether or not an application should run in the container in the first place. If you wish to exclude applications in their entirety from the container, see **Auto-Containment Rules** instead.
Do not virtualize access to the specified registry keys/values	Contained applications can access Windows Registry Keys and Values on the local system but cannot save any changes to them. However, you can define exceptions to this rule. Click the 'Exclusions' link to define registry keys/values which contained files are allowed to modify. (***Default = Disabled***) See **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. (***Default = Disabled***)
Show highlight frame for contained programs	If enabled, CCS will display a green border around programs running in the container on the endpoint. (***Default = Disabled***)
Detect programs which require elevated	If enabled, CCS will proactively track programs that require admin

Containment Settings - Table of Parameters	
privileges e.g. installers or updates	privileges to run. An program that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry. (***Default = Disabled***)
Do not show privilege elevation alerts	If 'Detect...' is enabled (see setting above) then an alert is shown to the end-user when a new or unrecognized program requires admin or elevated privileges to run. If you do not want these alerts to be shown, select this option and choose the action to be taken for unrecognized programs:  □ Do not show privilege elevations alerts Run contained Run contained Run unlimited Run unlimited and trust Block □ Do not show internal Containment services applications (***Default = Disabled***)
Do not show internal Containment services among the contained applications	If enabled, any processes started by CCC/CCS will not be shown in the 'Active Process List' in CCS. You can view contained processes in CCS by clicking: • Tasks' > 'General Tasks' > 'View Active Processes' • Right-click anywhere in the interface > select 'Show Contained only' (***Default = Enabled***)
Do not report to ITSM about internal Containment services	If enabled, no information about contained processes started by CCC/CCS will be sent to ITSM. Click 'Security Sub-Systems' > 'Containment' in ITSM to view a history of contained applications and processes. (***Default = Enabled***)

To define exclusions for files and folders

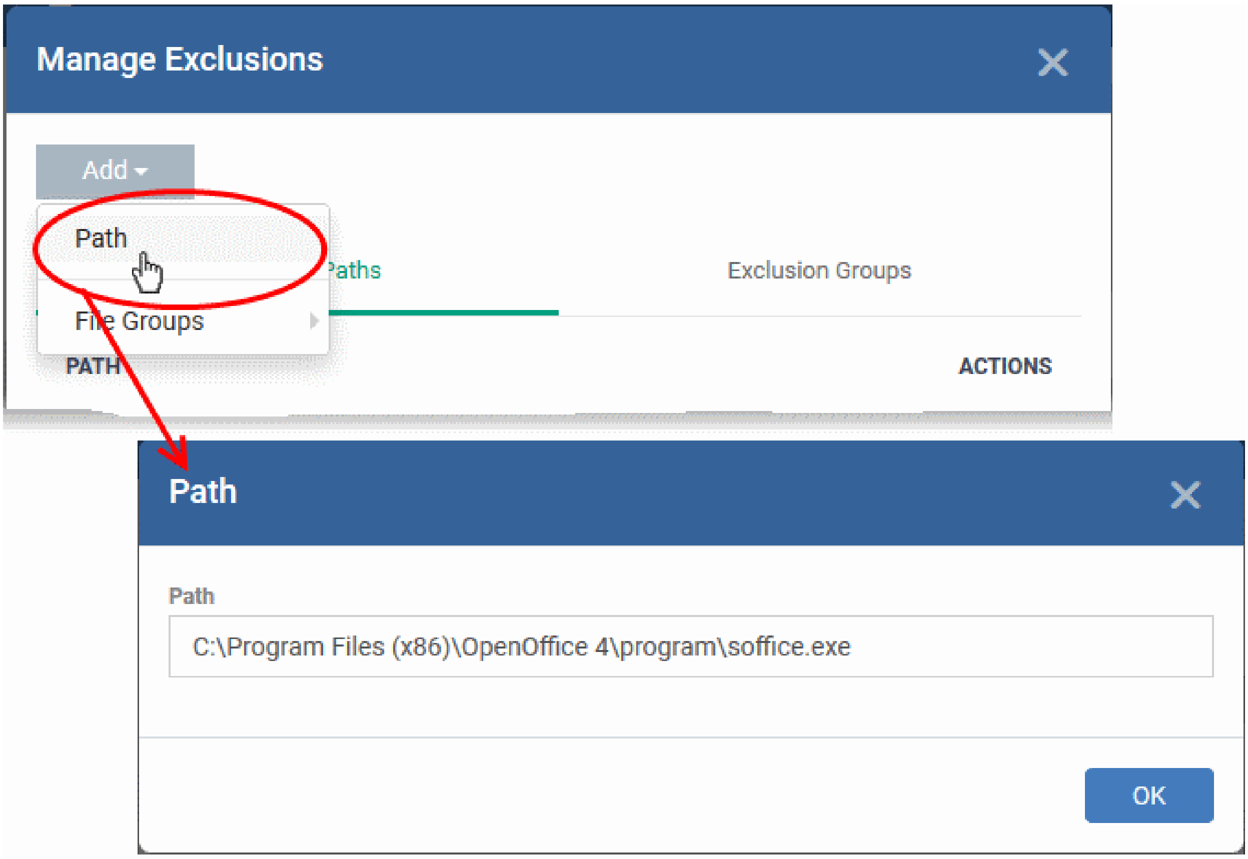
> **Note**. This section explains how to create an exclusion which allows an application in the container to access specific files and folders on the local system. If you want to entirely exclude an application from the container, then please see **Auto-Containment Rules** instead.

- Enable the 'Do not virtualize access to the specified files/folders' option then click 'Exclusions'.



You can add/edit file groups here

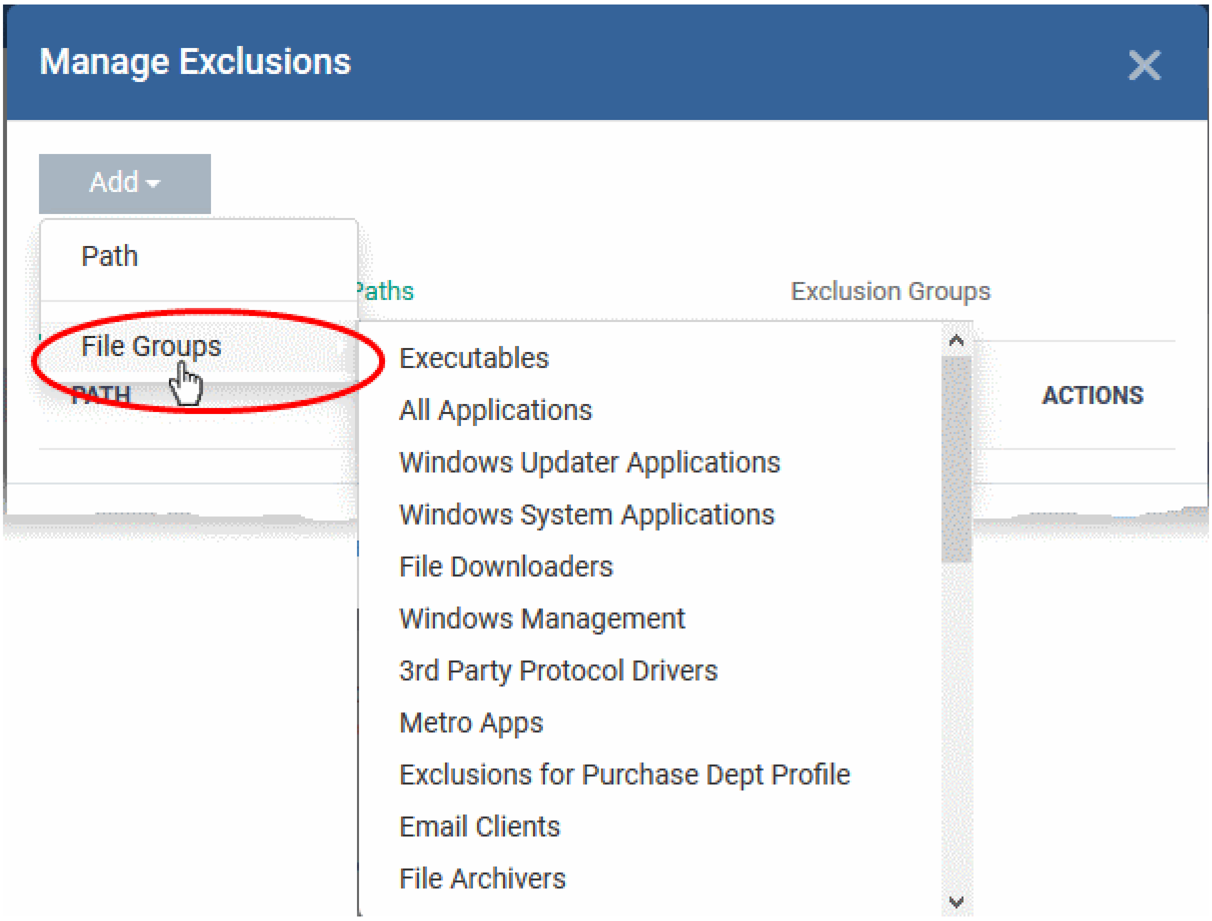
- The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:
  - **Exclusion Paths** - The individual files that are added to the list, with their installation path
  - **Exclusion Groups** - The file groups that are added to the list. A file group is a group of executable 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



C:\Program Files (x86)\OpenOffice 4\program\soffice.exe

- Enter the storage/installation path of the file to be added to the exclusions list

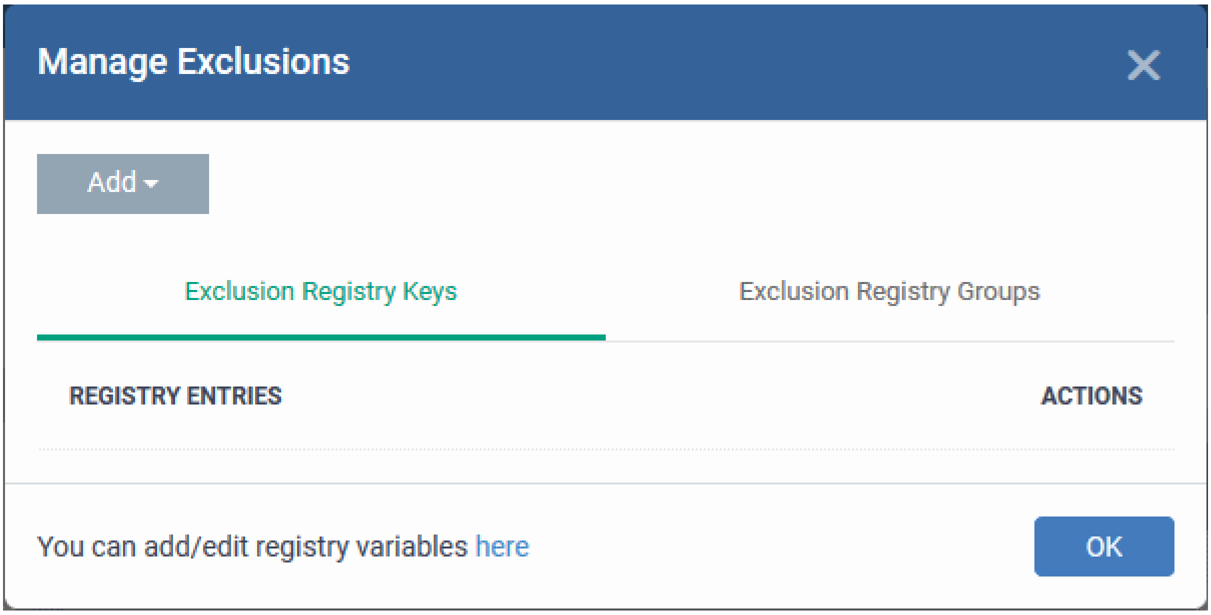
- To add a File Group to exclusions, choose File Groups from the Add drop-down and choose the File Group.



- 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

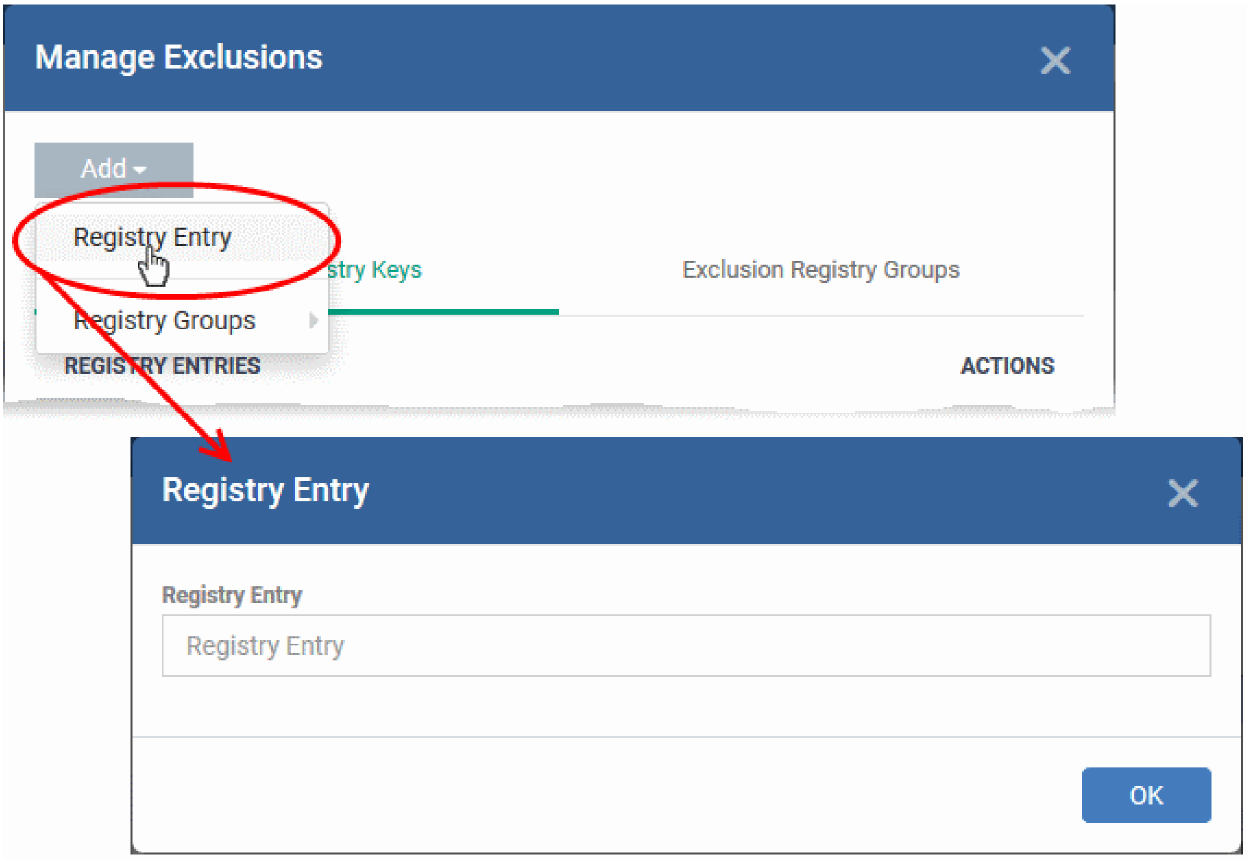
- Click 'Exclusions' beside 'Do not virtualize access to specified registry keys/values'.



You can add/edit registry variables here

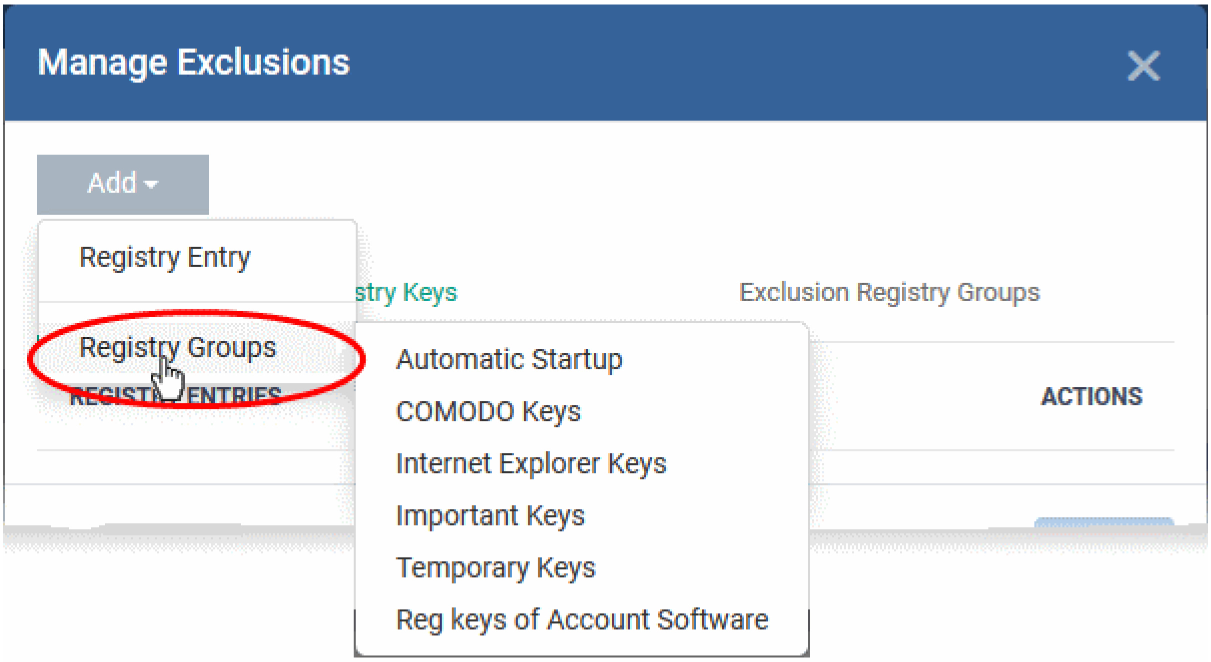
The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:

- **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.

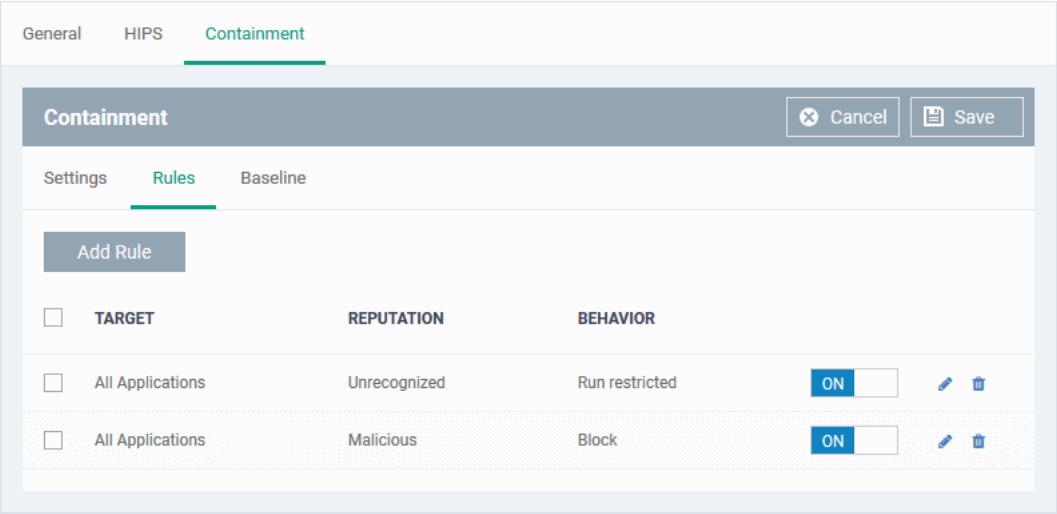
- Click the 'Save' button.

Configure Auto-Containment Rules

- Containment rules determine whether a program should be allowed to run with full privileges, run outside the container, run restricted, or run inside the container.
- For easy identification, CCS will show a green border around programs that are running in the container on an endpoint, if configured in the **containment settings**.

To open the rules interface:

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click the 'Containment' tab (click 'Add Profile Section' > 'Containment' if you haven't added it yet)
- Click the 'Rules' tab to view and manage auto-containment rules.:



□	TARGET	REPUTATION	BEHAVIOR		
□	All Applications	Unrecognized	Run restricted	ON	
□	All Applications	Malicious	Block	ON	

- The table lists all rules configured for the profile.
- Rules at the top of the table have a higher priority than those at the bottom. The setting in the rule nearer the top will be applied in the event of a conflict between rules.

Containment Rules - Column Descriptions	
Column Heading	**Description**
Target	The files, file groups or locations to which the rule applies.
Reputation	The trust status of the files to which the rule should apply. The possible values are: • 'Any' • 'Malicious' • 'Trusted' • 'Unrecognized'.
Behavior	The action that will be taken on the targets if the rule criteria are met. Possible actions are: • Run virtually. File is sandboxed inside a fully virtual environment. • Run restricted. File is sandboxed with limited access to device resources. • Block. File is not allowed to run at all. • Ignore. File is not sandboxed and is allowed to run on the host without restriction.

- Use the slider to enable/disable a rule.
- Click the trash icon to remove a rule.
- Click the edit icon to modify a rule.

Target(s) can be filtered by numerous criteria. These are, however, optional, so admins can create a very simple rule to run an application in the container just by specifying the action and the target application.

Example:

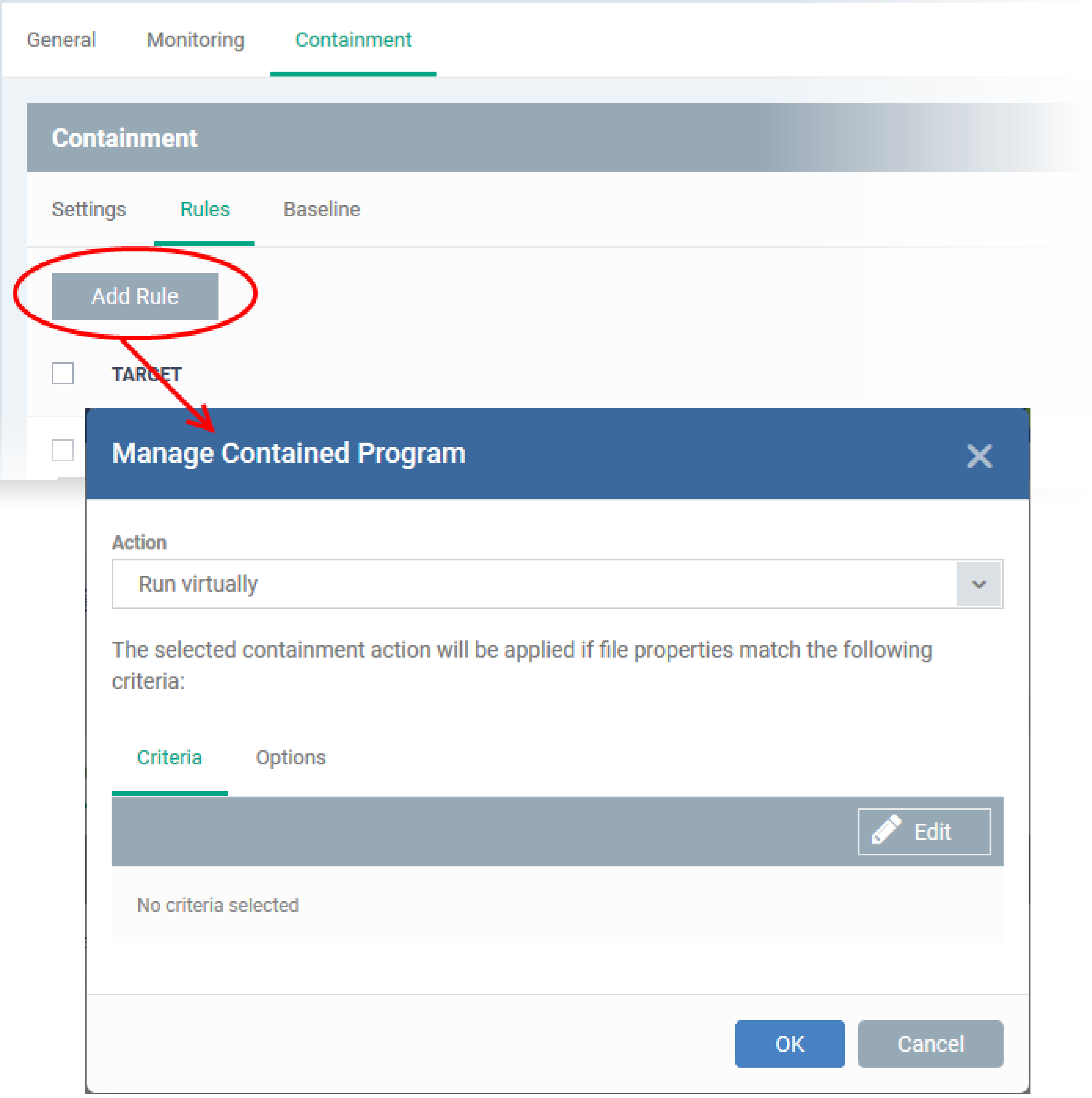
Run an application outside the container

- Open the containment tab and click 'Rules'
- Click 'Add Rule'
- Select 'Ignore' in the 'Action' drop-down
- Click 'Edit' in the 'Criteria' section to choose the application(s) you wish to exclude
- Choose the file, folder, file group or hash you want to exclude
- Click 'OK'
- Move the new rule to the top of the rules list (you can drag and drop rules)

To add a new rule

- Open the profile you wish to add the rule to
- Click the 'Containment' tab (click 'Add Profile Section' > 'Containment' if you haven't added it yet)
- Click the 'Rule' tab

- Click the 'Add Rule' button
- The 'Manage Contained Program' dialog will open:



Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

No criteria selected

The dialog shows the action at the top and contains two tabs:

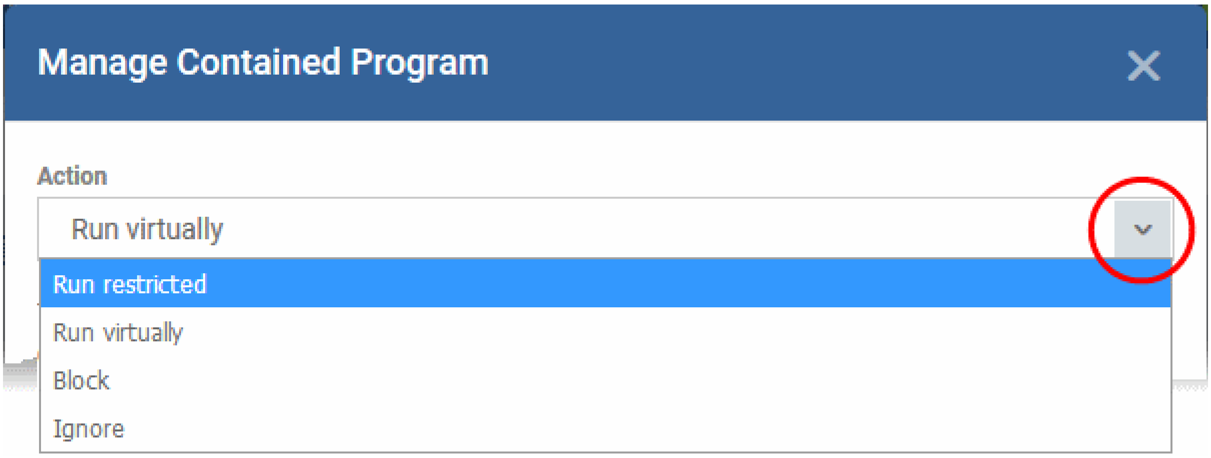
- Criteria - Define conditions upon which the rule should be applied.
- Options - Configure additional actions like logging, memory allowance and execution time restrictions.

Creating a new containment rule involves the following steps:

- **Step 1 - Choose the action**
- **Step 2 - Select the target file/group and set the filter criteria for the target files**
- **Step 3 - Select the options**

Step 1 - Choose the action

- The setting in the 'Action' drop-down and the restriction level in the 'Options' tab determine the privileges of an auto-contained application.



Manage Contained Program

Action: Run virtually

The options available in the 'Action' drop-down are:

- **Run 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.
- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be contained and allowed to run with all privileges.

Step 2 - Select the target file/group and set the filter criteria for the target files

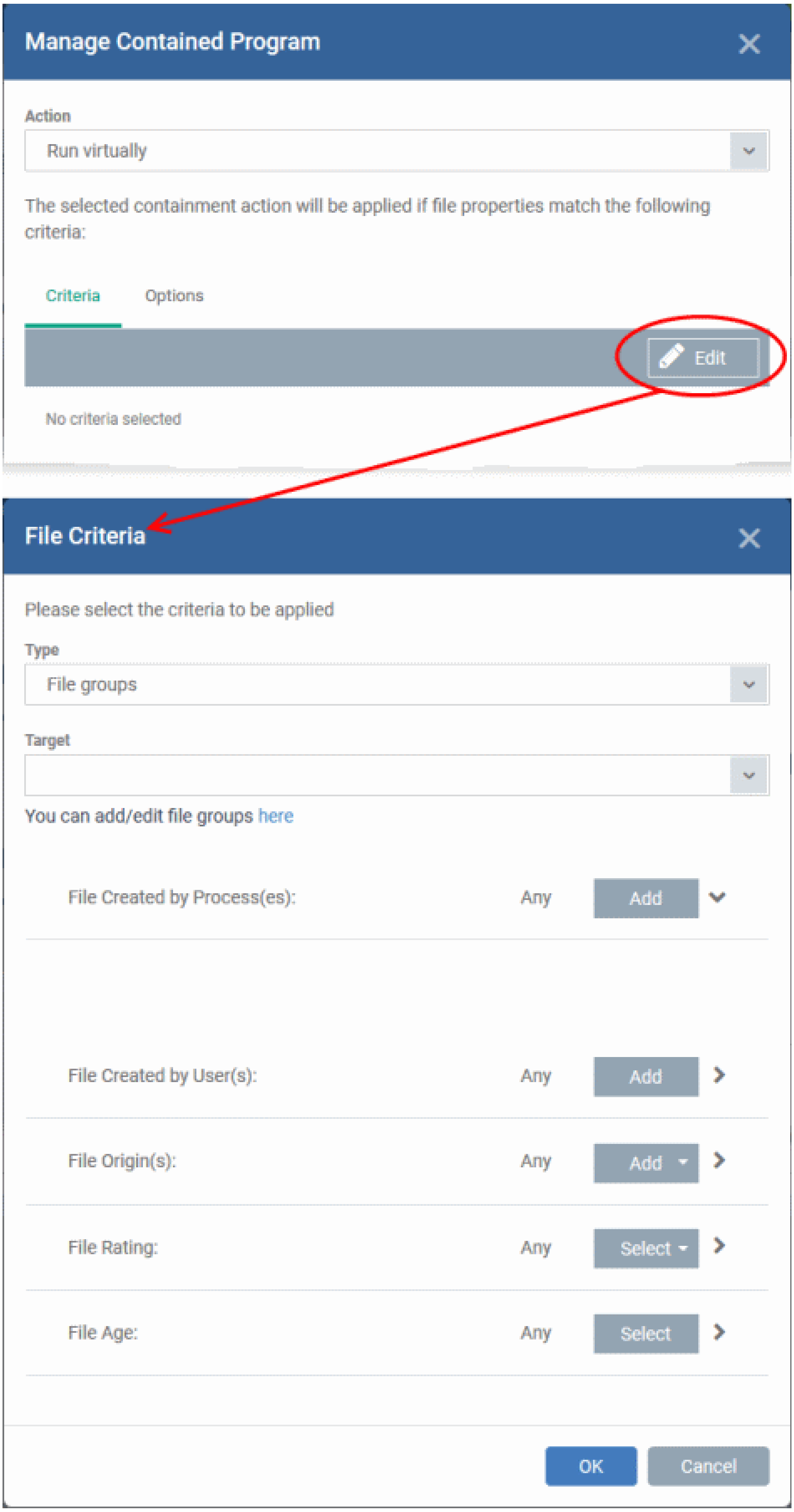
- The next step is to select the rule targets and configure filter parameters in the 'Criteria' tab.
- Filters let you target very specific types of file. For example, if you choose 'File Groups' as the type, 'Executables' as the target and add a 'File Origin' filter of 'Internet', then the rule only affects executables downloaded from the internet.
- Another example is if you want to allow unrecognized files created by a specific process to run outside the container:
    - Select 'Ignore' as the 'Action' then click 'Edit' in the 'Criteria' tab.
    - Select 'File Groups' as the type and 'All Applications' as the target
    - Select 'File created by process(es)' as the filter criteria
    - Click 'Add' and select 'Files' as the type.
    - Browse to the executable you wish to exempt.

To select the target and set filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right



Manage Contained Program

Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

No criteria selected

File Criteria

Please select the criteria to be applied

Type: File groups

Target:

You can add/edit file groups here

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

File Age: Any

The 'File Criteria' dialog will open. The file criteria dialog allows you:

- Select the target
- Configure the filter criteria

Select the target

- Select the type of target item from the 'Type' drop-down. The 'Target' field lets you choose a target application, file group, folder or hash as applicable:
  - **Files** - Add an executable as the target by entering its installation path + file name.
  - **File Groups** - File groups are handy, predefined groupings of one or more file types. For example, selecting 'Executables' would include all files with the extensions .exe .dll .sys .ocx .bat .pif .scr. Other predefined categories include 'Windows System Applications' , 'Windows Updater Applications' and 'Start Up Folders'. You can also create custom file groups in 'Settings' > 'System Templates' > 'File Groups Variables'. Refer to '**Creating and Managing File Groups**' for more details.
    - Select the predefined or custom file-group from the 'Target' drop-down.
  - **Folder** - Add the contents of a folder as the target.
    - Enter the path to the folder that contains the target files in the 'Target' field.
  - **File Hash** - 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.
    - Enter the SHA1 hash value of the target executable file in the 'Target' field.
  - **Process Hash** - Add a program as a target by specifying the SHA1 hash value of the process created by the executable. CCS monitors the files at the endpoint applied with the policy and if a process with the same hash value attempts to execute, the rule will be triggered and the program will be auto-contained as per the rule.
    - Enter the SHA1 hash value of the process created by the target file in the 'Target' field.

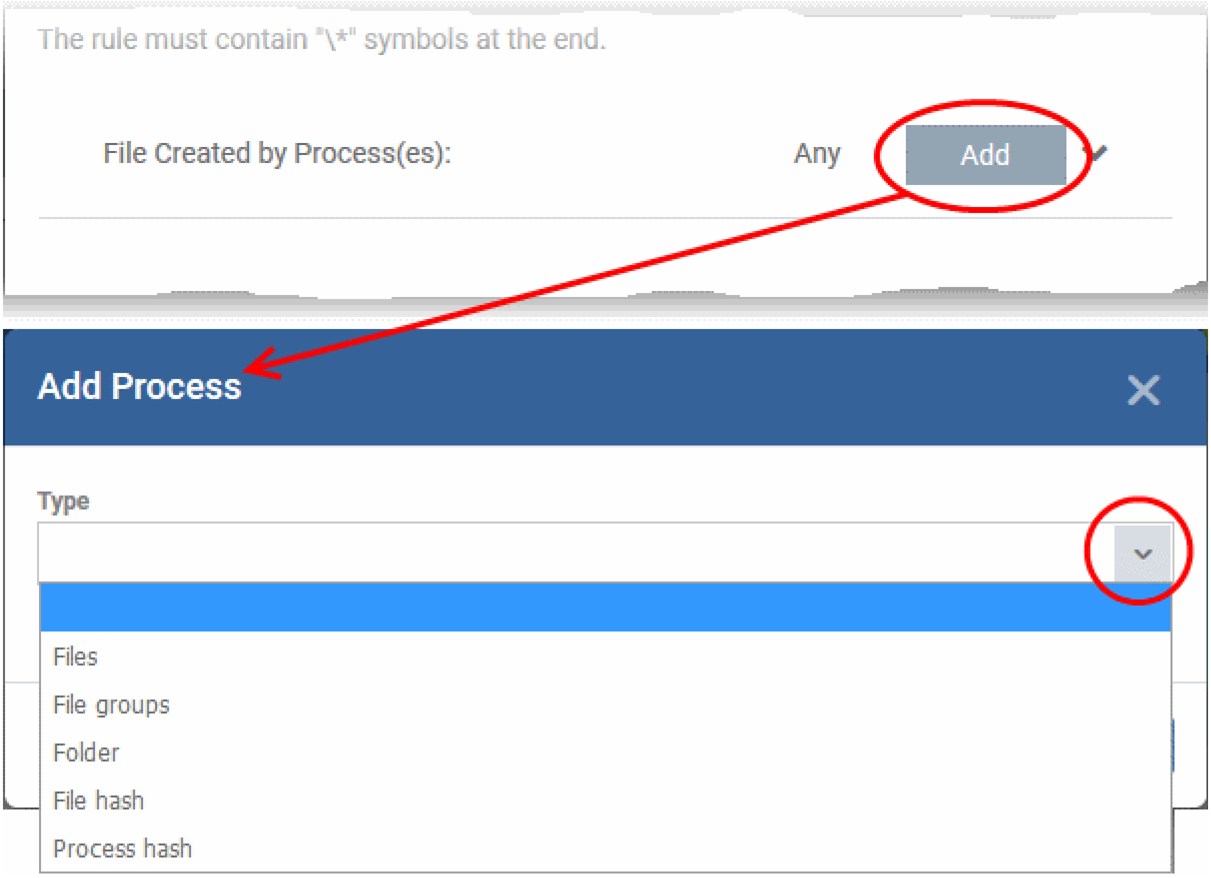
Configure the Filter Criteria and File Rating

You can set the filter criteria, so that the auto-containment action will be applied only to those items that meet the criteria, from the set of items contained in the target. The available filter criteria are:

- Process(es) that created the file
- User(s) that created the file
- The origin from which the file was downloaded
- The file rating
- The age of the file

To select the source process(es) to auto-contain the files created by them

- Click the 'Add' button in the 'File Created by Process(es)' stripe.


The rule must contain "*" symbols at the end.
File Created by Process(es):
Any
Add
Add Process
Type
Files
File groups
Folder
File hash
Process hash

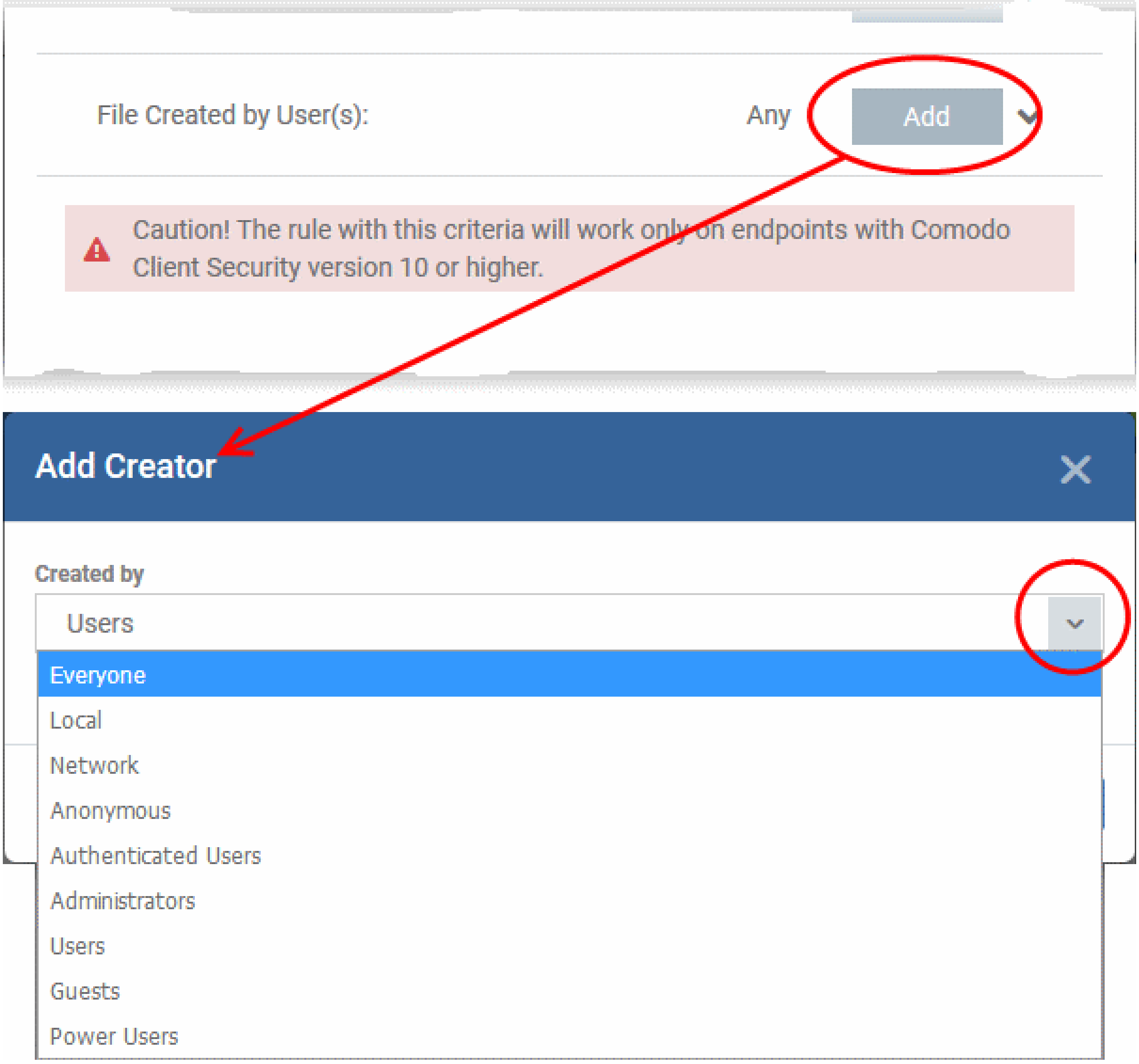
The 'Add Process' dialog will appear.

The options available from the 'Type' drop-down are same as those available under the 'Type' drop-down for specifying the target under the General tab. Refer to the explanations of available **target types** above for more details.

- Repeat the process to add more source processes
- To edit the source process items in the list, click the 'Edit' at the right of the item
- To remove an item, click 'Delete' at the right of the item

To select the user(s) to auto-contain the files created by them

- Click the 'Add' button in the 'File Created by User(s)' stripe.



File Created by User(s): Any Add

Caution! The rule with this criteria will work only on endpoints with Comodo Client Security version 10 or higher.

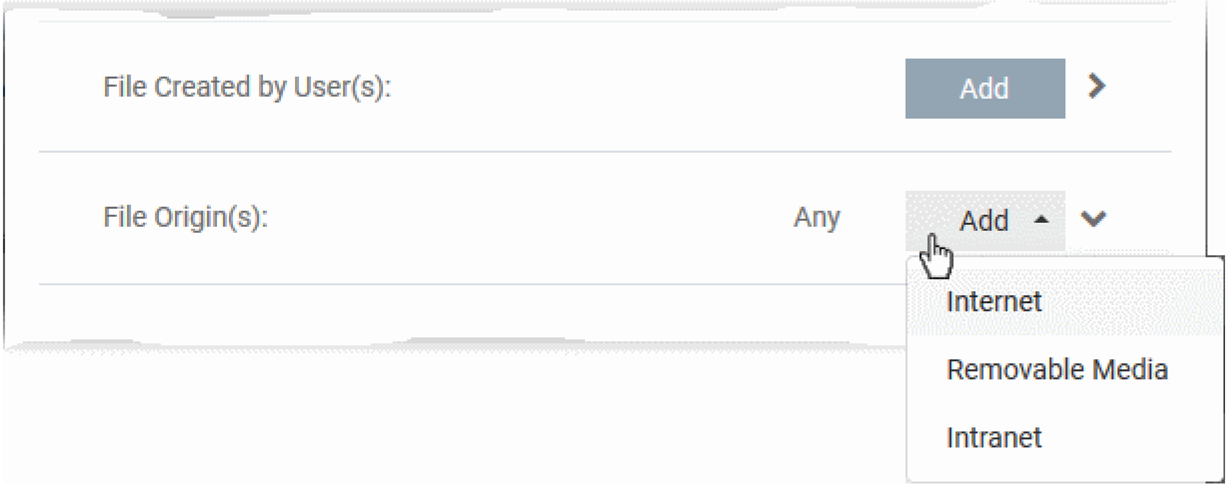
- The 'Add Creator' dialog will appear.
- Choose the pre-defined user group from the 'Created by' drop-down

The User Group will be added to the list of creators.

- Repeat the process to add mode user groups
- To remove the user group added by mistake or no longer needed in the list, click 'X' at the right end of the user name.

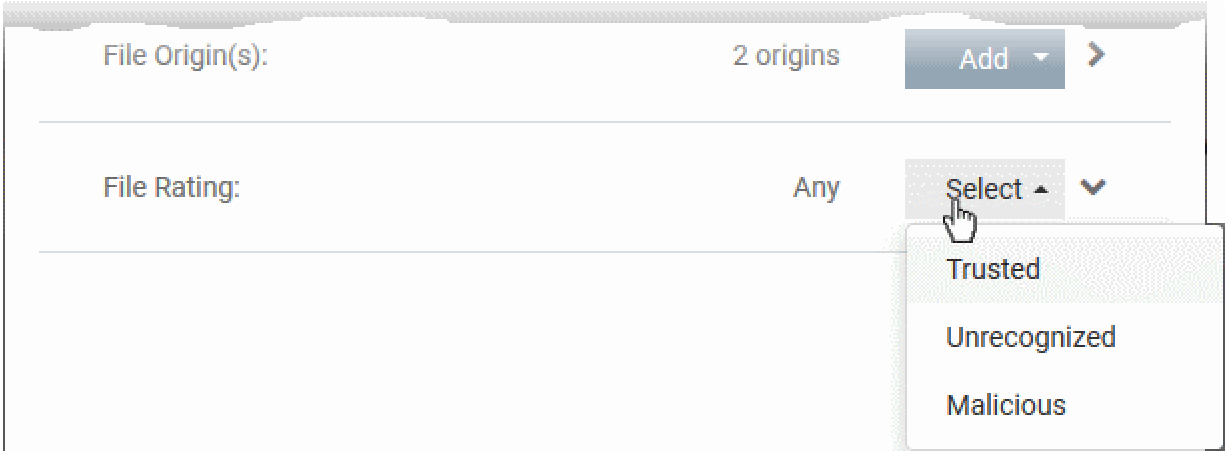
To select the sources(s) from which the file was downloaded/copied to the computer

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:



- **Internet** - The rule will only apply to files that were downloaded from the internet.
- **Removable Media** - The rule will apply only to items copied to the computer from removable storage devices like a USB drive, CD/DVD or portable hard disk drive
- **Intranet** - The rule will only apply to files that were downloaded from the local intranet.

- Repeat the process to add more sources
- To remove a source added by mistake or no longer needed in the list, click 'X' at the right end of the item
- To select the file rating as filter criteria
  - Click the 'Select' button in the 'File Rating' stripe

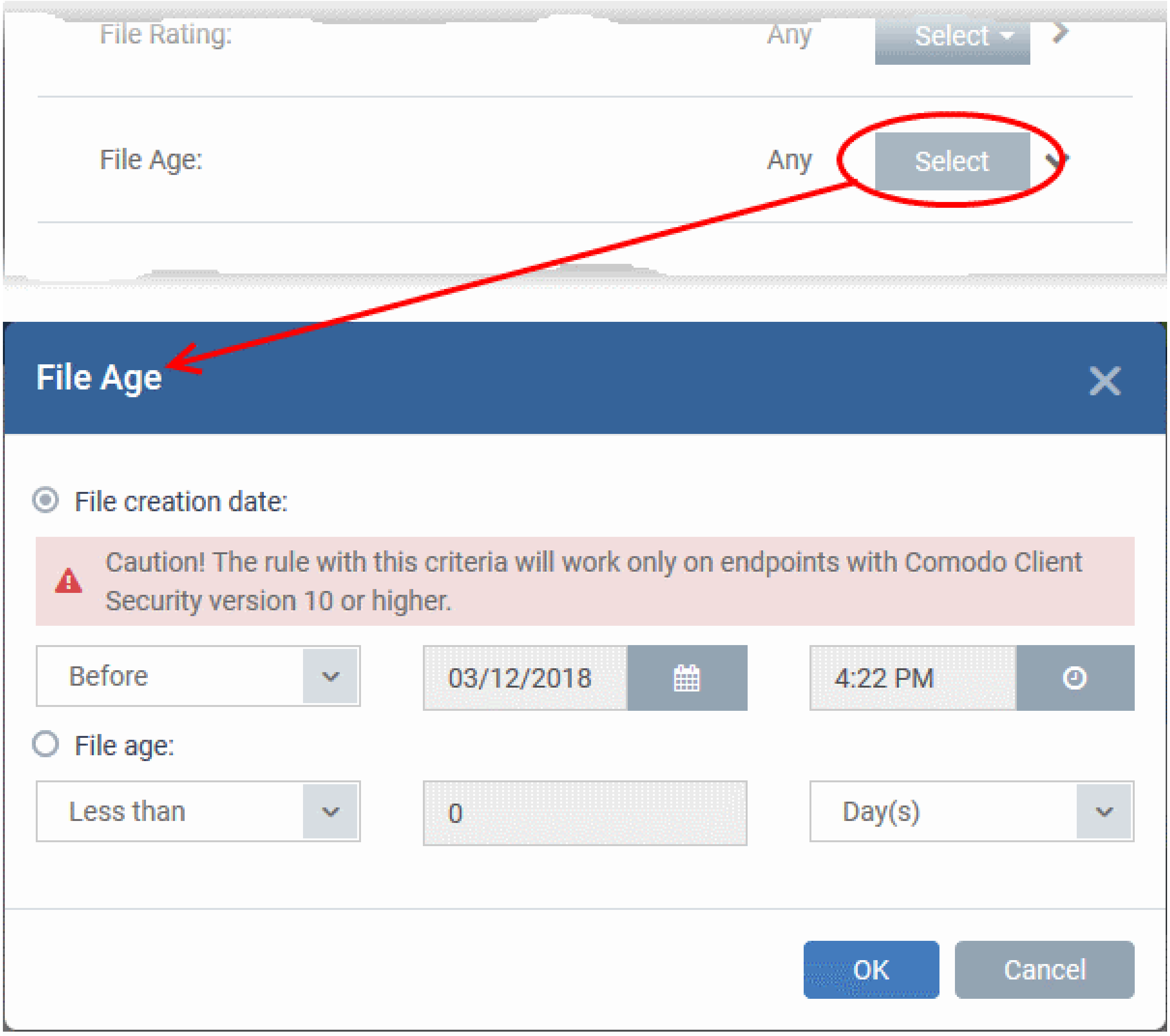


- Choose the source from the options:
- **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files as configured under File Rating configuration of the profile. Refer to the section explaining **File Rating configuration**.
- **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files.
- **Malicious** - Files are scanned according to a set procedure and categorized as malware.

- Repeat the process to add more file ratings
- To remove a rating added by mistake or no longer needed in the list, click 'X' at the right end of the item

To set the file age as filter criteria

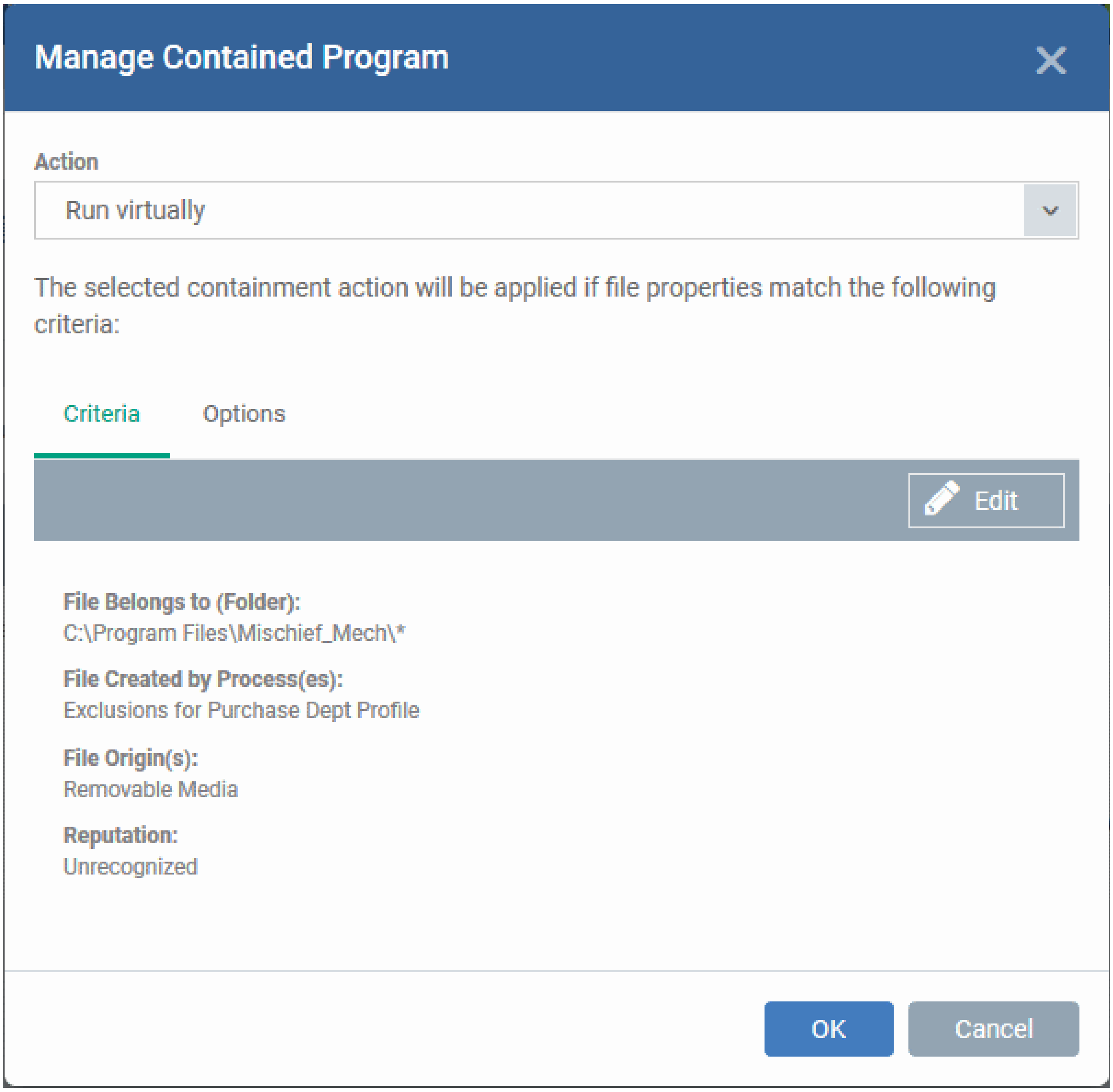
- Click the 'Select' button in the 'File age' stripe.



The 'File Age' dialog will appear. You can set the file age in two ways:

- **File Creation Date** - To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age** - To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than** - Include files whose age is less than the specified time period. Specify the time period using the two fields.
  - **More Than** - Include files whose age is greater than the specified time period. Specify the time period using the two fields.

- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

File Belongs to (Folder):
C:\Program Files\Mischief_Mech\*

File Created by Process(es):
Exclusions for Purchase Dept Profile

File Origin(s):
Removable Media

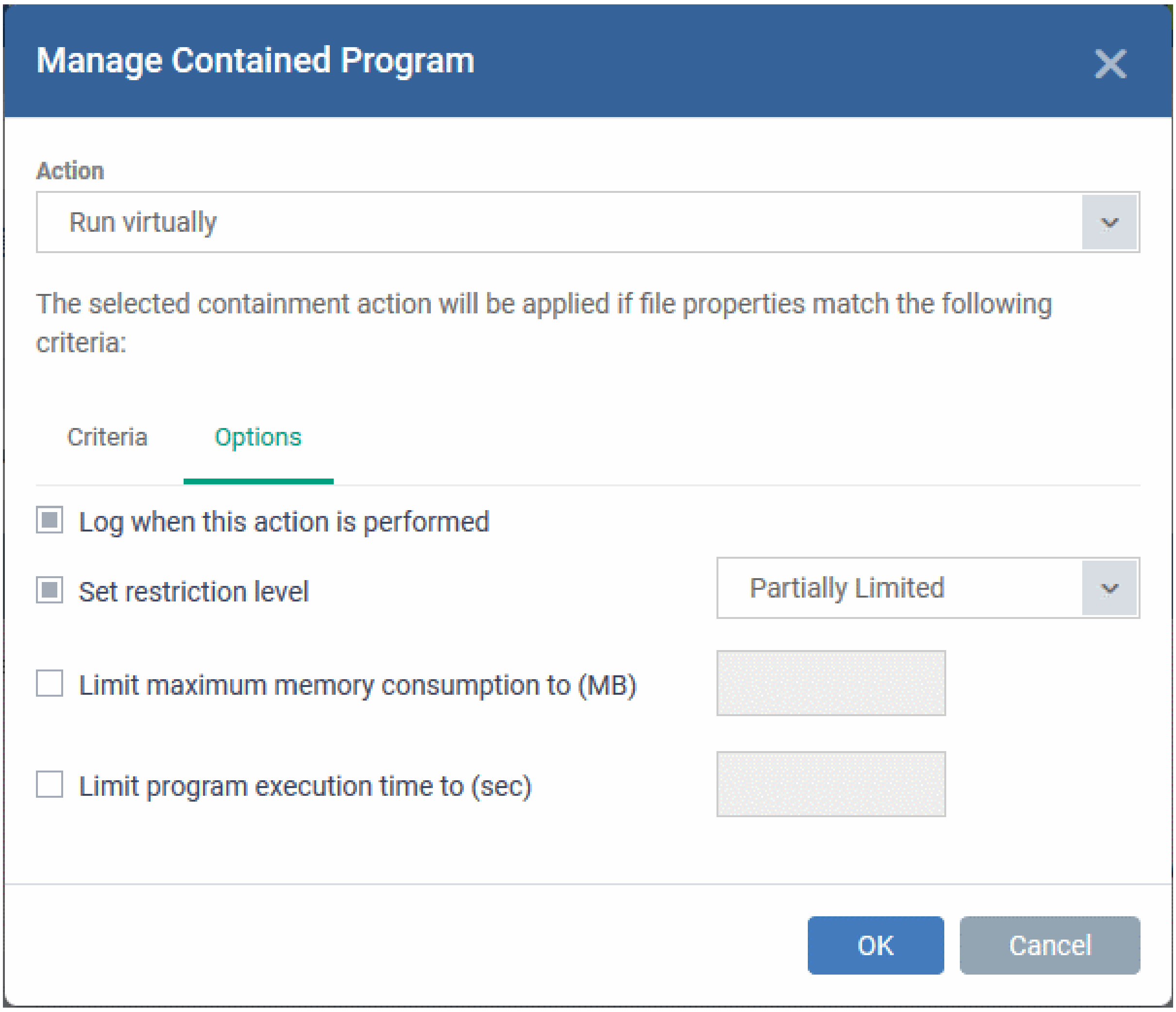
Reputation:
Unrecognized

Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

To select the options

- Click the 'Options' tab.



Manage Contained Program

Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

☑ Log when this action is performed

☑ Set restriction level: Partially Limited

☐ Limit maximum memory consumption to (MB)

☐ Limit program execution time to (sec)

The options will be displayed, depending on the 'Action' chosen in Step 1.

The options available for '**Ignore**' action are:

- **Log when this action is performed** - Choose whether or not to add the event to the CCS logs at the endpoint, whenever this rule is triggered.
- **Don't apply the selected action to child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CCS treats all the child processes as individual processes and forces them to run as per the file rating and the Containment rules.
  - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
  - If this option is selected, then the 'Ignore' rule will be applied only for the target application and all the child processes initiated by it will be checked and Containment rules individually applied as per their file rating.

The options available for '**Run Restricted**' and '**Run Virtually**' actions are:

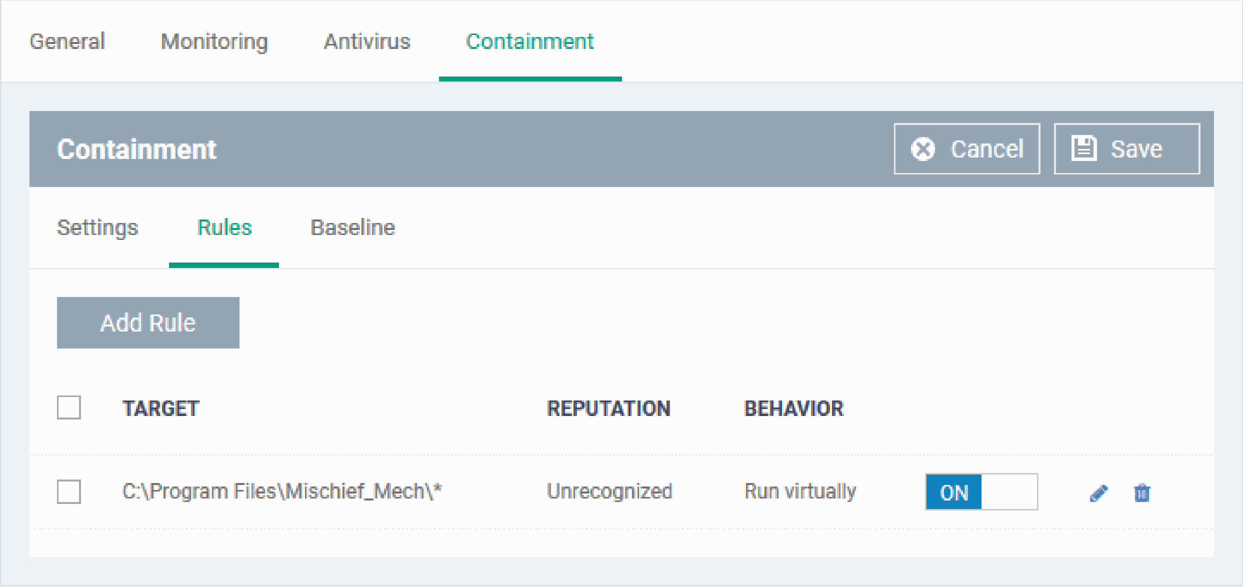
- **Log when this action is performed** - Choose whether or not to add the event to the CCS logs at the endpoint, whenever this rule is triggered.
- **Set Restriction Level** - When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked.
- You can select the '**Restriction Level**' from the following options:
- **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.(Default)

- **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** - Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** - Choose whether or not you wish to specify an upper limit for the time for which the target application can continuously be run.
  - If selected, 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.

The options available for '**Blocked**' action are:

- **Log when this action is performed** - Choose whether or not to add the event to the CCS logs at the endpoint, whenever this rule is triggered.
- **Quarantine program** - If selected, the applications satisfying the rule will be automatically quarantined. See **View and Manage Quarantined Items on Windows Devices** for more information.
- Choose the options and click 'OK' to save them for the rule. The rule will be added and displayed in the list.



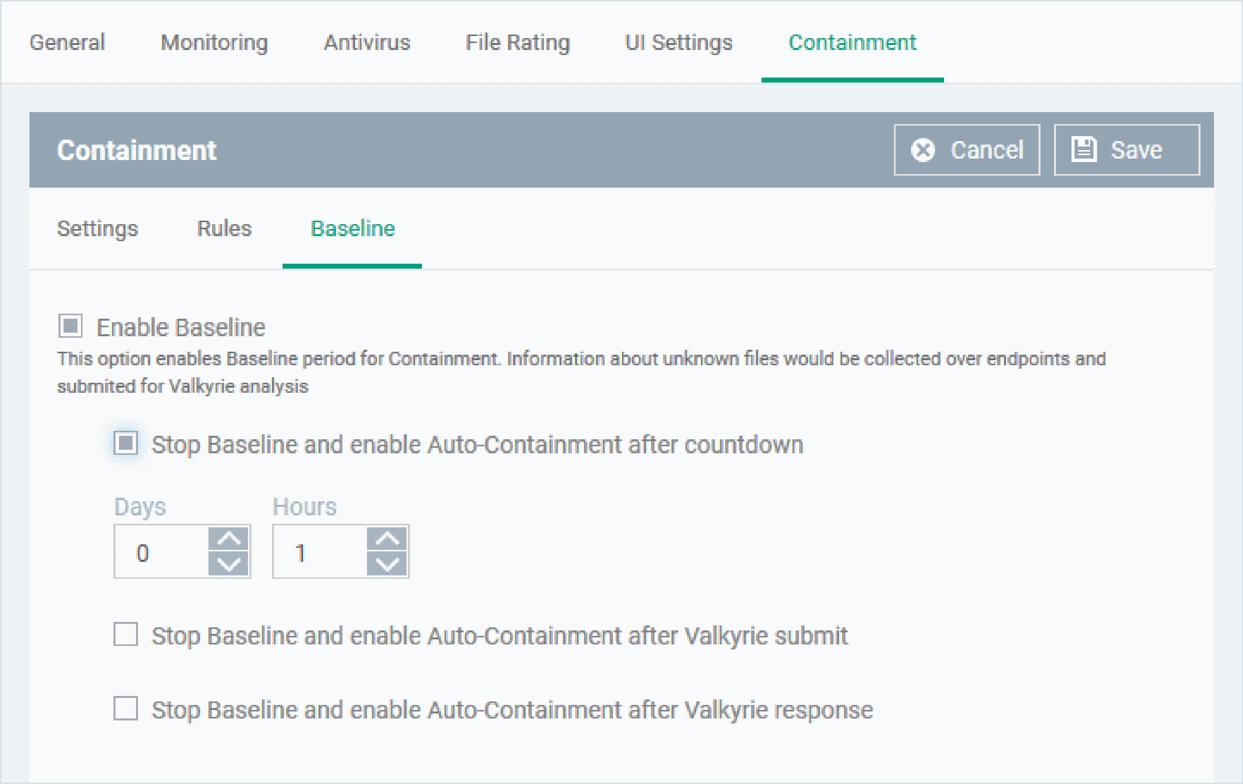
☐	TARGET	REPUTATION	BEHAVIOR		
☐	C:\Program Files\Mischief_Mech\*	Unrecognized	Run virtually	ON	

- Repeat the process to add more rules
- You can move the rule up or down depending on the priority to be given to it, with respect to the other rules.
- You can edit or remove rules at any time using the options at the right.

Baseline Settings

- 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.



☒ Enable Baseline

This option enables Baseline period for Containment. Information about unknown files would be collected over endpoints and submited for Valkyrie analysis

☒ Stop Baseline and enable Auto-Containment after countdown

Days 0 Hours 1

☐ Stop Baseline and enable Auto-Containment after Valkyrie submit

☐ Stop Baseline and enable Auto-Containment after Valkyrie response

Baseline Settings - Table of Parameters	
Form Element	**Description**
Enable Baseline	Enables you to choose one of the three options underneath. (***Default = Disabled***)
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 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. (***Default = Disabled***)
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. (***Default = Disabled***)
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. (***Default = Disabled***)

- 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.

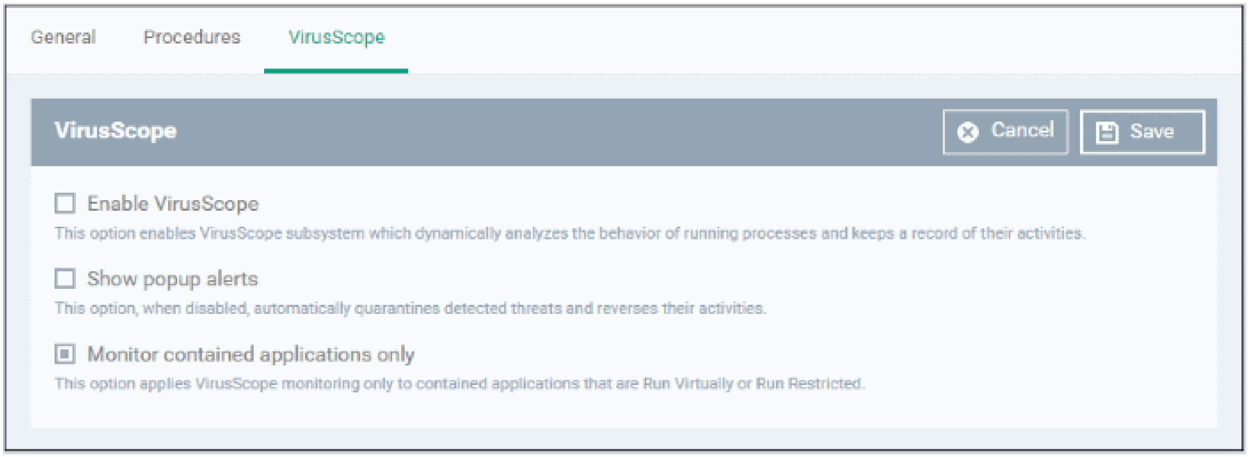
VirusScope alerts give the end-user, the opportunity to quarantine the process & reverse its changes or to let the process go ahead.

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.



☐ Enable VirusScope

This option enables VirusScope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

☐ Show popup alerts

This option, when disabled, automatically quarantines detected threats and reverses their activities.

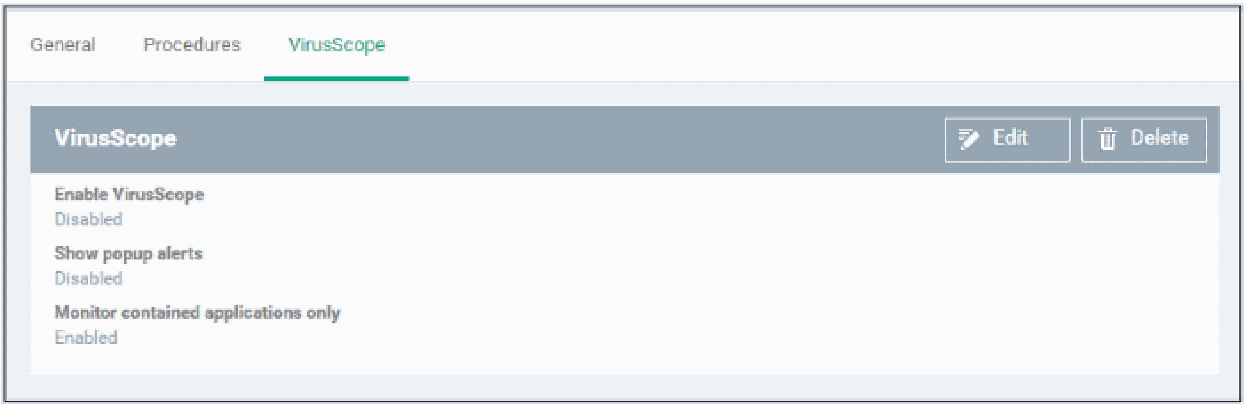
▣ Monitor contained applications only

This option applies VirusScope monitoring only to contained applications that are Run Virtually or Run Restricted.

VirusScope Configuration - Table of Parameters	
Form Element	**Description**
Enable Viruscope	Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities 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.



VirusScope

Enable VirusScope
Disabled

Show popup alerts
Disabled

Monitor contained applications only
Enabled

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**.

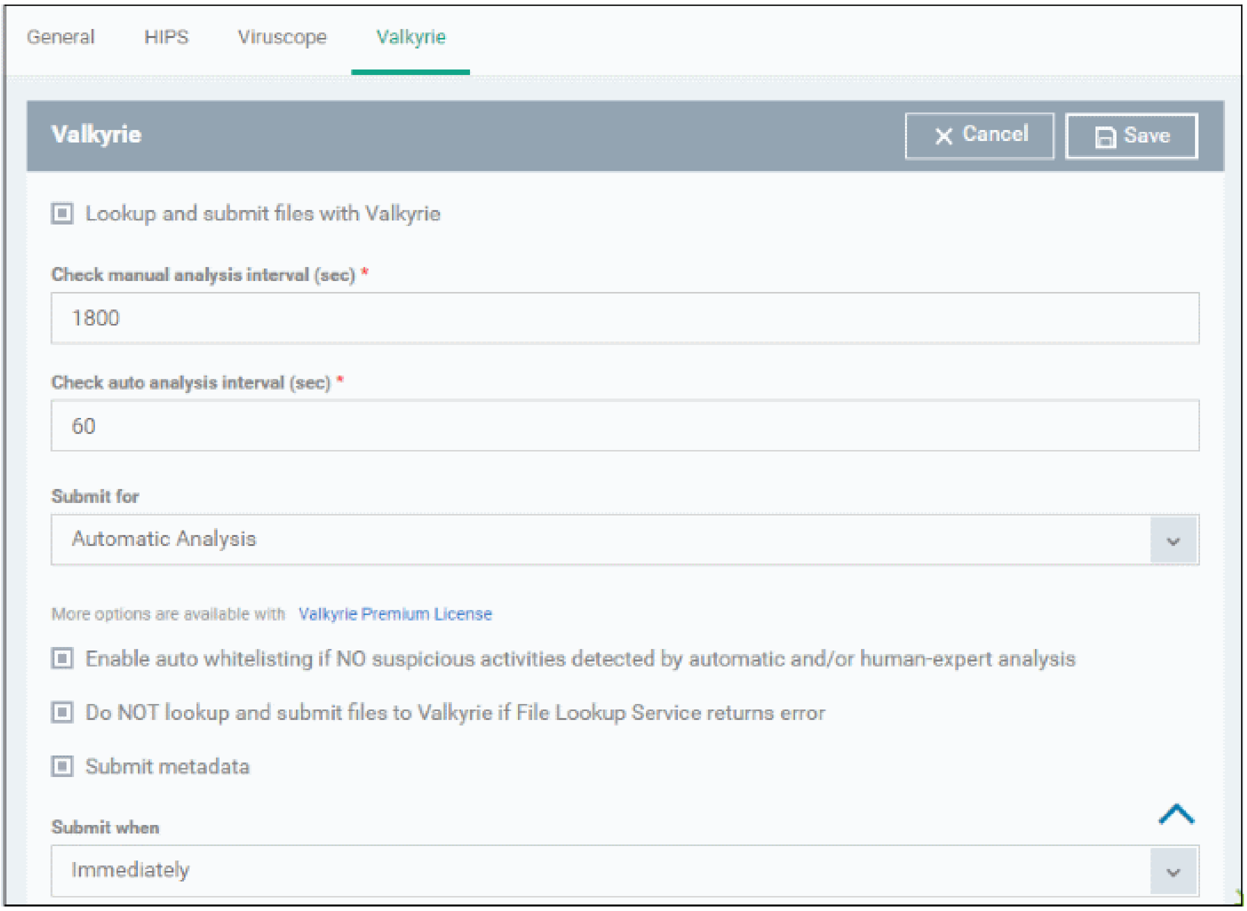
Note: The version of Valkyrie that comes with the free version of ITSM is limited to the online testing service. The Premium version of ITSM also includes manual testing of files by Comodo research labs, helping enterprises quickly create definitive whitelists of trusted files. Valkyrie is also available 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.



☐ Lookup and submit files with Valkyrie

Check manual analysis interval (sec) *
1800

Check auto analysis interval (sec) *
60

Submit for
Automatic Analysis

More options are available with Valkyrie Premium License

☐ Enable auto whitelisting if NO suspicious activities detected by automatic and/or human-expert analysis

☐ Do NOT lookup and submit files to Valkyrie if File Lookup Service returns error

☐ Submit metadata

Submit when
Immediately

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.

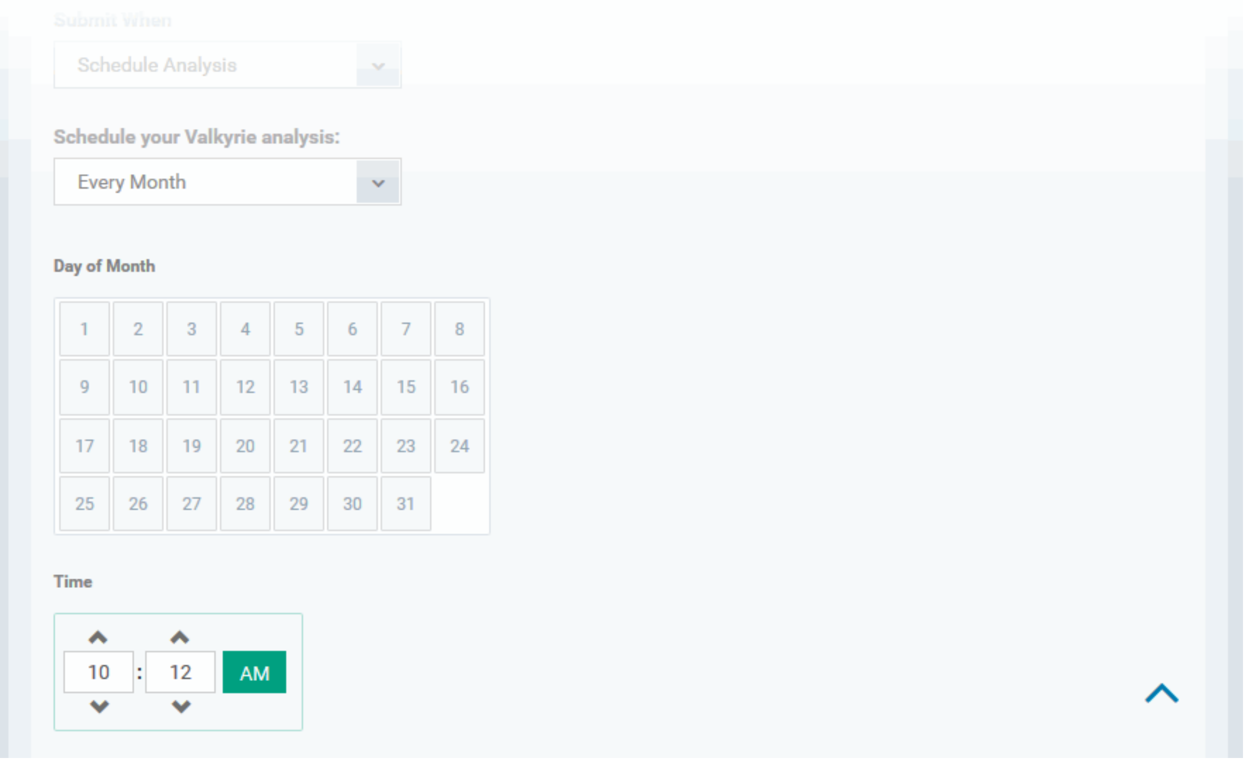
Fields marked * are mandatory.

- 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.



Submit When: Schedule Analysis

Schedule your Valkyrie analysis: Every Month

Day of Month

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	

Time: 10 : 12 AM

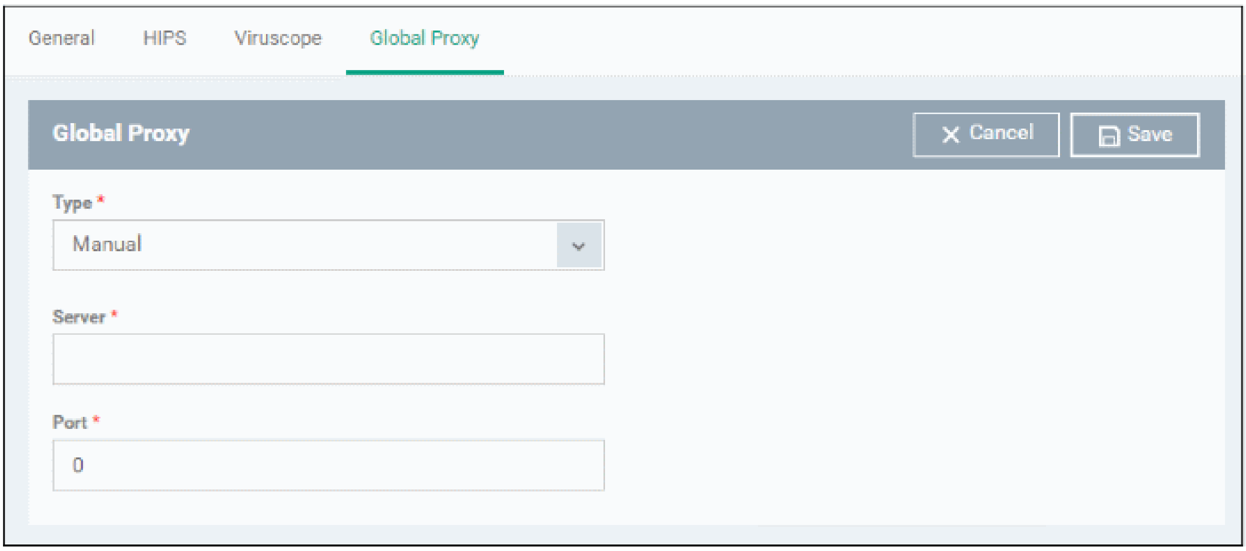
- To upload the unknown files daily choose 'Daily' from the drop-down at the top and set the time for upload in HH:MM format in the combo boxes under 'Time'.
- To upload the unknown files once per week, choose 'Every Week' from the drop-down at the top. Choose the day of the week from the 'Day of Week' 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



Type *: Manual

Server *:

Port *: 0

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

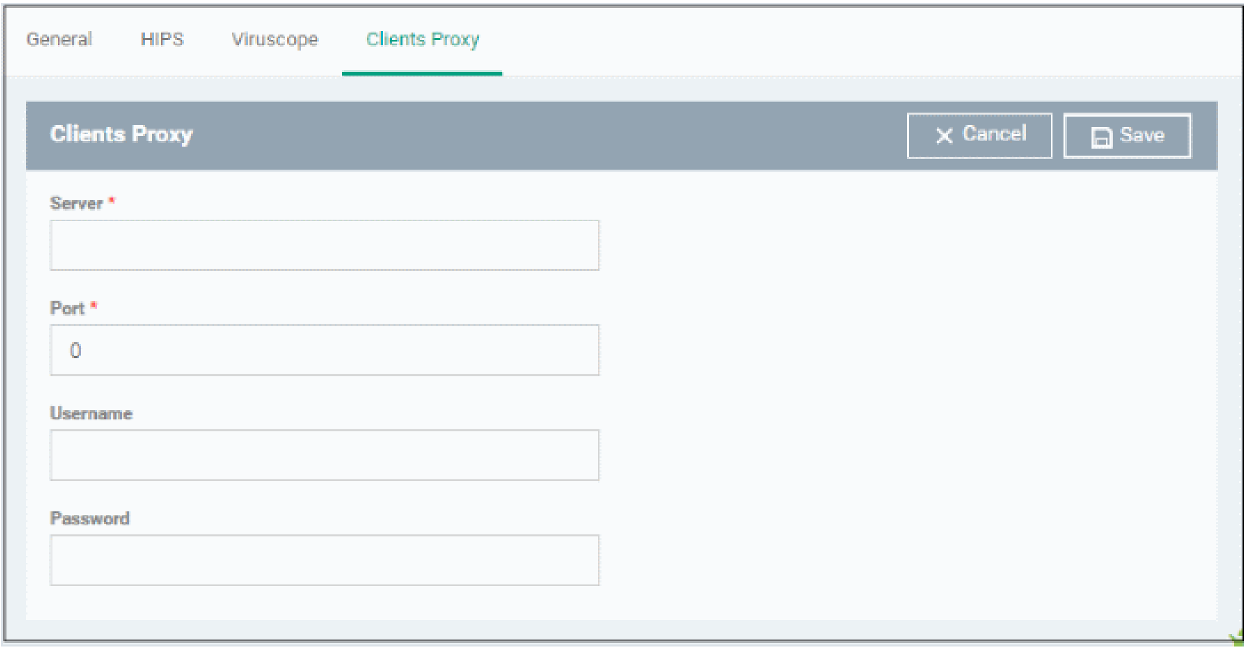
The Clients Proxy settings allows you to specify a proxy server through which Comodo Client Security (CCS) and Comodo Client Communication (CCC) in the endpoints using this profile should connect to ITSM management portal and Comodo servers. If you choose not to set these, then CCS and CCC will connect 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

Server *

Port *
0

Username

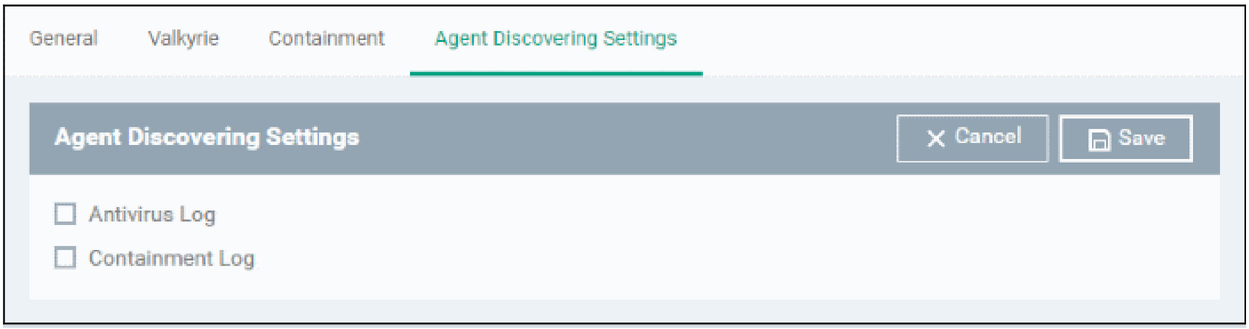
Password

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. CCC and CCS Application UI Settings

- The UI settings screen lets you configure the appearance of Comodo Client Communication (CCC) and Comodo Client Security (CCS).
- You can re-brand CCC and CCS with your own company name, logo, product name and product logo. In addition, you can:
   - Add your support website, phone number and email to the GUI
   - Select which components of CCS should be visible to end-users in the GUI

To configure UI settings

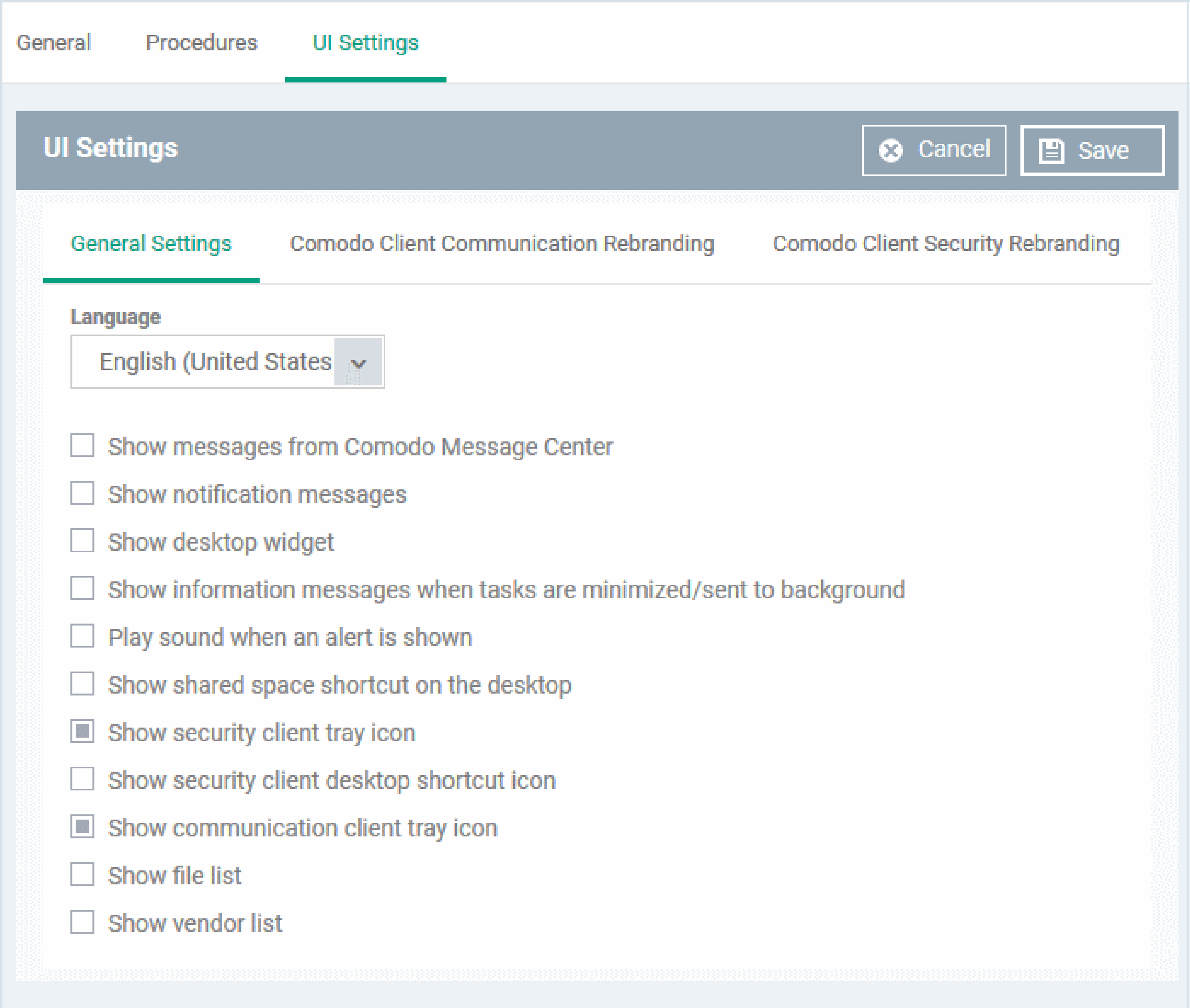
- Click 'Configuration Templates' > 'Profiles'
- Click the Windows profile in which you want to configure UI appearance
- Click 'Add Profile Section' > 'UI Settings'

The UI settings screen contains three tabs:

- **General Settings** - Select GUI language and which components/shortcuts are shown in the interface to the end-user.
- **Comodo Client Communication Rebranding** - Customize CCC with your own brand name, company logo and more.
- **Comodo Client Security Rebranding** - Customize CCS with your own brand name, company logo and more.

General Settings

'General Settings' lets you select interface language and which components/shortcuts are shown on the CCS interface at the endpoint.


General
Procedures
UI Settings
UI Settings
Cancel
Save
General Settings
Comodo Client Communication Rebranding
Comodo Client Security Rebranding

Language: English (United States

- □ Show messages from Comodo Message Center
- □ Show notification messages
- □ Show desktop widget
- □ Show information messages when tasks are minimized/sent to background
- □ Play sound when an alert is shown
- □ Show shared space shortcut on the desktop
- ☑ Show security client tray icon
- □ Show security client desktop shortcut icon
- ☑ Show communication client tray icon
- □ Show file list
- □ Show vendor list

General Settings - Table of Parameters	
Form Element	**Description**
Language	The language which should be used in the Comodo Client Security interface. (***Default = English (United States)***)
Show messages from Comodo Message Center	Message Center notifications appear as pop-ups at the bottom right-hand corner of the screen. They contain news about updates, offers and other items of interest. • Select whether or not the messages should be displayed to end-users.. (***Default = Disabled***)
Show notification messages	Notifications inform end-users about actions and status updates. CCS notices appear in the bottom right hand corner of the screen (just above the tray icons). • Select whether or not notifications should be shown to end-users. (***Default = Disabled***)
Show desktop widget	The widget contains shortcuts to important CCS tasks and information about security levels, traffic and background tasks. • Select whether or not the widget should be shown on endpoint desktops. (***Default = Disabled***)
Show information messages when tasks are minimized/sent to background	These messages inform end-users of the effects of minimizing or moving a running task to the background. For example, when a virus scan task is moved to the background. • Select whether or not information messages should be displayed to end-users. (***Default = Disabled***)
Play sound when an alert is shown	If selected, CCS plays a chime whenever it raises a security alert. (***Default = Disabled***)
Show Shared Space shortcut on the desktop	'Shared Space' is the special folder on an endpoint where contained applications are allowed to save files. The shared space shortcut provides access to this folder. • Select whether or not the shortcut should be shown to end-users. (***Default = Disabled***)
Show security client tray icon	Select whether or not the CCS icon should be shown in the system tray. (***Default = Enabled***)
Show security client desktop shortcut icon	Select whether or not the CCS desktop shortcut should be displayed. (***Default = Disabled***)
Show communication client tray icon	Select whether or not the CCC application shortcut icon should be

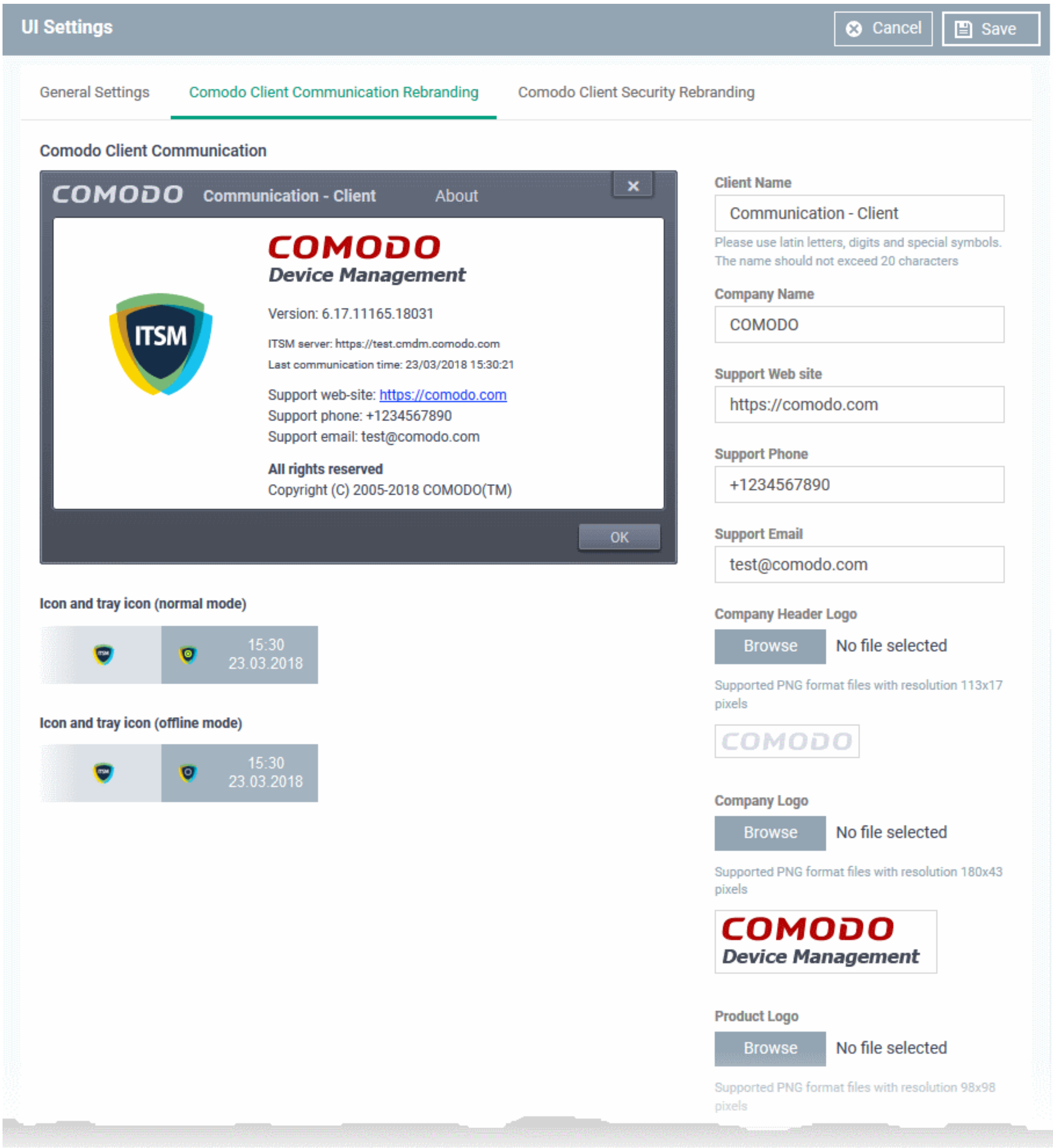
General Settings - Table of Parameters	
	available in the system tray. (***Default = Enabled***)
Show file list	CCS can show a list of files on a device along with their trust ratings ('Trusted', 'Unrecognized' or 'Malicious'). This is available in 'Advanced Settings' > 'Security Settings' > 'File Rating' > 'File List'. For more details click the link **https://help.comodo.com/topic-399-1-790-10397-File-List.html**. • Select whether or not the file list should be available to end-users. (***Default = Disabled)***
Show vendor list	CCS can show a list of list of trusted vendors in 'Advanced Settings' > 'Security Settings' > 'File Rating' > 'Trusted Vendors List'. Files published by vendors in the list are automatically trusted and skipped during antivirus scans. • Select whether or not the vendor list should be available to end-users. For more details click the link **https://help.comodo.com/topic-399-1-790-10401-Trusted-Vendors-List.html** (***Default = Disabled***)

- Click 'Save' to apply your changes to the profile.

Comodo Client Communication Rebranding

The rebranding tab lets you change the appearance and interface texts of Comodo Client Communication. This is especially useful for customers who wish to white-label the CCC interface for their clients.

- You can change the company name, support website, phone number and email.
- You can upload replacement images for company logo, header logo, product icons and product logo.
- The online editor lets you preview your changes in real-time.



UI Settings

Cancel | Save

General Settings | Comodo Client Communication Rebranding | Comodo Client Security Rebranding

Comodo Client Communication

COMODO Communication - Client About

COMODO Device Management

Version: 6.17.11165.18031

ITSM server: https://test.cmdm.comodo.com

Last communication time: 23/03/2018 15:30:21

Support web-site: https://comodo.com

Support phone: +1234567890

Support email: test@comodo.com

All rights reserved

Copyright (C) 2005-2018 COMODO(TM)

OK

Icon and tray icon (normal mode)

15:30 23.03.2018

Icon and tray icon (offline mode)

15:30 23.03.2018

Client Name: Communication - Client

Please use latin letters, digits and special symbols. The name should not exceed 20 characters

Company Name: COMODO

Support Web site: https://comodo.com

Support Phone: +1234567890

Support Email: test@comodo.com

Company Header Logo: Browse No file selected

Supported PNG format files with resolution 113x17 pixels

Company Logo: Browse No file selected

Supported PNG format files with resolution 180x43 pixels

Product Logo: Browse No file selected

Supported PNG format files with resolution 98x98 pixels

- Start typing in the fields to see your changes reflected in the example image.
- Make sure all images you upload are the correct size and file format (.png)

Comodo Client Communication Rebranding - Table of Parameters	
Form Element	**Description**

Comodo Client Communication Rebranding - Table of Parameters	
Client Name	Enter a custom name for the application. You can use alphabetical, numeral and special characters. Maximum = 20 characters.

Comodo Client Communication Rebranding - Table of Parameters	
Company Name	Your company name.

Comodo Client Communication Rebranding - Table of Parameters	
Support Website	The URL of your support website. The URL will be shown in the 'About' dialog of the CCC application.

Comodo Client Communication Rebranding - Table of Parameters	
Support Phone	Your customer support phone number. This number will be shown in the 'About' dialog of the CCC application.

Comodo Client Communication Rebranding - Table of Parameters	
Support Email	Your customer support email address. This address will be shown in the 'About' dialog.of the CCC application

Comodo Client Communication Rebranding - Table of Parameters	
Company Header Logo	Logo shown at the top-left corner of the application window. Accepted image size = 113 x 17 pixels Accepted image file format = .png

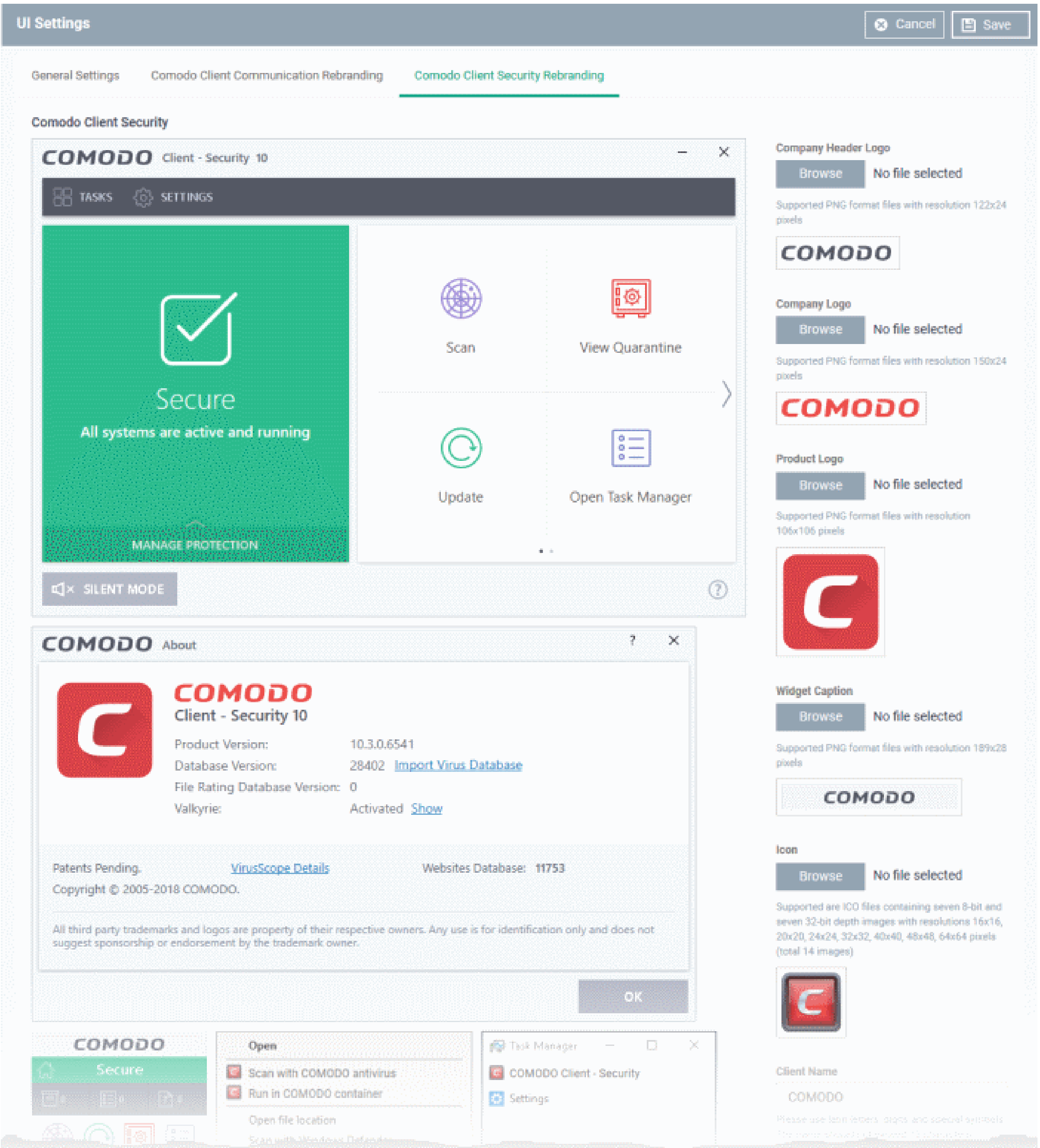
Comodo Client Communication Rebranding - Table of Parameters	
Company Logo	Logo shown at the top of the CCC 'About' dialog. Accepted image size = 180 x 43 pixels Accepted image file format = .png

Comodo Client Communication Rebranding - Table of Parameters	
Product Logo	Logo shown at the left of the CCC 'About' dialog. Accepted image size = 98 x 98 pixels Accepted image file format = .png

Comodo Client Communication Rebranding - Table of Parameters	
Icon	Windows start menu and shortcut icon. Accepted image sizes = 16 x 16, 20 x 20, 32 x 32, 40 x 40, 48 x 48 and 64 x 64 pixels Accepted image file format = .png
Tray Icon (normal mode)	Tray icon shown when the agent is connected to ITSM. Accepted image sizes = 16 x 16 pixels Accepted image file format = .png
Tray Icon (offline mode)	Tray icon shown when the agent is not connected to ITSM. Accepted image sizes = 16 x 16 pixels Accepted image file format = .png

- Click 'Save' to apply your new design to the profile.

Comodo Client Security Rebranding



Product Version: 10.3.0.6541

Database Version: 28402 Import Virus Database

File Rating Database Version: 0

Valkyrie: Activated Show

Patents Pending. VirusScope Details Websites Database: 11753

Copyright © 2005-2018 COMODO.

All third party trademarks and logos are property of their respective owners. Any use is for identification only and does not suggest sponsorship or endorsement by the trademark owner.

Company Header Logo

Browse No file selected

Supported PNG format files with resolution 122x24 pixels

Company Logo

Browse No file selected

Supported PNG format files with resolution 150x24 pixels

Product Logo

Browse No file selected

Supported PNG format files with resolution 106x106 pixels

Widget Caption

Browse No file selected

Supported PNG format files with resolution 189x28 pixels

Icon

Browse No file selected

Supported are ICO files containing seven 8-bit and seven 32-bit depth images with resolutions 16x16, 20x20, 24x24, 32x32, 40x40, 48x48, 64x64 pixels (total 14 images)

Client Name

COMODO

Please use latin letters, digits and special symbols

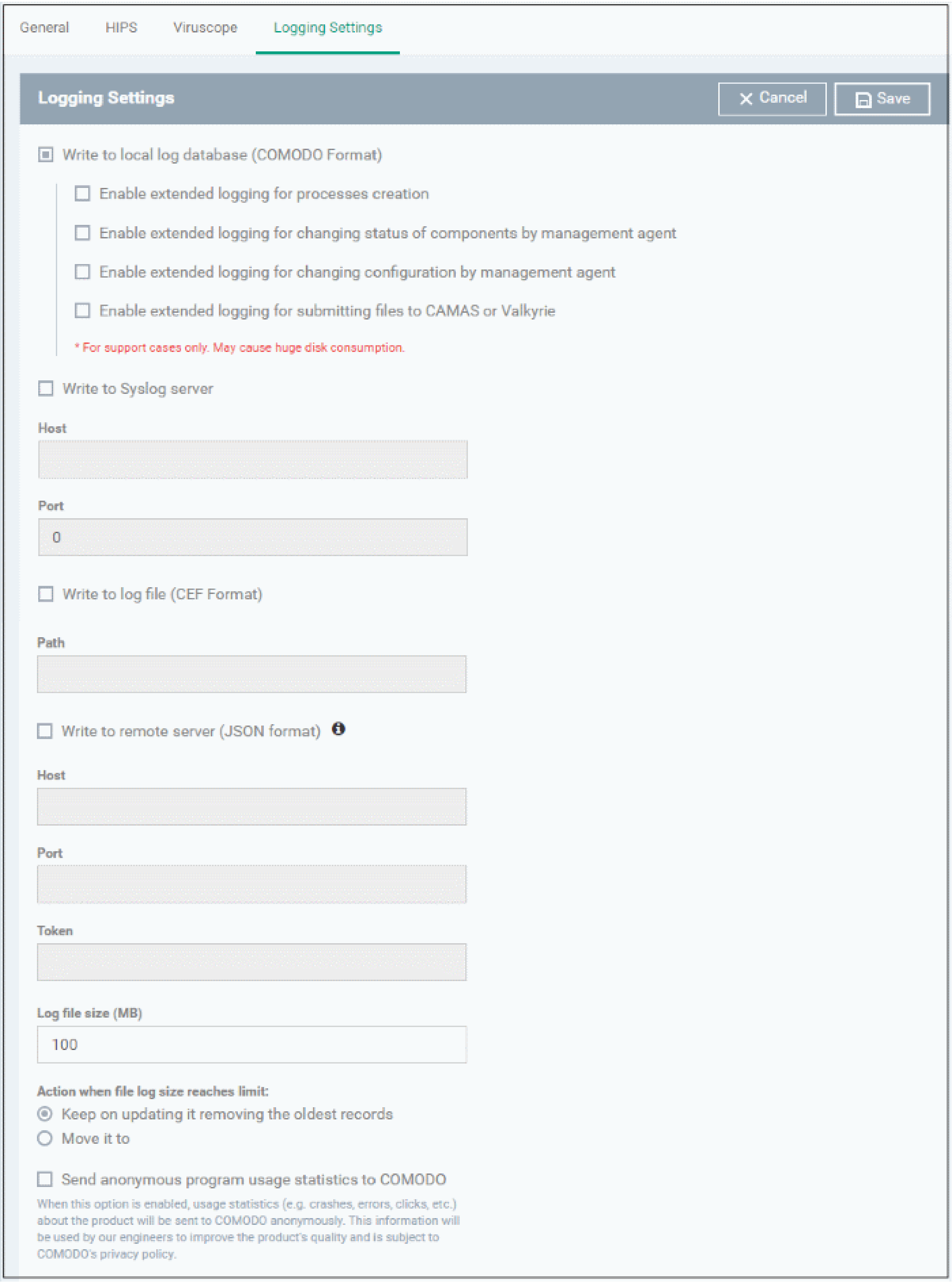
- Start typing in the fields to see your changes reflected in the example images.
- Make sure all images you upload are the correct size and file format (.png)
- The changes you make here will be rolled out to all interfaces in CCS.
- You cannot modify the UI in a default profile.

Comodo Client Communication Rebranding - Table of Parameters	
Form Element	**Description**
Company Header Logo	Logo shown at the top-left corner of the application window. Accepted image size = 122 x 24 pixels Accepted image file format = .png
Company Logo	Logo shown in various CCS interfaces. Accepted image size = 150 x 24 pixels Accepted image file format = .png
Product Logo	Logo shown on the left side of the CCS 'About' dialog. Accepted image size = 106 x 106 pixels Accepted image file format = .png
Widget Caption	Logo shown on the header of the CCS desktop widget. Accepted image size = 189 x 28 pixels Accepted image file format = .png
Icon	Windows start menu and shortcut icon. Also shown in various other interfaces of the application. Accepted image sizes = 16 x 16, 20 x 20, 32 x 32, 40 x 40, 48 x 48 and 64 x 64 pixels Accepted image file format = .png
Client Name	Enter a custom name for the application. This will be shown in the interface and will be used as the product name in the Windows 'Start' menu. You can use letters, numbers and special characters. Maximum = 20 characters.

- Click 'Save' to apply your settings to the profile.
- Click the 'Edit' button if you wish to modify a design that you have saved.

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.



☒ Write to local log database (COMODO Format)

□ Enable extended logging for processes creation

□ Enable extended logging for changing status of components by management agent

□ Enable extended logging for changing configuration by management agent

□ Enable extended logging for submitting files to CAMAS or Valkyrie

* For support cases only. May cause huge disk consumption.

□ Write to Syslog server

Host

Port

0

□ Write to log file (CEF Format)

Path

□ Write to remote server (JSON format)

Host

Port

Token

Log file size (MB)

100

Action when file log size reaches limit:

● Keep on updating it removing the oldest records

○ Move it to

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors, clicks, etc.) about the product will be sent to COMODO anonymously. This information will be used by our engineers to improve the product's quality and is subject to COMODO's privacy policy.

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.
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.

Logging Settings Configuration - Table of Parameters		
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	Radio button	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	Radio button	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	If enabled, ITSM will periodically send program usage and crash data to Comodo for analysis. This data is useful as it helps us quickly identify areas of the program which need to be improved. Disable this option if you do not want to send usage statistics. You privacy is guaranteed as all data is anonymized and sent over a secure and encrypted channel. (Default = 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

Allows you to password-protect access to Comodo Client Security (CCS) and Comodo Client Communication (CCC) on managed endpoints.

Background Note:

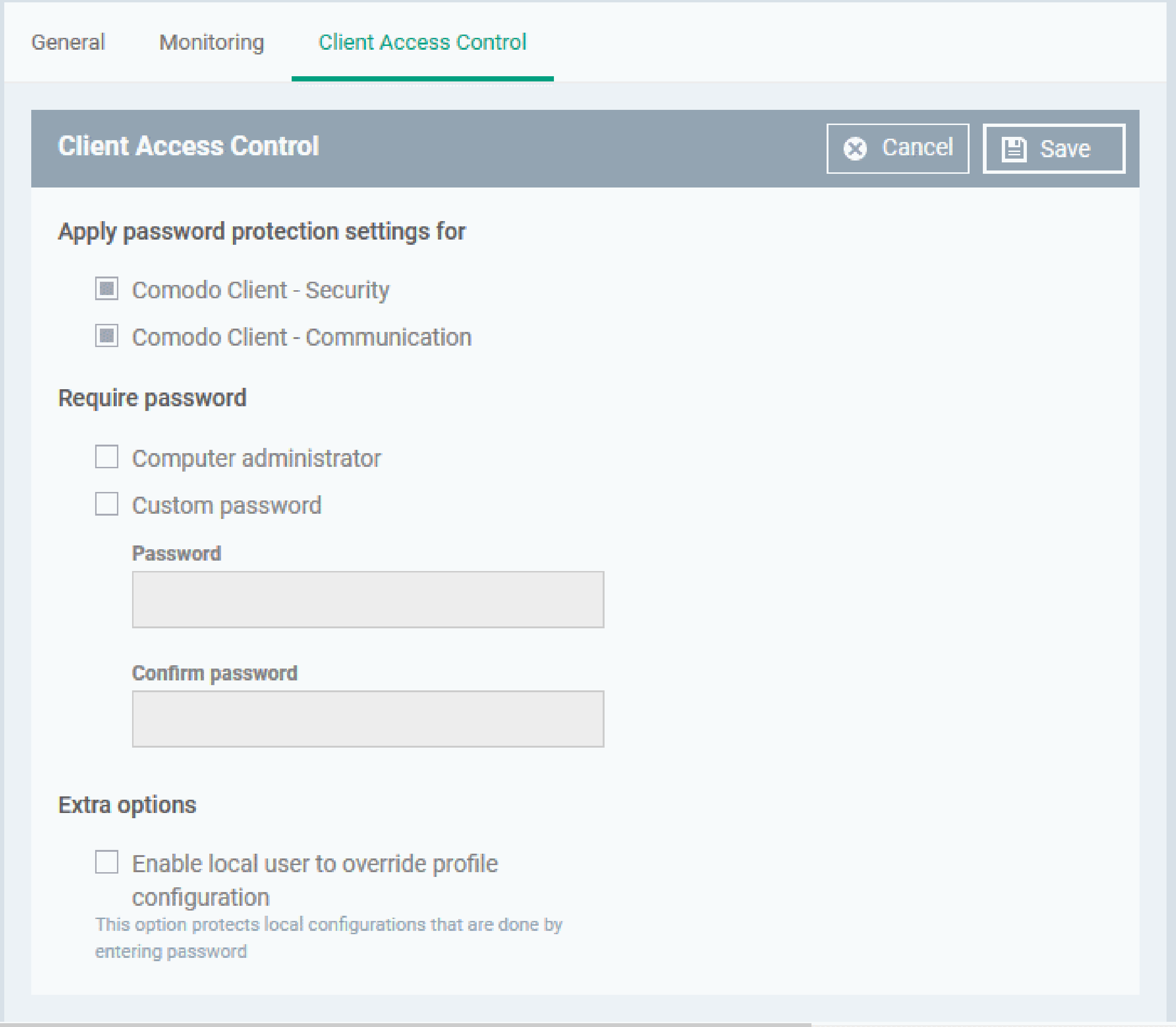
The security configuration of the antivirus, firewall, containment and HIPS modules are managed by their configuration profile(s). However, administrators or end-users are allowed to access the CCS interface locally to configure security settings. This is useful if:

- A custom configuration is required for a specific endpoint
- Administrators can use an endpoint to create a model configuration which can be imported to ITSM as a profile. Refer to **Importing Windows Profiles** for more details.

ITSM periodically checks endpoints to see if the local CCS settings matches with the endpoint's ITSM profile. By default, ITSM will revert any manual changes made. If you want the manual changes not to be overridden, you can configure the 'Client Access Control' section in the profile accordingly.

To configure Client Access Control Settings

- Click 'Client Access Control' from the 'Add Profile Section' drop-down



Apply password protection settings for

☒ Comodo Client - Security

☒ Comodo Client - Communication

Require password

□ Computer administrator

□ Custom password

Password

Confirm password

Extra options

□ Enable local user to override profile configuration

This option protects local configurations that are done by entering password

- 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.
- Extra Options:
  - Enable local user to override profile configuration - If enabled, the manual changes made to the security setting parameters in the local installation of CCS will not be reverted to the settings as per the profile. This is useful if you want to allow the local user to configure CCS as per their wish or use the endpoint to manually configure the security settings of different components of CCS and import it as a profile. See **Importing Windows Profiles** for more details.
- Click 'Save' to apply your changes to the profile.

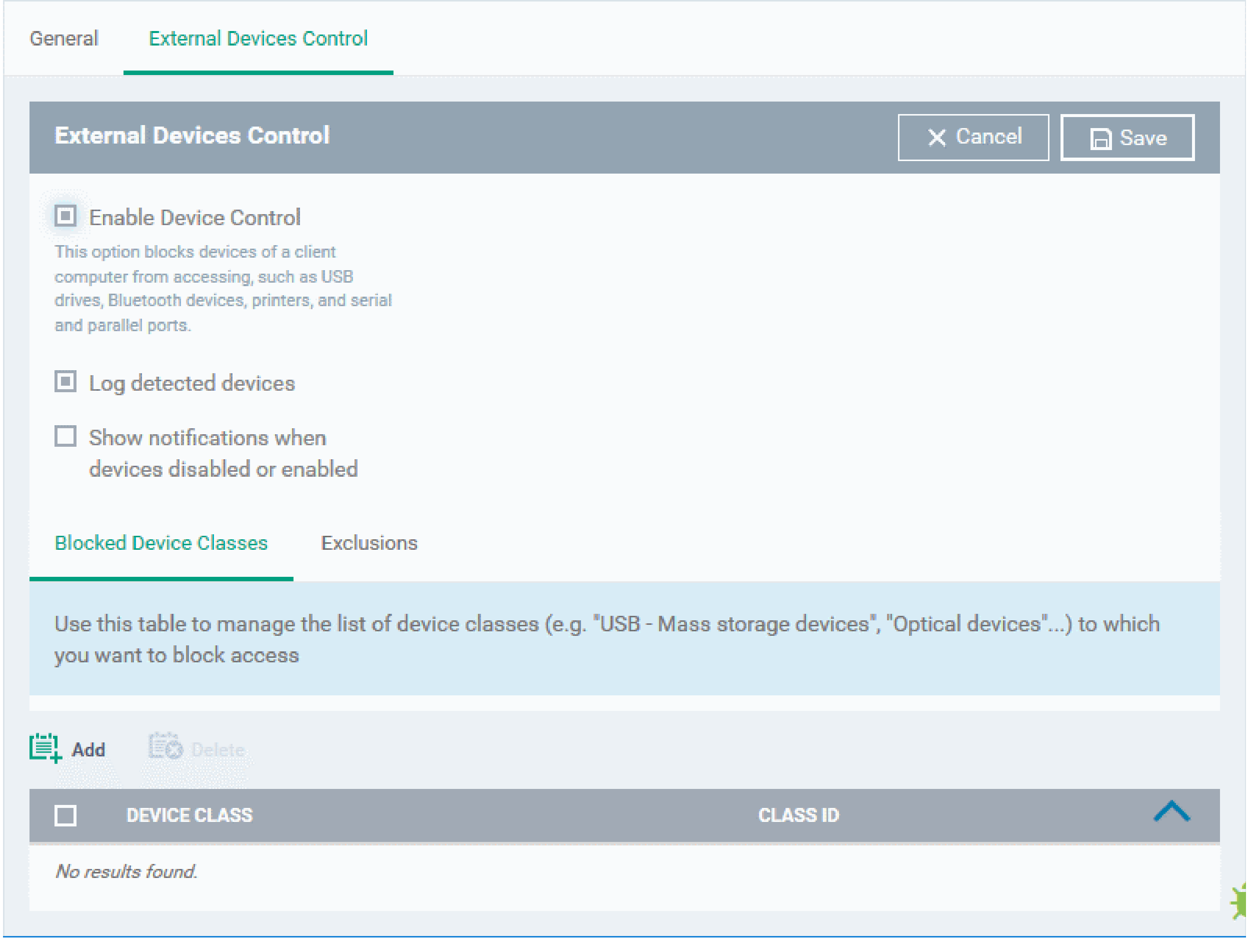
6.1.3.1.15. External Devices Control Settings

External Device Control Settings allows administrators to define a list of devices that should be blocked on endpoints using this profile. For example, you can block access to USB storage devices, human interface devices, Bluetooth devices, infrared devices, IDE ATA/ATAPI controllers. ITSM blocks access to devices connected through both serial and parallel ports and creates a log of their connection activities.

You can create exclusions for external devices which you want to allow to connect to managed endpoints. Devices can be added as exclusion by specifying their Device Ids. You can use wildcard characters in the device ID if you want to include a series of devices with similar device IDs.

To configure External Devices Control Settings

- Click 'Configuration Templates' > 'Profiles' then click the name of the profile to which you want to add the section.
- Click 'Add Profile Section' > 'External Devices Control'



General | External Devices Control

External Devices Control

☒ Enable Device Control

This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

☒ Log detected devices

☐ Show notifications when devices disabled or enabled

Blocked Device Classes | Exclusions

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

☐	DEVICE CLASS	CLASS ID
	No results found.	

The settings screen allows you to configure the general settings and to define lists of blocked device types and exclusions.

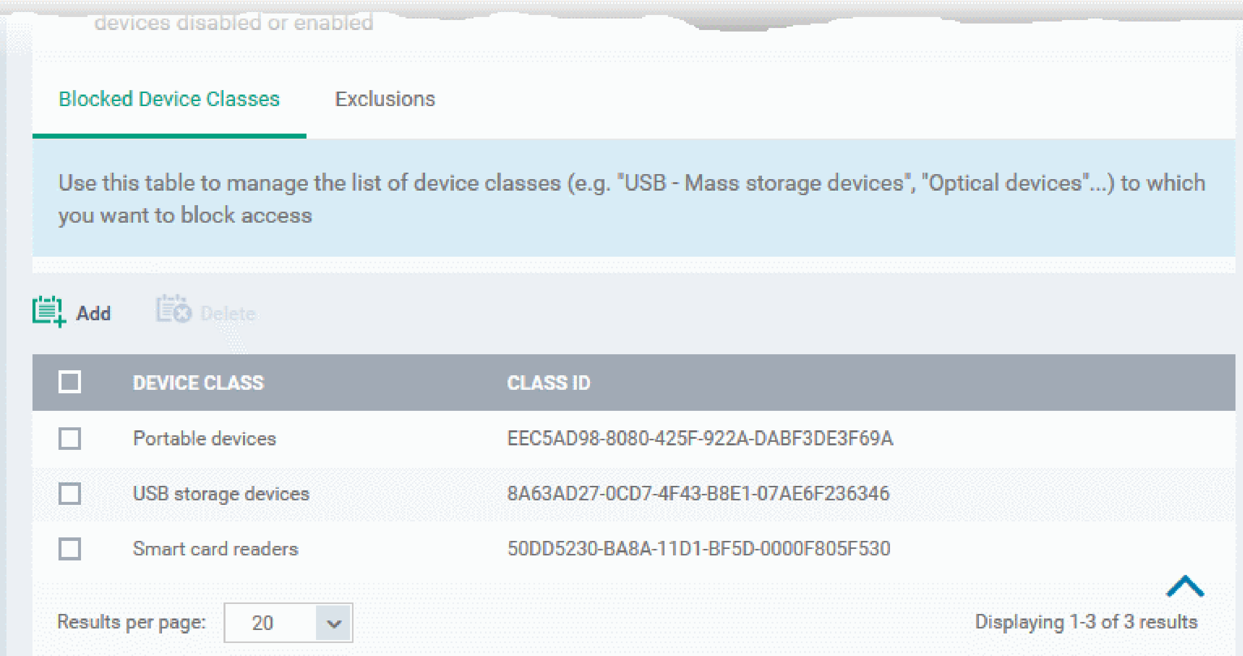
- **Enable Device Control** - Allows you to enable or disable the external device control feature. This is useful if you want to configure external device control settings for a profile during its creation and enable it at a later time
- **Log detected devices** - Allows you to enable or disable logging 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.



devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

□	DEVICE CLASS	CLASS ID
□	Portable devices	EEC5AD98-8080-425F-922A-DABF3DE3F69A
□	USB storage devices	8A63AD27-0CD7-4F43-B8E1-07AE6F236346
□	Smart card readers	50DD5230-BA8A-11D1-BF5D-0000F805F530

Results per page: 20

Displaying 1-3 of 3 results

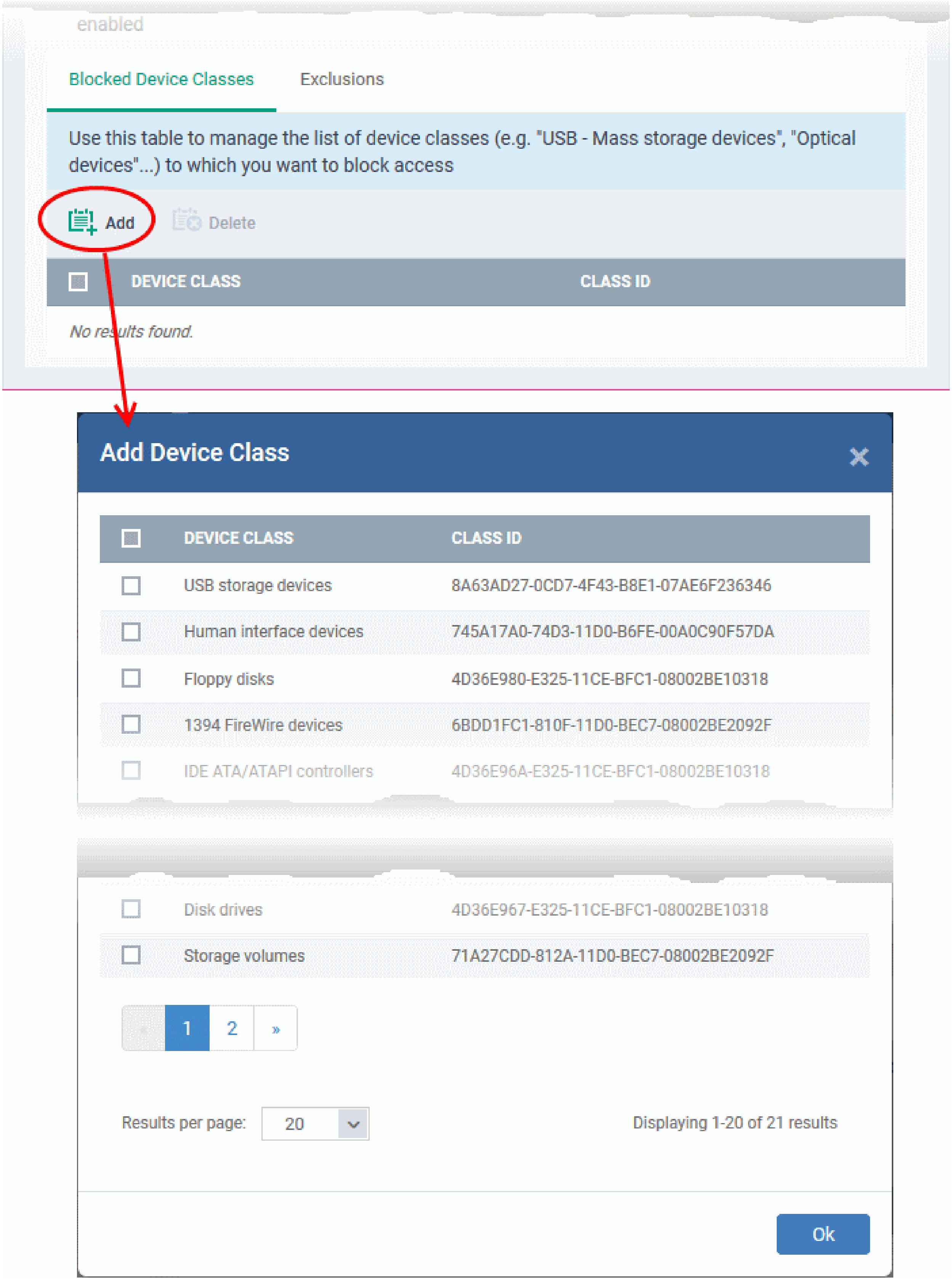
Blocked Device Classes - Column Descriptions	
Column Header	**Description**
Device Class	Displays the device type as per global hardware classification
Class ID	Displays the Globally Unique Identifier (GUID) of the device class

Tip. Block 'Portable Devices' in addition to 'USB storage devices' if you want to stop users connecting their phones to access the phone's memory card

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.



Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

□	DEVICE CLASS	CLASS ID

No results found.

Add Device Class

□	DEVICE CLASS	CLASS ID
□	USB storage devices	8A63AD27-0CD7-4F43-B8E1-07AE6F236346
□	Human interface devices	745A17A0-74D3-11D0-B6FE-00A0C90F57DA
□	Floppy disks	4D36E980-E325-11CE-BFC1-08002BE10318
□	1394 FireWire devices	6BDD1FC1-810F-11D0-BEC7-08002BE2092F
□	IDE ATA/ATAPI controllers	4D36E96A-E325-11CE-BFC1-08002BE10318
□	Disk drives	4D36E967-E325-11CE-BFC1-08002BE10318
□	Storage volumes	71A27CDD-812A-11D0-BEC7-08002BE2092F

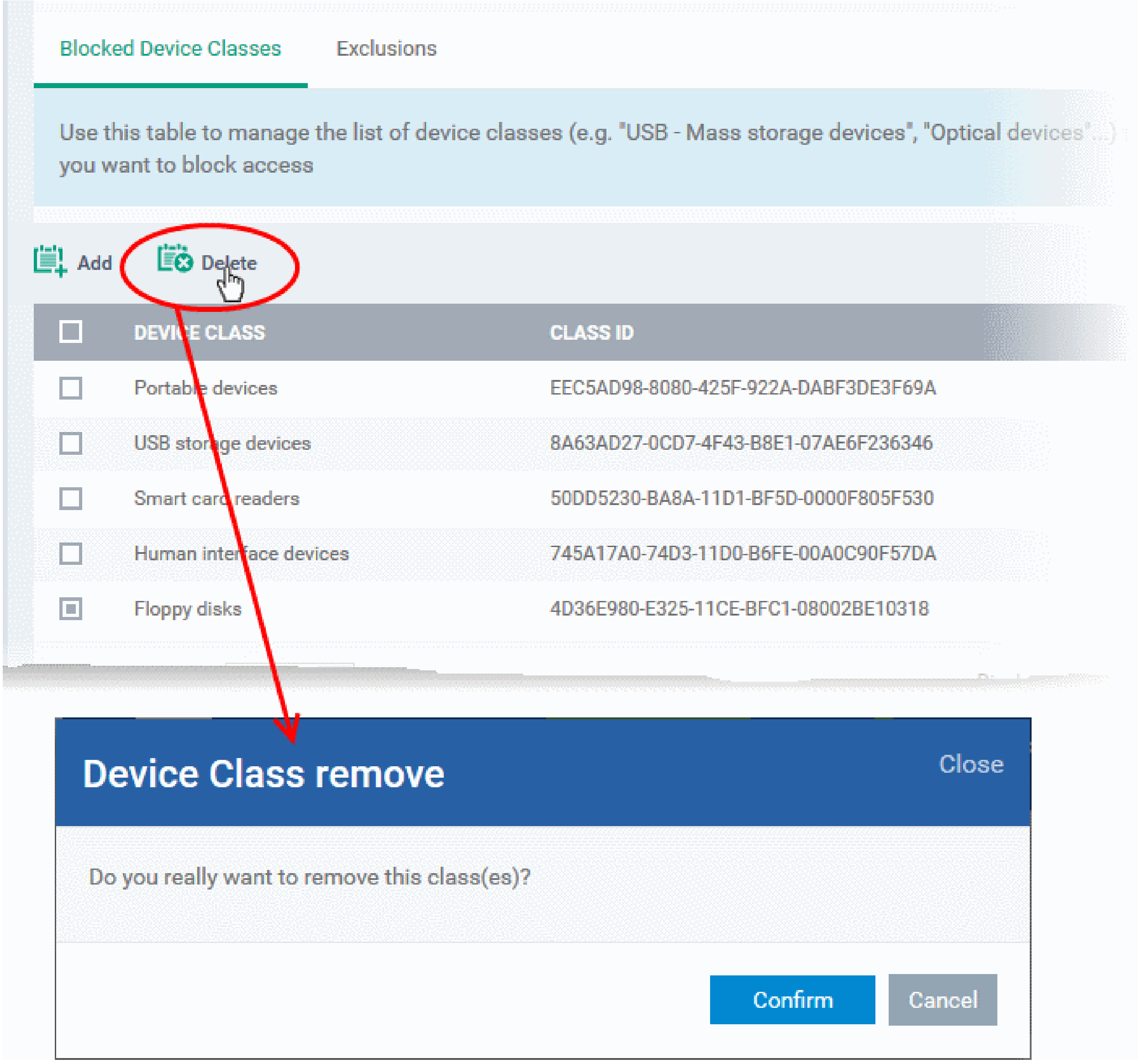
Results per page: 20

Displaying 1-20 of 21 results

- 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'



Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) you want to block access

□	DEVICE CLASS	CLASS ID
□	Portable devices	EEC5AD98-8080-425F-922A-DABF3DE3F69A
□	USB storage devices	8A63AD27-0CD7-4F43-B8E1-07AE6F236346
□	Smart card readers	50DD5230-BA8A-11D1-BF5D-0000F805F530
□	Human interface devices	745A17A0-74D3-11D0-B6FE-00A0C90F57DA
▣	Floppy disks	4D36E980-E325-11CE-BFC1-08002BE10318

Device Class remove

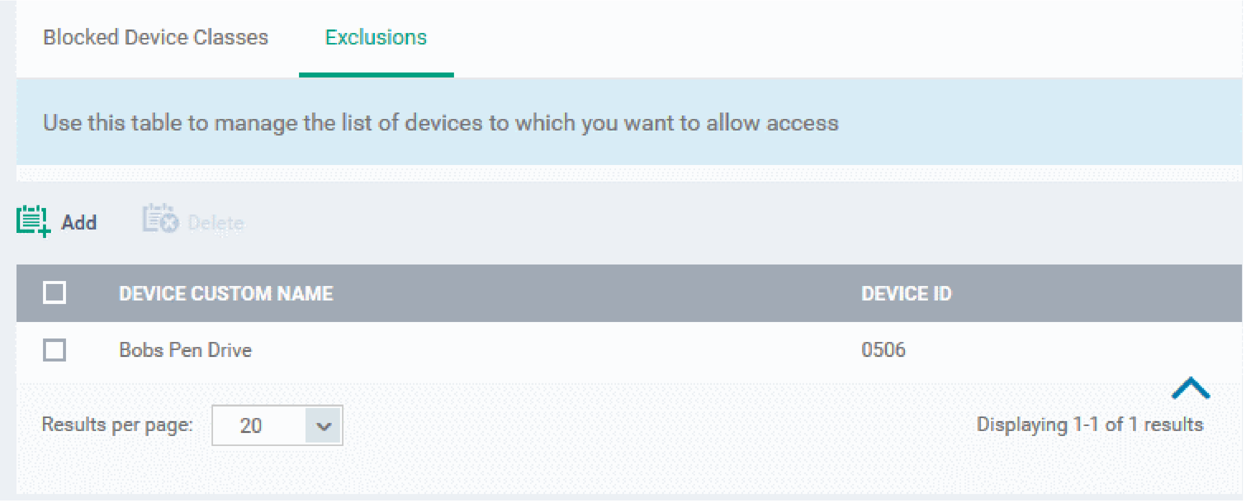
Do you really want to remove this class(es)?

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).



Use this table to manage the list of devices to which you want to allow access

□	DEVICE CUSTOM NAME	DEVICE ID
□	Bobs Pen Drive	0506

Results per page: 20

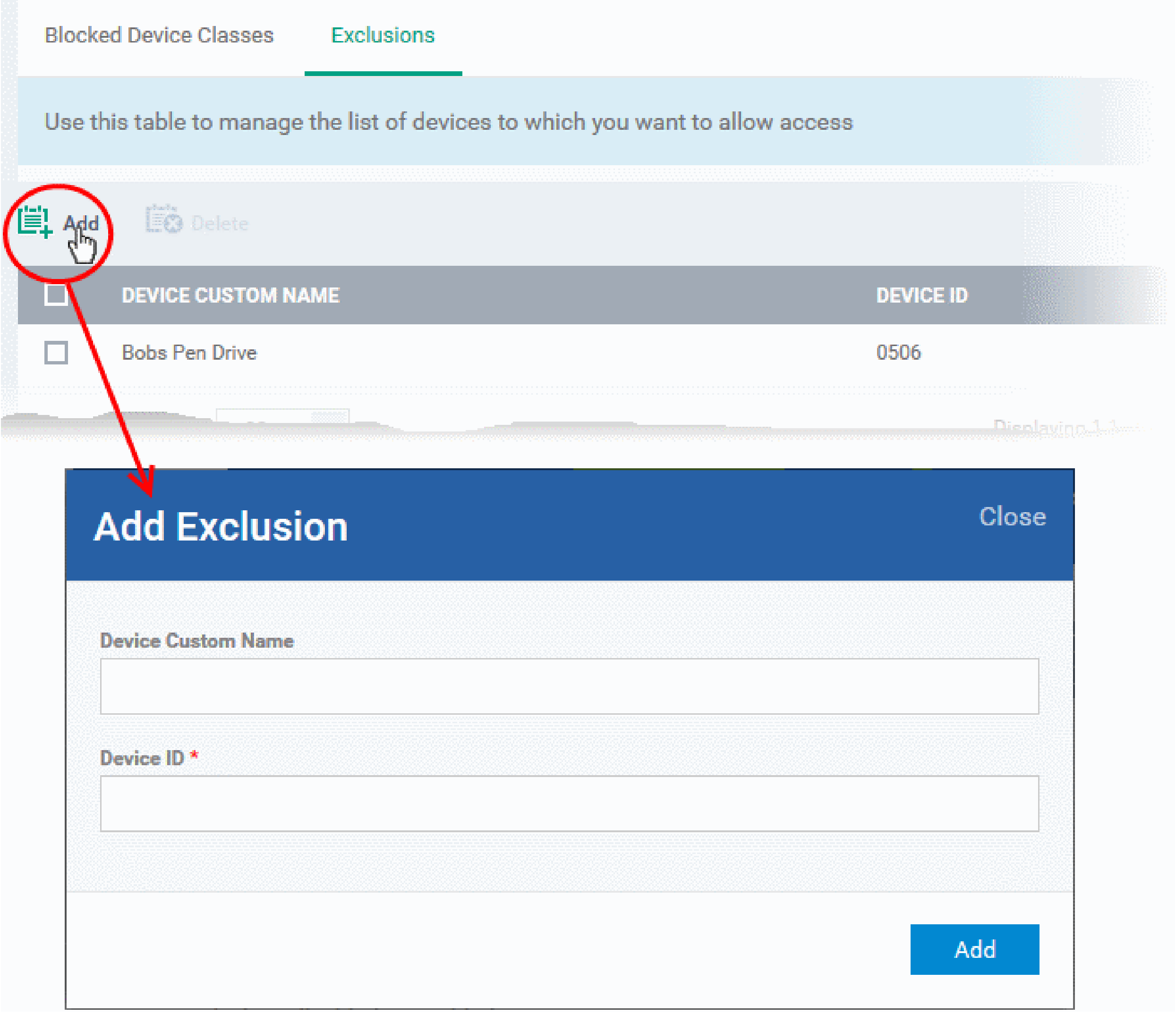
Displaying 1-1 of 1 results

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.



Use this table to manage the list of devices to which you want to allow access

□	DEVICE CUSTOM NAME	DEVICE ID
□	Bobs Pen Drive	0506

Add Exclusion

Device Custom Name

Device ID *

- Enter a name for the device in the 'Device Custom Name' field (optional)
- Enter the unique device identifier in the 'Device ID' field

Tip: You can use a wildcard character '*' in the Device ID if you want to cover a range of devices with similar IDs. For example, to include all USB storage devices whose device IDs start with "4C5310", you could enter:

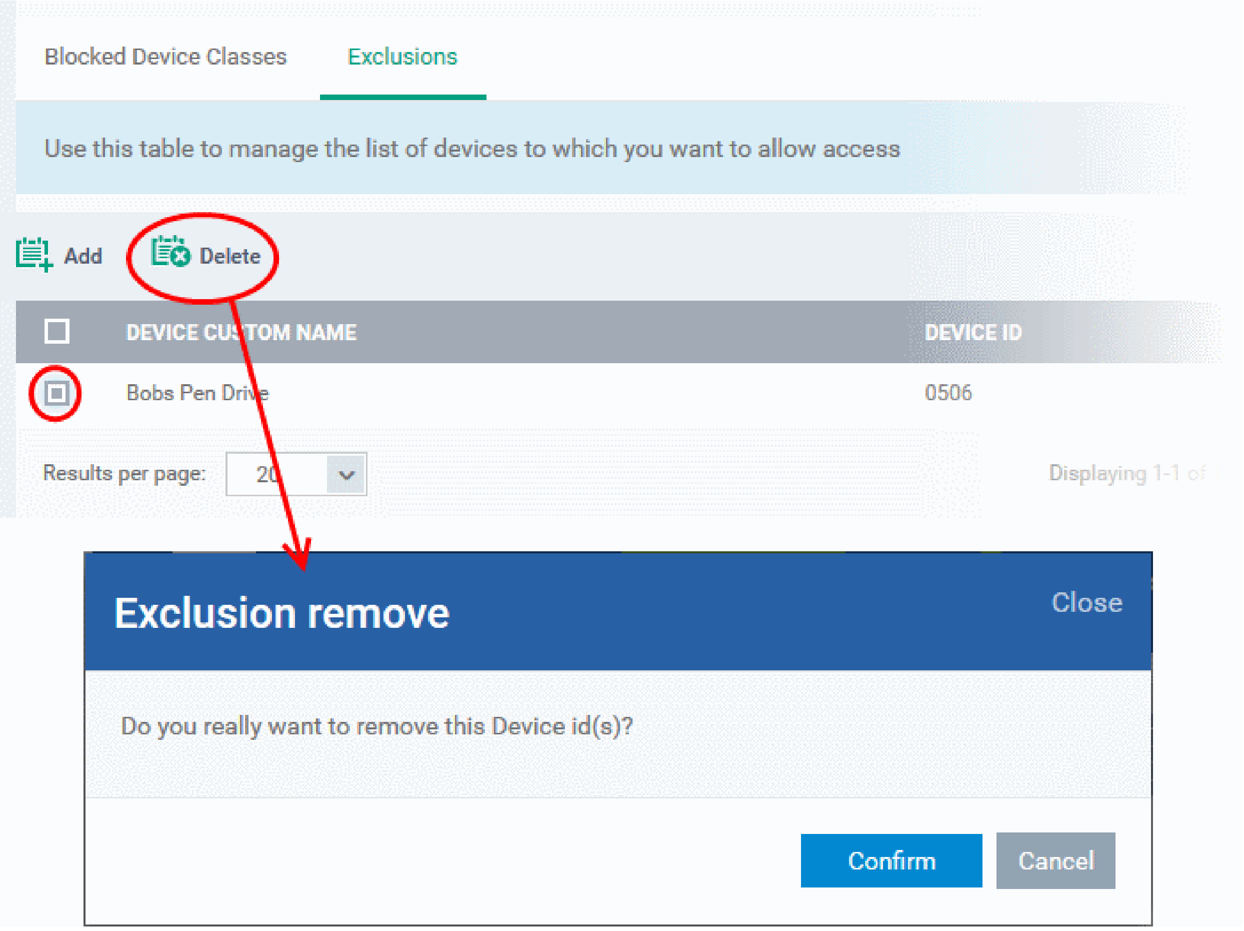
USBSTOR\DISK&VEN_SANDISK\4C5310*

- 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'



Use this table to manage the list of devices to which you want to allow access

DEVICE CUSTOM NAME	DEVICE ID
Bobs Pen Drive	0506

Results per page: 20

Displaying 1-1 of

Exclusion remove

Do you really want to remove this Device id(s)?

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 you to define performance and availability conditions for various events and services. An alert will be triggered if the conditions are breached. You can also configure automatic procedures to run if an alert is generated.

ITSM allows you to monitor services, processes, events, disk space, RAM usage and more. You can also create custom monitoring scripts.

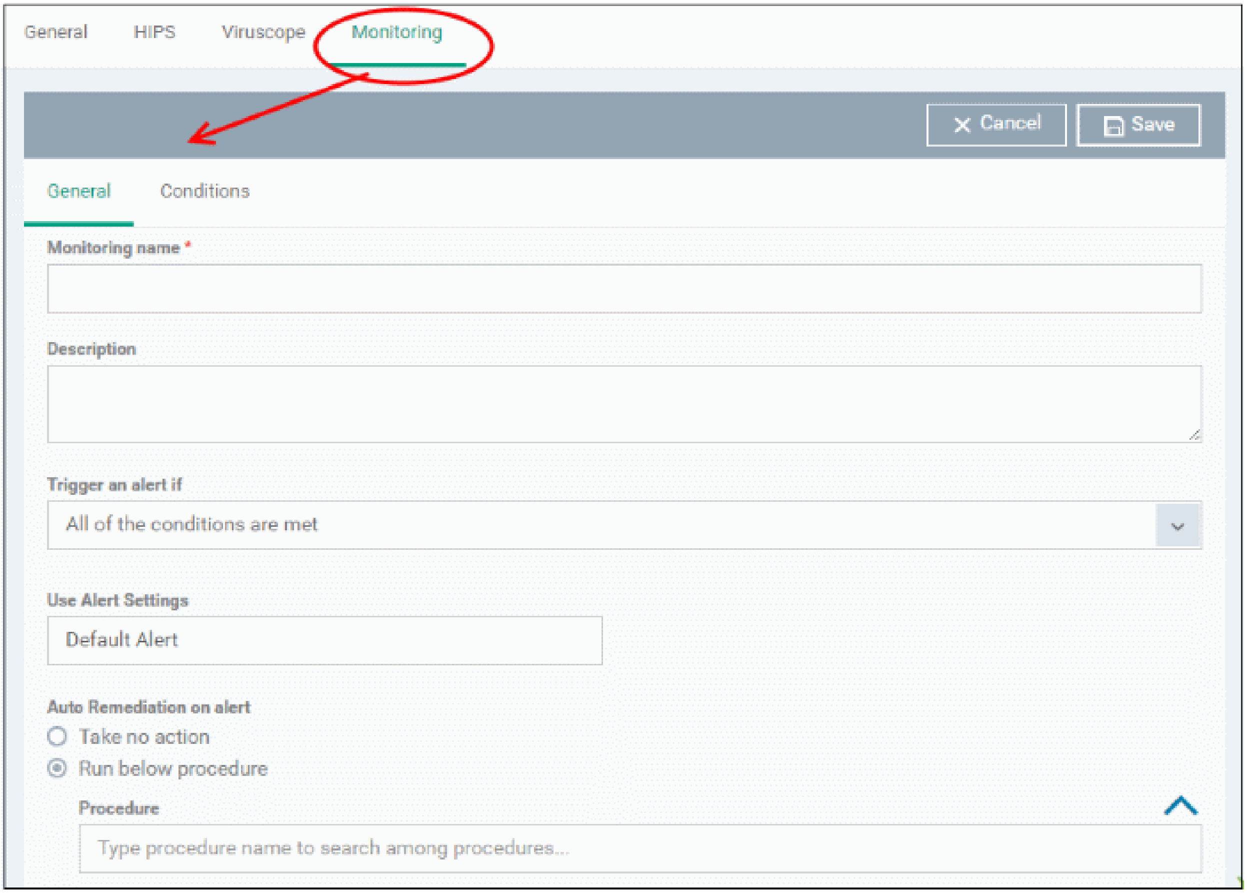
Note

- ITSM communicates with Comodo servers and agents on devices in order to monitor events, deploy profiles, provide updates and more.
- You need to configure your firewall accordingly to allow these connections. See **Appendix 1** for details of the IPs, host-names and ports used by ITSM.

To configure monitoring settings

- Choose 'Monitoring' from the 'Add Profile Section' drop-down

The 'Monitoring' screen will be displayed.



Monitoring name *

Description

Trigger an alert if: All of the conditions are met

Use Alert Settings: Default Alert

Auto Remediation on alert
○ Take no action
● Run below procedure

Procedure: Type procedure name to search among procedures...

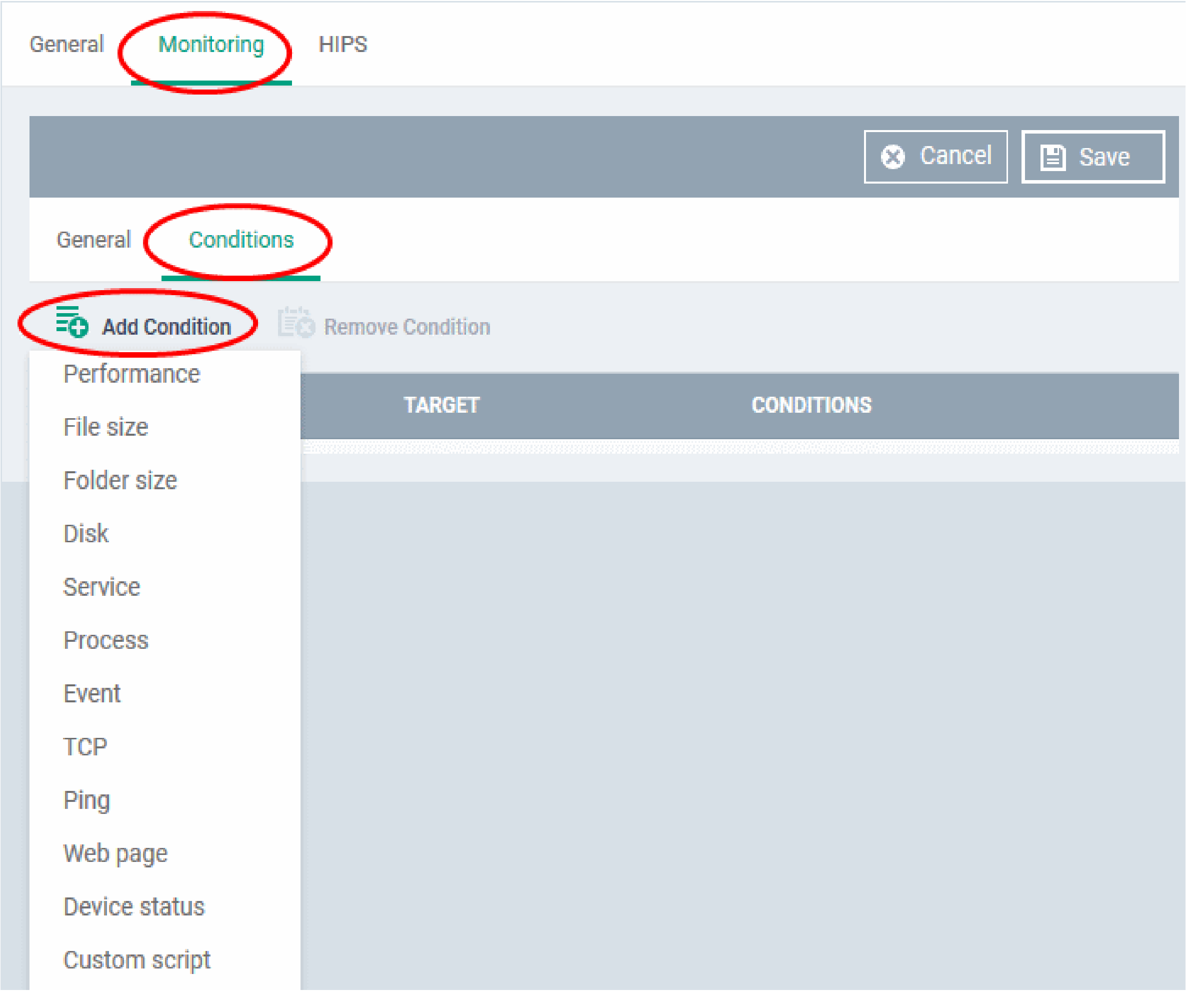
General Tab

- 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'

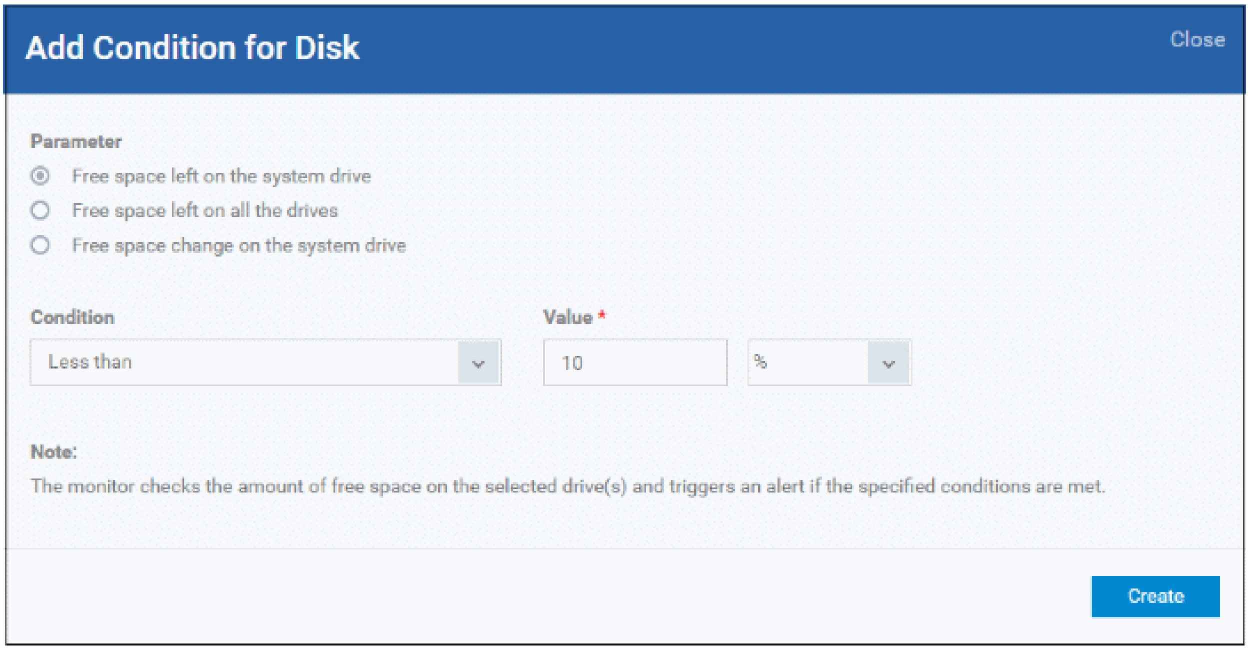


Monitoring Conditions	
Name of the Condition	**Description**
Performance	Checks the usage of CPU, RAM and Network on devices and triggers an alert if the specified conditions are met.
File Size	Checks the disk space used by a specified file on target computers and triggers an alert when the specified 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'.
Custom Script	Allows you to create custom monitoring conditions as required. Refer to **Adding Custom Monitoring Conditions** for more details.

Add Monitoring Conditions

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.



Add Condition for Disk

Parameter
- ● Free space left on the system drive
- ○ Free space left on all the drives
- ○ Free space change on the system drive

Condition: Less than

Value *: 10 %

Note:
The monitor checks the amount of free space on the selected drive(s) and triggers an alert if the specified conditions are met.

- Click 'Create' after specifying the conditions.

The monitoring parameters added for the profile will be listed.

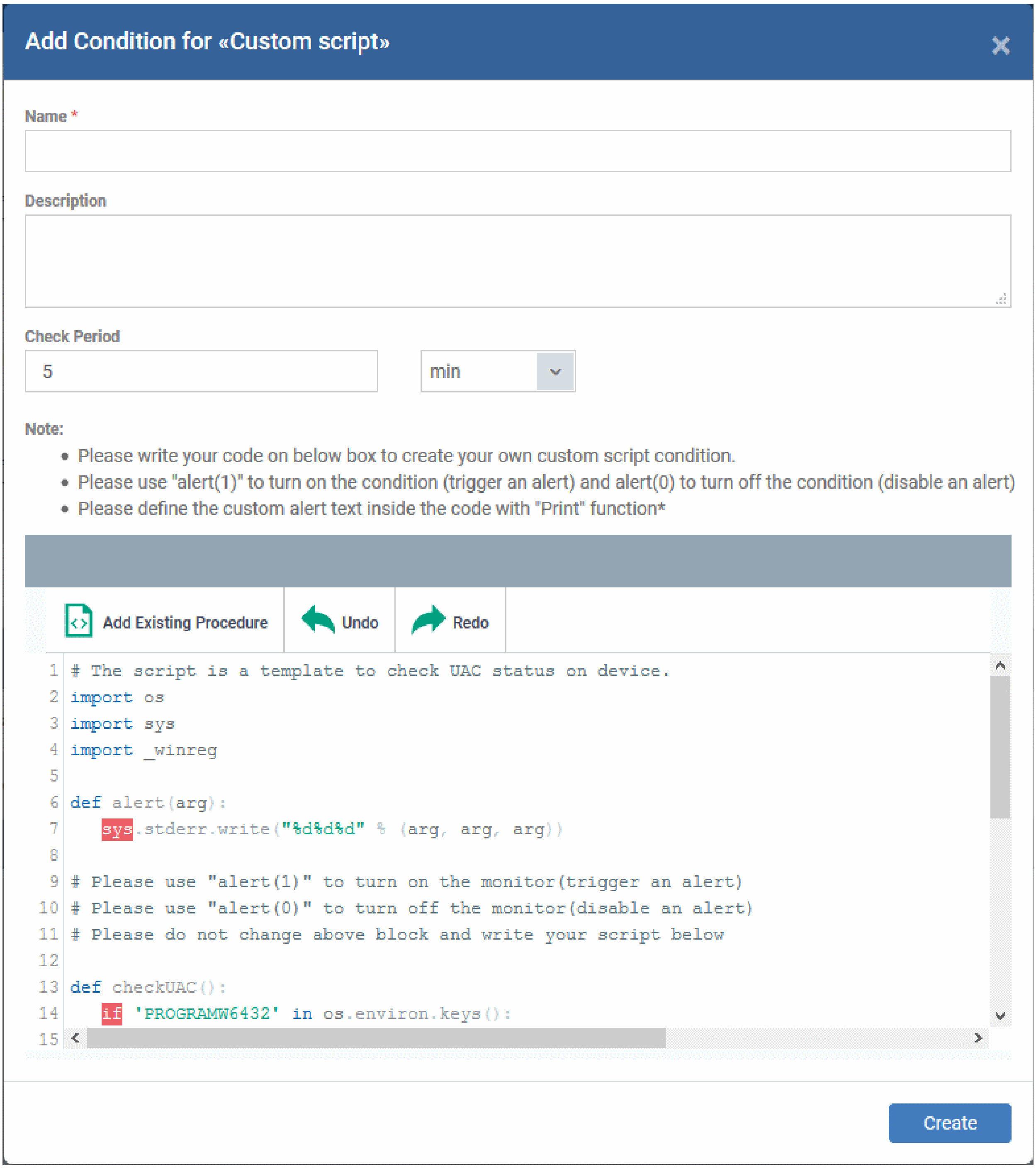
Add Custom Monitoring Conditions

- ITSM allows you to create custom monitoring conditions per your business requirements.
- You can create custom scripts in python and can define which items should be monitored. You can also define the threshold before an alert is generated.
- Predefined script monitors are available in 'Configuration Templates' > 'Procedures' > 'Predefined Procedures' > 'Monitors'. These are available for selection in the 'Add Existing Procedure' >'Procedure name' drop-down.

To add a custom script to the monitoring conditions

- Choose 'Custom script' from the 'Add Condition' drop-down

The 'Add Condition for Custom Script' form will appear.



Note:

- Please write your code on below box to create your own custom script condition.
- Please use "alert(1)" to turn on the condition (trigger an alert) and alert(0) to turn off the condition (disable an alert)
- Please define the custom alert text inside the code with "Print" function*

```
# The script is a template to check UAC status on device.
import os
import sys
import _winreg

def alert(arg):
    sys.stderr.write("%d%d%d" % (arg, arg, arg))

# Please use "alert(1)" to turn on the monitor(trigger an alert)
# Please use "alert(0)" to turn off the monitor(disable an alert)
# Please do not change above block and write your script below

def checkUAC():
    if 'PROGRAMW6432' in os.environ.keys():
```

Add Condition for Custom Script - Table of Parameters	
Form Element	**Description**
Name	Enter a name for the script, shortly describing its purpose.
Description	Enter a short description for the script.
Check Period	Enter the time interval at which the script should be run on the endpoints to which the profile is applied. Tip: Ensure that the check period is greater than the time taken for the script to run and complete, so that successive executions of the script do not overlap.
Script	Enter your Python script in the text editor.

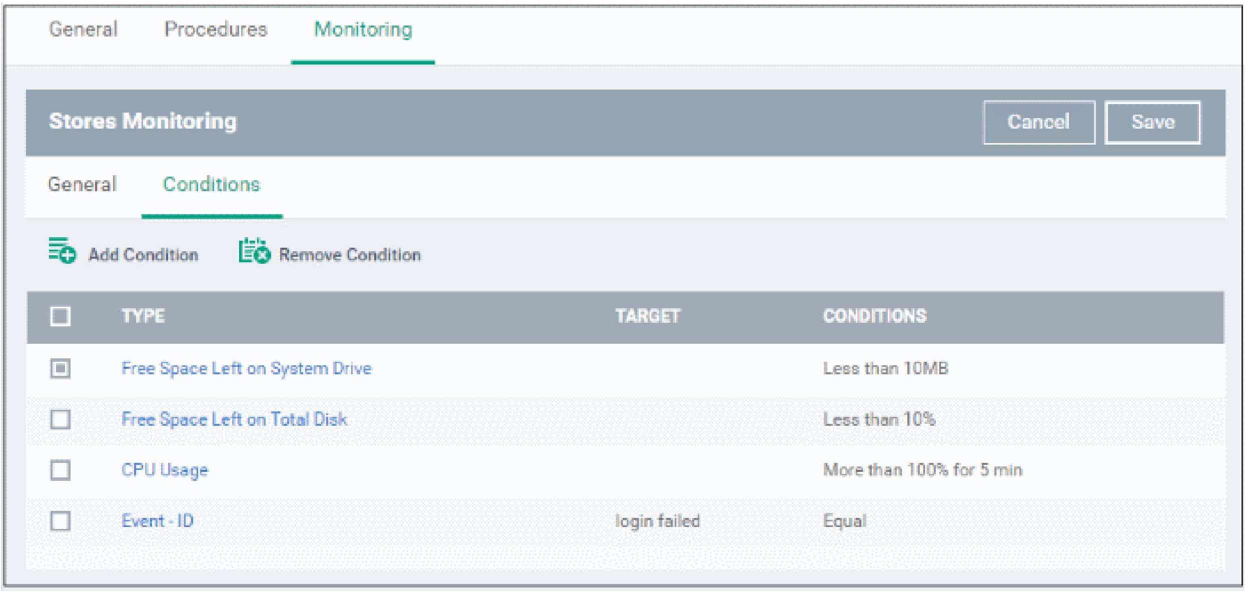
Add Condition for Custom Script - Table of Parameters	

	Note 1: Keep the following lines intact in the editor and enter your script below these:
	`import os`
	`import sys`
	`import _winreg`
	`def alert(arg):`
	`    sys.stderr.write("%d%d%d" % (arg, arg, arg))`
	`# Please use "alert(1)" to turn on the monitor(trigger an alert)`
	`# Please use "alert(0)" to turn off the monitor(disable an alert)`
	`# Please do not change above block and write your script below`
	
	Note 2: If you want an alert to be triggered if the condition is met set the argument to alert parameter to 1, i.e. 'alert(1)'.
	If you do not want an alert to be triggered even if the condition is met set the argument to alert parameter to 0, i.e. 'alert(0)'.
	Note 3: You can import an existing script procedure in ITSM if you wish to create a new custom monitor script using an existing procedure as a starting point. To do so, click 'Add Existing Procedure' and choose the existing procedure. Edit the script as per your requirement as per Note 1. For more details on procedures, refer to the section **Managing Procedures**.
	Note 4: In addition to the above, Python script monitors by the Comodo development team are available in the 'Monitors' folder under 'Configuration Templates' > 'Procedures' > 'Predefined Procedures'. You can add these predefined scripts by clicking 'Add Existing Procedure' and select from the 'Procedure name' drop-down and can be used directly without any changes. Feel free to try any script that fits your needs. If you require custom scripts from Comodo, please raise a request at https://c1forum.comodo.com/forum/script-library/4460-script-requests-comodo-will-write-the-scripts-for-you-for-free

- Complete the form and click 'Create'

The custom monitor will be added to the list of monitors under the 'Monitoring' tab.

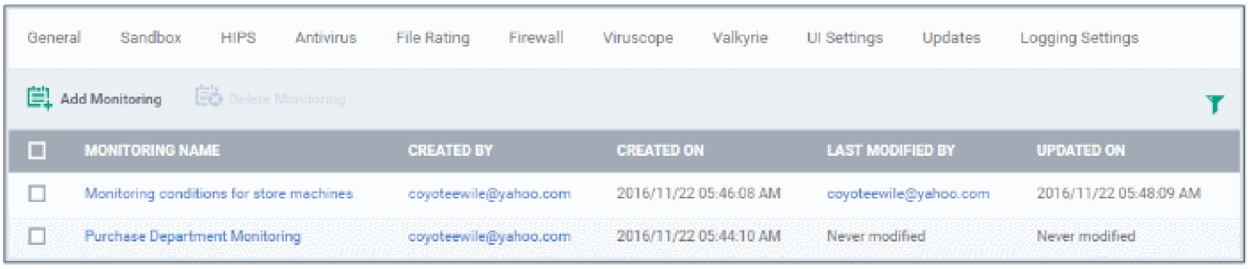
- Repeat the process for adding more monitoring conditions.



☐	TYPE	TARGET	CONDITIONS
☒	Free Space Left on System Drive		Less than 10MB
☐	Free Space Left on Total Disk		Less than 10%
☐	CPU Usage		More than 100% for 5 min
☐	Event - ID	login failed	Equal

- To remove a monitoring condition, select the check box beside it and click 'Remove Condition' at the top.
- Click 'Save' to apply your changes.

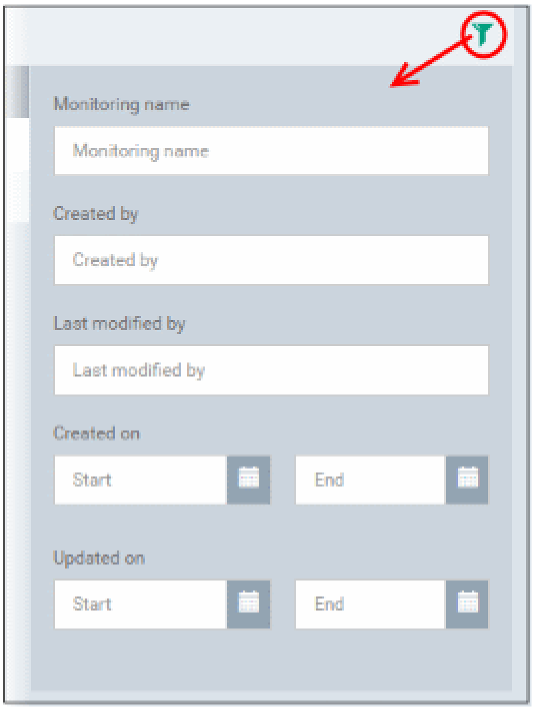
- Repeat the process to add more monitors. The added monitors will be listed under the 'Monitoring ' tab in the profile.



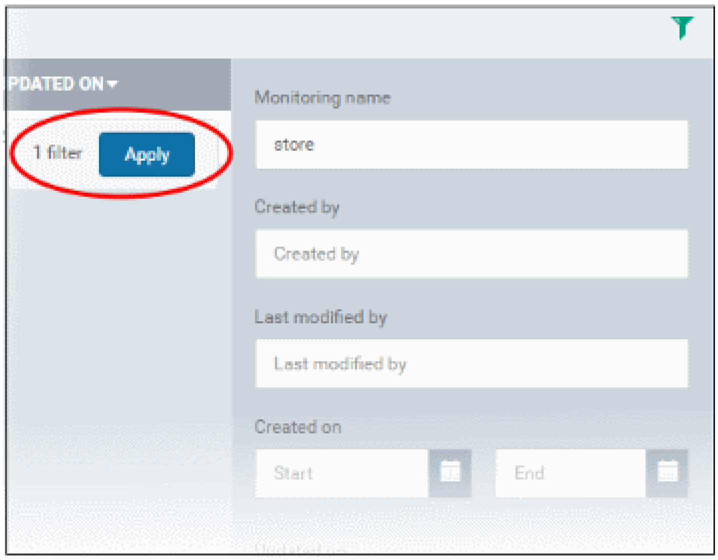
☐	MONITORING NAME	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
☐	Monitoring conditions for store machines	coyoteewile@yahoo.com	2016/11/22 05:46:08 AM	coyoteewile@yahoo.com	2016/11/22 05:48:09 AM
☐	Purchase Department Monitoring	coyoteewile@yahoo.com	2016/11/22 05:44:10 AM	Never modified	Never modified

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'



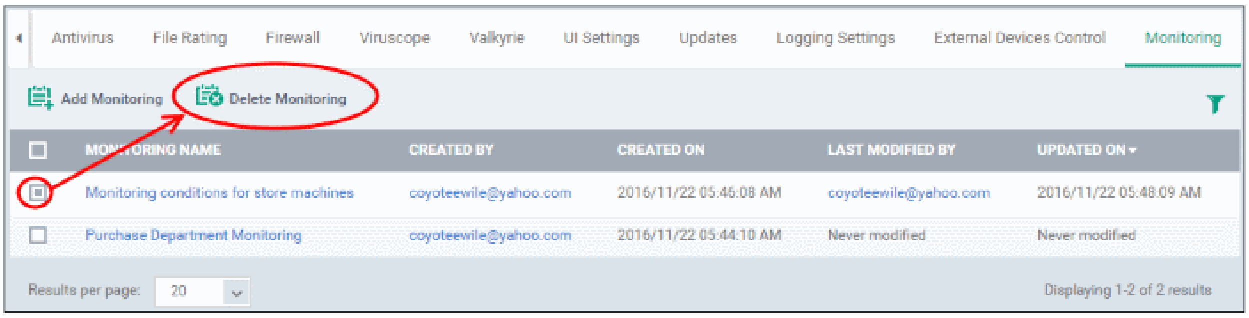
Monitoring name: store

- 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.

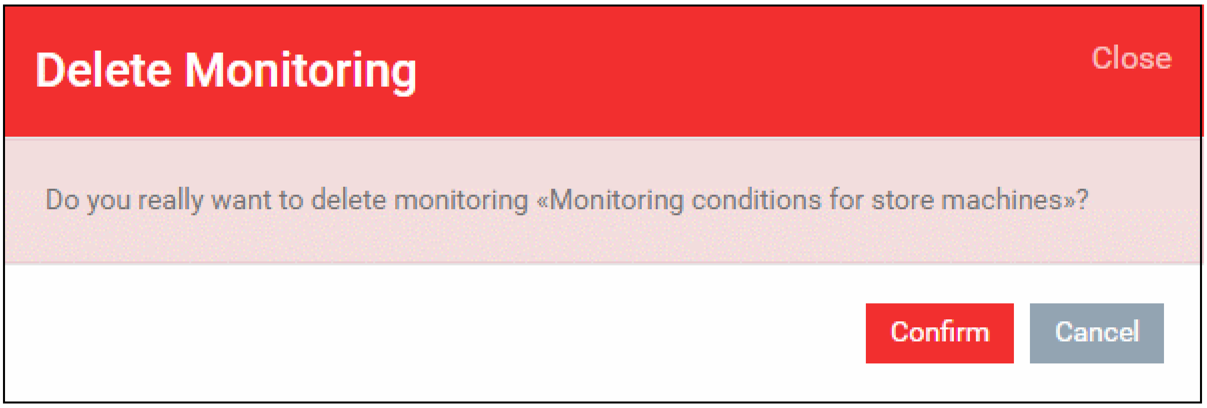
To remove a monitor from the profile, select it and click 'Delete Monitoring' at the top.



□	MONITORING NAME	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
☑	Monitoring conditions for store machines	coyoteewile@yahoo.com	2016/11/22 05:46:08 AM	coyoteewile@yahoo.com	2016/11/22 05:48:09 AM
□	Purchase Department Monitoring	coyoteewile@yahoo.com	2016/11/22 05:44:10 AM	Never modified	Never modified

Results per page: 20 Displaying 1-2 of 2 results

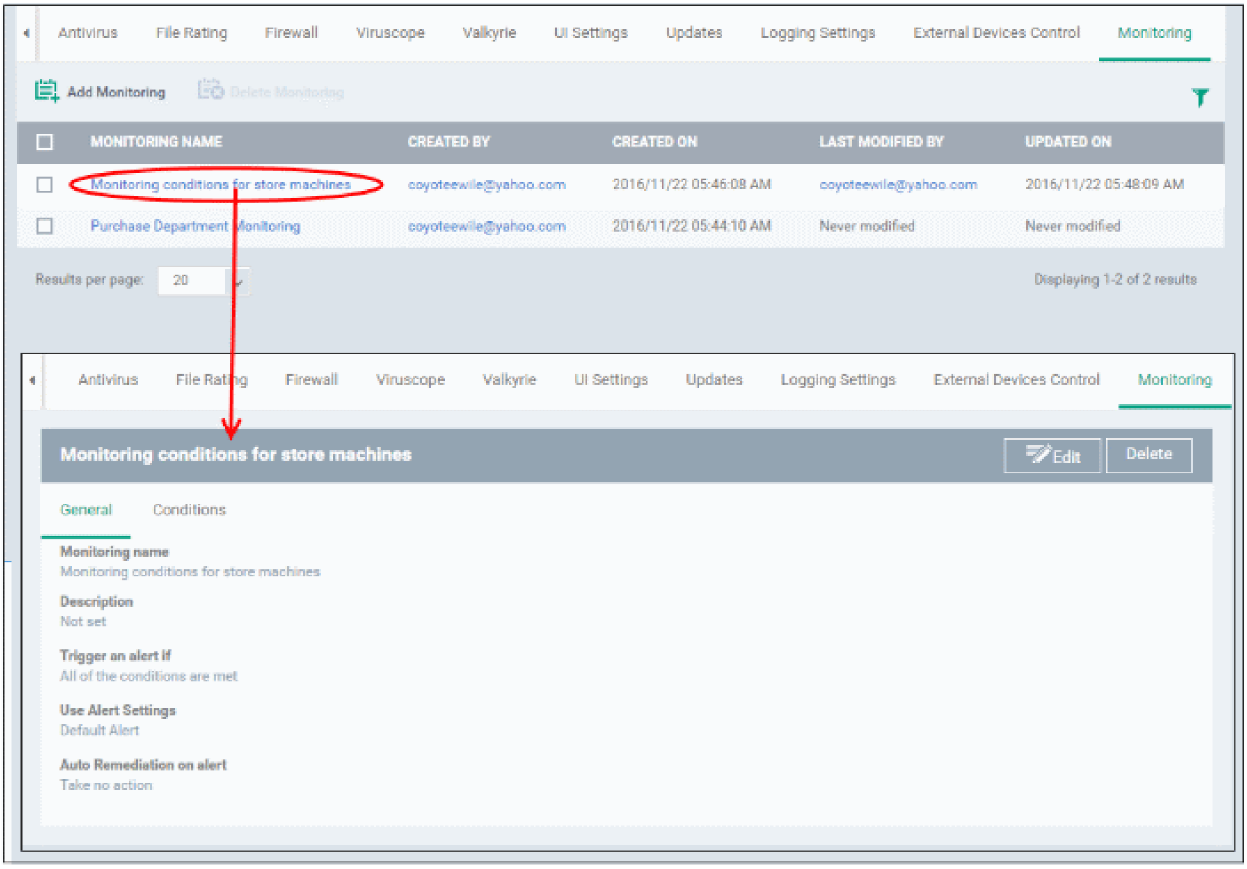
A confirmation message will be displayed.



Delete Monitoring Close

Do you really want to delete monitoring «Monitoring conditions for store machines»?

- Click 'Confirm' to remove the selected monitor.
- To edit a monitor, click the name and then the 'Edit' button on the right.



□	MONITORING NAME	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
□	Monitoring conditions for store machines	coyoteewile@yahoo.com	2016/11/22 05:46:08 AM	coyoteewile@yahoo.com	2016/11/22 05:48:09 AM
□	Purchase Department Monitoring	coyoteewile@yahoo.com	2016/11/22 05:44:10 AM	Never modified	Never modified

Results per page: 20 Displaying 1-2 of 2 results

Monitoring conditions for store machines

Monitoring name
Monitoring conditions for store machines

Description
Not set

Trigger an alert if
All of the conditions are met

Use Alert Settings
Default Alert

Auto Remediation on alert
Take no action

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.

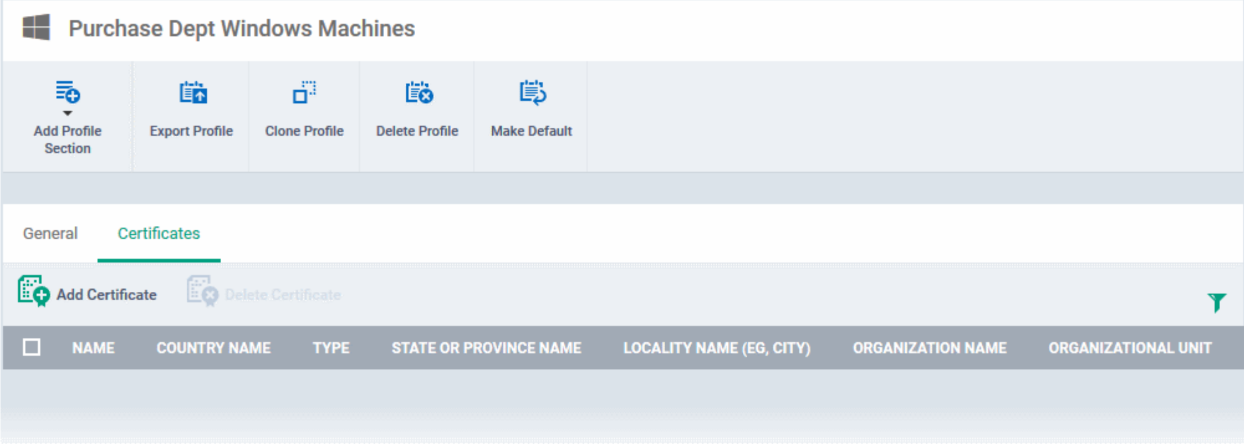
In addition to user authentication, client certificates can be used for email signing and encryption.

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

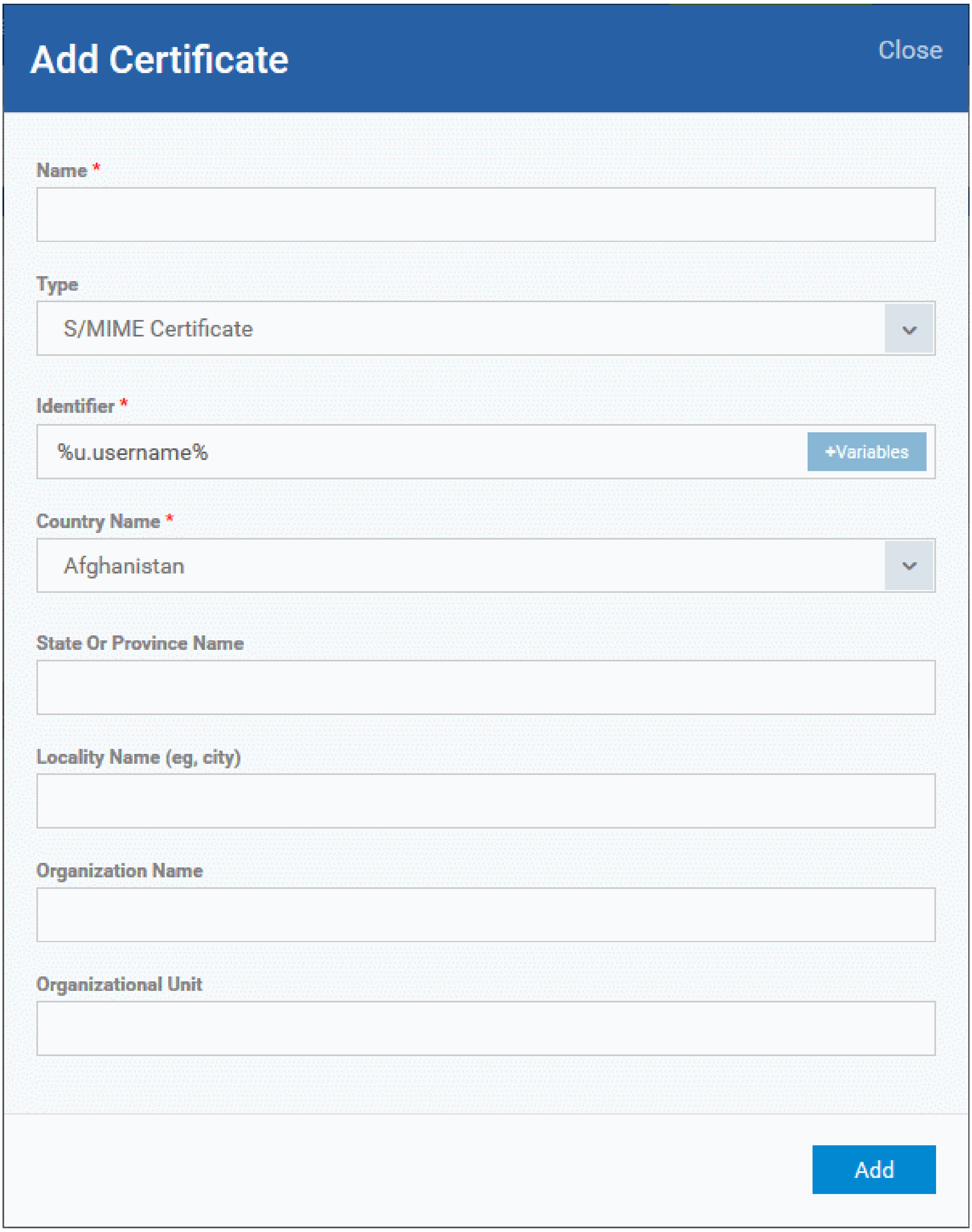
- Choose 'Certificates' from the 'Add Profile Section' drop-down

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

Name *

Type: S/MIME Certificate

Identifier *: %u.username%

Country Name *: Afghanistan

State Or Province Name

Locality Name (eg, city)

Organization Name

Organizational Unit

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.

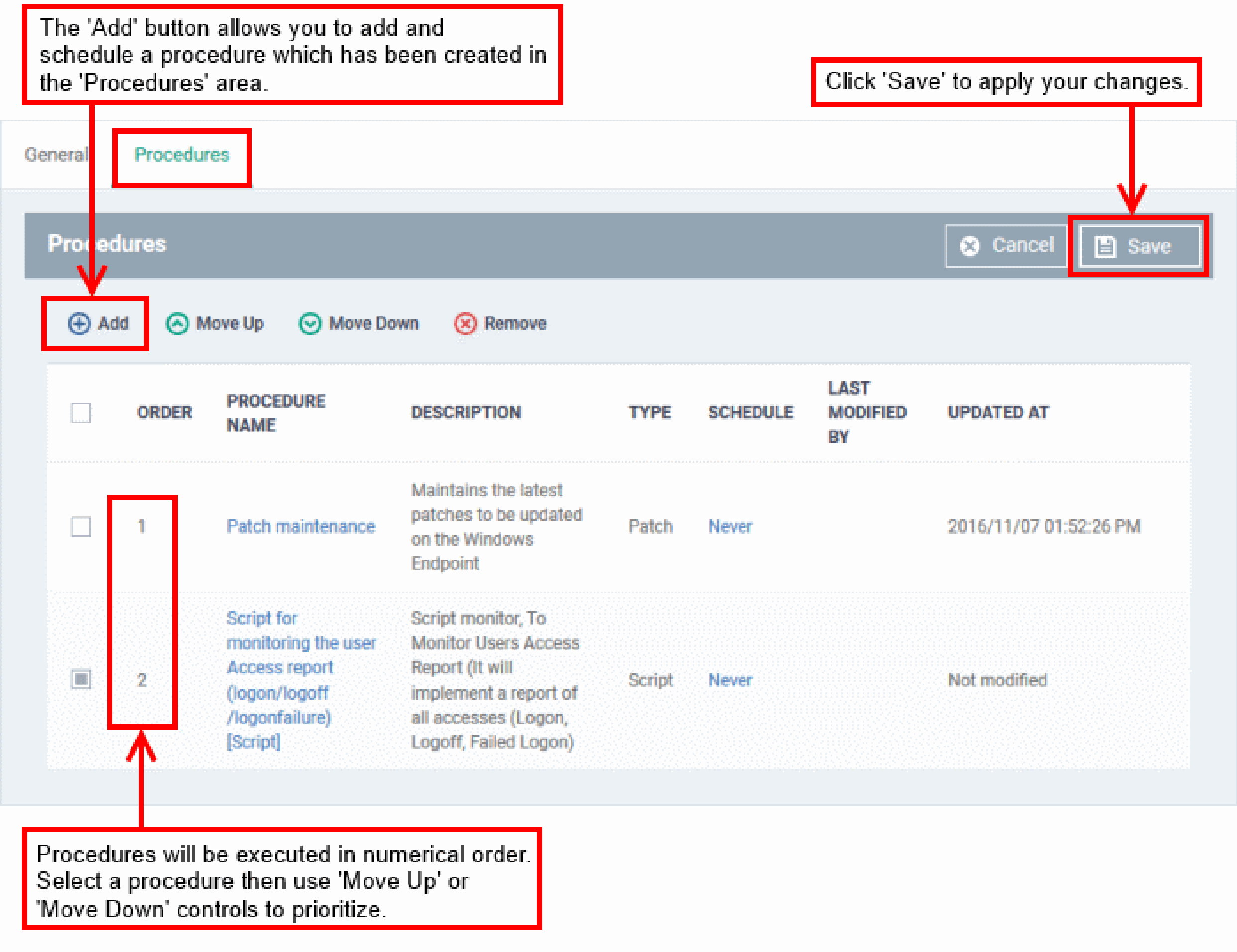
The certificate requests will be generated from the devices once the profile is applied to them.

6.1.3.1.18. Procedure Settings

- ITSM allows you to run scripts and patches as procedures to run on Windows devices.
- You can also automate procedure deployment by adding them to a profile along with a schedule.
- The 'Procedures' area of a profile lets you 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'



The 'Add' button allows you to add and schedule a procedure which has been created in the 'Procedures' area.

Click 'Save' to apply your changes.

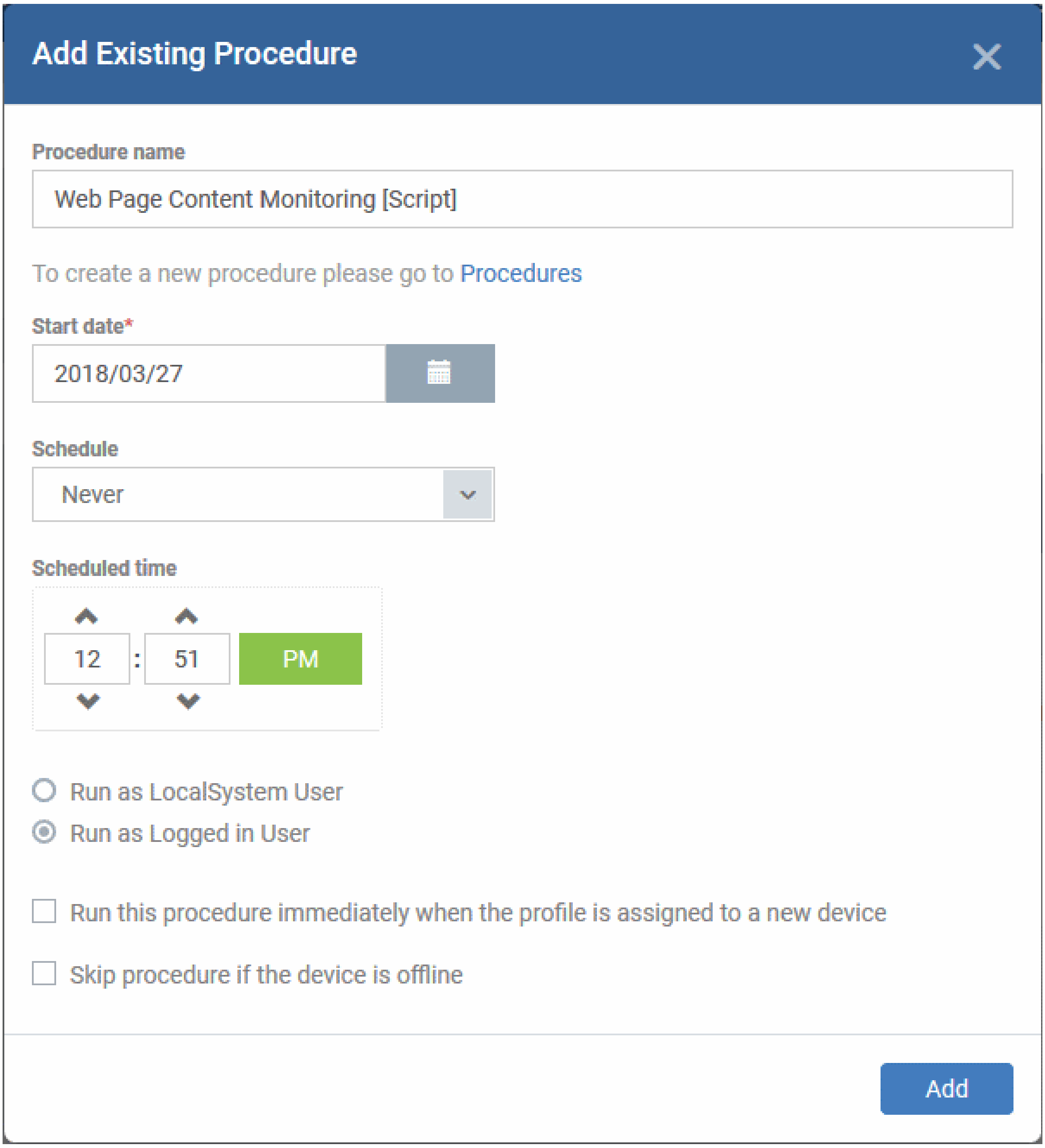
□	ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
□	1	Patch maintenance	Maintains the latest patches to be updated on the Windows Endpoint	Patch	Never		2016/11/07 01:52:26 PM
▣	2	Script for monitoring the user Access report (logon/logoff /logonfailure) [Script]	Script monitor, To Monitor Users Access Report (It will implement a report of all accesses (Logon, Logoff, Failed Logon)	Script	Never		Not modified

Procedures will be executed in numerical order. Select a procedure then use 'Move Up' or 'Move Down' controls to prioritize.

- Note. Procedures are actually created and configured in the 'Procedures' area ('Configuration Templates' > 'Procedures').
- Related. **Manage 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'.



Add Existing Procedure

Procedure name

Web Page Content Monitoring [Script]

To create a new procedure please go to Procedures

Start date*

2018/03/27

Schedule

Never

Scheduled time

12 : 51 PM

○ Run as LocalSystem User

● Run as Logged in User

□ Run this procedure immediately when the profile is assigned to a new device

□ Skip procedure if the device is offline

Add Existing Procedure to a Profile - Form Parameters	
Parameter	**Description**
Procedure Name	Choose an existing 'Patch' or 'Script' procedure by typing the first few characters of the procedure name. Make sure you have already approved the procedure. See **View and Manage Procedures** for help to configure procedures in ITSM.
Schedule Options	Create a schedule for the procedure to run periodically on the devices applied with this profile. (optional) • Select the 'Start date' for the procedure by clicking the calendar icon beside 'Start Date'.. • Select the period fro the schedule from the 'Schedule' drop-down. The available options are:

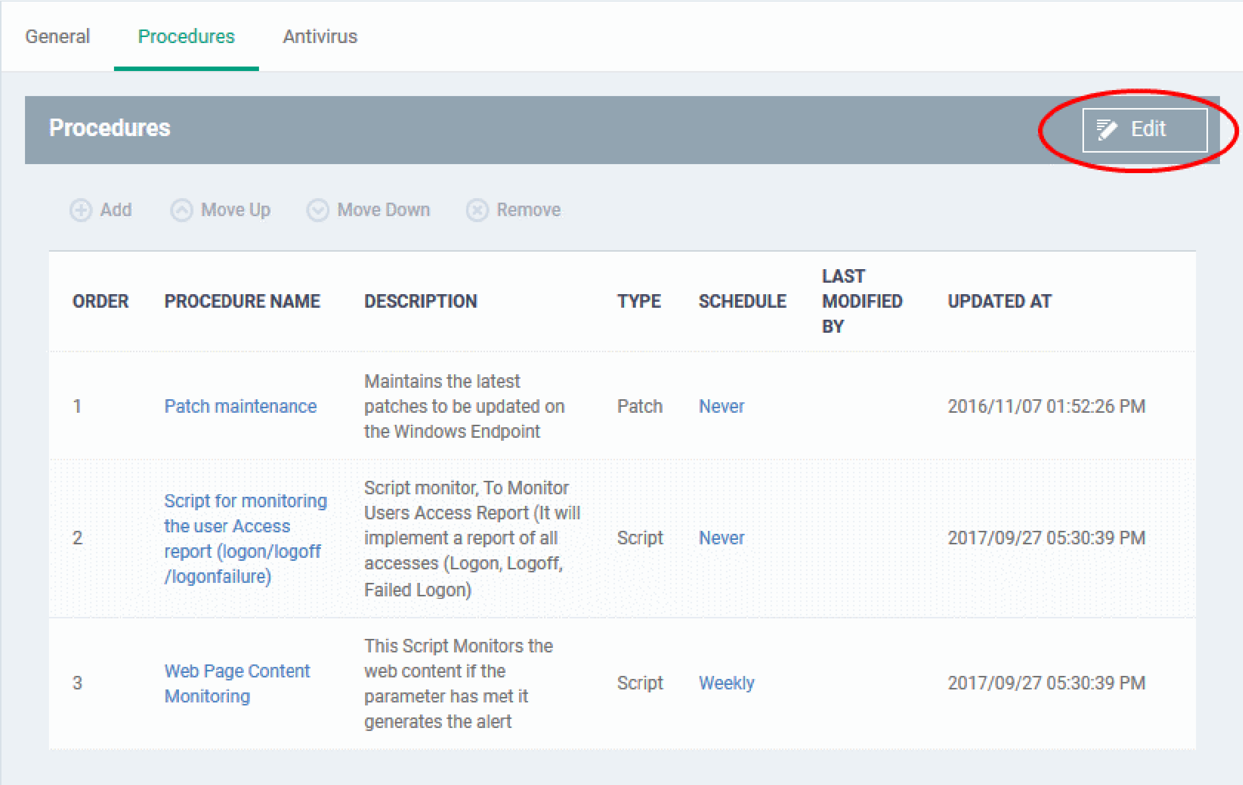
	- Never - Daily - Weekly - If chosen you need to select the days of the week on which the procedure is to be run - Monthly - If chosen you need to select the dates of a month on which the procedure is to be run - Set the time at which the procedure is to run on the scheduled days from the 'Scheduled' 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.
User Account Options	- 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. - This applies only to 'Script' procedure
Execution Options	**Run this procedure immediately when the profile is assigned to a new device** The procedure will run on target devices as soon as the profile is applied to the device, in addition to any schedule. **Skip procedure if the device is offline** The procedure will be aborted is the device is not connected to ITSM at the time of execution. By default, procedures are queued for later deployment if the device is not connected to ITSM. The task will be executed as soon as it comes online. - Select this option If you do not want the task to be added to the queue.

- Configure the options and click 'Save'
- Repeat this process to add multiple procedures.

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 'Configuration Templates' > 'Profiles'
- Open the Windows profile containing the procedures component to be edited
- Click the 'Procedures' tab
- Click 'Edit' and select the procedure that needs to be modified.



ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
1	Patch maintenance	Maintains the latest patches to be updated on the Windows Endpoint	Patch	Never		2016/11/07 01:52:26 PM
2	Script for monitoring the user Access report (logon/logoff /logonfailure)	Script monitor, To Monitor Users Access Report (It will implement a report of all accesses (Logon, Logoff, Failed Logon)	Script	Never		2017/09/27 05:30:39 PM
3	Web Page Content Monitoring	This Script Monitors the web content if the parameter has met it generates the alert	Script	Weekly		2017/09/27 05:30:39 PM

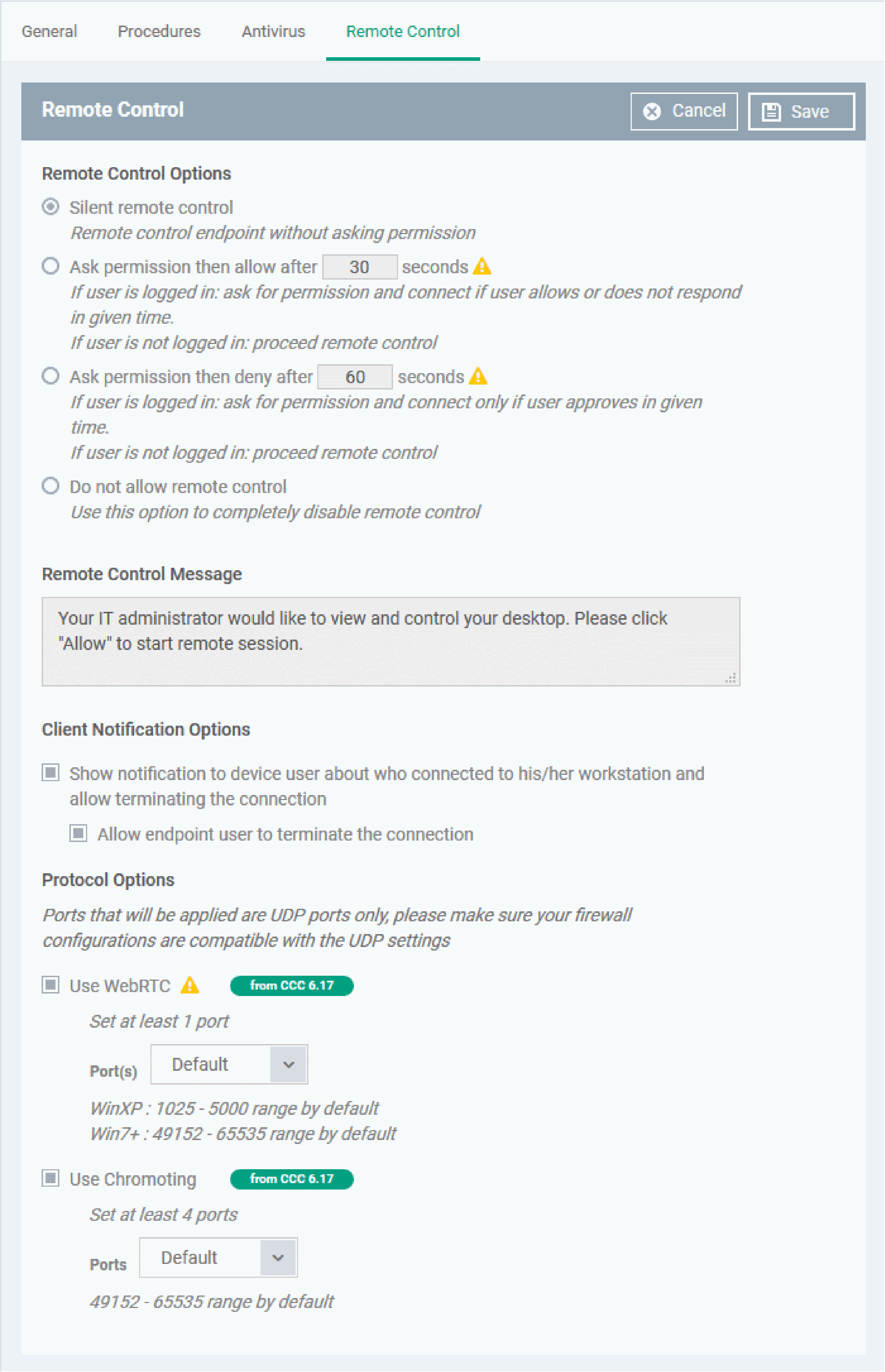
- Then click either 'Add', 'Move Up', 'Move down', or 'Remove' based on the changes that need to take effect.
  - Click 'Add' to add another procedure to the existing list
  - Click 'Move Up' to increase the priority of the procedure.
  - Click 'Move Down' to decrease the priority of the procedure.
  - Click 'Remove' to delete the procedure.
- Click 'Save'.

6.1.3.1.19. Remote Control Settings

- 'Remote Control' settings let you choose the protocol and ports used for remote connections.
- You can also configure notifications which are shown to end-users before and during a session.
- See **Remote Management of Windows and Mac OS Devices** if you need help to set up the remote control service

To configure Remote Control Settings

- Click 'Configuration Templates' > 'Profiles'
- Open the profile that you want to configure (click the profile name to do this)
- Click 'Add Profile Section' and choose 'Remote Control' from the drop-down.
  - If 'Remote Control' is not in the 'Add...' menu then it has already been added to the profile.
- Click the 'Remote Control' tab on the profile file-menu:



Remote Control

Remote Control Options

● Silent remote control
Remote control endpoint without asking permission

○ Ask permission then allow after 30 seconds ⚠
If user is logged in: ask for permission and connect if user allows or does not respond in given time.
If user is not logged in: proceed remote control

○ Ask permission then deny after 60 seconds ⚠
If user is logged in: ask for permission and connect only if user approves in given time.
If user is not logged in: proceed remote control

○ Do not allow remote control
Use this option to completely disable remote control

Remote Control Message

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

☑ Show notification to device user about who connected to his/her workstation and allow terminating the connection

☑ Allow endpoint user to terminate the connection

Protocol Options

Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings

☑ Use WebRTC ⚠ from CCC 6.17

Set at least 1 port

Port(s) Default

WinXP : 1025 - 5000 range by default
Win7+ : 49152 - 65535 range by default

☑ Use Chromoting from CCC 6.17

Set at least 4 ports

Ports Default

49152 - 65535 range by default

Remote Control Options:

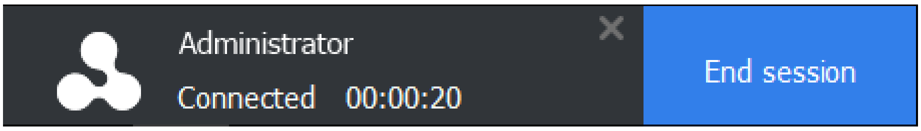
- Silent remote control - The remote connection will be established without showing a request to the user.
- Ask permission then allow after NN seconds - A message will be shown to the user which requests them to accept the connection. The connection will be established if the user does not respond within the timeout period.
    - Enter the timeout period (in seconds) in the text box
- Ask permission then deny after NN seconds - A message will be shown to the user which requests them to accept the connection. The connection attempt will be abandoned if the user does not respond within the timeout period.
    - Enter the timeout period (in seconds) in the text box
- Do not allow remote control - Disable the ability to take remote control of the endpoint.

Remote Control Message

- Enter the text of the request message. For example, 'Your administrator would like to take control of your desktop. Click 'Allow' to accept the connection request.'
- Please note that you can enter the message only on choosing the second or third notification options from the remote control settings.

Client Notification Options

This area lets you configure the notification box which is shown on the endpoint when a remote session is active:



- Show notification to device user about who... - Enable or disable the notification box
    - Allow endpoint user to terminate the connection - Choose whether or not the 'End Session' button is shown in the notification box. If enabled, the end-user will be able to close the connection.

Protocol Options

These options let you configure the protocol used for the remote session.

- These settings apply to CRC version 6.17 and above.
- You can also specify custom ports to be used by the protocol for an additional layer of safety. This allows you to keep only the specified ports open and block other ports for security.

> **Note**: Please make sure you do not assign well-known special ports. We recommend the following port range for custom use: 49152-65535.

- Use WebRTC - CRC will use WebRTC protocol to connect to the device. This option is mandatory and cannot be deselected.
- Ports - Select the port type to be used by WebRTC protocol and specify the ports. The available options are:
    - Default - WebRTC will use port range 1025 - 5000 for Windows XP and port range 49152 - 65535 for Windows 7 and later versions
    - Custom - Allows you to specify a single custom port to be used by WebRTC
    - Custom Range - Allows you to specify a port range to be used by WebRTC
- Use Chromoting - Chromoting provides a better quality of remote control and experience and is

supported only by Windows 7 and later.

  - If selected, CRC will use Chromoting to connecting to devices Windows 7 and later and use WebRTC for Windows XP devices.
  - If not selected, CRC will use only WebRTC to connect to devices with any Windows version.
- Ports - Select the port type to be used by Chromoting protocol and specify the ports. The available options are:
  - Default - Chromoting will use the port range 49152 - 65535
  - Custom Range - Allows you to specify a port range to be used by Chromoting. Enter a range covering at least 4 ports.

- Click 'Save' to apply your changes to the profile.

6.1.3.2. Import 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

The current security configuration of the CCS installation on the endpoints depends on:

- The configuration profiles applied o the endpoint
- Manual configuration of the parameters at the endpoint.

Note: If you are manually configuring the security parameters, ensure that the option 'Enable local user to override profile configuration' is selected in the 'Client Access Control' section in the profile(s) in action on the endpoint. Otherwise your manual settings will be reverted and the security parameters will be automatically set as per the configuration profile(s) effective on the endpoint during the next polling cycle of the Comodo Client Communication (CCC). Refer to the section **Client Access Control** for more details.

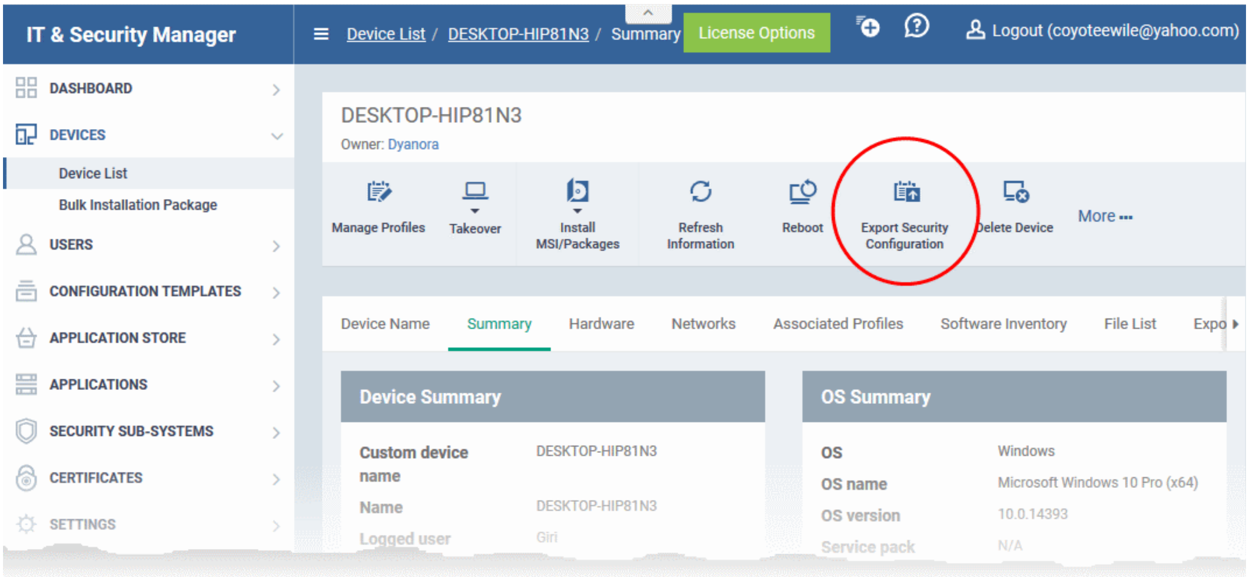
You can export the CCS configuration from a managed Windows device in two ways:

- **Export configuration of a selected device from ITSM interface**
- **Manually export the CCS configuration from the selected device**

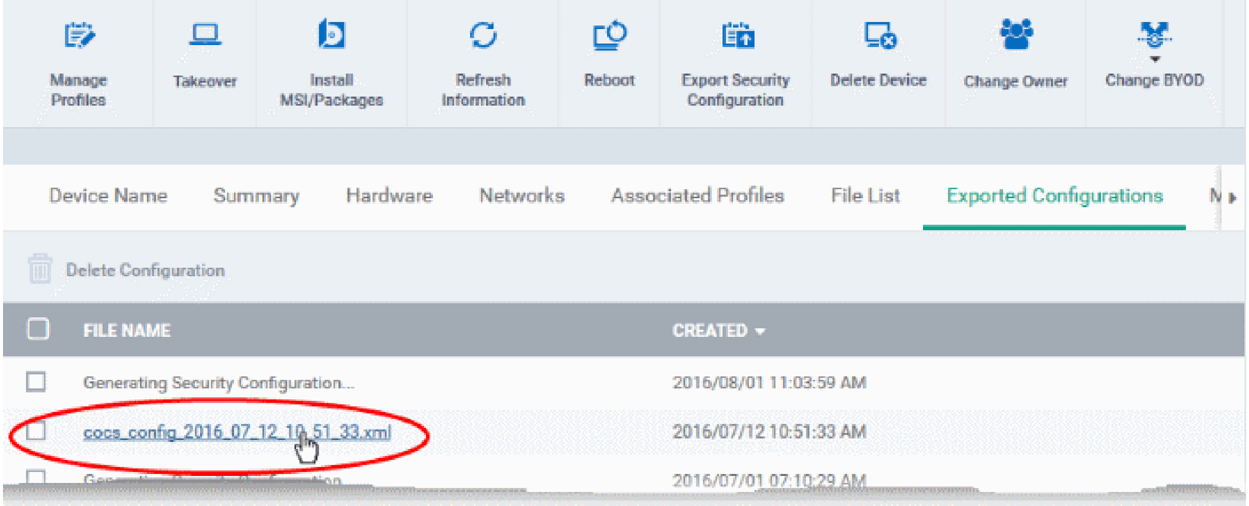
Export Configuration from ITSM interface

- 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':



☐	FILE NAME	CREATED
☐	Generating Security Configuration...	2016/08/01 11:03:59 AM
☐	cocs_config_2016_07_12_10_51_33.xml	2016/07/12 10:51:33 AM
☐	Generating Security Configuration	2016/07/01 07:10:29 AM

- 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=""

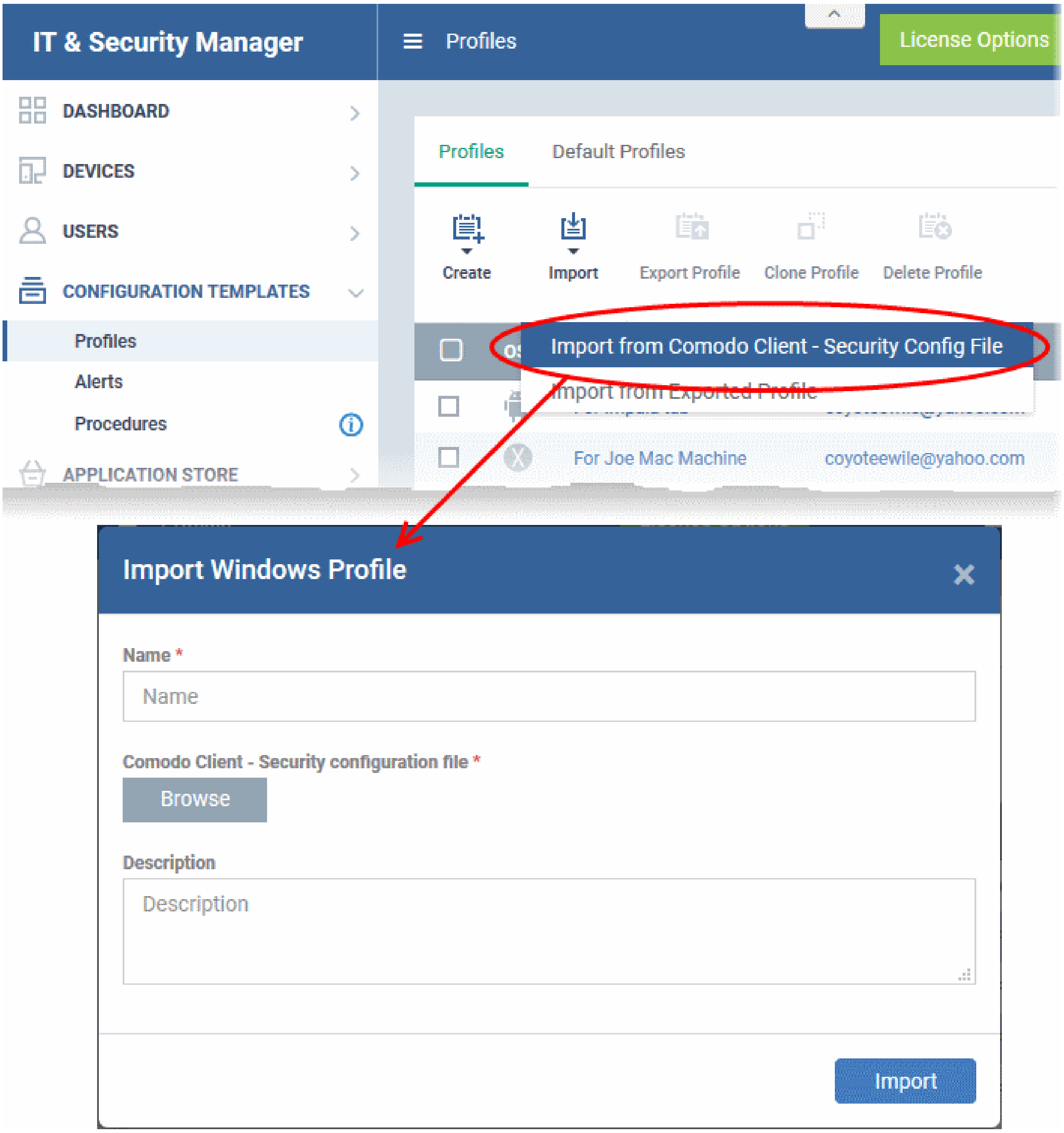
  For example, C:\Program Files\COMODO\COMODO Internet Security\cfpconfg.exe --xcfgExport="C:\winconfigprofile.xml" --filter=""

- 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).

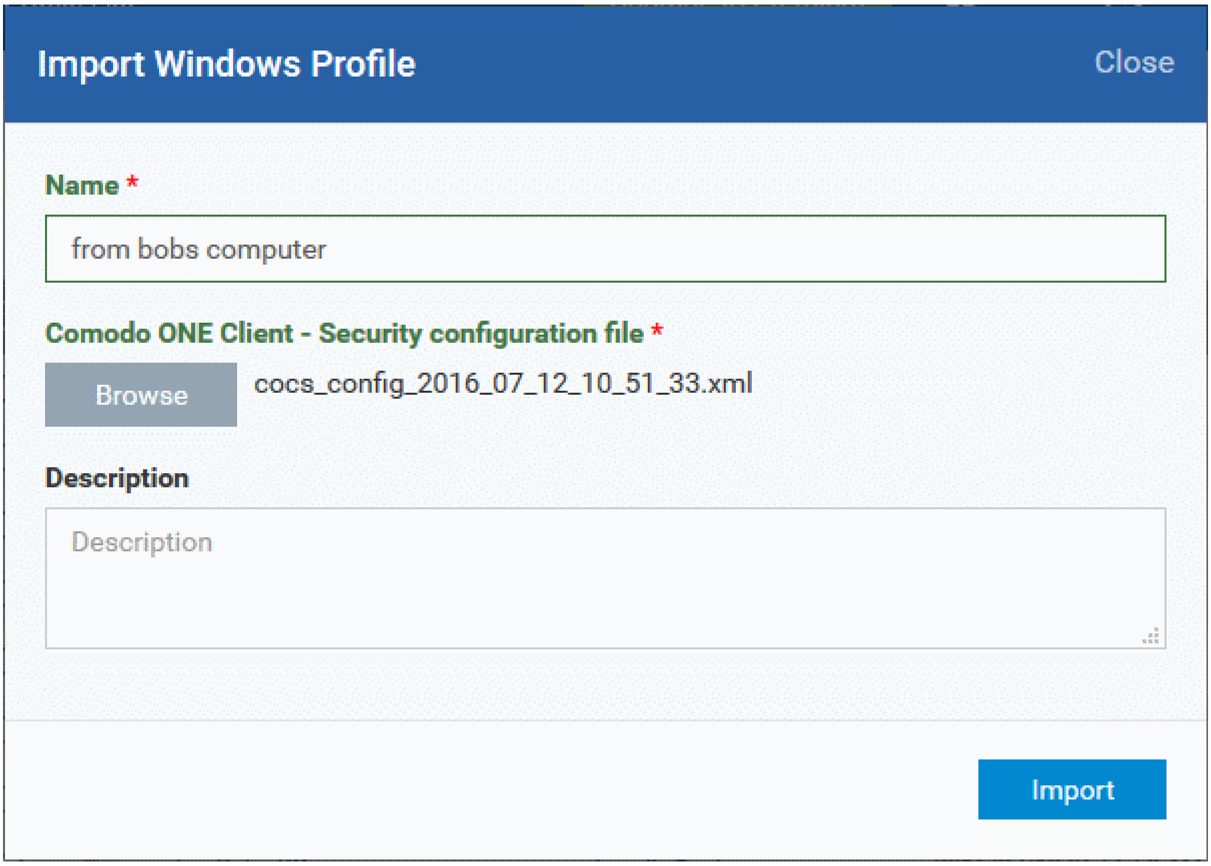
Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)

- 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'.



Import Windows Profile

Name *

from bobs computer

Comodo ONE Client - Security configuration file *

Browse cocs_config_2016_07_12_10_51_33.xml

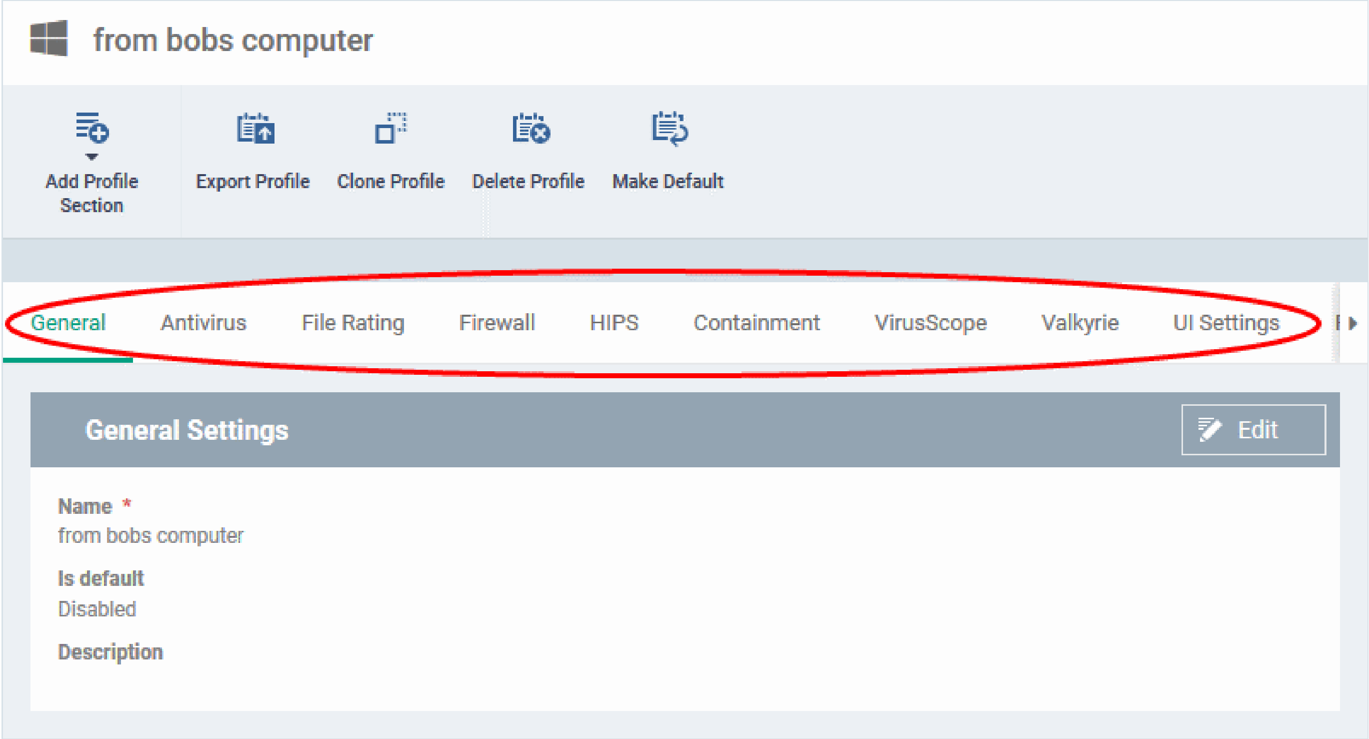
Description

Description

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.



from bobs computer

General Settings

Name *
from bobs computer

Is default
Disabled

Description

- 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 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. See **Creating Mac OS Profiles** for more details.
- Clone an existing profile and modify its settings as per your requirements. See **Cloning a Profile**, for more details on creating a new profile by Cloning a profile.

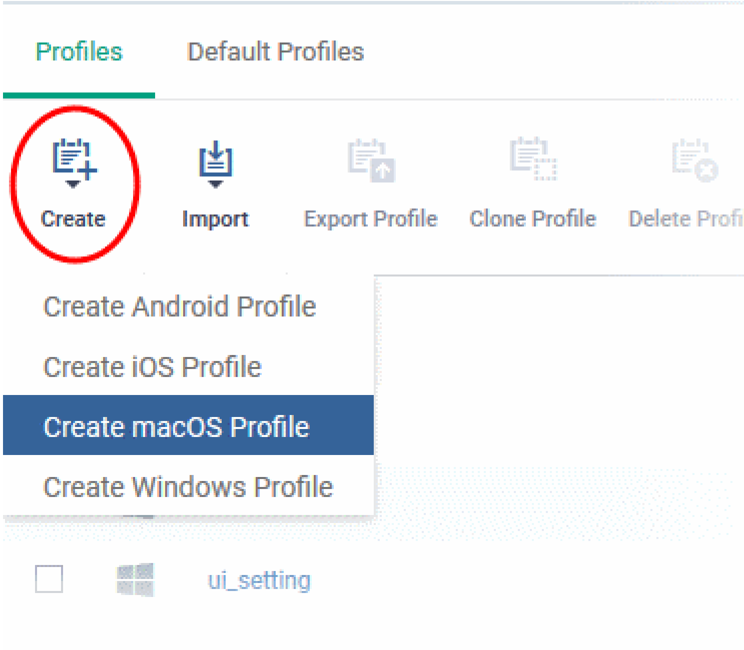
6.1.4.1. Create a Mac OS Profile

Process in brief:

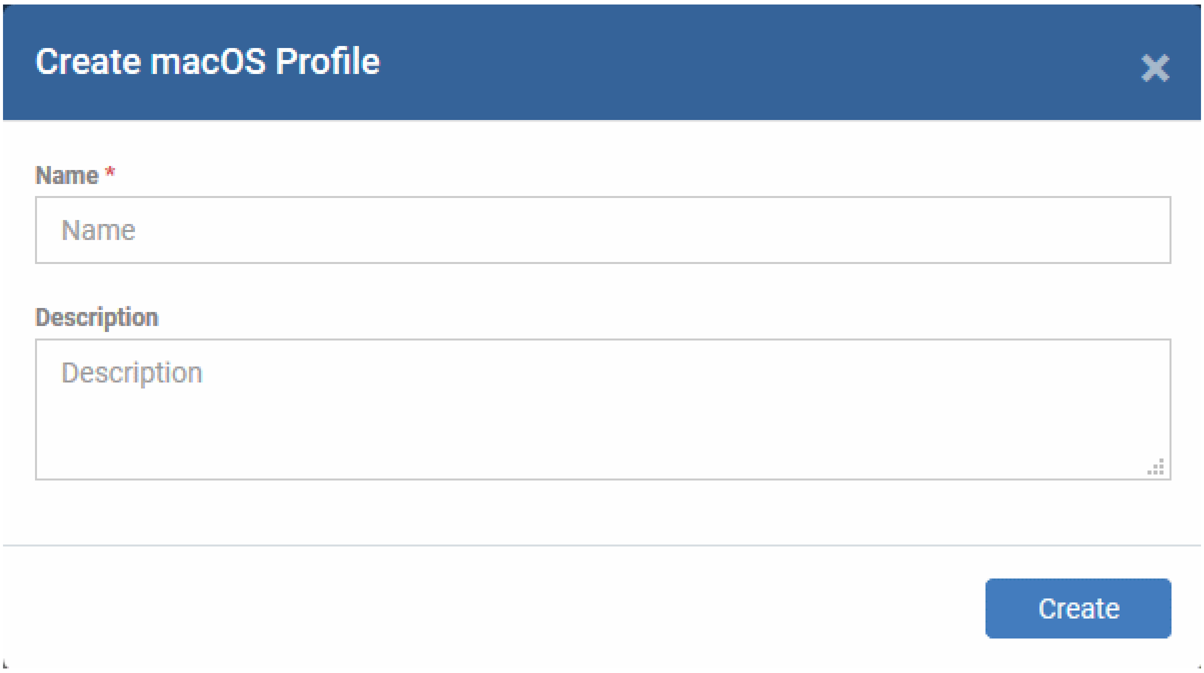
- Click 'Configuration Templates' on the left then choose 'Profiles'
- Click 'Create' then select 'Create Mac OS Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profiles' screen.
- New profiles have only one section - 'General'. You can configure settings for Comodo Antivirus and other items 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 Mac OS Profile'

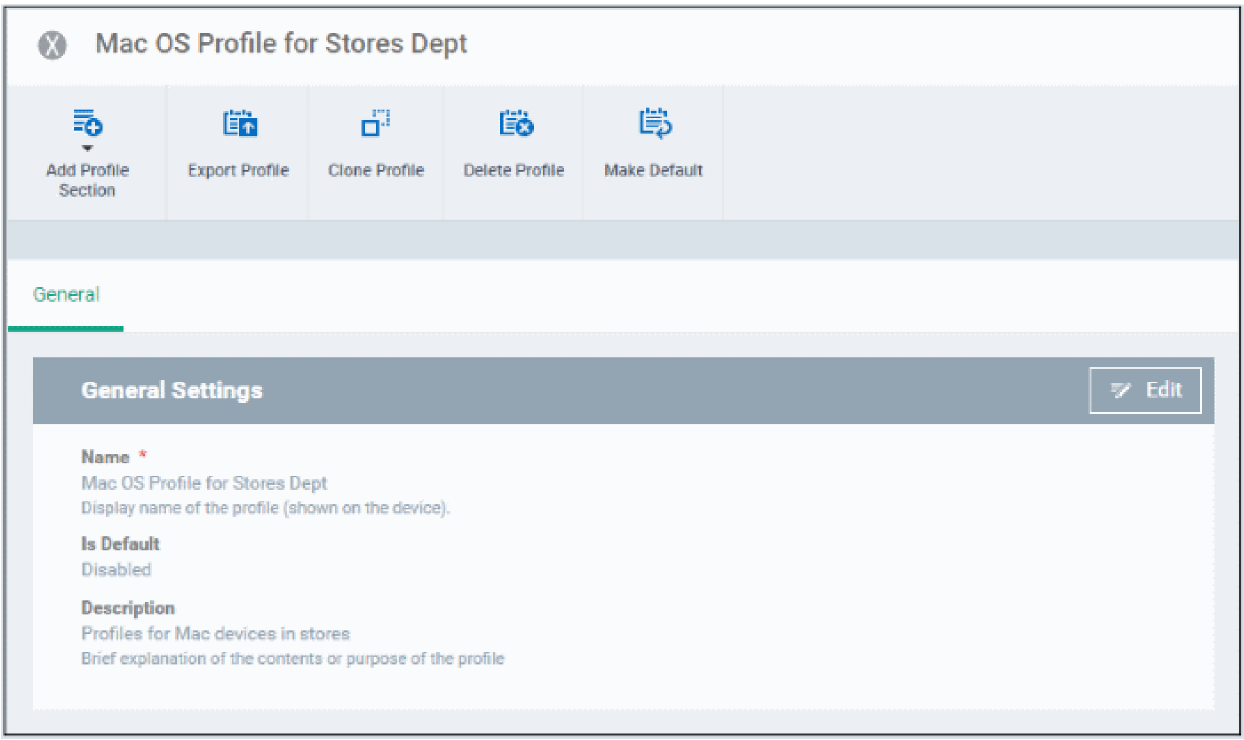


The 'Create Mac OS Profile' dialog will appear.



- 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.



Mac OS Profile for Stores Dept

Name *
Mac OS Profile for Stores Dept
Display name of the profile (shown on the device).

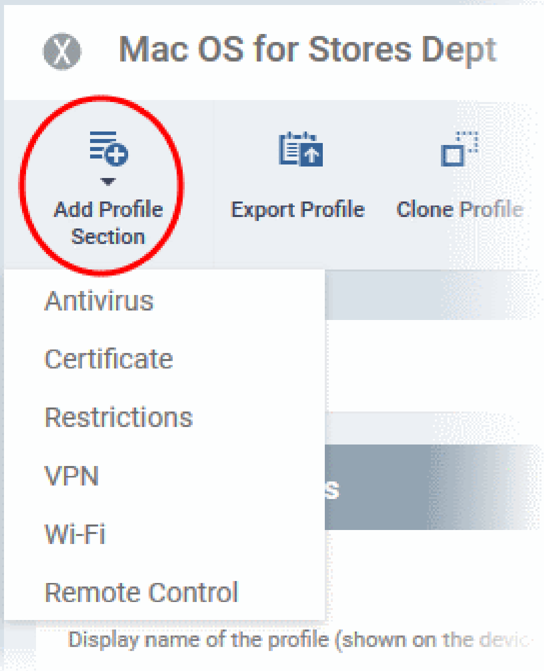
Is Default
Disabled

Description
Profiles for Mac devices in stores
Brief explanation of the contents or purpose of the profile

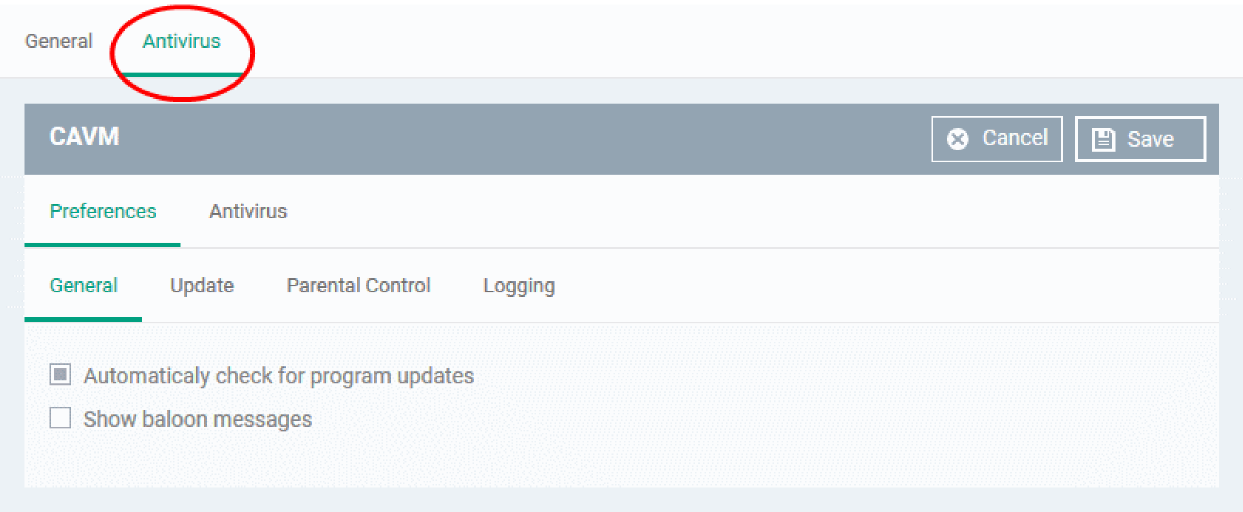
- If you want this profile to be a default policy, click the 'Make Default' button at the top. Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable the 'Is Default'.check box.
- Click 'Save'.

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.



☒ Automaticaly check for program updates

□ Show baloon messages

Following sections explain more about each of the settings:

- **Antivirus**
- **Certificate**
- **CCM Certificates**
- **Restrictions**
- **VPN**
- **Wi-Fi**
- **Remote control**

6.1.4.1.1. Antivirus Settings for Mac OS Profile

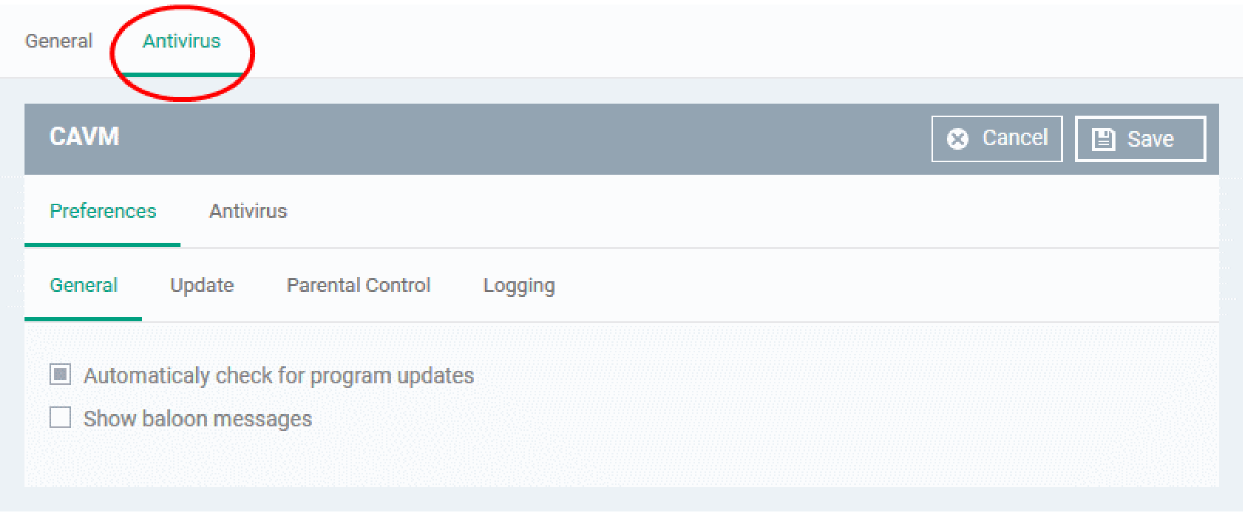
The antivirus settings screen has sub-sections that allow you to configure real-time scans custom scans, exclusions and more for the profile.

To configure Antivirus settings for Mac OS profile

- Click 'Configuration Templates' > 'Profiles'
- Click 'Add Profile Section' then 'Antivirus' (if you haven't yet added the AV section)

  OR
- Open the 'Antivirus' tab if it was already added.

The antivirus settings screen will open:



☒ Automaticaly check for program updates

□ Show baloon messages

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**

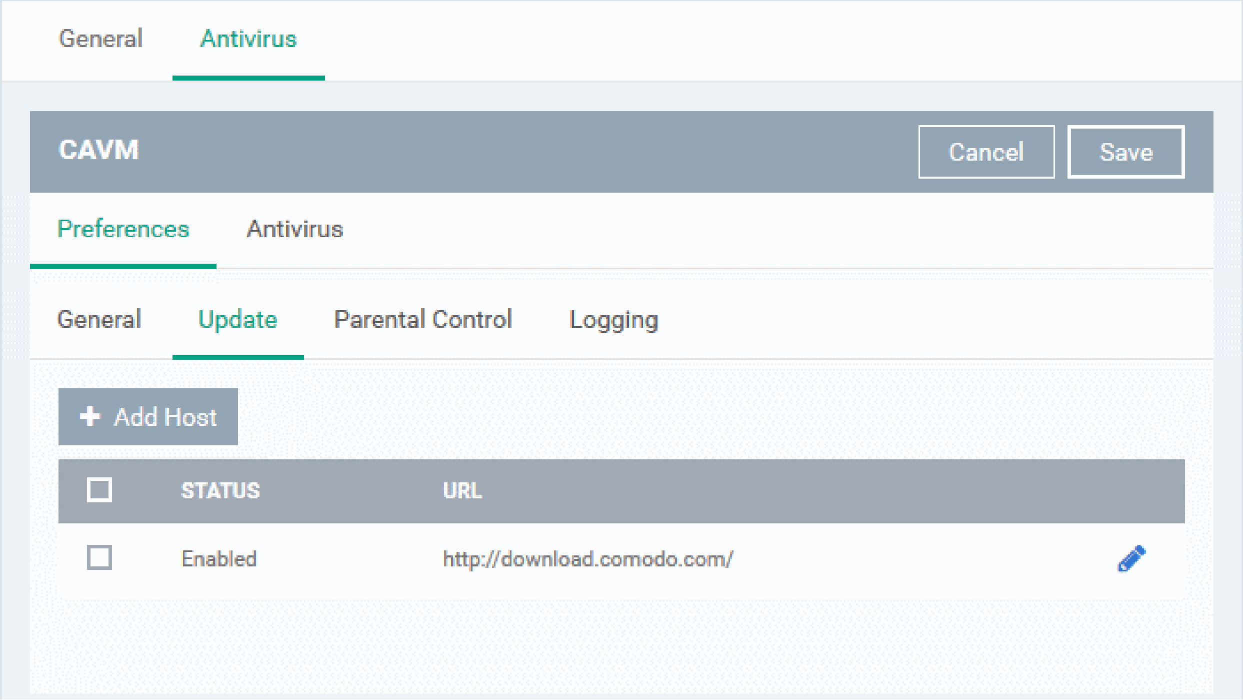
To configure general behavior settings

- 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'

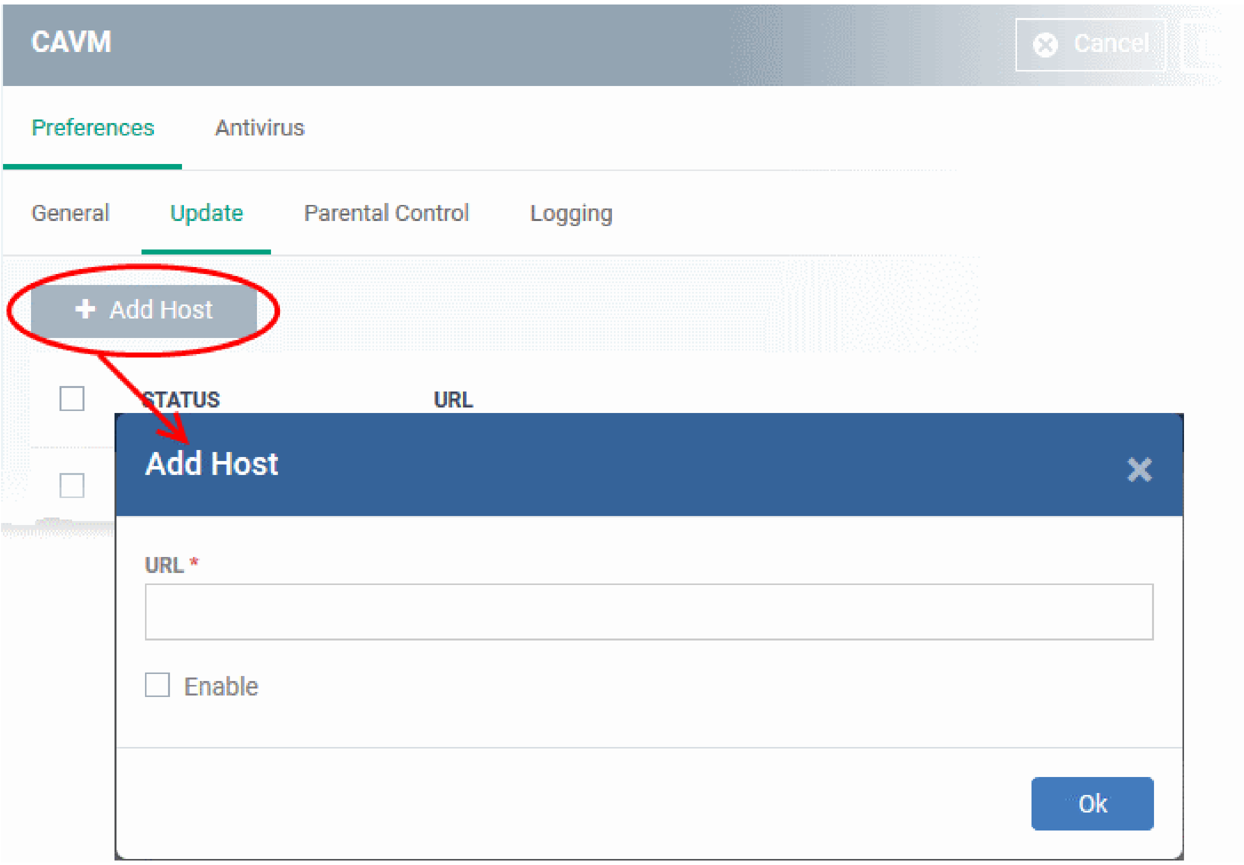


STATUS	URL
Enabled	http://download.comodo.com/

- 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'



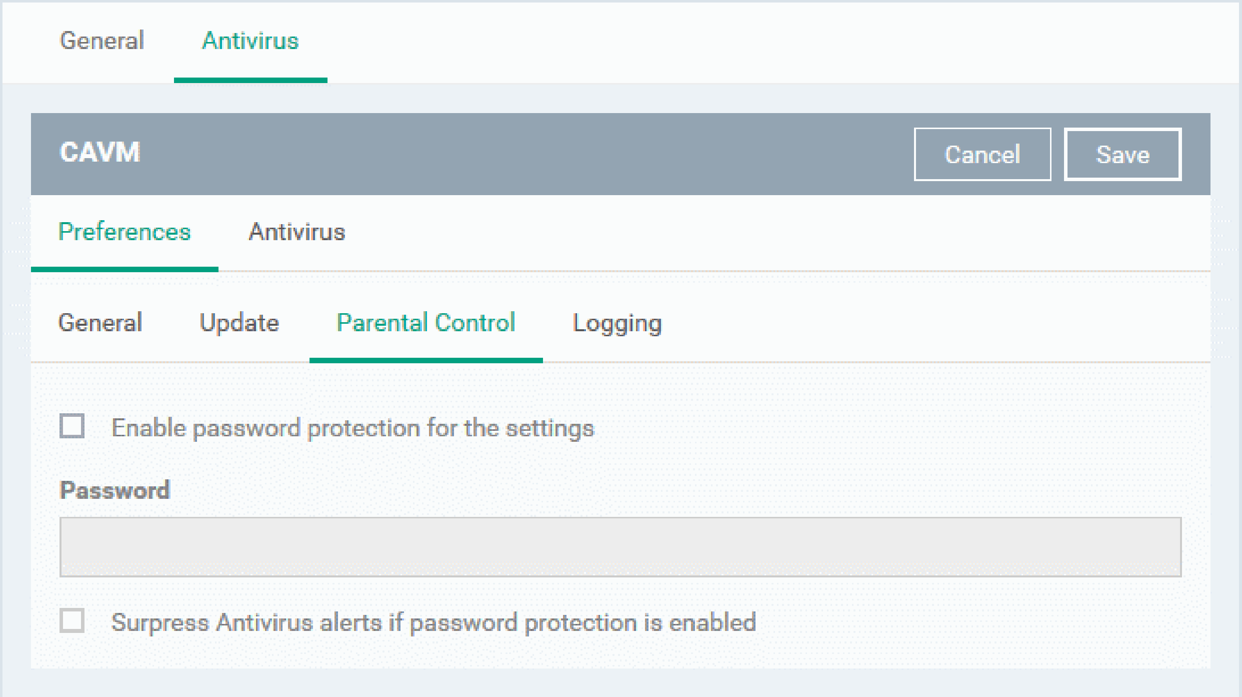
The 'Add Host' dialog will appear.

- 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

Password

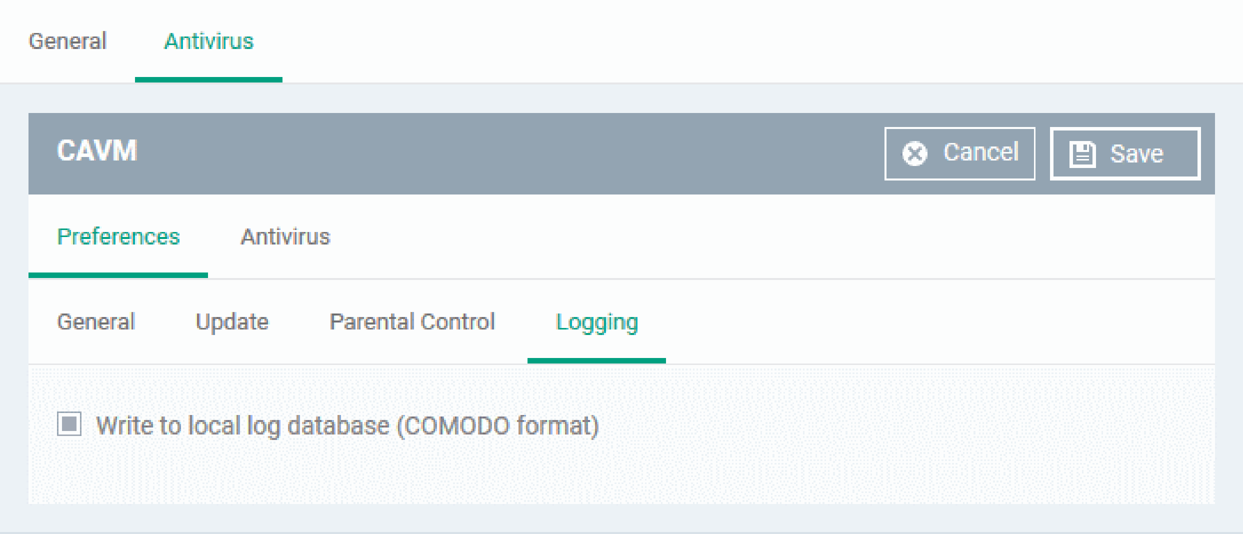
□ Surpress Antivirus alerts if password protection is enabled

- **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 alerts will be displayed.

  For example, a virus may be attempting to copy itself to a user's computer. 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, thus exposing the machine to risk.

To configure 'Log' settings

- Click the 'Logging' tab under 'Preferences'



■ Write to local log database (COMODO format)

By default, CAVM maintains 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, de-select 'Write to local log database (COMODO format)'.

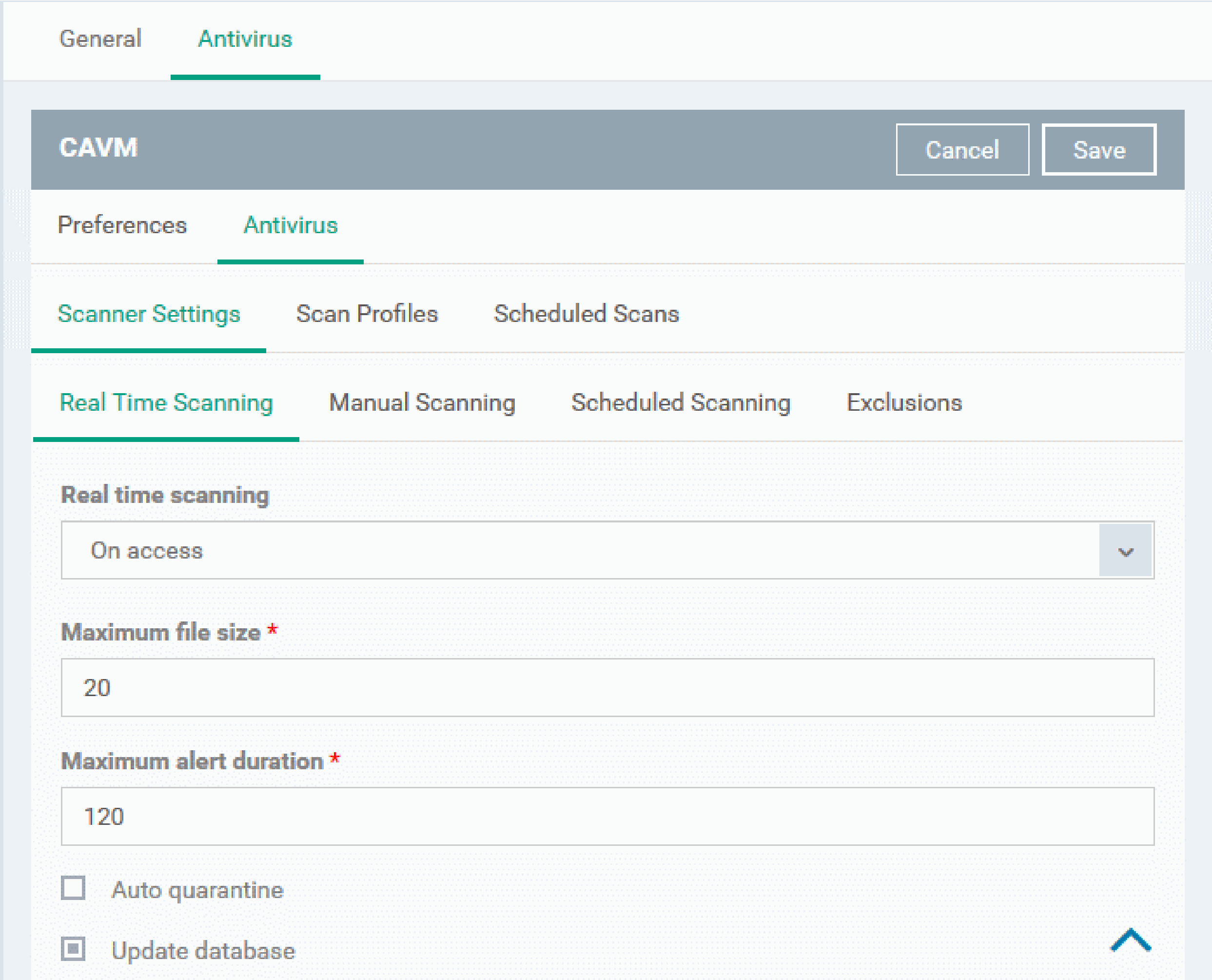
Configuring Antivirus Settings

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



Real time scanning: On access

Maximum file size *: 20

Maximum alert duration *: 120

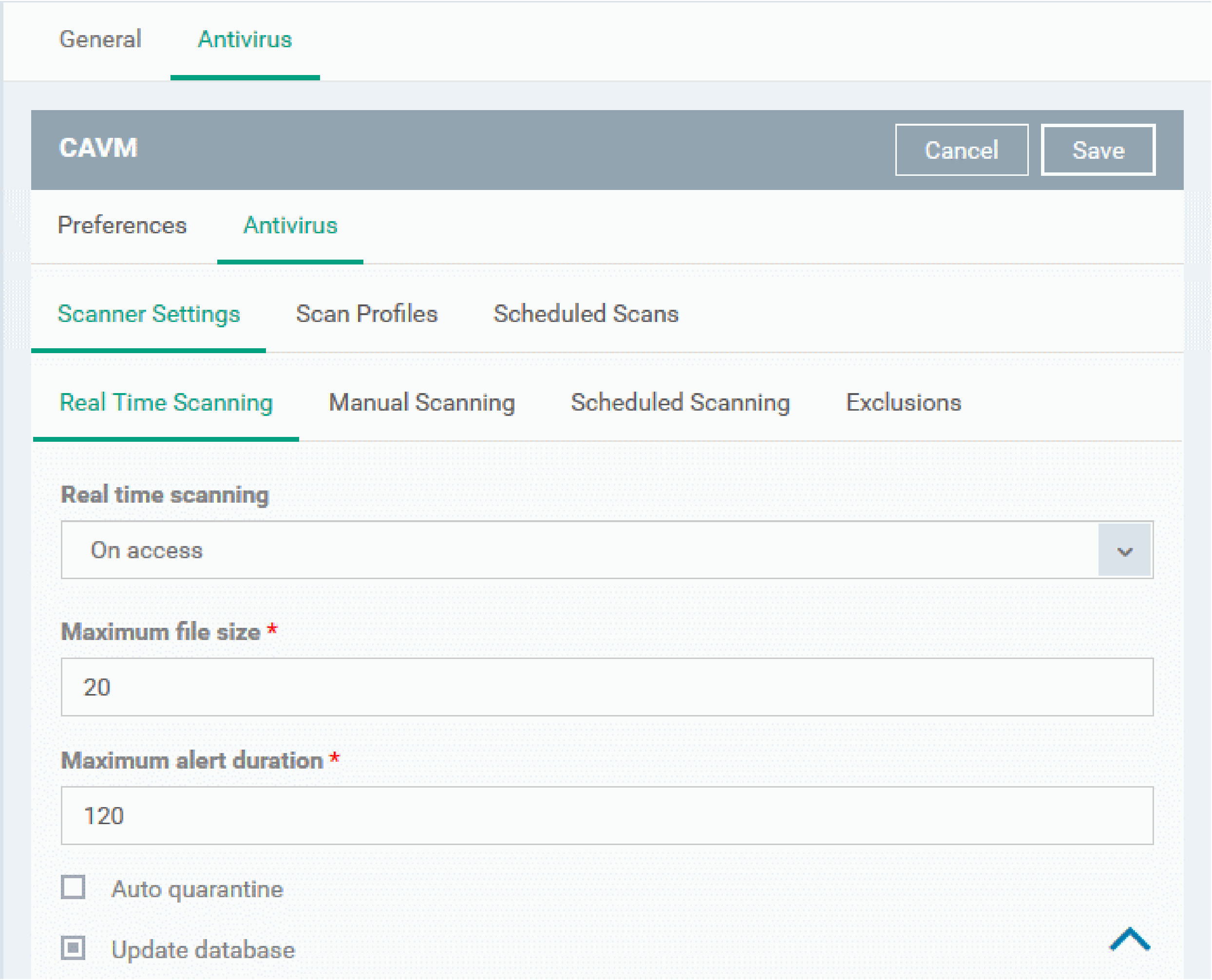
☐ Auto quarantine

▣ Update database

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

On access

Maximum file size *

20

Maximum alert duration *

120

□ Auto quarantine

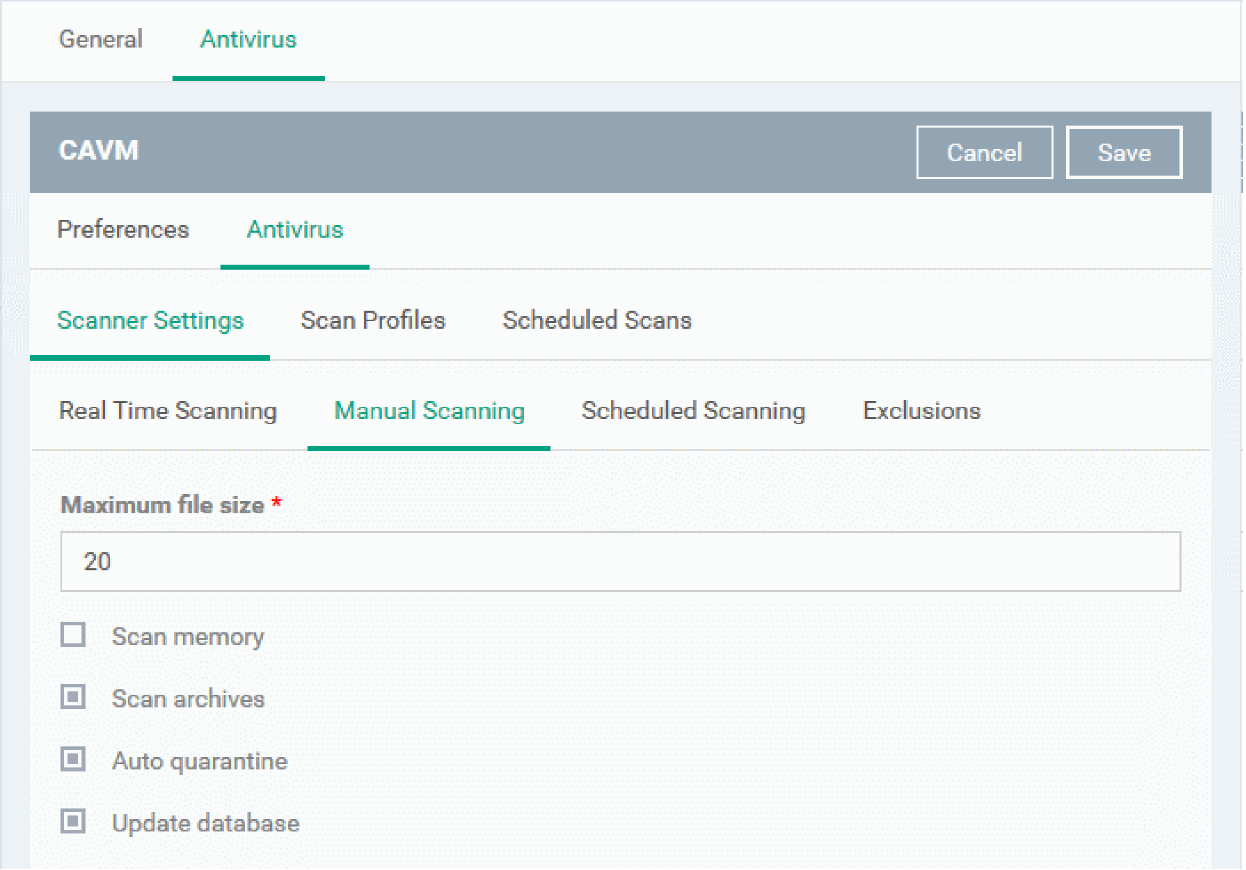
☒ Update database

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**.



Maximum file size *

20

□ Scan memory

▣ Scan archives

▣ Auto quarantine

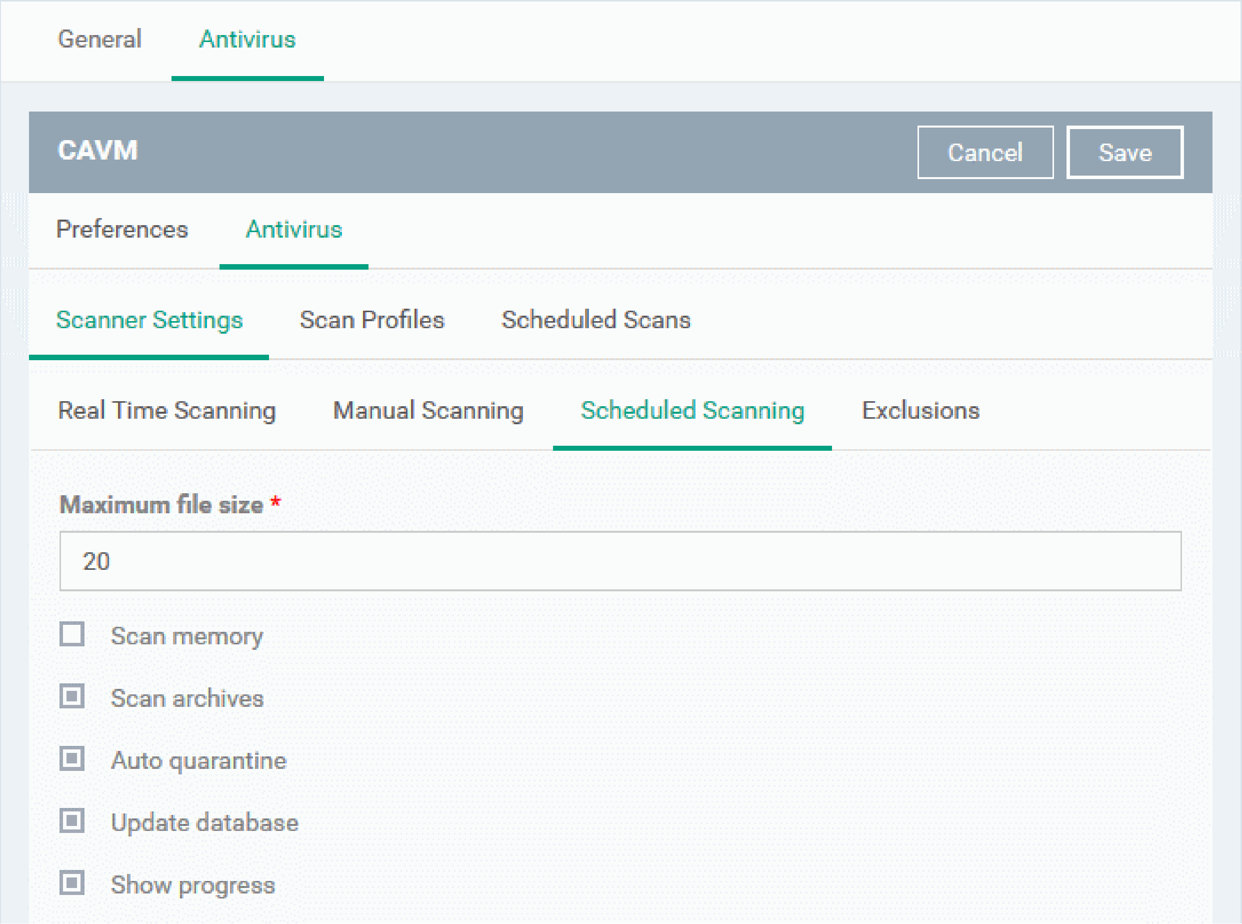
▣ Update database

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,

Manual Scanning Settings - Table of Parameters		
		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***).

- 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**'.



Maximum file size *

20

□ Scan memory

☑ Scan archives

☑ Auto quarantine

☑ Update database

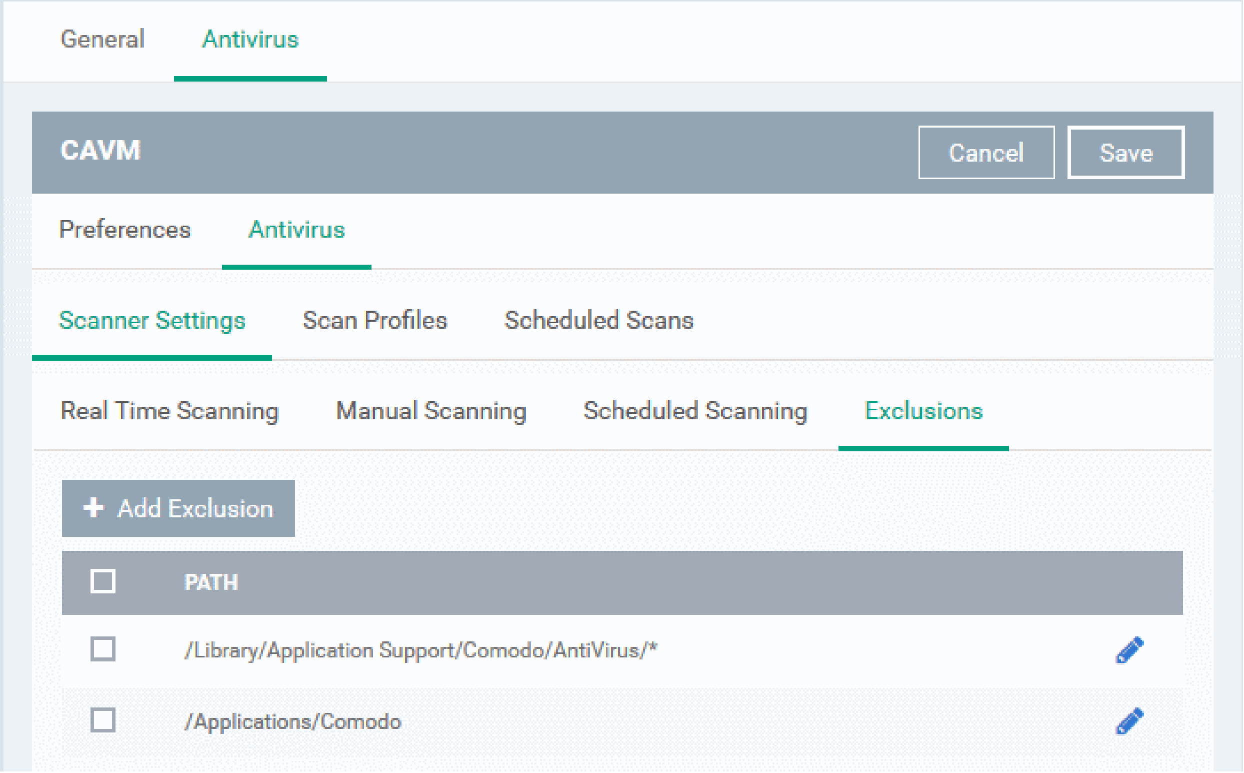
☑ Show progress

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***

Scheduled Scanning Settings - Table of Parameters		
		=20MB).
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'

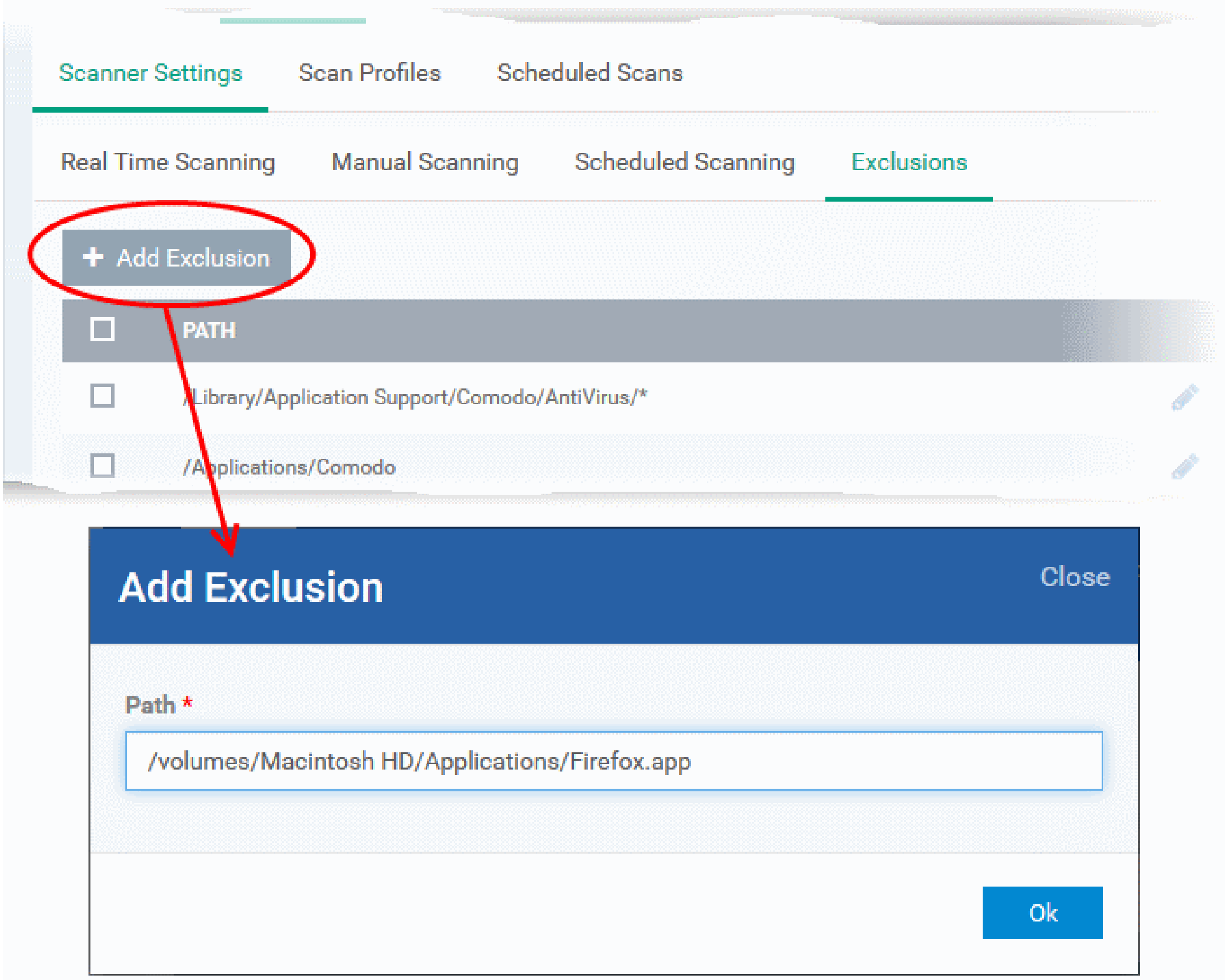
Tip: The 'Exclusions' Settings interface allows you to specify the items that should be excluded by the AV scanner. These files will be skipped during realtime, on-demand and scheduled scans.



□	PATH
□	/Library/Application Support/Comodo/AntiVirus/*
□	/Applications/Comodo

A list of excluded items will be displayed.

- Click 'Add Exclusion'

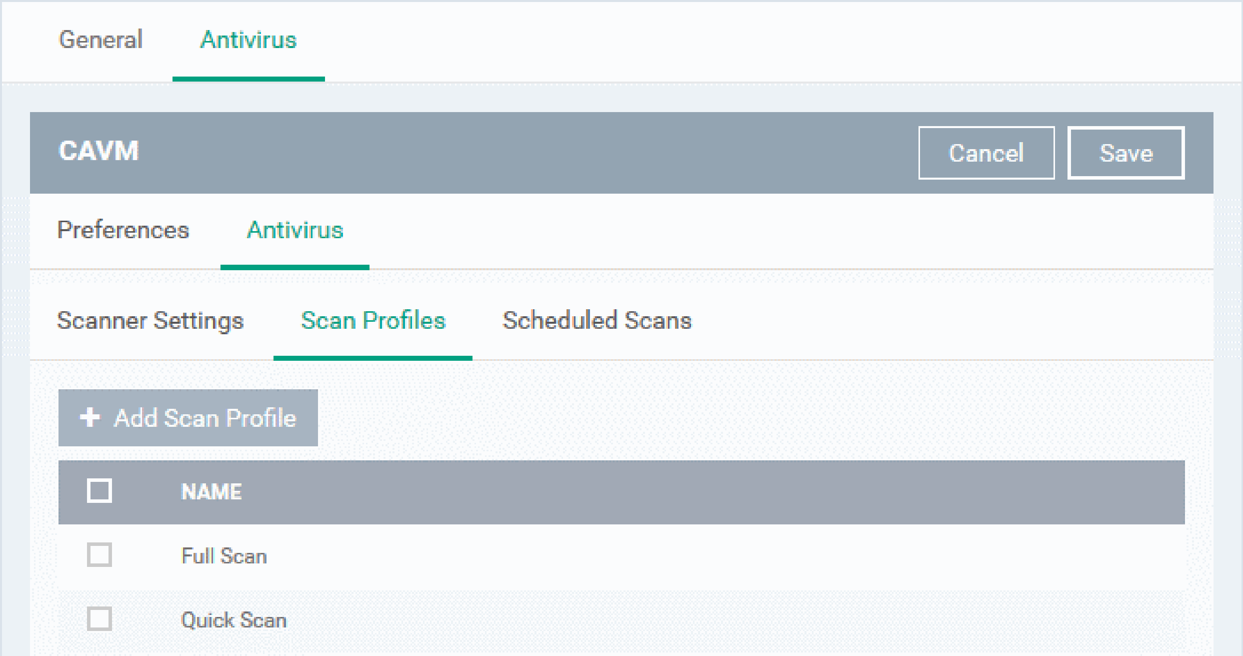


/volumes/Macintosh HD/Applications/Firefox.app

- 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

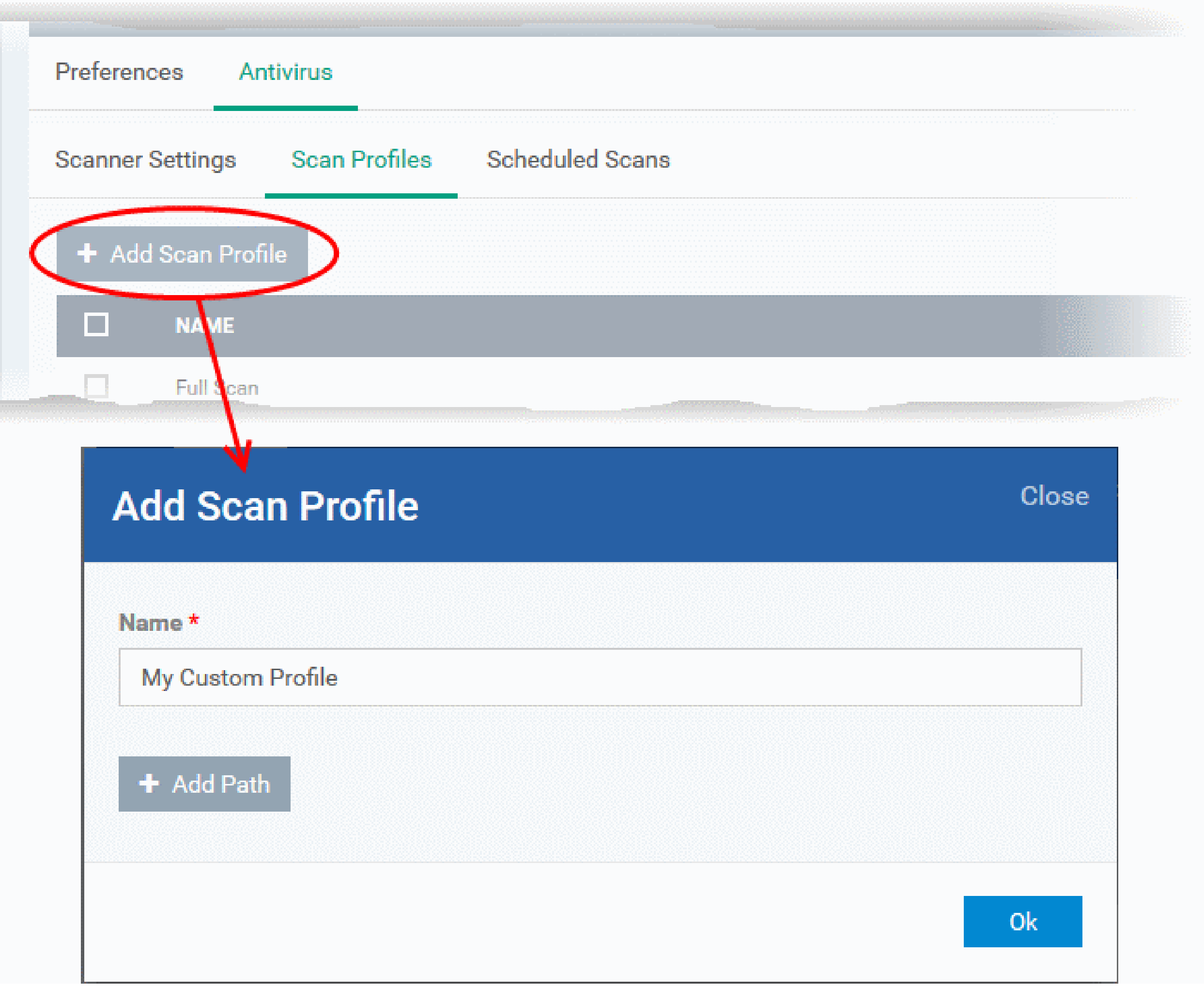
To create Scan Profiles click the 'Scan Profiles' tab under 'Antivirus'

> 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'

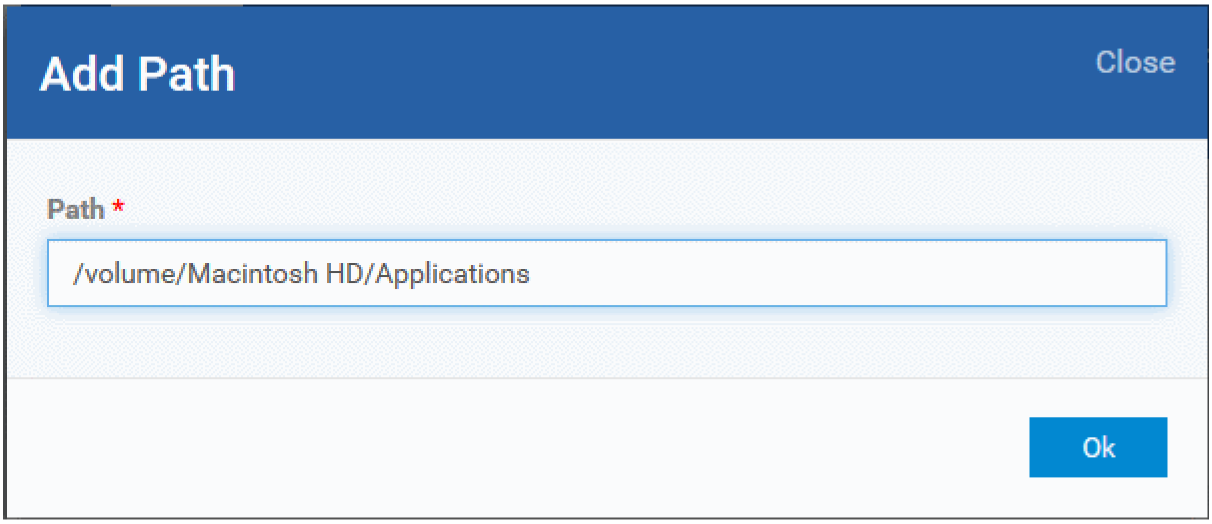


Name *: My Custom Profile

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

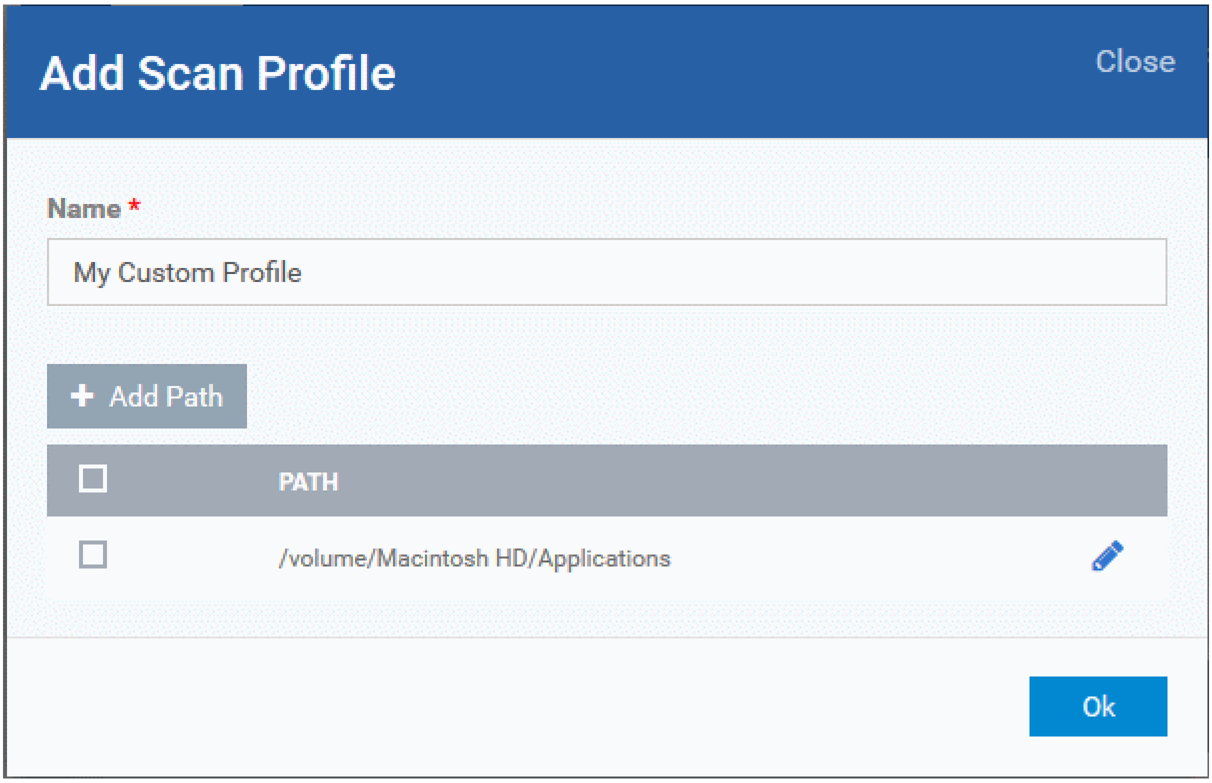


/volume/Macintosh HD/Applications

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.

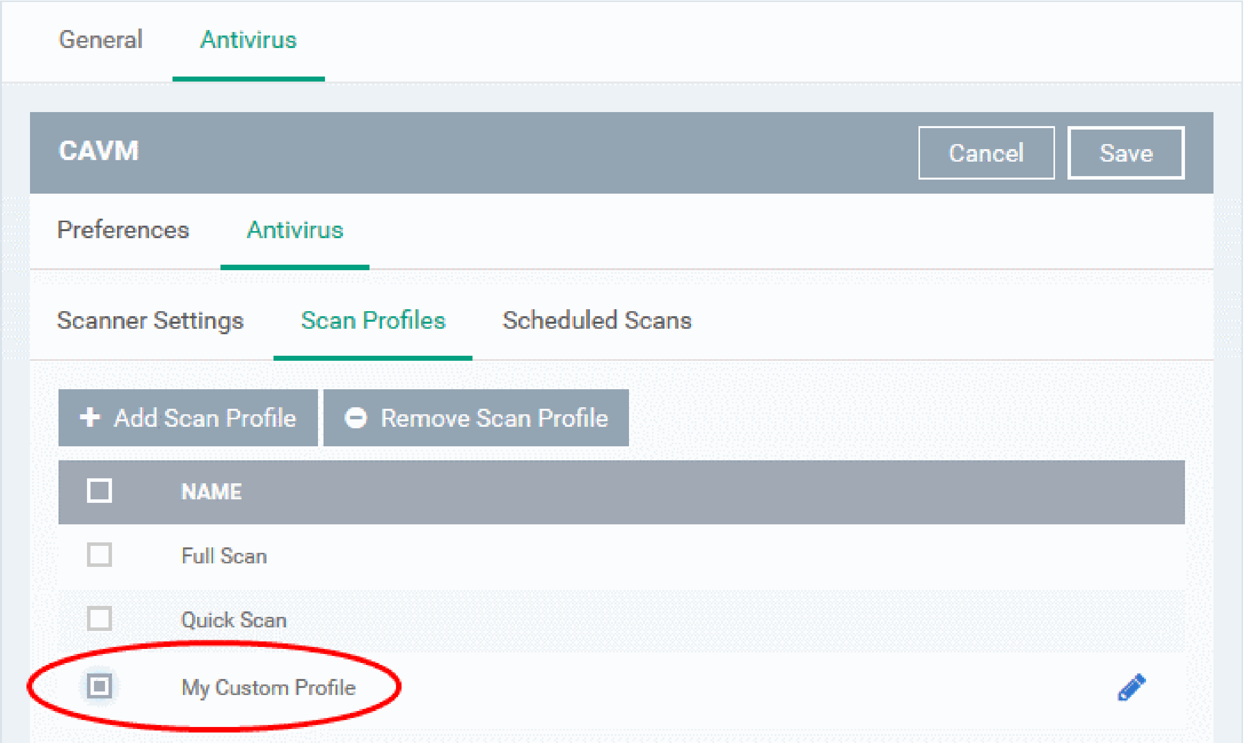


My Custom Profile

□	PATH
□	/volume/Macintosh HD/Applications

- 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'.



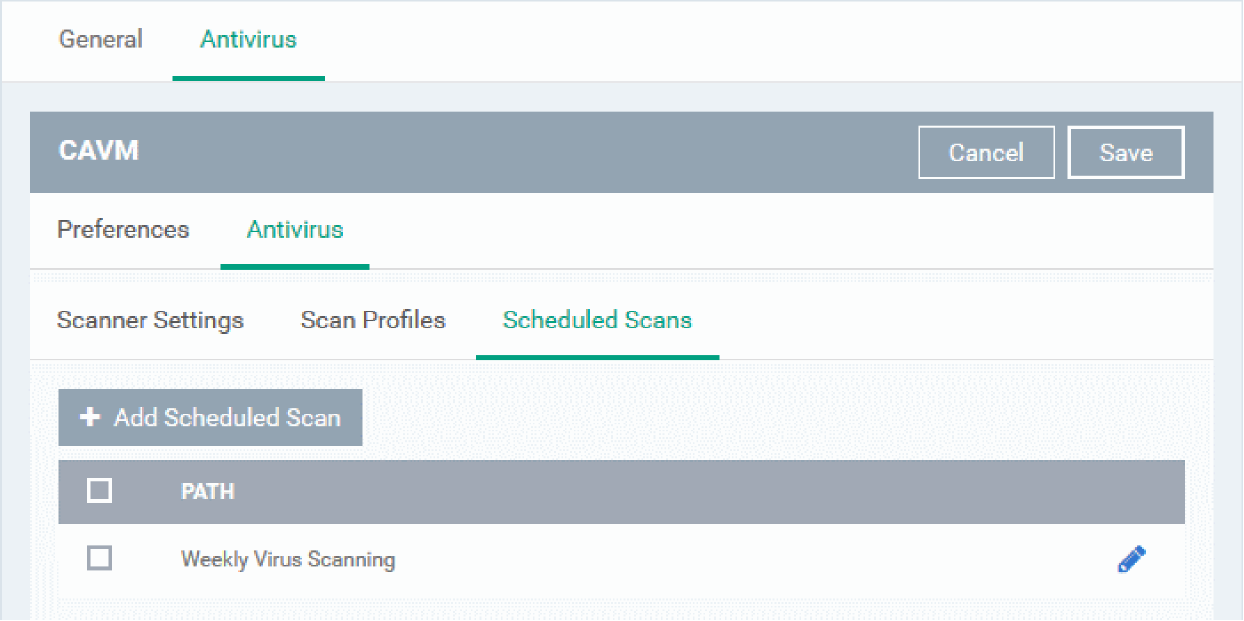
The custom profile will be added to the list.

- 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 customization 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.

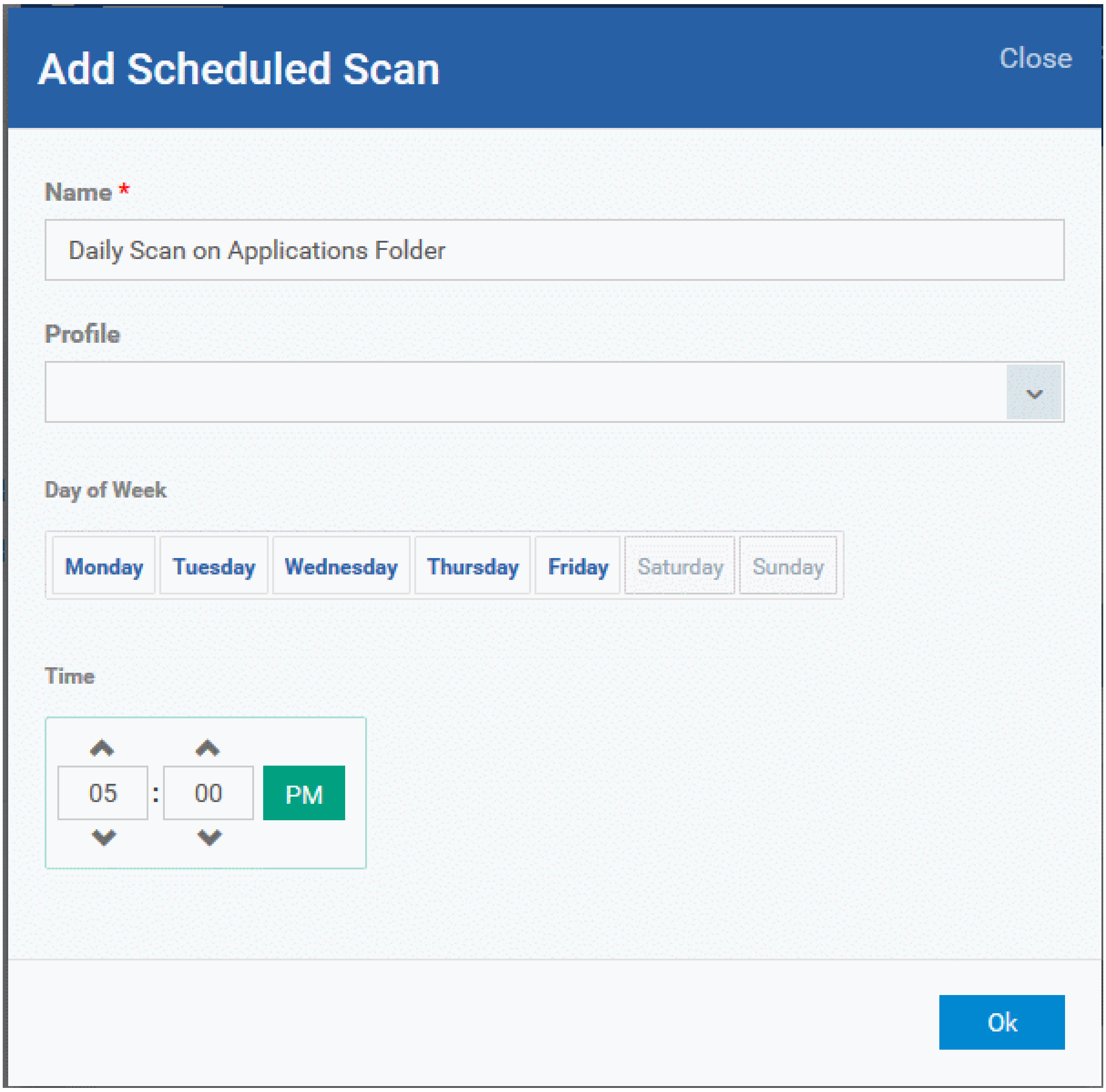
You can add any number of scheduled scans for a profile to run at a time that suits your preference. A scheduled scan may contain any profile of your choice.



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.



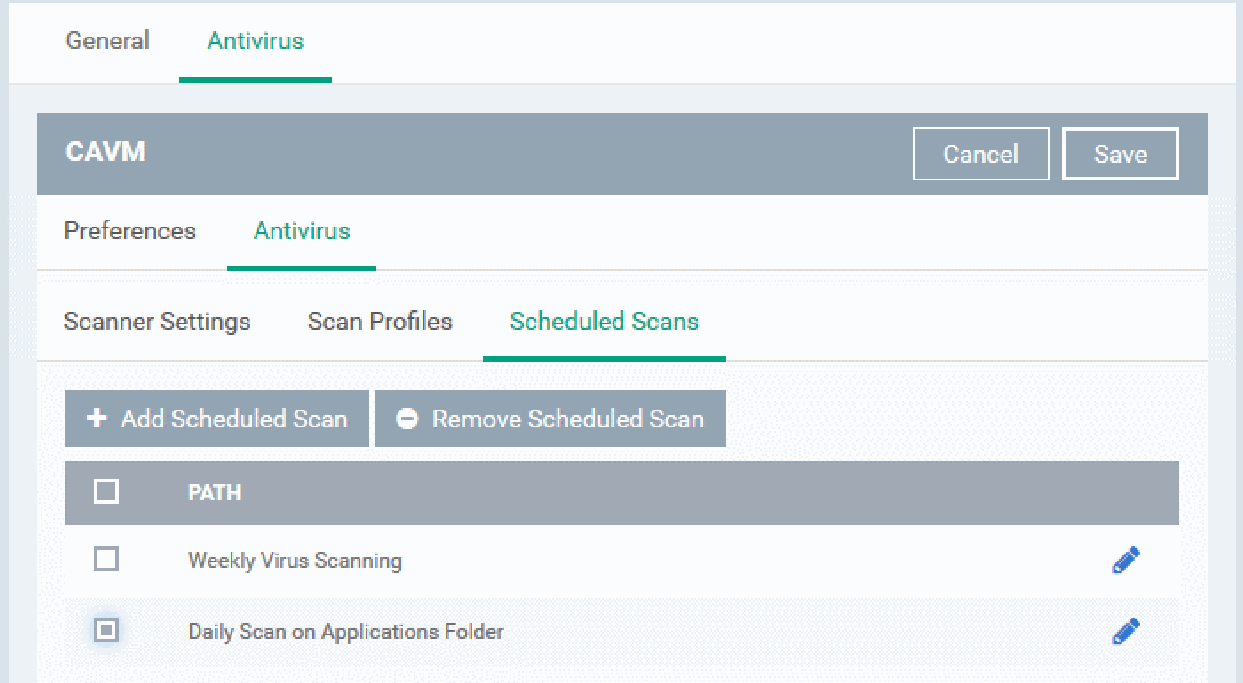
Name *: Daily Scan on Applications Folder

Time: 05 : 00 PM

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.



□	PATH
□	Weekly Virus Scanning
☑	Daily Scan on Applications Folder

- 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.

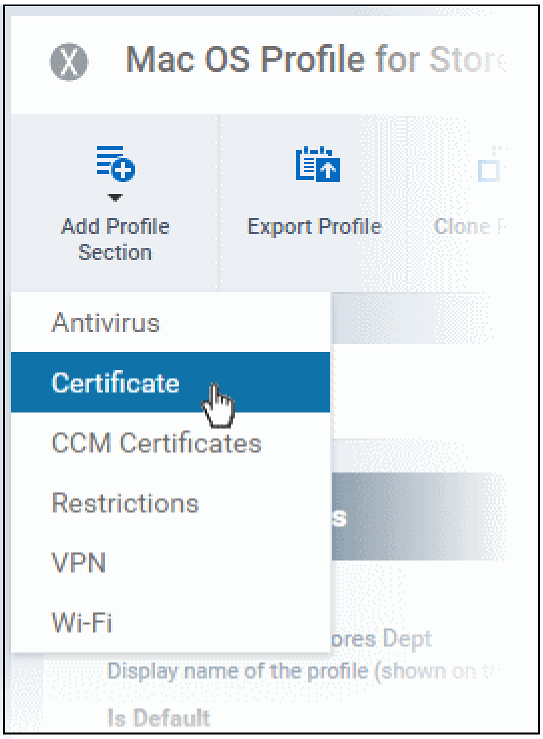
The settings will be saved and displayed under the 'Antivirus' tab. You can edit the settings or remove the section at anytime. Refer to the section **Editing Configuration Profiles** for more details.

6.1.4.1.2. Certificate Settings for Mac OS Profile

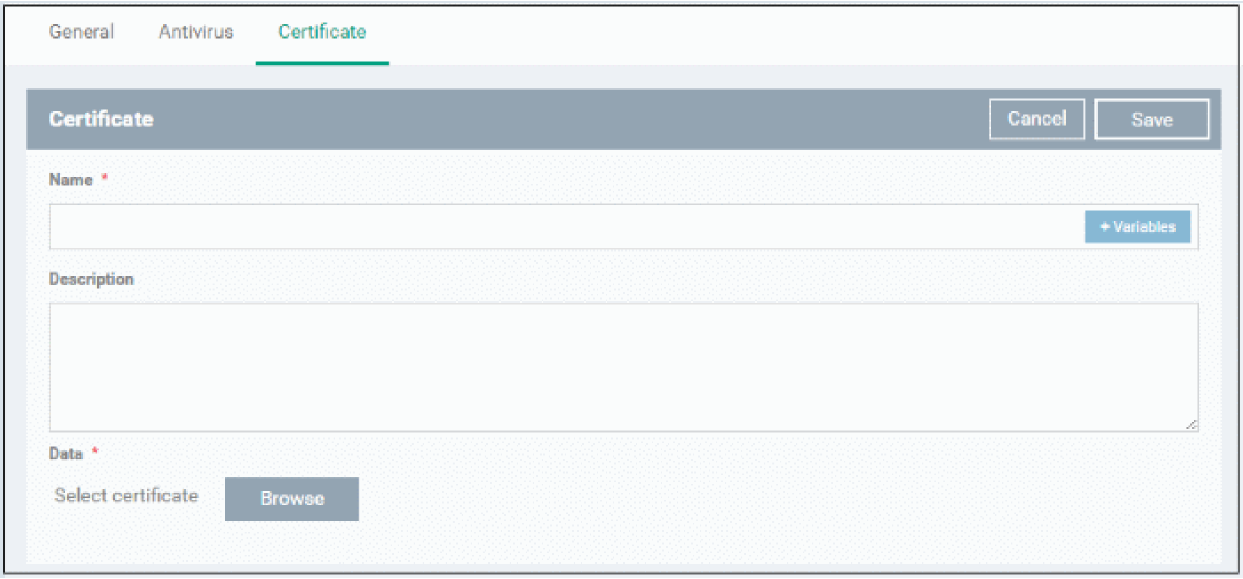
The 'Certificate Settings' section is used to upload certificates that can be selected for use in other settings such as 'Wi-Fi, 'Exchange Active Sync', 'VPN' and so on. You can also enroll user or device certificates from Comodo Certificate Manager (CCM) after activating your CCM account under Settings > Portal Set-Up > Certificates Activation.

To configure Certificate settings for Mac OS profile

- Choose 'Certificate' from the 'Add Profile Section' drop-down



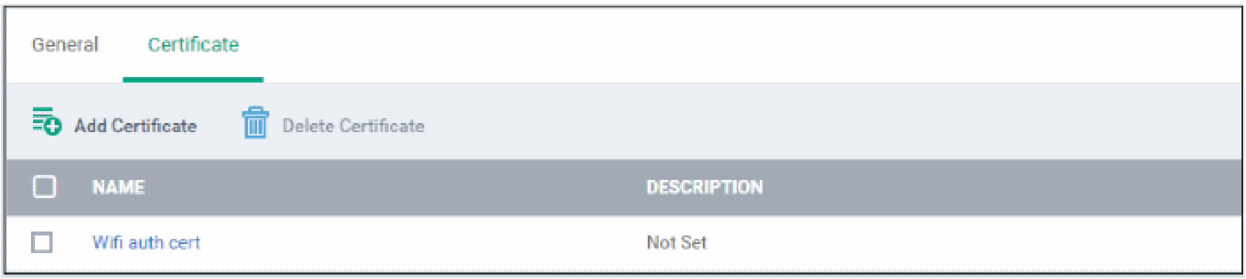
The 'Certificate' settings screen will be displayed.



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.



☐	NAME	DESCRIPTION
☐	Wifi auth cert	Not Set

- 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 Mac OS 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.

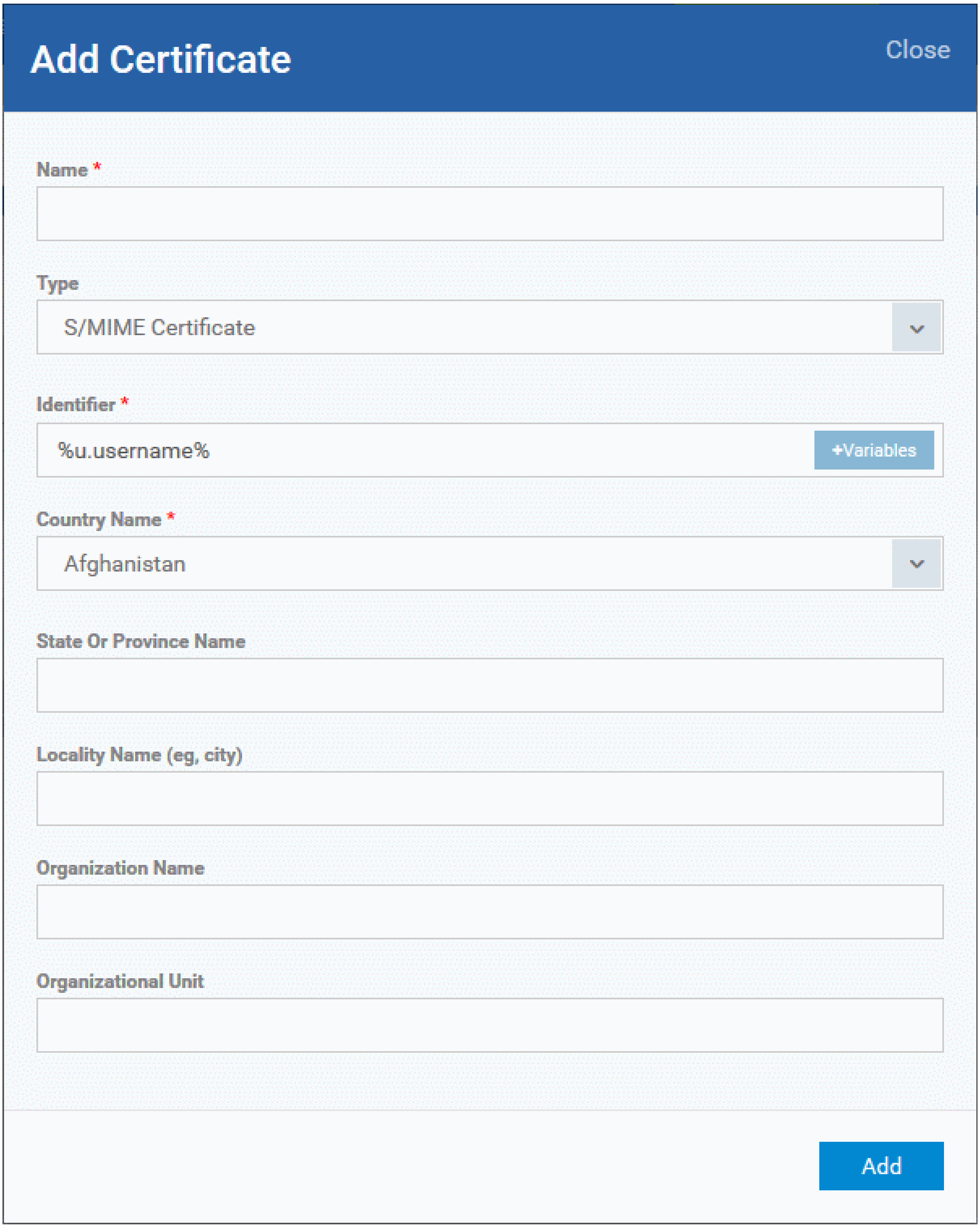
In addition to user authentication, client certificates can also be used for email signing and encryption (users will need to import the certificate to their email client).

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

Name *

Type: S/MIME Certificate

Identifier *: %u.username%

Country Name *: Afghanistan

State Or Province Name

Locality Name (eg, city)

Organization Name

Organizational Unit

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

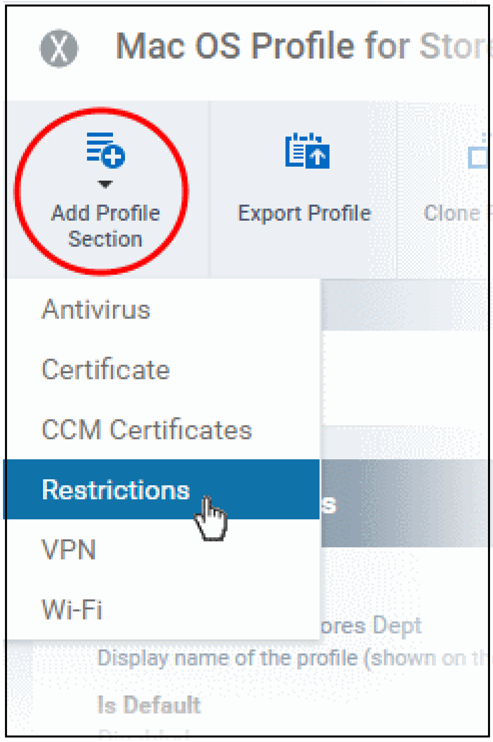
Certificate requests will be generated on the devices once the profile is applied to them.

6.1.4.1.4. Restrictions Settings for Mac OS Profile

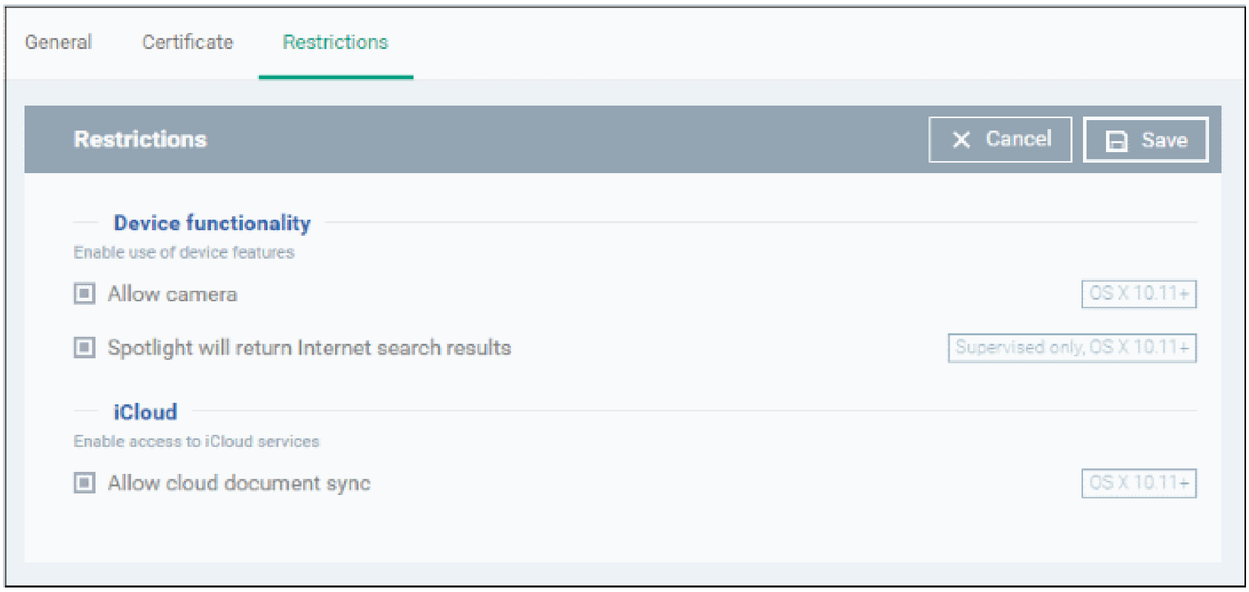
The 'Restrictions' section allows you to modify the profile to enable or disable selected device features:

To configure Restrictions settings

- Click 'Restrictions' from the 'Add Profile Section' drop-down



The 'Restrictions' settings screen will be displayed.



Device functionality

Enable use of device features

□ Allow camera — OS X 10.11+

□ Spotlight will return Internet search results — Supervised only, OS X 10.11+

iCloud

Enable access to iCloud services

□ Allow cloud document sync — OS X 10.11+

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, documents, emails, apps contacts and more on the device.

Restrictions Settings - Table of Parameters		
		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.

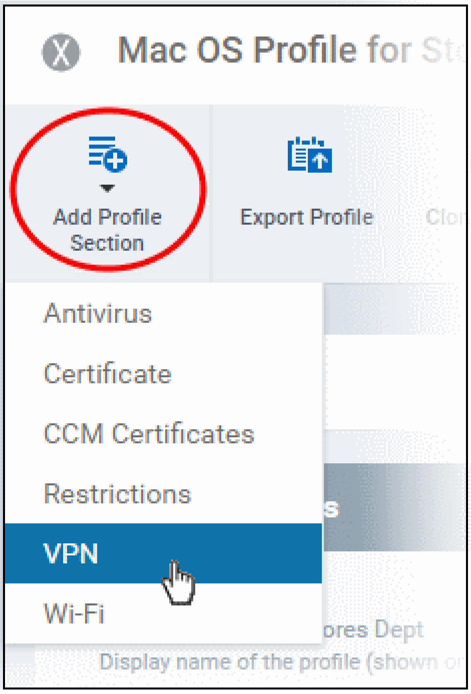
The saved 'Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.4.1.5. VPN Settings for Mac OS Profile

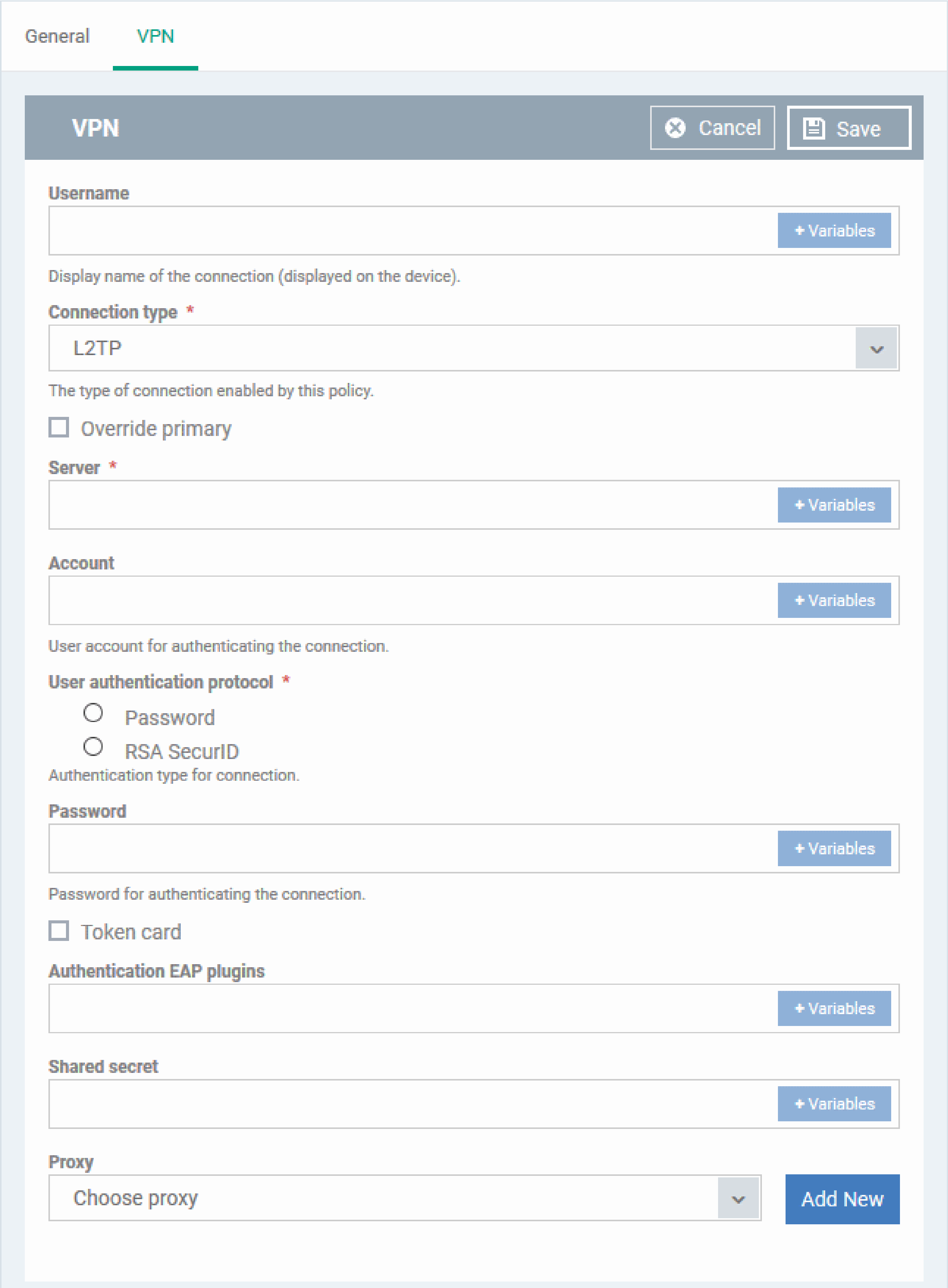
The 'VPN' section allows you to configure the VPN connection settings for the profile.

To configure VPN settings

- Click 'VPN' from the 'Add Profile Section' drop-down



The settings screen for VPN will be displayed.



Username

Display name of the connection (displayed on the device).

Connection type *

L2TP

The type of connection enabled by this policy.

□ Override primary

Server *

Account

User account for authenticating the connection.

User authentication protocol *

○ Password

○ RSA SecurID

Authentication type for connection.

Password

Password for authenticating the connection.

□ Token card

Authentication EAP plugins

Shared secret

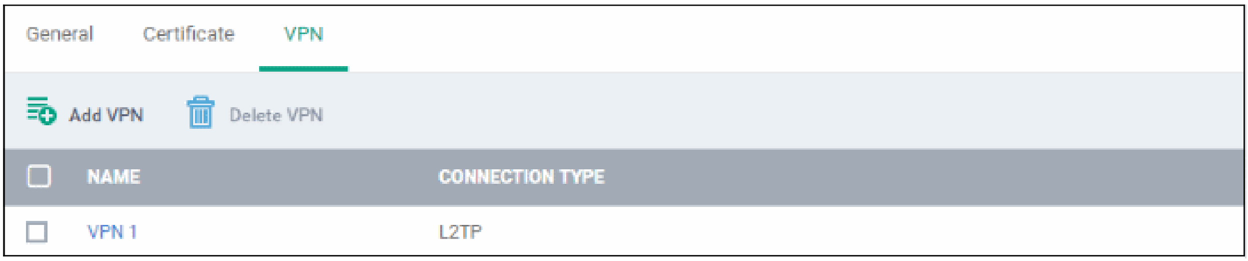
Proxy

Choose proxy

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.



☐	NAME	CONNECTION TYPE
☐	VPN 1	L2TP

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'

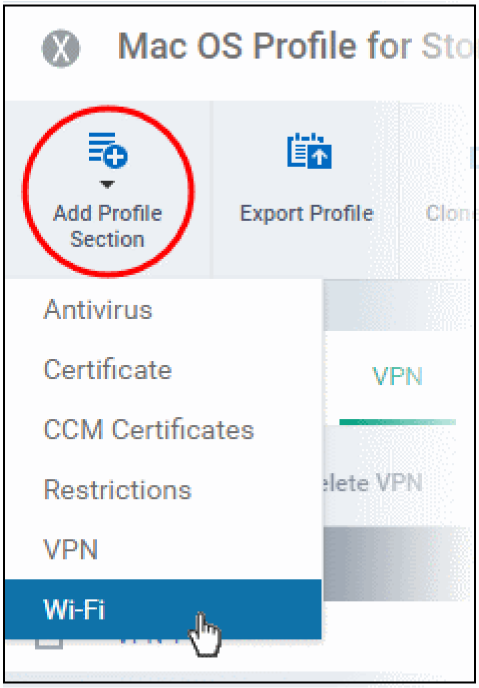
The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.4.1.6. Wi-Fi Settings for Mac OS Profile

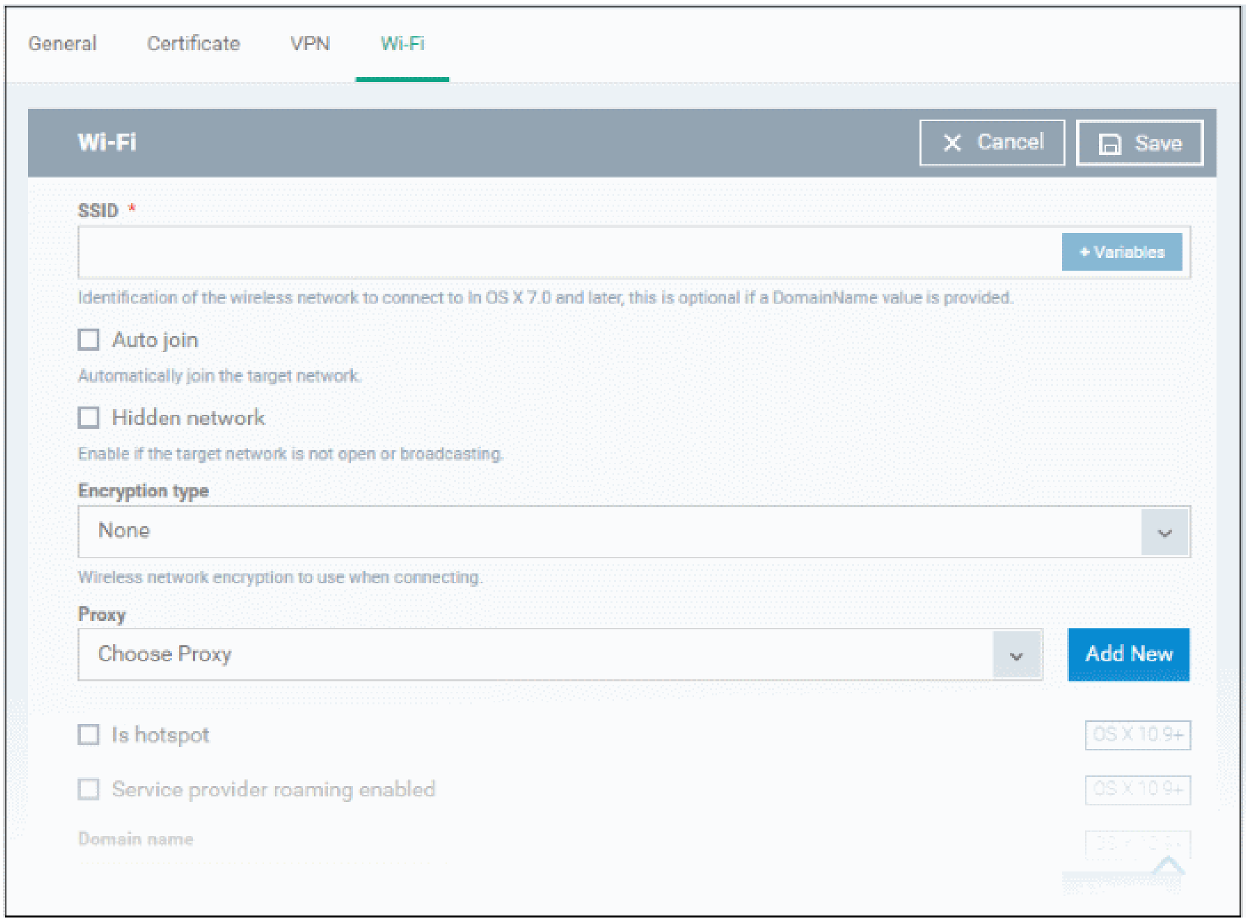
The 'Wi-Fi' section allows you to configure Wi-Fi connection settings for the profile.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Profile Section' drop-down



The 'Wi-Fi' settings screen will be displayed.



SSID *

+ Variables

Identification of the wireless network to connect to In OS X 7.0 and later, this is optional if a DomainName value is provided.

□ Auto join

Automatically join the target network.

□ Hidden network

Enable if the target network is not open or broadcasting.

Encryption type

None

Wireless network encryption to use when connecting.

Proxy

Choose Proxy

Add New

□ Is hotspot OS X 10.9+

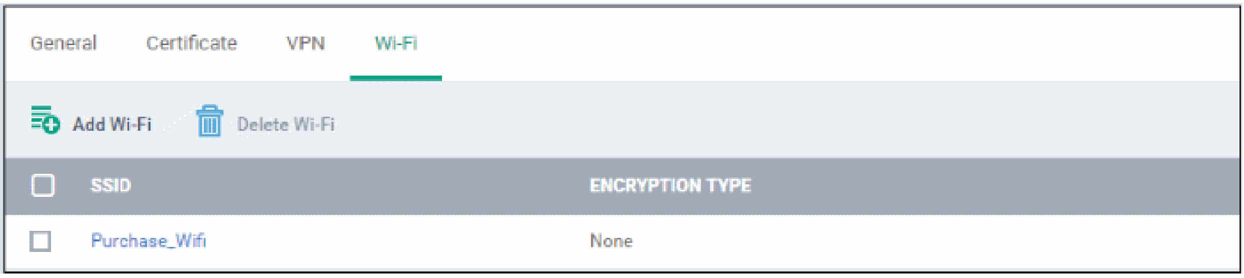
□ Service provider roaming enabled OS X 10.9+

Domain name

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.



□	SSID	ENCRYPTION TYPE
□	Purchase_Wifi	None

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.

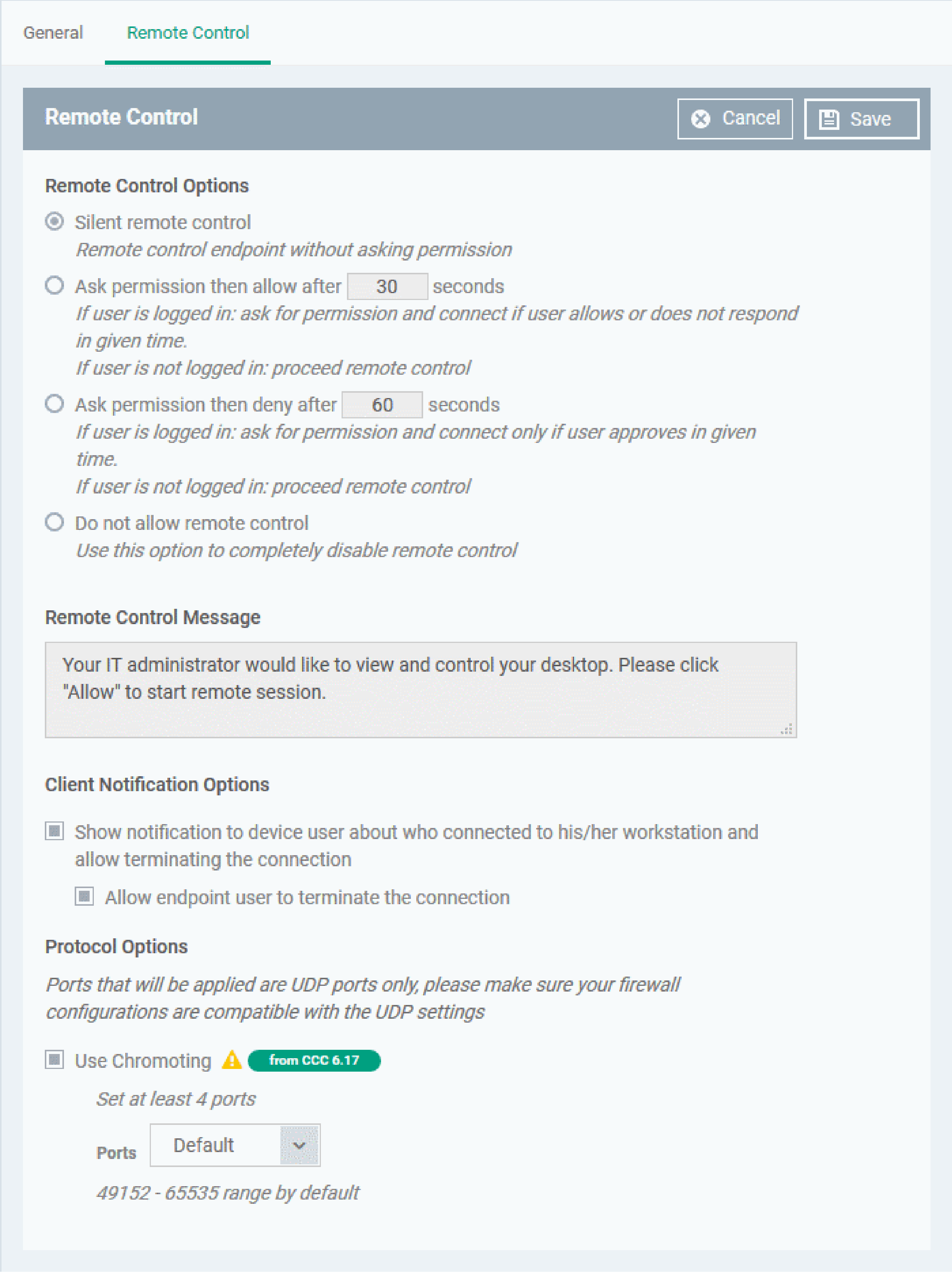
6.1.4.1.7. Remote control Settings for Mac OS Profile

- 'Remote Control' settings let you configure protocol used during remote control sessions.

- You can also customize the message which is shown to Mac OS end-users when you make a remote connection to their computer.
- See **Remote Management of Windows and Mac OS Devices** if you need help to setup the remote control service.

To configure Remote Control Settings for MAC OS

- Click 'Configuration Templates' > 'Profiles'
- Select a Mac OS profile that you want to configure
- Click 'Add Profile Section' at the top and choose 'Remote Control' from the drop-down.
    - Note: If 'Remote Control' is not in the 'Add...' menu then it has already been added to the profile.
- The 'Remote Control' tab will open:



General | Remote Control

Remote Control

Remote Control Options

● Silent remote control
Remote control endpoint without asking permission

○ Ask permission then allow after 30 seconds
If user is logged in: ask for permission and connect if user allows or does not respond in given time.
If user is not logged in: proceed remote control

○ Ask permission then deny after 60 seconds
If user is logged in: ask for permission and connect only if user approves in given time.
If user is not logged in: proceed remote control

○ Do not allow remote control
Use this option to completely disable remote control

Remote Control Message

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

☒ Show notification to device user about who connected to his/her workstation and allow terminating the connection

☒ Allow endpoint user to terminate the connection

Protocol Options

Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings

☒ Use Chromoting ⚠ from CCC 6.17

Set at least 4 ports

Ports: Default

49152 - 65535 range by default

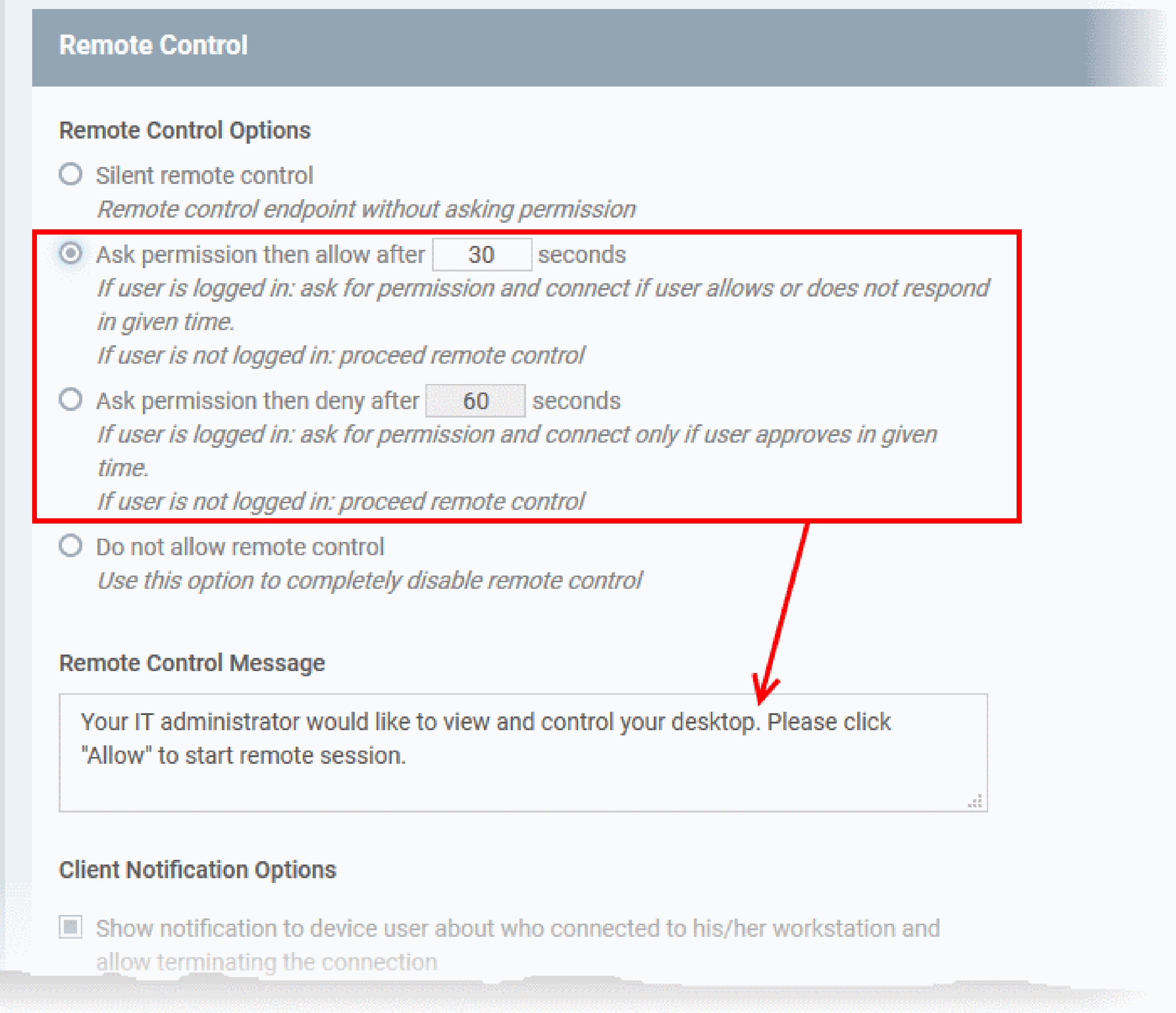
Remote Control Options:

- Silent remote control -The remote connection will start without requesting permission from the user.
- Ask permission then allow after NN seconds:
  - A message will be shown to the user which requests them to accept the connection. The connection will be automatically established if the user does not respond within the specified time.

  - Specify the timeout period (in seconds) in the text box
- Ask permission then deny after NN seconds:
  - A message will be shown to the user which requests them to accept the connection. The connection attempt will be terminated automatically if the user does not respond within the specified time.
  - Specify the timeout period (in seconds) in the text box.
- Do not allow remote control**:** Disable the ability to take remote control of the endpoint.

Remote Control Message

- Enter the text of the request message. For example, 'Your administrator would like to take control of your desktop. Click 'Allow' to accept the connection request.'
  - Please note that you can enter the message only if you choose the second or third notification options.



Remote Control

Remote Control Options

○ Silent remote control
Remote control endpoint without asking permission

● Ask permission then allow after 30 seconds
If user is logged in: ask for permission and connect if user allows or does not respond in given time.
If user is not logged in: proceed remote control

○ Ask permission then deny after 60 seconds
If user is logged in: ask for permission and connect only if user approves in given time.
If user is not logged in: proceed remote control

○ Do not allow remote control
Use this option to completely disable remote control

Remote Control Message

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

☑ Show notification to device user about who connected to his/her workstation and allow terminating the connection

Client Notification Options

This area lets you configure the notification box which is shown on the endpoint when a remote session is active:

- Show notification to device user about who connected to his/her workstation and allow terminating the connection - Let the end user know which ITSM user is connected to their machine.
  - Allow endpoint user to terminate the connection - Choose whether the 'End Session' button should be shown in the notification box or not. If enabled, the end-user will be able to close the connection.

Protocol Options

These settings let you choose the protocol used to connect to Mac OS devices.

- These settings apply to CRC version 6.17 and above.
- You can also specify custom ports to be used by the protocol for an additional layer of safety. This allows you to keep only the specified ports open and block other ports for security.

Note: Please make sure you do not assign well-known special ports. We recommend the following port range for custom use: 49152-65535.

- Use Chromoting - CRC will use Chromoting protocol to connect to the device. This option is mandatory and cannot be deselected.
- Ports - Select the port type to be used by Chromoting protocol and specify the ports. The available options are:
  - Default - Chromoting will use the port range 49152 - 65535
  - Custom Range - Allows you to specify a port range to be used by Chromoting. Enter a range covering at least 4 ports.

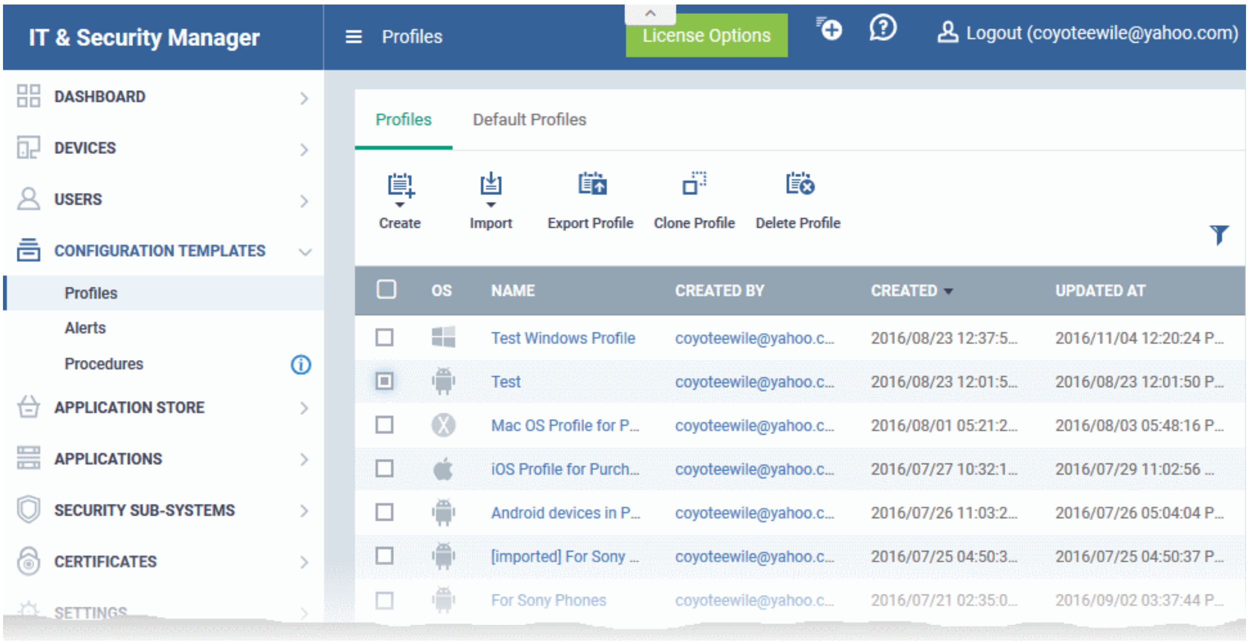
Note: Chromoting is supported by Windows 7 and later versions. If CRC is installed on a Windows XP admin machine, it will not be able to connect to a Mac OS device.

- Click 'Save' to apply your changes to the profile.

6.2. View and Manage Profiles

The 'Profiles' screen shows all available profiles 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 then choose 'Profiles' from the options.



☐	OS	NAME	CREATED BY	CREATED ▾	UPDATED AT
☐		Test Windows Profile	coyoteewile@yahoo.c...	2016/08/23 12:37:5...	2016/11/04 12:20:24 P...
☐		Test	coyoteewile@yahoo.c...	2016/08/23 12:01:5...	2016/08/23 12:01:50 P...
☐		Mac OS Profile for P...	coyoteewile@yahoo.c...	2016/08/01 05:21:2...	2016/08/03 05:48:16 P...
☐		iOS Profile for Purch...	coyoteewile@yahoo.c...	2016/07/27 10:32:1...	2016/07/29 11:02:56 ...
☐		Android devices in P...	coyoteewile@yahoo.c...	2016/07/26 11:03:2...	2016/07/26 05:04:04 P...
☐		[imported] For Sony ...	coyoteewile@yahoo.c...	2016/07/25 04:50:3...	2016/07/25 04:50:37 P...
☐		For Sony Phones	coyoteewile@yahoo.c...	2016/07/21 02:35:0...	2016/09/02 03:37:44 P...

The interface contains two tabs:

- Profiles - Displays a list of all profiles created in ITSM.
- Default Profiles - Lists all default profiles. All newly enrolled devices are assigned a default profile

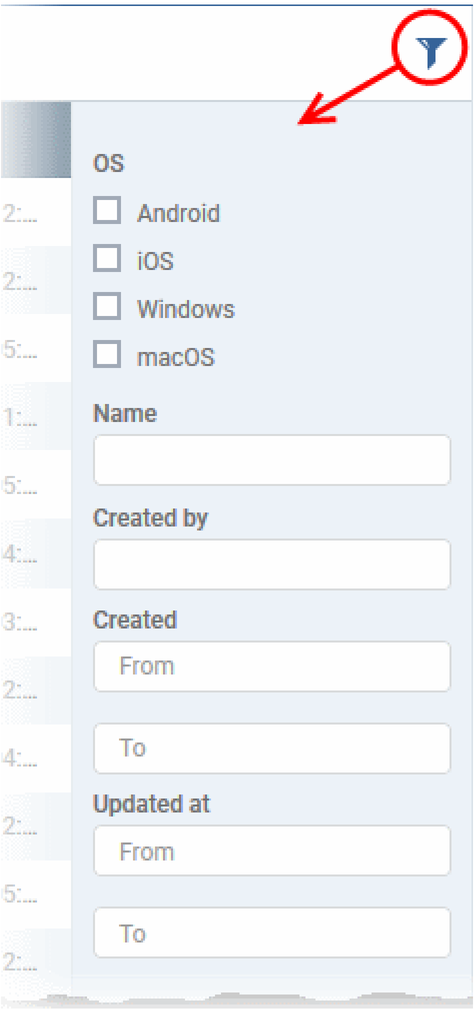
appropriate to their operating system. Refer to **Managing Default Profiles** for more details.

The 'Profiles' tab opens by default.

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 Mac OS 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



OS

□ Android
□ iOS
□ Windows
□ macOS

Name

Created by

Created

From

To

Updated at

From

To

- 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

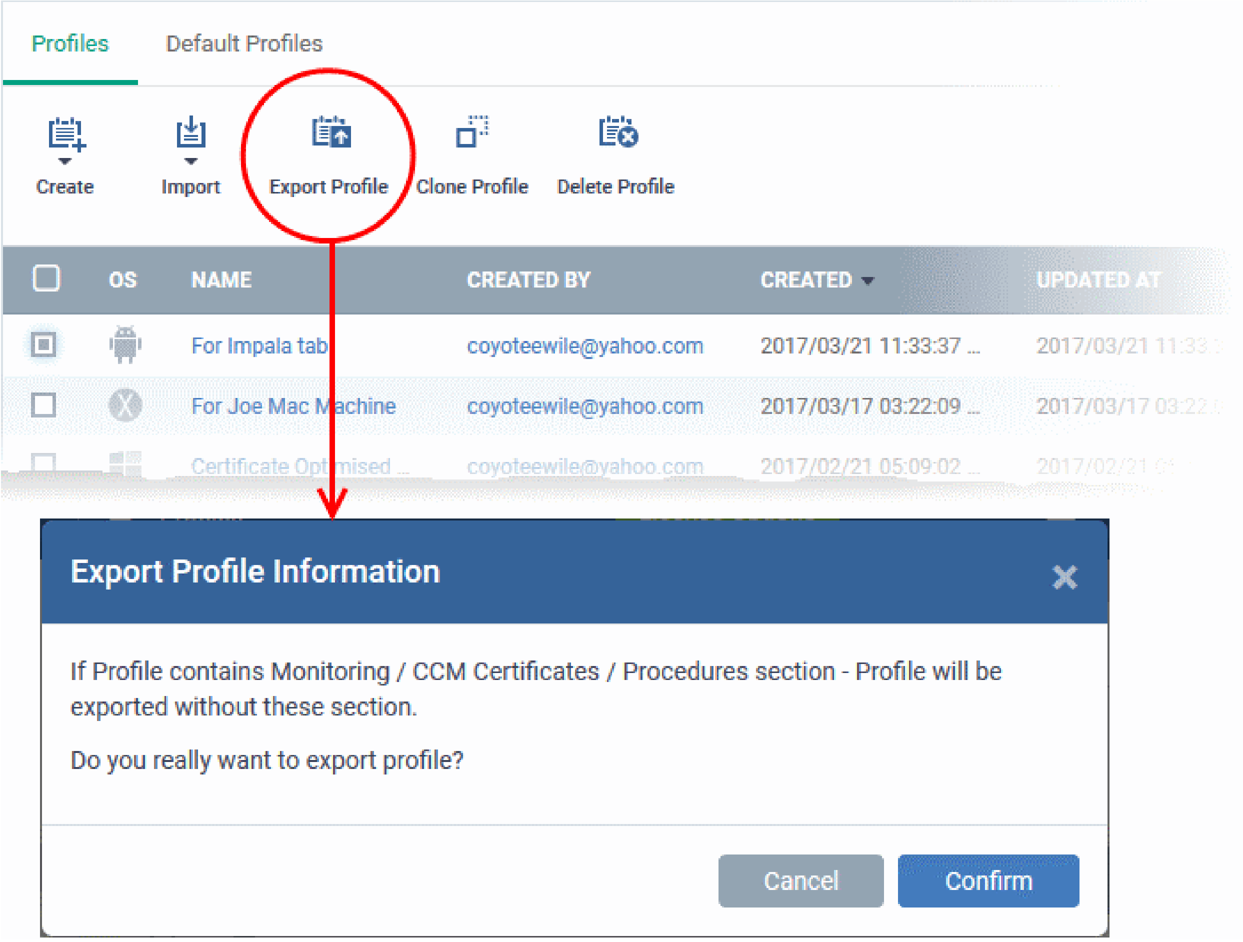
6.2.1. Export and Import Configuration Profiles

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 'Profiles' interface by clicking 'Configuration Templates' > 'Profiles' then select the 'Profiles' tab.
- Select the profile you want to export and click the 'Export profile' button:



If Profile contains Monitoring / CCM Certificates / Procedures section - Profile will be exported without these section.

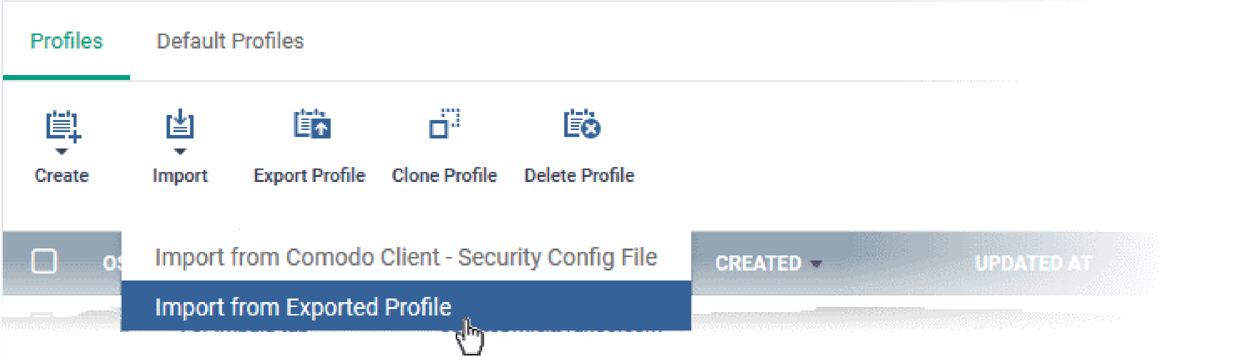
Do you really want to export profile?

You will see a prompt stating that monitoring, CCM certificate and procedures sections will be omitted from exported profiles.

- Click 'Confirm' to export the profiles to .cfg file
- Exported files can be imported back into ITSM as a profile at any time.

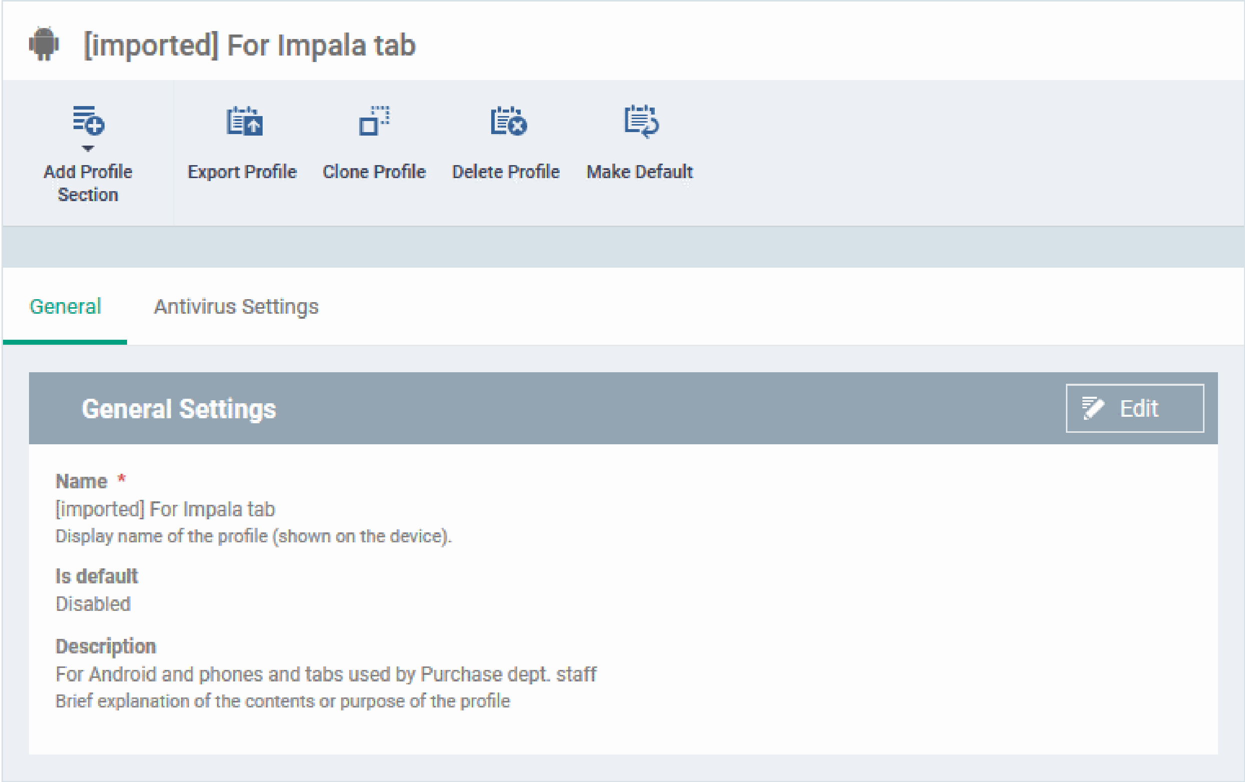
To import a profile from a saved .cfg file

- 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.



Name *
[imported] For Impala tab
Display name of the profile (shown on the device).

Is default
Disabled

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

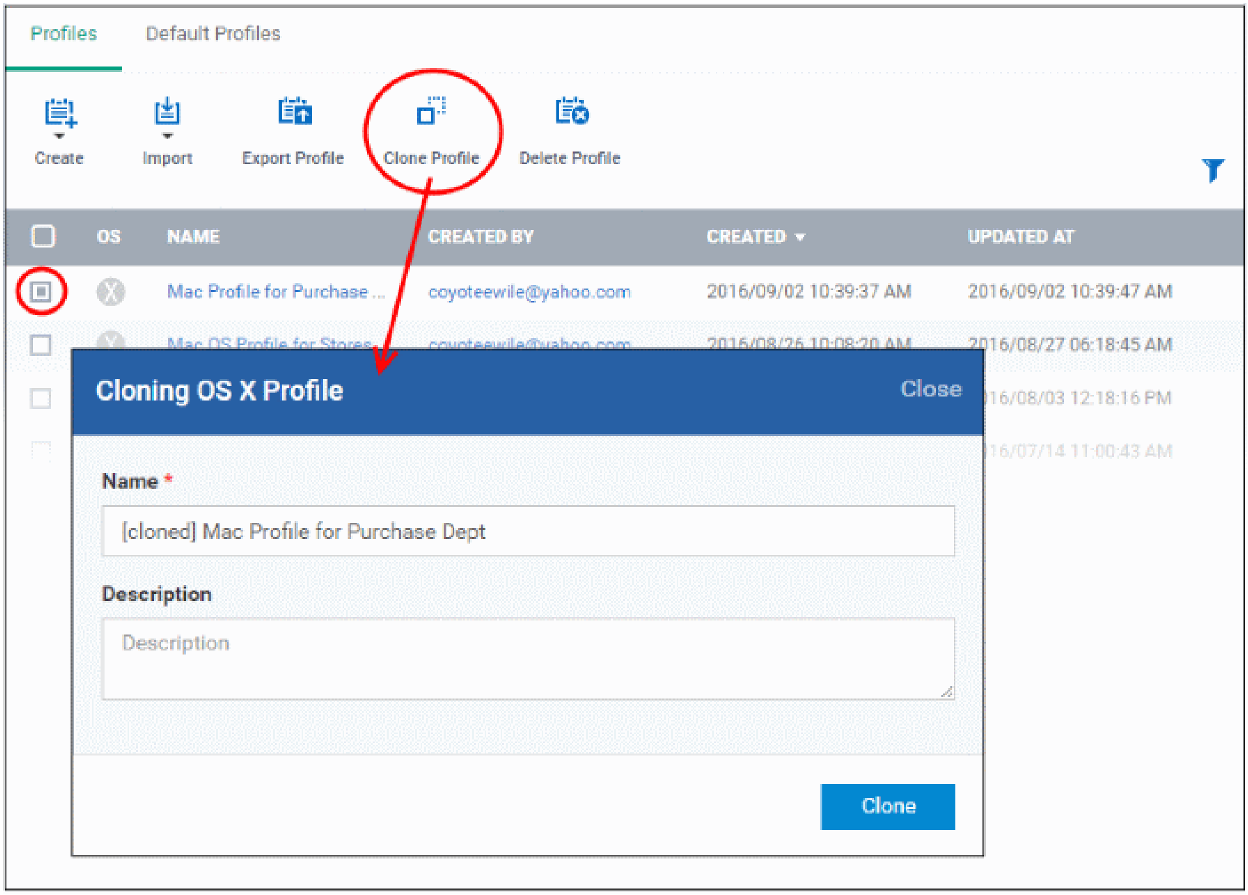
To create a clone of a profile

- 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.



	OS	NAME	CREATED BY	CREATED	UPDATED AT
☑		Mac Profile for Purchase ...	coyoteewile@yahoo.com	2016/09/02 10:39:37 AM	2016/09/02 10:39:47 AM
□		Mac OS Profile for Stores	coyoteewile@yahoo.com	2016/08/26 10:08:20 AM	2016/08/27 06:18:45 AM
□					16/08/03 12:18:16 PM
□					16/07/14 11:00:43 AM

Cloning OS X Profile — Close

Name *: [cloned] Mac Profile for Purchase Dept

Description: Description

Clone

The 'Cloning Mac OS 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 Edit 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

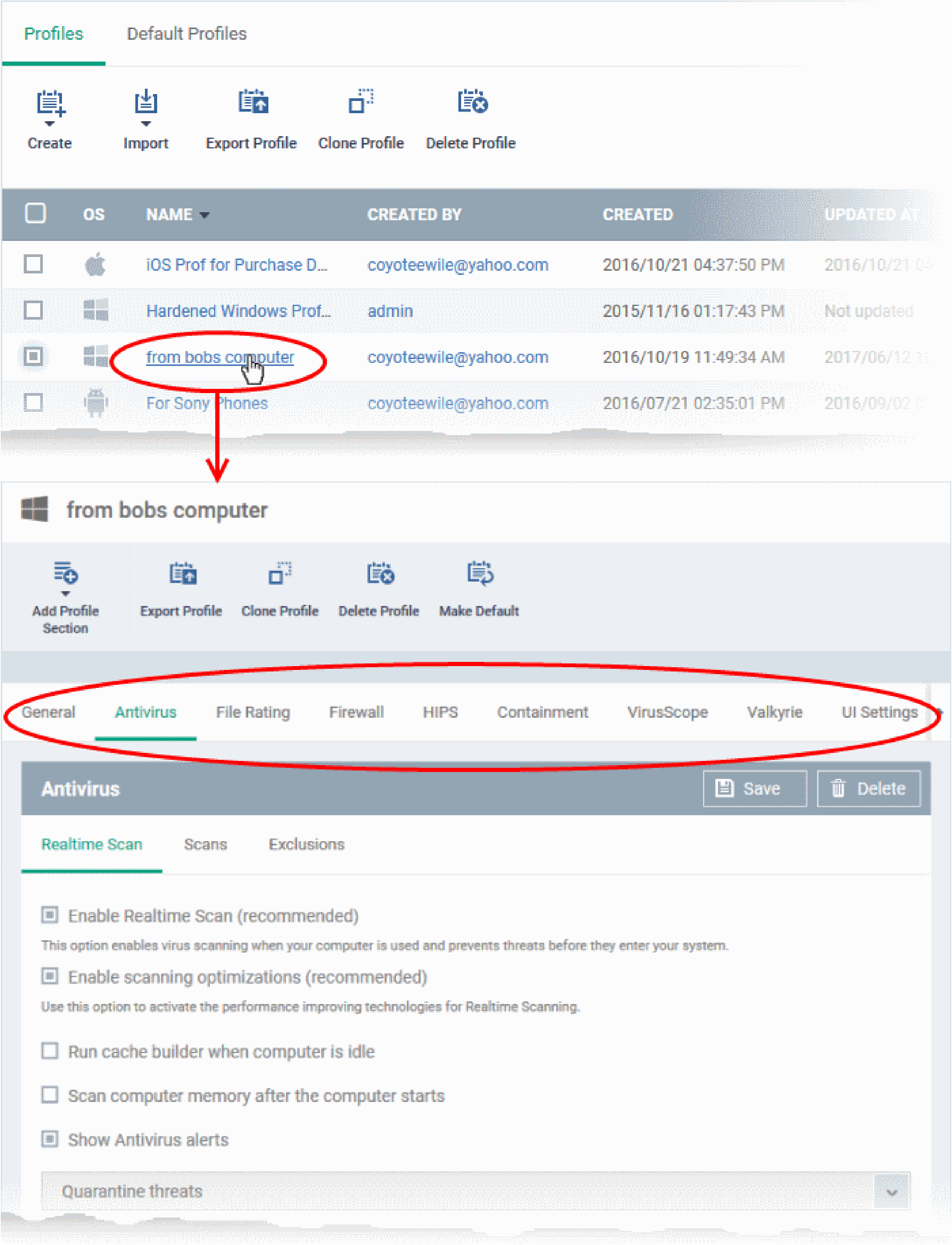
For more details on the options available under each component, refer to the sections **Profiles for Android Devices**, **Profiles for iOS Devices**, **Profiles for Mac OS Devices** and **Profiles for Windows Devices**.

6.3. Edit 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.



□	OS	NAME	CREATED BY	CREATED	UPDATED AT
□		iOS Prof for Purchase D...	coyoteewile@yahoo.com	2016/10/21 04:37:50 PM	2016/10/21 04
□		Hardened Windows Prof...	admin	2015/11/16 01:17:43 PM	Not updated
☒		from bobs computer	coyoteewile@yahoo.com	2016/10/19 11:49:34 AM	2017/06/12 11
□		For Sony Phones	coyoteewile@yahoo.com	2016/07/21 02:35:01 PM	2016/09/02 0

from bobs computer

☒ Enable Realtime Scan (recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☒ Enable scanning optimizations (recommended)

Use this option to activate the performance improving technologies for Realtime Scanning.

□ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☒ Show Antivirus alerts

Quarantine threats

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 Edit 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 Delete Profile button at the top

6.4. Manage 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. 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.

- There are default profiles for each operating system - Windows, Mac OS, Android and iOS.
- You can remove the 'default' status from any profile, including built-in 'Optimum' profiles. However, it is mandatory to have at least one default profile for each operating system.
- Each device enrolled to ITSM will have the appropriate default profile applied if no user or user group profile(s) are specified. This ensures all new devices have at least one profile upon enrollment.

Note: If a user or user group profile exists for an operating system, then these will be applied instead of the default profile. If the user profiles are removed then the default profile(s) will be automatically installed to take their place.

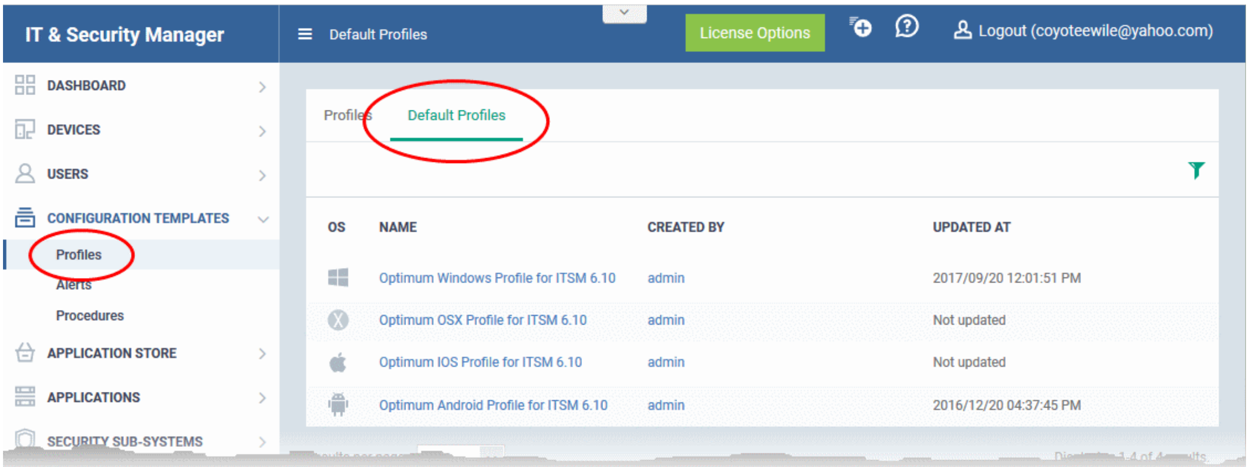
You can remove these default profiles from the devices at anytime from the Device Management interface. See **Assigning Configuration Profiles to Selected Devices** for more details.

The behavior of default profiles is as follows:

- When a profile is set as default, it will be applied to new devices during enrollment, if no profiles are associated with the user
- When all profiles associated with device are removed, the default profile(s) will be automatically applied to the device
- When a default profile is canceled from being default, it will be will be unassigned from enrolled devices

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' > 'Profiles' on the left.
- Choose the 'Default Profiles' tab on the top.



OS	NAME	CREATED BY	UPDATED AT
	Optimum Windows Profile for ITSM 6.10	admin	2017/09/20 12:01:51 PM
	Optimum OSX Profile for ITSM 6.10	admin	Not updated
	Optimum IOS Profile for ITSM 6.10	admin	Not updated
	Optimum Android Profile for ITSM 6.10	admin	2016/12/20 04:37:45 PM

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

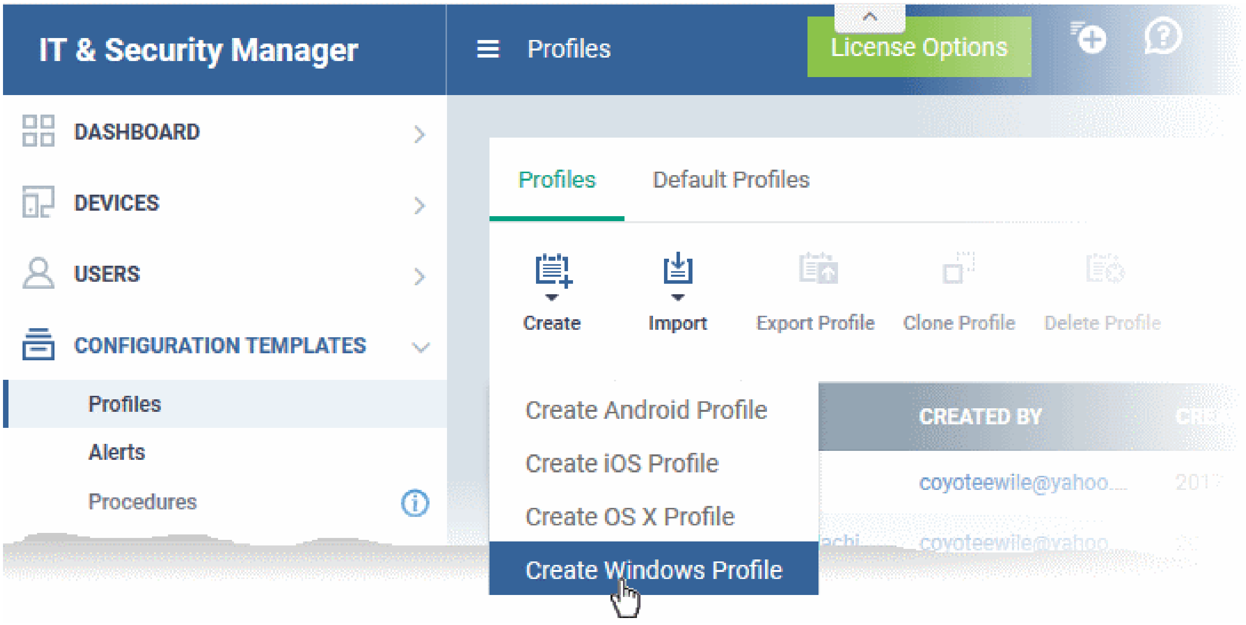
Creating a default profile

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.

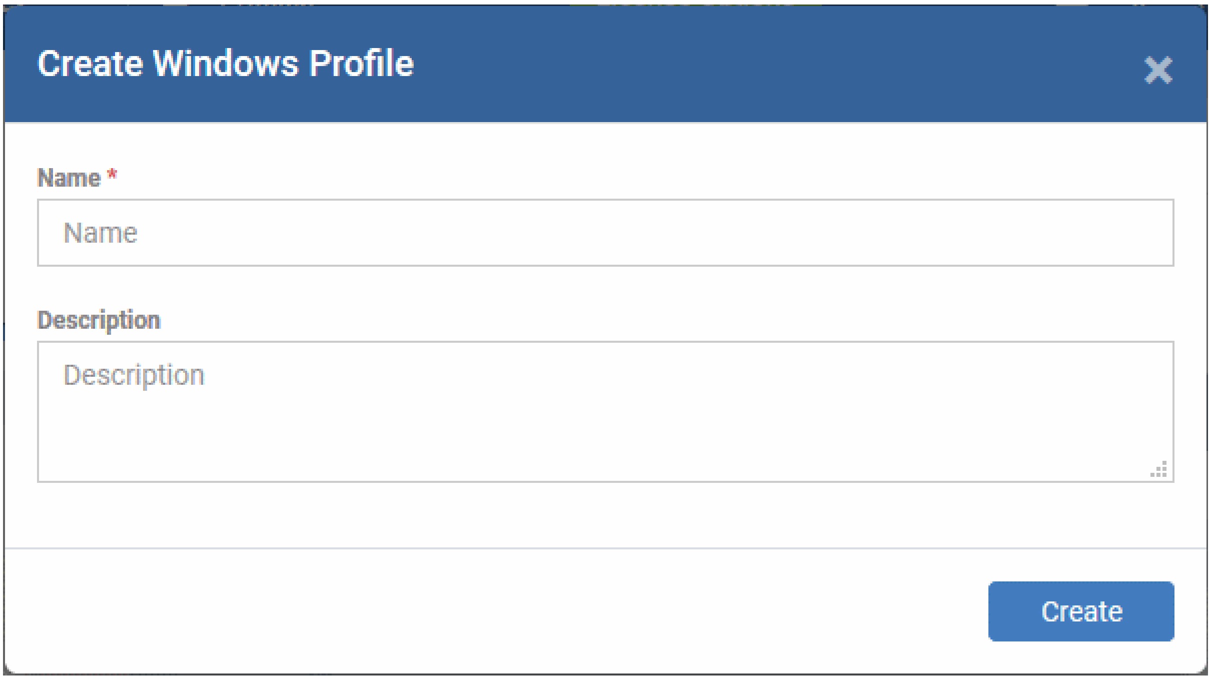
- Creating a default profile from the create profiles screen
- Creating a default profile from the edit screen of existing profiles

To create a default profile from the create profile screen

- Click 'Configuration Templates' on the left then choose 'Profiles' from the options
- Click the 'Profiles' tab
- Choose the type of profile that you want to create from the 'Create' drop-down

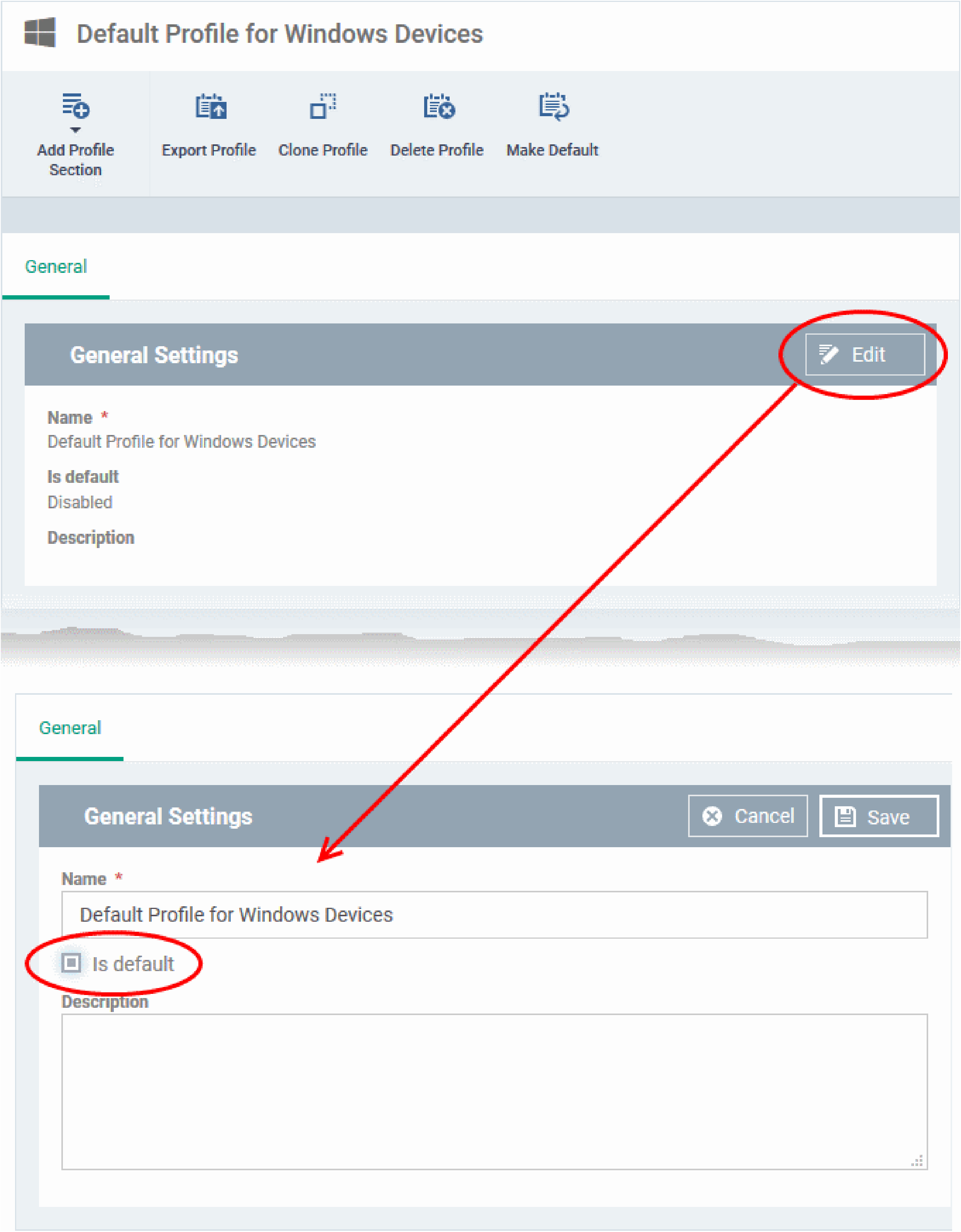


The 'Create OS Profile' screen will be displayed.



- 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.



Name *
Default Profile for Windows Devices

Is default
Disabled

Description

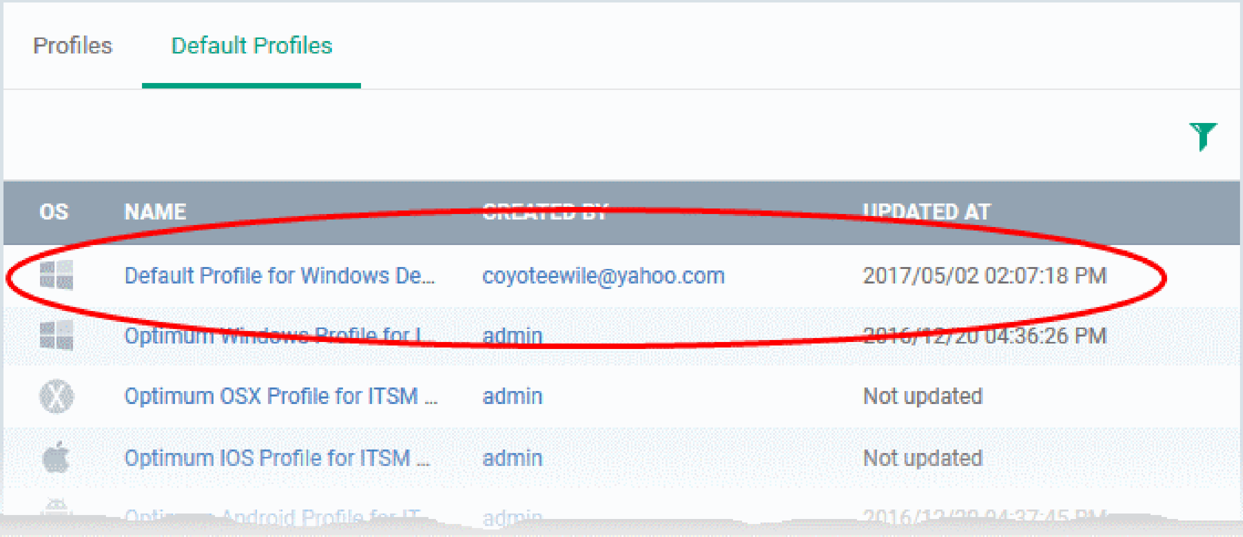
Name *
Default Profile for Windows Devices

☐ Is default

Description

- Click on the 'Edit' button Edit 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.

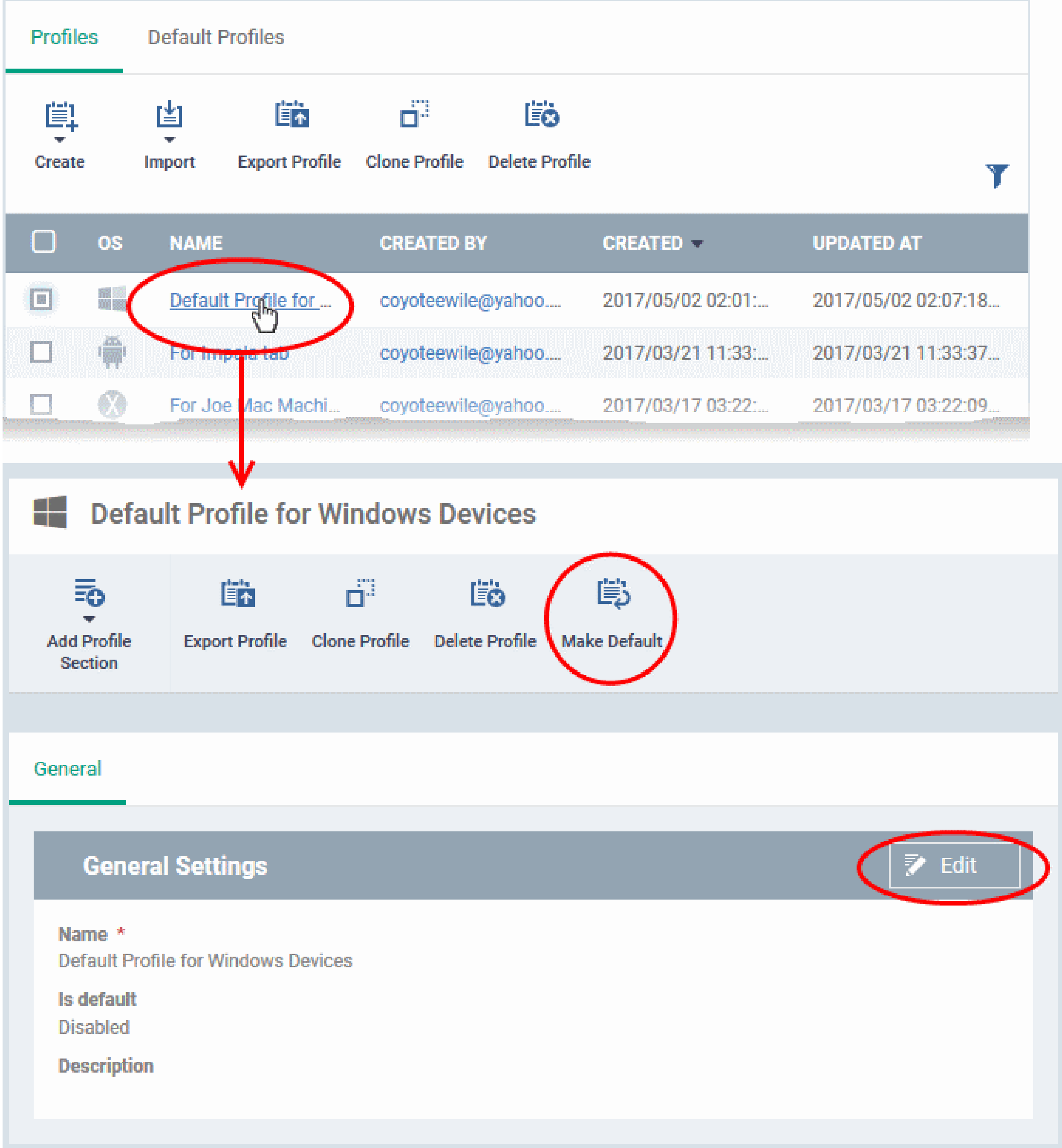


OS	NAME	CREATED BY	UPDATED AT
	Default Profile for Windows De...	coyoteewile@yahoo.com	2017/05/02 02:07:18 PM
	Optimum Windows Profile for I...	admin	2016/12/20 04:36:26 PM
	Optimum OSX Profile for ITSM ...	admin	Not updated
	Optimum IOS Profile for ITSM ...	admin	Not updated
	Optimum Android Profile for IT...	admin	2016/12/20 04:37:45 PM

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 select 'Profiles' from the options.
- Click the 'Profiles' tab on the top.
- Click the name of the profile that you want to set as a default profile



☐	OS	NAME	CREATED BY	CREATED ▾	UPDATED AT
☐		Default Profile for ...	coyoteewile@yahoo....	2017/05/02 02:01:...	2017/05/02 02:07:18...
☐		For Impala tab	coyoteewile@yahoo....	2017/03/21 11:33:...	2017/03/21 11:33:37...
☐		For Joe Mac Machi...	coyoteewile@yahoo....	2017/03/17 03:22:...	2017/03/17 03:22:09...

Default Profile for Windows Devices

General Settings

Name *
Default Profile for Windows Devices

Is default
Disabled

Description

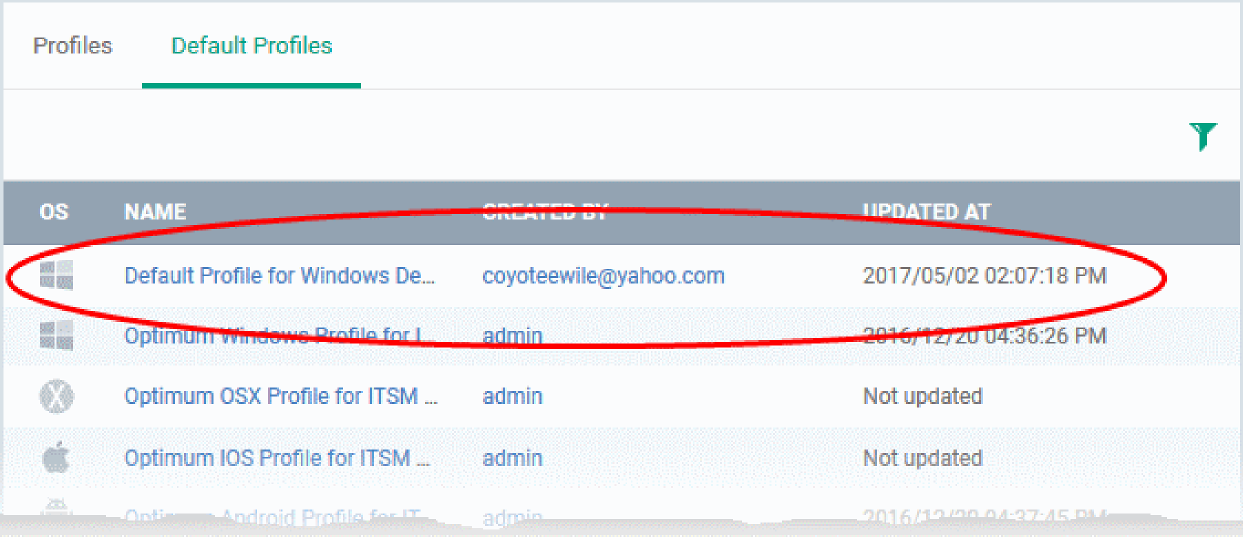
The profile details screen of the selected profile will be displayed.

- Click the 'Edit' button Edit 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.

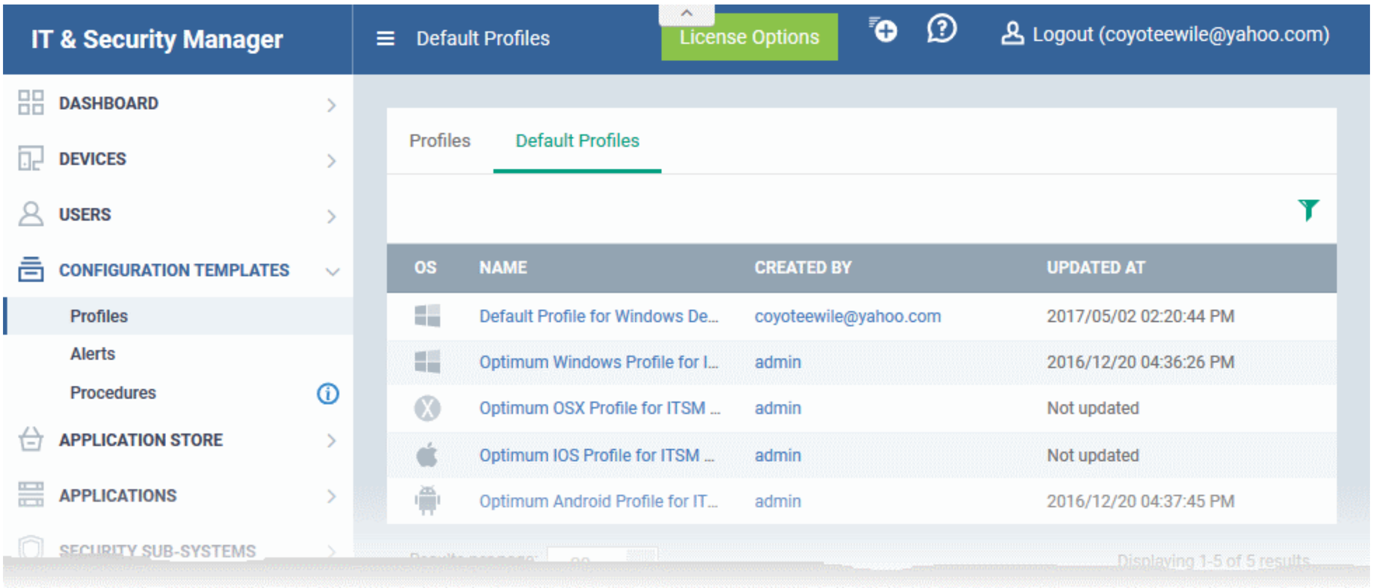


OS	NAME	CREATED BY	UPDATED AT
	Default Profile for Windows De...	coyoteewile@yahoo.com	2017/05/02 02:07:18 PM
	Optimum Windows Profile for I...	admin	2016/12/20 04:36:26 PM
	Optimum OSX Profile for ITSM ...	admin	Not updated
	Optimum IOS Profile for ITSM ...	admin	Not updated
	Optimum Android Profile for IT...	admin	2016/12/20 04:37:45 PM

To view and manage default profiles

- Click 'Configuration Templates' on the left then choose 'Profiles' from the options
- Click the 'Default Profiles' tab

The list of default profiles will be displayed.



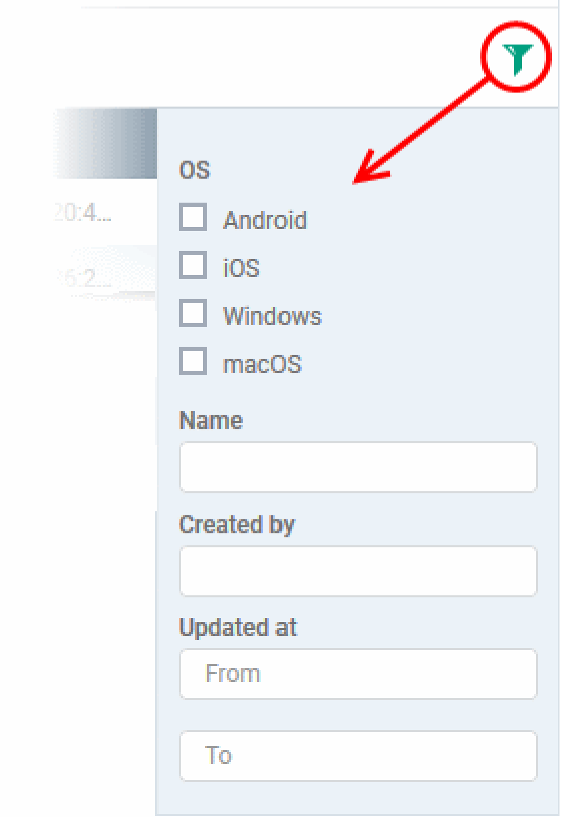
OS	NAME	CREATED BY	UPDATED AT
	Default Profile for Windows De...	coyoteewile@yahoo.com	2017/05/02 02:20:44 PM
	Optimum Windows Profile for I...	admin	2016/12/20 04:36:26 PM
	Optimum OSX Profile for ITSM ...	admin	Not updated
	Optimum IOS Profile for ITSM ...	admin	Not updated
	Optimum Android Profile for IT...	admin	2016/12/20 04:37:45 PM

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 respective 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.

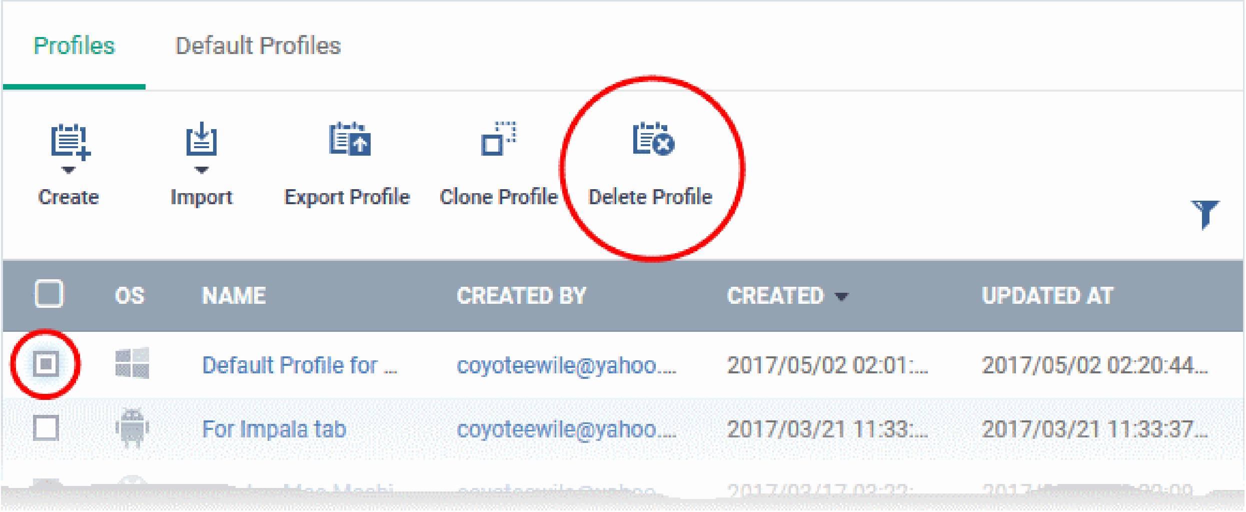
- To display all the profiles again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the filter options

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, if the user/user group is not applied with any profiles. These default profiles will be automatically overridden by the profiles 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' > 'Profiles' screen. Please note that default profiles that are shipped with ITSM cannot be removed.



□	OS	NAME	CREATED BY	CREATED	UPDATED AT
▣		Default Profile for ...	coyoteewile@yahoo....	2017/05/02 02:01:...	2017/05/02 02:20:44...
□		For Impala tab	coyoteewile@yahoo....	2017/03/21 11:33:...	2017/03/21 11:33:37...

- 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.

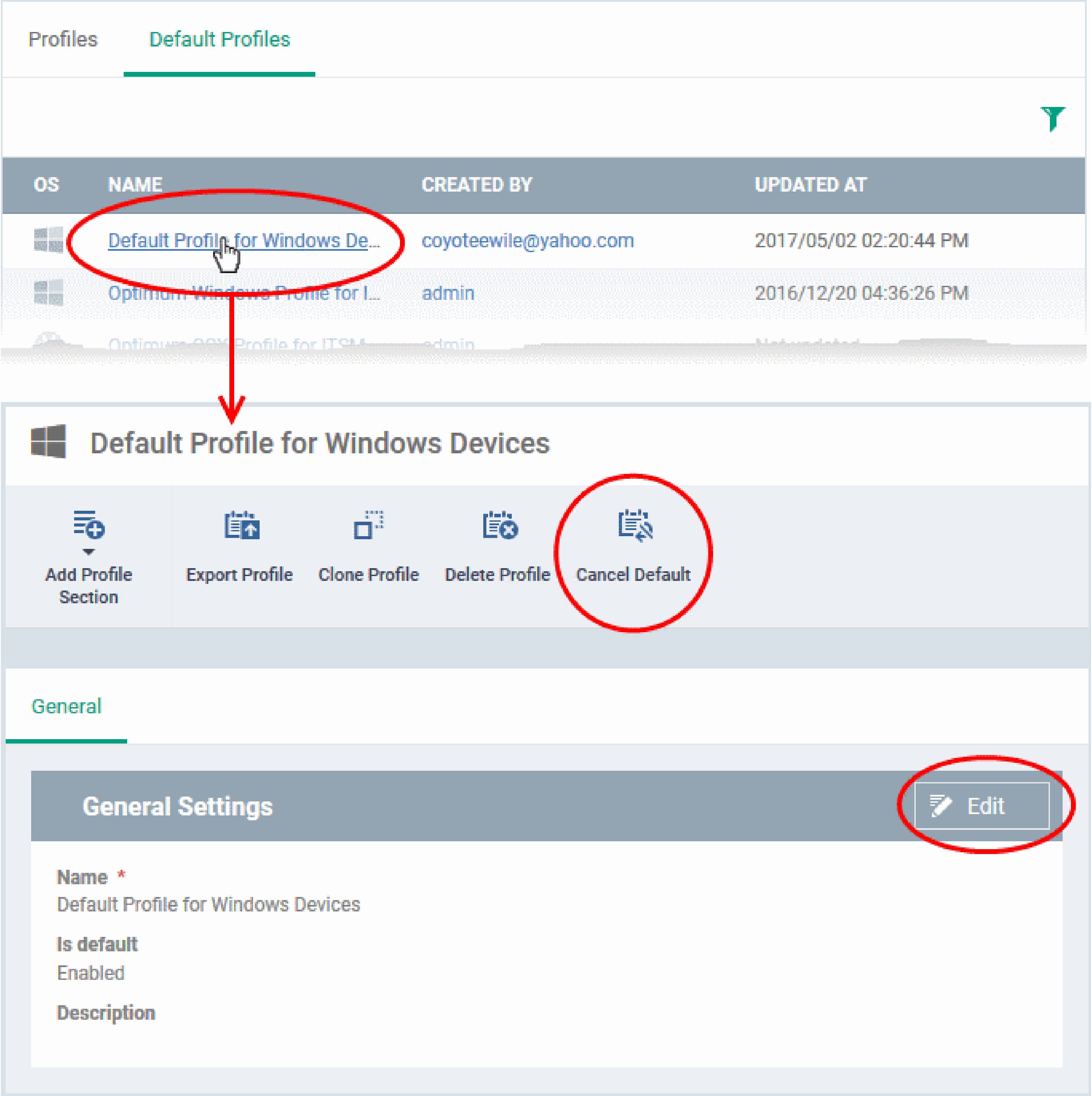
Note: It is mandatory to have at least one default profile for each operating system in ITSM. You cannot remove a default profile if that is the only one default profile available for the respective operating system. If you want to do so, assign a different profile as default profile for the operating system before removing it.

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' > 'Profiles' on the left then choose the 'Default Profiles' tab.



OS	NAME	CREATED BY	UPDATED AT
	Default Profile for Windows De...	coyoteewile@yahoo.com	2017/05/02 02:20:44 PM
	Optimum Windows Profile for I...	admin	2016/12/20 04:36:26 PM

Default Profile for Windows Devices

General Settings

Name *
Default Profile for Windows Devices

Is default
Enabled

Description

- 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.

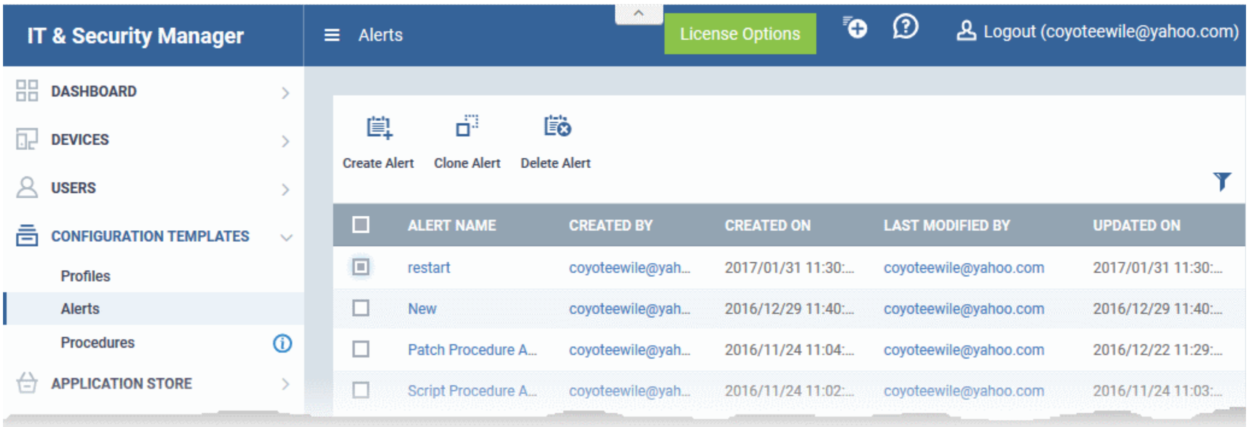
Note: It is mandatory to have at least one default profile for each operating system in ITSM. You cannot cancel a default profile if that is the only one default profile available for the respective operating system. If you want to do so, assign a different profile as default profile for the operating system before canceling it.

6.5. Manage Alerts

You can specify that an alert is created if certain criteria are met. For example, you can set an alert if a procedure fails to run on devices or if a monitoring condition is breached. 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.



□	ALERT NAME	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
☒	restart	coyoteewile@yah...	2017/01/31 11:30:...	coyoteewile@yahoo.com	2017/01/31 11:30:...
□	New	coyoteewile@yah...	2016/12/29 11:40:...	coyoteewile@yahoo.com	2016/12/29 11:40:...
□	Patch Procedure A...	coyoteewile@yah...	2016/11/24 11:04:...	coyoteewile@yahoo.com	2016/12/22 11:29:...
□	Script Procedure A...	coyoteewile@yah...	2016/11/24 11:02:...	coyoteewile@yahoo.com	2016/11/24 11:03:...

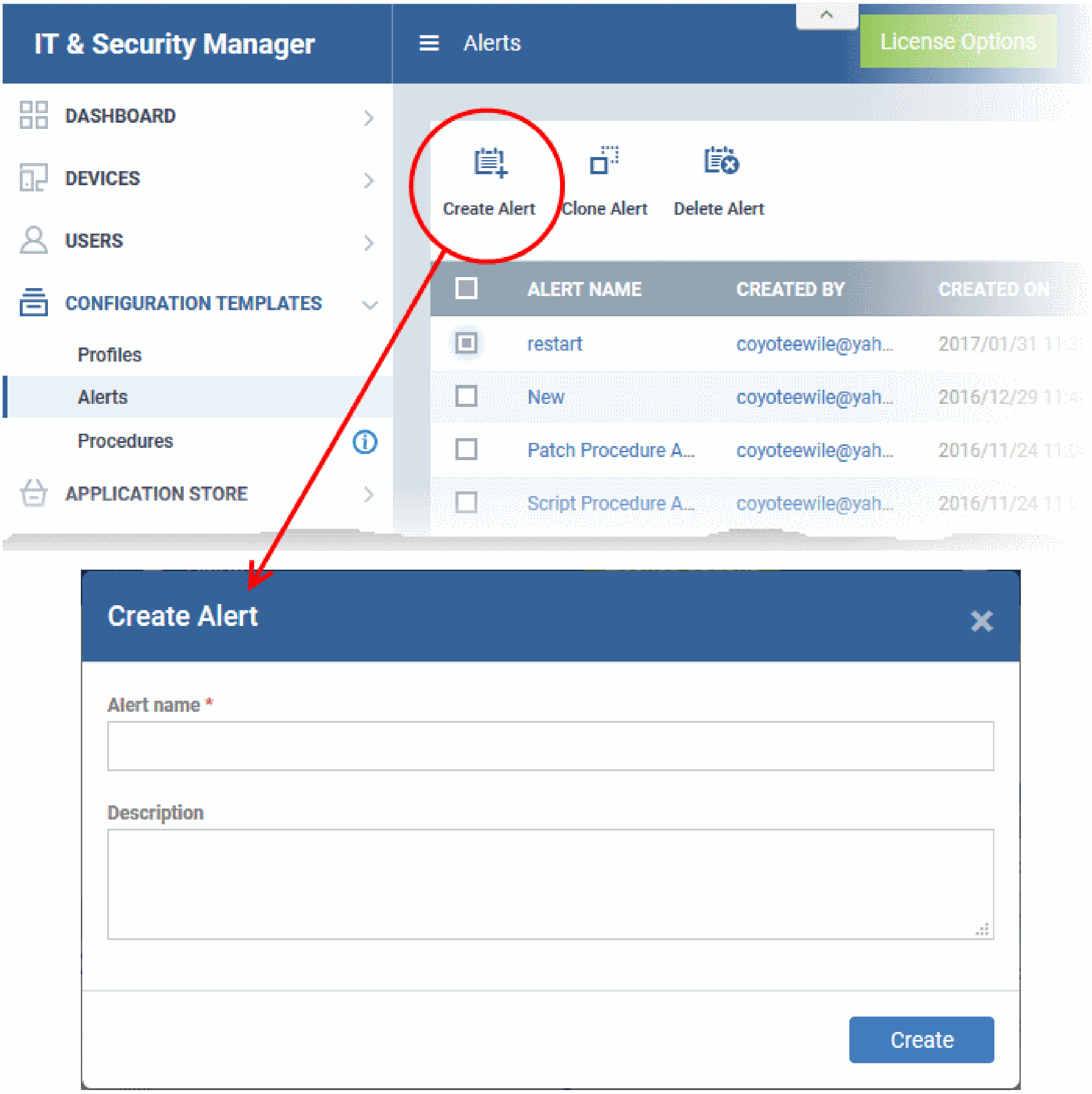
Note - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit files for analysis, monitor Windows events and provide alerts and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports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

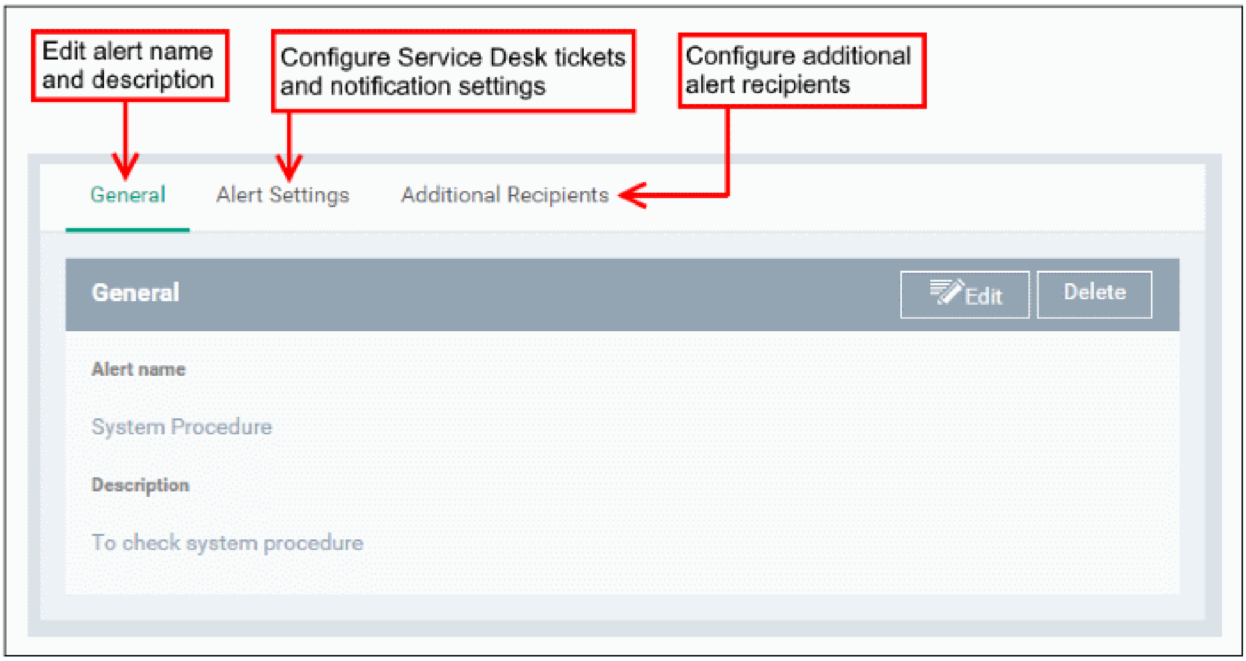


☐	ALERT NAME	CREATED BY	CREATED ON
☐	restart	coyoteewile@yah...	2017/01/31 11:3
☐	New	coyoteewile@yah...	2016/12/29 11:4
☐	Patch Procedure A...	coyoteewile@yah...	2016/11/24 11:0
☐	Script Procedure A...	coyoteewile@yah...	2016/11/24 11:0

Alert name *

Description

- Enter a name and description for your alert and click 'Create'
- After saving, you will be taken to the alert configuration screen. The 'General' section allows you to modify basic settings:


Edit alert name and description
Configure Service Desk tickets and notification settings
Configure additional alert recipients
General
Alert Settings
Additional Recipients
Edit
Delete

General

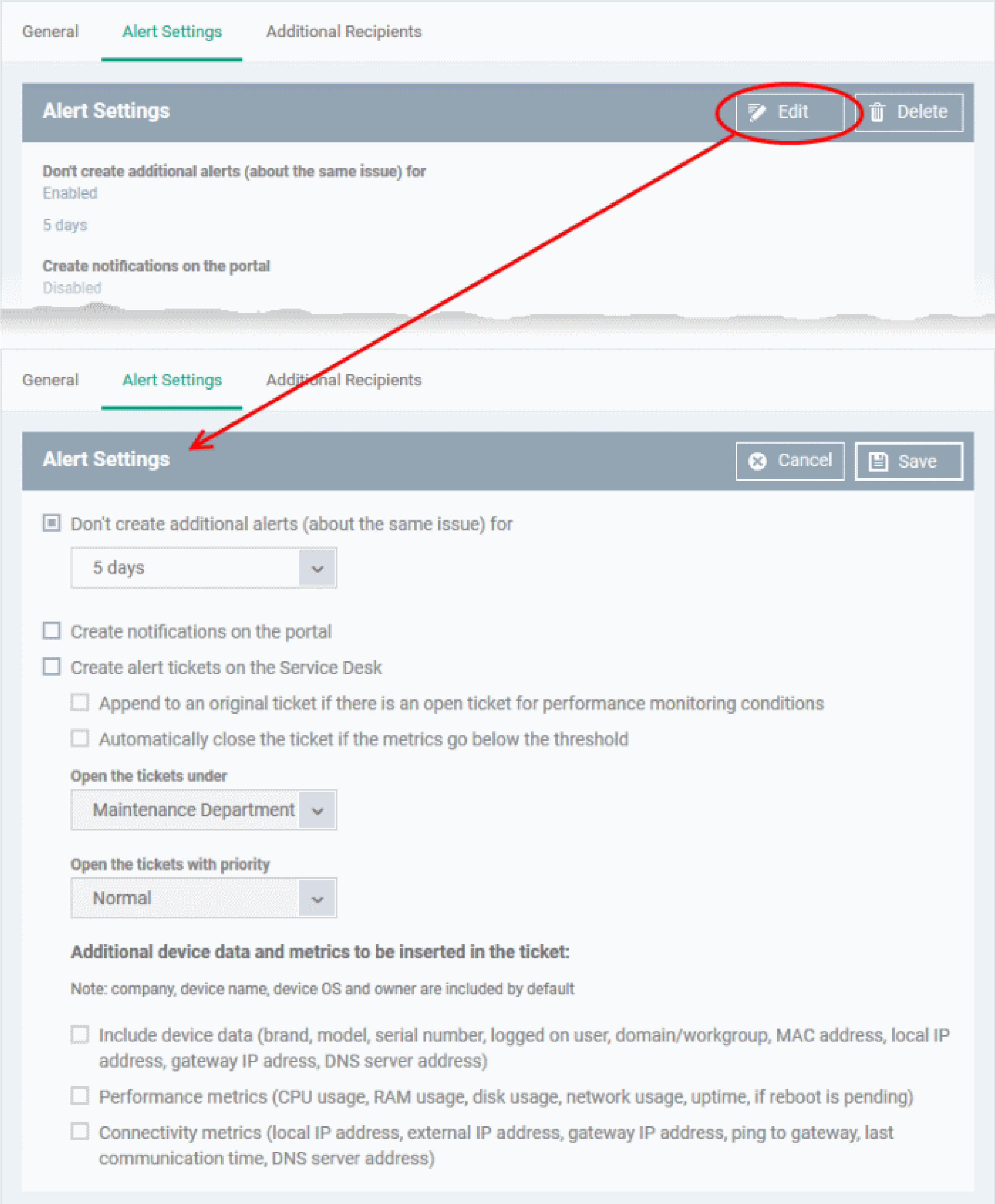
Alert name

System Procedure

Description

To check system procedure

- To configure alert settings, click 'Alert Settings' tab and then 'Edit'



Don't create additional alerts (about the same issue) for
Enabled
5 days

Create notifications on the portal
Disabled

☒ Don't create additional alerts (about the same issue) for

5 days

□ Create notifications on the portal

□ Create alert tickets on the Service Desk

□ Append to an original ticket if there is an open ticket for performance monitoring conditions

□ Automatically close the ticket if the metrics go below the threshold

Open the tickets under
Maintenance Department

Open the tickets with priority
Normal

Additional device data and metrics to be inserted in the ticket:

Note: company, device name, device OS and owner are included by default

□ Include device data (brand, model, serial number, logged on user, domain/workgroup, MAC address, local IP address, gateway IP adress, DNS server address)

□ Performance metrics (CPU usage, RAM usage, disk usage, network usage, uptime, if reboot is pending)

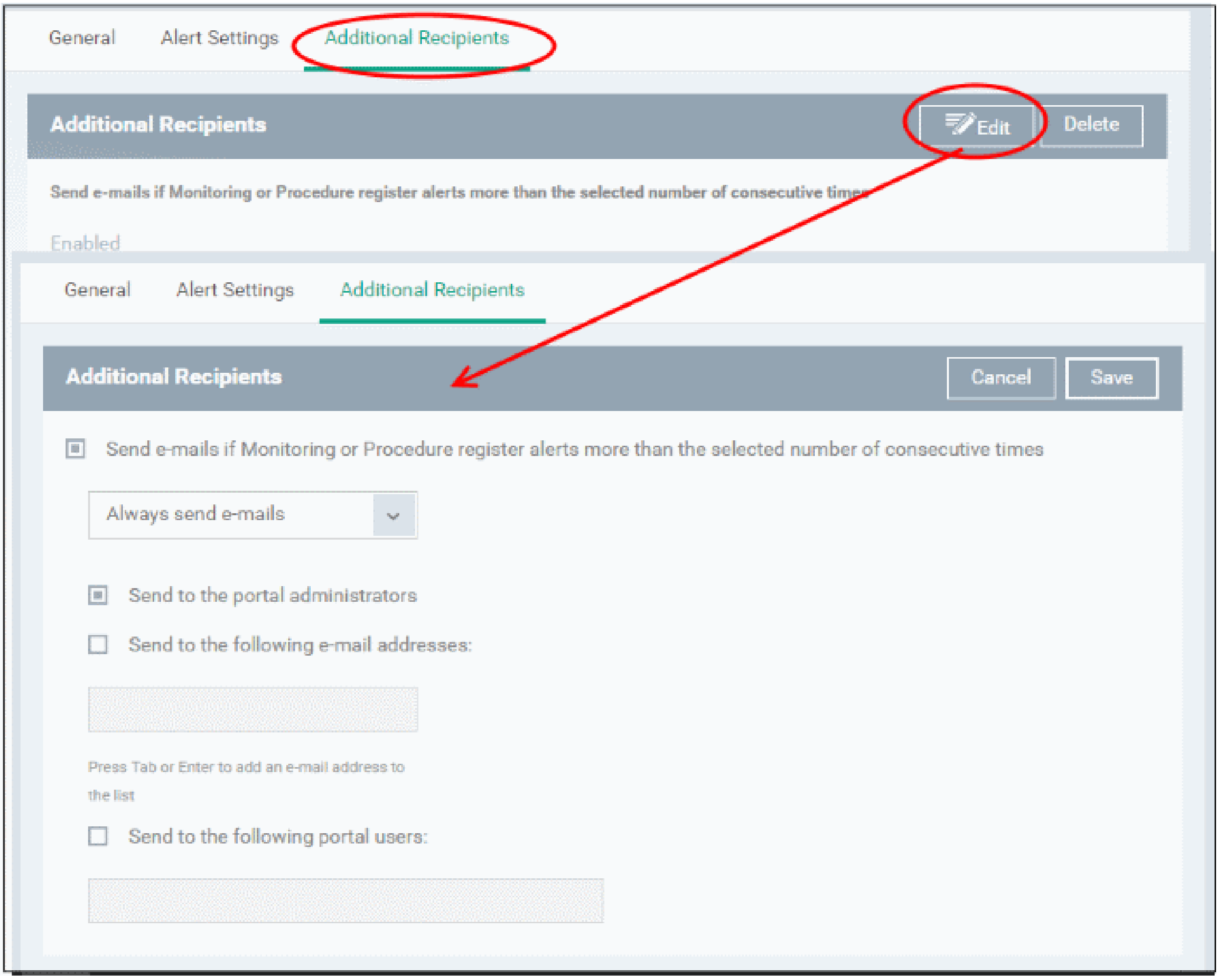
□ Connectivity metrics (local IP address, external IP address, gateway IP address, ping to gateway, last communication time, DNS server address)

- **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 type, device OS and the owner information are included in the ticket. To add additional device data and metrics to the ticket, select the respective options.
  - **Include Device Data** - Adds device information like brand, model. IP address and so on
  - **Performance Metrics** - Adds device performance information like CPU usage, RAM usage, disk usage, network usage and more
  - **Connectivity Metrics** - Adds information on network to which the device is connected, like local IP address, external IP address, gateway IP address and more

- 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

Enabled

☒ Send e-mails if Monitoring or Procedure register alerts more than the selected number of consecutive times

Always send e-mails

☒ Send to the portal administrators

☐ Send to the following e-mail addresses:

Press Tab or Enter to add an e-mail address to the list

☐ Send to the following portal users:

- **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

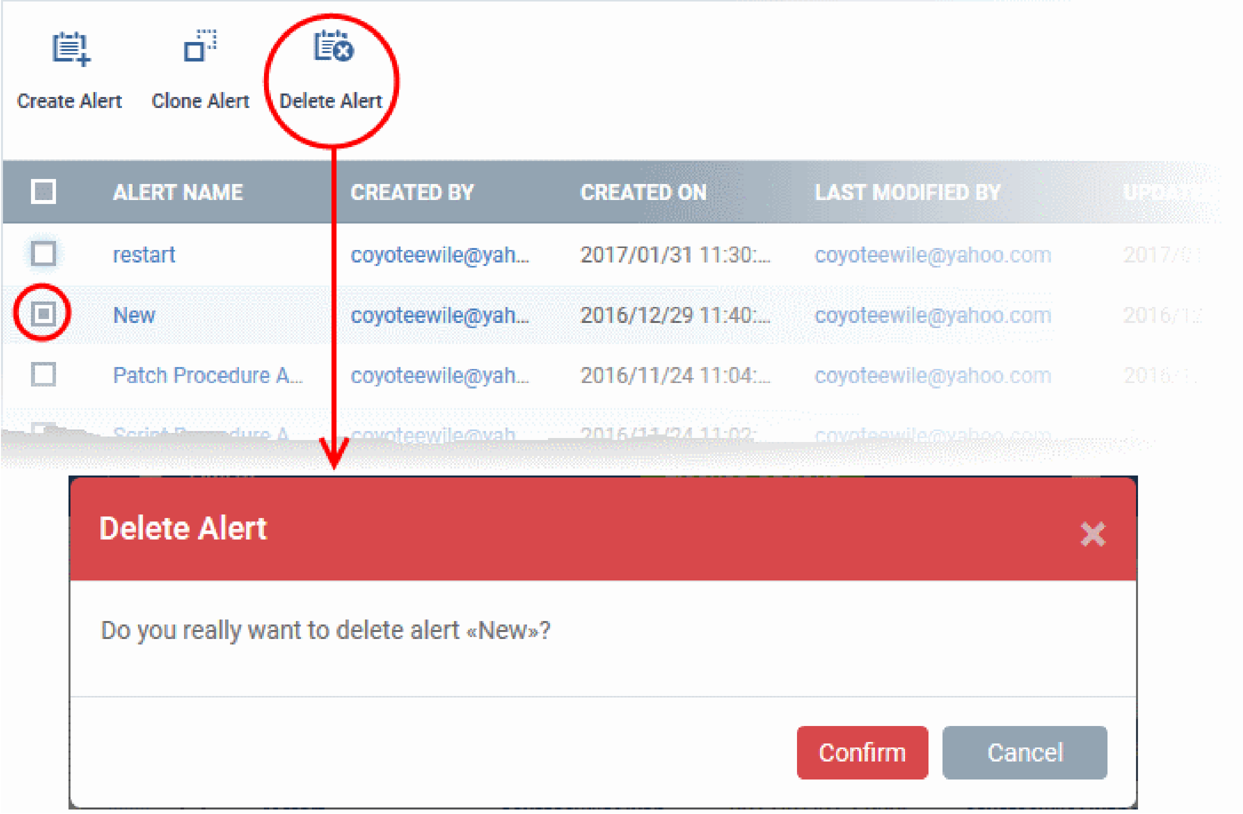
To edit an alert:

- 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:



□	ALERT NAME	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATE...
□	restart	coyoteewile@yah...	2017/01/31 11:30:...	coyoteewile@yahoo.com	2017/0...
▣	New	coyoteewile@yah...	2016/12/29 11:40:...	coyoteewile@yahoo.com	2016/1...
□	Patch Procedure A...	coyoteewile@yah...	2016/11/24 11:04:...	coyoteewile@yahoo.com	2016/1...
□	Script Procedure A...	coyoteewile@yah...	2016/11/24 11:02:...	coyoteewile@yahoo.com	

Delete Alert

Do you really want to delete alert «New»?

6.6. Manage 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 resolve common issues, pinpoint and resolve problems, 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
- Select third party applications to be updated for a 3rd party 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. View and Manage Procedures

- Click 'Configuration Templates' > 'Procedures' to open the procedures interface.

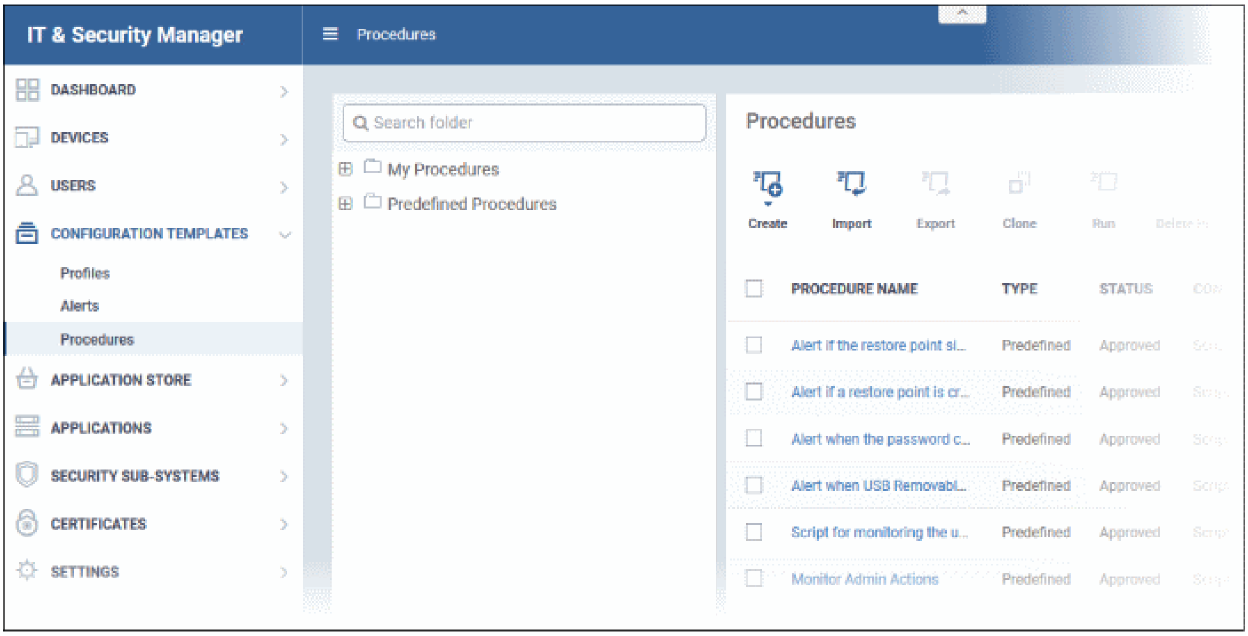
'Procedures' are available in two categories which are shown in folders on the left - 'Predefined Procedures' and 'My Procedures' (custom procedures).

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.



□	PROCEDURE NAME	TYPE	STATUS
□	Alert if the restore point si...	Predefined	Approved
□	Alert if a restore point is cr...	Predefined	Approved
□	Alert when the password c...	Predefined	Approved
□	Alert when USB Removabl...	Predefined	Approved
□	Script for monitoring the u...	Predefined	Approved
□	Monitor Admin Actions	Predefined	Approved

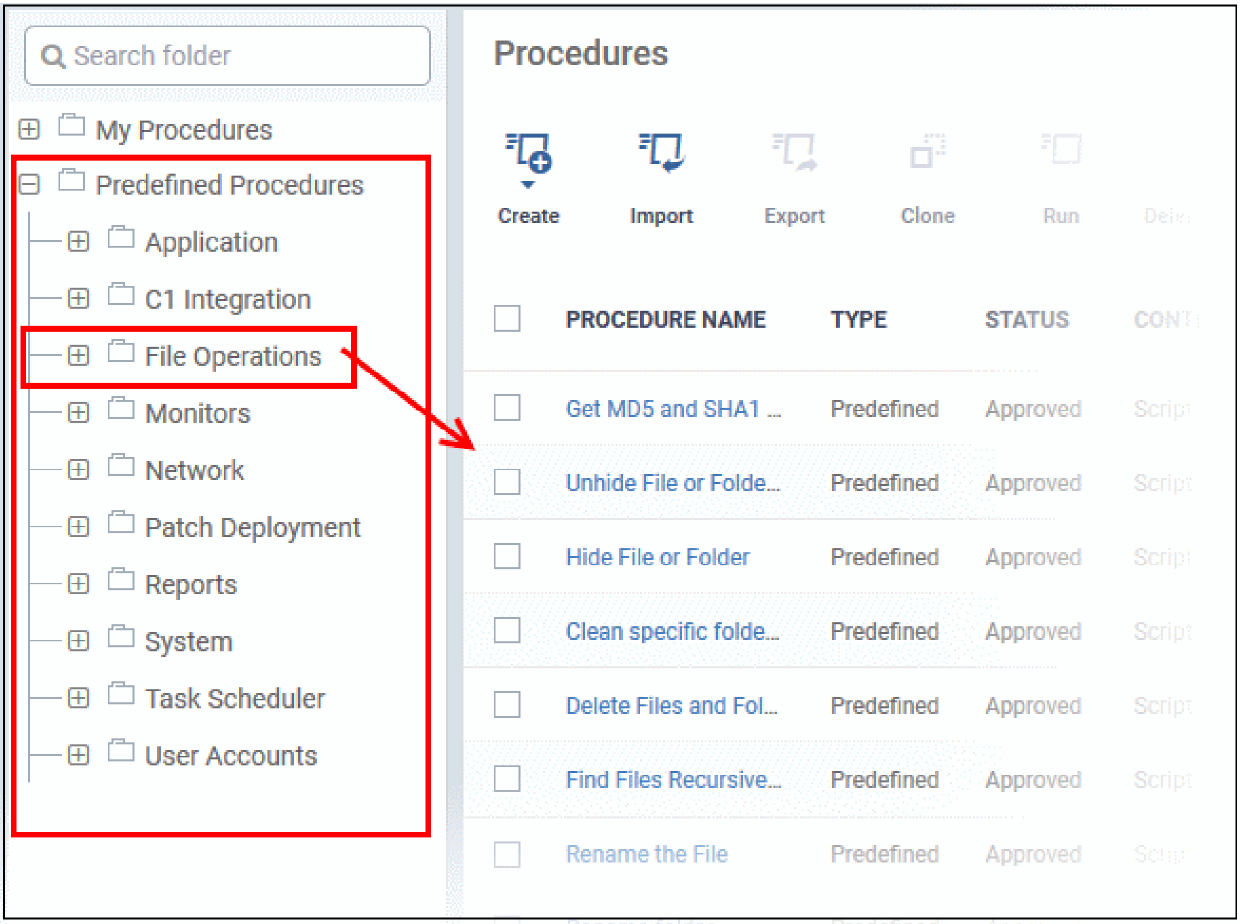
Procedures - Column Descriptions	
Column Heading	**Description**
Procedure Name	The name of the procedure
Type	Indicates whether the procedure is a custom or a predefined procedure.
Status	Indicates the status of the procedure. The statuses are: • Created • Edited • Ready to review • Approved • Declined
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:



□	PROCEDURE NAME	TYPE	STATUS	CONT
□	Get MD5 and SHA1 ...	Predefined	Approved	Script
□	Unhide File or Folde...	Predefined	Approved	Script
□	Hide File or Folder	Predefined	Approved	Script
□	Clean specific folde...	Predefined	Approved	Script
□	Delete Files and Fol...	Predefined	Approved	Script
□	Find Files Recursive...	Predefined	Approved	Script
□	Rename the File	Predefined	Approved	Script

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.
C1 Integration	Script procedures to install/modify or communicate with other C1 products
File Operations	Copy, move/delete files/folders, find and remove duplicate files, compress/decompress folders, clean up temporary files and downloaded files and more.
Monitors	Predefined script monitors that can be used in the **monitoring settings** of a

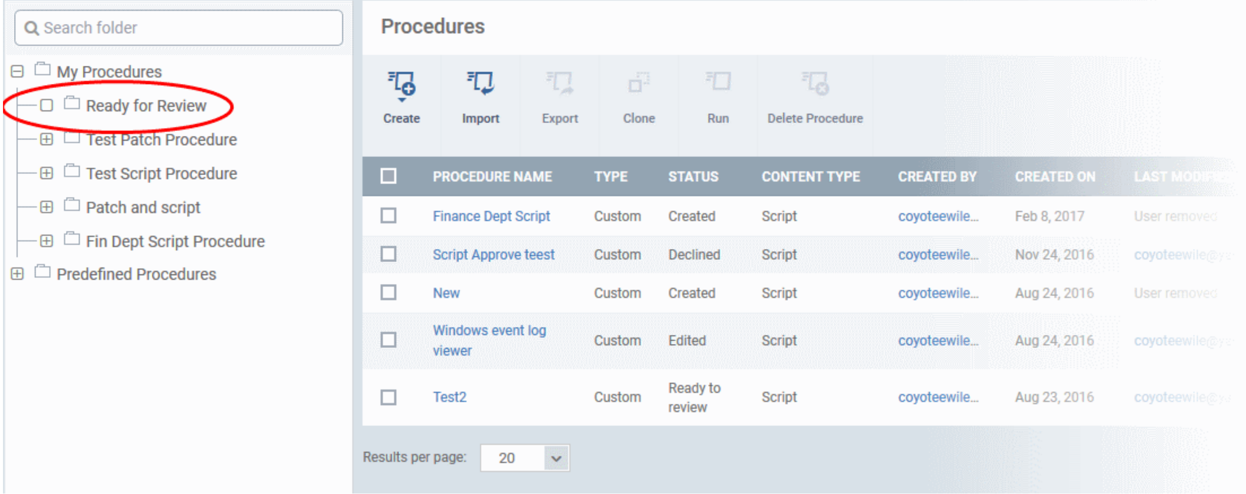
	Windows profile. See **Adding Custom Monitoring Conditions** for more details.
Network	View TCP/IP settings, save/restore network configurations, clear DNS cache and more
Patch Deployment	Installation and update of OS patches of different categories.
Reports	Contains procedures for obtaining various system logs.
System	Rebooting devices, create restore point, enable/disable USB ports, mapping network drives, running disk defragmentation, fixing disk errors and more.
Task Scheduler	Creating new tasks and schedule them, run tasks 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').

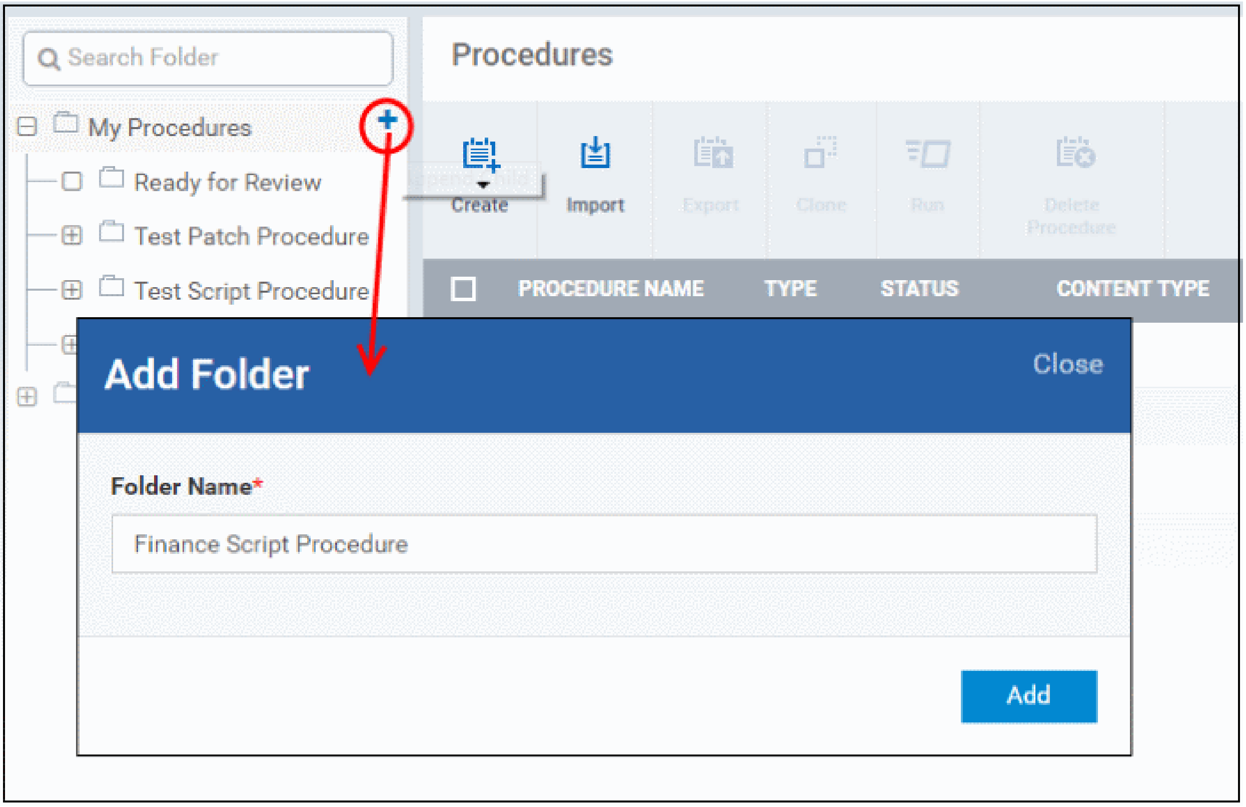


☐	PROCEDURE NAME	TYPE	STATUS	CONTENT TYPE	CREATED BY	CREATED ON	LAST MODIF
☐	Finance Dept Script	Custom	Created	Script	coyoteewile...	Feb 8, 2017	User removed
☐	Script Approve teest	Custom	Declined	Script	coyoteewile...	Nov 24, 2016	coyoteewile@y
☐	New	Custom	Created	Script	coyoteewile...	Aug 24, 2016	User removed
☐	Windows event log viewer	Custom	Edited	Script	coyoteewile...	Aug 24, 2016	coyoteewile@y
☐	Test2	Custom	Ready to review	Script	coyoteewile...	Aug 23, 2016	coyoteewile@y

Results per page: 20

To add a sub folder to the My Procedures folder:

- Place your mouse on the 'My Procedures' folder and click '+' beside it

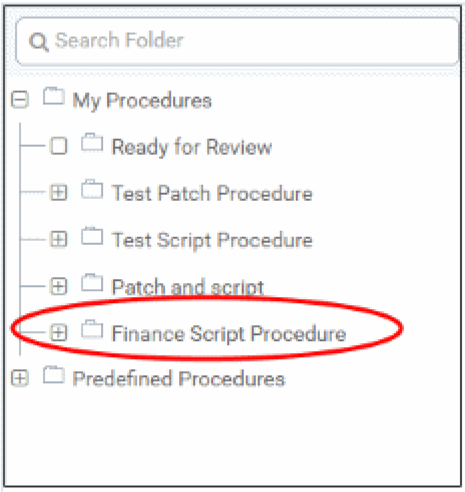


Folder Name*

Finance Script Procedure

- 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'



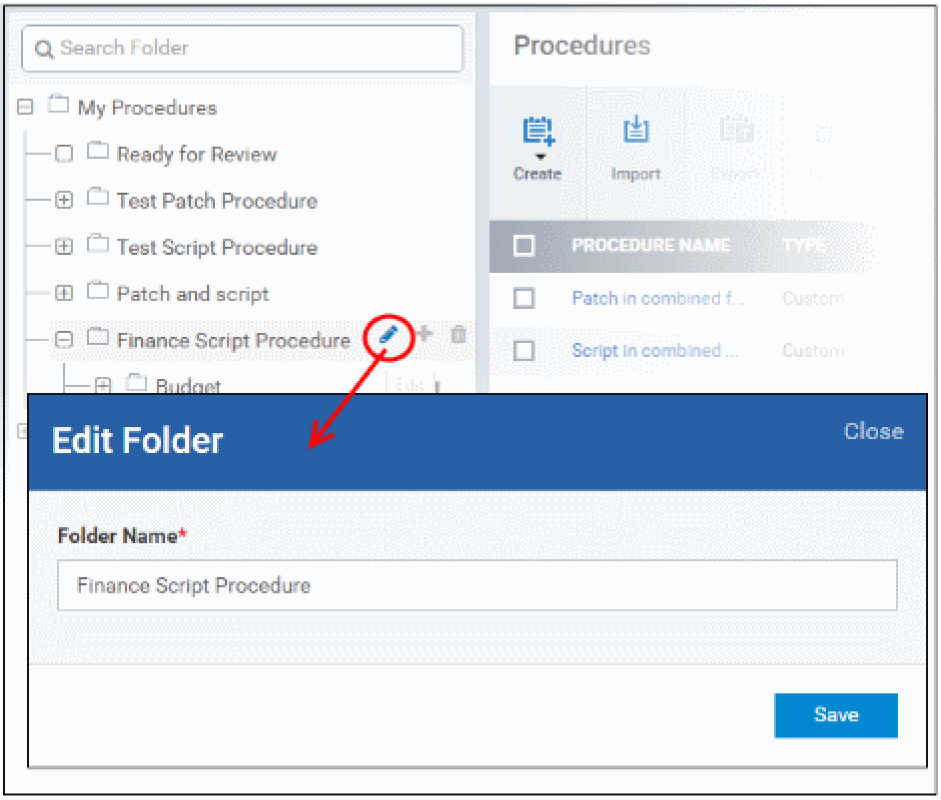
You can also add sub-folders of a sub-folder. Once sub folders are created, you can create new procedures inside them or import/clone predefined procedures.

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'



Folder Name*

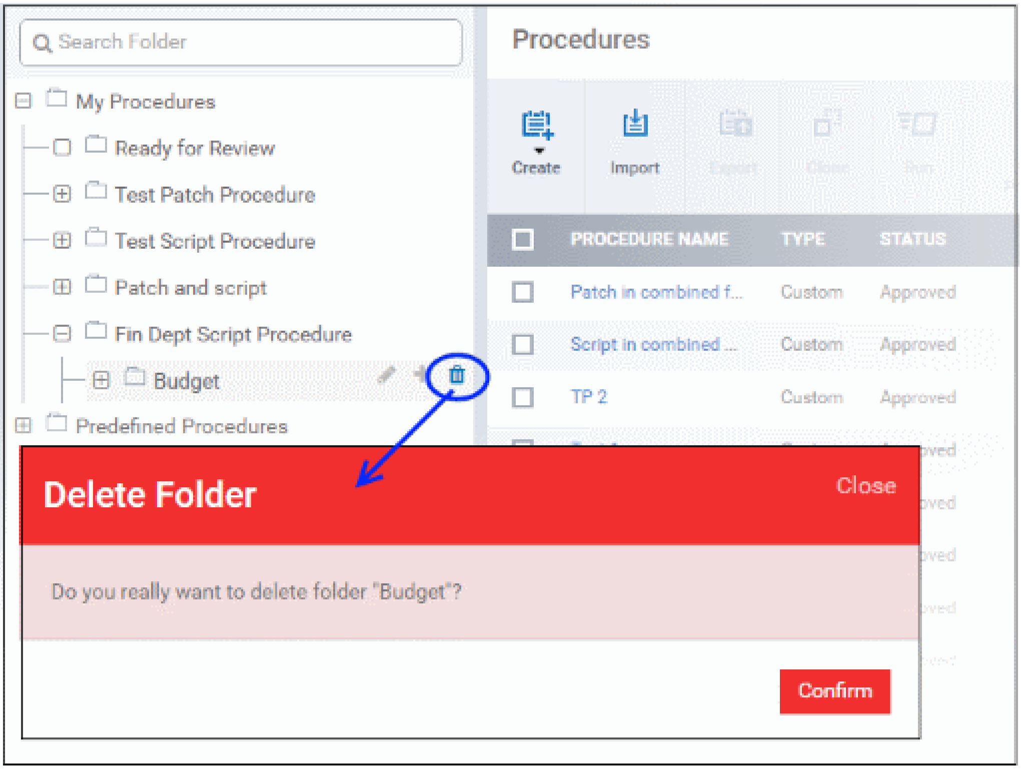
Finance Script Procedure

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



Do you really want to delete folder "Budget"?

- Click 'Confirm' to update the tree.

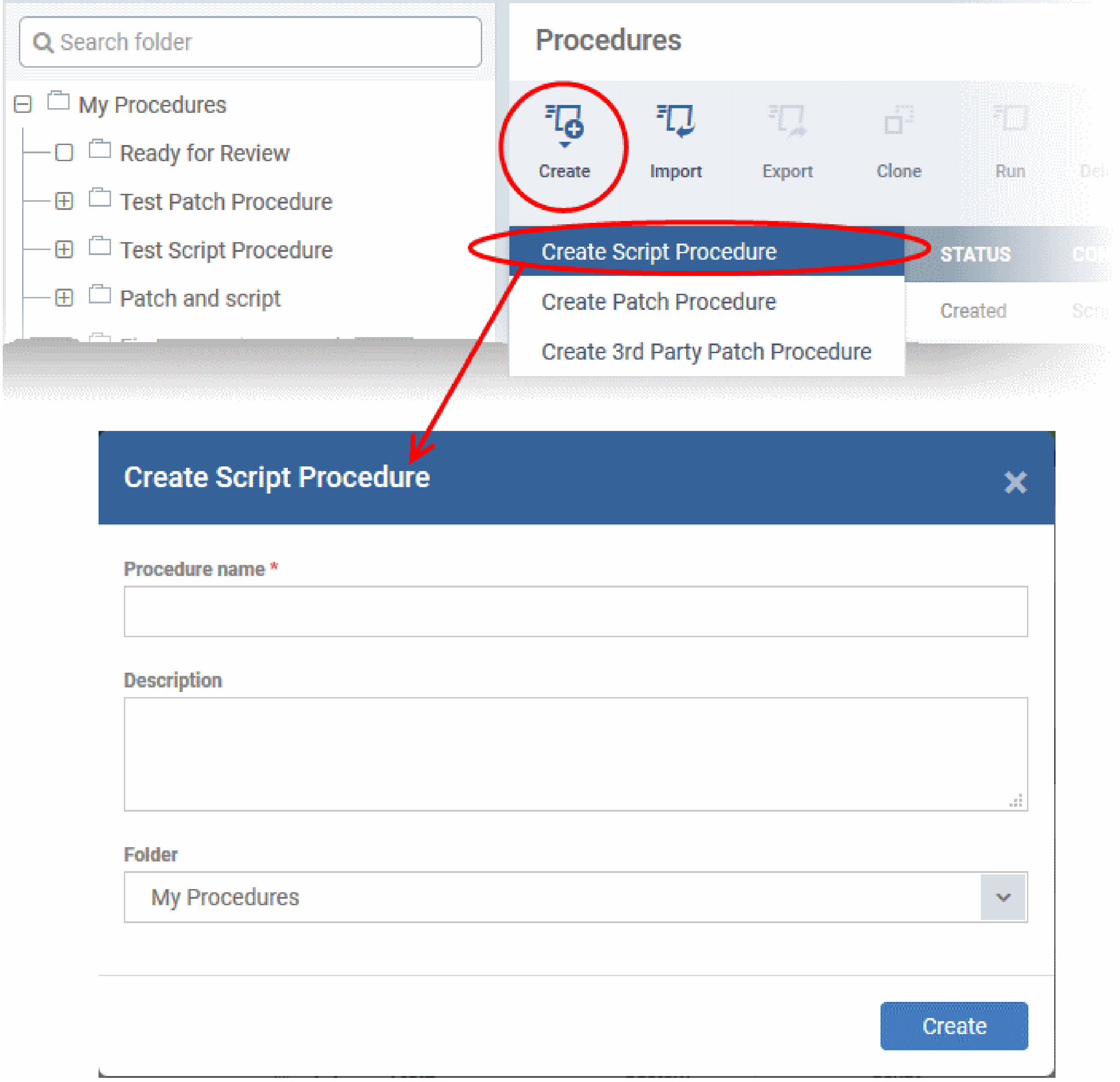
6.6.2. Create a Custom Procedure

ITSM allows you to create custom script / patch procedures according to your requirements. Click the following links to find out more:

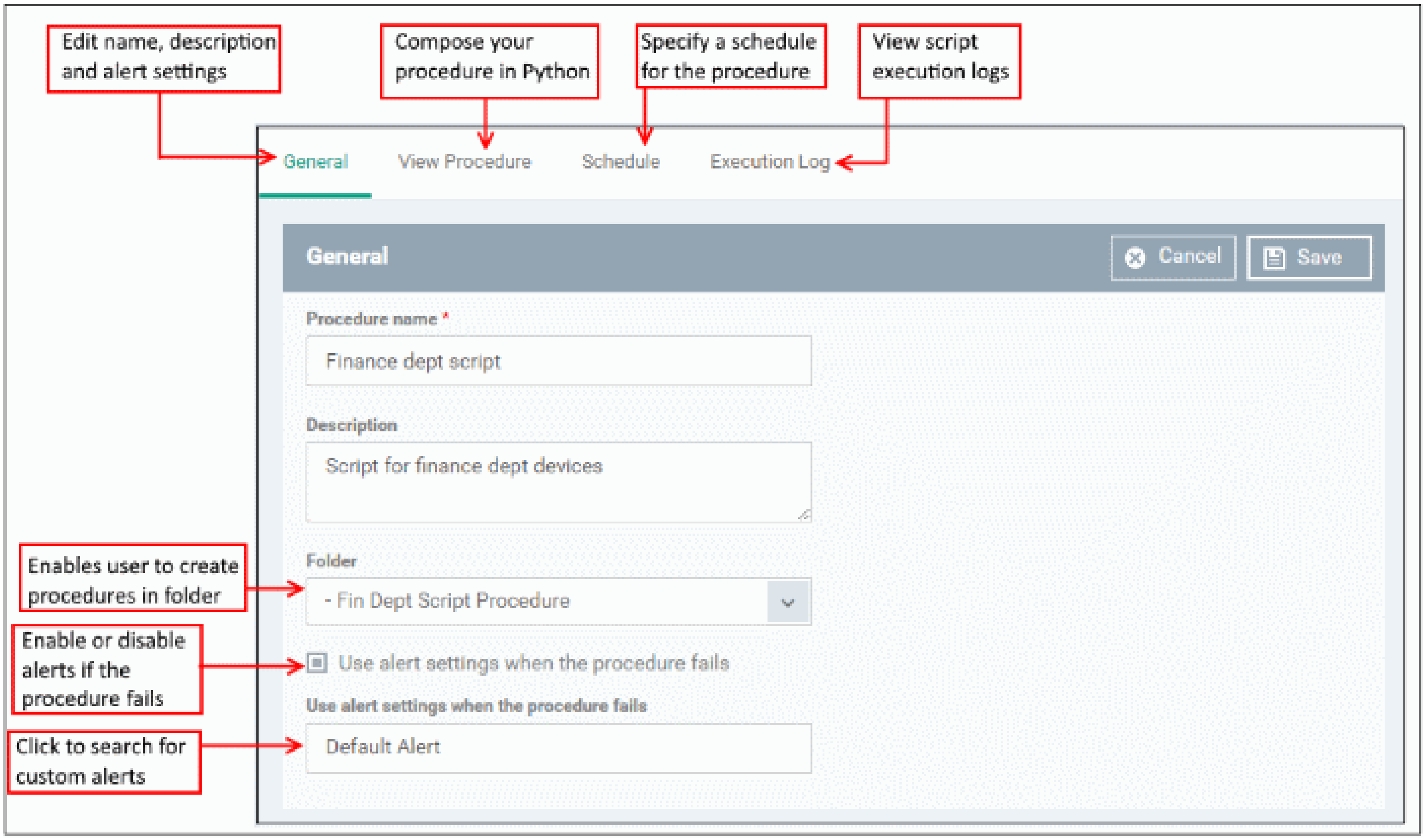
- **Creating a custom script procedure**
- **Creating a custom patch procedure**
- **Creating a custom 3rd Party application patch procedure**

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:



Edit name, description and alert settings

Compose your procedure in Python

Specify a schedule for the procedure

View script execution logs

Enables user to create procedures in folder

Enable or disable alerts if the procedure fails

Click to search for custom alerts

Procedure name * Finance dept script

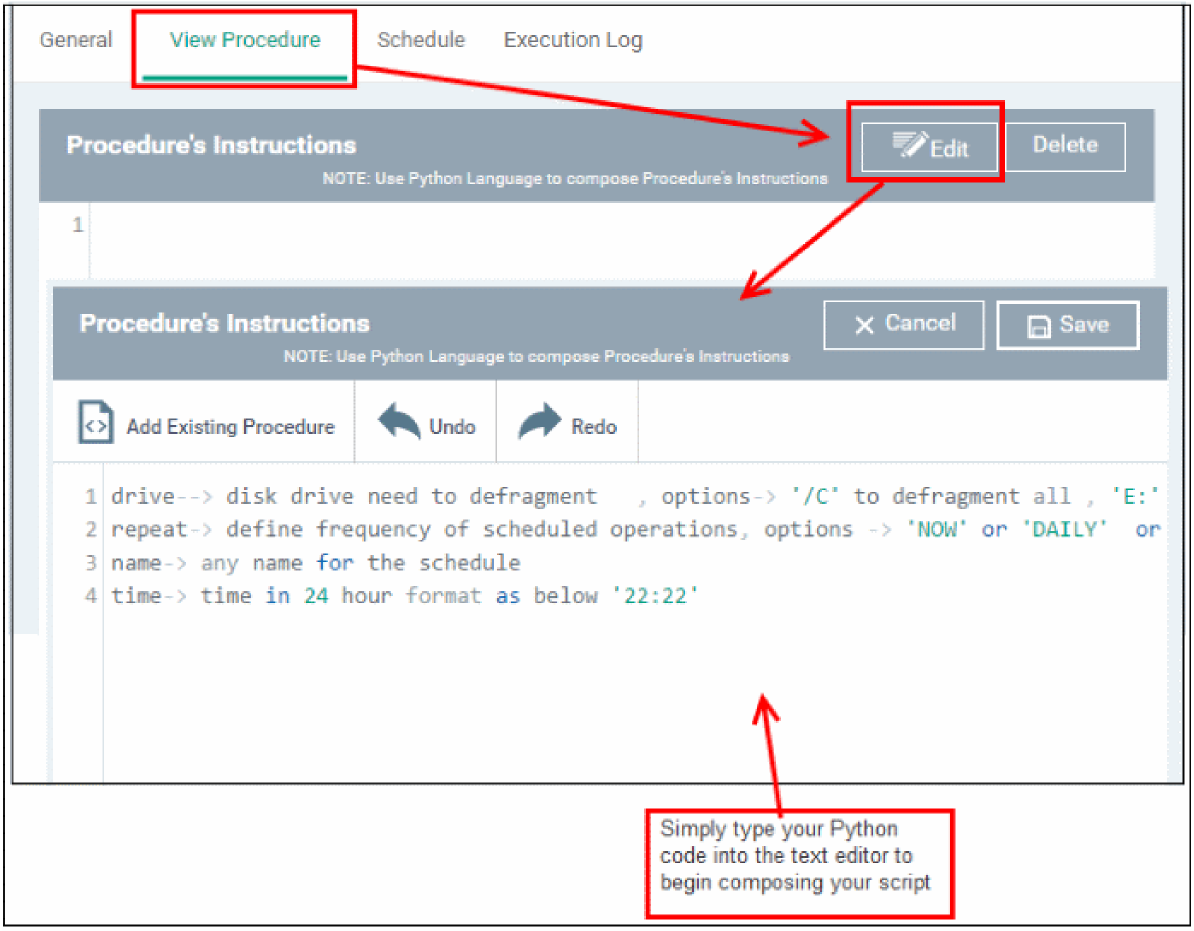
Description Script for finance dept devices

Folder - Fin Dept Script Procedure

☑ Use alert settings when the procedure fails

Use alert settings when the procedure fails: Default Alert

- 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:



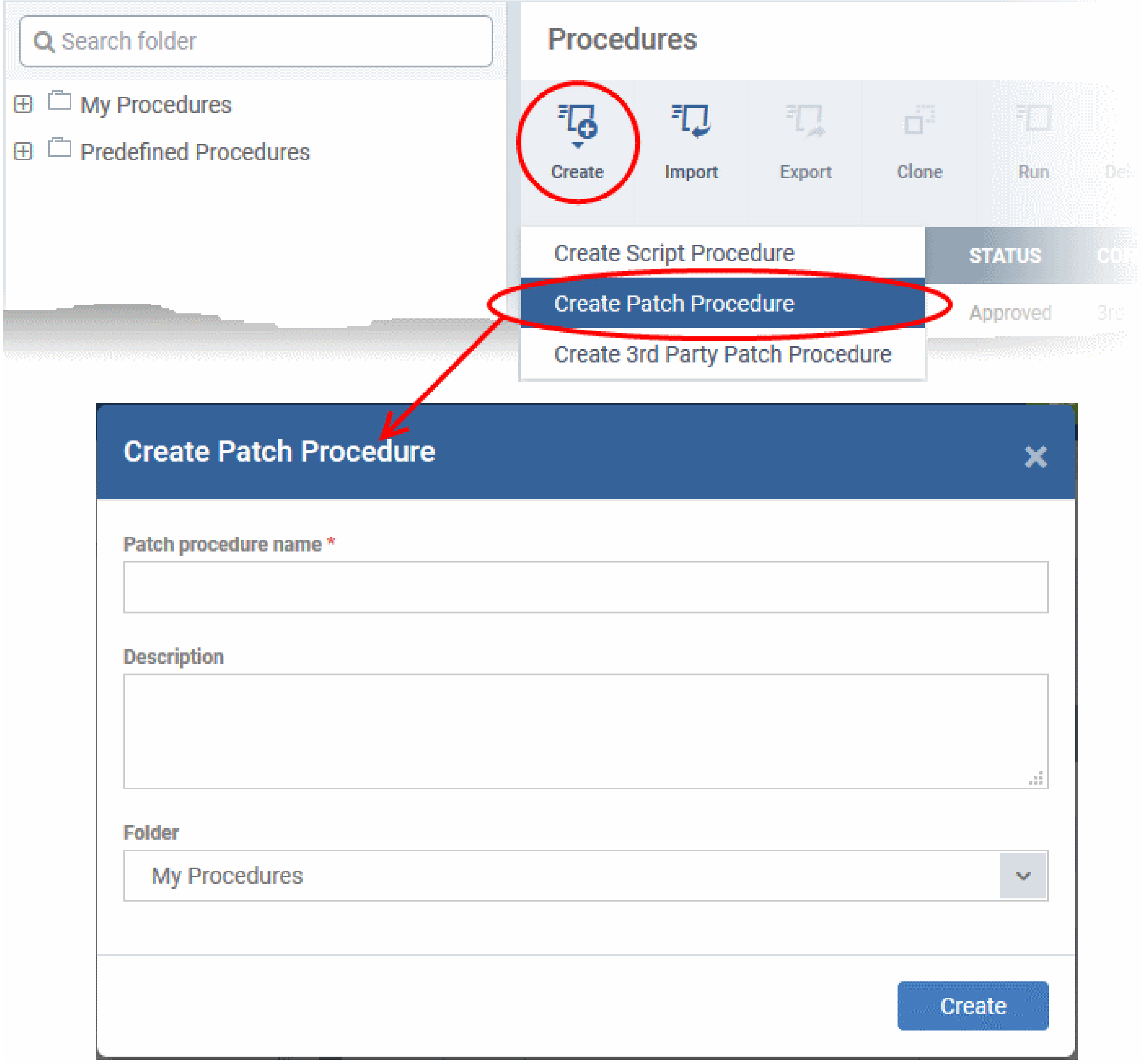
```
drive--> disk drive need to defragment   , options-> '/C' to defragment all , 'E:'
repeat-> define frequency of scheduled operations, options -> 'NOW' or 'DAILY'  or
name-> any name for the schedule
time-> time in 24 hour format as below '22:22'
```

Simply type your Python code into the text editor to begin composing your script

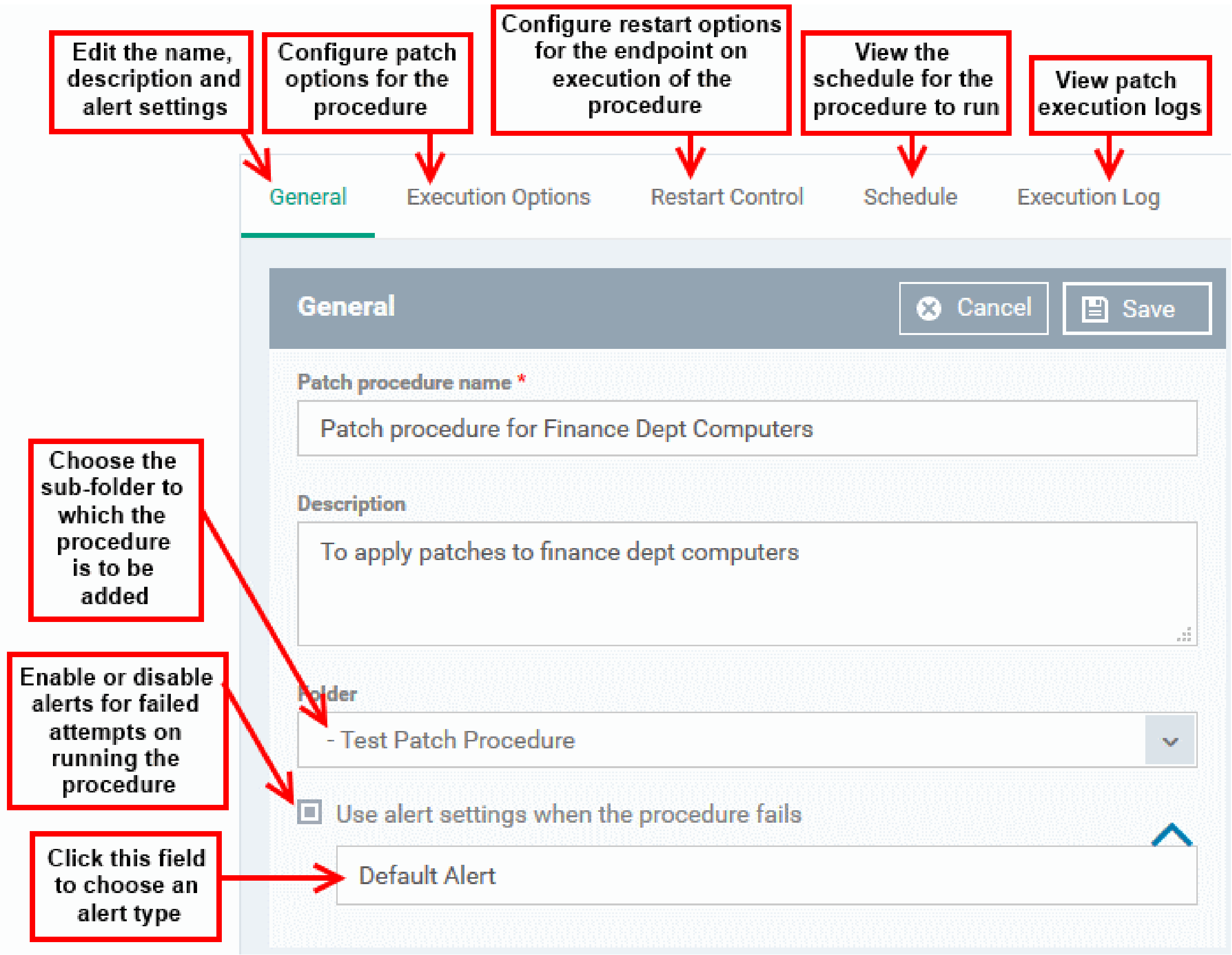
- After saving your script you need to **approve** it before it can be deployed in a profile.
- The 'Schedule' tab will be auto-populated once you deploy the procedure to a configuration profile and create a schedule for the procedure to run in the profile. Refer to the section **Add a Procedure to a 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. Comodo runs a free script library at **https://scripts.comodo.com/** which contains Python scripts covering a wide range of tasks. Feel free to try any script that fits your needs. You can also use this site to request a new script for a particular task you think will be useful. You can contribute your own scripts to the MSP forum at **https://forum.mspconsortium.com/forum/script-library**
- 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:



Edit the name, description and alert settings
Configure patch options for the procedure
Configure restart options for the endpoint on execution of the procedure
View the schedule for the procedure to run
View patch execution logs
General
Execution Options
Restart Control
Schedule
Execution Log
Choose the sub-folder to which the procedure is to be added
Enable or disable alerts for failed attempts on running the procedure
Click this field to choose an alert type
Cancel
Save

General

Patch procedure name *

Patch procedure for Finance Dept Computers

Description

To apply patches to finance dept computers

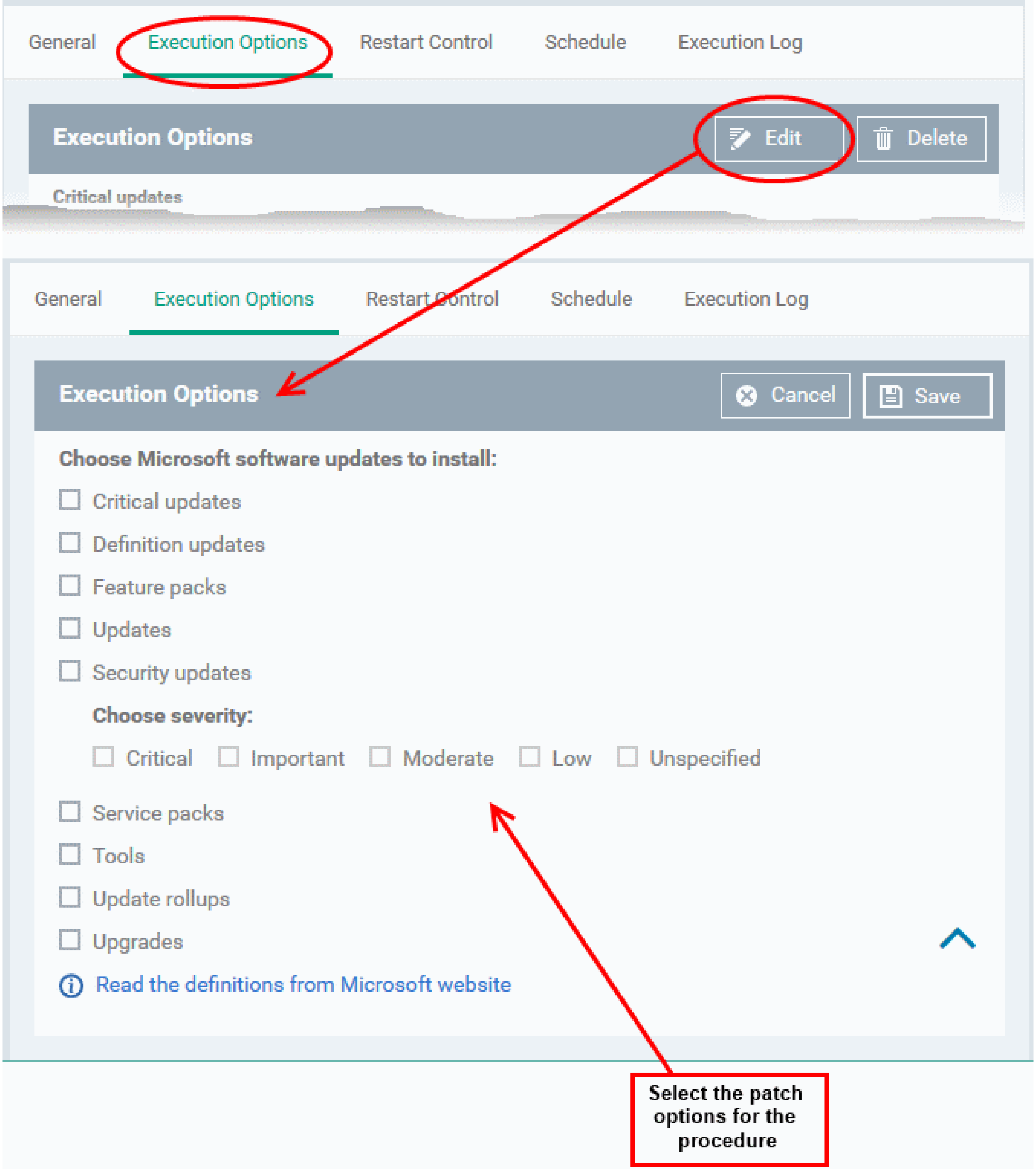
Folder

- Test Patch Procedure

☑ Use alert settings when the procedure fails

Default Alert

- 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.



Choose Microsoft software updates to install:

- □ Critical updates
- □ Definition updates
- □ Feature packs
- □ Updates
- □ Security updates

Choose severity:

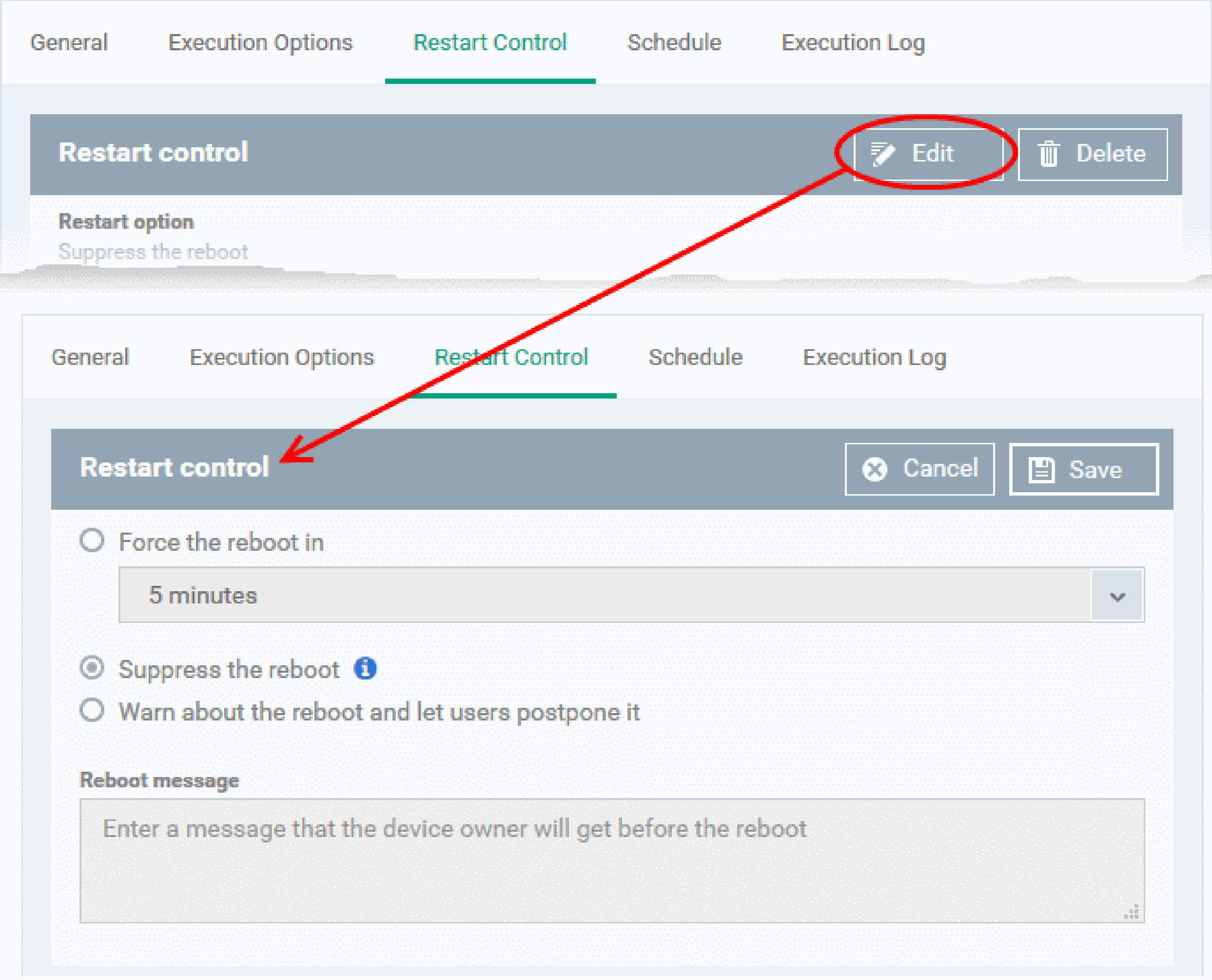
□ Critical □ Important □ Moderate □ Low □ Unspecified

- □ Service packs
- □ Tools
- □ Update rollups
- □ Upgrades

Read the definitions from Microsoft website

Select the patch options for the procedure

- 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.



Restart option
Suppress the reboot

○ Force the reboot in

5 minutes

● Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message

Enter a message that the device owner will get before the reboot

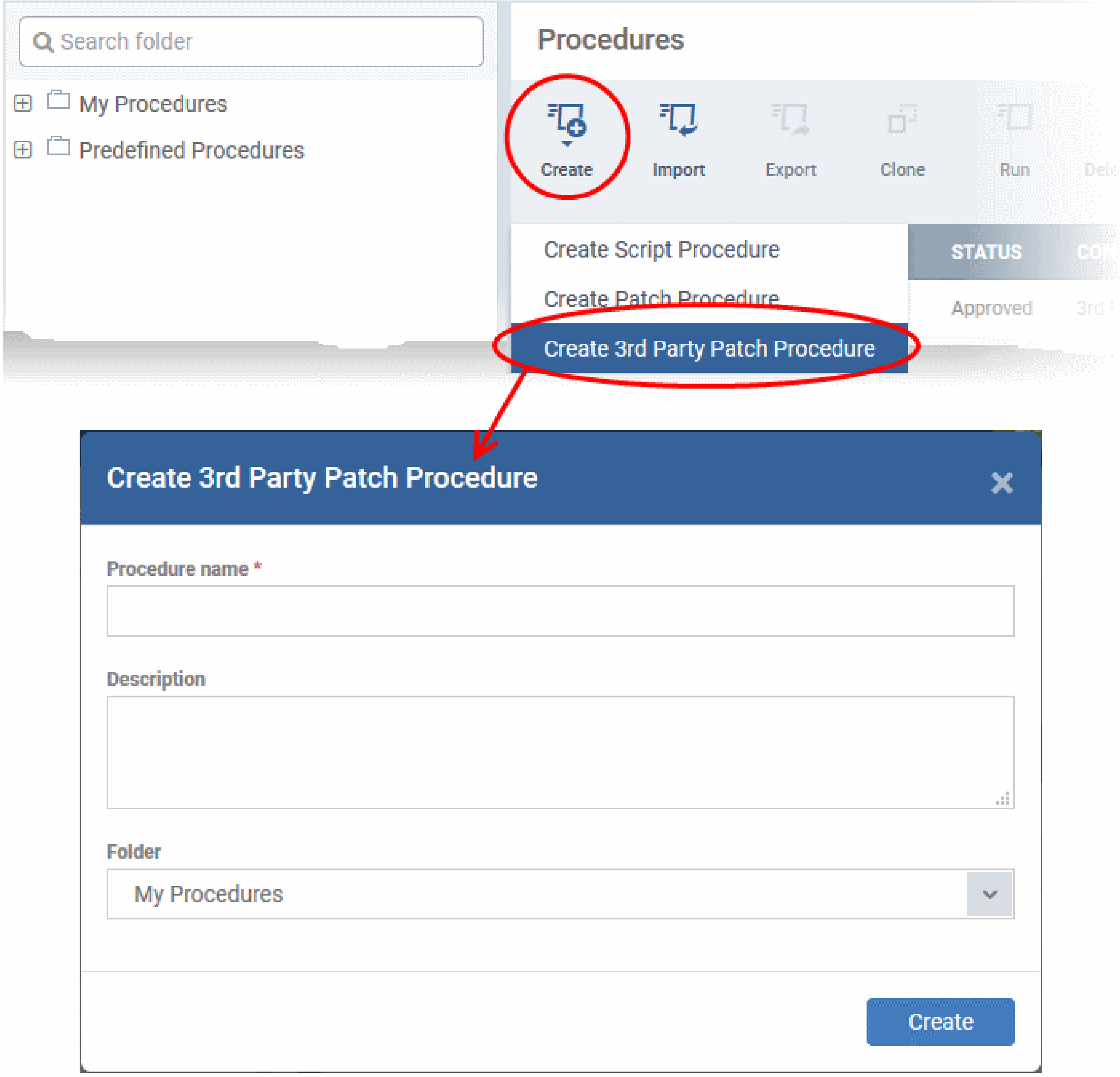
- You can choose to:
  - Continue the operation of the endpoint without restart by selecting 'Suppress the reboot'
  - Force restart the endpoint a certain period of time after the procedure has completed.

    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 will be automatically approved, added to the 'Procedures' list and 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.

To create a custom 3rd party patch procedure

- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create 3rd Party Patch Procedure'



Create 3rd Party Patch Procedure

Procedure name *

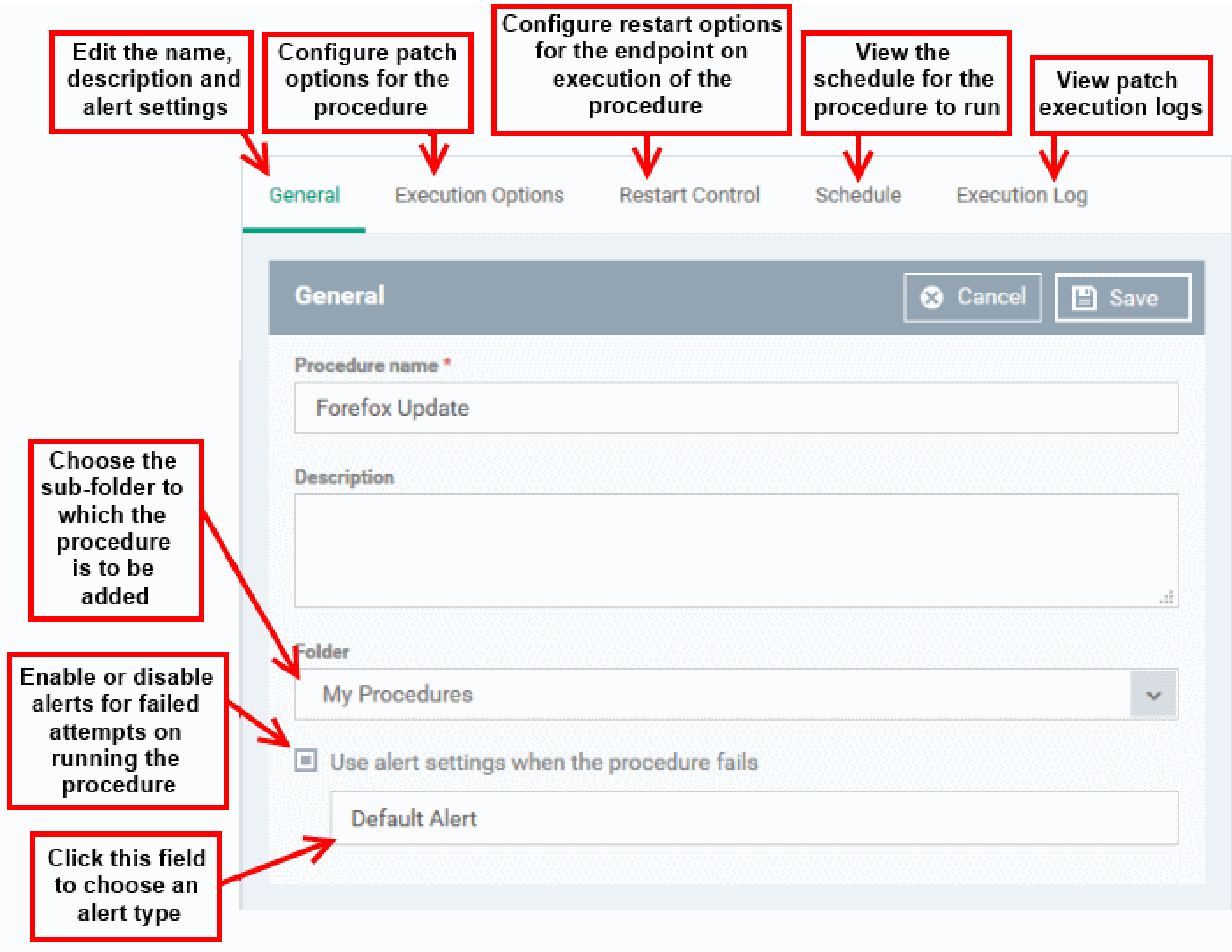
Description

Folder

My Procedures

Create

- Enter a name and description for your 3rd party 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
- Click 'Edit' if you want to change the general parameters.



Edit the name, description and alert settings
Configure patch options for the procedure
Configure restart options for the endpoint on execution of the procedure
View the schedule for the procedure to run
View patch execution logs
General
Execution Options
Restart Control
Schedule
Execution Log
General
Cancel
Save
Choose the sub-folder to which the procedure is to be added
Enable or disable alerts for failed attempts on running the procedure
Click this field to choose an alert type

Procedure name *

Forefox Update

Description

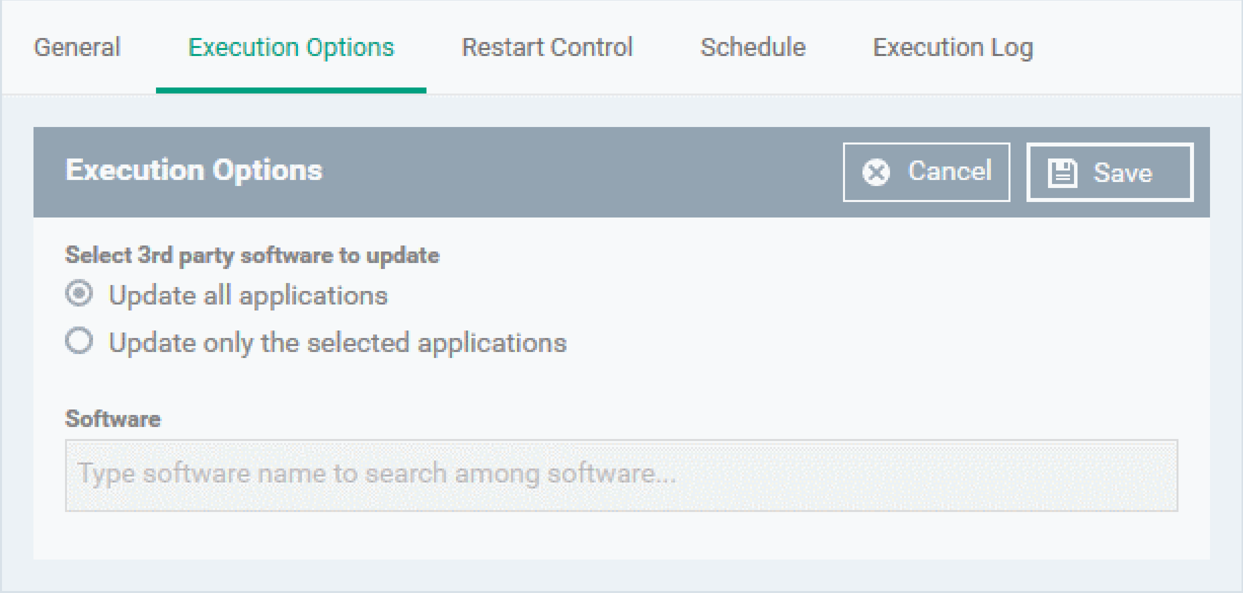
Folder

My Procedures

☐ Use alert settings when the procedure fails

Default Alert

- To configure patch options for your procedure, click the 'Execution Options' tab followed by the 'Edit' button. You can select the applications to be updated from the options.



Select 3rd party software to update

● Update all applications

○ Update only the selected applications

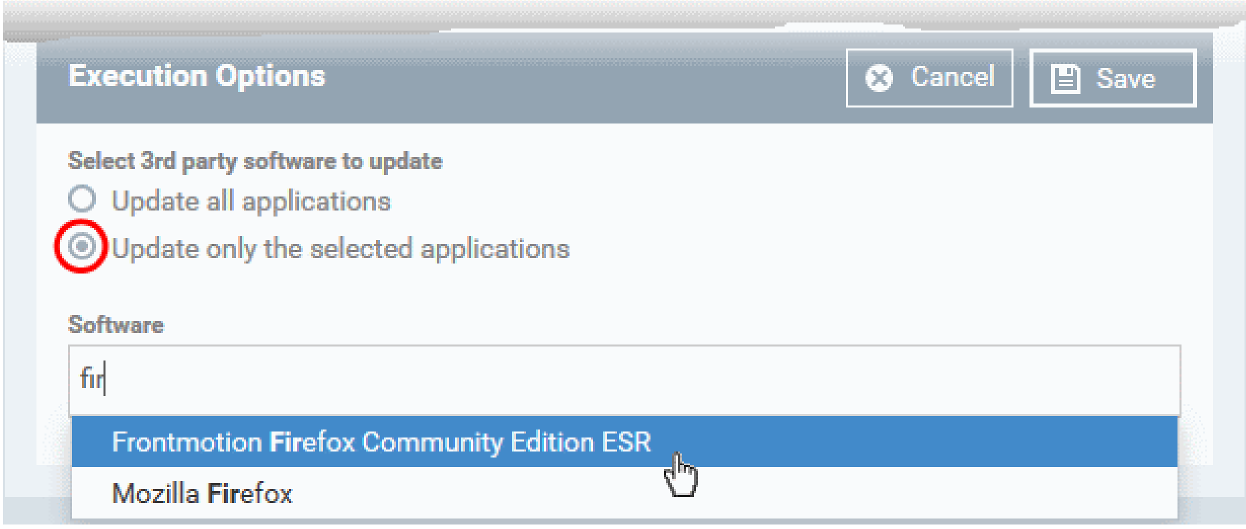
Software

Type software name to search among software...

- **Select 3rd party software to update** - Allows you to choose whether all upgradable applications identified at the endpoint to be updated or only specific application(s) is/are to be updated.
  - **Update all applications** - Select this option if you want all outdated applications in the endpoint to be updated on running the procedure
  - **Update only the selected applications** - Select this option if you want only specified applications

are to be updated on the endpoint, then specify the applications to be updated.

- Start entering the first few characters of the application. The upgradable applications identified from all managed endpoints and matching the search criteria will be displayed as options
- Select the application from the list



Select 3rd party software to update

○ Update all applications

● Update only the selected applications

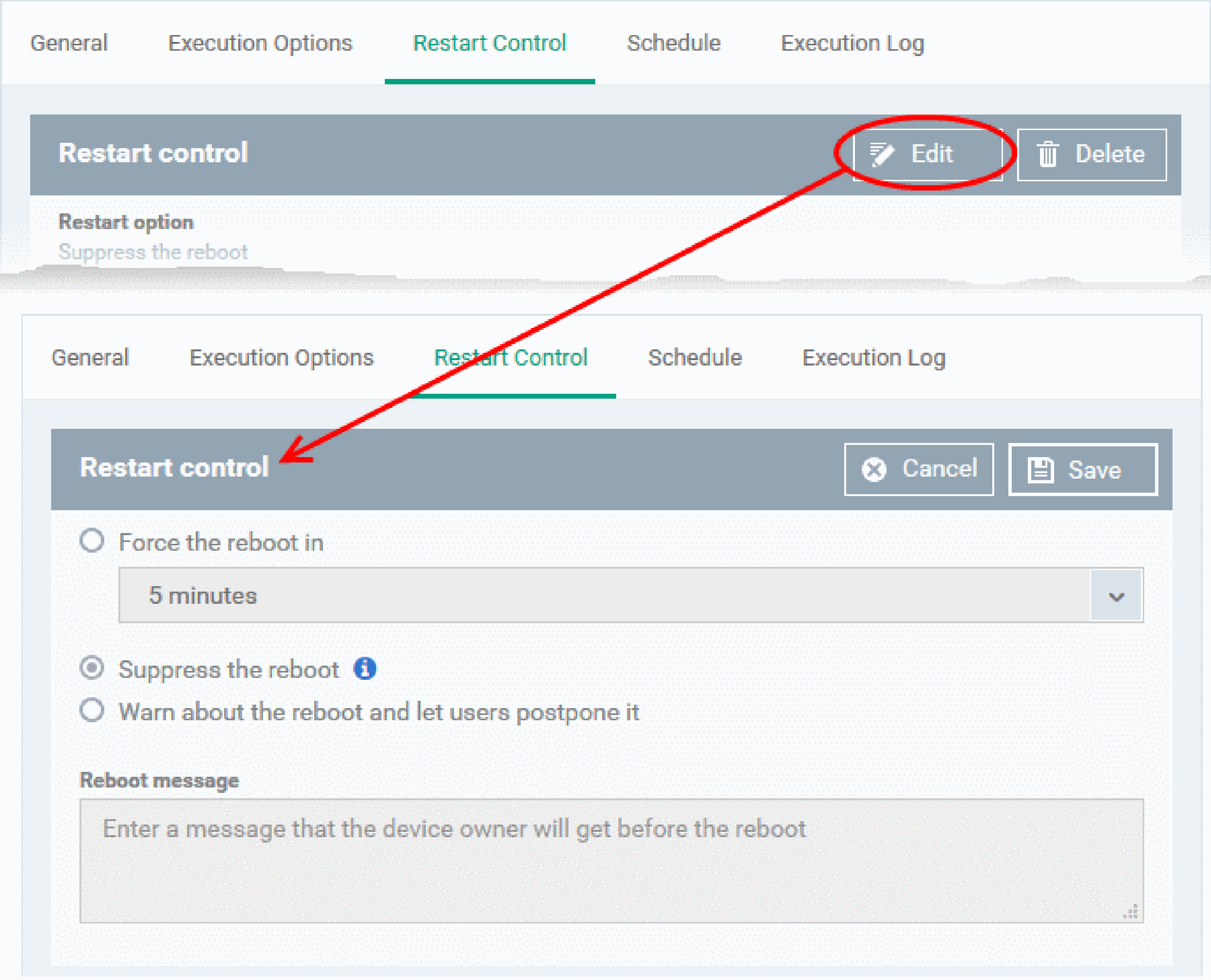
Software

fir

Frontmotion **Fire**fox Community Edition ESR

Mozilla **Fire**fox

- 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.



Restart option

Suppress the reboot

○ Force the reboot in

5 minutes

● Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message

Enter a message that the device owner will get before the reboot

- 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.

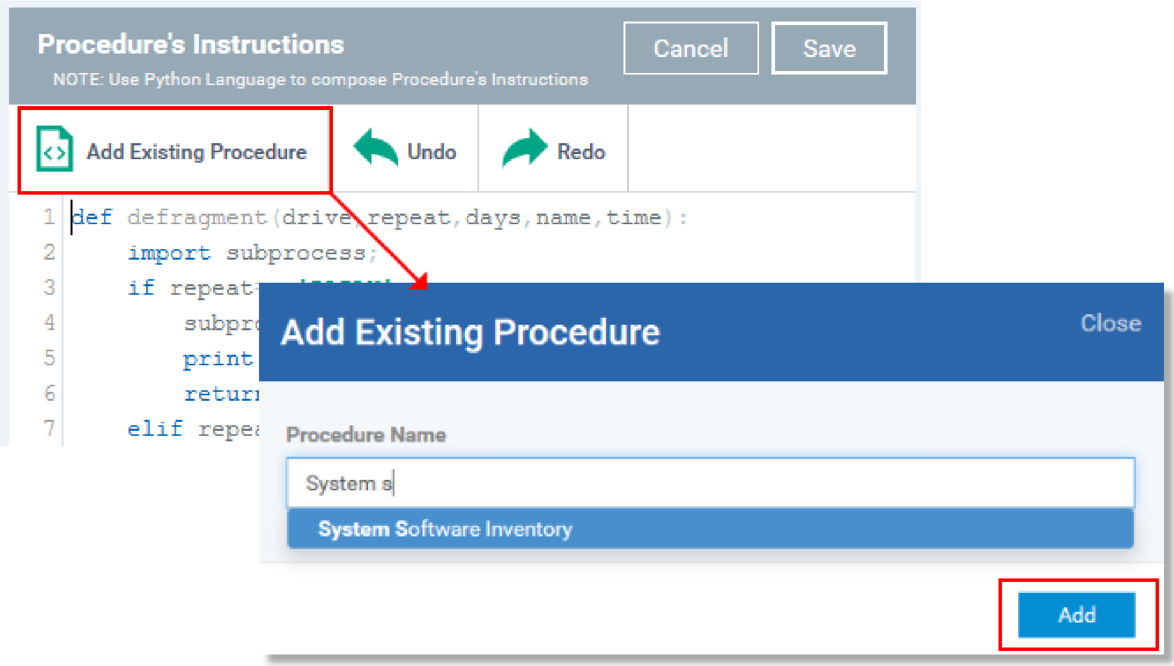
- The 'Schedule' tab will be auto-populated once you add the procedure to a configuration profile and schedule its execution. See **Add a Procedure to a Profile / Procedure Schedules** for more details.
- The 'Execution Log' will be auto-populated after the procedure has been successful executed as part 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 will be automatically approved, added to the 'Procedures' list and can be deployed in a profile.

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.



```
def defragment(drive,repeat,days,name,time):
    import subprocess;
    if repeat-
        subpr
        print
        retur
    elif repe
```

Procedure Name: System s

System Software Inventory

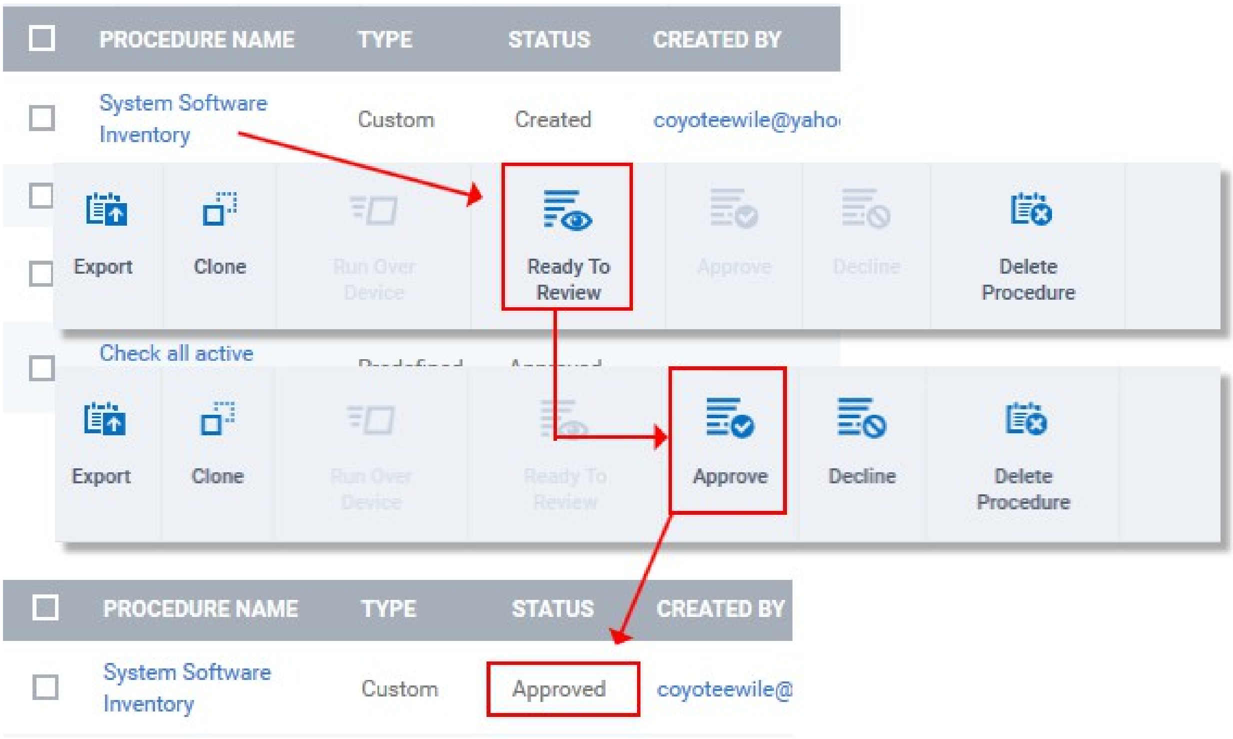
- Click 'Save' for your changes to take effect.

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.



□	PROCEDURE NAME	TYPE	STATUS	CREATED BY
□	System Software Inventory	Custom	Created	coyoteewile@yaho
□	Check all active	Predefined	Approved	

□	PROCEDURE NAME	TYPE	STATUS	CREATED BY
□	System Software Inventory	Custom	Approved	coyoteewile@

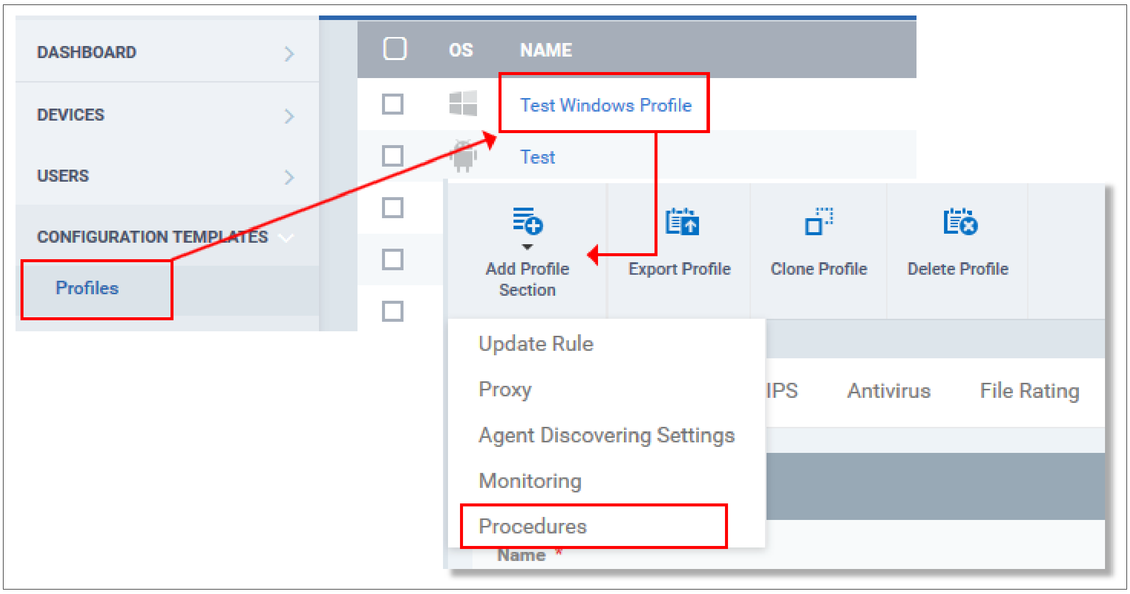
- Approved procedures can be selected and added to a profile.

6.6.5. Add a Procedure to a Profile / Procedure Schedules

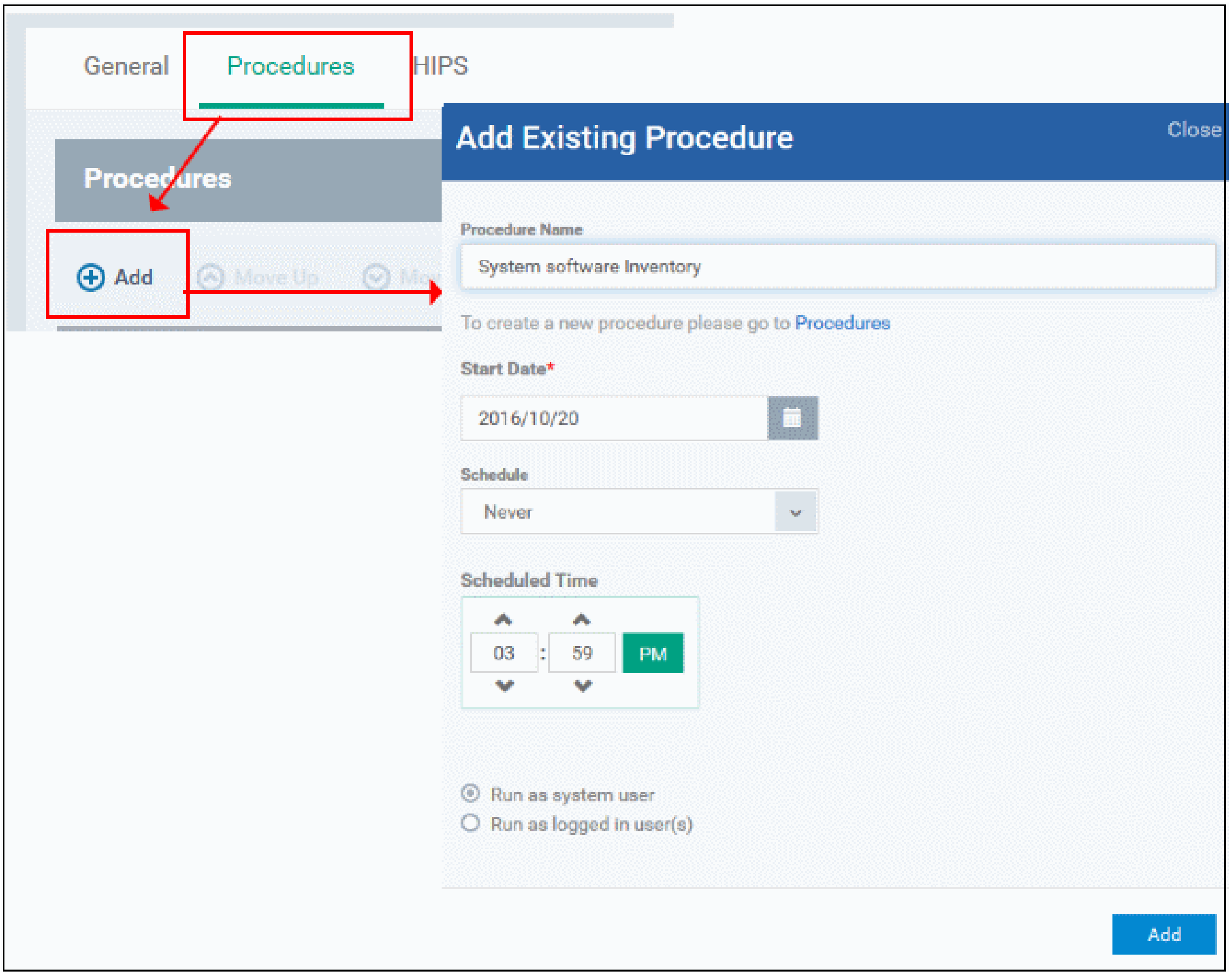
Note. Procedure schedules for both script and patch procedures are actually configured in the 'Profiles' area. You set a schedule for a procedure when you add a procedure to a profile. The 'Schedule' tab in the procedures area essentially allows you to view profiles which are scheduled to use the procedure.

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



Procedure Name: System software Inventory

To create a new procedure please go to Procedures

Start Date*: 2016/10/20

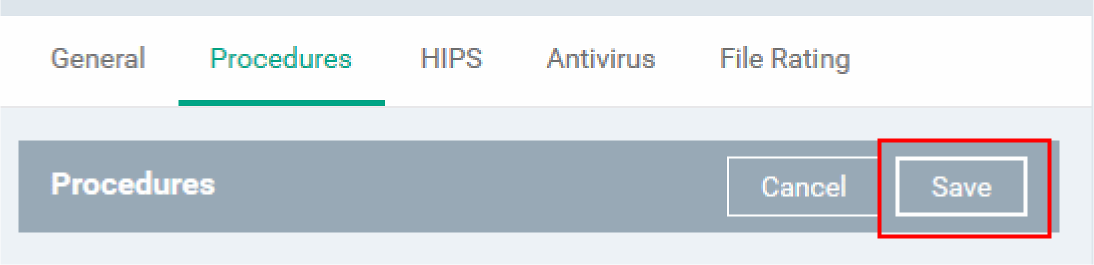
Schedule: Never

Scheduled Time: 03 : 59 PM

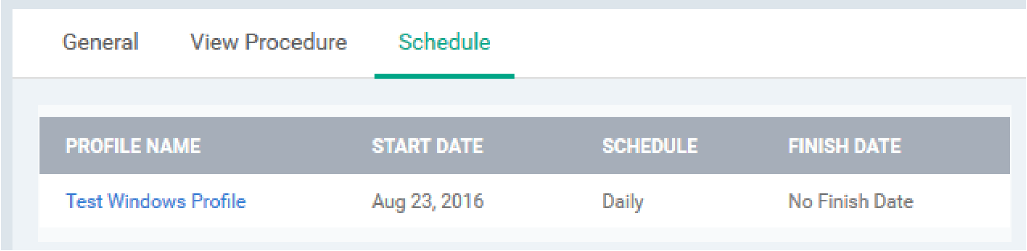
● Run as system user
○ Run as logged in user(s)

- 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:



PROFILE NAME	START DATE	SCHEDULE	FINISH DATE
Test Windows Profile	Aug 23, 2016	Daily	No Finish Date

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.

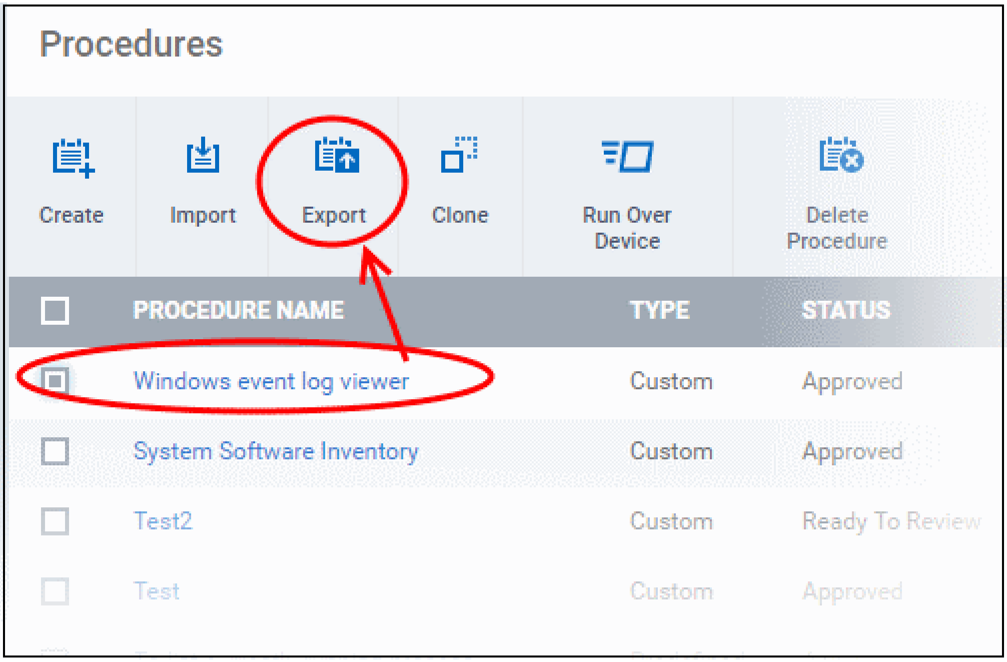
6.6.6. Import / Export / Clone Procedures

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.

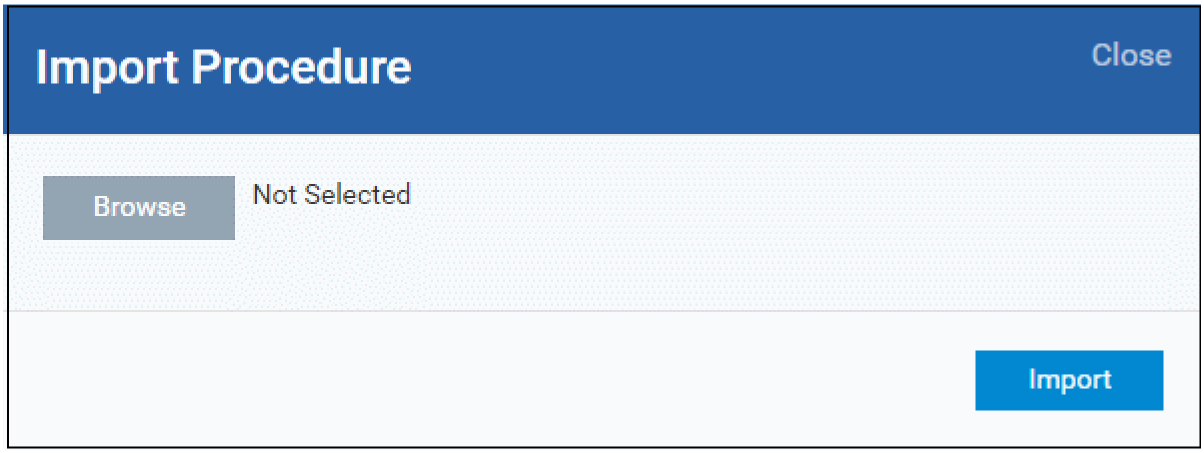


☐	PROCEDURE NAME	TYPE	STATUS
☒	Windows event log viewer	Custom	Approved
☐	System Software Inventory	Custom	Approved
☐	Test2	Custom	Ready To Review
☐	Test	Custom	Approved

The selected procedure file will be saved in your default download location.

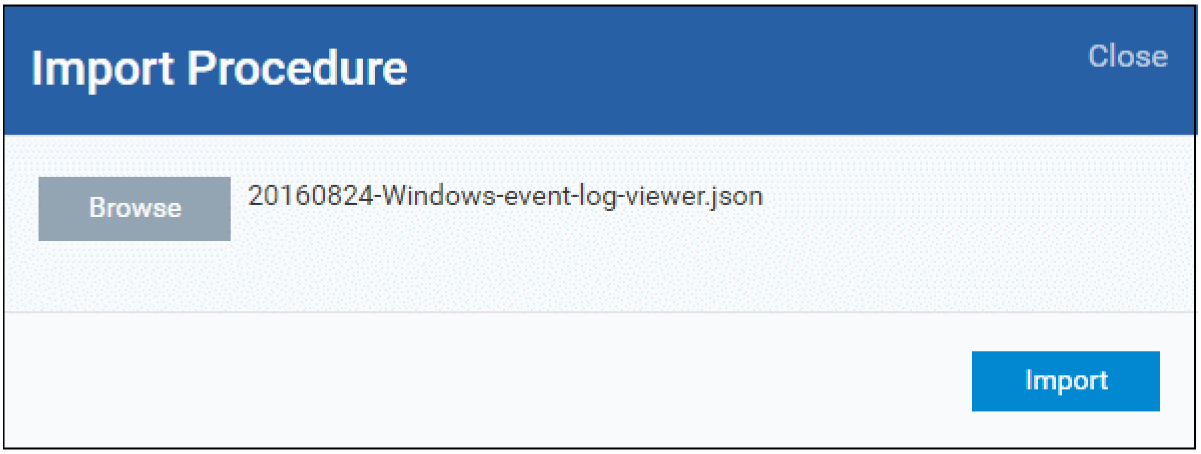
To import a procedure

- 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.



Import Procedure

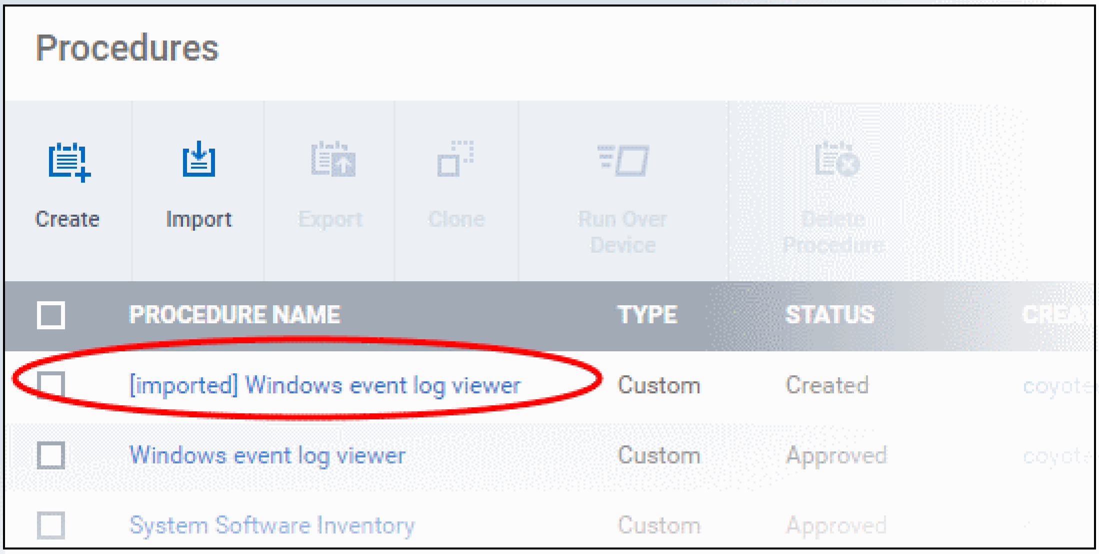
Close

Browse 20160824-Windows-event-log-viewer.json

Import

- Click 'Import'

The procedure will be added to the list with the word 'Imported' to distinguish it from other procedures.



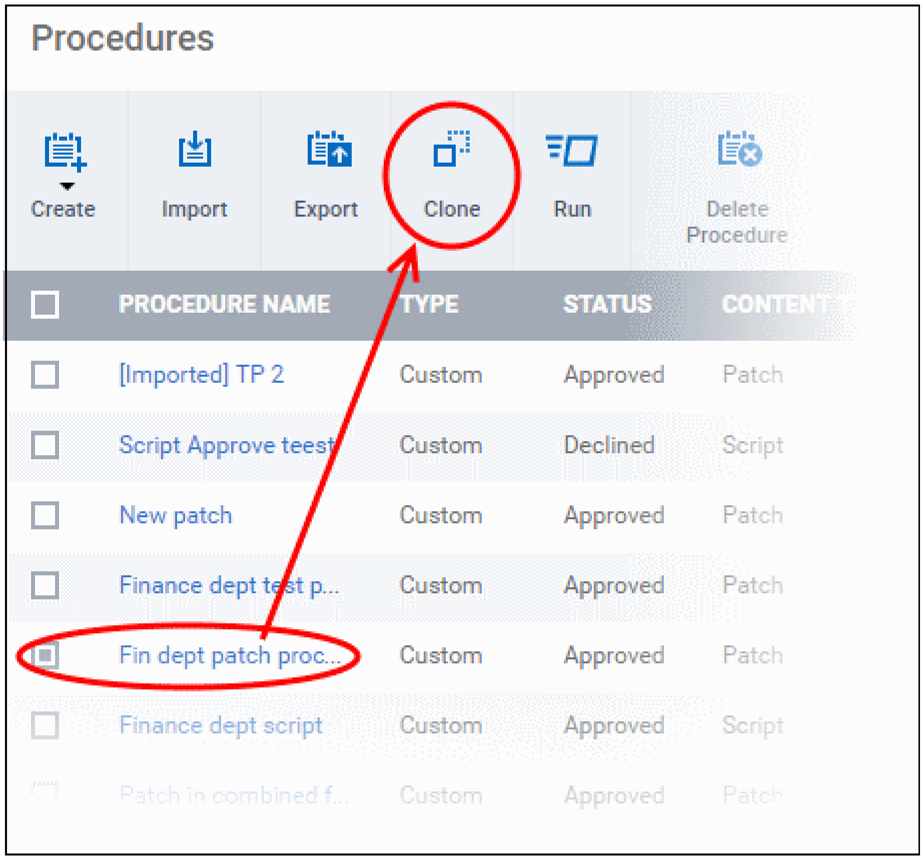
Procedures

□	PROCEDURE NAME	TYPE	STATUS	CREA
□	[imported] Windows event log viewer	Custom	Created	coyot
□	Windows event log viewer	Custom	Approved	coyot
□	System Software Inventory	Custom	Approved	

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.

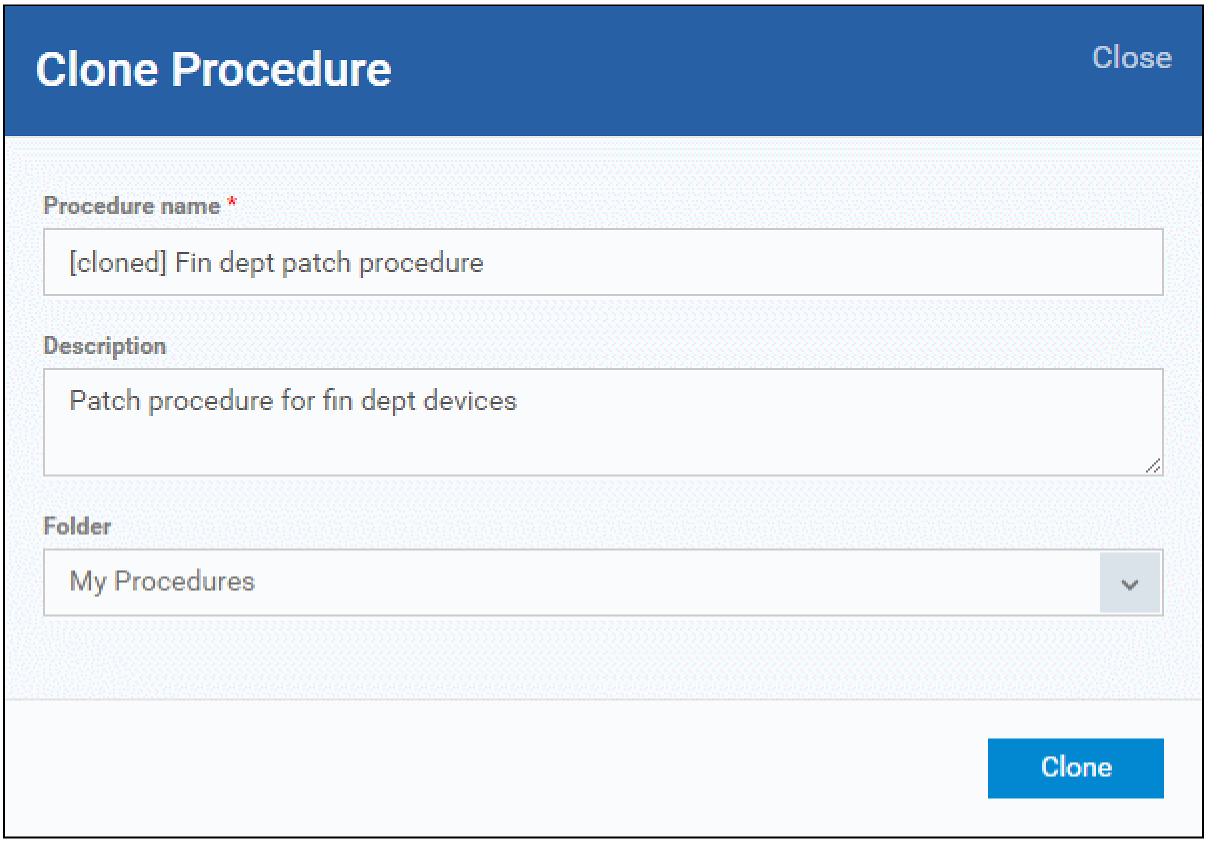
To clone a procedure

- Click 'Configuration Templates' > 'Procedures'
- Select the procedure and click 'Clone' at the top.



□	PROCEDURE NAME	TYPE	STATUS	CONTENT T
□	[Imported] TP 2	Custom	Approved	Patch
□	Script Approve teest	Custom	Declined	Script
□	New patch	Custom	Approved	Patch
□	Finance dept test p...	Custom	Approved	Patch
☒	Fin dept patch proc...	Custom	Approved	Patch
□	Finance dept script	Custom	Approved	Script
□	Patch in combined f...	Custom	Approved	Patch

The 'Clone Procedure' dialog will be displayed with name of the selected procedure auto filled in the name field.



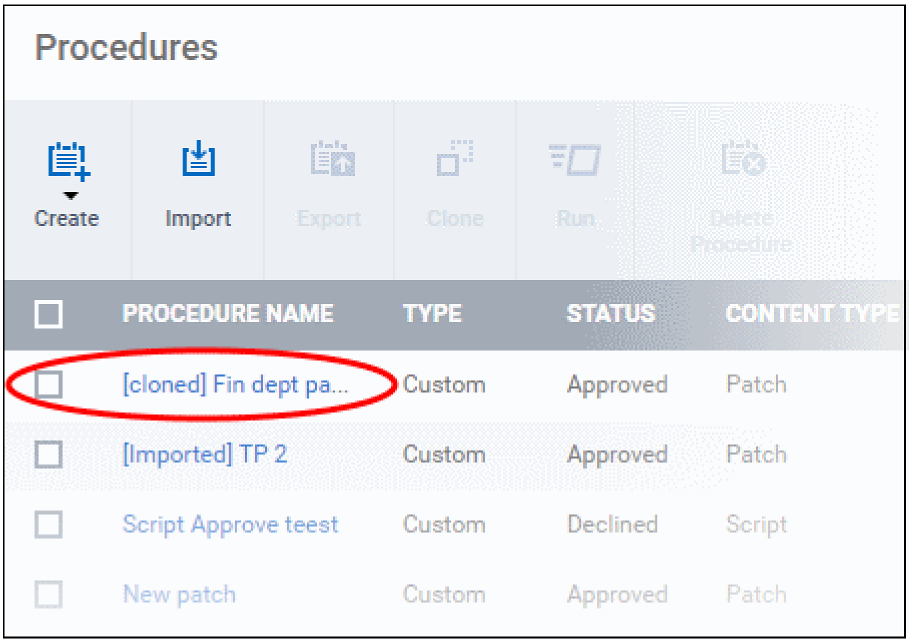
Procedure name *
[cloned] Fin dept patch procedure

Description
Patch procedure for fin dept devices

Folder
My Procedures

- 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:



□	PROCEDURE NAME	TYPE	STATUS	CONTENT TYPE
□	[cloned] Fin dept pa...	Custom	Approved	Patch
□	[Imported] TP 2	Custom	Approved	Patch
□	Script Approve teest	Custom	Declined	Script
□	New patch	Custom	Approved	Patch

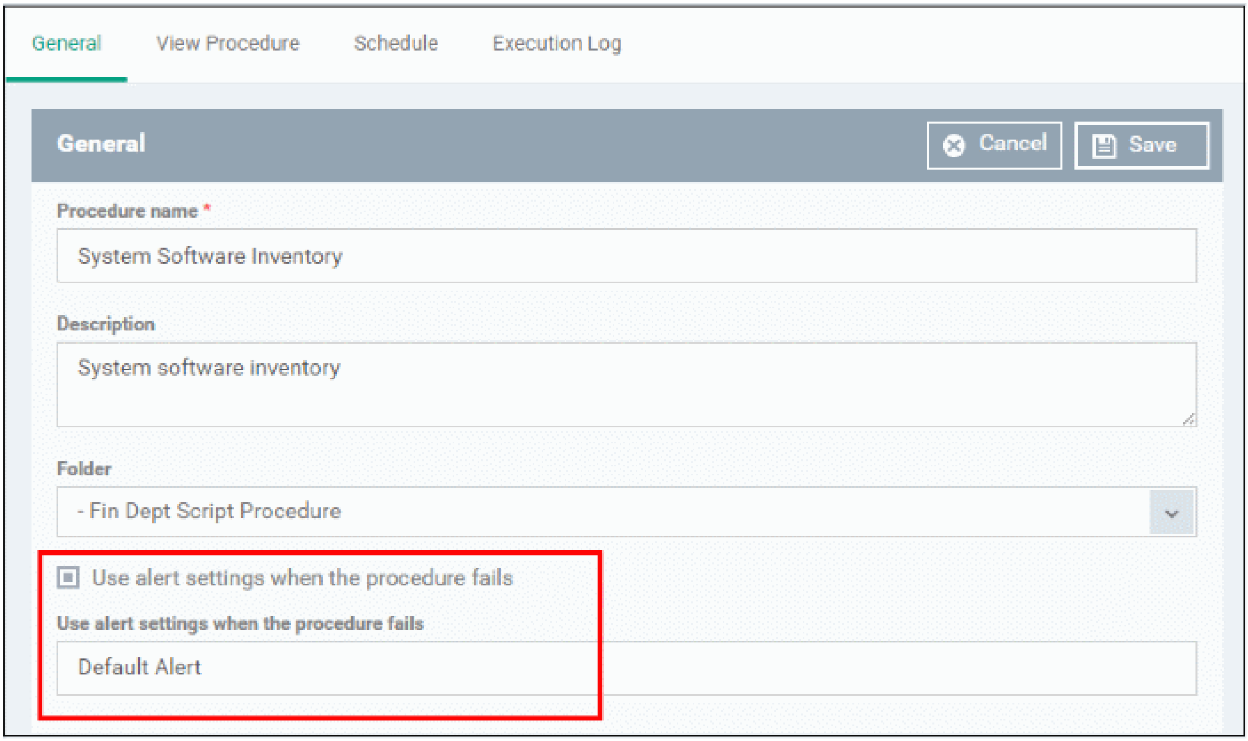
Please note the status of the cloned procedure will be same as that of the procedure that was cloned. For example, if the status was approved then the cloned procedure will also be of the same status. Please note the procedure has to be **approved** in order to deploy it in profiles.

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.



Procedure name *

System Software Inventory

Description

System software inventory

Folder

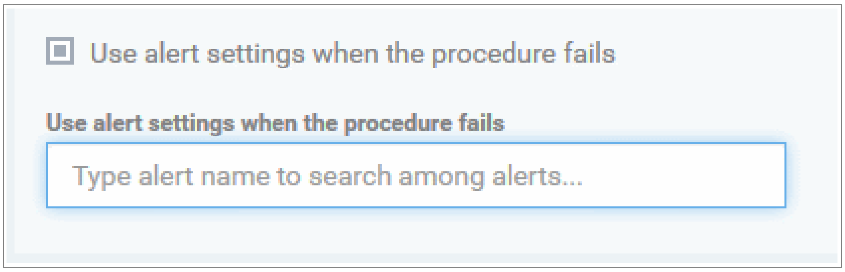
- Fin Dept Script Procedure

▣ Use alert settings when the procedure fails

Use alert settings when the procedure fails

Default Alert

- 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.

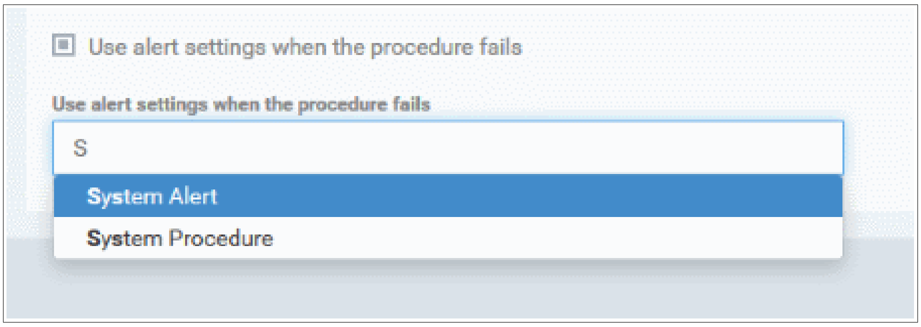


▣ Use alert settings when the procedure fails

Use alert settings when the procedure fails

Type alert name to search among alerts...

- Enter fully or partly the name of the predefined alert in the field. Matching alerts will be displayed.



▣ Use alert settings when the procedure fails

Use alert settings when the procedure fails

S

- 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

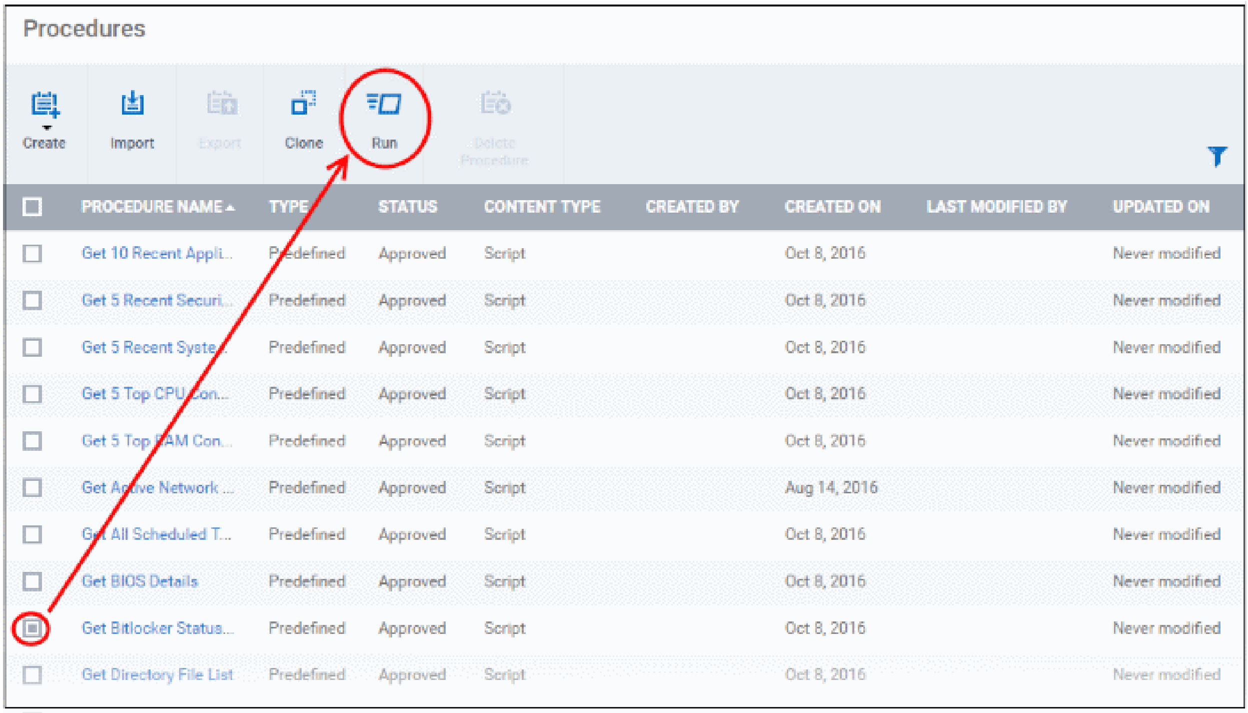
Procedures can be run on devices in three ways:

- 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

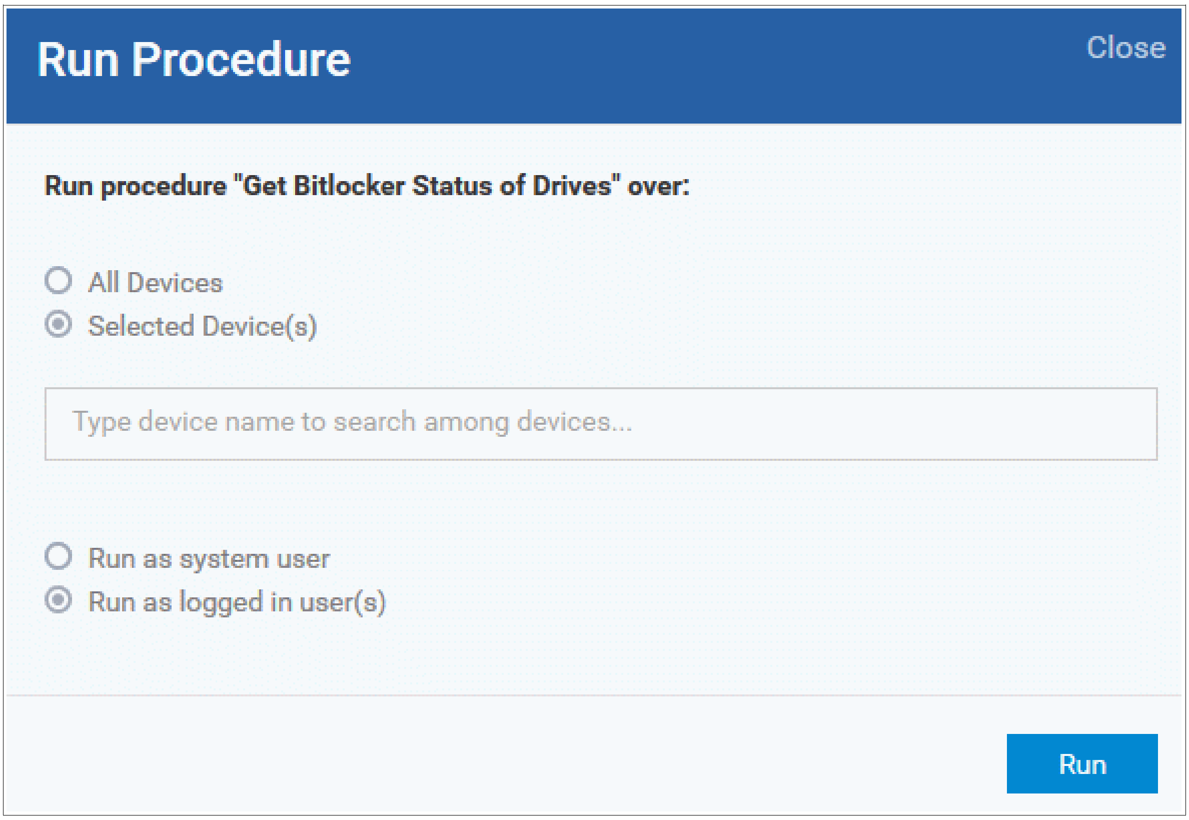
- Click 'Configuration Templates' > 'Procedures'
- Select the check box beside the procedure that you want to apply. Please note only **approved** procedures can be applied. You can also run only one procedure at a time.



□	PROCEDURE NAME ▲	TYPE	STATUS	CONTENT TYPE	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
□	Get 10 Recent Appli...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get 5 Recent Securi...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get 5 Recent Syste...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get 5 Top CPU Con...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get 5 Top RAM Con...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get Active Network ...	Predefined	Approved	Script		Aug 14, 2016		Never modified
□	Get All Scheduled T...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get BIOS Details	Predefined	Approved	Script		Oct 8, 2016		Never modified
☑	Get Bitlocker Status...	Predefined	Approved	Script		Oct 8, 2016		Never modified
□	Get Directory File List	Predefined	Approved	Script		Oct 8, 2016		Never modified

- Click 'Run' at the top

The 'Run' dialog will be displayed:



Run Procedure

Close

Run procedure "Get Bitlocker Status of Drives" over:

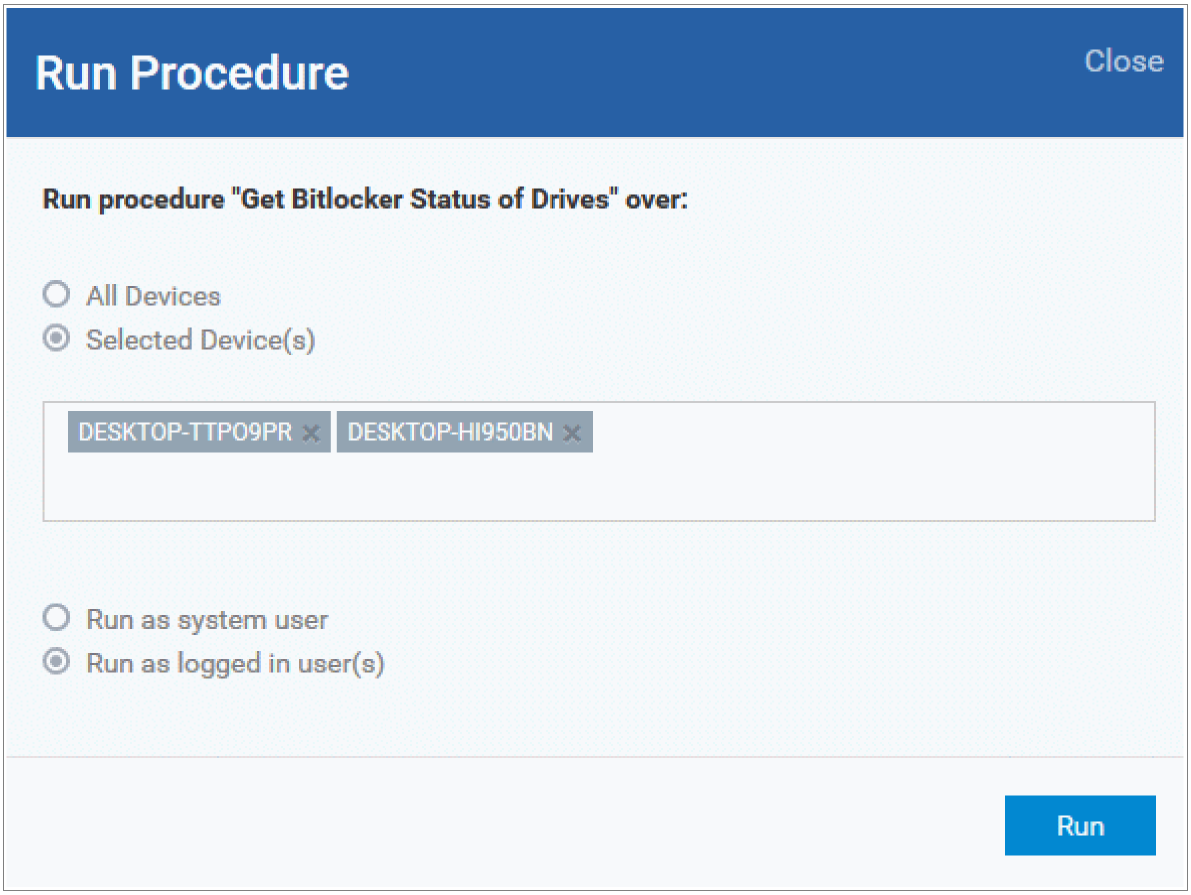
○ All Devices
● Selected Device(s)

Type device name to search among devices...

○ Run as system user
● Run as logged in user(s)

Run

- 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.



Run Procedure

Close

Run procedure "Get Bitlocker Status of Drives" over:

○ All Devices
● Selected Device(s)

DESKTOP-TTPO9PR ✕ DESKTOP-HI950BN ✕

○ Run as system user
● Run as logged in user(s)

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. 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.

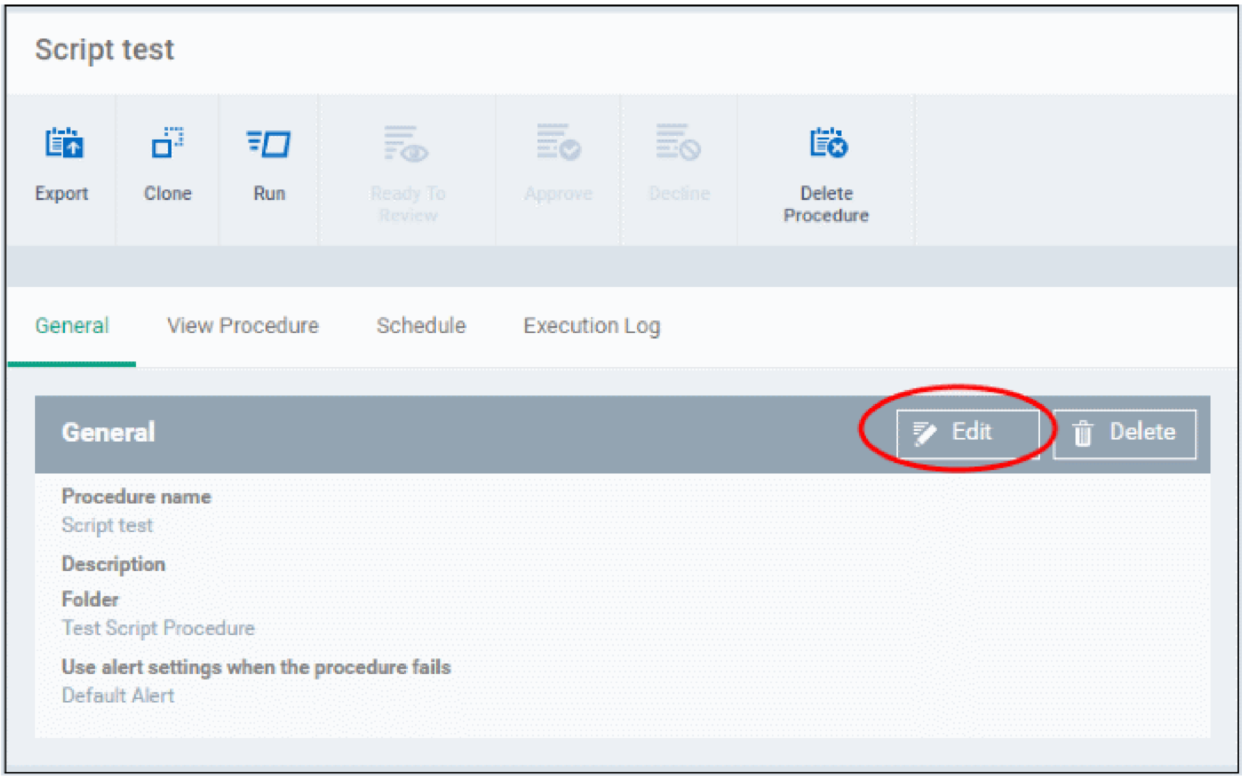
6.6.9. Edit / Delete Procedures

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

- Click 'Configuration Templates' > 'Procedures'
- Click on the script procedure that you want to modify and click 'Edit' at the top right



Procedure name
Script test
Description
Folder
Test Script Procedure
Use alert settings when the procedure fails
Default Alert

General

- Modify the procedure name, description and / or alert settings

View Procedure

- Click 'Edit'

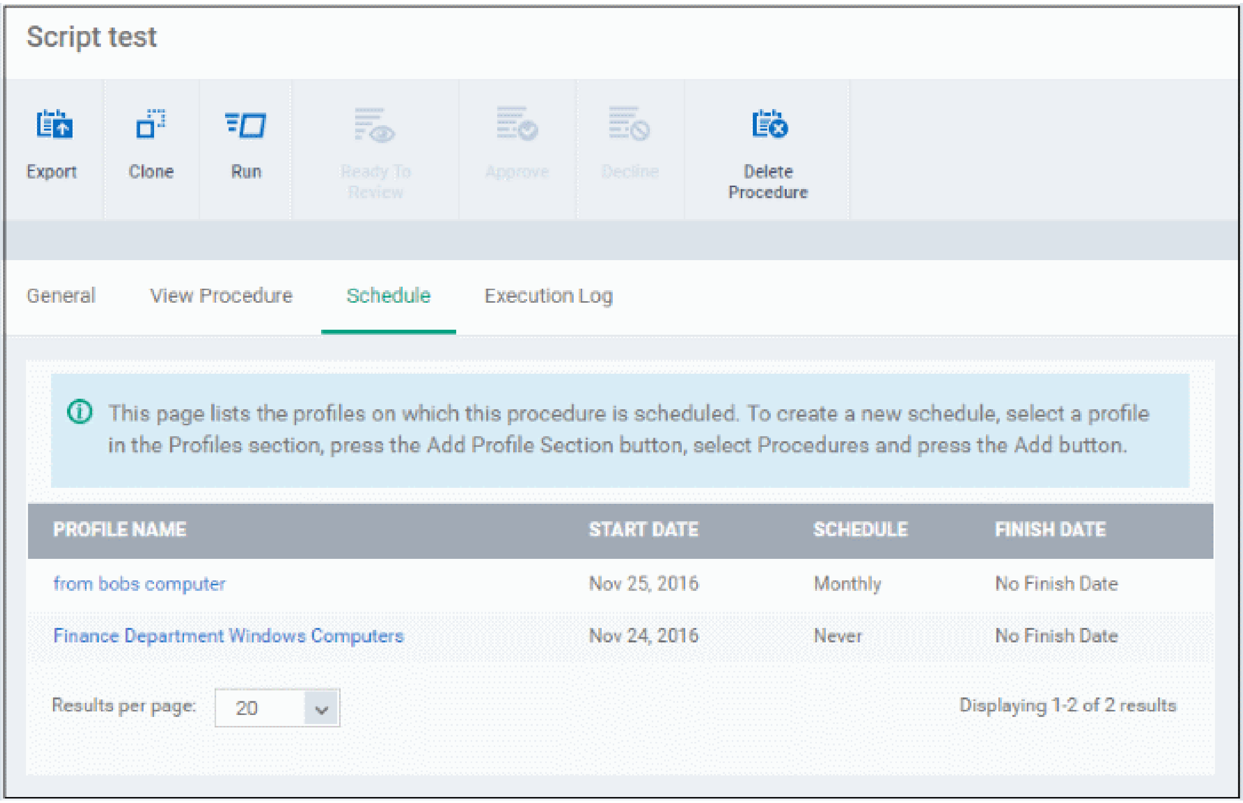
- Modify the script and / or add another existing procedure

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.



This page lists the profiles on which this procedure is scheduled. To create a new schedule, select a profile in the Profiles section, press the Add Profile Section button, select Procedures and press the Add button.

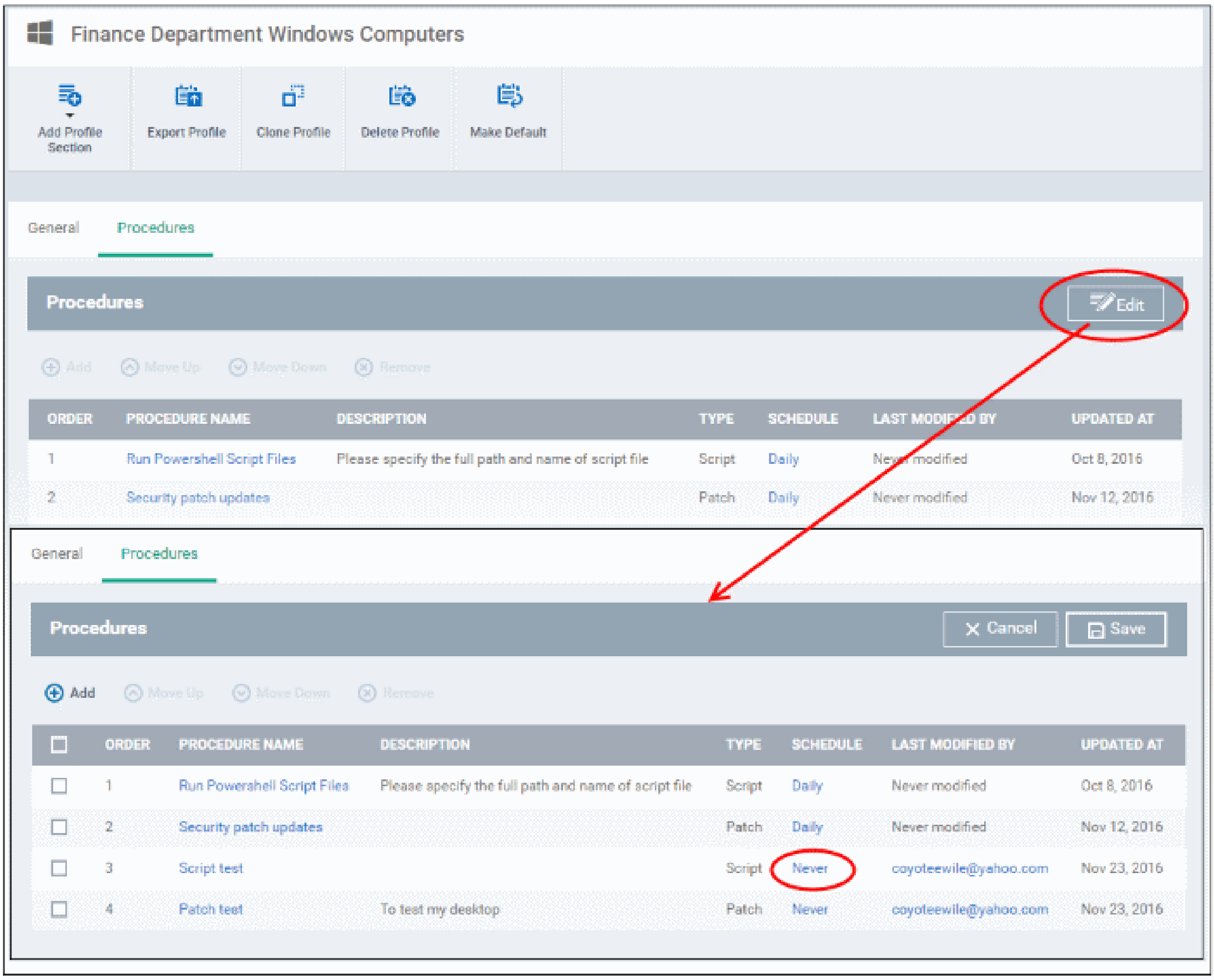
PROFILE NAME	START DATE	SCHEDULE	FINISH DATE
from bobs computer	Nov 25, 2016	Monthly	No Finish Date
Finance Department Windows Computers	Nov 24, 2016	Never	No Finish Date

Results per page: 20

Displaying 1-2 of 2 results

- 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.



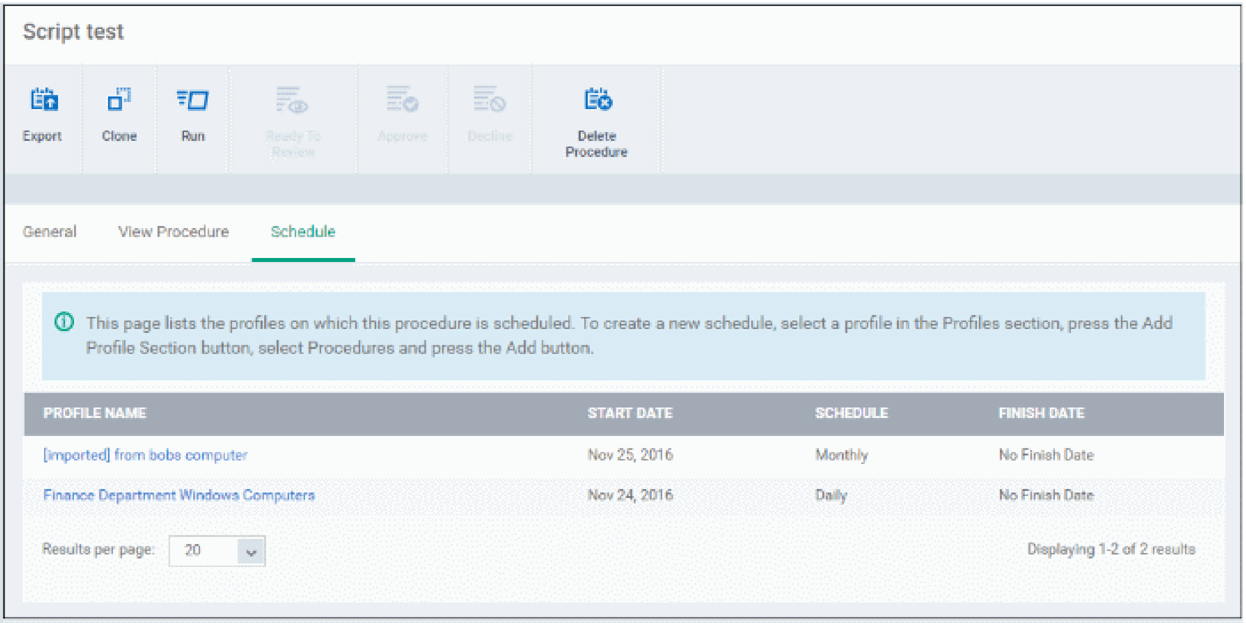
ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
1	Run Powershell Script Files	Please specify the full path and name of script file	Script	Daily	Never modified	Oct 8, 2016
2	Security patch updates		Patch	Daily	Never modified	Nov 12, 2016

□	ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
□	1	Run Powershell Script Files	Please specify the full path and name of script file	Script	Daily	Never modified	Oct 8, 2016
□	2	Security patch updates		Patch	Daily	Never modified	Nov 12, 2016
□	3	Script test		Script	Never	coyoteewile@yahoo.com	Nov 23, 2016
□	4	Patch test	To test my desktop	Patch	Never	coyoteewile@yahoo.com	Nov 23, 2016

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.



Script test

This page lists the profiles on which this procedure is scheduled. To create a new schedule, select a profile in the Profiles section, press the Add Profile Section button, select Procedures and press the Add button.

PROFILE NAME	START DATE	SCHEDULE	FINISH DATE
[imported] from bobs computer	Nov 25, 2016	Monthly	No Finish Date
Finance Department Windows Computers	Nov 24, 2016	Daily	No Finish Date

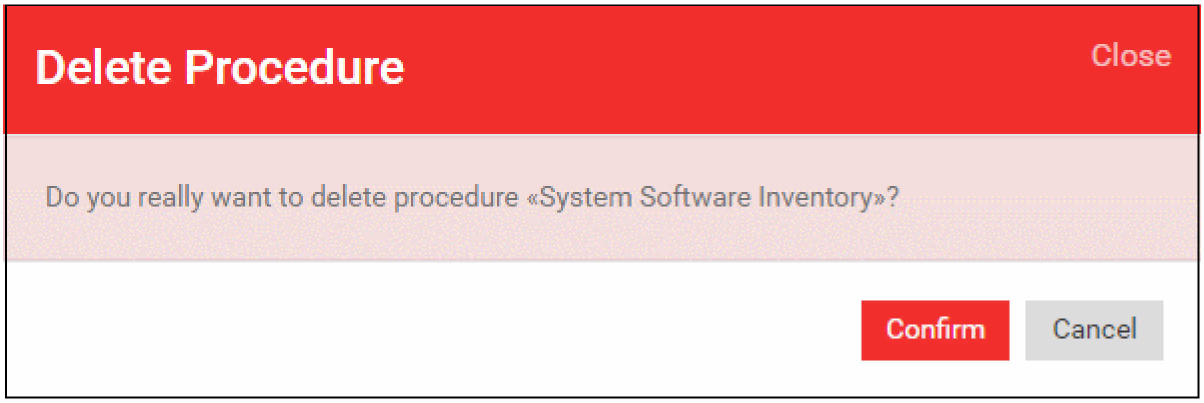
Results per page: 20

Displaying 1-2 of 2 results

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.



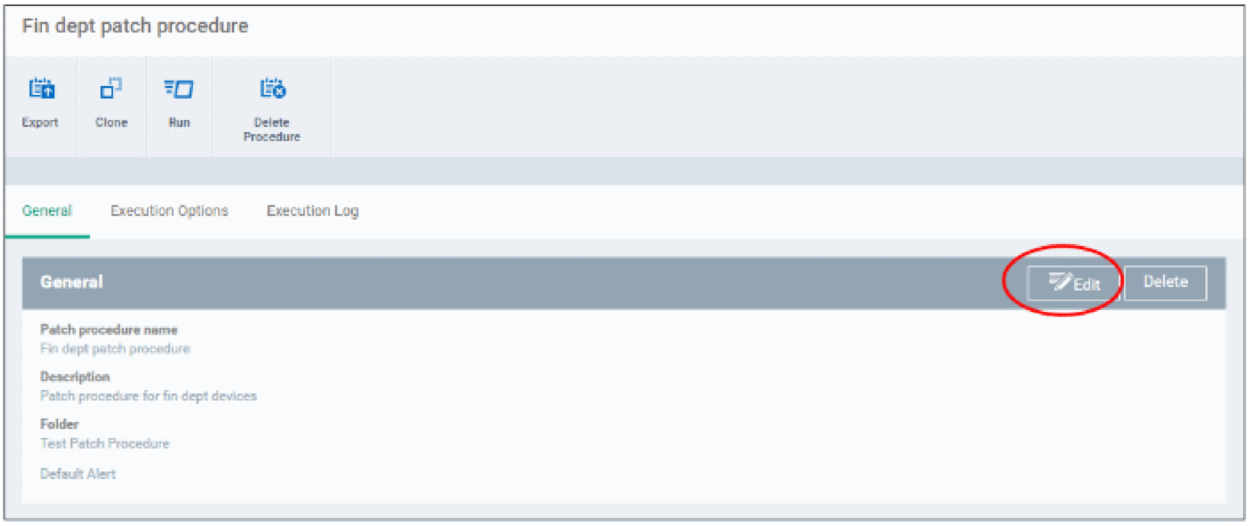
Delete Procedure

Do you really want to delete procedure «System Software Inventory»?

- 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

Patch procedure name
Fin dept patch procedure

Description
Patch procedure for fin dept devices

Folder
Test Patch Procedure

Default Alert

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

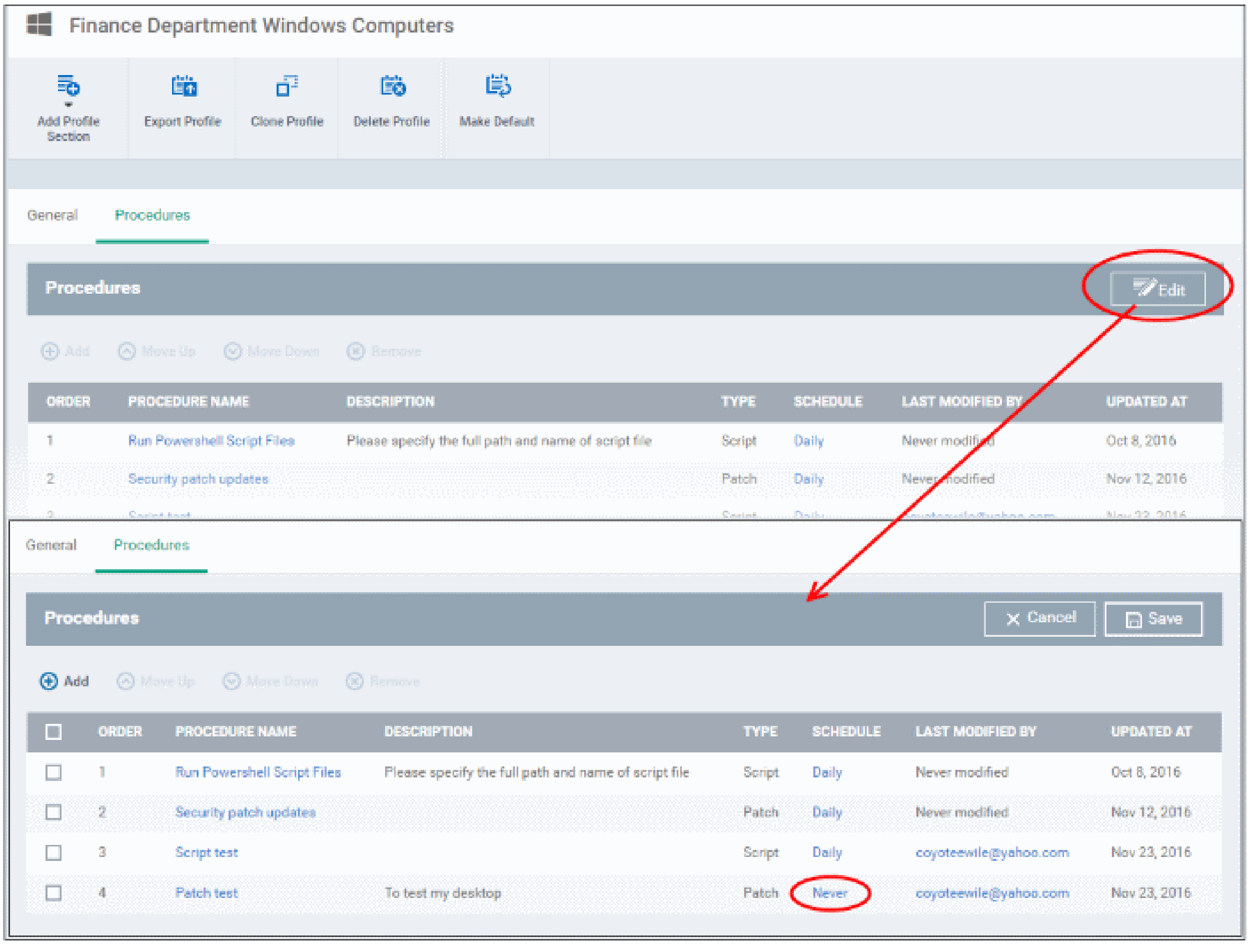
- Displays the results of the patch procedure that was executed, both manually and scheduled on Windows profiles.

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.



ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
1	Run Powershell Script Files	Please specify the full path and name of script file	Script	Daily	Never modified	Oct 8, 2016
2	Security patch updates		Patch	Daily	Never modified	Nov 12, 2016
3	Script test		Script	Daily	coyoteewile@yahoo.com	Nov 23, 2016

□	ORDER	PROCEDURE NAME	DESCRIPTION	TYPE	SCHEDULE	LAST MODIFIED BY	UPDATED AT
□	1	Run Powershell Script Files	Please specify the full path and name of script file	Script	Daily	Never modified	Oct 8, 2016
□	2	Security patch updates		Patch	Daily	Never modified	Nov 12, 2016
□	3	Script test		Script	Daily	coyoteewile@yahoo.com	Nov 23, 2016
□	4	Patch test	To test my desktop	Patch	Never	coyoteewile@yahoo.com	Nov 23, 2016

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 or patch procedure can be viewed in the '**Logs**' section of a device as well as from the 'Procedures' interface. Click the following links for more details:

- **Viewing script procedure results**
- **Viewing patch procedure results**

Viewing Script Procedure Results

Script procedure logs can be viewed from two interfaces - 'Device List' and 'Procedures'.

- Devices > Device List > *Open a Windows device* > Logs > Script Logs - Displays results for all script procedures run on a selected device.
- Configuration Templates > Procedures > *Open a script procedure* > Execution Log - Displays all devices on which the selected script procedure was run.

Script procedures results on a particular device

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

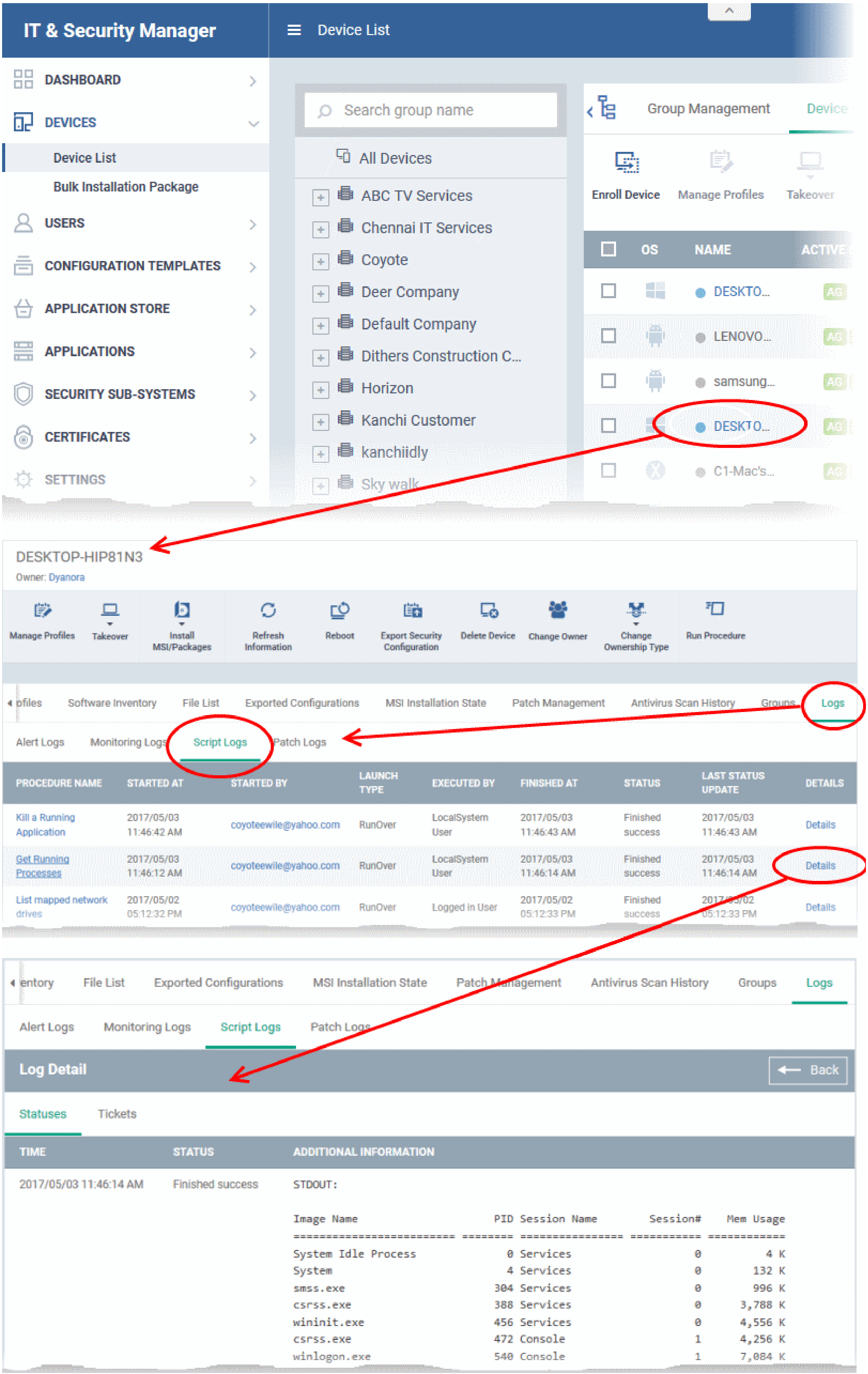
      Or
    - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Logs' tab in the device details interface
- Select the 'Script Logs' sub-tab

This will open a list of all script 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' in the row of the procedure name.

The 'Log Details' pane will display the specific results of the procedure.

For example, the 'Get Running Processes' results will show a list of all processes found running on the device, under the 'Statuses' tab:



□	OS	NAME	ACTIVE
□		DESKTO...	AG
□		LENOVO...	AG
□		samsung...	AG
□		DESKTO...	AG
□		C1-Mac's...	AG

DESKTOP-HIP81N3

Owner: Dyanora

PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	EXECUTED BY	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
Kill a Running Application	2017/05/03 11:46:42 AM	coyoteewile@yahoo.com	RunOver	LocalSystem User	2017/05/03 11:46:43 AM	Finished success	2017/05/03 11:46:43 AM	Details
Get Running Processes	2017/05/03 11:46:12 AM	coyoteewile@yahoo.com	RunOver	LocalSystem User	2017/05/03 11:46:14 AM	Finished success	2017/05/03 11:46:14 AM	Details
List mapped network drives	2017/05/02 05:12:32 PM	coyoteewile@yahoo.com	RunOver	Logged in User	2017/05/02 05:12:33 PM	Finished success	2017/05/02 05:12:33 PM	Details

Log Detail

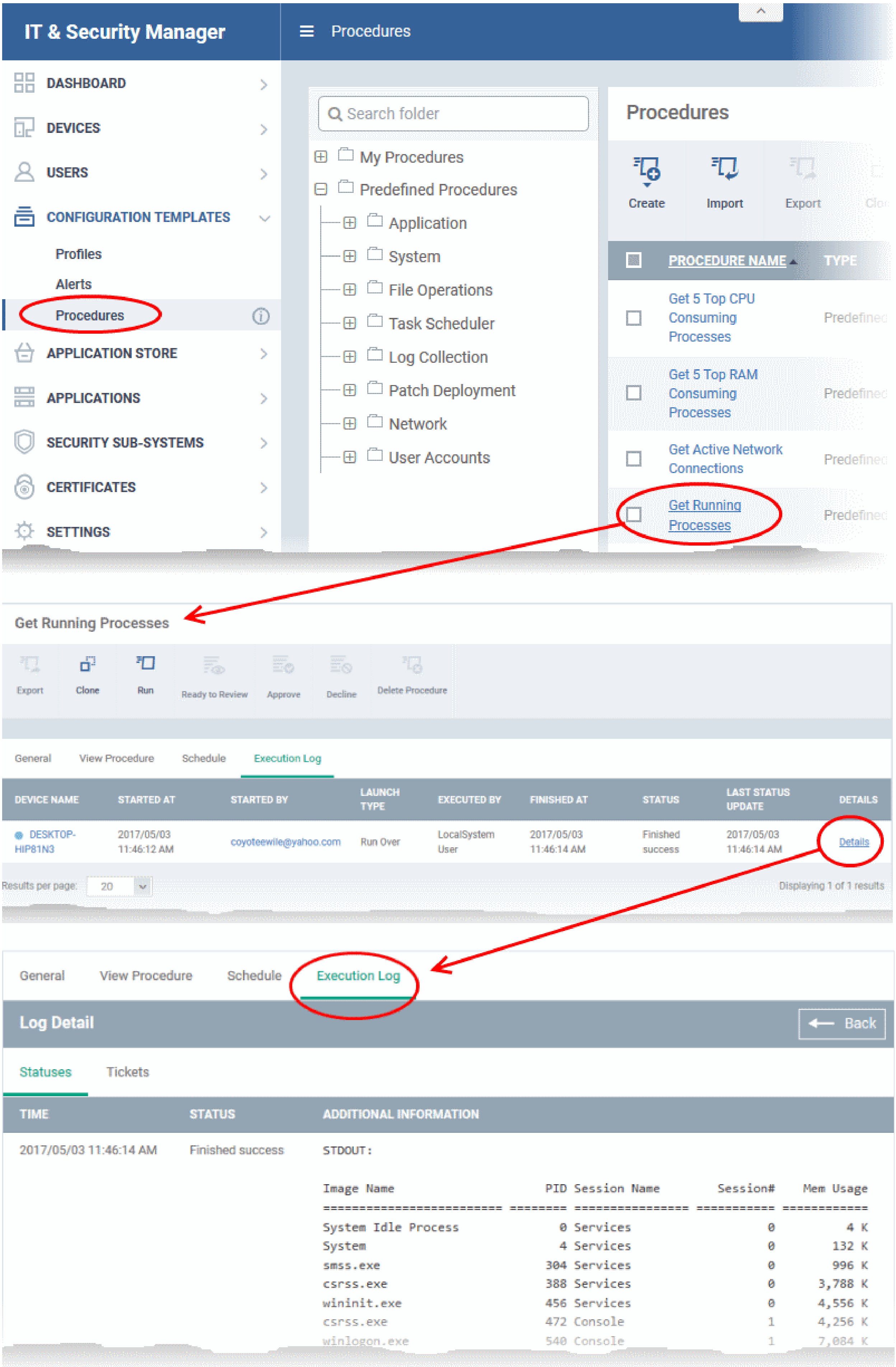
TIME	STATUS	ADDITIONAL INFORMATION
2017/05/03 11:46:14 AM	Finished success	STDOUT:

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        132 K
smss.exe                       304 Services                   0        996 K
csrss.exe                      388 Services                   0      3,788 K
wininit.exe                    456 Services                   0      4,556 K
csrss.exe                      472 Console                    1      4,256 K
winlogon.exe                   540 Console                    1      7,084 K
```

- The 'Tickets' tab 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 selected 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' in the 'Procedure Details' screen.
- 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' in the row of the device.
- The 'Log Details' pane will display the specific results of the procedure. For example, the 'Get Running Processes' results will show a list of all processes that were found running on the device by the script, under the 'Statuses' tab.



□	PROCEDURE NAME ▲	TYPE
□	Get 5 Top CPU Consuming Processes	Predefined
□	Get 5 Top RAM Consuming Processes	Predefined
□	Get Active Network Connections	Predefined
□	Get Running Processes	Predefined

Get Running Processes

DEVICE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	EXECUTED BY	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
DESKTOP-HIP81N3	2017/05/03 11:46:12 AM	coyoteewile@yahoo.com	Run Over	LocalSystem User	2017/05/03 11:46:14 AM	Finished success	2017/05/03 11:46:14 AM	Details

Results per page: 20 Displaying 1 of 1 results

TIME	STATUS	ADDITIONAL INFORMATION
2017/05/03 11:46:14 AM	Finished success	STDOUT:

```
STDOUT:

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        132 K
smss.exe                       304 Services                   0        996 K
csrss.exe                      388 Services                   0      3,788 K
wininit.exe                    456 Services                   0      4,556 K
csrss.exe                      472 Console                    1      4,256 K
winlogon.exe                   540 Console                    1      7,084 K
```

- 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

Patch procedure results can be viewed from two interfaces - 'Device List' and 'Procedures'.

- Devices > Device List > *Open a Windows device* > Logs > Patch Logs - Displays results for all patch procedures run on a selected device.
- Configuration Templates > Procedures > *Open a patch procedure* > Execution Log - Displays all devices on which the selected patch procedure was run.

Patch procedures results on a particular device

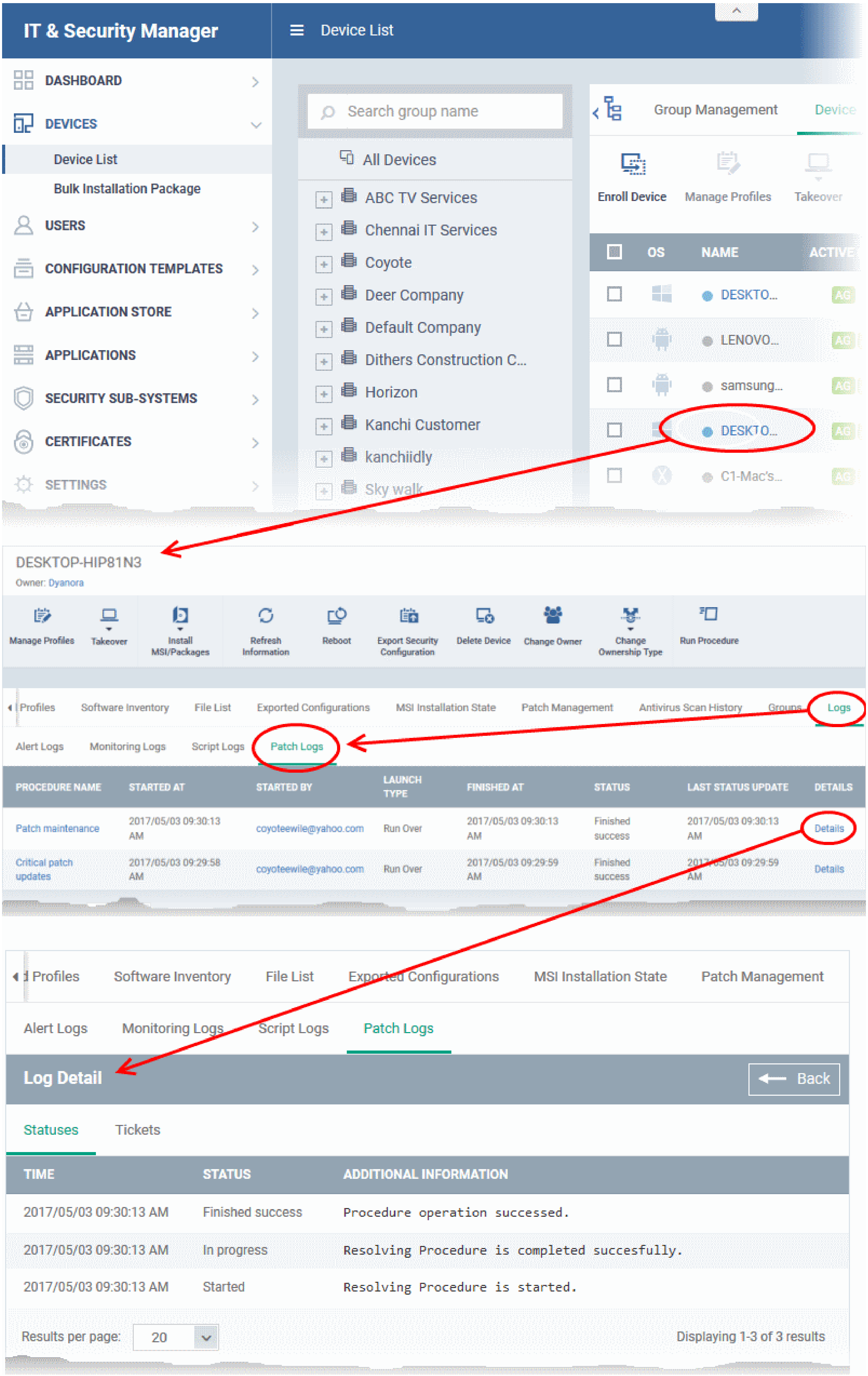
- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane
  - Select a company or a group to view the list of devices in that group

    Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Click on any Windows device then select the 'Logs' tab in the device details interface
- Select the 'Patch Logs' sub-tab

This will open a list of all patch 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' in the row of the procedure name.

  The 'Log Details' pane will display the specific results of the procedure under the 'Statuses' tab:



PROCEDURE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
Patch maintenance	2017/05/03 09:30:13 AM	coyoteewile@yahoo.com	Run Over	2017/05/03 09:30:13 AM	Finished success	2017/05/03 09:30:13 AM	Details
Critical patch updates	2017/05/03 09:29:58 AM	coyoteewile@yahoo.com	Run Over	2017/05/03 09:29:59 AM	Finished success	2017/05/03 09:29:59 AM	Details

TIME	STATUS	ADDITIONAL INFORMATION
2017/05/03 09:30:13 AM	Finished success	Procedure operation successed.
2017/05/03 09:30:13 AM	In progress	Resolving Procedure is completed succesfully.
2017/05/03 09:30:13 AM	Started	Resolving Procedure is started.

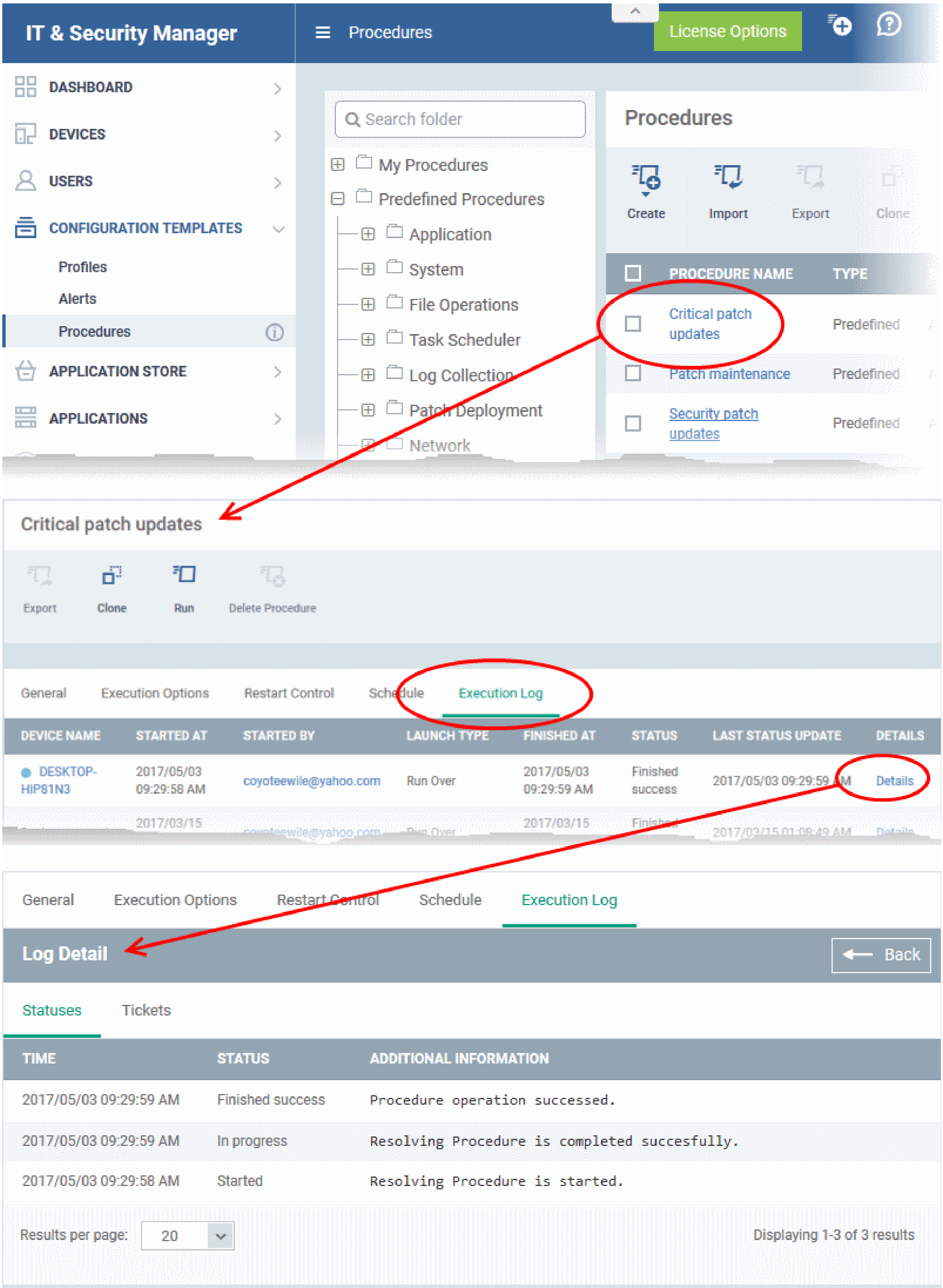
Results per page: 20

Displaying 1-3 of 3 results

- The 'Tickets' tab displays a list of 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 selected patch procedure run on all devices

- Click 'Configuration Templates' > 'Procedures'.
- Click the name of the patch procedure under 'My Procedures' or 'Predefined Procedures' for which you want to view results, then click 'Execution Log' in the Procedure Details screen.
- 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' in the row of the device.
- The 'Log Details' pane will display the specific results of the procedure. For example, the 'Get Running Processes' results will show a list of all processes that were found running on the device by the script, under the 'Statuses' tab.



PROCEDURE NAME	TYPE
Critical patch updates	Predefined
Patch maintenance	Predefined
Security patch updates	Predefined

DEVICE NAME	STARTED AT	STARTED BY	LAUNCH TYPE	FINISHED AT	STATUS	LAST STATUS UPDATE	DETAILS
DESKTOP-HIP81N3	2017/05/03 09:29:58 AM	coyoteewile@yahoo.com	Run Over	2017/05/03 09:29:59 AM	Finished success	2017/05/03 09:29:59 AM	Details
	2017/03/15	coyoteewile@yahoo.com	Run Over	2017/03/15	Finished	2017/03/15 01:08:49 AM	Details

TIME	STATUS	ADDITIONAL INFORMATION
2017/05/03 09:29:59 AM	Finished success	Procedure operation successed.
2017/05/03 09:29:59 AM	In progress	Resolving Procedure is completed succesfully.
2017/05/03 09:29:58 AM	Started	Resolving Procedure is started.

Results per page: 20

Displaying 1-3 of 3 results

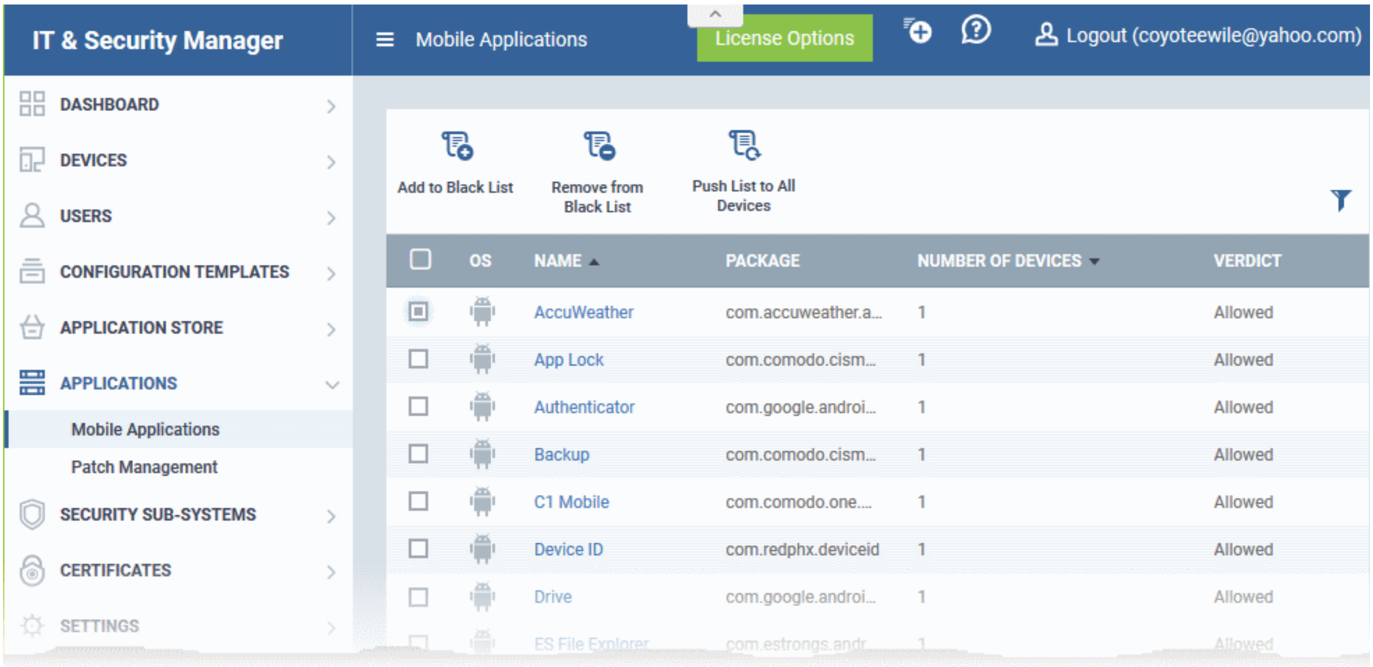
- The 'Tickets' tab displays a list of tickets which were created as a result of a failed procedure. Clicking the ticket link will open the ticket in service desk.

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.



□	OS	NAME ▲	PACKAGE	NUMBER OF DEVICES ▼	VERDICT
▣		AccuWeather	com.accuweather.a...	1	Allowed
□		App Lock	com.comodo.cism...	1	Allowed
□		Authenticator	com.google.androi...	1	Allowed
□		Backup	com.comodo.cism...	1	Allowed
□		C1 Mobile	com.comodo.one....	1	Allowed
□		Device ID	com.redphx.deviceid	1	Allowed
□		Drive	com.google.androi...	1	Allowed
□		ES File Explorer	com.estrongs.andr...	1	Allowed

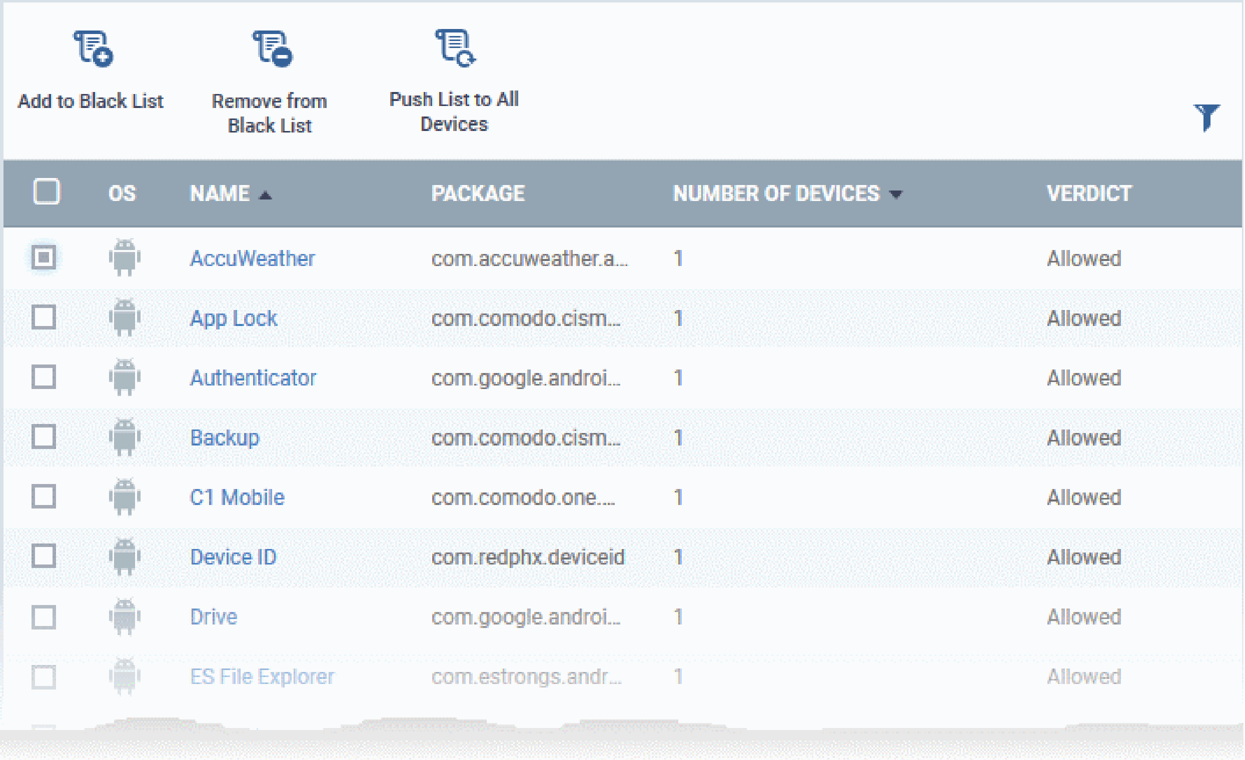
The following sections explain in more detail on:

- Viewing Applications Installed on Android and iOS Devices
  - Blacklisting and Whitelisting Applications
- Installing OS Patches On Windows Endpoints

7.1. View 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 then choose 'Mobile Applications' from the options.

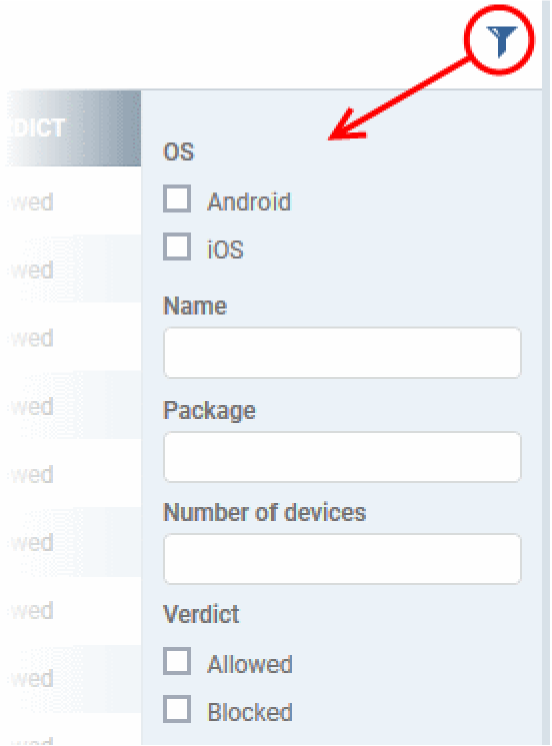


☐	OS	NAME ▲	PACKAGE	NUMBER OF DEVICES ▼	VERDICT
☒		AccuWeather	com.accuweather.a...	1	Allowed
☐		App Lock	com.comodo.cism...	1	Allowed
☐		Authenticator	com.google.androi...	1	Allowed
☐		Backup	com.comodo.cism...	1	Allowed
☐		C1 Mobile	com.comodo.one....	1	Allowed
☐		Device ID	com.redphx.deviceid	1	Allowed
☐		Drive	com.google.androi...	1	Allowed
☐		ES File Explorer	com.estrongs.andr...	1	Allowed

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.

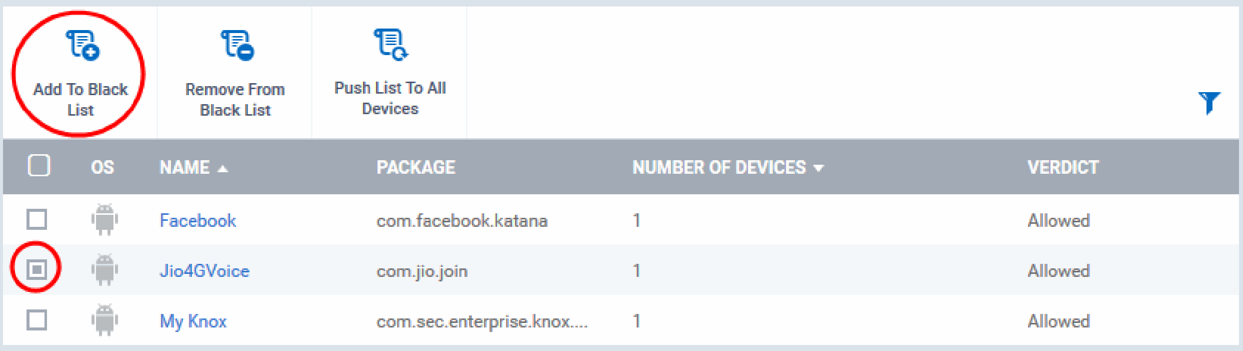
7.1.1. Blacklist and Whitelist Applications

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.

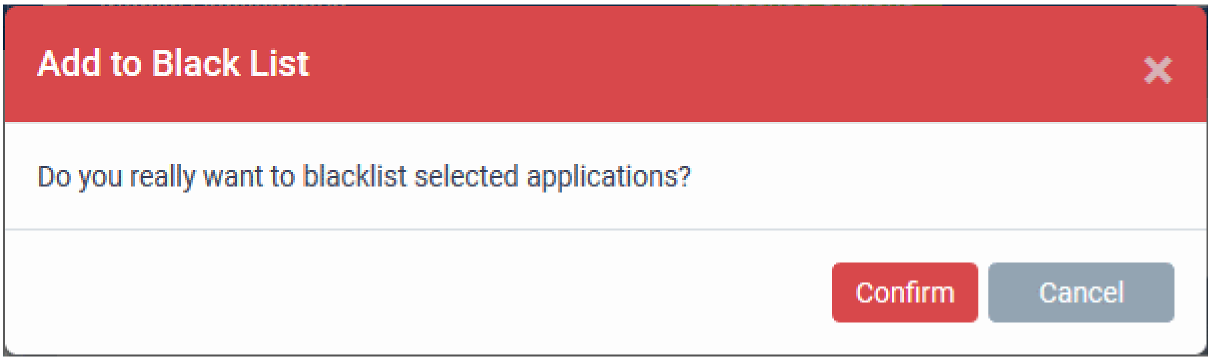


☐	OS	NAME ▲	PACKAGE	NUMBER OF DEVICES ▾	VERDICT
☐		Facebook	com.facebook.katana	1	Allowed
☒		Jio4GVoice	com.jio.join	1	Allowed
☐		My Knox	com.sec.enterprise.knox....	1	Allowed

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.



Do you really want to blacklist selected applications?

- Click 'Confirm'.

The selected apps will be added to the 'Black List' and their status will change to 'Blocked'

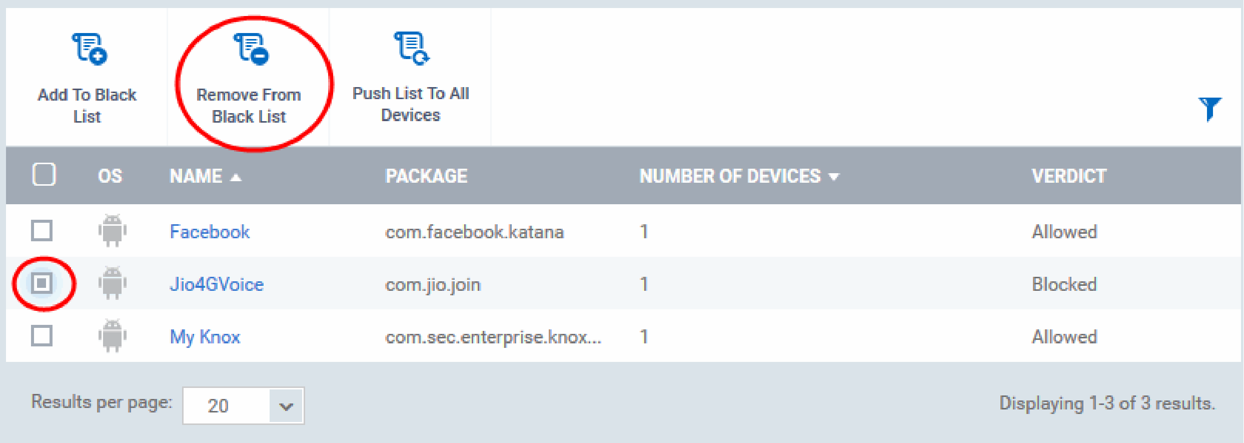
- To block the apps immediately in the devices on which they are currently installed, click 'Push List to All Devices' from the top.

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.



☐	OS	NAME ▲	PACKAGE	NUMBER OF DEVICES ▼	VERDICT
☐		Facebook	com.facebook.katana	1	Allowed
☑		Jio4GVoice	com.jio.join	1	Blocked
☐		My Knox	com.sec.enterprise.knox...	1	Allowed

Results per page: 20

Displaying 1-3 of 3 results.

- 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'.

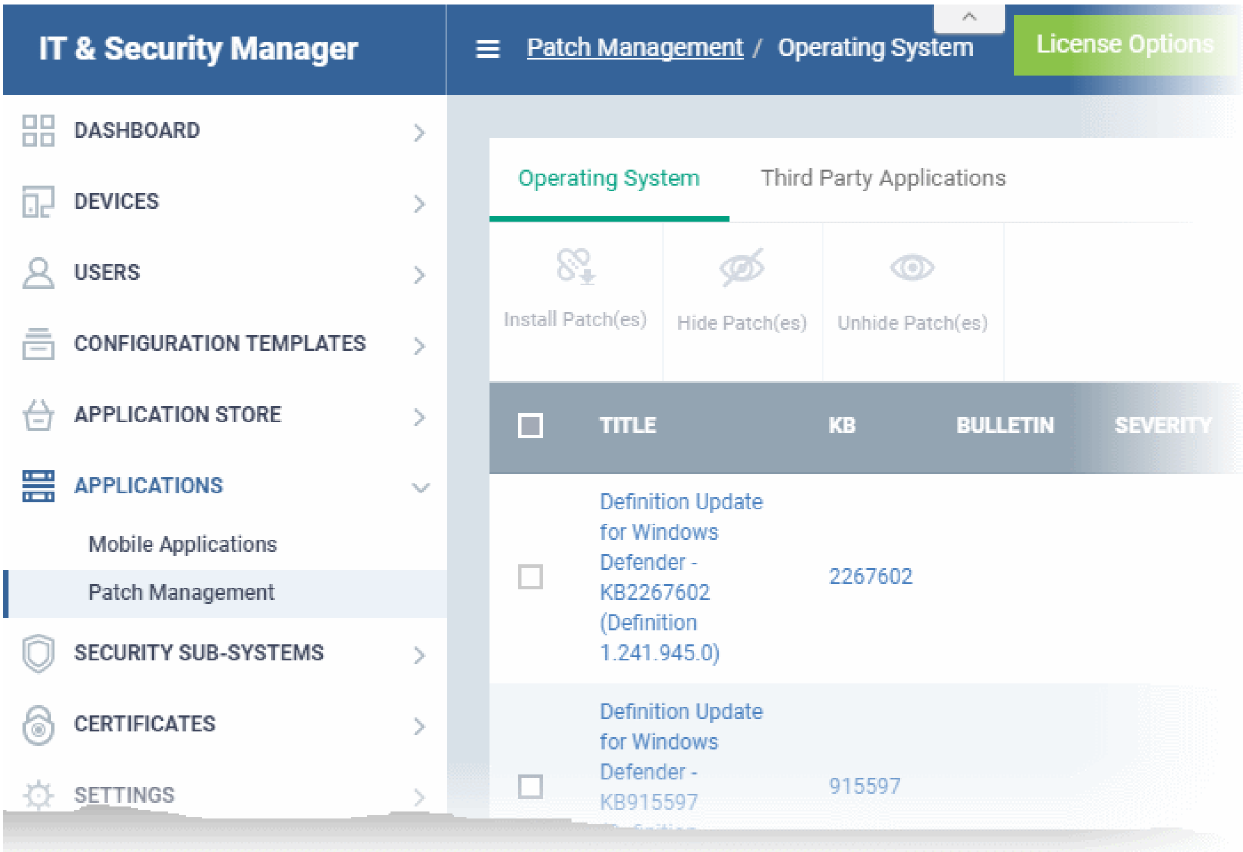
7.2. Patch Management

The 'Patch Management' area allows you to deploy OS updates and patch 3rd party applications on managed Windows devices.

Tip: As an alternative, you can apply patches to individual devices from the 'Device Management' interface. See '**Viewing and Installing Windows and 3rd Party Application Patches**' to find out more.

To open the 'Patch Management' interface

- Click 'Applications' > 'Patch Management':



□	TITLE	KB	BULLETIN	SEVERITY
□	Definition Update for Windows Defender - KB2267602 (Definition 1.241.945.0)	2267602		
□	Definition Update for Windows Defender - KB915597	915597		

The interface contains two tabs:

- **Operating System** - All OS patches available for deployment through ITSM. Each patch has additional details such as classification, the Windows component to which the patch applies, severity, release date, installation status and links to knowledgebase articles. The interface allows you to install selected patches on all managed devices. See **Install OS Patches on Windows Endpoints** for more details.
- **Third Party Applications** - All updates available for 3rd party applications installed on managed Windows endpoints. You can update selected applications on all required endpoints. See **Install 3rd Party Application Patches on Windows Endpoints** for more details. See '**ITSM Supported 3rd Party Applications**' to view a list of supported applications.

7.2.1. Install OS Patches on Windows Endpoints

The 'Operating System' tab of the 'Patch Management' interface allows admins to deploy patches to all managed Windows devices or to selected endpoints.

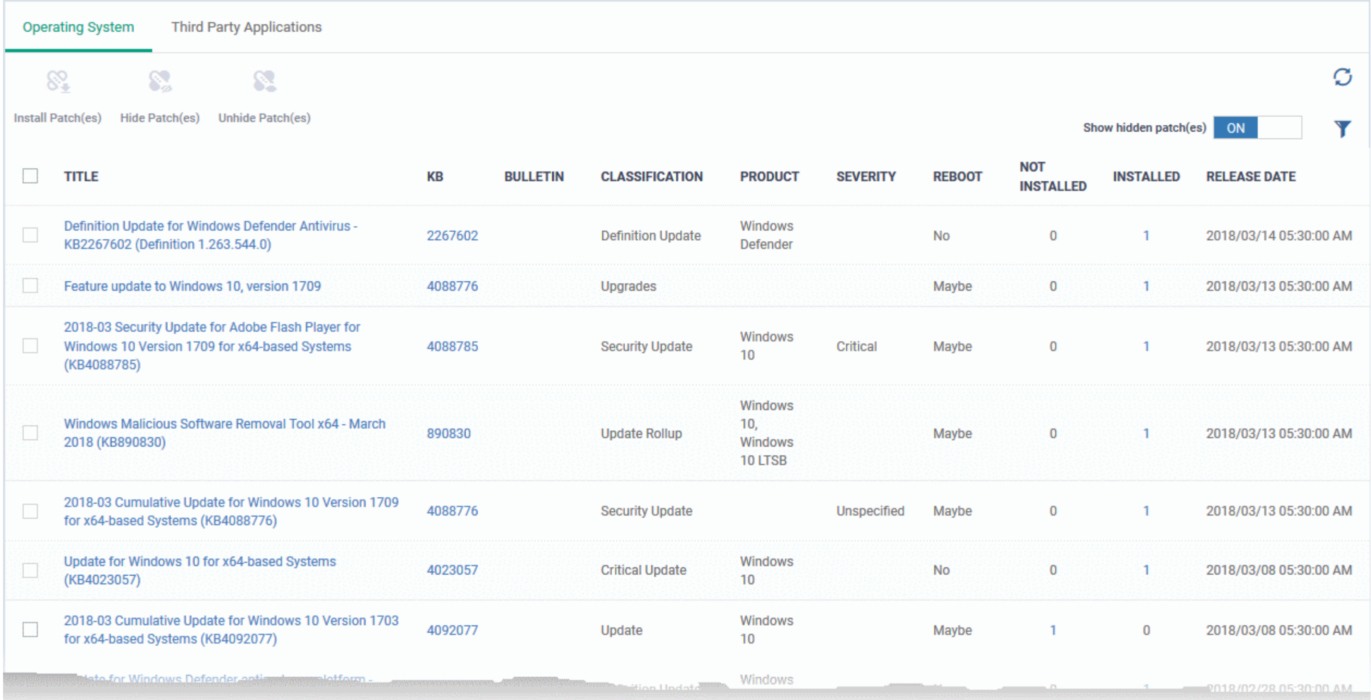
- ITSM checks the Microsoft update servers for available Windows patches and updates lists them in the interface.
- The interface also displays details about each patch, including its classification, the Windows component to which it applies, release date, severity, previous versions, Microsoft bulletins and number of endpoints which require the patch.
- The interface lets you view granular details about any patch and shows a list of devices to which it is relevant. You can also deploy the patch devices which require it.
- You can choose to hide patches if you do not want to deploy them. Hidden patches will not be available for deployment in the '**Device Management**' screen and will not be executed if added to a **patch procedure**.

To open the Operating System interface

- Click 'Applications' on the left and choose 'Patch Management' from the options

- Select the 'Operating System' tab

The interface will list all available OS patches and update packages for managed Windows endpoints:



Show hidden patch(es) ON

	TITLE	KB	BULLETIN	CLASSIFICATION	PRODUCT	SEVERITY	REBOOT	NOT INSTALLED	INSTALLED	RELEASE DATE
□	Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.544.0)	2267602		Definition Update	Windows Defender		No	0	1	2018/03/14 05:30:00 AM
□	Feature update to Windows 10, version 1709	4088776		Upgrades			Maybe	0	1	2018/03/13 05:30:00 AM
□	2018-03 Security Update for Adobe Flash Player for Windows 10 Version 1709 for x64-based Systems (KB4088785)	4088785		Security Update	Windows 10	Critical	Maybe	0	1	2018/03/13 05:30:00 AM
□	Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)	890830		Update Rollup	Windows 10, Windows 10 LTSB		Maybe	0	1	2018/03/13 05:30:00 AM
□	2018-03 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB4088776)	4088776		Security Update		Unspecified	Maybe	0	1	2018/03/13 05:30:00 AM
□	Update for Windows 10 for x64-based Systems (KB4023057)	4023057		Critical Update	Windows 10		No	0	1	2018/03/08 05:30:00 AM
□	2018-03 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4092077)	4092077		Update	Windows 10		Maybe	1	0	2018/03/08 05:30:00 AM

Patch Management Table - Column Descriptions	
Column Heading	**Description**
Title	The descriptive name of the patch. • Clicking the name will open the 'Patch Details' interface that displays the details of the patch. See **Viewing Details of a Patch** for more details.
KB	The knowledgebase article number that describes the patch. • Clicking the number will take you to the Microsoft Knowledgebase article web page.
Bulletin	The Microsoft Bulletin number that contains details about the patch release. • Clicking the number will take you to the respective 'Microsoft Security Bulletin' page.
Classification	The category of the patch. The possible values are: • Update - Fixes a specific non-critical problem but not a security-related bug. • Definition update - Contains updates to a product's definition database. For example, an update to the virus signature database for Windows Defender. • Critical Update - Fixes a specific critical problem but not a security-related bug. • Security update - Fixes a version specific, security related vulnerability • Update rollup - Contains a collection of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. These updates generally target a specific Windows component. • Driver - Adds software for controlling peripherals or add-on devices that could

	be connected to the endpoint • Feature pack - Adds new functionality distributed after an OS release. • Service pack - Contains a collection of hotfixes, security updates, critical updates, updates, and additional fixes. • Tool - Installs a utility or feature for a specific task or a set of tasks. • Upgrades - Upgrades the Windows OS version on the endpoint to the latest build.
Product	The Windows component to which the patch applies.
Severity	The level of severity for the patch. The severity levels are: • Critical • Important • Low • Moderate • Unspecified
Reboot	Whether or not the endpoint requires a restart to complete the patch installation.
Not Installed	The number of managed endpoints on which the patch is yet to be installed. • Click the number to view the patch details screen at the 'Device List' tab. See the explanation of **Viewing Details of a Patch** for more details on the 'Patch Details' screen. • The 'Device List' tab shows devices to which the patch is relevant. You can deploy the patch to those devices which need it. • See **Installing a patch on selected endpoints** for more details.
Installed	The number of managed endpoints on which the patch has been already installed. • Click the number to view the patch details screen at the 'Device List' tab. See **Viewing Details of a Patch** for more details on the 'Patch Details' screen. • The 'Device List' tab shows devices along with the installation status of the selected patch. • You can select devices on which the patch is required and start the installation process. See the explanation of **Installing a patch on selected endpoints** for more details.
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 Management**' 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.

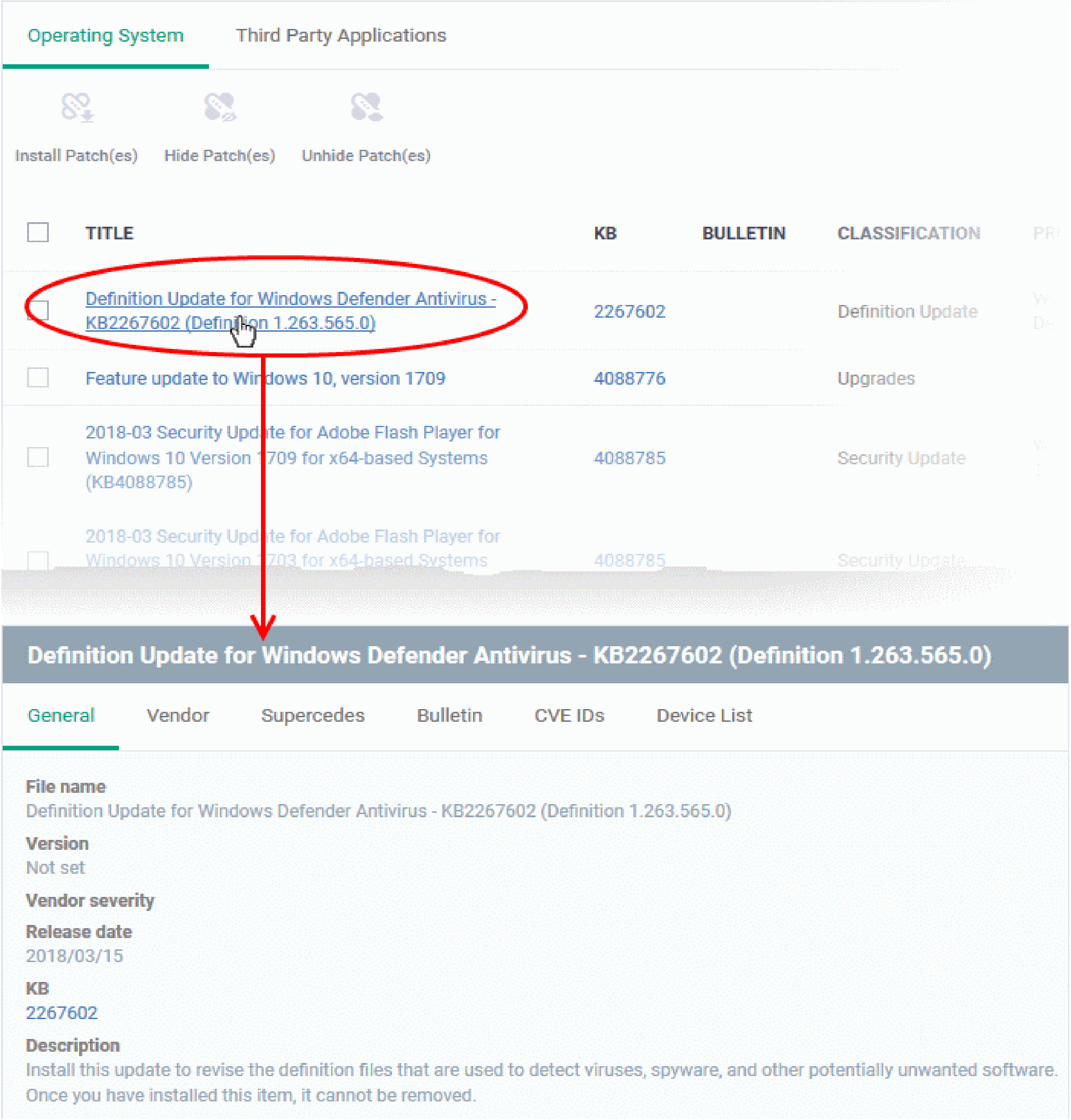
- Click any column header to sort the items in ascending/descending order of the entries in that column.

The 'Operating System Patch Management' interface allows you to:

- View Details of a Patch
- Hide Patches
- Restore Hidden Patches
- Install selected patches on all managed endpoints at once
- Install a patch on selected endpoints
- Search specific patches in the Patch Management interface

View Details of a Patch

- Click the name of any patch to open its patch details screen.



	TITLE	KB	BULLETIN	CLASSIFICATION	PR
□	Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.565.0)	2267602		Definition Update	W D
□	Feature update to Windows 10, version 1709	4088776		Upgrades	
□	2018-03 Security Update for Adobe Flash Player for Windows 10 Version 1709 for x64-based Systems (KB4088785)	4088785		Security Update	
□	2018-03 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems	4088785		Security Update	

Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.565.0)

File name
Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.263.565.0)

Version
Not set

Vendor severity

Release date
2018/03/15

KB
2267602

Description
Install this update to revise the definition files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

The complete details of the patch are displayed under five tabs:

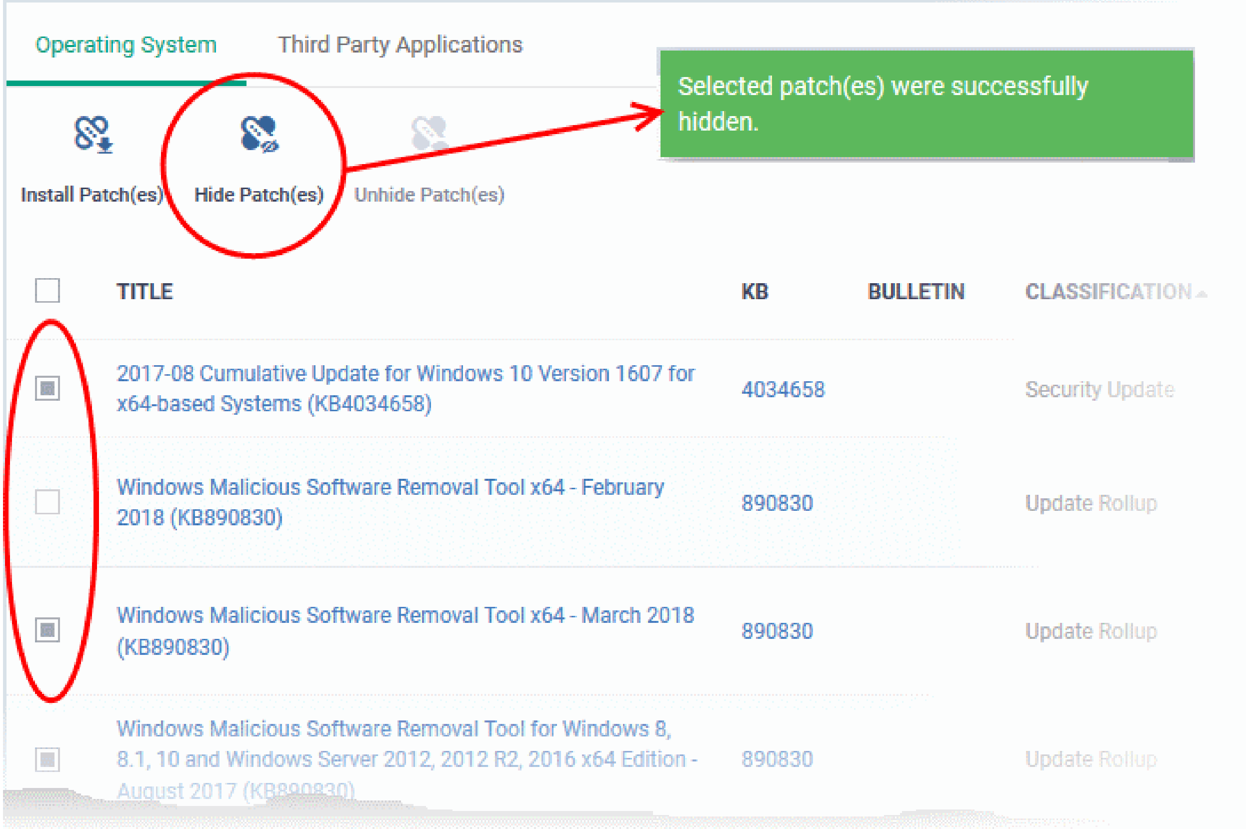
- **General** - Displays the name and general description, version number, severity as set by the vendor, release date and a link to the knowledgebase (KB) article for the patch release.
- **Vendor** - Indicates the publisher of the patch, with a link to the support page for the patch from the vendor
- **Security Patch Info** - Displays the information on previous patches that are superseded by the patch
- **Bulletin** - Contains the Bulletin ID and a short summary of the bulletin published by the vendor for the patch.
- **CVE IDs** - Displays the Common Vulnerabilities and Exposure (CVE) Identity numbers set for the patch by the vendor.
- **Device List** - The list of managed Windows endpoints with the installation status of the patch on them You can install the patch on selected the endpoints from the list. See the explanation of **Installing a patch on selected endpoints** for more details.

Hide Patches

- You can hide those patches that you do not want to be rolled out to the endpoints, from the list.
- These patches will also be not available for deployment from the '**Device Management**' screen and will not be executed as well if added to a **patch procedure**.
- You can view the hidden patches by using the 'Show hidden patch(es) toggle button and install these patches onto endpoints.

To hide unwanted patch(es)

- Select the patch(es) you want to hide and click 'Hide Patch'



Selected patch(es) were successfully hidden.

☐	TITLE	KB	BULLETIN	CLASSIFICATION
☑	2017-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4034658)	4034658		Security Update
☐	Windows Malicious Software Removal Tool x64 - February 2018 (KB890830)	890830		Update Rollup
☑	Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)	890830		Update Rollup
☑	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - August 2017 (KB890830)	890830		Update Rollup

To view the hidden patches again, you have to **unhide** them.

Restore Hidden Patches

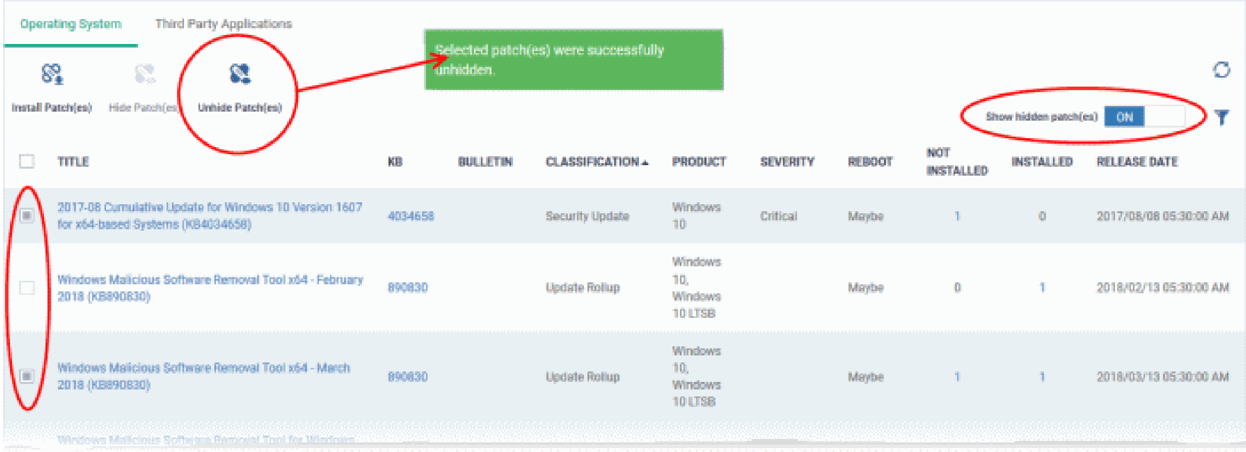
- Restored patches will also be available for installation in the **Device Management** interface and can be added to a **patch procedure**.

To view hidden patches and restore them

- Slide the 'Show hidden patch(es)' button to 'On'

The hidden patches will be shown with dark gray background stripe.

- Select the hidden patch(es) from the list and click 'Unhide Patch'



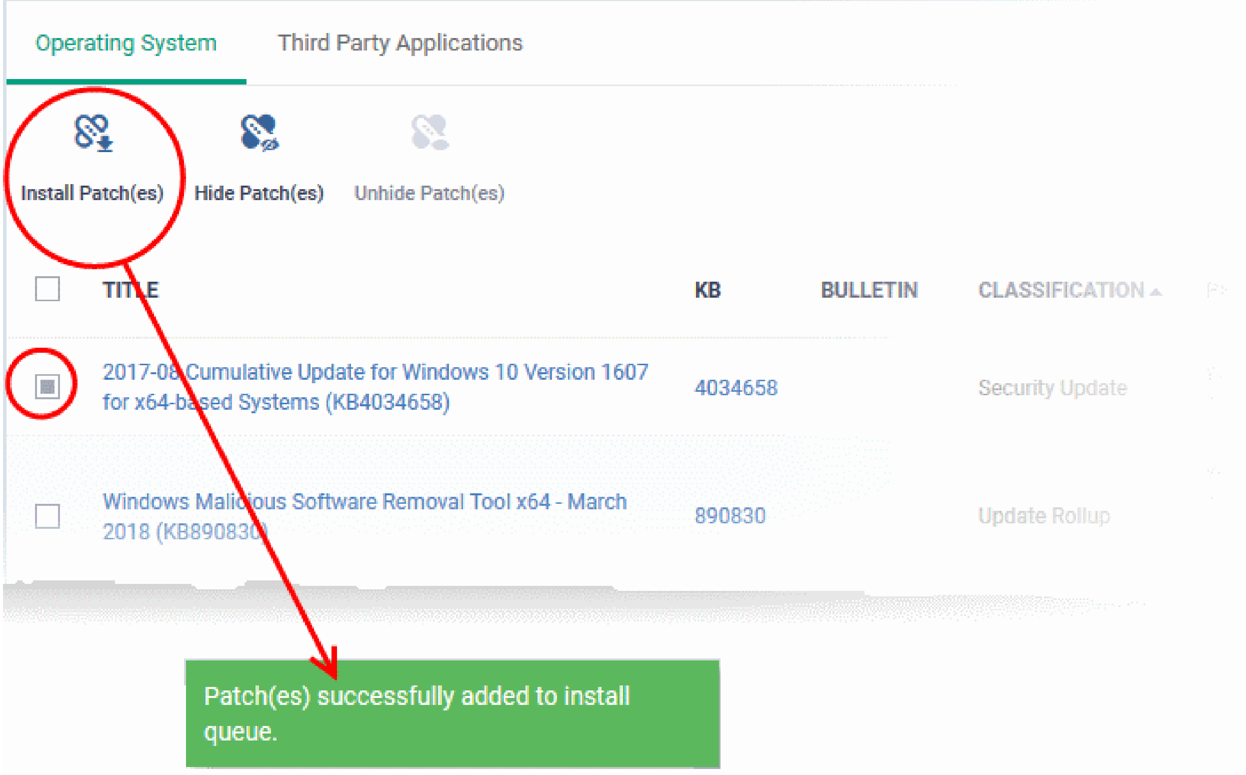
Selected patch(es) were successfully unhidden.

□	TITLE	KB	BULLETIN	CLASSIFICATION ▲	PRODUCT	SEVERITY	REBOOT	NOT INSTALLED	INSTALLED	RELEASE DATE
▣	2017-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4034658)	4034658		Security Update	Windows 10	Critical	Maybe	1	0	2017/08/08 05:30:00 AM
□	Windows Malicious Software Removal Tool x64 - February 2018 (KB890830)	890830		Update Rollup	Windows 10, Windows 10 LTSB		Maybe	0	1	2018/02/13 05:30:00 AM
▣	Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)	890830		Update Rollup	Windows 10, Windows 10 LTSB		Maybe	1	1	2018/03/13 05:30:00 AM
	Windows Malicious Software Removal Tool for Windows									

A confirmation message will be displayed. The patches will be re-added to the list.

Install patch(es) on all managed endpoints at-once

- Select the patch(es) to be installed from the list and click 'Install Selected Patch'



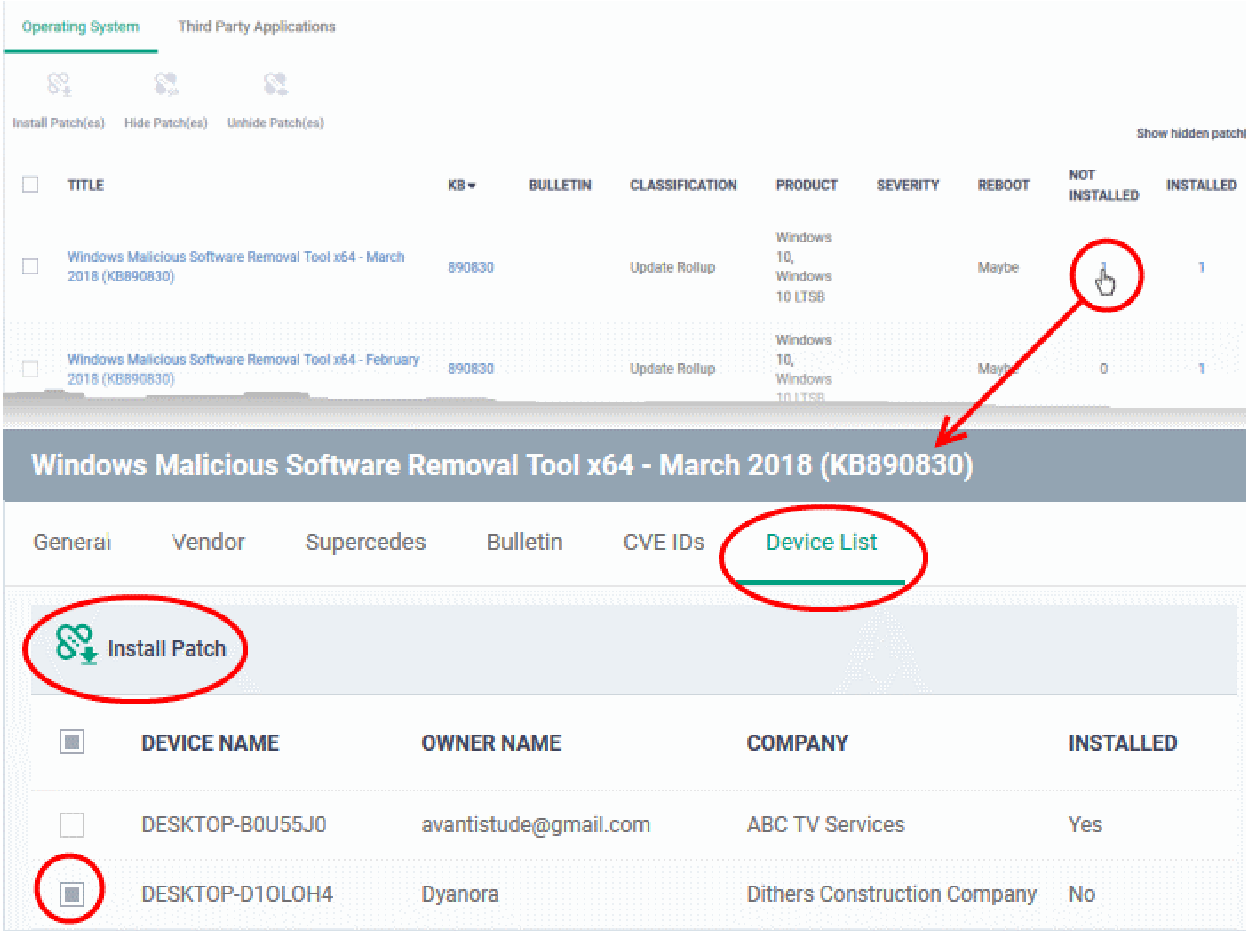
□	TITLE	KB	BULLETIN	CLASSIFICATION ▲
▣	2017-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4034658)	4034658		Security Update
□	Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)	890830		Update Rollup

Patch(es) successfully added to install queue.

A confirmation message will be displayed. The command will be sent and the selected patch(es) will be installed on the endpoint(s).

Install a patch on selected endpoints

- Click the number in the 'Not Installed' column of the patch you want to install.



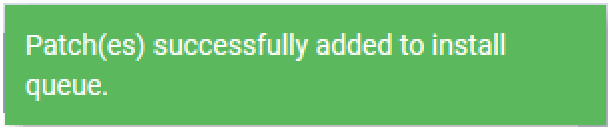
□	TITLE	KB	BULLETIN	CLASSIFICATION	PRODUCT	SEVERITY	REBOOT	NOT INSTALLED	INSTALLED
□	Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)	890830		Update Rollup	Windows 10, Windows 10 LTSB		Maybe	1	1
□	Windows Malicious Software Removal Tool x64 - February 2018 (KB890830)	890830		Update Rollup	Windows 10, Windows 10 LTSB		Maybe	0	1

Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)

☒	DEVICE NAME	OWNER NAME	COMPANY	INSTALLED
□	DESKTOP-B0U55J0	avantistude@gmail.com	ABC TV Services	Yes
☒	DESKTOP-D1OLOH4	Dyanora	Dithers Construction Company	No

The 'Patch Details' screen will open at the 'Device List' tab. This displays a list of all managed devices to which the patch is relevant. The 'Installed' column indicates whether the selected patch is installed on the device.

- Select the device(s) on which the patch is to be installed and click 'Install Patch'.
- A confirmation dialog will appear:



Patch(es) successfully added to install queue.

The command will be sent to the selected device(s) and a schedule will be created for installation of the selected patch on the devices.

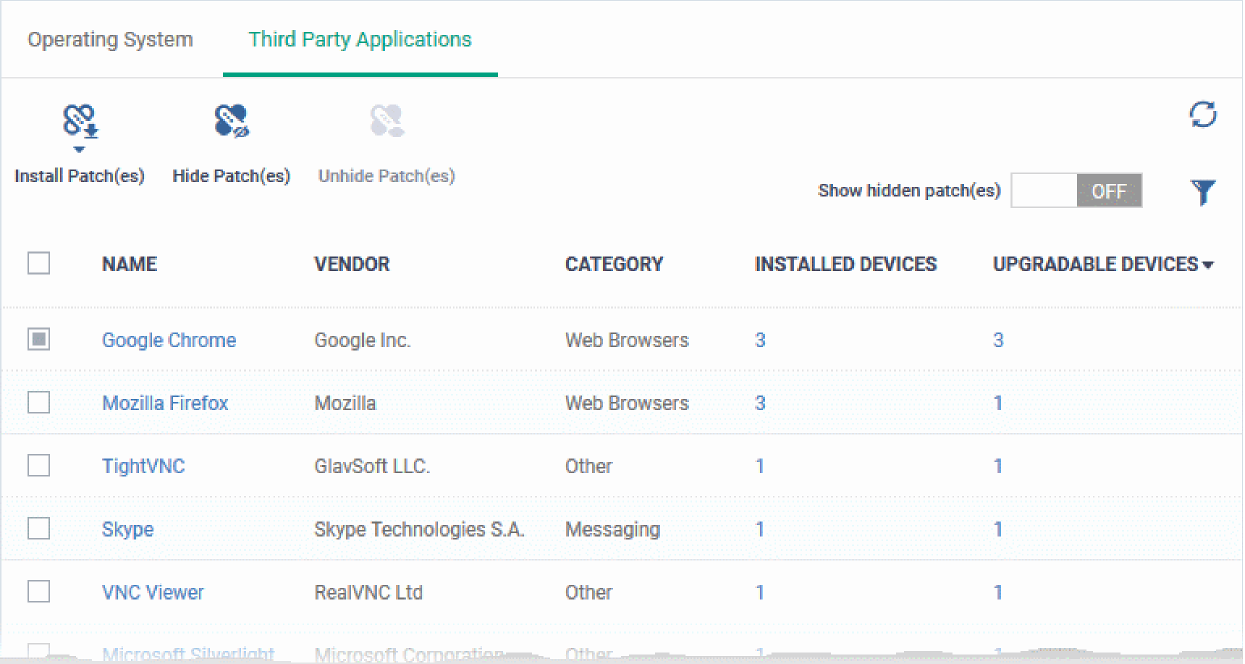
Search specific patches in the Patch Management interface

- Click the funnel icon on the right to filter patches by various criteria, including by name, by KB number, by bulletin number, by classification, by severity, and by whether a restart is required for the patches.
- Start typing the name of a patch in the search field to find a particular patch. Select the patch from the search suggestions and click 'Apply'
- To display all items again, clear any filters and search criteria 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.

7.2.2. Install 3rd Party Application Patches on Windows Endpoints

The 'Third Party Applications' area allows you to apply patches and updates to apps on Windows devices.

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab:



☐	NAME	VENDOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE DEVICES
☒	Google Chrome	Google Inc.	Web Browsers	3	3
☐	Mozilla Firefox	Mozilla	Web Browsers	3	1
☐	TightVNC	GlavSoft LLC.	Other	1	1
☐	Skype	Skype Technologies S.A.	Messaging	1	1
☐	VNC Viewer	RealVNC Ltd	Other	1	1
☐	Microsoft Silverlight	Microsoft Corporation	Other	1	1

- The interface lists any 3rd party applications on managed endpoints that require updates
- Each row shows the name of the software that needs to be updated. It also shows you how many devices have the software installed and how many of those require the update.
- You can apply updates to all devices or to individual devices:
  - Patch All - Use the check-boxes on the left to choose the software you want to patch. Click 'Install Patches' to apply the update to all devices which require patching.
  - Patch Individual - Click the number in the 'Upgradable Devices' row > Select the devices you want to update > Click 'Install Patches'

Third Party Applications Table - Column Descriptions	
Column Heading	**Description**
Name	Name of the software. • Click the name to view application details. • See **View Details of an Application** for more details.
Vendor	The software publisher.
Category	The type of the application. Possible values include: • Comodo Products • Runtime applications • Web Browsers • Utilities

	• Messaging • File Compression utilities • Developer Tools • Documents • Online Storage • Other
Installed Devices	Total number of devices on which the application is installed. This figure includes devices with patched and unpatched versions of the software.
Upgradable Devices	Number of devices which need to be patched because they are using an older version of the software.
Controls	
Install Patch(es)	Allows you to install the patches/updates.
Hide Patch(es)	Allows you to hide selected patches that you do not want to update. Hidden patches will not be available for deployment on the 'Device Management' screen and will not be executed as well if added to a **patch procedure**.
Unhide Patch(es)	Allows you to unlock hidden patches.
Show hidden patch(es)	Allows you to view hidden patches and, if required, install them on endpoints. Use the toggle button to hide / view hidden applications.

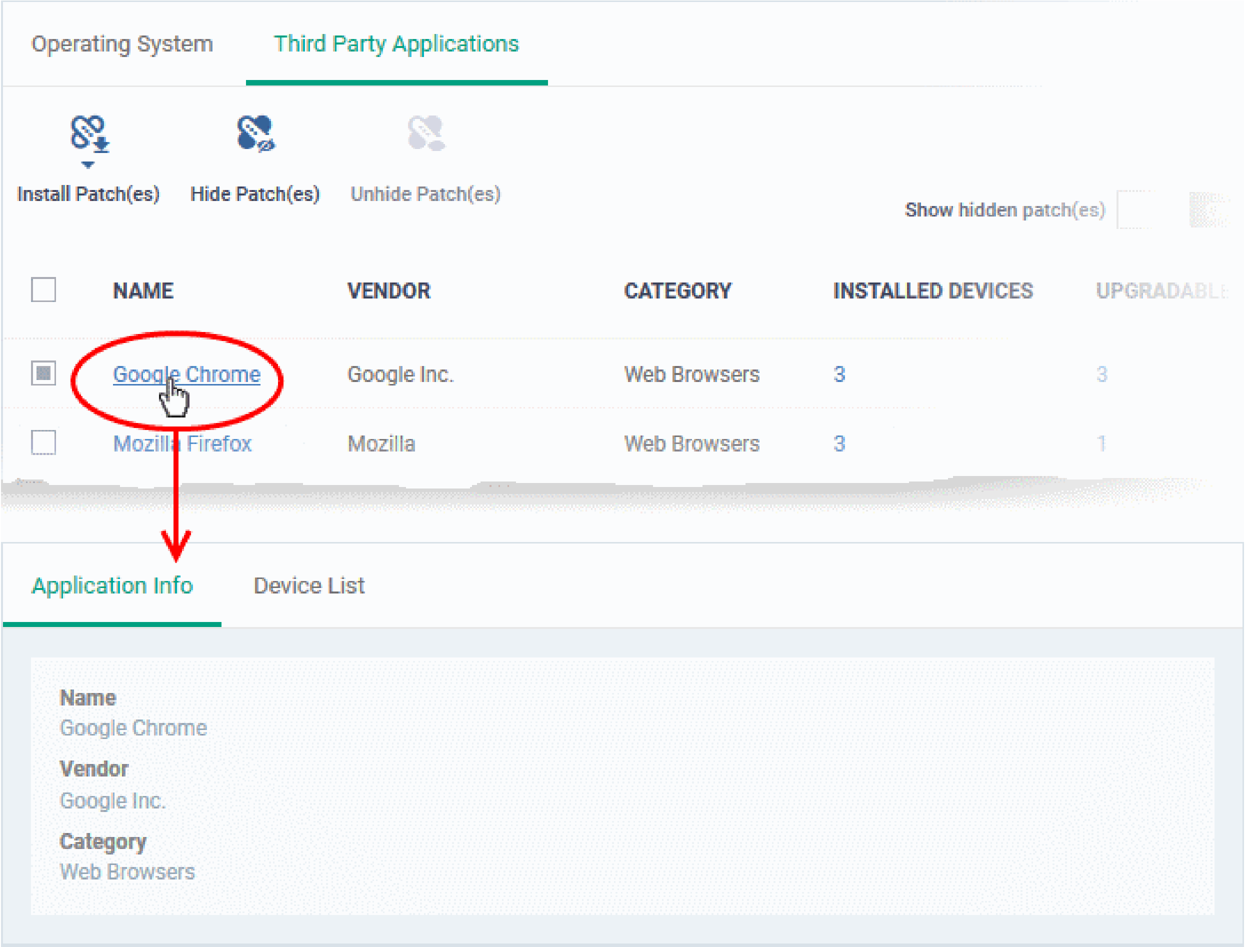
- Click any column header to sort items in ascending/descending order of entries in that column.
- Click the funnel icon on the right to search for applications by name, vendor and/or category.
- See '**ITSM Supported 3rd Party Applications**' for a full list of supported 3rd party applications.

The 'Patch Management' > 'Third Party Applications' interface allows you to:

- **View Details of an Application**
- **Hide Applications**
- **Restore Hidden Applications**
- **Update selected applications on all upgradable devices at once**
- **Update an application on selected devices**

View Details of an Application

- Click the name of any application to open its application details screen



	NAME	VENDOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE
☒	Google Chrome	Google Inc.	Web Browsers	3	3
□	Mozilla Firefox	Mozilla	Web Browsers	3	1

Name
Google Chrome

Vendor
Google Inc.

Category
Web Browsers

The details of the application are displayed under two tabs:

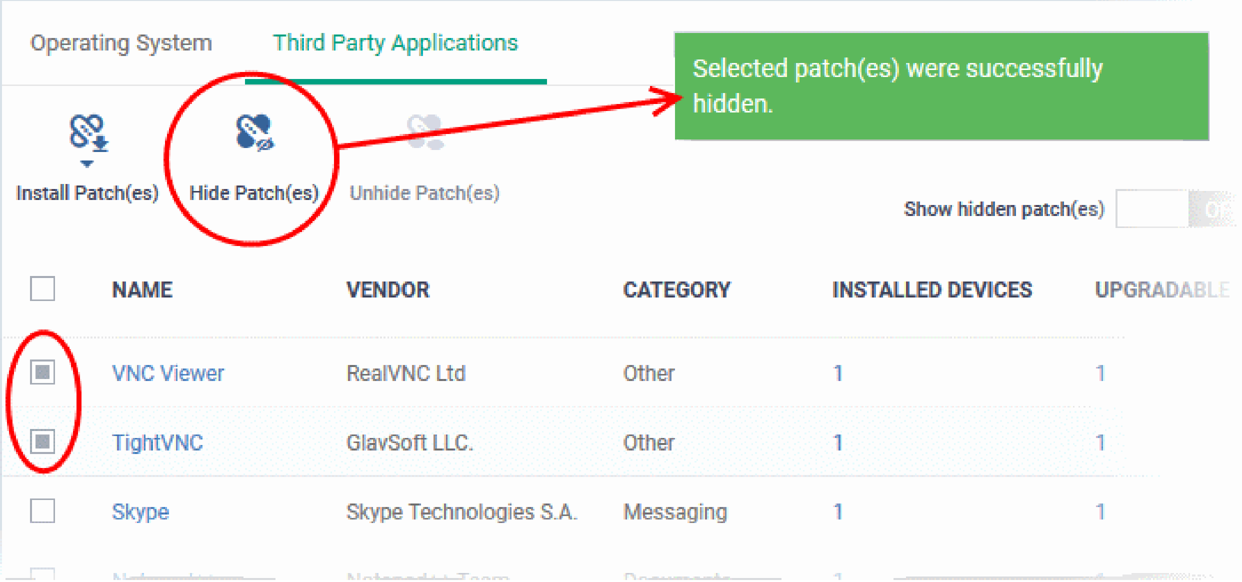
- **General** - Displays the name, software publisher and the category of the application.
- **Device List** - Displays the list of managed devices on which the application is installed, with the details like the installed version, installation path and the device owner. You can update the application on the devices where required from this screen. See Update an Application On Selected Devices for more details.

Hide Applications

- You can hide those applications that you do not want to update
- These applications will also be not available for update from the '**Device Management**' screen and will not be executed as well if added to a **patch procedure**.
- You can view the hidden applications by using the 'Show hidden patch(es) toggle button and update these applications on selected on devices.

To hide upgradable applications

- Select the application(s) to be hidden from the list and click 'Hide Patch(s)'



Selected patch(es) were successfully hidden.

☐	NAME	VENDOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE
☒	VNC Viewer	RealVNC Ltd	Other	1	1
☒	TightVNC	GlavSoft LLC.	Other	1	1
☐	Skype	Skype Technologies S.A.	Messaging	1	1

A confirmation message will be displayed. The selected applications will be hidden from the list.

- To view the hidden applications, use the 'Show hidden patch(es)' switch on the top right
- To re-add the hidden applications to the list, you have to **unhide** them.

Restore Hidden Applications

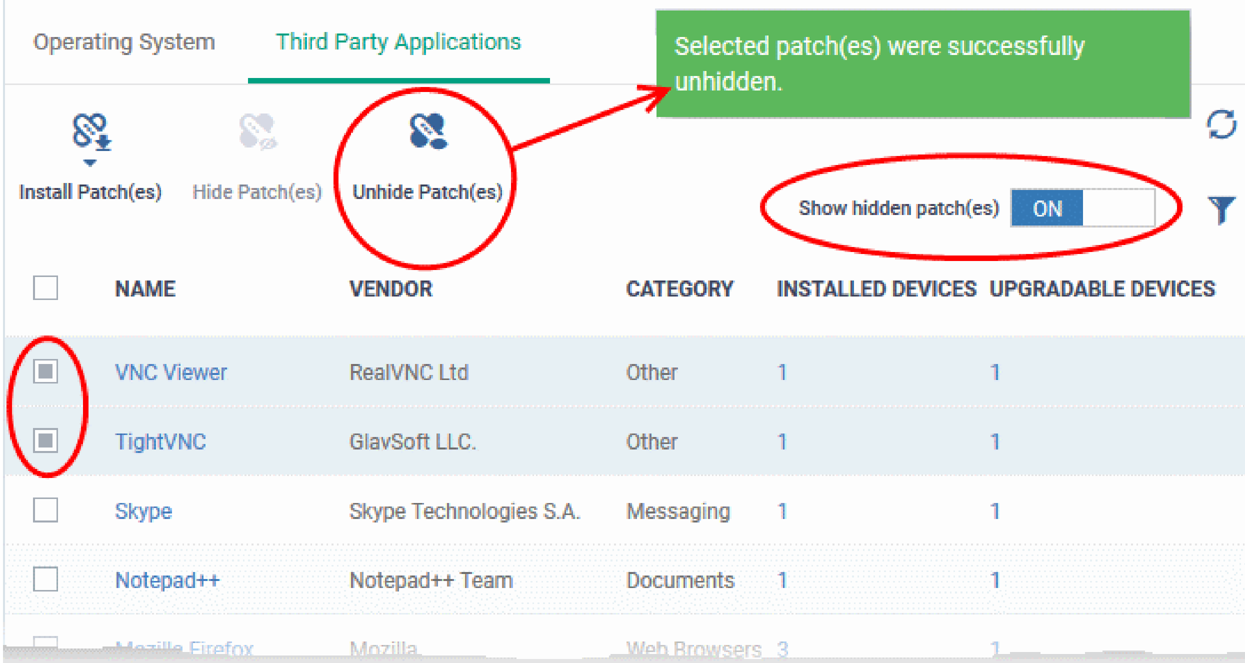
- You can make the hidden applications to be re-added to the 'Third Party Applications' interface.
- Restored applications will also be available for being updated from the **Device Management** interface and can be added to a **patch procedure**.

To view hidden upgradable applications and restore them

- Slide the 'Show hidden patch(es)' button to 'On'

The hidden applications will be shown with dark gray background stripe.

- Select the hidden patch(es) from the list and click 'Unhide Patch(es)'



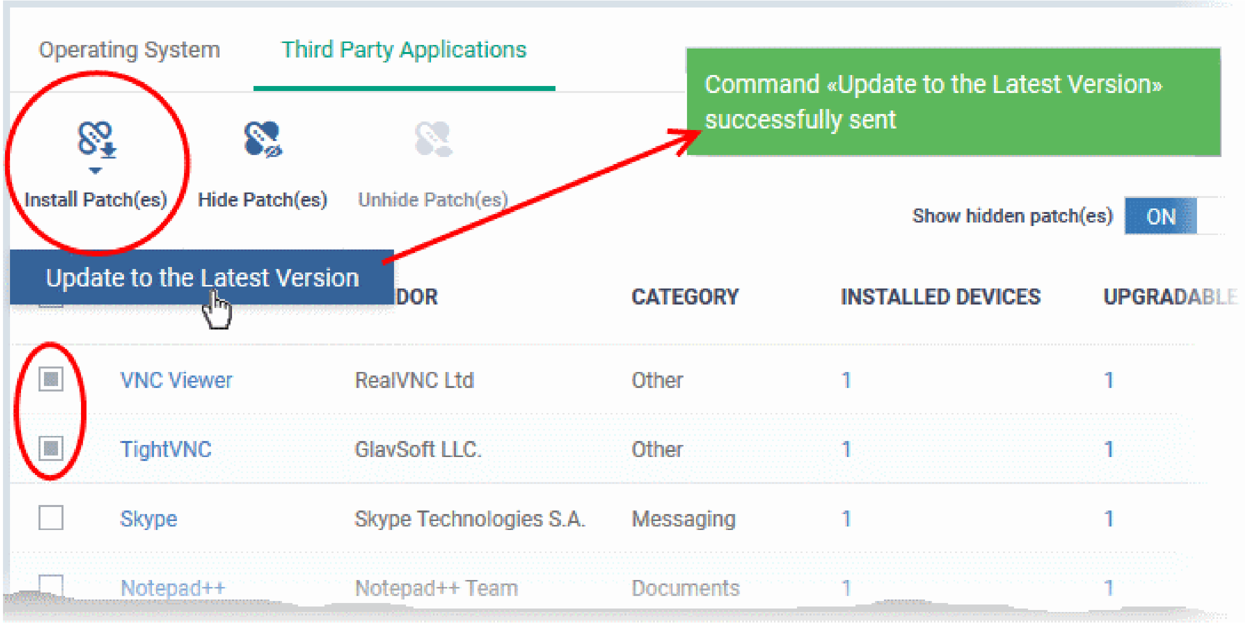
Selected patch(es) were successfully unhidden.

☐	NAME	VENDOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE DEVICES
☒	VNC Viewer	RealVNC Ltd	Other	1	1
☒	TightVNC	GlavSoft LLC.	Other	1	1
☐	Skype	Skype Technologies S.A.	Messaging	1	1
☐	Notepad++	Notepad++ Team	Documents	1	1
☐	Mozilla Firefox	Mozilla	Web Browsers	3	1

A confirmation message will be displayed. The applications will be re-added to the list.

Update Selected Applications on All Upgradable Devices at once

- Select the application(s) to be updated, click 'Install Patch(es)' and choose 'Update to Latest Version'



Command «Update to the Latest Version» successfully sent

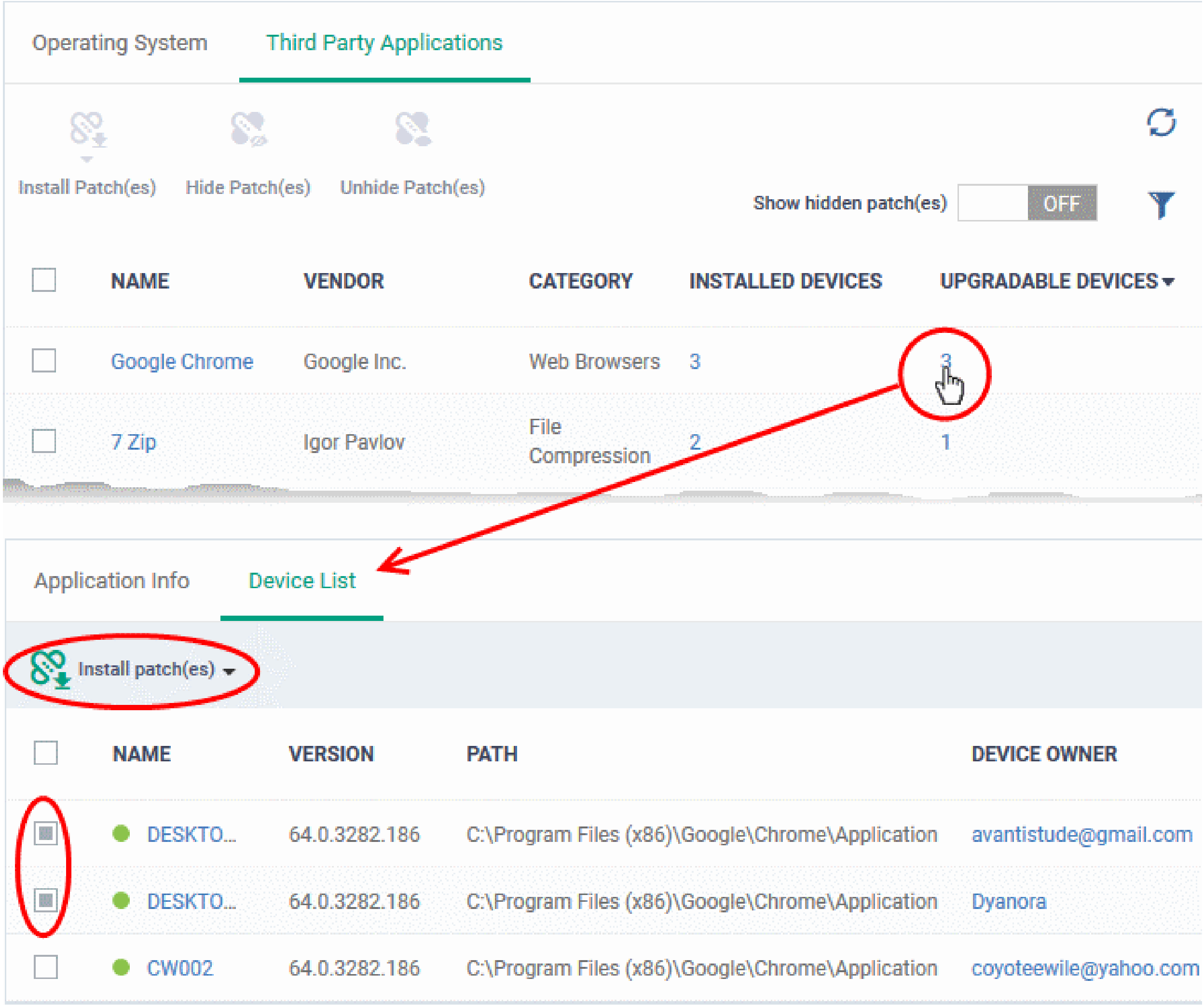
		DOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE
☑	VNC Viewer	RealVNC Ltd	Other	1	1
☑	TightVNC	GlavSoft LLC.	Other	1	1
□	Skype	Skype Technologies S.A.	Messaging	1	1
□	Notepad++	Notepad++ Team	Documents	1	1

A command will be sent to Comodo Client Communication (CCC) on the devices to commence the update.

- Once the command is received, CCC will check whether the update has already been downloaded by other devices in the network.
    - If the update is available, CCC establishes a peer-to-peer network with the device and downloads the patch. This reduces bandwidth usage as the update is downloaded from the local network.
    - If the update is not available on any devices in the local network, CCC downloads the update from the ITSM patch portal.

Update an Application on Selected Devices

- Click the number in the 'Upgradable Devices' column of the application to be updated



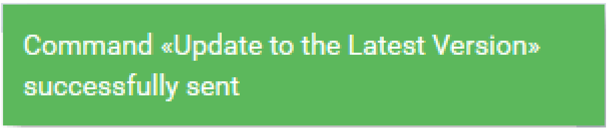
□	NAME	VENDOR	CATEGORY	INSTALLED DEVICES	UPGRADABLE DEVICES
□	Google Chrome	Google Inc.	Web Browsers	3	3
□	7 Zip	Igor Pavlov	File Compression	2	1

□	NAME	VERSION	PATH	DEVICE OWNER
☒	● DESKTO...	64.0.3282.186	C:\Program Files (x86)\Google\Chrome\Application	avantistude@gmail.com
☒	● DESKTO...	64.0.3282.186	C:\Program Files (x86)\Google\Chrome\Application	Dyanora
□	● CW002	64.0.3282.186	C:\Program Files (x86)\Google\Chrome\Application	coyoteewile@yahoo.com

The application details screen will appear with the 'Device List' tab open, with a list of devices on which the application can be updated.

- Select the device(s) on which the application is to be updated
- Click 'Install patch(es)' and choose 'Update to Latest Version'

A command will be sent to the endpoint(s) to schedule installation of the patch/update the application to the latest version.



Command «Update to the Latest Version» successfully sent

A command will be sent to Comodo Client Communication (CCC) on the devices to commence the update.

- Once the command is received, CCC will check whether the update has already been downloaded by other devices in the network.
    - If the update is available, CCC establishes a peer-to-peer network with the device and downloads the patch. This reduces bandwidth usage as the update is downloaded from the local network.
    - If the update is not available on any devices in the local network, CCC downloads the update from the ITSM patch portal.

7.2.2.1. ITSM Supported 3rd Party Applications

The following table provides the names of third party applications that can be updated on enrolled Windows endpoints:

- 7-Zip (32-bit)
- 7-Zip (64-bit)
- Adobe Acrobat Reader DC
- Adobe Flash Player ActiveX
- Adobe flash player NPAPI
- Adobe ShockWave Player
- BeyondCompare
- ccleaner
- ccleanerpro
- Citrix Group Policy Management
- Combined Community Codec Pack 32 bit
- Combined Community Codec Pack 64bit
- HipChat
- Citrix Receiver
- cutepdfwriter
- Cyberduck
- Defraggler
- FastStone Image Viewer
- FileZillaClient (32-bit)
- FileZillaClient (64BIT)
- Foobar
- Foxit Reader
- FrontMotion Firefox Community Edition (en-US)
- FrontmotionFirefoxCommunityEdition ESR
- GIMP 32bit
- GIMP 64 BIT
- Glary Utilities
- GOM Player
- Google Drive
- ImgBurn
- InfranView32bit
- EPI
- Evernote
- FashStoneImageViewer
- goodsync
- collageIt
- Editpadlite32bit
- Editpadlite64bit
- FreeArc
- jetclean
- PDF24 Creator
- Pdf -Viewer
- Safari
- zoom
- vncviewer32bit
- Dymo Label
- Adobe AIR
- AIMP
- keepasspasswordsafe2
- keepasspasswordsafe1
- Trillian32bit
- TED Notepad
- Renweb
- poedit
- PDF-XChange Editor 32bit
- PDF-XChange Editor 64bit
- emuletorrent
- wisediskcleaner
- CrystalDiskInfo
- TreeSize Free V4.0.3
- KerioControlVPNClient 32bit
- PKZip
- Jitsi32 bit
- Notepad++ (64-Bit)
- UltraVnc32bit
- Auslogics Duplicate File Finder
- Auslogics Registry Defrag
- Smart Defrag
- NoteTab Light
- Slik Subversion (x86)
- Slik Subversion (x86)
- BitLord
- Kingsoft Office 2013
- AutoIt
- FreeFixer
- Duplicate Cleaner Pro
- Pale Moon (x86 en-US)
- Pale Moon (x64 en-US)
- Sandboxie (32-bit) 5.2
- MPC-HC 1.7.13 (32-bit)
- MPC-HC 1.7.13 (64-bit)
- Zotero
- PICAXE Editor
- NoMachine
- Ant Movie Catalog
- Ant Renamer
- QTranslate
- EPIM-Outlook Sync
- GlassWire
- Universal Extractor
- Reflector 64 bit
- Screenpresso
- IE7Pro
- D&D Interceptor
- Unlocker
- Globalmapper
- tekla BIMsight 32 bit
- Reflector
- tekla BIMsight 64 bit

- InfranView64bit
- IZArc
- JDK 32 bit
- JDK 64BIT
- JRE 32BIT
- JRE 64BIT
- KeePass Password Safe 1
- KeePass Password Safe 2
- K-Lite Codec Pack Basic
- K-Lite Codec Pack Full
- K-Lite Codec Pack Standard
- K-Lite Mega Codec Pack
- LibreOffice - (32-bit)
- LiberOffice - (64BIT)
- Malwarebytes
- MediaMonkey
- Microsoft Silverlight 32bit
- Microsoft Silverlight 64bit
- Mozilla Firefox - (32-bit)
- Mozilla Firefox - (64-bit)
- Mozilla Firefox ESR
- Mozilla Thunderbird
- MozyHome
- Notepad++ (32-bit)
- Oracle VM Virtualbox
- Operastable
- OpenOffice
- paint.net 32bit
- PeaZip - (32-bit)
- PeaZip - 64BIT
- Putty - (32-bit)
- Putty 64BIT
- Recuva
- SeaMonkey
- Skype
- Speccy
- SugarSync
- Krita (x86)
- Google Earth pro
- Visual Studio Code 32bit
- Visual Studio Code 64 bit
- Zimbra Desktop
- Google earth
- HipChat
- Xmind
- snagit(windows 10 only supported)
- CDBurnerXP 32 bit
- CDBurnerXP 64 bit
- Flashget
- grepwin 64 bit
- Irfan view 64 bit
- jetclean
- Microsoft AntiXSS v4.3.0
- plex media server 32 bit
- spybot
- Musicbee
- Foxit phantom pdf
- bluebeam vu
- Zimbra Desktop
- windows phone app for desktop
- Tortoise git 32 bit
- Seamonkey 64 bit
- microsoft visual C++ 32 bit
- Microsoft Visual Studio Code
- krita (64bit)
- Free RAR Extract Frog
- vnc viewer 64 bit
- mediainfo
- winsnap
- Microsoft Power BI Desktop (32 bit)
- R for Windows
- Druva inSync
- npassword
- Maxthon Cloud Browser
- arallelsClient-64 bit
- PNotes.net
- AppInventor Setup
- netbeansIDE 8.2
- Avs media player
- dual monitor tools
- MozyPro
- Zoom player max 14
- pcon-planner 32 bit
- pcon-planner 64 bit
- AVS documentconvertor-4.0.3.252
- HttpWatch basic
- advanced installer
- RD Tabs 32 bit
- RD Tabs 64 bit
- Hard copy pro
- crashplan 32 bit
- EncryptOnClick
- Exact audio copy
- DC++
- Microsoft visual studio code x64
- HelpNDoc 5.4.1.404 Personal Edition
- VitalSource Bookshelf
- adobe digital edition
- Adblock Plus for IE (32-bit)
- Printkey -pro
- vnc enterprise edition
- crash plan 64 bit
- DU Meter
- AnkhSVN 32 bit
- Uninstall DisplayCAL
- AVS Media Player
- VNC Enterprise Edition

- SumatraPDF - (32-bit)
- SumatraPDF- 64 bit
- TeamViewer
- TeraCopy
- Libreoffice
- Logitech Setpoint
- LogMeinHemachi
- TightVNC - (32-bit)
- TightVNC - (32-bit)
- VLC media player - (32-bit)
- VLC media player - (64-bit)
- VNC Server - (32-bit)
- Wise Force Deleter (No Arch)
- Winamp
- WinMerge
- WinRAR - (32-bit)
- WinRAR - (64-bit)
- WinSCP
- WinZip - (32-bit)
- WinZip - (64-bit)
- Wireshark - (32-bit)
- Wireshark -(64-bit)
- XnView
- XnConvert (32-bit)
- XnConvert (64 bit)
- FileZilaClient
- PDFsamBasic
- realvnc64 bit
- irfanview32bit
- classicshell
- qbittorrent32bit
- qbittorrent64bit
- wisefolderhider
- grepwin32bit
- wisecare365
- RJ Text edit 32bit
- RJ Text edit 64 BIT
- BitComet
- anydvd
- mumble
- active presenter
- netsetman
- Avant Browser
- AirServer Universal (x64)
- AirServer Universal (x32)
- Mp3tag
- Calibre(x32)
- Calibre(x64)
- owncloud
- Media Player Classic Home (x32)
- Media Player Classic Home (x64)
- exacqVision Client 8.6.1.115131 (x64)
- exacqVision Client 8.6.1.115131 (x32)
- Miranda IM 32bit
- WinHTTrack Website Copier 32bit
- WinHTTrack Website Copier 64bit
- Microsoft PowerPoint Viewer
- pot player 32bit
- WinDjView
- FastStone Capture
- Honeycam
- Bandizip
- Honeyview
- Syncbackfree
- Plantronics Hub Software
- Mozilla Firefox ESR (x64 en-US)
- Auslogics Browser Care
- Auslogics Registry Cleaner
- AVS Image Converter
- Synology Surveillance Station Client 32 bit
- Kerio Outlook Connector
- SciTE Text Editor
- SciTE Text Editor 64bit
- Duplicate cleaner pro
- VNC Enterprise Edition
- Synology Surveillance Station Client 64bit
- MySQL Workbench 6.3
- cabos
- jing
- iReport
- Rstudio
- LogMeIn Hamachi
- Compatibility Pack for the 2007 Office system
- Foxit Advanced PDF Editor
- Microsoft SQL Server 2008 R2 Native Client
- MySQL Connector 6.1.11
- Apple Mobile Device Support
- Spiceworks Desktop
- LogMeIn Client
- Jabra Direct
- IIS(32 and 64 bit)
- Apple Software Update 2.4.8.1
- Tsprint client
- Microsoft Web Deploy
- PDFTools Version
- Synology Surveillance Station Client
- synology survivellance
- Vulkan Run Time Libraries
- audacity 64 bit
- paint.net32 bit
- audacity 32 bit

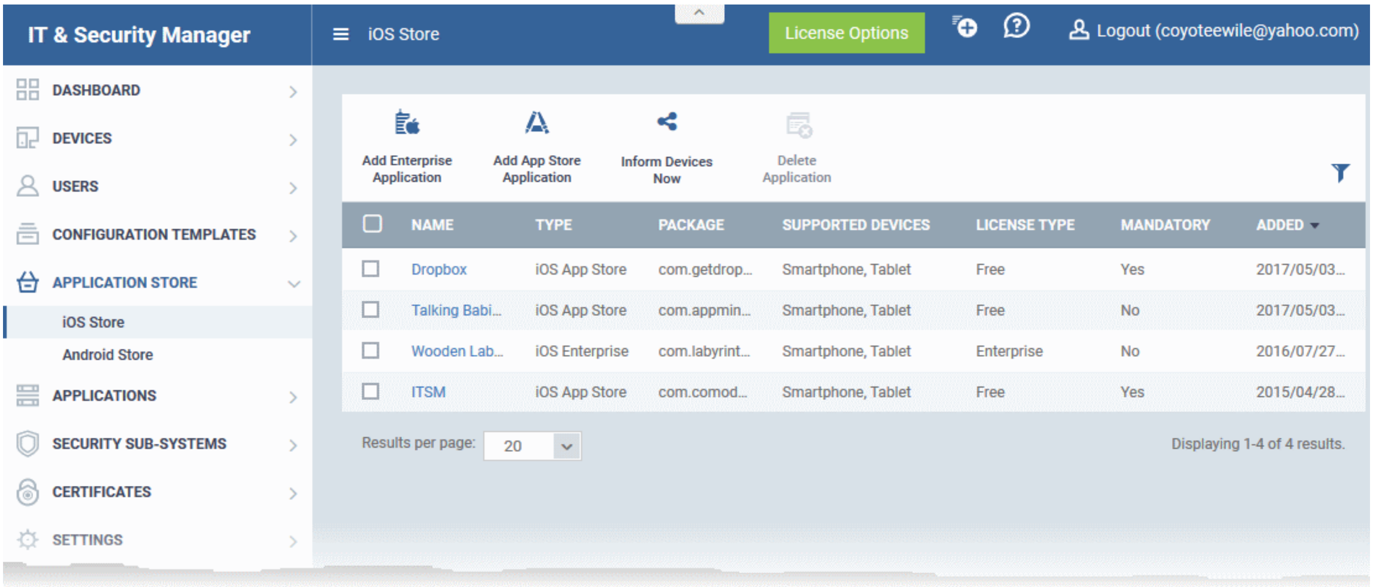
8. App Store

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.



☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDATORY	ADDED ▾
☐	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes	2017/05/03...
☐	Talking Babi...	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No	2017/05/03...
☐	Wooden Lab...	iOS Enterprise	com.labyrint...	Smartphone, Tablet	Enterprise	No	2016/07/27...
☐	ITSM	iOS App Store	com.comod...	Smartphone, Tablet	Free	Yes	2015/04/28...

Results per page: 20

Displaying 1-4 of 4 results.

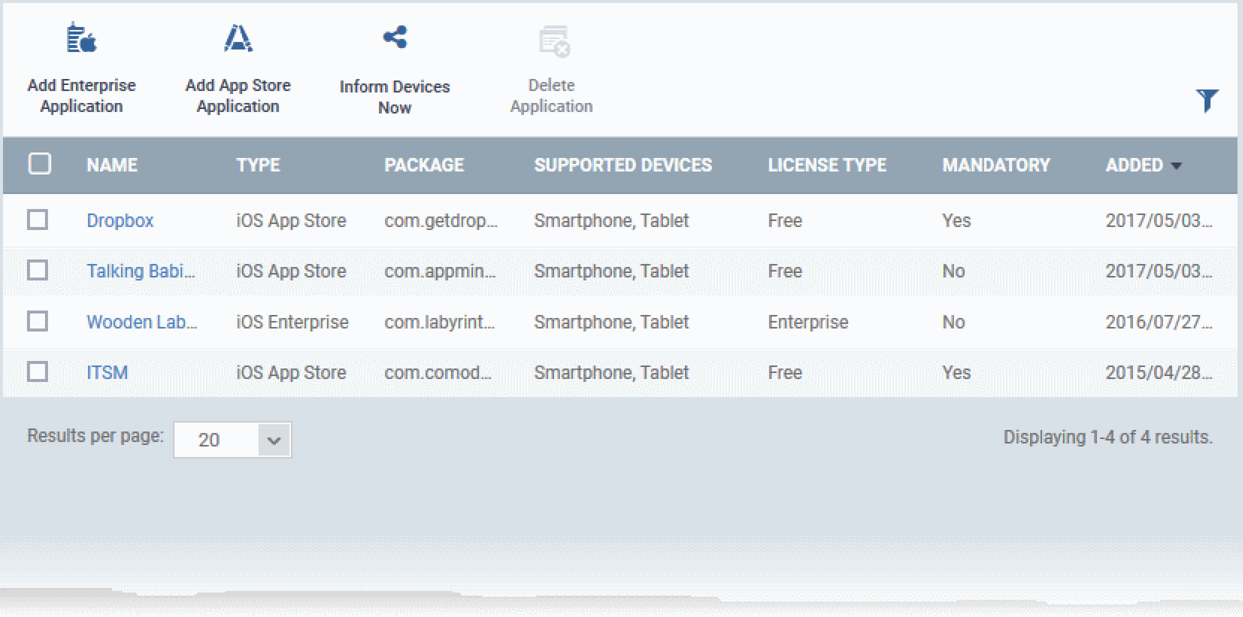
The following sections contain more details on each app type:

- 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' on the left then choose 'iOS Store' from the options.



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDATORY	ADDED
□	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes	2017/05/03...
□	Talking Babi...	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No	2017/05/03...
□	Wooden Lab...	iOS Enterprise	com.labyrint...	Smartphone, Tablet	Enterprise	No	2016/07/27...
□	ITSM	iOS App Store	com.comod...	Smartphone, Tablet	Free	Yes	2015/04/28...

Results per page: 20

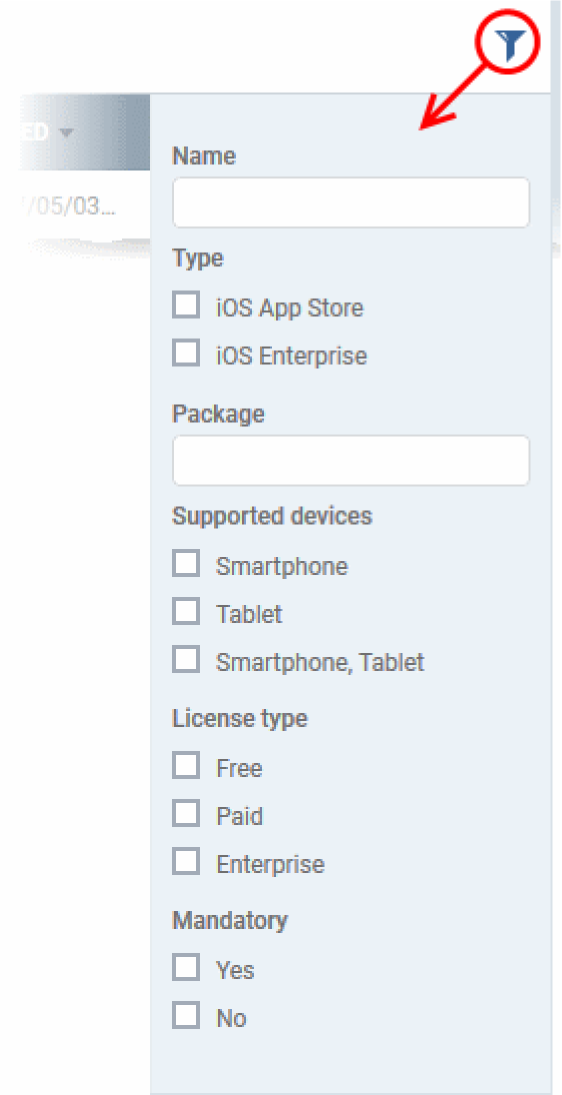
Displaying 1-4 of 4 results.

'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.



Name

Type

□ iOS App Store

□ iOS Enterprise

Package

Supported devices

□ Smartphone

□ Tablet

□ Smartphone, Tablet

License type

□ Free

□ Paid

□ Enterprise

Mandatory

□ Yes

□ No

- 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. Add iOS Apps and Install 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:

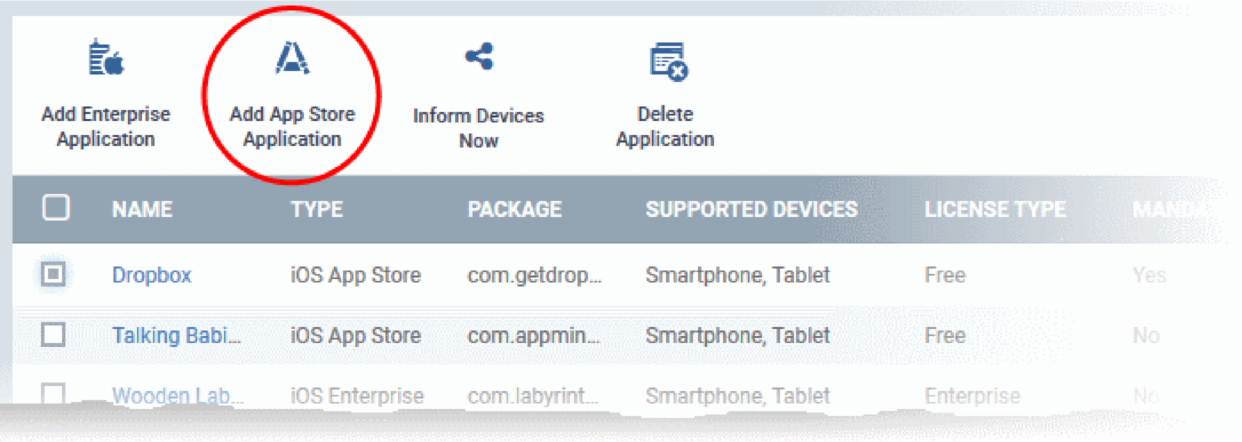
- **Adding iOS Apps from App Store**
- **Adding Custom/Enterprise iOS Apps**

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.

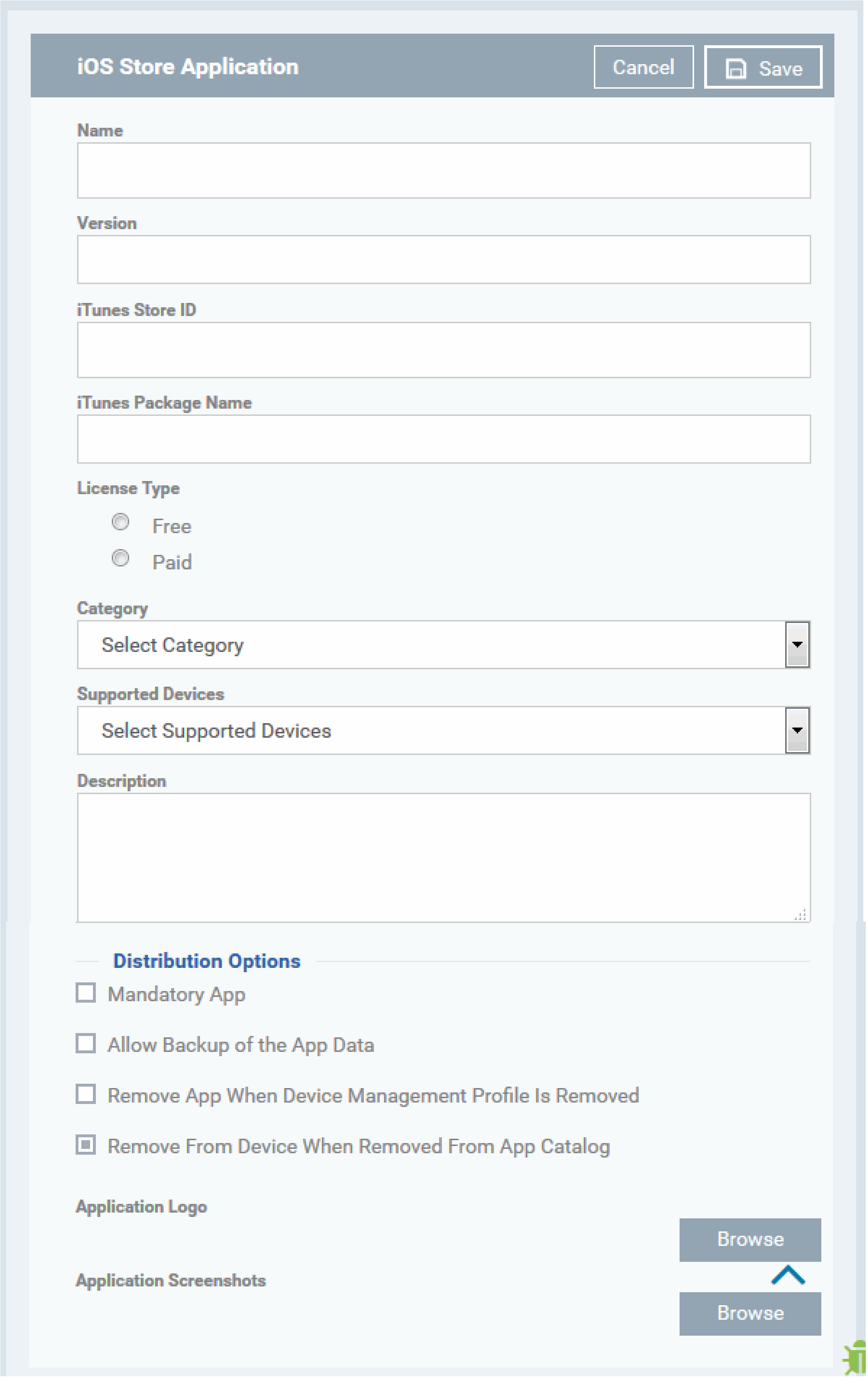
To add an iOS App from App Store

- Click 'Application Store' on the left then choose 'iOS Store' to open the 'iOS Store' interface
- Click on 'Add App Store Application' from the options at the top.



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDA
▣	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes
□	Talking Babi...	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No
□	Wooden Lab...	iOS Enterprise	com.labyrint...	Smartphone, Tablet	Enterprise	No

The 'iOS Store Application' screen will open:



iOS Store Application

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

Application Screenshots

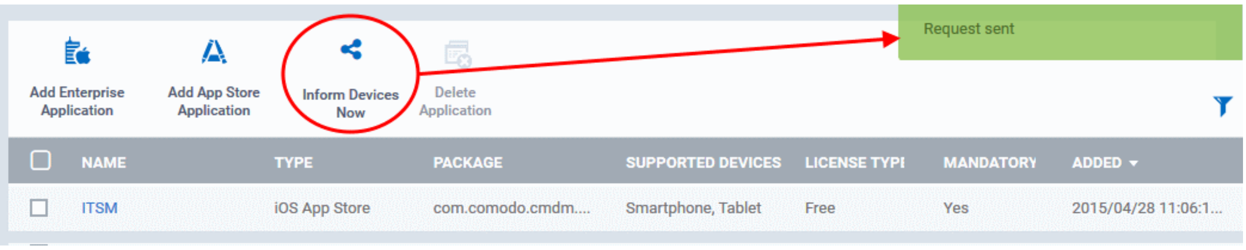
Apple Store Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Allows you to enter the name of the application. • Start entering the first few letters of the name of the application. ITSM will search for Apps from the App Store using the letters entered as search 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.



☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPI	MANDATORY	ADDED ▾
☐	ITSM	iOS App Store	com.comodo.cmdm....	Smartphone, Tablet	Free	Yes	2015/04/28 11:06:1...

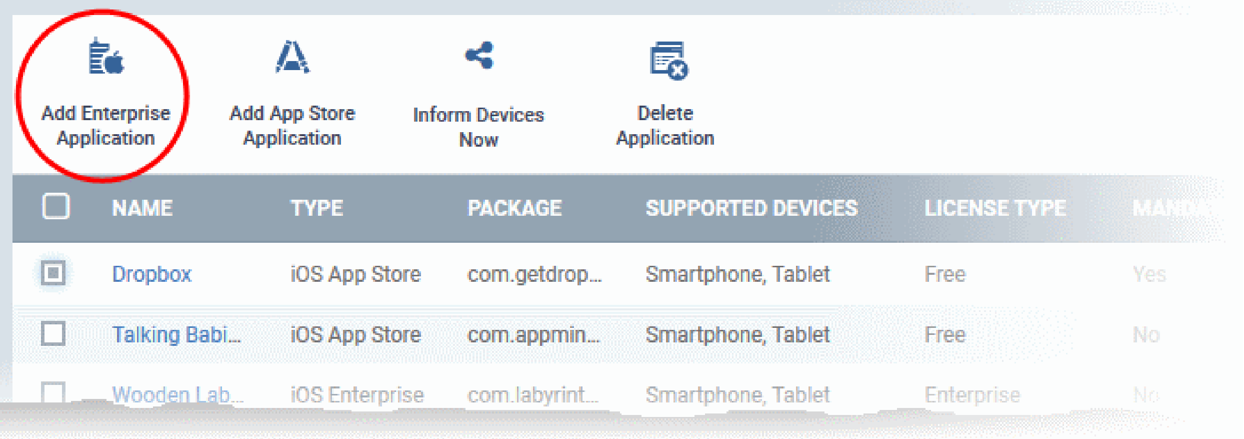
Adding Custom/Enterprise iOS Apps

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.

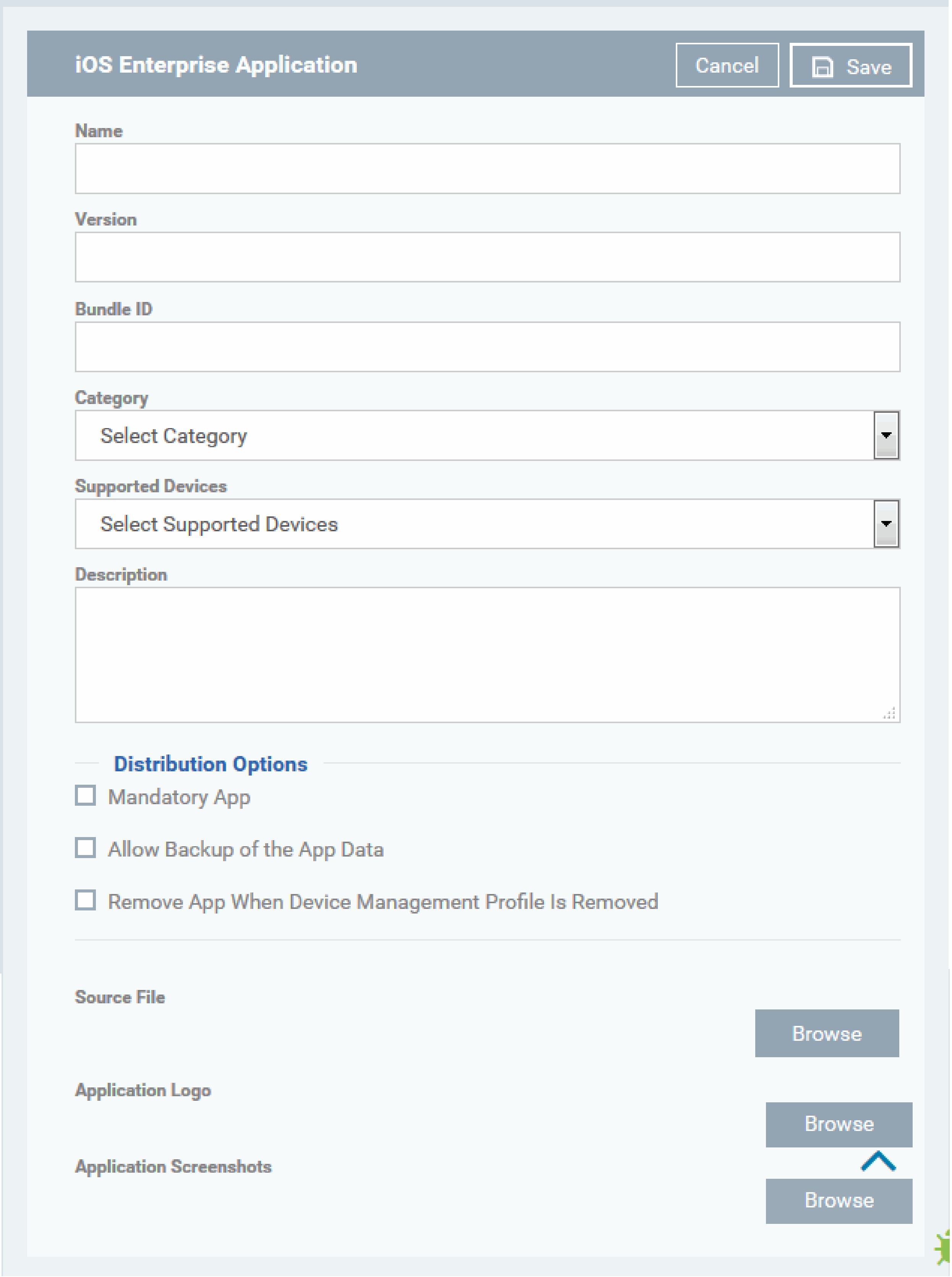
To add Custom/Enterprise iOS Apps

- 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.



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MAND
▣	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes
□	Talking Babi...	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No
□	Wooden Lab...	iOS Enterprise	com.labyrint...	Smartphone, Tablet	Enterprise	No

The 'iOS Enterprise Application' screen will open.



iOS Enterprise Application

Cancel | Save

Name

Version

Bundle ID

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

Source File — Browse

Application Logo — Browse

Application Screenshots — Browse

- Click 'Browse' under 'Source File', navigate to the location of the .ipa file to be uploaded, select the file and click 'Open'

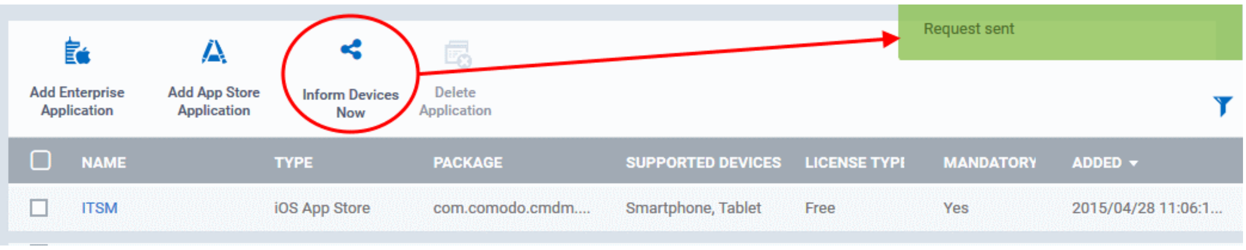
The file will be uploaded and the details will be auto-populated.

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.



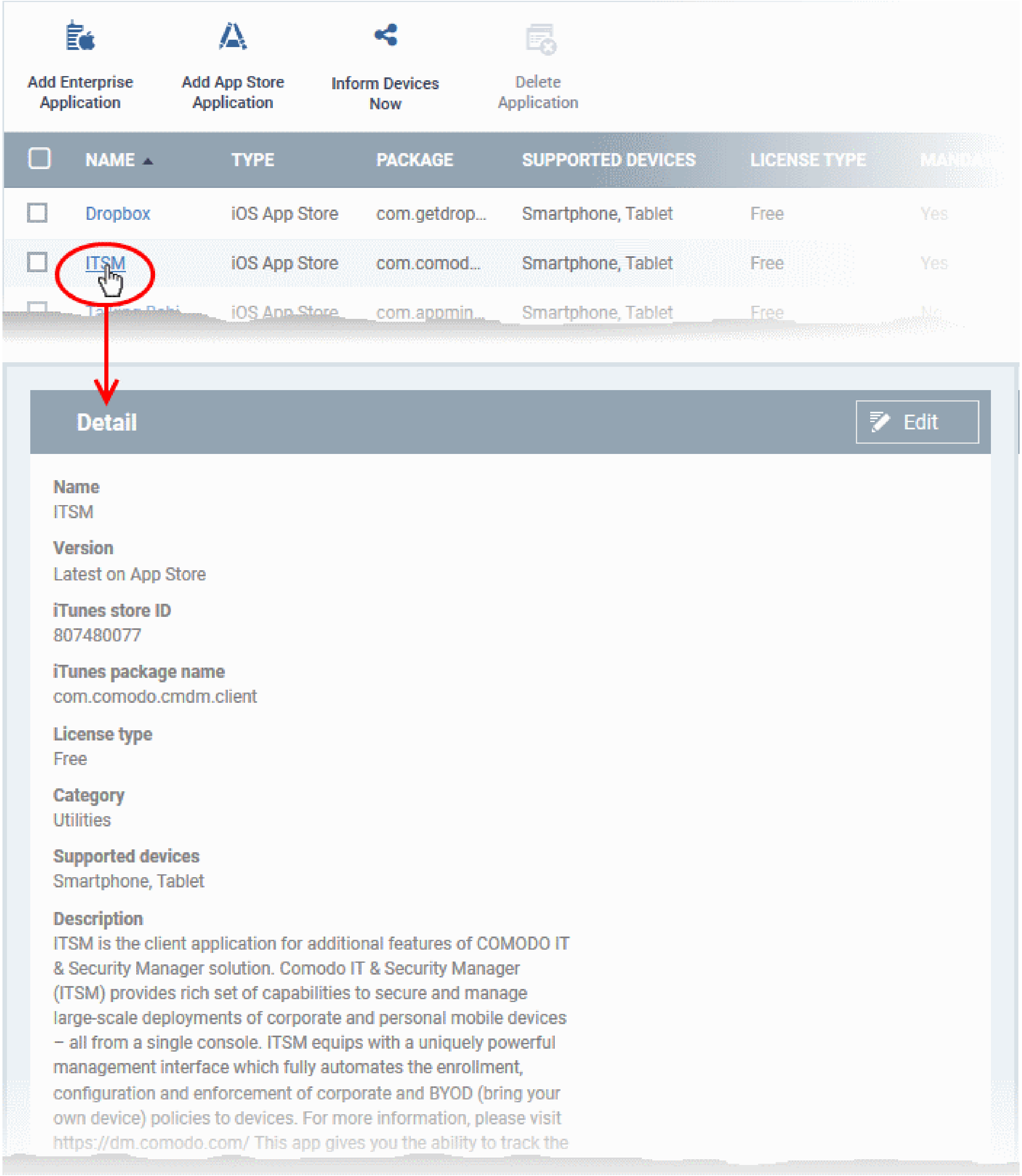
☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPI	MANDATORY	ADDED
☐	ITSM	iOS App Store	com.comodo.cmdm....	Smartphone, Tablet	Free	Yes	2015/04/28 11:06:1...

8.1.2. Manage 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' on the left then choose 'iOS Store'
- Click the name of the App.



□	NAME ▲	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDA
□	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes
□	ITSM	iOS App Store	com.comod...	Smartphone, Tablet	Free	Yes
□	[illegible]	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No

Detail

Name
ITSM

Version
Latest on App Store

iTunes store ID
807480077

iTunes package name
com.comodo.cmdm.client

License type
Free

Category
Utilities

Supported devices
Smartphone, Tablet

Description
ITSM is the client application for additional features of COMODO IT & Security Manager solution. Comodo IT & Security Manager (ITSM) provides rich set of capabilities to secure and manage large-scale deployments of corporate and personal mobile devices – all from a single console. ITSM equips with a uniquely powerful management interface which fully automates the enrollment, configuration and enforcement of corporate and BYOD (bring your own device) policies to devices. For more information, please visit https://dm.comodo.com/ This app gives you the ability to track the

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 Edit at the top right .

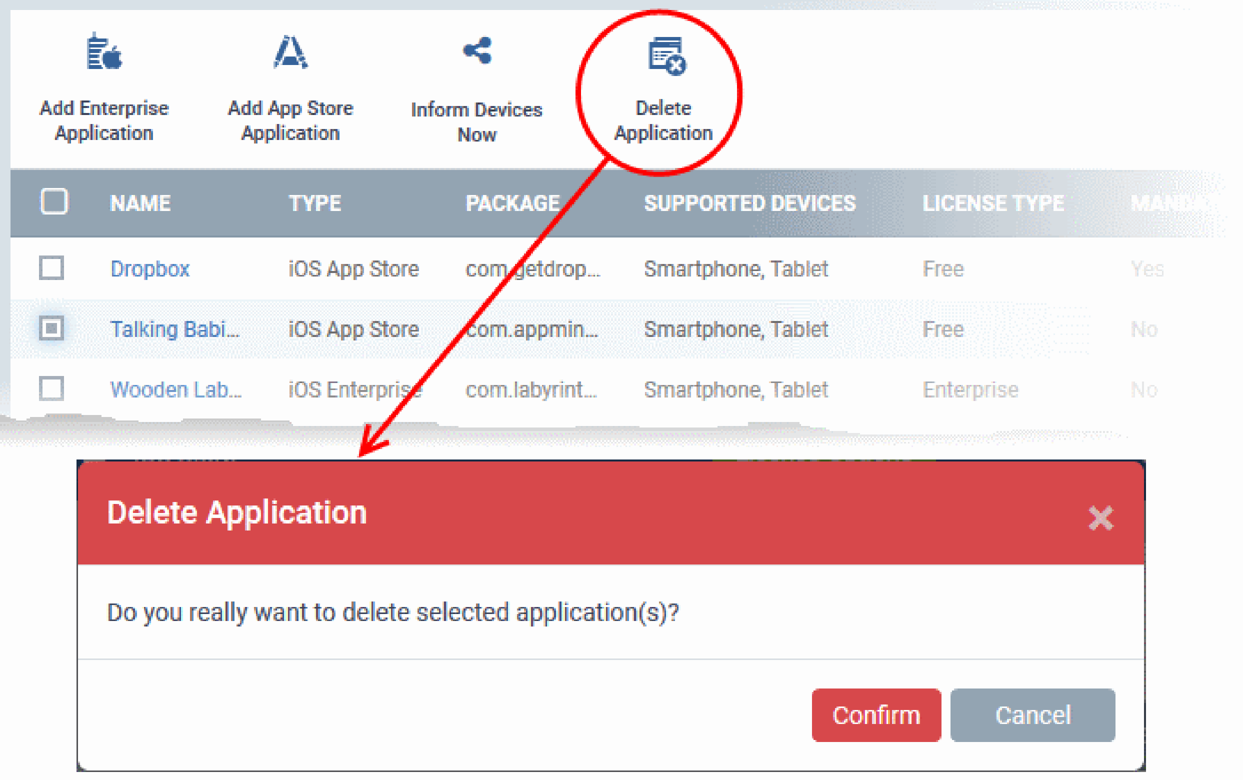
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section **Adding iOS Apps and Installing them on Devices**.

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' on the left then choose 'iOS Store'
- Select the App(s) to be removed and click 'Delete Application' from the options above the table.



☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDA
☐	Dropbox	iOS App Store	com.getdrop...	Smartphone, Tablet	Free	Yes
☒	Talking Babi...	iOS App Store	com.appmin...	Smartphone, Tablet	Free	No
☐	Wooden Lab...	iOS Enterprise	com.labyrint...	Smartphone, Tablet	Enterprise	No

Delete Application ×

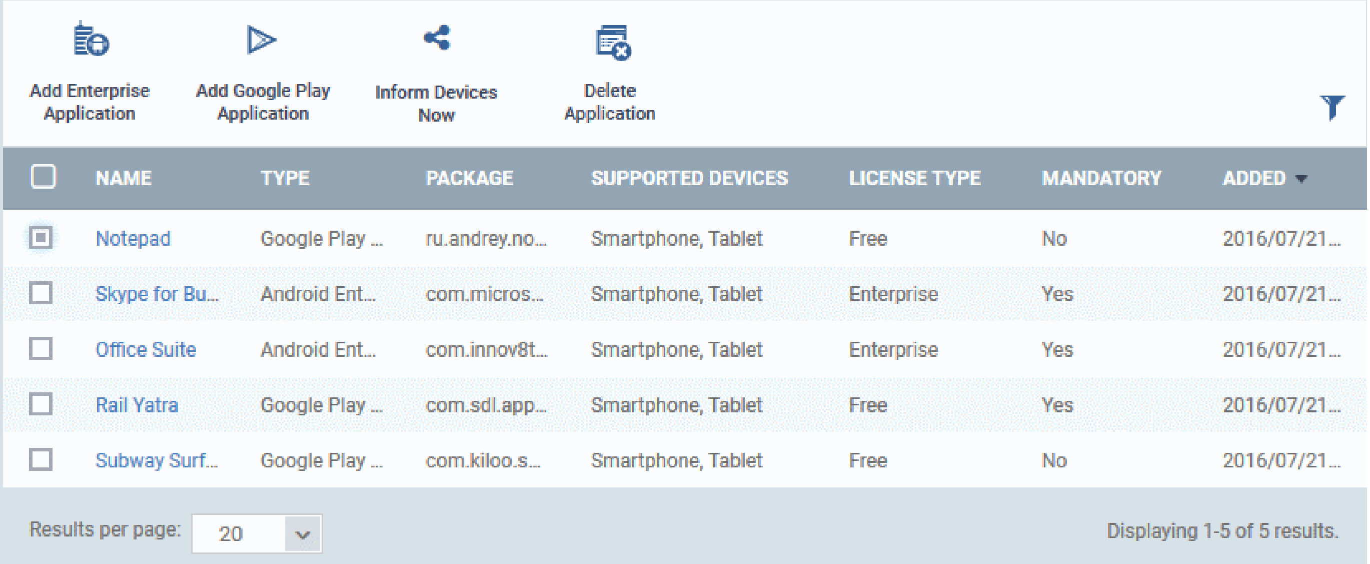
Do you really want to delete selected application(s)?

- 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' on the left then choose 'Android Store' from the options.



☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDATORY	ADDED
☐	Notepad	Google Play ...	ru.andrey.no...	Smartphone, Tablet	Free	No	2016/07/21...
☐	Skype for Bu...	Android Ent...	com.micros...	Smartphone, Tablet	Enterprise	Yes	2016/07/21...
☐	Office Suite	Android Ent...	com.innov8t...	Smartphone, Tablet	Enterprise	Yes	2016/07/21...
☐	Rail Yatra	Google Play ...	com.sdl.app...	Smartphone, Tablet	Free	Yes	2016/07/21...
☐	Subway Surf...	Google Play ...	com.kiloo.s...	Smartphone, Tablet	Free	No	2016/07/21...

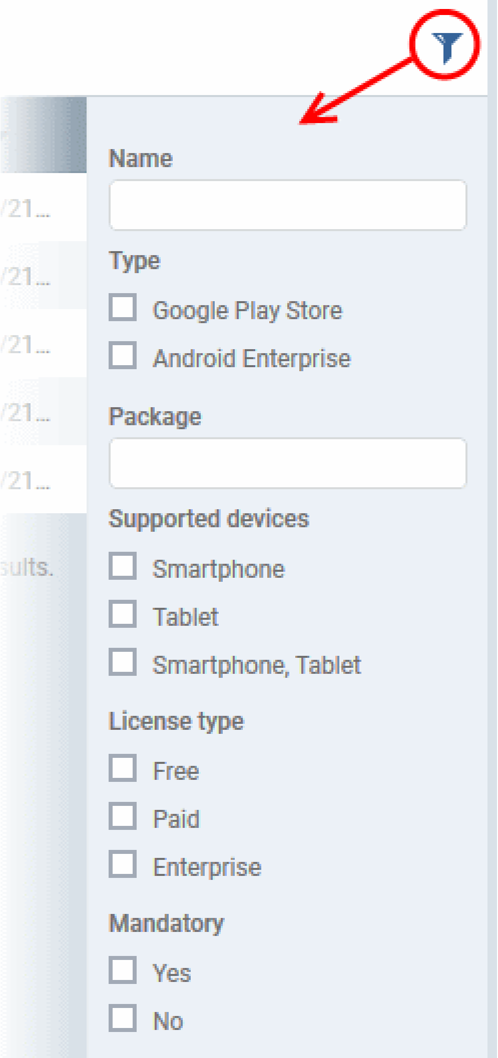
Results per page: 20 Displaying 1-5 of 5 results.

'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.
Type	Indicates the source type of the app. Possible types are: • Google Play Store Application • Android Enterprise Application 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 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'.



Name

Type

□ Google Play Store

□ Android Enterprise

Package

Supported devices

□ Smartphone

□ Tablet

□ Smartphone, Tablet

License type

□ Free

□ Paid

□ Enterprise

Mandatory

□ Yes

□ No

- 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. Add Android Apps and Install 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:

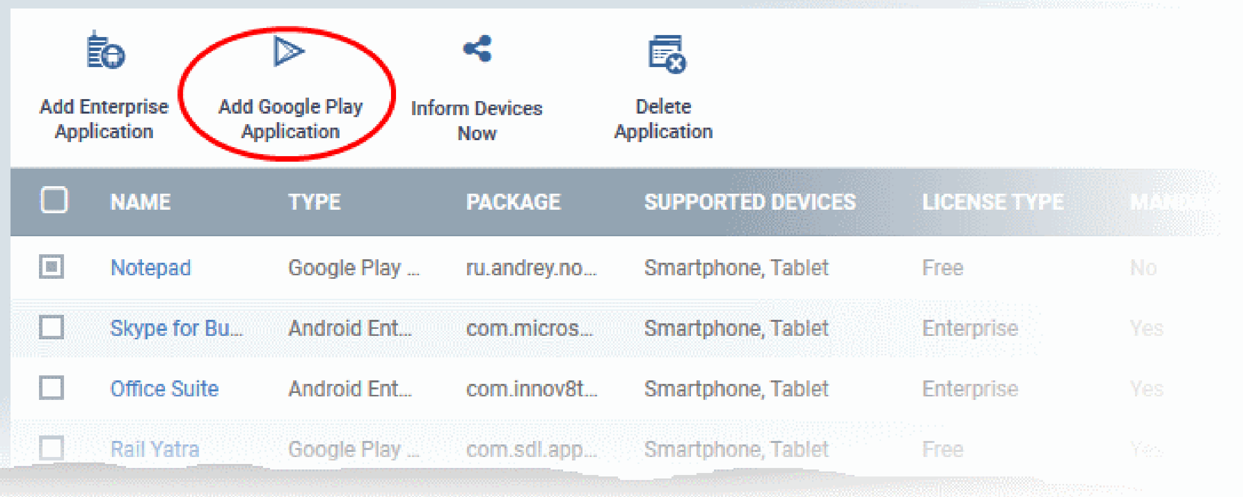
- Adding Android Apps from App Store
- Adding Custom/Enterprise Android Apps

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.

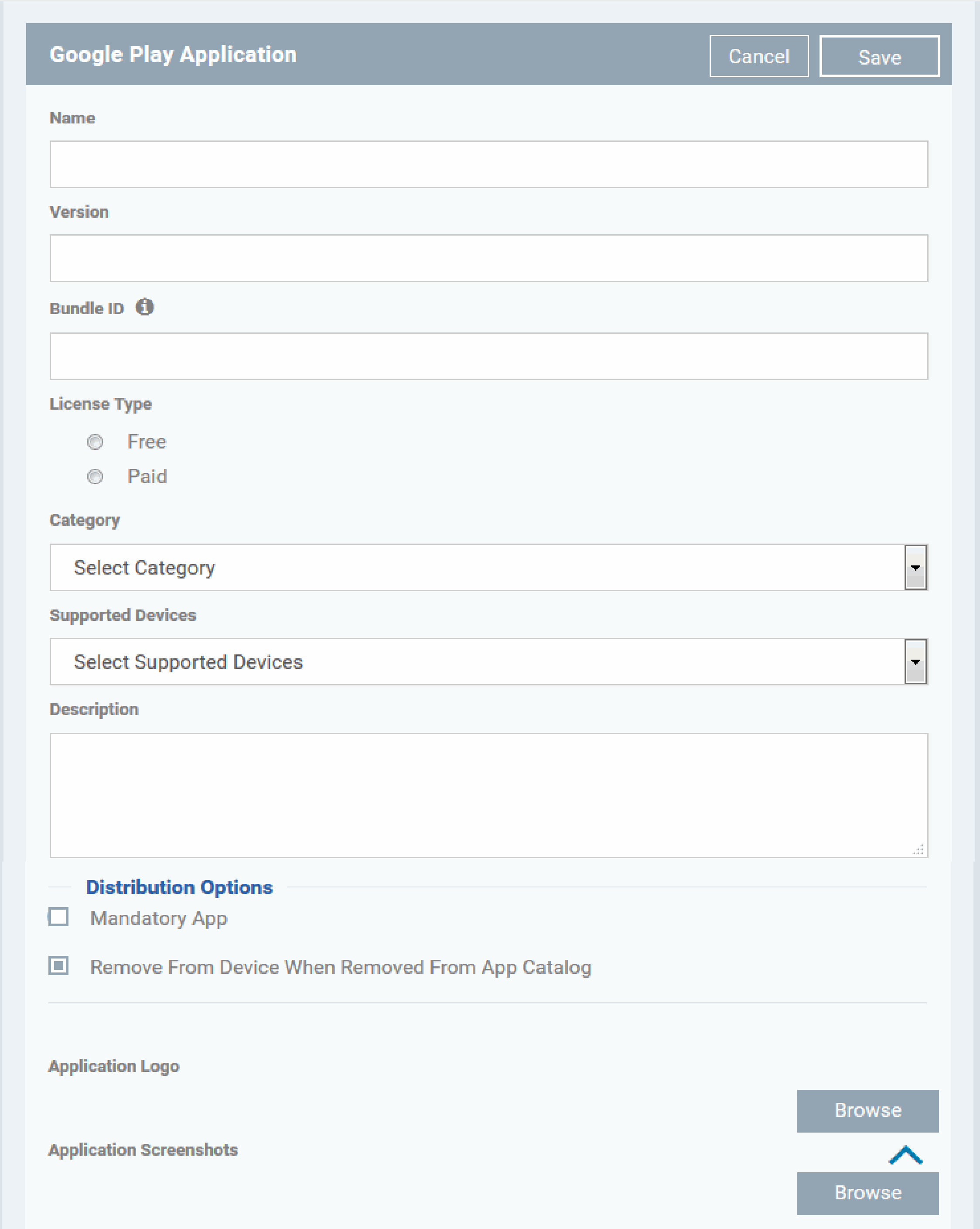
To add an Android App from Google Play Store

- Click 'Application Store' on the left then choose 'Android Store' to open the 'Android Store' interface
- Click 'Add Google Play Application' from the options at the top.



☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDA
▣	Notepad	Google Play ...	ru.andrey.no...	Smartphone, Tablet	Free	No
☐	Skype for Bu...	Android Ent...	com.micros...	Smartphone, Tablet	Enterprise	Yes
☐	Office Suite	Android Ent...	com.innov8t...	Smartphone, Tablet	Enterprise	Yes
☐	Rail Yatra	Google Play ...	com.sdl.app...	Smartphone, Tablet	Free	Yes

The 'Google Play Application' screen will open.



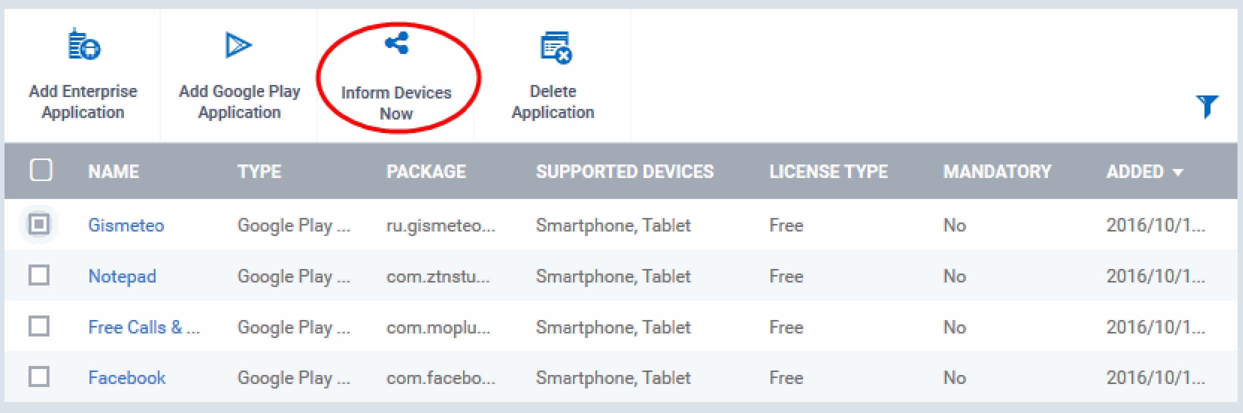
Google Play Application - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	Allows you to enter the name of the application. • Start entering the first few letters of the name of the application. ITSM will search for Apps from the Google Play Store using the letters entered 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

Google Play Application - Table of Parameters		
		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.
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.



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDATORY	ADDED
☒	Gismeteo	Google Play ...	ru.gismeteo...	Smartphone, Tablet	Free	No	2016/10/1...
□	Notepad	Google Play ...	com.ztnstu...	Smartphone, Tablet	Free	No	2016/10/1...
□	Free Calls & ...	Google Play ...	com.moplu...	Smartphone, Tablet	Free	No	2016/10/1...
□	Facebook	Google Play ...	com.facebo...	Smartphone, Tablet	Free	No	2016/10/1...

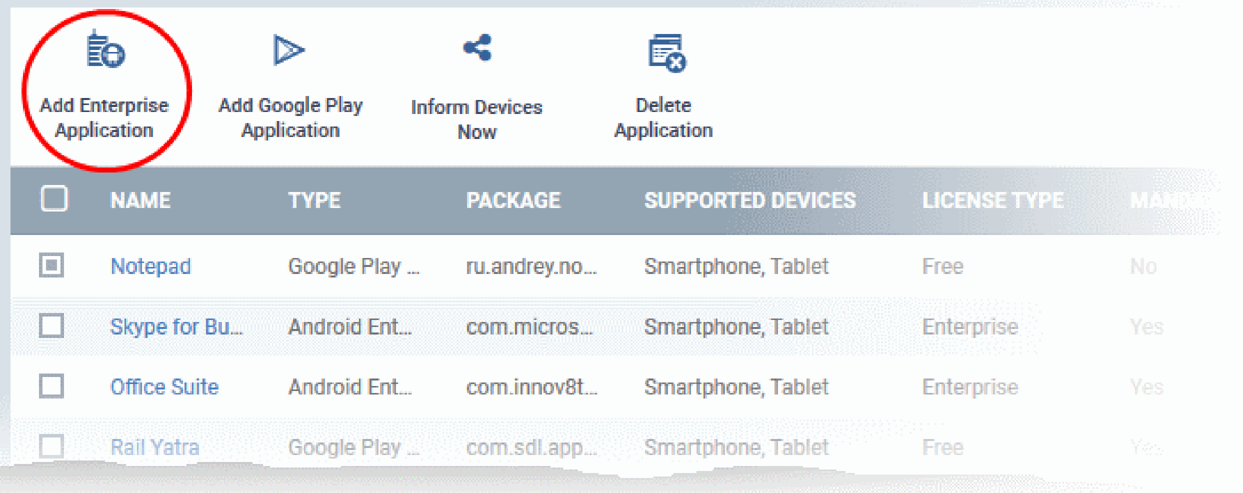
Adding Custom/Enterprise Android Apps

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.

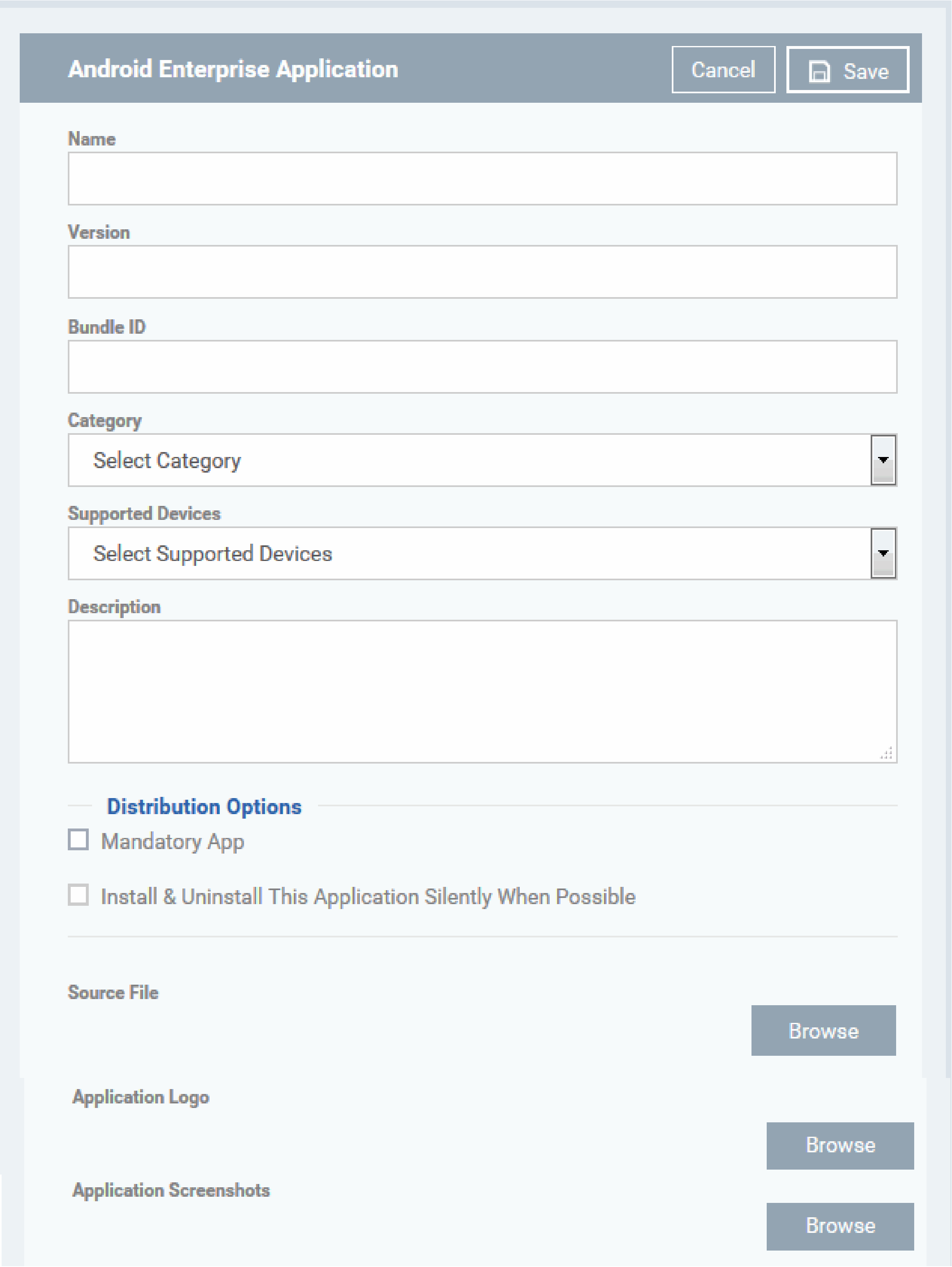
To add Custom/Enterprise Android Apps

- Click 'Application Store' on the left then choose 'Android Store'
- Click 'Add Enterprise Application' from the options at the top.



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MAND...
☒	Notepad	Google Play ...	ru.andrey.no...	Smartphone, Tablet	Free	No
□	Skype for Bu...	Android Ent...	com.micros...	Smartphone, Tablet	Enterprise	Yes
□	Office Suite	Android Ent...	com.innov8t...	Smartphone, Tablet	Enterprise	Yes
□	Rail Yatra	Google Play ...	com.sdl.app...	Smartphone, Tablet	Free	Yes

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'

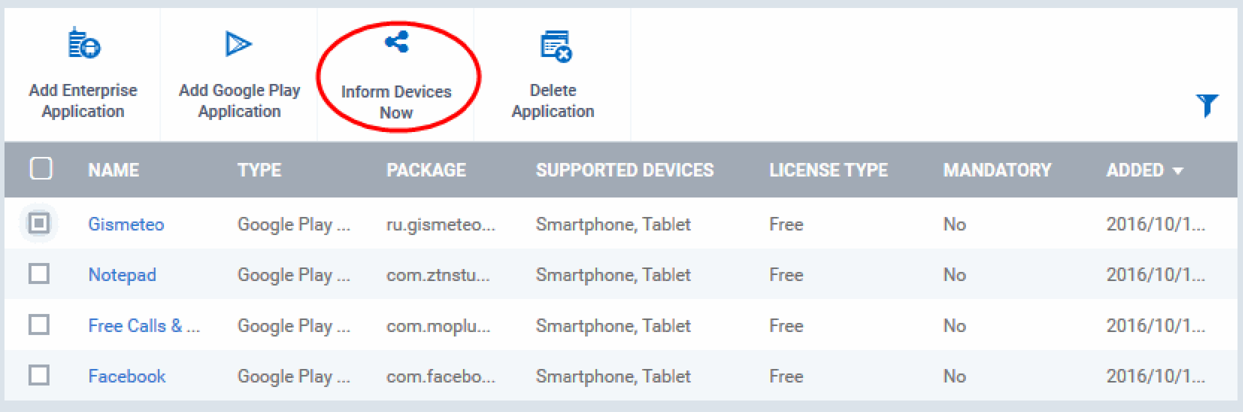
The file will be uploaded and the details will be auto-populated.

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.



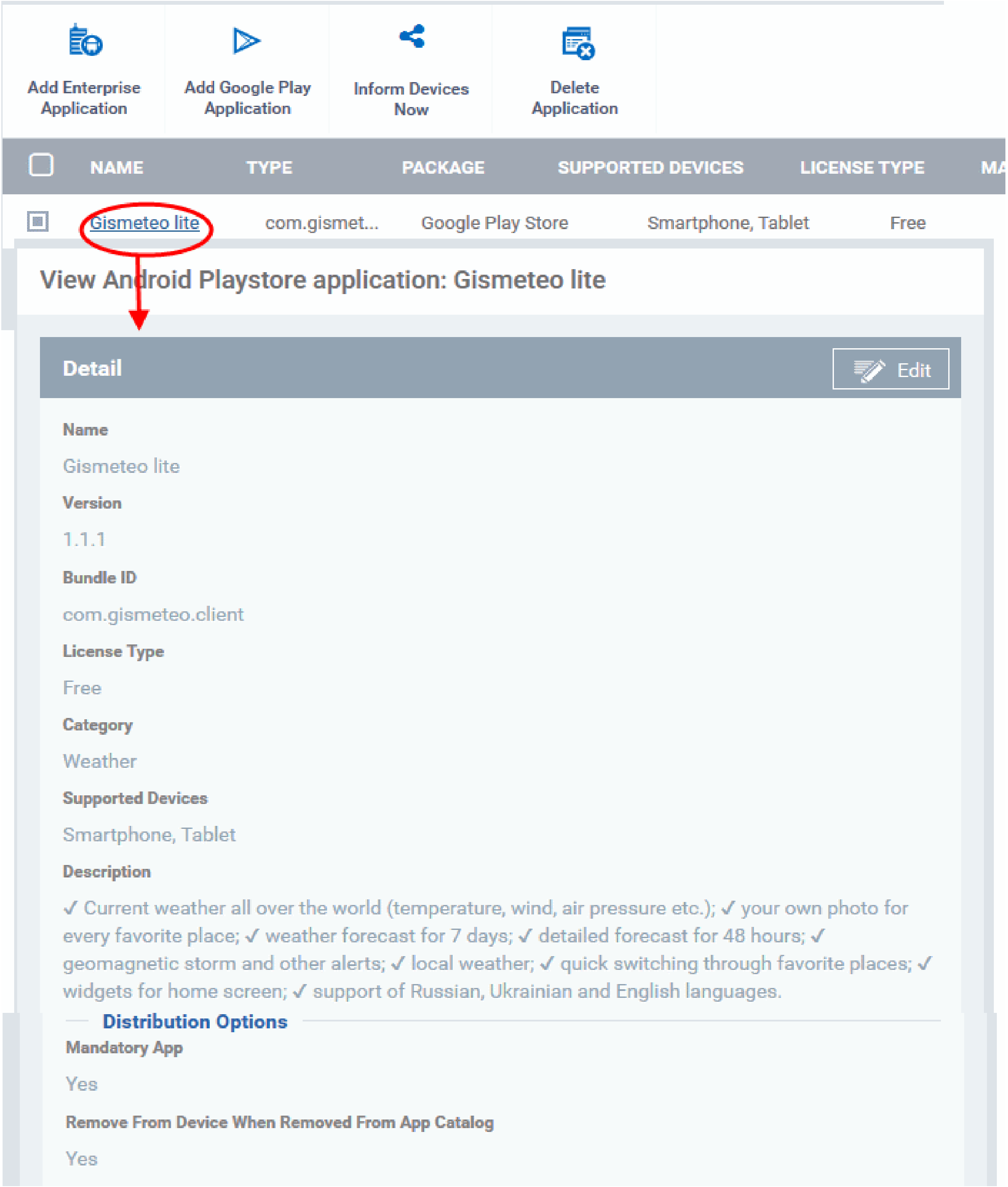
☐	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDATORY	ADDED
▣	Gismeteo	Google Play ...	ru.gismeteo...	Smartphone, Tablet	Free	No	2016/10/1...
☐	Notepad	Google Play ...	com.ztnstu...	Smartphone, Tablet	Free	No	2016/10/1...
☐	Free Calls & ...	Google Play ...	com.moplu...	Smartphone, Tablet	Free	No	2016/10/1...
☐	Facebook	Google Play ...	com.facebo...	Smartphone, Tablet	Free	No	2016/10/1...

8.2.2. Manage 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' on the left then choose 'Android Store'
- Click the name of the App



□	NAME	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MA
□	Gismeteo lite	com.gismet...	Google Play Store	Smartphone, Tablet	Free	

View Android Playstore application: Gismeteo lite

Detail

Name
Gismeteo lite

Version
1.1.1

Bundle ID
com.gismeteo.client

License Type
Free

Category
Weather

Supported Devices
Smartphone, Tablet

Description
✓ Current weather all over the world (temperature, wind, air pressure etc.); ✓ your own photo for every favorite place; ✓ weather forecast for 7 days; ✓ detailed forecast for 48 hours; ✓ geomagnetic storm and other alerts; ✓ local weather; ✓ quick switching through favorite places; ✓ widgets for home screen; ✓ support of Russian, Ukrainian and English languages.

Distribution Options

Mandatory App
Yes

Remove From Device When Removed From App Catalog
Yes

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 [Edit] at the top right .

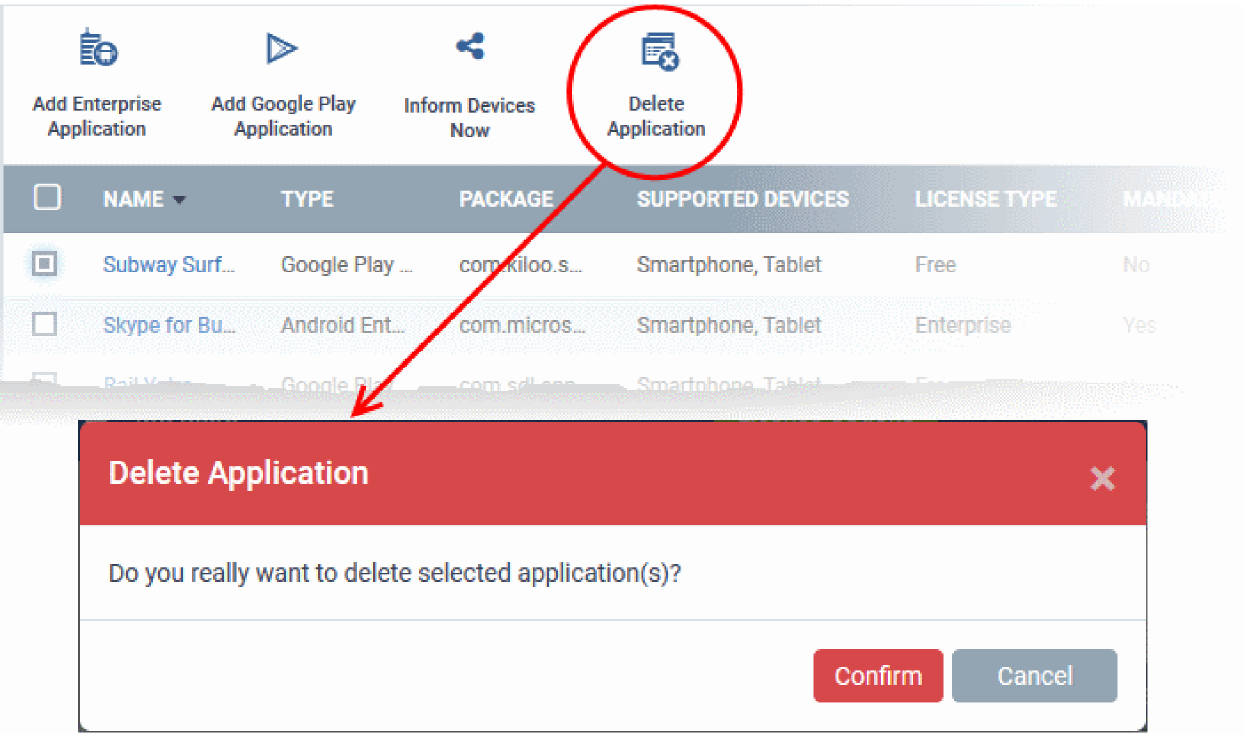
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section **Adding Android Apps and Installing them on Devices**.

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' on the left and choose 'Android Store'
- Select the App(s) to be removed and click 'Delete Application' from the options.



□	NAME ▾	TYPE	PACKAGE	SUPPORTED DEVICES	LICENSE TYPE	MANDA
▣	Subway Surf...	Google Play ...	com.kiloo.s...	Smartphone, Tablet	Free	No
□	Skype for Bu...	Android Ent...	com.micros...	Smartphone, Tablet	Enterprise	Yes

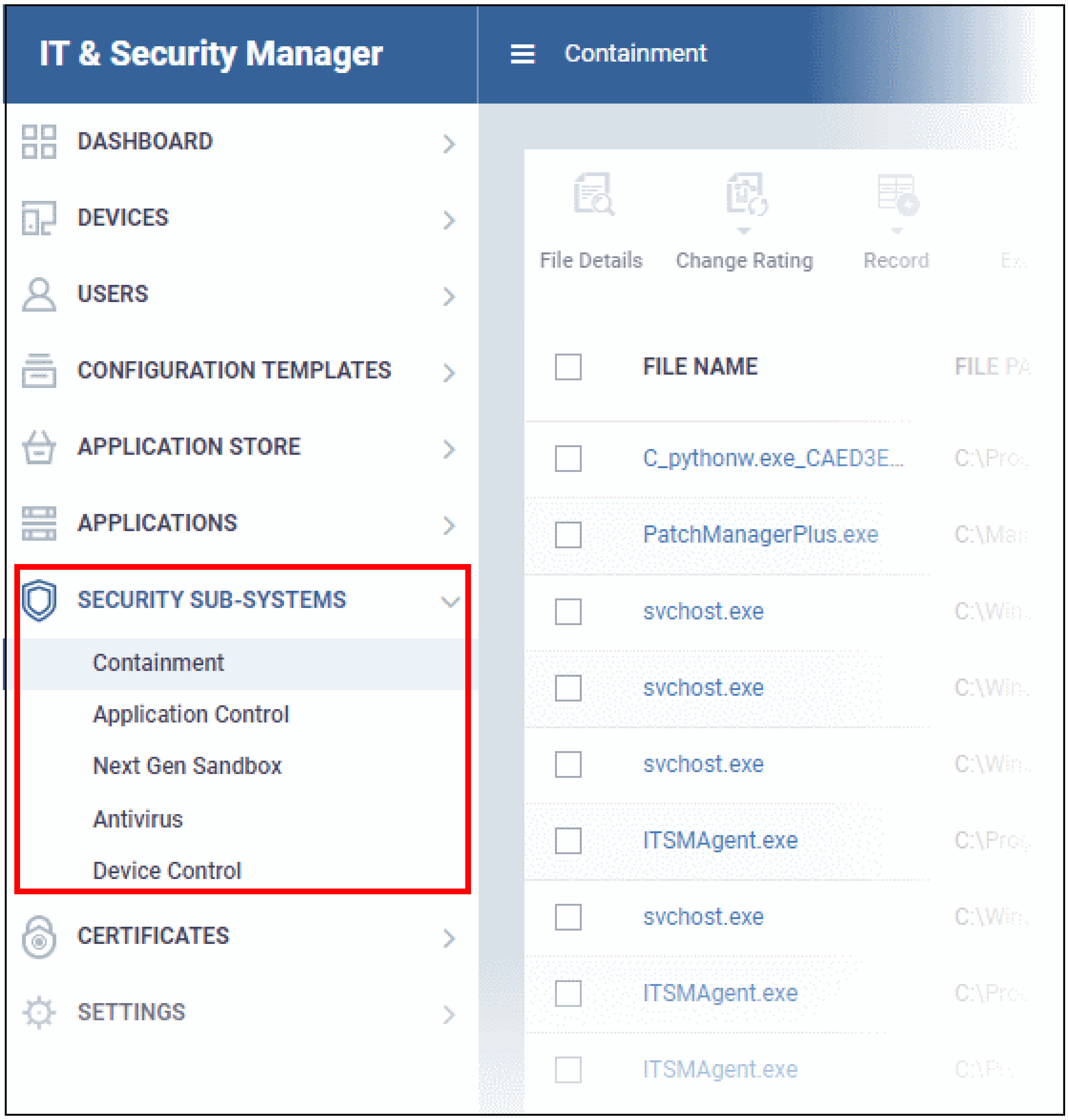
Delete Application ✕

Do you really want to delete selected application(s)?

9.Security Sub Systems

The 'Security Sub systems' menu allows admins to view the infection status of managed Android, Mac OS and Windows devices. You can also initiate on-demand virus and file rating scans and launch virus database updates. Admins can view a list of malware detected on devices and take appropriate actions against them. The interface also contains a history of threats identified. This area also allows administrators to:

- View the trust rating of applications and files discovered on managed Windows devices. These ratings are from the Comodo file look-up system. Admins can change a file's rating if required.
- View a list of unknown files which are currently running inside the container on the endpoint. Files may be automatically run in the container as a result of the profile applied to an endpoint, or manually run inside the container by the user.
- View a list of unknown files which were automatically submitted to Valkyrie for analysis.
- View and manage files that were moved to quarantine by CCS on Windows endpoints, and by CAVM on Mac OS endpoints.
- View a list of external connection attempts from devices. Connection attempts will be allowed or blocked per rules defined in the profiles applied to the device.



The following sections contain more details on each area:

- Viewing Contained Applications
- Manage File Trust Ratings on Windows Devices
- Viewing List of Valkyrie Analyzed Files
- Antivirus and File Rating scans
  - Running Antivirus and/or File Rating Scans on Devices
  - Handling Malware on Scanned Devices
  - Updating Virus Signature Database on Windows and Mac OS Devices
- Viewing and Managing Identified Malware
- Viewing and Managing Quarantined Items from Windows Devices
- Viewing and Managing Quarantined Items on Mac OS Devices
- Viewing Threats History
- Viewing History of External Device Connection Attempts

9.1. View Contained Applications

- The Containment module is a secure, isolated environment in which unknown/unrecognized files are run.
- Contained applications are not permitted to modify files, user data or other processes on the host machine.

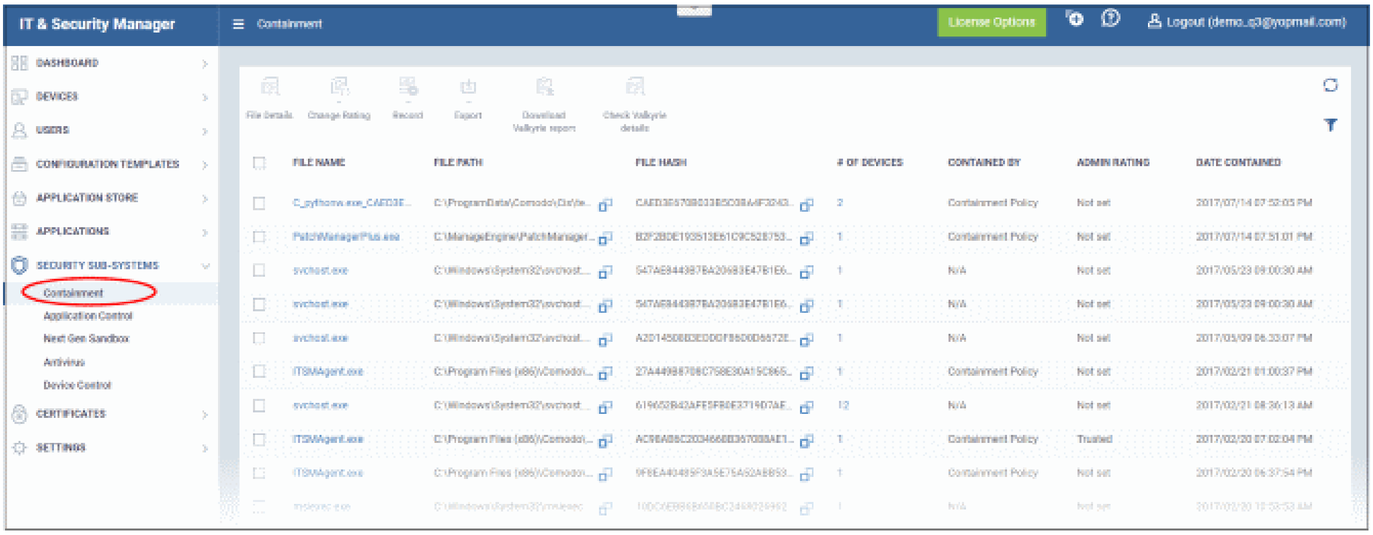
An application could be run inside the container because:

- It was auto-contained by rules in the ITSM configuration profile applied to the endpoint. See '**Containment Settings**' in **Creating Windows Profiles** for more details about containment rules in a profile.
- It was auto-contained by local Comodo Client Security rules on the endpoint
- The endpoint user ran the program inside the container on a 'one-off' basis. This can be helpful to test the behavior of new executables that have they downloaded.

Administrators can view all programs that ran inside the container from the 'Containment' interface. Admins can also view the activity of processes started by contained applications. Admins have the option to rate a contained file as trusted or malicious.

To open the 'Containment' file list interface:

- Click 'Security Sub-Systemss' on the left then 'Containment'



	FILE NAME	FILE PATH	FILE HASH	# OF DEVICES	CONTAINED BY	ADMIN RATING	DATE CONTAINED
□	C_pythonw.exe_CAFD3E...	C:\ProgramData\Comodo\Cis\te...	CAED3E570B033E5C08A4F3243...	2	Containment Policy	Not set	2017/07/14 07:52:05 PM
□	PatchManagerPlus.exe	C:\ManageEngine\PatchManager...	B2F2BDE193513E61C9C528753...	1	Containment Policy	Not set	2017/07/14 07:51:01 PM
□	svchost.exe	C:\Windows\System32\svchost...	547AE844387BA20683E47B1E6...	1	N/A	Not set	2017/05/23 09:00:30 AM
□	svchost.exe	C:\Windows\System32\svchost...	547AE844387BA20683E47B1E6...	1	N/A	Not set	2017/05/23 09:00:30 AM
□	svchost.exe	C:\Windows\System32\svchost...	A2D1450BD3EDDDF8600D6572E...	1	N/A	Not set	2017/05/09 06:33:07 PM
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	27A449B8708C758E30A15C865...	1	Containment Policy	Not set	2017/02/21 01:00:37 PM
□	svchost.exe	C:\Windows\System32\svchost...	619652B42AFE5FB0E3719D7AE...	12	N/A	Not set	2017/02/21 08:36:13 AM
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	AC9EAB8C2034668B367088AE1...	1	Containment Policy	Trusted	2017/02/20 07:02:04 PM
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	9F8EA40485F3A5E75A52AEB53...	1	Containment Policy	Not set	2017/02/20 06:37:54 PM
□	msiexec.exe	C:\Windows\System32\msiexec	100CXEB86B66BC2468029492	1	N/A	Not set	2017/02/20 10:53:53 AM

Containment - Column Descriptions	
Column Heading	**Description**
File Name	The name of the contained executable file. • Click the name of a file to view its details. • See **View details of a contained application** for more details.
File Path	The location of the contained file on the local endpoint. • Click the ⧉ icon to copy the path to the clipboard.
File Hash	SHA1 hash value of the file. • Click the ⧉ icon to copy the hash value to the clipboard.
Number of Devices	The quantity of endpoints on which the item was identified. • Click the number to view a list of endpoints on which the item was found. • This also allows you to view the activities of processes started by the item. For more details, see **Device List Screen** below.

Contained By	The reason the file was contained.
Action	The permission level at which the file was executed in the container, or the action that was taken upon it. The possible values are: • Restricted - The file was run inside the container but had limited access to the operating system resources. • Virtually - The file was completely isolated from the operating system and files on the computer. • Blocked - The file was not allowed to run at all. • Ignored - The file was allowed to run outside the container without any restrictions. • Unknown - The containment status was not determined.
Status	The execution state of the file inside the container. The possible values are: • Running • Complete • Failed
Admin Rating	The trust rating of the file as set by the administrator. Files can be rated as trusted, malicious or unrecognized.
Date Contained	Date and time the file ran in the contained environment.
Controls	
File Details	View full details of the contained file including the devices on which it was contained and its activity.
Change Rating	You can change the rating of the contained file as trusted, malicious malicious or unrecognized.
Record	Hide or delete a contained file record from the list.
Export	Export the list of contained files to a .csv file. The exported file can be viewed in 'Dashboard' > 'Reports'.
Download Valkyrie report	Valkyrie is Comodo's advanced file analysis and verdicting system. Each report contains an in-depth breakdown on the activity an unknown file, along with an overall verdict on its trustworthiness.
Check Valkyrie details	View Valkyrie file analysis of the contained file at **https://valkyrie.comodo.com**

- Click any column header to sort items in ascending/descending order of entries in that column.
- Click the funnel icon on the right to search for contained applications by name, file path, SHA1 file hash, admin rating, action, status and/or execution date.
- To display all the items again, remove / deselect the search key from filter 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 and choose the number.

Manage Contained Items

The 'Containment' interface allows you to:

- View details of a contained application
- Rate the files
- Hide / Unhide / Delete records
- Export file records as CSV file
- Download Valkyrie report
- View Valkyrie fie analysis report online

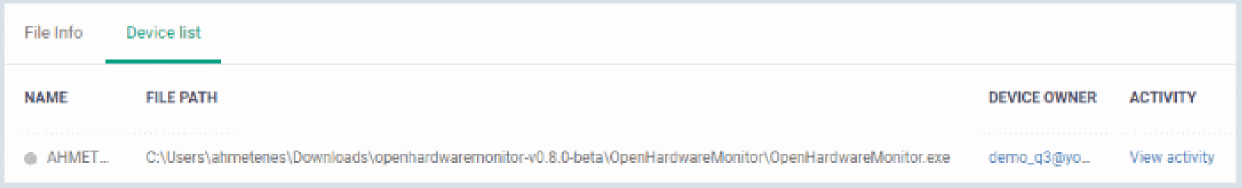
View details of a contained application

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file-name in the list OR select a file and click 'File Details'
- This will open the file details interface which shows:
    - **File Info** - General information such as file-name, path, age, hash and file-size.
    - **Device List** - Shows endpoints upon which the file was found. This tab also tells you the device owner and lists any activities by the file. The next sections contain more info on these items:

Device List Screen

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file-name in the list OR select a file and click 'File Details'
- Click the 'Device List' tab

The 'Device List' shows endpoints on which the file was discovered and its activities. Admins can view processes executed by the file with details on data handled by each process.



NAME	FILE PATH	DEVICE OWNER	ACTIVITY
● AHMET...	C:\Users\ahmetenes\Downloads\openhardwaremonitor-v0.8.0-beta\OpenHardwareMonitor\OpenHardwareMonitor.exe	demo_q3@yo...	View activity

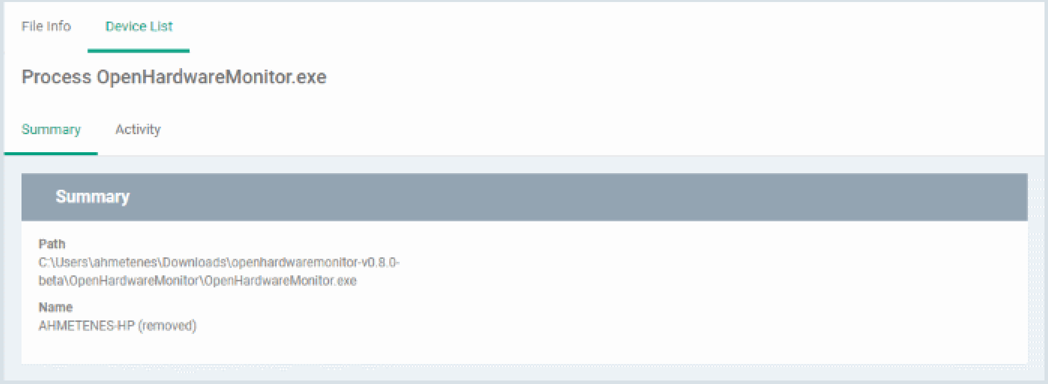
View File Activities on Endpoints

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file-name in the list OR select a file and click 'File Details'
- Click the 'Device List' tab
- Click the 'View Activity' link

Note: VirusScope must be enabled in the profile in effect on the endpoint for ITSM to collect file activity data. See **Configuring VirusScope Settings** in **Creating Windows Profiles** for more details.

The 'Process Activity' interface will open. It has two tabs.

- **Summary** - Shows basic file activity details



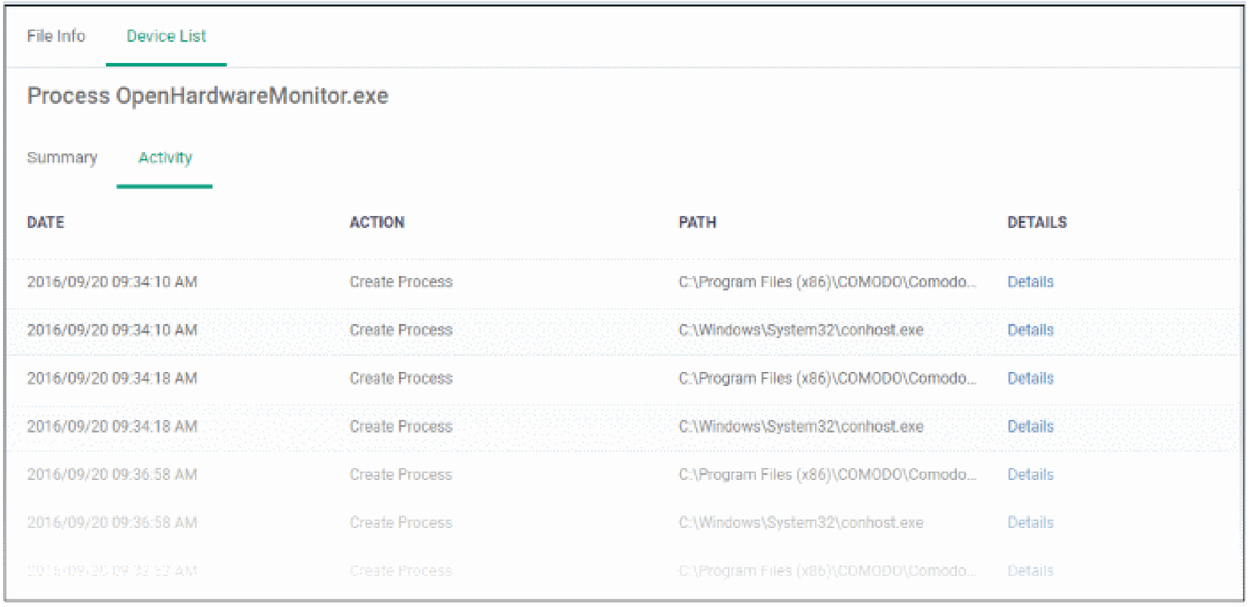
Process OpenHardwareMonitor.exe

Summary

Path
C:\Users\ahmetenes\Downloads\openhardwaremonitor-v0.8.0-beta\OpenHardwareMonitor\OpenHardwareMonitor.exe

Name
AHMETENES-HP (removed)

- **Activity** - Lists all processes executed by the files in chronological order:

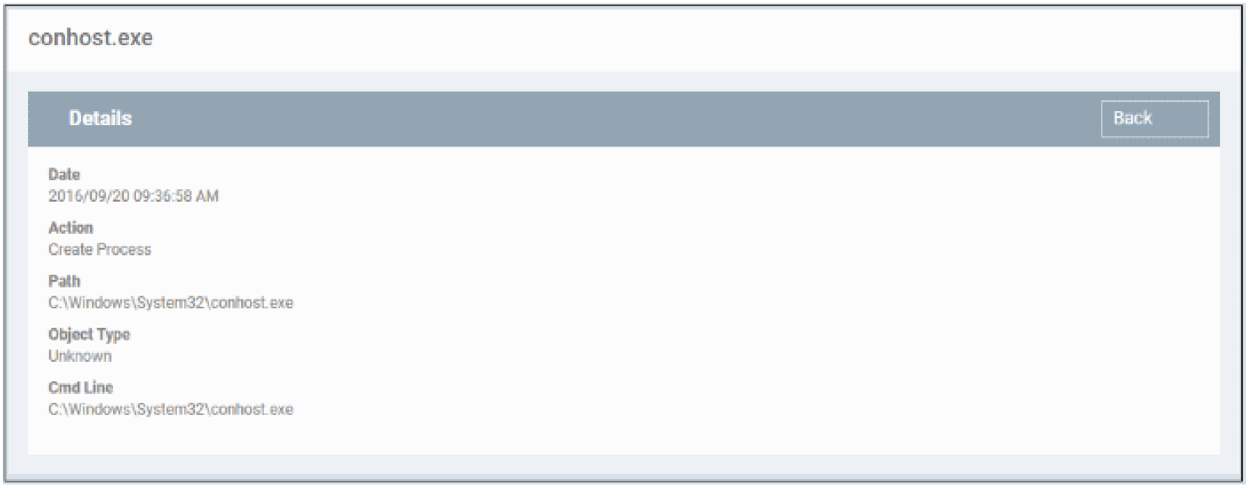


Process OpenHardwareMonitor.exe

DATE	ACTION	PATH	DETAILS
2016/09/20 09:34:10 AM	Create Process	C:\Program Files (x86)\COMODO\Comodo...	Details
2016/09/20 09:34:10 AM	Create Process	C:\Windows\System32\conhost.exe	Details
2016/09/20 09:34:18 AM	Create Process	C:\Program Files (x86)\COMODO\Comodo...	Details
2016/09/20 09:34:18 AM	Create Process	C:\Windows\System32\conhost.exe	Details
2016/09/20 09:36:58 AM	Create Process	C:\Program Files (x86)\COMODO\Comodo...	Details
2016/09/20 09:36:58 AM	Create Process	C:\Windows\System32\conhost.exe	Details
2016/09/20 09:32:52 AM	Create Process	C:\Program Files (x86)\COMODO\Comodo...	Details

The 'Activity' - Table of Column Descriptions	
Column Heading	**Description**
Date	Date and time the process was executed
Action	Task that was executed by the file
Path	Location of the file affected by the action
Details	View more information about the action

- To view the details of an activity, click the 'Details' link under the 'Details' column



conhost.exe

Date
2016/09/20 09:36:58 AM

Action
Create Process

Path
C:\Windows\System32\conhost.exe

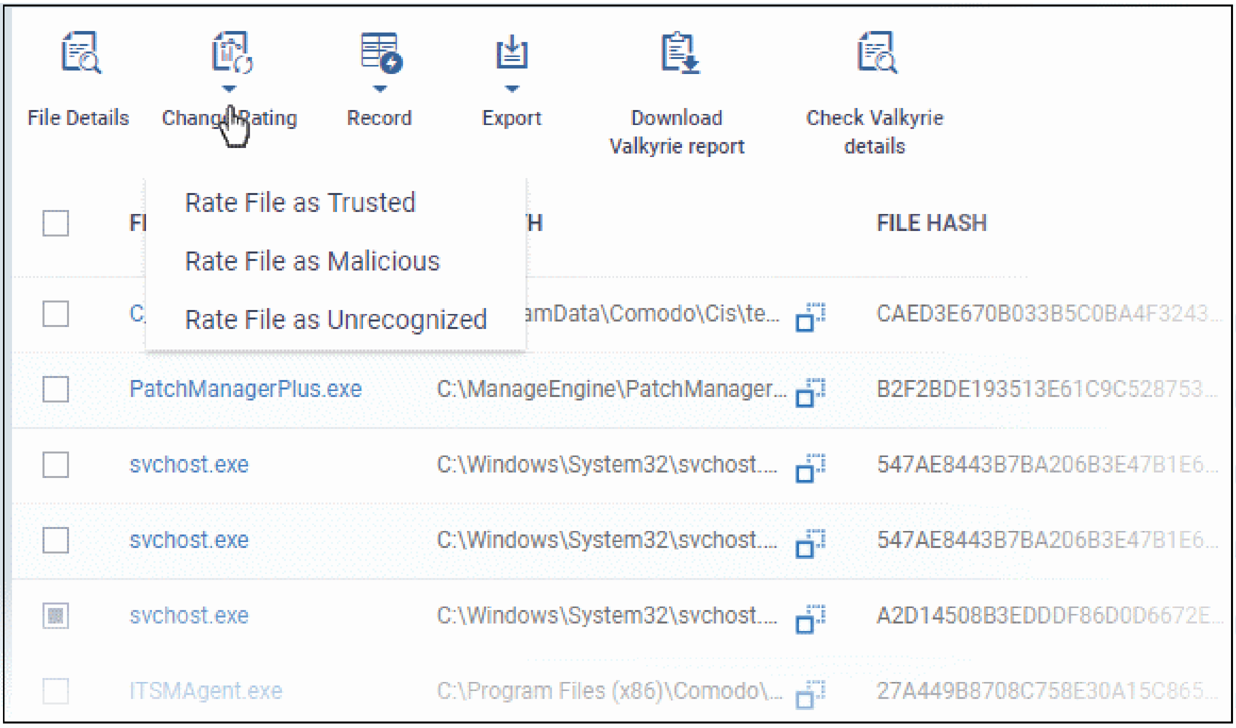
Object Type
Unknown

Cmd Line
C:\Windows\System32\conhost.exe

Rate files as trusted / malicious

If required, admins can rate contained files as unrecognized, trusted or malicious. Please make sure before marking a file as trusted. Any new file ratings will be sent to endpoints during the next sync.

- Click 'Security Sub-Systems' > 'Containment'
- Select the file(s) whose rating you wish to change
- Click the 'Change Rating' button
- Set your preferred rating from the options:



	FI	H		FILE HASH
□	C.	amData\Comodo\Cis\te...		CAED3E670B033B5C0BA4F3243...
□	PatchManagerPlus.exe	C:\ManageEngine\PatchManager...		B2F2BDE193513E61C9C528753...
□	svchost.exe	C:\Windows\System32\svchost....		547AE8443B7BA206B3E47B1E6...
□	svchost.exe	C:\Windows\System32\svchost....		547AE8443B7BA206B3E47B1E6...
▣	svchost.exe	C:\Windows\System32\svchost....		A2D14508B3EDDDF86D0D6672E...
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...		27A449B8708C758E30A15C865...

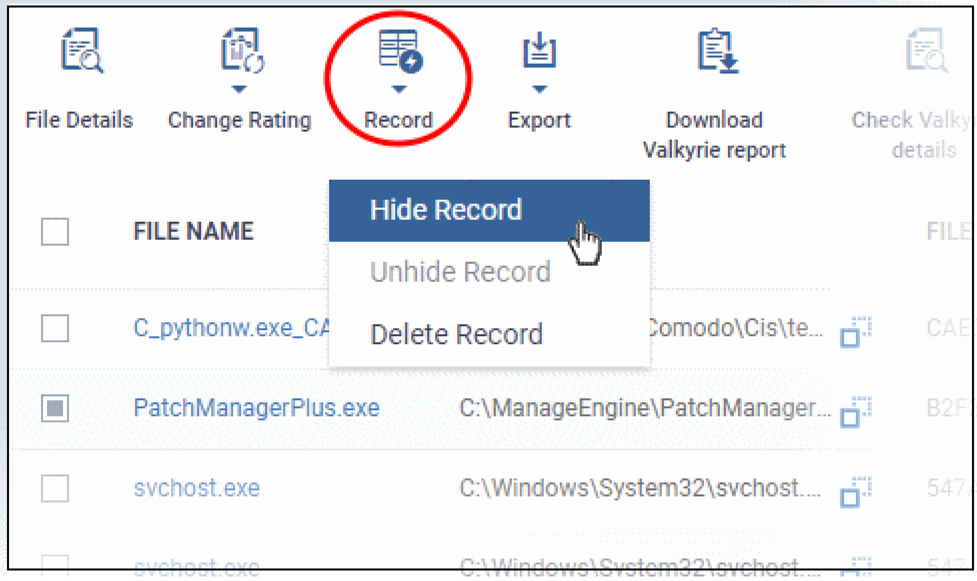
The new rating will be propagated to all endpoints during the next synchronization.

Hide / unhide / remove files from the list

The 'Record' button at the top allows you to change the visibility of file records and also to remove files from the list.

To hide a file record

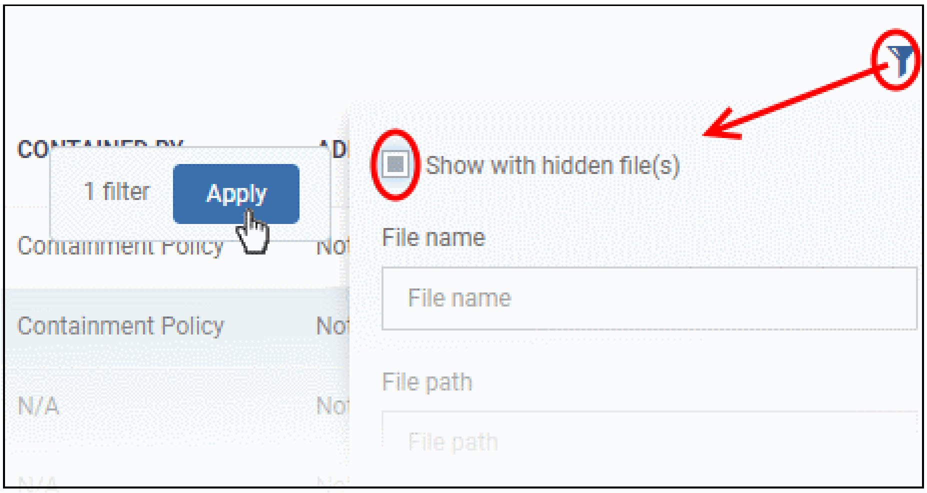
- Select a file, click 'Record' at the top and select 'Hide' from the options



The file will no longer will be displayed in the list. Please note you can hide multiple files at a time.

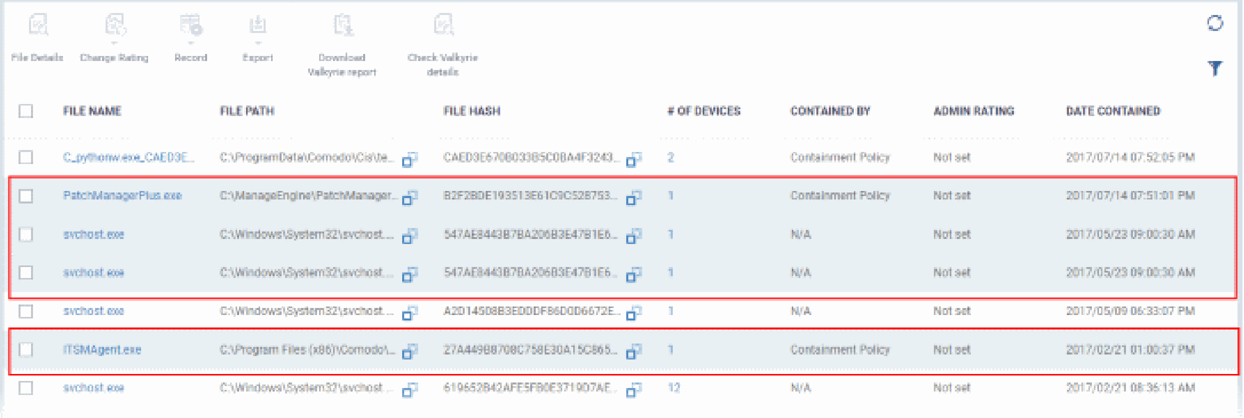
To unhide file records

- First click the filter icon, select 'Show with hidden file(s)'



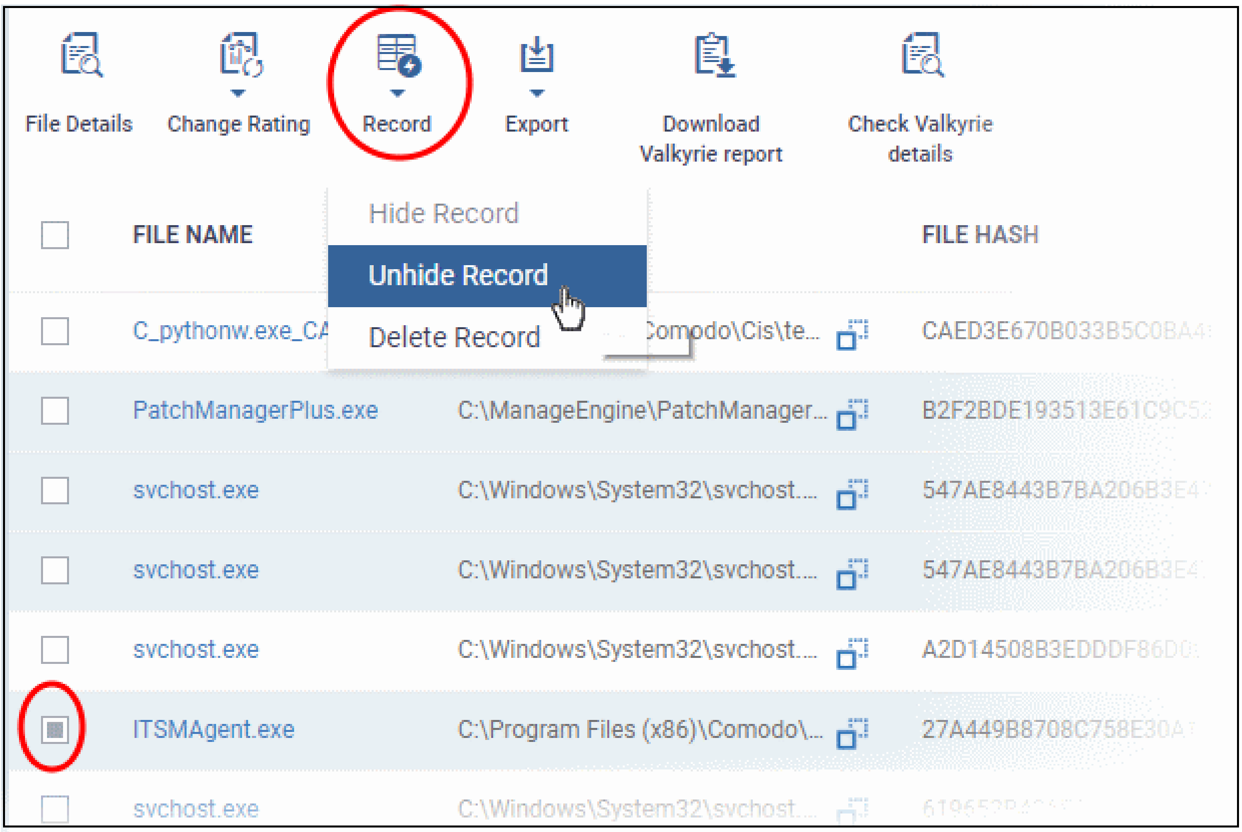
- Click 'Apply'

The hidden file records will now be visible and highlighted.



	FILE NAME	FILE PATH	FILE HASH	# OF DEVICES	CONTAINED BY	ADMIN RATING	DATE CONTAINED
□	C_pythonw.exe_CAED3E...	C:\ProgramData\Comodo\Cis\te...	CAED3E670B033B5C0BA4F3243...	2	Containment Policy	Not set	2017/07/14 07:52:05 PM
□	PatchManagerPlus.exe	C:\ManageEngine\PatchManager...	B2F2BDE193513E61C9C528753...	1	Containment Policy	Not set	2017/07/14 07:51:01 PM
□	svchost.exe	C:\Windows\System32\svchost....	547AE8443B7BA206B3E47B1E6...	1	N/A	Not set	2017/05/23 09:00:30 AM
□	svchost.exe	C:\Windows\System32\svchost....	547AE8443B7BA206B3E47B1E6...	1	N/A	Not set	2017/05/23 09:00:30 AM
□	svchost.exe	C:\Windows\System32\svchost....	A2D14508B3EDDDF86D0D6672E...	1	N/A	Not set	2017/05/09 06:33:07 PM
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	27A449B8708C758E30A15C865...	1	Containment Policy	Not set	2017/02/21 01:00:37 PM
□	svchost.exe	C:\Windows\System32\svchost....	619652B42AFE5FB0E37190 7AE...	12	N/A	Not set	2017/02/21 08:36:13 AM

- Select the file(s) that you want to unhide, click 'Record' at the top then 'Unhide' from the options.

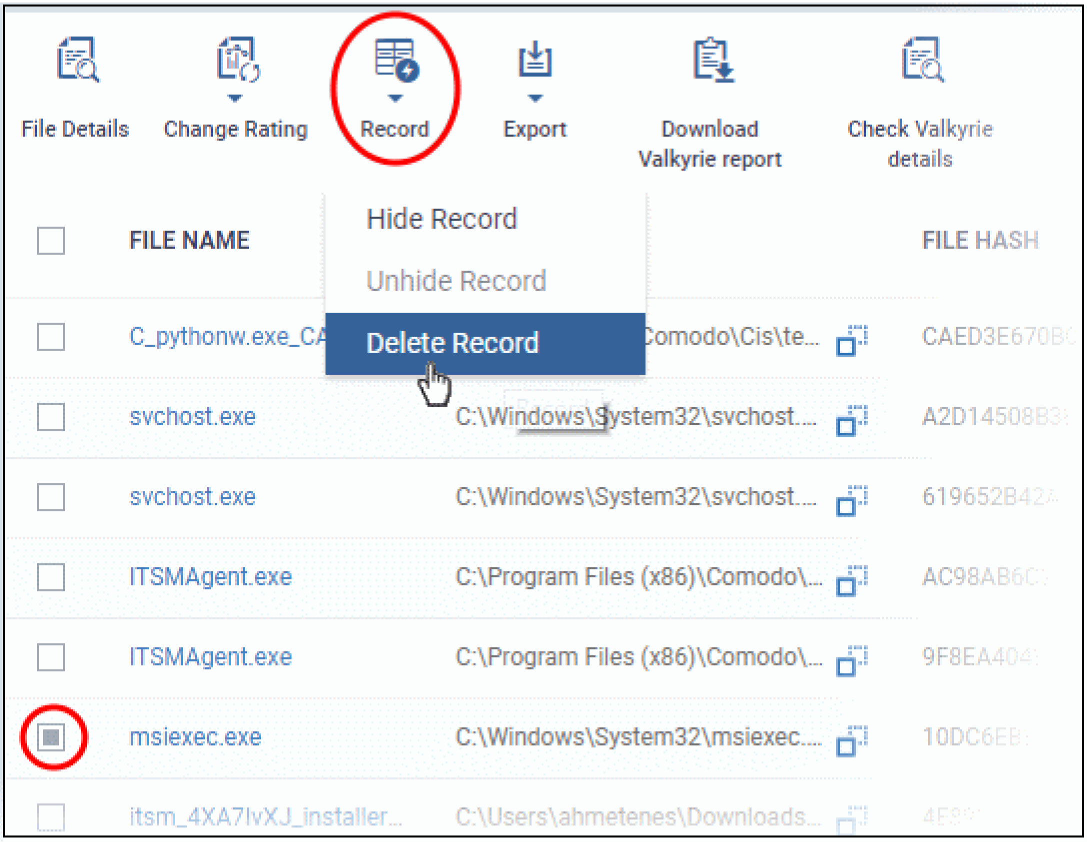


	FILE NAME		FILE HASH
□	C_pythonw.exe_CA	...Comodo\Cis\te...	CAED3E670B033B5C0BA4
□	PatchManagerPlus.exe	C:\ManageEngine\PatchManager...	B2F2BDE193513E61C9C52
□	svchost.exe	C:\Windows\System32\svchost....	547AE8443B7BA206B3E4
□	svchost.exe	C:\Windows\System32\svchost....	547AE8443B7BA206B3E4
□	svchost.exe	C:\Windows\System32\svchost....	A2D14508B3EDDDF86D0
■	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	27A449B8708C758E30A
□	svchost.exe	C:\Windows\System32\svchost....	619652B4

The selected hidden file records will now be visible.

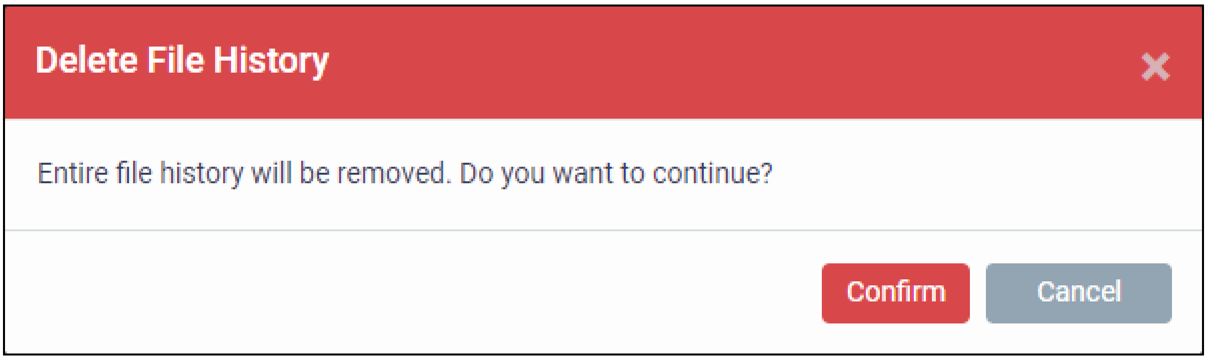
To remove file records

- To delete item(s), select from the list, click 'Record' at the top then 'Delete Record' from the options



	FILE NAME		FILE HASH
□	C_pythonw.exe_CA	omodo\Cis\te...	CAED3E670BC
□	svchost.exe	C:\Windows\System32\svchost....	A2D14508B3
□	svchost.exe	C:\Windows\System32\svchost....	619652B42A
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	AC98AB6C
□	ITSMAgent.exe	C:\Program Files (x86)\Comodo\...	9F8EA404
☑	msiexec.exe	C:\Windows\System32\msiexec....	10DC6EB
□	itsm_4XA7lvXJ_installer...	C:\Users\ahmetenes\Downloads...	4E8

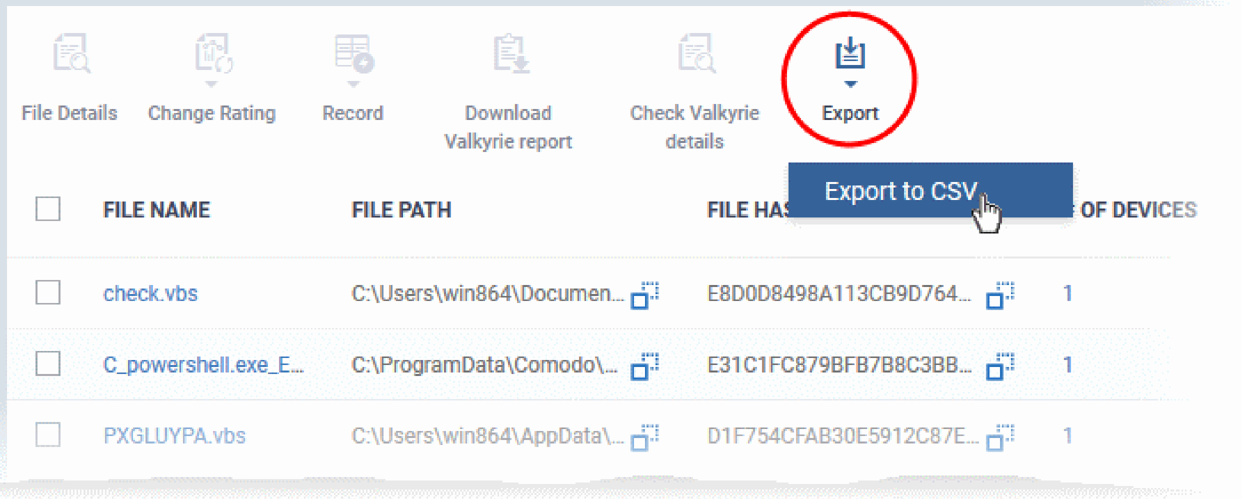
- Click 'Confirm' in the confirmation dialog to remove the item(s) from the 'Containment' interface.


Delete File History

Entire file history will be removed. Do you want to continue?

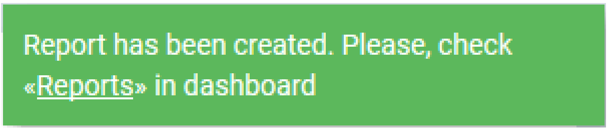
Export file records as a CSV file

- Click 'Security Sub-Systems' > 'Containment'
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



□	FILE NAME	FILE PATH	FILE HAS	OF DEVICES
□	check.vbs	C:\Users\win864\Documen...	E8D0D8498A113CB9D764...	1
□	C_powershell.exe_E...	C:\ProgramData\Comodo\...	E31C1FC879BFB7B8C3BB...	1
□	PXGLUYPA.vbs	C:\Users\win864\AppData\...	D1F754CFAB30E5912C87E...	1

The report will be generated in .csv file format.



Report has been created. Please, check «Reports» in dashboard

You can access the report in the 'Dashboard' > 'Reports' interface. See **Reports** if you need more help with this interface.

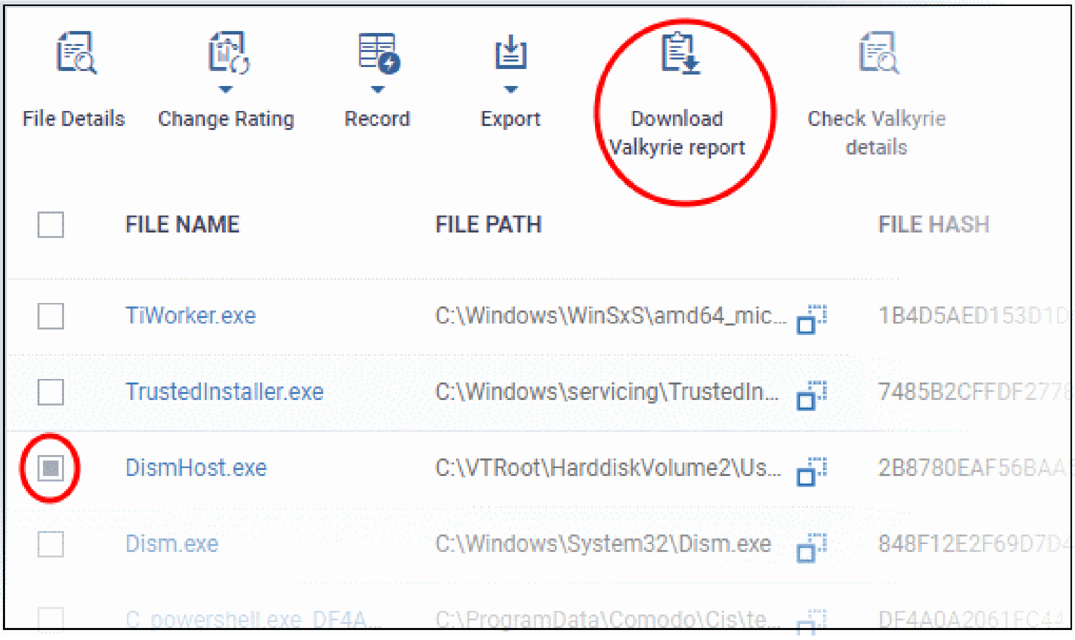
Valkyrie Reports

Files running in the container are analyzed and rated by Comodo's behavior analysis system, Valkyrie. Valkyrie tests unknown files with a range of static and dynamic behavioral checks to identify whether they are malicious or safe.

You can view the file rating in the '**Application Control**' interface also. You can download a Valkyrie report or view it online at **https://valkyrie.comodo.com/**

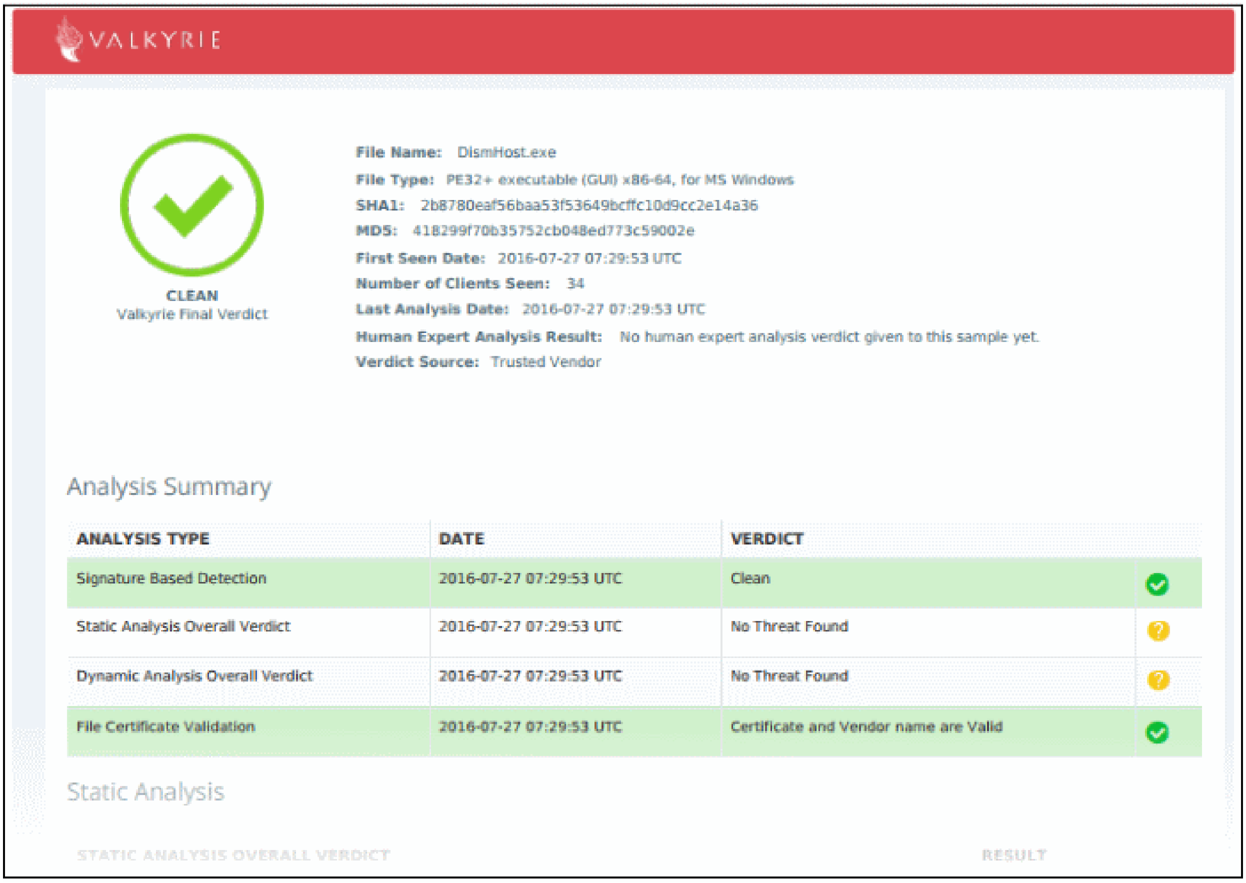
Download Valkyrie report

- Click 'Security Sub-Systems' > 'Containment'
- Select any file
- Click 'Download Valkyrie report':



	FILE NAME	FILE PATH	FILE HASH
□	TiWorker.exe	C:\Windows\WinSxS\amd64_mic...	1B4D5AED153D1D
□	TrustedInstaller.exe	C:\Windows\servicing\TrustedIn...	7485B2CFFDF2778
☒	DismHost.exe	C:\VTRoot\HarddiskVolume2\Us...	2B8780EAF56BAA
□	Dism.exe	C:\Windows\System32\Dism.exe	848F12E2F69D7D
□	C_powershell.exe_DF4A...	C:\ProgramData\Comodo\Cis\te...	DF4A0A2061FC44

This will open the Valkyrie report on the contained file in PDF format:



File Name: DismHost.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 2b8780eaf56baa53f53649bcffc10d9cc2e14a36
MD5: 418299f70b35752cb048ed773c59002e
First Seen Date: 2016-07-27 07:29:53 UTC
Number of Clients Seen: 34
Last Analysis Date: 2016-07-27 07:29:53 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Trusted Vendor

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-07-27 07:29:53 UTC	Clean	✓
Static Analysis Overall Verdict	2016-07-27 07:29:53 UTC	No Threat Found	?
Dynamic Analysis Overall Verdict	2016-07-27 07:29:53 UTC	No Threat Found	?
File Certificate Validation	2016-07-27 07:29:53 UTC	Certificate and Vendor name are Valid	✓

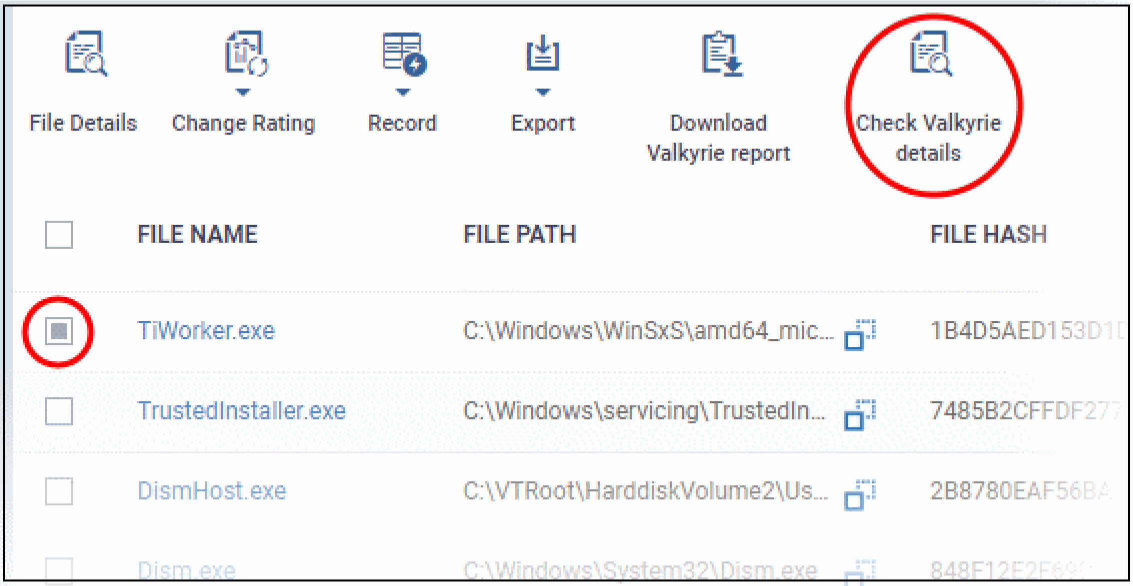
Static Analysis

STATIC ANALYSIS OVERALL VERDICT RESULT

You can also download and view the report at https://valkyrie.comodo.com/ after signing into your Valkyrie account.

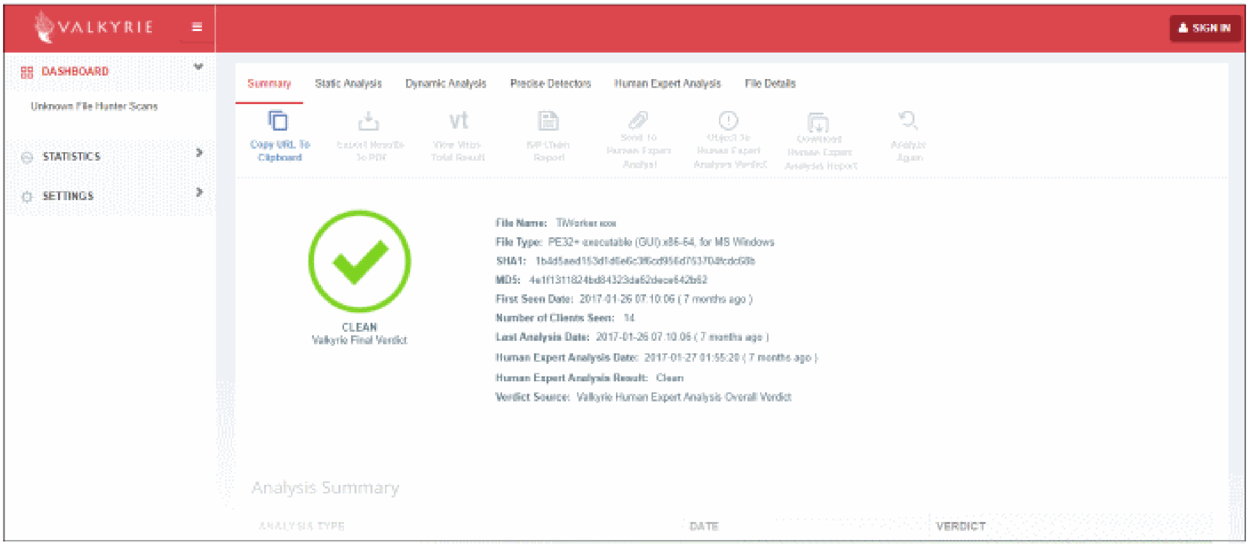
View Valkyrie fie analysis report online

- Select the file from the list and click 'Check Valkyrie Details' at the top.



	FILE NAME	FILE PATH	FILE HASH
☒	TiWorker.exe	C:\Windows\WinSxS\amd64_mic...	1B4D5AED153D1
□	TrustedInstaller.exe	C:\Windows\servicing\TrustedIn...	7485B2CFFDF27
□	DismHost.exe	C:\VTRoot\HarddiskVolume2\Us...	2B8780EAF56BA
□	Dism.exe	C:\Windows\System32\Dism.exe	848F12E2F69

You will be taken to the report summary page of the selected file at **https://valkyrie.comodo.com/**.



File Name: TiWorker.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 1b4d5aed153d1d6e6c3f6cd956d753704fcdc68b
MD5: 4e1f1311824bd84323da62deca642b62
First Seen Date: 2017-01-26 07:10:06 (7 months ago)
Number of Clients Seen: 14
Last Analysis Date: 2017-01-26 07:10:06 (7 months ago)
Human Expert Analysis Date: 2017-01-27 01:55:20 (7 months ago)
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

- View a more detailed version of the Valkyrie analysis by logging in at **https://valkyrie.comodo.com/**. You can use your Comodo One username and password to login.
- See **https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html** for help to use the Valkyrie online portal.

9.2. Manage File Trust Ratings on Windows Devices

- Click 'Security Sub-Systems' > 'Application Control' to open the 'Application Control' interface.
- Comodo Client Security (CCS) monitors all file activity on Windows devices. Every new executable is scanned against the Comodo white and blacklists then awarded a rating of '**Unrecognized**', '**Trusted**' or '**Malicious**'.
- Files that have a rating of 'Unrecognized' or 'Malicious' are reported to the 'Application Control' interface. Admins can change the rating of a file as required.
- You can configure file analysis in the 'File Rating settings' section of the configuration profile applied to the device. See **File Rating settings** in **Creating a Windows Profile** for more details.

- See **File Ratings Explained** for background information on file ratings.

The Application Control Interface

The 'Application Control' interface lets you view the trust rating of files on an endpoint. Possible ratings are 'Unrecognized', 'Trusted' or 'Malicious', with 'Unrecognized' and 'Malicious' files being reported to this interface. You can manually set the rating of a file at your discretion.

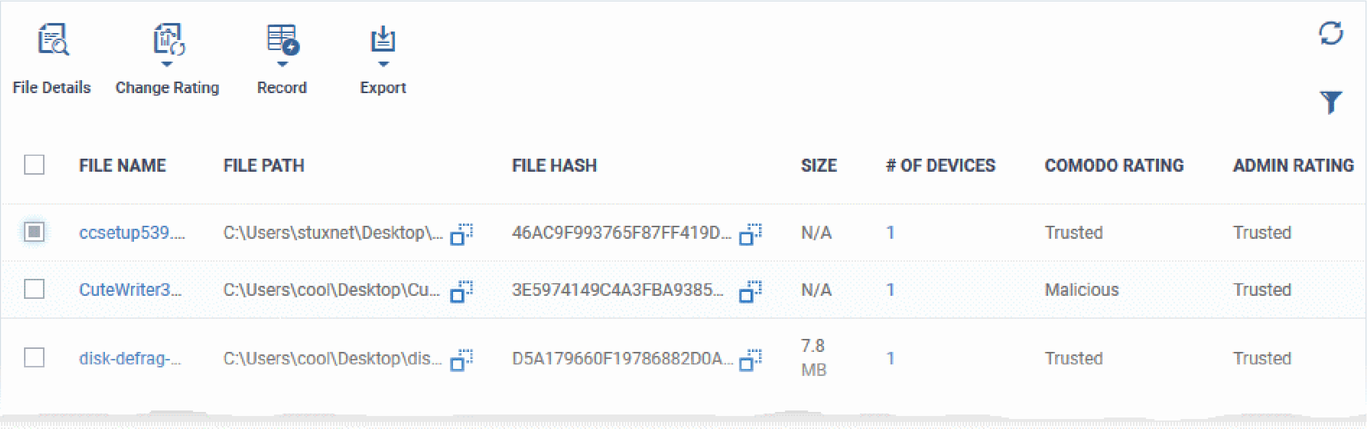
- Files rated as 'Trusted' are allowed to run as normal on the endpoint.
- Files rated as 'Malicious' are quarantined and not allowed to run.
- Files rated as 'Unrecognized' are run inside the container - an isolated operating environment. Contained applications are not permitted to access files or user data on the host machine.

Any rating you set for a file is pushed to all managed endpoints on which the file is installed.

- You can also view a history of purged files. Purged files are those which existed on devices at one point in time, but are not currently present on any device.
- Apply the 'Show Purged Files' filter to view these files. See the explanation of **Filter Options** below.

You can also hide items as required.

- Click 'Security Sub-Systems' > Application Control' to open the application control interface:



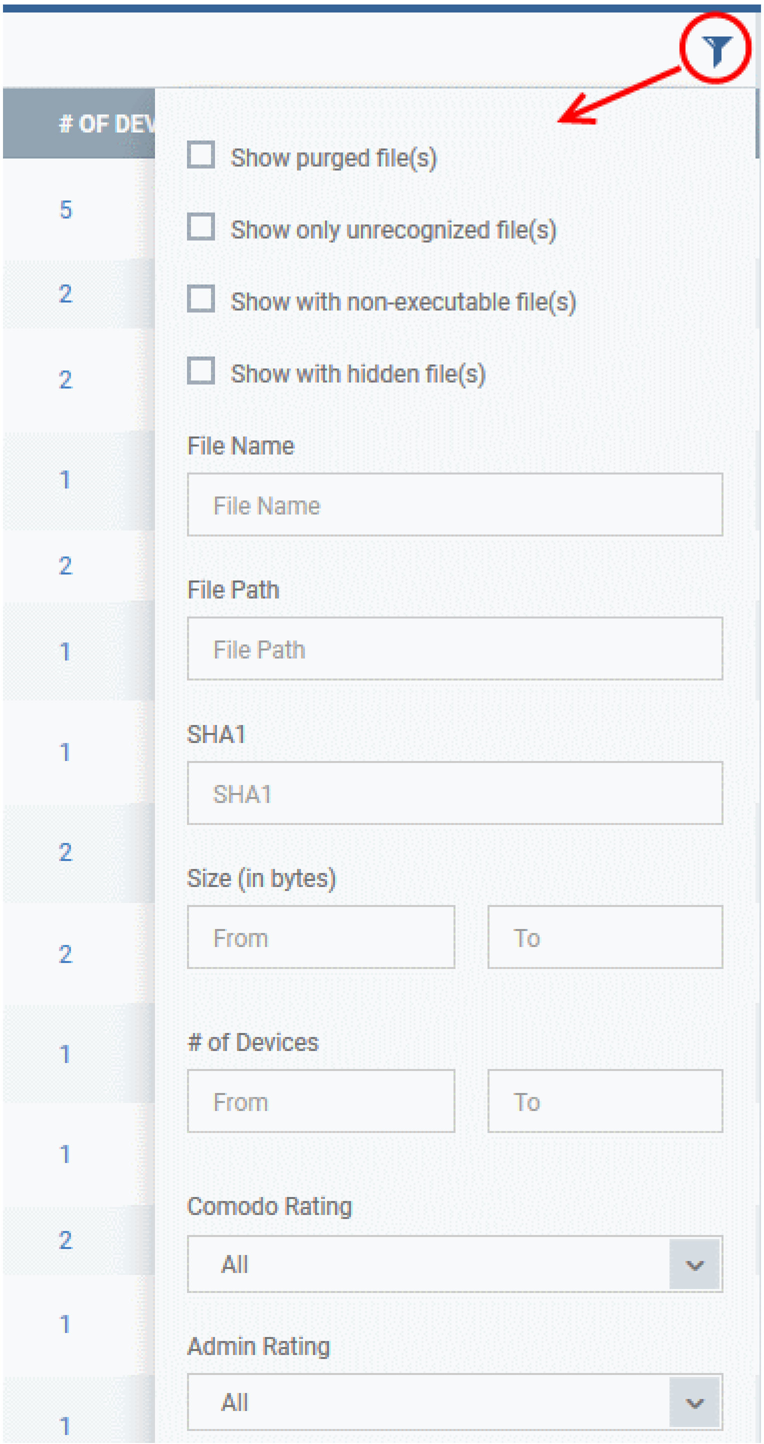
□	FILE NAME	FILE PATH	FILE HASH	SIZE	# OF DEVICES	COMODO RATING	ADMIN RATING
☒	ccsetup539....	C:\Users\stuxnet\Desktop\...	46AC9F993765F87FF419D...	N/A	1	Trusted	Trusted
□	CuteWriter3...	C:\Users\cool\Desktop\Cu...	3E5974149C4A3FBA9385...	N/A	1	Malicious	Trusted
□	disk-defrag-...	C:\Users\cool\Desktop\dis...	D5A179660F19786882D0A...	7.8 MB	1	Trusted	Trusted

Application Control - Table of Column Descriptions	
Column Heading	**Description**
File Name	The label of the application/executable file. • Click the name of a file to view its details. • See **View file details** given below for more details.
File Path	The installation location of the application on the endpoint. • Click the ⧉ icon to copy the path to the clipboard.
File Hash	The SHA1 hash value of the executable file. • Click the ⧉ icon to copy the hash value to the clipboard.
Size	The size of the executable file.
# of Devices	The number of endpoints on which the item was found. • Click the number to view the 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.
Comodo Rating	The rating of the file as per the Comodo File Look-up service, reported by the CCS installations at the endpoints. See **File Ratings Explained** for more details.
Admin Rating	Indicates the rating of the file as manually set by the administrator, if any.

Sorting, Search and Filter Options

- Click any column header to sort items in alphabetical order
- Click the funnel icon to open more filter options:



□ Show purged file(s)

□ Show only unrecognized file(s)

□ Show with non-executable file(s)

□ Show with hidden file(s)

File Name: File Name

File Path: File Path

SHA1: SHA1

Size (in bytes): From To

# of Devices: From To

Comodo Rating: All

Admin Rating: All

- Use the check-boxes to show or hide purged, non-executable, hidden or unrecognized files.
- Use the search fields to filter by file name, file path or SHA1 hash value. You can also filter by file size and the number of devices on which the file is present.
- Use the drop-down boxes to filter items by Comodo and/or Admin rating
- To display all items again, clear any search filters and click 'OK'.

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

Manage Applications

The Applications Control interface allows you to:

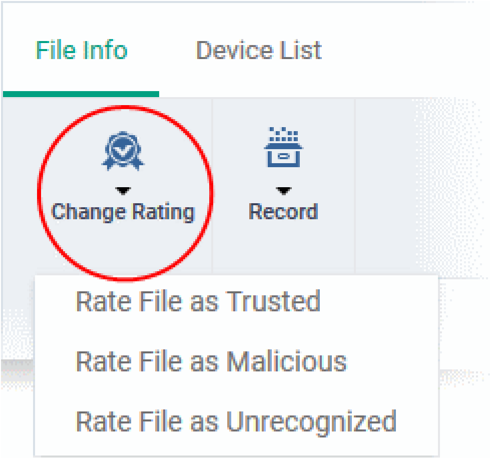
- View the details of files in the list
- View Process Activities of a File
- Assign Admin rating to a file
- Hide/Display selected files in the list
- Export the list of selected files to a CSV file
- Remove files from the list

View file details

- Simply click on a file in the list or select a file and click 'File Details' at the top. The 'file info' screen shows basic file details and the devices on which the file is present. You can also change the trust rating of the file in this area.

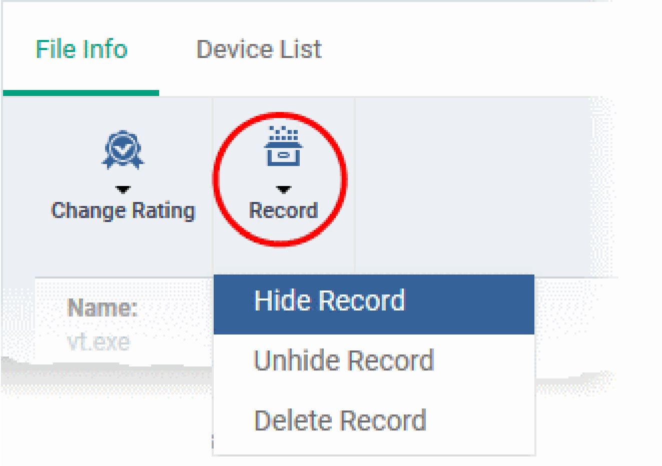
File information

- The file info screen shows file name, installation path, file type, version, size, hash values and the date the file was first encountered. The screen also shows the file's trust rating and the number of endpoints on which the file is present.
- The 'Change Rating' button allows you to manually set the file's rating as 'Trusted', 'Malicious' or 'Unrecognized':



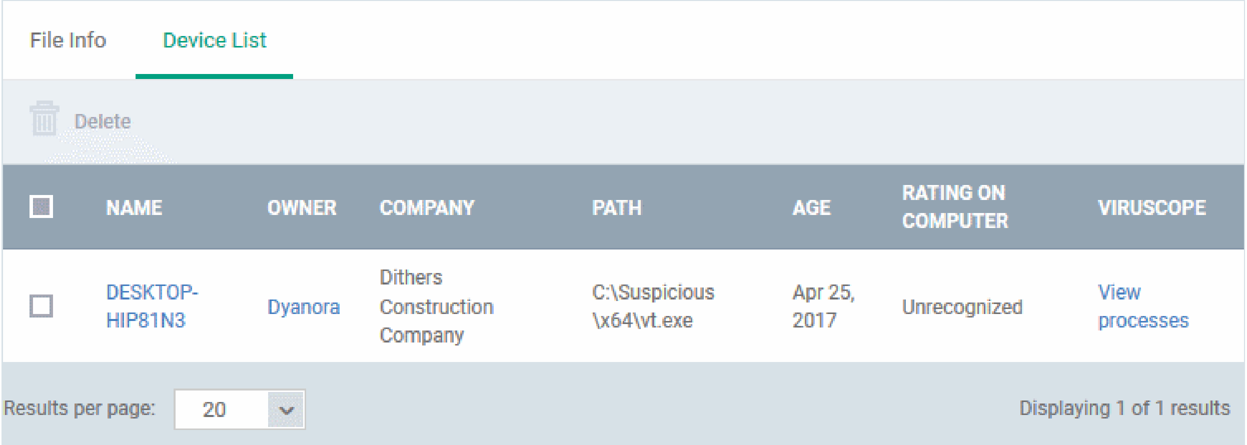
The new rating will be sent to all endpoints.

- The 'Record' button lets you hide, display or remove the file from the 'Application Control' list



Device List Screen

- Click 'Security Sub-Systems' > 'Application Control' then click on a file in the list.
- Next, select the 'Device List' tab to see a list of all devices on which the file is present
- The 'Device List' Screen can also be opened by clicking on the number in the 'Number of Devices' column in the 'Application Control' table.
- The device list screen shows each endpoint on which the item was discovered. The screen also shows the installation path, the installation date and the file rating assigned by Comodo Client Security. The Viruscope column shows detailed info on processes started by the file.



□	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSCOPE
□	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious \x64\vt.exe	Apr 25, 2017	Unrecognized	View processes

Results per page: 20

Displaying 1 of 1 results

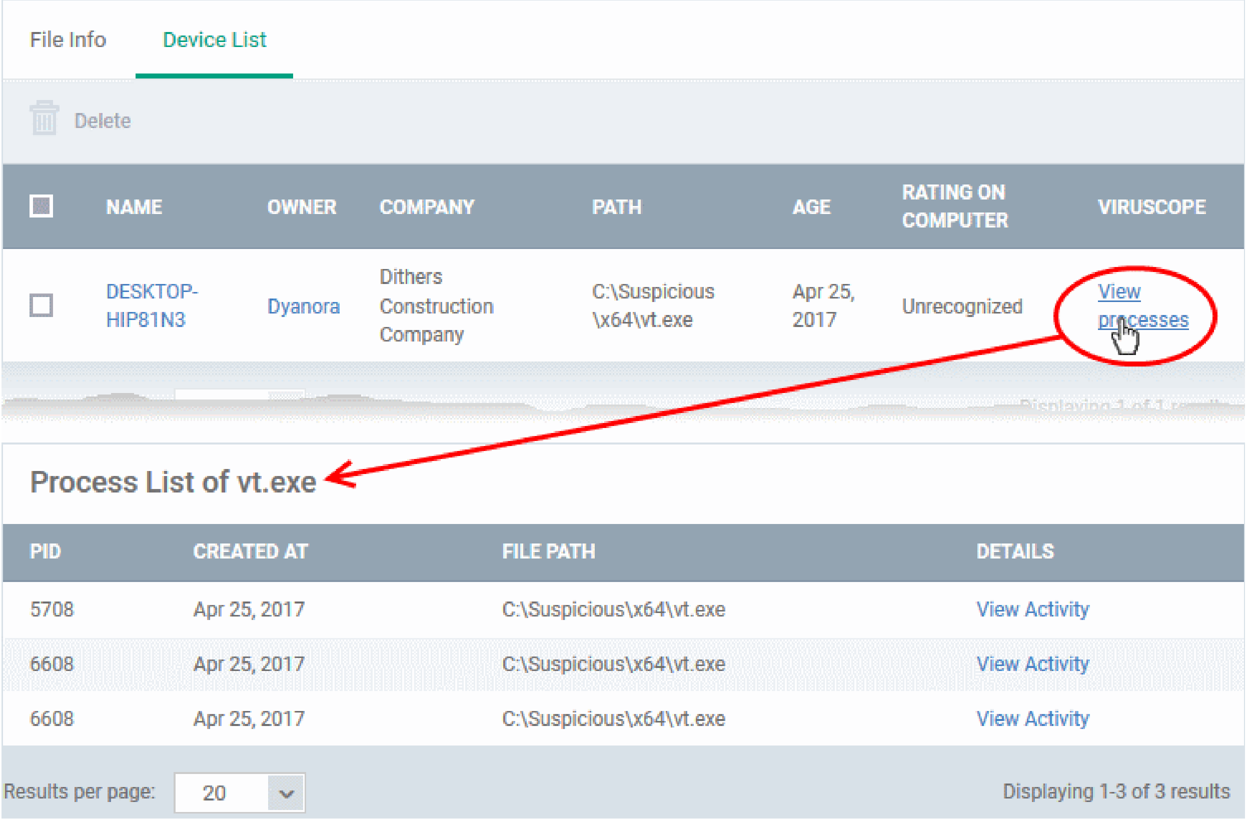
- You can remove the file from device(s) by selecting a device then clicking 'Delete'

View Process Activities of a File

Note: In order to fetch process activity data, VirusScope should be enabled in the profile in effect on the endpoint. Refer to **Configuring Viruscope Settings** in **Creating a Windows Profile** for more details.

To view the activities of a file on an endpoint

- Open the 'Device List' screen by clicking the file name or the number in the 'Number of Devices' column
- Click the 'View Processes' link in the 'Activity' column in the row of the device name.
- This will open a list of processes executed by the file on the selected endpoint:



File Info | Device List

Delete

☐	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSCOPE
☐	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious \x64\vt.exe	Apr 25, 2017	Unrecognized	View processes

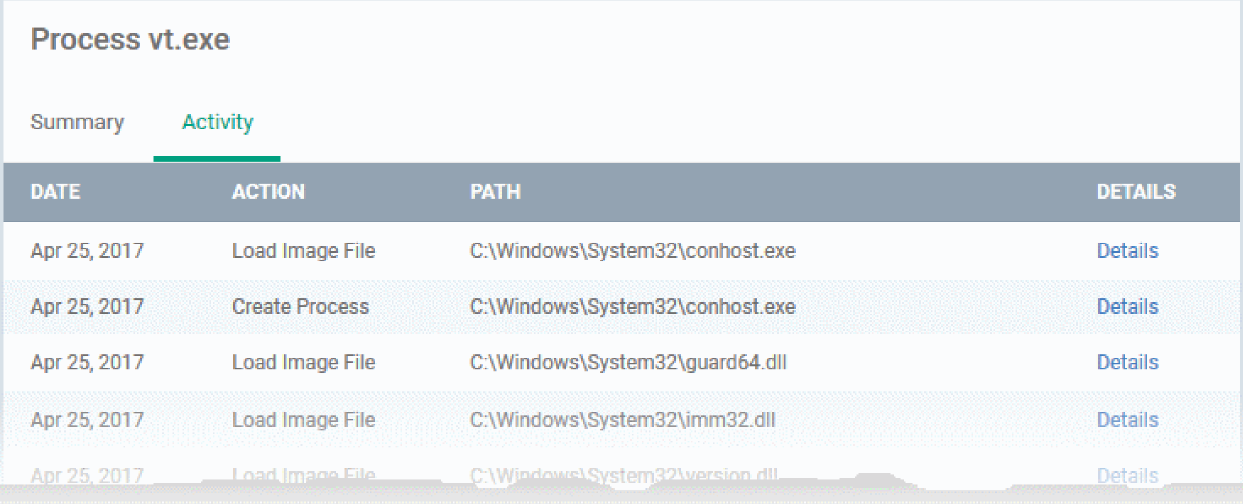
Process List of vt.exe

PID	CREATED AT	FILE PATH	DETAILS
5708	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity
6608	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity
6608	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity

Results per page: 20

Displaying 1-3 of 3 results

- Click 'View Activity' to see detailed information about each process. The 'Process Activity' interface 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.



Process vt.exe

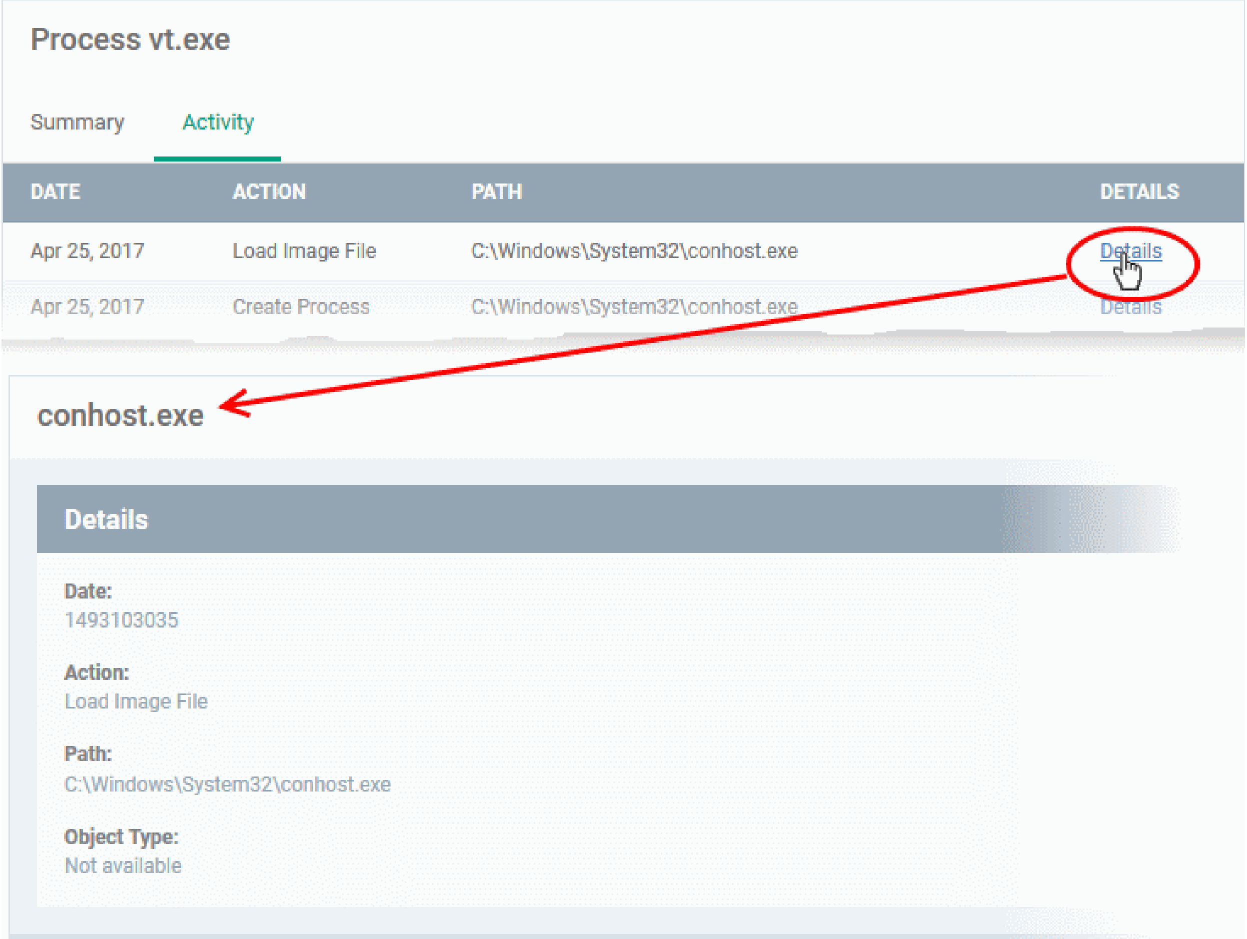
Summary | Activity

DATE	ACTION	PATH	DETAILS
Apr 25, 2017	Load Image File	C:\Windows\System32\conhost.exe	Details
Apr 25, 2017	Create Process	C:\Windows\System32\conhost.exe	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\guard64.dll	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\imm32.dll	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\version.dll	Details

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

- You can inspect a particular activity by clicking the 'Details' link:



Process vt.exe

DATE	ACTION	PATH	DETAILS
Apr 25, 2017	Load Image File	C:\Windows\System32\conhost.exe	Details
Apr 25, 2017	Create Process	C:\Windows\System32\conhost.exe	Details

conhost.exe

Details

Date:
1493103035

Action:
Load Image File

Path:
C:\Windows\System32\conhost.exe

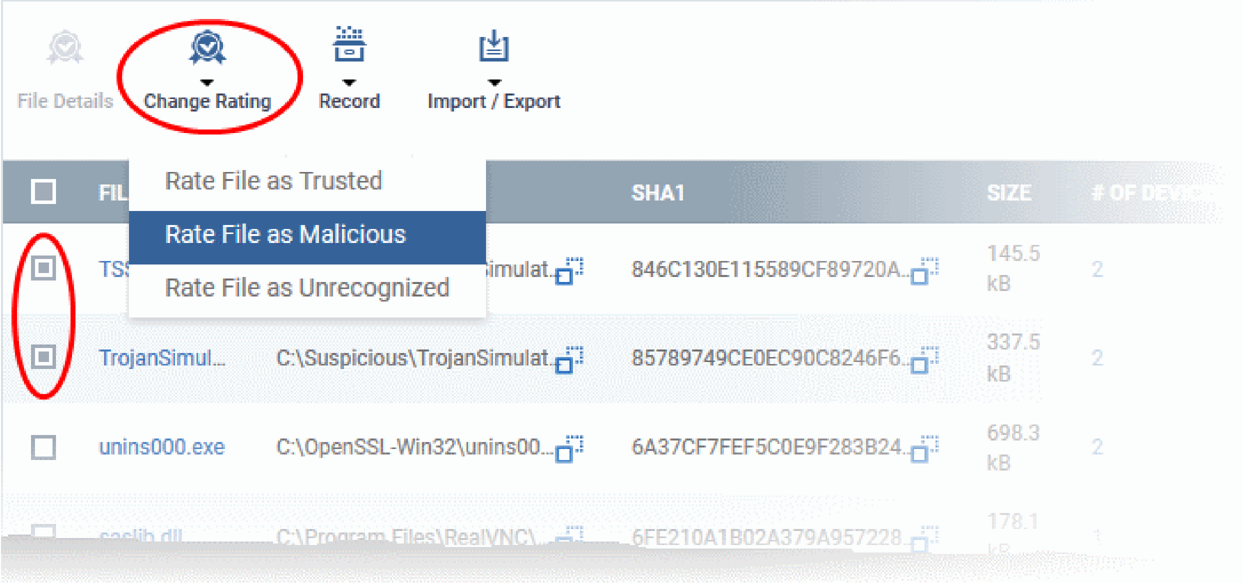
Object Type:
Not available

Assign Admin Rating to a File

- Each file on an endpoint is automatically scanned and assigned a trust rating by Comodo Client Security on the endpoint.
- These ratings can be either '**Unrecognized**', '**Trusted**' or '**Malicious**'. The rating for each file is shown in the 'Comodo Rating' column of the 'Application Control' interface.
- The file rating determines whether or how the file is allowed to run:
  - **Trusted** - The file will be allowed to run normally. It will, of course, still be subject to the standard protection mechanisms of Comodo Client Security (behavior monitoring, host intrusion prevention etc).
  - **Malicious** - The file will not be allowed to run. It will be automatically quarantined or deleted depending on admin preferences.
  - **Unknown** - The file will be run inside the container. The container is a virtual operating environment which is isolated from the rest of the endpoint. Files in the container write to a virtual file system, use a virtual registry and cannot access user or operating system data.
- Automatic file rating can be configured in the 'File Rating' section of the configuration profile active on the endpoint. See **File Rating settings** in **Creating a Windows Profile** for more details.
- Click 'Change Rating' in the 'Application Control' interface to manually set a rating for a selected file or files. The new rating will be propagated to all endpoints on which the item was identified and will determine the file's run-time privileges. Admin assigned ratings will be shown in the 'Admin Rating' column of the interface:

To assign a file rating to a file

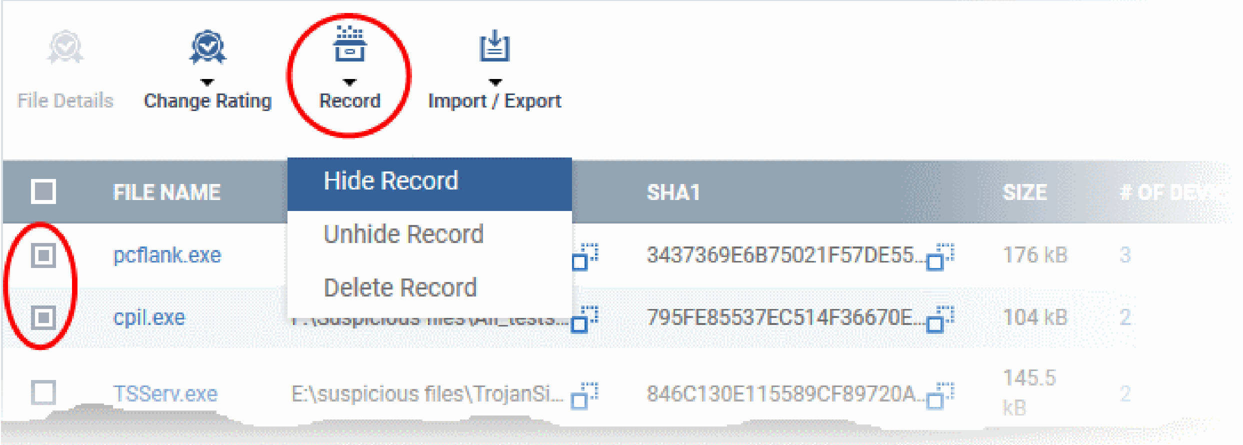
- Select the file(s) whose rating you want to change and click 'Change Rating'.
- Choose the rating you want to from the drop-down:


File Details
Change Rating
Record
Import / Export
Rate File as Trusted
Rate File as Malicious
Rate File as Unrecognized
FIL
SHA1
SIZE
# OF DEVICES
TSS
...imulat...
846C130E115589CF89720A...
145.5 kB
2
TrojanSimul...
C:\Suspicious\TrojanSimulat...
85789749CE0EC90C8246F6...
337.5 kB
2
unins000.exe
C:\OpenSSL-Win32\unins00...
6A37CF7FEF5C0E9F283B24...
698.3 kB
2
saslib.dll
C:\Program Files\RealVNC\...
6FE210A1B02A379A957228...
178.1 kB
1

As mentioned, the admin rating will be set and sent to all endpoints. The admin rating will determine the file's run-time privileges.

Hide/Display Selected Files

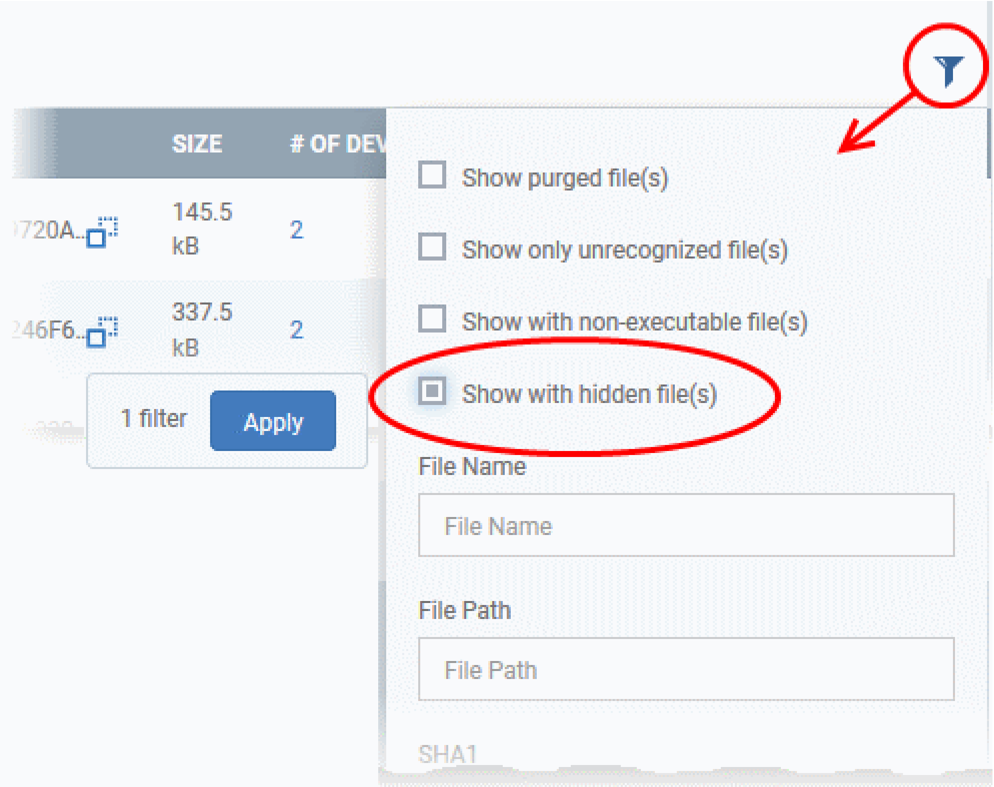
- Select the file(s) you want to hide and click 'Record' at the top



- Select 'Hide / Unhide / Delete Record' as required.

To view hidden files

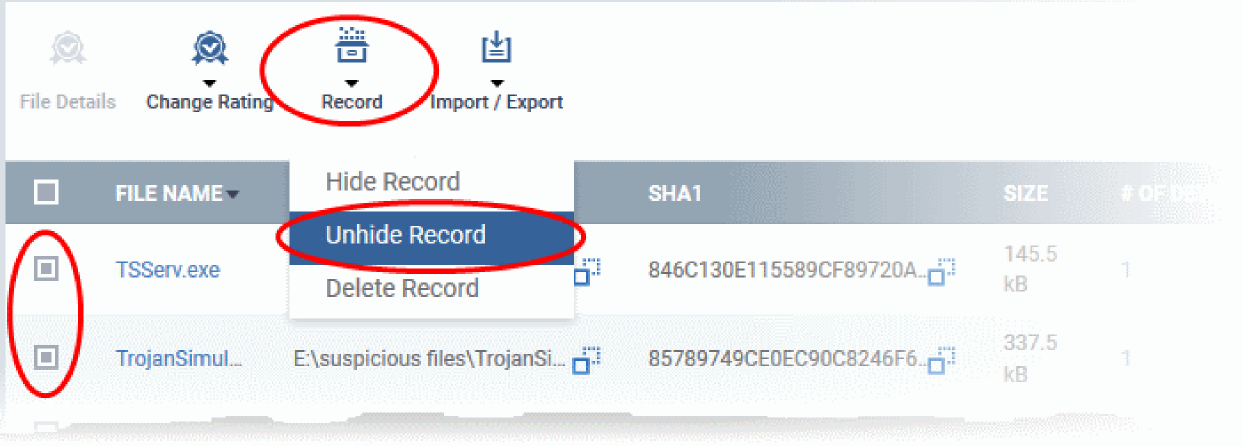
- Click the funnel icon at the top-right to open the filter options
- Select 'Show with hidden file(s)' and click 'Apply'



The hidden files will be included to the 'Application Control' interface. These files will be highlighted with a gray stripe.

To restore hidden files

- Click the funnel icon at the top-right to open the filter options
- Enable 'Show with hidden file(s)'
- Select the hidden files you want to restore click 'Record' and choose 'Unhide Record' from the drop-down

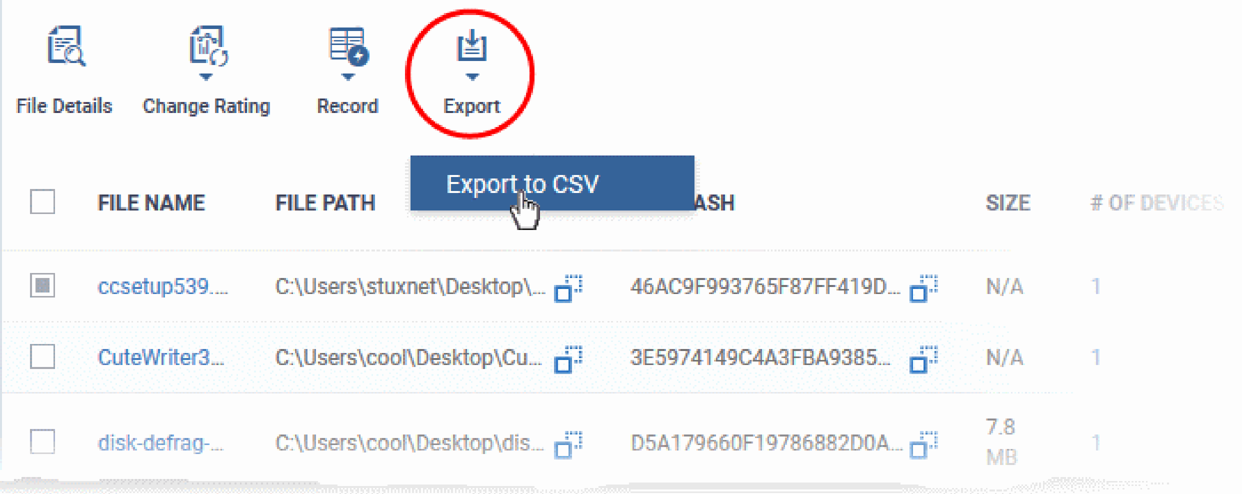


The files will be displayed in the file list permanently.

Export a Report of the Files List

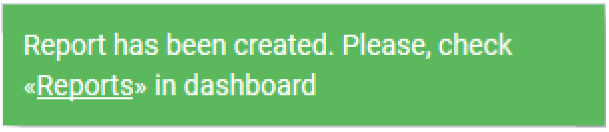
You can export a file-rating report in .csv format as follows:

- Click 'Security Sub-Systems' > 'Application Control'
- Click the funnel icon to apply any filters you require
- Click the 'Export' button and choose 'Export to CSV':



□	FILE NAME	FILE PATH	HASH	SIZE	# OF DEVICES
☒	ccsetup539....	C:\Users\stuxnet\Desktop\...	46AC9F993765F87FF419D...	N/A	1
□	CuteWriter3...	C:\Users\cool\Desktop\Cu...	3E5974149C4A3FBA9385...	N/A	1
□	disk-defrag-...	C:\Users\cool\Desktop\dis...	D5A179660F19786882D0A...	7.8 MB	1

The report will be generated in .csv file format.



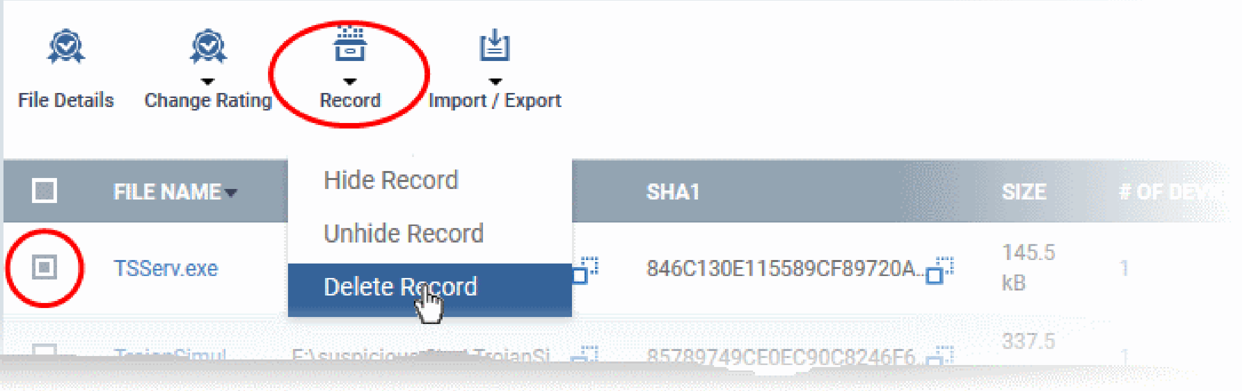
Report has been created. Please, check «Reports» in dashboard

The report will be available in the 'Dashboard' > 'Reports' interface. See **Reports** if you need more help with this interface.

Remove files from the list

You can hide files that you no longer wish to see in the list. The files will be removed from the list but will not be deleted from the endpoints.

- Select the files you want to remove and click 'Record' at the top
- Choose 'Delete Record' from the drop-down



□	FILE NAME	SHA1	SIZE	# OF DEVICES
☒	TSServ.exe	846C130E115589CF89720A...	145.5 kB	1
□	TrojanSimul...	85789749CE0EC90C8246F6...	337.5	1

9.2.1. File Ratings Explained

Comodo Client Security (CCS) rates the files identified from Windows devices as follows:

Unrecognized Files

Files that could not be identified as 'Trusted' or 'Malicious' by Comodo Client Security (CCS) are reported as 'Unrecognized' to ITSM . Administrators can review these files and can manually rate them as 'Trusted' or 'Malicious' as required.

Trusted Files

Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, Comodo Client security (CCS) on an endpoint will check the file against Comodo's master whitelist and blacklists. The file will be awarded 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 - Admins can assign a 'Trusted' rating to files from the Application Control interface
- User Rating - Users can assign a 'Trusted' rating to files at the local CCS installation in two ways:
    - In response to an alert. If an executable is unknown then it may generate a HIPS alert on the local endpoint. Users could choose 'Treat this as a Trusted Application' at the alert
    - The user can assign 'Trusted' rating to any file from the 'File List' interface.

  CCS creates a hash of all files assigned 'Trusted' status by the user. In this way, even if the file name is changed later, the file will retain its trusted status as the hash remains same. This is particularly useful for developers who are creating new applications that, by their nature, are unknown to the Comodo safe list.

Malicious Files

Files identified as malicious by the File Look-Up Service (FLS) will not be allowed to run by default. These files are reported as malware to ITSM.

9.3. View 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.

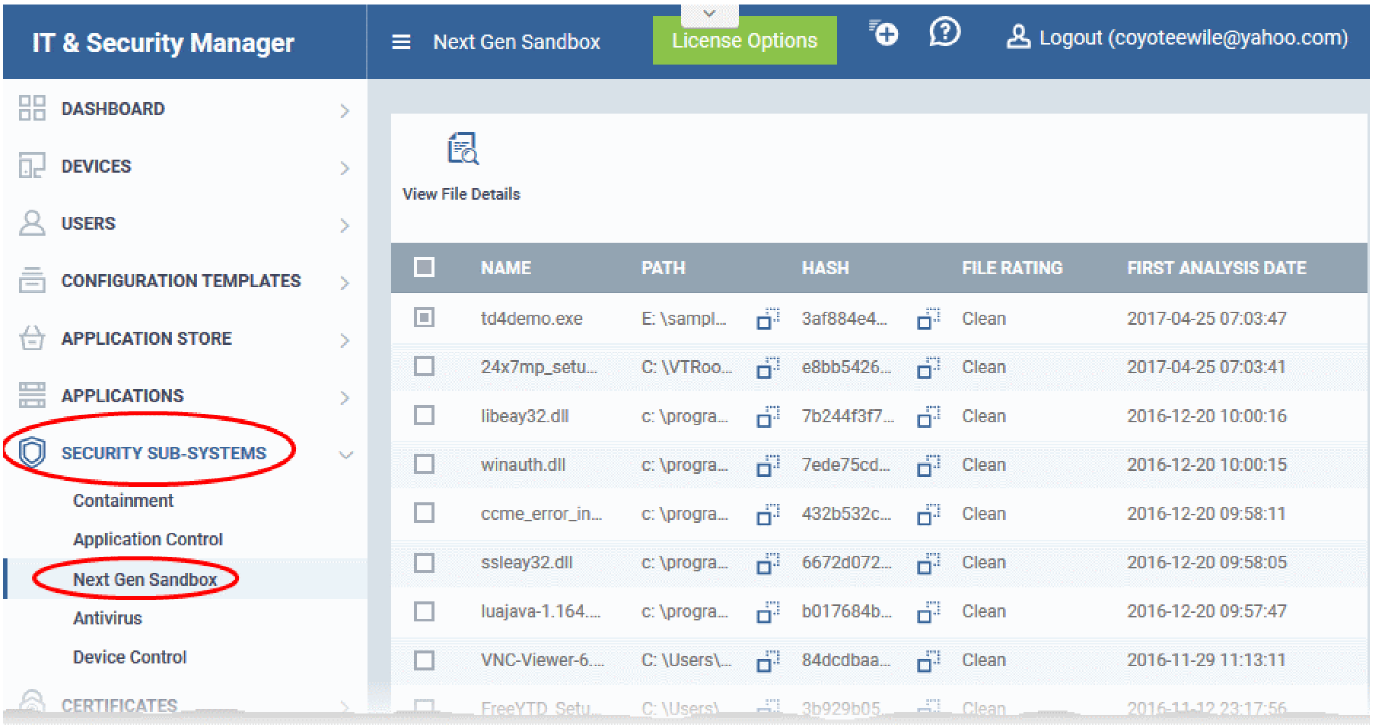
- Click 'Security Sub-Systems' > 'Next Gen Sandbox' to view all unknown files along with their Valkyrie ratings
- You can view Valkyrie statistics in the ITSM Dashboard by clicking 'Dashboard' > 'Valkyrie'.
- You can schedule unknown files for upload by configuring the Valkyrie component of the Windows 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**.

To open the 'Next Gen Sandbox' interface

- Click 'Security Sub-Systems' on the left and choose 'Next Gen Sandbox' from the options



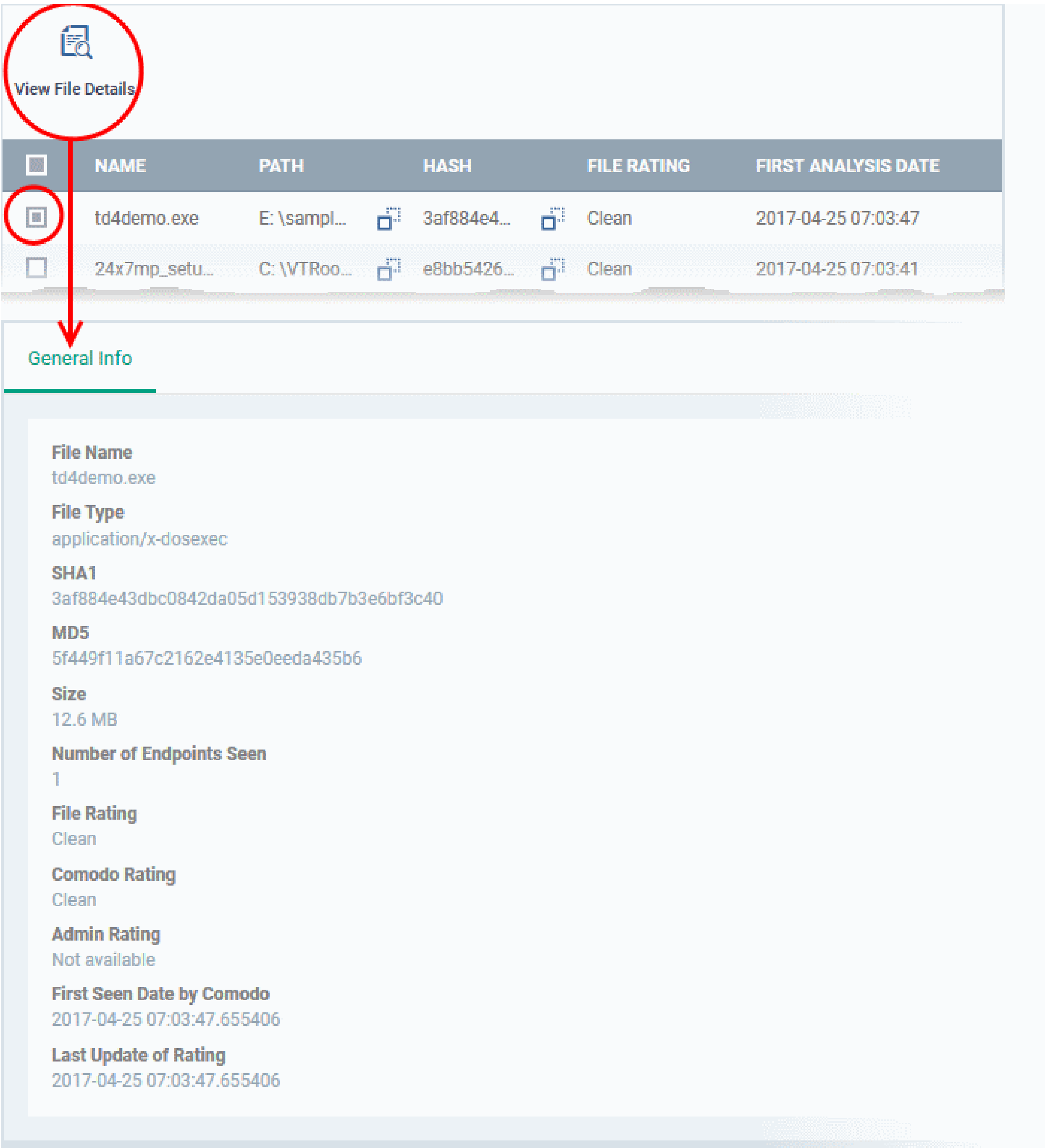
□	NAME	PATH	HASH	FILE RATING	FIRST ANALYSIS DATE
☒	td4demo.exe	E: \sampl...	3af884e4...	Clean	2017-04-25 07:03:47
□	24x7mp_setu...	C: \VTRoo...	e8bb5426...	Clean	2017-04-25 07:03:41
□	libeay32.dll	c: \progra...	7b244f3f7...	Clean	2016-12-20 10:00:16
□	winauth.dll	c: \progra...	7ede75cd...	Clean	2016-12-20 10:00:15
□	ccme_error_in...	c: \progra...	432b532c...	Clean	2016-12-20 09:58:11
□	ssleay32.dll	c: \progra...	6672d072...	Clean	2016-12-20 09:58:05
□	luajava-1.164....	c: \progra...	b017684b...	Clean	2016-12-20 09:57:47
□	VNC-Viewer-6....	C: \Users\...	84dcdbaa...	Clean	2016-11-29 11:13:11
□	FreeYTD_Setu...	C: \Users\...	3b929b05...	Clean	2016-11-12 23:17:56

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 on 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.

- Select a file and click the 'View File Details' button:



□	NAME	PATH	HASH	FILE RATING	FIRST ANALYSIS DATE
☒	td4demo.exe	E: \sampl...	3af884e4...	Clean	2017-04-25 07:03:47
□	24x7mp_setu...	C: \VTRoo...	e8bb5426...	Clean	2017-04-25 07:03:41

File Name
td4demo.exe

File Type
application/x-dosexec

SHA1
3af884e43dbc0842da05d153938db7b3e6bf3c40

MD5
5f449f11a67c2162e4135e0eeda435b6

Size
12.6 MB

Number of Endpoints Seen
1

File Rating
Clean

Comodo Rating
Clean

Admin Rating
Not available

First Seen Date by Comodo
2017-04-25 07:03:47.655406

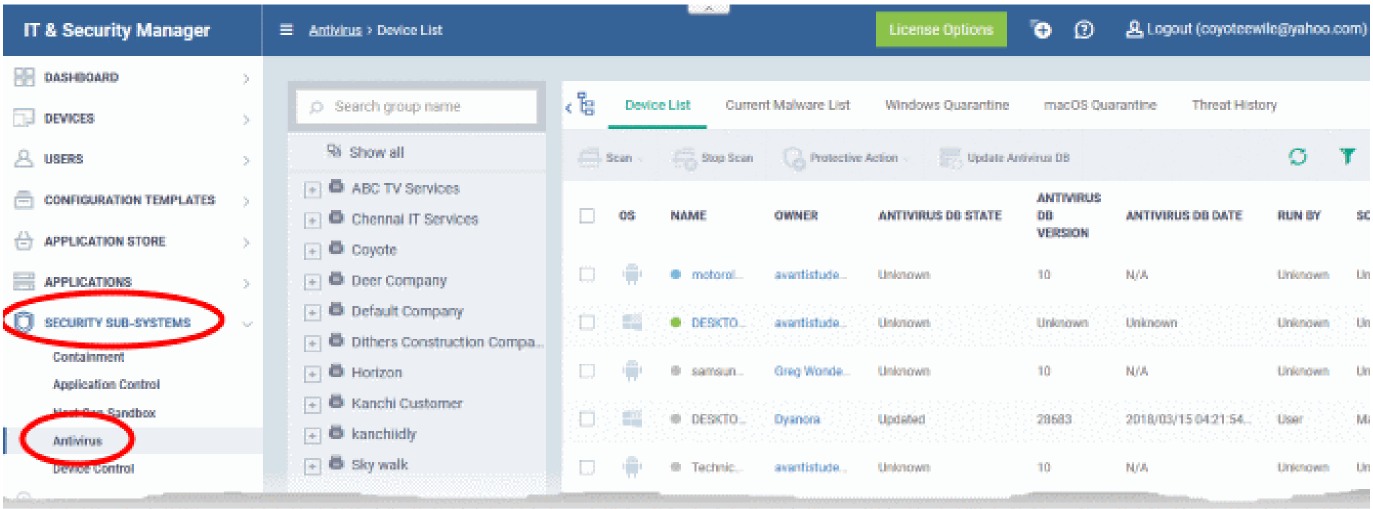
Last Update of Rating
2017-04-25 07:03:47.655406

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.

9.4. Antivirus and File Rating Scans

The 'Antivirus' section under 'Security Sub-systems' allows you to:

- View the current infection status of managed Windows, Mas OS and Android devices.
- Initiate antivirus and file rating scans on devices.
- View a consolidated list of all malware on all endpoints.
- View a list of all quarantined files on Windows and Mac OS devices
- View an all-time history of threats discovered on all endpoints
- Manually delete, quarantine or ignore malicious files



□	OS	NAME	OWNER	ANTIVIRUS DB STATE	ANTIVIRUS DB VERSION	ANTIVIRUS DB DATE	RUN BY	SC
□		motorol...	avantistude...	Unknown	10	N/A	Unknown	Un
□		DESKTO...	avantistude...	Unknown	Unknown	Unknown	Unknown	Un
□		samsun...	Greg Wonde...	Unknown	10	N/A	Unknown	Un
□		DESKTO...	Dyanora	Updated	28683	2018/03/15 04:21:54...	User	M
□		Technic...	avantistude...	Unknown	10	N/A	Unknown	Un

The Antivirus interface has five sub-tabs:

- **Device List** - Shows the infection status of all managed devices. The interface shows the date and type of the most recent scan and allows you to initiate on-demand scans on selected endpoints. You can also delete, quarantine or ignore all threats found on selected device(s). See **The Device List Interface** for more details.
- **Current Malware List** - Lists all unprocessed malware residing on managed devices. You can delete, ignore or quarantine specific pieces of malware on specific devices, or apply these actions to multiple threats at once. Refer to **Viewing and Managing Identified Malware** for more details.
- **Windows Quarantine** - Displays malware which has been quarantined by Comodo Client Security on Windows endpoints. You can delete or restore quarantined items and/or manually assign a trust rating. Refer to **Viewing and Managing Quarantined Items from Windows Devices** for more details.
- **Mac OS Quarantine** - Displays malware which has been moved to quarantine by Comodo Antivirus for MAC on Mac OS devices. You can delete or restore quarantined items and/or manually assign a trust rating. Refer to **Viewing and Managing Quarantined Items on Mac OS Devices** for more details.
- **Threat History** - Displays a log of all malicious items found on Android, Windows and Mac OS devices over time. Refer to the section **Viewing Threat History** for more details.

The Device List Interface

The 'Device List' screen displays the infection status of Android, Mac OS and Windows devices. From here you can:

- Run on-demand antivirus scans on selected devices
- Run file rating scans on Windows devices
- Choose the action to be taken on malware discovered by scans.
- Update the AV database on endpoints

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 Profiles**.

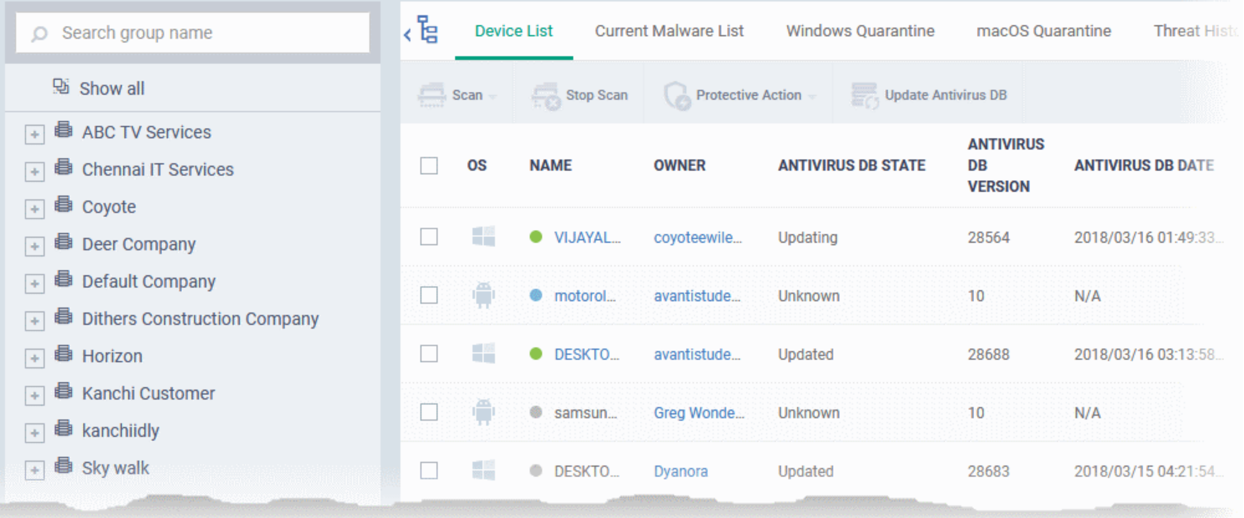
To open the 'Antivirus > Device List' interface:

- Click 'Security Sub-Systems' > 'Antivirus' on the left then open the 'Device List' tab

- Select a company and group from the middle-pane to view all devices in a particular group

  Or

- Select 'Show All' to view all devices enrolled to ITSM



- ABC TV Services
- Chennai IT Services
- Coyote
- Deer Company
- Default Company
- Dithers Construction Company
- Horizon
- Kanchi Customer
- kanchiidly
- Sky walk

	OS	NAME	OWNER	ANTIVIRUS DB STATE	ANTIVIRUS DB VERSION	ANTIVIRUS DB DATE
□		VIJAYAL...	coyoteewile...	Updating	28564	2018/03/16 01:49:33...
□		motorol...	avantistude...	Unknown	10	N/A
□		DESKTO...	avantistude...	Updated	28688	2018/03/16 03:13:58...
□		samsun...	Greg Wonde...	Unknown	10	N/A
□		DESKTO...	Dyanora	Updated	28683	2018/03/15 04:21:54...

The list displays all Android, Mac OS and Windows devices along with their last scan details, infection status and antivirus database update state.

Antivirus Device List - Column Descriptions	
Column Heading	**Description**
OS	The operating system of the device.
Name	The label 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. • Click the device name to view granular details about the device. • See **Manage Windows Devices**, **Manage Mac OS Devices** and **Manage Android / iOS Devices** for more details.
Owner	The name of the device user. • Click the user name to view more details about the user • See **View the User Details** for more details.
Antivirus DB State	The update status of the virus signature database on the device.
Antivirus DB Version	The version number of the virus signature database on the device
Antivirus DB Date	The date and time at which the AV database was last updated
Run By	The source that initiated the last scan. An antivirus scan or a file rating scan can be initiated in the following ways: • **Portal** - Manually run by an admin from the ITSM interface. See **Run Antivirus and/or File Rating Scans on Devices** for more details. • **User** - Manually run by the end-user at the endpoint, from the Comodo Client-Security (CCS) interface. • **Scheduled** - Automatically run as per the schedule defined in the configuration

	profiles effective on the device.
Scan Type	Indicates the type of the last scan ran on the device. The possible types of scan are: • Antivirus Full Scan - Applies to Windows, Mac OS and Android devices. • Antivirus Quick Scan - Applies to Windows, Mac OS and Android devices. • File Rating Quick Scan - Applies only to Windows devices. • Custom Scan - Applies to Windows and Mac OS devices. • Manual Scan - Applies to Windows and Mac OS devices • SD Card Scan - Applies only to Android devices.
Scan State	Status of the last scan run on the device. Possible states are: • Not scanned yet • Complete • Scanning • Failed • Viruses found • Canceled • Command sent
Scan Date	The date and time at which the last scan was run.
Malware Status	The infection status of the device based on results from real-time, on-demand and/or scheduled scans. Devices with untreated malware will be listed as 'Infected'. Clicking on 'Infected' will open the 'Current Malware List' which shows all malware on all managed devices. From here you can delete the malware or take other actions as required. See **Handle Malware on Scanned Devices** for more details.

The 'Antivirus' > 'Device List' interface allows you to:

- **Run Antivirus and/or File Rating Scans on Devices**
- **Handle Malware on Scanned Devices**
- **Update virus signature database on Windows and Mac OS Devices**

Sorting, Search and Filter Options

- Click any column header except 'Antivirus DB version' to sort items in ascending/descending order of the column header
- Click the funnel icon ▼ on the right to filter items by various criteria, including by OS, name, owner, AV DB update status, scan source, last scan type, last scan status, last scan date, malware status and AV DB version .
- Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. Click the arrow next to the 'Results per page' drop-down to increase results up to a maximum of 200.

9.4.1. Run Antivirus and/or File Rating Scans on Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List' to open the scan interface.

The interface lets you run virus and file rating scans on Android, Mac OS and Windows devices.

> **Note**: The scans interface lets you manage on-demand scans only. For automated scans, please create a scan schedule in a configuration profile then push it to selected devices/groups. See **Create Configuration Profiles** for more details.

To launch an on-demand scan

- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Device List' tab
  - Click a company name then a group in the middle pane to view all devices in a particular group

    Or
  - Select 'Show All' on the left menu to view all devices enrolled to ITSM
- Select the Android, Mac OS or Windows device(s) you wish to scan
- Choose a scan type from the 'Scan' drop-down
- The scan command will sent to the target devices and the scan will commence immediately

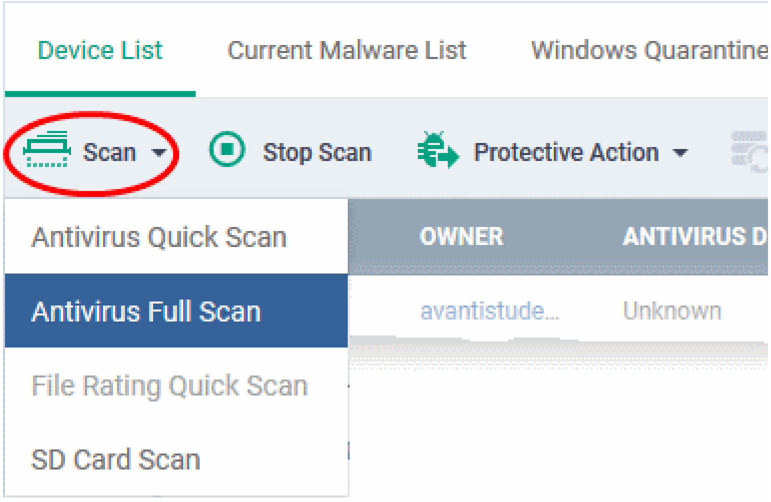
> **Tip**: You can access filters by clicking the funnel icon at the top right. For example, you may want to display only devices with Last Scan States of 'Unknown', 'Scan Failed' and 'Scan Canceled'.

The scan types available depend on the OS of the selected device(s). The scan type defines the areas to be scanned on the selected device(s). The following sections explain the scan process for:

- **Android Devices** (Quick Scan, Full Scan, SD Card Scan)
- **Windows Devices** (Quick Scan, Full Scan, File Rating Quick Scan)
- **Mac OS Devices** (Quick Scan, Full Scan)

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:

- **Antivirus Quick Scan** - Scans critical areas of the device which are highly prone to attack from viruses, rootkits and other malware. 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.

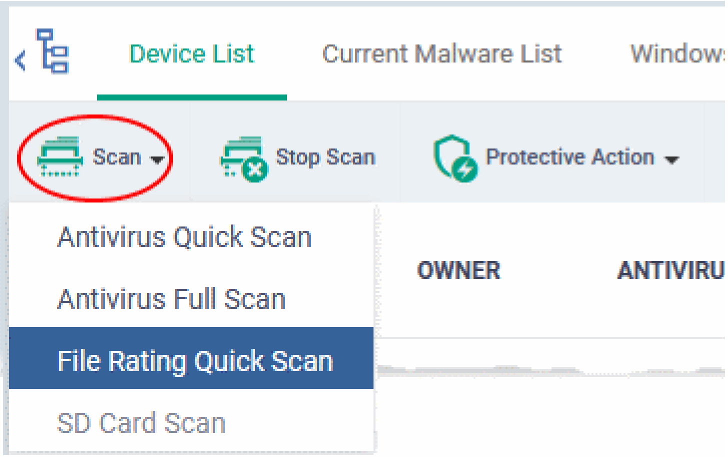
- **Antivirus Full Scan** - Scans all folders/files in both the system internal memory and the SD card.
- **SD Card Scan** - Scans all folders/files in the Secure Digital (SD) memory card mounted on the device.

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 scan, choose the devices and click 'Stop Scan' from the options at the top.
- If malware is found after the scan then the 'Last Scan State' will say 'Infected'. Infections identified after the scan will be treated according to settings in 'Settings' > 'Portal Set-Up' >Android Client Configuration' > 'Antivirus'. See **Configure Android Client Antivirus Settings** for more details.
- If 'Manual control' is chosen, then you have the option to uninstall or ignore from the 'Current Malware List'. See **View and Manage Identified Malware** for more details.
- You can also choose to uninstall or ignore the identified malware by clicking the respective buttons at the top. See **Handling Malware Identified from Scanned devices** section for more details.

Windows Devices

- Click 'Scan Device' and choose the 'Scan type/Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan types/profiles are:

- **Antivirus Quick Scan** - Scans critical areas of the device which are highly prone to attack from viruses, rootkits and other malware. Areas scanned include. Areas scanned include 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.
- **Antivirus 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.
- **File Rating Quick Scan** - Runs a cloud-based assessment of files on the device to determine the trust rating of each file. The 'Quick' rating scan checks commonly infected areas and memory.

Files are rated as:

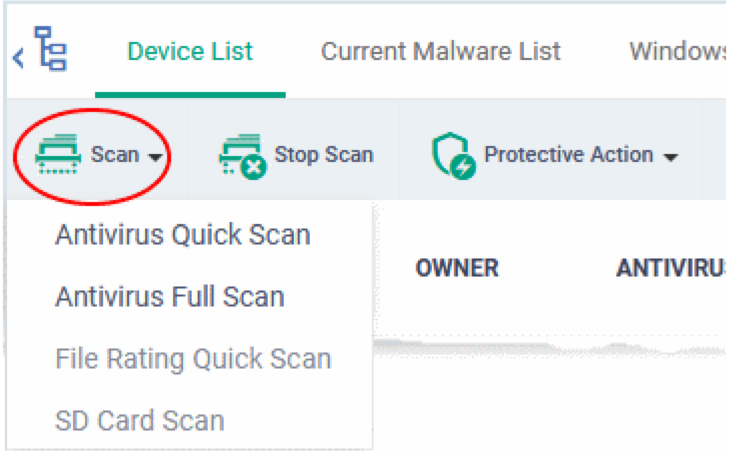
- **Trusted** - the file is safe
- **Unknown** - the trustworthiness of the file could not be assessed
- **Bad** - the file is unsafe and may contain malicious code

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Scan State' column for each device.

- If you want to terminate the scanning on selected devices, choose the devices and click 'Stop Scan' from the options at the top.
- If malware is found on completion of scan the 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. See **Handle 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. The Quarantine interface allows you to:
  - Delete an item, if it is identified as malicious
  - Restore the file to its original location on the endpoint if the item is a false-positive. You can also rate a file as 'Trusted' to restore it to the endpoint. Doing so will effectively white-list the file by giving it a 'Trusted' rating in the local CCS database.
- See **View and Manage Quarantined Items on Windows Devices** 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:

- **Antivirus Quick Scan** - Scans important operating system files and folders including system memory, auto-run entries, hidden services.
- **Antivirus Full Scan** - Scans every local drive, folder and file on your system including external devices, storage drives, digital cameras.

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 scan on certain devices, choose the devices and click '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. See **Handle Malware Identified from Scanned devices** for more details.
- Items moved to quarantine are encrypted and saved in the device itself, so that they are isolated from the rest of the system.
- You view the quarantined items from the 'Quarantine' interface. The Quarantine interface allows you to:
  - Delete an item, if it is identified as malicious
  - Restore the file to its original location on the endpoint if the item is a false-positive.

- See **View and Manage Quarantined Items on Mac OS Devices** for more details.

9.4.2. Handle Malware on Scanned Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List' to open the 'Device List' interface.

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 remove, ignore or quarantine malware using the 'Protective Action' button above the table.

Tip: The 'Security Sub-Systems' > 'Antivirus' 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 malware, please use the 'Current Malware List' instead. See **View and Manage Identified Malware** for more details.

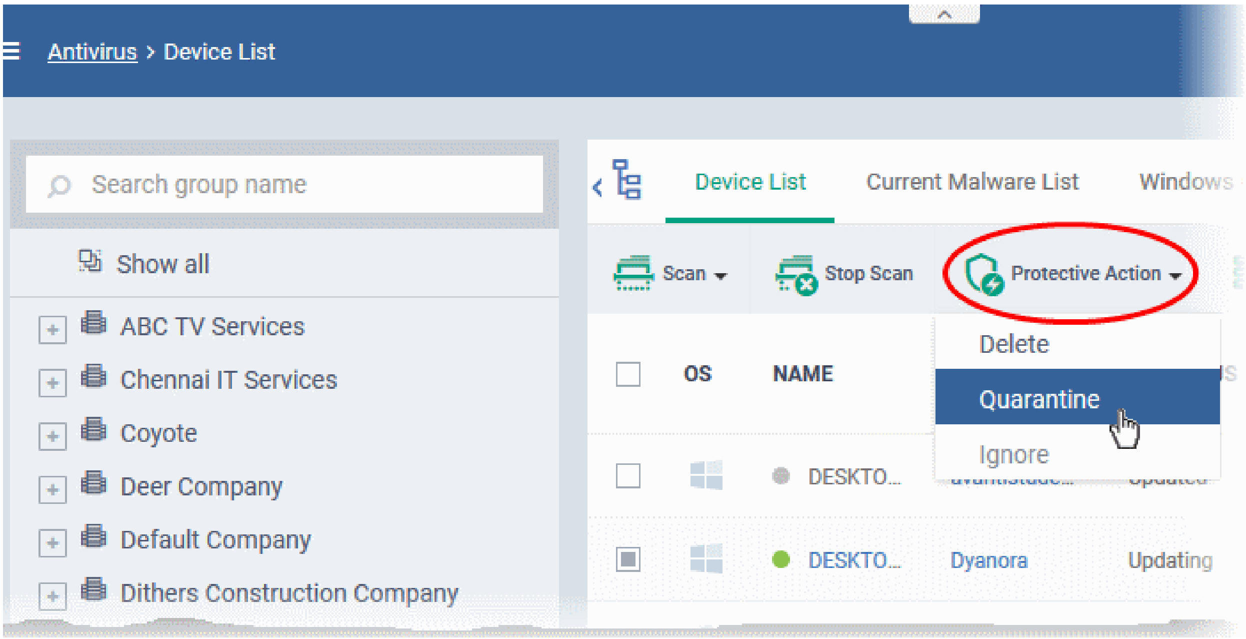
To remove / quarantine/ ignore ALL malware on selected devices

- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Device List' tab
    - Click a company name then a group in the middle pane to view all devices in a particular group

      Or
    - Select 'Show All' on the left menu to view all devices enrolled to ITSM
- Select device(s) with a malware status of 'Infected' using the check-box(es) on the left.

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 'Protective Action' above the table and select your desired action:

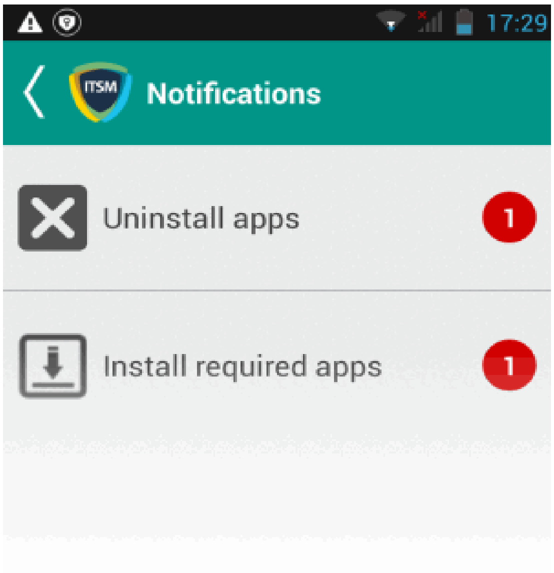


The actions available depend on the OS of the device chosen:

For Android Devices:

- **Delete** - Removes the malicious app
- **Ignore** - Ignores malware found by the last scan. The item will be identified as malware again on the next scan.

For the 'Delete' operation, a notification will be sent to the selected devices to uninstall the app(s):



17:29

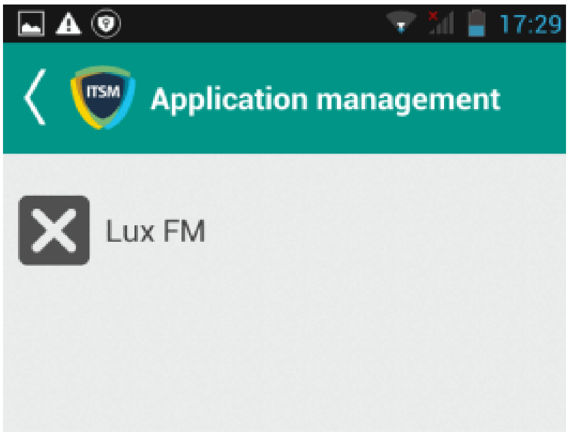
Notifications

Uninstall apps 1

Install required apps 1

The notification shows the number of threats which will be removed from the device.

- Touch the alert to view all items which are ready for removal.

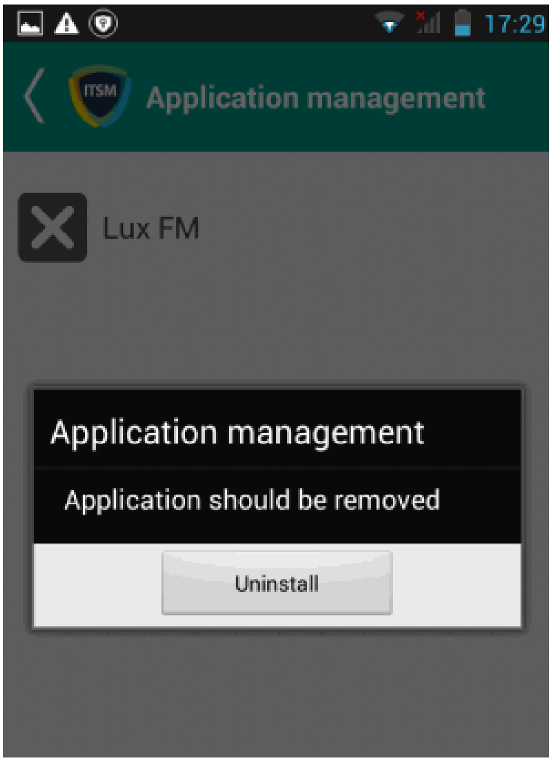


17:29

Application management

Lux FM

- Tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



Application management

Application should be removed

For Windows Devices

- **Delete** - Instructs CCS on the endpoint to clean the malware.
    - If a disinfection routine is available, CCS will disinfect it and retain the original file.
    - If a disinfection routine is not available, CCS will delete the application.
- **Quarantine** - Moves the malware to quarantine on the device.
    - You can review quarantined files by clicking 'Security Sub-Systems' > 'Antivirus' > 'Windows Quarantine'.
    - Based on their trustworthiness, you can remove them from the device or restore them to their original locations. See **View and Manage Quarantined Items on Windows Devices** for more details.

For Mac OS Devices

- **Delete** - 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** - Moves the malware to quarantine on the device. You can review quarantined files from the 'Security Sub-Systems' > 'Application Control' > ' Mac OS Quarantine' interface. Based on their trustworthiness, you can remove them from the device or restore them to their original locations. See **View and Manage Quarantined Items on Mac OS Devices** for more details.

9.4.3. Update Virus Signature Database on Windows and Mac OS Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List' to open the 'Device List' interface.

It is vital to make sure all managed endpoints have the latest virus database installed. You can update the database manually or according to a schedule:

Automatic Updates - ITSM lets you schedule automatic updates as follows:

- **Windows devices** - Configure the 'Update' component of the Windows profile applied to a device. See **Client Security Update** in **Creating Windows Profiles** for more details.
- **MAC OS devices** - Configure the 'Antivirus' component of the Mac OS profile applied to a device. See

Antivirus in **Antivirus Settings for Mac OS Profile** for more details.

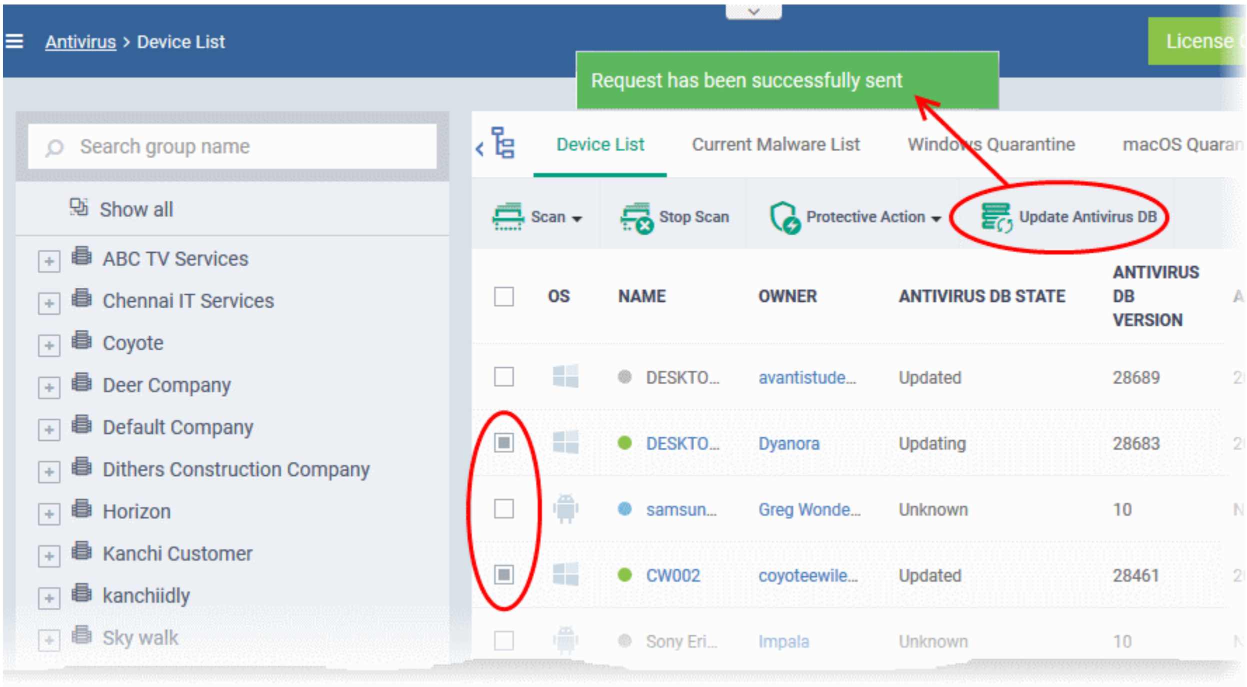
Manual Updates

- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Device List' tab
  - Click a company name then a group in the middle pane to view all devices in a particular group

    Or
  - Select 'Show All' on the left menu to view all devices enrolled to ITSM
- Select the Windows and/or 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 Antivirus DB' from the options at the top.



□	OS	NAME	OWNER	ANTIVIRUS DB STATE	ANTIVIRUS DB VERSION	A
□		DESKTO...	avantistude...	Updated	28689	2
☑		DESKTO...	Dyanora	Updating	28683	2
□		samsun...	Greg Wonde...	Unknown	10	N
☑		CW002	coyoteewile...	Updated	28461	2
□		Sony Eri...	Impala	Unknown	10	N

A command will be sent to target devices to start downloading the updates.

9.5. View and Manage Identified Malware

- Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List'
- The 'Current Malware List' shows malicious items on which no action has yet been taken.
- You can use this interface to clean, ignore or quarantine the items.

Notes:

Android Devices:

- If AV options are set to 'automatically uninstall' or 'ignore' in a device profile, then the item will be handled accordingly and not shown in the 'Current Malware List'.

  See **Antivirus Settings** in **Profiles for Android Devices** for more details.

Windows Devices:

For real-time virus monitoring:

- Threats will be shown in the list if:
  - 'Show antivirus alerts' is disabled and 'Block Threats' is chosen as the default action in the profile active on the device

    OR
  - 'Show antivirus alerts' is enabled and the user decides to block the threat at an alert.
- Threats will NOT be shown in the list if:
  - 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action

    OR
  - 'Show antivirus alerts' is enabled and the user quarantines the threat at an alert.
- Click 'Configuration Templates' > 'Profiles' > *Click the name of any Windows profile* > 'Antivirus' tab > Open the 'Realtime Scan' tab.
- See **Realtime Scan settings** in **Antivirus Settings** if you need more help with this.

For scheduled and manual scans:

- Threats will be shown in the list only if 'Automatically clean threats' is disabled in the profile active on the device.
- Click 'Configuration Templates' > 'Profiles' > *Click the name of any Windows profile* > 'Antivirus' tab > 'Scans' tab > Click the 'Edit' icon beside a profile > Open the 'Options' tab.
- See **Custom Scans** in **Antivirus Settings** if you need more help with this.

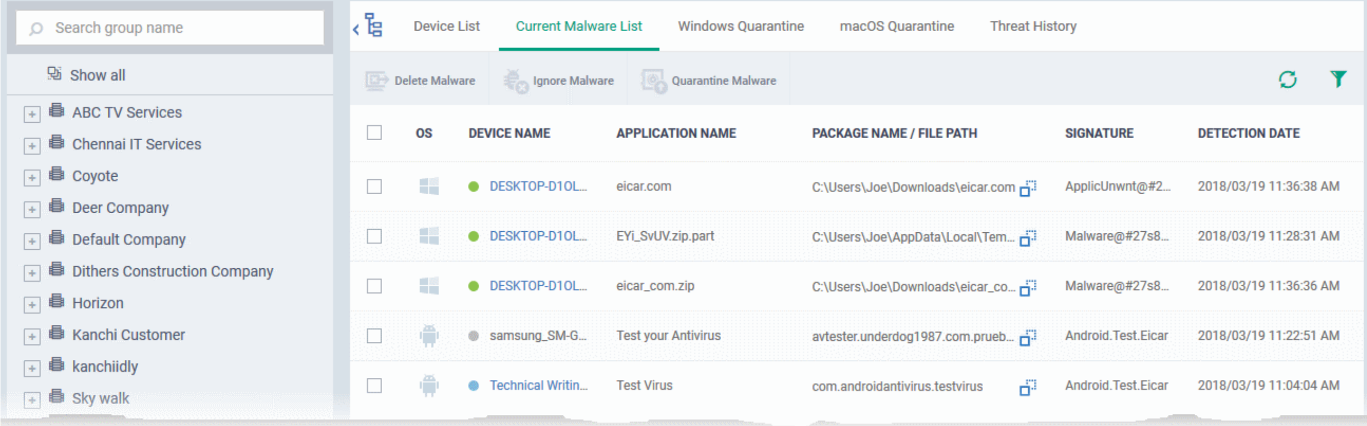
Mac OS Devices

- Threats will only appear in this list if 'Auto-Quarantine' is disabled in the profile on the device.
- Threats will NOT appear in this list if:
  - 'Auto quarantine' is enabled in 'Realtime scanning', 'Manual Scanning' and 'Scheduled Scanning'
  - 'Auto quarantine' is disabled but the user chooses to quarantine the item from an alert
- See **Antivirus Settings** under **Creating Mac OS Profiles** for more details.

To view the malware list

- Click 'Security Sub-Systems' on the left then choose 'Antivirus'
- Click the 'Current Malware List' tab
  - Click a company name then a group in the middle pane to view malware identified on devices in a particular group

    Or
  - Select 'Show All' on the left menu to view malware identified on all devices enrolled to ITSM



□	OS	DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	SIGNATURE	DETECTION DATE
□		● DESKTOP-D1OL...	eicar.com	C:\Users\Joe\Downloads\eicar.com	ApplicUnwnt@#2...	2018/03/19 11:36:38 AM
□		● DESKTOP-D1OL...	EYi_SvUV.zip.part	C:\Users\Joe\AppData\Local\Tem...	Malware@#27s8...	2018/03/19 11:28:31 AM
□		● DESKTOP-D1OL...	eicar_com.zip	C:\Users\Joe\Downloads\eicar_co...	Malware@#27s8...	2018/03/19 11:36:36 AM
□		● samsung_SM-G...	Test your Antivirus	avtester.underdog1987.com.prueb...	Android.Test.Eicar	2018/03/19 11:22:51 AM
□		● Technical Writin...	Test Virus	com.androidantivirus.testvirus	Android.Test.Eicar	2018/03/19 11:04:04 AM

A list of malware identified from all the enrolled Android, Windows and Mac OS devices will be displayed.

Current Malware List - Column Descriptions	
Column Heading	**Description**
OS	The operating system of the device on which the malware was identified.
Device Name	The label assigned to the device. If no name was assigned by the end-user then the model number of the device is used. Gray text color shows the device has been offline for the past 24 hours. • Click the device name to view granular details about the device. • See **Manage Windows Devices**, **Manage Mac OS Devices** and **Manage Android / iOS Devices** for more details.
Application Name	The name of the infected application.
Package Name / File Path	The install location of the file on the endpoint. Android devices - The package name or identifier is shown.
Signature	The name of the identified malware.
Detection Date	Date and time that the malware was discovered.

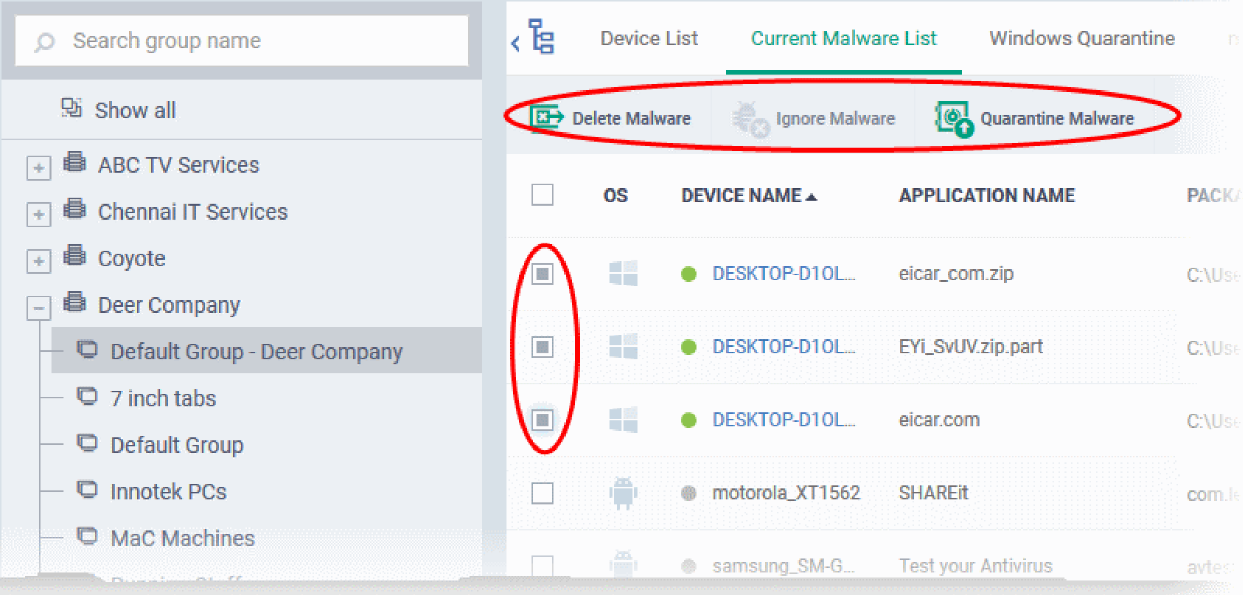
Sorting, Search and Filter Options

- Click any column header to sort items in ascending/descending order of the entries in that column
- Click the funnel icon on the right to filter items by various criteria, including by OS, device name, application name, package name/file path, signature and detection date.
- Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. Click the arrow next to the 'Results per page' drop-down to increase results up to a maximum of 200.

Take Actions on Threats

- You can uninstall/delete malicious items from the devices on which they were found.
- Alternatively, if you think an item is a false positive, you can choose to ignore it. The item will not be uninstalled from the device but will be removed from the 'Current Malware List'.
- If an item is found to be suspicious, you can choose to move it to quarantine for later analysis and removal.

The options at the top of the table let you take actions on selected items. The available actions depend on the operating system of the device(s).

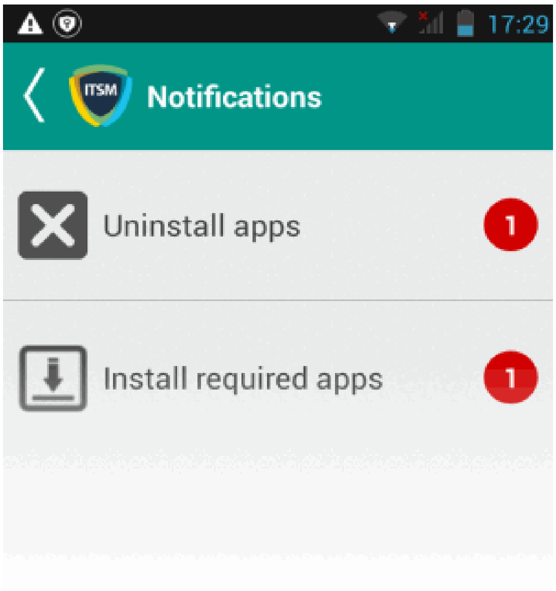


□	OS	DEVICE NAME ▲	APPLICATION NAME	PACK
▣		● DESKTOP-D1OL...	eicar_com.zip	C:\Use
▣		● DESKTOP-D1OL...	EYi_SvUV.zip.part	C:\Use
▣		● DESKTOP-D1OL...	eicar.com	C:\Use
□		● motorola_XT1562	SHAREit	com.le
□		● samsung_SM-G...	Test your Antivirus	avtes

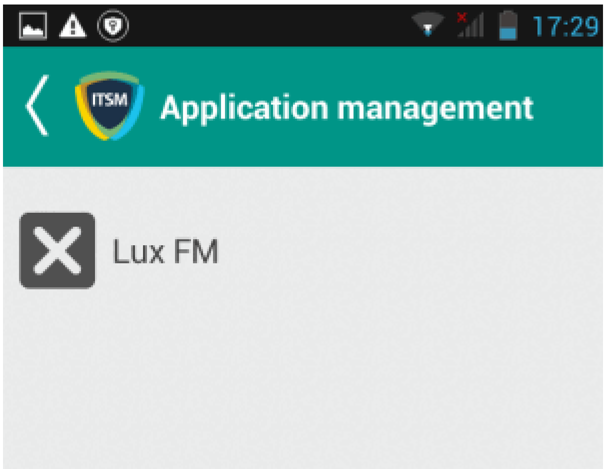
Threats identified on Android Devices

First, select the items on which you want to take the action. Then click one of the following:

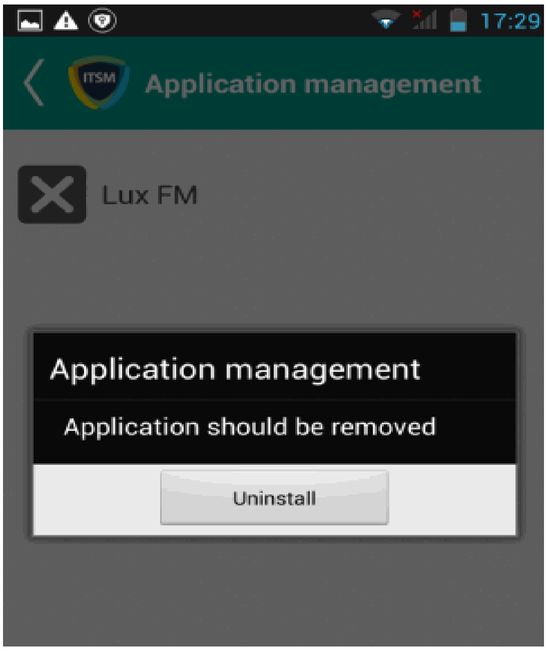
- **Ignore Malware** - Select if the item is a false positive. The item will remain on the device.
- **Delete Malware** - Select if you want to remove the malware from the device. The following notification will be sent to the affected device:



- Touch the alert to view a list of all items which are ready to be removed:



- Tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



Application management

Application should be removed

Threats identified on Windows Devices:

First, select the items on which you want to take the action. Then click one of the following:

- **Delete Malware** - Will remove the malware from the device.
- **Quarantine Malware** - The items will be moved to quarantine on the respective devices. You can delete the items from quarantine later, or restore them to their original locations. See **View and Manage Quarantined Items on Windows Devices** for more details.

Threats identified on Mac OS Devices:

First, select the items on which you want to take the action. Then click one of the following:

- **Delete Malware** - Will remove the malware from the device.
- **Quarantine Malware** - The items will be moved to quarantine on the respective devices. You can delete the items from quarantine later, or restore them to their original locations. See **View and Manage Quarantined Items on Mac OS Devices** for more details.

9.6. View and Manage Quarantined Items on Windows Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Windows Quarantine' to open the quarantine interface

- You can take actions on quarantined files and/or assign ratings to them

How do threats get quarantined?

Real time scans - Threats will be placed in quarantine if:

- 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action in the profile 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 quarantined the threat at an alert.
- See **Realtime Scan settings** in the section **Antivirus Settings** under **Creating Windows Profile**

On-demand / Scheduled scans - Threats will be placed in quarantine if:

- 'Automatically clean threats' is enabled and 'Quarantine' is set as the action in the profile on the device.
- See **Custom Scans** in **Antivirus Settings** if you need more help with this.

Manual quarantine:

- Admins can move threats to quarantine from the 'Current Malware List' interface.
- End-users can move files to quarantine on their endpoint.
- See **View and Manage Identified Malware** for more details.

Quarantined items are encrypted and not allowed to run.

The 'Windows Quarantine' interface lists all items quarantined by CCS enrolled endpoints.

Administrators can:

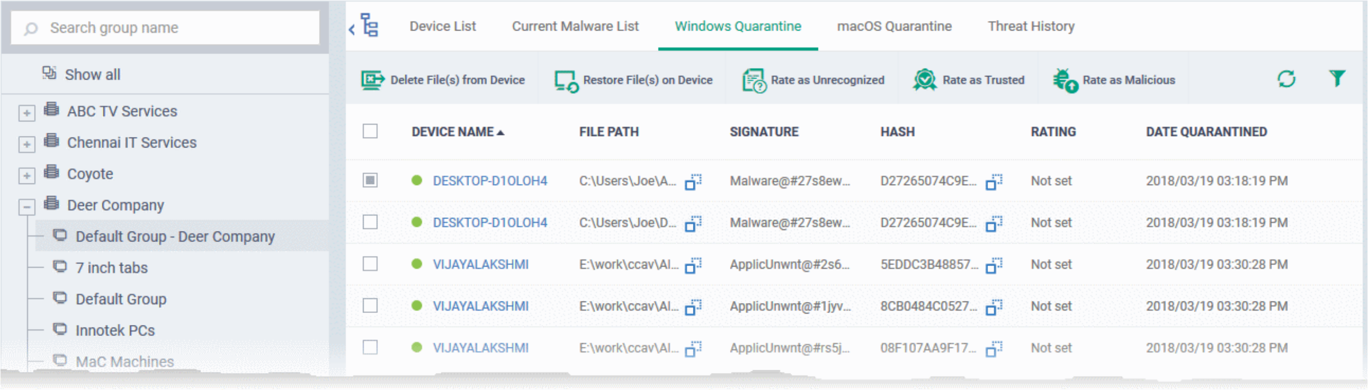
- Assign a rating to quarantined files (trusted, malicious or unrecognized)
- Delete them permanently
- Restore them to their original location

Files rated as 'Trusted' will be restored to their original location and awarded a 'Trusted' rating in the local CCS database.

To open the 'Windows Quarantine' interface

- Click 'Security Sub-Systems' on the left then choose 'Antivirus'
- Click the 'Windows Quarantine' tab
  - Click a company name then a group in the middle pane to view malware identified on devices in a particular group

    Or
  - Select 'Show All' on the left menu to view malware identified on all devices enrolled to ITSM



	DEVICE NAME ▲	FILE PATH	SIGNATURE	HASH	RATING	DATE QUARANTINED
☒	● DESKTOP-D1OLOH4	C:\Users\Joe\A...	Malware@#27s8ew...	D27265074C9E...	Not set	2018/03/19 03:18:19 PM
□	● DESKTOP-D1OLOH4	C:\Users\Joe\D...	Malware@#27s8ew...	D27265074C9E...	Not set	2018/03/19 03:18:19 PM
□	● VIJAYALAKSHMI	E:\work\ccav\Al...	ApplicUnwnt@#2s6...	5EDDC3B48857...	Not set	2018/03/19 03:30:28 PM
□	● VIJAYALAKSHMI	E:\work\ccav\Al...	ApplicUnwnt@#1jyv...	8CB0484C0527...	Not set	2018/03/19 03:30:28 PM
□	● VIJAYALAKSHMI	E:\work\ccav\Al...	ApplicUnwnt@#rs5j...	08F107AA9F17...	Not set	2018/03/19 03:30:28 PM

The 'Windows Quarantine' List - Table of Column Descriptions	
Column Heading	**Description**
Device Name	The label assigned to the device. If no name is assigned by the device user, then the model number of the device will be used. A gray text color indicates the device has been offline for 24 hours. • Click the device name to view granular details about the device. • See **Manage Windows Devices** for more details.
File Path	The installation path of the infected application. • Click the ⧉ icon to copy 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 • Click the ⧉ icon to copy the hash value to the clipboard.
Rating	The file's trust level as rated by CCS.
Date Quarantined	Date and time at which the malware was quarantined on the device.

The Windows Quarantine interface allows you to:

- **Restore False Positives from Quarantine**
- **Remove Malware files from the devices**
- **Rate files as 'Unrecognized', 'Trusted' or 'Malicious'**

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.
- Click 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.

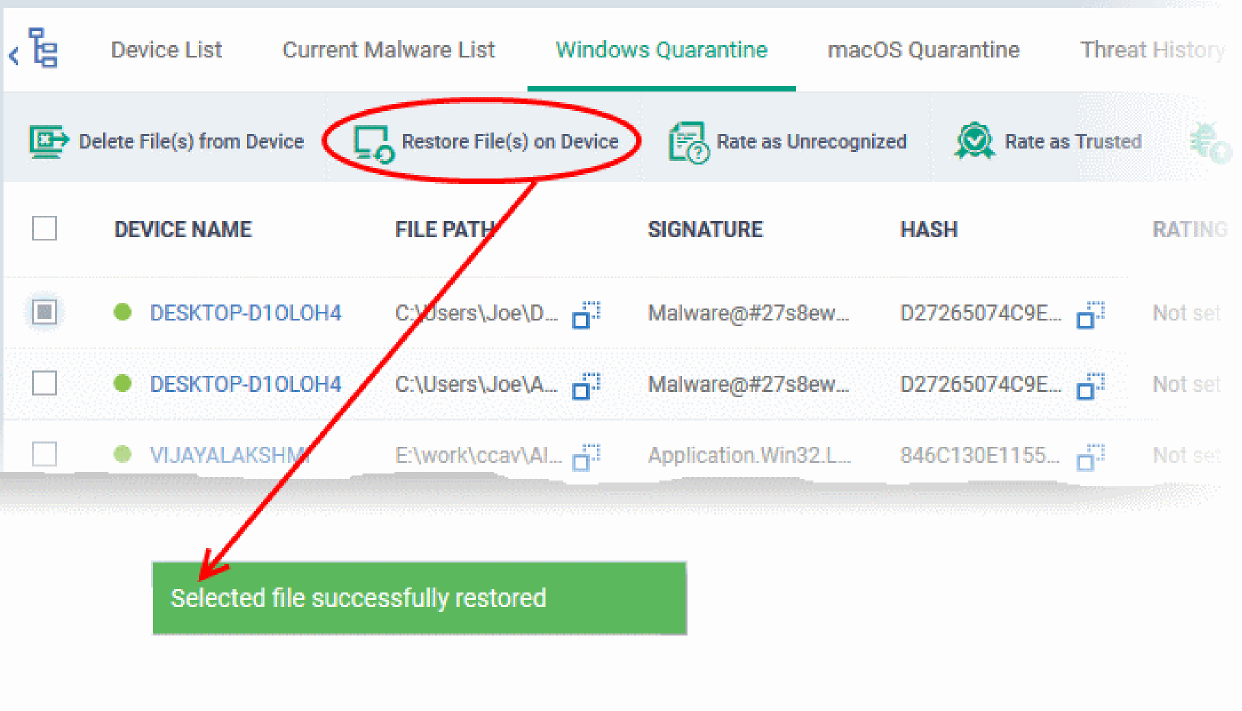
Manage Quarantined Items

- If your review confirms that a quarantined item is a genuine threat then it can be deleted from endpoints.
- Conversely, if an item is is found to be a false positive, you can restore it to its original location.
- You can also rate a file as unrecognized, trusted or malicious based on your assessment. The new verdict will be sent to all endpoints and will be reflected in the 'Unrecognized' and 'Trusted' interfaces.

Restore 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.

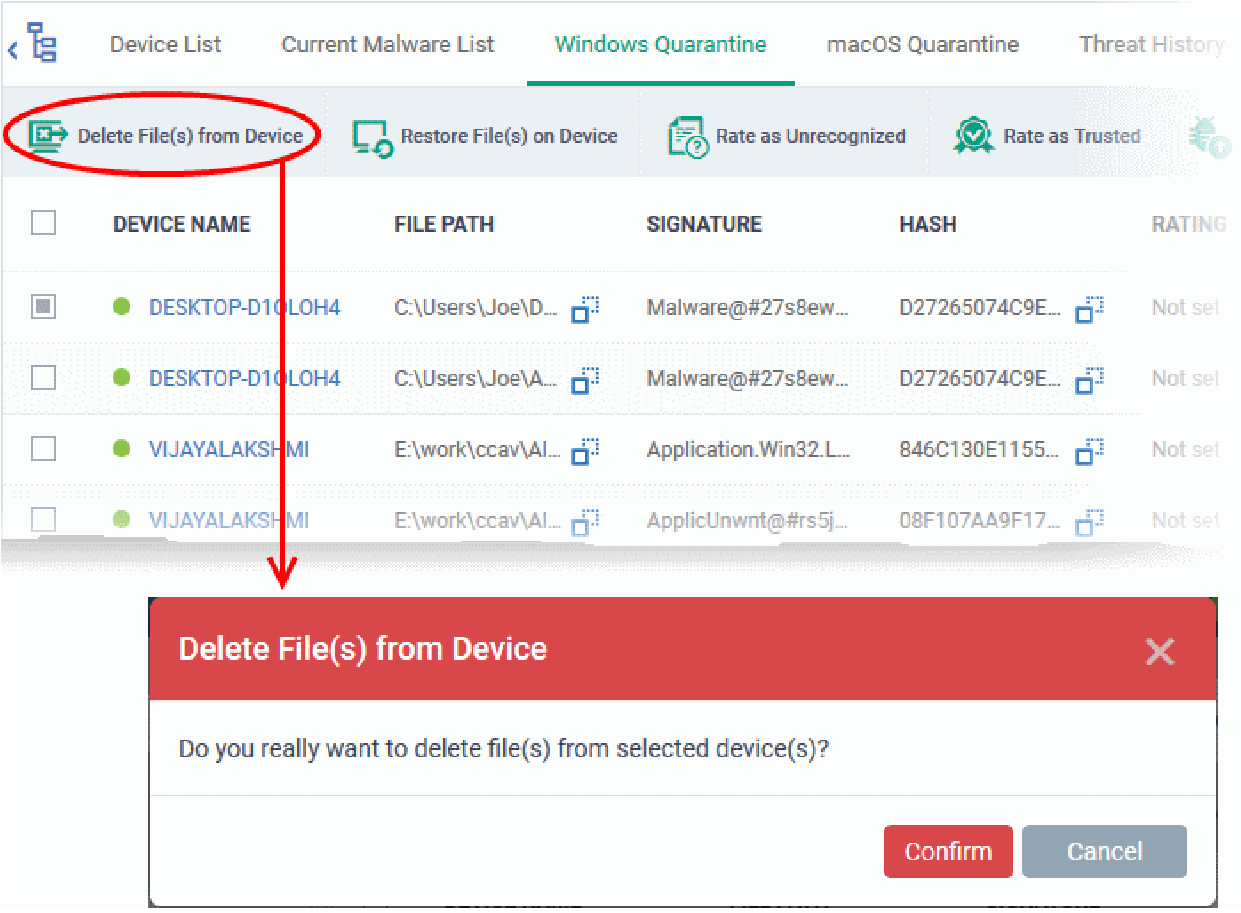


□	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING
☑	DESKTOP-D1OLOH4	C:\Users\Joe\D...	Malware@#27s8ew...	D27265074C9E...	Not set
□	DESKTOP-D1OLOH4	C:\Users\Joe\A...	Malware@#27s8ew...	D27265074C9E...	Not set
□	VIJAYALAKSHMI	E:\work\ccav\Al...	Application.Win32.L...	846C130E1155...	Not set

Selected file successfully restored

Remove Malware files from the devices

- Select it from the list and click 'Delete File From Device' from the options at the top.



☐	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING
☒	● DESKTOP-D1OLOH4	C:\Users\Joe\D...	Malware@#27s8ew...	D27265074C9E...	Not set
☐	● DESKTOP-D1OLOH4	C:\Users\Joe\A...	Malware@#27s8ew...	D27265074C9E...	Not set
☐	● VIJAYALAKSHMI	E:\work\ccav\Al...	Application.Win32.L...	846C130E1155...	Not set
☐	● VIJAYALAKSHMI	E:\work\ccav\Al...	ApplicUnwnt@#rs5j...	08F107AA9F17...	Not set

Delete File(s) from Device

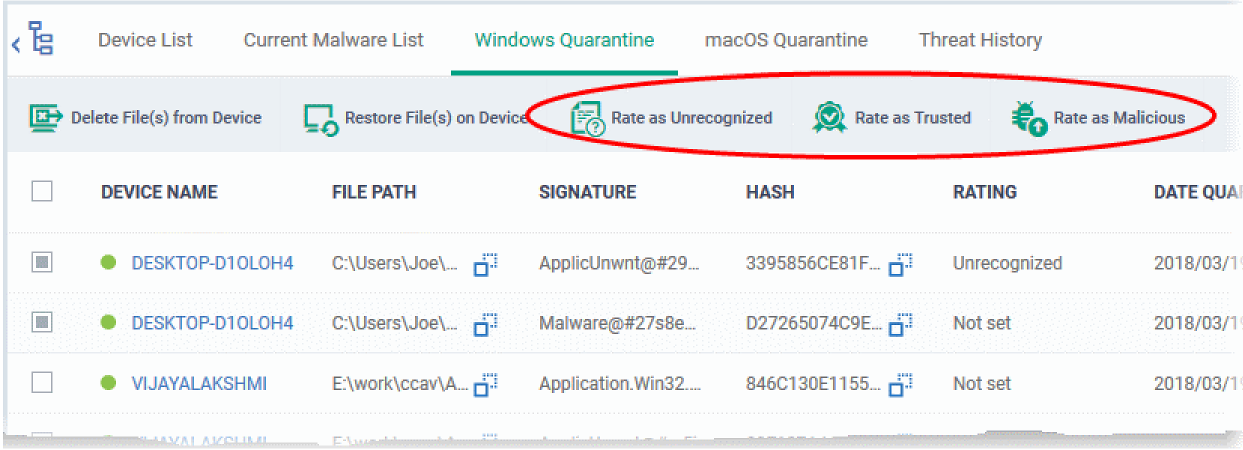
Do you really want to delete file(s) from selected device(s)?

- Click 'Confirm' in the confirmation dialog.

The file will be deleted from the device at which it was quarantined and from the list.

Rate files as 'Unrecognized', 'Trusted' or 'Malicious'

- If the rating of a quarantined file is changed to 'Trusted' or 'Unrecognized', the file is restored to its original location. The new rating is also stored in the CCS database on the device.
- To change the rating of a quarantined file, select it and click the appropriate button at the top:



☐	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING	DATE QUA
☒	● DESKTOP-D1OLOH4	C:\Users\Joe\...	ApplicUnwnt@#29...	3395856CE81F...	Unrecognized	2018/03/1
☒	● DESKTOP-D1OLOH4	C:\Users\Joe\...	Malware@#27s8e...	D27265074C9E...	Not set	2018/03/1
☐	● VIJAYALAKSHMI	E:\work\ccav\A...	Application.Win32....	846C130E1155...	Not set	2018/03/1

A confirmation will be displayed and the information will also be sent to the devices.

- Files rated as 'Malicious' will stay in quarantine on the device.
- Files rated as 'Unrecognized' will be restored to their original locations on the device. Future AV scans may flag them as 'malicious' again.

- Files rated as 'Trusted' will be restored to their original locations in the device. These files will be white-listed and skipped by future antivirus scans.

9.7. View and Manage Quarantined Items on Mac OS Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Mac OS Quarantine' to open the quarantine interface
- You can take actions on quarantined files and/or assign ratings to them

How do threats get quarantined on a MAC?

- 'Automatically quarantine threats found during scanning' is enabled in the antivirus section of the profile on the device
- 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 encrypted and not allowed to run.

See **Scanner Settings** in **Antivirus Settings for Mac OS Profile**, and **Viewing and Managing Identified Malware** for more details.

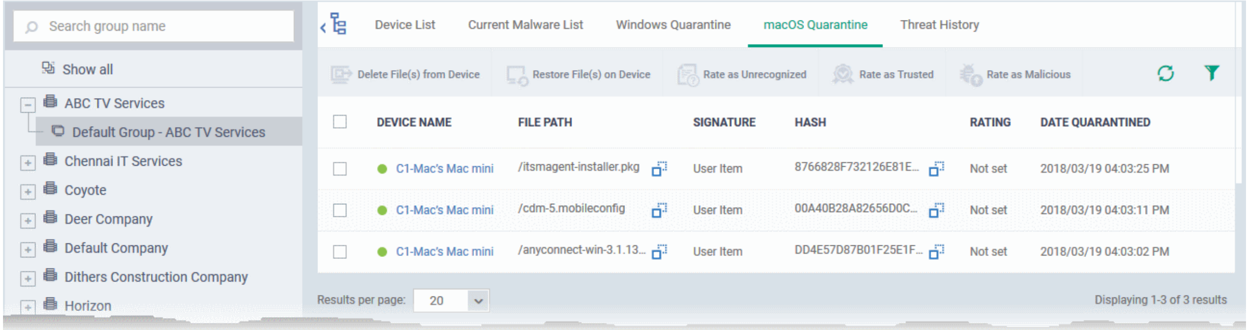
The 'Mac OS Quarantine' interface lists all items quarantined by CAVM on managed Mac OS endpoints.

Administrators can:

- Assign a rating to quarantined files (trusted, malicious or unrecognized)
- Delete them permanently
- Restore them to their original location

To open the Quarantine Files interface

- Click 'Security Sub-Systems' on the left and choose 'Antivirus' from the options
- Click the 'Mac OS Quarantine' tab



□	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING	DATE QUARANTINED
□	● C1-Mac's Mac mini	/itsmagent-installer.pkg	User Item	8766828F732126E81E...	Not set	2018/03/19 04:03:25 PM
□	● C1-Mac's Mac mini	/cdm-5.mobileconfig	User Item	00A40B28A82656D0C...	Not set	2018/03/19 04:03:11 PM
□	● C1-Mac's Mac mini	/anyconnect-win-3.1.13...	User Item	DD4E57D87B01F25E1F...	Not set	2018/03/19 04:03:02 PM

The 'Mac OS Quarantine' List - Table of Column Descriptions	
Column Heading	**Description**
Device Name	The label assigned to the device. If no name was assigned by the end-user, the model number of the device is used. A gray text color indicates the device has been offline for the past 24 hours. • Click the device name to view granular details about the device.

	• See **Manage Mac OS Devices** for more details.
File Path	The installation path of the infected application. • Click the ⧉ icon to copy 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 • Click the ⧉ icon to copy 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	Date and time at which the malware was quarantined on the device.

The 'Mac OS Quarantine' interface allows you to:

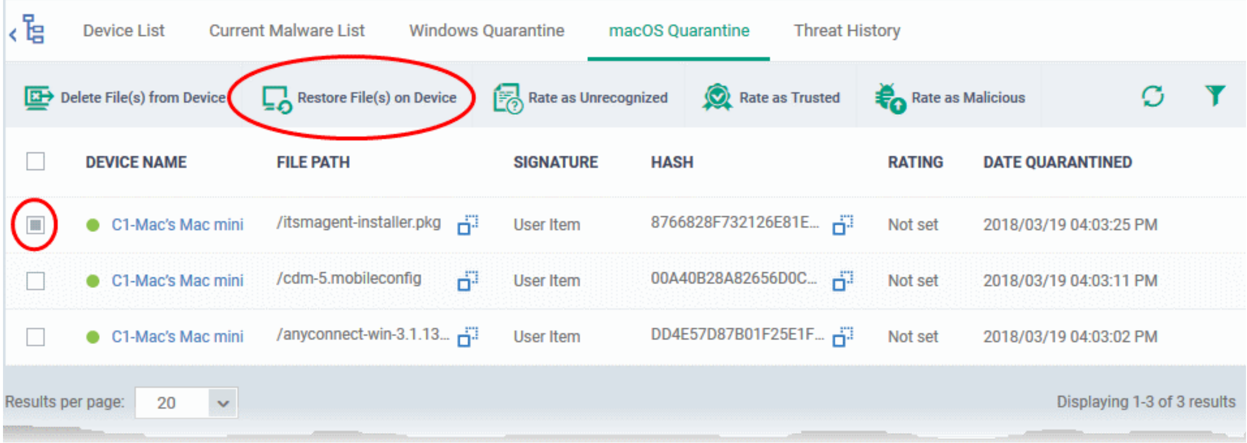
- **Restore False Positives from Quarantine**
- **Remove Malware files from the devices**
- **Rate files as 'Unrecognized', 'Trusted' or 'Malicious'**

Manage Quarantined Items

- If your review confirms that a quarantined item is a genuine threat then it can be deleted from endpoints.
- Conversely, if an item is is found to be a false positive, you can restore it to its original location.
- You can also rate a file as unrecognized, trusted or malicious based on your assessment. The rating applies only to Windows based files quarantined by Mac OS devices.
  - Files rated as 'Trusted' will restored to their original location.
  - The file rating will apply to all managed endpoints, regardless of operating system. If a file originally found on a MAC is subsequently discovered on a Windows device, it will be awarded the same rating on the Windows device.

Restore 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.



☐	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING	DATE QUARANTINED
☑	● C1-Mac's Mac mini	/itsmagent-installer.pkg ⧉	User Item	8766828F732126E81E... ⧉	Not set	2018/03/19 04:03:25 PM
☐	● C1-Mac's Mac mini	/cdm-5.mobileconfig ⧉	User Item	00A40B28A82656D0C... ⧉	Not set	2018/03/19 04:03:11 PM
☐	● C1-Mac's Mac mini	/anyconnect-win-3.1.13... ⧉	User Item	DD4E57D87B01F25E1F... ⧉	Not set	2018/03/19 04:03:02 PM

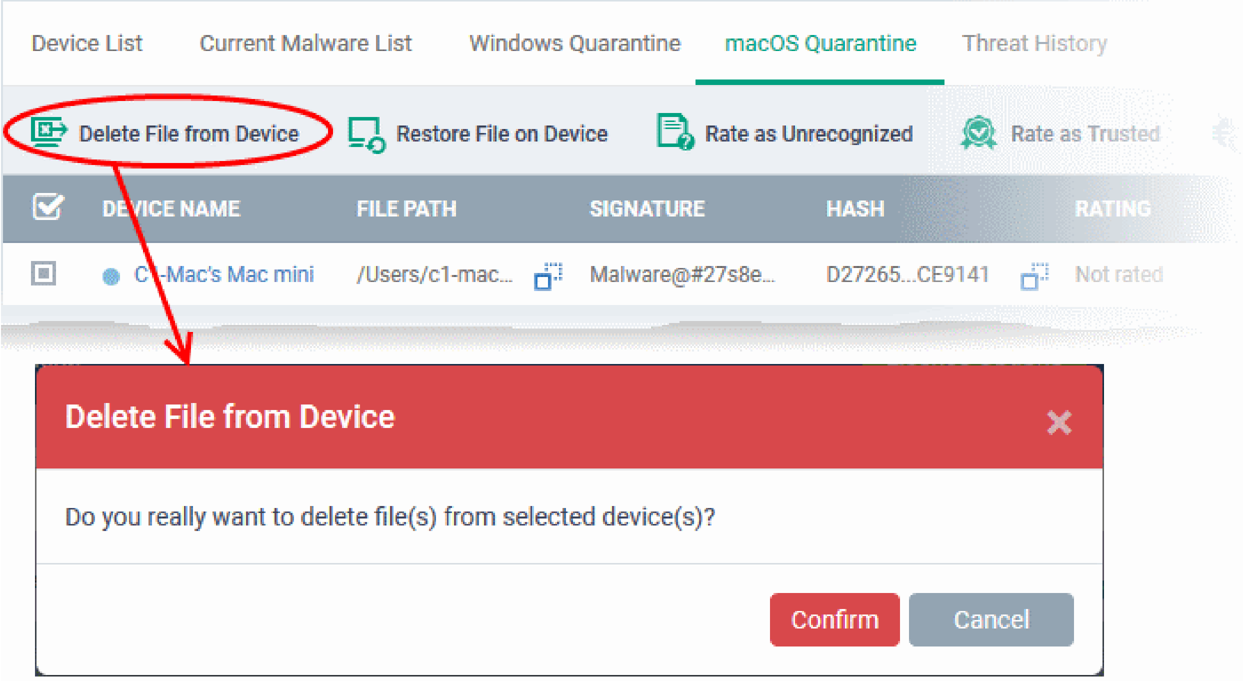
Results per page: 20

Displaying 1-3 of 3 results

The item will be restored to its original location from the quarantine and removed from the list.

Remove Malware files from the devices

- Select the item to be removed from the device from the list and click 'Delete File From Device'.



☑	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING
□	C1-Mac's Mac mini	/Users/c1-mac...	Malware@#27s8e...	D27265...CE9141	Not rated

Delete File from Device

Do you really want to delete file(s) from selected device(s)?

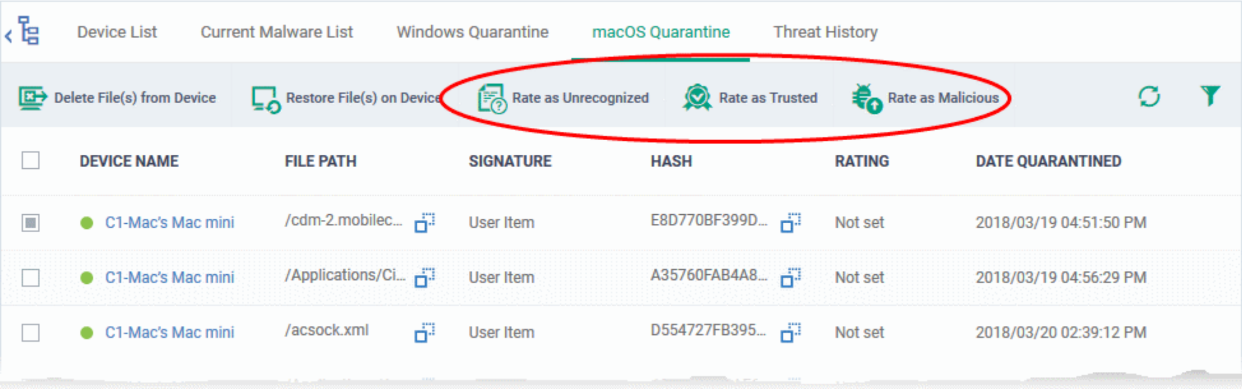
- Click 'Confirm' in the confirmation dialog.

The file will be deleted from the device at which it was quarantined and from the list.

Rate files as 'Unrecognized', 'Trusted' or 'Malicious'

ITSM allows administrators to change the trust rating of a files quarantined by Mac OS devices from this interface.

- The file rating applies only to Windows based files quarantined by Mac OS devices.
    - Files rated as 'Trusted' will be restored to their original location
    - The file rating will apply to all managed endpoints, regardless of operating system. If a file originally found on a MAC is subsequently discovered on a Windows device, it will be awarded the same rating on the Windows device.
- To change the file rating of a quarantined file, select it and click the respective rating button at the top



□	DEVICE NAME	FILE PATH	SIGNATURE	HASH	RATING	DATE QUARANTINED
☒	C1-Mac's Mac mini	/cdm-2.mobilec...	User Item	E8D770BF399D...	Not set	2018/03/19 04:51:50 PM
□	C1-Mac's Mac mini	/Applications/Ci...	User Item	A35760FAB4A8...	Not set	2018/03/19 04:56:29 PM
□	C1-Mac's Mac mini	/acsock.xml	User Item	D554727FB395...	Not set	2018/03/20 02:39:12 PM

A confirmation message is shown and the information will also be sent to all endpoints.

9.8. View Threat History

- Click 'Security Sub-Systems' > 'Antivirus' > 'Threat History' to view all malware discovered on devices since you deployed ITSM.

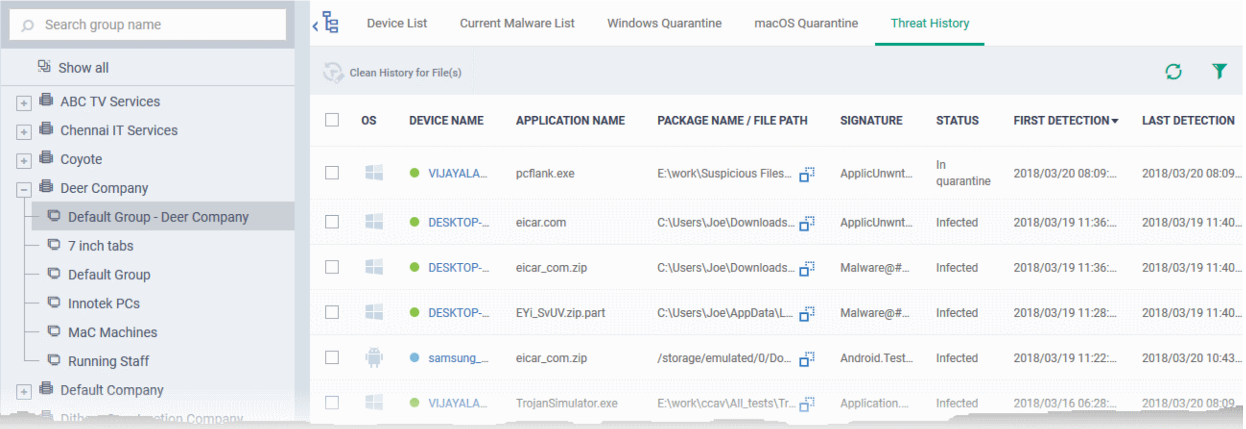
The 'Threat History' interface is a log of all malicious items found on Android, Windows and Mac OS devices over time. The list shows items that have been removed from devices and those which are still present.

- You can remove unnecessary entries from the list

To view threat history

- Choose 'Security Sub-systems' on the left then select 'Antivirus'.
- Click the 'Threat History' tab.
  - Click a company name then a group in the middle pane to view a log of malware identified on devices in a particular group

    Or
  - Select 'Show All' on the left menu to view a log of malware identified on all devices enrolled to ITSM



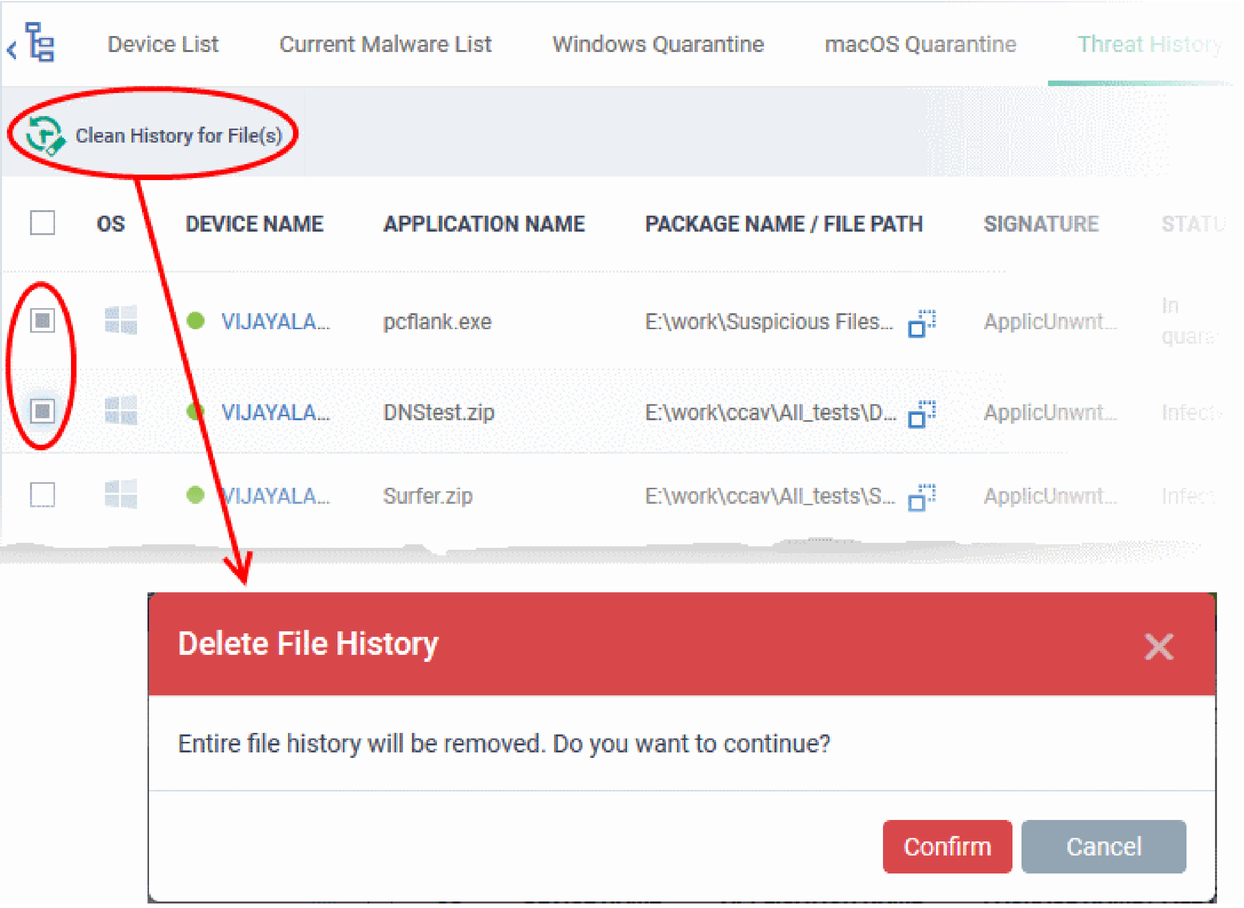
□	OS	DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	SIGNATURE	STATUS	FIRST DETECTION ▾	LAST DETECTION
□		● VIJAYALA...	pcflank.exe	E:\work\Suspicious Files...	ApplicUnwnt...	In quarantine	2018/03/20 08:09:...	2018/03/20 08:09...
□		● DESKTOP-...	eicar.com	C:\Users\Joe\Downloads...	ApplicUnwnt...	Infected	2018/03/19 11:36:...	2018/03/19 11:40...
□		● DESKTOP-...	eicar_com.zip	C:\Users\Joe\Downloads...	Malware@#...	Infected	2018/03/19 11:36:...	2018/03/19 11:40...
□		● DESKTOP-...	EYi_SvUV.zip.part	C:\Users\Joe\AppData\L...	Malware@#...	Infected	2018/03/19 11:28:...	2018/03/19 11:40...
□		● samsung_...	eicar_com.zip	/storage/emulated/0/Do...	Android.Test...	Infected	2018/03/19 11:22:...	2018/03/20 10:43...
□		● VIJAYALA...	TrojanSimulator.exe	E:\work\ccav\All_tests\Tr...	Application....	Infected	2018/03/16 06:28:...	2018/03/20 08:09...

Antivirus Threat History - Column Descriptions	
Column Heading	**Description**
OS	Indicates the operating system of the device on which the malware was found.
Device Name	The label assigned to the device. If no name was assigned by the end-user, the model number of the device is used. A gray text color indicates the device has been offline for the past 24 hours. • Click the device name to view granular details about the device. • See **Manage Windows Devices**, **Manage Mac OS Devices** and **Manage Android / iOS 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 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.

To remove unwanted entries from the 'Threat History' interface

- Select the log entry(ies) to be removed and click Clean History for File(s) at the top



Entire file history will be removed. Do you want to continue?

- Click 'Confirm' to remove the entries from the list
- Deleting file history will only remove the log entry. The file will not be removed from the device or from any other interfaces in which it is listed (for example, the quarantine list).

Sorting, Search and Filter Options

- Click any column header to sort items in ascending/descending order of the entries in that column
- Click the funnel icon on the right to filter items by various criteria, including by OS, device name, application name, package name/file path, signature, status and first/last detection dates.
- Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.
- By default ITSM returns 20 results per page when you perform a search. Click the arrow next to the 'Results per page' drop-down to increase results up to a maximum of 200.

9.9. View History of External Device Connection Attempts

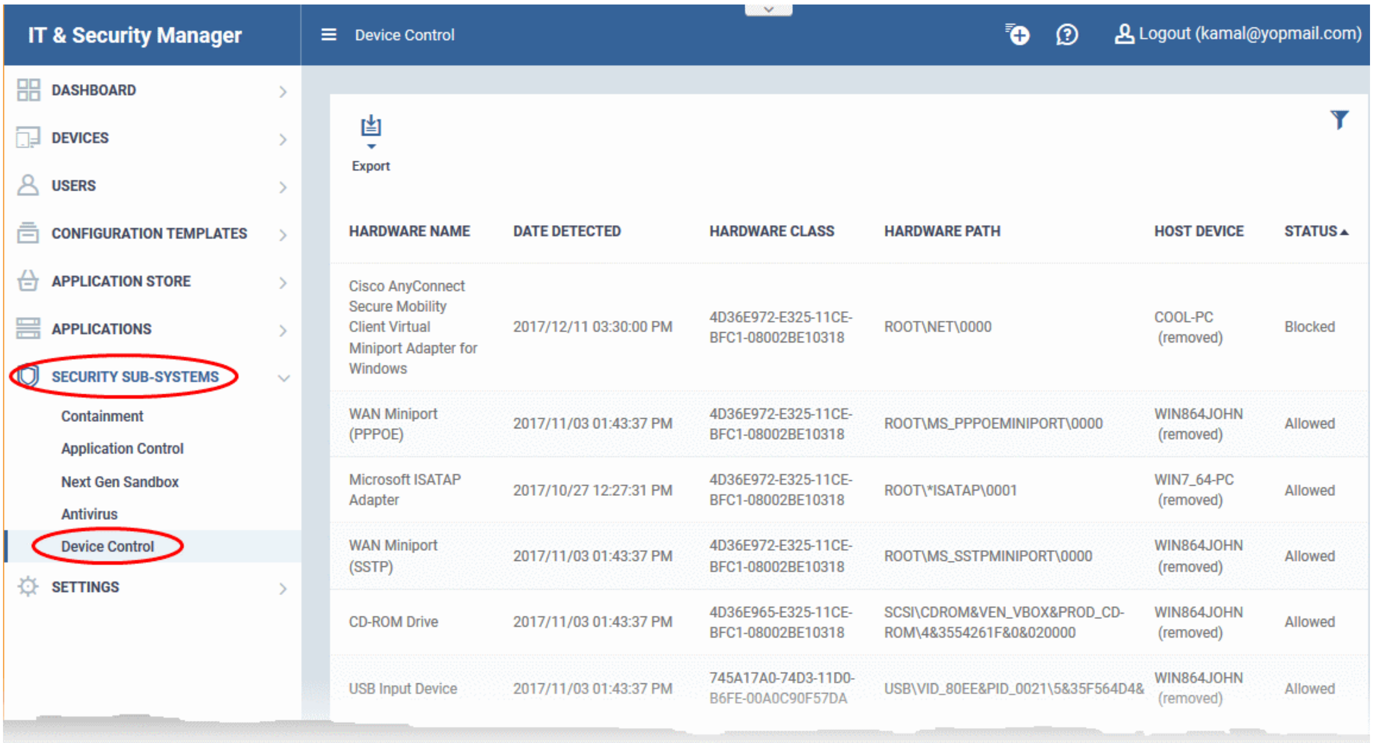
- Click 'Security Sub-Systems' > 'Device Control' to view all connection attempts from external devices to your Windows endpoints
- ITSM can create a log entry when an external device attempts to connect to a Windows endpoint. External

devices include USB devices, DVD drives, printers, Bluetooth devices etc.

- These logs are created when the Windows profile contains the 'External Devices Control' section. See **External Devices Control Settings** for more details.
- You can also generate a report of external device connection attempts.

To view a history of device connections:

- Click 'Security Sub-Systems' on the left then select 'Device Control'



HARDWARE NAME	DATE DETECTED	HARDWARE CLASS	HARDWARE PATH	HOST DEVICE	STATUS ▲
Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows	2017/12/11 03:30:00 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT\NET\0000	COOL-PC (removed)	Blocked
WAN Miniport (PPPOE)	2017/11/03 01:43:37 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT\MS_PPPOEMINIPORT\0000	WIN864JOHN (removed)	Allowed
Microsoft ISATAP Adapter	2017/10/27 12:27:31 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT*ISATAP\0001	WIN7_64-PC (removed)	Allowed
WAN Miniport (SSTP)	2017/11/03 01:43:37 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT\MS_SSTPMINIPORT\0000	WIN864JOHN (removed)	Allowed
CD-ROM Drive	2017/11/03 01:43:37 PM	4D36E965-E325-11CE-BFC1-08002BE10318	SCSI\CDROM&VEN_VBOX&PROD_CD-ROM\4&3554261F&0&020000	WIN864JOHN (removed)	Allowed
USB Input Device	2017/11/03 01:43:37 PM	745A17A0-74D3-11D0-B6FE-00A0C90F57DA	USB\VID_80EE&PID_0021\5&35F564D4&	WIN864JOHN (removed)	Allowed

Device Control - Column Descriptions	
Column Header	**Description**
Hardware Name	Displays the name of the external device which attempted to connect to a managed Windows device
Date Detected	The date and time at which the device was first detected
Hardware Class	The Globally Unique Identifier (GUID) of the device class which attempted to connect.
Hardware Path	The Device Instance Identifier of the external device which attempted to connect.
Host Device	The name of the Windows device to which the connection attempt was made. This column also shows the host's current connection status (connected or removed)
Status	Indicates whether the connection was allowed or blocked. This depends on the settings in the 'External Devices Control' section of the profile active on the host device.

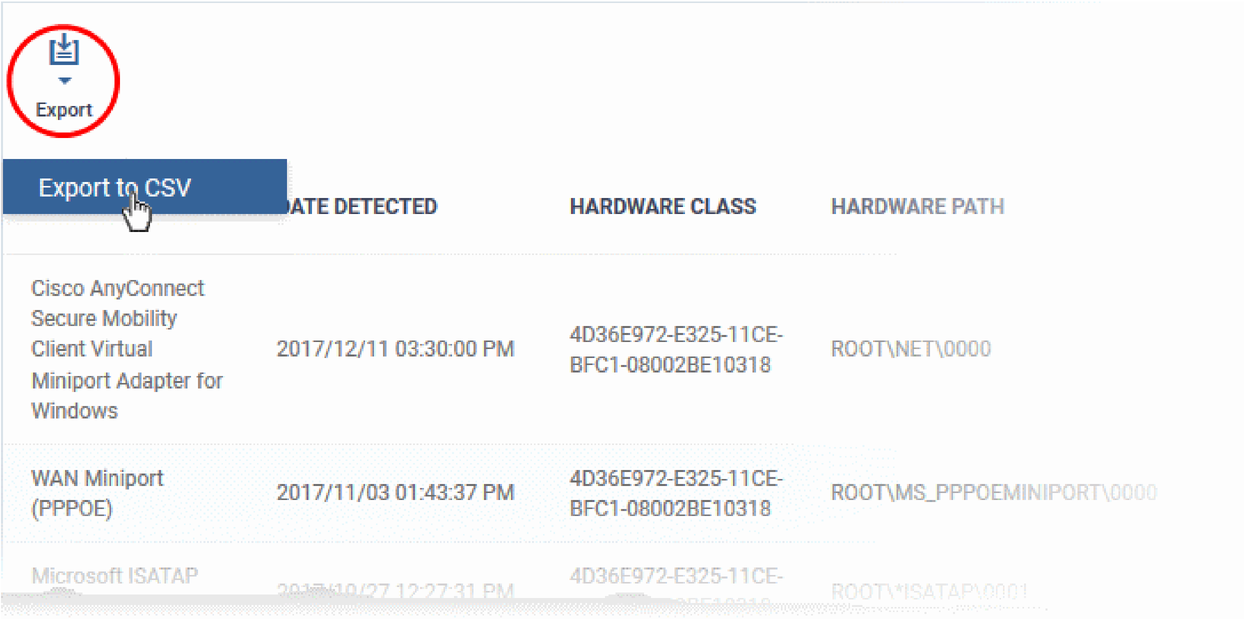
Sorting, Search and Filter Options

- 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 to filter the items based on device name, hardware class, hardware path, host, status and/or detection date.

- Enter the search criteria in the respective field 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.

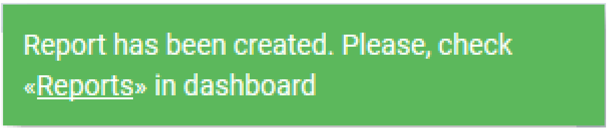
Generate a report containing log of device connection attempts

- Click 'Security Sub-Systems' > 'Containment'
- Click the funnel icon to apply filters to the report.
- Click the 'Export' button and choose 'Export to CSV':



	ATE DETECTED	HARDWARE CLASS	HARDWARE PATH
Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows	2017/12/11 03:30:00 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT\NET\0000
WAN Miniport (PPPOE)	2017/11/03 01:43:37 PM	4D36E972-E325-11CE-BFC1-08002BE10318	ROOT\MS_PPPOEMINIPORT\0000
Microsoft ISATAP	2017/10/27 12:27:31 PM	4D36E972-E325-11CE-	ROOT*ISATAP\0001

The report will be generated in .csv file format.



Report has been created. Please, check «Reports» in dashboard

The report can be accessed in the 'Dashboard' > 'Reports' interface. See **Reports** in **The Dashboard** if you need more help with this interface.

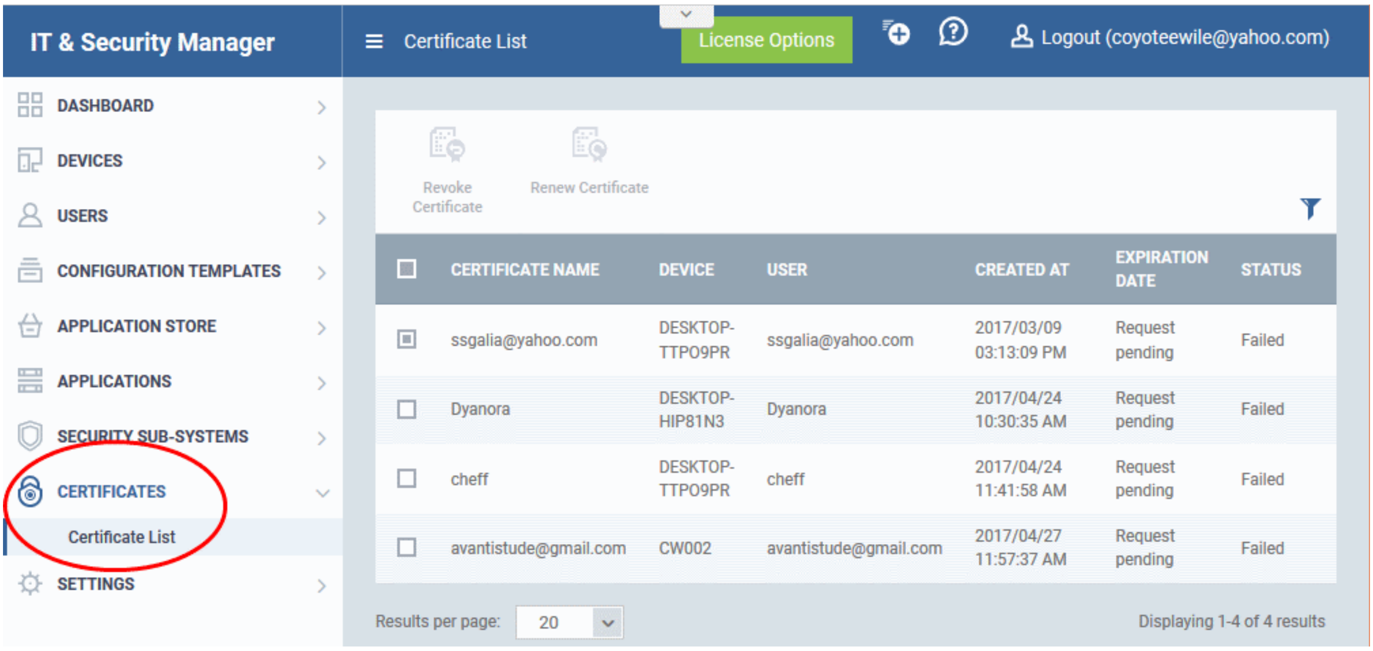
10. Manage Certificates Installed on Devices

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'



☐	CERTIFICATE NAME	DEVICE	USER	CREATED AT	EXPIRATION DATE	STATUS
☒	ssgalia@yahoo.com	DESKTOP-TTPO9PR	ssgalia@yahoo.com	2017/03/09 03:13:09 PM	Request pending	Failed
☐	Dyanora	DESKTOP-HIP81N3	Dyanora	2017/04/24 10:30:35 AM	Request pending	Failed
☐	cheff	DESKTOP-TTPO9PR	cheff	2017/04/24 11:41:58 AM	Request pending	Failed
☐	avantistude@gmail.com	CW002	avantistude@gmail.com	2017/04/27 11:57:37 AM	Request pending	Failed

Results per page: 20

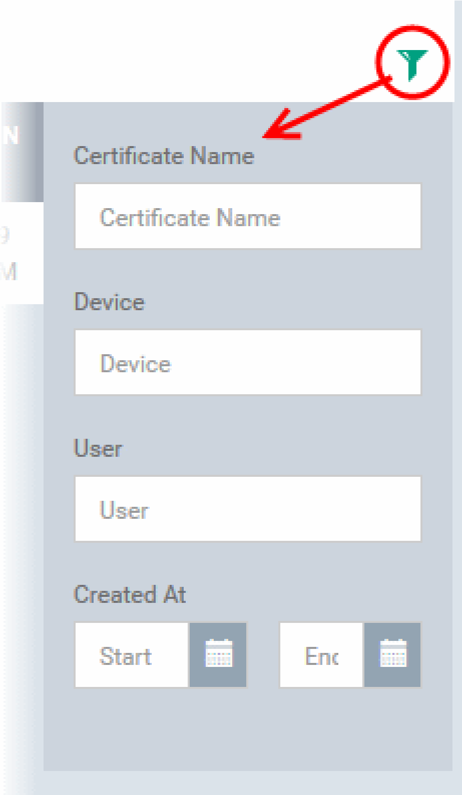
Displaying 1-4 of 4 results

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.

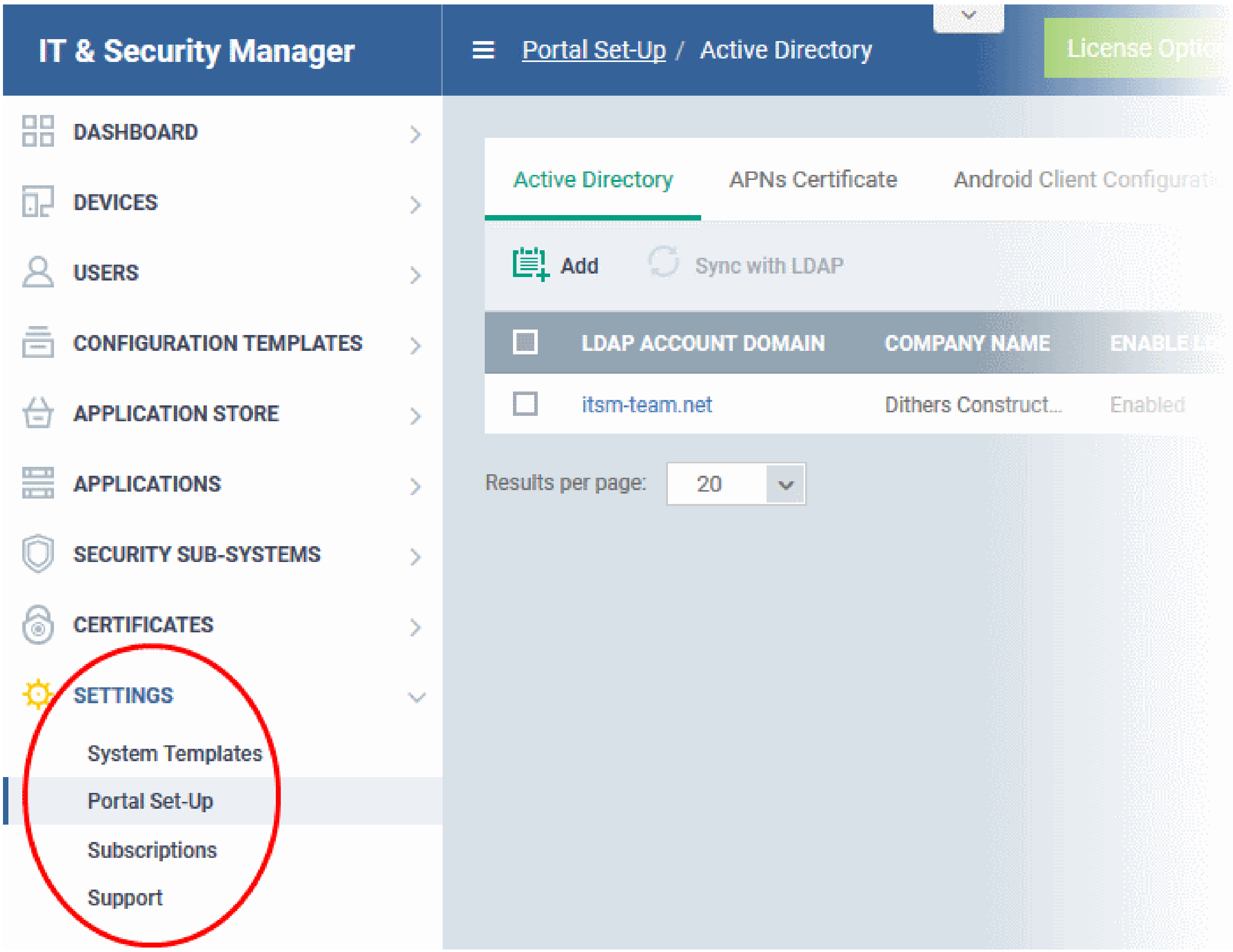
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default ITSM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

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. Configure 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.



□	LDAP ACCOUNT DOMAIN	COMPANY NAME	ENABLE LD
□	itsm-team.net	Dithers Construct...	Enabled

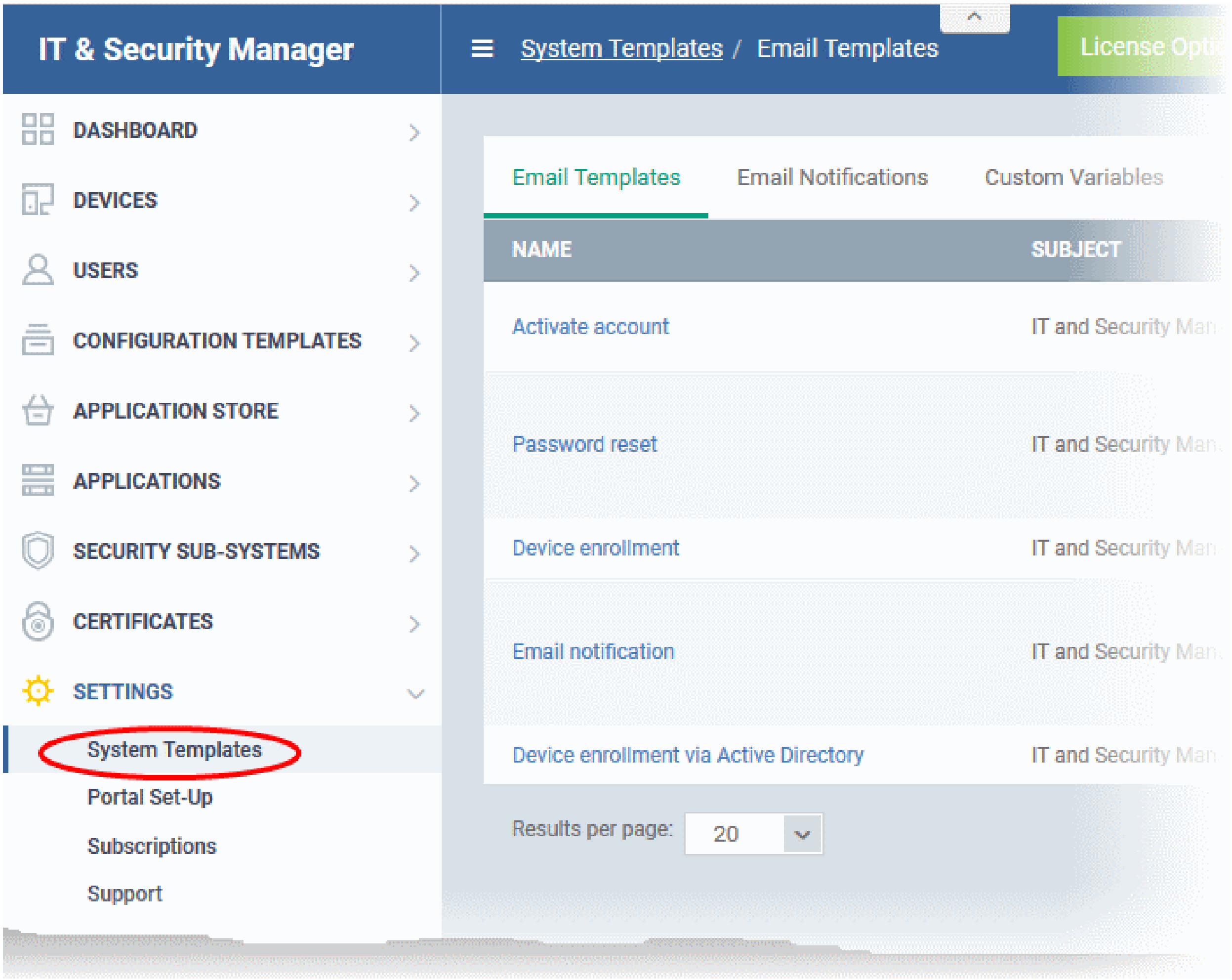
The following sections provide more details on each area:

- 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
    - 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

- Viewing and Managing Licenses
  - Upgrading or Adding a License
- Viewing Version and Support Information

11.1. Email Notifications, Templates and Custom Variables

The 'System Templates' area allows admins to manage email notifications and templates, and to specify variables and file groups that can be used in various profile settings.



NAME	SUBJECT
Activate account	IT and Security Man
Password reset	IT and Security Man
Device enrollment	IT and Security Man
Email notification	IT and Security Man
Device enrollment via Active Directory	IT and Security Man

The following sections explain more about:

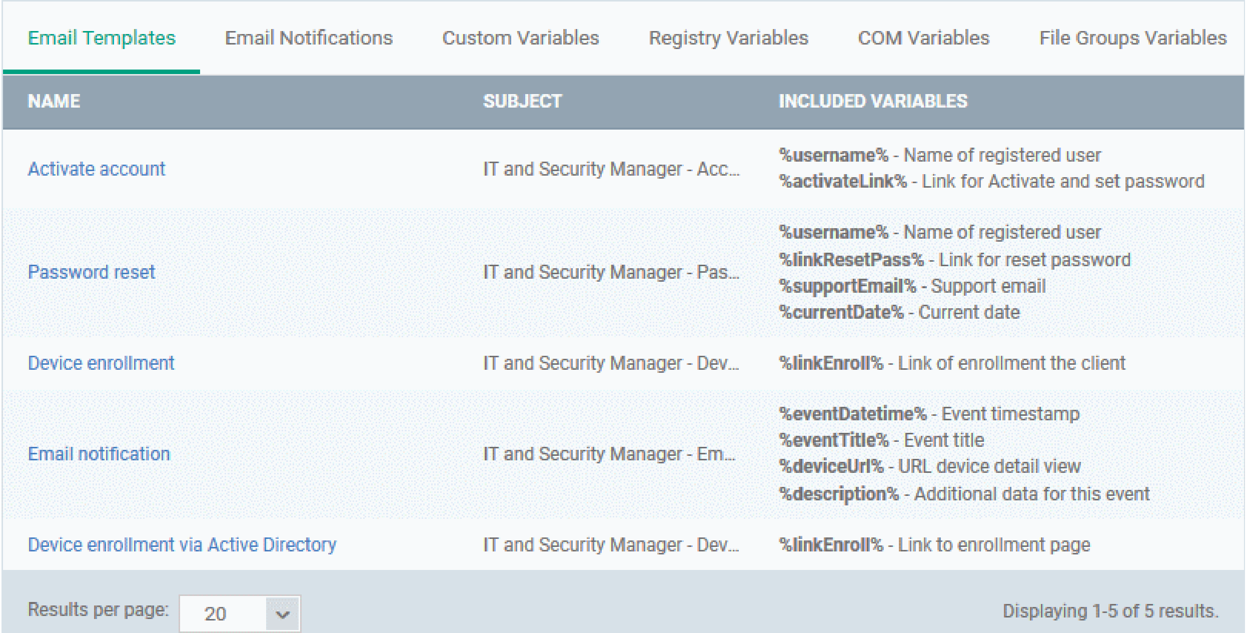
- Configuring Email Templates
- Configuring Email Notifications
- Creating and Managing Custom Variables
- Creating and Managing Registry Groups
- Creating and Managing COM Groups
- Creating and Managing File Groups

11.1.1. Configure 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



NAME	SUBJECT	INCLUDED VARIABLES
Activate account	IT and Security Manager - Acc...	**%username%** - Name of registered user **%activateLink%** - Link for Activate and set password
Password reset	IT and Security Manager - Pas...	**%username%** - Name of registered user **%linkResetPass%** - Link for reset password **%supportEmail%** - Support email **%currentDate%** - Current date
Device enrollment	IT and Security Manager - Dev...	**%linkEnroll%** - Link of enrollment the client
Email notification	IT and Security Manager - Em...	**%eventDatetime%** - Event timestamp **%eventTitle%** - Event title **%deviceUrl%** - URL device detail view **%description%** - Additional data for this event
Device enrollment via Active Directory	IT and Security Manager - Dev...	**%linkEnroll%** - Link to enrollment page

Results per page: 20

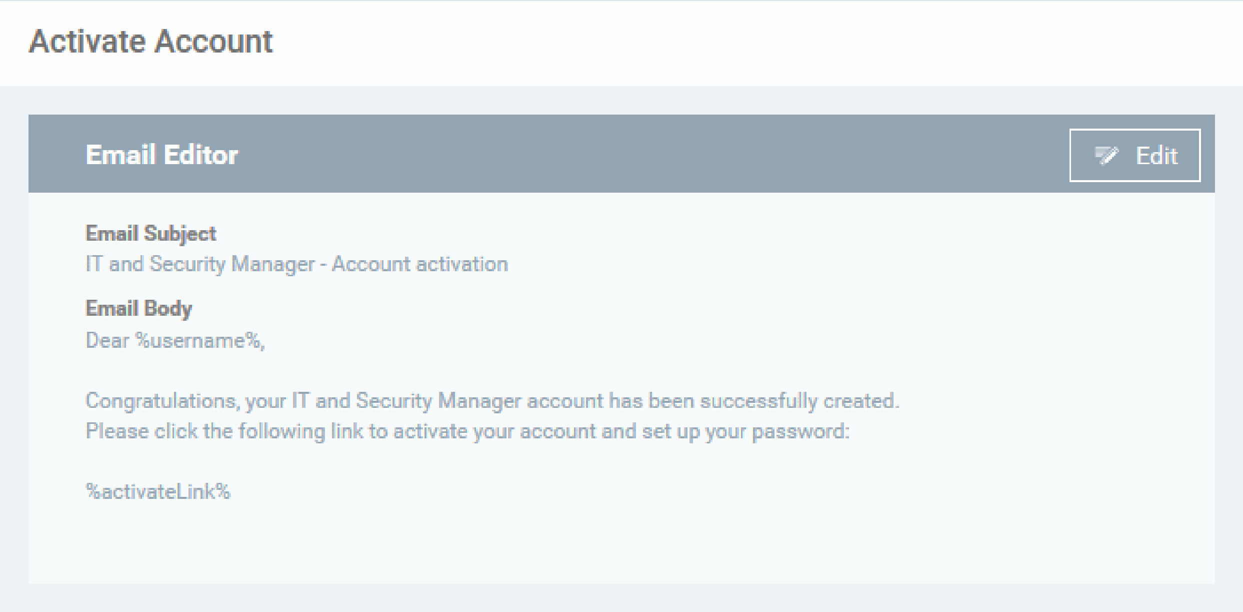
Displaying 1-5 of 5 results.

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:



Activate Account

Email Editor

Email Subject

IT and Security Manager - Account activation

Email Body

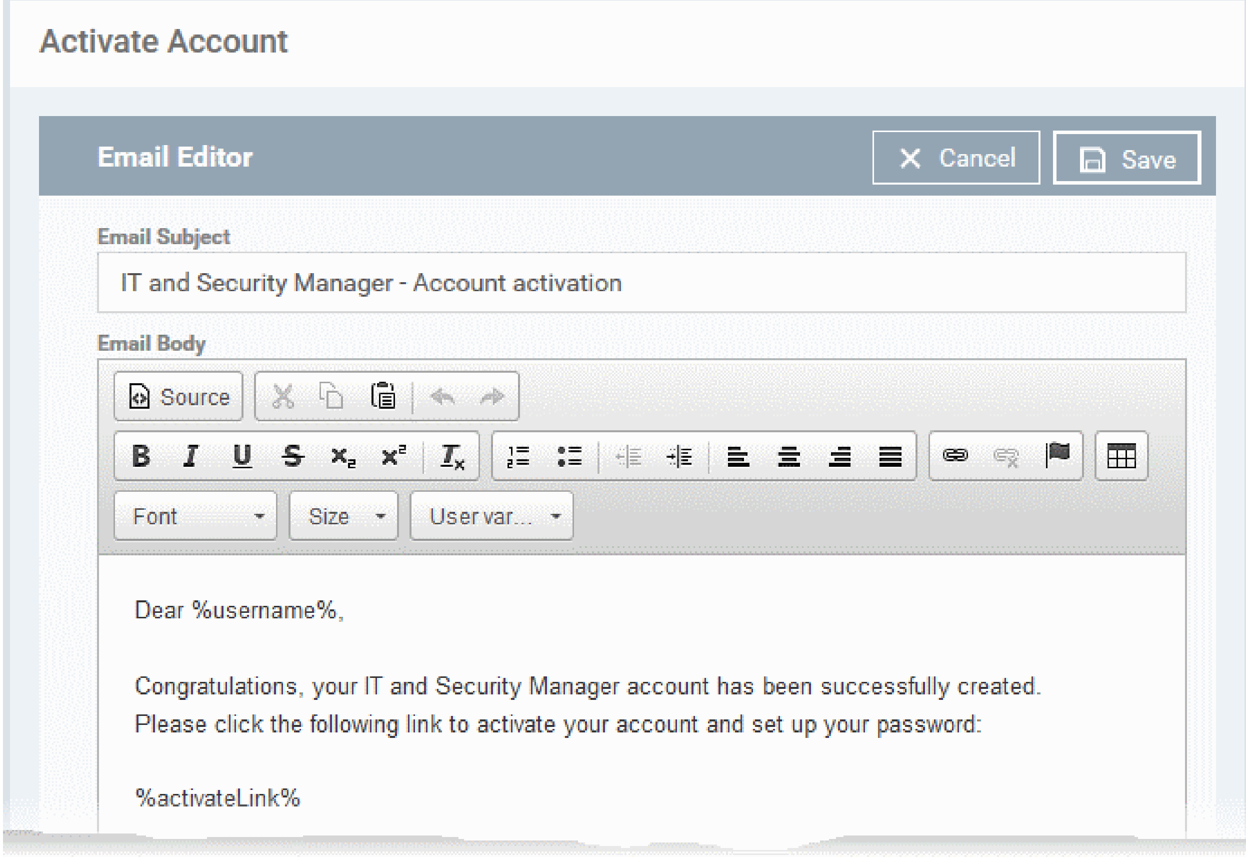
Dear %username%,

Congratulations, your IT and Security Manager account has been successfully created.
Please click the following link to activate your account and set up your password:

%activateLink%

- To edit the subject line and the message, click the edit button Edit on the top right.

The 'Email Editor' window will open.



Activate Account

Email Editor

Email Subject

IT and Security Manager - Account activation

Email Body

Dear %username%,

Congratulations, your IT and Security Manager account has been successfully created.
Please click the following link to activate your account and set up your password:

%activateLink%

- 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.

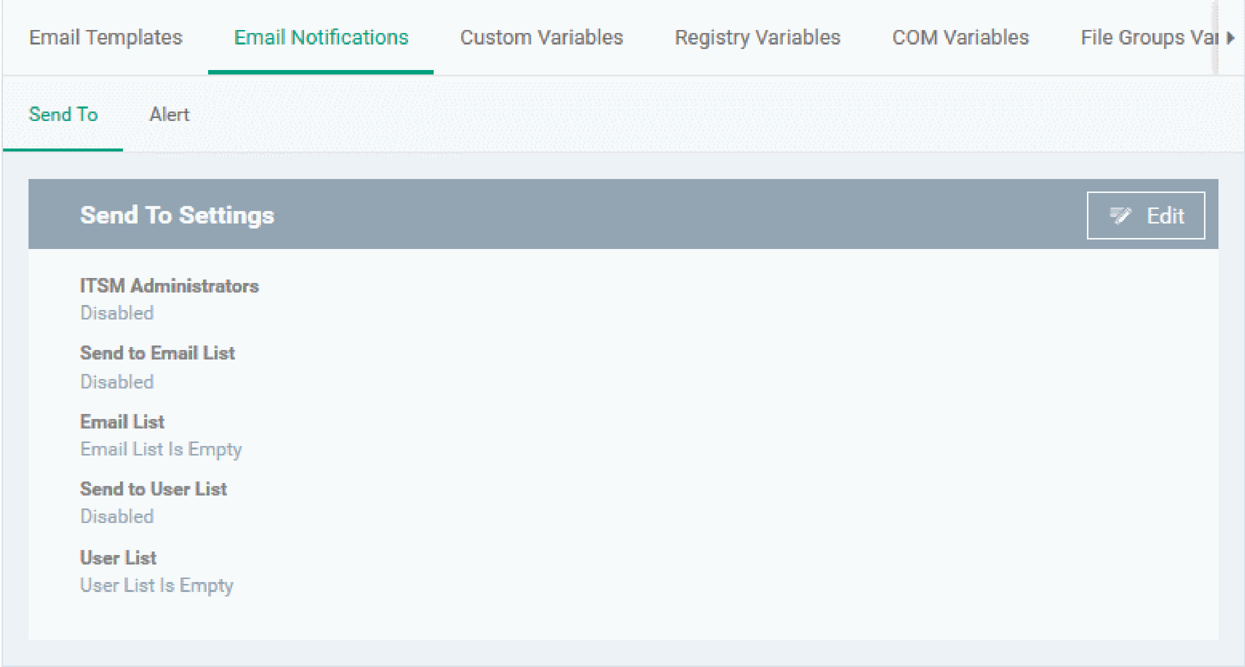
- Click the 'Save' button for your changes to take effect.

11.1.2. Configure 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



ITSM Administrators
Disabled

Send to Email List
Disabled

Email List
Email List Is Empty

Send to User List
Disabled

User List
User List Is Empty

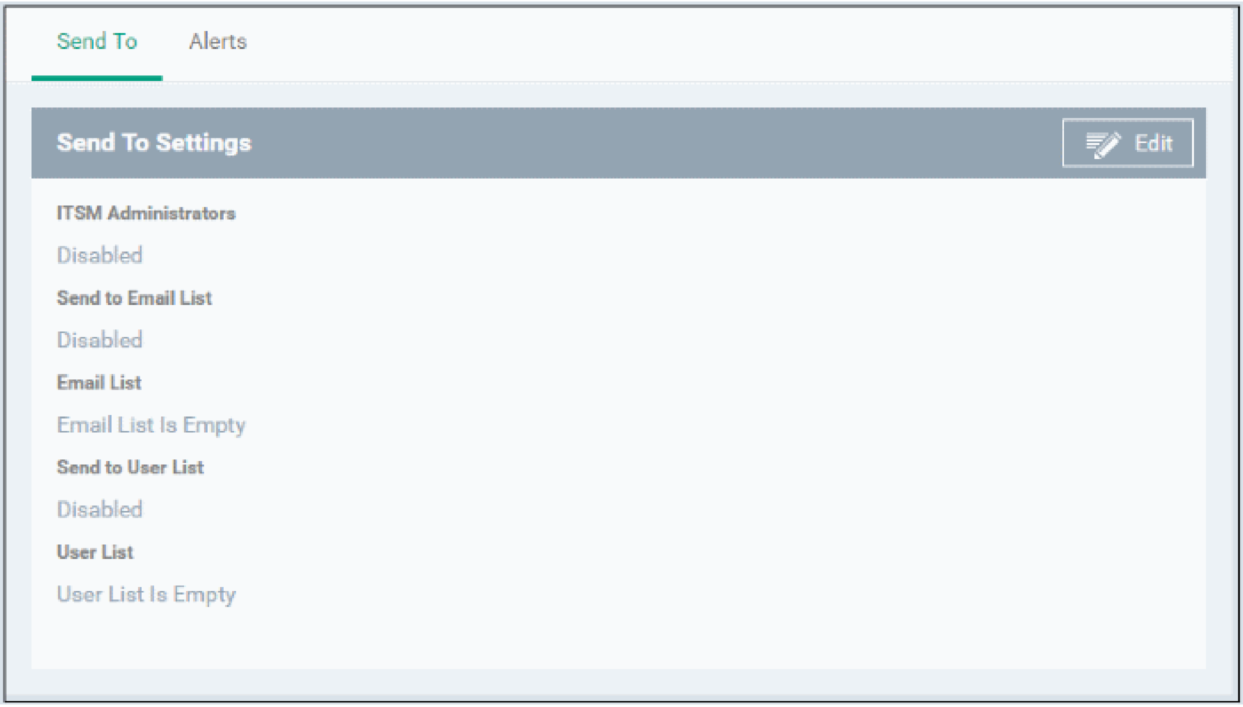
The interface contains two tabs.

- 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'

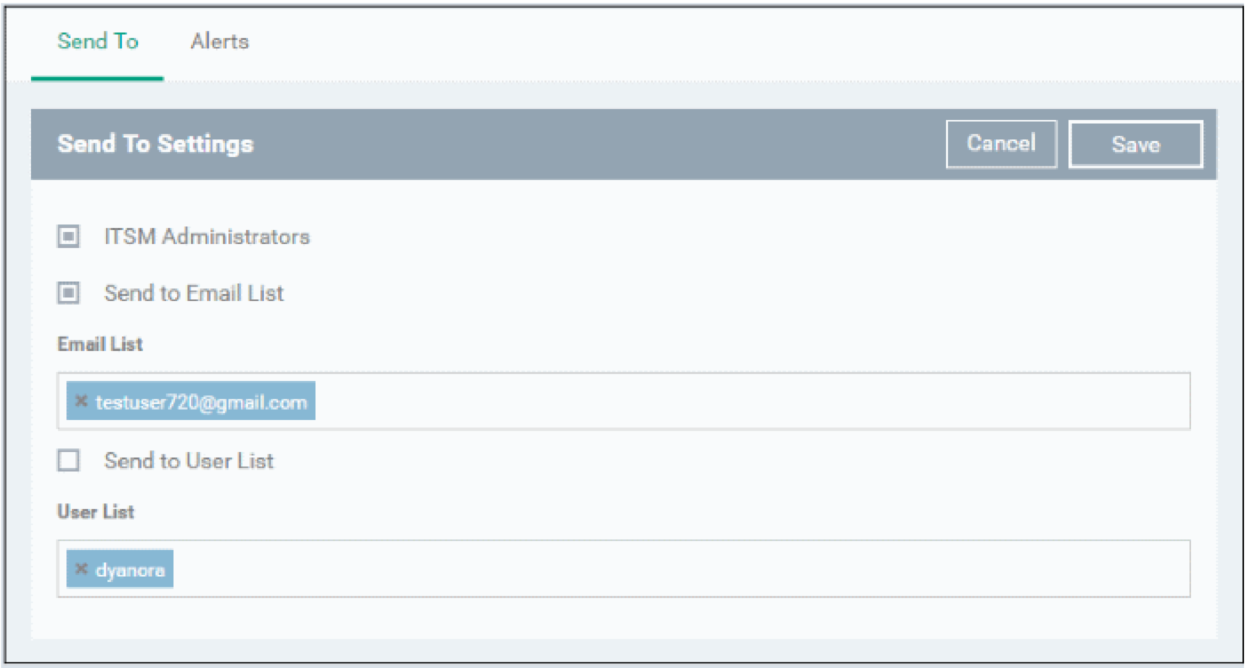
The 'Send to Settings' screen will be displayed.



ITSM Administrators
Disabled
Send to Email List
Disabled
Email List
Email List Is Empty
Send to User List
Disabled
User List
User List Is Empty

- **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



▣ ITSM Administrators

▣ Send to Email List

Email List

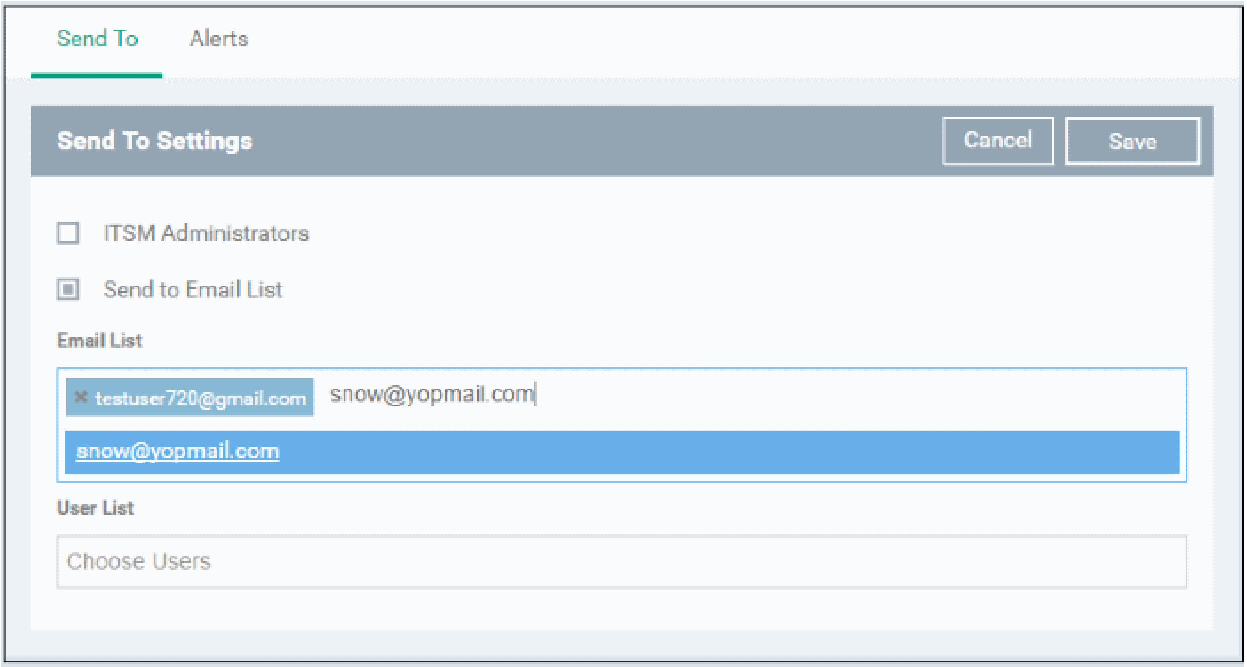
testuser720@gmail.com

□ Send to User List

User List

dyanora

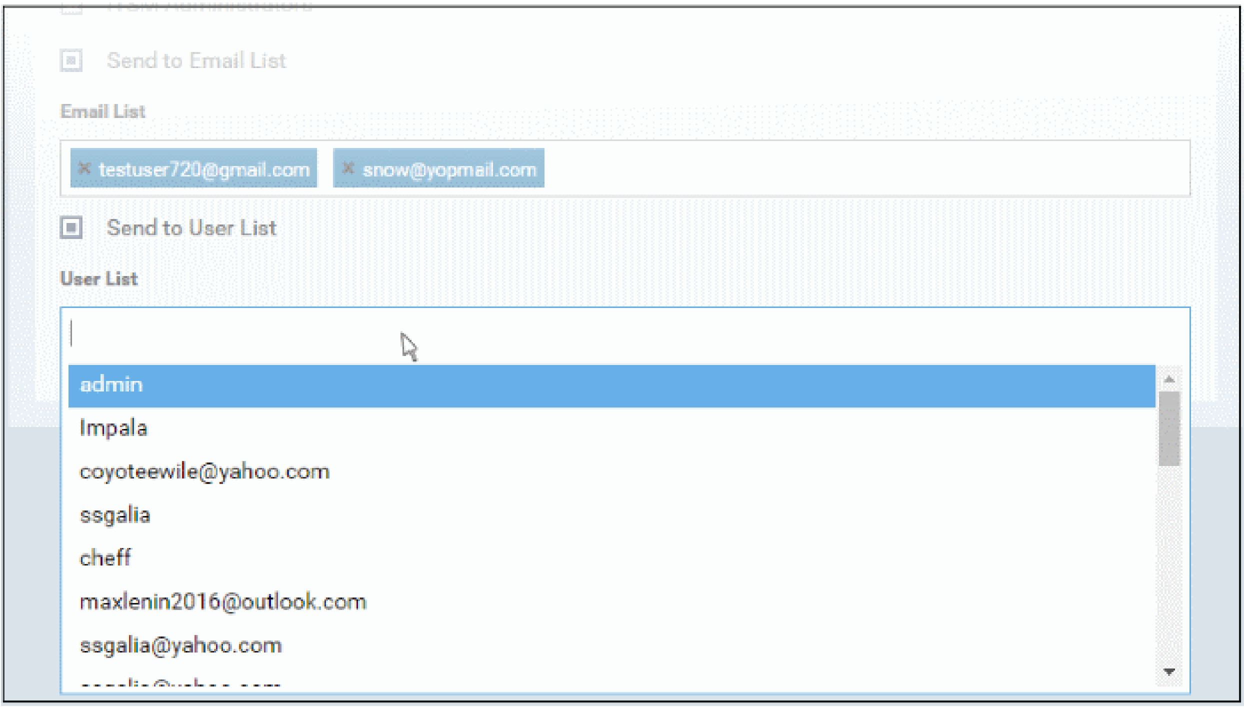
- To add recipients under 'Emails List', type the email address in the field and click the 'Enter' key or click the address that appear below the field.



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

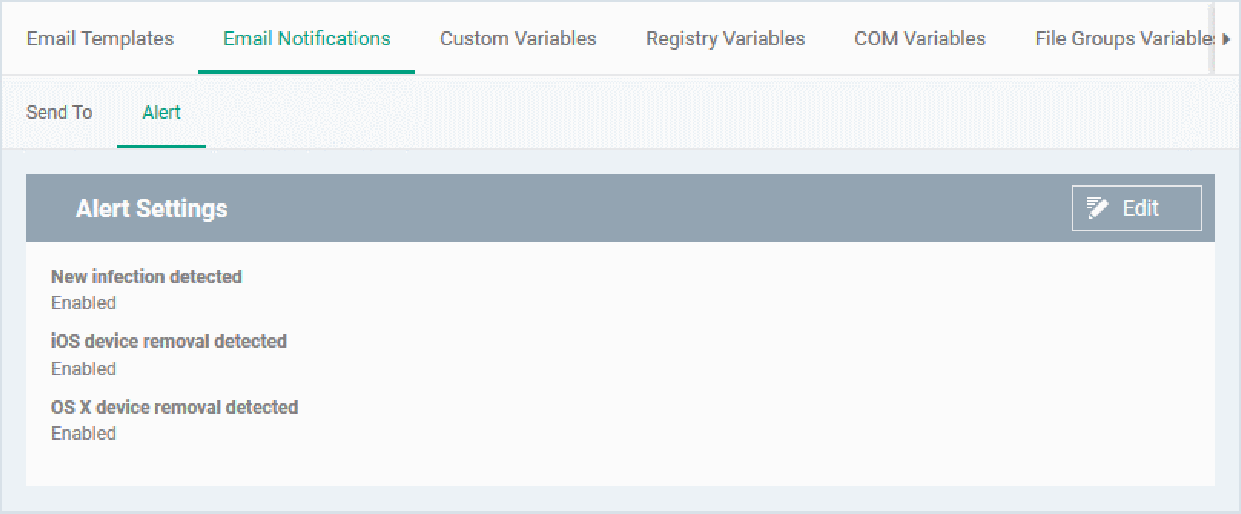
Please note the 'Send to Users List' check box should be enabled for the alerts to be sent to the users.

- 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.



New infection detected
Enabled

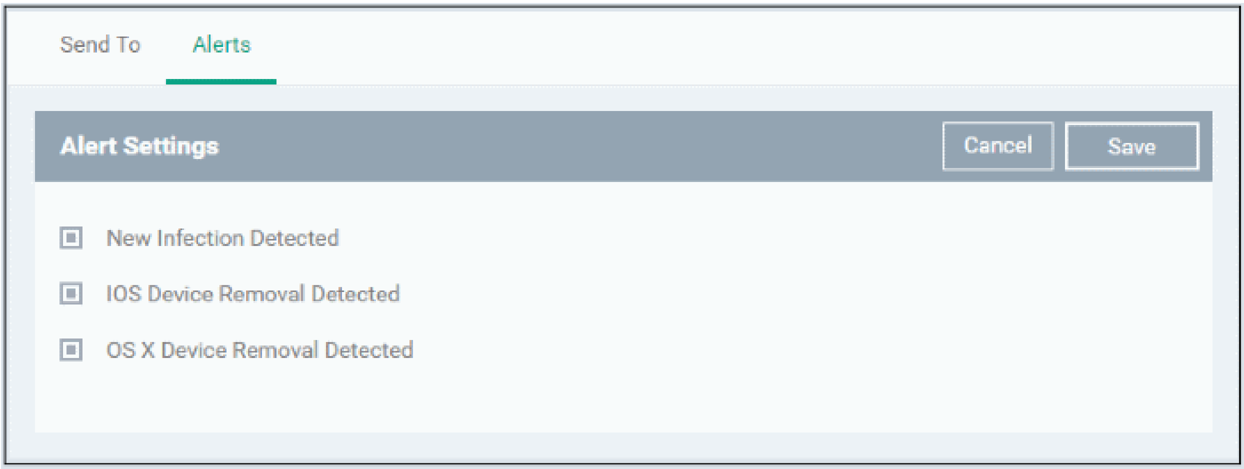
iOS device removal detected
Enabled

OS X device removal detected
Enabled

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
- **Mac OS Device Removal Detected** - If enabled, an alert will be sent if a Mac OS device is removed from ITSM.

Click the 'Edit' button at the top right to enable/disable the type of alert.



□ New Infection Detected

□ IOS Device Removal Detected

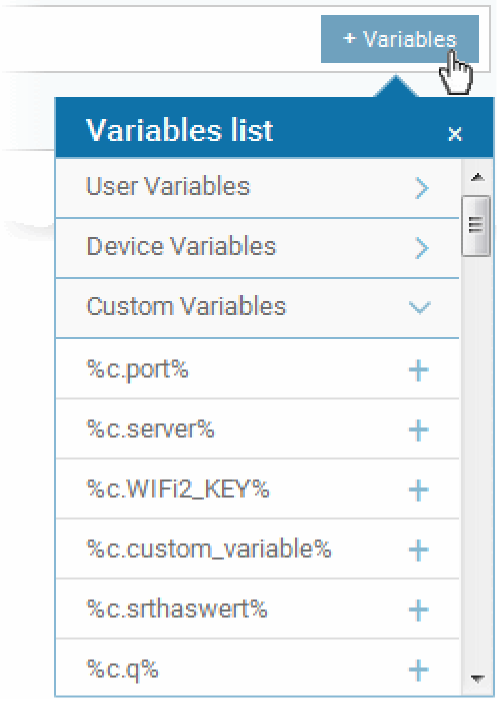
□ OS X Device Removal Detected

- 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. Create and Manage 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 + Variables 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:

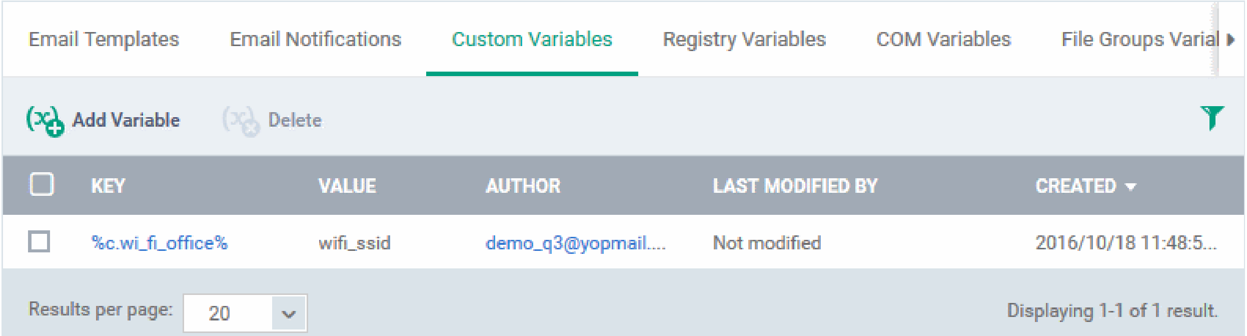


The first two, 'User Variables' and 'Device Variables', are hard coded and cannot be altered. These are useful for fetching the values of user and devices, for example user login details, email details from 'Users' > 'User List'. The last one, 'Custom Variables', can be created by administrators used 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



☐	KEY	VALUE	AUTHOR	LAST MODIFIED BY	CREATED
☐	%c.wi_fi_office%	wifi_ssid	demo_q3@yopmail....	Not modified	2016/10/18 11:48:5...

Results per page: 20

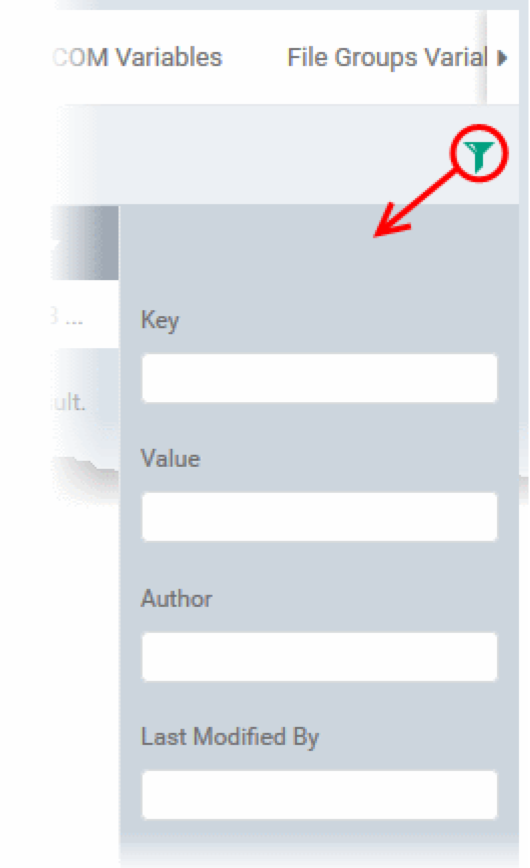
Displaying 1-1 of 1 result.

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



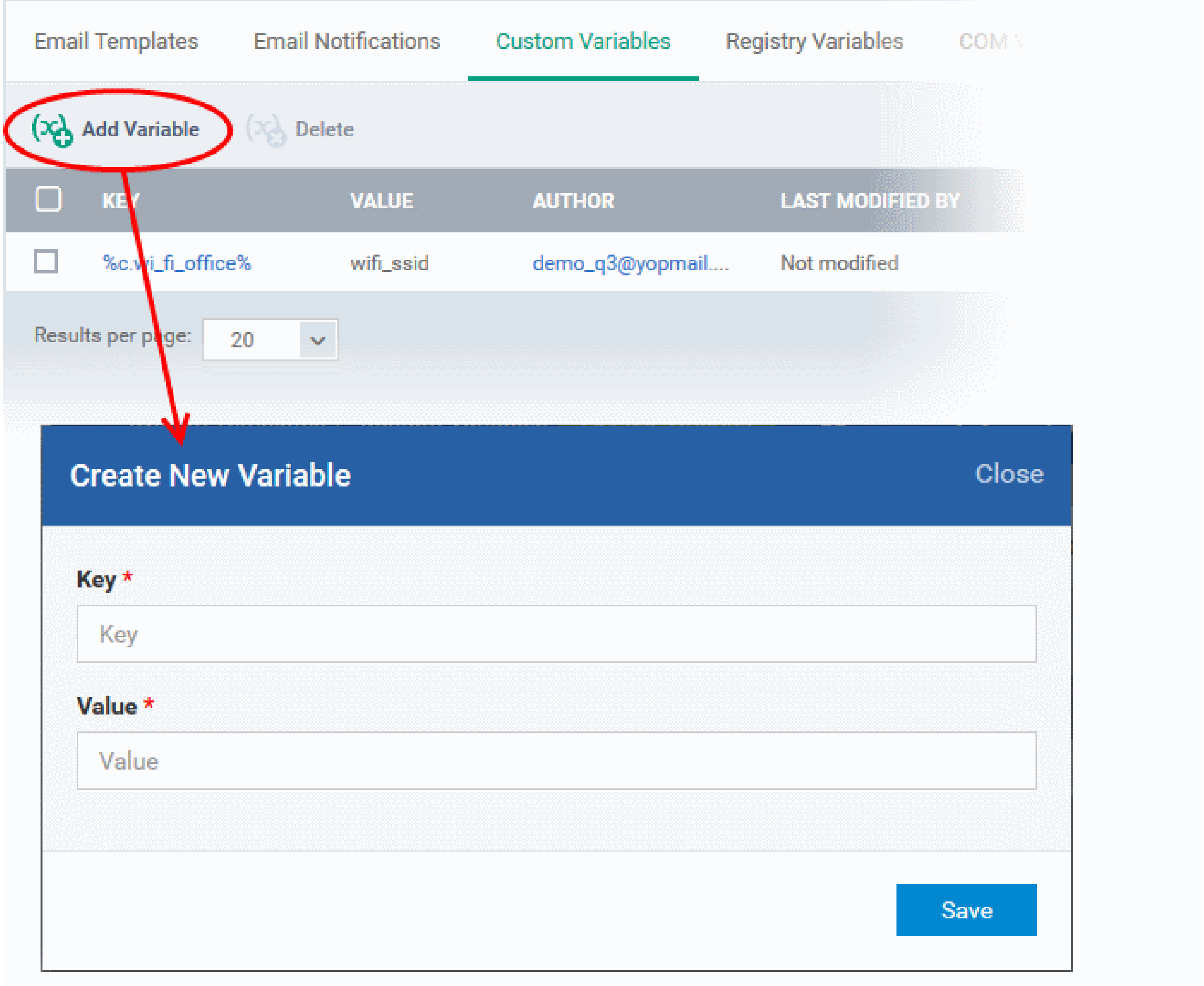
- To display variables which are based on 'Key', 'Value', 'Author' and 'Last Modified By', enter the text partially or fully in the respective fields and click the 'Apply' button.

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 'Settings' on the left, choose 'System Templates' and click the 'Custom Variables' tab
- Click 'Add Variable'



☐	KEY	VALUE	AUTHOR	LAST MODIFIED BY
☐	%c.wi_fi_office%	wifi_ssid	demo_q3@yopmail....	Not modified

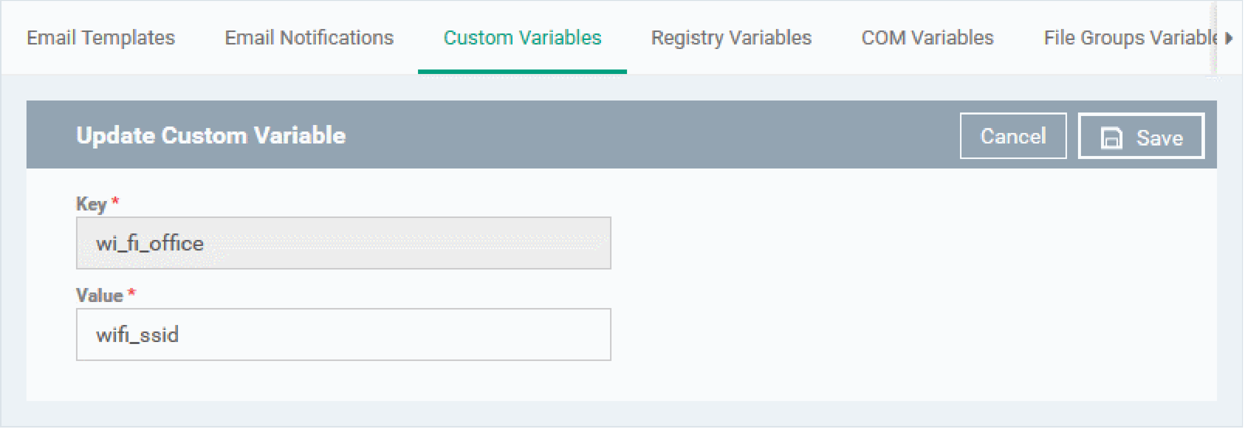
- In the 'Create New Variable' dialog enter a variable name in the 'Key' text box.
- In the 'Value' text field, enter the value for the variable.
- Click 'Save' to add the variable to ITSM.

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.



Key *
wi_fi_office

Value *
wifi_ssid

- 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

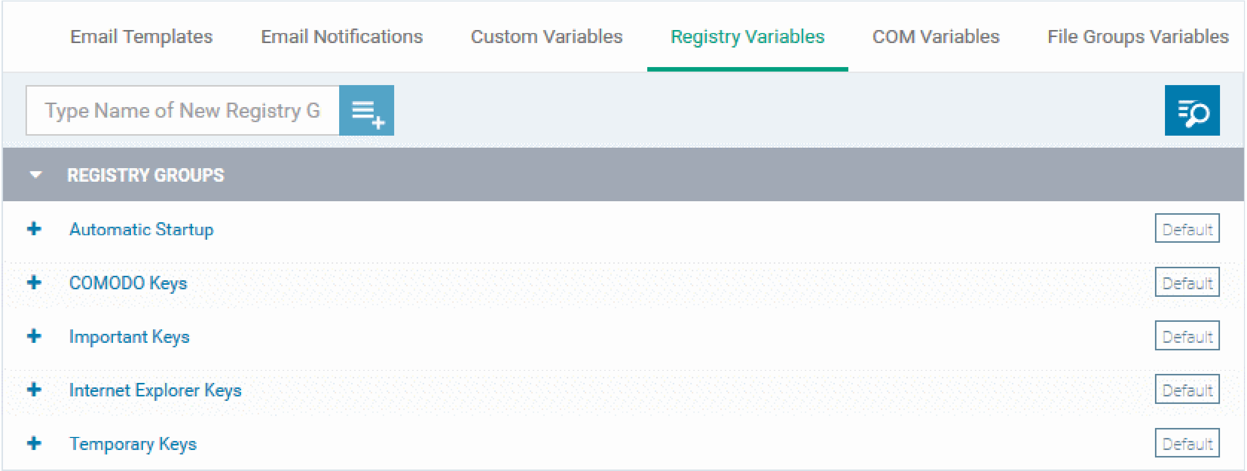
11.1.4. Create and Manage Registry Groups

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

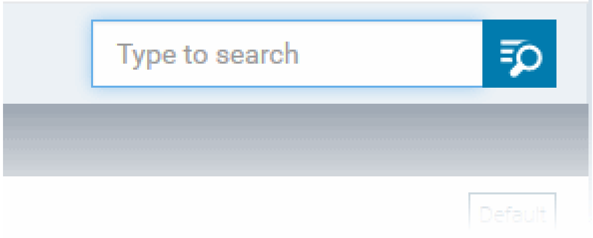


REGISTRY GROUPS	
Automatic Startup	Default
COMODO Keys	Default
Important Keys	Default
Internet Explorer Keys	Default
Temporary Keys	Default

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.

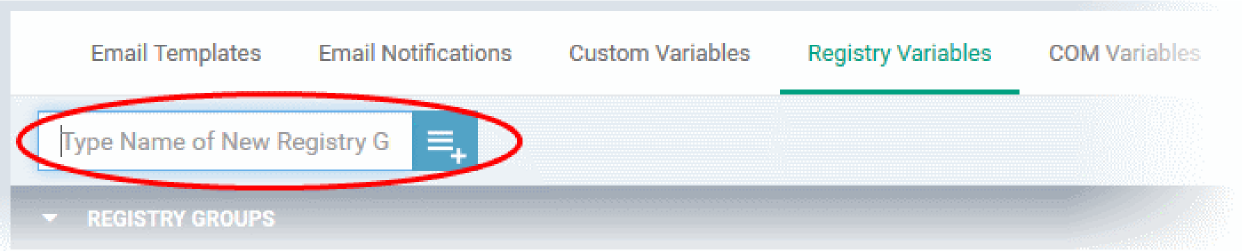
Sorting, Search and Filter Options

- 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



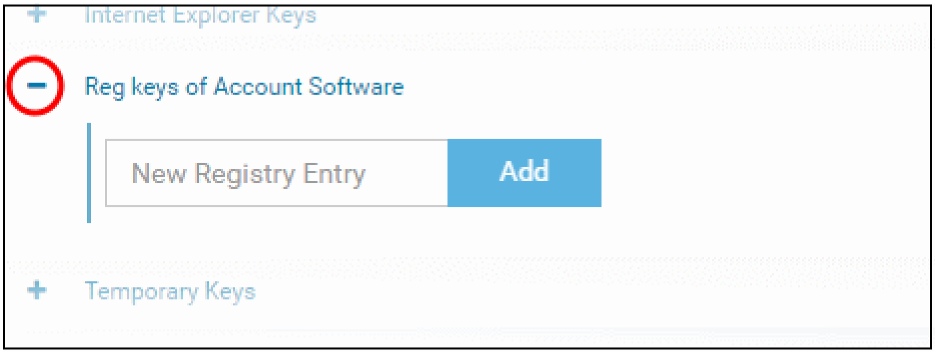
To add a new Registry group

- Enter the name of the new Registry Group in the New Registry Group field and click the '+' button.

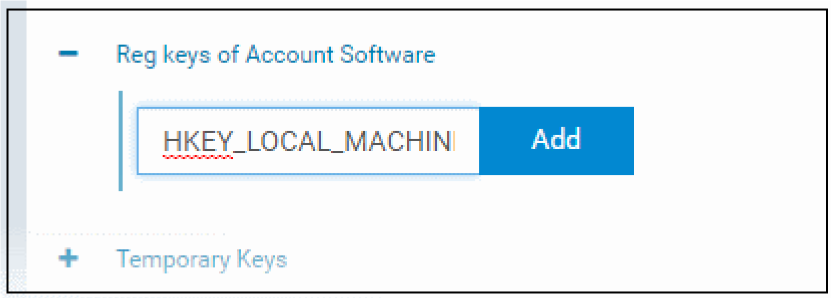


The new group will be added to the list. The next step is to add the Registry keys to the group.

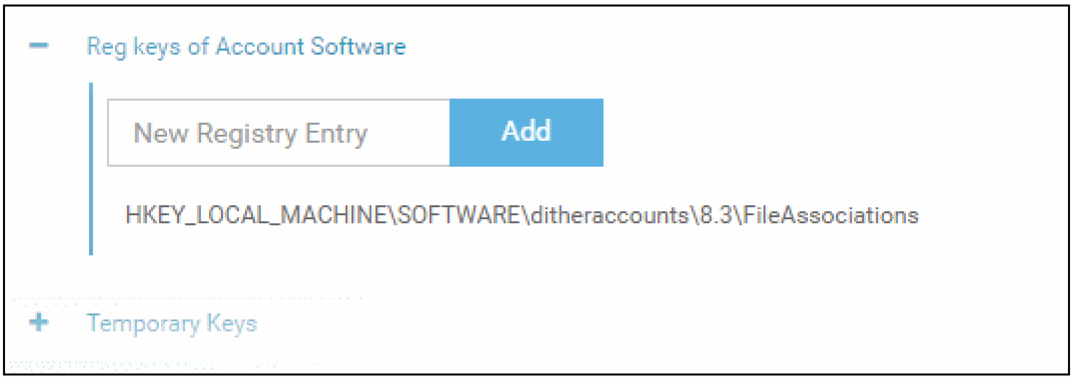
- Click the '+' at the left of the group name



- Enter the path of the registry key/value in the New Registry Entry field and click 'Add'

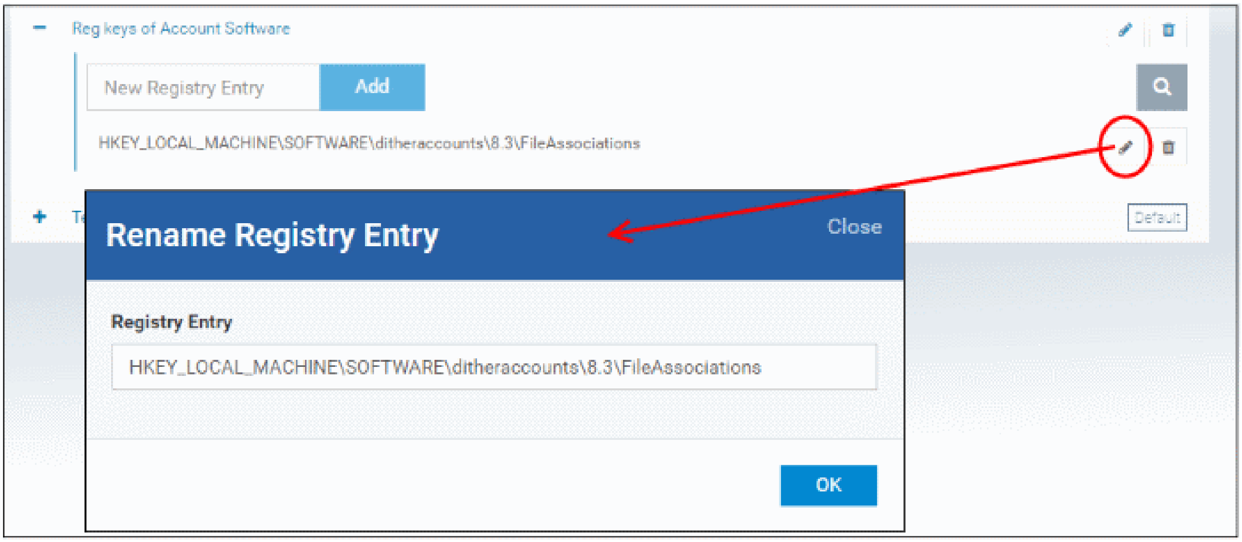


The key will be added to the group.



HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations

- 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.



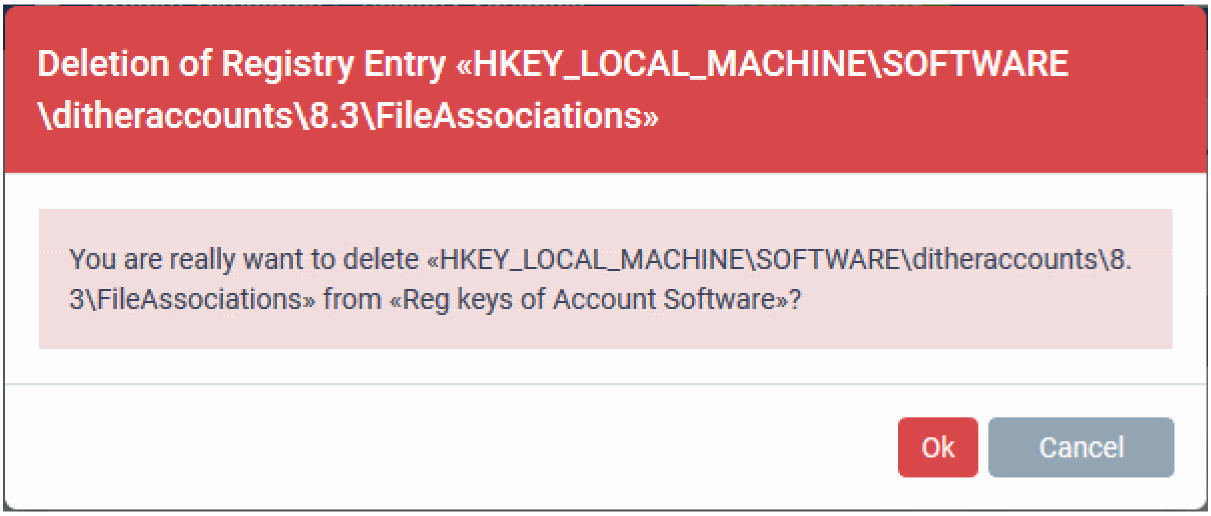
HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations

Registry Entry: HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations

- 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.

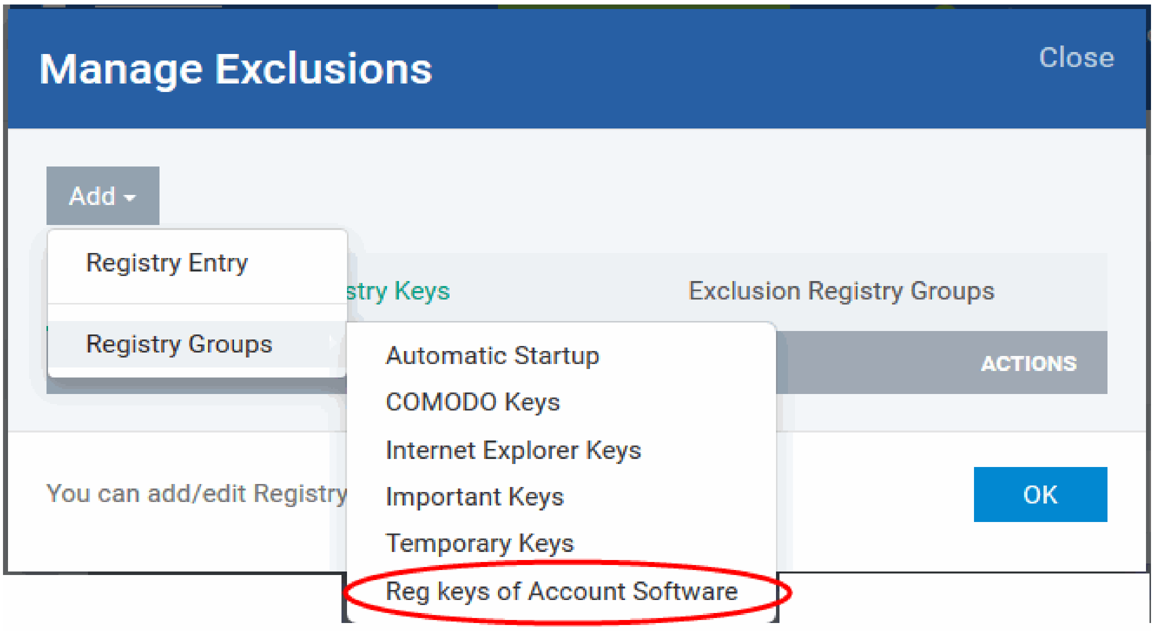


Deletion of Registry Entry «HKEY_LOCAL_MACHINE\SOFTWARE \ditheraccounts\8.3\FileAssociations»

You are really want to delete «HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations» from «Reg keys of Account Software»?

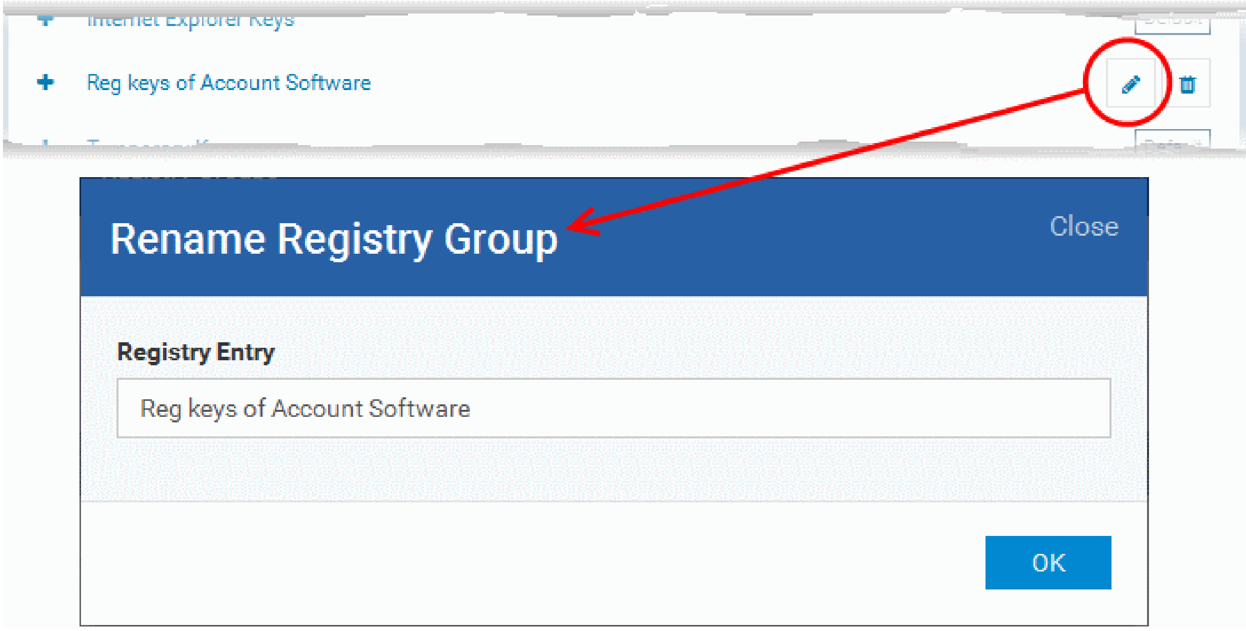
- Click 'OK' in the confirmation dialog.

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

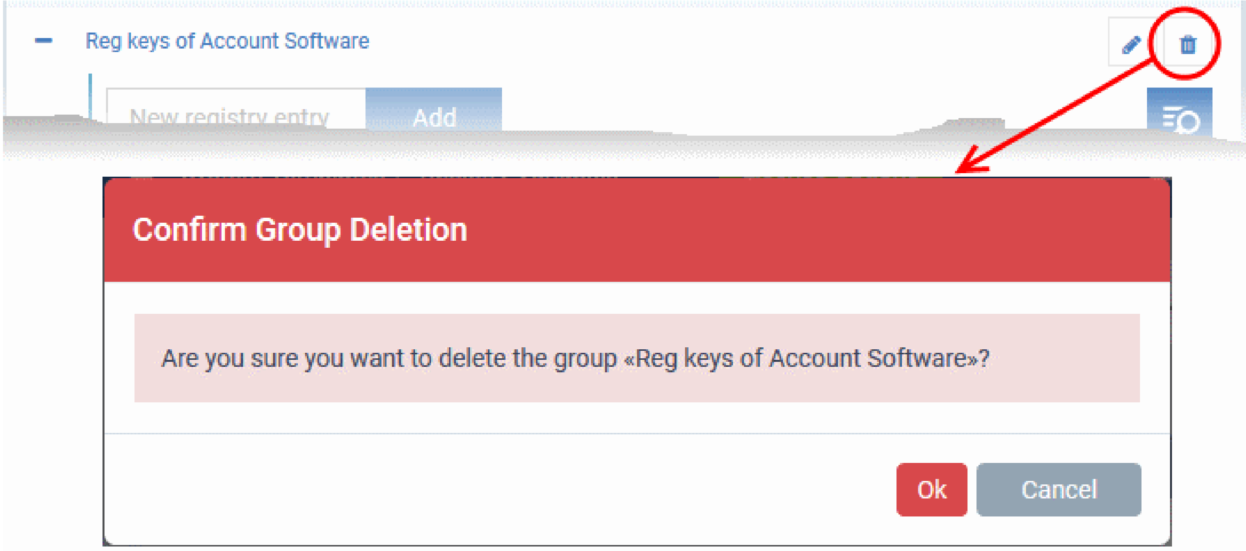
- Click the 'Edit' icon beside the Registry Group



- 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



Confirm Group Deletion

Are you sure you want to delete the group «Reg keys of Account Software»?

A confirmation dialog will appear.

- Click OK in the confirmation dialog.

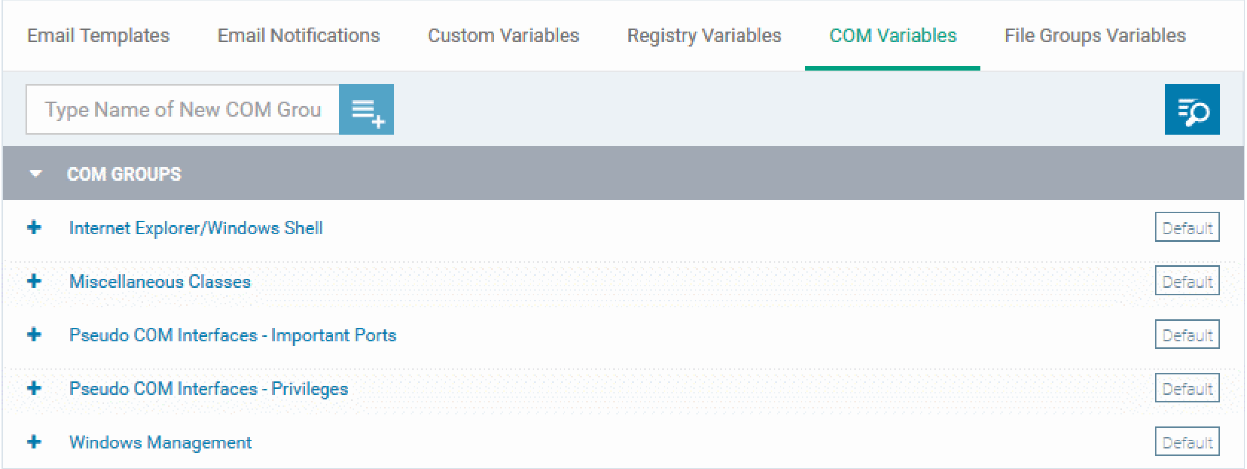
11.1.5. Create and Manage COM Groups

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



COM GROUPS

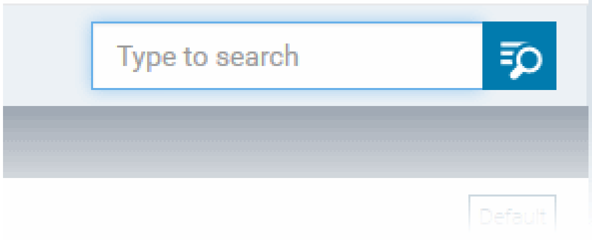
COM GROUPS	
+ Internet Explorer/Windows Shell	Default
+ Miscellaneous Classes	Default
+ Pseudo COM Interfaces - Important Ports	Default
+ Pseudo COM Interfaces - Privileges	Default
+ Windows Management	Default

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

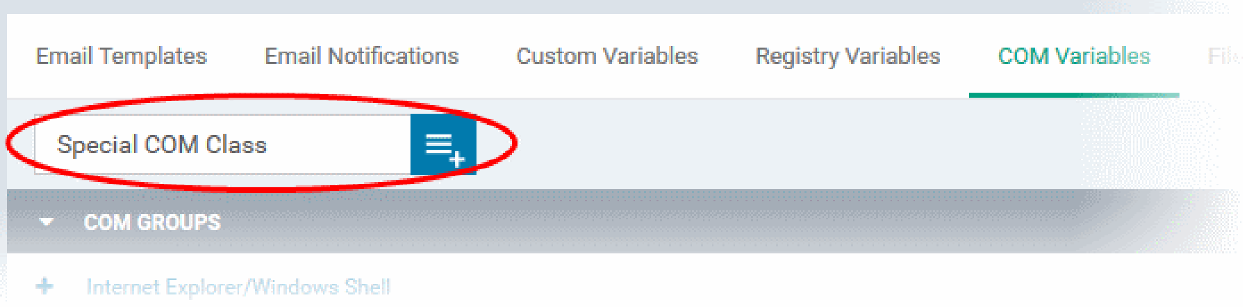
- Clicking on the 'COM Groups' column header will sort the items in ascending/descending order of the names of the groups.

- 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



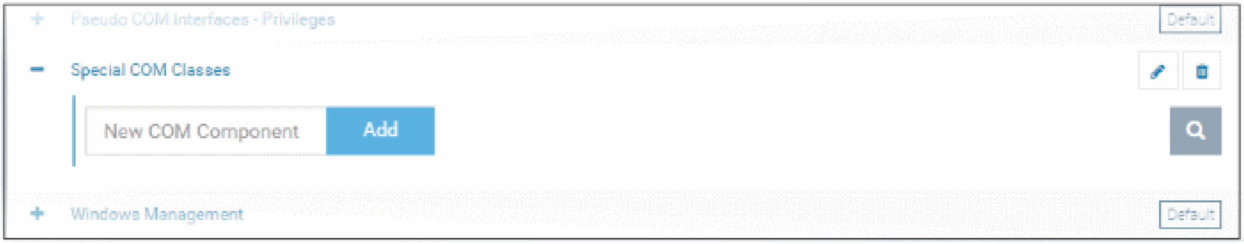
To add a new COM group

- Enter the name of the new COM Group in the 'Type Name of New COM Group' field and click the '+ ' button.

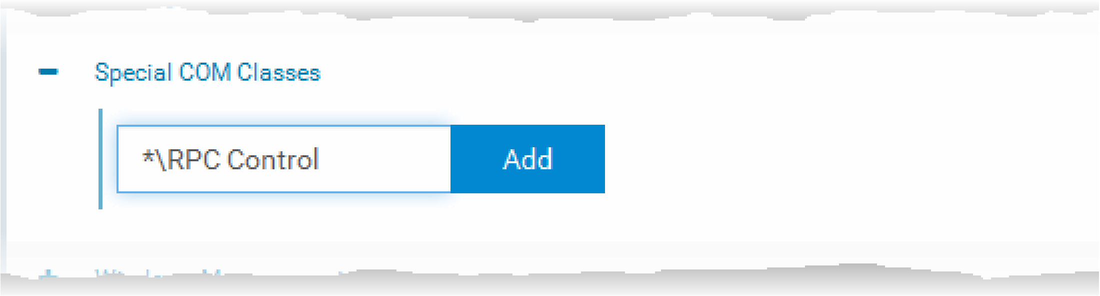


The new group will be added to the list. The next step is to add COM classes to the group.

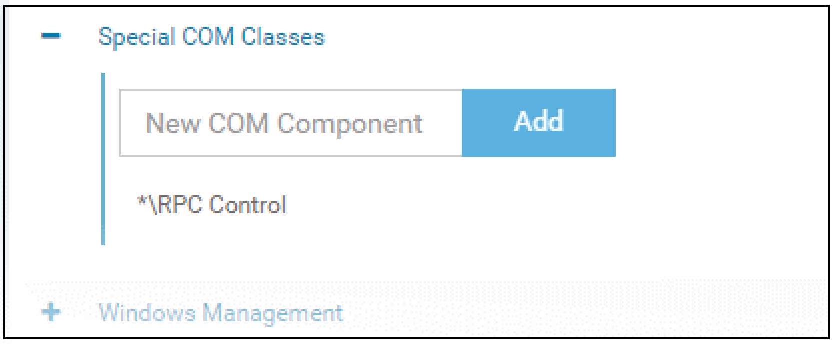
- Click the '+' at the left of the group name



- Enter the COM classes to be added to the group, in the 'New COM Component' field and click 'Add'

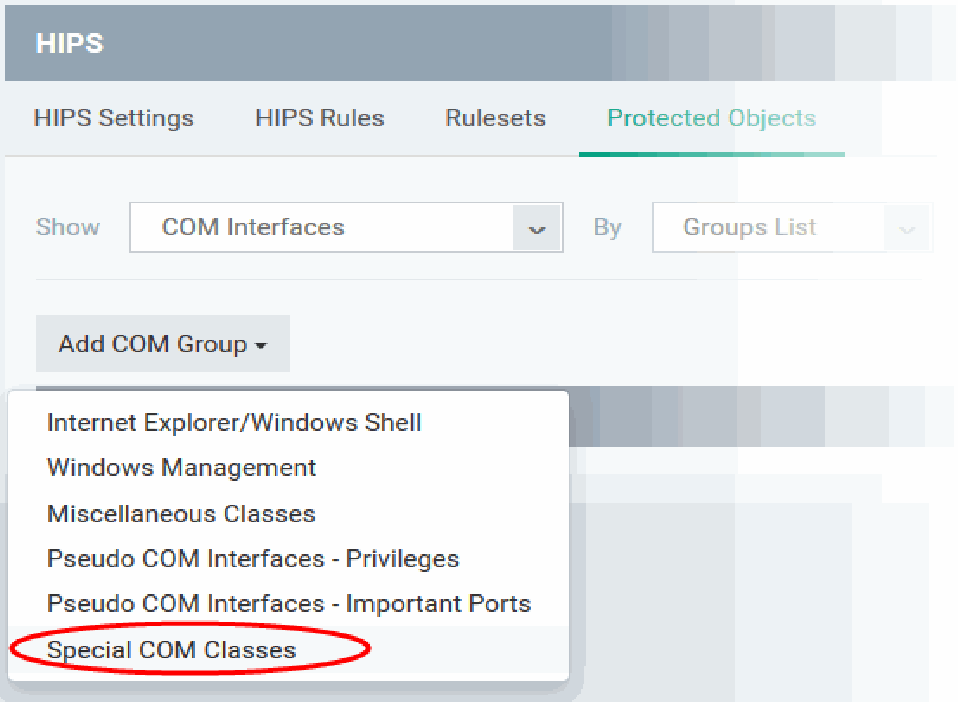


The COM class will be added to the group.

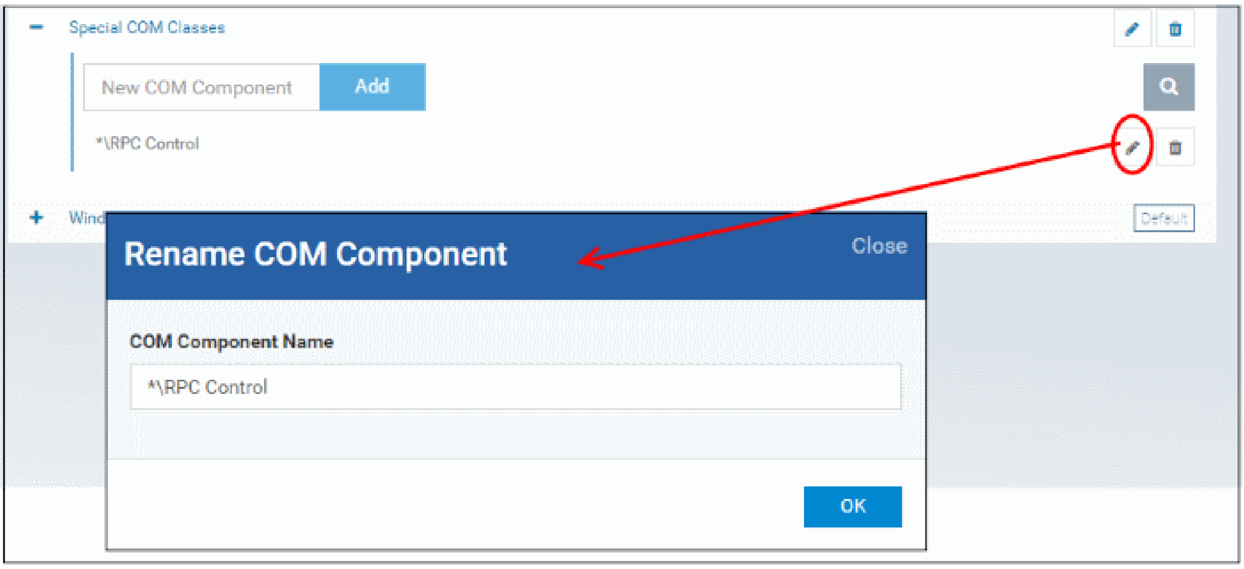


- Repeat the process to add more COM classes to the group.

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.



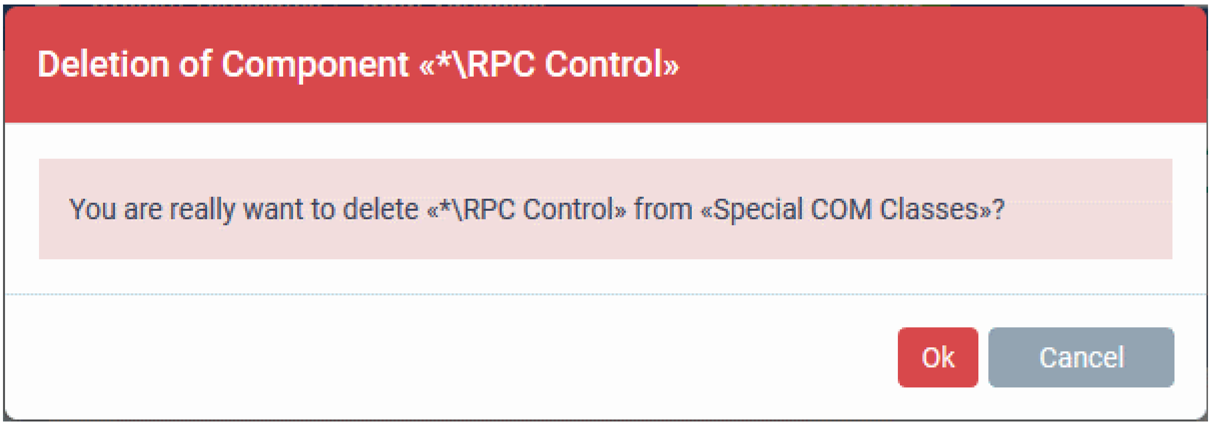
- To edit a class in the group, click the 'Edit' icon beside the class name.



- 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.



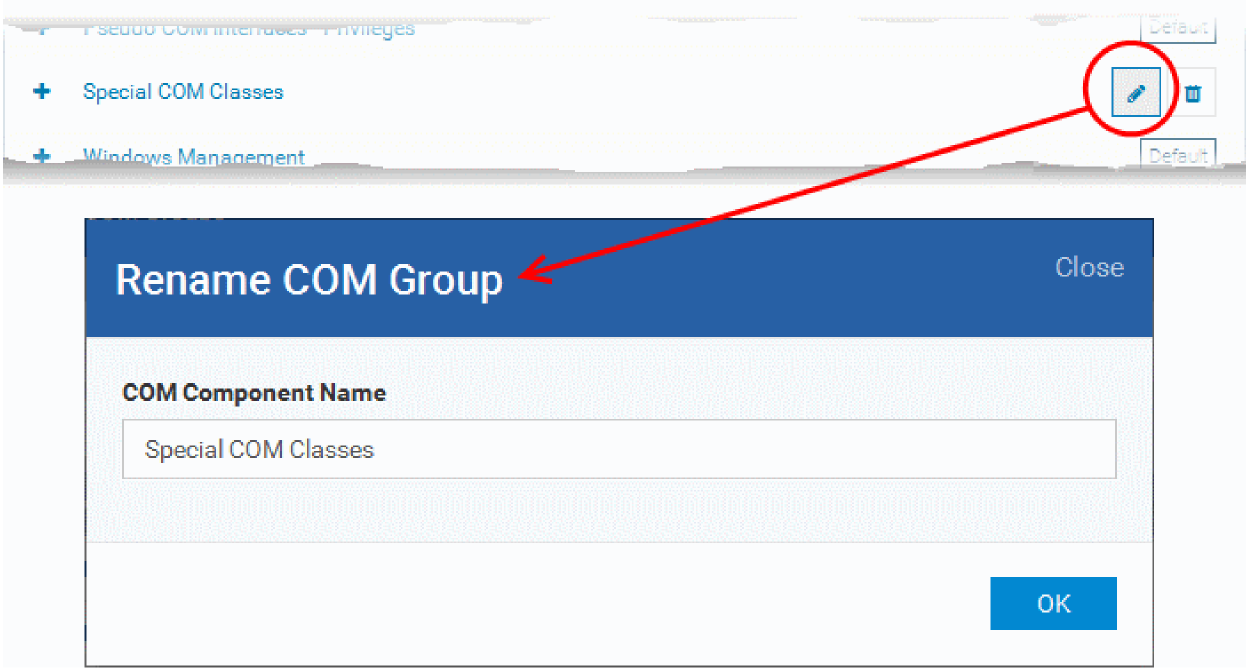
Deletion of Component «*\RPC Control»

You are really want to delete «*\RPC Control» from «Special COM Classes»?

- Click 'OK' in the confirmation dialog.

To edit the name of a COM Group

- Click the 'Edit' icon beside the COM Group



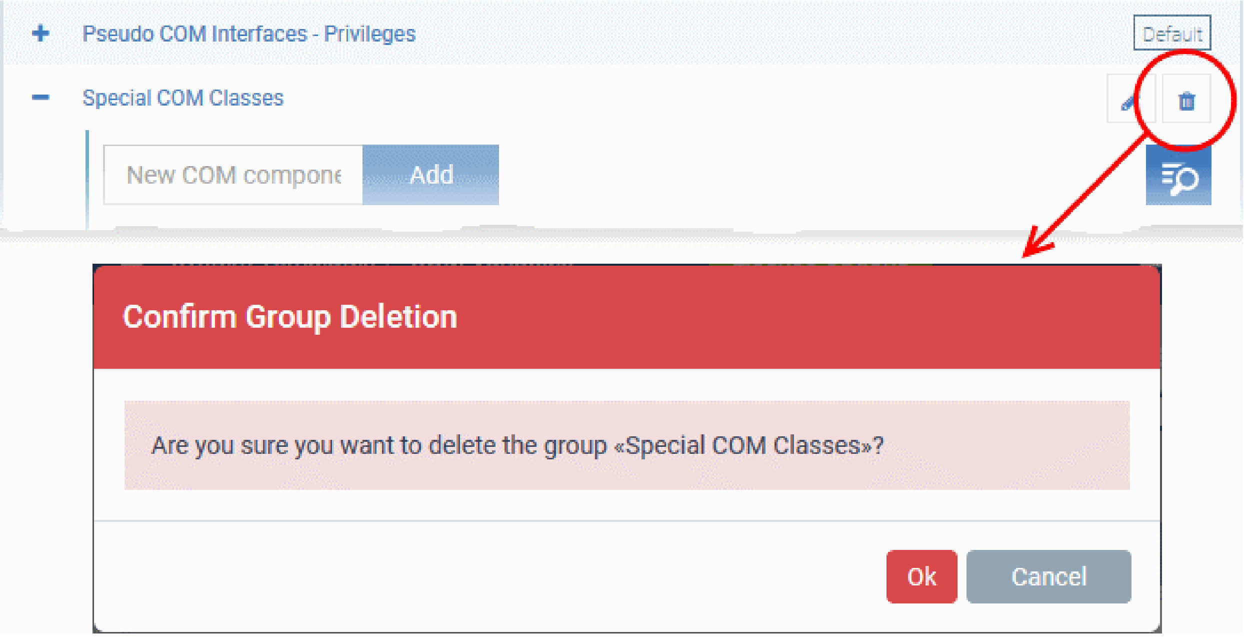
COM Component Name

Special COM Classes

- 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



Confirm Group Deletion

Are you sure you want to delete the group «Special COM Classes»?

A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

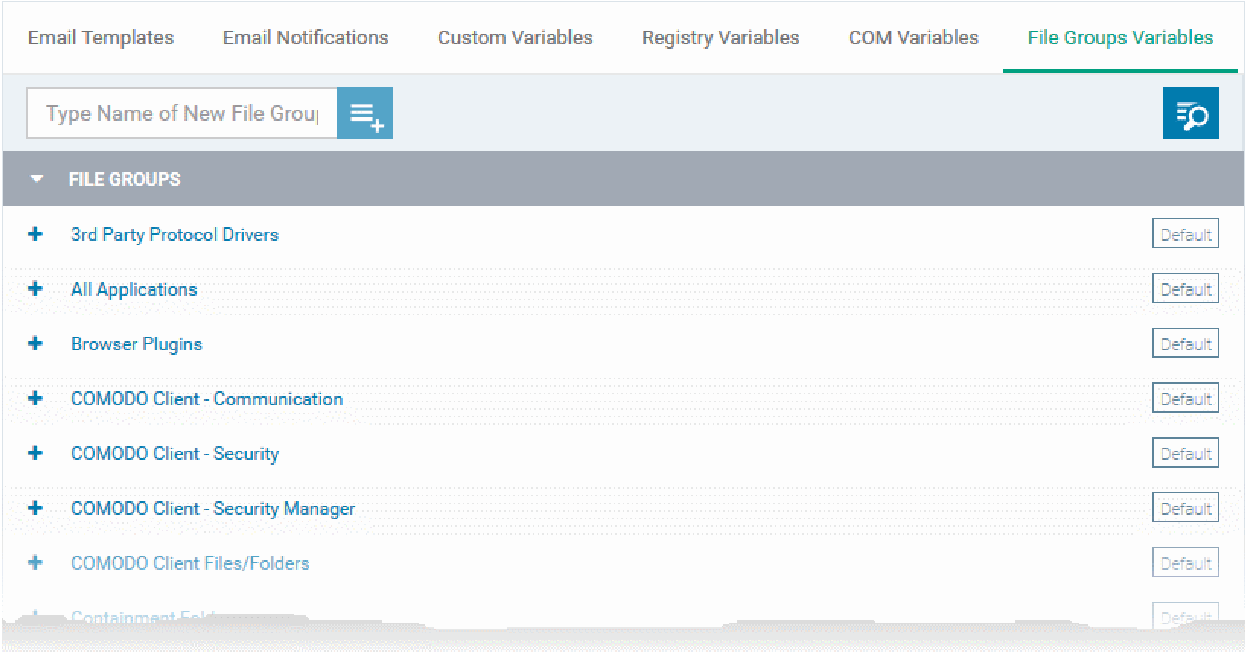
11.1.6. Create and Manage File Groups

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



Email Templates | Email Notifications | Custom Variables | Registry Variables | COM Variables | File Groups Variables

Type Name of New File Group

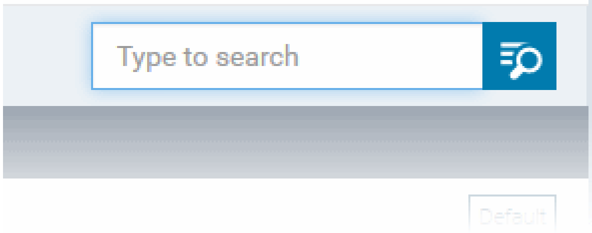
FILE GROUPS

+ 3rd Party Protocol Drivers	Default
+ All Applications	Default
+ Browser Plugins	Default
+ COMODO Client - Communication	Default
+ COMODO Client - Security	Default
+ COMODO Client - Security Manager	Default
+ COMODO Client Files/Folders	Default
+ Containment Fol...	Default

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.

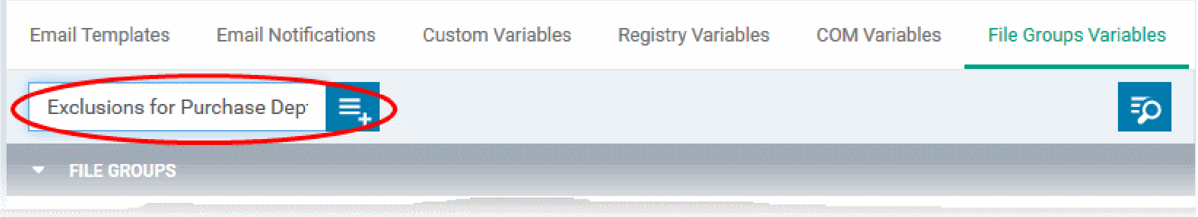
Sorting, Search and Filter Options

- 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



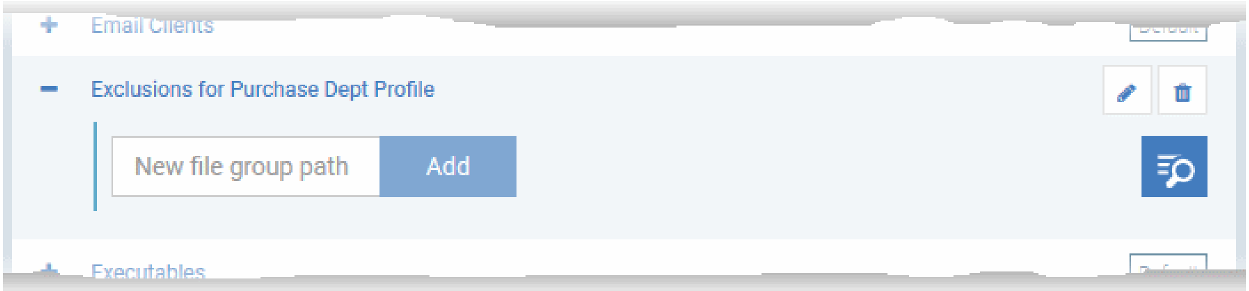
Email Templates | Email Notifications | Custom Variables | Registry Variables | COM Variables | File Groups Variables

Exclusions for Purchase Dep

FILE GROUPS

The new group will be added to the list. The next step is to add files to the group.

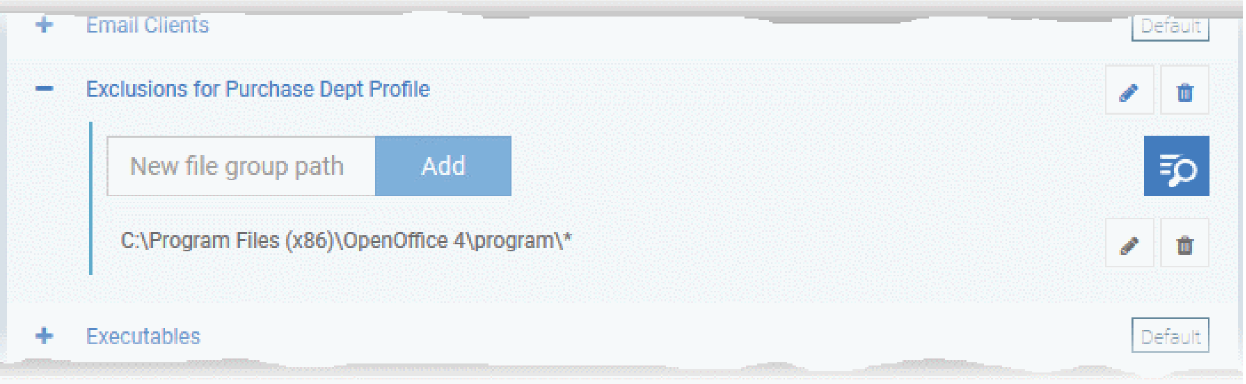
- Click the '+' at the left of the group name



- 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* "

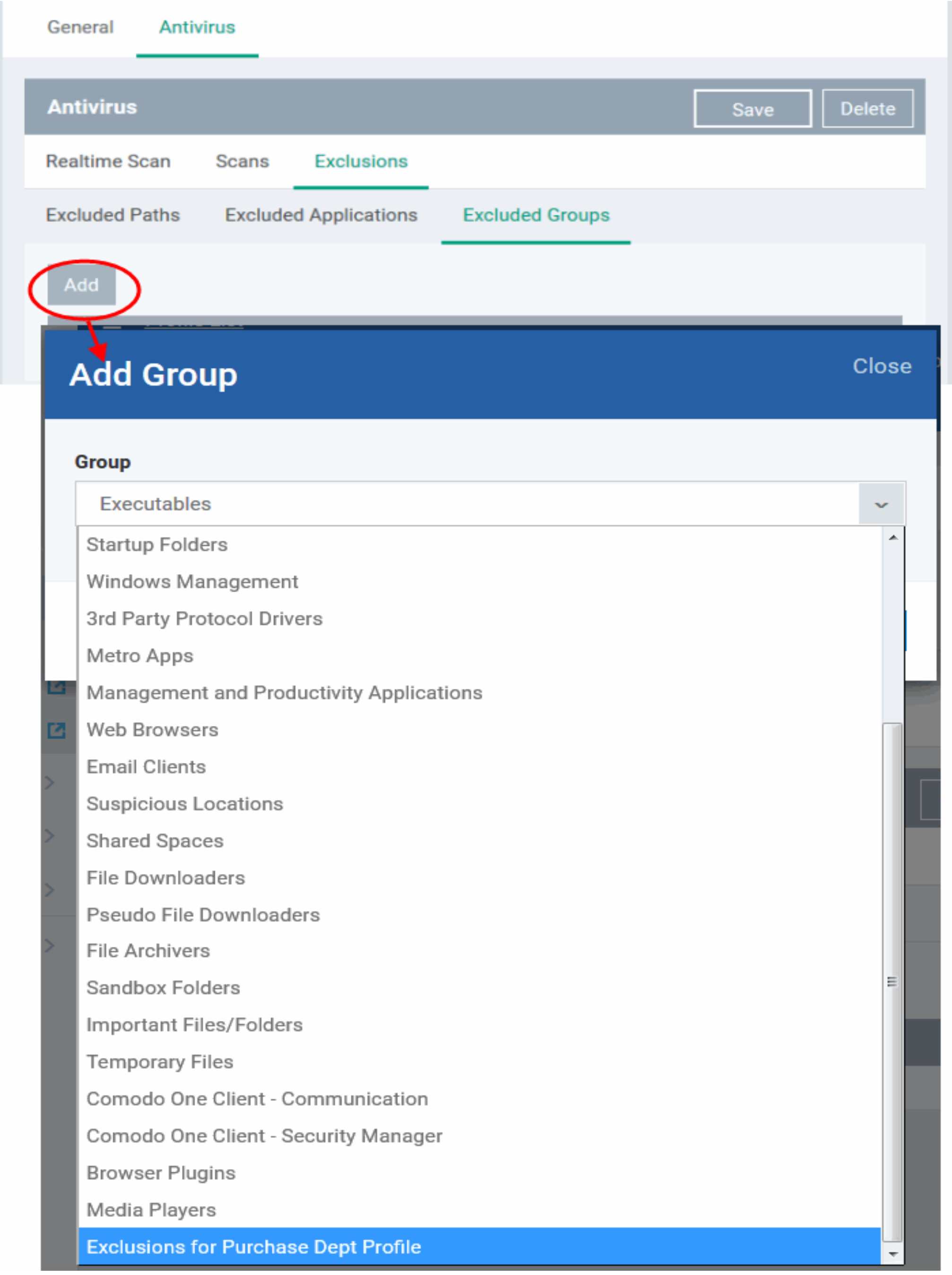
The file(s) will be added to the group.



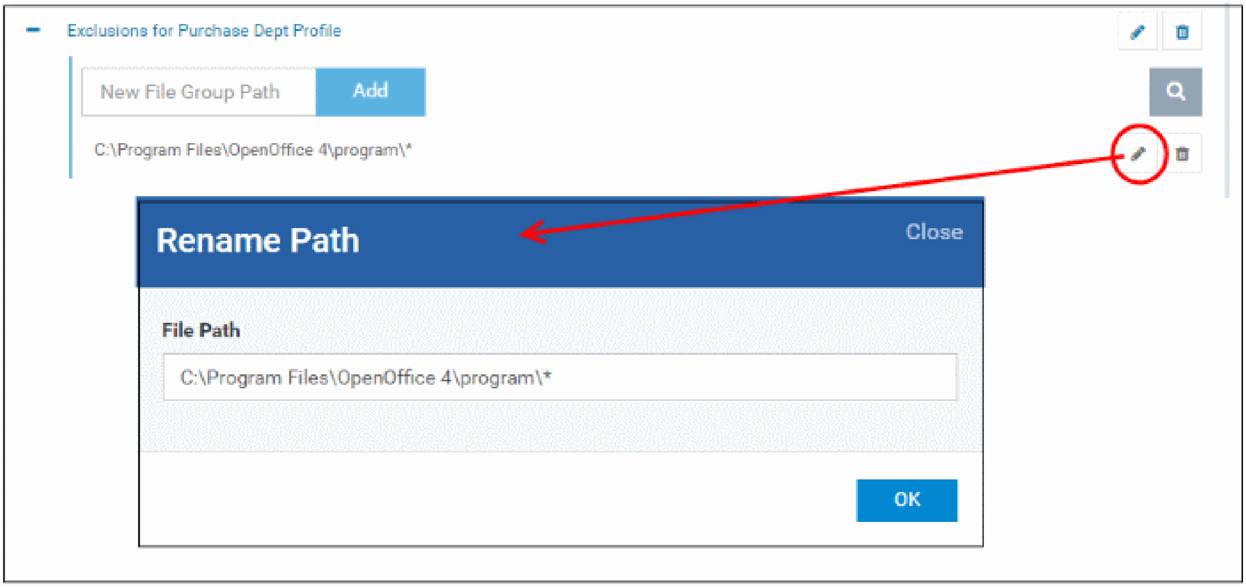
C:\Program Files (x86)\OpenOffice 4\program\*

- 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.

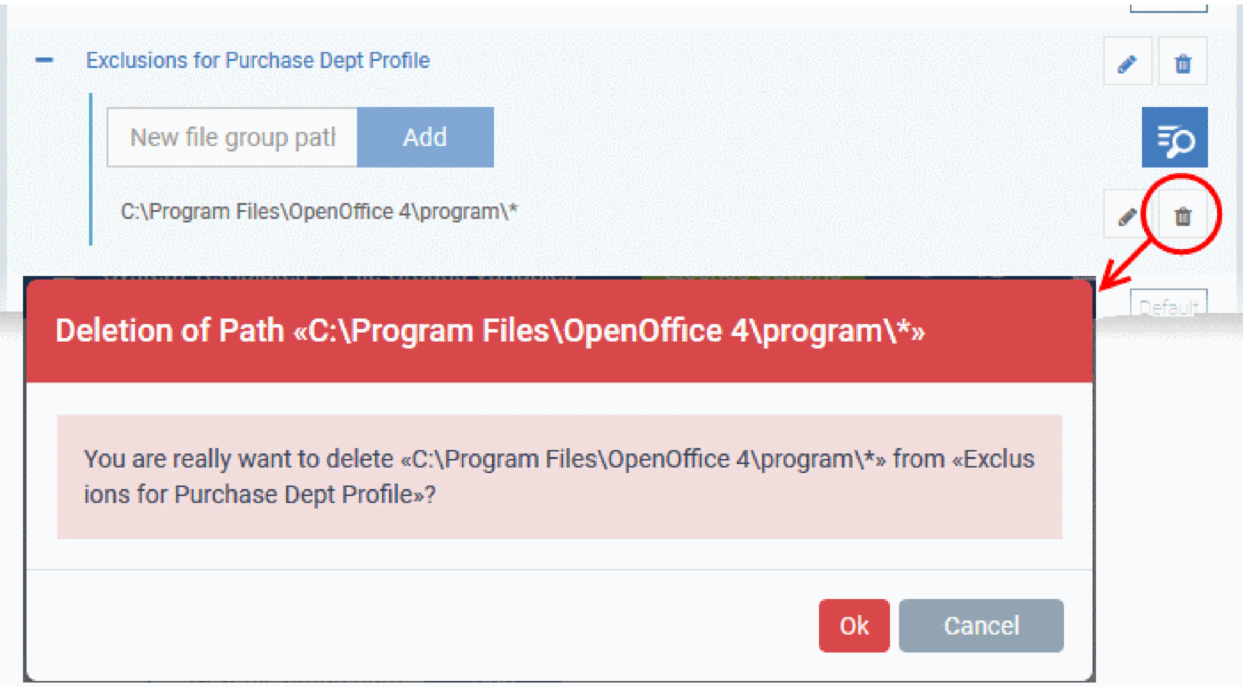


- To edit the files in the group, click the 'Edit' icon beside the file name.


Exclusions for Purchase Dept Profile
New File Group Path
Add
C:\Program Files\OpenOffice 4\program\*
Rename Path
Close
File Path
C:\Program Files\OpenOffice 4\program\*
OK

- 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.


Exclusions for Purchase Dept Profile
New file group patl
Add
C:\Program Files\OpenOffice 4\program\*
Deletion of Path «C:\Program Files\OpenOffice 4\program\*»

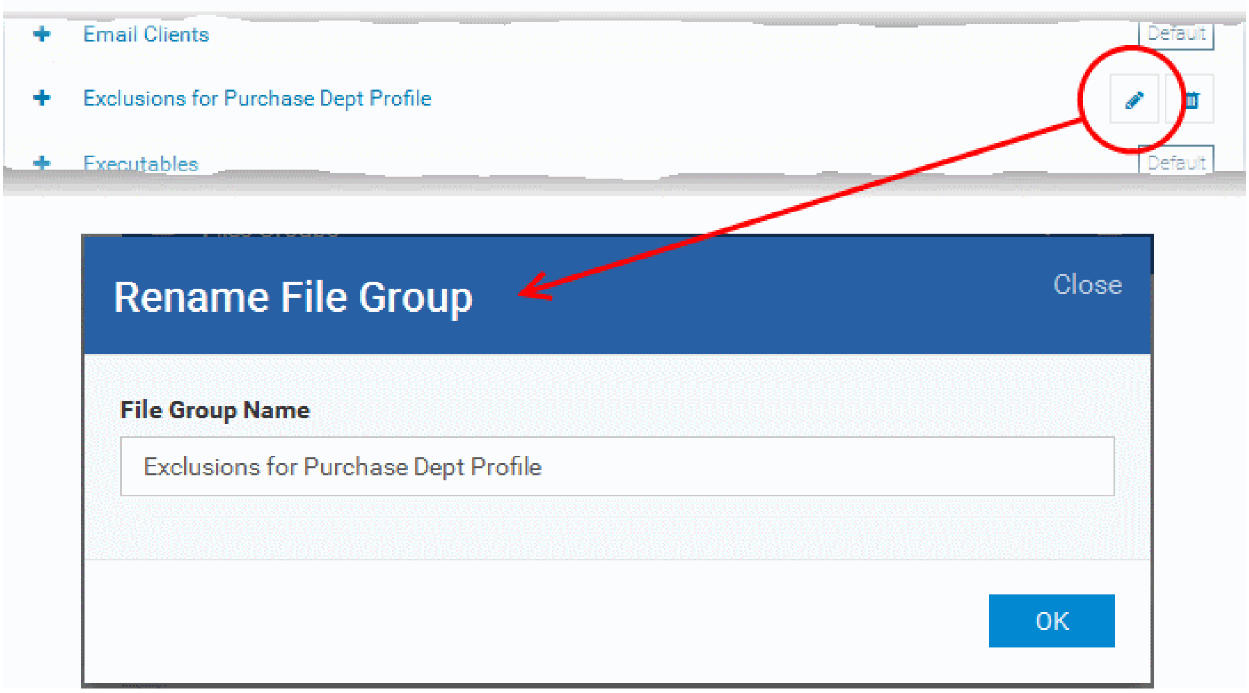
You are really want to delete «C:\Program Files\OpenOffice 4\program\*» from «Exclusions for Purchase Dept Profile»?

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



Rename File Group

Close

File Group Name

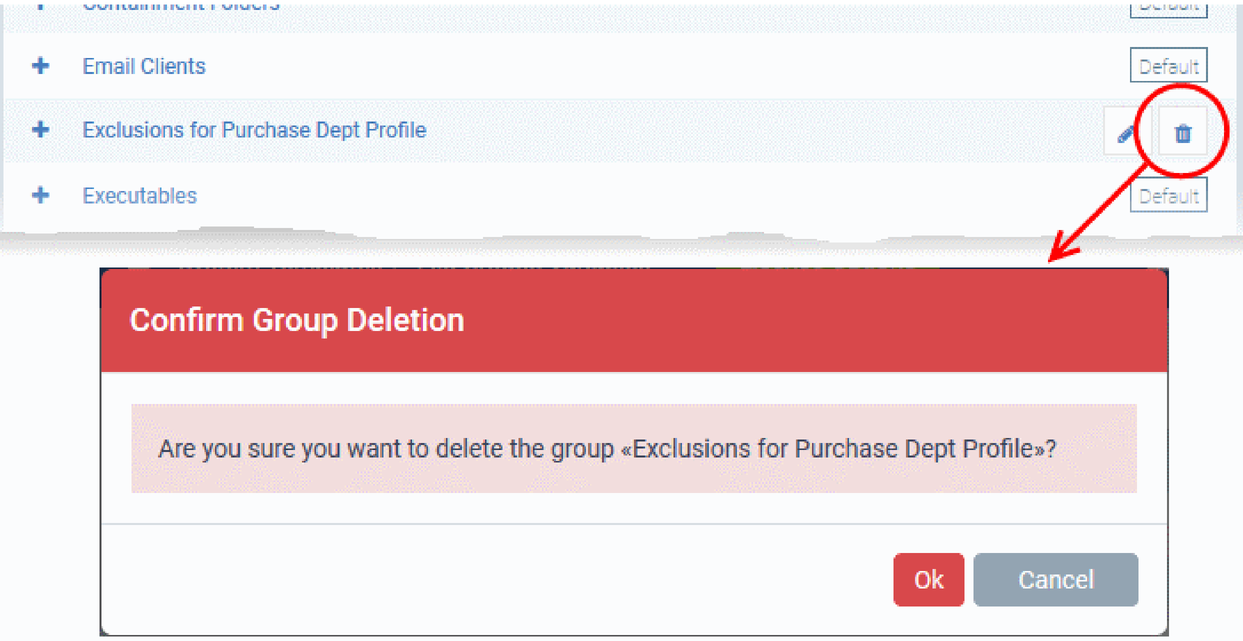
Exclusions for Purchase Dept Profile

OK

- 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



Confirm Group Deletion

Are you sure you want to delete the group «Exclusions for Purchase Dept Profile»?

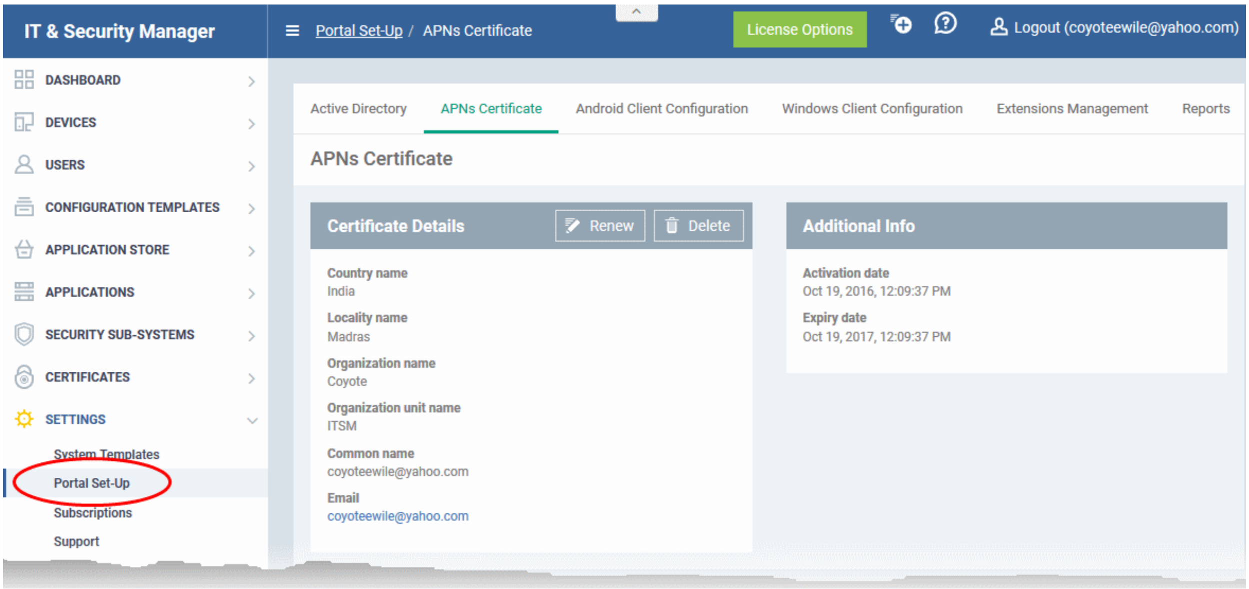
Ok Cancel

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.



Country name
India

Locality name
Madras

Organization name
Coyote

Organization unit name
ITSM

Common name
coyoteewile@yahoo.com

Email
coyoteewile@yahoo.com

Activation date
Oct 19, 2016, 12:09:37 PM

Expiry date
Oct 19, 2017, 12:09:37 PM

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. Import User Groups from LDAP

In addition to adding user groups manually, ITSM allows you 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.

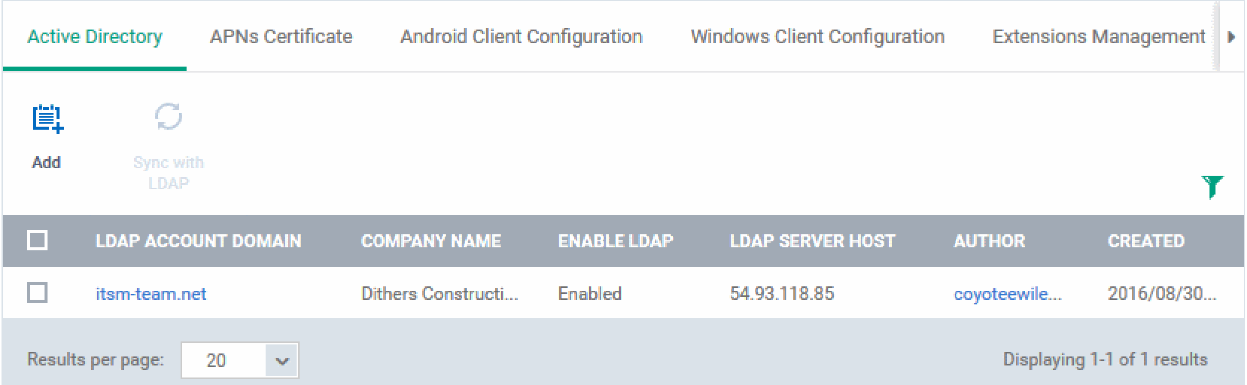
The process in brief:

- Add an LDAP server by specifying its IP address, domain and the login credentials of the AD server:
  - Click 'Settings' > 'Portal Set-Up' > select the 'Active Directory' tab > Click 'Add'
- Once added, users and user groups in the AD directory will be visible in the 'Active Directory' interface:
  - Click 'Settings' > 'Portal Set-Up' > select the 'Active Directory' tab > Click on an AD domain name > Click the 'User Groups' tab
- Select the users and groups you wish to import to ITSM
- Assign roles to users/user groups as required
- Synchronize LDAP with ITSM

- The selected users/user groups will be imported and placed into respective groups in ITSM
- The 'User List' and 'User Groups' interfaces let you view/manage users and enroll user devices. See **Users and User Groups** for more details.

To open the Active Directory interface

- Click 'Settings' on the left and select 'Portal Set-Up'
- Click 'Active Directory' from the top



□	LDAP ACCOUNT DOMAIN	COMPANY NAME	ENABLE LDAP	LDAP SERVER HOST	AUTHOR	CREATED
□	itsm-team.net	Dithers Constructi...	Enabled	54.93.118.85	coyoteewile...	2016/08/30...

Results per page: 20

Displaying 1-1 of 1 results

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

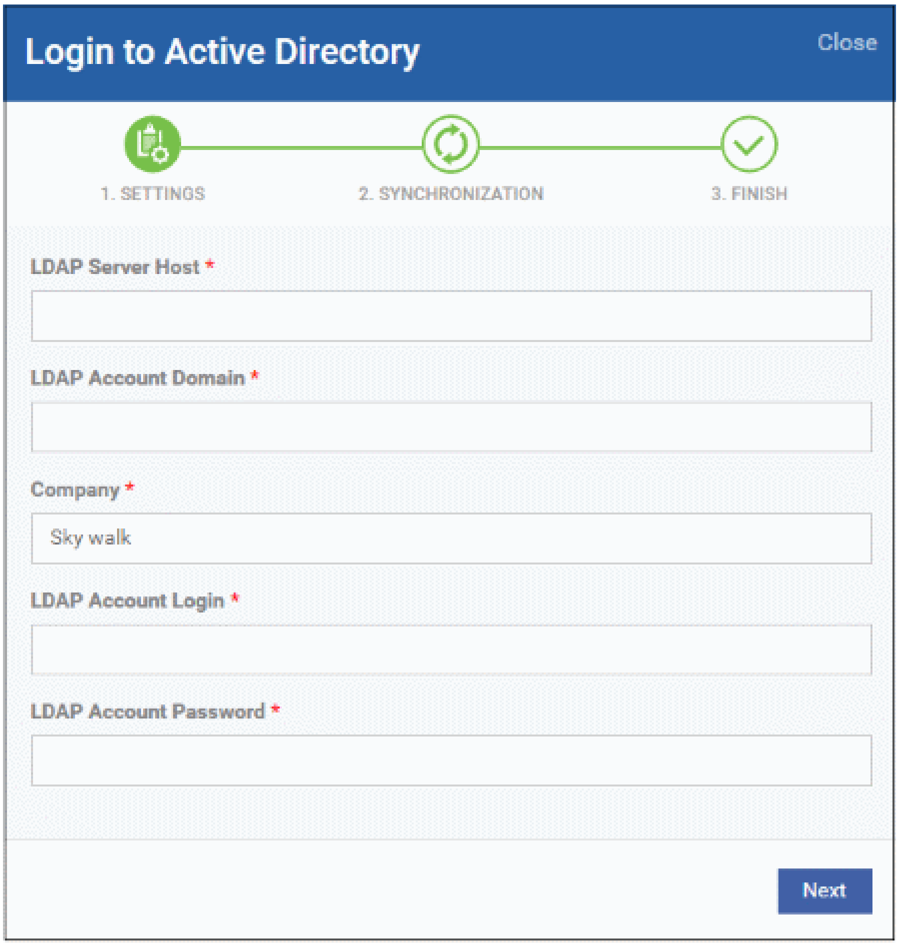
Note: ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, synchronize LDAP server via devices and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in **Appendix 1**.

To add LDAP accounts

- Click 'Add' at the top

The 'Login to Active Directory' dialog will be displayed.

Step 1 - Enter LDAP account details



Login to Active Directory

LDAP Server Host *

LDAP Account Domain *

Company *

Sky walk

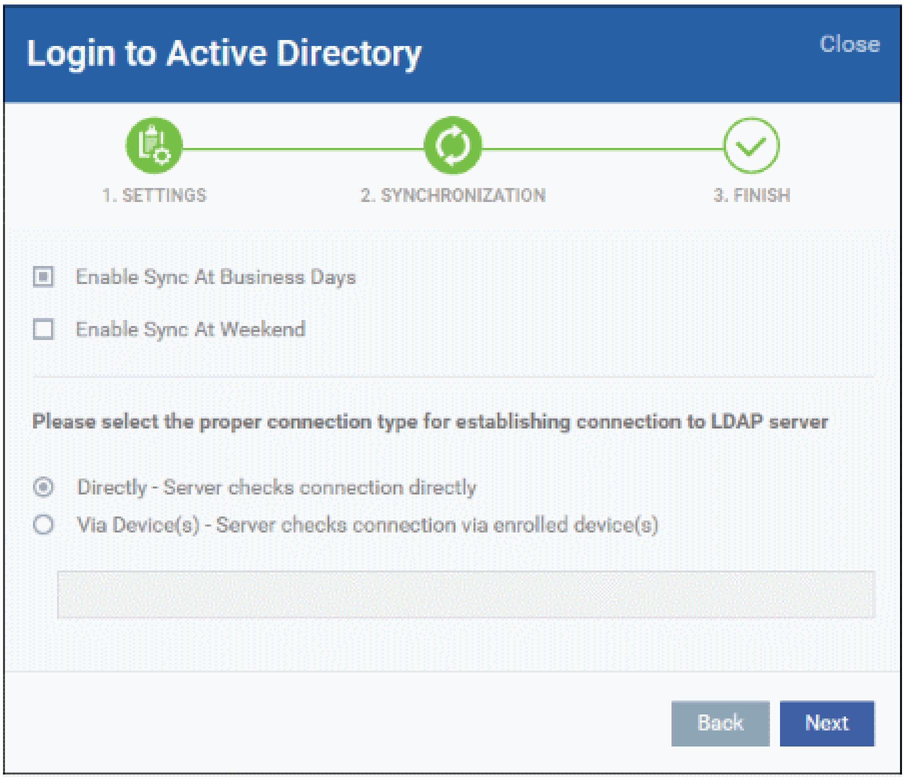
LDAP Account Login *

LDAP Account Password *

- **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



☒ Enable Sync At Business Days

□ Enable Sync At Weekend

Please select the proper connection type for establishing connection to LDAP server

● Directly - Server checks connection directly

○ Via Device(s) - Server checks connection via enrolled device(s)

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.

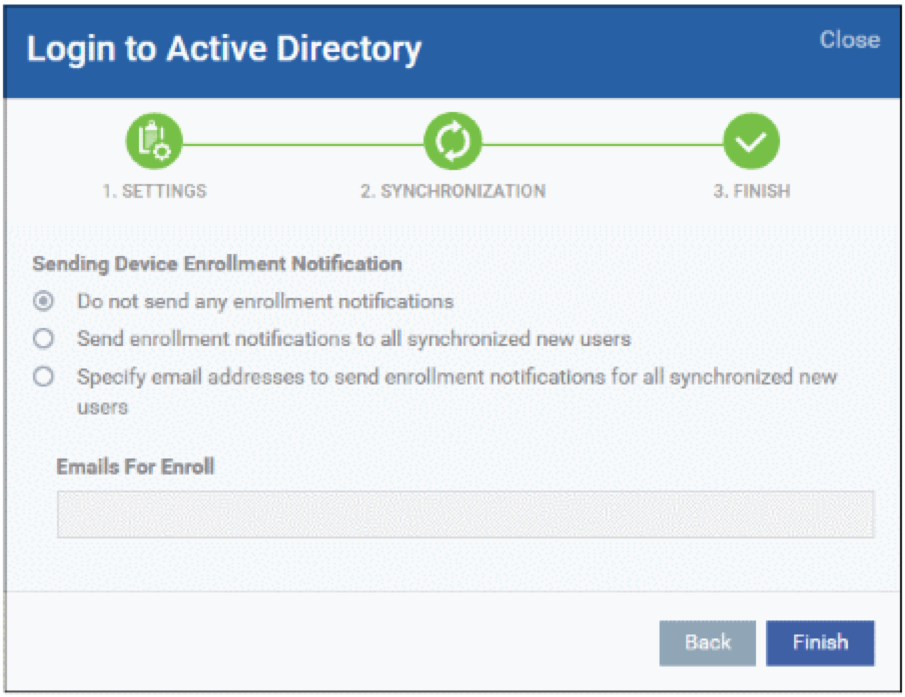
Note - you can manually sync at any time by clicking the 'Sync with LDAP' button.

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



Login to Active Directory

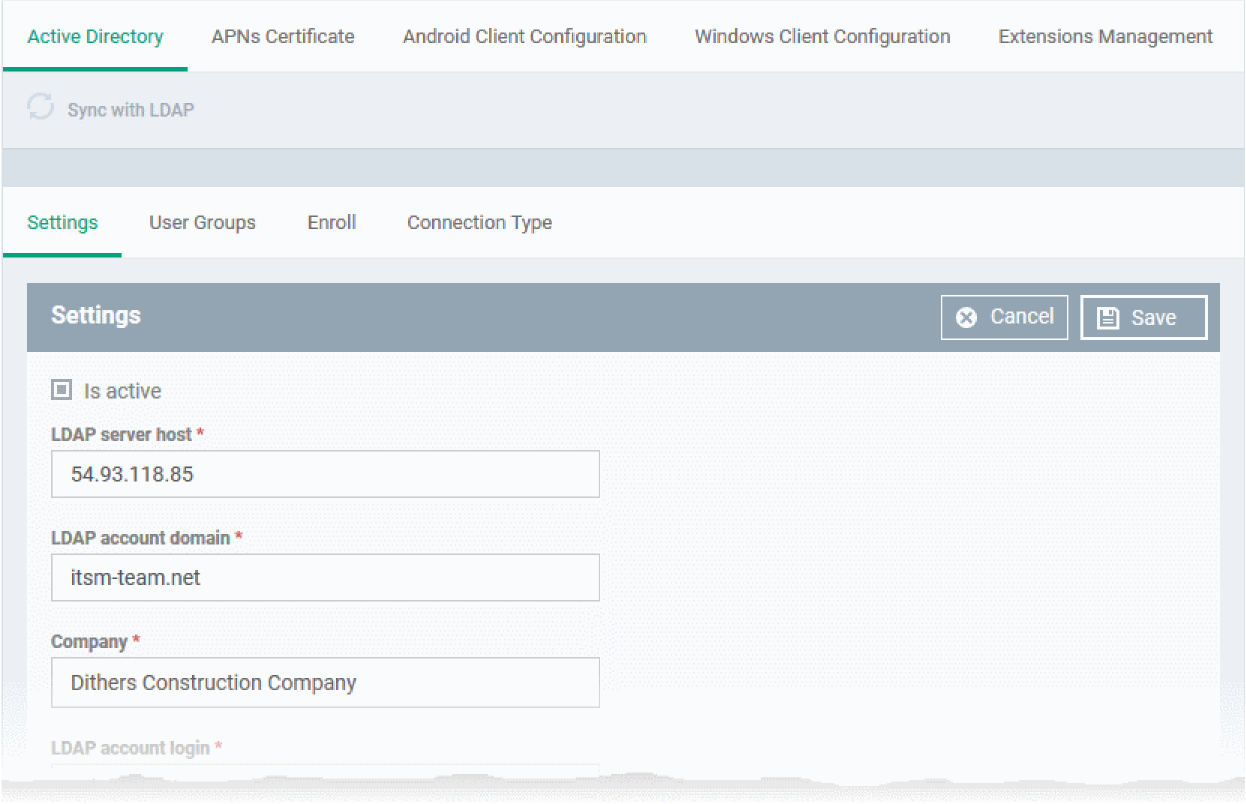
Sending Device Enrollment Notification

- ● Do not send any enrollment notifications
- ○ Send enrollment notifications to all synchronized new users
- ○ Specify email addresses to send enrollment notifications for all synchronized new users

Emails For Enroll

  - 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:



□ Is active

LDAP server host *: 54.93.118.85

LDAP account domain *: itsm-team.net

Company *: Dithers Construction Company

LDAP account login *

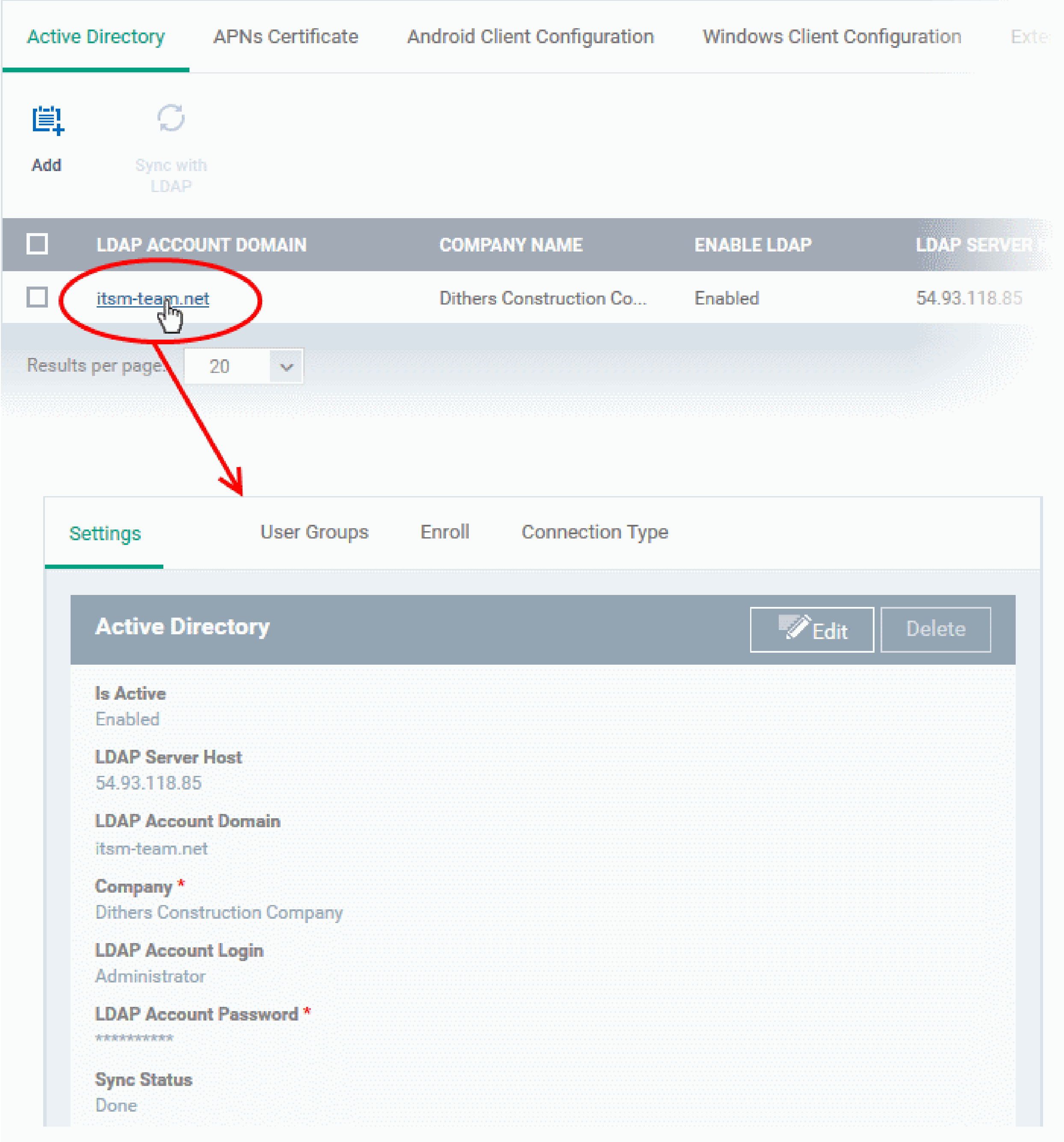
- Click 'Save' to complete the set up process.

The synchronization task will run and the user groups will be added. You have to select the group and enable sync to import users into their respective groups. You also have to select roles for imported users.

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.



□	LDAP ACCOUNT DOMAIN	COMPANY NAME	ENABLE LDAP	LDAP SERVER
□	itsm-team.net	Dithers Construction Co...	Enabled	54.93.118.85

Is Active
Enabled

LDAP Server Host
54.93.118.85

LDAP Account Domain
itsm-team.net

Company *
Dithers Construction Company

LDAP Account Login
Administrator

LDAP Account Password *
****

Sync Status
Done

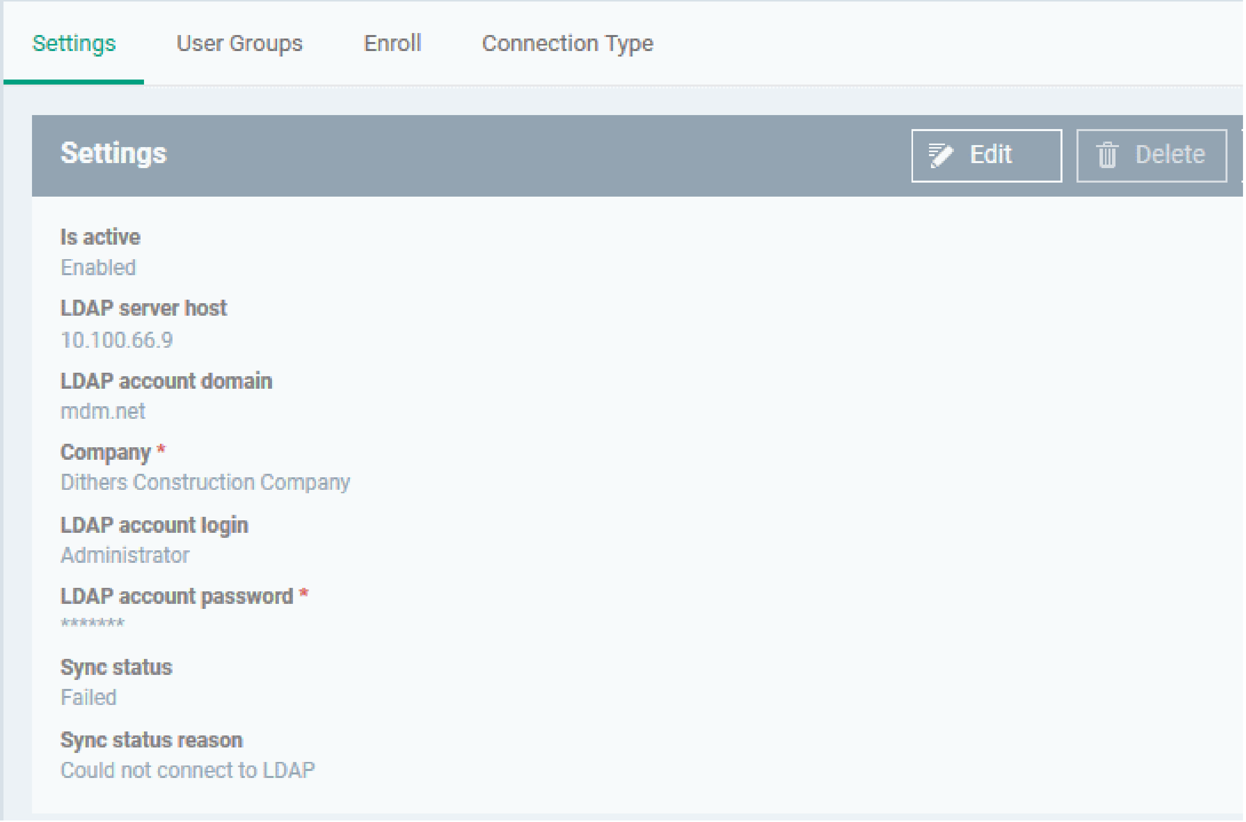
The Active Directory details will be displayed under four tabs:

- Settings
- User Groups
- Enroll

- Connection Type

Settings tab

The 'Settings' tab displays AD configuration details:



Is active
Enabled

LDAP server host
10.100.66.9

LDAP account domain
mdm.net

Company *
Dithers Construction Company

LDAP account login
Administrator

LDAP account password *
****

Sync status
Failed

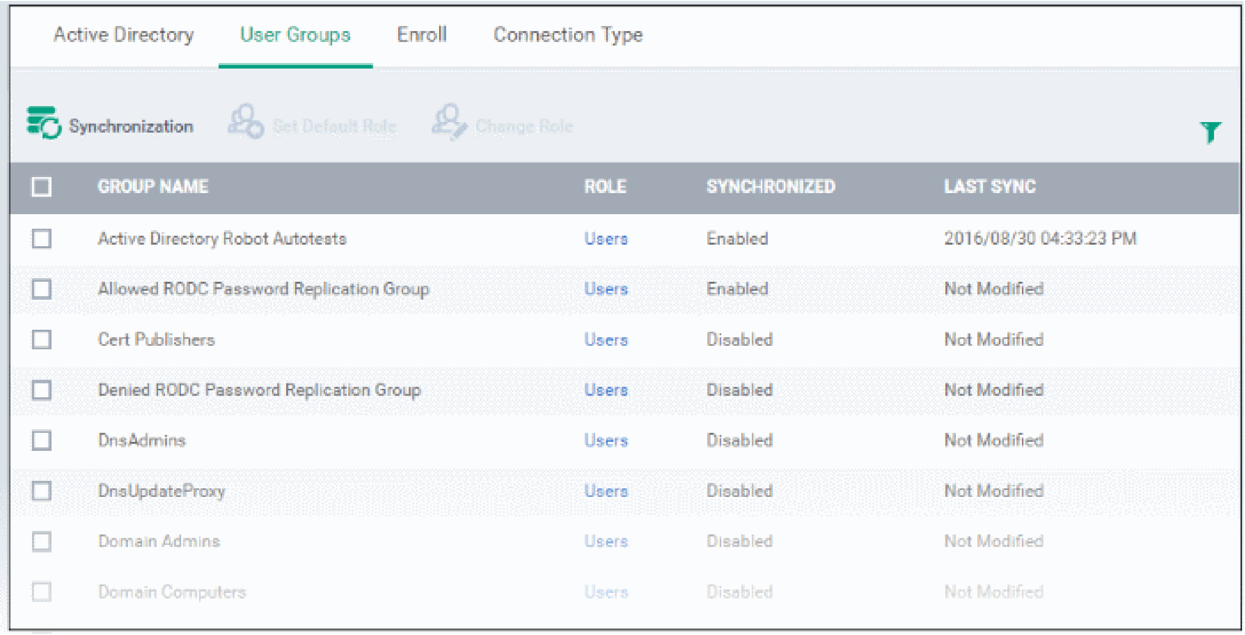
Sync status reason
Could not connect to LDAP

- Click 'Edit' to update any LDAP details and click the 'Save' button

User Groups tab

The 'User Groups' tab shows groups that were identified on the AD server. This includes users/groups created in the root folder and all sub-folders/custom folders on the AD server. This interface allows you to:

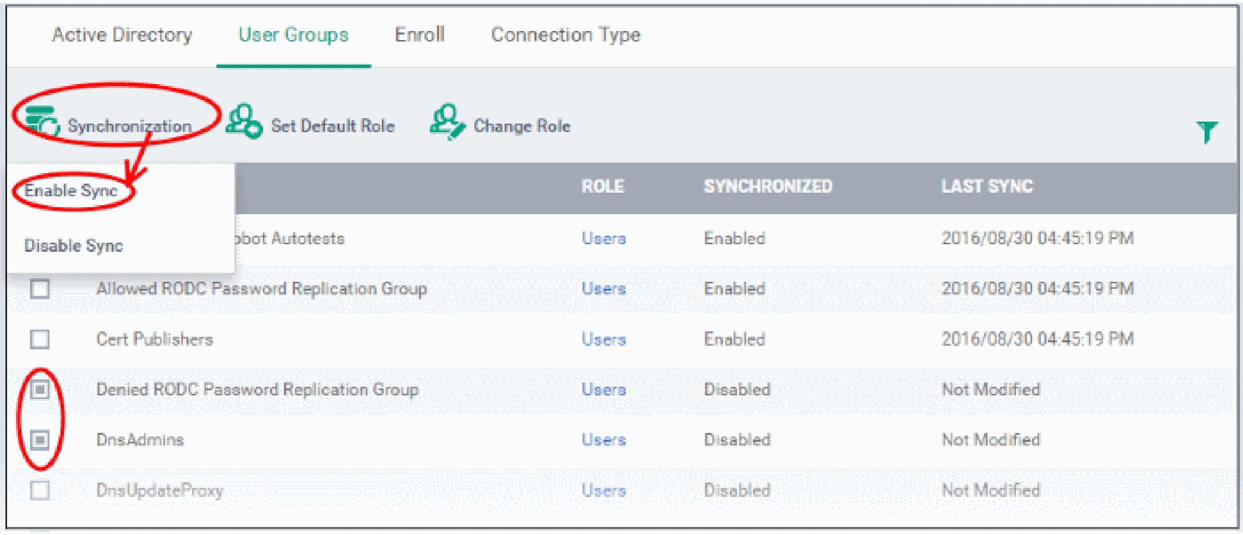
- Selectively enable/disable AD synchronization for groups. Synchronization allows ITSM to update its user list whenever users are added/removed from the AD sever.
- Select the roles to be applied to users in each AD group.
- Manually synchronize groups before importing to ITSM



□	GROUP NAME	ROLE	SYNCHRONIZED	LAST SYNC
□	Active Directory Robot Autotests	Users	Enabled	2016/08/30 04:33:23 PM
□	Allowed RODC Password Replication Group	Users	Enabled	Not Modified
□	Cert Publishers	Users	Disabled	Not Modified
□	Denied RODC Password Replication Group	Users	Disabled	Not Modified
□	DnsAdmins	Users	Disabled	Not Modified
□	DnsUpdateProxy	Users	Disabled	Not Modified
□	Domain Admins	Users	Disabled	Not Modified
□	Domain Computers	Users	Disabled	Not Modified

To enable/disable synchronization

- Select user group(s) from the list and click 'Synchronization' at the top:

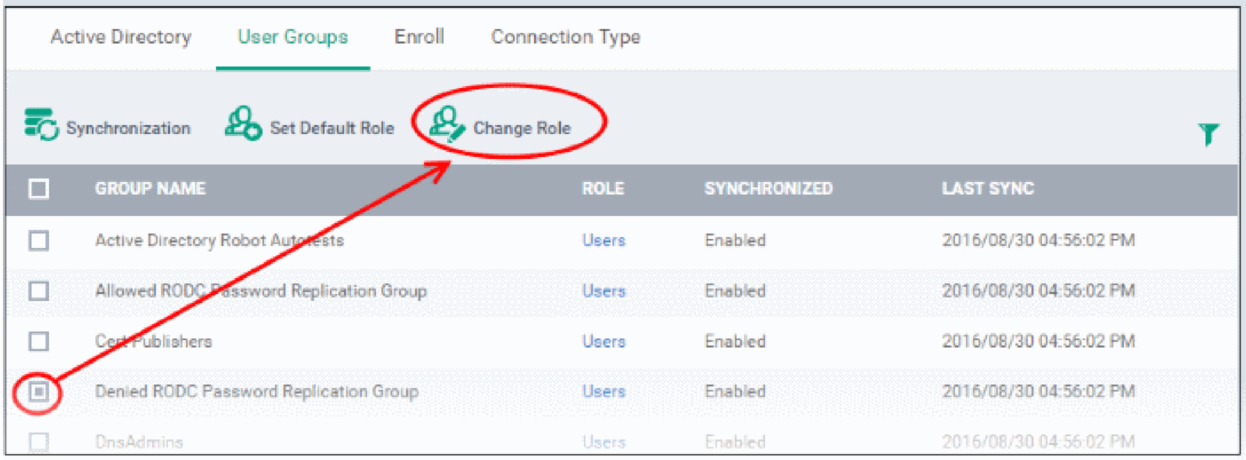


		ROLE	SYNCHRONIZED	LAST SYNC
	bot Autotests	Users	Enabled	2016/08/30 04:45:19 PM
□	Allowed RODC Password Replication Group	Users	Enabled	2016/08/30 04:45:19 PM
□	Cert Publishers	Users	Enabled	2016/08/30 04:45:19 PM
☑	Denied RODC Password Replication Group	Users	Disabled	Not Modified
☑	DnsAdmins	Users	Disabled	Not Modified
□	DnsUpdateProxy	Users	Disabled	Not Modified

- Select whether synchronization should be enabled or not from the drop-down. If enabled, ITSM will periodically synchronize with the group to import new users and remove deleted users.

To assign roles to the users to be imported

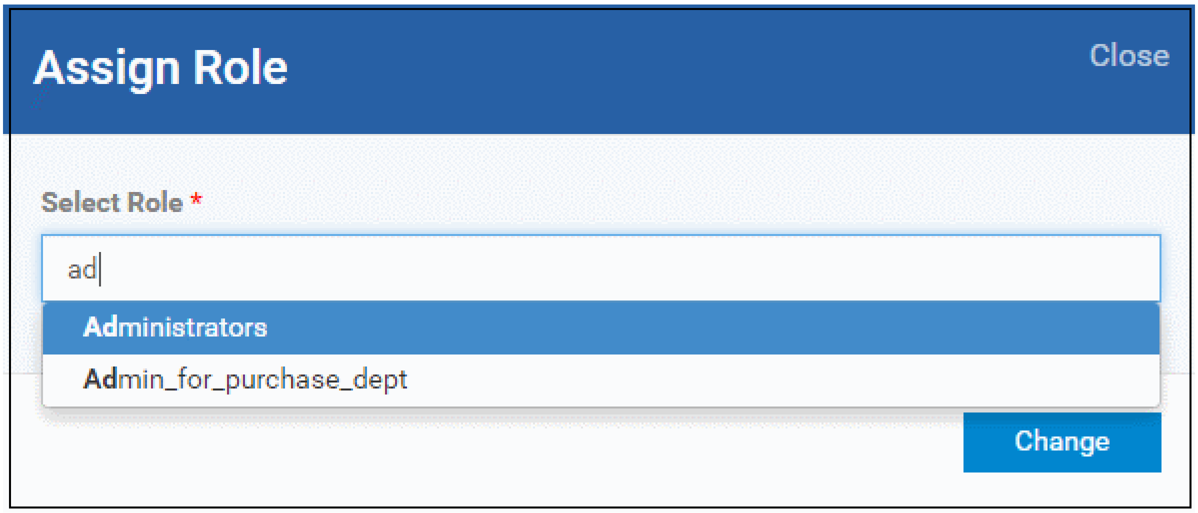
- Select the user(s)/user group(s).
- Select 'Set Default Role' to assign the default ITSM user role to the users. See **Set a role as the default role** if you need help with this.



□	GROUP NAME	ROLE	SYNCHRONIZED	LAST SYNC
□	Active Directory Robot Autotests	Users	Enabled	2016/08/30 04:56:02 PM
□	Allowed RODC Password Replication Group	Users	Enabled	2016/08/30 04:56:02 PM
□	Cert Publishers	Users	Enabled	2016/08/30 04:56:02 PM
☑	Denied RODC Password Replication Group	Users	Enabled	2016/08/30 04:56:02 PM
□	DnsAdmins	Users	Enabled	2016/08/30 04:56:02 PM

- Select 'Change Role' if you want to assign a different role to imported users.

The 'Assign Role' dialog will appear.



Select Role *: ad

- Select the role from the drop-down and click 'Change'.

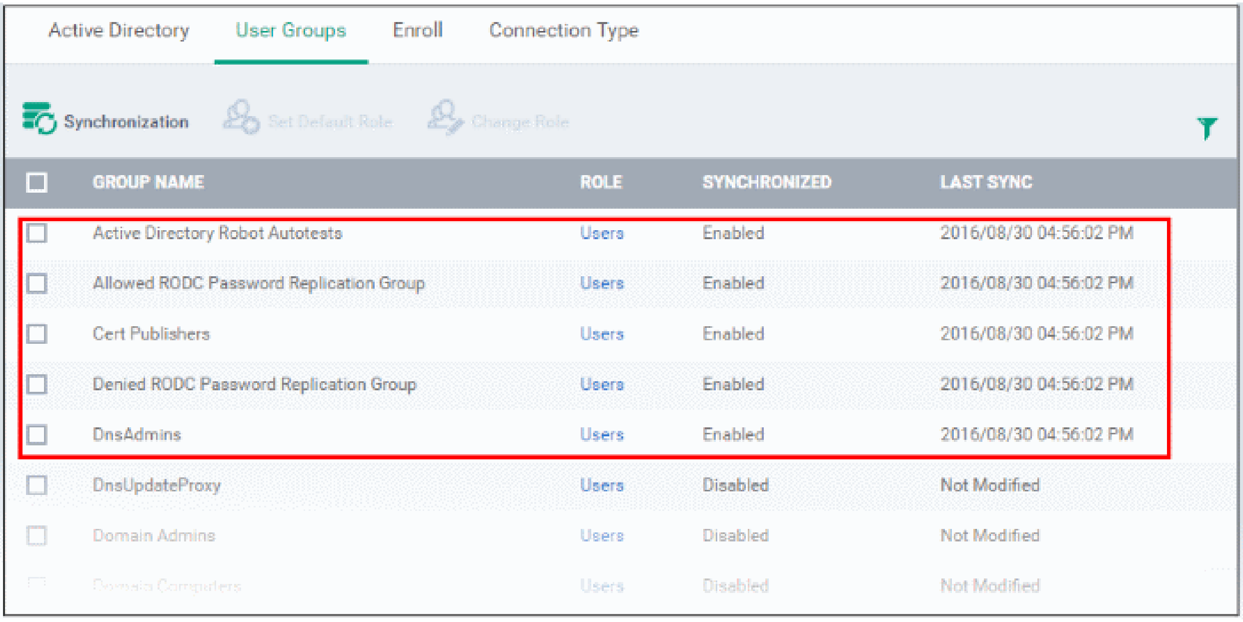
The selected role will be displayed in the 'Role' column for the user(s)/user group(s).

- Repeat the process to apply different roles to different user(s)/user group(s).

See '**Managing Roles Assigned to a User**' for more details on roles.

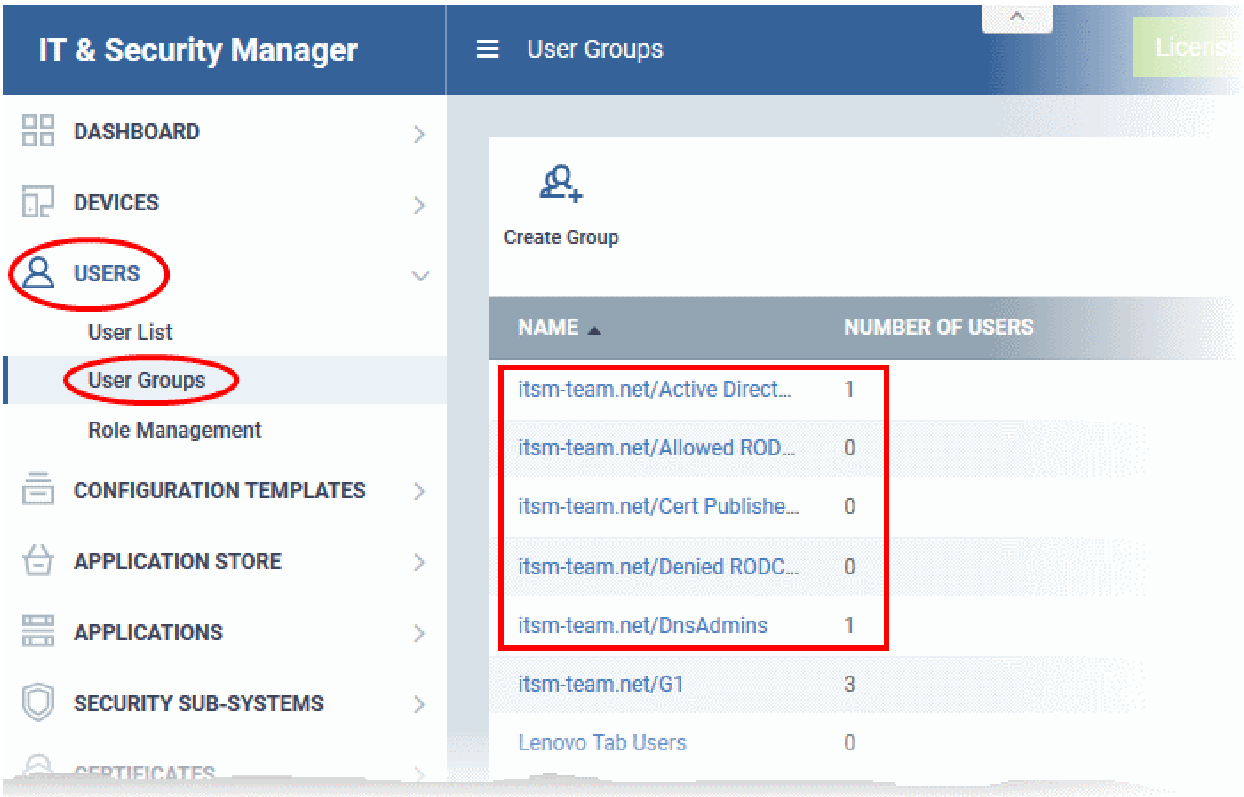
To import users from selected user group

- Click 'Sync with LDAP'



□	GROUP NAME	ROLE	SYNCHRONIZED	LAST SYNC
□	Active Directory Robot Autotests	Users	Enabled	2016/08/30 04:56:02 PM
□	Allowed RODC Password Replication Group	Users	Enabled	2016/08/30 04:56:02 PM
□	Cert Publishers	Users	Enabled	2016/08/30 04:56:02 PM
□	Denied RODC Password Replication Group	Users	Enabled	2016/08/30 04:56:02 PM
□	DnsAdmins	Users	Enabled	2016/08/30 04:56:02 PM
□	DnsUpdateProxy	Users	Disabled	Not Modified
□	Domain Admins	Users	Disabled	Not Modified
□	Domain Computers	Users	Disabled	Not Modified

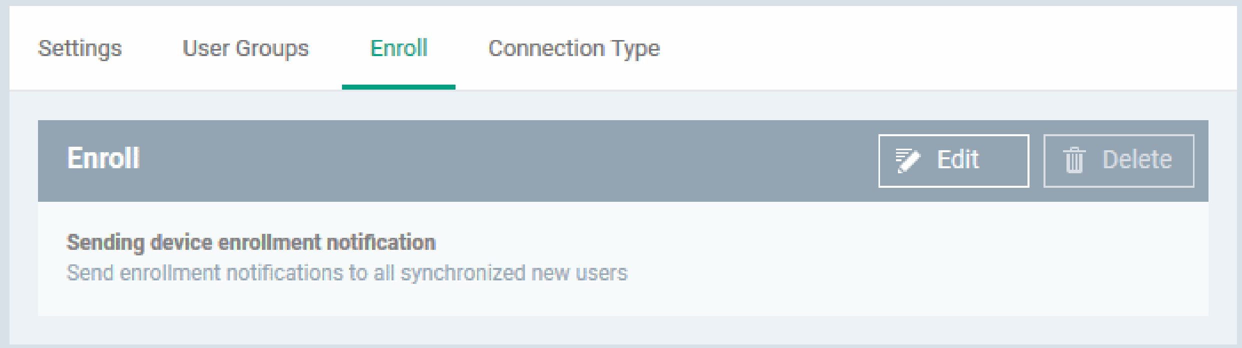
- The user(s)/user group(s) in the LDAP will be synchronized ITSM and the users will be imported into ITSM. The users will be added to the 'User List'/'User Groups' interface appropriately For more details on management of users, see the section '**Users and User Groups**'.



NAME ▲	NUMBER OF USERS
itsm-team.net/Active Direct...	1
itsm-team.net/Allowed ROD...	0
itsm-team.net/Cert Publishe...	0
itsm-team.net/Denied RODC...	0
itsm-team.net/DnsAdmins	1
itsm-team.net/G1	3
Lenovo Tab Users	0

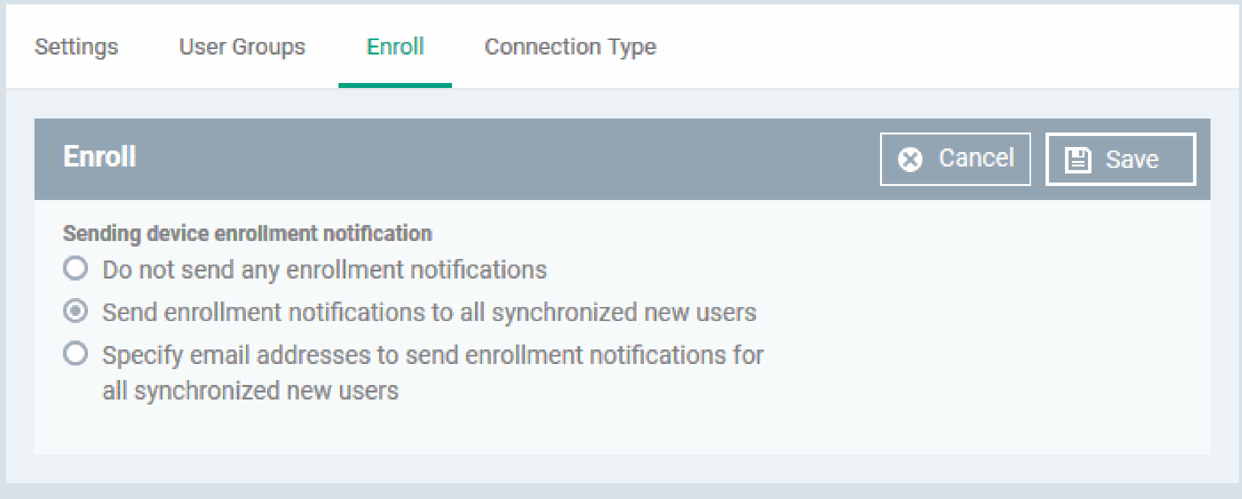
Enroll tab

The 'Enroll' tab displays the current setting of enrollment notification sent to imported users.



Sending device enrollment notification
Send enrollment notifications to all synchronized new users

- Click 'Edit' to change the enrollment notification type



Sending device enrollment notification

○ Do not send any enrollment notifications

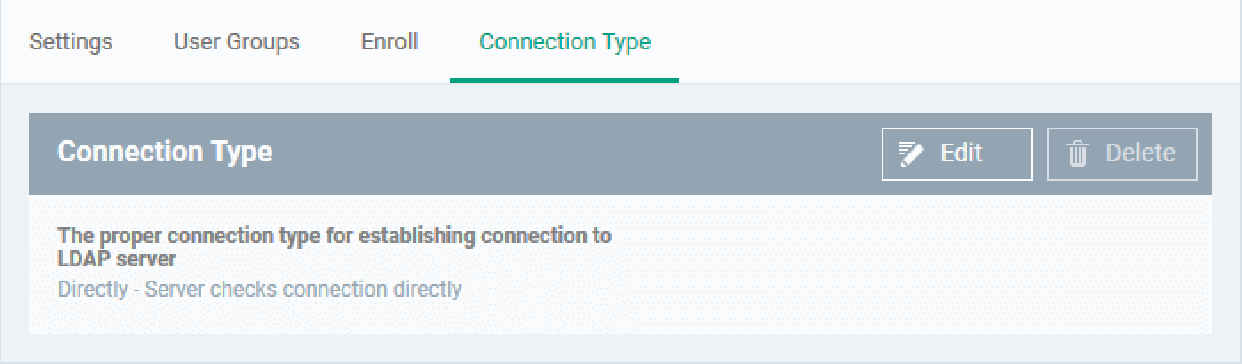
● Send enrollment notifications to all synchronized new users

○ Specify email addresses to send enrollment notifications for all synchronized new users

  - 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'

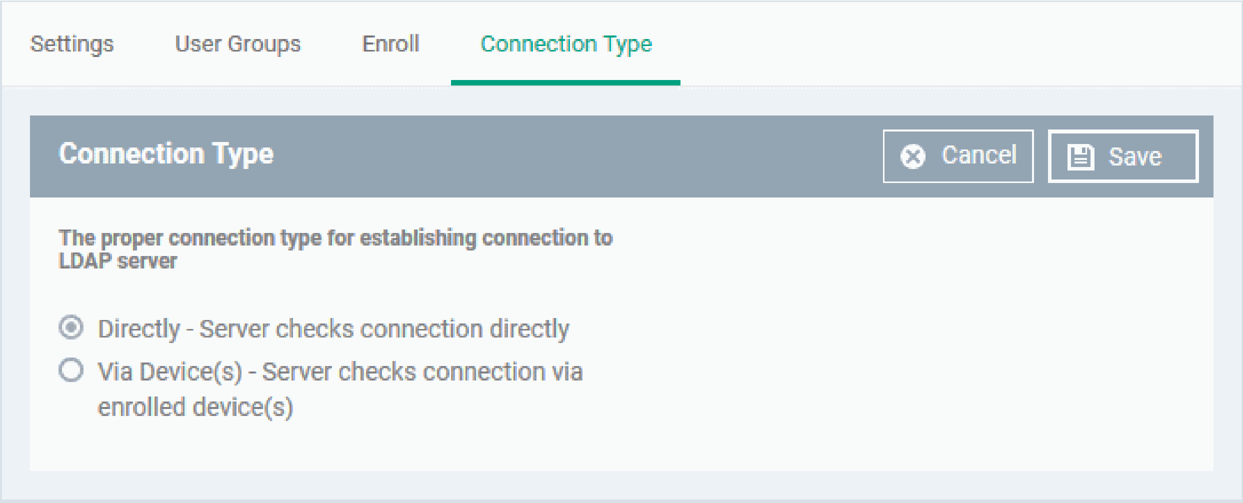
Connection Type Tab

The Connection Type tab displays how the AD server currently connects to ITSM.



The proper connection type for establishing connection to LDAP server
Directly - Server checks connection directly

- Click the 'Edit' button to change the connection type.



Connection Type

The proper connection type for establishing connection to LDAP server

● Directly - Server checks connection directly

○ Via Device(s) - Server checks connection via enrolled device(s)

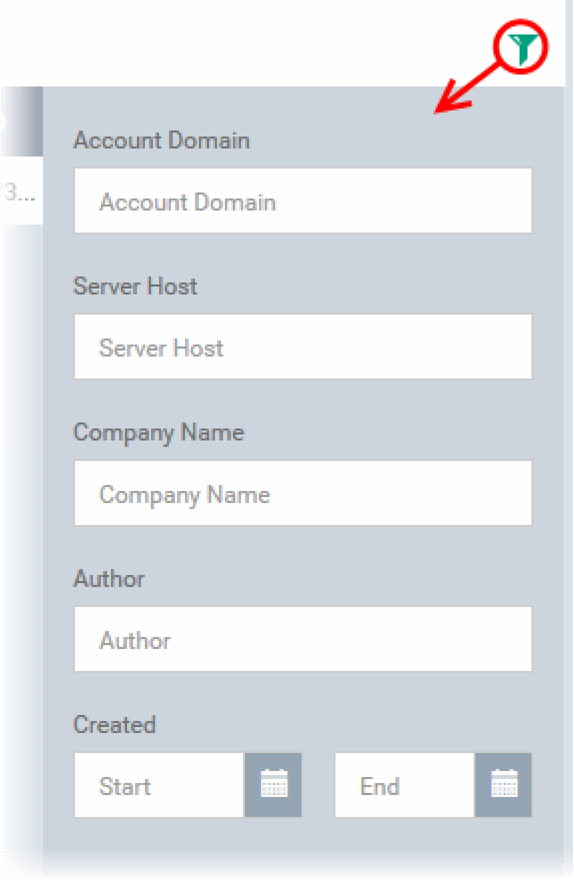
If the first option is selected, ITSM will connect to the configured LDAP server directly. The second option enables the ITSM server to connect to the LDAP server via enrolled devices. Multiple devices can be configured for the second option.

- 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.

Active Directory Interface - Sorting, Search and Filter Options

- Click on the column headers sorts items in alphabetical, ascending/descending order
- Click the funnel button to open filter options:



Account Domain: Account Domain

Server Host: Server Host

Company Name: Company Name

Author: Author

Created: Start End

- You can search for a specific LDAP account based by domain name, host, company and/or author. Enter your search criteria in the respective text boxes and click 'Apply'.
- You can also filter by the date the account was created. Use the calendar buttons at the bottom to select start and end dates then click 'Apply'.

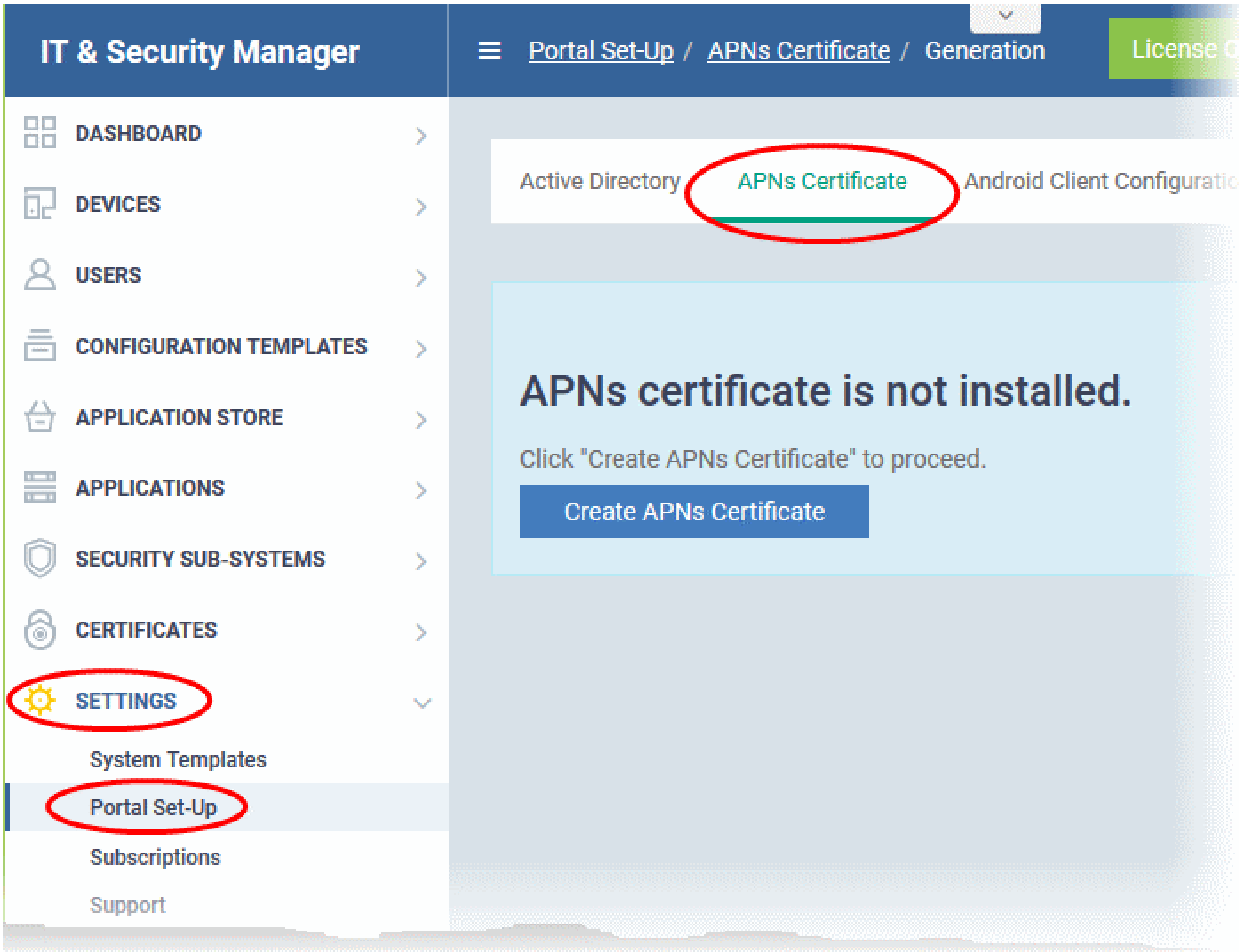
You can use any combination of filters to search for specific LDAP accounts.

11.2.2. Add 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.

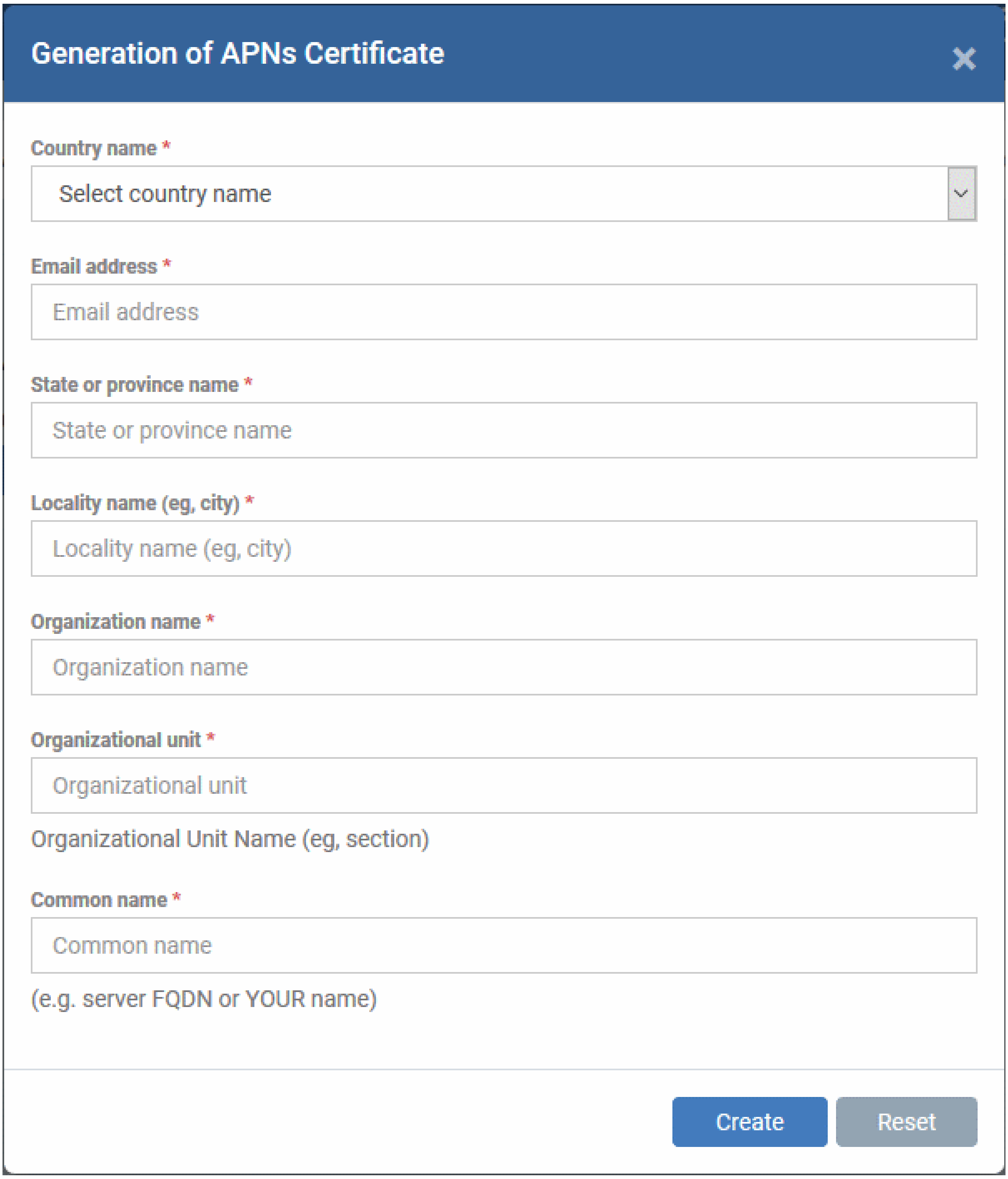


APNs certificate is not installed.

Click "Create APNs Certificate" to proceed.

- 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):



Generation of APNs Certificate

Country name *

Select country name

Email address *

Email address

State or province name *

State or province name

Locality name (eg, city) *

Locality name (eg, city)

Organization name *

Organization name

Organizational unit *

Organizational unit

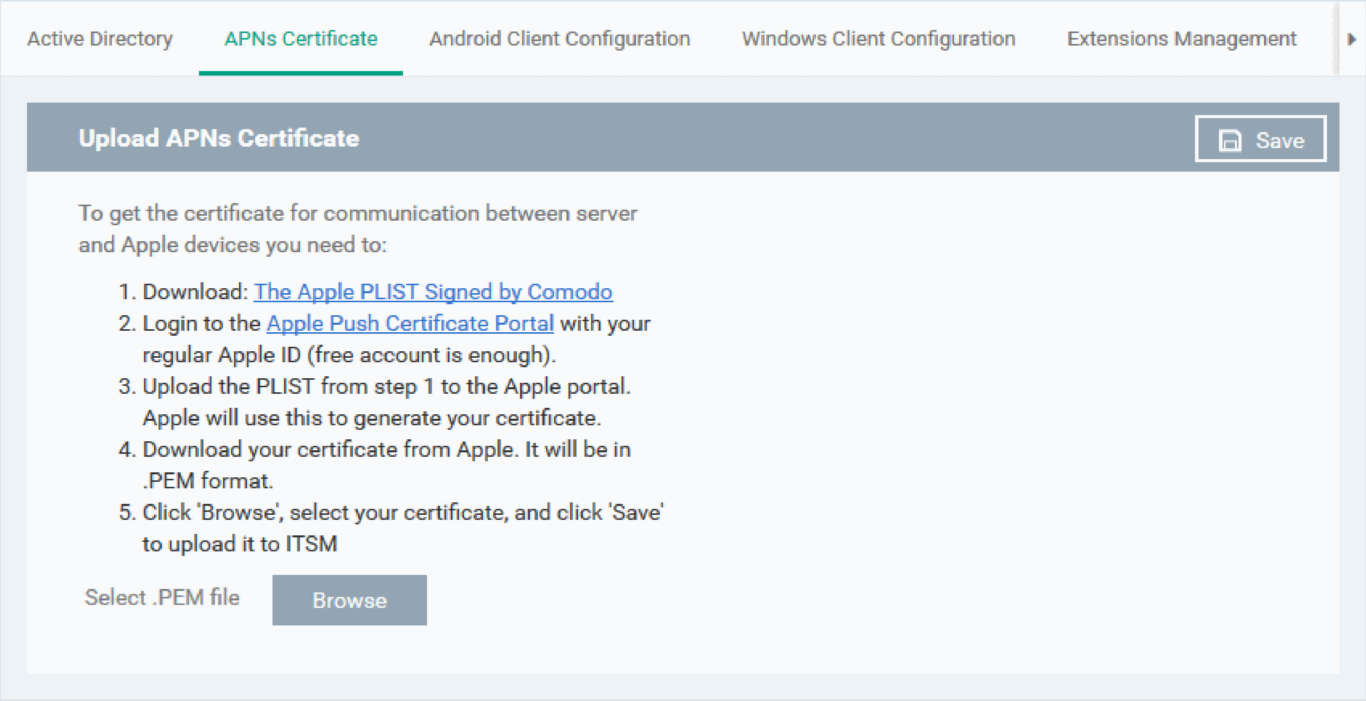
Organizational Unit Name (eg, section)

Common name *

Common name

(e.g. server FQDN or YOUR name)

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



Upload APNs Certificate

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

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

Select .PEM file

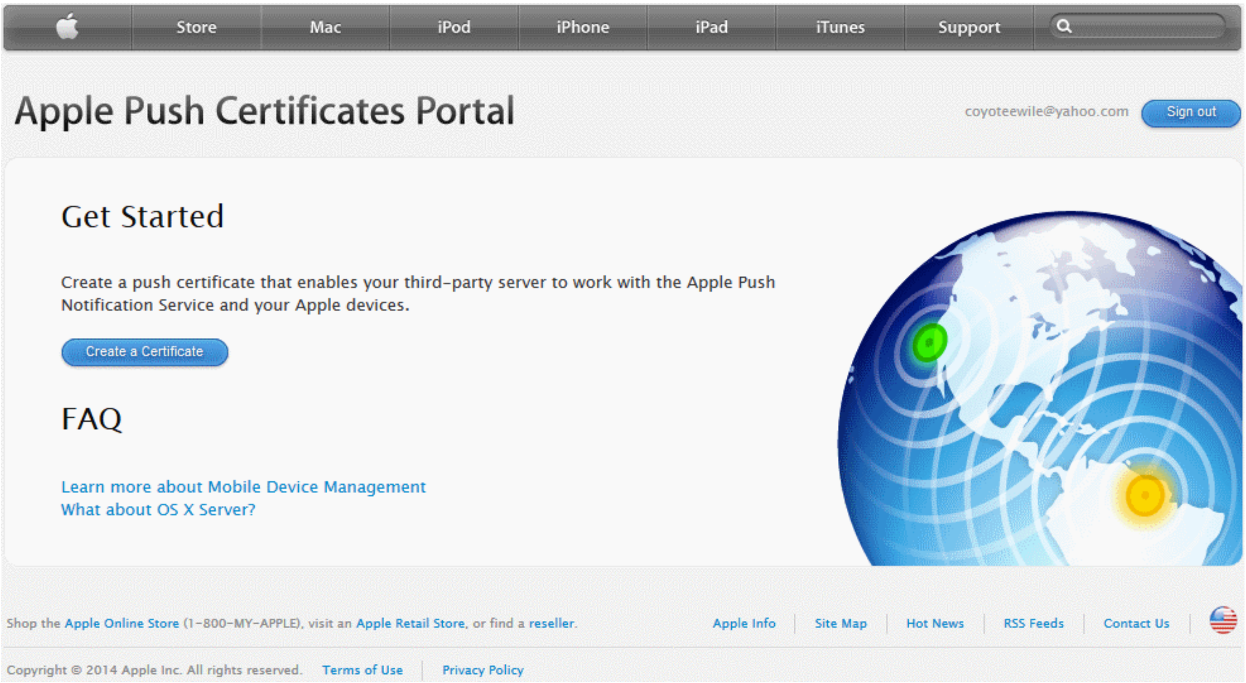
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.

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'.



Apple Push Certificates Portal

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

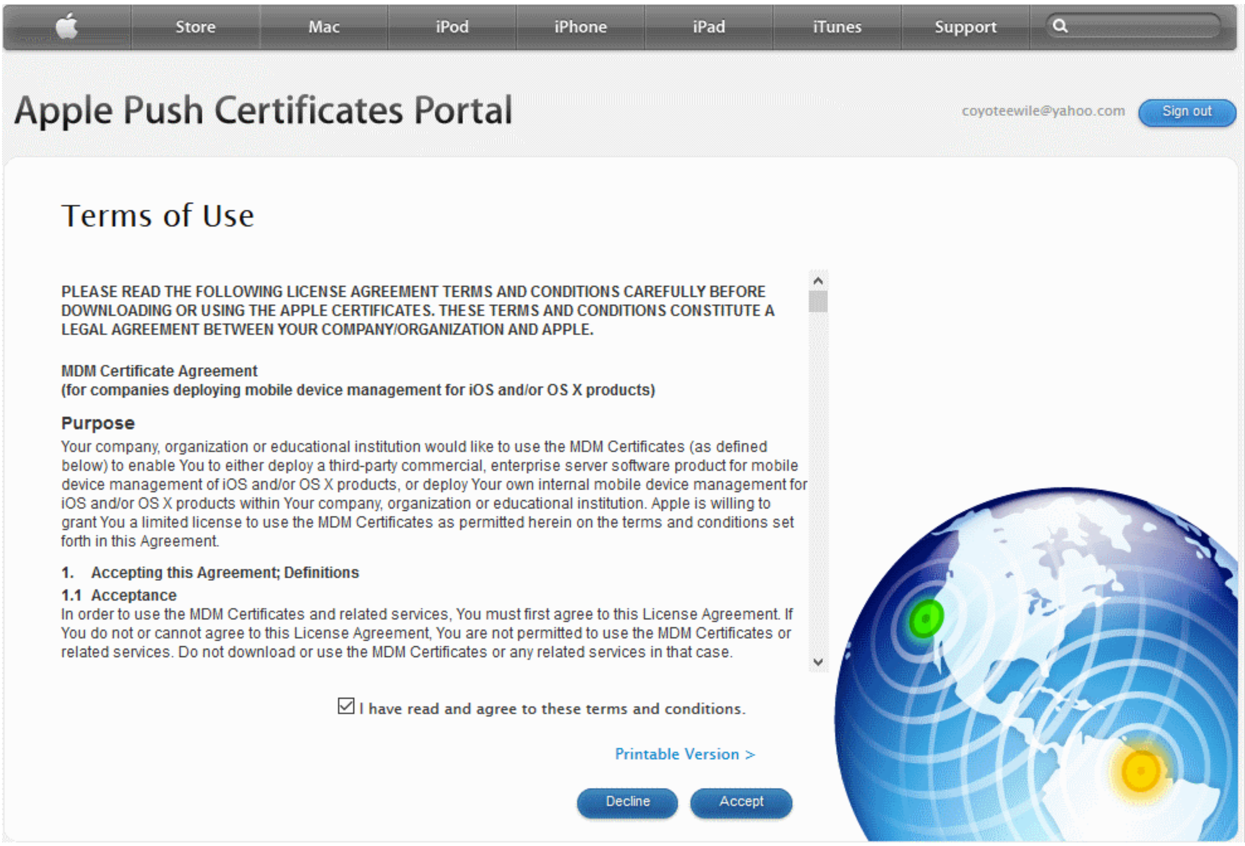
FAQ

Learn more about Mobile Device Management
What about OS X Server?

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

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



Apple Push Certificates Portal

coyoteewile@yahoo.com Sign out

Terms of Use

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

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

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

1. Accepting this Agreement; Definitions

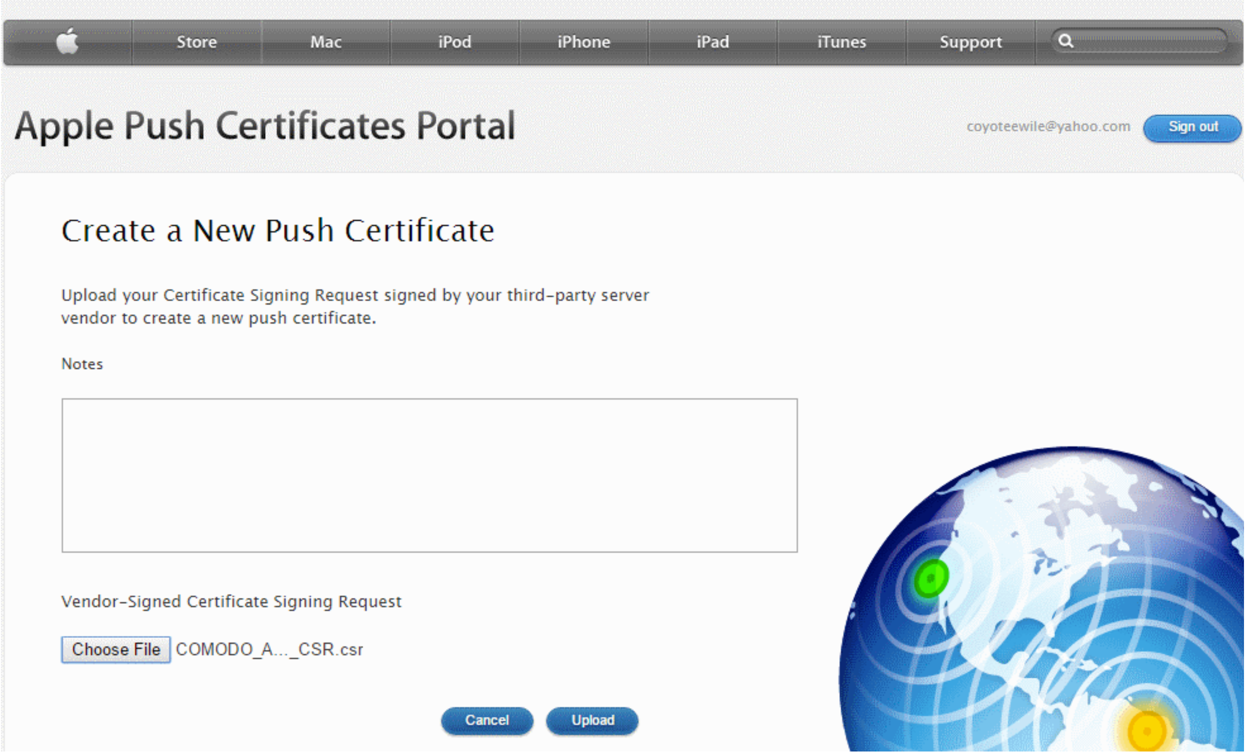
1.1 Acceptance
In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any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

☑ I have read and agree to these terms and conditions.

Printable Version >

Decline Accept

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



Apple Push Certificates Portal

coyoteewile@yahoo.com Sign out

Create a New Push Certificate

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

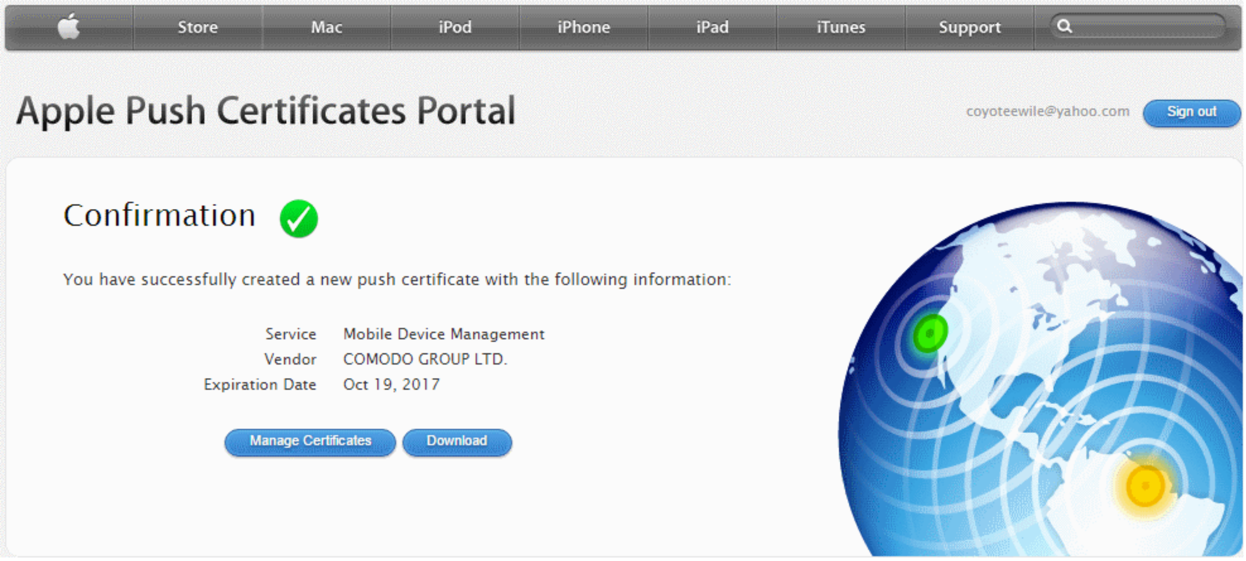
Notes

Vendor-Signed Certificate Signing Request

Choose File COMODO_A..._CSR.csr

Cancel Upload

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



Apple Push Certificates Portal

Confirmation ✓

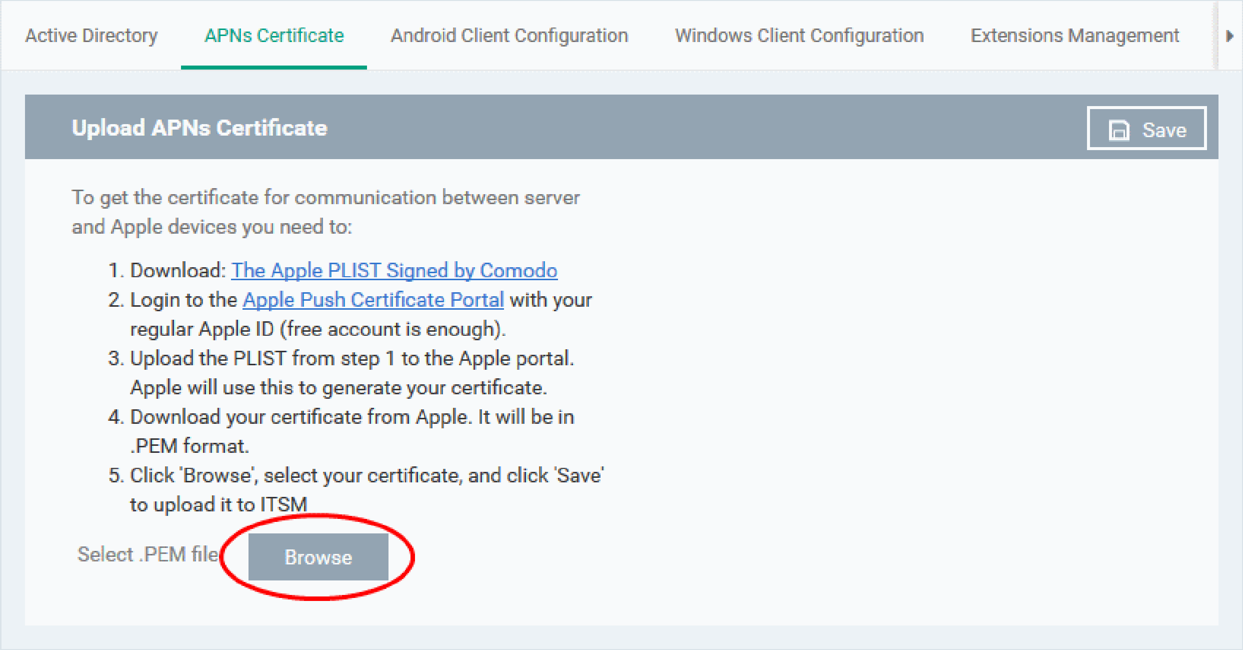
You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	COMODO GROUP LTD.
Expiration Date	Oct 19, 2017

- 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.



Upload APNs Certificate

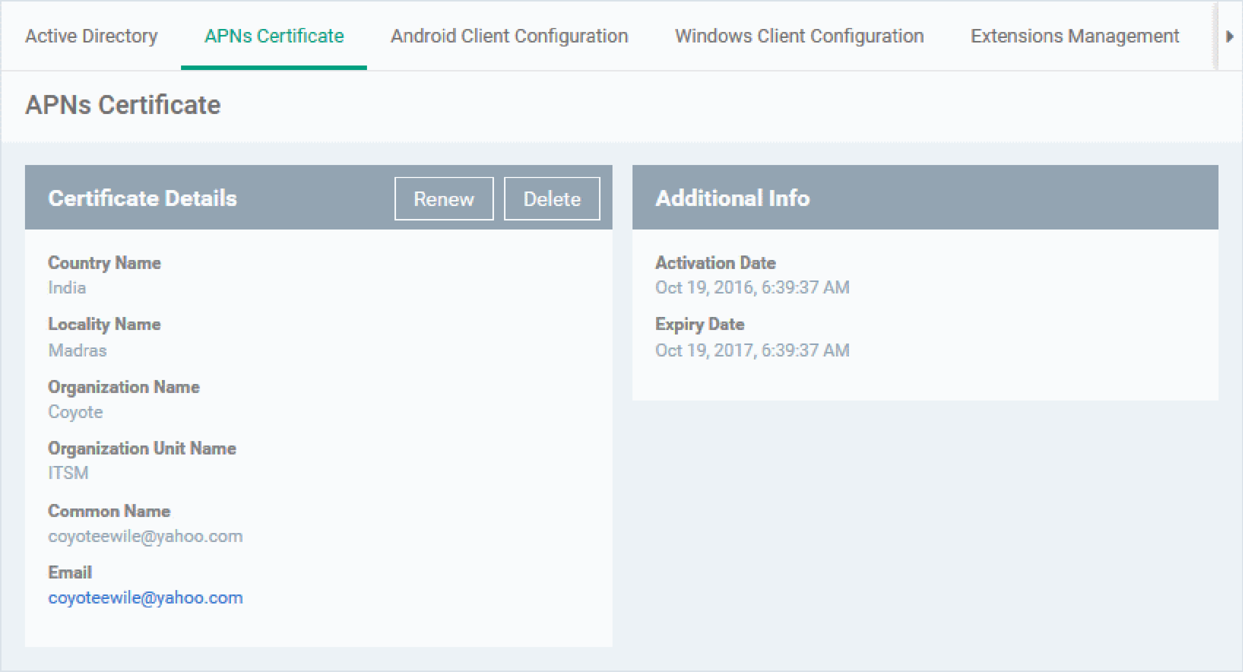
To get the certificate for communication between server and Apple devices you need to:

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

Select .PEM file

- Click 'Save' to upload your certificate.

The APNs Certificate details interface will open:



APNs Certificate

Certificate Details

Country Name
India

Locality Name
Madras

Organization Name
Coyote

Organization Unit Name
ITSM

Common Name
coyoteewile@yahoo.com

Email
coyoteewile@yahoo.com

Additional Info

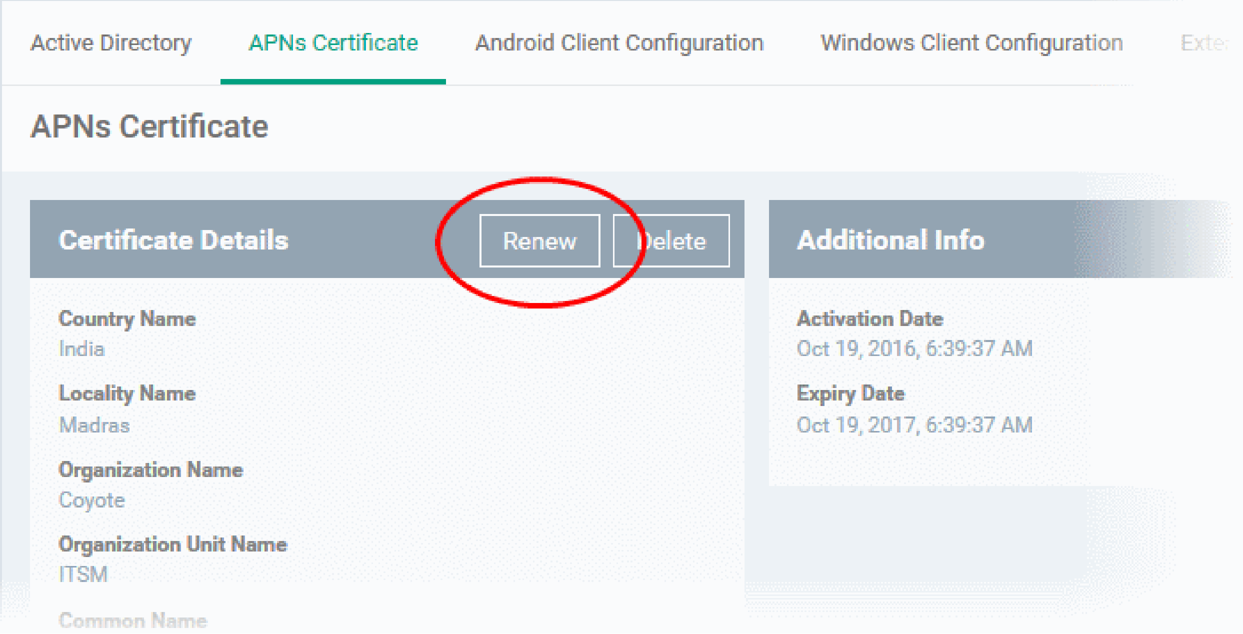
Activation Date
Oct 19, 2016, 6:39:37 AM

Expiry Date
Oct 19, 2017, 6:39:37 AM

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.



APNs Certificate

Certificate Details

Country Name
India

Locality Name
Madras

Organization Name
Coyote

Organization Unit Name
ITSM

Common Name

Additional Info

Activation Date
Oct 19, 2016, 6:39:37 AM

Expiry Date
Oct 19, 2017, 6:39:37 AM

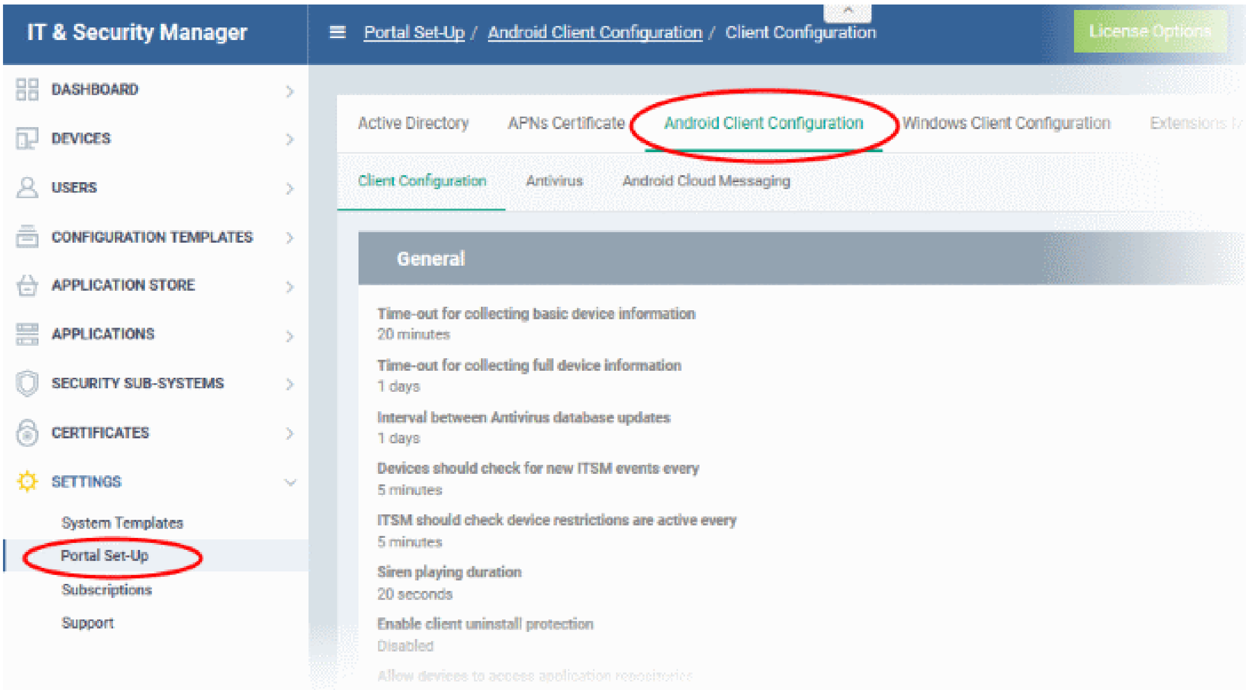
- Click 'Delete' only if you wish to remove the certificate so you can generate a new APNs certificate.

11.2.3. Configure 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



Time-out for collecting basic device information
20 minutes

Time-out for collecting full device information
1 days

Interval between Antivirus database updates
1 days

Devices should check for new ITSM events every
5 minutes

ITSM should check device restrictions are active every
5 minutes

Siren playing duration
20 seconds

Enable client uninstall protection
Disabled

Allow devices to access application repositories

The interface contains three tabs:

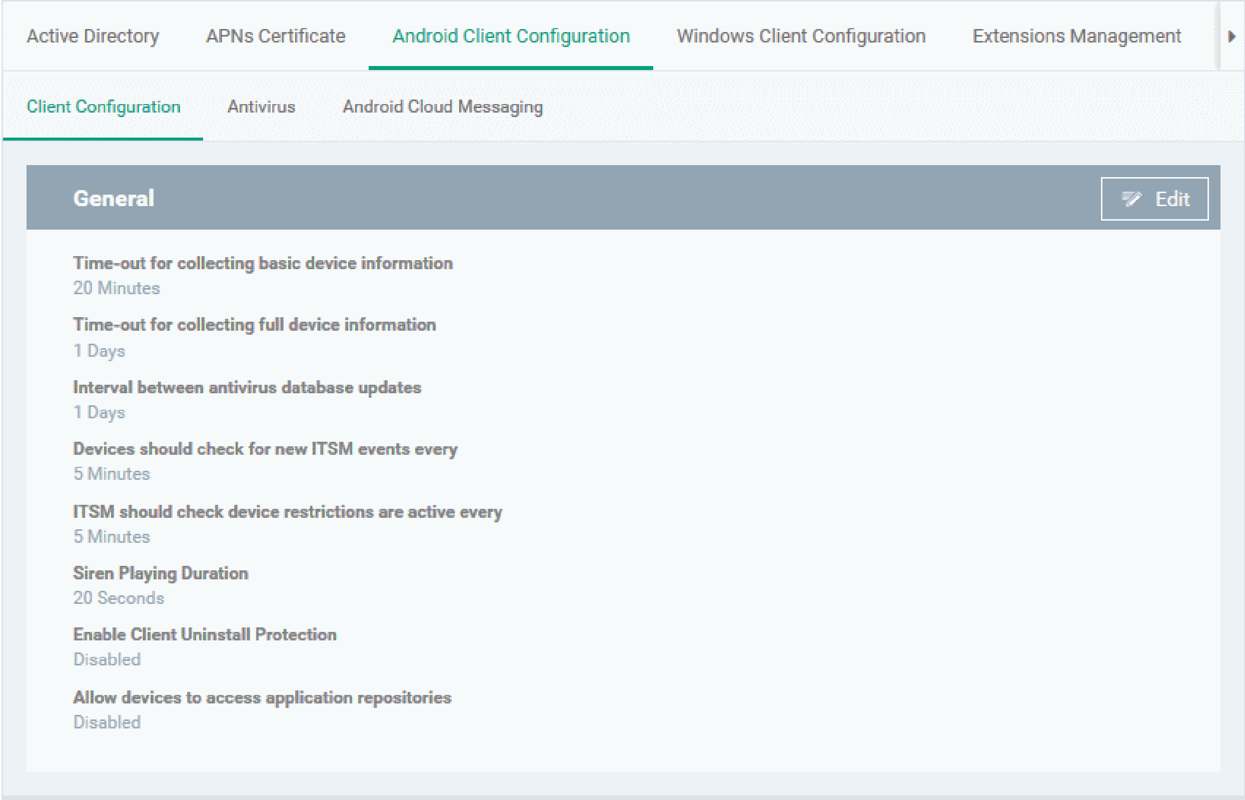
- **Client Configuration** - Allows you to configure general settings like agent and AV virus updates, polling intervals, client uninstall protection and so on. Refer to **Configuring General Settings** for more details.
- **Antivirus** - Allows you to specify whether Android viruses should be dealt 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. Configure 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



General

Time-out for collecting basic device information
20 Minutes

Time-out for collecting full device information
1 Days

Interval between antivirus database updates
1 Days

Devices should check for new ITSM events every
5 Minutes

ITSM should check device restrictions are active every
5 Minutes

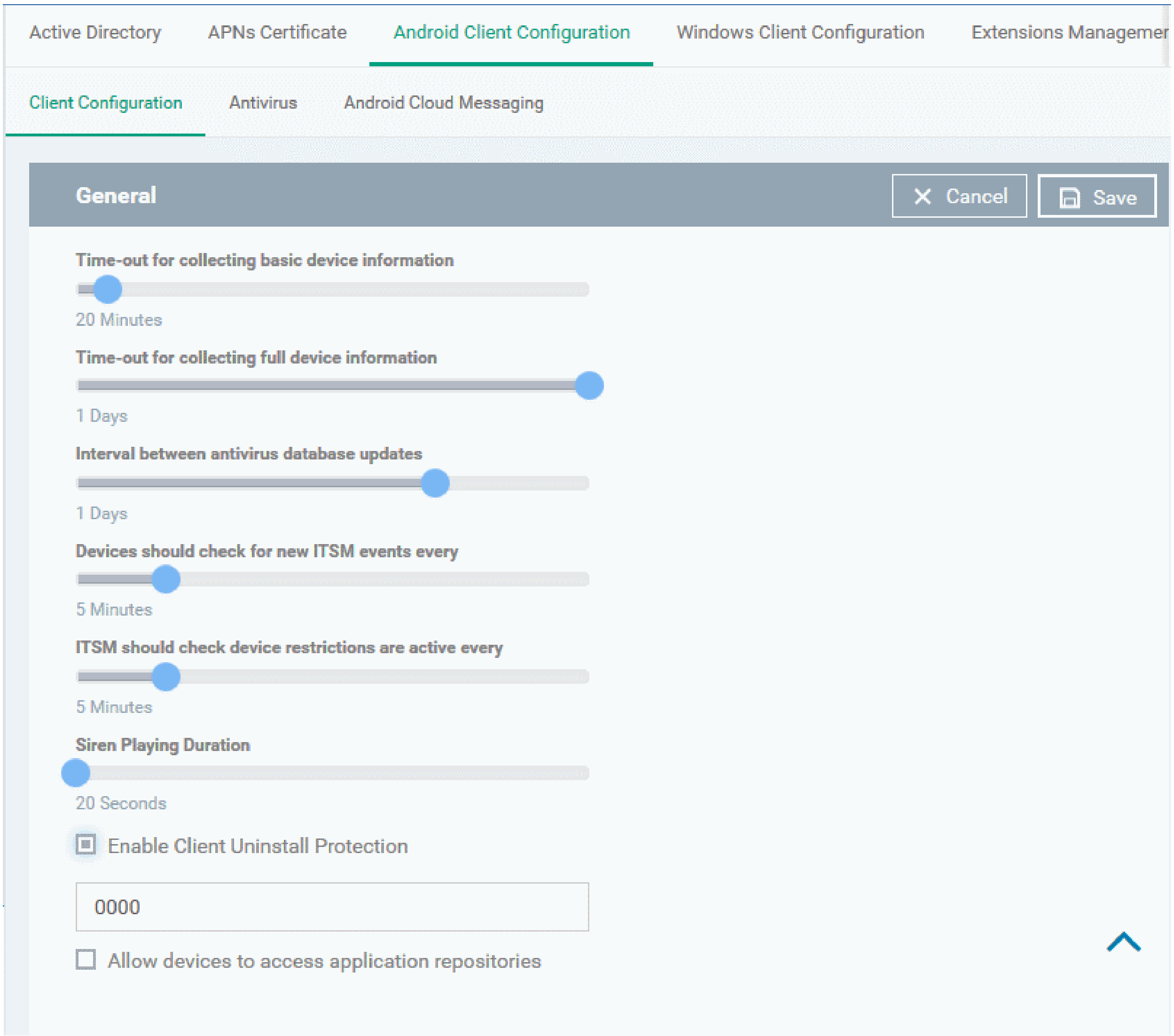
Siren Playing Duration
20 Seconds

Enable Client Uninstall Protection
Disabled

Allow devices to access application repositories
Disabled

The current settings for various parameters of Client Configuration will be displayed.

- To change the settings, click the edit button Edit on the top.



Time-out for collecting basic device information

20 Minutes

Time-out for collecting full device information

1 Days

Interval between antivirus database updates

1 Days

Devices should check for new ITSM events every

5 Minutes

ITSM should check device restrictions are active every

5 Minutes

Siren Playing Duration

20 Seconds

☒ Enable Client Uninstall Protection

0000

□ Allow devices to access application repositories

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. Configure Android Client Antivirus Settings

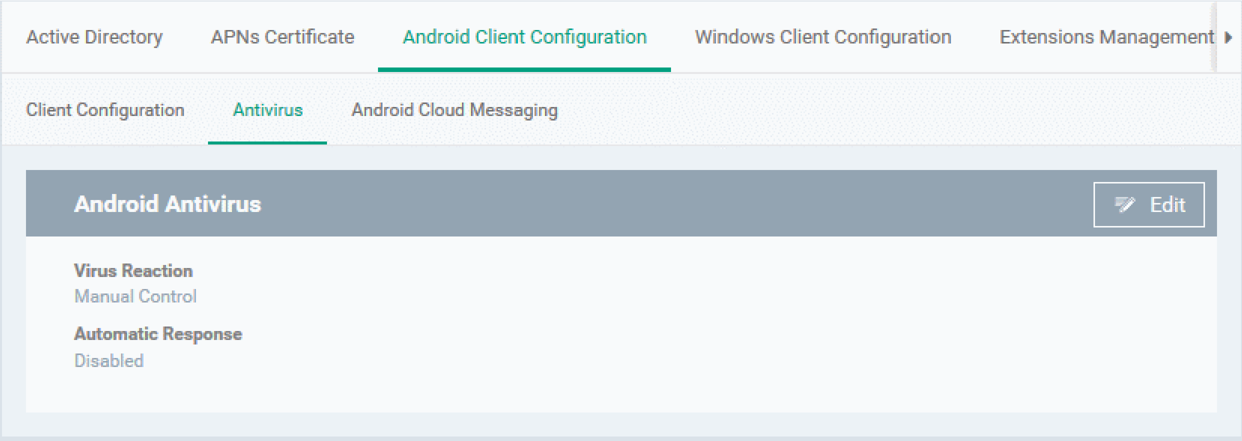
The Android Client Antivirus provides real-time protection against malware and malicious apps on Android devices. Administrators can also launch 'on-demand' scans from the ITSM administrative console on selected devices.

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:

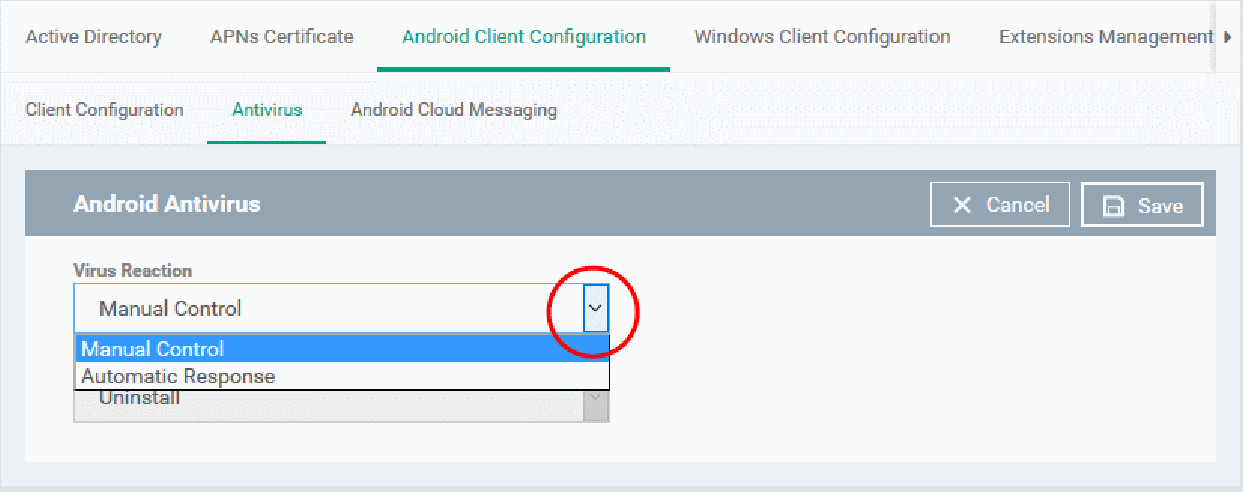


Virus Reaction
Manual Control

Automatic Response
Disabled

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.

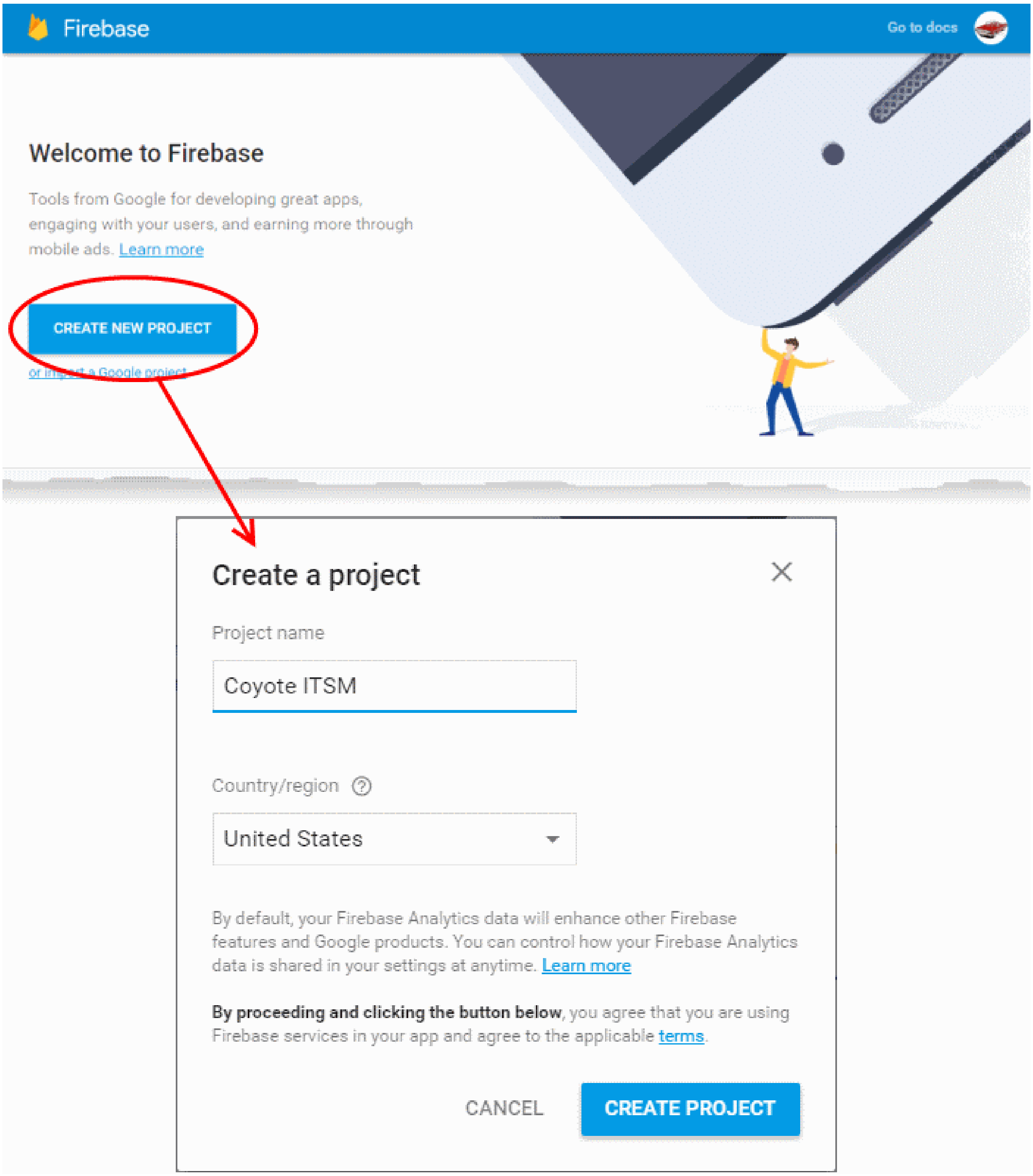
11.2.3.3. Add Google Cloud Messaging (GCM) Token

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.



Welcome to Firebase

Tools from Google for developing great apps, engaging with your users, and earning more through mobile ads. Learn more

Create a project

Project name: Coyote ITSM

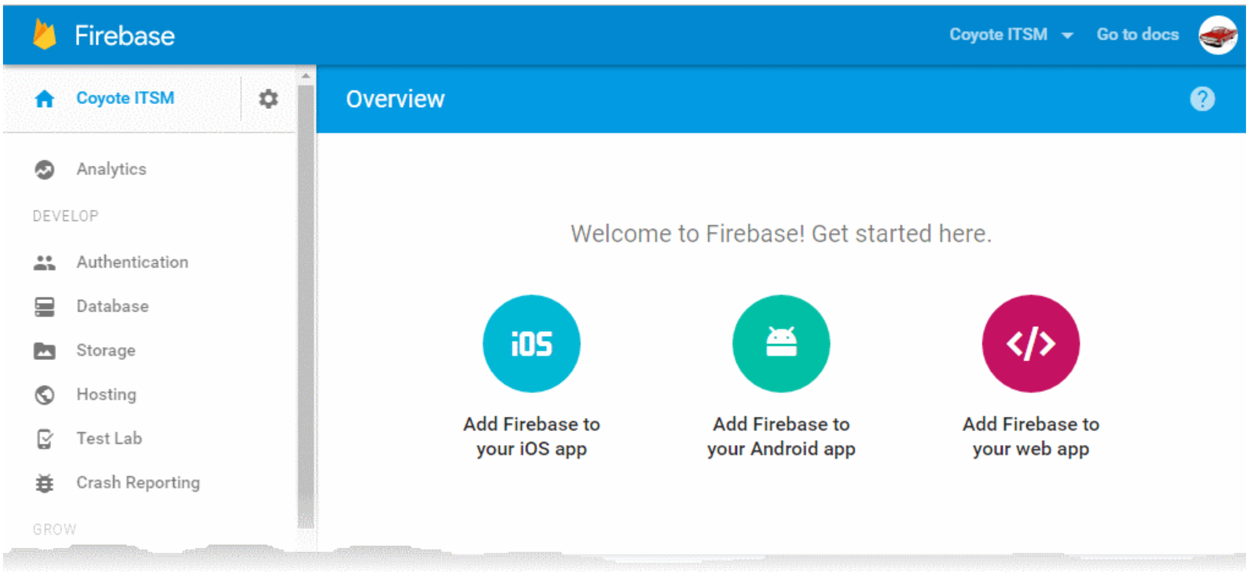
Country/region: United States

By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at anytime. Learn more

By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable terms.

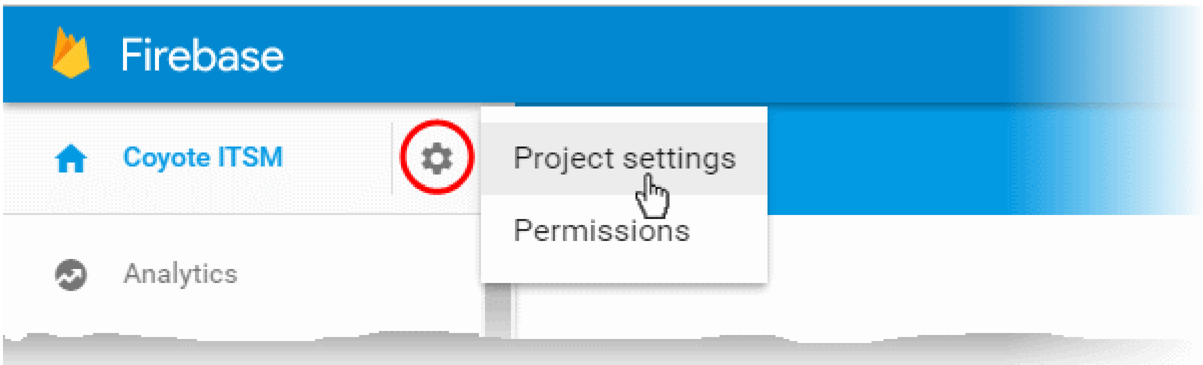
- Click 'Create Project'
- Type a name for the new project in the 'Project Name' field
- Select your country from the 'Country/region' drop-down
- Click 'Create Project'.

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



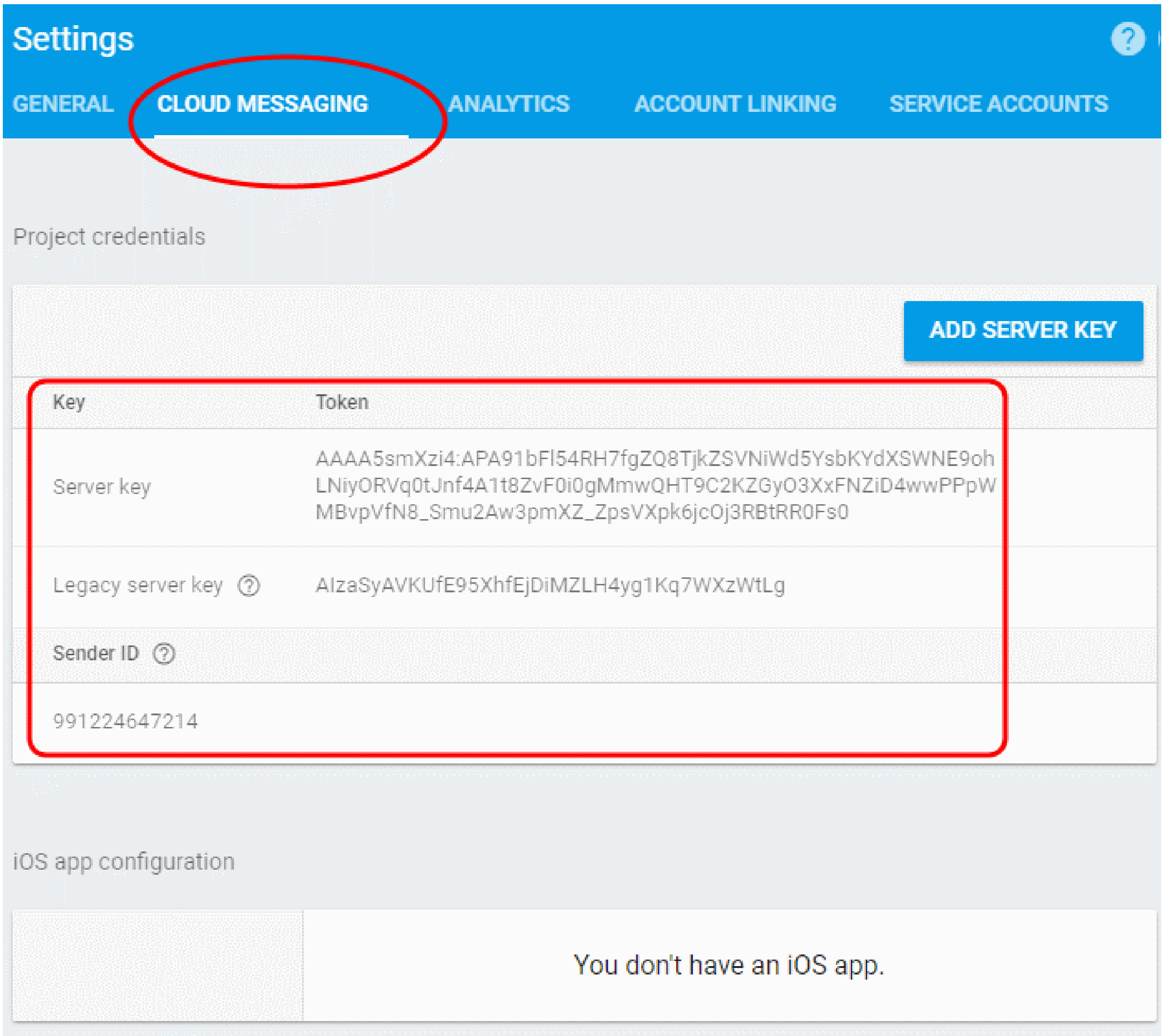
Step 2 - Obtain GCM Token and Project number

- 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.



Project credentials

Key	Token
Server key	AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0
Legacy server key	AIzaSyAVKUfE95XhfEjDiMZLH4yg1Kq7WXzWtLg

Sender ID

991224647214

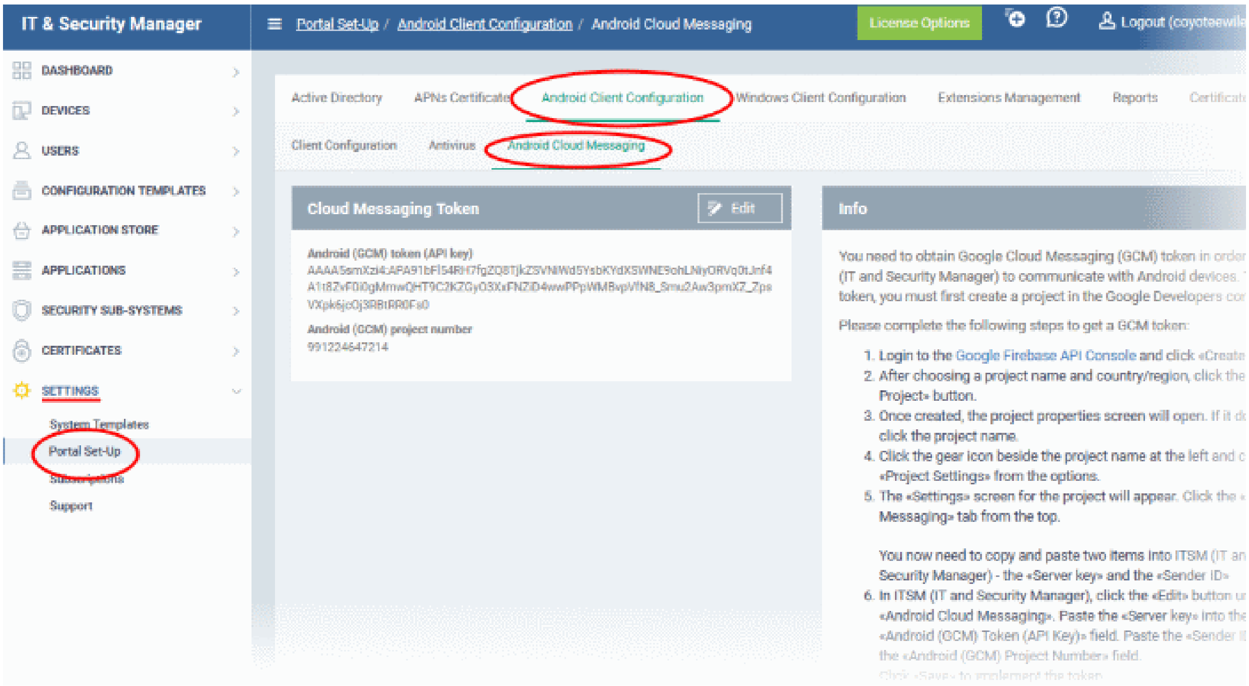
iOS app configuration

You don't have an iOS app.

- 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



Android (GCM) token (API key)
AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number
991224647214

You need to obtain Google Cloud Messaging (GCM) token in order (IT and Security Manager) to communicate with Android devices. token, you must first create a project in the Google Developers co

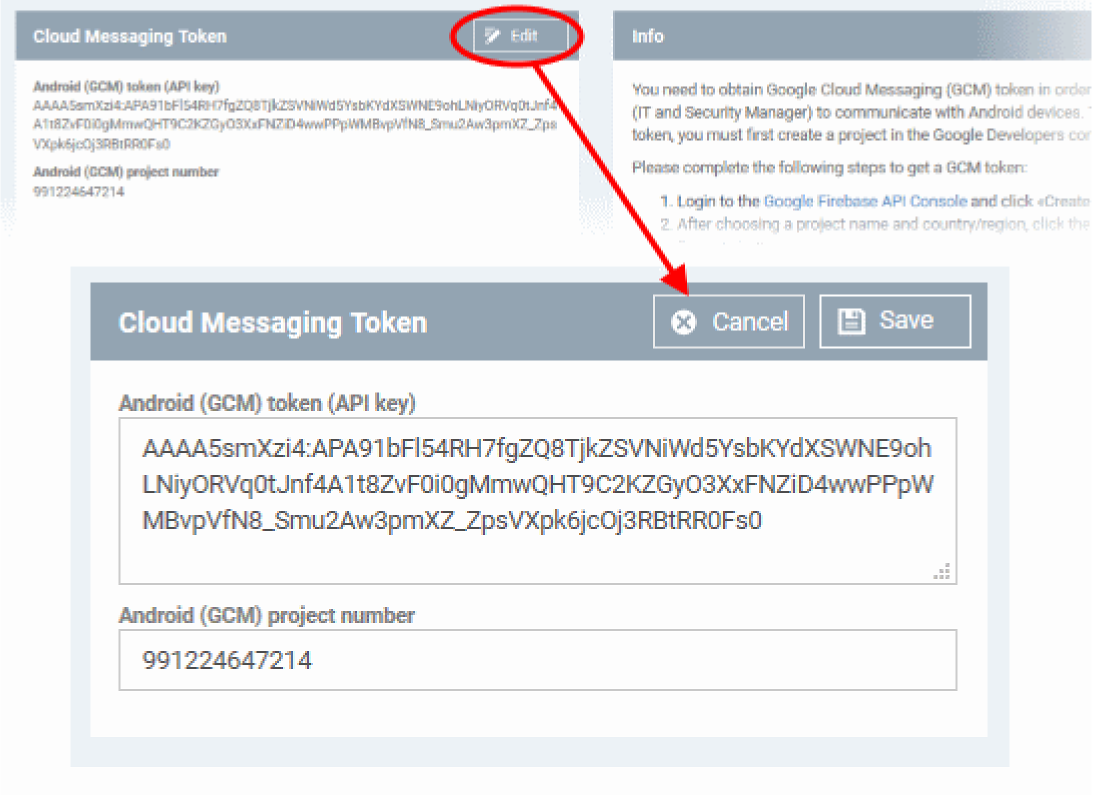
Please complete the following steps to get a GCM token:

1. Login to the Google Firebase API Console and click «Create
2. After choosing a project name and country/region, click the Project» button.
3. Once created, the project properties screen will open. If it d click the project name.
4. Click the gear icon beside the project name at the left and c «Project Settings» from the options.
5. The «Settings» screen for the project will appear. Click the « Messaging» tab from the top.

You now need to copy and paste two items into ITSM (IT an Security Manager) - the «Server key» and the «Sender ID»

6. In ITSM (IT and Security Manager), click the «Edit» button u «Android Cloud Messaging». Paste the «Server key» into the «Android (GCM) Token (API Key)» field. Paste the «Sender I the «Android (GCM) Project Number» field. Click «Save» to implement the token.

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



Android (GCM) token (API key)
AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number
991224647214

You need to obtain Google Cloud Messaging (GCM) token in order (IT and Security Manager) to communicate with Android devices. token, you must first create a project in the Google Developers co

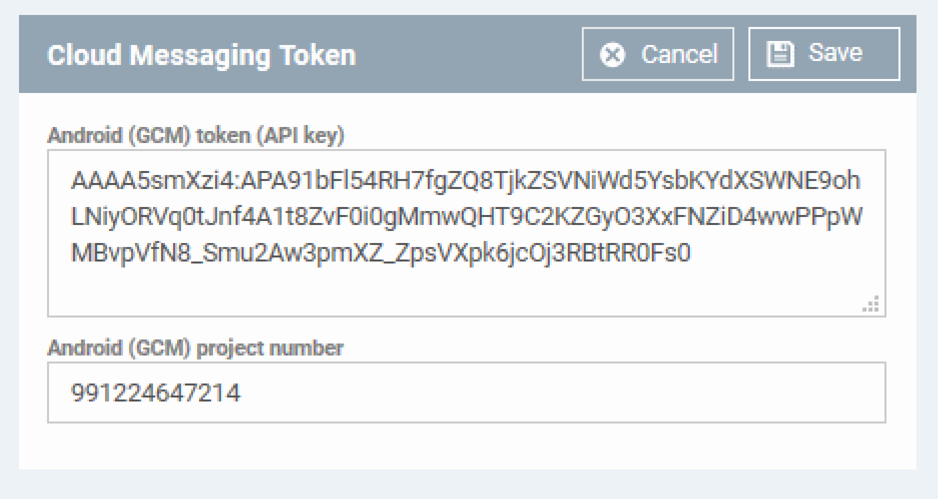
Please complete the following steps to get a GCM token:

1. Login to the Google Firebase API Console and click «Create
2. After choosing a project name and country/region, click the

Android (GCM) token (API key)
AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9oh LNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpW MBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number
991224647214

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



Android (GCM) token (API key)

AAAA5smXzi4:APA91bFl54RH7fgZQ8TjkZSVNiWd5YsbKYdXSWNE9ohLNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT9C2KZGyO3XxFNZiD4wwPPpWMBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jcOj3RBtRR0Fs0

Android (GCM) project number

991224647214

- Click 'Save'.

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

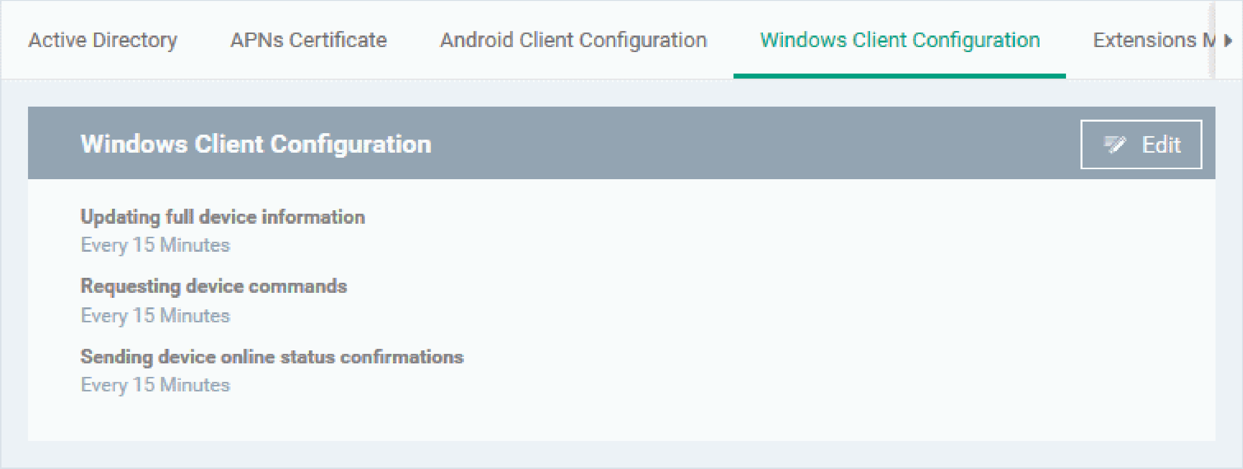
Your ITSM Portal will be now be able to communicate with Android devices using the unique token generated for your ITSM portal.

11.2.4. Configure 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



Active Directory
APNs Certificate
Android Client Configuration
Windows Client Configuration
Extensions M
Windows Client Configuration
Edit

Updating full device information
Every 15 Minutes

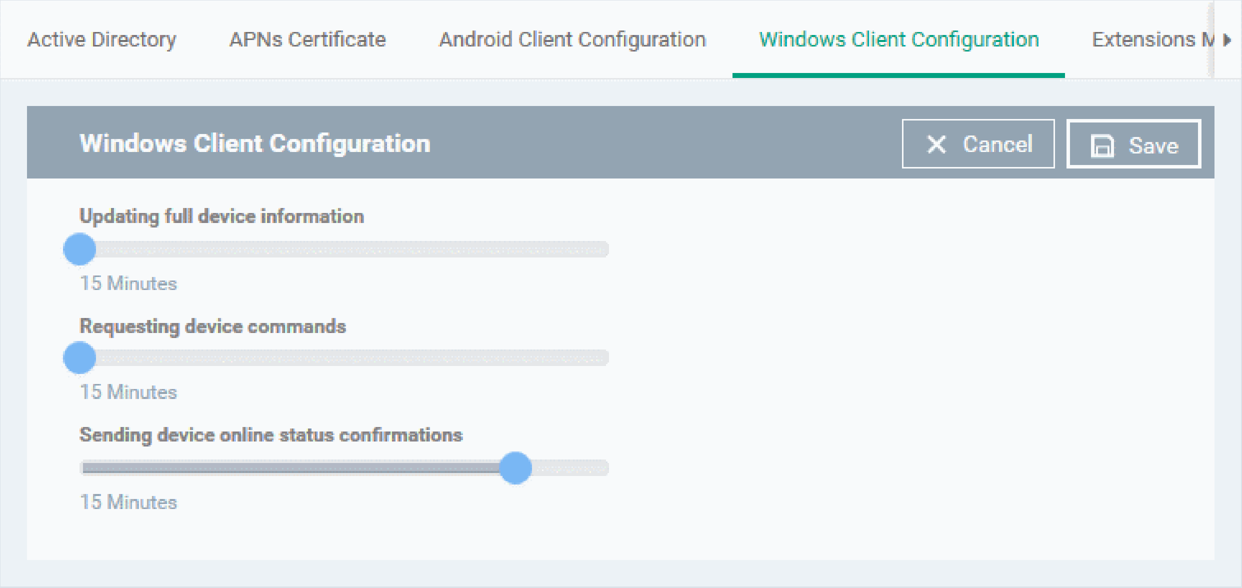
Requesting device commands
Every 15 Minutes

Sending device online status confirmations
Every 15 Minutes

The default values of the update intervals are displayed.

- Click the edit button Edit on the top right to modify these settings

The settings screen will be displayed.


Active Directory
APNs Certificate
Android Client Configuration
Windows Client Configuration
Extensions M
Windows Client Configuration
Cancel
Save

Updating full device information

15 Minutes

Requesting device commands

15 Minutes

Sending device online status confirmations

15 Minutes

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. Manage 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.
- **Comodo Remote Control** - Comodo Remote Control allows you to take control of managed endpoints

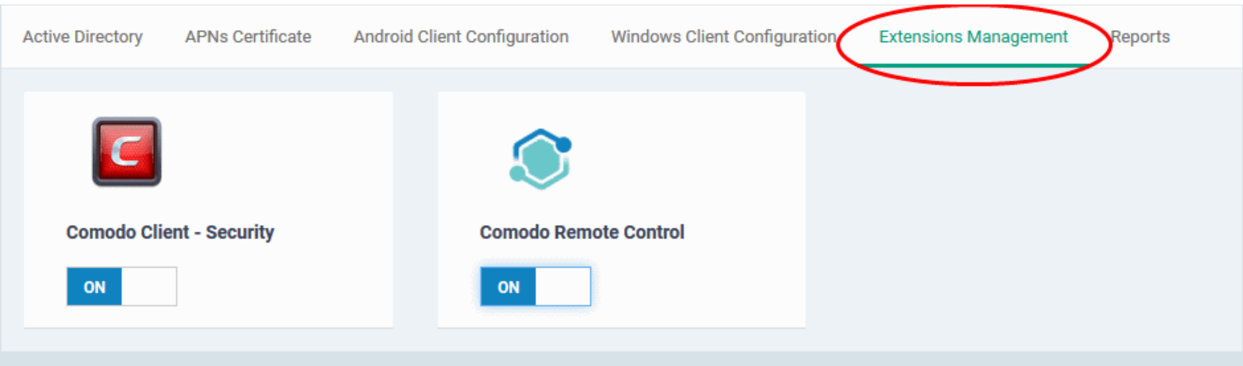
through remote desktop connection. This allows you to solve issues, install third party software, run system maintenance and more. You can take remote control in two ways:

- **Comodo Remote Control Viewer** (recommended) - Install the client viewer software on your admin computer to take control of any managed Windows endpoint.
- **Comodo Remote Monitoring and Management (RMM)** - Customers using our legacy RMM product can connect to Windows endpoints using the remote desktop feature built into that product.

You can take remote control of a Windows device from the Device List interface. For more details, refer to the section **Remote Management of Windows Devices**.

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 a tile to enable or disable an extension. Only extensions which are enabled will be available in the 'Device List' interface.
- Refer to '**Remotely Installing Packages onto Windows Devices**' and **Remote Management of Windows Devices** for more details.

11.2.6. Configure 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.

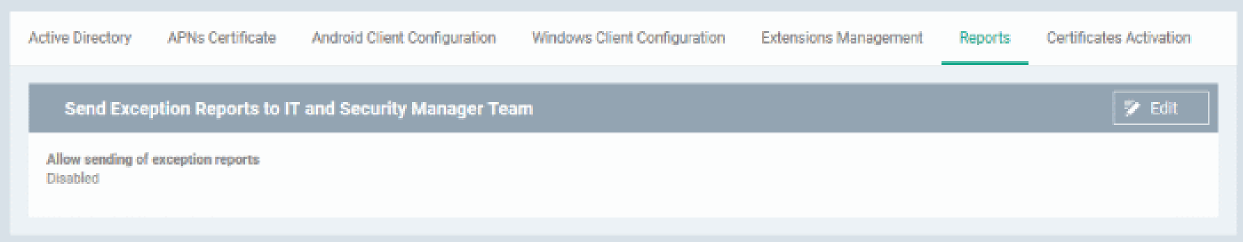
Exception reports are a valuable and constructive means of feedback that help Comodo to debug our products and improve the service we provide to our customers.

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

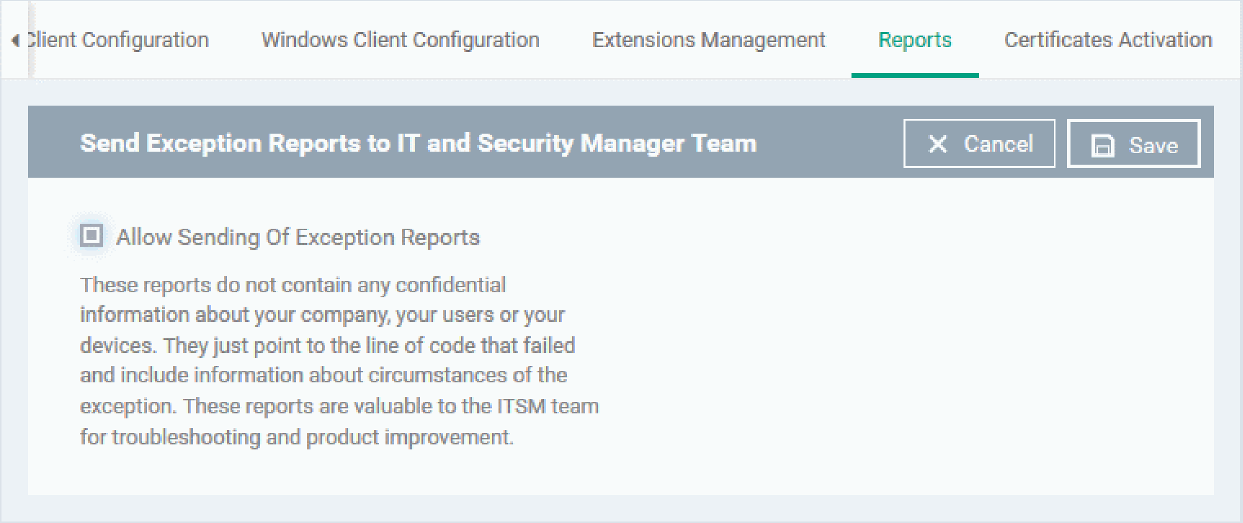
- Click 'Settings' on the left and select 'Portal Set-Up'.
- Click the 'Reports' tab



Send Exception Reports to IT and Security Manager Team

Allow sending of exception reports
Disabled

- To edit the settings click the edit button Edit at the top right.



Send Exception Reports to IT and Security Manager Team

□ Allow Sending Of Exception Reports

These reports do not contain any confidential information about your company, your users or your devices. They just point to the line of code that failed and include information about circumstances of the exception. These reports are valuable to the ITSM team for troubleshooting and product improvement.

- 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. Integrate 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:

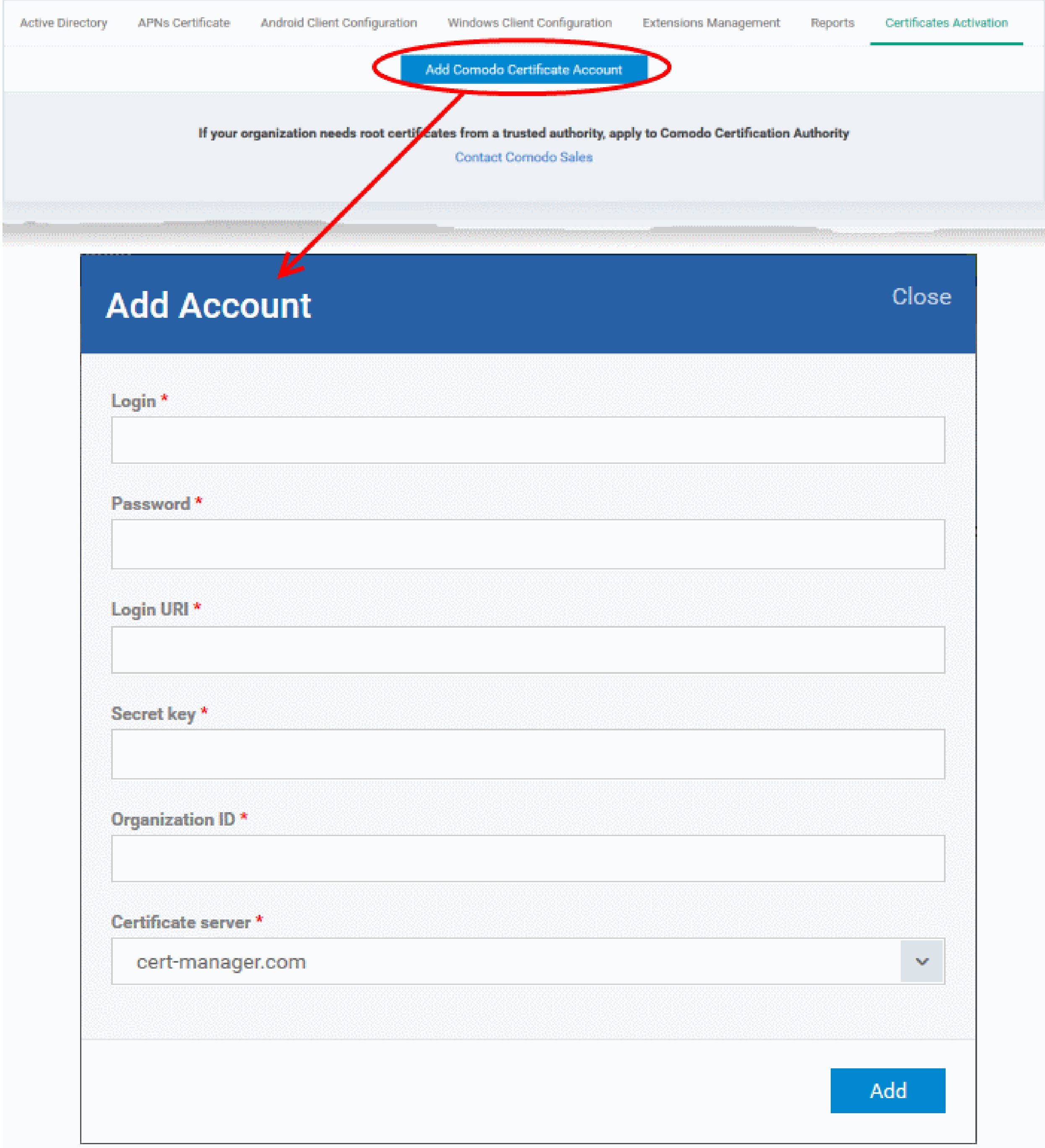
- The organization whose end-users/devices require certificates is added as an organization in CCM.
- The email domains used by end-users have been delegated to the organization in CCM.
- SMIME certificate enrollment through Web API has been enabled for the CCM organization, and a secret key has been 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**.

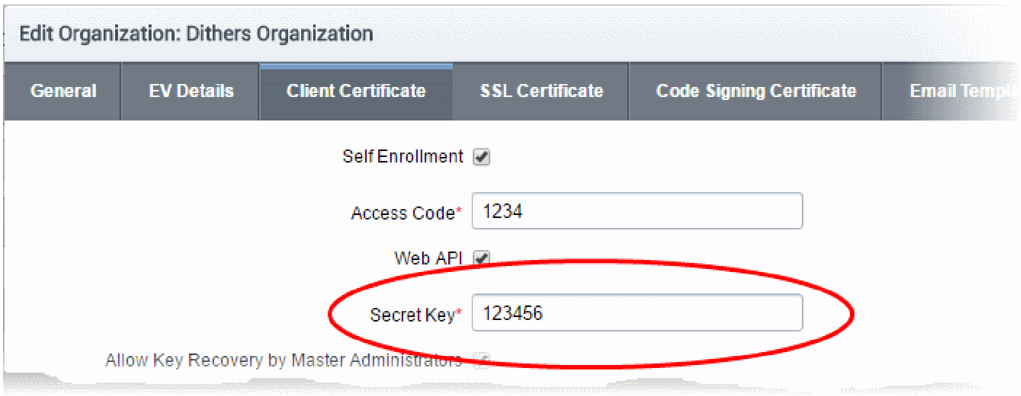
To add a CCM Account

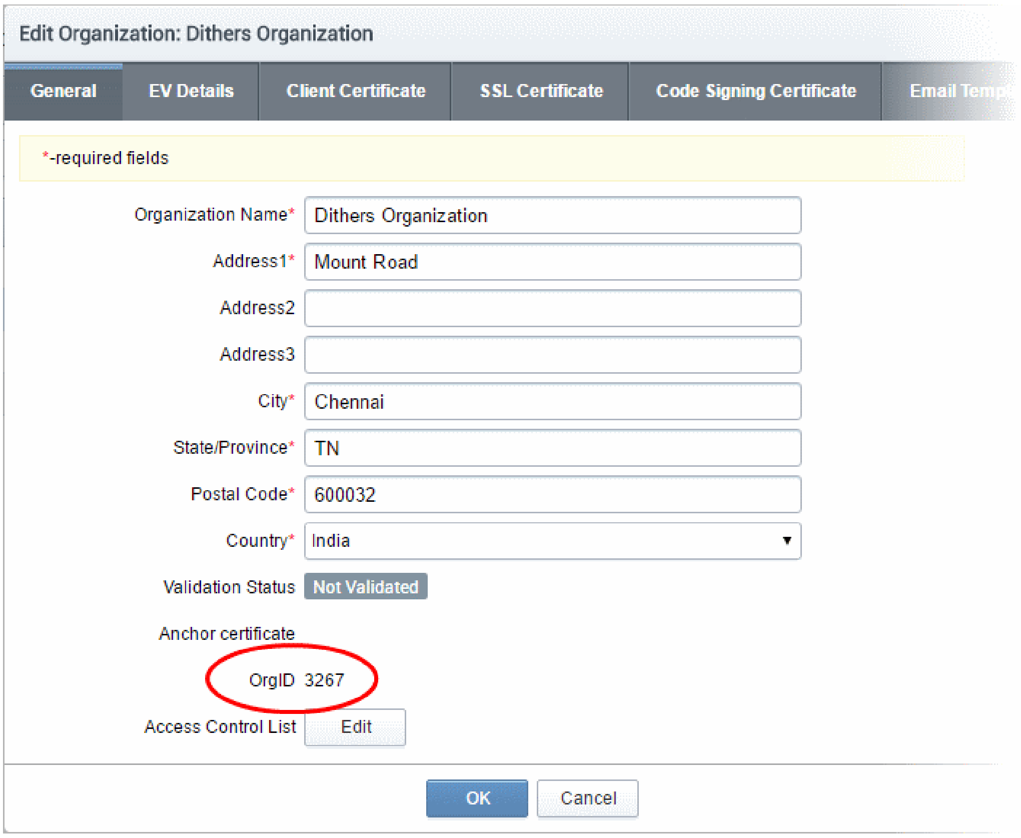
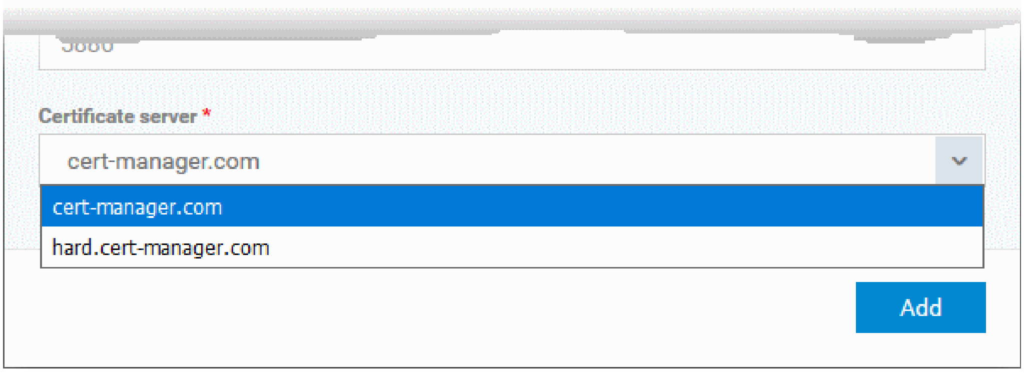
- Click 'Settings' on the left and select 'Portal Set-Up'
- Click the 'Certificate Activation' tab at the top
- Click 'Add Comodo Certificate Account'

The 'Add Account' dialog will open.



Add Account Dialog - Description of form parameters

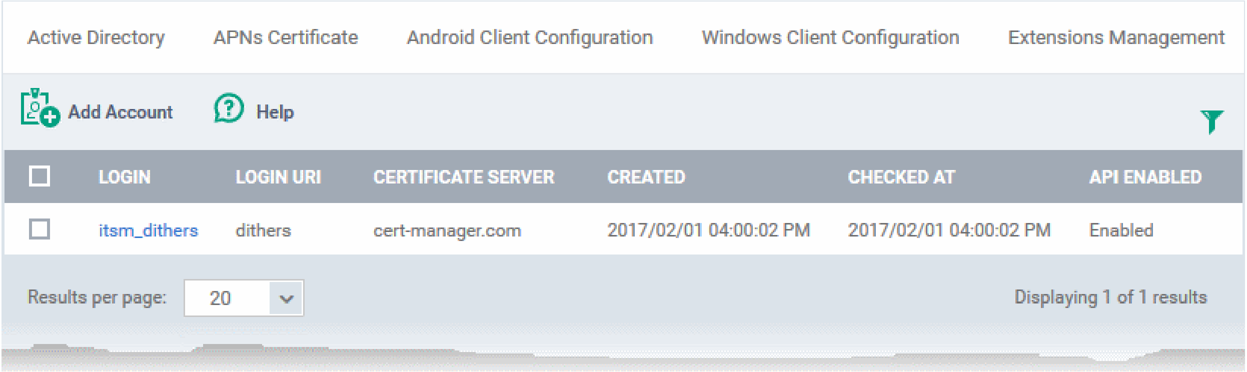
Field	Description
Login/Password	Enter the login credentials for the CCM MRAO Administrator account. This will allow ITSM to access CCM.
Login URI	Enter the customer URI of the CCM account which you wish to add to ITSM. Tip: The customer URI is the suffix of the URL used to access CCM. CCM URLs use the 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:  Edit Organization: Dithers Organization General EV Details Client Certificate SSL Certificate Code Signing Certificate Email Templ Self Enrollment ☑ Access Code* 1234 Web API ☑ Secret Key* 123456 Allow Key Recovery by Master Administrators ☑ 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:

	 Edit Organization: Dithers Organization General EV Details Client Certificate SSL Certificate Code Signing Certificate Email Temp OK Cancel Edit *-required fields Organization Name* Dithers Organization Address1* Mount Road Address2 Address3 City* Chennai State/Province* TN Postal Code* 600032 Country* India Validation Status Not Validated Anchor certificate OrgID 3267 Access Control List Edit 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:  Certificate server * cert-manager.com cert-manager.com hard.cert-manager.com

- 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:



□	LOGIN	LOGIN URI	CERTIFICATE SERVER	CREATED	CHECKED AT	API ENABLED
□	itsm_dithers	dithers	cert-manager.com	2017/02/01 04:00:02 PM	2017/02/01 04:00:02 PM	Enabled

Results per page: 20 Displaying 1 of 1 results

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. Set-up Administrator's Time Zone

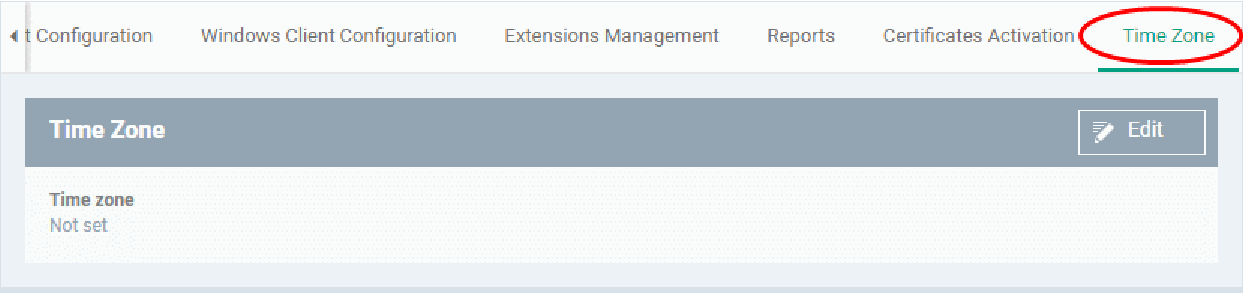
Administrators can set their time zone so that ITSM interfaces and logs will be displayed to each administrator using their local time.

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.

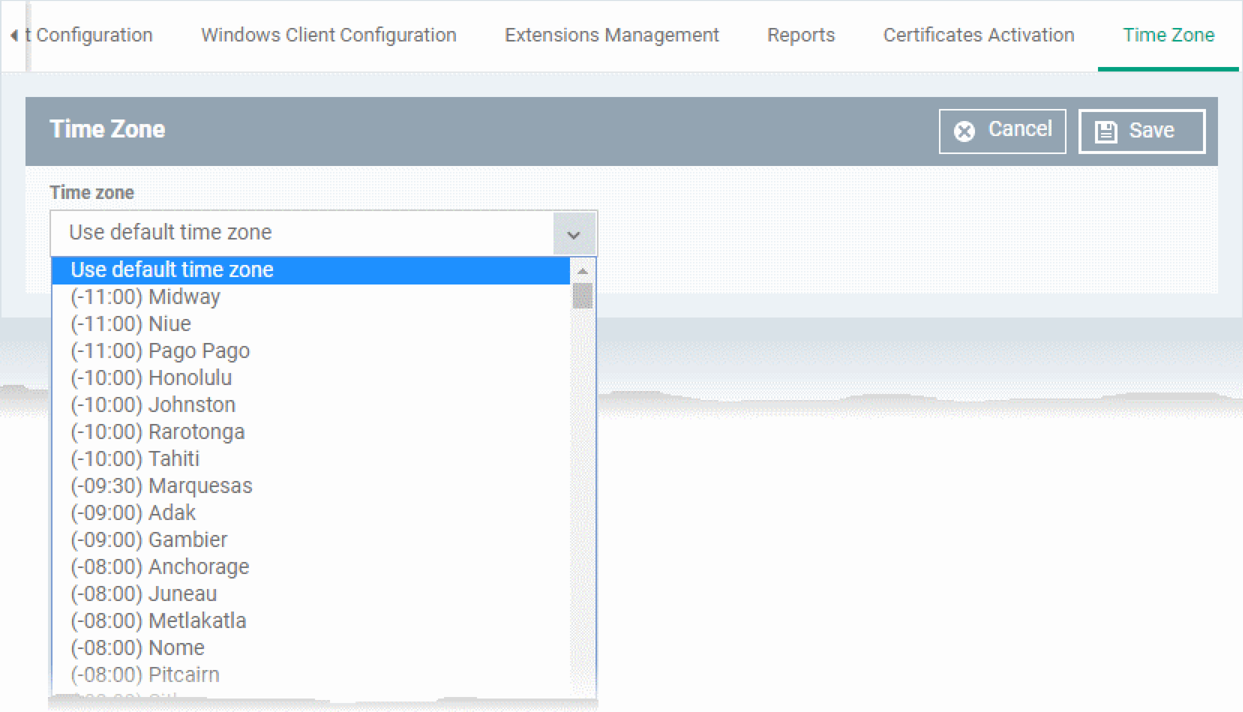
To set your time zone

- 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.

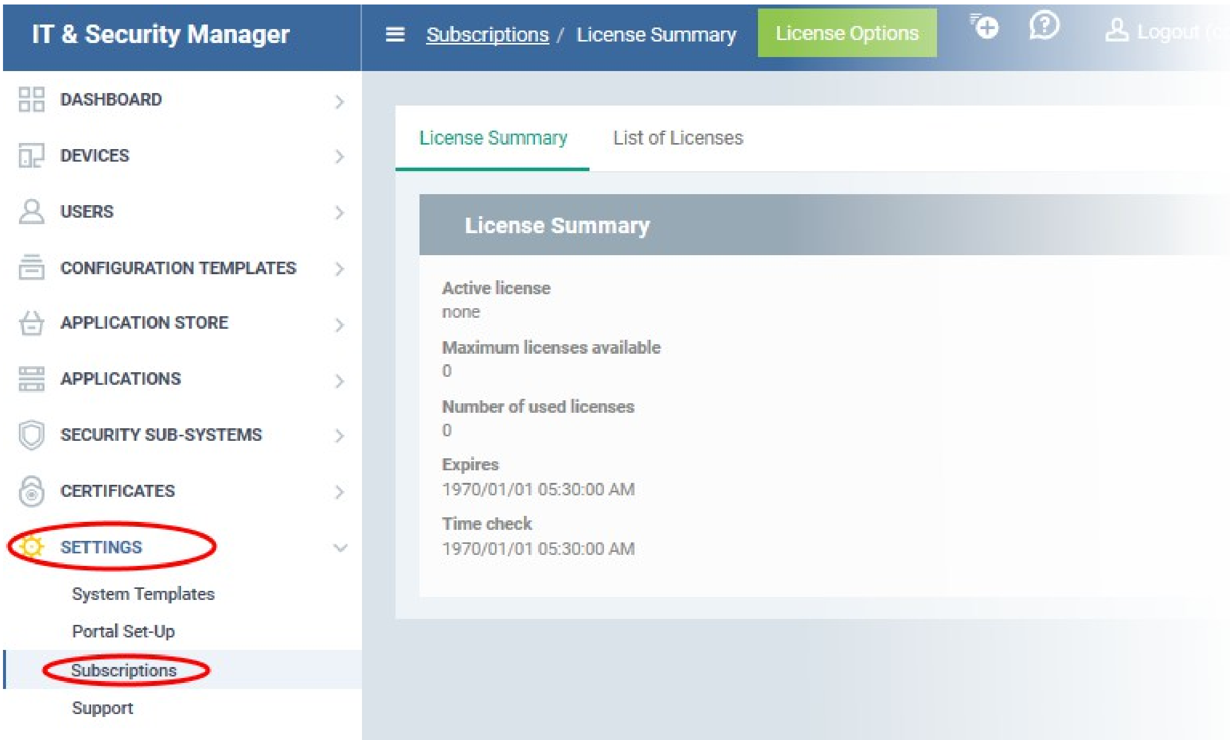
11.3. View and Manage Licenses

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.



License Summary

Active license
none

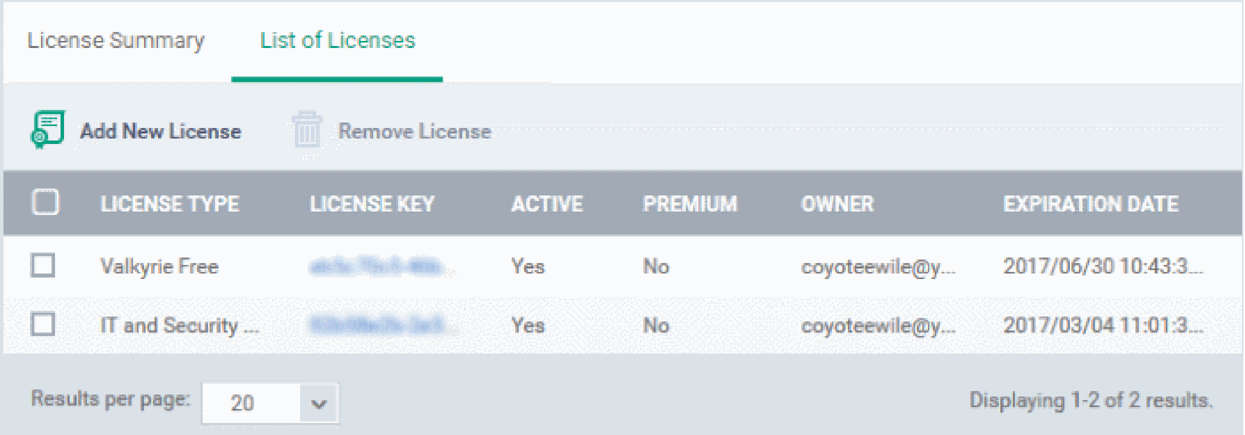
Maximum licenses available
0

Number of used licenses
0

Expires
1970/01/01 05:30:00 AM

Time check
1970/01/01 05:30:00 AM

- **List of Licenses** - Displays a list of licenses purchased so far with their details.

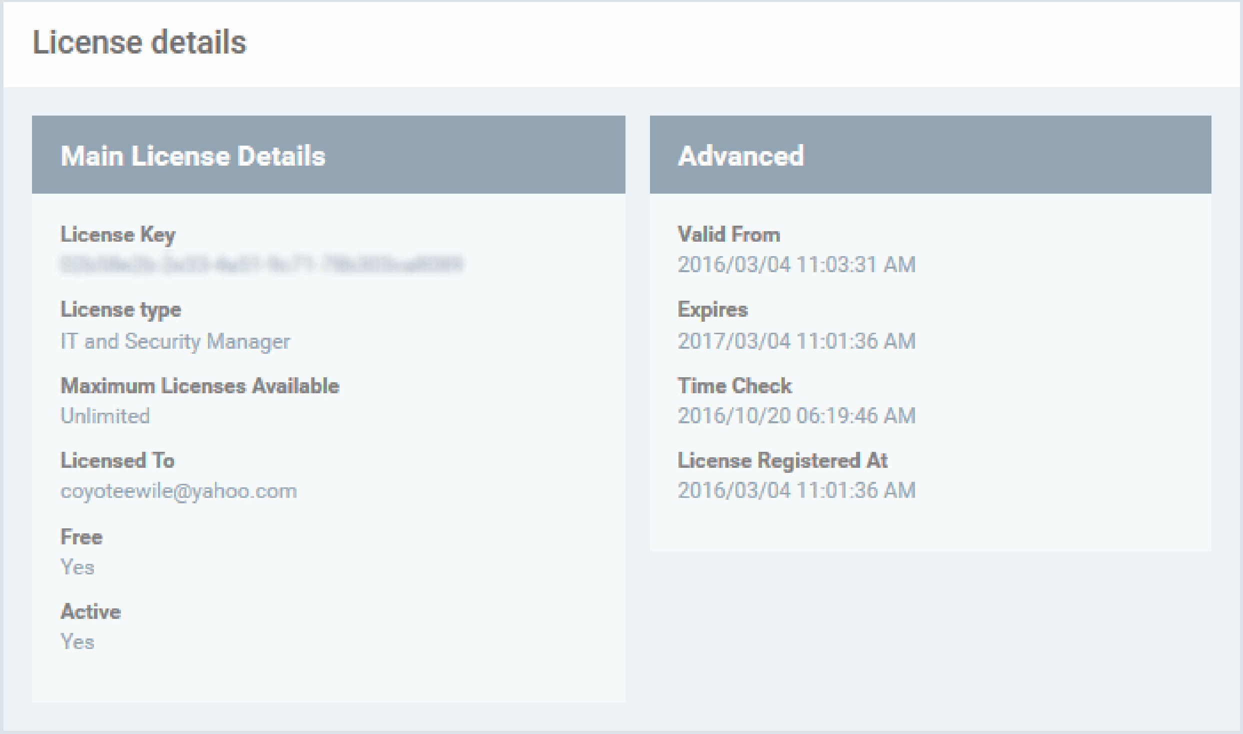


☐	LICENSE TYPE	LICENSE KEY	ACTIVE	PREMIUM	OWNER	EXPIRATION DATE
☐	Valkyrie Free	[illegible]	Yes	No	coyoteewile@y...	2017/06/30 10:43:3...
☐	IT and Security ...	[illegible]	Yes	No	coyoteewile@y...	2017/03/04 11:01:3...

Results per page: 20

Displaying 1-2 of 2 results.

- Clicking on the license key will display the details of the license.



License details

Main License Details

License Key
[redacted]

License type
IT and Security Manager

Maximum Licenses Available
Unlimited

Licensed To
coyoteewile@yahoo.com

Free
Yes

Active
Yes

Advanced

Valid From
2016/03/04 11:03:31 AM

Expires
2017/03/04 11:01:36 AM

Time Check
2016/10/20 06:19:46 AM

License Registered At
2016/03/04 11:01:36 AM

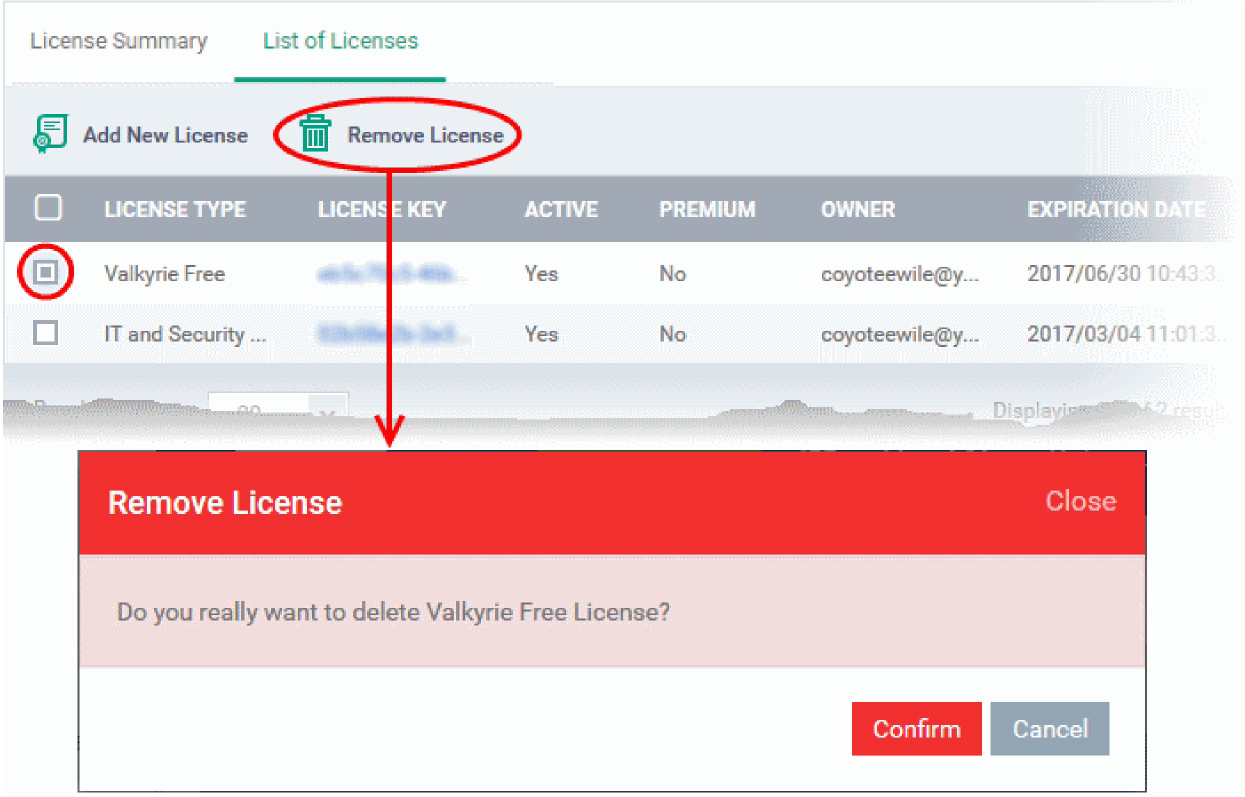
The next section **Upgrading or Adding the License** provides more details on upgrading your license for adding more number of users and renewing your license.

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



□	LICENSE TYPE	LICENSE KEY	ACTIVE	PREMIUM	OWNER	EXPIRATION DATE
☑	Valkyrie Free	[redacted]	Yes	No	coyoteewile@y...	2017/06/30 10:43:3...
□	IT and Security ...	[redacted]	Yes	No	coyoteewile@y...	2017/03/04 11:01:3...

Remove License

Do you really want to delete Valkyrie Free License?

- Click 'Confirm' that appears in the Remove License dialog.

The license will be removed from the list.

11.3.1. Upgrade or Add a License

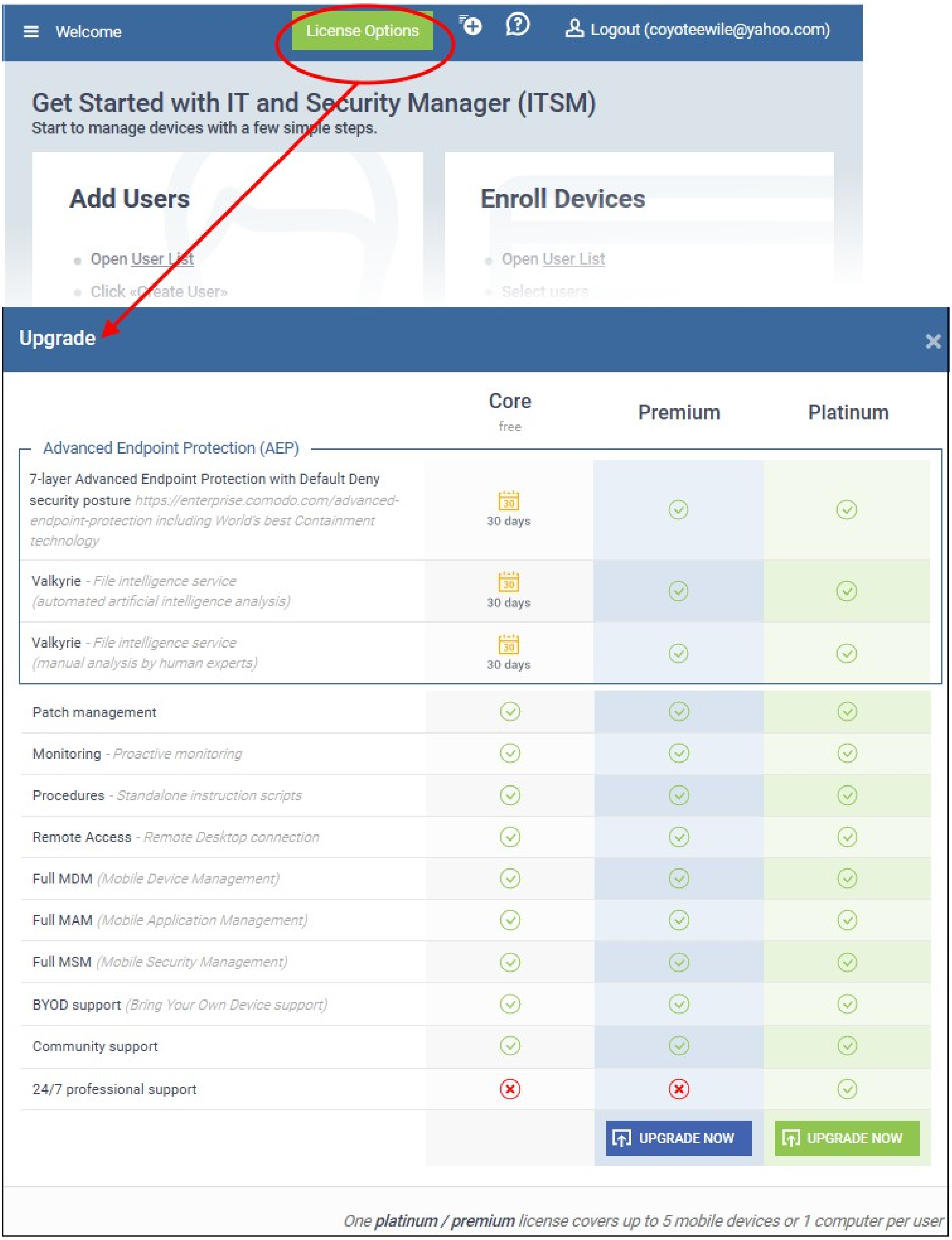
Administrators can add more users to their account by upgrading their license in the Comodo account management portal.

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



Get Started with IT and Security Manager (ITSM)

Start to manage devices with a few simple steps.

Add Users

- Open User List
- Click «Create User»

Enroll Devices

- Open User List
- Select users

Upgrade

	Core free	Premium	Platinum
Advanced Endpoint Protection (AEP)			
7-layer Advanced Endpoint Protection with Default Deny security posture *https://enterprise.comodo.com/advanced-endpoint-protection including World's best Containment technology*	30 days	✓	✓
Valkyrie - *File intelligence service (automated artificial intelligence analysis)*	30 days	✓	✓
Valkyrie - *File intelligence service (manual analysis by human experts)*	30 days	✓	✓
Patch management	✓	✓	✓
Monitoring - *Proactive monitoring*	✓	✓	✓
Procedures - *Standalone instruction scripts*	✓	✓	✓
Remote Access - *Remote Desktop connection*	✓	✓	✓
Full MDM *(Mobile Device Management)*	✓	✓	✓
Full MAM *(Mobile Application Management)*	✓	✓	✓
Full MSM *(Mobile Security Management)*	✓	✓	✓
BYOD support *(Bring Your Own Device support)*	✓	✓	✓
Community support	✓	✓	✓
24/7 professional support	✗	✗	✓
		UPGRADE NOW	UPGRADE NOW

*One **platinum / premium** license covers up to 5 mobile devices or 1 computer per user*

The 'Upgrade' screen will be displayed which lists the features of 'Premium' and 'Platinum' licenses.

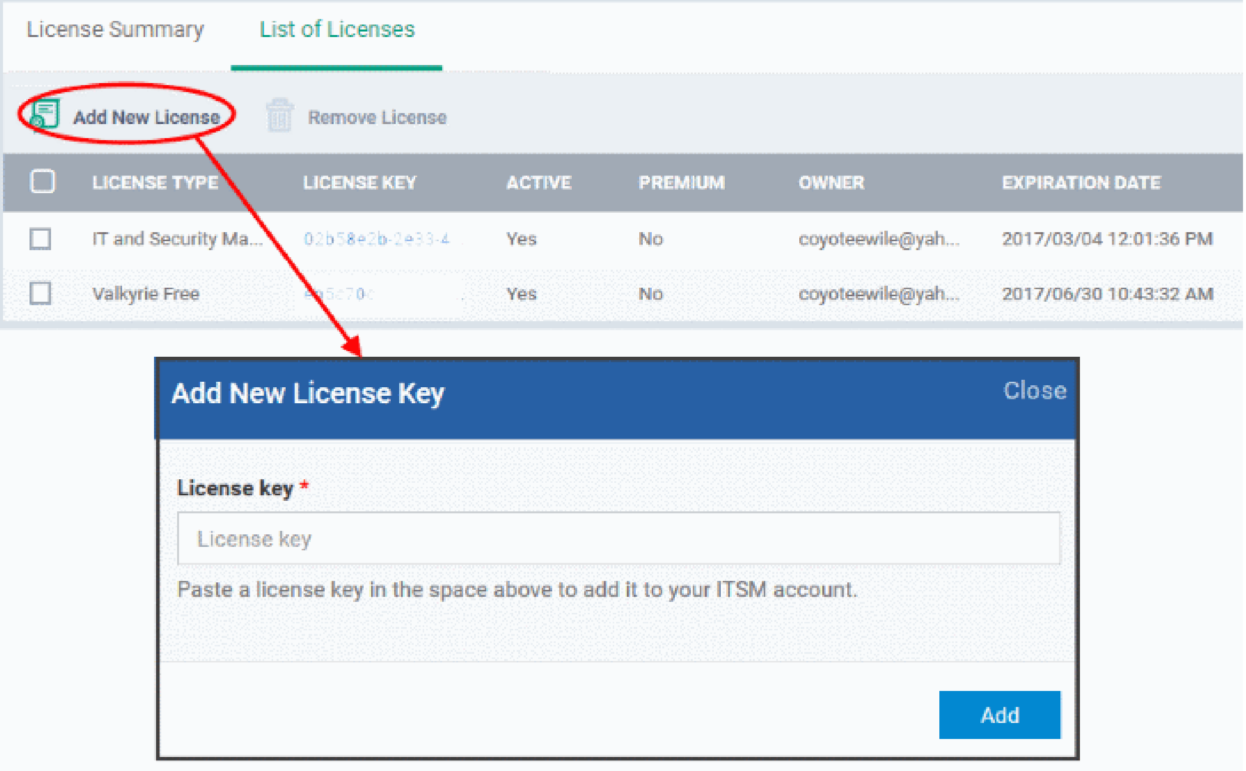
- Click 'Upgrade Now'

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.



☐	LICENSE TYPE	LICENSE KEY	ACTIVE	PREMIUM	OWNER	EXPIRATION DATE
☐	IT and Security Ma...	02b58e2b-2e33-4	Yes	No	coyoteewile@yah...	2017/03/04 12:01:36 PM
☐	Valkyrie Free	e95c70c	Yes	No	coyoteewile@yah...	2017/06/30 10:43:32 AM

Add New License Key

Close

License key *

License key

Paste a license key in the space above to add it to your ITSM account.

Add

- 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.

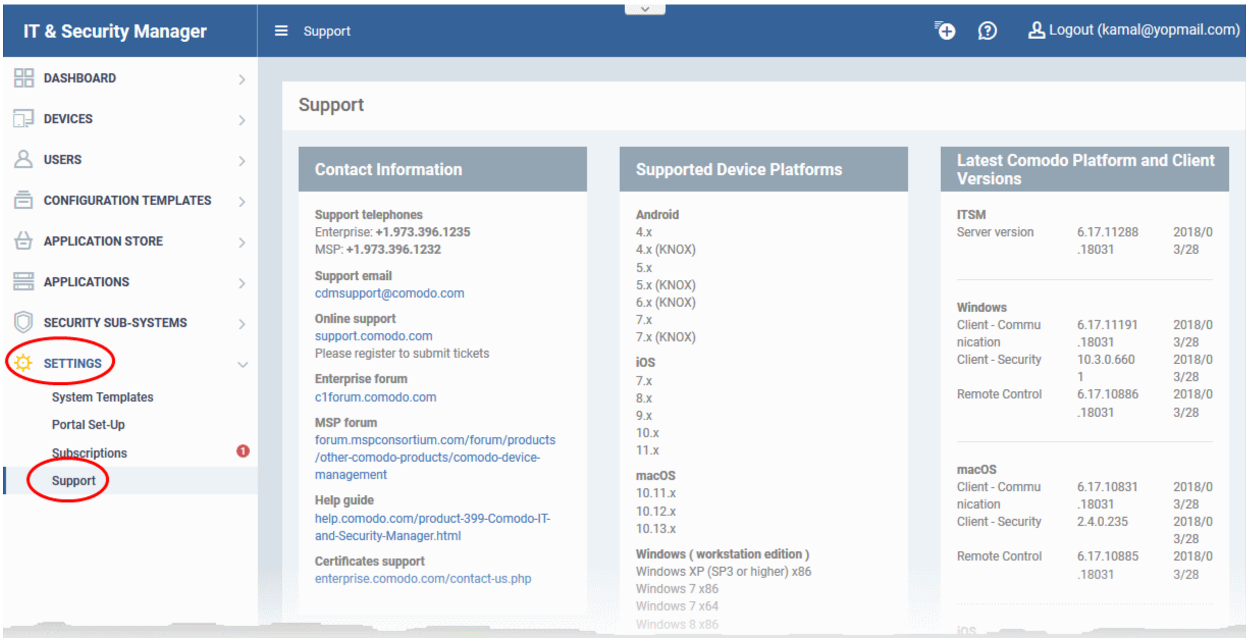
Renewal

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. View Version and Support Information

The 'Support' panel shows support contact information, the current product version number, and a list of platforms supported by this version of ITSM.

- Click 'Settings' on the left then 'Support' to access this interface.



Support

Contact Information

Support telephones
Enterprise: **+1.973.396.1235**
MSP: **+1.973.396.1232**

Support email
cdmsupport@comodo.com

Online support
support.comodo.com
Please register to submit tickets

Enterprise forum
c1forum.comodo.com

MSP forum
forum.mspconsortium.com/forum/products/other-comodo-products/comodo-device-management

Help guide
help.comodo.com/product-399-Comodo-IT-and-Security-Manager.html

Certificates support
enterprise.comodo.com/contact-us.php

Supported Device Platforms

Android
4.x
4.x (KNOX)
5.x
5.x (KNOX)
6.x (KNOX)
7.x
7.x (KNOX)

iOS
7.x
8.x
9.x
10.x
11.x

macOS
10.11.x
10.12.x
10.13.x

Windows (workstation edition)
Windows XP (SP3 or higher) x86
Windows 7 x86
Windows 7 x64
Windows 8 x86

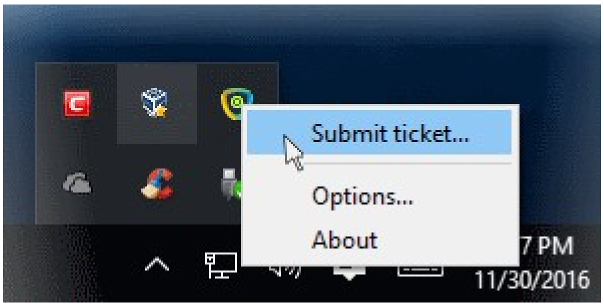
Latest Comodo Platform and Client Versions

ITSM		
Server version	6.17.11288.18031	2018/03/28
Windows		
Client - Communication	6.17.11191.18031	2018/03/28
Client - Security	10.3.0.6601	2018/03/28
Remote Control	6.17.10886.18031	2018/03/28
macOS		
Client - Communication	6.17.10831.18031	2018/03/28
Client - Security	2.4.0.235	2018/03/28
Remote Control	6.17.10885.18031	2018/03/28
iOS		

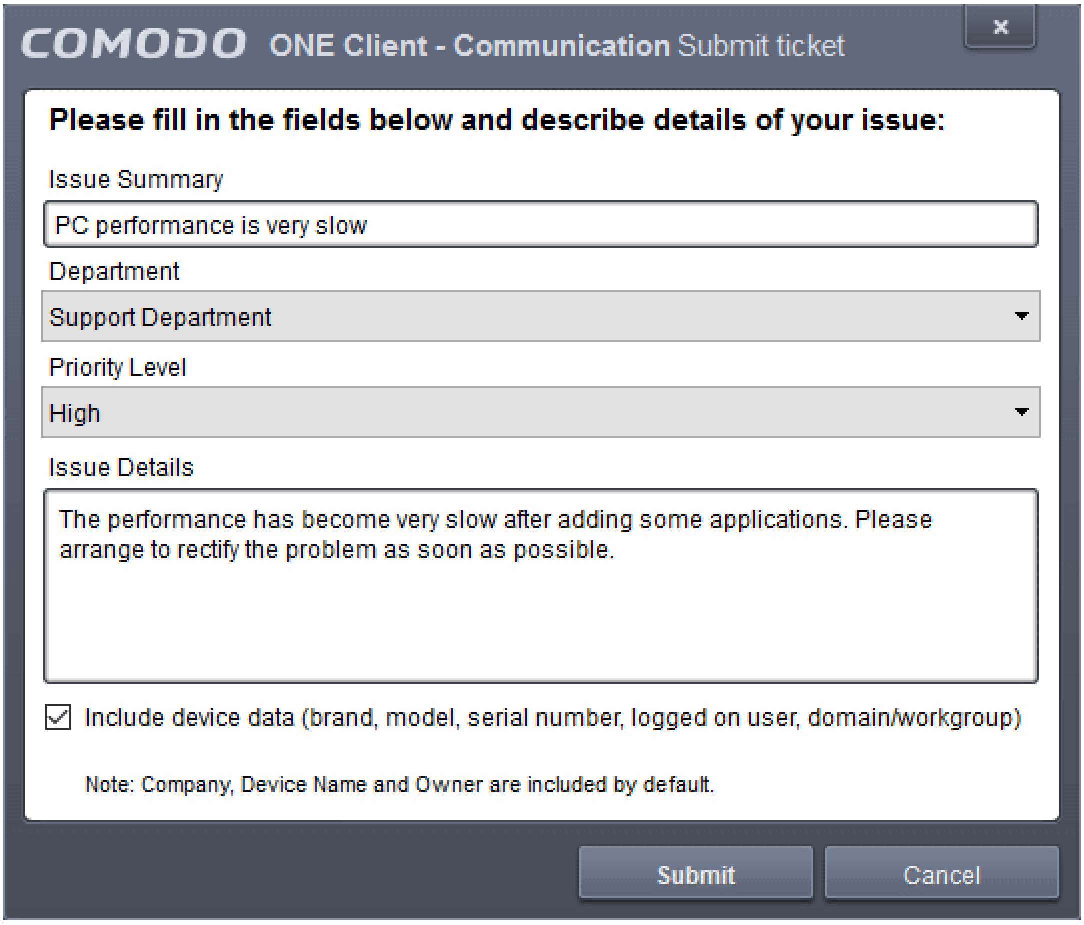
- **Contact Information** - Support telephone numbers and email addresses
- **Supported Device Platforms** - The devices and operating systems supported by this version of ITSM.
- **Latest Comodo Platform and Client Versions** - Version numbers of the ITSM server and agents.

Users also can create a support ticket from the Comodo Client - Communication (ITSM agent) tray icon on Windows and Mac OS 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



Please fill in the fields below and describe details of your issue:

Issue Summary: PC performance is very slow

Department: Support Department

Priority Level: High

Issue Details: The performance has become very slow after adding some applications. Please arrange to rectify the problem as soon as possible.

☑ Include device data (brand, model, serial number, logged on user, domain/workgroup)

Note: Company, Device Name and Owner are included by default.

Tip: The 'UI Settings' component of a configuration profile lets you rebrand the client with your own company logo and details. See **CCC and CCS Application UI Settings** in **Creating Windows Profiles** for help with this.

  - 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 1a: ITSM Services - IP Nos, Host Names and Port Details - EU Customers

Note: This page contains information for customers located in Europe. **Click here** to see USA information instead.

- ITSM communicates with Comodo servers, agents and security software on managed devices to monitor activity, provision updates, submit files for analysis and more.
- You need to configure your firewall accordingly to allow these connections.
- All client to server communications are encrypted over https connections using the strongest TLS protocols, RSA 2048 bit keys and SHA 256 algorithms.
- The tables on this page show firewall requirements for the following Comodo services:
    - **Comodo Client - Communication (CCC)**
    - **Comodo Client - Security (CCS)**
    - **ITSM Server (on premise installations)**
    - **Comodo Remote Control sessions**
    - **All settings grouped by port**

Comodo Client - Communication (CCC)

Comodo Client - Communication (CCC)					
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Criticality and notes**
CCC	Communication between device and ITSM server	subdomain.cmdm.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
Enrollment	To get client certificates	mdmsupport.comodo.com	54.93.214.133	443	Mandatory
Monitoring and alerts	Access to Monitoring and alerts server	plugins.cmdm.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
File rating management	Access to Local Verdict Server	subdomain.cmdm.comodo.com	Dynamic (Amazon load balancing)	443	Optional This is for reporting data from CCS
Windows push service (XMPP)	Device communication (push messages)	xmpp.cmdm.comodo.com	18.196.72.222 18.196.138.4 18.197.8.210	443	Mandatory
LDAP synchronization	Synchronization with LDAP via device	User's LDAP server host	User's LDAP server IP	389 636 (LDAPS)	Optional For LDAP sync via device only. Related to Device to LDAP

					server connections only
SSO	Single Sign On	one.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
Client Security installation	Download and install/upgrade Client Security agent. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change	download.comodo.com	178.255.82.5	443, 80	Optional For CCS installation/upgrade only
		cdn.download.comodo.com	104.16.61.31 104.16.60.31	443, 80	
OCSP	Client certificate revocation checking	http://ocsp.comodoca.com/	Dynamic load balancing	80	Optional For mobile devices only. Windows CCC do not perform CRL checking yet
CRL	Client certificate revocation checking	http://crl.comodoca.com/	Dynamic load balancing	80	Optional For mobile devices only. Windows CCC do not perform CRL checking yet
3rd Party Patch Management	3rd party applications updates	patchportal.one.comodo.com	23.229.69.170	443	Optional For 3rd party software updates only
Telemetry	Sending telemetry data for analysis	cescollector.cwatchapi.com	Dynamic (Amazon load balancing)	443	Optional

Comodo Client - Security (CCS)

Comodo Client - Security (CCS)						
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Protocol**	**Criticality and notes**
FLS	FLS lookup	fls.security.comodo.com	199.66.201.16	4447 (optional), 53	UDP	Mandatory - choose *either* UDP or TCP for FLS UDP is the main, preferred FLS lookup channel 53 - Default port.

						4447 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open.
	FLS lookup	fls.security.comodo.com	199.66.201.16	4448 (optional), 80	TCP	Mandatory - choose *either* UDP or TCP for FLS TCP is the reserve FLS lookup channel. 80 - Default port 4448 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open
Valkyrie	Valkyrie lookup	valkyrie.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	Optional Valkyrie lookup is currently disabled on CCS, CCS gets Valkyrie verdicts from LVS.
	Submit to Valkyrie	valkyrie.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	Mandatory
cdn.download.comodo.com	Update / upgrade mirror	cdn.download.comodo.com	104.16.61.31 104.16.60.31	80	HTTP	Mandatory
		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 can change	download.comodo.com	178.255.82.5	80	HTTP	Mandatory
		download.comodo.com	178.255.82.5	443	HTTPS	
LVS	Download the ITSM verdicts database	s3-eu-west-1.amazonaws.com	Dynamic (Amazon load balancing)	443	HTTPS	Mandatory
	LVS lookup	subdomain.cmdm.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	

OCSP	Client certificate revocation checking	http://ocsp.comodoca.com/	Dynamic load balancing	80	-	Optional CCS does not perform CRL checking yet
CRL	Client certificate revocation checking	http://crl.comodoca.com/	Dynamic load balancing	80	-	Optional CCS does not perform CRL checking yet

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	443

Comodo Remote Control

Comodo Remote Control						
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Protocol**	**Criticality and notes**
XMPP	Remote Control Session (with new version of Comodo RC*	xmpp.cmdm.comodo.com	18.196.72.222 18.196.138.4 18.197.8.210	443	HTTPS	Mandatory for both CRC host and target device
STUN server	To receive possible network configuration, external ip etc.	stun.l.google.com	Dynamic	19302	UDP	Mandatory for both CRC host and target device

Direct and relay connections	To establish direct or relay connection between CRC and target device.	-	52.29.123.206 (relay) 18.196.107.208 (relay) 23.236.135.51 (relay) 23.236.135.60 (relay)	1025 - 65535	UDP	Mandatory for both CRC host and target device

All settings grouped by port

This table contains the same information as the other four tables on this page but with services grouped by port number.

Settings Grouped by Port					
Port	**Service**	**IP**	**URL / Hostname**	**Protocol**	**Component**
443	CCC	Dynamic (Amazon load balancing)	subdomain.cmdm.comodo.com	HTTPS	Comodo Client Communication
	Enrollment	54.93.214.133	mdmsupport.comodo.com	HTTPS	
	Monitoring and alerts	Dynamic (Amazon load balancing)	plugins.cmdm.comodo.com	HTTPS	
	File rating management	Dynamic (Amazon load balancing)	subdomain.cmdm.comodo.com	HTTPS	
	Windows push service (XMPP)	18.196.72.222 18.196.138.4 18.197.8.210	xmpp.cmdm.comodo.com	HTTPS	
	SSO	69.4.89.244	one.comodo.com	HTTPS	
	3rd party patch management	23.229.69.170	patchportal.one.comodo.com	HTTPS	
	Client Security installation	178.255.82.5	download.comodo.com	HTTPS	
		104.16.61.31 104.16.60.31	cdn.download.comodo.com	HTTPS	
	Telemetry	Dynamic (Amazon load balancing)	cescollector.cwatchapi.com	HTTPS	
	Valkyrie	178.255.87.4	valkyrie.comodo.com	HTTPS	Comodo Client Security
	Update/upgrade.	178.255.82.5	download.comodo.co	HTTPS	

	Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change		m		
	Updates/upgrades mirror	104.16.61.31 & 104.16.60.31	cdn.download.comodo.com	HTTPS	
	LVS	Dynamic (Amazon load balancing)	s3-eu-west-1.amazonaws.com	HTTPS	
		Dynamic (Amazon load balancing)	subdomain.cmdm.comodo.com	HTTPS	
	License verification	91.199.212.166	accounts.comodo.com	HTTPS	ITSM server (on premise)
	Google cloud messaging	Dynamic	android.googleapis.com/gcm/send	HTTPS	
	Apple push notifications	Dynamic	gateway.push.apple.com	HTTPS	
	Local Verdict Server	ITSM server IP	ITSM server hostname	HTTPS	
	XMPP	18.196.72.222 18.196.138.4 18.197.8.210	xmpp.cmdm.comodo.com	HTTPS	Comodo Remote Control
80	Client Security installation	178.255.82.5	download.comodo.com	HTTPS	Comodo Client Communication
		104.16.61.31 104.16.60.31	cdn.download.comodo.com	HTTPS	
	OCSP	Dynamic load balancing	http://ocsp.comodoca.com/	HTTPS	
	CRL	Dynamic load balancing	http://crl.comodoca.com/	HTTPS	
	FLS Lookup	199.66.201.16	fls.security.comodo.com	HTTPS	Comodo Client Security
	Update/upgrade. Requests to download.comodo.com are redirected to	178.255.82.5	download.comodo.com	HTTPS	

	cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change				
	Updates/upgrades mirror	104.16.61.31 & 104.16.60.31	cdn.download.comodo.com	HTTPS	
	OCSP	Dynamic load balancing	http://ocsp.comodoca.com/	HTTPS	
	CRL	Dynamic load balancing	http://crl.comodoca.com/	HTTPS	
	Apple push notifications	Dynamic	gateway.push.apple.com	HTTPS	ITSM server (on premise)
25	Email	SMTP server IP	SMTP server hostname	SMTP	ITSM server (on premise)
53	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
4447 (Optional)	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
4448 (Optional)	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
389	LDAP synchronization	User's LDAP server IP	User's LDAP server IP	-	Comodo Client Communication
	LDAP synchronization	User's LDAP server IP	User's LDAP server IP	-	ITSM server (on premise)
636	LDAP synchronization	User's LDAP server IP	User's LDAP server IP	-	Comodo Client Communication
	LDAP synchronization	User's LDAP server IP	User's LDAP server IP	-	ITSM server (on premise)
2195	Apple push notifications	Dynamic	gateway.push.apple.com	-	ITSM server (on premise)
2196	Apple push notifications	Dynamic	gateway.push.apple.com	-	ITSM server (on premise)
19302	STUN server	Dynamic (Amazon load balancing)	stun.l.google.com	UDP	Comodo Remote Control
1025-65535	Direct and relay connections	52.29.123.206 (relay) 18.196.107.208 (relay)	N/A	UDP	Comodo Remote Control

Appendix 1b: ITSM Services - IP Nos, Host Names and Port Details - US Customers

Note: This page contains information for customers located in the USA. **Click here** to see Europe information instead.

- ITSM communicates with Comodo servers, agents and security software on managed devices to monitor activity, provision updates, submit files for analysis and more.
- You need to configure your firewall accordingly to allow these connections.
- All client to server communications are encrypted over https connections using the strongest TLS protocols, RSA 2048 bit keys and SHA 256 algorithms.
- The tables on this page show firewall requirements for the following Comodo services:
  - **Comodo Client - Communication (CCC)**
  - **Comodo Client - Security (CCS)**
  - **ITSM Server (on premise installations)**
  - **Comodo Remote Control sessions**
  - **All settings grouped by port**

Comodo Client - Communication (CCC)

Comodo Client - Communication (CCC)					
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Criticality and notes**
CCC	Communication between device and ITSM server	subdomain.itsm-us1.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
Enrollment	To get client certificates	mdmsupport.comodo.com	54.93.214.133	443	Mandatory
Monitoring and alerts	Access to Monitoring and alerts server	plugins.itsm-us1.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
File rating management	Access to Local Verdict Server	subdomain.itsm-us1.comodo.com	Dynamic (Amazon load balancing)	443	Optional This is for reporting data from CCS
Windows push service (XMPP)	Device communication (push messages)	xmpp.itsm-us1.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
LDAP synchronization	Synchronization with LDAP via device	User's LDAP server host	User's LDAP server IP	389 636 (LDAPS)	Optional For LDAP sync via device only. Related to

					Device to LDAP server connections only
SSO	Single Sign On	one-us.comodo.com	Dynamic (Amazon load balancing)	443	Mandatory
Client Security installation	Download and install/upgrade Client Security agent. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change.	download.comodo.com	178.255.82.5	443, 80	Optional For CCS installation/upgrade only
		cdn.download.comodo.com	104.16.61.31 104.16.60.31		
OCSP	Client certificate revocation checking	http://ocsp.comodoca.com/	Dynamic load balancing	80	Optional For mobile devices only. Windows CCC do not perform CRL checking yet
CRL	Client certificate revocation checking	http://crl.comodoca.com/	Dynamic load balancing	80	Optional For mobile devices only. Windows CCC do not perform CRL checking yet
3rd Party Patch Management	3rd party applications updates	patchportal.one.comodo.com	23.229.69.170	443	Optional For 3rd party software updates only
Telemetry	Sending telemetry data for analysis	cescollector.cwatchapi.com	Dynamic (Amazon load balancing)	443	Optional

Comodo Client - Security (CCS)

Comodo Client - Security (CCS)

Service	Purpose	Hostname	IP	Port	Protocol	Criticality and notes
FLS	FLS lookup	fls.security.comodo.com	199.66.201.16	4447 (optional), 53	UDP	Mandatory - choose *either* UDP or TCP for FLS UDP is the main, preferred FLS lookup channel

						53 - Default port. 4447 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open.
	FLS lookup	fls.security.comodo.com	199.66.201.16	4448 (optional), 80	TCP	Mandatory - choose *either* UDP or TCP for FLS TCP is the reserve FLS lookup channel. 80 - Default port 4448 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open
Valkyrie	Valkyrie lookup	valkyrie.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	Optional Valkyrie lookup is currently disabled on CCS, CCS gets Valkyrie verdicts from LVS.
	Submit to Valkyrie	valkyrie.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	Mandatory
cdn.download.comodo.com	Update / upgrade mirror	cdn.download.comodo.com	104.16.61.31 104.16.60.31	80	HTTP	Mandatory
		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 can change	download.comodo.com	178.255.82.5	80	HTTP	Mandatory
		download.comodo.com	178.255.82.5	443	HTTPS	Mandatory
LVS	Download the ITSM verdicts database	s3-eu-west-1.amazonaws.com	Dynamic (Amazon load balancing)	443	HTTPS	Mandatory
	LVS lookup	subdomain.itsm-	Dynamic (Amazon load	443	HTTPS	

		us1.comodo.com	balancing)			
OCSP	Client certificate revocation checking	*http://ocsp.comodoca.com/*	Dynamic load balancing	80	-	Optional CCS does not perform CRL checking yet
CRL	Client certificate revocation checking	*http://crl.comodoca.com/*	Dynamic load balancing	80	-	Optional CCS does not perform CRL checking yet

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	443

Comodo Remote Control

Comodo Remote Control						
Service	**Purpose**	**Hostname**	**IP**	**Port**	**Protocol**	**Criticality and notes**
XMPP	Remote Control Session (with new version of Comodo RC*	xmpp.itsm-us1.comodo.com	Dynamic (Amazon load balancing)	443	HTTPS	Mandatory for both CRC host and target device
STUN server	To receive possible network configuration, external ip etc.	stun.l.google.com	Dynamic	19302	UDP	Mandatory for both CRC host and target device

Direct and relay connections	To establish direct or relay connection between CRC and target device.	-	23.236.135.51 (relay) 23.236.135.60 (relay) 52.29.123.206 (relay)	1025 - 65535	UDP	Mandatory for both CRC host and target device

All settings grouped by port

This table contains the same information as the other four tables on this page but with services grouped by port number.

Settings Grouped by Port					
Port	**Service**	**IP**	**URL / Hostname**	**Protocol**	**Component**
443	CCC	Dynamic (Amazon load balancing)	subdomain.itsm-us1.comodo.com	HTTPS	Comodo Client Communication
	Enrollment	54.93.214.133	mdmsupport.comodo.com	HTTPS	
	Monitoring and alerts	Dynamic (Amazon load balancing)	plugins.itsm-us1.comodo.com	HTTPS	
	File rating management	Dynamic (Amazon load balancing)	subdomain.itsm-us1.comodo.com	HTTPS	
	Windows push service (XMPP)	Dynamic (Amazon load balancing)	xmpp.itsm-us1.comodo.com	HTTPS	
	SSO	69.4.89.244	one-us.comodo.com	HTTPS	
	3rd party patch management	23.229.69.170	patchportal.one.comodo.com	HTTPS	
	Client Security installation	178.255.82.5	download.comodo.com	HTTPS	
		104.16.61.31 104.16.60.31	cdn.download.comodo.com	HTTPS	
	Telemetry	Dynamic (Amazon load balancing)	cescollector.cwatchapi.com	HTTPS	
	Valkyrie	178.255.87.4	valkyrie.comodo.com	HTTPS	Comodo Client Security
	Update/upgrade. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN	178.255.82.5	download.comodo.com	HTTPS	

	provider, and those IP addresses can change				
	Updates/upgrades mirror	104.16.61.31 & 104.16.60.31	cdn.download.comodo.com	HTTPS	
	LVS	Dynamic (Amazon load balancing)	s3-eu-west-1.amazonaws.com	HTTPS	
		Dynamic (Amazon load balancing)	subdomain.itsm-us1.comodo.com	HTTPS	
	License verification	91.199.212.166	accounts.comodo.com	HTTPS	ITSM server (on premise)
	Google cloud messaging	Dynamic	android.googleapis.com/gcm/send	HTTPS	
	Apple push notifications	Dynamic	gateway.push.apple.com	HTTPS	
	Local Verdict Server	ITSM server IP	ITSM server hostname	HTTPS	
	XMPP	Dynamic (Amazon load balancing)	xmpp.itsm-us1.comodo.com	HTTPS	Comodo Remote Control
80	Client Security installation	178.255.82.5	download.comodo.com	HTTPS	Comodo Client Communication
		104.16.61.31 104.16.60.31	cdn.download.comodo.com	HTTPS	
	OCSP	Dynamic load balancing	http://ocsp.comodoca.com/	HTTPS	
	CRL	Dynamic load balancing	http://crl.comodoca.com/	HTTPS	
	FLS Lookup	199.66.201.16	fls.security.comodo.com	HTTPS	Comodo Client Security
	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 can change	178.255.82.5	download.comodo.com	HTTPS	
	Updates/upgrades mirror	104.16.61.31 & 104.16.60.31	cdn.download.comodo.com	HTTPS	
	OCSP	Dynamic load	http://ocsp.comodoca.co	HTTPS	

		balancing	m/		
	CRL	Dynamic load balancing	http://crl.comodoca.com/	HTTPS	
	Apple push notifications	Dynamic	gateway.push.apple.com	HTTPS	ITSM server (on premise)
25	Email	SMTP server IP	SMTP server hostname	SMTP	ITSM server (on premise)
53	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
4447 (Optional)	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
4448 (Optional)	FLS Lookup	199.66.201.16	fls.security.comodo.com	UDP	Comodo Client Security
389	LDAP synchronization	User's LDAP server IP	User's LDAP server IP		Comodo Client Communication
	LDAP synchronization	User's LDAP server IP	User's LDAP server IP		ITSM server (on premise)
636	LDAP synchronization	User's LDAP server IP	User's LDAP server IP		Comodo Client Communication
	LDAP synchronization	User's LDAP server IP	User's LDAP server IP		ITSM server (on premise)
2195	Apple push notifications	Dynamic	gateway.push.apple.com		ITSM server (on premise)
2196	Apple push notifications	Dynamic	gateway.push.apple.com		ITSM server (on premise)
19302	STUN server	Dynamic (Amazon load balancing)	stun.l.google.com	UDP	Comodo Remote Control
1025-65535	Direct and relay connections	23.236.135.51 (relay) 23.236.135.60 (relay) 52.29.123.206 (relay)	N/A	UDP	Comodo Remote Control

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 Mac OS Profile for ITSM (default profile)
- Optimum IOS Profile for ITSM (default profile)
- Optimum Android Profile for ITSM (default profile)

Windows Profile Settings

Section	Optimum	Standard	Hardened
Containment Rule	All malicious files are blocked and quarantined All files in suspicious and containment folders are blocked Metro apps are not contained All unrecognized files are contained	All malicious files are blocked and quarantined All files in suspicious and containment folders are blocked Metro apps are not contained Unrecognized files less than 2 days old are contained. Older unrecognized files run normally. The following exceptions apply: • All unrecognized files in user and program shared folders are contained. • Unrecognized files from the internet, intranet and removable media are contained • Unrecognized processes created by web browsers, mail clients and other major application types are contained	All malicious files are blocked and quarantined All files in suspicious and containment folders are blocked All unrecognized files are contained.
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 Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

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

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets. With offices in the US, China, Turkey, India, Romania and Ukraine, Comodo secures the online and offline eco-systems of thousands of clients worldwide.

Comodo Security Solutions, Inc

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.6361

Email: **EnterpriseSolutions@Comodo.com**

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