

COMODO
Creating Trust Online®



Comodo Device Manager

Software Version 5.0

Administrator Guide

Guide Version 5.0.021116

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo Device Manager.....	5
1.1.Key Concepts.....	8
1.2.Best Practices.....	9
1.3.Quick Start.....	10
1.4.Logging into your Administration Console.....	31
2.The Administrative Console.....	33
3.The Dashboard.....	34
4.Users and User Groups.....	46
4.1.Managing Users.....	46
4.1.1.Creating New User Accounts.....	49
4.1.2.Enrolling User Devices for Management.....	51
4.1.2.1.Enrolling Android Devices.....	54
4.1.2.2.Enrolling iOS Devices.....	61
4.1.2.2.1.Downloading and Installing CDM Client for iOS Devices.....	64
4.1.2.3.Enrolling Windows Endpoints.....	67
4.1.3.Viewing the Details of a User.....	69
4.1.3.1.Updating the Details of a User.....	70
4.1.4.Assigning Configuration Profile(s) to a Users' Devices.....	74
4.1.5.Removing a User.....	76
4.2.Managing User Groups.....	78
4.2.1.Creating a New User Group.....	80
4.2.2.Editing a User Group.....	81
4.2.3.Assigning Configuration Profiles to a User Group.....	85
4.2.4.Removing a User Group.....	88
5.Devices.....	89
5.1.Device List.....	90
5.1.1.Managing Windows Devices.....	92
5.1.1.1.Viewing and Editing Device Name.....	94
5.1.1.2.Viewing Summary Information.....	95
5.1.1.3.Viewing Network Information.....	97
5.1.1.4.Viewing and Managing Profiles Associated with the Device.....	97
5.1.1.5.Viewing list of Files in the Device.....	98
5.1.1.6.Viewing CES configurations exported from the Device.....	105
5.1.1.7.Viewing MSI files installed on the device through CDM.....	108
5.1.1.8.Viewing and Installing Windows Patches.....	109
5.1.2.Managing Android/iOS Devices.....	112
5.1.2.1.Viewing and Editing Device Name.....	114
5.1.2.2.Viewing Summary Information.....	115
5.1.2.3.Managing Installed Applications.....	117
5.1.2.4.Viewing and Managing Profiles Associated with the Device.....	119
5.1.2.5.Viewing Sneak Peak Pictures to Locate Lost Devices.....	120
5.1.2.6.Viewing the Location of the Device.....	122
5.1.3.Viewing the User Information.....	123
5.1.4.Removing a Device.....	124

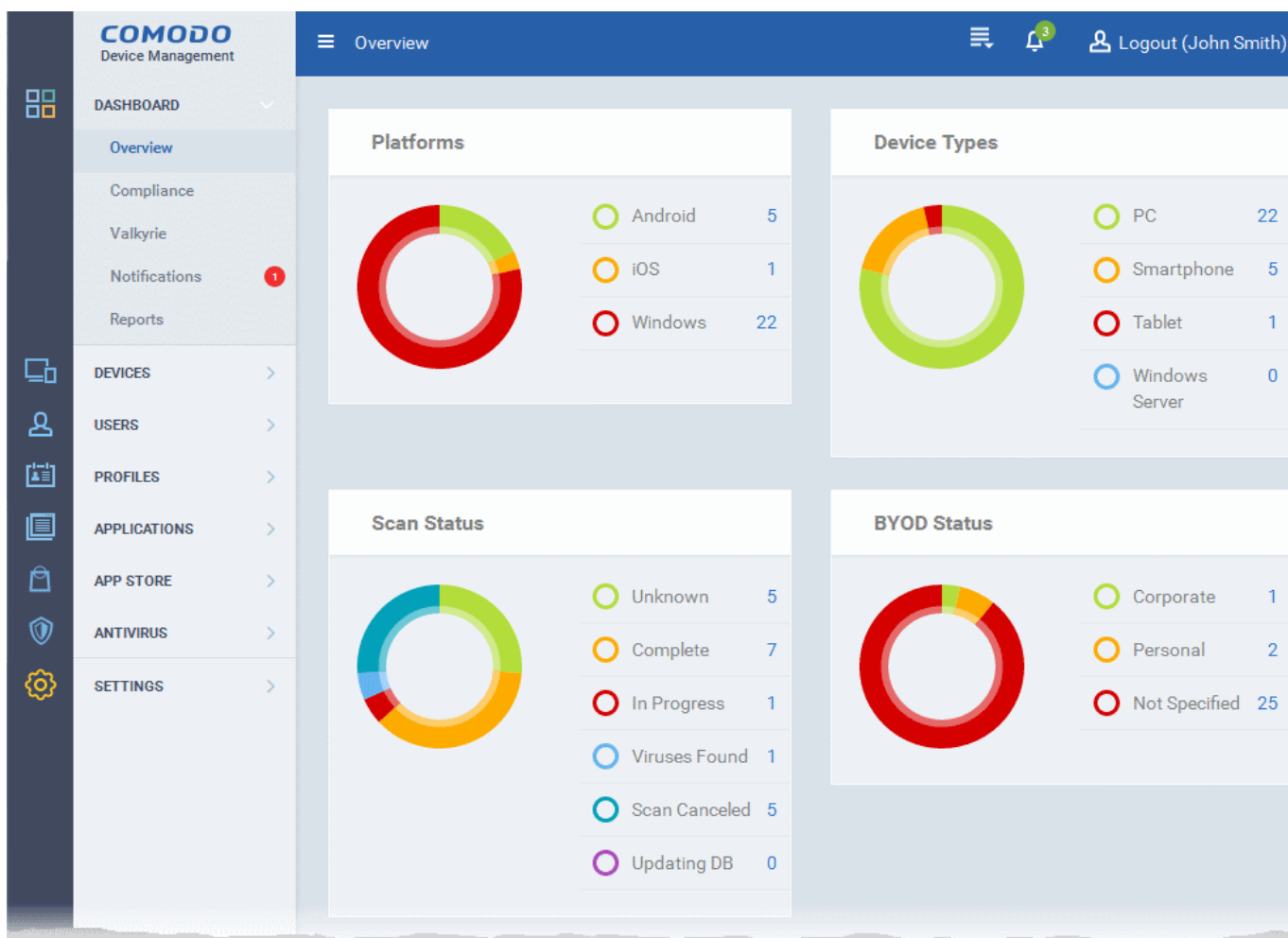
5.1.5.Remote Management of Windows Devices.....	127
5.1.6.Remotely Installing Packages onto Windows Devices.....	128
5.1.7.Installing Apps on Android/iOS Devices.....	130
5.1.8.Generating Alarm on Devices.....	131
5.1.9.Locking/Unlocking Selected Devices.....	134
5.1.10.Wiping Selected Devices.....	135
5.1.11.Assigning Configuration Profile to Selected Devices.....	137
5.1.12.Setting / Resetting Screen Lock Password for Selected Devices.....	139
5.1.13.Updating Device Information.....	141
5.1.14.Sending Text Message to Devices.....	142
5.2.Managing Device Groups.....	144
5.2.1.Creating Device Groups.....	147
5.2.2.Editing a Device Group.....	149
5.2.3.Assigning Configuration Profiles to a Device Group.....	152
5.2.4.Removing a Device Group.....	154
6.Configuration Profiles.....	155
6.1.Creating Configuration Profiles.....	156
6.1.1.Profiles for Android Devices.....	157
6.1.2.Profiles for iOS Devices.....	185
6.1.3.Profiles for Windows Devices.....	232
6.1.3.1.Creating Windows Profile.....	233
6.1.3.1.1.Antivirus Settings.....	238
6.1.3.1.2.File Rating Settings.....	251
6.1.3.1.3.Firewall Settings.....	253
6.1.3.1.4.Sandbox Settings.....	287
6.1.3.1.5.Viruscope Settings.....	301
6.1.3.1.6.HIPS Settings.....	303
6.1.3.1.7.Valkyrie Settings.....	329
6.1.3.1.8.CES Update Rule Settings.....	331
6.1.3.2.Importing Windows Profiles.....	332
6.2.Viewing and Managing Profiles.....	337
6.2.1.Exporting and Importing Configuration Profiles.....	339
6.2.2.Cloning a Profile.....	341
6.3.Editing Configuration Profiles.....	341
6.4.Managing Default Profiles.....	343
7.Applications.....	350
7.1.Viewing Applications Installed on Android and iOS Devices.....	351
7.1.1.Blacklisting and Whitelisting Applications.....	353
7.2.Viewing Applications Installed on Windows Devices.....	355
7.2.1.Viewing and Managing Unrecognized Files.....	356
7.2.2.Viewing and Managing Trusted Files.....	364
7.2.3.Viewing and Managing Malicious Files.....	370
7.2.4.Viewing list of Valkyrie Analyzed Files.....	375
7.3.Viewing and Managing Sandboxed Applications on Windows Devices.....	376
7.4.Viewing and Managing Software Vendors List.....	381
7.5.Installing OS Patches on Windows Endpoints.....	384

8.App Store.....	387
8.1.iOS Apps.....	388
8.1.1.Adding iOS Apps and Installing them on Devices.....	391
8.1.2.Managing iOS Apps.....	397
8.2.Android Apps.....	399
8.2.1.Adding Android Apps and Installing them on Devices.....	402
8.2.2.Managing Android Apps.....	407
9.Antivirus.....	409
9.1.Antivirus Scans.....	410
9.1.1.Running On-Demand Antivirus Scans on Devices.....	413
9.1.2.Handling Malware on Scanned devices.....	415
9.1.3.Updating Virus Signature Database at Windows Devices.....	417
9.2.Viewing and Managing Identified Malware.....	417
9.3.Viewing Threats History.....	421
9.4.Viewing and Managing Quarantined Items.....	424
10.Configuring Comodo Device Manager.....	425
10.1.Viewing and Managing Licenses.....	427
10.1.1.Upgrading or Adding the License.....	429
10.2.Configuring Variables and Groups	430
10.2.1.Creating and Managing Custom Variables.....	431
10.2.2.Creating and Managing Registry Groups.....	435
10.2.3.Creating and Managing COM Groups.....	439
10.2.4.Creating and Managing File Groups.....	443
10.3.Configuring Role Based Access Control for Users.....	449
10.3.1.Creating a New Role.....	452
10.3.2.Managing Permissions and Assigned Users of a Role.....	454
10.3.3.Removing a Role.....	459
10.3.4.Managing Roles Assigned to a User.....	460
10.4.Downloading CDM Installation Packages for Windows Devices.....	461
10.4.1.Downloading Package for installation through AD server.....	462
10.4.2.Downloading Offline Installation Package.....	463
10.5.Adding Apple Push Notification Certificate.....	465
10.6.Configuring the CDM Android Agent.....	470
10.6.1.Configuring General Settings.....	471
10.6.2.Configuring Android Client Antivirus Settings.....	474
10.6.3.Adding Google Cloud Messaging (GCM) Token.....	475
10.7.Configuring CDM Windows Client.....	483
10.8.Managing CDM Extensions.....	485
10.9.Configuring Email Templates.....	486
10.10.Configuring Email Notifications.....	489
10.11.Configuring CDM Reports.....	492
10.12.Importing User Groups from LDAP.....	493
10.13.Viewing Version and Support Information.....	499
About Comodo.....	501

1. Introduction to Comodo Device Manager

Comodo Device Manager (CDM) allows administrators to manage, monitor and secure mobile devices and Windows endpoints which connect to their enterprise wired and wireless networks.

Administrators must first add users to the CDM console and can then enroll devices 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. CDM also allows administrators to monitor the location of the device; run antivirus scans on the device; install/uninstall 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, view and manage malware identified from scans and Valkyrie analysis, manage OS update patches on Windows devices and more.



Each user license covers up to five mobile devices or one Windows endpoint for a single user. (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows endpoint). If more than 5 devices or 1 endpoint are added for the same user, then an additional user license will be consumed.

Guide Structure

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

Introduction to Comodo Mobile 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 CDM 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**

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

- **Devices List**
 - **Managing Windows Devices**
 - **Managing Android/iOS Devices**
 - **Viewing the User Information**
 - **Removing a Device**
 - **Remote Management of Windows Devices**
 - **Remotely Installing Packages onto Windows Devices**
 - **Installing Apps on Devices**
 - **Generating Alarm on Device**
 - **Locking/Unlocking Selected Devices**
 - **Wiping Selected Devices**
 - **Assigning Configuration Profiles to Selected Devices**
 - **Setting / Resetting Screen Lock Password for Selected Devices**
 - **Updating Device Information**
 - **Sending Text Message to Devices**
- **Managing Device Groups**
 - **Creating Device Groups**
 - **Editing a Device Group**
 - **Assigning Configuration Profiles to a Device Group**
 - **Removing a Device Group**

Configuration Profiles - 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**
- **Viewing and Managing Profiles**
- **Editing Configuration Profiles**
- **Managing Default Profiles**

Applications - Covers the management of applications installed on the managed devices, manage their ratings, manage software vendors list and OS update patches that can be pushed to Windows devices from the CDM console.

- **Viewing Applications Installed on Android and iOS Devices**
 - **Blacklisting and Whitelisting Applications**
- **Viewing Applications Installed on Windows Devices**
 - **Viewing and Managing Unrecognized Files**
 - **Viewing and Managing Trusted Files**
 - **Viewing and Managing Malicious Files**
 - **Viewing list of Valkyrie Analyzed Files**
- **Viewing and Managing Sandboxed Applications on Windows Devices**
- **Viewing and Managing Software Vendors List**
- **Installing OS Patches on Windows Endpoints**

App Store - Covers the management of applications that can be pushed to enrolled devices from the CDM 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**

Antivirus - Describes how to run AV scans on the enrolled devices, view threats and handle them manage quarantined items.

- **Antivirus Scans**
 - **Running On-Demand Antivirus Scans on Devices**
 - **Handling Malware on Scanned devices**
 - **Updating Virus Signature Database at Windows Devices**
- **Viewing and Managing Identified Malware**
- **Viewing Threats History**
- **Viewing and Managing Quarantined Items**

Configuring Comodo Device Manager - Contains explanations and tutorials on creating admin and user roles with different privilege levels and appropriately assigning them to enrolled users and configuring the behavior of various CDM components. Also covers management of subscriptions and renewal/upgrade of licenses, bulk enrollment of devices, AD server integration for importing user groups and so on.

- **Viewing and Managing Licenses**
 - **Upgrading or Adding the License**
- **Configuring Variables and Groups**
 - **Creating and Managing Custom Variables**
 - **Creating and Managing Registry Groups**
 - **Creating and Managing COM Groups**
 - **Creating and Managing File Groups**
- **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**
- **Downloading CDM Installation Packages for Windows Devices**

- [Downloading Package for installation through AD server](#)
- [Downloading Offline Installation Package](#)
- [Adding Apple Push Notification Certificate](#)
- [Configuring the CDM Android Agent](#)
 - [Configuring General Settings](#)
 - [Configuring Android Client Antivirus Settings](#)
 - [Adding Google Cloud Messaging \(GCM\) Token](#)
- [Configuring CDM Windows Client](#)
- [Managing CDM Extensions](#)
- [Configuring Email Templates](#)
- [Configuring Email Notifications](#)
- [Configuring CDM Reports](#)
- [Importing User Groups from LDAP](#)
- [Viewing Version and Support Information](#)

1.1. Key Concepts

Mobile Device - For the purposes of this guide, a mobile device is any Android or iOS smart phone or tablet that is allowed to connect to the enterprise network through a wireless connection. Comodo Device 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 Device Manager allows administrators to install Comodo Endpoint 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.

User - An employee or guest of the enterprise whose device(s) are managed by the CDM 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 Endpoint Security - Comodo Endpoint Security (CES) 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 Sandbox feature that runs unknown and unrecognized applications in an isolated environment at the endpoints. Each component of CES can be configured to offer desired security level by applying configuration profiles.

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

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

Notifications - Notifications are sent to devices by CDM 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. CDM 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 CDM extension to Comodo One customers and can be accessed from the CDM 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. CES 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 CDM interface.

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

Refer to [Enrolling Users' Devices for Management](#) for more details.

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

Refer to the section [Managing Device Groups](#) for more details.

5. The first level of defense on any device is to set a complex passcode policy. CDM 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. CDM offers flexible restrictions for Android devices over items such as Wi-Fi, packet data, bluetooth connectivity and use of camera. iOS restrictions are much more granular and also include App purchases, game center, voice dialing and more.

Refer to the restriction sections in [Profiles for Android Devices](#) and [Profiles for iOS Devices](#) for more details.

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

Refer to the section [Viewing Applications Installed on Enrolled Devices](#) for more details.

8. Keeping enrolled devices free from malware is vital to your organization's security. It is advisable to run antivirus scans

on devices regularly per your company's needs. CDM 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. CDM 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. CDM allows to configure different roles with different privileges and assign them to administrators as per organizational needs. Refer to the section **Configuring the Role-Based Access Control for Users** for more details.
10. Check the devices statuses regularly for compliance of deployed profiles and other reports. CDM provides at-a-glance view of platform details of devices, types of devices and other reports. Refer to the sections **The Dashboard** and **Device List** for more details.

1.3. Quick Start

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

Step 1 - Login to the Admin Console

Step 2 - Add Users

Step 3 - Enroll Users' Devices

Step 4 - Create Groups of Devices (optional)

Step 5 - Create Configuration Profiles

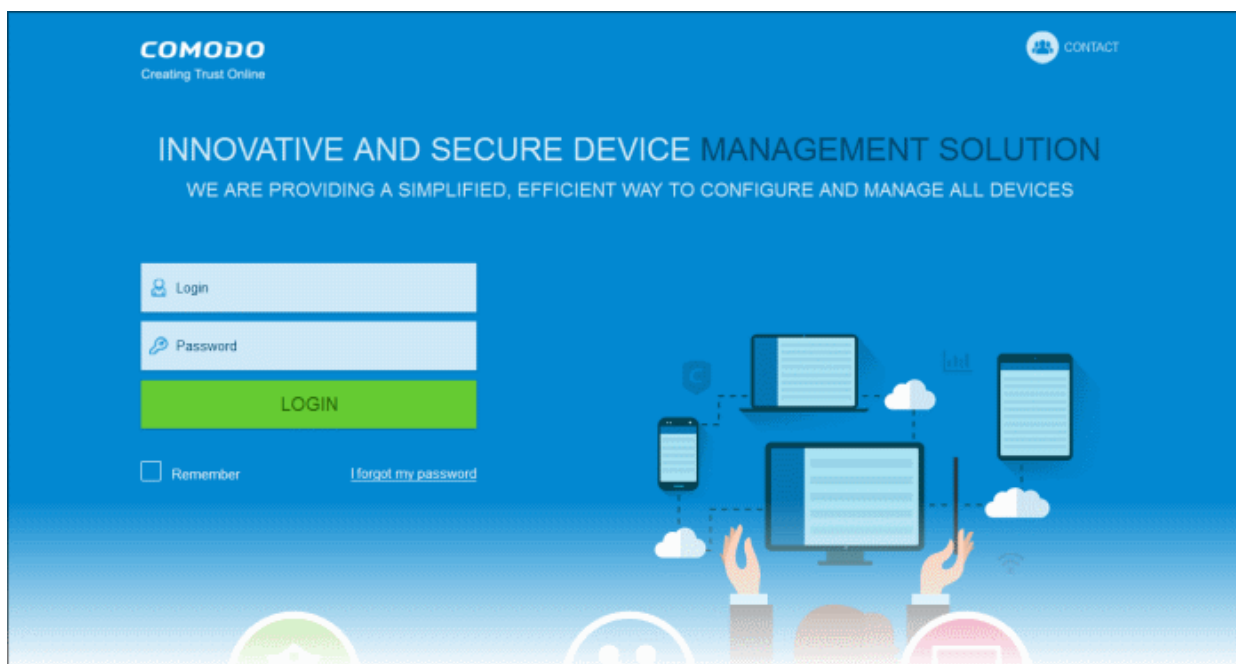
Step 6 - Applying profiles to devices or device groups

Note: This guide assumes you have already completed Comodo Device Manager set up and activation, and have acquired an Apple Push Notification (APN) certificate (iOS devices) and/or Google Cloud Messaging (GCM) token (Android devices). Refer to the online guide at <https://help.comodo.com/topic-214-1-633-8155-Comodo-Device-Manager---Cloud-Portal-Setup-Guide.html> if you need to find out more about adding APN certificates and GCM tokens.

Step 1 - Login to the Admin Console

The Comodo Device Manager (CDM) console can be viewed in any Internet browser.

- Enter the URL of your portal and the login credentials received through your Portal creation confirmation mail.



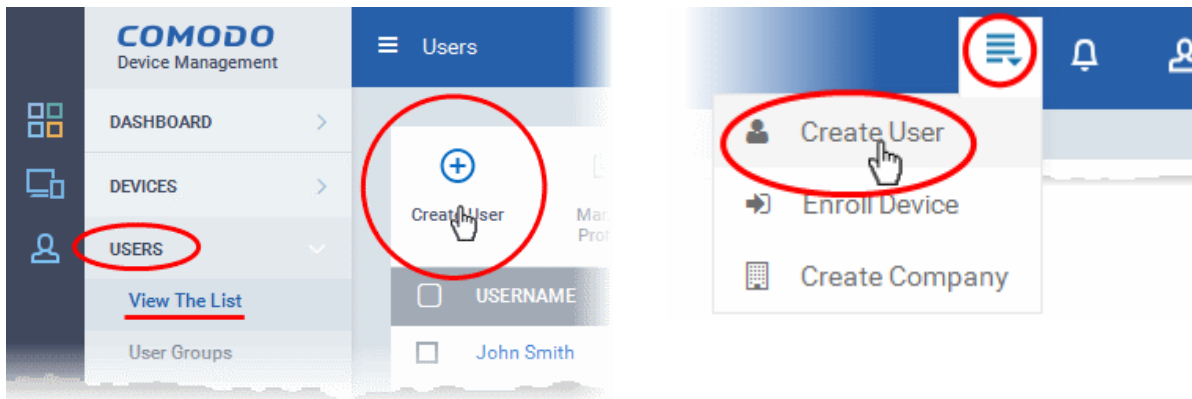
Step 2 - Add User

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

- **Comodo One users** - if you created only one company in C1, then any users you enroll here will be automatically assigned to that company. If you created more than one company in C1, the 'Enroll User' dialog will allow you to choose the company to which you want to assign the user.
- **CDM Users** - You can add users and enroll their devices without selecting any company. However, If you need the users/devices to be grouped under different companies, you can create companies in CDM and add device groups under them as explained in **Step 4 - Create Groups of Devices**.

To add a user

- Open the 'Users' interface by clicking the 'Users' tab from the left hand side and choosing 'View The List' from the options and click the 'Create User' above the table.
- or
- Choose 'Create User' from the drop-down at the top right:



The 'Create new user' form will open.

Create new User
Close

Username *

Email *

Phone number

Company *

Assign role

- Type a login username (mandatory), email address (mandatory) and phone number of the user to be added.
- Choose the company (mandatory), from the 'Company' drop-down.
 - Comodo One Users - The drop-down will display the companies added to C1. You can choose the company to which the user belongs. The user will be enrolled under the chosen company.
 - CDM users - Leave the selection as 'Default Company'.
- Choose a role for the user. A 'role' determines user permissions within the CDM console itself. CDM ships with two default roles:
 - **Administrators** - Full administrative privileges in the CDM console. The permissions for this role are not editable.
 - **Users** - In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to CDM.

You can create roles with different permission levels via the 'Role Management' screen (click 'Settings > Role Management'). You can edit the permissions of existing roles by clicking on the role in the list and add or remove permissions as required. Any new roles you create will become available for selection in the 'Roles' drop-down when creating a new user. See [Configuring the Role-Based Access Control for Users](#) and [Managing Roles assigned to a User](#) for more details.

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

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

- Repeat the process to add more number of users.

If an administrator is added, an activation mail will be sent to their registered email address. The new administrator needs to

activate their account and set the login password by clicking the activation link in the email.

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

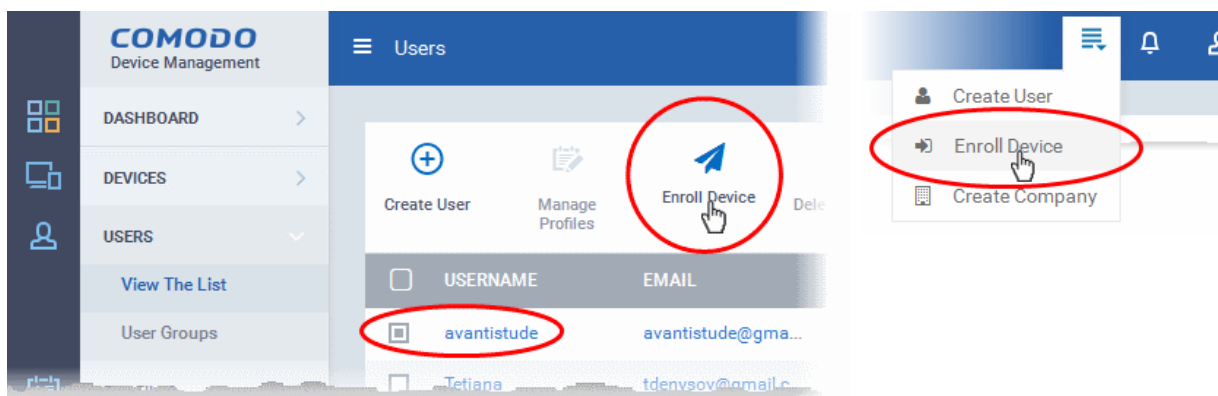
Step 3 - Enroll Users' devices

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

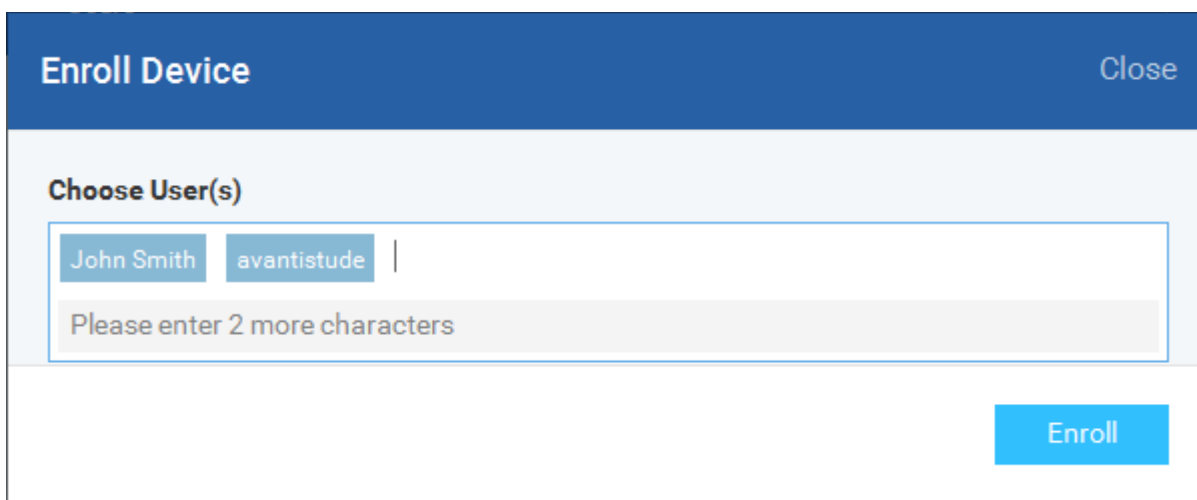
Each user license enables to enroll a maximum of five mobile devices or one Windows endpoint for a single user. (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows endpoint). If more than 5 devices or 1 endpoint are added for the same user, then an additional user license will be consumed. Administrators can purchase additional licenses from the Comodo website if required.

To enroll devices

- Click the 'Users' tab from the left and choose 'View The List' to open the 'Users' interface
- Select the user(s) whose devices are to be enrolled and click the 'Enroll Device' button above the table in the 'Users' interface'.
- Or
- Choose 'Enroll Device' from the drop-down at the top right



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

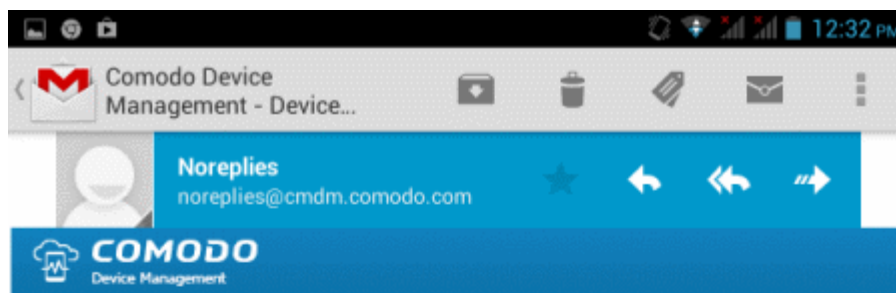


The 'Choose Users' field is pre-populated with the users chosen from the 'Users' interface, if you have chosen the users from the 'Users' interface before clicking 'Enroll Device' button.

- To add more users, start typing first few letters of the username and choose the user from the search results drop-down.
- Click 'Enroll'

A device enrollment email will be sent to each user. The email will contain a link to the enrollment page containing the

instructions and links to download the DM agent/profile for the device to be enrolled and configuring them. An example mail is shown below.



Welcome to Comodo Device Management!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Management 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
- iOS, Android or Windows.
- 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://mdmstage.comodo.od.ua:443/enroll/device/by/token/af25f8380a2d0491b12b2d4099944489>




- Clicking the link will take the user to the enrollment page containing the links to download and configure agent/profile for Android, iOS and Windows devices.

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.




Welcome to Comodo Device Management!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Management system. This system allows you to manage application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.


 **FOR ANDROID DEVICES**

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

After installation, enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/android/index/token/af25f8380a2d0491b12b2d4099944489>

 **FOR IOS DEVICES**


Enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/ios/index/token/af25f8380a2d0491b12b2d4099944489>

 **FOR WINDOWS DEVICES**

Enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/windows/index/token/af25f8380a2d0491b12b2d4099944489>

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:



FOR ANDROID DEVICES

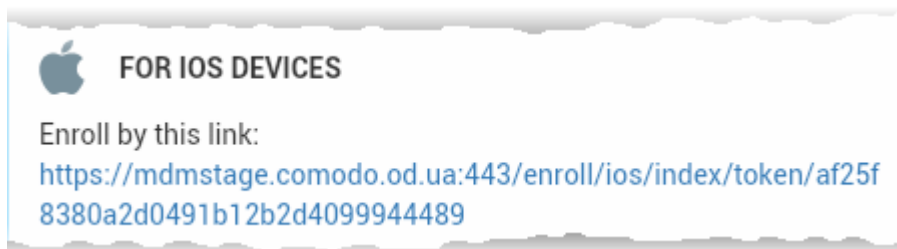
Download and install the Comodo Device Management app by tapping the following link:
<https://play.google.com/store/apps/details?id=com.comodo.mdm>

After installation, enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/android/index/token/af25f8380a2d0491b12b2d4099944489>

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

Enroll iPhones, iPods and iPads

The device enrollment email contains a single enrollment link under 'FOR IOS DEVICES'. The user clicks this link to download the CDM client authentication certificate and CDM profile. Once installed, the authentication certificate will be used to verify the user and the device when he or she attempts to connect to your network.



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.

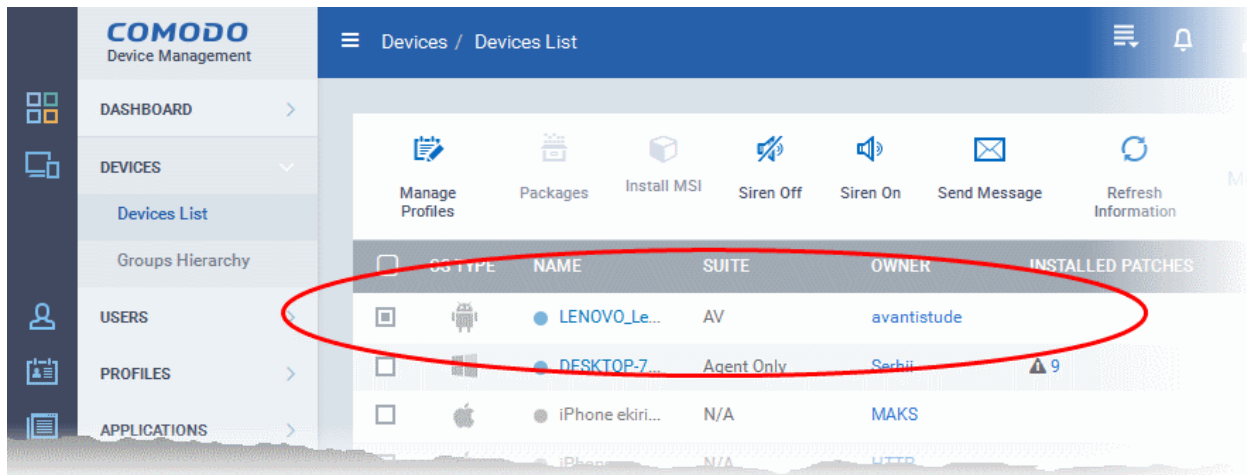
Enroll Windows PCs

The device enrollment page contains a single enrollment link under 'FOR WINDOWS DEVICES'.



The user clicks this link to download the Comodo Device Management client app. Once installed, the app will enroll the device into CDM . Upon successful enrollment, CDM will remotely install the endpoint security software Comodo Endpoint Security (CES) on to the device.

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



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

See **Devices** for more details.

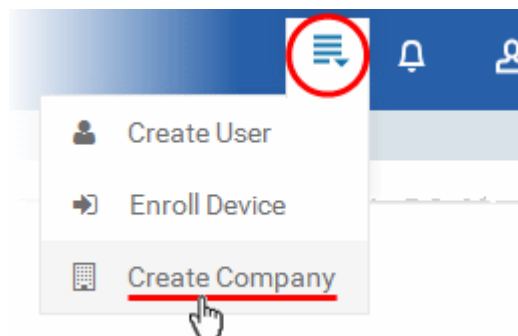
Step 4 - Create Groups of Devices (optional)

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

- **Comodo One Users** - Device Groups can be created under respective companies to which their users belong, if the companies are already defined in Comodo One.
- **CDM Users** - If no companies are added yet or if you want a group to be created under a new company, you can create a new company in CDM.

To create a company

- Choose 'Create Company' from the drop-down at the top right:



The 'Create new Company' dialog will appear.

Create new Company Close

Name *

Subdomain *

Email *

[Submit](#)

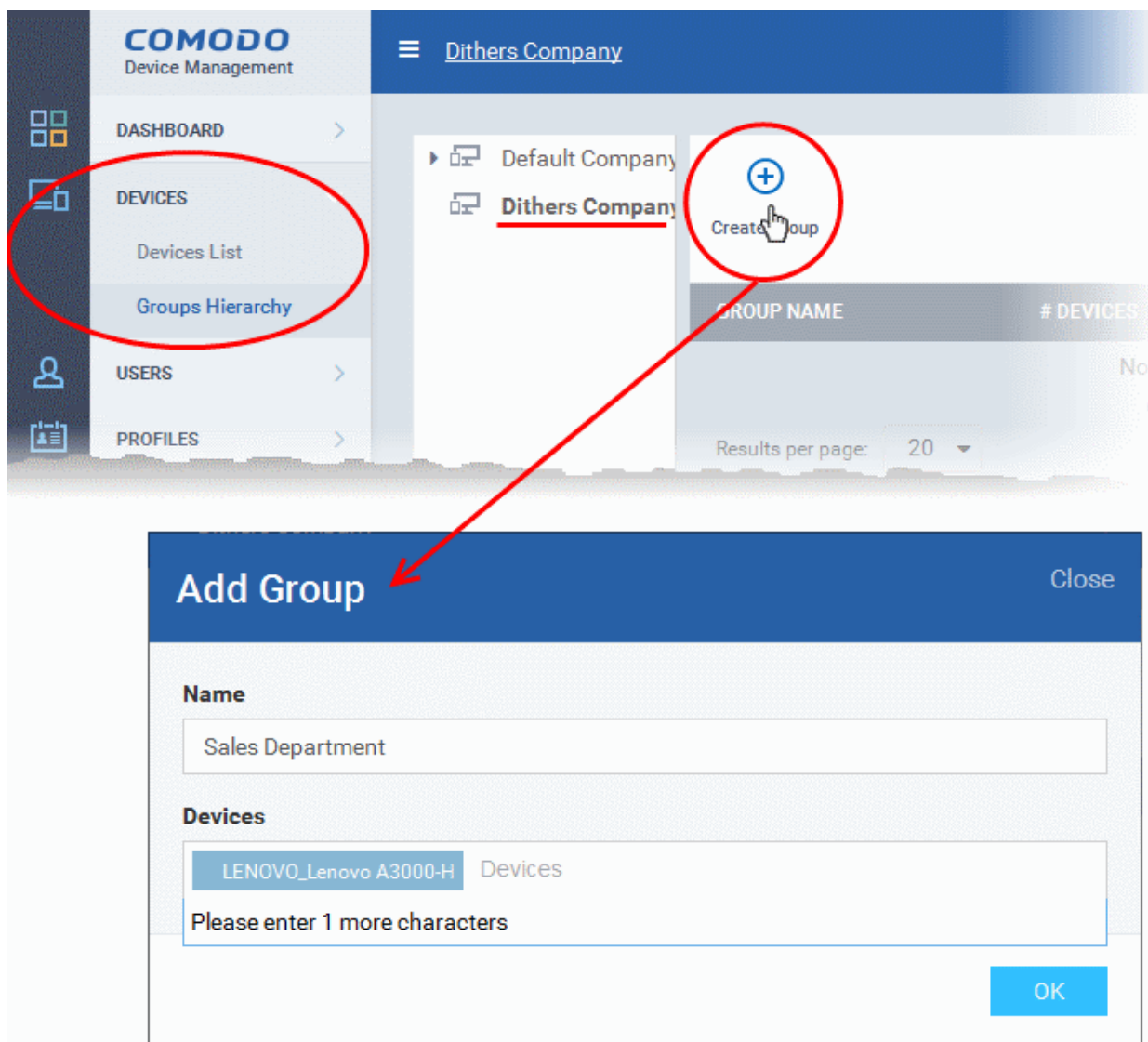
- Enter the company name (mandatory), the sub domain (mandatory) to be added to the URL to access the MDM interface for the company and the administrator email address (mandatory) for the company in the respective fields and click 'Submit'.

The company will be created.

- Repeat the process to add more companies.

To create a device group

- Click the 'Devices' tab from the left and choose 'Groups Hierarchy'
- Choose the Company under which you wish to create a new group from the left (optional)



- Click 'Create Group' from the top of the right pane

The 'Create/Edit Device Group' interface will open.

- You now have to name the group and choose the device(s). Enter a name in the 'Name' field. Type the first few letters of the device name in the Devices field and choose the device from the drop-down that appears. Repeat the process for adding more devices. You can also add devices after the group is created by clicking on the group name from the same screen > 'Add to Group' button and selecting the devices from the list.
- Click 'Save'. Repeat the process to create more groups. Refer to the section **Managing Device Groups** for more details.

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

Step 5 - Create Configuration Profiles

A configuration profile is a collection of settings which can be applied to mobile devices and PCs that have been enrolled into Comodo Device Manager. Each profile allows an administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.

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

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

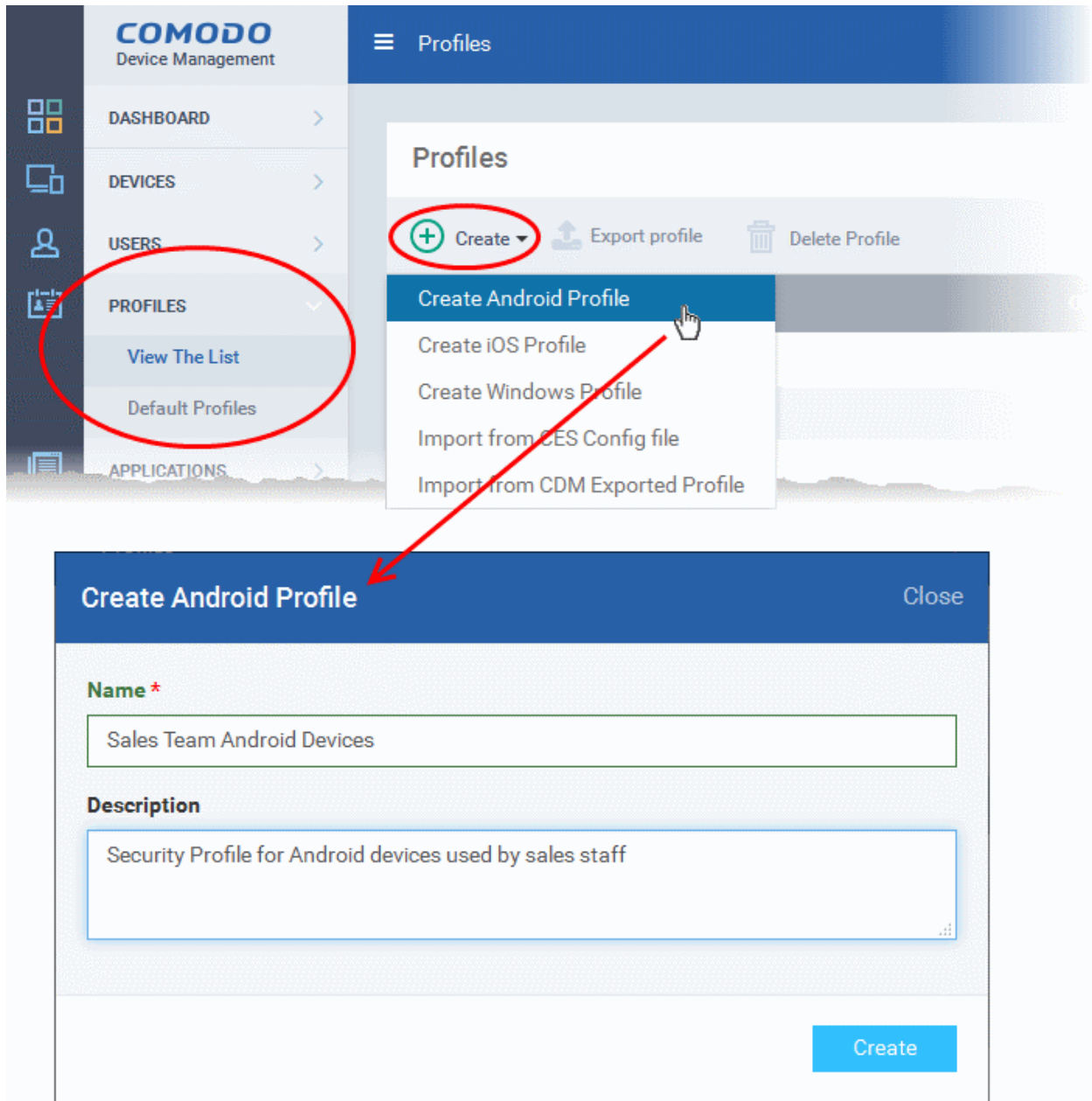
Profile specifications differ between iOS, Android and Windows Devices:

- **Android profiles**

- **iOS profiles**
- **Windows Profiles**

To create an Android Profile

- Click the 'Profiles' tab from the left and choose 'View The List'.
- 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.

Profiles / Sales Team Android Devices

Logout (John Smith)

Sales Team Android Devices

Add Export Profile Clone Profile Delete Profile


General

General Settings Edit

Name *
Sales Team Android Devices
Display name of the profile (shown on the device).

Is Default
Disabled

Description
Security Profile for Android devices used by sales staff
Brief explanation of the contents or purpose of the profile

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

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

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

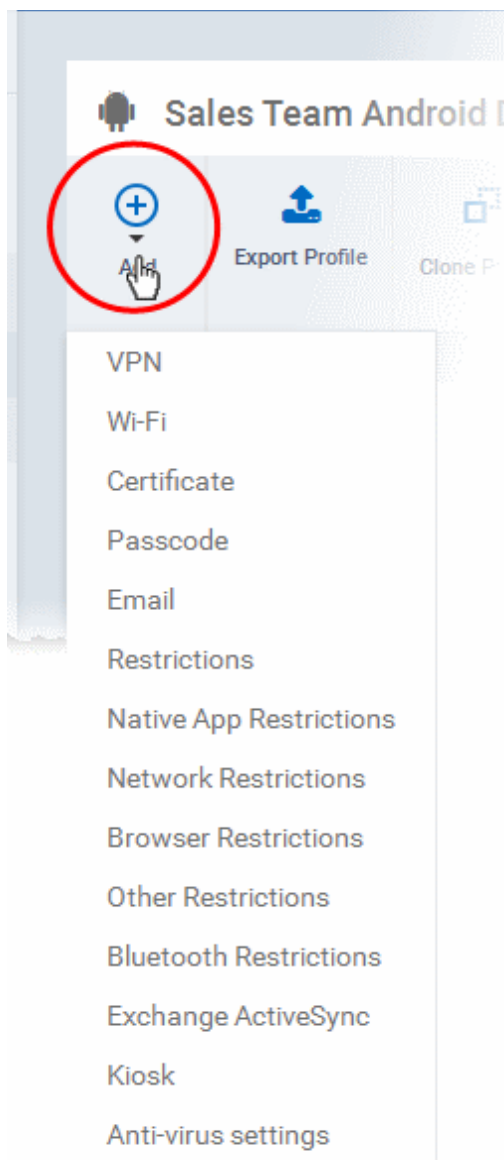
The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top. You can configure passcode settings, feature restrictions, antivirus settings Wi-Fi settings and more. If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another CDM 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.
- **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'.
- **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.
- **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.
- **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.



- **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.
- **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.
- **Browser Restrictions** - Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- **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.
- **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.
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers. This profile is supported for SAFE devices only.
- **Kiosk** - Enable and configure Kiosk Mode for SAFE devices like the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices and whether SMS/MMS are allowed. This profile is supported for SAFE devices only.
- **Antivirus Settings** - Schedule antivirus scans on the device and specify trusted Apps to be excluded from AV scans.

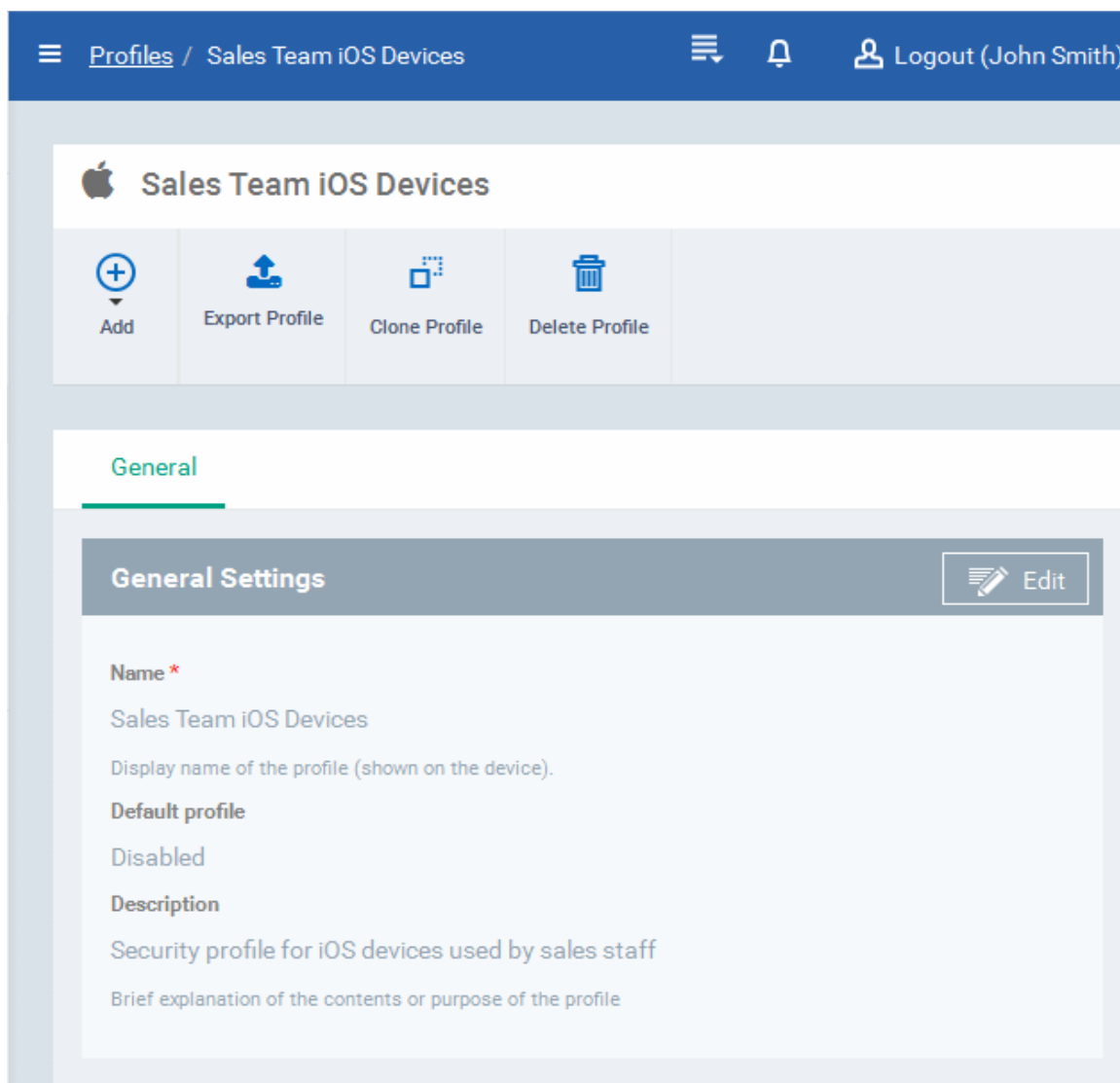
To create an iOS Profile


- Click the 'Profiles' tab from the left and choose 'Profile List'.
- Click 'Create' drop-down above the table and then click 'Create iOS Profile'.

The screenshot displays the Comodo Device Manager interface. On the left, a navigation sidebar includes 'DASHBOARD', 'DEVICES', 'USERS', 'PROFILES', and 'APPLICATIONS'. The 'PROFILES' menu item is circled in red. The main content area shows the 'Profiles' management page with a '+ Create' button circled in red. A dropdown menu is open, listing options: 'Create Android Profile', 'Create iOS Profile', 'Create Windows Profile', 'Import from CES Config file', and 'Import from CDM Exported Profile'. A red arrow points from the 'Create iOS Profile' option to a modal window titled 'Create iOS Profile'. The modal contains a 'Name' field with the text 'Sales Team iOS Devices' and a 'Description' field with the text 'Security profile for iOS devices used by sales staff'. A 'Create' button is visible at the bottom right of the modal.

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

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



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

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

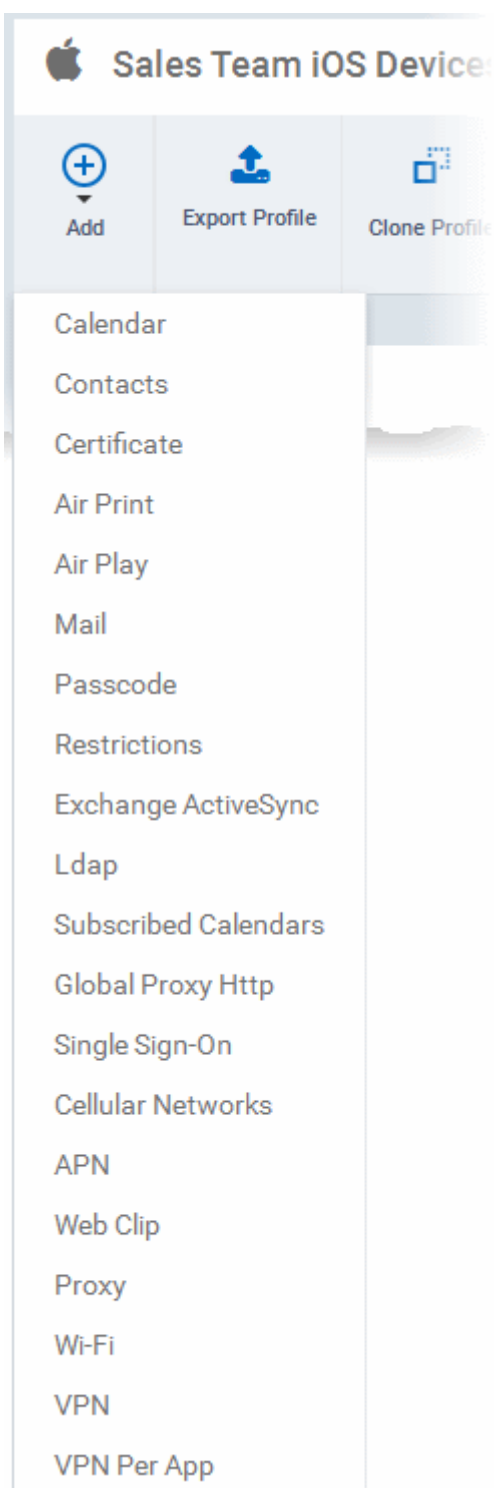
- Click 'Add' drop-down button and select the component from the list that you want to include for the profile

The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top. 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 CDM 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.
- **Calendar** - Configure CalDAV server and connection settings which will allow device integration with corporate scheduling and calendar services.
- **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).



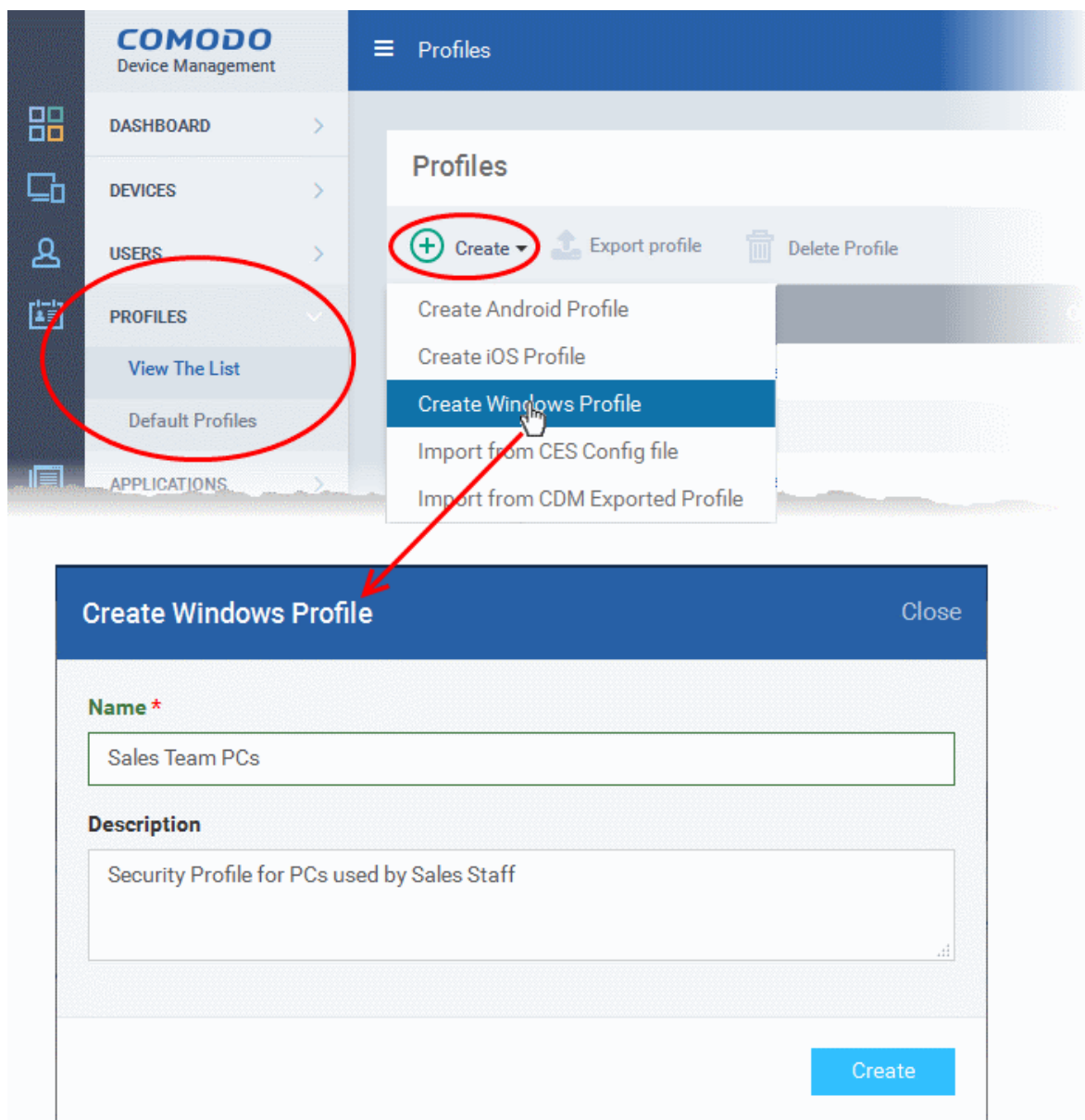
- **Certificate** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi', 'Exchange Active Sync', 'VPN' and so on.
- **Airprint** - Specify the location of Airprint printers so they can be reached by devices under this profile (iOS 7 +)
- **Airplay** - Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (iOS 7 +)
- **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.
- **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.
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.
- **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.
- **VPN Per APP** - Instead of forcing all BYOD traffic over the corporate VPN tunnel, 'Per-app VPN' functionality allows admins to choose specific 'managed apps' which should always connect via VPN. This improves user privacy and network performance by keeping all private browsing and emails off the corporate VPN. This section allows you to configure the VPN service that those managed apps will connect to.
- **LDAP** - Configure LDAP account settings for devices under this profile so users can connect to company address books and contact lists.
- **Subscribed Calendars** - Specify one or more calendar services which you wish to push notifications to devices under this profile.
- **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.
- **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.
- **Cellular Networks** - Configure cellular network settings. The 'cellulars' setting performs a similar role to the APN setting and actually replaces it in iOS 7 and above.
- **APN** - Specify an Access Point Name for devices on this profile. APN settings define the network path for all cellular data. This area allows you to configure a new APN name (GPRS access point), username/password and the address/port of the proxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.
- **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.

- **Proxy** - Allows you to specify the proxy server, and their credentials, to be used by the device for network connections.
- **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.
- **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 iOS 7 and above.
- **VPN Per App** - 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 exclusively for Safari domains. This profile is supported for iOS 7 and above.

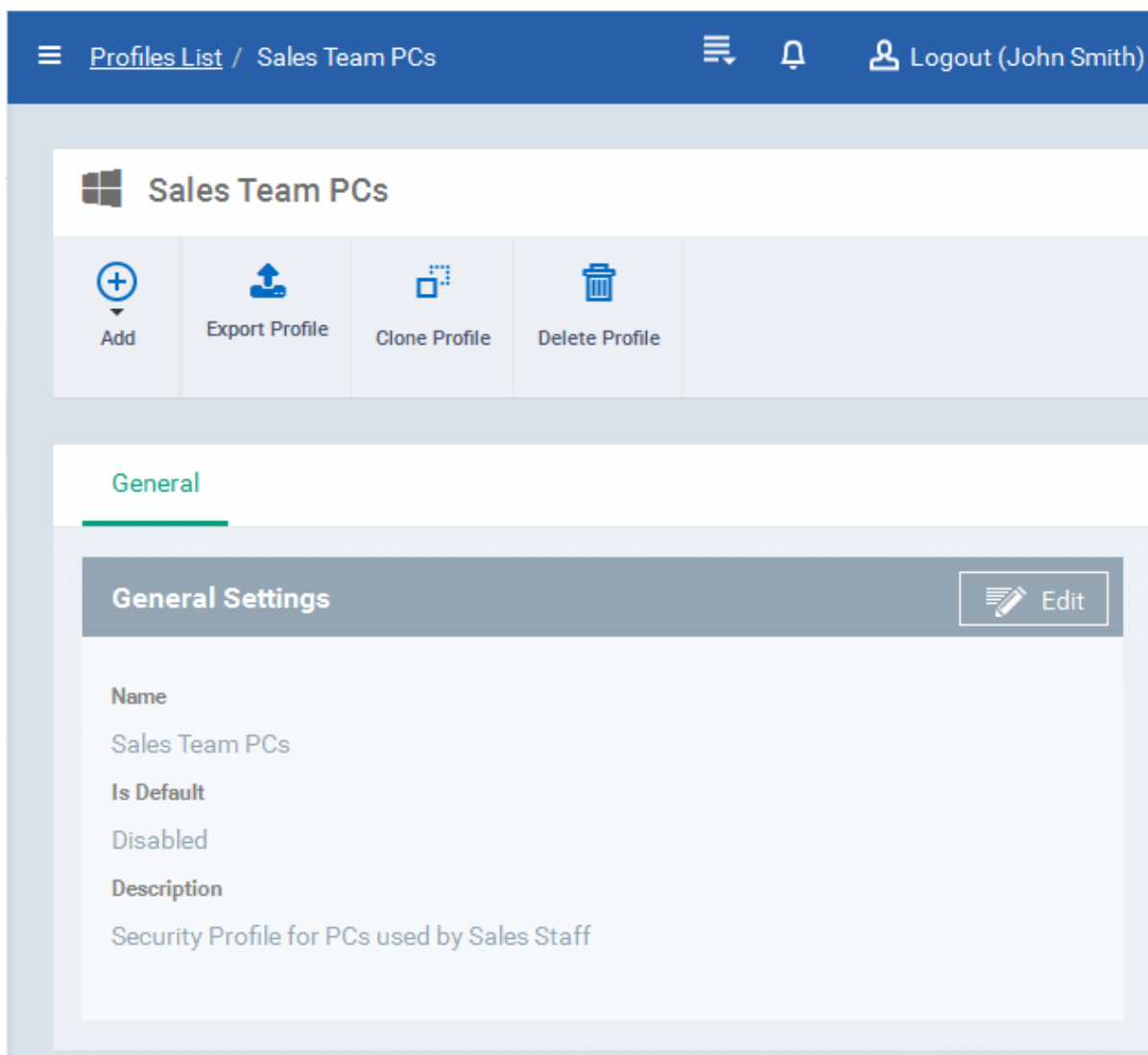
To create a Windows profile


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



- Enter a name and description for the profile (for example, 'Sales Dept endpoints', 'Win7 Machines' or 'Field Executives Laptops') and click 'Create'.

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



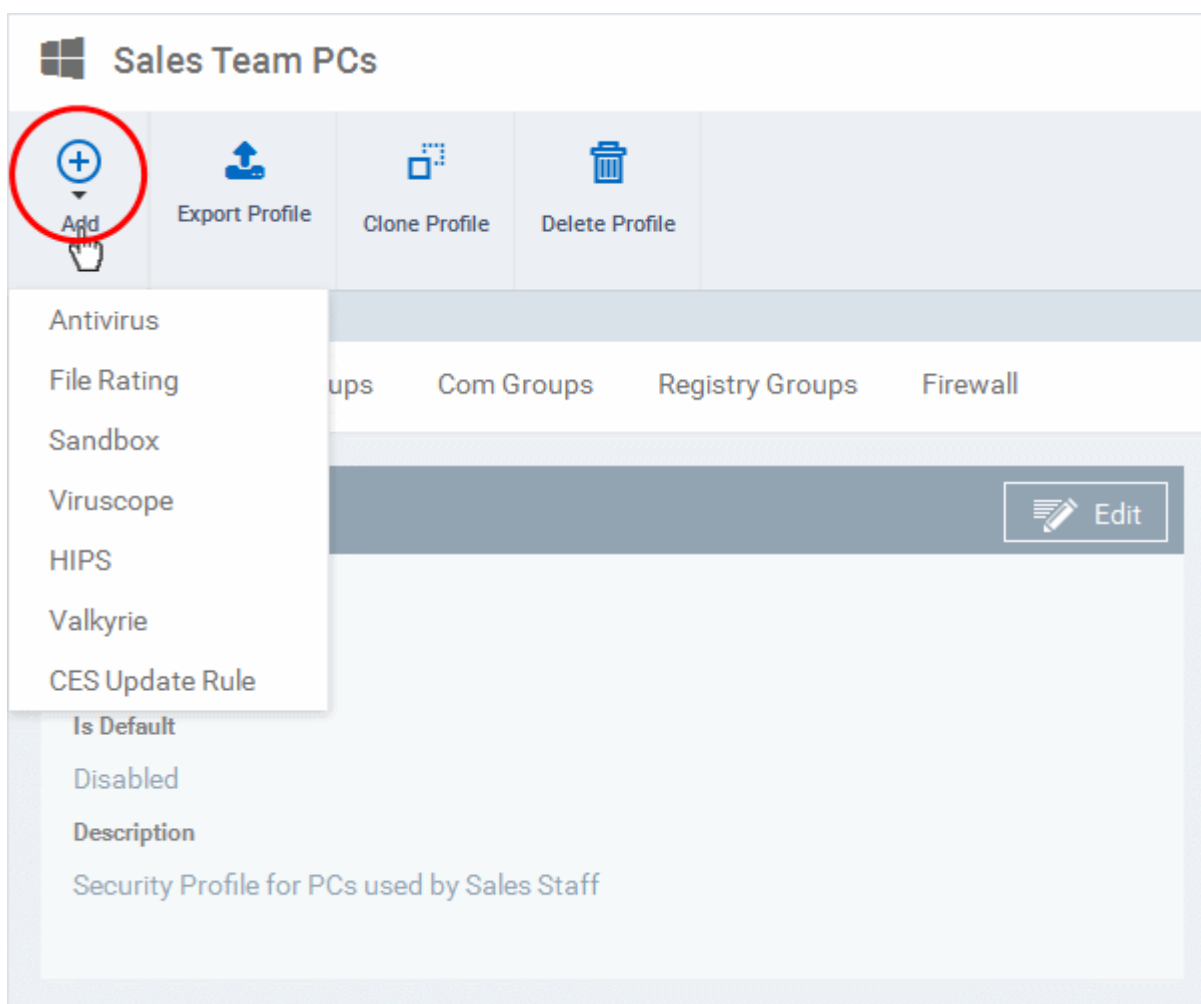
- If you want this profile to be a default policy, click on the 'Edit' button  at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- Click 'Save'.

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

- Click 'Add' 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 links at the top. You can configure Antivirus, Firewall, Sandbox, File Rating, Valkyrie, HIPS, Viruscope and Update settings. In addition, you can configure the File Groups, COM Groups and Registry Groups 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 CDM profile.



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

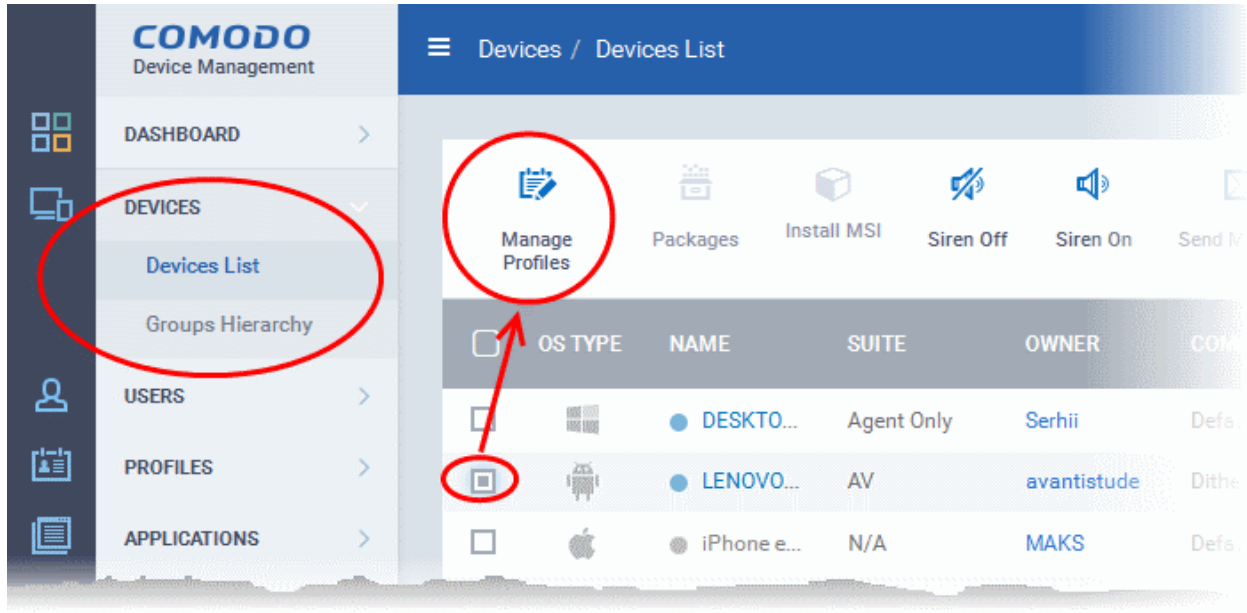
See [Profiles for Windows Devices](#) in the full guide for more information on these settings. In brief:

- **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.
- **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 CES, refer to the [help page explaining File rating Settings](#) in [CES online help guide](#).
- **Firewall** - Enable/Disable the Firewall component, configure Firewall behavior, add and manage Application and Global Firewall rules and more. For more details on Firewall in CES, refer to the [help page explaining Firewall Settings](#) in [CES online help guide](#).
- **Sandbox** - Enable Auto-Sandboxing of unknown files, add exclusions, and configure sandbox behavior and alert options and view and manage Sandbox Rules for auto-sandboxing applications.
- **Viruscope** - Enable Viruscope that monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten your privacy and/or security and configure options for alert generation. For more details on Viruscope in CES, refer to the [help page explaining Viruscope](#) in [CES online help guide](#).
- **HIPS** - Enable Host Intrusion Prevention System (HIPS) and its behavior, configure HIPS rules and define Protected Objects at the endpoints. For more details on HIPS in CES, refer to the [help page explaining HIPS Settings](#) in [CES 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.
- **CES Update Rule** - Set the conditions for the CES installations at the endpoints to automatically download and install

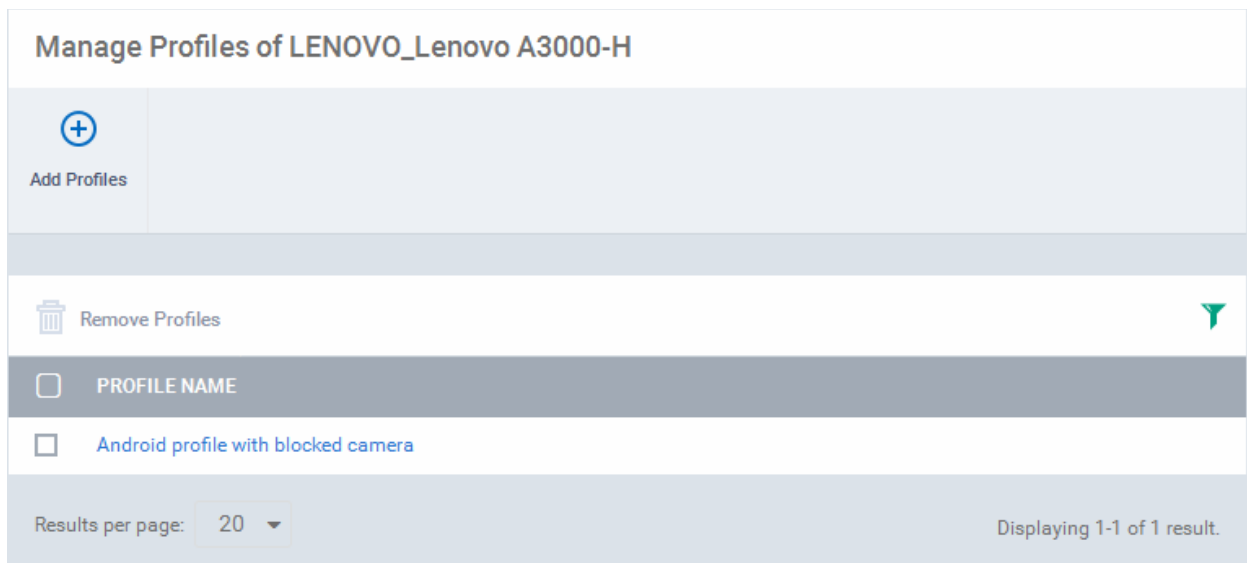
the program and virus database updates.

Step 6 - Apply profiles to devices or device groups

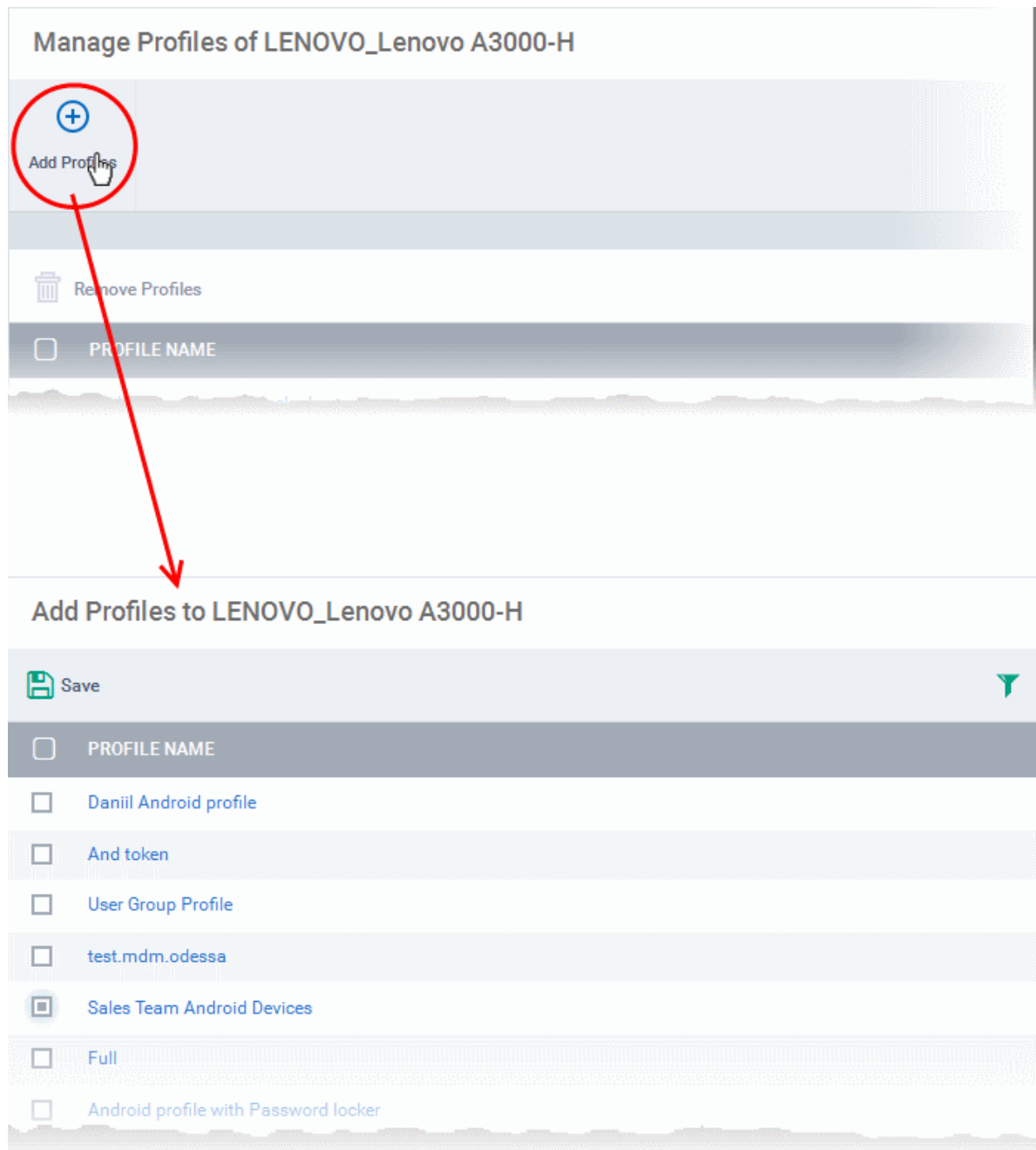
1. Click the 'Devices' tab from the left and choose 'Devices List' from the options.
2. Select the device to be managed and click 'Manage Profiles' from the options at the top .



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



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



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

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

To apply profiles to a *group* of devices

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

1. Click the 'Devices' tab from the left and choose 'Groups Hierarchy ' from the options.
2. Choose the Company to view the list of groups in the right pane
3. Click on the name of the device group
4. Click 'Manage Profiles'
5. Select the profile(s) to be applied to the devices in the group
6. Click 'Save' at the top left to add the selected profile(s) to the device group

If you have successfully followed all 6 steps of this quick start guide then you should have a created a basic working

environment from which more detailed strategies can be developed. Should you need further assistance, each topic is covered in more granular detail in the full administrator guide. If you have problems that you feel have not been addressed, then please contact mdmsupport@comodo.com.

1.4. Logging into your Administration Console

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



- Enter your username and password and click Login.

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





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

After successful login, the 'Get Started with Comodo Device Management' screen will be displayed.

The screenshot shows the Comodo Device Manager interface. On the left is a navigation sidebar with icons for Dashboard, Devices, Users, Profiles, Applications, App Store, Antivirus, and Settings. The main content area is titled 'Get Started with Comodo Device Management' and includes a sub-header 'Start to manage devices with a few simple steps.' Below this are four numbered steps, each with an icon and a list of actions:

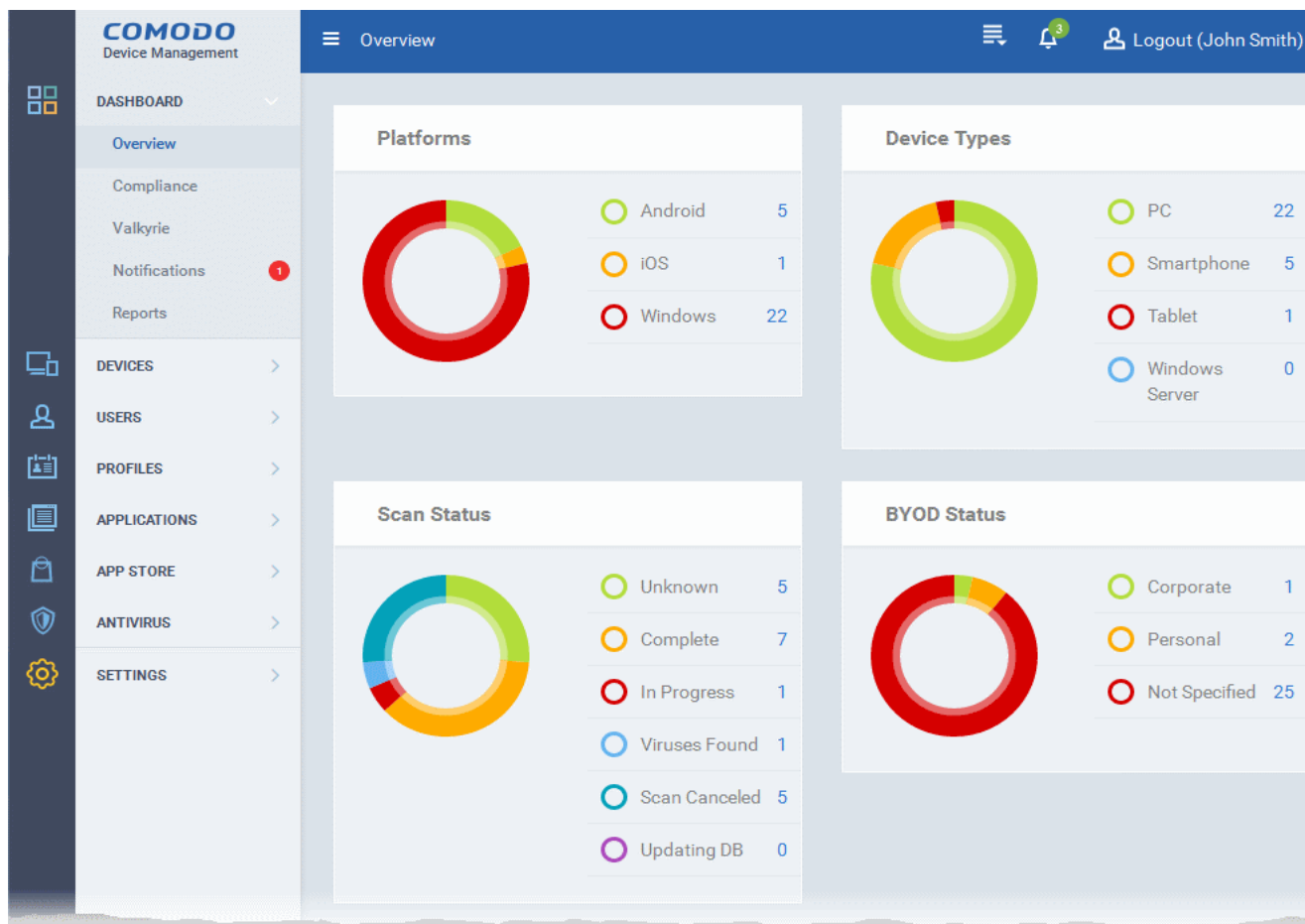
- 1. Add Users**: Includes an icon of a person. Steps: Open Users list; Click "Create User"; Or add users via Active Directory; Create User Groups if required.
- 2. Enroll Their Devices**: Includes an icon of a device with an arrow. Steps: Open Users List; Select users; Click Enroll Device; User(s) will receive enrollment emails.
- 3. Configure Device Profile**: Includes an icon of gears. Steps: Go to Profiles and click "Create"; Choose OS, name and description; Open the profile and click "Add" to configure security policy.
- 4. Associate Profile With Devices**: Includes an icon of a device with a profile icon. Steps: Open Devices 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. Refer to the section '[Creating New User Accounts](#)' for more details. The tile also contains shortcut to 'Active Directory' settings interface to integrate an AD server and import the user groups from it. Refer to the section '[Importing User Groups from LDAP](#)' for more details.
- **Enroll Their 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 Device' from the top. Refer to the section '[Enrolling User Devices for Management](#)' for more details.
- **Configure the profile** - Allows you to create and manage configuration profiles for Android, iOS and Windows devices by clicking the  icon. Refer to the section '[Configuration Profiles](#)' for more details.
- **Associate the profile with device** - Allows you to deploy and manage configuration profiles on devices by clicking the  icon. Refer to the section '[Devices](#)' for more details.

2. The Administrative Console

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



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

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

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

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

Profiles - Create and manage configuration profiles to be applied to enrolled iOS and Android Smartphones and Tablets and Windows endpoints. Refer to the section [Configuration Profiles](#) for more details.




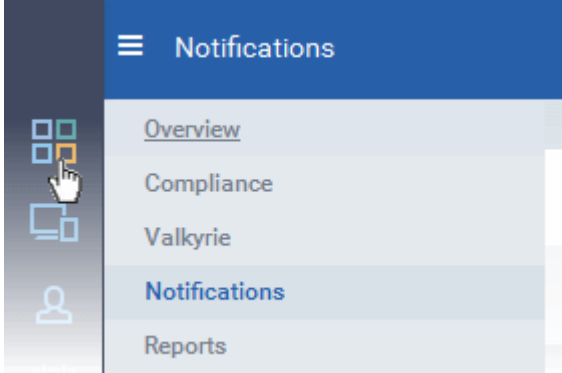


Applications - Allows administrators to view and manage applications installed on enrolled Android and iOS devices, view files installed on managed Windows devices, sandboxed programs, view and manage software vendors list and manage OS patch installation on to managed Windows devices. Refer to the section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

App Store - Allows administrators to add apps to be pushed to managed iOS and Android devices. Refer to the section [App Store](#) for more details.

Antivirus - Allows administrators to run AV scans and virus signature database updates on the enrolled devices, manage identified malware, view threats and manage quarantined items. Refer to the section [Antivirus](#) for more details.

Settings - Allows administrator to create admin and user roles with different privilege levels and appropriately assign them to users, configure the behavior of various CDM components and agents, renew/upgrade licenses and more. See [Configuring Comodo Mobile Device Manager](#) for more details.

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

	<p>Clicking this button will display the 'Create User' and 'Enroll Device' drop-down. Refer to the sections 'Creating New User Accounts' and 'Enrolling Users' Devices for Management' for more details.</p>
	<p>The number beside the bell icon indicates the unread CDM notifications. Click this to view the notification in the drop-down. On clicking the notification, or on 'See all notifications' link the 'List of Notifications' screen will open. Refer to the explanation of 'Notifications' in the section The Dashboard for more details.</p>
	<p>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.</p> 
	<p>Clicking the logo will open the 'Welcome' screen. Refer to the section 'Logging into your Administrative Console' for more details.</p>
	<p>Displays the username of the person currently logged in. Click this to log out of CDM interface.</p>

3. The Dashboard

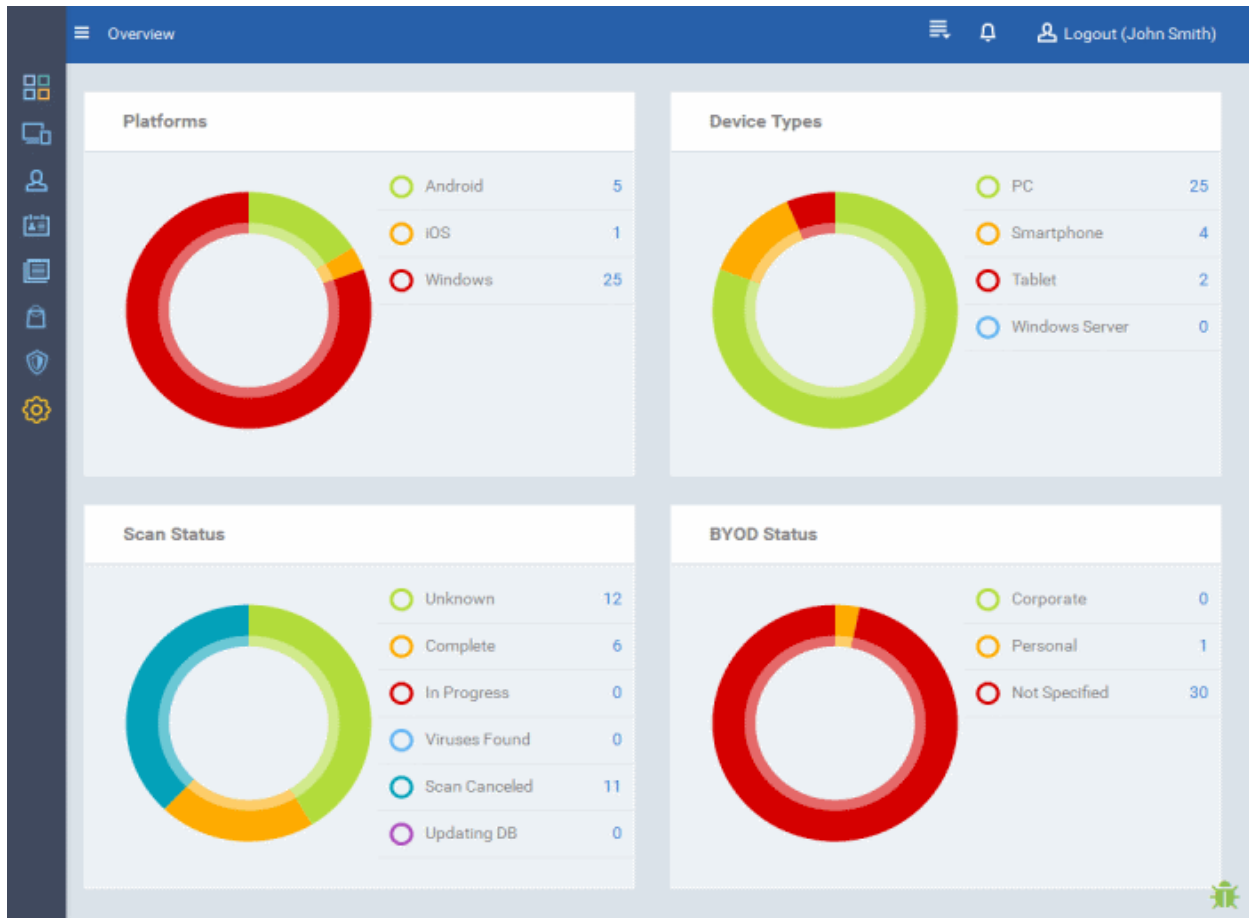
The Dashboard displays a snapshot summary of devices enrolled to Comodo Device Manager (CDM), their types, ownership, Antivirus (AV) scan status and Compliance status of devices, as pie charts. The dashboard also enables you to view the results of Valkyrie tests, a list of sent notifications and to generate reports.

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

- **Overview** - Displays statistical information of types of managed devices, antivirus scan results ownership details as pie-charts. Refer to the section [Overview](#) for more details.
- **Compliance** - Displays statistical information on compliance of managed devices to the security profiles applied to them. Refer to the section [Compliance](#) for more details.
- **Valkyrie** - Displays the results of analysis of unknown files automatically uploaded from managed Windows devices from Valkyrie, as pie-chart. Refer to the section [Valkyrie](#) for more details.
- **Notifications** - Displays a list of notifications sent to the administrator by CDM. Refer to the section [Notifications](#) for more details.
- **Reports** - Displays the list of reports generated by CDM and enables you to generate new reports. Refer to the section [Reports](#) for more details.

Overview

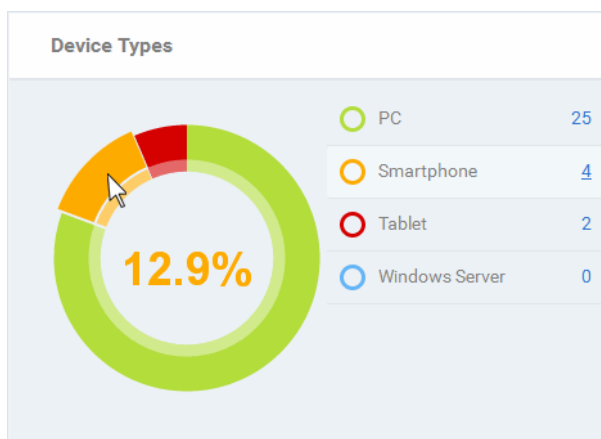
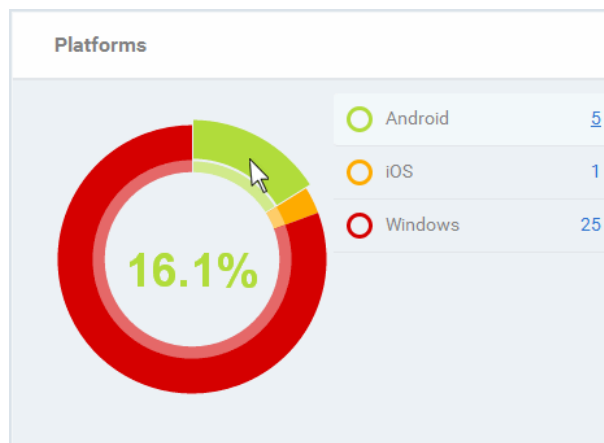
The overview screen provides a snapshot summary of devices enrolled to Comodo Device Manager (CDM), their types, ownership, Antivirus (AV) scan status as pie charts.



Platform Details

The 'Platform details' pie chart and legends provides at-a-glance comparison of devices of different Operating Systems. Placing the mouse cursor over a sector or on the respective legend displays the details.

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



Device Types

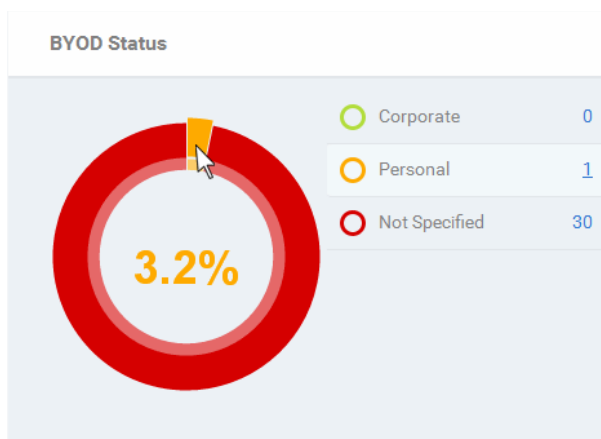
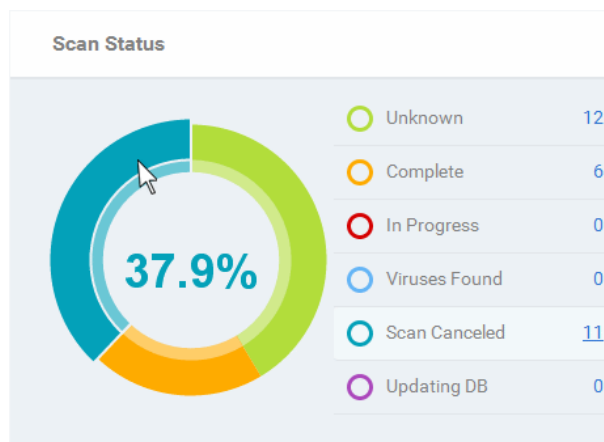
The 'Device Types' pie chart and legends provides at-a-glance comparison of devices of different types like smart phones, Windows server, PC and tablets. Placing the mouse cursor over a sector or on the respective legend displays the details.

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

Scan Status

The 'Scan status' pie chart and legends provides at-a-glance comparison of devices of different AV scan status, like completed, infected and so on. Placing the mouse cursor over a sector or on the respective legend displays the details.

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



BYOD Status

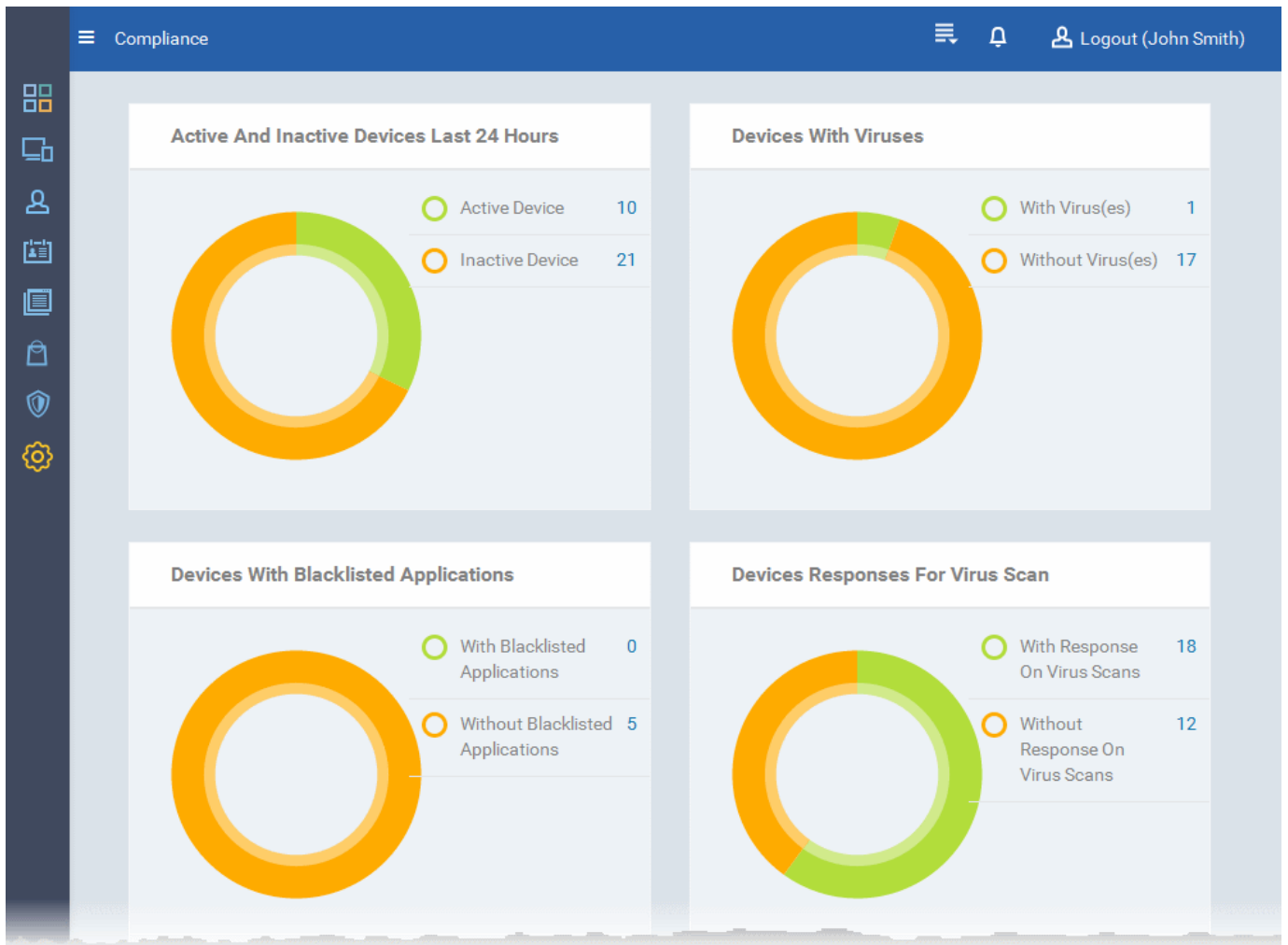
The 'BYOD status' pie chart and legends provides at-a-glance comparison of ownership of enrolled devices, like personal devices of the users, company owned devices lent to the users and so on. Placing the mouse cursor over a sector or on the respective legend displays the details.

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

Compliance

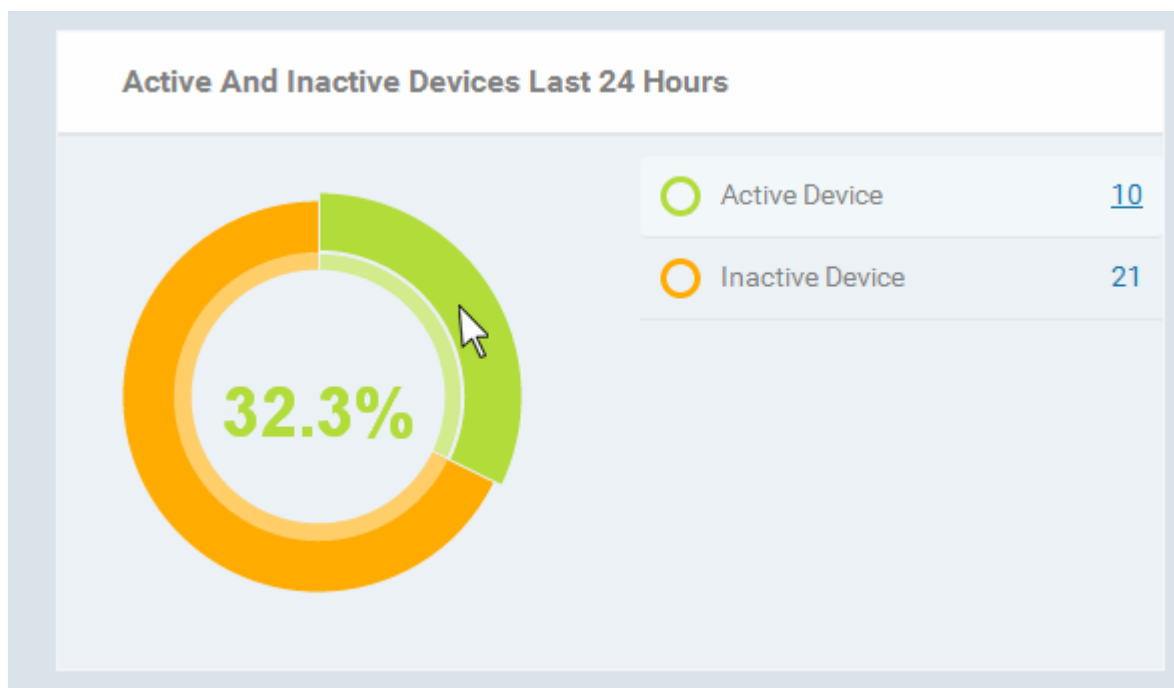
The compliance report of devices is a graphical summary of devices that are complaint and non-complaint, viruses status in the devices, blacklisted applications status and virus scan status in the enrolled devices.

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



Active / Inactive Devices

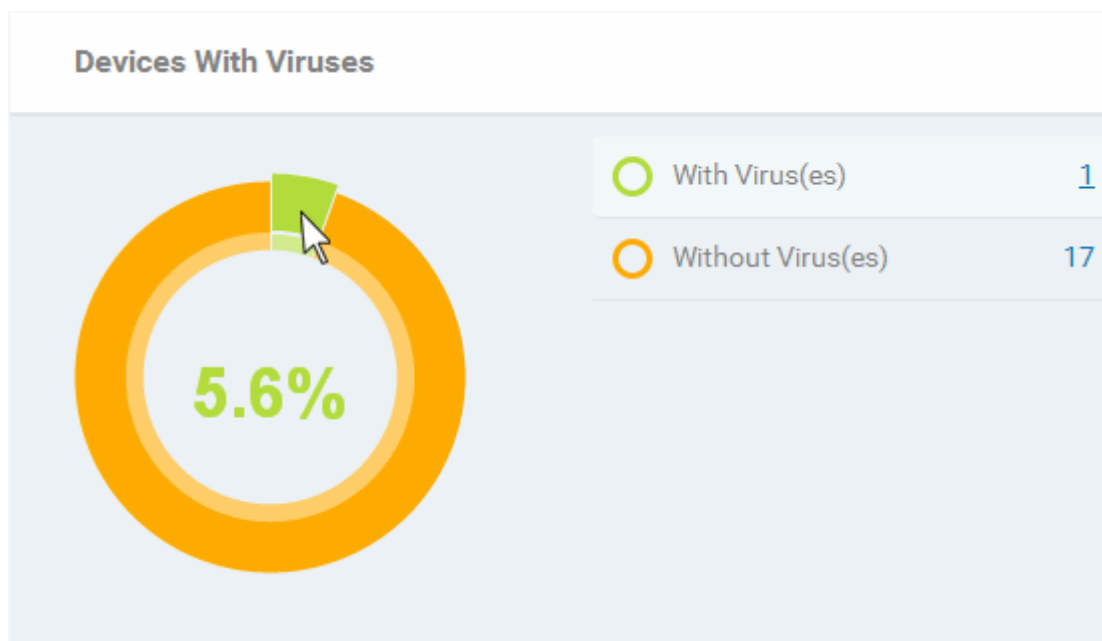
The pie-chart shows the summary of connectivity status of devices enrolled to CDM. In CDM, devices that are not connected for more than 20 minutes will be marked as inactive devices. Placing the mouse cursor over a sector or on the respective legend displays the details.



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

Devices With Viruses

The pie chart and the legend display the status of enrolled devices that are affected and not affected by viruses after a virus scan. Placing the mouse cursor over a sector or on the respective legend displays the details. Refer to the section '[Antivirus Scans](#)' for details about scanning for viruses on enrolled devices.

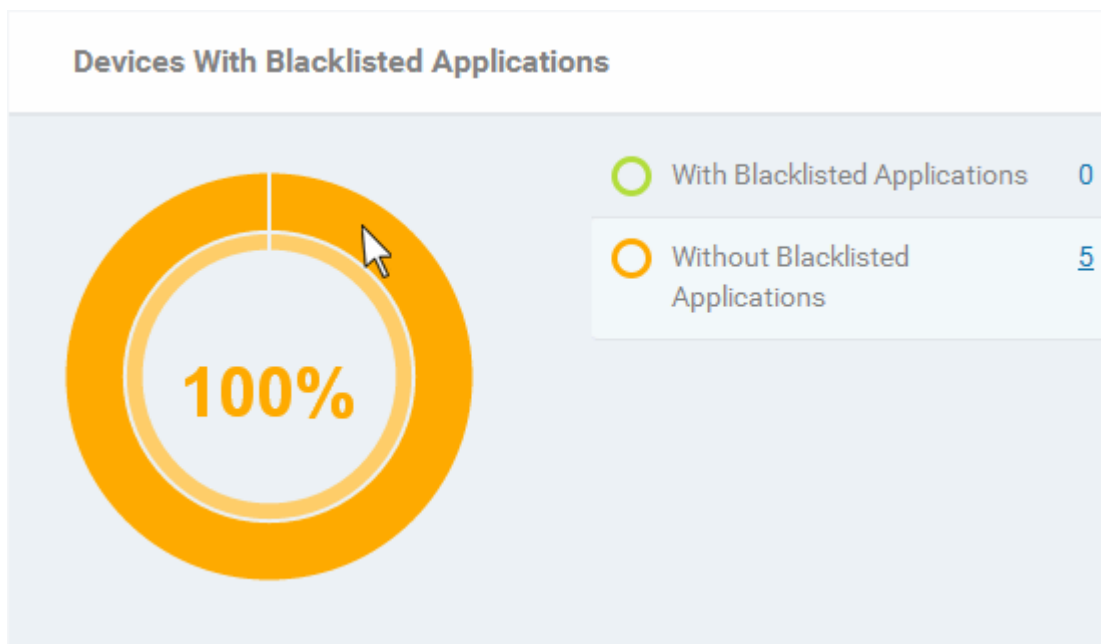


Clicking on any of the legend will open the respective 'Device List' page with a list of devices in respective category. For example, clicking on the 'With virus(es)' legend will open the 'Device List' with the list of devices identified with viruses. Refer to the section '[Devices](#)' for more details.

Devices with Blacklisted Application(s)

The pie chart and legend display the status of enrolled devices that have and do not have blacklisted applications in them.

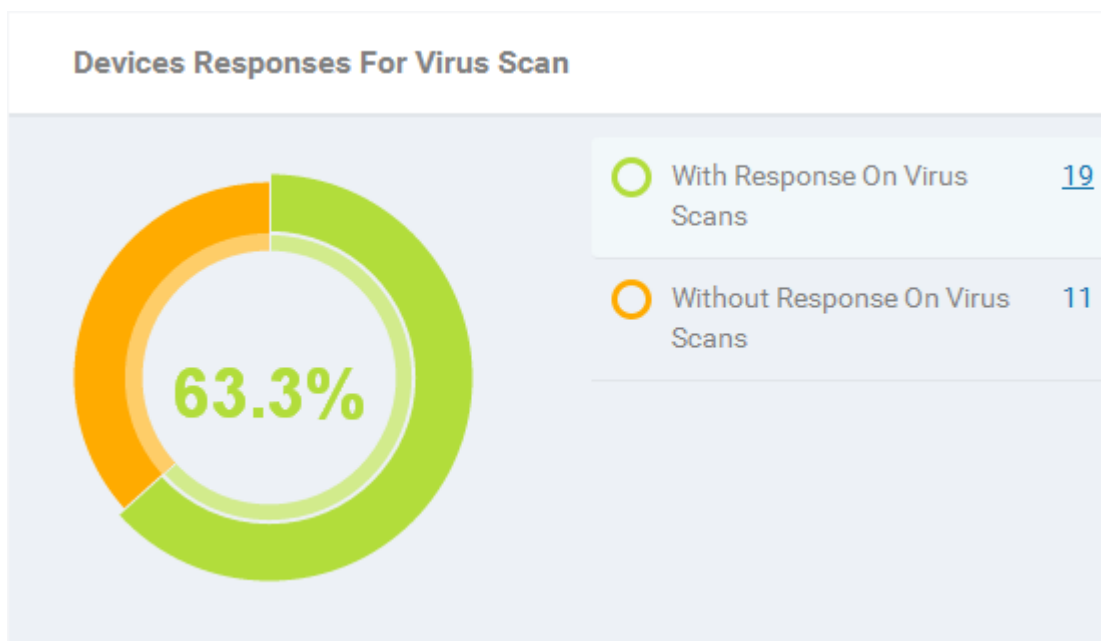
Placing the mouse cursor over a sector or on the respective legend displays the details. Refer to the section [Applications](#) for details about adding and removing apps from blacklist.



Clicking on any of the legend will open the respective 'Device List' page with a list of devices in respective category. For example, clicking on the 'With Blacklisted Applications' legend will open the 'Device List' with the list of devices identified with Blacklisted applications. Refer to the section [Devices](#) for more details.

Devices Responses for Virus Scan

The pie chart and legend display the status of enrolled devices that are responding and not responding to virus scans. Placing the mouse cursor over a sector or on the respective legend displays the details. Refer to the section [Antivirus Scans](#) for details about scanning for viruses on enrolled devices.

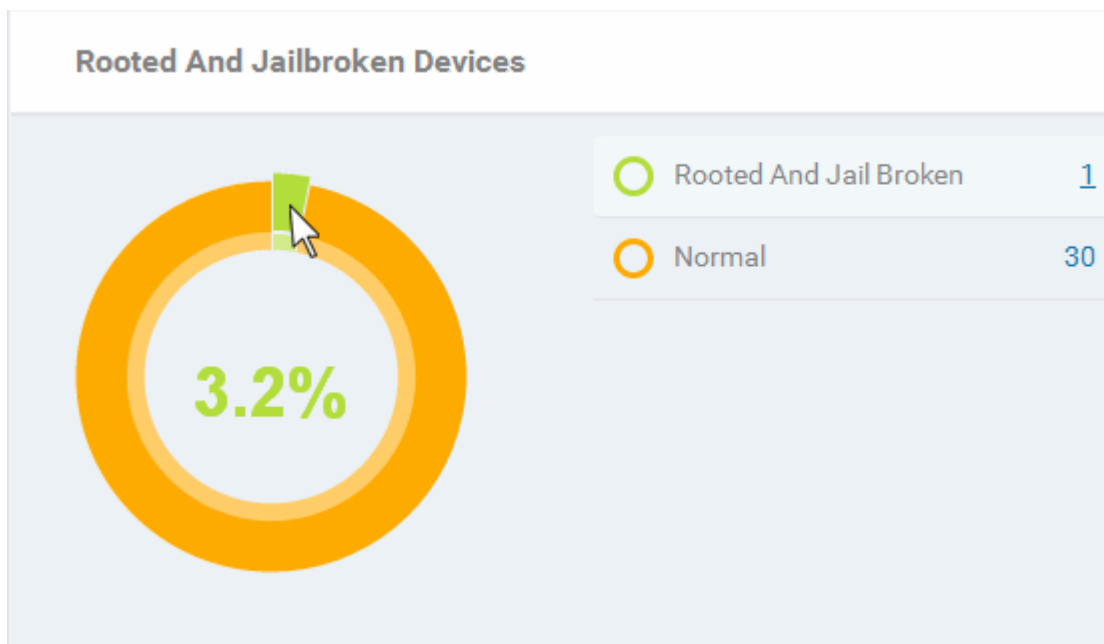


Clicking on any of the legend will open the respective 'Antivirus Device List' page containing list of devices in that category. For example, clicking on the 'With response on virus scan' legend will open the 'Antivirus Device List' page displaying the list of devices that are responding to scan command.

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

Rooted & Jailbroken Devices

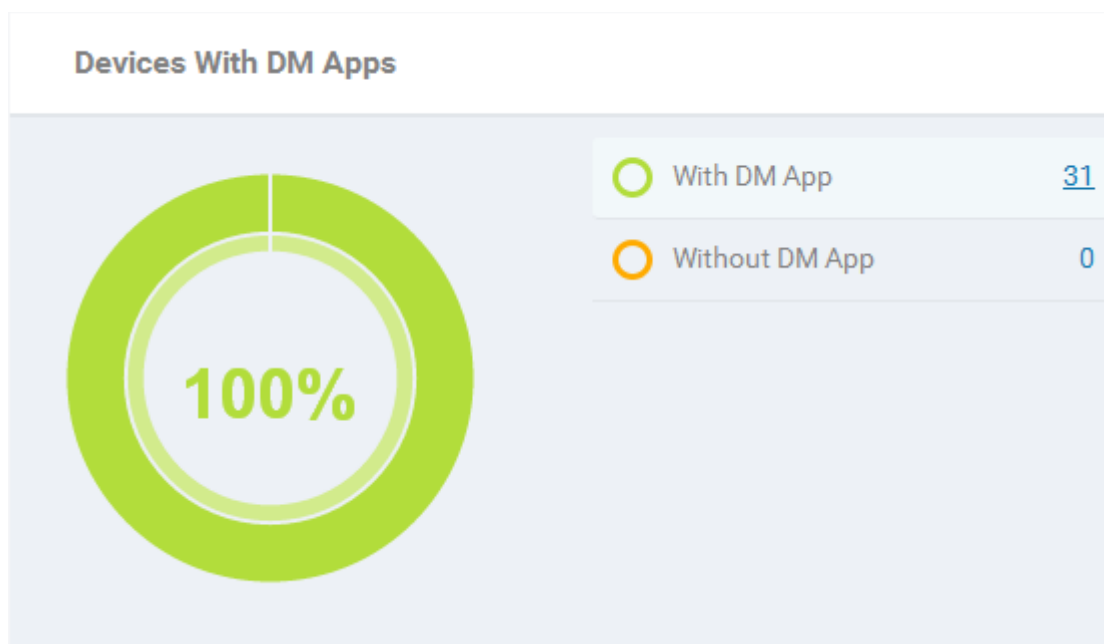
The pie chart and legend display the details of enrolled devices that are rooted and jailbroken. Placing the mouse cursor over a sector or on the respective legend displays the details.



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

Devices With DM Apps

The pie chart and legend displays the details of enrolled devices that have CDM app. iOS devices communicate with CDM server via the CDM profile that was installed during enrollment and do not require CDM app. Installing CDM app helps to enhance the functionality such as getting location details of the device, sending messages from the admin panel and so on. For Android and Windows devices, the devices can be enrolled only by using the CDM app. Placing the mouse cursor over a sector or on the respective legend displays the details.



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

Valkyrie

Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Administrators can take advantage of this service by applying a configuration profile to Comodo Endpoint Security which will automatically schedule unknown files for upload. All results will be displayed in the Valkyrie dashboard. For more details on configuring **Valkyrie Settings** in CDM, refer to **Creating Windows Profile**.

Note: The version of Valkyrie that comes with the free version of CDM is limited to the online testing service. The Premium version of CDM 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.

The screenshot shows the Valkyrie dashboard interface. On the left, a 'File Statistics' section features a donut chart with a 4.1% label. Below the chart is a legend with the following data:

Category	Count
Unrecognized	750
Sandboxed	34
Quarantined	3
Globally Trusted	21
Globally Blocked	18

The right-hand side of the dashboard, titled 'Valkyrie', contains a descriptive paragraph and two upgrade options:

- FREE basic** (with limited functionality): [Start subscription for FREE](#)
- PREMIUM** (with full functionality): [BUY Premium](#)

Below the premium option, there is a text input field for 'Valkyrie License key' and a [Submit](#) button.


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

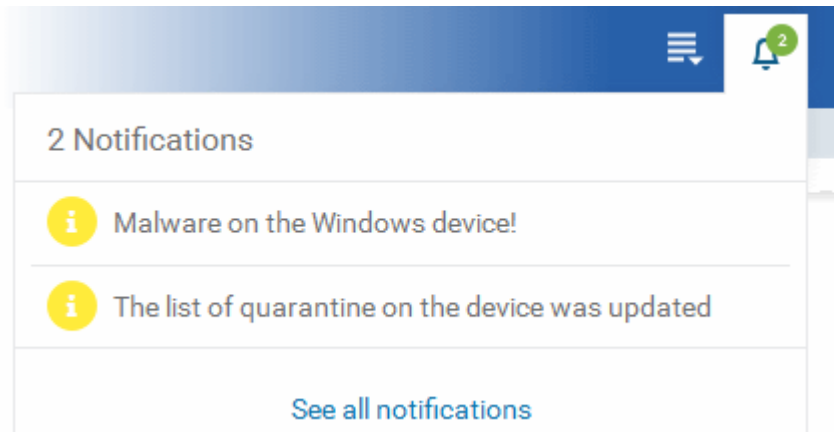
The right hand side pane allows you to upgrade to Premium version of CDM or to activate Valkyrie, if you have purchased the license separately.

Notifications

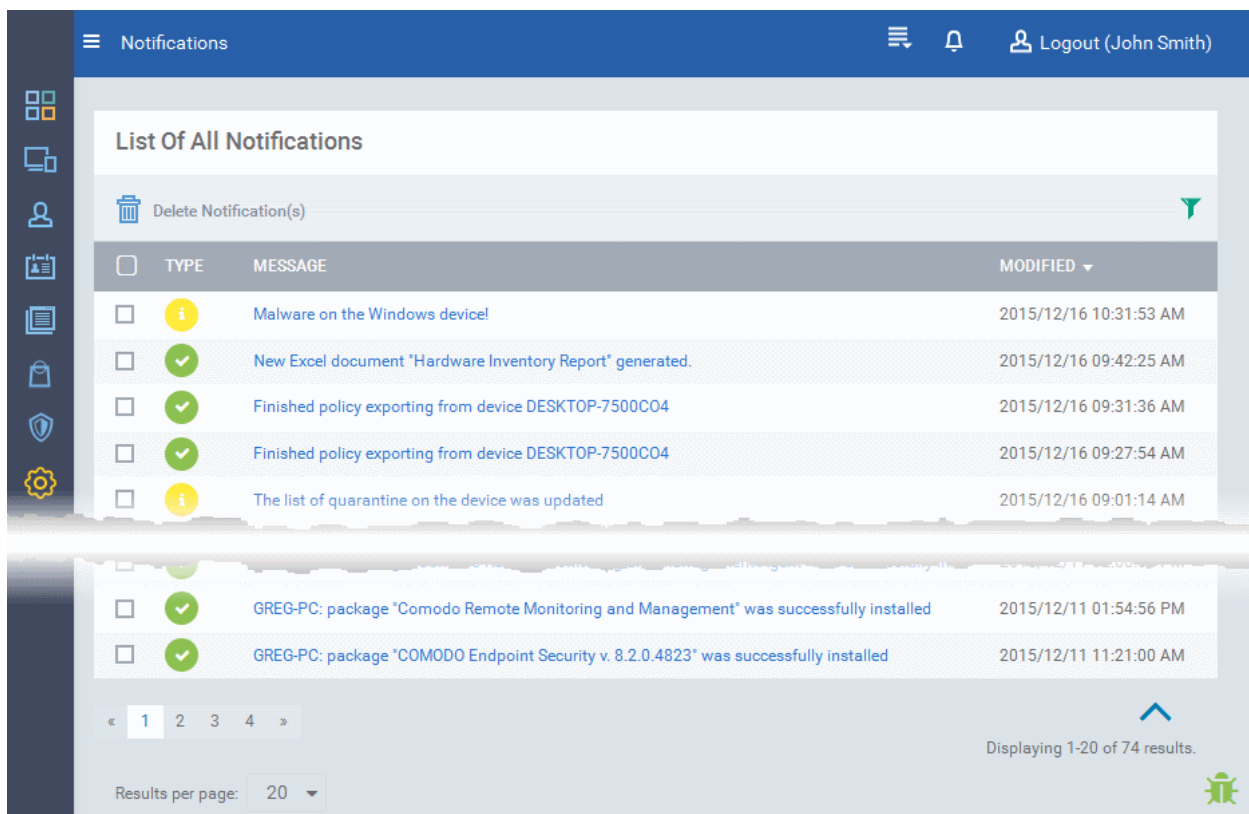
The 'Notifications' dashboard allows the administrator to view the notifications from CDM. CDM generates notifications on various events like:

- Installation of CES at a device
- Identification of malware on Android devices from realtime, scheduled scans and on-demand scans
- Identification of threats or malicious files and subsequently moving them to quarantine by CES installations at Windows endpoint.

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



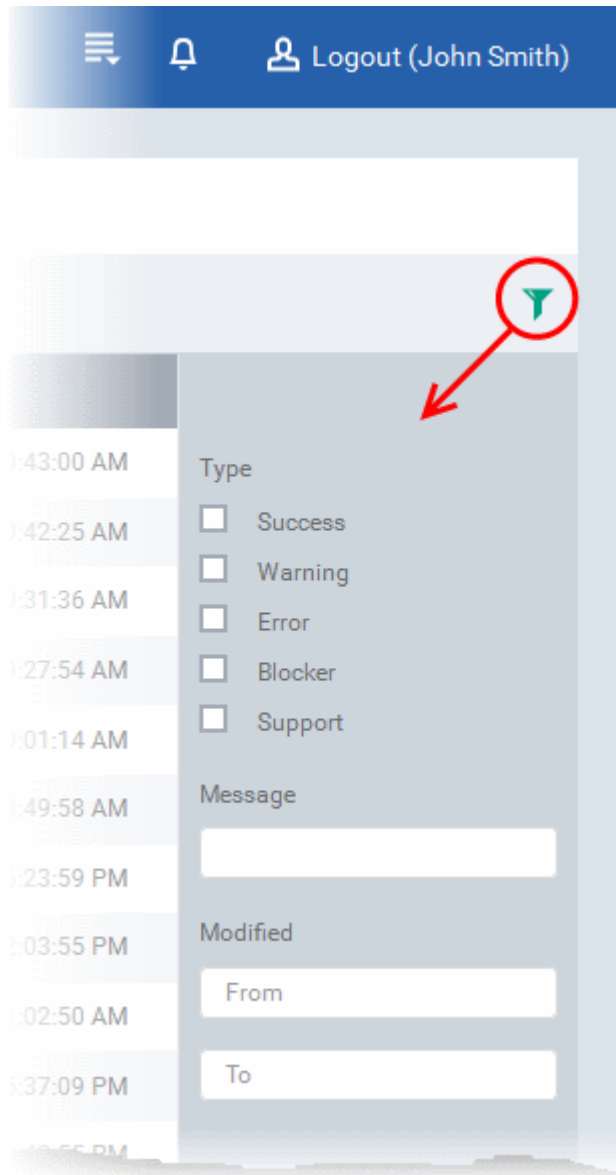
Tip: CDM is capable of sending notifications as emails. You can instruct CDM to send automated email notifications to selected administrators by configuring 'Email Notifications' under Settings. Refer to the section [Configuring Email Notifications](#).



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.
Modified	The date and time at which the notification was modified.

- The message also acts as a shortcut to view the details of the notification. Clicking on a message will open the interface relevant to the message for more details. For example, clicking on 'Malware Found on Windows device' message will open the 'Antivirus Current Malware List' screen with the list of malware identified.

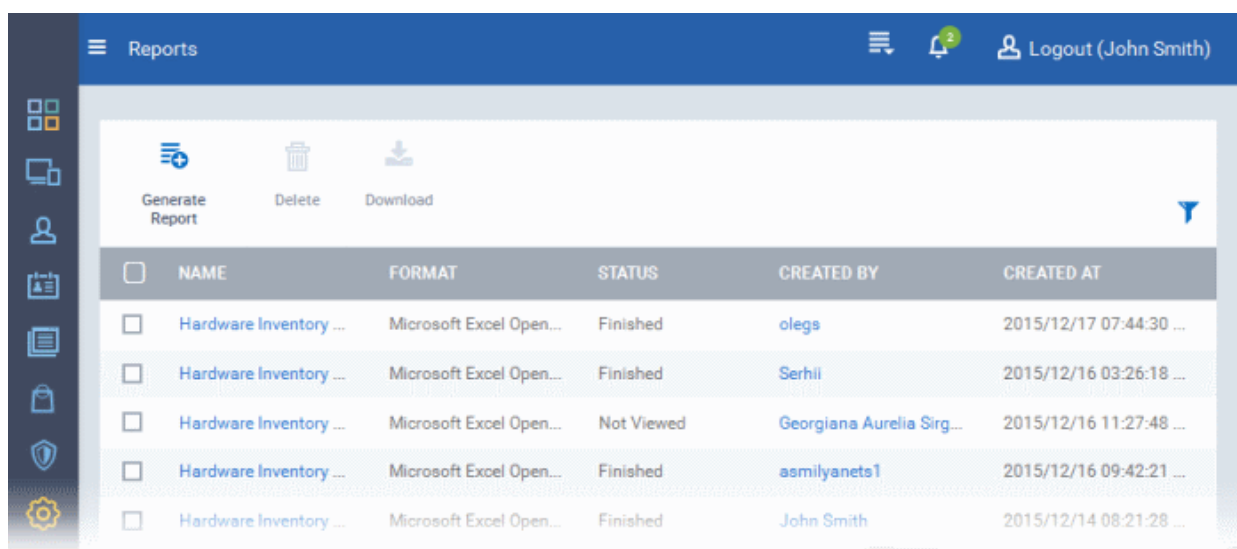
- To sort the filter in ascending/descending order of the date/time at which they were generated, click on the Modified column header.
- To filter or search for specific notification, click the funnel icon at the top right choose the notification type, enter the message to be searched in part or full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



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

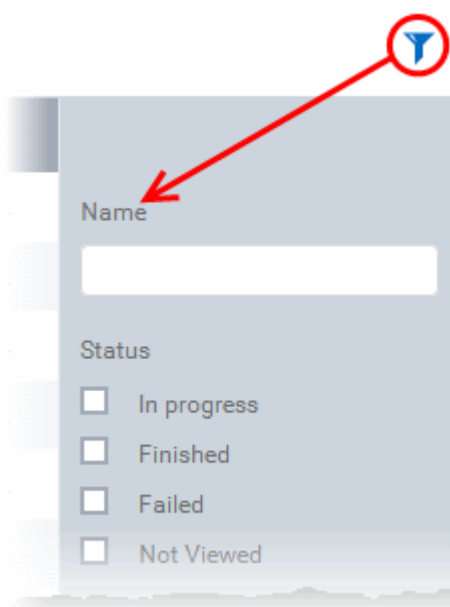
Reports

CDM is capable of generating reports of hardware inventory of managed devices in spreadsheet (.xls) format. The Reports interface under the Dashboard allows you to generate new reports and to view and download them.



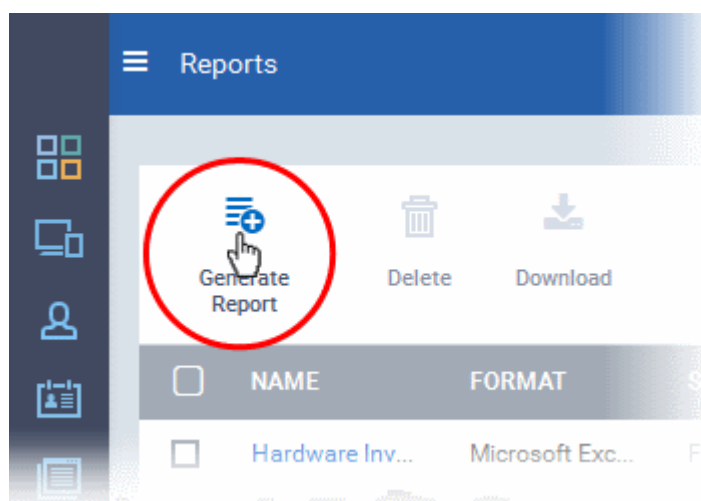
<input type="checkbox"/>	NAME	FORMAT	STATUS	CREATED BY	CREATED AT
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	olegs	2015/12/17 07:44:30 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	Serhii	2015/12/16 03:26:18 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Not Viewed	Georgiana Aurelia Sirg...	2015/12/16 11:27:48 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	asmilyanets1	2015/12/16 09:42:21 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	John Smith	2015/12/14 08:21:28 ...

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

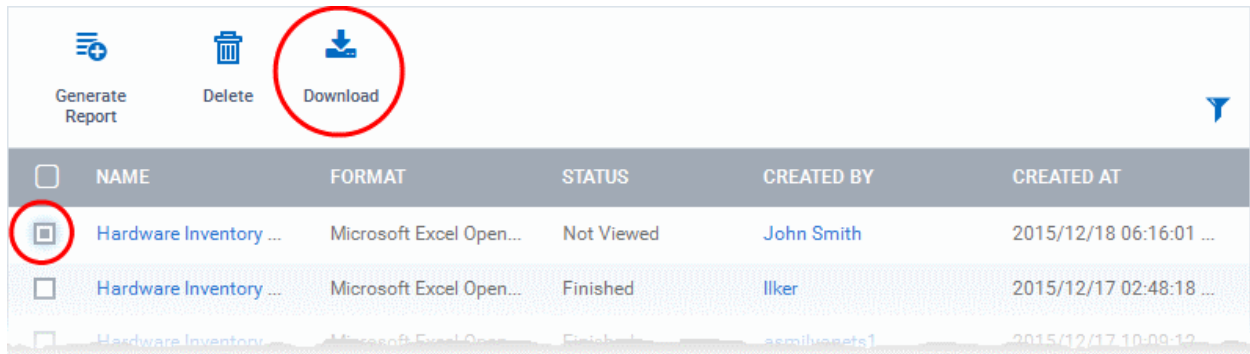


To generate a report

- Click 'Generate Report' from the top.

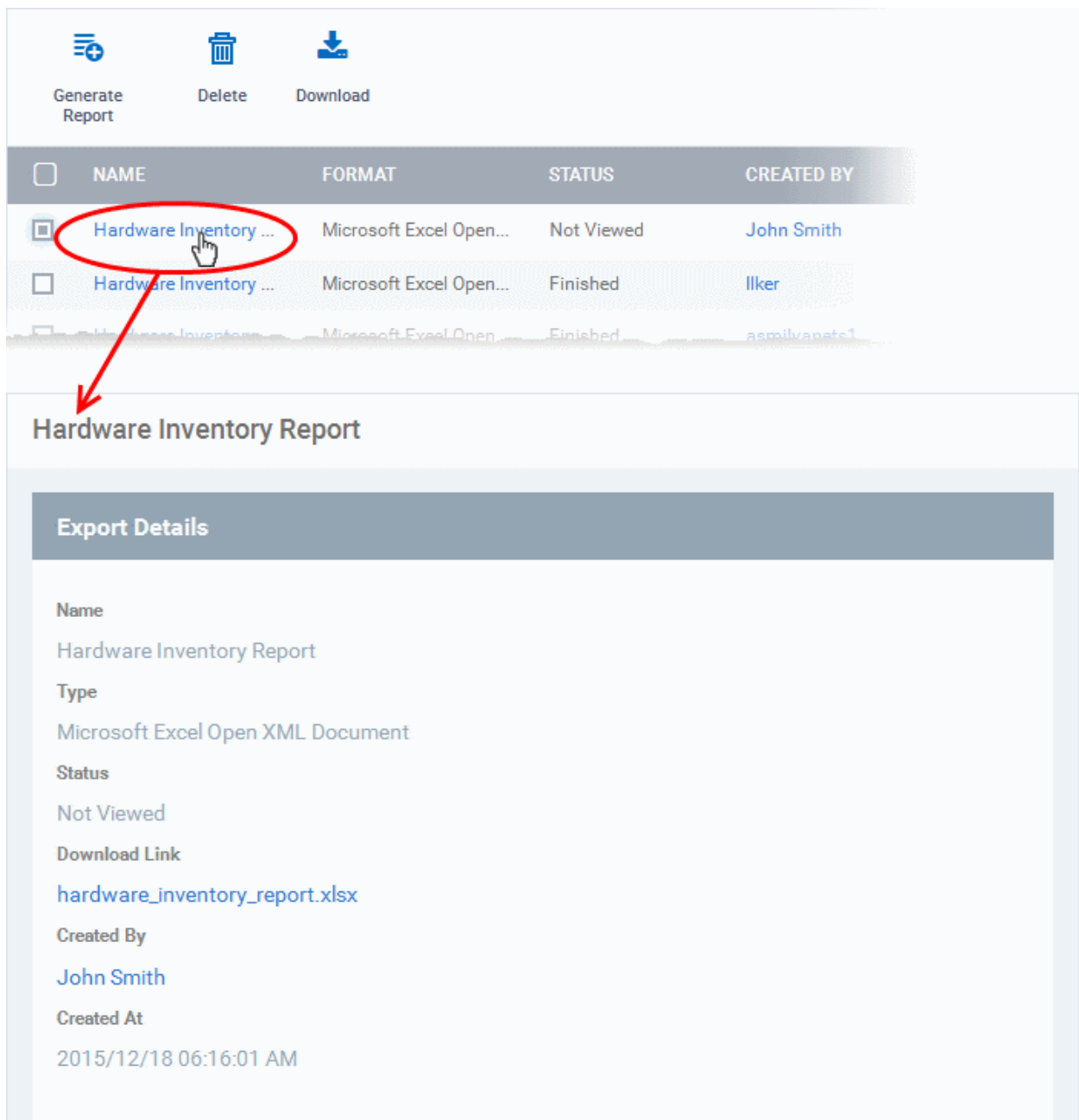


A new report will be generated.



<input type="checkbox"/>	NAME	FORMAT	STATUS	CREATED BY	CREATED AT
<input checked="" type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Not Viewed	John Smith	2015/12/18 06:16:01 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	Ilker	2015/12/17 02:48:18 ...
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	asmilyanets1	2015/12/17 10:09:12 ...

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



<input type="checkbox"/>	NAME	FORMAT	STATUS	CREATED BY
<input checked="" type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Not Viewed	John Smith
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	Ilker
<input type="checkbox"/>	Hardware Inventory ...	Microsoft Excel Open...	Finished	asmilyanets1

Hardware Inventory Report

Export Details

Name
Hardware Inventory Report

Type
Microsoft Excel Open XML Document

Status
Not Viewed

Download Link
[hardware_inventory_report.xlsx](#)

Created By
[John Smith](#)

Created At
2015/12/18 06:16:01 AM

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

4. Users and User Groups

One of the first steps in setting up Comodo Device Manager is to add users. Once users have been added, you can enroll iOS, Android or Windows devices associated with that user. Once user devices have been enrolled, administrators can apply security profiles, run antivirus scans, remotely manage and obtain reports from them. Administrators can also create user groups and apply device actions/profiles to all users in the group.

Click the 'Users' link on the left to create and manage users and user groups:

	USERNAME	EMAIL	PHONE NUMBER	LAST LOGIN	# OF DEVICES
<input type="checkbox"/>	SAS	test.mdm.ode...	12345678	2016/01/15 0...	6
<input type="checkbox"/>	John Smith	fiatlena@gm...		2016/01/18 0...	3
<input type="checkbox"/>	Sviatoslav	test.mdm.ode...	+320565454	2016/01/15 0...	3
<input type="checkbox"/>	Serhii	test.mdm.ode...	+32165449887	2016/01/15 1...	3
<input type="checkbox"/>	CmenaH	test.mdm.ode...	12345678	2016/01/15 0...	2
<input type="checkbox"/>	greg	test.mdm.ode...		2016/01/17 0...	2
<input type="checkbox"/>	makazov	maxim.guzee		2016/01/15 1	2

The following sections explain more about each area:

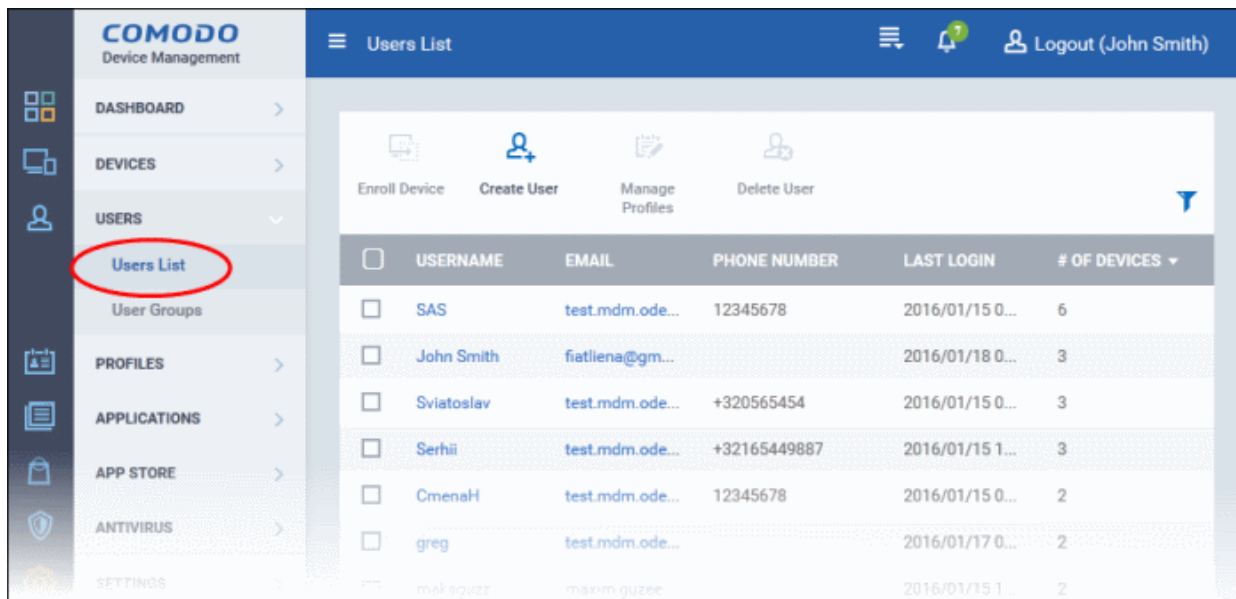
- **Managing Users**
 - **Creating New User Accounts**
 - **Enrolling Users' Devices for Management**
 - **Viewing the Details of a User**
 - **Assigning Configuration Profile(s) to a Users' Devices**
 - **Removing a User**
- **Managing User Groups**
 - **Creating a New User Group**
 - **Editing a User Group**
 - **Assigning Configuration Profile to a User Group**
 - **Removing a User Group**

4.1. Managing Users

Administrators can enroll user accounts to CDM 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 CDM.


The 'Users' interface displays a list of user accounts that are enrolled to CDM 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 'Users' interface, click the 'Users' tab on the left and select 'Users List'



Users List Table - Column Descriptions	
Column Heading	Description
Username	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.
Phone Number	The registered phone number of the user.
Last Login	Indicates the date and time of the users last login session.
# of Devices	Indicates the remaining number of devices that can be enrolled for the user.

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 CDM 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](#)
- [Viewing the Details of a User](#)
- [Updating the Details of a User and Resetting Password](#)
- [Assigning Configuration Profile\(s\) to a Users' Devices](#)
- [Removing a User](#)

4.1.1. Creating New User Accounts

The 'Users List' interface allows the administrator to create new administrator and end-user accounts. After a user is created, an enrollment mail will be sent to them which requests them to activate their account and set their account password.

CDM also allows administrators to bulk enroll users and Windows endpoints via Active Directory (AD) group policy. Please refer to the sections '[Downloading CDM Installation Packages for Windows Devices](#)' and '[Importing User Groups from LDAP](#)' for more details. This section explains how to enroll users from the 'Users List' interface.

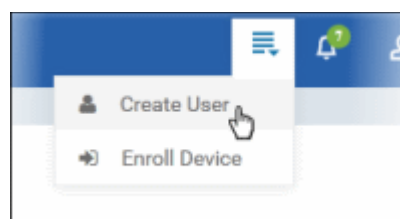
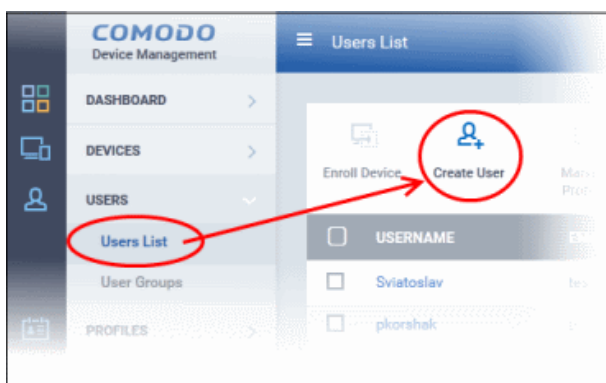
Important Note: User device(s) can only be enrolled after the user has been added to the system.

Each user license covers up to five mobile devices or one Windows endpoint for a single user (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows endpoint). If more than 5 devices or 1 endpoint are added for the same user, then an additional user license will be consumed. 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' > 'Users List' then click the 'Create User' button
- or
- Choose 'Create User' from the menu button at the top right:



The 'Create new user' form will open:

Create new User
Close

Username *

Email *

Phone number

Company *

Assign role

'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	<ul style="list-style-type: none"> Comodo One Users - The drop-down will display the companies added to C1. You can choose the company to which the user belongs. The user will be enrolled under the chosen company. CDM users - Leave the selection as 'Default Company'.
Assign role	Drop-down	<p>Select the role to be assigned to the new user from the 'Assign role' drop-down.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Assign role</p> <input type="text" value="Users"/> <ul style="list-style-type: none"> Users Administrators Users </div> <p style="text-align: right;"><input type="submit" value="Submit"/></p> <p>CDM ships with two default roles:</p> <ul style="list-style-type: none"> Administrators - Can login to the CDM administrative interface and access all management interfaces. Users - The users or owners of Android, iOS and Windows devices. Users cannot login to the administrative console by default.

'Create new user' Form - Table of Parameters		
		You can create custom roles with access to selected areas of the administrative console and can assign them to users as required. All the roles created in CDM will appear in the 'Assign Role' drop-down for selection, while adding a new user. Refer to the section Configuring Role Based Access Control for Users for more details.

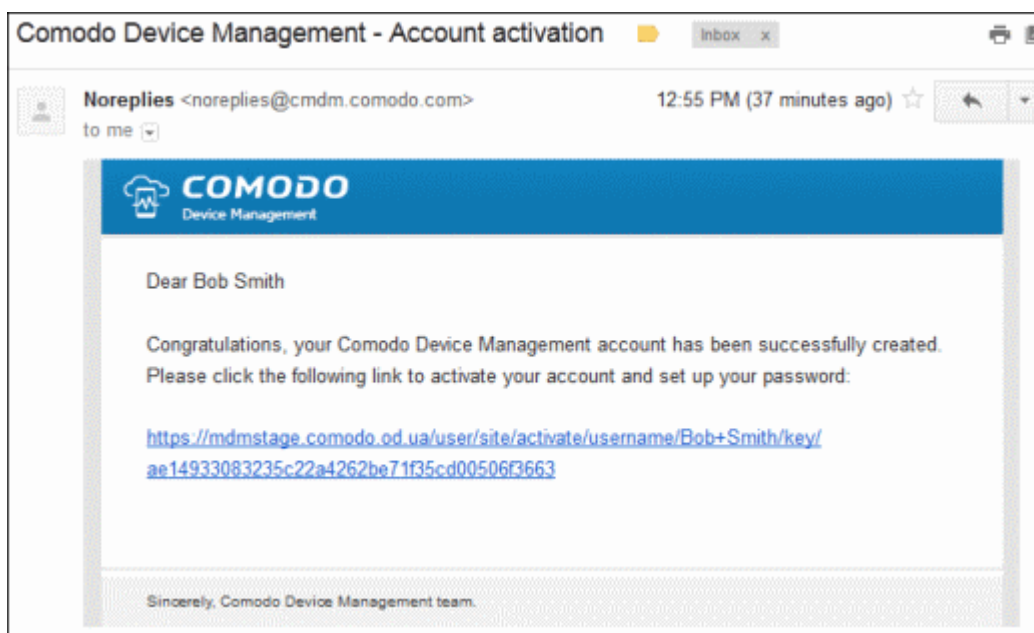
- Enter the details, select the role for the new user and click the 'Submit' button.

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

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

- Repeat the process to add more users.

Account activation mails are sent to new administrators and users assigned to a role with admin console privileges. They can activate their account and set their login password by clicking the link in the email. An example mail is shown below:



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

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

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

4.1.2. Enrolling User Devices for Management

In order to centrally manage mobile/laptop/desktop devices, each device needs to be enrolled to Comodo Device Manager (CDM). 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.

CDM 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 CDM and creating a software installation group policy for their Active Directory (AD) server. Please refer to the sections '**Downloading CDM**

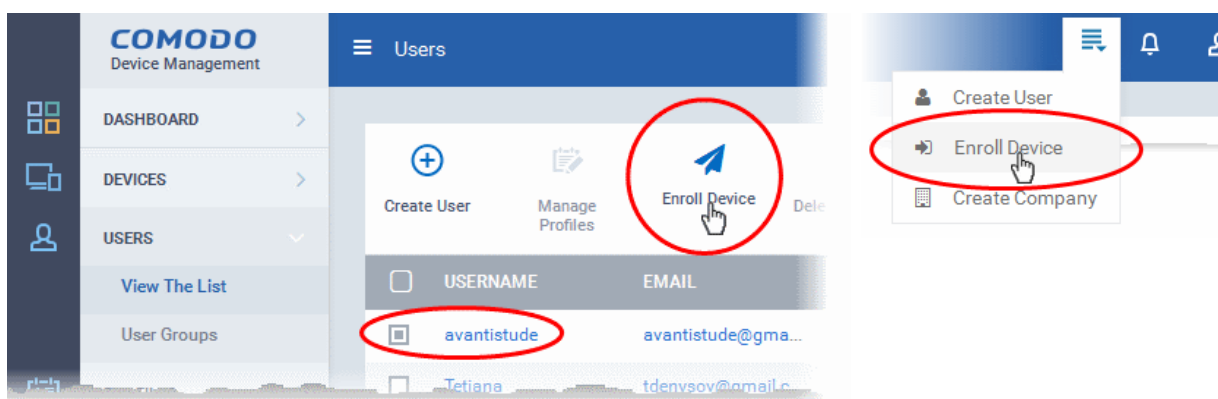
Installation Packages for Windows Devices and **'Importing User Groups from LDAP'** for more details. This section explains how to enroll users' devices from the 'Users List' interface.

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

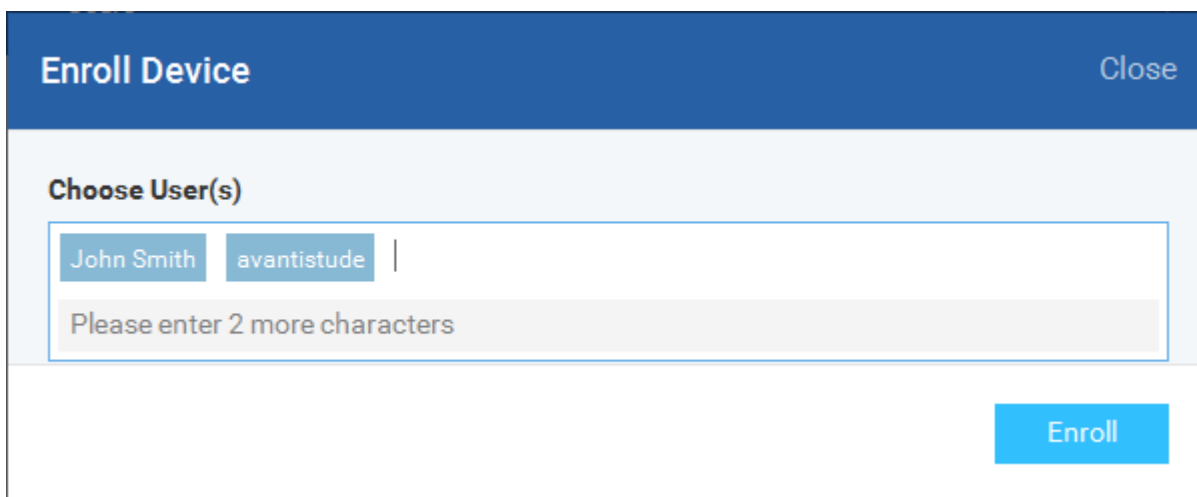
Refer to the section **Viewing and Managing Licenses** for more details.

To enroll devices

- Click 'Users' > 'Users List' from the left
- Select users for whom you want to enroll devices and click the 'Enroll Device' button above the table
- Or
- Choose 'Enroll Device' from the drop-down at the top right



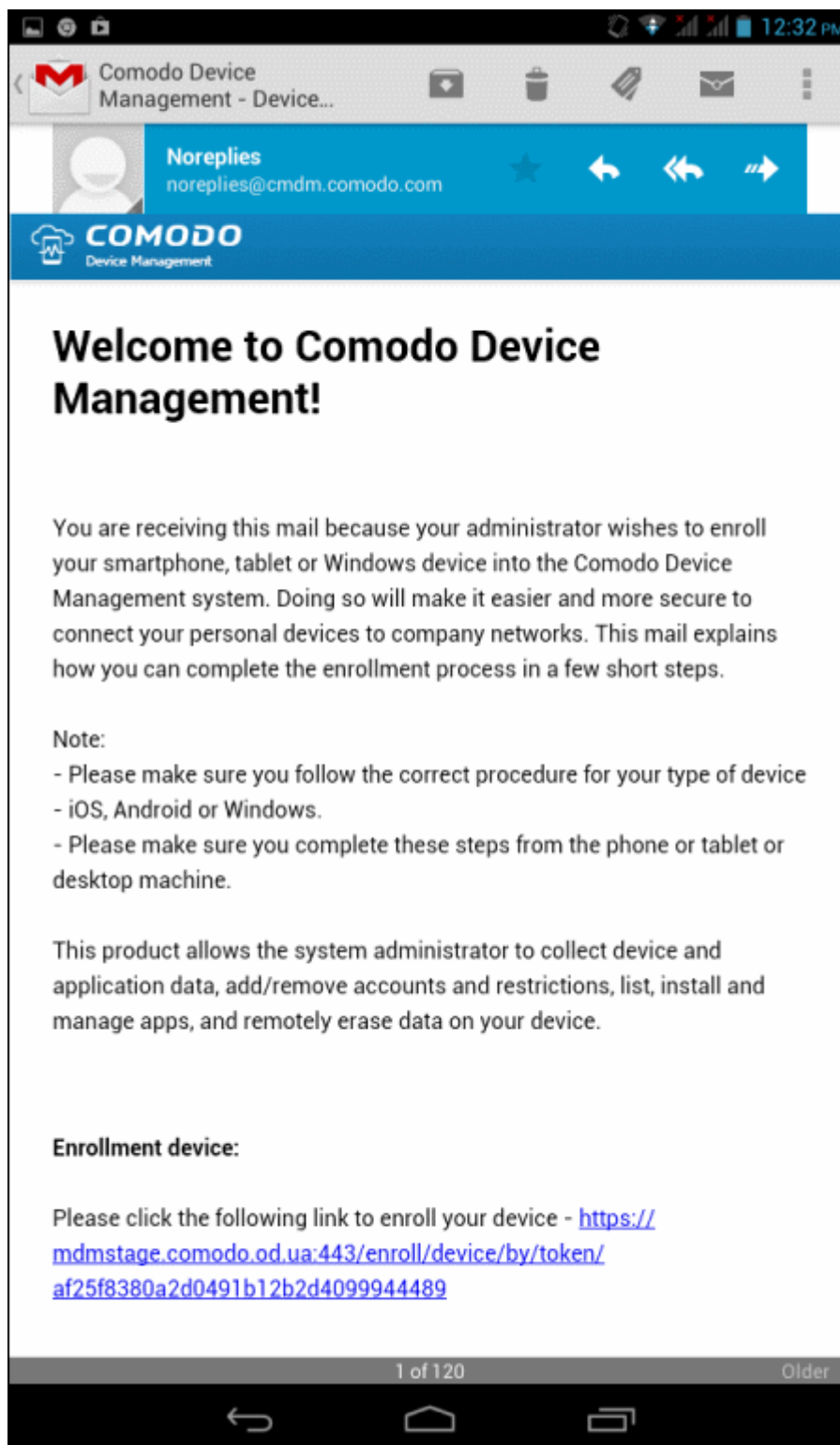
The 'Enroll Device' dialog will open for the chosen users.



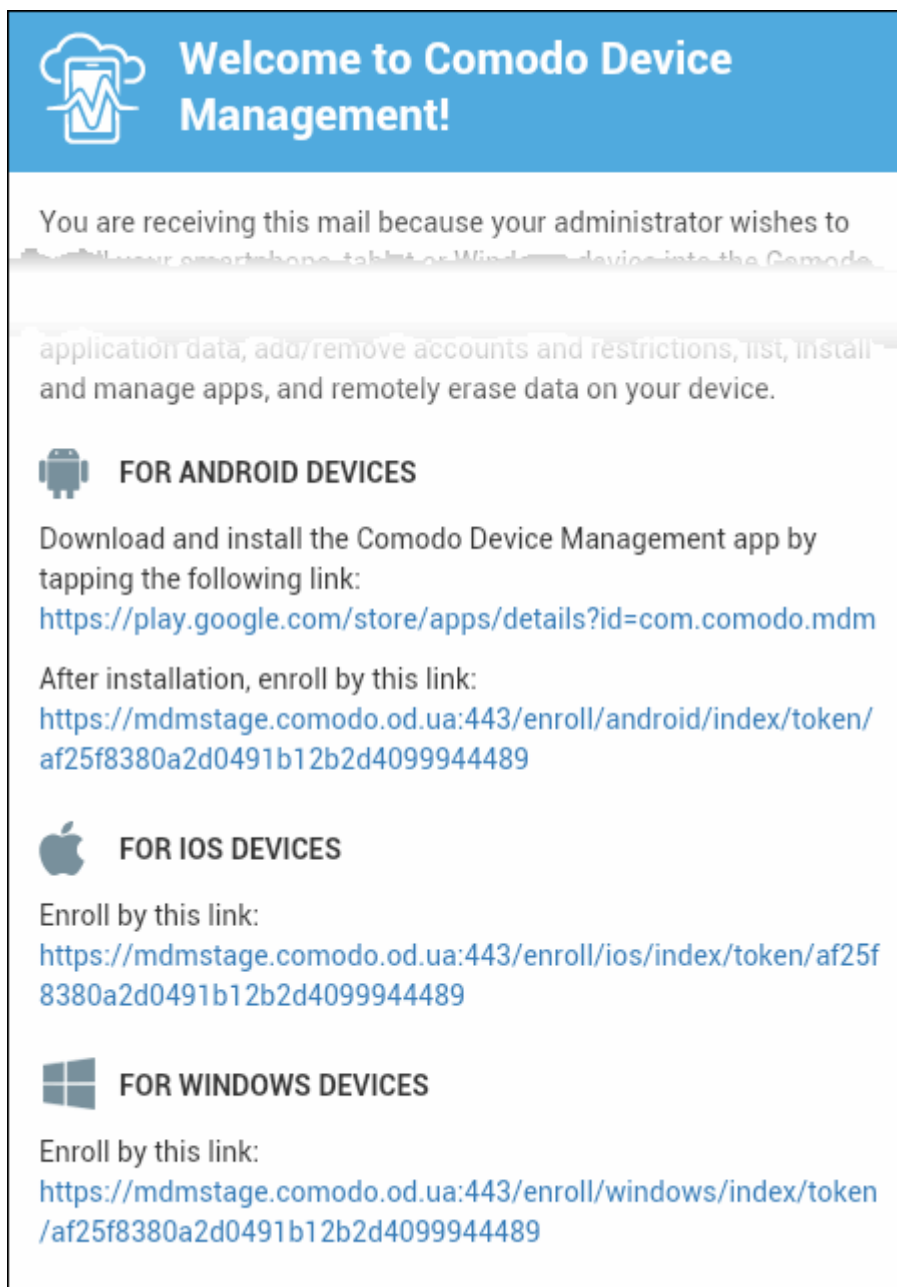
The 'Choose Users' field is pre-populated with the users you selected in the 'Users List' interface.

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

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 CDM agent/profile for the device. An example mail is shown below.



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

A screenshot of a welcome email from Comodo Device Manager. The email has a blue header with a white icon of a smartphone with a pulse line and the text "Welcome to Comodo Device Management!". The main body of the email is white with a light blue background. It contains the following text: "You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Manager application. This application allows you to view application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device." Below this, there are three sections: "FOR ANDROID DEVICES" with an Android icon, "FOR IOS DEVICES" with an Apple icon, and "FOR WINDOWS DEVICES" with a Windows icon. Each section provides a link to download the app and a link to enroll the device.

Welcome to Comodo Device Management!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Manager application. This application allows you to view application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR ANDROID DEVICES

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

After installation, enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/android/index/token/af25f8380a2d0491b12b2d4099944489>

FOR IOS DEVICES

Enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/ios/index/token/af25f8380a2d0491b12b2d4099944489>

FOR WINDOWS DEVICES

Enroll by this link:
<https://mdmstage.comodo.od.ua:443/enroll/windows/index/token/af25f8380a2d0491b12b2d4099944489>

The following sections explain more on:

- [Enrolling Android Devices](#)
- [Enrolling iOS Devices](#)
- [Enrolling Windows Endpoints](#)

4.1.2.1. Enrolling Android Devices

After the administrator has added devices for a user, the user will receive an enrollment email with a link to a page containing the enrollment instructions and links to download the android CDM agent and to configure it. The user should open the email in the Android device to be enrolled and follow the instructions. The Android device enrollment involves two steps.

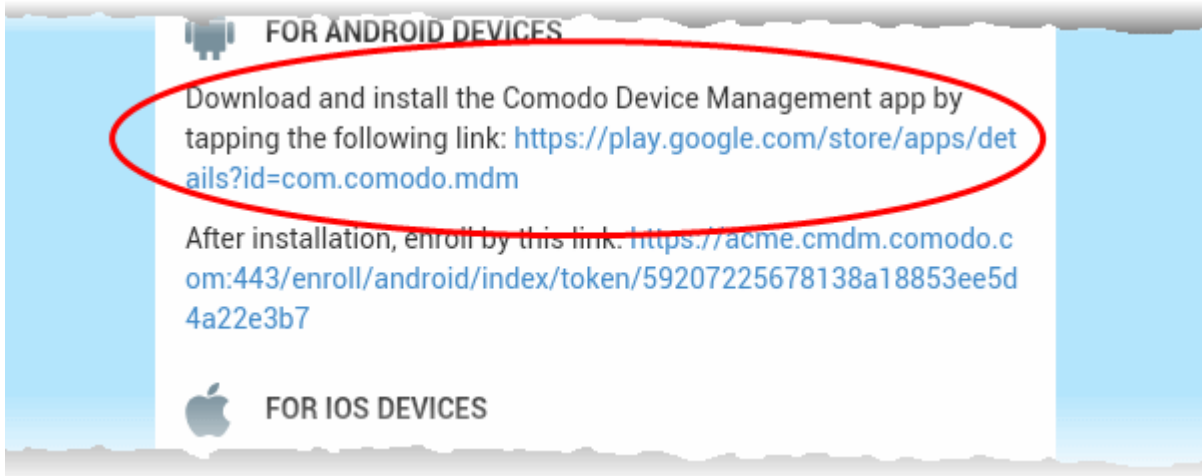
- [Step 1 - Downloading and Installing the agent](#)
- [Step 2 - Configuring the agent](#)

[Step 1 - Downloading and Installing the agent](#)

- Open the mail in the device and tap the enrollment link in it. You will be taken to the enrollment page through your

browser in the device.

- Tap the first link under 'For Android Devices'



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

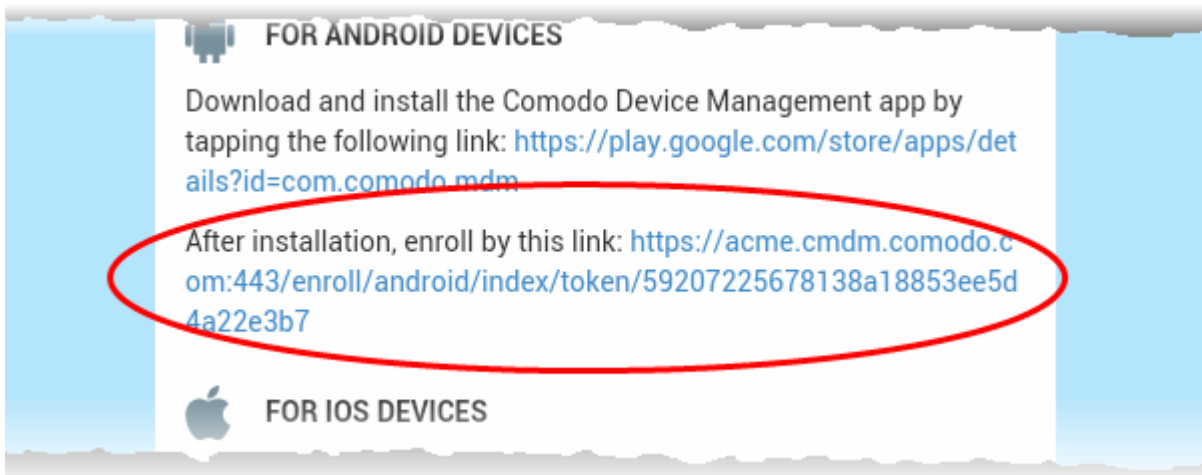
Step 2 - Configuring the agent

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

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

Automatic Configuration

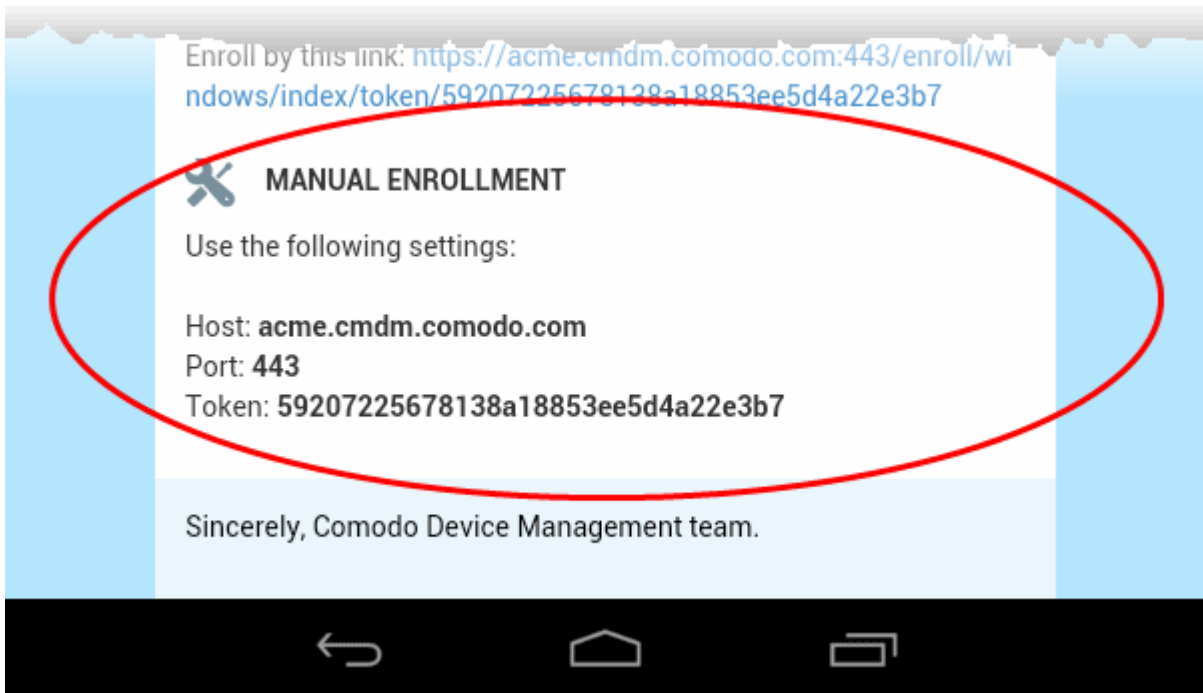
- Tap the enrollment link contained in the enrollment page after the completion of installation.



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

Manual Configuration

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



To manually configure the agent

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

Server Settings

A screenshot of the "COMODO Server Settings" configuration screen on a mobile device. The screen has a blue header with the Comodo logo and the text "COMODO Server Settings". Below the header, there are two input fields: "Server URL" and "Server port". Both fields are currently empty. At the bottom of the screen, there is a large blue button labeled "Connect". The top of the screen shows the status bar with icons for signal, Wi-Fi, and battery, and the time "12:19 pm".

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

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

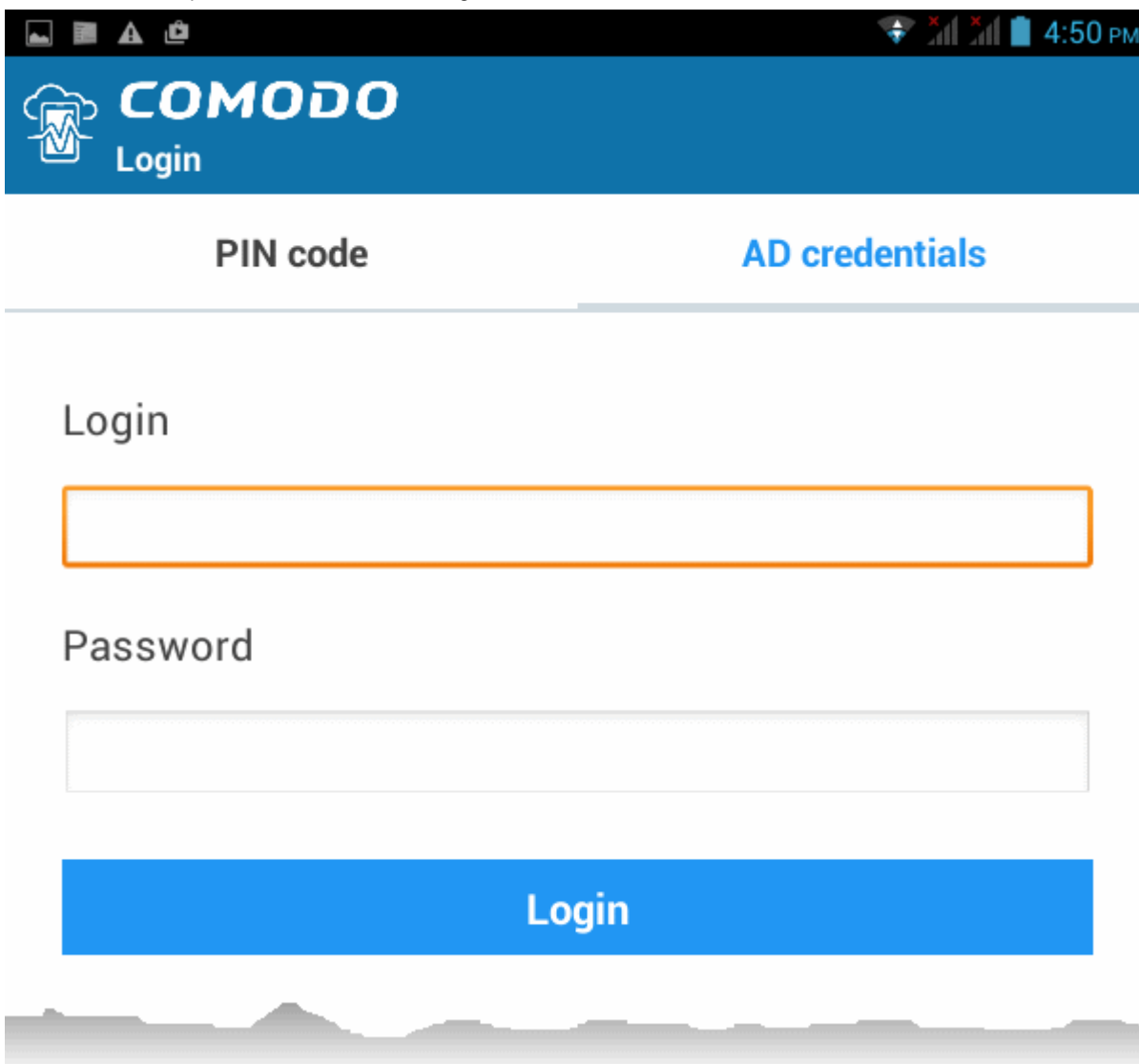
Logging-in to the Console

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

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

Entering PIN

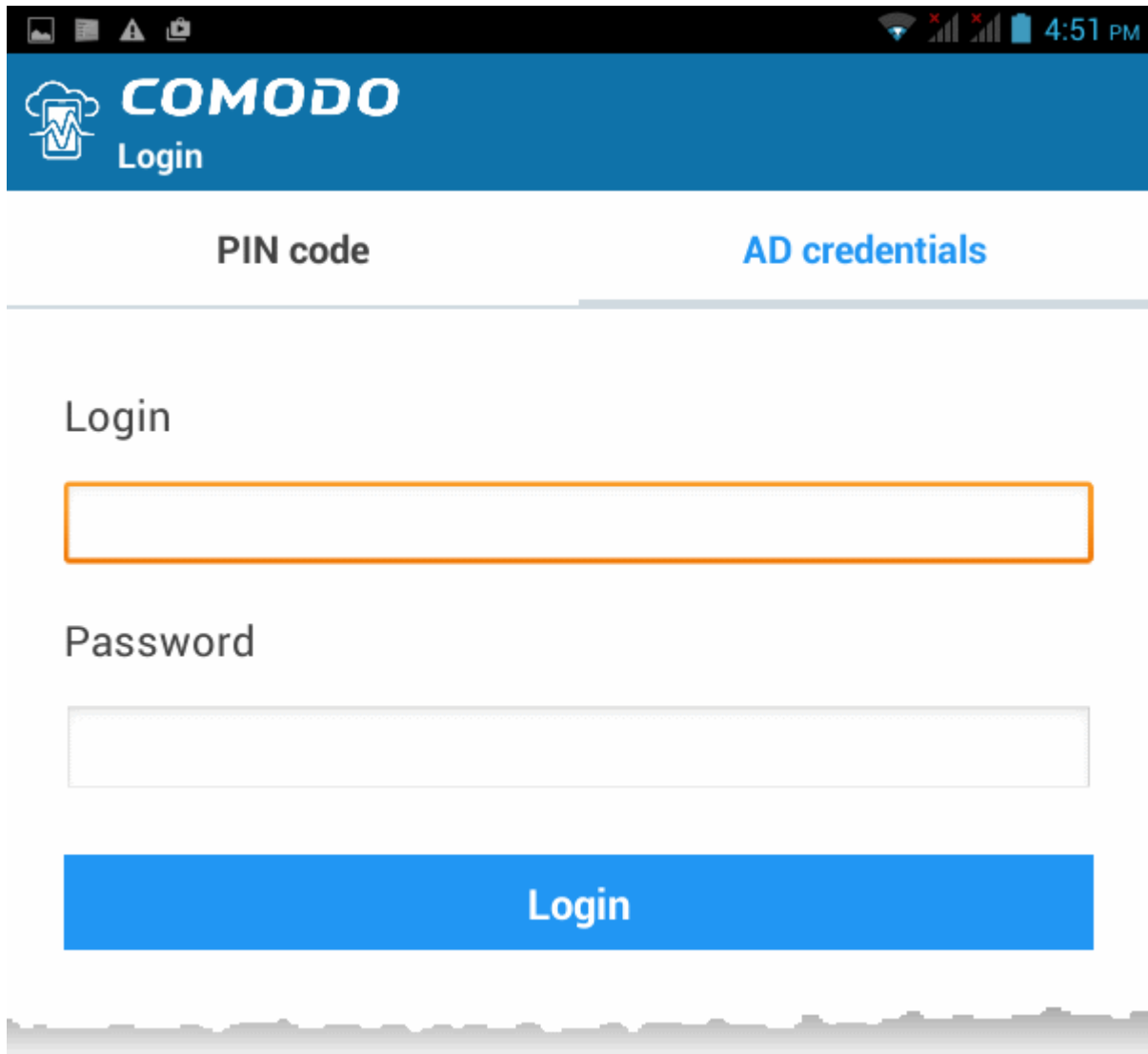
- Tap the 'Pin Code' tab in the 'Login' screen



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

Entering your username and password

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



The screenshot shows a mobile application interface for logging into Comodo Device Manager. At the top, there is a blue header with the Comodo logo and the word 'Login'. Below the header, there are two tabs: 'PIN code' and 'AD credentials'. The 'AD credentials' tab is selected and highlighted in blue. Underneath the tabs, there is a 'Login' label, followed by an empty text input field for the username. Below that is another empty text input field for the password. At the bottom of the form is a large blue button with the word 'Login' in white text. The background of the screen is white with a subtle grey cityscape silhouette at the bottom.

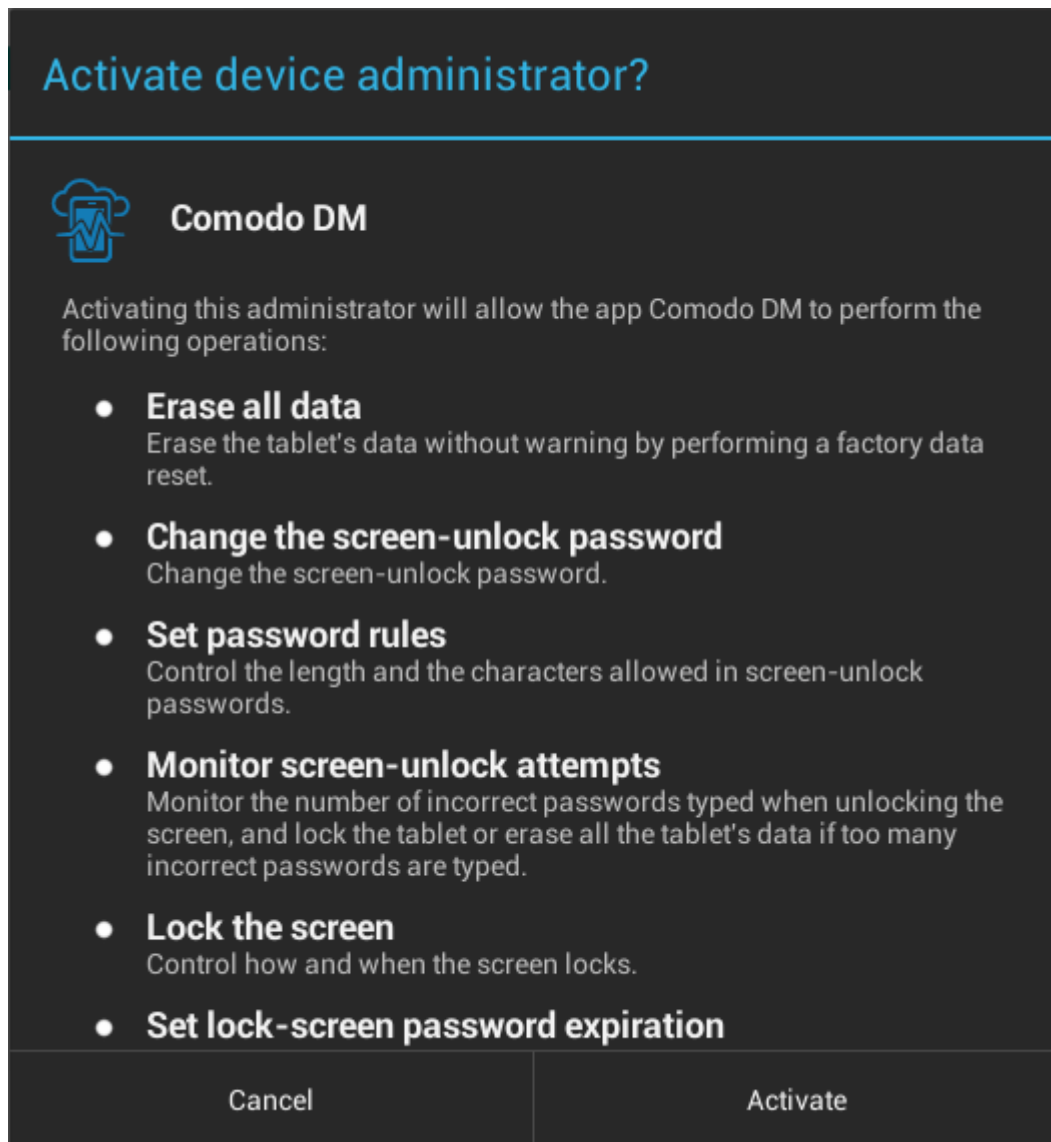
- Enter your username contained in your account activation email and the password you set for your CDM account.
- Tap the 'Login' button

End User License Agreement

The EULA screen will appear.

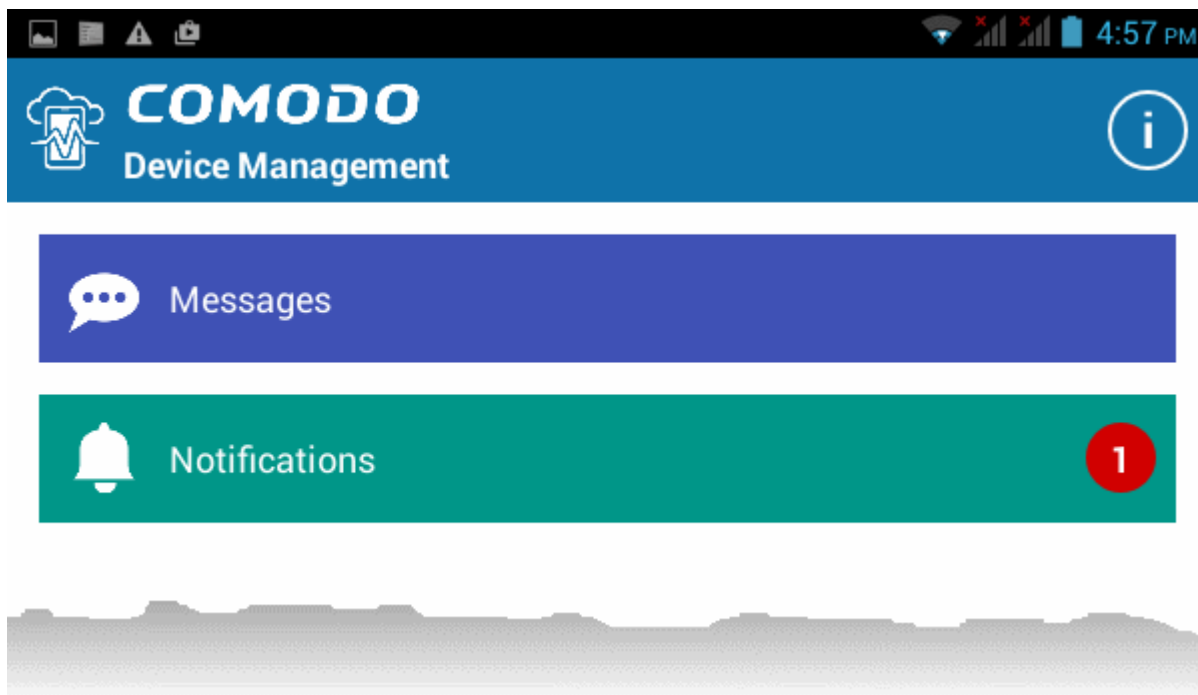


- Scroll down the screen, read the EULA fully and click the 'I ACCEPT' button at the bottom. The Agent activation screen will appear.



- Tap 'Activate'.

The CDM agent home screen will appear.



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

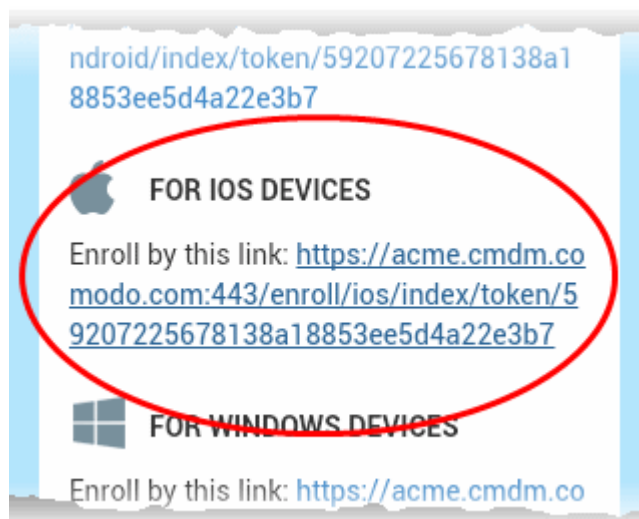
4.1.2.2. Enrolling iOS Devices

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

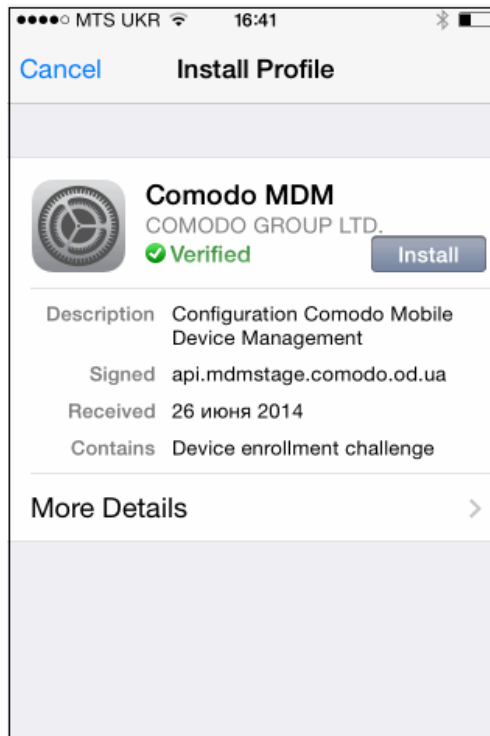
Note: The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

To enroll an iOS device

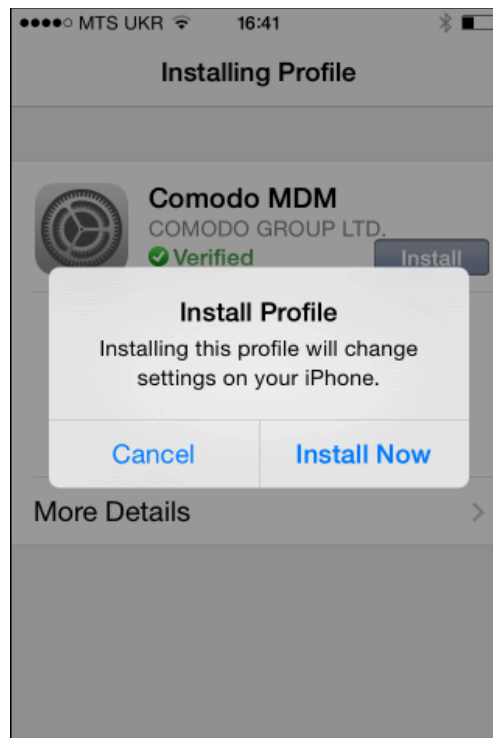
- Open the mail in the device and tap the enrollment link in it. You will be taken to the enrollment page through your browser in the device.
- Tap the enrollment link under "For IOS Devices"



The 'Install Profile' wizard will start.

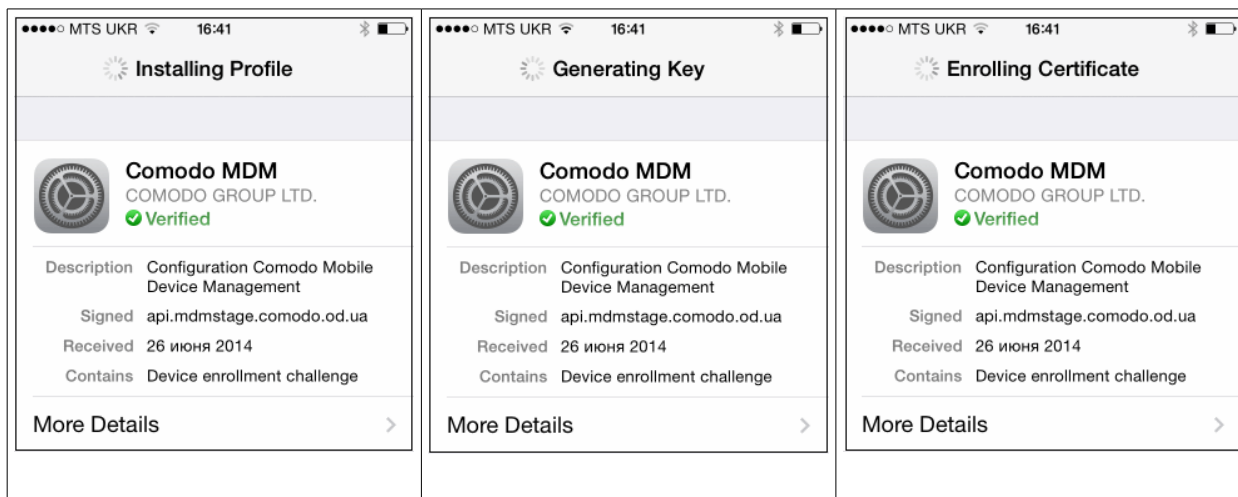


- Tap 'Install'. A confirmation dialog will be displayed.

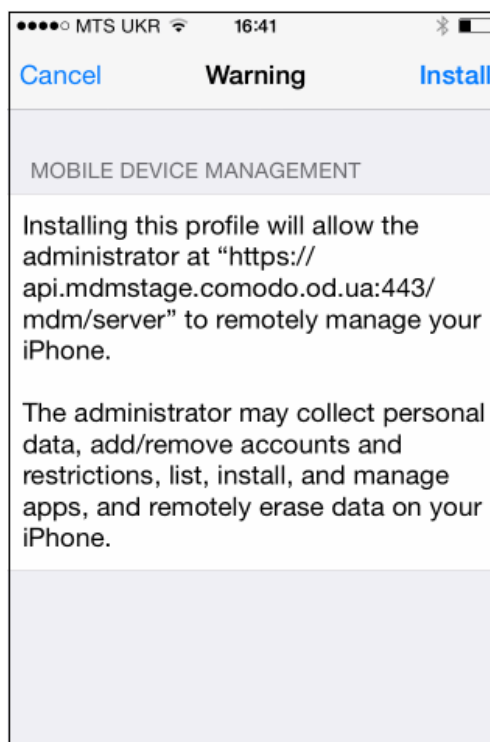


- Tap 'Install Now'.

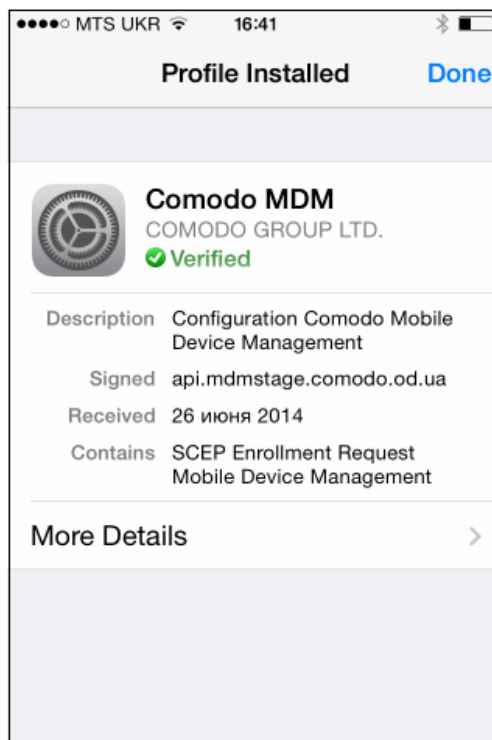
The CDM Profile installation progress will be displayed.



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



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



- Tap 'Done' to finish the Comodo DM profile installation wizard.

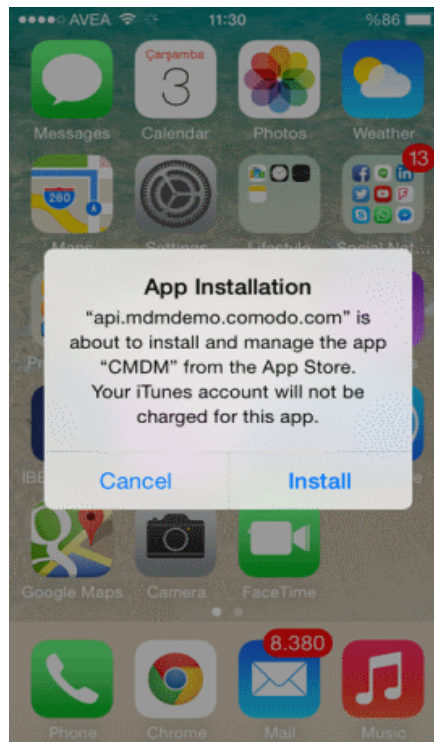
You can view the CDM profile listed in the profiles screen of the device.

4.1.2.2.1. Downloading and Installing CDM Client for iOS Devices

The iOS devices enrolled into CDM for management as explained in the previous section '[Enrolling iOS Devices](#)' do not support some features such as apps management, GPS location and messaging. To get full functionality, users need to download CDM client from iTunes website at <https://itunes.apple.com/us/app/CDM/id807480077?mt=8>. CDM client supports iOS 6.0 and higher versions and is compatible with iPhone, iPad and iPod Touch.

To download and install CDM client on iOS devices

- Visit the iTunes website at <https://itunes.apple.com/us/app/CDM/id807480077?mt=8> and tap the CDM icon

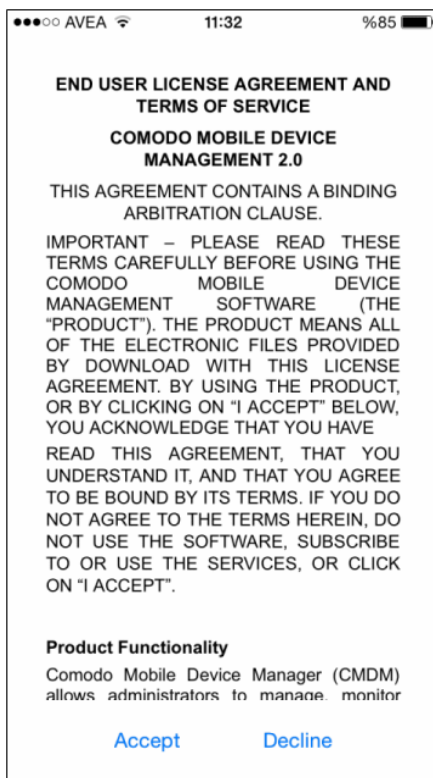


- Tap 'Install'

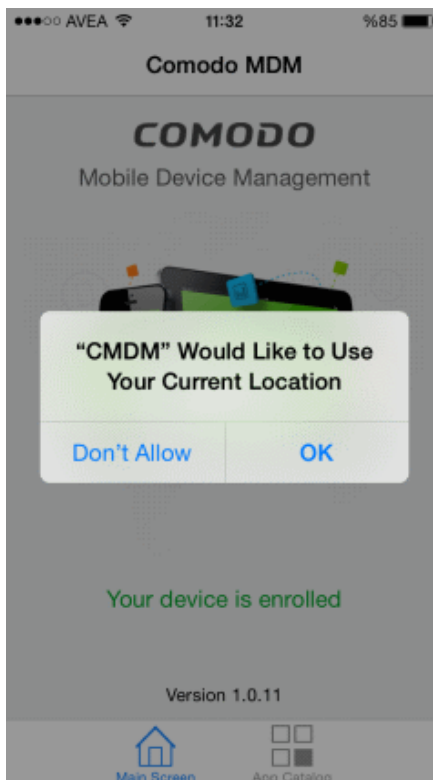
The CDM app will be downloaded and installed on the device.



- Tap on the CDM icon

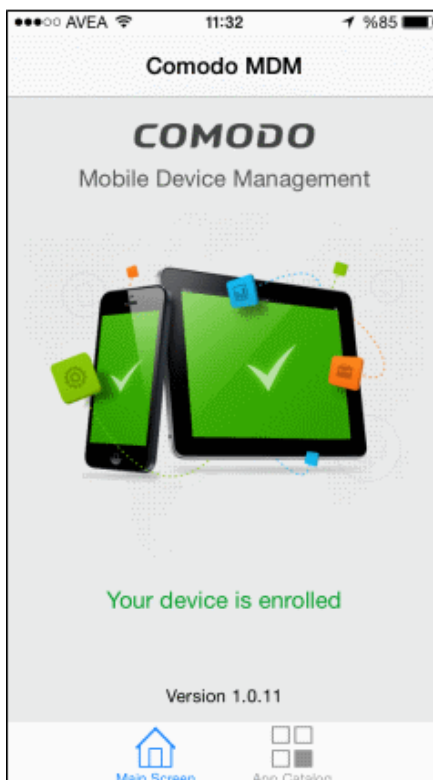


- Read the End User License Agreement fully and tap 'Accept'

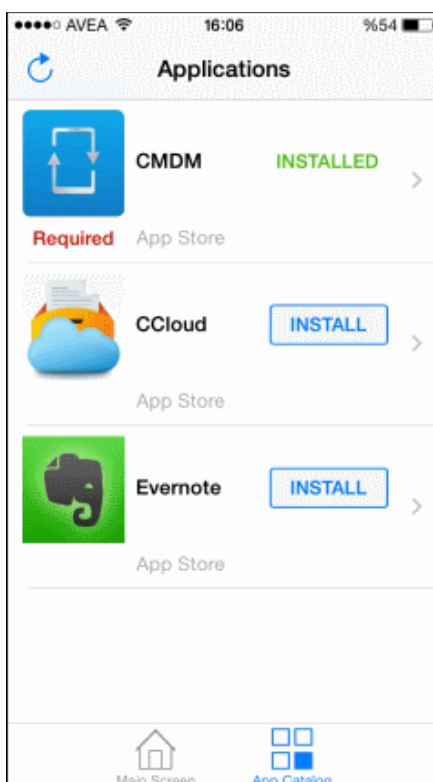


- Tap 'OK'.

The device will be successfully enrolled.



Tapping 'App Catalog' will display the iOS apps that are installed, required to be installed and available for installing. Refer the section Installing Apps on Devices for more details.

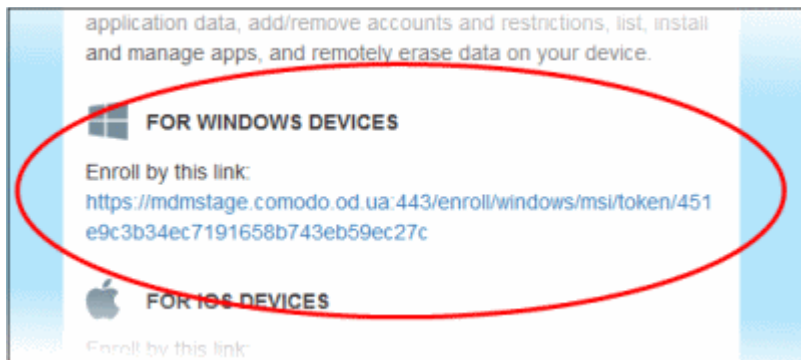


4.1.2.3. Enrolling Windows Endpoints

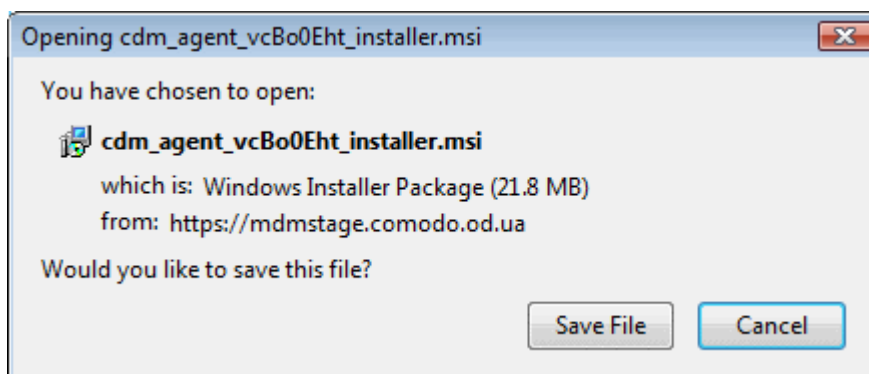
After the administrator has added devices for a user, the user will receive an enrollment email with a link to the enrollment page. The enrollment page will contain the enrollment instructions and a link to download the CDM agent for Windows endpoints. The user should open the email at the Windows endpoint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

To enroll a Windows device


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



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



The download dialog for the CDM agent setup file will appear.

- Download and save the setup file to the local drive
- Double click on the setup file 

On completion of installation, the device will be automatically enrolled o the CDM server and a confirmation message will be displayed.



Once the device is enrolled, the next step is to install CES onto the endpoint in order for the default or assigned Windows profiles to take effect. Refer to the section [Remotely Installing Packages onto Windows Devices](#) for more details.

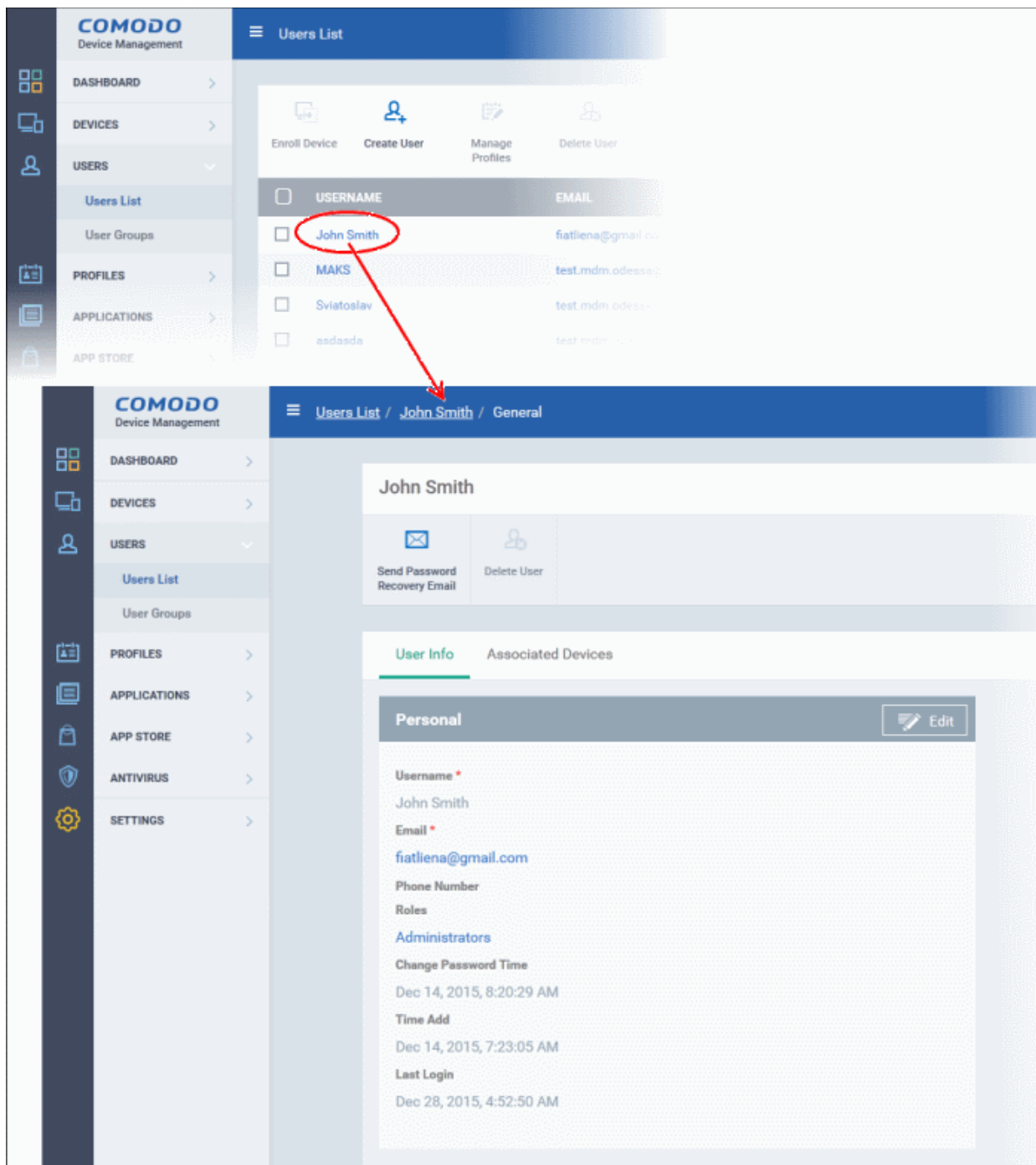
4.1.3. Viewing the Details of a User

The administrator can view the details of a user account at anytime from the 'Users' interface.

To view the details

- Open 'Users' interface by clicking 'Users' > 'Users List'
- Simply click the name of the user

The 'User Details' screen will open.



The administrator can update the details of the user by clicking the 'Edit' icon at the top right. Refer to [Updating Details of a User](#) for more details.

4.1.3.1. Updating the Details of a User

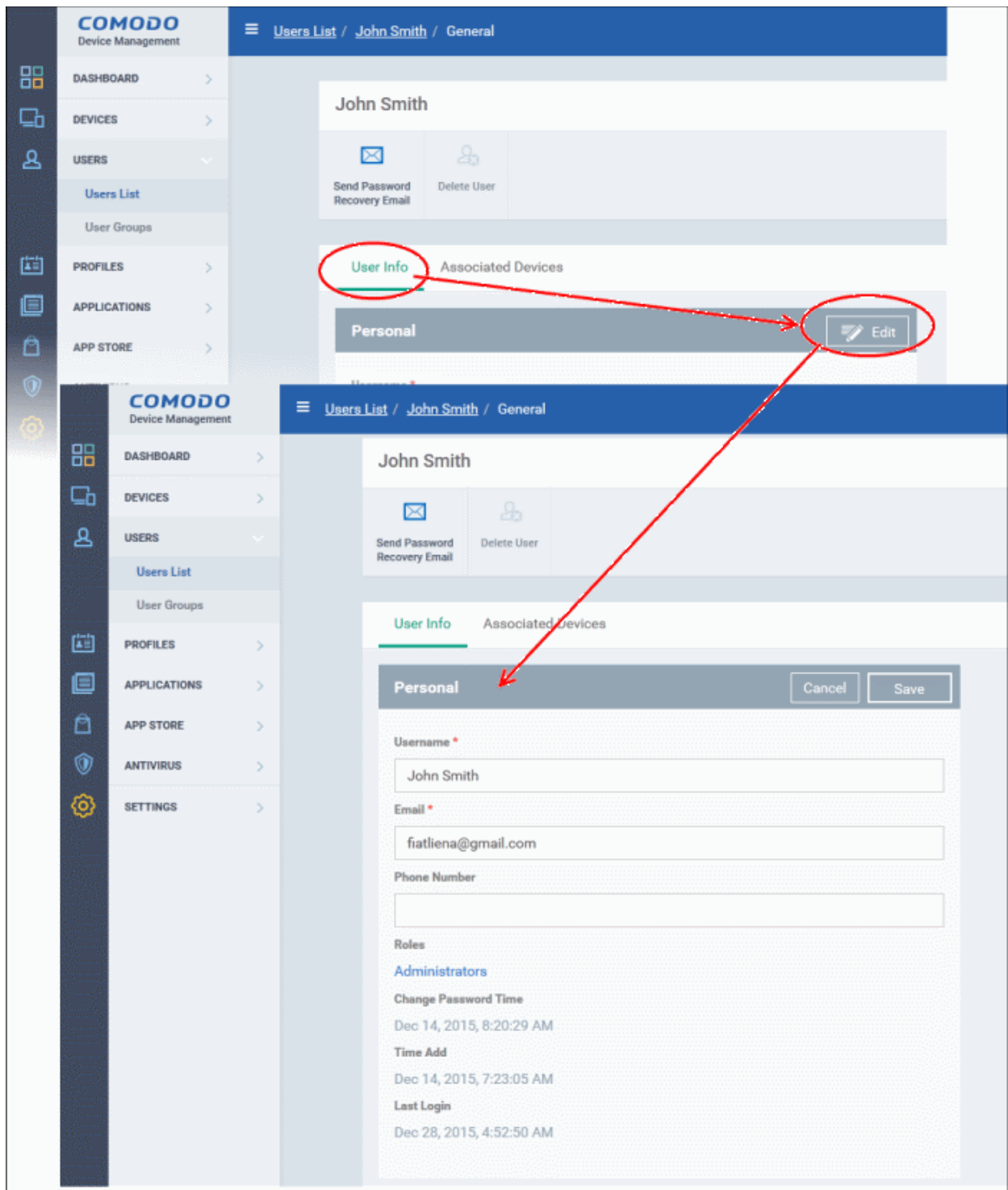
The administrator can update the login username, email address and phone number of a user at any time through the user details interface. The interface also allows to view the devices that are associated for the user as well as send a password recovery email.

To update the details of a user

- Open 'Users' interface by clicking 'Users' > 'Users List'
- Click on the username of the user whose details are to be updated.

The user details screen will open.

- Click the 'User Info' link and then the 'Edit' button at the top right



Update User Form - Table of Parameters

Form Element	Type	Description
Username	Text Field	Allows you to change the login username for 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.

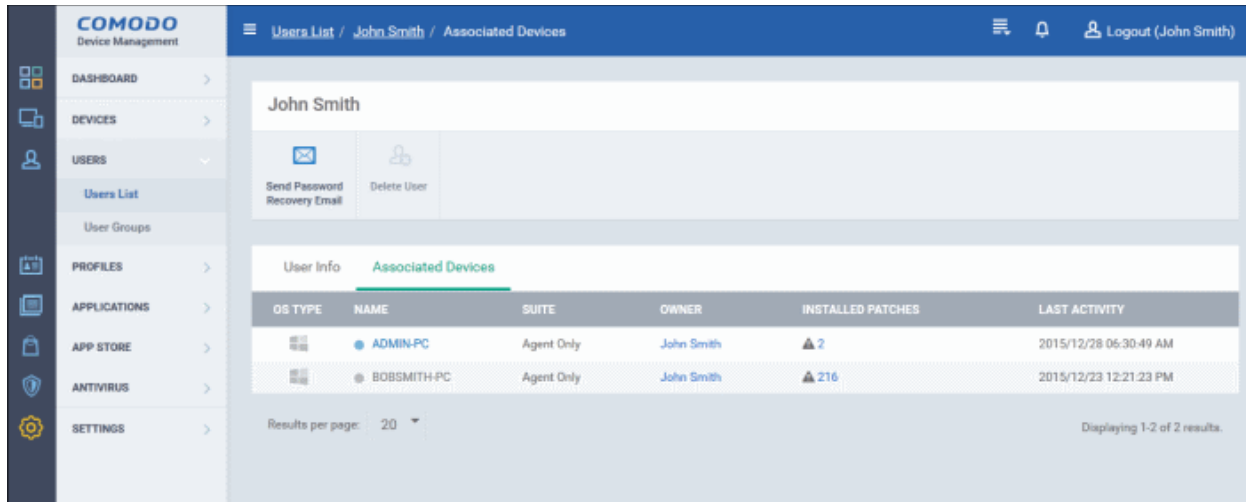
- Click 'Save' from the top for your changes to take effect

The role assigned to the user is displayed under 'Roles' in the screen. Clicking the role name will open the user role management screen that allows to manage user's role. Refer to the section '[Managing Roles Assigned to a User](#)' for more details.

To view the devices associated with the user

- Click the 'Associated Devices' link

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



Associated Devices - Column Descriptions

Column Heading	Description
OS Type	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.
Suite	Indicates components of the endpoint security software/agent installed on the device.
Owner	Indicates the owner/user of the device. Clicking the user name will open the View User interface, displaying the details of the user. Refer to the section ' Viewing the Details of a User ' for more details.
Last Activity	Indicates the date and time at which the device was last polled by CDM.

To send password reset email

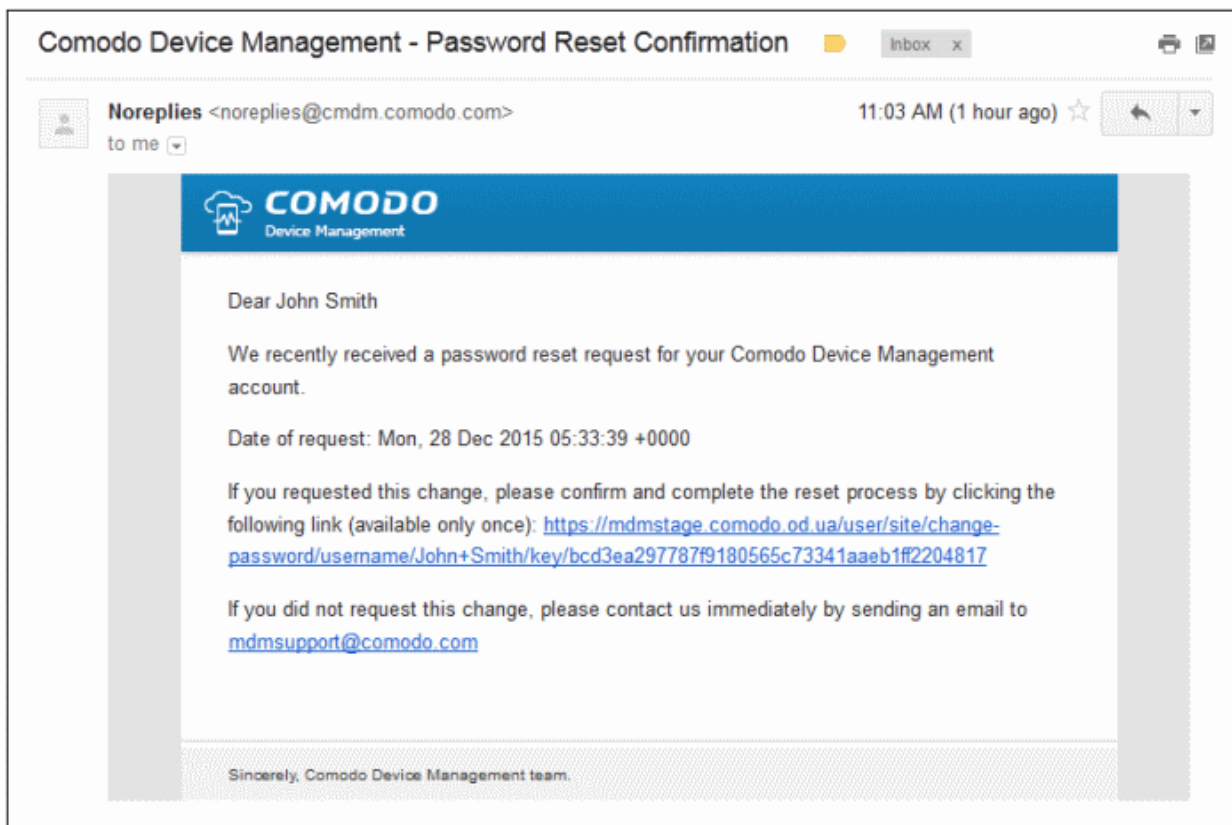
If a user has forgotten his/her, the administrator can send a password reset email to the user from this interface.

- Open 'Users' interface by clicking 'Users' > 'Users List'

The user details screen will open.

- Click the 'Send Password Recovery Email'

A 'Password Reset Confirmation' message will be sent to the registered email address of the user.



On clicking the password reset process link, the 'Password Reset' form will be displayed:

A blue-themed form titled 'PASSWORD RESET'. It asks the user to fill out the form with their login credentials. The form contains three input fields: 'Password', 'Password confirmation', and 'Verification Code'. To the right of the 'Verification Code' field is a CAPTCHA image with the word 'keagib' in a stylized font. Below the input fields is a large green button labeled 'SET THE PASSWORD'. At the bottom of the form, there is a note: 'Please enter the letters as they are shown in the image above. Letters are not case-sensitive.'

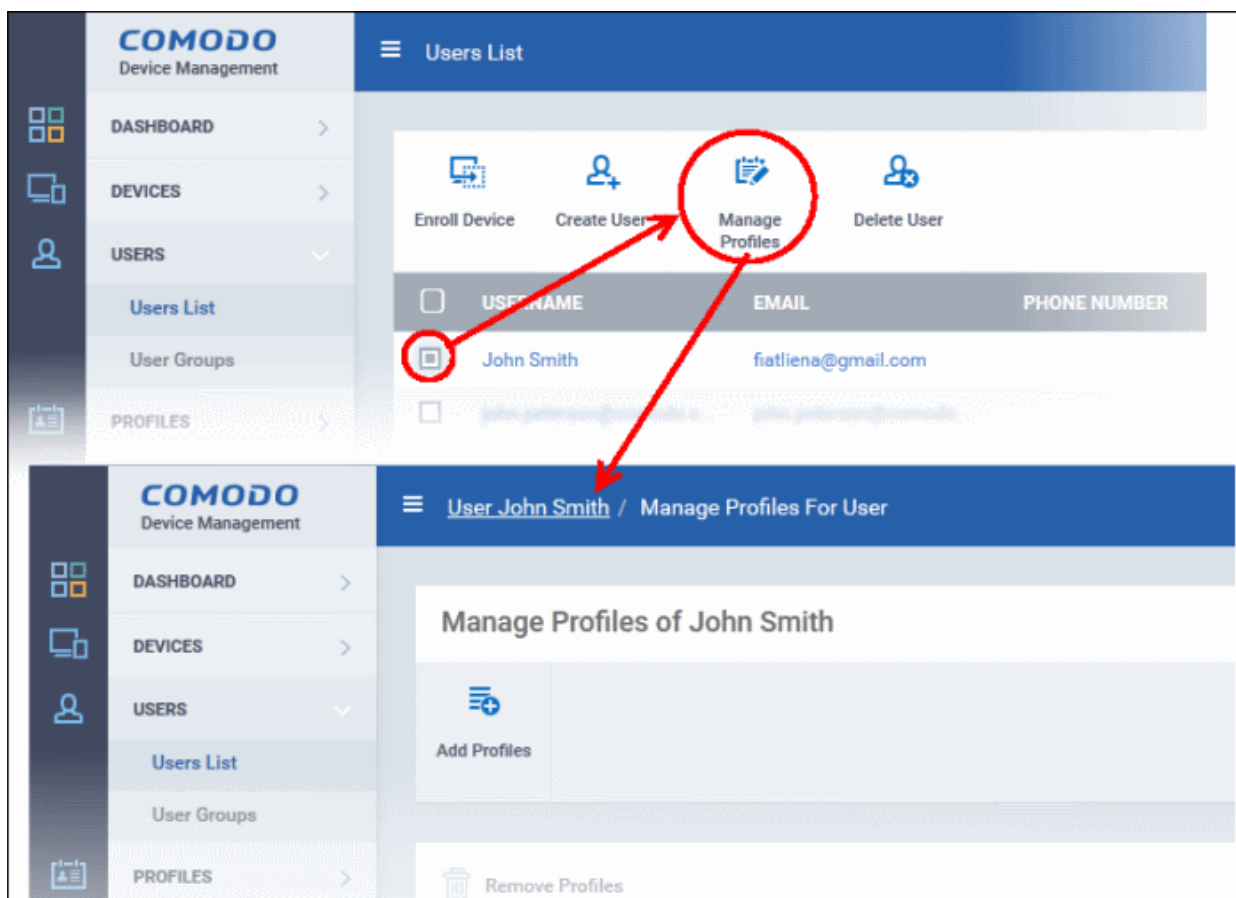
The user has to fill out the form and click 'Set the Password'. The password will be saved and the user can login to CDM interface using the new password.

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

CDM allows administrators to assign profile(s) to user(s) so that the selected profiles will be deployed on all the devices associated with the user(s). The administrator will be able to select profiles pertaining to different OS types and the profiles will be applied to the respective devices. This is particularly useful if organizations wants to roll out profiles to devices on user basis.

To assign configuration profile to user

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

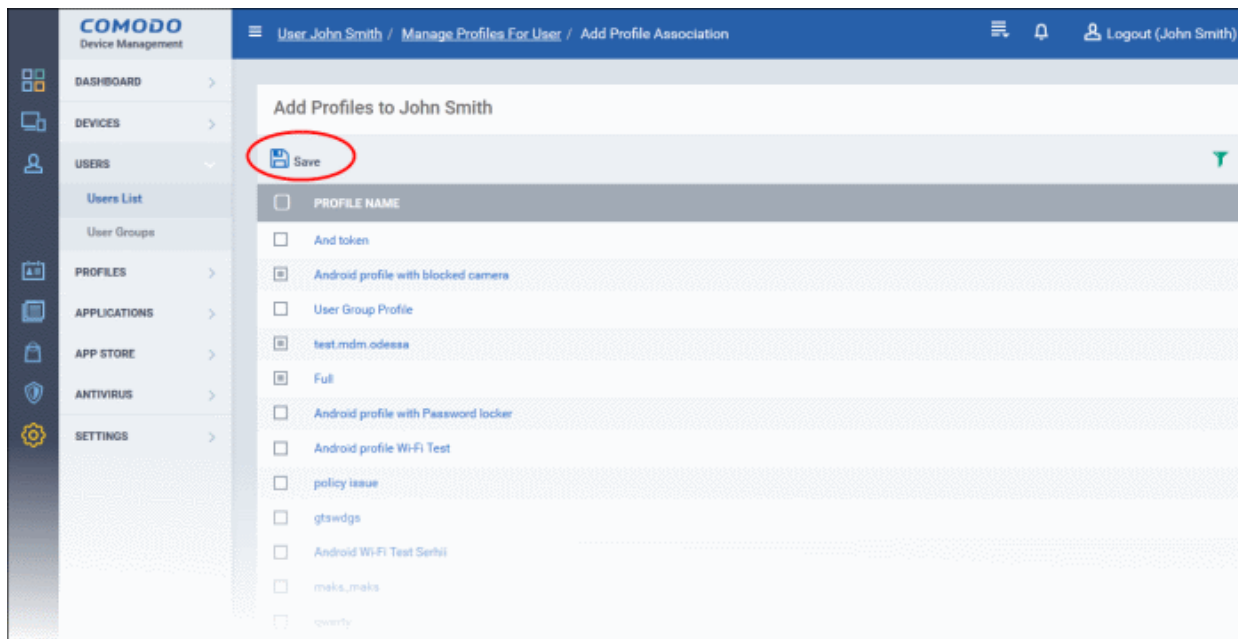


- Click 'Manage Profiles'.

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

To add new profiles

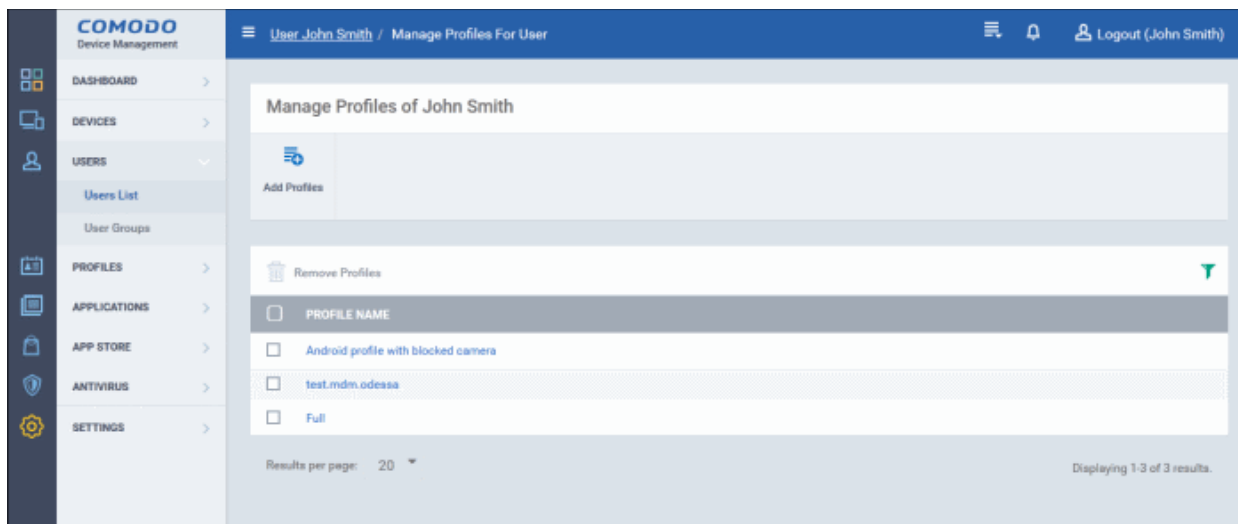
- Click 'Add Profiles'



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

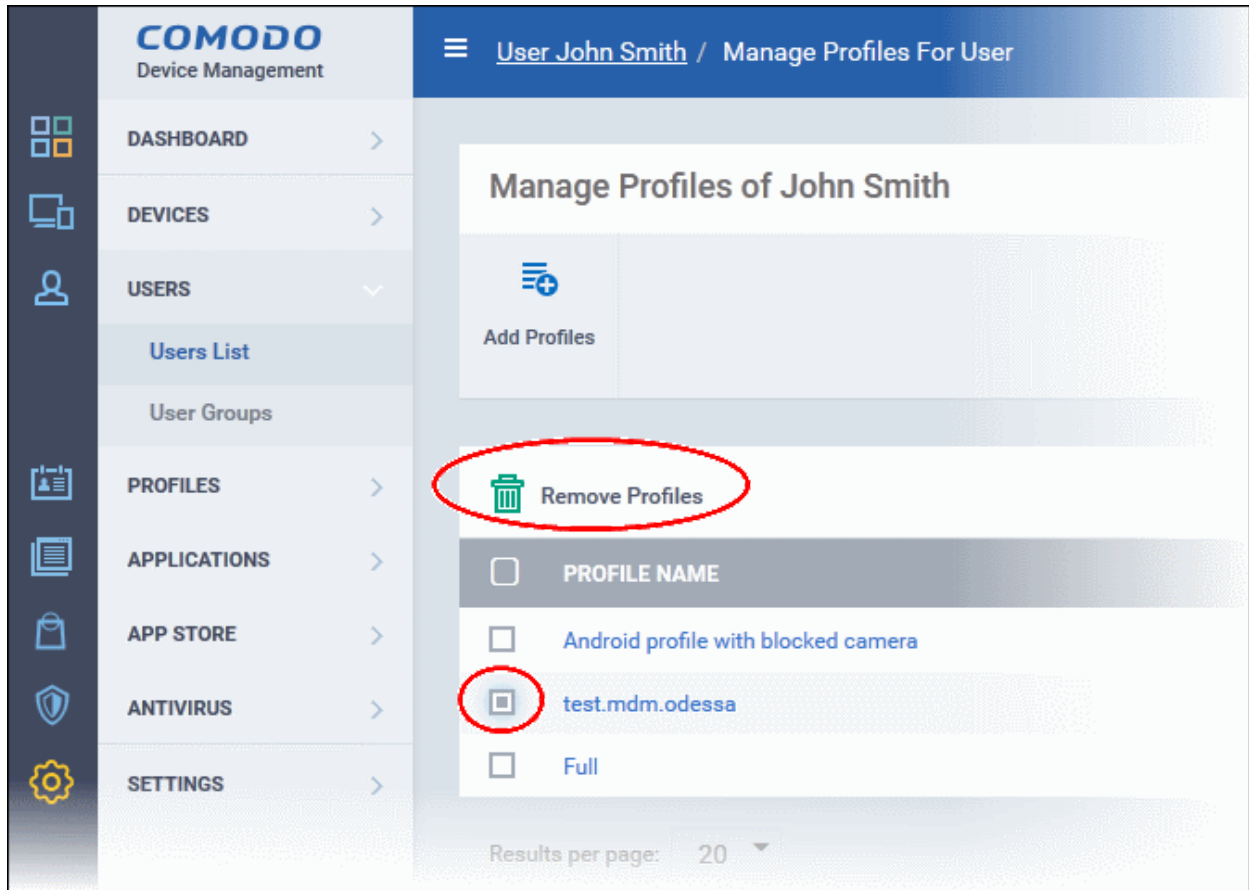
- Click the funnel icon at the right to search for particular profile(s)
- Select the the profile(s) to be added and click 'Save'.

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



To remove a profile

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



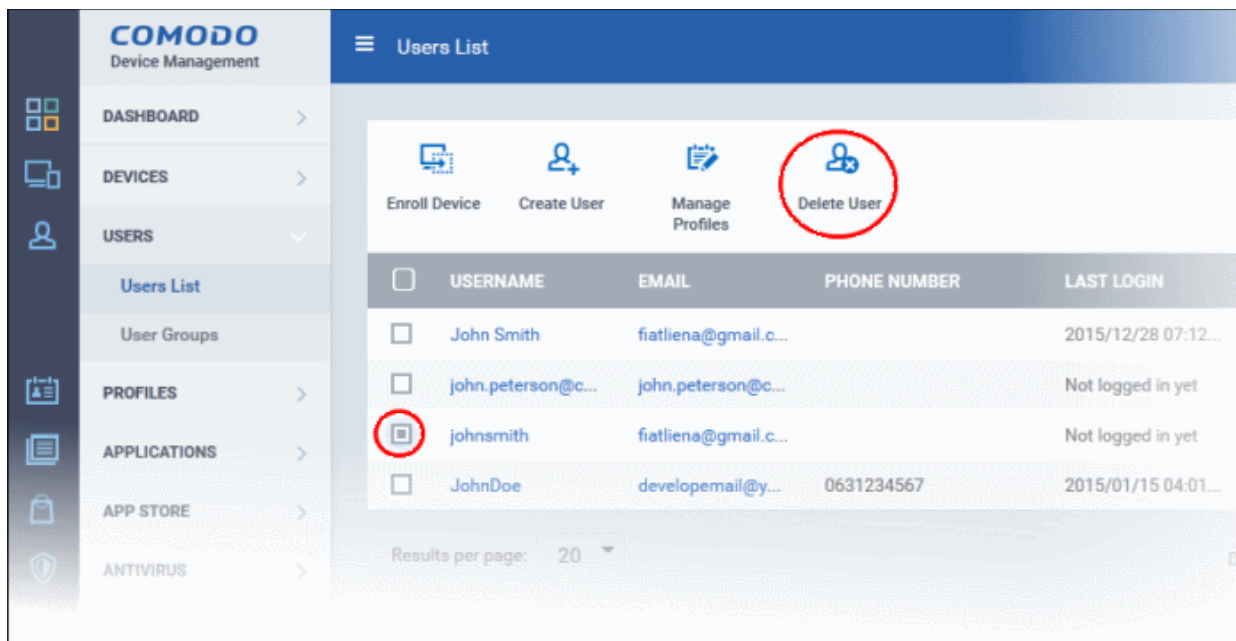
The selected profile(s) will be removed.

4.1.5. Removing a User

The administrator can remove a user and the device(s) associated with the user and no longer be managed by CDM from the 'Users' interface.

To remove a user

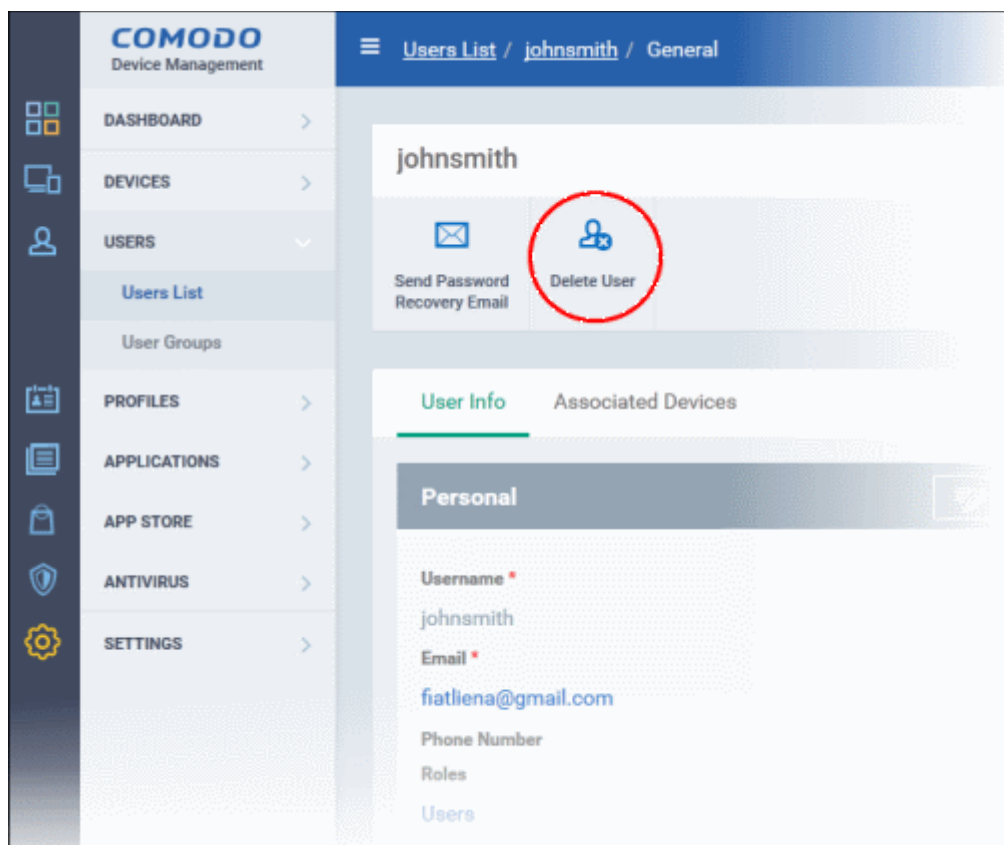
- Open Users interface by clicking 'Users' > 'Users List'
- Select the user to be removed and click 'Delete'



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

The user details screen will open.

- Click 'Delete' at the top



The user will be removed from CDM.

Note: Once a user is removed the device(s) associated with the user will also be removed from CDM. The configuration profiles applied to the user's device(s) by CDM will also be removed from the devices.

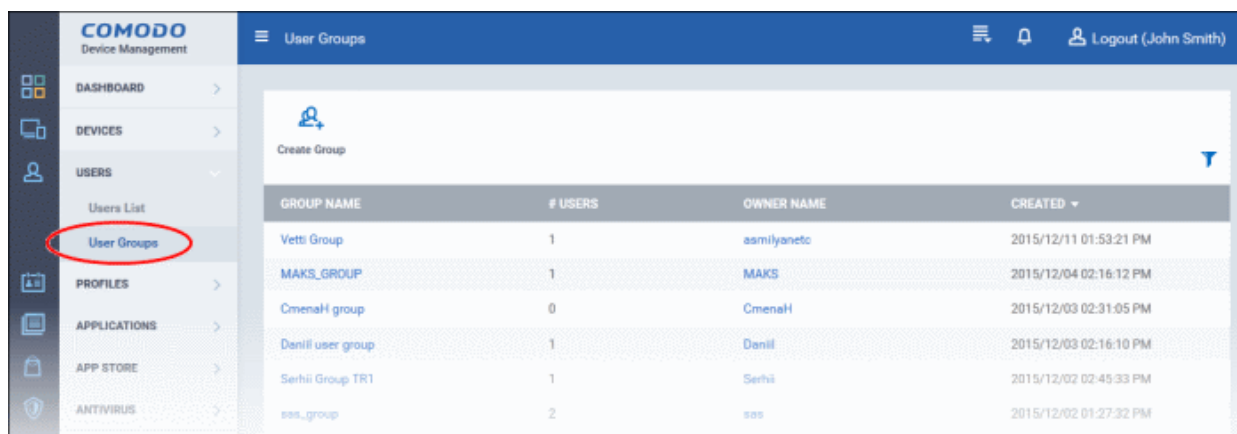
4.2. Managing User Groups

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

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


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

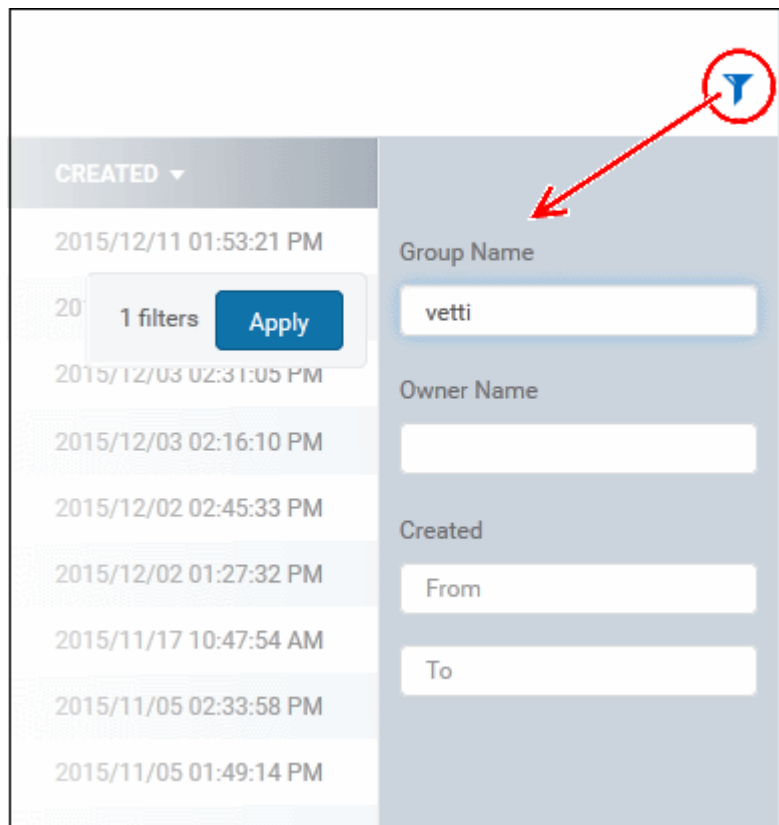
To open the 'User Groups' interface, click the 'Users' tab from the left and choose 'User Groups' from the options.



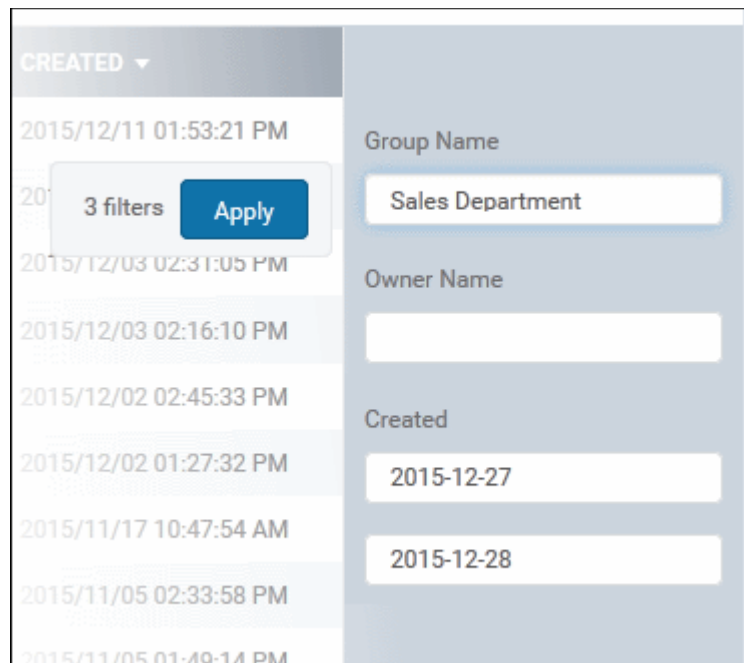
Group of Users List - Column Descriptions	
Column Heading	Description
Group name	The name assigned to the user group by the administrator. Clicking the name of a group will open the group details interface that displays the list of users included in the group and allows you to add or remove users to/from the group. Refer to the section Editing a User Group for more details.
# Users	Displays the number of users in the group.
Owner Name	Indicates the administrator that has created the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section Viewing the details of the User for more details.
Created	Indicates the date and time at which the group was created

Sorting, Search and Filter Options

- Clicking 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 CDM returns 20 results per page when you perform a search. To increase the number of results displayed

per page up to 200, click the arrow next to 'Results per page' drop-down.

Refer to the following sections for more details about:

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

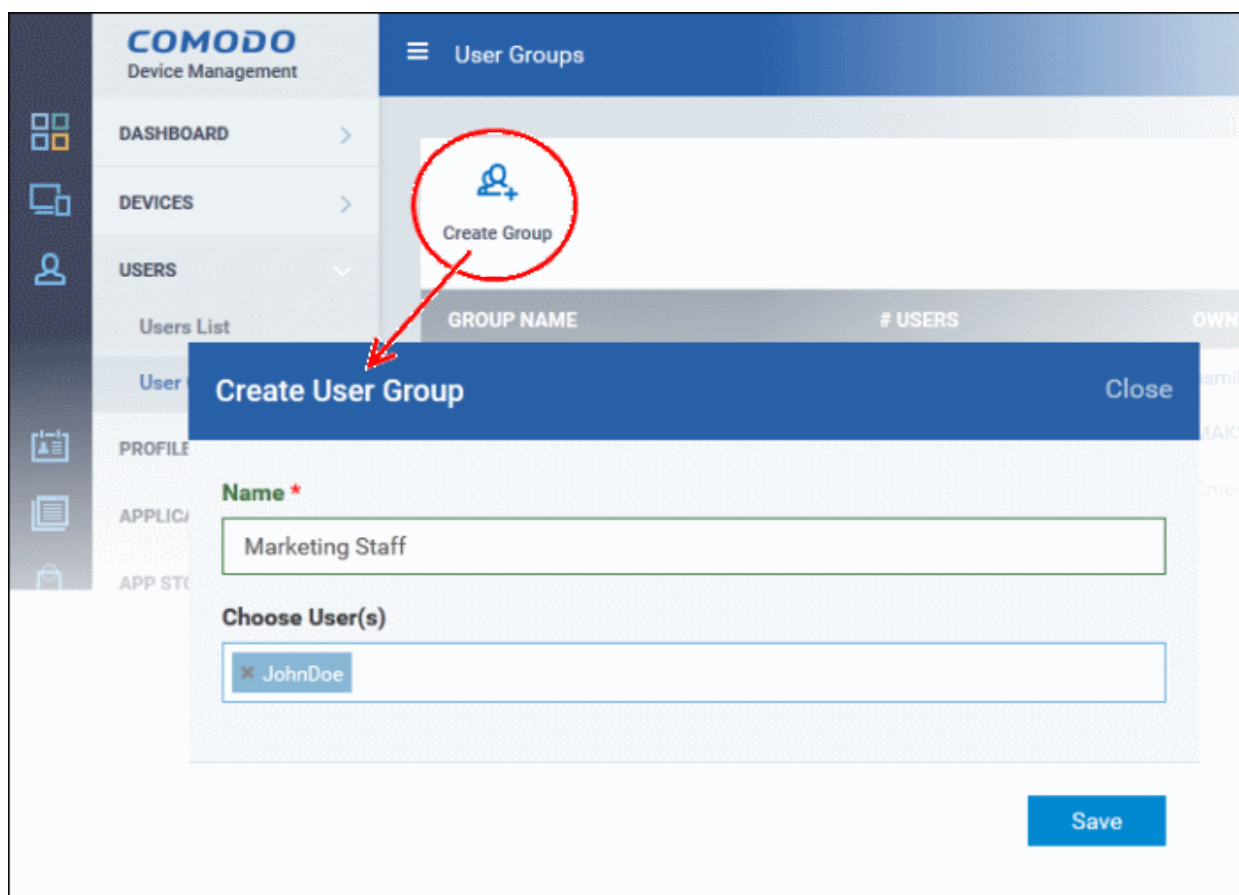
4.2.1. Creating a New User Group

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

To create a new user group

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

The 'Create User Group' dialog will open.

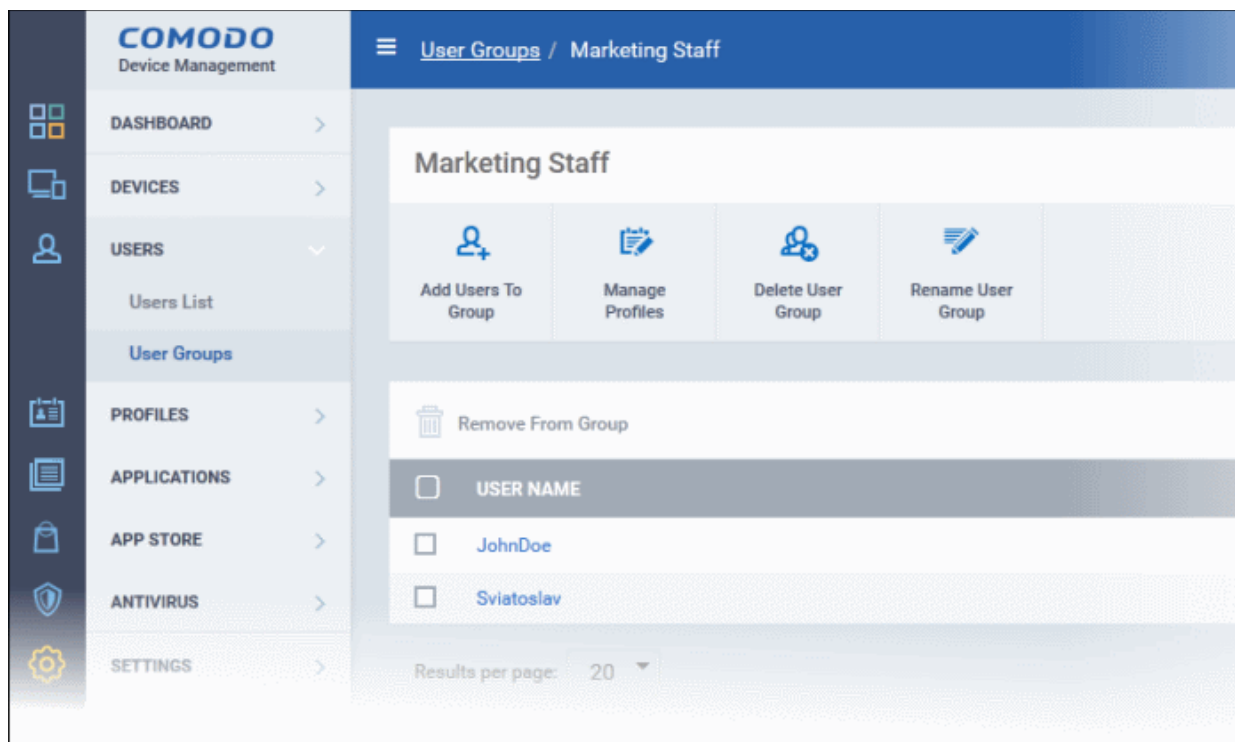


'Create User Group' dialog - Table of Parameters

Form Element	Type	Description
Name	Text Field	Allows you to enter a name shortly describing the group of users.
Choose Users	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 list that appear. Repeat the process for adding more number of users. <ul style="list-style-type: none"> • Note: You can add users at a later stage also.

- Fill the details and click 'Save'.

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



- Repeat the process to add more groups.

The users can be added to or removed from the groups at anytime. Refer to the section [Editing a User Group](#) for more details.

Appropriate configuration profiles can now be applied to the new user groups. Refer to [Assigning Configuration Policy to a User Group](#) for more details.

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

4.2.2. Editing a User Group

The administrator can rename a group, view the users of a group, add or remove users and can remove a group, from the group details interface.

To view and edit user groups

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

The screenshot displays the Comodo Device Manager interface. The left sidebar contains navigation options: DASHBOARD, DEVICES, USERS (with sub-options Users List and User Groups), PROFILES, APPLICATIONS, APP STORE, ANTIVIRUS, and SETTINGS. The main content area is titled 'User Groups' and shows a 'Create Group' button and a table of existing groups:

GROUP NAME	# USERS	OWNER NAME
Marketing Staff	2	John Smit
Vetti Group	1	asmilyane
MAKS_GROUP	1	MAKS

Below the table, the 'Marketing Staff' group details are shown, including a 'Remove From Group' button and a list of users:

<input type="checkbox"/>	USER NAME
<input type="checkbox"/>	JohnDoe
<input type="checkbox"/>	Sviatoslav

At the bottom of the details view, it shows 'Results per page: 20'.

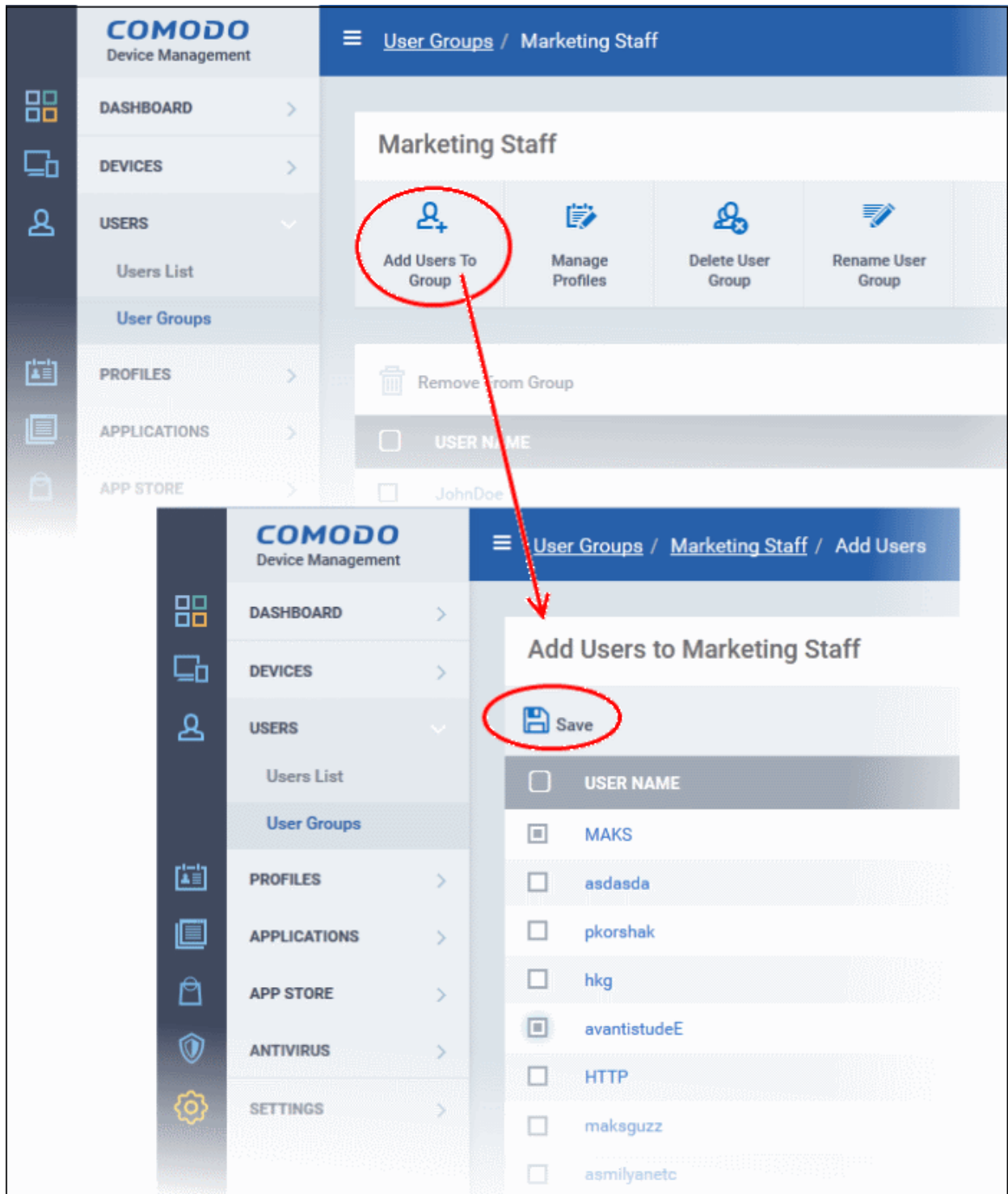
The user group details interface will open with the list of users in the group and allows you to:

- **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 CDM, excluding those in the group will be displayed.

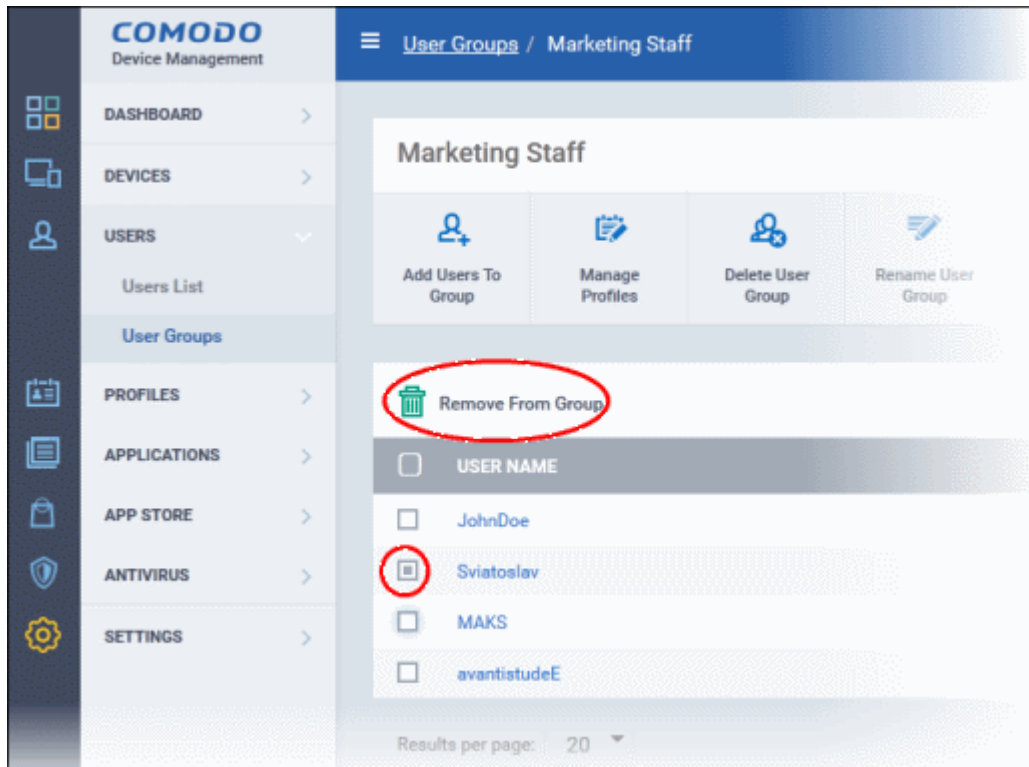


- Select the users to be added to the group and click 'Save'.

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

To remove a user from the group

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

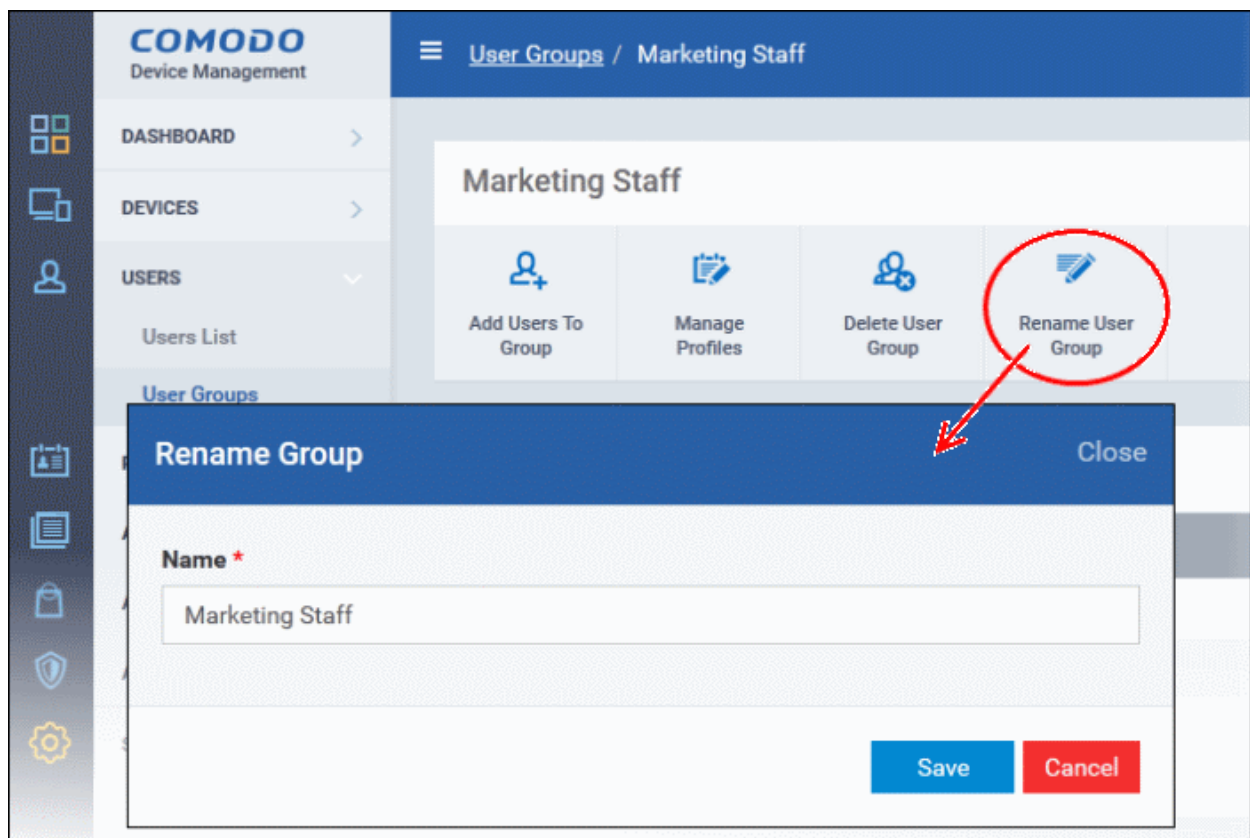


If a user is removed from a group, the profiles in effect on the user's device because of association with the group, will also be removed.

To rename a group

- Click 'Rename User Group' at the top

The 'Update Group' dialog will open:



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

The group will be updated with the new name.

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

4.2.3. Assigning Configuration Profiles to a User Group

The administrator can view the current configuration profiles applied to a user group and apply new configuration profiles to it. The profiles will be applied instantly to all the devices belonging to all the users in the group. The administrator will be able to select profiles pertaining to different OS types and the profiles will be applied to the respective devices. This is particularly useful if organizations want to roll out profiles to devices on user group basis.

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 choosing 'User Groups' from the options.
- Click on the name of the group that is to be assigned a profile.

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

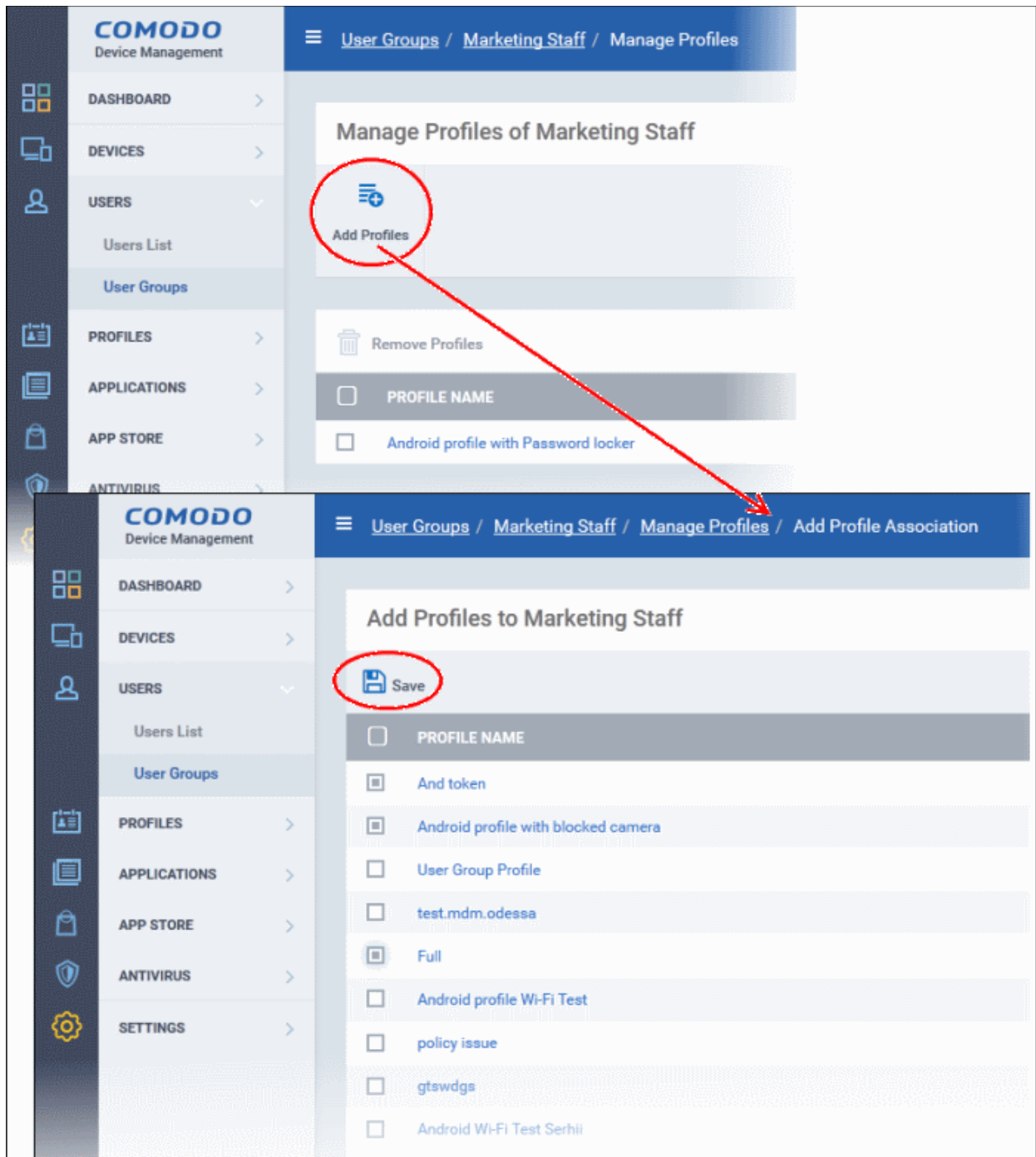
- Click 'Manage Profiles' at the top.

The image shows two screenshots of the Comodo Device Manager interface. The top screenshot displays the 'Marketing Staff' user group page. The 'Manage Profiles' button is circled in red, with a red arrow pointing to the bottom screenshot. The bottom screenshot shows the 'Manage Profiles of Marketing Staff' page, which includes an 'Add Profiles' button, a 'Remove Profiles' button, and a table with a 'PROFILE NAME' header and one entry: 'Android profile with Password locker'. The 'Results per page' is set to 20.

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

To add a new profile

- Click 'Add Profiles'



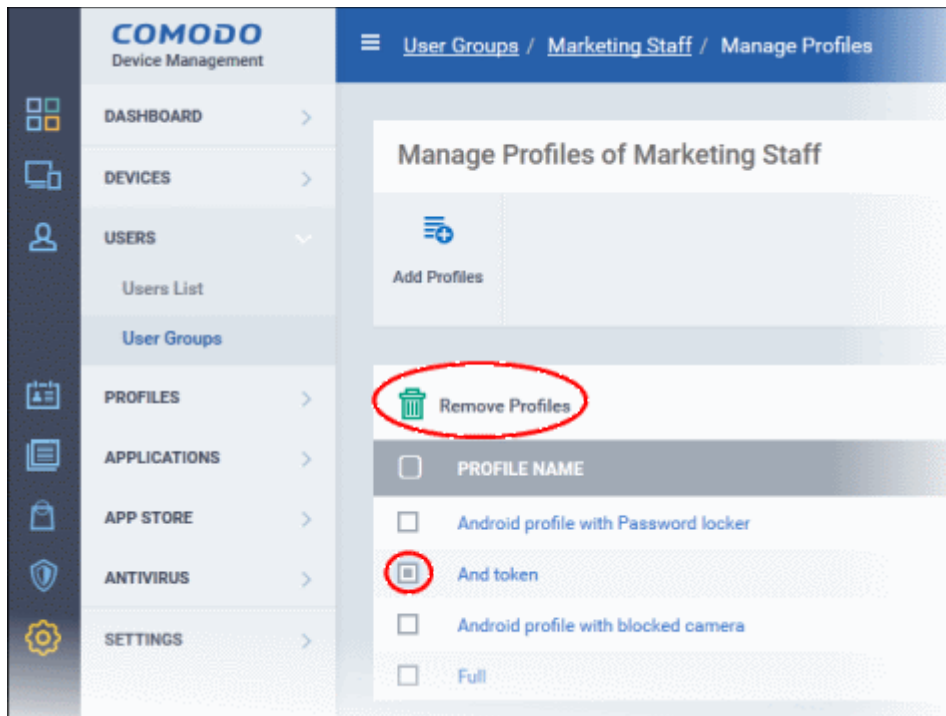
A list of all configuration profiles, available in CDM, excluding those already applied to the group will be displayed.

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

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

To remove a profile from a group

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



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

4.2.4. Removing a User Group

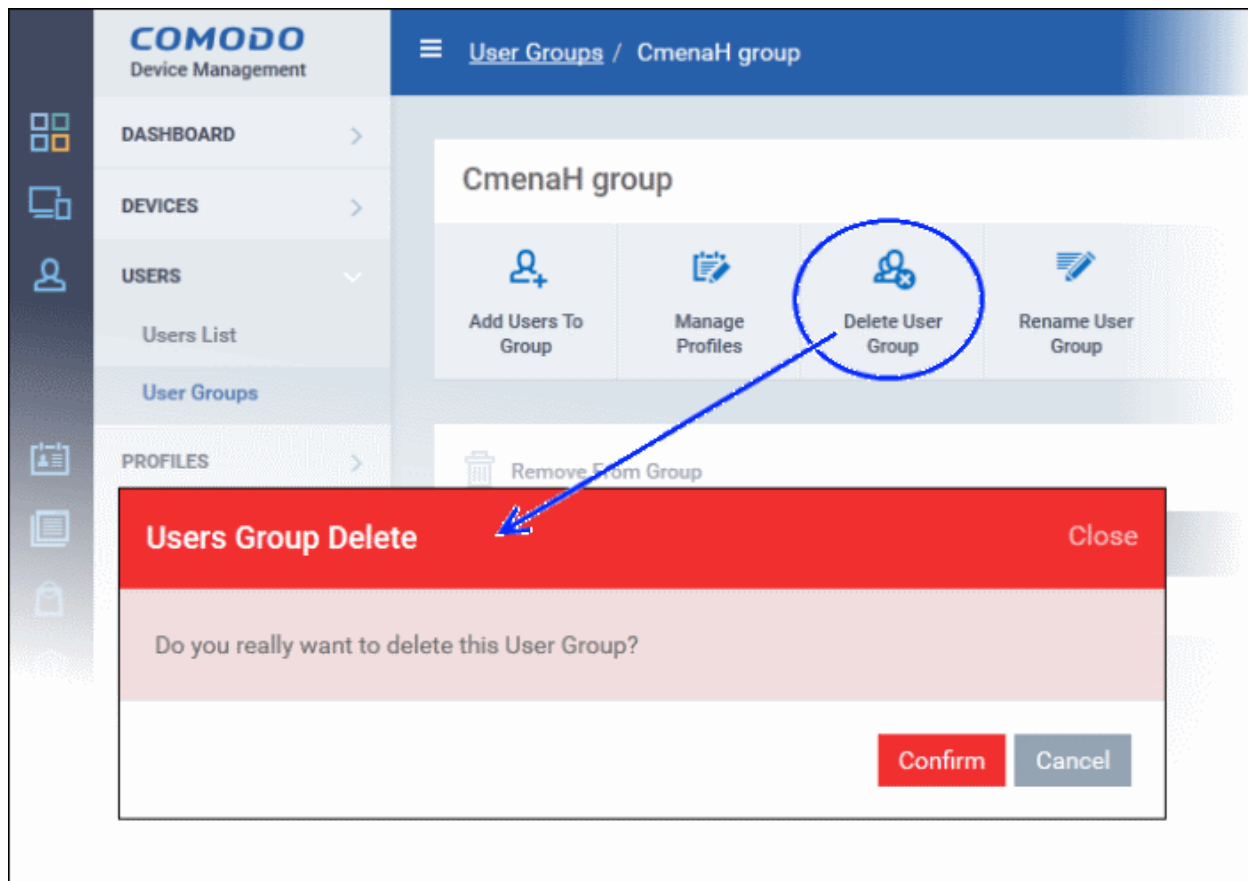
Administrators can remove unwanted user group(s) in CDM. Doing so will remove the group but will not delete the users from CDM. However, any profile(s) associated with the group will be removed from the devices of group members.

To remove a user group

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

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

- Click 'Delete User Group' at the top.



- Click 'OK' in the confirmation dialog. The user group will be removed from CDM.

5. Devices

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

Please use the following links to find out more:

- **The Device List**
 - [Managing Windows Devices](#)
 - [Managing Android / iOS Devices](#)
 - [Viewing the User Information](#)
 - [Removing a Device](#)
 - [Accessing Windows Device through Remote Desktop](#)
 - [Installing CDM Packages Windows Devices](#)
 - [Installing Third Party MSI Packages on Windows Devices](#)
 - [Installing Apps on Android / iOS Devices](#)
 - [Generating 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 Messages to Devices](#)
- **Managing Device Groups**

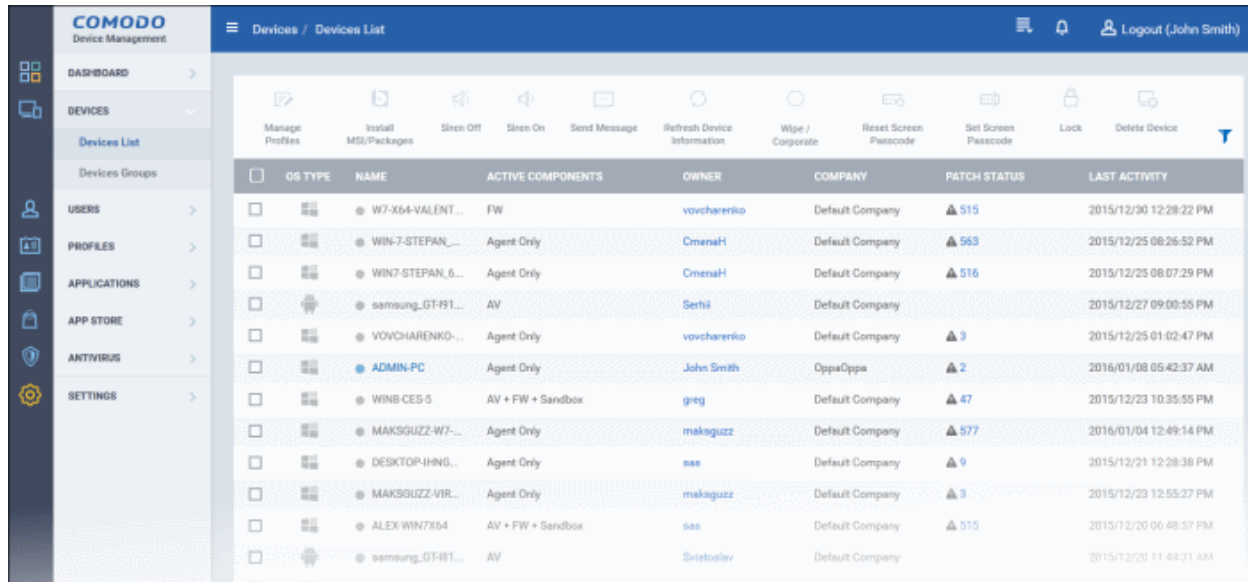
- [Creating Device Groups](#)
- [Editing Device Groups](#)
- [Assigning Configuration Profile to Groups](#)
- [Removing a Device Group](#)

5.1. Device List

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


- Add or remove profiles on any selected device
- Install CIS and other packages on Windows endpoints
- 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 CDM management
- View detailed information about any device by simply clicking the device name
- View and edit device owner information by clicking the owner name
- View and implement pending updates by clicking the number in the 'Patch Status' column

To open the Device List, click the 'Devices' link on the left then select 'Devices List':




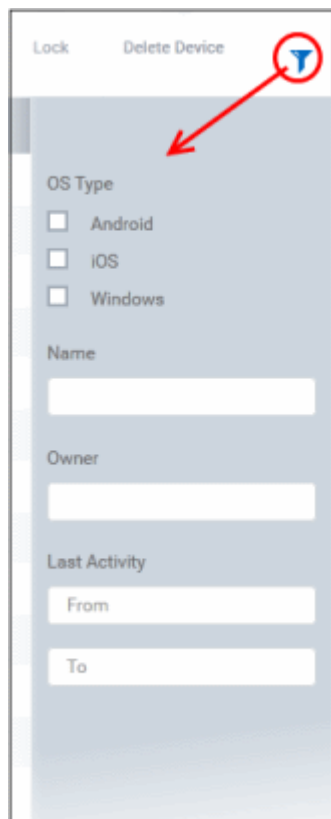
The Devices interface will open with a list of devices enrolled to CDM.

Devices - Column Descriptions	
Column Heading	Description
OS Type	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. Grey text color indicates the device is offline for the past 24 hours. Clicking the device name will open the granular device details interface. Refer to the sections Managing Windows Devices and Managing Android / iOS Devices for more details.

Active Components	The Comodo software items installed on the device. For Android devices the agent will automatically install the AV (antivirus) component. For iOS devices, only the agent (CDM client) will be installed. For Windows endpoints, the available components are - Agent Only, AV, FW (firewall) and Sandbox.
Owner	Indicates the device user. Clicking the user name will open the 'View User' interface. Refer to Viewing the User Information for more details.
Company	Indicates the name of the company to which the device is enrolled. For customers using CDM as a standalone application, this will display as 'Default Company'. For Comodo One users, the name of the C1 company will be displayed.
Patch Status	Indicates the quantity of pending updates for Window devices. A check-mark <input checked="" type="checkbox"/> indicates the device is up-to-date and all patches are installed. A exclamation mark followed by a number  indicates patches are available for the device. Refer to Viewing and Installing Windows Patches for more details.
Last Activity	The most recent date that the device contacted Comodo Device Manager.

Sorting, Search and Filter Options

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



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

The screenshot shows a search filter interface. On the left, there is a list of filters with a '1 filters' button and an 'Apply' button. On the right, there is a search form with the following fields:

- Name: Admin
- Owner: John
- Last Activity: From (calendar icon) To (calendar icon)

- To filter the devices based on their last activities detected 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 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 CDM 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:

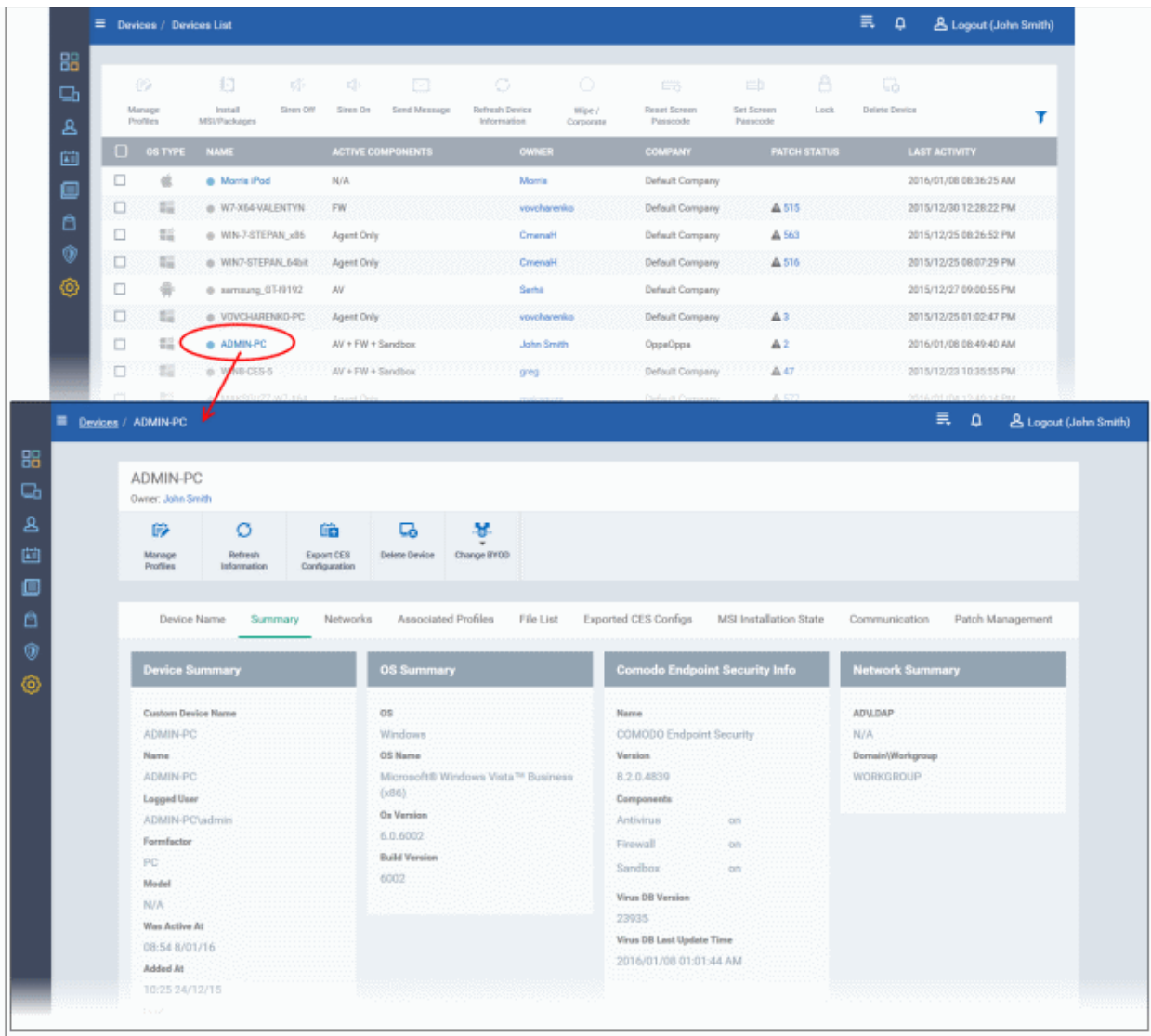
- Managing Windows Devices**
 - Viewing and Editing Windows Device Name
 - Viewing Summary Information
 - Viewing Network Information
 - Viewing and Managing Profiles Associated with Windows Device
 - Viewing List of Files in the Device
 - Viewing CES Configuration Exported from the Device
 - Viewing MSI Files Installed on the Device through CDM
 - Viewing and Installing Windows Patches
- 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

5.1.1. Managing Windows Devices

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

To view details of and manage a Windows device

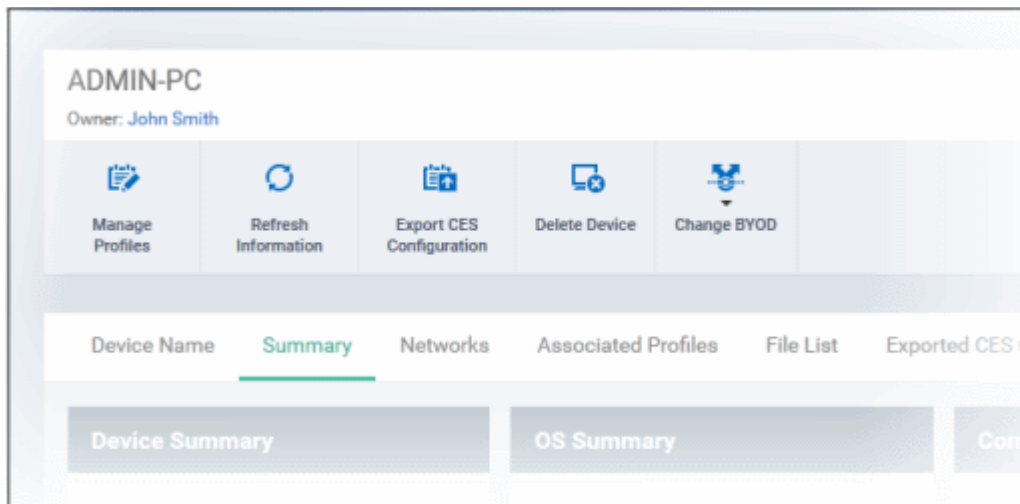
- Click 'Devices' and choose 'Devices List'
- Click the name of any Windows device



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

- **Device Name** - Displays the name of the device and allows to change it for administrative purpose and easy management. Refer to the section [Viewing and Editing Device Name](#) for more details.
- **Summary** - Displays the general details of the device including device information, OS details, Network details and security configuration. Refer to the section [Viewing Summary Information](#) for more details.
- **Networks** - Displays the device's network details such as its MAC address, its IP address and more. Refer to the section [Viewing Network Information](#) for more details.
- **Associated Profiles** - Displays the details of the profiles deployed on the device. Refer to the section [Viewing and Managing Profiles Associated with the Devices](#) for more details.
- **File List** - Displays the list of files available on the device that are rated as Unrecognized, Trusted and Malicious. Refer to the section [Viewing List of Files in the Device](#) for more details.
- **Exported CES Configurations** - Displays the details of exported CES configuration files. Refer to the section [Viewing CES Configurations Exported from the Device](#) for more details.
- **MSI Installation State** - Displays the list of MSI files that are installed on the device via CDM. Refer to the section [Viewing MSI Files Installed on the Device through CDM](#) for more details.
- **Patch Management** - Displays the list of available patches for the devices and their statuses whether installed or not. Refer to the section [Viewing and Installing Windows Patches](#) for more details.

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



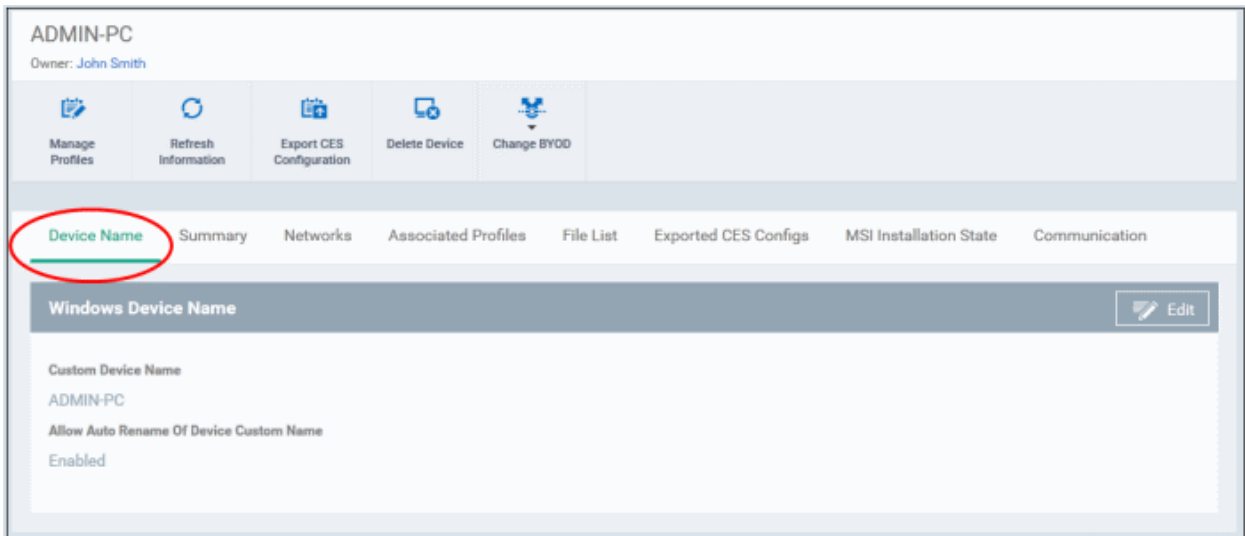
- **Manage Profiles** - Allows you to add or remove device profiles. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. Refer to the section **Updating Device Information** for more details.
- **Export CES Configuration** - Allows you to export the devices current CES configuration as a profile. Exported profiles can be viewed under the **Exported CES Configs** tab. These can then be imported later as a Windows profile, potentially for deployment to other devices. Refer to the section **Importing Windows Profiles** for more details.
- **Delete Device** - Removes the device from CDM. Refer to the section **Removing a Device** for more details.
- **Change BYOD** - Changes the BYOD status of the device. Refer to the section **'Viewing Summary Information'** for more details.

5.1.1.1. Viewing and Editing Device Name

The name of the device assigned by user or if no name was assigned, the model number of the device. You can change this to a more friendly name if required. Please note the new name will be applied in CDM only and will not change the name on the endpoint.

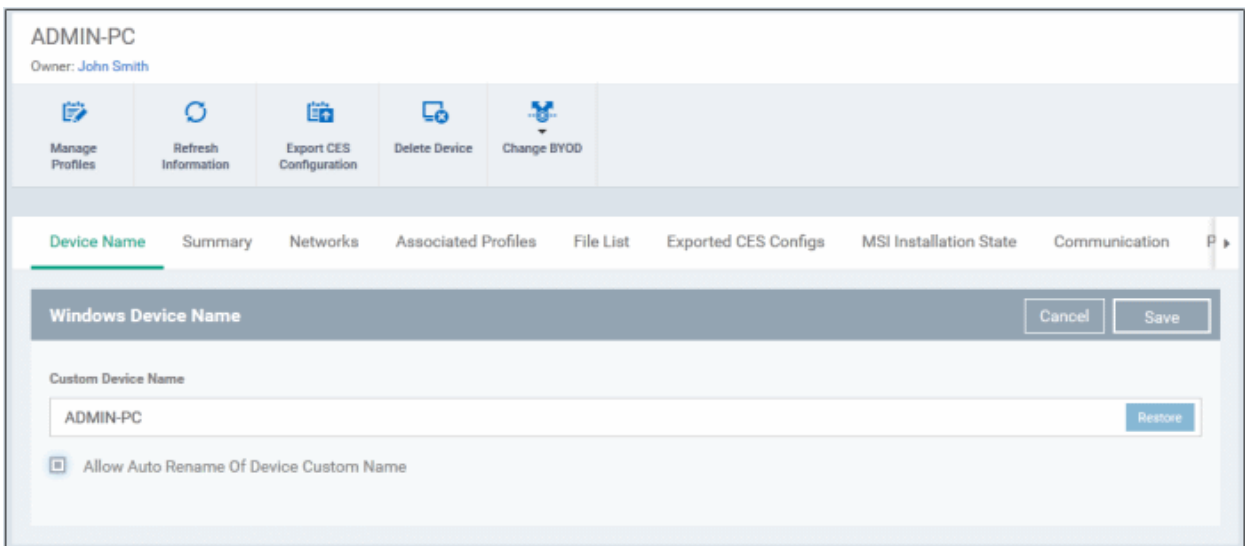
To change the device's name

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



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

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



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

The device will be listed with its new name. The 'Restore' button at the right in the field restores the device's name as it was at the time of enrollment.


5.1.1.2. Viewing Summary Information


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


To view the device information summary


- Click 'Devices' and choose 'Devices List'
- Click the name of any Windows device. By default, the 'Device Summary' will be displayed, else click the 'Summary' tab.


ADMIN-PC
Owner: John Smith


Manage Profiles


Refresh Information


Export CES Configuration


Delete Device


Change BYOD

Device Name **Summary** Networks Associated Profiles File List Exported CES Configs MSI Installation State Communication

Device Summary	OS Summary	Comodo Endpoint Security Info	Network Summary				
<p>Custom Device Name ADMIN-PC</p> <p>Name ADMIN-PC</p> <p>Logged User ADMIN-PC\admin</p> <p>Formfactor PC</p> <p>Model N/A</p> <p>Was Active At 03:34 12/01/16</p> <p>Added At 10:25 24/12/15</p> <p>Uuid 61d7d653-4d24-4d3d-827e-d2e94b16bbc0</p> <p>Service Pack Service Pack 2</p> <p>Device Management Agent Version 5.0.1441.7781</p> <p>Processor Intel(R) Core(TM) i3 CPU 540 @ 3.07GHz 3.06 GHz</p> <p>Serial Number 0</p> <p>System Model VirtualBox</p> <p>System Manufacturer innotek GmbH</p> <p>BYOD Status Corporate</p>	<p>OS Windows</p> <p>OS Name Microsoft® Windows Vista™ Business (x86)</p> <p>Os Version 6.0.6002</p> <p>Build Version 6002</p>	<p>Name COMODO Endpoint Security</p> <p>Version 8.2.0.4839</p> <p>Components</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Antivirus</td><td style="text-align: right;">on</td></tr> <tr><td>Sandbox</td><td style="text-align: right;">on</td></tr> </table> <p>Virus DB Version 23958</p> <p>Virus DB Last Update Time 2016/01/11 09:01:06 PM</p>	Antivirus	on	Sandbox	on	<p>AD\LDAP N/A</p> <p>Domain\Workgroup WORKGROUP</p>
Antivirus	on						
Sandbox	on						

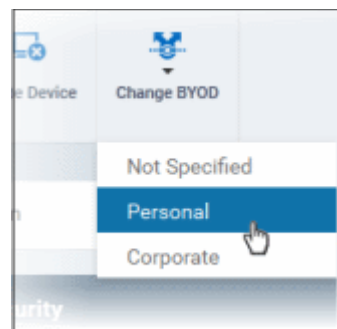
- **Device Summary** - Provides details such as computer name, type, OS, model, manufacturer, currently logged-in user, Active Directory (AD) domain to which the endpoint is connected and more.
- **OS Summary** - Provides details about the device Operating System (OS) of the endpoint.
- **CES Info** - Provides details about version of the endpoint security software installed on the endpoint, the components of CES installed and their status and AV database details.
- **Network Summary** - Provides details of the network to which the endpoint is connected

By default, the BYOD status of a newly enrolled device will be 'Not Specified'. To specify the BYOD type, choose the type from the 'Change BYOD' drop-down at the top right. The available options are:

Comodo Device Manager - Administrator Guide | © 2016 Comodo Security Solutions Inc. | All rights reserved

96

- Personal
- Corporate

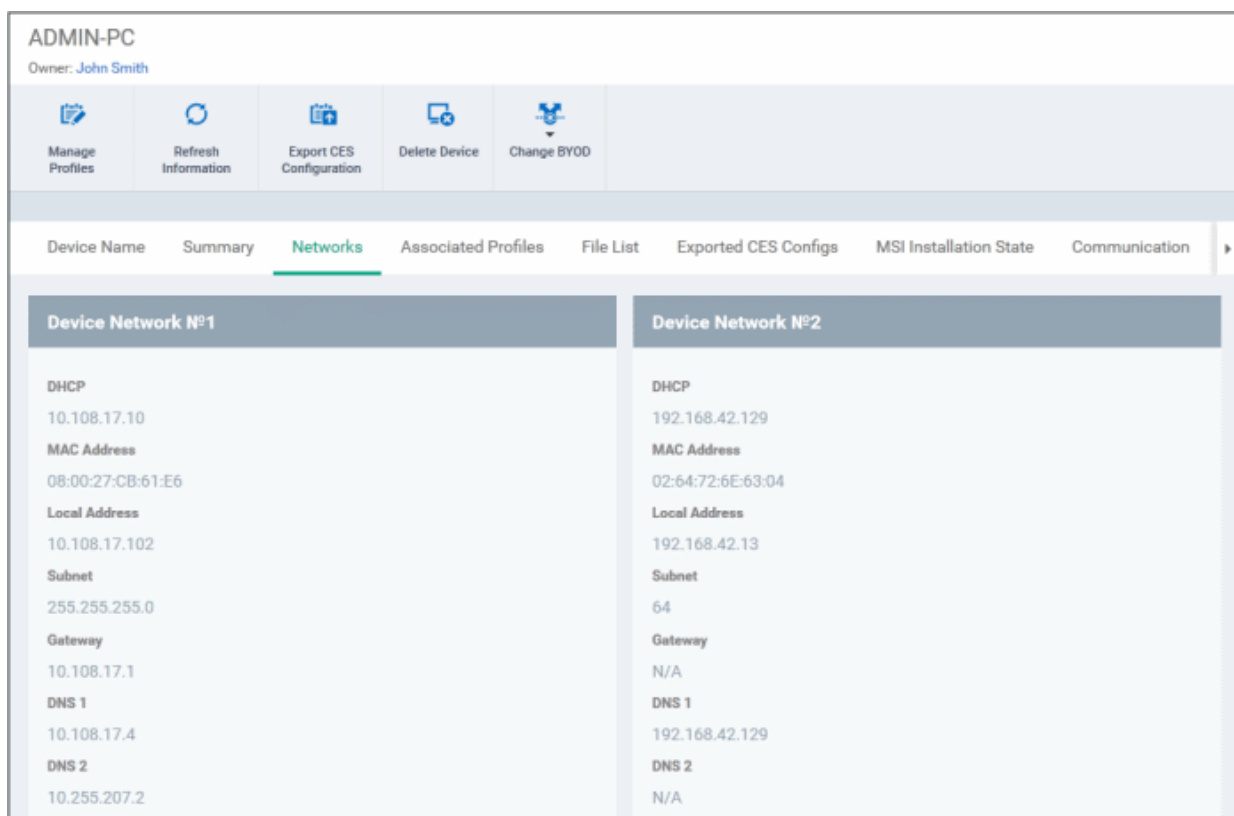


5.1.1.3. Viewing Network Information

The 'Networks' screen displays the network details of the Windows endpoint.

To view the networks details of the device

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



The networks details such as the DHCP server, local addresses, subnet and more are displayed.

5.1.1.4. Viewing and Managing Profiles Associated with the Device

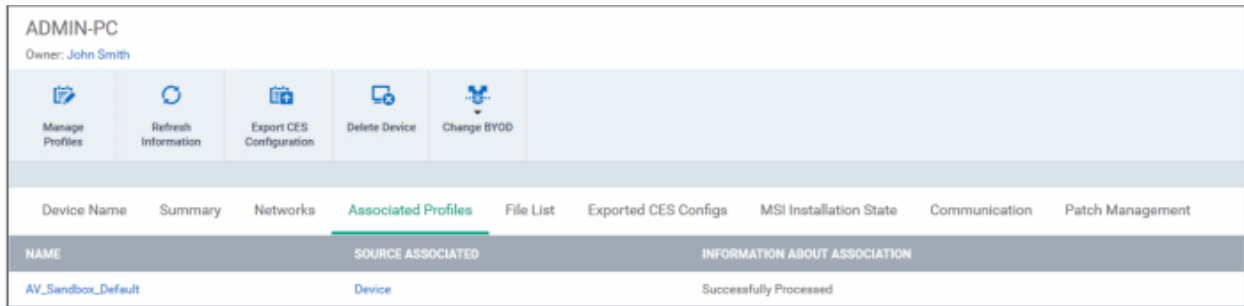
The 'Associated Profiles' tab displays a list of configuration profiles in effect on the endpoint. It also allows the administrator to add or remove profiles to the device. If multiple profiles are associated with the device, the most restrictive policy will be applied.

For more details on profiles and groups of profiles, refer to the chapter [Configuration Profiles](#).

To view and manage the profiles associated with the device

- Click 'Devices' and choose 'Devices List'

- Click the name of any Windows device, then select the 'Associated Profiles' tab



Associated Profiles - Column Descriptions	
Column Heading	Description
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section Editing Configuration Profiles for more details.
Source Associated	<p>Indicates the source through which the profile has been applied to the device. Configuration profiles are applied to a device in different ways:</p> <ul style="list-style-type: none"> Profiles can be directly applied to the device. Refer to the section Assigning Configuration Profiles to Selected Devices for more details The profiles applied to a user is deployed to all the devices belonging to the user. Refer to the section Assigning Configuration Profile(s) to a Users' Devices for more details The profiles applied to a user group is deployed to all the devices belonging to all the users in the group. Refer to the section Assigning Configuration Profile to a User Group for more details The profiles applied to a device group is deployed to all the member devices in the group. Refer to the section Assigning Configuration Profile to Device Groups for more details <p>Clicking on the source opens the respective details interface.</p>
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 Profile to Selected Devices](#) for more details.

5.1.1.5. Viewing list of Files in the Device

Comodo Endpoint 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'. File ratings can be configured as part of a Windows profile - see [File Rating settings](#) for more details. The File List screen allows you to view and change the ratings of discovered files on a particular device, and to clear the rating history of files. Note - if you wish to see all files across all managed devices, please view the 'Applications' section.

To view and manage file ratings on a device

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

The interface contains three tabs:

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

Viewing and Managing Unrecognized Files on a Device

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


- Click the 'Unrecognized' tab

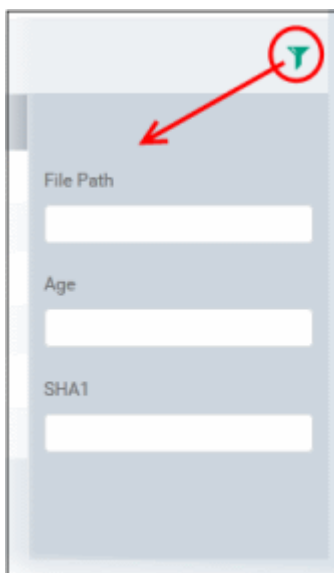
The 'Unrecognized' Files List - Table of Column Descriptions

Column Heading	Description
File Name	Displays the file name of the 'Unrecognized' item.

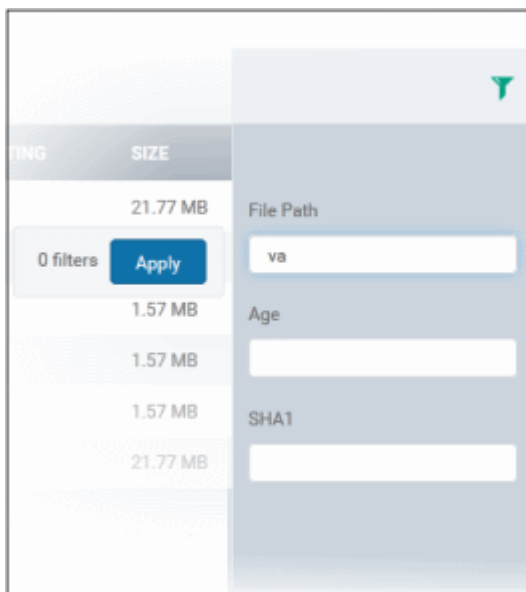
File Path	The installation location of the file on the endpoint
Age	The time at which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved here by the administrator.
Size	The size of the unrecognized file.

Sorting, Search and Filter Options

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



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



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

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

Managing Unrecognized Files

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

Viewing and Managing Trusted Files on the Device


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

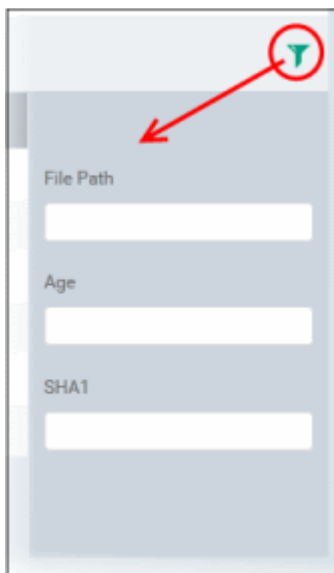
- Click the 'Trusted' tab

Device Name	Summary	Networks	Associated Profiles	File List	Exported CES Configs	MSI Installation State	Communication	Patch Management
<div style="display: flex; justify-content: space-between;"> Unrecognized Trusted Malicious </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Move To Unrecognized Move To Malicious Clean History For This File </div>								
FILE NAME	FILE PATH	AGE	SHA1	VERSION	ADMIN RATING	SIZE		
<input type="checkbox"/> Gui.dll	C:\Program Files (x86...	17 days	FCC7BBB50F12D8C6D0C932CAF47EF041148D8...	5.0.1441.7781	No	2.14 MB		
<input type="checkbox"/> qhttpserver.dll	C:\Program Files (x86...	17 days	BC6092EDE8358B96B4A14548681B8055A89E8B...	5.0.1441.7781	No	76.5 KB		
<input type="checkbox"/> ApplicationManagem...	C:\Program Files (x86...	17 days	27223CC1B9122AD07A2570BE3E25B0B9178B5E...	5.0.1441.7781	No	36 KB		
<input type="checkbox"/> CDMService.exe	C:\Program Files (x86...	17 days	B8C7EB5A4C7B1F657504C4A235E566FAE75514...	5.0.1441.7781	No	1.59 MB		
<input type="checkbox"/> CDMAgent.exe	C:\Program Files (x86...	17 days	CDC3D7DC2420249C2320F8C5D352CECEE5C3A...	5.0.1441.7781	No	1.58 MB		
<input type="checkbox"/> sc.exe	C:\Windows\System3...	2373 days	0B1F81F5E209FED6DF3255F6C820555CF17A83...	6.1.7600.16385 (win7...	No	44 KB		
<input type="checkbox"/> cdm_agent_kc13f5qk	C:\Users\Valentin\De...	13 days	71133DF3503227AFCF8ED3E4FFC3CDE588FF1		No	11.0 KB		

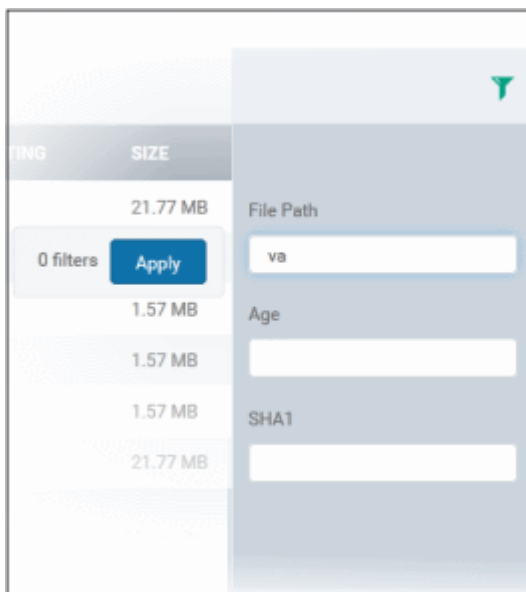
The 'Trusted ' List - Table of Column Descriptions	
Column Heading	Description
File Name	Displays the file name of the 'Trusted' item.
File Path	The installation location of the file at the endpoint
Age	The time from which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to Trusted Files list by the administrator.
Size	The size of the file.

Sorting, Search and Filter Options

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



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



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

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

Managing Trusted Files

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

Viewing and Managing Malicious Files on the Device

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

- Click the 'Malicious' tab


Device Name	Summary	Networks	Associated Profiles	File List	Exported CES Configs	MSI Installation State	Communication	Patch Management
Unrecognized Trusted Malicious								
<input type="button" value="Move To Unrecognized"/> <input type="button" value="Move To Trusted"/> <input type="button" value="Clean History For This File"/>								
FILE NAME	FILE PATH	AGE	SHA1	VERSION	ADMIN RATING	SIZE		
<input type="checkbox"/> consent.exe	C:\Windows\System32...	45 days	19A1D5E7FE8D57B332DF4A25D8F43E8377E31B72	6.0.6000.16386 (vista,...	Yes	80.5 KB		

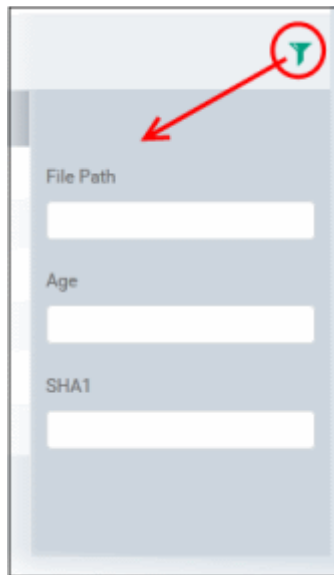
The 'Malicious Files' List - Table of Column Descriptions

Column Heading	Description
File Name	Displays the file name of the 'malicious' item.
File Path	The installation location of the file at the endpoint
Age	The time from which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file

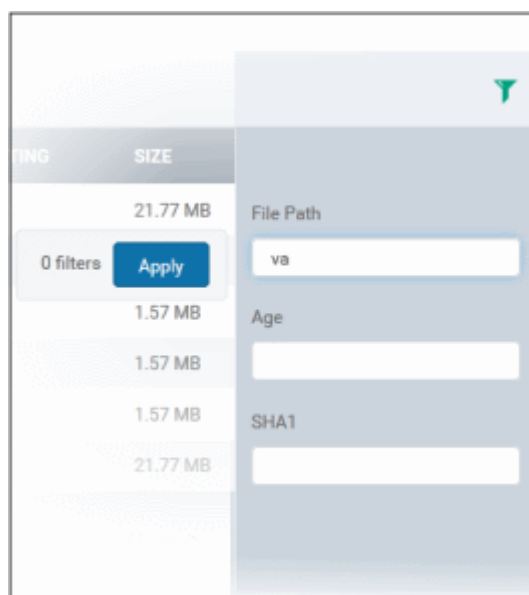
Admin Rating	Indicates whether the file was moved here by the administrator.
Size	The size of the unrecognized file.

Sorting, Search and Filter Options

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



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



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

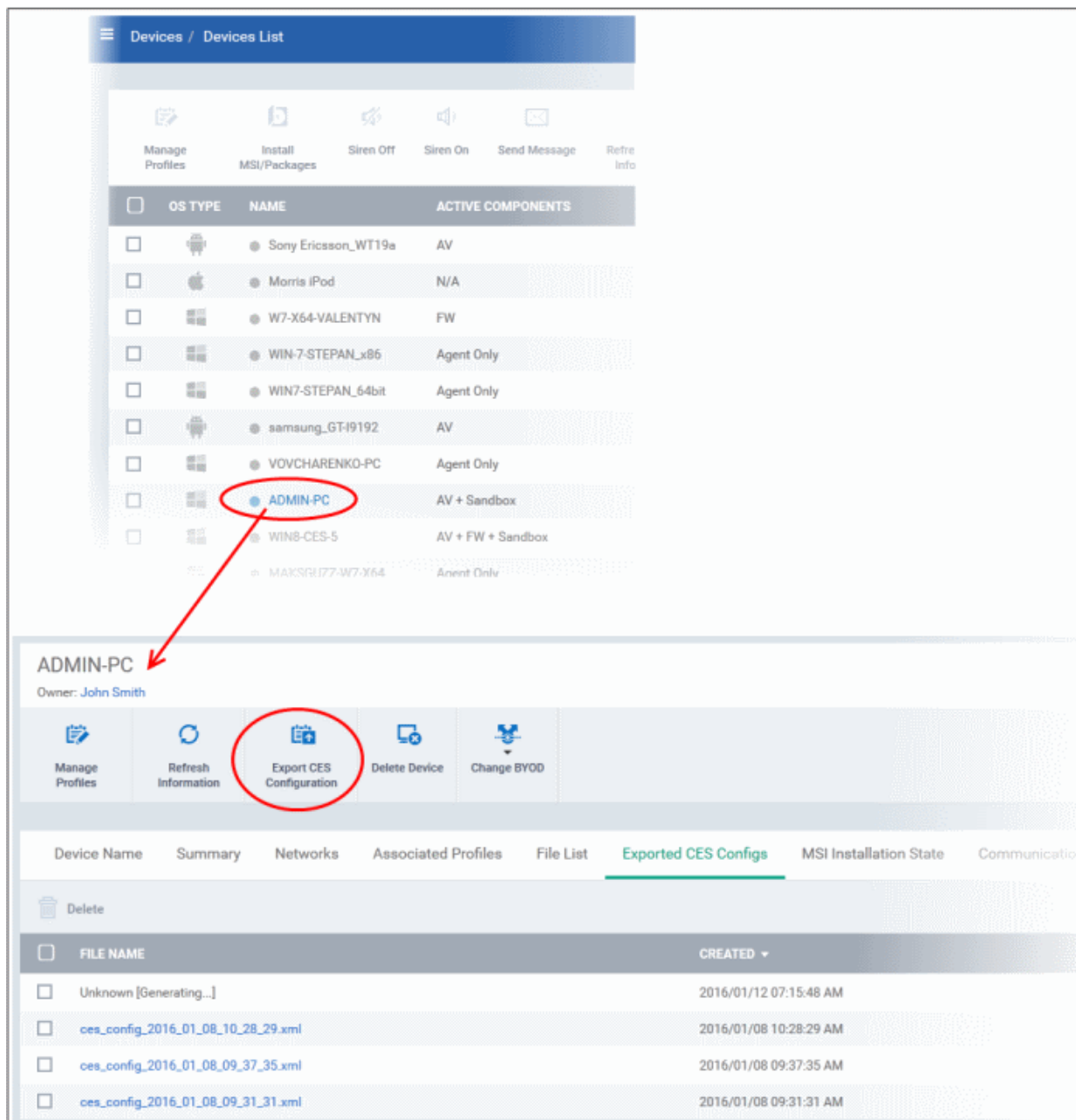
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Malicious Files

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

5.1.1.6. Viewing CES configurations exported from the Device

CDM allows you to create a new Windows profile using an existing CES configuration on an endpoint. To export a CES configuration, click on the Windows device from the list and click the 'Export CES Configuration' button at the top.



The CES configuration will be exported as an .xml file with date/time stamp suffix in the file name. The profile will be saved on the CDM server and can be viewed by clicking the 'Exported CES Configs' tab:

To view and manage exported profiles:

- Click 'Devices' and choose 'Devices List'
- Click the name of any Windows device, then select the 'Exported CES Configs' tab

Device Name	Summary	Networks	Associated Profiles	File List	Exported CES Configs	MSI Installation State	Communication	Patch Management
Delete								
<input type="checkbox"/>	FILE NAME				CREATED ▾			
<input type="checkbox"/>	ces_config_2016_01_12_07_16_55.xml				2016/01/12 07:16:55 AM			
<input type="checkbox"/>	ces_config_2016_01_08_10_28_29.xml				2016/01/08 10:28:29 AM			
<input type="checkbox"/>	ces_config_2016_01_08_09_37_35.xml				2016/01/08 09:37:35 AM			
<input type="checkbox"/>	ces_config_2016_01_08_09_31_31.xml				2016/01/08 09:31:31 AM			

The 'Exported CES Configs' 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 CES configuration was exported

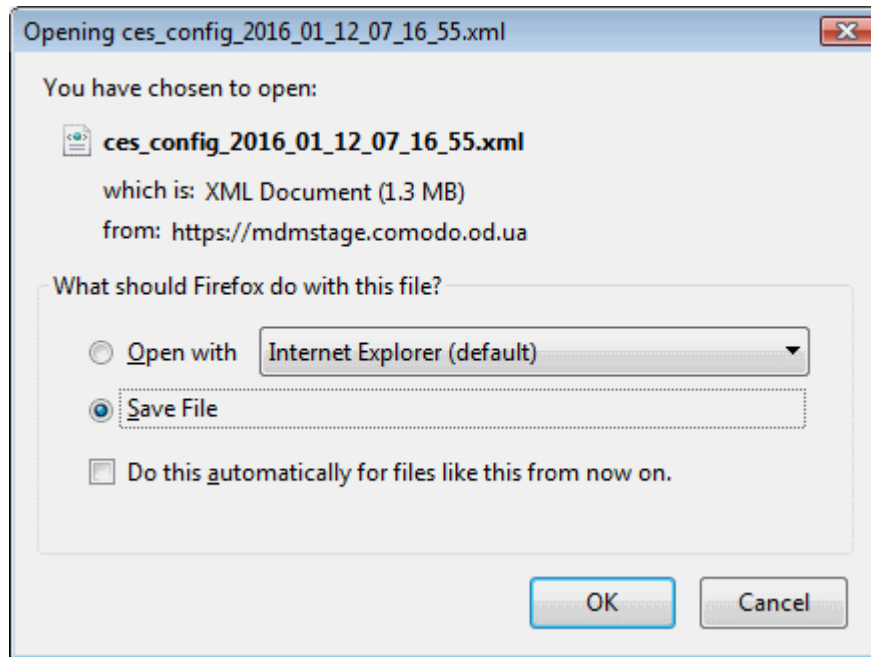
- Clicking on the column header sorts the items based on alphabetical or ascending/descending order of entries in that column.

To save the exported CES configuration

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

Device Name	Summary	Networks	Associated Profiles	File List	Exported CES Configs	MSI Installation State
Delete						
<input type="checkbox"/>	FILE NAME				CREATED ▾	
<input type="checkbox"/>	ces_config_2016_01_12_07_16_55.xml				2016/01/12 07:16:55 AM	
<input type="checkbox"/>	ces_config_2016_01_08_10_28_29.xml				2016/01/08 10:28:29 AM	
<input type="checkbox"/>	ces_config_2016_01_08_09_37_35.xml				2016/01/08 09:37:35 AM	
<input type="checkbox"/>	ces_config_2016_01_08_09_31_31.xml				2016/01/08 09:31:31 AM	

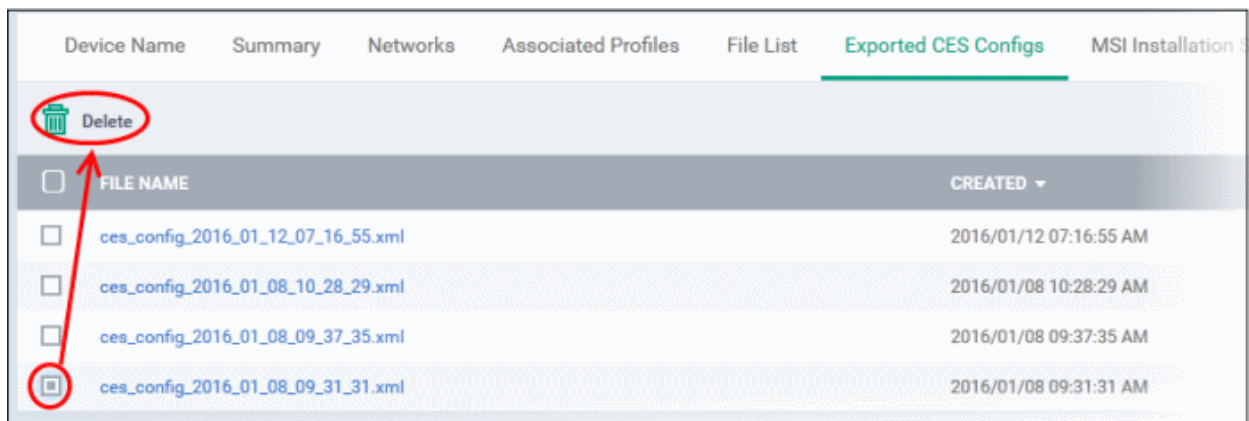
The 'Opening...' dialog will be displayed.



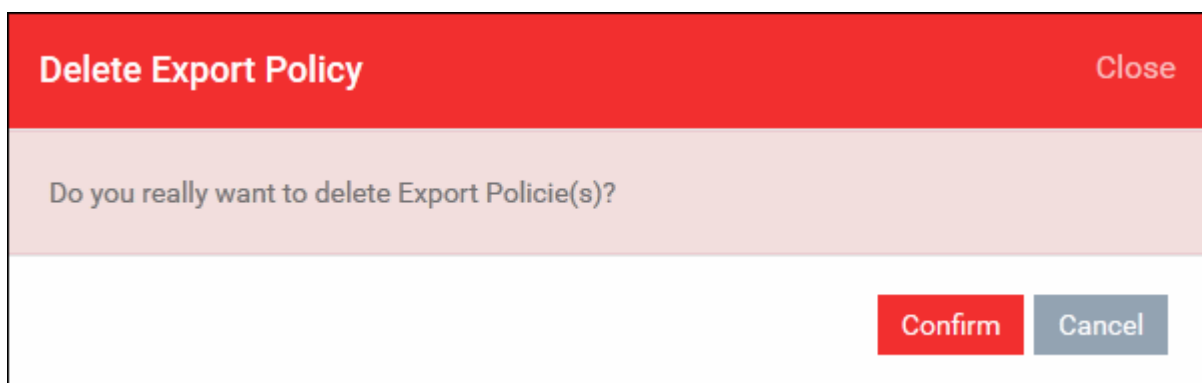
- Click 'OK' to download the file to the computer from which the CDM console is accessed and save it at a safe location.

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

- To delete a file from the list, select it and click 'Delete'



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

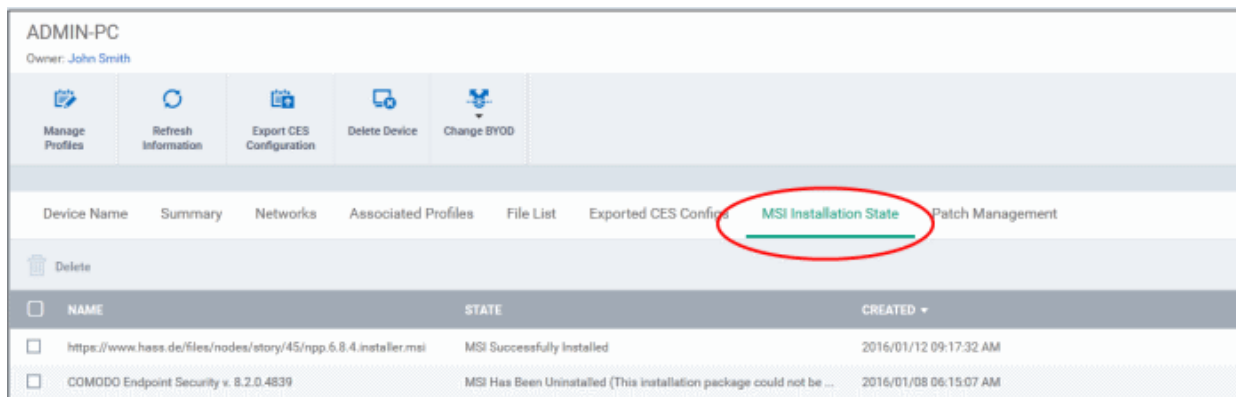


5.1.1.7. Viewing MSI files installed on the device through CDM

The 'MSI Installation State' screens displays the details of MSI packages that were installed via CDM. The installation of MSI packages can be done from the 'Devices List' interface. Refer to the section '[Installing Third Party MSI Packages on Windows Devices](#)' for more details.

To view MSI file installation list on the device

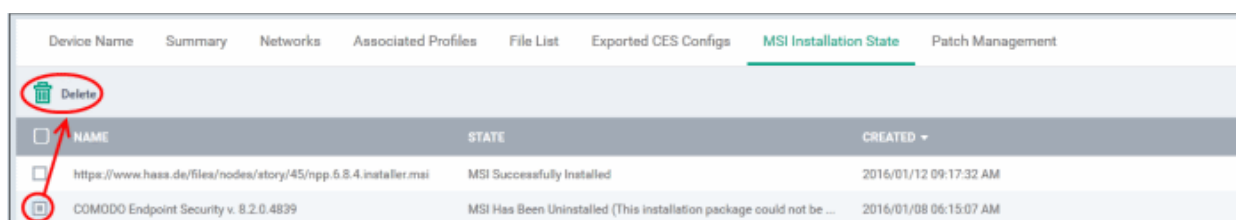
- Click 'Devices' and choose 'Devices List'
- Click the name of any Windows device, then select the 'MSI Installation State' tab



MSI Installation State - Table of Column Descriptions

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

- Clicking on the column header sorts the items based on alphabetical or ascending/descending order of entries in that column.
- To delete a file from the list, select it and click 'Delete'



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



5.1.1.8. Viewing and Installing Windows Patches

Windows machines have to be kept up-to-date with the latest patches in order to protect them from vulnerabilities and malicious attacks. The Patch Management feature in the 'Devices' interface allows administrators to view the list of installed patches on an endpoint and, if desired, to deploy new patches remotely. CDM maintains the latest record of available patches, determines which patches are appropriate and allows administrators to install multiple patches simultaneously.

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

Important Note: The Patch Management feature will be visible only if this is enabled in Settings > Extensions. Refer to the section '[Managing CDM Extension](#)' for more details.

To view and install patches on Windows endpoints

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


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

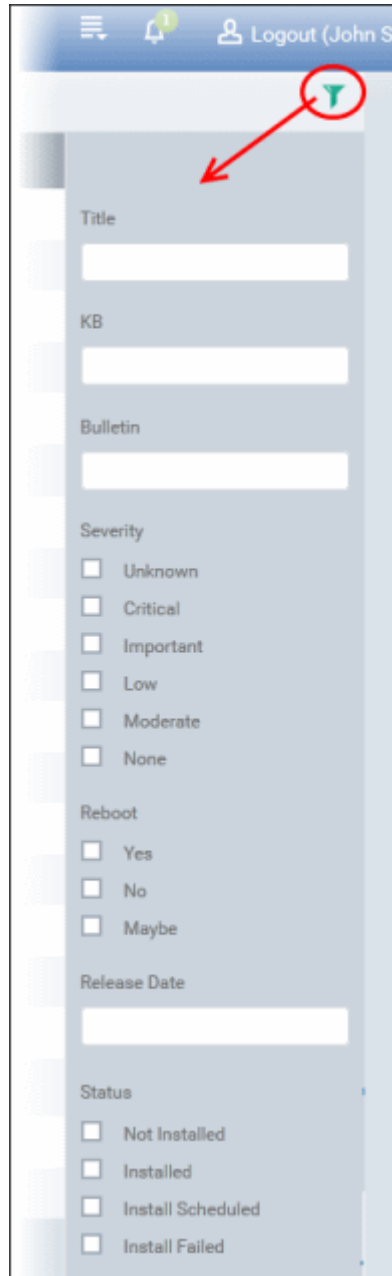
The screenshot displays the 'Patch Management' section for a device named 'ADMIN-PC'. The interface includes a sidebar with navigation options and a main content area with a table of installed patches. The table has the following columns: Title, KB, Bulletin, Severity, Reboot, Release Date, and Status. The table lists 20 patches, including updates for Microsoft .NET Framework, Windows Vista, and Windows 7. The status of each patch is indicated as 'Installed' or 'Not Installed'.

Patch Management Table - Column Descriptions	
Column Heading	Description
Title	The name of the patch
KB	Opens the Microsoft knowledge base article on the patch.
Bulletin	Opens the Microsoft TechCenter security bulletin on the patch.
Severity	Indicates the level of severity of the patch as determined by Microsoft. The severity levels are: <ul style="list-style-type: none"> Unknown Critical Important Low Moderate None
Reboot	Indicates whether a reboot is required after patch installation
Release Date	The date on which the patch was released by Microsoft

Status	Indicates whether the patch is installed or not on the endpoint
--------	---

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 patches or search for a specific patch, enter the details in part or full and /or select the check box and click 'Apply'.
 - Title - Filters the items based on the name of the patch
 - KB - Filters the items based on the KB number
 - Bulletin - Filters the items based on the entered bulletin details
 - Severity - Filters the items based on the selected severity level
 - Reboot - Filters the items based on the selected reboot option
 - Release Date - Filters the items based on the entered release date

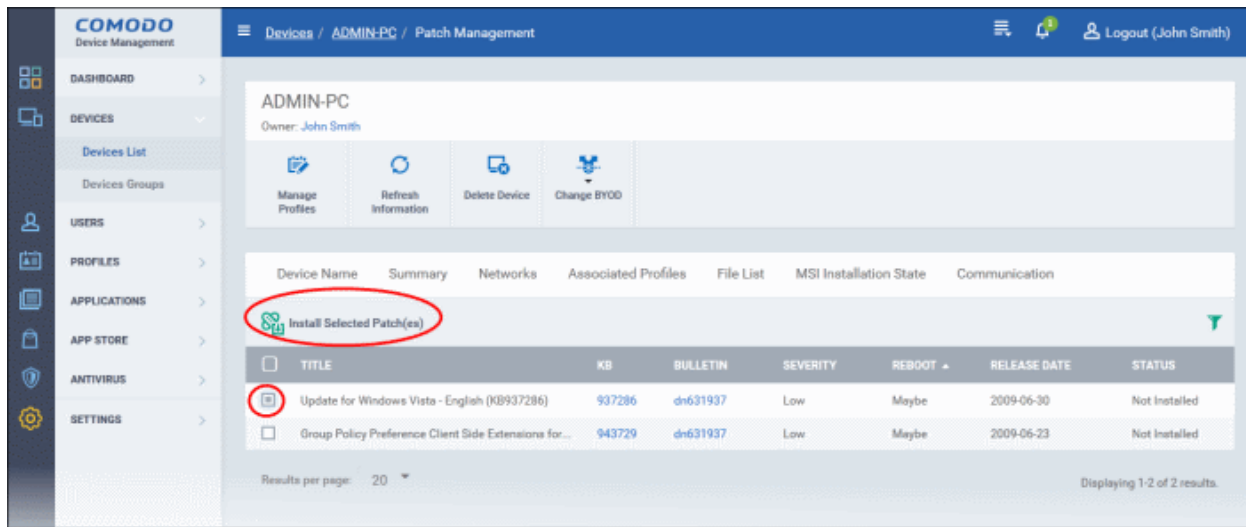
- Status - Filters the items based on the patch installed status

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

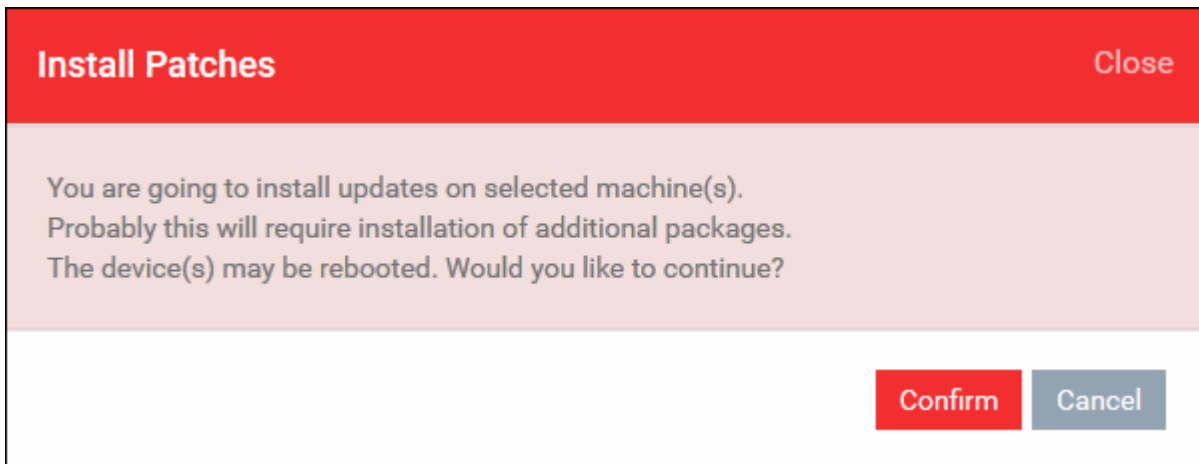
- To display all the items again, remove / deselect the search key from the filters and click 'Apply'.
- By default CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

To install patch(es) on an endpoint

- Identify and review patch(es) with a status of 'Not Installed'
- To simplify this, use the filter funnel to display only 'Not Installed' patches
- Select the check-box(es) next to the patches you wish to install
- Click 'Install Selected Patch(es)'



A warning dialog will be displayed.



- Click 'Confirm' to proceed with the installation

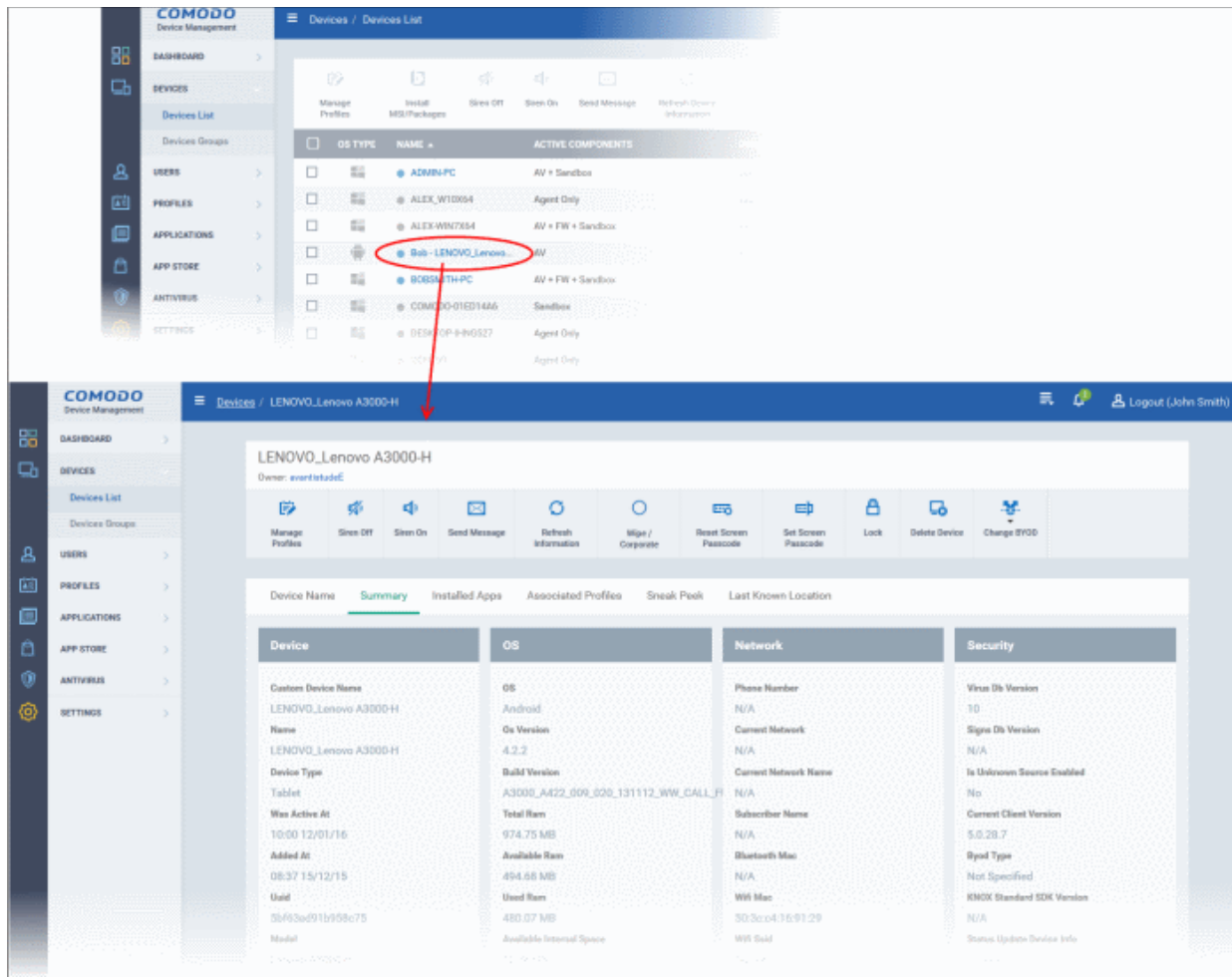
The command will be sent and the selected patch(es) will be installed on the endpoint.

5.1.2. Managing Android/iOS Devices

The administrator can view the complete hardware and software details of any enrolled mobile device and manage the installed applications and configuration profiles in effect on any individual device. Also, the administrator can send message to the device, raise an alarm to locate the device if it is lost or misplaced, remotely lock the device, view the current location of the device on the map, view the photographs picked up by the Sneakpeak feature and so on.

To view details of and manage an individual device

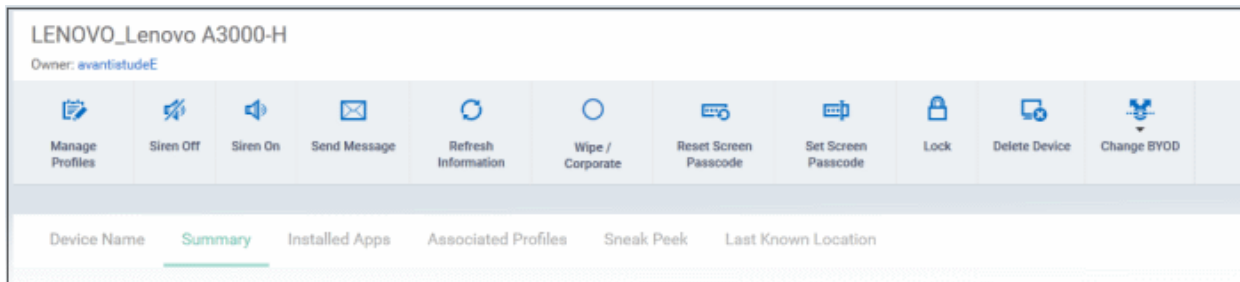
- Click 'Devices' and choose 'Devices List'
- Click the name of any Android/iOS device



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

- **Device Name** - Displays the name of the device and allows to change it for administrative purpose and easy management. Refer to the section [Viewing and Editing Device Name](#) for more details.
- **Summary** - Displays the general details of the device including device information, OS details, Network details and security configuration. Refer to the section [Viewing Summary Information](#) for more details.
- **Installed apps** - Displays a list of all the applications installed on the device and enables the administrator to manage the applications. Refer to [Managing Apps Installed on a Device](#) for more details. (Not applicable for Windows Devices).
- **Associated Profiles** - Enables the administrator to view the configuration profiles in effect on the device and to add new profiles or remove existing profiles. Refer to the section [Managing Profiles associated with the Device](#) for more details.
- **Sneak Peak** - Displays the pictures captured by the Sneak Peak feature of CDM. If enabled at the profile associated with the device, the Sneak Peak feature captures the photographs the possessor that tries to login to the lost or stolen device using guessed passcodes. This enables the administrator to identify the possessor of the device lost by or stolen from an end-user. Refer to the section [Viewing Sneak Peak Pictures](#) for more details. (Not applicable for Windows Devices).
- **Last Known Location** - Displays the location of the device during its last polling cycle, on a map. The administrator can also view the current location of the device by updating the location information. Refer to the section [Viewing the Location of the Device](#) for more details.

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



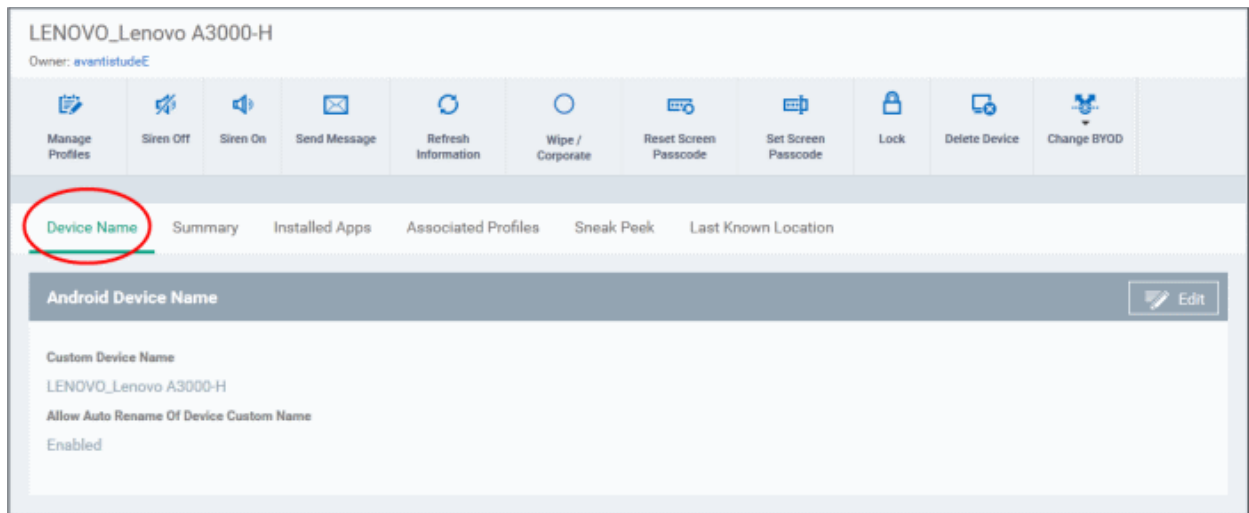
- **Manage Profiles** - Allows you to add or remove device profiles. Refer to the section **Assigning Configuration Profiles to Selected Devices** for more details.
- **Siren Off/Siren On** - Allows you to generate an alarm on the device to locate it, if it is misplaced. Refer to the section **Generating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

5.1.2.1. Viewing and Editing Device Name

The name of the device assigned by user or if no name was assigned, the model number of the device. You can change this to a more friendly name if required. Please note the new name will be applied in CDM only and will not change the name on the device.

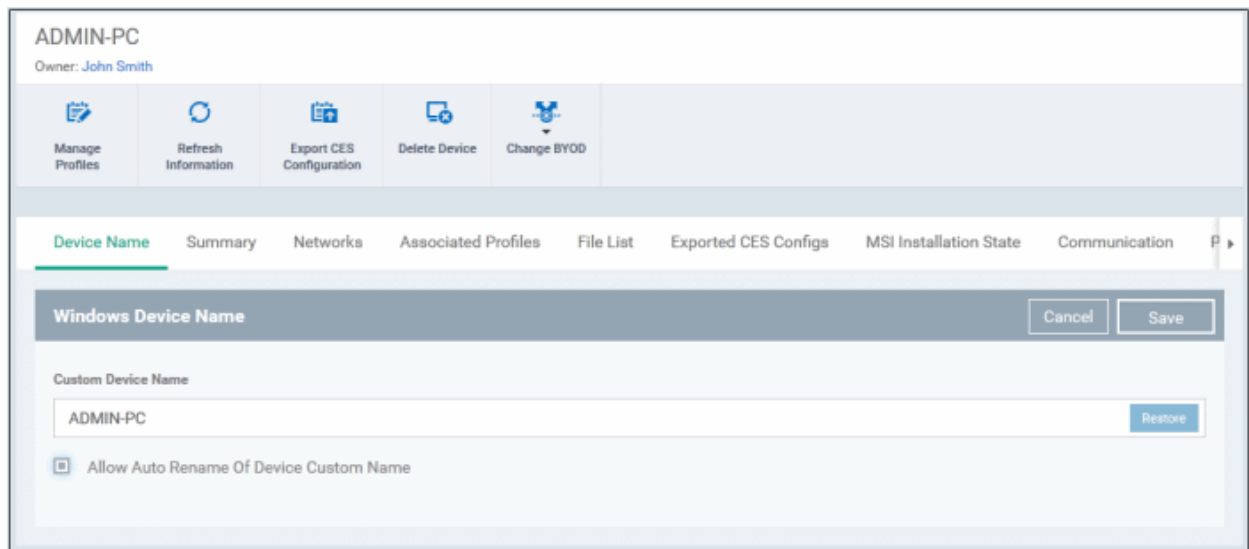
To change the device's name

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



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

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



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

The device will be listed with its new name. The 'Restore' button at the right in the field restores the device's name as it was at the time of enrollment.

5.1.2.2. Viewing Summary Information

The 'Summary' tab in the device details interface displays the general information of the device.

To view the device information summary

- Click 'Devices' and choose 'Devices List'
- Click the name of any Android/iOS device. By default, the 'Device Summary' will be displayed, else click the 'Summary' tab.

LENOVO_Lenovo A3000-H
Owner: avantistudeE

[Manage Profiles](#)
[Siren Off](#)
[Siren On](#)
[Send Message](#)
[Refresh Information](#)
[Wipe / Corporate](#)
[Reset Screen Passcode](#)
[Set Screen Passcode](#)
[Lock](#)
[Delete Device](#)
[Change BYOD](#)

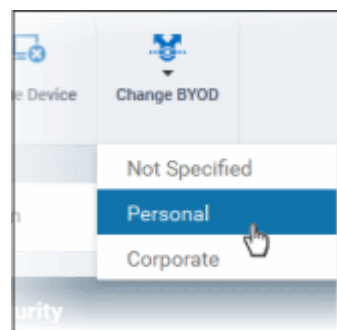
[Device Name](#)
[Summary](#)
[Installed Apps](#)
[Associated Profiles](#)
[Sneak Peek](#)
[Last Known Location](#)

Device	OS	Network	Security
Custom Device Name LENOVO_Lenovo A3000-H	OS Android	Phone Number N/A	Virus Db Version 10
Name LENOVO_Lenovo A3000-H	Os Version 4.2.2	Current Network N/A	Signs Db Version N/A
Device Type Tablet	Build Version A3000_A422_009_020_131112_WW_CAL	Current Network Name N/A	Is Unknown Source Enabled No
Was Active At 10:58 12/01/16	Total Ram 974.75 MB	Subscriber Name N/A	Current Client Version 5.0.28.7
Added At 08:37 15/12/15	Available Ram 475.51 MB	Bluetooth Mac N/A	Byod Type Not Specified
Uuid 5bf63ed91b958c75	Used Ram 499.24 MB	Wifi Mac 50:3c:c4:16:91:29	KNOX Standard SDK Version N/A
Model Lenovo A3000-H	Available Internal Space 12.36 GB	Wifi Ssid "Airnet"	Status Update Device Info Updated
IMEI 862589025614495	Total Internal Space 13.25 GB	Roaming No	Device Info Refreshed At 10:58 12/01/16
Serial Number YSRODABQDABH55LZ	Available Sdcard Space 0 MB	Cellular Technology Unknown	Passcode Enabled Inactive
Battery Level 59 %	Total Sdcard Space 0 MB		Data Protection Inactive
BYOD Status Not Specified			

- **Device Summary** - Provides device details such as brand, model and International Mobile Equipment Identification (IMEI) number.
- **OS Summary** - Provides details about the device Operating System (OS).
- **Network Summary** - Provides details about the mobile and WiFi networks to which the device is connected.
- **Security info** - Provides details about device storage encryption and passcode settings for screen unlock

By default, the BYOD status of a newly enrolled device will be 'Not Specified'. To specify the BYOD type, choose the type from the 'Change BYOD' drop-down at the top right. The available options are:

- Personal
- Corporate



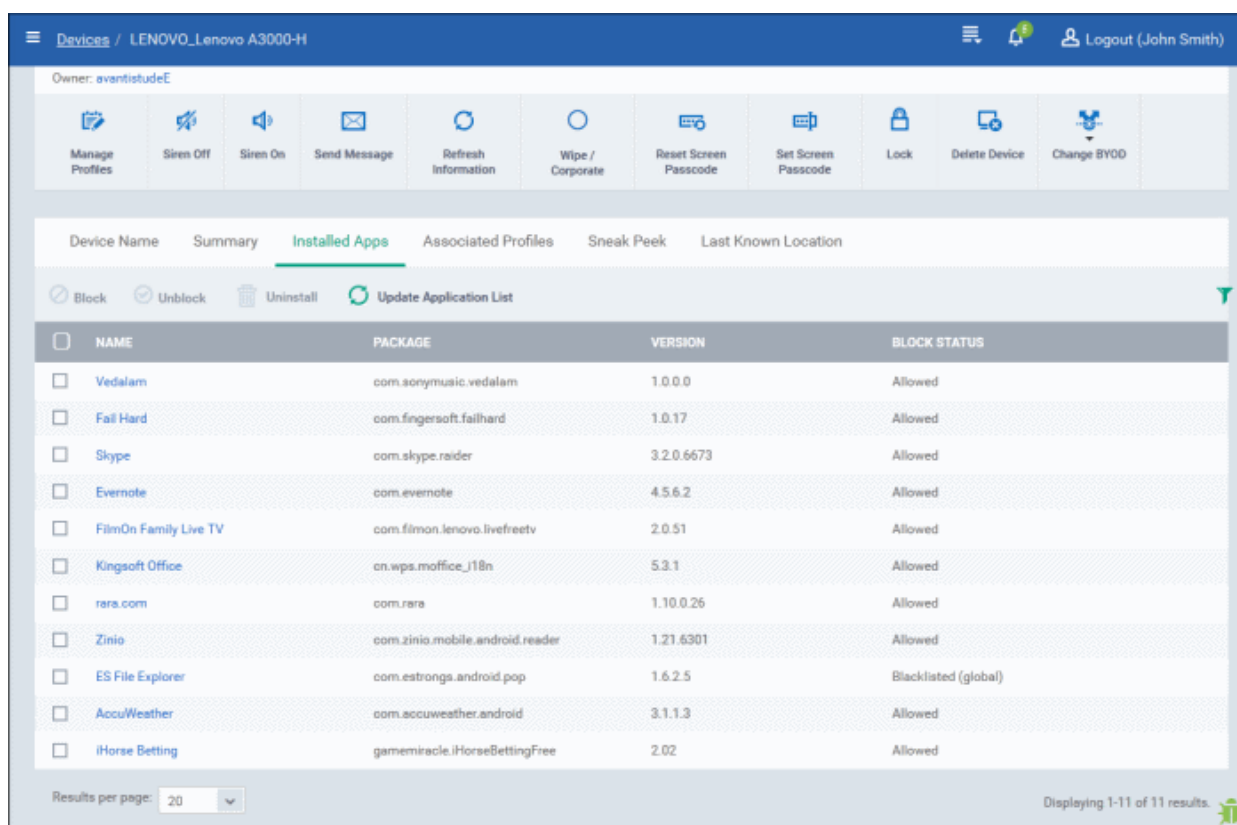
5.1.2.3. Managing Installed Applications

The 'Installed Apps' tab in the device details interface displays a list of all the applications installed on the device and allows the administrator to block/unblock apps as required and uninstall selected apps that are found suspicious, not trust worthy, or junk apps from the device. The administrator can also identify the other enrolled devices, in which the same application has been installed, in order to replicate the corrective action, executed on the selected device.

Note: The 'Installed Apps' tab is not available for Windows Endpoints.

To manage installed apps

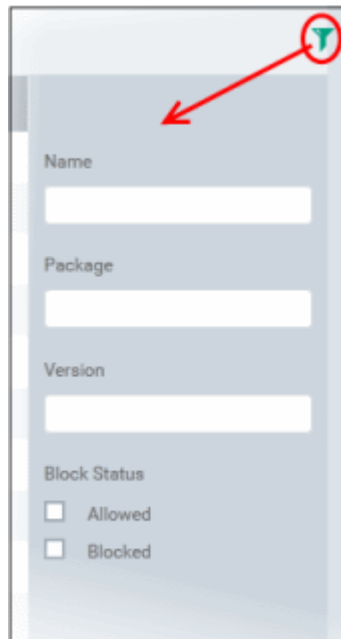
- Click 'Devices' and choose 'Devices List'
- Click the name of any Android/iOS device then select the 'Installed Apps' tab



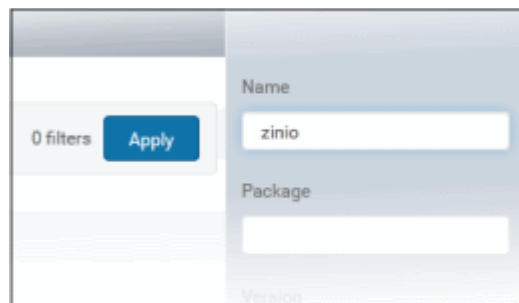
Installed Apps - Column Descriptions	
Column Heading	Description
Name	The name of the application. Clicking the name of the application will open the ' Devices ' interface, listing only the devices in which the same application is installed. This makes it easier for the administrator to identify the devices and block or uninstall a suspicious, malicious or junk application from other devices too.
Package	Indicates the source of the application, i.e downloaded android/.iOS package, from which the application has been installed.
Version	Indicates the version of the application.
Block Status	Indicates whether the application is allowed to run, blocked, blacklisted or in the process of uninstalling.

Sorting and Filtering Options

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



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

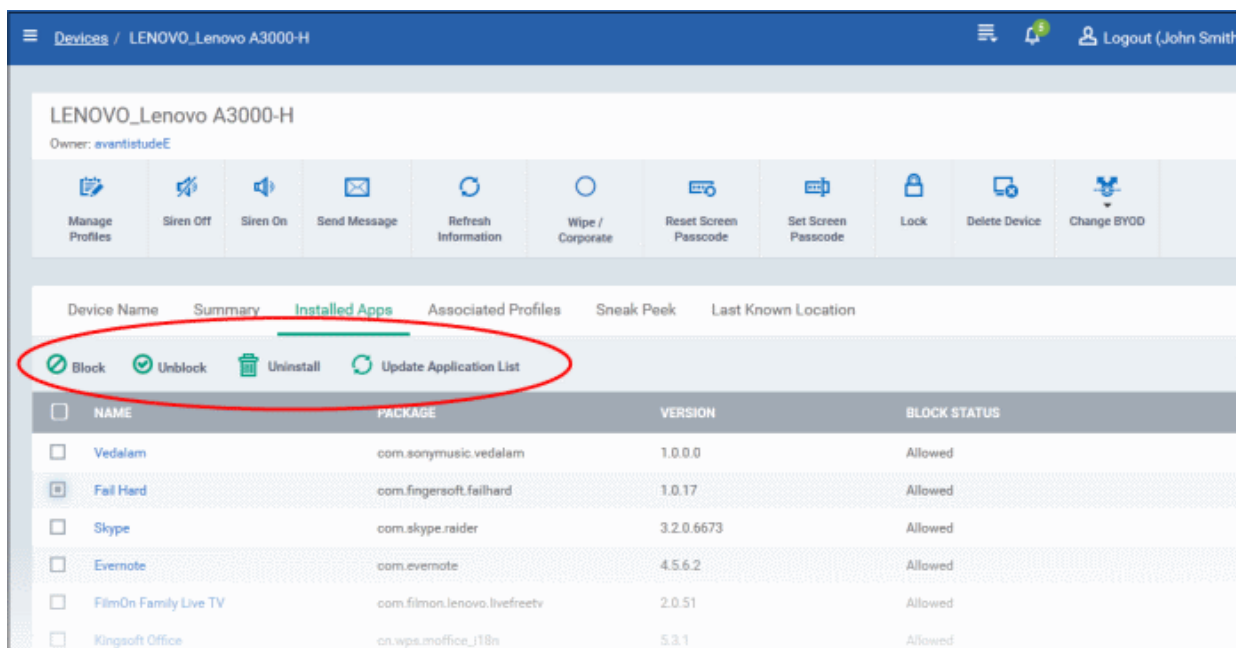


- To filter the list to display only the allowed applications or blocked applications, choose the option under 'Block Status'. You can use any combination of filters at-a-time to search for specific devices.

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CDM 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.

Blocking, unblocking, uninstalling and updating application list

- To block unwanted app(s) from execution in the device, select the app(s) and click 'Block'.
- To release blocked apps(s) and allow them to run, select the blocked app(s) and click 'Unblock'
- 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 and the app will be immediately blocked. Upon user seeing the notification and clicking 'Uninstall' from the notification, the app will be uninstalled from the device.



- Normally the list of apps in a device is updated to CDM every 24 hrs. To update the list immediately, click 'Update Application List'.

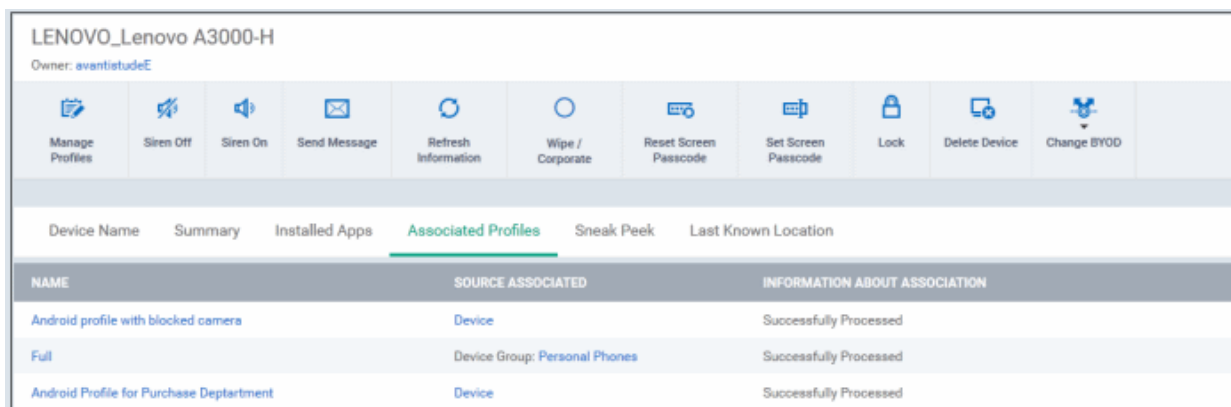
5.1.2.4. Viewing and Managing Profiles Associated with the Device

The 'Associated Profiles' tab displays a list of configuration profiles in effect on the device/endpoint. It also allows the administrator to add or remove profiles to the device. If multiple profiles are associated with the device, the most restrictive policy will be applied. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

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

To view and manage associated profiles

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



Associated Profiles - Column Descriptions	
Column Heading	Description
Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section Editing Configuration Profiles for more details.
Source Associated	<p>Indicates the source through which the profile has been applied to the device. Configuration profiles are applied to a device in different ways:</p> <ul style="list-style-type: none"> • Profiles can be directly applied to the device. Refer to the section Assigning Configuration Profiles to Selected Devices for more details • The profiles applied to a user is deployed to all the devices belonging to the user. Refer to the section Assigning Configuration Profile(s) to a Users' Devices for more details • The profiles applied to a user group is deployed to all the devices belonging to all the users in the group. Refer to the section Assigning Configuration Profile to a User Group for more details • The profiles applied to a device group is deployed to all the member devices in the group. Refer to the section Assigning Configuration Profile to Device Groups for more details <p>Clicking on the source opens the respective details interface.</p>
Information about Association	Indicates the status of profile application to the device.

Adding or Removing Profiles

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

5.1.2.5. Viewing Sneak Peak Pictures to Locate Lost Devices

The 'Sneak Peak' tab displays the photographs grabbed by the device through the 'Sneak Peak' feature.

The 'Sneak Peak' 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 Peak feature can be enabled in the device profile along with the threshold of 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).

The administrator can view Sneak Peak images by going to 'View Device' > 'Sneak Peak'.

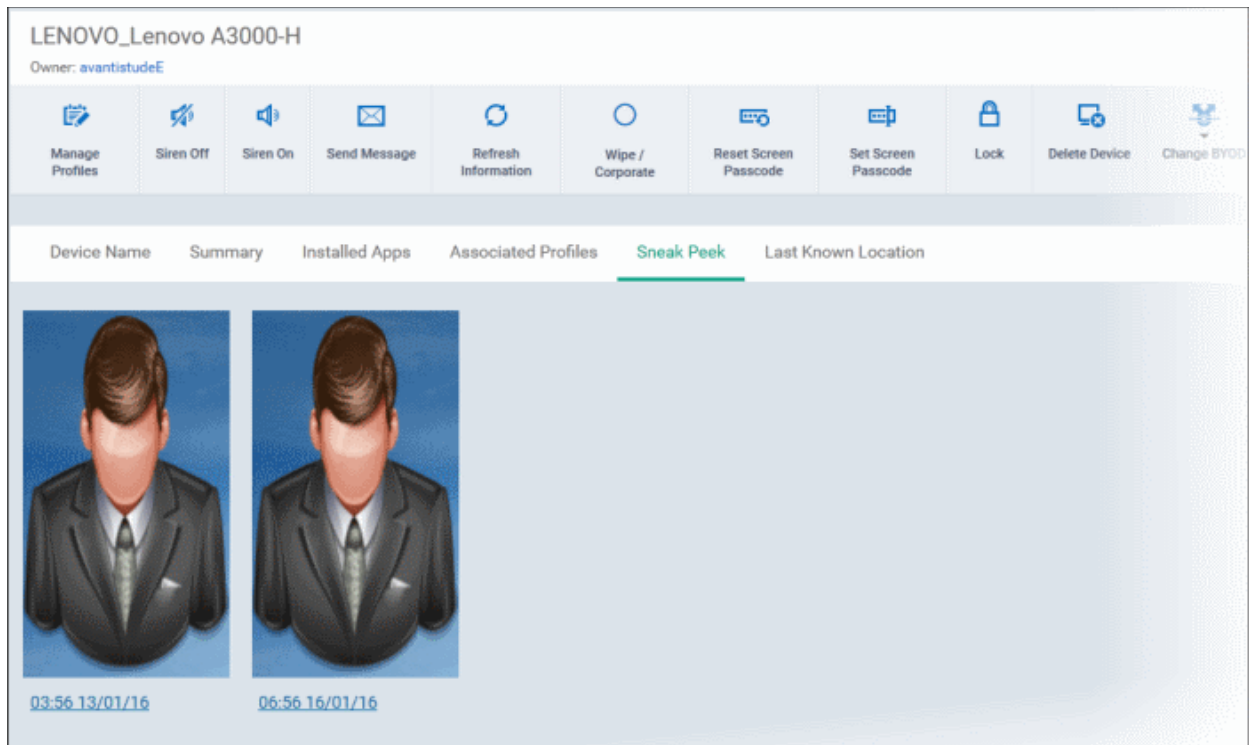
If the front camera is not available on the device, a photograph is taken using the rear facing camera.

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

To view Sneak Peak pictures

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

The photographs collected for wrong password entries will be displayed.



Note: The images shown above are for illustration purposes only. The actual photographs picked-up by the device camera will be displayed in the interface.

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

LENOVO_Lenovo A3000-H Close

Latitude	Longitude	Date
13.0301814	80.2380583	07:17 13/01/16

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

5.1.2.6. Viewing the Location of the Device

The 'Last Known Location' tab displays the location of the device in a map, during the last polling time of the CDM agent. The can view the current location of the device by updating the details from the same interface. This is useful if the phone is lost or stolen or if the administrator wishes to track the device for other reasons.

To view the location

- Click 'Devices' and choose 'Devices List'

- Click the name of any Android / iOS device then select the 'Last Known Location' tab

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

Provider	Longitude	Latitude	Accuracy	Date
network	80.2380202	13.0301474	39	07:47 13/01/16

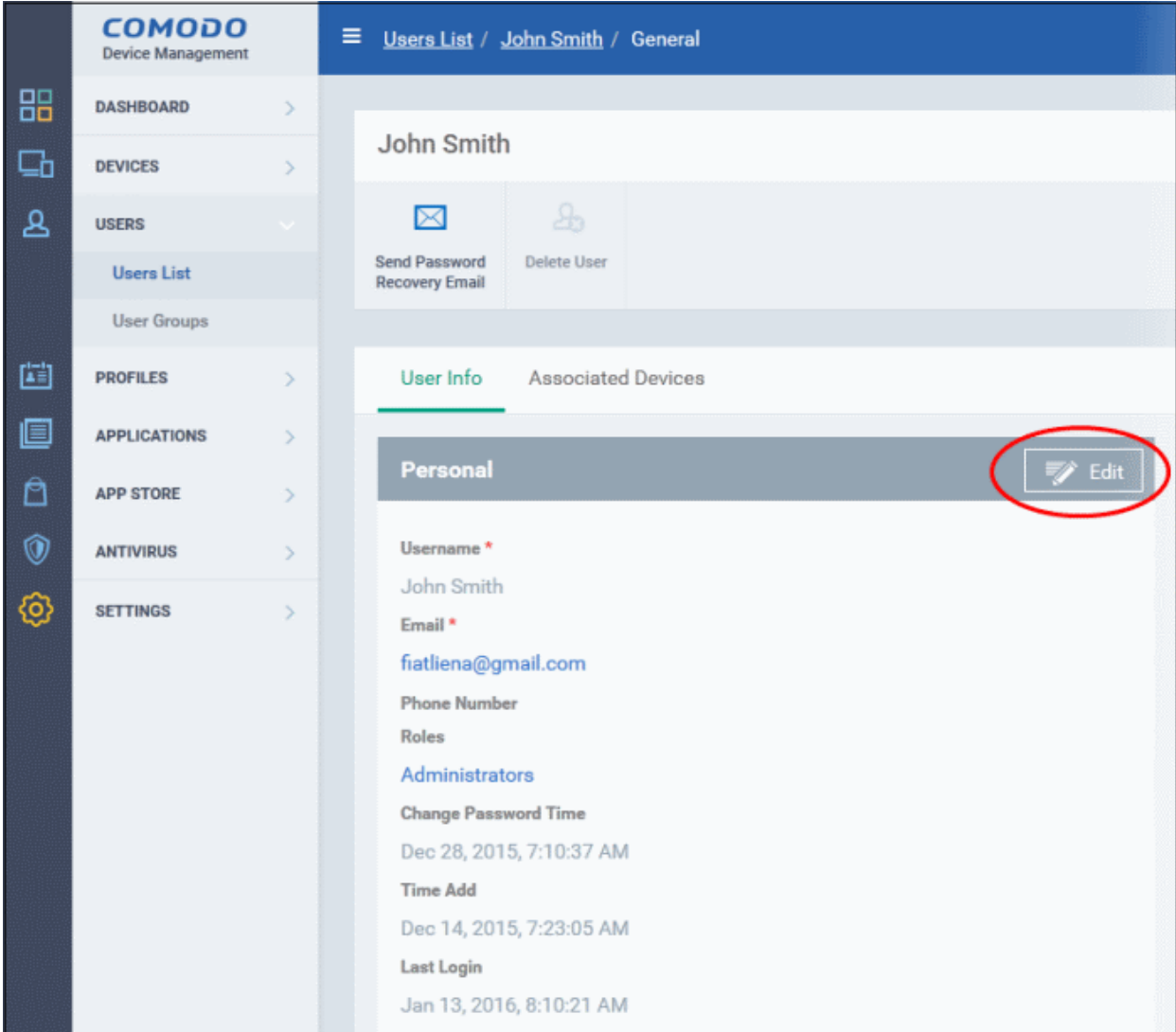
- To view the current location of the device, click 'Update'.
- To update the device location device instantly using device GPS, click 'Locate by force GPS'.

5.1.3. Viewing the User Information

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

To view the user information of a device

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



The screenshot shows the Comodo Device Manager interface. On the left is a navigation sidebar with options: DASHBOARD, DEVICES, USERS (expanded to show Users List and User Groups), PROFILES, APPLICATIONS, APP STORE, ANTIVIRUS, and SETTINGS. The main content area is titled 'Users List / John Smith / General'. It features a header for 'John Smith' with two action buttons: 'Send Password Recovery Email' and 'Delete User'. Below this are two tabs: 'User Info' (selected) and 'Associated Devices'. The 'User Info' tab shows a 'Personal' section with an 'Edit' button circled in red. The user details listed are: Username * (John Smith), Email * (fiatliena@gmail.com), Phone Number, Roles, Administrators, Change Password Time (Dec 28, 2015, 7:10:37 AM), Time Add (Dec 14, 2015, 7:23:05 AM), and Last Login (Jan 13, 2016, 8:10:21 AM).

- Click the 'Edit' button to modify user details. For more details on this area, see '[Viewing the Details of the User](#)' section.

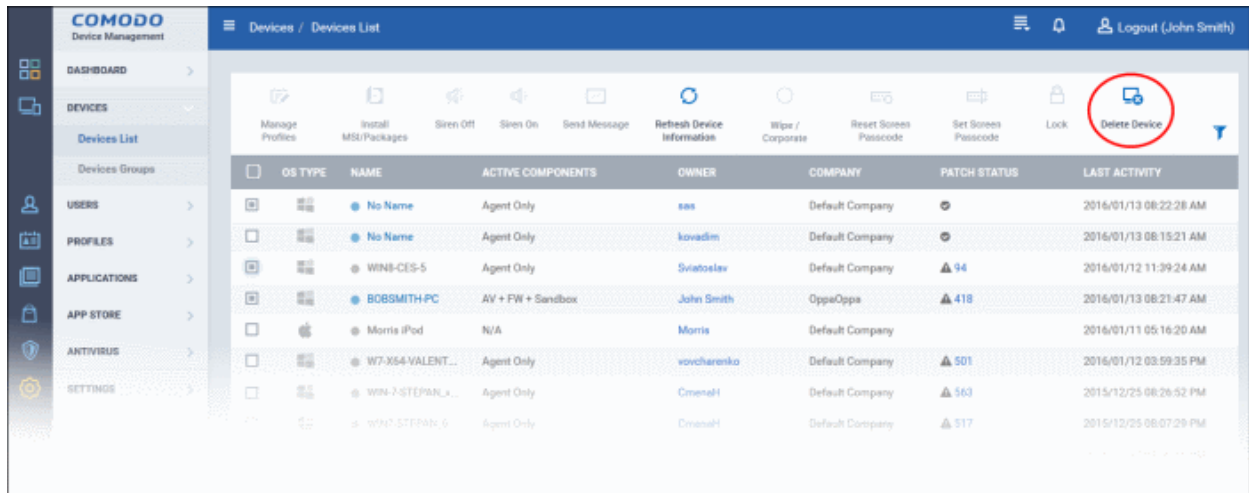
5.1.4. Removing a Device

The devices that no longer require management can be removed from CDM through the 'Devices' interface.

Warning: Once a device is de-enrolled, the CDM agent configuration profiles will be automatically wiped and all the apps installed and managed by CDM will be uninstalled from the device. The CDM app can also be manually removed from the devices by the users. If the device needs to be re-added for management, a new token should be sent to user and the device is to be re-enrolled as explained in the section [Adding Devices for Management](#).

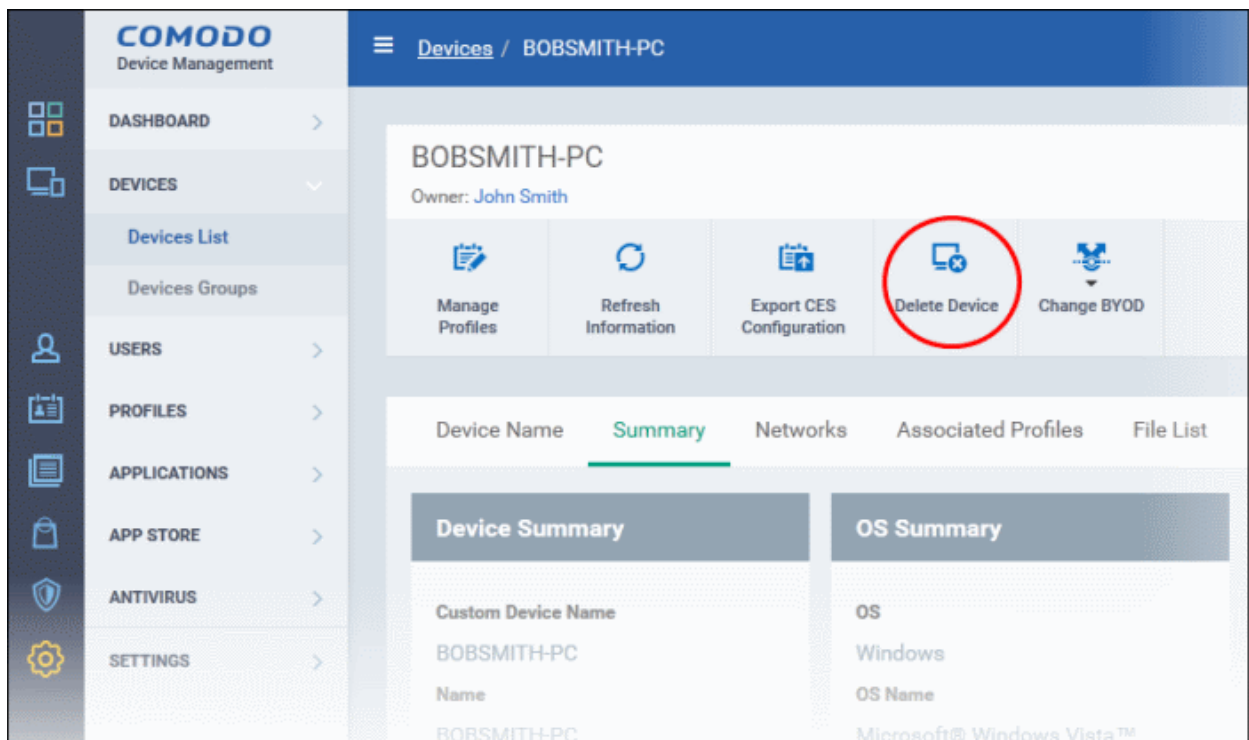
To remove a device from CDM

- Click 'Devices' and choose 'Devices List'
- Select the device(s) to be removed from the list
- Click 'Delete Device' from the options at the top

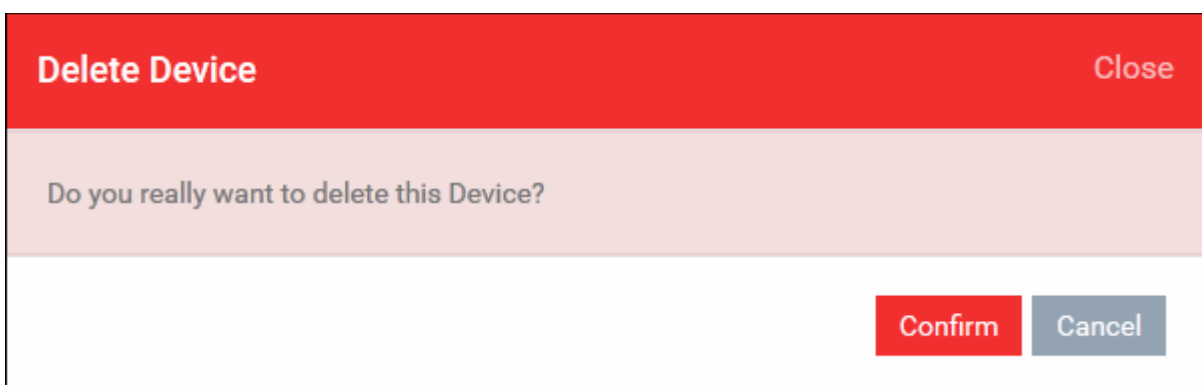


Alternatively, you can remove a device from its device details interface.

- Click 'Devices' and choose 'Devices List'
- Click on the name of the device to be removed to open the device details interface
- Click 'Delete Device' from the options at the top



- Click 'Confirm' to remove the device



The device will be removed from CDM.

To remove CDM app on Android devices

- Navigate to 'Settings' > 'Apps'
- Tap 'Comodo DM'
- Tap the 'Uninstall' button.

The CDM app will be removed from the device.

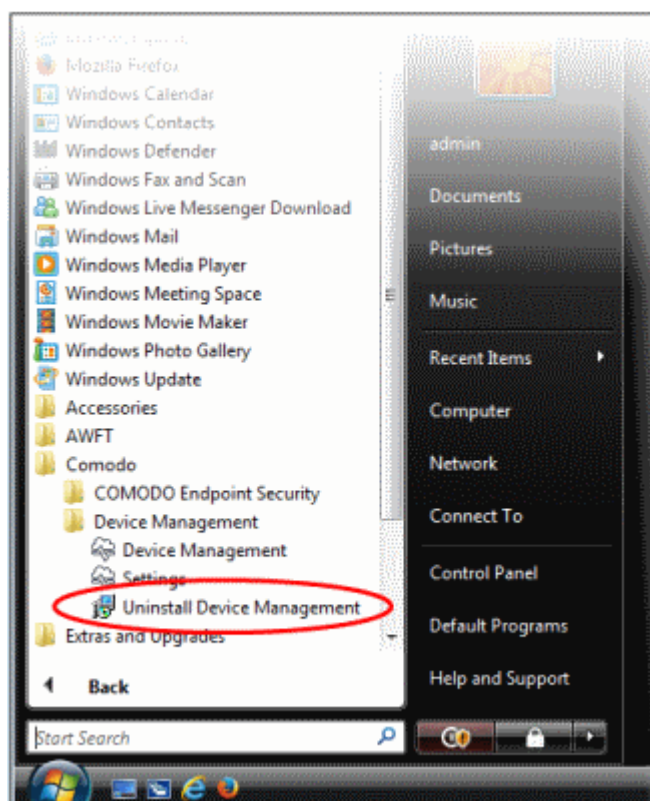
To remove CDM profile from iOS devices

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

The CDM profile will be removed from the device.

To remove CDM agent from Windows Endpoints

- Click Start > All Programs > Comodo > Device Management > Uninstall Device Management and follow the Uninstallation Wizard.



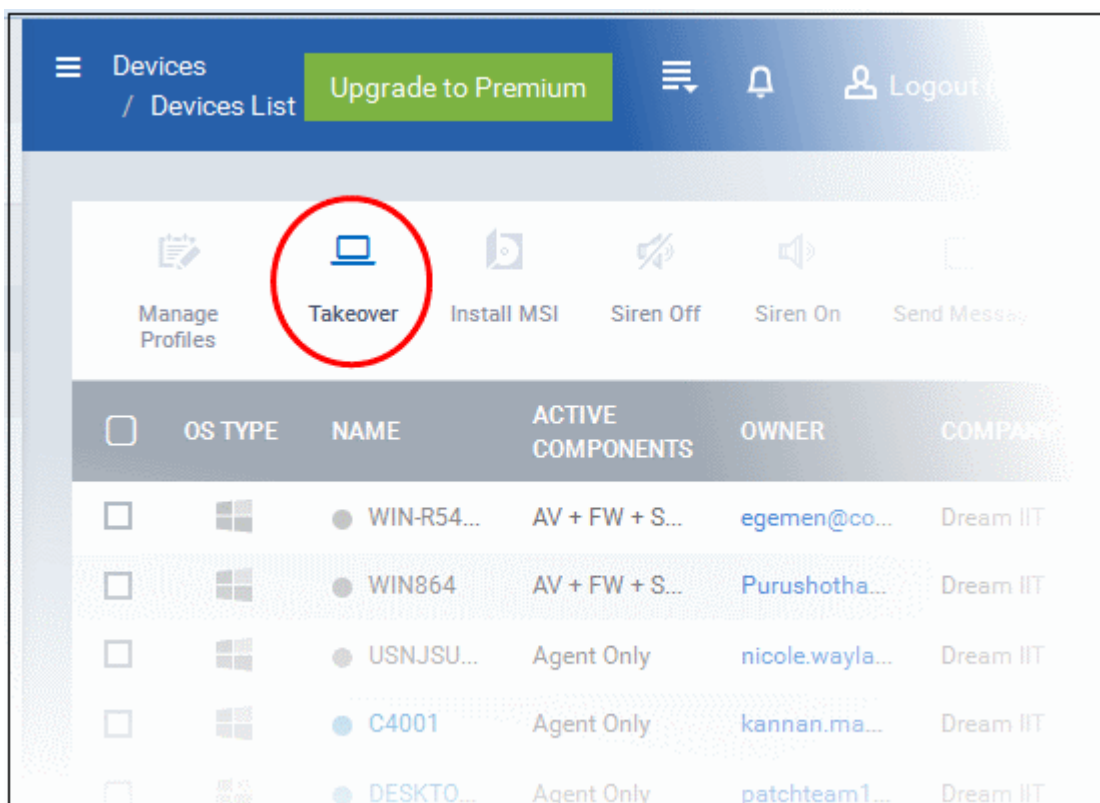
Note: You have to uninstall CES separately from the endpoint.

5.1.5. Remote Management of Windows Devices

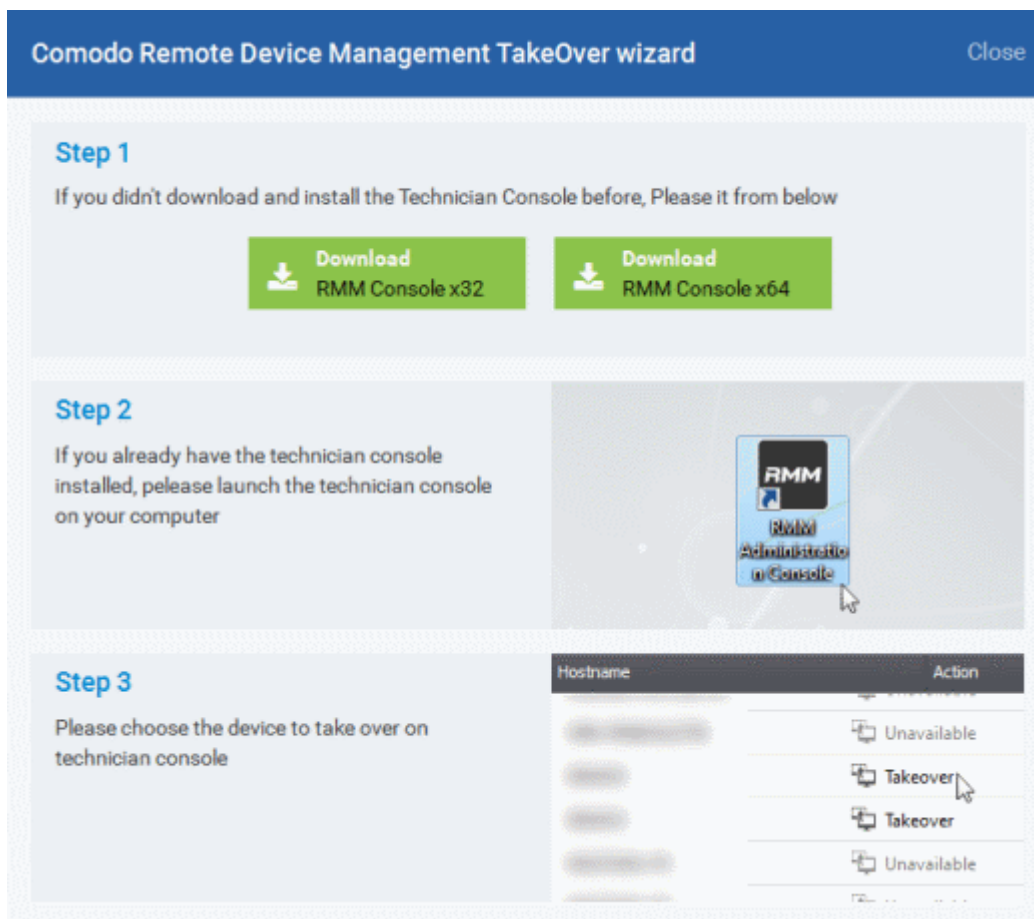
Comodo's Remote Monitoring and Management (RMM) grants administrators complete visibility and control over the system they manage. RMM is available for C1 customers and they can takeover Windows devices via remote desktop using the RMM administrative console. In order to that, administrators should:

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

To download the RMM admin console, click the 'Takeover' button from the devices list screen



The 'Remove Device Management Takeover Wizard' will be displayed



- Download the appropriate RMM Console and install it. If you already have it, then open the RMM administrative console
- Click 'Takeover' from the Devices screen of the RMM admin console.

Please note the RMM extension should be 'On'. Refer to the section '[Managing CDM Extensions](#)' for more details.

For more details about RMM, refer to the guide at <https://help.comodo.com/topic-289-1-719-8539-Introduction-to-Remote-Monitoring-and-Management-Module.html>.

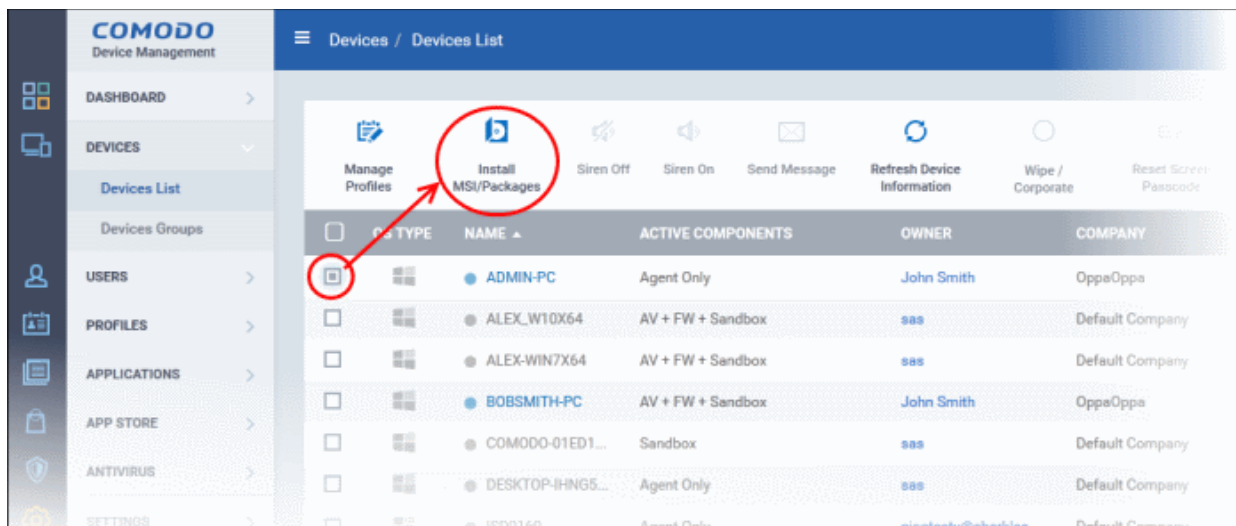
5.1.6. Remotely Installing Packages onto Windows Devices

CDM allows administrators to install Comodo applications such as Comodo Endpoint Security, RMM agent and other third-party MSI packages from the devices list screen.

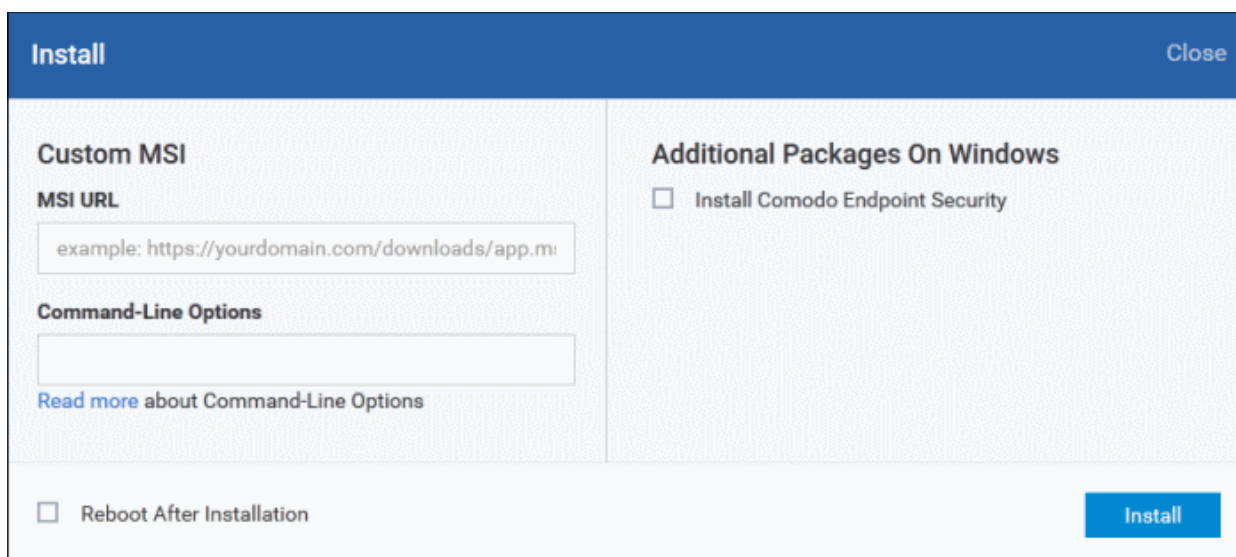
Note: The option to install RMM agent onto Windows endpoints is available for administrators that have logged in via Comodo One interface for managing devices.

To install MSI / CDM packages

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



The 'Install' screen will be displayed.



The CDM packages that are available for installation onto endpoints will be displayed on the right side and on the left side you can provide the third-party MSI package URL and command-lines (if required).

- [Installing CDM Packages](#)
- [Installing Third Party MSI Packages](#)

To install CDM packages

- Select the application under 'Additional Packages on Windows' (currently only Comodo Endpoint Security is available).
- Select the 'Reboot after Installation' check box if you want the endpoint to automatically restart after the completion of installation.
- Click the 'Install' button

The command to install will be sent from CDM for the process to begin and after the CES installation is completed, the security components that are active depends on the applied profile. Refer to the sections [Assigning Configuration Profiles to Selected Devices](#), [Assigning Configuration Profile\(s\) to a Users' Devices](#), [Assigning Configuration Profile to a User Group](#) and [Assigning Configuration Profile to Device Groups](#) for more details.

To install third-party MSI packages

- In the 'MSI URL' field, enter the URL of the MSI installer in full 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 after Installation' check box if you want the endpoint to automatically restart after the completion of installation.

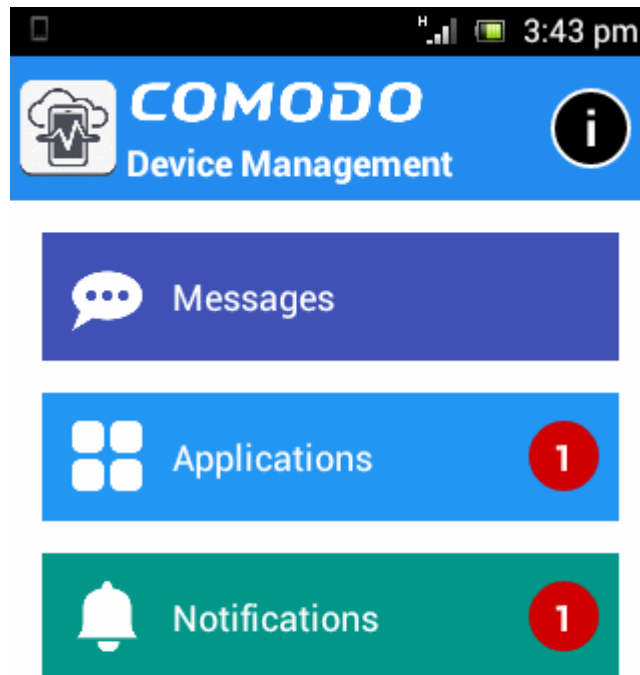
The command to install will be sent from CDM for the installation process to begin.

5.1.7. Installing Apps on Android/iOS Devices

CDM 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 CDM **App Store**. The sync between the CDM server and the devices takes place every 24 hours, or immediately if 'Inform Devices Now' clicked in the 'App Catalog' interface. For more details on uploading application packages to the CDM App Store, refer to the section **App Store**.

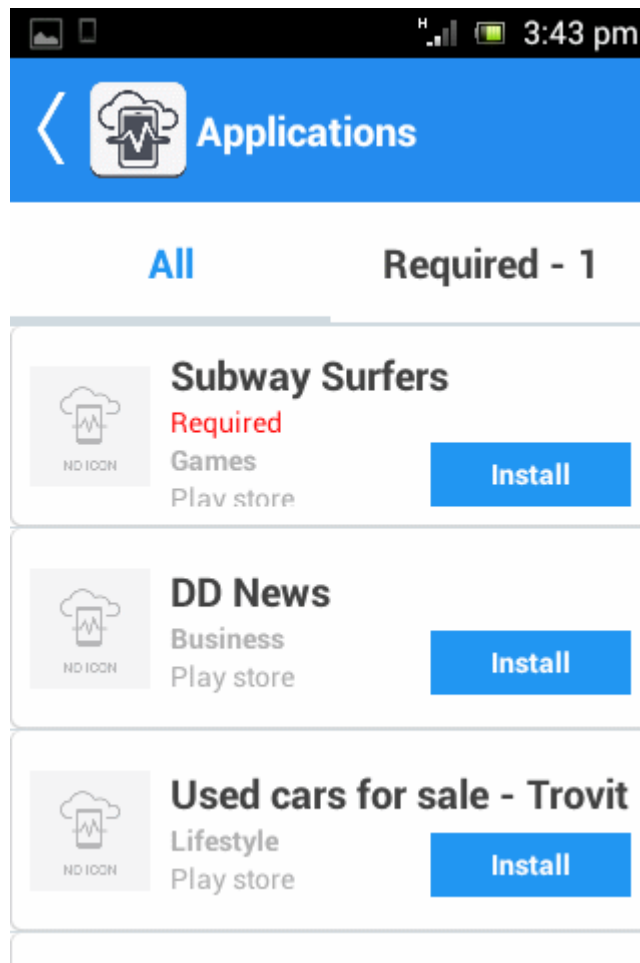
The list of Google Play Store/App Store Apps and the Custom/Enterprise Applications that are added to the CDM App Store can be viewed from any enrolled device and installed on the device.

The 'Applications' stripe in the CDM app on the device indicates the number of mandatory apps that are available in the App Store and yet to be installed on the device.



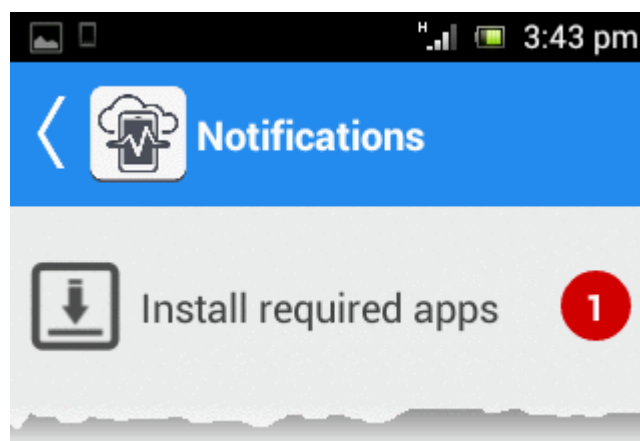
- Click the 'Applications' stripe

The list of apps available from the CDM App Store and yet to be installed on a device will be displayed under two tabs.



- **All** - Displays the list of all the apps available for installation, including the mandatory and optional apps.
- **Required** - Displays the list of apps that are required to be installed on the device to comply with the CDM profile applied to the device.
- Tap 'Install' to download and install the apps.

CDM also sends notification alerts to the devices if a mandatory app or a recommended app is uploaded to the **App Store**.



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

5.1.8. Generating Alarm on Devices

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

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

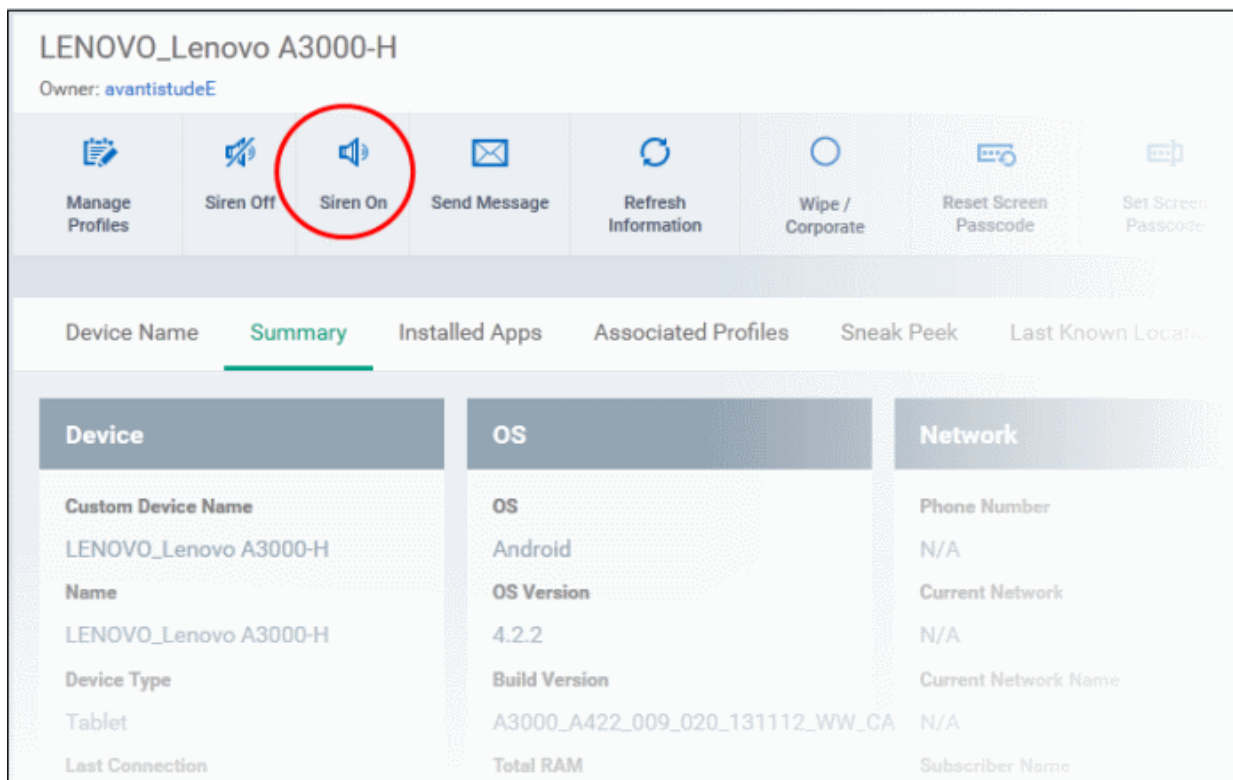
Note: This feature is available only for Android devices.

The following sections contain more information on:

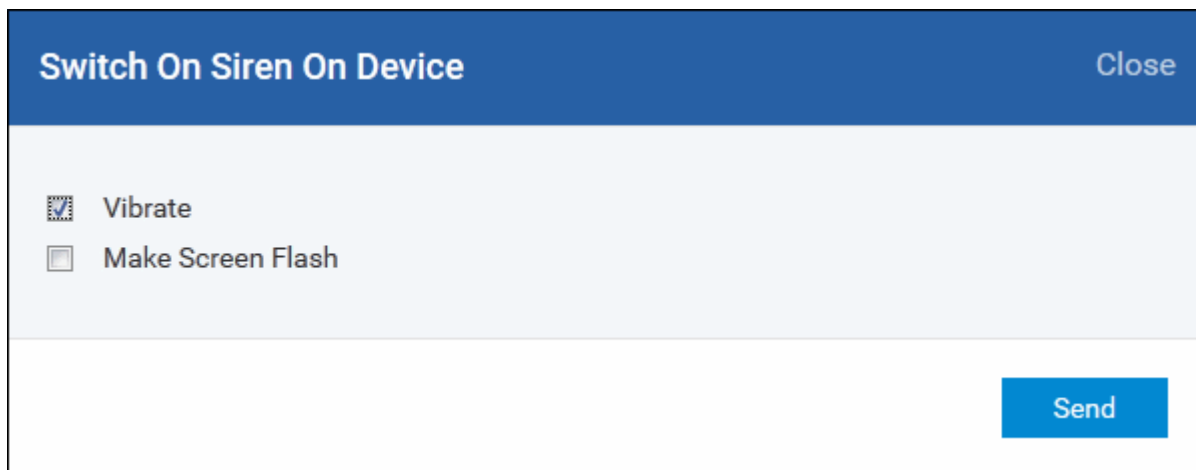
- **Generating alarm on a single device**
- **Generating alarm on several devices**

To generate alarm on a single device

- Click 'Devices' and choose 'Devices List'
- Click the name of the device on which the alarm is to be generated, to open the device details interface
- Click the 'Siren On' option from the top.



The alarm options dialog will open.



- Vibrate - The device will vibrate along with the siren

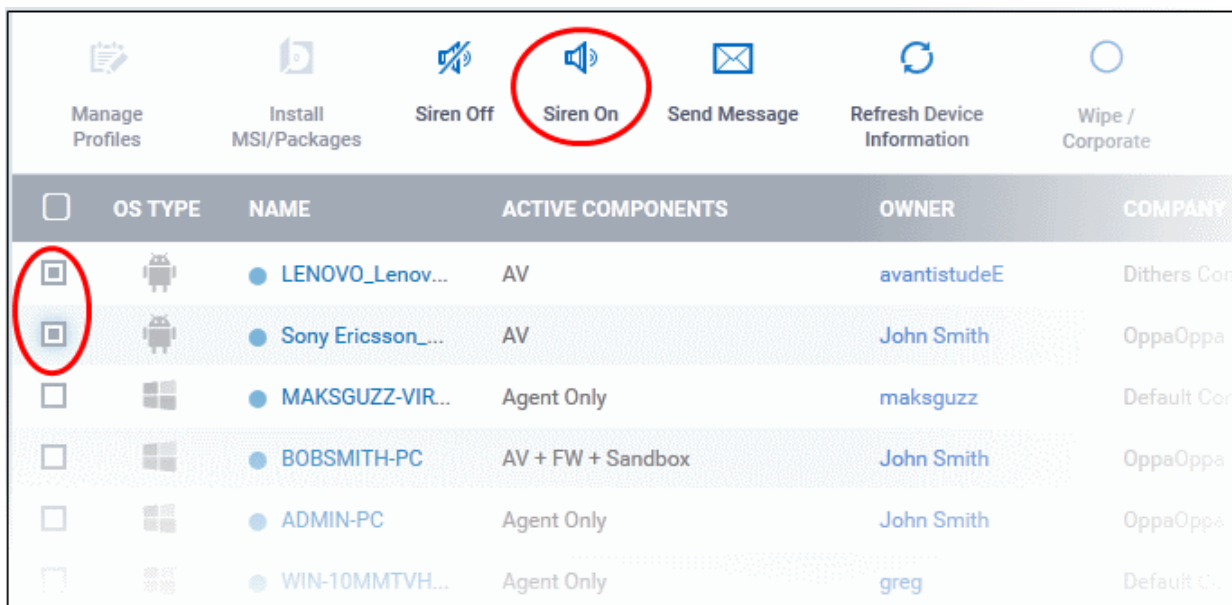
- Make screen flash - The device screen will flash intermittently along with the siren
- Click the 'Send' button.

The command will be sent and the device will start to emit the alarm at a loud volume.

- To switch off the alarm, click 'Siren Off' from the same interface.

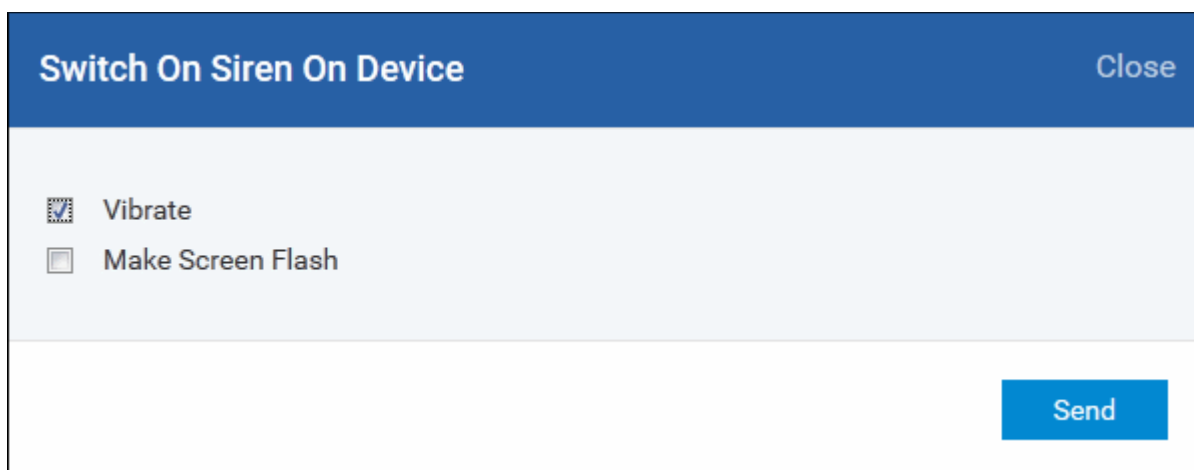
To generate alarm on several devices

- Click 'Devices' and choose 'Devices List'
- Select the devices on which the alarm has to be generated



- Click the 'Siren On' option from the top.

The alarm options dialog will open.



- Vibrate - The device(s) will vibrate along with the siren
- Make screen flash - The devices' screen will flash intermittently along with the siren
- Click the 'Send' button.

The command will be sent to the devices immediately and they will start emitting the alarm at a loud volume.

To stop the alarm

- Select the device(s) in which the alarm needs to be stopped from the Devices List interface.
- Click Siren Off from the options at the top.

5.1.9. Locking/Unlocking Selected Devices

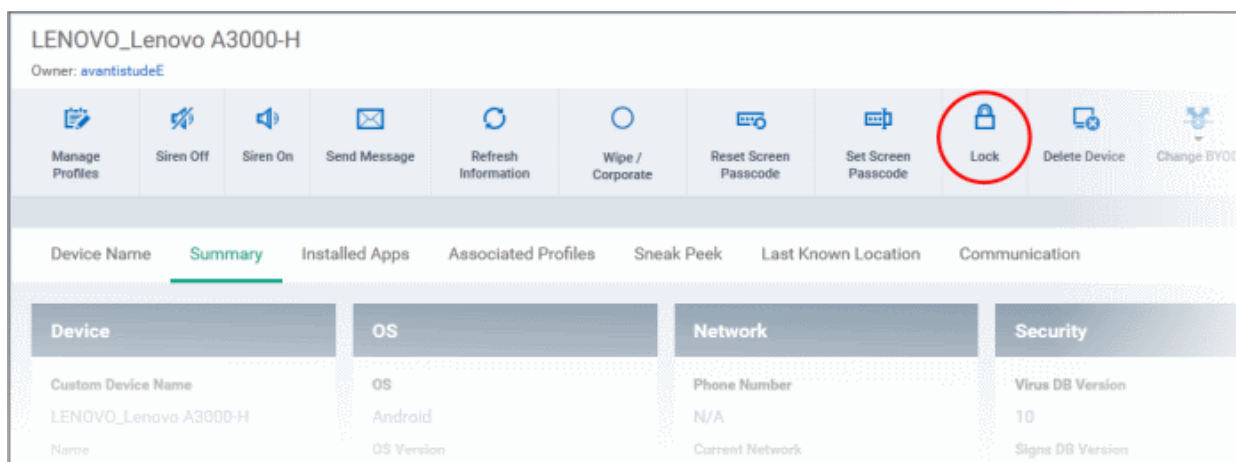
Administrators can remotely send screen lock commands from the CDM devices screen to prevent mislaid devices from being accessed by unauthorized persons, or to generally block access to a device. After the lock command is sent, the selected device(s) are automatically locked. The user can unlock by entering the screen lock password in the device.

The following sections contain more information on:

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

To remotely lock a single device

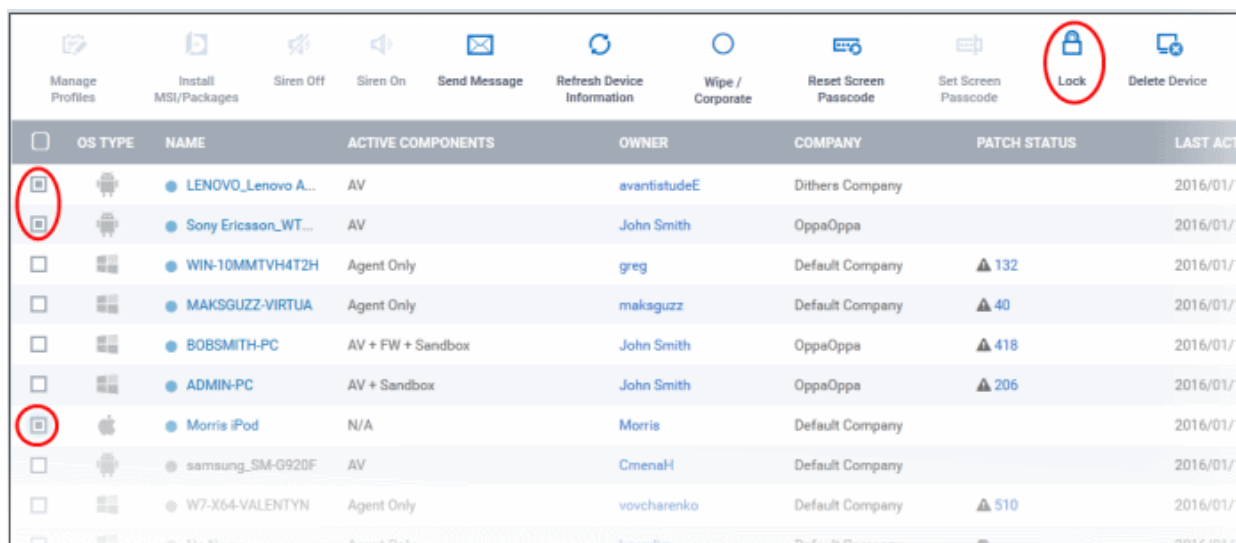
- Click 'Devices' and choose 'Devices List'
- Click the name of the device to be locked, to open the device details interface
- Click the 'Lock' option from the top click 'More...' and choose 'Lock' from the options



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

To remotely lock several devices at-once

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



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

5.1.10. Wiping Selected Devices

Information security is of utmost importance in any organization. Confidential corporate documents and sensitive information like usernames and passwords of users, contacts, stored messages, browser bookmarks, pictures and so on, stored in the device/SD card, are prone to be misused by criminals from a stolen or lost device. In order to prevent the leak of such information, the administrator can remotely erase the contents stored in a lost device from the 'Devices' interface.

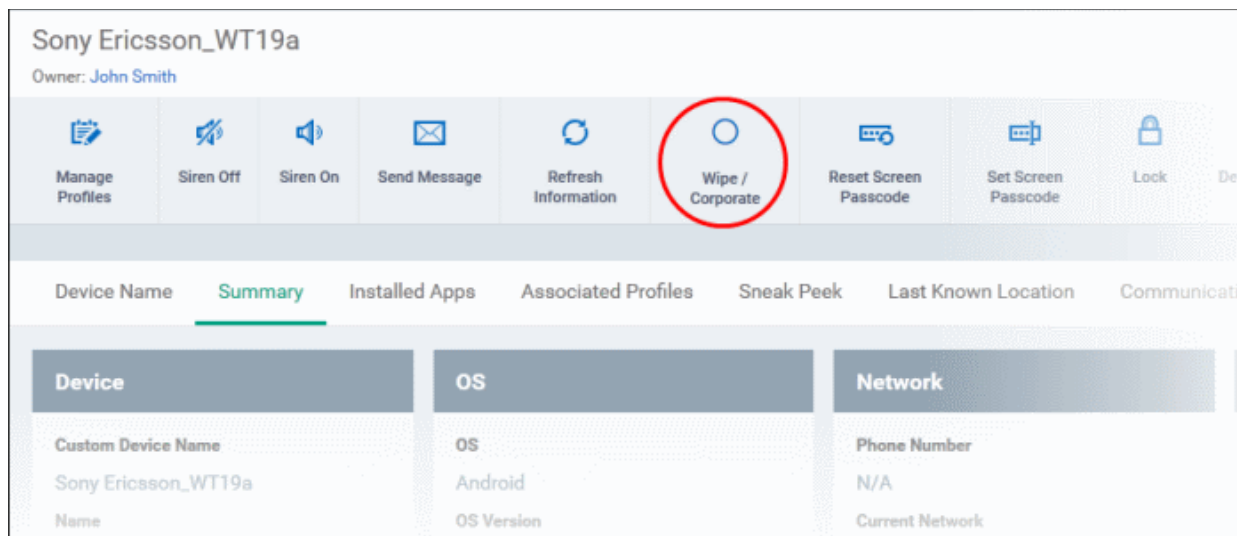
Tip: The administrator can also configure the device to automatically wipe itself, if it has been mislaid or stolen. If somebody enters wrong passwords on a lost or stolen device attempting to unlock the screen for specified number of times, the device will wipe automatically. The automatic wipe feature can be enabled in the device profile along with the threshold of how many incorrect attempts should be allowed. To view this in the interface, 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).

Following sections explain on:

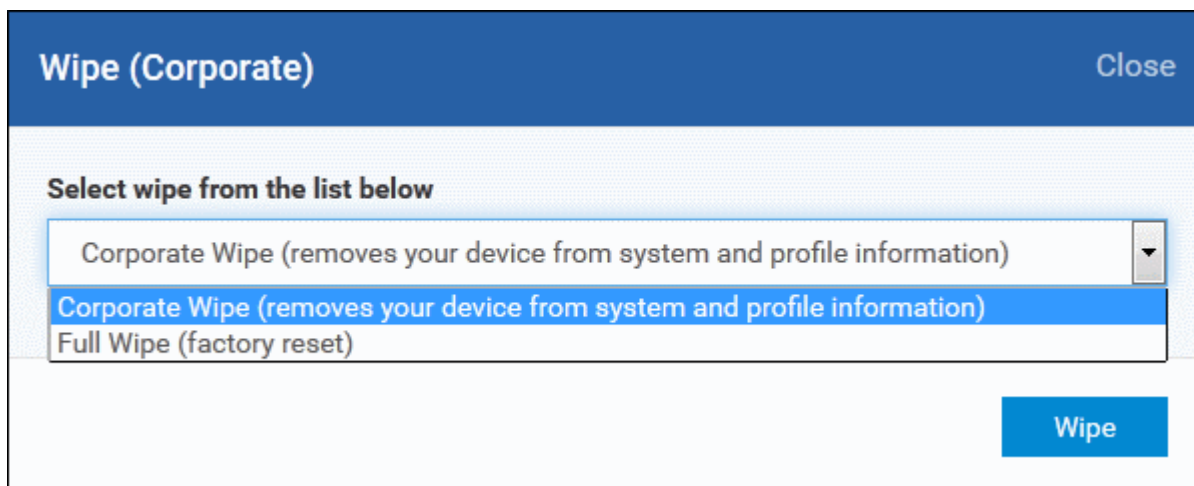
- [Wiping a single device](#)
- [Wiping several devices at-once](#)

To erase the contents stored in a selected device

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



The 'wipe options' dialog will open.

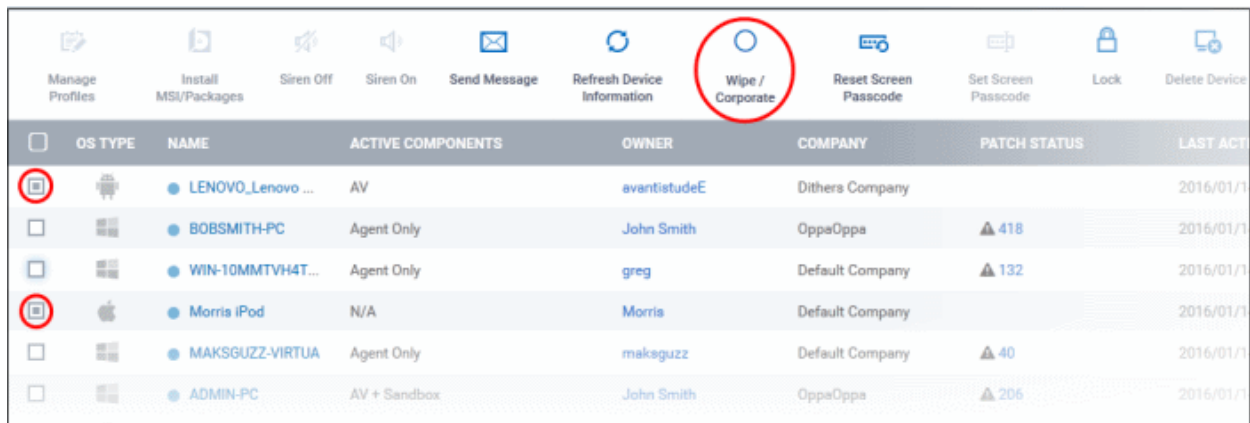


- Select the content to be erased.
 - To remove only CDM agent and configuration profiles, select 'Corporate Wipe' from the drop-down
 - To erase all the data from the device and the SD card, select 'Full Wipe' from the drop-down. The device will be returned to default factory settings after the wipe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

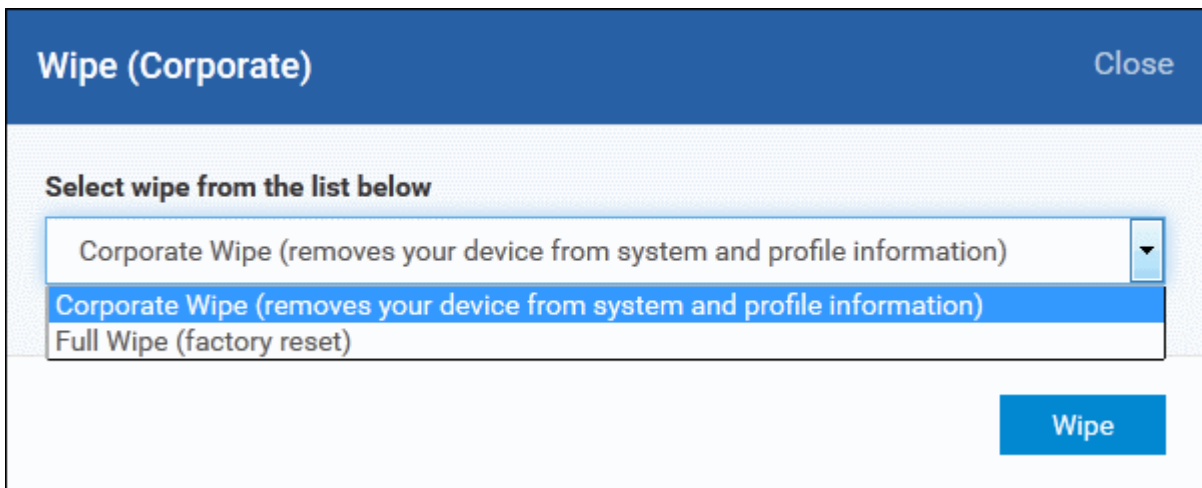
The wipe command will be sent and the data stored in the device will be deleted as per the wipe option chosen.

To erase the contents from several devices

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



The 'wipe options' dialog will open.



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

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

5.1.11. Assigning Configuration Profile to Selected Devices

The administrator can view the view the current configuration profiles in effect on a selected device, apply new configuration profiles or remove existing profiles from the 'Devices' interface. The profile applied from this interface adds up to the device along with the existing profiles applied to the device group to which the device is a member of, to the user and to the user group to which the user is a member of. In case the settings in a profile clashes with another profile, CDM 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.

For more details on profiles, refer to the chapter [Configuration Profiles](#).

To manage profiles applied to a device

- Click 'Devices' and choose 'Devices List'
- Select the device to be managed and click 'Manage Profiles' from the options at the top .

<input type="checkbox"/>	OS TYPE	NAME	ACTIVE COMPONENTS	OWNER	COMPANY	PATCH STA
<input type="checkbox"/>	Windows	BOBSMITH-PC	AV + FW + Sandbox	John Smith	OppaOppa	▲ 380
<input type="checkbox"/>	Windows	WIN-10MMTVH4T...	Agent Only	greg	Default Company	▲ 132
<input checked="" type="checkbox"/>	Android	LENOVO_Lenovo ...	AV	avantistudeE	Dithers Company	
<input type="checkbox"/>	iOS	Morris iPod	N/A	Morris	Default Company	
<input type="checkbox"/>	Windows	MAKSGUZZ-VIRTUA	Agent Only	maksguzz	Default Company	▲ 40
<input type="checkbox"/>	Windows	ADMIN-PC	AV + Sandbox	John Smith	OppaOppa	▲ 213
<input type="checkbox"/>	Windows	Sony Ericsson WT	AV	John Smith	OppaOppa	

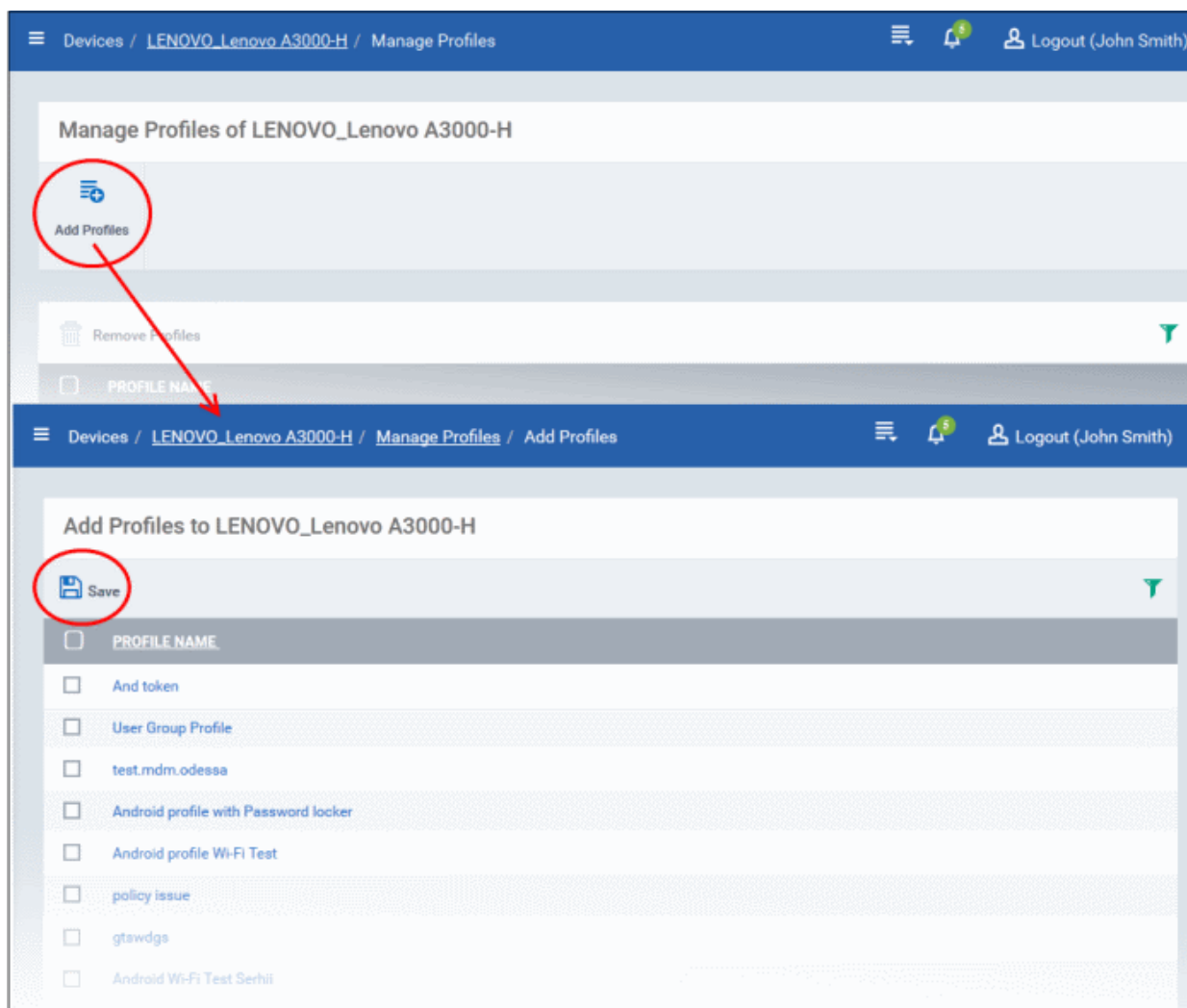
- Alternatively, click on the name of the device to be managed to open the device details interface and choose 'Manage Profiles' from the options at the top

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

<input type="checkbox"/>	PROFILE NAME
<input type="checkbox"/>	Android profile with blocked camera
<input type="checkbox"/>	Android Profile for Purchase Department

Note: If the device is in a group, the profiles applied to the group will not be indicated here. To view the the profiles applied to a device group refer to the section [Assigning Configuration Profiles to a Device Group](#).

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

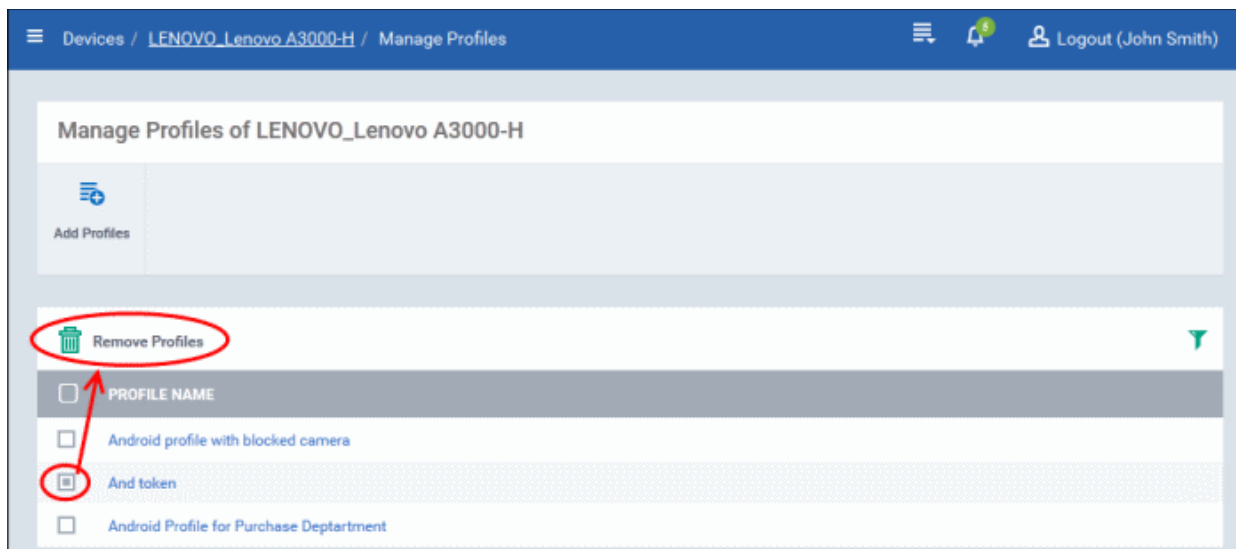


A list of all profiles applicable to the chosen device, excluding those that are already applied to the device will be displayed.

- Select the profile(s) to be applied to the device

Tip: You can use the search and filter options that appear on clicking the funnel icon at the top right to search for the profile(s) to be applied.

- Click 'Save' at the top left to add the selected profile(s) to the device.
- To remove existing profile(s), select the profiles to be removed from the 'Manage Profiles' interface and click on 'Remove Profiles' from the options that appear on top.



The selected profile(s) will be removed from the device immediately.

5.1.12. Setting / Resetting Screen Lock Password for Selected Devices

The administrator can remotely set a new screenlock passcode or reset existing code for the enrolled devices from the devices interface.

Note: For iOS devices, setting new passcode from CDM is not supported.

Following sections explain on:

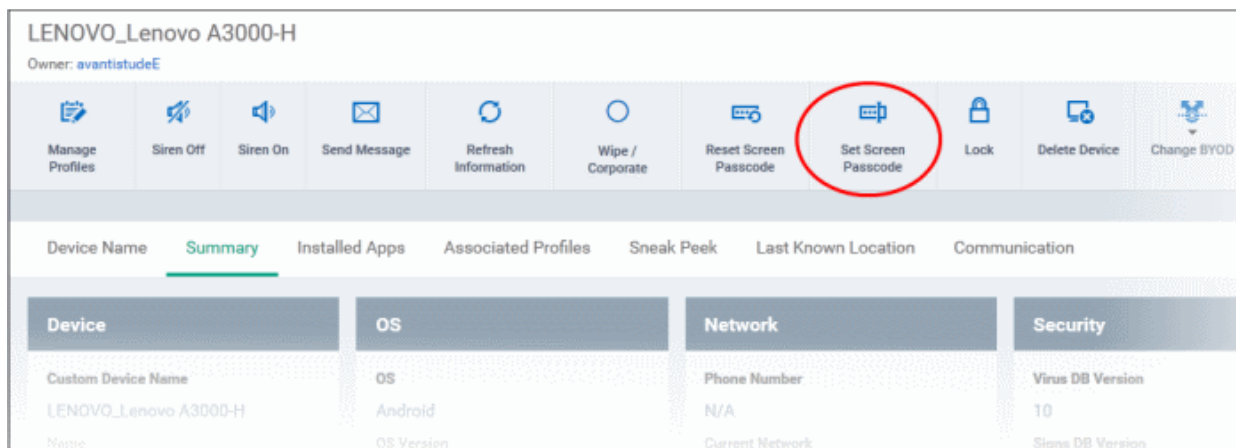
- [Settings and resetting password for a single device](#)
- [Settings and resetting password for several devices at-once](#)

To set a new screen lock password or remove password for a single device

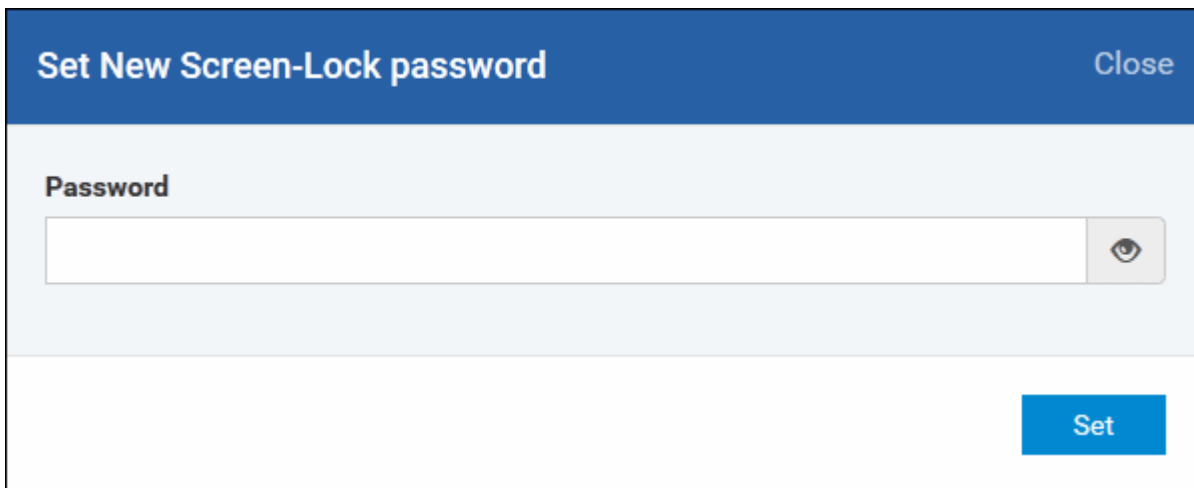
- Click 'Devices' and choose 'Devices List'
- Click on the name of the device for which a new password is to be created or existing password is to be reset

The device details interface will open.


- To set a new password, choose 'Set New Screen Passcode' from the options at the top or click 'More...' and choose 'Set New Screen Passcode' from the options.



The 'Set New Screen-Lock password' dialog will appear.



- Enter the new password in the 'password' text field.

Tip: You can use the eye icon  at the right end of the text field to display or hide the password typed.

- Click 'Set'.

The command will be sent to the device and next time this new password should be entered on the device to unlock the screen.

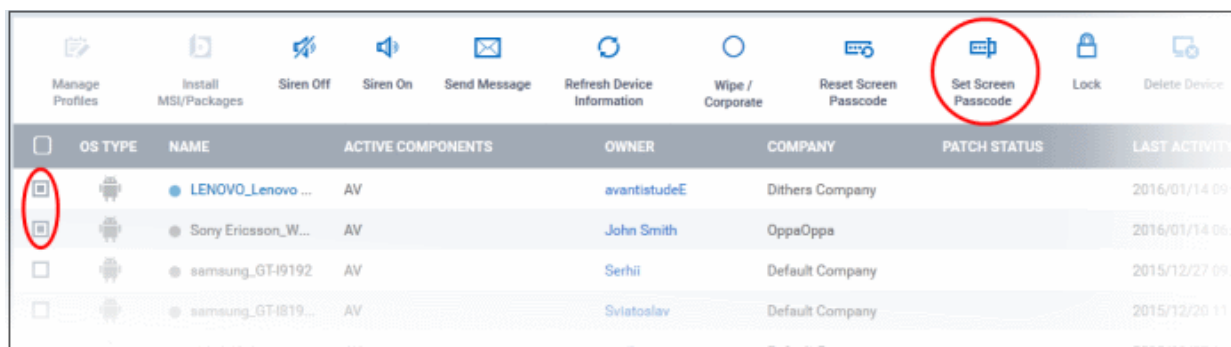
Note: If a Passcode profile has been configured for the selected device, make sure to enter the new password that complies with the profile.

- To clear the existing password of 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 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.


To set a new screen lock password or remove password for several devices

- Click 'Devices' and choose 'Devices List'
- Select the devices to set/reset password.
- To set a new password, choose 'Set New Screen Passcode' from the options at the top or click 'More...' and choose 'Set New Screen Passcode' from the options.



The 'Set New Screen-Lock password' dialog will appear.

- Enter the new password in the 'password' text field.

Tip: You can use the eye icon  at the right end of the text field to display or hide the password typed.

- Click 'Set'.

The command will be sent to all the devices at-once. From the next unlock operation, the users should enter the new password to unlock the device.

Note: If a Passcode profile has been configured for the selected devices, make sure to enter the new password that complies with the profile.

- To clear the existing passwords of the devices, select the devices and choose 'Reset Screen Passcode' from the options at the top or click 'More...' and choose 'Reset Screen Passcode' from the options.

The command will be sent to all the devices and the current screen lock password will be cleared. A message also will be sent to the device regarding the screen lock password change. If a Password profile is configured in the device, the user will be required to enter a new password that complies with the profile.

5.1.13. Updating Device Information

CDM agent in the enrolled devices sends full information such as memory status, name of the device, IMEI number, roaming state, MAC address of bluetooth, MAC address of WiFi and so on to the server at periods configured in the settings interface. If required, these information can be fetched on real time by clicking the 'Refresh Device Information' option in the 'Devices' interface.

Following sections explain on:

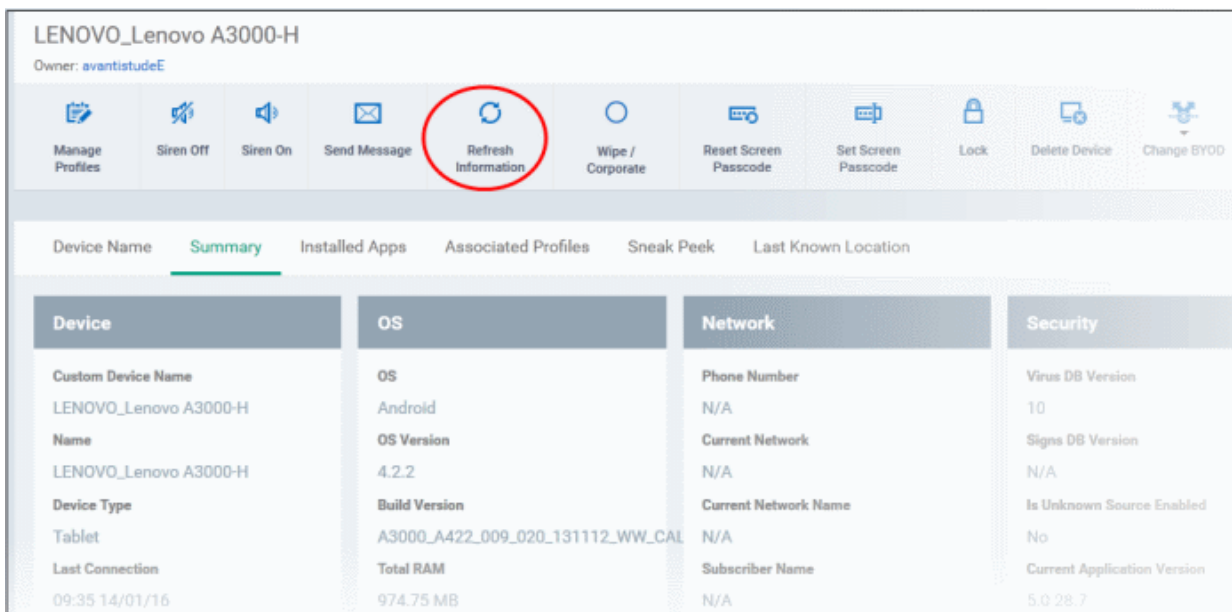
- **Updating information from a single device**
- **Updating information from several devices at-once**

To update device information from a single device

- Click 'Devices' and choose 'Devices List'
- Click on the name of the device to refresh information.

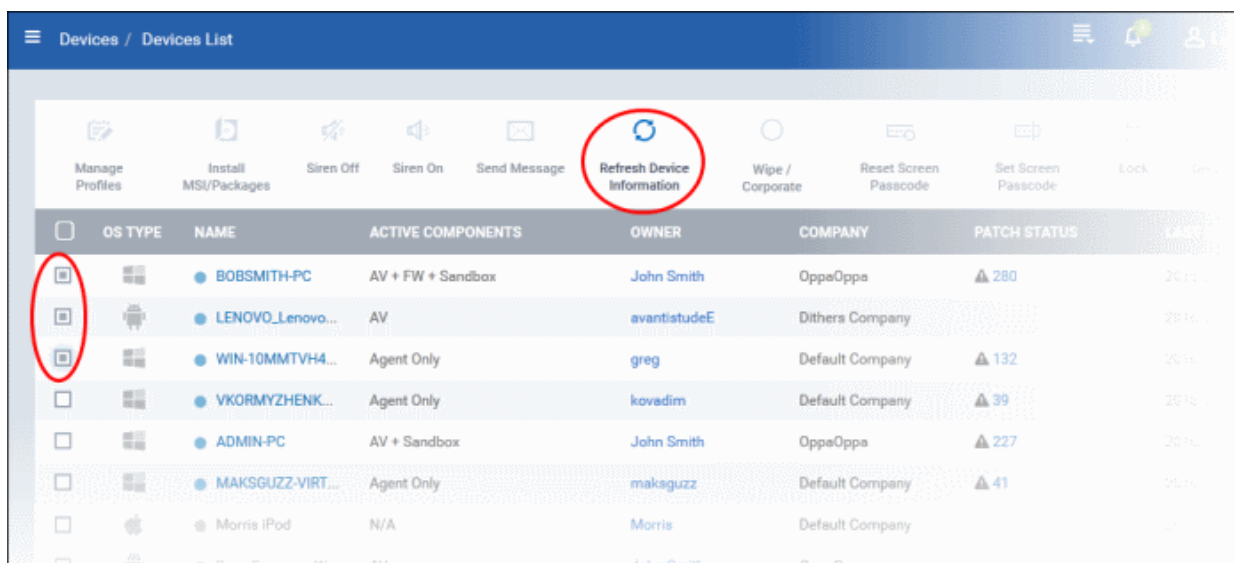
The device details interface will open with information on the device fetched from last polling time of the agent installed on the device.

- Click 'Refresh Information' from the options at the top or click 'More...' and choose 'Refresh Information' from the options.



To update device information from several devices

- Click 'Devices' and choose 'Devices List'
- Select the devices to refresh information from.
- Click 'Refresh Device Information' from the options at the top or click 'More...' and choose 'Refresh Device Information' from the options.



5.1.14. Sending Text Message to Devices

CDM allows administrators to send text messages to enrolled devices. This will come in handy if the user(s) should be sent some important notifications, corporate messages and so on.

Note: For iOS devices, the CDM client should be installed for this feature to be supported.

Following sections explain on:

- **Sending message to a single device**
- **Sending message to several devices at-once**

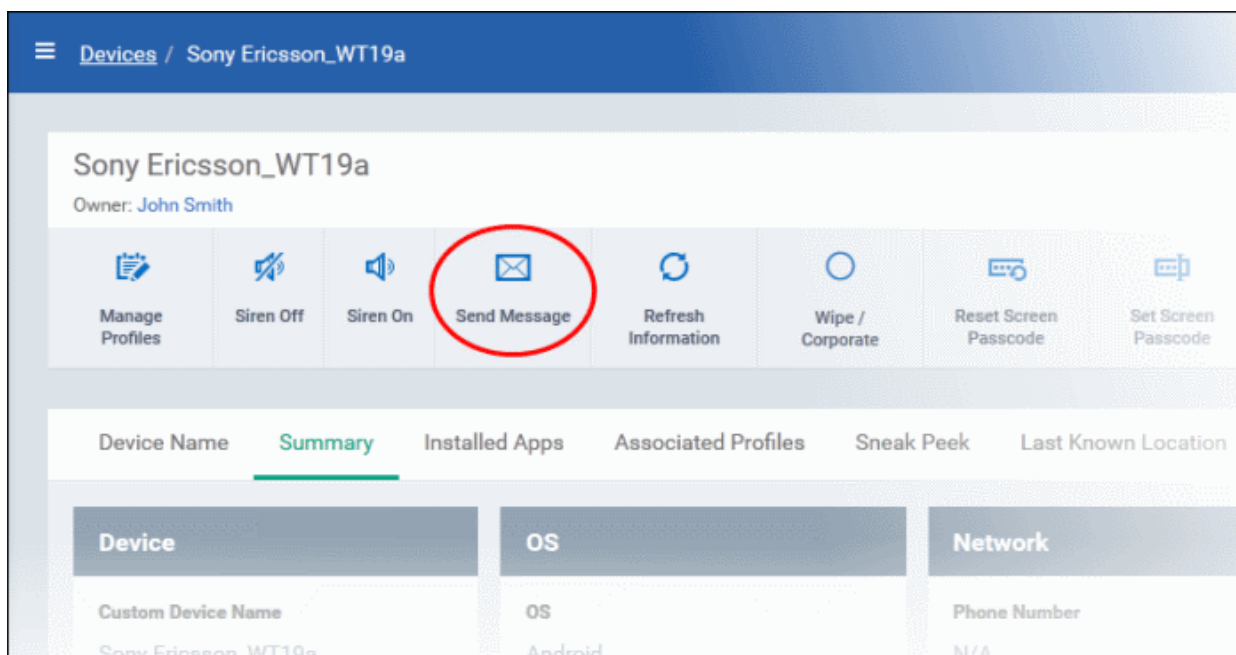
To send text message to a single device

- Click 'Devices' and choose 'Devices List'

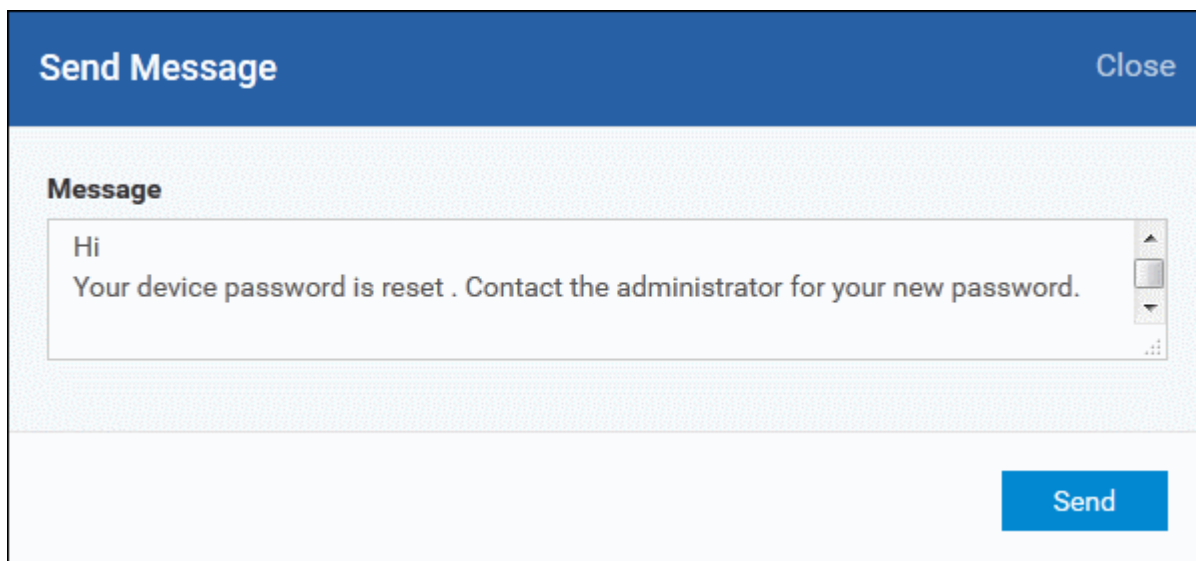
- Click on the name of the device to send the message.

The device details interface will open.

- Click 'Send Message' from the options at the top.



The 'Send Message' dialog will open.

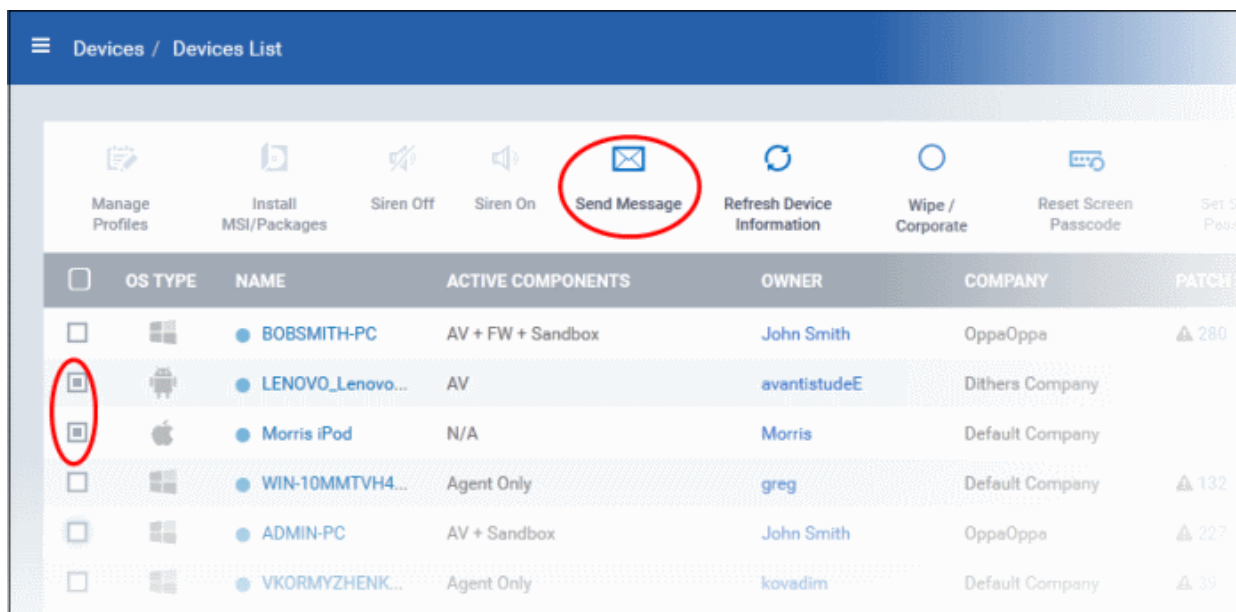


- Enter the text message in the 'Message' field.
- Click on the 'Send' button.

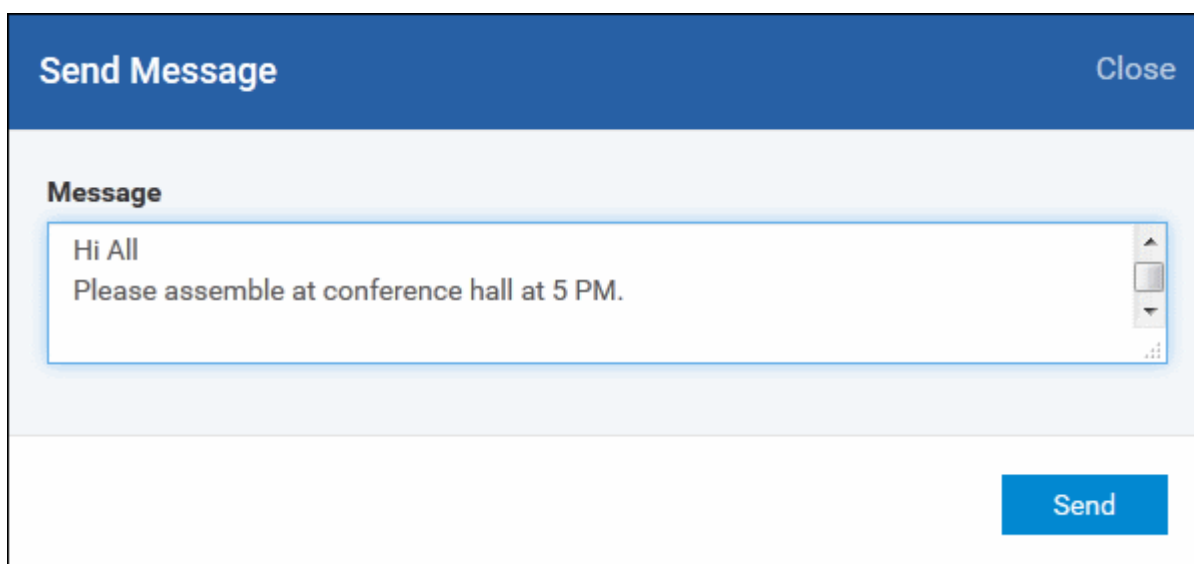
The message will be sent to the device for the user's attention.

To send a text message to several devices at-once

- Click 'Devices' and choose 'Devices List'
- Select the devices to which you wish to send messages
- Click 'Send Message' from the options at the top



The 'Send Message' dialog will open.



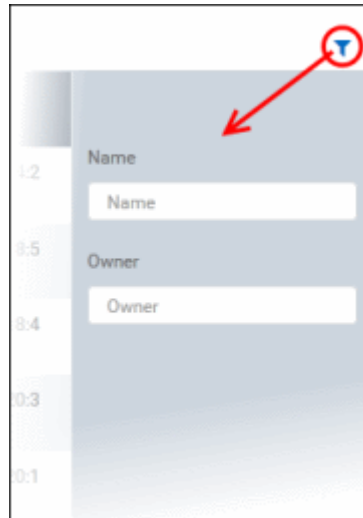
- Enter the text message in the 'Message' field.
- Click on the 'Send' button.

The message will be sent to the selected devices for the users' attention.

5.2. Managing Device Groups

Comodo Device Manager allows the administrator to create logical device groups of Android, iOS and Windows devices for convenient management of large number of devices. For example, the devices can be grouped under a company as per the structure of the organization and/or depending on types of devices. The administrator may create groups of devices called 'Sales Department', 'Accounts Department', 'Android Tablets', '7" iPads', 'Android Smart Phones', 'iPhones', 'Executive Laptops' or 'All Managed Mobile Devices'.

Each group can contain devices of different OS types. Once created, the administrator can manage all devices belonging to that group together. Dedicated configuration profiles can be created for and applied for each group as per their requirements and the allowable user privileges and applied appropriately to the device groups. The profiles for different OS types applied to a group will be deployed on the devices of respective OS types. CDM allows a single device to be enrolled as a member of more than one group as per the management requirements and the configuration profiles applied to all the groups to which the device is a member of, will be applied to the device. In case the settings in a profile clashes with another profile, CDM follows the 'Most



- To filter the items or search for a specific group device based on group name and admin that created the group, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

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

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CDM 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 Device Groups](#)
- [Editing a Device Group](#)
- [Assigning Configuration Profiles to a Device Group](#)
- [Removing a Device Group](#)

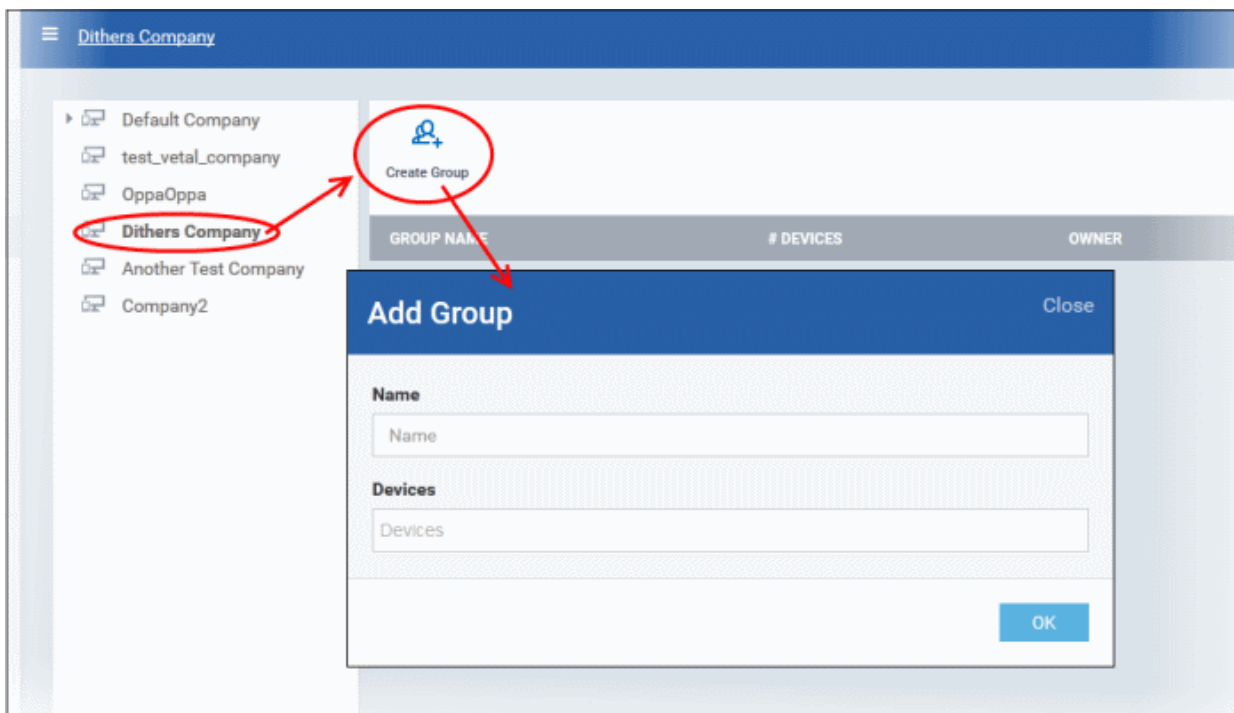
5.2.1. Creating Device Groups

The administrator can create device groups as required and import managed devices into it. The grouping of devices enables pushing selected configuration profiles to all the devices pertaining to a group at-once. Profiles of different OS types applied to a group, will be deployed to devices of respective OS types.

To create a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- Click on the company/department name that you want to create a group
- Click 'Create Group' from the top left

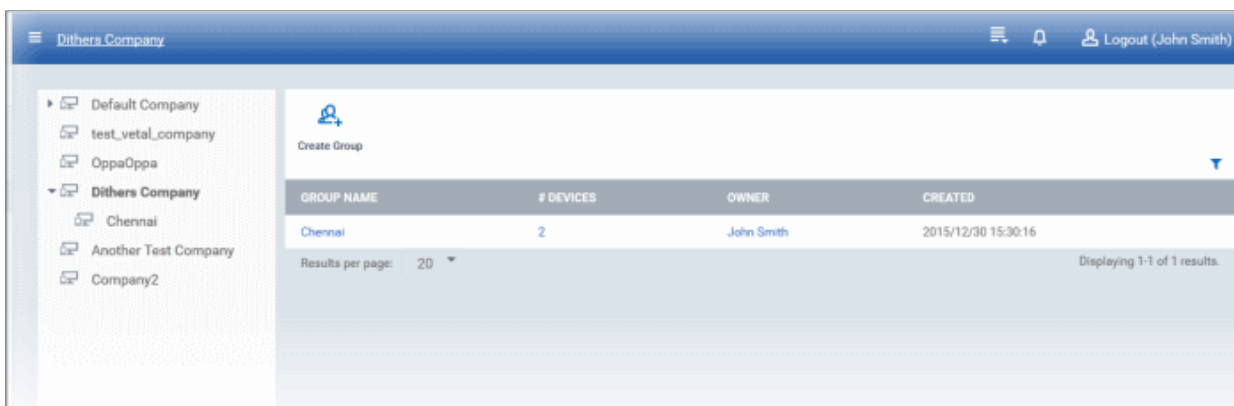
The 'Add Group' interface will open.



'Add Group' dialog - Table of Parameters		
Form Element	Type	Description
Name	Text Field	Allows you to enter a name describing the group of devices.
Devices	Text Field	Allows you to add the enrolled devices to the group. To add a device, start typing the first few letters of the device name and select the device from the predictions list that appear. Repeat the process for adding more number of devices. Note: You can add devices at a later stage too.

- Fill the details and click 'Save'.

The new group will be created and the device group details screen will be displayed with the list of devices in the group allowing you to add or remove devices and to manage profiles applied to the devices in the group. Refer to the section **Editing a Device Group** for more details.



- Repeat the process to add more groups.

The new groups will be listed for the selected company/department. The added groups will also be listed in the hierarchical structure on the left for the company/department. Appropriate configuration profiles can now be applied to each new group. Refer to **Assigning Configuration Policy to a Group** for more details.

5.2.2. Editing a Device Group

The administrator can view the member devices of a group, add or remove devices, rename a group, manage configuration policies applied to the device in a group from the device group details interface.

To view and edit device a device group


- Click the 'Devices' tab from the left and choose 'Device Groups'
- Click on the company/department name that you want to edit its group
- Click on the name of the group either under the hierarchical structure or from the list on the right to be edited. The group details interface for the selected group will open.

The screenshot illustrates the Comodo Device Manager interface. On the left, a sidebar shows a hierarchical tree of companies, with 'Dithers Company' expanded and 'Chennai' selected. The main area displays a table of device groups, with 'Chennai' selected. Below the table, the 'Chennai' group details are shown, including a 'Remove From Group' button and a table of devices.

GROUP NAME	# DEVICES	OWNER	CREATED
Chennai	2	John Smith	2015/12/30 15:30:16

DEVICE NAME	IMEI	OWNER
ADMIN-PC	N/A	John Smith
WIN8-CES-1	N/A	Sviatoslav

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 that allows to search for a particular device.
- To filter the items or search for a specific group device based on its name, enter the search criteria in part or full in the text box and click 'Apply'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

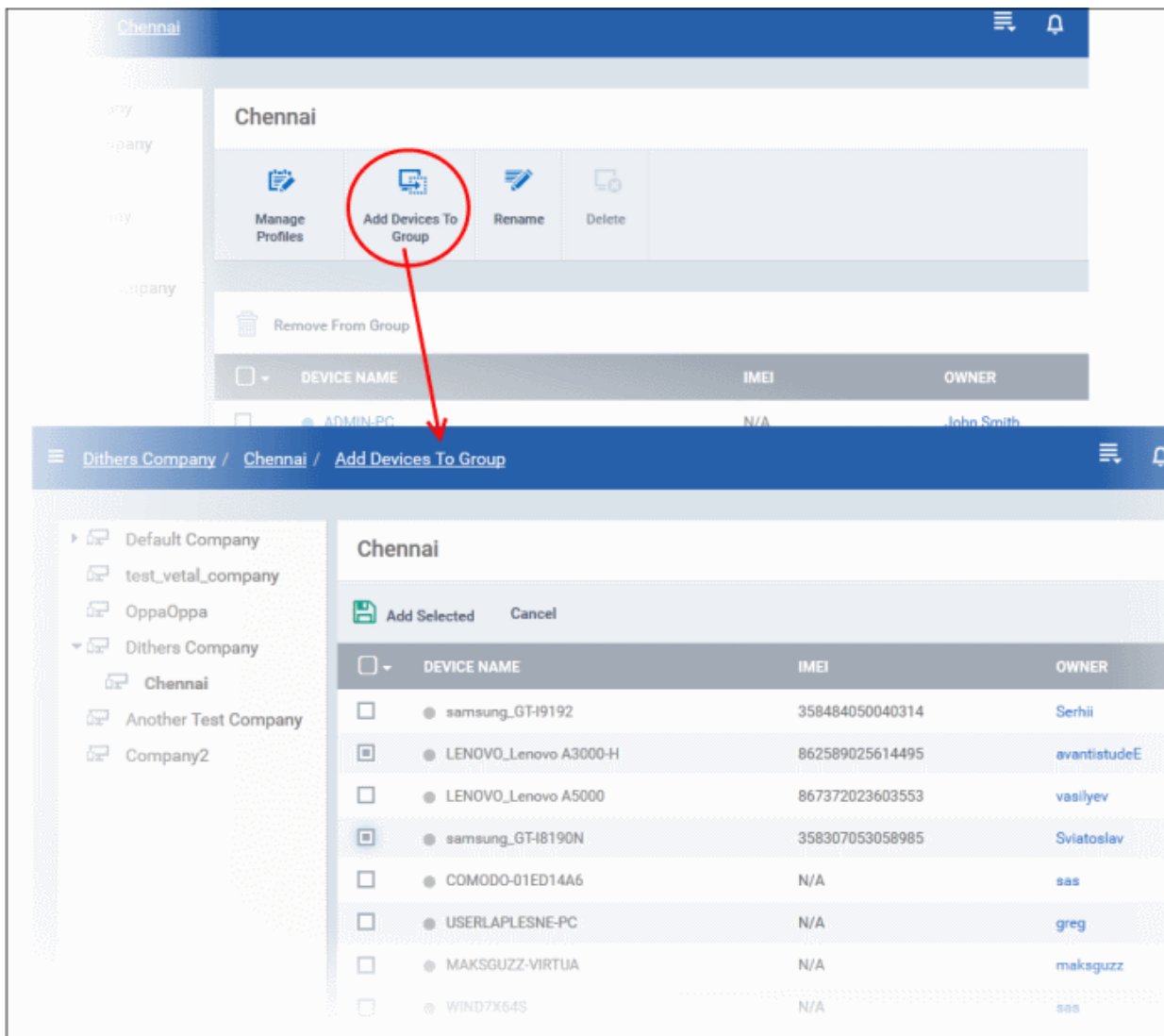
The device group details interface allows you to:

- **Add new devices to the group**
- **Remove devices from the group**
- **Rename the group**
- **Assign Configuration profiles to the device group**
- **Remove the group**

To add new devices to the group

- Click 'Add Devices to Group' at the top.

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

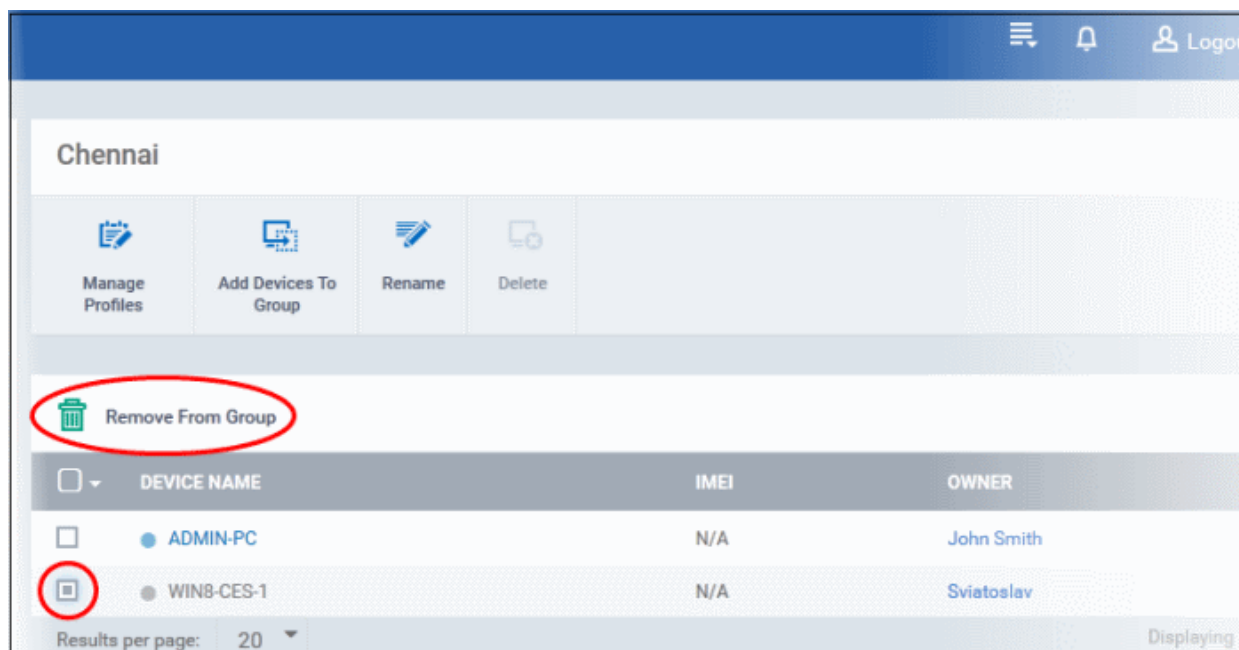


- Select the devices to be added to the group and click 'Add Selected'.

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

To remove devices from the groups

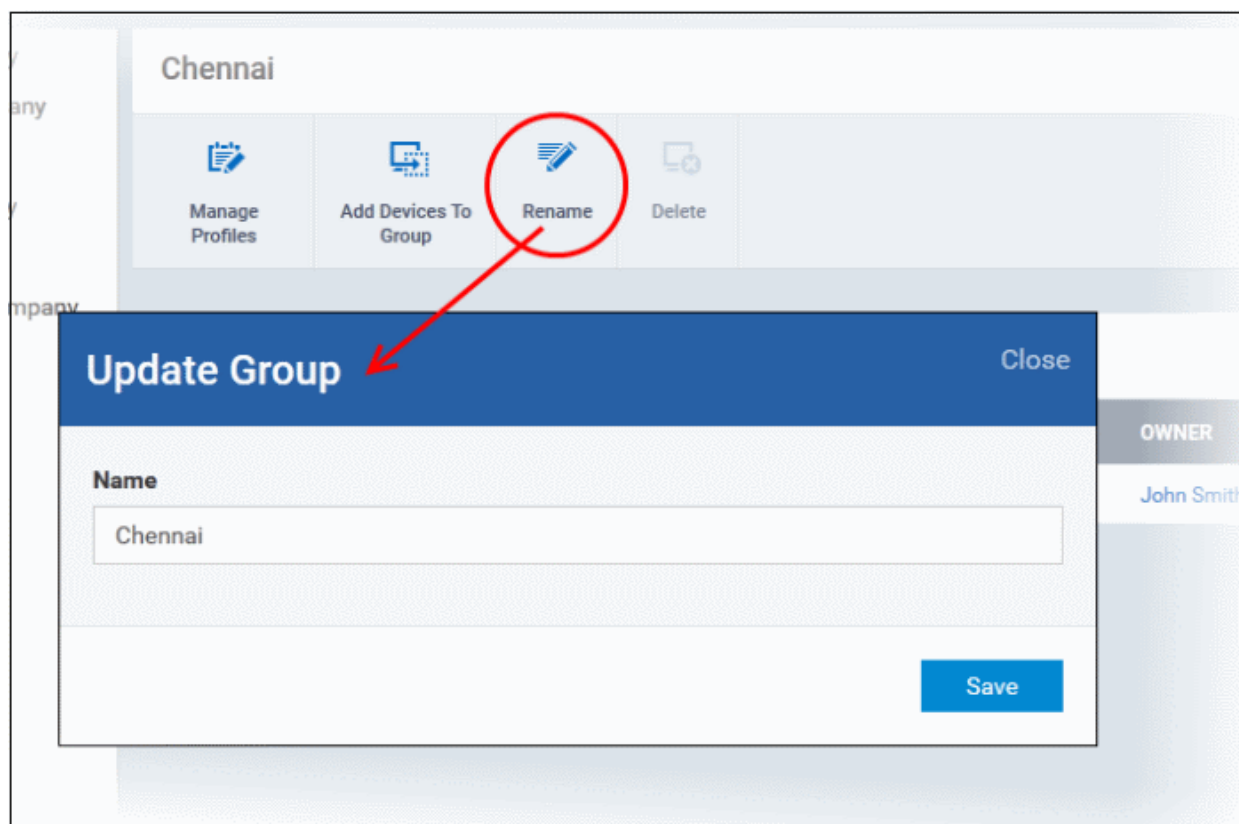
- Choose the devices to be removed from the device group details interface
- Click 'Remove from Group'



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

To rename a group

- Click on the 'Rename' button at the top



The 'Update Group' dialog will open

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

The group will be updated with the new name.

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

5.2.3. Assigning Configuration Profiles to a Device Group

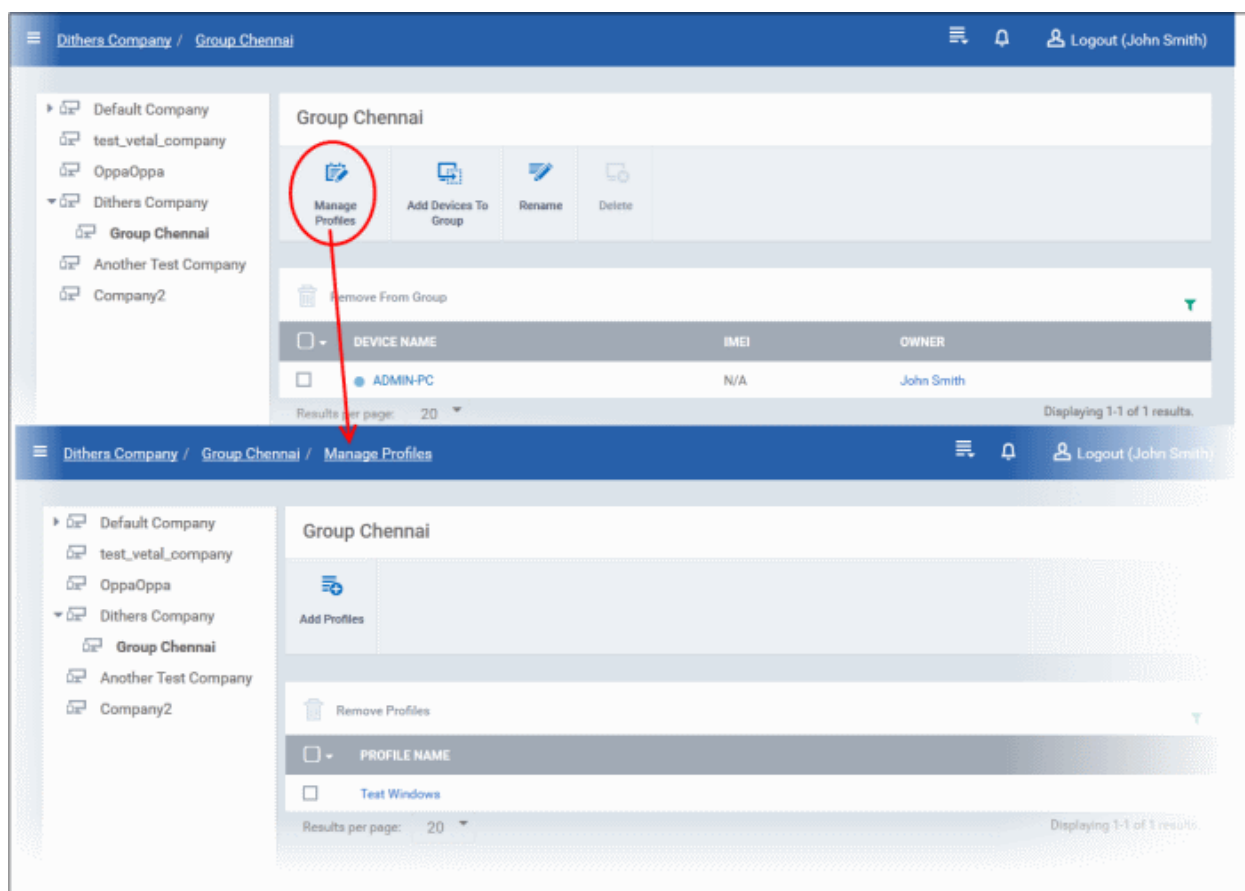
The administrator can view the configuration profiles currently assigned to the device group, add new profiles or remove existing profiles from the device group details interface.

For more details on profiles, refer to the chapter [Configuration Profiles](#).

To view and manage the profiles applied to a group

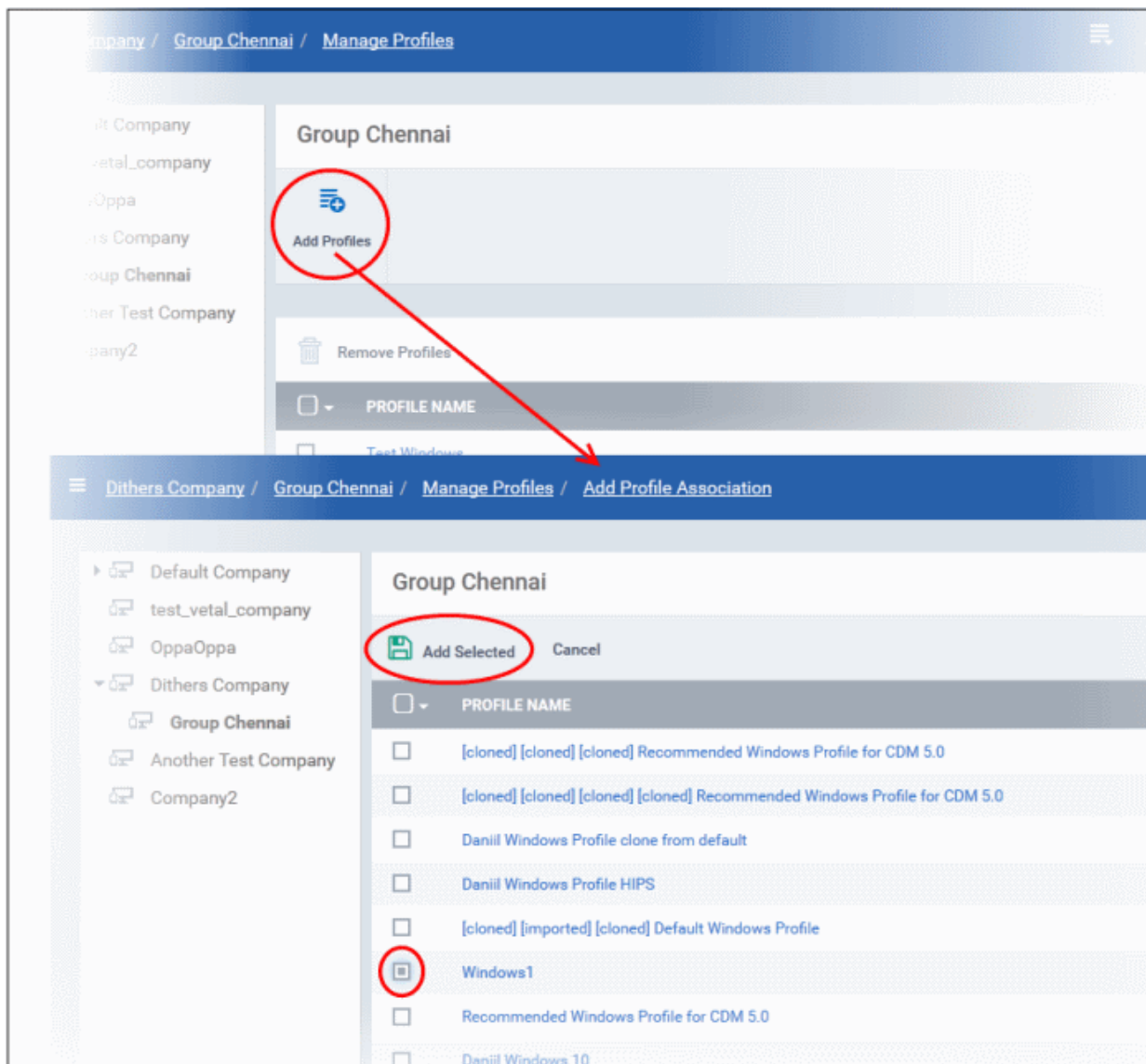
- Click the 'Devices' tab from the left and choose 'Device Groups'
- Click on the company/department name that you want to edit its group
- Click on the name of the group either under the hierarchical structure or from the list on the right to be edited. The group details interface for the selected group will open.
- Click the 'Manage Profiles' from the options at the top.

The 'Manage Profiles' interface will open displaying a list of configuration profiles associated with the device group.



To add a new profile

- Click 'Add Profiles' from the top.



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

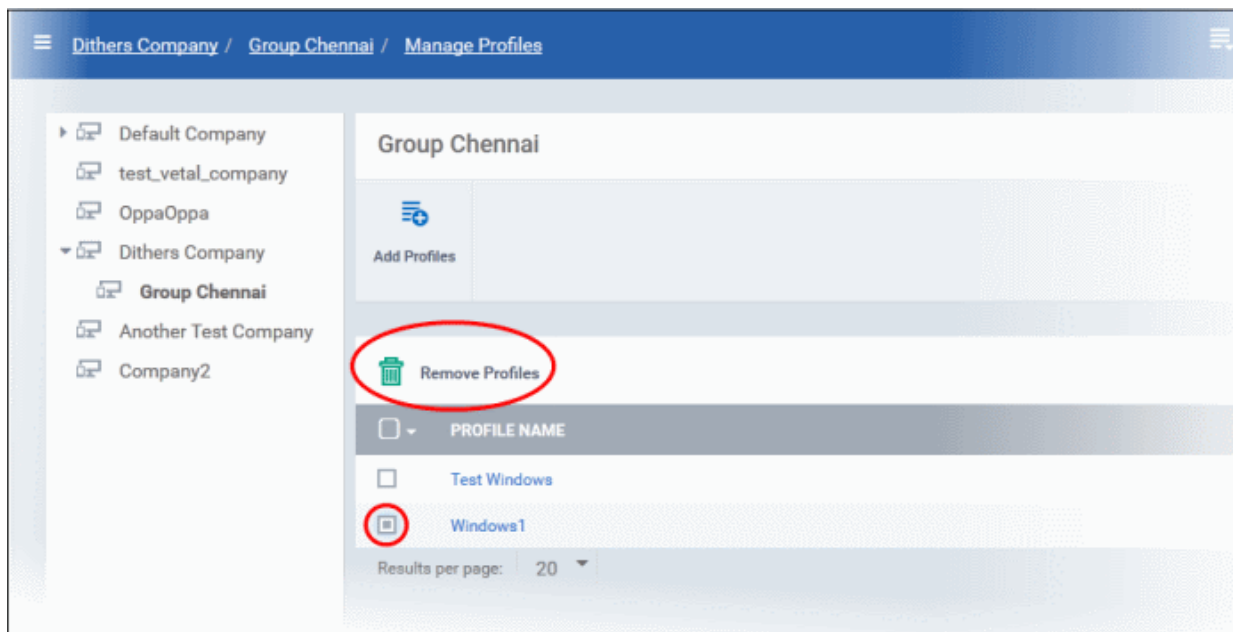
- Select the profiles to be applied to the devices in the group and click 'Save'.

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'



The profile(s) will be removed from all the member devices of the group.

Note: Disassociating a profile from the device group will remove the profile from the member device 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, user group to which the user is a member of or to the device directly, the profile will not be removed from the device.

5.2.4. Removing a Device Group

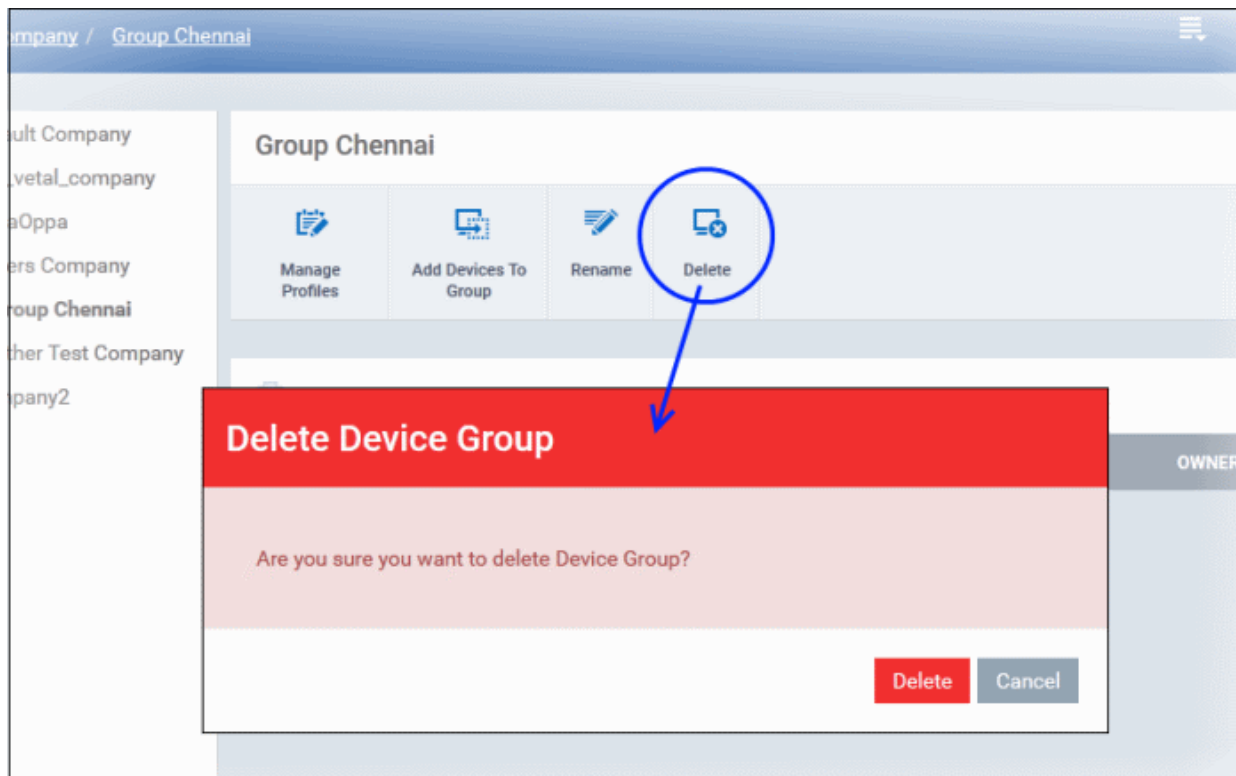
The administrator can remove a unwanted device group(s) from CDM. Please note you cannot delete a device group unless the devices in them are deleted first.

To remove a device group

- Click the 'Devices' tab from the left and choose 'Device Groups'
- Click on the company/department name that you want to remove its group
- Click on the name of the group either under the hierarchical structure or from the list on the right to be removed. The group details interface for the selected group will open.

Please note that you can remove a device group only if there are no devices in it.

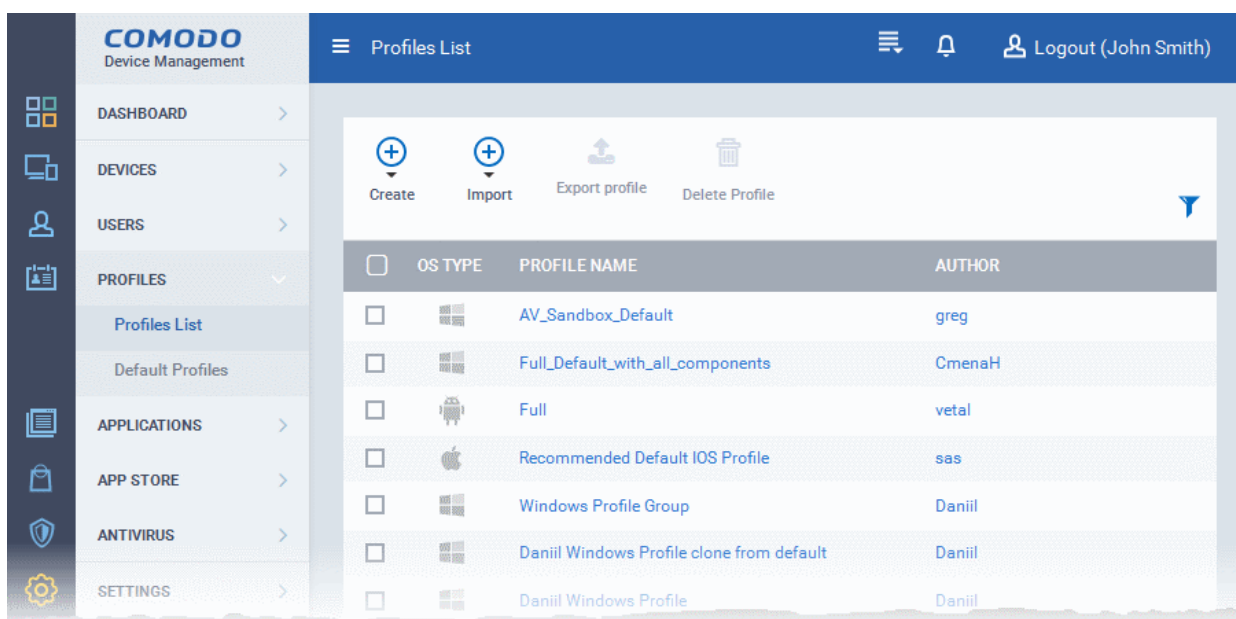
- Click on the 'Delete' button at the top.



- Click 'Delete' in the confirmation dialog. The device group will be removed from CDM.

6. Configuration Profiles

A configuration profile is a collection of settings which can be applied to devices that have been enrolled into Comodo Device 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 and Windows devices. Once created, a profile can be applied to an individual device, to a group of devices or designated as a 'default' profile.



The 'Profiles' tab contains two sub sections:

- **Profiles List** - Contains a list of every iOS, Android and Windows profile that has been added to CDM. Profiles listed here can be applied to individual devices/groups or designated as a 'default' profile. You can add new profiles, export Windows profiles as configuration file (in .cfg format) and import Windows profiles from a stored configuration file or from a managed Windows device.
- **Default Profiles** - Default profiles are those that are automatically applied to a device upon its initial enrollment into Comodo Device Manager. Administrators can choose to keep the default profile in place or can subsequently move the device to another profile.

The interface allows the administrator to:

- **Create/Import Configuration Profiles**
- **View the Profiles**
- **Edit Configuration Profiles**
- **Manage Default Profiles**

6.1. Creating Configuration Profiles

The 'Profiles List' screen allows you to create new profiles as well as to edit or delete existing profiles in the list. To open this screen, click the 'Profiles' tab from the left and choose 'Profiles List'.

<input type="checkbox"/>	OS TYPE	PROFILE NAME	AUTHOR
<input type="checkbox"/>	Windows	AV_Sandbox_Default	greg
<input type="checkbox"/>	Windows	Full_Default_with_all_components	CmenaH
<input type="checkbox"/>	Android	Full	vetal
<input type="checkbox"/>	iOS	Recommended Default iOS Profile	sas
<input type="checkbox"/>	Windows	Windows Profile Group	Daniil
<input type="checkbox"/>	Windows	Daniil Windows Profile clone from default	Daniil
<input type="checkbox"/>	Windows	Daniil Windows Profile	Daniil

The 'Create' drop-down above the table allows you to create new profiles for Android, iOS and Windows devices. You can create any number of profiles with different parameters and settings for different device settings for application to respective devices. A single device can be applied with any number of profiles. If multiple profiles are associated with the device, the most restrictive policy will be applied. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

In addition to creating a new Windows profile by defining security settings for each component of CES, you can import the configuration of CES with the current security settings of individual Antivirus, Firewall, Sandbox components at an endpoint as a profile for application to other endpoints.

The interface also allows you to export an existing Windows profile as a configuration file in .cfg format. You can import the profile at a later time from a saved .cfg file to create a new file.

The following sections explain on:

- **Creating 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 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 Windows Profile** - You can define parameters and configure various settings for the Antivirus, Firewall,

Sandbox components of the endpoint security software Comodo Endpoint Security (CES) installed on the Windows Endpoints and save them as a profile. Refer to the section **Profiles for Windows Devices** for more details.

- **Importing Windows Profile** - You can import a profile from a stored configuration file or import the configuration of CES with the current security settings of individual CES components at an endpoint as a profile. Refer to the section **Importing Windows Profiles** for more details.

6.1.1. Profiles for Android Devices

Android profiles allow you to specify a device's network access rights, restrictions and other general system settings.

To create an Android profile

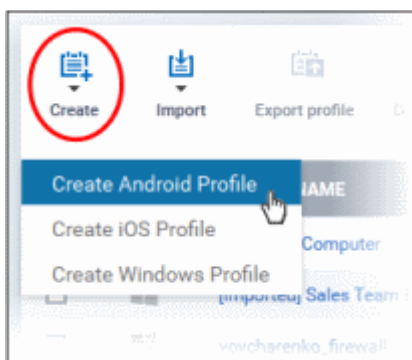
- Click 'Profiles' from the left then choose 'Profiles List'
- Click 'Create' then select 'Create Android Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profile List'.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Section' button. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices and device groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.

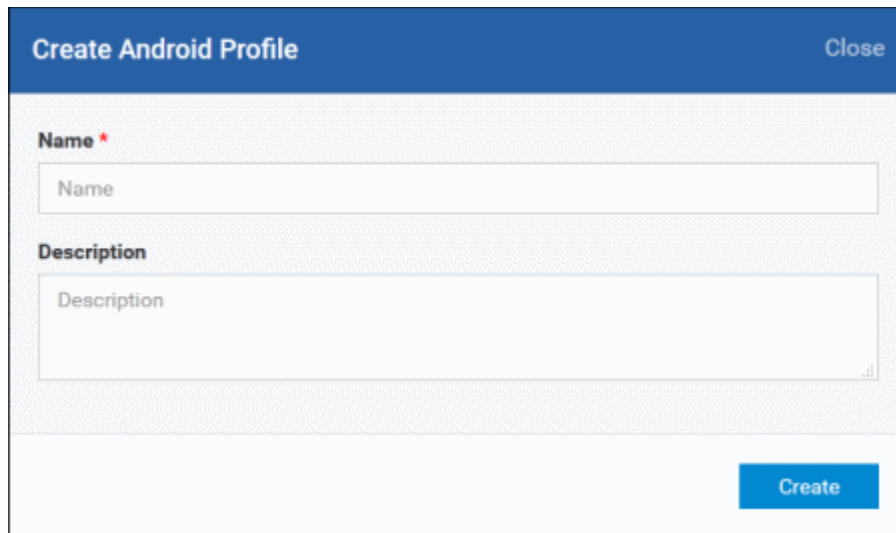
- To create a new profile, click 'Profiles > Profile List > Create':

To create a Android profile

- Open the 'Profiles List' interface by clicking 'Profiles' from the left and choosing 'Profiles List'
- Click 'Create' drop-down above the table and then click 'Create Android Profile'

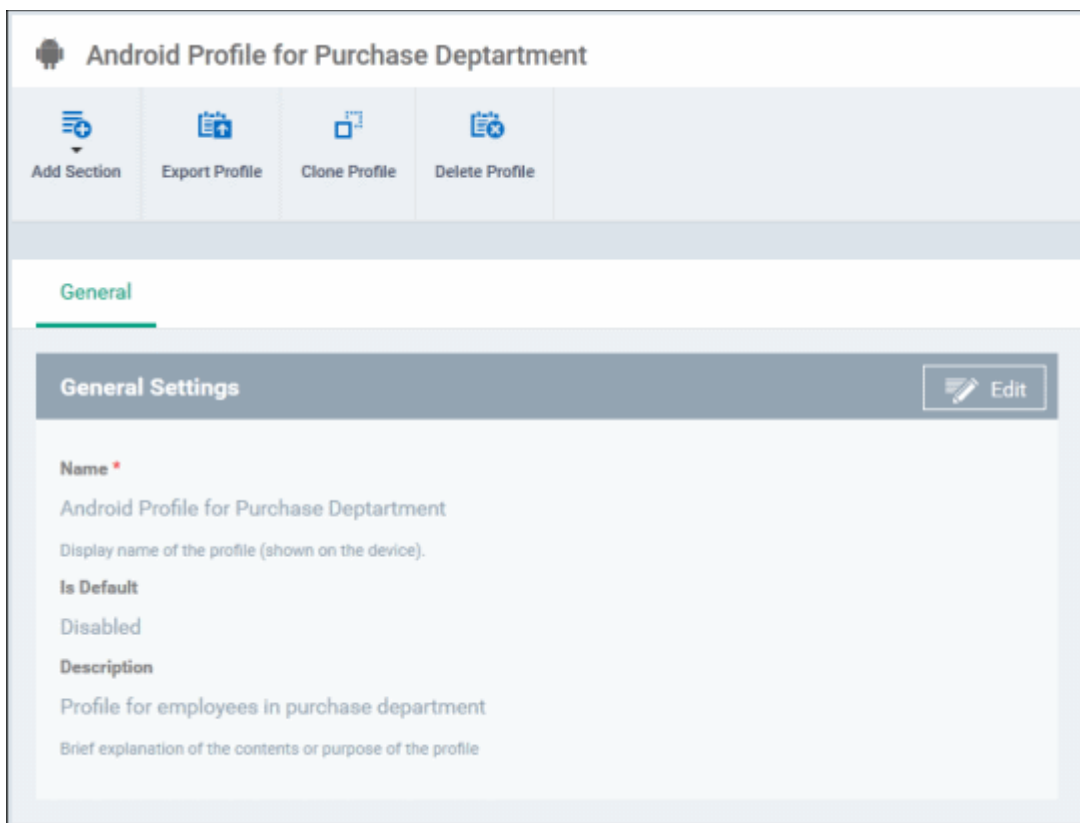


The 'Create Android Profile' screen will be displayed.

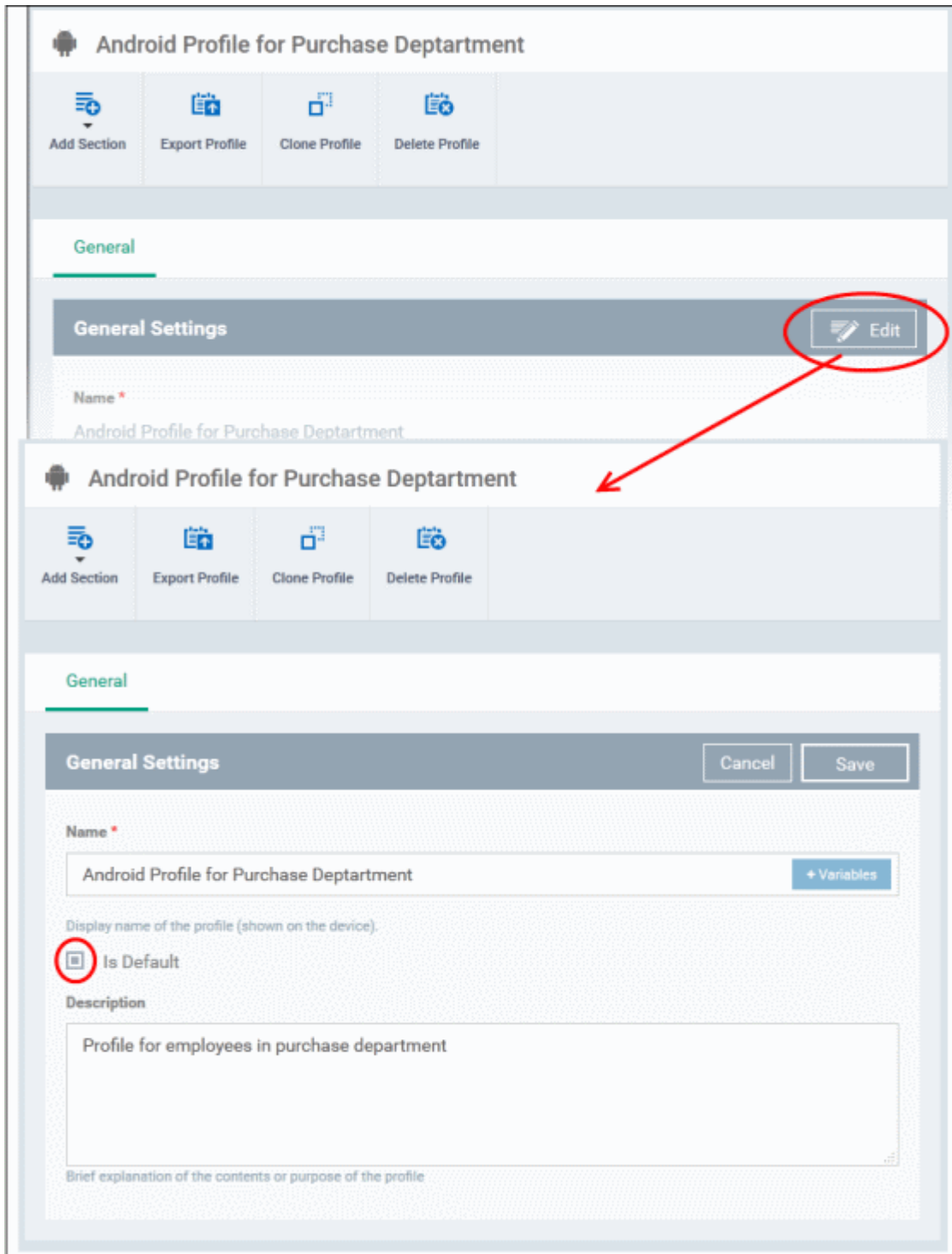


- Enter a name and description for the profile
- Click the 'Create' button

The Android profile will be created and the 'General Settings' section will be displayed with its default profile status as disabled.



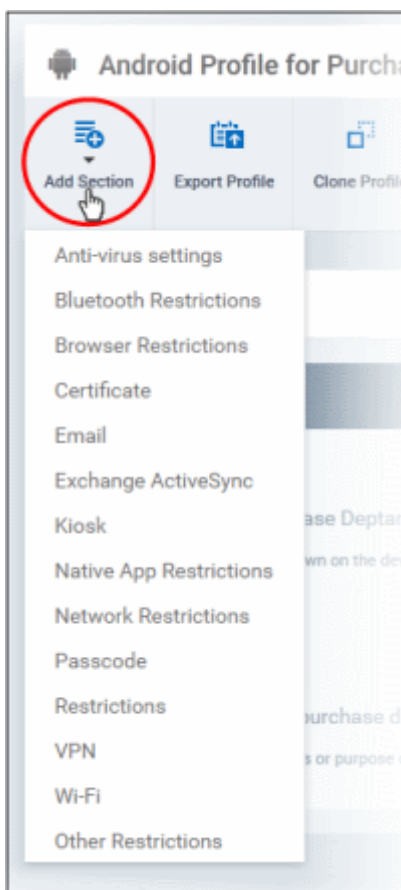
- If you want this profile to be a default policy, click on the 'Edit' button at the top right of the 'General' settings screen and select the check box beside 'Is Default'.



- Click the 'Save' button.

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

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

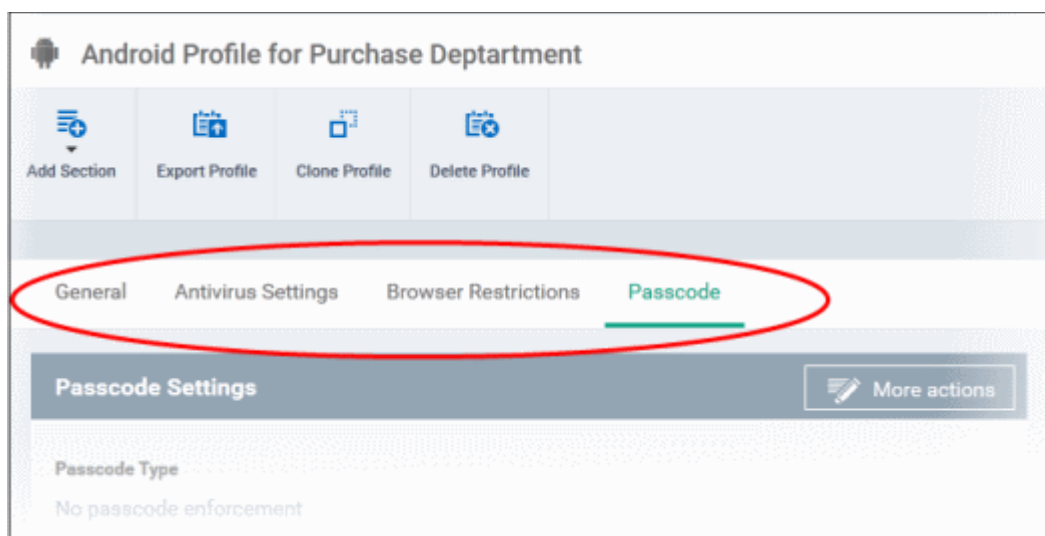


Note: Many Android profile settings have small information boxes next to them which indicate the OS and/or device required for the setting to work correctly.

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 and after saving the settings, it will be available as links at the top.



Following sections explain more about each of the settings:

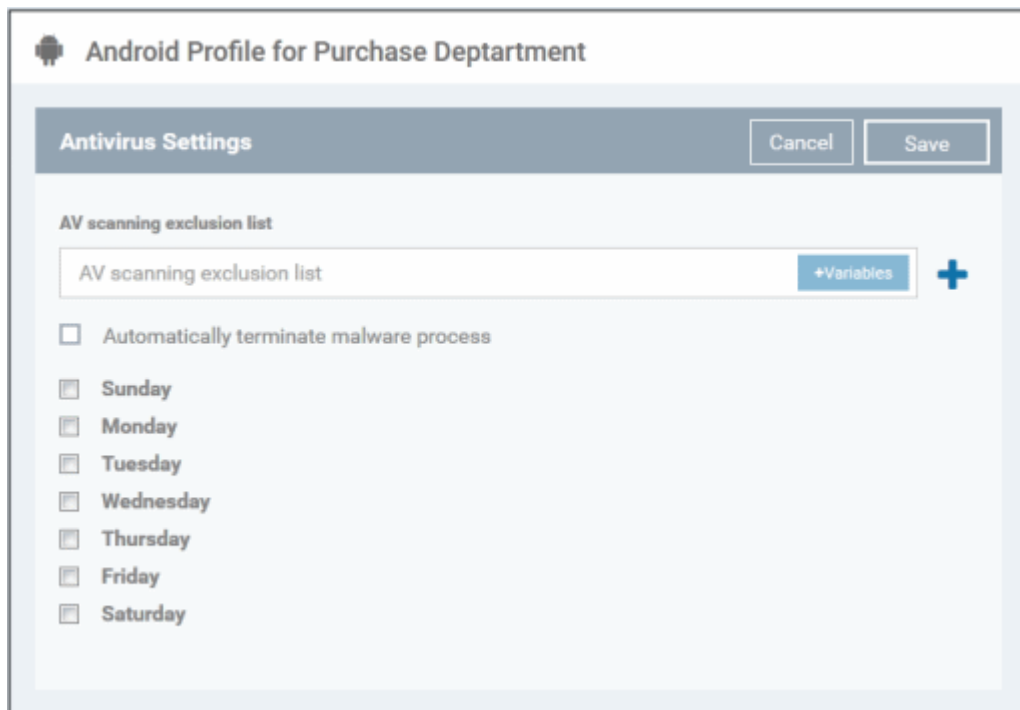
- **Antivirus**

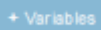
- [Bluetooth Restrictions](#)
- [Browser Restrictions](#)
- [Certificate](#)
- [Email](#)
- [Exchange Active Sync](#)
- [Kiosk](#)
- [Native App Restrictions](#)
- [Network Restrictions](#)
- [Passcode](#)
- [Restrictions](#)
- [VPN](#)
- [Wi-Fi](#)
- [Other Restrictions](#)




To configure Antivirus settings

- Click 'Anti-virus settings' from the 'Add Section' drop-down

The 'Antivirus Settings' screen will be displayed.



Antivirus Settings - Table of Parameters		
Form Element	Type	Description
AV scanning exclusion list	Text Field	Allows the administrator to add trusted Apps in the field. Antivirus scans will not be performed for these files. Enter the bundle identifier of the app that you want to exclude from antivirus scanning. For example, livio.pack.lang.en_US. You can also add variables by clicking the 'Variables' button  and

Antivirus Settings - Table of Parameters		
		clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables . Click  to add more 'AV scanning exclusions list' fields. To remove an item from the 'AV scanning exclusion list' field, click the  button beside it.
Automatically terminate malware process	Checkbox	If enabled, any malware process detected during scanning will be terminated immediately on the devices.
Schedule scan	Checkbox	Select if you want to automate the process of antivirus scanning. Select the checkbox beside the day(s) that you want the scheduled scan to run.

- Click the 'Save' button.

The saved 'Antivirus 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 Bluetooth Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Bluetooth Restrictions' from the 'Add Section' drop-down

The 'Bluetooth Restrictions Settings' screen will be displayed.

Bluetooth Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Device discovery via Bluetooth	Checkbox	Allows discovery of other devices via Bluetooth.
Allow Bluetooth Pairing	Checkbox	Allows users' devices to pair with other their devices via Bluetooth.
Allow Outgoing Calls	Checkbox	Allows users to make calls using Bluetooth enabled devices (eg. hands-free devices)

Bluetooth Restrictions Settings - Table of Parameters		
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.

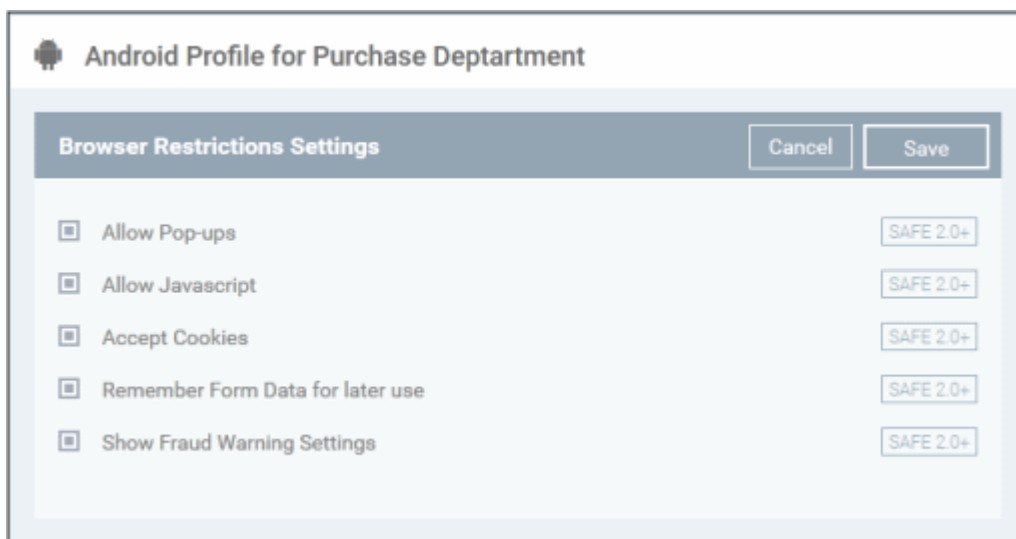
The saved 'Bluetooth Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Browser Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Browser Restrictions' from the 'Add Section' drop-down

The 'Browser Restrictions Settings' screen will be displayed.



Browser Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Pop-ups	Checkbox	Pop-ups in browsers will be allowed in the users' devices.
Allow Javascript	Checkbox	Applications running on Java scrips will be allowed.
Accept Cookies	Checkbox	Users will be allowed to modify Cookies settings on their devices.
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 use Fraud Warning Settings on their devices.

- Click the 'Save' button.



The saved 'Browser 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 Certificate settings

The 'Certificate Settings' section is used to upload certificates and 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.

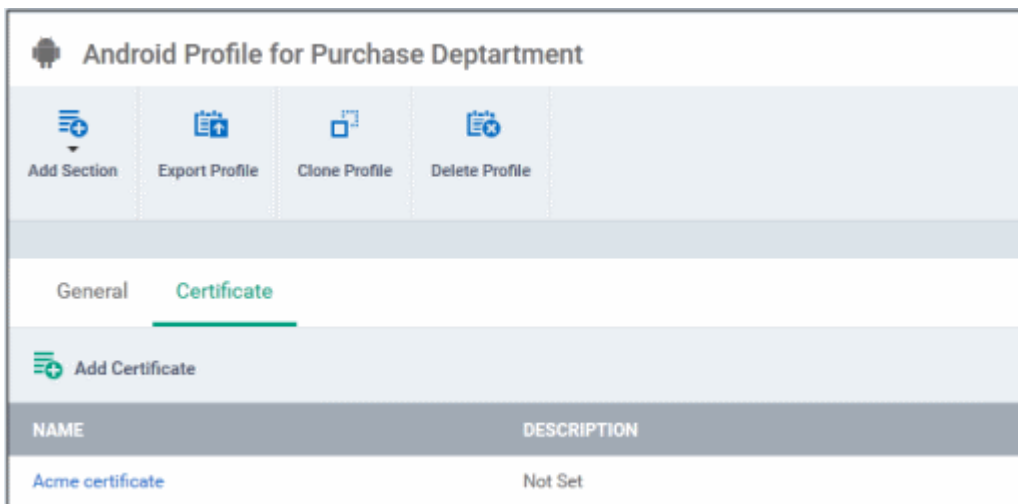
- Click 'Certificate' from the 'Add Section' drop-down

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  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. The extension should be in the format pub, crt or key.

- Click the 'Save' button.

The saved 'Certificate Settings' screen will be displayed with options to edit the settings or delete the section. You can add multiple Certificate sections for a profile and will be listed under the Certificate link in the profile.



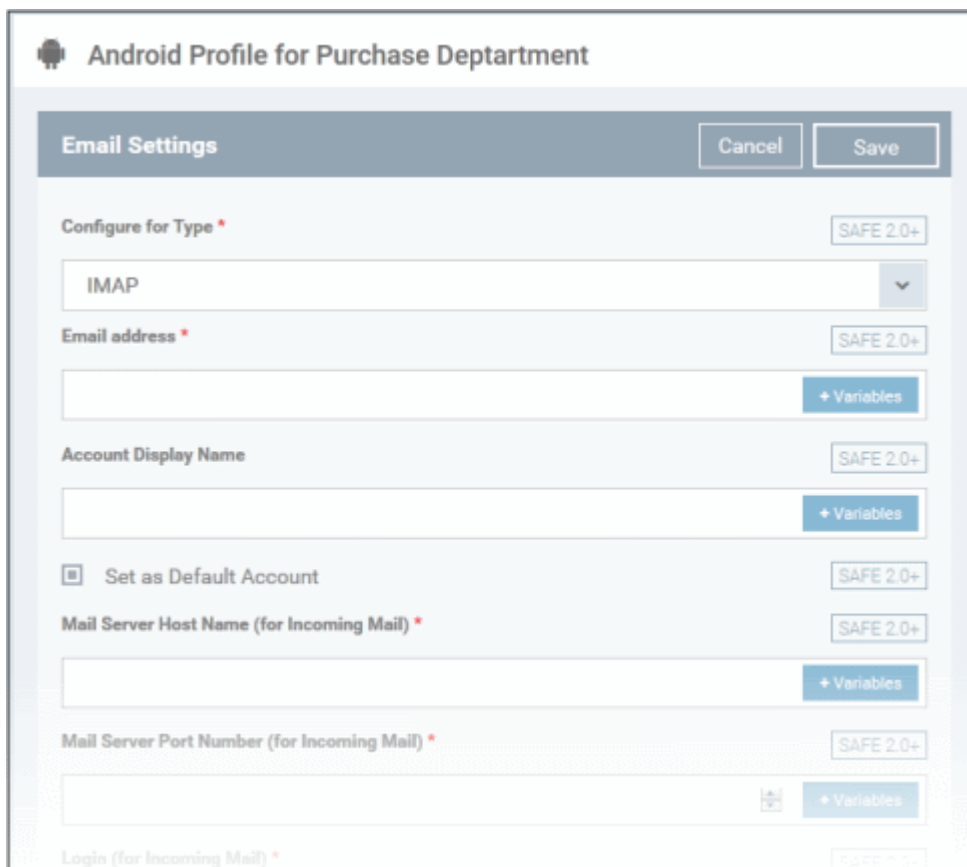
- To add another Certificate, click 'Add Certificate' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

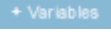



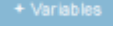







To configure Email settings

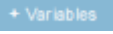





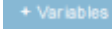

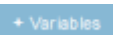



Note: The feature is supported for Samsung for Enterprise (SAFE) devices only. The administrator can configure the email settings on the devices through this settings.

- Click 'Email' from the 'Add Section' drop-down

The settings screen for Email 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  , and click  beside '%u.mail%' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Account Display Name	Text Field	If the profile is for a single user, enter the name to identify the user's email account at the incoming mail server. If the profile is for several users, click the 'Variables' button  , and click  beside '%u.login%' from the 'User Variables list'. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Set as Default Account	Checkbox	If enabled, the email account will be set as default for the users.
Mail Server Host Name (for Incoming Mail) *	Text Field	For a single user, enter the host name or IP address of the incoming mail server. For several users, add the variable to fetch the incoming mail server hostname/IP address by clicking the 'Variables' button  and clicking  beside the variable. For more details on variables, refer to the section Configuring Custom Variables .
Mail Server Port Number (for Incoming Mail) *	Text Field	For a single user, enter the server port number used for incoming mail service. For POP3, it is usually 110 and if SSL is enabled it is 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  and clicking  beside the variable. For more details on variables, refer to the section Configuring Custom Variables .
Login (for Incoming Mail)*	Text Field	If the profile is for a single user, enter the username for the email account of the user at the incoming mail server. If the profile is for several users, click the 'Variables' button  , select '%u.mail%' from the 'User Variables' list and click  . The email usernames of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Password (for Incoming Mail)*	Text Field	If the profile is for a single user, enter the password for the email account of the user at the incoming mail server. If the profile is for several users, click the 'Variables' button  and click  beside the variable from the list. The email passwords of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Use SSL Incoming	Checkbox	If enabled, communication between incoming mail server and devices is encrypted using SSL (Secure Socket Layer Protocol).
Accept All Certificates (for Incoming Mail)	Checkbox	If enabled, the device automatically accepts all SSL certificates.

Email Settings - Table of Parameters		
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  and click  beside the variable from the list. For more details on variables, refer to the section Configuring Custom Variables .
Mail Server Port Number (for Outgoing Mail) *	Text box	For a single user, enter the server port number used for outgoing (SMTP) mail service. If no port number is specified then ports 25, 587 and 465 are used in the given order. For several users, include the variable to fetch the outgoing mail server port number by clicking the 'Variables' button  and clicking  beside the variable from the list. For more details on variables, refer to the section Configuring Custom Variables .
Login (for outgoing Mail)*	Text Field	If the profile is for a single user, enter the username for the email account of the user at the outgoing (SMTP) mail server. If the profile is for several users, click the 'Variables' button  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 more details on variables, refer to the section Configuring Custom Variables .
Password (for outgoing Mail)*	Text Field	If the profile is for a single user, enter the password for the email account of the user at the outgoing (SMTP) mail server. If the profile is for several users, click the 'Variables' button  and click  beside the variable created to fetch the email password of the user from the 'User Variables' list. The email passwords of the users to whom the profile is associated will be automatically added to the profile while rolling out to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Use SSL (for Outgoing Mail)	Checkbox	If enabled, communication between outgoing mail server and devices is encrypted using SSL.
Accept All Certificates (for Outgoing Mail)	Checkbox	If enabled, the device automatically accepts all SSL certificates.
Accept TLS Certificates (for Outgoing Mail)	Checkbox	If enabled, automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol).
Sender Name	Text Field	For a single user, enter the name that should appear in the 'From' field of the sent emails from the device. For several users, add the variable to fetch the sender name by clicking the 'Variables' button  and clicking  beside the variable. For more details on variables, refer to the section Configuring Custom Variables .
Set Signature	Text Field	Enter the signature and other details that will appear at the end of the mails sent from the device. You can add variables to the text by clicking the 'Variables' button  and clicking  beside the variable. For more details on variables, refer to the section Configuring Custom Variables .

Email Settings - Table of Parameters		
		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 saved 'Email 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 Exchange ActiveSync settings

CDM allows you to configure users to access their mail accounts in Exchange Server.



Note: Please make sure that the intended users are not restricted to use Email client on their devices. Refer to the section **Native App Restriction** for more details.



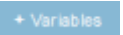





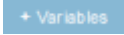



- Click 'Exchange Active Sync' from the 'Add Section' drop-down

The 'Active Sync Settings' screen will be displayed.

The screenshot shows the 'Active Sync Settings' configuration screen for an Android profile. The title is 'Android Profile for Purchase Department'. Below the title is a dark blue header with 'Active Sync Settings', 'Cancel', and 'Save' buttons. The main area contains five form fields, each with a 'SAFE 2.0+' label and a '+ Variables' button:

- Email Address ***: Text input field with a 'SAFE 2.0+' label and a '+ Variables' button.
- User Name ***: Text input field with a 'SAFE 2.0+' label and a '+ Variables' button.
- Domain ***: Text input field with a 'SAFE 2.0+' label and a '+ Variables' button.
- Server Address ***: Text input field with a 'SAFE 2.0+' label and a '+ Variables' button.
- Password**: Text input field with a 'SAFE 2.0+' label and a '+ Variables' button.

Exchange ActiveSync Settings - Table of Parameters		
Form Element	Type	Description
Email Address *	Text Field	Click the 'Variables' button  and click  beside '%u.mail' from the

Exchange ActiveSync Settings - Table of Parameters		
		User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables .
User Name *	Text Field	Click the 'Variables' button  and click  beside '%u.login' from the User Variables' list. The username of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables .
Domain *	Text Field	Enter the domain name in the field. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Server Address *	Text Field	Enter the server address of the ActiveSync. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Password	Text Field	Leave the field blank. The user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Account Display Name	Text Field	If the profile is for a single user, enter the name to identify the user's email account at the exchange server. If the profile is for several users, click the 'Variables' button  and click  beside '%u.login%' from the 'User Variables list'. The email address of the users to whom the profile is associated will be automatically added to the profile while rolling out the same to the devices. For more details on variables, refer to the section Configuring Custom Variables .
Email Signature	Text Field	Enter the signature and other details that will appear at the end of the mails sent from the device. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Maximum Email Size	Comobo Box	The maximum size of email that the user can download from the server. Use the controls or enter the value in the field. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Sync Emails	Drop-down	Choose the period for which the emails are to be kept synchronized between the device and the exchange server from the recent past, from the drop-down.
Sync Calendar	Drop-down	Select the period for which the calendar events are to be synchronized between the device and the exchange server, from the drop-down.
Use SSL	Checkbox	If enabled, communication between the device and the exchange server is encrypted using SSL (Secure Socket Layer Protocol).
As Default Account	Checkbox	If enabled, the email address will be used as default for sending out emails.
Accept All Certificates	Checkbox	If enabled, the device automatically accepts all SSL certificates.
Can Sync Contacts	Checkbox	Select this option if you wish to allow synchronization of user contacts between device and exchange server.

Exchange ActiveSync Settings - Table of Parameters		
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 Vibrate 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 saved 'Active Sync 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.

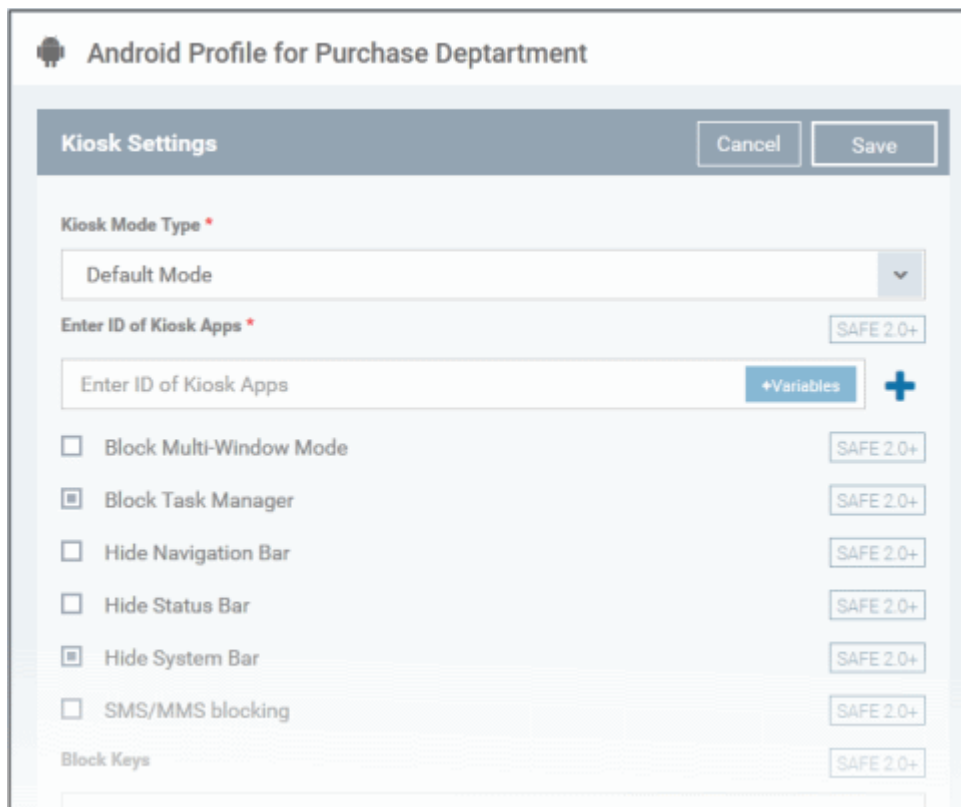
To configure Kiosk settings





Note: The feature is supported for Samsung for Enterprise (SAFE) devices only.

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. The main goal of Kiosk mode is to lock a device into a particular application, to either allow a single app or multiple apps, to take over the screen of a device, such as in-house applications, or to prevent users from opening other applications that should not be accessible to them, such as in retail environments. For example, if employees are using an Galaxy Tab for a corporate app, or admins simply need to ensure devices are only running a single application - Kiosk mode will ensure your devices are being used as intended.

- Click 'Kiosk' from the 'Add Section' drop-down

The 'Kiosk Settings' screen will be displayed.



Kiosk Settings - Table of Parameters		
Form Element	Type	Description
Kiosk Mode Type	Drop-down	<p>The two Kiosk modes are:</p> <ul style="list-style-type: none"> • 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 CDM console. <p>Restrictions on access to other device functions, such as task manager and the status bar, can also be configured for either mode.</p>
If 'Single App' is selected as Kiosk Mode Type:		
Enter ID of Kiosk Apps	Text Field	Enter the ID of the app that will run in Kiosk mode.
If 'Default mode' is selected as Kiosk Mode Type:		
Enter ID of Kiosk Apps	Text Field	<p>Enter the ID of the apps that will run in Kiosk mode. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Click  to add more 'App IDs for allowed Apps om Kiosk Mode' fields.</p> <p>To remove a field, click the  button beside it.</p>
Block Multi-Window Mode	Checkbox	If selected, users cannot open multiple windows.

Kiosk Settings - Table of Parameters		
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	Text Field	<p>This feature allows to block keypad buttons available on the devices. For example, if you do not want the device owners to use Caps Lock key and so on, then these can be blocked.</p> <p>To select the key to be blocked, click in the 'Block Keys' field:</p> <div style="text-align: center; border: 1px solid #ccc; padding: 5px; width: fit-content; margin: 10px auto;"> Select Keys </div> <p>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.</p> <div style="text-align: center; border: 1px solid #ccc; padding: 5px; width: fit-content; margin: 10px auto;"> ✕ 2 ✕ 5 ✕ Envelope ✕ F9 </div>
The following features will be visible if 'Default mode' is selected as Kiosk Mode Type:		
Show messenger App	Checkbox	If selected, the messenger app will be available.
Show email App	Checkbox	If selected, email app will be available.
Show dialer App	Checkbox	If selected, dialer app will be available.
Show admin bypass button	Checkbox	If selected, the 'Admin bypass button' will be available, which an admin can tap, enter the password to exit from the Kiosk mode.
Admin bypass password	Text Field	Enter the password required to exit the Kiosk mode. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .

- Click the 'Save' button.

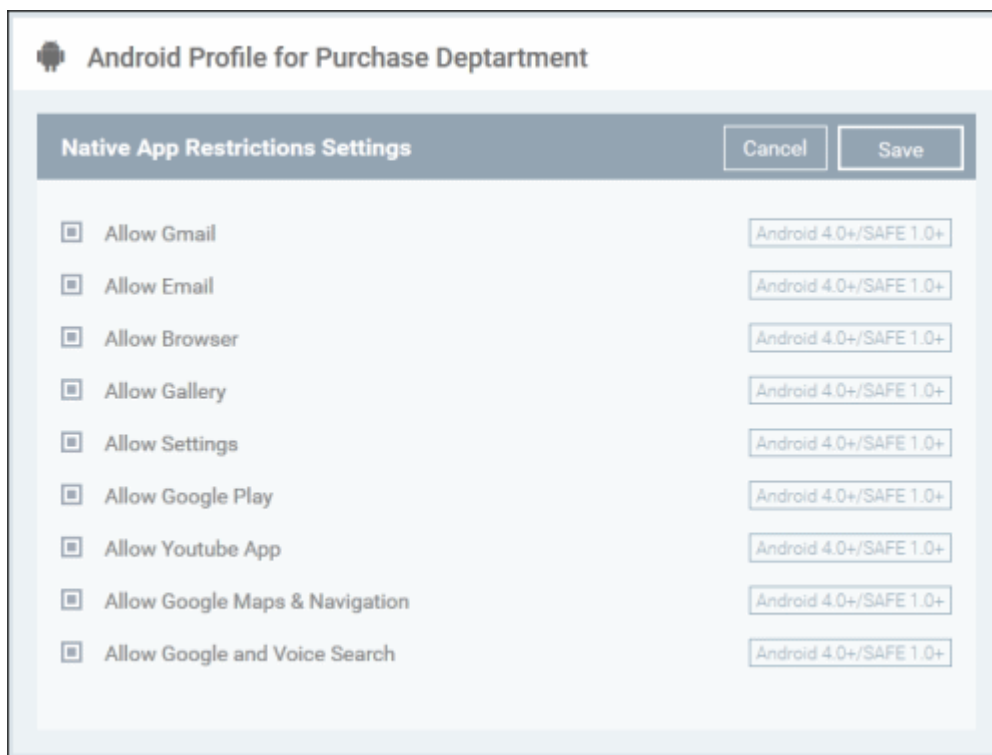
The saved 'Kiosk Settings' screen will be displayed with options to edit the settings or delete the section. Refer to the section [Editing Configuration Profiles](#) for more details.

To configure Native App Restrictions settings

Applications such as Gmail, Email client, Gallery, that come built-in with the device operating system 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 Section' drop-down

The 'Native App Restriction Settings' screen will be displayed.



Native Application Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Gmail	Checkbox	Select this to allow users to access Gmail app.
Allow Email	Checkbox	Select this to allow users to access default Email app.
Allow Browser	Checkbox	If enabled, users can access default browser on their devices.
Allow Gallery	Checkbox	If enabled, users can access Gallery on their devices.
Allow Settings	Checkbox	Select this to enable users to change device settings.
Allow Google Play	Checkbox	If enabled, users can access Google Play on thier mobile devices.
Allow YouTube App	Checkbox	If enabled, users can access YouTube.
Allow Google Maps & Navigation	Checkbox	If enabled, users can access Google Maps and Navigation app on their via mobile devices.
Allow Google and Voice Search	Drop-down	If enabled, users can use Google and Voice Search services.

- Click the 'Save' button.

The saved 'Native App Restriction 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 Network Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click 'Network Restrictions' from the 'Add Section' drop-down

The 'Network Restriction Settings' screen will be displayed.

Android Profile for Purchase Department

Network Restrictions Settings
Cancel
Save

Allow Emergency Calls only
 Allow Voice Roaming
 Allow Sync during Roaming
 Allow Data Roaming
 Allow USB Tethering
 Allow wi-fi access point settings editing
 Allow user to add Wi-Fi networks

Wi-Fi Network Minimum Security Level

Open

Allow SMS

All

Allow MMS

All

Blacklisted SSIDs

Blacklisted SSIDs
+Variables
+

SAFE 2.0+

SAFE 3.0+

SAFE 1.0+

SAFE 2.2+

SAFE 2.2+

SAFE 2.2+

SAFE 2.2+

SAFE 2.0+

SAFE 3.0+





SAFE 3.0+

SAFE 2.2+

Network Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Emergency Calls only	Checkbox	Allows users to make emergency calls only.
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/disable data roaming option in their devices.
Allow USB Tethering	Checkbox	Allows users to share USB with other similar devices.
Allow Wi-Fi access point settings editing	Checkbox	Allows users to edit the Wi-Fi access point settings.
Allow user to add Wi-Fi networks	Checkbox	Allows users to add 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: <ul style="list-style-type: none"> Open WEP WPA 802.1x EAP (LEAP)

Comodo Device Manager - Administrator Guide | © 2016 Comodo Security Solutions Inc. | All rights reserved

174

Network Restrictions Settings - Table of Parameters		
		<ul style="list-style-type: none"> 802.1x EAP (FAST) 802.1x EAP (PEAP) 802.1x EAP (TTLS) 802.1x EAP (TLS)
Allow SMS	Drop-down	<p>Allows text messages per the options selected:</p> <ul style="list-style-type: none"> 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	<p>Allows multimedia messages per the options selected:</p> <ul style="list-style-type: none"> 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	<p>Specify the name (SSID) of the wireless network that should be blacklisted. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Click the  button to add more 'Blacklisted SSID' fields. To remove a Blacklisted SSID field from the screen, click the minus  button beside it.</p>

- Click the 'Save' button.

The saved 'Network Restriction 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 Passcode settings

- Click 'Passcode' from the 'Add Section' drop-down

The settings screen for Passcode will be displayed.

Android Profile for Purchase Department

Passcode Settings
Cancel Save

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 Peak

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: <ul style="list-style-type: none"> No passcode enforcement Only letters Letters and numbers Only numbers 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.

Passcode Settings - Table of Parameters		
Form Element	Type	Description
Maximum Failed Attempts for Sneak Peak	Drop-down	<p>Select the maximum number of allowed unsuccessful login attempts for 'Sneak Peak' feature (4-16). Set the value as '0' for unlimited.</p> <p>The 'Sneak Peak' feature in CDM instructs the device to capture the photograph of the person entering the passcode through the front camera and forward it to the CDM server, if the passcode is entered incorrectly a certain number of times.</p> <p>The photograph(s) sent by the device can be viewed from the View Device interface that can be accessed by clicking 'Inventory' > 'Devices' > the device name > 'Sneak Peak' tab. Refer to the section Viewing Sneak Peak Pictures to Locate Lost Devices for more details.</p> <p>This can be useful to identify the possessor and location of the device if it is lost or stolen and if somebody tries to login to the device using guessed passcodes.</p> <p>Note: If the device does not have a front camera, the rear camera will capture a photograph and forward to the CDM server.</p>
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	<p>Configure the password reuse policy by setting the number of unique new passcodes that must be associated with the user before an old passcode can be used.</p> <p>This feature is available for Android 3.0 and later versions only.</p>

- Click the 'Save' button.

The saved 'Password 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 Restrictions settings

- Click 'Restrictions' from the 'Add Section' drop-down

The 'Restriction Settings' screen will be displayed.

Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow Turn-off background Sync	Checkbox	Select this to allow users to disable background synchronization setting on their devices.
Allow Bluetooth	Checkbox	Select this to allow users to enable / disable Bluetooth on their devices.
Allow Camera	Checkbox	Select this to allow users to use the camera
Allow Un-encrypted devices	Checkbox	Select this to enable users to use device without turning on the storage encryption feature. This feature is available for Android 3.0 and later versions only.
Allow to run Apps installed from unknown sources	Checkbox	Select this to allow users to run installed applications that were download from unknown sources
Cellular Connection Control	Radio Buttons	<p>Choose whether or not to allow the device to connect to Internet through cellular network (2G/3G/4G) from the options.</p> <ul style="list-style-type: none"> 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' in the device.

Restrictions Settings - Table of Parameters		
WiFi Connection Control	Radio Buttons	<p>Choose whether or not to allow the device to connect to WiFi networks and hotspots from the options.</p> <ul style="list-style-type: none"> 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	<p>Choose whether or not to allow the location services on the device from the options:</p> <ul style="list-style-type: none"> 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 saved 'Restriction 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 VPN settings



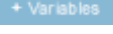

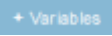

Note: The feature is supported for only Samsung for Enterprise (SAFE) devices.

- Click 'VPN' from the 'Add Section' drop-down

The settings screen for VPN will be displayed.

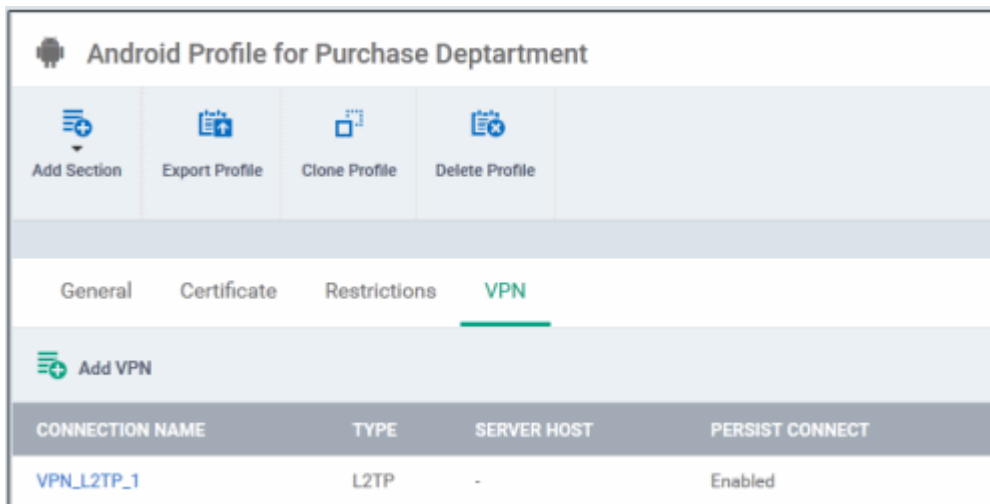
VPN Settings - Table of Parameters

Form Element	Type	Description
Configure for type	Drop-down	Choose the VPN connection type from drop-down. The options available are: L2TP, PPTP, L2TP/IPSec PSK, IPSec, XAuth PSK and IPSec XAuth RSA.
VPN Connection Name	Text Field	Enter the name of the connection, which will be displayed on the device. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Host name of the VPN Server	Text Field	Enter the IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Username	Text Field	For a single user account for VPN connection, enter the username for connection to the network. For several users, click the 'Variables' button , + Variables select the variable for fetching the VPN username from the 'Variables list' and click + . The usernames of the users to whom the profile is associated will be automatically included in the profile while rolling out the profile to respective devices. For more details on variables, refer to the section Configuring Custom Variables .

VPN Settings - Table of Parameters		
Password	Text Field	If the profile is for a single user account for VPN connection, enter the password for the account. If the profile is for several users, click the 'Variables' button  , 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  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:		
<ul style="list-style-type: none"> • Enable L2TP Secret 	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
<ul style="list-style-type: none"> • 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:		
<ul style="list-style-type: none"> • Enable Encryption 	Checkbox	If selected, the connection is encrypted between the devices and the VPN server.
If L2TP/IPSec PSK is selected:		
<ul style="list-style-type: none"> • Enable L2TP Secret 	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
<ul style="list-style-type: none"> • 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'
<ul style="list-style-type: none"> • 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:		
<ul style="list-style-type: none"> • IP Sec Identifier 	Text Field	Enter the IPSec identifier in the field. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
<ul style="list-style-type: none"> • 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'
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: <ul style="list-style-type: none"> • 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 saved 'VPN Settings' screen will be displayed with options to edit the settings or delete the VPN section. You can add multiple VPN sections for a profile and will be listed under the VPN link in the profile.

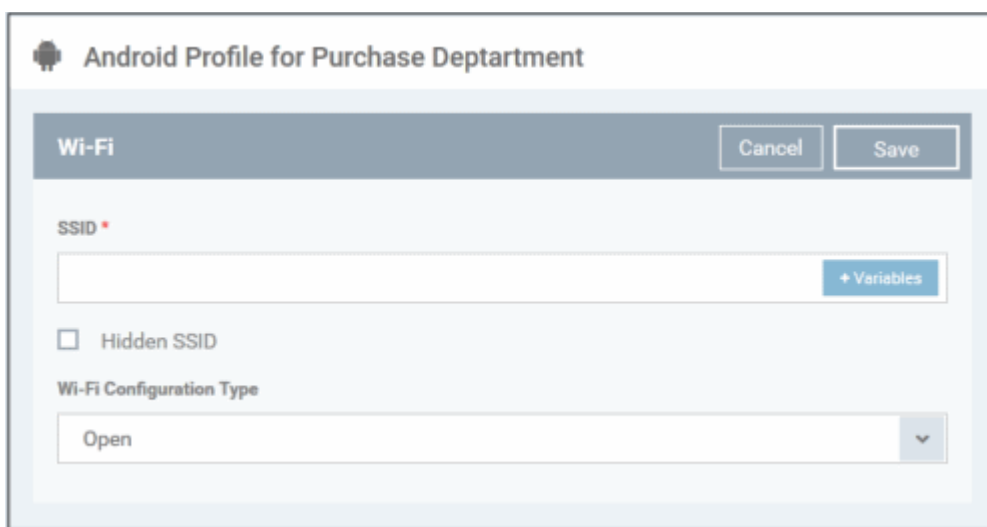


- To add another VPN section, click 'Add VPN' above the 'Connection Name' column
- Click on the link under 'Connection Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Section' drop-down



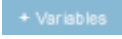

The settings screen for Wi-Fi will be displayed.



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 the access hidden wireless network also. The 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:

Wi-Fi Settings - Table of Parameters	
	<ul style="list-style-type: none"> • Open • WEP • WPA / WPA2 - PSK • 802.1x EAP <p>The settings for each type is explained in the next table Wi-Fi configuration type settings.</p>

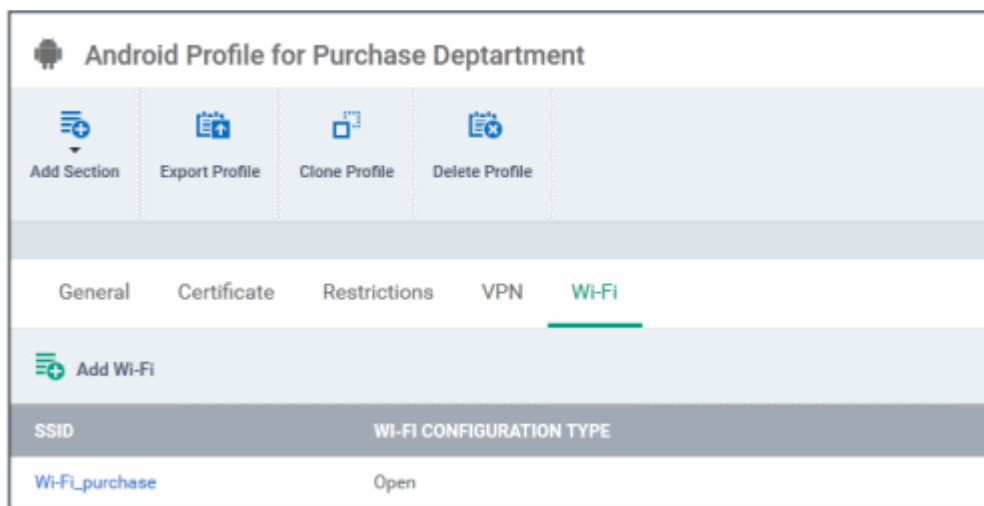
Wi-Fi Configuration Type settings

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  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  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
802.1x EAP	<p>1. EAP Authentication Protocol - Select the EAP authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <ul style="list-style-type: none"> • PEAP • TLS • TTLS <p>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.</p> <ul style="list-style-type: none"> • None • PAP • MSCHAP • MSCHAPV2 • GTC <p>3. Certificate - Select the user certificate from the drop-down or upload it using the 'Add New' button.</p> <p>4. CA Certificate - Select the CA certificate from the drop-down or upload it using the 'Add New' button.</p> <p>5. Authentication Username - Enter the username for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p>6. Authentication Password - Enter the password for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p>7. Authentication Domain - Enter the details for RADIUS Server authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p>

Wi-Fi Configuration Type Settings - Table of Parameters	
	<p>8. Anonymous Identity - Enter the username that can be used for anonymous access. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p>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.</p> <p>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.</p>

- Click the 'Save' button after entering or selecting the parameters.

The saved 'Wi-Fi' settings' screen will be displayed with options to edit the settings or delete the section. You can add multiple Wi-Fi sections for a profile and will be listed in the SSID column.



- To add another Wi-Fi section, click 'Add Wi-Fi' above the 'SSID' column name
- Click on the link under 'SSID' to edit the setting or delete the section. 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 Section' drop-down

The 'Other Restrictions Settings' screen will be displayed.

Other Restrictions Settings - Table of Parameters		
Form Element	Type	Description
Allow USB	Checkbox	Allows users to establish connections via USB ports.
Use Network Time	Checkbox	Allows users to enable/disable network provided values in Date & Time settings.
Allow Microphone	Checkbox	Allows users to use microphone. If this is disabled, users can use microphone for receiving and making calls only.
Allow Near Field Communication (NFC)	Checkbox	Allows devices to establish connection via NFC
Allow Mock Locations	Checkbox	Allows users to enable/disable 'Mock Location' in developer mode settings.
Allow SD Card	Checkbox	Users can use SD card on their devices.
Allow SD Card Write	Checkbox	Users can store data on the SD card.
Allow Screen Capture	Checkbox	Users can take screenshot of the device screen.
Allow Clipboard	Checkbox	Users will be allowed to use clipboard memory.
Backup my data	Checkbox	Users will be allowed to take a backup of data in their devices.
Visible Passwords	Checkbox	Allows users to enable/disable show password feature.
Allow USB Debugging	Checkbox	Allows users to enable/disable 'USB Debugging' option in developer mode settings.
Allow Factory Reset	Checkbox	Users are allowed to reset the device to factory settings.
Allow OTA Upgrade	Checkbox	Over-the-air (OTA) upgrade is the wireless delivery of data or new software to mobile phones and tablets.

- Click the 'Save' button.

The saved 'Other 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.

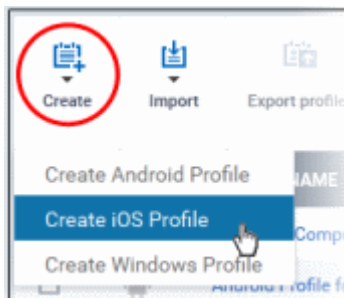
6.1.2. Profiles for iOS Devices

iOS Profiles allow you to specify a device's network access rights, restrictions and other general system settings.

To create an iOS profile

- Click 'Profiles' from the left then choose 'Profiles List'
- Click 'Create' then select 'Create iOS Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profile List'.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Section' button. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices and device groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

- This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.
- To create a new profile, click 'Profiles > Profile List > Create':

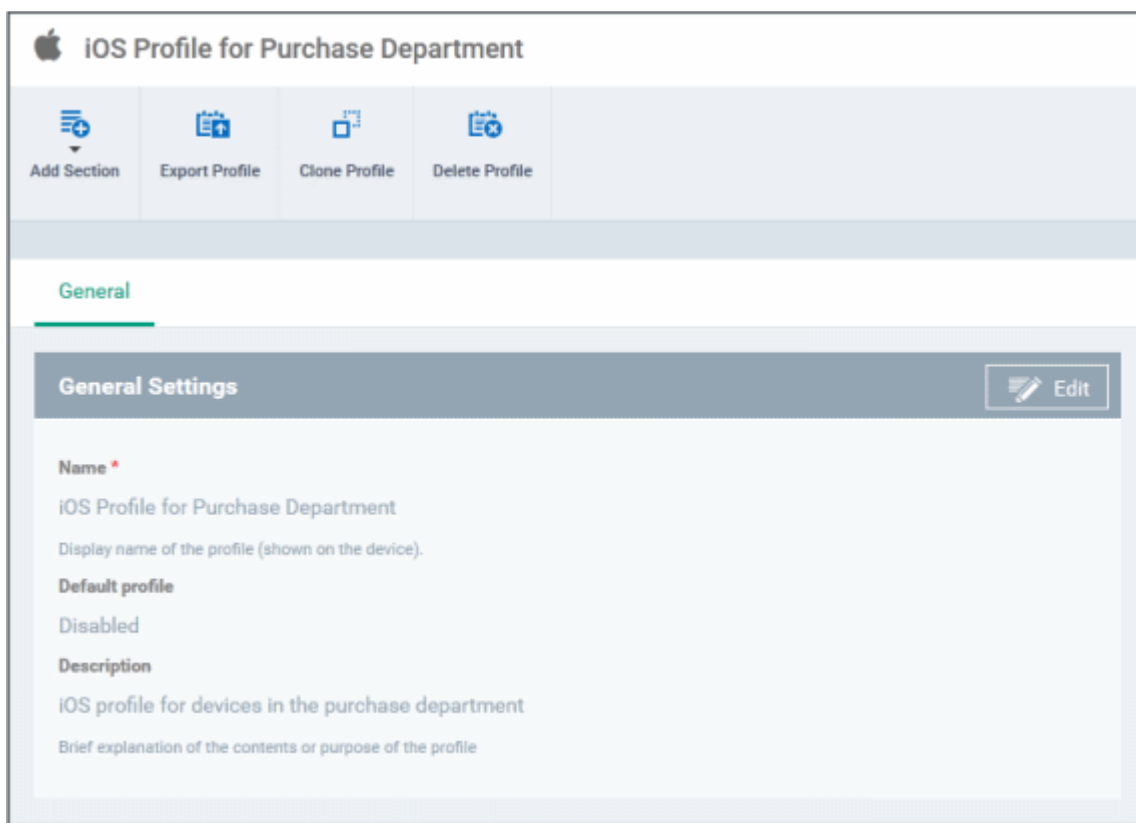


The 'Create iOS Profile' screen will be displayed.

A screenshot of a web form titled 'Create iOS Profile' with a 'Close' button in the top right corner. The form has two input fields: 'Name' with a red asterisk indicating it is required, and 'Description'. Below the input fields is a blue 'Create' button.

- 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 with its default profile status as disabled.



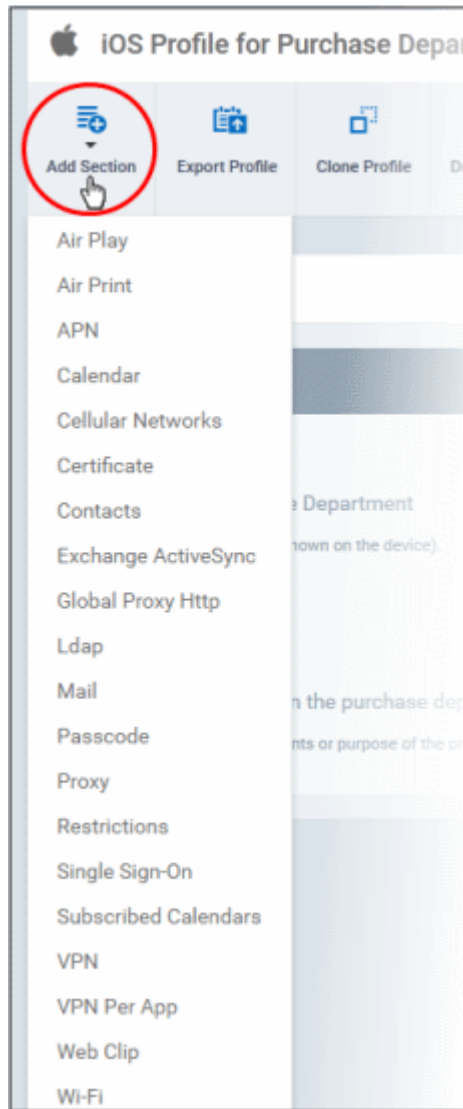
- If you want this profile to be a default policy, click on the 'Edit' button at the top right of the 'General' settings screen and select the check box beside 'Default Profile'.

The screenshot displays the 'General Settings' for an iOS profile named 'iOS Profile for Purchase Department'. The interface includes a top navigation bar with 'Add Section', 'Export Profile', 'Clone Profile', and 'Delete Profile' buttons. Below the profile name, there are icons for 'Add Section', 'Export Profile', 'Clone Profile', and 'Delete Profile'. The 'General Settings' section contains a 'Name' field with the value 'iOS Profile for Purchase Department' and a 'Description' field with the value 'iOS profile for devices in the purchase department'. A 'Default profile' checkbox is checked and circled in red. A red arrow points from the 'Edit' button in the top right corner to the 'Default profile' checkbox. The 'Save' button is visible in the bottom right corner of the settings panel.

- Click the 'Save' button.

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

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

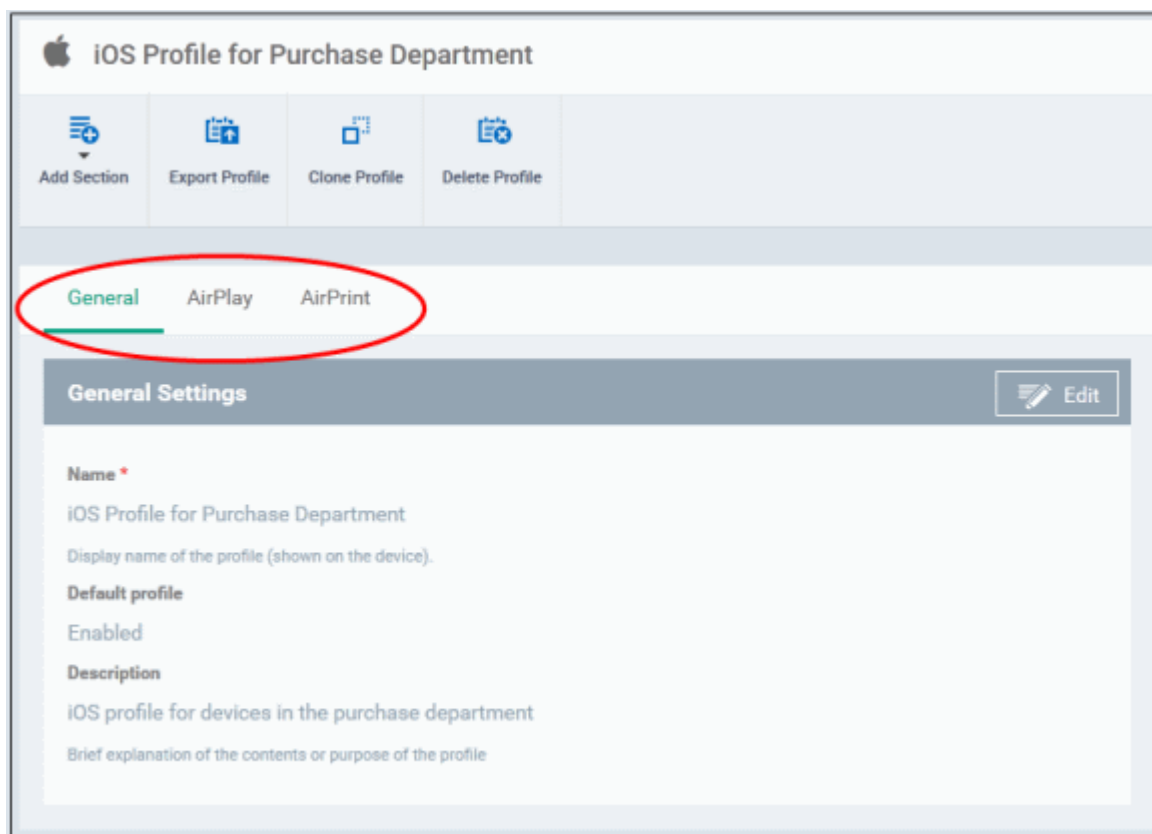


Note: Many iOS profile settings have small information boxes next to them which indicate the iOS version required for the setting to work correctly.

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 and after saving the settings, it will be available as links at the top.











Following sections explain more about each of the settings:

- [Air Play](#)
- [Air Print](#)
- [APN](#)
- [Calendar](#)
- [Cellular Networks](#)
- [Certificate](#)
- [Contacts](#)
- [Exchange Active Sync](#)
- [Global Proxy HTTP](#)
- [LDAP](#)
- [Mail](#)
- [Passcode](#)
- [Proxy](#)
- [Restrictions](#)
- [Single Sign-On](#)
- [Subscribed Calendars](#)
- [VPN](#)
- [VPN Per App](#)
- [Web Clip](#)
- [Wi-Fi](#)

To configure AirPlay settings

- Click 'Air Play' from the 'Add Section' drop-down

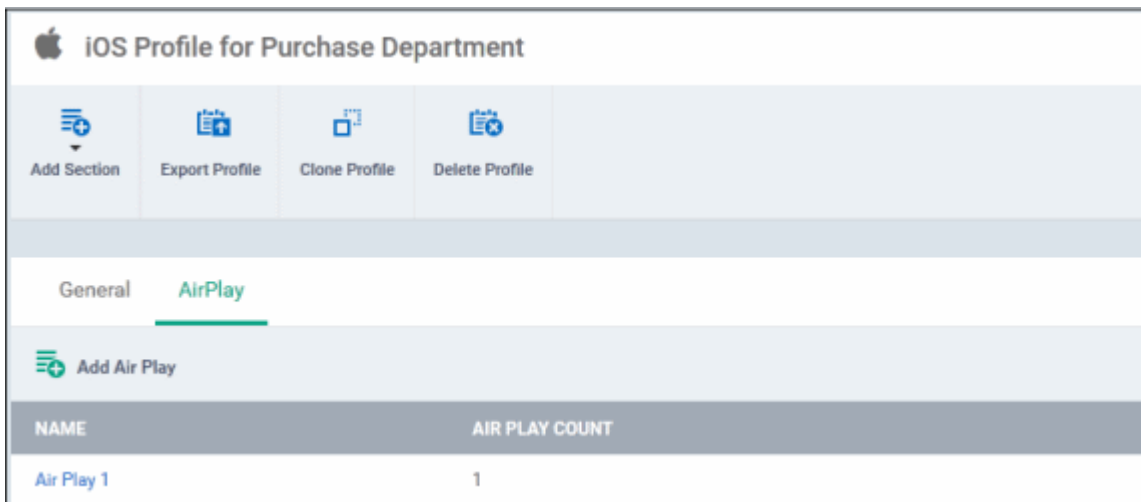
The 'Air Play' settings screen will be displayed.

AirPlay Settings Configuration - Table of Parameters		
Form Element	Type	Description
White List Devices ID	Text Field	<p>Enter the device ID of AirPlay destinations that you want to whitelist. The ID numbers of the devices should be entered in the format as given below: XX:XX:XX:XX:XX:XX</p> <p>Note: The whitelist is applicable for supervised iOS 7+ devices and will not apply for all other devices.</p> <p>You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p> Click  button to add more 'Device ID' fields. To remove an AirPlay destination device, click the  button beside it.</p>
Device Name	Text Field	<p>Enter the name of the AirPlay destination device that you entered above. You can also add a variable to the field by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Click the 'Add' button to add more 'Device name' and 'Password' fields. To remove an AirPlay device, click the  button beside it.</p>
Password	Text Field	Enter the password for the AirPlay destination that you entered above.

AirPlay Settings Configuration - Table of Parameters		
Add	Button	Click this button to add another 'Devices' section.

- Click the 'Save' button.

The saved 'Air Play' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Air Play sections for a profile and will be listed under the AirPlay link in the profile.

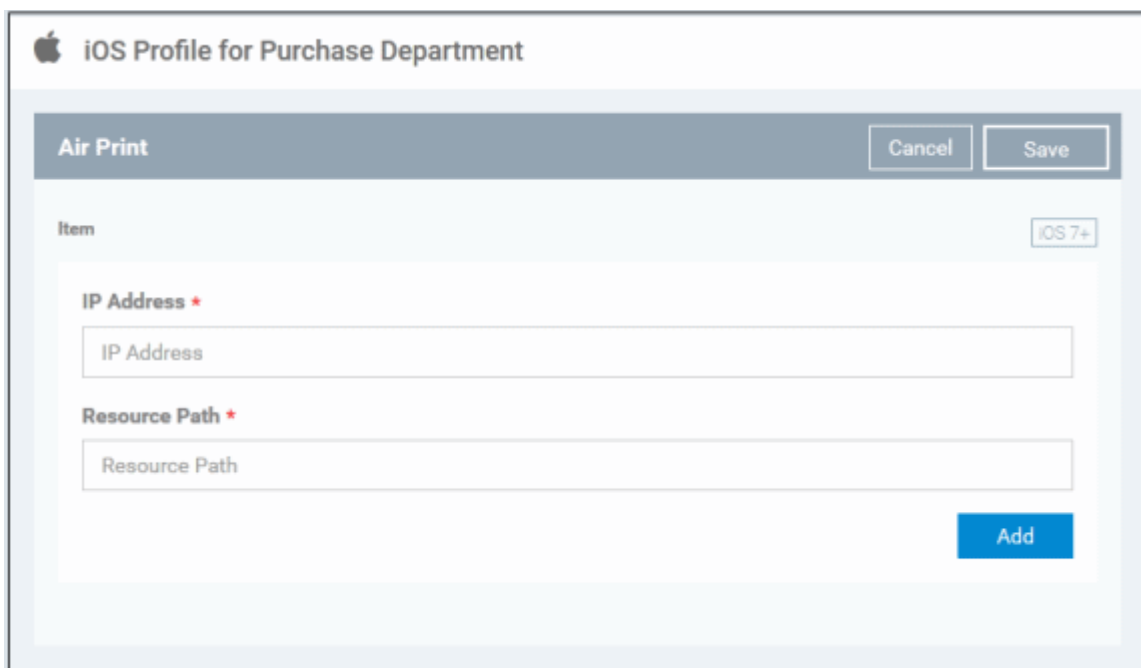







- To add another Air Play section, click 'Add Air Play' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure AirPrint settings

- Click 'Air Print' from the 'Add Section' drop-down

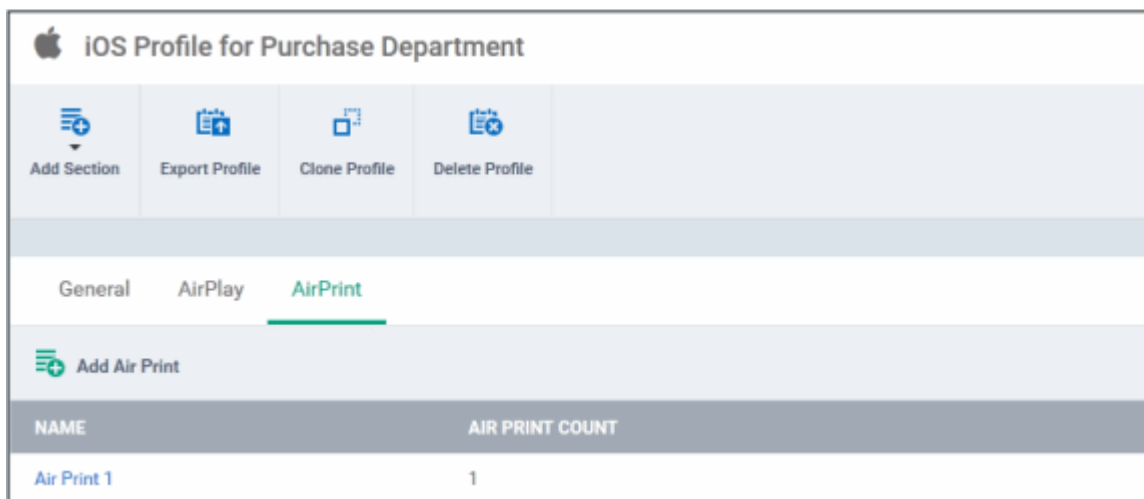
The 'Air Print' settings screen will be displayed.



AirPrint Settings - Table of Parameters		
Form Element	Type	Description
IP Address	Text Field	Enter the device ID of AirPrint destination (printer). You can also add variables by clicking the 'Variables' button  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 'IP address' and 'Resource path' fields. To remove an AirPrint device, click the x button beside it.
Resource Path	Text Field	Enter the resource path of the printer, for example, printers/ HP_LaserJetPro_M1136_series. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Add	Button	Click this button to add another AirPrint section.

- Click the 'Save' button.

The saved 'Air Print' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Air Print sections for a profile and will be listed under the AirPrint link in the profile.



- To add another Air Print section, click 'Add Air Print' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section ['Editing Configuration Profiles'](#) for more details.

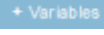









To configure APN settings

Note: The APN settings is deprecated in favor of the Cellular settings in iOS 7 and later versions.

- Click 'APN' from the 'Add Section' drop-down

The 'APN' settings screen will be displayed.

APN Settings - Table of Parameters

Form Element	Type	Description
Access Point Name (APN)	Text Field	Enter the name of the GPRS access point provided by the carrier. You can also add variables by clicking the 'Variables' button  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  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  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  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  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 saved 'APN' 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 Calendar settings

- Click 'Calendar' from the 'Add Section' drop-down

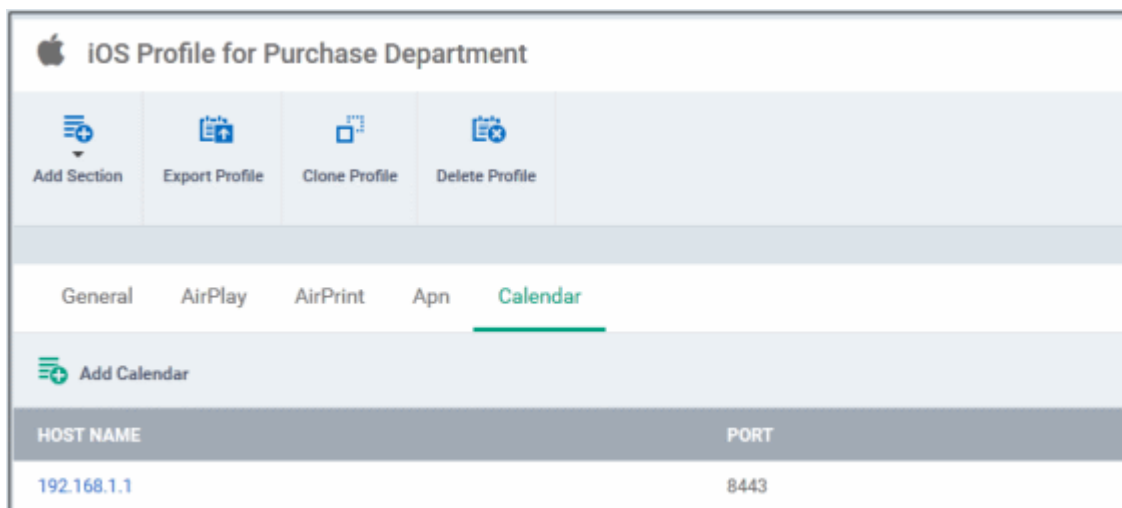
The 'Calendar Settings' screen will be displayed.

Calendar Settings - Table of Parameters		
Form Element	Type	Description
Account Description	Text Field	Enter the display name of the CalDav account. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Account Host Name	Text Field	Enter the CalDav host name or IP address. You can also add variables by

Calendar Settings - Table of Parameters		
		clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Account 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 .
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 .

- Click the 'Save' button after entering or selecting the parameters.

The saved 'Calendar Settings' screen will be displayed with options to edit the settings or delete the section. You can add multiple 'Calendar' sections for a profile and will be listed under the 'Calendar' link in the profile.



- To add another Calendar section, click 'Add Calendar' above the 'Host Name' column
- Click on the link under 'Host Name' to edit the setting or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure Cellular Network settings



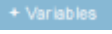




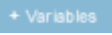



Note: A cellular network setting cannot be applied if an APN setting is already installed. This feature is available for iOS 7 and later versions only.

- Click 'Cellular Networks' from the 'Add Section' drop-down

The 'Cellular Networks' settings screen will be displayed.

Cellular Settings - Table of Parameters

Form Element	Type	Description
Name	Text Field	Enter the name for this configuration, specifying the cellular service provider. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Authentication Type	Drop-down	Select the authentication type from the drop-down. The options are CHAP or PAP.

Cellular Settings - Table of Parameters		
Username	Text Field	Enter the user name used for authentication. You can also add variables by clicking the 'Variables' button  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  and clicking  beside the 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  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  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  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  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 saved 'Cellular Network' 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 Certificate settings

The 'Certificate Settings' section is used to upload certificates and 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.

- Click 'Certificate' from the 'Add 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. The extension should be in the format pub, crt or key.

- Click the 'Save' button.

The saved 'Certificate Settings' screen will be displayed with options to edit the settings or delete the section. You can add multiple Certificate sections for a profile and will be listed under the Certificate link in the profile.

- To add another Certificate section, click 'Add Certificate' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Contacts settings

- Click 'Contacts' from the 'Add Section' drop-down

The 'Contacts Settings' screen will be displayed.

iOS Profile for Purchase Department

Contacts Settings [Cancel] [Save]

Account Description
[Text Field] + Variables
The display name of the account (e.g. "Company CardDAV Account")

Account Hostname *
[Text Field] + Variables
The CardDAV hostname or IP address and port number



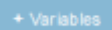

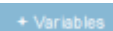

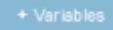

Account Port *
[Text Field] + Variables

Account Username
[Text Field] + Variables
The CardDAV username

Account Password
[Text Field] + Variables
The CardDAV password

Use SSL
Enable Secure Socket Layer communication with CardDAV server

Principal URL
[Text Field] + Variables
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  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  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  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  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 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, the users can access the account without entering the password.
Use SSL	Checkbox	If enabled, SSL connection will be established with the CardDav server.
Principal URL	Text Field	Enter the Principal URL of the CardDav account.

- Click the 'Save' button after entering or selecting the parameters.








The saved 'Contacts 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 Exchange ActiveSync settings

- Click 'Exchange ActiveSync' from the 'Add Section' drop-down

The 'Exchange' settings screen will be displayed.

Exchange 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

Exchange ActiveSync Settings - Table of Parameters		
		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  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  and click  beside '%u.mail' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section Configuring Custom Variables .
User Name	Text Field	User name for the account. Click the 'Variables' button  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  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.

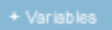

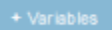



- Click the 'Save' button.

The saved 'Exchange' 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 Global HTTP proxy settings

- Click 'Global Proxy HTTP' from the 'Add Section' drop-down

The 'Global Proxy HTTP' settings screen will be displayed.

Global HTTP Proxy Settings - Table of Parameters		
Form Element	Type	Description
Name	Text Field	Enter the name of the that will be displayed to the users for the policy. YYou can also add variables by clicking the 'Variables' button  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: <ul style="list-style-type: none"> • 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  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  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 saved 'Global Proxy HTTP' 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 LDAP settings

- Click 'LDAP' from the 'Add Section' drop-down

The 'LDAP' settings screen will be displayed.

iOS Profile for Purchase Department

Ldap Cancel Save

Account Description
 + Variables
 The display name of the account (e.g. "Company LDAP Account")

Account Hostname *
 + Variables
 The LDAP hostname or IP address

Account Username
 + Variables
 The username for this LDAP account

Account Password
 + Variables
 The password for this LDAP account

Use SSL
 Enable Secure Socket Layer for this connection.

Search Settings

Description



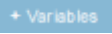



Scope
 ▼

Search Base

Add

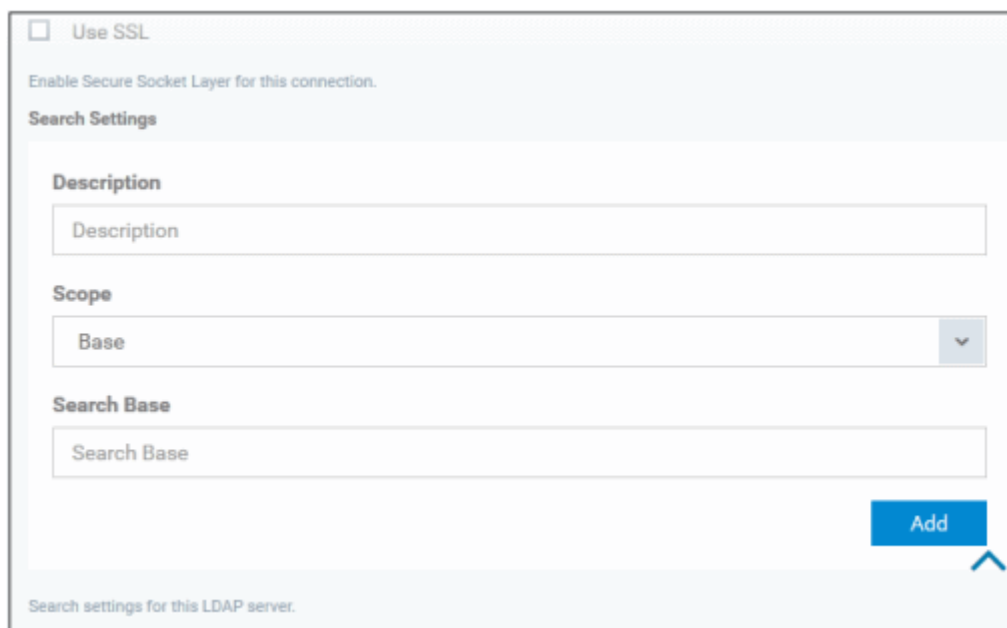
LDAP Settings - Table of Parameters

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

LDAP Settings - Table of Parameters		
		Custom Variables.
Account Hostname	Text Field	Enter the LDAP hostname or IP address. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Account Username	Text Field	The username for the LDAP account. You can also add variables by clicking the 'Variables' button  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  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.



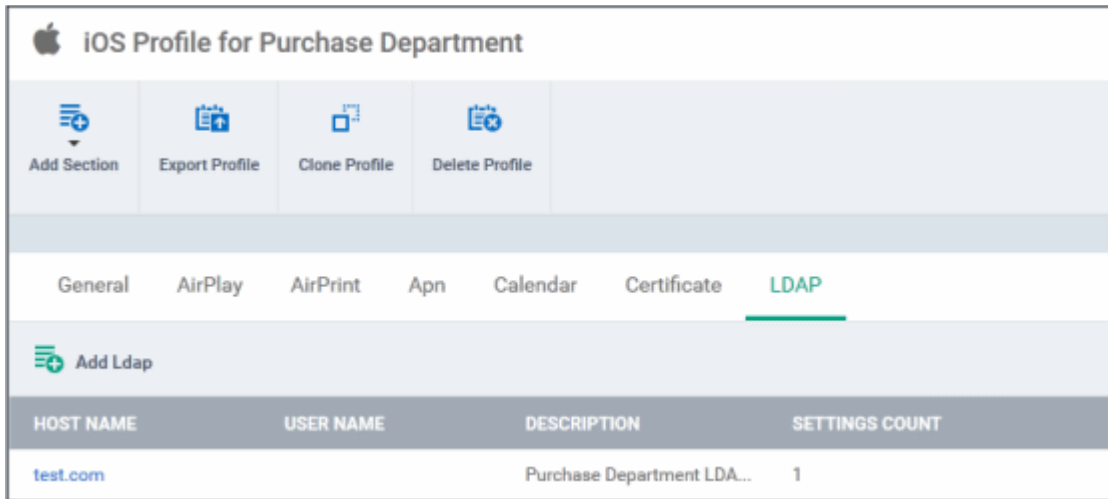
The screenshot shows a web interface for LDAP settings. At the top, there is a checkbox for 'Use SSL' with the text 'Enable Secure Socket Layer for this connection.' Below this is the 'Search Settings' section. It contains three input fields: 'Description' (a text field), 'Scope' (a drop-down menu currently showing 'Base'), and 'Search Base' (a text field). A blue 'Add' button is located at the bottom right of the form. At the very bottom, there is a small note: '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. <ul style="list-style-type: none"> • 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.

LDAP Search Settings - Table of Parameters		
Search base	Text Field	Enter the search base for which the search will be restricted. For example, you might want to allow users to search only for other email users via LDAP.

- You can add more 'Search Settings' by clicking the  button below.
- To remove a search item, click the  button.
- Click the 'Save' button.

The saved 'LDAP' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple LDAP sections for a profile and will be listed under the LDAP link in the profile.





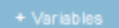





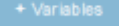

- To add another LDAP section, click 'Add Ldap' above the 'Host Name' column
- Click on a link under 'Host Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Mail settings

- Click 'Mail' from the 'Add Section' drop-down

The 'Mail' settings screen will be displayed.

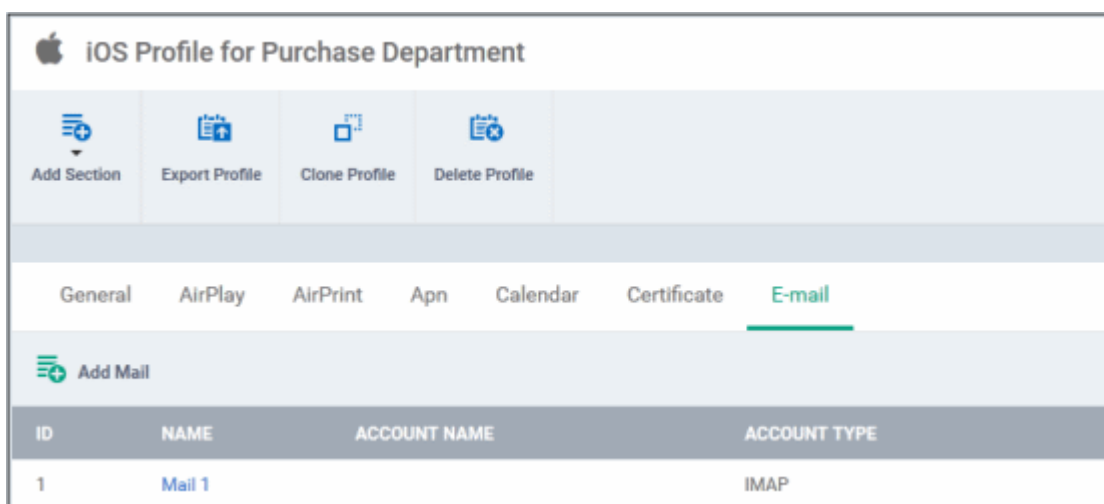
Mail Account Settings - Table of Parameters		
Form Element	Type	Description
Email Account Description	Text Field	Enter a description for the email account. You can also add variables by clicking the 'Variables' button and clicking beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Allowed values for Email Type	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 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	Click the 'Variables' button 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	Click the 'Variables' button 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 .
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)	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 and clicking

Mail Account Settings - Table of Parameters		
address)		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  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	Click the 'Variables' button  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 .
The Authentication Method for the Incoming Mail Server	Drop-down	Select the type of authentication method for the mail account from the drop-down. The options available are: <ul style="list-style-type: none"> • 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  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
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  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	Click the 'Variables' button  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: <ul style="list-style-type: none"> • None • Password • CRAM MD5 • NTLM • HTTP MD5

Mail Account Settings - Table of Parameters		
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 will be used for outgoing also.
Disable Mail Recents Syncing	Checkbox	If enabled, recently used emailed addresses are not synced with other devices via iCloud.
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 saved 'Mail' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Mail sections for a profile and will be listed under the E-mail link in the profile.



- To add another Mail section, click 'Add Mail' above the 'ID' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Passcode settings

- Click 'Passcode' from the 'Add Section' drop-down

The 'Passcode Settings' screen will be displayed.

Apple iOS Profile for Purchase Department

[Add Section](#) [Export Profile](#) [Clone Profile](#) [Delete Profile](#)

[General](#) [AirPlay](#) [AirPrint](#) [Apn](#) [Calendar](#) [Certificate](#) [Passcode](#)

Passcode Settings

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
+ Variables

Days (1-730) after which passcode must be changed.

Maximum idle time
Default

Device automatically locks when minutes elapse.

Passcode history
+ Variables





The number (1-50) of unique passcodes required before reuse.

Maximum grace period for device lock
Default

Maximum amount of time device can be locked without prompting for passcode on unlock.

Maximum number of failed attempts
Default

Number of passcode entry attempts allowed before all data on device will be erased.

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  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  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.

- Click the 'Save' button.

The saved 'Passcode 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 Proxy settings

- Click 'Proxy' from the 'Add Section' drop-down

The 'Proxy' settings screen will be displayed.

iOS Profile for Purchase Department

Proxy [Cancel] [Save]

Name *
[Text Field] [+ Variables]

Proxy type *
Manual [Dropdown Arrow]

Proxy server
[Text Field] [+ Variables]
Fully qualified address and port of the proxy server.

Proxy server port
[Text Field] [+ Variables]

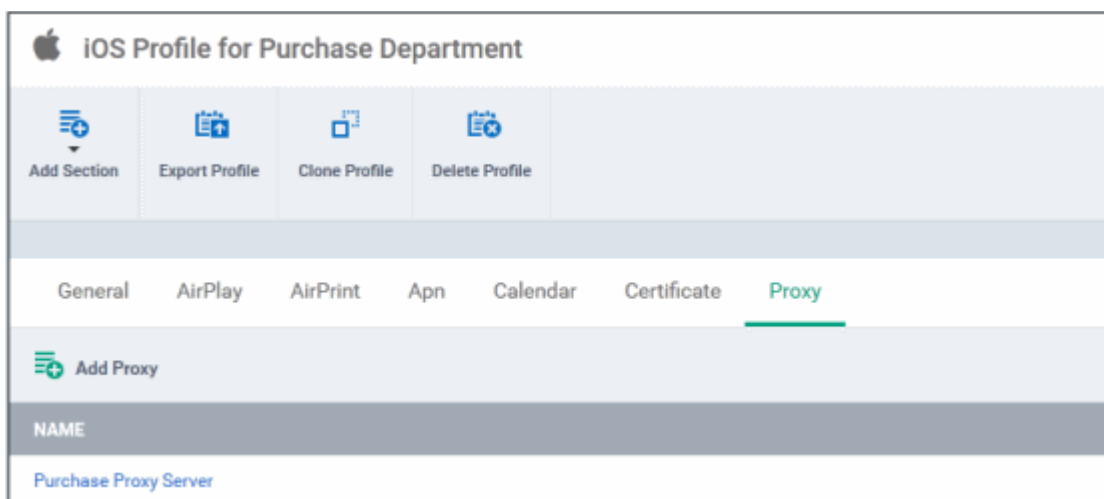
Proxy username
[Text Field] [+ Variables]
Username used to connect to the proxy server.

Proxy password
[Text Field] [+ Variables]
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	<p>Select the proxy type from the drop-down. The options available are:</p> <ul style="list-style-type: none"> • None • Manual • Auto <p>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.</p> <p>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.</p>

- Click the 'Save' button.

The saved 'Proxy' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Proxy sections for a profile and will be listed under the Proxy link in the profile.

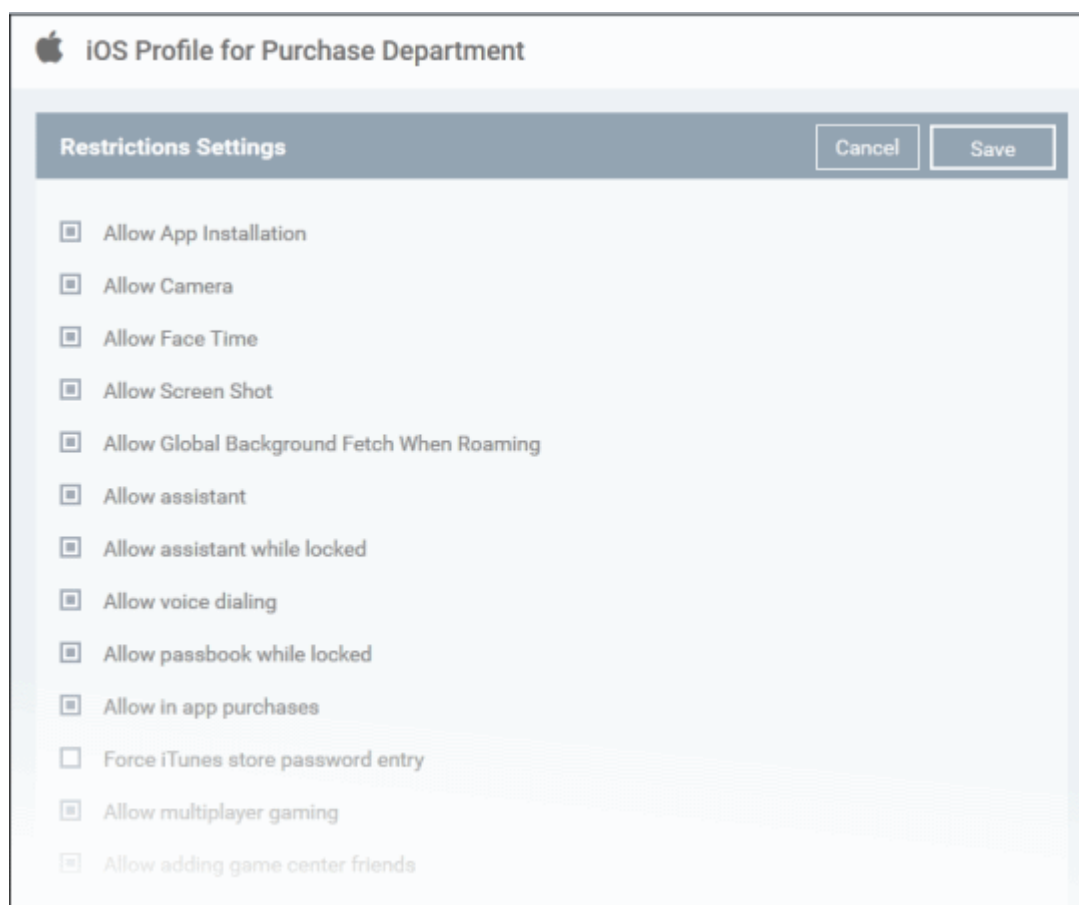


- To add another Proxy section, click 'Add Proxy' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Restrictions settings





- Click 'Restrictions' from the 'Add Section' drop-down

The 'Restrictions Settings' screen will be displayed.



Restrictions Settings - Table of Parameters		
Device Functionality		
Form Element	Type	Description
Allow App Installation	Checkbox	Select this to allow the user to access App Store, iTunes and install or update apps. If left unchecked, the App Store icon is removed from the device's home screen and the user cannot access it.
Allow Camera	Checkbox	Select this to allow 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	Select this to allow the user to use FaceTime. Please note the 'Allow Camera' feature should be 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 when roaming to sync even when an account is not accessed by a user.
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 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
Force iTunes store password entry	Checkbox	If enabled, users have to enter their Apple ID password for making any purchase.
Allow multiplayer gaming	Checkbox	Select this to allow the user to play multiplayer game in Game Center.
Allow adding game center friends	Checkbox	If enabled, users can add friends in Game Center.
Allow You Tube	Checkbox	If enabled, users can access You Tube. If left unchecked, You Tube app is disabled and its icon removed from the home screen.
Allow i Tunes	Checkbox	If enabled, users can access iTune store. If left unchecked, iTune store is disabled and its icon removed from the home screen.
Allow Safari	Checkbox	Select this to allow the user to browse the Internet using Safari. If left unchecked, the Safari browser app is disabled and its icon removed from the home screen.
Safari allow auto fill	Checkbox	If enabled, users can use the feature to automatically fill details in a web form such as user name, password, credit card details and so on.
Safari allow java script	Checkbox	If enabled, java script features will be supported in Safari.
Safari allow popups	Checkbox	If enabled, popups will be allowed.
Safari force fraud warning	Checkbox	If enabled, Safari alerts users when visiting websites that are identified as compromised or fraudulent.
Safari accept cookies	Drop-down	Select from the drop-down when to accept all cookies. The options available are:

Restrictions Settings - Table of Parameters		
		<ul style="list-style-type: none"> • Always • Never • From visited site
Allow cloud backup	Checkbox	If enabled, users can backup their device data to iCloud.
Allow cloud document sync	Checkbox	If enabled, users can synchronize documents between iCloud and their device.
Allow photo stream	Checkbox	Users can use Photo Stream if this checkbox is enabled. If a profile with this restriction is applied to a device, Photo Stream photos will be removed from the device and no photos from Camera Roll will be uploaded to Photo Stream.
Allow shared stream	Checkbox	If enabled, users can share and view photos in Photo Stream.
Allow diagnostic submission	Checkbox	If enabled, iOS diagnostic information will be sent to Apple.
Allow untrusted TLS prompt	Checkbox	If enabled, users will be prompted if they want to trust unverified certificates. This settings applies to Calendar accounts, Contacts, Safari and to Mail.
Force encrypted backup	Checkbox	If left unchecked, in iTunes users have the option to encrypt or not encrypt backups from the device to a local computer. If this checkbox is enabled, in iTunes users are forced to encrypt the backup.
Allow explicit content	Checkbox	If enabled, explicit content include music and video will be displayed in iTunes store instead being hidden. Content providers flag explicit content for easy identification.
Allow iBookstore	Checkbox	If enabled, users can access iBookstore, an online bookstore from Apple. Note: This option is available for supervised devices only.
Allow iBookstore erotica		If enabled, users can access explicit or adult content materials from iBookstore. Note: This option is available for supervised devices only.
Allow account modification	Checkbox	Select this to allow account modification on devices. Note: This feature is available for iOS 7 and later versions 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 later versions and supervised devices only.
Allow app cellular data modification	Checkbox	If enabled, users can make changes to cellular data usage for apps on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Allow assistant user generated content	Checkbox	Select this to enable Siri to query user generated content from the Internet on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Allow cloud keychain sync	Checkbox	If enabled, users can sync Apple Keychain on iCloud on devices. Note: This feature is available for iOS 7 and later versions.
Allow find my friends modification	Checkbox	Select this to enable Find My Friends on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Allow fingerprint for unlock	Checkbox	Select this to enable Touch ID to unlock devices.

Restrictions Settings - Table of Parameters		
		Note: This feature is available for iOS 7 and later versions.
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 later versions 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 in 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 in Notification Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and 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.
Allow OTAPKI updates	Checkbox	Select this option to allow over-the-air public key infrastructure (OTAPKI) updates on devices. 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 profile. 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.
Autonomous single app mode permitted app IDs	Text Field	<p>Enter the app identifier in the field. The user will able to see only the app entered in this field. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <ul style="list-style-type: none"> To add Autonomous single app mode permitted app IDs, click . To remove the field, click the  beside it. <p>Note: This feature is available for iOS 7 and later versions and supervised devices only.</p>
Rating region	Drop-down	Select the region whose ratings are to be followed, from the drop-down.
Rating movies	Drop-down	Choose the rating to allow watching the movies with the chosen rating.
Rating TV Shows	Drop-down	Choose the rating to allow watching the TV shows with the chosen rating.
Rating apps	Drop-down	Choose the rating to allow using apps with the chosen rating.

- 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

This settings is used to configure Kerberos authentication process and is available in iOS 7 or later versions only.

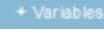

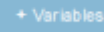



- Click 'Single Sign-On' from the 'Add Section' drop-down









The 'Single Sign On' settings screen will be displayed.

The screenshot shows the 'Single Sign On' configuration interface for an iOS profile. It includes the following elements:

- Title:** 'Single Sign On' with 'Cancel' and 'Save' buttons.
- Name:** A text field with a '+ Variables' button and an 'iOS 7+' version indicator.
- Principal Name:** A text field with a '+ Variables' button and an 'iOS 7+' version indicator.
- Realm:** A text field with a '+ Variables' button and an 'iOS 7+' version indicator.
- Url Prefix Matches:** A text field with a '+ Variables' button, a plus sign (+) for adding more matches, and an 'iOS 7+' version indicator.
- App Identifier Matches:** A text field with a '+ Variables' button, a plus sign (+) for adding more matches, and an 'iOS 7+' version indicator.

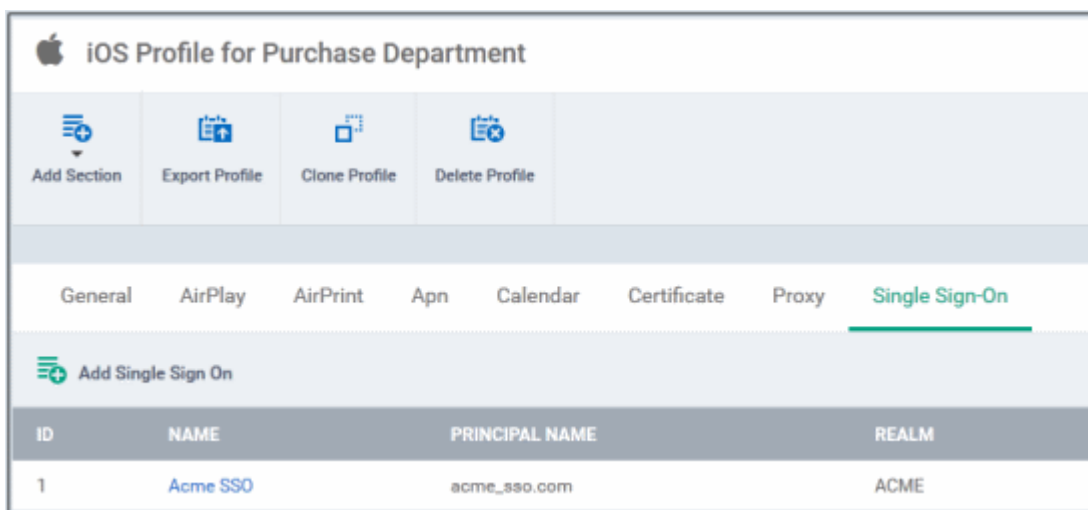
Single Sign-On Settings - Table of Parameters

Form Element	Type	Description
Name	Text Field	Enter the name for the account. You can also add variables by clicking the 'Variables' button  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  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 in proper capitals. You can also add variables by clicking the 'Variables' button  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

Single Sign-On Settings - Table of Parameters		
		<p>'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Click  button to add more 'URL prefix matches' fields. To remove a URL prefix, click the minus  button beside it.</p>
App identifier matches	Text Field	<p>Enter the bundle ID of apps that are allowed to use for this login. If this field is left blank, this login matches all app IDs. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Click  button to add more 'App identifier matches' fields. To remove an App identifier match, click the minus  button beside it.</p>

- Click the 'Save' button.

The saved 'Single Sign-On' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Single Sign-On sections for a profile and will be listed under the Single Sign-On link in the profile.



- To add another SSO section, click 'Add Single Sign-On' above the 'ID' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section **Editing Configuration Profiles** for more details.

To configure Subscribed Calendar settings

- Click 'Subscribed Calendars' from the 'Add Section' drop-down

The 'Subscribed Calendar' settings screen will be displayed.

Subscribed Calendar [Cancel] [Save]





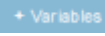

Description
[Text Field] [+ Variables]
The description of the calendar subscription.

URL *
[Text Field] [+ Variables]
The URL of the calendar file.

Username
[Text Field] [+ Variables]
The username for this subscription.

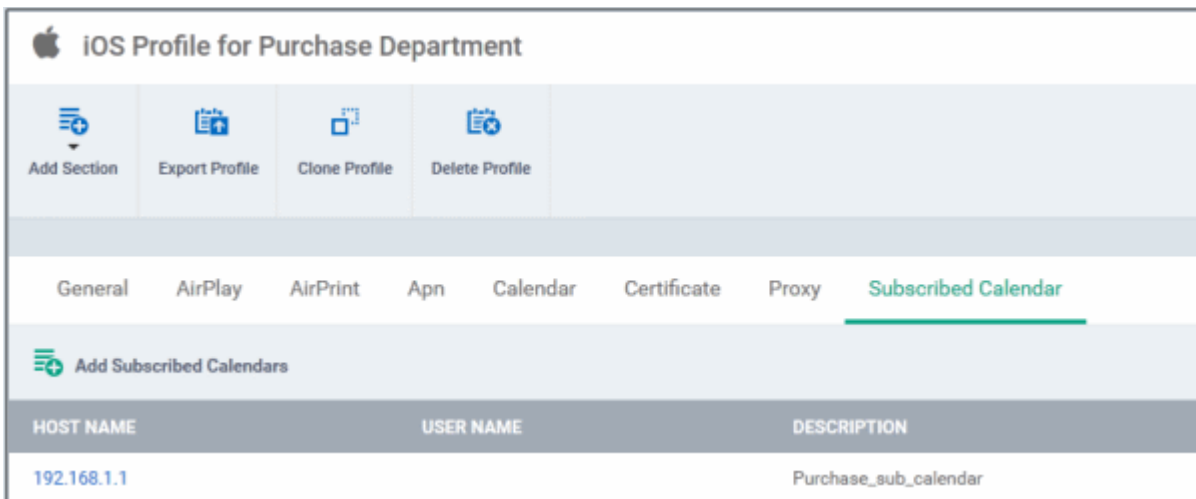
Password
[Text Field] [+ Variables]
The password for this subscription.

Use SSL
Enable Secure Socket Layer for this connection.

Subscribed Calendars Settings - Table of Parameters		
Form Element	Type	Description
Description	Text Field	Enter the description of the calendar subscription. You can also add variables by clicking the 'Variables' button  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 subscribed calendar file. You can also add variables by clicking the 'Variables' button  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. Click the 'Variables' button  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 server.

- Click the 'Save' button.

The saved 'Subscribed Calendar' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Subscribed Calendar sections for a profile and will be listed under the Subscribed Calendar link in the profile.

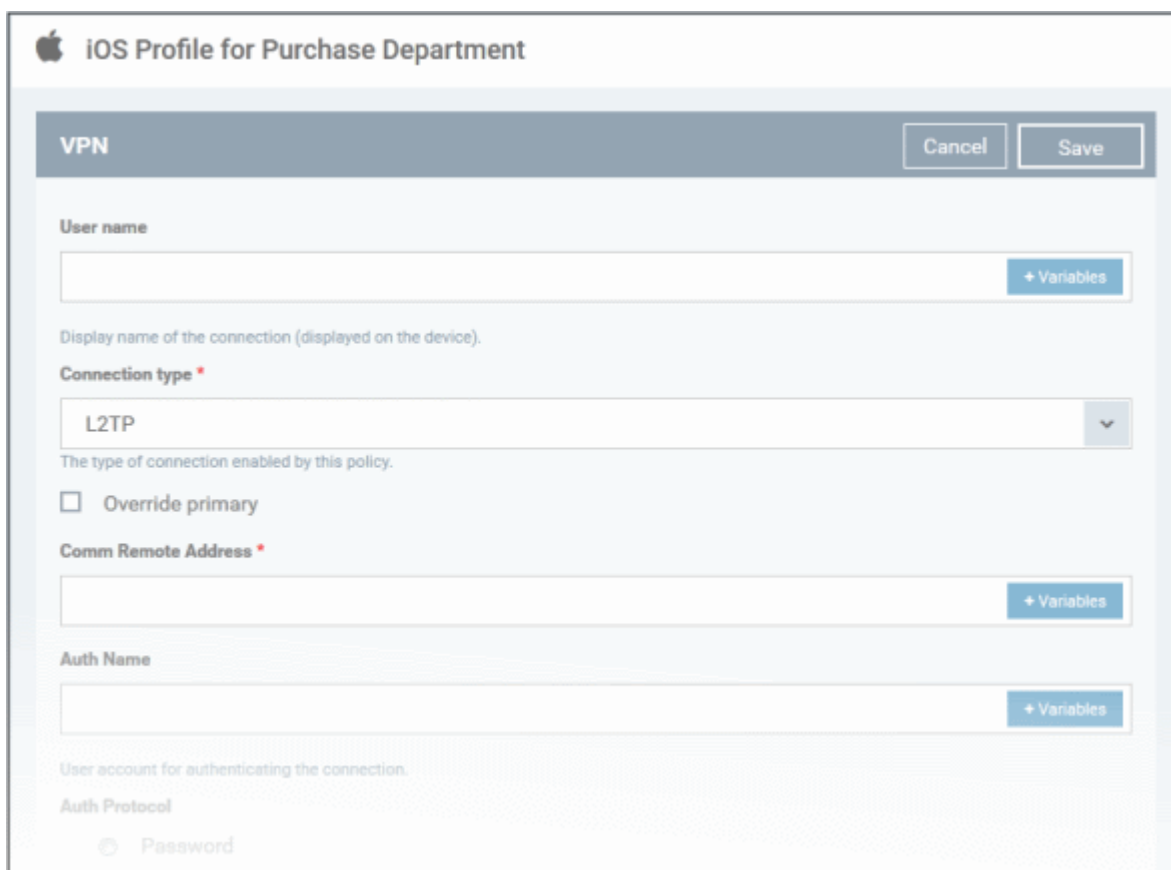


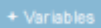

- To add another Subscribed Calendar section, click 'Add Subscribed Calendar' above the 'Host Name' column
- Click on a link under 'Host Name' to edit the setting or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

To configure VPN settings

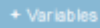

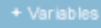







- Click 'VPN' from the 'Add Section' drop-down

The settings screen for VPN will be displayed.





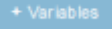

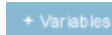









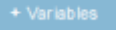

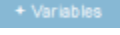


VPN Settings - Table of Parameters		
Form Element	Type	Description
User name	Text Field	Enter the name of the connection, which will be displayed on the device. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables .
Connection type	Drop-down	Choose the VPN connection type from drop-down. The options available are: L2TP, PPTP, IPSec, Cisco Any Connection, Juniper SSL, F5 SSL and Open VPN. The settings for each type is explained in the next table, VPN connection type settings .
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: <ul style="list-style-type: none"> None Manual Auto <p>If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields.</p> <p>If you select 'Auto', enter the URL of the Proxy Pac.</p>


VPN Connection Type settings

VPN Connection Type Settings - Table of Parameters	
Connection Type	Description
L2TP	<ul style="list-style-type: none"> Override Primary - Enable this to 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  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  and clicking  beside the variable you want to add. Auth Protocol - Select the authentication method whether 'Password' or 'RSA SecurID' Auth Password - This is enabled only if 'Password' is selected in 'Auth Protocol'. The user must enter the password or include a variable by clicking the 'Variables' button  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  and clicking  beside the variable you want to add. Shared secret - Applicable only if RSA SecurID is being used. The user must enter the shared secret or add a variable by clicking the 'Variables' button  and clicking  beside the variable.

VPN Connection Type Settings - Table of Parameters	
	<p>For more details on variables, refer to the section Configuring Custom Variables.</p>
PPTP	<ul style="list-style-type: none"> • Override Primary - Enable this to 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 whether 'Password' or 'RSA SecurID' • Auth Password - This is enabled only if 'Password' is selected in 'Auth Protocol'. The user must enter the password or add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable. • 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. • Encryption Level - Select the encryption level from the drop-down. The options available are, None, Automatic and Maximum (128 bit). • Shared secret - Applicable only if RSA SecurID is being used. The user must enter the shared secret or add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable. <p>For more details on variables, refer to the section Configuring Custom Variables.</p>
IP SEC	<ul style="list-style-type: none"> • Override Primary - Enable this to override the primary server. • Server - 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. • Account - Enter the VPN account name. You can also add variables by clicking the 'Variables' button + Variables and clicking + beside the variable you want to add. • Password - The user should enter the password for the account or add a variable by clicking the 'Variables' button + Variables and clicking + beside the variable. • Authentication Method - Select the authentication method from the drop-down either Shared secret / Group name or Certificate. <ul style="list-style-type: none"> • Shared secret / Group name - If this is selected, then the user should enter the shared secret and group name in the 'Shared secret' and 'Local identifier' fields. If 'Hybrid authentication' is selected, then the authentication should end with the hybrid in the 'Local identifier' field. • Certificate - If this is selected, the following options are available: <ul style="list-style-type: none"> • Password encryption - The password will be encrypted • Prompt for VPN PIN - If selected, the user will be prompted to enter the VPN Pin while connecting. • On demand enabled - If selected, the VPN connection is determined depending on the domains added in the Domain field and type selected.

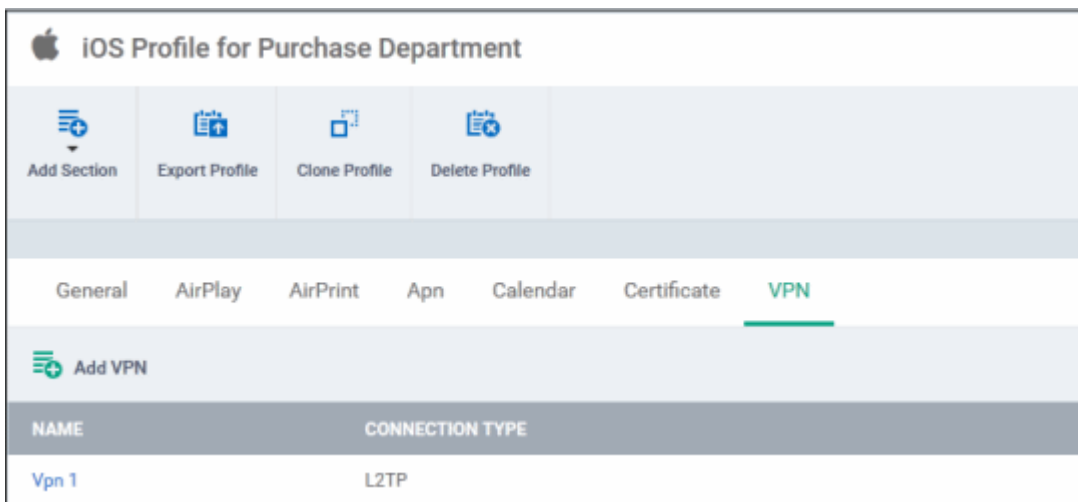
VPN Connection Type Settings - Table of Parameters	
	<ul style="list-style-type: none"> Choose Certificate - Select the certificate from the drop-down or upload it using the 'Add New' button. Domain - This is enabled only if 'On demand enabled' is selected. Enter the domain names which when the users visit will initiate a VPN connection depending on the type selected. Type - Determines whether the VPN connection should be established or not. <ul style="list-style-type: none"> Always establish - Initiates a VPN connection for the specified domains. Never establish - The specified domains should never trigger a VPN connection attempt. Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails. Click the  button to include more domain sections. To remove a domain section, click the  button beside it. <p>For more details on variables, refer to the section Configuring Custom Variables.</p>
Cisco AnyConnection, F5 SSL and Open VPN	<ul style="list-style-type: none"> Override Primary - Enable this to override the primary server. Certificate - Select the required certificate from the drop-down or click the 'Add New' button to upload the certificate. Remote Address - Enter IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button  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  and clicking  beside the variable you want to add. Auth Password - The password for the VPN connection. The user must enter the password or add a variable by clicking the 'Variables' button  and clicking  beside the variable. Authentication Method - Select the authentication method from the drop-down either Shared secret / Group name or Certificate. Shared secret / Group name - If this is selected, then the user should enter the shared secret in the 'Group' field. Certificate - If this is selected, the following options are available: <ul style="list-style-type: none"> Group - Enter the shared secret ID Certificate - Select the authentication certificate or click the 'Add New' button and upload the certificate. On demand enabled - If selected, the VPN connection is determined depending on the domains added in the Domain field and type selected. Domain - This is enabled only if 'On demand enabled' is selected. Enter the domain names which when the users visit will initiate a VPN connection depending on the type selected. Type - Determines whether the VPN connection should be established or not. <ul style="list-style-type: none"> Always establish - Initiates a VPN connection for the specified domains. Never establish - The specified domains should never trigger a VPN connection

VPN Connection Type Settings - Table of Parameters	
	<p>attempt.</p> <ul style="list-style-type: none"> Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails. Click the  button to include more domain sections. To remove a domain section, click the  button beside it. <p>For more details on variables, refer to the section Configuring Custom Variables.</p>
Juniper SSL	<ul style="list-style-type: none"> Override Primary - Enable this to override the primary server. Certificate - Select the required certificate from the drop-down or click the 'Add New' button to upload the certificate. Remote Address - Enter IP address or host name of the VPN server. You can also add variables by clicking the 'Variables' button  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  and clicking  beside the variable you want to add. Realm - Enter the name of the authentication server. You can also add variables by clicking the 'Variables' button  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  and clicking  beside the variable you want to add. Authentication Method - Select the authentication method from the drop-down either Shared secret / Group name or Certificate. <ul style="list-style-type: none"> Shared secret / Group name - If this is selected, then the user should enter the shared secret in the 'Group' field. Certificate - If this is selected, the following options are available: <ul style="list-style-type: none"> Group - Enter the shared secret ID Certificate - Select the authentication certificate or click the 'Add New' button and upload the certificate. On demand enabled - If selected, the VPN connection is determined depending on the domains added in the Domain field and type selected. Domain - This is enabled only if 'On demand enabled' is selected. Enter the domain names which when the users visit will initiate a VPN connection depending on the type selected. Type - Determines whether the VPN connection should be established or not. <ul style="list-style-type: none"> Always establish - Initiates a VPN connection for the specified domains. Never establish - The specified domains should never trigger a VPN connection attempt. Establish if needed - The specified domains should trigger a VPN connection attempt if domain name resolution fails. Click the  button to include more domain

VPN Connection Type Settings - Table of Parameters	
	<p>sections. To remove a domain section, click the  button beside it.</p> <p>For more details on variables, refer to the section Configuring Custom Variables.</p>

- Click the 'Save' button.

The saved 'VPN' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple VPN sections for a profile and will be listed under the name link in the profile.







- To add another VPN section, click 'Add VPN' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Per-App VPN settings

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 Section' drop-down

The settings screen for VPN will be displayed.

- **On Demand Match App Enabled** - Select this checkbox to enable per-app VPN connection.
- **Safari domains** - Enter the domain that will trigger this VPN connection in Safari. You can also add variables by clicking the 'Variables' button  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 saved 'VPN Per App' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple VPN Per App sections for a profile and will be listed under the name link in the profile.

NAME	CONNECTION TYPE
Vpn 1	L2TP

- To add another VPN Per App section, click 'Add VPN Per App' above the 'Name' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Web Clip settings





- Click 'Web Clip' from the 'Add Section' drop-down

The 'Web Clip Settings' screen will be displayed.

The screenshot shows the 'Web Clip Settings' configuration screen for an 'iOS Profile for Purchase Department'. At the top, there are 'Cancel' and 'Save' buttons. The settings are organized into sections:

- Label:** A text input field with a '+ Variables' button. Below it, a note states: 'The name to display for the Web Clip.'
- Url:** A text input field with a '+ Variables' button. Below it, a note states: 'The URL to be displayed when selecting the Web Clip.'
- Is Removable:** A checkbox. Below it, a note states: 'Enable removal of the Web Clip.'
- Pre Composed:** A checkbox. Below it, a note states: 'The icon will be displayed with no added visual effects.'
- Full Screen:** A checkbox. Below it, a note states: 'Controls whether the web clip launches as a Full Screen application.'
- Icon:** A 'Browse' button. Below it, a note states: 'The icon used for the web clip.'

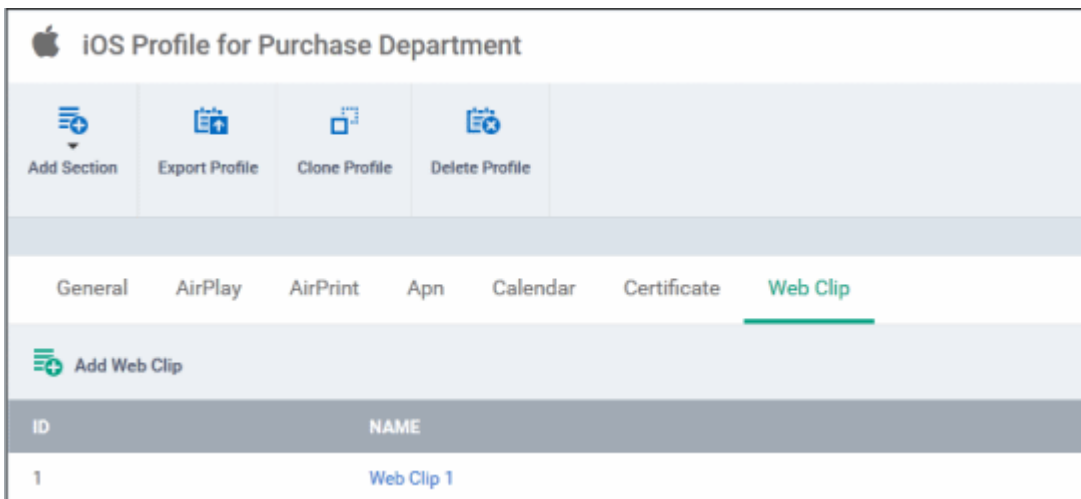
Web Clip Settings - Table of Parameters

Form Element	Type	Description
Label	Text Field	Enter the display name of the Web Clip. You can also add variables by clicking the 'Variables' button  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 also add variables by clicking the 'Variables' button  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.

Web Clip Settings - Table of Parameters		
Full Screen	Checkbox	If enabled, the Web Clip will be displayed as a full screen application.
Icon	Button	Upload the image to be used as icon for the Web Clip.

- Click the 'Save' button.

The saved 'Web Clip' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Web Clip sections for a profile and will be listed under the Web Clip link in the profile.



- To add another Web Clip section, click 'Add Web Clip' above the 'ID' column
- Click on a link under 'Name' to edit the setting or delete the section. Refer to the section '[Editing Configuration Profiles](#)' for more details.

To configure Wi-Fi settings

- Click 'Wi-Fi' from the 'Add Section' drop-down

The 'Wi-Fi' settings screen will be displayed.

iOS Profile for Purchase

Department

Wi-Fi
Cancel Save

SSID *

+ Variables

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
▼
Add New

Is hotspot

Service provider roaming enabled

Domain name iOS 7+

+ Variables

Displayed operator name iOS 7+

+ Variables





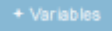

Roaming consortium ois iOS 7+



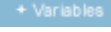



+Variables
+

NAI realm names iOS 7+

+Variables
↑

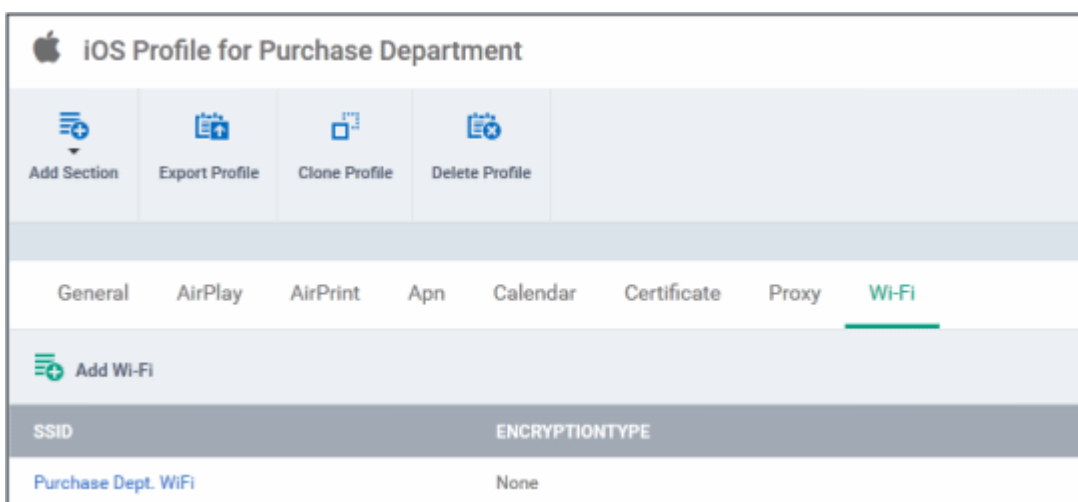
Wi-Fi Settings - Table of Parameters		
Form Element	Type	Description
SSID	Text Field	Enter a unique identifier (Service Set Identifier) of a wireless network that a device should connect to. Note: In iOS 7 and later versions, this is optional if Domain Name value is provided.
Auto Join	Checkbox	If enabled, devices will automatically connect to the configured wireless network.

Hidden Network	Checkbox	Specify whether the wireless network is hidden or not.
Encryption Type	Drop-down	<p>Select the type of encryption used by the wireless network from the drop-down. The options available are:</p> <ul style="list-style-type: none"> • None • WEP • WPA / WPA2 • Any • WEP Enterprise • WPA / WPA2 Enterprise • Any (Enterprise) <p>The Password field will appear if any of the options, WEP, WPA / WPA2 and Any (Personal) are chosen.</p> <p>If any of the Enterprise is chosen, then select the supported protocols and configure authentication. The options available are: TLS, LEAP, TTLS, PEAP, EAP-FAST, EAP-SIM, Use Pac and Provision Pac Anonymously.</p>
Password	Text Field	Leave the field blank. The user will be prompted to enter the password while accessing the Wi-Fi network.
Proxy	Drop-down	<p>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:</p> <ul style="list-style-type: none"> • None • Manual • Auto <p>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.</p> <p>If you select 'Auto', enter the URL of the Proxy Pac and click the 'Create' button.</p>
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	<p>Enter the domain name used for Wi-Fi hotspot 2.0 which the devices will connect to. This is optional and can be provided instead of Service Set Identifier. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
Displayed Operator Name	Text Field	<p>Enter the network operator name that will be displayed in the devices. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
Roaming Consortium OIs	Text Field	<p>Enter the Roaming Consortium Organization Identifier of the service provider to which the devices will connect to. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom</p>

		<p>Variables.</p> <p>To removed the field, click the  button beside it.</p> <p>Click the  button to add Roaming Consortium Ols fields.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
NAI Realm Names	Text Field	<p>Enter the Network Access Identifier (NAI) realm names used for Wi-Fi hotspot 2.0. You can also add variables by clicking the 'Variables' button  and clicking  beside the variable you want to add. For more details on variables, refer to the section Configuring Custom Variables.</p> <p>To remove the field, click the  beside it.</p> <p>Click the  button to add more NAI Realm Names.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>

- Click the 'Save' button.

The saved 'Wi-Fi' settings screen will be displayed with options to edit the settings or delete the section. You can add multiple Wi-Fi sections for a profile and will be listed under the Wi-Fi link in the profile.



- To add another Wi-Fi section, click 'Add Wi-Fi' above the 'SSID' column
- Click on a link under 'SSID' to edit the setting or delete the section. Refer to the section '**Editing Configuration Profiles**' for more details.

6.1.3. Profiles for Windows Devices

Windows profiles allow you to specify security settings for CES installed at the managed Windows devices.

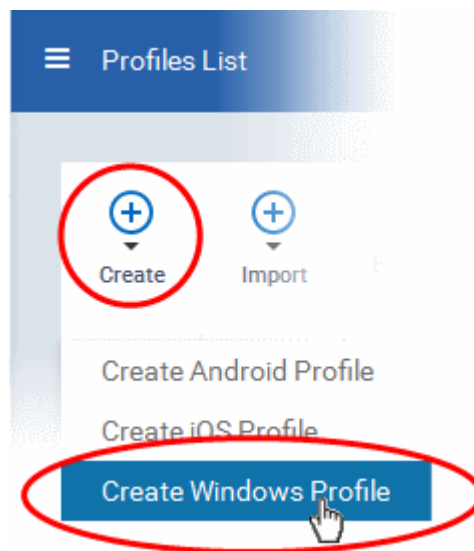
Security profiles to be applied to Windows endpoints can be added to CDM in two ways:

- Creating the profile by defining the parameters and settings for security components from the CDM interface. Refer to **Creating Windows Profiles** for more details.
- Importing a CES profile from a remotely managed PC or from from a stored configuration profile (.cfg file) into CDM. Refer to the section **Importing Windows Profiles** for more details.

6.1.3.1. Creating Windows Profile

To create a new Windows profile

- Click 'Profiles' from the left then choose 'Profiles List'
- Click 'Create' then select 'Create Windows Profile'
- Specify a name and description for your profile then click the 'Create' button. This profile will now appear in the 'Profile List'.
- New profiles have only one tab - 'General'. You can configure permissions and settings for various areas by clicking the 'Add Section' button. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices and device groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.
- This part of the guide explains the processes above in more detail, and includes in-depth descriptions of the settings available for each profile section.
- To create a new profile, click 'Profiles > Profile List > Create':



The 'Create Windows Profile' screen will be displayed.

Create Windows Profile Close

Name *


Description

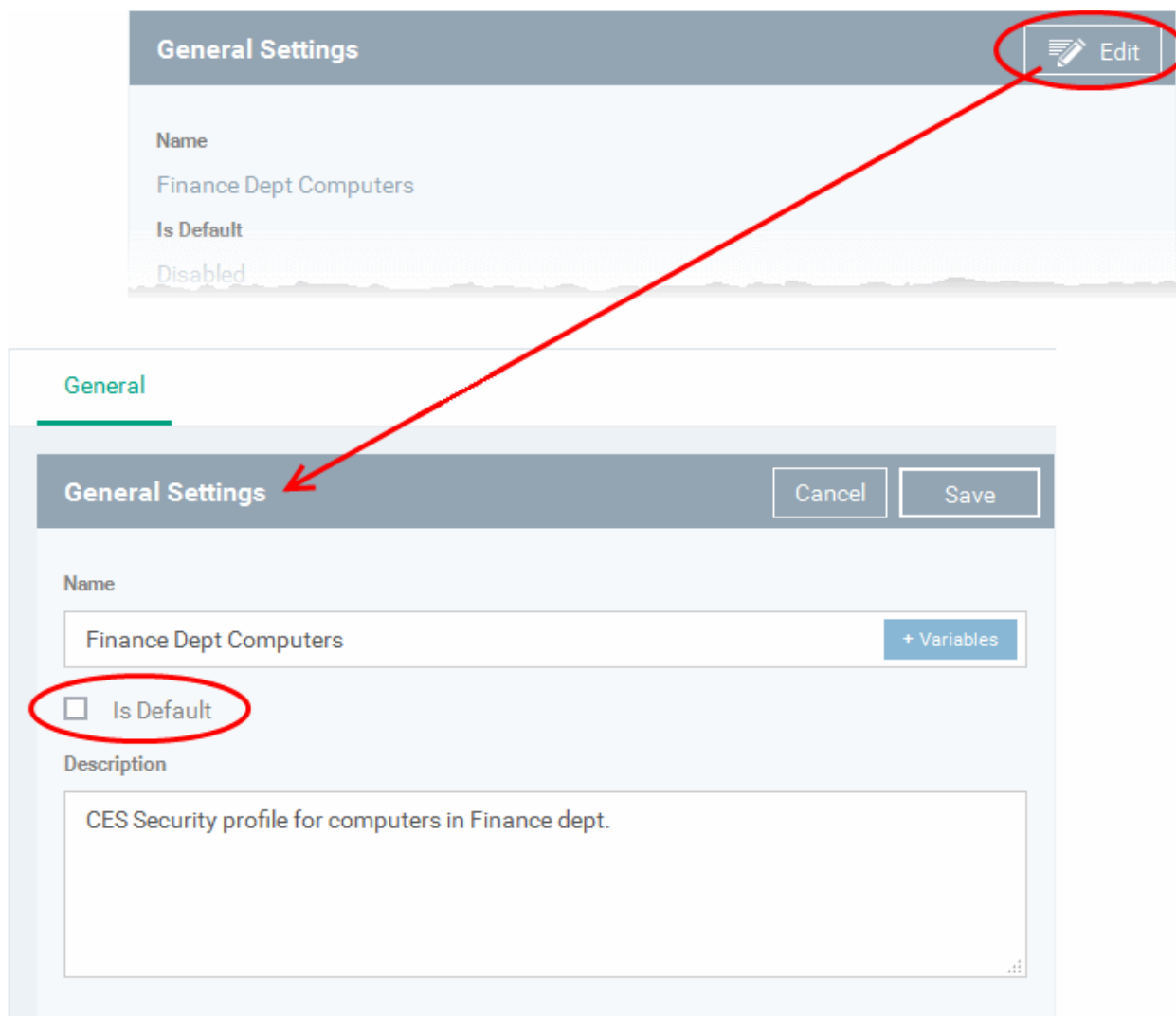
[Create](#)

- 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 with its default profile status as disabled.

The screenshot displays the 'Finance Dept Computers' profile settings in the Comodo Device Manager. The interface includes a top navigation bar with a menu icon, the breadcrumb 'Profiles List / Finance Dept Computers', a notification bell, and a user profile 'Logout (John Smith)'. Below the navigation bar, the profile name 'Finance Dept Computers' is shown with a Windows logo icon. A toolbar contains four actions: 'Add Section' (plus icon), 'Export Profile' (upload icon), 'Clone Profile' (copy icon), and 'Delete Profile' (trash icon). The 'General' section is active, showing a 'General Settings' panel with an 'Edit' button (pencil icon). The settings listed are: Name: Finance Dept Computers; Is Default: Disabled; Description: CES Security profile for computers in Finance dept.

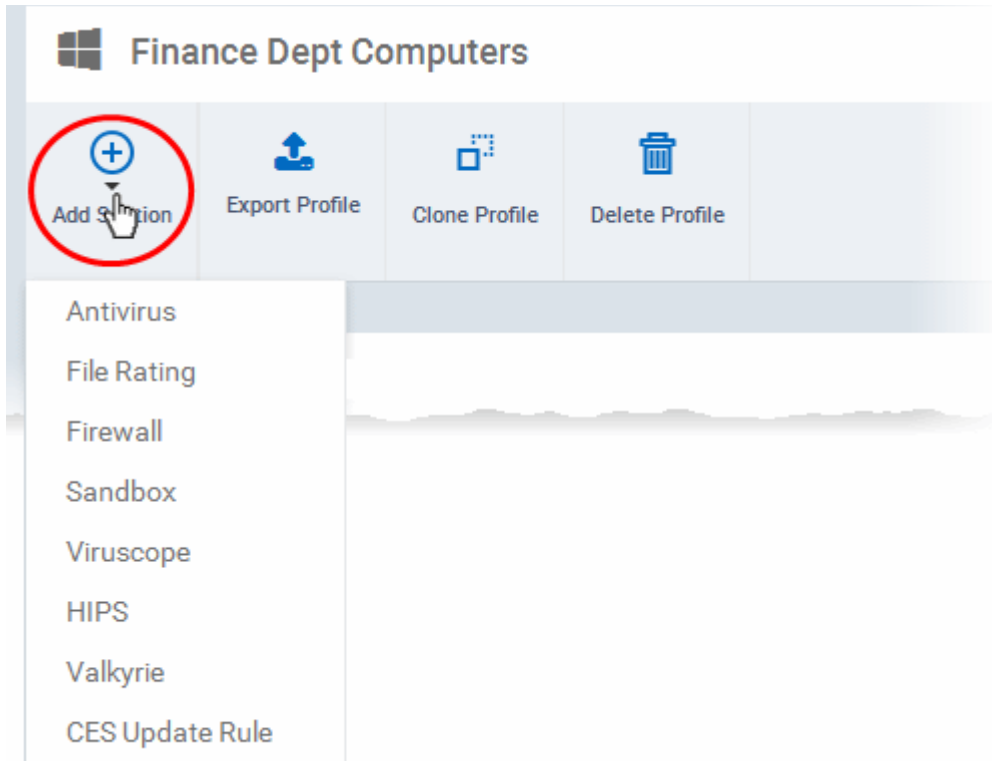
- If you want this profile to be a default profile, click on the 'Edit' button  at the top right of the 'General' settings screen and select the 'Is Default' option.



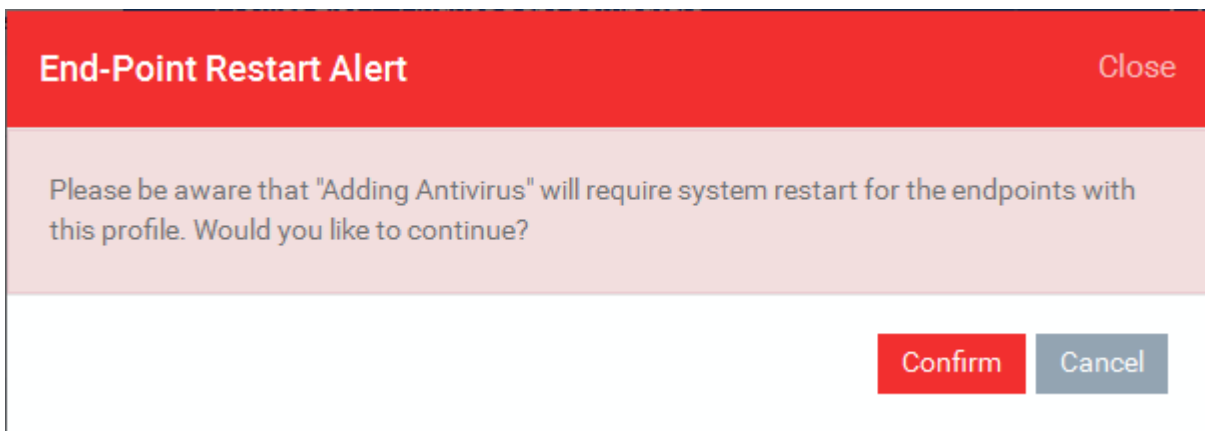
- Click the 'Save' button.

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

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

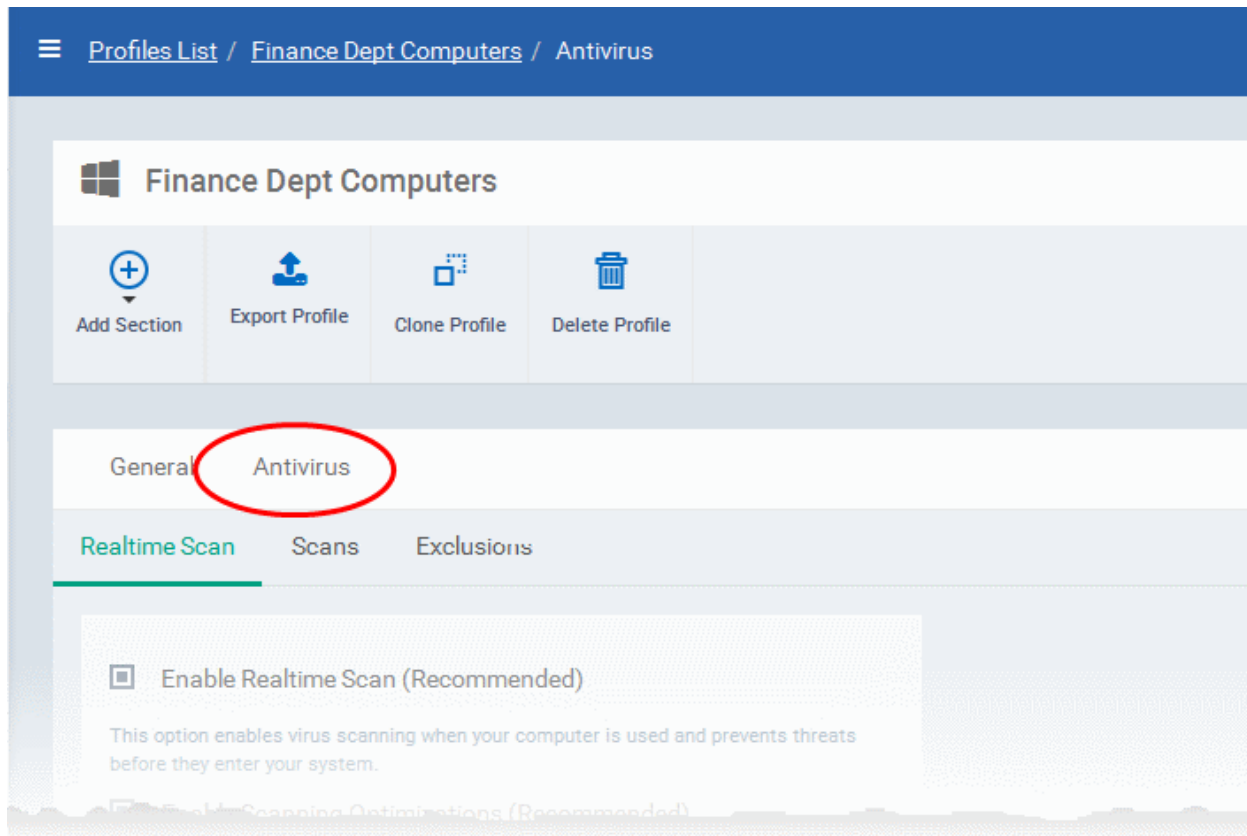


If the changes in the configuration of the component requires the restart of the endpoint to which the profile is applied, an alert dialog will be displayed.



- Click 'Confirm' to continue.

The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top.



Following sections explain more about each of the settings:

- **Antivirus**
- **File Rating**
- **Firewall**
- **Sandbox**
- **Viruscope**
- **HIPS**
- **Valkyrie**
- **CES Update Rule**

6.1.3.1.1. Antivirus Settings

The Antivirus setting screen has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe) for the profile.

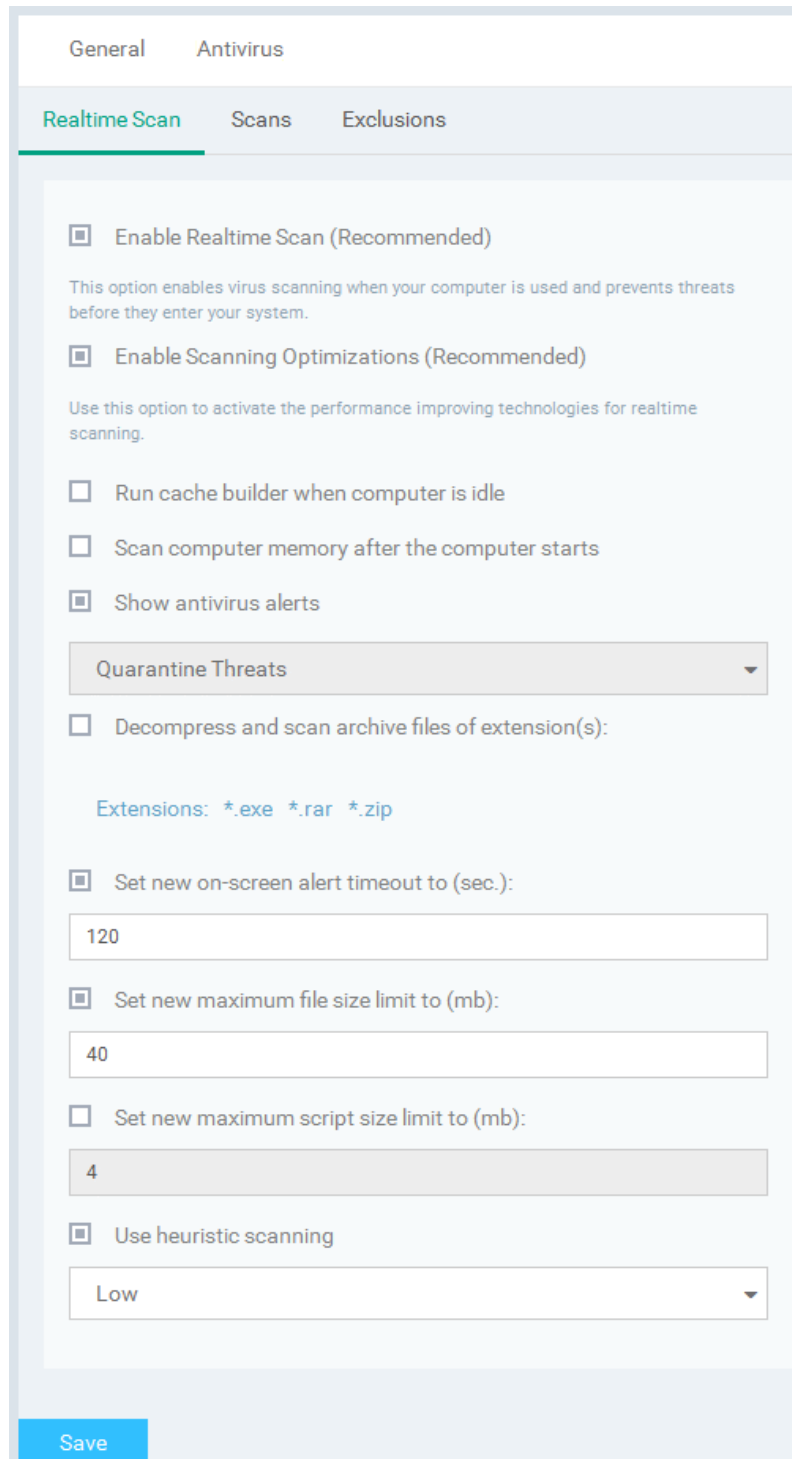
To configure Antivirus settings

- Choose 'Antivirus' from the 'Add' drop-down

The settings screen for Antivirus will be displayed.

- **Real Time Scan** - To set the parameters for on-access scanning
- **Scans** - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans
- **Exclusions** - To add items to be skipped on Antivirus scans at the devices, to which the profile is applied.

Realtime Scan Settings



Realtime Scan Settings - Table of Parameters	
Form Element	Description
Enable Realtime Scan	The Real time Scanning (aka 'On-Access Scanning') is always ON protection for checking files in real time when they are created, opened or copied. (as soon as a user interacts with a file, CES checks it). This instant detection of viruses assures the user, that the system is perpetually monitored for malware and enjoys the highest level of protection. <ul style="list-style-type: none"> Choose whether of not to enable real time scanning.
Enable Scanning Optimizations	CES will employ various optimization techniques like running the scan in the background in

	<p>order to reduce consumption of system resources and speed-up the scanning process.</p> <ul style="list-style-type: none"> Choose whether of not to enable scanning optimizations.
Run cache builder when computer is idle	The CES installation at the device runs the Antivirus Cache Builder whenever the computer is idle to boost real-time scanning
Scan computer memory after the computer start	Select this option to run the antivirus scan on the system memory during system start-up of the endpoint
Show antivirus alerts	<p>Allows you to configure whether or not to show antivirus alerts at the endpoints, when malware is encountered. Deselecting 'Show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CES should automatically take - either 'Block Threats' or 'Quarantine Threats'.</p> <ul style="list-style-type: none"> Quarantine threats - Moves the detected threat(s) to quarantine for your later assessment and action. Block threats - Stops the application or file from execution, if a threat is detected in it.
Decompress and scan archive files of extensions	<p>CES can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is selected. CES generates an alert even on the presence of viruses in compressed files before the end-user opens them.</p> <p>On selecting the option, you can add the archive file types that should be decompressed and scanned by clicking file types that are displayed below it and adding the new file types from the 'Extensions' dialog.</p>
Set new on-screen alert timeout to (secs)	Select the option to set the time period (in seconds) for which the alert message should stay on the screen at the endpoint. (Default = 120 seconds)
Set new maximum file size to (MB)	Select the option to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned. (Default = 40 MB)
Set new maximum script size limit to (MB)	Select the option to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (Default = 4 MB)
Use heuristics scanning	<p>Allows you to enable or disable Heuristics scanning and define scanning level.</p> <p>If enabled, you can select the level of Heuristic scanning from the drop-down:</p> <ul style="list-style-type: none"> Low - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (Default) Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives. High- Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too. <p>Background Note: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.</p> <p>This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.</p>

- Click the 'Save' button at the bottom.

Custom Scans

The 'Scans' pane allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CES:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To create a custom scan profile

- Click the 'Add' button in the Scans screen

The screenshot shows the 'Scans' pane in the Comodo Device Manager interface. The 'Add' button is circled in red, and a red arrow points to the 'Add Scan Profile' dialog box. The dialog box has a blue header with the title 'Add Scan Profile' and a 'Close' button. Below the header, there is a text prompt: 'Define items to be scanned, scanning options and running schedule.' The dialog is divided into several sections: 'Scan name' with a text input field containing 'Scan name'; 'Items' with three buttons: '+ Add File', '+ Add Folder', and '+ Add Region'; 'Options' with a text input field; and 'Schedule' with a text input field. At the bottom right, there are 'Cancel' and 'OK' buttons.

The 'Add Scan Profile' dialog will be displayed.

- Enter the name of the custom scan in the 'Scan name' field

By default, the 'Items' section will be displayed allowing you to specify the file name, folder and region to be included in the

custom scan profile.

- Add File - Allows you to add a specific file or you can also choose to add files with the same extension using the wildcard character
- Add Folder - Allows you to add a folder name
- Add Region - Allows you to add predefined regions to the profile. For example, 'Entire Computer', 'Commonly Infected Areas' and 'Memory'.

The entered/selected items will be displayed.

Add Scan Profile Close

Define items to be scanned, scanning options and running schedule.

Scan name

Finance Department Custom Scans

Items

[+ Add File](#) [+ Add Folder](#) [+ Add Region](#)

PROFILE ▲

Commonly Infected Areas

bank statements

10 25 50 100

Options

Schedule

Cancel **OK**

- To remove an item from the list, select it and click 'Remove'.

The next step is to define how the selected items should be scanned.

- Click 'Options'

Add Scan Profile Close

Define items to be scanned, scanning options and running schedule.

Scan name

Items

Options

- Enable Scanning optimizations**
This option increases the scanning speed significantly.
- Decompress and scan compressed files**
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning.
- Use cloud while scanning**

Background ▼

- Update virus database before running**
This option makes sure the database is updated before running the scan.
- Detect potentially unwanted applications**
Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download it.

Schedule

Cancel OK

Options Configuration - Table of Parameters	
Form Element	Description
Enable scanning optimizations	On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (Default = Enabled).
Decompress and scan compressed files	When this option is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (Default = Enabled).
Use cloud while scanning	Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. (Default = Disabled).
Automatically clean threats	On selecting this option, CES will automatically take action against the threats detected at the end of the scan, instead of showing the results screen with a list of threats identified. You can choose the action to be taken from the drop-down. The available options are: <ul style="list-style-type: none"> Disinfect Quarantine (Default = Enabled with Disinfect Threats option)
Use heuristics scanning	Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. (Default = Disabled). <p>Background Info: Comodo Endpoint Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.</p> <p>This allows CES to 'predict' the existence of new viruses - even if it is not contained in the current virus database.</p> <p>Low - Lowest sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.</p> <p>Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.</p> <p>High - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.</p>
Limit maximum file size to	Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected (Default = 40 MB).
Run this scan with	Enables you to set the priority of the scanning from High to Low and to run at background. (Default = Enabled)
Update virus database before running	Selecting this option makes CES to check for virus database updates and if available, update the database before commencing the scan. (Default = Enabled).
Detect potentially unwanted applications	When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and

Options Configuration - Table of Parameters	
	browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (Default = Disabled).

The next step is to schedule when the custom scan should be run.

- Click 'Schedule'

Schedule Settings - Table of Parameters	
Form Element	Description
Frequency	<ul style="list-style-type: none"> • Do not schedule this task - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning • Every Day - Runs the scan every day at the time specified • Every Week - Scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them. • Every Month - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
Run only when computer is not running on battery	This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adapter connected to mains supply and not on battery.
Run only when computer is IDLE	Select this option if you do not want to be disturbed when involved in computer related activities. The scheduled scan will run only if the computer is in idle state
Turn off computer if no threats are found at the end of the scan	Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.

- Click 'OK' to save the custom scan settings

General Antivirus

Realtime Scan **Scans** Exclusions

This page allow you to add, remove and edit scan profiles and scheduled tasks.


Add

NAME	STATUS
Finance Department Custom Scans	ON

10 25 50 100

Save

The added will be listed in the screen.

- Click the toggle switch under the 'Status' column beside the respective profile row to toggle between on and off status. The scan will be run only if it is enabled for the profile.
- To change the settings for the custom scan, click the edit button , edit the parameters and click 'OK'
- To remove a custom scan from the list, select it and click 'Remove'

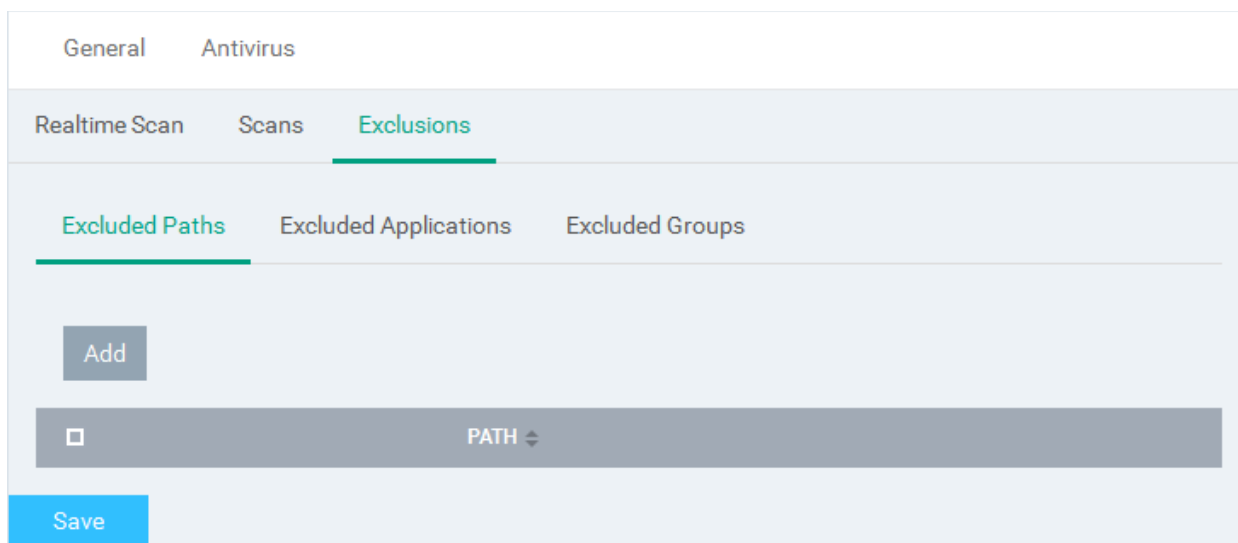
Exclusions

The 'Exclusions' screen under the Antivirus setting has three sub sections that allow you to add a list of paths, list of applications/files and 'File Groups' which should be excluded from the antivirus scan.

- Click 'Exclusions'

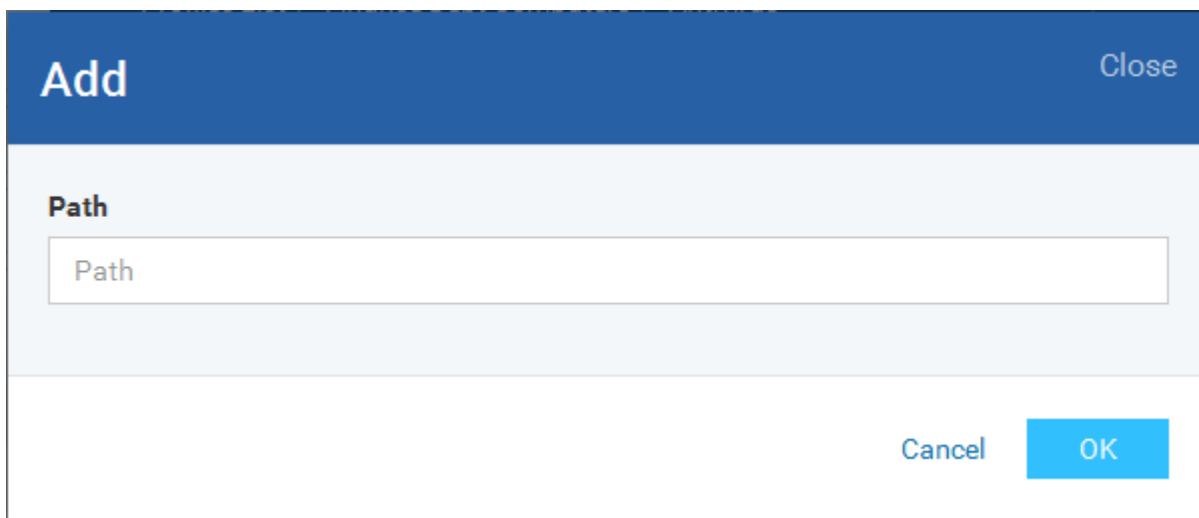
To add excluded paths

By default the 'Excluded Paths' screen will be displayed:



- Click 'Add'


The 'Add' dialog will be displayed:



- Enter the full path that should be excluded from scanning and click 'OK'.

The added excluded path will be added to the list.

The screenshot shows the 'Exclusions' section of the Comodo Device Manager interface. At the top, there are tabs for 'General' and 'Antivirus'. Below these are sub-tabs for 'Realtime Scan', 'Scans', and 'Exclusions', with 'Exclusions' being the active tab. Under 'Exclusions', there are three sub-sections: 'Excluded Paths', 'Excluded Applications', and 'Excluded Groups', with 'Excluded Paths' selected. The interface includes an 'Add' button and a 'Remove' button. A list of excluded paths is shown, with one entry: 'C:\Program Files\Paint.NET'. To the right of the list are radio buttons for selecting the number of exclusions: 10, 25, 50, and 100. A 'Save' button is located at the bottom left.

- 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'

The screenshot shows the 'Exclusions' section of the Comodo Device Manager interface, with the 'Excluded Applications' sub-tab selected. The 'Add' button is visible. The list of excluded applications is currently empty. The 'Save' button is located at the bottom left.

- Click 'Add'

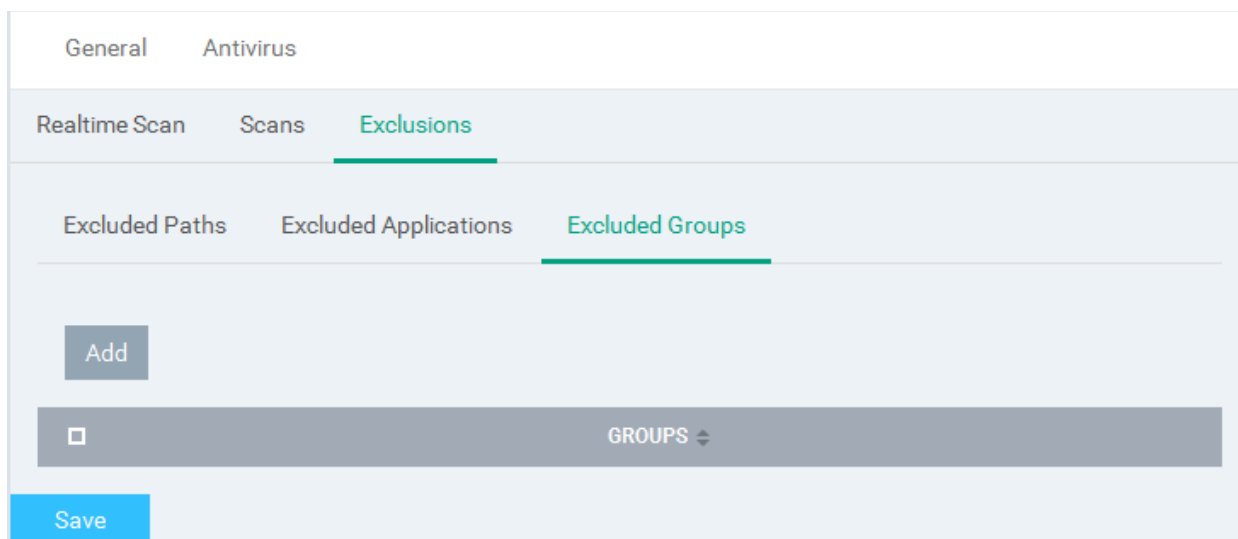
- Enter the full path including the application that should be excluded from scanning and click 'OK'
- Repeat the process to include more applications

- To change the application path, click the edit button , edit the parameters and click 'OK'
- To remove an application from the list, select it and click 'Remove'

To add Excluded Groups

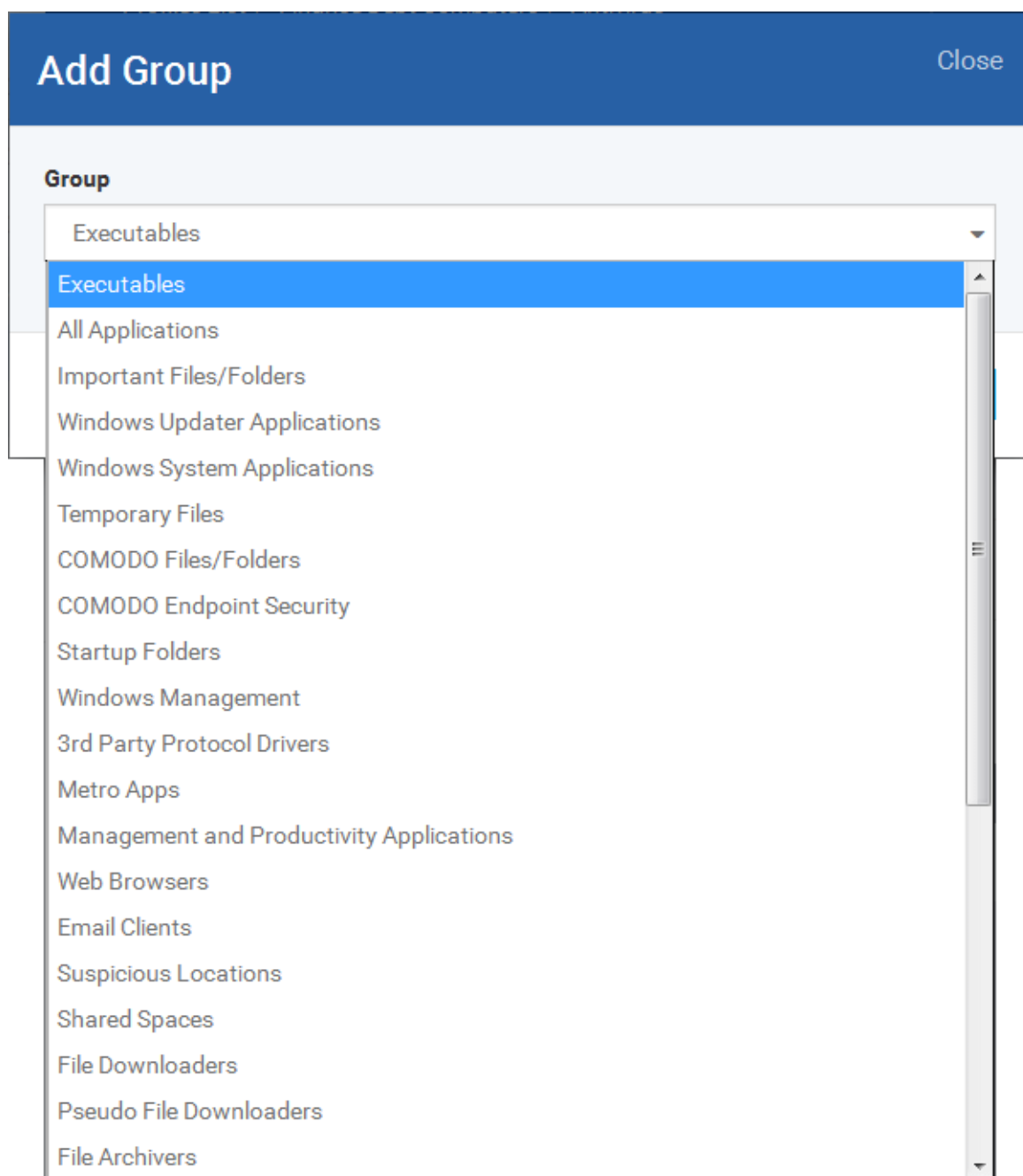
File Groups are handy, predefined groupings of one or more file types which make it easy to add an entire class of file types to Exclusions. CDM ships with a set of predefined 'File Groups' and, if required users, can add new File Groups and edit existing groups. Refer to the portion explaining '[File Groups](#)' under [Settings > Global Variables](#).

- Click 'Excluded Groups'



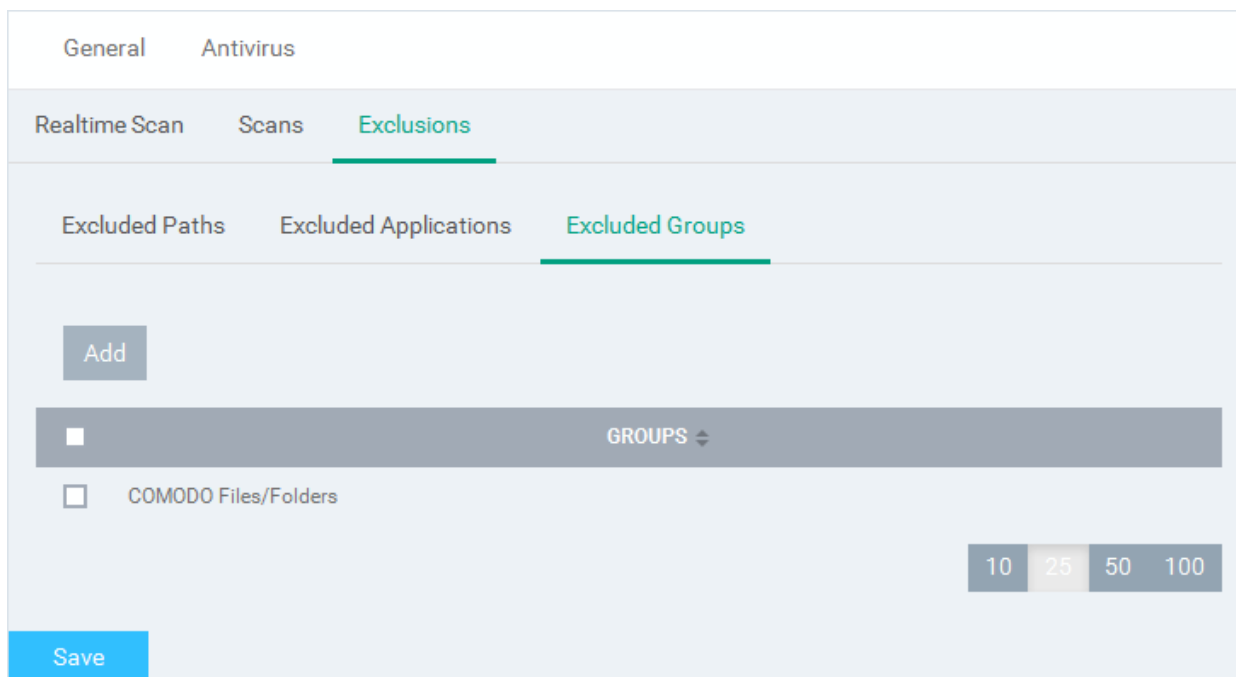
- Click Add.

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. File Rating Settings

The CES 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, CES 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: CES uses Ports 4446 and 4447 of the endpoint computers for TCP and UDP connections to the cloud. Comodo advises to maintain these ports free and not assigned to other applications, if this option is enabled.

The File Rating setting interface allows you to configure the overall behavior of 'File Rating' of CES installation at the Windows devices to which the profile is applied.

To configure File rating settings

- Click 'File Ratings' from the 'Add' drop-down

The settings screen for File Ratings will be displayed.

The screenshot shows the 'File Rating' configuration page for 'Finance Dept Computers'. The page has a blue header with navigation links: 'Profiles List / Finance Dept Computers / File Rating'. On the right of the header, there are icons for a menu, a notification bell with a '4' badge, and a 'Logout (John Smith)' button. The main content area has a title 'Finance Dept Computers' with a Windows logo icon. Below this is a 'File Rating' section with a 'Cancel' and 'Save' button. The section contains several checkboxes, all of which are currently unchecked:

- Enable Cloud Lookup
- Analyze unknown files in the cloud by uploading them for instant analysis
- Show Cloud Alert

Below these checkboxes is a note: 'This option,when disabled,automatically applies "Block and Terminate" action to malware detected by cloud scanning.'

- Trust applications signed by trusted vendors
- Trust applications signed by trusted installers
- Detect potentially unwanted applications
- Auto Rescan Is Enabled
- Auto Purge Is Enabled

Under the heading 'Auto Purge Period', there is a text input field with the placeholder text 'Set Auto Purge Period in Hours' and a small dropdown arrow icon on the right. Below the input field is the text 'Timeout to auto purge in hours.'

File Rating Configuration - Table of Parameters	
Form Element	Description
Enable Cloud Lookup	Allows you to enable or disable cloud based File Rating.
Analyze unknown files in the cloud by uploading them for instant analysis	When this option is enabled CES instructs to upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the the whitelist or blacklist according to the analysis.
Show Cloud Alert	This option allows you to configure whether or not to show alerts when malware is encountered. If this option is not selected, then CES will automatically apply 'Block and Terminate' action to malware detected by cloud scanning.
Trust applications signed by trusted vendors	When this option is enabled, CES will award trusted status to the executables and files that are digitally signed by vendors in the Trusted Vendors list using their code signing certificates. CDM ships with a pre-defined Trusted Software Vendors list that is applied in common to all Windows profiles. If required, the administrators can view and edit the Trusted Vendor List. Refer to the section Viewing and Managing Trusted Software Vendors List for more details.
Trust applications signed by trusted installers	When this option is enabled, CES will trust executables and files signed by trusted Installers or Updaters.
Detect potentially unwanted applications	When this option is selected, CES identifies the applications that: <ul style="list-style-type: none"> • A user may or may not be aware is installed on their computer, and/or • May have functionality and objectives that are not clear to the user. <p>Example: Potentially Unwanted Applications (PUAs) include adware and browser toolbars. PUAs are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet.</p> <p>On detecting a PUA, the CES installation at the endpoint raises an alert for the user to decide whether or not to run it and add it to the logs.</p>
Auto Rescan is enabled	On selecting this option, a schedule is created at the endpoint for CES to periodically scan the endpoint for unrecognized files and update the file list.
Auto Purge is enabled	When this option is selected, CES refreshes the file list and removes invalid and obsolete entries in the file list corresponding to the endpoint, at the time interval specified in the 'Auto Purge' Period field.
Auto Purge Period	The time interval at which the auto purge operations are performed. Enter the time interval in hours.

- Click the 'Save' button

The saved 'File Rating' settings screen will be displayed with options to edit the settings or delete the section. Refer to the section **Editing Configuration Profiles** for more details.

6.1.3.1.3. Firewall Settings

The Firewall Settings interface allows you to configure the overall behavior of Firewall component of CES installed at the endpoints to which the profile is applied. You can also configure network zones and portsets and to configure and deploy traffic filtering rules on an application specific and global basis.

To configure Firewall Settings and Traffic Filtering Rules

- Click 'Firewall' from the 'Add' 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

General
File Rating
Firewall

Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets

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

▲

Save
Delete

Firewall Configuration - Table of Parameters	
Form Element	Description
Enable Traffic Filtering	<p>Allows you to enable or disable Firewall protection at the endpoint. If enabled the following options are available:</p> <ul style="list-style-type: none"> Block All Mode - The firewall blocks all traffic in and out of endpoints regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any application and does not automatically create traffic rules for any applications. Choosing this option effectively prevents endpoints from accessing any networks, including the Internet. Custom Ruleset Mode - 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

Firewall Configuration - Table of Parameters	
	<p>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).</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.</p> <ul style="list-style-type: none"> • 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. <p>For more details on the Firewall Settings, see the of CES - Firewall Settings online help page at http://help.comodo.com/topic-84-1-604-7471-Firewall-Settings.html.</p>
Show popup alerts	<p>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:</p> <ul style="list-style-type: none"> • Block Requests • Allow Requests
Turn traffic animation effects on	<p>The CES tray icon can display a small animation whenever traffic moves to or from your computer.</p> <div style="text-align: center;">  </div> <p>You can enable or disable the animation to be displayed at the endpoint.</p>
Create rules for safe applications	<p>Comodo Firewall trusts the applications if:</p> <ul style="list-style-type: none"> • 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. <p>By default, CES 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.</p>

Firewall Configuration - Table of Parameters	
	Enabling this option instructs CES 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 CES installation. Advanced users can edit/modify the rules as they wish. (Default = Disabled)
Set alert frequency level	<p>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. (<i>Default=Disabled</i>)</p> <p>The options available are:</p> <ul style="list-style-type: none"> • 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. <p>The Alert Frequency settings refer only to connection attempts by applications or from IP addresses that you have not (yet) decided to trust.</p>
Set new on-screen alert timeout to:	Determines how long the Firewall shows an alert for, without any user intervention at the endpoint. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference by selecting this option and choosing the period from the drop-down combo-box.
Filter IPv6 traffic	<p>If enabled, the firewall component of CES at the endpoint will filter IPv6 network traffic in addition to IPv4 traffic.</p> <p>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.</p> <p>IPv6 on the other hand, uses 128 bits per address (delivering 3.4×10^{38} 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.</p>
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

Firewall Configuration - Table of Parameters	
	<p>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.</p> <p>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).</p>
Block fragmented IP traffic	<p>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.</p> <p>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.</p> <p>If you want the firewall component of CES at the endpoint to block the fragmented datagrams, enable this option. (Default = Disabled).</p>
Do Protocol Analysis	<p>Protocol Analysis is key to the detection of fake packets used in denial of service (DOS) attacks.</p> <p>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 = Disabled).</p>
Enable anti-ARP spoofing	<p>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 = Disabled).</p>

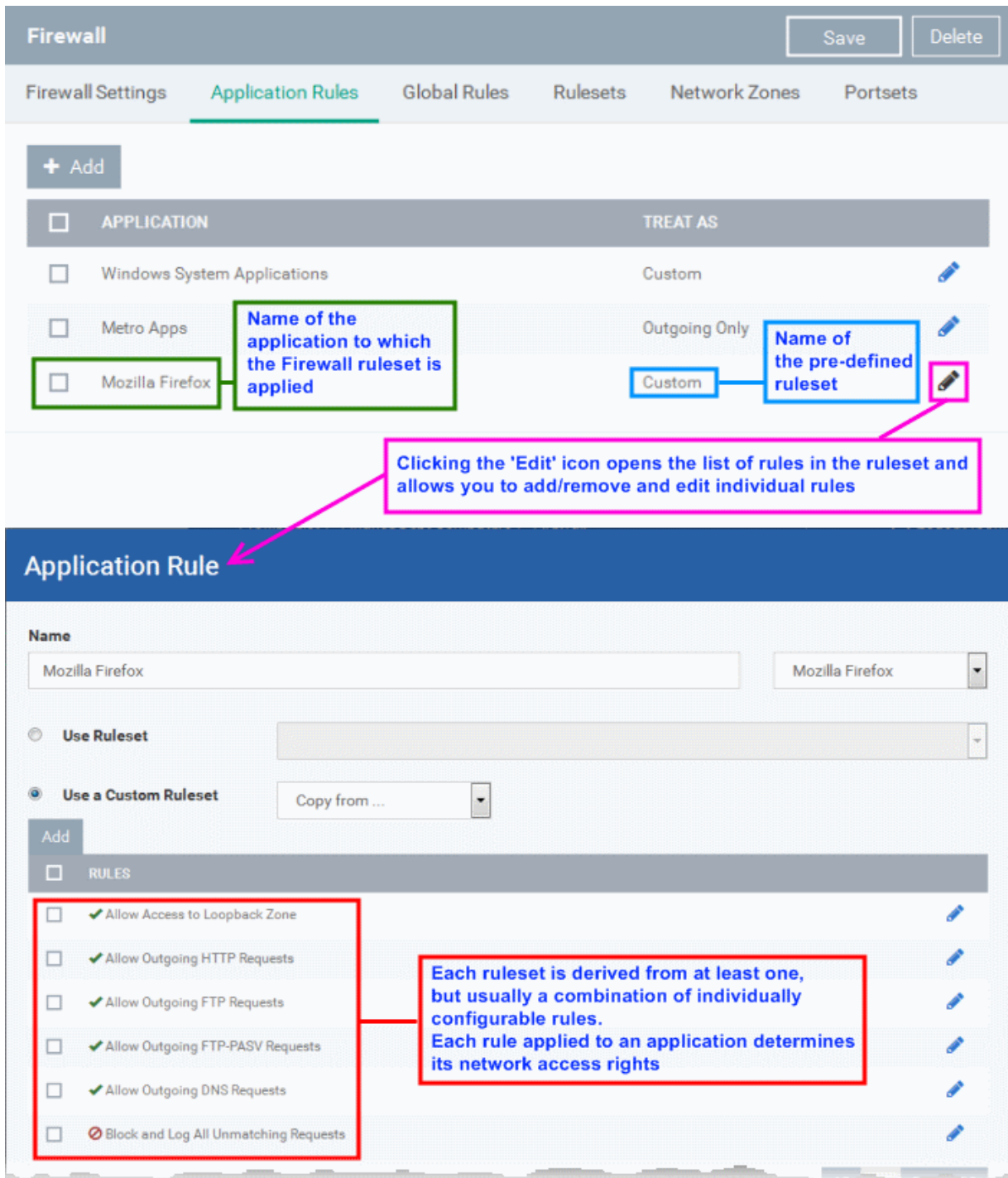
Application Rules

Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network access rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.

The screenshot shows the 'Firewall' configuration page. At the top, there are tabs for 'General', 'File Rating', 'Firewall', and 'HIPS'. Below these is a 'Firewall' header with 'Save' and 'Delete' buttons. Underneath is a sub-menu with 'Firewall Settings', 'Application Rules', 'Global Rules', 'Rulesets', 'Network Zones', and 'Portsets'. The 'Application Rules' sub-tab is selected. Below this is a '+ Add' button and a table with the following data:

<input type="checkbox"/>	APPLICATION	TREAT AS	
<input type="checkbox"/>	COMODO Endpoint Security	Outgoing Only	
<input type="checkbox"/>	Windows Updater Applications	Custom	
<input type="checkbox"/>	Windows System Applications	Custom	
<input type="checkbox"/>	Metro Apps	Outgoing Only	

The Application Rules interface allows you to create and manage application rules for regulating network access to individual applications at the endpoints to which the profile is applied.



Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Administrators can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see [Predefined Rule Sets](#).

- See [Application Rule interface](#) for an introduction to the rule setting interface
- See [Creating and Modifying Firewall Rulesets](#) to learn how to create and edit Firewall rulesets
- See [Understanding Firewall Rules](#) for an overview of the meaning, construction and importance of individual rules
- See [Adding and Editing a Firewall Rule](#) for an explanation of individual rule configuration

Application Rule interface

The rules in a Firewall ruleset can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using **Adding and Editing a Firewall Rule** is displayed in this list.

The Application Rule interface is displayed when you click the 'Add' button  or 'Edit' icon  beside a ruleset, from the options in 'Application Rules' interface.


Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see **Understanding Firewall Rules** for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied. Administrators can re-prioritize rules by using 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.**
- 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' button  at the top of the list in the 'Application Rules' interface.

The 'Application Rule' interface will open as shown below:

Application Rule

Name

My Rule My Rule

Use Ruleset

Use a Custom Ruleset

Copy from ...

Add

RULES

OK Cancel

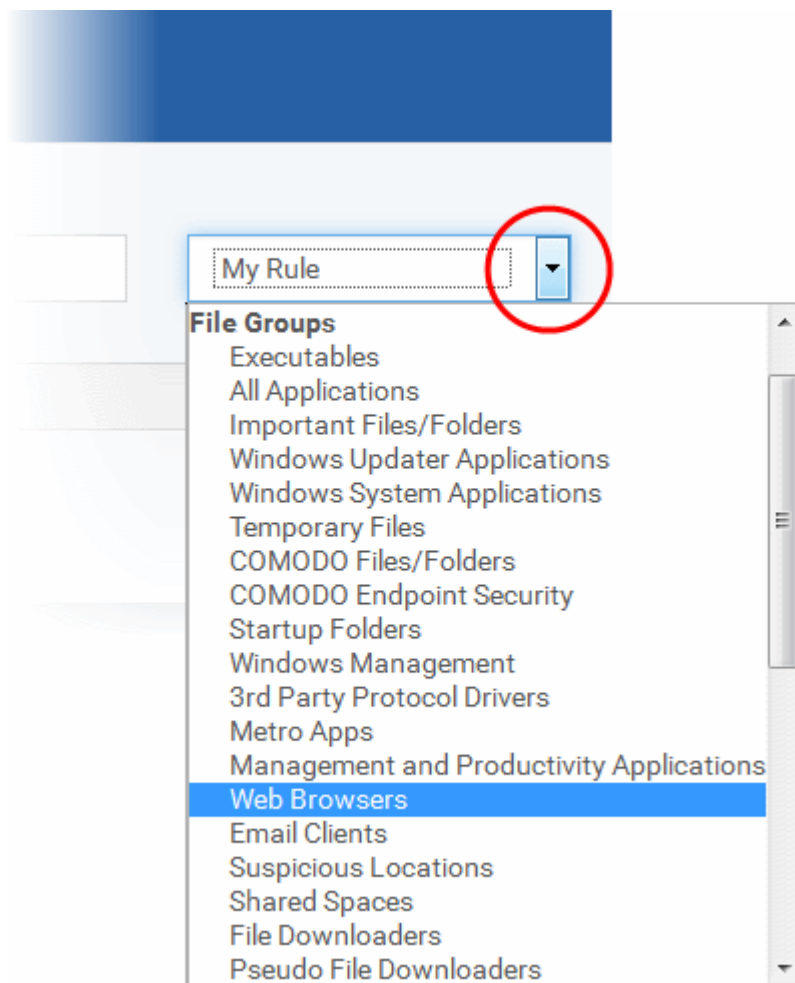
Because this is a new application, the 'Name' field is pre-entered with 'My Rule'. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

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

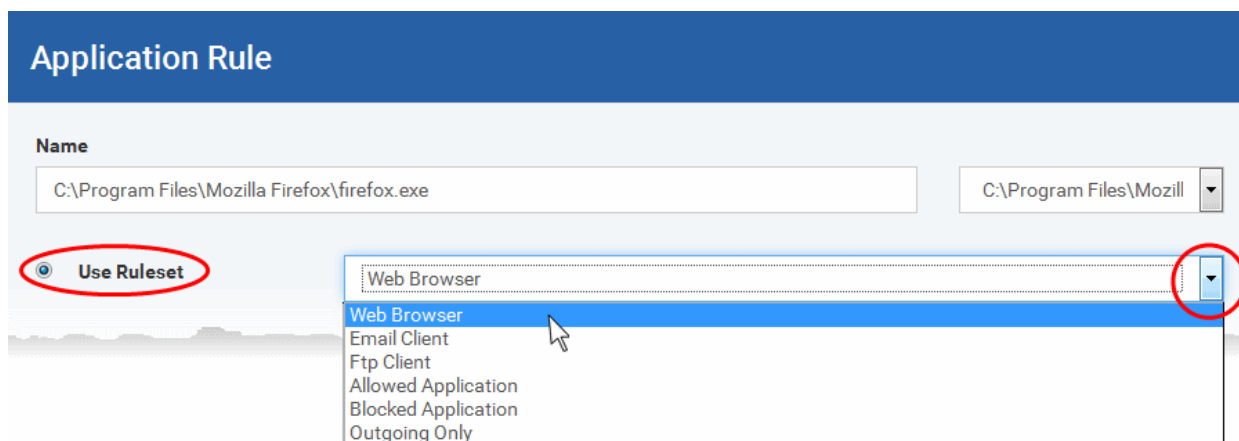
- Open the drop-down beside the 'Name' field and choose the Application Group to which the ruleset is to be applied. Choosing a 'File Group' allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset 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. CDM 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 > Global Variables](#).



Step 2 - Configure the rules for this application's ruleset

There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Allows you to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Firefox' browser. The name of the predefined ruleset you choose is displayed in the 'Treat As' column for that application in the **'Application Rules' interface (Default = Disabled)**.



Note: Predefined Rulesets, once chosen, cannot be modified *directly* from this interface - they can only be modified and defined using the **Application Rule** interface. If you require the ability to add or modify rules for an application then you are

effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - Designed for more experienced administrators, the Custom Ruleset option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset (*Default = Enabled*).

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 Log as firewall event if this rule is fired

Protocol

Direction

Description

Exclude (i.e. NOT the choice below)

Type

IP

General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' (*Default*), '**Block**' or '**Ask**'.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' (*Default*), '**ICMP**' or '**IP**' .

Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are '**In**', '**Out**' or '**In/Out**' (*Default*).
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the firewall event log viewer whenever this rule is called into operation. (i.e. when ALL conditions have been met) (*Default = Disabled*).
- **Description:** Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

Protocol

- i. **TCP**, '**UPD**' or '**TCP or UDP**'

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.

Firewall Rule

Action Log as firewall event if this rule is fired

Protocol

Direction

Description

Source Address Destination Address Source Port Destination Port

Exclude (i.e. NOT the choice below)

Type ▼

IP

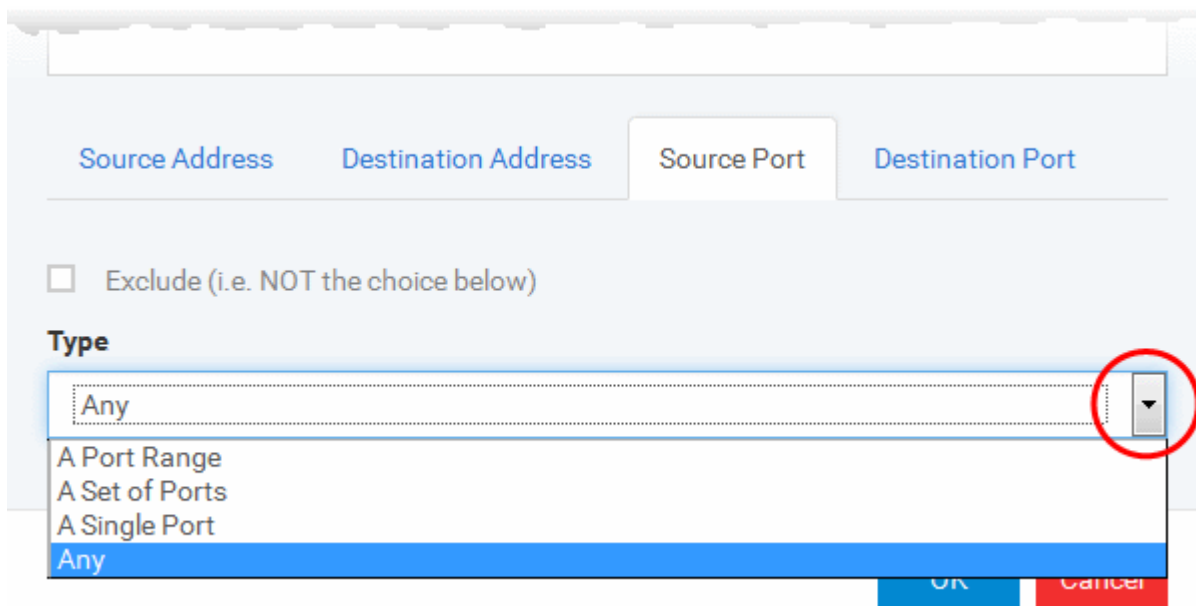
- Any Address
- Host Name
- IPv4 Address Range
- IPv4 Single Address
- IPv4 Subnet Mask
- IPv6 Single Address
- IPv6 Subnet Mask
- MAC Address
- Network Zone

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**'.

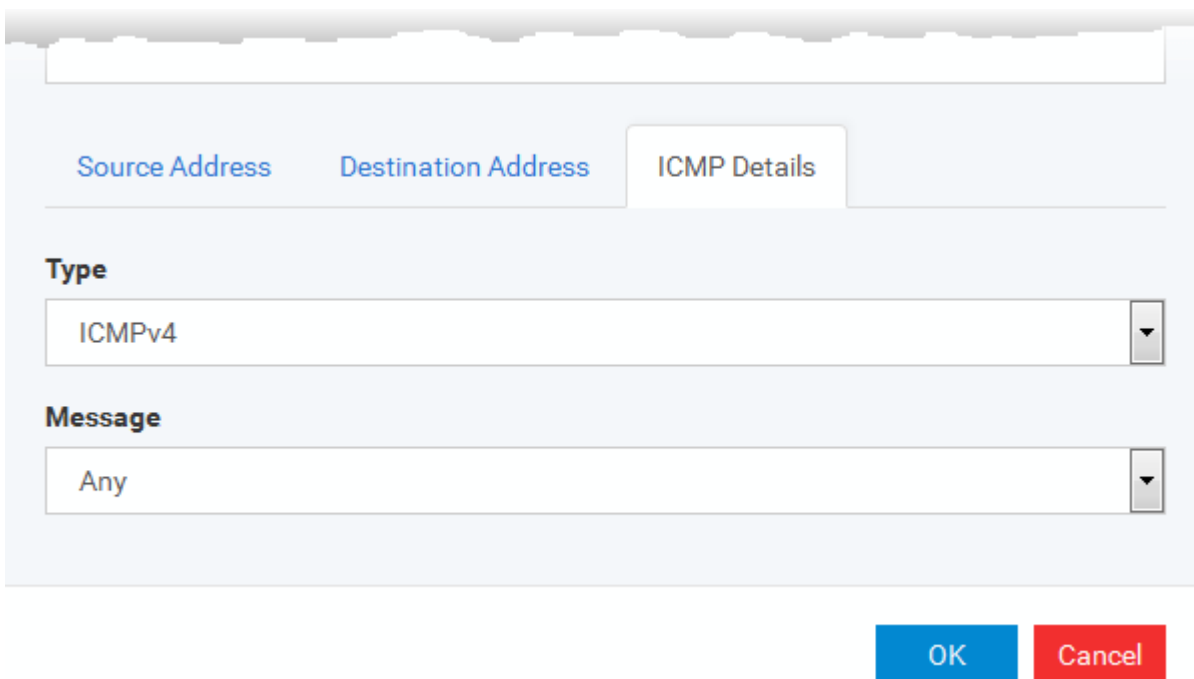
ii. **ICMP**

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.

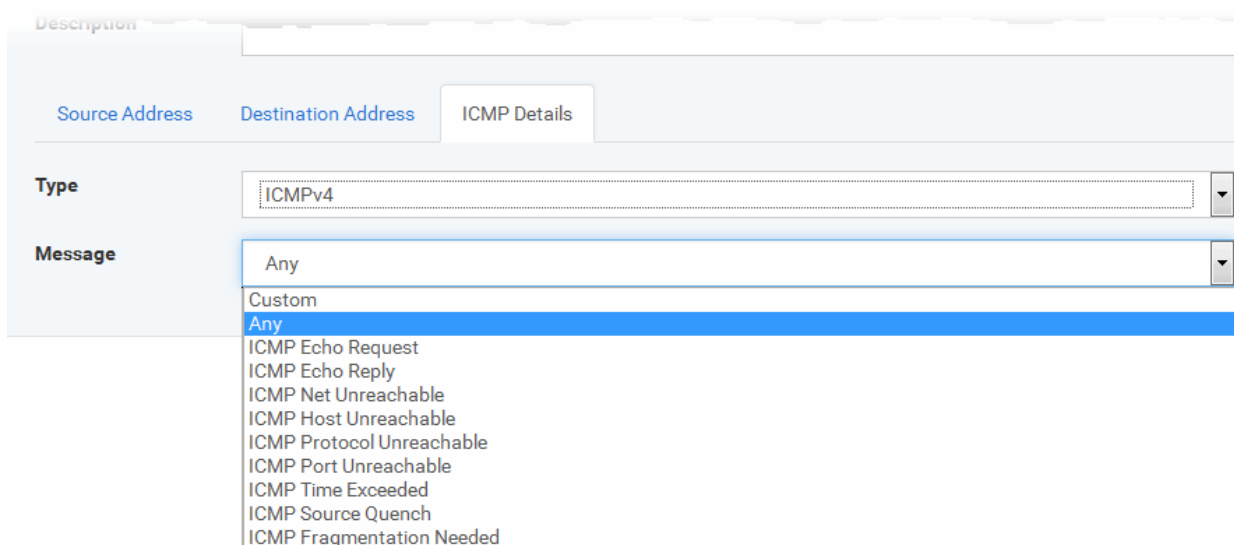
- **ICMP Details**

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

- Any Address
- Host Name
- IPv4 Address Range
- IPv4 Single Address
- IPv4 Subnet Mask
- IPv6 Single Address
- IPv6 Subnet Mask
- MAC Address
- Network Zone

- **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

- Custom
- Any
- TCP
- UDP
- ICMPv4
- IGMP
- Raw IP
- PUP
- GGP
- GRE
- RSVP
- ICMPv6

- Click 'OK' to save the firewall rule.

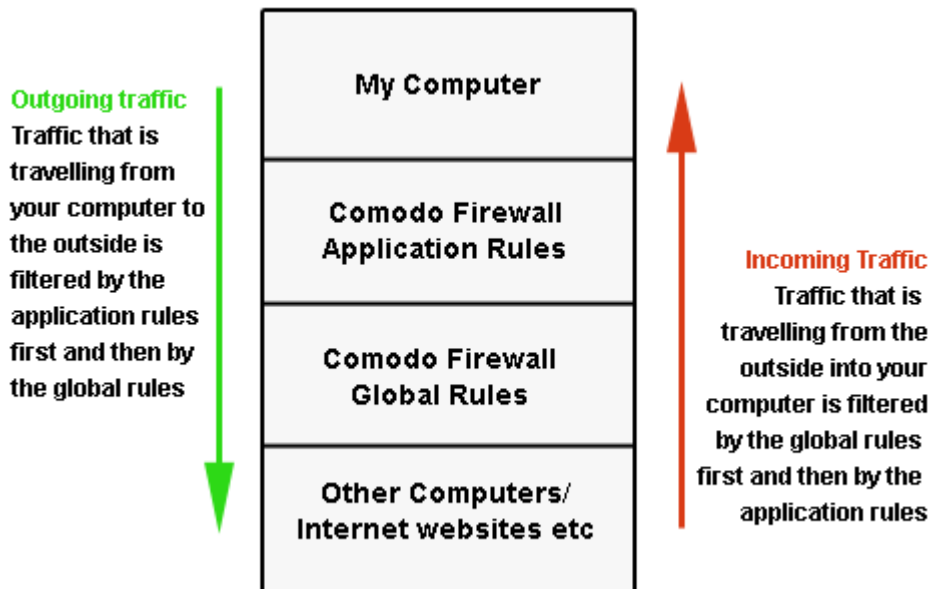
Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied

to all traffic traveling in and out of the computers applied with this profile.

Comodo Firewall analyzes every packet of data in and out of the computer using combination of Application and Global Rules.

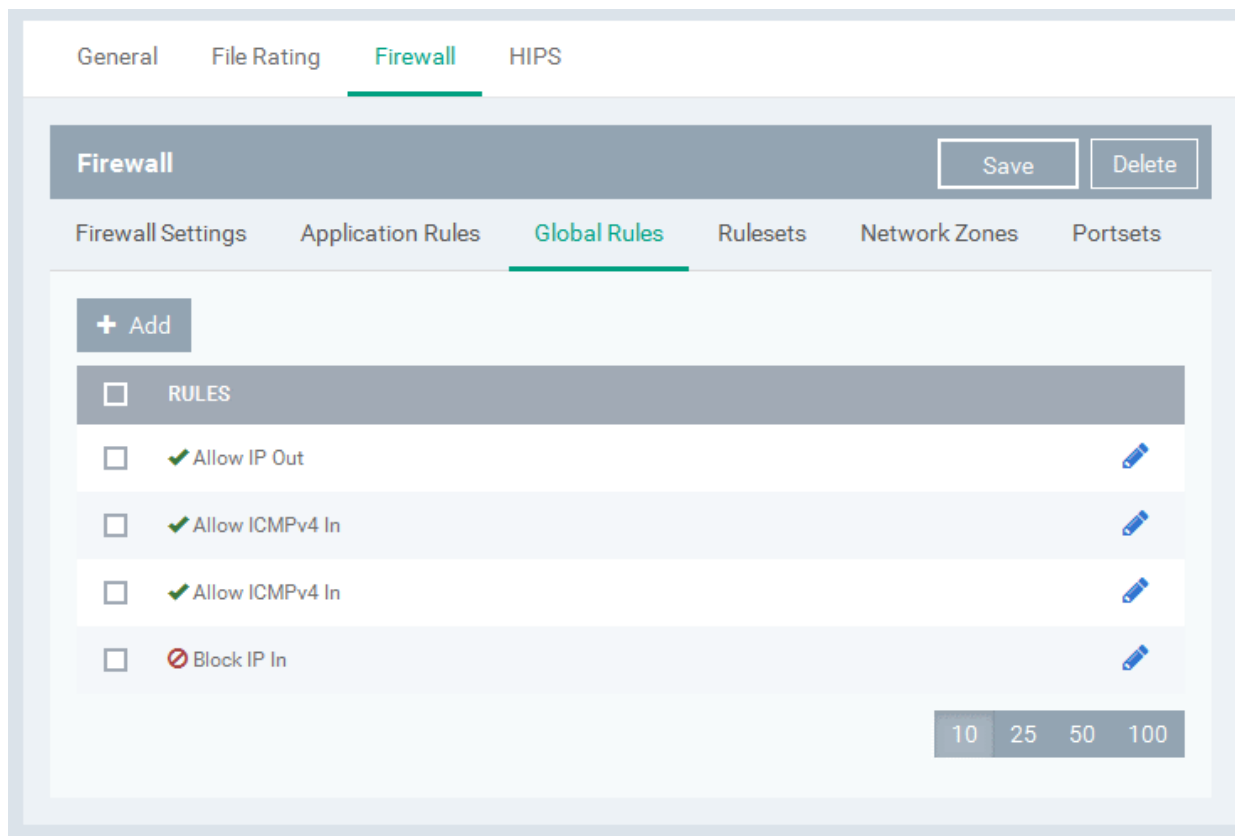
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.


Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

The 'Global Rules' panel in the under 'Firewall' tab allows you to view create and manage the global firewall rules.



The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add' button

 Add

on the top. To edit an existing global rule, click the edit icon  beside it.

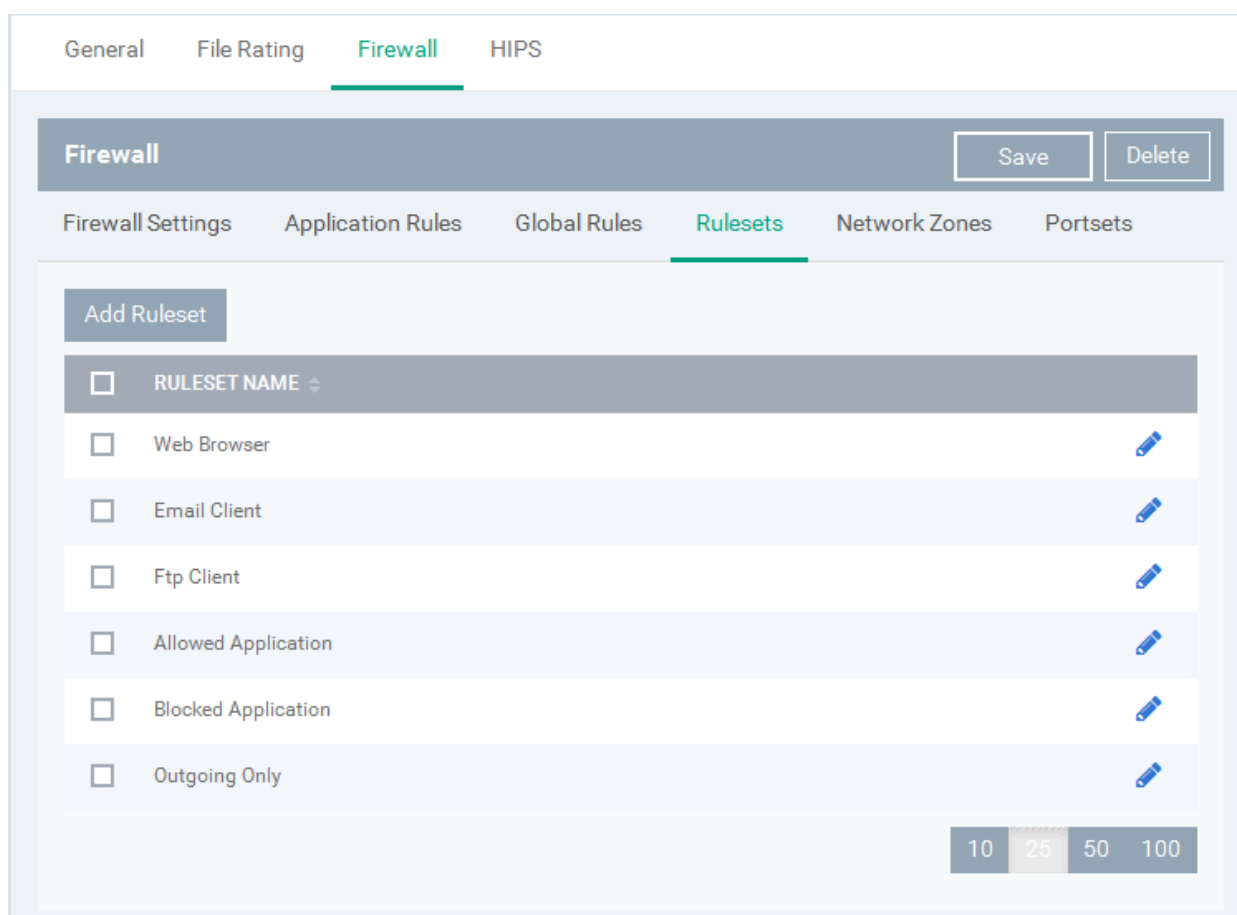
- See [Application Rules](#) for an introduction to the rule setting interface.
- See [Understanding Firewall Rules](#) for an overview of the meaning, construction and importance of individual rules.
- See [Adding and Editing a Firewall Rule](#) for an explanation of individual rule configuration.

Rulesets

As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. CDM ships with six predefined rulesets and allows you to create and manage custom rulesets as required. This section contains advice on the following:

- [Predefined Rulesets](#)
- [Creating a new ruleset](#)

The 'Rulesets' panel under the 'Firewall' tab allows you to view, create and manage the firewall rulesets.



The screenshot shows the 'Firewall' tab selected in the Comodo Device Manager interface. The 'Rulesets' sub-tab is active, displaying a list of predefined rulesets. Each rule set includes a checkbox and an edit icon. The rulesets listed are: 'RULESET NAME', 'Web Browser', 'Email Client', 'Ftp Client', 'Allowed Application', 'Blocked Application', and 'Outgoing Only'. At the bottom right of the panel, there are buttons for '10', '25', '50', and '100'.

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).

CIS ships with six predefined firewall rulesets for different categories of applications:

- Web Browser
- Email Client
- FTP Client
- Allowed Application
- Blocked Application
- Outgoing Only

These rulesets can be edited by adding new rules or reconfiguring the existing rules. For more details refer to the explanation of [Adding and Editing Firewall Rules](#) in the section 'Application Rules'.

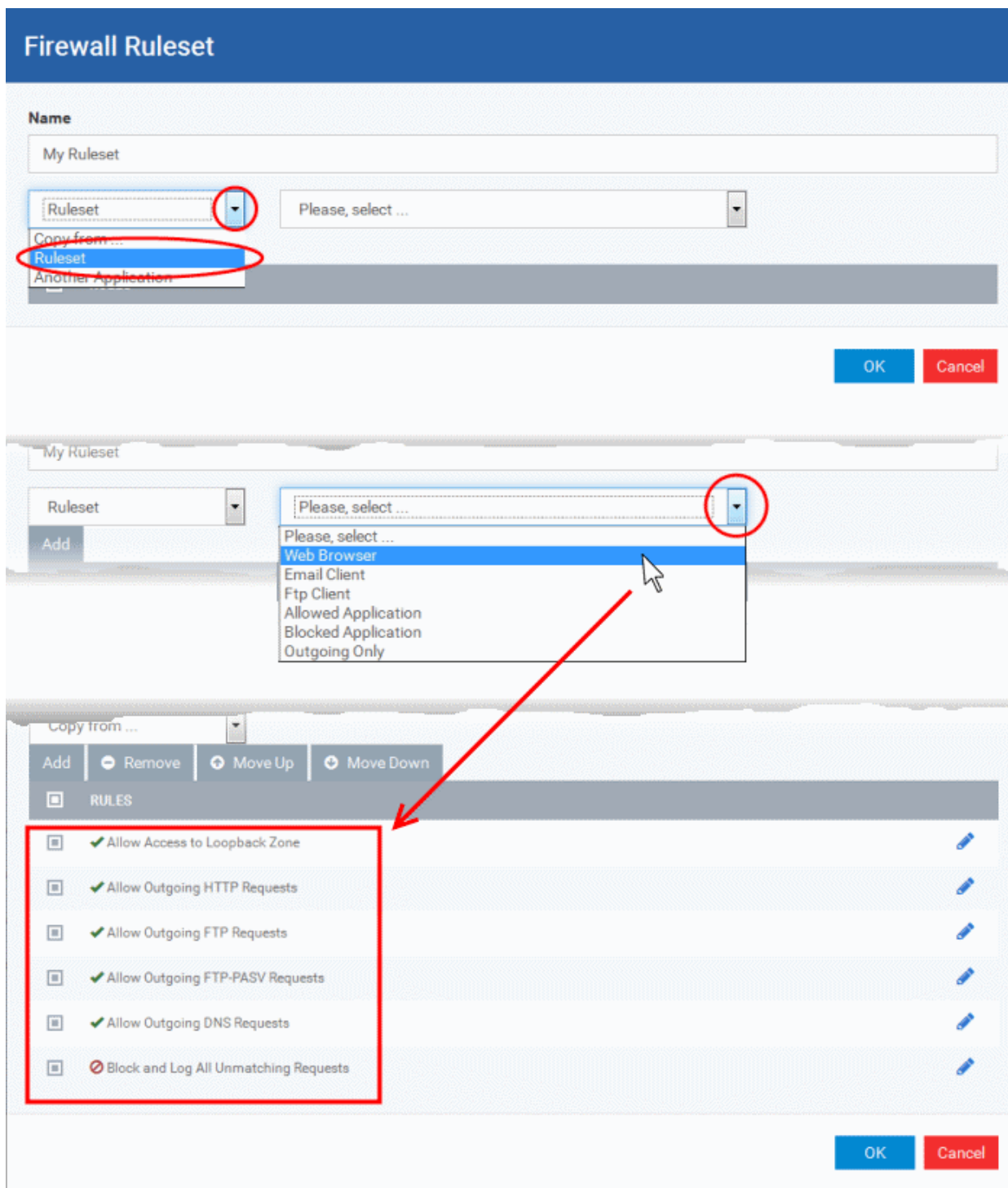
Creating a new ruleset

You can create new rulesets with network access control rules customized as per your requirements and can roll out them to required applications while [creating Firewall ruleset](#) for the applications individually.

To add a new Ruleset


- Click the 'Add Ruleset' button  from the top of the list of rulesets in the 'Rulesets' panel

The 'Firewall Ruleset' interface will open.



- As this is a new ruleset, you need to name it in the 'Name' field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for. Next you should add and configure the individual rules for this ruleset. See **'Adding and Editing a Firewall Rule'** for more advice on this. Once created, this ruleset can be quickly called from 'Use Ruleset' when **creating or modifying a Firewall ruleset**.

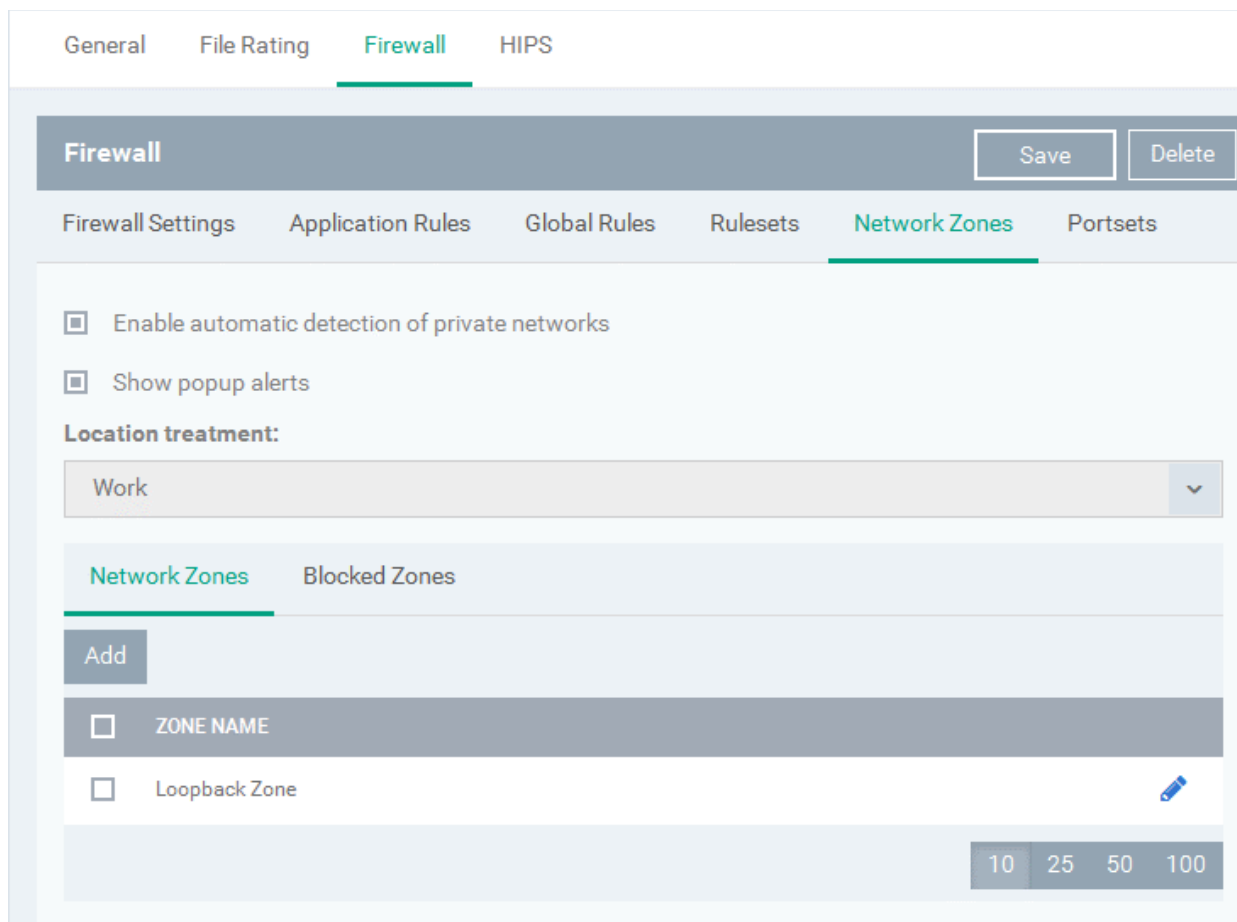
To view or edit an existing predefined Ruleset

- Click on the 'Edit' icon  beside Ruleset Name in the list.
- Details of the process from this point on can be found under **'Use Custom Rule Set'**.

Network Zones

The 'Network Zones' panel under the 'Firewall' tab allows you to:

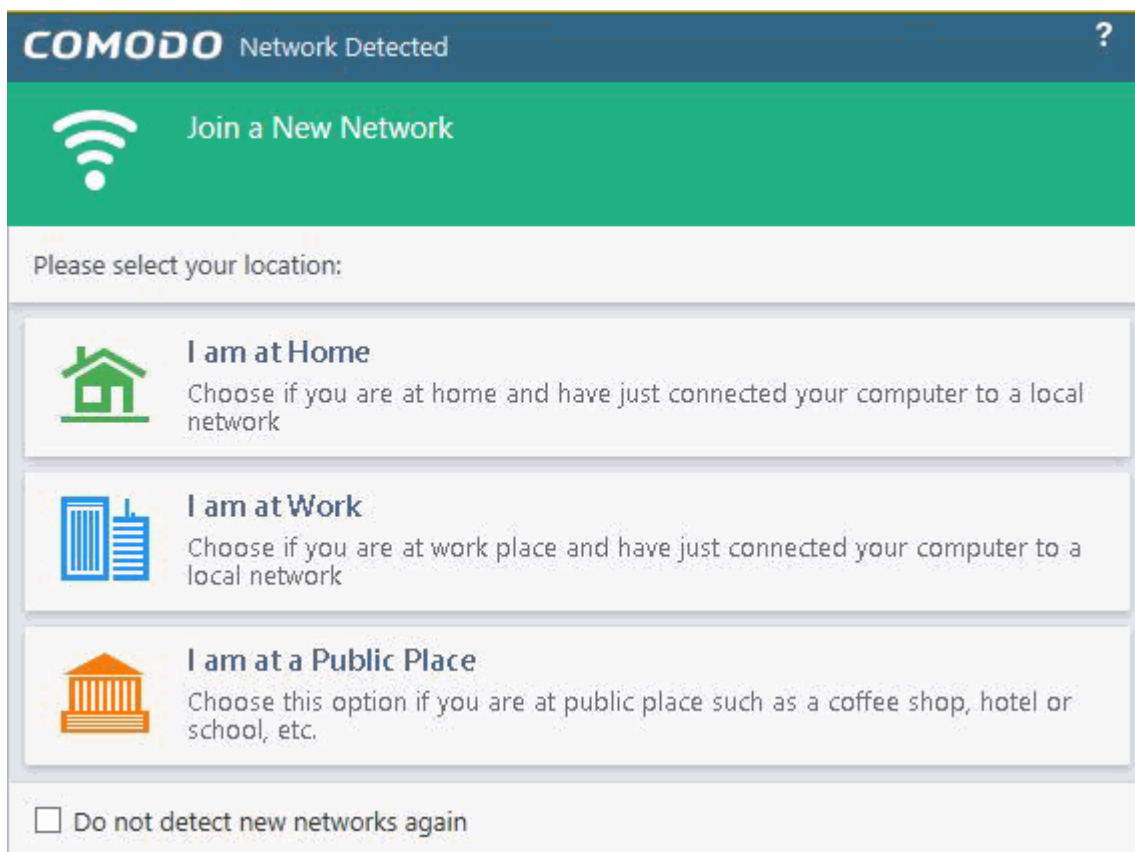
- Configure to detect any new network (wired or wireless) that the computer applied with this profile is trying to connect and provide alerts for the same
- Define network zones that are trusted, and to specify access privileges to them
- Define network zones that are untrusted, and to block access to them



The 'Network Zones' panel contains options for configuring the general network monitoring settings and lists of 'Allowed Network Zones' and 'Blocked Network Zones' under respective tabs. You can add and manage network zones to be allowed and blocked from this interface.

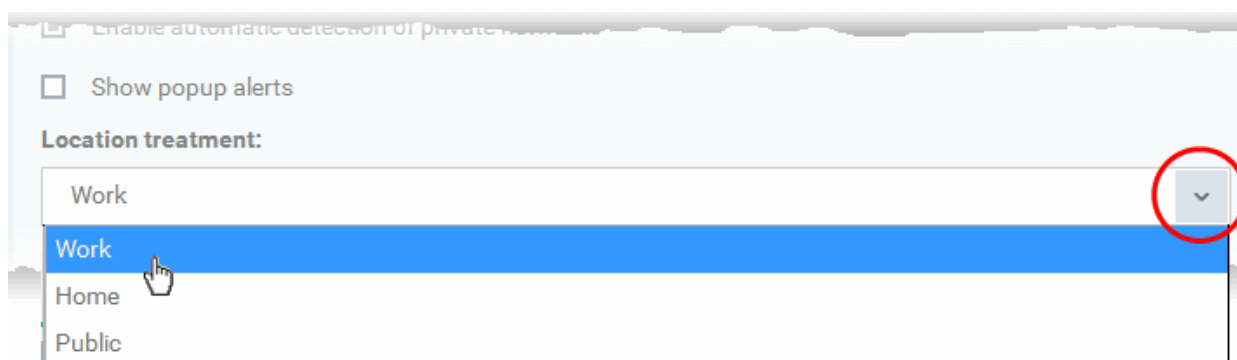
Network Monitoring Settings:

- **Enable automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether the computer applied with this security profile is connected to any new wired or wireless network (**Default = Enabled**). Deselect this option if you do not want the new connection attempts is to be detected and/or wish to manually set-up their own trusted networks (this can be done in **'Network Zones'**).
- **Show popup alerts and treat location as** - 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. CES will optimize its firewall settings for the new network, based on the selection. An example is shown below.



If you do not want the alert to be displayed to the end-user and wish the CES at the computer to decide on the type of network by default, de-select this option and choose the network type from the drop-down under Location Treatment. The available options are:

- Home
- Work
- Public



The panel has two tabs:

- **Network Zones** - Allows you to define network zones and to allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.
- **Blocked Zones** - Allows you to define trusted networks that are not trustworthy and to block access to them.

Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied.

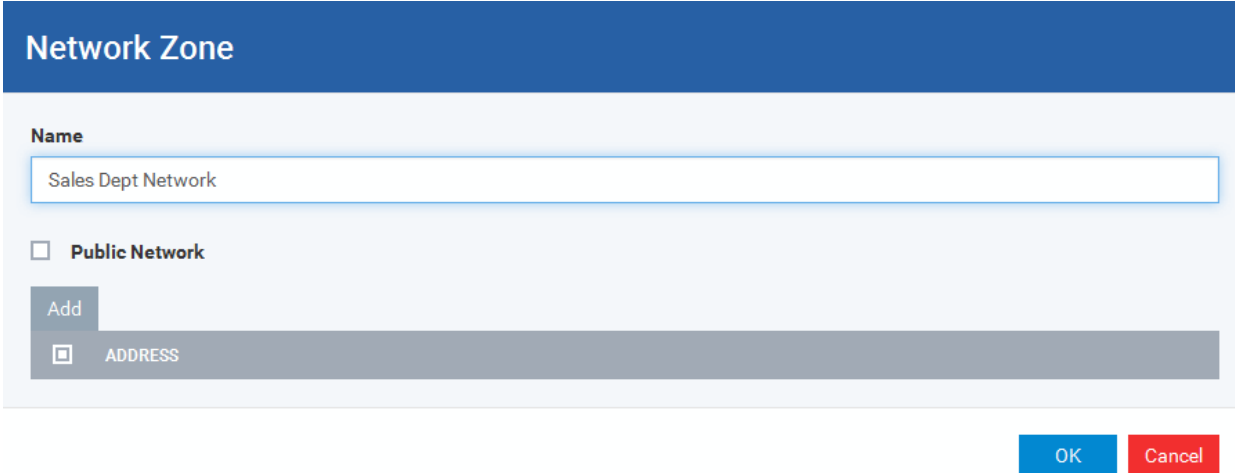
The 'Network Zones' tab in the 'Network Zones' panel displays a list of defined network zones and allows you to define network zones, to which the computer applied with this profile can connect, with access rights as defined by the firewall rules or blocked

access to.

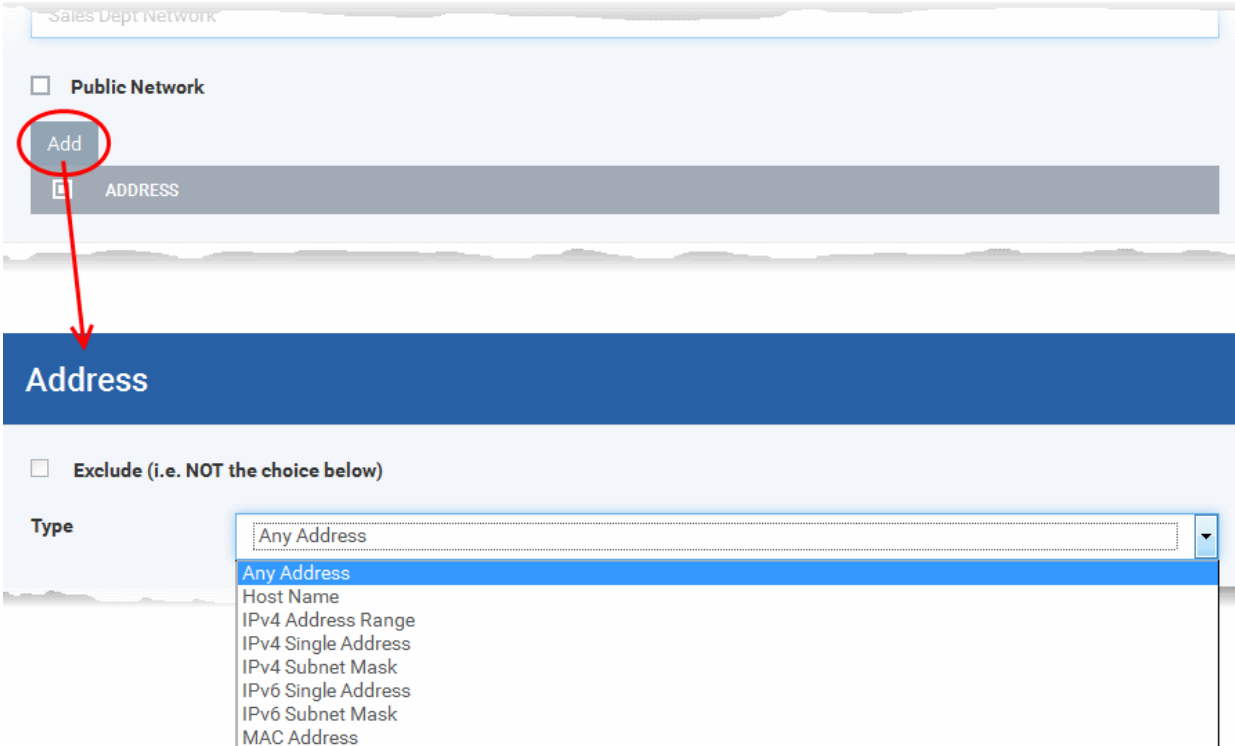
To define a new Network Zone

- Click the 'Add' button  at the top of the list.

The 'Network Zone' dialog will open.



- Enter a name for the new network zone in the 'Name' field.
- Select the checkbox 'Public Network' if you are defining a network zone for a network in a public place, for example, when you are connecting to a Wi-Fi network at an airport, restaurant etc., so that Comodo Firewall will optimize the configuration accordingly.
- Click Add to add the computers in the new network zone



The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below (*Default = Any Address*). The 'Exclude' check box will be enabled only if any other choice is selected from the drop-down box.

Address Types:

- 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

Source Address Destination Address Source Port Destination Port

Exclude (i.e. NOT the choice below)

Type


Network Zone

Network Zone

Loopback Zone

Sales Dept. Computers

OK Cancel

To edit a network zone, click the 'Edit' icon  beside the network zone name. The 'Network Zone' dialog will appear populated with the name and the addresses of the network zone. Edit the details as required. The process is similar to **defining a new network zone** as explained above.

Blocked Zones

A computer network enables users to share information and devices between computers and other users within the network. There are certain networks that you'll want to 'trust' and grant access to - for example your work network. Conversely, there may be other networks that you do not trust and want to restrict communication with - or even block entirely.

The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not wish to trust and the computers applied with this profile will be blocked access to them.

The 'Blocked Zones' tab allows you to view the list of blocked network zones and add new blocked zones.

The screenshot displays the 'Firewall' configuration page in Comodo Device Manager. At the top, there are tabs for 'General', 'File Rating', and 'Firewall'. Below these, there are sub-tabs for 'Firewall Settings', 'Application Rules', 'Global Rules', 'Rulesets', 'Network Zones', and 'Portsets'. The 'Network Zones' sub-tab is selected. The main content area includes a 'Firewall' header with 'Save' and 'Delete' buttons. Below this, there are two checkboxes: 'Enable automatic detection of private networks' and 'Show popup alerts'. A 'Location treatment:' dropdown menu is set to 'Work'. At the bottom, there are two tabs: 'Network Zones' and 'Blocked Zones'. The 'Blocked Zones' tab is active, showing a list of zones with a 'ZONE NAME' entry. There are 'Add' and 'Add from Network Zone' buttons above the list.

The 'Blocked Zones' tab displays a list of zones that are currently blocked and allows you to:

- **Deny access to an existing network zone**
- **Deny access to a network by manually defining a new blocked zone**

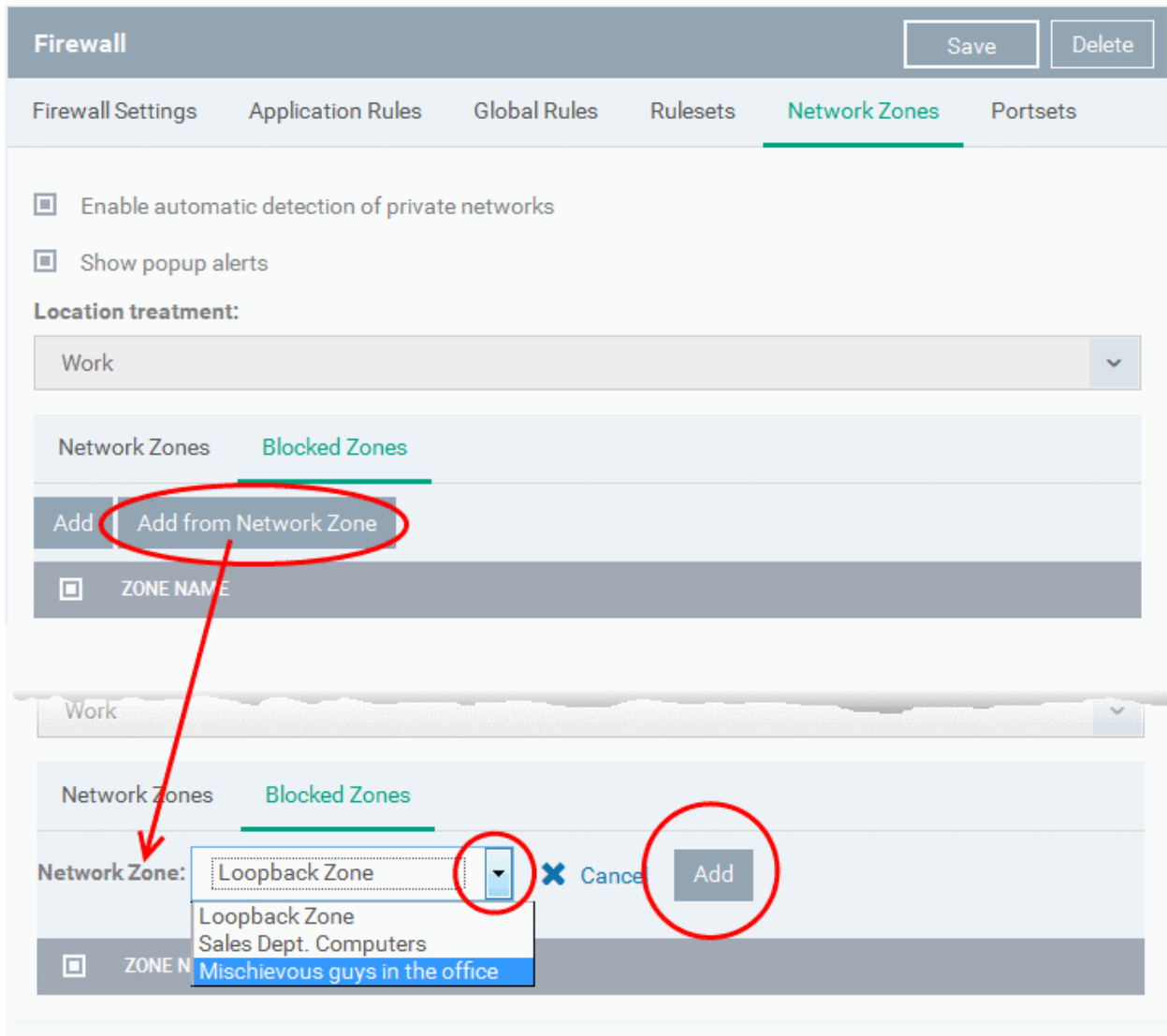
Note 1: You must create a zone before you can block it. There are two ways to do this;

1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *existing* zones from this interface (e.g. to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

To deny access to an existing network zone

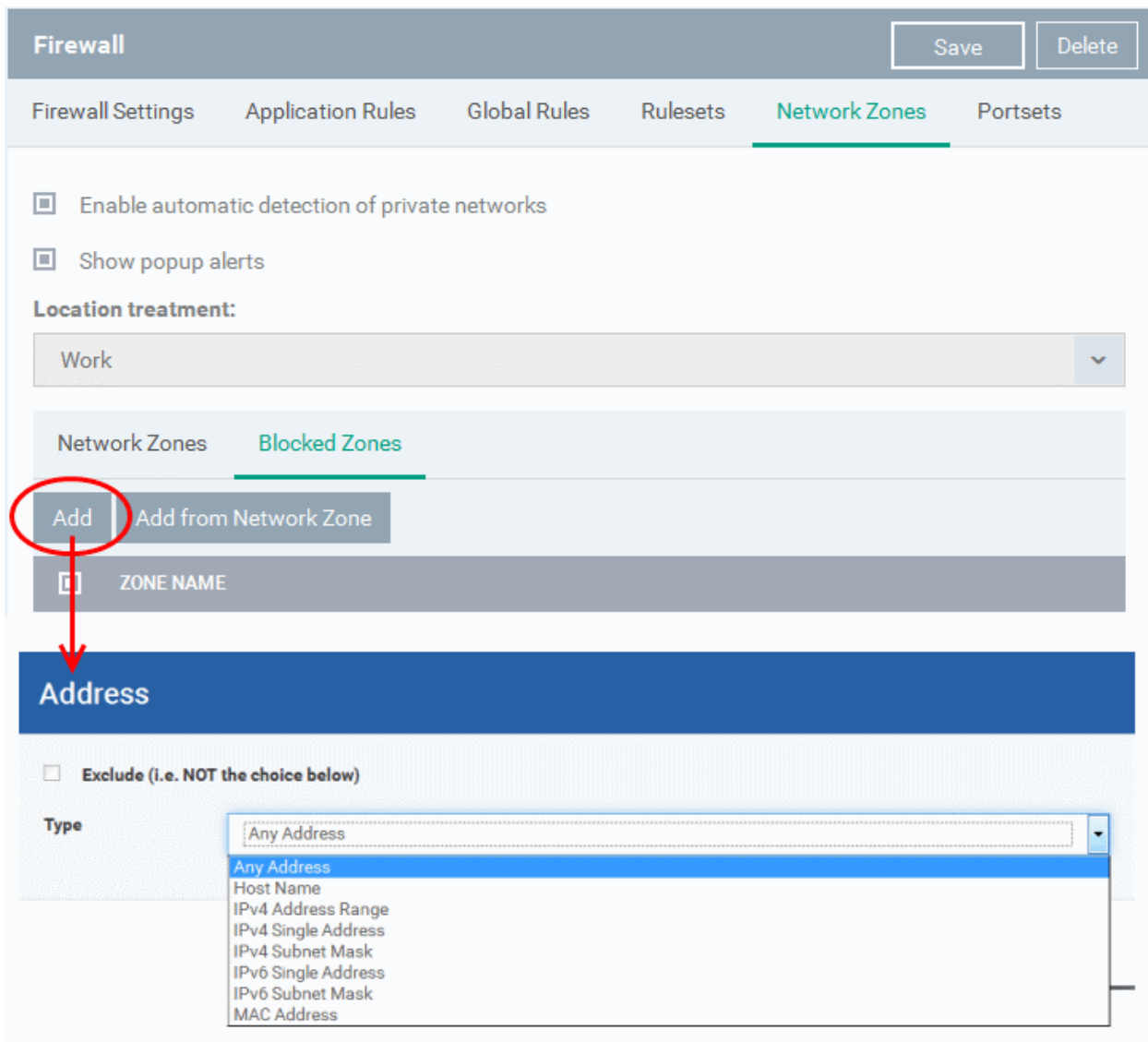
- Click 'Add from Network Zone' button from the top
- Choose the particular zone you wish to block from the 'Network Zone' drop-down.



- Click 'Add'
- Repeat the process to add more blocked network zones for the profile

To deny access to a network by manually defining a new blocked zone

- Click the 'Add' button from the top.



- Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

Address Types:

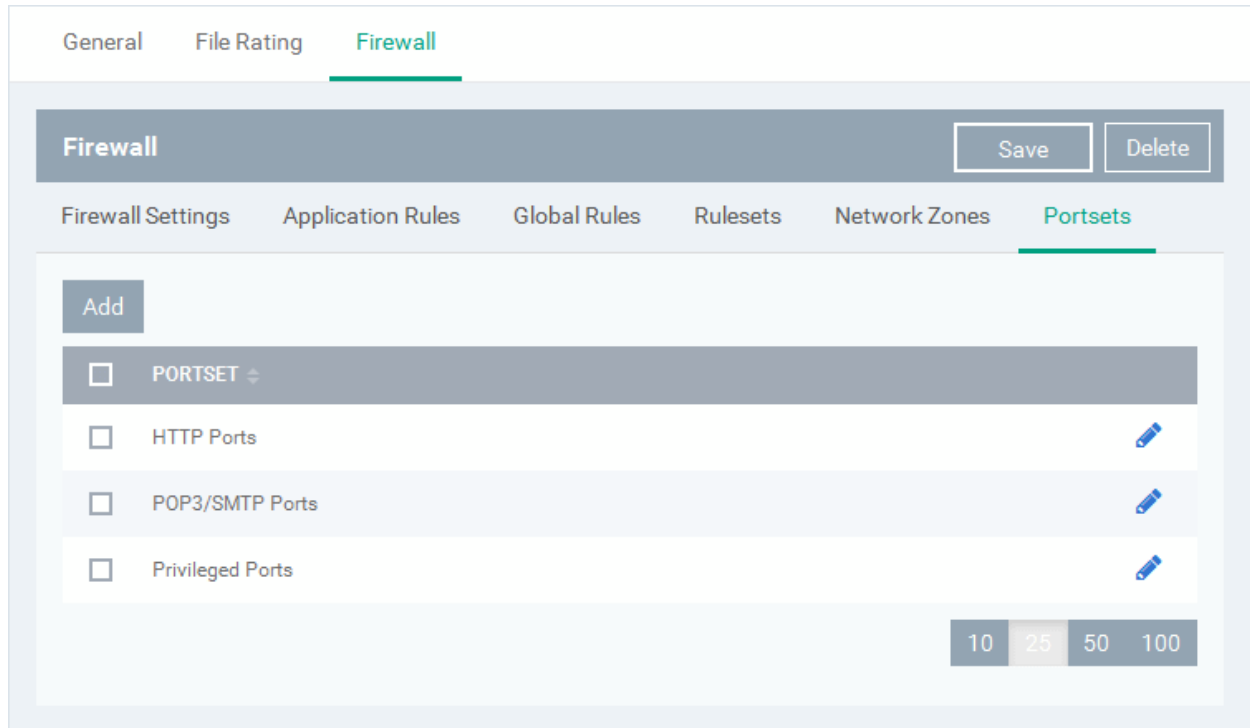
- i. Any Address - Will block connections from all IP addresses (0.0.0.0- 255.255.255.255)
 - ii. Host Name- Enter a named host which denotes an address on your network.
 - iii. IPv4 Range - Will block access to the IPv4 addresses you specify in the 'Start Range' and 'End Range' text boxes.
 - iv. IPv4 Single Address - Block access to a single address - e.g. 192.168.200.113.
 - v. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to block.
 - vi. IPv6 Single Address -Block access to a single address - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
 - vii. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
 - viii. MAC Address - Block access to a specific MAC address.
2. Select the address to be blocked and click OK


The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

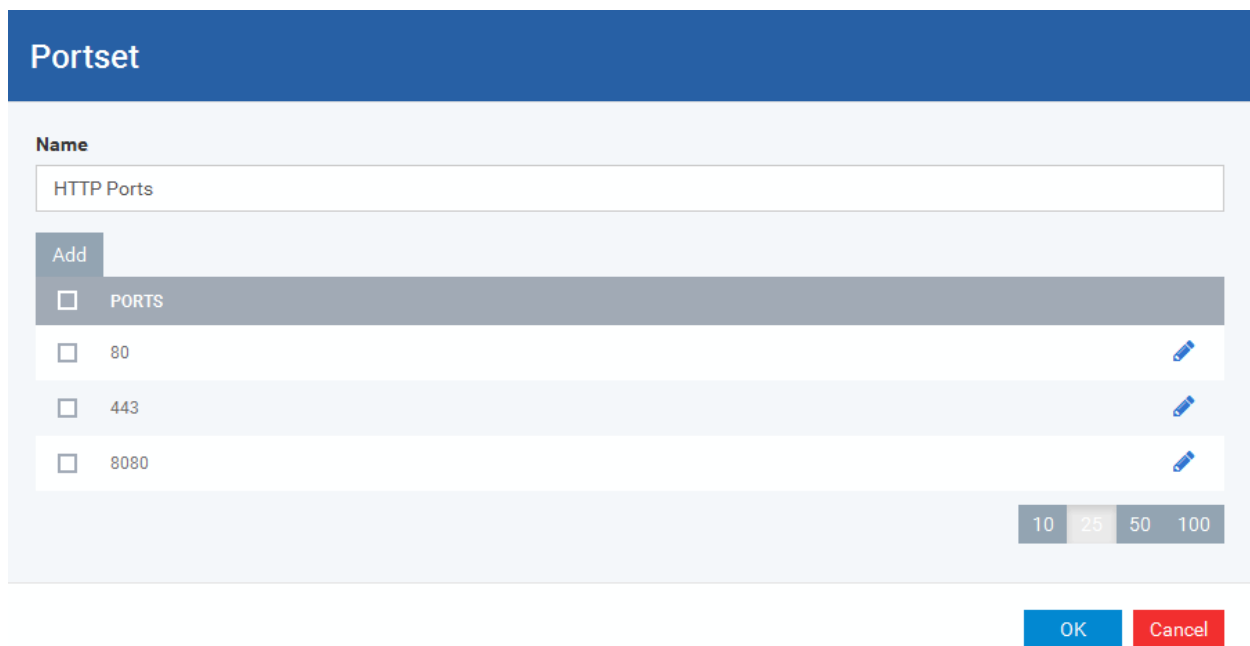
3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

Portsets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple **Application Rules** and **Global Rules**. The 'Port Sets' panel under the 'Firewall' tab allows you to view and manage pre-defined port sets and to add new port sets for the profile. The name of the port set is listed above the actual port numbers that belong to that set.



The panel lists all portsets that are defined for the profile. Clicking the 'Edit' icon  beside a name reveals the ports included in the set.



CDM ships with three default portsets:

- **HTTP Ports:** 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.

- **POP3/SMTP Ports:** 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
- **Privileged Ports:** 0-1023. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

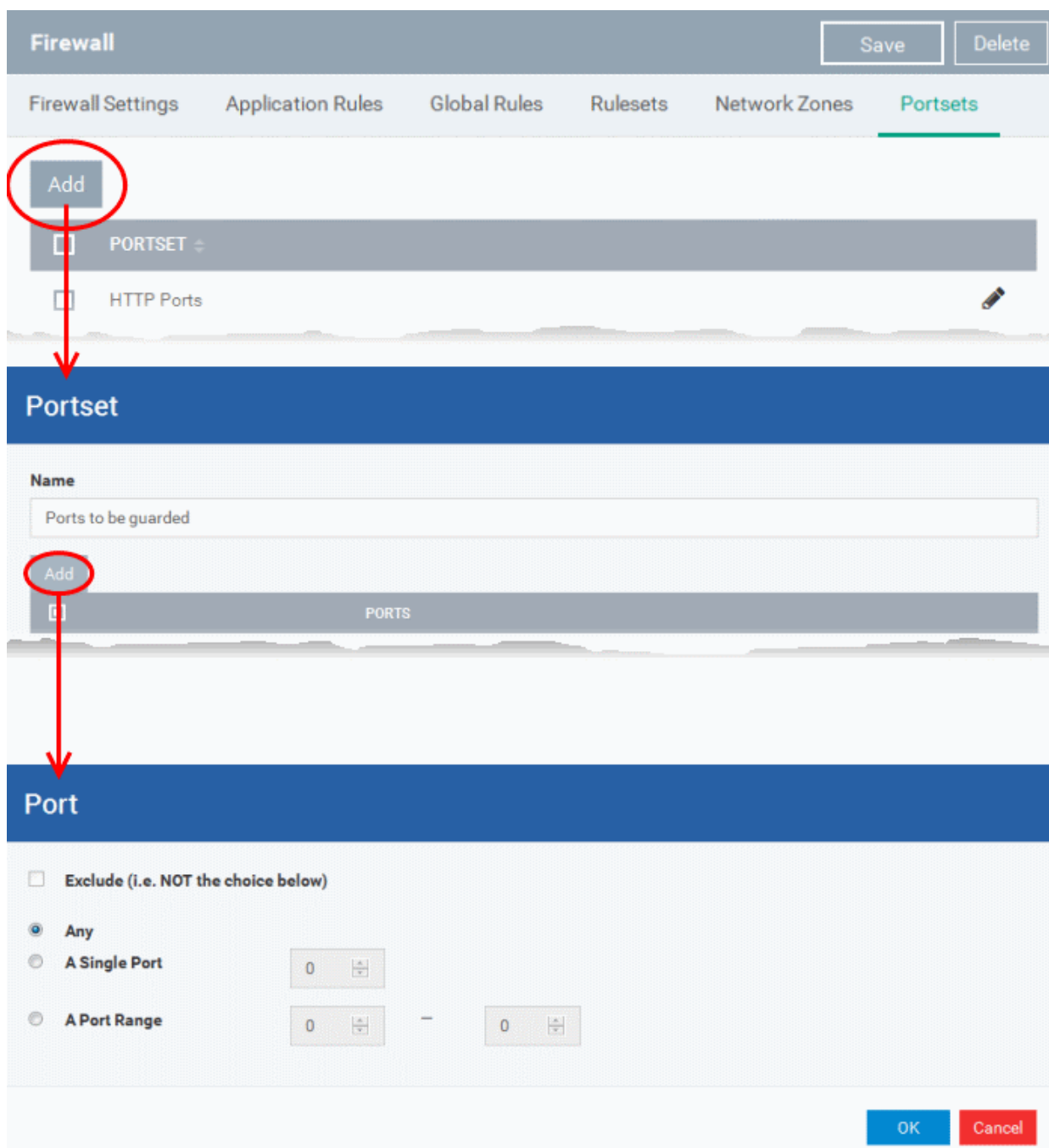
Defining a new Port Set

You can create new portsets and allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.

To add a new portset

- Click the 'Add' button from the top.

The 'Portset' dialog will open.



- Enter a name for the new portset in the 'Name' field.
- To add ports to the new portset, click the 'Add' button above the list of ports.
- Specify the ports to be included in the new portset:
 - **Any** - to choose all ports;
 - **A single port** - Define the port number in the combo box beside;
 - **A port range** - Enter the start and end port numbers in the respective combo boxes.
 - **Exclude** (i.e. NOT the choice below): The opposite of what you specify is applicable.
- Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
- Click 'OK' in the 'Portset' dialog to create the new portset.

Once created, a Portset can be:

- Quickly called as 'A Set of Ports' when **creating or modifying a Firewall Ruleset**

Firewall Rule

Action

Block

Log as firewall event if this rule is fired

Protocol

TCP

Direction

Out

Description

Allow Outgoing HTTP Requests

Source Address Destination Address **Source Port** Destination Port

Exclude (i.e. NOT the choice below)

Type

A Set of Ports

Port Set

HTTP Ports
POP3/SMTP Ports
Privileged Ports
Ports to be guarded

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 save 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.

6.1.3.1.4. Sandbox Settings

The CES installation at the managed computers can be configured to automatically run files that have a trust status of 'Unknown' in the sandbox. Files running in the sandbox are isolated from the rest of the computer and the data stored in it, to prevent them causing damage.

The Sandbox Settings interface allows you to configure the overall behavior of Sandbox component of CES installed at the endpoints and to create and manage auto-sandbox rules that define which types of files are to be auto-sandboxed and their restriction levels.

- Run with restricted access to operating system resources
- Run completely isolated from your operating system and files on your computer
- Completely block from running
- Allow to run outside the sandbox environment without restriction

For more information about defining rules, refer to the section [Auto-Sandbox Rules](#).

The Sandbox creates a new folder called 'Shared Space' at 'C:/Program Data/Shared Space' to share files between sandboxed applications the real file system in the computer. Applications running inside the sandbox will be allowed to store their data in the shared space for future sessions. This data can also be accessed by non-sandboxed applications.

To configure Sandbox settings

- Choose 'Sandbox' from the 'Add' drop-down

The settings screen for Sandbox will be displayed.

Finance Dept Computers

Sandbox Save

Settings Rules

Enable Auto-Sandbox
This option protects your computer against unknown malware by auto-sandboxing and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

Virtualize access to the specified files/folders Exclusions

Virtualize access to the specified registry keys/values Exclusions

Enable automatic startup for services installed in the Sandbox

Show highlight frame for virtualized programs

Detect programs witch require elevated privileges e.g. installers or updates

Show privilege elevations alerts Run Isolated

It contains two tabs.

- [Sandbox Settings](#)
- [Auto-Sandbox Rules](#)

Sandbox Settings

The 'Settings' pane under the 'Sandbox' tab allows you to configure the parameters that determine how proactive the Sandbox

should be and which types of files it should check.

Sandbox
Save

Settings Rules

Enable Auto-Sandbox
This option protects your computer against unknown malware by auto-sandboxing and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

Virtualize access to the specified files/folders [Exclusions](#)

Virtualize access to the specified registry keys/values [Exclusions](#)

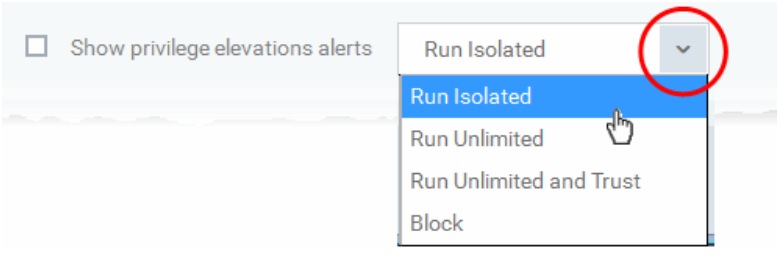
Enable automatic startup for services installed in the Sandbox

Show highlight frame for virtualized programs

Detect programs witch require elevated privileges e.g. installers or updates

Show privilege elevations alerts Run Isolated ▼

Sandbox Settings - Table of Parameters	
Form Element	Description
Enable Auto-Sandbox	Allows you to enable or disable Auto-Sandbox at the endpoint. If enabled, the CES at the endpoint will automatically run applications inside the sandbox, as per the rules defined. For more details on creating the rules, refer to the section ' Configuring Rules for Auto-Sandbox '.
Shared Space Settings	
'Shared Space' is a dedicated area at each endpoint that sandboxed applications are permitted to write to and which can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This is located by default at 'C:/Program Data/Shared Space'.	
Virtualize access to the specified files/folders	<p>Sandboxed applications can access folders and files on the 'real' system but cannot save any changes to them. However, you can define exclusions to this rule.</p> <p>On selecting this option, sandboxed applications cannot save any data to any of the files/folders in the real computer system. If you want to add files and folders in the real computer system as exclusions, that could be accessed by sandboxed applications leave this option unselected and add the files/folders to be excluded.</p> <p>Refer to the explanation of defining exclusions for Files/Folders, below this table.</p>
Virtualize access to the specified registry keys/values	<p>Sandboxed applications can access Windows Registry Keys and Values on the 'real' system but cannot save any changes to them. However, you can define exclusions to this rule.</p> <p>On selecting this option, sandboxed applications cannot save any data to any of the Registry Keys and Values in the real computer system. If you want to add Keys and Values as exclusions, that could be accessed by sandboxed applications, leave this option unselected and add the Keys/Values to be</p>

Sandbox Settings - Table of Parameters	
	<p>excluded.</p> <p>Refer to the explanation of defining exclusions for registry keys/values, below this table.</p>
Other Settings	
Enable automatic startup for services installed in the Sandbox	By default, CES installation at the endpoint does not permit sandboxed services to run at Windows startup. Select this check-box to allow them to do so at the endpoints applied with the profile.
Show highlight frame for virtualized programs	If enabled, CES will display a green border around the windows of programs that are running inside the sandbox at the endpoint.
Detect programs which require elevated privileges e.g. installers or updates	If enabled, the Sandbox displays alerts when an installer or updater requires administrator or elevated privileges to run at the endpoint. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry.
Show privilege elevation alerts	<p>If enabled, CES displays alerts when a new or unrecognized program, application or executable requires administrator or elevated privileges to run at the endpoint for the end-user to respond. (Default=Disabled)</p> <p>If you do not want the alerts to be displayed at the endpoint, leave this option un-selected and choose the action to be taken on those unrecognized programs from the drop-down beside it.</p> 

To define exclusions for files and folders

- Disable the 'Virtualize access to the specified files/folders' option and then click on the link 'Exclusions'.

File / Folders
Close

Add ▾

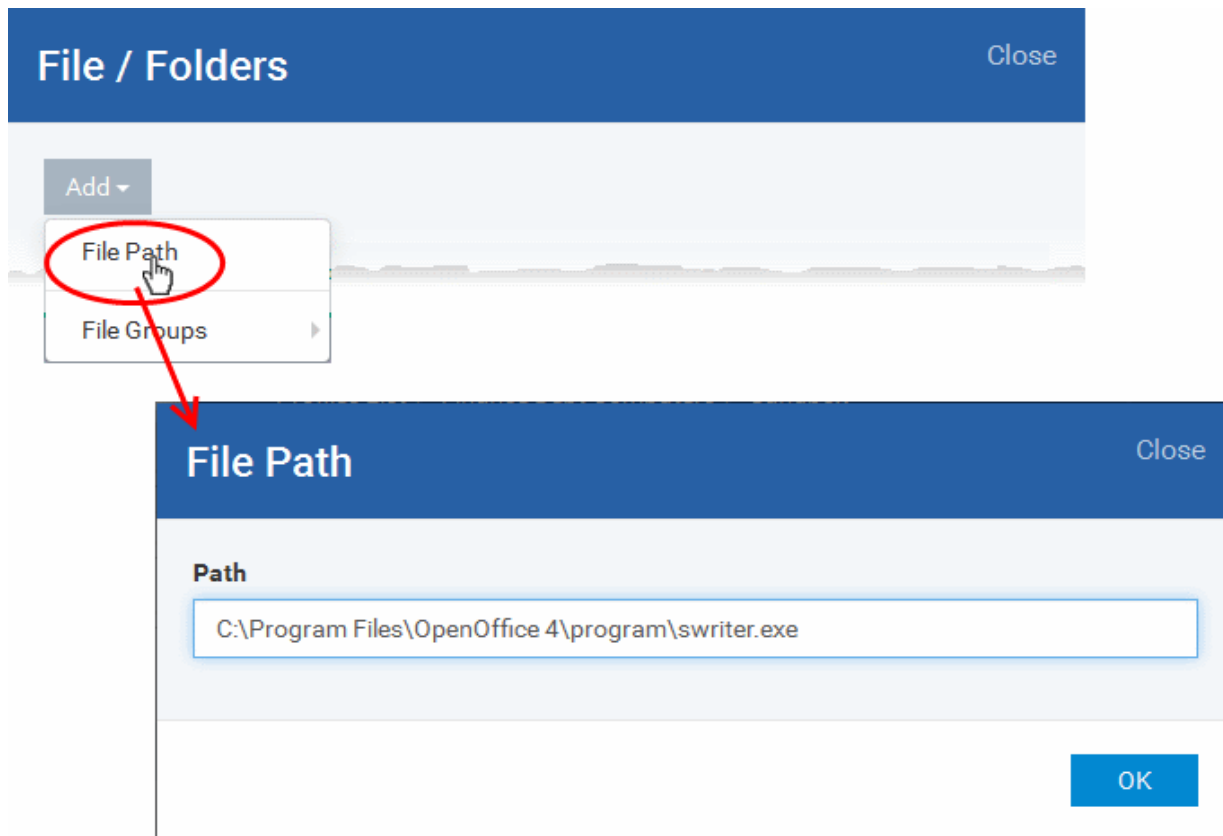
Exclusion Paths
Exclusion Groups

PATH	ACTIONS

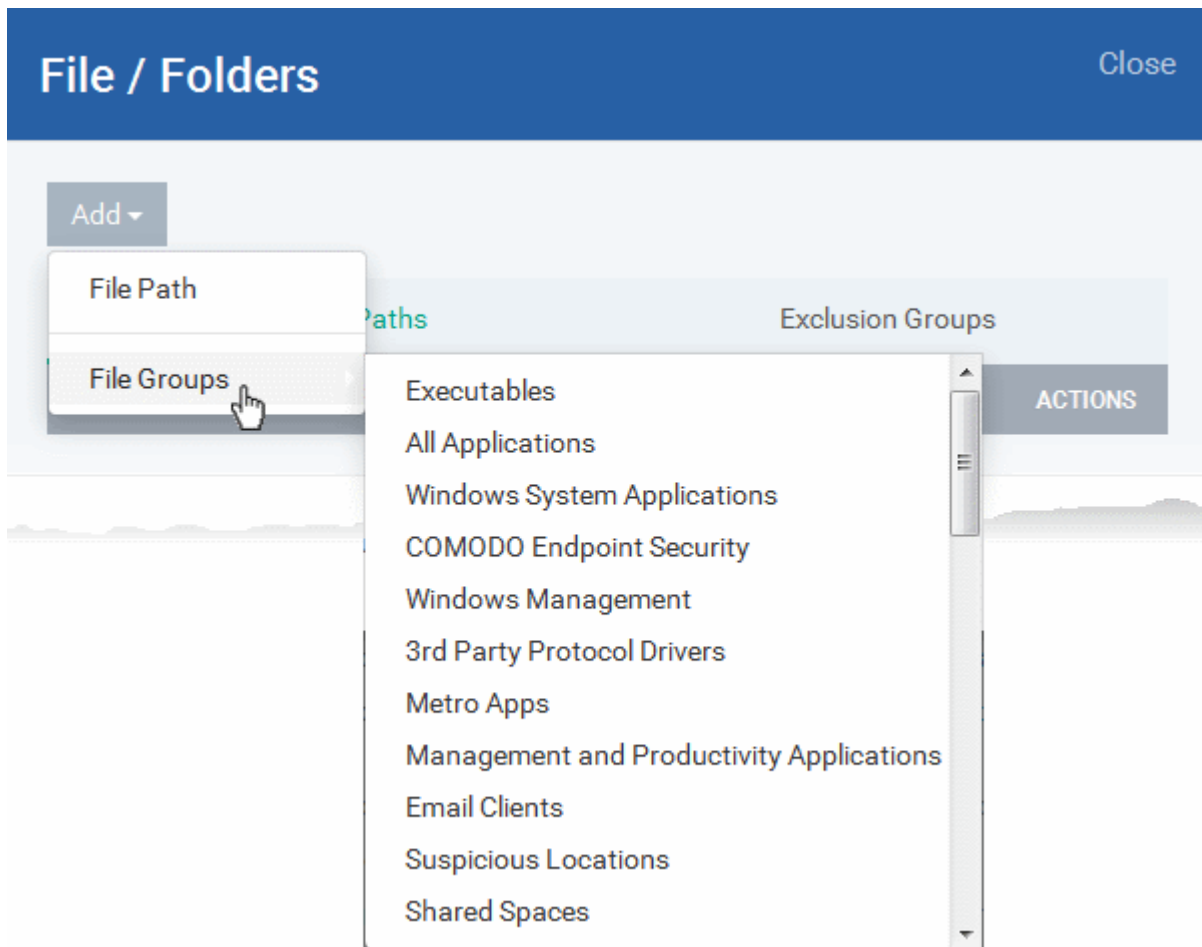
You can add/edit File Groups [here](#)
OK

- The 'Files/Folders' 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. CDM ships with a set of file groups. The administrator can create custom file groups from the Settings > 'Global Variables' interface. Refer to the portion explaining '**File Groups**' under **Settings > Global Variables**.
- To add a file path, choose File Path from the 'Add' Drop-down



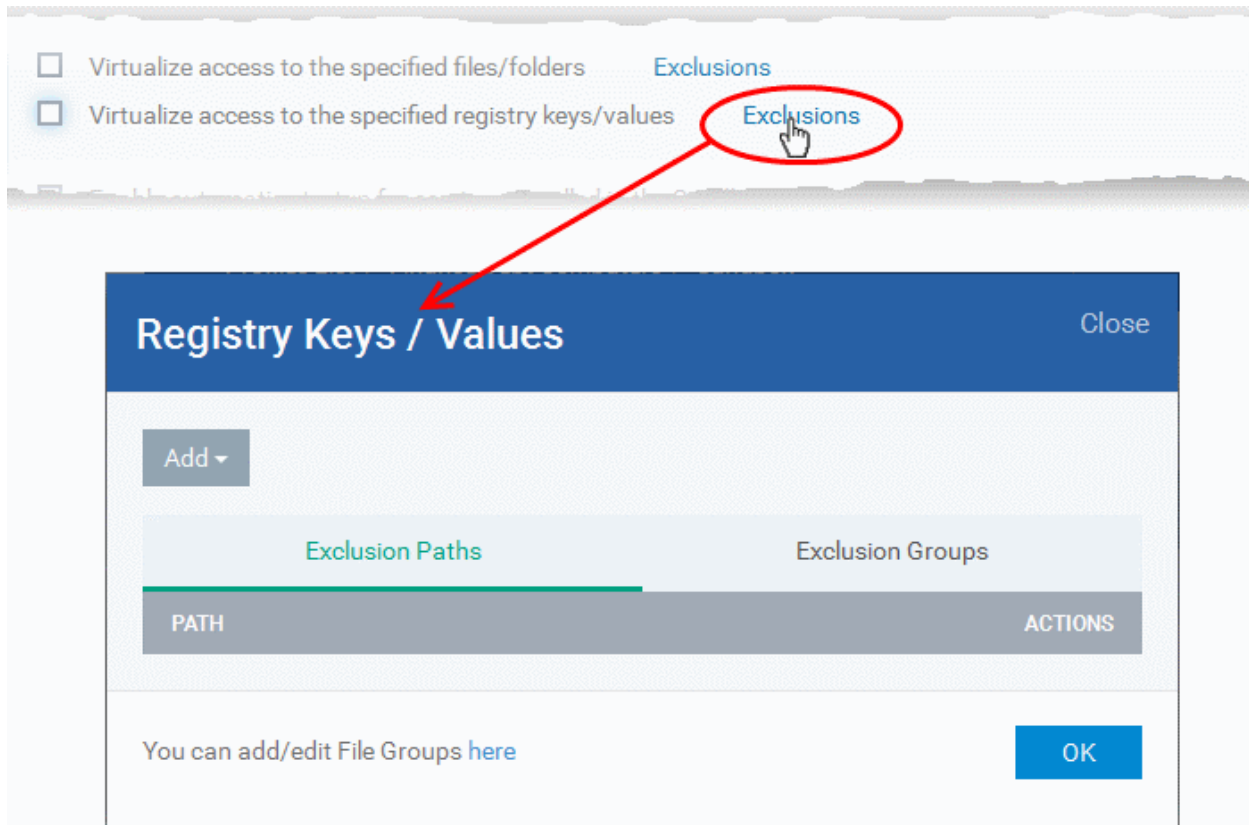
- Enter the storage/installation path of the file to be added to the exclusions list
- To add a File Group to exclusions, choose File Groups from the Add drop-down and choose the File Group.



- Click 'OK' to save your settings.
- You can edit or remove the exclusions using the respective buttons in the 'Action' column in the File/Folders interface.

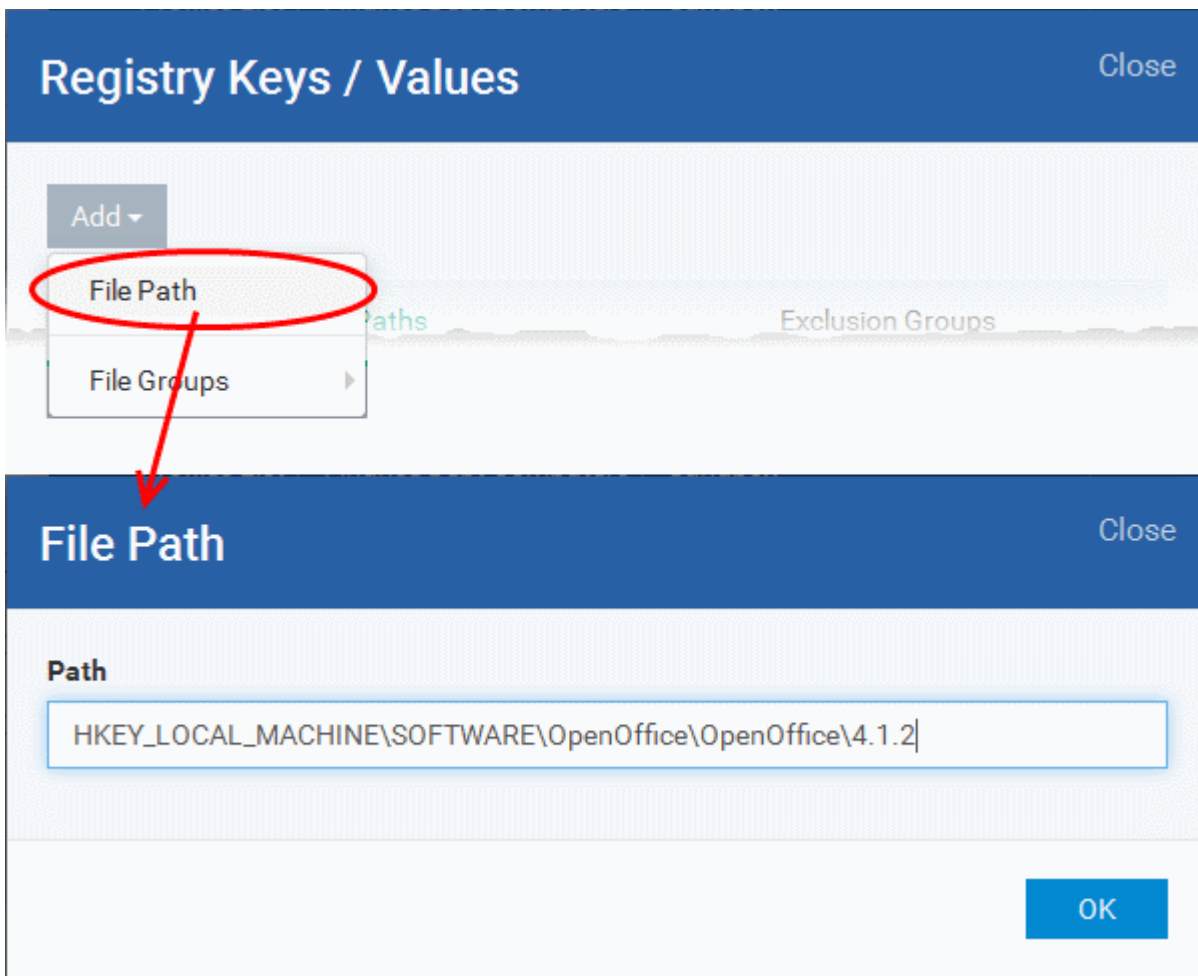
To define exclusions for specific Registry keys and values

- Disable the 'Virtualize access to the specified registry keys/values' then click on the link 'Exclusions'.

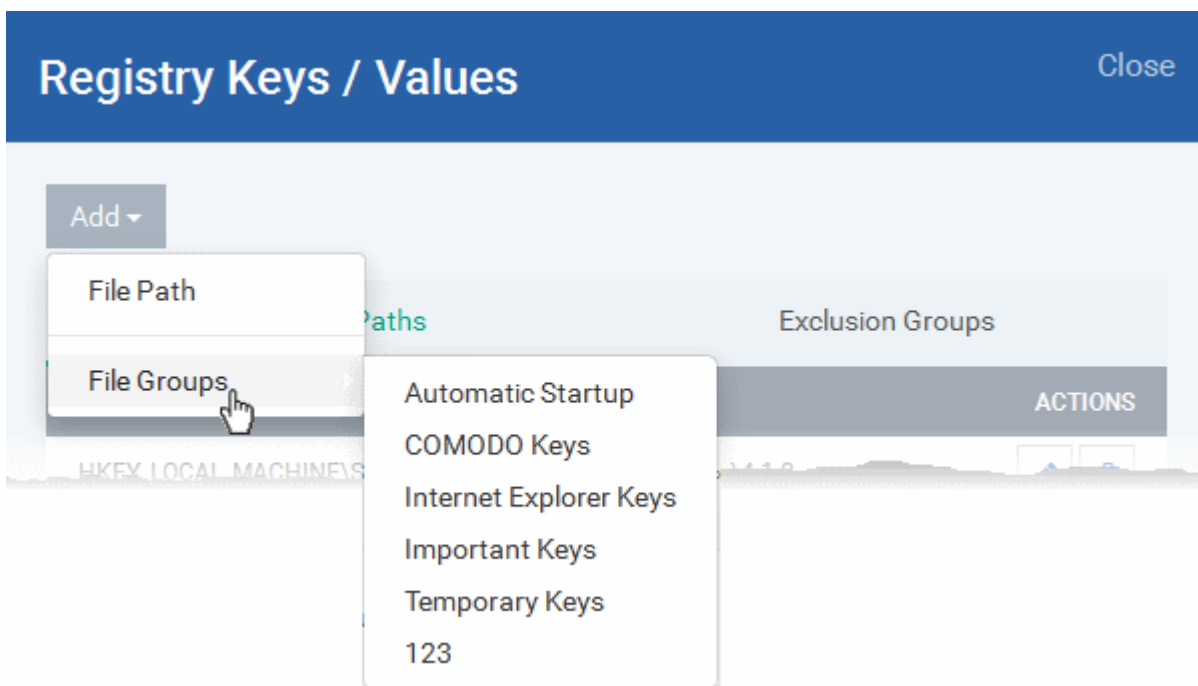


The 'Registry Keys / Values' dialog will appear with a list of defined exclusions under two tabs:

- **Exclusion Paths** - The Registry Keys /Values that are added to the list
- **Exclusion 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. CDM ships with a set of registry groups. The administrator can create custom registry groups from the Settings > 'Global Variables' interface. Refer to the portion explaining '**Registry Groups**' under **Settings > Global Variables**.
- 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 and click 'OK'
- To add a pre-defined 'Registry Group' to exclusions, choose 'Registry Groups' from the 'Add' drop-down and choose the Group.



- Click 'OK' to save your settings.

You can edit or remove the exclusions using the respective buttons in the 'Action' column in the Registry Keys / Values interface.

- Click the 'Save' button.

Configuring Rules for Auto-Sandbox

The Sandbox rules determine whether a program should be allowed to run with full privileges, ignored, run restricted or run in fully virtualized environment. For easy identification, CES will show a green border around programs that are running in the sandbox at the endpoints.

The table in the Rules screen displays the list of rules configured for the profile. Rules at the top of the table have a higher priority than those at the bottom and are applied first. In the event of a conflict between rules, the setting in the rule nearer to the top of the table will be applied.



Sandbox Rules - Column Descriptions	
Column Heading	Description
Action	Displays the operation that the sandbox should perform on the target files if the rule is triggered.
Target	The files, file groups or specified locations on which the rule will be executed.
Reputation	The trust status of the files to which the rule should apply. The possible values are: <ul style="list-style-type: none"> • 'Any' • 'Malware' • 'Trusted' • 'Unrecognized'.
Actions	Displays whether the rule is enabled or disabled. Click on 'Enable/Disabled' to toggle between the two states. The drop-down allows you to edit the rule or delete it. <div style="text-align: center;"> </div>

Sorting and filtering options

- Clicking on 'Action', 'Target' and 'Reputation' column headers will sort the rules in ascending/descending order

You can add new rules for automatically running specified programs inside the sandbox at the endpoints to which the profile is applied.

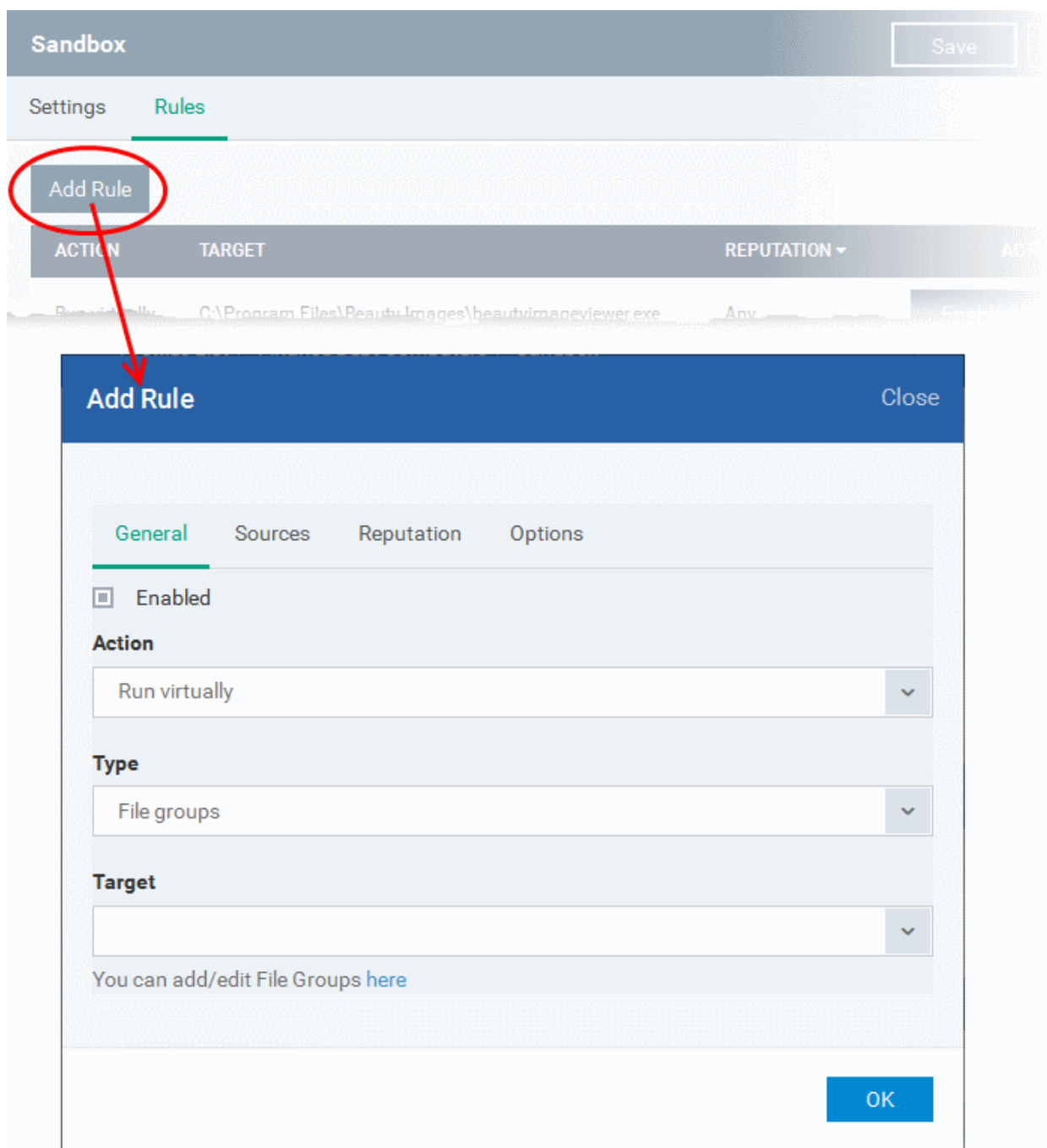
An Auto-sandbox rule can be created for:

- An individual target application at a specific endpoint by specifying the file path of the executable file;
- An individual target application at several endpoints by specifying its common file path or the Hash value of the executable file;
- All applications in a File Group.

The target(s) can be filtered by specifying 'Source', 'Reputation' and 'Options'. They are, however, optional, so the administrator can create a very simple rule to run an application in the sandbox just by specifying the action and the target application.

To add a new rule

- Click the 'Add Rule' button  from the 'Sandbox' interface.



The screenshot shows the 'Sandbox' interface with the 'Rules' tab selected. A red circle highlights the 'Add Rule' button, and a red arrow points to the 'Add Rule' dialog box. The dialog box has a title bar 'Add Rule' and a 'Close' button. It contains the following fields:

- Enabled
- Action**: Run virtually (dropdown)
- Type**: File groups (dropdown)
- Target**: (empty dropdown)

Below the 'Target' field, there is a link: "You can add/edit File Groups [here](#)". At the bottom right of the dialog box is an 'OK' button.

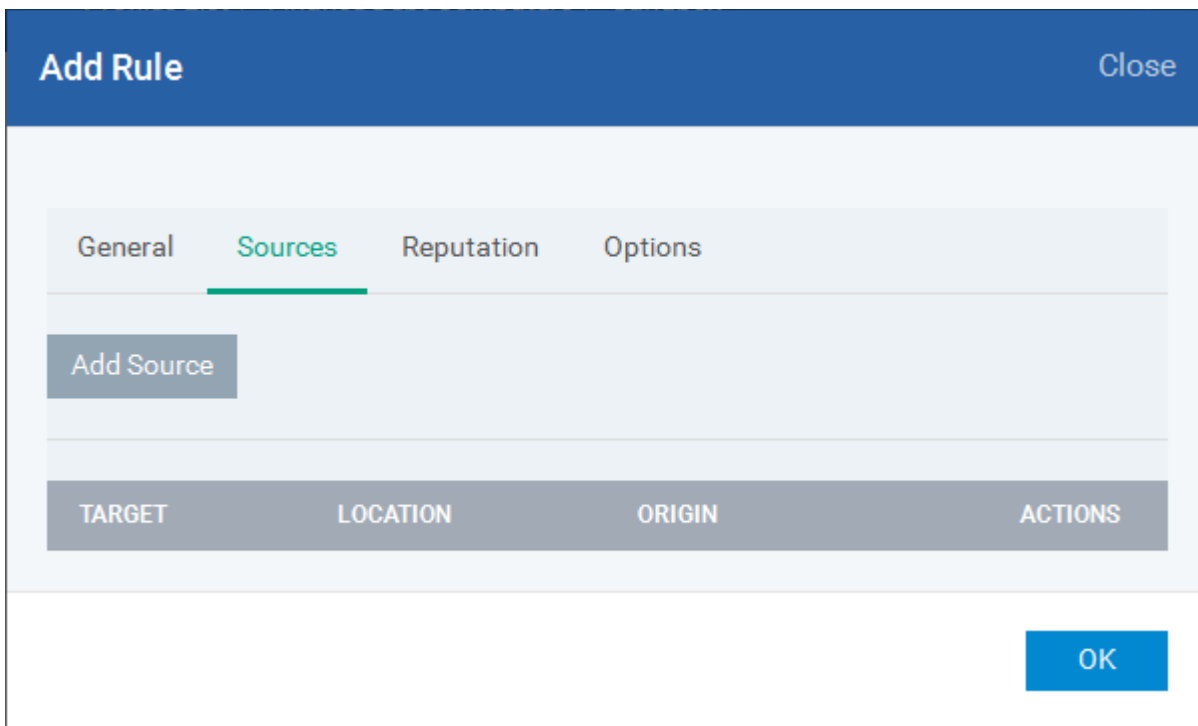
The 'Add Rule' dialog will displayed.

- Click the 'General' tab in the 'Add Rule' dialog

'Add Rule' dialog - General tab - Table of Parameters	
Form Element	Description
Enabled	Allows you to enable or disable the rule.
Action	<p>The 'Action' drop-down allows you to choose whether or not the sandbox has to allow the application to run and the restriction level to be applied. The restriction level determines the privileges to be assigned to the auto-sandboxed application to access the other software and hardware resources of the endpoint computer. The options available are:</p> <ul style="list-style-type: none"> • Run Restricted - The application is allowed to run and access the Operating System files and resources as per the Restriction Level set under the 'Restriction Level' drop-down. • 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 sandboxed and allowed to run with all privileges.
Type	<p>Allows you to select the target type from the drop-down. The options available are:</p> <ul style="list-style-type: none"> • File Groups • File Path • File Hash <p>Depending on the option selected here, the next field, 'Target' will allow you to select/enter the target details.</p>
Target	<p>Select the target application to which the auto-sandbox rule is to be applied.</p> <ul style="list-style-type: none"> • If 'File Groups' is selected in 'Type', the predefined file group will be available for selection from the 'Target' drop-down. <p>File Groups - File groups are handy, predefined groupings of one or more file types. Choosing File Groups allows the administrator to add a category of pre-set files or folders. For example, selecting 'Executables' would include all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such predefined categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc. CDM ships with a set of File Groups. The Administrator can also create custom File Groups from the 'Settings' > 'Global Variables' interface. Refer to the portion explaining 'File Groups' under Settings > Global Variables.</p> <ul style="list-style-type: none"> • If 'File Path' is selected in 'Type', enter the path of the file in the 'Target' field. <p>File Path - Allows you to add executable files as the target by entering the entire common path.</p> <ul style="list-style-type: none"> • If 'File Hash' is selected in 'Type', enter the SHA1 hash value of the file in the 'Target' field. <p>File Hash - Allows you to add a program as a target by specifying the SHA1 Hash value of the executable file. CES 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-sandboxed as per the rule.</p>

The next step is to define the source for the rule.

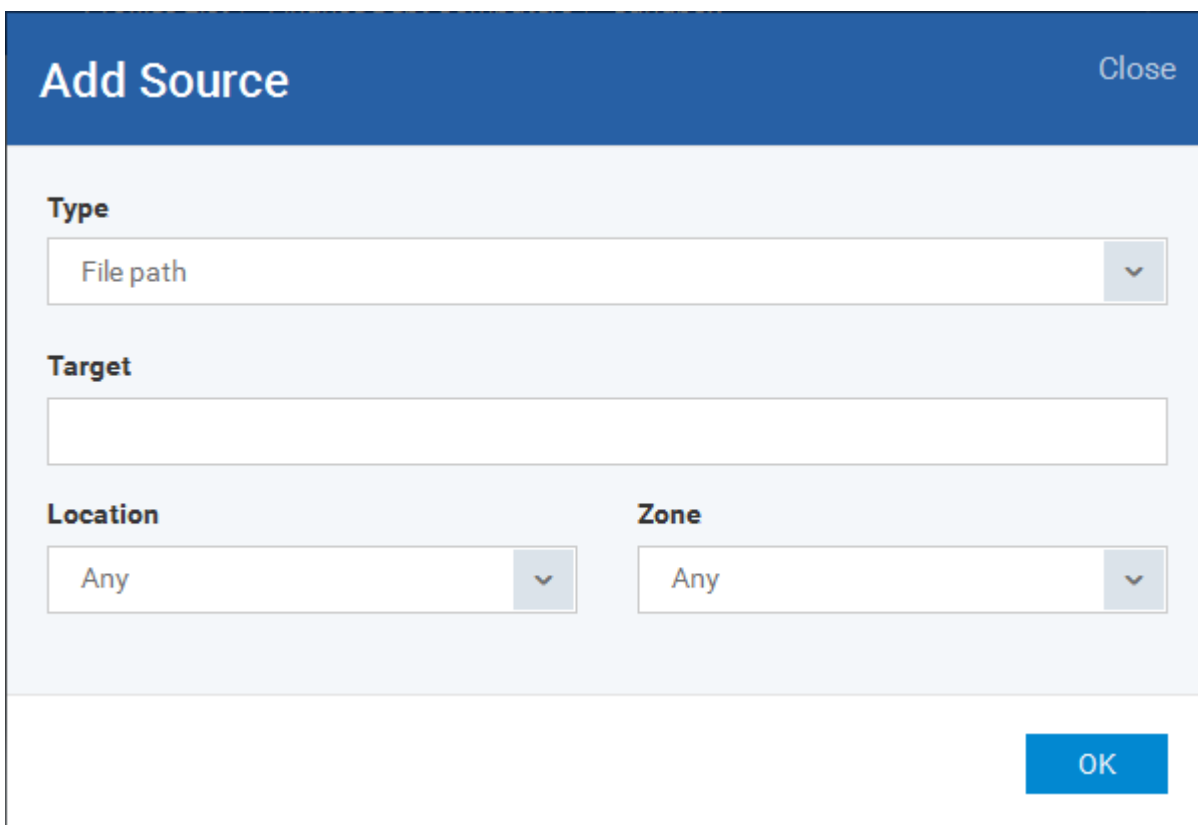
- Click the 'Sources' tab in the 'Add Rule' dialog



If you include a number of items for a rule but want the rule to be applied only for items from certain sources, you can specify the sources by clicking the 'Add Source' button.

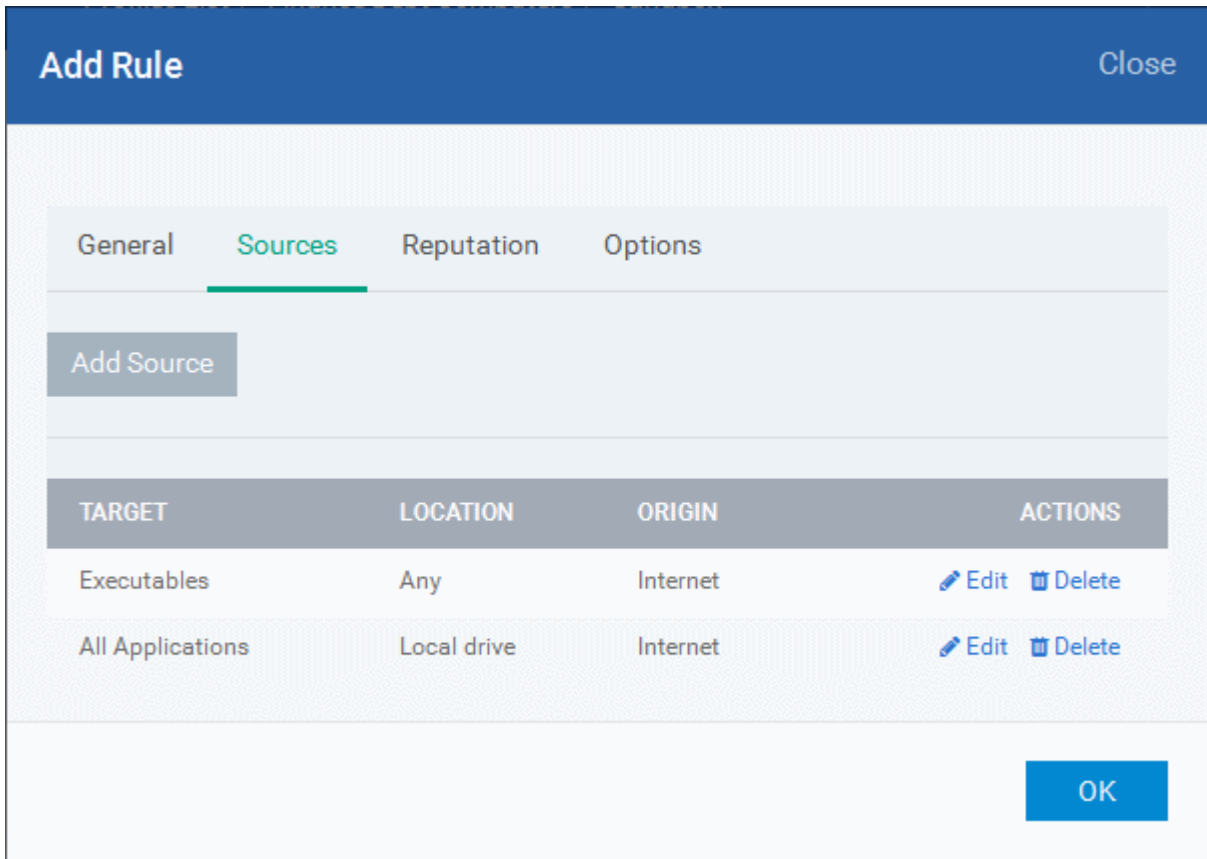
For example, if you include all executables in the 'Target' but want the rule to be applied only to executables that were downloaded from the Internet, then the filter can be applied in the 'Sources'. Another example is if you want to run unrecognized files from a network share, you have to create an ignore rule with All Applications as target and source located on network drives.

On clicking the 'Add Source' button, a new 'Add Source' dialog will be displayed.



'Add Source' dialog - Table of Parameters	
Form Element	Description
Type	<p>Allows you to select the target type from the drop-down. The options available are:</p> <ul style="list-style-type: none"> • File Groups • File Path • File Hash <p>Depending on the option selected here, the next field, 'Target' will allow you to select/enter the target details.</p>
Target	<p>Choose the source file that has created the application set as target in the Target field. The process of adding the source file is similar to adding a file for target. Refer to the description above for more details.</p> <ul style="list-style-type: none"> • For example, if the file was downloaded from Internet using a web browser, you can choose the File Group 'Web Browsers'. • If you are unsure of the source, choose 'All Applications' file group.
Location	<p>Choose the Location in which the application is stored from the drop-down. The options available are:</p> <ul style="list-style-type: none"> • Any - The rule will apply to the target application located on the local drive or on a removable drive of the endpoint or on a network drive. • Local Drive - The rule will apply only to the target application located on the local drive of the endpoint. • Removable Drive - The rule will apply only to the target application located on the removable drive connected to the endpoint. • Network Drive - The rule will apply only to the target application located on a network drive but executed at the endpoint.
Zone	<p>Choose the origin of the executable. The available options are:</p> <ul style="list-style-type: none"> • Any - The rule will apply to the target application downloaded, copied or moved from anywhere. • Internet - The rule will apply only to the target application downloaded from Internet. • Intranet - The rule will apply only to the target application downloaded from Intranet.

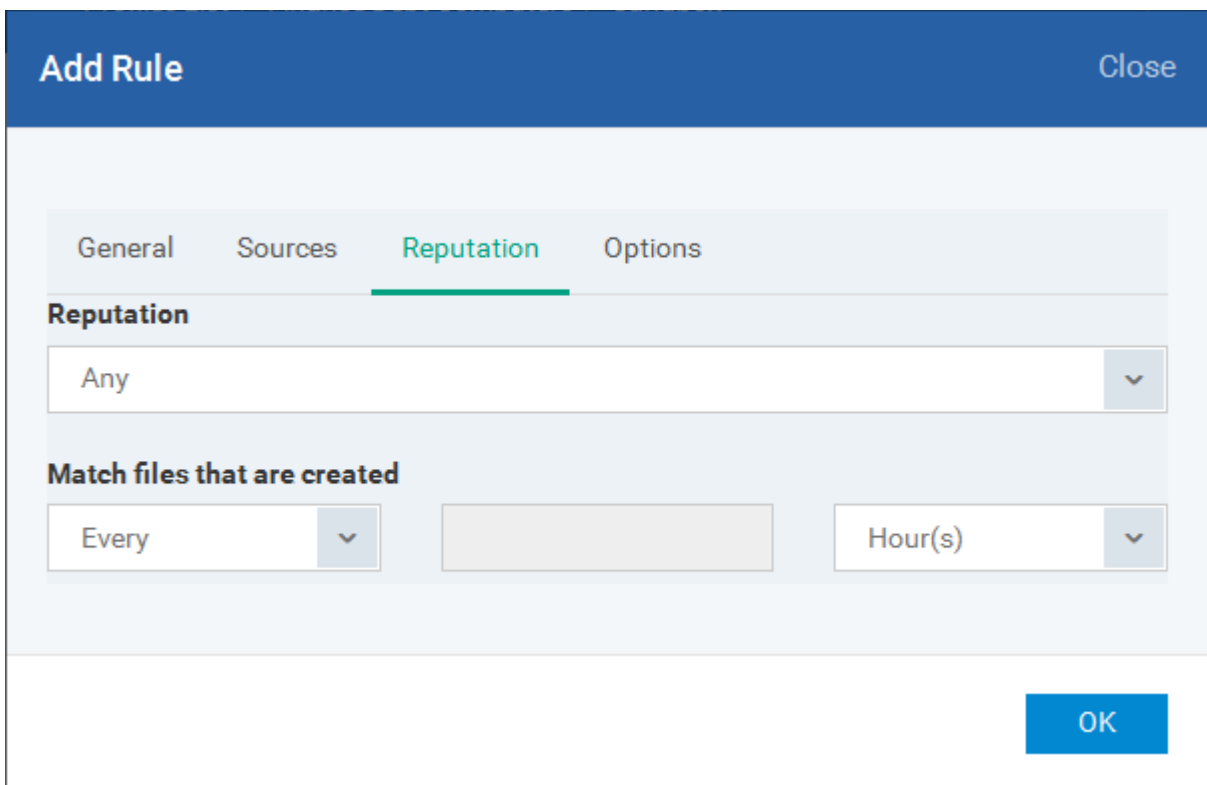
- Click 'OK'
- Repeat the process to add more sources. The source list will be displayed:



- Clicking on 'Target', 'Location' and 'Origin' column headers will sort the rules in ascending/descending order
- Click 'Edit' to change the source parameters
- Click 'Delete' to remove the source from the list

The next step is to define the reputation for the rule.

- Click the 'Reputation' tab in the 'Add Rule' dialog



'Add Rule' dialog - Reputation tab - Table of Parameters	
Form Element	Description
Reputation	<p>Allows you to narrow down the scope of applications to which the rule needs to be applied by choosing the File Rating from the 'Reputation' drop-down. The available options are:</p> <ul style="list-style-type: none"> • Any - Application of any file rating • Trusted - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files as configured under File Rating configuration of the profile. Refer to the section explaining File Rating configuration. • Unrecognized - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. • Malware - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions.
Match files that are created	<p>Allows you to narrow down the scope of applications to which the rule needs to be applied by specifying the age of the target files. The available options are:</p> <ul style="list-style-type: none"> • Every - Includes all the files that match the conditions set from the Target and Reputation fields. • More than - Includes the files whose age is more than the specified time period. Specify the time period using the next two drop-downs. • Less than - Includes the files whose age is less than the specified time period. Specify the time period using the next two drop-downs

The next step is to define the options for the rule.

- Click the 'Options' tab in the 'Add Rule' dialog

Add Rule Close

General Sources Reputation **Options**

Log when this action is performed

Set restriction level to Partially limited v

Limit maximum memory consumption to (MB) MB

Limit program execution time to (sec) Secs

OK

'Add Rule' dialog - Options tab - Table of Parameters	
Form Element	Description
Log when this action is performed	Allows you choose whether or not to add the event to the CES logs at the endpoint, whenever this rule is triggered.
Set Restriction Level to	<p>You can choose whether or not the restriction level is to be applied to the programs run inside the sandbox by selecting or deselecting this option.</p> <p>This option is available only if you have chosen 'Run restricted' or 'Run virtually' as the 'Action' for the rule. For 'Run Restricted' action, the option is selected by default. If this option is selected, you should choose the restriction level to be applied from the drop-down. The available options are:</p> <ul style="list-style-type: none"> • Partially Limited - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. • Limited - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges. • Restricted - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting. • Untrusted - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
Limit maximum memory consumption to (MB)	<p>Allows you to choose whether or not you wish to set an upper limit for the size of system memory that the processes run by the target application can use.</p> <p>This option is available only if you have chosen 'Run restricted' or 'Run virtually' as the 'Action' for the rule.</p> <ul style="list-style-type: none"> • If selected, enter the upper limit of size of system memory (in MB) that the process(es) can use.
Limit program execution time to (secs)	<p>Allows you to choose whether or not you wish to specify an upper limit for the time for which the target application can continuously be run.</p> <p>This option is available only if you have chosen 'Run restricted' or 'Run virtually' as the 'Action' for the rule.</p> <ul style="list-style-type: none"> • Enter the maximum time in seconds for which the program can be allowed to run. On lapse of the time, the program will be automatically terminated.

- Click 'OK' to save the rule

The saved 'Sandbox' 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. Viruscope Settings

The 'Viruscope' component of CES 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 enduser. 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 CES 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.

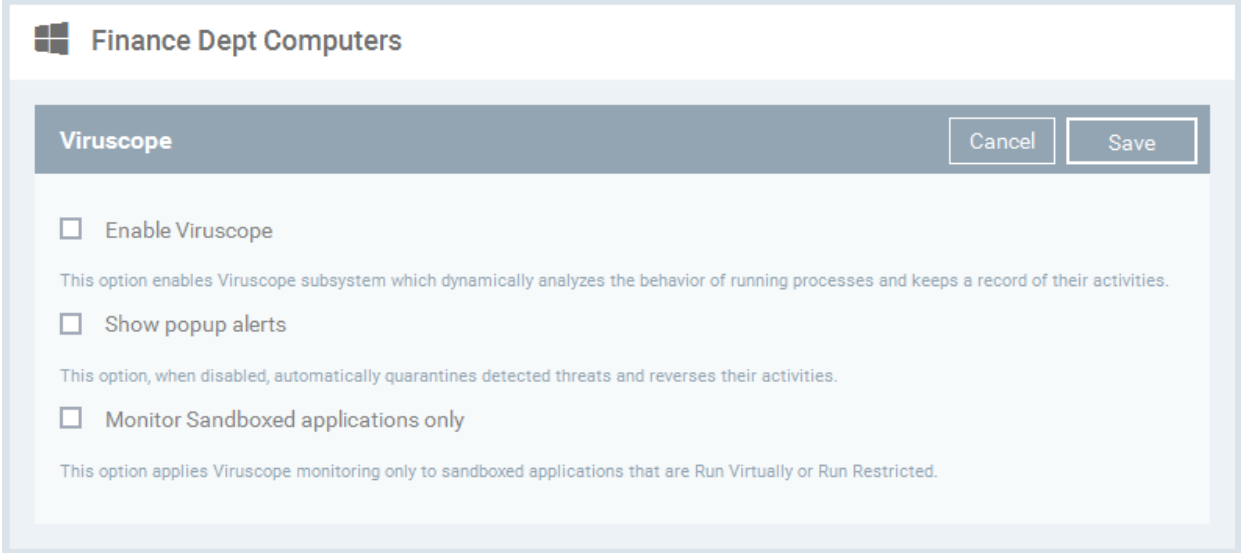
Viruscope alerts give the end-user, the opportunity to quarantine the process & reverse its changes or to let the process go ahead.

The Viruscope settings screen allows you to configure the behavior of Viruscope component of CES at the endpoint computer, to which the profile is applied.

To configure Viruscope settings

- Choose 'Viruscope' from the 'Add' drop-down

The Viruscope settings screen will be displayed.

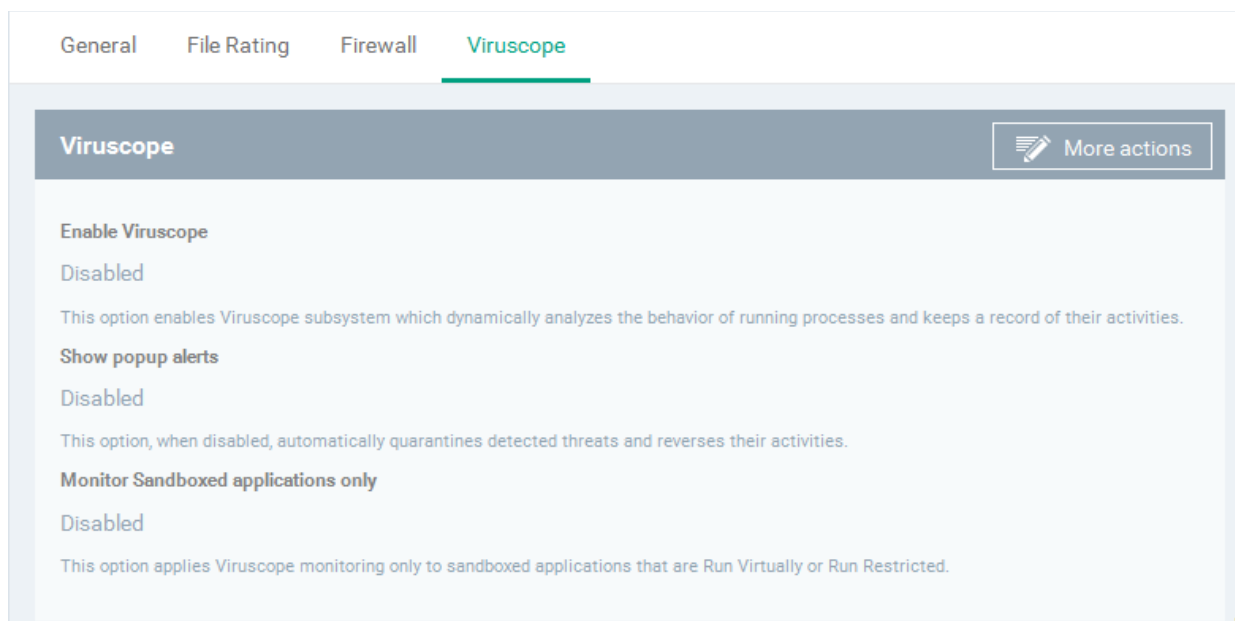


Viruscope Configuration - Table of Parameters

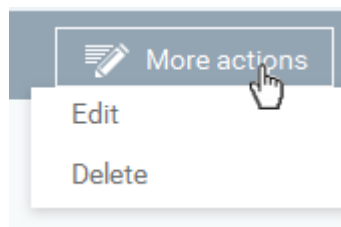
Form Element	Description
Enable Viruscope	Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities of all the running processes and generates alerts on suspicious activities
Show popup alerts	Allows you to configure whether or not to show Viruscope alerts when a suspicious 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 sandboxed applications only	Viruscope can monitor all the processes running at the endpoint. If you want it only to monitor the processes pertaining to auto-sandboxed applications or applications manually added to run inside the sandbox, select this option.

- Click the 'Save' button.

The Viruscope component will be added to the Windows profile.



- To edit or delete the component, click More Actions and choose the option.



The saved 'Viruscope' 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.

6.1.3.1.6. 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 Endpoint 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' 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.

Finance Dept Computers

Add Section | Export Profile | Clone Profile | Delete Profile

General | File Rating | Firewall | Viruscope | **HIPS**

HIPS Save Delete

HIPS Settings | HIPS Rules | Rulesets | Protected Objects

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: 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

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. <i>(Default=Enabled)</i> 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'.

HIPS Settings - Table of Parameters	
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; align-items: center;"> <input type="checkbox"/> Enable HIPS </div> <div style="margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid #ccc; padding: 5px; width: 80%;"> <p>Safe Mode</p> <hr/> <p>Paranoid Mode</p> <p style="background-color: #007bff; color: white; padding: 2px;">Safe Mode</p> <hr/> <p>Clean PC Mode</p> <hr/> <p>Training Mode</p> </div> <div style="text-align: center; width: 10%;"> <div style="border: 2px solid red; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 0 auto;"> ▼ </div> </div> <div style="width: 10%; text-align: right;"> <p style="color: #007bff;">Monitoring Settings</p> </div> </div> </div> </div> <p>The available options are:</p> <ul style="list-style-type: none"> 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 Endpoint Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses <i>your</i> configuration settings to filter critical system activity. Similarly, the Comodo Endpoint Security does automatically create 'Allow' rules for any 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 teh endpoints are safe to run.
Monitoring Settings	<p>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.</p>

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

<input type="checkbox"/> Interprocess Memory Access	<input type="checkbox"/> Processes Execution
<input type="checkbox"/> Windows/WinEvent Hooks	<input type="checkbox"/> Win Messages
<input type="checkbox"/> Device Driver Installations	<input type="checkbox"/> DNS/RPC Client Service
<input type="checkbox"/> Processes' Terminations	

Objects to Monitor Against Modifications

<input type="checkbox"/> Protected COM Interfaces	<input type="checkbox"/> Protected Registry Keys
<input type="checkbox"/> Protected Files/Folders	

Objects to Monitor Against Direct Access

<input type="checkbox"/> Physical Memory	<input type="checkbox"/> Disks
<input type="checkbox"/> Computer Memory	<input type="checkbox"/> 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 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

HIPS Settings - Table of Parameters

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 Endpoint 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)*.

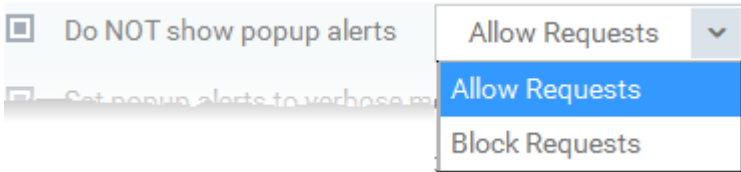
Objects To Monitor Against Modifications:

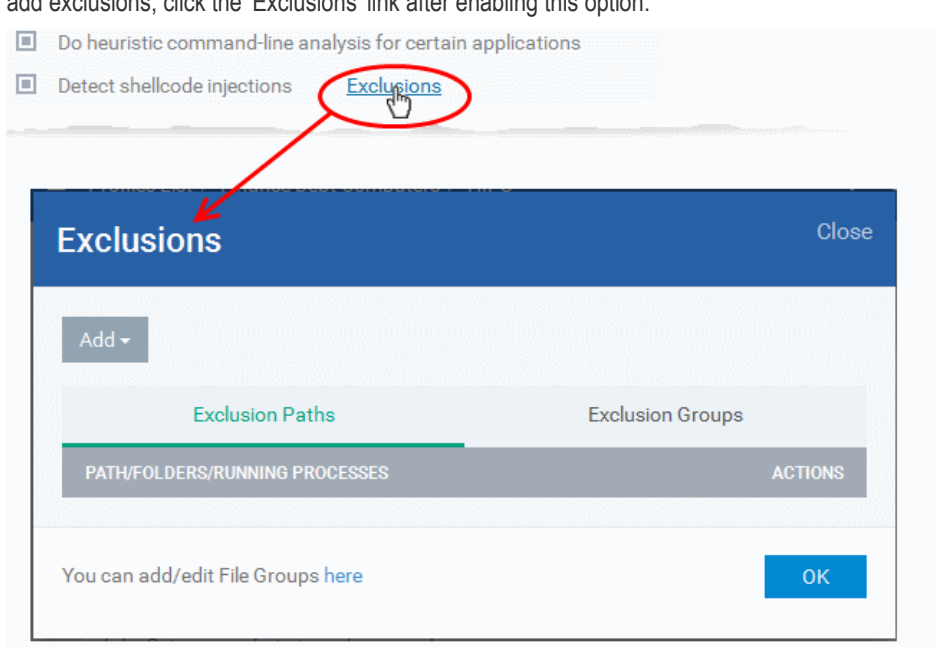
- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. *(Default = Enabled)*
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. *(Default = Enabled)*.
- **Protected Files/Folders** 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 Endpoint 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:

- **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 Endpoint 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)*.

HIPS Settings - Table of Parameters	
	<ul style="list-style-type: none"> 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 <i>(Default = Enabled)</i>. 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 Endpoint Security generates alerts every time an application attempts to establish direct access to the keyboard <i>(Default = Enabled)</i>. <p>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-rides any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface.</p>
Do NOT show popup alerts	<p>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 <i>(Default = Enabled)</i>.</p> <p>If you choose not to show alerts then you have a choice of default responses that CES should automatically take - either 'Block Requests' or 'Allow Requests'.</p> 
Set popup alerts to verbose mode	<p>Enabling this option instructs CES to display HIPS alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests <i>(Default = Enabled)</i>.</p>
Create rules for safe applications	<p>Automatically creates rules for safe applications in HIPS Ruleset <i>(Default = Enabled)</i></p> <p>Note: HIPS trusts the applications if:</p> <ul style="list-style-type: none"> The application/file is rated as 'Trusted' in the File List 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.
Set new on-screen alert timeout to	<p>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.</p>
Advanced Settings	
Enable adaptive mode under low system resources	<p>Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CES functions to fail. With this option enabled, CES 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 <i>(Default = Enabled)</i>.</p>
Block unknown requests when the application is not running	<p>Selecting this option blocks all unknown execution requests if Comodo Endpoint 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 CES security settings then it is OK to leave this option disabled. <i>(Default = Disabled)</i></p>
Enable enhanced protection mode (Requires a system restart)	<p>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</p>

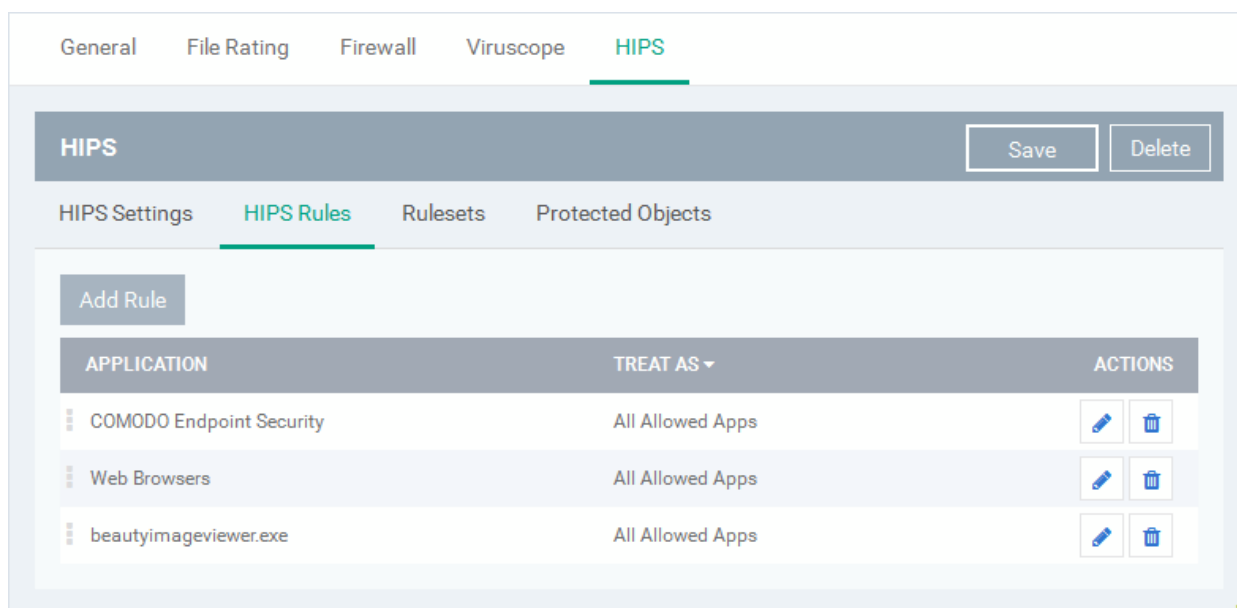
HIPS Settings - Table of Parameters	
	versions of CES could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CIS requires a system restart for enabling enhanced protection mode. (<i>Default = Disabled</i>)
Do heuristic command-line analysis for certain applications	<p>Selecting this option instructs Comodo Endpoint Security to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscript.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, CES 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 (<i>Default = Enabled</i>).</p> <ul style="list-style-type: none"> If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'. <p>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.</p>
Detect shellcode injections	<p>Enabling this setting turns-on the Buffer over flow protection.</p> <p>Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.</p> <p>Turning-on buffer overflow protection instructs the Comodo Endpoint 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.</p> <p>Comodo recommends this setting is left enabled (<i>Default = Enabled</i>).</p> <p>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.</p>  <p>The process of adding exclusions is similar to adding exclusions for virtualization in Sandbox Settings. Refer to the explanation of adding files / folders to be excluded in the previous section</p>

HIPS Settings - Table of Parameters	
	Sandbox Settings.

HIPS Rules

The 'HIPS Rules' screen allows you to view the list of active HIPS rulesets applied to different groups of or individual applications and to create and manage rules for the profile. You can change the ruleset applied to a selected application or application group.

Note: HIPS Rulesets are to be created before applying them to an individual application or an application group. Refer to the next section [Rulesets](#) for details on creating new rulesets.



HIPS Rules - Column Descriptions	
Column Header	Description
Application	Name of the individual application or the application to which the ruleset is applied
Treat As	The ruleset applied. For more details on the rulesets, refer to the next section Rulesets .
Actions	Contains control buttons to edit or remove the rule

Creating and Modifying Hips Rules

To begin defining an application's HIPS rule, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step2 - **Configure the rules for this application's ruleset.**

Step 1 - Select the application that you wish the ruleset is to be applied

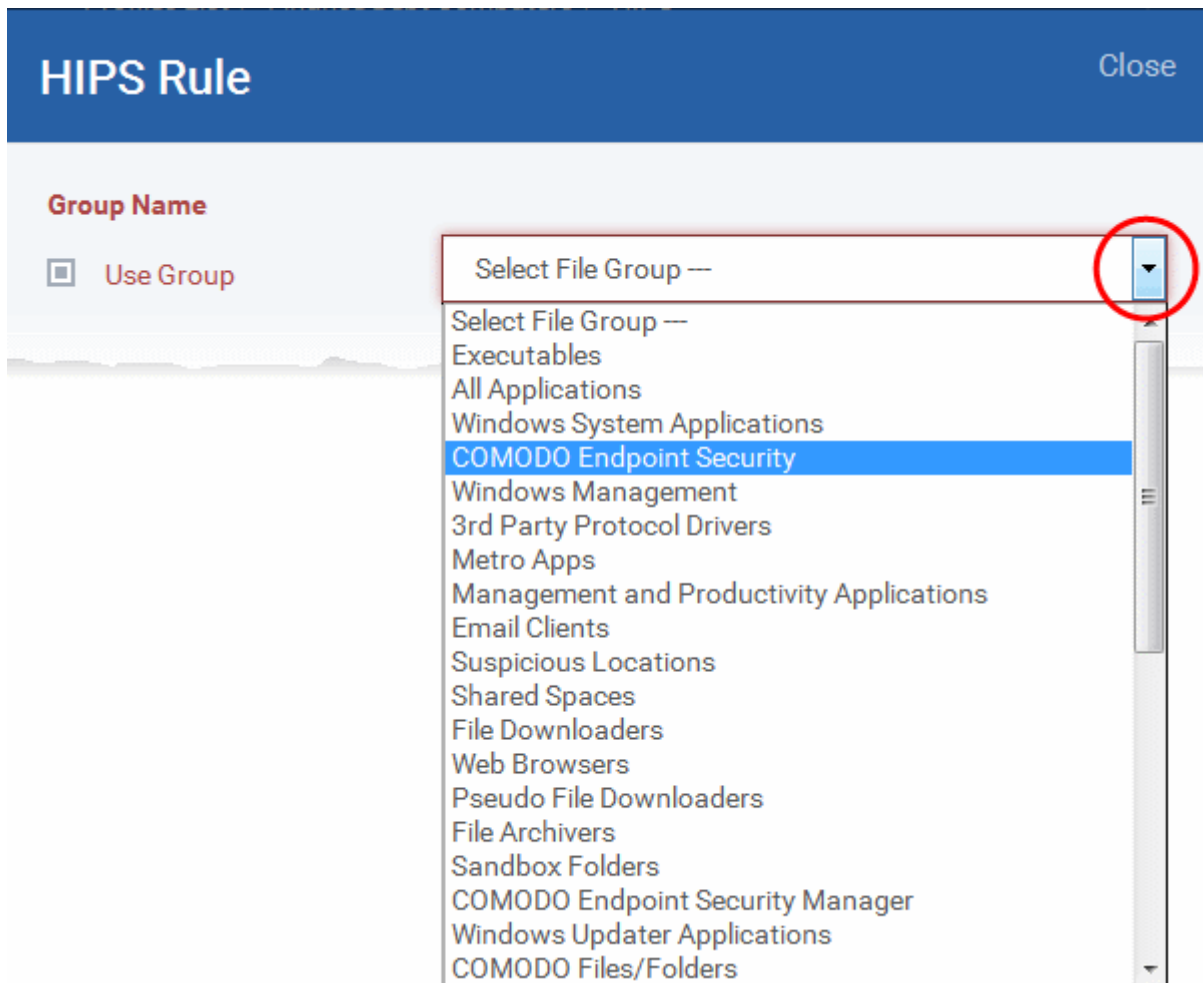
- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add Rule' button at the top of the list in the 'HIPS Rules' interface.

The 'HIPS Rule' interface will open as shown below:

The screenshot shows the HIPS configuration interface. At the top, there are tabs for 'HIPS Settings', 'HIPS Rules', 'Rulesets', and 'Protected Objects'. The 'HIPS Rules' tab is active. A table lists applications with columns for 'APPLICATION', 'TREAT AS', and 'ACTION'. The first row is 'COMODO Endpoint Security' with 'All Allowed Apps' and 'All Allowed Apps'. A red circle highlights the 'Add Rule' button, and a red arrow points from it to a 'HIPS Rule' dialog box. The dialog box has a 'Name' field, a 'Use Group' checkbox, a 'Use Ruleset' radio button, a 'Use a Custom Ruleset' radio button, a 'Copy From' button, and an 'Ok' button.

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: CDM 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 > Global 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
Close

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 Rights
Protection Settings

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 ▼	

Ok

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 ▾

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 change the options for the 'Access Rights' and 'Protection Settings'.

Rulesets

All Allowed Apps
Windows System Applications

OK

Access Rights

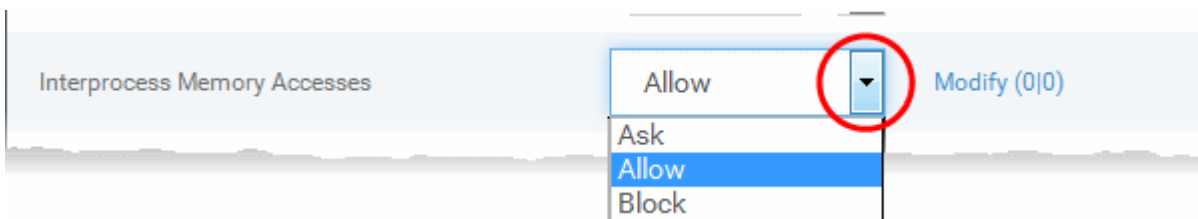
Protection Settings

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

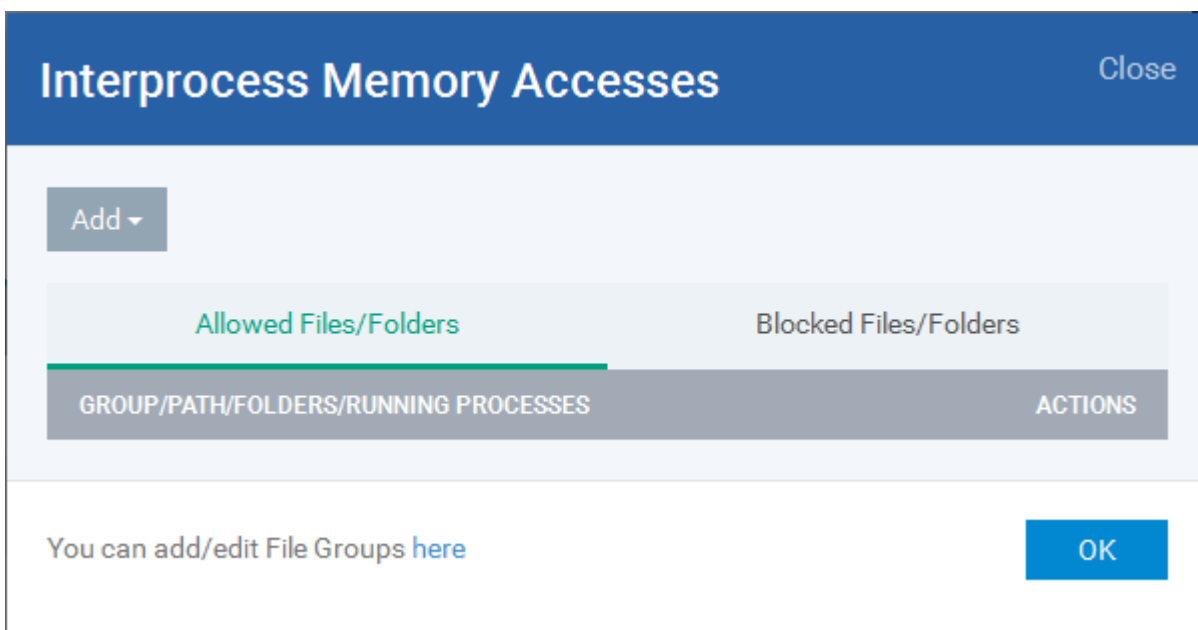
In simplistic terms 'Access Rights' determine what the application *can do to other processes and objects* whereas 'Protection Settings' determine what the application *can have done to it by other processes*.

- i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset.

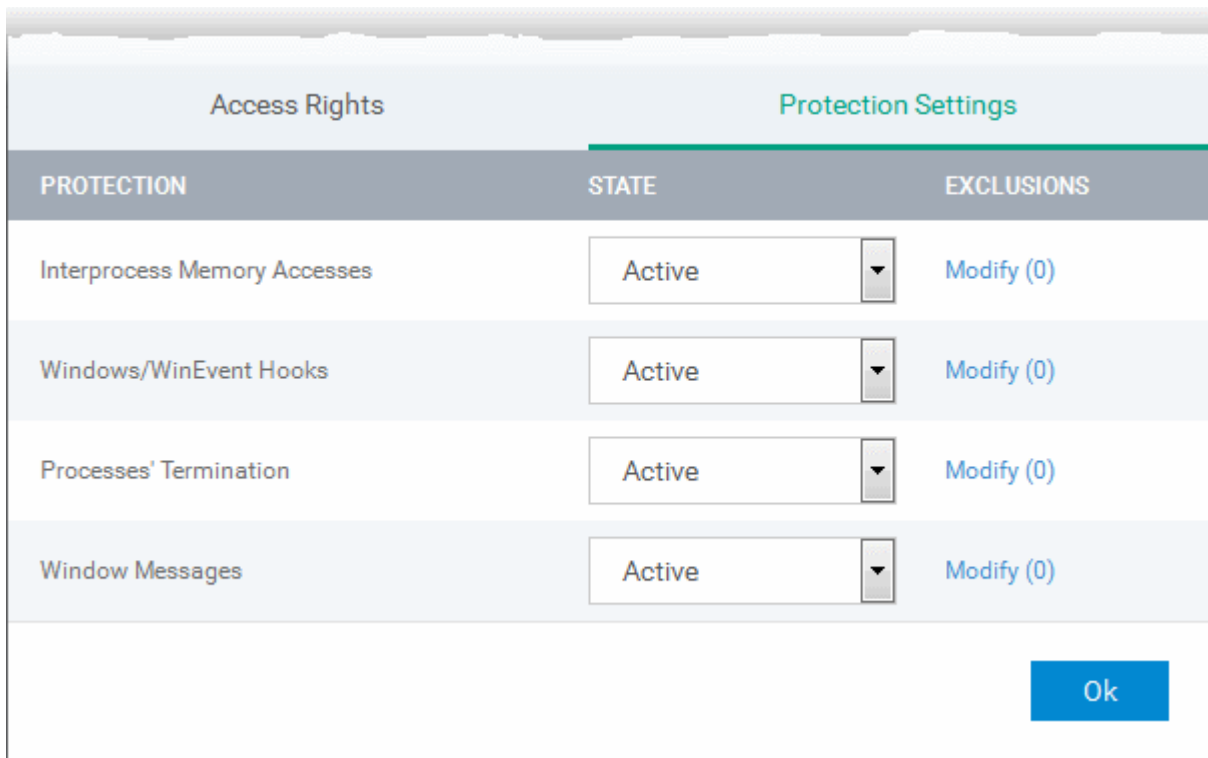


Refer to the section **HIPS Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:

- 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.



- Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. ([click here](#) for an explanation of available options).
- ii. **Protection Settings** - Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection State' column. Select 'Inactive' to disable such protection.

[Click here](#) to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

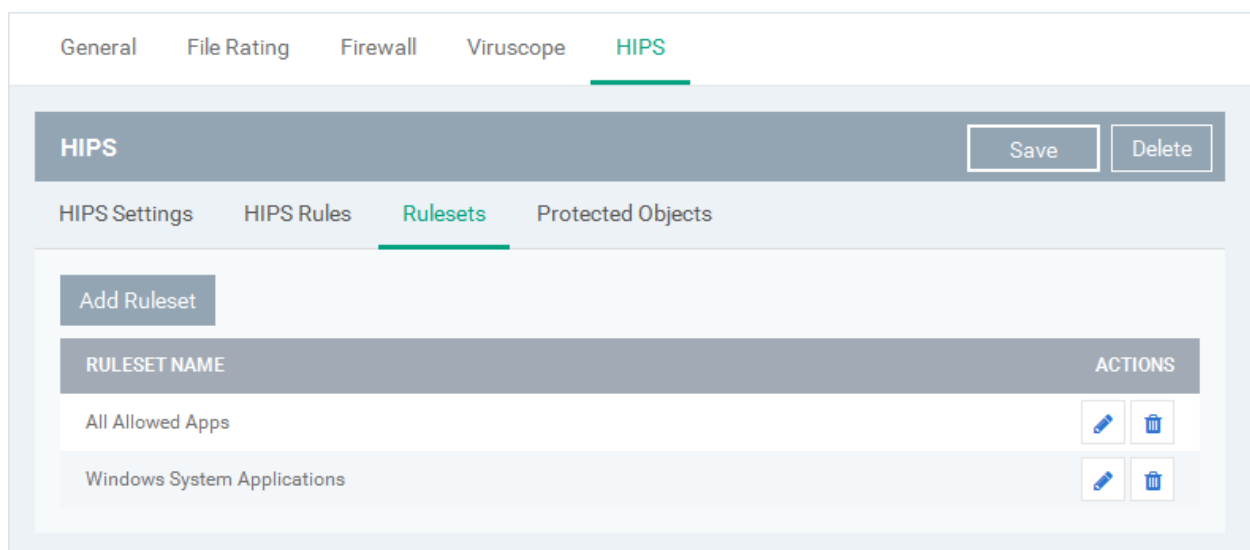
Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

7. Click 'OK' to confirm your settings.


Rulesets

A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of rules and each of these rules is defined by a set of conditions/settings/parameters. Rulesets concern an application's access rights to memory, other programs, the registry etc.

The Rulesets screen under the the 'HIPS' tab displays the list of rulesets and allows you to add and manage new rulesets.



To add a new ruleset

- Click the 'Add Ruleset' button  above the list of rulesets.

The 'HIPS Ruleset' dialog will appear.

HIPS Ruleset Close

Name

Name

Access Rights Protection Settings

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

Disk

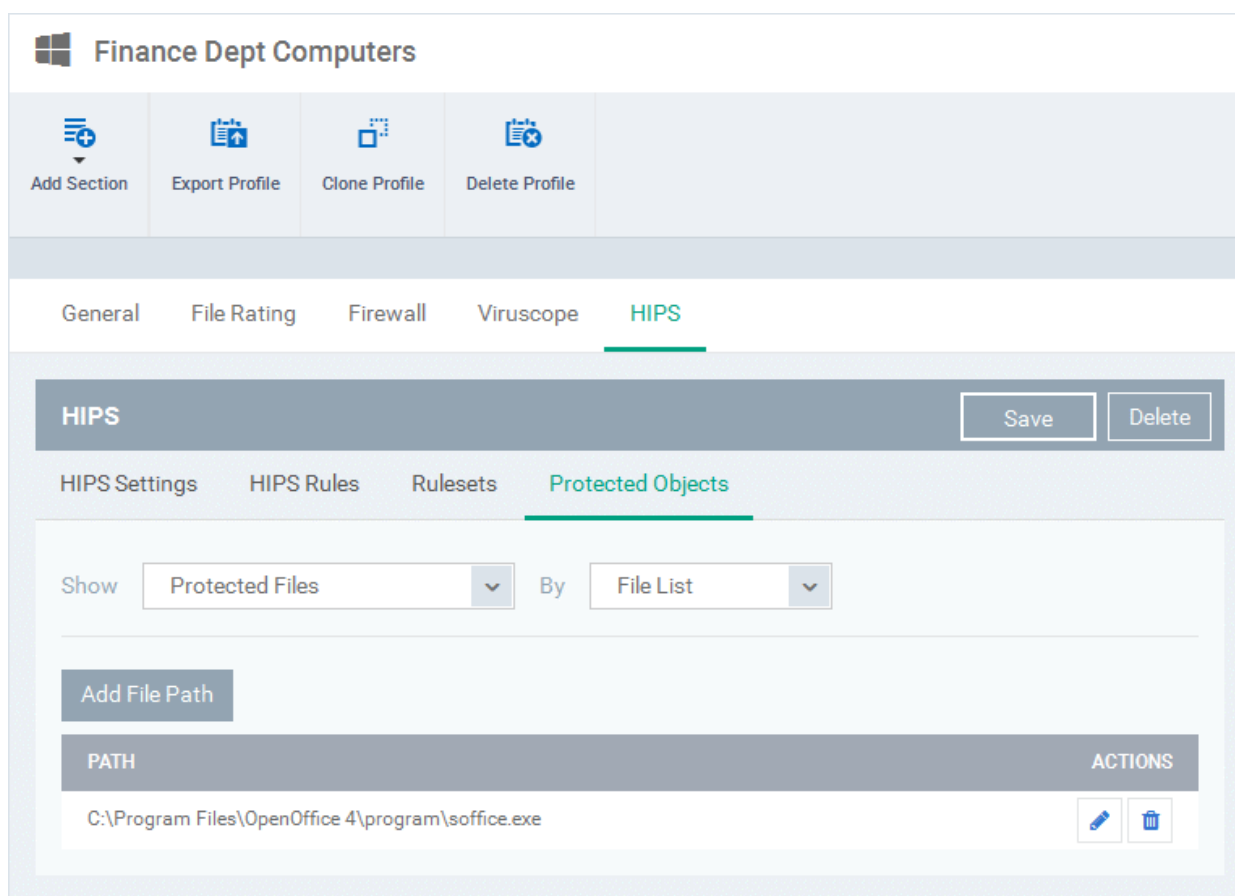
Keyboard

Ok

- 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 'Sandboxed' programs will be blocked from accessing them.



The 'Show' drop-down allows you to choose the category of protected objects to be displayed in the list and add and manage the protected objects of that category. You can add following categories of protected objects:

- **Protected Files** - Allows you to view and specify programs, applications, files and 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 Sandboxed programs

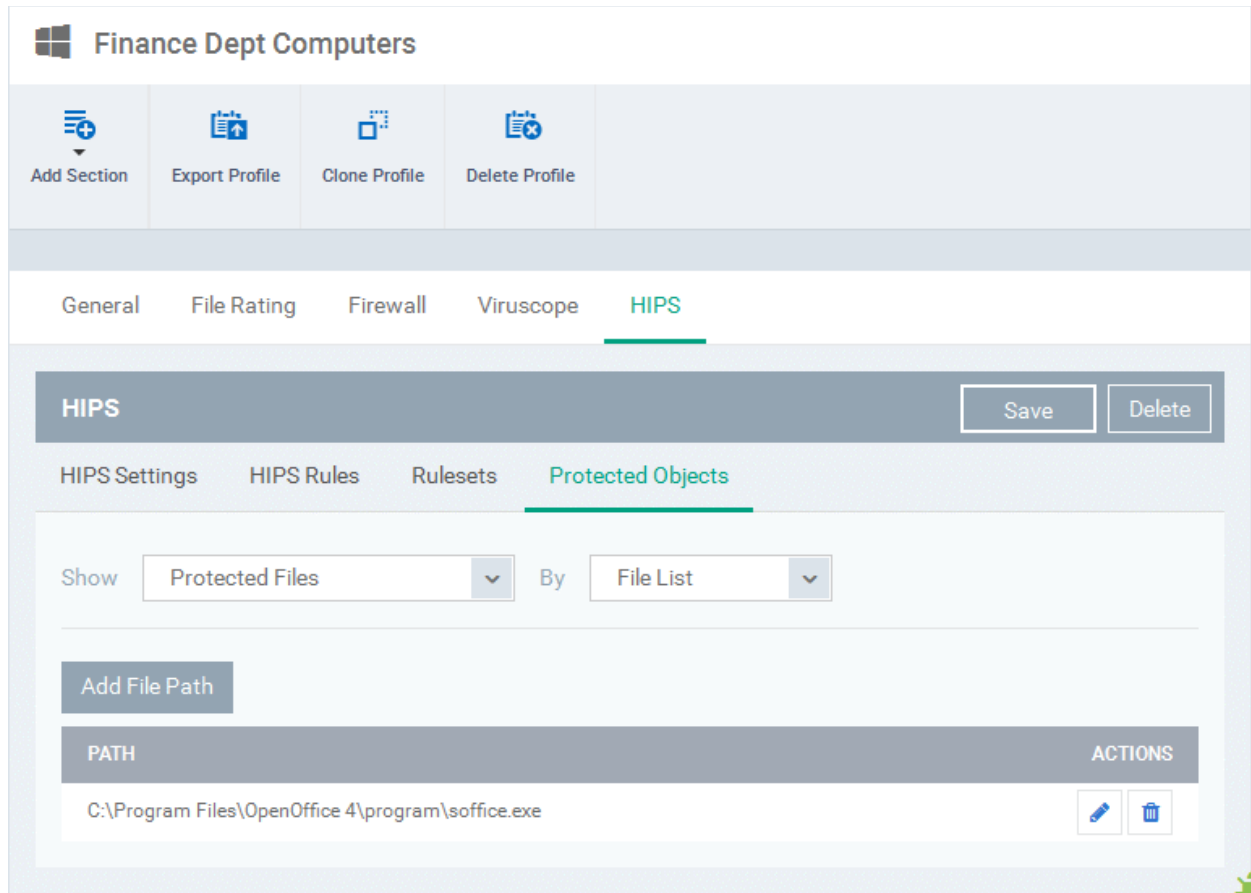
Protected Files

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 Endpoint Security blocks this attempt and produces a 'Protected File Access' pop-up alert.

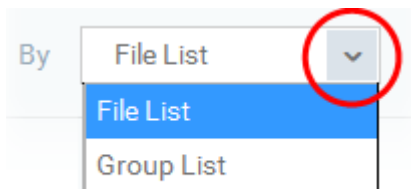
If you add a file to 'Protected Files', but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. Refer to the explanation of **adding 'Exceptions' at the end of this section** for more details about how to allow access to files placed in Protected Files.

- To view the list of Protected Files, choose 'Protected Files' from the 'Show' drop-down in the 'Protected Objects'

interface



The Protected File list is displayed under two categories, which can be selected from the drop-down at the right.

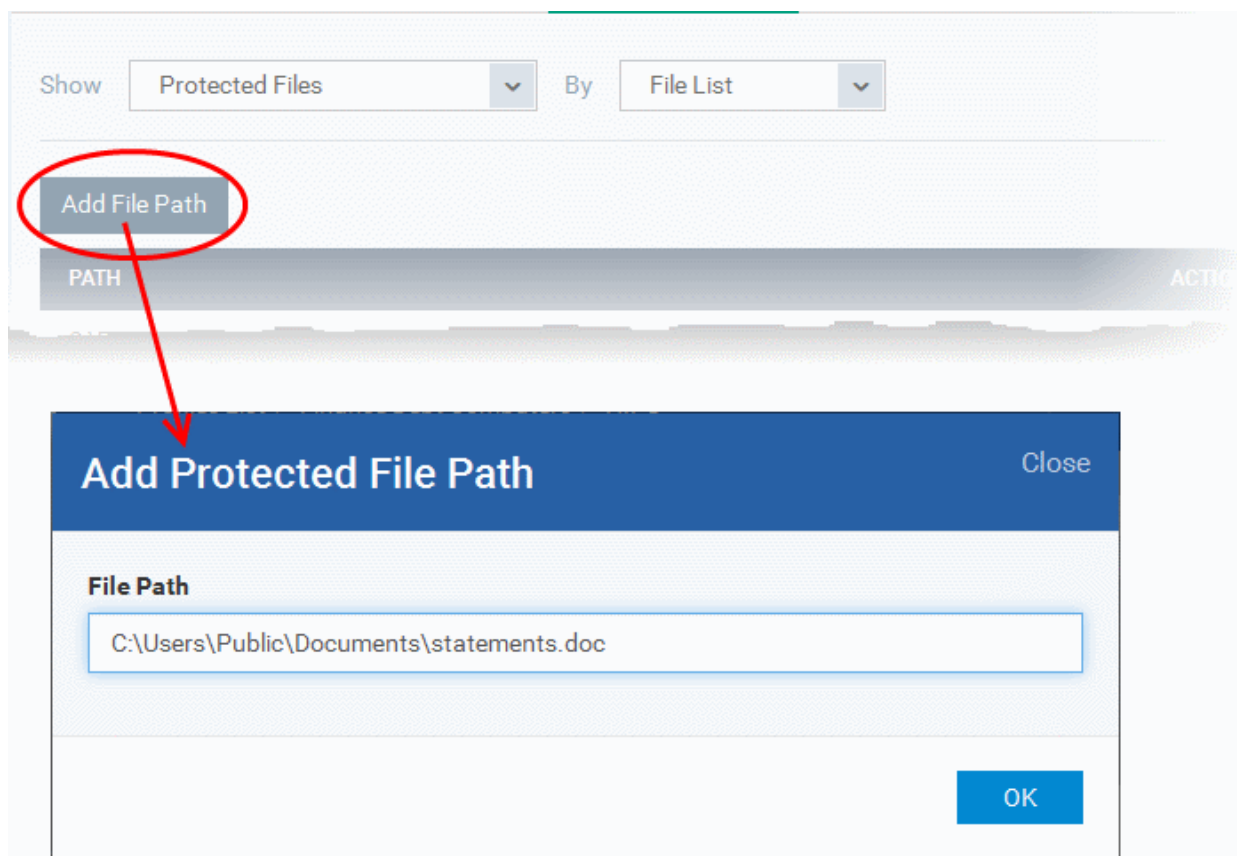


- To view the list of individual files, programs, applications added to the Protected Files list and manage them, choose 'File List'
- To view the File Groups added to the Protected File list, choose 'Group List'

You can add individual files, programs, applications or file/groups to 'Protected Files'.

To add an individual file, program or an application

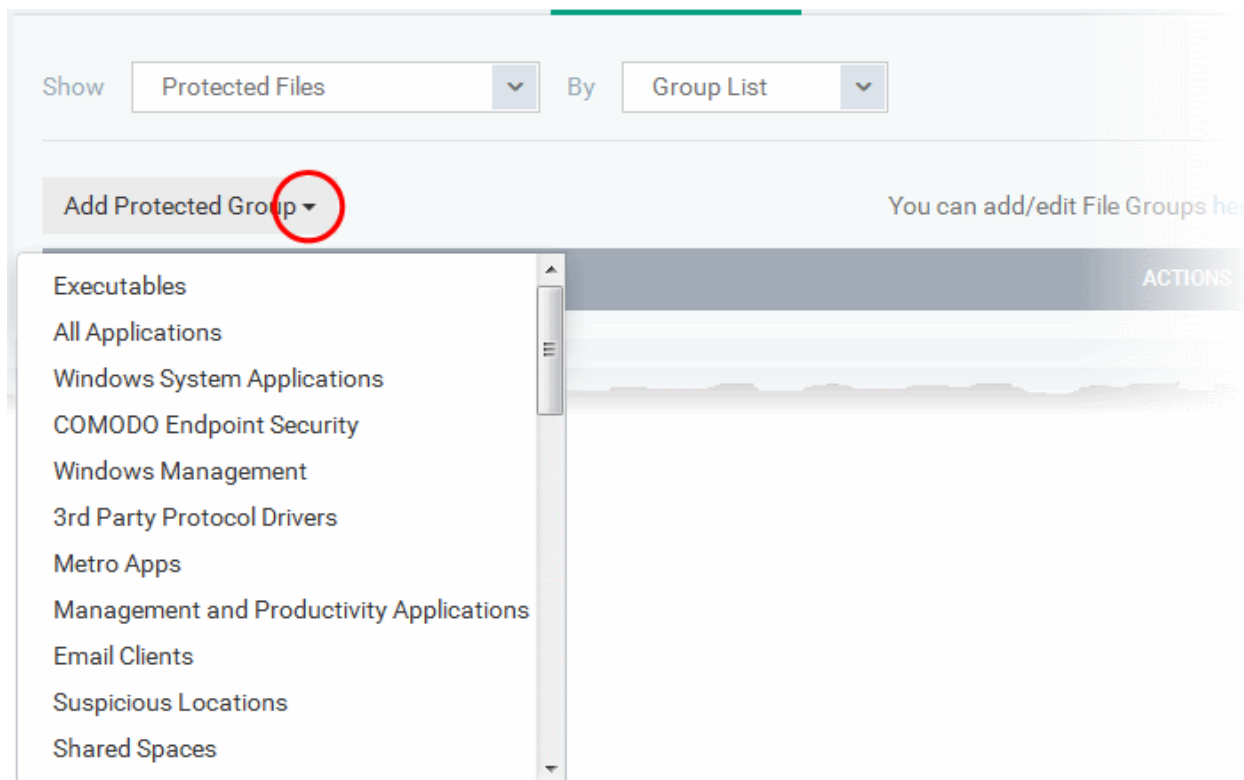
- Choose 'File List' from the drop-down at the right and click the 'Add File Path' button.



- Enter the installation/storage path with file name of the file to be protected, in the managed computers, in the 'Add Protected File Path' dialog and click 'OK'.
- Repeat the process to add more files.
- To edit the path of an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add an application/file group to the Protected Files list

- Choose 'Group List' from the drop-down at the right and click the 'Add Protected Group' button



- Choose the file group from the drop-down and click 'OK'.

Note: CDM 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' > 'Global 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 'scal' 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
Close

Name

Use Group account.ods

Use Ruleset Use Ruleset --

Use a Custom Ruleset Copy From ▾

Access Rights
Protection Settings

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 ▾	
Disk	Ask ▾	
Keyboard	Ask ▾	

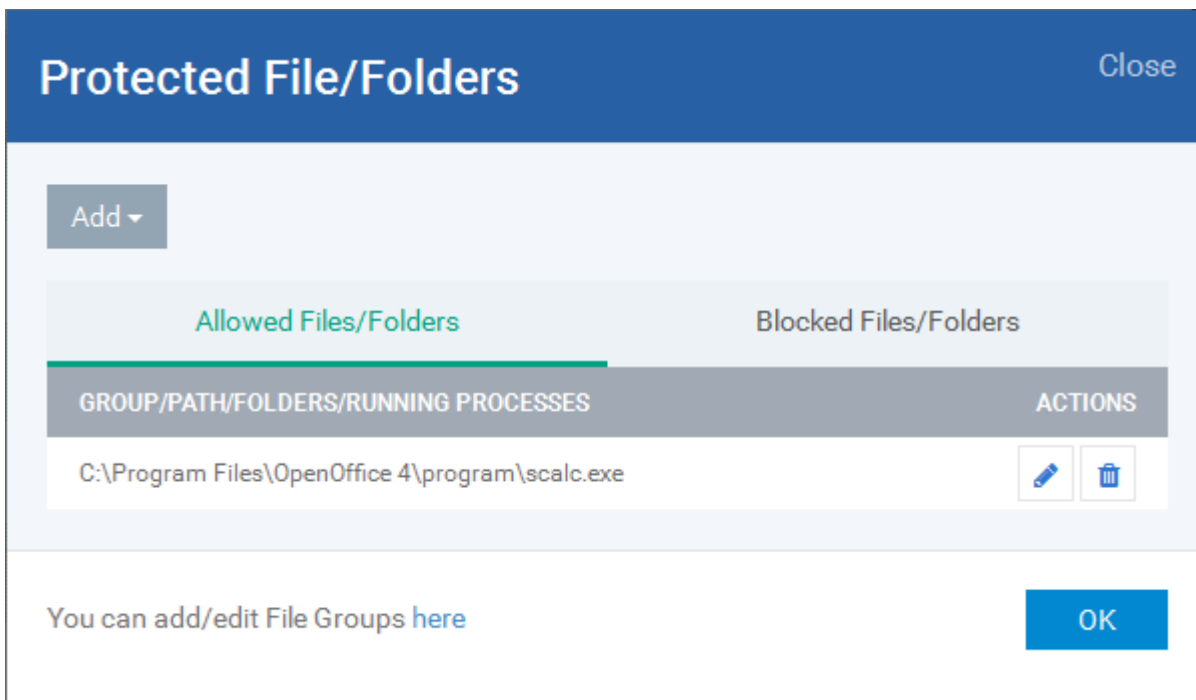
Ok

- Click the 'Modify' beside 'Protected File/Folders'

Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'. The 'Protected Files/Folders' interface will appear.

- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or

'Block' rule in the 'Access Rights'.

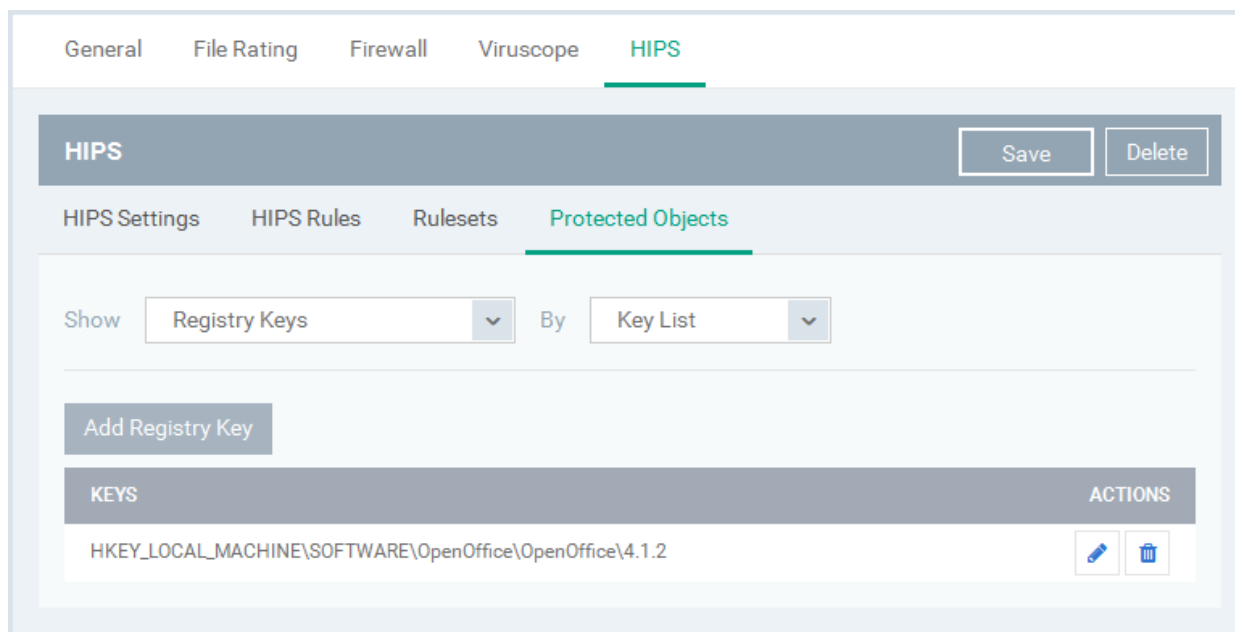


Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area' (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

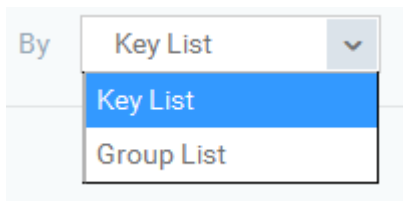
Registry Keys

The 'Registry Keys' list under 'Protected Objects' interface allows you to view and manage list of critical registry keys and registry groups to be protected against modification. Irreversible damage can be caused to the managed endpoint if important registry keys are corrupted or modified in any way. It is essential that the registry keys are protected against any type of attack.

To view the list of Protected Registry Keys, choose 'Registry Keys' from the 'Show' drop-down in the 'Protected Objects' interface



The Protected Registry Keys list is displayed under two categories, which can be selected from the drop-down at the right.

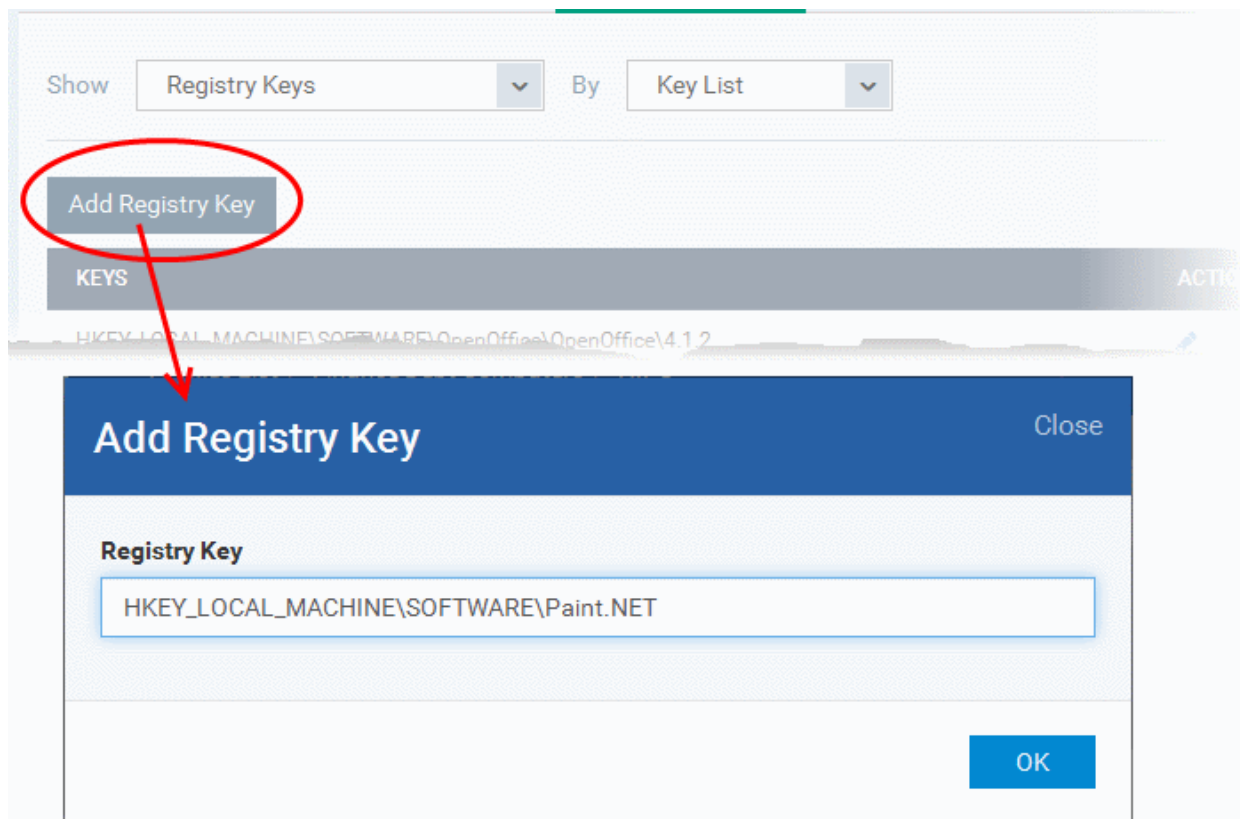


- To view the list of individual keys and values, and manage them, choose 'Key List'
- To view the Registry Groups, choose 'Group List'

You can add individual registry keys and Registry groups to Protected Registry Keys list.

To add an individual key

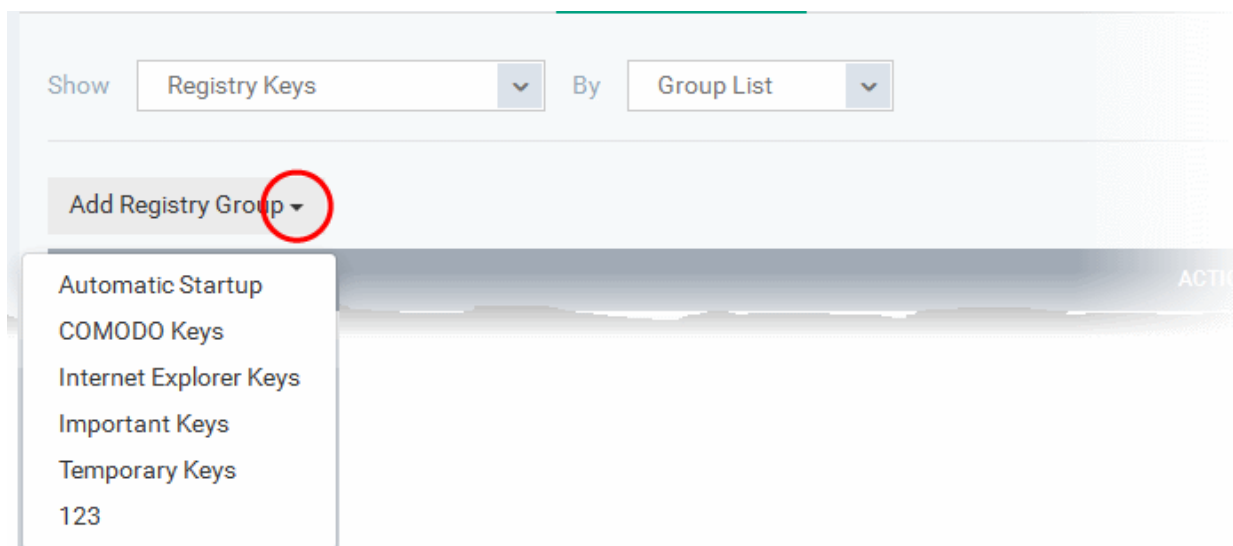
- Choose 'Key List' from the drop-down at the right and click the 'Add Registry Key' button.



- Enter the key name to be protected in the 'Add Registry Key' dialog and click 'OK'.
- Repeat the process to add more keys.
- To edit an item in the list, click the 'Edit' icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add an Registry group to the Protected Registry Keys list

- Choose 'Group List' from the drop-down at the right and click the 'Add Protected Files' button



- Choose the Registry group from the drop-down and click 'OK'.

Note: CDM 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' > 'Global variables' interface. Refer to the section [Registry Groups](#) for more details.

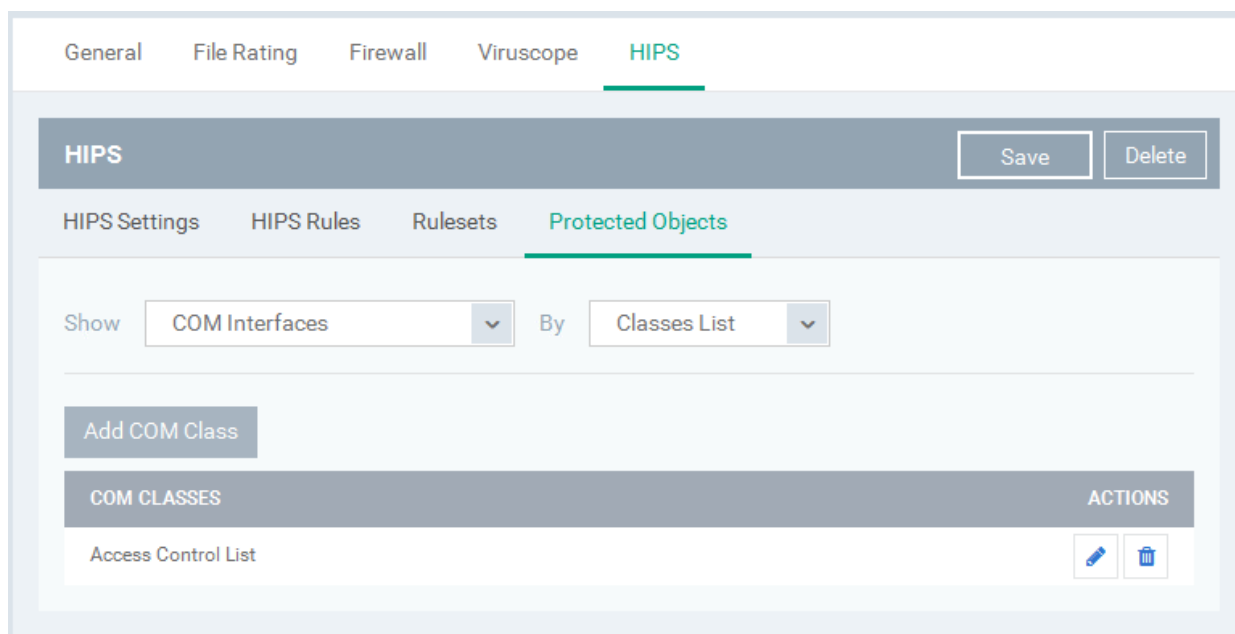
- Repeat the process to add more Registry groups.
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

COM Interfaces

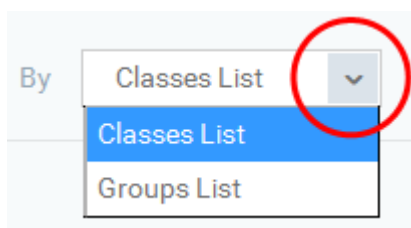
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers 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 Endpoint Security at the managed computer against modification, corruption and manipulation by malicious processes.

- To view the list of Protected COM interfaces, choose 'COM Interfaces' from the 'Show' drop-down in the 'Protected Objects' interface



The Protected COM Interfaces list is displayed under two categories, which can be selected from the drop-down at the right.

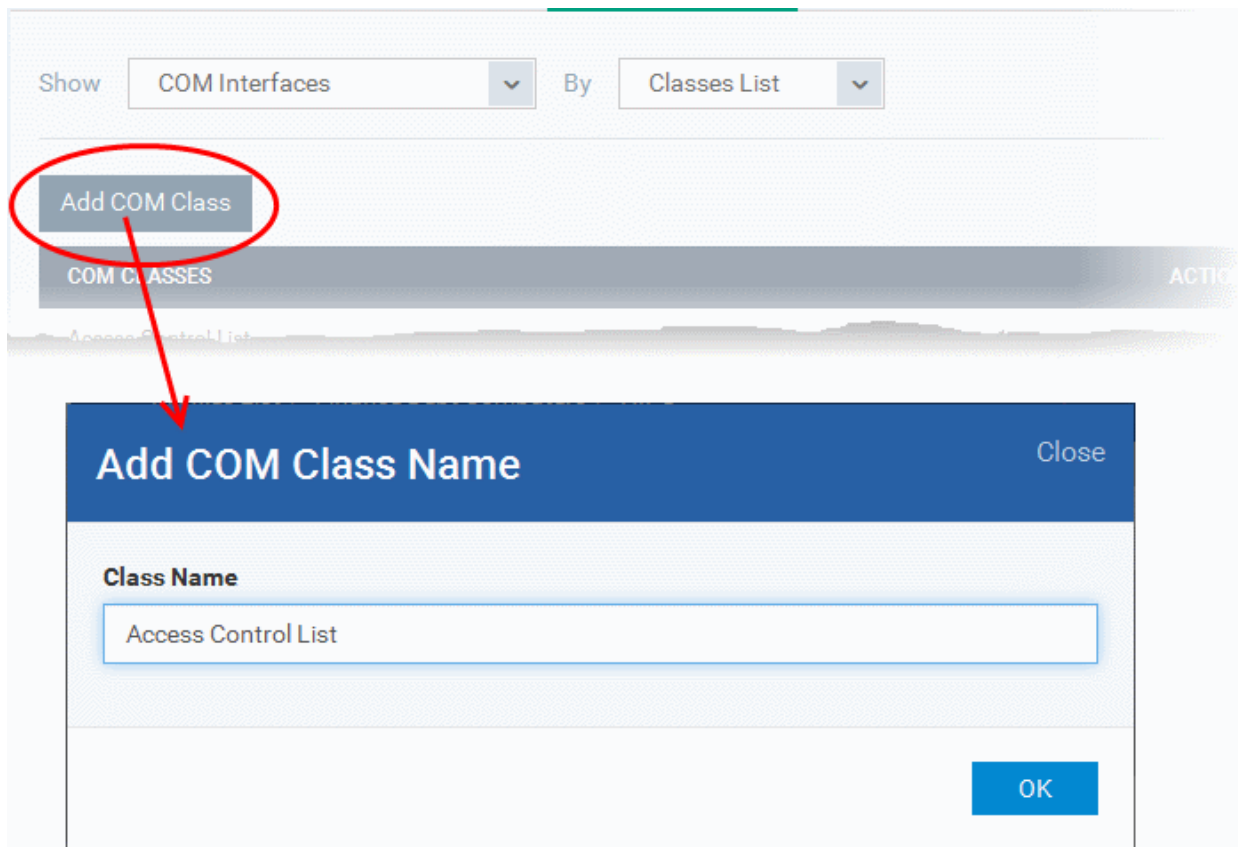


- To view the list of individual COM Interfaces/Classes and manage them, choose 'Classes List'
- To view the COM Groups and manage them, choose 'Group List'

You can add individual COM Interfaces/Classes and/or pre-defined COM groups to 'Protected COM Objects' list.

To add an individual COM object

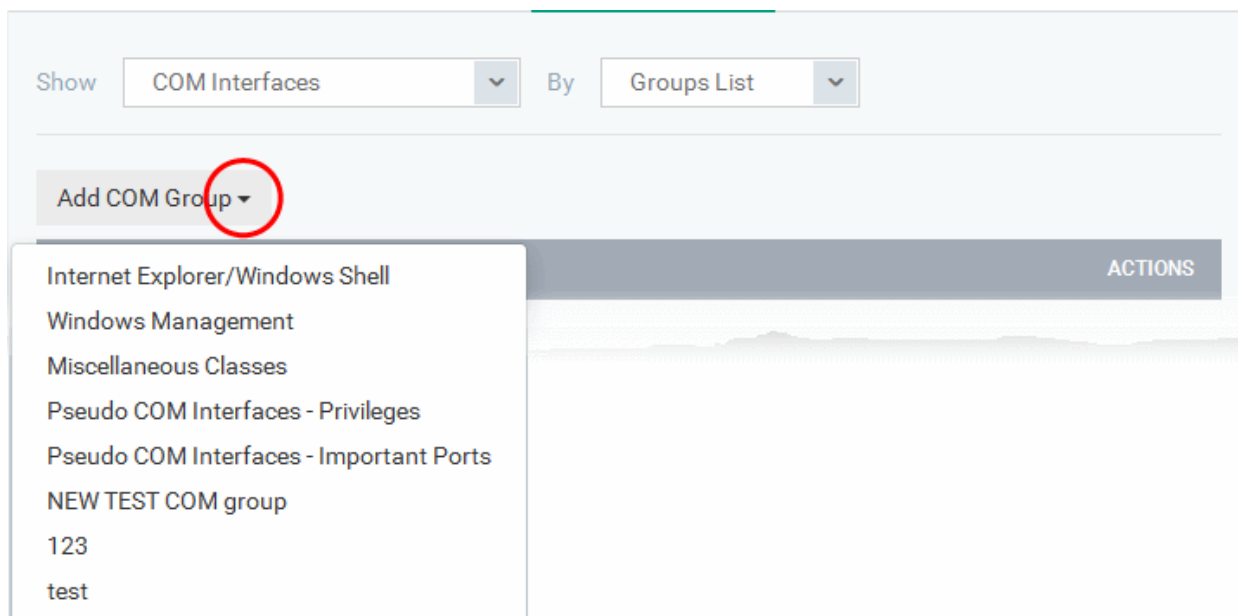
- Choose 'Classes List' from the drop-down at the right and click the 'Add COM Class' button



- Enter the name of the COM object to be protected at the managed computer, in the 'Add COM Class Name' dialog and click 'OK'.
- Repeat the process to add more COM objects.
- To edit an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

To add a predefined COM Group to the Protected COM objects list

- Choose 'Group List' from the drop-down at the right and click the 'Add COM Group' button



- Choose the file group from the drop-down and click 'OK'.

Note: CDM 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' > 'Global 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

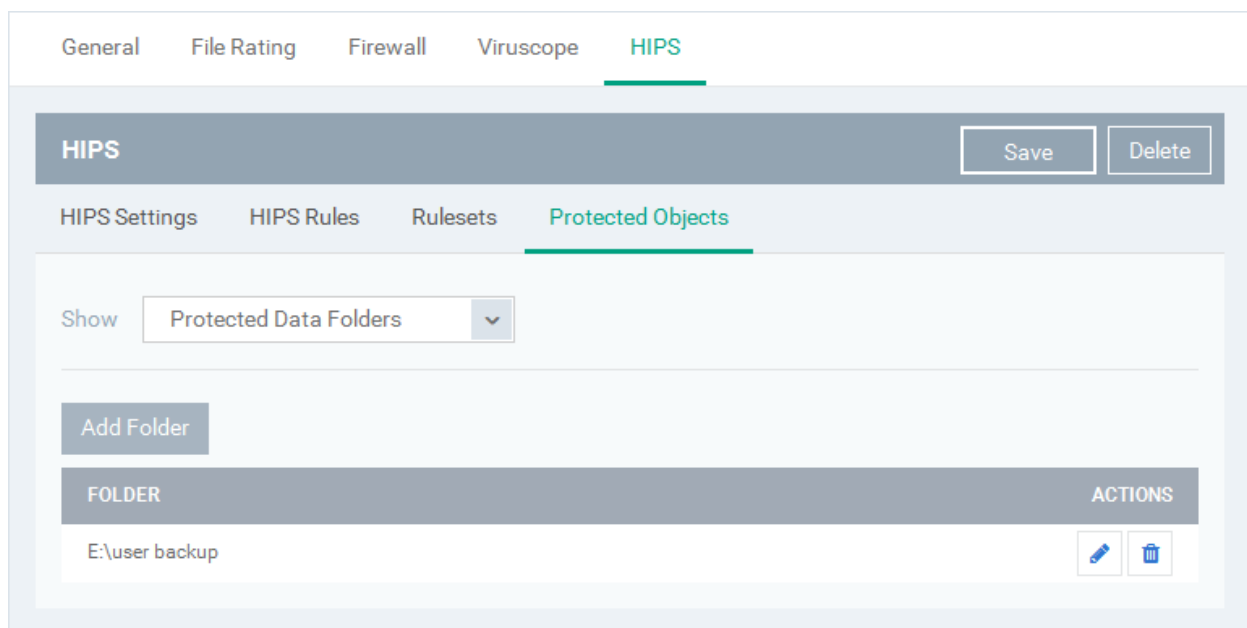
Protected Data Folders

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 sandbox.

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 sandboxed 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 sandboxed programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

The Protected Data Folders list under Protected Objects allows you define protected data folders at the managed computers and to manage them.

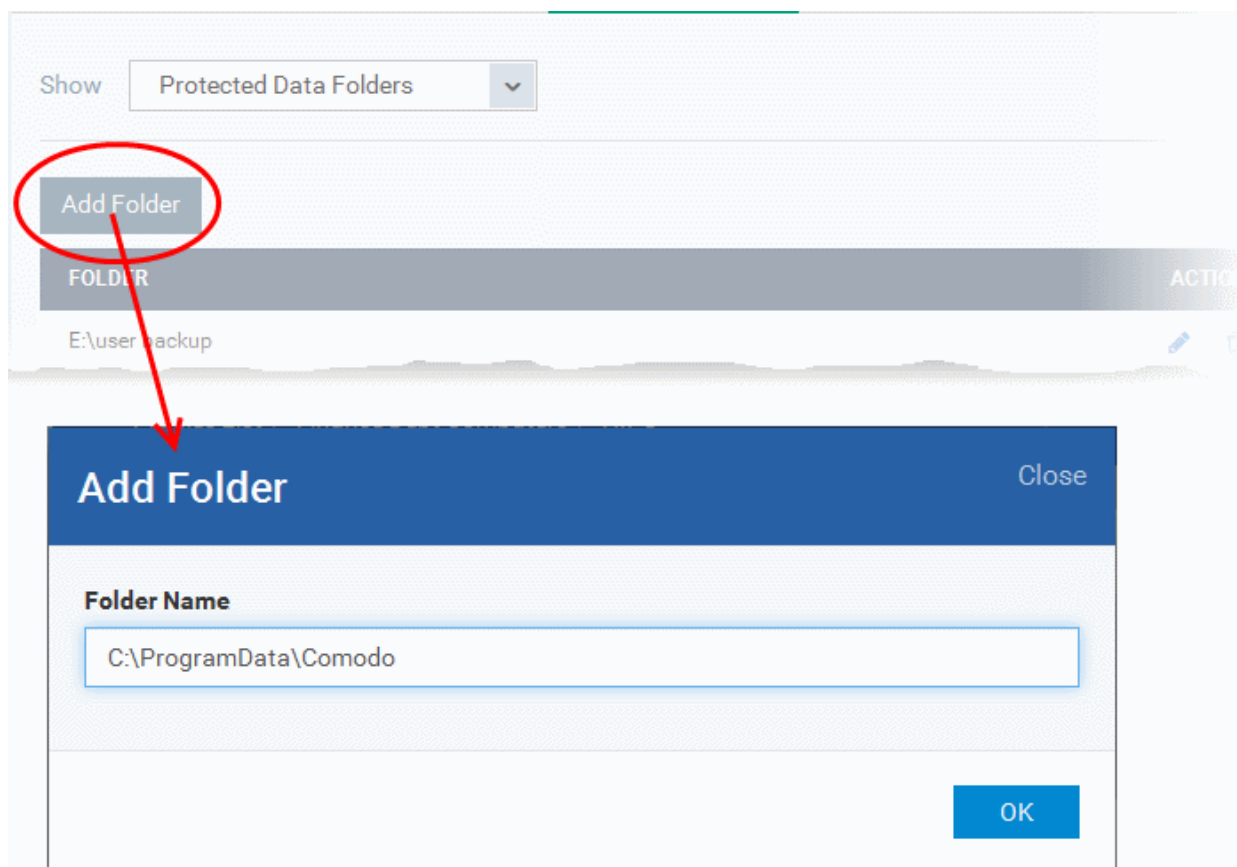
- To open the Protected Data Folders list, choose 'Protected Data Folders' from the Show drop-down in the Protected Objects interface.



You can add standard folders at the managed computers as Protected Data Folders. Data files to be protected from sandboxed 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 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

6.1.3.1.7. 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 Endpoint 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 Valkyrie's results is all displayed in the [The Dashboard](#).

Note: The version of Valkyrie that comes with the free version of CDM is limited to the online testing service. The Premium version of CDM 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

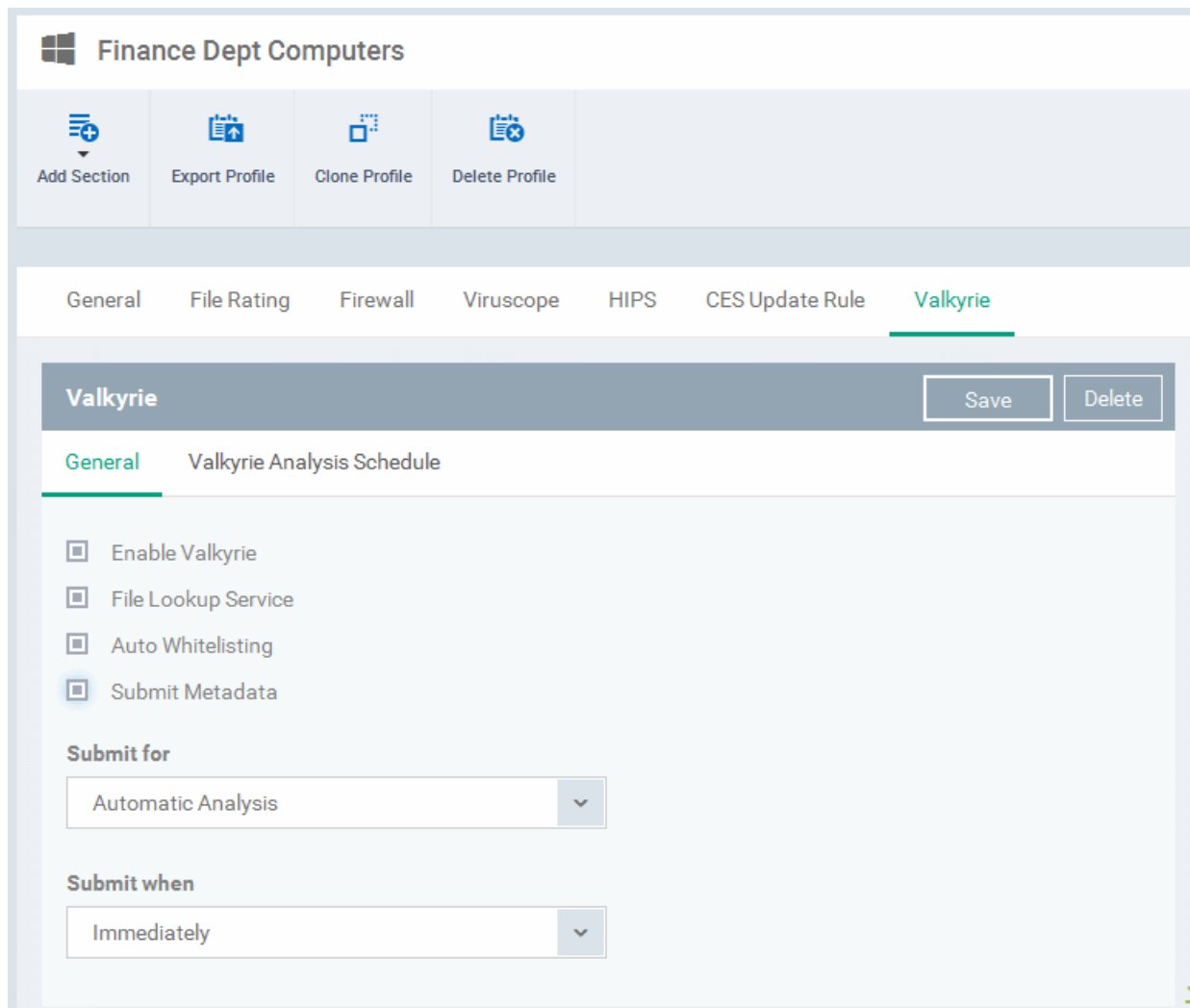
- Click 'Valkyrie' from the 'Add' drop-down in the Windows Profile interface

The 'Valkyrie' settings screen will be displayed. It contains two tabs:

- **General** - Allows you to enable/disable Valkyrie, choose the analysis services to be used and so on.
- **Valkyrie Analysis Schedule** - Allows you to create a schedule for file submission

General

The 'General' settings panel under the 'Valkyrie' tab allows you to enable/disable Valkyrie and choose the analysis services to be used.



Valkyrie Settings - Table of Parameters	
Form Element	Description
Enable Valkyrie	Allows you to enable or disable the Valkyrie in the profile. If enabled, you can choose the services to which the unknown files are to be submitted from the options below.
File Lookup Service	Choose this option if you want the files to be submitted to the cloud file lookup service
Auto-Whitelisting	Choose this option if you wish the files identified as harmless by Valkyrie to be added to your local whitelist
Submit Metadata	Choose this option if you wish the unknown file is to be submitted to Valkyrie, along with their metadata. Metadata gives information about the file source, author, date of creation and so forth.
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.
Submit when	Choose when the unknown files are to be submitted. The options available are: <ul style="list-style-type: none"> Immediately - CES uploads the file to Valkyrie as soon as it encounters an Unknown file Schedule Analysis - CES accumulates the unknown files and uploads them as per the

Valkyrie Settings - Table of Parameters	
	schedule set under the Valkyrie Analysis Schedule tab.

Valkyrie Analysis Schedule

The Valkyrie Analysis Schedule tab allows you to create a schedule for CES to upload unknown files.

The screenshot displays the 'Valkyrie' settings page. At the top, there are navigation tabs: General, File Rating, Firewall, Viruscope, HIPS, CES Update Rule, and Valkyrie. The 'Valkyrie' tab is selected. Below the tabs, there are 'Save' and 'Delete' buttons. The main content area is titled 'Valkyrie Analysis Schedule'. It includes a section 'Schedule your Valkyrie analysis:' with a dropdown menu currently set to 'Every Month'. Below this is a 'Day of Month' calendar grid where the 10th is highlighted. At the bottom, there is a 'Time' section with a digital clock interface showing '12:00 PM'.

- 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'.

6.1.3.1.8. CES Update Rule Settings

The CES installations at the managed computers automatically download periodic virus signature database updates and program updates on order to detect and identify even zero-day malware in order to ensure continuous protection from ever emerging threats.

The CES Update Rule Settings component of Windows profile allows you to configure the schedule for the managed computers to check for updates and download them from Comodo servers, if available.

To configure CES Update Settings

- Click 'CES Update Rule Settings' from the 'Add' drop-down in the Windows Profile interface

The screenshot shows the 'CES Update Rule' configuration window. At the top, there are tabs for 'General', 'File Rating', 'Firewall', 'Viruscope', 'HIPS', and 'CES Update Rule'. Below the tabs, the title 'CES Update Rule' is displayed on the left, and 'Save' and 'Delete' buttons are on the right. Underneath, there are two radio buttons: 'When IDLE' (which is selected) and 'Scheduled'.

- When Idle - The managed computer will check for updates from Comodo servers when they go idle and download the updates, if available.
- Scheduled - Allows you to create a daily/weekly schedule for the managed computer to check for updates

To create an update schedule

- Choose 'Scheduled'
- To check for updates daily at a specified time, choose 'Every Day' and set the time in the Time combo boxes, in HH:MM format

This screenshot shows the 'CES Update Rule' configuration window with 'Scheduled' selected. The 'When IDLE' radio button is unselected, and the 'Scheduled' radio button is selected. Under 'Select Day of Week', the 'Every Day' checkbox is unchecked, and a dropdown menu shows 'Wednesday'. Below that, the 'Time' section has two spinners set to '05' and '30'.

- To check for updates on a specified day of the week at a specified time, de-select 'Every Day', choose the day from the drop-down and set the time in the 'Time' combo boxes, in HH:MM format
- Click 'Save' in the title bar to save your update settings to the profile.

6.1.3.2. Importing Windows Profiles

In addition to creating a new Windows profile from the Comodo Device Manager interface, you can create new profiles for rolling out to required endpoints or endpoint group(s) in the following ways:

- Importing the current security configuration of the CES application from a remote managed endpoint and saving it as a new profile
- Export a profile from CDM as a configuration file in .cfg format and import it as a new profile
- Clone an existing profile and edit it for minor changes to create a new profile

This section explains in detail on [Importing CES configuration from a selected endpoint](#).

- For more details on [Importing configuration 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 CES Configuration from a Managed Device

Importing the configuration from a CES application facilitates to add a profile with settings fine tuned as required for the endpoints to which the profile is to be applied. For importing the configuration, you can choose a machine that can be considered a template of sorts for other equivalently configured machines (i.e. having the same hardware/software - a computer used to image other endpoints in the organization is ideal for this purpose).

Creating a Windows profile by importing from an endpoint involves the following steps:

- **Step 1 - Export the current configuration from the selected device as an .xml file**
- **Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s).**

Step 1 - Export the current configuration from the selected device as an .xml file

You can export the current CES configuration from a selected managed Windows device in two ways:

- **Exporting configuration of a selected device from CDM interface**
- **Manually exporting the CES configuration from the selected device**

Export Configuration from CDM interface

You can export the current configuration of CES as per profiles applied to a selected device and the manual configuration of the security components of the CES installation, as a new configuration file and import it as a new profile.

To export the configuration from a device

- Open the 'Device List' interface from the CDM console by clicking 'Devices' > 'Devices List' from the left hand side navigation
- Click on the name of the device from which the configuration is to be imported to open its 'Device Details' interface
- Click on the 'Export CES configuration' button at the top

The screenshot shows the Comodo Device Manager interface. The left sidebar contains navigation options: DASHBOARD, DEVICES (with sub-options: Devices List, Devices Groups), USERS, PROFILES, APPLICATIONS, APP STORE, ANTIVIRUS, and SETTINGS. The main content area is titled 'BOBSMITH-PC' with the owner 'John Smith'. Below the title is a row of action buttons: 'Manage Profiles', 'Refresh Information', 'Export CES Configuration' (circled in red), 'Delete Device', and 'Change BYOD'. Below the buttons is a tabbed interface with tabs for 'Device Name', 'Summary' (selected), 'Networks', 'Associated Profiles', 'File List', and 'Exported CES Configs'. The 'Summary' tab displays a table with four columns: 'Device Summary', 'OS Summary', 'Comodo Endpoint Security Info', and 'Network Summary'.

Device Summary	OS Summary	Comodo Endpoint Security Info	Network Summary
Custom Device Name BOBSMITH-PC	OS Windows	Name COMODO Endpoint Security	AD/LDAP N/A
Name BOBSMITH-PC	OS Name Microsoft® Windows Vista™ Business (x86)	Version 8.2.0.4835	Domain/Workgroup WORKGROUP
Logged User BOBSMITH-PC\Bob	Os Version 6.0.6002	Components Virus DB Version	
Formfactor PC	Build Version 6002	N/A	
Model N/A		Virus DB Last Update Time N/A	

The CES configuration will be exported as .xml file with date/time stamp suffix in the file name and saved at the CDM server. You can view the list of exported configuration files from the device under 'Exported CES Configs' tab from the Device Details interface.

- Open the Device Details interface of the device by clicking 'Device' > 'Device List' from the left and clicking the Device name from the list.
- Click the 'Exported CES Configs' tab

The list of configuration files exported from the device at different time points will be displayed with date/time stamp suffix in their file names.

- Click on the file name that you want to import as a profile to download the file to the computer from which the CDM console is accessed and save it at a safe location.
- Then move on to **Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s).**

Manually exporting the CES configuration from the selected device

The 'Advanced Settings' interface of CES installation at the endpoint enables granular and precise configuration of various settings, options and parameters of each of the security components like Antivirus, Firewall, Sandbox, host intrusion protection system and Viruscope as per the requirements.

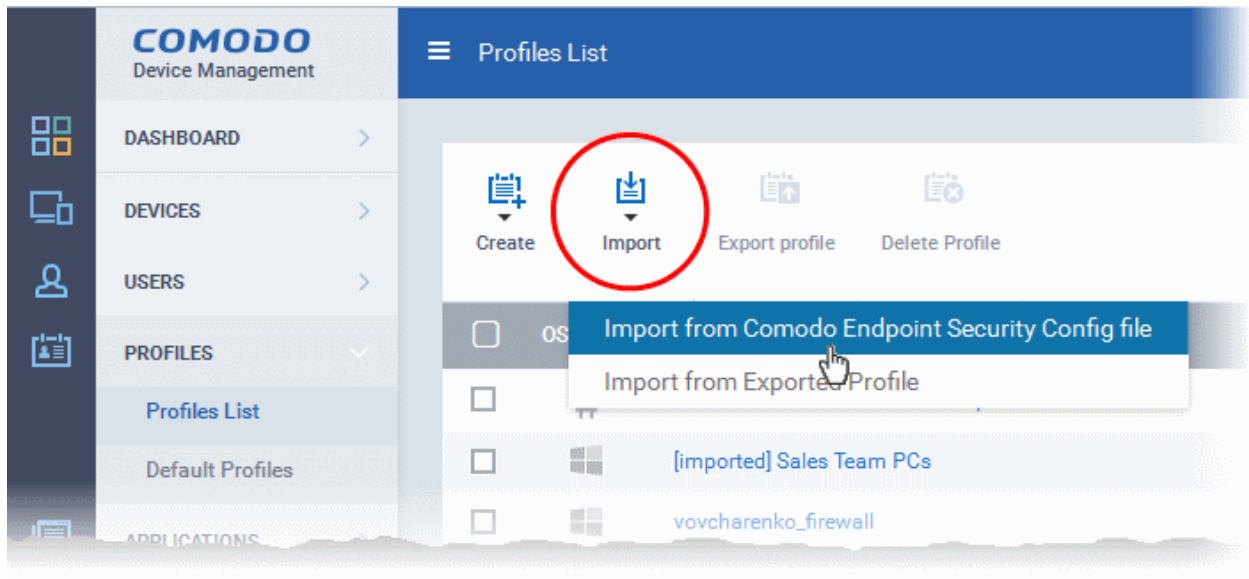
- Configure the security settings of CES at an endpoint. Refer to the page explaining the Advanced Settings in the online help guide of CES at <https://help.comodo.com/topic-84-1-604-7334-Introduction-to-Comodo-Endpoint-Security.html>.
- To export the current configuration as an xml file, run the command on the endpoint as given below:

```
C:\[installation folder of CES]\cfpconfig.exe --xcfgExport="C:\<filename>.xml" --filter=""
```

 For example, C:\Program Files\COMODO\COMODO Internet Security\cfpconfig.exe --xcfgExport="C:\winconfigprofile.xml" --filter=""
- Transfer the .xml file from the endpoint to the computer from which the CDM console is accessed through any out-of-band communication method like email or network file sharing.
- 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)

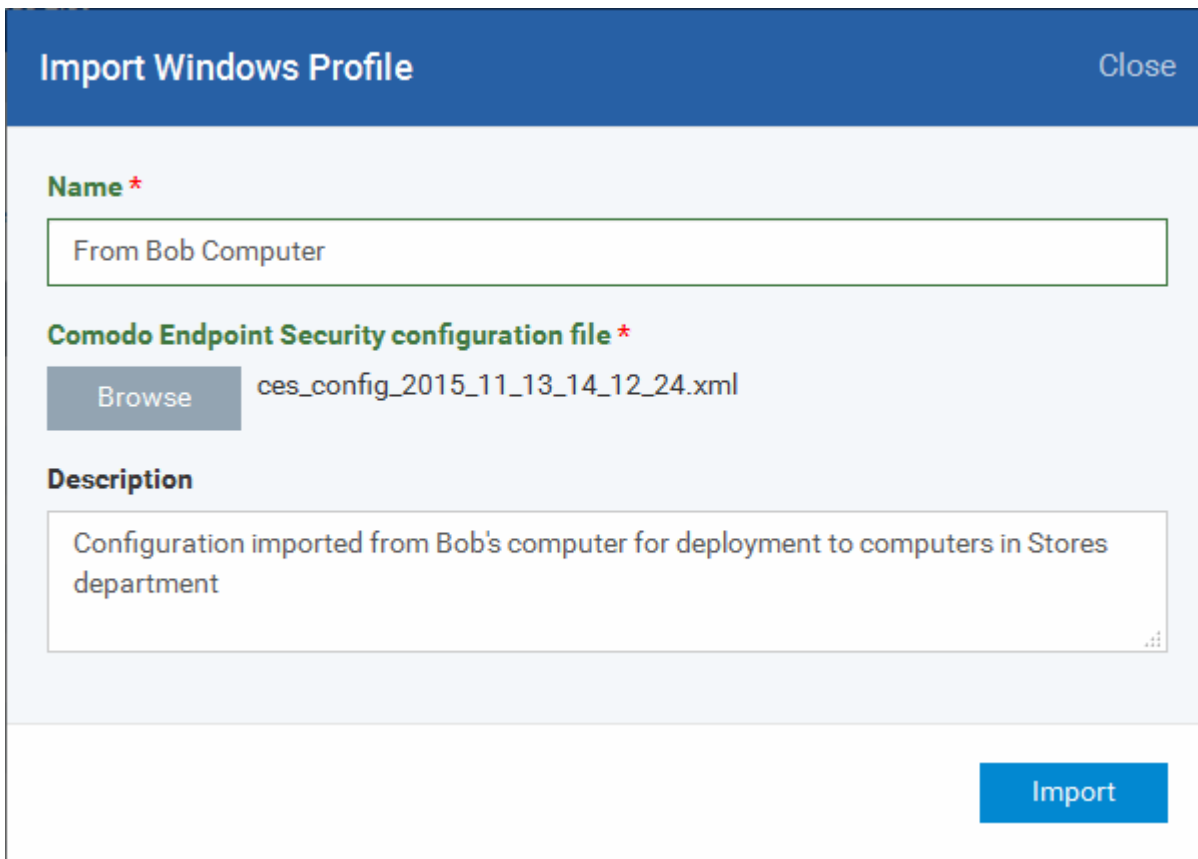
- Open the 'Profiles List' interface in the CDM console by clicking 'Profiles' > 'Profiles List' from the left hand side navigation
- Click 'Import' from the top of the list and choose 'Import from 'Comodo Endpoint Security Config file' from the drop-down



The 'Import Windows Profile' dialog will be displayed:

The 'Import Windows Profile' dialog box is shown. It has a title bar with 'Close' on the right. The 'Name *' field contains 'From Bob Computer'. The 'Comodo Endpoint Security configuration file *' field has a 'Browse' button. The 'Description' field contains 'Configuration imported from Bob's computer for deployment to computers in Stores department'. An 'Import' button is located at the bottom right.

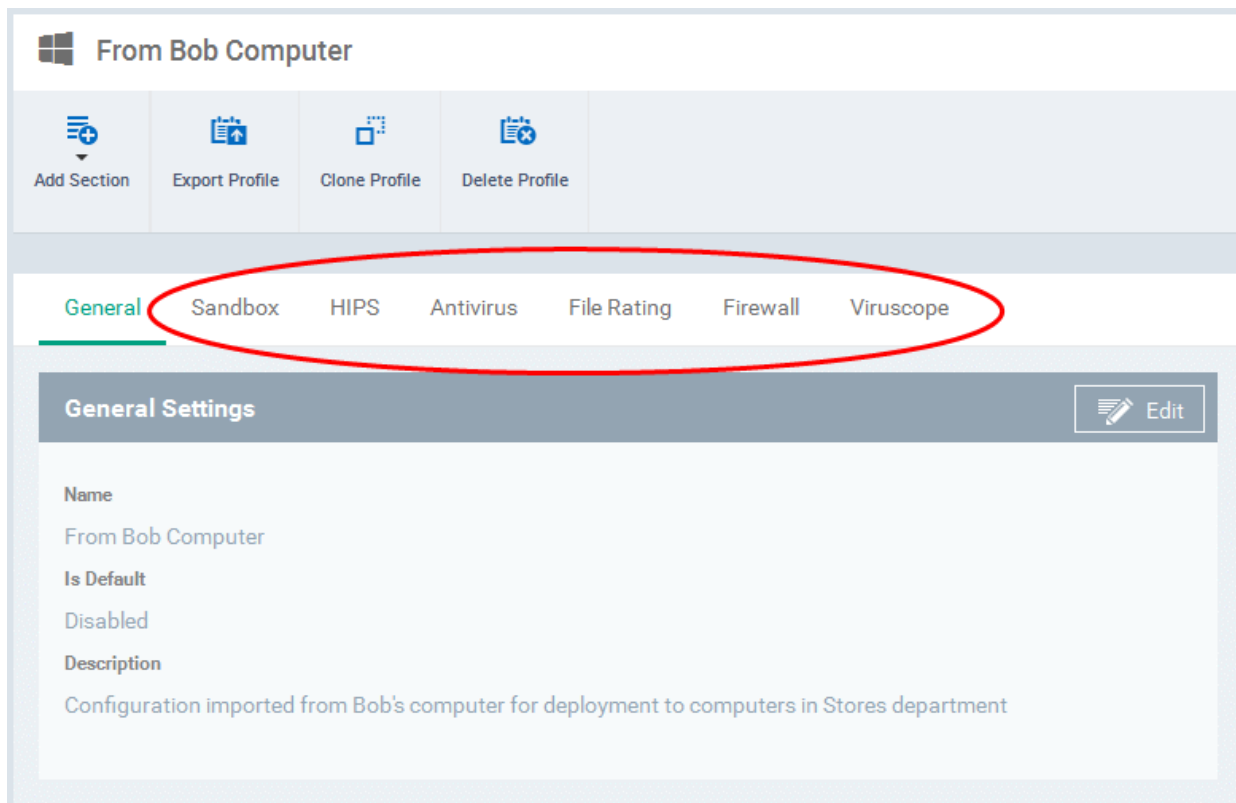
- Enter a name and description for the profile.
- Click 'Browse', navigate to the location in your computer where the .xml file is saved, select the file and click 'Open'.



The selected file will be displayed beside the 'Browse' button.

- Click the 'Import' button.

The Windows Profile interface will open, with the security components pre-configured as per the settings in the configuration file.



- The imported profile will not be in default status. To change the name of the profile and/or to enable it as a default



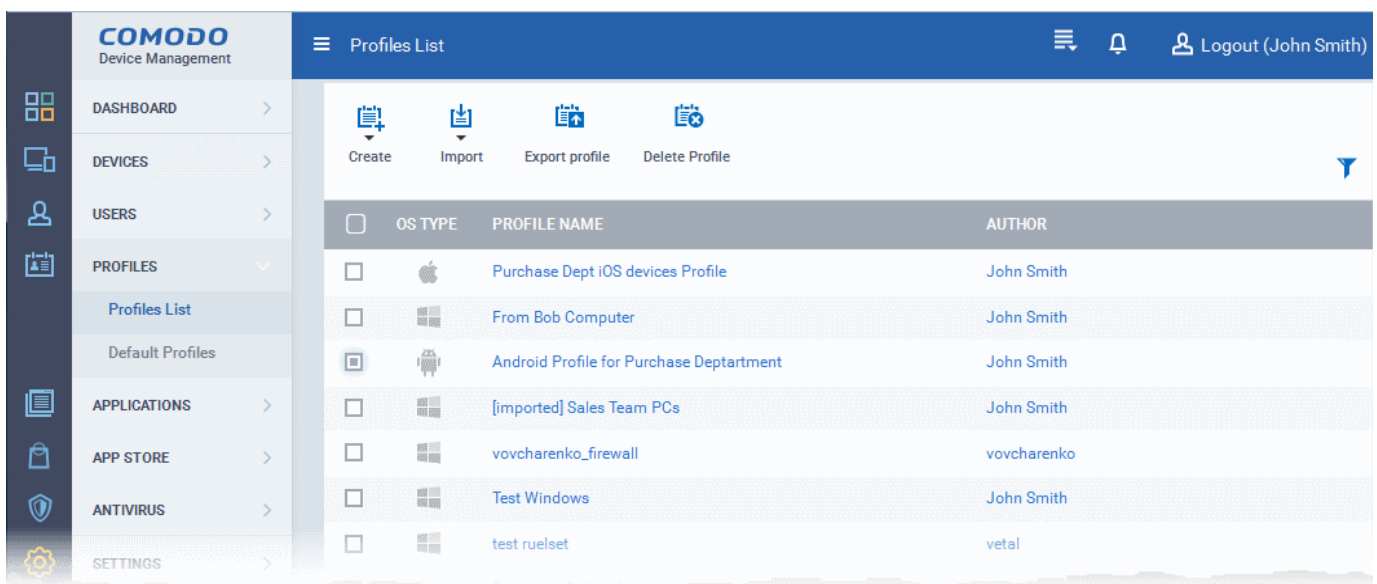
profile, click on the 'Edit' button at the top right of the 'General' settings screen, edit the settings and click the 'Save' button.

- You can add new profile components by clicking 'Add Section' button and/or edit the settings for any security component by clicking the respective 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](#).

6.2. Viewing and Managing Profiles

Profiles that are available for Android, iOS and Windows devices are listed in the 'Profiles List' interface. The screen also allows an administrator to create a new profile, export an existing profile, clone a profile, import a new profile from an exported file and remove a profile.

To open the 'Profiles List' interface, click 'Profiles' from the left and choose 'Profiles List' from the options.

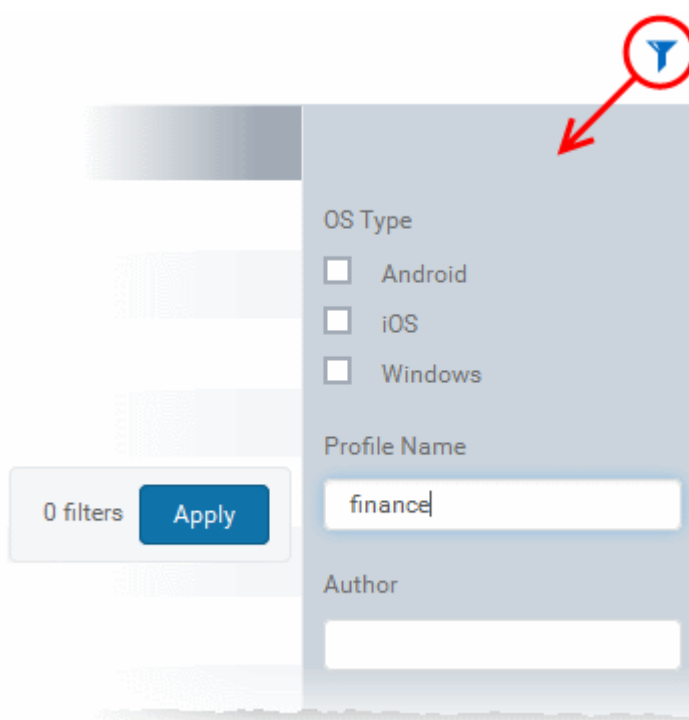


Profiles List - Column Descriptions		
Column Heading	Description	
OS Type	Displays the OS type which the profile supports.	
Profile Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Profile' interface. Refer to the section Editing Configuration Profiles for more details.	
Author	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.	
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 Windows profile	Allows administrators to create a new Windows profile. Refer to the section ' Creating Windows Profiles ' for more details.
Import	Import from Comodo Endpoint Security Config file	Allows administrators to import the security configuration from CES installation from a remote endpoint as a Windows profile. 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.
Export profile		Allows administrators to export 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 profiles in ascending/descending order of entries under it.
- Clicking the funnel icon enables you to search for profiles based on the filter parameters



- To display the profiles that are based on 'Profile Name' and 'Author', enter the text partially or fully in the respective fields and click the 'Apply' button.
- To display the profiles that are based on 'OS' type, select the check box and click the 'Apply' button.

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

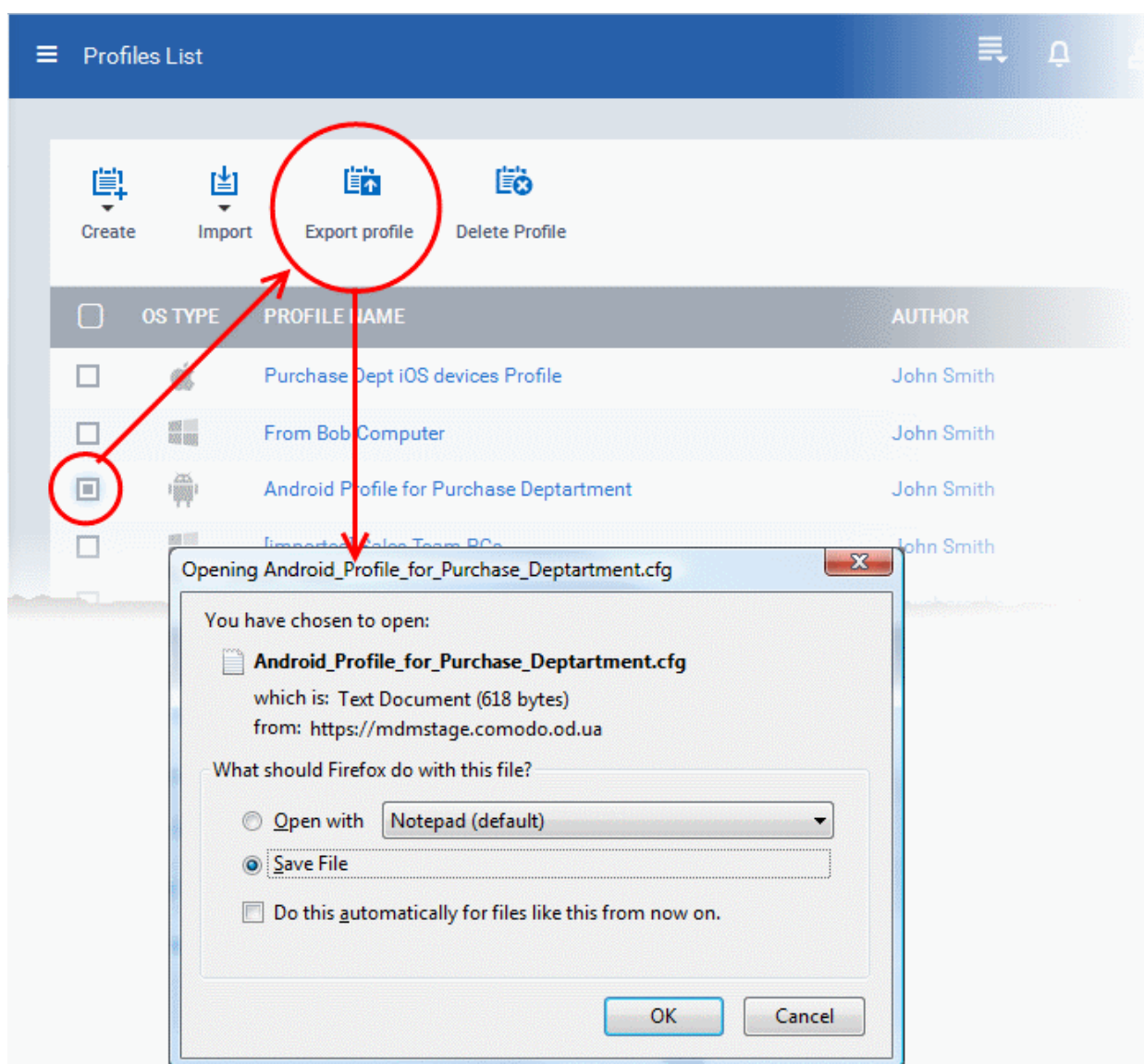
6.2.1. Exporting and Importing Configuration Profiles

Comodo Device Manager allows you to export any of existing Android, iOS and Windows configuration profiles and save it for future implementation. The exported profile can be saved in .cfg format and can be re-imported into CDM console at anytime.

This is useful, for example, if you have created a profile and want it to use at a future time, you can export it and save it as a profile and import it, when required and roll it to managed devices or devices groups as required.

To export a profile

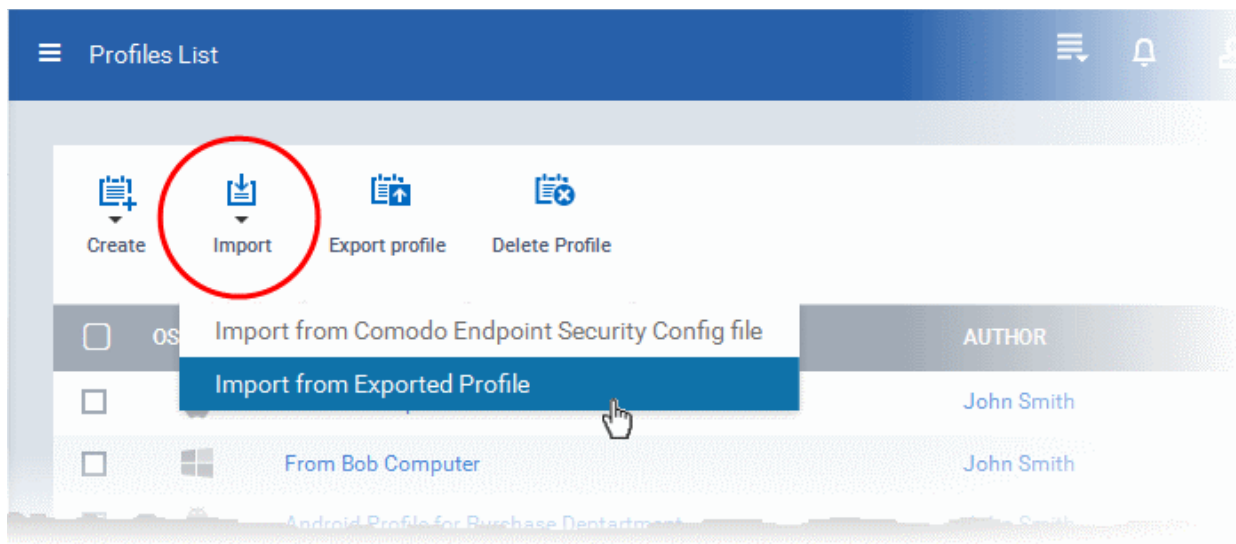
- Open the 'Profiles List' interface by clicking 'Profiles' from the left and choosing 'Profiles List' from the options.
- Select the profile you want to export, from the list and click 'Export profile' from the top.



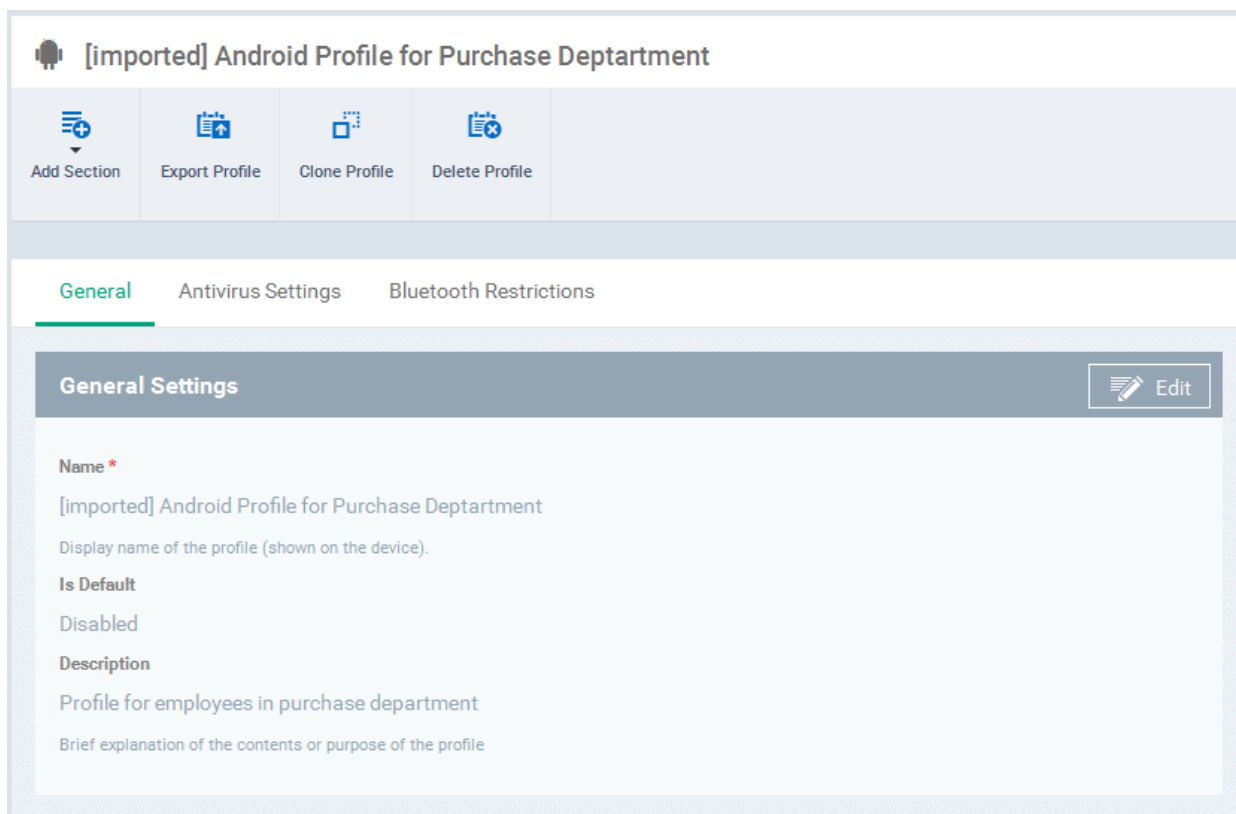
- Save the file at a safe location in .cfg format.


To import a profile from a saved .cfg file

- Open the 'Profiles List' interface by clicking 'Profiles' from the left and choosing 'Profiles List' 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 preconfigured as per the imported profile.



- The imported profile will not be in default status. 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 add new profile components by clicking 'Add Section' button and/or edit the settings for any security component by clicking the respective tab. For more details on the options available under each component, refer to the sections [Profiles for Android Devices](#), [Profiles for iOS Devices](#) and [Profiles for Windows Devices](#).

6.2.2. Cloning a Profile

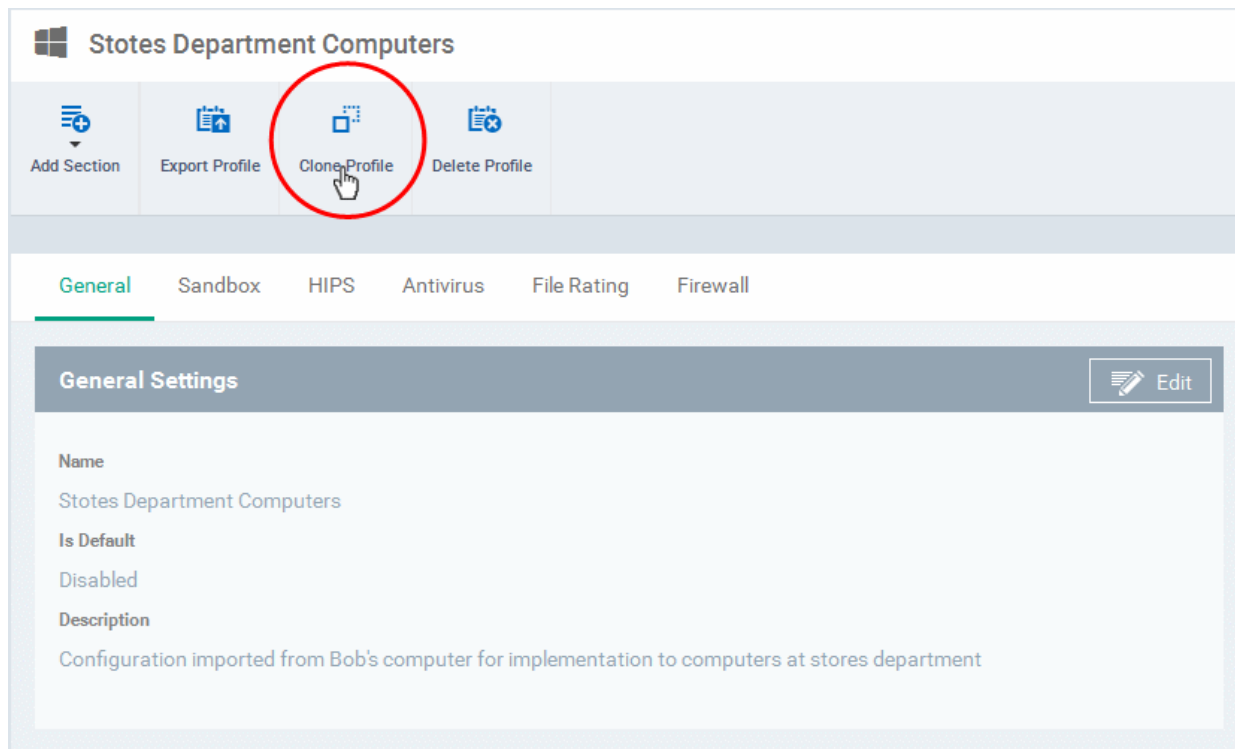
CDM allows you to create new configuration profiles using existing an profile as base and making minor changes to the configuration parameters for deployment on to different managed devices or device groups. You can create a clone of an existing profile and rename and edit the the settings to create the new profile.

To create a clone of a profile


- Open the 'Profiles List' interface by clicking 'Profiles' from the left and choosing 'Profiles List' from the options.
- 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



A new profile will be created bearing the same name with [cloned] as prefix.

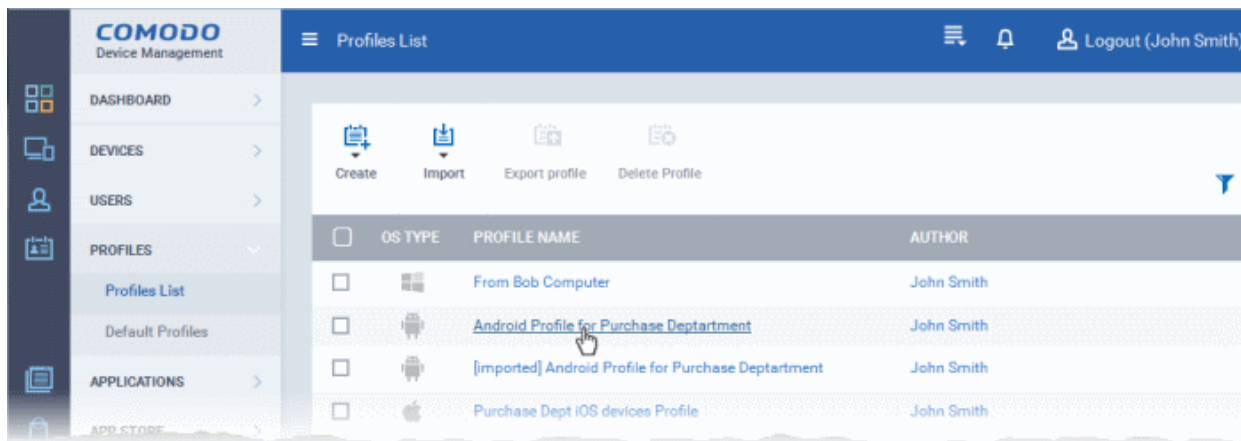
- The cloned profile will not be in default status. To change the name of the profile and/or to enable it as a default profile, click on the 'Edit' button  at the top right of the 'General' settings screen, edit the settings and click the 'Save' button.
- You can add new profile components by clicking 'Add Section' button and/or edit the settings for any security component by clicking the respective tab. For more details on the options available under each component, refer to the sections [Profiles for Android Devices](#), [Profiles for iOS Devices](#) and [Profiles for Windows Devices](#).

6.3. Editing Configuration Profiles

A Profile that is already created can be edited according to the requirements of the organization, for example, for adding or removing security components and changing configuration parameters of the components.

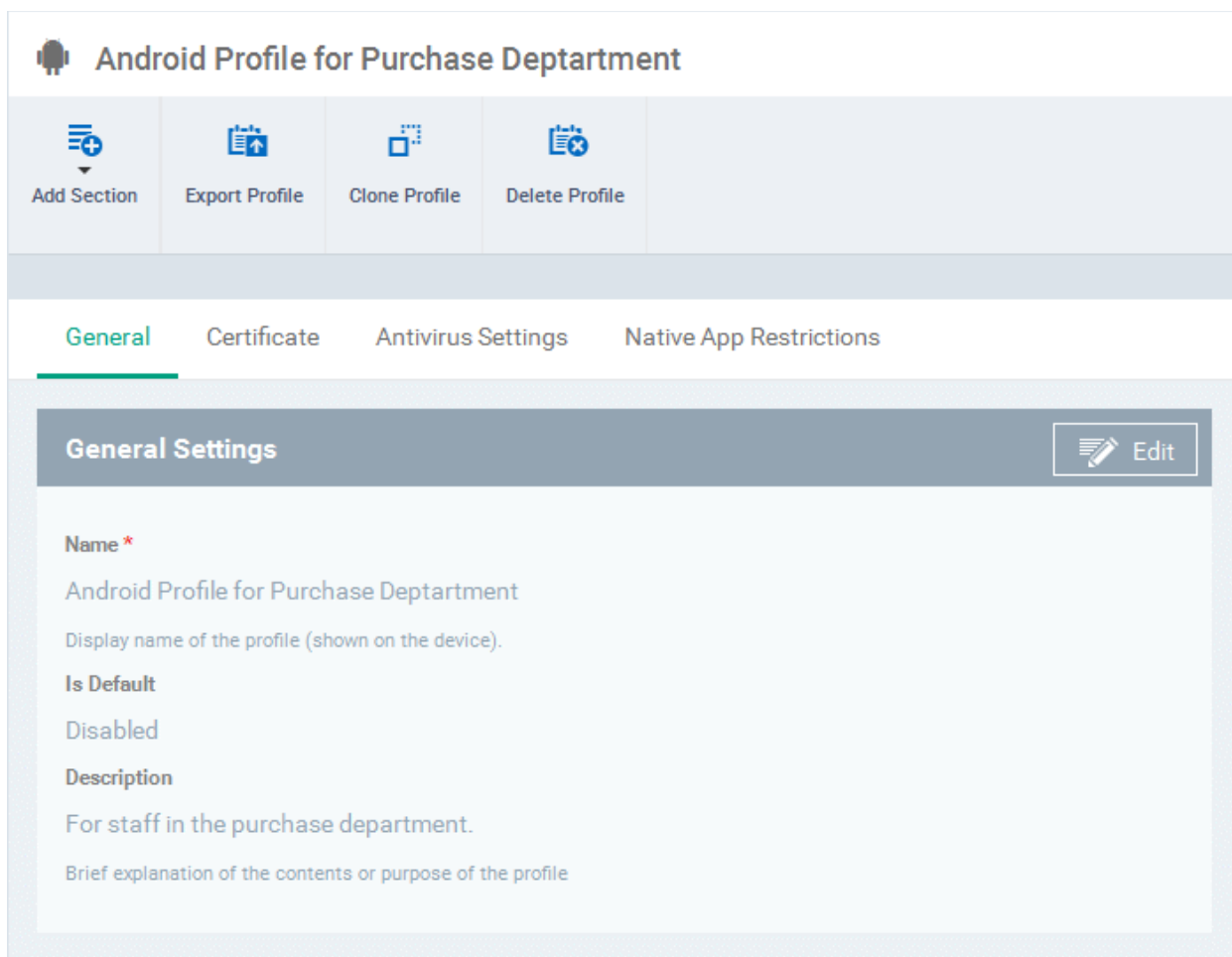
To edit a profile

- Click the 'Profiles' tab from the left and choose 'Profiles List' from the options.
- Click on the name of the profile that you want edit from the list.



The profile settings screen will be displayed.

- Select the component in the profile that you want to edit



The editing steps are similar to creating a new profile. Refer to the sections [Profiles for Android Devices](#), [Profiles for iOS Devices](#) and [Creating Windows Profiles](#) for more details.

- Click 'Save' for your changes to take effect for the profile
- To delete a component from the profile, click 'Delete' from the edit options



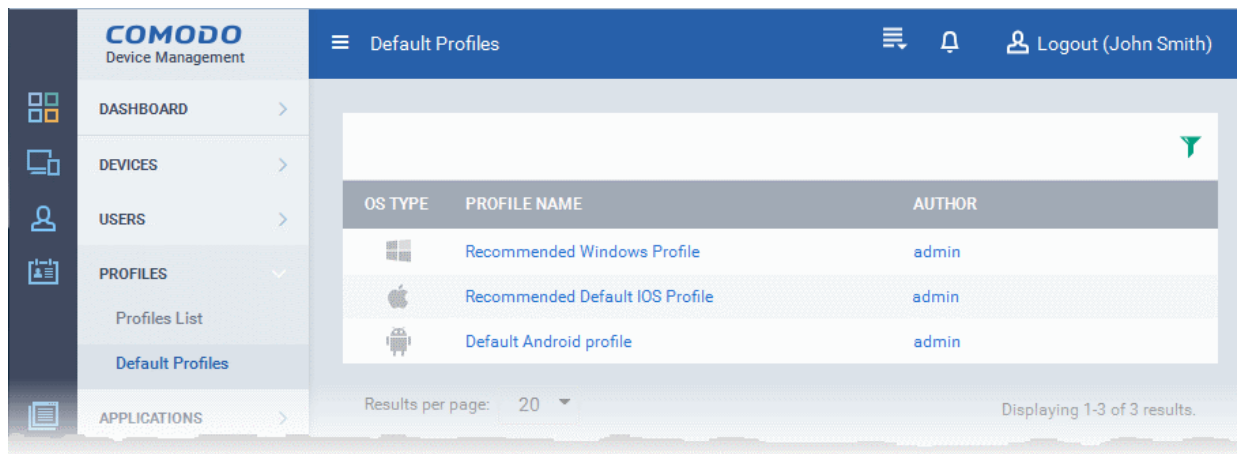
- To delete the profile itself, click the 'Delete Profile' button at the top [Delete Profile](#).

6.4. Managing Default Profiles

Default profiles are very useful if you want to control the newly enrolled devices with certain policies before applying profiles according to the needs of the organization. You can create many default profiles, but make sure the settings in them do not conflict. If the settings in default profiles do conflict, then the Most Restricted policy will be applied. For example, if camera is enabled in a policy and disabled in another, then it will be disabled in the applied devices.

CDM is shipped with a default profile for each OS type and you can make an existing profile as default. When you create a new profile from the 'Profiles' interface, you have the option to make the profile as also a default profile. Default profiles are automatically assigned to devices at the time of enrollment.

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 'Profiles' on the left and then 'Default Profiles' from the options.



The above image displays the default profiles that are shipped with CDM. You can edit a default profile and remove its default status, edit a profile and make it as a default.

Click the following links for more details:

- [Creating a default profile](#)
- [Viewing list of default profiles](#)
- [Assigning default profiles to devices](#)
- [Removing a default profile](#)

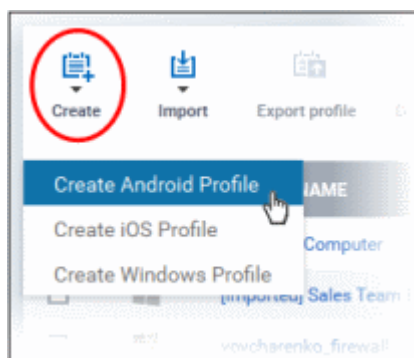
Creating a default profile

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 'Profile' on the left and then choose 'Profiles List' from the options
- Choose the type of profile that you want to create from the 'Create' drop-down

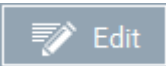


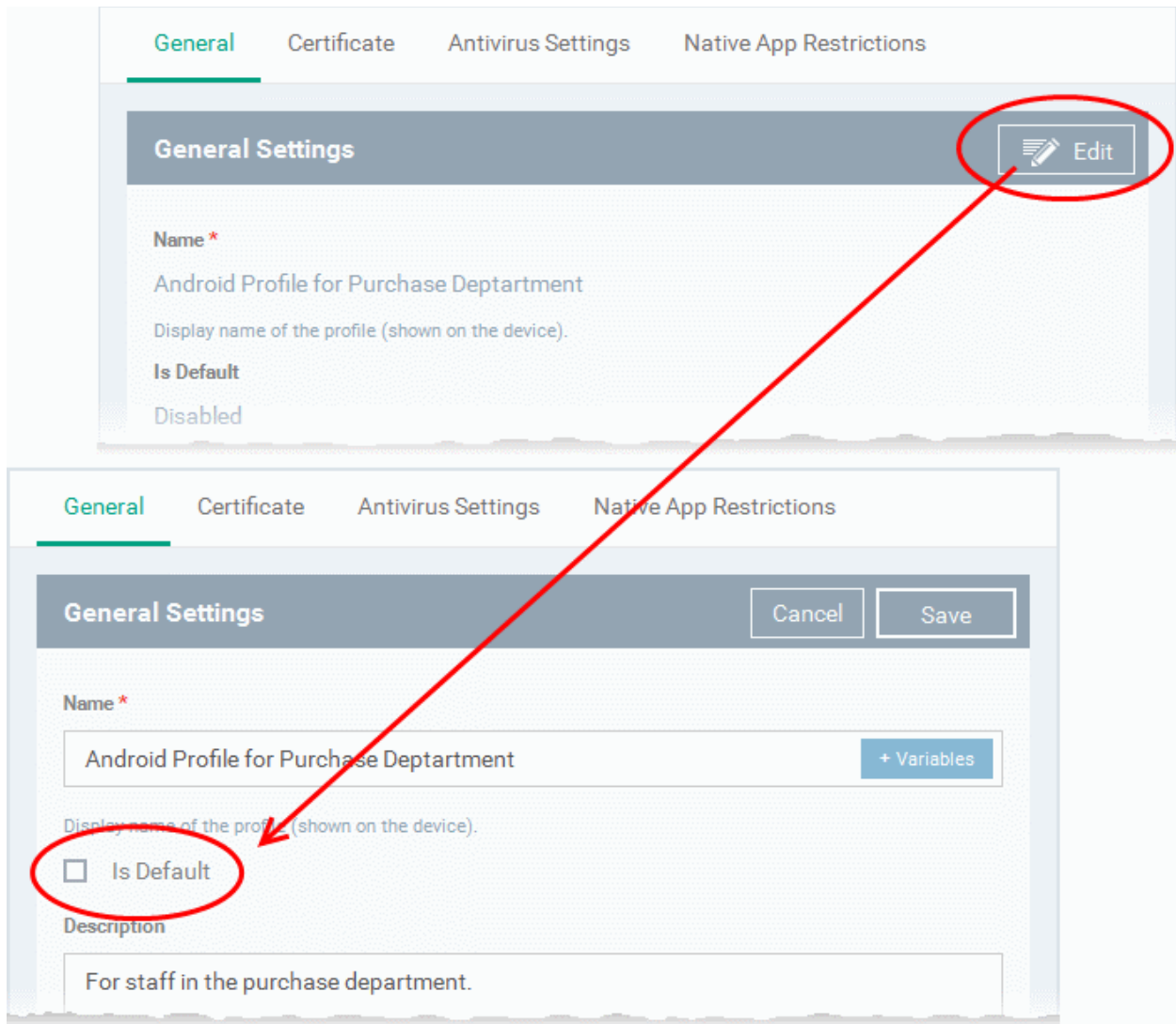
The 'Create OS Profile' screen will be displayed.

A screenshot of the 'Create Android Profile' dialog box. The dialog has a blue title bar with the text 'Create Android Profile' and a 'Close' button on the right. Below the title bar, there are two text input fields. The first is labeled 'Name' and has a red asterisk next to it. The second is labeled 'Description'. At the bottom right of the dialog, there is a blue button labeled 'Create'.

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

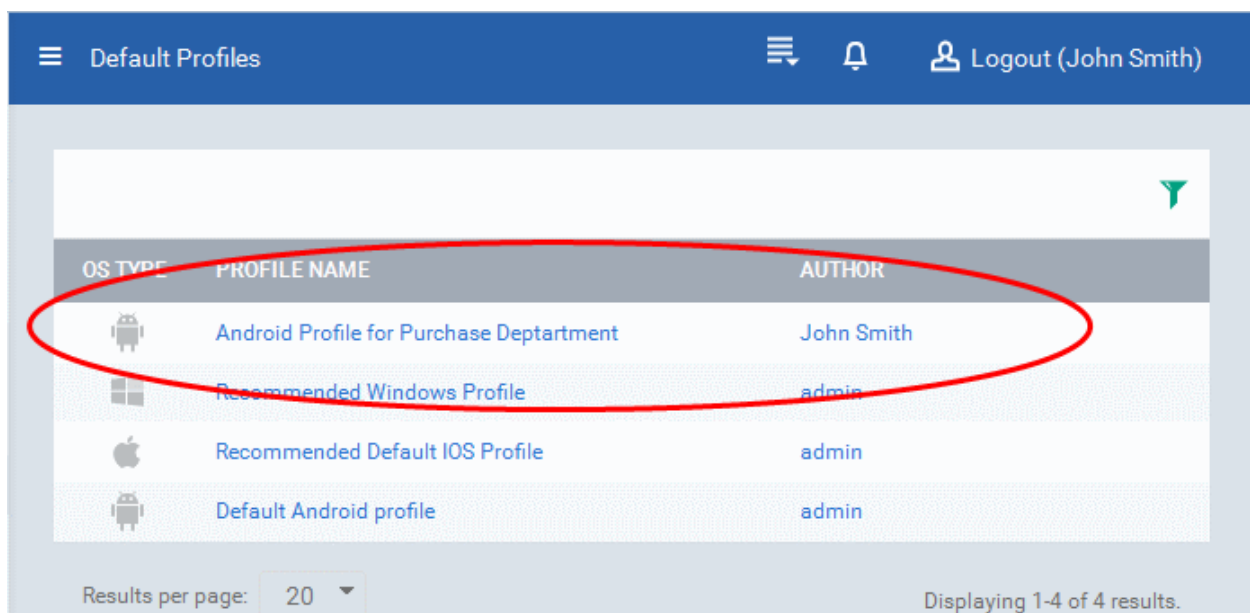
The selected OS type profile will be created and the 'General Settings' section will be displayed with its default profile status as disabled.

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



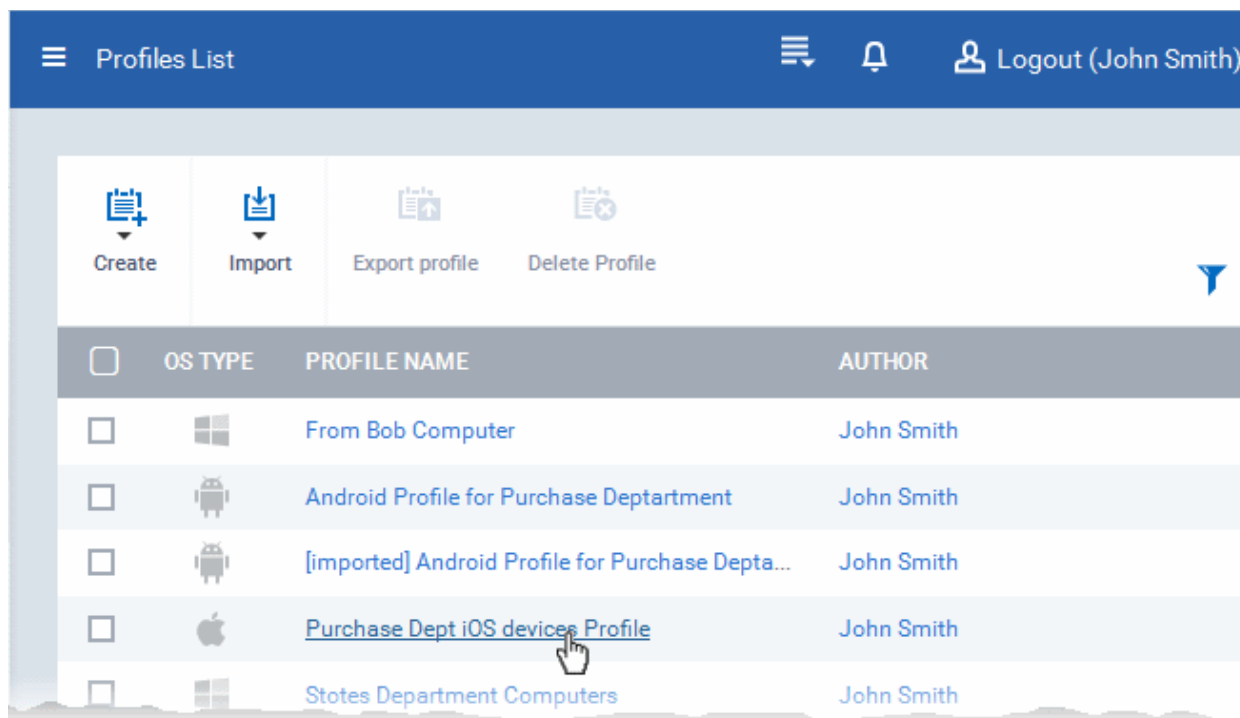
- Click the 'Save' button.

The profile will be saved as a 'Default Profile' and listed in the 'Default Profiles' screen.



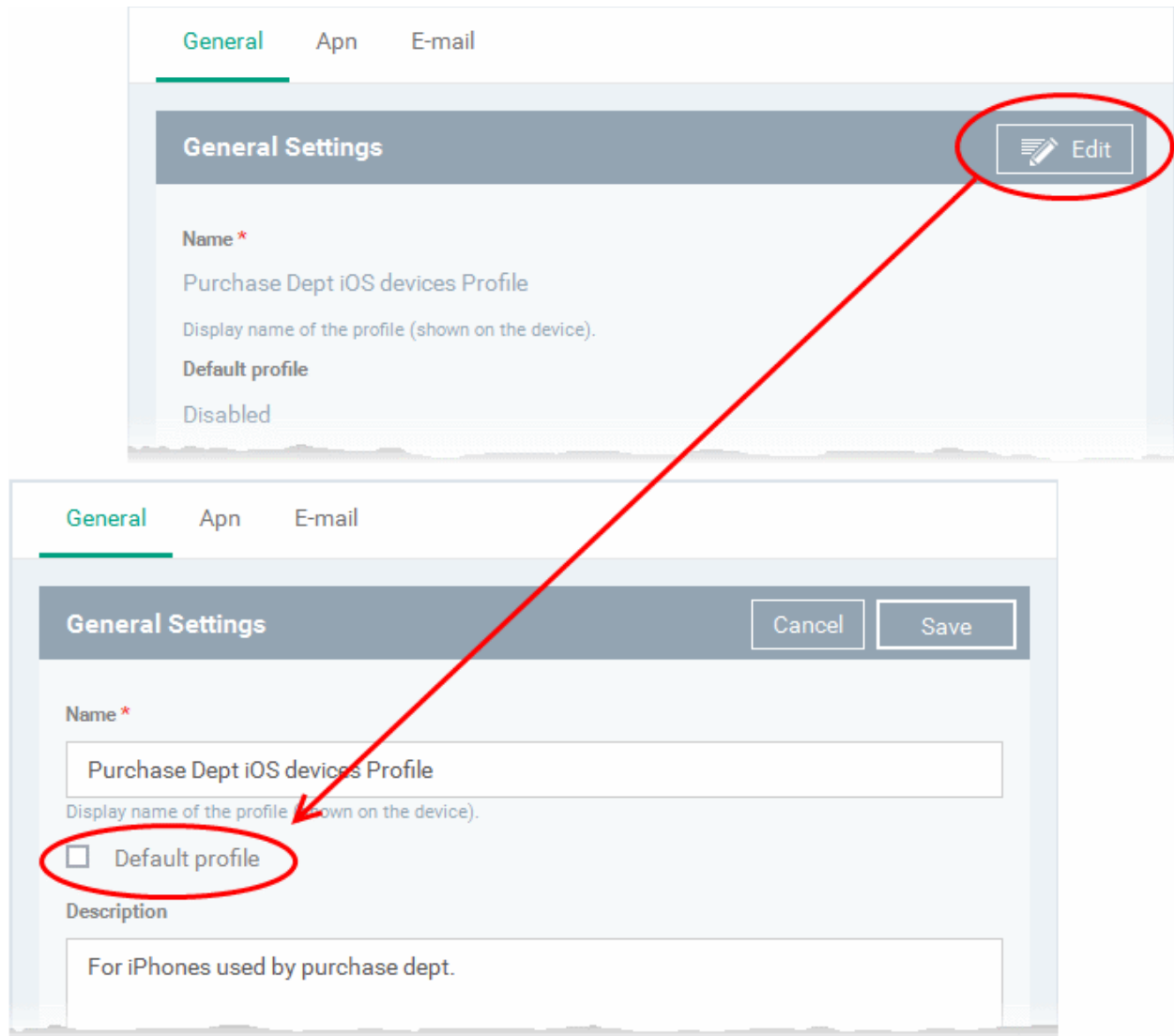
To create a default profile from the existing profiles screen

- Click 'Profile' on the left and choose 'Profiles List' from the options
- Click on the profile name that you want make as a default profile



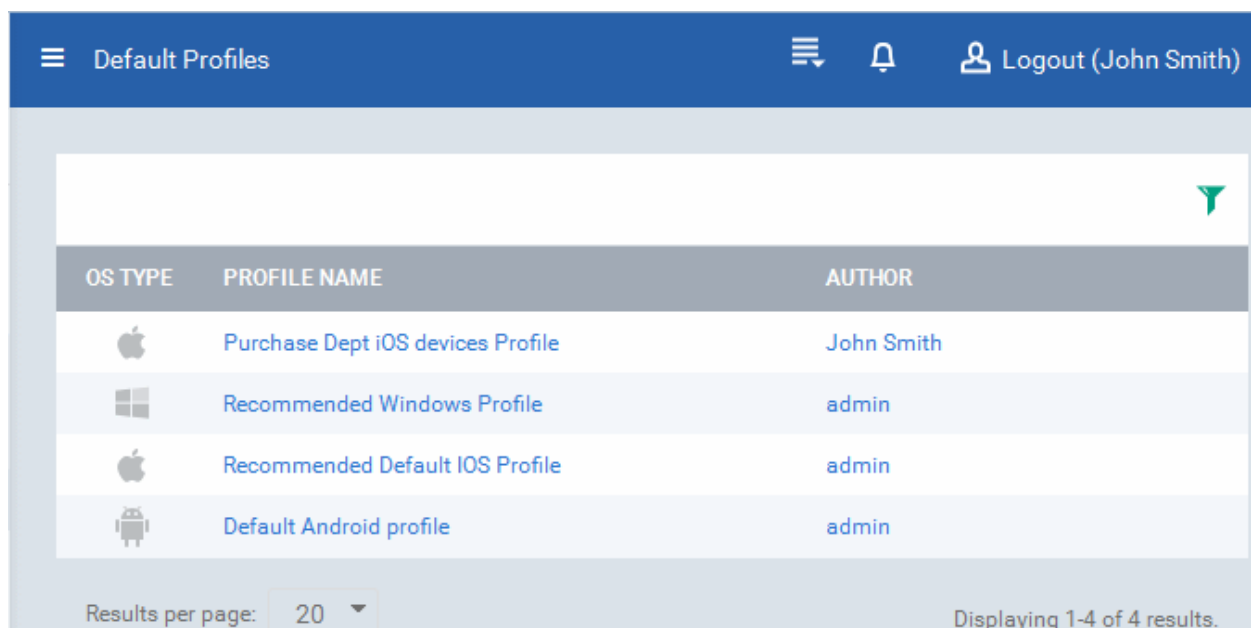
The profile settings screen of the selected profile will be displayed.

- Click the 'Edit' button  at the top right of the 'General' settings screen



- Select the box beside 'Default profile'
- Click the 'Save' button.

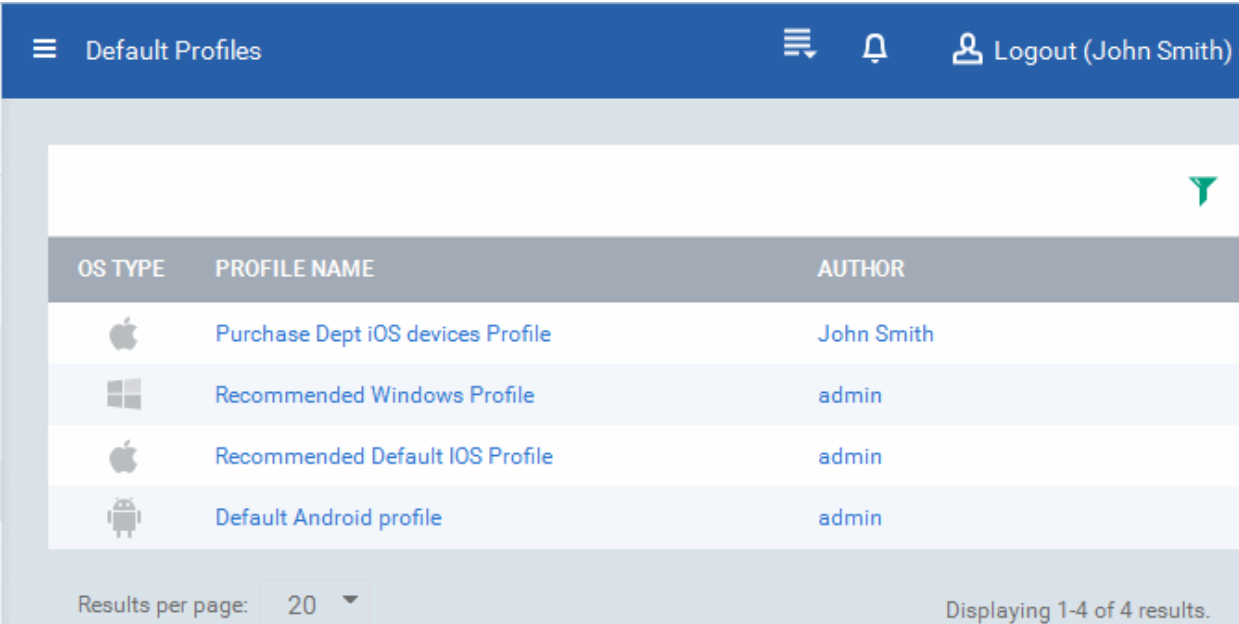
The profile will be saved as a 'Default Profile' and listed in the 'Default Profiles' screen.







To view the list of default profiles

- Click 'Profiles' from the left and choose 'Default Profiles' from the options

The list of default profiles will be displayed.



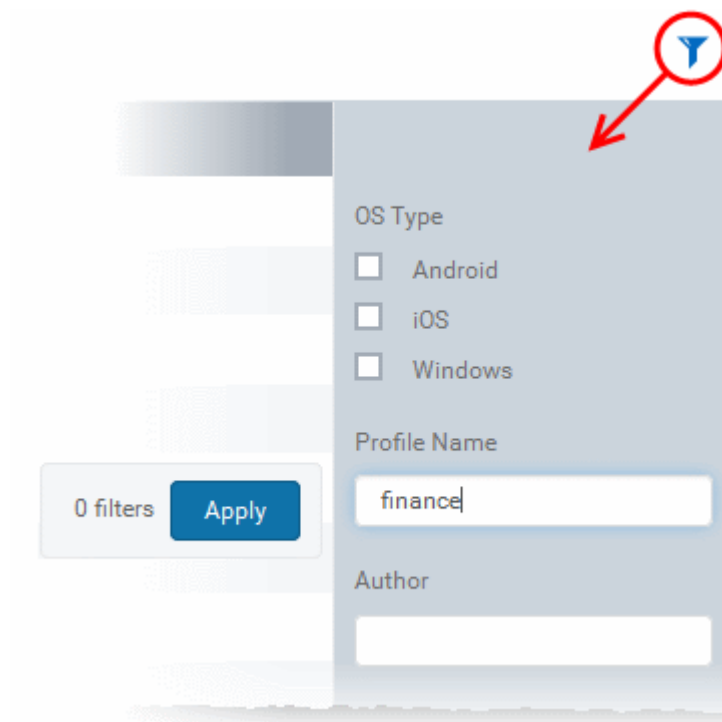
OS TYPE	PROFILE NAME	AUTHOR
	Purchase Dept iOS devices Profile	John Smith
	Recommended Windows Profile	admin
	Recommended Default IOS Profile	admin
	Default Android profile	admin

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

Profiles - Column Descriptions	
Column Heading	Description
OS Type	Displays the OS type which the profile supports.
Profile 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.
Author	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.

Sorting, Search and Filter Options

- Clicking on any of the column headers will sort the profiles in ascending/descending order of entries under it.
- Clicking the funnel icon enables you to search for profiles based on the filter parameters



- To display the profiles that are based on 'Profile Name' and 'Author', enter the text partially or fully in the respective fields and click the 'Apply' button.
- To display the profiles that are based on 'OS' type, select the check box and click the 'Apply' button.

The profiles that matches the entered/selected parameters will be displayed in the screen.

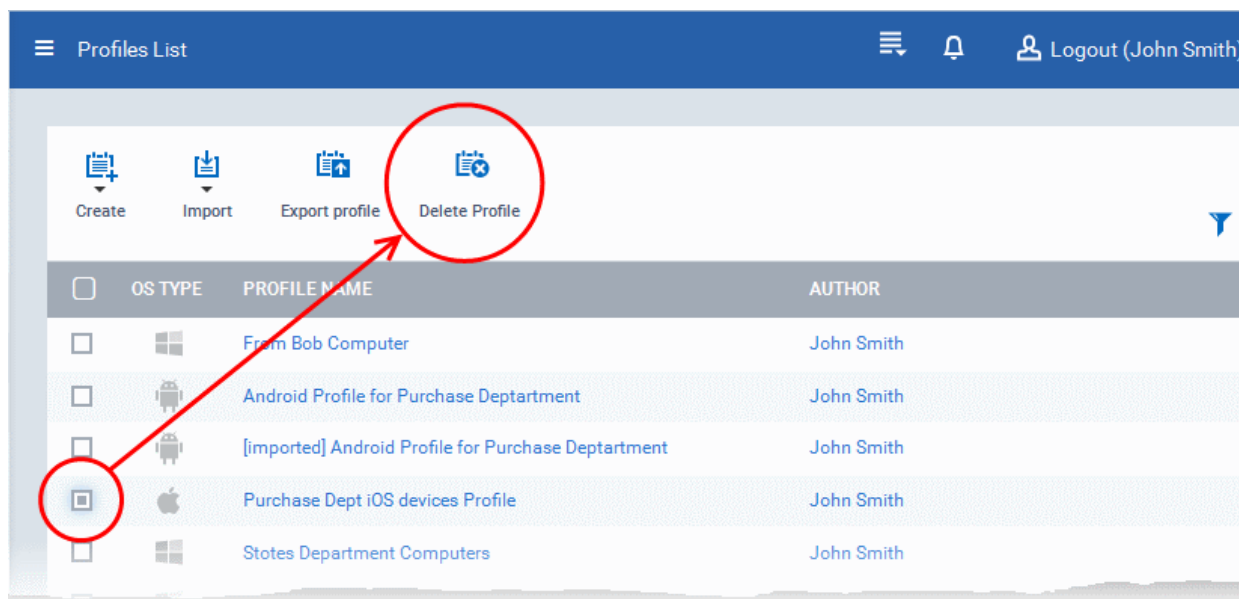
- To display all the profiles again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the filter options

Assigning default profiles to devices

Devices that are enrolled for the first time will be automatically assigned the default profiles according to their operating system. These default profiles will be automatically overridden by the profiles that are assigned to the devices by the administrator according the organizational requirements. Please note the default profiles that were installed initially will be 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 'Profiles list' screen.



- Select the check box beside the default profile in the '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 list' too. Please note that even if default profile(s) are removed from the list, the device(s) will still retain the configured settings from the profiles till a new profile(s) are assigned to them.

7. Applications

Comodo Device Manager (CDM) provides visibility and control to the administrator over the applications and files installed on the users' devices. The 'Applications' tab allows the administrator to:

- View the list of all the applications that are currently installed on all the enrolled mobile Android and iOS devices, identify malicious applications installed on enrolled devices and blacklist them. Once blacklisted, the application will not be allowed to run on all the device(s) on which it is installed.
- View the lists of applications and files discovered from the managed Windows devices under Unrecognized, Trusted and Malicious categories as categorized by the CES installation at the devices. The administrator can move the files between the categories based on their analysis.
- View the list of files that were run inside the sandbox at the managed Windows endpoints
- View the list of software vendors of the applications discovered from managed Windows devices with their trust status and mark them as trusted/untrusted. Applications from the untrusted vendors will also be treated as 'Untrusted' by the CES installations at the endpoint.
- View the constantly updated list of Windows patches available for deployment to managed Windows devices and install selected patches on to the devices.

The screenshot displays the 'Mobile Applications' section of the Comodo Device Manager. The left sidebar contains navigation options: DASHBOARD, DEVICES, USERS, PROFILES, APPLICATIONS (with a sub-menu for Mobile Applications, Windows File List, Windows Sandbox History, Software Publishers, and Patch Management), APP STORE, ANTIVIRUS, and SETTINGS. The main content area shows a table of applications with the following columns: OS TYPE, NAME, PACKAGE, NUMBER OF DEVICE, and BLACK LIST TYPE. Above the table are three action buttons: 'Add To Black List', 'Remove From Black List', and 'Push List To All Devices'. The table lists ten applications, all with a 'BLACK LIST TYPE' of 'Allowed'.

<input type="checkbox"/>	OS TYPE	NAME	PACKAGE	NUMBER OF DEVICE	BLACK LIST TYPE
<input type="checkbox"/>	Android	ES File Explorer	com.estrongs.and...	2	Allowed
<input type="checkbox"/>	Android	Evernote	com.evernote	2	Allowed
<input type="checkbox"/>	Android	Skype	com.skype.raider	2	Allowed
<input type="checkbox"/>	Android	RepoTest	com.nikedlab.Rep...	2	Allowed
<input type="checkbox"/>	Android	VK	com.vkontakte.an...	1	Allowed
<input type="checkbox"/>	Android	FilmOn Family Live	com.filmon.lenov...	1	Allowed
<input type="checkbox"/>	Android	Kingsoft Office	cn.wps.moffice_j1...	1	Allowed
<input type="checkbox"/>	Android	2GIS	ru.dublgis.dgismo...	1	Allowed
<input type="checkbox"/>	Android	IMAX	com.planet.imax	1	Allowed
<input type="checkbox"/>	Android	Calculator MobiCalc	my.android.calc	1	Allowed

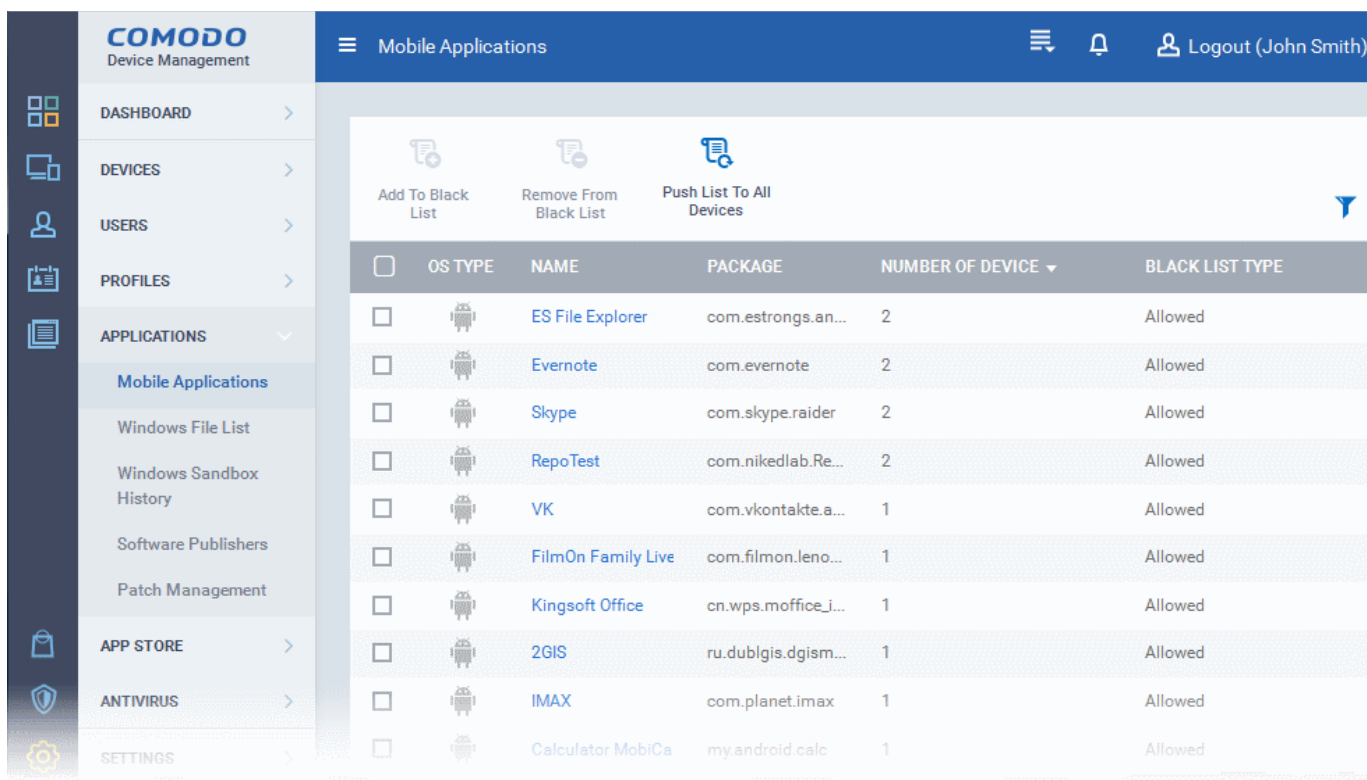
Following sections explain in detail on:

- [Viewing Applications Installed on Android and iOS Devices](#)
 - [Blacklisting and Whitelisting Applications](#)
- [Viewing Applications Installed on Windows Devices](#)
 - [Viewing and Managing Unrecognized Files](#)
 - [Viewing and Managing Trusted Files](#)
 - [Viewing and Managing Malicious Files](#)
 - [Viewing list of Valkyrie Analyzed Files](#)
- [Viewing and Managing Sandboxed Applications on Windows Devices](#)
- [Viewing and Managing Software Vendors List](#)

7.1. Viewing Applications Installed on Android and iOS Devices


The 'Mobile Applications' interface displays a list of all the applications identified from all the enrolled Android and iOS devices with details like the package name and number of devices on which the app is found. The administrator can determine authenticity of the applications and blacklist the applications found 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.

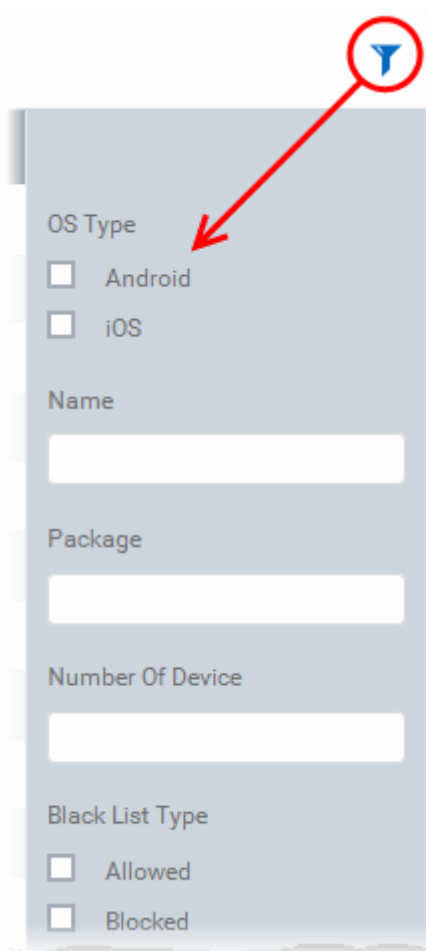
To access the 'Mobile Applications' interface, click the 'Applications' tab from the left and choose 'Mobile Applications' from the options.



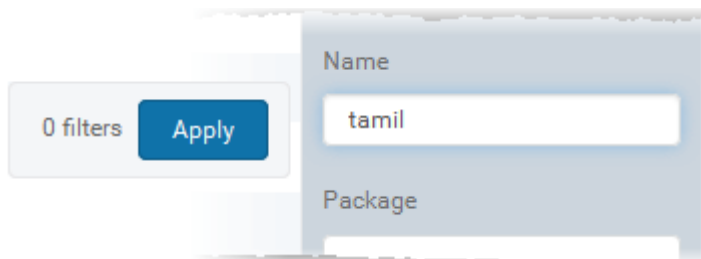
Mobile Applications interface - Column Descriptions	
Column Heading	Description
OS Type	Indicates OS type of the app.
Name	Name of the application. Clicking the name of an application opens the ' Devices ' interface with a list of only those devices on which the app is installed, enabling the administrator 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.
Blacklist Type	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 of the devices to be displayed in the list.
- To filter the items based on their blacklist status, select the state under 'Blacklist Type'

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 CDM 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 blacklist.

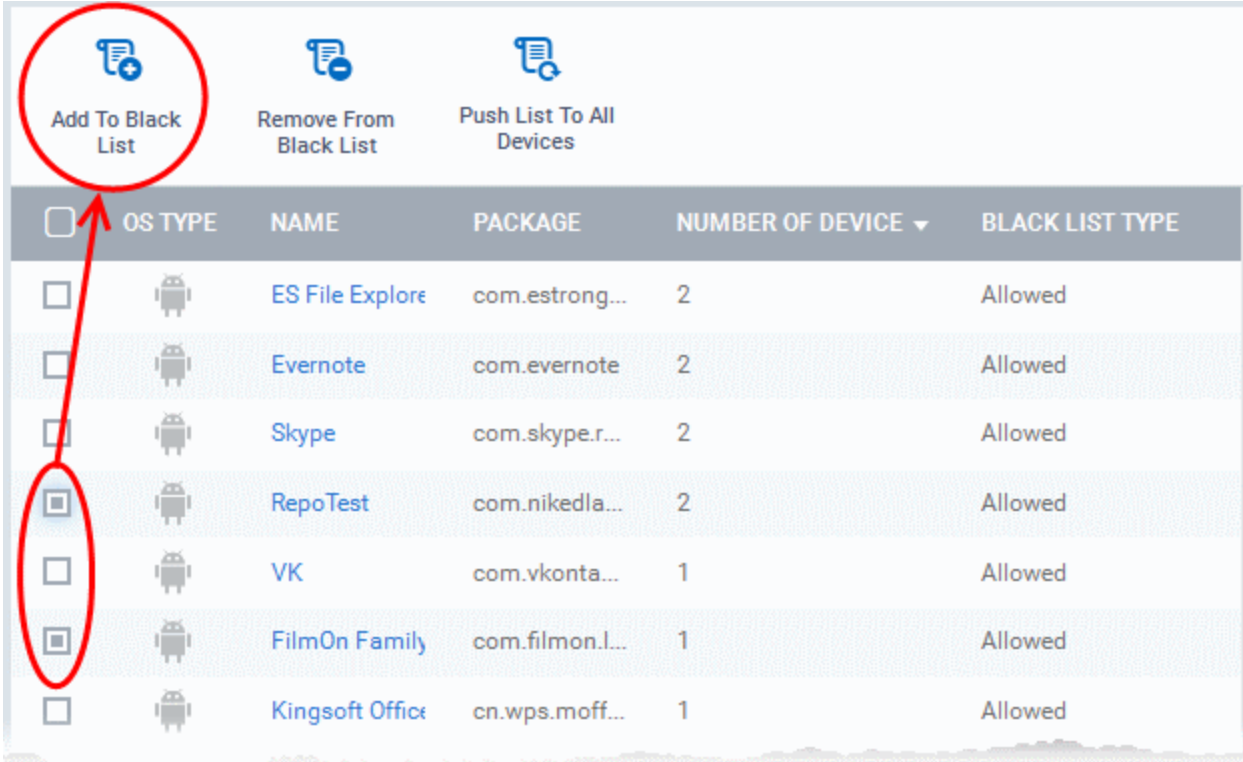
7.1.1. Blacklisting and Whitelisting Applications

The 'Mobile Applications' interface displays all the apps that are installed on or removed from all the enrolled devices. The administrator can analyze the list and if any suspicious or malicious application is identified, administrator can block the application in the devices in which they are installed and prevent other devices to install the application in future, by moving it to the blacklist.

The blacklisted files can be moved to whitelist and allowed to run at the devices, if they are find trustworthy at a later time.

To move selected apps to blacklist

- Click the 'Applications' tab from the left and choose 'Applications' from the options.
- Select the apps to be black listed.

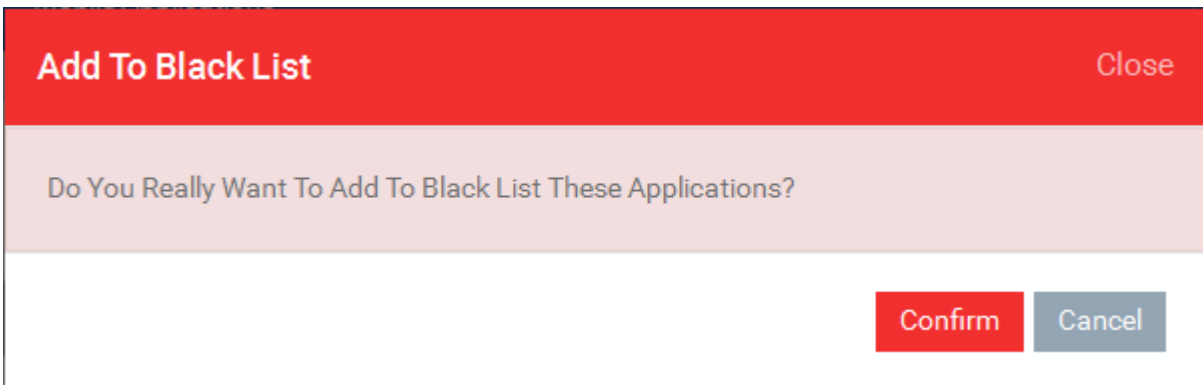


<input type="checkbox"/>	OS TYPE	NAME	PACKAGE	NUMBER OF DEVICE	BLACK LIST TYPE
<input type="checkbox"/>	Android	ES File Explore	com.strong...	2	Allowed
<input type="checkbox"/>	Android	Evernote	com.evernote	2	Allowed
<input type="checkbox"/>	Android	Skype	com.skype.r...	2	Allowed
<input checked="" type="checkbox"/>	Android	RepoTest	com.nikedla...	2	Allowed
<input type="checkbox"/>	Android	VK	com.vkonta...	1	Allowed
<input checked="" type="checkbox"/>	Android	FilmOn Family	com.filmon.l...	1	Allowed
<input type="checkbox"/>	Android	Kingsoft Office	cn.wps.moff...	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' option from the top.

A confirmation dialog will appear.



Add To Black List Close

Do You Really Want To Add To Black List These Applications?

Confirm Cancel

- Click 'Confirm'.

The selected apps will be included to the Black List and their status will change to 'Blocked'

- To block the apps immediately in the devices on which they are installed, click 'Push List to All Devices' from the options at the top.

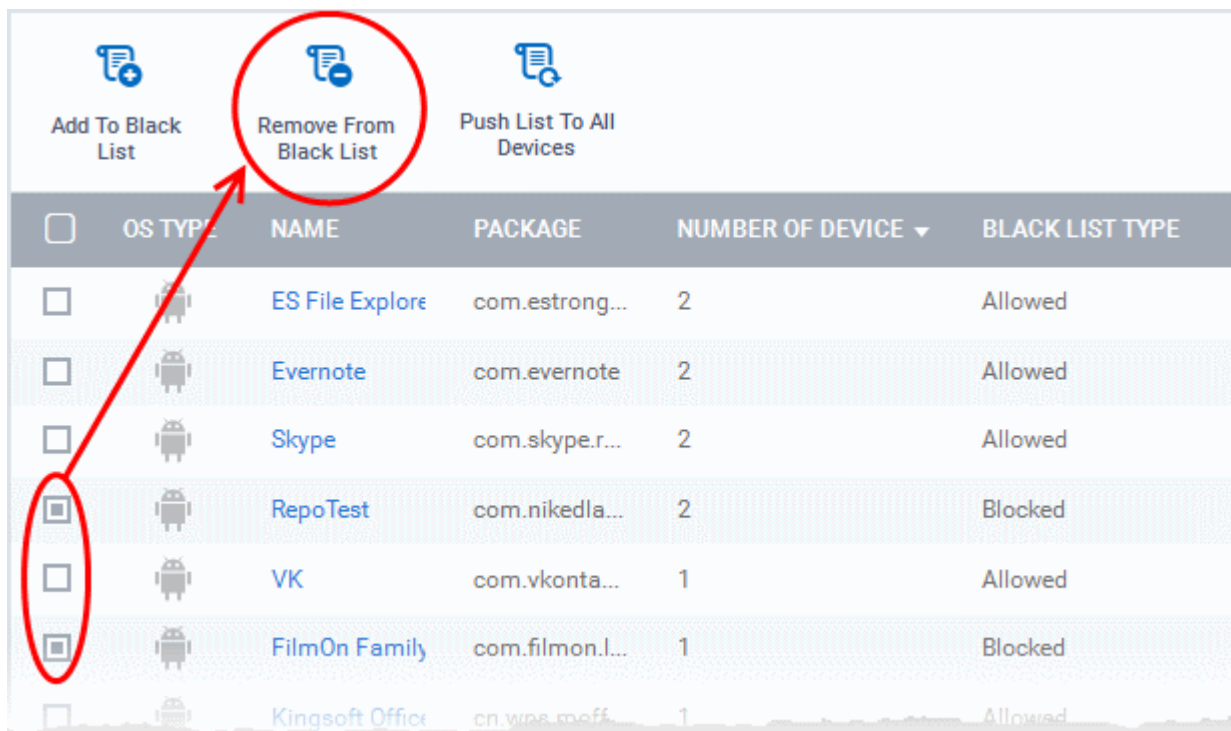
Unblocking Blacklisted Apps

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 in the devices.

To remove trustworthy apps from blacklist

- Click the 'Applications' tab from the left and choose 'Mobile Applications' from the options.
- Select the apps with 'Blocked' status, to be whielisted.



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 'Remove From Black List' from the options 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' from the options at the top.

7.2. Viewing Applications Installed on Windows Devices

The CES installation at each enrolled Windows device watches all file system activities at the endpoint. Every new executable file introduced to the computer, is first scanned against the Comodo certified safe files database and rated as 'Unrecognized', 'Trusted' or 'Malicious' as configured in the File Rating settings in the configuration profile active on the endpoint. Refer to the explanation of **File Rating settings** in the section **Creating a Windows Profile** for more details.

The 'Windows File List' interface allows the administrator to view consolidated lists of all the items that are rated as 'Unrecognized', 'Trusted' or 'Malicious' by the CES installations at all the endpoints. The administrator can analyze the trustworthiness of the items and move the files between to the lists depending on the nature of the files. The files added to the 'Trusted Files' list are automatically given trusted status and are allowed to run without generating any alert. File added to the 'Malicious' Files list are prohibited to run at all the endpoints.

The Windows File List also allows to view the list of files uploaded from the managed Windows devices to Valkyrie for analysis as per the Valkyrie component settings in the profile active on them and the analysis results from Valkyrie. Refer to the explanation of **Valkyrie Settings** in the section **Creating a Windows Profile** for more details.

To access the 'Windows File List' interface, click the 'Applications' tab from the left and choose 'Windows File List' from the options.

FILE NAME	FILE PATH	AGE	SHA1	VERSION	ADMIN RATING	SIZE	# DEVICES
jom.exe	C:\Qt\Tools\QtCreator\bin\jom...	21 days	D79CBFD32FB39A20...		No	2.46 MB	2
qtcreator_ct...	C:\Qt\Tools\QtCreator\bin\qtr...	21 days	70F6C2E5BC76536D...		No	8.5 KB	2
qtcreator.exe	C:\Qt\Tools\QtCreator\bin\qtr...	21 days	D9F9D27737074BC7...		No	808.5 KB	2
CDMAgent.e...	C:\Program Files (x86)\COMO...	16 days	413432E2B570A207...	5.0.0.0	No	1.57 MB	2
CDM (1).msi	C:\Users\Alex\Downloads\CD...	17 days	D8A1898E5CC2277C...		No	21.77 MB	1
AM_Delta_P...	C:\Windows\SoftwareDistribut...	17 days	DFD1F4B70E7CB59B...	1.213.293.0	No	677.27 KB	1
CDM (4).msi	C:\Users\WIN7_X64_MAKS\De...	17 days	80702C0BE94155FF...		No	21.77 MB	1
CDMAgent.e...	C:\Program Files (x86)\COMO...	18 days	62D0D66D372A727E...	4.5.1337.2667	No	1.57 MB	3
CDMAgent.e...	C:\Program Files (x86)\COMO...	18 days	8DEF70D025054E5C...	5.0.1360.2678	No	1.57 MB	6

The interface contains four tabs:

- **Unrecognized** - Displays the list of files reported as 'Unrecognized' by the CES installations at the endpoints. The administrator can move items to 'Trusted Files' list or 'Malicious Files' list, depending on the trustworthiness of the files from this interface. Refer to the section [Viewing and Managing Unrecognized Files](#) for more details.
- **Trusted** - Displays the global 'Trusted Files' list. The administrator can move items to this list from Unrecognized Files or Malicious Files lists. Refer to the section [Viewing and Managing Trusted Files](#) for more details.
- **Malicious** - Displays the global 'Malicious Files' list. The administrator can manually add files or move items to this list from Unrecognized Files or Trusted Files lists and move false positives to Unrecognized Files or Trusted Files lists. Refer to the section [Viewing and Managing Malicious Files](#)
- **Valkyrie Processed Files** - Displays the list of unknown files uploaded by managed Windows devices for cloud based analysis by Valkyrie with their results from Valkyrie. Refer to the section [Viewing List of Valkyrie Analyzed Files](#) for more details.

7.2.1. Viewing and Managing Unrecognized Files

The 'Unrecognized' interface displays a consolidated list of unrecognized files reported by the CES installations at the endpoints.


To open the Unrecognized Files interface

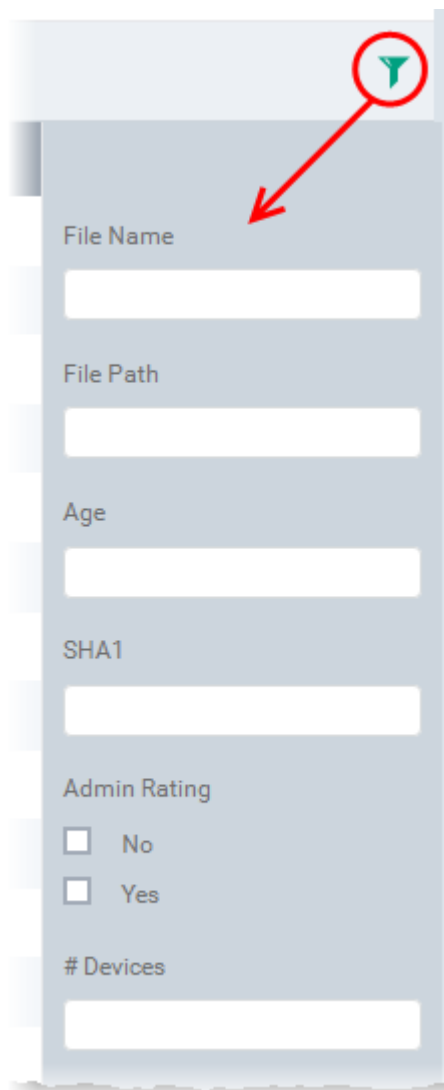
- Click the 'Applications' from the left and choose 'Windows File List' from the options
- Click the 'Unrecognized' tab from the top.

Unrecognized								
Trusted Malicious Valkyrie Processed Files								
<input type="checkbox"/> Move To Trusted <input type="checkbox"/> Move To Malicious <input type="checkbox"/> Clean History For This File								
<input type="checkbox"/>	FILE NAME	FILE PATH	AGE	SHA1	VERSION	ADMIN RATING	SIZE	# DEVICES
<input type="checkbox"/>	cpil.exe	D:\Suspicious Files\All_tests\cp...	3373 days	795FE85537EC514F3...		No	104 KB	1
<input type="checkbox"/>	CPILSuite.exe	D:\Suspicious Files\All_tests\cp...	3385 days	DCF2DFCB39003683...	1.0.0.1	No	1.54 MB	1
<input type="checkbox"/>	TSServ.exe	D:\Suspicious Files\All_tests\Tr...	4751 days	846C130E115589CF8...		No	145.5 KB	1
<input type="checkbox"/>	TrojanSimul...	D:\Suspicious Files\All_tests\Tr...	4751 days	85789749CE0EC90C8...		No	337.5 KB	1
<input type="checkbox"/>	pcflank.exe	D:\Suspicious Files\All_tests\P...	3515 days	3437369E6B75021F5...	1.0	No	176 KB	1
<input type="checkbox"/>	Ghost.exe	D:\Suspicious Files\Ghost\Ghos...	3350 days	DF3328F9944867C3C...	1.1	No	11 KB	1

The 'Unrecognized' Files List - Table of Column Descriptions	
Column Heading	Description
File Name	Displays the file name of the 'Unrecognized' item.
File Path	The installation location of the file at the endpoint
Age	The time from which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to Unrecognized Files list by the administrator.
Size	The size of the unrecognized file.
# Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device' interface with a list of endpoints from which the item was identified and allow the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device Screen below.

Sorting, Search and Filter Options

- Clicking on File Name, File Path, Admin Rating and/or # Devices column header sorts the items based on alphabetical order of entries in that column.
- Clicking the funnel button  at the right end opens the filter options.



File Name

File Path

Age

SHA1

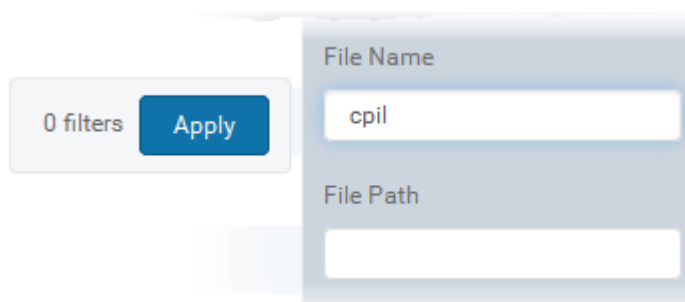
Admin Rating

No

Yes

Devices

- To filter the items or search for a specific file name, file path, age of the file, SHA1 hash value of the file and /or number of devices from which the file was discovered, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



0 filters **Apply**

File Name

File Path

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 CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

Managing Unrecognized Files

The Unrecognized Files interface allow you to:

- **View the details of files in the list**
- **Move selected files to global 'Trusted Files' or 'Malicious Files' list**
- **Removing files from the list**

View the details of files in the list

- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- **File Info** - Displays the general information on the selected item.
- **Device** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Unrecognized Files' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.

Windows File Rating / File Info

File Info Device

✓ Move To Trusted ✓ Move To Malicious

File Summary

File Name
TSServ.exe

File Path
D:\Suspicious Files\All_tests\TrojanSimulator\TSServ.exe

Age
4751 days

Hash Sha1
846C130E115589CF89720A8075F37C489FC59673

Version

Size
145.5 KB

Admin Rating
No

Actual Verdict
Unrecognized

The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, age, whether manually moved to Unrecognized files list and the actual file rating result by the local CES installation at the endpoint.

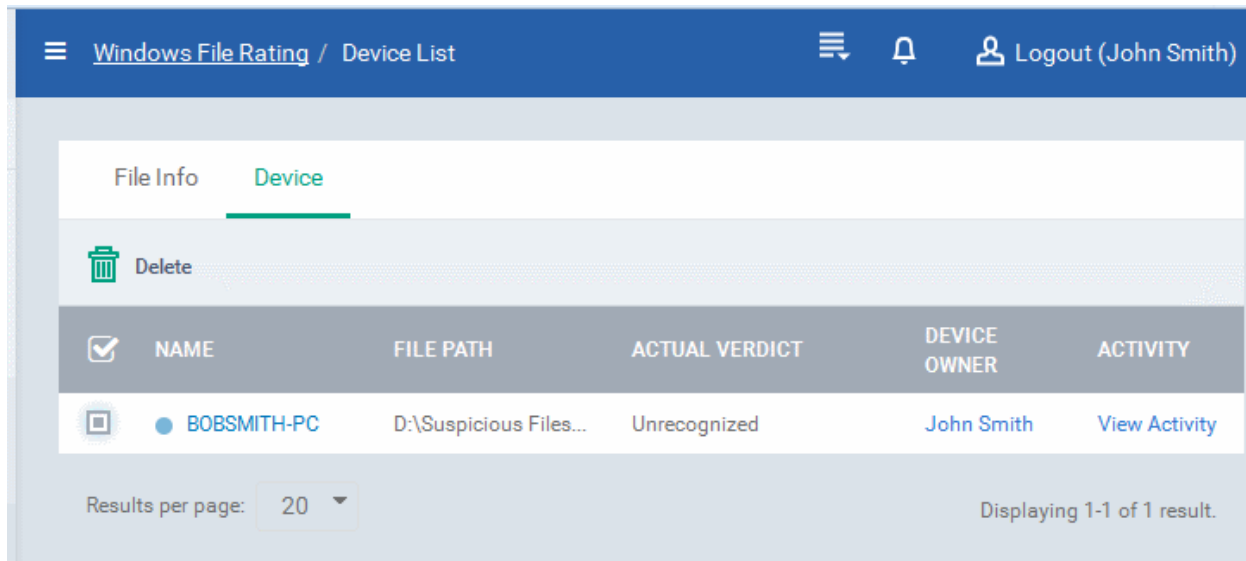
- If the item is found to be trustworthy you can move it to the Trusted Files list by clicking 'Move to Trusted' from the options at the top
- If the item is found to be malicious you can move it to malicious files list and block it at all the enrolled endpoints by clicking 'Move to Malicious' from the options at the top

Devices Screen

The 'Device' screen can be opened by clicking the 'Device' tab in the 'File Info' interface.

Tip - The Device Screen can also be opened by clicking on the number displayed in the '#Devices' column in the Unrecognized Files list table.

The 'Device' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.



- If you want to delete the file from selected devices, select the devices from the list and click 'Delete'.

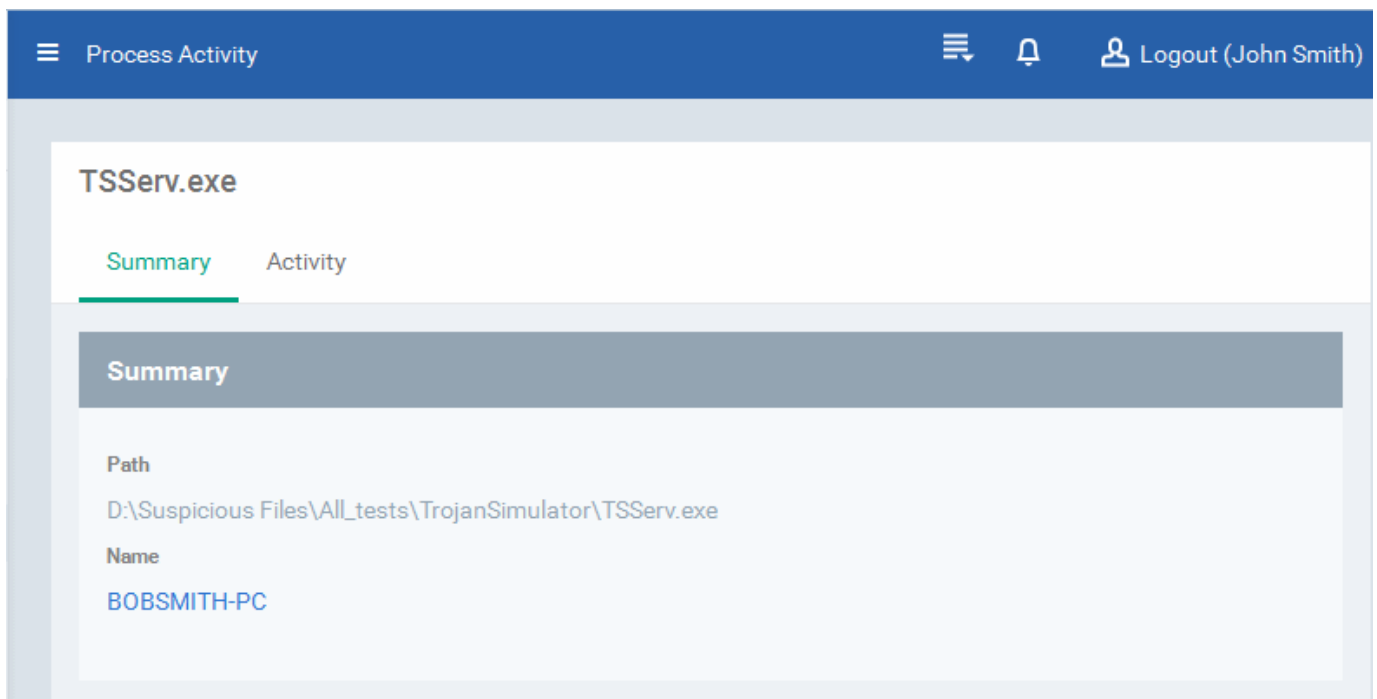
Viewing Process Activities of the File

Note: In order for CDM to fetch the data on activities of the files from an endpoint and display them, Viruscope should have been enabled in the profile in effect on the endpoint. Refer to the explanation of [Configuring Viruscope Settings](#) in the section [Creating a Windows Profile](#) for more details.

- To view the activities of the file at an endpoint, click the 'View Activity' link in the 'Activity' column

The 'Process Activity' interface will open. It has two tabs.

- **Summary** - Displays the details of the process(es) executed by the unrecognized file at the endpoint.



- **Activity** - Displays a chronological order of process activities with details of files modified by the process.

☰ Process Activity ☰ 🔔 👤 Logout (John Smith)

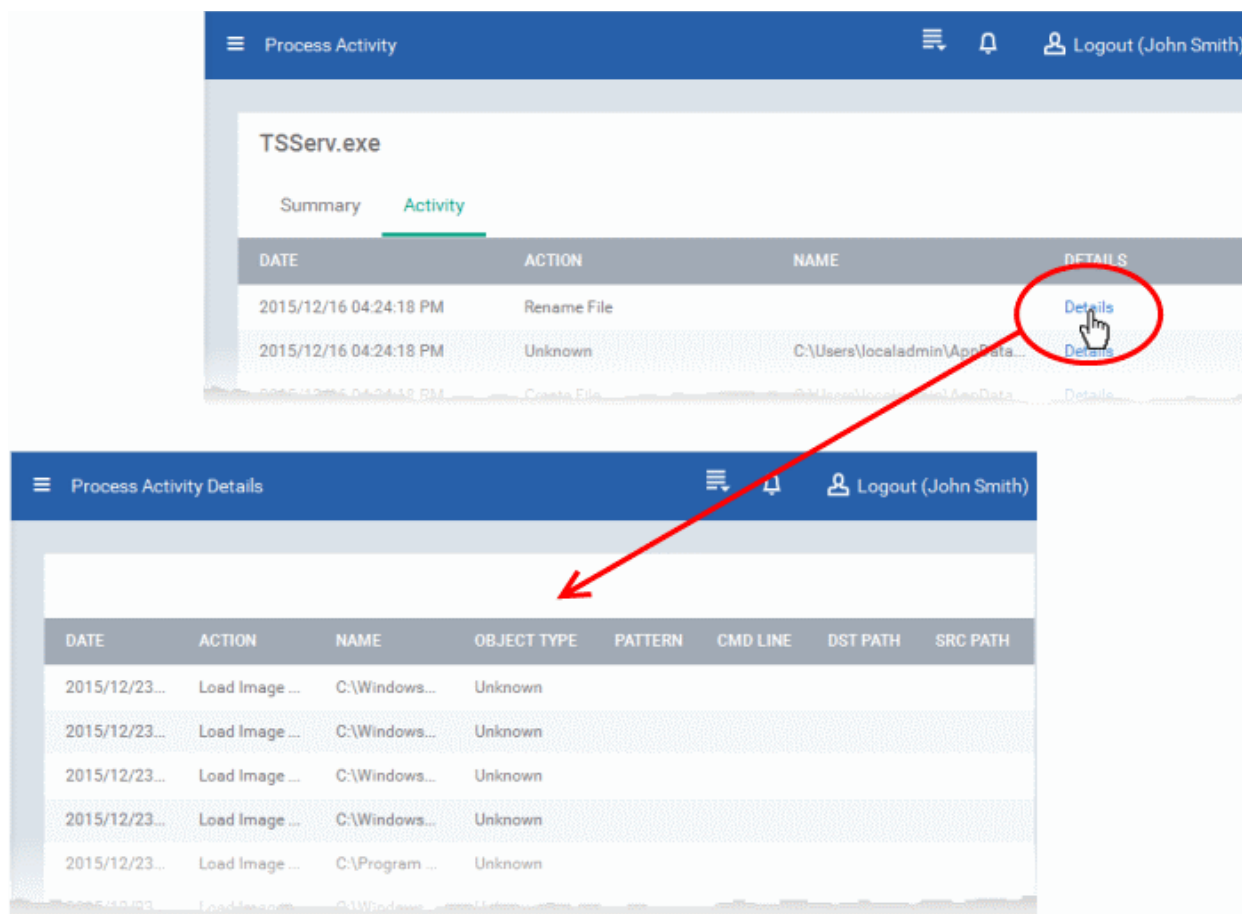
TSServ.exe

Summary Activity

DATE	ACTION	NAME	DETAILS
2015/12/16 04:24:18 PM	Rename File		Details
2015/12/16 04:24:18 PM	Unknown	C:\Users\localadmin\AppData...	Details
2015/12/16 04:24:18 PM	Create File	C:\Users\localadmin\AppData...	Details
2015/12/16 04:24:18 PM	Unknown		Details
2015/12/16 04:24:18 PM	Rename File		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
Name	Indicates the target file affected by the process
Details	Contains link to view the details of the action

- To view the details of an activity, click the 'Details' link under the 'Details' column.



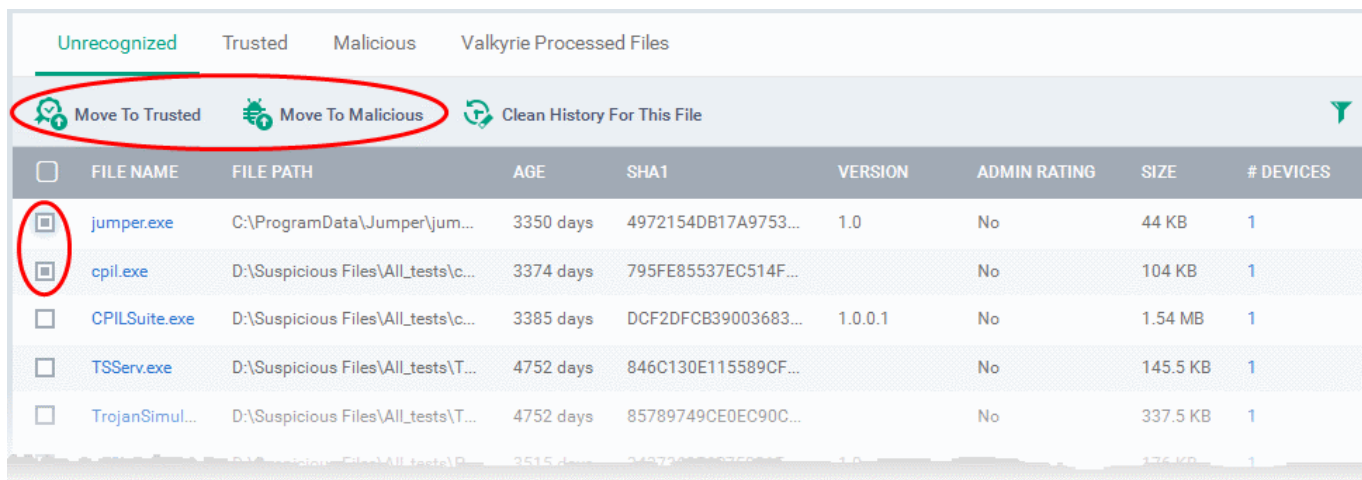
Moving Selected Files to 'Trusted Files' or 'Malicious Files' list

If an unrecognized item is identified as trustworthy by the administrator, the file can be added to the global 'Trusted Files' list. Files added to trusted file list will be skipped from real-time, on-demand and scheduled antivirus scans at the endpoints, till the next AV database update.

Tip: If a file is to be excluded from all types of AV scans in future, the administrator can add the file to the Exclusions list in the configuration profile applied to the endpoint. Refer to the explanation of adding **Exclusions to Antivirus Component** in the section **Creating a Windows Profile** for more details.

If an unrecognized item is identified as a malware by the administrator, the file can be added to the global 'Malicious Files' list. Files added to malicious files list will not be allowed to run at the endpoints.

- To move item(s) to the 'Trusted Files' list, select the items and click 'Move to Trusted' from the options at the top.



- To move item(s) to the 'Malicious Files' list, select the item, click 'Move to Malicious' from the options at the top.

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

Removing files from the list

If an unrecognized item is identified as a false-positive, the administrator can remove it from the 'Unrecognized Files' list.

- To remove or delete an item, select the item from the list and click 'Clean History For This File' from the options at the top.

The screenshot shows the 'Unrecognized' tab in the Comodo Device Manager. At the top, there are four buttons: 'Move To Trusted', 'Move To Malicious', and 'Clean History For This File'. The 'Clean History For This File' button is circled in red. Below the buttons is a table with the following columns: FILE NAME, FILE PATH, AGE, SHA1, and VERSION. The table contains several rows of files, including 'jumper.exe', 'cpil.exe', 'CPILSuite.exe', 'TSServ.exe', and 'TrojanSimul...'. The 'jumper.exe' row is selected, and its checkbox is circled in red. A red arrow points from the 'Clean History For This File' button to a dialog box titled 'Delete File History'. The dialog box contains the text 'Entire file history will be removed. Do you want to continue?' and two buttons: 'Confirm' and 'Cancel'.

FILE NAME	FILE PATH	AGE	SHA1	VERSION
<input checked="" type="checkbox"/> jumper.exe	C:\ProgramData\Jumper\jum...	3350 days	4972154DB17A9753...	1.0
<input checked="" type="checkbox"/> cpil.exe	D:\Suspicious Files\All_tests\c...	3374 days	795FE85537EC514F...	
<input type="checkbox"/> CPILSuite.exe	D:\Suspicious Files\All_tests\c...	3385 days	DCF2DFCB39003683...	1.0.0.1
<input type="checkbox"/> TSServ.exe	D:\Suspicious Files\All_tests\T...	4752 days	846C130E115589CF...	
<input type="checkbox"/> TrojanSimul...	D:\Suspicious Files\All_tests\T...	4752 days	85789749CE0EC90C...	

- Click 'Confirm' in the confirmation dialog to remove the item from the 'Unrecognized Files' list.

The file will only be removed from the Unrecognized Files list. If the same file is identified from the same of a different endpoint, it will be again be added to the list unless the file is moved to 'Trusted Files' list or 'Malicious Files' list.

7.2.2. Viewing and Managing Trusted Files

Files included in the 'Trusted Files' list are automatically given CES trusted status. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, CES at the endpoints will check the file against our 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.
- Administrator rating - The Administrator moving files identified as trustworthy from 'Unrecognized Files' list or 'Malicious Files' list.

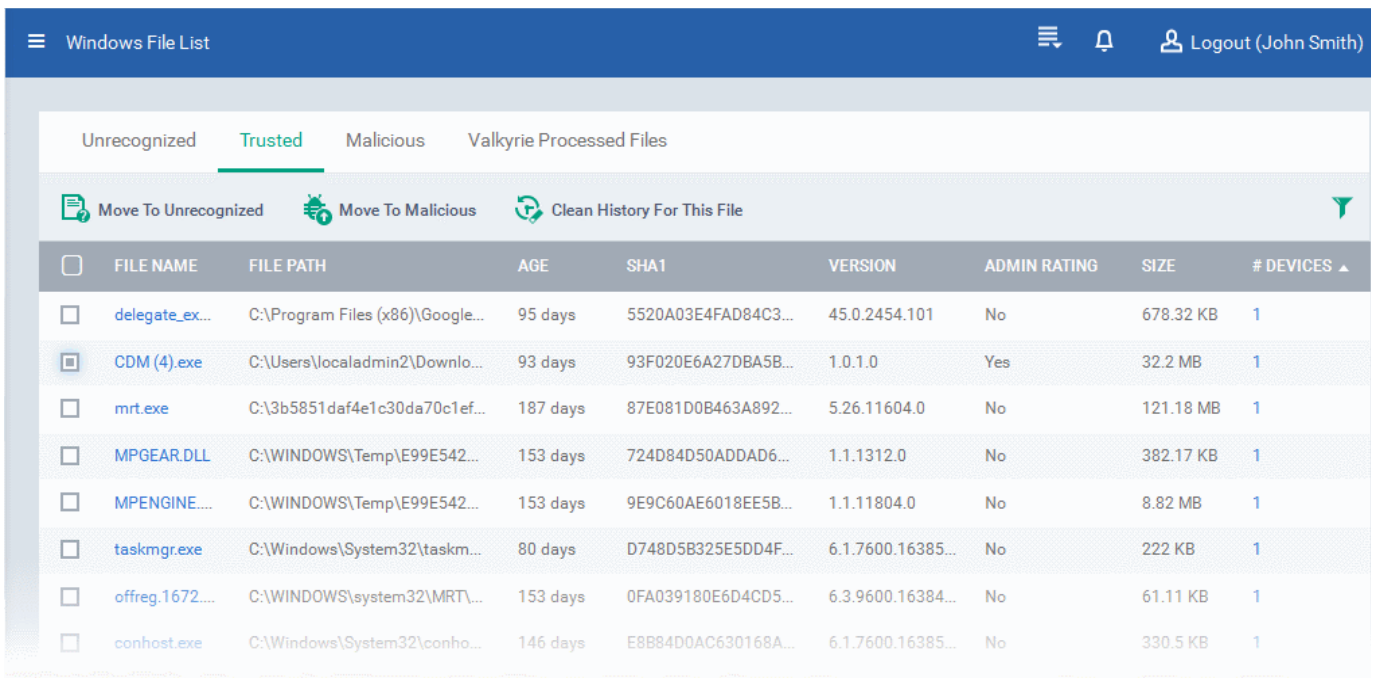
- User Rating - The user can assign 'Trusted' status to the files through local CES installation in two ways:
 - If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, the user could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted'.
 - The user can assign 'Trusted' rating to any desired file from the 'File List' interface.

For the files assigned with 'Trusted' status by the user, CES generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

The 'Trusted' tab under 'Windows File List' interface displays a consolidated list of Trusted files reported by the CES installations at the endpoints.

To open the Trusted Files interface

- Click the 'Applications' from the left and choose 'Windows File List' from the options
- Click the 'Trusted' tab from the top.




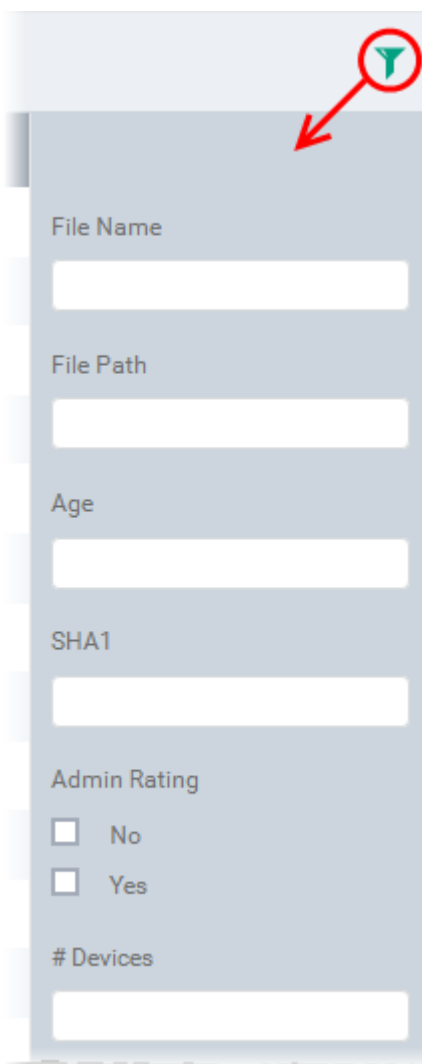
The 'Trusted ' List - Table of Column Descriptions

Column Heading	Description
File Name	Displays the file name of the 'Trusted' item.
File Path	The installation location of the file at the endpoint
Age	The time from which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to Trusted Files list by the administrator.
Size	The size of the file.
# Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the

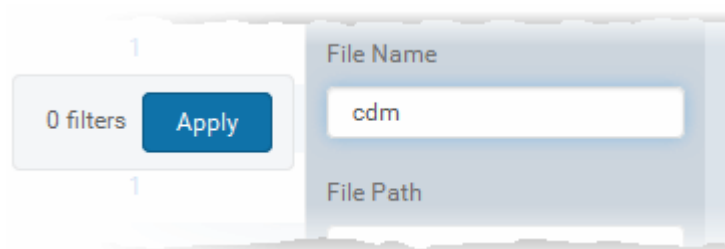
number opens the 'Device' interface with a list of endpoints from which the item was identified and allow the administrator to view the activities of the processes executed by the item. For more details, refer to description under **Device Screen** below.

Sorting, Search and Filter Options

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



- To filter the items or search for a specific file name, file path, age of the file, SHA1 hash value of the file and /or number of devices from which the file was discovered, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



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

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

Managing Trusted Files

The 'Trusted' Files interface allows you to:

- **View the details of files in the list**
- **Move selected files to 'Unrecognized Files' or 'Malicious Files' list**
- **Removing files from the list**

View the details of files in the list

- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- **File Info** - Displays the general information on the selected item.
- **Device** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Trusted' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.

Windows File Rating / File Info

Logout (John Smith)

File Info Device

✓ Move To Unrecognized ✓ Move To Malicious

File Summary

File Name
opera.exe

File Path
C:\Program Files (x86)\Opera\34.0.2036.25\opera.exe

Age
26 days

Hash Sha1
AF6C12AFA52DB702E958D0C461D4D285B0E5FB70

Version
34.0.2036.25

Size
615.62 KB

Admin Rating
No

Actual Verdict
Trusted

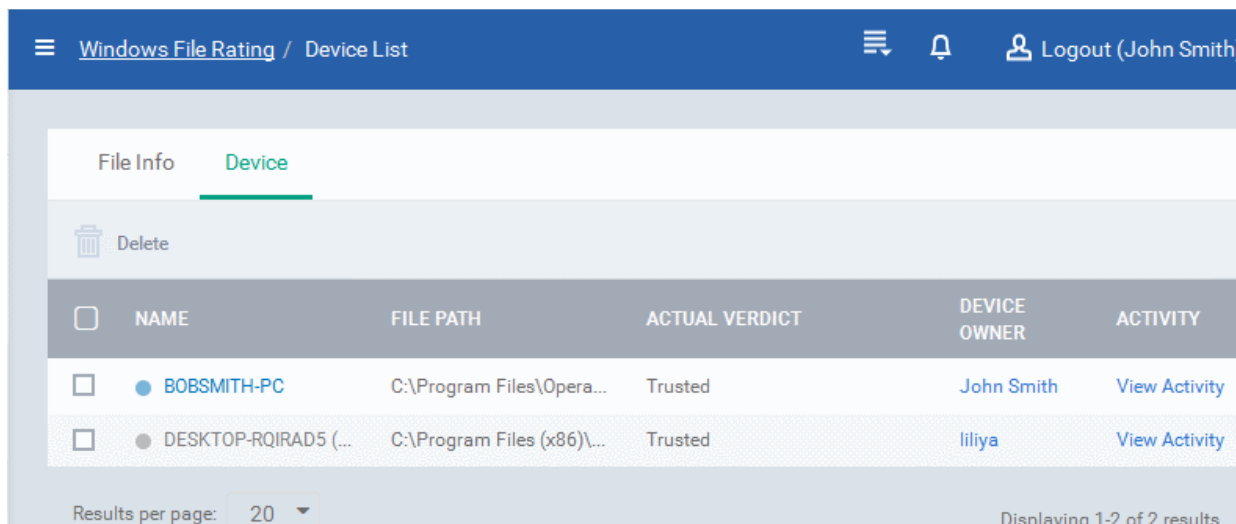
The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, age, whether manually moved to Trusted files list and the actual file rating result by the local CES installation at the endpoint.

- If the item is found to be suspicious, you can move it to the Unrecognized Files list by clicking 'Move to Unrecognized' from the options at the top
- If the item is found to be malicious you can move it to malicious files list and block it at all the enrolled endpoints by clicking 'Move to Malicious' from the options at the top

Devices Screen

The 'Device' screen can be opened by clicking the 'Device' tab in the 'File Info' interface.

The 'Device' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.

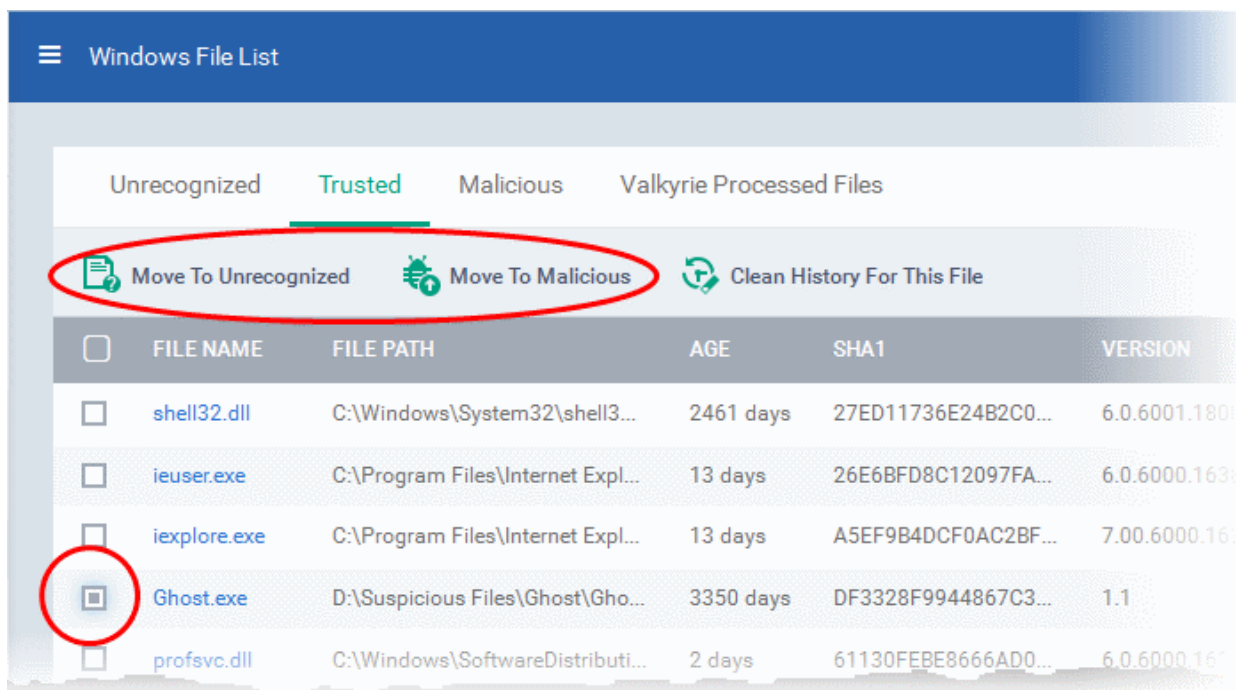


The Device interface allows the administrator to view the activities of the file at the selected endpoint. Refer to the explanation of **Viewing Process Activities of the File** in the previous section for more explanation.

Moving Selected Files to 'Unrecognized Files' or 'Malicious Files' list

Items that are added to the 'Trusted Files' list by mistake can be moved to 'Unrecognized Files' list or global 'Malicious Files' list.

- To move item(s) to the 'Unrecognized Files' list, select the items and click 'Move to Unrecognized' from the options at the top.



- To move item(s) to the 'Malicious Files' list, select the item, click 'Move to Malicious' from the options at the top.

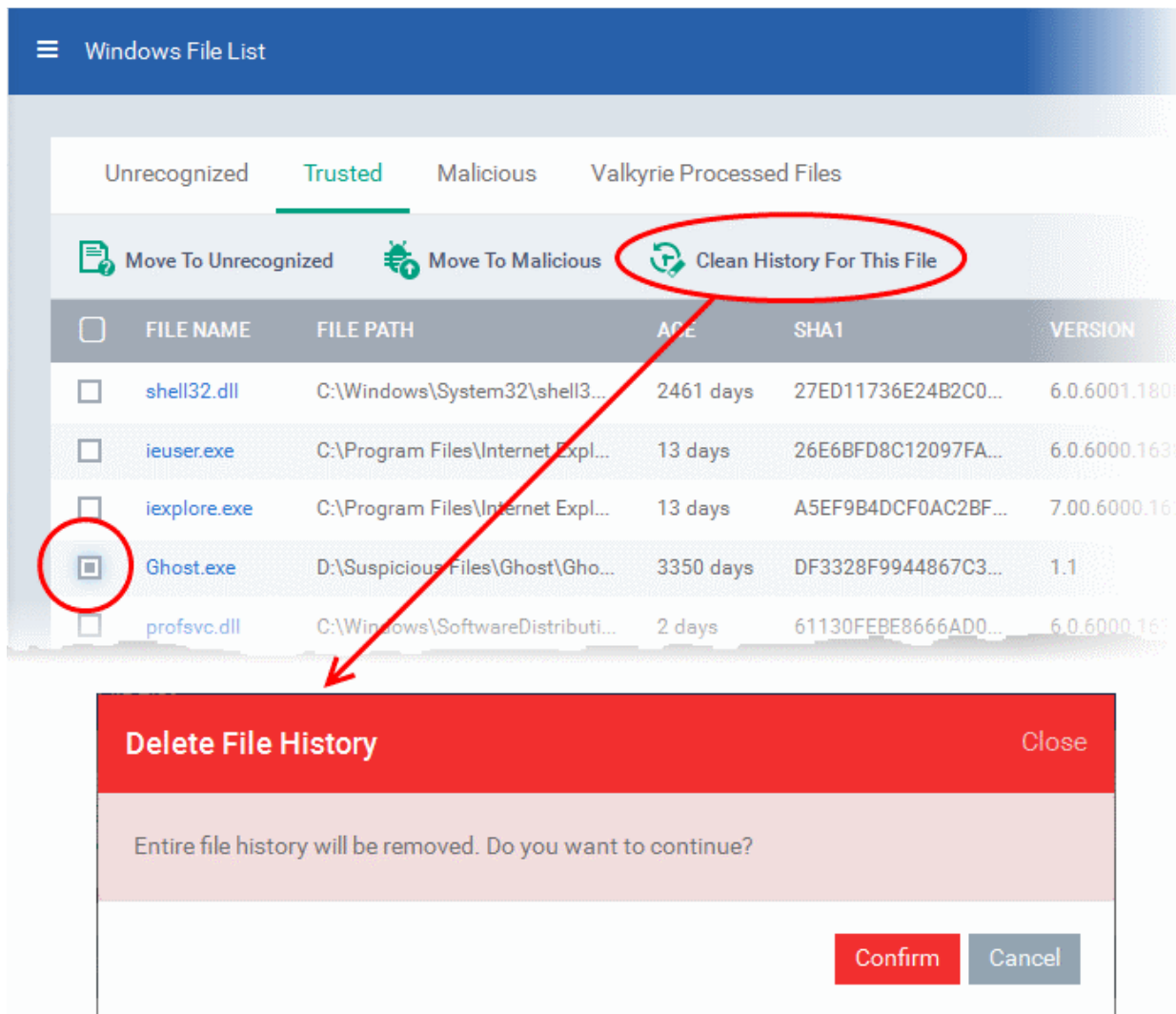
Tip: You can filter or search for specific files using the filter options that appear on clicking the funnel icon at the top right.

Removing files from the list

If an item in 'Trusted Files' list is identified as not trustworthy, the administrator can remove it from the 'Trusted Files' list.

- To remove or delete an item, select the item from the list and click 'Clean History For This File' from the options at the

top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Trusted Files' list.

The file will only be removed from the 'Trusted' Files list and not from the endpoints.

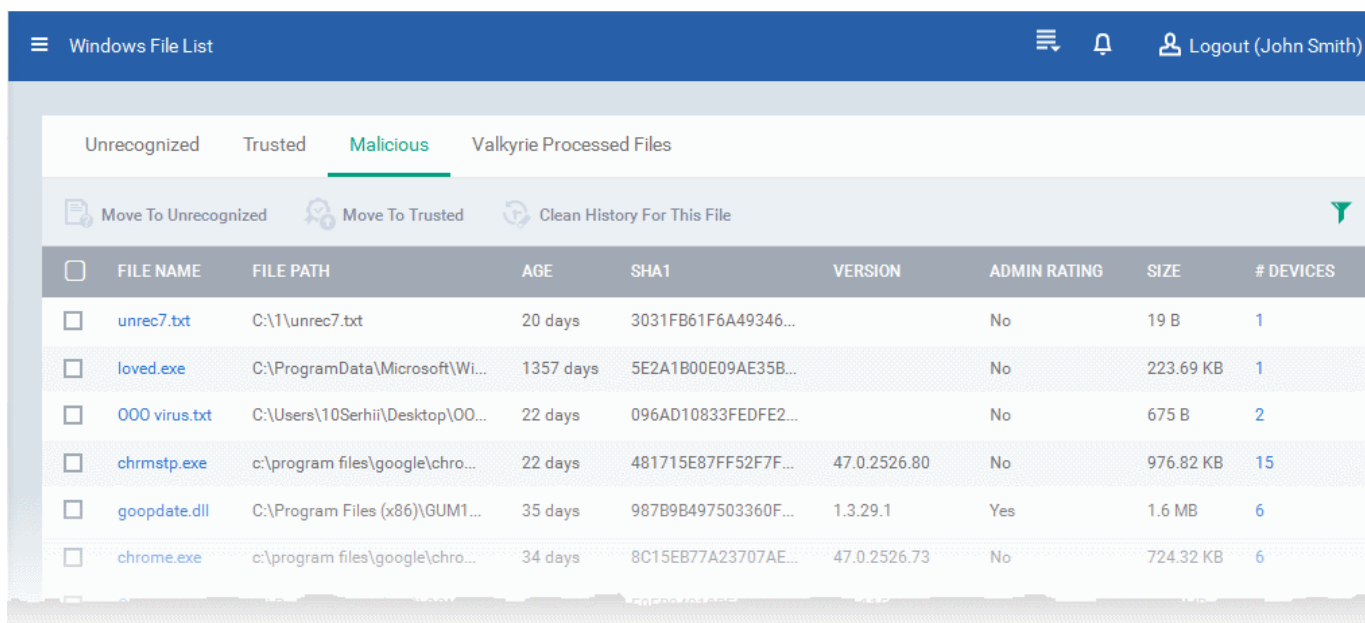
7.2.3. Viewing and Managing Malicious Files

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

The 'Malicious' tab under 'Windows File List' interface displays a consolidated list of malicious files reported by the CES installations at the endpoints.


To open the Malicious Files List interface

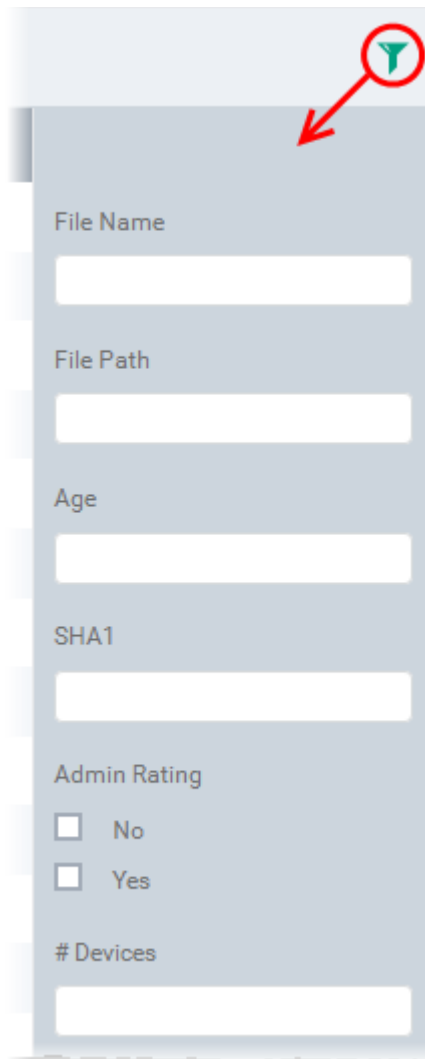
- Click the 'Applications' from the left and choose 'Windows File List' from the options
- Click the 'Malicious' tab from the top.



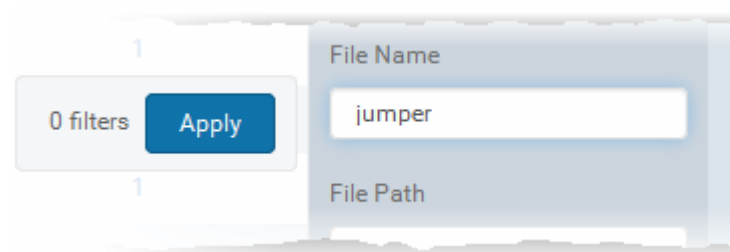
The 'Malicious Files' List - Table of Column Descriptions	
Column Heading	Description
File Name	Displays the file name of the 'malicious' item.
File Path	The installation location of the file at the endpoint
Age	The time from which the file was installed at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Version	Displays the version number of the executable file
Admin Rating	Indicates whether the file was moved to Unrecognized Files list by the administrator.
Size	The size of the unrecognized file.
# Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device' interface with a list of endpoints from which the item was identified and allow the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device Screen below.

Sorting, Search and Filter Options

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



- To filter the items or search for a specific file name, file path, age of the file, SHA1 hash value of the file and /or number of devices from which the file was discovered, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



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

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

Managing Malicious Items

The Malicious Files interface allow you to:

- **View the details of files in the list**

- **Move selected files to 'Unrecognized Files' or 'Trusted Files' list**
- **Removing files from the list**

View the details of files in the list

- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- **File Info** - Displays the general information on the selected item.
- **Device** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Malicious' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.

The screenshot displays the 'File Info' screen in the Comodo Device Manager. At the top, there is a blue navigation bar with a hamburger menu icon, the text 'Windows File Rating / File Info', and a 'Logout (John Smith)' button. Below the navigation bar, there are two tabs: 'File Info' (which is active and highlighted in green) and 'Device'. Under the 'File Info' tab, there are two buttons: 'Move To Unrecognized' and 'Move To Trusted', both with green checkmarks. The main content area is titled 'File Summary' and displays the following details:

- File Name:** pcflank.exe
- File Path:** D:\Suspicious Files\All_tests\PCFlank\PCFlank\pcflank.exe
- Age:** 3515 days
- Hash Sha1:** 3437369E6B75021F57DE5527C33EF7B1026E52D6
- Version:** 1.0
- Size:** 176 KB
- Admin Rating:** Yes
- Actual Verdict:** Malicious

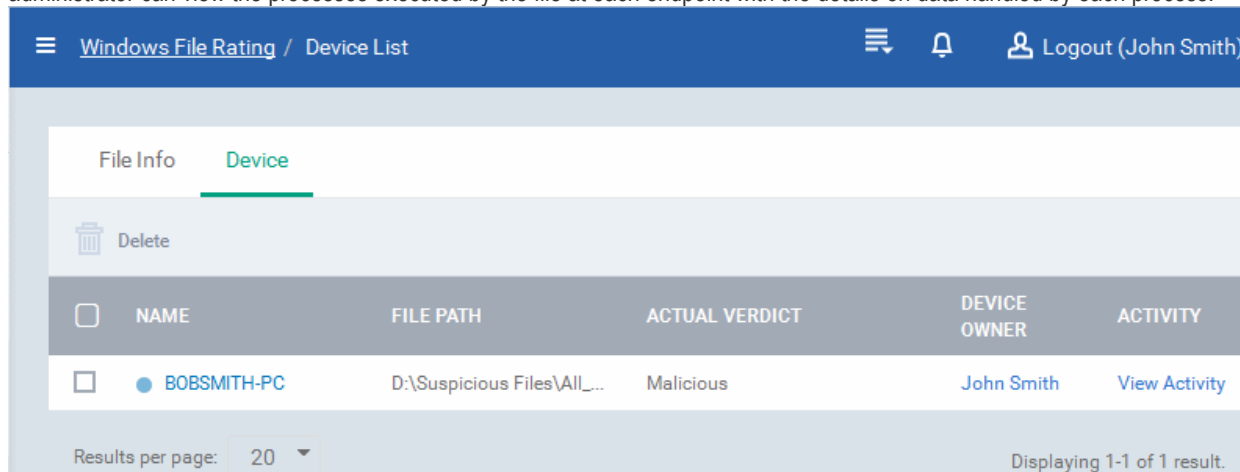
The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, age, whether manually moved to Trusted files list and the actual file rating result by the local CES installation at the endpoint.

- If the item is found to be suspicious, you can move it to the Unrecognized Files list by clicking 'Move to Unrecognized' from the options at the top
- If the item is found to be trustworthy, you can move it to Trusted files list by clicking 'Move to Trusted' from the options at the top

Device Screen

The 'Device' screen can be opened by clicking the 'Device' tab in the 'File Info' interface.

The 'Device' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.

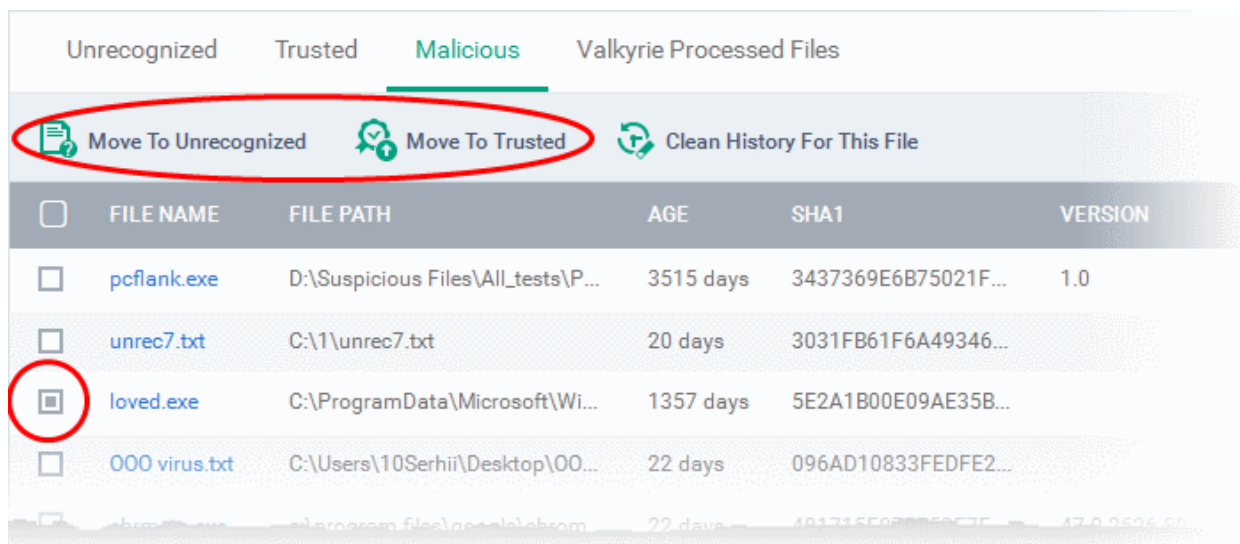


The Device interface allows the administrator to view the activities of the file at the selected endpoint. Refer to the explanation of [Viewing Process Activities of the File](#) in the previous section for more explanation.

Moving Selected Files to 'Unrecognized Files' or 'Trusted Files' list

Items that are added to the 'Malicious Files' list by mistake or found trustworthy can be moved to 'Unrecognized Files' list or global 'Trusted Files' list.

- To move item(s) to the 'Unrecognized Files' list, select the items and click 'Move to Unrecognized' from the options at the top.



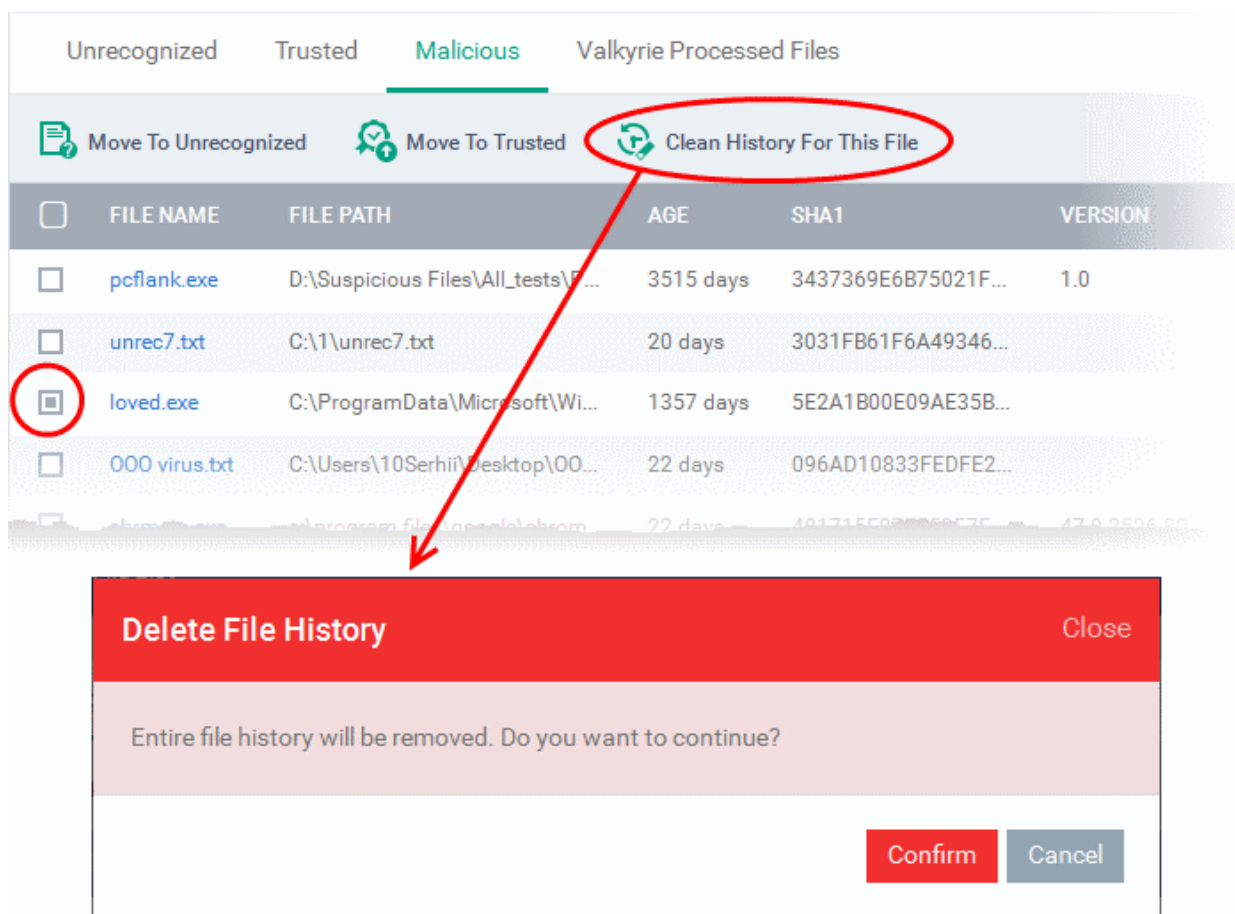
- To move item(s) to the 'Trusted Files' list, select the item, click 'Move to Trusted' from the options at the top.

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

Removing files from the list

If an item in the malicious file list is identified not a malware or need not be blocked any more, the administrator can remove it from the list.

- To remove or delete an item, select the item from the list and click 'Clean History For This File' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Malicious Files' list.

The file will only be removed from the Malicious Files list and not from the endpoints.

7.2.4. Viewing list of Valkyrie Analyzed Files

Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Each CES installation on a managed Windows Device is capable of uploading unknown files to Valkyrie for analysis.

Valkyrie results are shown in CDM at 'Applications > Windows File List > Valkyrie Processed Files'. You can also view Valkyrie results in the CDM Dashboard by clicking 'Dashboard > Valkyrie'

Administrators can schedule unknown files for upload by configuring the Valkyrie component of the Windows Profile applied to the Managed devices. For more details on configuring Valkyrie refer to the section **Valkyrie Settings** under **Creating Windows Profiles**.

Note: The version of Valkyrie that comes with the free version of CDM is limited to the online testing service. The Premium version of CDM 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.

The 'Valkyrie Processed Files' tab displays a consolidated list of Valkyrie ratings for every unknown file uploaded from managed Windows devices.

To open the 'Valkyrie Processed Files' List interface

- Click the 'Applications' from the left and choose 'Windows File List' from the options
- Click the 'Valkyrie Processed Files' tab from the top.

FILE HASH	FILE NAME	FILE PATH	FILE RATING	FIRST RECEIVE DATE
f326aa7df336c1de6a43b93d2a459ec92188ce4e		null	Clean	2015-12-26 01:52:58
dc24a1fbe219c11b19bfbb2b34e16956f49c7cb7		null	Clean	2015-12-26 01:52:33
db2c2585c748d76e20efd108ac9d2efcd0c2eec4	hpcpp093.dll	\\10.100.66.103\c:\windows\system32\spool\prtprocs\x64\hpcpp093.dll	No Threat Found	2015-12-25 18:29:36
d8c39767b05d9f7e926d43bc3110464624aec6c3	tsccvid64.dll	\\10.100.66.103\C:\Windows\SysWOW64\tscvid64.dll	No Threat Found	2015-12-25 18:29:15
b45092ca2fb65ab306d016328496d8ce48f52f56	vtcdrv.sys	null	No Threat Found	2015-12-25 18:30:50
b445102277134ad1f947a8c4631c9d191693507	188f53eb.exe	null	No Threat Found	2015-12-25 18:49:17

The 'Valkyrie Processed Files' List - Table of Column Descriptions	
Column Heading	Description
File Hash	Displays the hash value of the uploaded unknown file, derived using SHA1 hash algorithm.
File Name	Displays the file name of the 'malicious' item.
File Path	The installation location of the file at the endpoint from which it has been uploaded to Valkyrie
File Rating	Displays the verdict for the file from the Valkyrie. The possible values are: <ul style="list-style-type: none"> 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 a malware and should not be run
First Receive Date	Indicates date and time at which the file was received at Valkyrie for the first time for analysis.

7.3. Viewing and Managing Sandboxed Applications on Windows Devices

The Sandbox component of CES on each endpoint provides an isolated environment in which suspicious, unknown/unrecognized or unstable programs are run. Sandboxed applications are not permitted to access files or user data on the host machine.

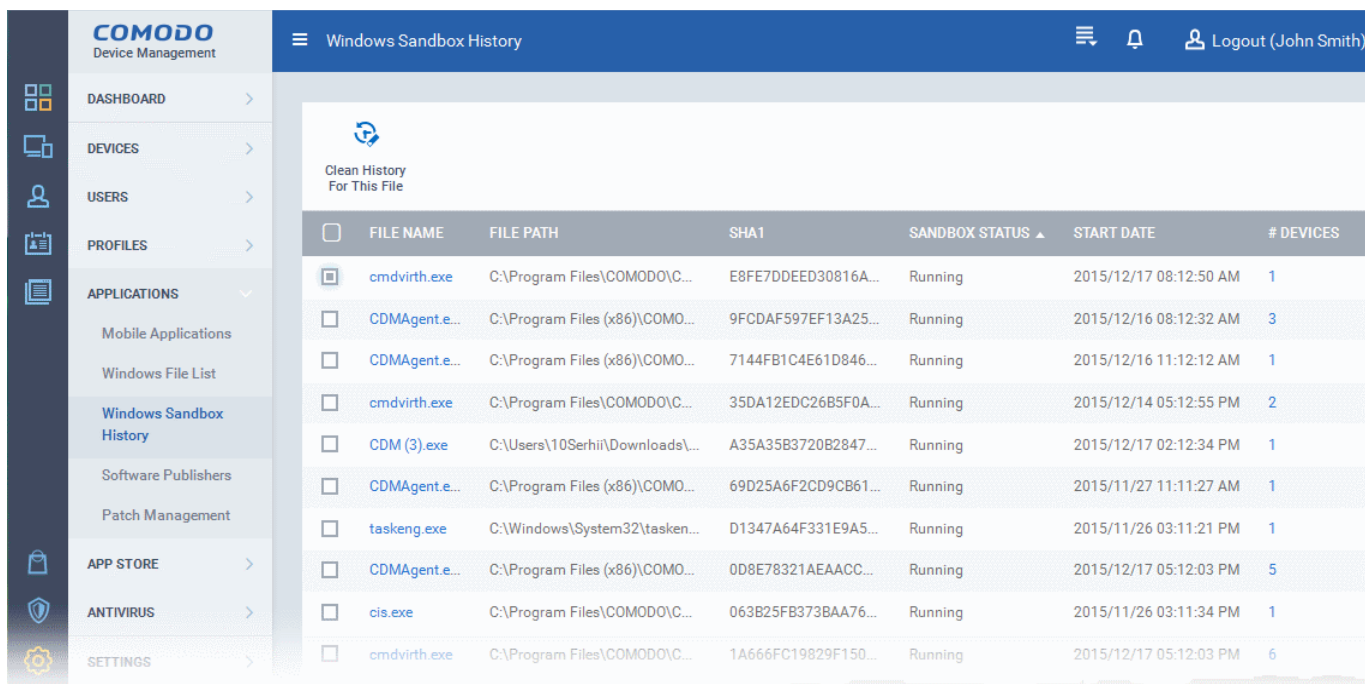
The CES installations at each managed endpoint run selected applications at the endpoints inside the sandbox when:

- The application is auto-sandboxed based on the Sandbox rules defined in the configuration profile applied to the endpoint. Refer to the description under **Sandbox Settings** in the section **Creating a Windows Profile** for more details on setting the Sandbox Rules for a profile.
- The application is auto-sandboxed based on the Sandbox rules configured at the CES installation at the endpoint
- The user at the endpoint runs a program inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that have they downloaded or for applications that they are not sure that you trust.

The administrator can view a consolidated list of all the programs that were executed and currently being executed inside the

sandbox at all the endpoints, irrespective of whether they are auto-sandboxed or manually ran inside the sandbox, from the 'Windows Sandbox History' interface. The administrator can also view the activities of the processes executed by the sandboxed applications.

- To open the 'Windows Sandbox History' interface, click 'Applications' from the left and choose 'Windows Sandbox History' from the options.



The 'Windows Sandbox History' - Column Descriptions	
Column Heading	Description
File Name	Displays the file name of the 'sandboxed' executable.
File Path	The installation location of the file at the endpoint
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
Sandbox Status	Indicates whether the executable is currently running inside the sandbox at the endpoint, completed execution or failed to execute.
Start Date	The date and time at which the file was started execution inside the sandbox.
# Devices	Indicates the number of endpoint computers on which the item was identified. Clicking the number opens the 'Device' interface with a list of endpoints from which the item was identified and allow the administrator to view the activities of the processes executed by the item. For more details, refer to description under Device Screen below.

- Clicking on 'File Name', 'File Path', 'Sandbox Status', 'Start Date' and/or '# Devices' column header sorts the items based on alphabetical order of entries in that column.

Managing Sandboxed Items

The 'Windows Sandbox Files' interface allow you to:

- View the details of the sandboxed applications**
- Remove files from the list**

Viewing the details of sandboxed items

- To view the details of a file, the endpoints from which it was identified and activities of it at the endpoint click on its file name.

The file information interface will be displayed. The interface contains two tabs:

- **File Info** - Displays the general information on the selected item.
- **Device** - Displays the list of endpoints up on which the item was identified with its activities at each endpoint.

File Information Screen

The 'File Info' screen is displayed by default whenever the name of an item is clicked from the 'Windows Sandbox Files' interface. To return to the 'File Info' screen from 'Devices' screen, click the 'File Info' tab from the top.

Windows Sandbox History / qcreator_ctrlc_stub.exe / File Info

File Info Devices List

File Summary

File Name
qcreator_ctrlc_stub.exe

File Path
C:\Qt\Tools\QtCreator\bin\qcreator_ctrlc_stub.exe

Age
22 days

Hash Sha1
70F6C2E5BC76536D4B6B48E2A9C5A51322C12B3C

Version

Size
8.5 KB

The 'File Info' screen displays a summary of the file details like file name, file installation path, version, size, file hash value, and its age.

Devices Screen

The 'Device' screen can be opened by clicking the 'Device' tab in the 'File Info' interface.

The 'Device' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process.

Windows Sandbox History / qcreator_ctrlc_stub.exe / Devices List

File Info Devices List

NAME	FILE PATH	DEVICE OWNER	ACTIVITY
BOBSMITH-PC	C:\Qt\Tools\QtCreator\bin\qcreator_ctrlc_stub.exe	dev	View Activity
DESKTOP-KLHUSSV (removed)	C:\Qt\Tools\QtCreator\bin\qcreator_ctrlc_stub.exe	dev	View Activity

Results per page: 20

Displaying 1-2 of 2 results.

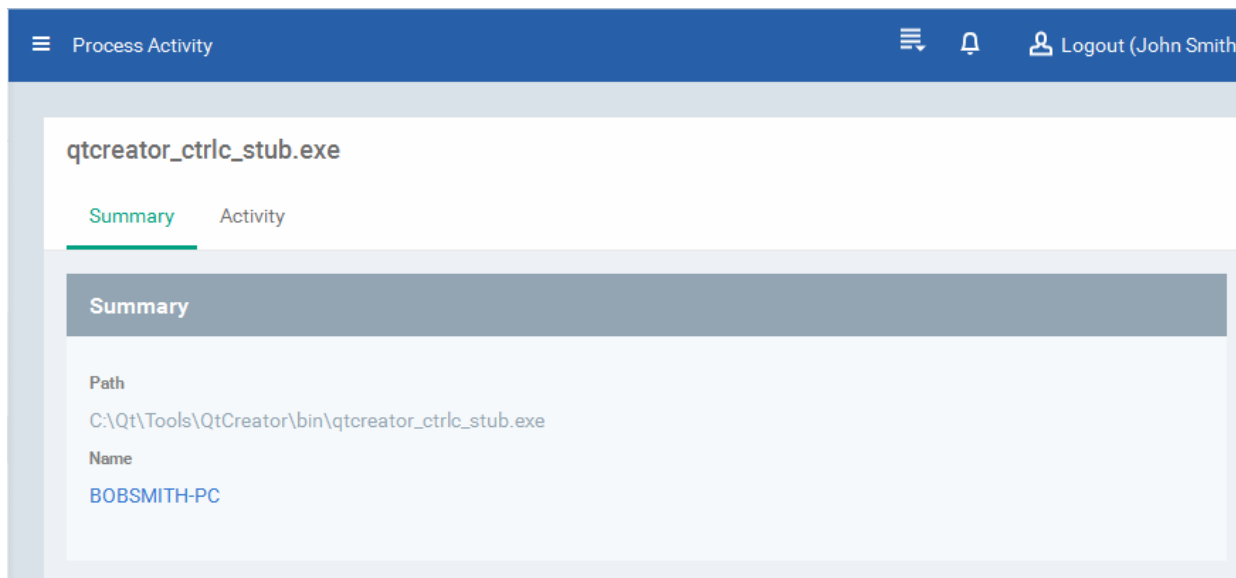
Viewing Process Activities of the File

Note: In order for CDM to fetch the data on activities of the files from an endpoint and display them, Viruscope should have been enabled in the profile in effect on the endpoint. Refer to the explanation of [Configuring Viruscope Settings](#) in the section [Creating a Windows Profile](#) for more details.

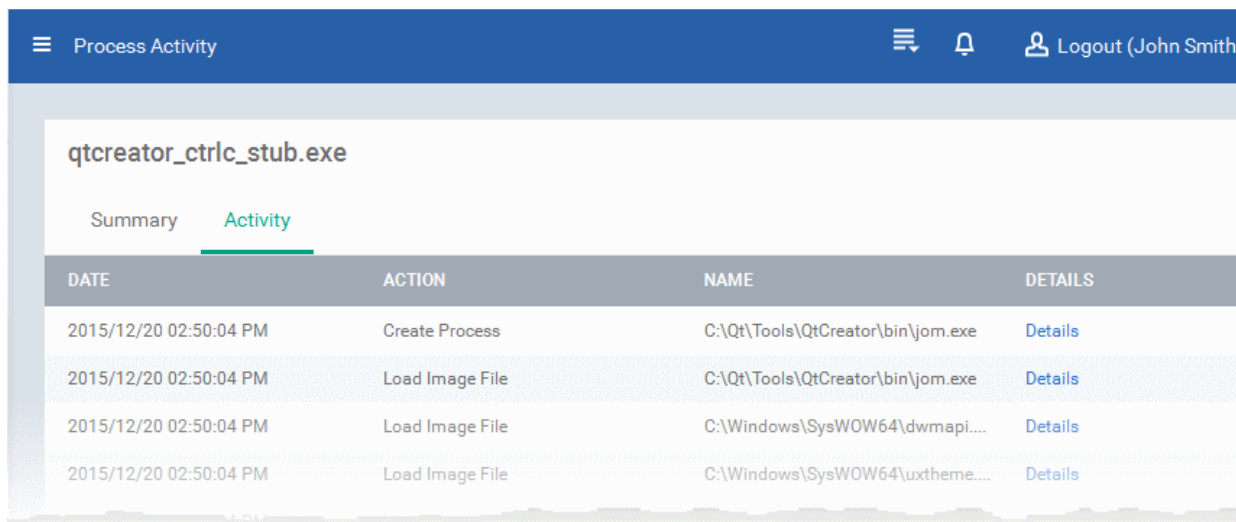
- To view the activities of the file at an endpoint, click the 'View Activity' link in the 'Activity' column

The 'Process Activity' interface will open. It has two tabs.

- Summary** - Displays the details of the process(es) executed by the sandboxed file at the endpoint.



- Activity** - Displays a chronological order of process activities with details of files modified by the process.



Column Heading	Description
Date	Indicates the date and time of process execution
Action	Indicates the action executed by the process on the target file
Name	Indicates the target file affected by the process

Details	Contains link to view the details of the action
---------	---

- To view the details of an activity, click the 'Details' link under the 'Details' column.

qtcreator_ctrlc_stub.exe

Summary Activity

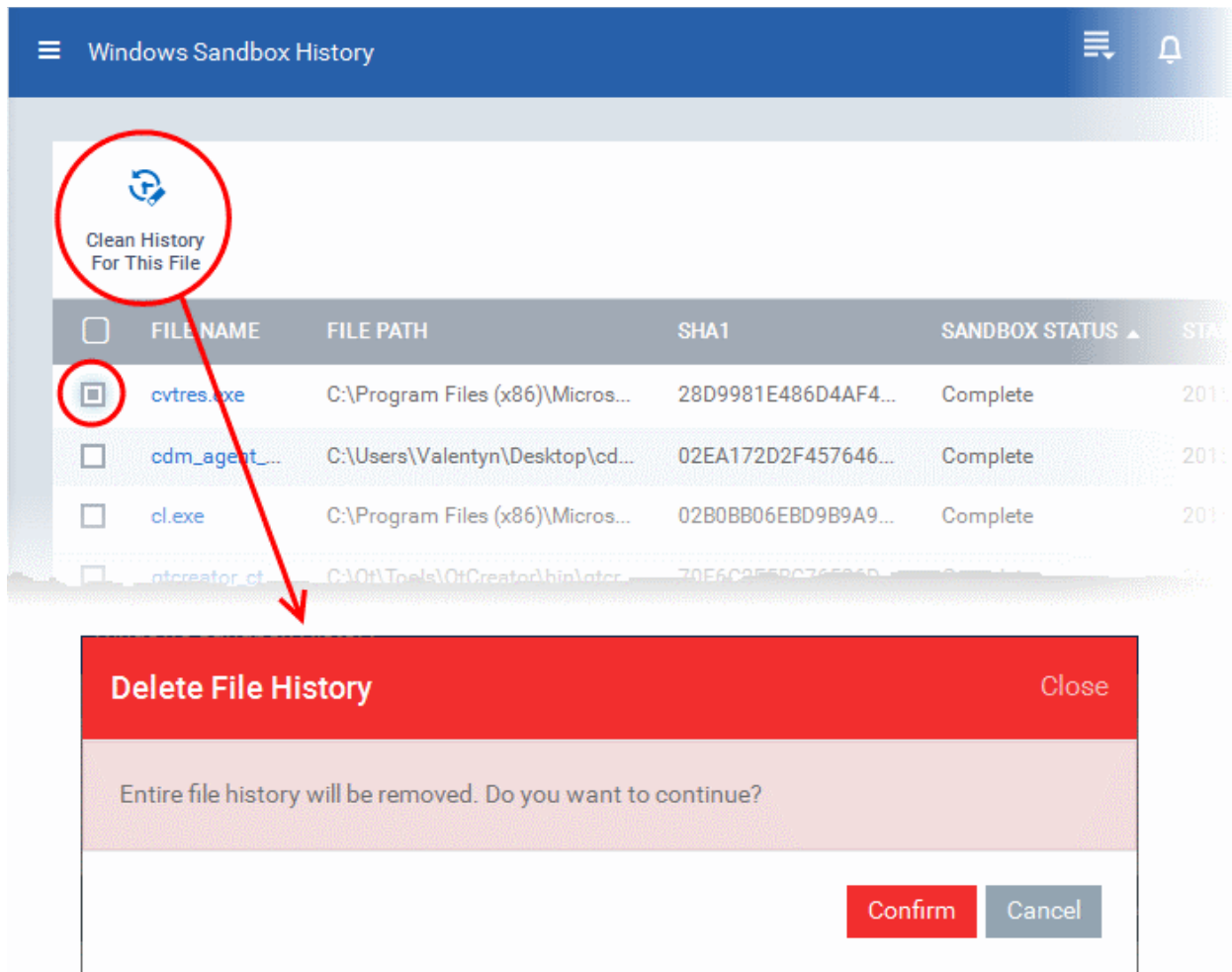
DATE	ACTION	NAME	DETAILS
2015/12/20 02:50:04 PM	Create Process	C:\Qt\Tools\QtCreator\bin\jom.exe	Details
2015/12/20 02:50:04 PM	Load Image File	C:\Qt\Tools\QtCreator\bin\jom.exe	Details
2015/12/20 02:50:04 PM	Load Image File	C:\Windows\SysWOW64\dwmapi...	Details
2015/12/20 02:50:04 PM	Load Image File	C:\Windows\SysWOW64\uxtheme...	Details

DATE	ACTION	NAME	OBJECT TYPE	PATTERN	CMD LINE	DST PATH	SRC PATH
2015/12/23 0...	Load Image File	C:\Windows\S...	Unknown				
2015/12/23 0...	Load Image File	C:\Windows\S...	Unknown				
2015/12/23 0...	Load Image File	C:\Windows\S...	Unknown				
2015/12/23 0...	Load Image File	C:\Windows\S...	Unknown				

Removing files from the list

The administrator can remove unwanted items from the 'Windows Sandbox History' interface.

- To delete an item, select the item from the list and click 'Clean History For This File' from the options at the top.



- Click 'Confirm' in the confirmation dialog to remove the item from the 'Windows Sandbox History' interface.

7.4. Viewing and Managing Software Vendors List

Comodo Endpoint Security uses the following methods to identify trusted files on Windows devices:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, CES will check it against Comodo's master files whitelists 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.
- Consults local administrator and user rating

An application is also 'Trusted' if it is published by a 'Trusted Software Vendor'. To ensure software authenticity, the publisher/vendor must digitally sign their software using a code signing certificate obtained from a trusted Certificate Authority (CA).

Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

- Content Source: The software they are downloading and are about to install really comes from the publisher that signed it.
- Content Integrity: That the software they are downloading and are about to install has not be modified or corrupted since it was signed.

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

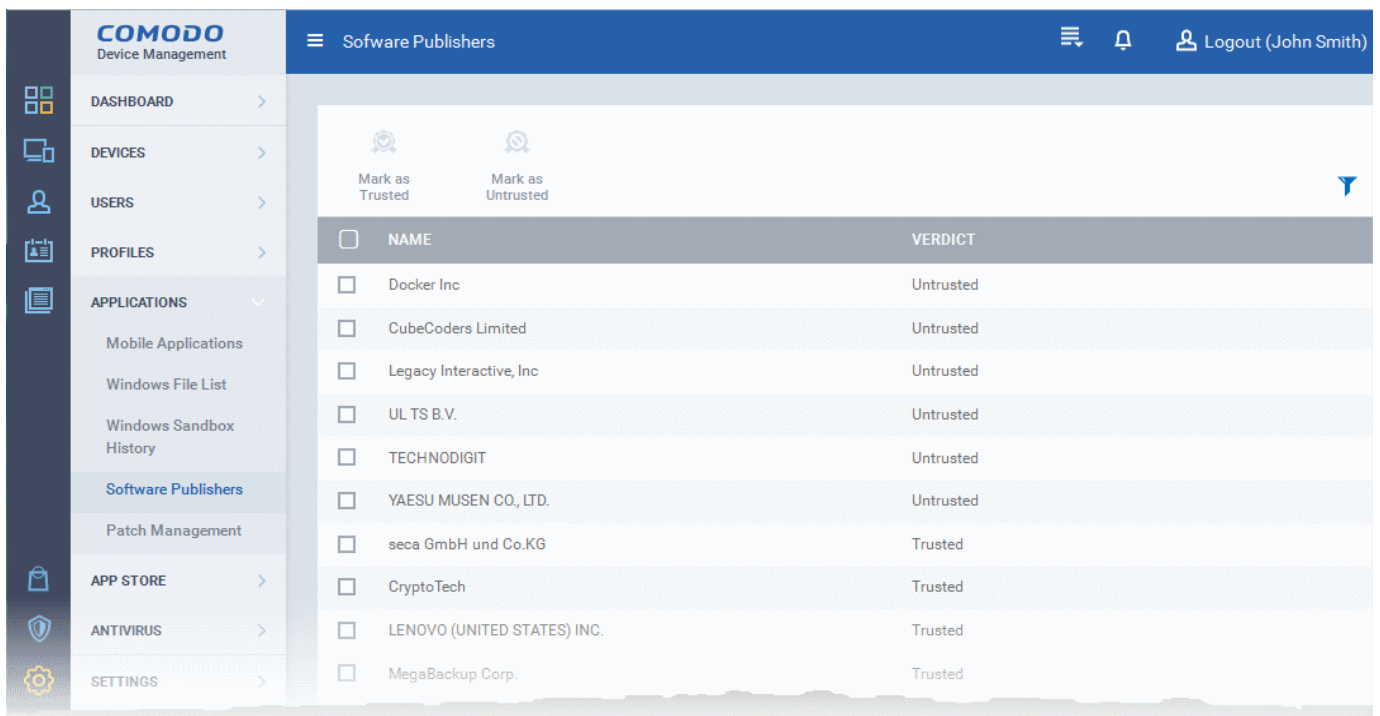
The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the option 'Trust applications digitally signed by trusted vendors' is enabled in the 'File Rating' component of the Windows profile applied to an endpoint, then it will be automatically trusted by CES at the endpoint (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question.

- Browse to the folder containing the .exe file.
- Right click on the .exe file.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).
- This displays the name of the CA that signed the software.
- Select the certificate and click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate.


The Software Publishers interface under the Applications tab displays a consolidated list of vendors of the applications identified from all the managed Windows devices, with their Trust status as per constantly updated global Trusted Vendor List maintained by Comodo. It also allows the administrator to change the trust status of vendors for their enterprise.

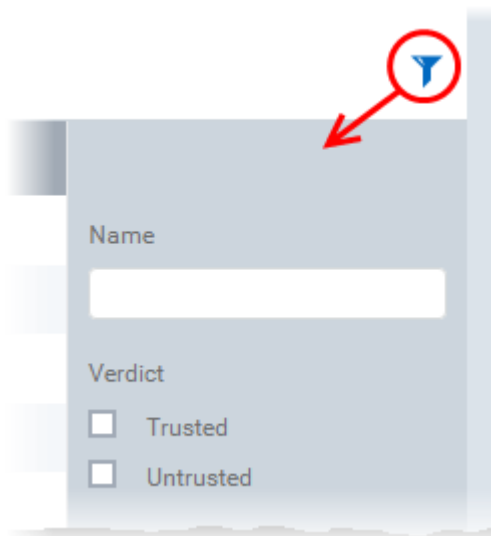


The 'Software Publishers' - Column Descriptions

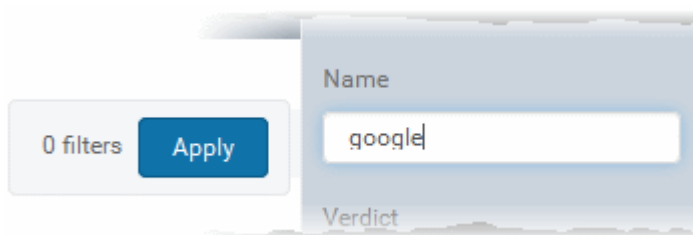
Column Heading	Description
Name	Displays the name vendor.
Verdict	Indicates whether the vendor is trusted or untrusted, based on global Trusted Vendor List.

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 name, enter the search criteria in part or full in the 'Name' text boxes and click 'Apply'.



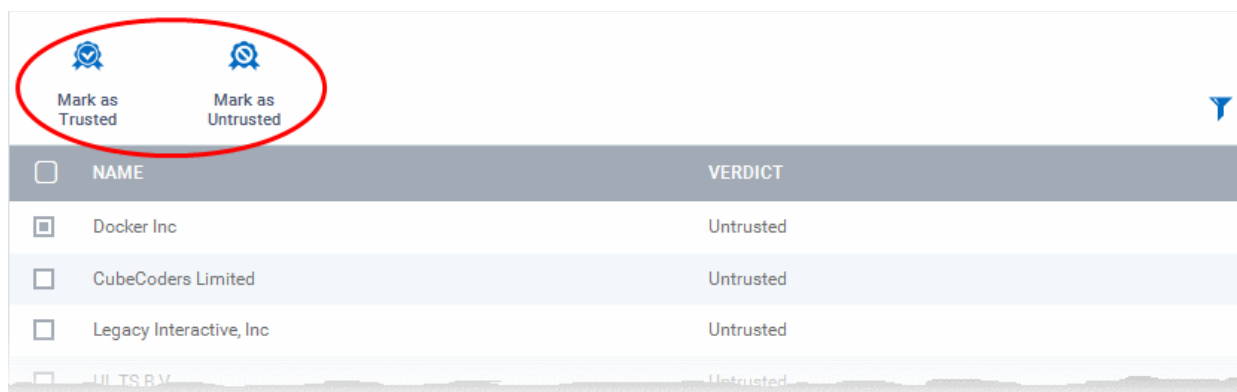
- To filter the items based on their trust status, choose the option under 'Verdict' and click 'Apply'.

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

- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CDM 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.

Trust Status of Software Vendors

The default trust status of the vendors are as per the global Trusted Vendors List, constantly updated and maintained at Comodo. Administrators can rate a vendor as trusted or untrusted based on their assessment for their enterprise.



- To change the Untrusted Vendor to Trusted, choose the vendor and click 'Mark as Trusted' at the top.
- To change the Trusted Vendor to Untrusted, choose the vendor and click 'Mark as Untrusted' at the top.

7.5. Installing OS Patches on Windows Endpoints

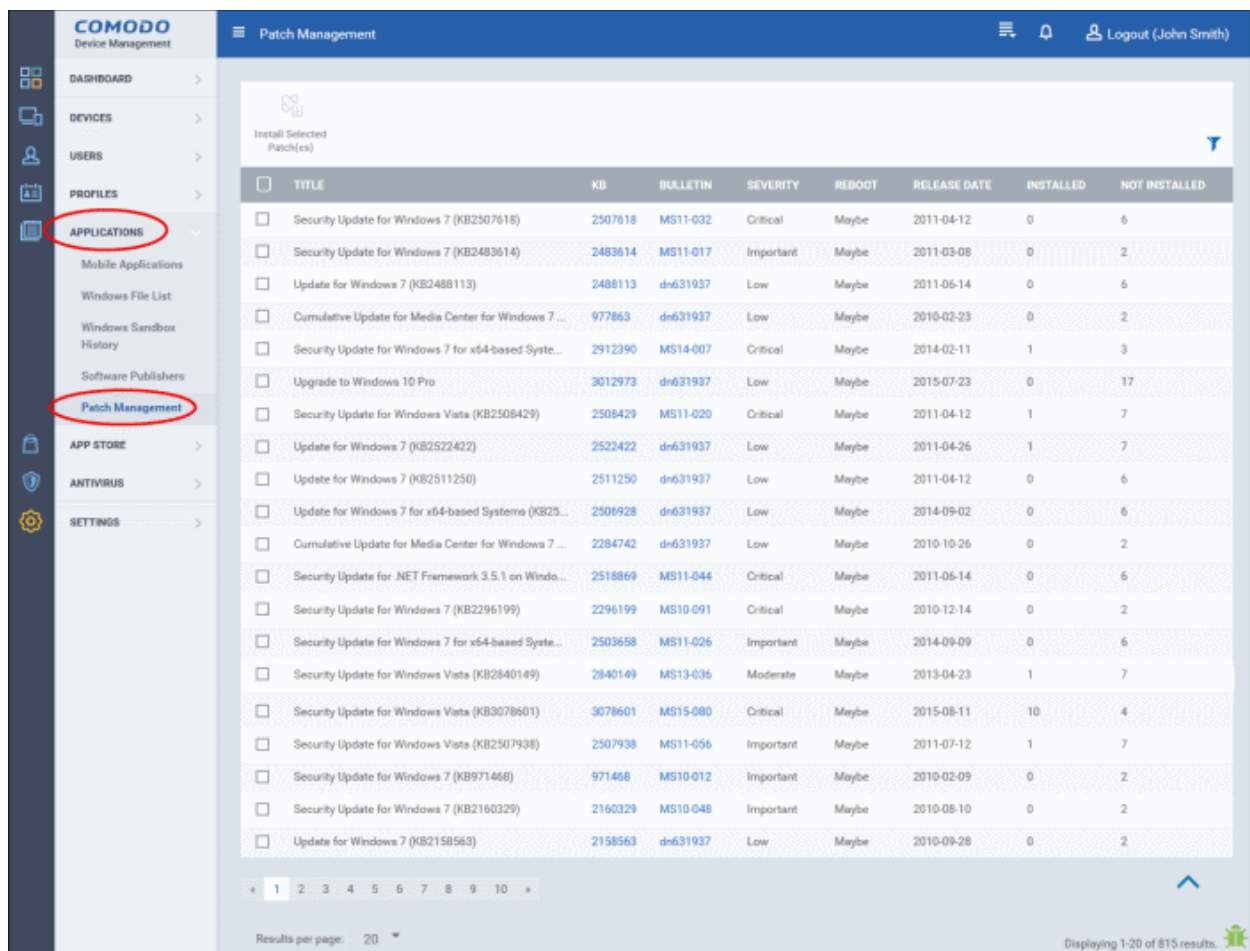
CDM allows administrators to install patches to selected Windows devices from the 'Devices' interface or all the managed devices from the 'Applications' section. Refer to the section '[Viewing and Installing Windows Patches](#)' to know more about installing patches to individual Windows devices. The 'Patch Management' feature under the 'Applications' section allows to deploy patches to all the managed Windows devices. The screen displays the available patches, number of endpoints they are installed and not installed, patch release date and its severity.

Important Note: The Patch Management feature will be visible only if this is enabled in Settings > Extensions. Refer to the section '[Managing CDM Extension](#)' for more details.

To view and install patches on Windows endpoints

- Click the 'Applications' tab from the left and select 'Patch Management' from the options


The list of all the OS patches and update packages that are applicable to the operating systems of the managed endpoints will be displayed.



Patch Management Table - Column Descriptions	
Column Heading	Description
Title	The name of the patch
KB	Clicking this link will take you to the Microsoft web page that provides the details of the patch.
Bulletin	Clicking this link will take you to the 'Security Bulletins' page hosted by Microsoft.
Severity	Indicates the level of severity for the patch. The severity levels are:

	<ul style="list-style-type: none">• Unknown• Critical• Important• Low• Moderate• None
Reboot	Indicates whether a reboot is required after the patch installation
Release Date	The date on which the patch was released by Microsoft
Installed	Indicates the number of managed endpoints the patch is installed
Not Installed	Indicates the number of managed endpoints to which the patch is yet to be installed

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 patches or search for a specific patch, enter the details in part or full and /or select the check box and click 'Apply'.
 - Title - Filters the items based on the name of the patch
 - KB - Filters the items based on the KB number
 - Bulletin - Filters the items based on the entered bulletin details
 - Severity - Filters the items based on the selected severity level
 - Reboot - Filters the items based on the selected reboot option
 - Release Date - Filters the items based on the entered release date
 - Installed - Filters the items based on the number of endpoints on which the patches are installed
 - Not Installed - Filters the items based on the number of endpoints on which the patches are yet to be installed

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

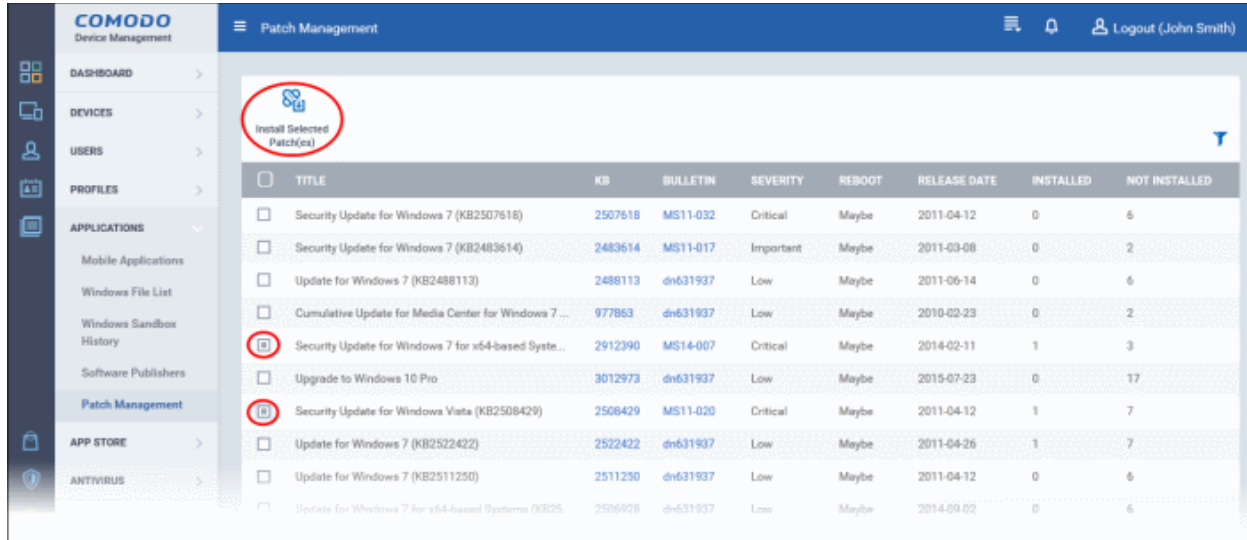
- To display all the items again, remove / deselect the search key from the filters and click 'Apply'.
- By default CDM returns 20 results per page when you perform a search. To increase the number of results displayed

per page up to 200, click the arrow next to 'Results per page' drop-down.

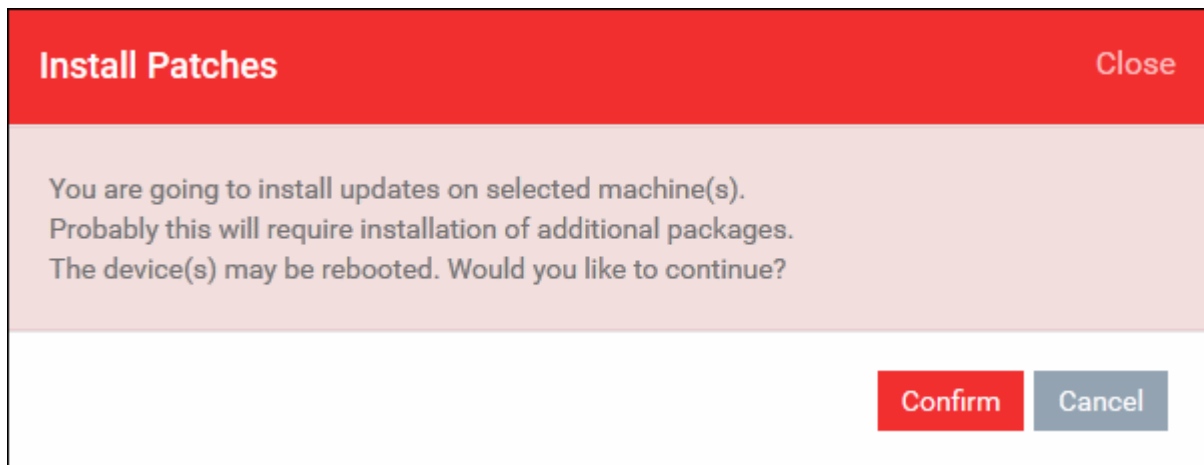
To install patch(es) on managed endpoints

Patches that are available and the number of endpoints on which they are installed and not installed can be found under the 'Installed' and 'Not Installed' columns.

- Select the patch(es) to be installed from the list and click 'Install Selected Patch(es)'



A warning dialog will be displayed.



- Click 'Confirm' to proceed with the installation

The command will be sent and the selected patch(es) will be installed on the endpoint(s).

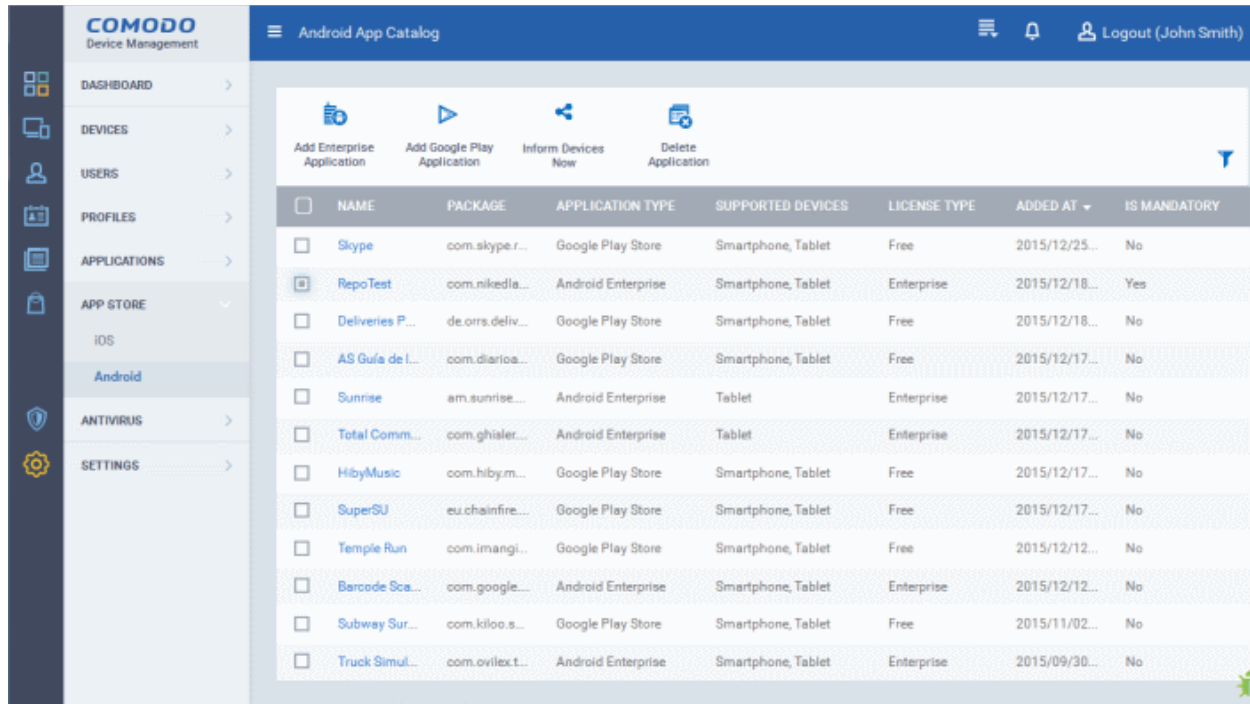
8.App Store

The App Store allows administrators to add and manage Android and iOS applications and push them to managed devices. CDM maintains a repository of custom and enterprise apps from Google Play and the Apple 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 Apple Store, you can specify the app name or bundle identifier. CDM 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 CDM directly. The device agent will download the app from the CDM 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 by tapping the 'Application' stripe in the CDM agent interface.

The App Store tab contains two sub tabs for adding and managing Android and iOS applications.



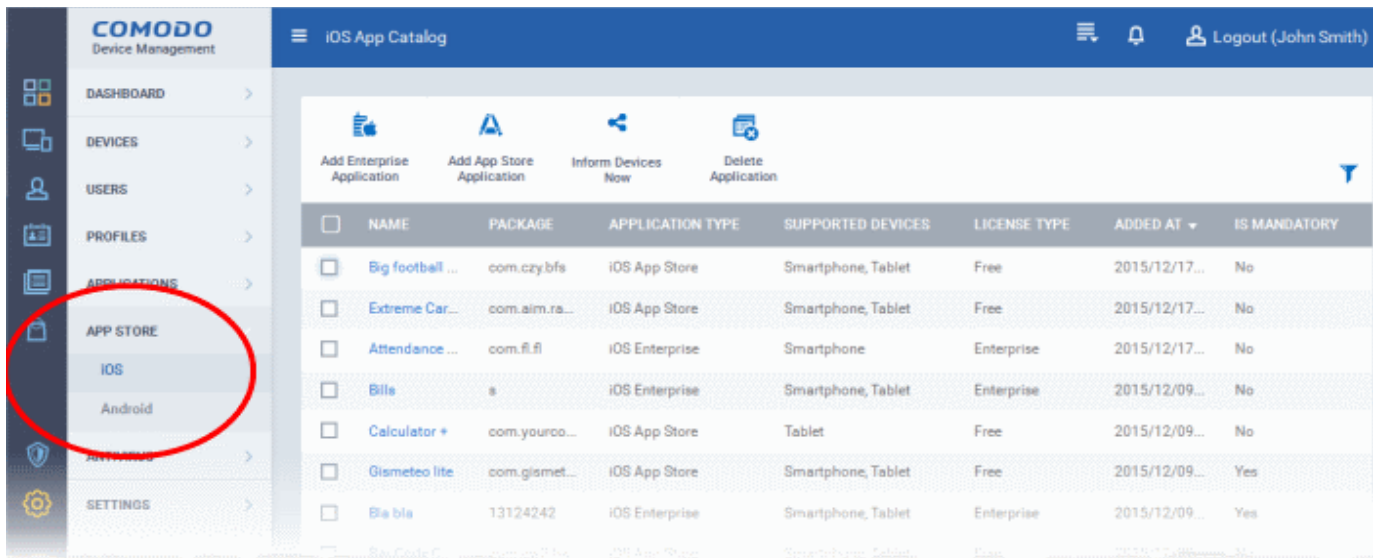
The following sections contain more details on each app type:

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

8.1.iOS Apps


The 'iOS App Catalog' 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 App Catalog' interface, click 'App Store' from the left and choose 'iOS' from the options.



'iOS App Catalog' - Column Descriptions	
Column Heading	Description
Name	Displays the name of the application. Clicking on the name of an app opens the 'Application Details' screen that displays the details like description, version number, license type, whether the app is mandatory or optional, download URL. The Application Details screen also allows you to edit the app details . Refer to the section Managing iOS Apps for more details.
Package	Displays the Bundle Identifier of the app.
Application Type	Indicates the source type of the app. Possible types are: <ul style="list-style-type: none"> • iOS App Store Application • iOS Enterprise Application uploaded by the administrator
Supported Devices	Displays the type of devices for which the application is compatible.
License Type	Indicates whether the app is a free, paid or enterprise version.
Added At	Displays the date and time at which the app was added to repository.
Is 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.

Sorting, Search and Filter Options

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

- To filter the items or search for a specific app based on the app name and/or its package name, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

- To filter the items based on their application type, select the criteria under 'Application 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 'Is 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 CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The following sections explain in detail on:

- [Adding iOS Apps and Installing them on Devices](#)
- [Managing iOS Apps](#)

8.1.1. Adding iOS Apps and Installing them on Devices

You can add iOS apps to the repository both from App Store and by uploading custom/enterprise apps for installation on to managed iOS smart phones and tablets.

The following sections provide more details on:

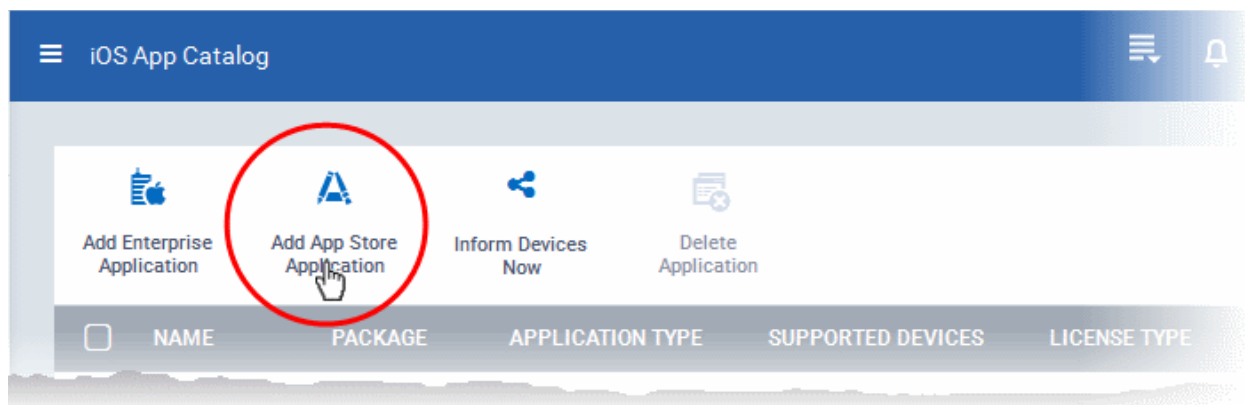
- [Adding iOS Apps from App Store](#)
- [Adding Custom/Enterprise iOS Apps](#)

Adding iOS Apps from App Store

The iOS Apps from the App Store can be added by simply specifying the name of the application as it is available in the App Store page. All the other details including the version, iTunes Store ID, iTunes Package name, and so on, will be automatically fetched from the App Store page and will be populated in the 'Add iOS App Store Application' screen. You can just enter first few letters in the name of the App, CDM 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 'App Store' from the left and choose 'iOS' to open the 'iOS App Catalog' interface
- Click on 'Add App Store Application' from the options at the top.



The 'Apple Store Application' screen will open.

Apple Store Application

Name

Version

iTunes Store ID

iTunes Package Name

License Type

Free
 Paid

Category

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

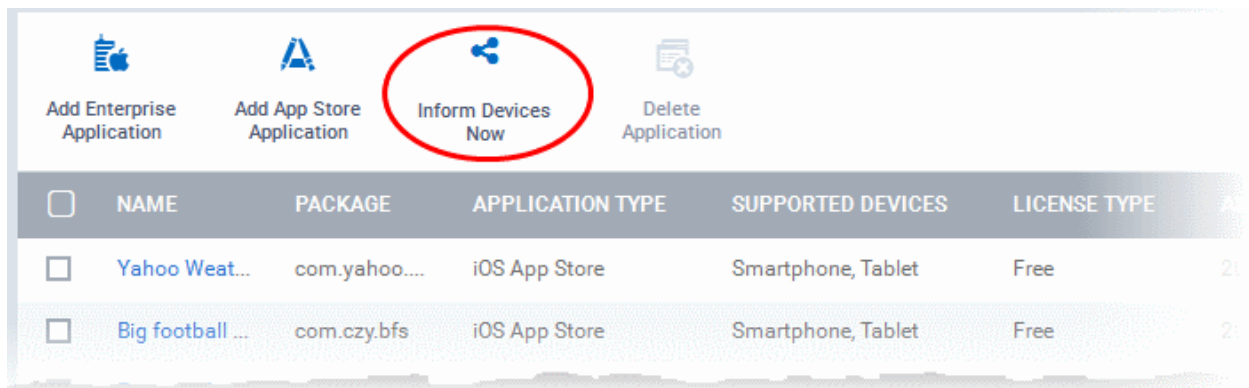
Apple Store Application - Table of Parameters		
Form Element	Type	Description
Name	Text Field	<p>Allows you to enter the name of the application.</p> <ul style="list-style-type: none"> Start entering the first few letters of the name of the application. <p>CDM will search for Apps from the App Store using the letters entered as search criteria and display the matching results as a drop-down</p> <ul style="list-style-type: none"> Choose the App to be added from the drop-down <p>On choosing the App all the other fields excluding the last few options will be auto-populated.</p>
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	<p>The iTunes Store ID number of the App. This field will be auto-populated on entering the correct App name in the 'Name' field.</p> <p>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/CDM/id807480077, the numbers after ID is the iTunes Store ID for this app.</p>
iTunes Package name	Text Field	<p>The package name of the app. This field will be auto-populated on entering the correct App name in the 'Name' field.</p> <p>For example, the Package name for CDM client is com.comodo.CDM.client</p>
License Type	Radio Button	<p>Allows you to specify whether the app is free or a paid version.</p> <p>This option will be pre-chosen depending on the App chosen in the 'Name' field.</p>
Category	Drop-down	<p>The category will be auto-selected depending on the App chosen in the 'Name' field</p> <p>The drop-down also enables you to choose the category to which the App belongs.</p>
Supported devices	Drop-down	<p>The device type will be auto-selected depending on the App chosen in the 'Name' field</p> <p>The drop-down also enables you to choose the device types to which the App is compatible.</p>
Description	Text Field	<p>The 'Description' field will be auto-populated with the description of the selected App, from the App Store page.</p> <p>The text field also enables you to enter your description or edit the existing description.</p>
Mandatory App	Checkbox	<p>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.</p> <p>Refer to the section Installing Apps on Devices for more details.</p>
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 when the CDM 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.

Apple Store Application - Table of Parameters		
Form Element	Type	Description
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 screenshots 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 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 'iOS App Catalog' interface.



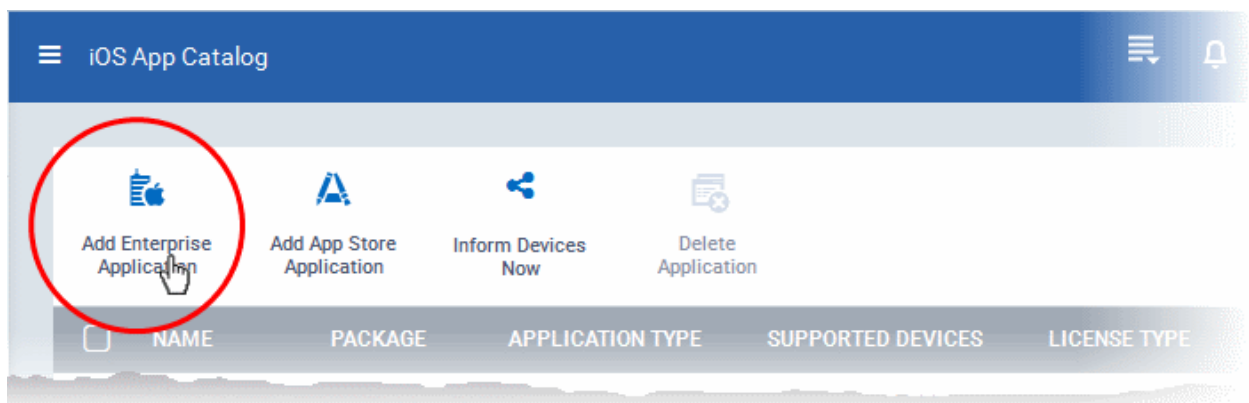
Adding Custom/Enterprise iOS Apps

Custom and Enterprise applications to be installed on the managed iOS devices can be added to the CDM 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 CDM console is accessed.

To add Custom/Enterprise iOS Apps

- Click 'App Store' from the left and choose 'iOS' to open the 'iOS App Catalog' interface
- Click on 'Add Enterprise Application' from the options at the top.



The 'Apple iOS Enterprise Application' screen will open.

Apple iOS Enterprise Application

[Cancel](#) [Save](#)

Name

Version

Bundle ID

Category
 ▼

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'

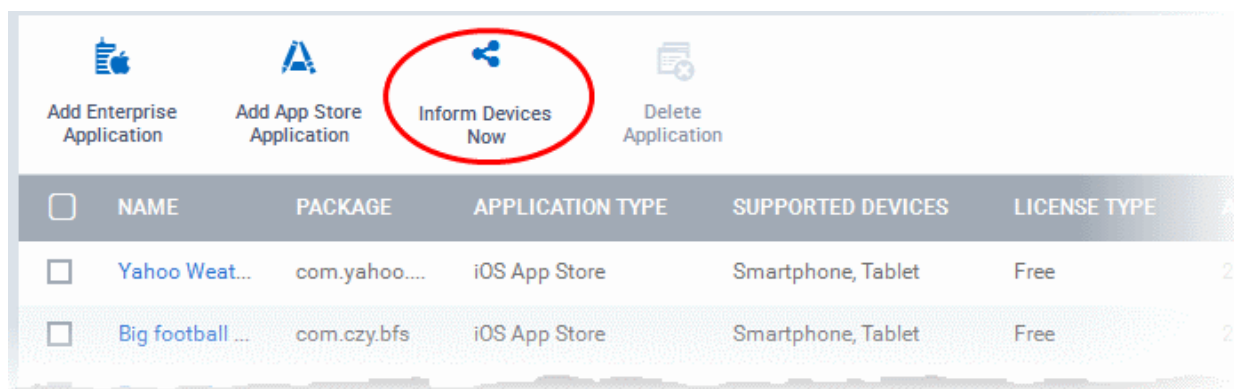
The file will be uploaded and the details will be auto-populated.

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/CDM/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 MDM profile is removed	Checkbox	If enabled, the app will be automatically uninstalled from the device, if the CDM profile applied to the device is removed.
Source File	Browse button	Enables you to navigate and select the source file for the app to be uploaded.
Application logo	Browse button	Enables you to upload the logo image for the App.
Application screenshots	Browse button	Allows you to upload screenshots of the app, if required.

- Click 'Save' after entering the details.

The App will be added to the App repository and will be listed in the 'App Catalog' interface and will be synched to the devices during their next poll.

- If you want the devices to be notified to install the app, click 'Inform Devices Now' from the options above the table in the 'App Catalog' interface.

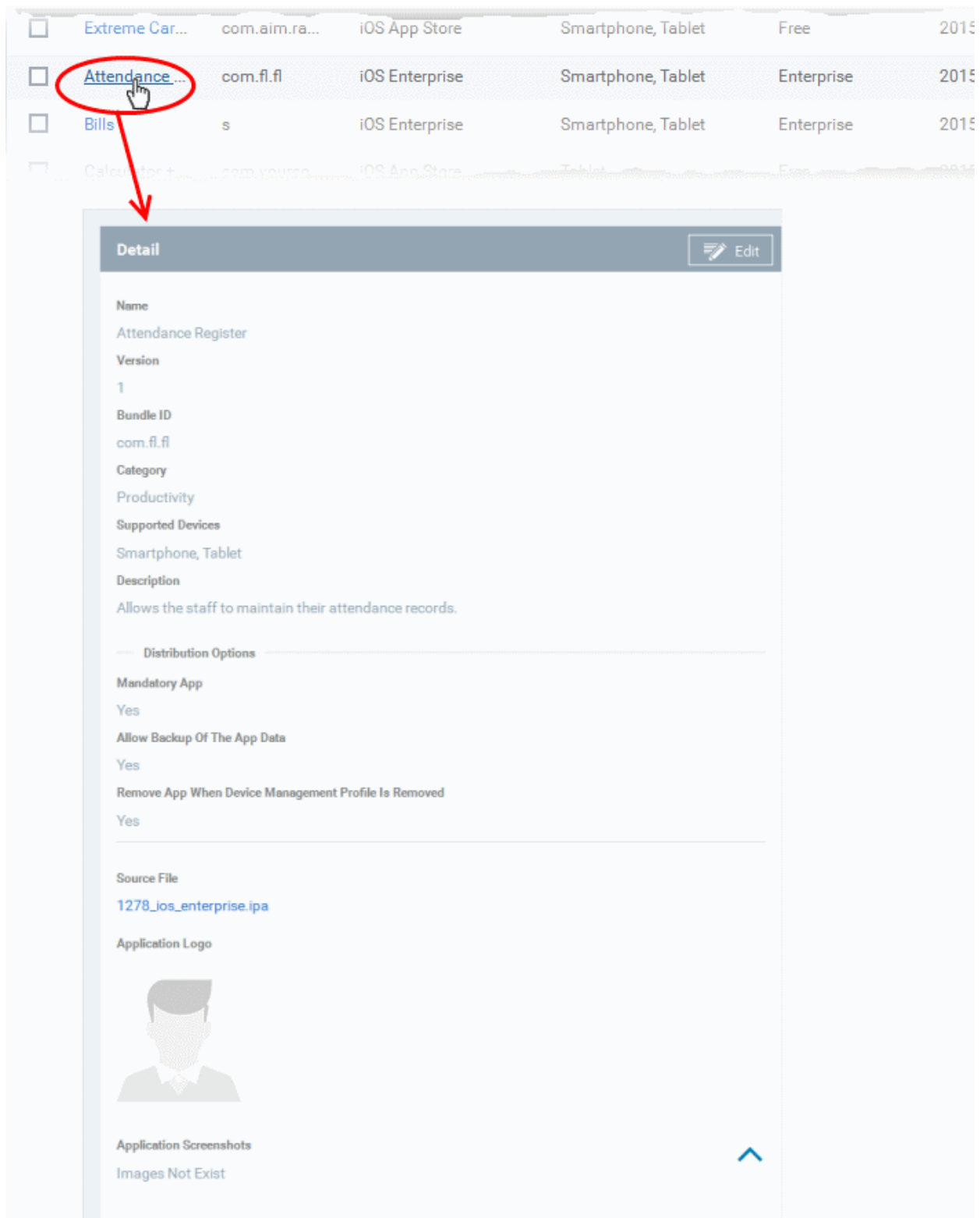


8.1.2. Managing iOS Apps

The 'Application Details' page for a selected application from the list in iOS App Catalog, displays complete details of the 'App' and allows you to edit the details.

To open the 'App Details' page

- Click 'App Store' from the left and choose 'iOS' to open the 'iOS App Catalog' interface
- Click on the name of the App.



The 'Application Details' page displays the details of the App, including the logo, screenshots and the download URL, depending on whether it is iOS App Store App or Custom/Enterprise App. The details page also allows you to edit the details of the App.

To edit the details of an application

- Click on the 'Edit' button  at the top right .

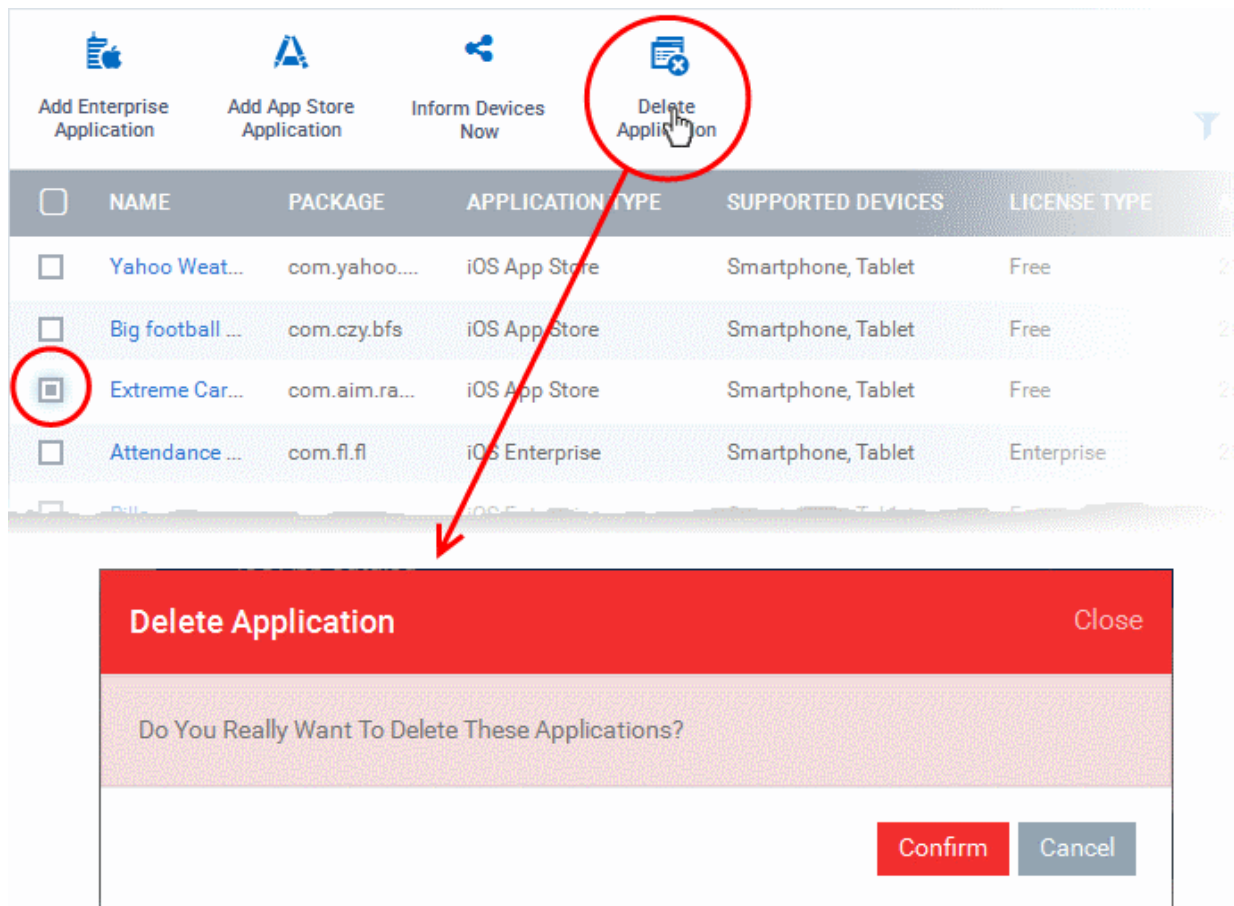
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section [Adding iOS Apps and Installing them on Devices](#).

Removing Apps from the iOS App Catalog

You can remove unwanted applications from the App Repository at any time. If the option 'Remove from device when removed from app catalog' is selected while adding/editing an App, the App will also be removed from the devices at which it is installed.

To remove selected Apps

- Click 'App Store' from the left and choose 'iOS' to open the 'iOS App Catalog' interface
- Select the App(s) to be removed and click 'Delete Application' from the options above the table.

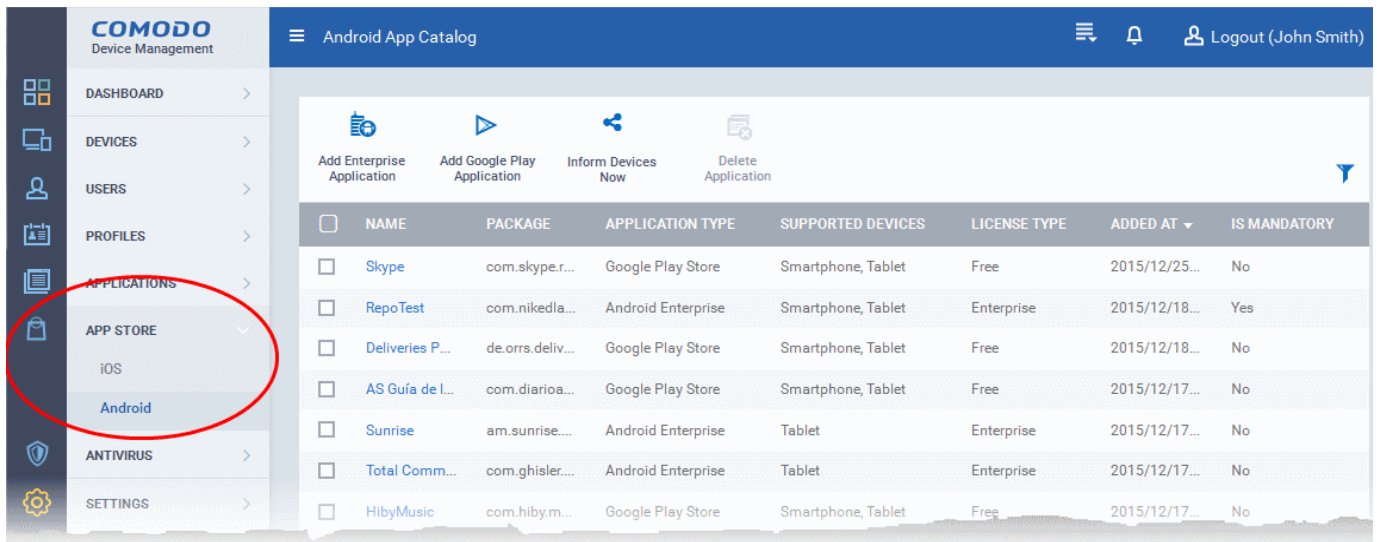


- Click Confirm in the confirmation dialog to remove the app(s)

8.2. Android Apps


The 'Android App Catalog' 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 to 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 App Catalog' interface, click 'App Store' from the left and choose 'Android' from the options.



'iOS App Catalog' - Column Descriptions	
Column Heading	Description
Name	Displays the name of the application. Clicking on the name of an app opens the 'Application Details' screen that displays the details like description, version number, license type, whether the app is mandatory or optional, download URL. The Application Details screen also allows you to edit the app details . Refer to the section Managing Android Apps for more details.
Package	Displays the Bundle Identifier of the app.
Application Type	Indicates the source type of the app. Possible types are: <ul style="list-style-type: none"> • Google Play Store Application • iOS Enterprise Application uploaded by the administrator
Supported Devices	Displays the type of devices for which the application is compatible.
License Type	Indicates whether the app is a free, paid or enterprise version.
Added At	Displays the date and time at which the app was added to repository.
Is 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.

Sorting, Search and Filter Options

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

- To filter the items or search for a specific app based on the app name and/or its package name, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

- To filter the items based on their application type, select the criteria under 'Application 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 'Is 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 CDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The following sections explain in detail on:

- [Adding Android Apps and Installing them on Devices](#)
- [Managing Android Apps](#)

8.2.1. Adding Android Apps and Installing them on Devices

You can add Android apps to the repository both from Google Play Store and by uploading custom/enterprise apps for installation on to managed Android smart phones and tablets.

The following sections provide more details on:

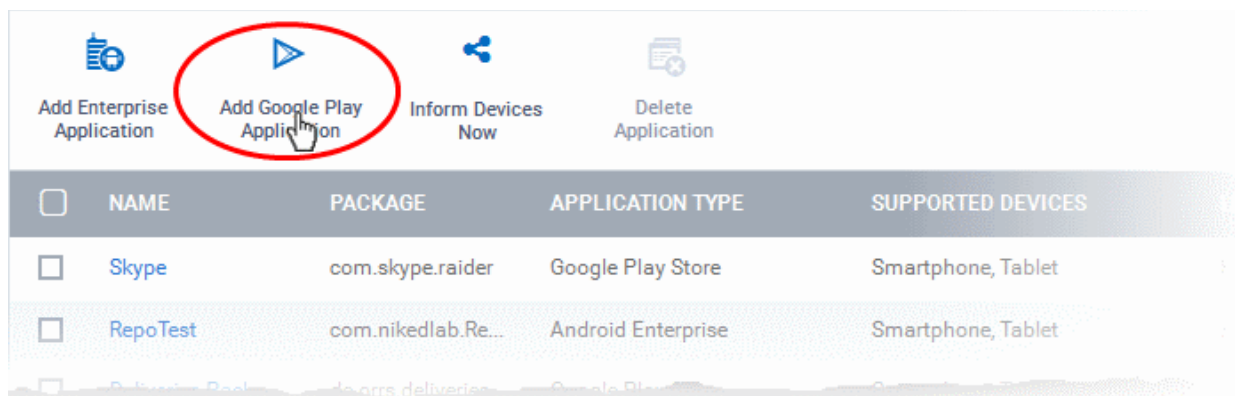
- [Adding Android Apps from App Store](#)
- [Adding Custom/Enterprise Android Apps](#)

Adding Android Apps from Google Play Store

The Android Apps from the Google Play Store can be added by simply specifying the name of the application as it is available in the Play Store page. All the other details including the version, bundle ID, app logo and so on, will be automatically fetched from the Google Play Store page and will be populated in the 'Google Play Application' screen. You can just enter first few letters in the name of the App, CDM 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 'App Store' from the left and choose 'Android' to open the 'Android App Catalog' interface
- Click on 'Add Google Play Application' from the options at the top.



The 'Google Play Application' screen will open.

Google Play Application
Cancel Save

Name

Version

Bundle ID i

License Type

Free

Paid

Category

Select Category
▼

Supported Devices

Select Supported Devices
▼

Description

Distribution Options

Mandatory App

Remove From Device When Removed From App Catalog

Application Logo

Application Screenshots

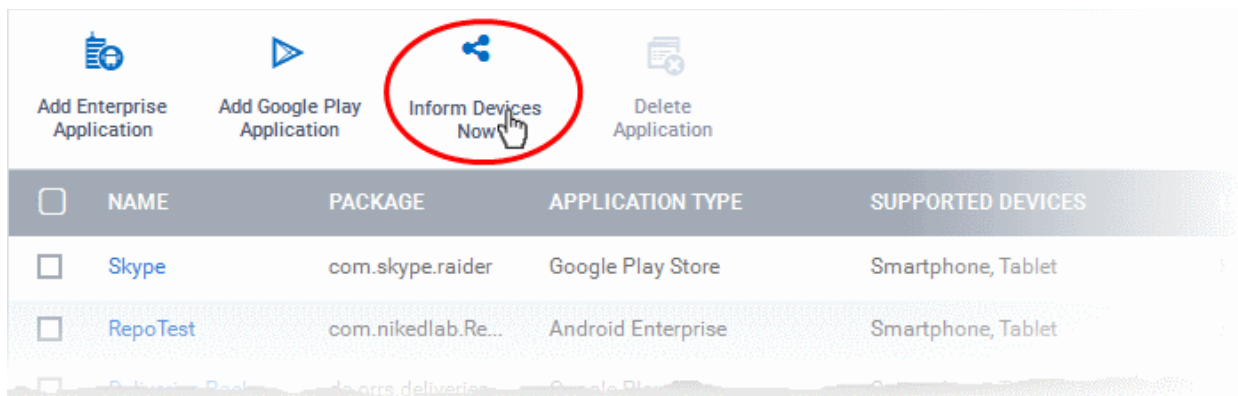
Google Play Application - Table of Parameters		
Form Element	Type	Description
Name	Text Field	<p>Allows you to enter the name of the application.</p> <ul style="list-style-type: none"> Start entering the first few letters of the name of the application. <p>CDM will search for Apps from the Google Play Store using the letters entered as search criteria and display the matching results as a drop-down</p> <ul style="list-style-type: none"> Choose the App to be added from the drop-down

Google Play Application - Table of Parameters		
		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.
Bundle ID	Text Field	<p>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:</p> <p>https://play.google.com/store/apps/details?id=com.comodo.pimsecure&hl=en</p> <p>The identifier, com.comodo.pimsecure, identifies this as Comodo Antivirus Free app.</p> <p>Clicking the help icon beside the field displays how to retrieve the bundle identifier for the Play Store Apps.</p> <p>This field will be auto-populated on entering the correct App name in the 'Name' field.</p>
License Type	Radio Button	<p>Allows you to specify whether the app is free or a paid version.</p> <p>This option will be pre-chosen depending on the App chosen in the 'Name' field.</p>
Category	Drop-down	<p>The category will be auto-selected depending on the App chosen in the 'Name' field.</p> <p>The drop-down also enables you to choose the category to which the App belongs.</p>
Supported devices	Drop-down	<p>The device type will be auto-selected depending on the App chosen in the 'Name' field.</p> <p>The drop-down also enables you to choose the device types to which the App is compatible.</p>
Description	Text Field	<p>Allows you to enter a description for the App.</p> <p>The 'Description' field will be auto-populated with the description of the selected App, from the Google Play Store page.</p> <p>The text field also enables you to edit the description or enter your own description of the app.</p>
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 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 'Android App Catalog' interface.



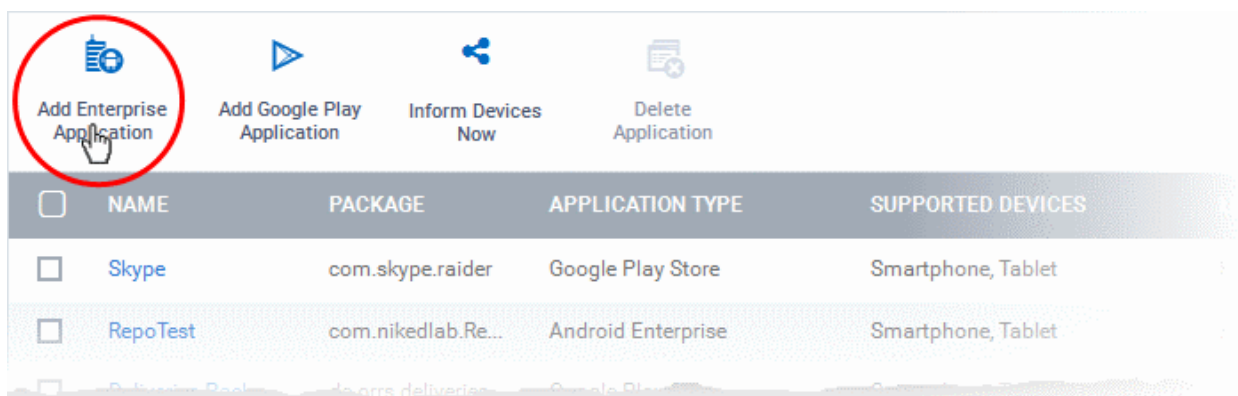
Adding Custom/Enterprise Android Apps

Custom and Enterprise applications to be installed on the managed Android devices can be added to the CDM App repository by simply 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 just need to manually enter only some of 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 CDM console is accessed.

To add Custom/Enterprise Android Apps

- Click 'App Store' from the left and choose 'Android' to open the 'Android App Catalog' interface
- Click on 'Add Enterprise Application' from the options at the top.



The 'Enterprise Android Application' screen will open.

Enterprise Android Application
Cancel Save

Name

Version

Bundle ID

Category

Select Category
▼

Supported Devices

Select Supported Devices
▼

Description

Distribution Options

Mandatory App

Install & Uninstall This Application Silently When Possible

Source File

Browse

Application Logo

Browse

Application Screenshots

Browse

- 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.

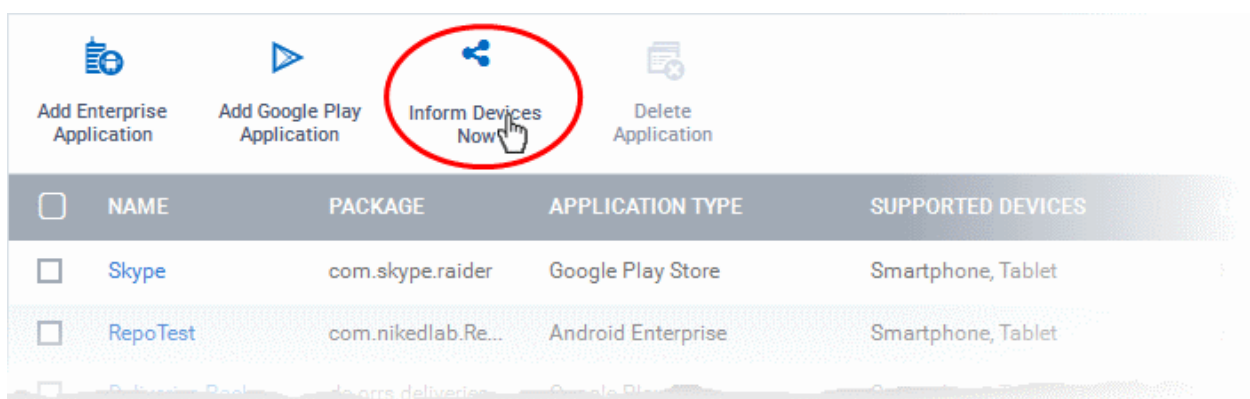
Add Enterprise Android Application - Table of Parameters		
Form Element	Type	Description
Name	Text Field	The name of the application as obtained from the .apk file. If the name is not auto-populated, enter the name of the app.
Version	Text Field	The version of the application as obtained from the .apk file. If it is not auto-

Add Enterprise Android Application - Table of Parameters		
		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 'App Catalog' 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 App Catalog' interface.



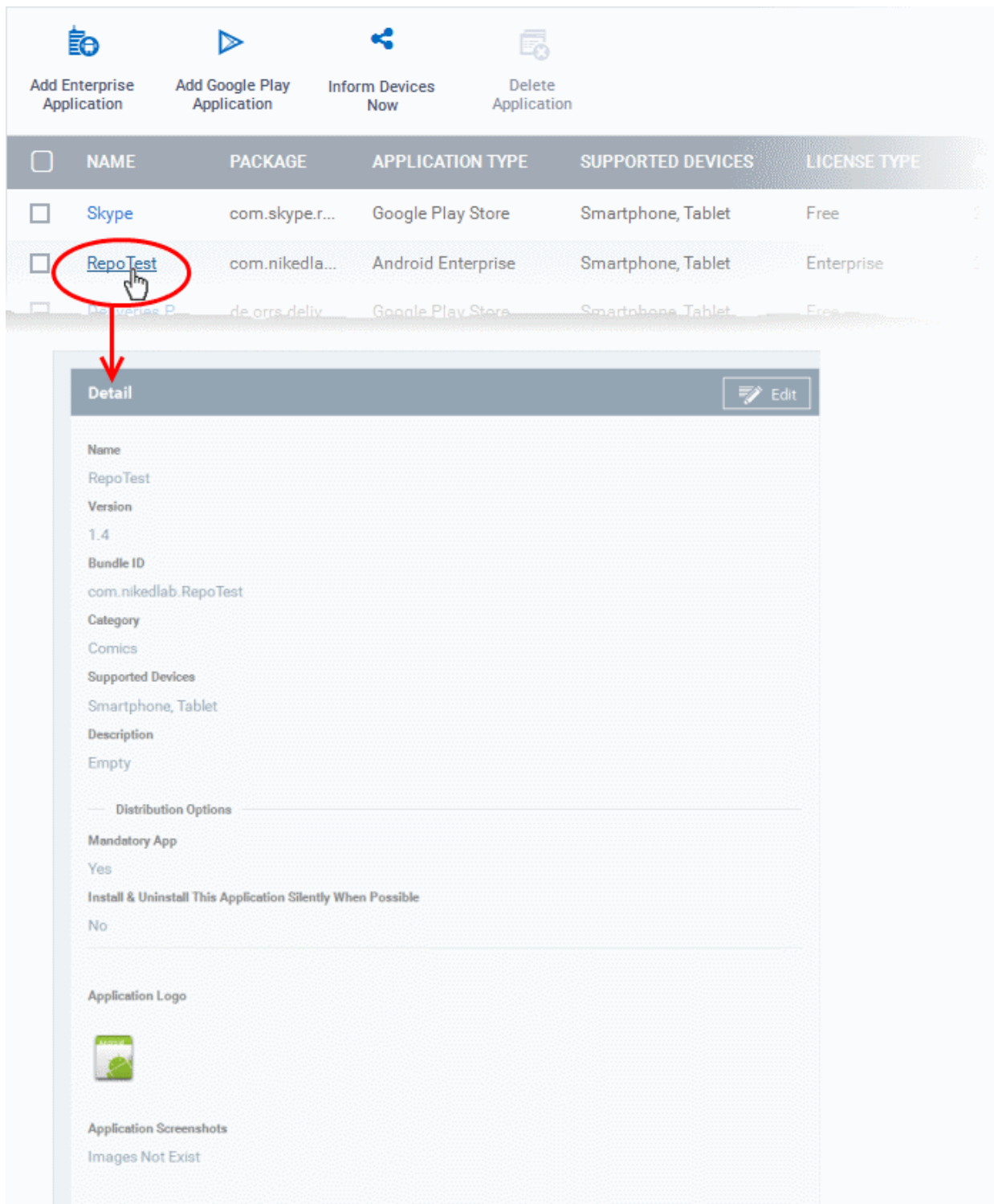
8.2.2. Managing Android Apps

The 'Application Details' page for a selected application from the list in Android App Catalog, displays complete details of the 'App' and allows you to edit the details.

To open the 'App Details' page

- Click 'App Store' from the left and choose 'Android' to open the 'Android App Catalog' interface

- Click on the name of the App.



The 'Application Details' page displays the details of the App, including the logo, screenshots and the download URL, depending on whether it is Google Play Store App or Custom/Enterprise App. The details page also allows you to edit the details of the App.

To edit the details of an application

- Click on the 'Edit' button  at the top right .

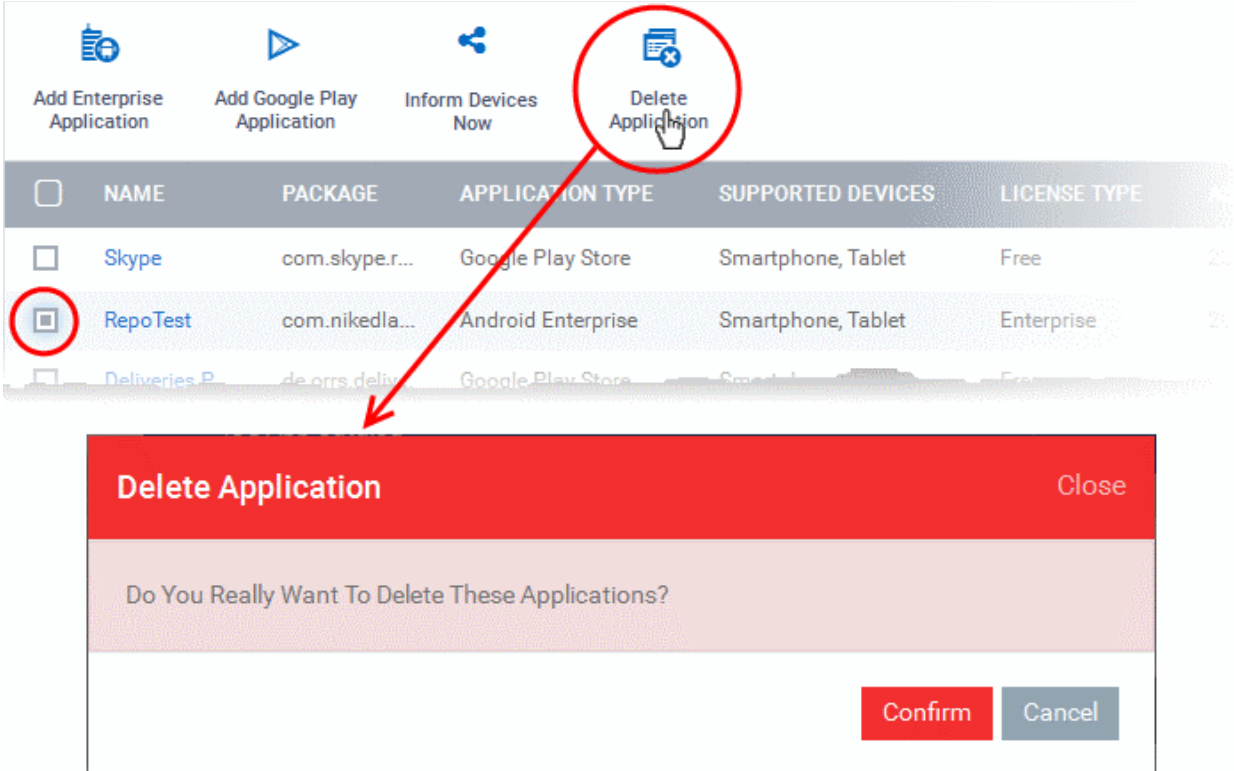
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, refer to the section [Adding Android Apps and Installing them on Devices](#).

Removing Apps from the iOS App Catalog

You can remove unwanted applications from the Android App Repository at any time. If the option 'Remove from device when removed from app catalog' is selected while adding/editing an App, the App will also be removed from the devices at which it is installed.

To remove selected Apps

- Click 'App Store' from the left and choose 'iOS' to open the 'iOS App Catalog' interface
- Select the App(s) to be removed and click 'Delete Application' from the options above the table.



The screenshot shows the 'Delete Application' dialog box in the Comodo Device Manager interface. The dialog box is titled 'Delete Application' and has a 'Close' button in the top right corner. The main text of the dialog box asks 'Do You Really Want To Delete These Applications?'. At the bottom right, there are two buttons: 'Confirm' (in red) and 'Cancel' (in grey). A red circle highlights the 'Delete Application' button in the top navigation bar, and a red arrow points from it to the dialog box. The background shows a table of applications with columns for NAME, PACKAGE, APPLICATION TYPE, SUPPORTED DEVICES, and LICENSE TYPE. The application 'RepoTest' is selected, indicated by a red circle around its checkbox.

<input type="checkbox"/>	NAME	PACKAGE	APPLICATION TYPE	SUPPORTED DEVICES	LICENSE TYPE	
<input type="checkbox"/>	Skype	com.skype.r...	Google Play Store	Smartphone, Tablet	Free	2:
<input checked="" type="checkbox"/>	RepoTest	com.nikedla...	Android Enterprise	Smartphone, Tablet	Enterprise	2:
<input type="checkbox"/>	Deliveries P...	de.grrs.deliv...	Google Play Store	Smartphone, Tablet	Free	2:

9. Antivirus

The 'Antivirus' interface allows administrators to view the infection status of Android and Windows devices, initiate on-demand scans and to initiate virus database updates. The interface also allows administrators to view and manage specific malware found on Android and Windows devices, to view a history of threats identified from all devices, and to view/manage items moved to quarantine on Windows endpoints.

OS TYPE	DEVICE NAME	OWNER	LAST SCAN ACTIVITY	MALWARE STATUS	LAST SCAN STATE
Windows	BOBSMITH...	John Smith	2016/01/08 06:49:30 ...	Clean	Complete
Windows	ADMIN-PC	John Smith	2016/01/08 06:54:20 ...	Clean	Scan Command Sent
Windows	WIN8-CES-1	Sviatoslav	2015/12/25 02:08:23 ...	Unknown	Scan Canceled
Android	samsung_G...	Sviatoslav	2015/12/25 01:59:33 ...	Clean	Scan Canceled
Windows	VM_8_1	pkorshak	2015/12/07 11:23:57 ...	Clean	Scan Canceled
Android	LENOVO_Le...	avantistudeE	2016/01/08 06:42:18 ...	Clean	Complete
Windows	MAKSGUZZ...	maksguzz	2016/01/04 12:44:06 ...	Clean	Complete
Windows	MAKSGUZZ...	maksguzz	2015/12/23 01:05:40 ...	Clean	Complete
Windows	USER-86F6...	agolovko-test	2015/12/15 01:46:00 ...	Clean	Scan Canceled

The following sections contain more details on each area:

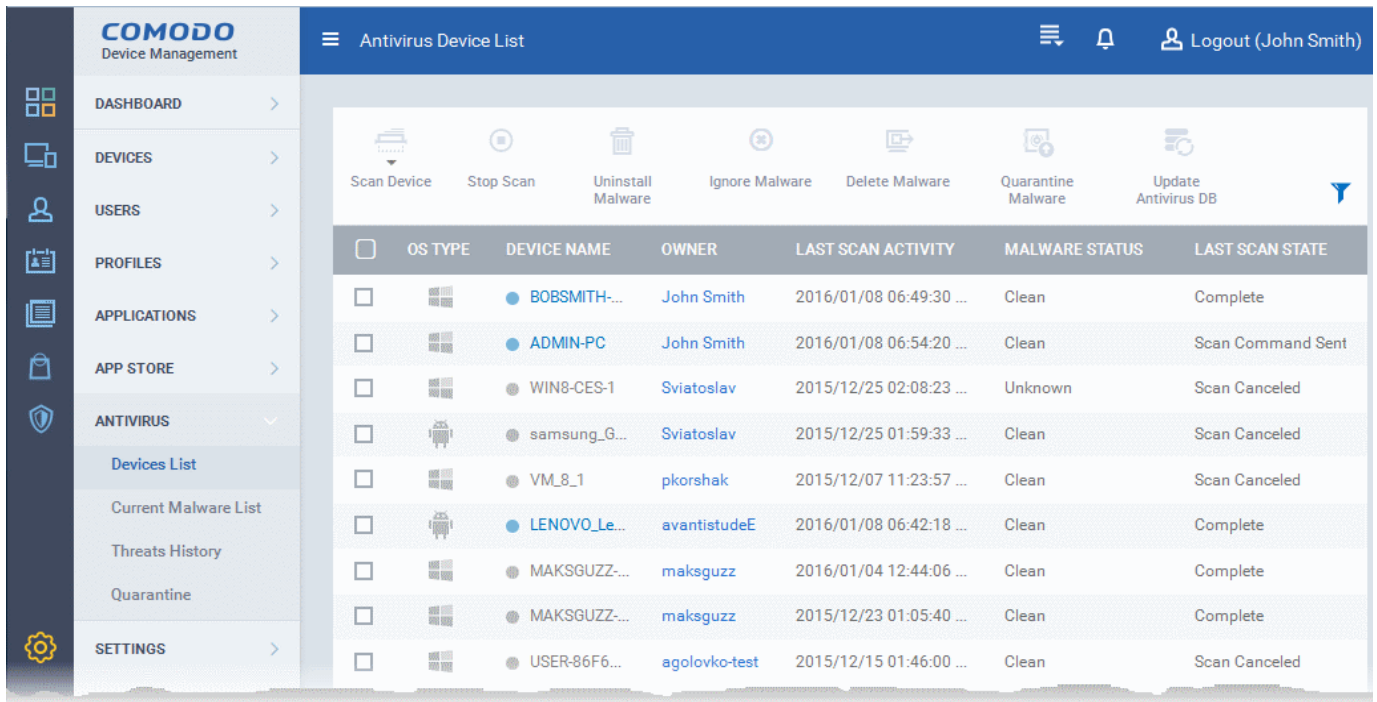
- **Antivirus scans**
 - **Running on-demand virus scans on devices**
 - **Handling malware found on devices**
 - **Updating virus signature database on devices**
- **Viewing and managing identified Malware**
- **Viewing Threats History**
- **Viewing and managing quarantined Items**

9.1. Antivirus Scans

The Antivirus 'Device List' displays the infection status of Android and Windows devices and enables you to run on-demand antivirus scans on selected devices. It also allows you to choose the action to be taken on discovered malware.

Note: Comodo Endpoint Security software on endpoint machines is capable of running scheduled antivirus scans. You can define the areas to be scanned and the schedule of the scan in the 'Antivirus' component of a Windows configuration profile. 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**.


- To open the Antivirus 'Device List' interface, click Antivirus from the left and choose 'Device List' from the options.

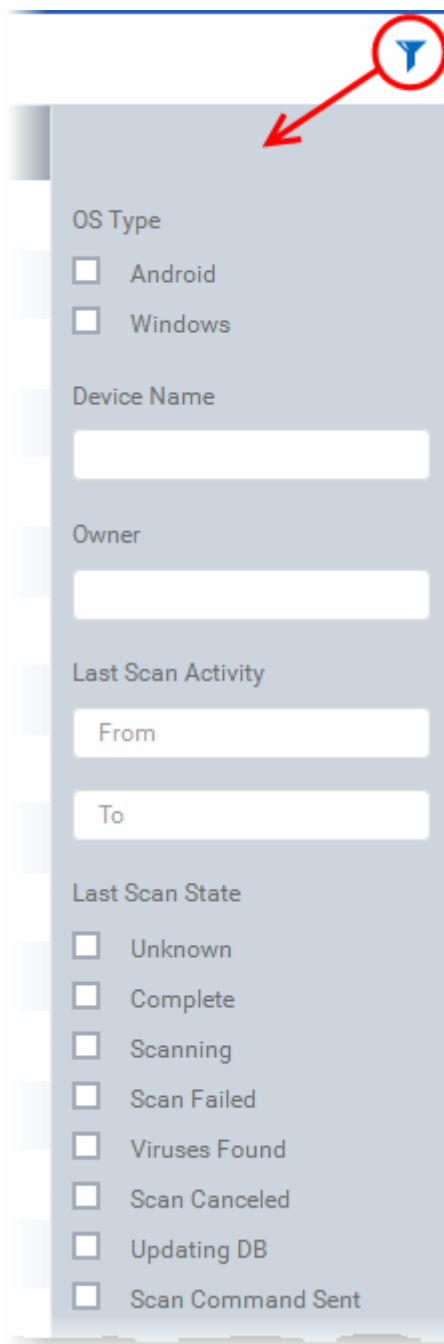


The list displays all Android and Windows devices along with the device owner, date of the last virus scan, infection status and the progress of the most recent scan.

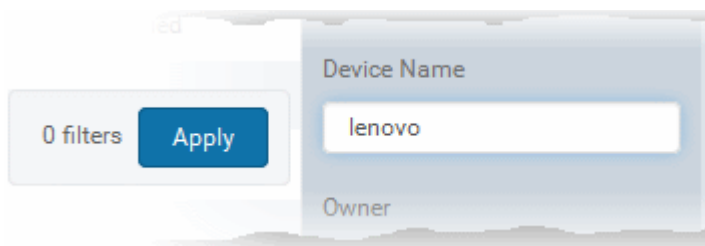
AV Scan - Column Descriptions	
Column Heading	Description
OS Type	Indicates whether the device is an Android device or a Windows endpoint.
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the device name opens the detailed 'View Device' interface. Refer to the sections Managing Windows Devices and Managing Android/iOS Devices for more details.
Owner	Indicates the owner/user of the device. Clicking the user name will open the 'View User' interface, displaying the details of the user. Refer to the section Viewing the Details of a User for more details.
Last Scan Activity	Indicates the date and time at which the last antivirus scan was run.
Malware Detection Status	Indicates whether the device is found infected or not, from the results of the last scan.
Last Scan State	Indicates the status of last run scan or currently running scan.

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 device based on device name and/or owner, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- To filter the items based on OS types, select the OS types of the devices to be displayed in the list
- To filter the devices last scanned within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under 'Last Scan Activity', using the calendars that appear on clicking inside the respective field and click 'Apply'.

- To filter the devices based on their last or current scan status, select the status under 'Last Scan State' and click 'Apply'.

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

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

Following sections explain more about:

- [Running On-Demand Antivirus Scans on Devices](#)
- [Handling Malware identified from Scanned Devices](#)
- [Updating virus signature database at selected Devices](#)

9.1.1. Running On-Demand Antivirus Scans on Devices

The 'Antivirus Devices List' scans interface allows administrators to initiate on-demand virus scans on Android and Windows devices.

Note: The scans interface allows you to manage on-demand scans only. For automatic or scheduled AV scans, administrators should specify the scan schedule in a configuration profile then push it to the selected devices or groups. Refer to the section [Creating Configuration Profiles](#) for more details.

To launch an on-demand AV scan

- Choose 'Antivirus' from the left then select 'Device List'.
- Select the Android or Windows device(s) you wish to scan.
- Click 'Scan Device'

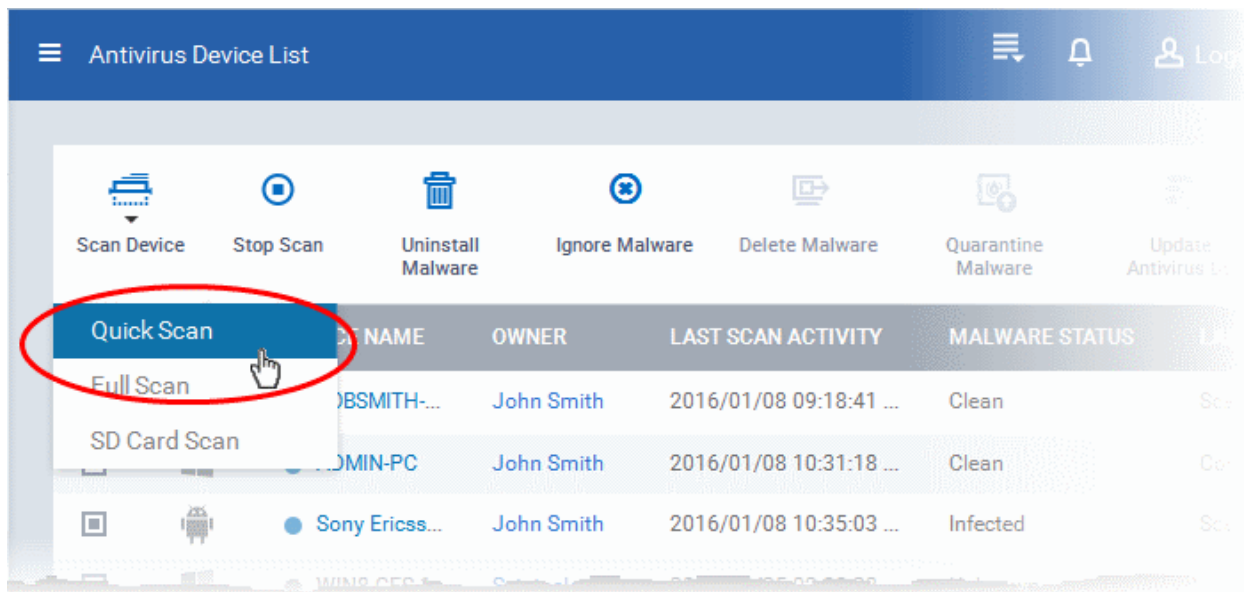
Tip: You can filter or search for specific devices using the filter options that appear on clicking the funnel icon at the top right. For example, you may want to display only devices with scan states of 'Unknown', 'Scan Failed' and 'Scan Canceled'.

The next step is to choose the scan profile that defines the areas to be scanned in the selected device(s). The profiles differ depending on the OS type of the chosen devices. The following sections explain the scan process for:

- [Android Devices](#)
- [Windows Devices](#)

Android Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Quick Scan** - Scans the critical areas of the device, which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include RAM, hidden services and other significant areas like system files. These areas are of great importance to the health of the device so it is essential to keep them free of infection.
- **SD Card Scan** - Scans all folders/files in the Secure Digital (SD) memory card mounted on the device.
- **Full scan** - Scans all the folders/files in both the system internal memory and the SD card.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

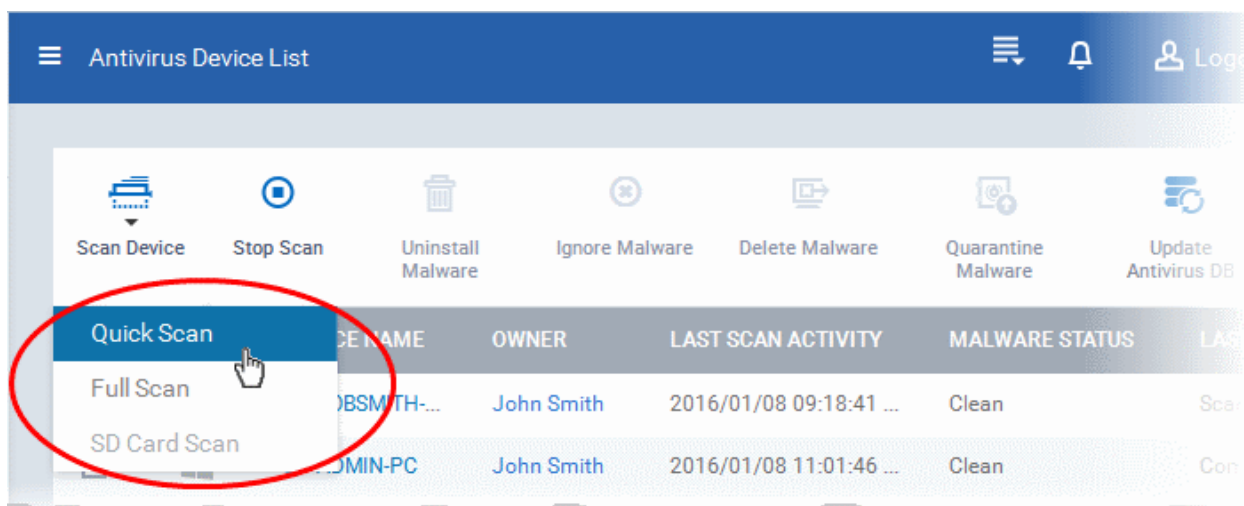
- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found on completion of scan the Last Scan State will indicate 'Infected'. The infections identified after the scan will be treated as configured in the Android Client Antivirus Settings interface accessible by clicking 'Settings' > 'Android Client Configuration' > 'Antivirus'. Refer to the section [Configuring Android Client Antivirus Settings](#) for more details. If 'Manual control' is chosen, then the administrators have the option to uninstall or ignore from the results displayed in the Current Malware List interface. Refer to the section [Viewing and Managing Identified Malware](#) for more details.

The administrator can also choose to uninstall or ignore the identified malware by clicking the respective buttons at the top. Refer to the [Handling Malware Identified from Scanned devices](#) section for more details.

Windows Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Quick Scan** - The 'Quick Scan' scans critical areas of the computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of each computer so it is essential to keep them free of infection.
- **Full Scan** - The 'Full Scan' scans every local drive, folder and file on each computer. Any external devices like USB drives, digital camera and so on are also scanned.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scan' from the options at the top.

If malware is found on completion of scan the Last Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. Refer to the next section **Handling Malware Identified from Scanned devices** for more details.

Items moved to quarantine are encrypted and saved in the endpoint itself, so that they are isolated from the rest of the system. You view the quarantined items from the 'Quarantine' interface and have the option to delete the file, if the item is identified as malicious or restore it at the endpoint if the item is a false-positive. Refer to the section **Viewing and Managing Quarantined Items** for more details.

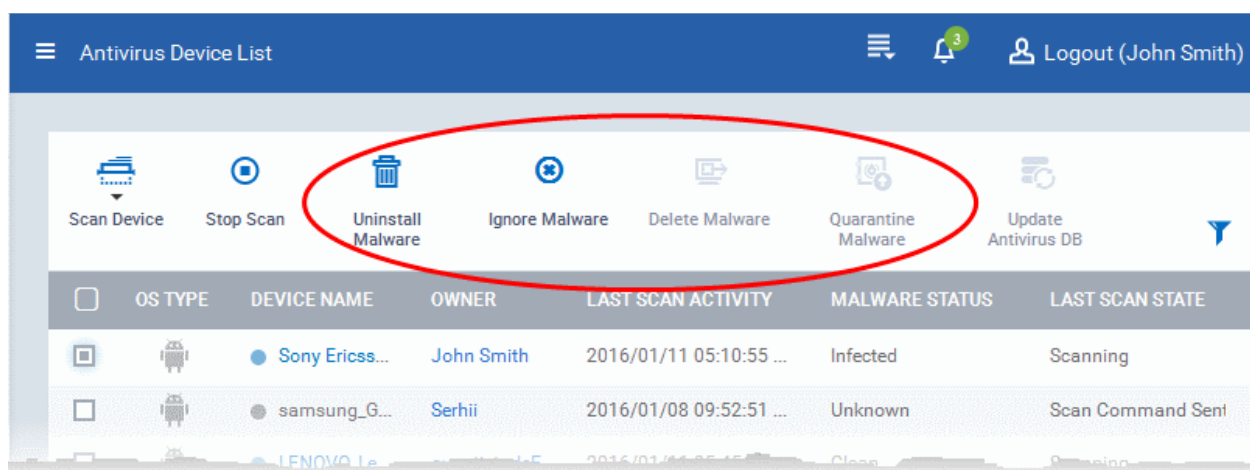
9.1.2. Handling Malware on Scanned devices

If malware is detected on a managed Android or Windows device, the 'Malware Status' column will display 'Infected' or 'Virus Found'. You can choose to remove, ignore or quarantine detected malware using the buttons above the table.

Tip: The 'Antivirus > Device List' interface allows you apply actions to all malware identified on a particular device. If you want to review and apply actions to individual pieces of a malware on a device, please use the 'Current Malware List' instead. Refer to the section **Viewing and Managing Identified Malware** for more details.

To choose the action to be taken on the detected malware

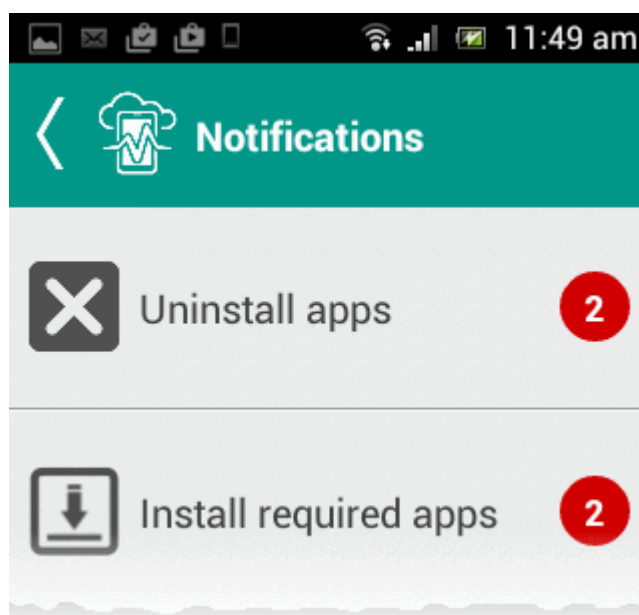
- Choose 'Antivirus' from the left then select 'Device List'.
- Select an infected Android or Windows device(s) using the check-boxes on the left.
- Choose an action from the top row:



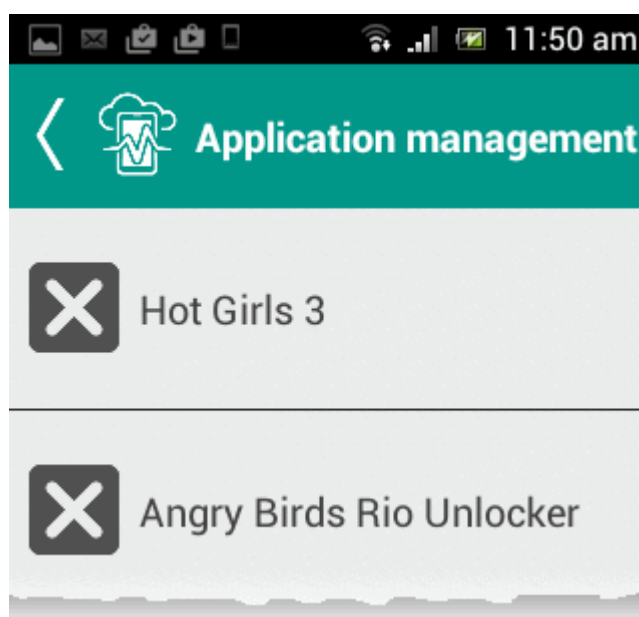
For Android Devices:

- **Uninstall Malware** - Uninstalls the malicious app
- **Ignore Malware** - Ignores the malware for the current scan. On the next scan, the item will be again identified as malware

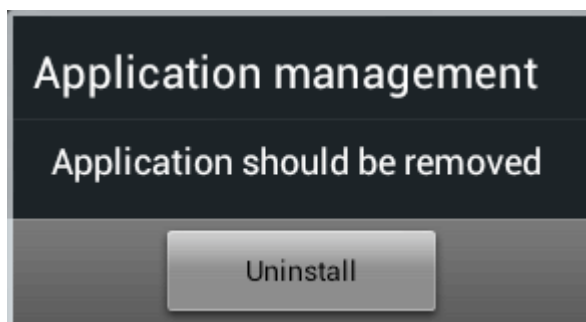
For the uninstall operation, a notification will be sent to all affected devices:



The notification will indicate the number of threats to be removed from the device. On touching the alert, a list of items to be removed will be displayed.



The user needs to tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



For Windows Devices

- Delete Malware - CDM instructs the CES application at the endpoint to clean the malware. If a disinfection routine is available for the selected infection(s), CES will disinfect the application and retain the application. If a disinfection routine is not available, CES will remove the application.
- Quarantine Malware - Moves the detected malware to the Quarantine in the device for later analysis. You can view quarantined files from the 'Quarantine' interface. Based on their trustworthiness, you can remove them from the device or restore them to their original locations. Refer to the section [Viewing and Managing Quarantined Items](#) for more details.

9.1.3. Updating Virus Signature Database at Windows Devices

In order to guarantee continued and effective antivirus protection on managed Windows devices, it is imperative that their virus databases are updated as regularly as possible. CDM allows you to automate the periodical virus database updates at the managed Windows devices by the configuring a schedule in the Endpoint Security Update Rule component in the Windows profile applied to the device. Refer to the explanation of configuring the [Endpoint Security Update Rule](#) component under the section [Creating Windows Profile](#) for more details.

You can also manually update the virus signature database at the managed Windows devices as and when required. The 'Device List' interface under 'Antivirus' allows you to remotely update the virus databases at selected devices.

To update virus signature database on selected endpoints

- Choose 'Antivirus' from the left then select 'Device List'.
- Select the Windows device(s) on which you wish to update the virus database.

	OS TYPE	DEVICE NAME	OWNER	LAST SCAN ACTIVITY	MALWARE STATUS	LAST SCAN STATE
<input type="checkbox"/>	Windows	ALEX-WIN7X64	sas	2015/12/20 06:48:54 PM	Clean	Complete
<input checked="" type="checkbox"/>	Windows	WIN10-CES-2	Serhii	2015/12/14 02:20:01 PM	Clean	Scan Canceled
<input checked="" type="checkbox"/>	Windows	WIN10-CES-4	Serhii	2016/01/11 05:43:50 AM	Unknown	Scanning

Tip: You can filter the list or search for specific device(s) by clicking the funnel icon at the top right of the table.

- Click 'Update Antivirus DB' from the options at the top.

A command will be sent to the CDM agent at the selected endpoints to start download the updates from the Comodo's update servers.

9.2. Viewing and Managing Identified Malware

The 'Current Malware List' interface displays a list of malicious apps, push ads, unsafe apps and threats identified from enrolled Android and Windows devices during on-access, scheduled and on-demand antivirus scans. The administrator can choose to uninstall the malicious items from the devices or quarantine the item. The administrator can also choose to ignore the item and to remove it from the malware list, If the item is safe and trustworthy.

Note:

For Android Devices:

If AV settings in the configuration profile active on a device is configured to automatically uninstall or ignore, the identified malicious item will be cleaned accordingly and will not be displayed in the Current Malware List interface. Refer to the section

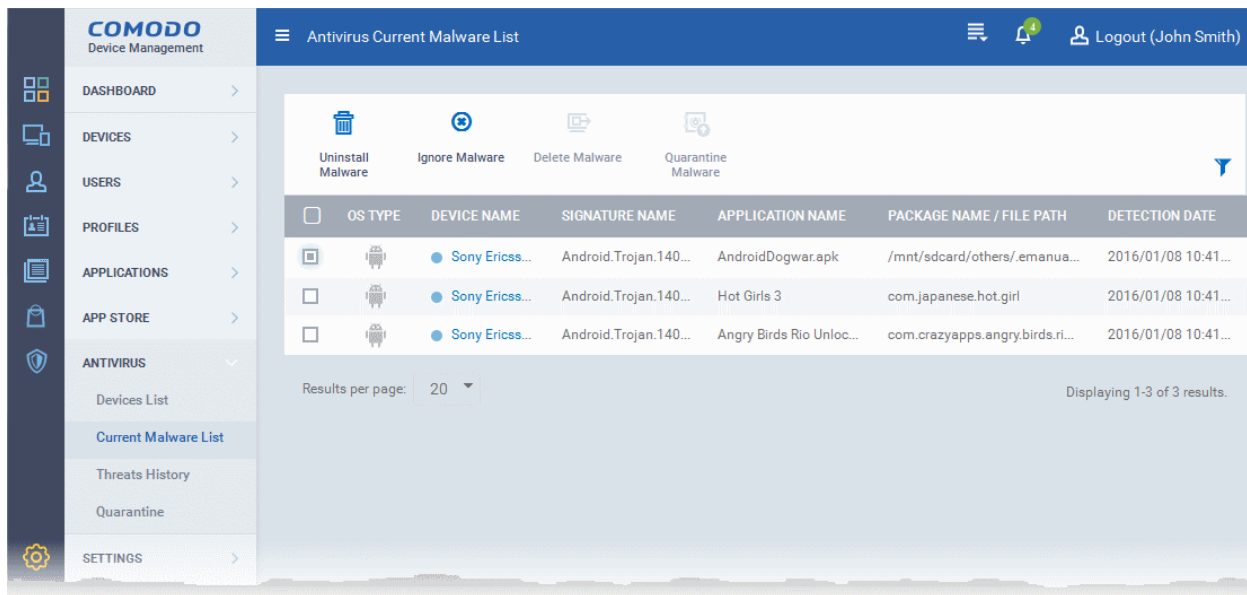
[Android Client Antivirus Settings](#) for more details.

For Windows Devices:

If 'Show antivirus alerts' is disabled and Quarantine Threats is chosen as default action in the 'Realtime Scan Settings' of the Antivirus component in the configuration profile active on the device, the identified threats will be moved to Quarantine automatically and will not be listed in this interface. If 'Show antivirus alerts' is enabled, and if the end user chooses to quarantine the threat from the displayed alert, the threat will be moved to quarantine at the device and not be displayed in this interface. Only if 'Block Threats' is chosen in both the cases, the threats will be displayed in this interface. Refer to the explanation of [Realtime Scan settings](#) in the section [Antivirus Settings](#) under [Creating Windows Profile](#) for more details.

To view the malware list


- Choose 'Antivirus' from the left then select 'Current Malware List'.



A list of malware identified from all the enrolled Android and Windows devices will be displayed.

Current Malware List - Column Descriptions	
Column Heading	Description
OS Type	Indicates operating system of the device from which the malware was identified.
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the section Managing an Individual Device for more details.
Signature Name	The name of the virus signature identified from the infected application.
Application Name	The name of the infected application.
Package Name	The Android package name or identifier of the package from which the app was installed.
Detection Date	The precise date and time at which the malware was identified.

Sorting, Search and Filter Options

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

OS Type

Android

iOS

Windows

Device Name

Signature Name

Application Name

Package Name / File Path

Detection Date

From

To

- To filter the items or search for a specific malware based on device name, signature name, infected application name, and/or package name/file path, enter the search criteria in part or full in the respective text boxes and click 'Apply'.

3 of 3 results.

0 filters **Apply**

Device Name

sony

Signature Name

- To filter the items based on OS types, select the OS types of the infected devices for respective items to be displayed in the list
- To filter the threats identified within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under 'Detection Date', using the calendars that appear on clicking inside the respective field and click 'Apply'.
- To filter the devices based on their last or current scan status, select the status under 'Last Scan State' and click 'Apply'.

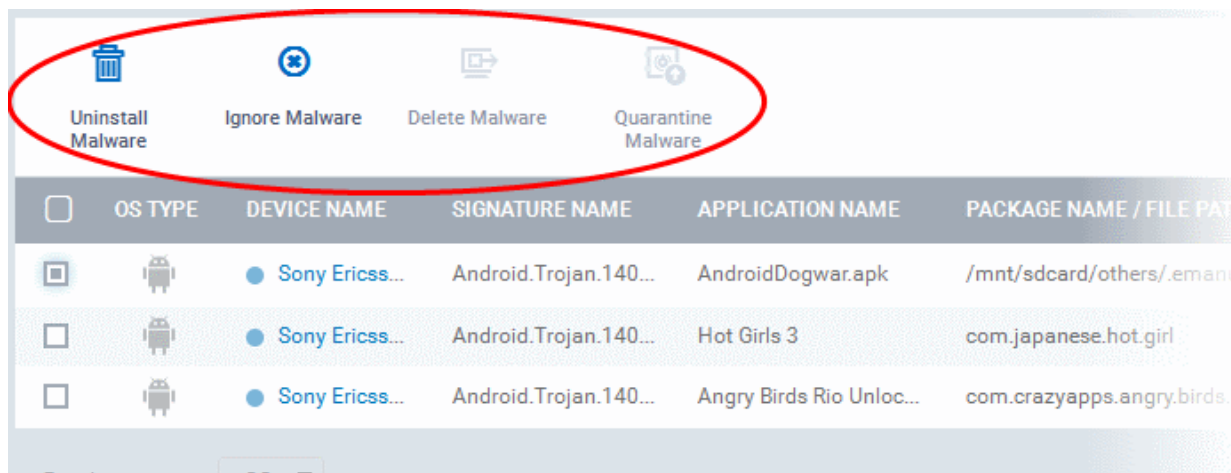
You can use any combination of filters at-a-time to search for specific devices.

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

Handling the Threats

If the item identified as malware is found to be a genuine virus, malicious app or a threat, the administrator can uninstall/delete from the devices at which it was found. If an item is found to be a false positive, the administrator can choose to ignore the item. The item will not be uninstalled from the device but will be removed from the 'Current Malware List' interface. If an item is found to be suspicious, the administrator can choose to move it to quarantine for later analysis and removal.

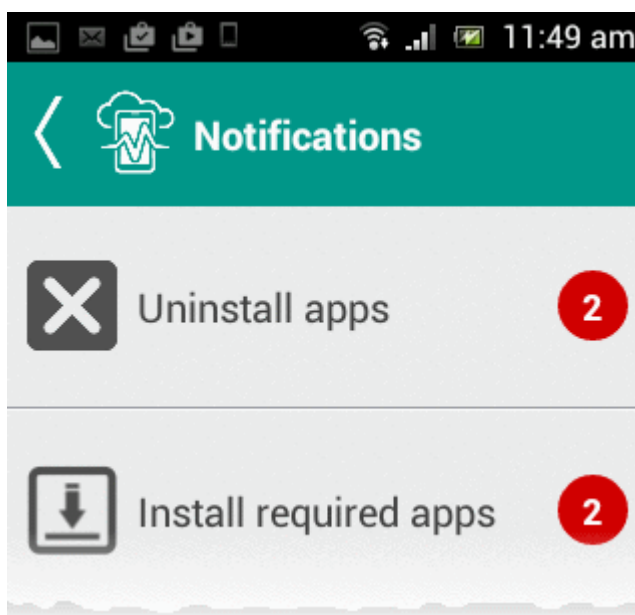
The options at the top of the table allow you to choose the action to be taken on selected items.



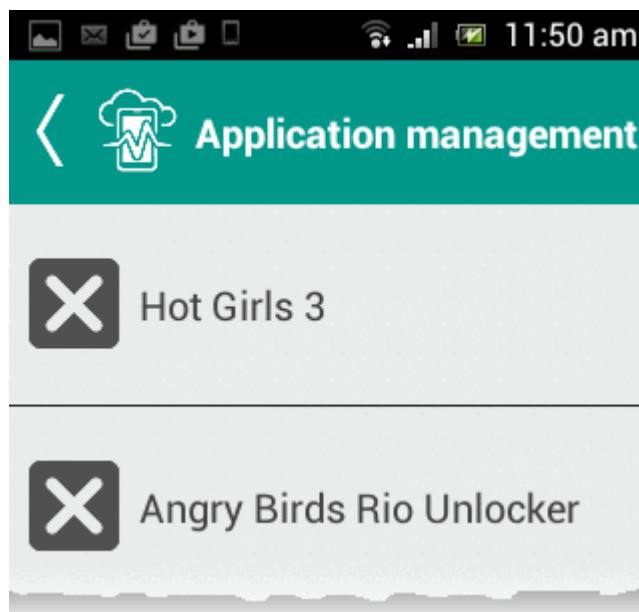
For threats identified from Android Devices

- If the identified item is a false positive, select the app from the list and click 'Ignore' from the options at the top.
- To remove malware package(s), select the packages from the list and click 'Uninstall' from the options at the top.

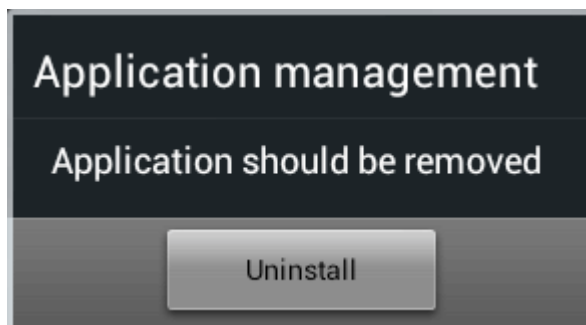
For the uninstall operation, a notification will be sent to all affected devices.



The notification will indicate the number of threats to be removed from the device. On touching the alert, a list of items to be removed will be displayed.



The user needs to tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



For threats identified from Windows Devices:

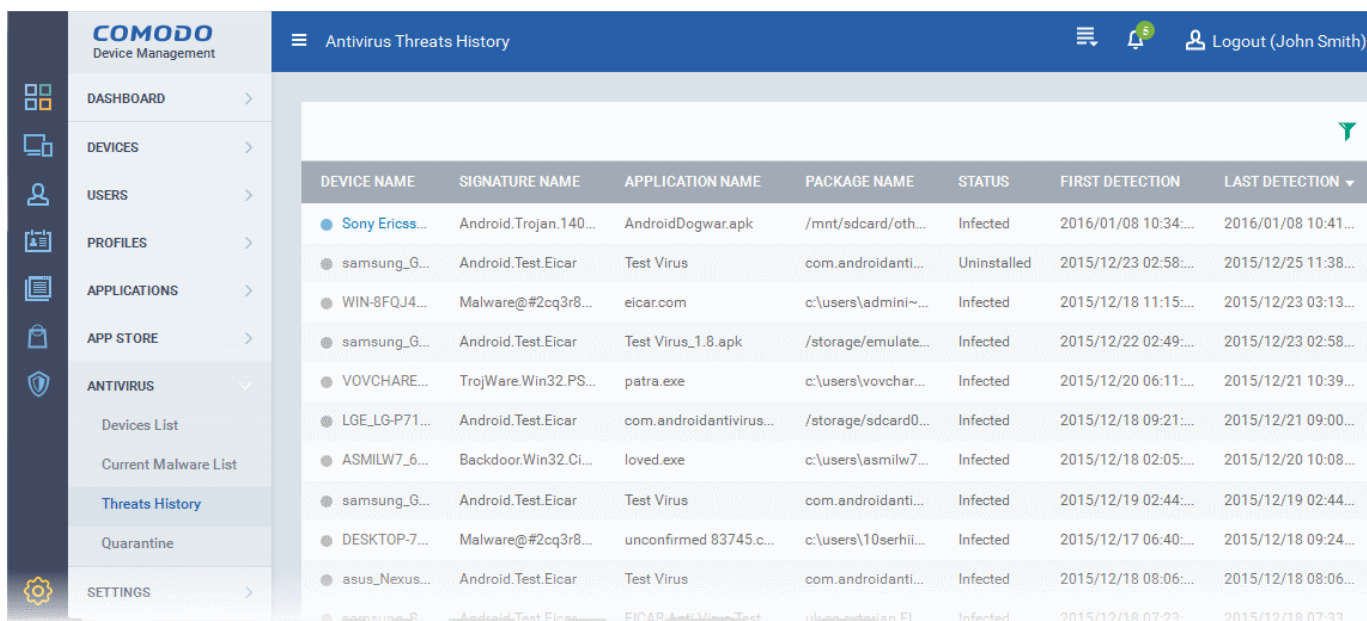
- If the identified item is a virus, select the app from the list and choose 'Delete'. If a disinfection routine is available in the CES for removing the malware, only the threat will be removed from the applications. Else, the infected application will be removed from the device.
- If the identified item is suspicious, select the item(s) and click 'Quarantine Malware'. The item(s) will be moved to quarantine in the respective device(s). You can analyze the quarantined files and if they are found trustworthy, you can restore them to their original locations, else remove them from the devices. Refer to the section [Viewing and Managing Quarantined Items](#) for more details.

9.3. Viewing Threats History

The 'Threats History' interface displays the list of all the threats and malware identified from Android and Windows devices during realtime, scheduled and on-demand scans in the past. The list includes both the items that are removed from the devices and those yet to be removed.


To view the history of threats identified

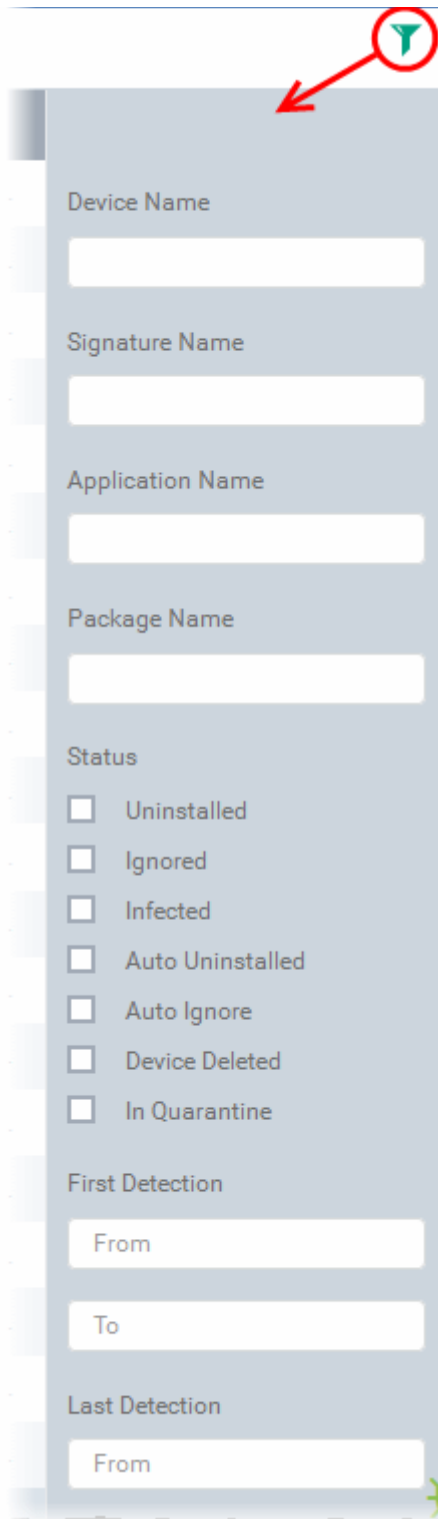
- Choose Antivirus from the left and the select 'Threats History'.



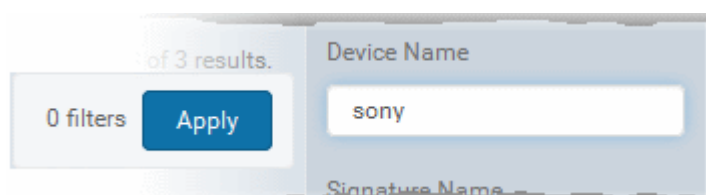
Antivirus Threats History - Column Descriptions	
Column Heading	Description
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the section Managing an Individual Device for more details.
Signature Name	The name of the virus signature identified from the infected application.
Application Name	The name of the infected application.
Package Name	The Android package name or identifier of the package from which the app was installed.
Status	Indicates whether the malware was uninstalled or yet to be uninstalled
First Detection	Indicates the precise date and time of the scan at which the malware was first identified from the device.
Last Detection	Indicates the precise date and time of the scan at which the malware was last identified from the device.

Sorting, Search and Filter Options

- Clicking 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 malware based on device name, signature name, infected application name, and/or package name/file path, enter the search criteria in part or full in the respective text boxes and click 'Apply'.



- To filter the items based on their infection status(es), select the status(es)

- To filter the threats based on time at which they were first identified or last identified within a specific time period, enter the start and end dates of the period in the 'From' and 'To' fields under respective categories, using the calendars that appear on clicking inside the respective field and click 'Apply'.

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

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

9.4. Viewing and Managing Quarantined Items

The Comodo Endpoint Security (CES) installations at the managed endpoints automatically move programs, executables and files identified as potential threats from real-time, scheduled and on-demand scans to quarantine within the respective endpoint. If:

- 'Show antivirus alerts' is disabled and 'Quarantine Threats' is chosen as default action in the 'Realtime Scan Settings' of the Antivirus component in the configuration profile active on the device
- 'Show antivirus alerts' is enabled in the Realtime Scan Settings in the Antivirus component of the configuration profile active on the device and if the end user chooses to quarantine the threat from the displayed alert
- The administrator moves an identified threat from the Current Malware List interface to quarantine

Items moved to quarantine are saved in an encrypted format and not allowed to run at the endpoint.

Refer to the explanation of **Realtime Scan settings** in the section **Antivirus Settings** under **Creating Windows Profile** and the section **Viewing and Managing Identified Malware** for more details.

The 'Antivirus Quarantine' interface displays a consolidated list of all the items quarantined by all the CES installations at the enrolled endpoints. The administrator can analyze the trustworthiness of the items and delete them permanently or restore them to their original location from this interface.

To view and manage quarantined items

- Choose 'Antivirus' from the left and choose Quarantine.

Antivirus Quarantine - Column Descriptions

Column Heading	Description
Device Name	The name assigned to the device by the user. Clicking the name of the device will open the 'View Device' interface that displays the complete details of the device and enables the administrator to

	locate the device and to apply configuration profiles. Refer to the section Managing an Individual Device for more details.
File Name	The name of the malware identified from the infected application.
Path	The installation path of the infected application.
Virus ID	The identification number of the virus signature used to identify the malware.
Date	Indicates the precise date and time at which the malware was first identified from the device.

- Clicking on 'File Name', 'Path', 'Virus ID' and/or 'Date' column headers sorts the items based on alphabetical order of entries in that column.
- By default CDM returns 20 results per page. To increase the number of results displayed per page up to 200, click the drop-down arrow next to 'Results per page' drop-down and choose the number.

If the item identified as malware is found to be a genuine virus, malicious app or a threat, the administrator can delete it from the endpoints at which it was found. If an item is found to be a false positive, the administrator can choose to restore the item to its original location at the endpoint.

- If the identified item is a false positive, select the item from the list and click 'Restore On Device' from the options at the top.
- To remove malware from the Quarantine at the device(s), select the item from the list and click 'Delete From Device' from the options at the top.



10. Configuring Comodo Device Manager

The 'Settings' tab allows administrators to create admin and user roles with different privilege levels, assign appropriate roles to enrolled users, configure AD integration, download CES and Agent installation packages for bulk installation through AD rules, and configure the behavior of various CDM components. Administrators can also manage subscriptions, renew/upgrade licenses and configure Google Cloud Messaging (GCM) and Apple Push Notification (APN) certificates.

The screenshot shows the Comodo Device Manager interface. The top navigation bar includes the Comodo logo, a hamburger menu, the current page 'Subscriptions / Summary', a notification bell with a '2' badge, and a 'Logout (John Smith)' button. The left sidebar lists various management options: DASHBOARD, DEVICES, USERS, PROFILES, APPLICATIONS, APP STORE, ANTIVIRUS, and SETTINGS. Under 'SETTINGS', 'Subscriptions' is selected. The main content area displays 'Summary License Details' for an active license. The license ID is 2a8491b5-5226-43a4-8fdd-6ac0a20c59f3. The maximum licenses available is infinity (∞), and the number of used licenses is 31. The license expires on 2016/05/12 06:37:32 AM, and the time check was performed on 2016/01/12 01:19:21 AM.

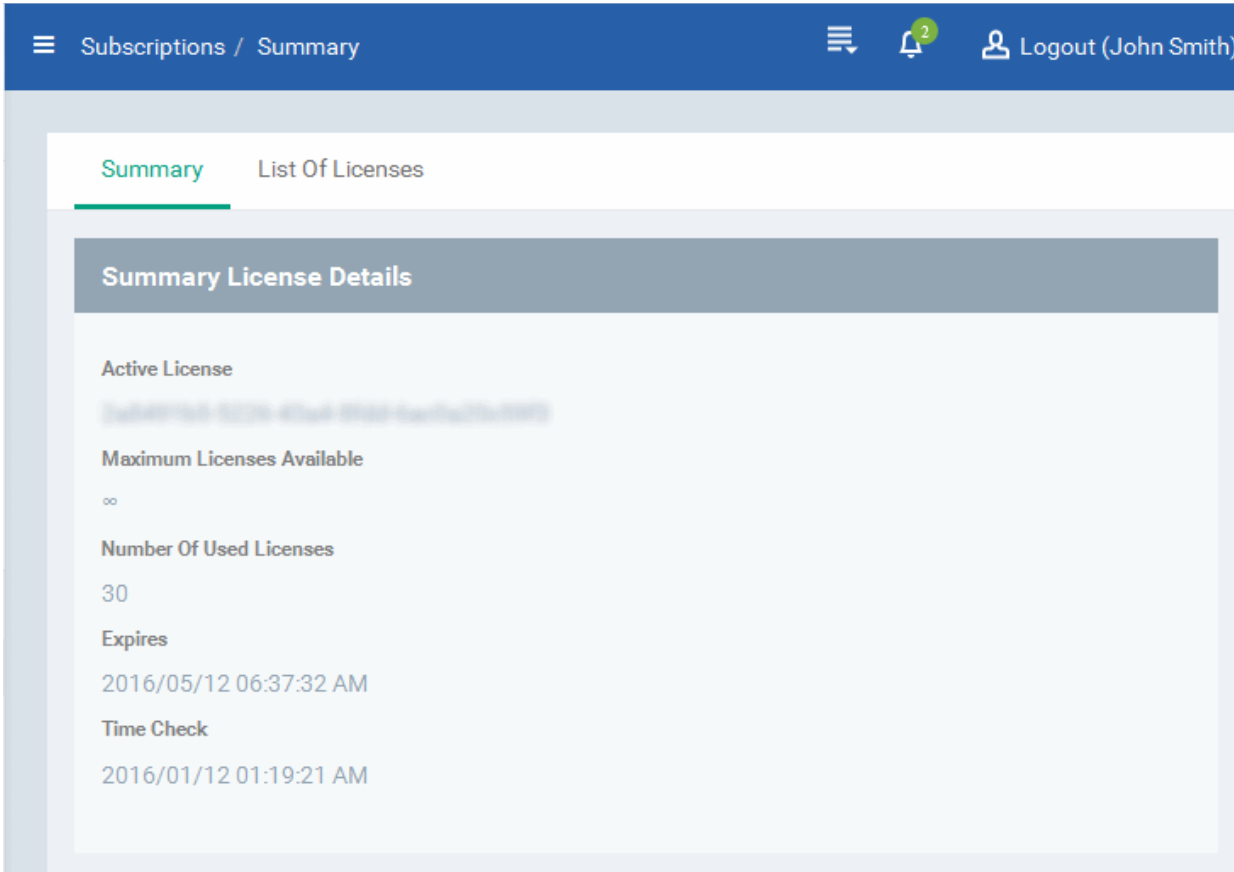
The following sections provide more details on each area:

- [Viewing and Managing Licenses](#)
- [Configuring Variables and Groups](#)
 - [Configuring Custom Variables](#)
 - [Configuring Registry Groups](#)
 - [Configuring COM Groups](#)
 - [Configuring File Groups](#)
- [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](#)
- [Downloading AD Installation Packages](#)
- [Adding Apple Push Notification Certificate](#)
- [Configuring CDM Android Agent](#)
 - [Configuring General Settings](#)
 - [Configuring Antivirus Settings](#)
 - [Adding Google Cloud Messaging \(GCM\) Token](#)
- [Configuring CDM Windows Client](#)
- [Managing CDM Extensions](#)
- [Configuring Email Templates](#)
- [Configuring Email Notifications](#)
- [Configuring Exception Reports](#)
- [Importing User Groups from LDAP](#)
- [Viewing Version and Support Information](#)

10.1. Viewing and Managing Licenses

The 'Subscriptions' interface displays details about licenses purchased, their type and validity status and the number of users and devices allowed on each. The 'Subscriptions' screen also allows the administrator to add new licenses.

- To open the 'Subscription' interface, choose 'Settings' from the left and select 'Subscriptions'.



The screenshot shows the 'Subscriptions / Summary' page. The page has a blue header with a hamburger menu, the text 'Subscriptions / Summary', a notification bell with a '2' badge, and a 'Logout (John Smith)' button. Below the header, there are two tabs: 'Summary' (active) and 'List Of Licenses'. The 'Summary License Details' section displays the following information:

- Active License**: [Redacted]
- Maximum Licenses Available**: ∞
- Number Of Used Licenses**: 30
- Expires**: 2016/05/12 06:37:32 AM
- Time Check**: 2016/01/12 01:19:21 AM

It contains two tabs:

- **Summary** - Displays a summary of details of your currently active license(s). An example is shown above.
- **List of Licenses** - Displays a list of licenses purchased so far with their details.

Subscriptions / List Of Licenses Logout (John Smith)

Summary List Of Licenses

[Add New License](#) [Remove License](#)

LICENSE KEY	LICENSE TYPE	ACTIVE	PREMIUM	LICENSED TO	EXPIRES
XXXXXXXXXX	COMODO Device Ma...	No	No	Test Testing	2015/05/06 09:2...
XXXXXXXXXX	Support	No	Yes	Madan Prasad	2014/06/21 01:4...
XXXXXXXXXX	Support	No	Yes	Madan Prasad	2014/05/19 09:5...
XXXXXXXXXX	COMODO Device Ma...	Yes	No	girdharana	2016/07/30 01:5...
XXXXXXXXXX	COMODO Device Ma...	Yes	Yes	Madan Prasad	2018/12/10 09:3...
XXXXXXXXXX	COMODO Device Ma...	Yes	Yes	Madan Prasad	2018/01/30 09:2...
XXXXXXXXXX	Valkyrie Free	Yes	No	XXXXXXXXXX	2016/12/25 03:0...
XXXXXXXXXX	COMODO Device Ma...	Yes	No	girdharana	2016/05/12 06:3...
XXXXXXXXXX	COMODO Device Ma...	No	Yes	Madan Prasad	2015/01/30 09:2...
XXXXXXXXXX	COMODO Device Ma...	Yes	No	XXXXXXXXXX	2016/08/04 11:2...

Results per page: 20 Displaying 1-10 of 10 results.

- Clicking on the license key will display the details of the license.

License details

Main License Details	Advanced
<p>License Key</p> <p>XXXXXXXXXX</p> <p>License type</p> <p>COMODO Device Management</p> <p>Maximum Licenses Available</p> <p>∞</p> <p>Organization</p> <p>Dithers</p> <p>Licensed To</p> <p>girdharana@comodo.com</p> <p>Free</p> <p>Yes</p> <p>Active</p> <p>Yes</p>	<p>Valid From</p> <p>2015/06/10 10:05:38 AM</p> <p>Expires</p> <p>2016/05/12 06:37:32 AM</p> <p>Time Check</p> <p>2016/01/12 07:19:21 AM</p> <p>License Registered At</p> <p>2015/05/13 06:37:32 AM</p>

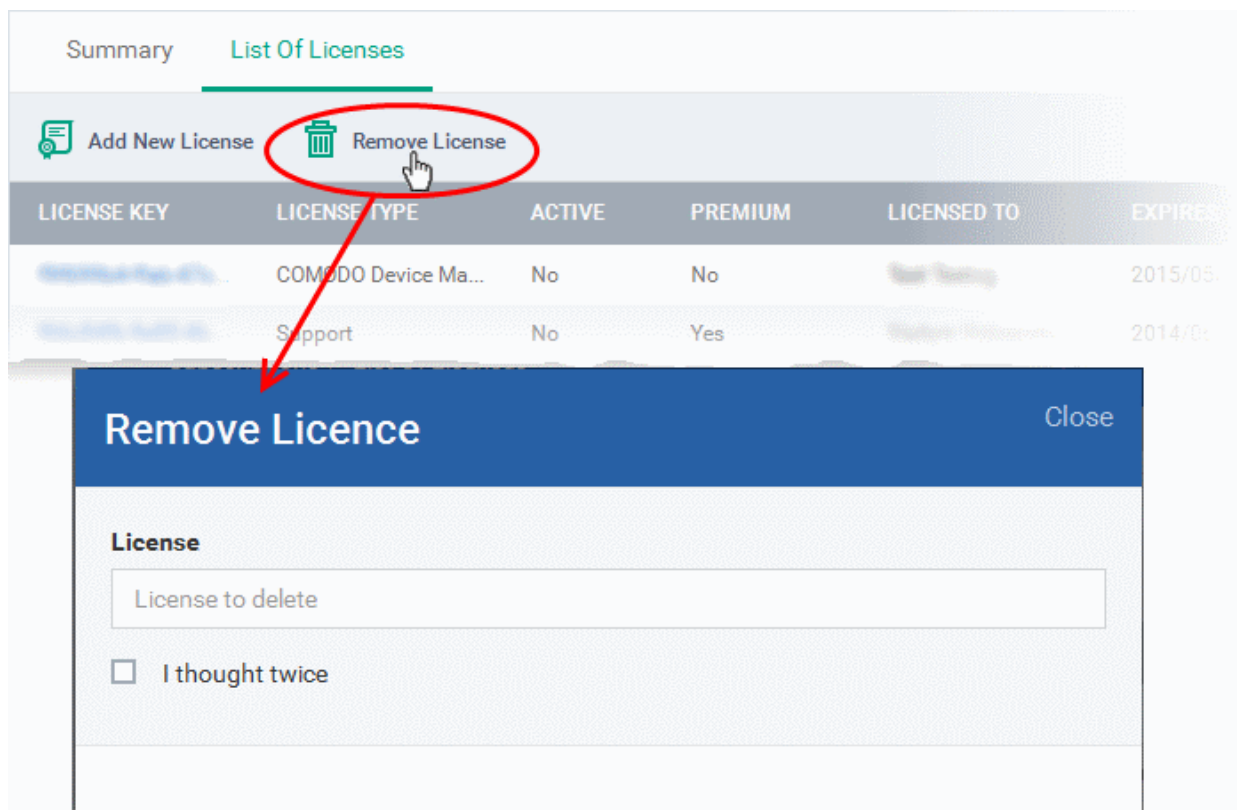
The next section **Upgrading or Adding the License** provides more details on upgrading your license for adding more number of users and renewing your license.

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'
- Copy the license key to be removed to your clip board
- Click 'Remove License' from the top of the 'List of Licenses' interface



- Paste the license key in the 'License' field
- Confirm your choice of removal by selecting 'I thought twice'
- Click OK that appears in the Remove License dialog after confirming your choice

The license will be removed from the list.

10.1.1. Upgrading or Adding the License

Administrators can add more users to their account by upgrading their license in the Comodo account management portal.

To upgrade a license

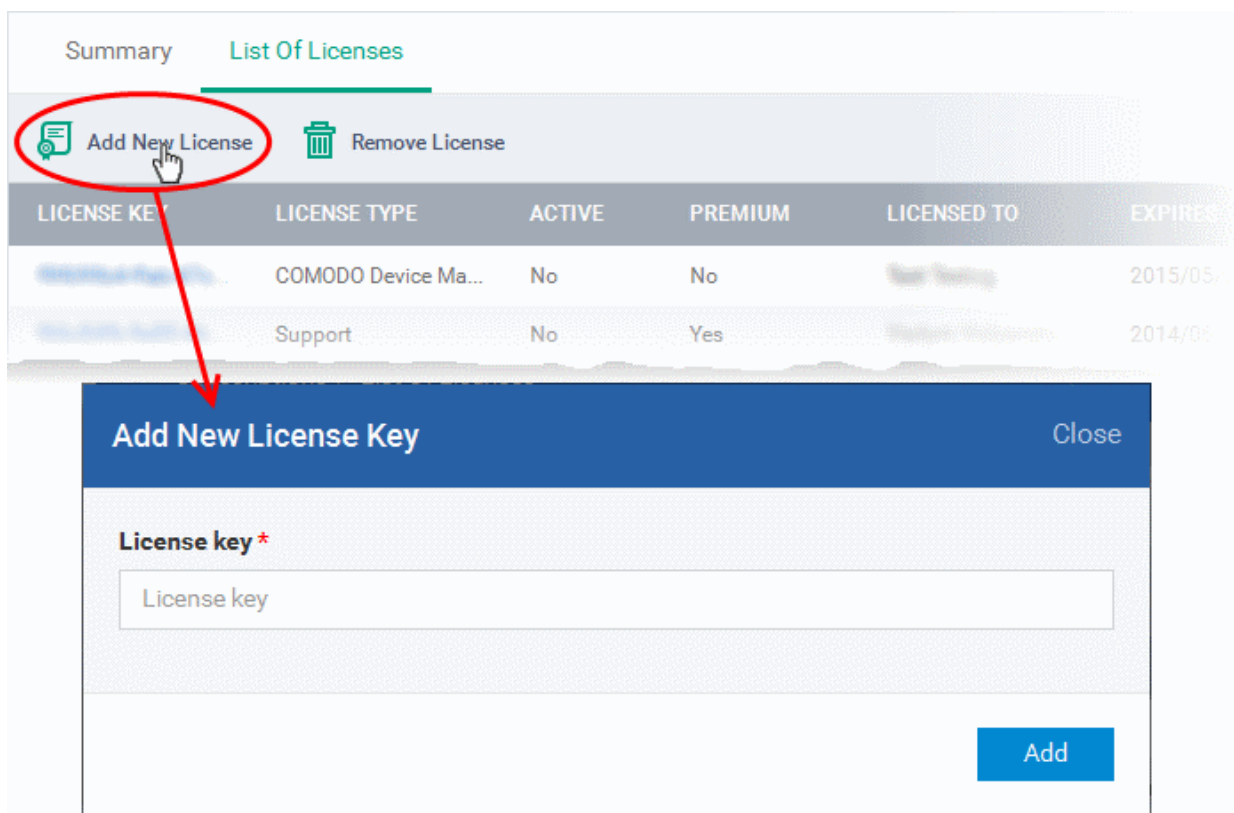
- Log in at <https://accounts.comodo.com> with your Comodo username and password
- Select 'Comodo Device Management' and complete the purchase process.

Your license key will be sent via email to your registered email address.

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 on 'List Of Licenses' tab to open the 'Subscriptions/List of Licenses interface
- Click 'Add new license' at the top left.



- Enter the license keys from your license confirmation email.
- Click 'Add'.

Your new license will be activated. The license key will be displayed in the 'Subscription and license' panel

- To view the license details and activation status, click on the license key.

New License

Please ensure to validate your license within 10 days after registration and starting using CDM, else access to CDM will 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 MDM portal for 30 days only after the expiry of the license. After this grace period, access to the CDM will be blocked.

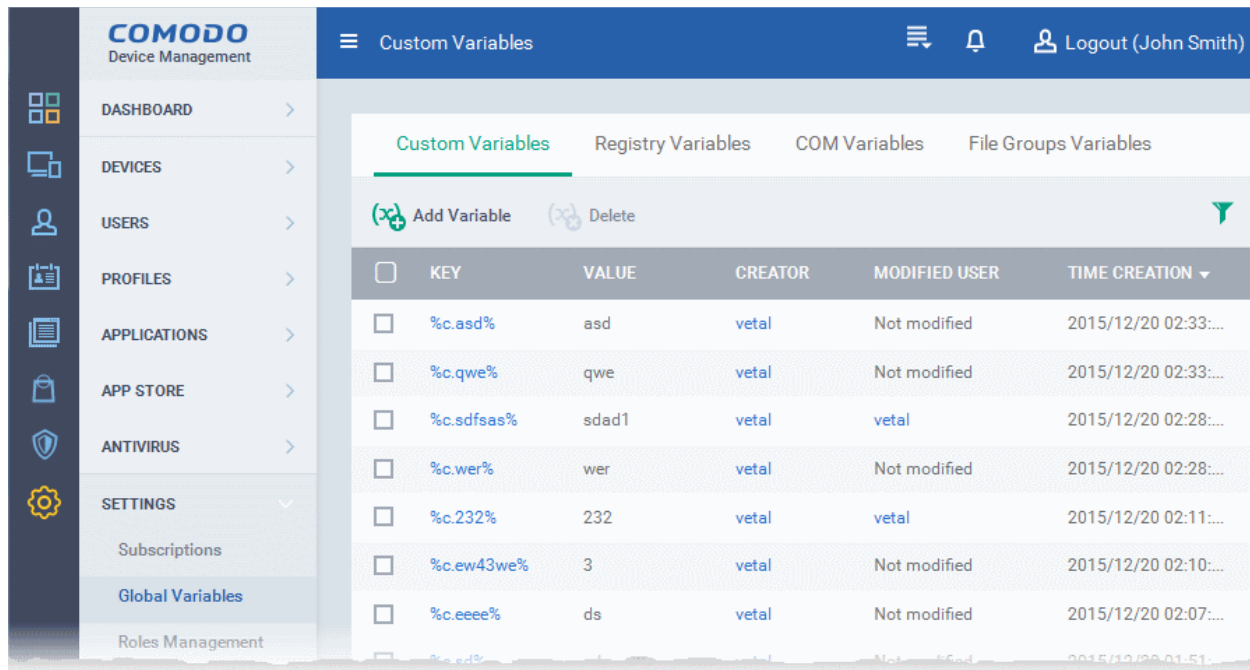
10.2. Configuring Variables and Groups

The 'Global Variables' interface under 'Settings' allows you to create and manage:

- Custom variables that can be used in creating configuration profiles for the managed Android, iOS and Windows devices for defining various parameters.
- Collections of registry keys and values of different categories as 'Registry Groups'. The Registry Groups can be used to include the respective keys and values while configuring Sandbox rules, HIPS rules and more for Windows configuration Profiles.
- Collections of COM interfaces as 'COM' groups. The COM groups can be used to include respective COM interfaces in HIPS rules for Windows Configuration Profiles
- Collections of files as a 'File Group'. The File Groups can be used to include respective files as exclusions from AV scans, Firewall rules, Sandbox rules and HIPS rules for Windows Configuration Profiles

These variables and groups can be created in common for CDM and can be used while creating different configuration profiles for the managed devices.

- To open the Global Variables interface, select Settings from the left and choose 'Global Variables'.

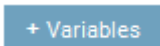


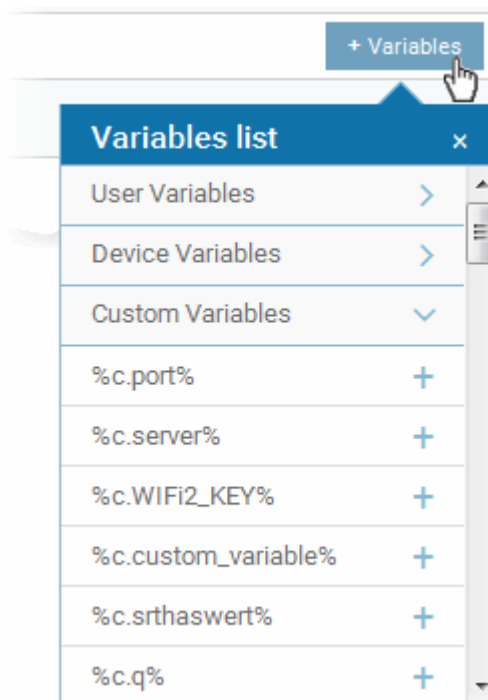
Following sections explain more about:

- [Creating and Managing Custom Variables](#)
- [Creating and Managing Registry Groups](#)
- [Creating and Managing COM Groups](#)
- [Creating and Managing File Groups](#)

10.2.1. Creating and Managing Custom Variables

CDM is capable of fetching values for variables defined for various settings and configuration profiles. There are three types of variables available in CDM namely 'User Variables', 'Device Variables' and 'Custom Variables', that can be used by the administrator for configuring various settings.

The 'Variables' button  will appear in the fields that can be entered with variables, while configuring various settings for a profile. The 'Variables List' will appear with the list of variables added to CDM on clicking this button, enabling you to choose the variable to be entered to the field.

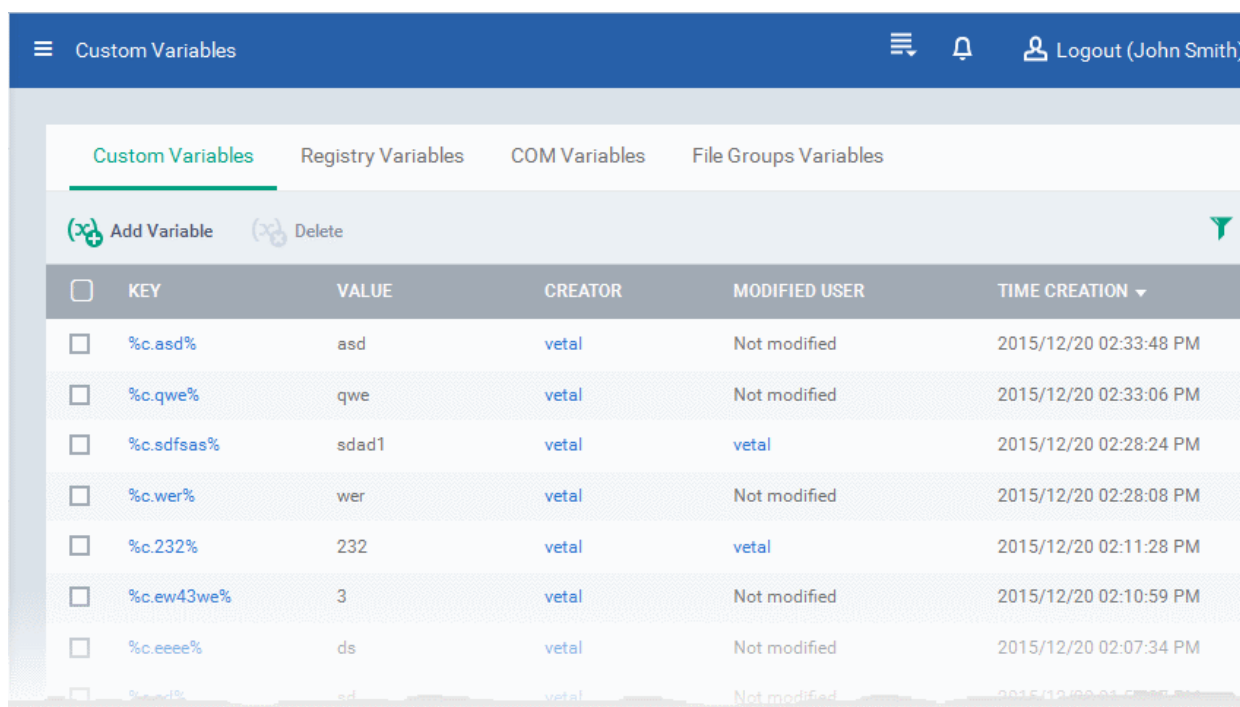


The first two, 'User Variables' and 'Device Variables', are hard coded and cannot be altered. These are useful for fetching the values of user and devices, for example user login details, email details from 'Users' > 'Users'. The last one, 'Custom Variables', can be created by the administrators and the variables created for use in configuration of various settings.

The custom variables can be added to CDM 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

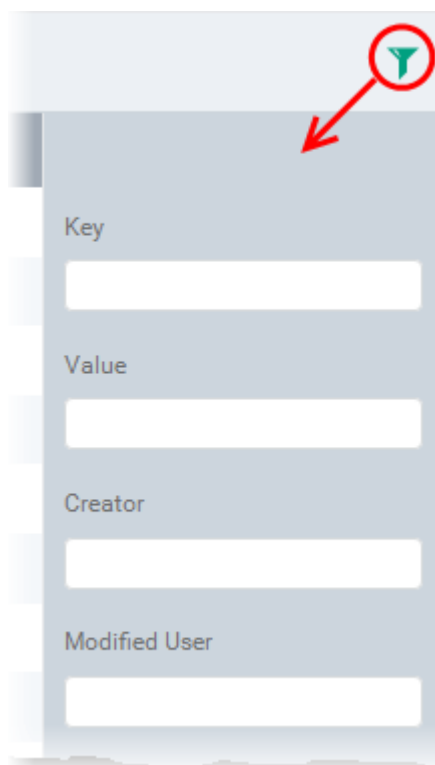
- Choose 'Settings' from the left and select Global Variables
- Click the 'Custom Variables' tab from the top of the interface



Custom Variables - Column Descriptions	
Column Heading	Description
Key	Displays the name of key for the value in the next column. Clicking the key will open the 'Update Custom Variable' interface that allows to edit the value for the key.
Value	Displays the value for the key in the preceding column.
Creator	Displays the name of administrator that has created the custom variables. 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 the User for more details.
Modified User	Displays the name of the user that last modified the custom variable.
Time Creation	Displays the custom variable created date and time.

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 the variable that are based on 'Key', 'Value', 'Creator' and 'Modified User', enter the text partially or fully in the respective fields and click the 'Apply' button.

The custom variables that matches the entered parameters will be displayed in the screen.

- To display all the variables again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the filter option

To create a new Custom Variable

- Click the 'Settings' from the left, choose 'Global Variables' and click on 'Custom Variables' tab
- Click 'Add Variable'

The screenshot shows the 'Custom Variables' tab in the Comodo Device Manager interface. At the top, there are tabs for 'Custom Variables', 'Registry Variables', 'COM Variables', and 'File Groups Variables'. Below the tabs, there are two buttons: 'Add Variable' (circled in red) and 'Delete'. Below these buttons is a table with columns: KEY, VALUE, CREATOR, MODIFIED USER, and TIME CREATION. The table contains three rows of variables. A red arrow points from the 'Add Variable' button to a 'Create New Variable' dialog box. The dialog box has a title bar with 'Create New Variable' and a 'Close' button. It contains two text input fields: 'Key *' and 'Value *'. The 'Key' field contains the text 'Key' and the 'Value' field contains the text 'Value'. At the bottom right of the dialog box is a blue 'Save' button.

KEY	VALUE	CREATOR	MODIFIED USER	TIME CREATION
%c.asd%	asd	vetal	Not modified	2015/12/20 02:33:...
%c.qwe%	qwe	vetal	Not modified	2015/12/20 02:33:...
%c.sdfsas%	sdad1	vetal	vetal	2015/12/20 02:28:...

- 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 CDM.

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.

The screenshot shows the 'Update Custom Variable' dialog box. It has a title bar with 'Update Custom Variable' and two buttons: 'Cancel' and 'Save'. Below the title bar are two text input fields: 'Key *' and 'Value *'. The 'Key' field contains the text 'Wi-Fi_office' and the 'Value' field contains the text '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

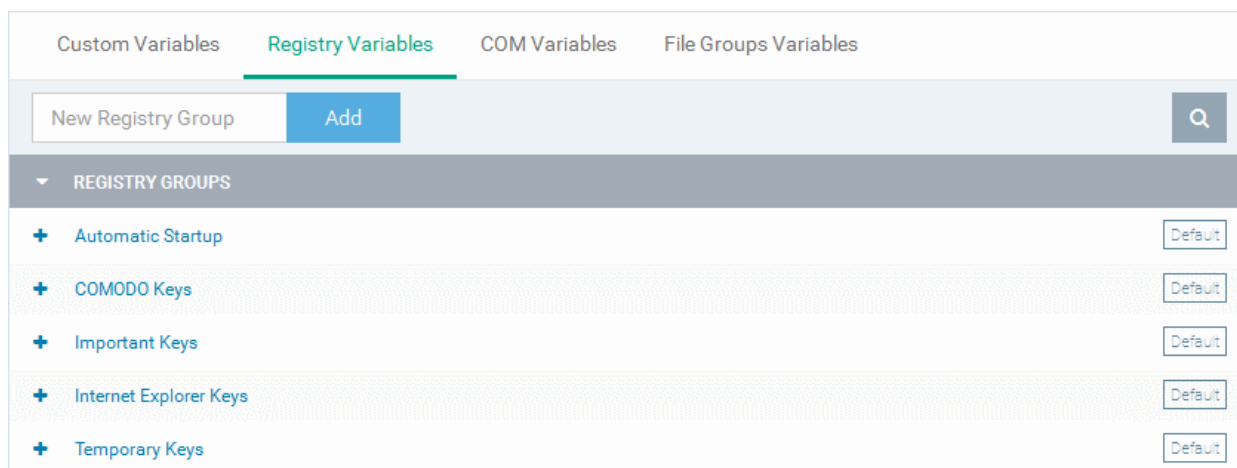
10.2.2. Creating and Managing Registry Groups

Each Registry group is a predefined batch of one or more registry keys and values that fall under a specific category. Creating a Registry Group allows the administrator to specify the group as an exclusion to sandbox rules when configuring 'Sandbox Settings' in a Windows profile. CDM ships with a set of predefined Registry Groups that are available for use in configuration profiles. If required, administrators can add new groups and edit existing groups.

The 'Registry Variables' tab in the 'Global Variables' interface allows the administrator to view, create and manage pre-defined and custom Registry groups. The groups added to this interface will be available for selecting while configuring Windows Profiles from the 'Profiles' interface.

To open the 'Registry Groups' interface

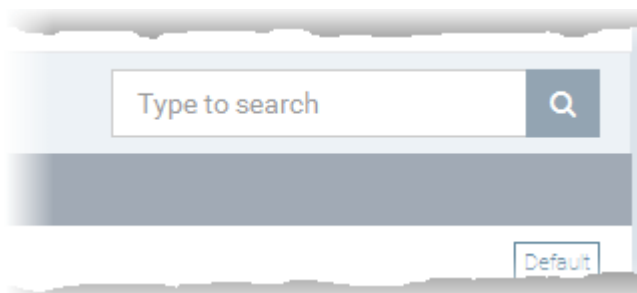
- Choose 'Settings' from the left and select 'Global Variables'
- Click 'Registry Variables' from the top



The list of default and user-defined Registry groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

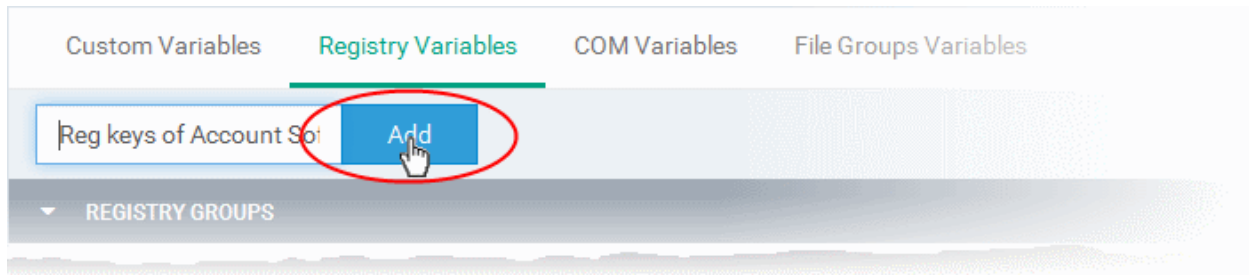
Sorting, Search and Filter Options

- Clicking on the 'Registry Groups' column header will sort the items in ascending/descending order of the names of the Registry groups.
- To filter or search for a specific Registry group, click the search icon at the top right and enter the name of the group on part or full



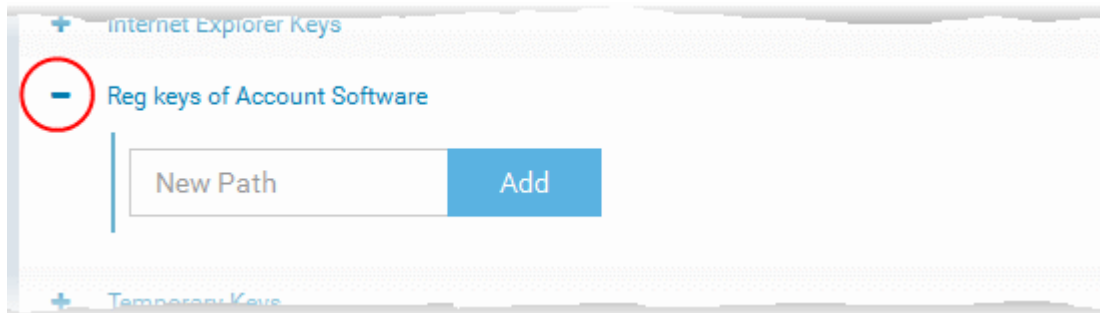
To add a new Registry group

- Enter the name of the new Registry Group in the New Registry Group field and click 'Add'.

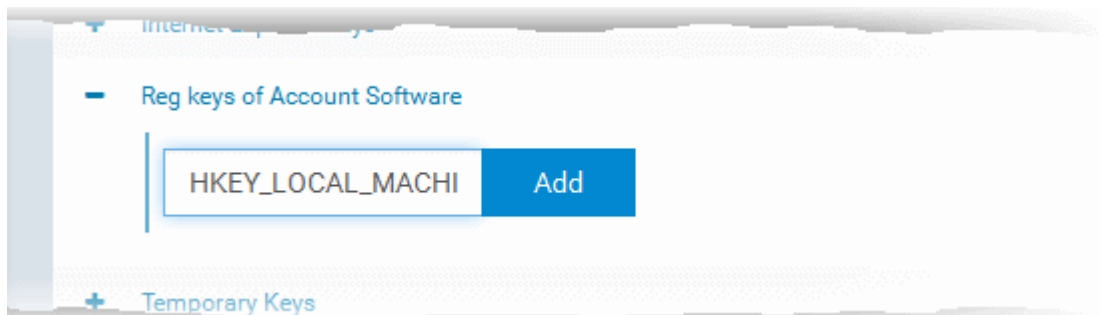


The new group will be added to the list. The next step is to add the Registry keys to the group.

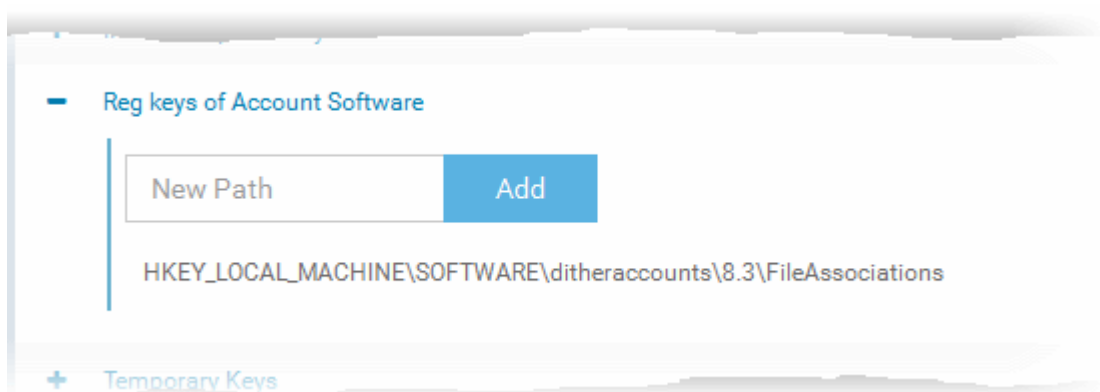
- Click the '+' at the left of the group name



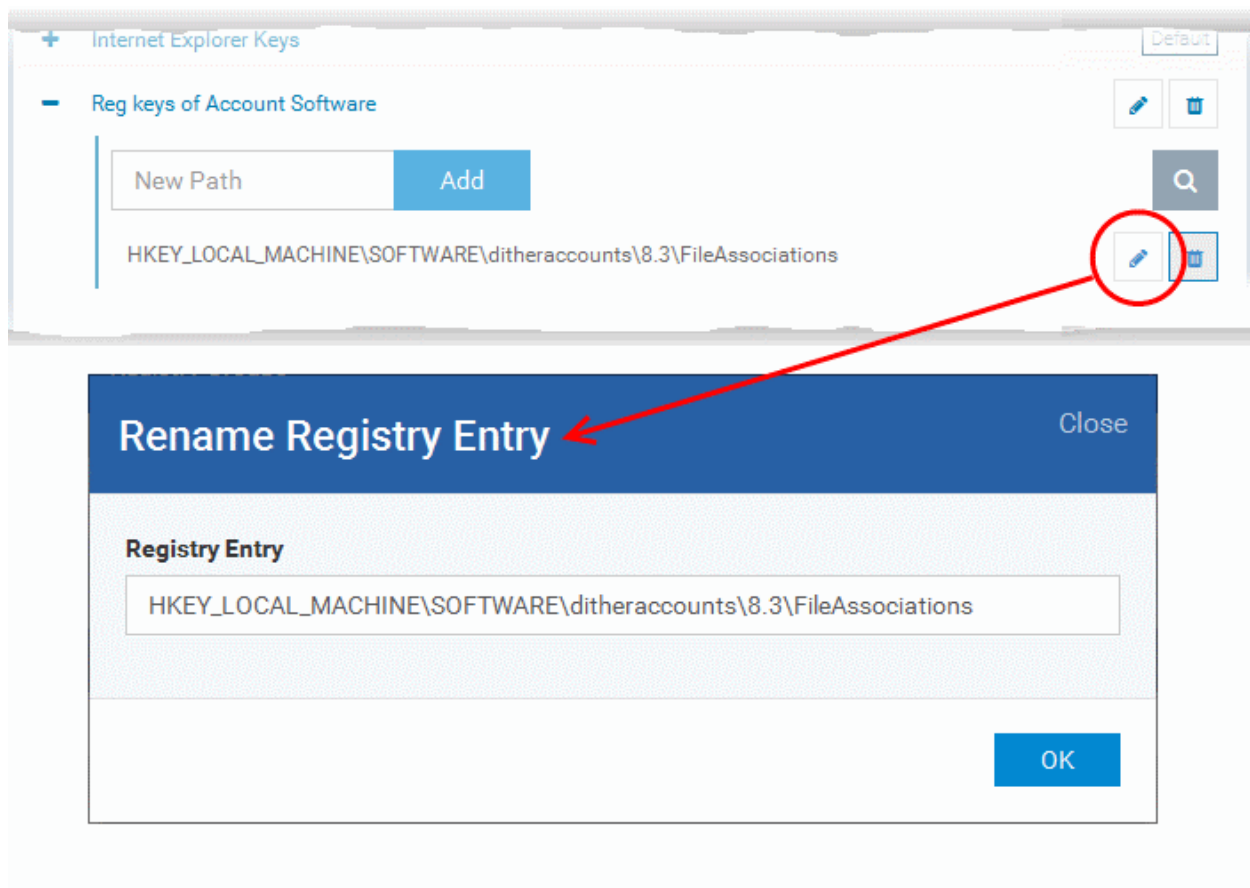
- Enter the path of the registry key/value in the New Path field and click 'Add'



The key will be added to the group.

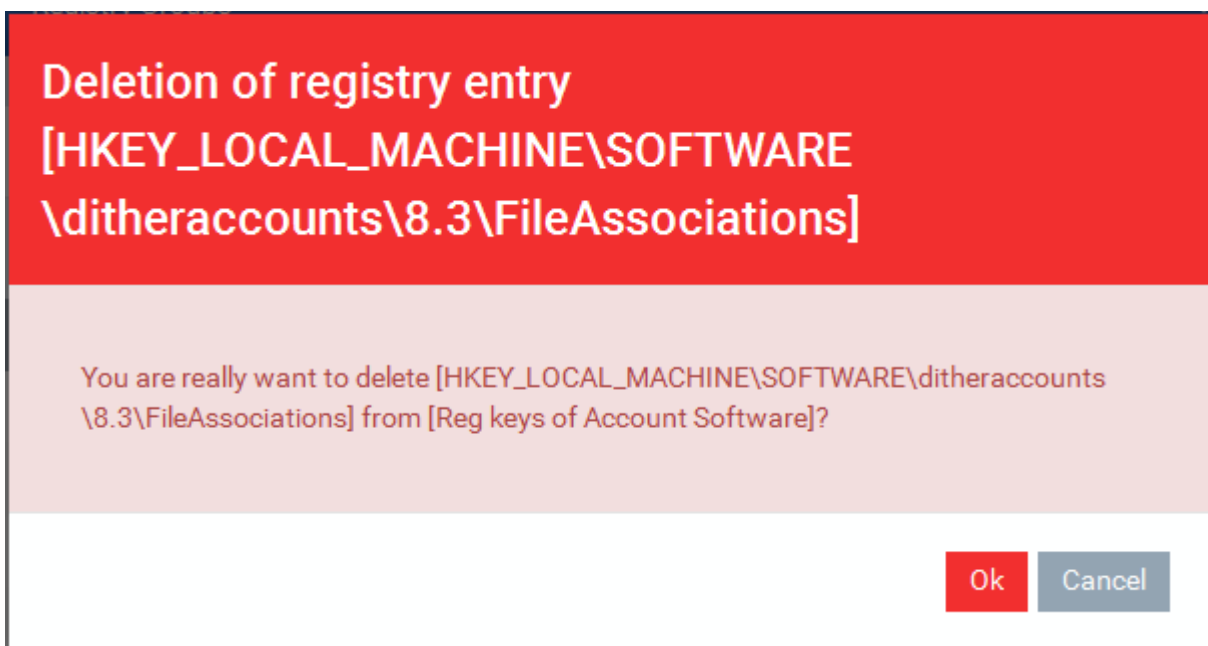


- Repeat the process to add more Registry keys and values to the group.
- To edit the key/value in the group, click the 'Edit' icon beside the key name.



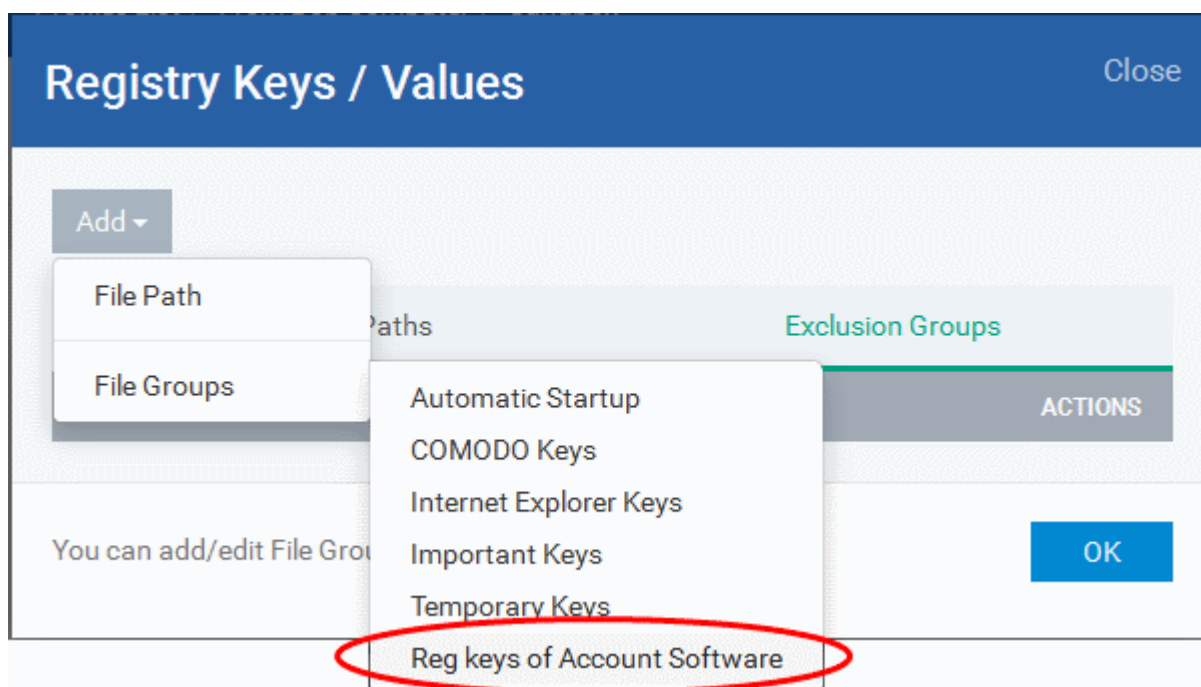
- Edit the entry and click 'OK' to save your changes
- To remove the key added by mistake or an unwanted key from the group, click the trash can icon beside the key name.

A confirmation dialog will appear.



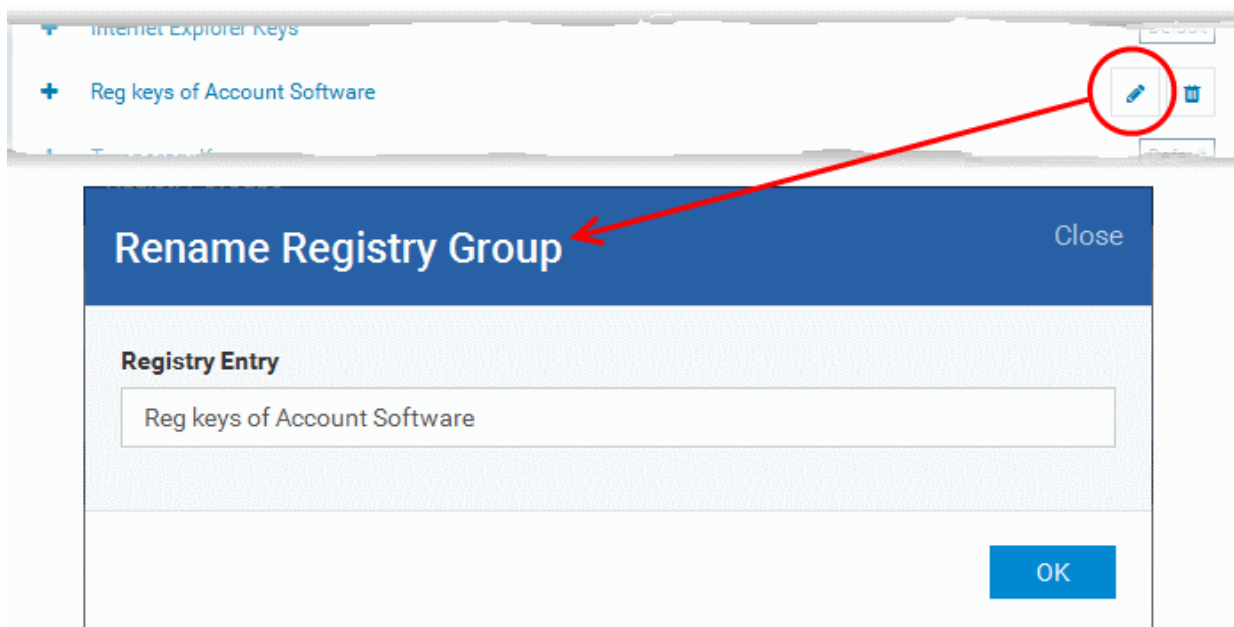
- Click 'OK' in the confirmation dialog.

Once a registry group is added, it will be available for selection in the 'Sandbox' > 'Registry Key Exclusions' dialog in the 'Windows Profile' interface.



To edit the name of a Registry Group

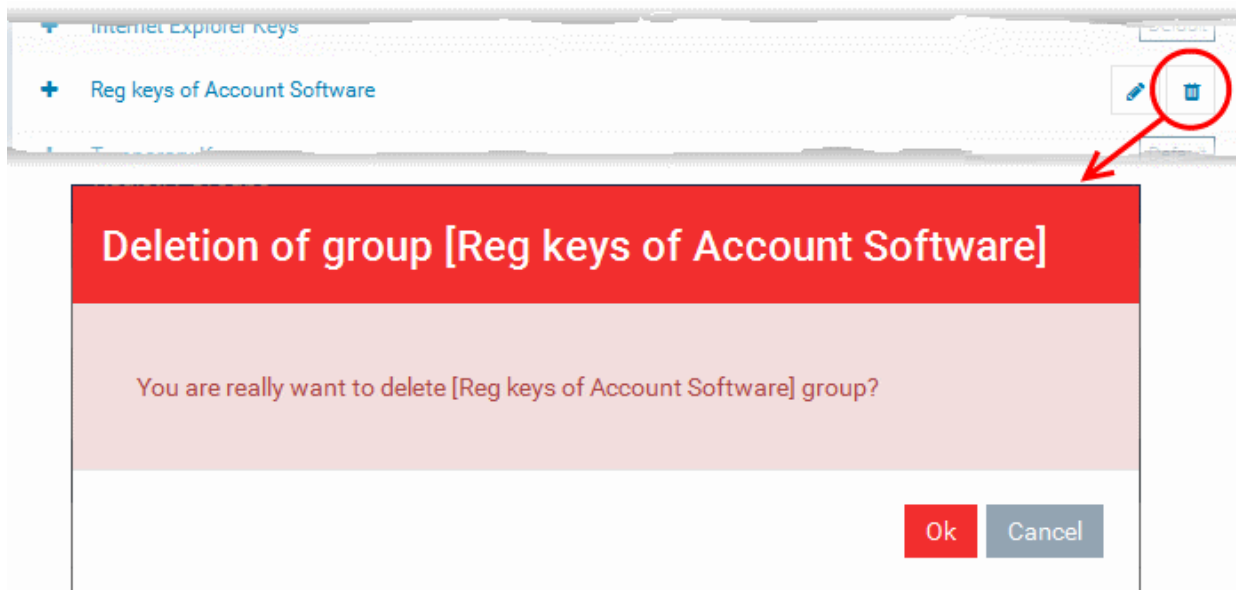
- Click the 'Edit' icon beside the Registry Group



- Enter the new name for the group in the Rename Registry Group dialog and click 'OK'

To remove a Registry Group

- Click the Thrash can icon beside the Registry Group



A confirmation dialog will appear.

- Click OK in the confirmation dialog.

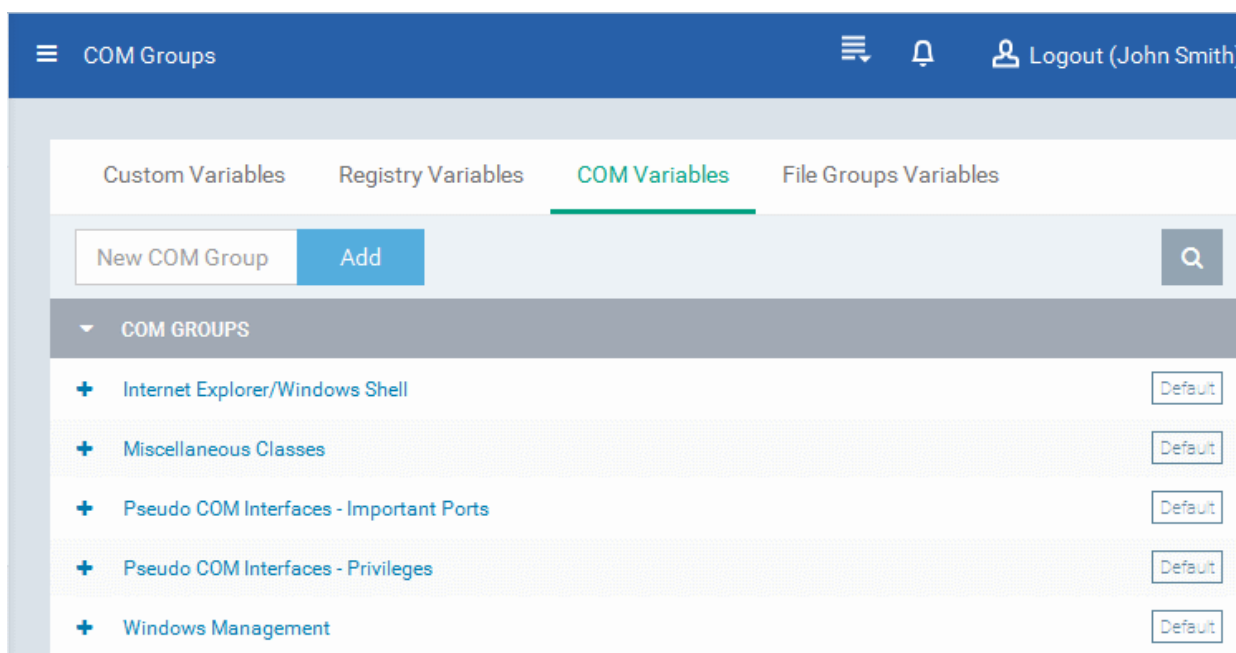
10.2.3. Creating and Managing COM Groups

Each COM group is a handy collection of COM interfaces falling under a certain category. Creating a COM group in CDM allows administrators to add the group to the 'Protected Objects' list in the HIPS settings of a Windows profile. CDM ships with a set of predefined COM Groups and if required, administrators can add new COM Groups, edit and manage them.

The COM Variables tab under the 'Global Variables' interface allows administrator 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

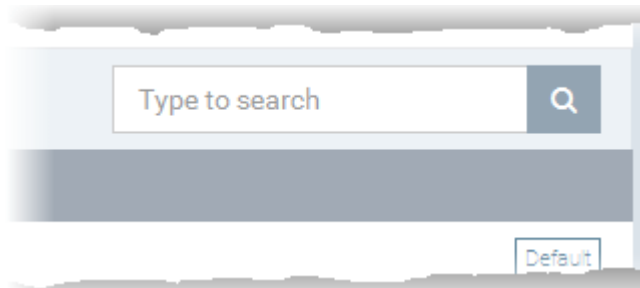
- Choose 'Settings' from the left and select 'Global Variables'
- Click 'COM Variables' from the top



The list of default 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 'New COM Group' field and click 'Add'.

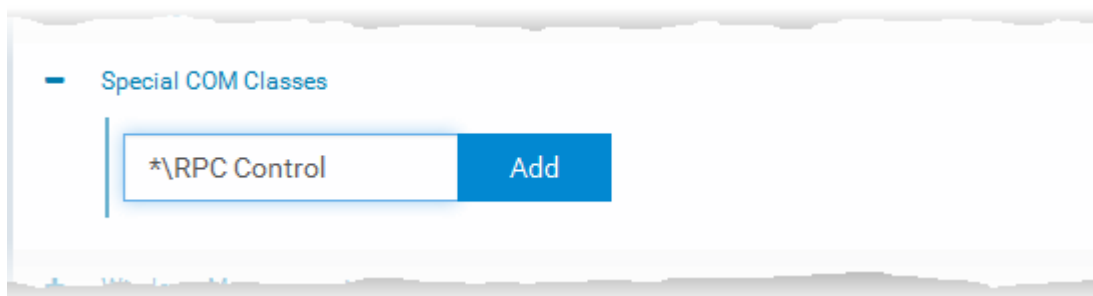


The new group will be added to the list. The next step is to add COM classes to the group.

- Click the '+' at the left of the group name



- Enter the COM classes to be added to the group, in the 'New Path' field and click 'Add'

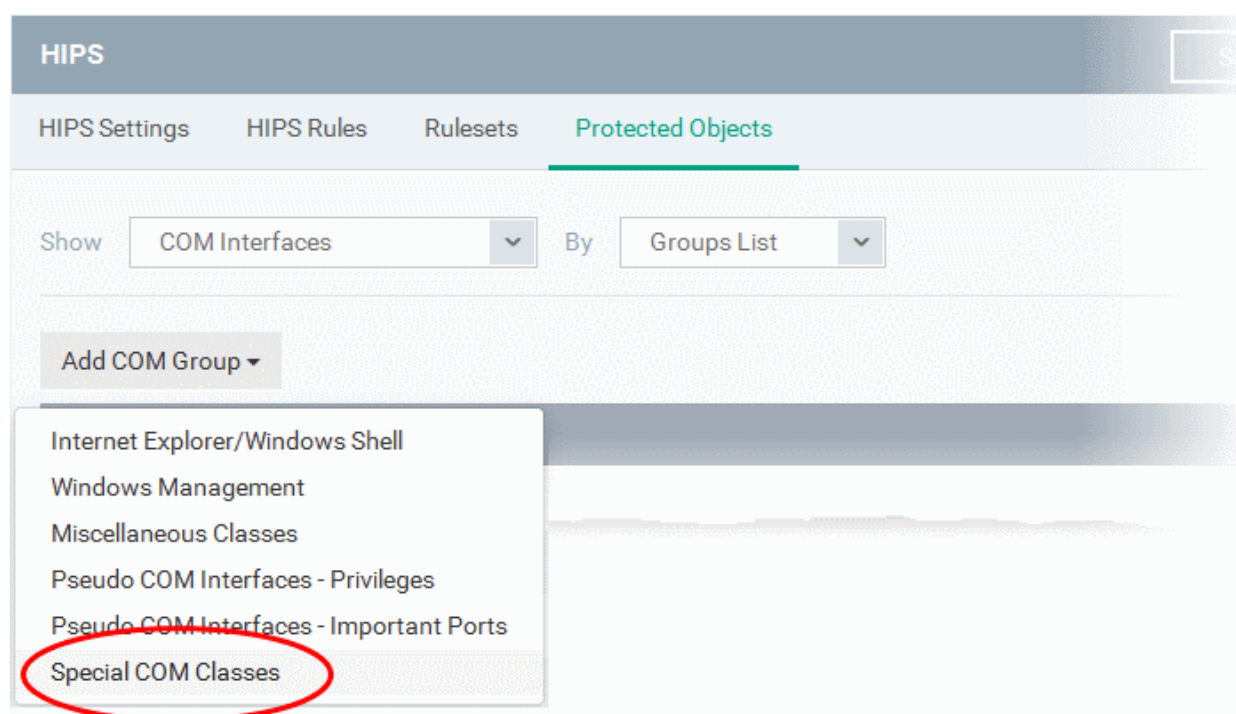


The COM class will be added to the group.

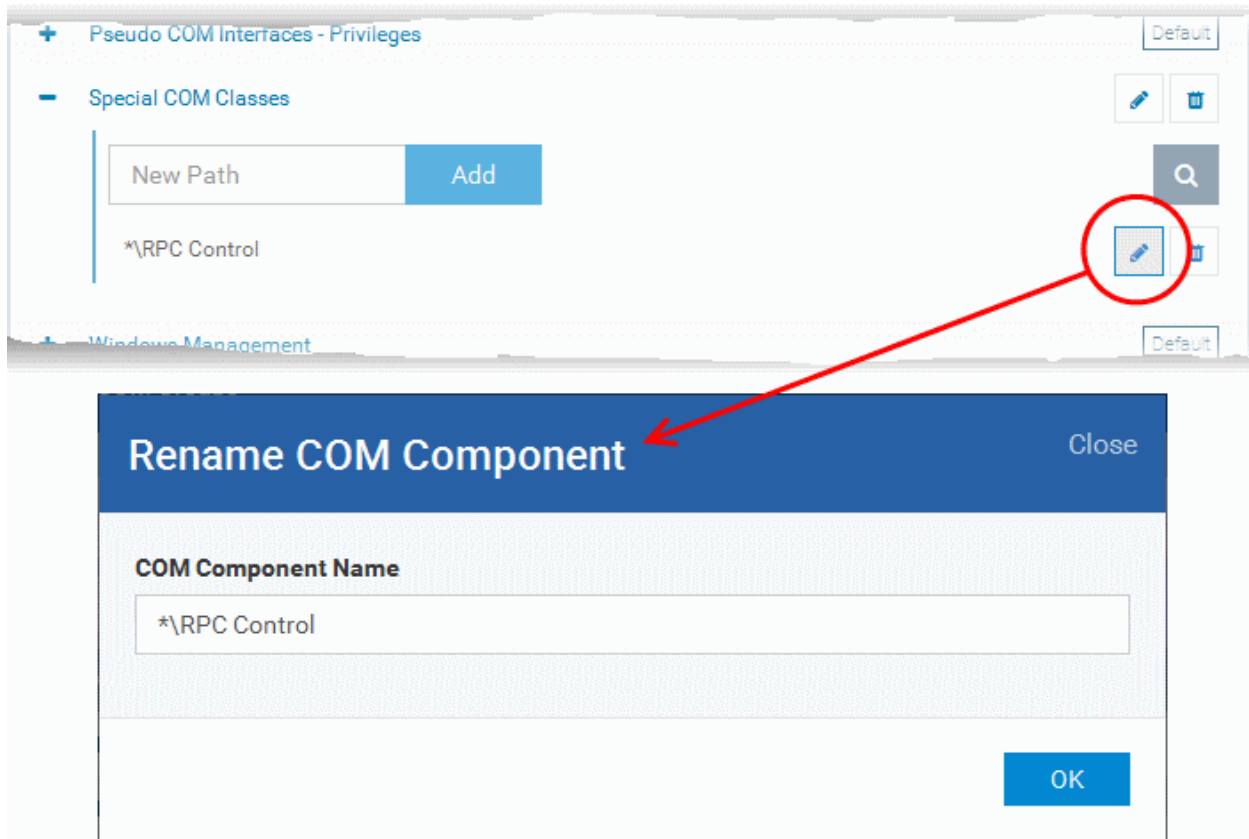


- Repeat the process to add more COM classes to the group.

Once a COM group is added, it will be available for selection in the 'HIPS' > 'Protected Objects' > 'Groups List' interface in the 'Windows Profile' interface.

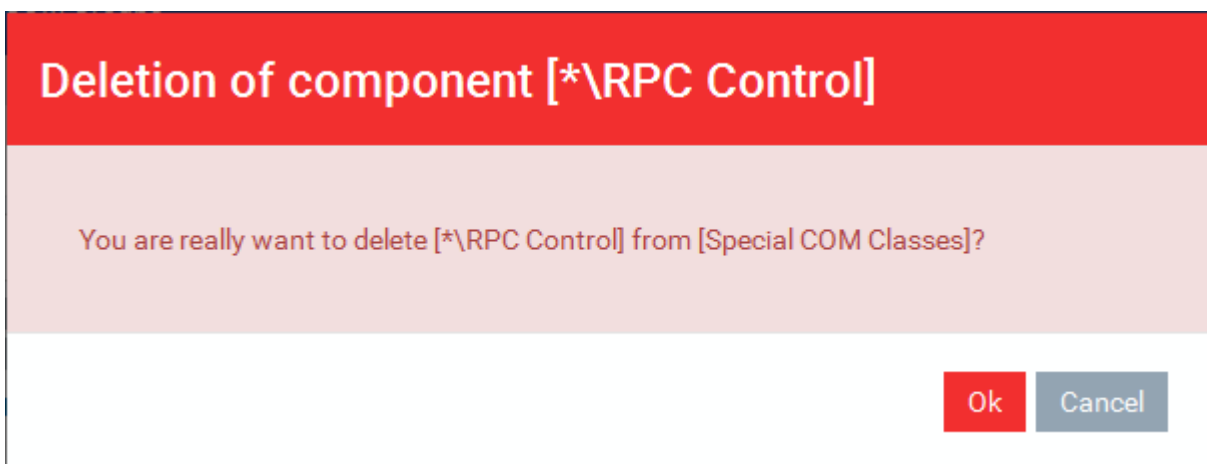


- To edit a class in the group, click the 'Edit' icon beside the class name.



- 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.

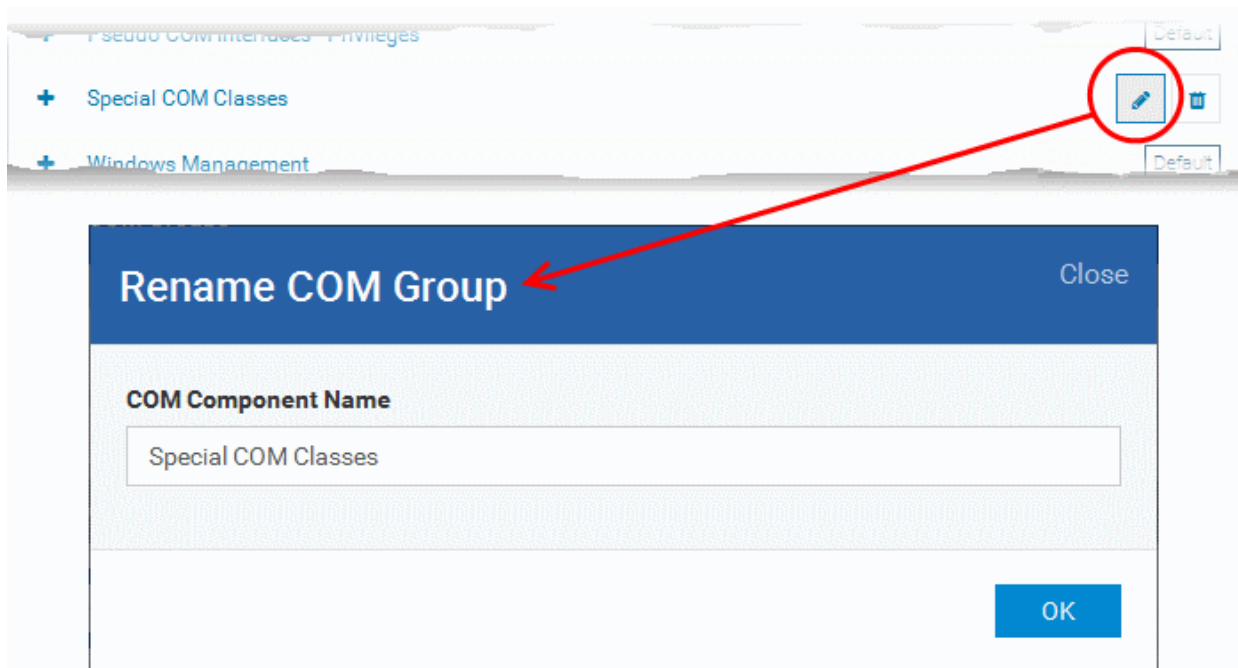
A confirmation dialog will appear.



- Click 'OK' in the confirmation dialog.

To edit the name of a Registry Group

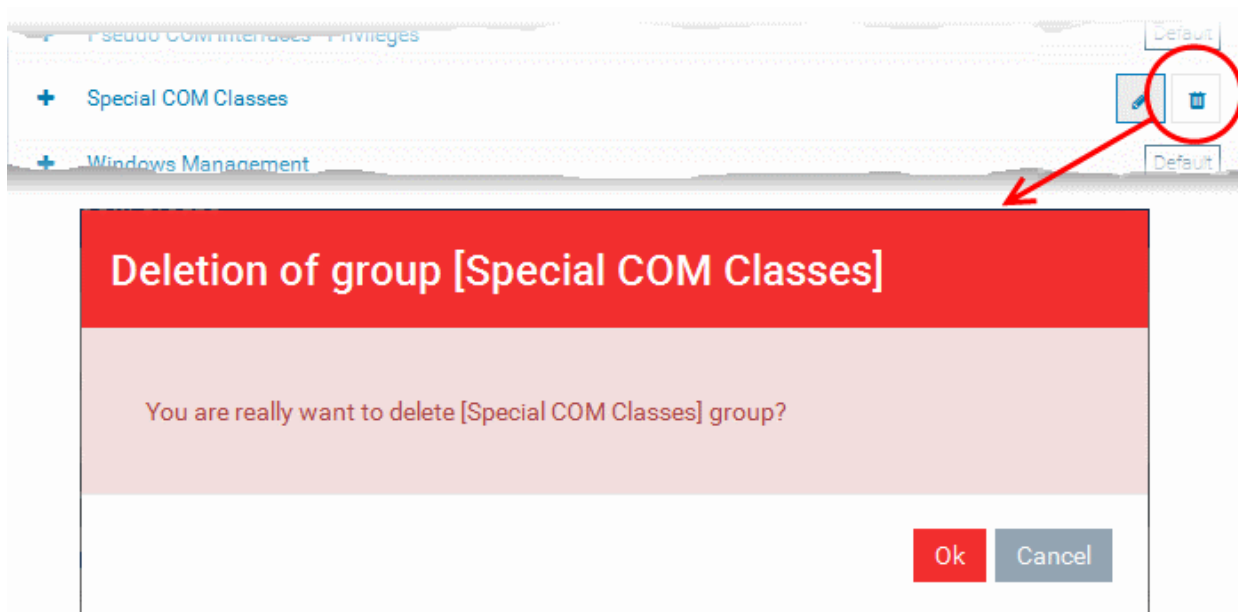
- Click the 'Edit' icon beside the COM Group



- Enter the new name for the group in the Rename COM Group dialog and click 'OK'

To remove a COM Group

- Click the Thrash can icon beside the COM Group



A confirmation dialog will appear.

- Click OK in the confirmation dialog.

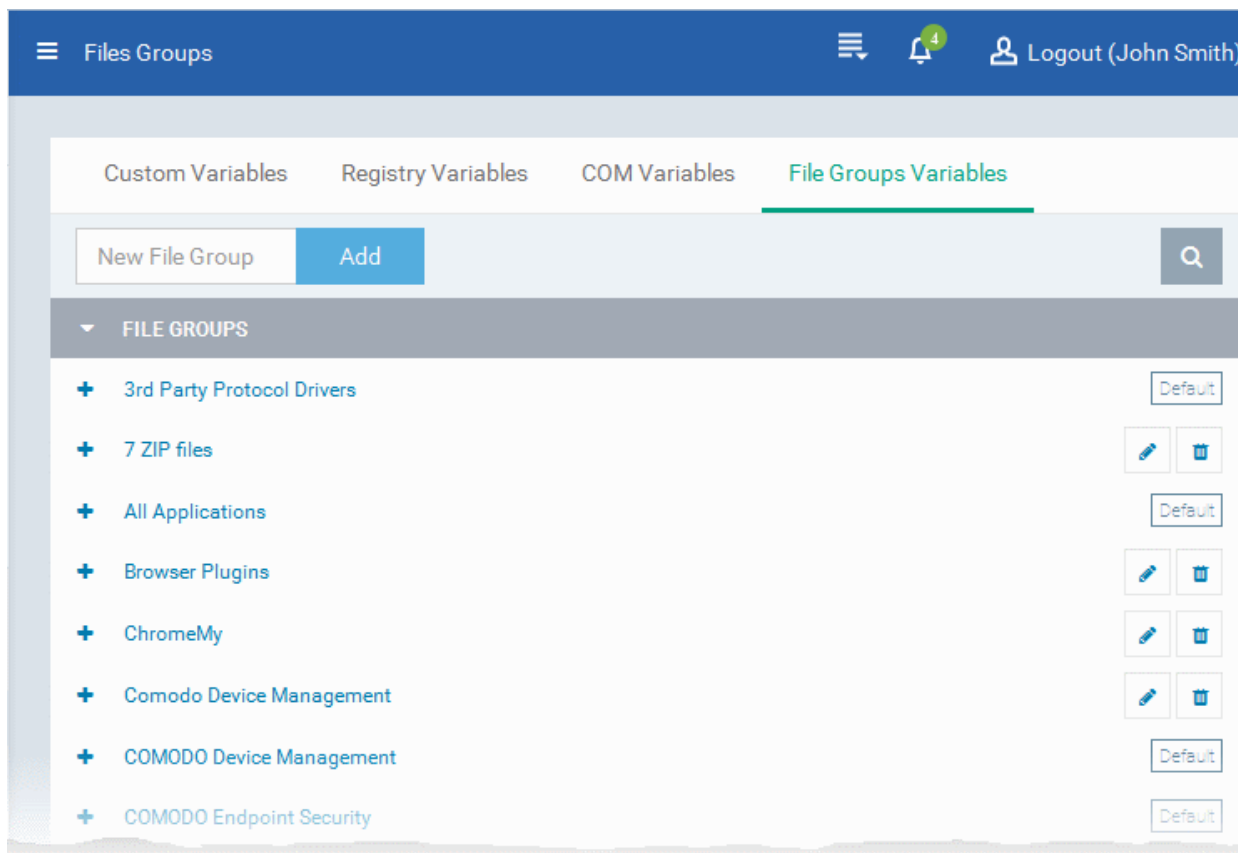
10.2.4. Creating and Managing File Groups

File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various functions such as adding them to Exclusions for AV scans, HIPS monitoring, auto-sandbox rules and so on in Windows Profiles. CDM 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 'Global Variables' interface allows the administrator 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

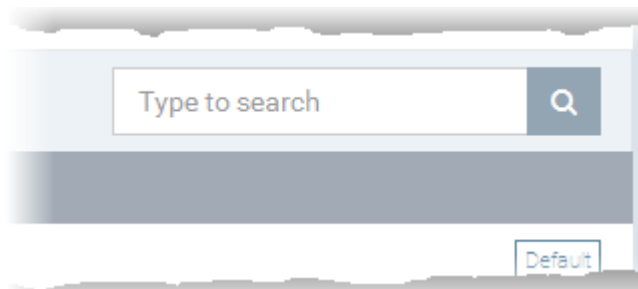
- Choose 'Settings' from the left and select 'Global Variables'
- Click 'File Groups Variables' from the top



The list of default and user-defined File groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

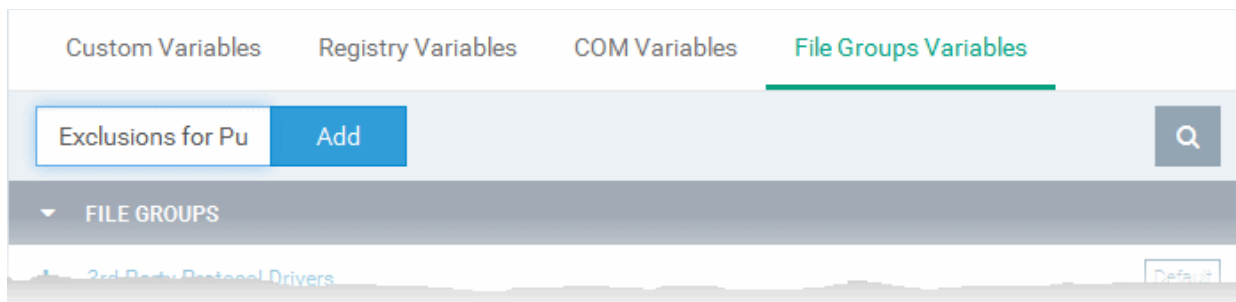
Sorting, Search and Filter Options

- Clicking on the 'File Groups' column header will sort the items in ascending/descending order of the names of the groups.
- To filter or search for a specific File group, click the search icon at the top right and enter the name of the group on part or full



To add a new File group

- Enter the name shortly describing the group in the 'New File Group' field and click 'Add'.



The new group will be added to the list. The next step is to add files to the group.

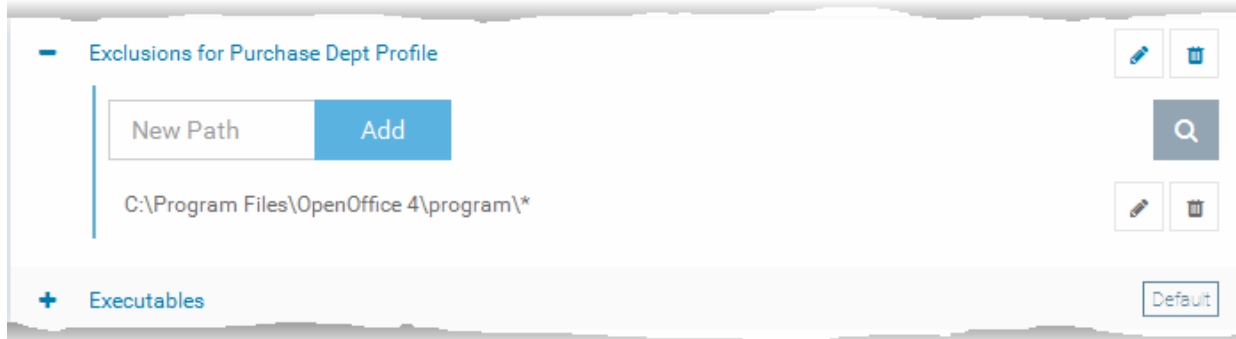
- Click the '+' at the left of the group name



- Enter the full standard folder/file path of the file to be added to the group in the 'New Path' field and click 'Add'

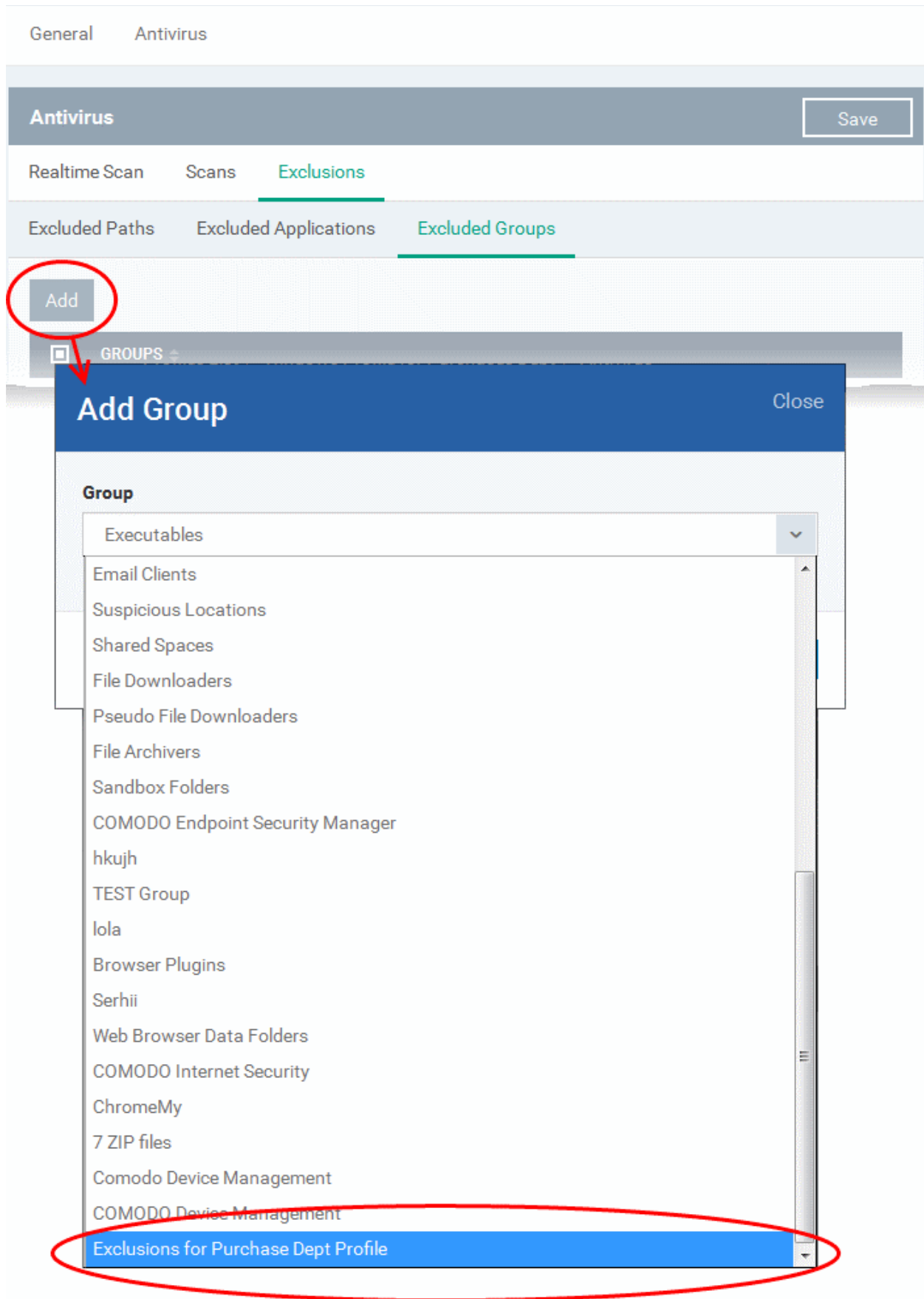
Tip: To include all the files in a folder, place the wildcard character in the place of file name in the folder path. For example: "C:\My Files*" "

The file(s) will be added to the group.

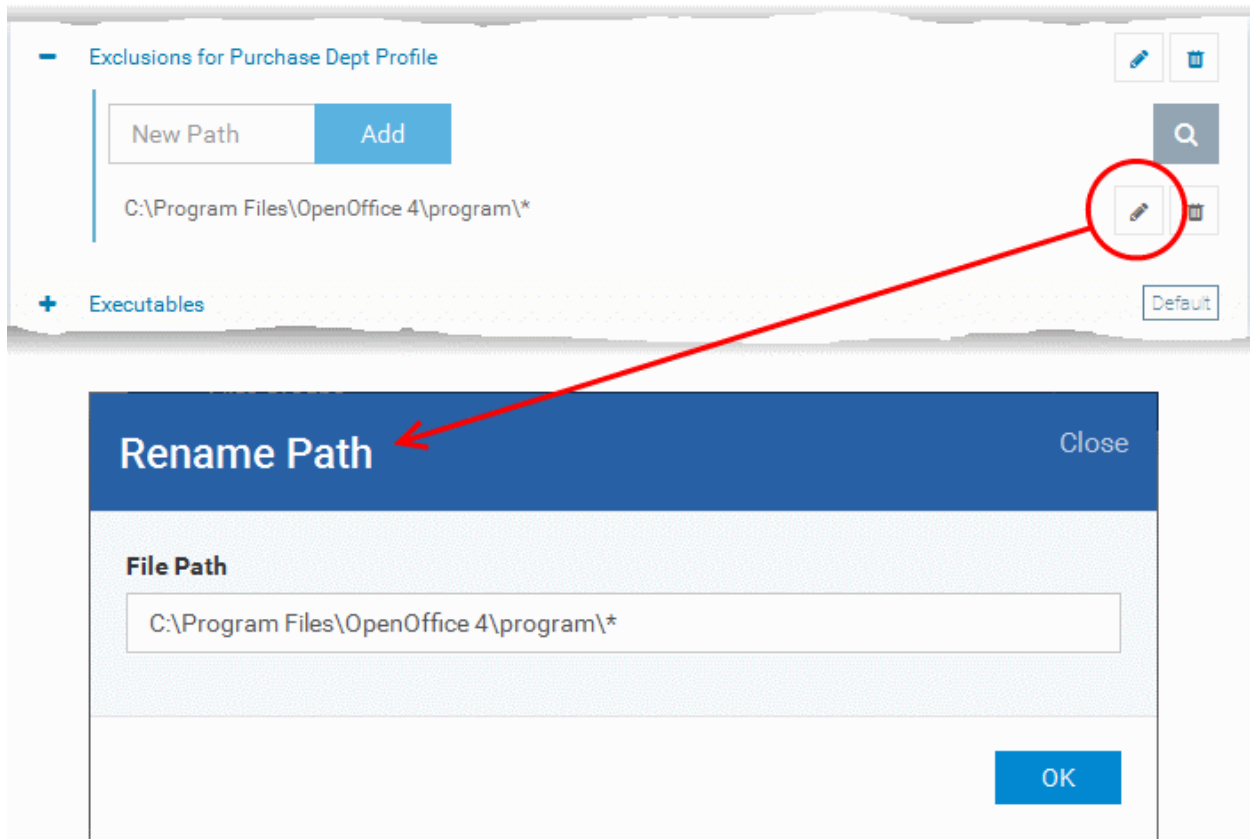


- Repeat the process to add more files to the group.

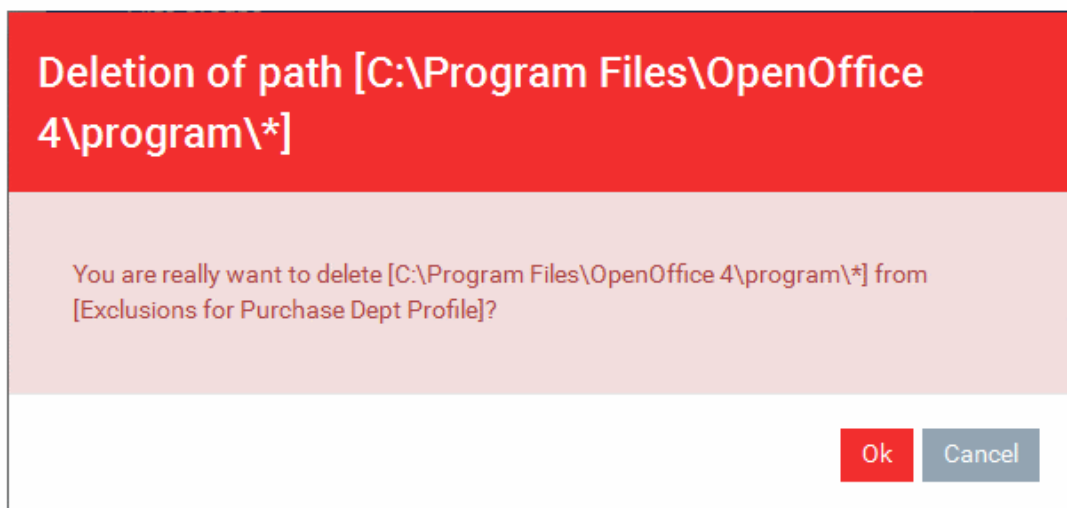
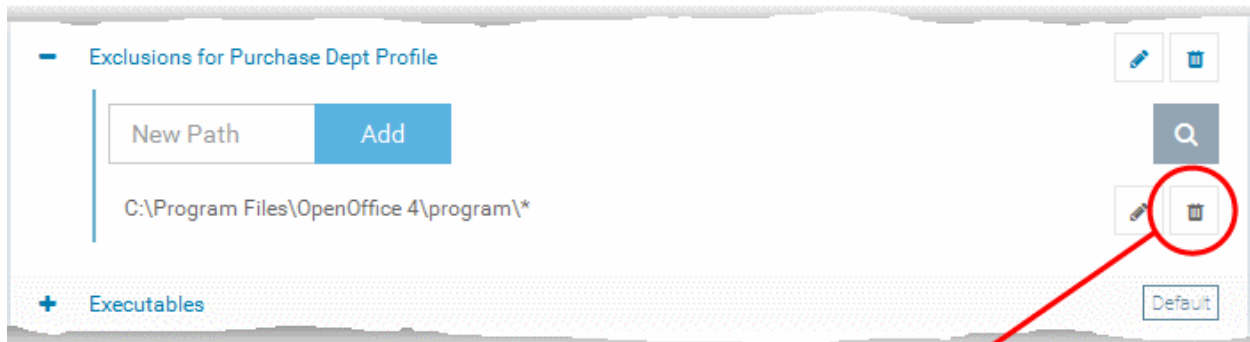
Once a File Group is added, it will be available for selection in applicable settings interfaces for defining the File Groups, example, for adding to 'Exclusions' list in 'Antivirus Settings' panel , in the 'Windows Profile' interface.



- To edit the files in the group, click the 'Edit' icon beside the file name.



- Edit the file path in the Rename Path dialog and click 'OK'.
- To remove a file added by mistake or an unwanted file from the group, click the trash can icon beside the file name.

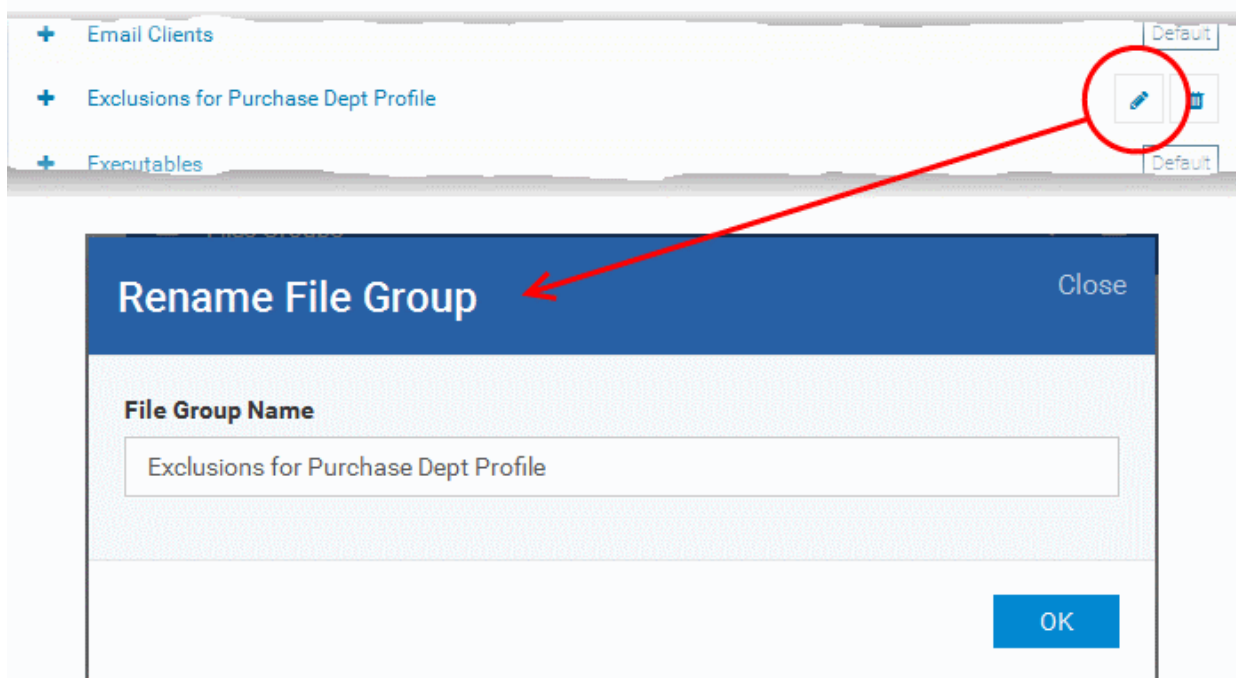


A confirmation dialog will appear.

- Click OK in the confirmation dialog

To edit the name of a File Group

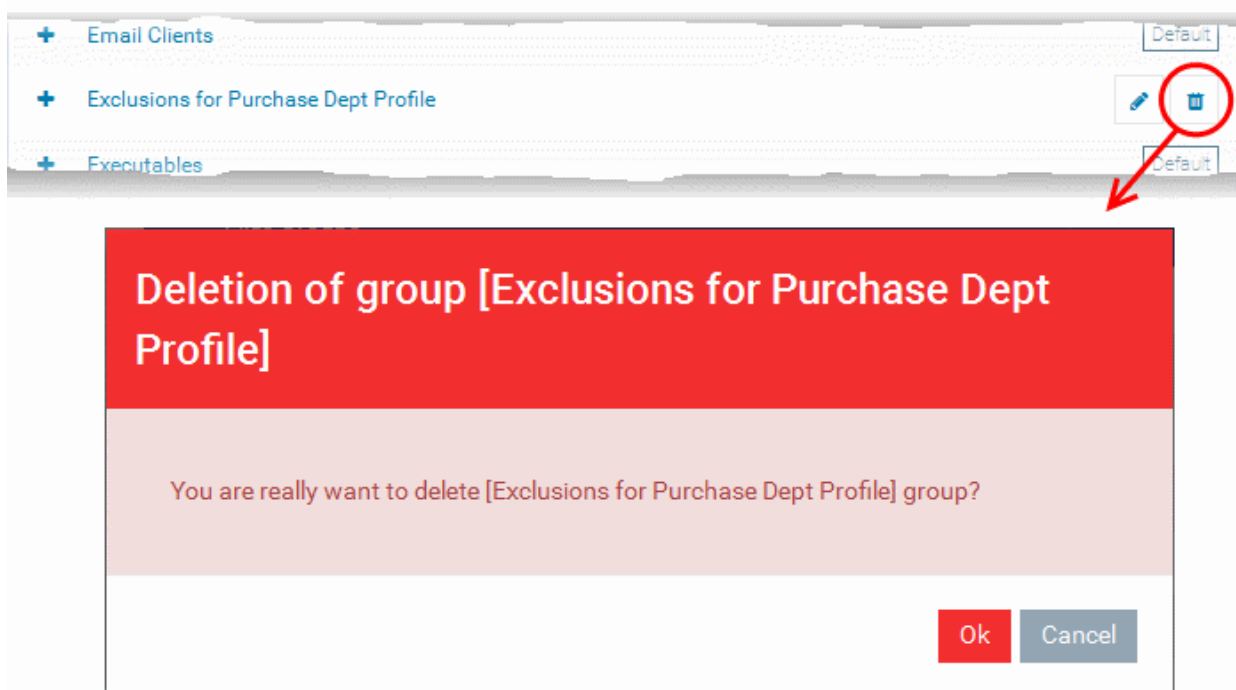
- Click the 'Edit' icon beside the File Group



- Enter the new name for the group in the 'Rename File Group' dialog and click 'OK'

To remove a File Group

- Click the Thrash can icon beside the File Group



A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

10.3. Configuring Role Based Access Control for Users

Users that are added to Comodo Device Manager (CDM) have administrative privileges and access to different areas of the interface, depending on the roles assigned to them. Administrators can create different roles with different access privileges and assign them to enrolled users as required. A single user can be assigned any number of roles.

The 'Role Management' interface allows administrators to create new roles with required permissions and assign roles to users. It contains two tabs:

- Roles - allows you to create and edit roles and configure each role's permissions
- Users - allows you to view and assign roles to users
- To open the 'Roles Management' interface, choose 'Settings' from the left and select 'Roles Management'.

NAME	DESCRIPTION	# OF USERS
NewRoleForTesting	Role with disabled all the permis...	1
Kirill	Kirill	1
Users [Default role]	Users of the system	66
Administrators	Administrators of the system	103

Roles

The Roles interface allows administrators to create various roles including administrative roles with different access permissions and privilege levels as required, for various departments in an organization and user roles with limited privilege levels. The roles created through this interface will be available for selection while adding a new user, enabling assigning the appropriate role to the new user. The administrator can add more roles or remove assigned roles to a user at a later time.

One of the roles created through this interface can be set as a default role. When a new user is added, the default role will be assigned to him/her, if no role is not selected by the administrator. The user can be assigned with a different role, at a later time, as required.

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

The screenshot shows the 'Roles Management / Roles' page. At the top, there is a navigation bar with a menu icon, the text 'Roles Management / Roles', a notification bell with '3' alerts, and a 'Logout (John Smith)' button. Below the navigation bar, there are tabs for 'Roles' (selected) and 'Users'. To the right, it says 'Default role: [Users](#)'. There is an 'Add Role' button with a plus icon. The main content is a table with three columns: 'NAME', 'DESCRIPTION', and '# OF USERS'. The table lists four roles: 'NewRoleForTesting' (1 user), 'Kirill' (1 user), 'Users [Default role]' (66 users), and 'Administrators' (103 users). Below the table, there is a pagination control showing '1' and '2' with arrows, and a 'Results per page: 20' dropdown menu. At the bottom right, it says 'Displaying 21-24 of 24 results.'

Roles - Column Descriptions	
Column Heading	Description
Name	The name of the role. Clicking on the name will open the 'Roles Management > Permissions' screen, allowing you to view and manage the permissions assigned to the role. Managing Permissions and Assigned Users of a Role for more details.
Description	The short description of the role.
#Of Users	Displays the number of users to whom the role was assigned. Clicking on the number opens the 'Role Management' > 'Members' screen allowing you assign the role to new users/ removing the role from existing users. Refer to the section 'Viewing the users assigned with the role' for more details.

Sorting Options

- Clicking on any of the column headers will sort the items in ascending/descending order of entries in that column.

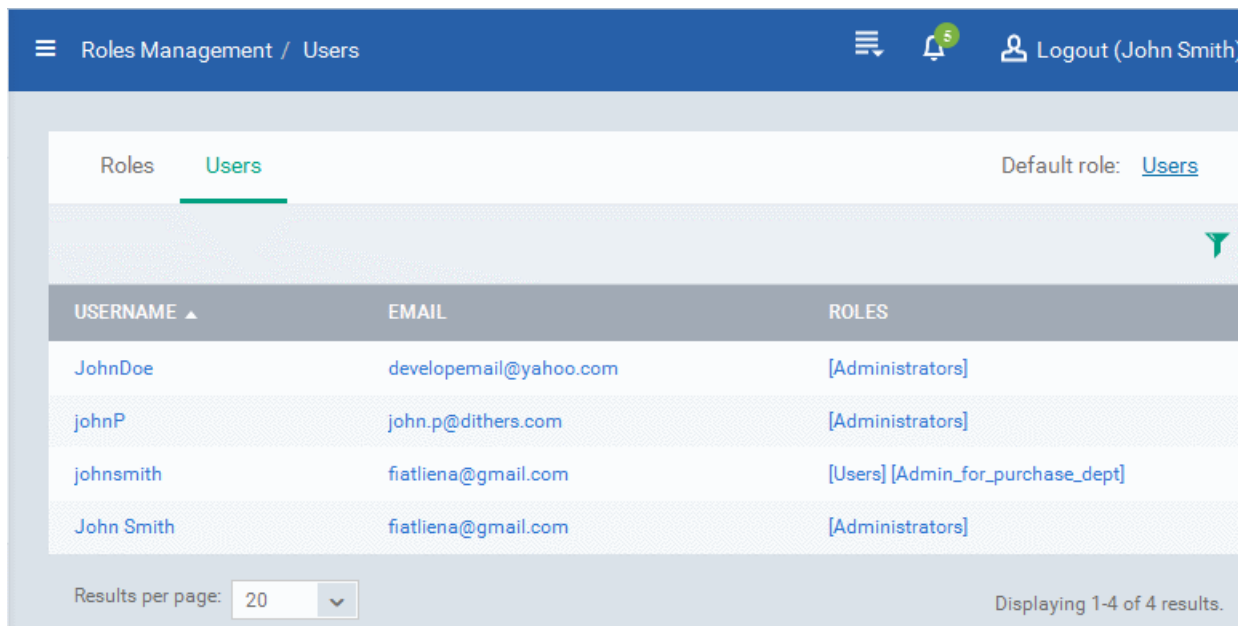
From the Roles interface, the administrator can:

- **Create a new role**
- **Manage a Role**
 - **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 the administrator to view the list of users added to CDM and the roles assigned to them. The administrator can also edit the roles assigned to each user from this interface.

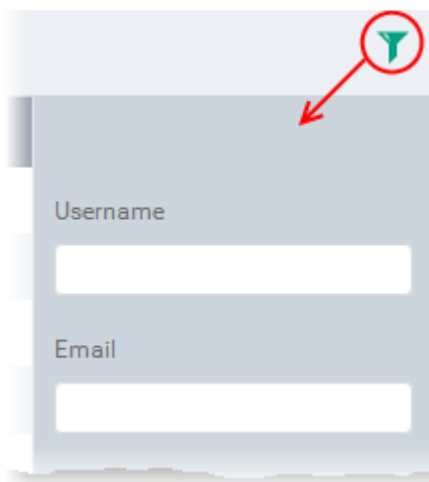
- To switch to 'Users' interface, click on the 'Users' tab.



Users - Column Descriptions	
Column Heading	Description
Username	The Login username of the user. Clicking on the username will open 'User Management > 'Users' screen allowing you to assign new roles to the user or to remove existing roles 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 management pane of the role. Refer to the section 'Managing Permissions and Assigned Users of a Role' for more details.

Sorting and Search Options

- Clicking on 'Username' and 'Email' column headers will sort the items in ascending/descending order of entries in that column.
- Click the funnel icon to search for items based on the filter parameter



- To display the users that are based on 'Username', and 'Email', enter the text partially or fully in the respective fields

and click the 'Apply' button.

The users that matches the entered parameters will be displayed in the screen.

- To display all the users again, clear the selections in the filter and click the 'Apply' button.
- Click on the funnel icon again to close the search option

The Users interface allows the administrator to:

- **Add or Remove roles to a user**

10.3.1. Creating a New Role

The administrator can create several roles with different permissions and privilege levels for administrators and users belonging to different departments of an organization.

To create a new role

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

The screenshot displays the 'Roles Management / Roles' interface. At the top, there is a navigation bar with a menu icon, the text 'Roles Management / Roles', a notification bell with '3', and a 'Logout (John Smith)' button. Below this, there are tabs for 'Roles' and 'Users', and a 'Default role: Users' indicator. A red circle highlights the 'Add Role' button, which is a green plus sign with a white plus sign inside. A red arrow points from this button to a 'Create New Role' dialog box. The dialog box has a blue header with the title 'Create New Role' and a 'Close' button. It contains two text input fields: 'Name *' with the value 'Admin_for_purchase_dept' and 'Description *' with the value 'With privileges applicable for purchase dept.'. A blue 'Create' button is located at the bottom right of the dialog box.

The 'Create new Role' wizard will start.

- Enter an appropriate name for the role to be created in the 'Name' text box.
- Enter a short description for the role in the 'Description' text box.

- Click 'Create'.

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


- Click on the name of the role to select the permissions to be assigned for the new role.

The screenshot shows the 'Roles' configuration interface. At the top, there are tabs for 'Roles' and 'Users', and a 'Default role' label. Below the tabs is an 'Add Role' button. A table lists existing roles:

NAME	DESCRIPTION	# OF USERS
Admin_for_purchase_dept	With privileges applicable for Pur...	0
ROLE_FOR_TEST	DO NOT DELETE !!!!! role for auto-...	0
...	...	1

Below the table, the selected role 'Admin_for_purchase_dept' is shown with a 'Make Default' link and 'Delete Role' and 'Edit' buttons. The 'Permissions' tab is active, showing a 'Save' button and a table of permissions:

PERMISSION	DESCRIPTION
<input type="checkbox"/> audit.threats	Access to threats report page
<input type="checkbox"/> inventory.devices.actions	Actions with devices. Child permission is: 'inventory.o
<input type="checkbox"/> audit.user-activity&devices	Access to user activity and devices report page. Child
<input type="checkbox"/> inventory.antivirus	Access right to antivirus (full control). Child permisio
<input type="checkbox"/> inventory.devices.applications	Access to application on devices part (read only). Chi
<input type="checkbox"/> inventory.devices.applications.manage	Access to application on devices part (full control). C
<input type="checkbox"/> inventory.devices.manage	Manage devices (full control). Child permission is: '

- Select the permissions to be assigned for the new role
- If you want to edit the role name/description or delete the role, click edit button  and select the required option from the drop-down
- If you want to make this as default role, so as to be applied to any new user enrolled to CDM without specifying a role at the time of enrollment, click 'Make Default'.
- Click 'Save' for your changes to take effect.

You can also assign the newly created role to users by clicking the 'Members' tab.

To assign the new role to selected users

- Click the 'Members' tab.

The 'Role Management' > 'Members' screen will open with a list of all the users enrolled so far to CDM.

The screenshot shows the 'Members' tab for the role 'Admin_for_purchase_dept'. The table below represents the data shown in the interface:

ACTION	USERNAME	EMAIL
Assign	a2	test.mdm.odessa@gmail.com
Assign	Acceptance	g.chebo@gmail.com
Assign	admin	test.mdm.odessa@gmail.com
Assign	Administrator	test.robot.odessa@gmail.com

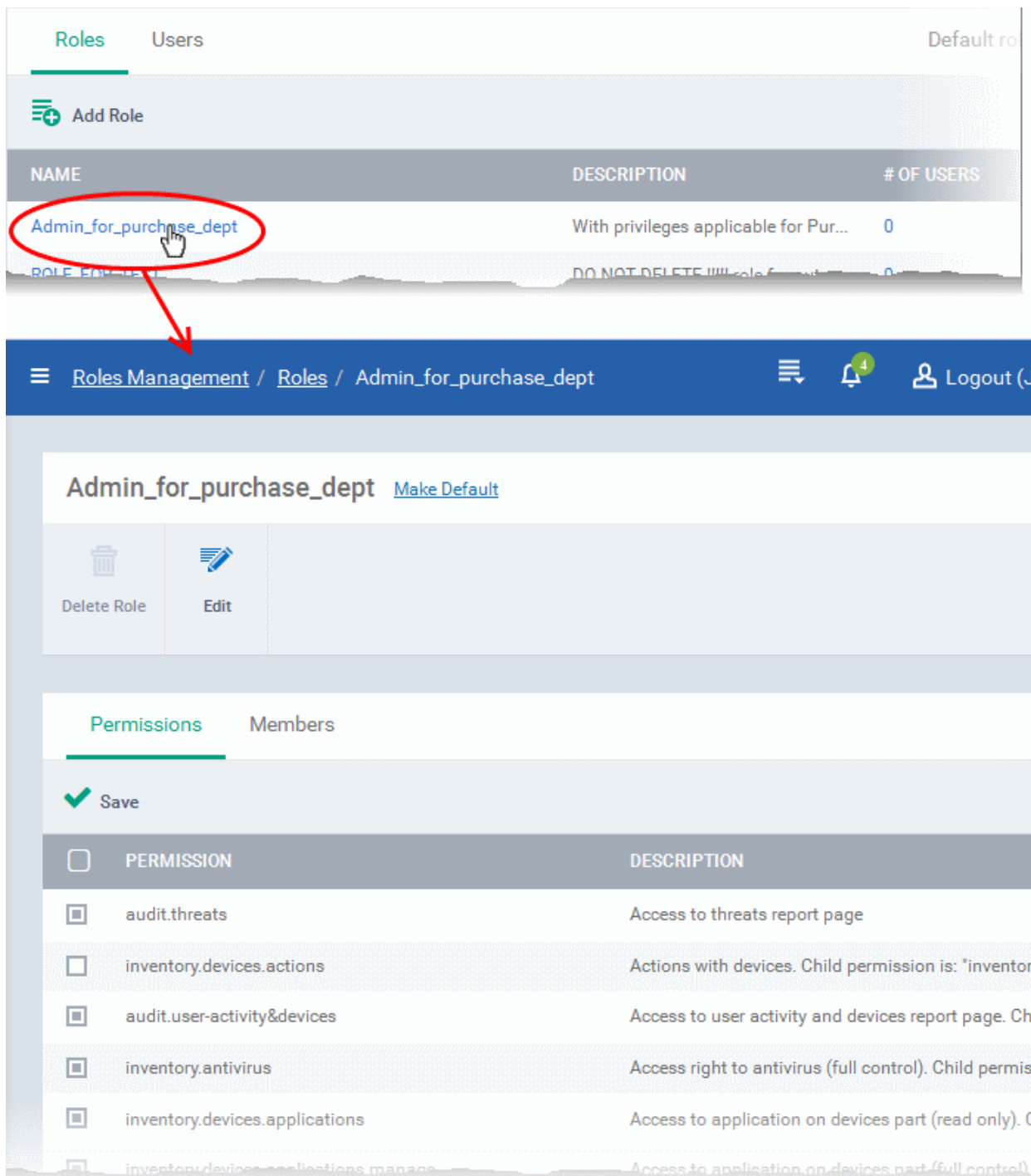
- To assign the role to a user, click the 'Assign' link under the Action column for the respective user.
- Repeat the process to assign the role to other users
- To remove the role from a user assigned by mistake, click the 'Revoke' link in the 'Action' column for the user to whom the role is already assigned.

10.3.2. Managing Permissions and Assigned Users of a Role

The administrator can view and modify any role created in the CDM at any time from the 'Roles' interface.

To view and manage a role

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

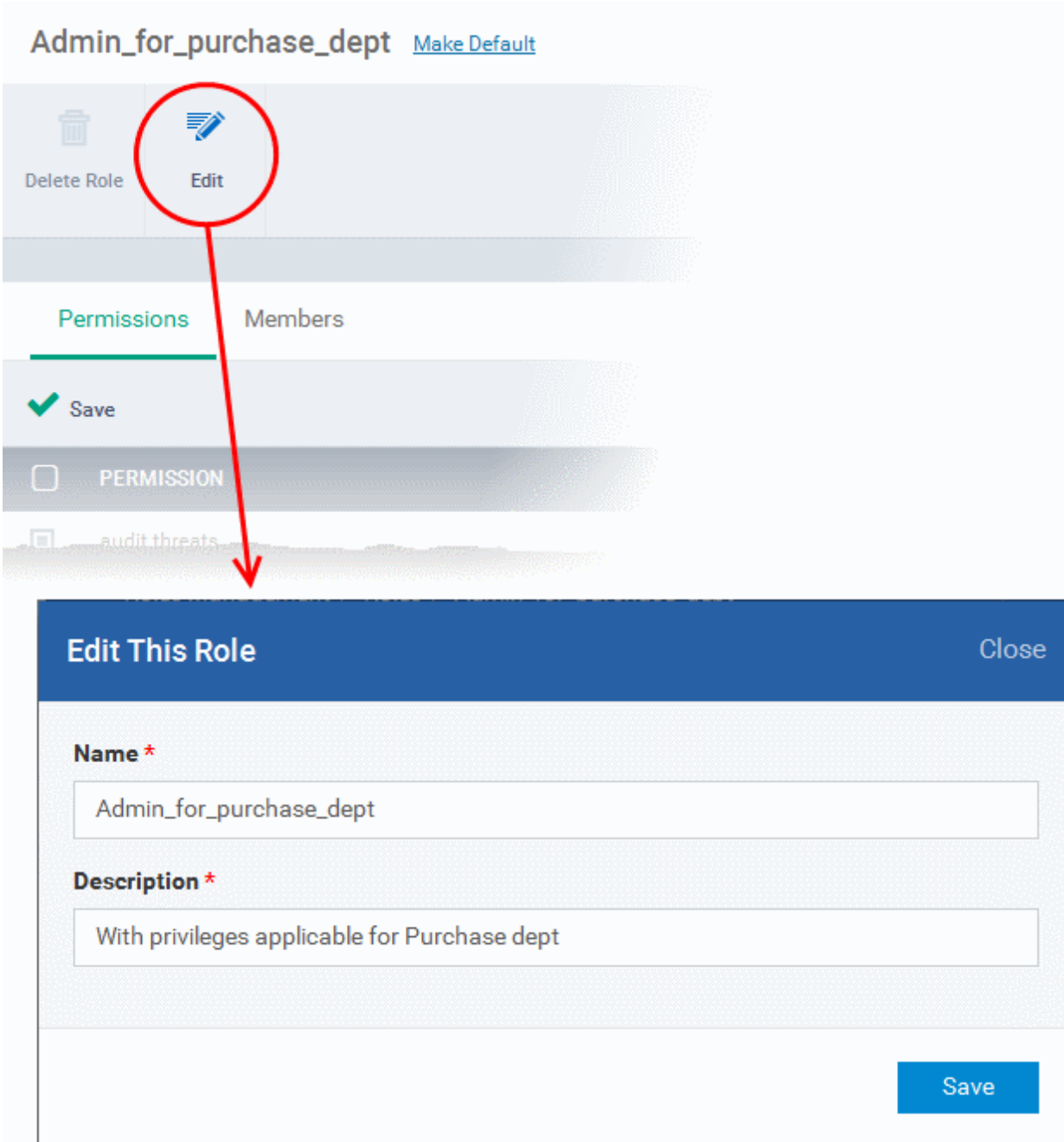


The 'Role Management' interface allows you to:

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

To edit a name and description of the role

- Click 'Edit' button  on the top



The screenshot shows the 'Admin_for_purchase_dept' role management interface. The 'Edit' button is circled in red, and a red arrow points from it to the 'Edit This Role' dialog box. The dialog box has a blue header with the title 'Edit This Role' and a 'Close' button. It contains two text input fields: 'Name *' with the value 'Admin_for_purchase_dept' and 'Description *' with the value 'With privileges applicable for Purchase dept'. A blue 'Save' button is located at the bottom right of the dialog box.

- To change the name of the role, enter the new name in the name text box
- To change the description of the role, enter the new role in the Description text box.
- Click 'Save' for your changes to take effect.

To manage the permissions assigned to the role

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

The screenshot shows the 'Admin_for_purchase_dept' role configuration page. At the top, there is a breadcrumb trail: 'Roles Management / Roles / Admin_for_purchase_dept'. On the right, there are navigation icons, a notification bell with a '4' badge, and a 'Logout (John Smith)' button. Below the breadcrumb, the role name 'Admin_for_purchase_dept' is displayed with a 'Make Default' link. There are two buttons: 'Delete Role' (with a trash icon) and 'Edit' (with a pencil icon). Below these, there are two tabs: 'Permissions' (active) and 'Members'. A green checkmark and 'Save' button are visible. The main content is a table with two columns: 'PERMISSION' and 'DESCRIPTION'. The table lists several permissions, some of which are selected with checkboxes.

<input type="checkbox"/>	PERMISSION	DESCRIPTION
<input checked="" type="checkbox"/>	audit.threats	Access to threats report page
<input type="checkbox"/>	inventory.devices.actions	Actions with devices. Child permission is: "inventory.devices".
<input checked="" type="checkbox"/>	audit.user-activity&devices	Access to user activity and devices report page. Child permi...
<input checked="" type="checkbox"/>	inventory.antivirus	Access right to antivirus (full control). Child permissions are...
<input checked="" type="checkbox"/>	inventory.devices.applications	Access to application on devices part (read only). Child per...
<input checked="" type="checkbox"/>	inventory.devices.applications.manage	Access to application on devices part (full control). Child ne...

- Select the new permissions to be assigned to the role.
- Deselect the permissions to be removed from the role.
- Click 'Save' for your changes to take effect.

To view the list of users assigned with the role

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

Roles Management / Roles / Admin_for_purchase_dept

Admin_for_purchase_dept [Make Default](#)

Delete Role Edit

Permissions **Members**

ACTION	USERNAME ▲	EMAIL
Assign	a2	test.mdm.odessa@gmail.com
Assign	Acceptance	g.chebo@gmail.com
Assign	admin	test.mdm.odessa@gmail.com
Assign	Administrator	test.robot.odessa@gmail.com
Assign	agaber	alexey.gaber@comodo.com

The 'Action' column indicates the users that are assigned the selected role. 'Revoke' means the user is assigned the role and 'Assign' indicates the role is not assigned.

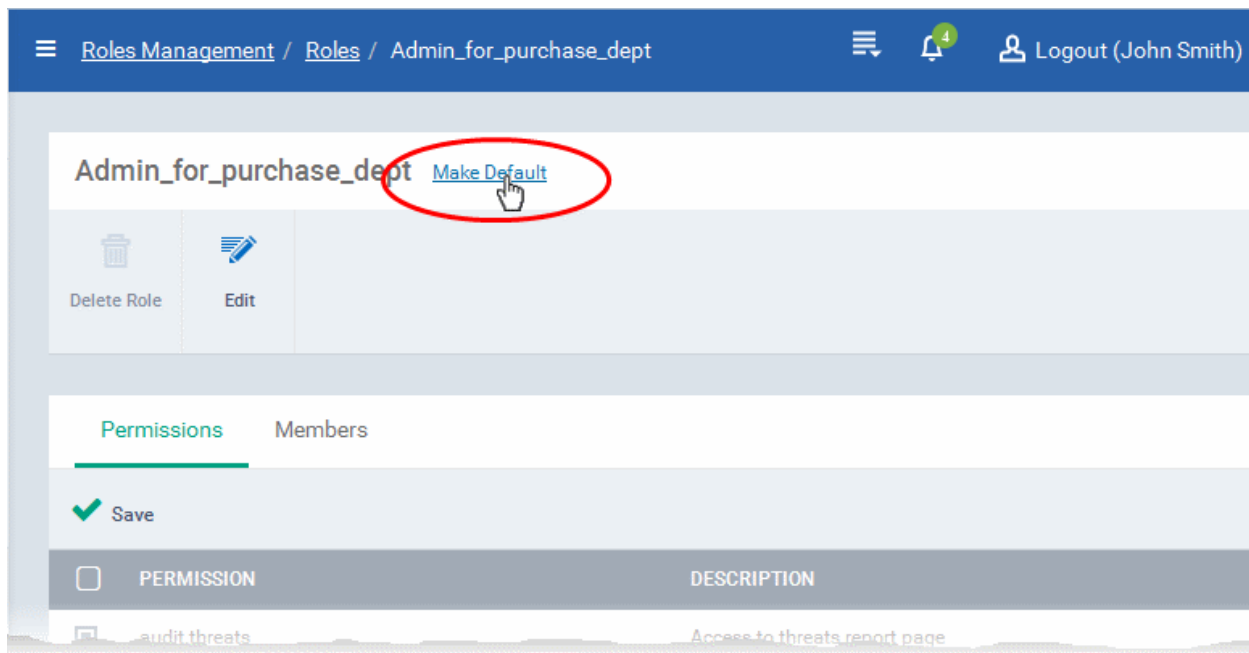
- To assign the role for a new user, click 'Assign'
- To remove the role from an assigned user, click 'Revoke'

Clicking on a username leads to the respective 'Assign the Role(s) to User' screen. Refer to the section **Managing Roles assigned to a User** for more details.

To make the role as a default role

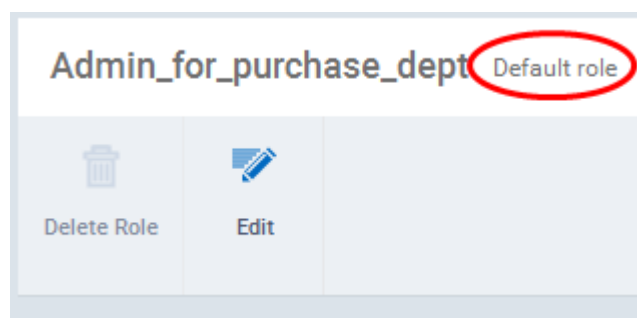
A default role will be automatically applied to users that are not selected a role during enrollment.

- Click on the name of the role from the 'Roles' interface to open 'Role Management' interface



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

The role will be made as default role and displayed.

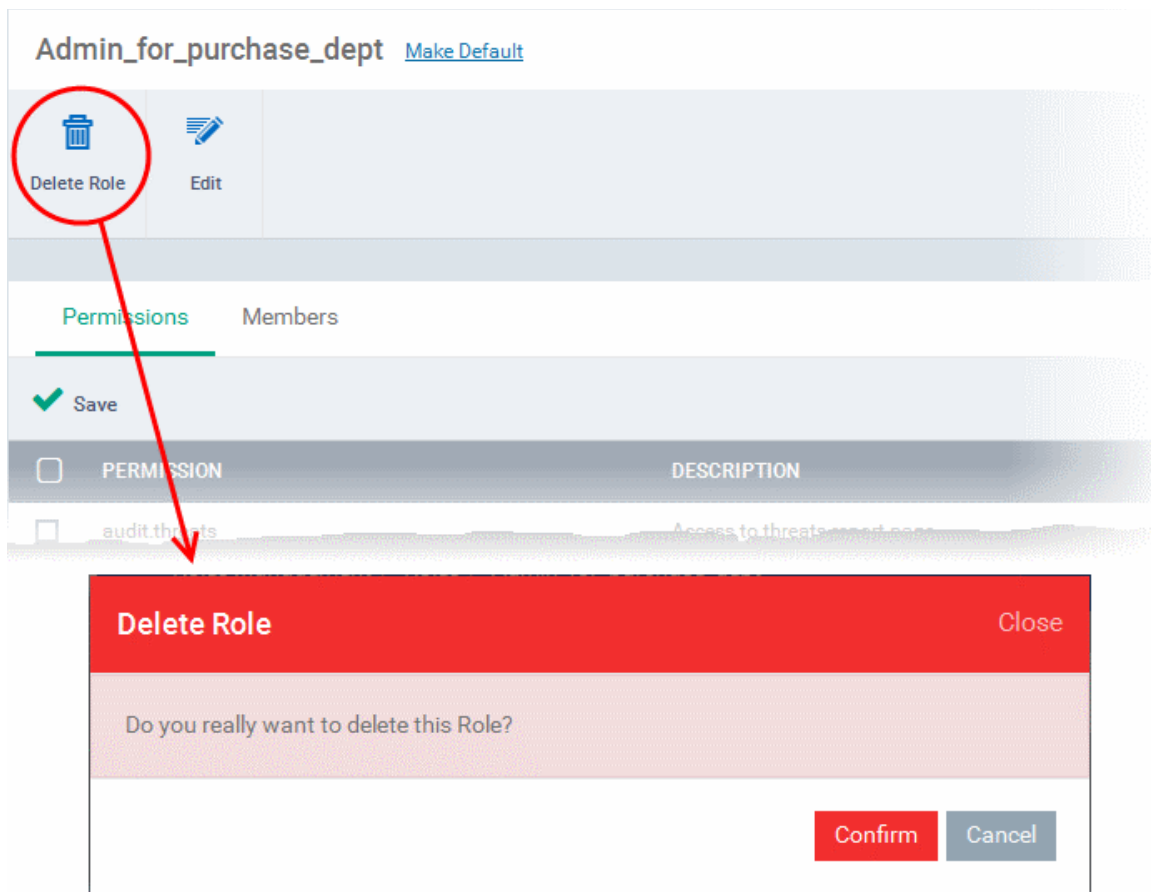


10.3.3. Removing a Role

If required, the administrator can remove roles that are no longer deemed necessary. The roles that are assigned to users cannot be removed. Before removing a role the administrator should remove the role from all the users to whom it has been assigned. Also, the role defined as default cannot be deleted.

To remove a role

- Choose 'Settings' from the left and select 'Roles Management'.
- Click the 'Roles' tab.
- Click on the 'Role' name to open the 'Role Management' interface
- Click Delete Role from the top



A confirmation dialog will appear.

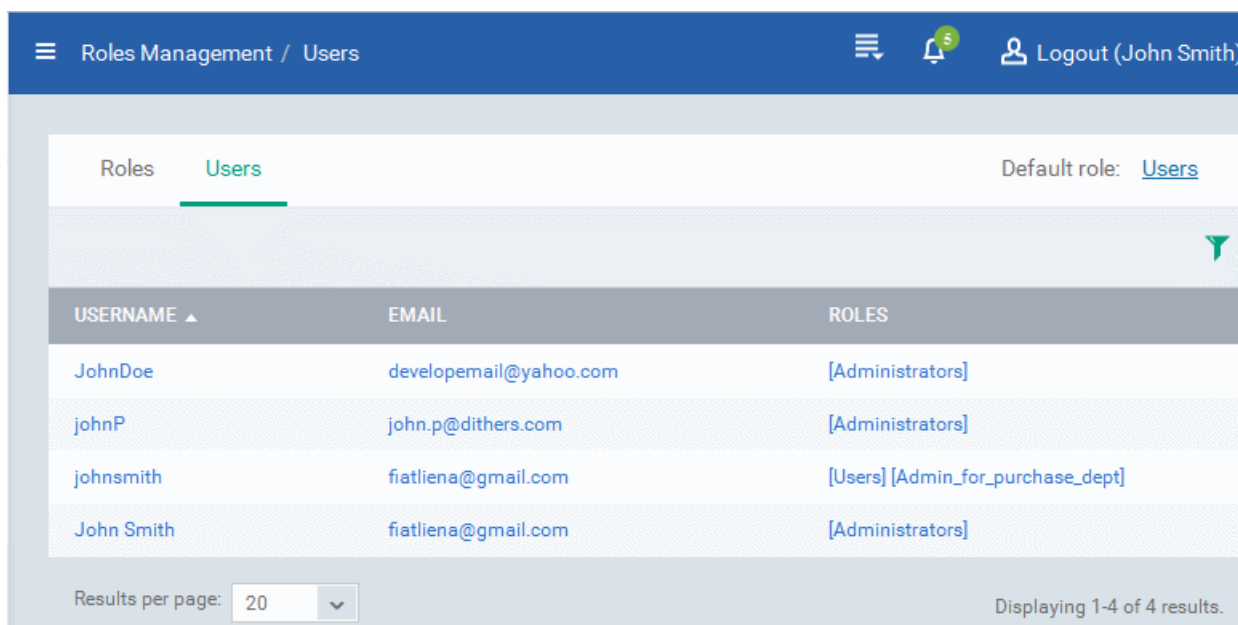
- Click 'OK' to remove the role.

10.3.4. Managing Roles Assigned to a User

The 'Users' interface allows the administrator to add new roles and to remove roles assigned to a user.

To open the Users interface

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



The list of users with their email addresses and roles assigned to them will be displayed.

To manage roles assigned to a user

- Click on the username that you want to manage the roles

The 'Assign the Role(s) to User' interface will open with a list of all the roles created in CDM . The roles assigned to the user will be indicated as 'Revoke' under the 'Action' column.

Roles		Users	Default role: Users
Roles of johnsmith			
ACTION	ROLE NAME		
Assign	ROLE_FOR_DELETE		
Revoke	Admin_for_purchase_dept		
Assign	ROLE_FOR_TEST		
Assign	johnsmith		

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

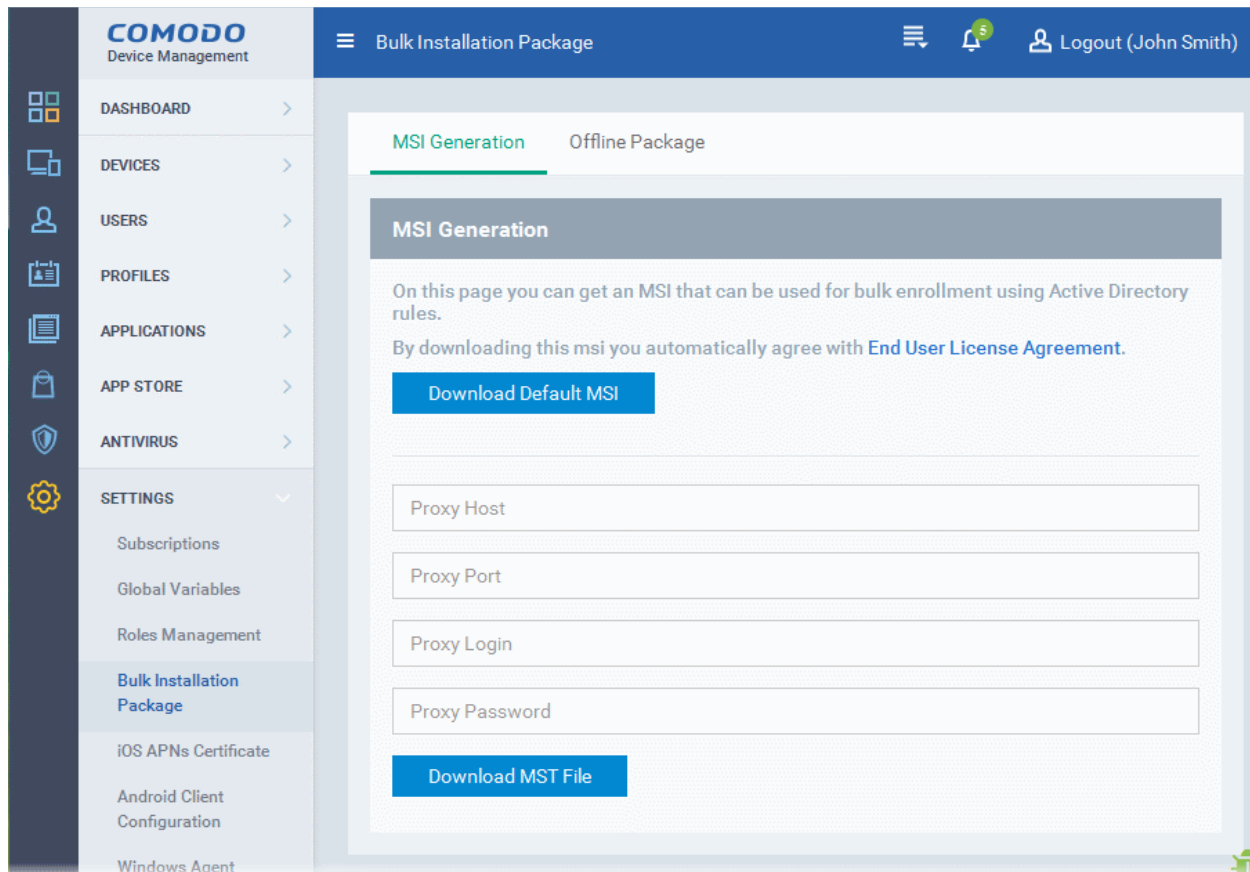
10.4. Downloading CDM Installation Packages for Windows Devices

Comodo Device Manager requires an agent to be installed on each managed Windows device to enable communication with the CDM Central Service Server.

- For individual devices, the agent will be automatically installed during device enrollment and will establish a connection to the server. Refer to the section **Enrolling Windows Endpoints** for more details.
- Administrators can bulk enroll networked devices by downloading the installation package from CDM and creating a software installation group policy for their Active Directory (AD) server.
- Administrators can also manually enroll devices by downloading the installation package from CDM and installing it on a target device.

The 'Bulk Installation Package' interface allows administrators to download agent and CES installation packages for offline installation and for installation via Active Directory rules.

- To open the Bulk Installation Package screen, choose 'Settings' from the left and select 'Bulk Installation Package'.



The interface contains two tabs:

- **MSI Generation** - Allows administrators to download installation packages for deployment via AD server. Refer to the section [Downloading Package for installation through AD server](#) for more details.
- **Offline package** - Allows administrators to download installation package for offline installation and enrolling devices for specific users. Refer to the section [Downloading Offline Installation Package](#) for more details.

10.4.1. Downloading Package for installation through AD server

Installation via Active Directory group policy allows the bulk enrollment of network devices for management through CDM. You can download the default MSI package for direct installation and / or transformed MST installation file for installation through a proxy server.

To download the installation package

- Choose 'Settings' from the left and choose 'Bulk Installation Package'
- Click the 'MSI Generation' tab
- To download the agent installation file for direct installation from the AD server via Group Policy Object (GPO), click 'Download Default MSI'.

MSI Generation
Offline Package

MSI Generation

On this page you can get an MSI that can be used for bulk enrollment using Active Directory rules.

By downloading this msi you automatically agree with [End User License Agreement](#).

Download Default MSI

Download MST File

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 CDM server to begin importing the device.

- To download the installation file for installation through proxy server
 - 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
- Click 'Download MST File'

CDM will create a .mst transform file containing the proxy server installation commands. 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 CDM server to begin importing the device .

By default, The Devices enrolled via AD server will be assigned to the user account of the administrator that initiated the import process.

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>.

10.4.2. Downloading Offline Installation Package

Administrators can download an installation package containing the agent and the CES application for offline installation. This is useful for endpoints which could not be reached by CDM server for auto - installation of the agent during its enrollment.

To download the installation package

- Choose 'Settings' from the left and choose 'Bulk Installation Package'
- Click the 'Offline Package' tab

Prerequisite - The end-user of the device should have already been added to CDM. Administrators can download installation package only for existing users.

The screenshot shows the 'Offline Package' configuration window. At the top, there are two tabs: 'MSI Generation' and 'Offline Package', with 'Offline Package' selected. Below the tabs is a header bar with 'Offline Package' on the left and 'Update installer's packages' on the right. The main content area is divided into sections: 'Choose Version' with radio buttons for 'Comodo Endpoint Security x86' (selected) and 'Comodo Endpoint Security x64'; 'Additional Options' with a checkbox for 'Include initial Anti-virus signature database'; 'Choose A Profile To Apply During Installation' with a text input field labeled 'Profile'; and 'Choose A User To Apply During Installation *' with a text input field labeled 'User'. At the bottom left is a blue button labeled 'Download installer'.

- Choose the 64 bit or 32 bit version of CES appropriate for the target operating system.
- If you want the latest version of the virus signature database to be installed along with CES, choose 'Include initial Anti-virus signature database'. This allows initial antivirus scans to be run without first updating the database on the endpoints.
- Choose the Windows configuration profile to be applied to the endpoint upon enrollment.
 - Enter the first few characters of the name of the profile you want to apply and select from the predictions 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 at later time. Refer to the section [Viewing and Managing Profiles Associated with the Device](#) for more details.

- Specify the user whose device is to be enrolled
 - Enter the first few characters of a user name and select from the predictions that appear.
- Click 'Download Installer'.

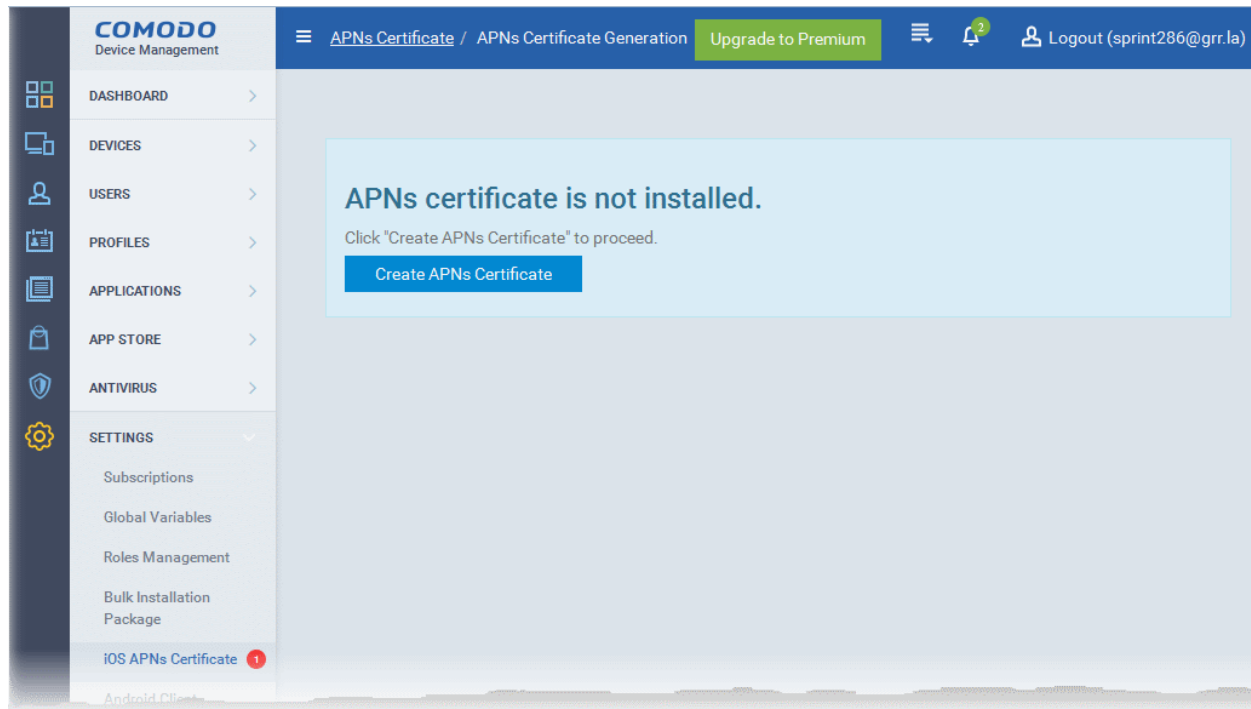
CDM will create a custom installation file in .msi format for installation on to the user's device. Administrators should transfer the file to the target device for manual installation. Once installed, the agent will establish communication with the CDM server and the device will be automatically enrolled.

10.5. Adding Apple Push Notification Certificate

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

Step 1- Generate your PLIST

- In the CDM interface, choose 'Settings' from the left and select 'iOS APN's Certificate'.



- Click the 'Create APNs Certificate' button from the right pane at the top-right to open the APN certificate application form. The fields on this form are for a Certificate Signing Request (CSR):

APNs certificate is not installed.

Click "Create APNs Certificate" to proceed.

Create APNs Certificate

Generation of APNs Certificate Close

Country Name *

Email Address *
State Or Province Name *
Locality Name (eg, city) *
Organization Name *
Organizational Unit *

Organizational Unit Name (eg, section)

Common Name *

(e.g. server FQDN or YOUR name)

Create Reset

- 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 Apple APNs Certificate

Upload Apple APNs Certificate Cancel Save

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

1. Download: [The Apple PLIST Signed by COMODO](#)
2. Login to Apple web site with your Apple ID (regular free account is enough): [Apple Push Certificate Portal](#)
3. Upload the Apple PLIST signed by Comodo to Apple to generate APNs certificate.
4. Download generated APNs Certificate from Apple.
5. Upload APNs certificate into Device Management system.

Apple APNs Certificate *

Select .PEM file Browse

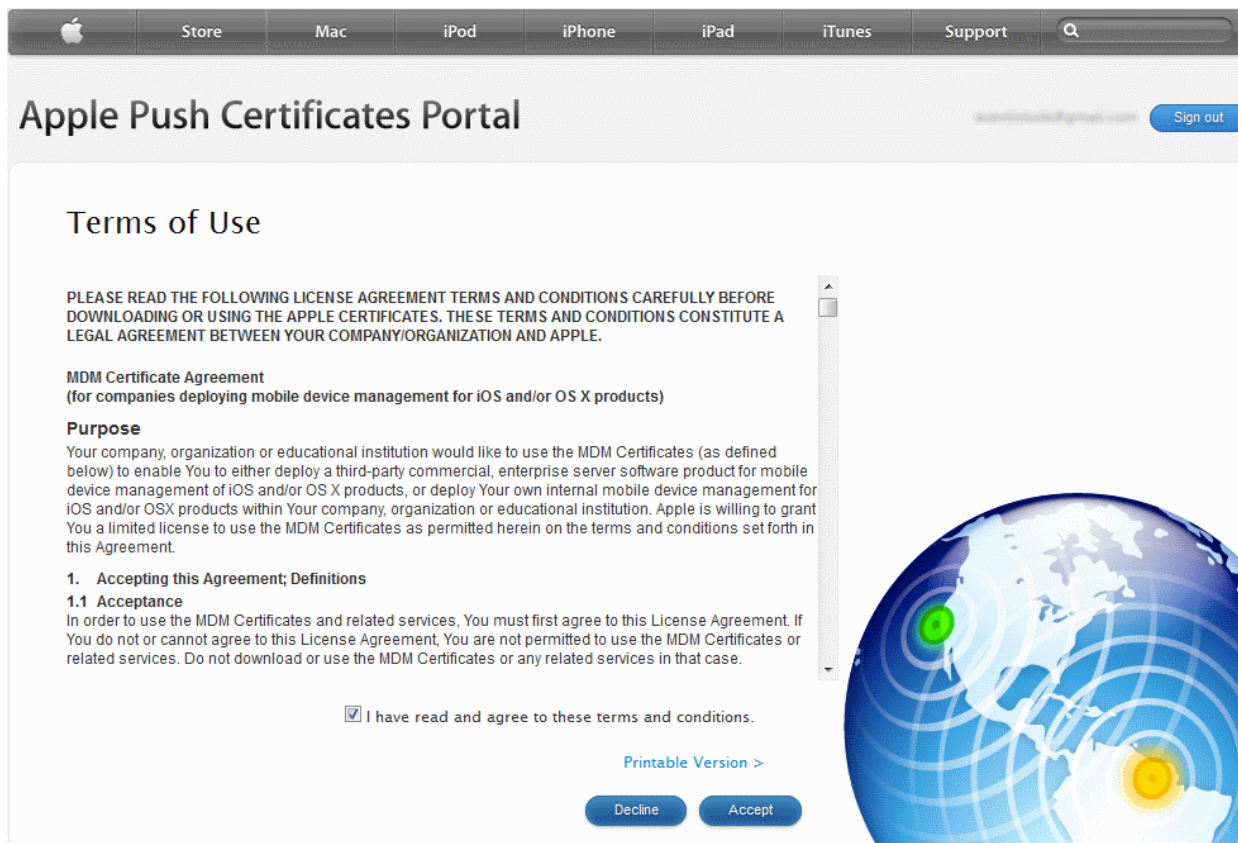
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO_Apple_CSR.csr'. Please save this to your local drive.

Step 2 - Obtain Your Certificate From Apple

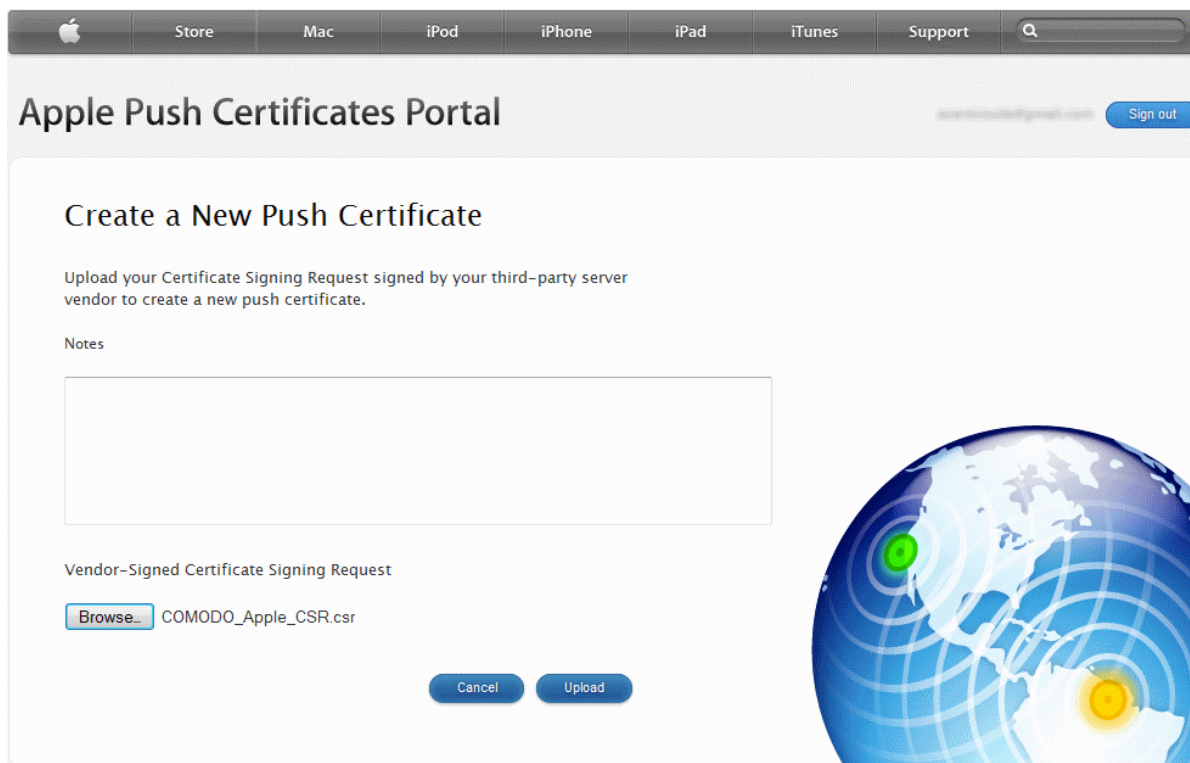
- Login to the 'Apple Push Certificates Portal' with your Apple ID at <https://identity.apple.com/pushcert/>.
If you do not have an Apple account then please create one at <https://appleid.apple.com>.
- Once logged in, click 'Create a Certificate'.



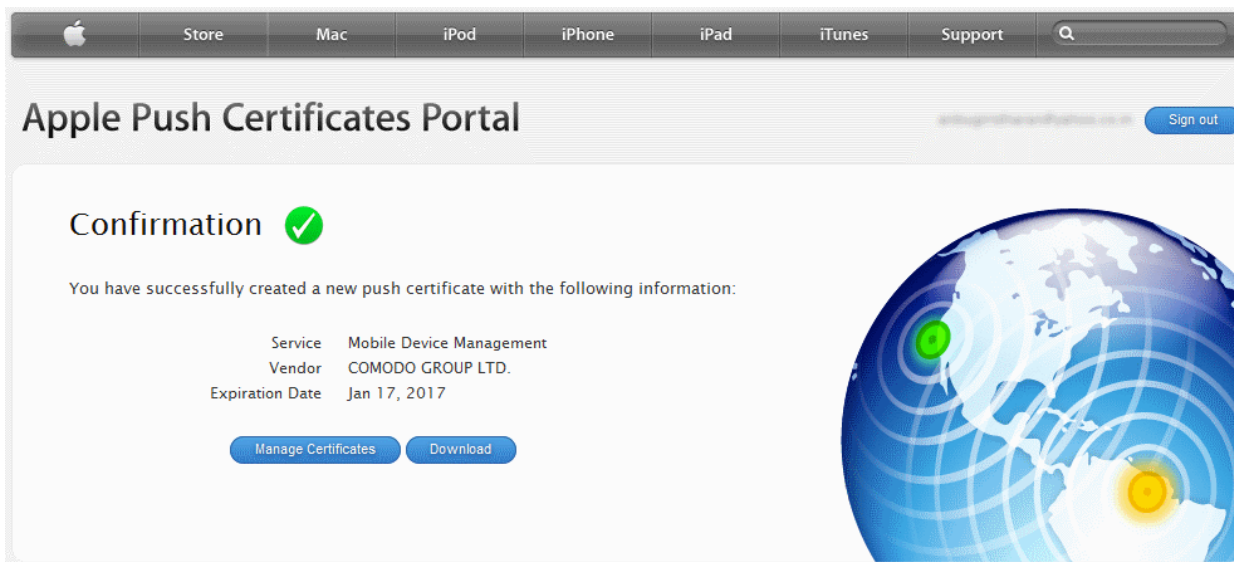
You will need to agree to Apple's EULA to proceed.



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



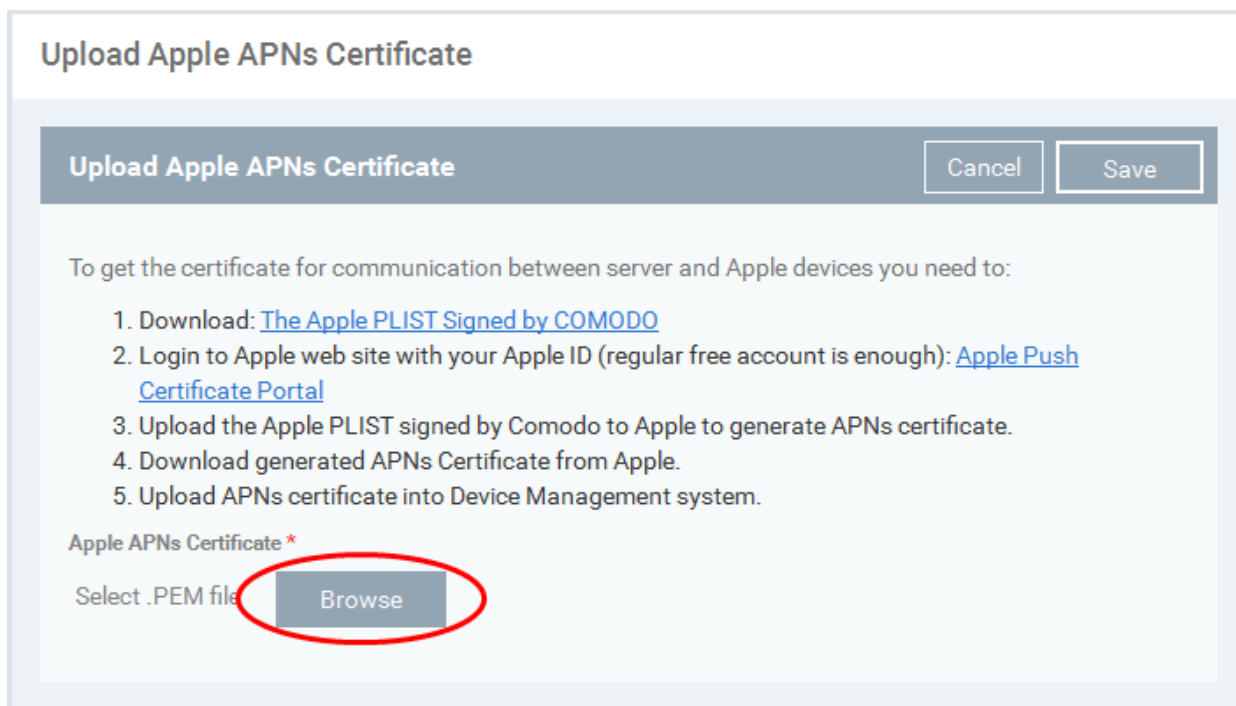
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



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

Step 3- Upload your certificate to CDM

- Next, return to the CDM interface and open the APNs interface. Click the 'Browse' button to locate your certificate file then click 'Save' to upload your certificate.



The APNs Certificate details interface will open:

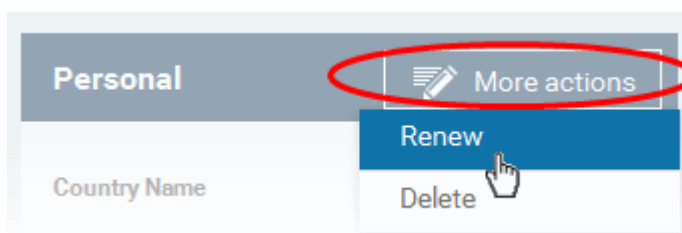
iOS APNs Certificate

Personal	Additional Info
<p>Country Name India</p> <p>Locality Name Kanchipuram</p> <p>Organization Name Self Org</p> <p>Organization Unit Name Self Org</p> <p>Common Name www.comodo.com</p> <p>Email admin@comodo.com</p>	<p>Time Activate Jan 18, 2016, 11:11:36 AM</p> <p>Time Expire Jan 17, 2017, 11:11:36 AM</p>

Your CDM Portal will now be able to communicate with iOS devices.

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 the 'More Actions' button and choose 'Renew'.



- To remove the certificate for generating a new APNs certificate, click the 'More Actions' button and choose 'Delete'.

10.6. Configuring the CDM Android Agent

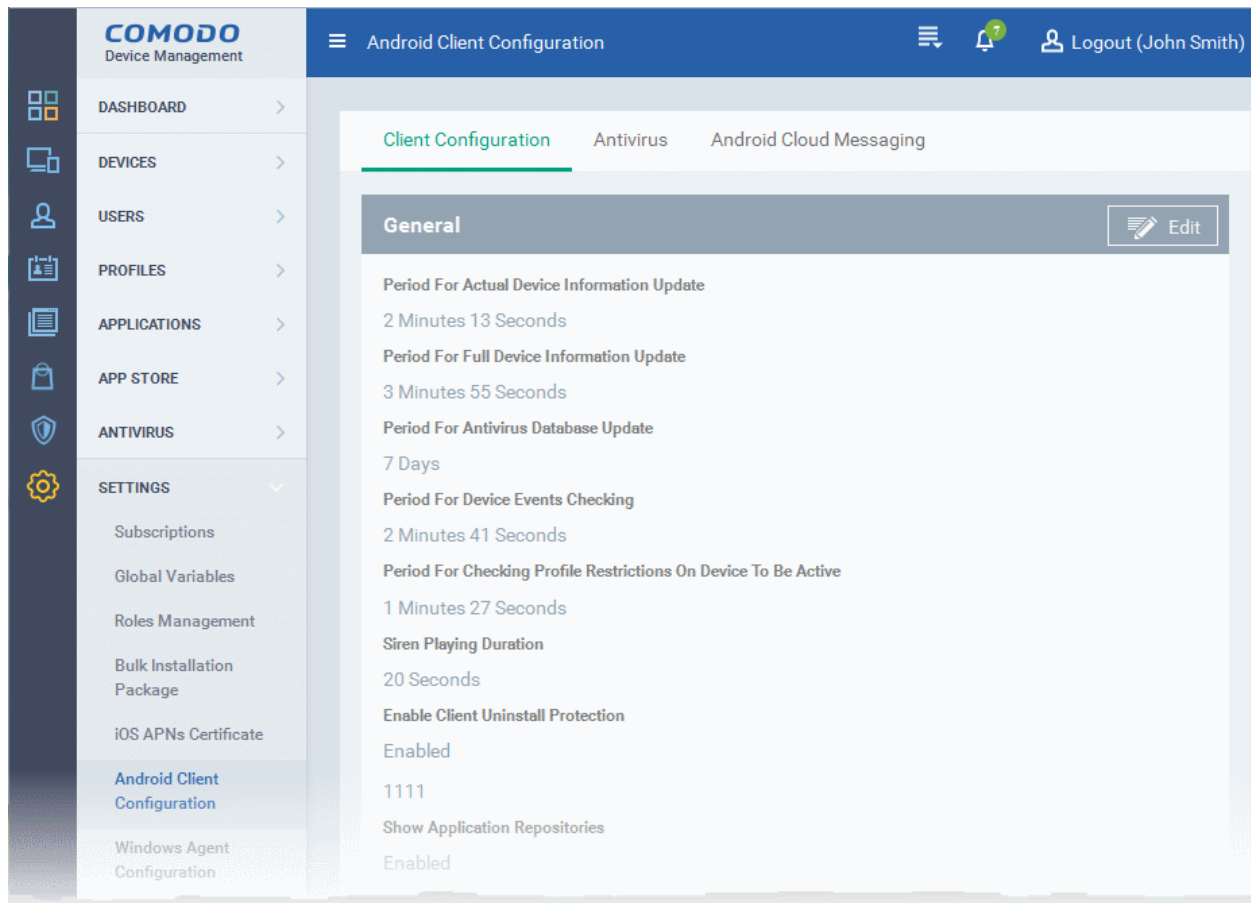
The 'Android Client Configuration' area allows you generate a Google Cloud Messaging token, configure the general behavior of the CDM agent and to configure basic antivirus settings.

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 CDM and Android devices. Refer to the section [Adding Google Cloud Messaging \(GCM\) Token](#) for more details.

To open the 'Android Client Configuration' screen, choose 'Settings' from the left and select 'Android Client Configuration':

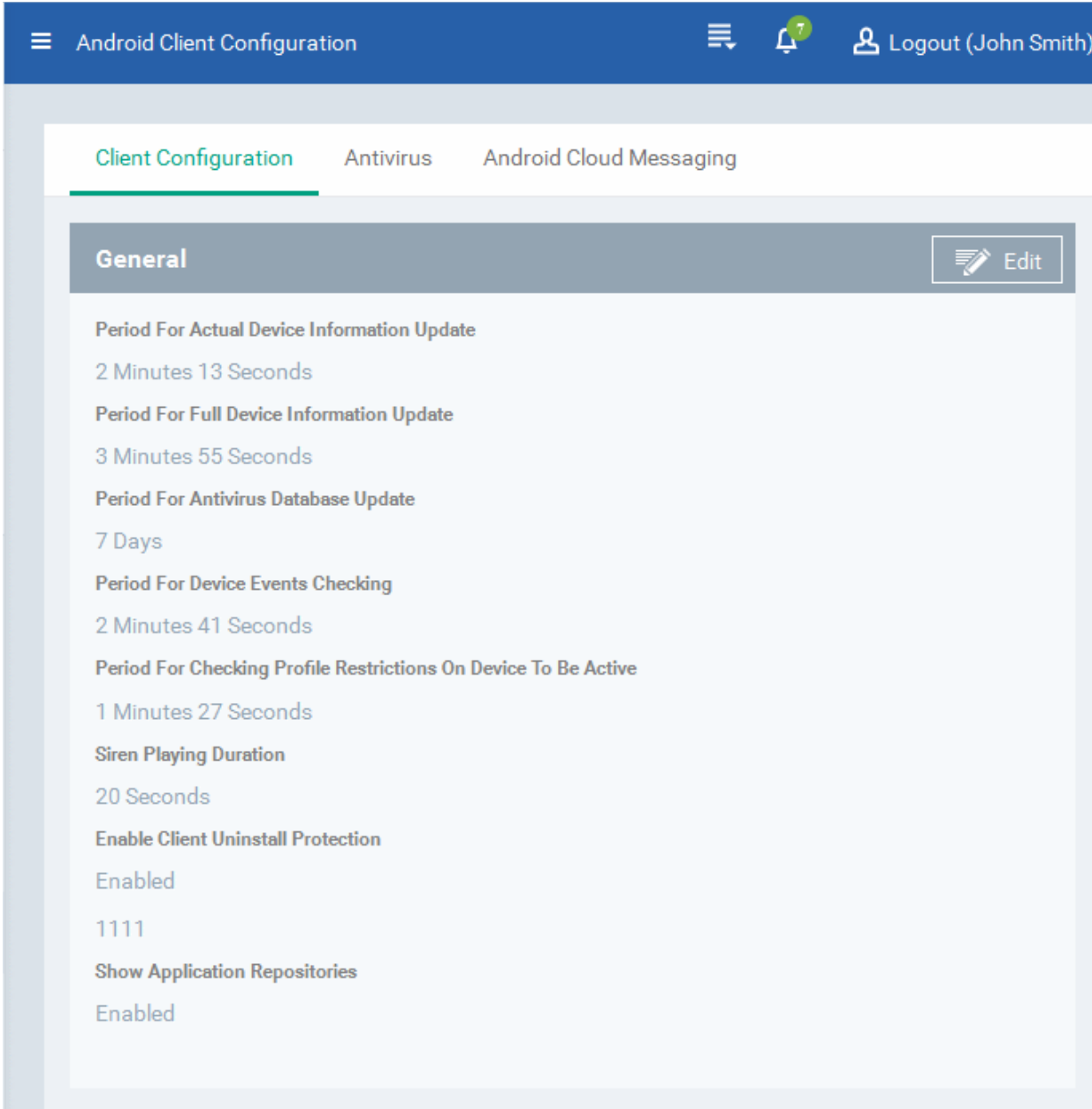


10.6.1. Configuring General Settings

The Android 'Client Configuration' area allows you to configure various settings related to update periods, device alarms, uninstall protection and the visibility of application repositories on the device.

To open the Android 'Client Configuration' interface:

- Choose 'Settings' from the left and select 'Android Client Configuration'.
- Click the 'Client Configuration' tab:



Android Client Configuration

Client Configuration Antivirus Android Cloud Messaging

General Edit

Period For Actual Device Information Update
2 Minutes 13 Seconds

Period For Full Device Information Update
3 Minutes 55 Seconds

Period For Antivirus Database Update
7 Days

Period For Device Events Checking
2 Minutes 41 Seconds

Period For Checking Profile Restrictions On Device To Be Active
1 Minutes 27 Seconds

Siren Playing Duration
20 Seconds

Enable Client Uninstall Protection
Enabled

1111

Show Application Repositories
Enabled

- Click the edit button  on the top right to modify these settings

The settings screen will be displayed.

Client Configuration Antivirus Android Cloud Messaging

General Cancel Save

Period For Actual Device Information Update

 2 Minutes 13 Seconds

Period For Full Device Information Update

 3 Minutes 55 Seconds

Period For Antivirus Database Update

 7 Days

Period For Device Events Checking

 2 Minutes 41 Seconds

Period For Checking Profile Restrictions On Device To Be Active

 1 Minutes 27 Seconds

Siren Playing Duration

 20 Seconds

Enable Client Uninstall Protection

Show Application Repositories

Android Client Configuration Settings	
Parameter	Description
Period for actual device information update	The update time interval for device information such as battery level, CPU usage, location of the device (GPS) and current WiFi SSID.
Period for full device information update	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.
Period for antivirus database update	The time intervals at which the antivirus database should be updated on the device.
Period for device events checking	The time interval at which the device should check CDM for new push notifications.
Period for checking profile	The time interval at which the client checks that its profile restrictions are in place.

restrictions on device to be active	
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. <ul style="list-style-type: none"> Select the 'Enable client uninstall protection' check box and specify a password in the text box. <p>The CDM agent can be uninstalled from any enrolled device only after entering the password.</p>
Show 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.

10.6.2. Configuring Android Client Antivirus Settings

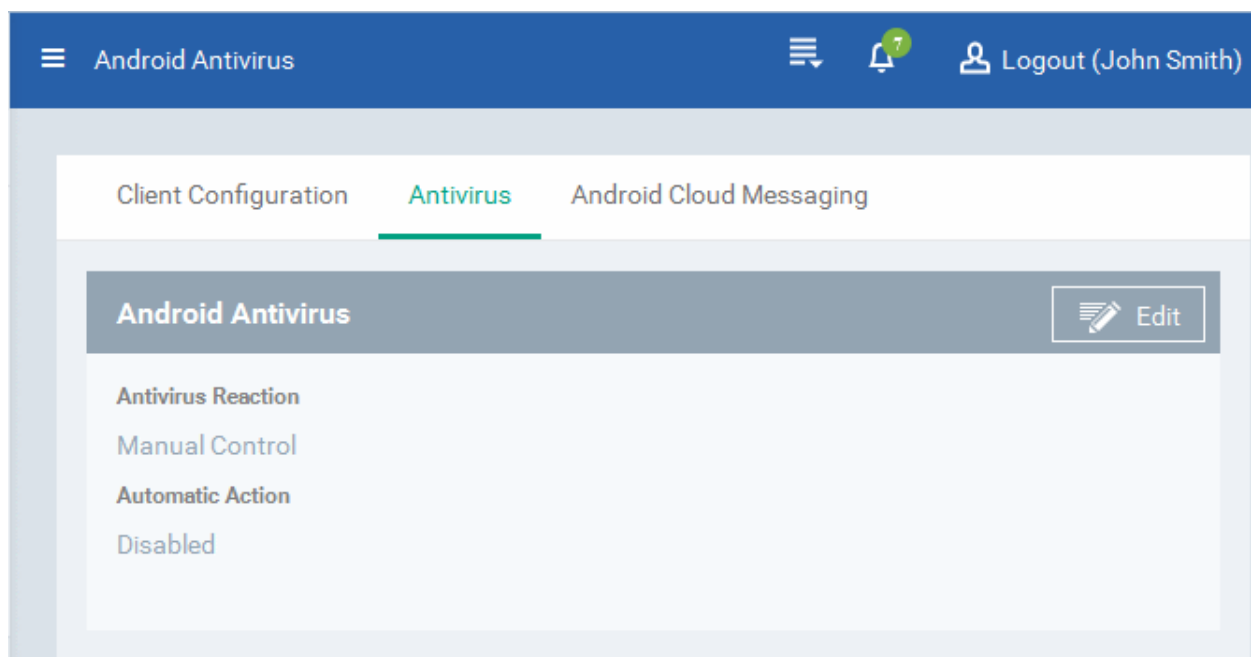
The Android Client Antivirus provides real-time protection against malware and malicious apps on Android devices. Administrators can also launch 'on-demand' scans from the CDM administrative console on selected devices.

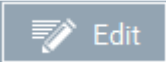
The antivirus settings area allows administrators to configure whether threats identified by the antivirus should be automatically removed or handled manually .

- 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.

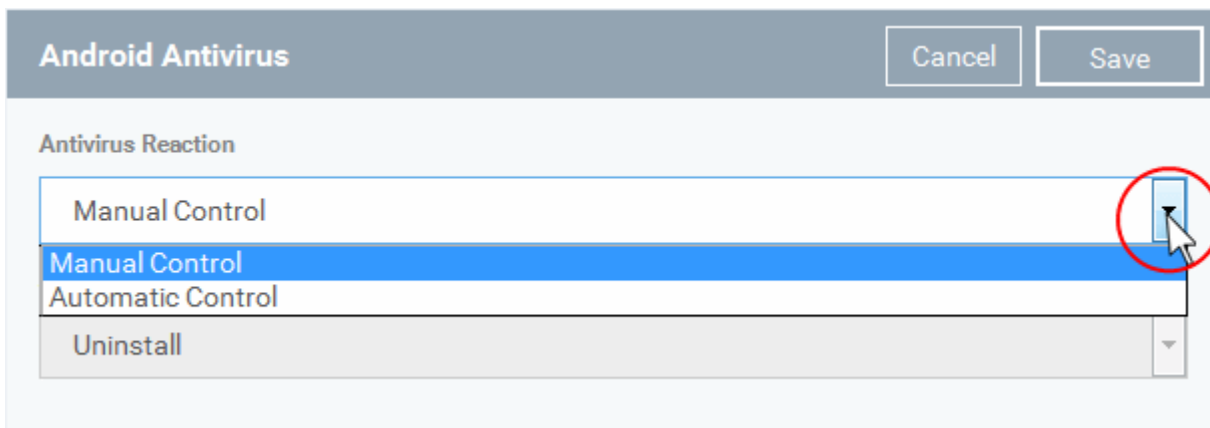
To configure antivirus settings

- Choose 'Settings' from the left and select 'Android Client Configuration'.
- Click the 'Antivirus' tab:



- Click the edit button  if you wish to modify the settings.

The settings screen will be displayed.



Android Client Antivirus Settings - Table of Parameters	
Parameter	Description
Antivirus Reaction	<p>Choose the type of action to be taken if malware is discovered on the device. The options are:</p> <ul style="list-style-type: none"> Manual control Automatic control <p>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.</p>
Automatic Action	<p>If 'Automatic control' is chosen from the 'Antivirus Reaction' drop-down, select the action to be taken on the app identified as infected by CDM. The options available are:</p> <ul style="list-style-type: none"> Uninstall Ignore

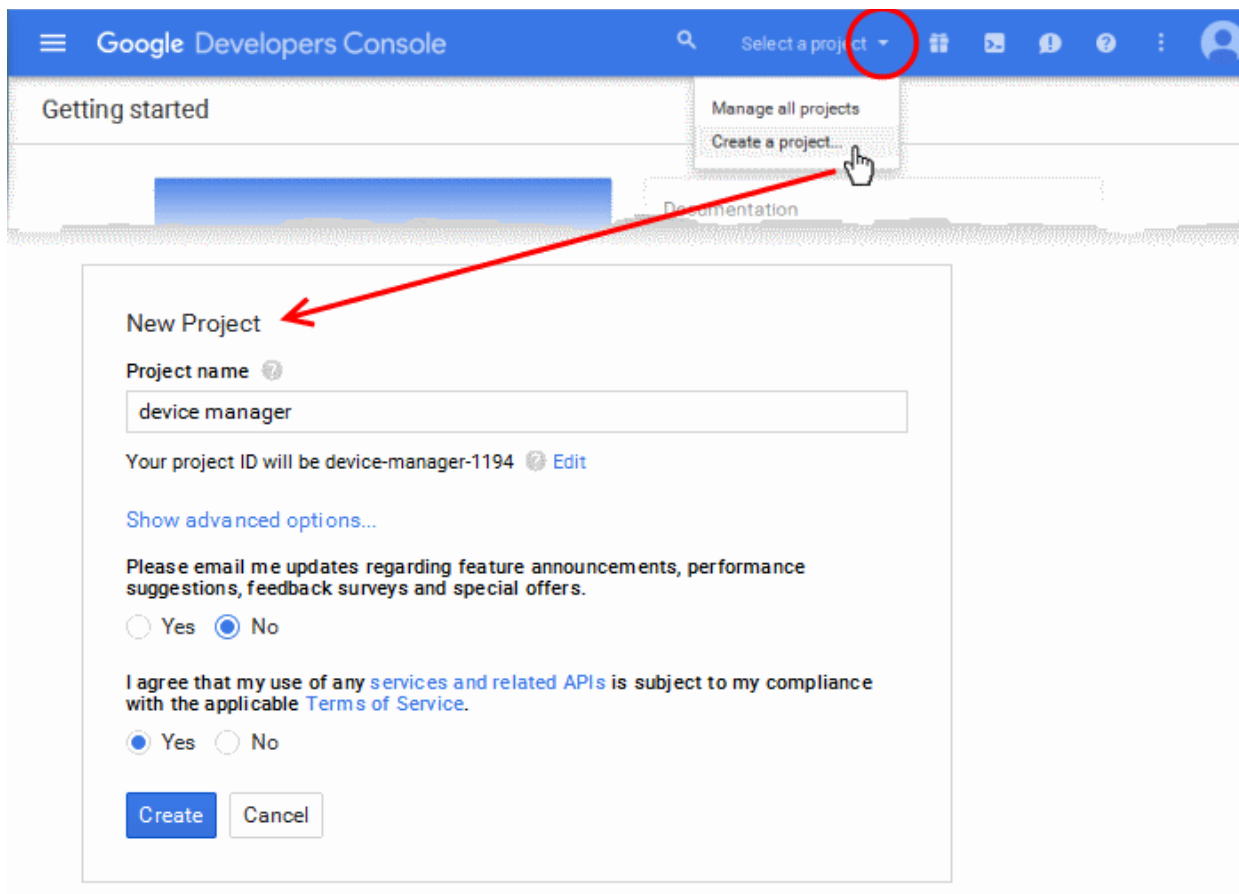
- Click 'Save' for your settings to take effect.

10.6.3. Adding Google Cloud Messaging (GCM) Token

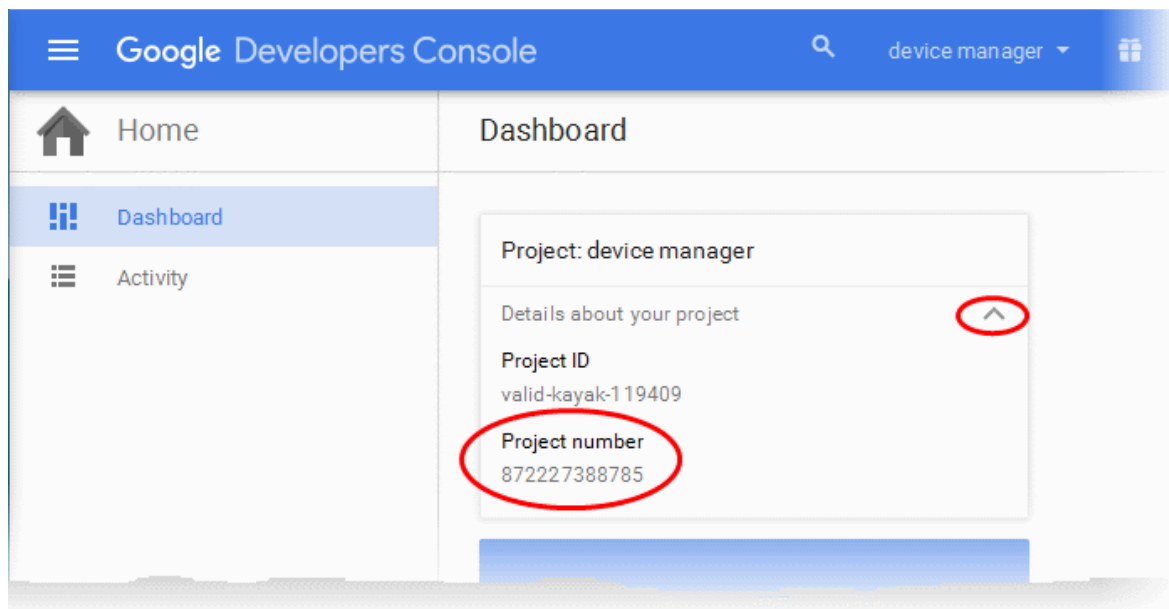
You need to obtain a Google Cloud Messaging (GCM) token in order for CDM to communicate with Android devices. To get the token, you must first create a project in the Google Developers console.

Comodo Device Manager ships with a default API token which is hard-coded and not visible in the interface. However, you can also generate a unique Android GCM token for your CDM account. To generate a GCM token, you must have created a Mobile Backend Project at <https://console.developers.google.com/>. Please follow the steps given below to create a project and upload a token.

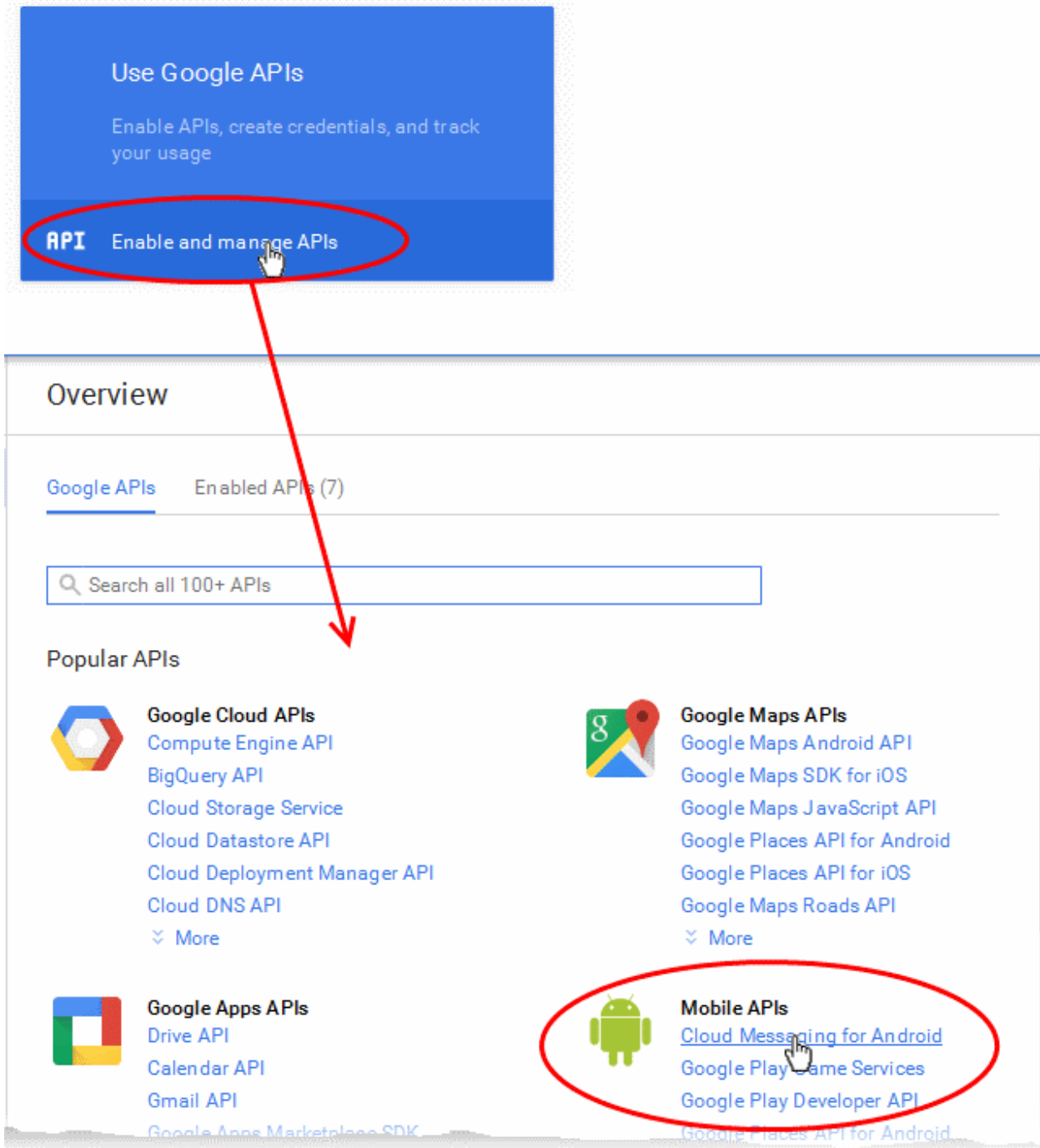
- Step 1** - Login to the Google API Console at <https://console.developers.google.com/> and choose 'Create a project' from the 'Select a project' drop-down at the top right.
 - Type a name for the project and click 'Create'. Your project ID will be auto-generated.



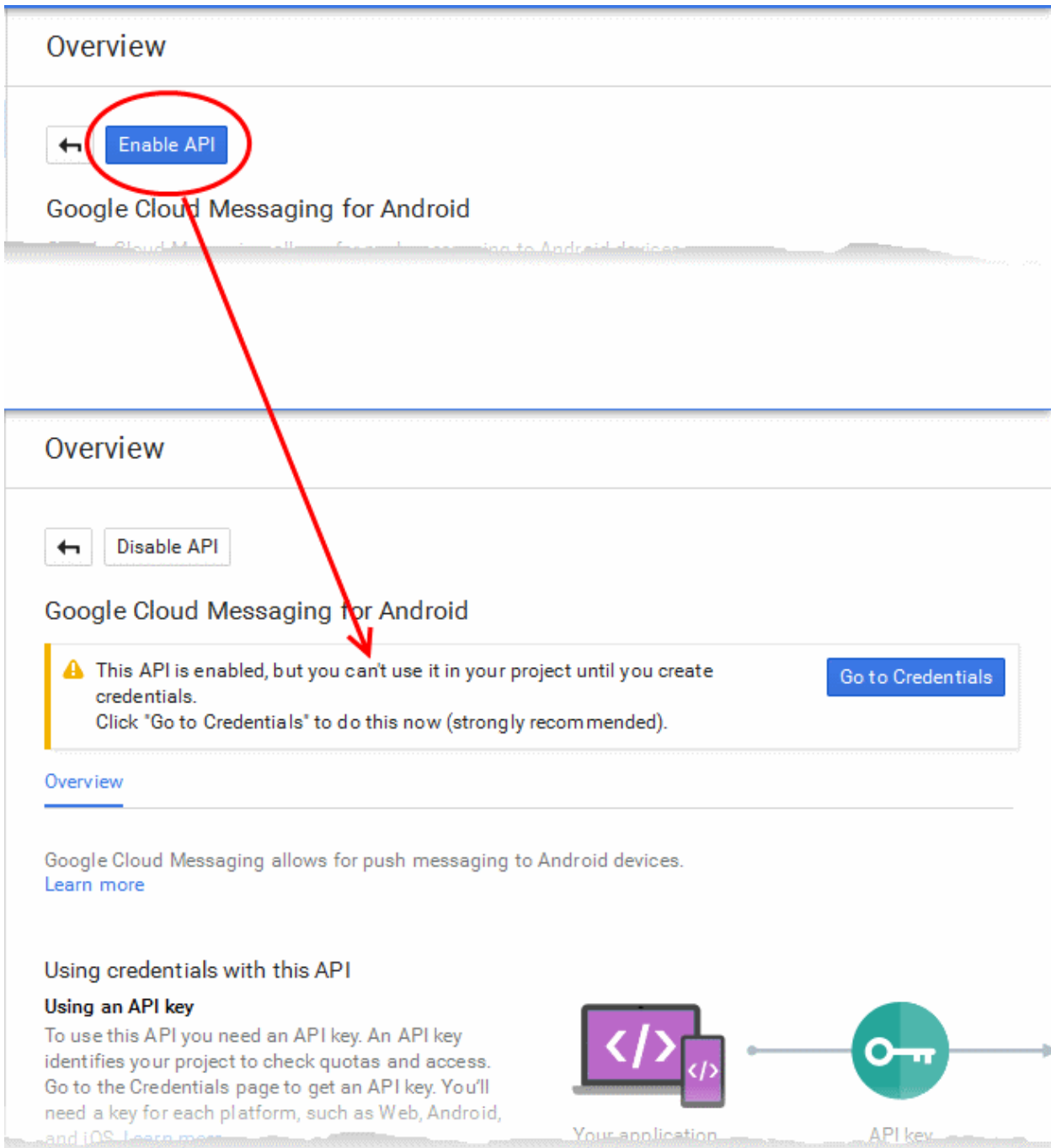
- **Step 2** - After the project is created, the Project Dashboard screen will be displayed. If not, choose the project from the 'Select a project' drop-down at the top right:



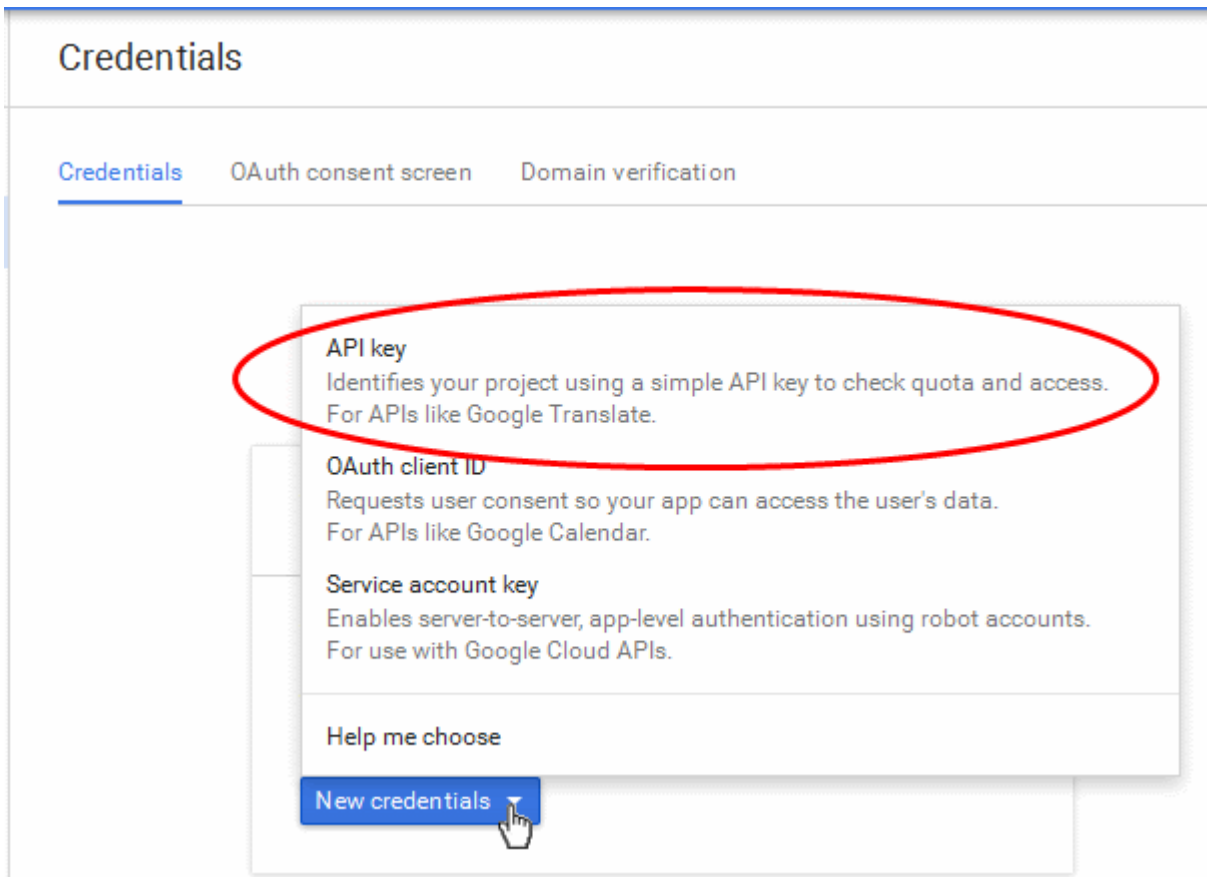
- Click the drop-down beside 'Details about your project' and note down the 'Project number'
- **Step 3** - Click 'Enable and Manage APIs' use 'Use Google APIs' from the same screen.



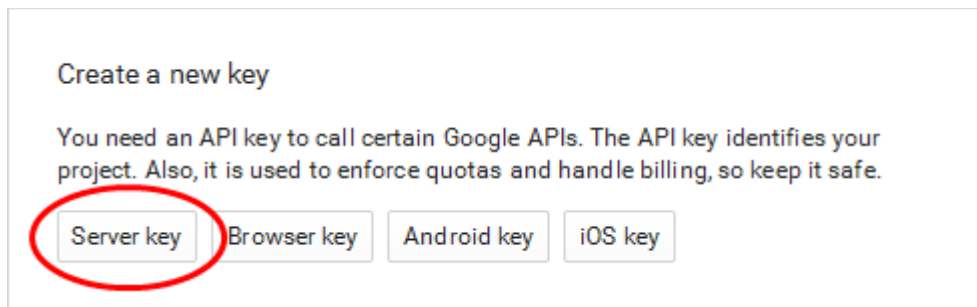
- **Step 4** - Click on "Cloud Messaging for Android" under 'Mobile APIs' in the list of available services.
 - In the next screen, ensure that the service is enabled for the project, else click the 'Enable API' at the top enable the service.



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




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



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

Credentials



Create server API key

This key should be kept secret on your server

Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request's userIp parameter, if specified. If the userIp parameter is missing, your machine's IP address will be used instead. [Learn more](#)

Name

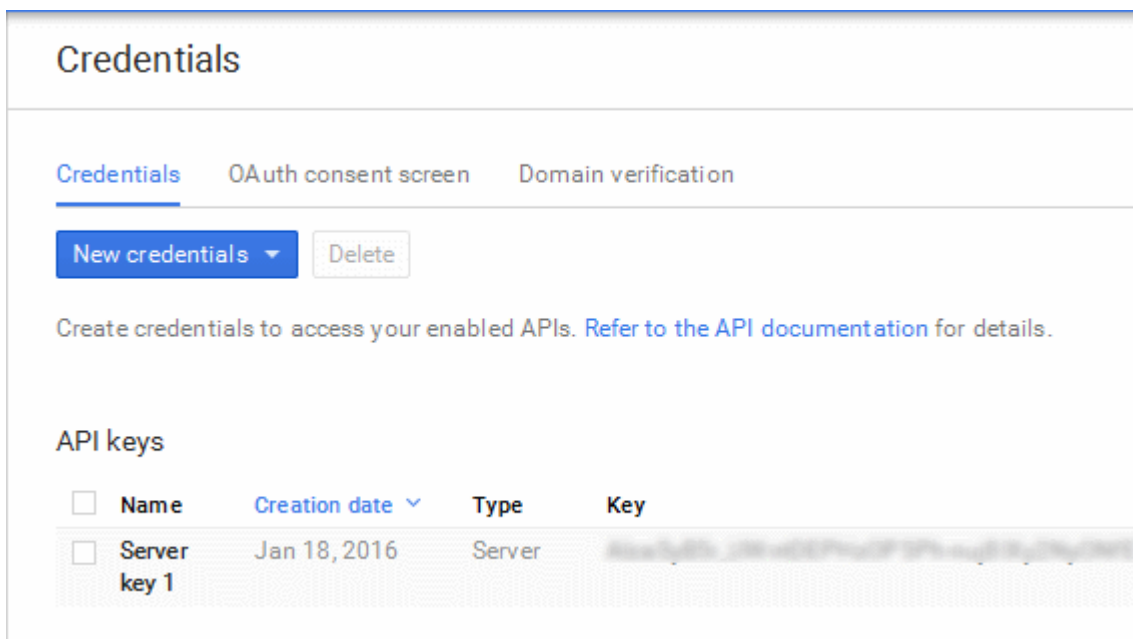
Accept requests from these server IP addresses (Optional)
Examples: 192.168.0.1, 172.16.0.0/12, 2001:db8::1 or 2001:db8::/64

Note: It may take up to 5 minutes for settings to take effect

The API Key will be generated and displayed in a pop-up.....

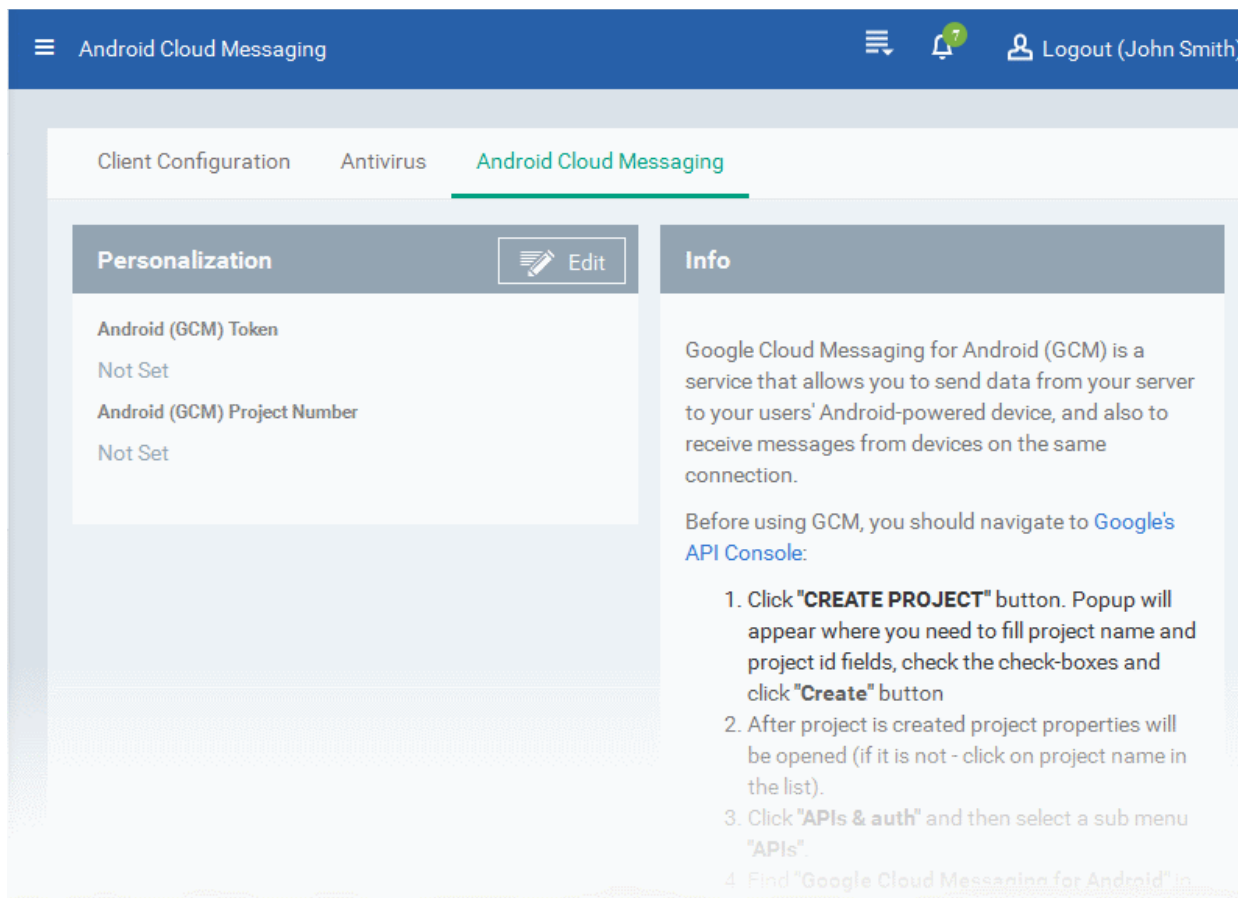


.... and under the 'Credentials' tab.

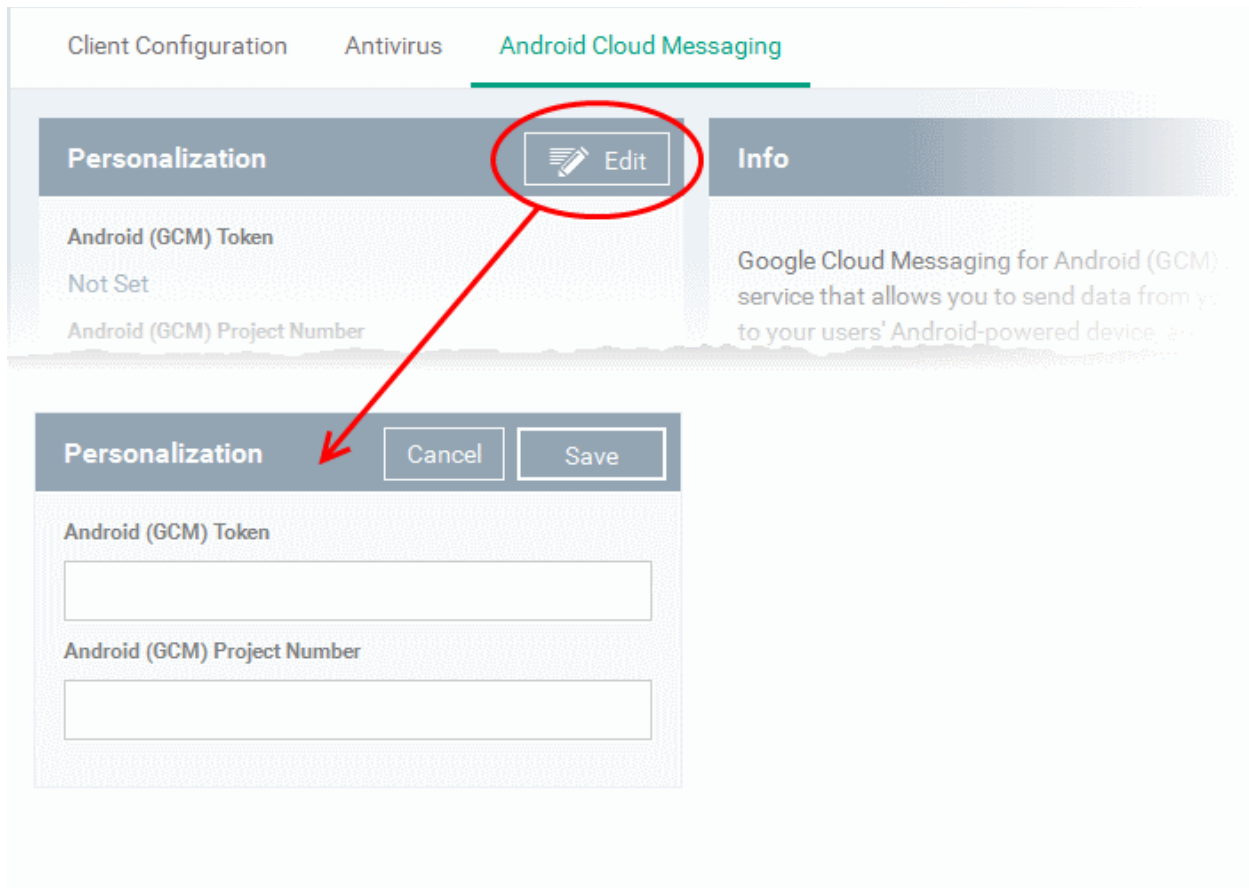


You need the API key and the project number to be entered in the CDM interface.

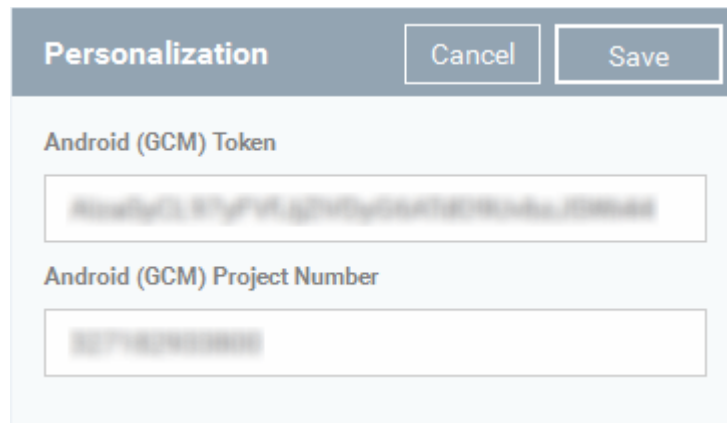
- Note down the API key in a safe place.
- **Step 9** - Next, login to CDM. Click 'Settings' > 'Android Client Configuration' and choose 'Android Cloud Messaging' tab



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

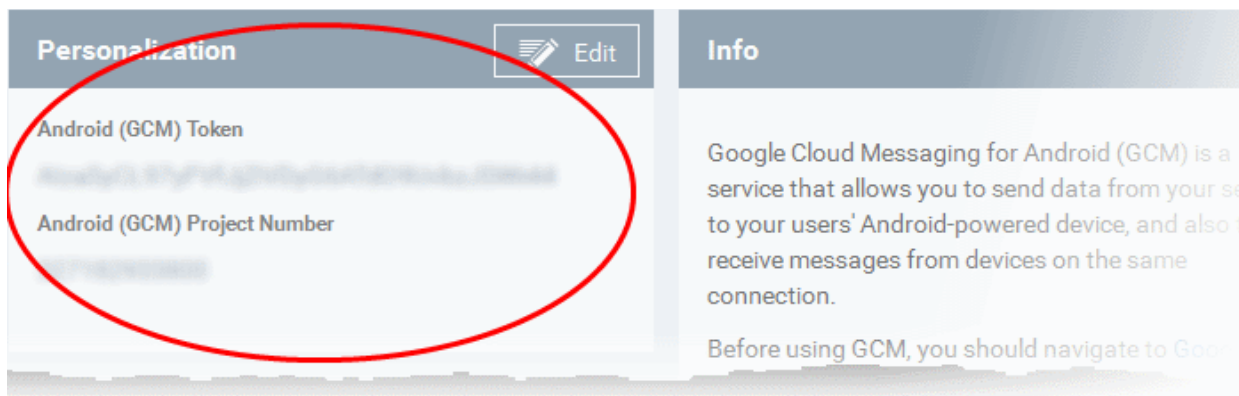


- Paste the API token to 'Android (GCM) Token' field.
- Enter the Project Number in the Android (GCM) Project Number field.



- Click 'Save'.

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



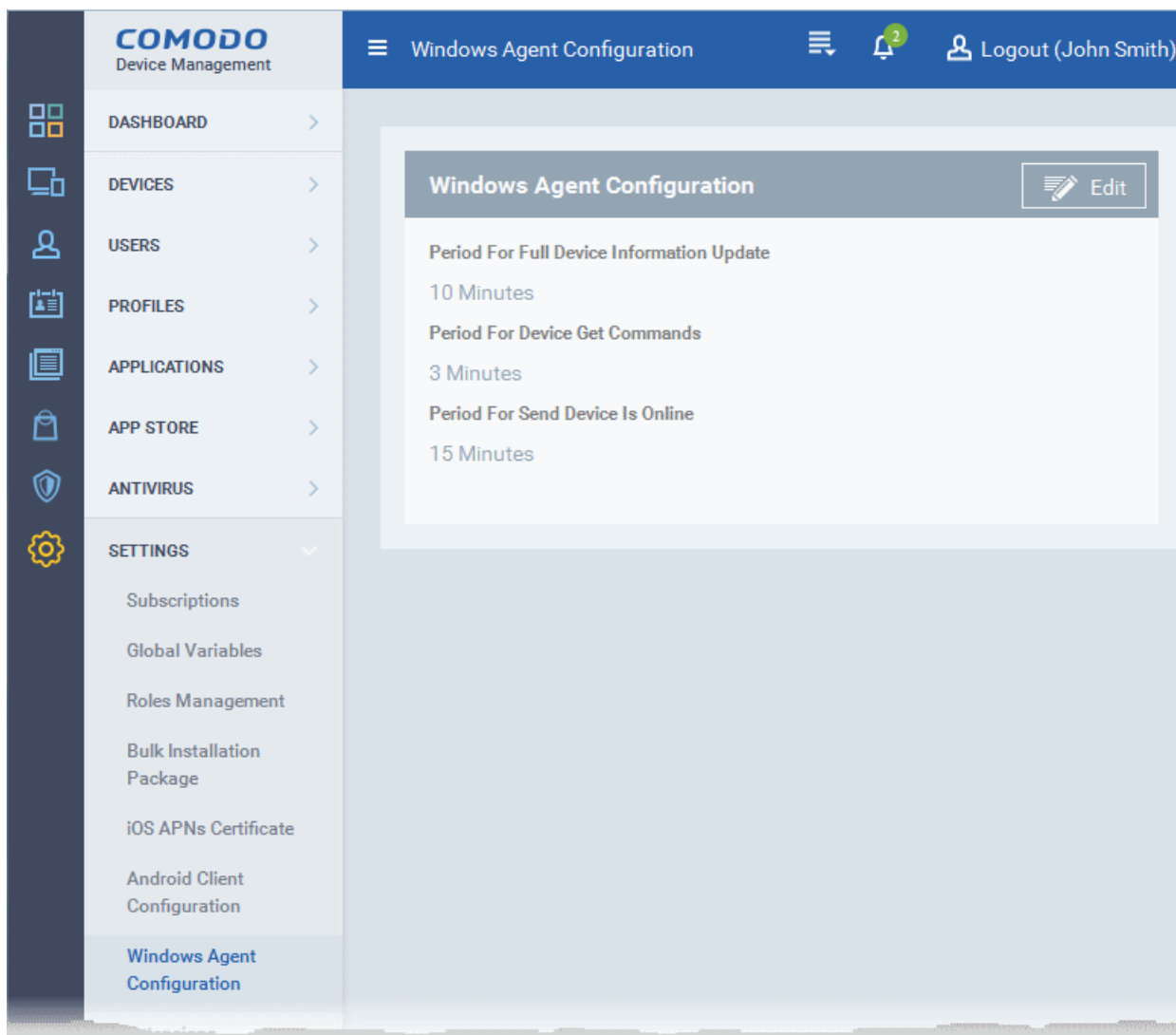
Your CDM Portal will now be able to communicate with Android devices.

10.7. Configuring CDM 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 CDM.

To configure the windows agent

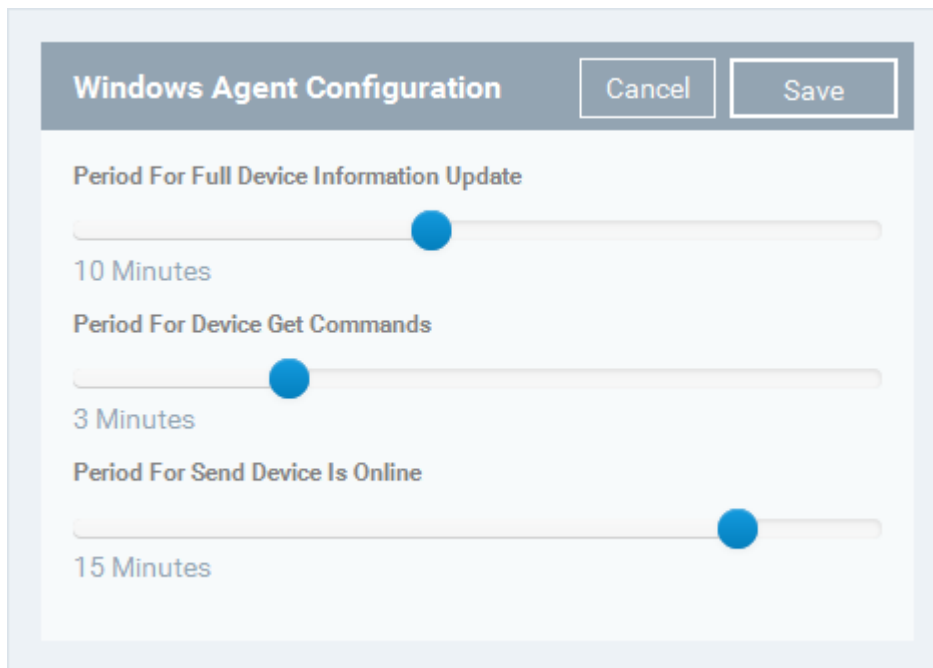
- Choose 'Settings' from the left and select 'Windows Agent Configuration'



The default values of the update intervals are displayed.

- Click the edit button  on the top right to modify these settings

The settings screen will be displayed.



Windows Agent Configuration Settings	
Parameter	Description
Period for full device information update	The update time interval for complete device information such as memory status, name of the device, OS summary, security information from the CES installation and network information. Use the slider to set the update interval. (Default = 10 minutes)
Period for Device Get Commands	The time interval at which the agent on the device should poll the CDM 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 = 3 minutes)
Period for Send Device is Online	The time period during which the agent on the device should send a message confirming that it is online and connected. If CDM 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.

10.8. Managing CDM Extensions

CDM Extensions are additional software modules which administrators can add to CDM to expand its functionality. Once added, each extension can be controlled and managed from the CDM interface. The 'Extensions Management' interface allows administrators to enable or disable modules.

The extensions available are:

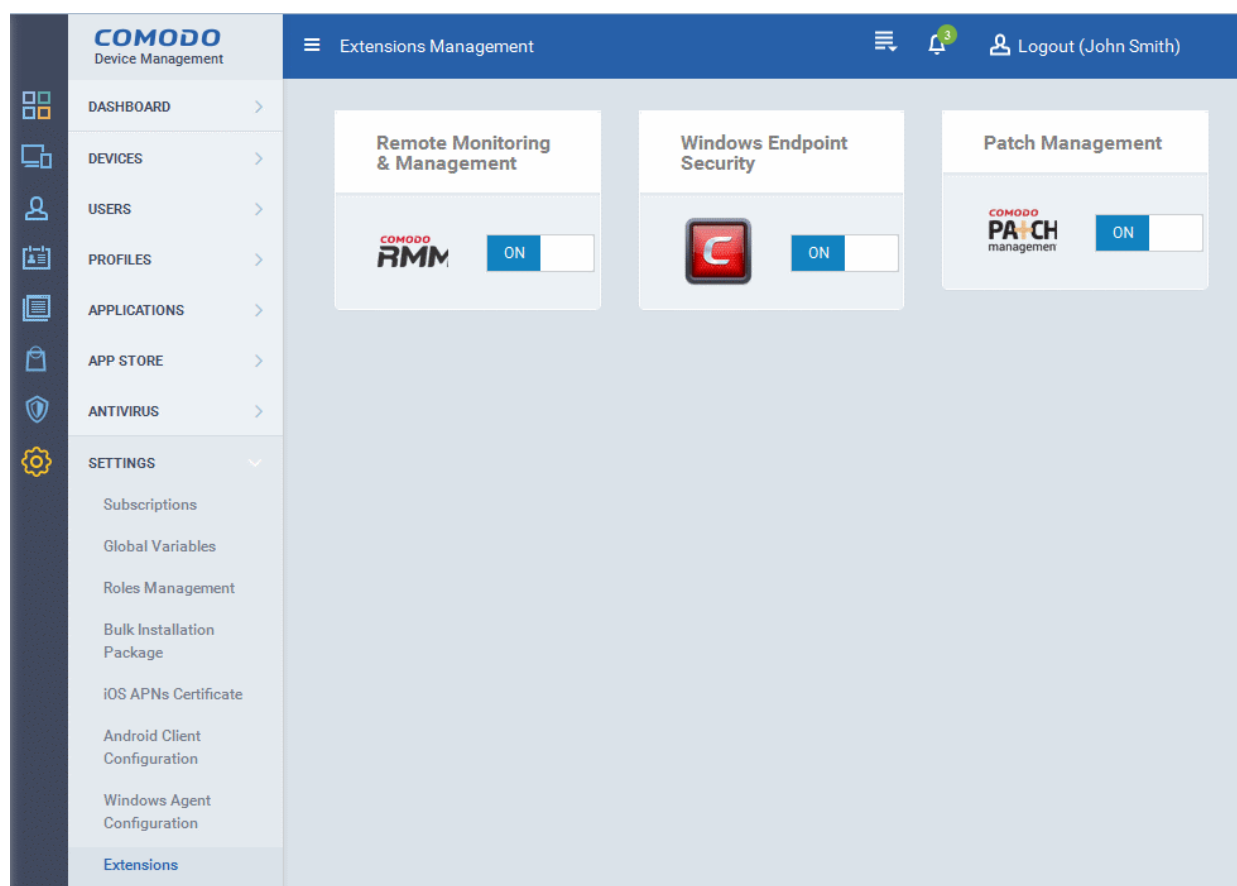
- **Remote Monitoring and Management Module** - Remote Monitoring and Management (RMM) Module is an efficient endpoint monitoring application that allows administrators to monitor and manage multiple endpoints from one centralized console. RMM requires an agent to be installed on the managed Windows endpoint. CDM allows the agent to be installed on to required endpoints from the 'Devices' interface. Refer to the section [Remotely Installing Packages onto Windows Devices](#) for more details. Once installed, the device can be monitored for software and hardware activities and managed from the 'Devices' interface. Refer to the section [Remote Management of Windows Devices](#) for more details.

Note: The RMM Module Extension is available only for Comodo One customers.

- **Comodo Endpoint Security** - Comodo Endpoint Security 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 Sandbox feature that runs unknown and unrecognized applications in an isolated environment at the endpoints. CES 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, CES can be configured for optimal security by applying configuration profiles. Refer to the section [Profiles for Windows Devices](#) for more details.
- **Patch Management Module** - The Patch Management Module provides administrators with granular control over the deployment of Windows update/security patches on managed Windows devices. You can view the patch status of devices and deploy new patches on to them from the 'Device Details' interface. Refer to the section [Viewing and Installing Windows Patches](#) for more details. Also you can view the list of available patches and install them on all applicable devices at once from Patch Management interface. Refer to the section [Installing OS Patches on Windows Endpoints](#) for more details.

To access the 'Extensions Management' interface

- Choose 'Settings' from the left and select 'Extensions'



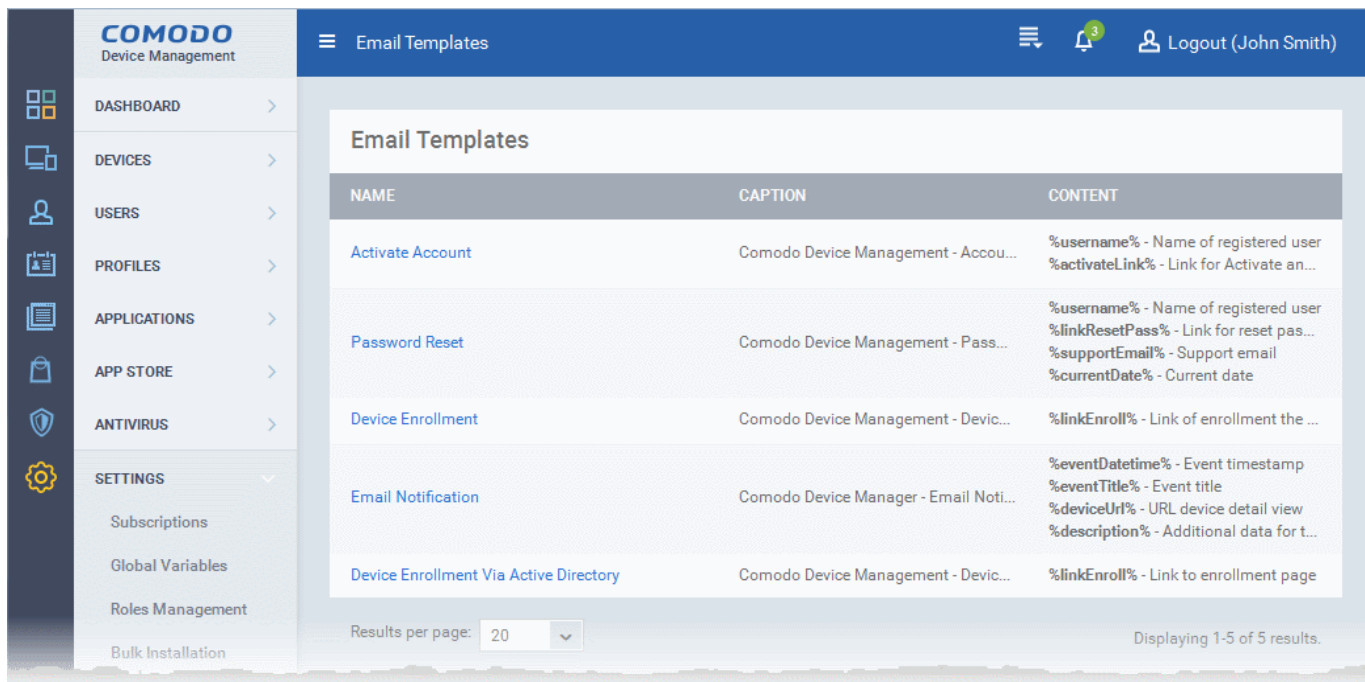
- Use the toggle switch in the respective tile to enable or disable the extensions

10.9. Configuring Email Templates

CDM sends five types of automated notification emails to end-users for user account activation, device enrollment, password reset and so on, using predefined templates. The administrator can customize the templates according to the organizational requirements, for example, editing email subject and content, inserting appropriate variables and so on.

The 'Email Templates' interface allows the administrator to view the templates and edit them.

- To open the 'Email Templates' interface, choose 'Settings' from the left and select 'Email Templates'.

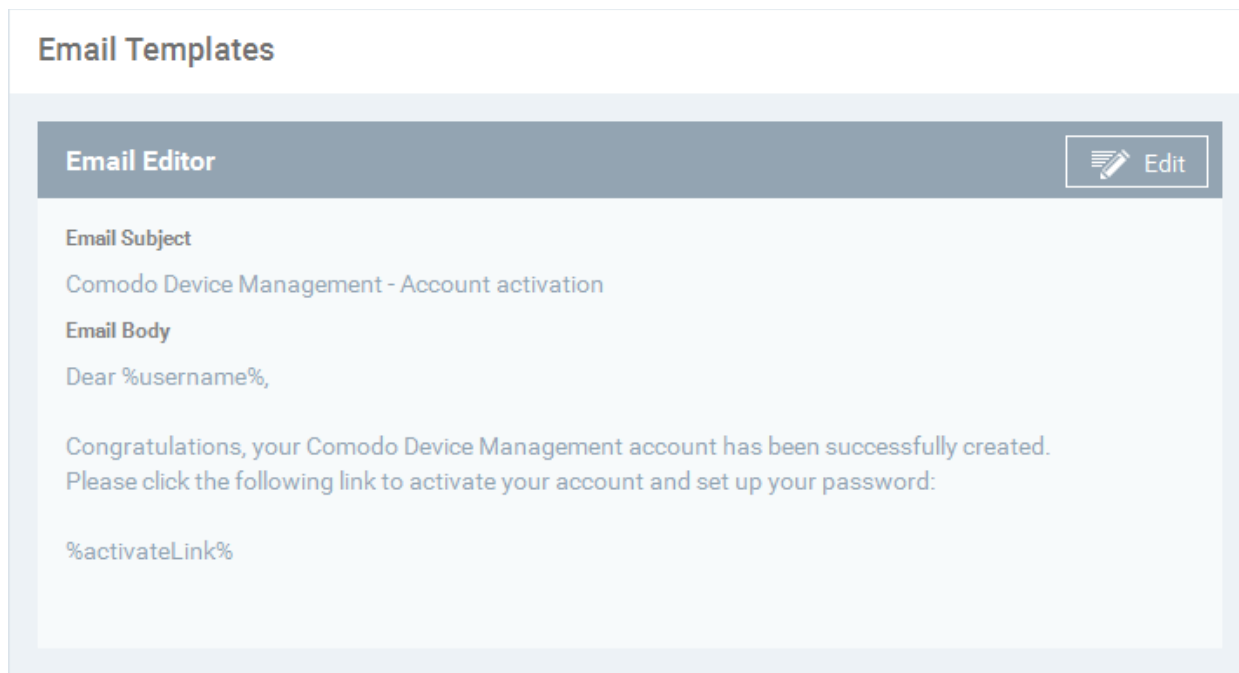



Email Templates- Column Descriptions	
Column Heading	Description
Name	Indicates the name of email template. This cannot be edited.
Caption	Displays the subject line of the email.
Content	Displays the variables contained in the email, with their values. These cannot be edited.

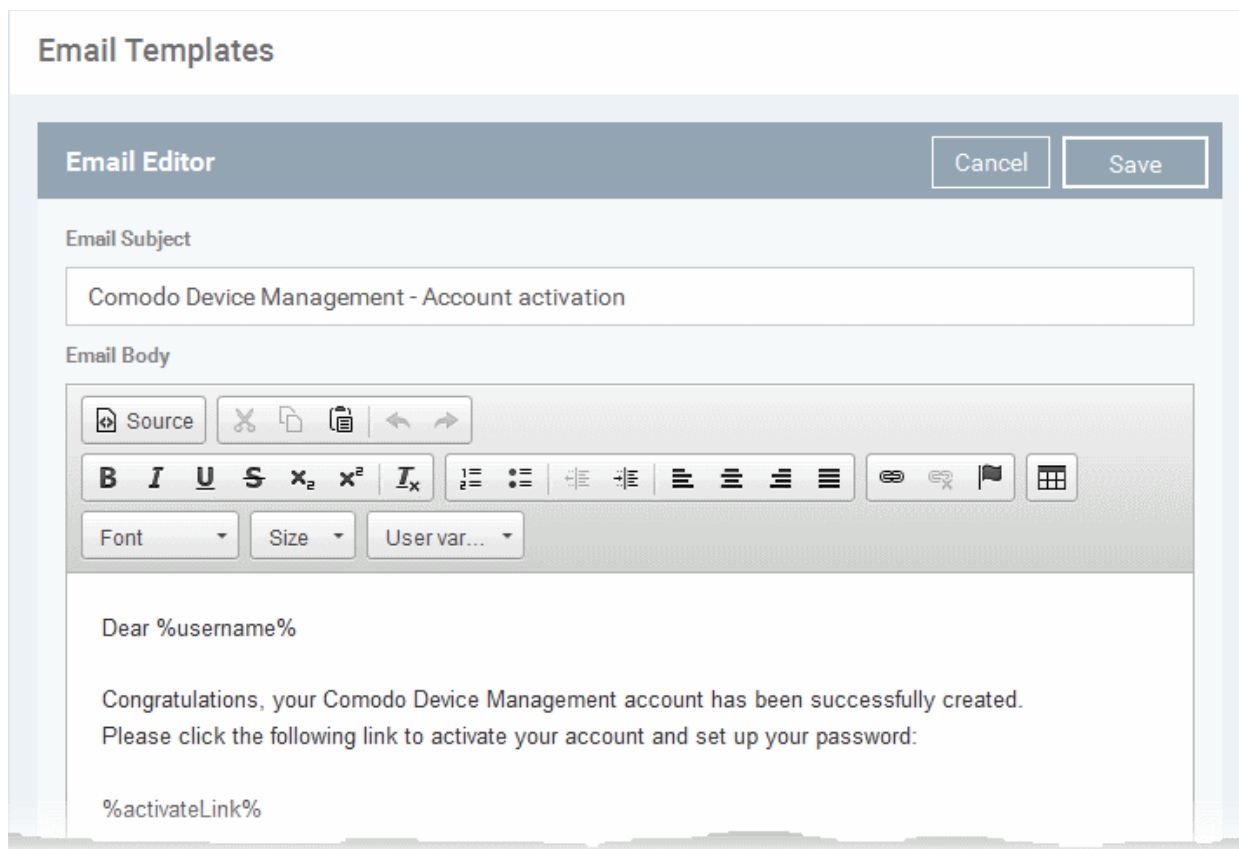
To edit an email template

- Choose 'Settings' from the left and select 'Email Templates'.
- 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 'Account Activation' link, the following template editor will be displayed with the message.



- To edit the subject line and the message, click the edit button  on the top right. The Editor window will open.



- Edit the subject line and email content of the template per your requirements and insert the variables available in the toolbar wherever required.

Note: For each type of email template, appropriate variables will be available in the toolbar. Make sure not to change the variable name as these will not work at all or fetch wrong values.

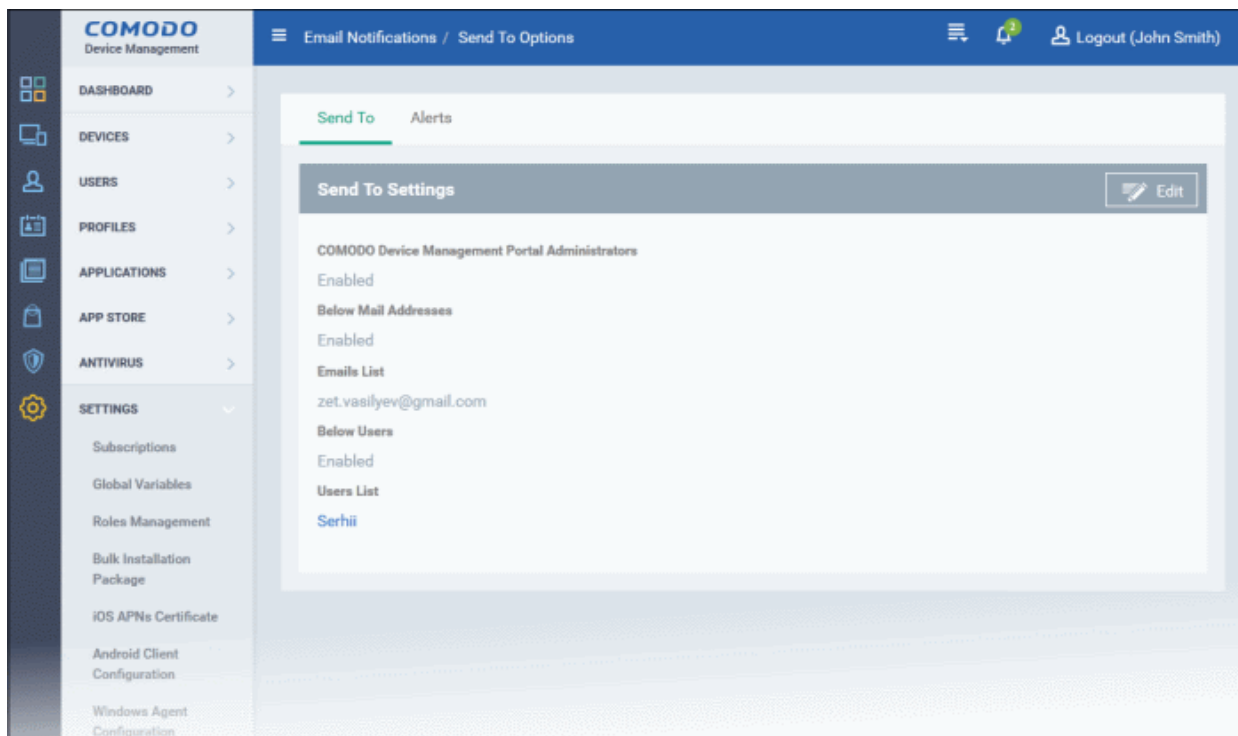
- Click the 'Save' button for your changes to take effect.

10.10. Configuring Email Notifications

CDM can be configured to send alert emails to administrators and users if a new infection is detected and / or if a iOS device is removed.

- To open the 'Email Notifications' screen, click 'Settings' from the left and choose 'Email Notifications'.

By default, the 'Email Notifications / Send to Options' screen will be displayed.

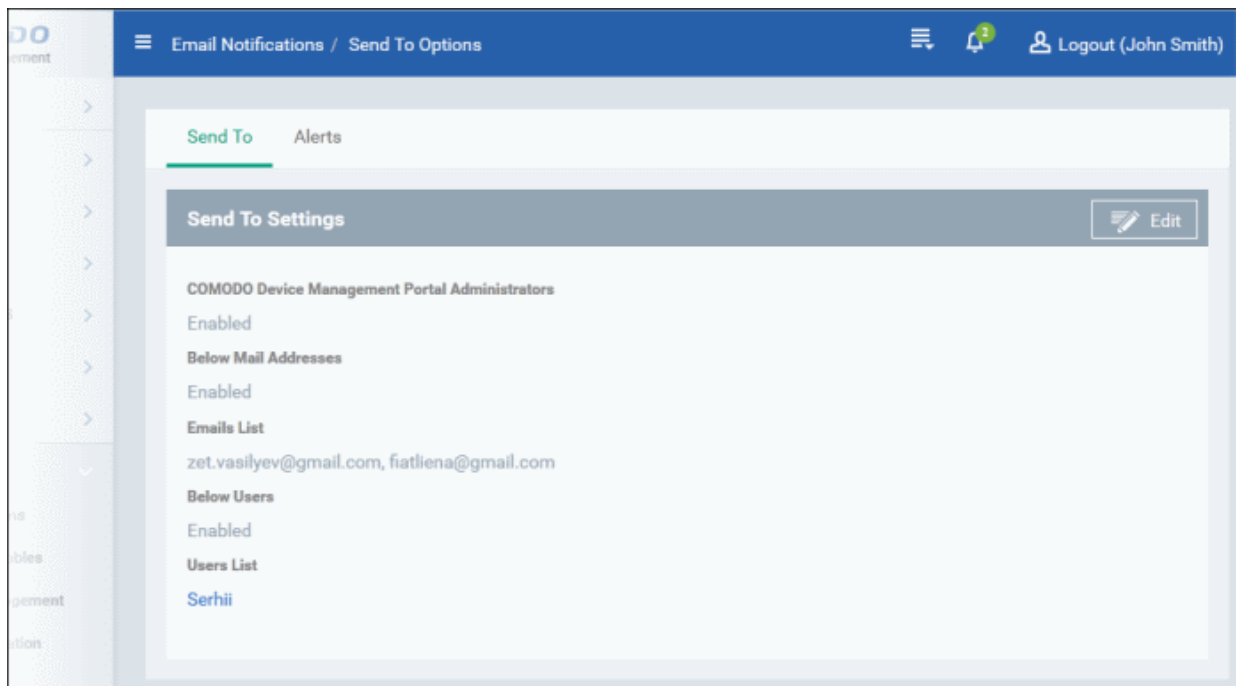


- Send To - Allows to configure the alert recipients email addresses
- Alerts - Allows to configure the type of alert for which the email notifications will be sent

To configure email alert recipients

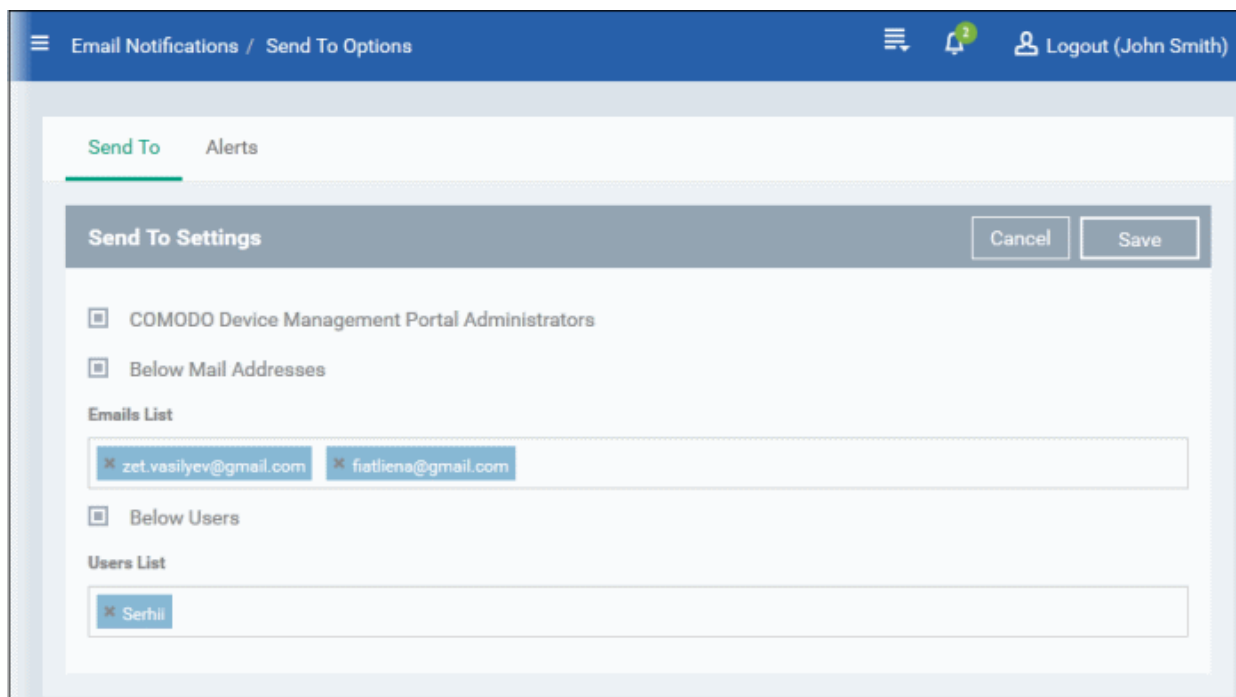
- Click 'Send To'

The 'Send to Options' screen will be displayed.

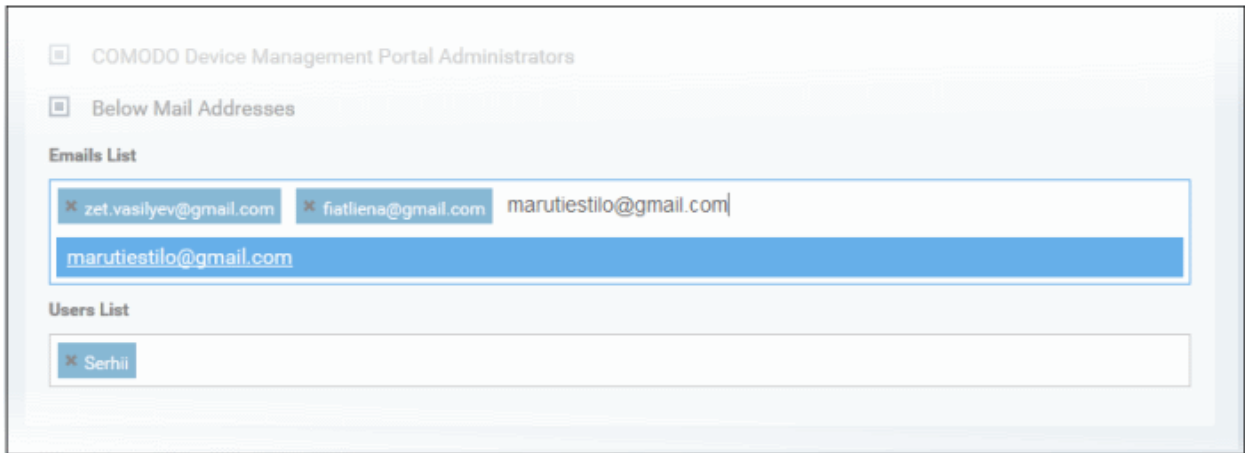


- **Comodo Devices Management Portal Administrators** - If enabled, the alerts will be sent to all CDM administrators
- **Below Mail Addresses** - If enabled, the alerts will be sent to recipients whose addresses are added under 'Emails List'
- **Emails List** - Allows to add or remove email recipients from the list
- **Below Users** - If enabled, the alerts will be sent the CDM users that are added under 'Users List'
- **User List** - Allows to add or remove CDM users from the list

Click the 'Edit' button at the top right to add new recipients and / or edit the current details



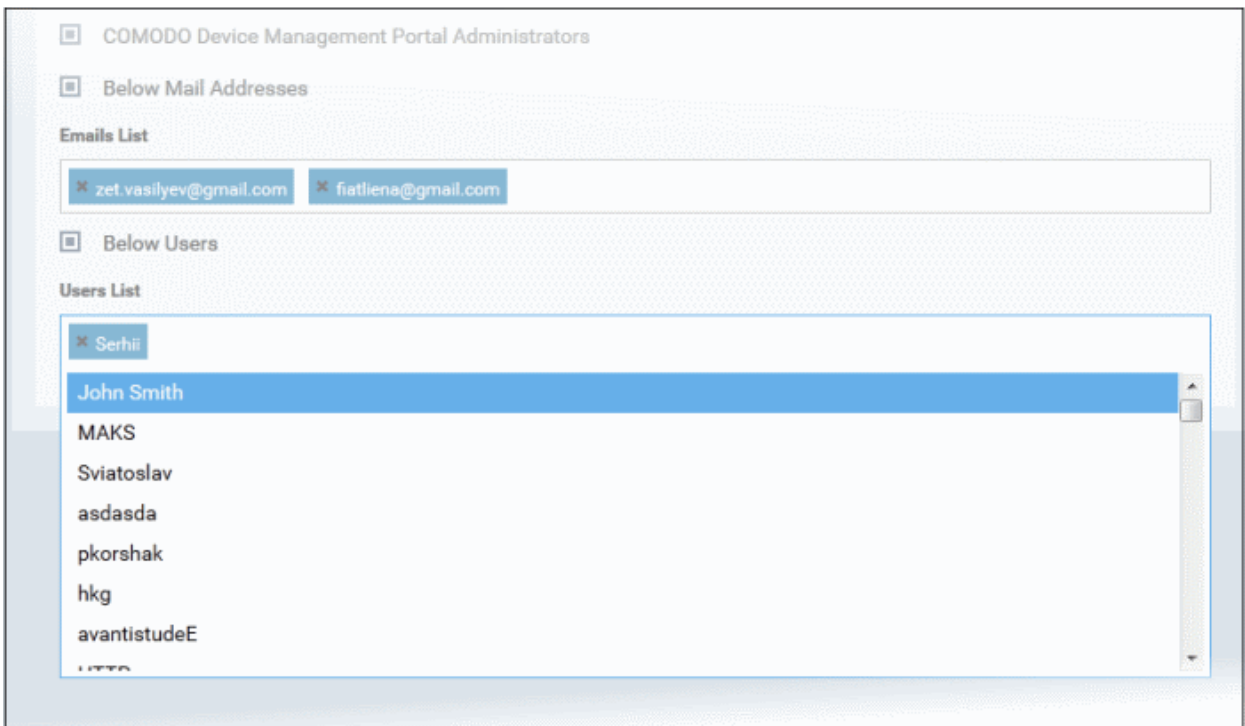
- To add recipients under 'Emails List', type the email address in the field and click the 'Enter' key or click the address that appear below the field.



Please note the 'Below Mail Addresses' check box should be enabled for the alerts to be sent.

- To add CDM users as recipients, click in the 'Users List' field

The available CDM users will be listed.



- Select the users from the list

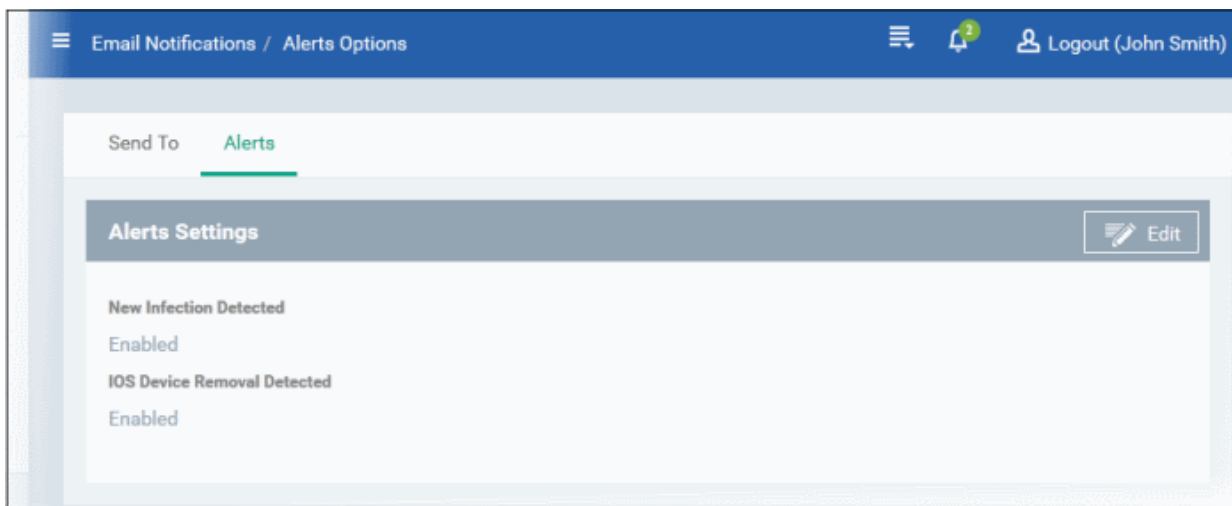
Please note the 'Below Users' check box should be enabled for the alerts to be sent to the users.

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

To configure alert settings

- Click 'Alerts'

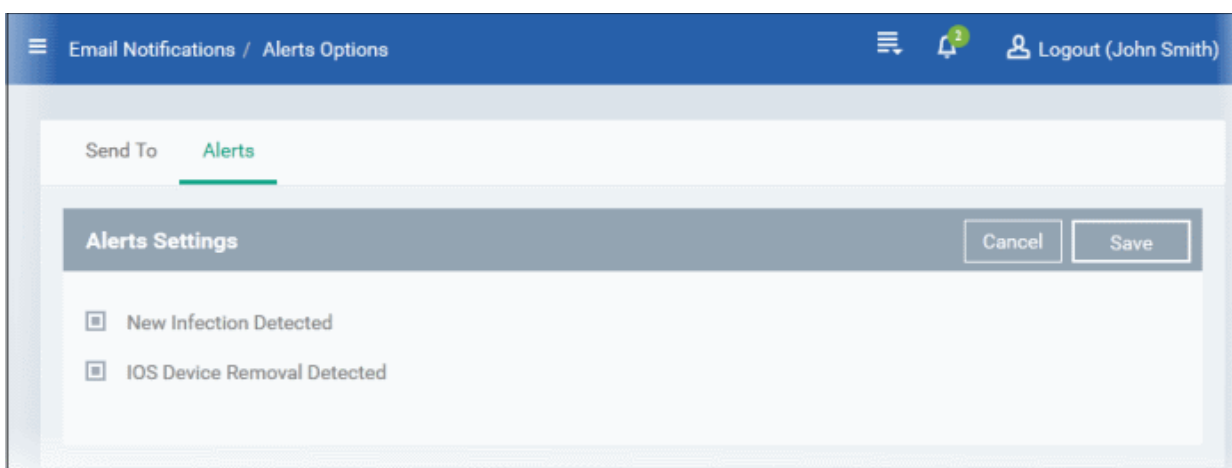
The 'Alert Options' screen will be displayed.



The list of events for which the alerts will be sent to configured recipients will be displayed.

- **New Infection Detected** - If enabled, an alert will be sent if a new malware is detected by CDM
- **iOS Device Removal Detected** - If enabled, an alert will be sent if an iOS device is removed from CDM

Click the 'Edit' button at the top right to enable/disable the type of alert



- Select / deselect the check boxes besides the alerts to enable / disable them
- Click the 'Save' button for the changes to take effect

10.11. Configuring CDM Reports

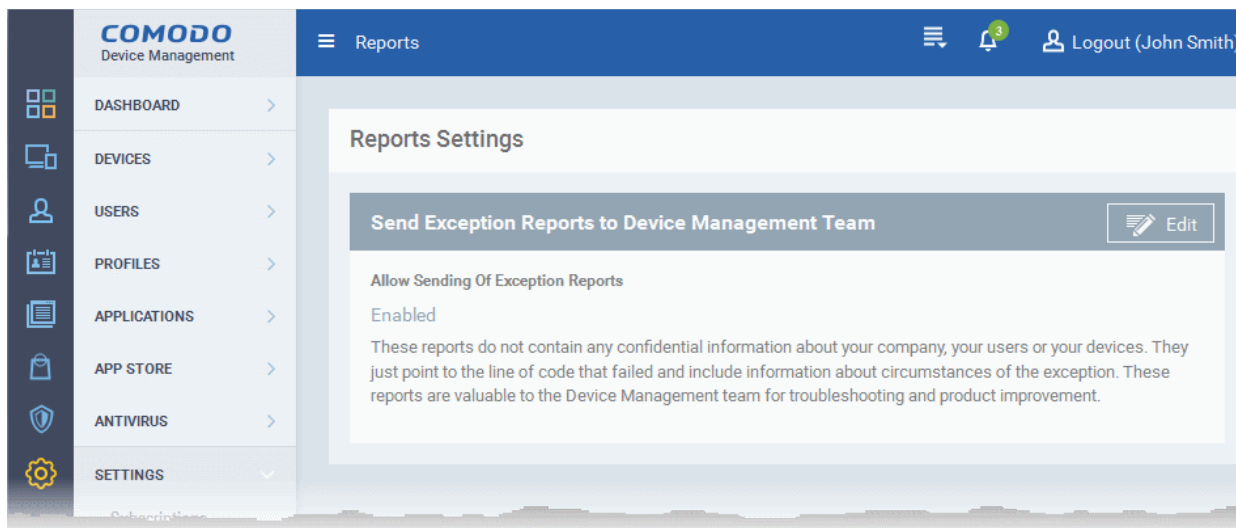
CDM undergoes rigorous Quality Assurance testing before release to ensure that the software is as stable and reliable as possible. However, in rare situations, CDM may run into an exception which needs to be addressed. If this setting is enabled, an exception report will automatically be sent to Comodo if CDM 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.

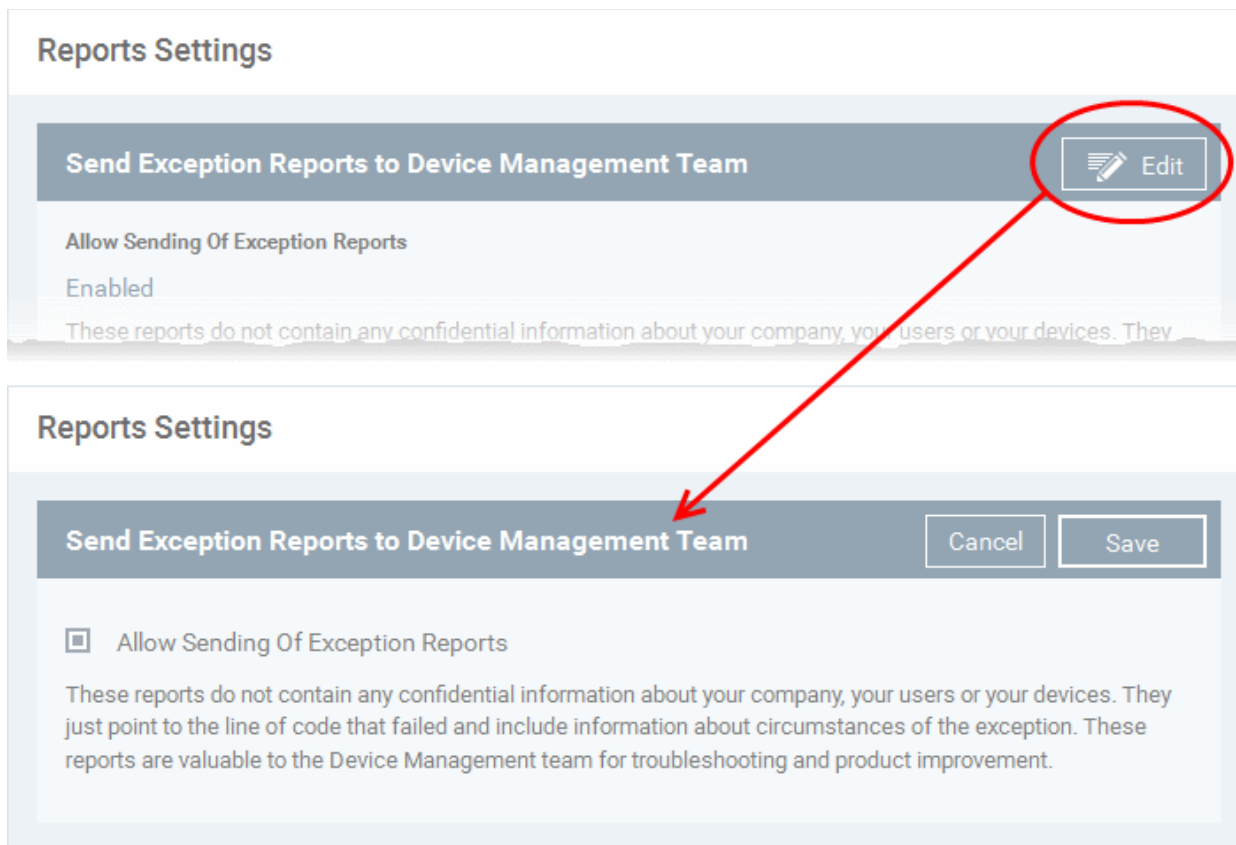
These reports contain only the line of code that failed with additional information about the circumstances of the exception. They do not contain any private information about your company or your users.

The 'Reports' interface allows you to enable or disable automated sending of exception reports.

- To open the Reports interface, choose 'Settings' from the left and select 'Reports'.



- To edit the settings click the edit button  from the top right.

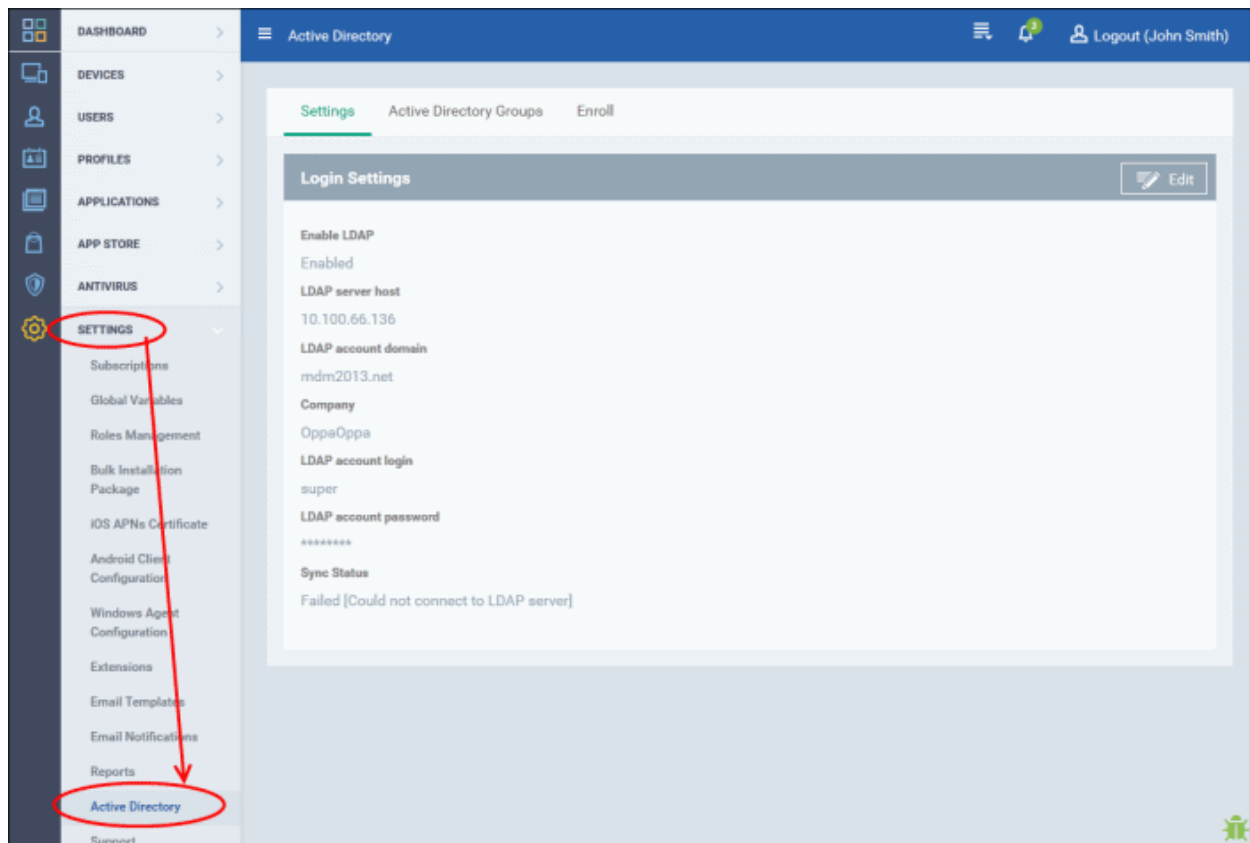


- Select the 'Allow sending of exception reports' allow the CDM to send the error reports to 'Comodo'.
- Click 'Save' for your settings to take effect.

10.12. Importing User Groups from LDAP

In addition to adding user groups manually, CDM enables administrators to import user groups from Active Directory (AD). You can configure CDM to access your AD server through the Lightweight Directory Access Protocol (LDAP) to import the user groups.

- Click the 'Settings' link on the left, then 'Active Directory' to configure importing users from active directory



- **Settings** - Allows to configure the LDAP server details
- **Active Directory Groups** - Allows to sync with the configured LDAP server and import user groups
- **Enroll** - Allows to configure whether user groups should be imported along with their devices

Settings

- Click the 'Settings' tab and then the 'Edit' button at the top right to configure the LDAP server details

LDAP Server Settings	
Parameter	Description
Enable LDAP	Select the check box to enable importing user groups from LDAP server
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	<ul style="list-style-type: none"> Comodo One (C1) customers - Select the company from the drop-down Stand-alone CDM customers - Select 'Default Company' from the drop-down
LDAP account password	Enter the password for the LDAP account
Sync status	Displays the latest status of LDAP synchronization that was initiated from the Active Directory Groups tab

- Click the 'Save' button for the changes to take effect

The next step is to initiate synchronization of the LDAP server for importing user groups, which can be done in the **Active Directory Groups** tab.

Active Directory Groups

After configuring the LDAP server settings as explained **above**, you can start importing the user groups. Click the 'Active Directory Groups' tab.

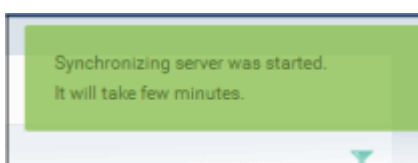


- **Sync with LDAP Server** - Allows to connect with the configured LDAP server to import user groups
- **Change LDAP Roles** - Allows to assign roles for the users in the groups

To import user groups from the LDAP server

- Click 'Sync with LDAP Server'

The synchronization process will start and a message will be displayed.



After the process is completed, the imported user groups will be displayed with no roles assigned to them.

The screenshot shows the 'Active Directory Groups' section after synchronization. The table now contains the following data:


GROUP NAME	#USER COUNT	IMPORT DATE	ASSIGNED ROLE
Domain Computers	1	28 Sep, 2015	Select role
Schema Admins	1	28 Sep, 2015	Select role
Domain Admins	1	28 Sep, 2015	Select role
Administrators	1	28 Sep, 2015	Select role
Pre-Windows 2000 Compatible ...	1	28 Sep, 2015	Select role
Network Configuration Operators	0	28 Sep, 2015	Select role
Remote Desktop Users	0	28 Sep, 2015	Select role
Print Operators	0	28 Sep, 2015	Select role
\\S_IUSRS	0	28 Sep, 2015	Select role

Imported User Groups List from LDAP - Column Descriptions

Column Heading	Description
Group name	The name of the imported user group from the LDAP server. User groups that have at least one user in them will be displayed in blue text. Clicking the name of a group will open the 'Active Directory Groups' details interface that displays the list of users included in the group and allows you to add or remove users to/from the group. Refer to the section ' Viewing the Details of a User ' for more details.
# User Count	Displays the number of users in the group.
Import Date	The date at which the user group was imported to CDM from the LDAP server

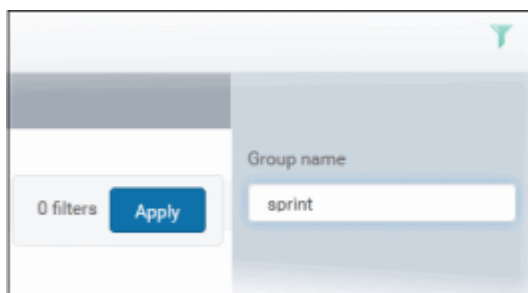
Assigned Role	By default, the imported users in the group will be assigned the default role . Click 'Select role' link beside a group or select a group and click 'Change LDAP Roles' at the top to assign a role. Refer to ' To assign role for the imported users ' for more details.
---------------	---

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 group name, enter the search criteria in part or full 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 CDM 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 assign role for the imported users

By default, users in the group that are imported will have no roles assigned to them. To assign a role for the users, click the 'Select role' for the group or select the group(s) and click 'Change LDAP Roles' > 'Assign Selected Role'

--	--

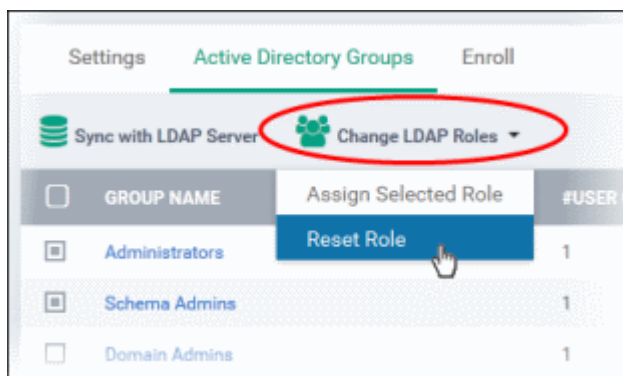
The 'Assign Role' dialog for the selected group(s) will be displayed:



- Select the roles from the 'Assign Roles' drop-down and click the 'Assign' button.

The selected role will be assigned to the users in the group. For more details about roles, refer to the section '[Configuring Role Based Access Control for Users](#)'.

- To remove the roles assigned to users, select the group(s) and click 'Reset Role' from the 'Change LDAP Roles' drop-down. The users will be automatically be assigned the **default role** after resetting.



Enroll

The 'Enroll' screen allows administrators to configure whether devices should be also be enrolled along with the users and send enroll emails.

- Click the 'Enroll' tab, then click 'Edit' at the top right

- **Add users but don't add their devices automatically** - If selected, users in the groups will not be able to enroll their devices. To do so, the users will have to first login into the application using their LDAP credentials (this will add them to CDM) and administrators will have to send enrollment email for the users from User's page. On successful enrollment, the users will be available in the respective group imported from LDAP.

If the 'Add users but don't add their devices automatically' checkbox is deselected, administrators can choose not to send any enrollment mails, to send enrollment mails to all or enter users' email addresses / alias email addresses, each address separated by a comma. However, the users will not be added into their respective group unless they authenticate themselves with their LDAP credentials in the page after clicking the second link in the enrollment mail.

- Click the 'Save' button.

The 'The settings were saved and applied successfully' info will be displayed and mails sent to users automatically as per the selection.

The user groups imported into CDM and can be viewed by clicking Users > User groups. The users will be added into their respective group only after they authenticate themselves with their LDAP credentials in the page after clicking the second link in the enrollment mail.

Refer to the section '[Managing User Groups](#)' for more details on User Groups.

Refer to the section '[Managing Users](#)' for more details on Users.

10.13. Viewing Version and Support Information

The 'Support' panel displays support contact information, the current product version number, and contains a list of platforms supported by this version of CDM.

- To open the 'Support' pane, choose 'Settings' from the left and select 'Support'.

The screenshot shows the 'Support' page in the Comodo Device Manager interface. The page is structured as follows:

- Contact Information:**
 - Support Telephones:
 - US: +1.703.637.9361
 - US Enterprise: +1.973.396.1235
 - US MSP: +1.973.396.1232
 - International: +1.888.256.2608
 - FREE
 - Support email: cdmsupport@comodo.com
 - Online Support: support.comodo.com
Please register to submit tickets
 - Enterprise Forum: forum1.comodo.com/forum/comodo-device-management
 - MSP forum: forum.mspconsortium.com/forum/products/other-comodo-products/comodo-device-management
- Supported Device Platforms:**
 - Android:
 - 4.x
 - 4.x (KNOX)
 - 5.x
 - 5.x (KNOX)
 - iOS:
 - 7.x
 - 8.x
 - Windows (Workstation edition)
 - Windows XP (SP3 or higher) x86
 - Windows 7 x86
 - Windows 7 x64
 - Windows 8 x86
 - Windows 8 x64
 - Windows 8.1 x86
 - Windows 8.1 x64
 - Windows 10 x86
 - Windows 10 x64
 - Windows (Server edition)
 - Windows 2008 Server R2
 - Windows 2012 Server R2
- Summary Details:**
 - Server Version: 5.0.1461.7790

- **Contact Information** - Displays the telephone numbers and email addresses for contacting Comodo for purchasing new licenses and contacting product support.
- **Supported Device Platforms** - Displays the list of types of devices that can be managed by CDM, with their supported OS versions.
- **Summary Details** - Displays the version number of CDM server.

About Comodo

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

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

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: EnterpriseSolutions@Comodo.com

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