COMODO
Creating Trust Online®

# Comodo
# Endpoint Manager

Software Version 6.32

# Administrator Guide

Guide Version 6.32.010620

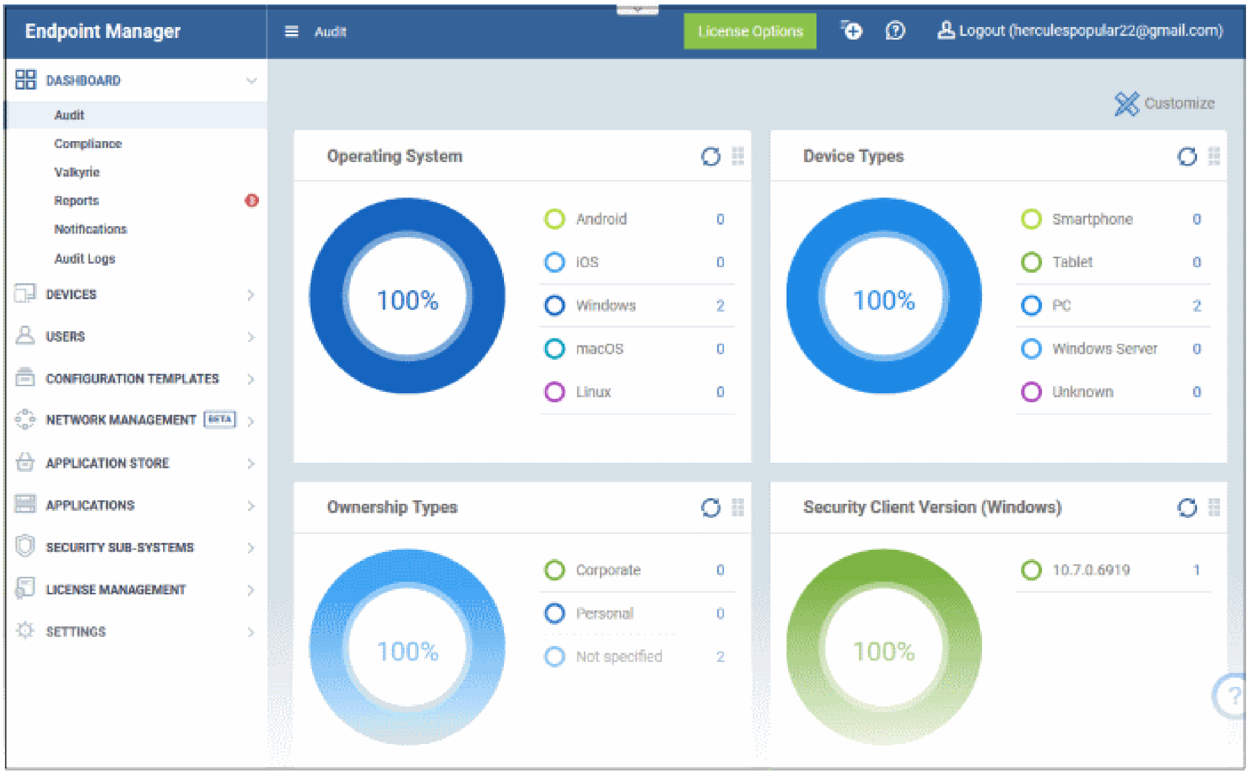
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

# Table of Contents

# 1. Introduction to Endpoint Manager

Endpoint Manager (EM) lets you manage, monitor and secure devices which connect to your network.

- Admins must first add users to EM then enroll devices/endpoints for those users. Supported operating systems include Android, iOS, Mac OS, Windows and Linux.
- Once a device has been added, admins can apply profiles which determine the device's network access rights, security settings and other features.
- Each license covers one device per user. You will need additional licenses for each device you add for a user.



## Guide Structure

This guide will take you through the configuration and use of Endpoint Manager and is broken down into the following sections:

**Introduction to Endpoint Manager** - High level overview of the service which introduces the features and concepts that are discussed later in the guide.

**The Administrative Console**

**The Dashboard**

**Users and User Groups**

- **Manage Users**
  - **Create New User Accounts**
  - **Enroll Users Devices for Management**
  - **View Details of a User**
  - **Assign Configuration Profile(s) to Users' Devices**
  - **Remove a User**
- **Manage User Groups**

## 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. Endpoint 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.

**User** - An employee or guest of the enterprise whose device(s) are managed by the EM 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 admin-defined grouping of Android, iOS, Linux, MAC or Windows devices. Configuration profiles applied to a device group will be deployed to all devices in the group.

**Quarantine** - Malware found on managed networks can either be deleted or isolated in a secure environment known as 'quarantine'. Files moved to quarantine are encrypted so they cannot be executed. Admins can review quarantined items and delete or release the files. Quarantined files can also be added to the local whitelist and submitted to Comodo as a potential false-positive.

**Configuration Profile** - A configuration profile is a collection of settings applied to managed devices which determines their network access rights, overall security policy, antivirus scan schedule, and other preferences. Profiles are operating system specific and can be applied to individual devices, device groups, users or user groups. Endpoint Manager ships with a 'default' profile for each supported operating system (iOS, Android, MAC, Linux and Windows). The default profile is automatically applied to a user/device ***if*** no custom profile exists.

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

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

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

**Communication Client (a.k.a EM Agent)** - The communication client (CC) is an agent which needs to be installed on all devices so they can be managed by Endpoint Manager. The client is responsible for receiving and executing tasks. Tasks include implementing configuration profiles, fetching device details, running antivirus scans, adding or removing apps and wiping the device.

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

**Notifications** - Notifications are generated if a threat is found on a device, or if an app is installed or removed. You can choose to send notifications to admins only, to a mailing list, or to specific users. Threat notifications are also shown in the Endpoint Manager dashboard.

**Patch Management** - The patch management module lets you monitor and install updates for Windows and 3rd party software on Windows devices.

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

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

## 1.2. Best Practices

1. 'Default' profiles are automatically applied to a device if no custom profile exists for the device. Endpoint Manager ships with default profiles for each supported operating system, but you can also mark any custom profile as 'default' if you wish.

   See **Manage 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. You can apply multiple profiles 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. Adding or removing a profile from a device would let you quickly troubleshoot if a particular setting is causing issues.

   See **Create Configuration Profiles** for more details.

3. Each license allows you to enroll one mobile device or one Windows / Mac / Linux endpoint for a single user. You will need additional licenses for each device you add for a user. We encourage admins to evaluate the average number of devices per user and to set max. enrollments accordingly.

   See **Enroll Users' Devices for Management** for more details.

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

   See **Manage Device Groups** for more details.

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

   See **Profiles for Android Devices** and **Profiles for iOS Devices** for more details.
7. Keeps an eye on the apps you allow in your organization. Apps can be useful and productive to your employees but some may pose a malware or data-leak risk for your organization. EM 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. You can also remotely uninstall unwanted applications from Windows devices.

   See **Applications** 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. EM 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. You can create custom roles for users which determine their permissions within Endpoint Manager. See **Configure the Role-Based Access Control for Users** for more details.
10. Keep on top of your devices. Check device status regularly for compliance with deployed profiles, and take advantage of Endpoint Manager's detailed reporting system. See **The Dashboard** and **Manage Devices** and **Security Dashboards** or more details.

## 1.3. Quick Start

**Click here** to view the Endpoint Manager quick-start guide.

## 1.4. Login into the Admin Console

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

- Comodo Dragon and Comodo One customers:
- Login to your Comodo Dragon or Comodo One account
- Click 'Applications' > 'Endpoint Manager'.

Note. Endpoint Manager admins created in Endpoint Manager itself can login directly to the EM console:

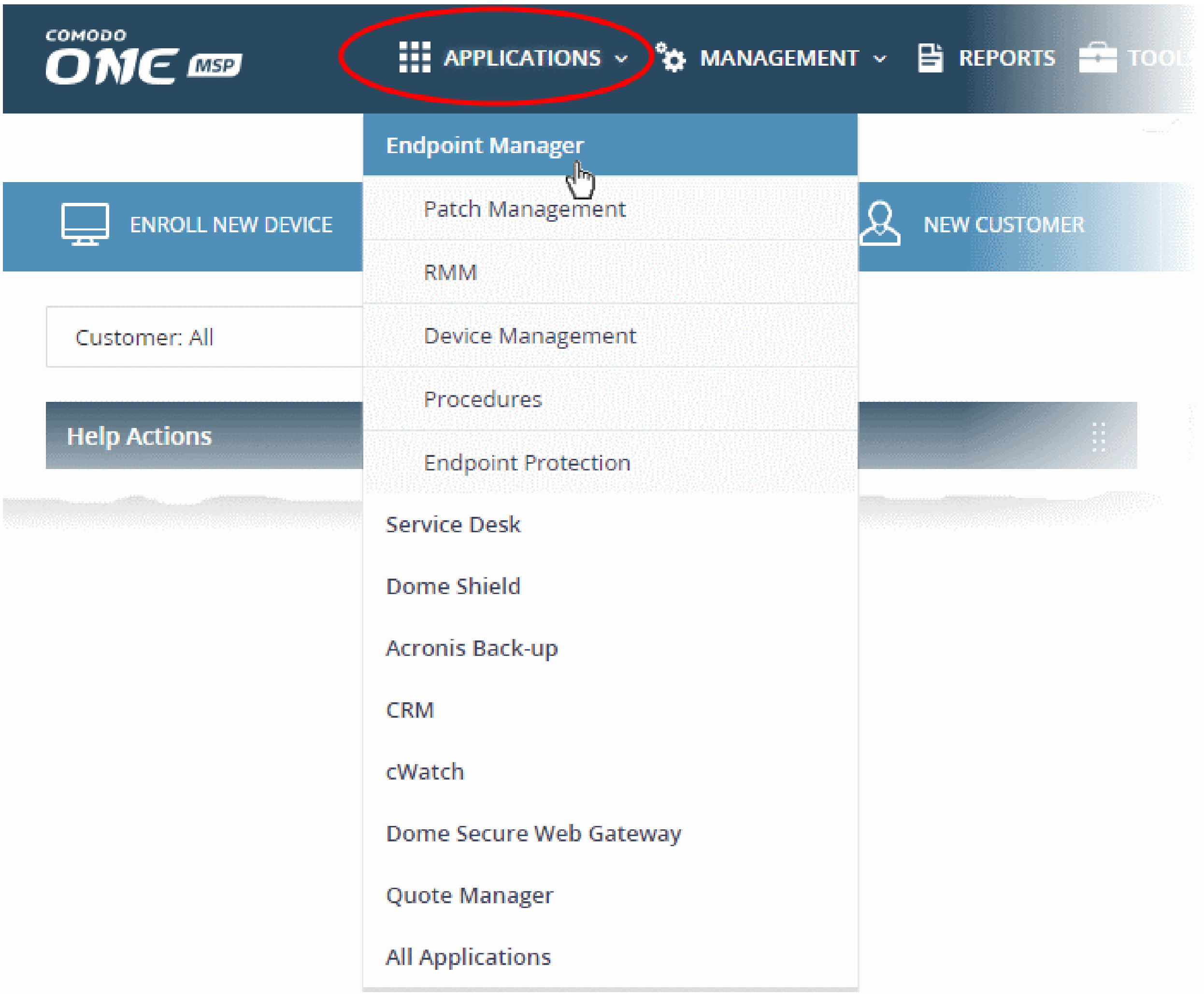
- MSP account - Login at https://<your company name>-msp.cmdm.comodo.com/user/site/login
- Enterprise account - Login at https://<your company name>.cmdm.comodo.com/user/site/login

**Endpoint Manager standalone customers:**

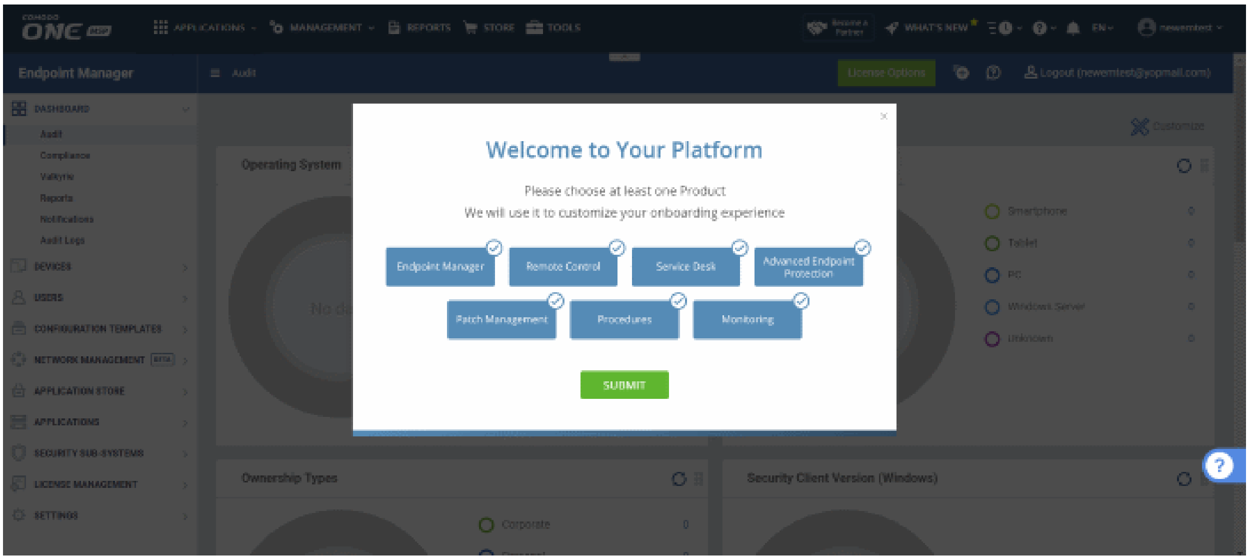
- Login at: https://<your company name>.cmdm.comodo.com/user/site/login
  - Where <your company name> is your Endpoint Manager company name.
- We sent you this URL in your account confirmation email.

Usernames and passwords are case sensitive. Please make sure that you use the correct case and caps lock is OFF.

Click 'I forgot my password' if you can't recall your password. A mail will be sent to your registered email with a link to reset your password.



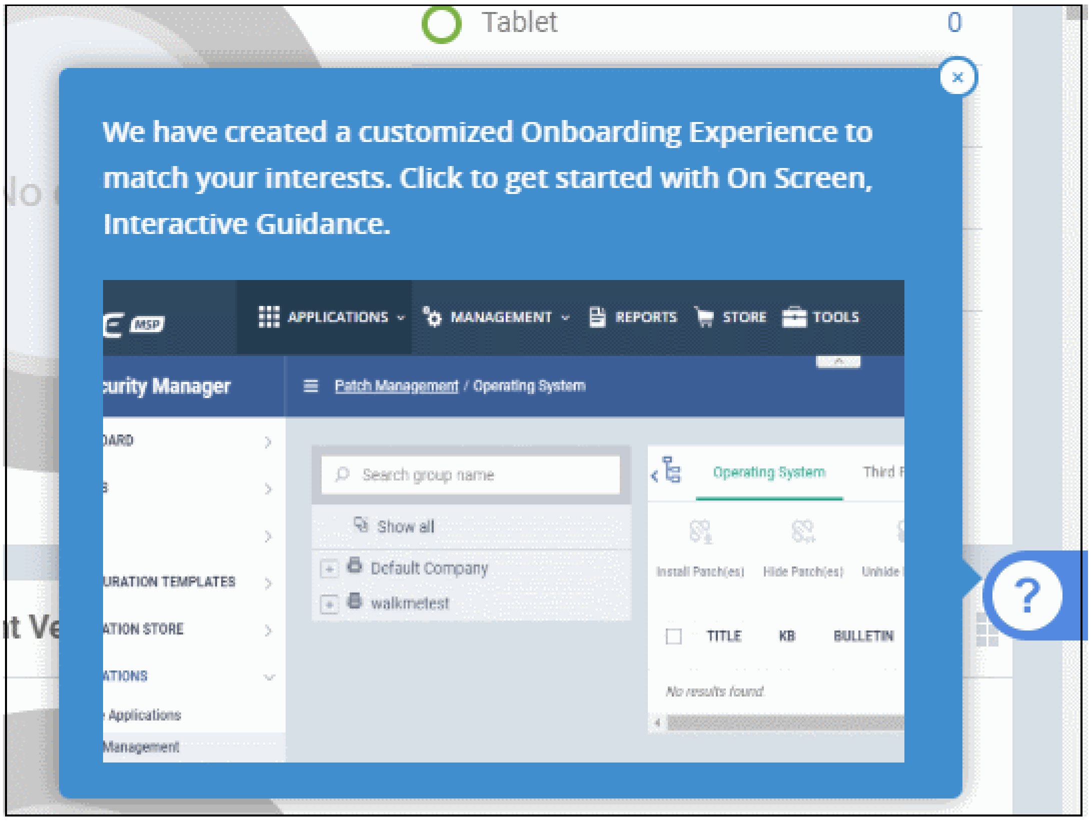
The EM welcome screen is shown after logging-in:


Welcome to Your Platform

Please choose at least one Product

We will use it to customize your onboarding experience

- Select the product that you want help with and click 'Submit'
- Interactive guides - Click the help icon at bottom-right to view walk-through tutorials on common tasks:

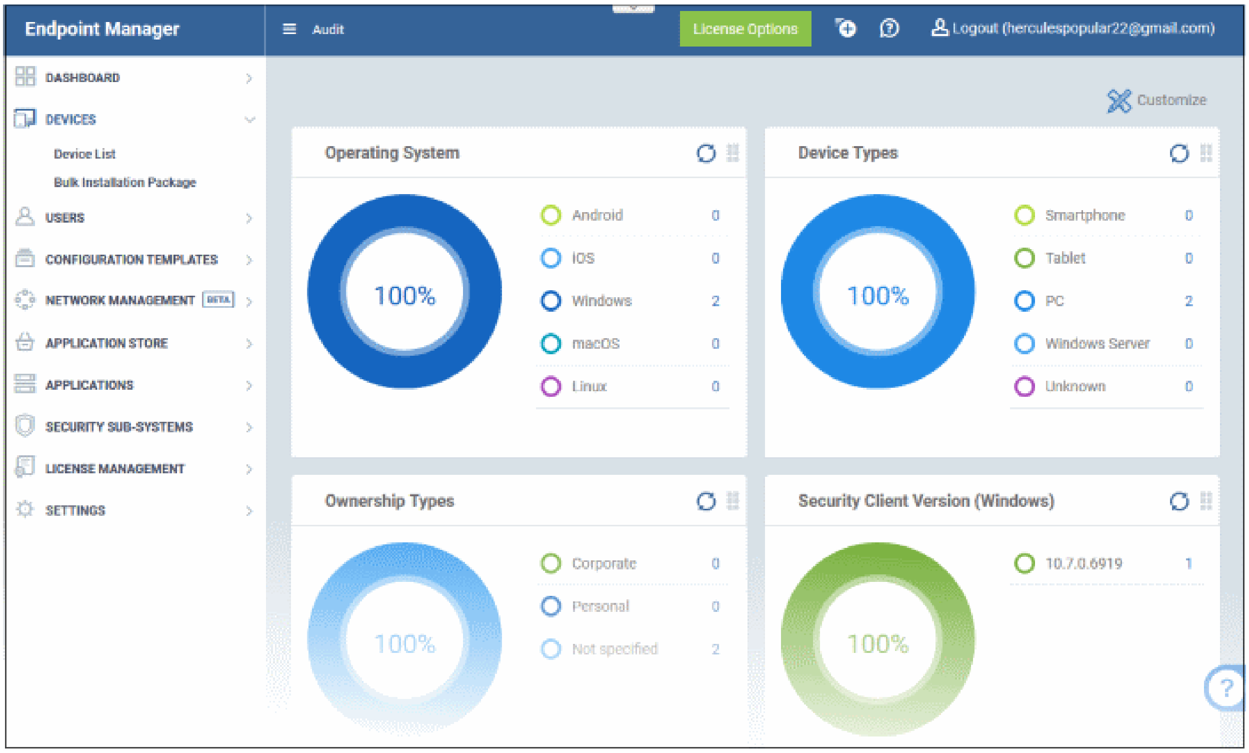


We have created a customized Onboarding Experience to match your interests. Click to get started with On Screen, Interactive Guidance.

**Note** - You need to configure your firewall to allow Endpoint Manager to communicate with our servers and your managed devices. IPs, host-names and ports are detailed in **Appendix 1**.

# 2. The Admin Console

The admin console is the nerve center of Endpoint Manager (EM), allowing you to add users, enroll devices, apply configuration profiles, run virus scans and more.



Once logged-in, admins can access different areas of the console using the menu on the left.

**Dashboard** - Contains charts and graphs which show the structure and security status of devices in your network. See **The Dashboard** for more details.

**Devices** - Manage and control enrolled devices, remotely install applications, generate sirens, wipe, lock and power off enrolled devices, remotely install and manage apps on devices, manage device groups and more. See **Devices and Device Groups** for more details.

**Users** - Create and manage users and user groups, enroll of their devices and assign configuration profiles to devices. See **Users and User Groups** for more details.

**Configuration Templates** - Profiles govern a device's network access rights, scan schedule and other system settings. You can create and manage profiles for iOS, Android Windows, Mac OS and Linux devices. See **Configuration Templates** for more details.

**Network Management** - Run device discovery scans on your networks. Discovery scans help you identity what endpoints are connected to a network. You can then enroll these devices to Endpoint Manager. See **Network Management** for more details.

**Application Store** - Repository of applications which can be pushed to iOS/Android/Windows devices directly from EM. See **Application Store** for more details.

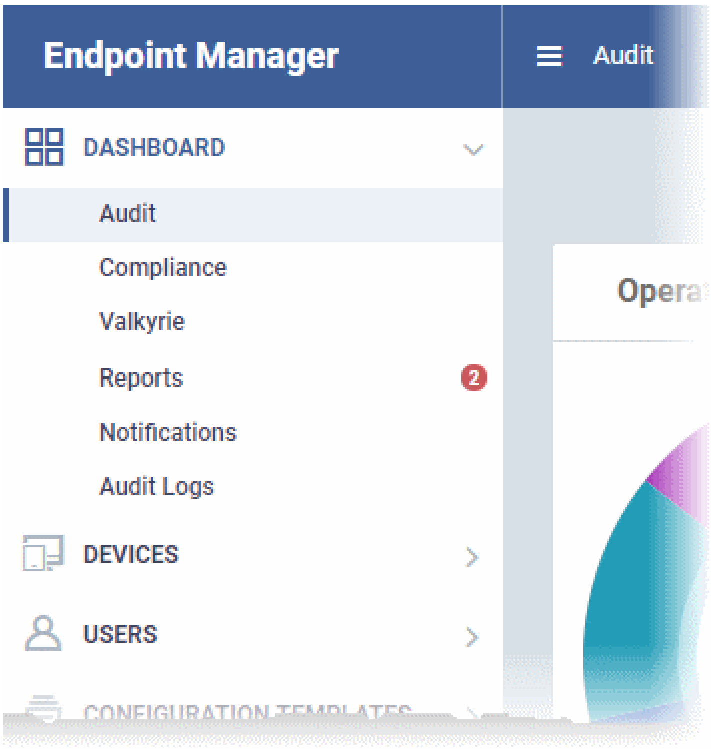
**Applications** - View and manage applications installed on Android, iOS and Windows devices. Manage patches on Windows devices. See **Applications** for more details.

**Security Sub-Systems** - View event logs, run AV scans and database updates. View and manage malware, quarantined items and contained applications. See **Security Sub-Systems** for more details.

**License Management** - Manage your subscriptions, distribute seats from a single license to different customers, and assign seats from multiple licenses to the same customer. See **License Management** for more information.

**Settings** - Configure email notifications, active directory, Google Cloud Messaging (GCM) and Apple Push Notification (APN) certificates and more. See **Configure Endpoint Manager** for more details.

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

| | |
|---|---|
| ⊕ | Clicking this button will display the 'Create User' and 'Enroll Device' drop-down. See '**Create New User Accounts**' and '**Enroll Users' Devices for Management**' for more details. |
| ? | Contains links to the online user guide, to the Comodo Dragon / Comodo One MSP and Enterprise forums and allows you to email our support department. |
| ☰ | Click the menu button to open or close the left-hand menu:<br><br> Endpoint Manager<br>Audit<br>DASHBOARD<br>Audit<br>Compliance<br>Valkyrie<br>Reports<br>2<br>Notifications<br>Audit Logs<br>DEVICES<br>USERS<br>CONFIGURATION TEMPLATES<br>Opera |
| Endpoint Manager | Click the logo to open the 'Welcome' screen. See **Login into the Admin Console** for more details. |
| Logout (coyoteewile@yahoo.com) | The username of the person currently logged in.<br>• Click this to log out of EM console. |
| License Options | Allows you to upgrade to the 'Premium' or 'Managed' version of EM. |

# 3. The Dashboard

- Click 'Dashboard' in the left menu to open this page.

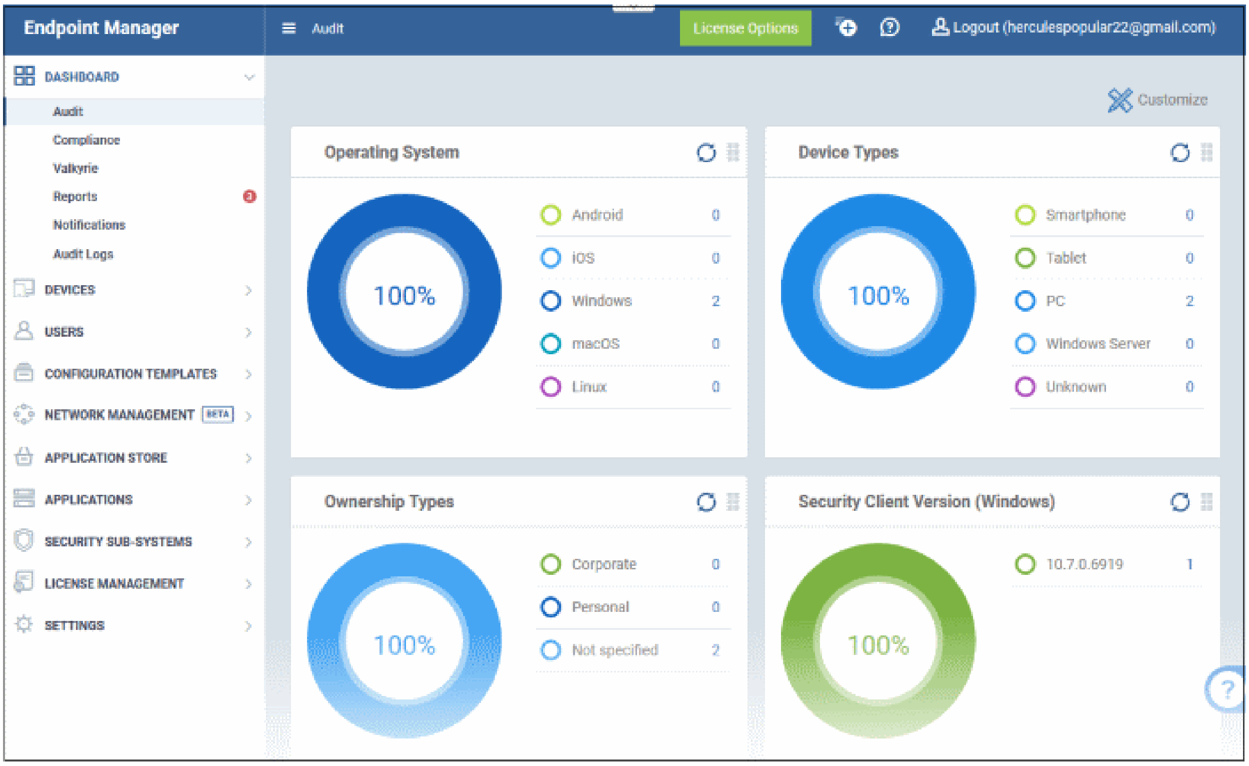
The dashboard shows real-time data about the operating system, connection status and security posture of all devices enrolled to Endpoint Manager (EM). It contains pie charts showing device types, platforms, ownership, scan status and compliance status. The dashboard also lets you view Valkyrie results, view notifications, and generate reports.

The dashboard is divided into six sections:

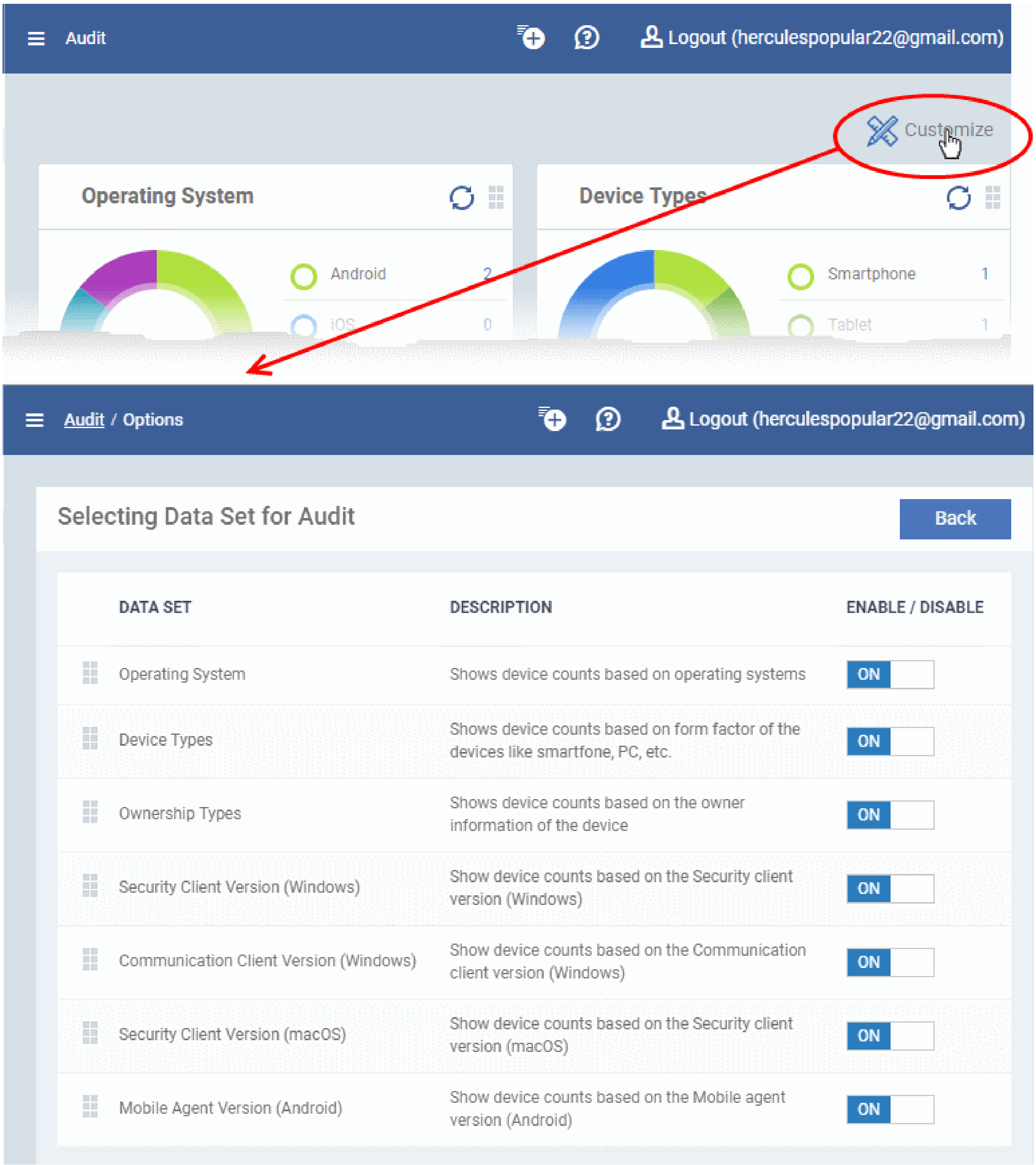
- **Audit** - Charts which show the operating systems and client versions installed on devices on your network. Also contains charts which show the types of devices in your network, and whether the devices are personal or corporate. See the **Audit** section for more details.
- **Compliance** - Statistics which detail how compliant your devices are with EM security policies. For example, device connection status, devices with viruses, devices with blacklisted applications, rooted and jailbroken devices, and device scan status. See **Compliance** for more details.
- **Valkyrie** - A summary of verdicts on unknown files submitted to the Valkyrie file analysis system. See **Valkyrie** for more details.
- **Reports** - A list of all reports generated by Endpoint Manager. You can also create new reports from here. See **Reports** section for more information.
- **Notifications** - A list of notifications sent to the administrator by EM. See **Notifications** for more details.
- **Audit Logs** - A list of actions taken on managed devices by admins and staff. Example actions include applying profiles, remote installation of packages and more. See **Audit Logs** for more details.

## Audit

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



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



Selecting Data Set for Audit

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

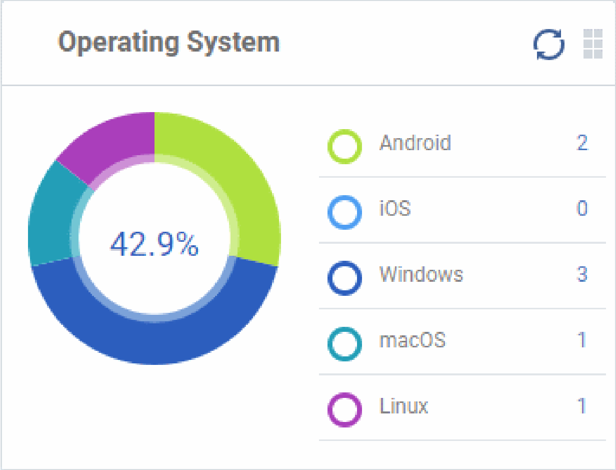
- Use the 'On/Off' switches to add or remove charts from the dashboard
- Click the 'Customize' ico Customize to view the number of charts removed from the default view
- Click and hold the icon at top right of a tile to move it around the page.

## Operating System

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

- Click on an item in the legend to view the respective 'Device List' page.

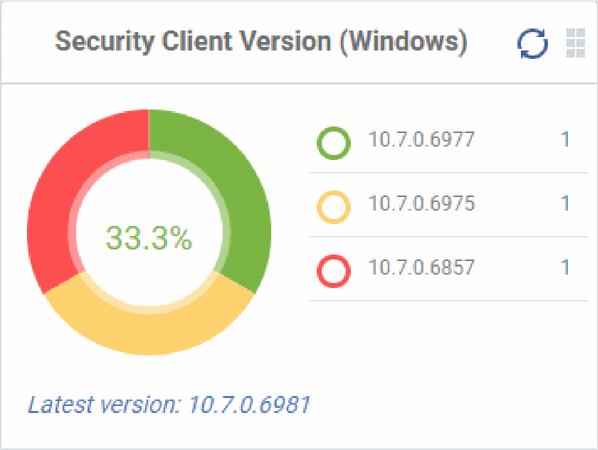
For example, clicking on 'Android' in the legend will open the 'Device List' page displaying the list of Android devices. See '**Devices**' for more details.



Operating System

42.9%

| | |
|---|---|
| ○ Android | 2 |
| ○ iOS | 0 |
| ○ Windows | 3 |
| ○ macOS | 1 |
| ○ Linux | 1 |



Security Client Version (Windows)

33.3%

| | |
|---|---|
| ○ 10.7.0.6977 | 1 |
| ○ 10.7.0.6975 | 1 |
| ○ 10.7.0.6857 | 1 |

*Latest version: 10.7.0.6981*

## Security Client Version (Windows)

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

- The number of devices using each version is shown to the right of the version number.
  - Click the number to view all devices using that version.
- The latest version of the client is shown underneath the chart.

Update to the latest version - Click the number, select the target devices, then click 'Install or Update Packages'.

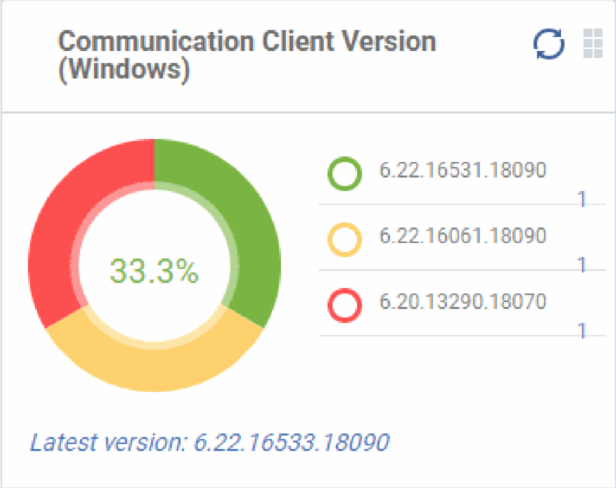
See **Remotely Install and Update Packages on Windows Devices** for more details.

## Communication Client Version (Windows)

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

- The number of devices using each version is shown to the right of the version number.
  - Click the number to view all devices using that version.
- The latest version of the client is shown underneath the chart.
- Update to the latest version - Click the number, select the target devices, then click 'Install or Update Packages'.

See **Remotely Install and Update Packages on Windows Devices** for more details.

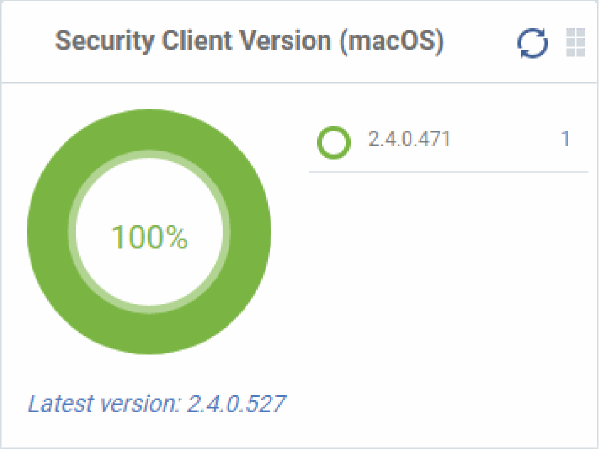


Communication Client Version (Windows)

33.3%

| | |
|---|---|
| ○ 6.22.16531.18090 | 1 |
| ○ 6.22.16061.18090 | 1 |
| ○ 6.20.13290.18070 | 1 |

*Latest version: 6.22.16533.18090*



### Security Client Version (Mac OS)

The versions of the security client installed on MAC OS devices on your network. The security client is the Comodo Client Security for MAC (CCS for Mac) software on an endpoint.

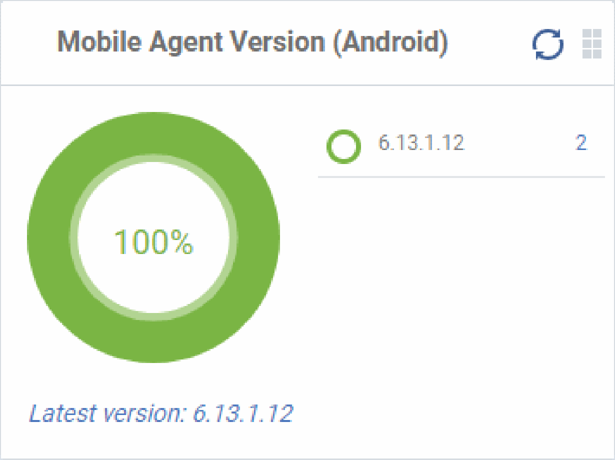
- The number of devices using each version is shown to the right of the version number.
    - Click the number to view all devices using that version.
- The latest version of the client is shown underneath the chart.
- Update to the latest version - Click the number, select the target devices, then click 'Install or Update Packages'.

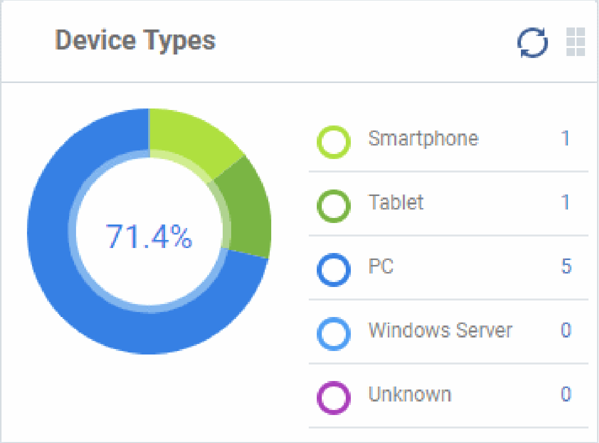
See **Remotely Install Packages on Mac OS Devices** for more details.

### Mobile Agent Version (Android)

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

- The number of devices using each version is shown to the right of the version number.
    - Click the number to view all devices using that version.
- The latest version of the client is shown underneath the chart.
- Update to the latest version - Click the number, select the target devices, then click 'Install or Update Packages'.





### Device Types

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

- Click an item in the legend to view the respective 'Device List' page.

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

### Ownership Types

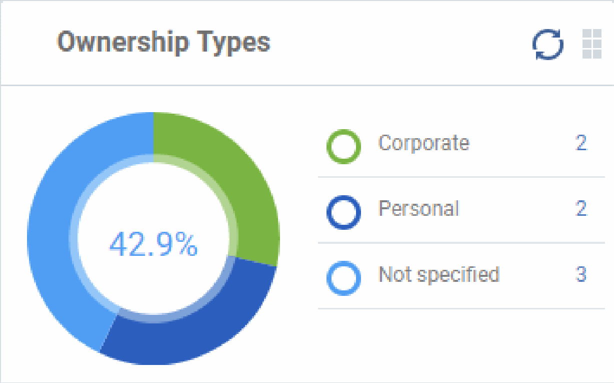
Ownership types can be 'Corporate', 'Personal' or 'Not Specified'.

- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'Personal' in the legend will show all devices in that category. See 'Devices' for more details.

Change ownership type:

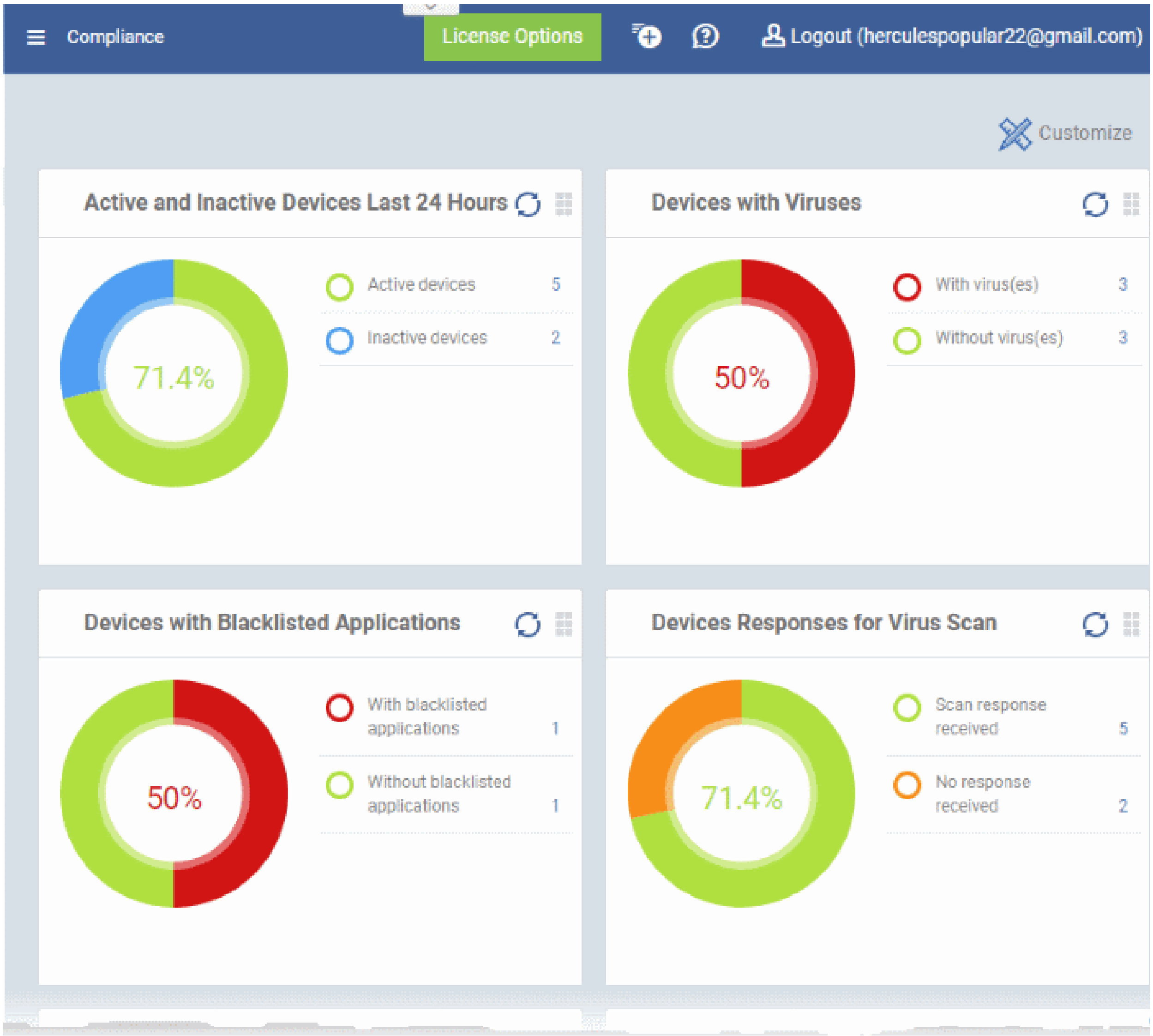
- Click 'Devices' > 'Device List' > *click a device name* > Click 'Owner' button > 'Change ownership'.



## Compliance

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

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

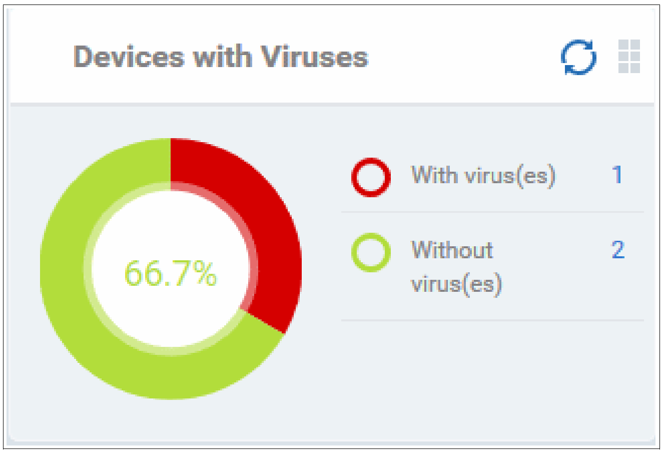

Compliance
License Options
Logout (herculespopular22@gmail.com)
Customize
Active and Inactive Devices Last 24 Hours
71.4%
Active devices 5
Inactive devices 2
Devices with Viruses
50%
With virus(es) 3
Without virus(es) 3
Devices with Blacklisted Applications
50%
With blacklisted applications 1
Without blacklisted applications 1
Devices Responses for Virus Scan
71.4%
Scan response received 5
No response received 2

- To customize the charts shown in the interface, click the 'Customize' button

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

### Devices With Viruses

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

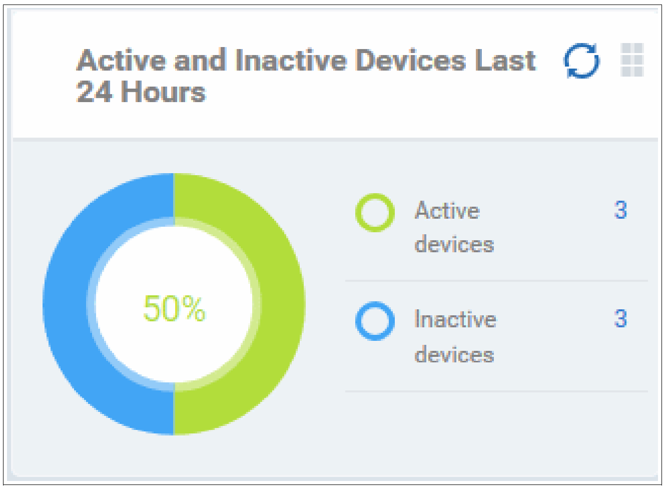


- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'With virus(es)' will open the 'Device List' page displaying devices that contain viruses. See '**Devices**' for more details.

### Active and Inactive Devices Last 24 Hours

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

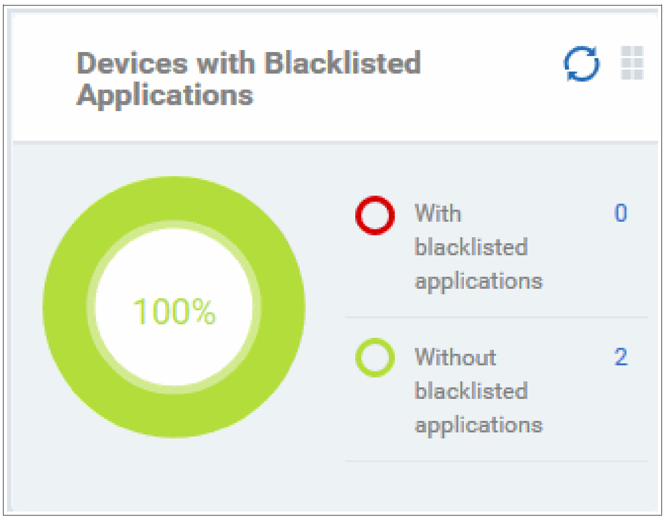


- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'Active Devices' will open the 'Device List' page displaying the list of active devices. Similarly clicking on the 'Inactive Device' legend will open the 'Device List' page displaying the list of inactive devices. The devices screens allow you to manage the enrolled devices. See '**Devices**' for more details.

### Devices with Blacklisted Applications

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



Devices with Blacklisted Applications

100%

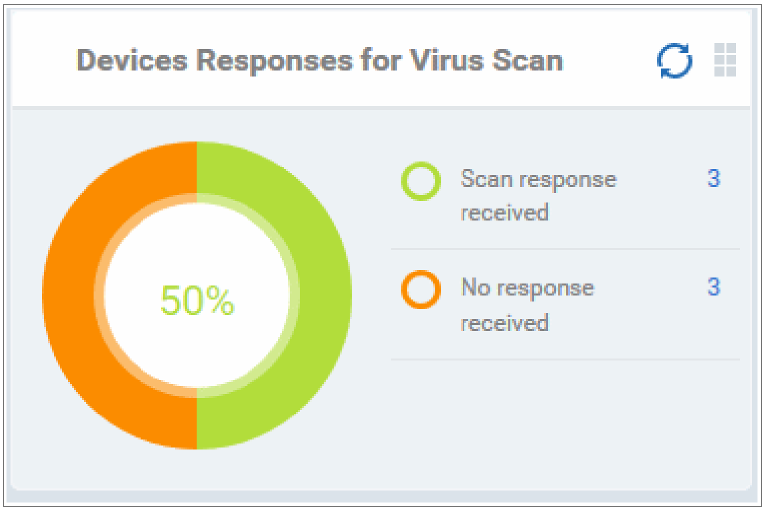
| | | |
|---|---|---|
| ○ | With blacklisted applications | 0 |
| ○ | Without blacklisted applications | 2 |

- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'With Blacklisted Applications' legend will open the 'Device List' page displaying the list of devices that have blacklisted applications on them. See '**Devices**' for more details.

**Devices Responses for Virus Scan**

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



Devices Responses for Virus Scan

50%

| | | |
|---|---|---|
| ○ | Scan response received | 3 |
| ○ | No response received | 3 |

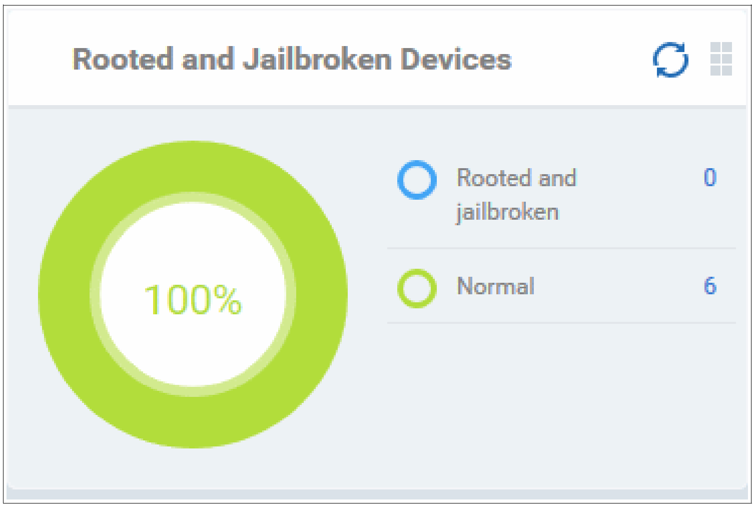
- Click an item in the legend to view the respective 'Device List' page.

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

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

**Rooted And Jail-broken Devices**

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



Rooted and Jailbroken Devices

| | |
|---|---|
| Rooted and jailbroken | 0 |
| Normal | 6 |

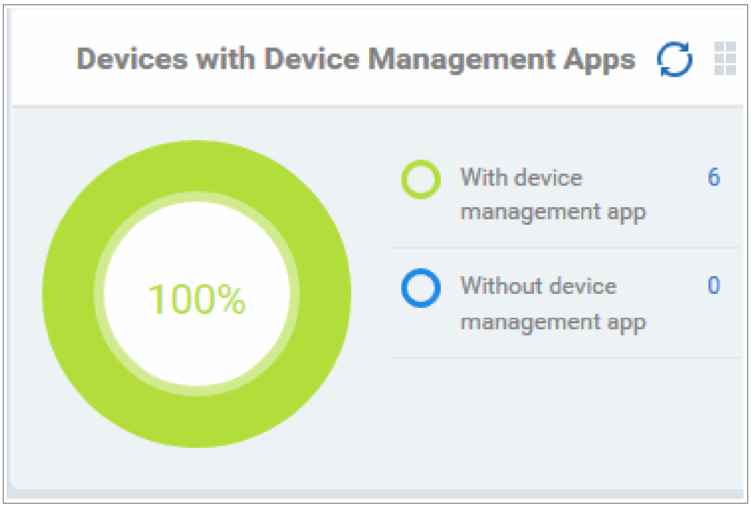
- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'Normal' in the legend will open the 'Device List' page displaying the list of devices that are normal, that is, not rooted or jail-broken. See '**Manage Devices**' for more details.

**Devices With Device Management Apps**

Shows how many devices have the communication client. Android, Windows. Mac OS and Linux devices can only be enrolled with the EM app/communication Client (CC). iOS devices communicate with EM via the EM profile that was installed during enrollment and do not require the app. However, installing the app will provide enhanced functionality such as device location and the ability to send messages to the device from the admin panel.

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



Devices with Device Management Apps

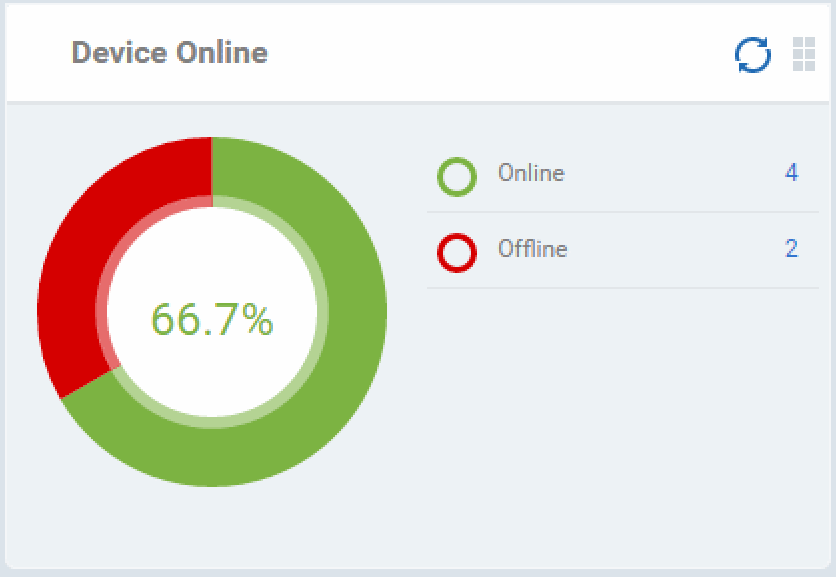
| | |
|---|---|
| With device management app | 6 |
| Without device management app | 0 |

- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'With device management App' will open the 'Device List' page displaying the list of devices that have the EM app installed. See '**Manage Devices**' for more details.

**Device Online**

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

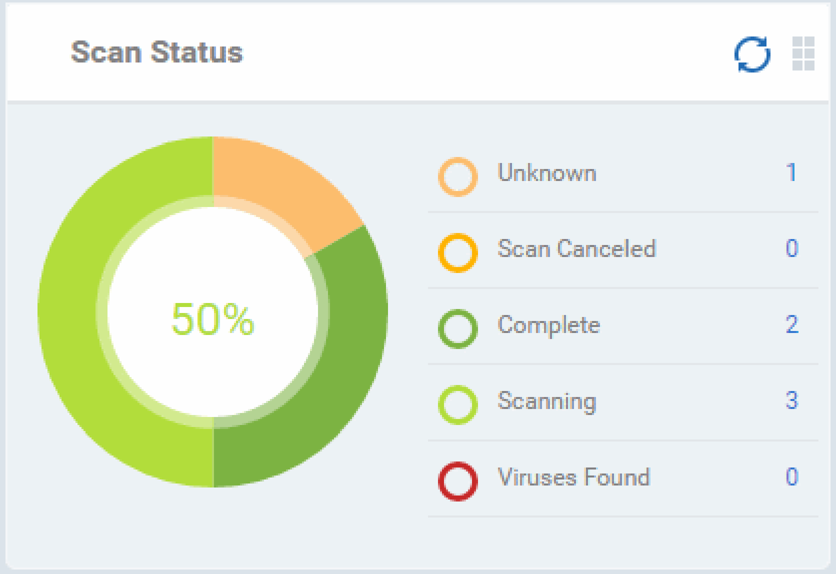


- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'Online' will open the 'Device List' page displaying the list of devices that are online. See '**Manage Devices**' for more details.

**Scan Status**

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

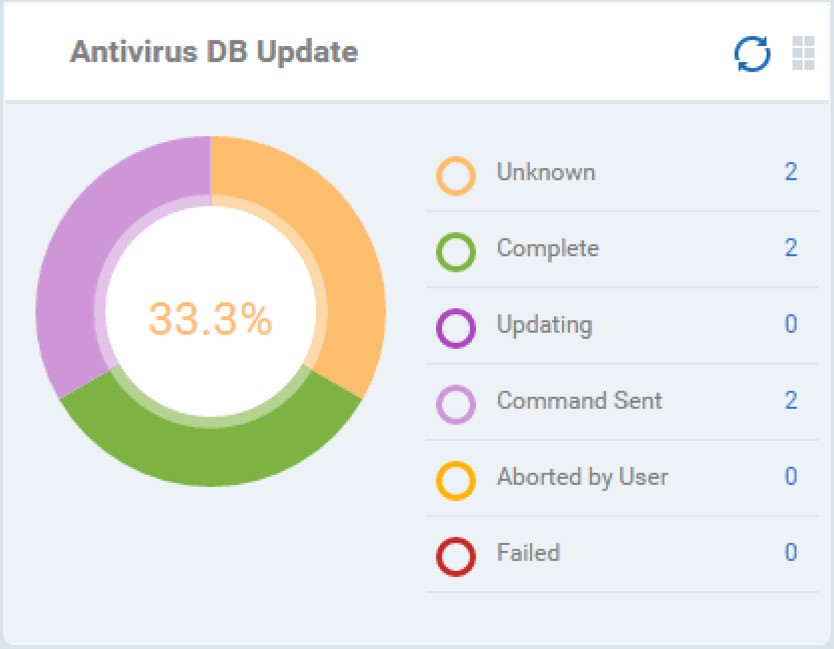


- Click an item in the legend to view the respective 'Device List' page.

For example, clicking on 'Virus Found' in the legend will open the 'Antivirus Device List' page displaying the list of devices in which the malware were detected. See '**Antivirus Scans**' for more details.

**Antivirus DB Update**

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



Antivirus DB Update

| | |
|---|---|
| Unknown | 2 |
| Complete | 2 |
| Updating | 0 |
| Command Sent | 2 |
| Aborted by User | 0 |
| Failed | 0 |

- Click an item in the legend to view the respective 'Device List' page.

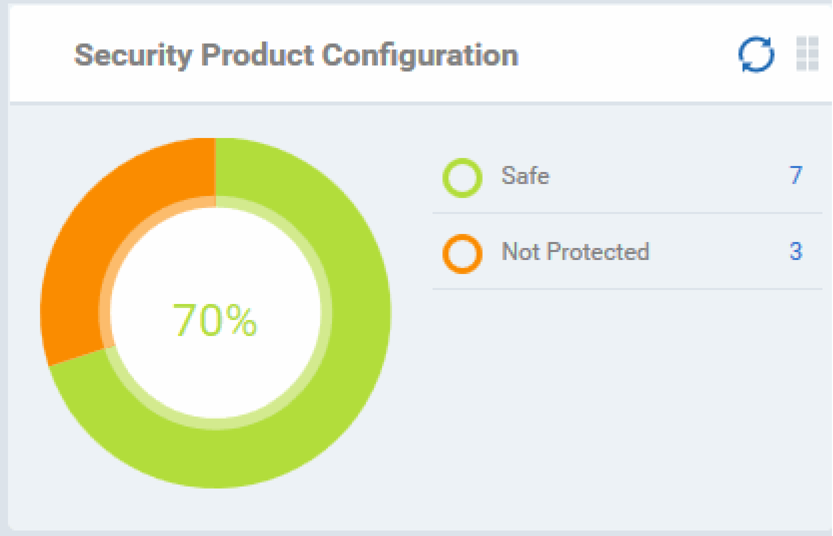
For example, clicking on 'Complete' in the legend will show devices which have the latest virus database. See **Antivirus Scans**' for more details.

**Security Product Configuration**

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

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

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



Security Product Configuration

| | |
|---|---|
| Safe | 7 |
| Not Protected | 3 |

- Click an item in the legend to view the respective 'Device List' page.

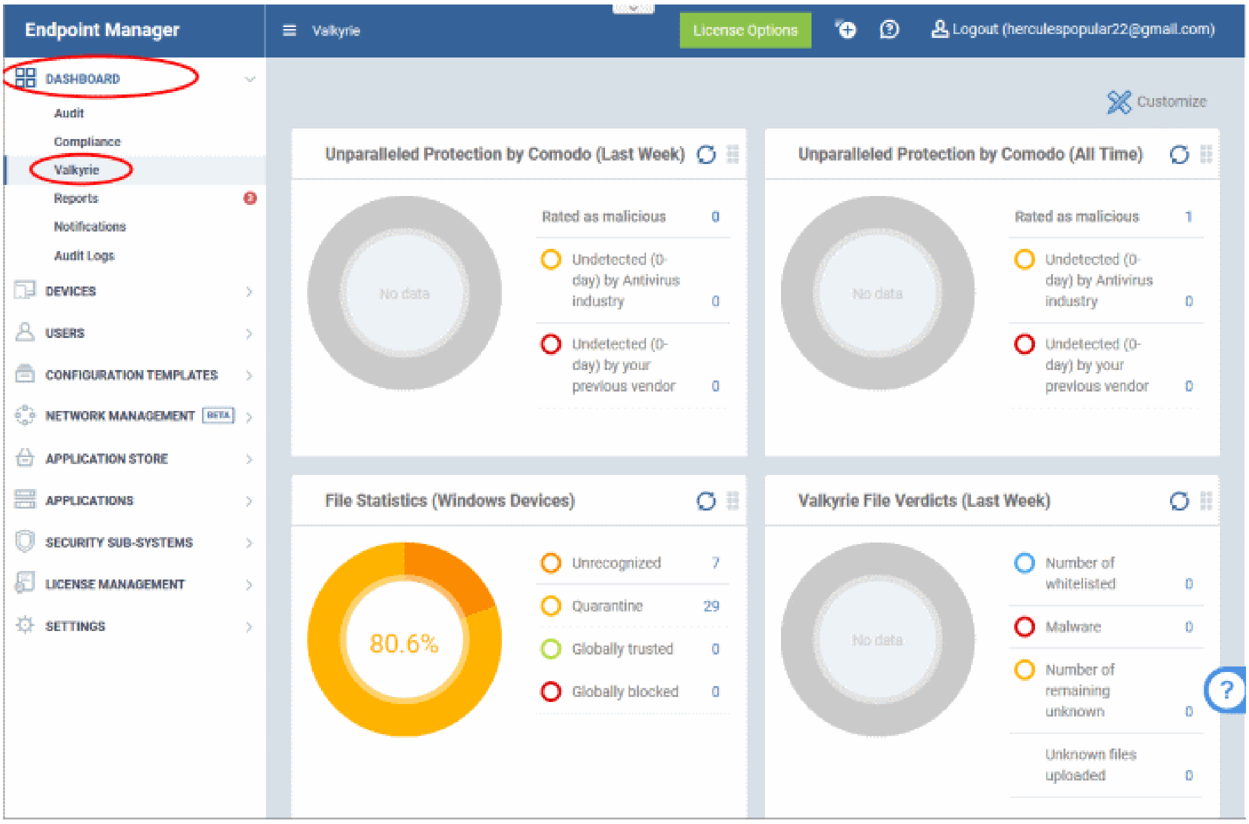
For example, clicking on 'Safe' will open the 'Device List' page displaying the list of devices that have Antivirus installed. See '**Devices**' for more details.

## Valkyrie

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

- To use the service, apply a profile to CCS that contains the 'Valkyrie' component.
    - Click 'Configuration Templates' > 'Profiles'
    - Click the name of the profile you want to edit, or click 'Create' to make a new profile
    - Click the 'Add Profile Section' button > 'Valkyrie'
    - Click 'Save'
- All results will be displayed in the Valkyrie dashboard. See **Valkyrie Settings** in **Creating Windows Profile** for more details.

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



Unparalleled Protection by Comodo (Last Week)

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

Unparalleled Protection by Comodo (All Time)

| | |
|---|---|
| Rated as malicious | 1 |
| Undetected (0-day) by Antivirus industry | 0 |
| Undetected (0-day) by your previous vendor | 0 |

File Statistics (Windows Devices)

| | |
|---|---|
| Unrecognized | 7 |
| Quarantine | 29 |
| Globally trusted | 0 |
| Globally blocked | 0 |

Valkyrie File Verdicts (Last Week)

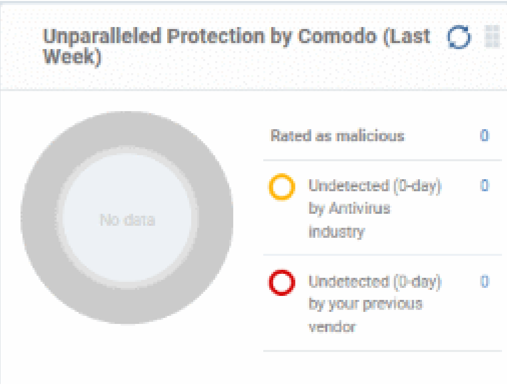
| | |
|---|---|
| Number of whitelisted | 0 |
| Malware | 0 |
| Number of remaining unknown | 0 |
| Unknown files uploaded | 0 |

### Unparalleled Protection by Comodo (Last Week)

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

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

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

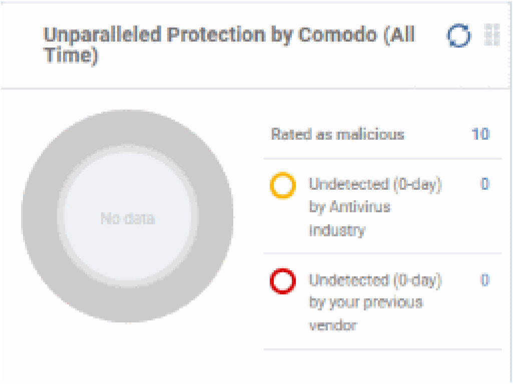


Unparalleled Protection by Comodo (Last Week)

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

### Unparalleled Protection By Comodo (All Time)

Shows the number of threats identified by Valkyrie since installation versus the user's previous vendor and the



Unparalleled Protection by Comodo (All Time)

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

antivirus industry as a whole.

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

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

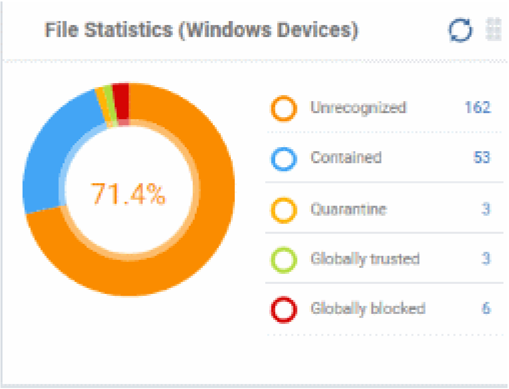
### File Statistics (Windows Devices)

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

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

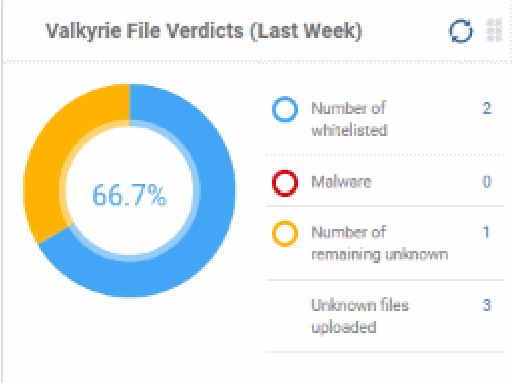
- Click any item in the legend will to open the respective 'File List' page.

For example, clicking on 'Unrecognized' will open the 'Application Control' > 'Unrecognized' page displaying the list of unrecognized files detected from enrolled devices. See '**Manage File Trust Ratings on Windows Devices**.' for more details.



File Statistics (Windows Devices)

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



Valkyrie File Verdicts (Last Week)

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

### Valkyrie File Verdicts (Last Week)

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

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

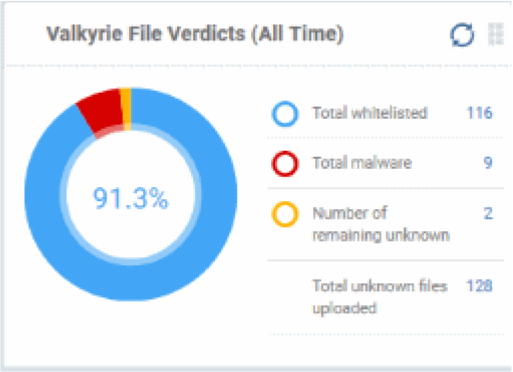
See **Manage File Trust Ratings on Windows Devices**, for more details on Windows File List screen.

### Valkyrie File Verdicts (All Time)

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

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

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



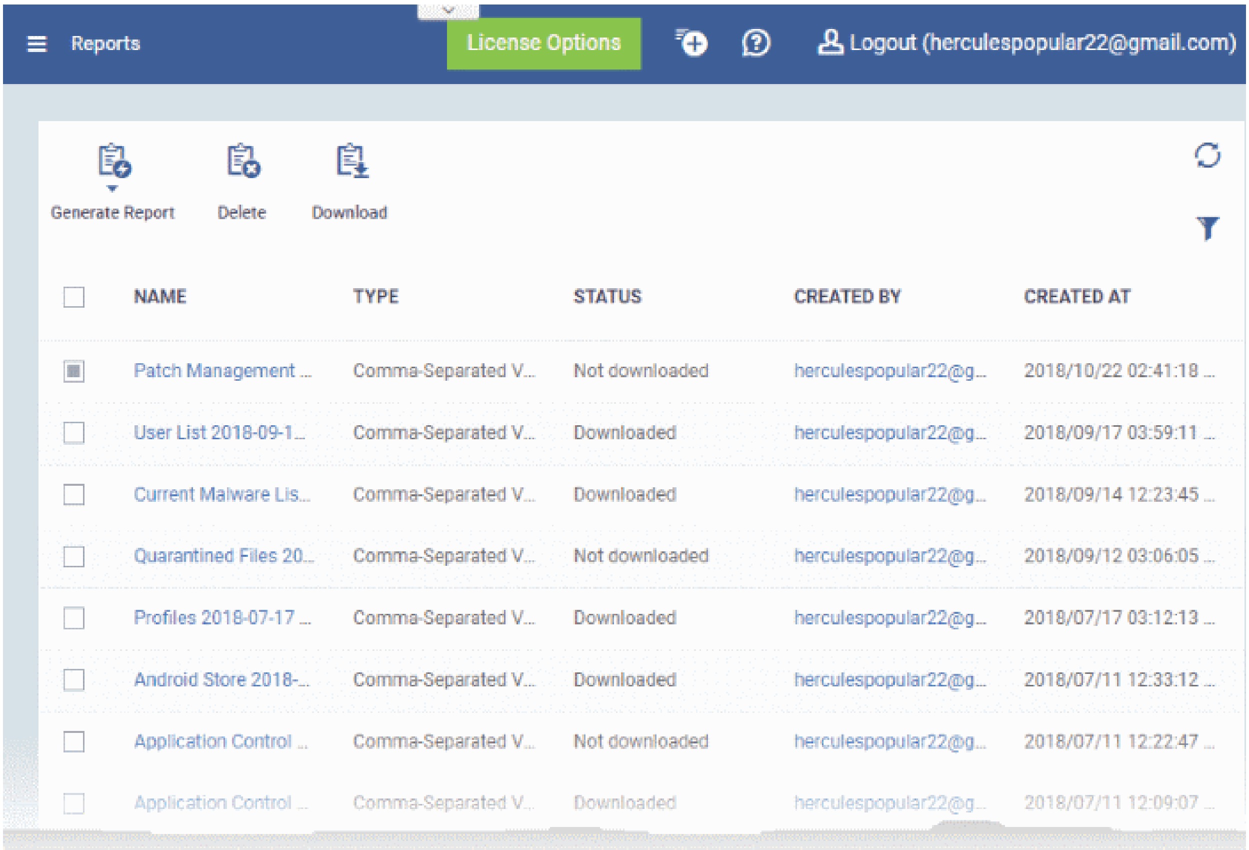
Valkyrie File Verdicts (All Time)

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

## Reports

Endpoint Manager can create a wide variety of reports on system and malware activity on your fleet of devices.

- Click 'Dashboard' on the left then select 'Reports'
- The reports interface lets you generate and download many different report types:



| □ | NAME | TYPE | STATUS | CREATED BY | CREATED AT |
|---|---|---|---|---|---|
| ☒ | Patch Management ... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018/10/22 02:41:18 ... |
| □ | User List 2018-09-1... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018/09/17 03:59:11 ... |
| □ | Current Malware Lis... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018/09/14 12:23:45 ... |
| □ | Quarantined Files 20... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018/09/12 03:06:05 ... |
| □ | Profiles 2018-07-17 ... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018/07/17 03:12:13 ... |
| □ | Android Store 2018-... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018/07/11 12:33:12 ... |
| □ | Application Control ... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018/07/11 12:22:47 ... |
| □ | Application Control ... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018/07/11 12:09:07 ... |

| Column Header | Description |
|---|---|
| Name | The subject of the report.<br>• Click the name to view report details and download the report. |
| Type | The file format of the report. |
| Status | Whether or not the report has been downloaded by any user. |
| Created By | The admin who generated the report.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created At | The date and time the report was generated |

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

There are two ways you can generate reports:

1. **'Dashboard' > 'Reports' interface -** Lets you generate following report types:
    - Android Antivirus

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

These reports are generated in spreadsheet (.xls) file format.

2. **From specific interfaces**:

- Users menu
  - User List - Click 'Users' > 'User Groups' > 'Export'. Click here for more details.
  - User Groups - Click 'Users' > 'User Groups' > 'Export'. Click here for more details.
  - Role Management:
    - Roles - Click 'Users' > 'Role Management' > 'Roles' > 'Export'. Click here for more details.
    - Users - Click 'Users' > 'Role Management' > 'Users' > 'Export'. Click here for more details.
- Devices main menu
  - Device List - Click 'Devices' > 'Device List' > 'Export'. Click here for more details.
  - Device Details > File List - Click 'Devices' > 'Device List' > Any Windows Device > 'File List' > 'Export'. Click here for more details.
- Configuration Templates' menu
  - Profiles - Click 'Configuration Templates' > 'Profiles' > 'Export'. Click here for more details.
  - Alerts - Click 'Configuration Templates' > 'Alerts' > 'Export'. Click here for more details.
  - 'Procedures' main menu
    - Procedures List - Click 'Configuration Templates' > 'Procedures' > 'Export'. Click here for more details.
    - Procedure Execution Logs - Click 'Configuration Templates' > 'Procedures' > 'any scrip procedure' > 'Execution Log' sub-tab > 'Export'. Click here for more details.
- Application Store menu
  - iOS Store - Click 'Application Store' > 'iOS Store' > 'Export'. Click here for more details.
  - Android Store - Click 'Application Store' > 'iOS Store' > 'Export'. Click here for more details.
- Applications menu
  - Mobile Applications - Click 'Applications' > 'Mobile Applications' > 'Export'. Click here for more details.
  - Patch Management - Click 'Applications' > 'Patch Management' > 'Operating System' tab > 'Export'. Click here for more details.
- Security Subsystems menu
  - Containment - Click 'Security Sub-Systems' > 'Containment' > 'Export'. Click here for more details.
  - Application Control - Click 'Security Sub-Systems' > 'Application Control' > 'Export'. Click here for more details.
  - Valkyrie - Click 'Security Sub-Systems' > 'Valkyrie' > 'Export'. Click here for more details.
  - Device Control - Click 'Security Sub-Systems' > 'Device Control' > 'Export'. Click here for more details.
  - Antivirus:
    - Device List - Click 'Security Sub-Systems' > 'Antivirus' > 'Device List' tab > 'Export'. Click here for more details.
    - Current Malware List - Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List' tab > 'Export'. Click here for more details.

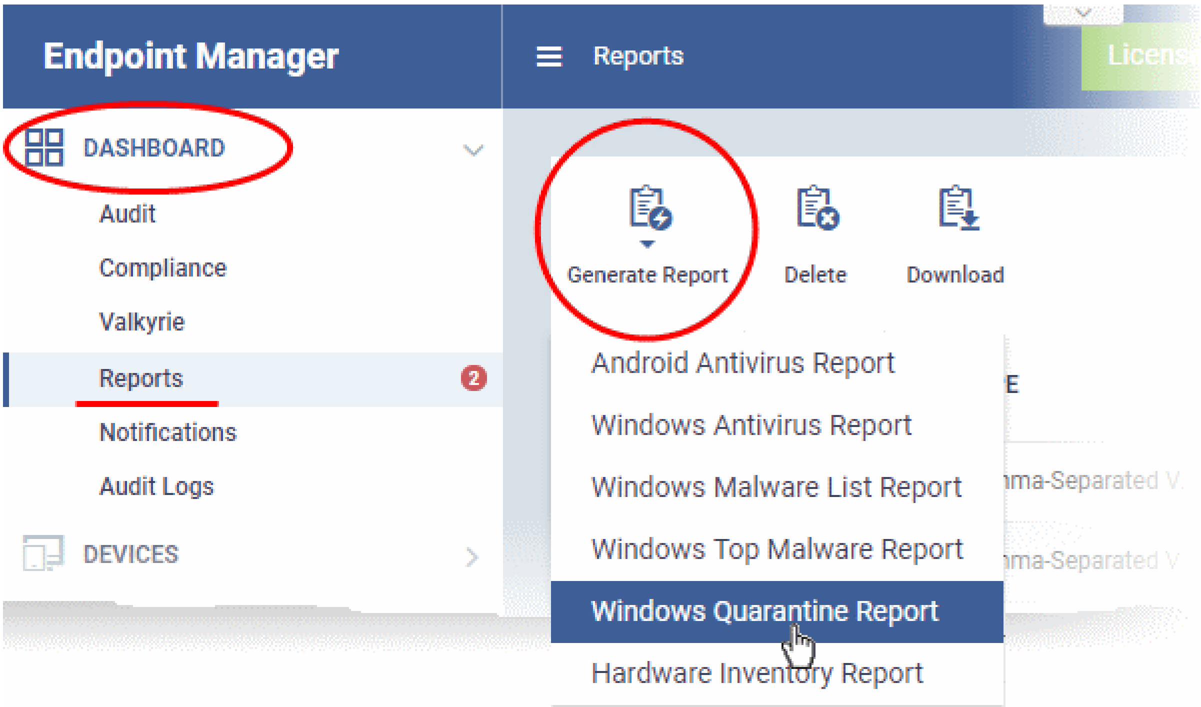
  - **Quarantined Files** - Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files' tab > 'Export'. **Click here** for more details.
  - **Threat History** - Click 'Security Sub-Systems' > 'Antivirus' > 'Threat History' tab > 'Export'. **Click here** for more details.
  - **Autoruns Items** - Click 'Security Sub-Systems' > 'Antivirus' > 'Autoruns Items' tab > 'Export'. **Click here** for more details.

- **License Management** menu
  - **Licenses** - Click 'License Management' > 'License Management' > 'Licenses' tab > 'Export'. **Click here** for more details
  - **Customers** - Click 'License Management' > 'License Management' > 'Licenses' tab > select a license > 'Details' > 'Customers' tab > 'Export'. **Click here** for more details

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

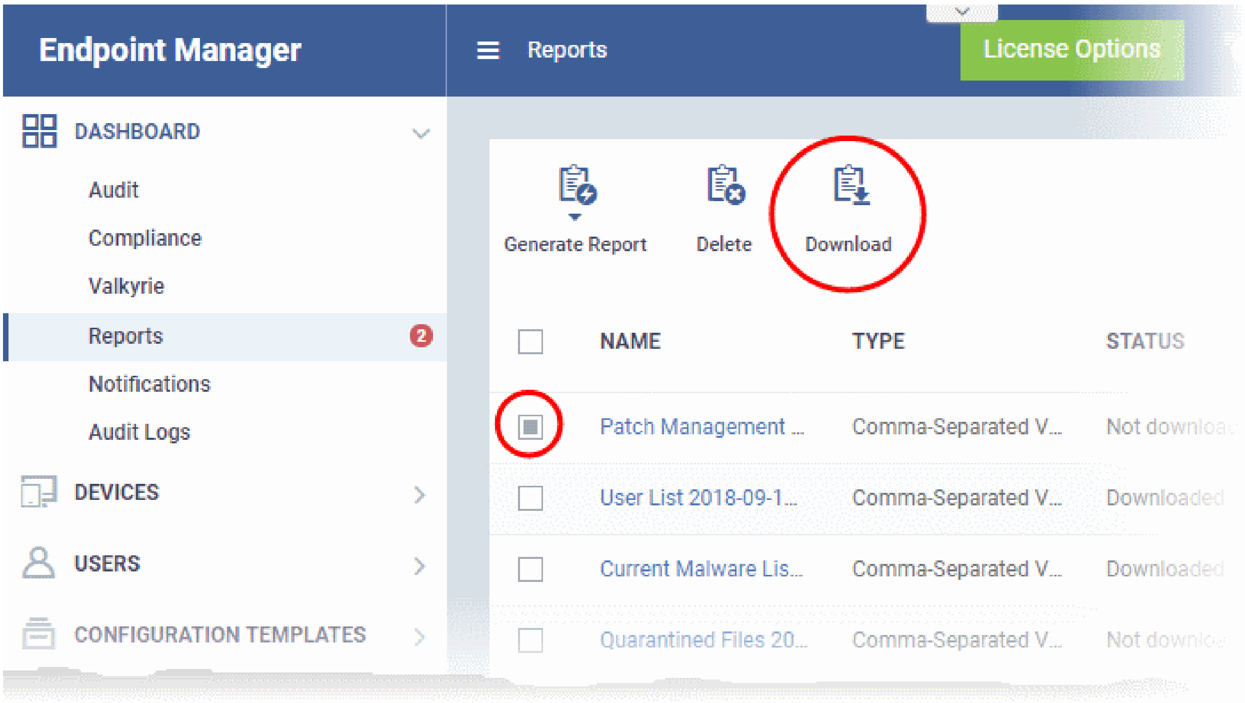
### Generate a report from the 'Reports' interface

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



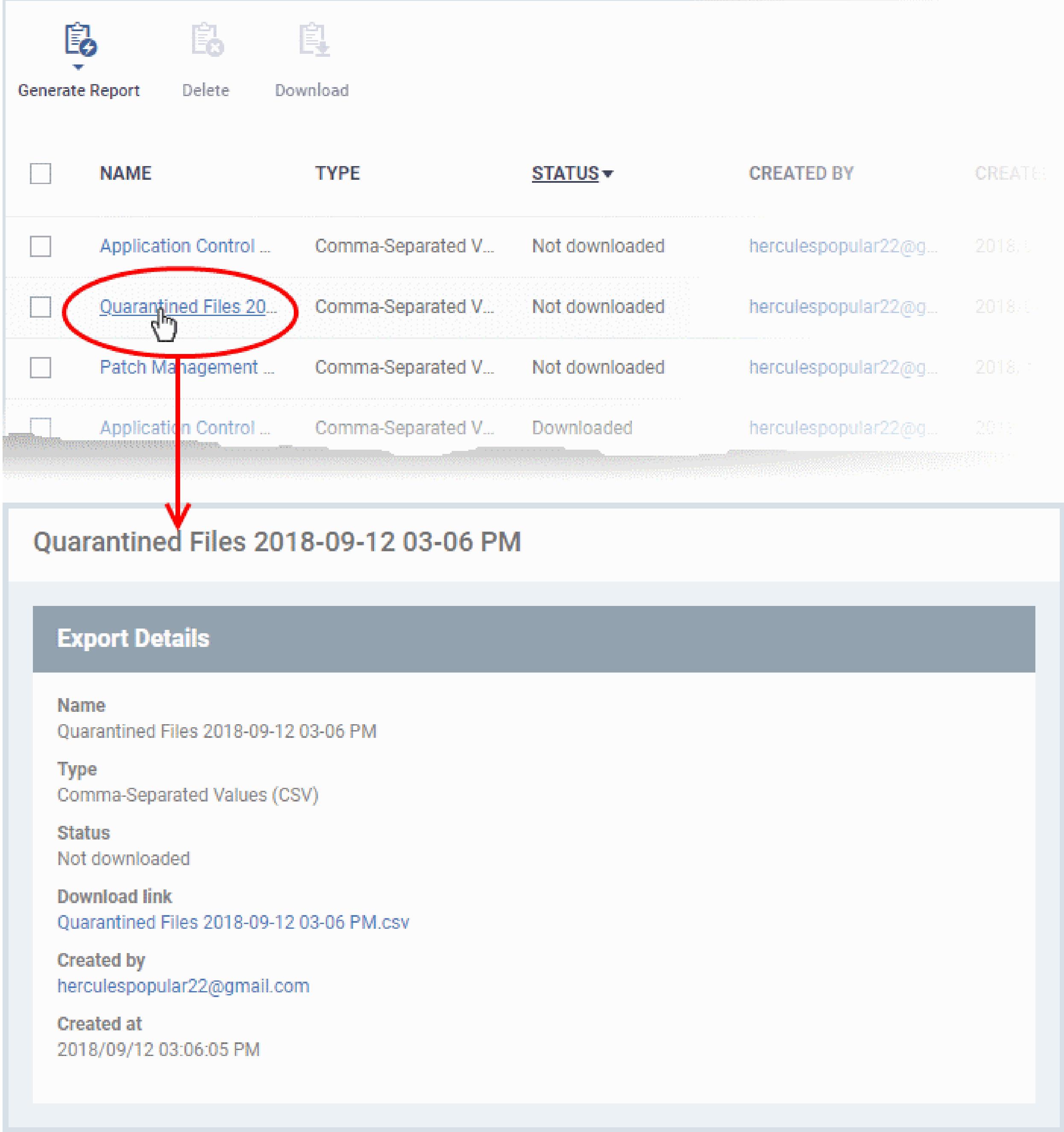
A new report will be generated for the selected report type.

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



| | NAME | TYPE | STATUS |
|---|---|---|---|
| ☒ | Patch Management ... | Comma-Separated V... | Not downloa |
| □ | User List 2018-09-1... | Comma-Separated V... | Downloaded |
| □ | Current Malware Lis... | Comma-Separated V... | Downloaded |
| □ | Quarantined Files 20... | Comma-Separated V... | Not downlo |

- Click a report name to view report details.



| □ | NAME | TYPE | STATUS ▾ | CREATED BY | CREATE |
|---|---|---|---|---|---|
| □ | Application Control ... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018. |
| □ | Quarantined Files 20... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018. |
| □ | Patch Management ... | Comma-Separated V... | Not downloaded | herculespopular22@g... | 2018. |
| □ | Application Control ... | Comma-Separated V... | Downloaded | herculespopular22@g... | 2018 |

Quarantined Files 2018-09-12 03-06 PM

Export Details

Name
Quarantined Files 2018-09-12 03-06 PM

Type
Comma-Separated Values (CSV)

Status
Not downloaded

Download link
Quarantined Files 2018-09-12 03-06 PM.csv

Created by
herculespopular22@gmail.com

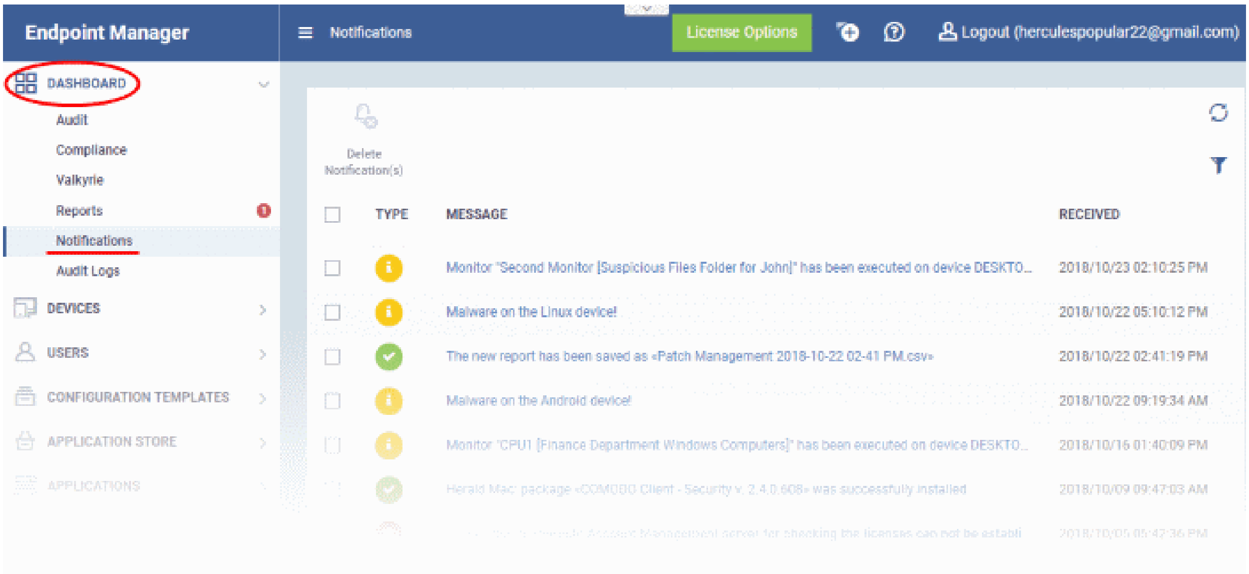
Created at
2018/09/12 03:06:05 PM

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

## Notifications

- The number of unread messages you have is shown on the notification icon: 🔔 43

- Click the icon to view the messages.



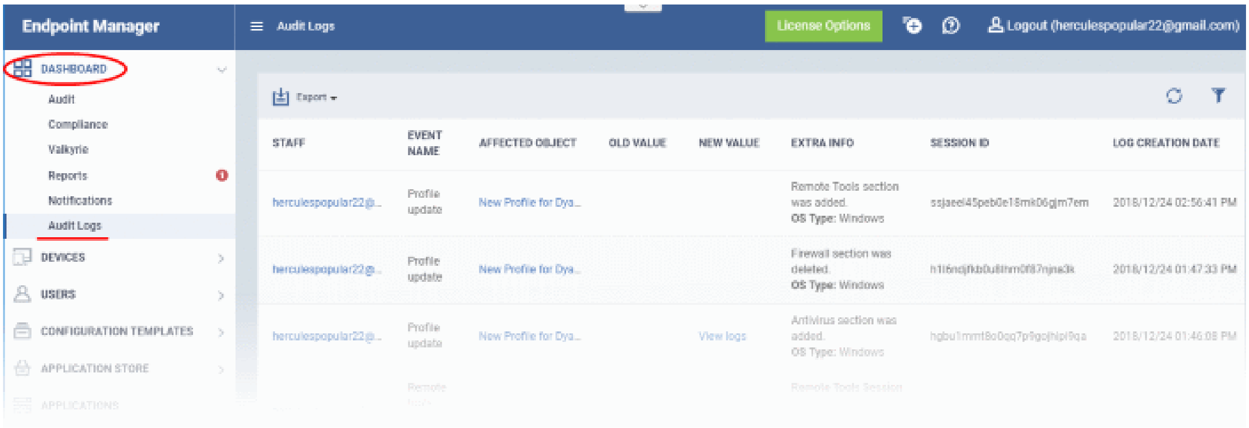
| □ | TYPE | MESSAGE | RECEIVED |
|---|---|---|---|
| □ | ℹ | Monitor "Second Monitor [Suspicious Files Folder for John]" has been executed on device DESKTO... | 2018/10/23 02:10:25 PM |
| □ | ℹ | Malware on the Linux device! | 2018/10/22 05:10:12 PM |
| □ | ✓ | The new report has been saved as «Patch Management 2018-10-22 02-41 PM.csv» | 2018/10/22 02:41:19 PM |
| □ | ℹ | Malware on the Android device! | 2018/10/22 09:19:34 AM |
| □ | ℹ | Monitor "CPU1 [Finance Department Windows Computers]" has been executed on device DESKTO... | 2018/10/16 01:40:09 PM |
| □ | ✓ | Herald Mac: package «COMODO Client - Security v. 2.4.0.608» was successfully installed | 2018/10/09 09:47:03 AM |
|  |  | [illegible] Account Management server for checking the licenses can not be establi | 2018/10/05 05:47:36 PM |

- Message titles also act as shortcuts to the relevant interface. For example, clicking on 'Malware Found on Windows device' message opens the 'Antivirus Current Malware List' screen.

> **Tip**: You can also receive notifications as emails. Click 'Settings' > 'Email Notifications' to configure them. See **Configure Email Notifications** if you need help with this.

## Audit Logs

- Endpoint Manager keeps a log of actions implemented on managed devices by administrators and staff. These logs can be useful when troubleshooting issues.
- Logged actions include enrollment and removal of devices, applying a security profile, creating and editing security profiles, package installations, remote take-over sessions, restarting a device, removing a device, remote disconnections, changes to containment settings, updates to file group variables, remote file transfers and more.
- The 'Audit Logs' interface shows all log entries along with details such as the name of the staff member who applied the action, the affected device, the action taken and more.
- Audit logs are maintained for up to one year for PCI-DSS compliance.
- You can generate a report containing logs for the past three months as a comma separated values (CSV) file.
- Click 'Dashboard' > 'Audit Logs' in the left-menu to open the log interface:



| STAFF | EVENT NAME | AFFECTED OBJECT | OLD VALUE | NEW VALUE | EXTRA INFO | SESSION ID | LOG CREATION DATE |
|---|---|---|---|---|---|---|---|
| herculespopular22@... | Profile update | New Profile for Dya... | | | Remote Tools section was added.<br>**OS Type:** Windows | ssjaeel45peb0e18mk06gjm7em | 2018/12/24 02:56:41 PM |
| herculespopular22@... | Profile update | New Profile for Dya... | | | Firewall section was deleted.<br>**OS Type:** Windows | h1l6ndjfkb0u8lhm0f87njna3k | 2018/12/24 01:47:33 PM |
| herculespopular22@... | Profile update | New Profile for Dya... | | View logs | Antivirus section was added.<br>OS Type: Windows | hgbu1mmt8o0qq7p9gojhipl9qa | 2018/12/24 01:46:08 PM |
| | Remote [illegible] | | | | Remote Tools Session | | |

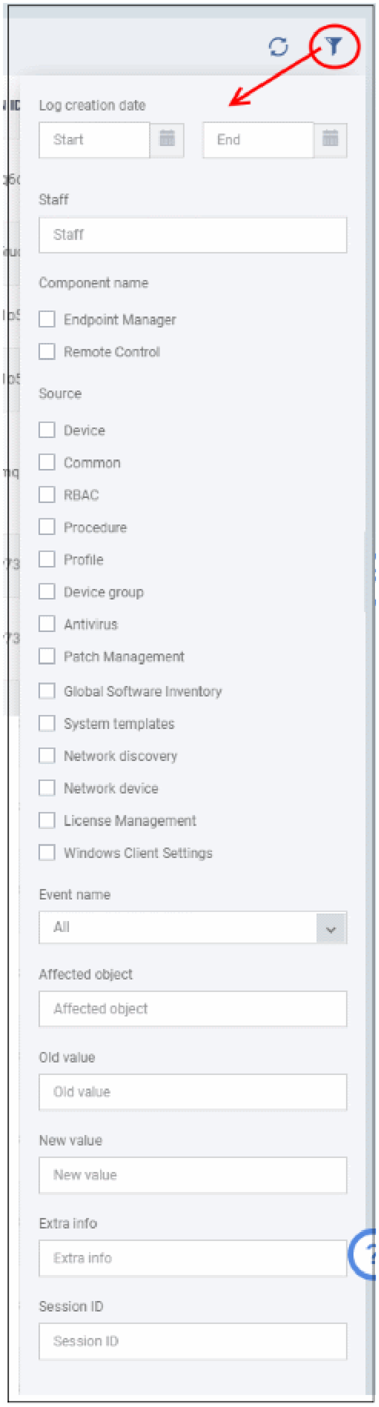
| Audit Logs - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Staff | Username of the admin or staff member who executed the action.<br>- Click the staff name to view their details. See **View user details** if you need help with the details interface. |
| Event Name | The action executed on the device. Examples include enrollment of devices, remote installation of Comodo and third party MSI packages, remote take-overs and device removals. |
| Affected Object | The device, device group, profile, procedure or file group on which the action was executed.<br>- Click the name to view more details about the item<br>- The details interface allows you to view and manage the respective item. |
| Old Value | The previous setting or value before the action was implemented.<br>For example, if a Comodo package is remotely updated, the old version number of the package will be shown here. |
| New Value | The new setting or value after the action was implemented.<br>For example, if a Comodo package is remotely updated, the version number of the new package will be shown here. |
| Extra Info | Additional details about the action. Additional details include devices on which the procedure was run, package installation parameters, profiles applied/removed, malware quarantined, antivirus scans run and so on.<br>- Script or patch procedures - Click the 'Selected Devices' link to view devices on which the procedure was run.<br>- Click a device name in the list to view its 'Device Details' interface |
| Session ID | String used to identify the connection session between the device and the EM server during the action. |
| Log Creation Date | Date and time of the event. |
| **Controls** | |
| Export | Generate a comma separated values (CSV) file of logs for a selected time period. |

| | |
|---|---|
| | The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Generate Audit Logs Reports** for more details. |

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

**Search and filter options**

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



Log creation date

Start | End

Staff

Staff

Component name

□ Endpoint Manager

□ Remote Control

Source

□ Device

□ Common

□ RBAC

□ Procedure

□ Profile

□ Device group

□ Antivirus

□ Patch Management

□ Global Software Inventory

□ System templates

□ Network discovery

□ Network device

□ License Management

□ Windows Client Settings

Event name

All

Affected object

Affected object

Old value

Old value

New value

New value

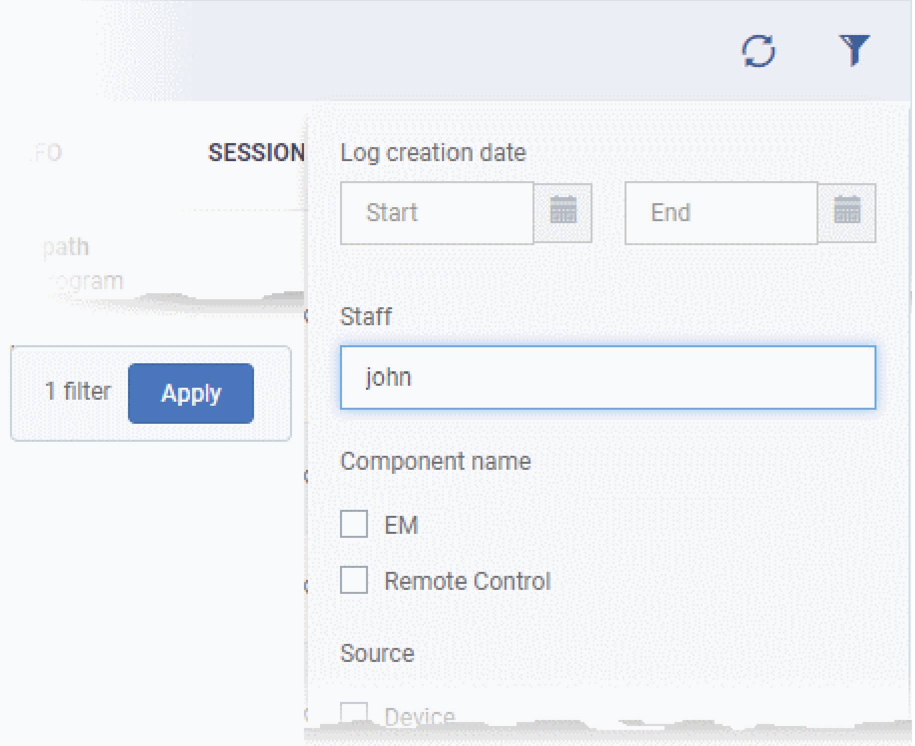
Extra info

Extra info

Session ID

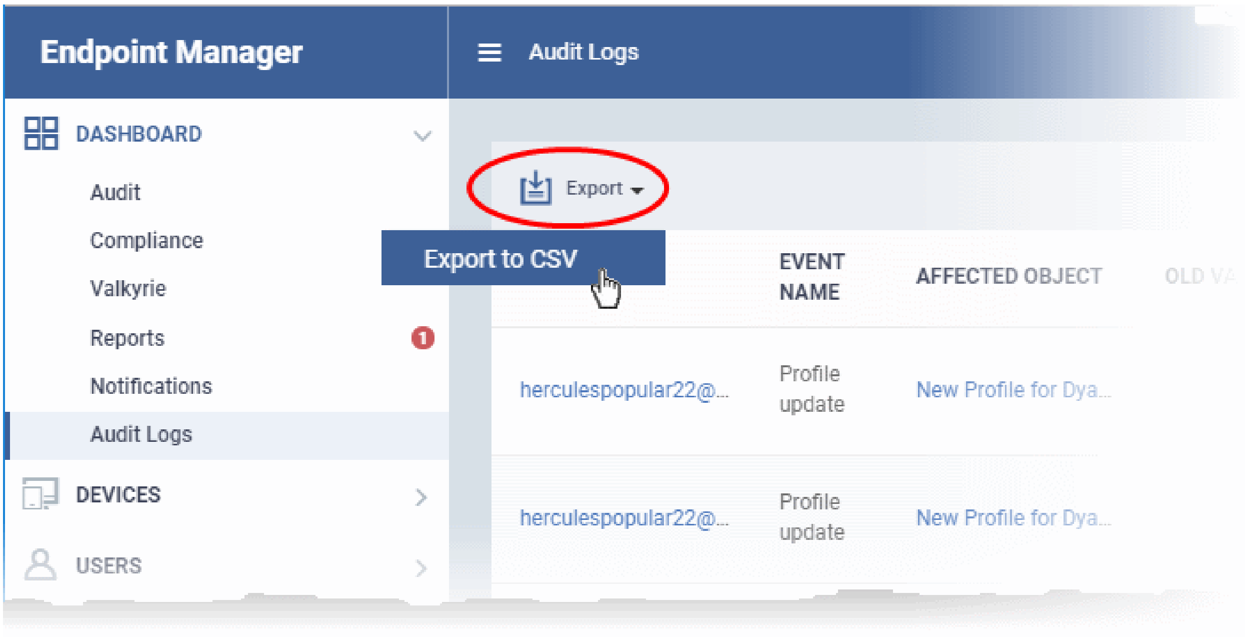
Session ID

- You can filter items by various criteria or search for specific events.
- Click 'Apply' to run your filter.



## Generate Audit Logs Reports

- Click 'Dashboard' > 'Audit Logs'.
- Click the funnel icon to filter which records are included in the report.
    - Click 'Export' above the table then choose 'Export to CSV'. You can export logs for up to the past 90 days (Day 1 - Day 90).



- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

# 4. Users and User Groups

- One of the first steps in setting up Endpoint Manager is to add users.
- Once you have added users, you can enroll the devices which belong to them. You can enroll iOS, Android, Windows, Mac OS and Linux devices.
- After enrolling a device, you can remotely manage and apply security policies to it. You can create user groups in order to apply policies to multiple devices.
- You can also assign users to a 'role'. A role determines what areas a user can access, and what tasks they can perform. You can assign users one of the built-in roles, or create a custom role with custom privileges.

There are two places you can add users to Endpoint Manager:

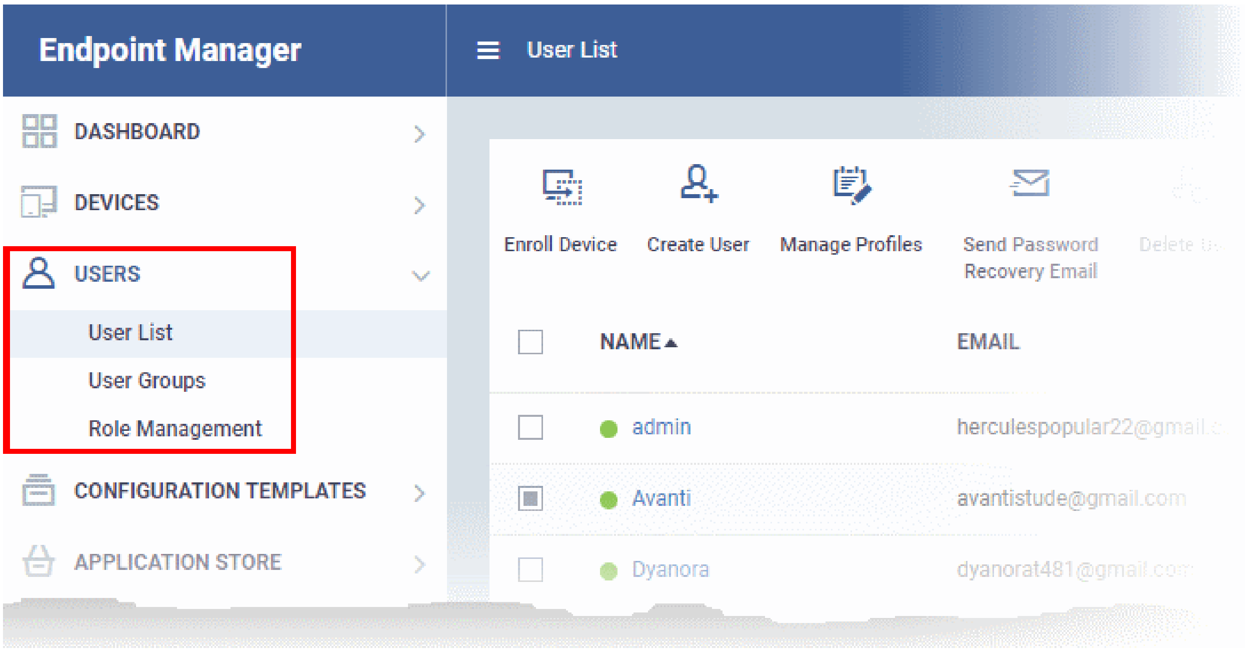
- The Comodo Dragon or Comodo One interface (preferred)
- The Endpoint Manager interface

Users added via Dragon / C1 will also be available in other modules like Service Desk and Quote Manager. Users added via Endpoint Manager will only be available in Endpoint Manager.

- Comodo Dragon Platform customers - See **https://help.comodo.com/topic-457-1-981-14319-Manage-Admins,-Staff-and-Roles.html** for details on how to add users via CD.
- Comodo One customers - See **https://help.comodo.com/topic-289-1-716-8482-Manage-Administrators-and-Roles.html** for details on how to add users via C1.

The following sections describe how to add users via the EM interface.

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



| ☐ | NAME ▲ | EMAIL |
|---|---|---|
| ☐ | ● admin | herculespopular22@gmail.c |
| ☒ | ● Avanti | avantistude@gmail.com |
| ☐ | ● Dyanora | dyanorat481@gmail.com |

The following sections explain more about each area:

- **Manage Users**
  - **Create New User Accounts**
    - **Manually Add Users**
    - **Import Users from a CSV file**
  - **Enroll Users' Devices for Management**
  - **View the Details of a User**
  - **Assign Configuration Profile(s) to a Users' Devices**

## 4.1. Manage Users

- Click 'Users' > 'User List'
- You can enroll users to EM and assign them roles with differing privilege levels (as 'administrators', 'technicians', 'users' or any other custom role).
- Devices belonging to users can only be enrolled after adding them to EM.
- Users can be added using any of the following methods:
  - Manually add user accounts
  - Import users from a comma separated values (.csv) file
  - Bulk enroll users and Windows endpoints from Active Directory (AD)

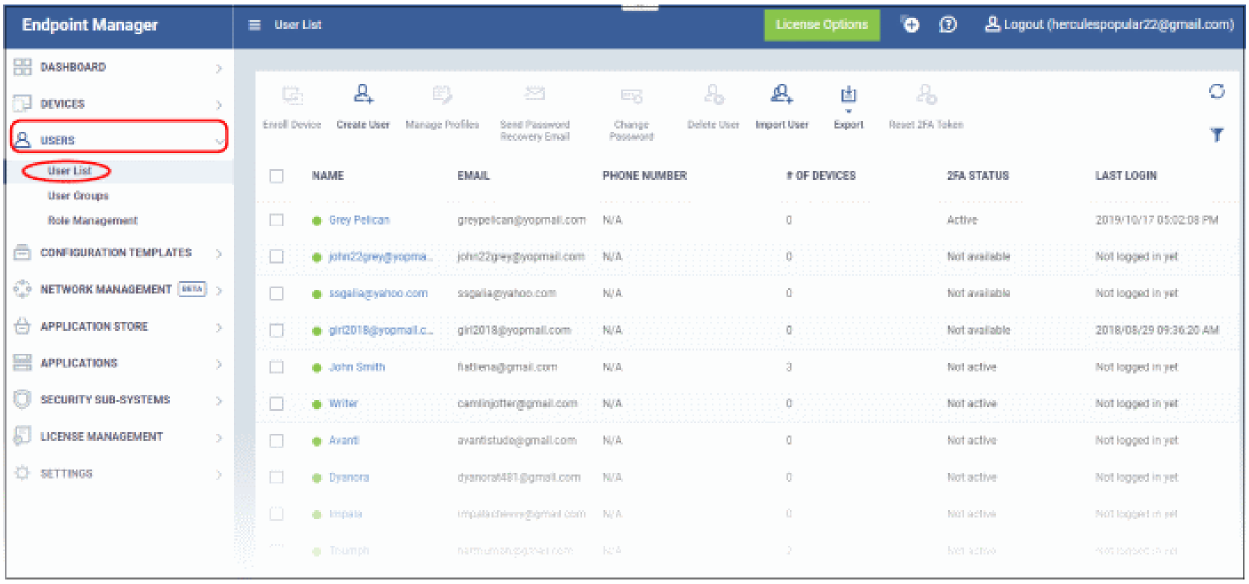
**Comodo Dragon customers** - Staff added in the CD interface are automatically added as users in EM.

See **https://help.comodo.com/topic-457-1-981-14319-Manage-Admins,-Staff-and-Roles.html** if you need help to add staff/ manage roles in CD.

**Comodo One** - Staff added in the C1 interface are automatically added as users in EM.

See **https://help.comodo.com/topic-289-1-716-8482-Managing-Administrators-and-Roles.html** if you need help to add staff/ manage roles in C1.

- The 'Users List' shows all user accounts that have been added to EM. Admins can add/manage users, enroll user devices, manage device configuration profiles and more.
- Click 'Users' > 'User List'



| NAME | EMAIL | PHONE NUMBER | # OF DEVICES | 2FA STATUS | LAST LOGIN |
|---|---|---|---|---|---|
| Grey Pelican | greypelican@yopmail.com | N/A | 0 | Active | 2019/10/17 05:02:08 PM |
| john22grey@yopma... | john22grey@yopmail.com | N/A | 0 | Not available | Not logged in yet |
| ssgalia@yahoo.com | ssgalia@yahoo.com | N/A | 0 | Not available | Not logged in yet |
| girl2018@yopmail.c... | girl2018@yopmail.com | N/A | 0 | Not available | 2018/08/29 09:36:20 AM |
| John Smith | fiatlena@gmail.com | N/A | 3 | Not active | Not logged in yet |
| Writer | camlinjotter@gmail.com | N/A | 0 | Not active | Not logged in yet |
| Avanti | avantistudo@gmail.com | N/A | 0 | Not active | Not logged in yet |
| Dyanora | dyanora481@gmail.com | N/A | 0 | Not active | Not logged in yet |
| Impala | impalachevy@gmail.com | N/A | 0 | Not active | Not logged in yet |
| Triumph | harmuman@gmail.com | N/A | 2 | Not active | Not logged in yet |

| Column Heading | Description |
|---|---|
| Name | The login username of the user.<br>• Click the username to view and edit user details. See '**View the Details of a User**' for more info. |
| Email | The registered email address of the user. Account activation and device enrollment mails are sent to this address. |
| Phone Number | The registered phone number of the user. |
| Number of Devices | The total number of devices enrolled for the user. |
| 2FA Status | Indicates whether two-factor authentication (2FA) is enabled or not.<br>• Active - Indicates 2FA is activated by the user<br>• Not active - Indicates 2FA is not yet configured by the user for the first time<br>• Not configured - Indicates 2FA was reset by admin and user is yet to re-configure it again.<br>• Not available - Indicates the user is added via C1 / Dragon portal. For these users, 2FA is done in the portal. |
| Last Login | Date and time that the user most recently accessed EM. |
| **Controls** | |
| Enroll Device | Add user devices for management by EM. You can enroll Android, iOS, Mac, Windows and Linux devices. See **Enroll User Devices for Management** for more details. |
| Create User | Manually add user accounts to EM.<br>• You can only add devices for users after you have enrolled the users themselves.<br>• Users can also be designated as administrators.<br>• See **Manually Add Users** for more details. |
| Manage Profiles | A profile determines the security configuration and network access rights of a device. See **Apply configuration profiles to devices** for more details. |

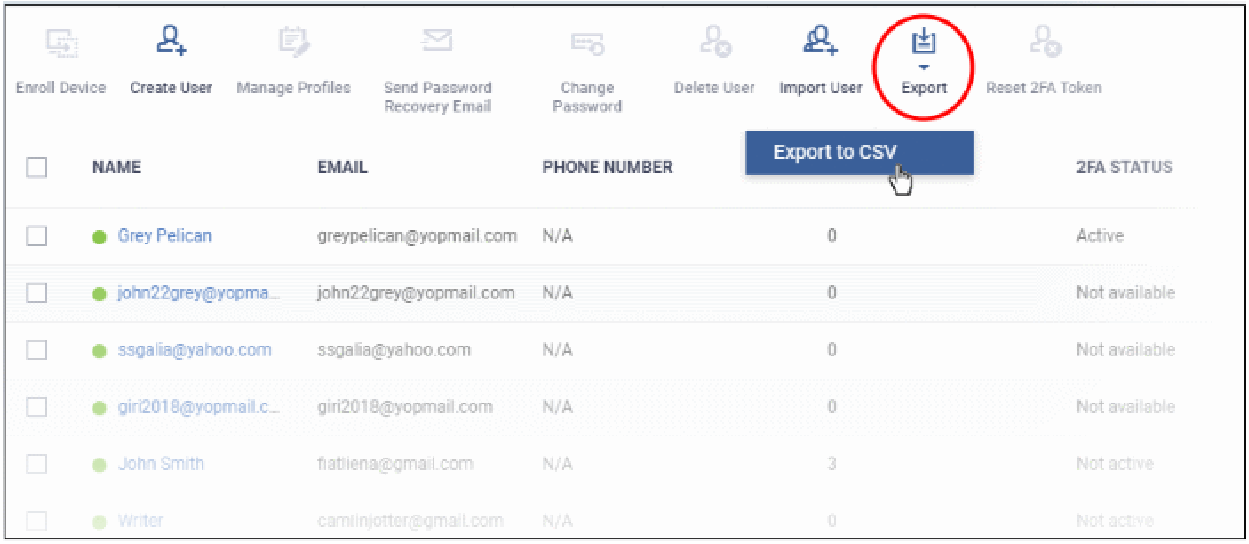
| | |
|---|---|
| Send Password Recovery Email | Reset the password of users who have admin privileges. The password allows them to login to the EM console. See **Send password recovery emails for users to access the EM console** for more details. |
| Change Password | Generate new password for a user. See **Generate New Password for a User** for more details. |
| Delete User | Terminate selected user accounts. See **Remove a User** for more details. |
| Import User | Add new users by importing them from a comma separated values (CSV) file. See **Import Users from a CSV File** for more help. |
| Export | Save a copy of the current user list as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of Users** for more details. |
| Reset 2FA Token | Force users to configure new two-factor authentication codes. See **Reset Two Factor Authentication Token for a User** for more details. |

## Sorting, Search and Filter Options

- Click any column header to sort items in ascending/descending order
- Click the funnel button at the right end to open the filter options.
- To display all items again, clear all filter fields and click 'OK'.
- By default, 20 search results are shown per page. Click the arrow next to 'Results per page' to increase the number up to a max of 200.

## Export the List of Users

- Click 'Users' > 'User List'.
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | NAME | EMAIL | PHONE NUMBER | | 2FA STATUS |
|---|---|---|---|---|---|
| □ | Grey Pelican | greypelican@yopmail.com | N/A | 0 | Active |
| □ | john22grey@yopma... | john22grey@yopmail.com | N/A | 0 | Not available |
| □ | ssgalia@yahoo.com | ssgalia@yahoo.com | N/A | 0 | Not available |
| □ | giri2018@yopmail.c... | giri2018@yopmail.com | N/A | 0 | Not available |
| □ | John Smith | fiatliena@gmail.com | N/A | 3 | Not active |
| □ | Writer | camlinjotter@gmail.com | N/A | 0 | Not active |

- The CSV file will be available in 'Dashboard' > 'Reports'

- See **Reports** in **The Dashboard** for more details.

Please use the following links to find out more:

- **Create New User Accounts**
  - **Manually Add Users**
  - **Import Users from a CSV File**
- **Enroll Users' Devices for Management**
  - **Enroll Android Devices**
  - **Enroll iOS Devices**
  - **Enroll Windows Endpoints**
  - **Enroll Mac OS Endpoints**
  - **Enroll Linux OS Endpoints**
- **View User Details**
  - **Update the Details of a User**
- **Assign Configuration Profile(s) to a User's Devices**
- **Remove a User**
- **Generate New Password for a User**
- **Reset Two Factor Authentication Token for a User**

## 4.1.1. Create New User Accounts

- You can add new accounts using any of the following methods:
  - **Manually add users**. Add individual users to EM
    - Click 'Users' > 'User List' > 'Create User' to start this process.
    - You need to specify their name, email address, the company they belong to, and their EM role.
    - See **Manually Add Users** if you need help with this.
  - **Import users from .csv file**. Import a list of users from a comma separated values file.
    - Click 'Users' > 'User Import' to start this process
    - The file should contain the following, separated values: 'Username' (mandatory), 'Email address' (mandatory) and 'Phone number' (optional).
    - The file should not contain column headers and each line should contain a single user.
    - Users are assigned the role you specify in the import dialog.
    - See **Import Users from a CSV File** if you need help with this
- New users will receive an enrollment mail which requests they activate their account and set their password.
- You can also bulk enroll users and Windows endpoints from Active Directory (AD) group policy. See **Bulk Enrollment of Devices** and '**Import User Groups from LDAP**' for more details.

**Comodo Dragon customers** - Staff added in the CD interface are automatically added as users in EM.

See **https://help.comodo.com/topic-457-1-981-14319-Manage-Admins,-Staff-and-Roles.html** if you need help to add staff/ manage roles in CD.

**Comodo One** - Staff added in the C1 interface are automatically added as users in EM.

See **https://help.comodo.com/topic-289-1-716-8482-Managing-Administrators-and-Roles.html** if you need help to add staff/ manage roles in C1.

**Device licenses**: User devices can only be enrolled after the user has been added to the system.

- Each device license covers one device per user
- You need an additional license for each mobile device or endpoint you add for the same user. You can purchase additional licenses from the Comodo website if required. See **View and Manage Licenses** for more details.

The following sections explain how to:

- **Manually add users**
- **Import users from a CSV file**

### 4.1.1.1. Manually Add Users

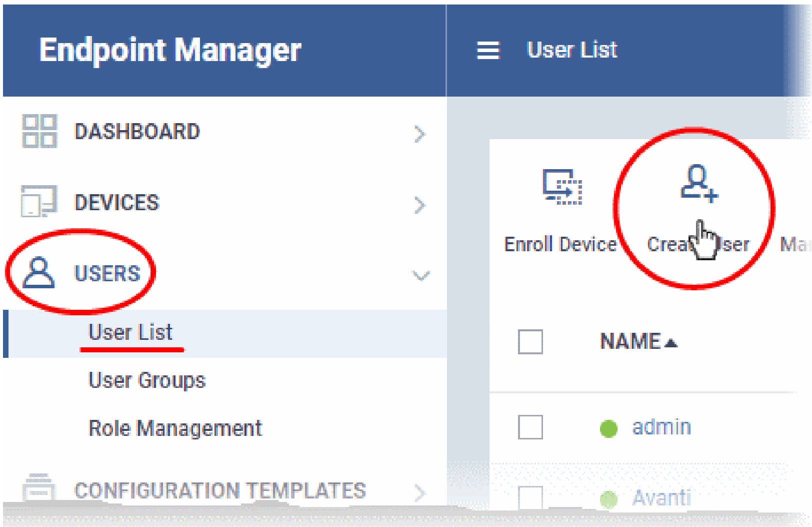
- Click 'Users' > 'User List' > 'Create User' button
- You can add new users by specifying their name, email address and other details.
- Once added, you can enroll Windows, Android, iOS, Mac OS and Linux devices for the user.
- New users with admin roles will receive an account activation email. They can login to Endpoint Manager after activating their account.

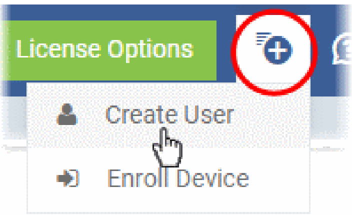
**Add a new user**

- Click 'Users' > 'User List'
- Click the 'Create User' button

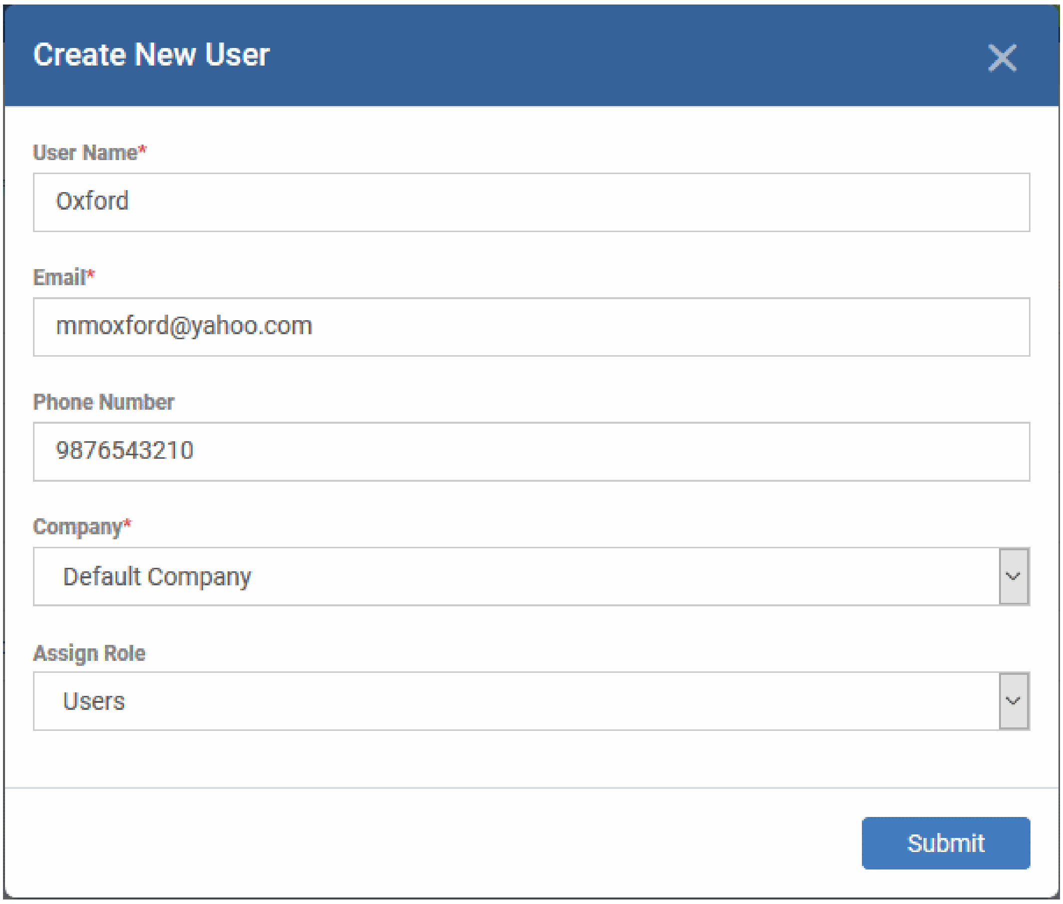
  or

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





The 'Create New User' appears:



Create New User

User Name*

Oxford

Email*

mmoxford@yahoo.com

Phone Number

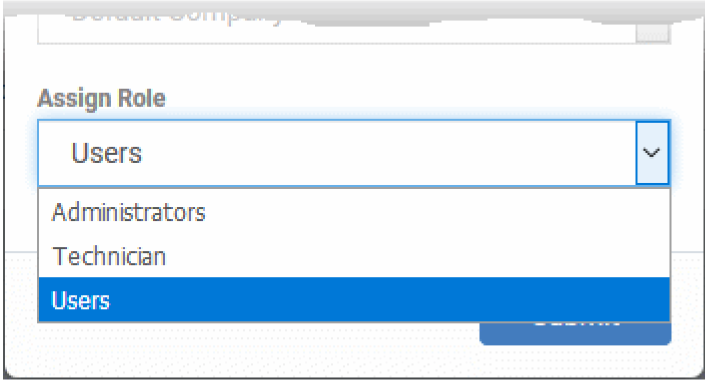
9876543210

Company*

Default Company

Assign Role

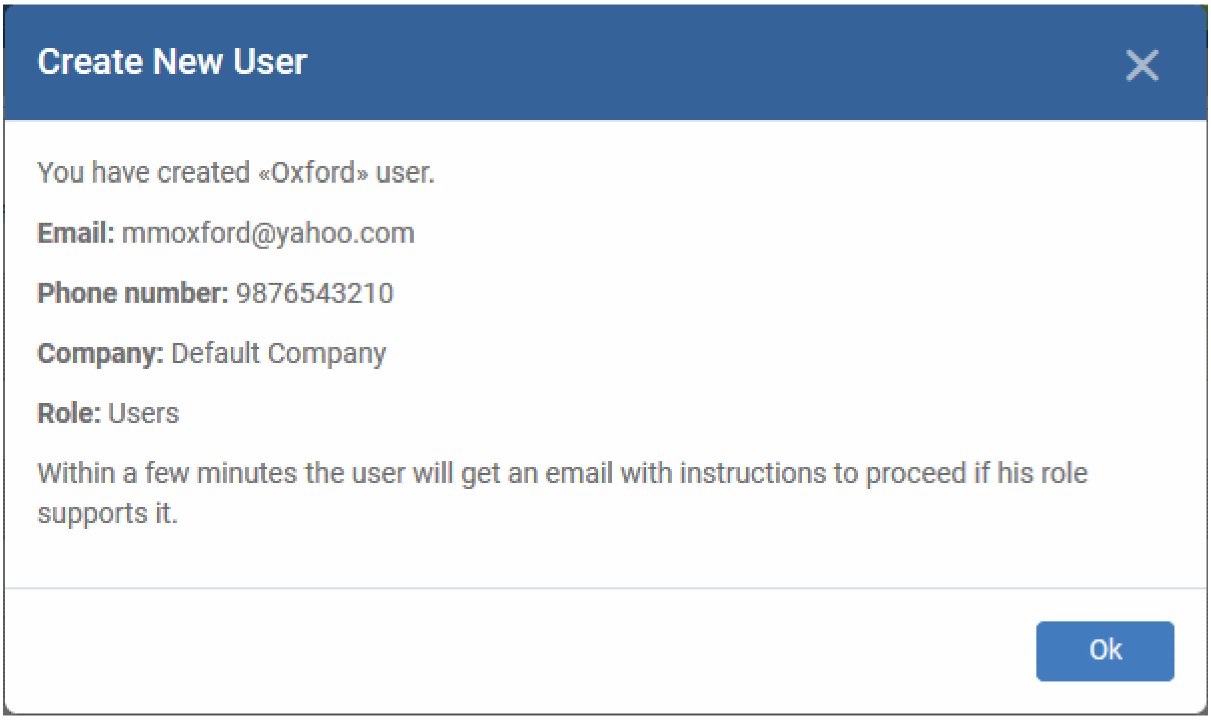
Users

| '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 email address of the user for registration to EM. 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 | The contact number of the user. |
| Company | Drop-down | Choose the company to which the user belongs.<br>• MSP customers can add users from any company they have added to their account.<br>• Enterprise and EM stand-alone customers can only add users to the default company. |
| Assign role | Drop-down | Select the role to be assigned to the new user from the 'Assign role' drop-down.<br><br> Assign Role<br>Users<br>Administrators<br>Technician<br>Users<br>EM ships with four default roles:<br>• Account Admin - Can login to EM and access all management interfaces. You cannot assign account admin to a user. The role is automatically assigned to the person who opened the Comodo Dragon or C1 account. This role is not editable.<br>• Administrators - Can login to EM and access all management interfaces. This role can be edited as required.<br>• Technician - Can login to EM and access all management interfaces. The technician role has fewer privileges than the administrator role. This role can be edited as required.<br>• Users - Cannot login to EM. If required, you can change role permissions to have access to the admin console. See **Configure Role Based Access Control for Users** for more details.<br>You can create custom roles which grant access to selected areas of EM. These roles can be assigned to users as required. All roles created in EM and CD or C1 will appear in the 'Assign Role' drop-down when adding a new user. See **Configure 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 in the 'Role Management' interface ('Users' > 'Role Management'). See **Managing Permissions and Assigned Users of a Role** if you need help with this.

A confirmation will be displayed:



Create New User

You have created «Oxford» user.

**Email:** mmoxford@yahoo.com

**Phone number:** 9876543210

**Company:** Default Company

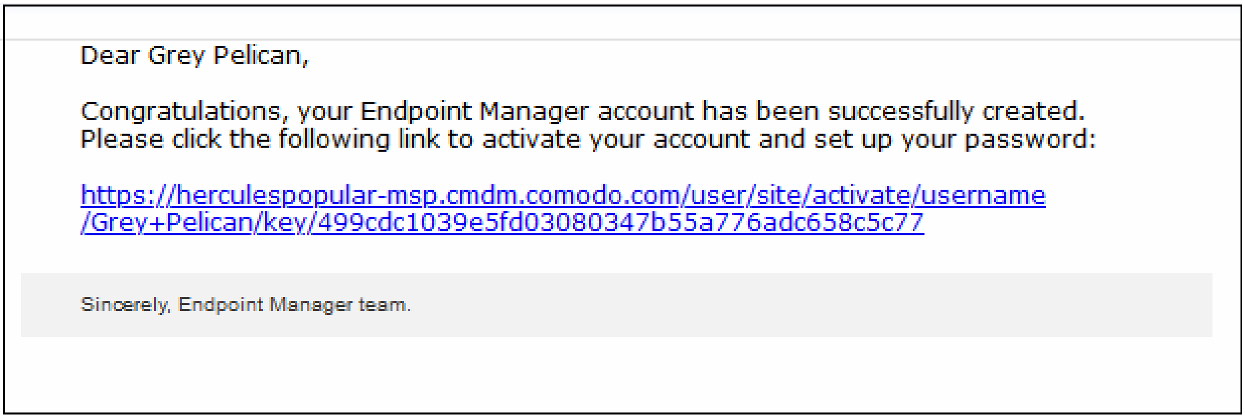
**Role:** Users

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

- Repeat the process to add more users.

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

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



Dear Grey Pelican,

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

https://herculespopular-msp.cmdm.comodo.com/user/site/activate/username/Grey+Pelican/key/499cdc1039e5fd03080347b55a776adc658c5c77

Sincerely, Endpoint Manager team.

- User clicks the link and activates his EM account.
- Upon activation, the user will be able to login to EM with his user-name and password. Login at: https://<*your company name*>-msp.cmdm.comodo.com/ as shown in the mail link.
- Users added via EM can login to EM console only and cannot login to Dragon / C1 portal.
- If the portal administrator has configured two-factor authentication, then the user has to follow the on-screen instructions to setup this during login.

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

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

### 4.1.1.2. Import Users from a CSV File

- Click 'Users' > 'User List' > 'Import User'
- You can load a list of new users by importing them from a comma separated values (CSV) file
- You can also specify the role to be assigned to all users in the list
- After adding a user, you can enroll Windows, Android, iOS, Mac OS and Linux devices for them

#### Process in brief

- Create a CSV file containing the list of users using spreadsheet applications like Microsoft Excel or OpenOffice Calc and save it on your admin computer
- The file should contain the following, separated values: 'Username' (mandatory), 'Email address' (mandatory) and 'Phone number' (optional).
- The file should not contain column headers and each line should contain a single user.
- In the EM admin console, click 'Users' > 'User List' > 'Import User'
- Browse to and select the CSV file you want to import
- Select a company and a role for the imported users
- Upload the file
- The users will be imported and enrolled to EM

#### Requirements for .csv file

There are two mandatory fields and one optional field per user account:

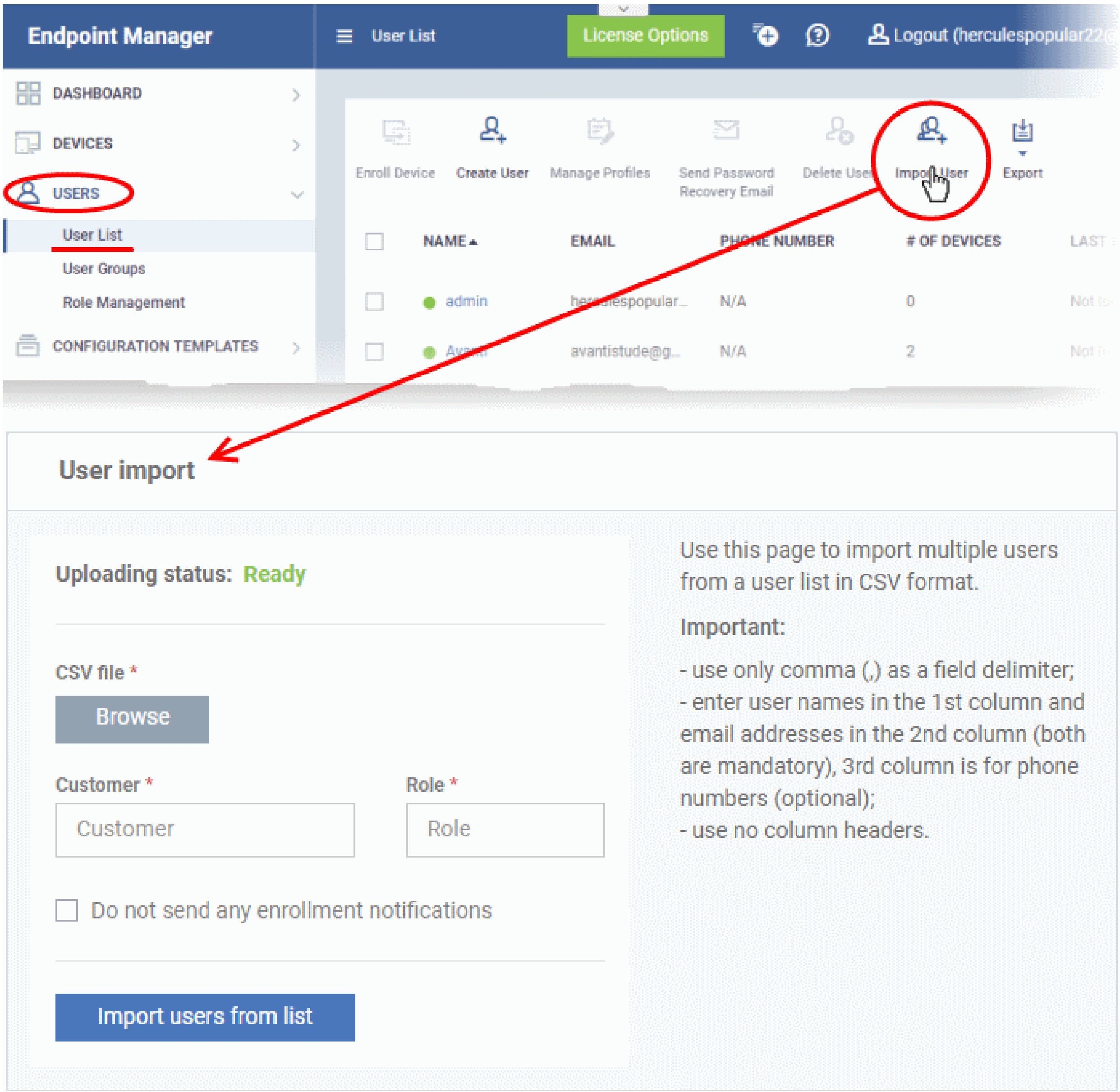
  - Username (mandatory)
  - Email address (mandatory)
  - Phone number (optional)
- Each line in the CSV file should contain one user entry
- The CSV file should not contain column headers

Example:

"james", "james@ditherscons.com", "9876543210"

**To import users from a list**

- Click 'Users' > 'User List'
- Click 'Import User' on the top



User import

Uploading status: Ready

CSV file *

Customer * Customer

Role * Role

□ Do not send any enrollment notifications

Use this page to import multiple users from a user list in CSV format.

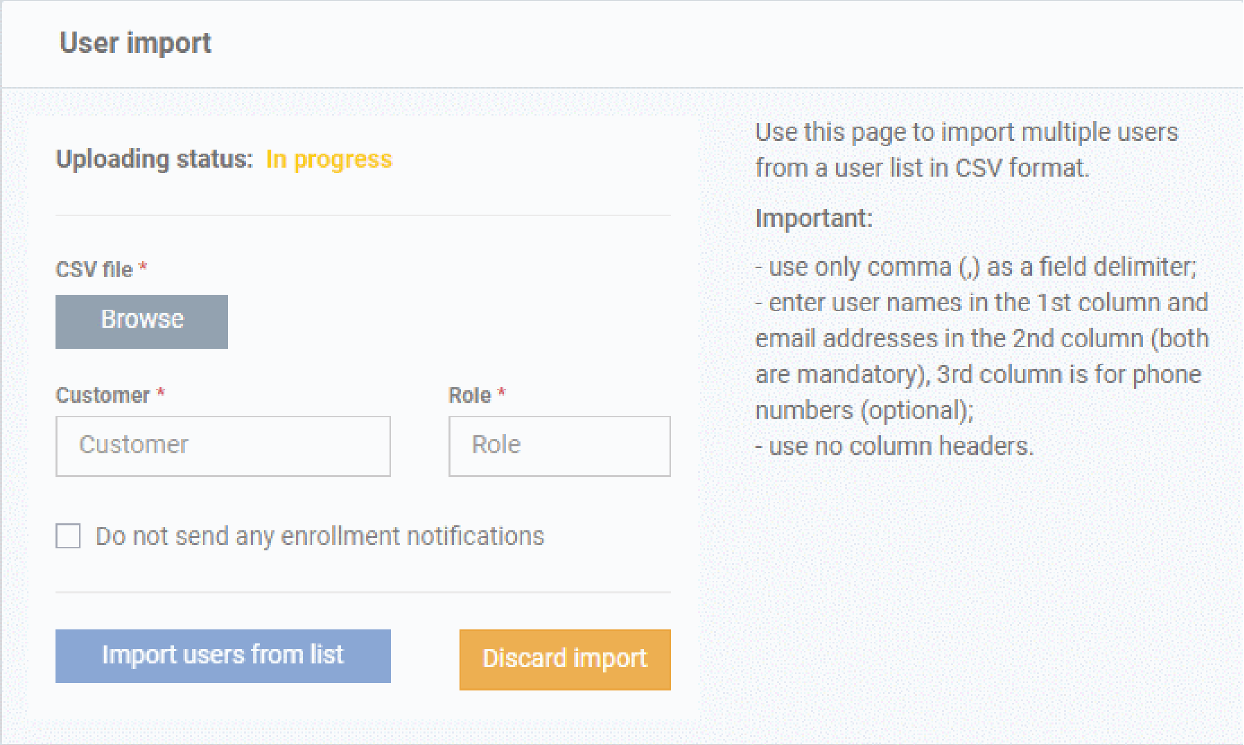
Important:

- use only comma (,) as a field delimiter;
- enter user names in the 1st column and email addresses in the 2nd column (both are mandatory), 3rd column is for phone numbers (optional);
- use no column headers.

| 'User Import' Form - Table of Parameters | |
|---|---|
| **Parameter** | **Description** |
| CSV File | Click 'Browse' navigate to the location of the CSV file and select the file |
| Company | The company to which the users belongs.<br>• Comodo Dragon MSP and Comodo One MSP customers can add users from Companies/Organizations enrolled in their account.<br>• Start entering first few letters of the company name and select the company from the options<br>• Comodo Dragon Enterprise, Comodo One Enterprise and EM stand-alone customers can only add users to the default company.<br>• Enter 'Default Company' in the Company field |
| Role | The role to be assigned to all users in the list.<br>• Start entering first few letters of the name of the role and select the role from the options |

| | |
|---|---|
| | EM ships with four default roles:<br>• Account Admin - Can login to EM and access all management interfaces. You cannot assign account admin to a user. The role is automatically assigned to the person who opened the Comodo Dragon or C1 account. This role is not editable.<br>• Administrators - Can login to EM and access all management interfaces. This role can be edited as required.<br>• Technician - Can login to EM and access all management interfaces. The technician role has fewer privileges than the administrator role. This role can be edited as required.<br>• Users - Cannot login to EM. If required, you can change role permissions to have access to the admin console. See **Configure Role Based Access Control for Users** for more details.<br>You can create custom roles which grant access to selected areas of EM. These roles can be assigned to users as required. All roles created in EM and CD or C1 will appear in the 'Role' drop-down when importing new users. See **Configure Role Based Access Control for Users** for more details. |
| Do not send any enrollment notifications | Select whether or not the account creation notification mail or account activation mail is to be sent to the imported users.<br>Note: The notification mails will not be sent if you select 'Users' role for the new users. |

- Configure the parameters and click 'Import users from List'



User import

Uploading status: In progress

CSV file *

Customer *

Role *

□ Do not send any enrollment notifications

Use this page to import multiple users from a user list in CSV format.

Important:

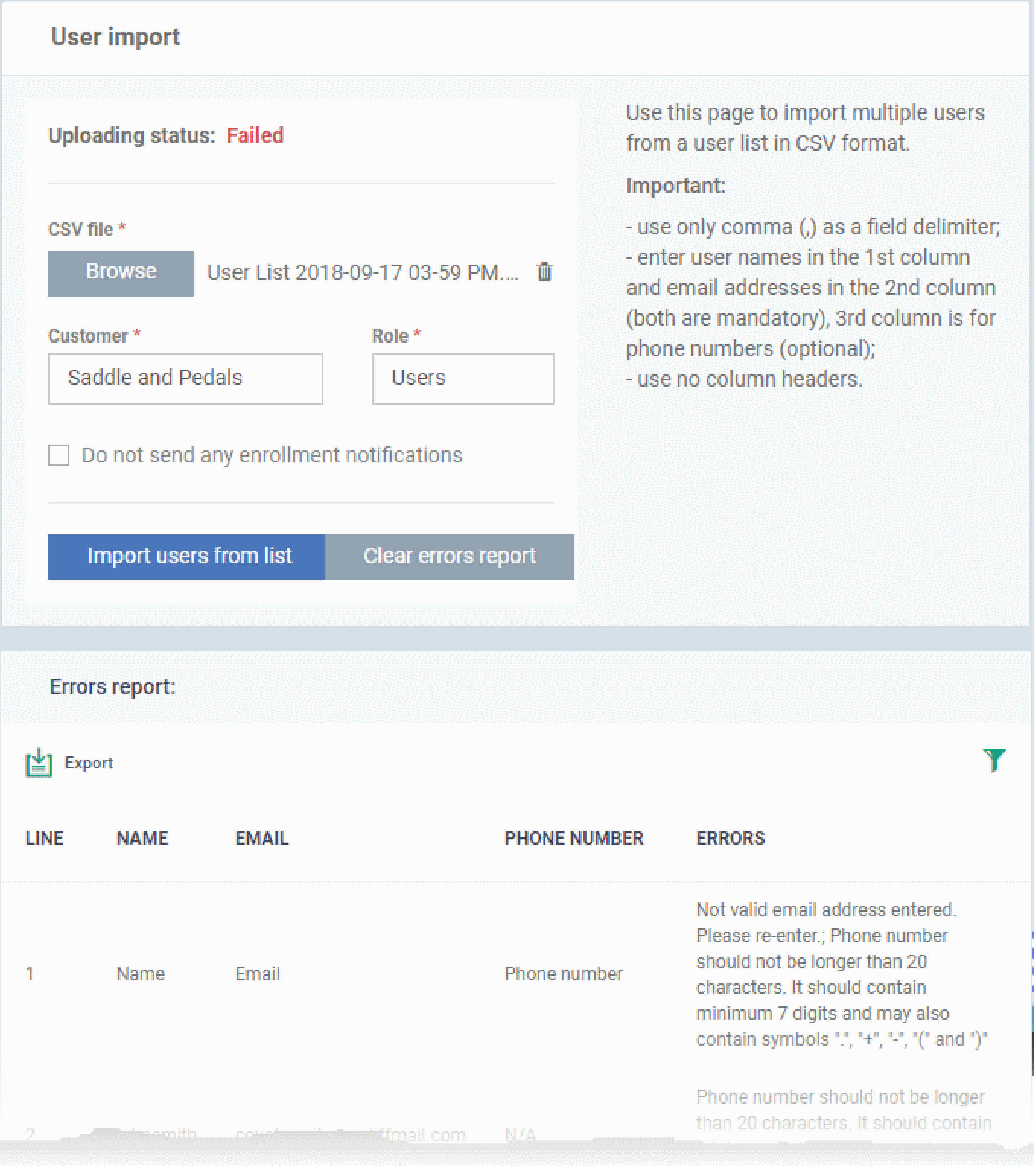
- use only comma (,) as a field delimiter;
- enter user names in the 1st column and email addresses in the 2nd column (both are mandatory), 3rd column is for phone numbers (optional);
- use no column headers.

The progress will be displayed.

- If you want to stop the import process, click 'Discard Import'
- Once the users have been imported, you can enroll devices for them.
- Users will receive an account activation mail if they are assigned a role that has access to the admin console. This includes the standard ' Administrator' and 'Technician' roles.

- Tip - Enable 'Do not send any enrollment notifications' in the import screen if you do not want to send these mails.

- Users click the link in the mail to activate their account and configure their password.
- You will receive an error report if the import fails. See the following screenshot:



User import

Uploading status: Failed

CSV file *

Browse | User List 2018-09-17 03-59 PM....

Customer *: Saddle and Pedals

Role *: Users

□ Do not send any enrollment notifications

Import users from list | Clear errors report

Use this page to import multiple users from a user list in CSV format.

Important:

- use only comma (,) as a field delimiter;
- enter user names in the 1st column and email addresses in the 2nd column (both are mandatory), 3rd column is for phone numbers (optional);
- use no column headers.

Errors report:

Export

| LINE | NAME | EMAIL | PHONE NUMBER | ERRORS |
|---|---|---|---|---|
| 1 | Name | Email | Phone number | Not valid email address entered. Please re-enter.; Phone number should not be longer than 20 characters. It should contain minimum 7 digits and may also contain symbols ".", "+", "-", "(" and ")" |
| 2 | smith | tiffmail.com | N/A | Phone number should not be longer than 20 characters. It should contain |

- The report can help pinpoint errors so you can rectify them.
  - Click 'Export' to download the error report in .csv format
  - Click 'Clear errors report' to remove the report and retry the import.

## 4.1.2. Enroll User Devices for Management

You need to enroll devices to Endpoint Manager in order to manage those devices going forward. Reminder - you must first have **added users** before you can add their devices.

- Click 'Users' > 'User List' > select users > click 'Enroll Device'.
- Complete the wizard to send device enrollment mail to your users. Users must open the mail on the device itself. See the tutorial below.
- The mail contains an enrollment token. Multiple devices can be enrolled with the same token by the user simply responding to the mail from each device. Each token is valid for 90 days.
- Each license covers one device per user. You will need additional licenses for each device you add for a user. See **Manage Licenses** if you need help with this.
- You can also bulk enroll users and Windows endpoints by creating a software installation policy in Active Directory (AD). See **Enroll Windows Devices Via AD Group Policy** and '**Import User Groups from LDAP**' for more details.
- You can also enroll iOS devices using your Apple DEP account. See '**Integrate Apple DEP with Endpoint Manager**'
- This section explains how to enroll devices for multiple users

**Tutorial**

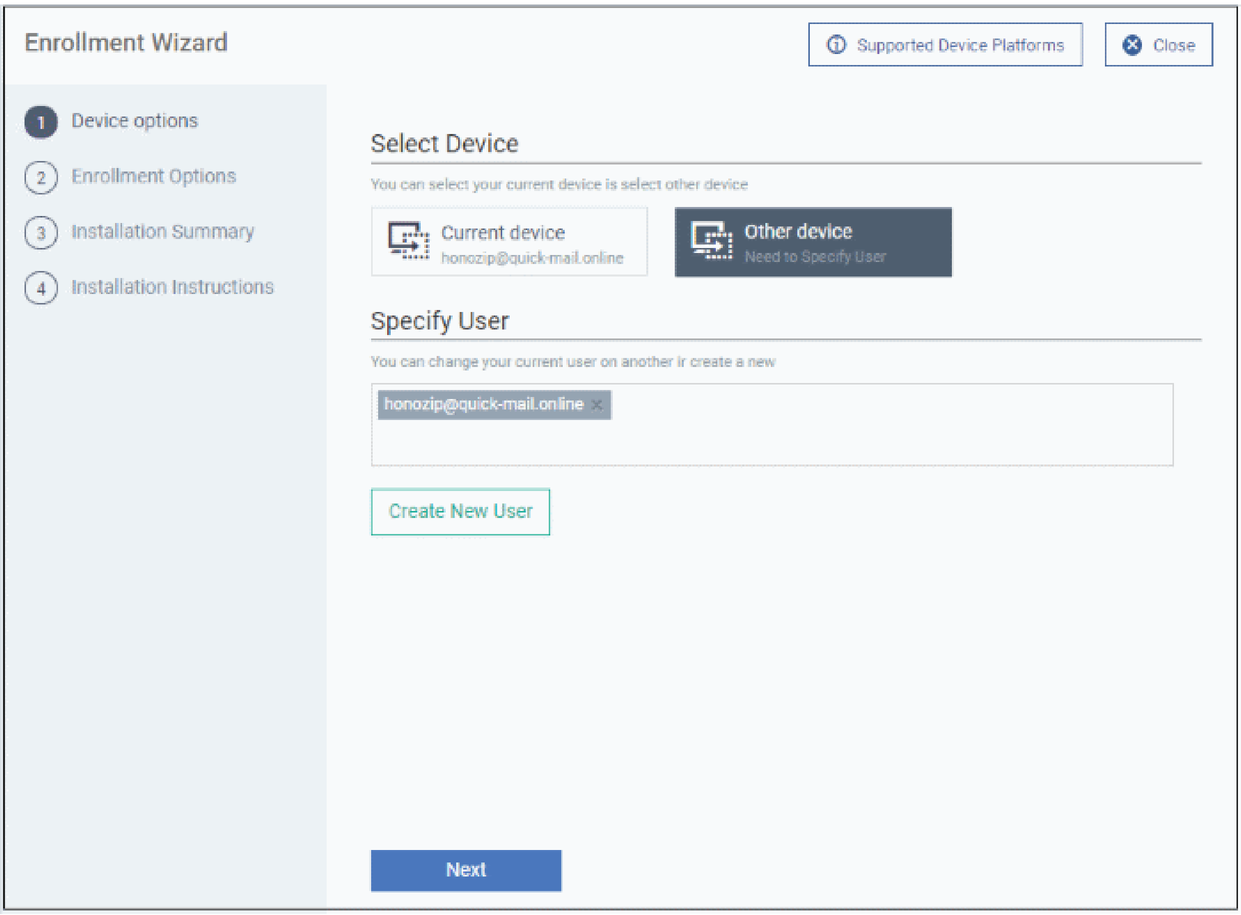
- Click 'Users' > 'User List' on the left
- Select the users for whom you want to add devices

  Or
- Click the 'Add' button ⊕ on the menu bar then 'Enroll Device'.

This starts step 1 of the device enrollment wizard:

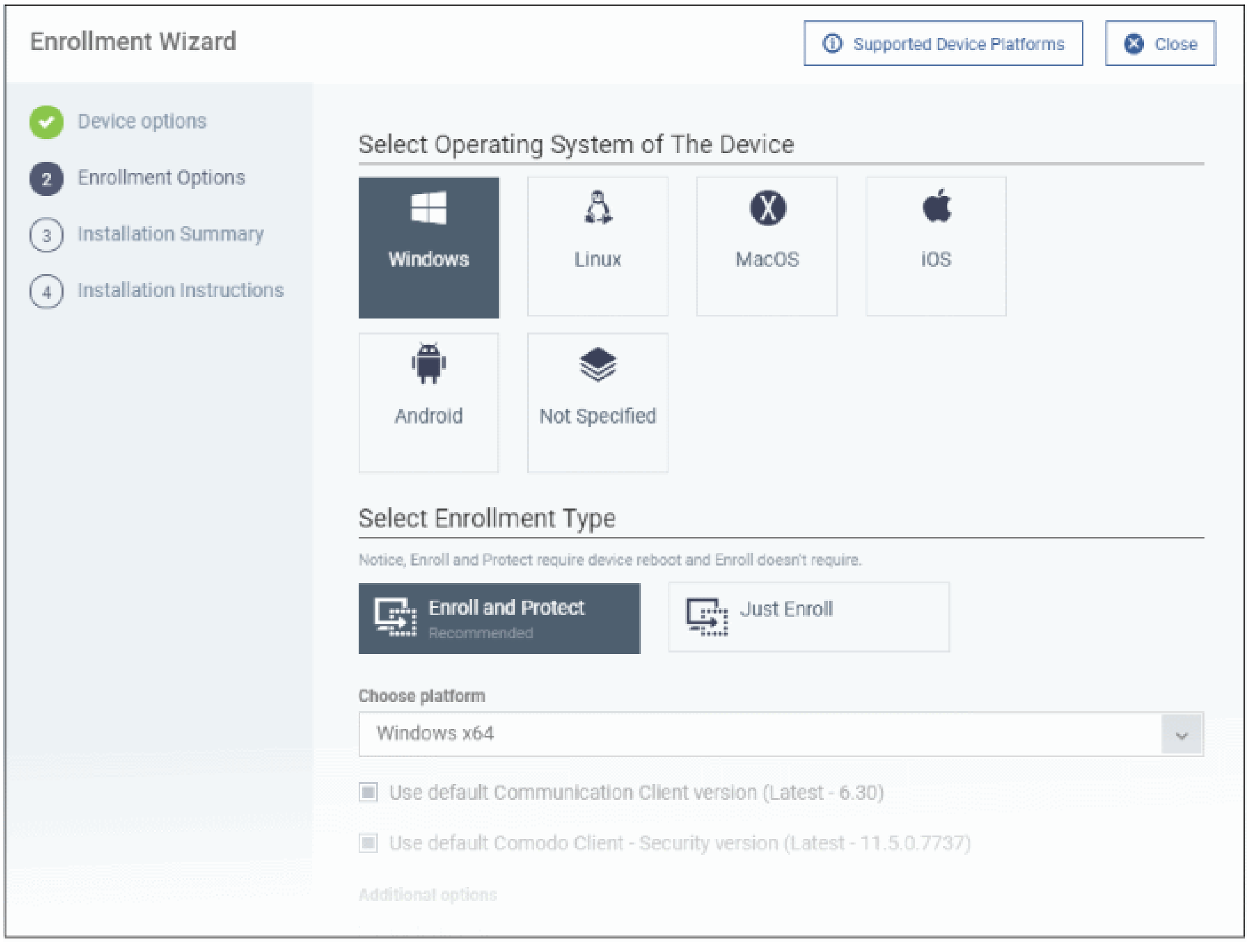
**Step 1 - Device Options**

- **Current device -** Enrolls the device you are currently using. You may disregard this option at this stage as we are adding multiple devices with the 'Other device' option.
- **Other device -** Add devices owned by the users you selected previously. Those users should already be listed in the 'Specify User' box:


Enrollment Wizard
Supported Device Platforms
Close
1 Device options
2 Enrollment Options
3 Installation Summary
4 Installation Instructions
Select Device
You can select your current device is select other device
Current device
honozip@quick-mail.online
Other device
Need to Specify User
Specify User
You can change your current user on another ir create a new
honozip@quick-mail.online
Create New User
Next

- You can add additional, existing users by simply typing their email address in the box. Endpoint Manager will auto-suggest users that have already been created.
- **Create New User -** Click if you want to add a new user to Endpoint Manager. You cannot add devices unless you have first added the users that own them. The add-user process is explained **here**.
- Click 'Next' to proceed to step 2.

**Step 2 - Enrollment Options**



Notice, Enroll and Protect require device reboot and Enroll doesn't require.

Choose platform: Windows x64

☐ Use default Communication Client version (Latest - 6.30)

☐ Use default Comodo Client - Security version (Latest - 11.5.0.7737)

**TLDR -**

- Click 'Not Specified' if you only want to install the communication client on target devices. The wizard will detect the target operating system and send the appropriate client to the device user.
- Click one of the operating system tiles if you also want to install the security client. Make sure the target devices use the operating system you selected.

There are two broad ways you can enroll devices:

**Option 1 - Enroll + Protect - Single Operating System**

- Click one of the operating system boxes to enroll devices of that type. Please make sure all your target devices use this operating system.
- The wizard will send enrollment mails that only provision the OS you choose. For example - If you select the 'Windows' box, then the wizard will send enrollment mails which only contain download links for the Windows clients.
- Once you have chosen the OS, you can customize enrollment options as required. You can configure items such as enrollment type, reboot policy, client version, configuration profile and device name.

**Option 2 - Enroll Only - Multiple Operating Systems**

- Click the 'Not Specified' box. This option installs only the communication client, and doesn't install the security client.
- Your target devices can be a mix of operating systems rather than a single OS. This option auto-detects the OS of the device and emails the appropriate client link to the user.

- The latest version of the communication client is installed on each device. The MDM profile is installed on MAC devices
- Note - You can use this option to quickly connect devices to Endpoint Manager, then go back later and install the security client if required.

**Enrollment Type**

Applies to Windows, Mac and Linux devices.

- **Enroll and Protect** - Installs both the communication client and the security client.
- **Just Enroll** - Installs only the communication client

Background. There are two types of client:

- **Communication Client** - Connects the device to Endpoint Manager for central management. It is mandatory to install this client.
- **Security Client** - This is the security software. Depending on the operating system, it includes antivirus, firewall, threat-containment, web-filtering, and more. It is optional to install this client.

Click 'Next' to **skip to step 3** if you are happy with your choices on this page.

OR

Use the following links to read more about the various settings per OS:

- **Windows**
- **Linux**
- **Mac OS**
- **iOS / Android**

**Windows**

| Setting | Description |
|---|---|
| Choose platform | Select Window OS version. 64 bit, 32 bit, or hybrid.<br>The hybrid package will auto-detect and install the correct version. |
| Use default Communication Client version | This client enrolls the endpoint for central management.<br>• You can only change the CCC version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed. |
| Use default Communication Client Security version | This client installs security software such as antivirus, firewall and auto-containment.<br>• You can only change the CCS version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed. |
| Additional options | **AV Database** - Choose whether to include the latest virus database with the installation package. This increases the size of the package.<br>If disabled, the client will download the latest database anyway when you run the first virus scan. |
| Configuration Profile | A configuration profile is a collection of settings which specify a device's network access rights, security settings, antivirus scan schedule, and more. |

| | |
|---|---|
| | The default is 'Windows - Security Level 1' profile. Choose a different profile if required.<br>• The default profile is recommended for most users and can always be changed later if required.<br>• If you want to change it, type the first few characters of a profile name and choose from the suggestions that appear.<br>• You can view the settings in a profile at 'Configuration Templates' > 'Profiles'. |
| Set Reboot Options | Endpoints need to be restarted to complete CCS installation. You have the following restart options:<br>• **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message is shown to the user prior to the restart.<br>• **Suppress reboot -** Endpoint is not auto-restarted. The installation is finalized when the user next restarts the endpoint.<br>• **Warn about reboot and let users postpone it -** Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.<br>Optional. Type a custom message in the 'Reboot Message' field. |
| Device Name Options | • Do Not Change - The device's existing name is used to identify the device in Endpoint Manager.<br>• Change - Enter a new device name. Note - You can restore the original name from the device list screen if required. |

- Click 'Next' to proceed to step 3

**Linux**

| Setting | Description |
|---|---|
| Choose platform | Select Linux OS version<br>• Ubuntu / Debian (Hybrid Package)<br>• RHEL / CentOS (Hybrid Package)<br>• 'Hybrid' just means the package is suitable for both types of OS. |
| Device Name Options | • Do Not Change - The device's existing name is used to identify the device in Endpoint Manager.<br>• Change - Enter a new device name. Note - You can restore the original name from the device list screen if required. |

- Click 'Next' to proceed to step 3

**MacOS**

| Setting | Description |
|---|---|

| | |
|---|---|
| Select Method | • With MDM profile (recommended) - Installs both the communication client and the Endpoint manager configuration profile. You can use the full suite of Endpoint Manager tools on your devices<br>• Without MDM profile - Installs only the communication client for connection to EM. 'Profile-less' enrollment lets you use Endpoint Manager to manage security while using another platform for general Mac management. |
| Device Name Options | • Do Not Change - The device's existing name is used to identify the device in Endpoint Manager.<br>• Change - Enter a new device name. Note - You can restore the original name from the device list screen if required. |

- Click 'Next' to proceed to step 3

**iOS / Android**

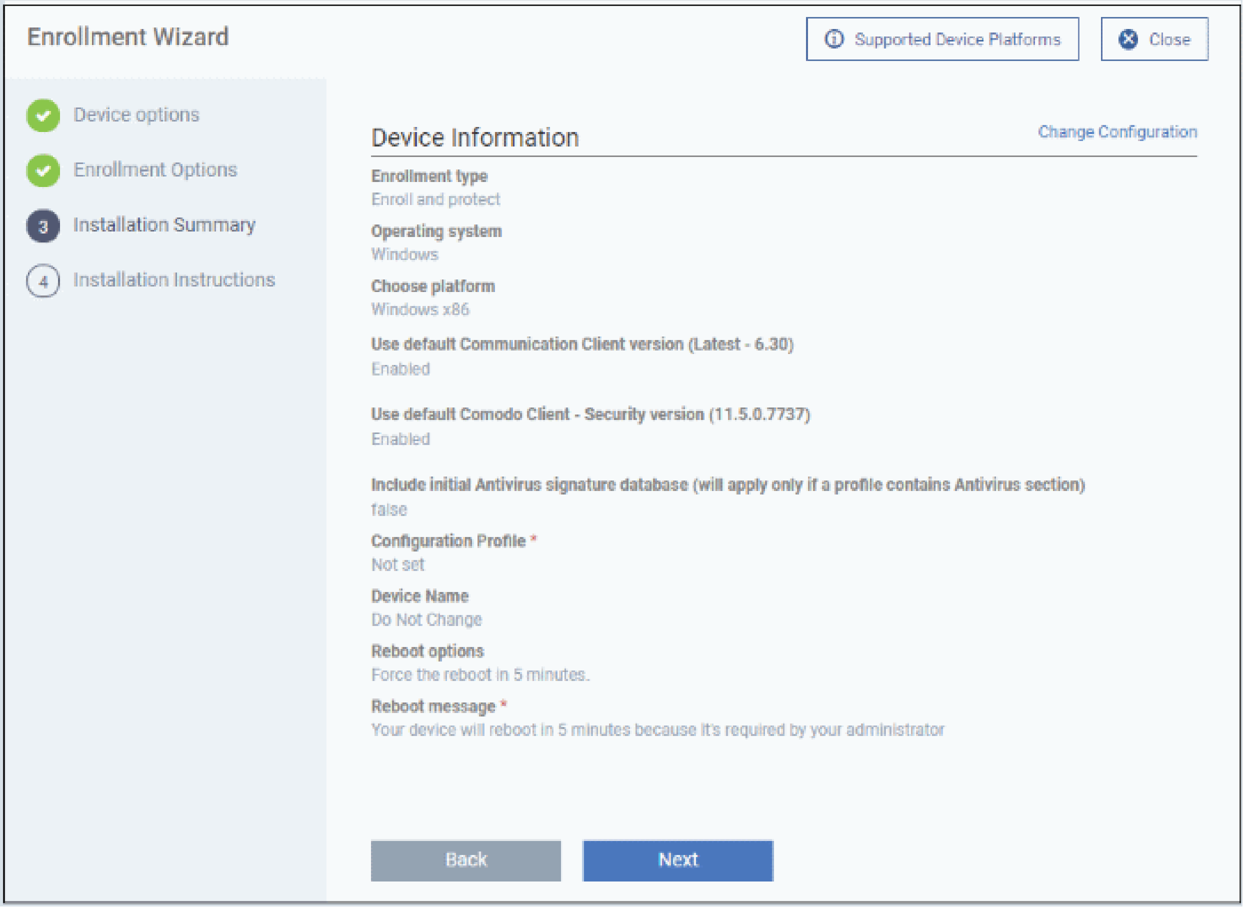
**Device Name Options**:

- **Do Not Change -** The device's existing name is used to identify the device in Endpoint Manager.
- **Change -** Enter a new device name. Note - You can restore the original name from the device list screen if required.
- Click 'Next' to proceed to step 3

**Step 3 - Installation Summary**

Review your choices so far.

The summary you see depends on the operating system and enrollment type:



Device Information

Enrollment type
Enroll and protect

Operating system
Windows

Choose platform
Windows x86

Use default Communication Client version (Latest - 6.30)
Enabled

Use default Comodo Client - Security version (11.5.0.7737)
Enabled

Include initial Antivirus signature database (will apply only if a profile contains Antivirus section)
false

Configuration Profile *
Not set

Device Name
Do Not Change

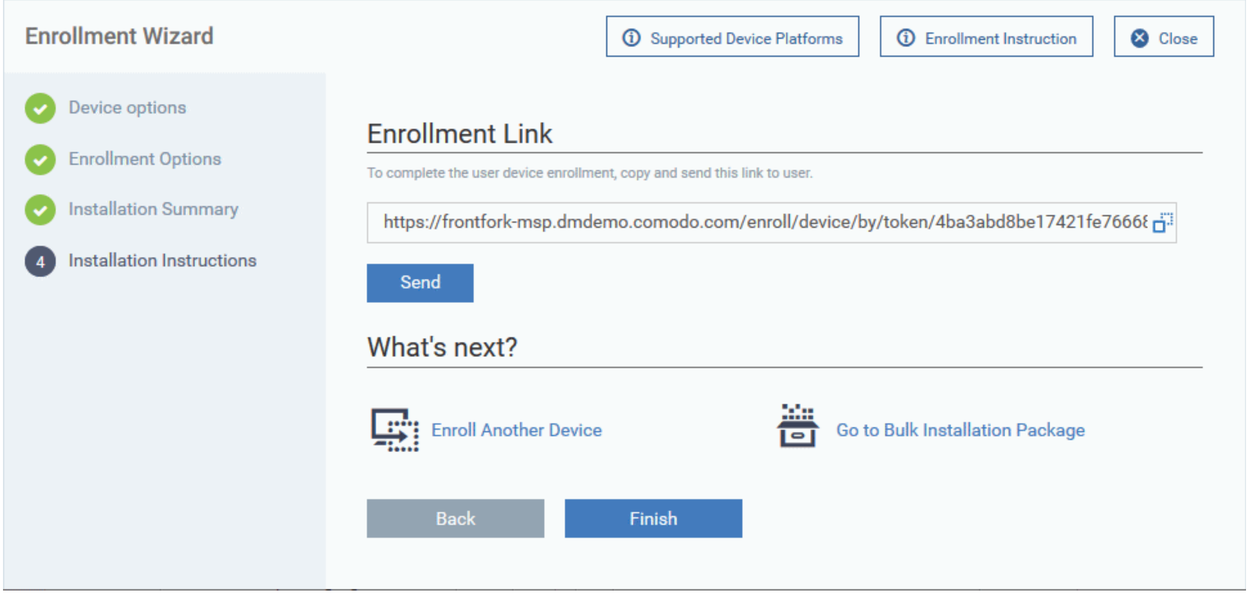
Reboot options
Force the reboot in 5 minutes.

Reboot message *
Your device will reboot in 5 minutes because it's required by your administrator

- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4

### Step 4 - Installation Instructions

The final step is to send out the enrollment emails to the device owners:



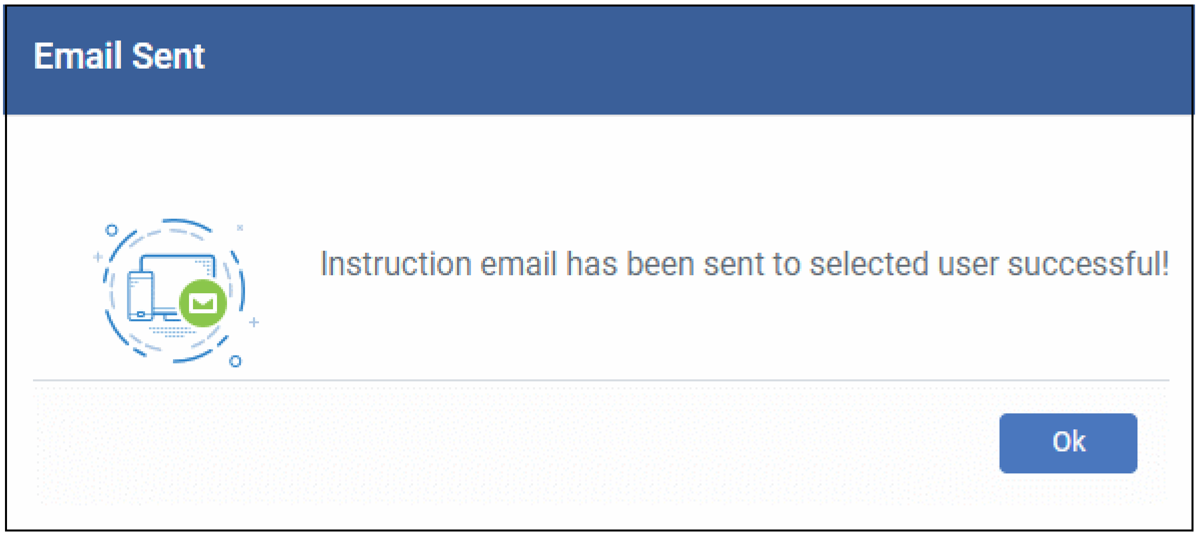
Enrollment Link

To complete the user device enrollment, copy and send this link to user.

https://frontfork-msp.dmdemo.comodo.com/enroll/device/by/token/4ba3abd8be17421fe7666

What's next?

- **Send -** Click this to send enrollment mails to users with the settings you choose in steps 1, 2 and 3.



Email Sent

Instruction email has been sent to selected user successful!

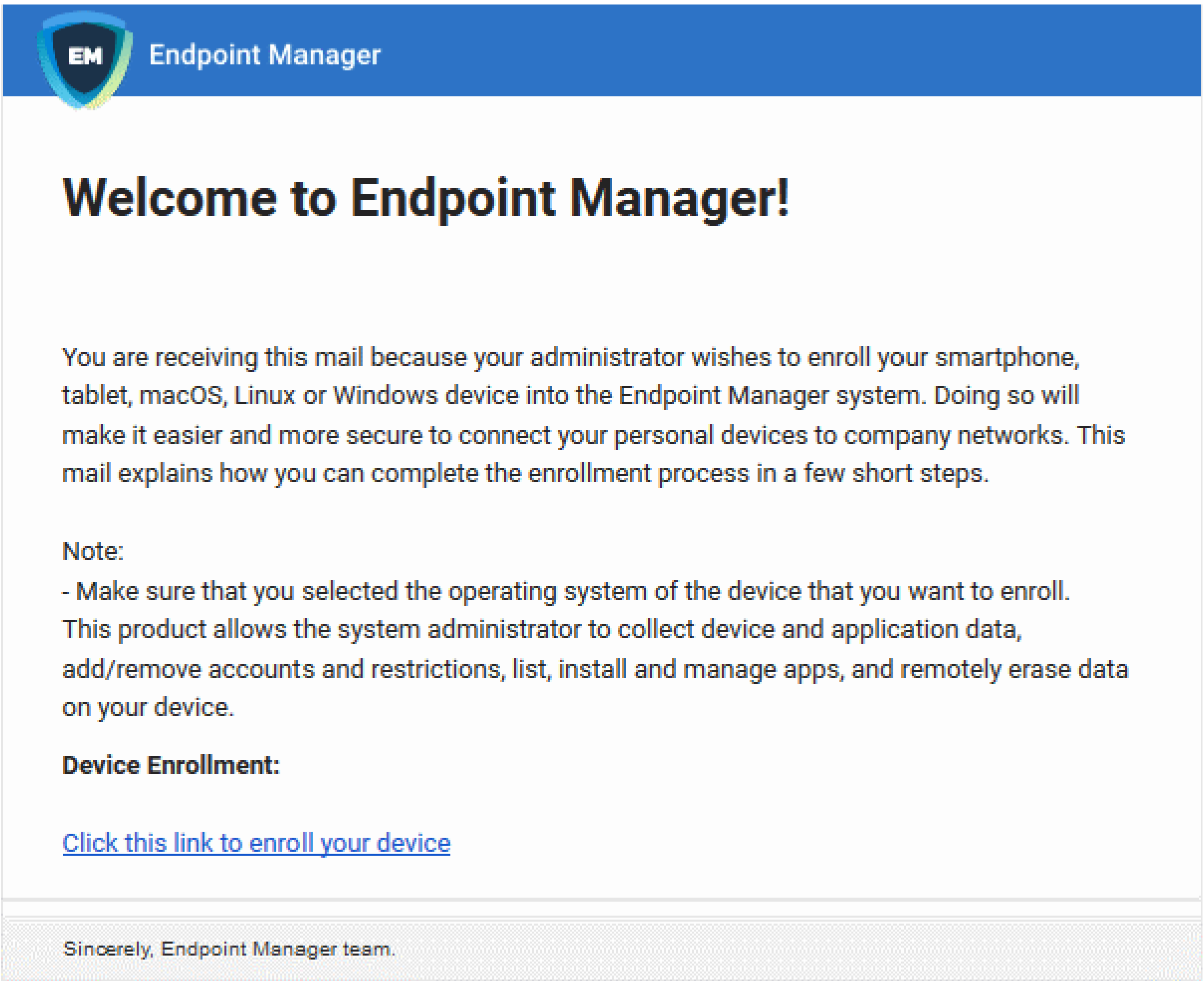
    - **Enroll Another Device -** Takes you back to step 1
    - **Go to Bulk Installation Package -** Takes you to bulk installation package screen to configure and enroll users in bulk. See '**Bulk Enrollment of Devices**'

- Click 'Finish' to close the window.

Note - If you chose 'Current Device' in step 1, then you can enroll your device in two ways:

1. Download the client in the final step. Follow the instructions and complete the enrollment procedure.
2. Click 'Enrollment Instructions' at top-right, click the appropriate enrollment link to your device and complete the procedure.

An example mail that is sent to users is shown below:



Welcome to Endpoint Manager!

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

Note:
- Make sure that you selected the operating system of the device that you want to enroll.
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

**Device Enrollment:**

Click this link to enroll your device

Sincerely, Endpoint Manager team.

- Clicking the link will take the user to a page which lets them download the appropriate communication client/profile:

**Tip**: Here's two other ways you can enroll devices for users:

- Click 'Users' > 'User List' > click the name of a user to open their details screen > click 'Enroll Device'
- Click 'Devices' > 'Device List' > 'Enroll Device'

The following sections contain help per device operating system:

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

**Note** - See **Appendix 1** for a list of ports that Endpoint Manager uses to communicate with endpoints and Comodo servers.

### 4.1.2.1. Enroll Android Devices

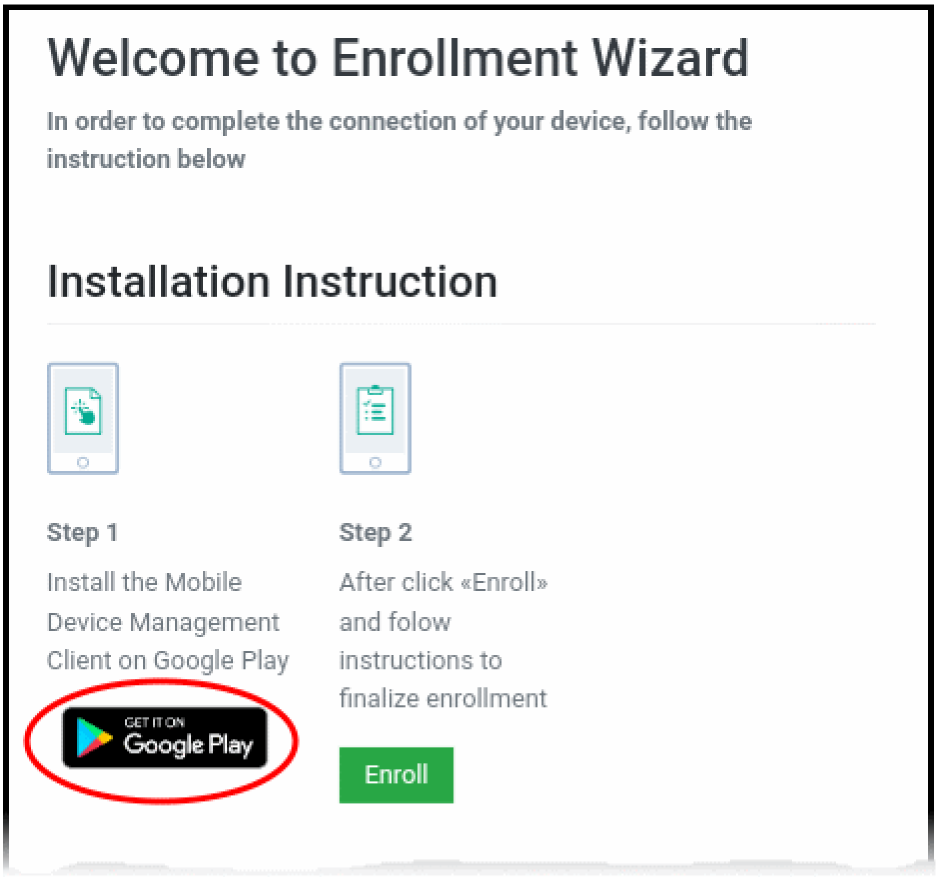
- After you have **completed the setup process**, Endpoint Manager will send an email to your users containing device enrollment instructions.
- Users should open the mail on the device itself.

Android device enrollment involves two steps:

- **Step 1 - Download and Install the communication client**
- **Step 2 - Configure the client**

## Step 1 - Download and Install the communication client

- Open the mail on the device you want to enroll
- Tap the link in the mail to start the enrollment wizard
- Tap the 'Get it on Google Play' button:



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installation Instruction

Step 1

Install the Mobile Device Management Client on Google Play

Step 2

After click «Enroll» and folow instructions to finalize enrollment

- Download and install the client software from Google Play

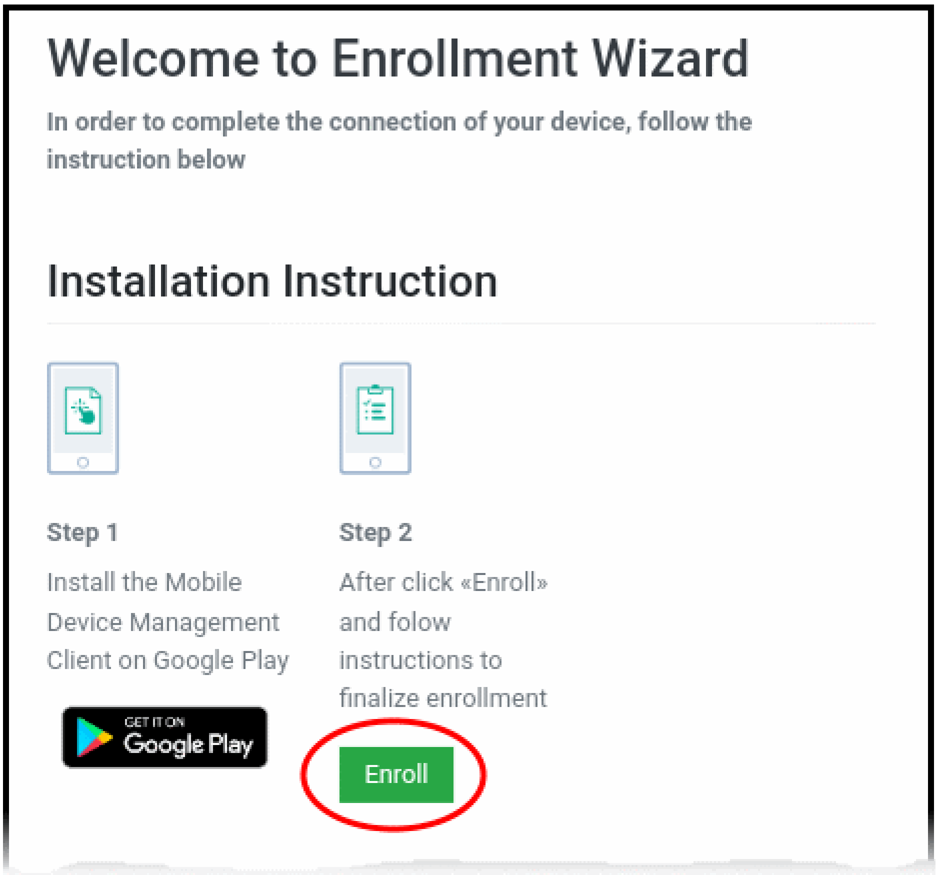
## Step 2 - Configure the communication client

The next step is to configure the client to connect to Endpoint Manager. There are two ways to do this:

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

## Automatic Configuration

- After installation in step 1, go back to the device enrollment page and tap the 'Enroll' button under 'Step 2':



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installation Instruction

Step 1

Install the Mobile Device Management Client on Google Play

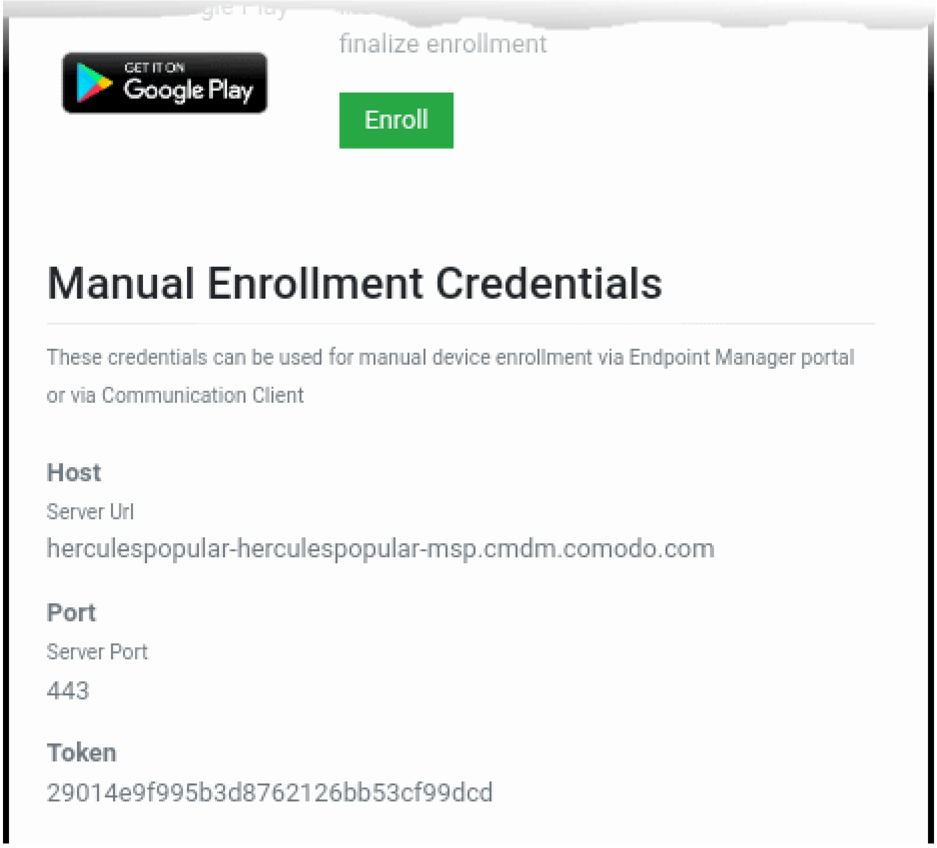
Step 2

After click «Enroll» and folow instructions to finalize enrollment

The client is automatically configured and the **End User License Agreement** screen appears.

### Manual Configuration

Users can manually configure the communication client to connect to Endpoint Manager by entering the server settings and token string (aka PIN). You can find these items on the enrollment page:



Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

Host
Server Url
herculespopular-herculespopular-msp.cmdm.comodo.com

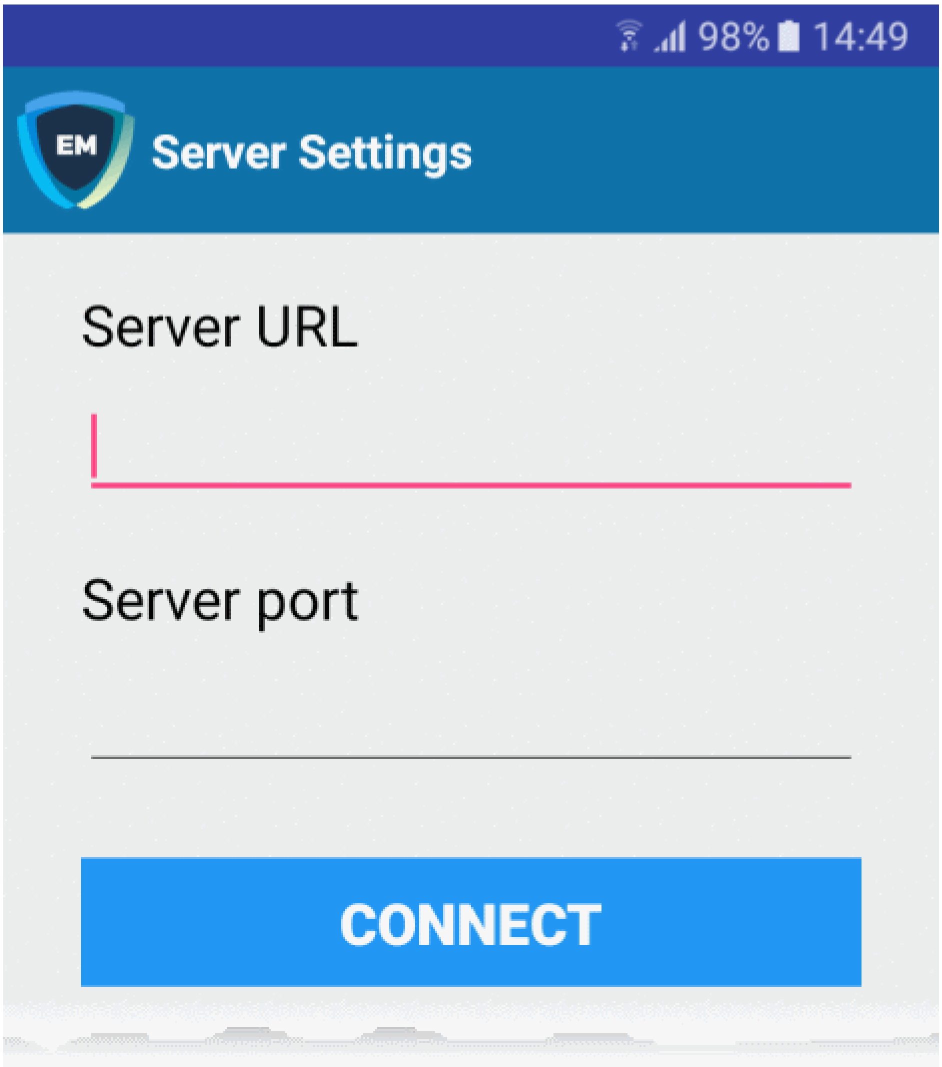
Port
Server Port
443

Token
29014e9f995b3d8762126bb53cf99dcd

**Manually configure the client**

- Open the client by tapping the client icon on your device.
- This starts the client configuration wizard. Enroll the device by entering the server settings and unique token.

### Server Settings



- **Server URL** - The server URL is listed on the enrollment page as described above.
- **Server port** -The server port is also listed on the enrollment page. Default = 443.

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

## Login to the Console

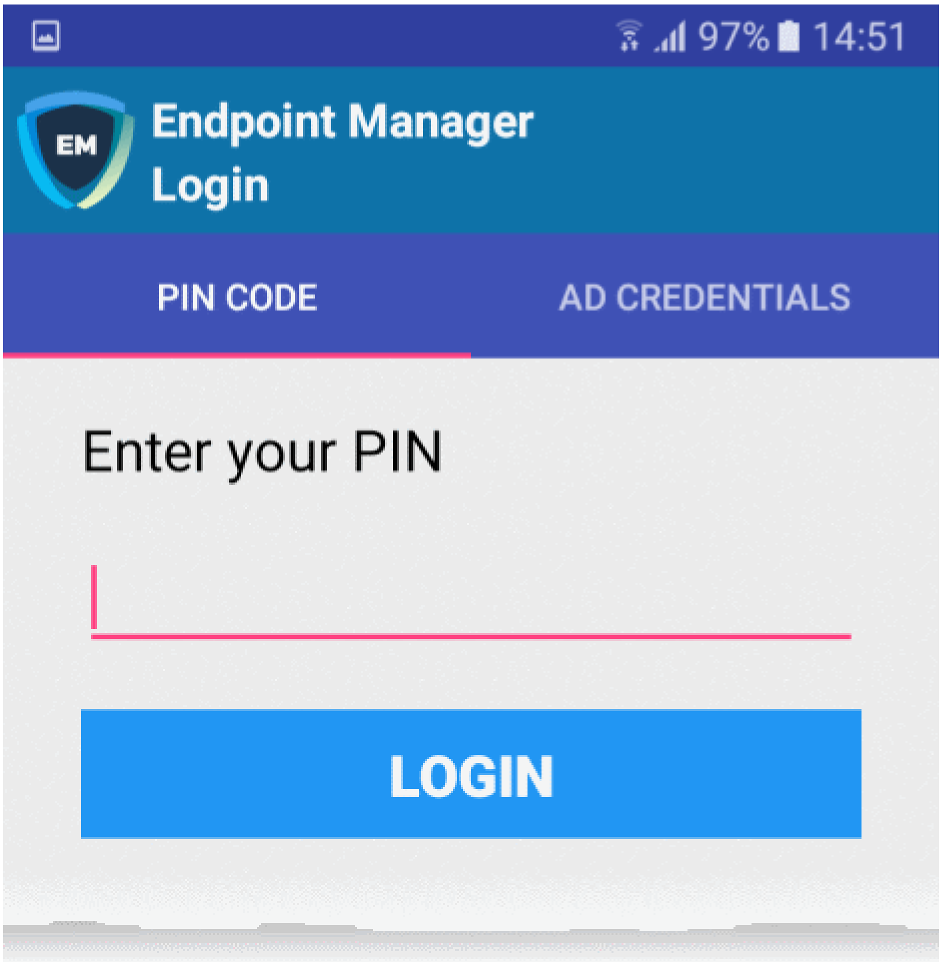
There are two ways to login to the console:

- Enter the token from the enrollment page in the 'PIN Code' tab

  OR
- Enter your domain username and password

### Enter the token from the enrollment page

- Open the communication client
- Open the 'Pin Code' tab:



- Enter the token from the enrollment page as the PIN
- Tap 'Login' then agree to the **EULA**.

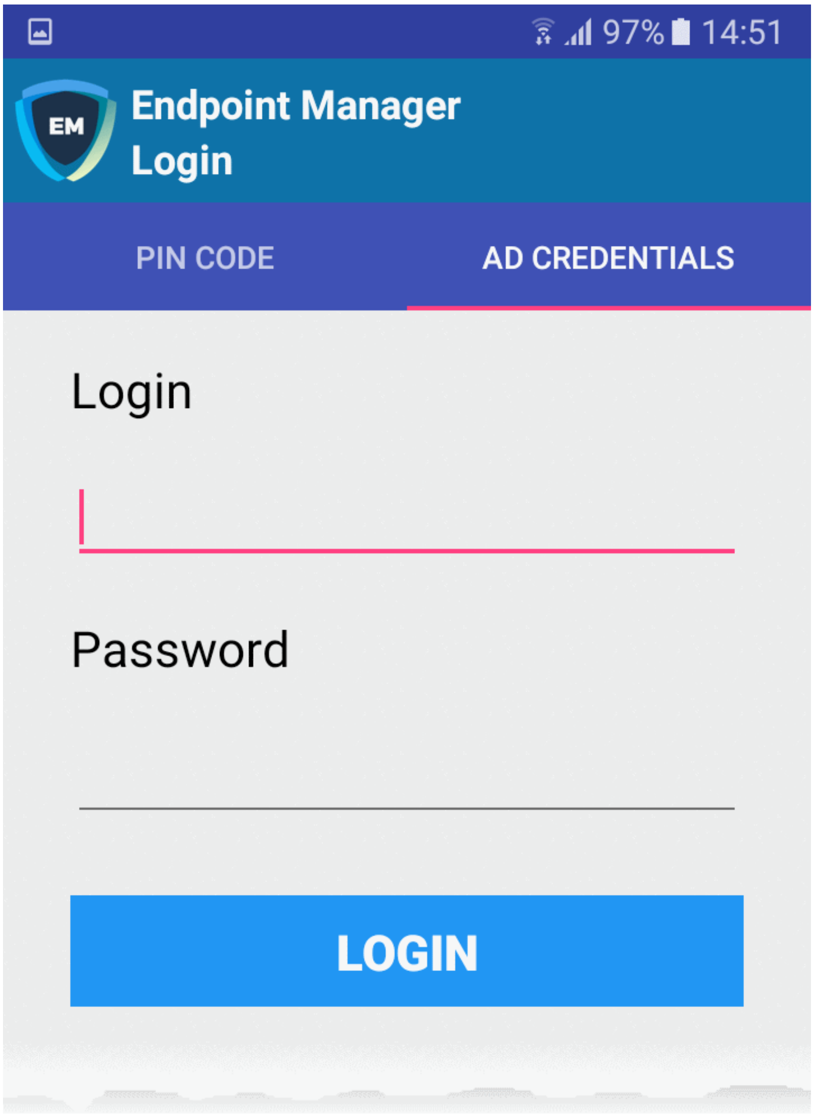
**Domain username and password**

- Open the communication client
- Open the 'AD Credentials' tab

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

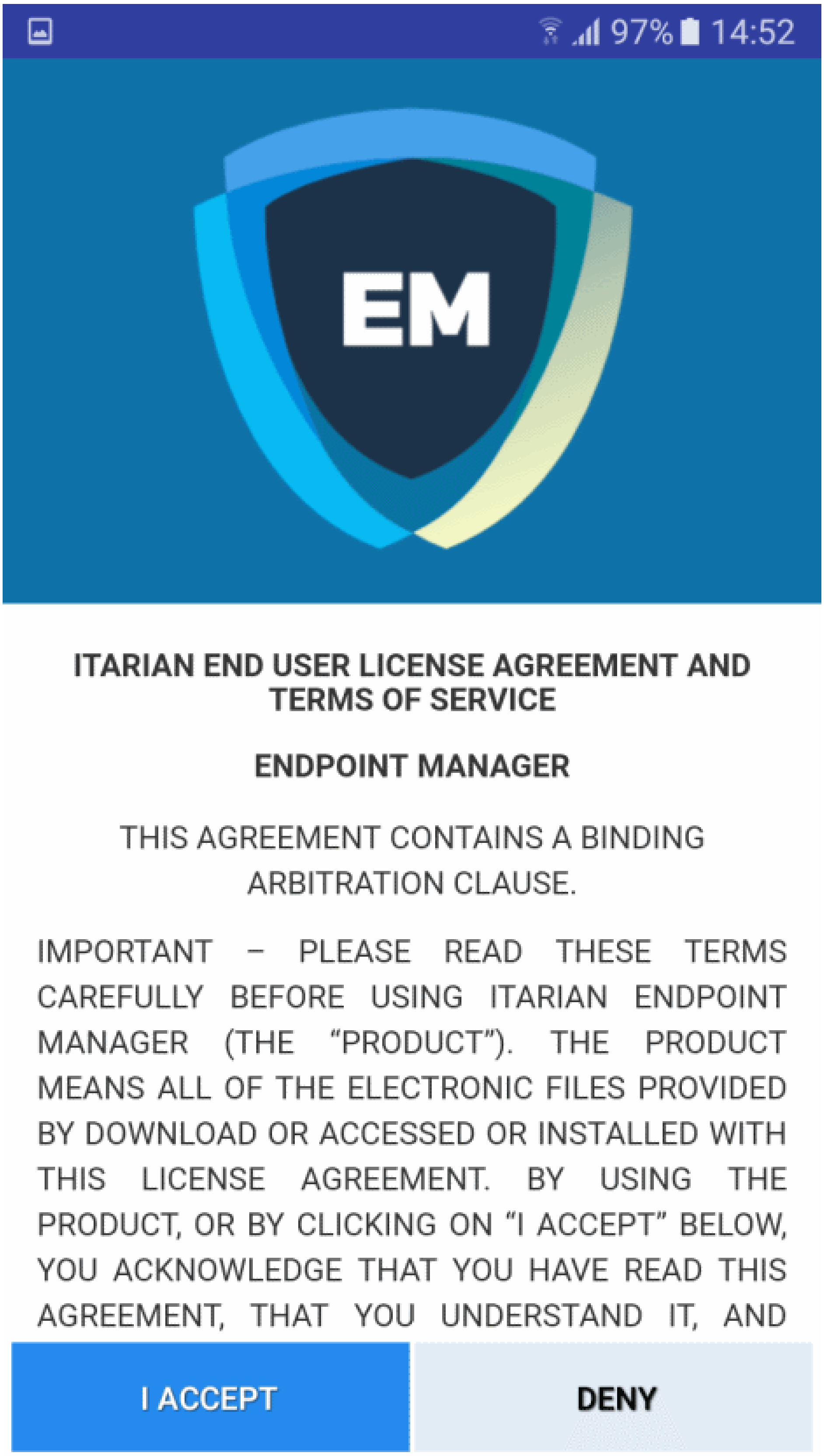
- The AD server to be integrated with EM
- The users to be imported from AD to EM.

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



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

## End User License Agreement



97% 14:52

ITARIAN END USER LICENSE AGREEMENT AND TERMS OF SERVICE

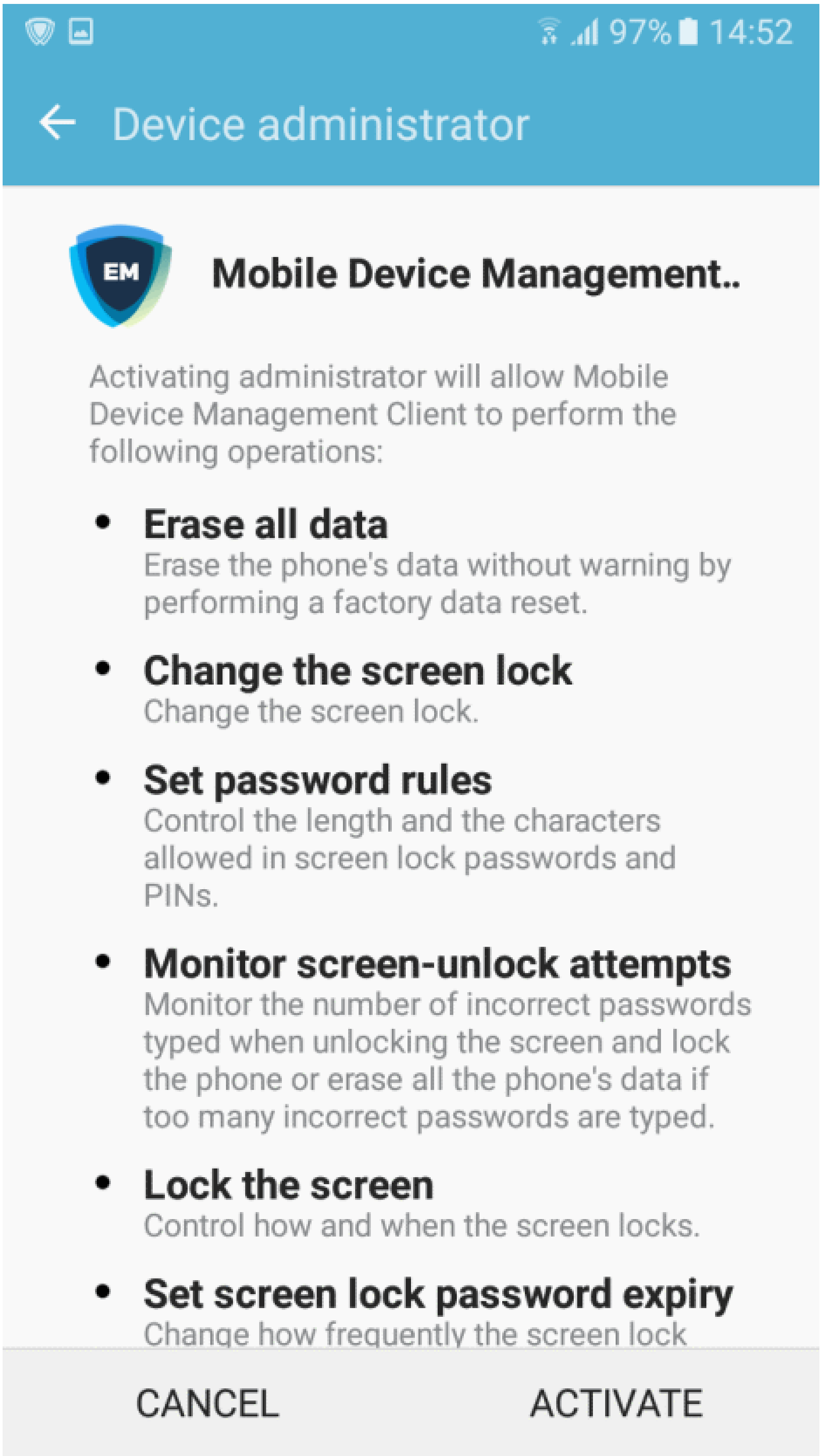
ENDPOINT MANAGER

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING ITARIAN ENDPOINT MANAGER (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD OR ACCESSED OR INSTALLED WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND

- Scroll down then click the 'I Accept' button

This starts the client activation screen. Activation requires the client is given some privileges:



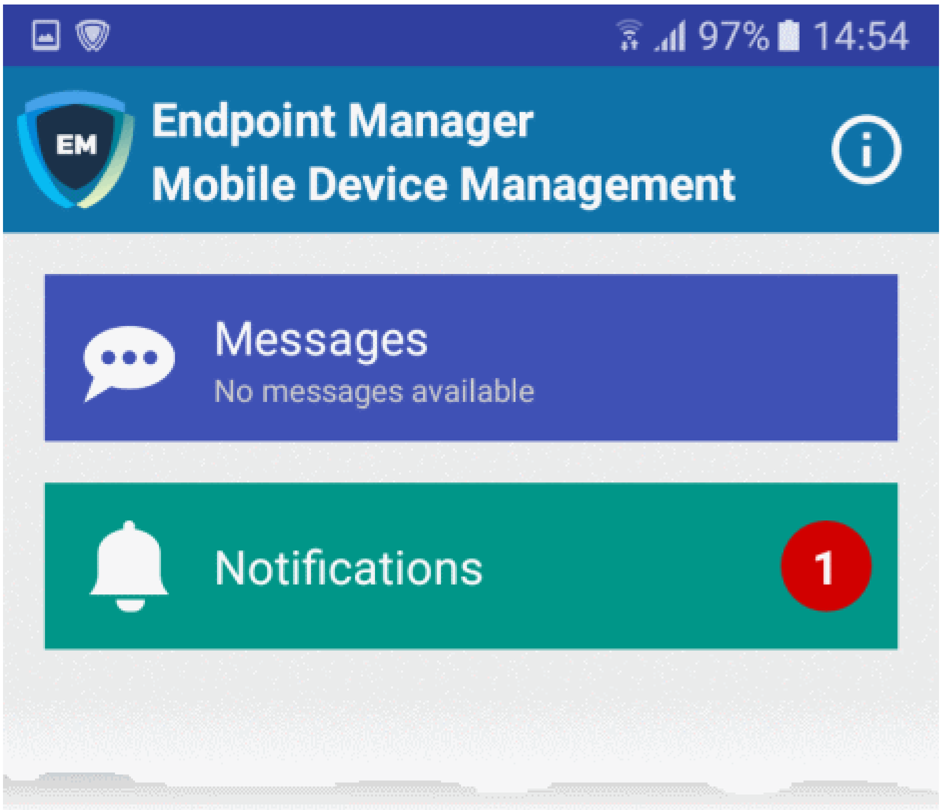
Mobile Device Management..

Activating administrator will allow Mobile Device Management Client to perform the following operations:

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

- Tap 'Activate'.

The communication client home screen opens:



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

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

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

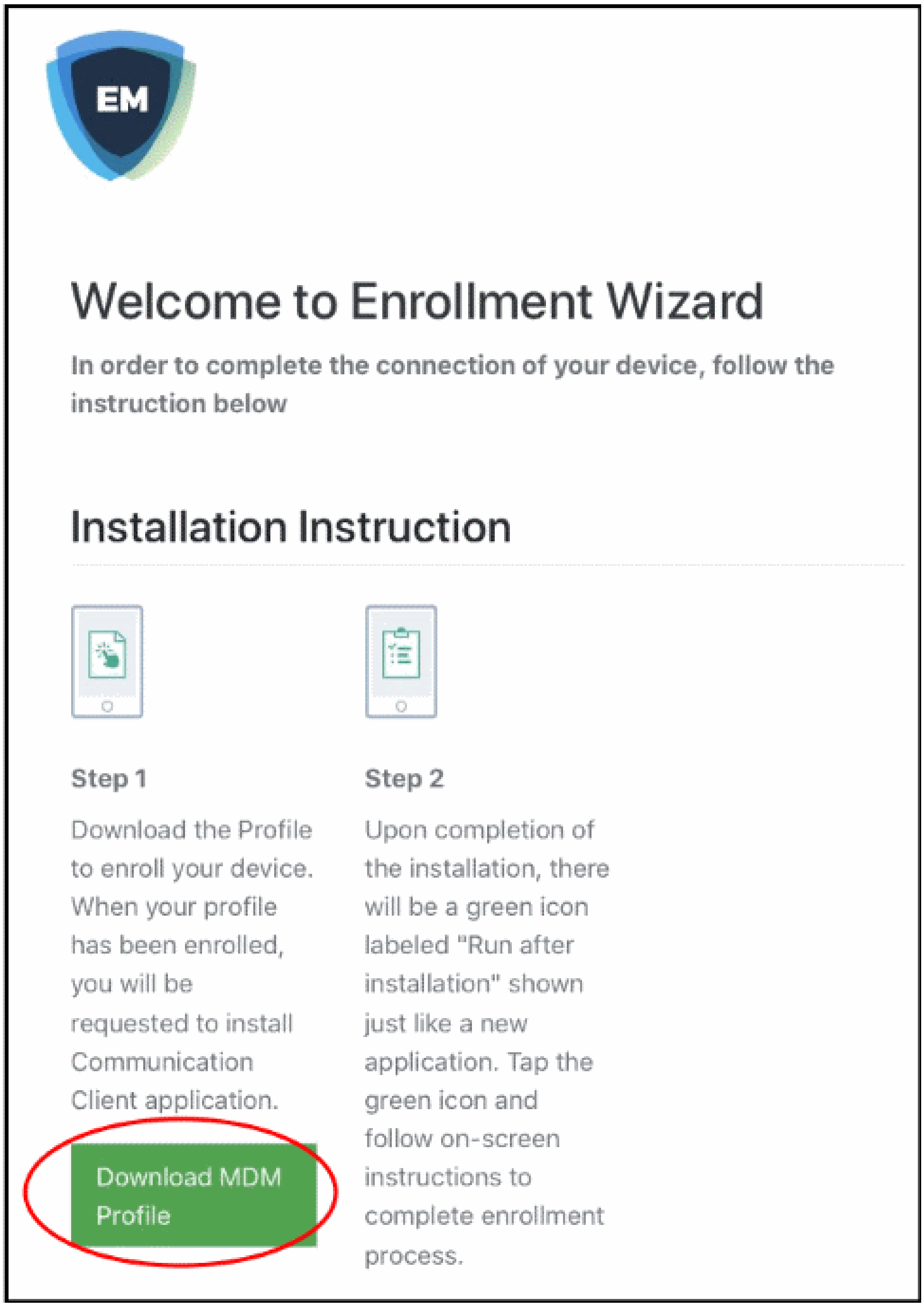
## 4.1.2.2. Enroll iOS Devices

- After you have **completed the setup process**, Endpoint Manager will send an email to your users containing device enrollment instructions.
- Users should open the mail on the device itself.

**Note:** Users must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks or enters standby mode.

**Enroll an iOS device**

- Complete the steps in **4.1.2.Enroll User Devices for Management** if you haven't done so already. Those steps will send an enrollment email to the device owners.
- Device owners should open the mail on the device itself and tap the enrollment link. This will take them to the device enrollment wizard.



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installation Instruction

Step 1

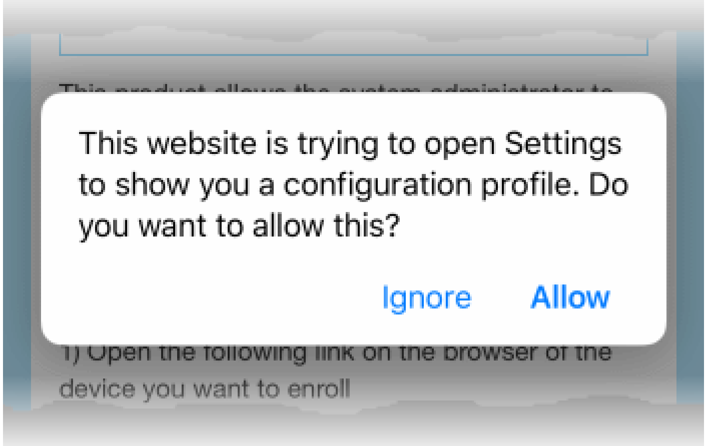
Download the Profile to enroll your device. When your profile has been enrolled, you will be requested to install Communication Client application.

Step 2

Upon completion of the installation, there will be a green icon labeled "Run after installation" shown just like a new application. Tap the green icon and follow on-screen instructions to complete enrollment process.

- Click 'Download MDM Profile' in 'Step 1':

A confirmation is shown:

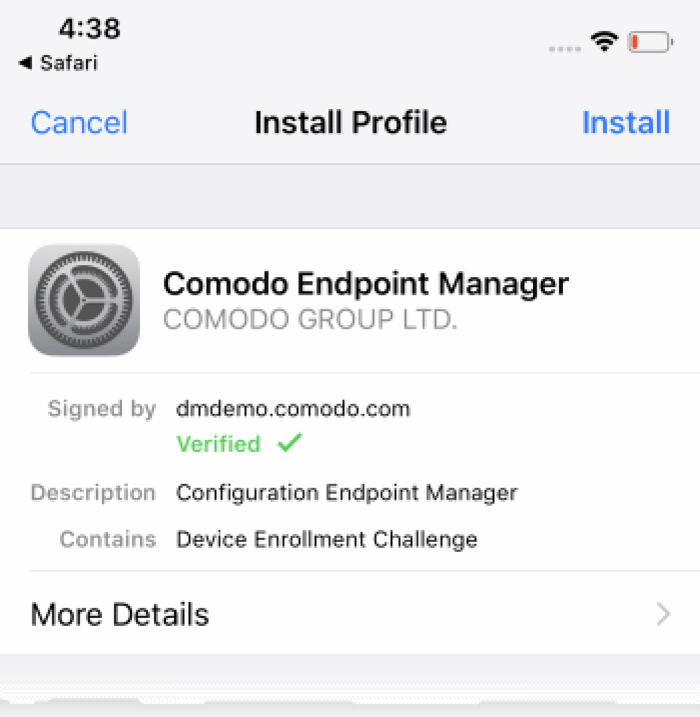


This product allows the system administrator to

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

1) Open the following link on the browser of the device you want to enroll

- Click 'Allow'. The 'Install Profile' wizard starts:



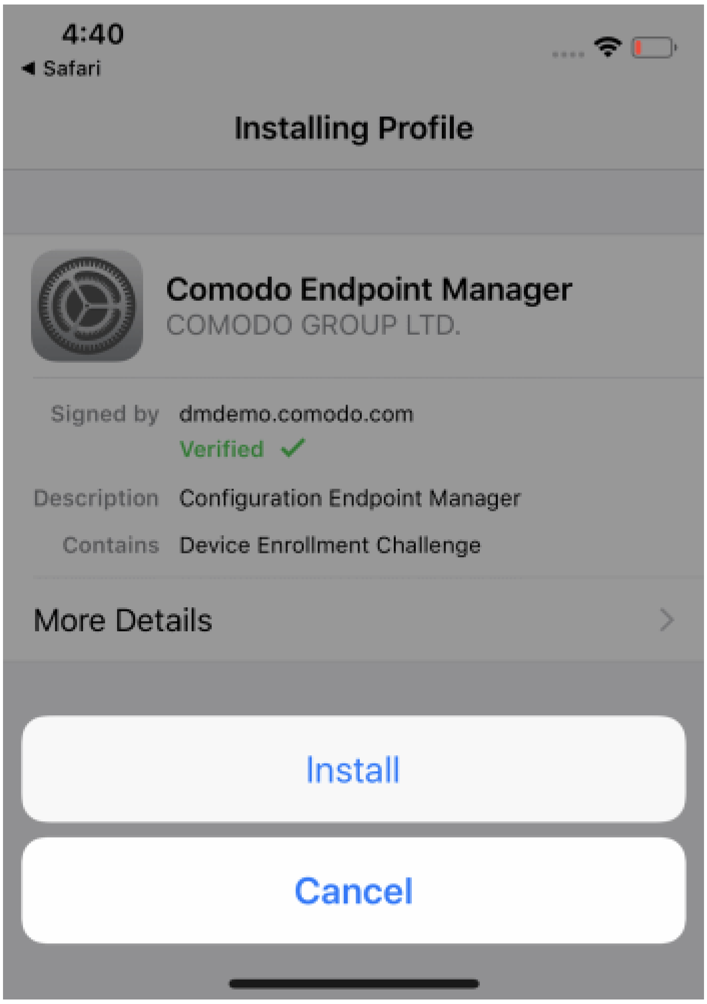
Comodo Endpoint Manager
COMODO GROUP LTD.

Signed by dmdemo.comodo.com
Verified ✓

Description Configuration Endpoint Manager

Contains Device Enrollment Challenge

- Tap 'Install'...



4:40
◂ Safari

Installing Profile

Comodo Endpoint Manager
COMODO GROUP LTD.

Signed by dmdemo.comodo.com
Verified ✓

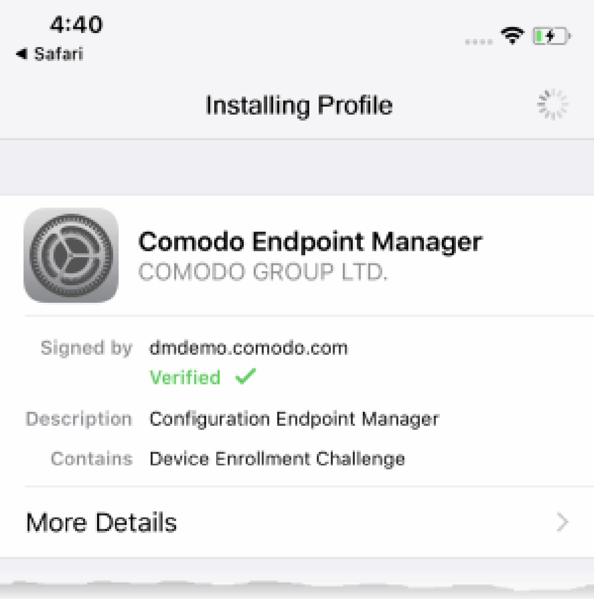
Description Configuration Endpoint Manager

Contains Device Enrollment Challenge

More Details >

- ...then 'Install' again.

The profile and certificate installation processes will start:



4:40
◂ Safari

Installing Profile

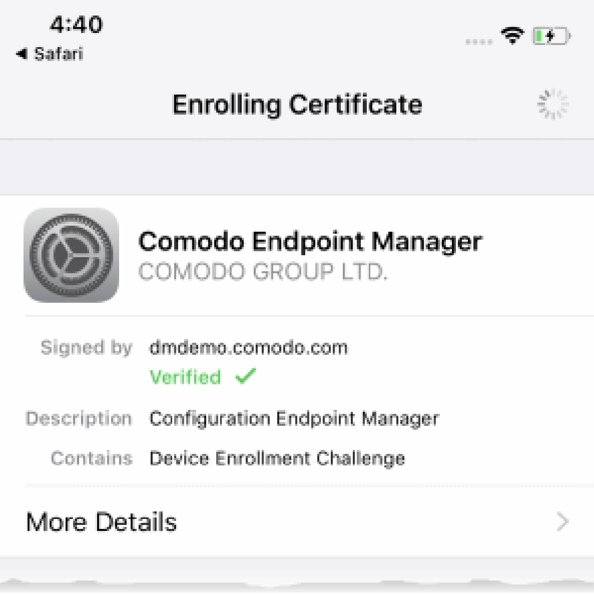
Comodo Endpoint Manager
COMODO GROUP LTD.

Signed by dmdemo.comodo.com
Verified ✓

Description Configuration Endpoint Manager

Contains Device Enrollment Challenge

More Details >



4:40
◂ Safari

Enrolling Certificate

Comodo Endpoint Manager
COMODO GROUP LTD.

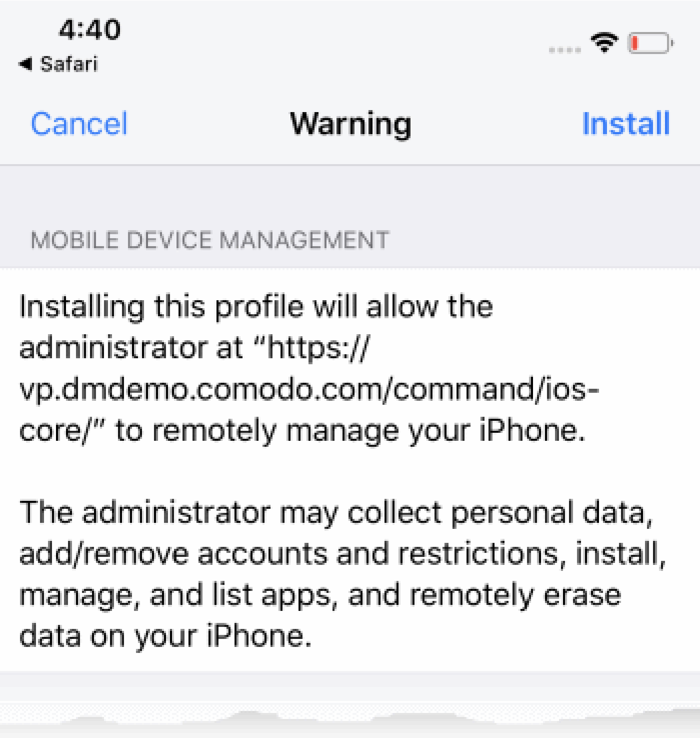
Signed by dmdemo.comodo.com
Verified ✓

Description Configuration Endpoint Manager

Contains Device Enrollment Challenge

More Details >

- When that has finished, read the privacy information then click 'Install' to continue:



4:40

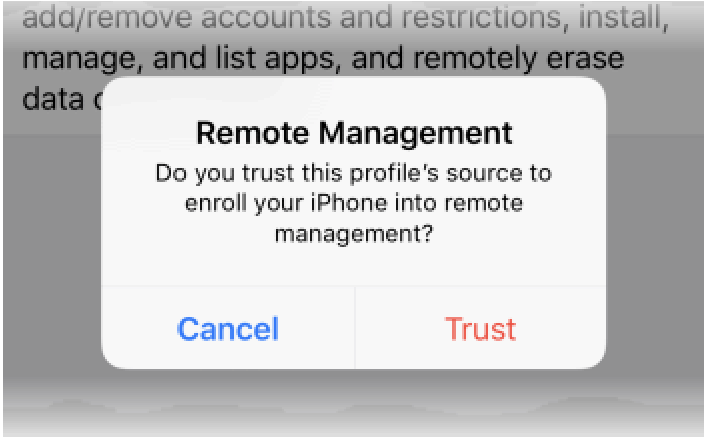
◀ Safari

MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://vp.dmdemo.comodo.com/command/ios-core/” to remotely manage your iPhone.

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

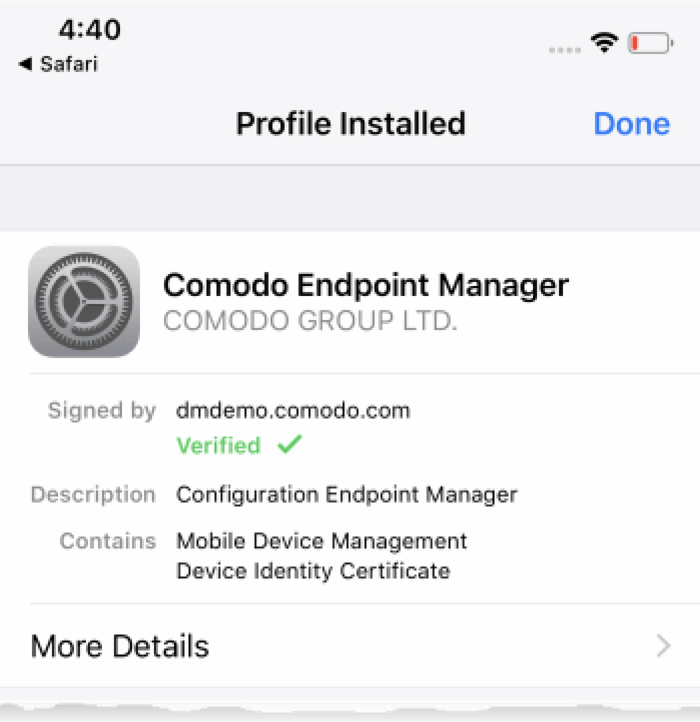
- Click 'Trust' at the remote management screen to continue installation:



add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data c

Remote Management

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



Profile Installed

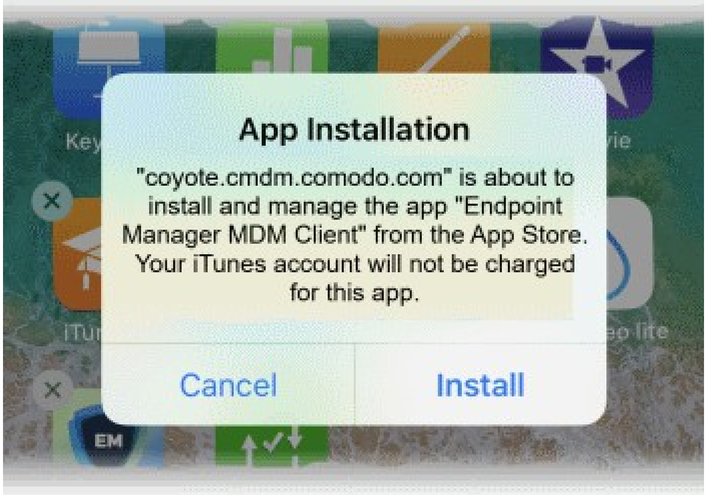
Comodo Endpoint Manager
COMODO GROUP LTD.

Signed by dmdemo.comodo.com
Verified ✓

Description Configuration Endpoint Manager

Contains Mobile Device Management
Device Identity Certificate

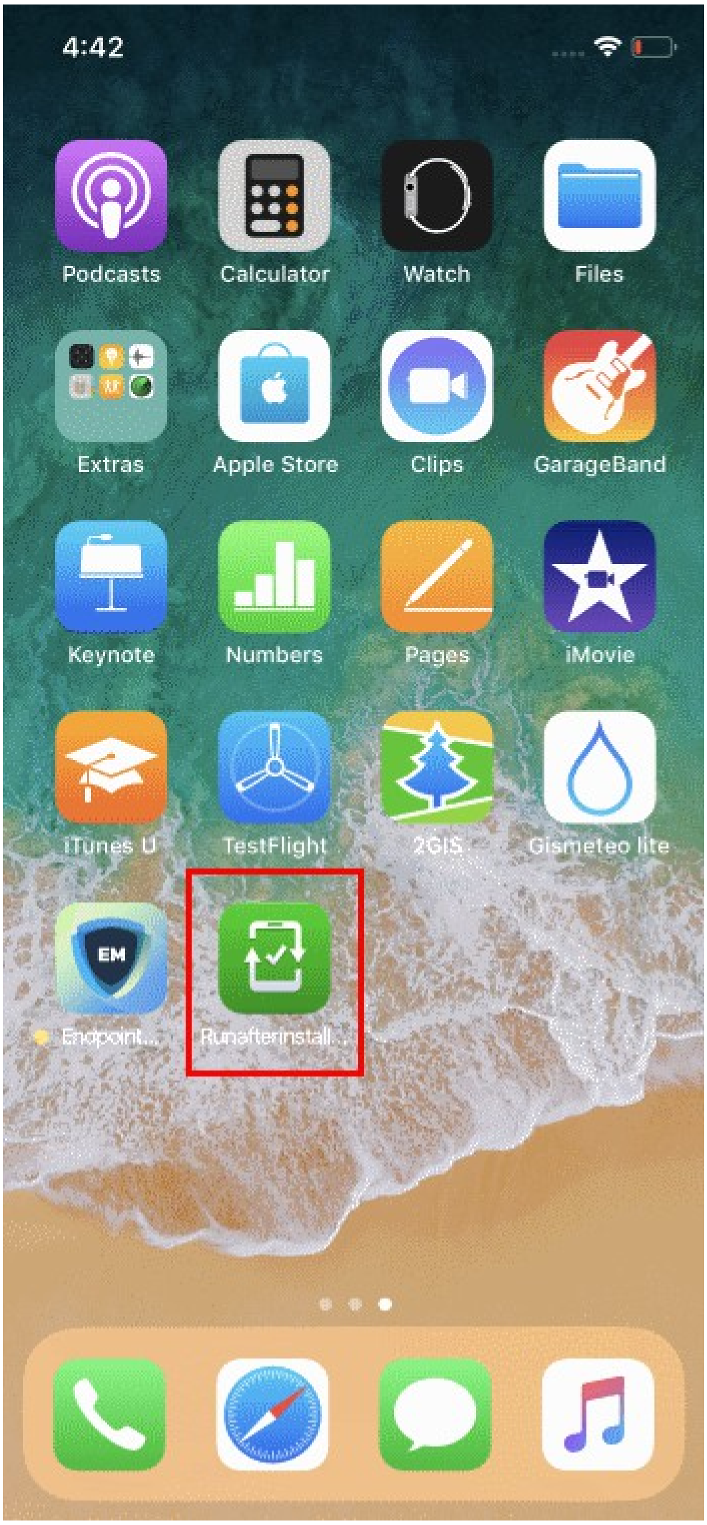
- Tap 'Done' to finish profile installation.
- After installing the profile, the communication client installation process will begin. The client is essential to connect the device to Endpoint Manager:



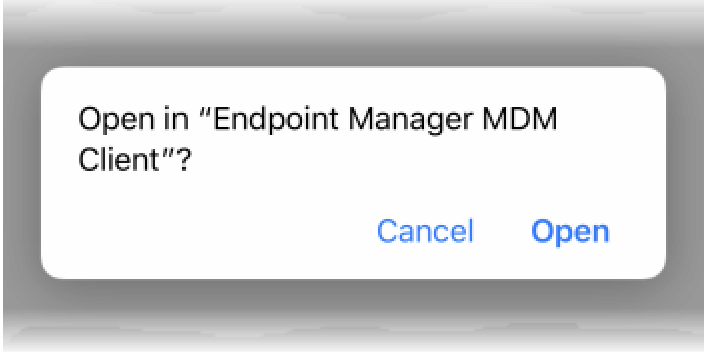
App Installation

"coyote.cmdm.comodo.com" is about to install and manage the app "Endpoint Manager MDM Client" from the App Store. Your iTunes account will not be charged for this app.

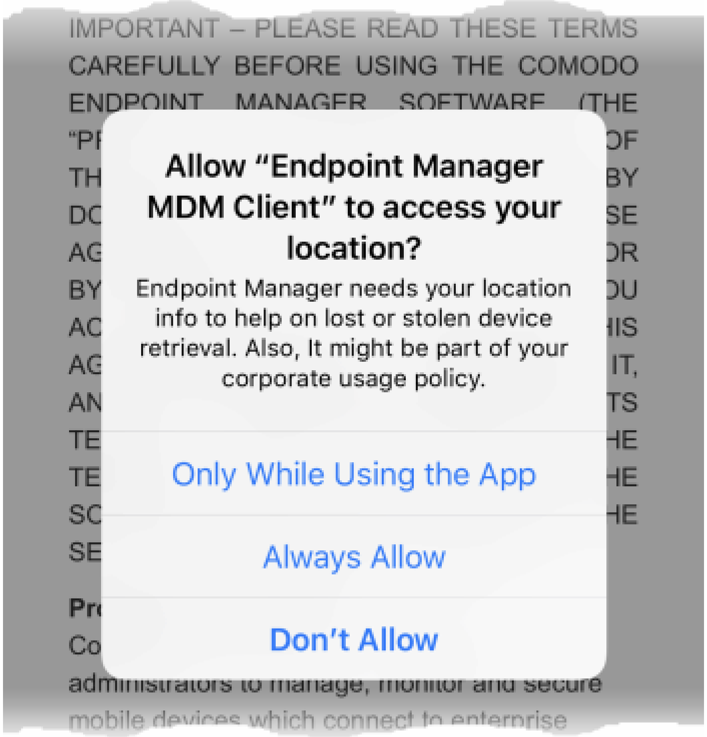
- The app is downloaded from the Apple store using the user's account.
- After installation, tap the green 'Run After Install' icon on the home screen:



- Next, select 'Open' to begin the installation process:


Open in "Endpoint Manager MDM Client"?

- The client requires access to device location to continue the setup process:



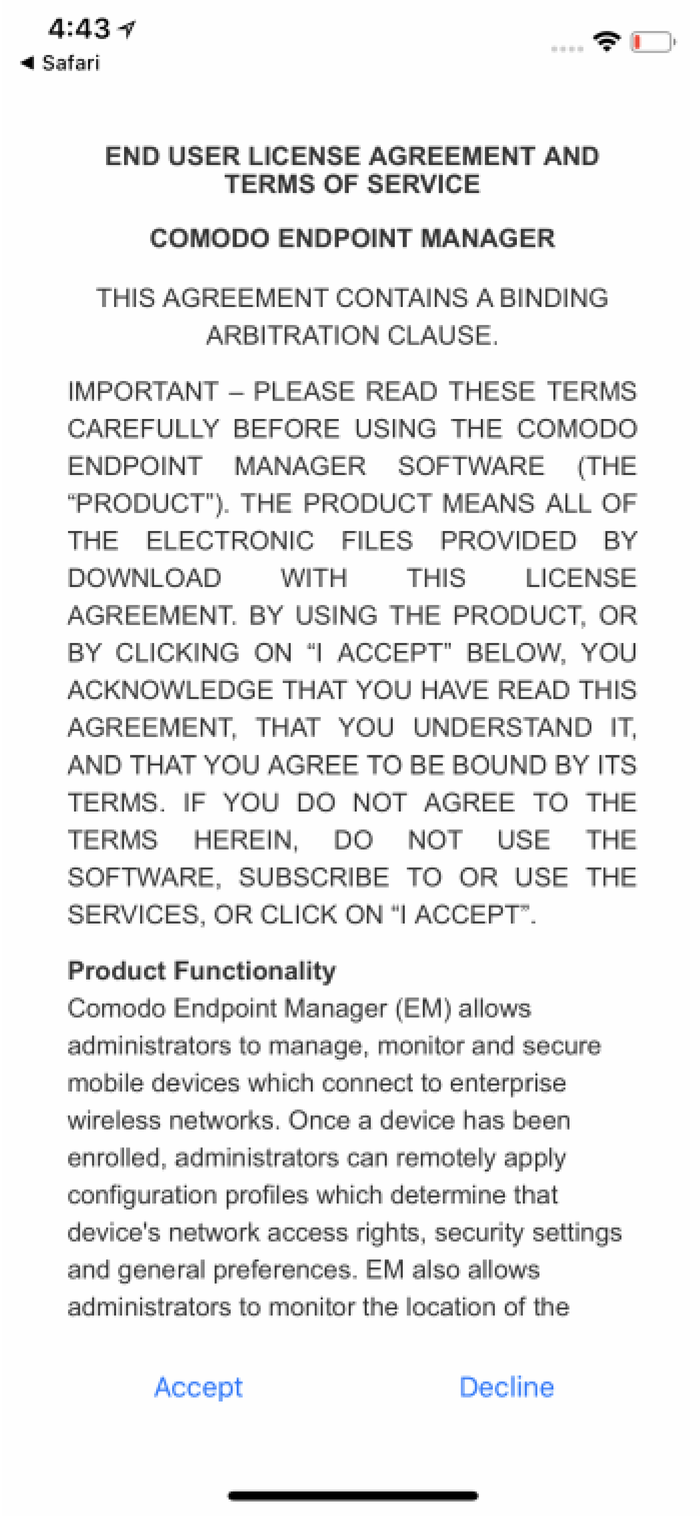
IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ENDPOINT MANAGER SOFTWARE (THE

**Allow "Endpoint Manager MDM Client" to access your location?**

Endpoint Manager needs your location info to help on lost or stolen device retrieval. Also, It might be part of your corporate usage policy.

administrators to manage, monitor and secure mobile devices which connect to enterprise

- Tap 'Always Allow'.
- Read and accept the EULA:



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

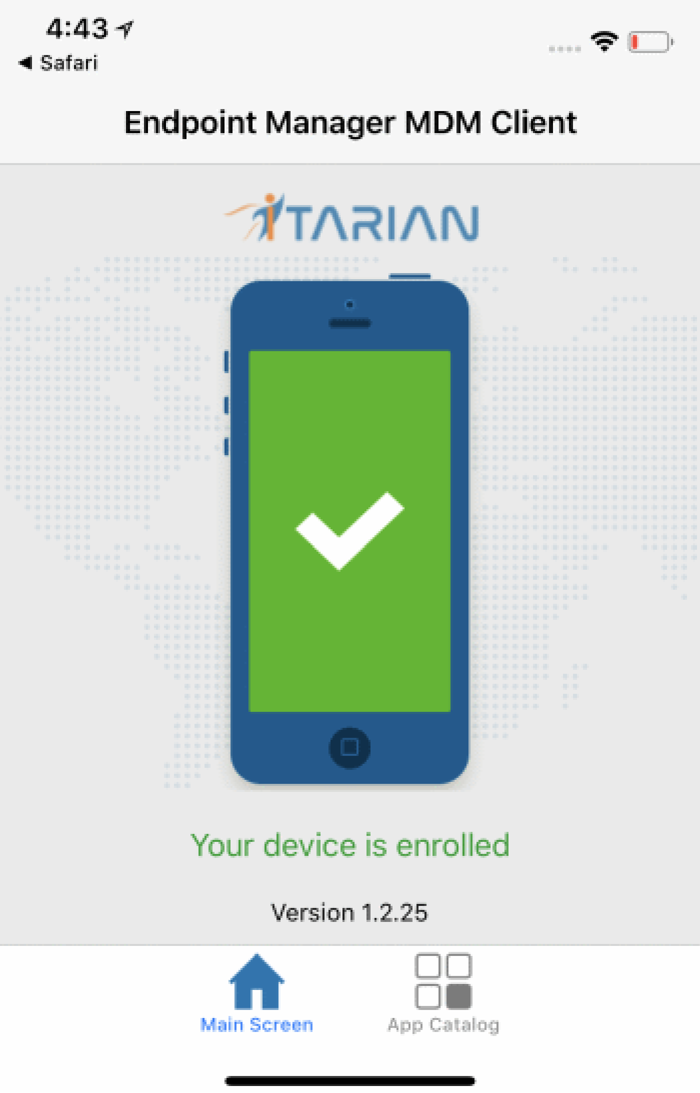
COMODO ENDPOINT MANAGER

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

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

**Product Functionality**
Comodo Endpoint Manager (EM) allows administrators to manage, monitor and secure mobile devices which connect to enterprise wireless networks. Once a device has been enrolled, administrators can remotely apply configuration profiles which determine that device's network access rights, security settings and general preferences. EM also allows administrators to monitor the location of the

- The device will be successfully enrolled to Endpoint Manager once the client is installed:



- App Catalog - View installed apps, required apps and available apps.

An Endpoint Manager security profile will be applied to the device as follows:

- If a custom profile is assigned to the user in EM then those profiles are applied to the device. See **Assign Configuration Profiles to User Devices** and **Assign Configuration Profiles to a User Group** for more.
- If no profiles are defined for the user then all 'default' iOS profiles are applied to the device. See **Manage Default Profiles** for more on this.

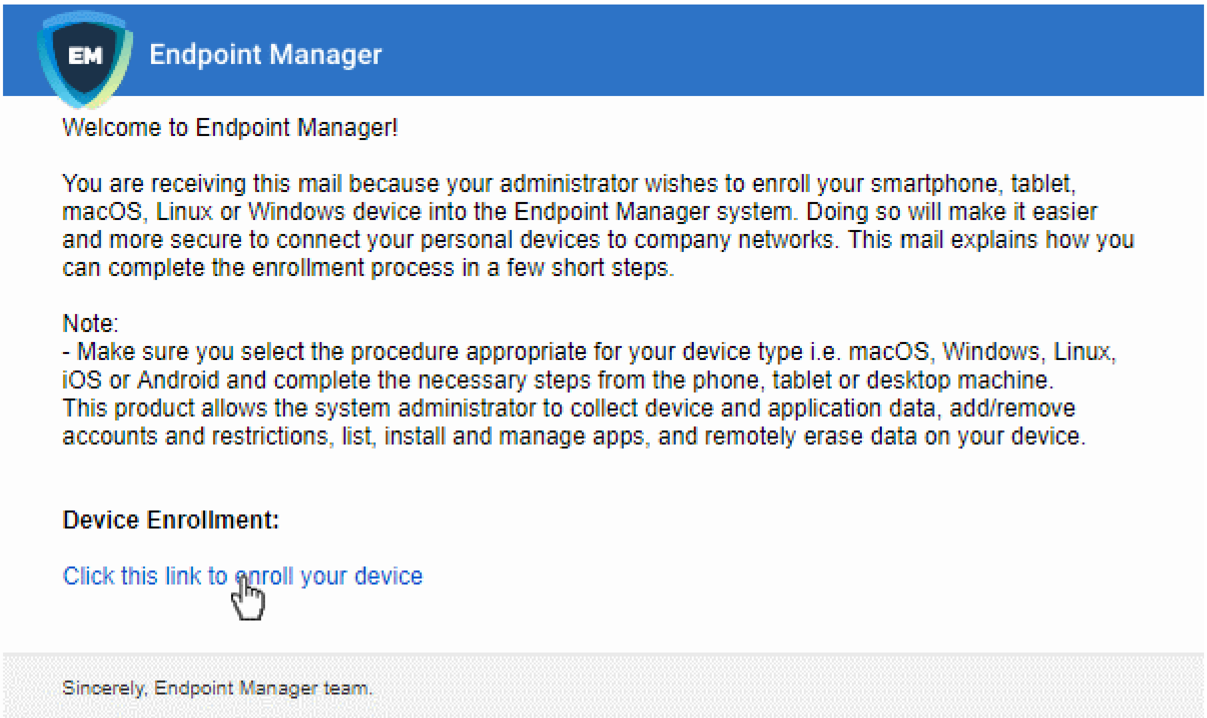
The device can now be remotely managed from the EM console.

### 4.1.2.3. Enroll Windows Endpoints

- After you have **completed the setup process**, Endpoint Manager will send an email to your users containing device enrollment instructions.
- Users should open the email on the Windows endpoint you want to enroll. After installation, the communication client will automatically connect to the EM server.

**Enroll a Windows device**

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



Welcome to Endpoint Manager!

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

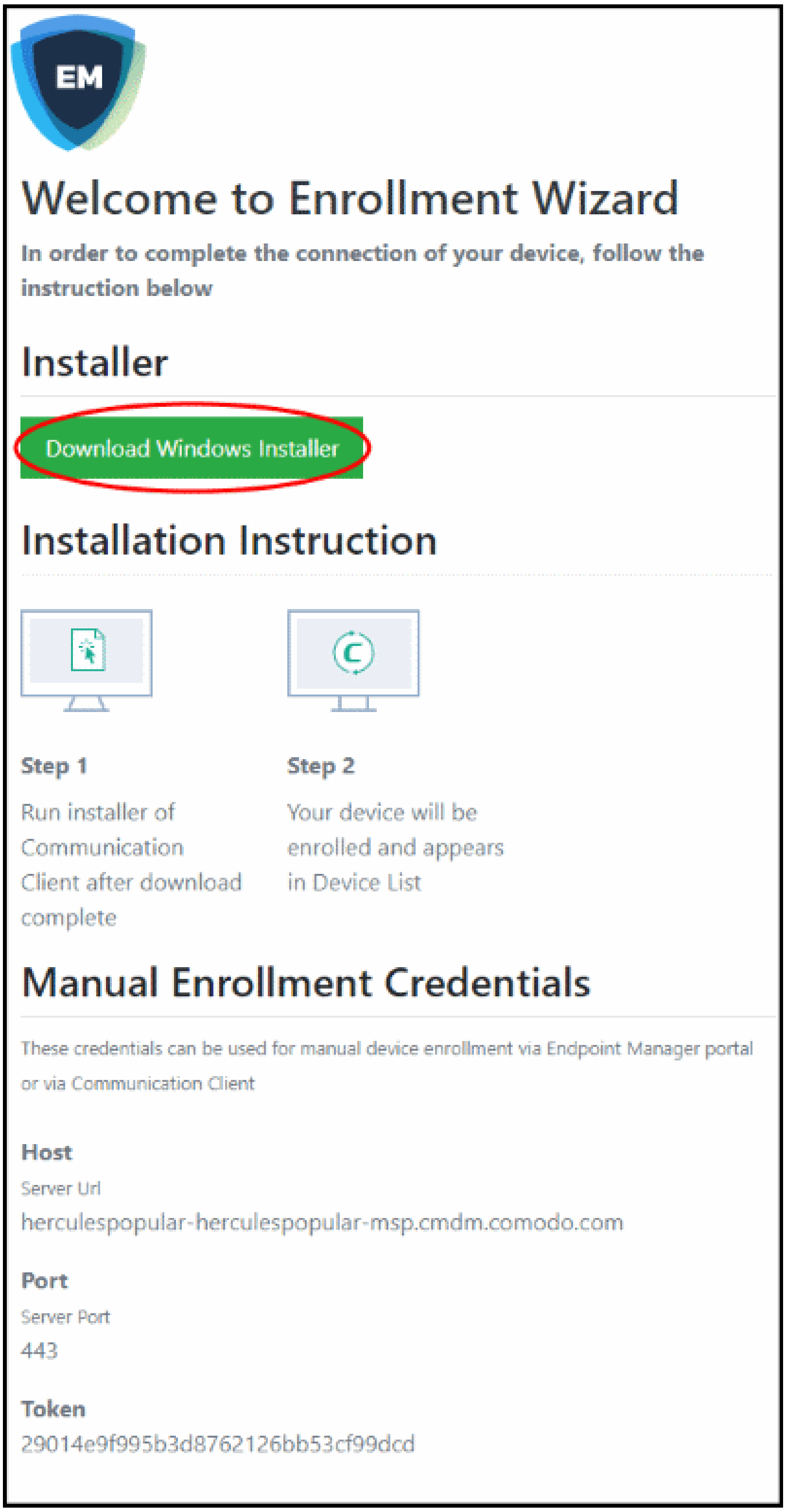
Note:
- Make sure you select the procedure appropriate for your device type i.e. macOS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

**Device Enrollment:**

Click this link to enroll your device

Sincerely, Endpoint Manager team.

- Click the enrollment link in the email to open the device enrollment page
- The device enrollment wizard starts.
- Click the 'Download Windows Installer' button:



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Installation Instruction

Step 1

Run installer of Communication Client after download complete

Step 2

Your device will be enrolled and appears in Device List

Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

Host

Server Url

herculespopular-herculespopular-msp.cmdm.comodo.com

Port

Server Port

443

Token

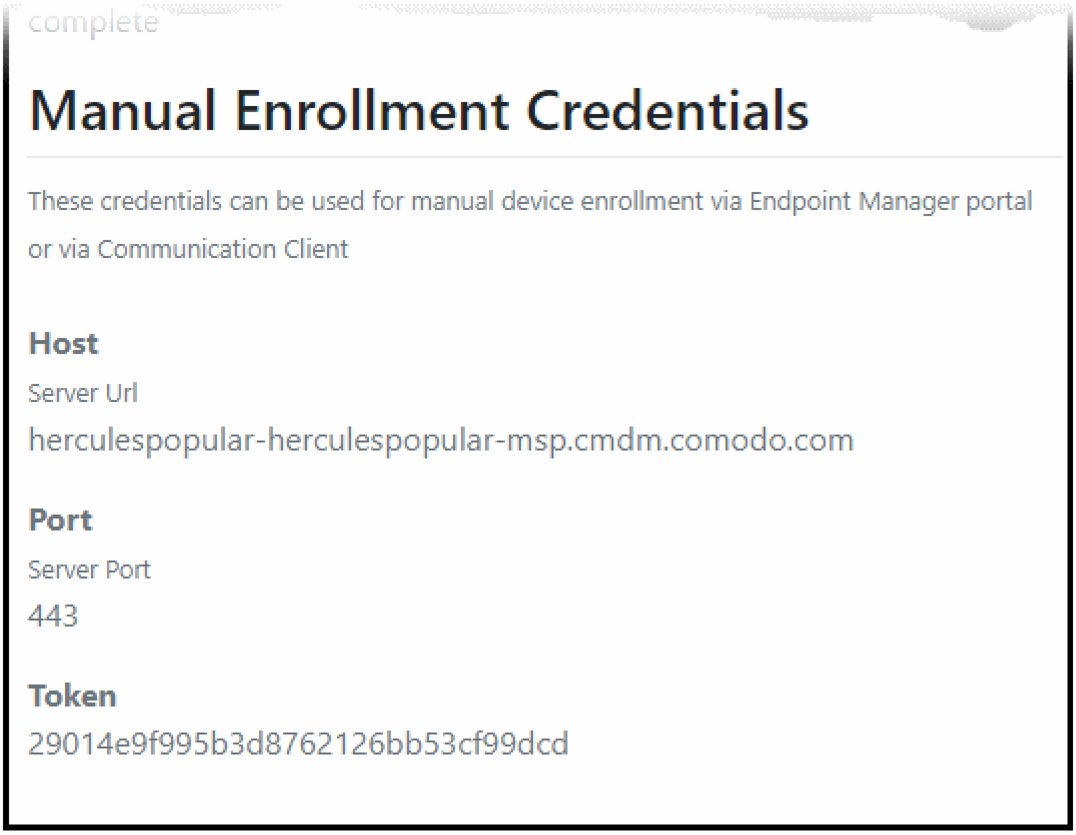
29014e9f995b3d8762126bb53cf99dcd

The EM client setup file gets downloaded.

- Double-click on the file to install the communication client.

The device automatically gets added to Endpoint Manager once installation is complete. The EM communication client icon appears at the bottom-right of the endpoint screen.

- If the client is not automatically enrolled after installation, you can manually enroll the device at a later time. This might happen, for example, if there are connectivity issues.
- You will need to enter the host, port and token ID to manually enroll. You can find these items at the end of the device enrollment page.



complete

Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

Host

Server Url

herculespopular-herculespopular-msp.cmdm.comodo.com

Port

Server Port

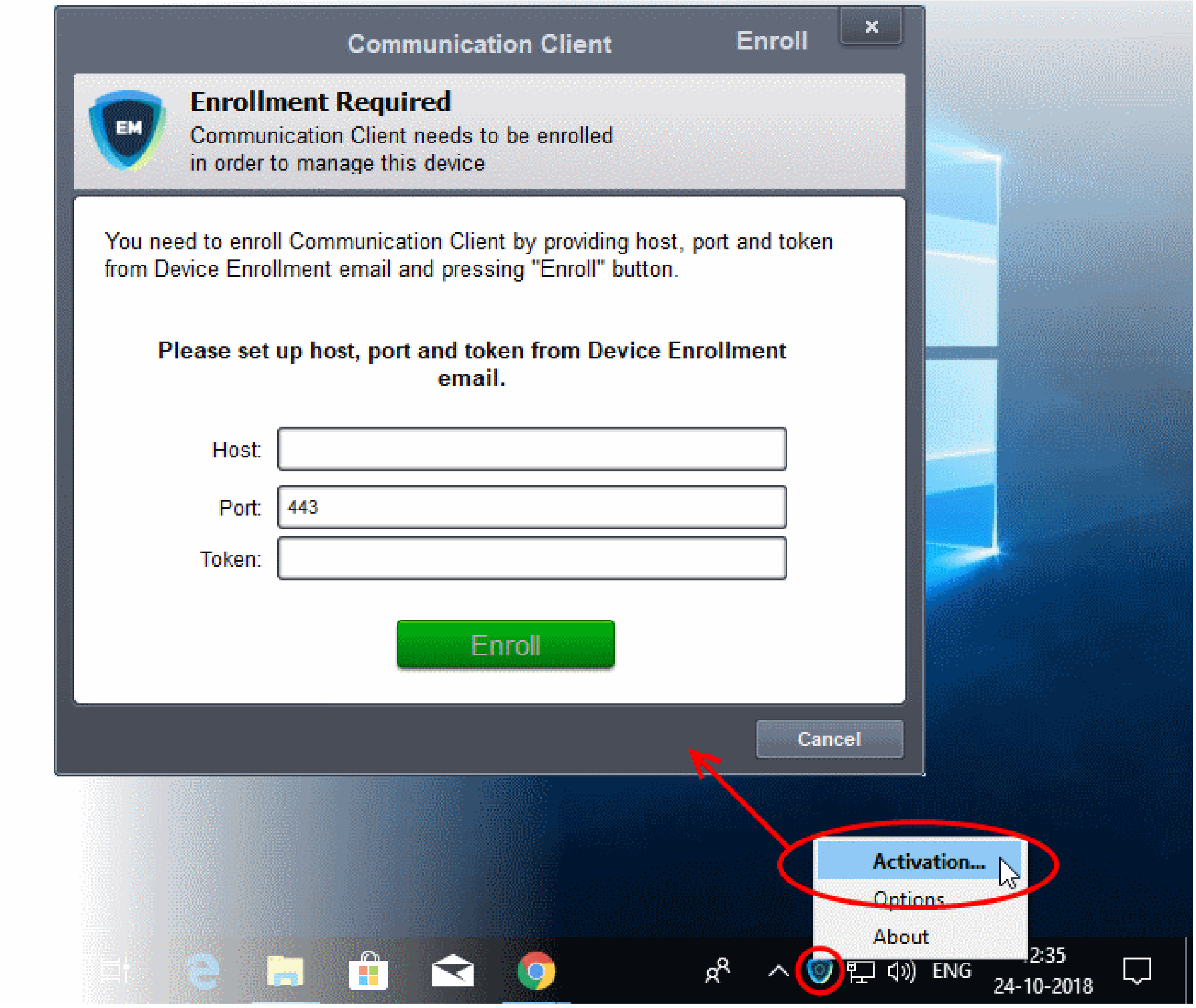
443

Token

29014e9f995b3d8762126bb53cf99dcd

**Manually enroll your device**

- Right-click on the communication client tray icon and select 'Activation'



Communication Client Enroll

**Enrollment Required**

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

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

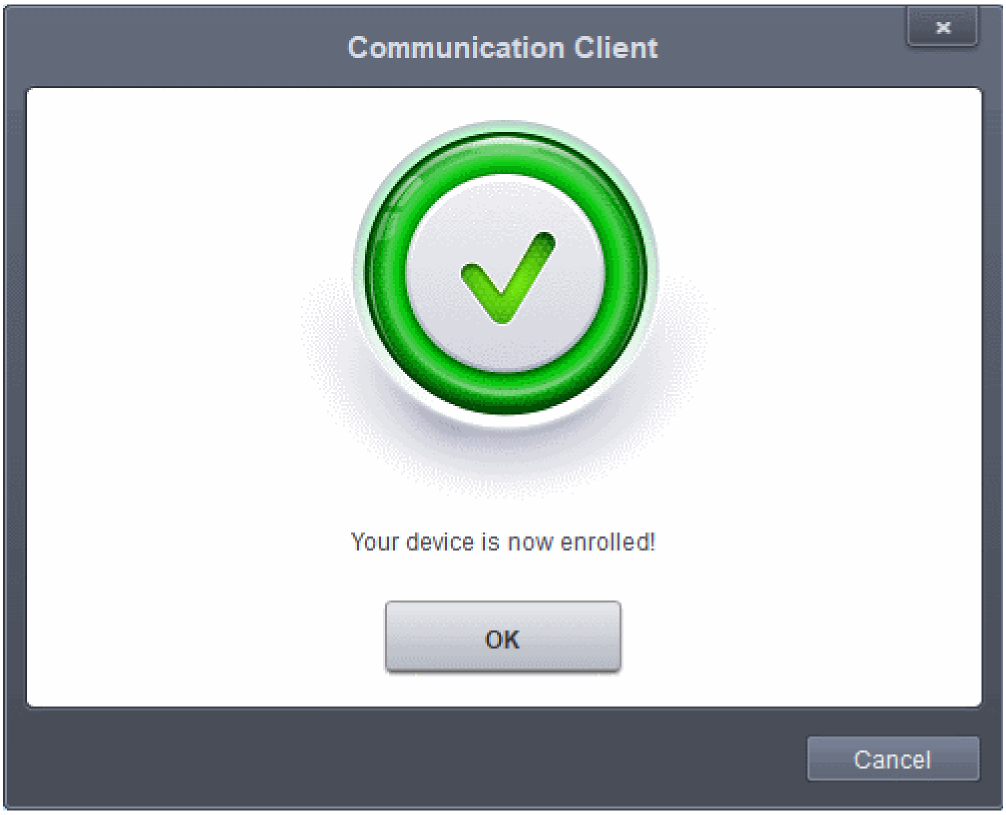
**Please set up host, port and token from Device Enrollment email.**

Host:

Port: 443

Token:

- Enter the host, port number and token in the respective fields. You can find these items in the device enrollment page.
- The client communicates with the EM server and enrolls the device.



Your device is now enrolled!

If Comodo Client Security (CCS) is included in the **setup process**, then it is installed automatically. Else you can install CCS manually after device enrollment is complete. See **Remotely Install and Update Packages on Windows Devices** for help with this.

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

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

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

Endpoint Manager allows you to rebrand the communication client (CC) and CCS applications to change the appearance and interface texts in their GUI. This is especially useful for customers who wish to white-label the CC/CCS interfaces for their clients.

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

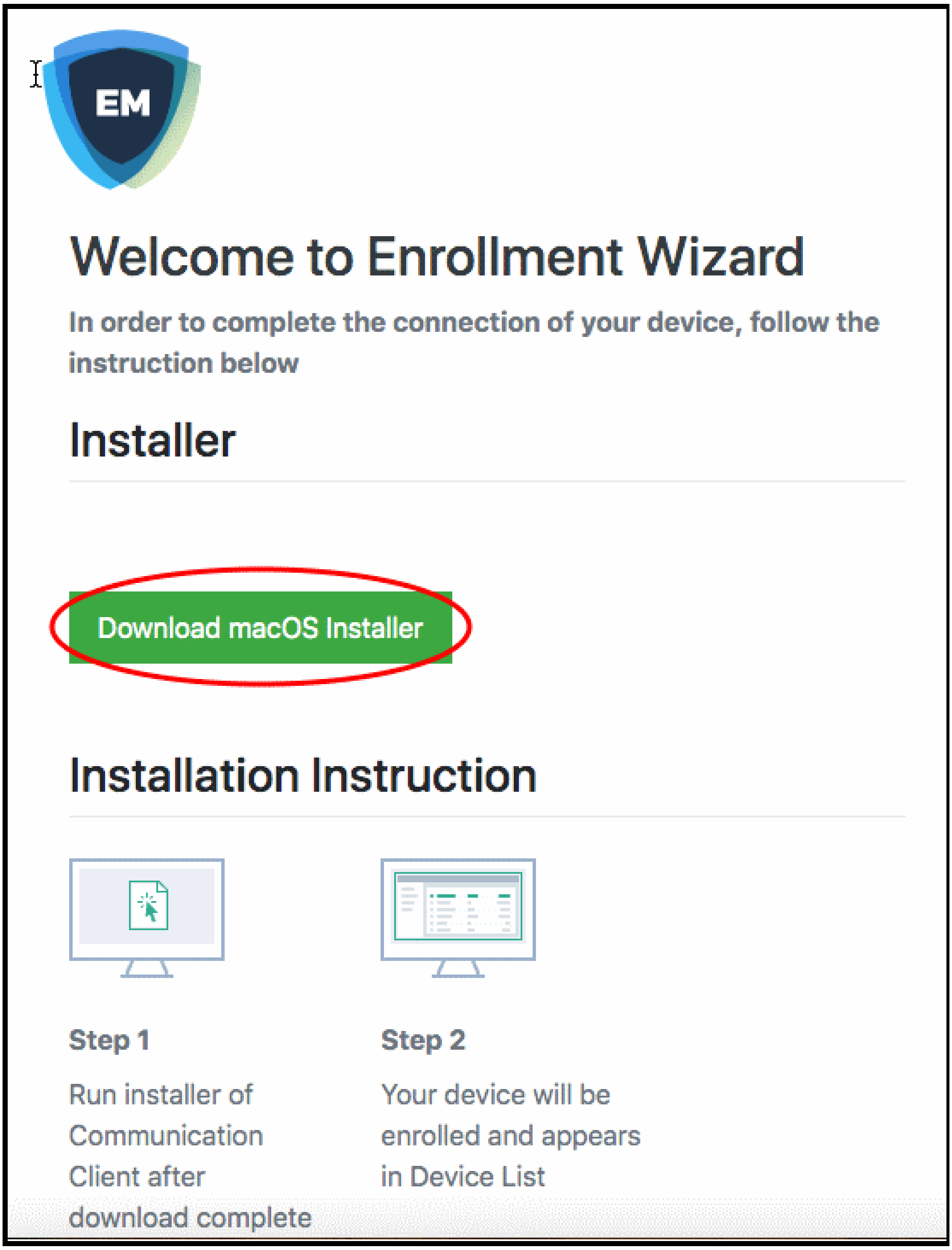
### 4.1.2.4. Enroll Mac OS Endpoints

MAC devices can be added either with or without installing the Endpoint Manager profile.

- Apple only allows one portal to use the protocol which manages devices. This causes issues with customers who want to use Endpoint Manager in conjunction with another management platform.
- 'Profile-less' enrollment lets you use Endpoint Manager to manage security while using another platform for general Mac management.
- However, you cannot manage the following items if you choose 'profile-less' enrollment:
  - Certificates
  - Restrictions
  - VPN
  - Wi-Fi
- You can configure whether or not EM profile is to be installed along with the communication client while enrolling user's device.
  - See the **settings for Mac OS devices** in the section **Enroll User Devices for Management** for help with this.

#### Enroll a Mac OS device

- Open the email on the device you want to enroll.
- Click the enrollment link in the email.
- The device enrollment wizard starts.
- Click the 'Download mac OS Installer' button:



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Installation Instruction

Step 1

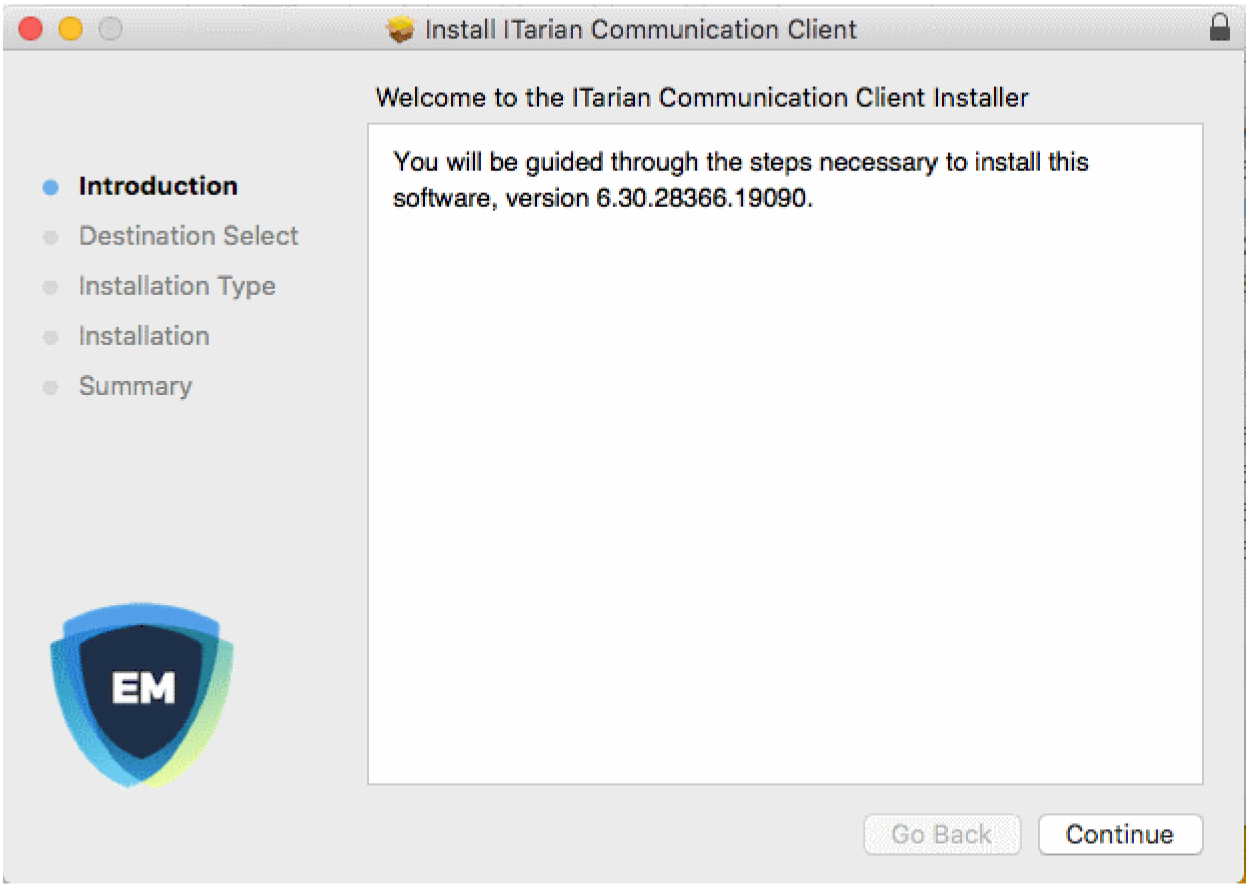
Run installer of Communication Client after download complete

Step 2

Your device will be enrolled and appears in Device List

The EM client setup package file gets downloaded.

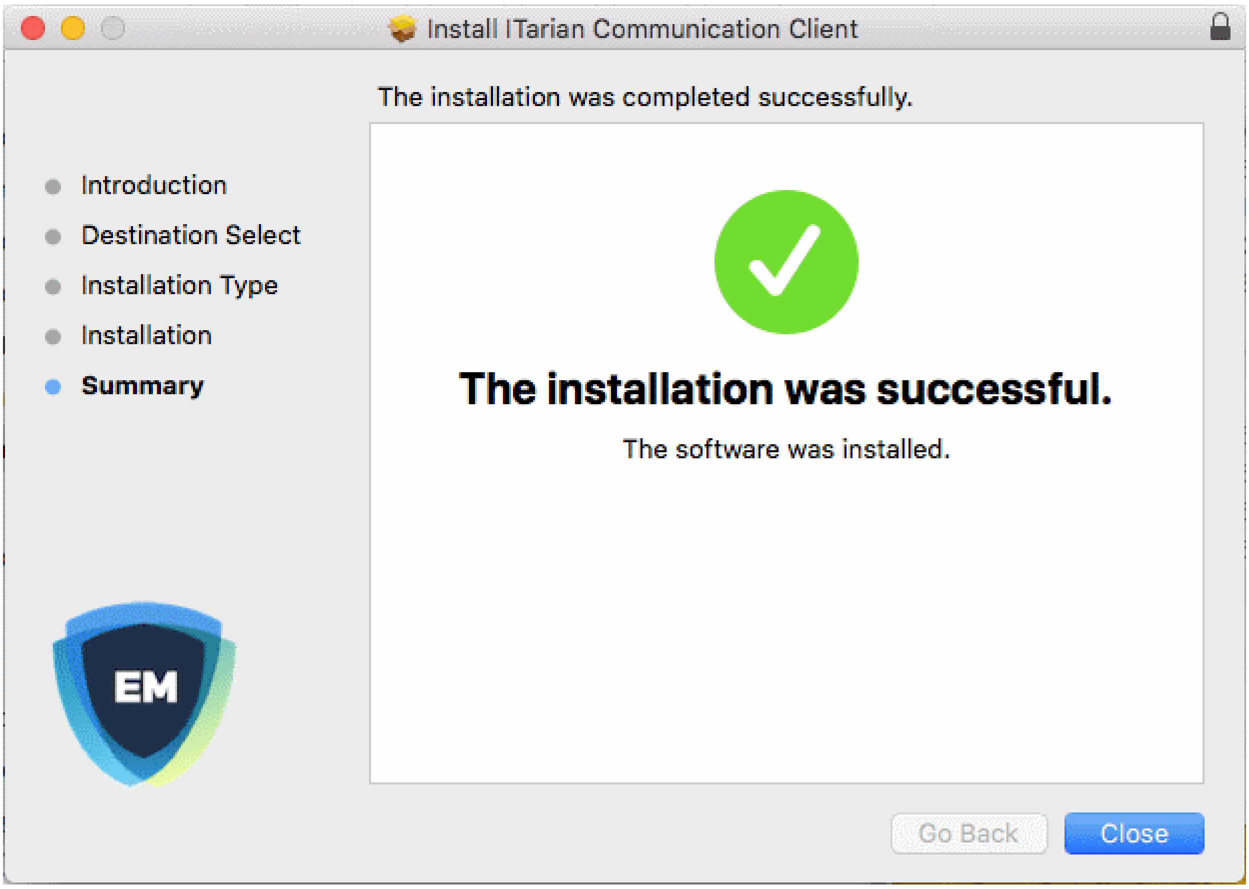
- Open the file to install the communication client.



Welcome to the ITarian Communication Client Installer

You will be guided through the steps necessary to install this software, version 6.30.28366.19090.

- Click 'Continue' and follow the installation wizard

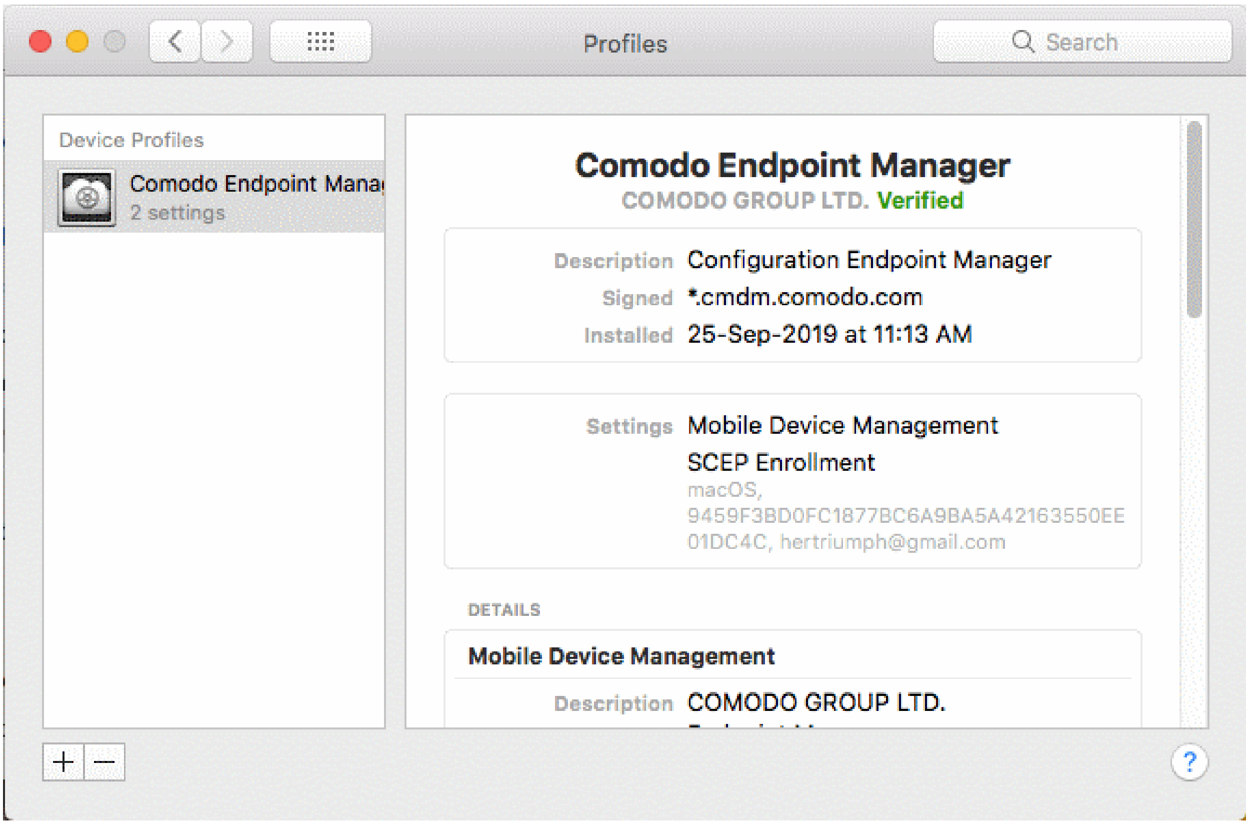


The installation was completed successfully.

The installation was successful.

The software was installed.

- If you have configured the package to install the EM profile, the device profiles screen appears when installation is complete:



Comodo Endpoint Mana
2 settings

**Comodo Endpoint Manager**

COMODO GROUP LTD. Verified

Description Configuration Endpoint Manager
Signed *.cmdm.comodo.com
Installed 25-Sep-2019 at 11:13 AM

Settings Mobile Device Management
SCEP Enrollment
macOS, 9459F3BD0FC1877BC6A9BA5A42163550EE01DC4C, hertriumph@gmail.com

DETAILS

**Mobile Device Management**

Description COMODO GROUP LTD.

The device automatically gets added to Endpoint Manager. The EM communication client icon appears at the top-right of the endpoint screen.

If Comodo Client Security (CCS) is included in the **setup process**, then it is installed automatically. Else you can install CCS manually after device enrollment is complete. See **Remotely Install Packages on Mac OS Devices** for help to do this.

- Endpoint Manager will apply any user-specific profiles to the device. See **Assign Configuration Profiles to User Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user, then the default profiles for Mac OS are applied. See **Manage Default Profiles** for more details.

### 4.1.2.5. Enroll Linux OS Endpoints

- After you **complete the setup process described in 4.1.2**, Endpoint Manager will send an email to your users containing device enrollment instructions.
- The email contains instructions on how to install the EM communication client on their device.
    - Users should open the email and complete the installation on the actual endpoint you want to enroll.
- After installing the communication client, the endpoint will automatically connect to the EM server.

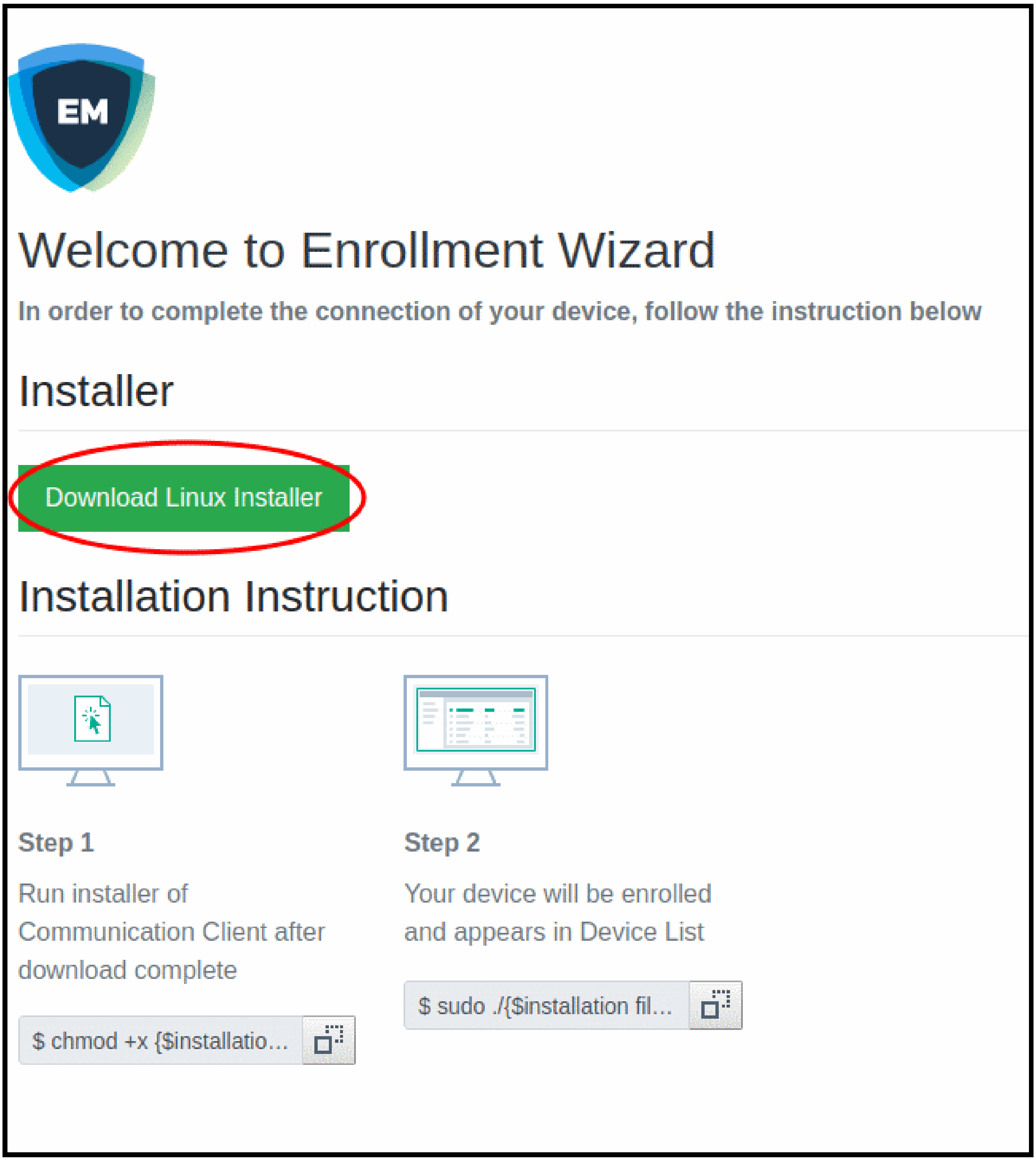
**Supported distributions**

- Ubuntu 18
- Ubuntu 16.04.2
- Cent OS 7
- Debian 8.8

- Red Hat Enterprise 7

**Enroll a Linux device**

- Open the mail on the target device and click the enrollment link. This will start the setup wizard.
- Click the 'Download Linux Installer' button and save the file:



Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Installation Instruction

Step 1

Run installer of Communication Client after download complete

$ chmod +x {$installatio…

Step 2

Your device will be enrolled and appears in Device List

$ sudo ./{$installation fil…

You can install the communication client on the Linux device by completing the following:

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

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

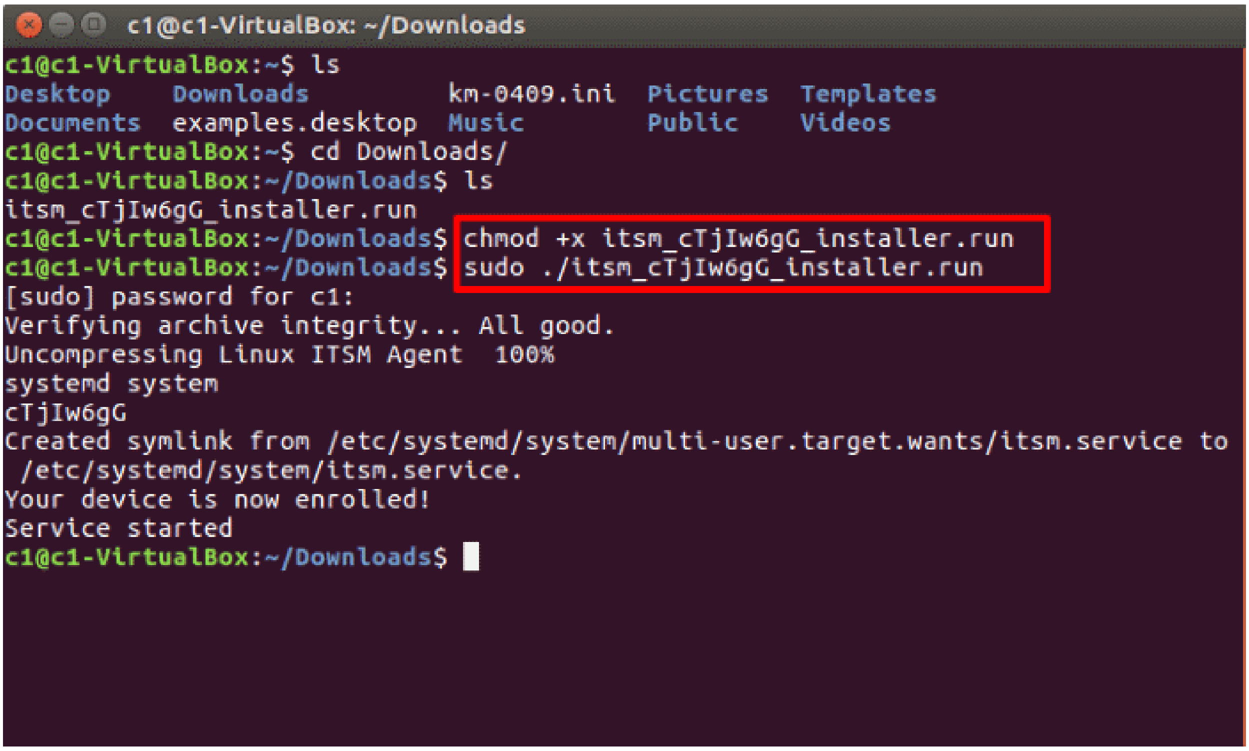
2. Run installer with root privileges - enter the following command:

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

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run



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

- After installation, the communication client will connect to the Endpoint Manager and enroll the device.
- If Comodo Client Security (CCS) is included in the **setup process**, then it is installed automatically. Else you can install CCS manually after device enrollment is complete. See **Remotely Install Packages on Linux Devices** for more details.
- After installing CCS, any EM configuration profiles associated with the user will be applied to the device. See **Assign Configuration Profile(s) to a Users' Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default profiles for Linux are applied. See **Manage Default Profiles** for more details.

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

## 4.1.3. View User Details

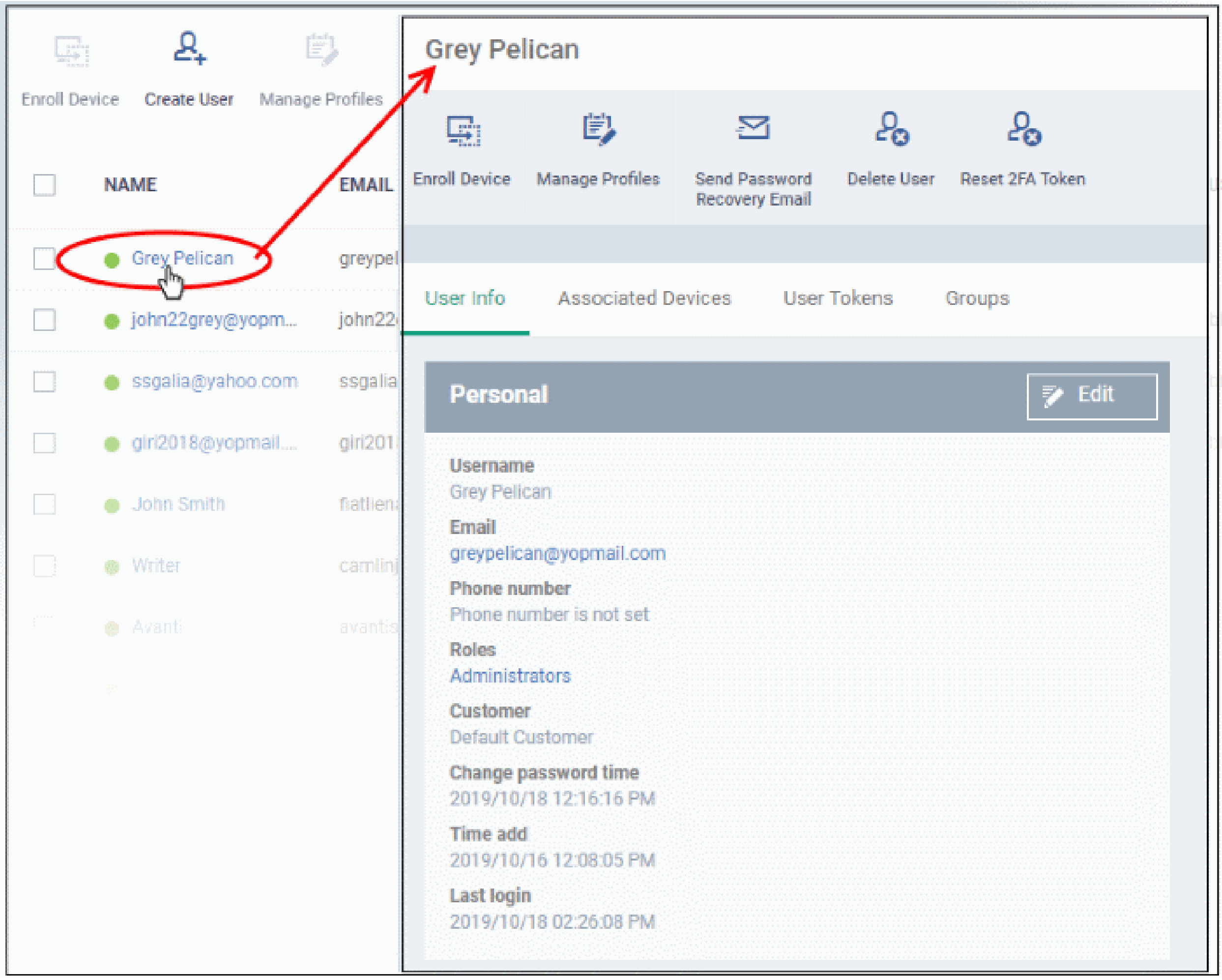
- Click 'Users' > 'User List'

The 'User List' interface lets you view and edit user account details at anytime.

**View user details**

- Click 'Users' > 'User List'
- Click the name of a user

The user details screen opens:



Username
Grey Pelican

Email
greypelican@yopmail.com

Phone number
Phone number is not set

Roles
Administrators

Customer
Default Customer

Change password time
2019/10/18 12:16:16 PM

Time add
2019/10/16 12:08:05 PM

Last login
2019/10/18 02:26:08 PM

- Click the 'Edit' button if you want to modify the user's details. See **Update Details of a User** if you want more help with these settings.
- This area only lets you edit users who were added directly to Endpoint Manager. You cannot edit users that were added via the Comodo Dragon or Comodo One portals.

The user details screen also lets you:

- **Add new devices for a user**
- **Apply configuration profiles to devices**
- **Send password recovery emails for users to access the EM console**
- **Reset two-factor authentication token for a user**
- **View and manage user devices**
- **View device enrollment tokens generated for users**
- **View and manage groups to which a user is a member**

## Add new devices for users

- Click 'Users' > 'User List'
- Click the name of a user
- Click 'Enroll Device' at the top of the details interface

The 'Enroll Devices' dialog will open with the user pre-populated. See **Enroll User Devices for Management** if you need help to complete this process.

### Apply Configuration Profiles to user devices

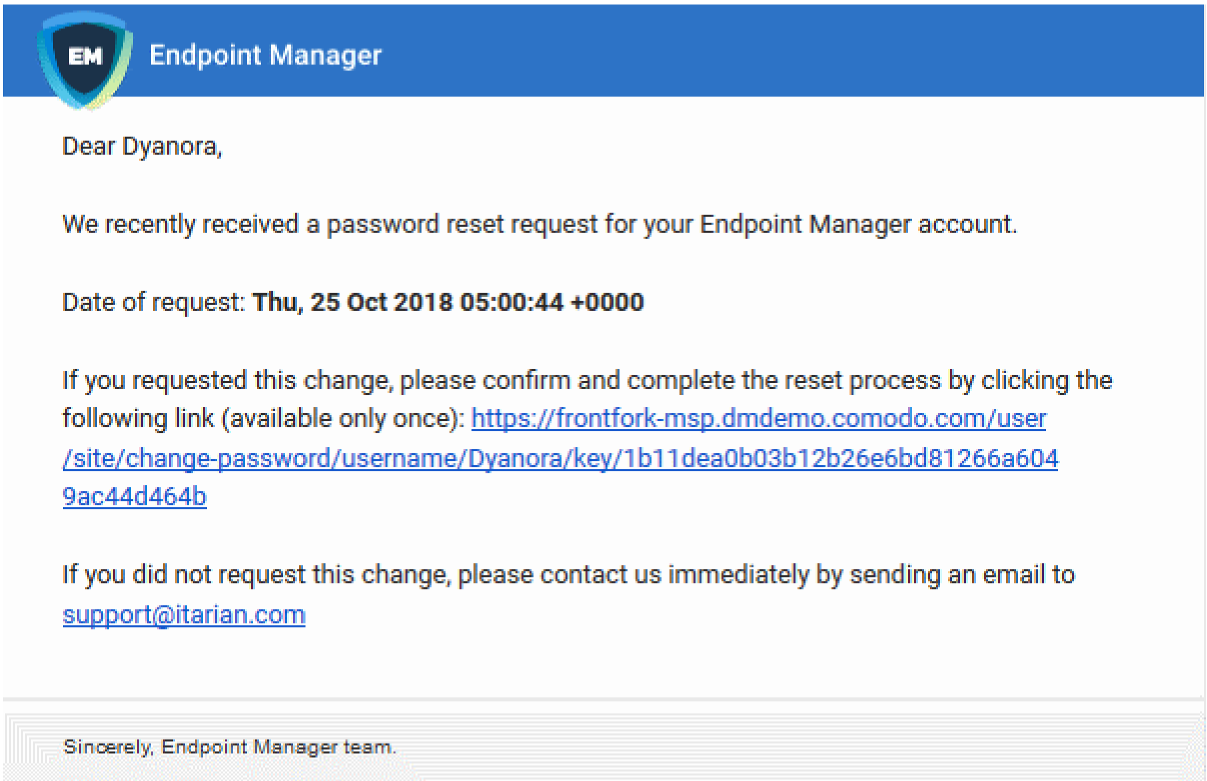
- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'Manage Profiles' button

This will open a list of profiles added to the user's devices. You can add new profiles which will be applied to their devices. See **Assign Configuration Profile(s) to a User's Devices** for more details.

### Send a password recovery email to users

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'Send Password Recovery Email' button to start the process.
    - Note - you can only send password emails to users added to Endpoint Manager. This option is not available for users added via the CD or C1 management portal.

The email contains a link which lets the user reset their password:



Endpoint Manager

Dear Dyanora,

We recently received a password reset request for your Endpoint Manager account.

Date of request: **Thu, 25 Oct 2018 05:00:44 +0000**

If you requested this change, please confirm and complete the reset process by clicking the following link (available only once): https://frontfork-msp.dmdemo.comodo.com/user/site/change-password/username/Dyanora/key/1b11dea0b03b12b26e6bd81266a6049ac44d464b

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

Sincerely, Endpoint Manager team.

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

### Reset two-factor authentication token for a user

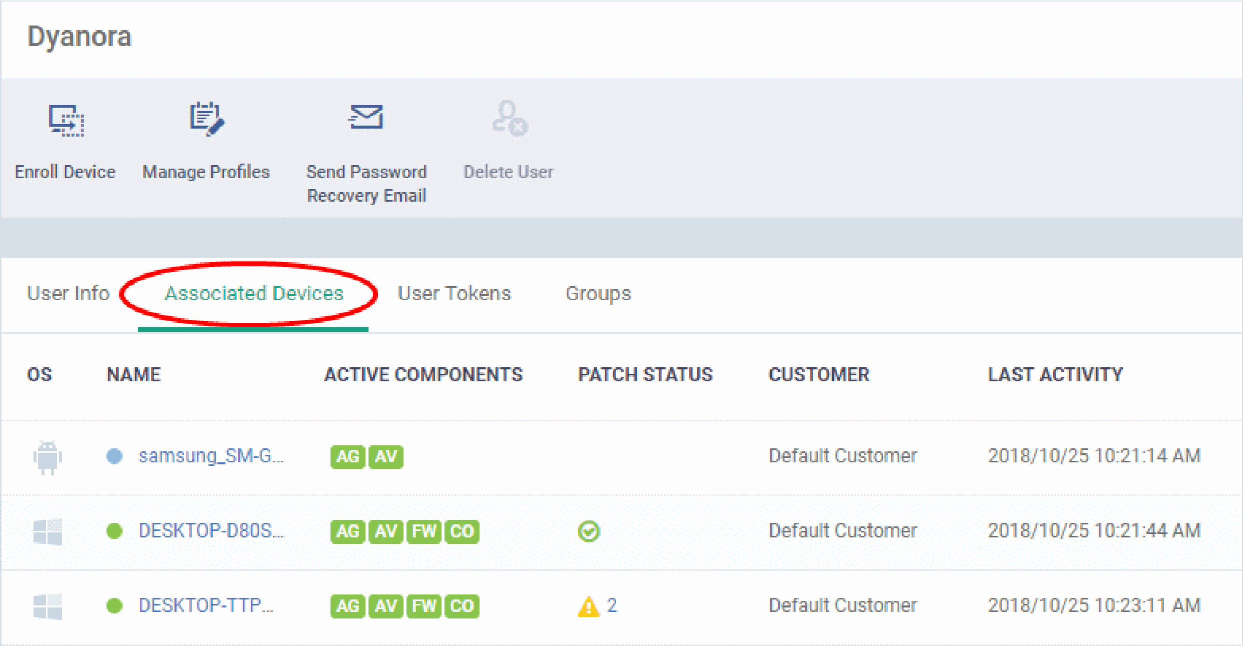
- Click 'Users' > 'User List'
- Click the name of a user
- Click 'Reset 2FA Token' above

This will start the reset procedure. See '**Reset Two Factor Authentication Token for a User** for more details.

### View devices associated with a user

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'Associated Devices' link

This tab shows all devices enrolled for the user:



| OS | NAME | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LAST ACTIVITY |
|---|---|---|---|---|---|
| | samsung_SM-G... | AG AV | | Default Customer | 2018/10/25 10:21:14 AM |
| | DESKTOP-D80S... | AG AV FW CO | ✓ | Default Customer | 2018/10/25 10:21:44 AM |
| | DESKTOP-TTP... | AG AV FW CO | ⚠ 2 | Default Customer | 2018/10/25 10:23:11 AM |

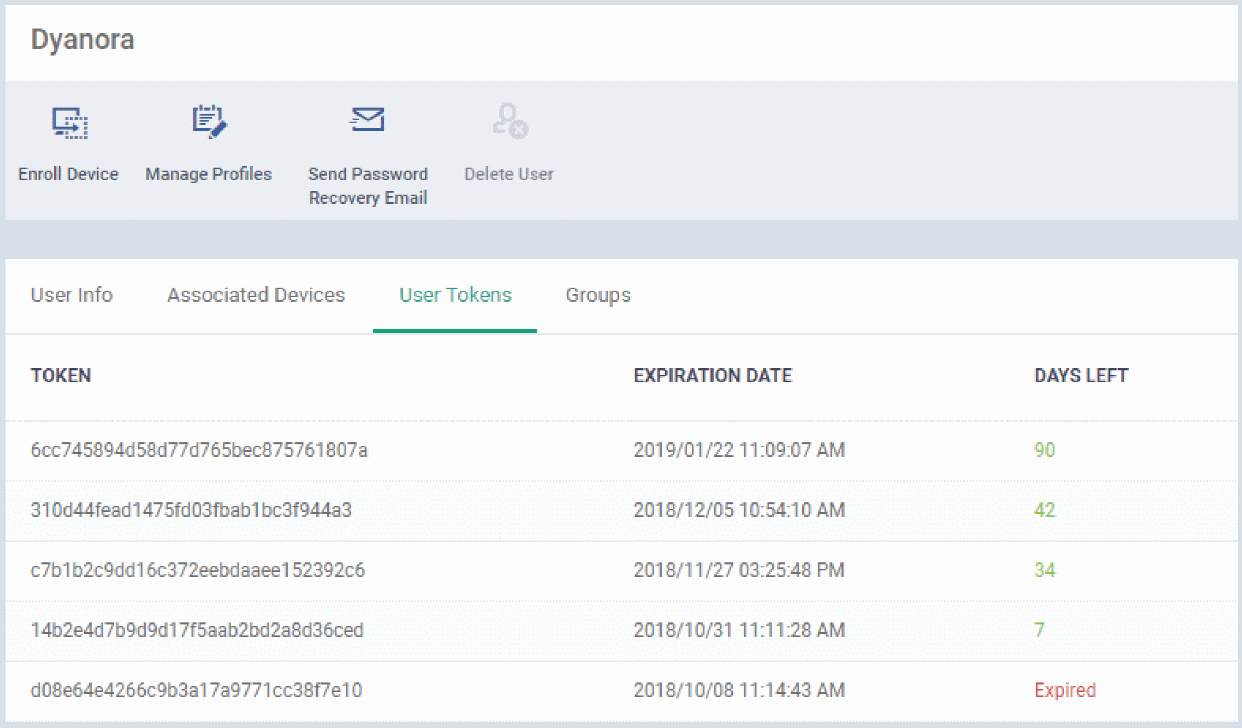
| Associated Devices - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| OS | The operating system of the device. |
| Name | The label of the device as assigned by the user.<br>• If no name is assigned, the model number of the device will be used as the name of the device.<br>• Click the name of the device to open the 'Summary' screen of the Device Details interface.<br>• See '**View Summary Information**' for more details. |
| Active Components | The endpoint security components running on the device. For example, Antivirus, Firewall, Containment etc. |
| Patch Status | How many OS patches and updates are ready for installation on the endpoint. Patch status is only available for Windows endpoints.<br>• Click the number to open the 'Patch Management' tab of the 'Device Details' interface. It allows you to initiate installation of the missing patches.<br>• See **View and Manage Patches for Windows and 3rd Party Applications** for more details. |
| Company | The customer organization to which the device was registered. |
| Last Activity | The date and time at which the device last communicated with the EM server. |

## View User Tokens

Endpoint Manager generates a unique token for each user when you enroll a device for them. This token is used by the communication client on the device to authenticate the enrollment request to Endpoint Manager. A single token can be used to enroll any number of devices for the same user. A token is valid for 90 days.

The 'User Tokens' interface displays a list of generated user tokens. You can use these tokens to manually enroll device for specific users

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'User Tokens' link

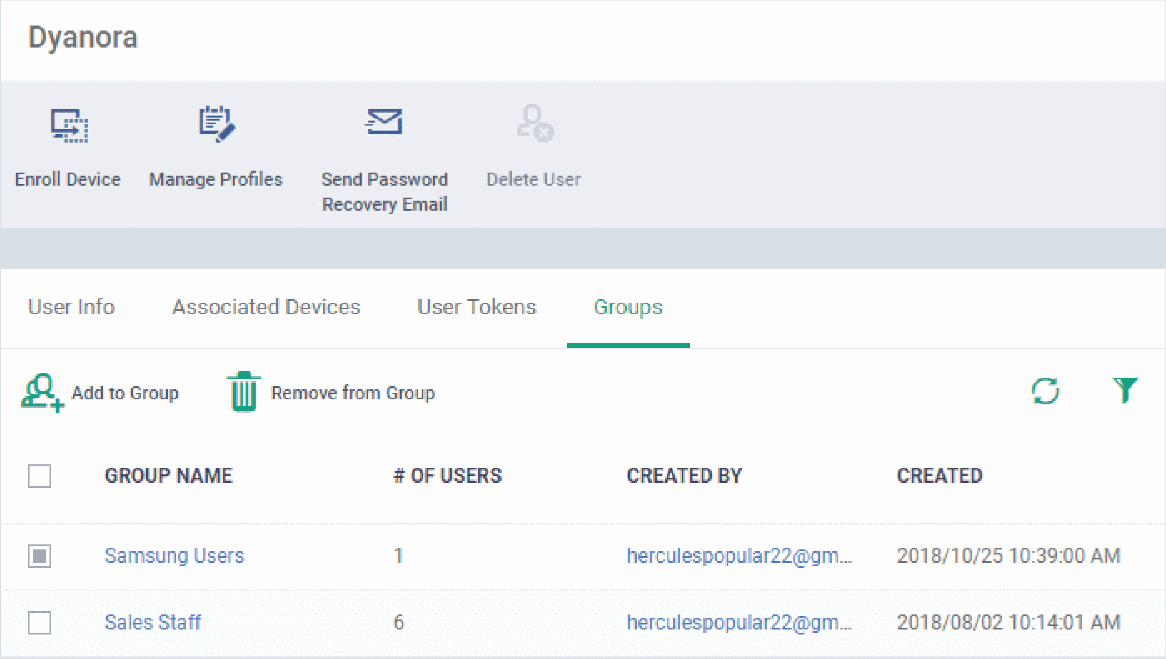


| TOKEN | EXPIRATION DATE | DAYS LEFT |
|---|---|---|
| 6cc745894d58d77d765bec875761807a | 2019/01/22 11:09:07 AM | 90 |
| 310d44fead1475fd03fbab1bc3f944a3 | 2018/12/05 10:54:10 AM | 42 |
| c7b1b2c9dd16c372eebdaaee152392c6 | 2018/11/27 03:25:48 PM | 34 |
| 14b2e4d7b9d9d17f5aab2bd2a8d36ced | 2018/10/31 11:11:28 AM | 7 |
| d08e64e4266c9b3a17a9771cc38f7e10 | 2018/10/08 11:14:43 AM | Expired |

| User Tokens - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Token | The unique serial number of each enrollment token. |
| Expiration Date | Date till which the token is valid. Users can enroll devices using the same token until expiry. |
| Days left | How many days remain until the token expires. |

### To view and manage user groups to which the user belongs

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'Groups' tab to view all groups to which the user belongs:



| ☐ | GROUP NAME | # OF USERS | CREATED BY | CREATED |
|---|---|---|---|---|
| ■ | Samsung Users | 1 | herculespopular22@gm... | 2018/10/25 10:39:00 AM |
| ☐ | Sales Staff | 6 | herculespopular22@gm... | 2018/08/02 10:14:01 AM |

| Groups - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Group Name | The label of the user group<br>• Click the group name to open the 'Group Details' interface.<br>• See **Edit a User Group** for more details. |
| Number of Users | The total count of users in the group. |
| Created By | The administrator who added the group.<br>• Click the name to open the 'User Details' interface of the administrator. |
| Created | The date and time at which the group was created. |

### 4.1.3.1. Update the Details of a User

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'Edit' button

The 'User Details' pane lets you update the username, email address and phone number of a user. You can also view devices associated with the user and send them a password recovery email.

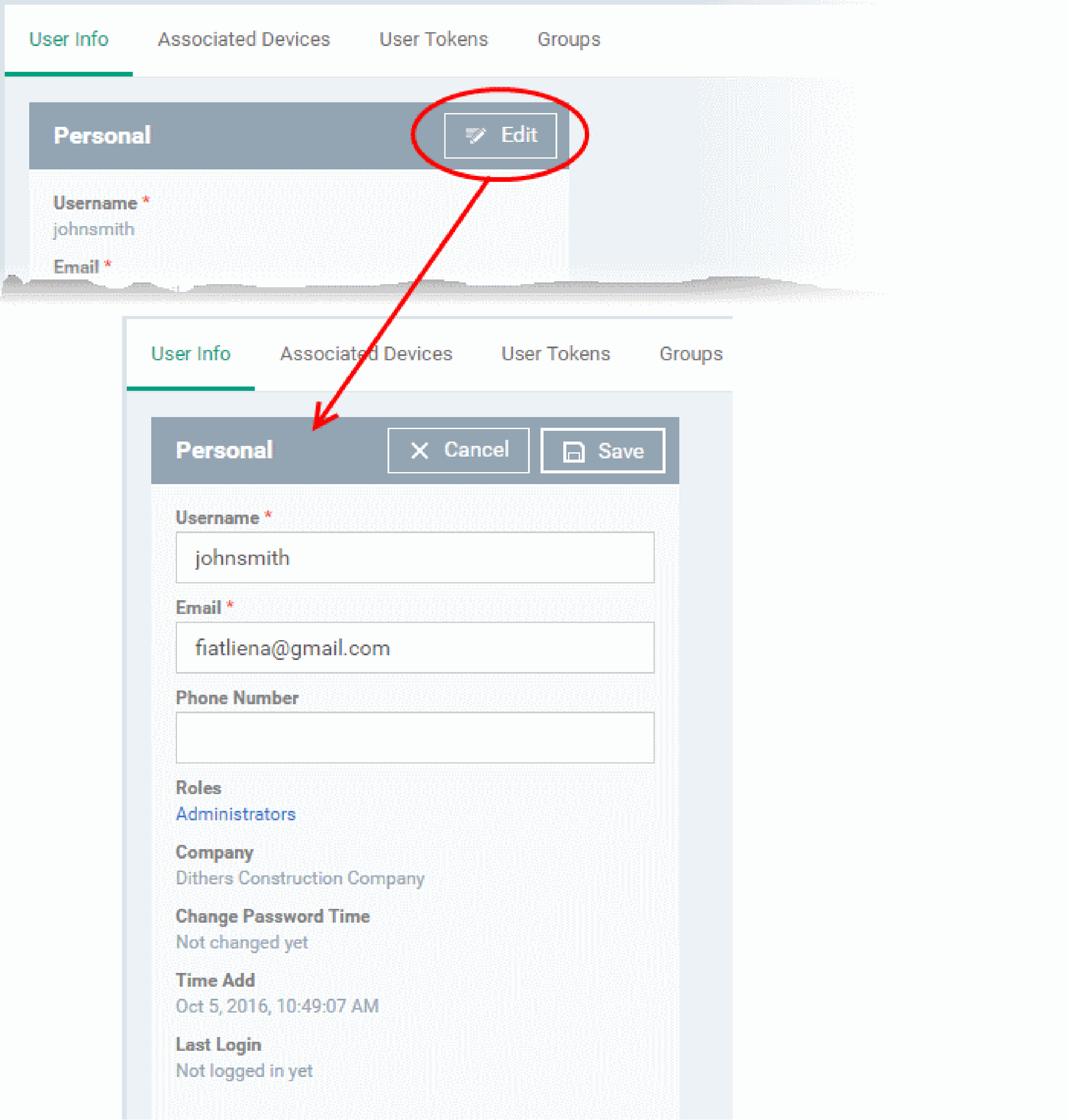
**Note**: The 'Edit' option is only available for users added in the Endpoint Manager interface. It is not available for users that were added via the CD or C1 portals. Those users must be edited in the CD or C1 portal. All changes will be reflected in the EM interface.

**To update the details of a user**

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

The user details screen will open.

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



Username *
johnsmith

Email *
fiatliena@gmail.com

Phone Number

Roles
Administrators

Company
Dithers Construction Company

Change Password Time
Not changed yet

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

Last Login
Not logged in yet

- Update the username, email address of the user and the phone number as required.
- Click 'Save' at the top for your changes to take effect

The role assigned to the user is displayed under 'Roles'.

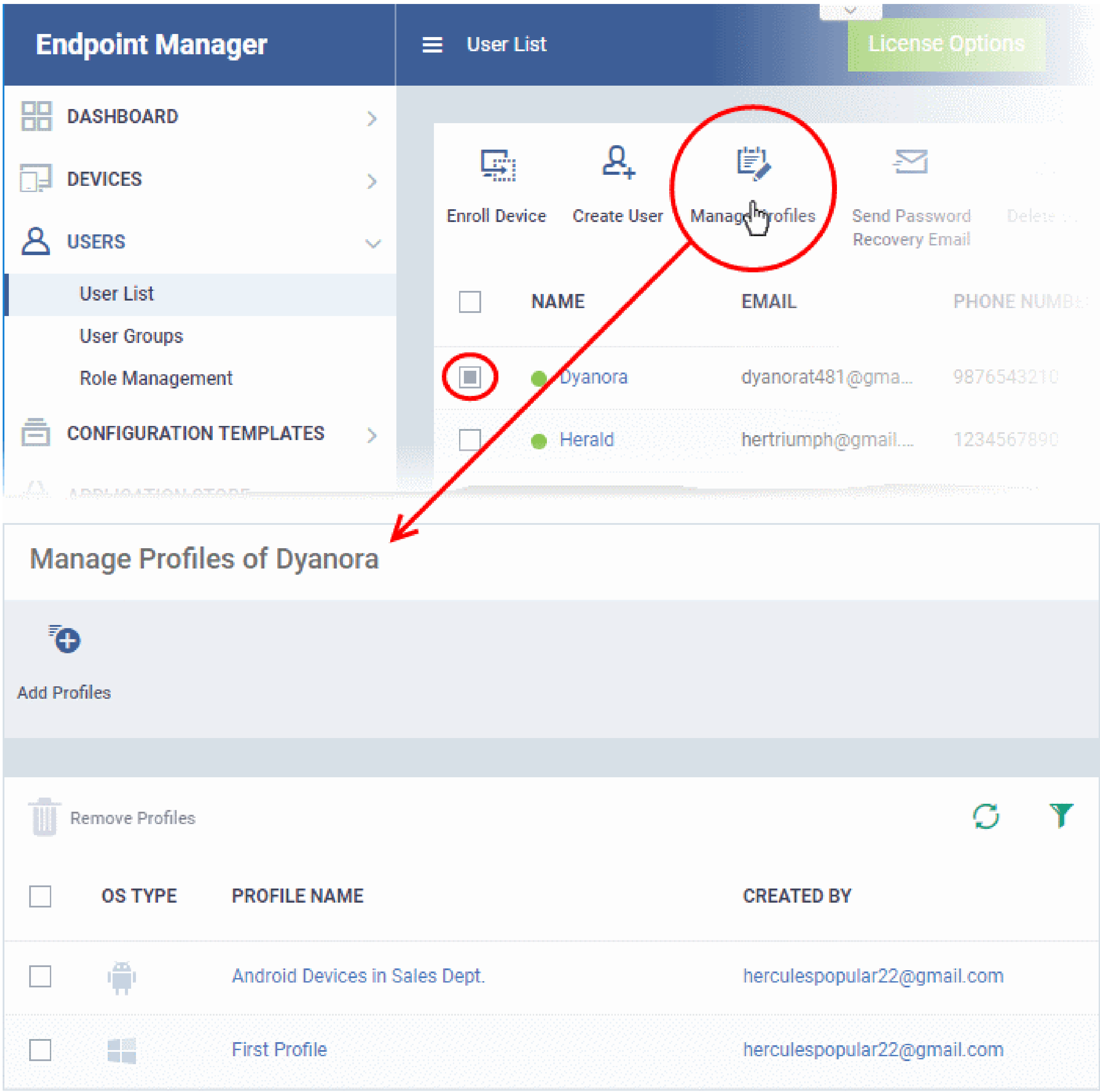
- Click the role name to change the role if required.
- See '**Manage Roles Assigned to a User**' for more details.

## 4.1.4. Assign Configuration Profiles to User Devices

- Click 'Users' > 'User List'
- Profiles assigned to a user will apply to all devices owned by the user.
- You can apply multiple profiles for different operating systems to a user. Endpoint Manager will apply the appropriate profile to a device depending on its OS.

**To manage configuration profiles assigned to a user**

- Click 'Users' > 'User List'
- Select the user for whom you want to assign/remove profile(s)
- Click 'Manage Profiles'



| | NAME | EMAIL | PHONE NUMBE |
|---|---|---|---|
| ☒ | Dyanora | dyanorat481@gma... | 9876543210 |
| □ | Herald | hertriumph@gmail.... | 1234567890 |

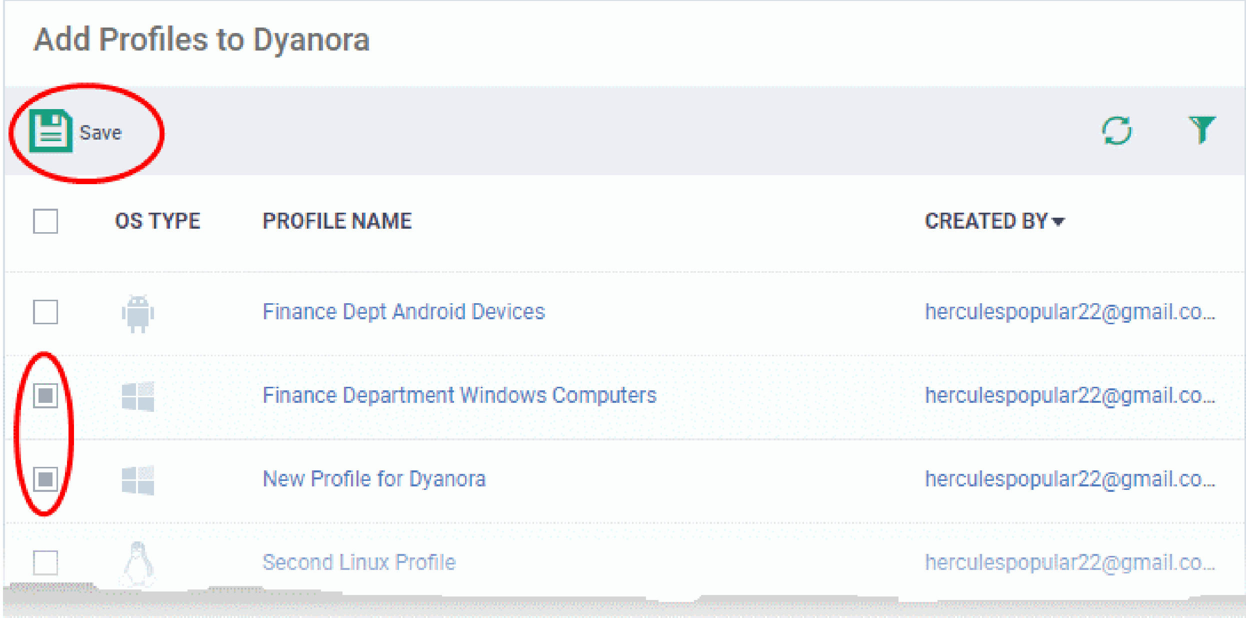
| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |
| □ | | First Profile | herculespopular22@gmail.com |

The list shows all profiles assigned to a user. You can add, remove or edit profiles as required.

**Tip**: Alternatively, click 'Users' > 'User List' > click on a username > 'Manage Profiles'.

**To add a new profile to a user**

- Click 'Users' > 'User List'
- Select the target user
- Click 'Manage Profiles'
- Click 'Add Profiles':

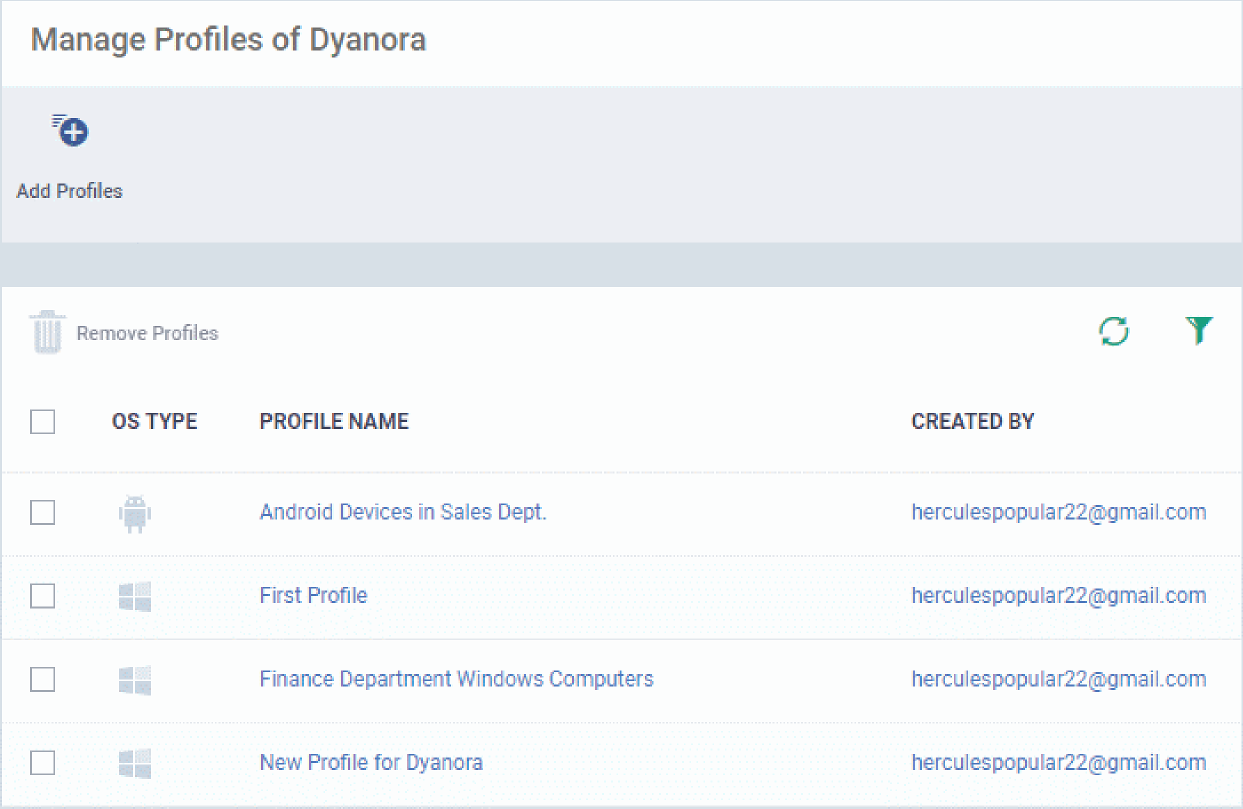


Add Profiles to Dyanora

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Finance Dept Android Devices | herculespopular22@gmail.co... |
| ☑ | | Finance Department Windows Computers | herculespopular22@gmail.co... |
| ☑ | | New Profile for Dyanora | herculespopular22@gmail.co... |
| □ | | Second Linux Profile | herculespopular22@gmail.co... |

- The next screen shows all profiles that you can add to the user. The list excludes profiles which are already assigned to the user.
- Select the profiles you want to add and click 'Save'
  - Click the funnel icon on the right if you want to search for a particular profile

The new profiles will be automatically deployed to the user's devices.



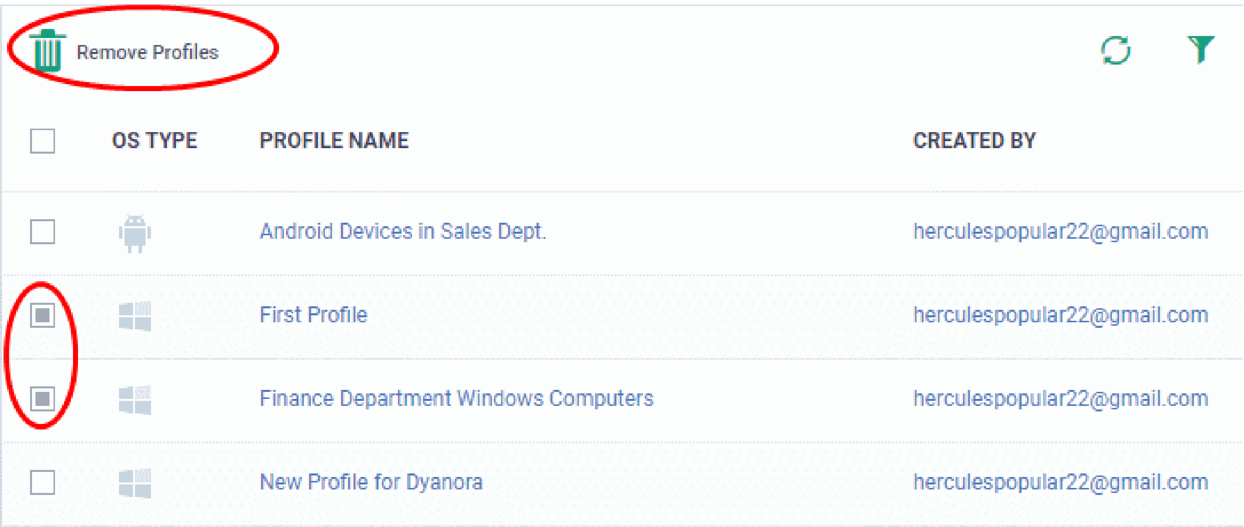
Manage Profiles of Dyanora

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |
| □ | | First Profile | herculespopular22@gmail.com |
| □ | | Finance Department Windows Computers | herculespopular22@gmail.com |
| □ | | New Profile for Dyanora | herculespopular22@gmail.com |

**To remove a profile**

- Click 'Users' > 'User List'
- Select the target user
- Click 'Manage Profiles'

- Select the profiles you want to disassociate and click 'Remove Profiles'



Remove Profiles

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |
| ☑ | | First Profile | herculespopular22@gmail.com |
| ☑ | | Finance Department Windows Computers | herculespopular22@gmail.com |
| □ | | New Profile for Dyanora | herculespopular22@gmail.com |

- The selected profiles will be immediately removed from devices belonging to the user. See note below:

**Note**: There are 4 ways you can assign a profile to a device:

1. Assign the profile the device owner, aka the 'user'.

- Click 'Users' > 'User List' > click a username > 'Manage Profiles' > 'Add Profiles'

2. Assign the profile to the device itself.

- Click 'Devices' > 'Device List' > click a device name > 'Manage Profiles' > 'Add Profiles'

3. Assign a profile to a device group. Make the device a member of the group.

- Click 'Devices' > 'Device List' > 'Group Management' tab > click a group name > 'Manage Profiles'

4. Assign a profile to a user group. Make the user (device owner) a member of the group

- Click 'Users' > 'User Groups' > click a group name > 'Manage Profiles' / 'Associated Devices'

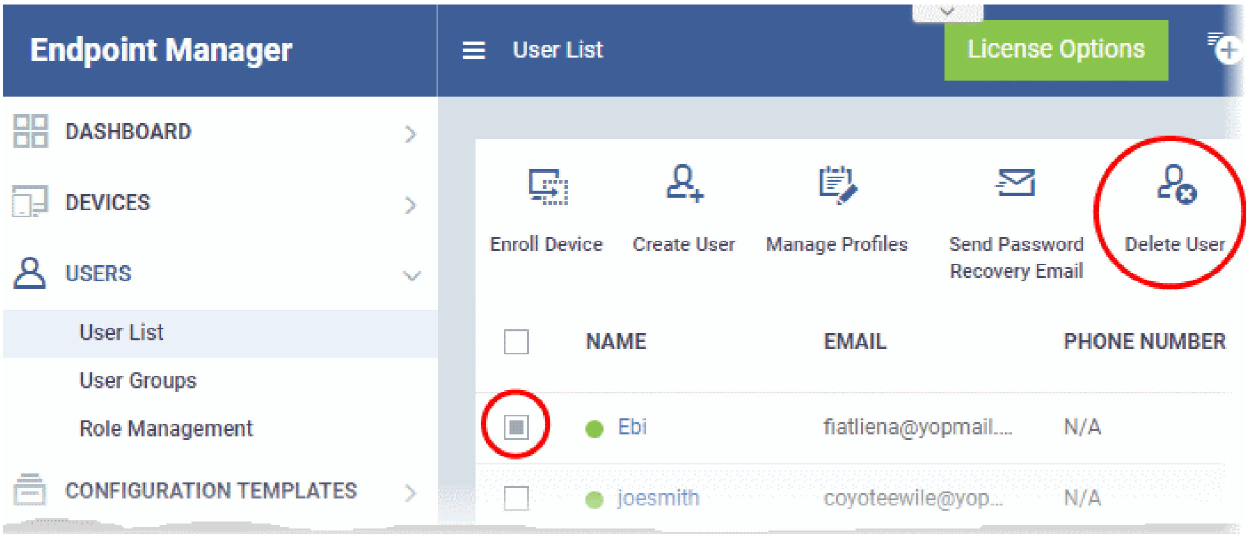
Removing a profile as described in this section will only remove profiles which arrived on the device via method # 1 above.

The profile may remain on the device if it was (also) deployed via methods 2, 3 or 4 above.

## 4.1.5. Remove a User

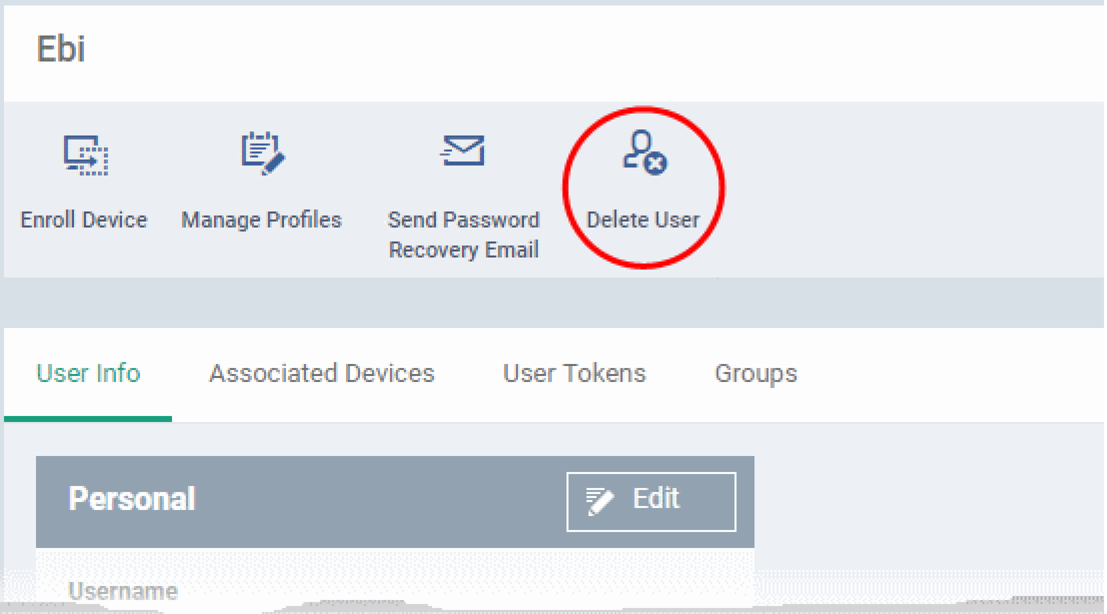
You can remove users if their devices no longer need to be managed by Endpoint Manager.

- Click 'Users' > 'User List'
- Select the target user and click 'Delete User':

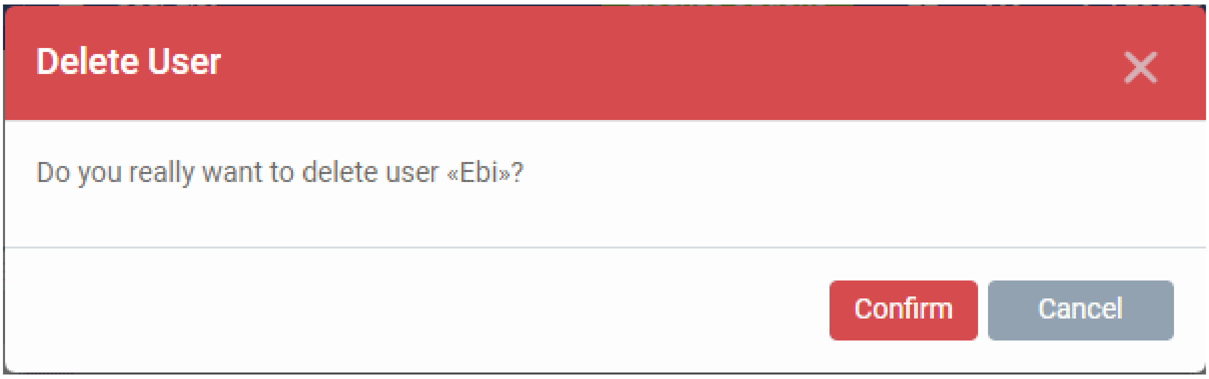


| | NAME | EMAIL | PHONE NUMBER |
|---|---|---|---|
| ☒ | Ebi | fiatliena@yopmail.... | N/A |
| □ | joesmith | coyoteewile@yop... | N/A |

- Alternatively, click on the name of the user
- Click 'Delete User' in the 'User Details' screen.



- Click 'Confirm' in the confirmation dialog



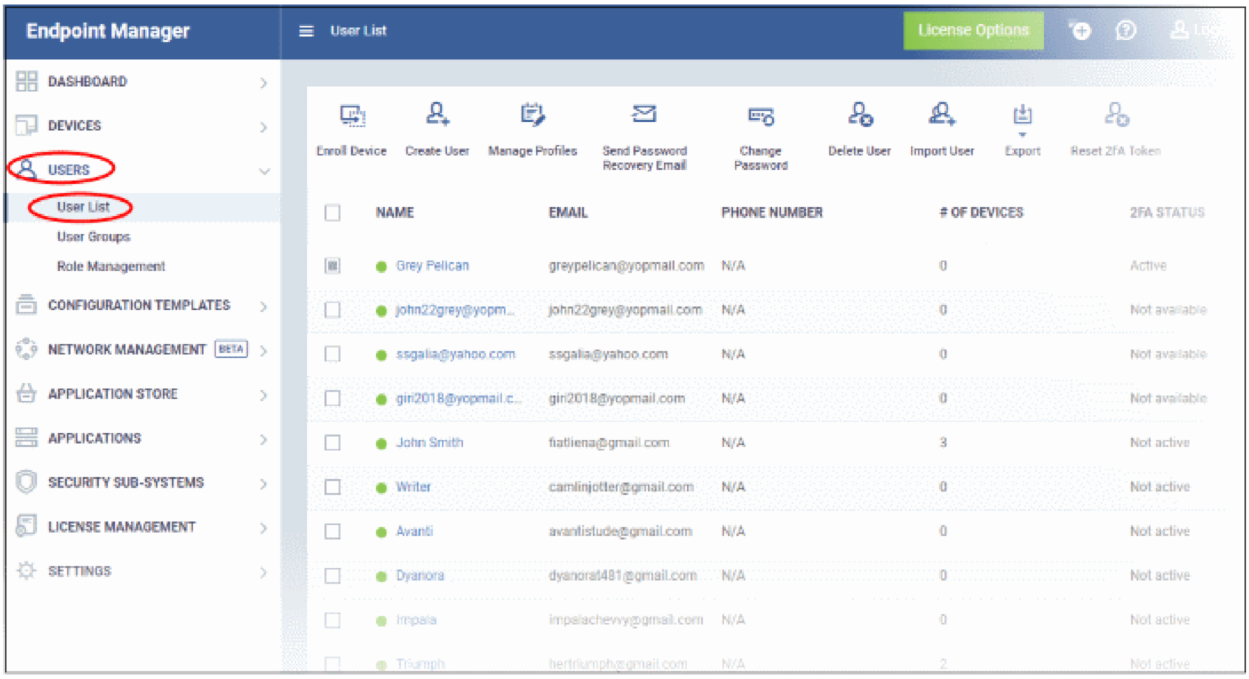
Do you really want to delete user «Ebi»?

**Note 1**: Users added via the CD or C1 portal cannot be removed via the EM interface. They can only be removed from the source portal through which they were added. Once removed they are automatically deleted from EM.

**Note 2**: Users cannot be removed if they still have devices. Ensure all devices associated with a user are removed or reassigned to another user. See **Remove a Device** and **Change Device's Owner** for more details.

## 4.1.6. Generate New Password for a User

- Click 'Users' > 'User List' > select a user > click 'Change Password'
- This area lets you manually set a new password for a user, instead of letting them reset their own password.



| | NAME | EMAIL | PHONE NUMBER | # OF DEVICES | 2FA STATUS |
|---|---|---|---|---|---|
| ☒ | Grey Pelican | greypelican@yopmail.com | N/A | 0 | Active |
| □ | john22grey@yopm... | john22grey@yopmail.com | N/A | 0 | Not available |
| □ | ssgalia@yahoo.com | ssgalia@yahoo.com | N/A | 0 | Not available |
| □ | giri2018@yopmail.c... | giri2018@yopmail.com | N/A | 0 | Not available |
| □ | John Smith | fiatiena@gmail.com | N/A | 3 | Not active |
| □ | Writer | camlinjotter@gmail.com | N/A | 0 | Not active |
| □ | Avanti | avantistude@gmail.com | N/A | 0 | Not active |
| □ | Dyanora | dyanorat481@gmail.com | N/A | 0 | Not active |
| □ | Impala | impalachevvy@gmail.com | N/A | 0 | Not active |
| □ | Triumph | hertriumph@gmail.com | N/A | 2 | Not active |

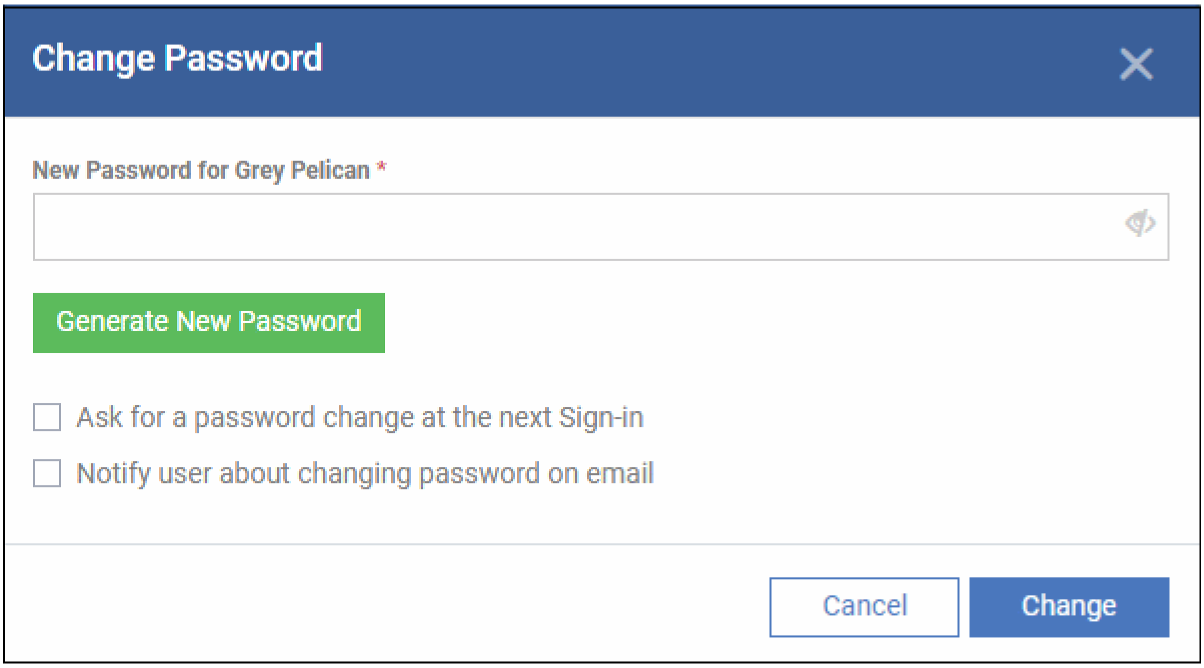
Note - This interface only applies to users that were created in Endpoint Manager itself. It does not change the passwords of users who were created in the C1 / Dragon portal.

There are two possible ways to change user passwords:

- **Send a password recovery email -** Let the user reset their own password. **Click here** for more details.
- **Generate a new password -** Create a new password on behalf of the user. This section explains this method.

**Generate a new password.**

- Click 'Users' > 'User List'
- Select the user and click 'Change Password'
- This opens the reset dialog:


Change Password

New Password for Grey Pelican *

□ Ask for a password change at the next Sign-in

□ Notify user about changing password on email

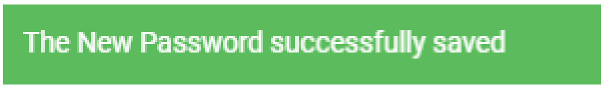
Type a new password for the user in the box provided. Alternatively, click 'Generate New Password' to have Endpoint Manager create a random password.

**Ask for a password change at the next Sign-in -** After logging in with the new password you provide, users will be forced to change their password again. This improves privacy by ensuing only the user knows their own password.

**Notify user about changing password on email -** Will send an email to users that informs them their password has been reset.

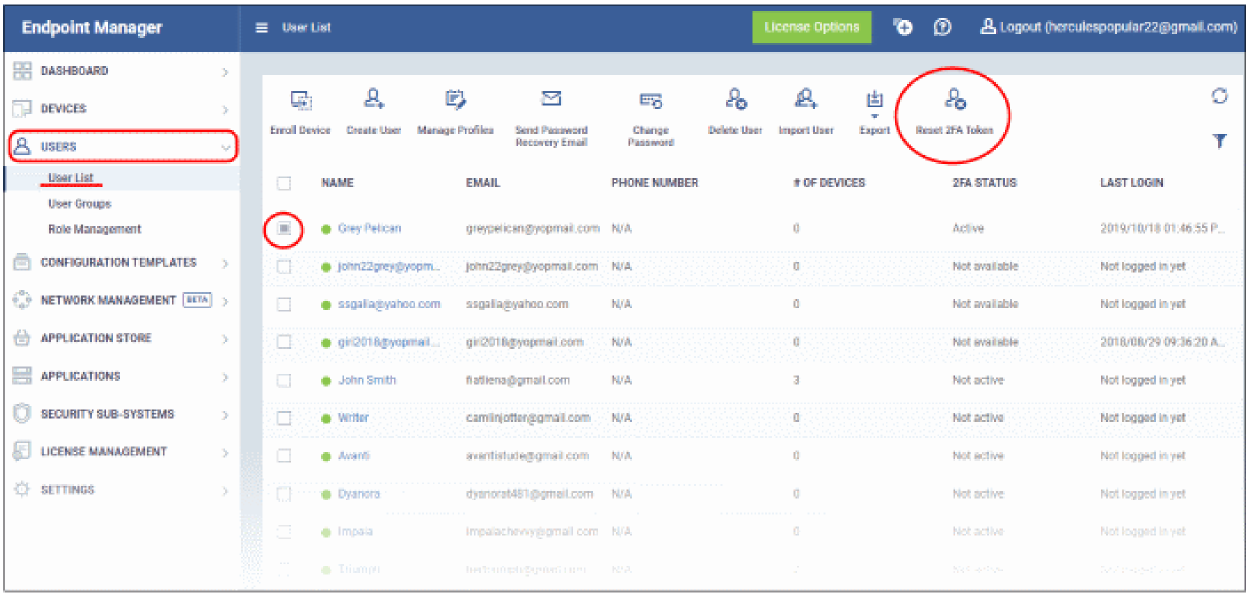
- Click 'Change'

The following confirmation is shown:


The New Password successfully saved

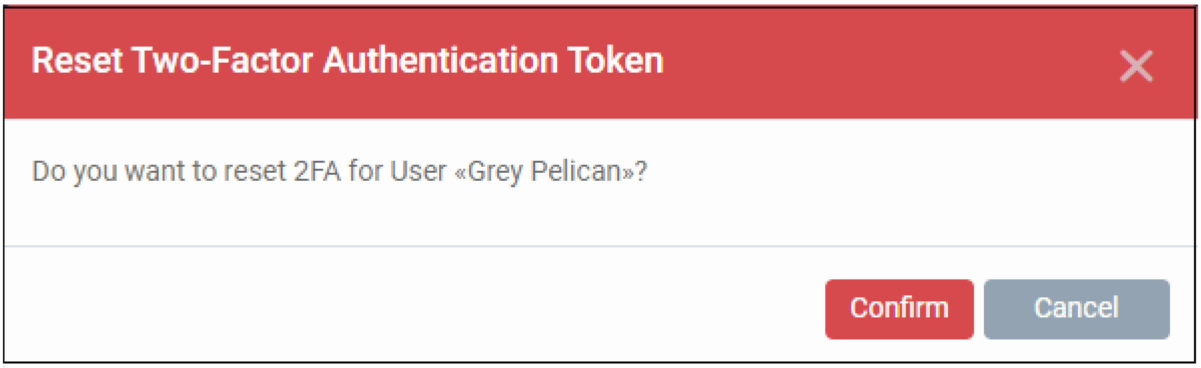
## 4.1.7. Reset Two Factor Authentication Token for a User

- Click 'Users' > 'User List' > select a user > click 'Reset 2FA token'
- This feature lets you force admins whose use two-factor authentication (2FA) to reset it at their next login.
    - **Click here** if you want to know how to setup 2FA in Endpoint Manager.
- Note: This action does not reset 2FA on C1 logins. It only affects 2FA for admins who were created in Endpoint Manager itself.



| | NAME | EMAIL | PHONE NUMBER | # OF DEVICES | 2FA STATUS | LAST LOGIN |
|---|---|---|---|---|---|---|
| ☑ | Grey Pelican | greypelican@yopmail.com | N/A | 0 | Active | 2019/10/18 01:46:55 P... |
| □ | john22grey@yopm... | john22grey@yopmail.com | N/A | 0 | Not available | Not logged in yet |
| □ | ssgalla@yahoo.com | ssgalla@yahoo.com | N/A | 0 | Not available | Not logged in yet |
| □ | giri2018@yopmail... | giri2018@yopmail.com | N/A | 0 | Not available | 2018/08/29 09:36:20 A... |
| □ | John Smith | flatlena@gmail.com | N/A | 3 | Not active | Not logged in yet |
| □ | Writer | camlinjotter@gmail.com | N/A | 0 | Not active | Not logged in yet |
| □ | Avanti | avantistude@gmail.com | N/A | 0 | Not active | Not logged in yet |
| □ | Dyanora | dyanora1481@gmail.com | N/A | 0 | Not active | Not logged in yet |
| □ | Impala | impalachevy@gmail.com | N/A | 0 | Not active | Not logged in yet |

- Click 'Users' > 'User List'
- Select the user and click 'Reset 2FA Token' above
    - Alternatively click the name of the user then click 'Reset 2FA Token'

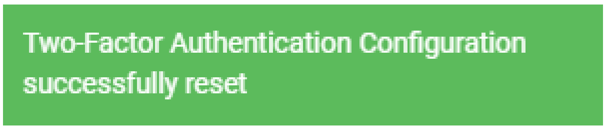


Reset Two-Factor Authentication Token

Do you want to reset 2FA for User «Grey Pelican»?

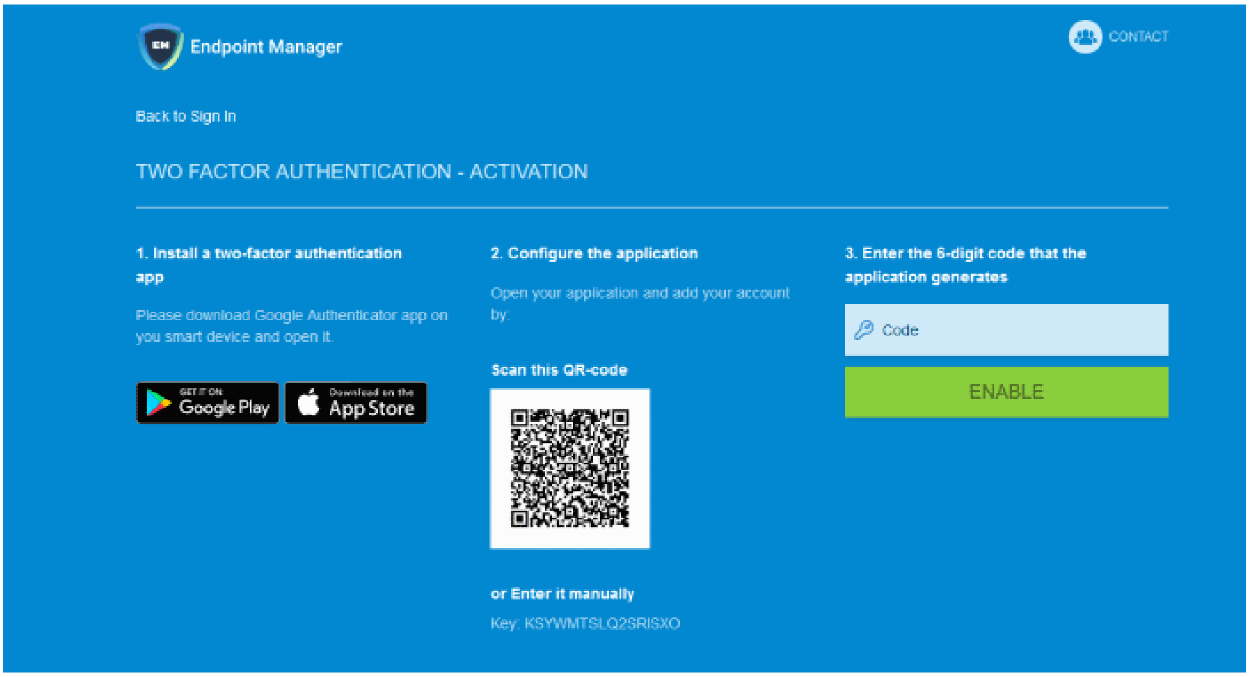
- Click 'Confirm'

A success message is shown:



Two-Factor Authentication Configuration successfully reset

Admin after entering into his / her EM credentials in the login page next time is asked to configure 2FA again.



TWO FACTOR AUTHENTICATION - ACTIVATION

1. Install a two-factor authentication app

Please download Google Authenticator app on you smart device and open it.

2. Configure the application

Open your application and add your account by:

Scan this QR-code

or Enter it manually

Key: KSYWMTSLQ2SRISXO

3. Enter the 6-digit code that the application generates

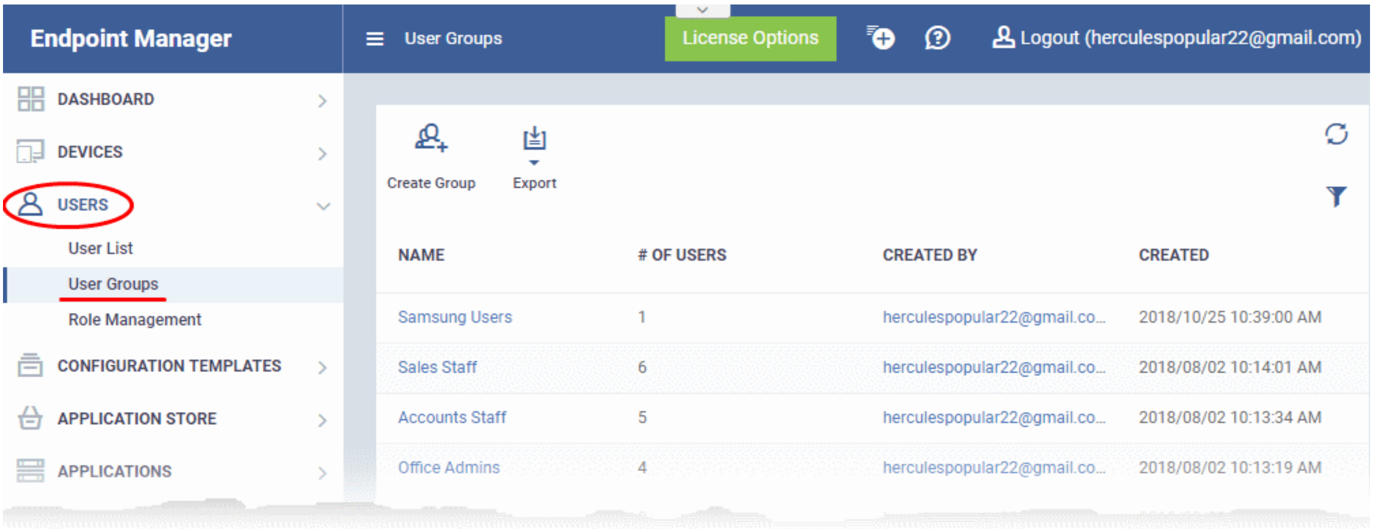
The tutorial to configure 2FA is explained in detail **here**.

## 4.2. Manage User Groups

- Click 'Users' > 'User Groups'
- Endpoint Manager lets you to create logical groups of users to simplify and streamline user management. For example, users could be grouped according to existing corporate units ('Sales Dept.', 'Accounts Dept.') and/or by type of user.
- Once created, dedicated configuration profiles can be applied to each user group as required. See **Configuration Profiles** for more help with profiles.
- You can also import users/user groups from Active Directory using LDAP. EM periodically synchronizes with AD to ensure any user updates are mirrored in the EM database. See **Import User Groups from LDAP** for more details.

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

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

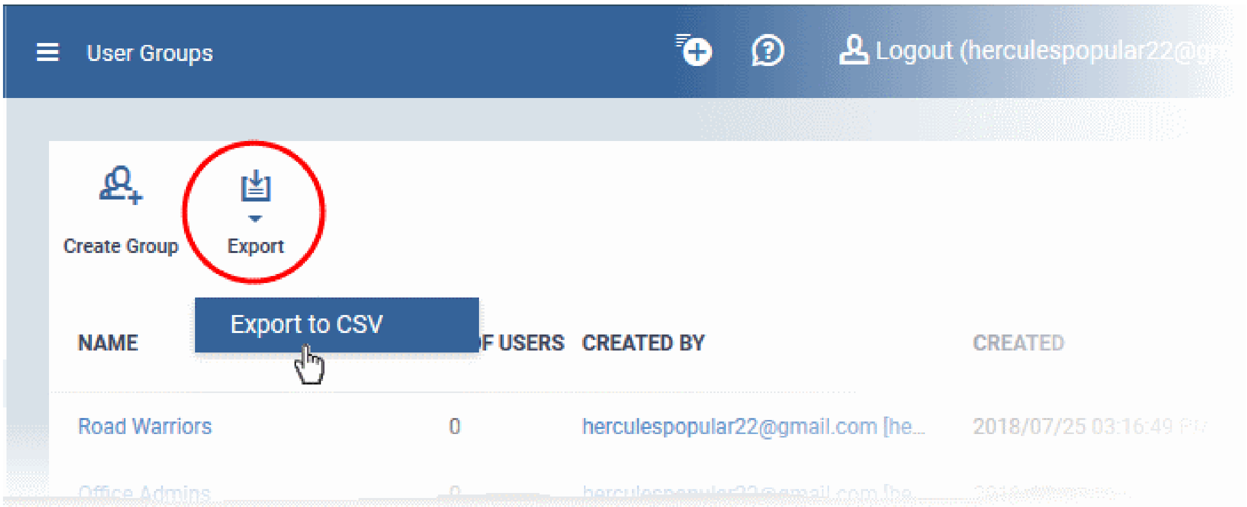


| NAME | # OF USERS | CREATED BY | CREATED |
|---|---|---|---|
| Samsung Users | 1 | herculespopular22@gmail.co... | 2018/10/25 10:39:00 AM |
| Sales Staff | 6 | herculespopular22@gmail.co... | 2018/08/02 10:14:01 AM |
| Accounts Staff | 5 | herculespopular22@gmail.co... | 2018/08/02 10:13:34 AM |
| Office Admins | 4 | herculespopular22@gmail.co... | 2018/08/02 10:13:19 AM |

| User Groups - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The user group label.<br>• Click the name of a group to view and manage its members, assign configuration profiles and more. See **Edit a User Group** for more details. |
| Number of Users | Shows how many users are in the group. |
| Created By | The administrator who created the group.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created | Date and time at which the group was created. |
| **Controls** | |
| Create Group | Add a new user group to EM and include users into it. See **Create a New User Group** for more details. |
| Export | Save the list of user groups as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of User Groups** for more details. |

## Export the List of User Groups

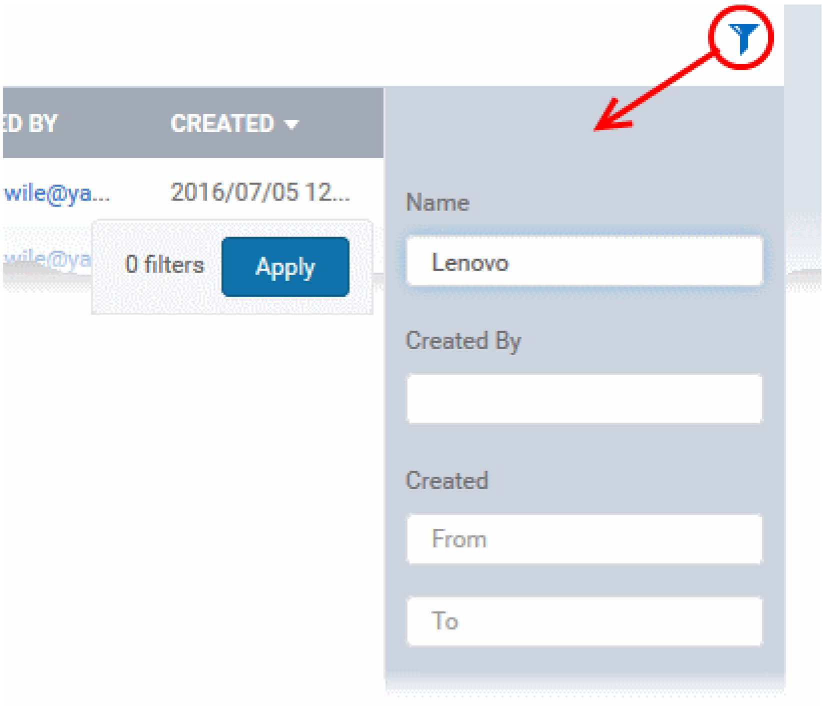
- Click 'Users' > 'User Groups'.
- Click the 'Export' button above the table then choose 'Export to CSV':



- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Sorting, Search and Filter Options

- Click any column header to sort groups in alphabetic or ascending/descending order of the entries in the column.
- Click the funnel button at the right end to open the filter options.



The 'User Groups' interface allows you to:

- **Create a New User Group**
- **Edit a User Group**
- **Assign Configuration Profile(s) to a User Groups**
- **Remove a User Group**

## 4.2.1. Create a New User Group

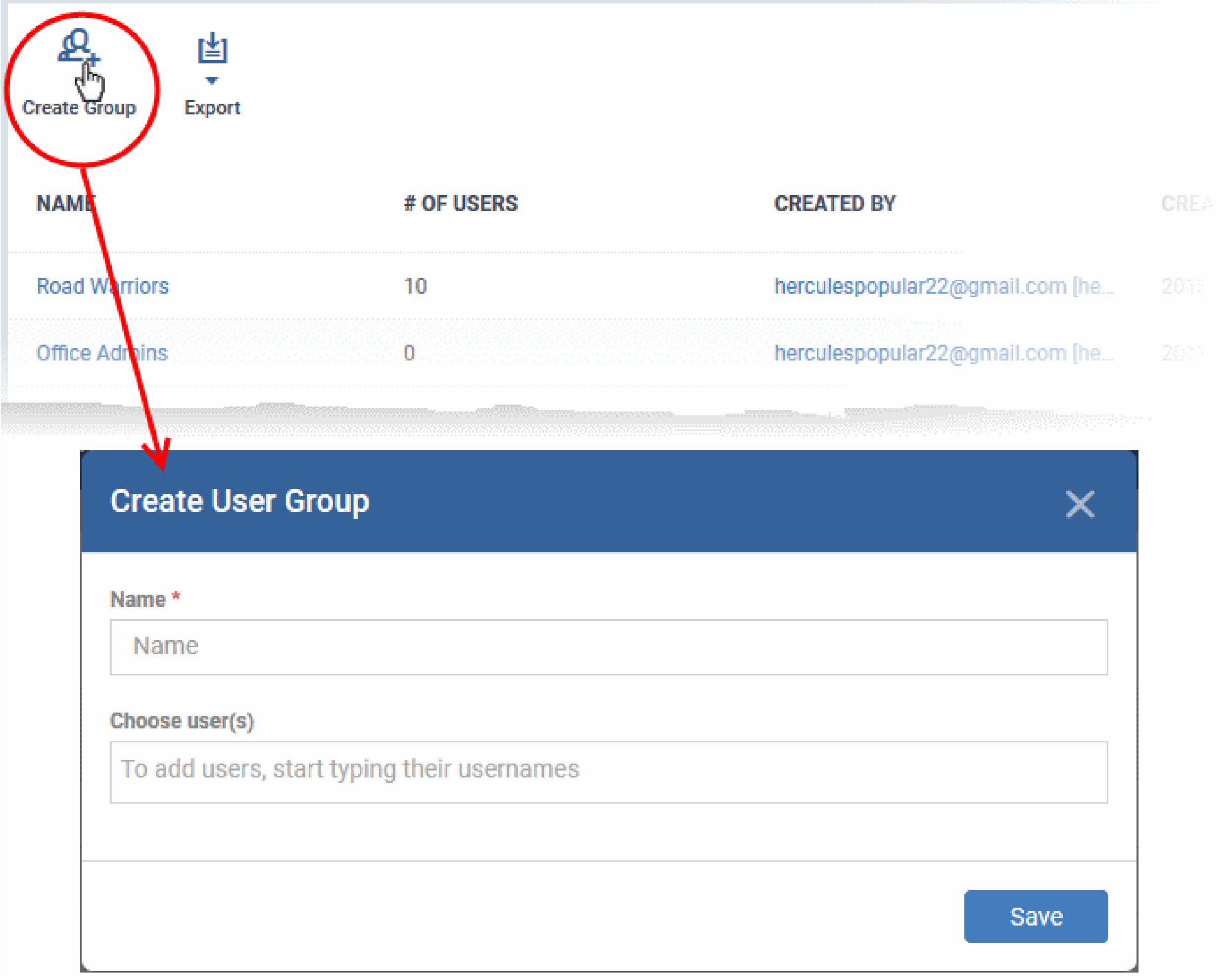
- Click 'Users' > 'User Groups'

The 'User Groups' interface lets you add and populate new user groups. 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**

- Click 'Users' > 'User Groups'
- Click 'Create Group' above the table.

The 'Create User Group' dialog will open:



| NAME | # OF USERS | CREATED BY | CREA |
|---|---|---|---|
| Road Warriors | 10 | herculespopular22@gmail.com [he... | 201 |
| Office Admins | 0 | herculespopular22@gmail.com [he... | 201 |

Create User Group

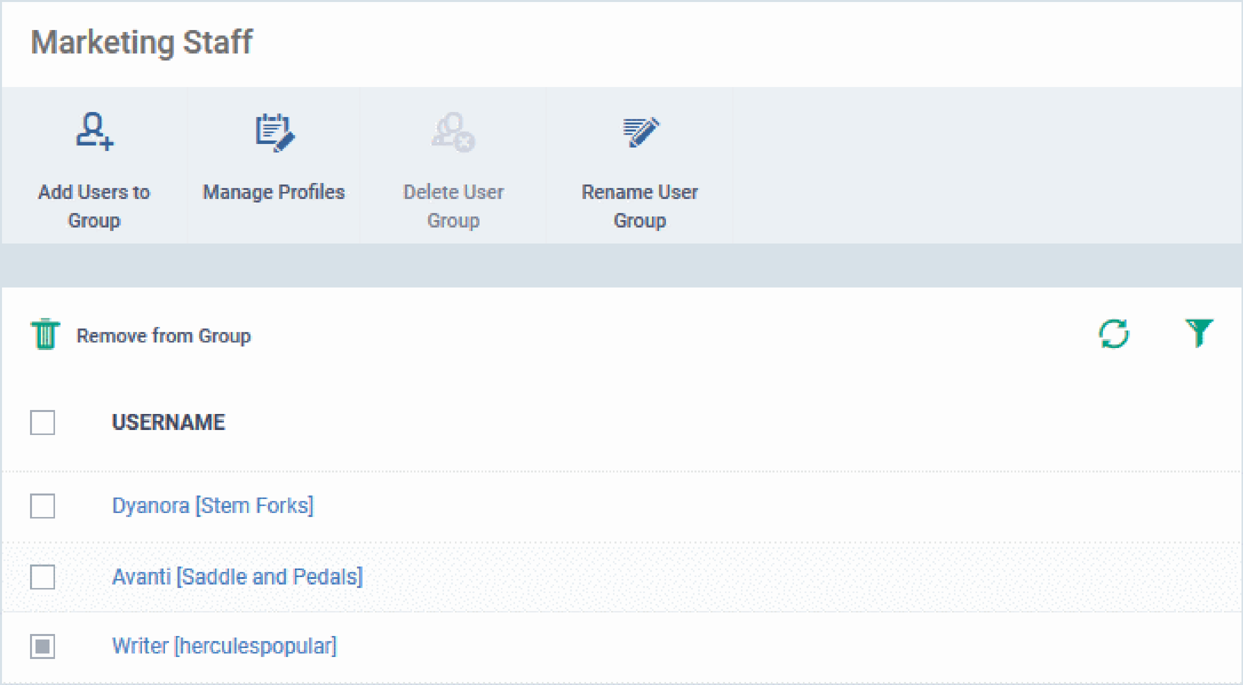
Name *

Name

Choose user(s)

To add users, start typing their usernames

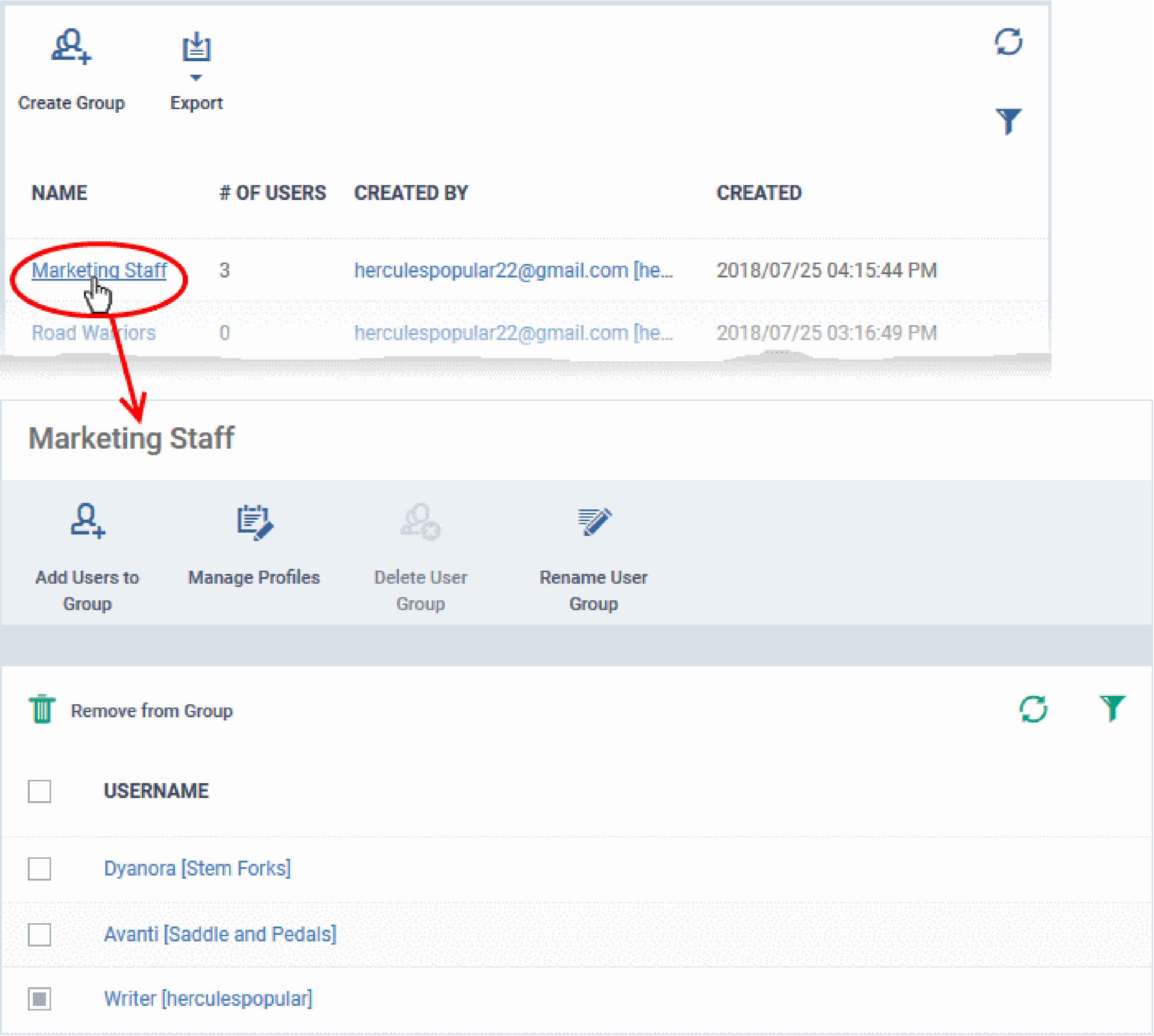
- **Name** - Type a label for the user group.
- **Choose User(s)** - Add users to the group.
  - Start typing the first few letters of a username and select from the suggestions.
  - Repeat the process to add more users.
  - Note: You can skip this step and add users later if required. See **Edit a User Group** for more details.
- The group will be saved and the group details screen will open.
- Profiles can now be applied to the group. See **Assign Configuration Policy to a User Group** for more details.
- Users can be added or removed from the group at anytime. See **Edit a User Group** for more details.



**Note**: A single user can be a member of more than one group. Profiles from every group of which the user is a member will be applied to the user's device. If the settings in one profile clash with another profile, EM will implement the most restrictive setting. For example, if one profile allows the use of the camera but another profile blocks it, then the device will not be able to use the camera.

### 4.2.2. Edit a User Group

- The group details screen lets you manage group members, rename the group, or delete the group.
- Click 'Users' > 'User Groups'.
- Click the name of the group you want to edit:



| NAME | # OF USERS | CREATED BY | CREATED |
|---|---|---|---|
| Marketing Staff | 3 | herculespopular22@gmail.com [he... | 2018/07/25 04:15:44 PM |
| Road Warriors | 0 | herculespopular22@gmail.com [he... | 2018/07/25 03:16:49 PM |

Marketing Staff

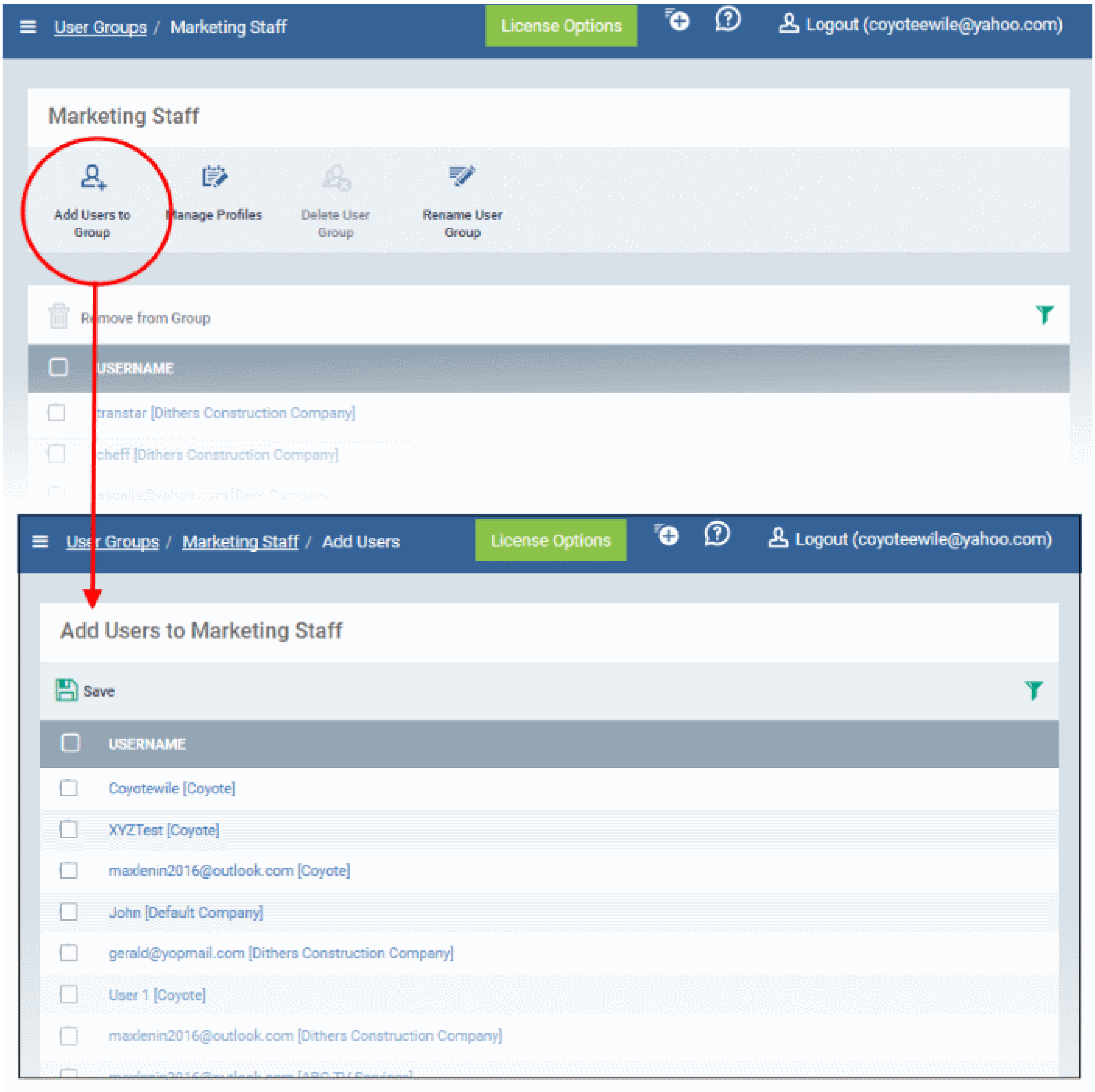
| □ | USERNAME |
|---|---|
| □ | Dyanora [Stem Forks] |
| □ | Avanti [Saddle and Pedals] |
| ▣ | Writer [herculespopular] |

The group details screen allows you to:

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

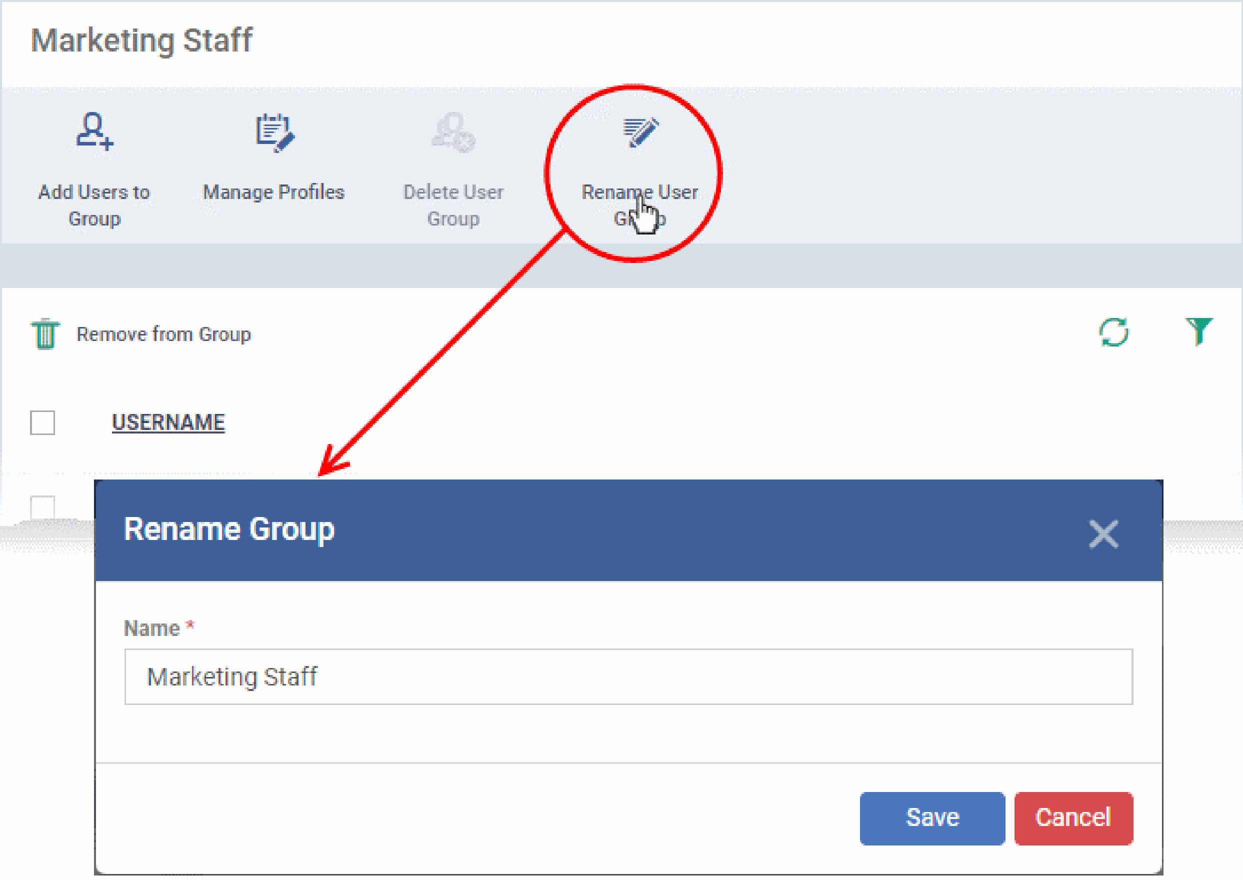
**To add new user(s) to the group**

- Click 'Add Users To Group'.
- Select the users you want to add and click 'Save'.
- All group profiles will be applied to the new user's devices. These profiles will be removed from the device if you remove the user from the group.


User Groups / Marketing Staff
License Options
Logout (coyoteewile@yahoo.com)
Marketing Staff
Add Users to Group
Manage Profiles
Delete User Group
Rename User Group
Remove from Group
USERNAME
transtar [Dithers Construction Company]
cheff [Dithers Construction Company]
User Groups / Marketing Staff / Add Users
License Options
Logout (coyoteewile@yahoo.com)
Add Users to Marketing Staff
Save
USERNAME
Coyotewile [Coyote]
XYZTest [Coyote]
maxlenin2016@outlook.com [Coyote]
John [Default Company]
gerald@yopmail.com [Dithers Construction Company]
User 1 [Coyote]
maxlenin2016@outlook.com [Dithers Construction Company]

**To rename a group**

- Click 'Users' > 'User Groups'.
- Click the name of the group you want to re-name.
- Click the 'Rename User Group' button
- Enter the new label in the 'Name' text box and click 'Save':



Name *

Marketing Staff

## 4.2.3. Assign Configuration Profiles to a User Group

- Click 'Users' > 'User Groups'

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

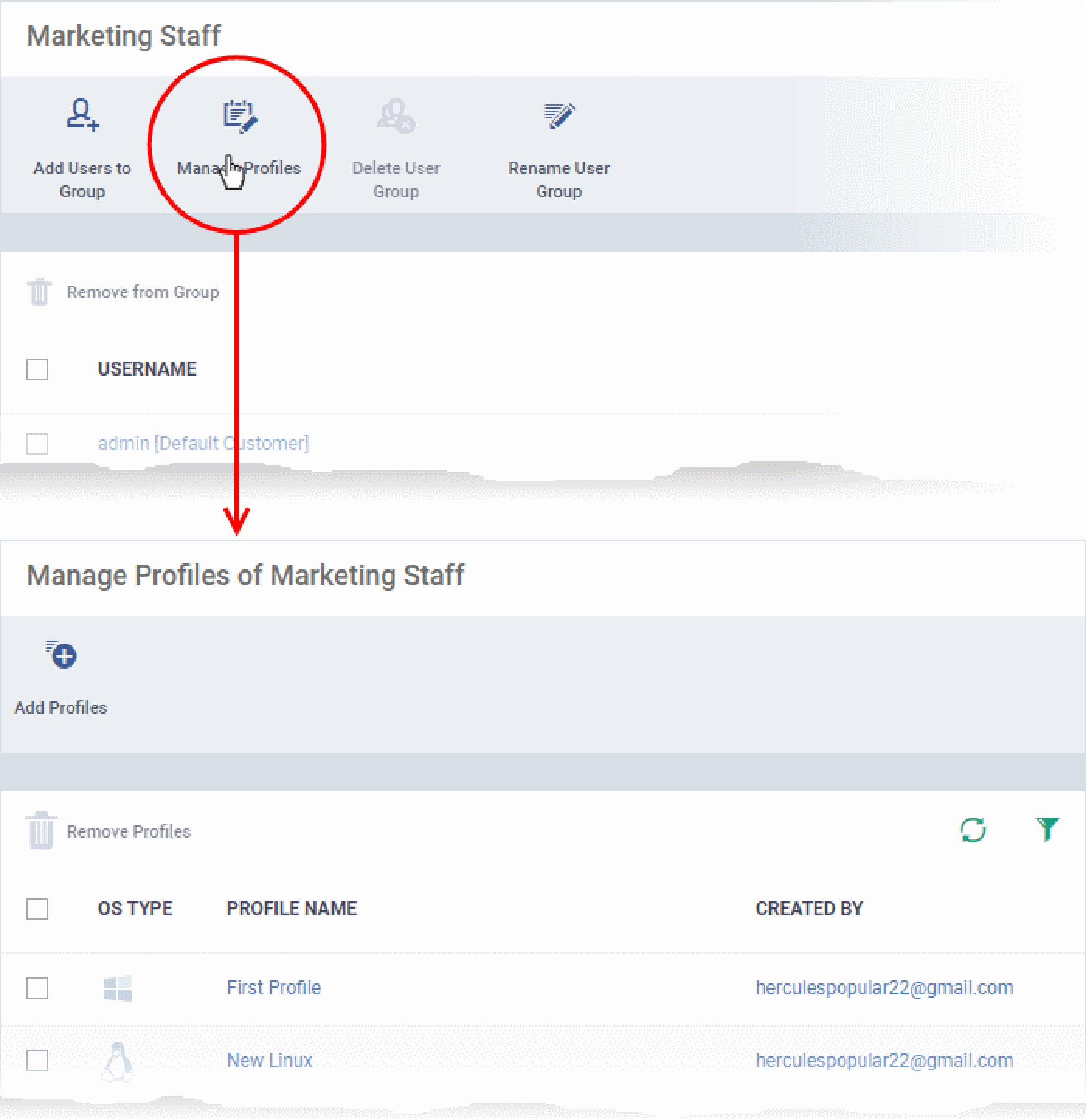
For more details on profiles, See **Create Configuration Profiles**.

**To view and manage the profiles applied to a group**

- Click 'Users' > 'User Groups'.
- Click on the name of the group whose profiles you wish to manage.

The group details interface opens with a list of all users in the group.

- Click 'Manage Profiles' at the top.



Marketing Staff

| □ | USERNAME |
|---|---|
| □ | admin [Default Customer] |

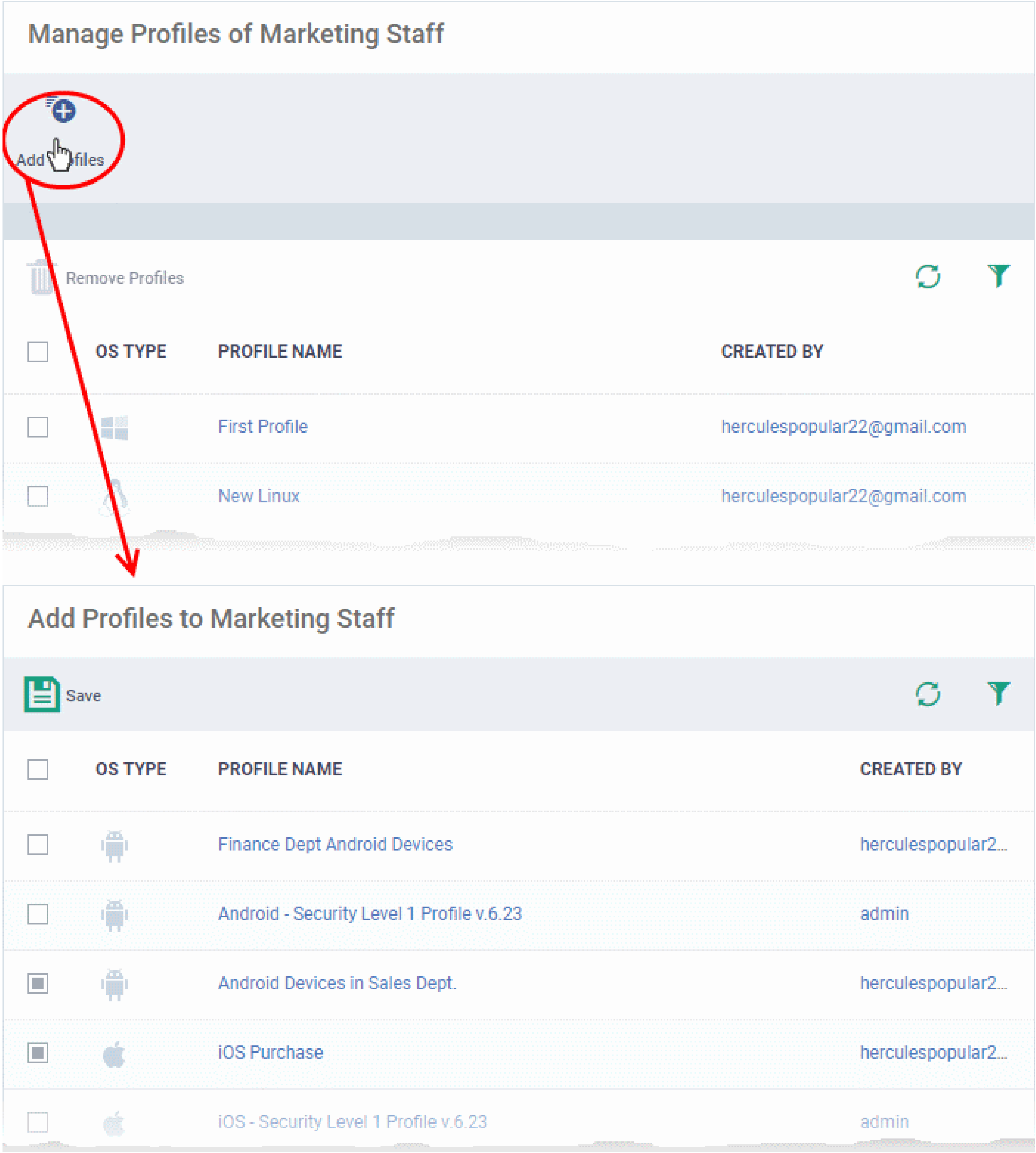
Manage Profiles of Marketing Staff

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | First Profile | herculespopular22@gmail.com |
| □ | | New Linux | herculespopular22@gmail.com |

The 'Manage Profiles For User Group' interface opens showing the profiles associated with the group.

**To add a new profile**

- Click 'Add Profiles'



Manage Profiles of Marketing Staff

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | First Profile | herculespopular22@gmail.com |
| □ | | New Linux | herculespopular22@gmail.com |

Add Profiles to Marketing Staff

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Finance Dept Android Devices | herculespopular2... |
| □ | | Android - Security Level 1 Profile v.6.23 | admin |
| ☑ | | Android Devices in Sales Dept. | herculespopular2... |
| ☑ | | iOS Purchase | herculespopular2... |
| □ | | iOS - Security Level 1 Profile v.6.23 | admin |

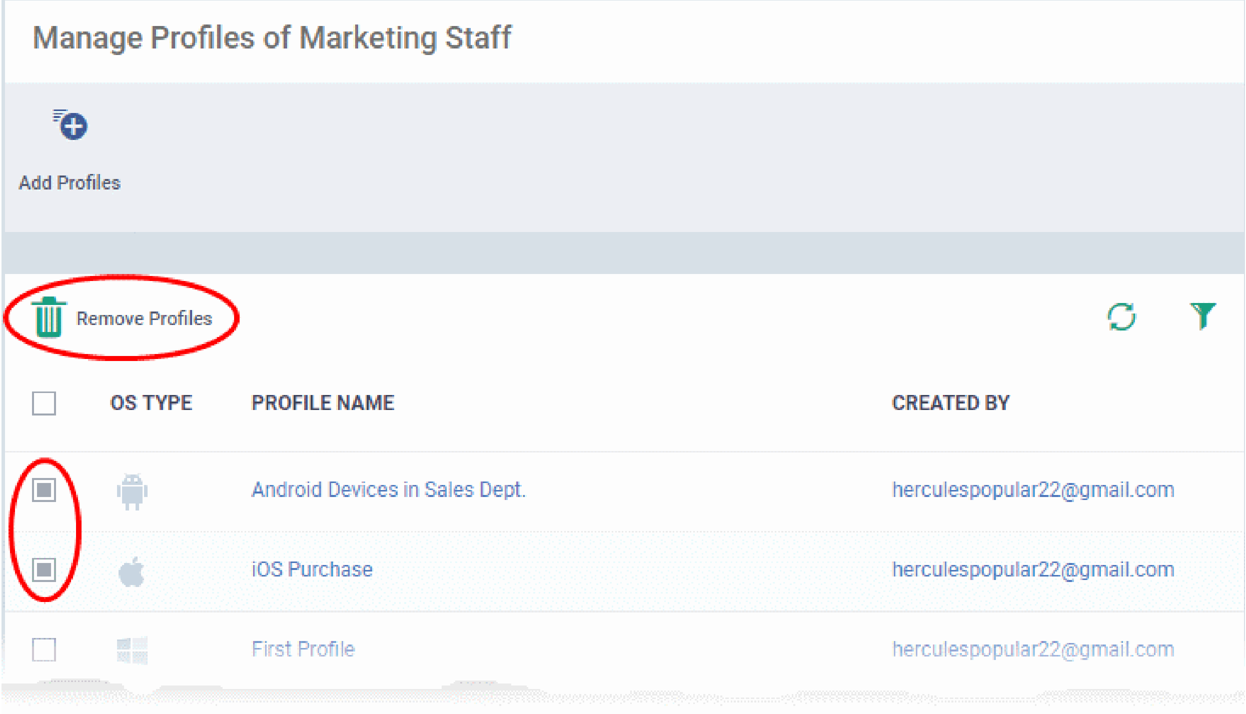
A list of all configuration profiles, available in EM, excluding those already applied to the group will be displayed.

- 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**

- Click 'Users' > 'User Groups'.
- Click on the name of the group whose profiles you wish to manage.
- Click 'Manage Profiles' at the top of the 'Group Details' interface.
- Select the profile from the 'Manage Profiles' interface and click 'Remove Profiles'



Manage Profiles of Marketing Staff

| ☐ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| ☒ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |
| ☒ | | iOS Purchase | herculespopular22@gmail.com |
| ☐ | | First Profile | herculespopular22@gmail.com |

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

**Note** - Disassociating a profile from a user group will remove the profile from devices belonging to the users in that group only if it is applied because the user 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 device, user of the device or a group to which the device belongs), then the profile will not be removed.

## 4.2.4. Remove a User Group

- Click 'Users' > 'User Groups'

The 'User Groups' interface lets you remove unwanted user group(s) in Endpoint Manager.

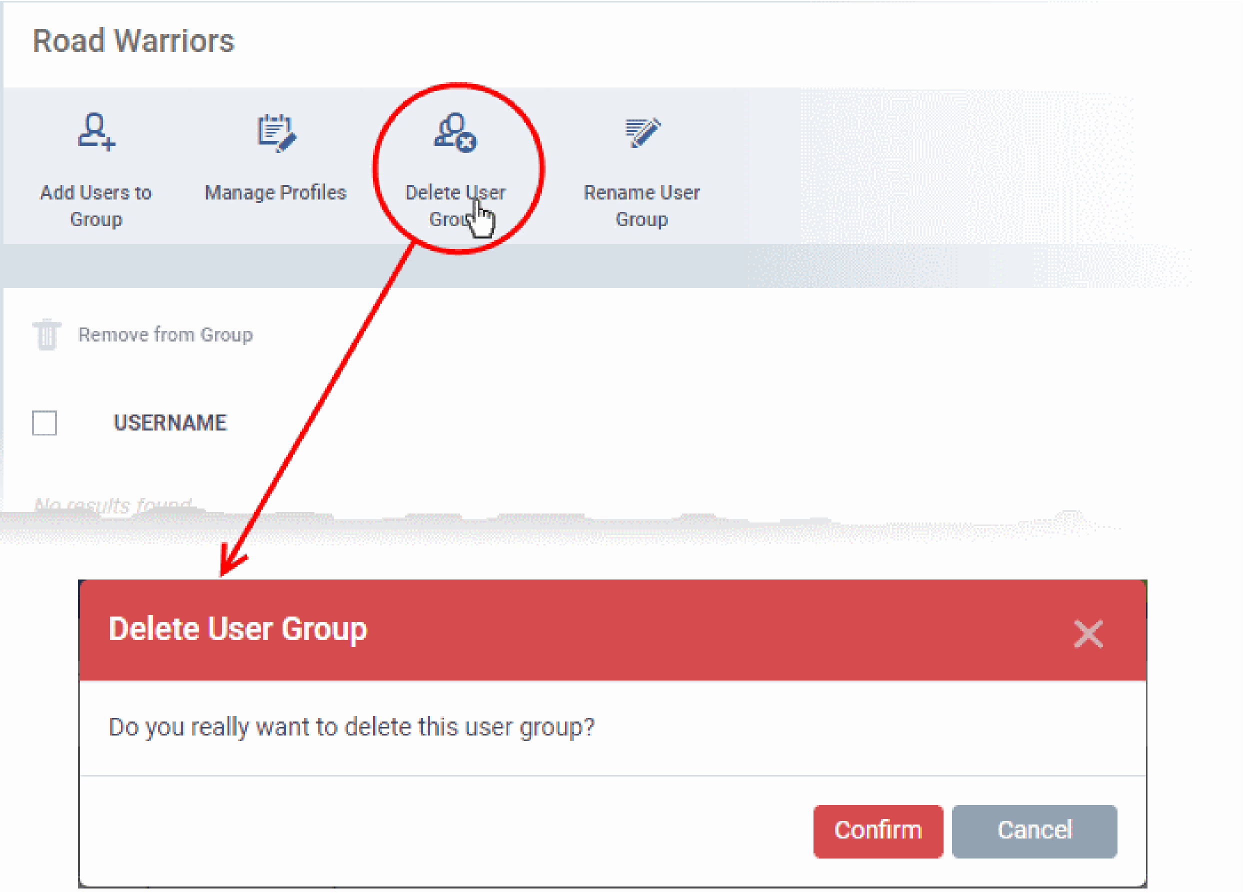
**Note**: Only Groups that do not contain any members in it can be removed. Ensure that all users are removed from the group before removing it. See the **explanation of removing users from a group** in **Edit a User Group** for more details.

**To remove a user group**

- Click 'Users' > 'User Groups'
- Click the name of the group to be removed.

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

- Click 'Delete User Group' at the top.



Delete User Group

Do you really want to delete this user group?

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

# 4.3. Configure Role Based Access Control for Users

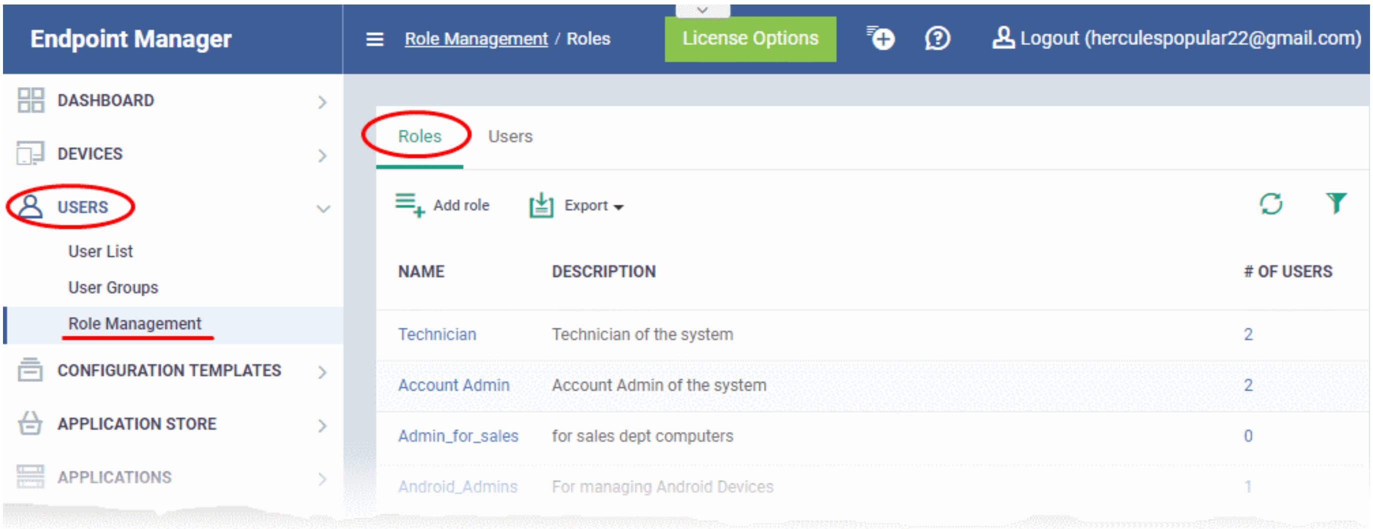
- Click 'Users' > 'Role Management'
- User privileges depend on the roles assigned to them. Admins can create roles with different access privileges and assign them to users as required. A single user can be assigned to any number of roles.
- Staff created in Comodo Dragon or Comodo One can be added to any role for any company. This allows you to assign different roles to the same staff member for different companies.
- You can restrict a role to specific companies/groups. Staff can only manage the devices of companies/groups allowed by their role.
- You can also create roles with read-only privileges. These allow staff to view assigned interfaces but not make changes.

The role management area has two tabs:

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

### Roles

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



| NAME | DESCRIPTION | # OF USERS |
|---|---|---|
| Technician | Technician of the system | 2 |
| Account Admin | Account Admin of the system | 2 |
| Admin_for_sales | for sales dept computers | 0 |
| Android_Admins | For managing Android Devices | 1 |

- Custom roles and built-in roles are available for selection when adding a new user.
- Admins can add or remove roles at any time. You can also change the role of any user at any time.
- New users are assigned the 'User' role by default. However, you have the option to make any role the default.

<table>
<tr><th colspan="2">Roles - Column Descriptions</th></tr>
<tr><th>Column Heading</th><th>Description</th></tr>
<tr><td>Name</td><td>Role label.<br>• Click a role name to open the 'Role Management' > 'Role Permissions' screen.<br>• You can view and manage permissions assigned to the role.<br>• See '<b>Manage Permissions and Assign Users of a Role</b>' for more details.</td></tr>
<tr><td>Description</td><td>A short description of the role.</td></tr>
<tr><td>Number of Users</td><td>Shows how many users are assigned to the role.<br>• Click the number to open the 'Assign Users' screen, which lets you manage users assigned to the role. See '<b>View users assigned to a role</b>' for more details.</td></tr>
<tr><th colspan="2">Controls</th></tr>
<tr><td>Add Role</td><td>Create new roles and assign them to users. See <b>Create a New Role</b> for more details.</td></tr>
<tr><td>Export</td><td>Save the list of user roles as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See <b>Export the List of Roles</b> for more details.</td></tr>
</table>

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

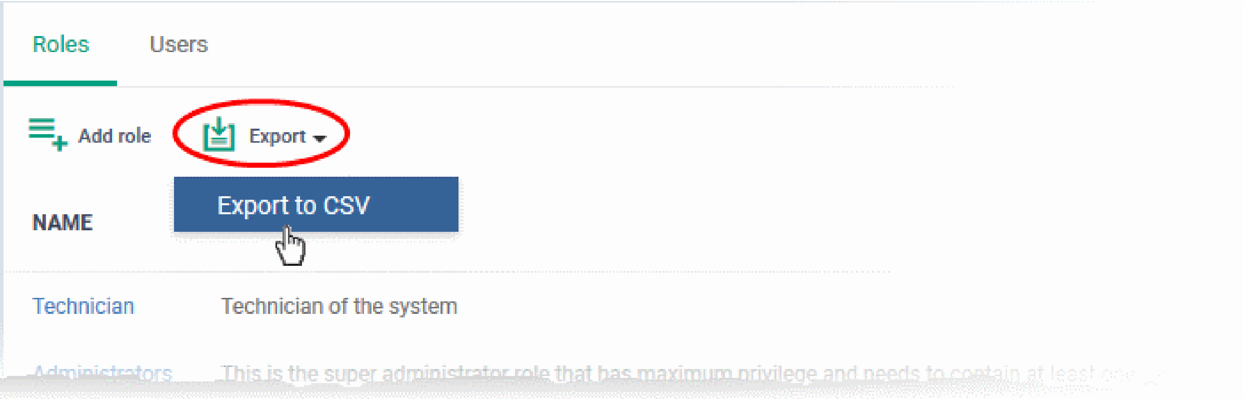
The roles interface allows you to:

- **Create a new role**
- **Manage Roles**
  - **Edit a role name and description of a role**
  - **Manage the permissions assigned to a role**

  - **Manage the users assigned with a role**
- **Remove a Role**

## Export the List of Roles

- Click 'Users' > 'Role Management'.
- Select the 'Roles' tab
- Click the 'Export' button above the table then choose 'Export to CSV':

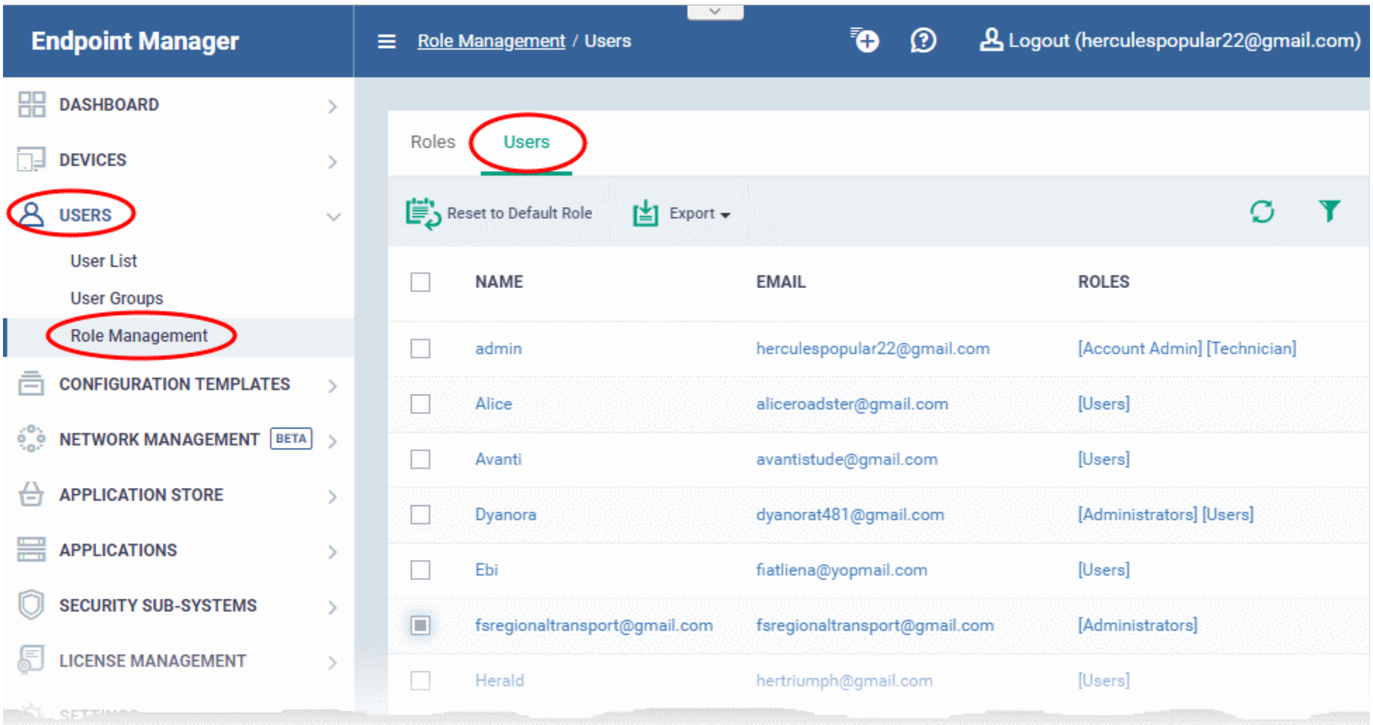


| NAME | |
|---|---|
| Technician | Technician of the system |
| Administrators | This is the super administrator role that has maximum privilege and needs to contain at least one |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Users

- The 'Users' interface lets you view users added to EM and the roles assigned to them.
- You can also edit the roles assigned to each user from this interface.
- Click the 'Users' tab to switch to the 'Users' interface:



| | NAME | EMAIL | ROLES |
|---|---|---|---|
| □ | admin | herculespopular22@gmail.com | [Account Admin] [Technician] |
| □ | Alice | aliceroadster@gmail.com | [Users] |
| □ | Avanti | avantistude@gmail.com | [Users] |
| □ | Dyanora | dyanorat481@gmail.com | [Administrators] [Users] |
| □ | Ebi | fiatliena@yopmail.com | [Users] |
| □ | fsregionaltransport@gmail.com | fsregionaltransport@gmail.com | [Administrators] |
| □ | Herald | hertriumph@gmail.com | [Users] |

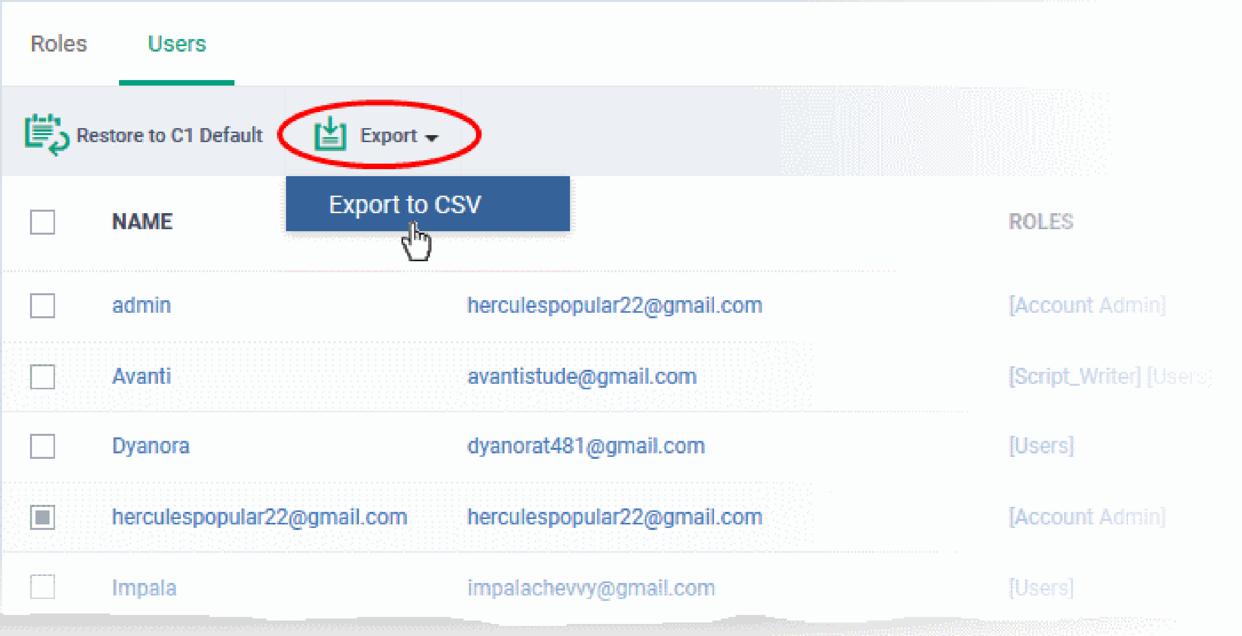
**Users - Column Descriptions**

| Column Heading | Description |
|---|---|
| Name | The login username of the user.<br>• Click a username to view and manage roles assigned to the user. See **Manage Roles assigned to a User** for more details. |
| Email | The registered email address of the user. |
| Roles | The user roles assigned to the user.<br>Click a role name to view and manage permissions assigned to the role. See '**Manage Permissions and Assigned Users of a Role**' for more details. |
| **Controls** | |
| Reset to Default Role | Revert the user's role to the Comodo Dragon or Comodo One system default role.<br>Applies only to users imported from Comodo Dragon or Comodo One. It doesn't apply to users added via EM.<br>See **Restore user role** in **Manage Roles Assigned to a User** for more. |
| Export | Save the list of users as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'.<br>See **Export the List of Users** for more details. |

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

## Export the List of Users

- Click 'Users' > 'Role Management'.
- Select the 'Users' tab
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | NAME | | ROLES |
|---|---|---|---|
| □ | admin | herculespopular22@gmail.com | [Account Admin] |
| □ | Avanti | avantistude@gmail.com | [Script_Writer] [Users] |
| □ | Dyanora | dyanorat481@gmail.com | [Users] |
| ☑ | herculespopular22@gmail.com | herculespopular22@gmail.com | [Account Admin] |
| □ | Impala | impalachevvy@gmail.com | [Users] |

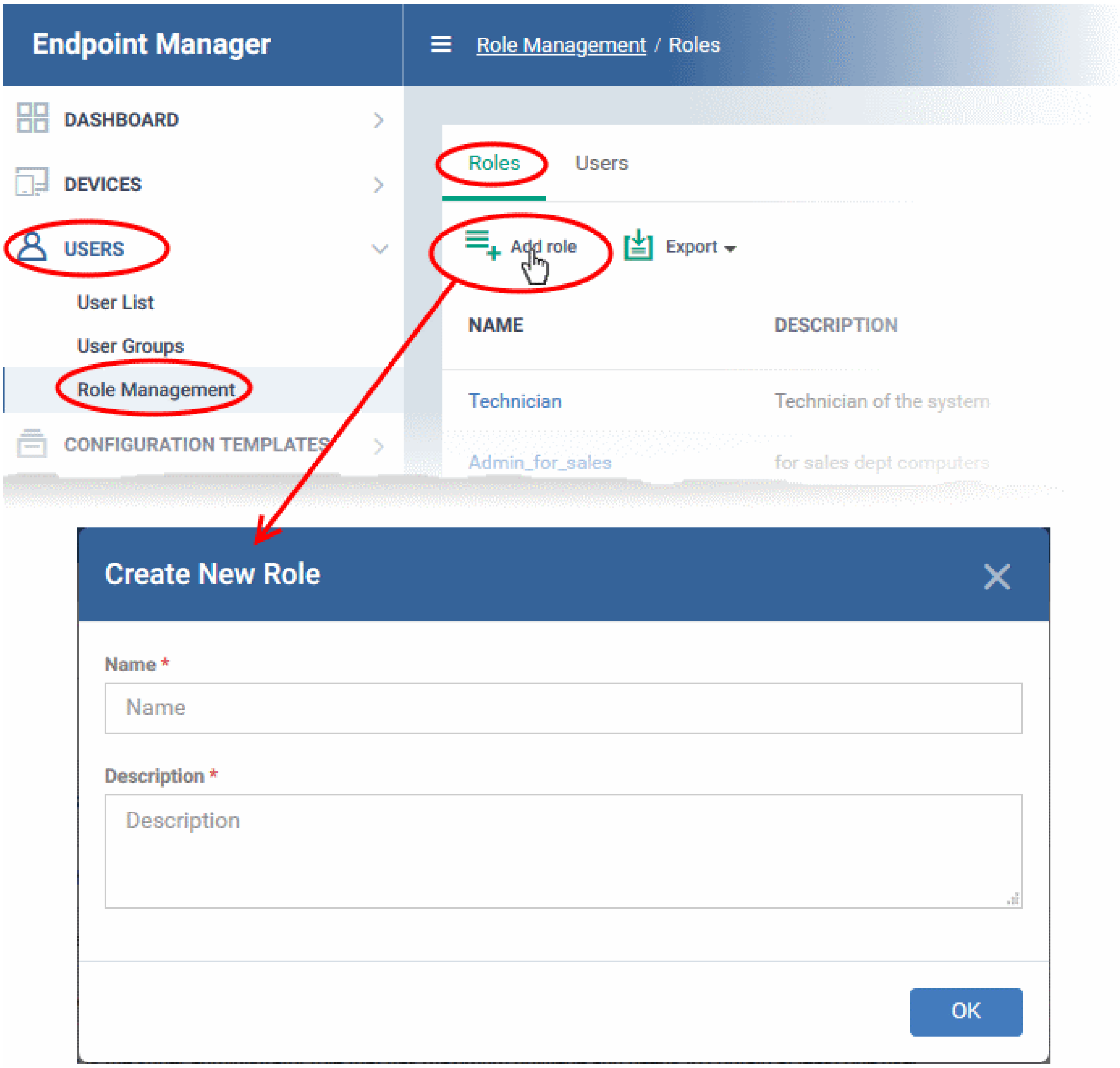
- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

The 'Users' interface allows administrators to:

- Manage Roles Assigned to a User

## 4.3.1. Create a New Role

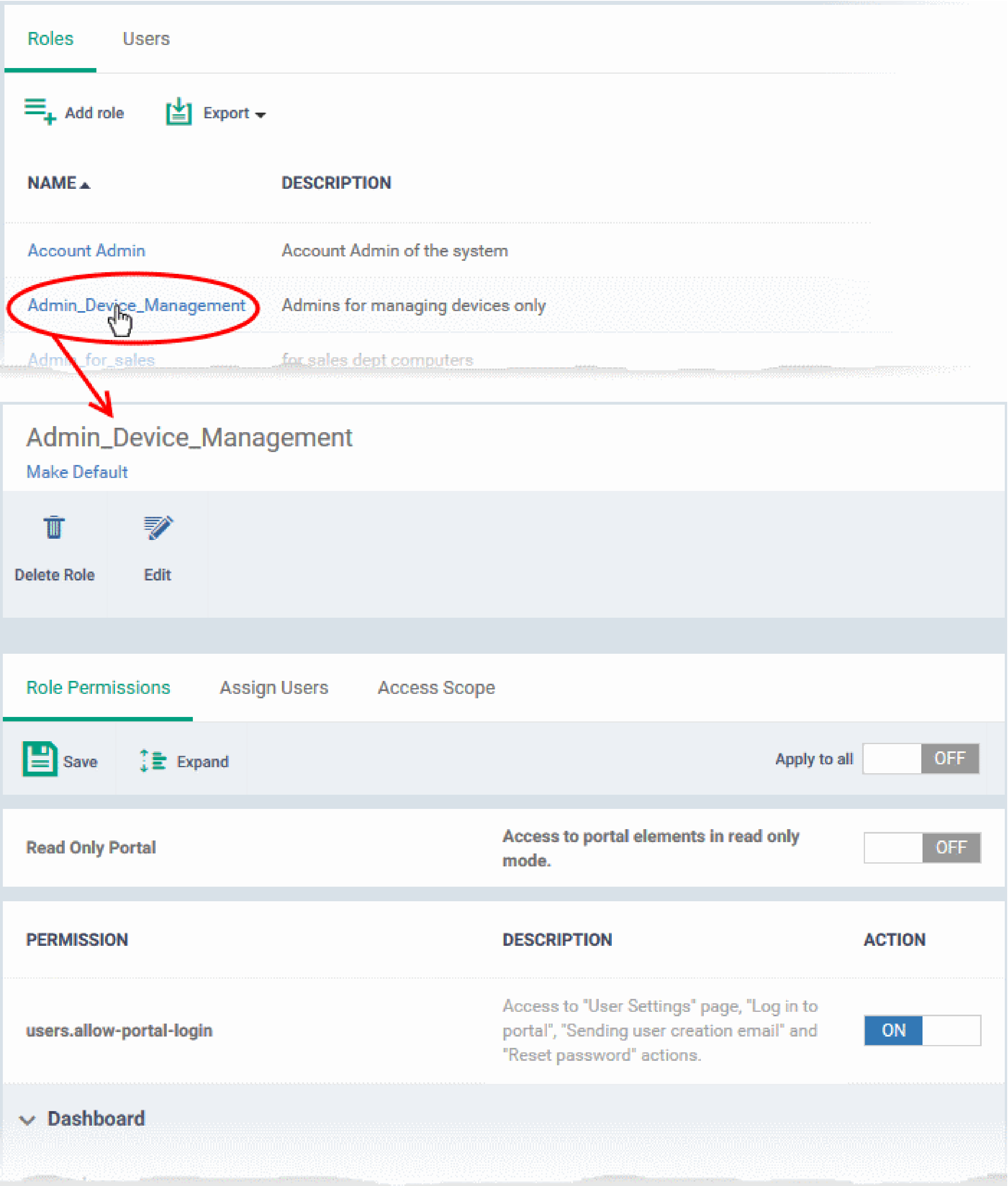
- Click 'Users' > 'Role Management'
- Click the 'Roles' tab
- Click 'Add Role':



Create a name and description for the role then click 'OK'.

The new role is added to the list in the 'Roles' screen.

- Click on the new role to edit its permissions, assign users, and specify which entities the role is allowed to manage.



| NAME ▲ | DESCRIPTION |
|---|---|
| Account Admin | Account Admin of the system |
| Admin_Device_Management | Admins for managing devices only |
| Admin_for_sales | for sales dept computers |

Admin_Device_Management

Apply to all: OFF

| | | |
|---|---|---|
| Read Only Portal | Access to portal elements in read only mode. | OFF |

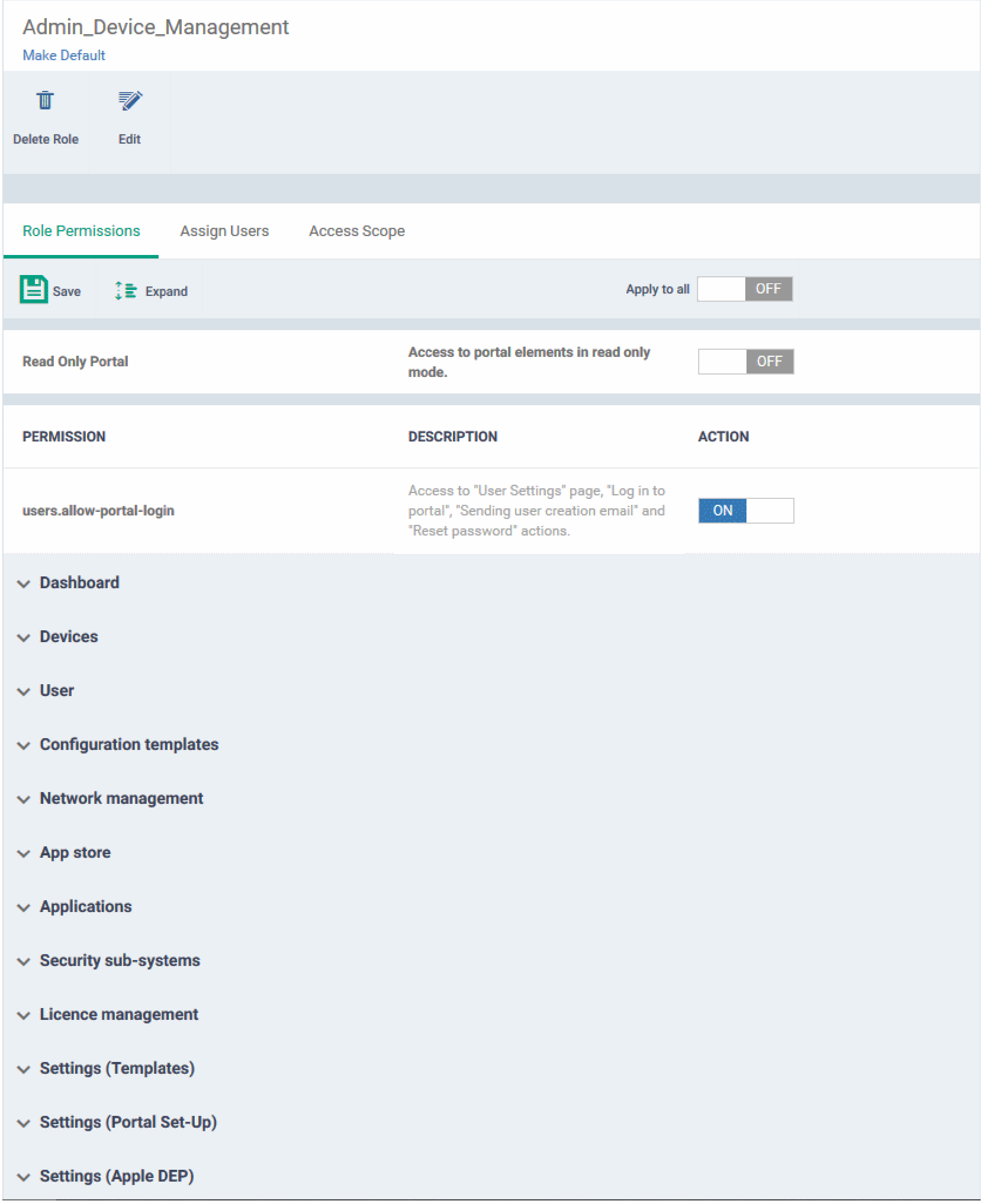
| PERMISSION | DESCRIPTION | ACTION |
|---|---|---|
| users.allow-portal-login | Access to "User Settings" page, "Log in to portal", "Sending user creation email" and "Reset password" actions. | ON |

The edit screen has three tabs:

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

**Select access rights and privileges for the role**

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



Admin_Device_Management

| PERMISSION | DESCRIPTION | ACTION |
|---|---|---|
| Read Only Portal | Access to portal elements in read only mode. | OFF |
| users.allow-portal-login | Access to "User Settings" page, "Log in to portal", "Sending user creation email" and "Reset password" actions. | ON |

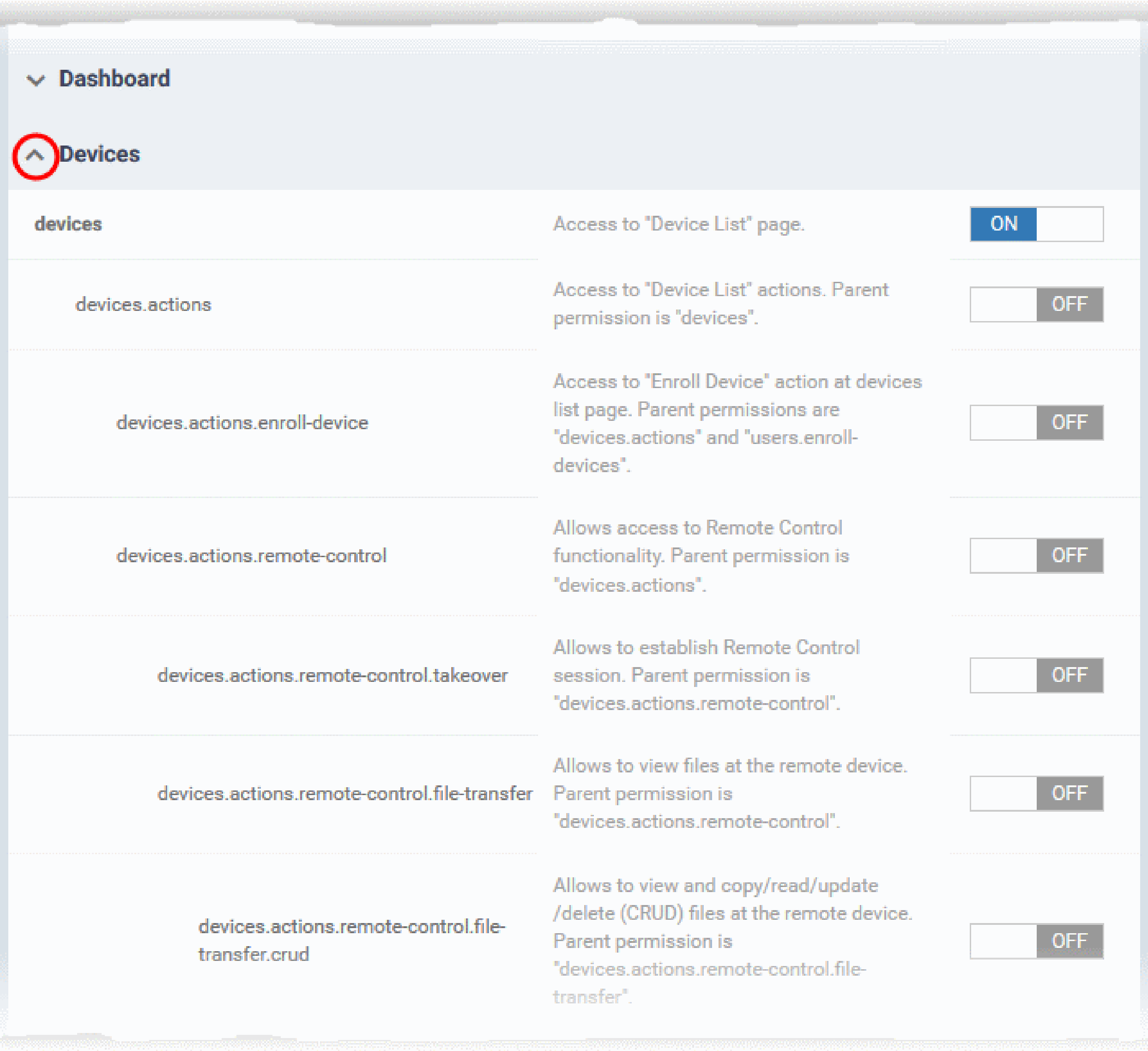
- **Read Only Portal -** Role-members can view areas to which you assign them permission, but cannot make changes.
    - The read-only switch applies to every permission you enable in the list below.
- **Users.allow-portal-login -** Role-members can login to Endpoint Manager (EM). EM sends an account activation mail to users assigned to the role. The user can login to EM and manage as per the permissions you assign below.

Each item in the list lets you choose permissions for a specific area.

- Click the down arrow next to a module name to view its permissions

OR

- Click 'Expand' at the top to view all permissions



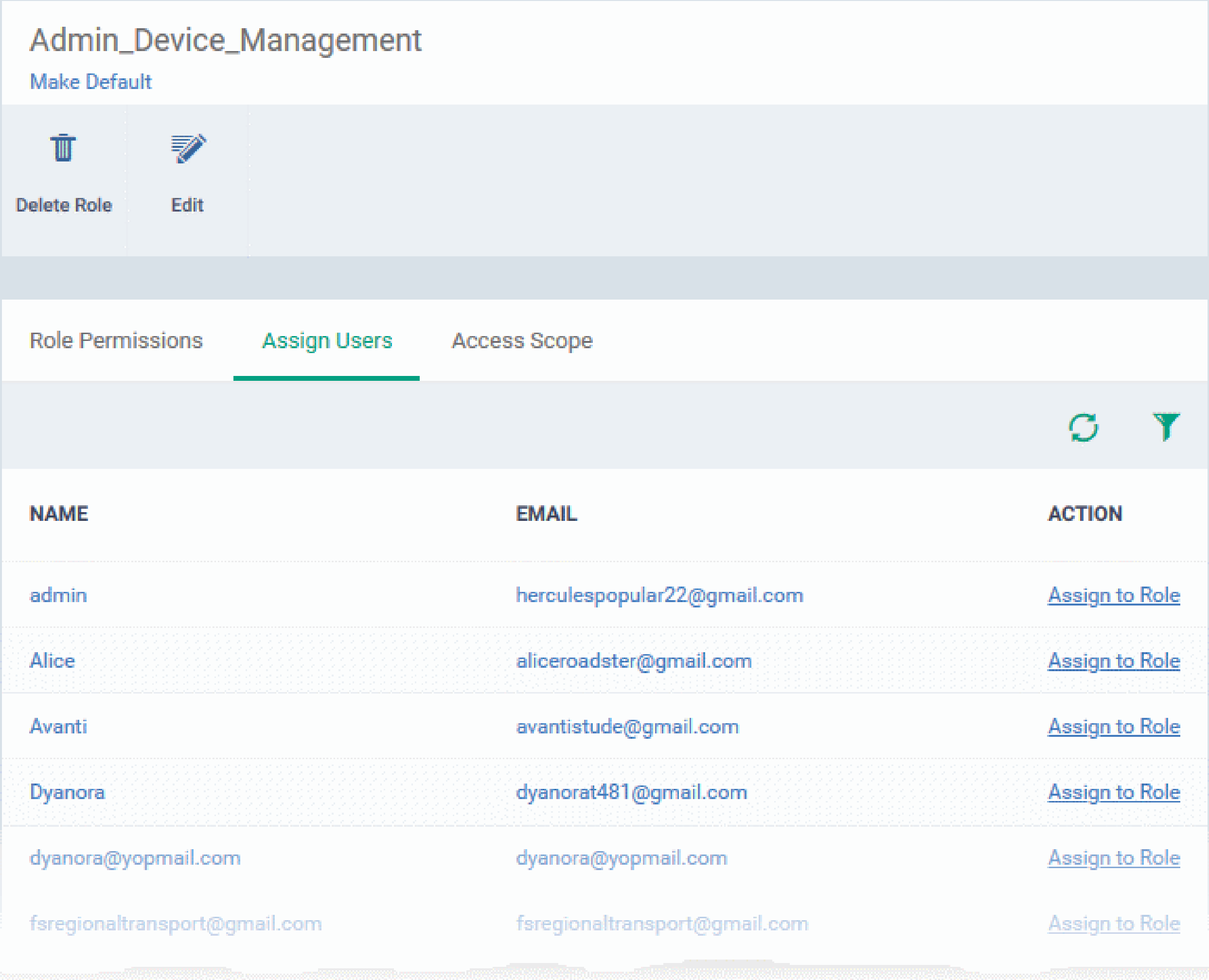
| | | |
|---|---|---|
| devices | Access to "Device List" page. | ON |
| devices.actions | Access to "Device List" actions. Parent permission is "devices". | OFF |
| devices.actions.enroll-device | Access to "Enroll Device" action at devices list page. Parent permissions are "devices.actions" and "users.enroll-devices". | OFF |
| devices.actions.remote-control | Allows access to Remote Control functionality. Parent permission is "devices.actions". | OFF |
| devices.actions.remote-control.takeover | Allows to establish Remote Control session. Parent permission is "devices.actions.remote-control". | OFF |
| devices.actions.remote-control.file-transfer | Allows to view files at the remote device. Parent permission is "devices.actions.remote-control". | OFF |
| devices.actions.remote-control.file-transfer.crud | Allows to view and copy/read/update /delete (CRUD) files at the remote device. Parent permission is "devices.actions.remote-control.file-transfer". | OFF |

- Use the switches on the right to enable or disable specific permissions
- Use the 'Apply to all' switch to enable or disable all permissions
- Click 'Save' for your settings to take effect

**Assign the new role to selected users**

- Click the 'Assign Users' tab.

This opens a list of all enrolled users:



| NAME | EMAIL | ACTION |
|---|---|---|
| admin | herculespopular22@gmail.com | Assign to Role |
| Alice | aliceroadster@gmail.com | Assign to Role |
| Avanti | avantistude@gmail.com | Assign to Role |
| Dyanora | dyanorat481@gmail.com | Assign to Role |
| dyanora@yopmail.com | dyanora@yopmail.com | Assign to Role |
| fsregionaltransport@gmail.com | fsregionaltransport@gmail.com | Assign to Role |

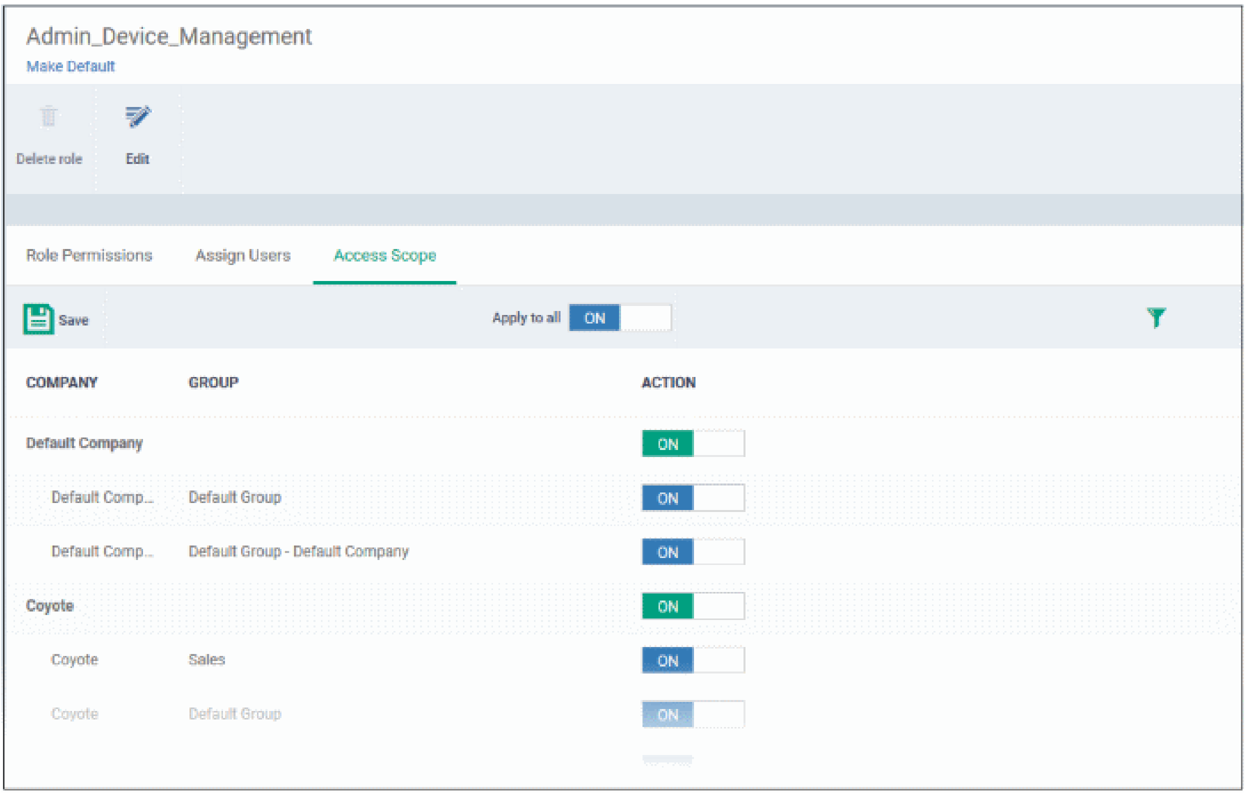
- **Assign to Role** - Click to place the user in a particular role.

**Tip**: You can search for specific users by clicking the funnel icon at top-right.

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

- Click the 'Access Scope' tab.

This opens a list of all companies added to Endpoint Manager. **Device groups** in each company are listed below the company name.



Admin_Device_Management

Make Default

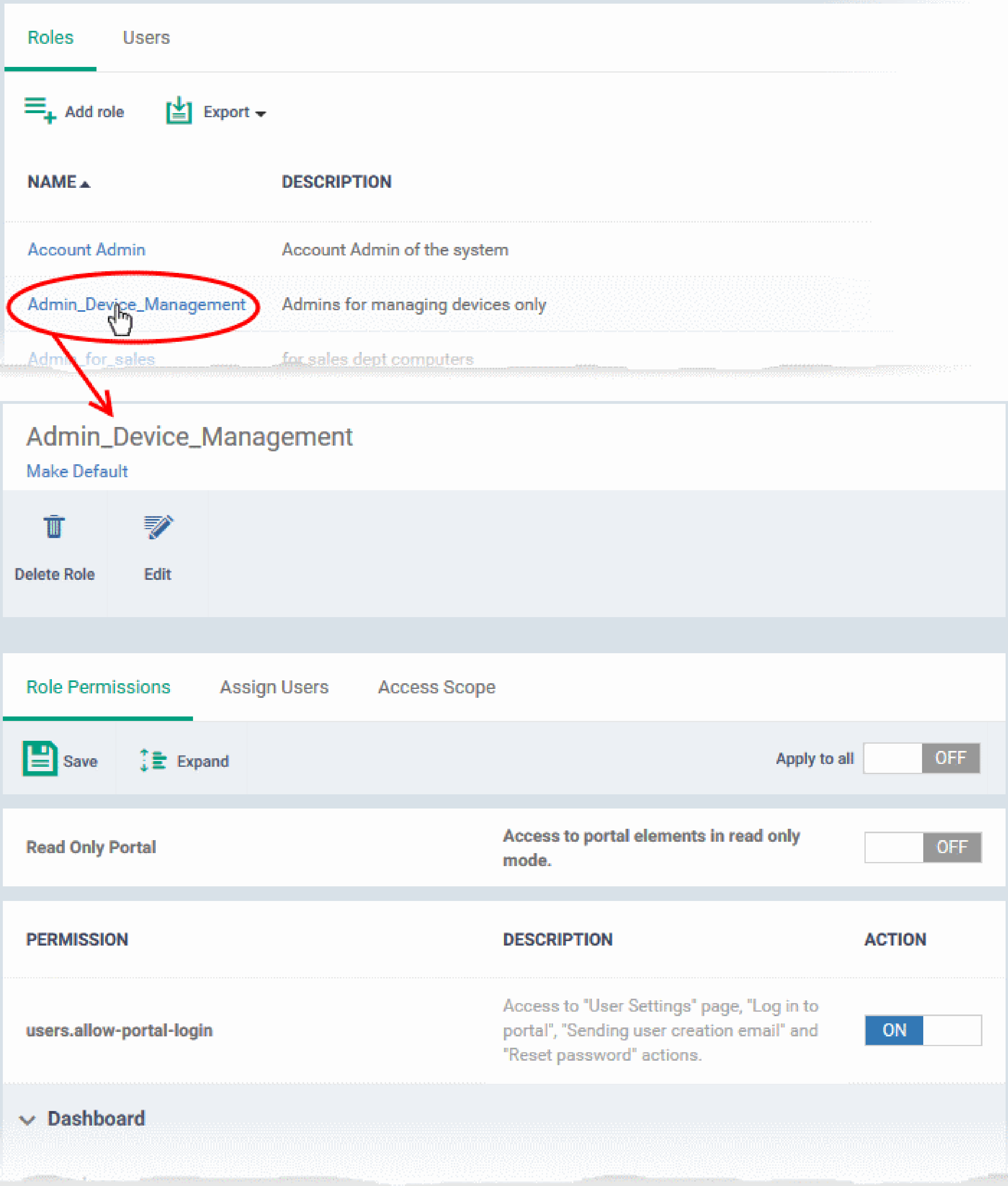
| COMPANY | GROUP | ACTION |
|---|---|---|
| Default Company | | ON |
| Default Comp... | Default Group | ON |
| Default Comp... | Default Group - Default Company | ON |
| Coyote | | ON |
| Coyote | Sales | ON |
| Coyote | Default Group | ON |

Configure the access scope of the role as follows:

- Use the green 'master' switch next to a company name to enable/disable the ability to manage groups under the company.
- Use the switch next to a device group to control access to a specific group.
- Apply to All - Enable or disable access to all companies and groups on the page.
- Click 'Save' for your settings to take effect
- Click the edit button Edit to modify the role's name and description. Please note that you cannot modify the built-in roles, Account Admin, Administrators and Technician.
- Click 'Make Default' if you want this to be the role that is initially assigned to new users.

## 4.3.2. Manage Permissions and Users Assigned to a Role

- Click 'Users' > 'Role Management' on the left.
- Click the 'Roles' tab.
- Click a role name to view its details

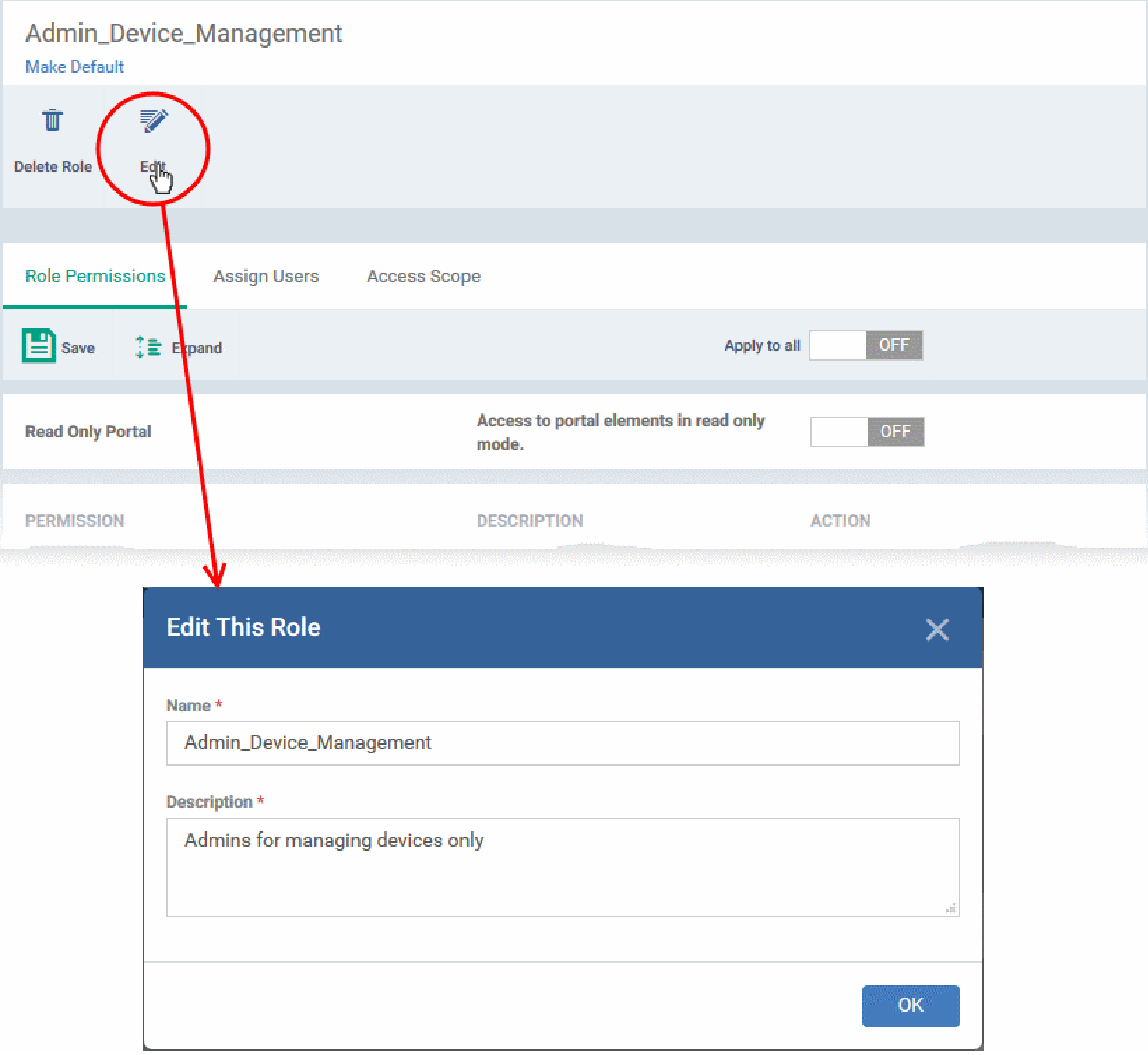


The role management area lets you:

- Edit the name and description of a role
- Add or remove permissions assigned to a role
- View users assigned to a role
- Assign / remove a role to / from users
- Select companies and device groups accessible to a role
- Set a role as the default role

**Edit the name and description of the role**

- Click the 'Edit' button Edit at the top



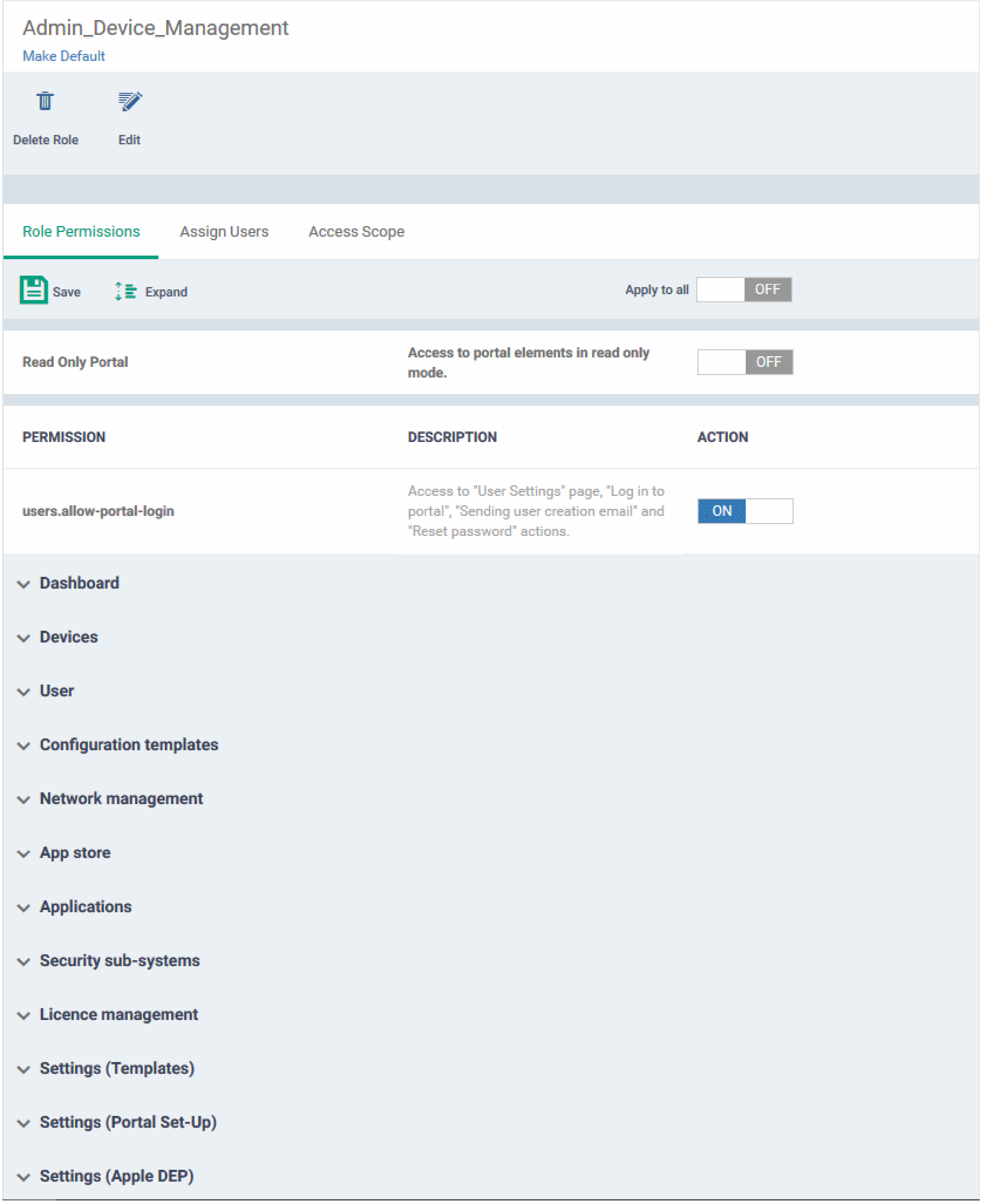
Name *: Admin_Device_Management

Description *: Admins for managing devices only

- Modify the name and / or description as required
- Click 'Ok' for your changes to take effect.

**Add or remove permissions assigned to a role**

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



Admin_Device_Management

Make Default

Apply to all: OFF

| Read Only Portal | Access to portal elements in read only mode. | OFF |
|---|---|---|

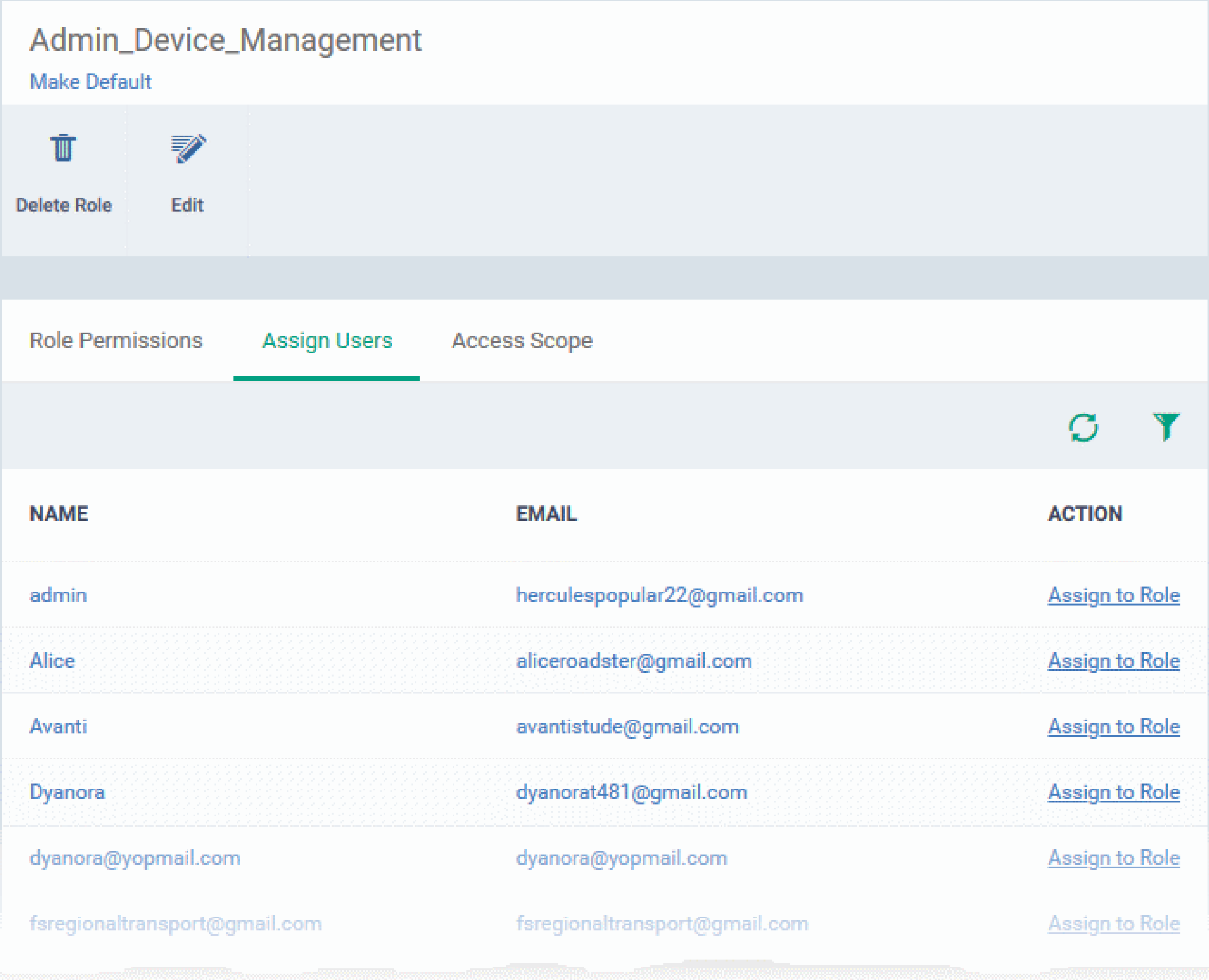
| PERMISSION | DESCRIPTION | ACTION |
|---|---|---|
| users.allow-portal-login | Access to "User Settings" page, "Log in to portal", "Sending user creation email" and "Reset password" actions. | ON |

- Dashboard
- Devices
- User
- Configuration templates
- Network management
- App store
- Applications
- Security sub-systems
- Licence management
- Settings (Templates)
- Settings (Portal Set-Up)
- Settings (Apple DEP)

- Adding or removing the permissions is similar to assigning permissions while creating a role. See the **explanation of assigning permissions** in the previous section **Create a New Role** for help on this.

### View users assigned to a role

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



| NAME | EMAIL | ACTION |
|---|---|---|
| admin | herculespopular22@gmail.com | Assign to Role |
| Alice | aliceroadster@gmail.com | Assign to Role |
| Avanti | avantistude@gmail.com | Assign to Role |
| Dyanora | dyanorat481@gmail.com | Assign to Role |
| dyanora@yopmail.com | dyanora@yopmail.com | Assign to Role |
| fsregionaltransport@gmail.com | fsregionaltransport@gmail.com | Assign to Role |

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

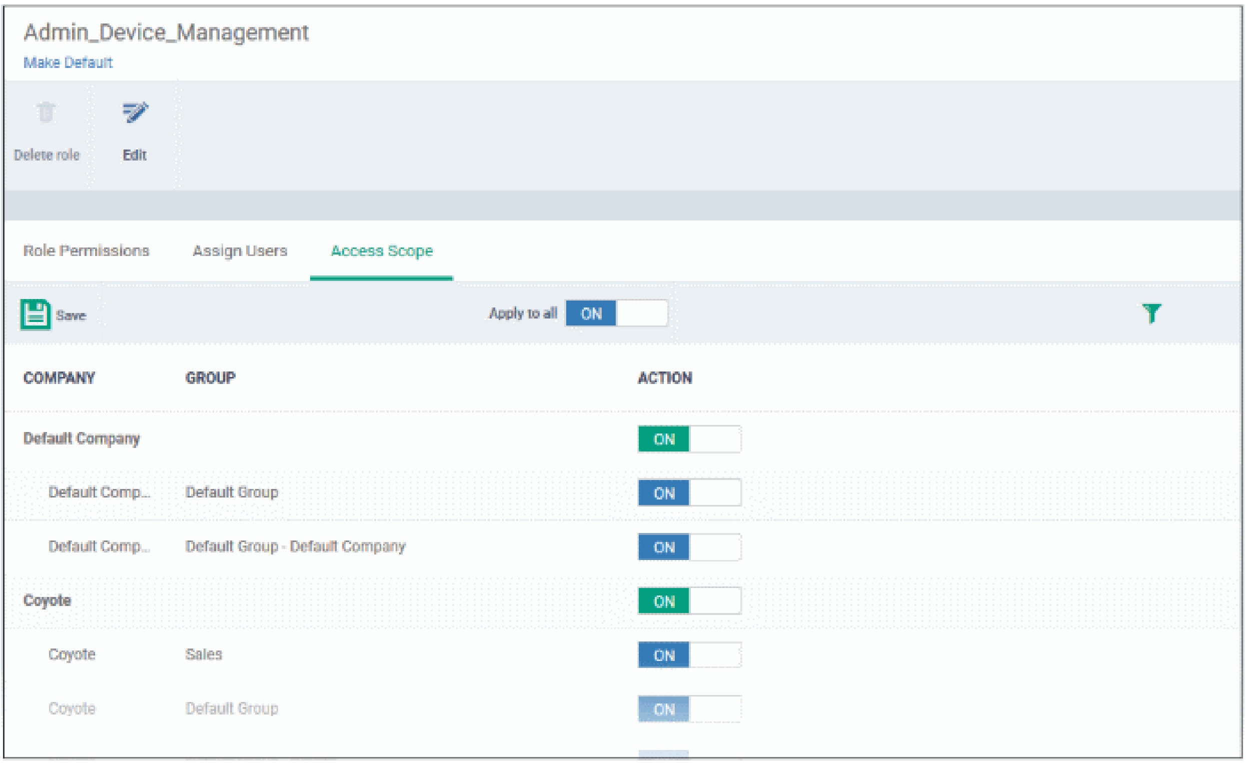
- Click the 'Assign to Role' links to place a user in the role.
- Click the 'Remove from Role' link to unassign a user from the role.

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

- Click a username to open a list of all roles assigned to that user. You can to add or remove roles from the user as required. See **Manage Roles Assigned to a User** for more details.

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

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



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

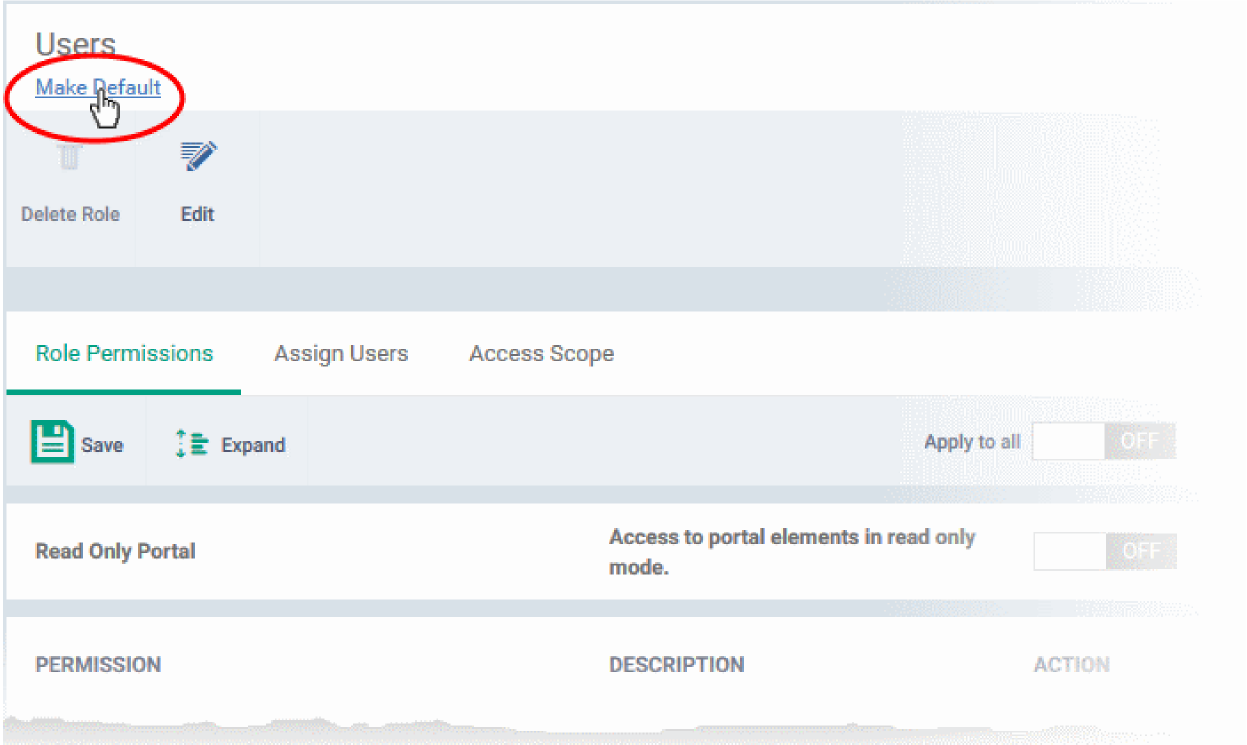
- Use the green 'master' switch beside a company name to enable or disable the ability to manage groups belonging to the company. Please note you should have provided appropriate devices **role permission**.
- Use the switch beside a device group to enable or disable access to the specific group within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

### Set a role as the default role

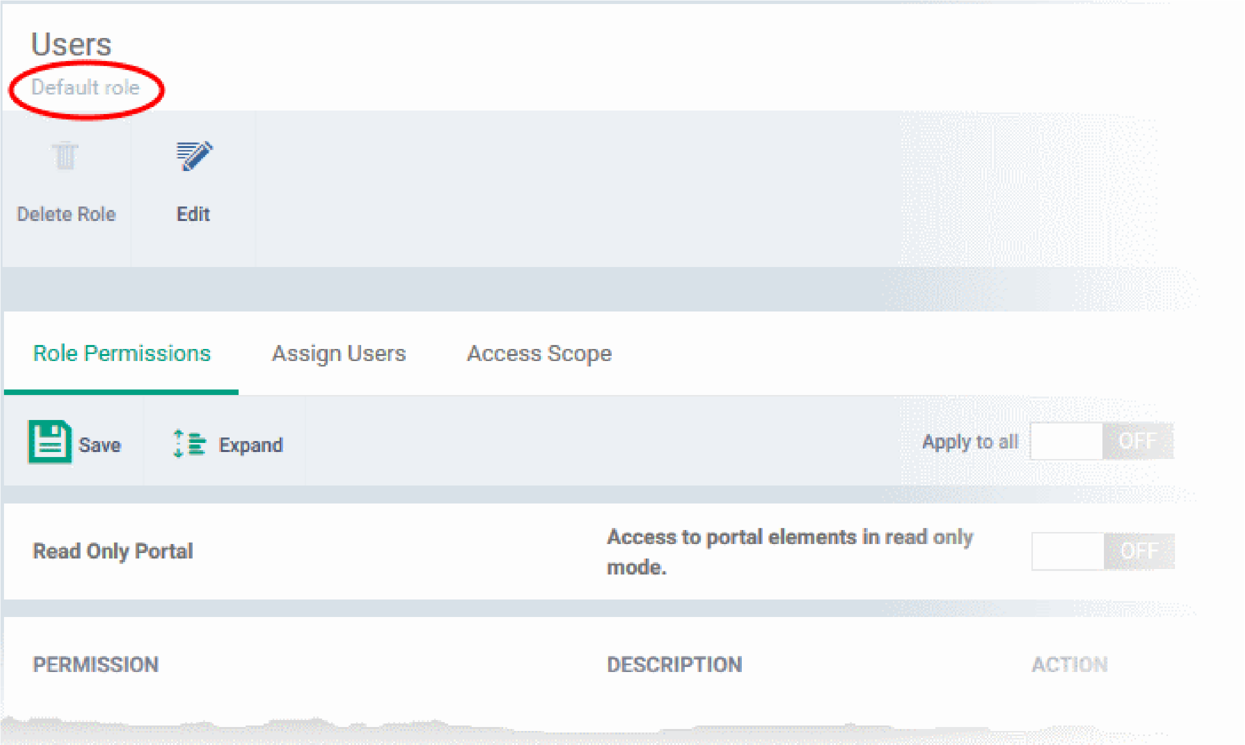
- The default role is automatically applied to any new user unless the admin specifies a different role when adding the user
- The default role is automatically applied to users if their current role is removed

### Set the default role

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



The role is set as default. This is indicated as follows:



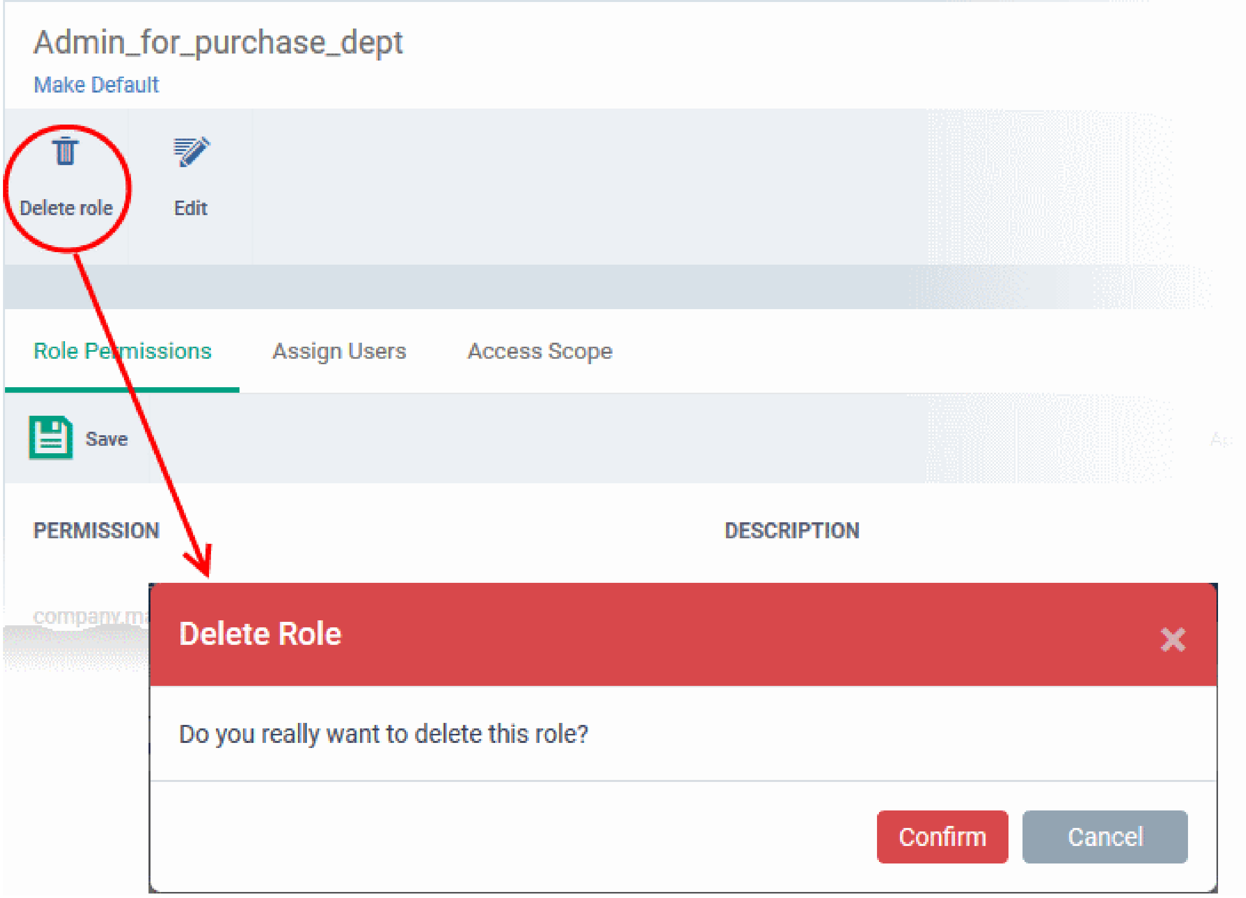
## 4.3.3. Remove a Role

Administrators can delete roles that are no longer deemed necessary.

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

**Remove a role**

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



Do you really want to delete this role?

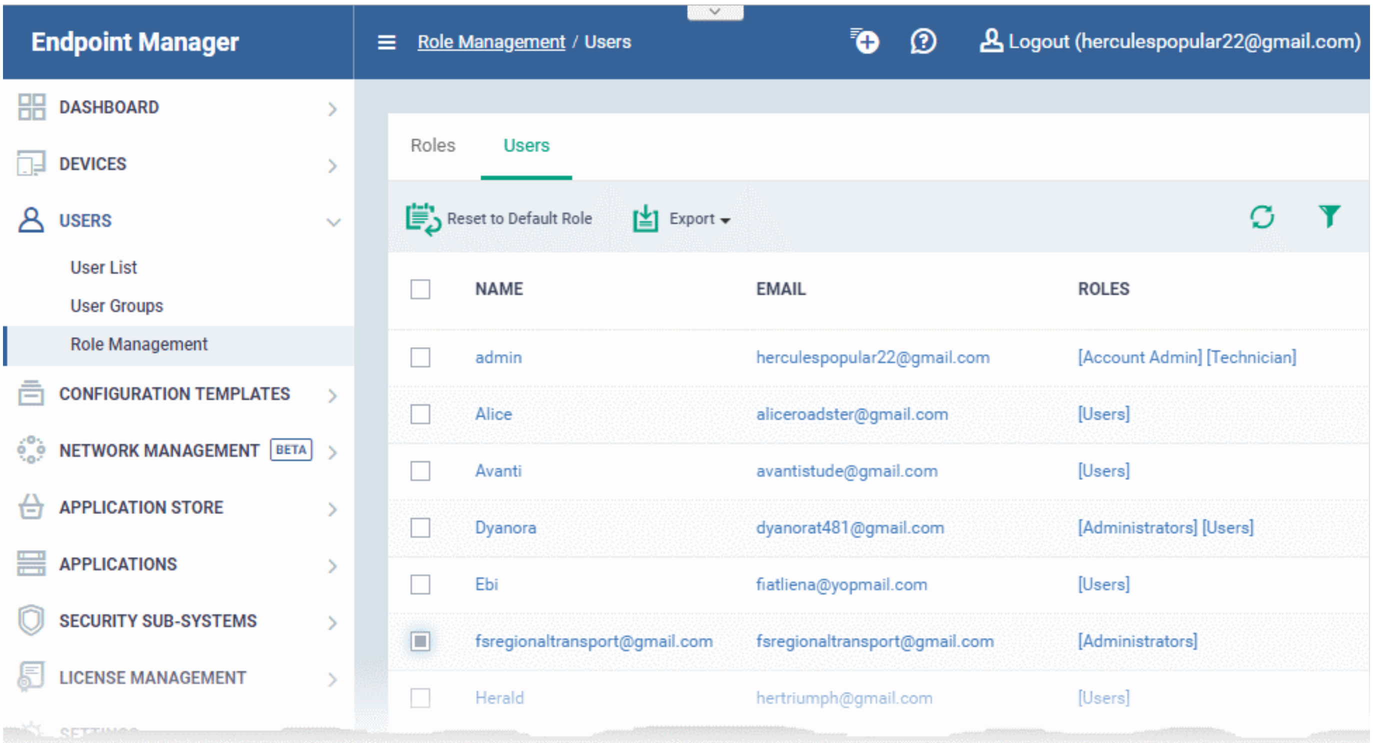
- Click 'Confirm' to remove the role.

## 4.3.4. Manage Roles Assigned to a User

- The 'Users' tab lets you view the roles assigned to each user. A role governs a users permissions and access rights within Endpoint Manager.
- You can add new roles to a user, or remove roles from a user.
  - Note - you cannot assign or remove the 'Account Admin' role. This is automatically assigned to the person that created the CD or C1 account.
- Comodo Dragon and Comodo One customers - All staff created in CD and C1 will be available for selection in all roles, and for all companies. This lets you assign different roles to the same staff member for different companies.
- You can specify which companies a role can access in the role's 'Access scope':
  - Click 'Users' > 'Role Management'
  - Click the 'Roles' tab
  - Click on a role name to open its details page
  - Open the 'Access Scope' tab
  - Enable or disable access to specific companies as required.

### View the list of users with roles assigned to them

- Click 'Users' > 'Role Management'.
- Select the 'Users' tab.



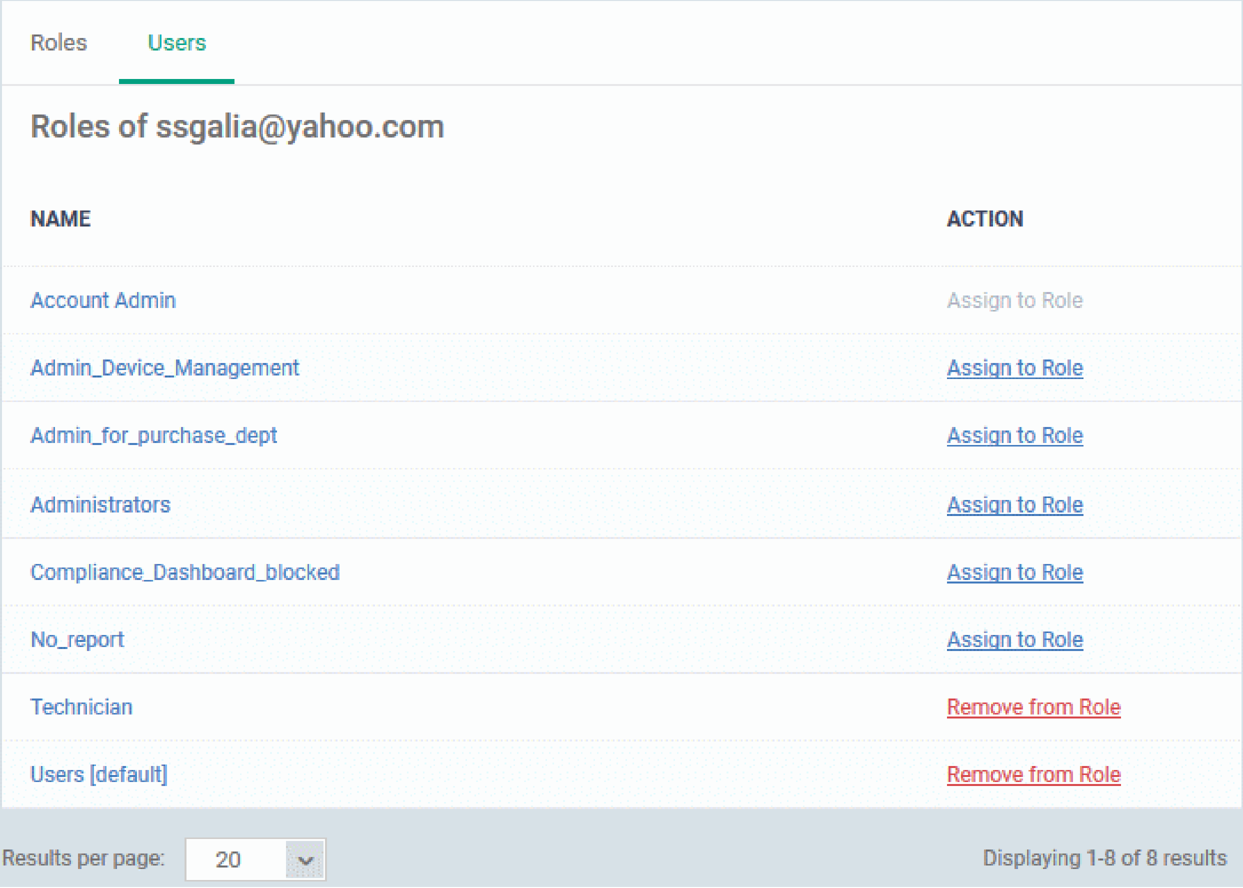
| | NAME | EMAIL | ROLES |
|---|---|---|---|
| □ | admin | herculespopular22@gmail.com | [Account Admin] [Technician] |
| □ | Alice | aliceroadster@gmail.com | [Users] |
| □ | Avanti | avantistude@gmail.com | [Users] |
| □ | Dyanora | dyanorat481@gmail.com | [Administrators] [Users] |
| □ | Ebi | fiatliena@yopmail.com | [Users] |
| ▣ | fsregionaltransport@gmail.com | fsregionaltransport@gmail.com | [Administrators] |
| □ | Herald | hertriumph@gmail.com | [Users] |

The 'Users' interface lets you to:

- **Add or remove roles assigned to a user**
- **Revert a user's role to the Comodo Dragon or Comodo One system default role**

### Manage roles assigned to a user

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



Roles of ssgalia@yahoo.com

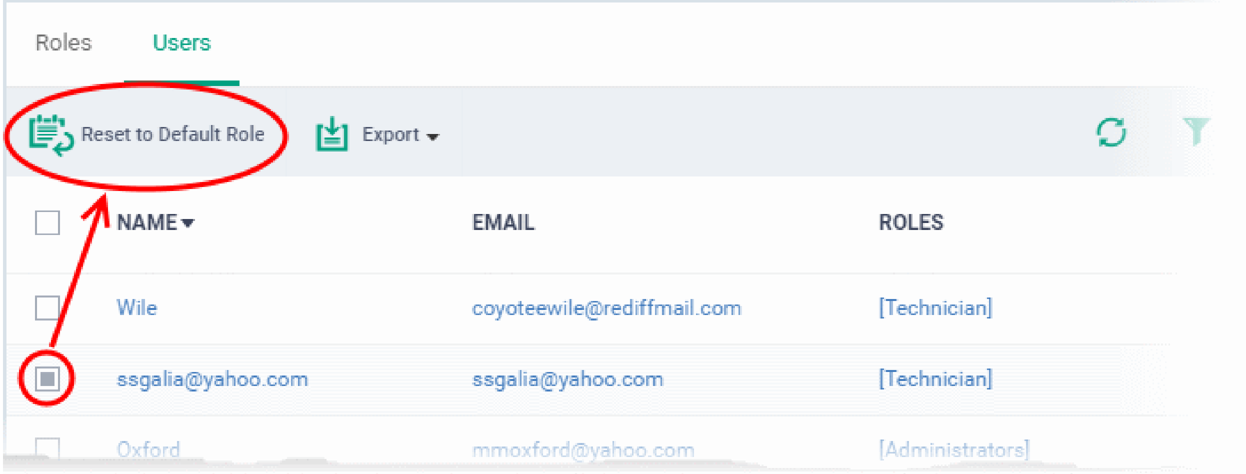
| NAME | ACTION |
|---|---|
| Account Admin | Assign to Role |
| Admin_Device_Management | Assign to Role |
| Admin_for_purchase_dept | Assign to Role |
| Administrators | Assign to Role |
| Compliance_Dashboard_blocked | Assign to Role |
| No_report | Assign to Role |
| Technician | Remove from Role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

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

### Reset the roles to CD or C1 default

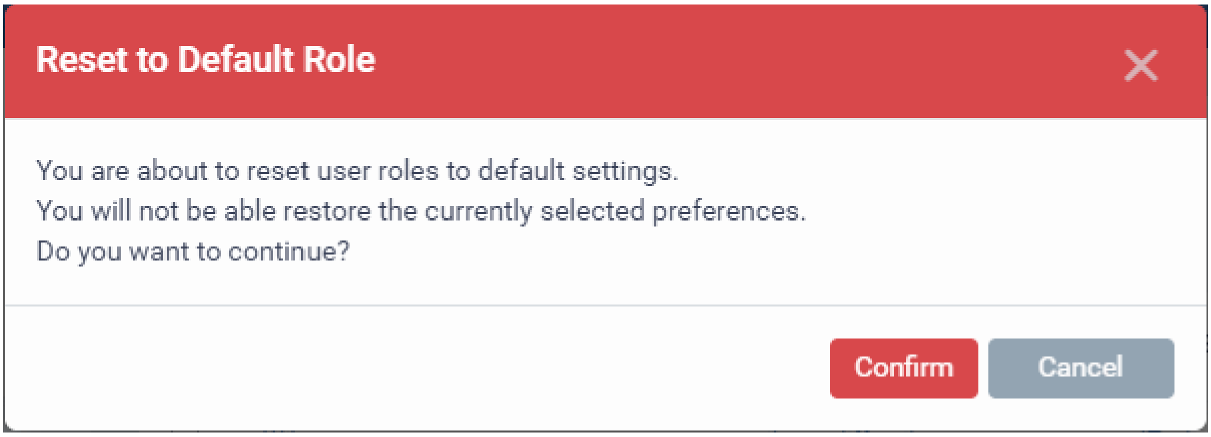
The following only applies to users added via the CD or C1 portal. It does not apply to users added via the Endpoint Manager interface.

- Click 'Users' > 'Role Management'.
- Click the 'Users' tab.



| □ | NAME | EMAIL | ROLES |
|---|---|---|---|
| □ | Wile | coyoteewile@rediffmail.com | [Technician] |
| ☑ | ssgalia@yahoo.com | ssgalia@yahoo.com | [Technician] |
| □ | Oxford | mmoxford@yahoo.com | [Administrators] |

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



Reset to Default Role

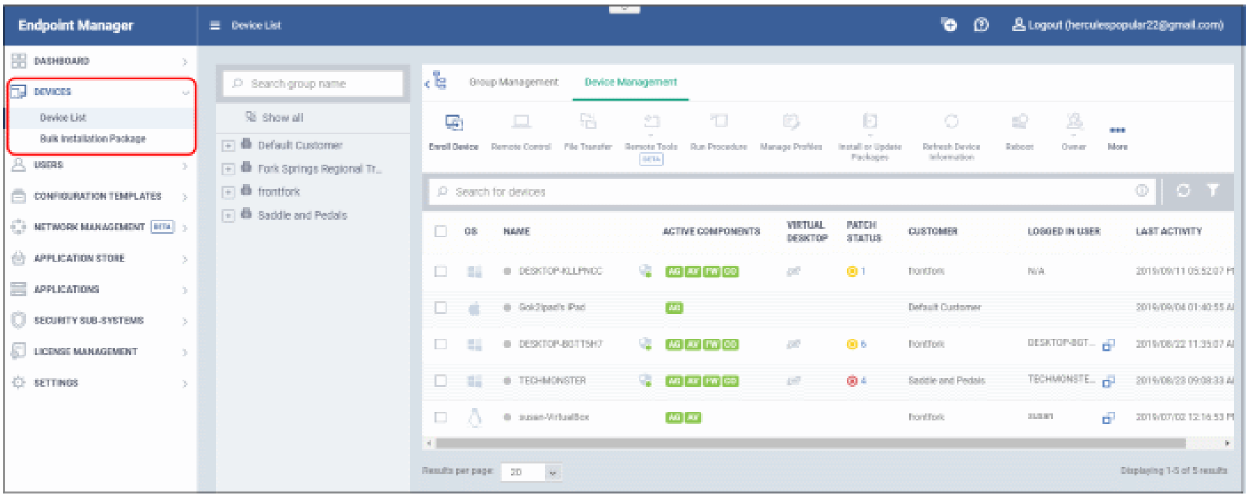
You are about to reset user roles to default settings.
You will not be able restore the currently selected preferences.
Do you want to continue?

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

# 5. Devices and Device Groups

The 'Devices' area allows you to:

- View, manage, and take actions on enrolled devices and device groups.
- Download the packages required for endpoint enrollment (including via Active Directory).
- Download the Remote Control tool, which allows staff to access Windows and Mac endpoints



| OS | NAME | ACTIVE COMPONENTS | VIRTUAL DESKTOP | PATCH STATUS | CUSTOMER | LOGGED IN USER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|
| | DESKTOP-KLLPNCC | AG AV FW CO | | 1 | frontfork | N/A | 2019/09/11 05:52:07 PI |
| | Gok2ipad's iPad | AG | | | Default Customer | | 2019/09/04 01:40:55 AI |
| | DESKTOP-BOTTSH7 | AG AV FW CO | | 6 | frontfork | DESKTOP-BOT... | 2019/08/22 11:35:07 AI |
| | TECHMONSTER | AG AV FW CO | | 4 | Saddle and Pedals | TECHMONSTE... | 2019/08/23 09:08:33 AI |
| | susan-VirtualBox | AG AV | | | frontfork | susan | 2019/07/02 12:16:53 PI |

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

- **Device Management** - Shows all devices added to Endpoint Manager. Use the links in the middle column to view devices which belong to a specific company or group.

  This area lets you add and manage devices, manage device profiles, install CCS, take remote control of Windows and Mac OS devices, remotely lock devices and more. See '**Manage Devices**' for more details.

  - **Note**: See **Enroll User Devices** if you want help add new devices.

- **Group Management** - Create new device groups, view and manage membership of existing groups, apply profiles to groups and more. You can choose the group you wish to manage from the list on the left. See '**Manage Device Groups**' for more details.

- **Bulk Installation Package** - Download the communication client packages required to manually enroll devices and/or bulk-enroll devices from Active Directory. You can also download the Remote Control tool which allows you to interact with remote Windows and Mac OS endpoints. See **Bulk Enrollment of Devices** for more details.

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

### Process in short:

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

Please use the following links to find out more:

- **Manage Device Groups**
  - **Create Device Groups**
  - **Edit Device Groups**
  - **Assign Configuration Profile to Groups**
  - **Remove a Device Group**
- **Manage Devices**
  - **Add New Devices**
  - **Manage Windows Devices**
  - **Manage Mac OS Devices**
  - **Manage Linux Devices**
  - **Manage Android / iOS Devices**
  - **View User Information**
  - **Remove a Device**
  - **Remote Management of Windows and Mac OS Devices**
  - **Remotely Browse Folders and Files on Windows Devices**
  - **Remotely View and Manage Processes Running on Windows Devices**
  - **Remotely View and Manage Services Running on Windows Devices**
  - **Apply Procedures to Windows Devices**
  - **Remotely Install and Update Packages on Windows Devices**
  - **Remotely Install Packages on Mac OS Devices**
  - **Remotely Install Packages on Linux Devices**
  - **Install Apps on Android / iOS Devices**
  - **Generate an Alarm on a Device**
  - **Lock / Unlock Selected Devices**
  - **Wipe Selected Devices**
  - **Assign Configuration Profile to Devices**
  - **Set or Reset Screen Lock Passwords**
  - **Update Device Information**

- Send Text Messages to Devices
- Restart Selected Windows Devices
- Change a Device's Owner
- Change Device Ownership Status
- Generate Device List Report

- Bulk Enrollment of Devices
  - Enroll Windows and Mac OS Devices by Installing the EM Communication Client Package
  - Enroll the Android and iOS Devices of Active Directory Users
  - Download and Install the Remote Control Tool

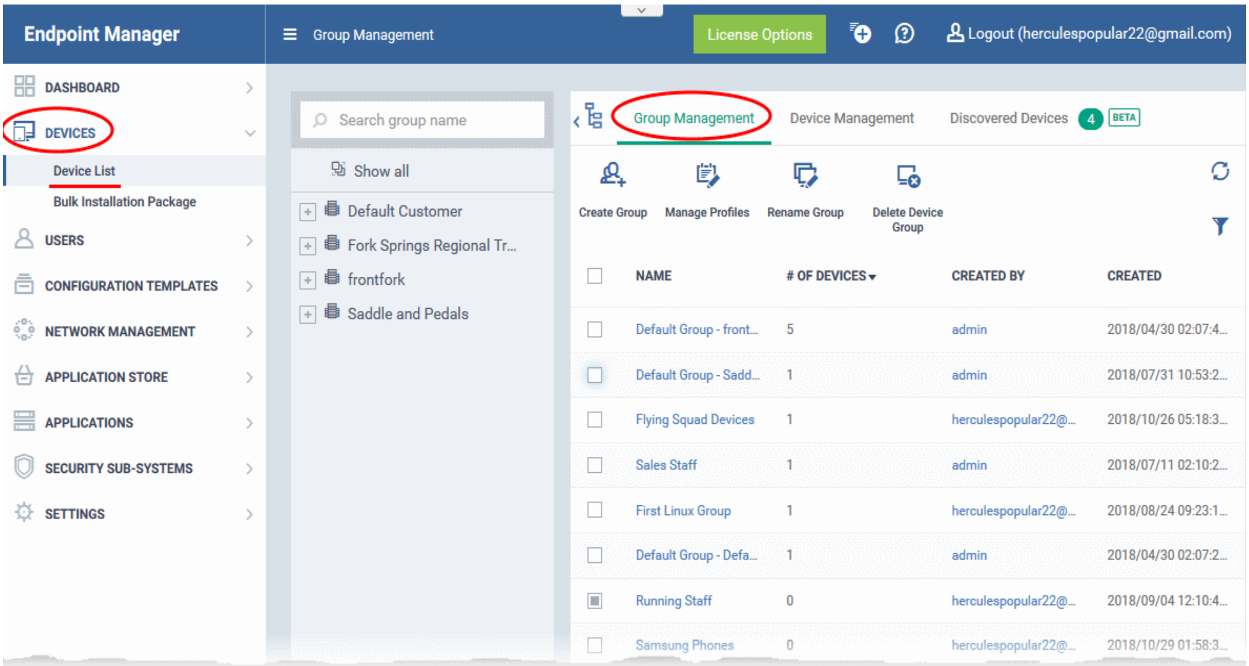
## 5.1. Manage Device Groups

- Click 'Devices' > 'Device List > 'Group Management'

Device groups make it easy to manage large numbers of Android, iOS, Mac, Windows or Linux devices.

The ability to create device groups depends on your account type. See the table below for details:

| | |
|---|---|
| Comodo Dragon MSP Customers | Can create separate device groups for each Company/Organization enrolled in their Dragon account. All companies and groups can be selected from the list to the left of the main pane. |
| Comodo Dragon Enterprise Customers | Can only create groups under the 'Default Company'. |
| Comodo One MSP Customers | Can create separate device groups for each Company/Organization enrolled in their Comodo One account. All companies and groups can be selected from the list to the left of the main pane. |
| Comodo One Enterprise Customers | Can only create groups under the 'Default Company'. |
| Endpoint Manager Stand-alone Customers | Can only create groups under the 'Default Company'. |



| NAME | # OF DEVICES | CREATED BY | CREATED |
|---|---|---|---|
| Default Group - front... | 5 | admin | 2018/04/30 02:07:4... |
| Default Group - Sadd... | 1 | admin | 2018/07/31 10:53:2... |
| Flying Squad Devices | 1 | herculespopular22@... | 2018/10/26 05:18:3... |
| Sales Staff | 1 | admin | 2018/07/11 02:10:2... |
| First Linux Group | 1 | herculespopular22@... | 2018/08/24 09:23:1... |
| Default Group - Defa... | 1 | admin | 2018/04/30 02:07:2... |
| Running Staff | 0 | herculespopular22@... | 2018/09/04 12:10:4... |
| Samsung Phones | 0 | herculespopular22@... | 2018/10/29 01:58:3... |

- Click a customer or group name in the middle pane to view devices belonging to that entity.

- The group management tab also lets you create new groups, import devices into groups, assign configuration profiles to groups and more.

**To view and manage device groups**

- Click 'Devices' > 'Device List'
- Click the 'Group Management' tab
  - Select a company to view the list of groups in that company

    Or
  - Select 'Show All' to view every device group added to EM

| Device Groups - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of the device group.<br>• Click a group name to view all devices in that group.<br>• You can add or remove devices to/from the group, manage group configuration profiles, export the device list to .csv and more. See **Edit a Device Group** for more details. |
| Number of Devices | How many devices are in the group. |
| Created By | The administrator who created the group.<br>• Click the name to view the details of the administrator. See **View User Information** for more details. |
| Created | The date and time at which the group was created. |

## Sorting, Search and Filter Options

- Click any column header to sort items in alphabetical or numerical order
- Click the funnel icon ▼ to configure filters
- Use the search box to find a specific group

## Profiles

Configuration profiles containing specific settings can be created for any group. If a device is enrolled in multiple groups, then the group profiles of all groups are applied to the device. If the settings in one group profile clash with those of another, EM follows the most restrictive policy. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera.

For more details on creating and managing configuration profiles, see **Configuration Templates**.

See the following sections for more details about:

- **Create Device Groups**
- **Edit a Device Group**
- **Assign Configuration Profiles to a Device Group**
- **Remove a Device Group**

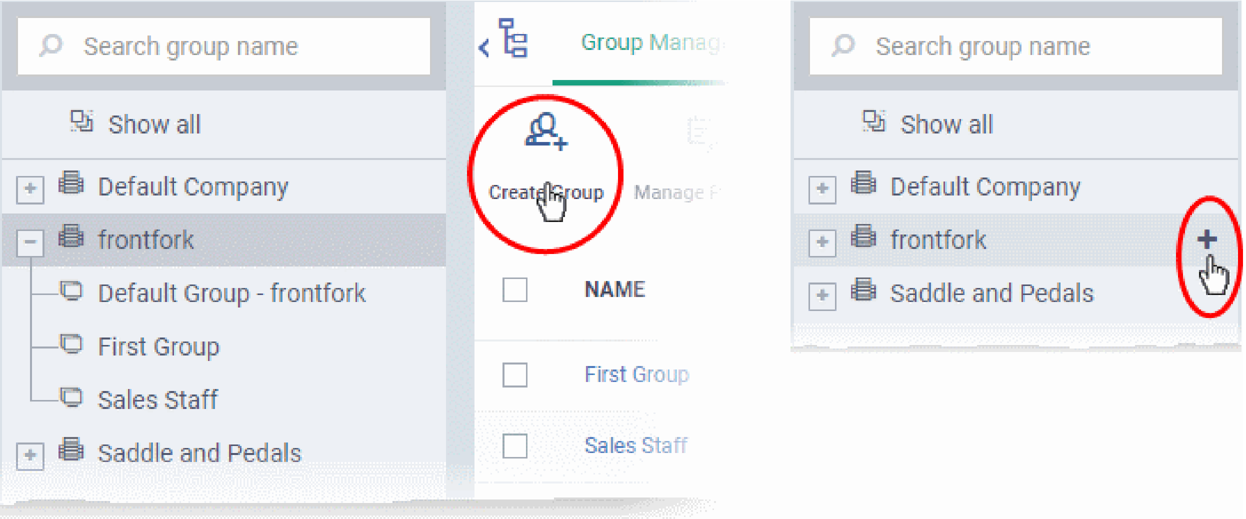
## 5.1.1. Create Device Groups

- Placing devices into a group lets you run actions and apply profiles to multiple devices at once.

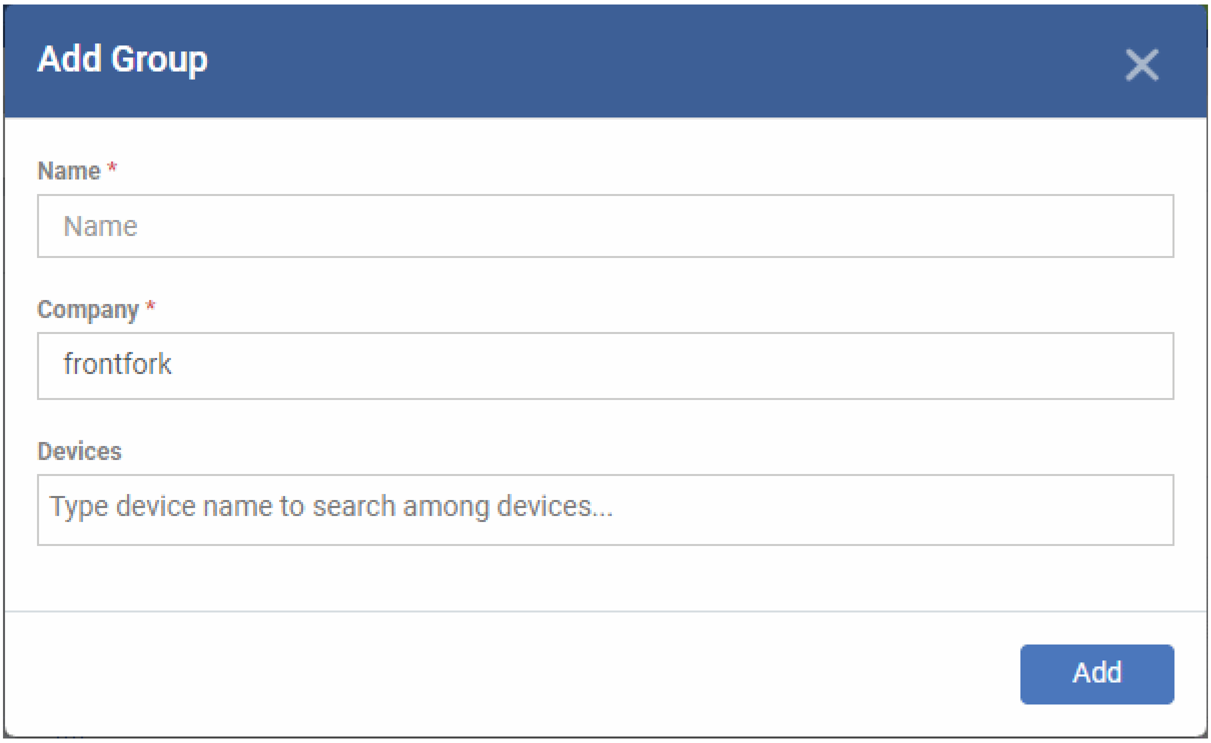
- OS-specific profiles will be automatically applied to relevant devices.

**To add a new device group**

- Click 'Devices' > 'Device List'
- Click the 'Group Management 'tab
- Select a company/department on the left (CD MSP and C1 MSP customers only)
- Click the 'Create Group' button
    - MSP customers can also place their mouse over the company name and click the '+' sign that appears:



The 'Add Group' interface will open.

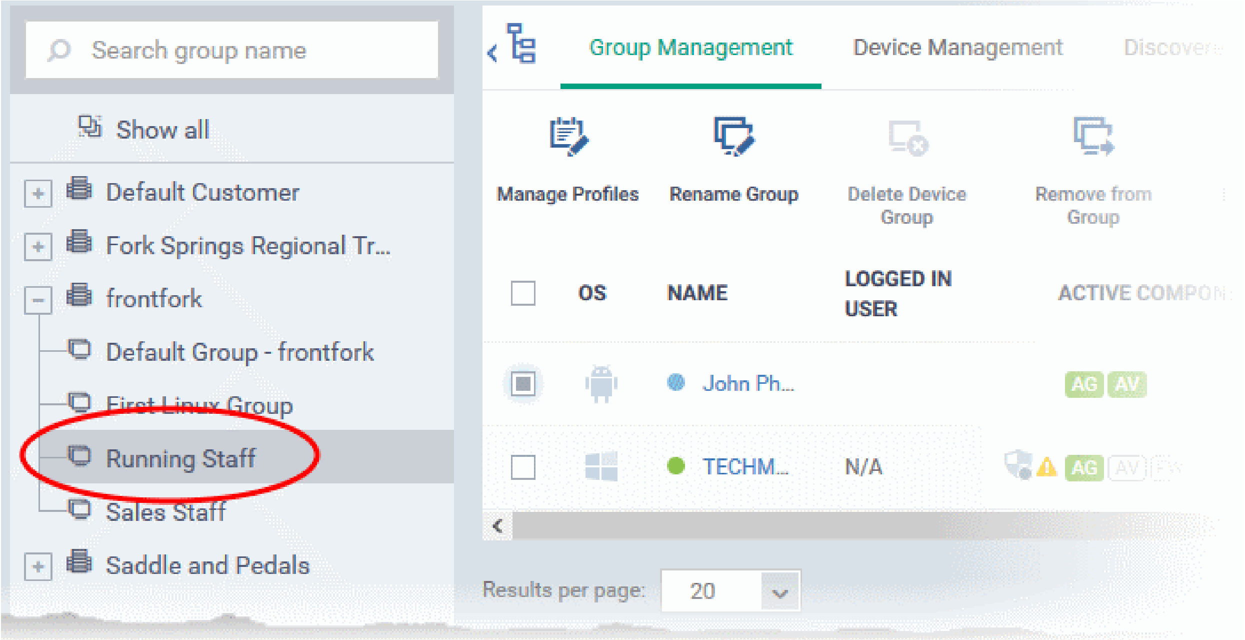


| 'Add Group' dialog - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Name | Create a label to identify the group. |

| 'Add Group' dialog - Table of Parameters | |
|---|---|
| | |
| Company | The parent company of the group. The company to which the group belongs.<br>• If you already selected a company on the left then this field is pre-populated. You cannot edit this field.<br>• If you selected 'Show All' then you need to choose a parent company for the group.<br>  • Type first few letters of the company name and select the company from the options. |
| Devices | Choose devices which will be members of the group.<br>• Type the first few letters of the device name and select from the suggestions.<br>• Repeat the process to add more devices.<br>• Note - You can only add devices which are enrolled to the parent company.<br>**Tip**: You can add devices at a later stage too. |

- Fill the details and click 'Add'.

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

## 5.1.2. Edit a Device Group

The 'Group Management' interface lets you view/add/remove devices, rename the group and manage group policies.

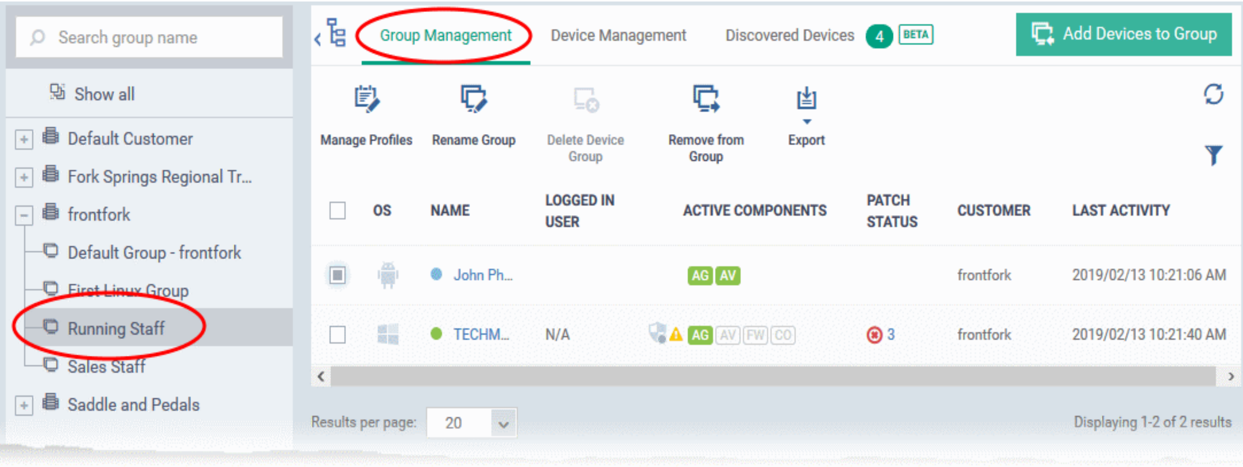
- **View or edit a device group**
- **Add new devices to a group**

- **Remove devices from a group**
- **Rename a group**
- **Assign Configuration profiles to a device group**
- **Export the list of devices in a group**
- **Remove a group**

### View or edit a device group

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

The group management interface for the selected group will open.



| | OS | NAME | LOGGED IN USER | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|
| ☐ | | John Ph... | | AG AV | | frontfork | 2019/02/13 10:21:06 AM |
| ☐ | | TECHM... | N/A | AG AV FW CO | 3 | frontfork | 2019/02/13 10:21:40 AM |

The list of devices included in the group will be displayed, with their details.

| Device Group Details - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the device. |
| Name | The label assigned to the device by the user.<br>• Grey text color indicates the device has been offline for the past 24 hours.<br>• If no name is assigned, the model number of the device will be used as the name. You can assign a new name as required.<br>• Click the device name to view device details.<br>• See **Manage Windows Devices**, **Manage Mac OS Devices**, **Manage Linux Devices** and **Managing Android / iOS Devices** for more details. |
| Logged in User | The name of the user currently signed-in to the device.<br>• The user name is prefixed with the active directory (AD) domain or workgroup that the user is currently logged-in to:<br>• Active Directory - Name is shown as <AD domain name>\<user name><br>• Workgroup - Name is shown as <workgroup name>\<user name><br>• No network - Name is shown as <device name>\<user name> |

| | |
|---|---|
| | • Click the ⧉ icon to copy the username to the clipboard. |
| Active Components | • Comodo Client Security modules which are enabled on the device<br>• Examples include 'Antivirus', 'Firewall', 'Containment' and 'Agent Only'<br>The possible components for each OS are as follows:<br>• Android - Antivirus and agent (EM communication client)<br>• iOS - Agent<br>• Windows - Antivirus, agent, firewall and containment.<br>• Mac OS - Antivirus and agent<br>• Linux - Antivirus and agent |
| Patch status | The number of patches available for Windows endpoints. Patch statuses are as follows:<br>✓ - No patches required. All patches are up-to-date.<br>⊗ - Critical patches are available.<br>The number to the right shows how many are pending. Click the number to view and manage the patches. See **View and Install Windows and 3rd Party Application Patches** for more details.<br>⊗ - Optional patches are available. Click the number to the right to view and manage the patches. |
| Customer | The name of the company to which the device is enrolled.<br>• CD MSP customers / C1 MSP customers customers can enroll devices to any of the companies they have created in CD / C1.<br>• CD Enterprise customers / C1 Enterprise / EM standalone customers can only use the 'Default company'. |
| Last Activity | The date and time at which the device last communicated with the EM server. |
| **Controls** | |
| Add Devices to Group | Add devices of any operating system to the group. See **Add new devices to a group** for more details. |
| Manage Profiles | View and apply configuration profiles to all member devices in the group at once. See **Assign Configuration Profiles to a Device Group** for more details. |
| Rename Group | Change the label of the group. |
| Delete Device Group | Remove unwanted device groups from EM.<br>Note - You cannot delete a device group unless it is empty. Remove all member devices before deleting.<br>See **Remove a Device Group** for more details. |
| Remove from Group | Remove unwanted devices from the group. See **Remove devices from a group** for more details. |
| Export | Save a list of devices in the group in .csv format.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of Devices in a Group** for more details. |

- Click column headers to sort the items in ascending/descending order of entries in that column.

## Search and Filter Options

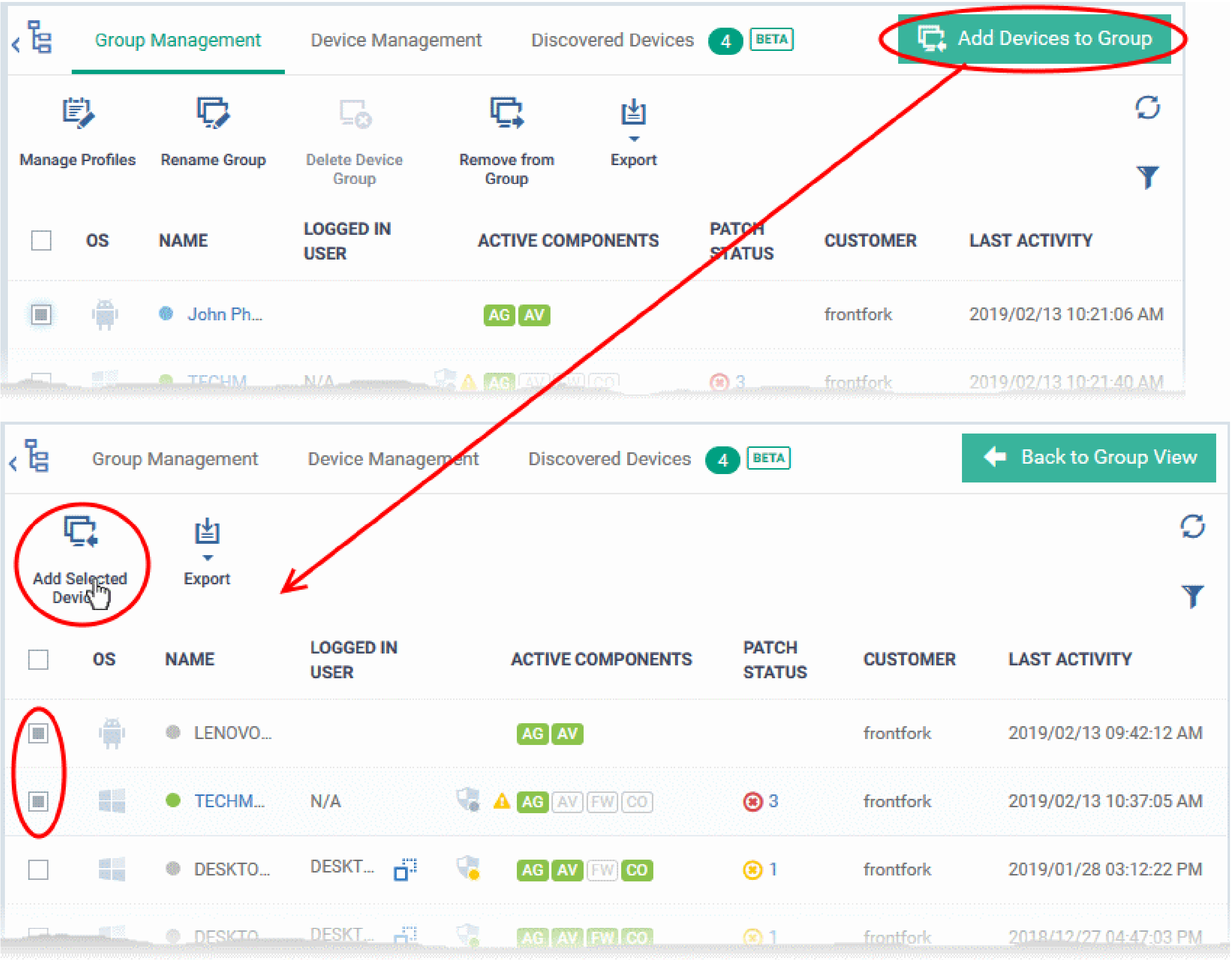
- Click the funnel button at the right end to open the filter options.
    - To filter the items or search for a device based on its OS, online status, name, patch status, company, currently logged-in user and/or a period of last activity, enter the search criteria in part or full in the text box and click 'Apply'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- EM 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.

## Add New Devices to a Group

- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Click 'Add Devices to Group' at the top right.

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

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



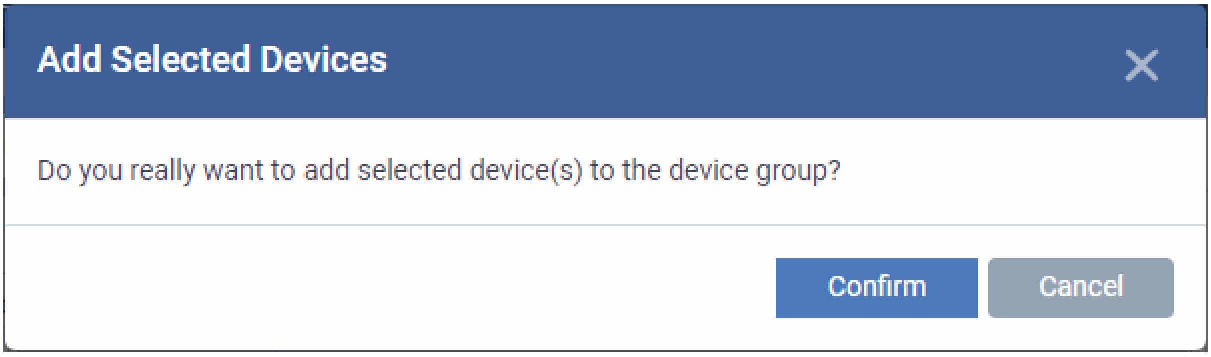
| | OS | NAME | LOGGED IN USER | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|
| □ | | John Ph... | | AG AV | | frontfork | 2019/02/13 10:21:06 AM |
| □ | | TECHM... | N/A | AG AV FW CO | 3 | frontfork | 2019/02/13 10:21:40 AM |

| □ | OS | NAME | LOGGED IN USER | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|
| ☑ | | LENOVO... | | AG AV | | frontfork | 2019/02/13 09:42:12 AM |
| ☑ | | TECHM... | N/A | AG AV FW CO | 3 | frontfork | 2019/02/13 10:37:05 AM |
| □ | | DESKTO... | DESKT... | AG AV FW CO | 1 | frontfork | 2019/01/28 03:12:22 PM |
| □ | | DESKTO... | DESKT... | AG AV FW CO | 1 | frontfork | 2018/12/27 04:47:03 PM |

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

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

A confirmation dialog will appear.



Add Selected Devices

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

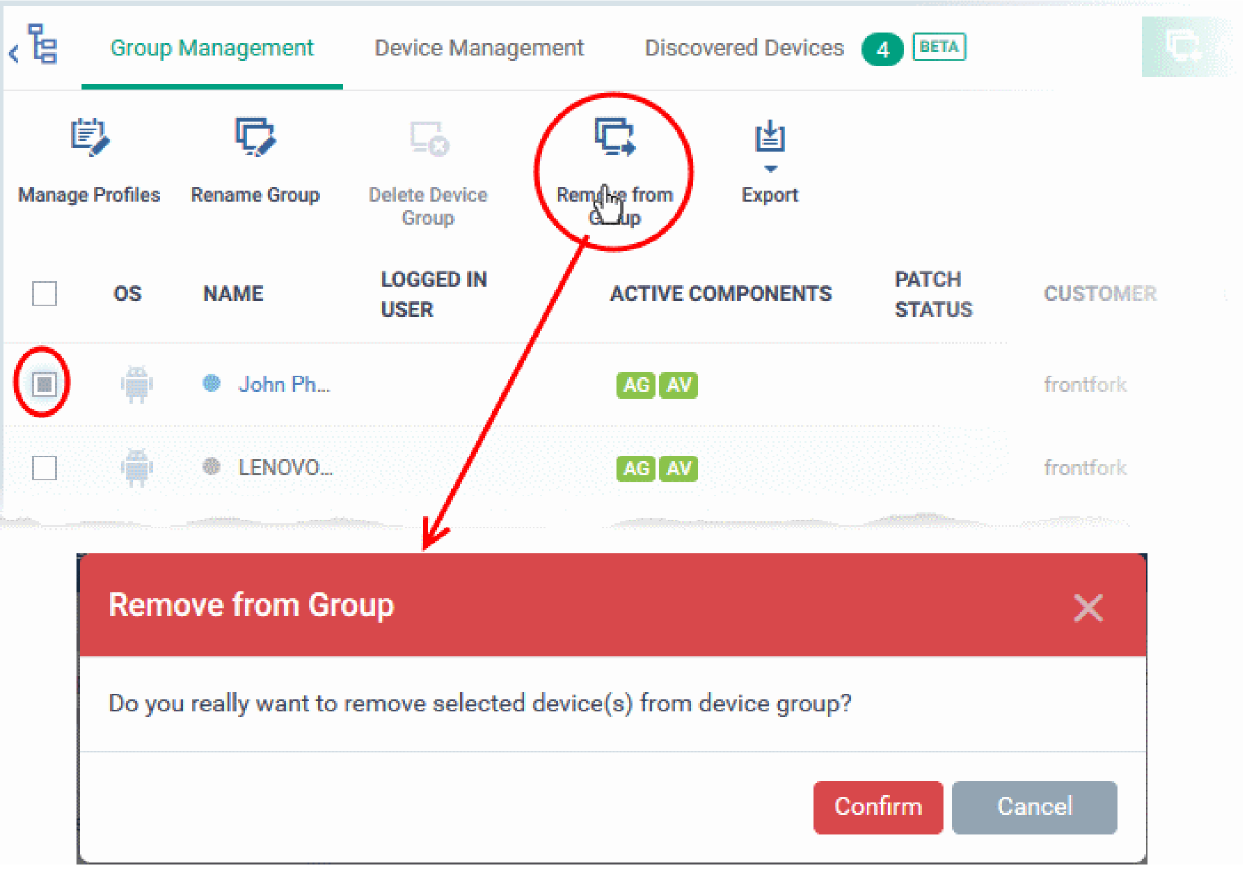
- Click 'Confirm'. The devices will be added to the group.

Once the device(s) are added to the group, the configuration profiles, associated with the group, will be applied to the device, in addition to the profiles, which are already in effect on the device.

**Tip**: You can add a device to a group from the 'Device Details' interface too. For more details, see **View and Manage Device Group Membership**.

## Remove Devices from a Group

- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Choose the devices you want to remove
- Click 'Remove from Group'



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

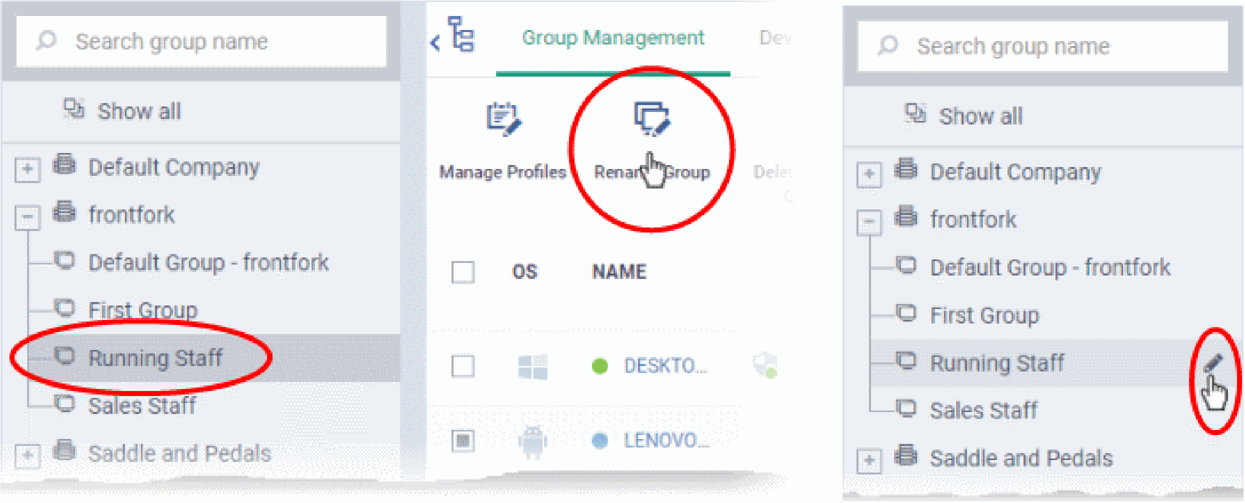
  - Click 'Confirm' in the confirmation dialog.

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

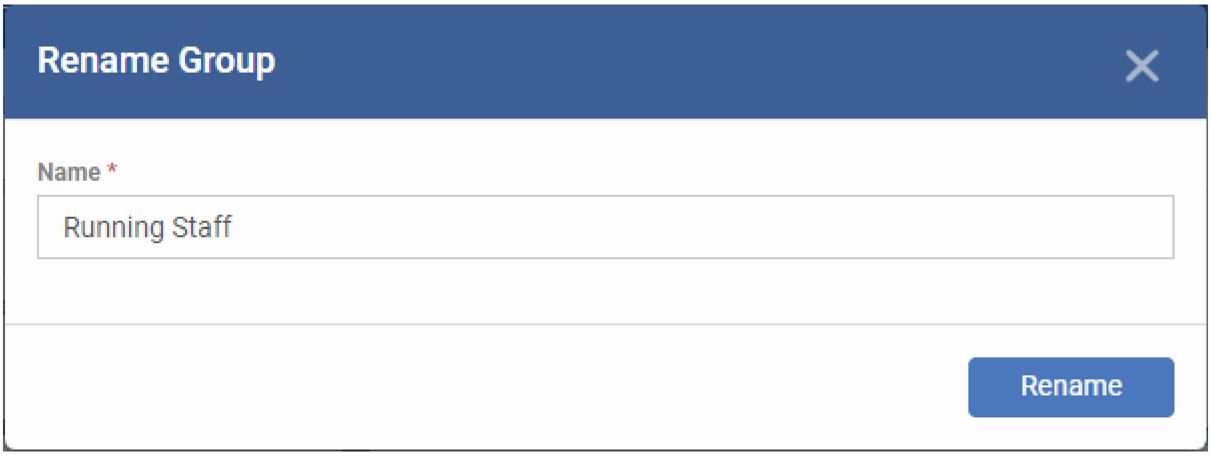
**Tip**: You can remove the membership of a device to a group, from the 'Device Details' interface too. For more details, see **View and Manage Device Group Membership**.

## Rename a Group

- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Click 'Rename Group'
  - Alternatively, move your mouse over the group name and click the pencil icon



The 'Rename Group' dialog will open.



Name *

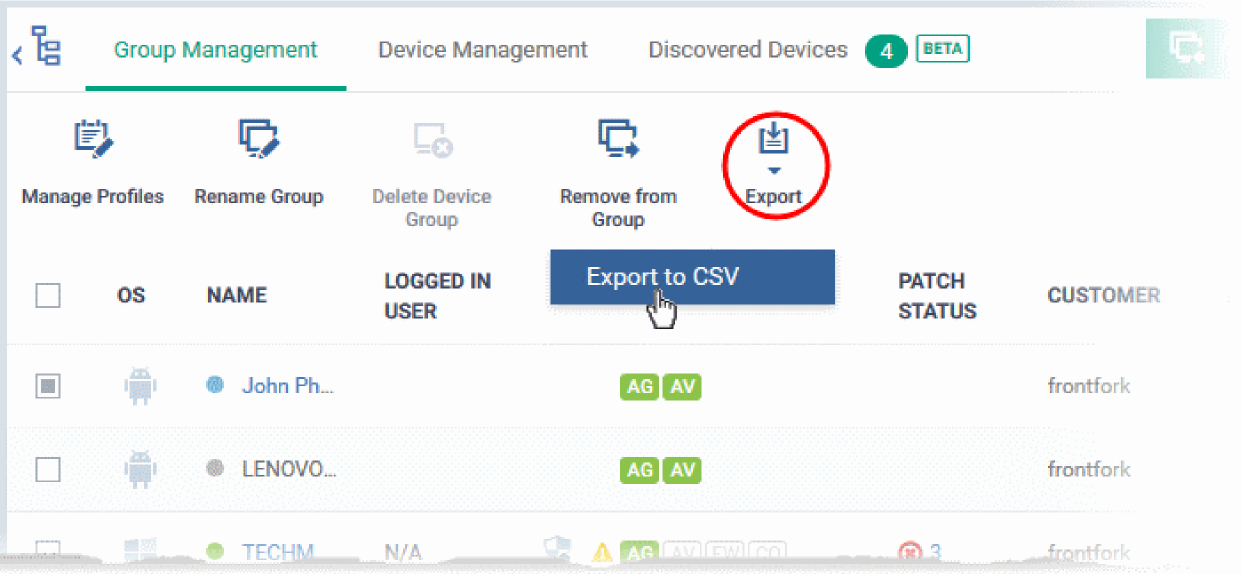
Running Staff

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

The group will be updated with the new name.

## Export the List of Devices in a Group

- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Click the 'Export' button above the table then choose 'Export to CSV':



| ☐ | OS | NAME | LOGGED IN USER | | PATCH STATUS | CUSTOMER |
|---|---|---|---|---|---|---|
| ☒ | | John Ph... | | AG AV | | frontfork |
| ☐ | | LENOVO... | | AG AV | | frontfork |
| ☐ | | TECHM | N/A | AG AV FW CO | 3 | frontfork |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

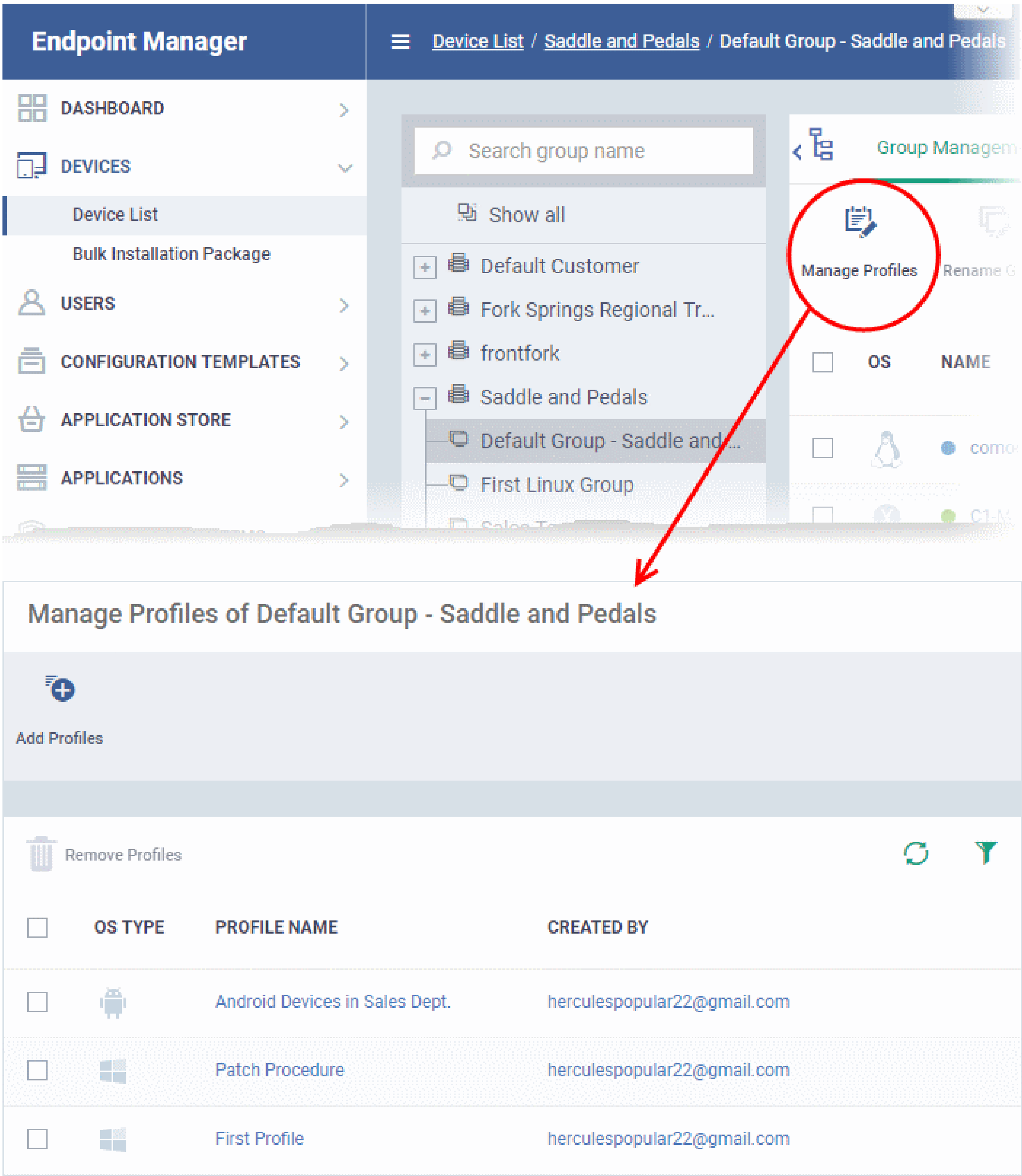
## 5.1.3. Assign Configuration Profiles to a Device Group

You can view profiles currently assigned to a device group, add new profiles or remove existing profiles.

- See **Configuration Profiles** if you need help to create a profile.

**To view and manage the profiles applied to a group**

- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Click 'Manage Profiles' from the options at the top
- This will show a list of all profiles associated with the device:

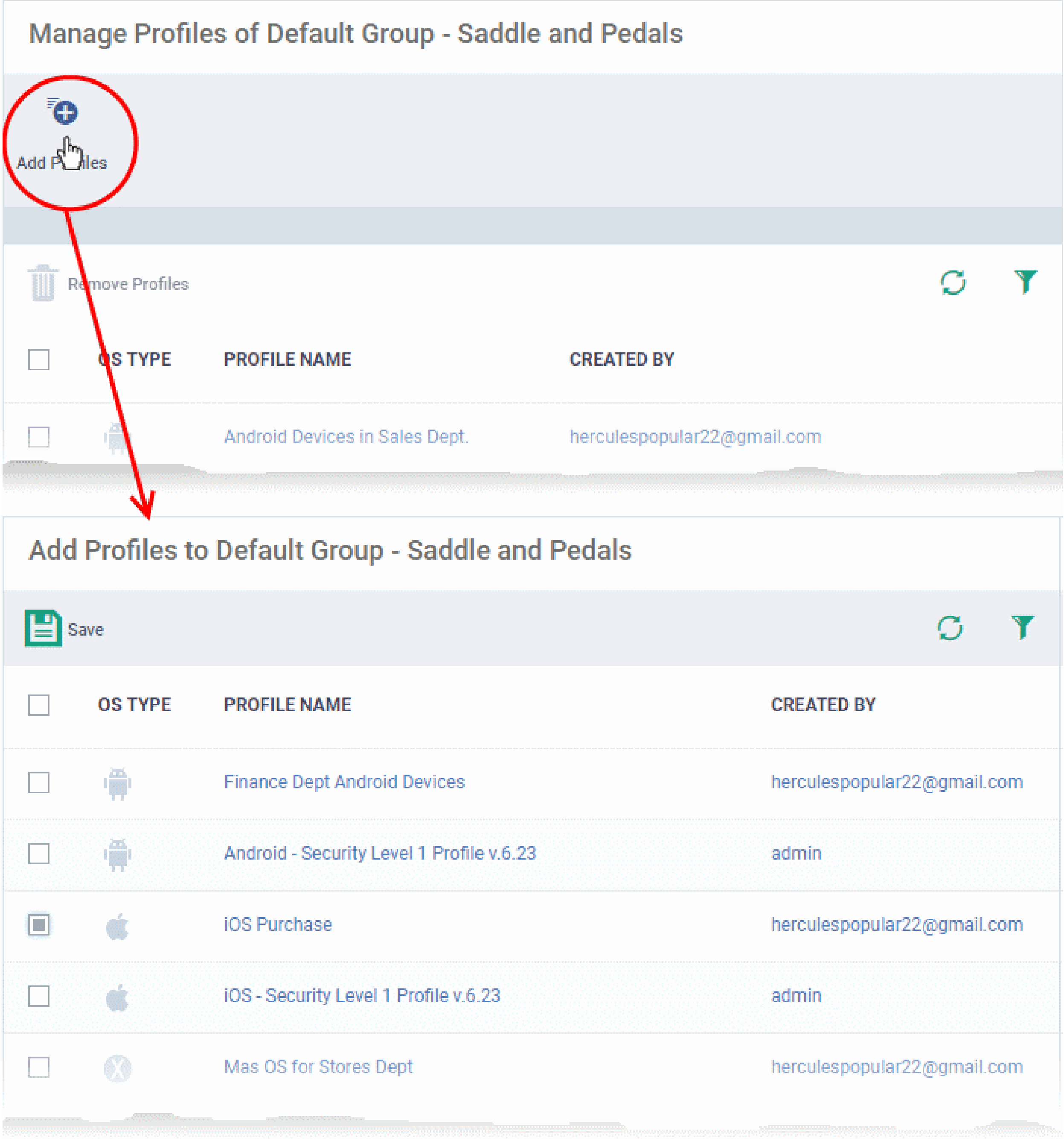


Manage Profiles of Default Group - Saddle and Pedals

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |
| □ | | Patch Procedure | herculespopular22@gmail.com |
| □ | | First Profile | herculespopular22@gmail.com |

**To add a new profile**

- Click 'Add Profiles' at the top.
- Select the profiles you want to apply to the group then click 'Save'.



Manage Profiles of Default Group - Saddle and Pedals

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Android Devices in Sales Dept. | herculespopular22@gmail.com |

Add Profiles to Default Group - Saddle and Pedals

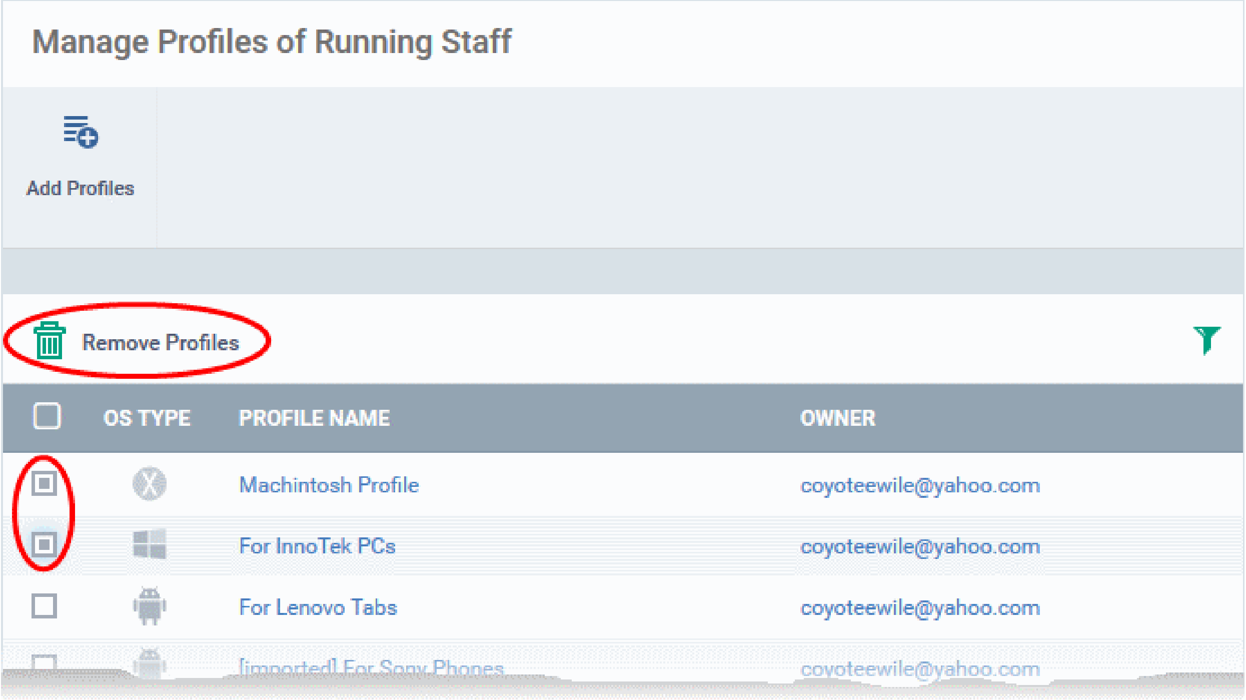
| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | Finance Dept Android Devices | herculespopular22@gmail.com |
| □ | | Android - Security Level 1 Profile v.6.23 | admin |
| ☑ | | iOS Purchase | herculespopular22@gmail.com |
| □ | | iOS - Security Level 1 Profile v.6.23 | admin |
| □ | | Mas OS for Stores Dept | herculespopular22@gmail.com |

**Tip**: Click the funnel icon at top-right to filter the list or search for a specific profile.

EM applies all profiles which are appropriate for a device's operating system.

**To remove a profile from a group**

- Select the profile(s) to be removed, from the 'Manage Profiles' interface and click 'Remove Profiles'



Manage Profiles of Running Staff

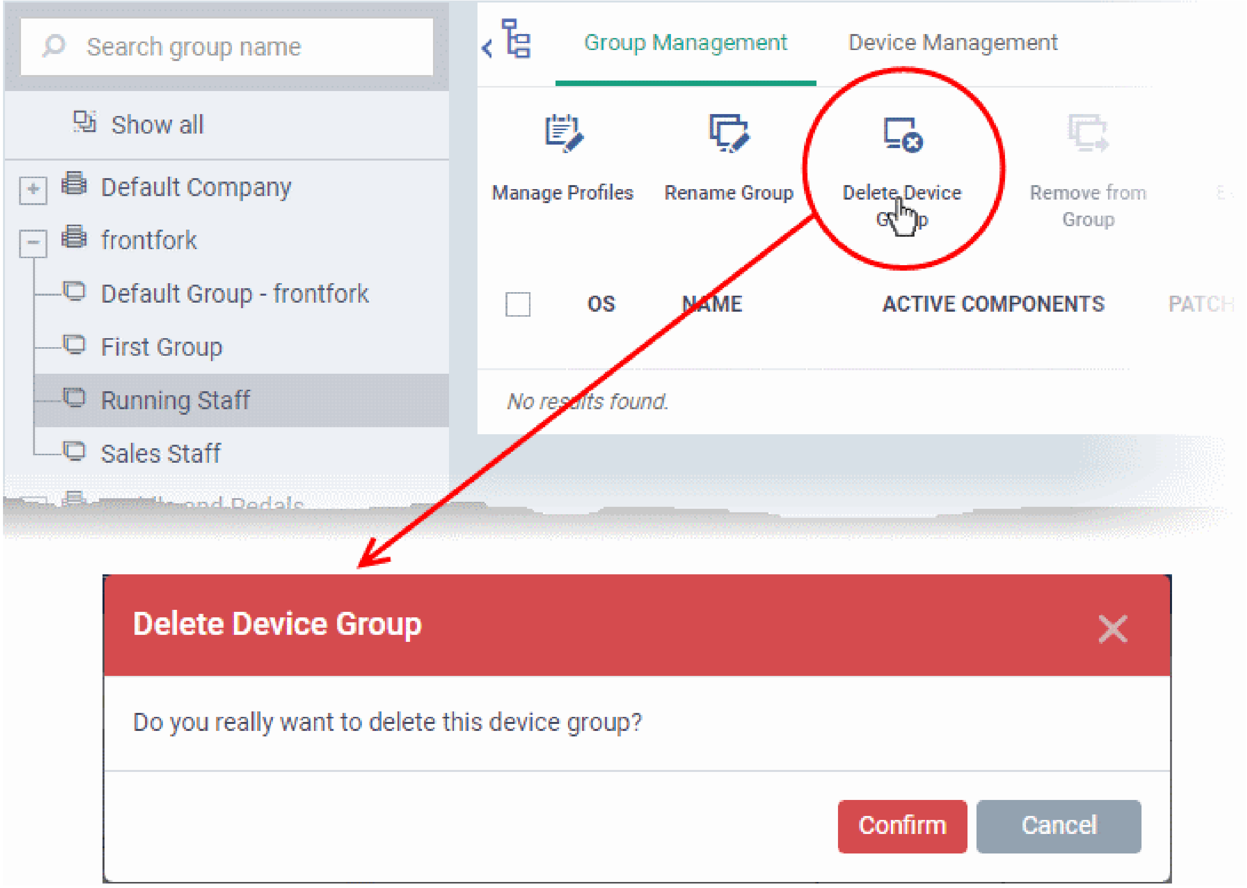
| ☐ | OS TYPE | PROFILE NAME | OWNER |
|---|---|---|---|
| ☑ |  | Machintosh Profile | coyoteewile@yahoo.com |
| ☑ |  | For InnoTek PCs | coyoteewile@yahoo.com |
| ☐ |  | For Lenovo Tabs | coyoteewile@yahoo.com |
| ☐ |  | [imported] For Sony Phones | coyoteewile@yahoo.com |

The profile(s) will be removed from member devices of the group, where applied, according to their operating system(s).

**Note**: Disassociating a profile from a device group will remove the profile from devices only if it is applied because the device is a member of that group. If the same profile is applied to a member device through some other source, (like the profile is applied to the user of the device or a group to which the user belongs), then the profile will not be removed.

## 5.1.4. Remove a Device Group

- Note - you cannot delete a device group unless it is empty. Remove all member devices first.
- Click 'Devices' > 'Device List'
- CD MSP / C1 MSP customers customers - choose the parent company on the left
- Click the name of the group you want to edit
- Click the 'Group Management' tab
- Ensure there are no devices in the group. See **Remove all devices from the group** if required.
- Click 'Delete Device Group'.



Delete Device Group

Do you really want to delete this device group?

- Click 'Confirm' to apply your changes

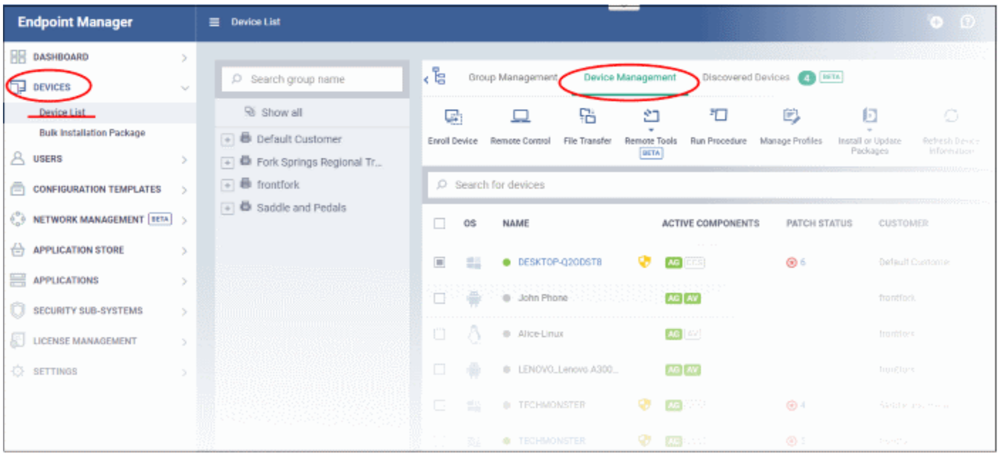
The device group will be removed from EM.

## 5.2. Manage Devices

- Click 'Devices' > 'Device List' > 'Device Management'

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

- The 'Device Management' screen is an inventory of all mobile devices and endpoints for a company.
- It shows each device's connection and patch status, which security components are enabled, recent activity, and more.



From this area you can:

- Enroll new devices for management (Windows, Mac, Linux, iOS and Android)
- Add or remove profiles on any selected device
- Install Comodo Client Security and other packages on Windows, Mac OS and Linux endpoint
- Take remote control of Windows and Mac OS devices
- Browse folders and files on Windows endpoints
- View and manage processes and services on Windows endpoints
- View applications installed on Windows endpoints
- Remotely uninstall applications from Windows endpoints
- Remotely run procedures on Windows endpoints
- Remotely install OS and third-party application patches on Windows endpoints
- Remotely restart Windows endpoints
- Sound an alarm on mobile devices
- Send custom text messages to mobile devices
- Remotely wipe mobile devices
- Remotely lock mobile and Mac OS devices
- Reset lock-screen passcodes
- 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 manage device group memberships of a device
- Generate a device details reports

**Open the 'Device Management' interface**

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

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

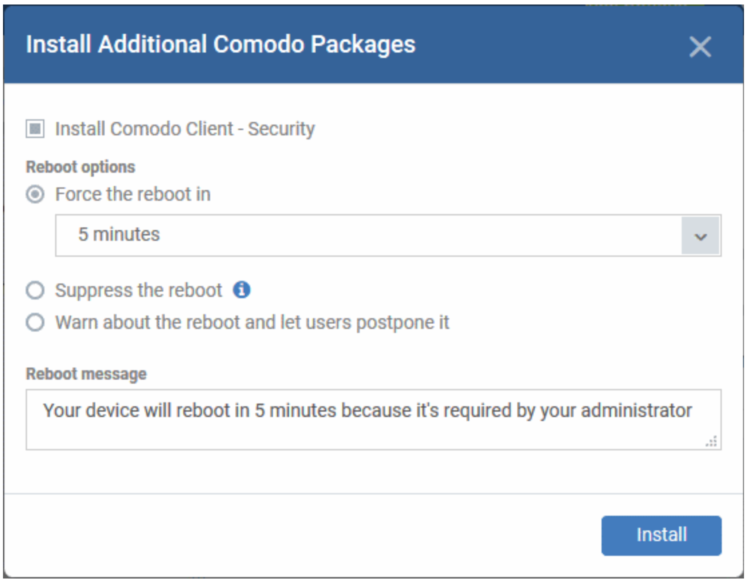
- Select 'Show All' to view every device enrolled to EM.

| Column Heading | Description |
|---|---|
| OS | The operating system of the device. |
| Name | The label assigned to the device by the user. If no name is assigned, the device model number is used as the name.<br>The circle to the left of the name shows the device's connection status:<br>● Gray - Device is not reachable. The connection might be down or the endpoint is switched off.<br>● Blue - Slow connection. The device is connected but commands and messages may take some time to execute since the endpoint is busy.<br>● Green - Good connection. Commands should be executed in real time.<br>Windows endpoints also have a shield icon to the right of their name. The shield has a |

colored circle on it which indicates the status of Comodo Client Security (CCS):

Yellow - CCS is not installed on the endpoint.

- Click the shield icon to remotely install CCS on the endpoint.
- The 'Install Additional Comodo Packages' dialog will appear.



**Install Additional Comodo Packages** ✕

☑ Install Comodo Client - Security

**Reboot options**

● Force the reboot in

5 minutes

○ Suppress the reboot ⓘ

○ Warn about the reboot and let users postpone it

**Reboot message**

Your device will reboot in 5 minutes because it's required by your administrator

Install

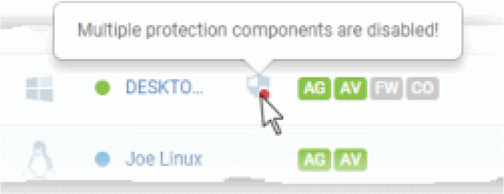
- CCS requires the endpoint to be restarted in order for the installation to take effect.
- Configure the 'Restart' options and click 'Install'.
- See the **explanation of remote installation of CCS** in **Remotely Install and Update Packages on Windows Devices** for more details

Gray - Outdated clients. Communication Client (CC) and/or Comodo Client Security (CCS) on the endpoint require updates.

Note. This status is only shown on endpoints that have CC 6.16 + and CCS 10.0 + installed.

Red - The endpoint is at risk. One or more of security components (AV, FW or containment) may have been disabled by the user.

- Place your mouse over the icon to view the warning:



Multiple protection components are disabled!

Amber - The endpoint needs attention. The virus signature database might be out-dated or the endpoint needs to be re-started after installation of CCS.

- Place your mouse over the icon to view the full message

Green - The endpoint is secure. All installed components are up and running.

Blue - CCS is in 'Silent Mode'.

**Note**: CCS lets users enable 'Silent Mode' if they do not want to be

| | |
|---|---|
| | disturbed by product notifications. For example, when running a full-screen presentation.<br>Alerts and notifications are suppressed and operations that could interfere with their work are postponed.<br>⚠ - Communication with CCS on the endpoint has been lost.<br>• Click the device name to open the device details interface. See **Manage Windows Devices**, **Manage Mac OS Devices** and **Manage Android / iOS Devices** for more details. |
| Active Components | Indicates which modules are installed on the device. Possible components are 'Agent', 'Antivirus' (AV), 'Firewall' (FW) and 'Containment'.<br>• Android devices - The agent will automatically install the AV (antivirus) component.<br>• iOS devices - Only the agent (EM client) will be installed<br>• Windows endpoints - Available components are - Agent, AV, FW (firewall) and Containment. These components are installed automatically when a profile featuring the components is installed.<br>• Mac OS endpoints - Available components are EM Agent and AV<br>The color of the icon shows the status of the component:<br>• Green - Installed and active<br>• Gray - Installed but disabled by profile setting<br>• Blue (only applies to the 'Containment' module) - The containment module is baselining the device. During the baseline period, unknown files are auto-submitted to Valkyrie for analysis, but are not placed in containment. See **Baseline Settings** in **Containment Settings** for help to configure baseline settings.<br>• Blank - Component is not installed. |
| Virtual Desktop | The status of the virtual desktop on the endpoints:<br>• Running - The virtual desktop is open on the endpoint<br>• Not Running - The virtual desktop is not open on the endpoint<br>• Unsupported - The version of the security and/or communication client on the endpoint does not support the virtual desktop. Alternatively, it can mean the security client is not installed at all. |
| Patch status | • The number of patches available for Windows endpoints. Patch status icons are as follows:<br>✓ - No patches required. All patches are up-to-date.<br>⊗ - Critical patches are available.<br>The number to the right shows how many are pending. Click the number to view and manage the patches. See **View and Install Windows and 3rd Party Application Patches** for more details.<br>⊗ - Optional patches are available. Click the number to the right to view and manage the patches. |

| | |
|---|---|
| Customer | The name of the company to which the device is enrolled.<br>• Comodo One MSP customers can enroll devices to any of the companies they have created in C1.<br>• Comodo One Enterprise customers / EM standalone customers can only use the 'default company'. |
| Logged in User | The name of the user currently signed-in to the device.<br>• The user name is prefixed with the active directory (AD) domain or workgroup that the user is currently logged-in to:<br>• Active Directory - Name is shown as <AD domain name>\<user name><br>• Workgroup - Name is shown as <workgroup name>\<user name><br>• No network - Name is shown as <device name>\<user name><br>• Click the ⧉ icon to copy the username to the clipboard. |
| Last Activity | The date and time at which the device last communicated with the EM agent. |

- Click a column header to sort items in ascending/descending order of entries in that column.
- Use the search box at the top to filter devices by any parameter in the table.
- Click the funnel button ▼ on the right to view more filters.

Please use the following links to find out more:

- **Add New Devices**
- **Manage Windows Devices**
  - **View and Edit Device Name**
  - **View Summary Information**
  - **View Hardware Information**
  - **View Network Information**
  - **View and Manage Profiles Associated with Windows Device**
  - **View and Manage Applications Installed on a Device**
  - **View List of Files on the Device**
  - **View CCS Configuration Exported from the Device**
  - **View MSI Files Installed on the Device through Endpoint Manager**
  - **View and Install Windows and Third Party Application Patches**
  - **View Antivirus Scan History**
  - **View and Manage Device Group Memberships**
  - **View Device Logs**
- **Manage Mac OS Devices**
  - **View and Edit Mac OS Device Name**
  - **View Summary Information**
  - **Manage Installed Applications**
  - **View and Manage Profiles Associated with the Device**
  - **View Mac OS Packages Installed on the Device through Endpoint Manager**
  - **View and Manage Device Group Memberships**
- **Manage Linux Devices**
  - **View and Edit Linux Device Name**
  - **View Summary Information of Linux Device**

    - View Network Information of a Linux Device
    - View and Manage Profiles Associated with a Linux Device
    - View Linux Packages Installed on a Device through Endpoint Manager
    - View and Manage Device Group Memberships
- Manage Android / iOS Devices
    - View and Edit Device Name
    - View Summary Information
    - Manage Installed Applications
    - View and Managing Profiles Associated with the Device
    - View Sneak Peek Pictures to Locate Lost Device
    - View the Location of the Device
    - View and Manage Device Group Memberships

## 5.2.1. Add New Devices

Device enrollment is covered in the users section of this guide.

- See **Enroll User Devices** for help to add new devices.

## 5.2.2. Manage Windows Devices

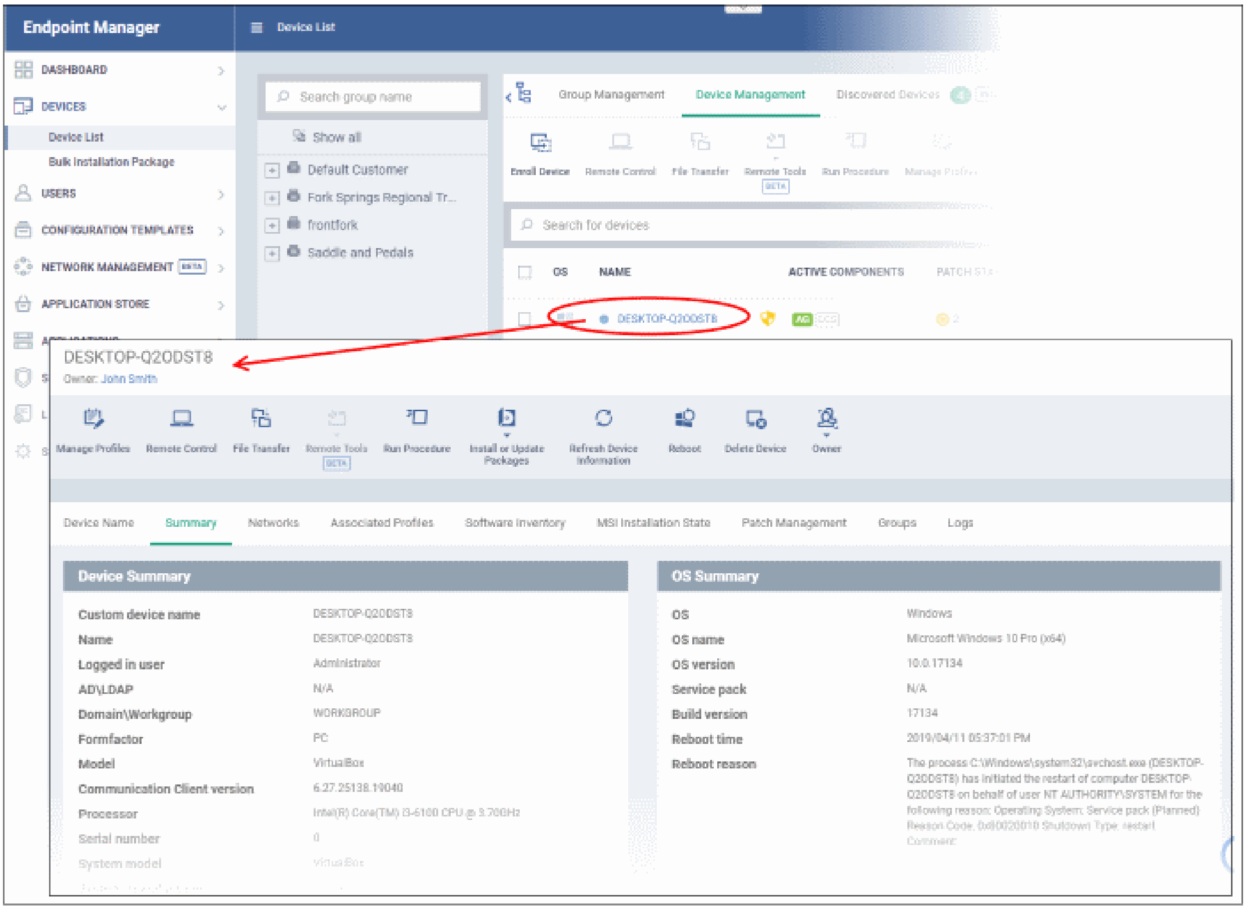
- The device details page lets you view a device's hardware and software, installed components and network connections.
- You can also manage device profiles, installed applications, patches and device group membership.

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

**View and manage a Windows device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the main configuration pane
    - Select a company or group to view devices in that group

      Or
    - Select 'Show all' to view every device enrolled to Endpoint Manager
- Click the name of any Windows device to open its details pane:



Device Summary

| | |
|---|---|
| Custom device name | DESKTOP-Q2ODST8 |
| Name | DESKTOP-Q2ODST8 |
| Logged in user | Administrator |
| AD\LDAP | N/A |
| Domain\Workgroup | WORKGROUP |
| Formfactor | PC |
| Model | VirtualBox |
| Communication Client version | 6.27.25138.19040 |
| Processor | Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz |
| Serial number | 0 |
| System model | VirtualBox |

OS Summary

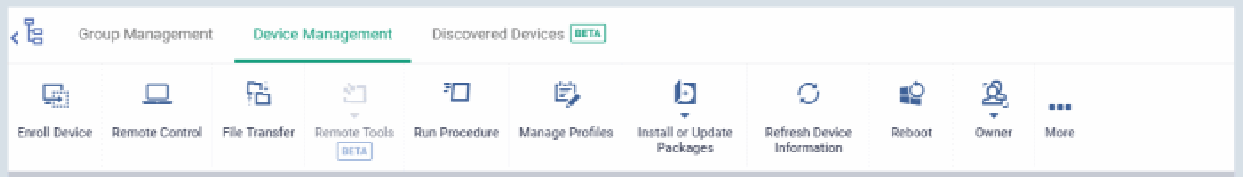
| | |
|---|---|
| OS | Windows |
| OS name | Microsoft Windows 10 Pro (x64) |
| OS version | 10.0.17134 |
| Service pack | N/A |
| Build version | 17134 |
| Reboot time | 2019/04/11 05:37:01 PM |
| Reboot reason | The process C:\Windows\system32\svchost.exe (DESKTOP-Q2ODST8) has initiated the restart of computer DESKTOP-Q2ODST8 on behalf of user NT AUTHORITY\SYSTEM for the following reason: Operating System: Service pack (Planned) Reason Code: 0x80020010 Shutdown Type: restart Comment: |

The details screen contains a maximum of thirteen tabs:

- **Device Name** - The device label. You can change this as per your preference. See **View and Edit Device Name** for more details.
- **Summary** - General details about the device. This includes hardware and OS information, resource usage data, and an overview of CCS configuration. See **View Summary Information** for more details.
- **Hardware** - Hardware configuration of the selected device. This tab is only available if legacy Comodo RMM agent is installed. See **View Hardware Information** for more details.
- **Networks** - Information about the device's network card, MAC address, IP address, and more. See **View Network Information** for more details.
- **Associated Profiles** - Details of the profiles deployed on the device. See **View and Manage Profiles Associated with the Device** for more details.
- **Software Inventory** - Applications installed on the device. See **View Applications Installed on a Device** for more details.
- **File List** - Inventory of files on the device along with their file rating ('Unrecognized', 'Trusted' or 'Malicious'). See **View the Files on a Device** for more details. Note - the 'File List' tab is only available if Comodo Client Security is installed on the device. See **Remotely Install and Update Packages on Windows Devices** for more details.
- **Exported Configurations** - Saved Comodo Client Security configuration files. These files let you export CCS settings to different endpoints. See **View CCS Configurations Exported from the Device** for more details. Note - the 'Exported Configurations' tab is only available for devices with Comodo Client Security installed. See **Remotely Install and Update Packages on Windows Devices** for more details.
- **MSI Installation State** - MSI packages that have been installed on the device via Endpoint Manager. See **View MSI Files Installed on the Device through Endpoint Manager** for more details.

- **Patch Management** - A list of available patches for the device. See **View and Install Windows and 3rd Party Application Patches** for more details.
- **Antivirus Scan History** - A list of all threats identified on the device over time, and the actions taken by Endpoint Manager in response. See **View Antivirus Scan History** for more details. Note - the 'Antivirus Scan History' tab is only available if Comodo Client Security is installed on the device. See **Remotely Install and Update Packages on Windows Devices** for more details.
- **Groups** - A list of device groups to which the endpoint belongs. You can also manage group membership from here. See **View and Manage Device Group Membership** for more details.
- **Logs** - View event logs from activities recorded on the device. See **View Device Logs** for more details.
    - **Alert Logs** - Alerts generated because of a breach of monitoring conditions or because of a procedure deployment.
    - **Monitoring Logs** - Monitoring rules can be added to an EM policy to observe resource usage on a device. For example, you may wish to create a log entry if CPU usage goes above 75% for a certain period of time.
    - **Script Logs** - Script procedures that were run on the Windows device. Scripts can be run manually or automatically via a profile schedule.
    - **Patch Logs** - A record of operating system patch installations. Patches can be installed manually or automatically via a profile schedule.
    - **Third Party Patch Logs** - A record of patch installations for non-Comodo applications.
    - **Installation Logs** - Apps installed on the device from the Windows Application store (Application Store > Windows Application Store). See **Install Windows Apps on Devices** for more details.

You can remotely perform various tasks on the device using the buttons above the table:



- **Manage Profiles** - Add/remove configuration profiles to/from the device. These profiles are in addition to any group profiles applied to the device. See **Assign Configuration Profiles to Selected Devices** for more details.
- **Remote Control** - Take-over managed endpoints over a remote desktop connection. See **Remote Management of Windows and Mac OS Devices** for more details.

**Tip**: Customers using our legacy RMM product can connect to Windows endpoints using the RDP feature built into that product. See **https://help.comodo.com/topic-289-1-719-8539-Introduction-to-Remote-Monitoring-and-Management-Module.html** for more details.

- **File Transfer** - Use the remote control tool to manage Windows devices remotely. See **Remotely Manage Folders and Files on Windows Devices using Remote Control Tool** for more details.
- **Remote tools** - Explore files and folders on the managed Windows device. See **Remotely Browse Folders and Files on Windows Devices** for more details.
- **Run Procedure** - Execute script, patch and third-party application patch procedures on the device. See **Apply Procedures to Windows Devices** for more details.
- **Install or update MSI Packages** - Remotely install Comodo endpoint security software and third party Windows packages. See **Remotely Install and Update Packages on Windows Devices** for more details.
- **Refresh Device Information** - Contacts the device and updates system information. See **Update Device Information** for more details.
- **Reboot** - Remotely restart the device. See **Restart Selected Windows Devices** for more details.

- **Export Security Configurations** - Export the device's current CCS configuration as a profile. Exported profiles can be viewed under the **Exported CCS Configurations** tab. These can then be imported later as a Windows profile, potentially for deployment to other devices. See **Import Windows Profiles** for more details.
- **Delete Device** - Removes the device from Endpoint Manager. See **Remove a Device** for more details.
- **Change Owner** - Change the user with whom the device is associated. You can also change the type of device to corporate or personal. See **Change a Device's Owner** and **Change the Ownership Status of a Device** for more details.

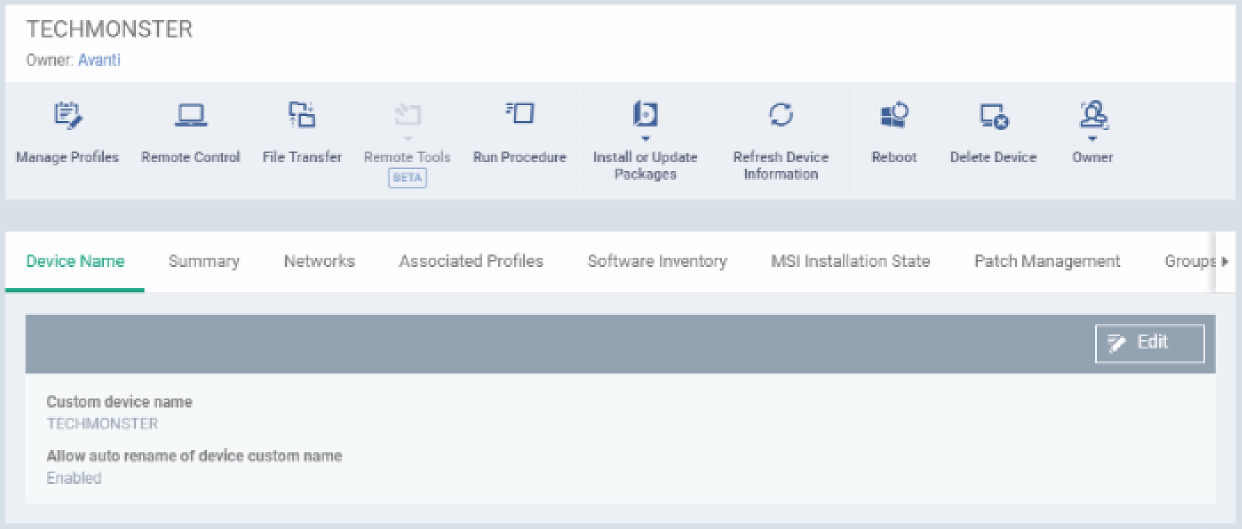
### 5.2.2.1. View and Edit Device Name

- Enrolled devices are listed by the name assigned to them by their owner. For example, 'Franks-PC'
- If no name was assigned then the manufacturer device name or model number is used.
- Custom Device Name - You can change the label of the device according to your preference. The custom name will apply in Endpoint Manager but will not change the name on the endpoint itself.
- Allow Auto Rename of Device Custom Name - If enabled, the custom name is replaced automatically by the actual device name during the next sync. Disable this option if you want to retain the custom name.

**Change a device name**

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

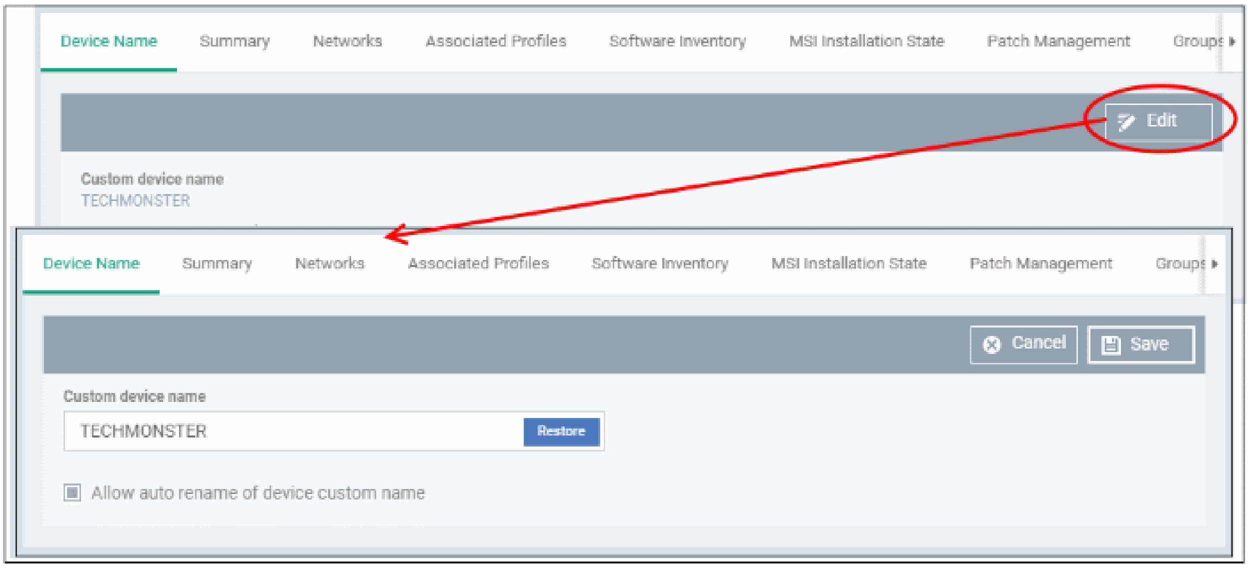
      Or
    - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Device Name' tab



Custom device name
TECHMONSTER

Allow auto rename of device custom name
Enabled

- Custom device name - The current name of the device.
- Allow auto rename of device custom name - Indicates whether the actual device name will automatically replace any custom name during the next sync.
- To change the name of the device, click the 'Edit' button at the right.



  - Enter the new name in the 'Custom Device Name' field
  - Make sure the 'Allow Auto Rename of Device Custom Name' is disabled to retain the custom name in the list. If this is enabled, the custom name will be automatically replaced with the device's name or model number during the next sync with the EM communication client on the device.
- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

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

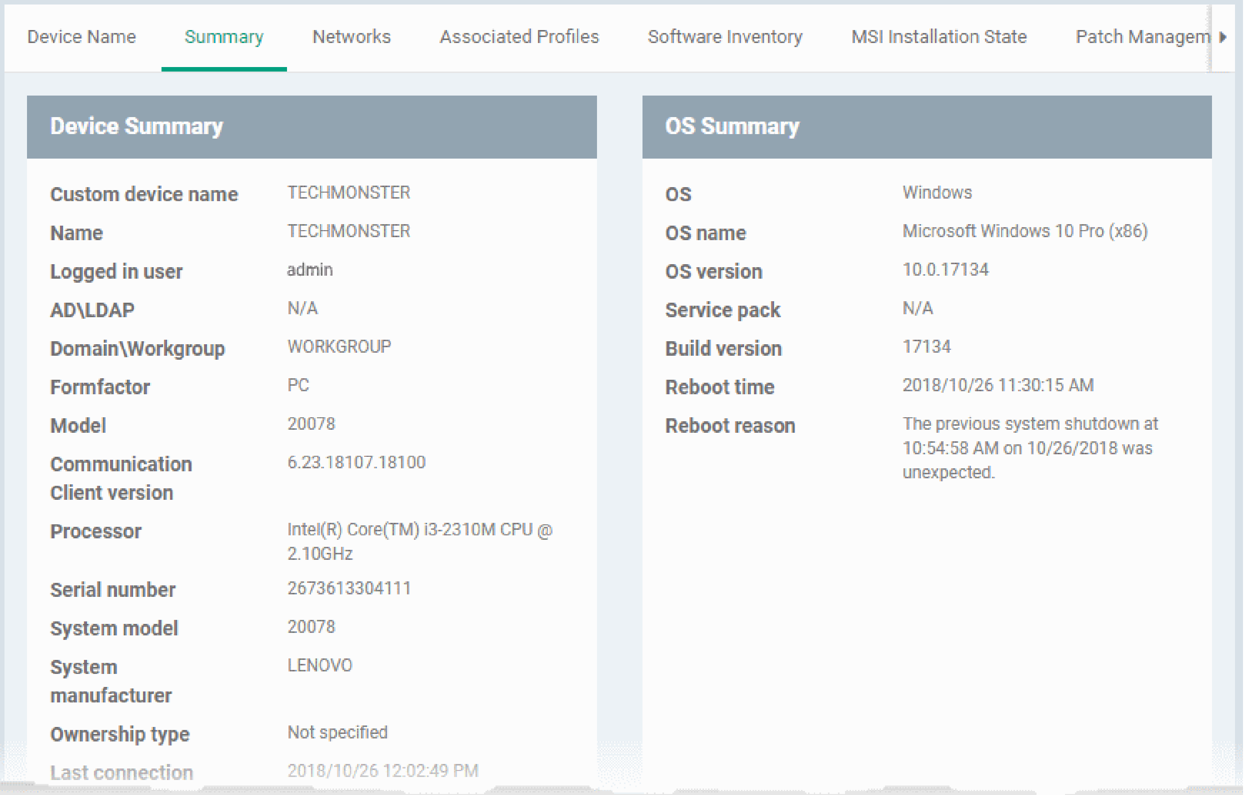
### 5.2.2.2. View Summary Information

The 'Summary' tab contains general device information, including operating system details, hardware details, last activity, CCS configuration and resource usage.

**To view the device summary**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view devices in that group

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click on the name of a Windows device then open the 'Summary' tab:



**Device Summary**

| | |
|---|---|
| Custom device name | TECHMONSTER |
| Name | TECHMONSTER |
| Logged in user | admin |
| AD\LDAP | N/A |
| Domain\Workgroup | WORKGROUP |
| Formfactor | PC |
| Model | 20078 |
| Communication Client version | 6.23.18107.18100 |
| Processor | Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz |
| Serial number | 2673613304111 |
| System model | 20078 |
| System manufacturer | LENOVO |
| Ownership type | Not specified |
| Last connection | 2018/10/26 12:02:49 PM |

**OS Summary**

| | |
|---|---|
| OS | Windows |
| OS name | Microsoft Windows 10 Pro (x86) |
| OS version | 10.0.17134 |
| Service pack | N/A |
| Build version | 17134 |
| Reboot time | 2018/10/26 11:30:15 AM |
| Reboot reason | The previous system shutdown at 10:54:58 AM on 10/26/2018 was unexpected. |

- **Device Summary -** Basic hardware, software, user and connection information. Includes device name, user, operating system, active directory domain, ownership type, IP address, local time zone and more.
- **OS Summary -** Detailed information about the device operating system. Includes OS build, service pack availability, last restart time, reason for last reboot and more.
- **Security Products Info -** Details about the Comodo security client installed on the endpoint. The security client provides the antivirus, firewall and containment services required to protect the device. Information in this section includes active security components, database update status, the amount of time remaining in baseline mode, and more.
- **Performance Metrics -** Current hardware resource usage on the device. Includes CPU, RAM , network and disk. The details are refreshed every 30 seconds.

### 5.2.2.3. View Hardware Information

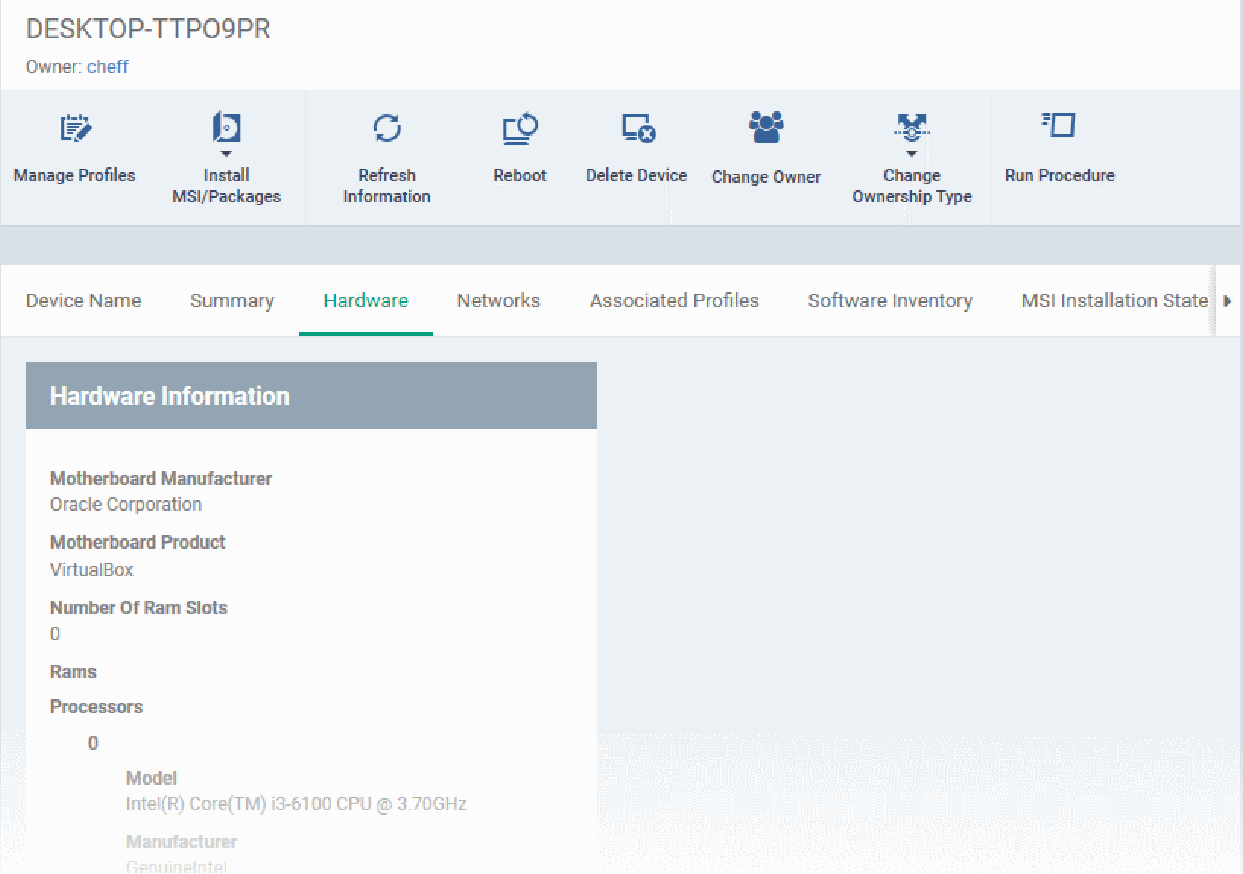
**Note**: This section is only available for devices that have the legacy Comodo RMM agent installed.

This screen contains basic details about a device's motherboard and hardware setup (RAM slots, processor type etc).

**To view a device's hardware details**

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

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Hardware' tab



DESKTOP-TTPO9PR

Owner: cheff

Hardware Information

Motherboard Manufacturer
Oracle Corporation

Motherboard Product
VirtualBox

Number Of Ram Slots
0

Rams

Processors

0

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

Manufacturer
GenuineIntel

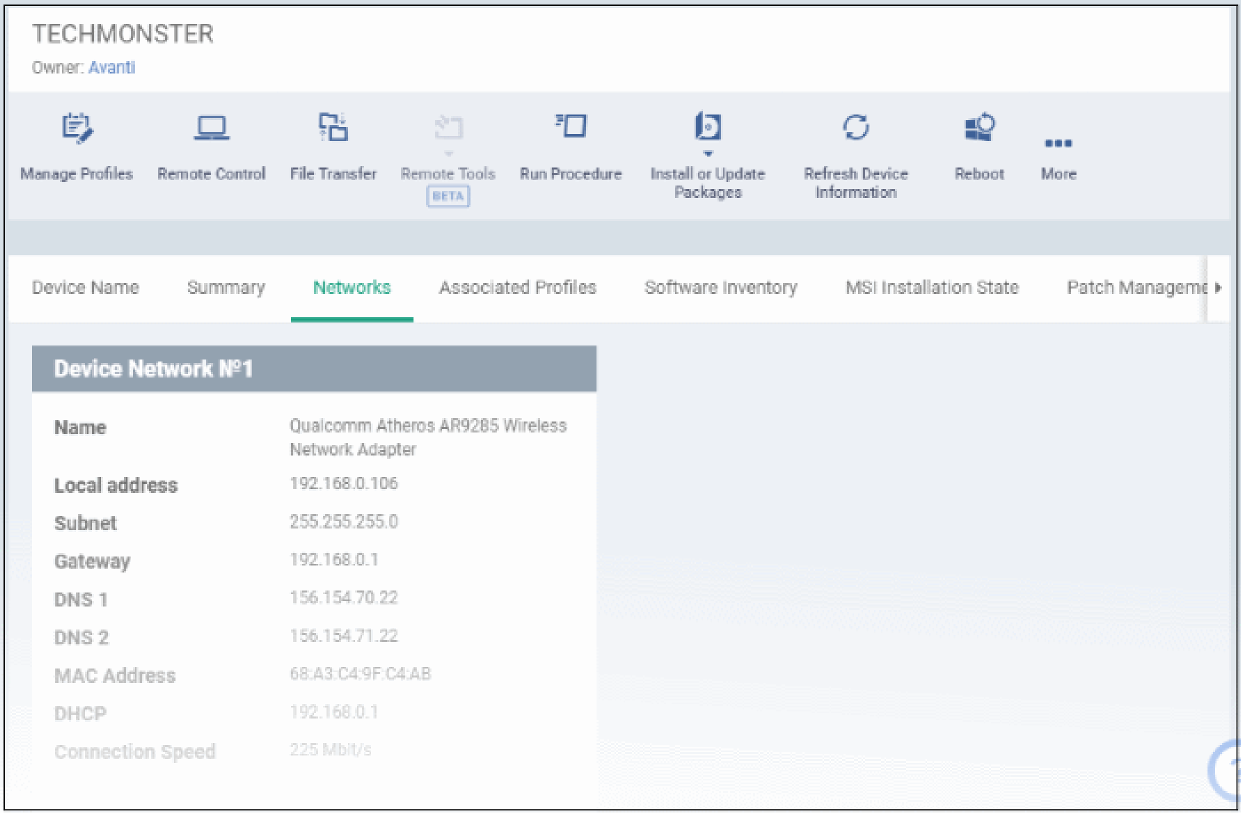
### 5.2.2.4. View Network Information

The 'Networks' screen shows details about the networks to which an endpoint is connected.

**View a device's network details**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view devices in that group

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Networks' tab



TECHMONSTER

Owner: Avanti

**Device Network №1**

| | |
|---|---|
| Name | Qualcomm Atheros AR9285 Wireless Network Adapter |
| Local address | 192.168.0.106 |
| Subnet | 255.255.255.0 |
| Gateway | 192.168.0.1 |
| DNS 1 | 156.154.70.22 |
| DNS 2 | 156.154.71.22 |
| MAC Address | 68:A3:C4:9F:C4:AB |
| DHCP | 192.168.0.1 |
| Connection Speed | 225 Mbit/s |

## 5.2.2.5. View Maintenance Windows Associated with Device

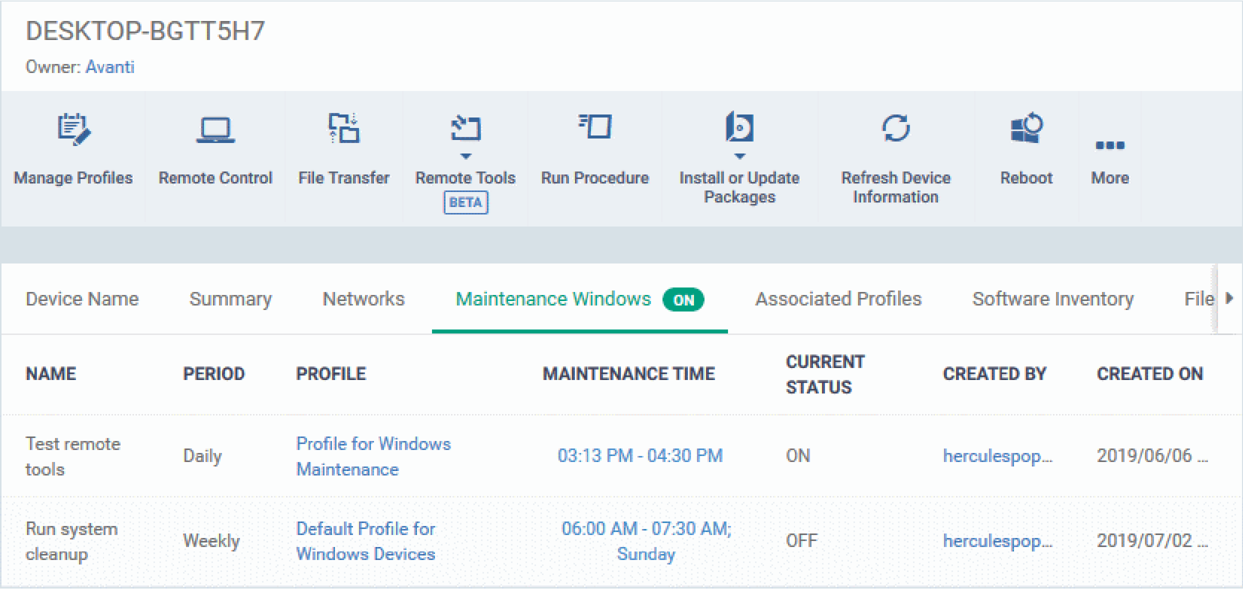
The maintenance windows tab lists all maintenance windows to which the device is assigned.

- A maintenance window is a scheduled time-slot when your Endpoint Manager procedures will run. A procedure is a task you want to run on your devices. For example, to patch all Windows endpoints.
- You create a maintenance window by adding a 'Maintenance Window' section to a Windows profile. You can then assign any procedures in the profile to the maintenance window.
- The procedures will run on all devices to which the profile is applied at the time set in the maintenance window.
- See **Maintenance Window Settings** for more help on this topic.

**View maintenance windows associated with a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
    - Select a company or a group to view the list of devices in that group

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Maintenance Windows' tab

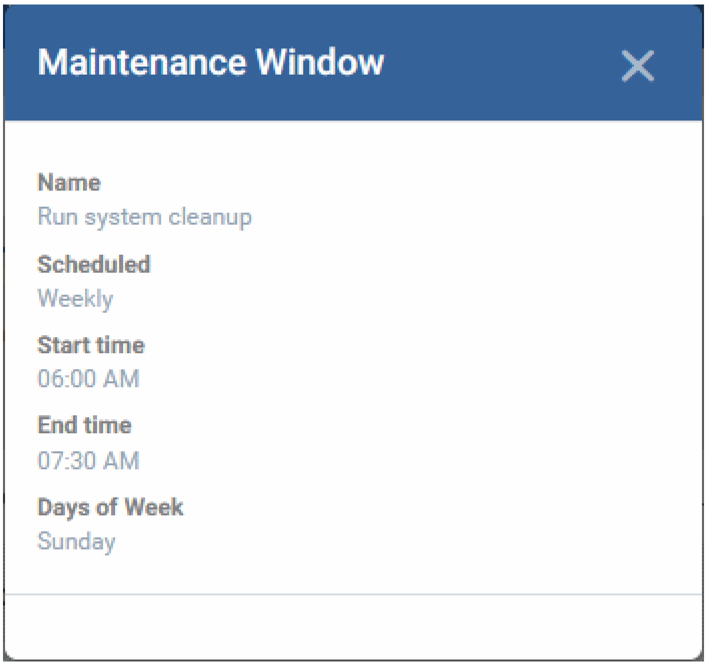


| NAME | PERIOD | PROFILE | MAINTENANCE TIME | CURRENT STATUS | CREATED BY | CREATED ON |
|---|---|---|---|---|---|---|
| Test remote tools | Daily | Profile for Windows Maintenance | 03:13 PM - 04:30 PM | ON | herculespop... | 2019/06/06 ... |
| Run system cleanup | Weekly | Default Profile for Windows Devices | 06:00 AM - 07:30 AM; Sunday | OFF | herculespop... | 2019/07/02 ... |

- A green 'On' icon means that the device is in at least one active maintenance window.
- As mentioned earlier, a maintenance window is a section in a configuration profile. The 'Profile' column shows you which profile(s) have maintenance windows which include this device.
- The 'Current Status' column shows you whether the maintenance window is active or not.

**Maintenance Windows - Column Descriptions**

| Column Heading | Description |
|---|---|
| Name | The label of the maintenance window.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Period | How often the maintenance window runs. |
| Profile | The profile to which the maintenance window belongs.<br>• Click profile name to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Maintenance Time | The time slot defined in the maintenance window<br>• Click the time slot to view the details of the maintenance window. An example is shown below: |

| | |
|---|---|
| |  Maintenance Window<br>Name<br>Run system cleanup<br>Scheduled<br>Weekly<br>Start time<br>06:00 AM<br>End time<br>07:30 AM<br>Days of Week<br>Sunday |
| Current Status | Whether or not the maintenance window is active. |
| Created by | The administrator who created the profile.<br>• Click the name of an administrator to view their user details. See **View the details of the User** for more details. |
| Created on | The date and time at which the profile was created. |

- Click any column header except 'Maintenance Time' and 'Current Status' to sort items in alphabetical or ascending/descending order.

### 5.2.2.6. View and Manage Profiles Associated with a Device

The 'Associated Profiles' tab lists all active configuration profiles on an endpoint. A profile may be applied to a device for any of the following reasons:

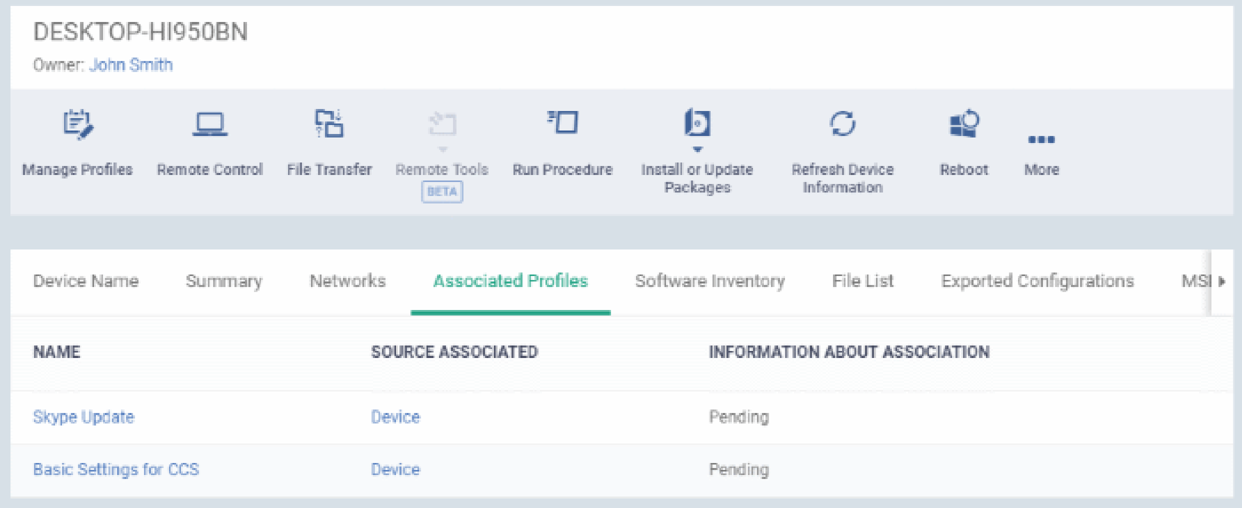
- Because it is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- The device belongs to a device group which has a group profile
- The user belongs to a user group which has a group profile

For more details on configuration profiles, see **Profiles for Windows Devices**.

**To view and manage the profiles associated with a device**

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

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Associated Profiles' tab


DESKTOP-HI950BN
Owner: John Smith

| NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSOCIATION |
|---|---|---|
| Skype Update | Device | Pending |
| Basic Settings for CCS | Device | Pending |

| Associated Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The profile label.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Source Associated | The source through which the profile was applied to the device. Configuration profiles can be applied to a device in different ways:<br>• Profiles can be directly applied to the device. See **Assign Configuration Profiles to Selected Devices** for more details<br>• Profiles applied to a user are deployed to all devices belonging to them. See **Assign Configuration Profile(s) to a User's Devices** for more details<br>• Profiles applied to a user group are deployed to all devices owned by group members. See **Assign Configuration Profile to a User Group** for more details<br>• Profiles applied to a device group are deployed to all member devices in the group. See **Assign Configuration Profile to a Device Groups** for more details<br>• Click a source to view its details interface. |
| Information about Association | The status of profile application to the device. |

- Click the 'Name' column header to sort the items in the alphabetical order of the names of the items

### Add or Remove Profiles

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

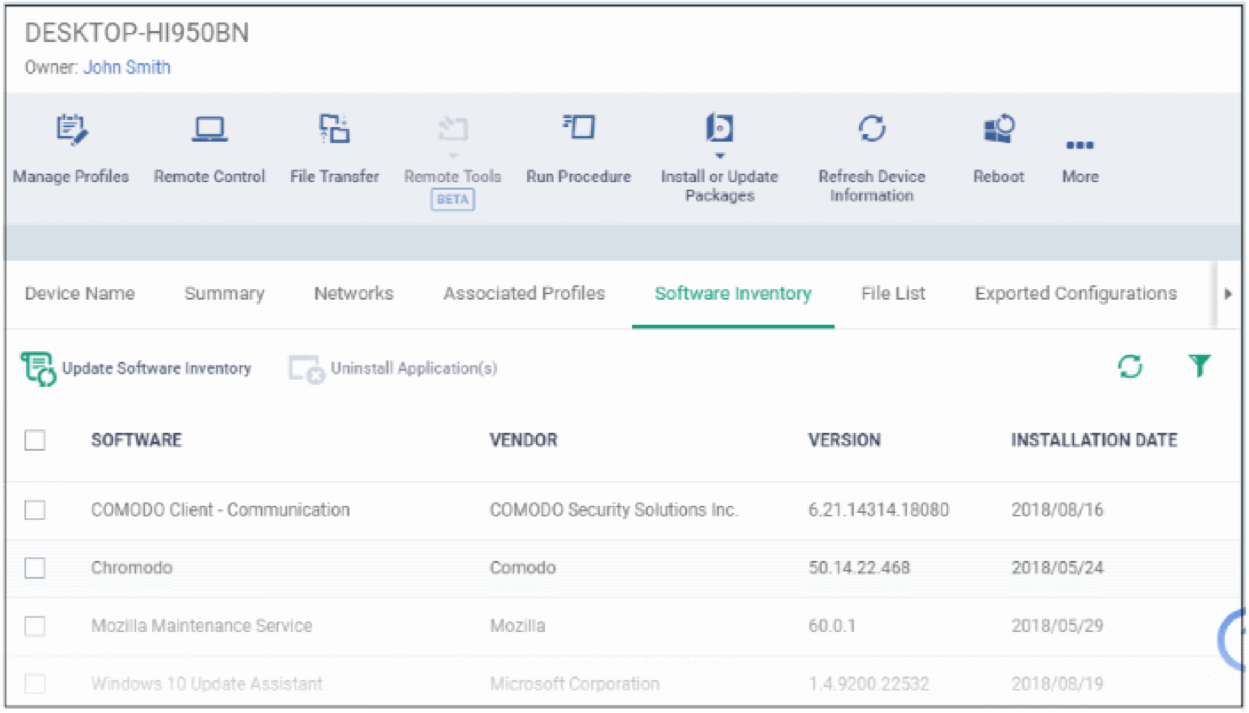
## 5.2.2.7. View and Manage Applications Installed on a Device

- The 'Software Inventory' is a list of all applications installed on a device.
- The interface also lets you remotely uninstall applications.

**To view applications installed on a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view devices in the group

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of a Windows device then select the 'Software Inventory' tab:



DESKTOP-HI950BN

Owner: John Smith

| SOFTWARE | VENDOR | VERSION | INSTALLATION DATE |
|---|---|---|---|
| COMODO Client - Communication | COMODO Security Solutions Inc. | 6.21.14314.18080 | 2018/08/16 |
| Chromodo | Comodo | 50.14.22.468 | 2018/05/24 |
| Mozilla Maintenance Service | Mozilla | 60.0.1 | 2018/05/29 |
| Windows 10 Update Assistant | Microsoft Corporation | 1.4.9200.22532 | 2018/08/19 |

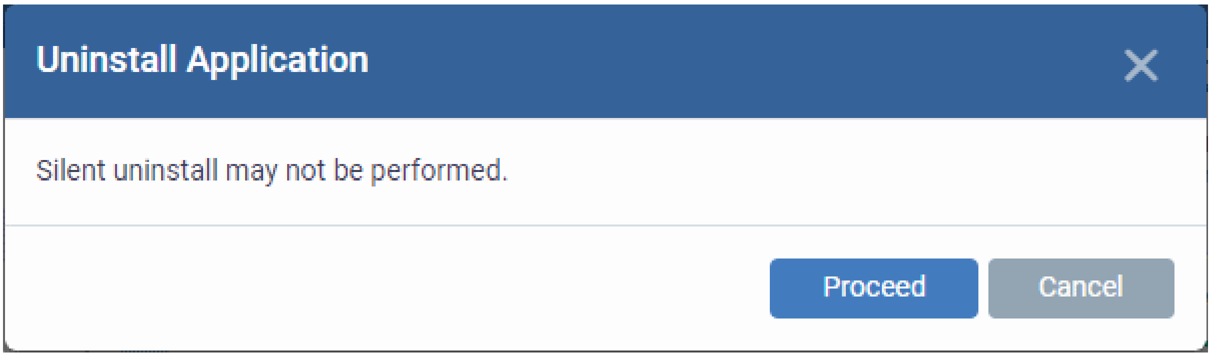
| Installed Apps - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Software | The name of the application. |
| Vendor | The publisher of the application. |
| Version | The version number of the application. |
| Installation Date | The date at which the application was installed on the device. |

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

## Remotely uninstall applications

Supported 3rd party applications can be remotely uninstalled from the Endpoint Manager. See **EM Supported 3rd Party Applications** for a full list.

- Select an application in the list
- Click 'Uninstall Selected Application'
- An uninstall command will be sent to the device.
- You will see the following message if the software cannot be uninstalled without notifying the device user:



Uninstall Application

Silent uninstall may not be performed.

- Click 'Proceed' to continue with the uninstall.

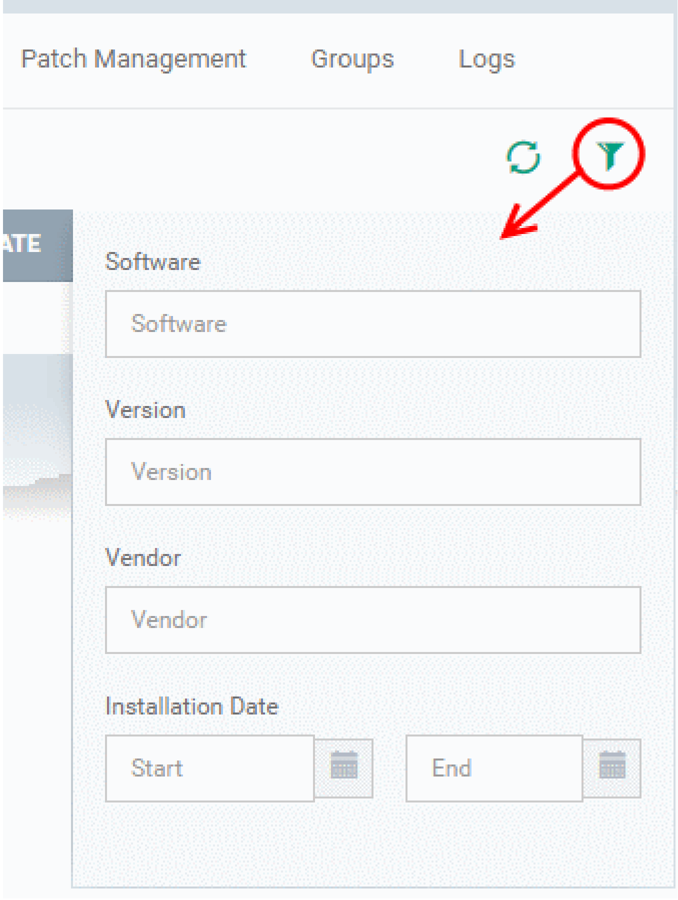
The application will be uninstalled from the selected device.

**Tip:**

- You can uninstall an application from *selected or all* Windows devices from the 'Global Software Inventory'.
- Click 'Applications' > 'Global Software Inventory' to access this area.
- See **View and Manage Applications Installed on Windows Devices** if you need more help with this.

## Sorting, Search and Filter Options

- Click the 'Software', 'Vendor' and 'Version' column headers to sort items in alphabetical or ascending/descending order
- Click the funnel button on the right to open filter options



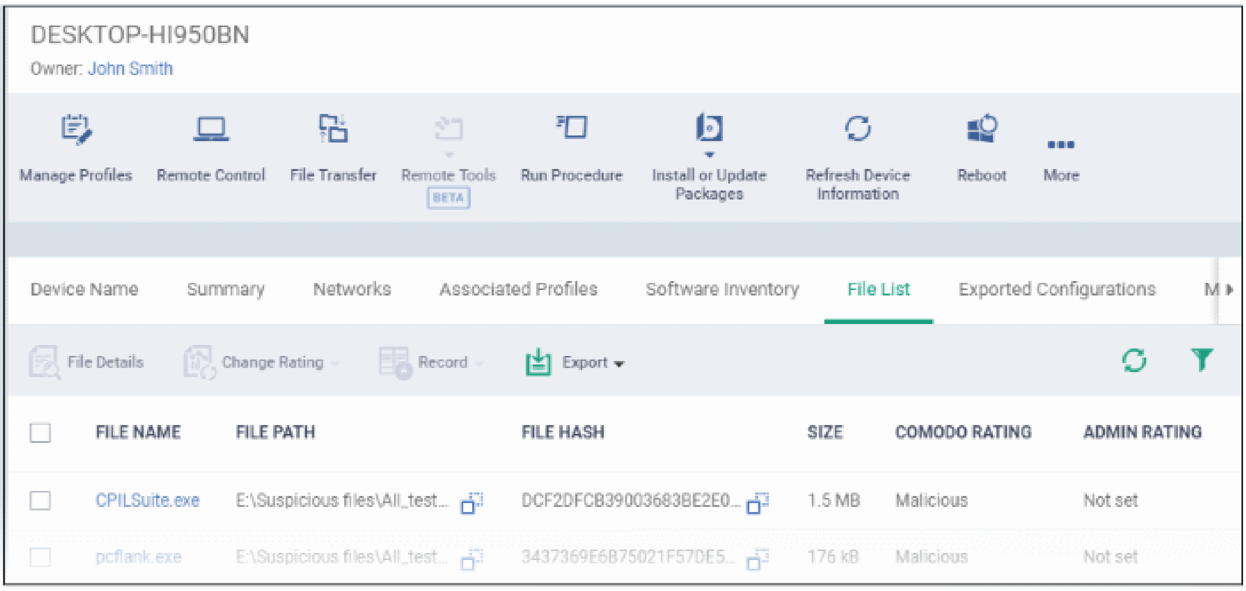
- Type search criteria in the search fields to find an application based on name, version and/or vendor.
- Enter 'Start' and 'End' dates to search for applications installed during a certain period of time.
- Click 'Apply' to run your filter
- To display all items again, remove all search terms and click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

### 5.2.2.8. View the Files on a Device

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

**View files on a Windows device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices
      Or
    - Select 'Show all' on the left to view every device enrolled to EM
- Click the name of a Windows device then select the 'File List' tab:



DESKTOP-HI950BN
Owner: John Smith

| □ | FILE NAME | FILE PATH | FILE HASH | SIZE | COMODO RATING | ADMIN RATING |
|---|---|---|---|---|---|---|
| □ | CPILSuite.exe | E:\Suspicious files\All_test... | DCF2DFCB39003683BE2E0... | 1.5 MB | Malicious | Not set |
| □ | pcflank.exe | E:\Suspicious files\All_test... | 3437369E6B75021F57DE5... | 176 kB | Malicious | Not set |

| File List - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| File Name | The label of the executable file or application. |
| File Path | The installation location of the application at the endpoint.<br>• Click the ⧉ icon to copy the path to the clipboard. |
| File Hash | The SHA1 hash value of the executable file.<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Size | The size of the executable file. |
| Comodo Rating | The trust rating of the file as per the Comodo File Look-up service, reported by the CCS installations at the endpoints |

| | |
|---|---|
| Admin Rating | The trust rating of the file as manually set by the administrator, if any. |

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

## Unrecognized Files

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

- The rating you set is purely a local trust rating for the file. It does not affect the global rating set by Comodo.
- The 'Valkyrie' section of a profile lets you auto-upload unknown files to the cloud for behavior analysis. See **Valkyrie Settings** for more details

**Background Note**: Valkyrie is a file verdicting service that tests unknown files with a range of static and dynamic checks. The results of these tests produce a trust verdict on the file. This verdict can be viewed in the 'Windows File List' > 'Valkyrie Processed Files' tab. See **View List of Valkyrie Analyzed Files** for more details.

## Trusted Files

Files are identified as trusted in the following ways:

- **Cloud-based file lookup service (FLS) -** Whenever a file is accessed, Comodo Client Security (CCS) checks the file's reputation on Comodo's online file database. It also consults the local list of trusted vendors.

  The file is classed as trusted if:

  - The app is from a vendor with a 'Trusted' status in the local vendor list in CCS
  - The app trusted is on Comodo's online file database (aka, it is whitelisted)

- **Admin rating -** Admins can assign a 'Trusted' rating to files from the Application Control interface

- **User Rating -** Users can assign a 'Trusted' rating to files at the local CCS installation in two ways:

  - In response to an alert. If an executable is unknown then it may generate a HIPS alert on the local endpoint. Users could choose 'Treat this as a Trusted Application' at the alert
  - The user can assign 'Trusted' rating to any file from the 'File List' interface.

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

## Malicious Files

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

## The File List screen

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

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

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

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

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

## Sorting, Search and Filter Options

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

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

## Manage Applications

The 'File List' interface allows you to:

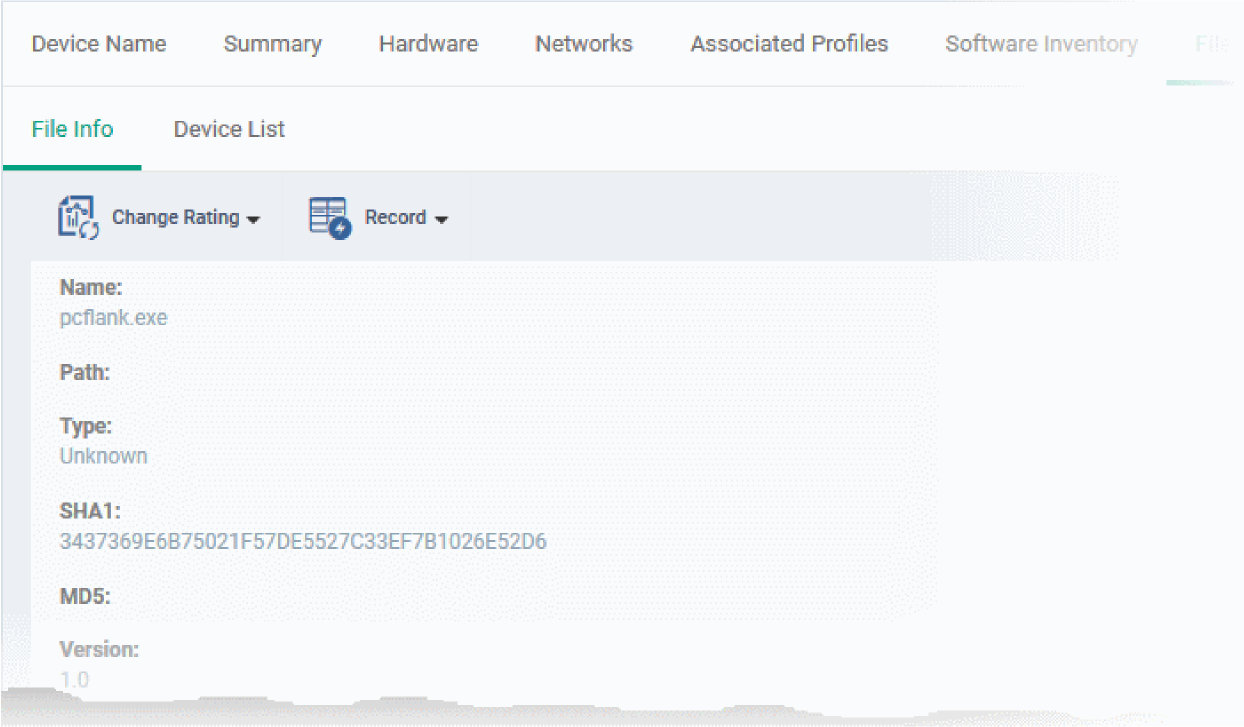
- **View the details of files in the list**
- **View Process Activities of a File**
- **Assign Admin rating to a file**
- **Hide/Display selected files in the list**
- **Export the list of selected files to a CSV file**
- **Remove files from the list**

## View file details

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

## File info

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



Name:
pcflank.exe

Path:

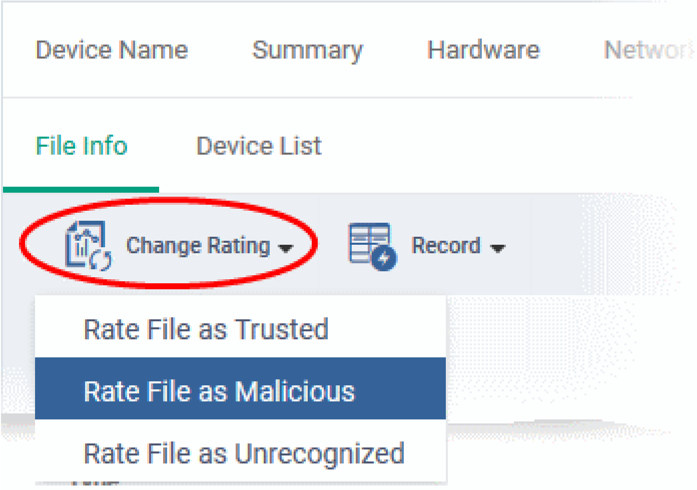
Type:
Unknown

SHA1:
3437369E6B75021F57DE5527C33EF7B1026E52D6

MD5:

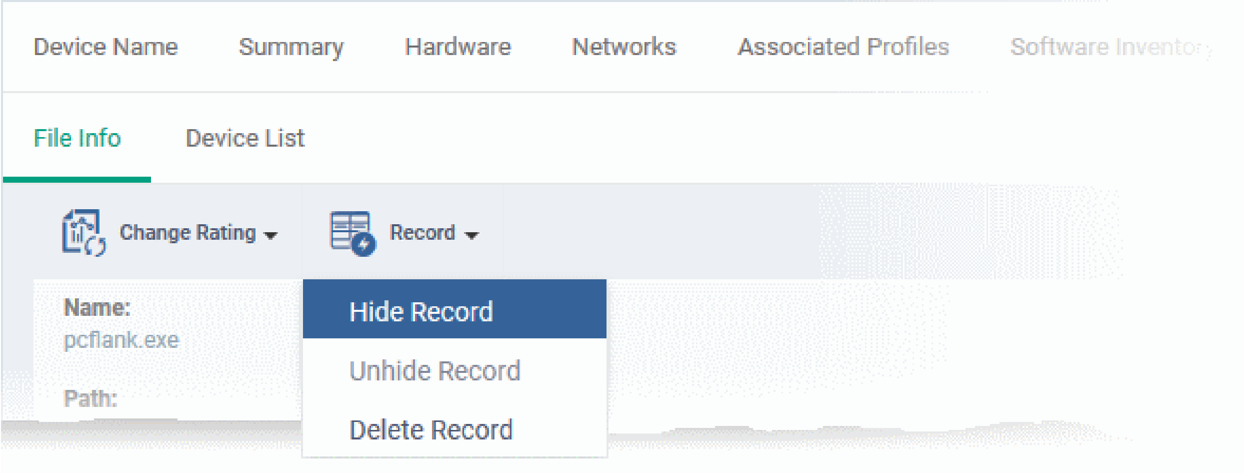
Version:
1.0

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



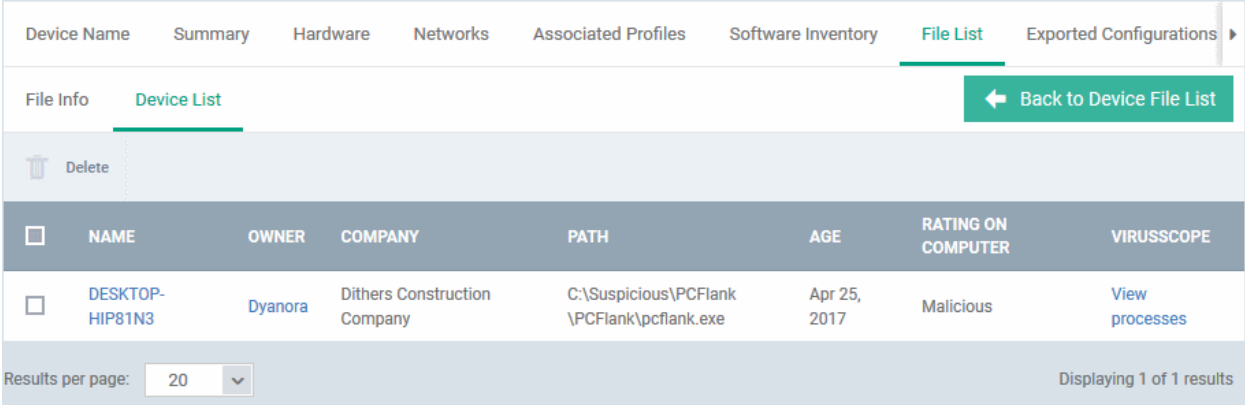
The new rating will be sent to all endpoints.

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



## Device List Screen

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



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

Results per page: 20

Displaying 1 of 1 results

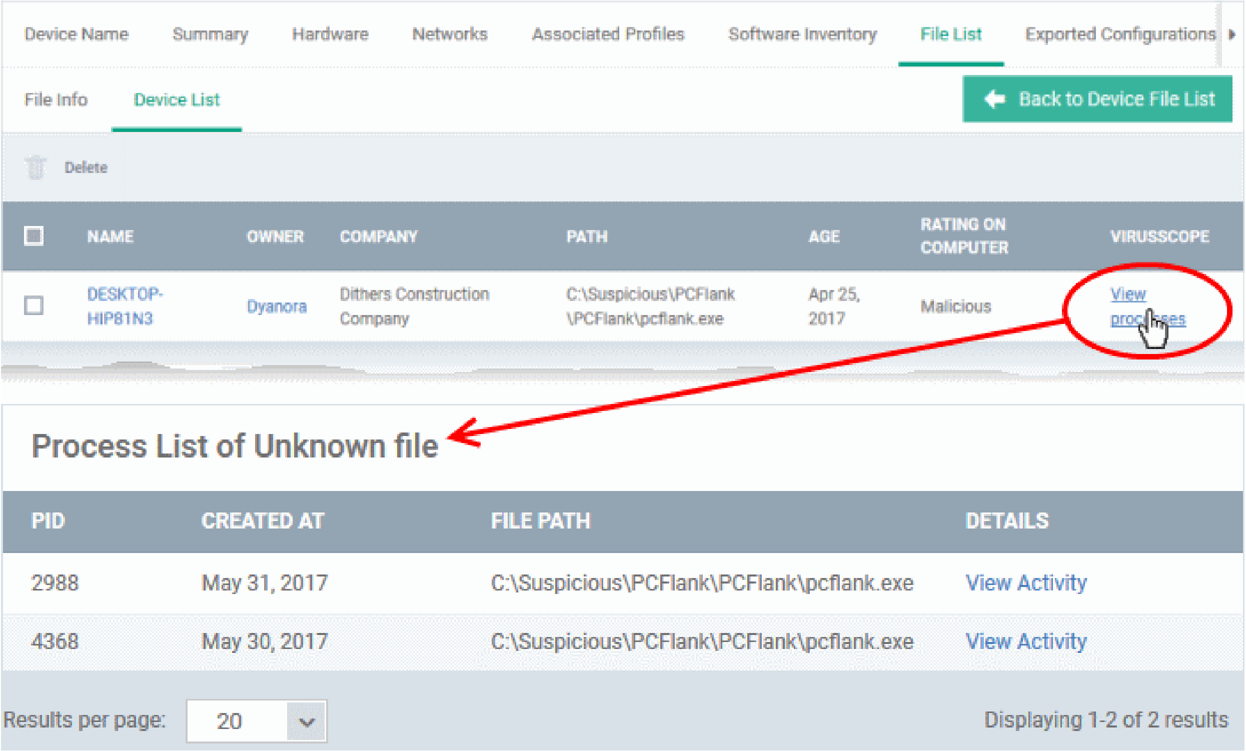
- You can remove the file from device(s) by selecting a device then clicking 'Delete'

## View Process Activities of a File

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

### To view the activities of a file on the endpoint

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



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

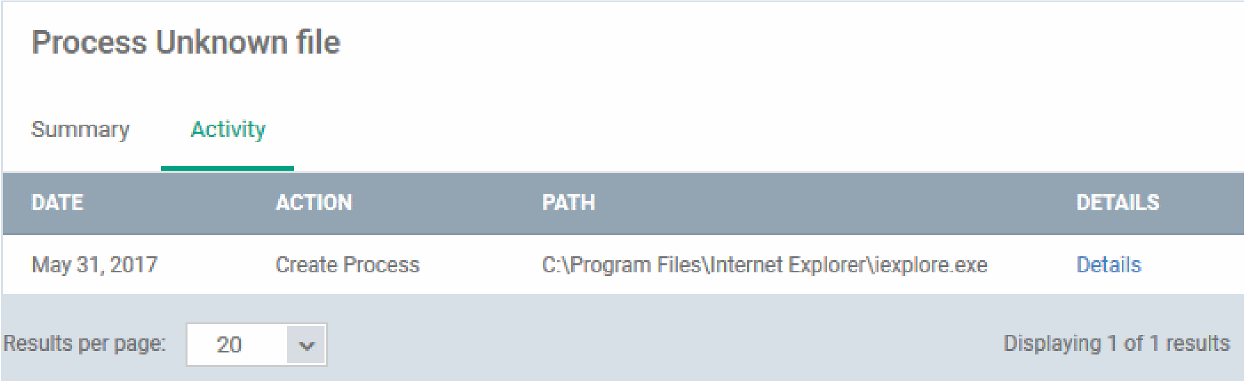
Process List of Unknown file

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

Results per page: 20

Displaying 1-2 of 2 results

- Click 'View Activity' to see detailed information about each process. The 'Process Activity' interface has two tabs:
  - **Summary -** Displays the name of the device and the installation path of the executable
  - **Activity -** Displays a chronological list of activities by the selected process, including details of files modified by the process.


Process Unknown file

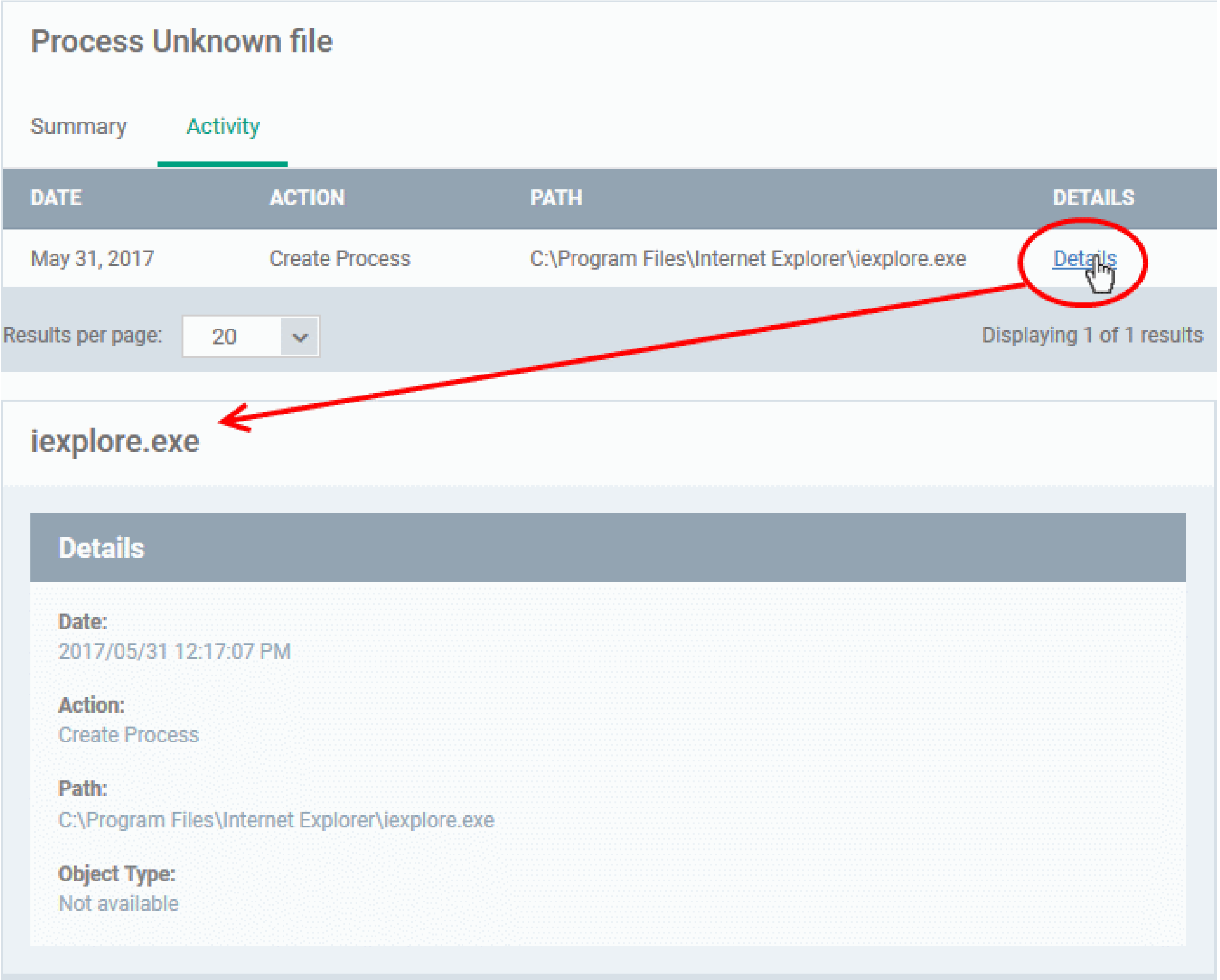
| DATE | ACTION | PATH | DETAILS |
|---|---|---|---|
| May 31, 2017 | Create Process | C:\Program Files\Internet Explorer\iexplore.exe | Details |

Results per page: 20

Displaying 1 of 1 results

| The 'Activity' - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Date | The date and time of process execution |
| Action | The task executed by the process on the target file |
| Path | The location of the target file |
| Details | A link to view more information about the action |

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



Process Unknown file

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

iexplore.exe

Details

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

Action:
Create Process

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

Object Type:
Not available

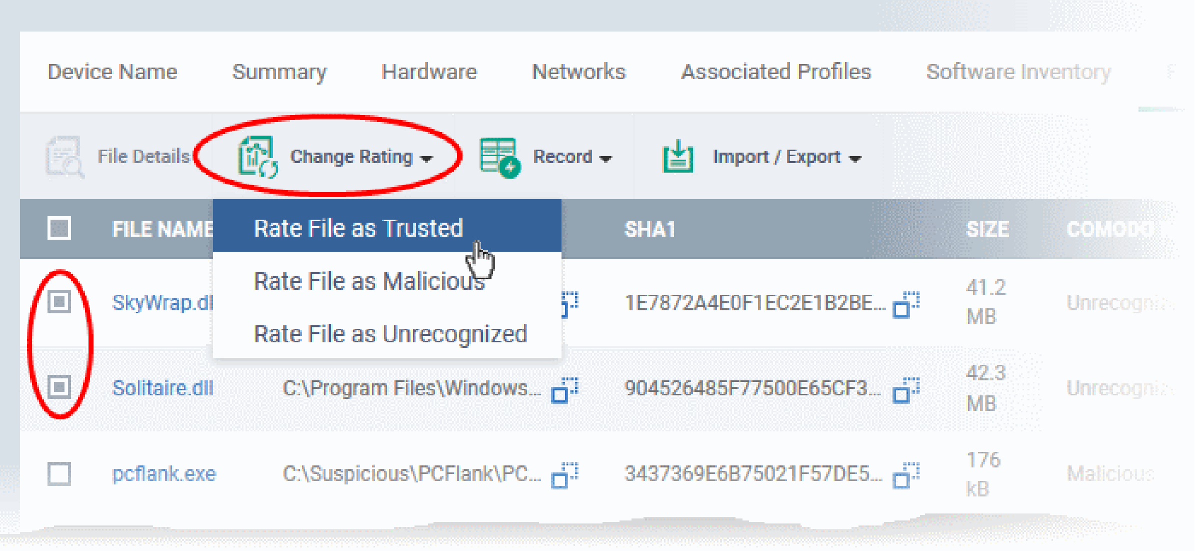
## Assign Admin Rating to a File

- Each file on an endpoint is automatically scanned and assigned a trust rating by Comodo Client Security.
- These ratings can be either '**Unrecognized**', '**Trusted**' or '**Malicious**'. The rating for each file is shown in the 'Comodo Rating' column of the 'File List' screen.
- The file rating determines whether or how the file is allowed to run:
  - **Trusted -** The file will be allowed to run normally. It will, of course, still be subject to the standard protection mechanisms of Comodo Client Security (behavior monitoring, host intrusion prevention etc).
  - **Malicious -** The file will not be allowed to run. It will be automatically quarantined or deleted depending on admin preferences.
  - **Unknown -** The file will be run inside the container. The container is a virtual operating environment which is isolated from the rest of the endpoint. Files in the container write to a virtual file system, use a virtual registry and cannot access user or operating system data.
- Automatic file rating can be configured in the 'File Rating' section of the configuration profile active on the endpoint. See **File Rating settings** in **Creating a Windows Profile** for more details.
- Click 'Change Rating' in the 'File List' interface to manually set a rating for a selected file or files. The new rating will be propagated to all endpoints and will determine the file's run-time privileges. Admin assigned ratings will be shown in the 'Admin Rating' column of the interface:

### To assign a file rating to a file

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

- Choose the rating you want to from the drop-down:

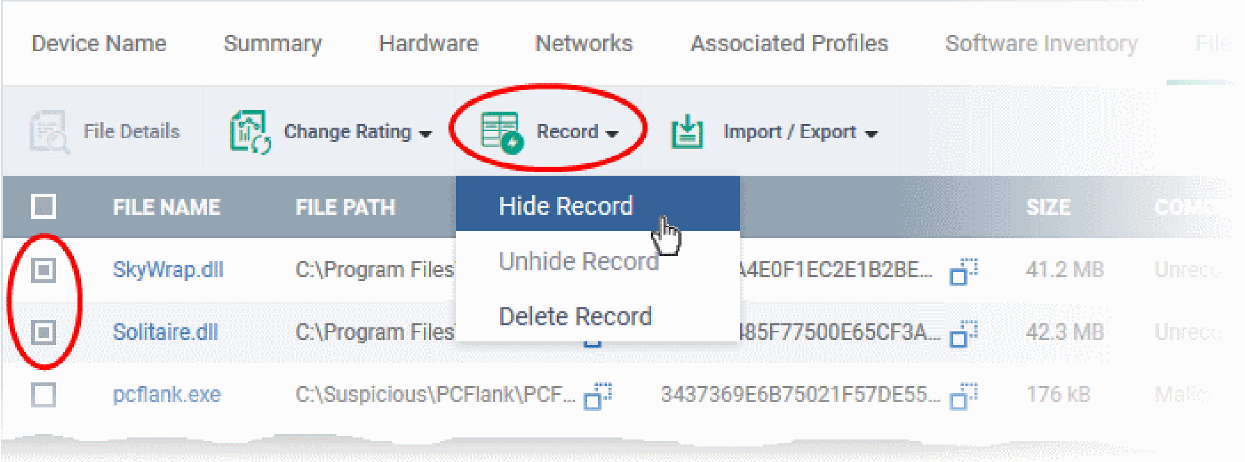


| ☐ | FILE NAME | | SHA1 | SIZE | COMODO |
|---|---|---|---|---|---|
| ☒ | SkyWrap.dl | | 1E7872A4E0F1EC2E1B2BE... | 41.2 MB | Unrecogni |
| ☒ | Solitaire.dll | C:\Program Files\Windows... | 904526485F77500E65CF3... | 42.3 MB | Unrecogni |
| ☐ | pcflank.exe | C:\Suspicious\PCFlank\PC... | 3437369E6B75021F57DE5...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

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

## Hide/Display Selected Files

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

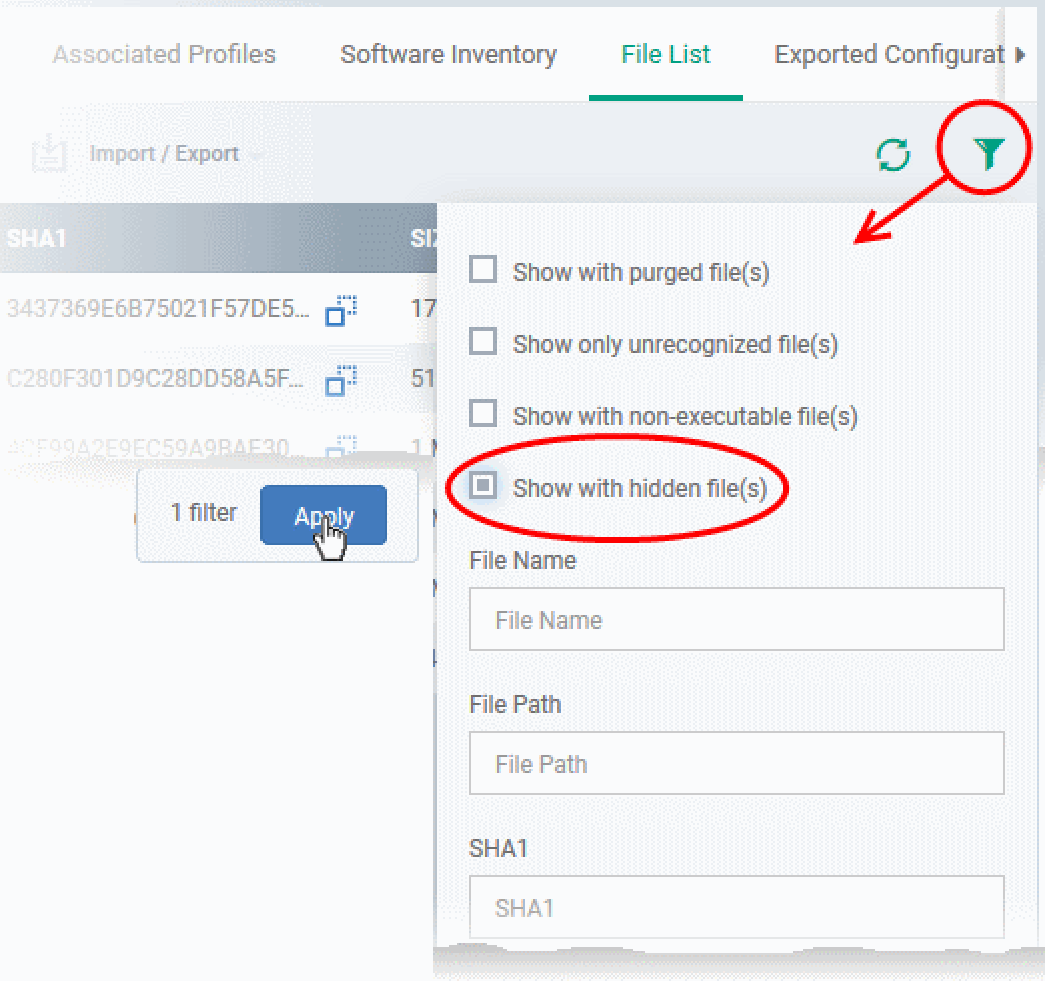


| ☐ | FILE NAME | FILE PATH | | SIZE | COM |
|---|---|---|---|---|---|
| ☒ | SkyWrap.dll | C:\Program Files | 4E0F1EC2E1B2BE... | 41.2 MB | Unrec |
| ☒ | Solitaire.dll | C:\Program Files | 85F77500E65CF3A... | 42.3 MB | Unrec |
| ☐ | pcflank.exe | C:\Suspicious\PCFlank\PCF... | 3437369E6B75021F57DE55...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

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

**To view hidden files**

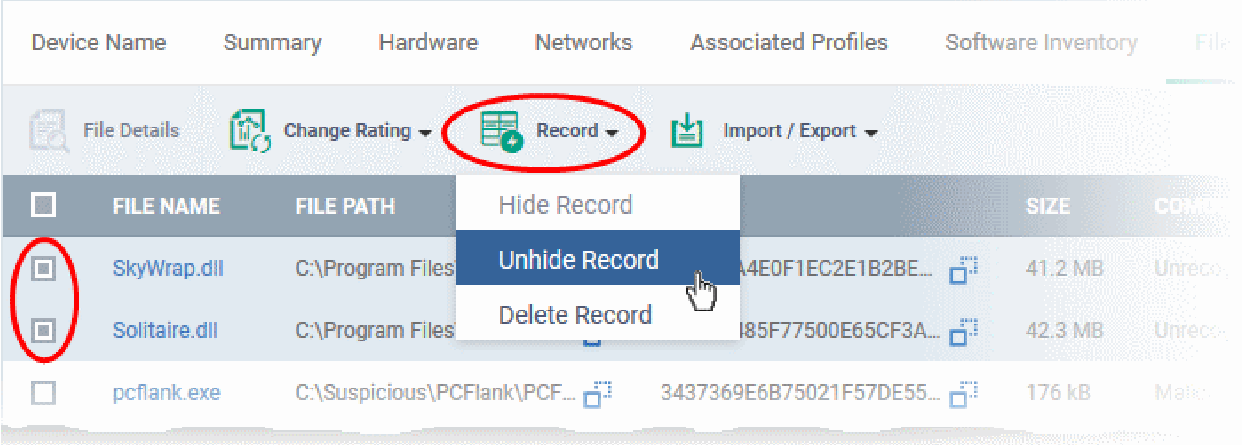
- Click the funnel icon at the top-right to open the filter options
- Select 'Show with hidden file(s)' and click 'Apply'



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

**To restore hidden files**

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

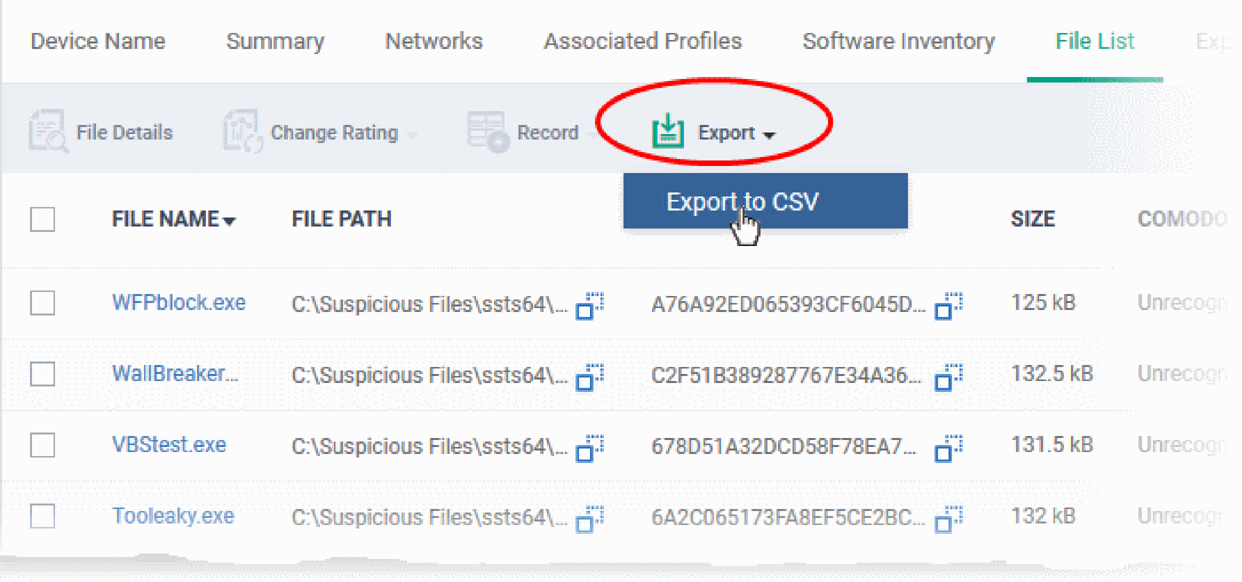


The files will be displayed in the permanently.

## Export the List of Files

You can export the 'File List' to a comma-separated values (CSV) file as follows:

- Click the 'Export' button above the table then choose 'Export to CSV':



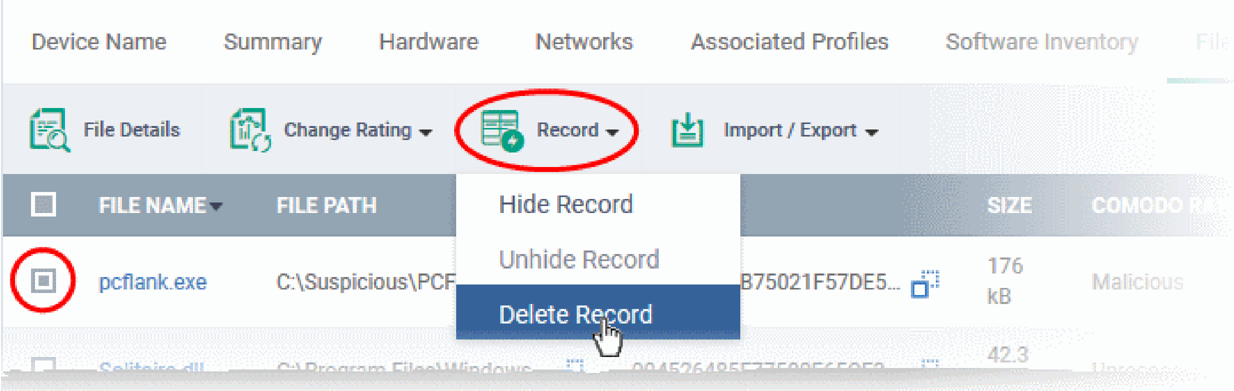
| □ | FILE NAME | FILE PATH | | SIZE | COMODO |
|---|---|---|---|---|---|
| □ | WFPblock.exe | C:\Suspicious Files\ssts64\... | A76A92ED065393CF6045D... | 125 kB | Unrecogr |
| □ | WallBreaker... | C:\Suspicious Files\ssts64\... | C2F51B389287767E34A36... | 132.5 kB | Unrecogr |
| □ | VBStest.exe | C:\Suspicious Files\ssts64\... | 678D51A32DCD58F78EA7... | 131.5 kB | Unrecogr |
| □ | Tooleaky.exe | C:\Suspicious Files\ssts64\... | 6A2C065173FA8EF5CE2BC... | 132 kB | Unrecogr |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Remove files from the list

You can remove items you no longer wish to see in 'File List' screen. Deleted files will only be removed from the list. They will remain on the endpoints themselves.

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



| □ | FILE NAME | FILE PATH | | SIZE | COMODO RA |
|---|---|---|---|---|---|
| ☒ | pcflank.exe | C:\Suspicious\PCF | B75021F57DE5... | 176 kB | Malicious |

## 5.2.2.9. View Exported Configurations and Import Profiles

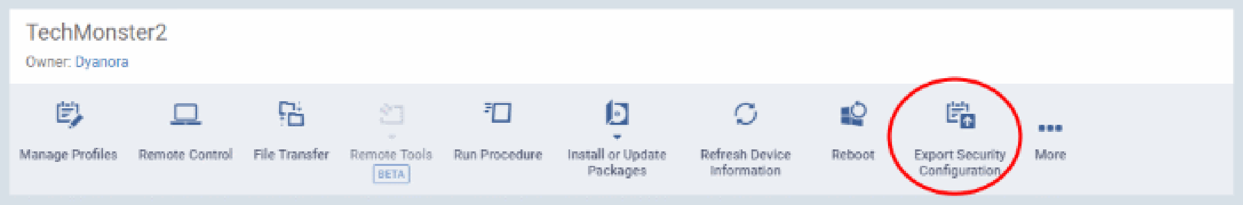
- You can create a new Windows profile out of the CCS configuration on an endpoint.
- This is useful if you want to copy the configuration of an endpoint to multiple other endpoints

**To export a CCS configuration**

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

    Or

  - Select 'Show all' on the left to view every device enrolled to EM
- Click on the Windows device whose configuration you wish to export to open its 'Device Details' interface
- Click the 'Export Security Configuration' button at the top.



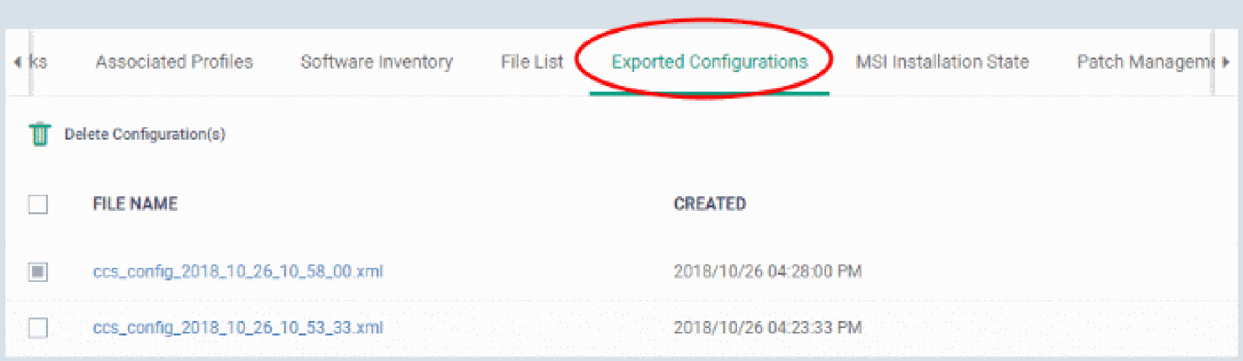
The CCS configuration will be exported as an .xml file with date/time stamp suffix in the file name. The profile will be saved on the EM server and can be viewed by clicking the 'Exported Configurations' tab of the device details interface of the same device.

**To view and manage exported profiles**

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

    Or

  - Select 'Show all' on the left to view every device enrolled to EM
- Click the name of a Windows device then select the 'Exported Configurations' tab:



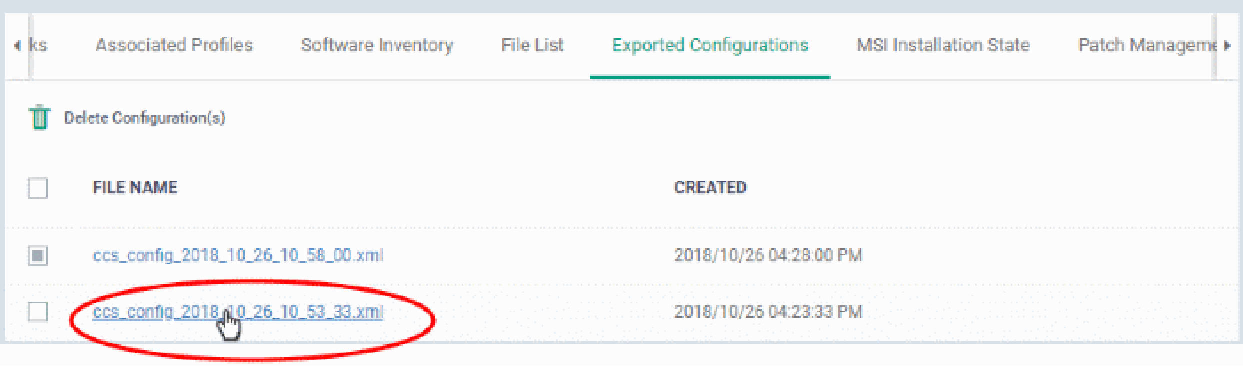
| □ | FILE NAME | CREATED |
|---|---|---|
| ☒ | ccs_config_2018_10_26_10_58_00.xml | 2018/10/26 04:28:00 PM |
| □ | ccs_config_2018_10_26_10_53_33.xml | 2018/10/26 04:23:33 PM |

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

- Click any column header to sort items in alphabetic or ascending/descending order

**To import and save the security configuration**

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

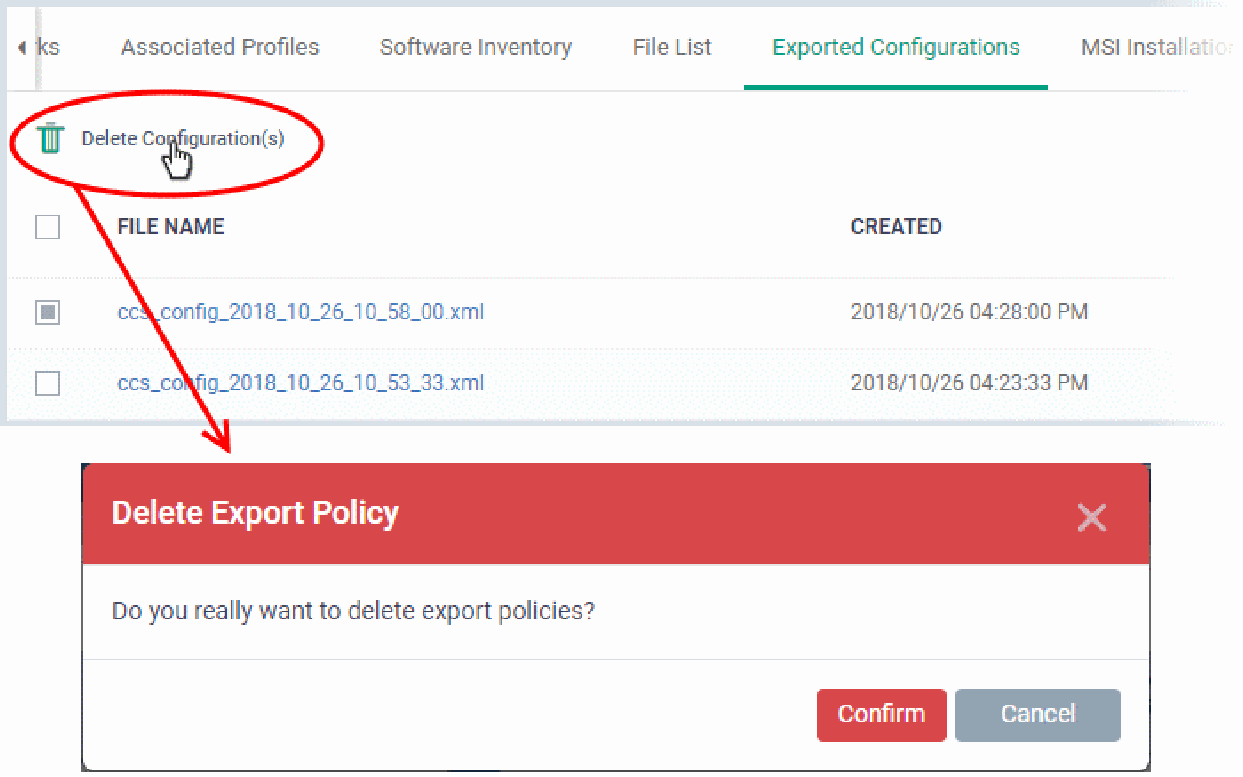


| ☐ | FILE NAME | CREATED |
|---|---|---|
| ☑ | ccs_config_2018_10_26_10_58_00.xml | 2018/10/26 04:28:00 PM |
| ☐ | ccs_config_2018_10_26_10_53_33.xml | 2018/10/26 04:23:33 PM |

The file will be imported as an .xml file.

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

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



| ☐ | FILE NAME | CREATED |
|---|---|---|
| ☑ | ccs_config_2018_10_26_10_58_00.xml | 2018/10/26 04:28:00 PM |
| ☐ | ccs_config_2018_10_26_10_53_33.xml | 2018/10/26 04:23:33 PM |

Delete Export Policy

Do you really want to delete export policies?

### 5.2.2.10. View MSI Files Installed on a Device through Endpoint Manager

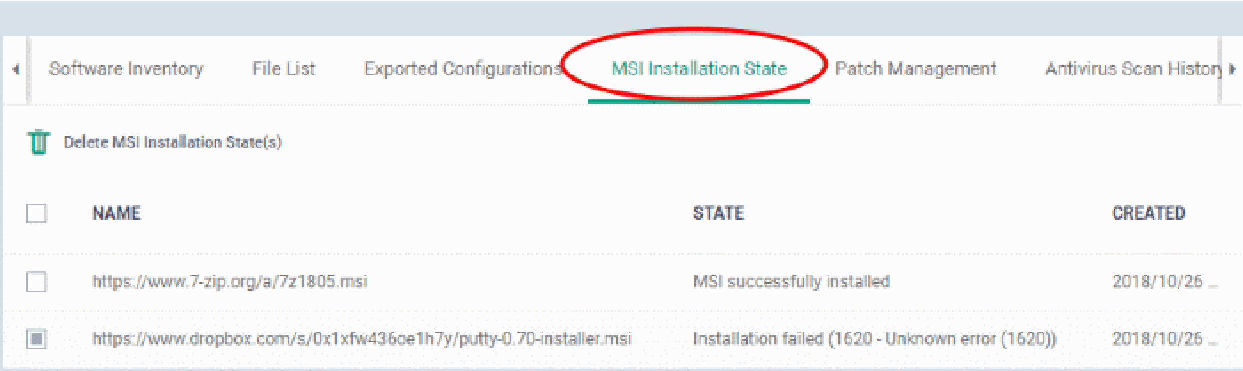
- You can remotely install Endpoint Manager packages onto managed endpoints.
- These may be Comodo applications or third-party MSI packages. See **Remotely Install and Update Packages on Windows Devices** if you want to know more about this process.

**To view MSI file installation list on the device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab then
  - Select a company or a group to view only their devices

    Or

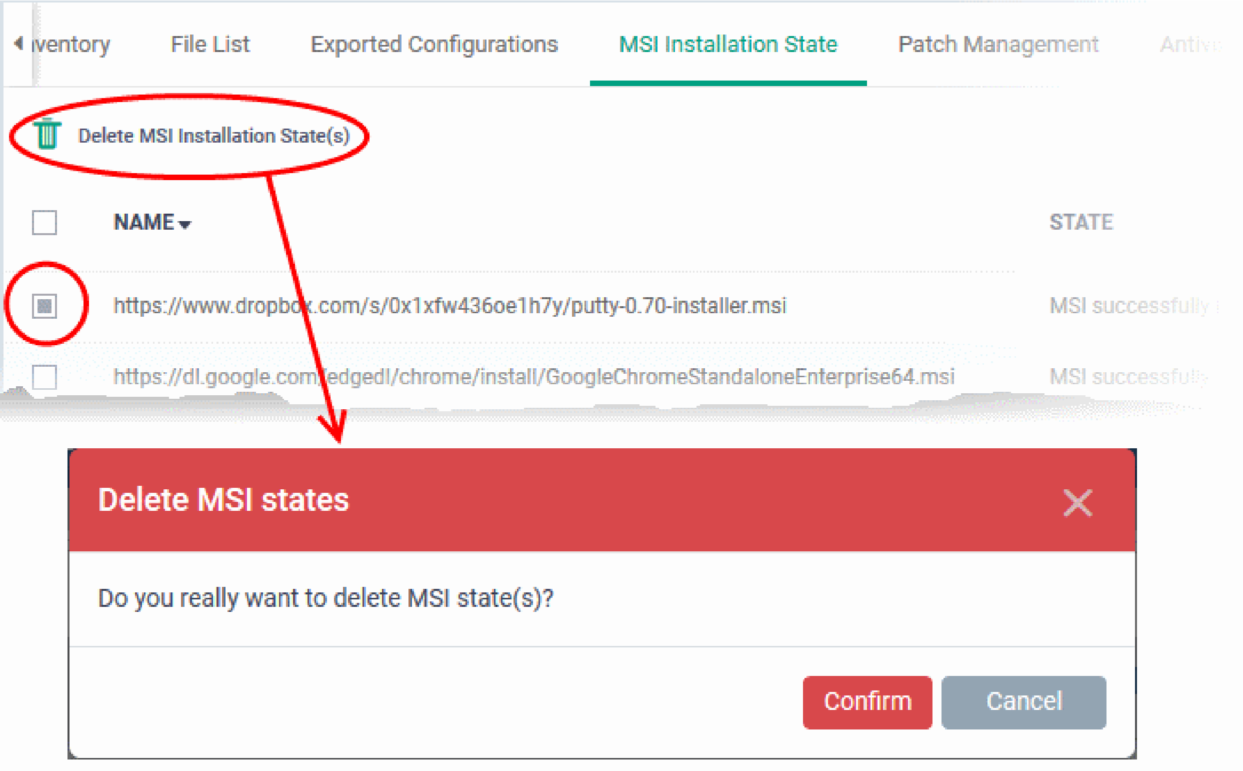
- Select 'Show all' to view every device added to EM
- Click on the name of a Windows device then select the 'MSI Installation State' tab:



| ☐ | NAME | STATE | CREATED |
|---|---|---|---|
| ☐ | https://www.7-zip.org/a/7z1805.msi | MSI successfully installed | 2018/10/26 ... |
| ■ | https://www.dropbox.com/s/0x1xfw436oe1h7y/putty-0.70-installer.msi | Installation failed (1620 - Unknown error (1620)) | 2018/10/26 ... |

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

- Click any column header to sort items in alphabetic or ascending/descending order
- To delete an entry from the list, select it and click 'Delete MSI Installation State(s)'.


ventory
File List
Exported Configurations
MSI Installation State
Patch Management
Antiv
Delete MSI Installation State(s)
NAME
STATE
https://www.dropbox.com/s/0x1xfw436oe1h7y/putty-0.70-installer.msi
MSI successfully i
https://dl.google.com/edgedl/chrome/install/GoogleChromeStandaloneEnterprise64.msi
MSI successfully
Delete MSI states
Confirm
Cancel

Do you really want to delete MSI state(s)?

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

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

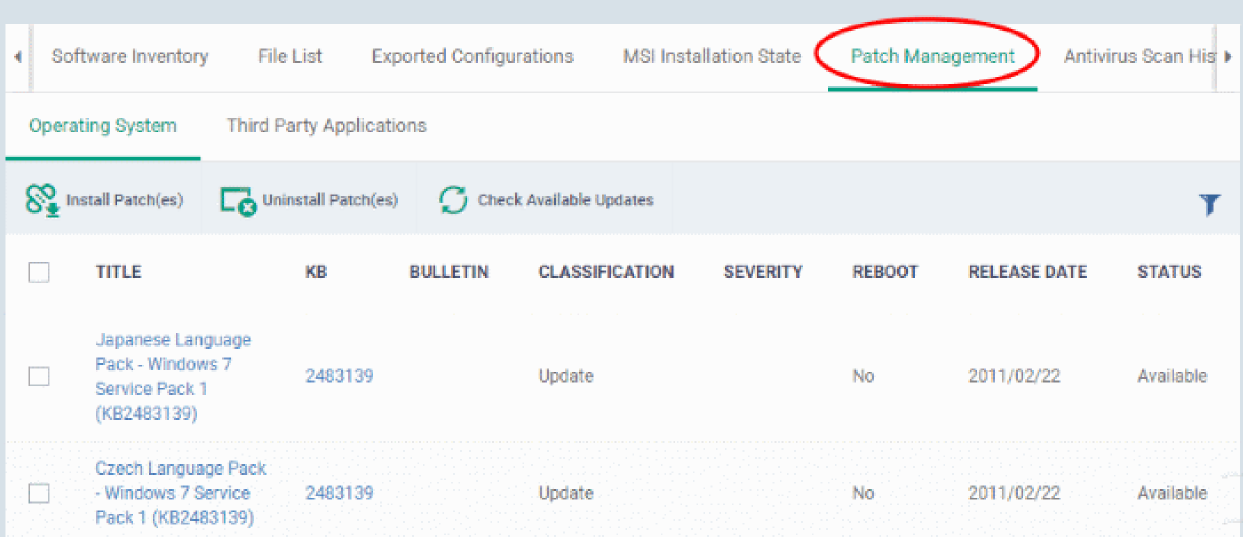
### 5.2.2.11. View and Manage Patches for Windows and 3rd Party Applications

- Windows and 3rd party applications have to be kept up-to-date to protect them from vulnerabilities.
- The details page of each device has a patch management tab which lets you view and install available patches. You can install multiple patches on a device simultaneously.
- This section tells you how to patch individual devices via the 'Device Details' screen.
    - Alternatively, there is a full patch management interface at 'Applications' > 'Patch Management'. Go here if you want to manage patches on multiple devices. See '**Patch Management**' for help with this.

> **Note**: Hidden OS patches are not visible in an individual device's patch management screen. You can hide/unhide them in the full patch management interface - click 'Applications' > 'Patch Management' > 'Operating System' tab.

**Process in brief**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page
- Select the 'Patch Management' tab
- Choose the patches you want to install from the 'Operating System' and 'Third Party' tabs
- Click 'Install Patches'. Each tab has a separate install button.



| □ | TITLE | KB | BULLETIN | CLASSIFICATION | SEVERITY | REBOOT | RELEASE DATE | STATUS |
|---|---|---|---|---|---|---|---|---|
| □ | Japanese Language Pack - Windows 7 Service Pack 1 (KB2483139) | 2483139 | | Update | | No | 2011/02/22 | Available |
| □ | Czech Language Pack - Windows 7 Service Pack 1 (KB2483139) | 2483139 | | Update | | No | 2011/02/22 | Available |

- **Operating System** - Shows all installed and pending OS patches for the device. Additional details are available for each patch, including classification, severity, release date, installation status and knowledgebase articles.
- **Third Party Applications** - Shows applications on the device for which updates are available. The version numbers of the currently installed version and the latest available version are shown. The 'severity' column tells you the importance of the update.

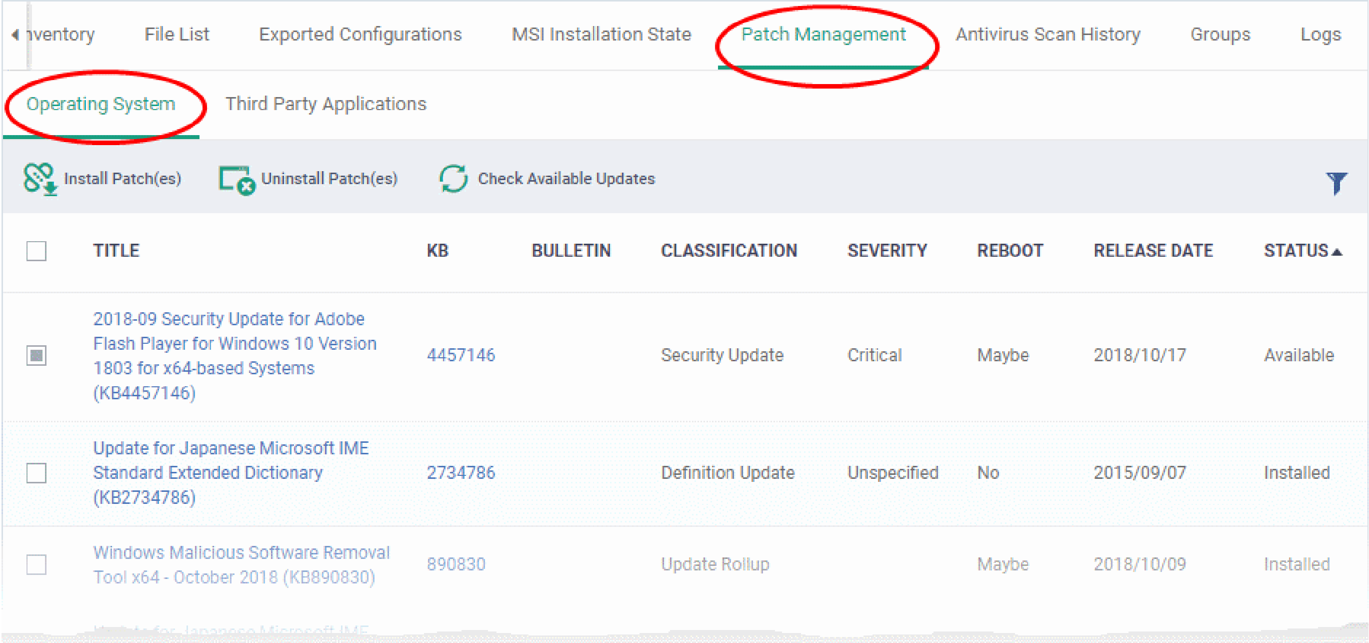
## View Windows patches available for a device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page

- Select the 'Patch Management' tab
- Click the 'Operating System' tab

**Note**:

- The 'Operating System' tab only shows Windows patches which are relevant to a device.
- Any hidden patches are not shown. Hidden patches can be configured in 'Application' > 'Patch Management'.
- For more details, see **hide patches** in **Install OS Patches on Windows Endpoints**.



| □ | TITLE | KB | BULLETIN | CLASSIFICATION | SEVERITY | REBOOT | RELEASE DATE | STATUS ▲ |
|---|---|---|---|---|---|---|---|---|
| ▣ | 2018-09 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4457146) | 4457146 | | Security Update | Critical | Maybe | 2018/10/17 | Available |
| □ | Update for Japanese Microsoft IME Standard Extended Dictionary (KB2734786) | 2734786 | | Definition Update | Unspecified | No | 2015/09/07 | Installed |
| □ | Windows Malicious Software Removal Tool x64 - October 2018 (KB890830) | 890830 | | Update Rollup | | Maybe | 2018/10/09 | Installed |

| Operating System Patches - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Title | The descriptive name of the patch.<br>• Click the name to view patch details. See **View Details of a Patch** for more details. |
| KB | The Microsoft knowledgebase article for the patch.<br>• Click the number to view the article. |
| Bulletin | The Microsoft bulletin number that contains details about the patch.<br>• Click the number to view the bulletin page. |
| Classification | The category of the patch. The possible values are:<br>• Update - Fixes a specific, non-critical problem. This type of patch does not address security-related bugs.<br>• Definition update - Updates to a product's internal database. For example, an update to the virus signature database for Windows Defender.<br>• Critical Update - Fixes a specific, critical OS problem or a critical security-related bug<br>• Security update - Fixes a version specific, security related vulnerability |

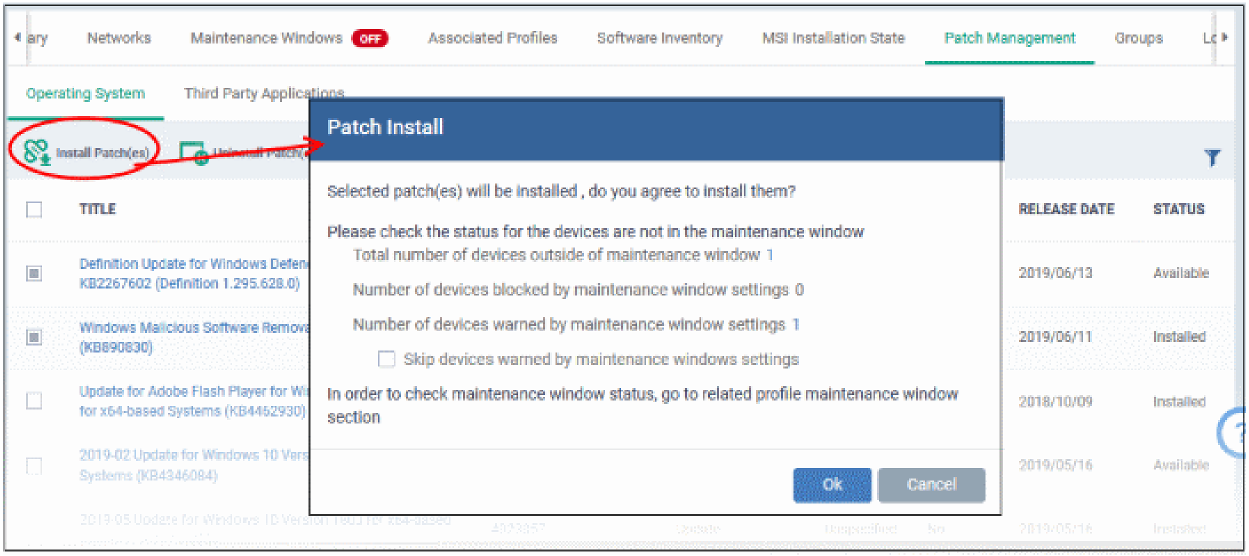
| | |
|---|---|
| | • Update rollup - A collection of updates, hotfixes, security updates and critical updates packaged together for easy deployment. These updates generally target a specific Windows component.<br>• Driver - Adds software for controlling peripherals or add-on devices that could be connected to the endpoint<br>• Feature pack - Adds new functionality distributed after an OS release.<br>• Service pack - Contains a collection of updates, hotfixes, security updates, critical updates and additional fixes.<br>• Tool - Installs a utility or feature for a specific task or a set of tasks.<br>• Upgrades - Updates the Windows OS version on the endpoint to the latest build. |
| Severity | The criticality of the patch. The severity levels are:<br>• Critical<br>• Important<br>• Low<br>• Moderate<br>• Unspecified |
| Reboot | Whether or not the endpoint requires a restart to complete the patch installation. |
| Release Date | The date on which the patch was released by Microsoft |
| Status | Whether the patch has been installed on the device or not. |
| **Controls** | |
| Install Patch(es) | Deploy selected patches to the device. See **Install missing patches on the device** for more details. |
| Uninstall Patch(es) | Remove previously installed patches or updates from the device. See **Uninstall patches from a device** for more details. |
| Check Available Updates | Refresh patch inventory with the latest updates available for the device. |

- Click any column header to sort the items in ascending/descending order of entries in that column
- Click the funnel icon on the right to filter patches by various criteria, including by severity, by whether a patch is available, or by patch installation status.

## Install missing patches on the device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page
- Select the 'Patch Management' tab
- Click the 'Operating System' tab
- Identify patches with 'Available' status
  - Click the funnel icon on the right
  - Select 'Available' from the 'Status' drop-down
  - Click 'Apply'

- Select the patches you want to install
- Click 'Install Patch(es)':



**Patch Install**

Selected patch(es) will be installed , do you agree to install them?

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 1

Number of devices blocked by maintenance window settings 0

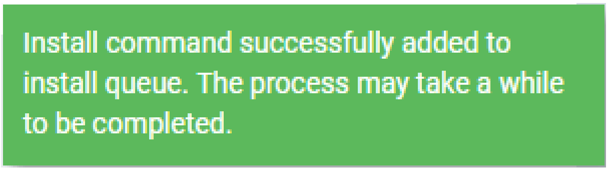
Number of devices warned by maintenance window settings 1

☐ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window section

Ok | Cancel

- **Maintenance window status -** Details of any **maintenance windows** in the device's profile.
  - **Total number of devices outside of maintenance window -** The number of devices that are not part of a maintenance window. The patches can run on these devices.
  - **Number of devices blocked by maintenance windows settings -** The number of devices on which you cannot run the patches because the admin has blocked patch installation outside the maintenance window.
  - **Number of devices warned by maintenance window settings -** The number of devices that are part of a maintenance window and have warnings enabled. You can still run the patches on these devices.
    - **Skip devices warned by maintenance windows settings -** A maintenance window is a time-slot reserved for running important tasks on target devices. Admins can enable a warning if somebody attempts to run a patch installation outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.
- Click 'OK'

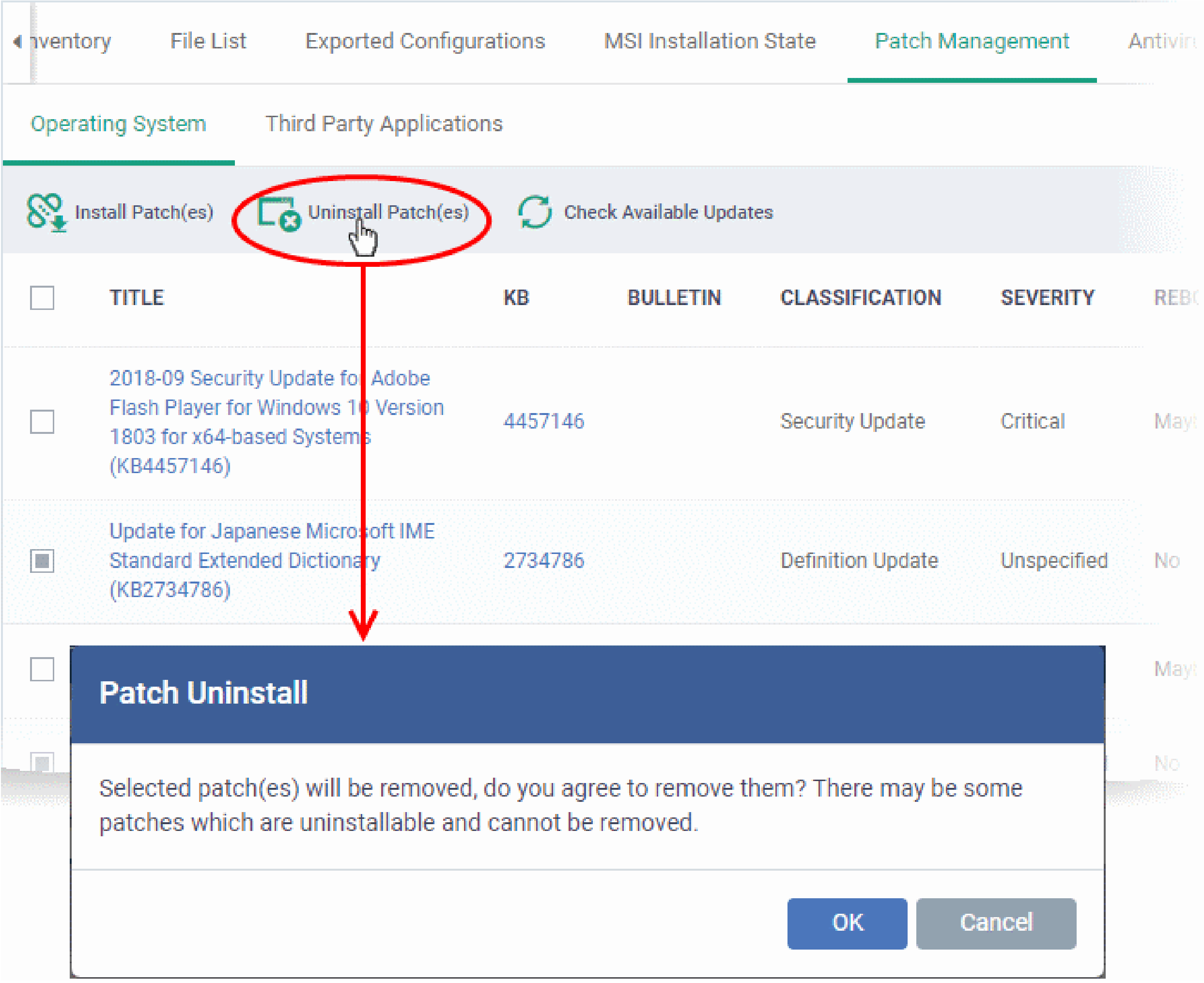

Install command successfully added to install queue. The process may take a while to be completed.

A command will be sent to install the selected patches.

## Uninstall patches and Windows updates from the device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page
- Select the 'Patch Management' tab
- Click the 'Operating System' tab
- Identify patches and updates with 'Installed' status

  - Click the funnel icon on the right
  - Select 'Installed' from the 'Status' drop-down
  - Click 'Apply'
- Select the items you want to uninstall
- Click 'Uninstall Patch(es)':



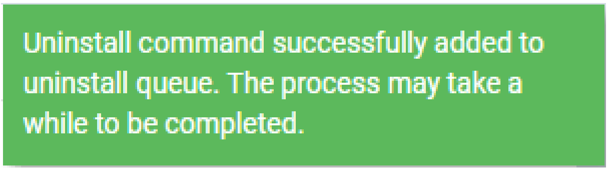
| ☐ | TITLE | KB | BULLETIN | CLASSIFICATION | SEVERITY | REB |
|---|---|---|---|---|---|---|
| ☐ | 2018-09 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4457146) | 4457146 | | Security Update | Critical | May |
| ■ | Update for Japanese Microsoft IME Standard Extended Dictionary (KB2734786) | 2734786 | | Definition Update | Unspecified | No |
| ☐ | | | | | | May |
| ■ | | | | | | No |

**Patch Uninstall**

Selected patch(es) will be removed, do you agree to remove them? There may be some patches which are uninstallable and cannot be removed.

OK Cancel

- Click 'OK' in the confirmation dialog

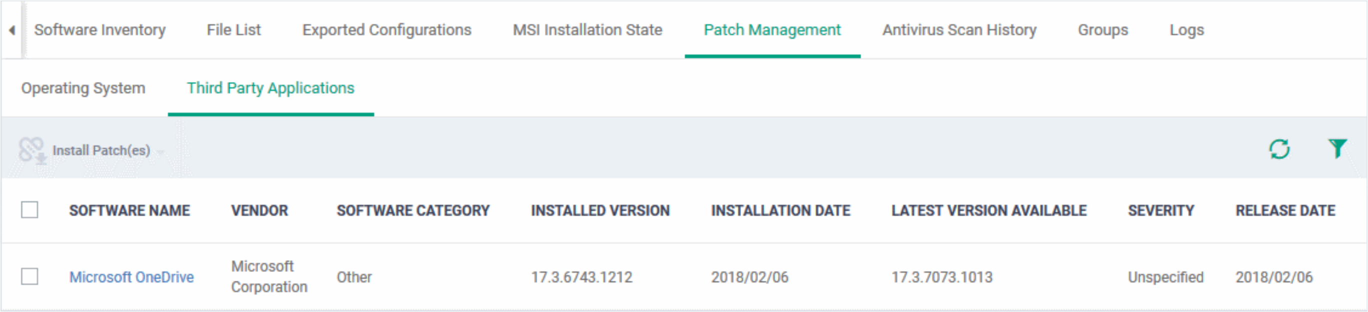


Uninstall command successfully added to uninstall queue. The process may take a while to be completed.

A command will be sent to remove the select patches/updates from the endpoint.

## View 3rd party application patches available for a device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page
- Click the 'Patch Management' tab then 'Third Party Applications':



| □ | SOFTWARE NAME | VENDOR | SOFTWARE CATEGORY | INSTALLED VERSION | INSTALLATION DATE | LATEST VERSION AVAILABLE | SEVERITY | RELEASE DATE |
|---|---|---|---|---|---|---|---|---|
| □ | Microsoft OneDrive | Microsoft Corporation | Other | 17.3.6743.1212 | 2018/02/06 | 17.3.7073.1013 | Unspecified | 2018/02/06 |

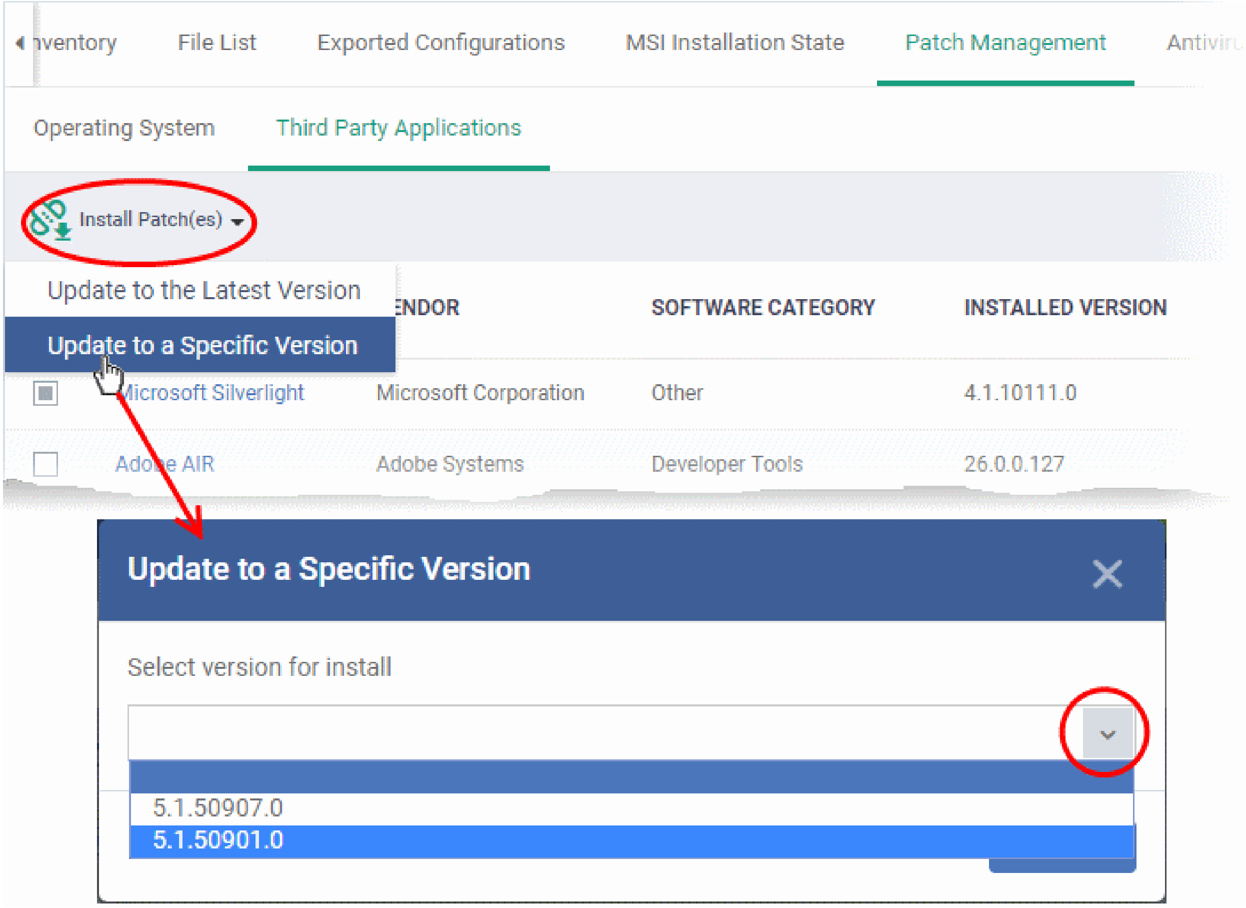
| Third Party Applications - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Software Name | The label of the third party application.<br>• Click the name to view general application details and a list of devices on which the (outdated) application is installed. See **View Details of an Application** in **Install 3rd Party Application Patches on Windows Endpoints** for more details. |
| Vendor | The software publisher. |
| Software Category | The type of the application. Possible values include:<br>• Comodo Products<br>• Runtime applications<br>• Web Browsers<br>• Utilities<br>• Messaging<br>• File Compression utilities<br>• Developer Tools<br>• Documents<br>• Online Storage<br>• Other |
| Installed Version | The version number of the application currently installed on the endpoint. |
| Installation Date | The date on which the application was installed on the endpoint. |
| Latest Version Available | The version number of the latest version of the application that is available from the publisher |
| Severity | Indicates the level of severity of the update as determined by Microsoft. The severity levels are:<br>• Unspecified<br>• Critical<br>• Important<br>• Low<br>• Moderate |
| Release Date | The date at which the latest version of the application was released. |

| Controls | |
|---|---|
| Install Patch(es) | Remotely install selected patches on the device. See **Install 3rd party application patches on a device** for more details. |

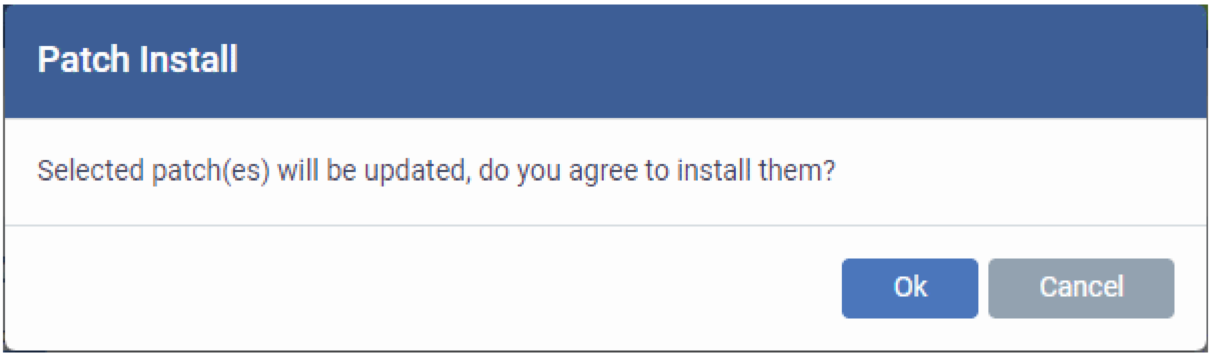
See **EM Supported 3rd Party Applications** to view a full list of applications that can be updated.

## Install 3rd party application patches on a device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
- Click the name of a Windows device to open its details page
- Select the 'Patch Management' tab then open 'Third Party Applications'
- Choose the patches you want to install
- Click the 'Install Patch(es)' button
- Select 'Update to the latest version' or 'Update to specific version' as required



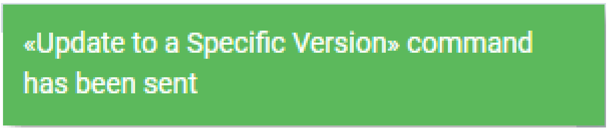
- Click 'Send'
- Click OK in the confirmation dialog:



Patch Install

Selected patch(es) will be updated, do you agree to install them?

- A command will be sent to the endpoint to install the patch:



«Update to a Specific Version» command has been sent

  - Once the command is received, the communication client (CC) on the endpoint will check whether the update is available on any other devices in the network.
  - If available, CC downloads the patch from the other device over a peer-to-peer connection. This reduces bandwidth consumption and speeds up the deployment process.
  - If the update is not available on the local network, CC downloads the update from the EM patch portal.

### 5.2.2.12. View Antivirus Scan History

The 'Antivirus Scan History' tab shows items identified as malware on an endpoint. You can also see the malware's installation path and the action taken against the file.

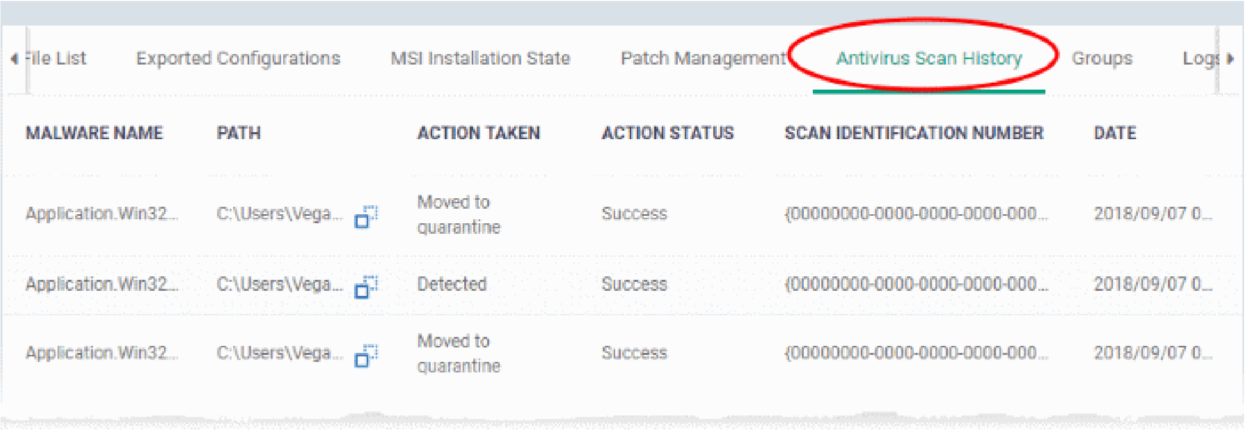
You can only view scan history on endpoints that have Comodo Client Security installed. The scan history covers manual scans and automatic scans run as part of a configuration profile.

**To view Antivirus Scan history of the device**

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

    Or
  - Select 'Show all' on the left to view every device enrolled to EM
- Click the name of a Windows device then select the 'Antivirus Scan History' tab:

**Note**: The 'Antivirus Scan History' tab is available only for endpoints with Comodo Client Security installed.



| MALWARE NAME | PATH | ACTION TAKEN | ACTION STATUS | SCAN IDENTIFICATION NUMBER | DATE |
|---|---|---|---|---|---|
| Application.Win32... | C:\Users\Vega... | Moved to quarantine | Success | {00000000-0000-0000-0000-000... | 2018/09/07 0... |
| Application.Win32... | C:\Users\Vega... | Detected | Success | {00000000-0000-0000-0000-000... | 2018/09/07 0... |
| Application.Win32... | C:\Users\Vega... | Moved to quarantine | Success | {00000000-0000-0000-0000-000... | 2018/09/07 0... |

| Antivirus Scan History- Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Malware Name | Descriptive label of the malicious item |
| Path | The installation location of the malicious item on the device |
| Action Taken | The CCS response to the item |
| Action Status | The success or failure of the action |
| Scan Identification Number | Unique identifier assigned to the scan which found the malware |
| Date | Date and time at which the scan was performed. |

### Sorting, Search and Filter Options

- Click any column header to sort items in alphabetic or ascending/descending order
- EM returns 20 results per page when you perform a search. Click the arrow next to 'Results per page' to increase the number of results up to 200.

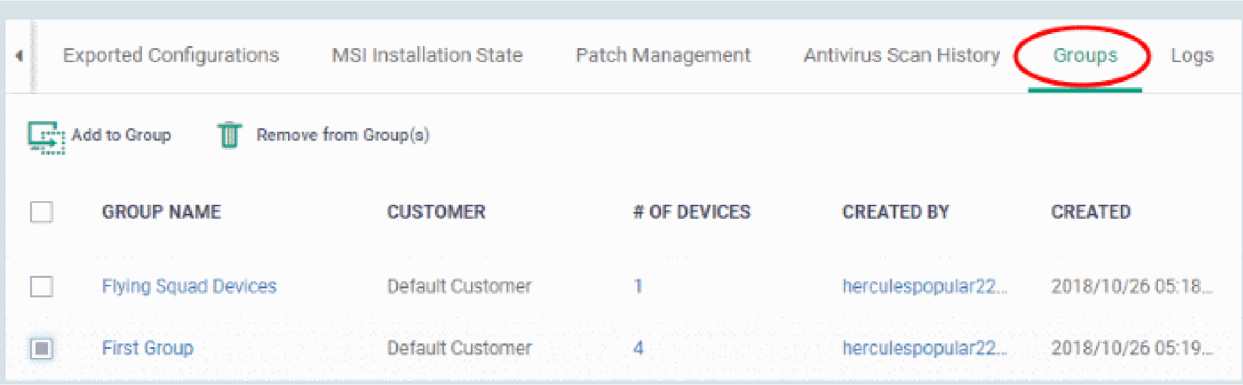
## 5.2.2.13. View and Manage Device Group Membership

The 'Groups' tab shows device groups to which the Windows endpoint belongs. You can remove the device from a group or add it to a new group.

**To view and manage device group membership**

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

      Or
    - Select 'Show all' on the left to view every device enrolled to EM
- Click the name of a Windows device then select the 'Groups' tab:



| | GROUP NAME | CUSTOMER | # OF DEVICES | CREATED BY | CREATED |
|---|---|---|---|---|---|
| □ | Flying Squad Devices | Default Customer | 1 | herculespopular22... | 2018/10/26 05:18... |
| ▣ | First Group | Default Customer | 4 | herculespopular22... | 2018/10/26 05:19... |

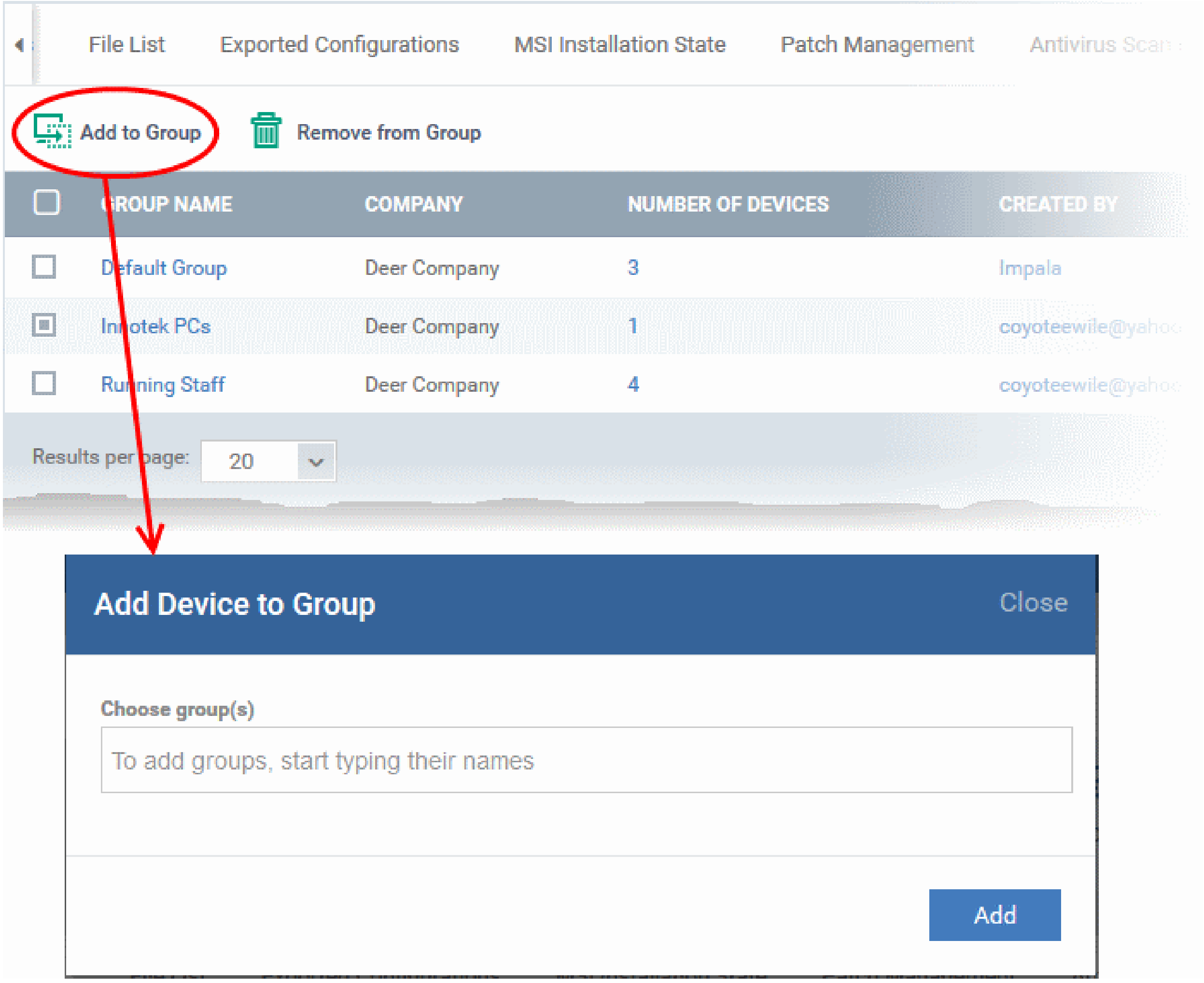
- The interface lists all groups of which the device is a member.
- Any group profiles will also be applied to the endpoint.

See **Assign Configuration Profiles to a Device Group**, for more details about applying configuration profiles to device groups.

| Device Groups - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Group | The group label.<br>• Click the group name to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Customer | The name of the company for which the group was created. |
| Number of Devices | The total count of devices in the group.<br>• Click the number to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Created By | Name of the admin who created the group.<br>• Click the name to view the admin's details.<br>• See **View the Details of a User** for more details. |
| Created | The date and time at which the group was created. |

**To add the device to a new group**

- Click 'Add to Group'



| □ | GROUP NAME | COMPANY | NUMBER OF DEVICES | CREATED BY |
|---|---|---|---|---|
| □ | Default Group | Deer Company | 3 | Impala |
| ▣ | Inntotek PCs | Deer Company | 1 | coyoteewile@yahoo |
| □ | Running Staff | Deer Company | 4 | coyoteewile@yahoo |

Choose group(s)

To add groups, start typing their names

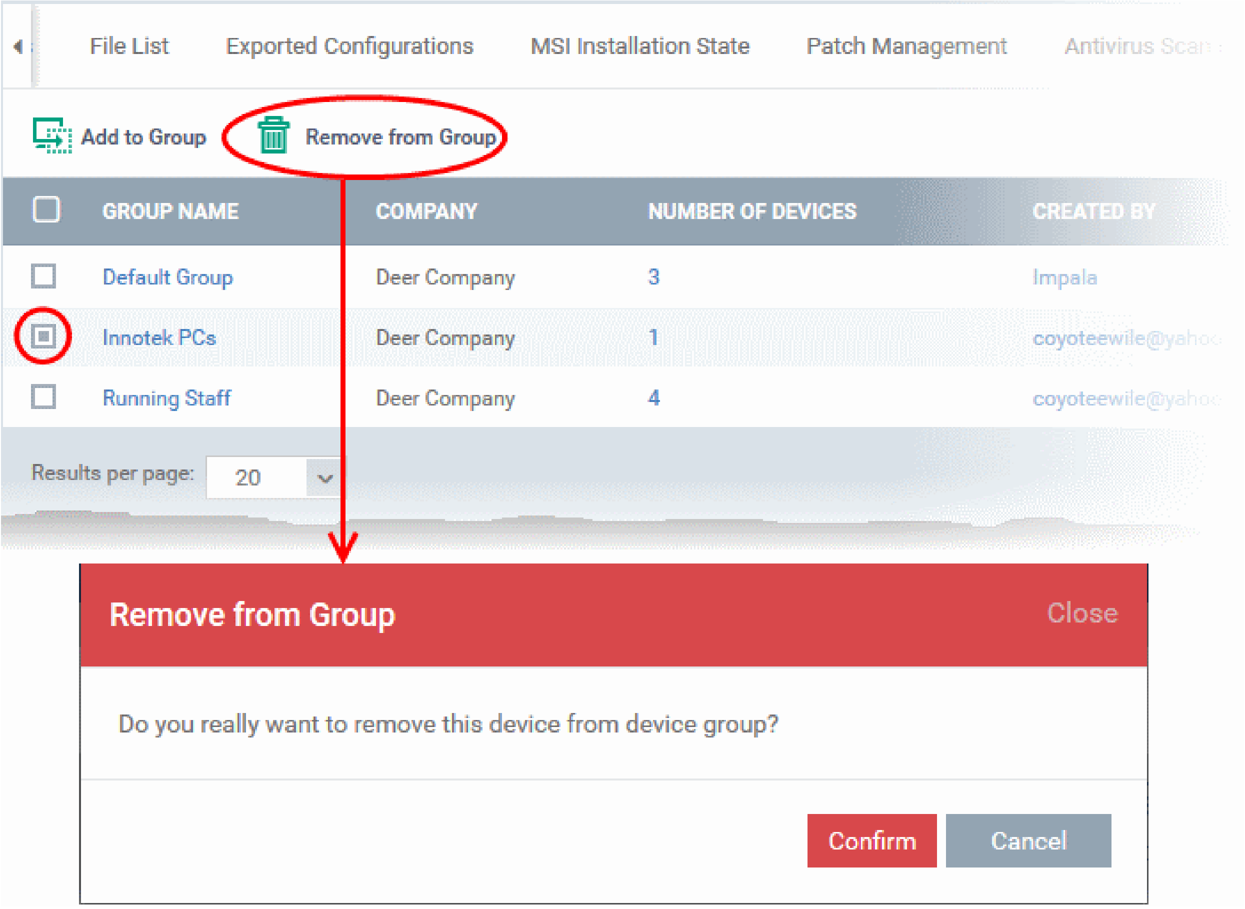
The 'Add Device to Group' dialog will appear.

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

The device will be added to the group or groups.

### To remove the device from a group

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



| □ | GROUP NAME | COMPANY | NUMBER OF DEVICES | CREATED BY |
|---|---|---|---|---|
| □ | Default Group | Deer Company | 3 | Impala |
| ▣ | Innotek PCs | Deer Company | 1 | coyoteewile@yahoo |
| □ | Running Staff | Deer Company | 4 | coyoteewile@yahoo |

Do you really want to remove this device from device group?

A confirmation dialog will appear.

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

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

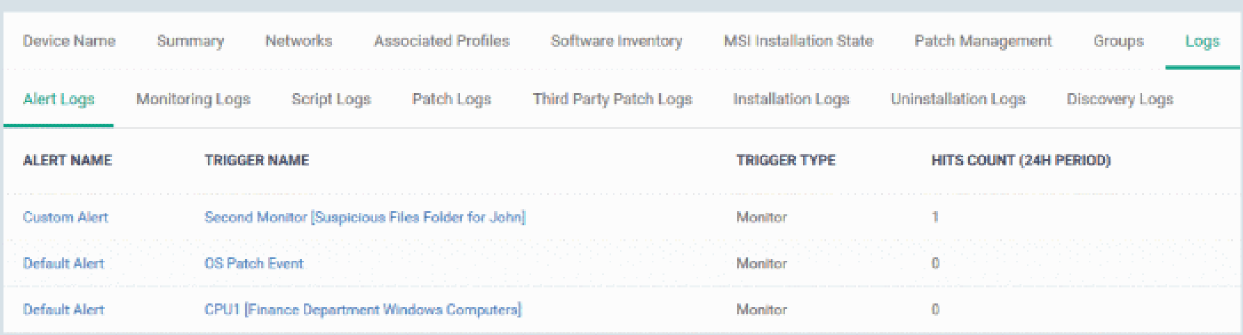
### 5.2.2.14. View Device Logs

The 'Logs' tab shows all events that occurred on a specific device. This contrasts to 'Dashboard' > '**Audit Logs**', which shows events on all devices.

**View device logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    OR
  - Select 'Show all' to view every device enrolled to EM
- Click the name of a Windows device
- Click the 'Logs' tab



| ALERT NAME | TRIGGER NAME | TRIGGER TYPE | HITS COUNT (24H PERIOD) |
|---|---|---|---|
| Custom Alert | Second Monitor [Suspicious Files Folder for John] | Monitor | 1 |
| Default Alert | OS Patch Event | Monitor | 0 |
| Default Alert | CPU1 [Finance Department Windows Computers] | Monitor | 0 |

There are eight types of logs, each shown on a different tab. Each row on these tabs is a specific event.

- The first column shows the template that caused the log to be generated. This is a named monitor, procedure or discovery task.
  - You can manage these templates in 'Configuration Templates' > 'Alerts' > 'Procedures' / 'Monitors'
  - The 'Alert Logs' tab has a slightly different layout. The template is shown in the 'Trigger Name' column
- The last column, 'Details', shows the contents of the log. Click this to view all steps that occurred in the event.
  - Again, this is slightly different in the 'Alert Logs' tab. 'Details' is replaced with 'Hit Count'.
- Each row represents a different event. For example, event logs are created when:
  - A procedure fails
  - A condition is breached in a monitor
  - An alert is generated on the device
  - A script or patch procedure is executed
  - An app from the 'Windows Application Store' is installed
  - An OS update is installed or uninstalled
  - A network discovery scan is run

Click on the following for details about each type of log:

- **Alert Logs**
- **Monitoring Logs**
- **Script Logs**
- **OS Patch Logs**

- **Third Party Patch Logs**
- **Installation Logs**
- **Uninstall Logs**
- **Discovery Logs**

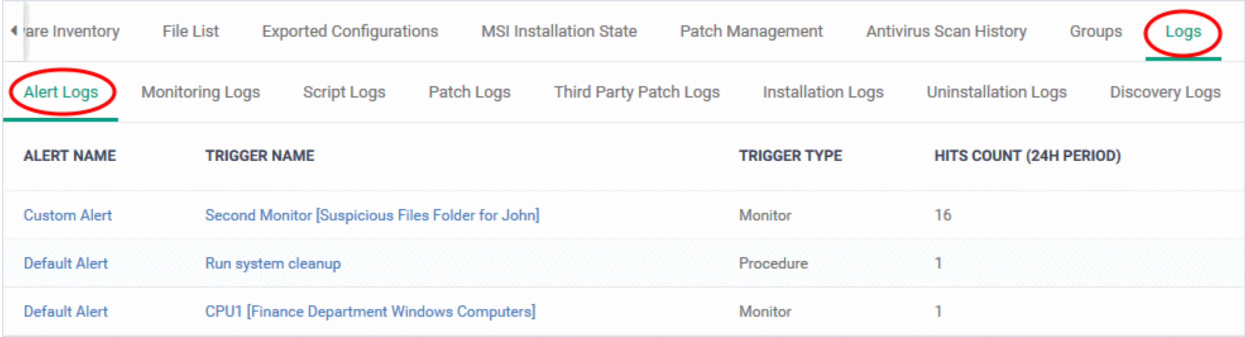
## View Alert Logs

A record of all events where an alert was generated on the endpoint. For example, logs are generated after a failed procedure deployment or a breach of monitoring conditions.

View alert logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Select 'Alert Logs'



| ALERT NAME | TRIGGER NAME | TRIGGER TYPE | HITS COUNT (24H PERIOD) |
|---|---|---|---|
| Custom Alert | Second Monitor [Suspicious Files Folder for John] | Monitor | 16 |
| Default Alert | Run system cleanup | Procedure | 1 |
| Default Alert | CPU1 [Finance Department Windows Computers] | Monitor | 1 |

| Alert Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Alert Name | The alert template used in the event.<br>• An alert template is just a collection of settings that determines alert recipients, information included, priority etc. The template does not specify the condition under which the alert is generated.<br>• The 'Trigger Name' is the actual procedure and monitor that generated the event.<br>• In the standard workflow, all procedures and monitors have the 'Default Alert' template applied to them. Click 'Configuration' > 'Templates' > 'Alerts' > 'Default Alert' to view the settings in the default template.<br>• You can also create your own alert templates. See '**Manage Alerts**' for more details.<br>• Click the alert name to view and configure its settings.<br>• Note - Discovery scan alert is not logged. |
| Trigger Name | The monitor or procedure that generated the alert. |

| | |
|---|---|
| | - Procedures - An alert is created if a procedure fails<br>- Monitors - An alert is created when one or more of the monitor's conditions are met<br>- Click the trigger name to view and configure its settings<br>- See **Manage Monitors** and **Manage Procedures** for more details. |
| Trigger Type | Can be 'Monitor' or 'Procedure' as explained above. |
| Hits Count (24 H Period) | The number of time this condition was triggered in the past 24 hours. |

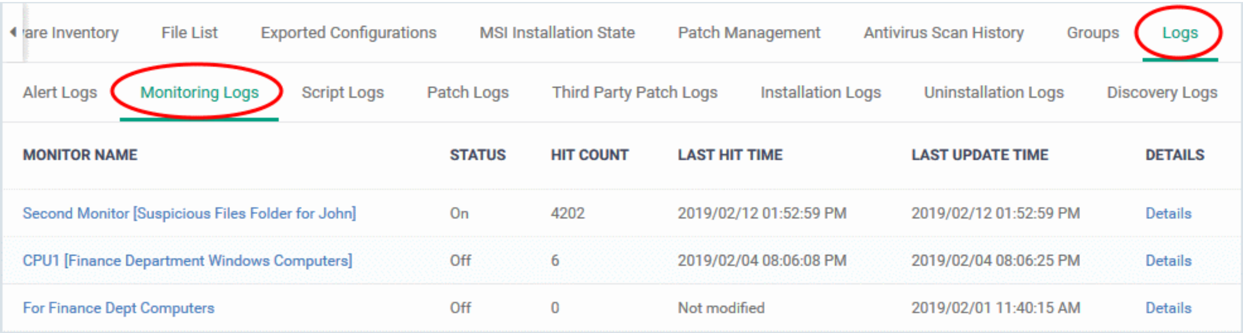
## View Monitoring Logs

- The 'Monitoring Logs' tab
  - Monitors are procedures which keep track of specific items on an endpoint. For example, you may set a monitor to track disk usage does not exceed a certain percentage.
  - Monitors can be added to the 'Monitoring' section of a configuration profile
- Logs are shown for the past 24 hours.
  - See **Manage Monitors** for help to create monitors.
  - See **Monitor Settings** for help to add monitors to profiles

### View monitoring logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Monitoring Logs'



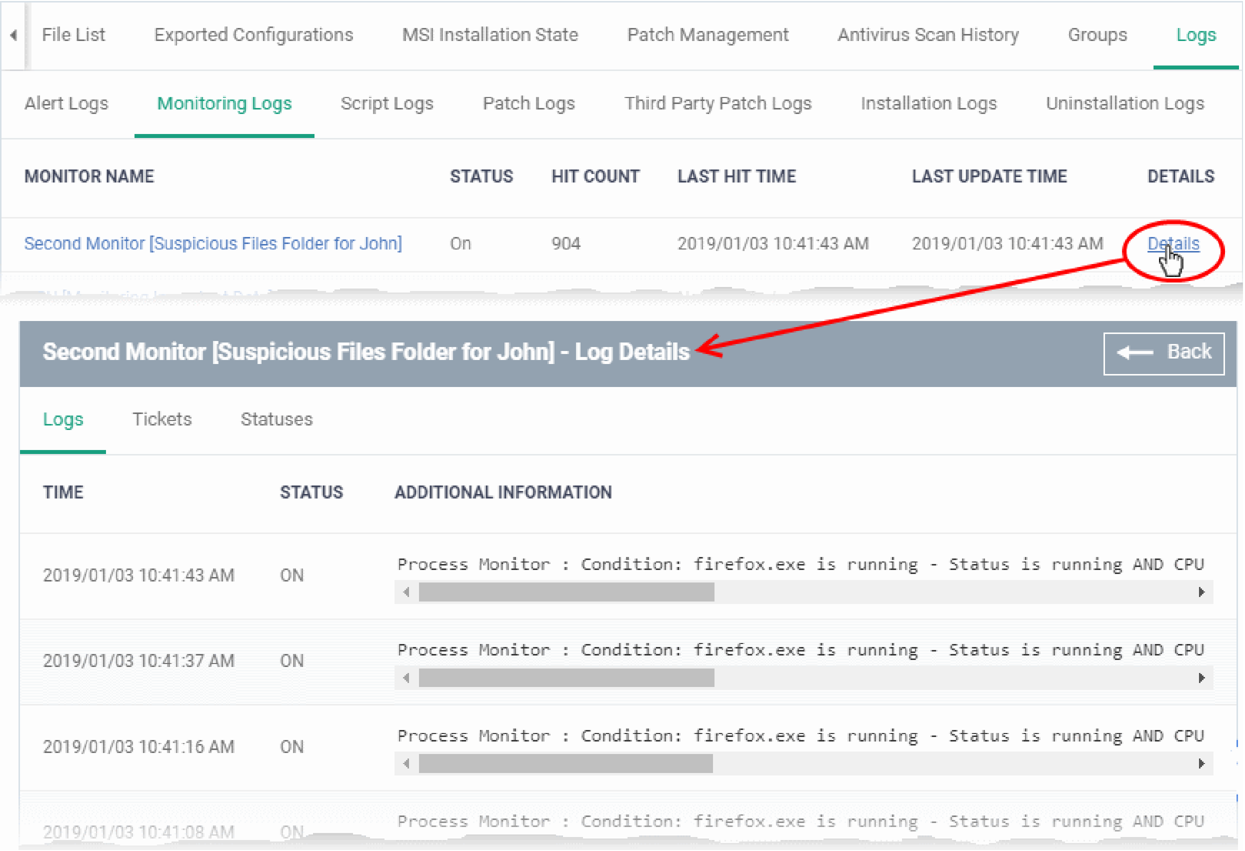
| MONITOR NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| Second Monitor [Suspicious Files Folder for John] | On | 4202 | 2019/02/12 01:52:59 PM | 2019/02/12 01:52:59 PM | Details |
| CPU1 [Finance Department Windows Computers] | Off | 6 | 2019/02/04 08:06:08 PM | 2019/02/04 08:06:25 PM | Details |
| For Finance Dept Computers | Off | 0 | Not modified | 2019/02/01 11:40:15 AM | Details |

| Monitoring Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The monitoring condition that was triggered to create the log.<br>- Click the name to view and manage the parameters of the monitor.<br>- See '**Monitor Settings**' and '**Manage Monitors**' for more details. |
| Status | Whether or not the monitor is currently active on the device. |
| Hit Count | The number of times the monitoring condition was breached during the last 24 hours. |

| | |
|---|---|
| Last Hit Time | Date and time the monitoring rule was last broken. |
| Last Update Time | Date and time when the information was last refreshed. |
| Details | • Click the 'Details' link to view a log of the breach events.<br>• See **View Details of Monitoring Logs** (given below) for more information. |

## View Details of Monitoring Logs

- Click the 'Details' link to view event information and the conditions of a monitor:



| MONITOR NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| Second Monitor [Suspicious Files Folder for John] | On | 904 | 2019/01/03 10:41:43 AM | 2019/01/03 10:41:43 AM | Details |

Second Monitor [Suspicious Files Folder for John] - Log Details

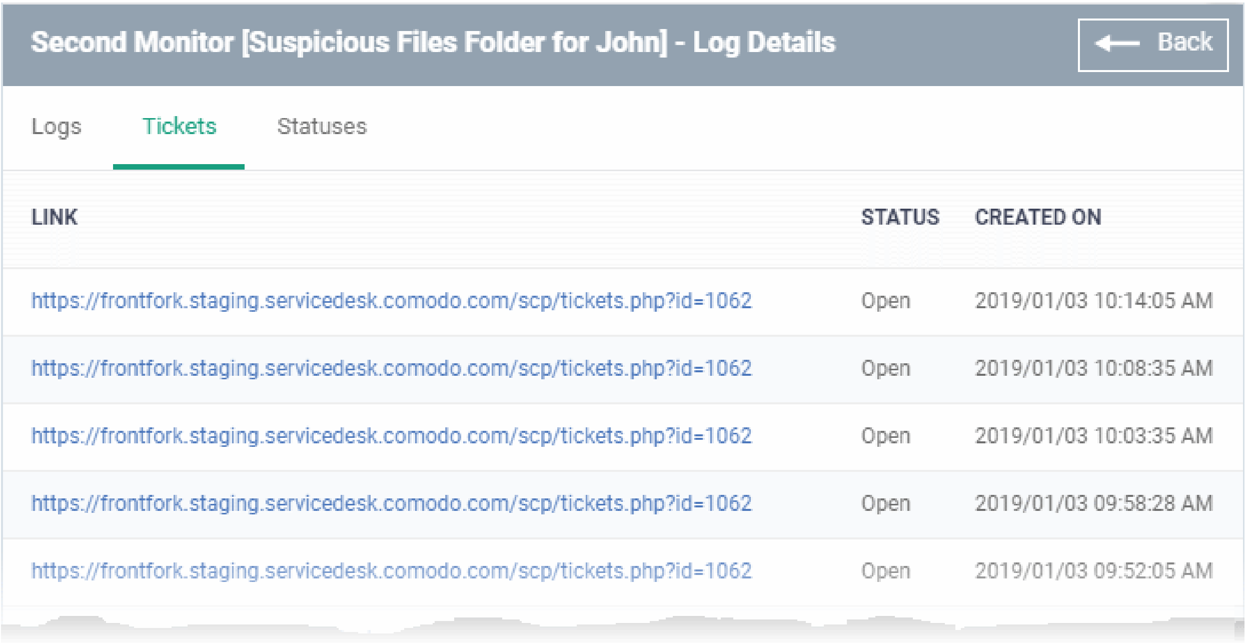
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/01/03 10:41:43 AM | ON | Process Monitor : Condition: firefox.exe is running - Status is running AND CPU |
| 2019/01/03 10:41:37 AM | ON | Process Monitor : Condition: firefox.exe is running - Status is running AND CPU |
| 2019/01/03 10:41:16 AM | ON | Process Monitor : Condition: firefox.exe is running - Status is running AND CPU |
| 2019/01/03 10:41:08 AM | ON | Process Monitor : Condition: firefox.exe is running - Status is running AND CPU |

Details are shown under three tabs:

**Logs** - The date and time when the event occurred. Also shows details about the monitoring rule that detected the event.

| Monitoring Log Details - 'Logs' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time of the event. |
| Status | The current status of the monitored condition on the device. |
| Additional Information | Details on the condition monitored and the breach |

**Tickets** - Shows any service desk tickets created by the events.

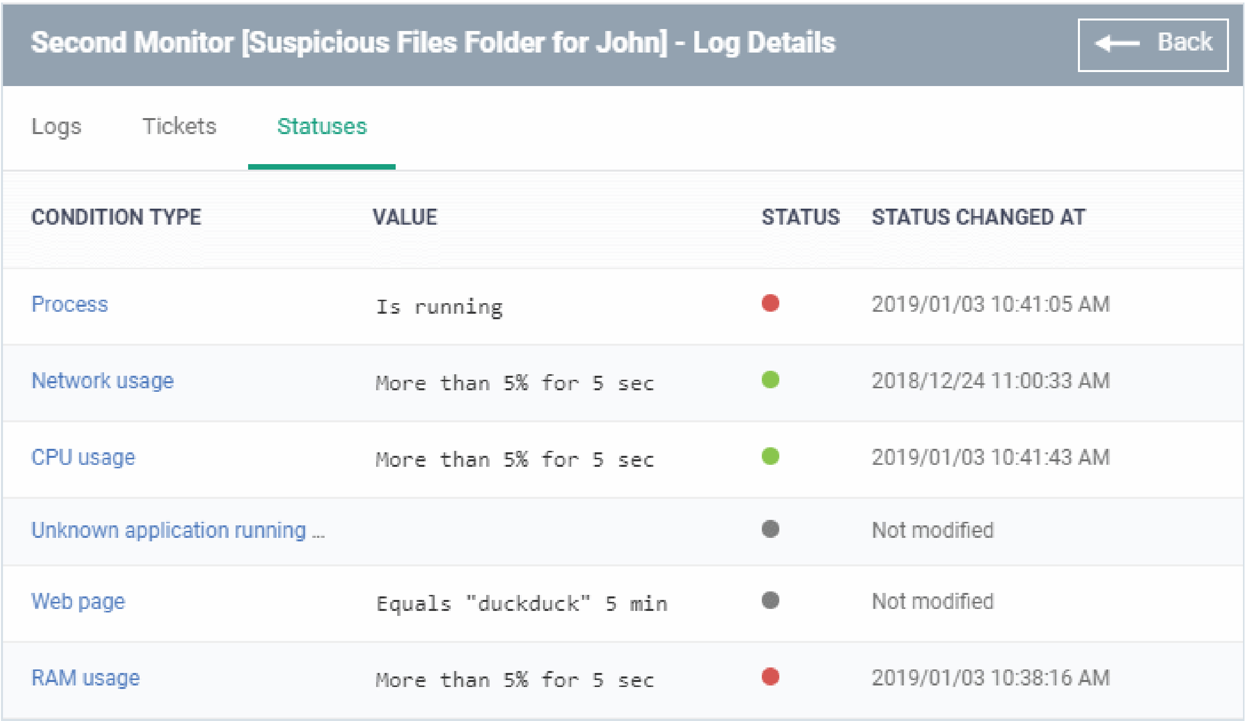


Second Monitor [Suspicious Files Folder for John] - Log Details

| LINK | STATUS | CREATED ON |
|---|---|---|
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2019/01/03 10:14:05 AM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2019/01/03 10:08:35 AM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2019/01/03 10:03:35 AM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2019/01/03 09:58:28 AM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2019/01/03 09:52:05 AM |

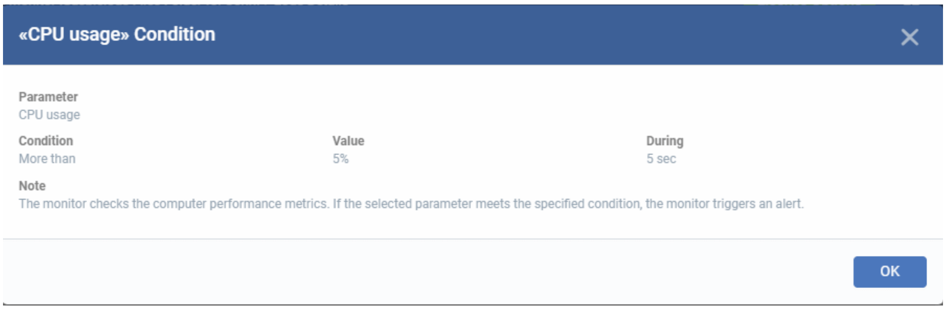
| Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

**Statuses -** Shows the current status of all conditions monitored on the device.



Second Monitor [Suspicious Files Folder for John] - Log Details

| CONDITION TYPE | VALUE | STATUS | STATUS CHANGED AT |
|---|---|---|---|
| Process | Is running | ● | 2019/01/03 10:41:05 AM |
| Network usage | More than 5% for 5 sec | ● | 2018/12/24 11:00:33 AM |
| CPU usage | More than 5% for 5 sec | ● | 2019/01/03 10:41:43 AM |
| Unknown application running ... | | ● | Not modified |
| Web page | Equals "duckduck" 5 min | ● | Not modified |
| RAM usage | More than 5% for 5 sec | ● | 2019/01/03 10:38:16 AM |

| Monitoring Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Condition Type | The observed parameter of the monitor.<br>Click the condition to view the details of the monitored parameter and configured thresholds. An example is shown below:<br><br>«CPU usage» Condition<br>Parameter: CPU usage<br>Condition: More than<br>Value: 5%<br>During: 5 sec<br>Note: The monitor checks the computer performance metrics. If the selected parameter meets the specified condition, the monitor triggers an alert.<br>OK |
| Value | The thresholds set for the parameter. |
| Status | Current state of the monitored parameter.<br>• Green - The device is operating within the thresholds of the monitored condition.<br>• Grey - Unknown<br>• Red - The device is exceeding the thresholds of the monitored condition. |
| Status Changed at | The date and time of the most recent change to the monitor status. |

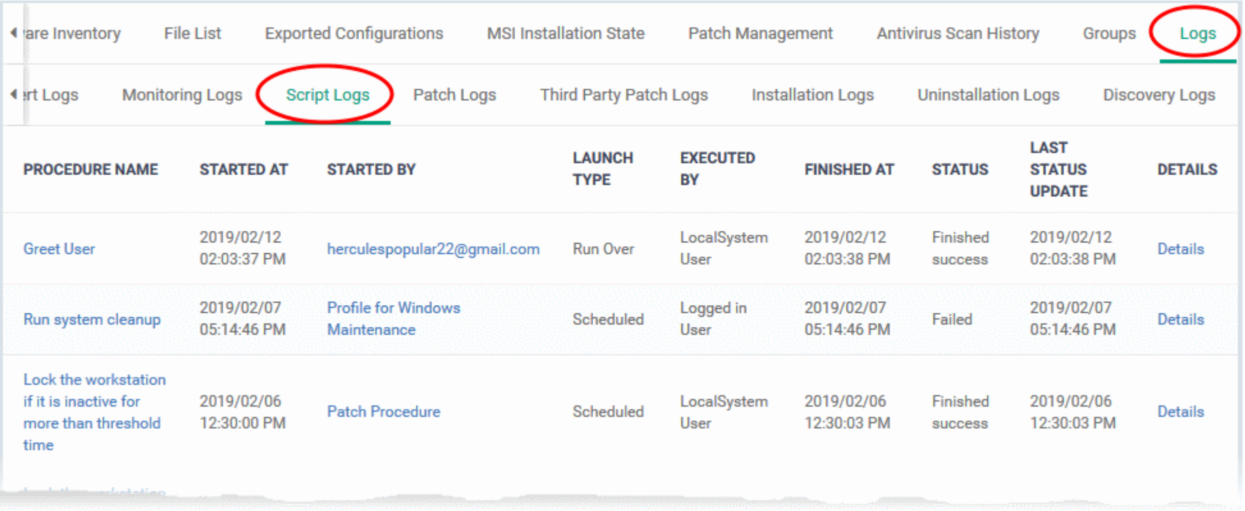
## View Script Procedure Logs

- The 'Script Logs' tab shows script procedures that were manually run on Windows devices as well as those run automatically via a profile.
- For more details on creating and running script procedures, see **Manage Procedures**.

**To view script procedures logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Script Logs'

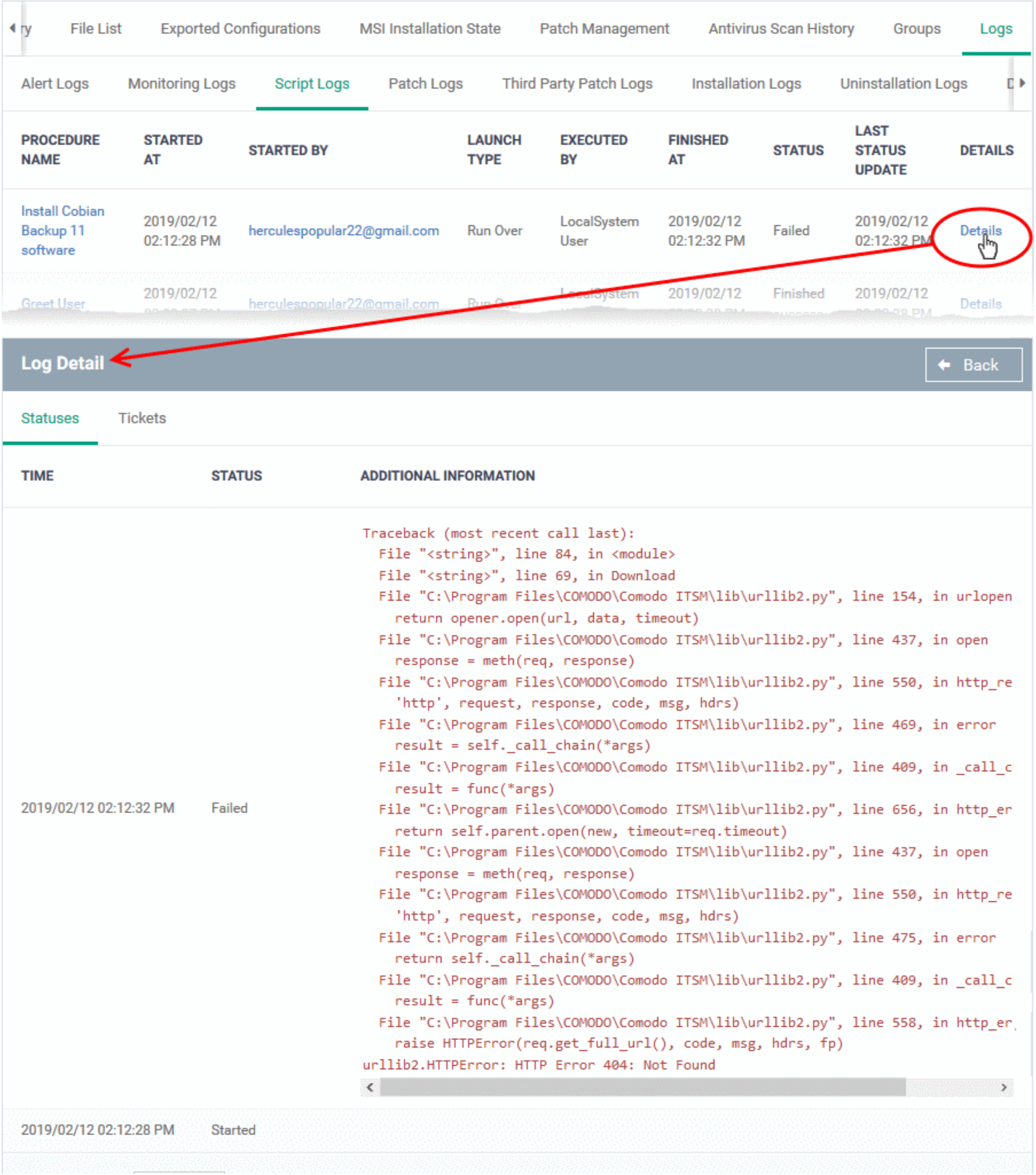


| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| Greet User | 2019/02/12 02:03:37 PM | herculespopular22@gmail.com | Run Over | LocalSystem User | 2019/02/12 02:03:38 PM | Finished success | 2019/02/12 02:03:38 PM | Details |
| Run system cleanup | 2019/02/07 05:14:46 PM | Profile for Windows Maintenance | Scheduled | Logged in User | 2019/02/07 05:14:46 PM | Failed | 2019/02/07 05:14:46 PM | Details |
| Lock the workstation if it is inactive for more than threshold time | 2019/02/06 12:30:00 PM | Patch Procedure | Scheduled | LocalSystem User | 2019/02/06 12:30:03 PM | Finished success | 2019/02/06 12:30:03 PM | Details |

| Script Procedure Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The label of the script procedure that was run on the device.<br>• Click the procedure name to view the configuration parameters of the script procedure.<br>• See **Manage Procedures** for more details. |
| Started At | The date and time when the procedure commenced. |
| Started By | Who or what launched the procedure.<br>• A profile name will be shown here if the procedure was scheduled in a profile which is active on the device.<br>• An admins name or email address will be shown if the procedure was run manually.<br>  • Click the name/email address to view the details of the admin. |
| Launch Type | Whether the procedure was scheduled or run manually. |
| Executed By | The user account type used by Endpoint Manager to execute the procedure. |
| Finished At | The date and time when the procedure was completed. |
| Status | Whether the script successfully executed or not.<br>You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details. |
| Last Status Update | The date and time when the information was last updated. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See the explanation of **View Details of Script Procedure Logs** given below. |

### View Script Procedure Log details

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



| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| Install Cobian Backup 11 software | 2019/02/12 02:12:28 PM | herculespopular22@gmail.com | Run Over | LocalSystem User | 2019/02/12 02:12:32 PM | Failed | 2019/02/12 02:12:32 PM | Details |
| Greet User | 2019/02/12 | herculespopular22@gmail.com | Run Over | LocalSystem | 2019/02/12 | Finished | 2019/02/12 | Details |

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/02/12 02:12:32 PM | Failed | |
| 2019/02/12 02:12:28 PM | Started | |

```
Traceback (most recent call last):
  File "<string>", line 84, in <module>
  File "<string>", line 69, in Download
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 154, in urlopen
    return opener.open(url, data, timeout)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 437, in open
    response = meth(req, response)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 550, in http_re
    'http', request, response, code, msg, hdrs)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 469, in error
    result = self._call_chain(*args)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 409, in _call_c
    result = func(*args)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 656, in http_er
    return self.parent.open(new, timeout=req.timeout)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 437, in open
    response = meth(req, response)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 550, in http_re
    'http', request, response, code, msg, hdrs)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 475, in error
    return self._call_chain(*args)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 409, in _call_c
    result = func(*args)
  File "C:\Program Files\COMODO\Comodo ITSM\lib\urllib2.py", line 558, in http_er
    raise HTTPError(req.get_full_url(), code, msg, hdrs, fp)
urllib2.HTTPError: HTTP Error 404: Not Found
```

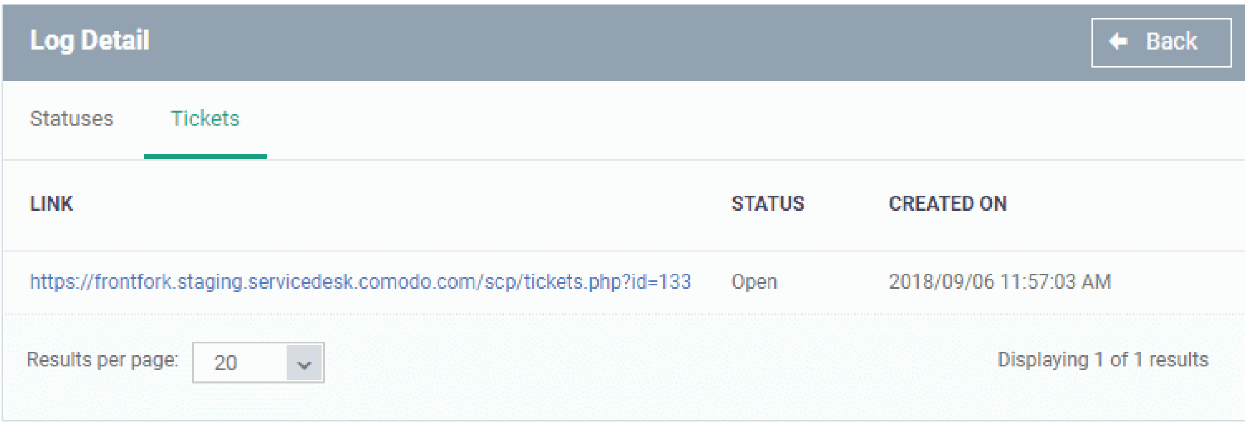
The details are displayed under two tabs:

**Statuses -** The date and time at which successive stages in the procedure were run, their success status and results.

| Script Procedure Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | The date and time of the procedure execution. |
| Status | Whether the execution was successful or not. |
| Additional Information | Provides details on the execution: |

| | |
|---|---|
| | • If successful, displays the results of the procedure execution<br>• If failed, displays the reason for not running the procedure |

**Tickets -** Displays tickets raised for any failed procedures.



| LINK | STATUS | CREATED ON |
|---|---|---|
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=133 | Open | 2018/09/06 11:57:03 AM |

Results per page: 20

Displaying 1 of 1 results

| Script Procedure Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

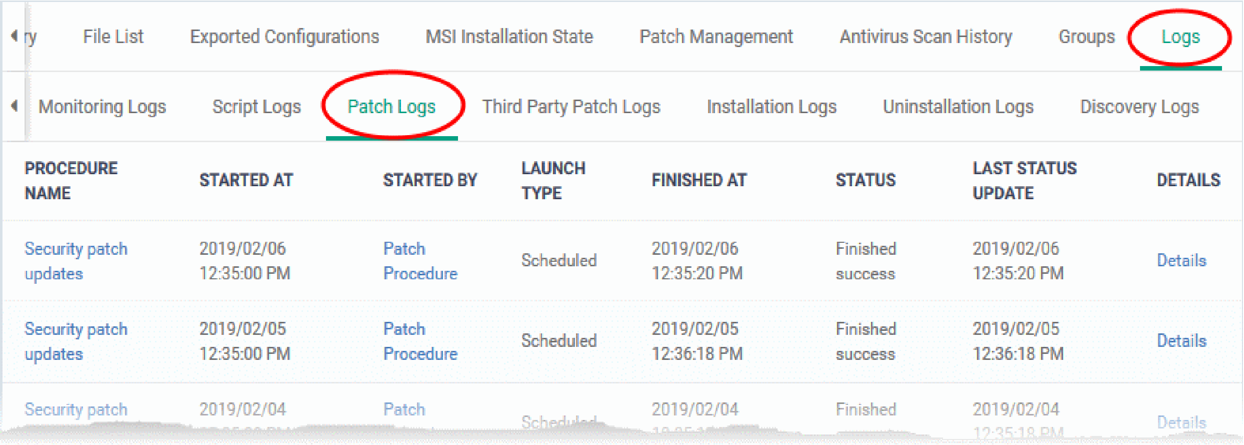
## View OS Patch Procedure Logs

- The 'Patch Logs' tab shows OS patch procedures that were manually run on Windows devices as well as those run automatically via a profile.
- For more details on creating and running patch procedures, see **Manage Procedures**.

**To view patch procedures logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Patch Logs'

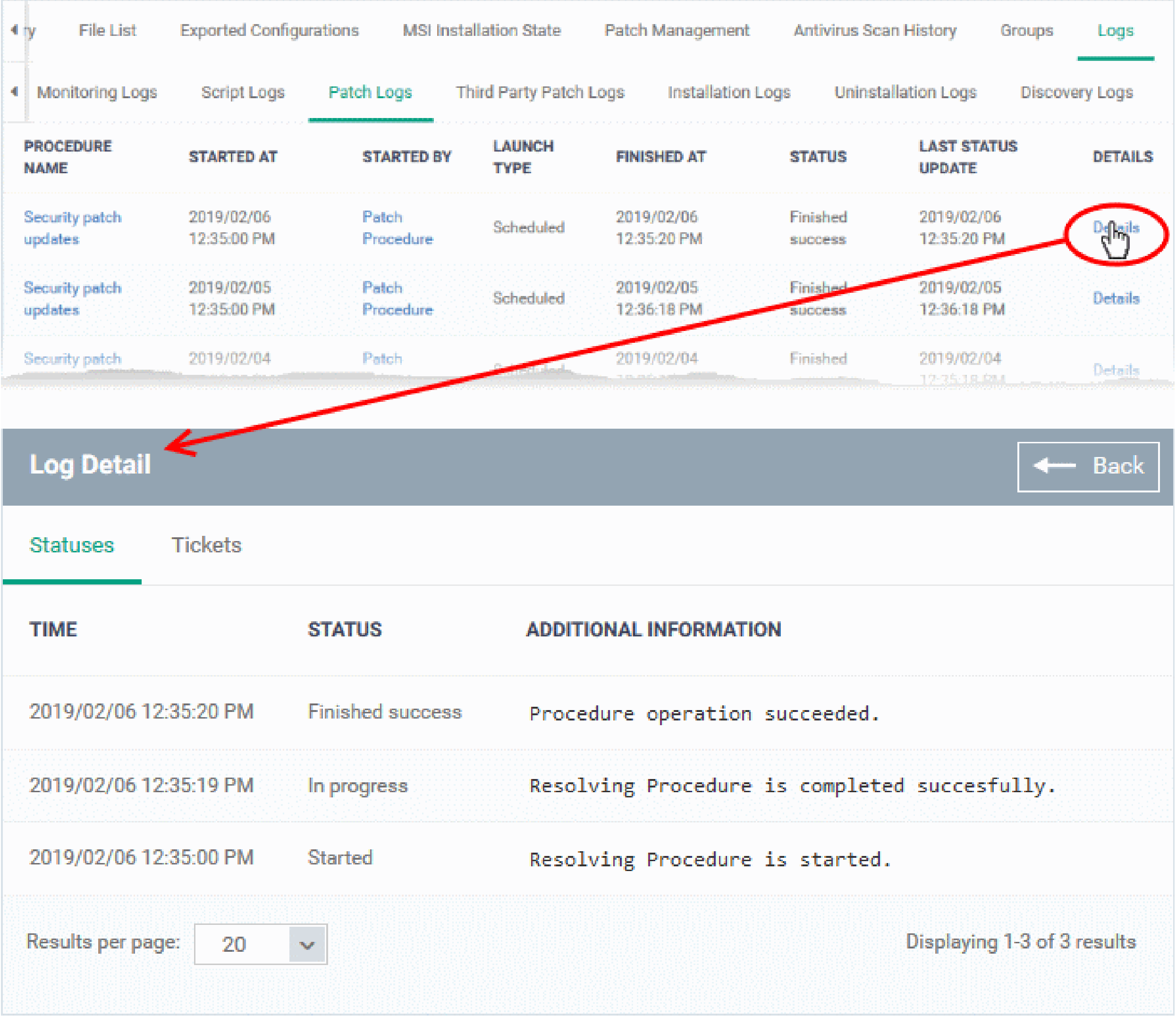


| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| Security patch updates | 2019/02/06 12:35:00 PM | Patch Procedure | Scheduled | 2019/02/06 12:35:20 PM | Finished success | 2019/02/06 12:35:20 PM | Details |
| Security patch updates | 2019/02/05 12:35:00 PM | Patch Procedure | Scheduled | 2019/02/05 12:36:18 PM | Finished success | 2019/02/05 12:36:18 PM | Details |
| Security patch | 2019/02/04 | Patch | Scheduled | 2019/02/04 | Finished | 2019/02/04 | Details |

| Patch Procedure Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The label of the patch procedure that was run on the device.<br>• Click the procedure name to view and manage the configuration parameters of it.<br>• See '**Manage Procedures**' for more details. |
| Started At | The date and time when the procedure commenced. |
| Started By | Who or what launched the procedure.<br>• A profile name will be shown here if the procedure was scheduled in a profile which is active on the device.<br>• An admins name or email address will be shown if the procedure was run manually.<br>• Click the name/email address to view the details of the admin.. |
| Launch Type | Whether the procedure was scheduled or run manually. |
| Finished At | The date and time when the procedure was completed. |
| Status | Whether the OS patch procedure was successfully executed or not.<br>You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details. |
| Last Status Update | The date and time when the information was last updated. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See the explanation of **View Details of OS Patch Procedure Logs** given below. |

### View OS Patch Procedure Log details

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



| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| Security patch updates | 2019/02/06 12:35:00 PM | Patch Procedure | Scheduled | 2019/02/06 12:35:20 PM | Finished success | 2019/02/06 12:35:20 PM | Details |
| Security patch updates | 2019/02/05 12:35:00 PM | Patch Procedure | Scheduled | 2019/02/05 12:36:18 PM | Finished success | 2019/02/05 12:36:18 PM | Details |
| Security patch | 2019/02/04 | Patch | Scheduled | 2019/02/04 | Finished | 2019/02/04 12:35:18 PM | Details |

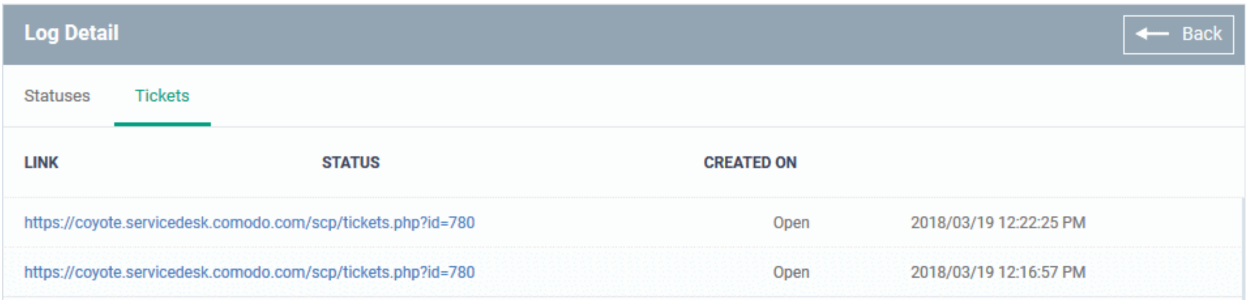
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/02/06 12:35:20 PM | Finished success | Procedure operation succeeded. |
| 2019/02/06 12:35:19 PM | In progress | Resolving Procedure is completed succesfully. |
| 2019/02/06 12:35:00 PM | Started | Resolving Procedure is started. |

The details are displayed under two tabs:

**Statuses -** The date and time at which successive stages in the procedure were run, their success status and results.

| OS Patch Procedure Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time of the procedure execution. |
| Status | Whether the execution was successful or not. |
| Additional Information | Provides details on the execution:<br>• If successful, displays the results of the procedure execution<br>• If failed, displays the reason for not running the procedure |

**Tickets -** Displays tickets raised for any failed procedures.



| LINK | STATUS | CREATED ON |
|---|---|---|
| https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780 | Open | 2018/03/19 12:22:25 PM |
| https://coyote.servicedesk.comodo.com/scp/tickets.php?id=780 | Open | 2018/03/19 12:16:57 PM |

| Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

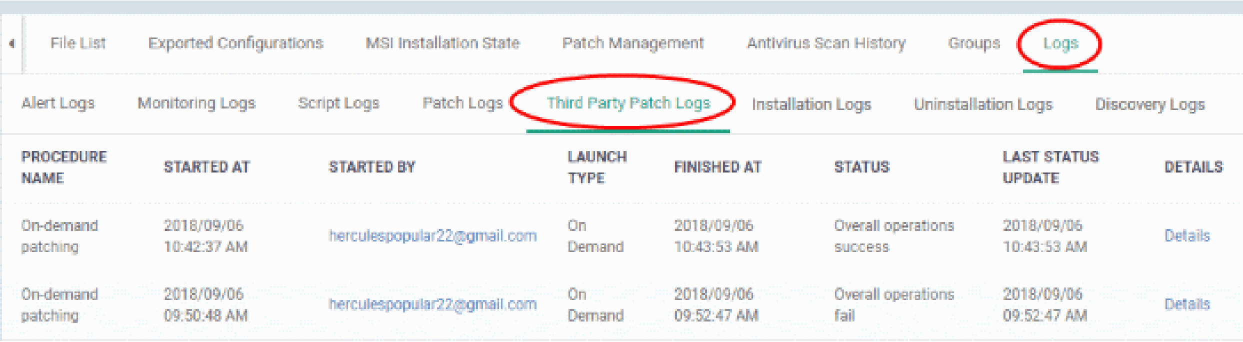
## View Third Party Patch Procedure Logs

- The third-party patch tab shows logs of patch deployments run on third party applications.
- This includes procedures that were run manually and those run automatically via a profile.
- If you need help to create patch procedures, see **Manage Procedures**.

**To view third party patch procedures logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Third Party Patch Logs'

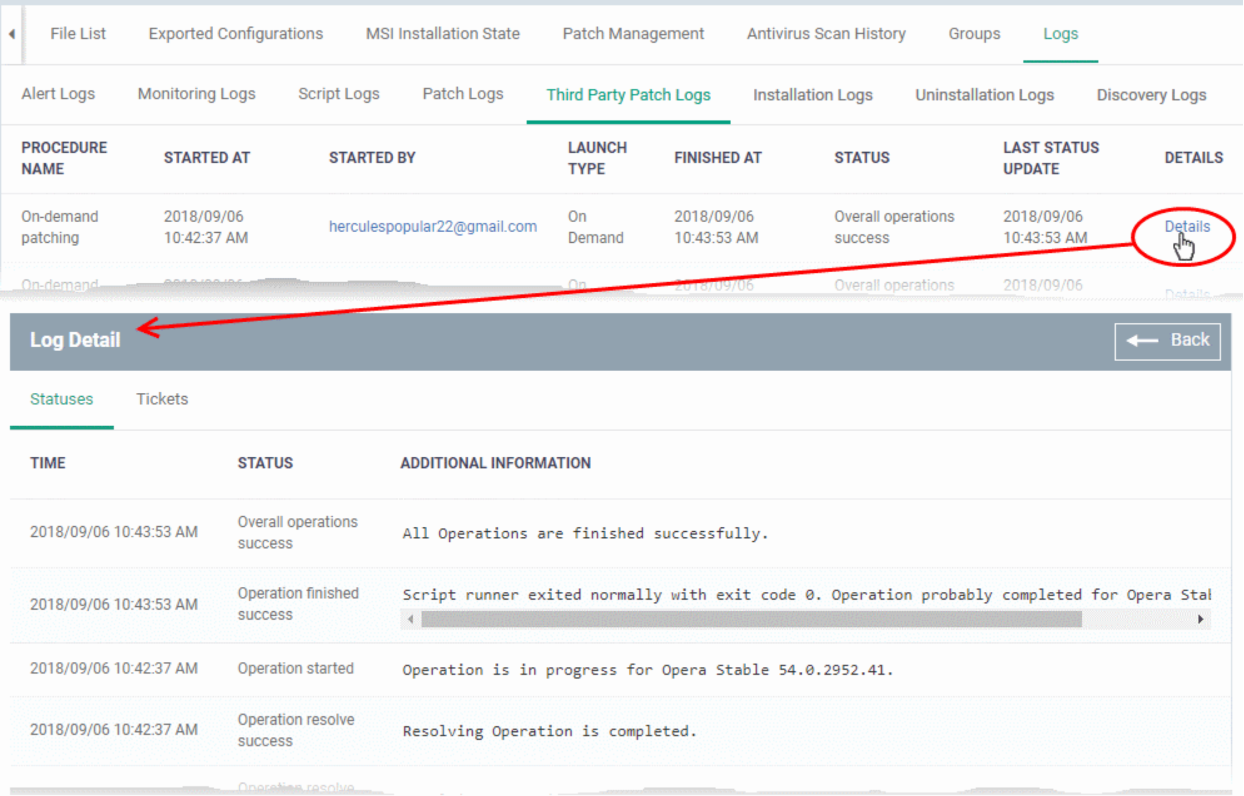


| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| On-demand patching | 2018/09/06 10:42:37 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 10:43:53 AM | Overall operations success | 2018/09/06 10:43:53 AM | Details |
| On-demand patching | 2018/09/06 09:50:48 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 09:52:47 AM | Overall operations fail | 2018/09/06 09:52:47 AM | Details |

| Third Party Patch Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The label of the procedure that was run on the device.<br>• Click the procedure name to view and manage the configuration parameters of the third party patch procedure.<br>• See '**Manage Procedures**' for more details. |
| Started At | The date and time when the procedure commenced. |
| Started By | Who or what launched the procedure.<br>• A profile name will be shown here if the procedure was scheduled in a profile which is active on the device.<br>• An admins name or email address will be shown if the procedure was run manually.<br>• Click the name/email address to view the details of the admin.. |
| Launch Type | Indicates whether the procedure was scheduled or run manually. |
| Finished At | The date and time when the procedure was completed. |
| Status | Whether the third party patch procedure was successfully executed or not.<br>• You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details. |
| Last Status Update | Date and time when the information was last updated. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See explanation of **View Details of Third Party Patch Procedure Logs** given below. |

### View Third Party Patch Procedure Log details

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



| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| On-demand patching | 2018/09/06 10:42:37 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 10:43:53 AM | Overall operations success | 2018/09/06 10:43:53 AM | Details |
| On-demand | | | On | 2018/09/06 | Overall operations | 2018/09/06 | Details |

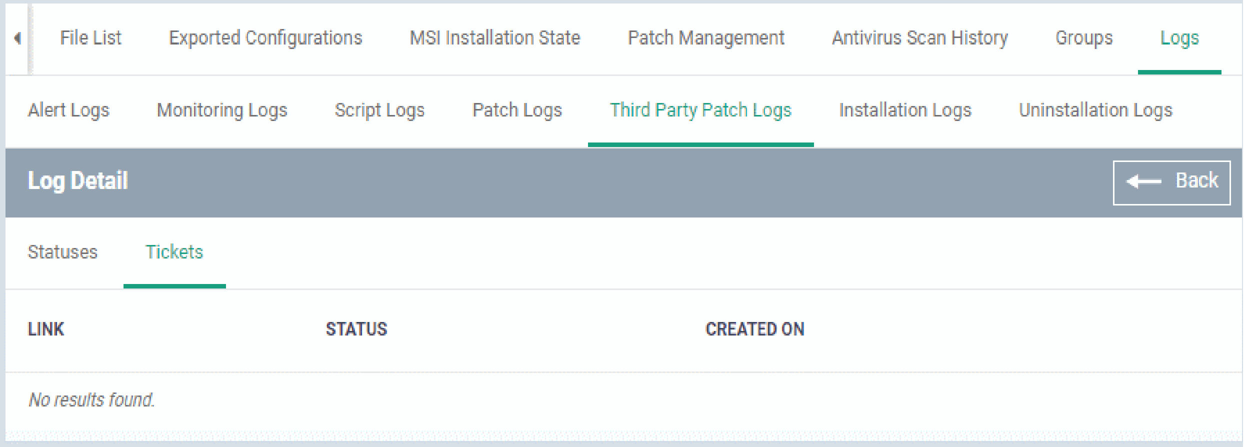
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/09/06 10:43:53 AM | Overall operations success | All Operations are finished successfully. |
| 2018/09/06 10:43:53 AM | Operation finished success | Script runner exited normally with exit code 0. Operation probably completed for Opera Stal |
| 2018/09/06 10:42:37 AM | Operation started | Operation is in progress for Opera Stable 54.0.2952.41. |
| 2018/09/06 10:42:37 AM | Operation resolve success | Resolving Operation is completed. |
| | Operation resolve | |

The details are displayed under two tabs:

**Statuses** - The date and time at which successive stages in the procedure were run, their success status and results.

| Third Party Patch Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time of the procedure execution. |
| Status | Whether the execution was successful or not. |
| Additional Information | Provides details on the execution:<br>• If successful, displays the results of the procedure execution<br>• If failed, displays the reason for not running the procedure |

**Tickets** - Displays tickets raised for any failed procedures.



| LINK | STATUS | CREATED ON |
|---|---|---|
| No results found. | | |

| Third Party Patch Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

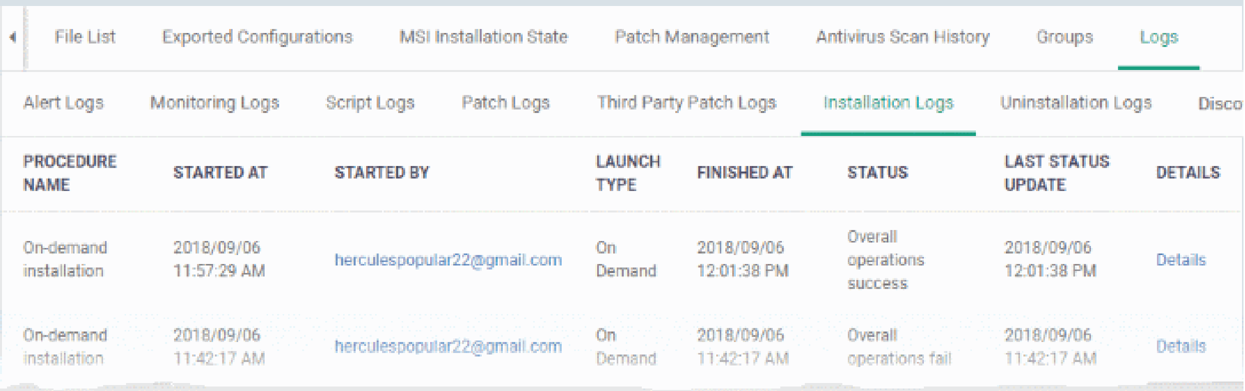
## View Installation Logs

- 'Installation Logs' tab - shows installations of third party applications from the Windows application Store ('Application Store' > 'Windows Application Store').
- See **Install Windows Apps on Devices** for more details on remote installation

**To view installation logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Installation Logs'



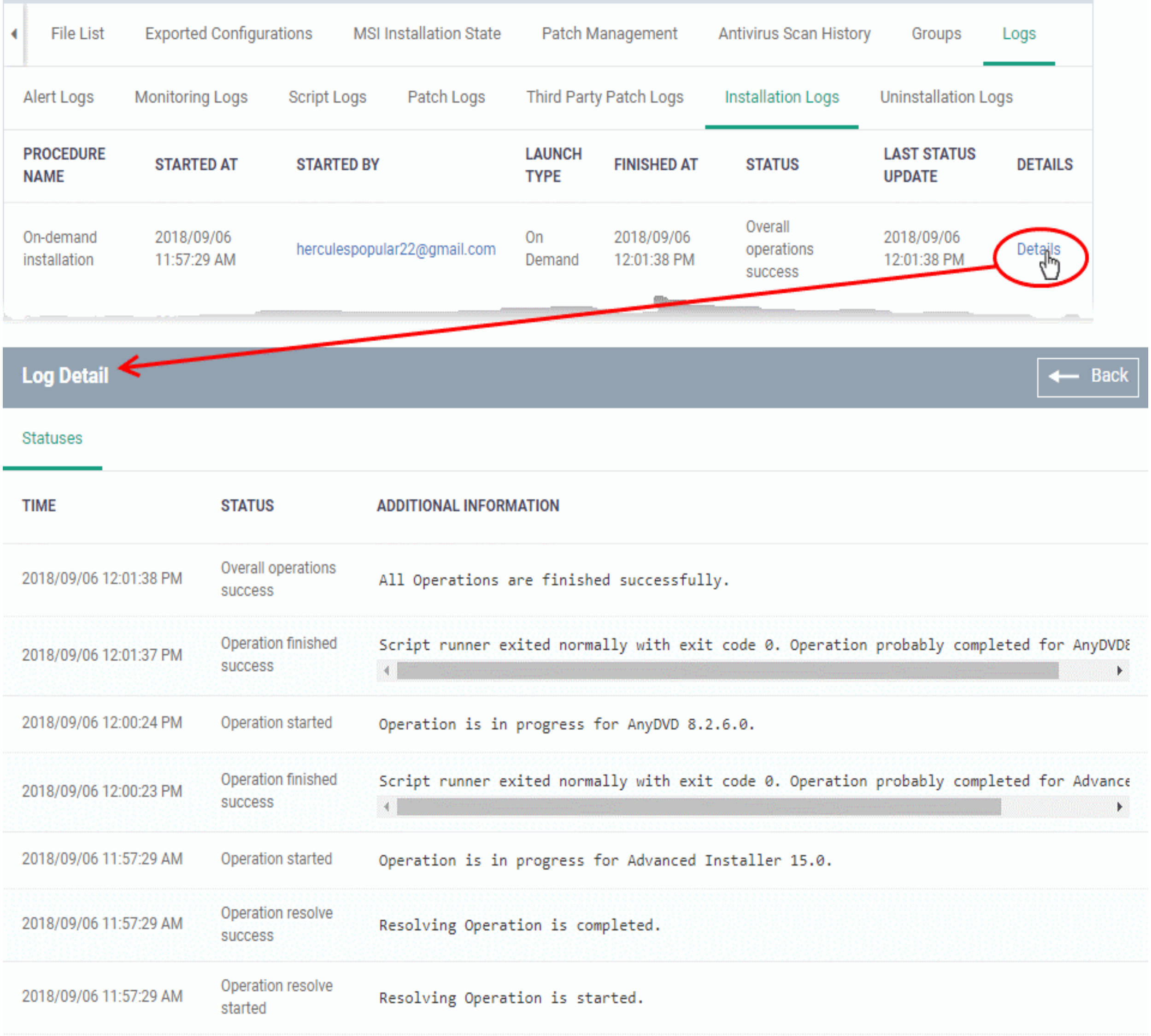
| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| On-demand installation | 2018/09/06 11:57:29 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 12:01:38 PM | Overall operations success | 2018/09/06 12:01:38 PM | Details |
| On-demand installation | 2018/09/06 11:42:17 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 11:42:17 AM | Overall operations fail | 2018/09/06 11:42:17 AM | Details |

| Installation Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The possible value is 'On-demand installation'. Install apps from 'Application Store' > 'Windows Application Store'. |
| Started At | The date and time when the installation commenced. |
| Started By | The administrator who started the remote installation.<br>• Click the name/email address to view the details of the admin.. |
| Launch Type | Indicates whether the procedure was scheduled or run manually. The possible value is 'On Demand' |

| | |
|---|---|
| Finished At | The date and time when the installation was completed. |
| Status | Whether the remote installation was successful, in progress, or failed. |
| Last Status Update | The date and time when the information was last refreshed. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See explanation of **View Details of Installation Logs** given below. |

### View Details of Installation Logs

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



| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| On-demand installation | 2018/09/06 11:57:29 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 12:01:38 PM | Overall operations success | 2018/09/06 12:01:38 PM | Details |

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/09/06 12:01:38 PM | Overall operations success | All Operations are finished successfully. |
| 2018/09/06 12:01:37 PM | Operation finished success | Script runner exited normally with exit code 0. Operation probably completed for AnyDVD8 |
| 2018/09/06 12:00:24 PM | Operation started | Operation is in progress for AnyDVD 8.2.6.0. |
| 2018/09/06 12:00:23 PM | Operation finished success | Script runner exited normally with exit code 0. Operation probably completed for Advance |
| 2018/09/06 11:57:29 AM | Operation started | Operation is in progress for Advanced Installer 15.0. |
| 2018/09/06 11:57:29 AM | Operation resolve success | Resolving Operation is completed. |
| 2018/09/06 11:57:29 AM | Operation resolve started | Resolving Operation is started. |

The 'Log Details' pane shows the date and time at which successive stages in the installation were run, their success status and results.

| Installation Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time each stage in the installation was run. |

| | |
|---|---|
| Status | Whether the execution was successful or not. |
| Additional Information | Show current installation progress.<br>• If the install fails, this area shows the reason. |

## View Uninstall Logs

- The uninstallation tab contains logs about the removal of third party applications from devices.

  There are two ways in which you can remotely uninstall applications:

  i. 'Device Details' interface - You can uninstall selected application(s) from an individual device.

  - Click 'Devices' > 'Device List' > 'Device Management'
  - Click the name of a Windows device and select the 'Software Inventory' tab
  - Select the applications and click 'Uninstall Selected Application' on the top
  - See **View and Manage Applications Installed on a Device** for more details

  ii. 'Global Software Inventory' interface - You can uninstall selected application(s) from all managed devices on which the are currently installed.

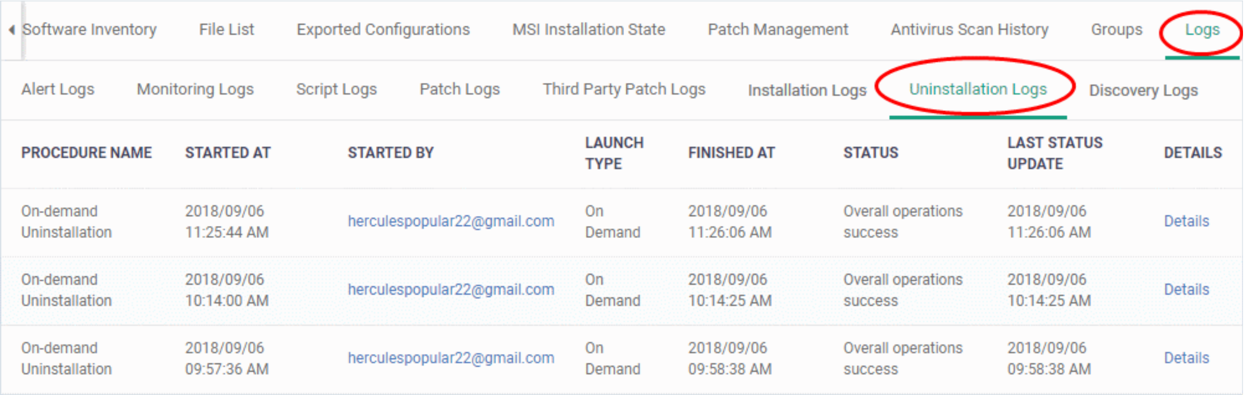
  - Click 'Applications' > 'Global Software Inventory'
  - Select the application to be uninstalled
  - Click 'Uninstall' on the top
  - See **View and Manage Applications Installed on Windows Devices** for more details

**To view uninstallation logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Select a company or a group to view just their devices

    Or

  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Uninstallation Logs'



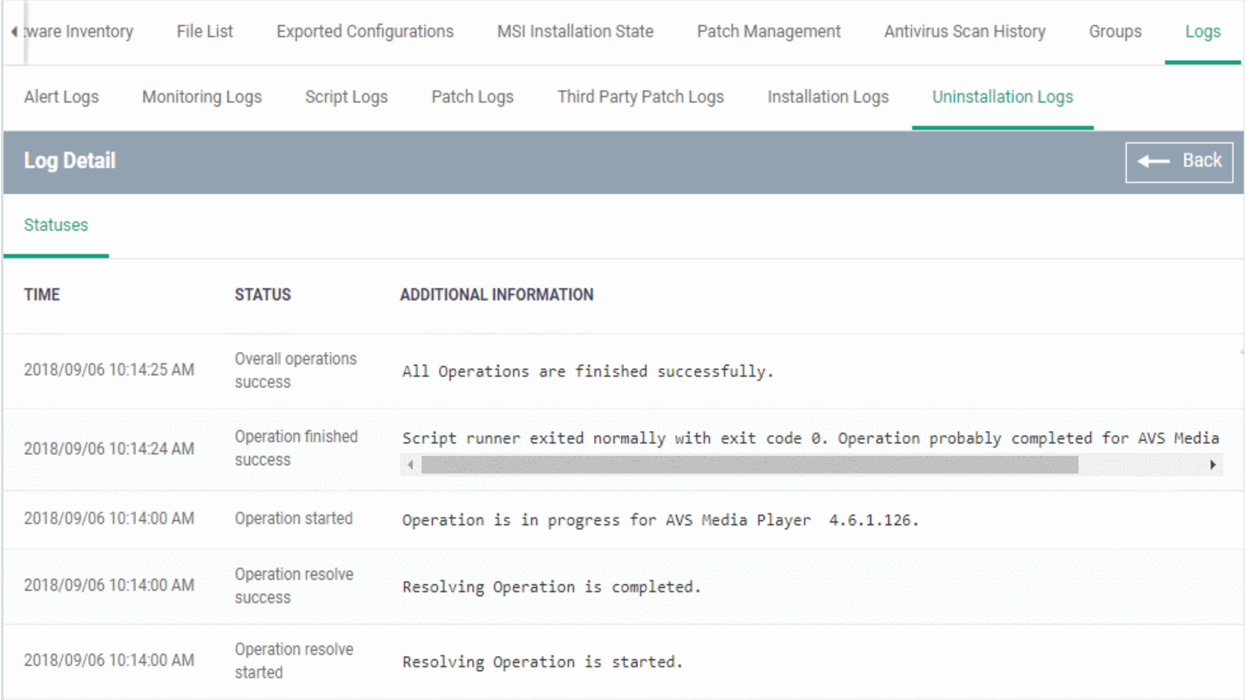
| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| On-demand Uninstallation | 2018/09/06 11:25:44 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 11:26:06 AM | Overall operations success | 2018/09/06 11:26:06 AM | Details |
| On-demand Uninstallation | 2018/09/06 10:14:00 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 10:14:25 AM | Overall operations success | 2018/09/06 10:14:25 AM | Details |
| On-demand Uninstallation | 2018/09/06 09:57:36 AM | herculespopular22@gmail.com | On Demand | 2018/09/06 09:58:38 AM | Overall operations success | 2018/09/06 09:58:38 AM | Details |

| Uninstallation Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The possible value is 'On-demand Uninstallation'. You can uninstall apps from devices by two ways explained above. |
| Started At | The date and time when the uninstallation commenced. |

| | |
|---|---|
| Started By | The administrator who started the remote uninstallation.<br>• Click the name/email address to view the details of the administrator. |
| Launch Type | Indicates whether the procedure was scheduled or run manually. The possible value is 'On Demand' |
| Finished At | The date and time when the uninstallation was completed. |
| Status | Whether the remote uninstallation was successful, in progress, or failed. |
| Last Status Update | The date and time when the information was last refreshed. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See explanation of **View Details of Uninstallation Logs** given below. |

### View Details of Uninstallation Logs

- Click the 'Details' link to view details about a remote uninstallation execution:



| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/09/06 10:14:25 AM | Overall operations success | All Operations are finished successfully. |
| 2018/09/06 10:14:24 AM | Operation finished success | Script runner exited normally with exit code 0. Operation probably completed for AVS Media |
| 2018/09/06 10:14:00 AM | Operation started | Operation is in progress for AVS Media Player  4.6.1.126. |
| 2018/09/06 10:14:00 AM | Operation resolve success | Resolving Operation is completed. |
| 2018/09/06 10:14:00 AM | Operation resolve started | Resolving Operation is started. |

The 'Log Details' pane shows the date and time at which successive stages in the uninstallation were run, their success status and results.

| Installation Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time each stage in the uninstallation was run. |
| Status | Whether the execution was successful or not. |
| Additional Information | Show current installation progress.<br>• If the uninstallation failed, this area shows the reason. |

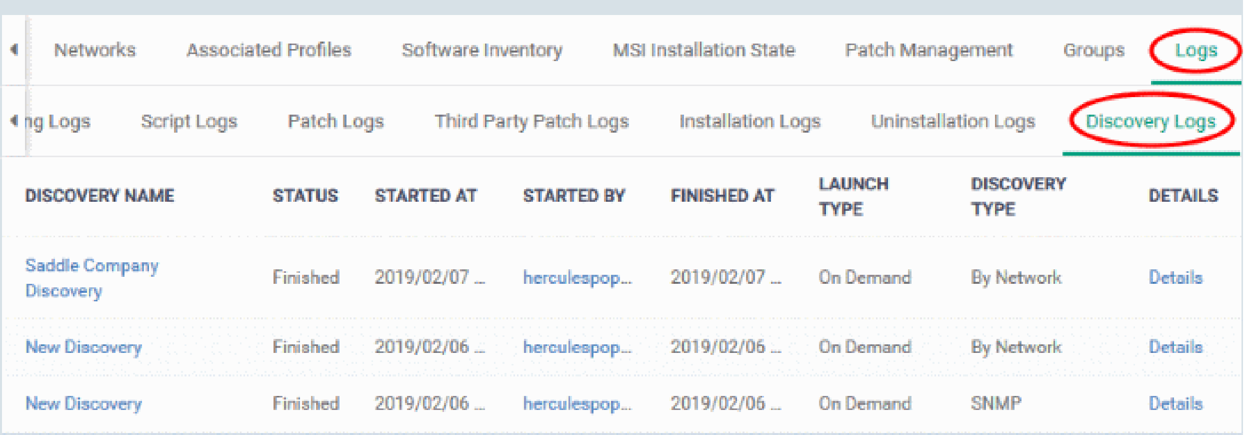
## View Discovery Logs

- A managed endpoint can be used as a probe device which runs discovery scans on a network.
- If a device has been used as a probe, then the discovery logs tab shows any scans run from it.
- See **Create, Manage and Run Network Discovery Tasks** if you want to learn more about discovery scans and probe devices.

View discovery logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Windows device then select the 'Logs' tab
- Click 'Discovery Logs'



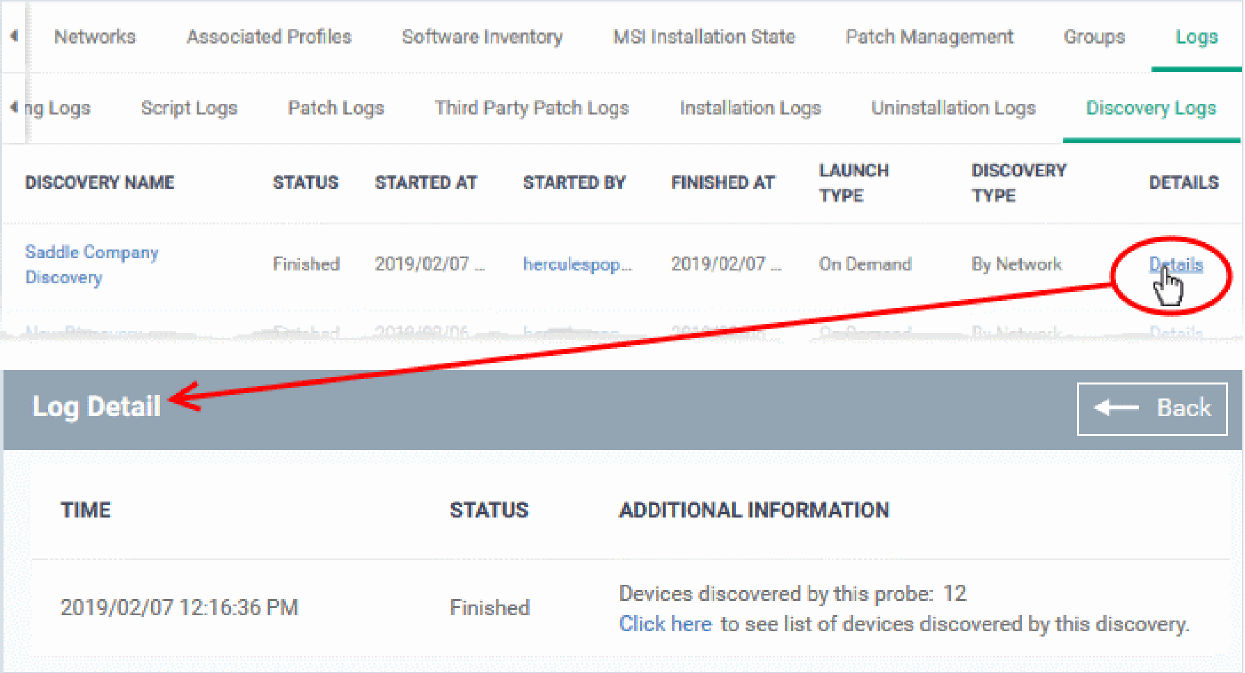
| DISCOVERY NAME | STATUS | STARTED AT | STARTED BY | FINISHED AT | LAUNCH TYPE | DISCOVERY TYPE | DETAILS |
|---|---|---|---|---|---|---|---|
| Saddle Company Discovery | Finished | 2019/02/07 ... | herculespop... | 2019/02/07 ... | On Demand | By Network | Details |
| New Discovery | Finished | 2019/02/06 ... | herculespop... | 2019/02/06 ... | On Demand | By Network | Details |
| New Discovery | Finished | 2019/02/06 ... | herculespop... | 2019/02/06 ... | On Demand | SNMP | Details |

| Installation Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Discovery Name | The label of the discovery scan task.<br>• Click the name to view task details<br>• See **Create, Manage and Run Network Discovery Tasks** to read more about discovery tasks and probe devices. |
| Status | Whether the scan is progress, queued or finished. |
| Started At | Date and time the scan commenced on the network. |
| Started By | The email address of the admin who launched the scan.<br>• Click the email address to view the details of the admin. See **View User Details** if you need help with this. |
| Finished At | The date and time the scan ended. |
| Launch Type | How the scan was started. For example, 'On Demand' means it was manually started by an admin. |
| Type of Discovery | Can be SNMP scan or network (IP) scan. |

|  |  |
|---|---|
| Details | • View more information about the scan. For example, this will tell you the number of devices found and their names.<br>• See **View Details of a Discovery Scan** below. |

### View Details of a Discovery Scan

- Click 'Details' in the row of a scan to view additional information:



| DISCOVERY NAME | STATUS | STARTED AT | STARTED BY | FINISHED AT | LAUNCH TYPE | DISCOVERY TYPE | DETAILS |
|---|---|---|---|---|---|---|---|
| Saddle Company Discovery | Finished | 2019/02/07 ... | herculespop... | 2019/02/07 ... | On Demand | By Network | Details |

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/02/07 12:16:36 PM | Finished | Devices discovered by this probe: 12<br>Click here to see list of devices discovered by this discovery. |

- 'Click here' link - View devices found by the scan.
  - See **Discovered Devices** for more details

## 5.2.3. Manage Mac OS Devices

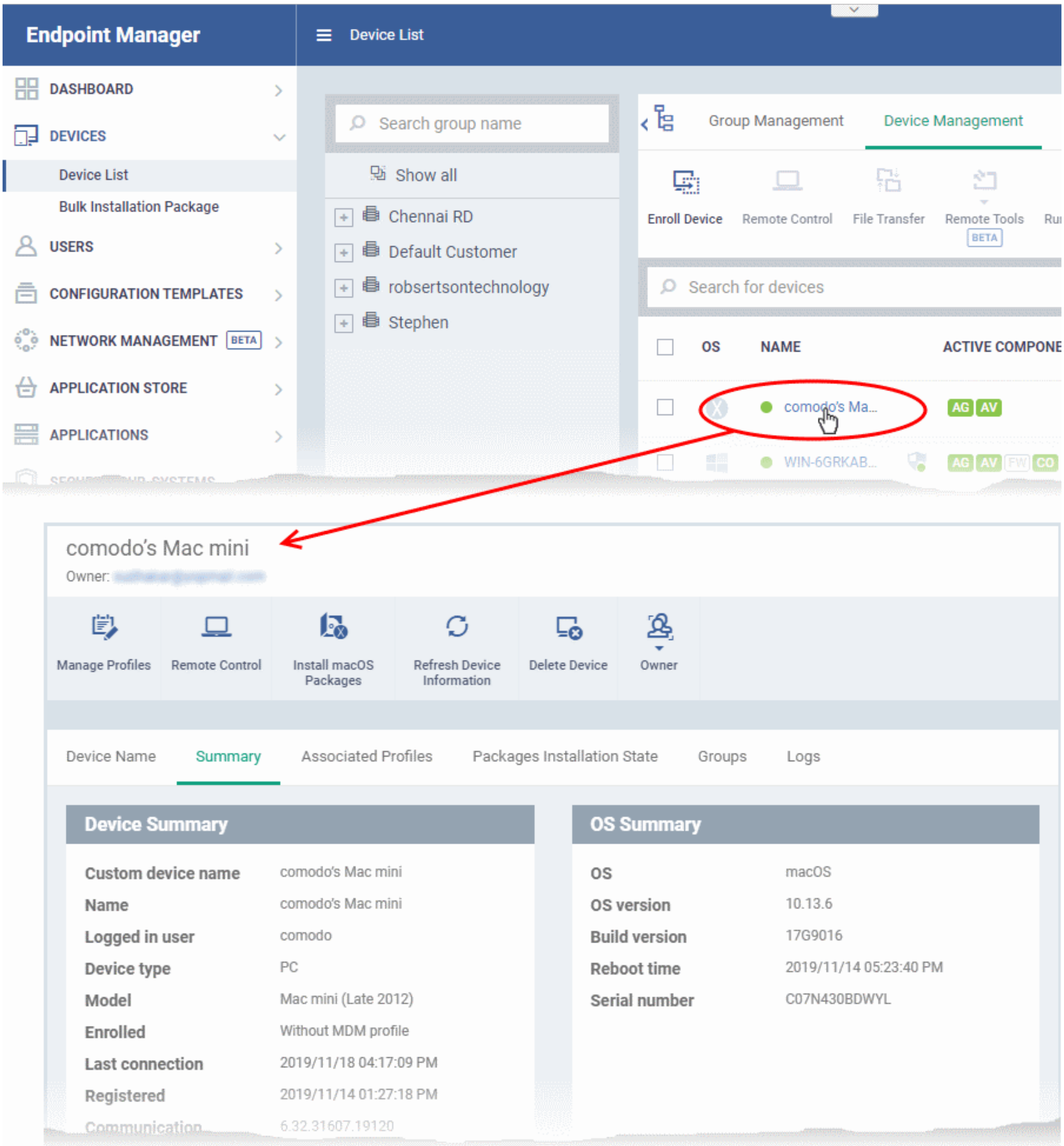
The MAC details page shows operating system and security information about the device. The screen also lets you manage device profiles, remotely install packages, configure group membership, and view device logs.

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

### View and manage Mac OS devices

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group in the middle column to view only their devices

    OR
  - Select 'Show all' to view every device added to EM
- Click the name of any Mac OS device to open its details page:



comodo's Mac mini

Owner: [redacted]

**Device Summary**

| | |
|---|---|
| Custom device name | comodo's Mac mini |
| Name | comodo's Mac mini |
| Logged in user | comodo |
| Device type | PC |
| Model | Mac mini (Late 2012) |
| Enrolled | Without MDM profile |
| Last connection | 2019/11/18 04:17:09 PM |
| Registered | 2019/11/14 01:27:18 PM |
| Communication | 6.32.31607.19120 |

**OS Summary**

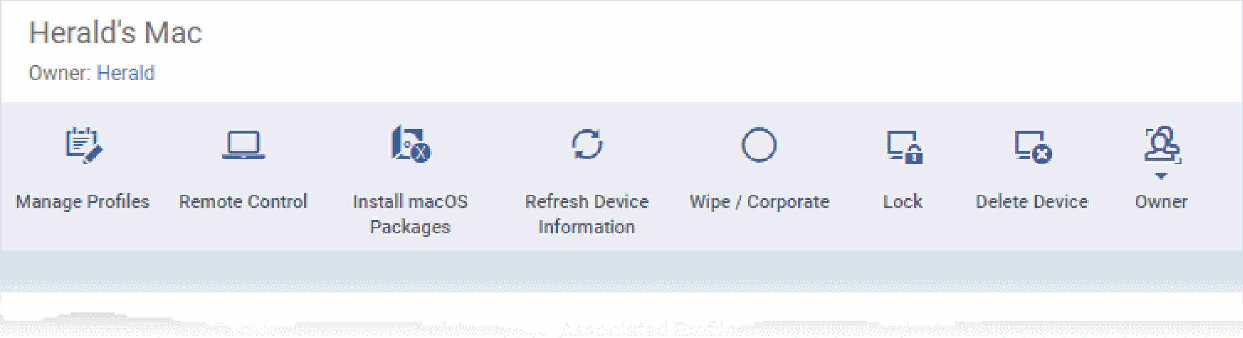
| | |
|---|---|
| OS | macOS |
| OS version | 10.13.6 |
| Build version | 17G9016 |
| Reboot time | 2019/11/14 05:23:40 PM |
| Serial number | C07N430BDWYL |

Device details are shown in seven tabs:

- **Device Name** - The device label. You can change this as per your preferences. See **View and Edit Mac OS Device Name** for more details.
- **Summary** - General details of the device, including device information, OS details, Network details and security configuration. See **Summary Information of Mac Device** for more details.
- **Installed Apps** - A list of applications currently installed on the device, along with their versions. See **View Installed Applications** for more details.
- **Associated Profiles** - Profiles deployed on the device. See **View and Manage Profiles Associated with the Device** for more details.
- **Package Installation State** - Mac OS packages that have been installed on the device via Endpoint Manager. See **View Mac OS Packages Installed on a Device through Endpoint Manager** for more details.

- **Groups** - Device groups to which the endpoint belongs. You can manage group membership from here. See **View and Manage Device Group Memberships** for more details.
- **Logs** - View events recorded on the device. This is covered in more detail in **View Mac Device Logs**.

You can run remote tasks on the device using the controls at the top of the interface:



- **Manage Profiles** - Add or remove device profiles. See **Assign Configuration Profiles to Selected Devices** for more details.
- **Remote Control** - Establish a remote desktop connection to an endpoint. See **Remote Management of Windows and Mac OS Devices** for more details
- **Install Mac OS Packages** - Remotely install Comodo Client Security (CCS) for Mac package. See **Remotely Install Packages onto Mac OS Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. See **Update Device Information** for more details.
- **Wipe / Corporate** - Delete data stored on the device if it is lost or stolen. See **Wipe Selected Devices** for more details.
- **Lock/Unlock Mac OS** - Remotely lock or unlock the device if it is lost, misplaced or stolen. See **Lock / Unlock Selected Devices** for more details.
- **Remove a Device** - Removes the device from Endpoint Manager. See **Remove a Device** for more details.
- **Owner** - Change the user with whom the device is associated. You can also change the type of device to corporate or personal. See **Change a Device's Owner** and **Change the Ownership Status of a Device** for more details.

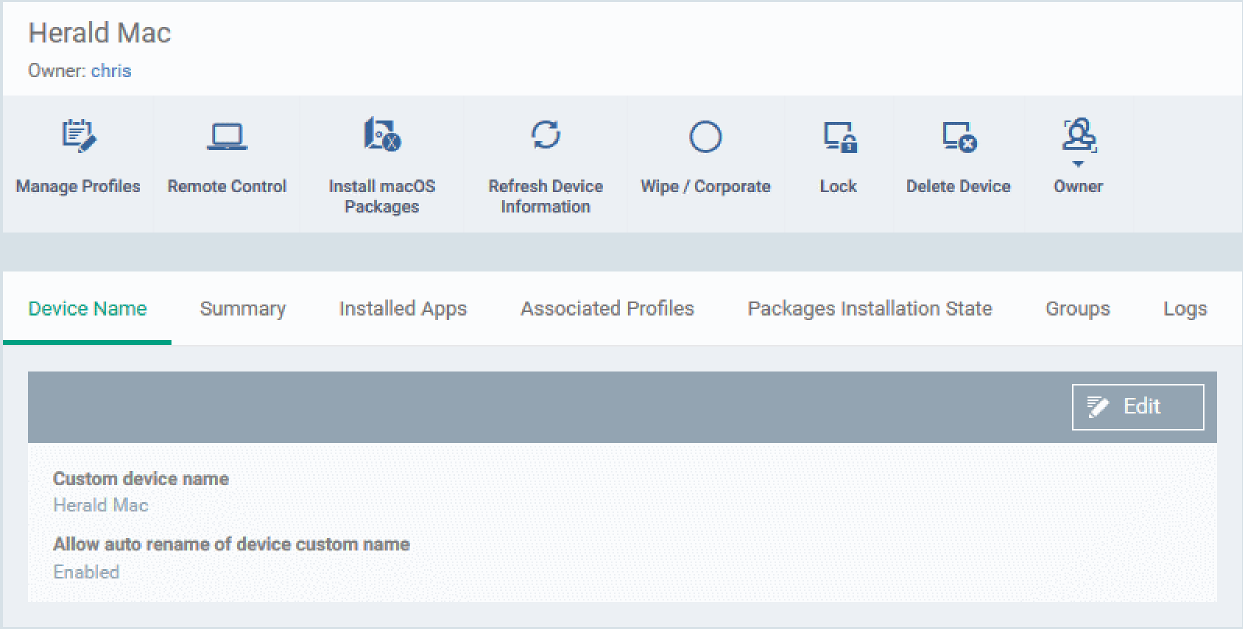
### 5.2.3.1. View and Edit Mac OS Device Name

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

**To change a device name**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' on the left to view every device enrolled to EM
- Click on any Mac OS device then select the 'Device Name' tab



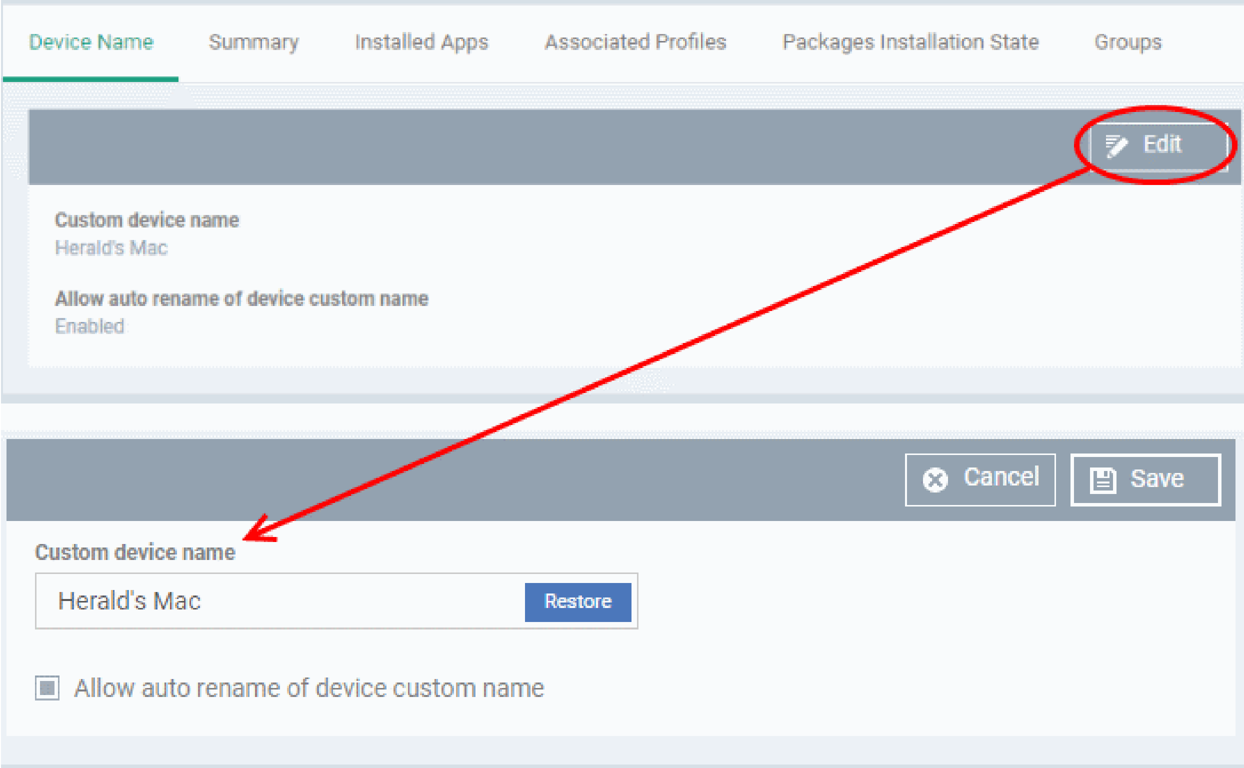
Herald Mac

Owner: chris

Custom device name
Herald Mac

Allow auto rename of device custom name
Enabled

- **Custom device name -** The current name of the device.
- **Allow auto rename of device custom name -** Enabled - The device's real name will automatically replace the custom name in this list during the next sync.
  - **Disabled** - the custom name is kept in EM
- Click the 'Edit' button at the right to change the name of the device.



Custom device name
Herald's Mac

Allow auto rename of device custom name
Enabled

Custom device name
Herald's Mac

▣ Allow auto rename of device custom name

- Enter the new name in the 'Custom Device Name' field
- Make sure the 'Allow Auto Rename of Device Custom Name' is disabled to retain the custom name in the list. If this is enabled, the custom name will be automatically replaced with the device's name or model number during the next sync with the EM communication client on the device.
- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

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

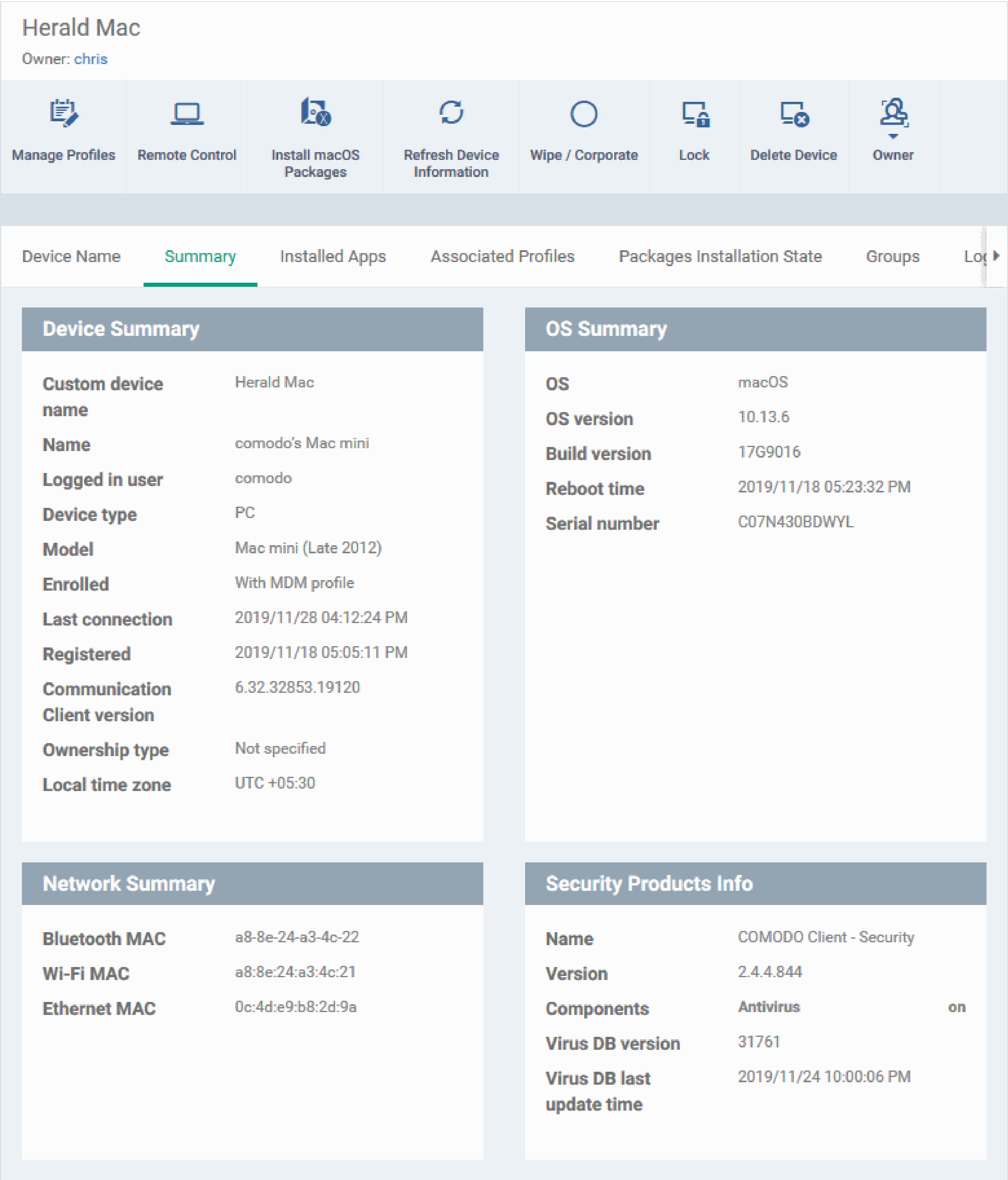
### 5.2.3.2. Summary Information of Mac Device

The 'Summary' tab shows the MAC device operating system, network connection, security configuration and more.

**View device summary**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group to view just their devices

    Or
  - Select 'Show all' to view every device add to EM
- Click on any Mac OS device then select the 'Summary' tab (if it is not already open).



Herald Mac

Owner: chris

**Device Summary**

| | |
|---|---|
| Custom device name | Herald Mac |
| Name | comodo's Mac mini |
| Logged in user | comodo |
| Device type | PC |
| Model | Mac mini (Late 2012) |
| Enrolled | With MDM profile |
| Last connection | 2019/11/28 04:12:24 PM |
| Registered | 2019/11/18 05:05:11 PM |
| Communication Client version | 6.32.32853.19120 |
| Ownership type | Not specified |
| Local time zone | UTC +05:30 |

**OS Summary**

| | |
|---|---|
| OS | macOS |
| OS version | 10.13.6 |
| Build version | 17G9016 |
| Reboot time | 2019/11/18 05:23:32 PM |
| Serial number | C07N430BDWYL |

**Network Summary**

| | |
|---|---|
| Bluetooth MAC | a8-8e-24-a3-4c-22 |
| Wi-Fi MAC | a8:8e:24:a3:4c:21 |
| Ethernet MAC | 0c:4d:e9:b8:2d:9a |

**Security Products Info**

| | | |
|---|---|---|
| Name | COMODO Client - Security | |
| Version | 2.4.4.844 | |
| Components | Antivirus | on |
| Virus DB version | 31761 | |
| Virus DB last update time | 2019/11/24 10:00:06 PM | |

- **Device Summary** - Device name, user, type, model, last sync time wit the client, whether or not MDM profile is installed, device ownership status and more.
- **OS Summary** - Details about the operating system of the device, including version and build.
- **Network Summary** - MAC addresses of the device for connection through Bluetooth, WiFi and Ethernet.
- **Security Products Info** - Details about Comodo Client Security (CCS) for Mac on the device, including version number, database version and update status.

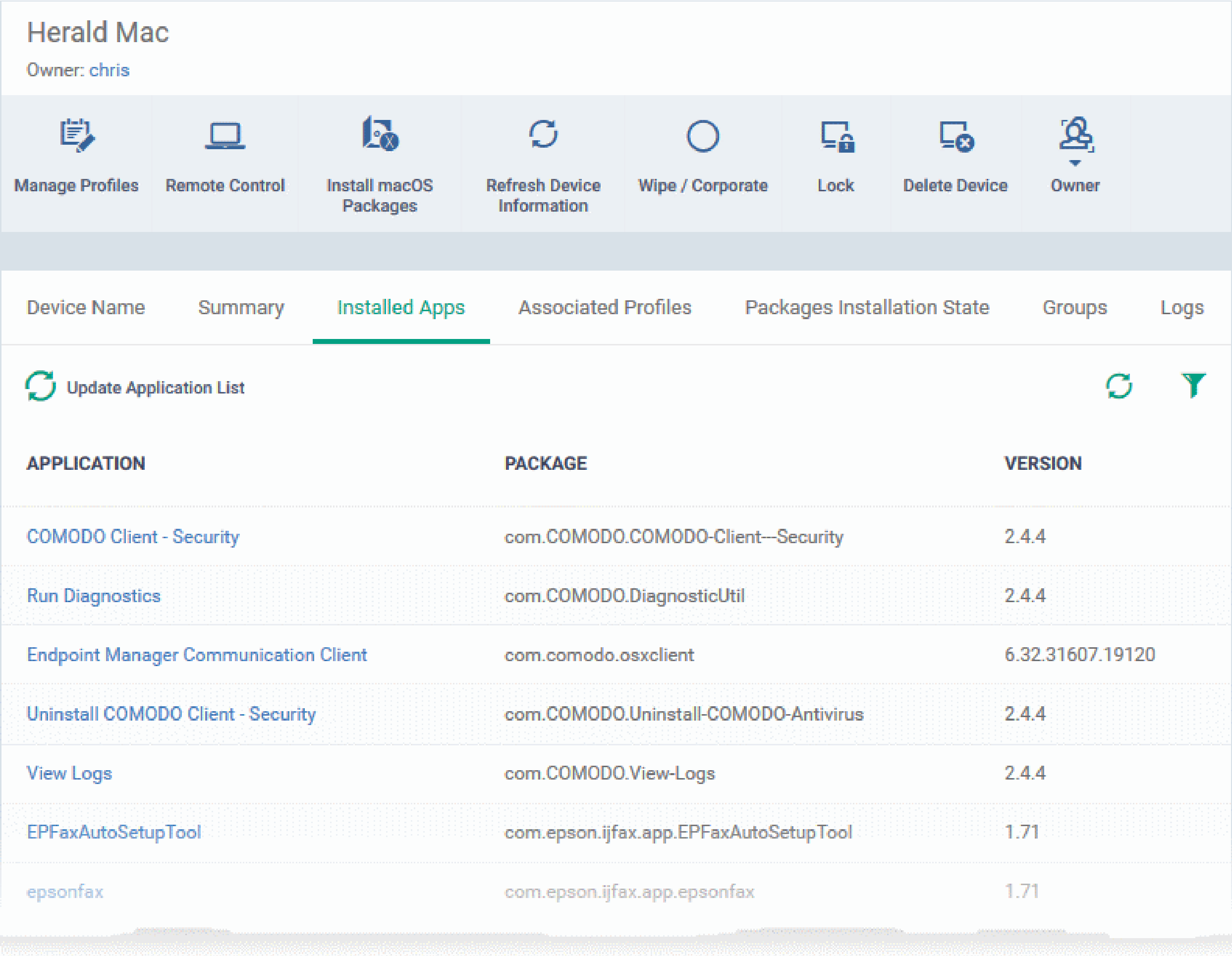
### 5.2.3.3. View Installed Applications

- The 'Installed Apps' tab shows a list of all applications installed on a device.

**View the list of applications**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Mac OS device then select the 'Installed Apps' tab


Herald Mac
Owner: chris

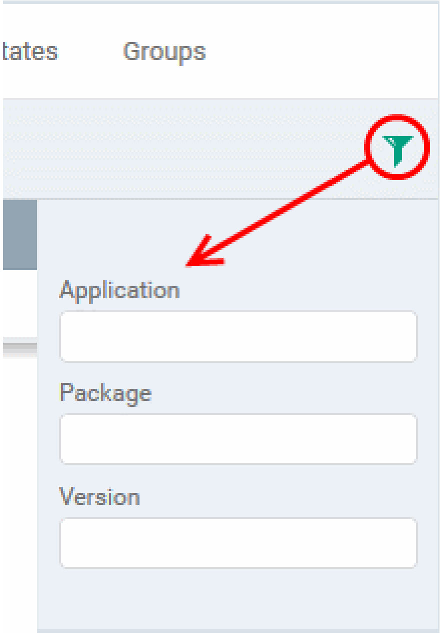
| APPLICATION | PACKAGE | VERSION |
|---|---|---|
| COMODO Client - Security | com.COMODO.COMODO-Client--Security | 2.4.4 |
| Run Diagnostics | com.COMODO.DiagnosticUtil | 2.4.4 |
| Endpoint Manager Communication Client | com.comodo.osxclient | 6.32.31607.19120 |
| Uninstall COMODO Client - Security | com.COMODO.Uninstall-COMODO-Antivirus | 2.4.4 |
| View Logs | com.COMODO.View-Logs | 2.4.4 |
| EPFaxAutoSetupTool | com.epson.ijfax.app.EPFaxAutoSetupTool | 1.71 |
| epsonfax | com.epson.ijfax.app.epsonfax | 1.71 |

| Column Heading | Description |
|---|---|
| Application | The name of the software. |

| | |
|---|---|
| | • Click the name of the application to view the list of all Mac OS devices on which the app is found.<br>• See **Manage Devices** for more details. |
| Package | The source of the application. The Mac OS package from which the application was installed. |
| Version | The version number of the application. |

## Sorting and Filtering Options

- Click any column header to sort the items in alphabetical order of entries in that column.
- Click the funnel icon on the right to open the filter options.



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

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

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

### 5.2.3.4. View and Manage Profiles Associated with a Device

The 'Associated Profiles' tab lists all currently active configuration profiles on an endpoint.

A profile can be applied to a device for any of these reasons:

- Because it is a default profile for the device's operating system.
- Because the profile was specifically applied to the device
- Because the profile was applied to the device owner. The profile is then applied to all devices that the user owns.
- Because the profile was applied to a device group. The device is a member of the group and so inherits the profile.

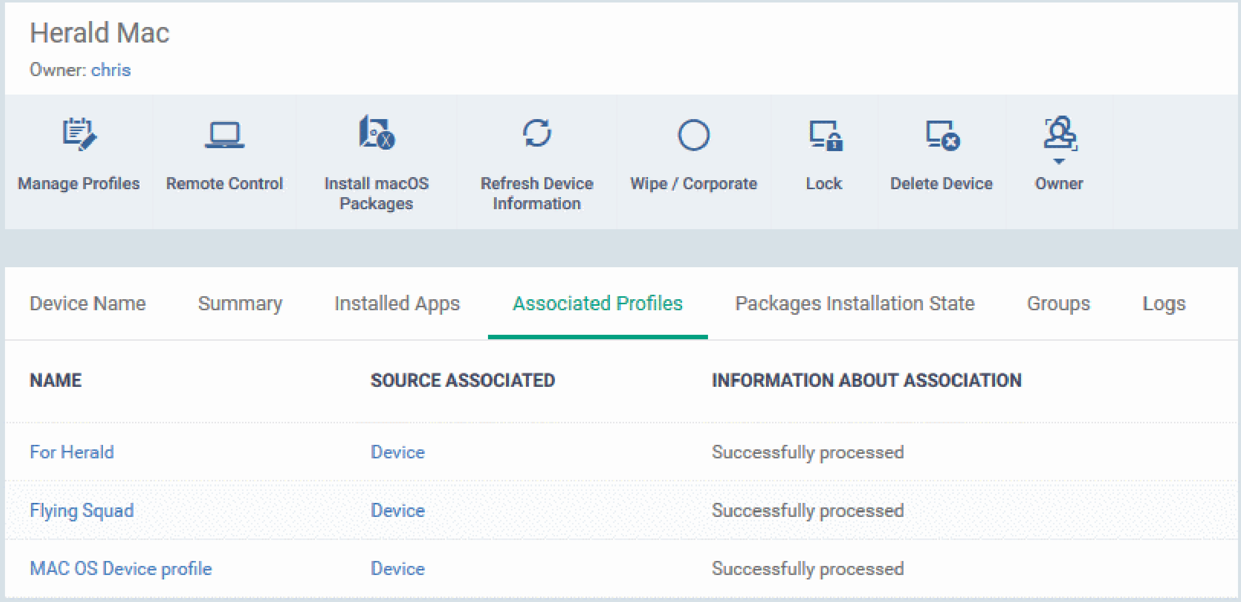
- Because the profile was applied to a user group. The device inherits the profile because its owner is a member of the user group.

See **Profiles for Mac OS Devices** for more details on configuration profiles.

**View and manage profiles associated with a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Mac OS device then select the 'Associated Profiles' tab



| NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSOCIATION |
|---|---|---|
| For Herald | Device | Successfully processed |
| Flying Squad | Device | Successfully processed |
| MAC OS Device profile | Device | Successfully processed |

| Column Heading | Description |
|---|---|
| Name | The profile label.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Source Associated | How the profile was applied to the device. Profiles can be applied to a device in different ways:<br>• **Profile was directly applied to a device**. See **View and Manage Profiles Associated with a Device** for more details<br>• **Profile was applied to a user**. These profiles are in-turn deployed to all devices belonging to the user. See **Assign Configuration Profiles to a Users' Devices** for more details<br>• **Profile was applied to a user group**. These profiles are deployed to all devices owned by group members. See **Assign Configuration Profile to a User Group** for more details<br>• **Profile was applied to a device group**. These profiles are deployed to all devices in the group. See **Assign Configuration Profile to a Device Group** for more details<br>• Click the source to view and manage profiles associated with that source. |

| | |
|---|---|
| Information about Association | Whether the profile has been successfully applied to the device or is pending. |

- Click the 'Name' column header to sort the items in the alphabetical order of the names of the items.

### Add or Remove Profiles

- Click 'Manage Profiles' to add or remove profiles. See **View and Manage Profiles Associated with a Device** for a full overview of this interface.

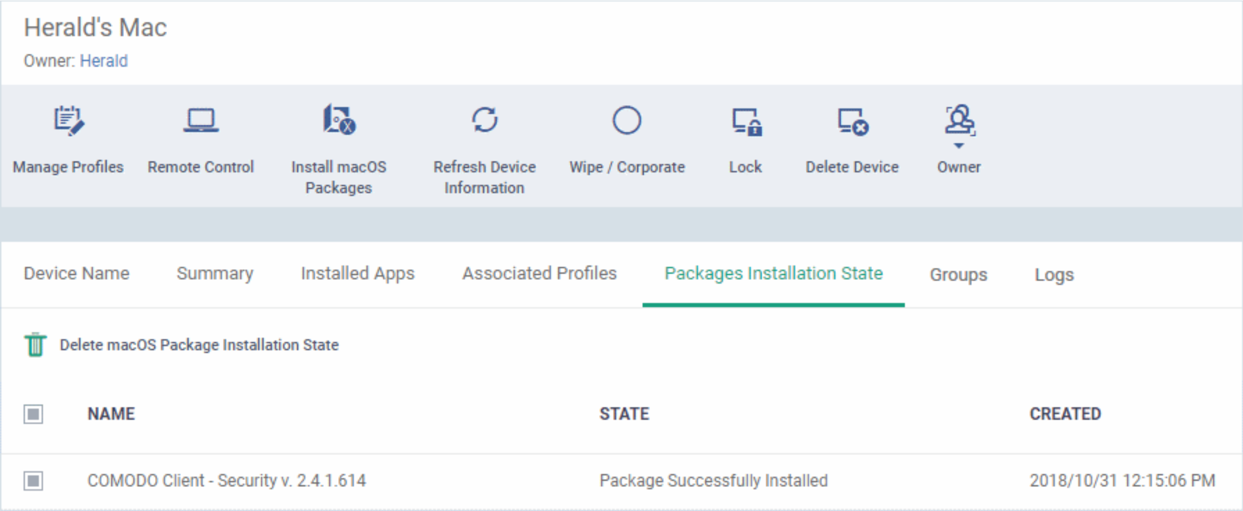
### 5.2.3.5. View Mac OS Packages Installed on a Device through Endpoint Manager

- Endpoint Manager lets you remotely install packages on managed Mac OS endpoints.

**Note**: Currently only CCS can be remotely installed on Mac OS devices from EM. Support for other EM packages and third party Mac OS packages will be available in the future versions.

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

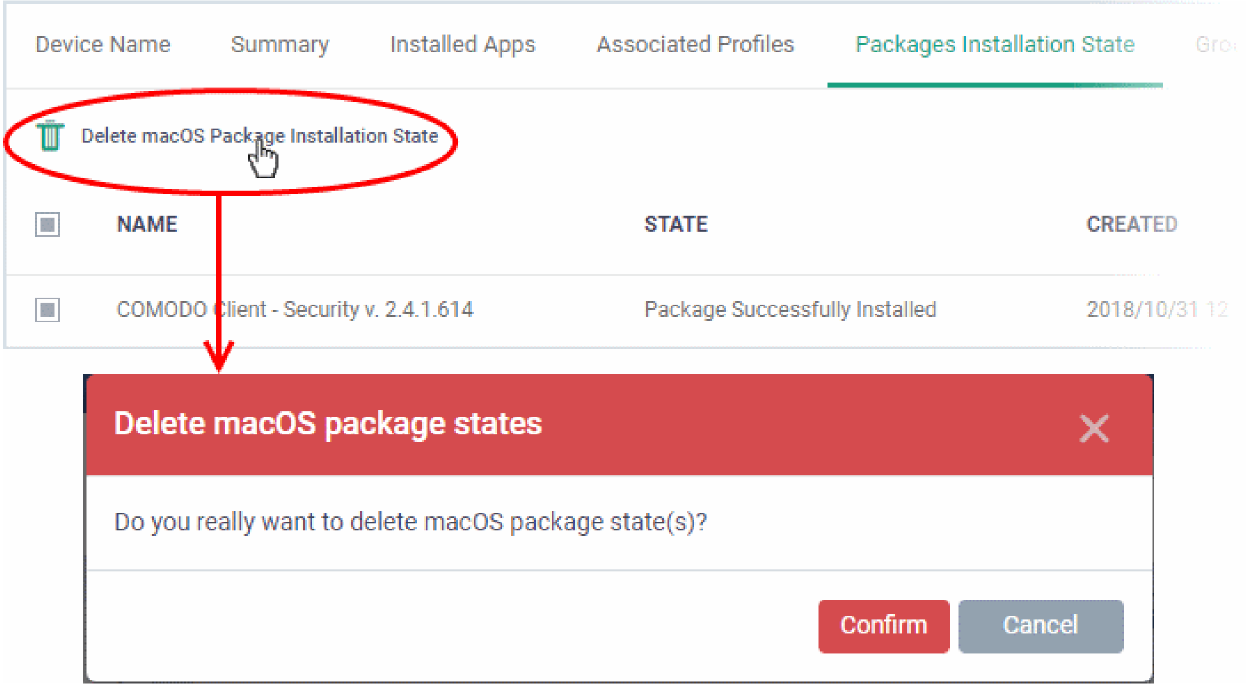
    Or
  - Select 'Show all' to view every device added to EM
- Click on any Mac OS device then select the 'Packages Installation State' tab



| ☐ | NAME | STATE | CREATED |
|---|---|---|---|
| ☐ | COMODO Client - Security v. 2.4.1.614 | Package Successfully Installed | 2018/10/31 12:15:06 PM |

| Column Heading | Description |
|---|---|
| Name | The label of the installation package. |
| State | Whether the installation was successful or not |
| Created | The date and time at which the installation command was sent. |

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Select an entry and click 'Delete mac OS Package Installation State' to remove it from the list.


Device Name
Summary
Installed Apps
Associated Profiles
Packages Installation State
Gro
Delete macOS Package Installation State

| ☐ | NAME | STATE | CREATED |
|---|---|---|---|
| ☐ | COMODO Client - Security v. 2.4.1.614 | Package Successfully Installed | 2018/10/31 12 |

**Delete macOS package states**

Do you really want to delete macOS package state(s)?

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

Note - the entry will be removed from the list but the package will not be uninstalled from the device.

More reading - see **Remotely Install Packages on Mac OS Devices**.

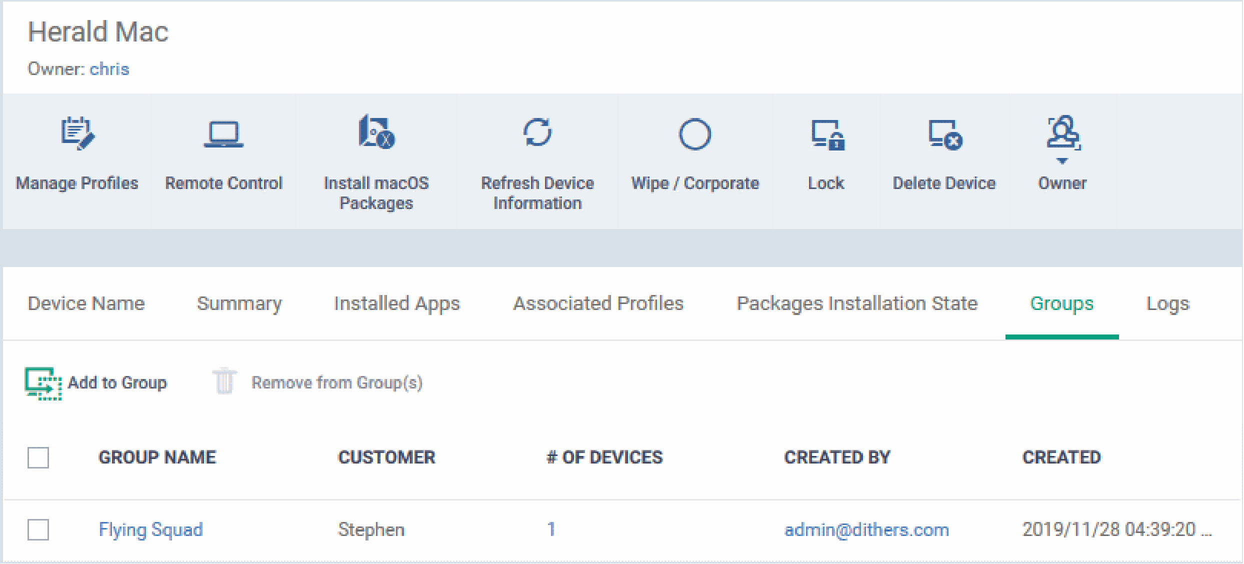
### 5.2.3.6. View and Manage Device Group Memberships

- Device groups let you deploy policies to multiple devices at once.

**Manage device group memberships**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of a Mac OS device then select 'the 'Groups' tab


Herald Mac

Owner: chris

| ☐ | GROUP NAME | CUSTOMER | # OF DEVICES | CREATED BY | CREATED |
|---|---|---|---|---|---|
| ☐ | Flying Squad | Stephen | 1 | admin@dithers.com | 2019/11/28 04:39:20 ... |

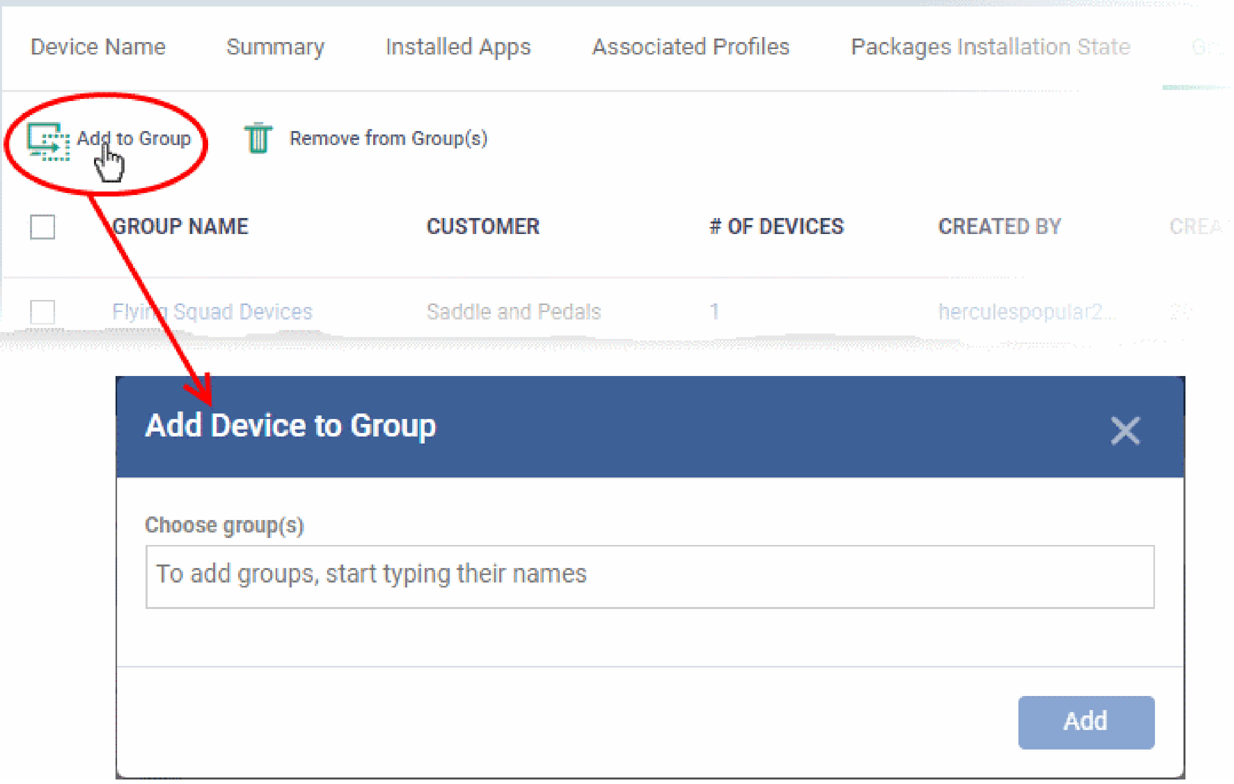
- The interface lists all groups of which the device is a member.
- Group profiles will also be applied to the endpoint.

See **Assign Configuration Profiles to a Device Group**, for more details about applying configuration profiles to device groups.

| Column Heading | Description |
|---|---|
| Group | The group label.<br>• Click the group name to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Customer | The name of the company for which the group was created. |
| Number of Devices | The total count of devices in the group.<br>• Click the number to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Created By | Name of the admin who created the group.<br>• Click the name to view the admin's details.<br>• See **View the Details of a User** for more details. |
| Created | The date and time at which the group was created. |

### Add the device to a new group

- Click 'Add to Group'
- Select the group to which you want to add the device:



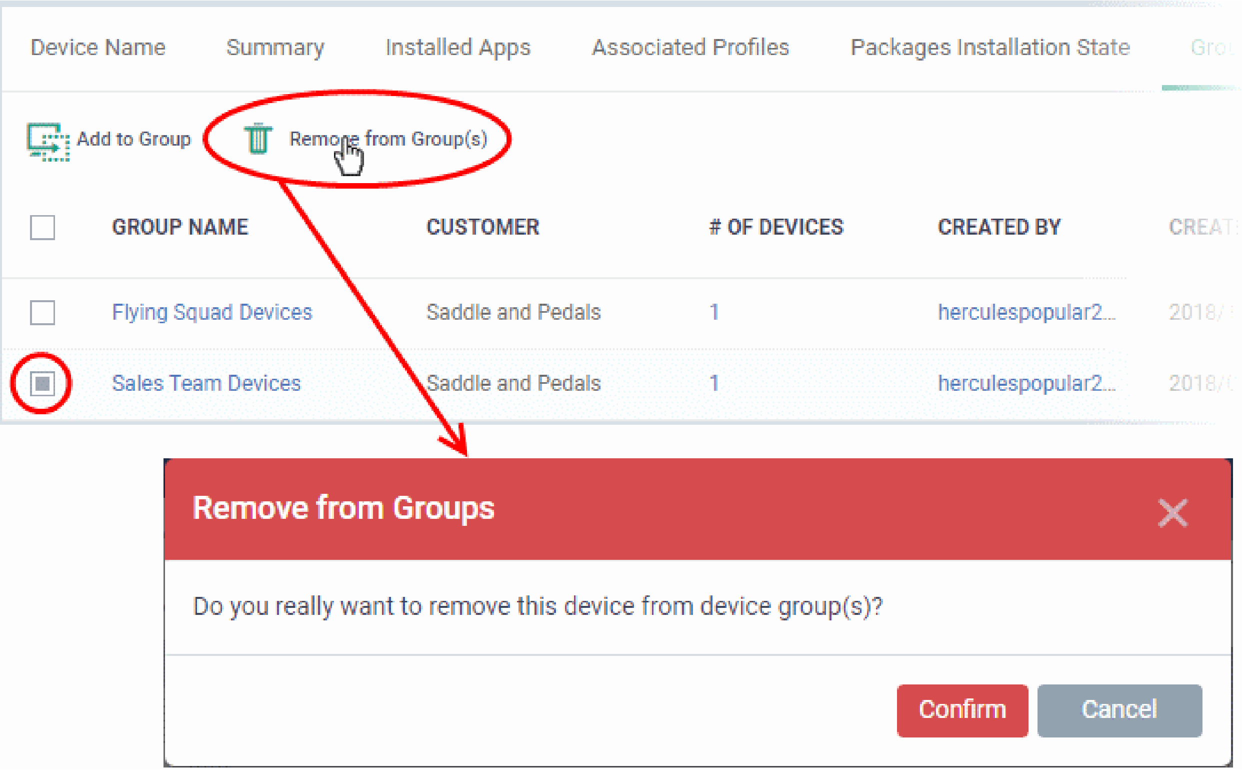
- Start entering the name of the group to which the device has to be associated in the 'Choose Group(s)' field and choose the group from the options.

- Repeat the process to add the device to other groups.
- Click 'Add'.

The device will be added to the group.

**Remove the device from a group**

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



| ☐ | GROUP NAME | CUSTOMER | # OF DEVICES | CREATED BY | CREAT |
|---|---|---|---|---|---|
| ☐ | Flying Squad Devices | Saddle and Pedals | 1 | herculespopular2... | 2018/ |
| ☑ | Sales Team Devices | Saddle and Pedals | 1 | herculespopular2... | 2018/ |

Remove from Groups

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

- Click 'Confirm' to remove the device from the selected groups.

Note - Any group profiles will also be removed from the device.

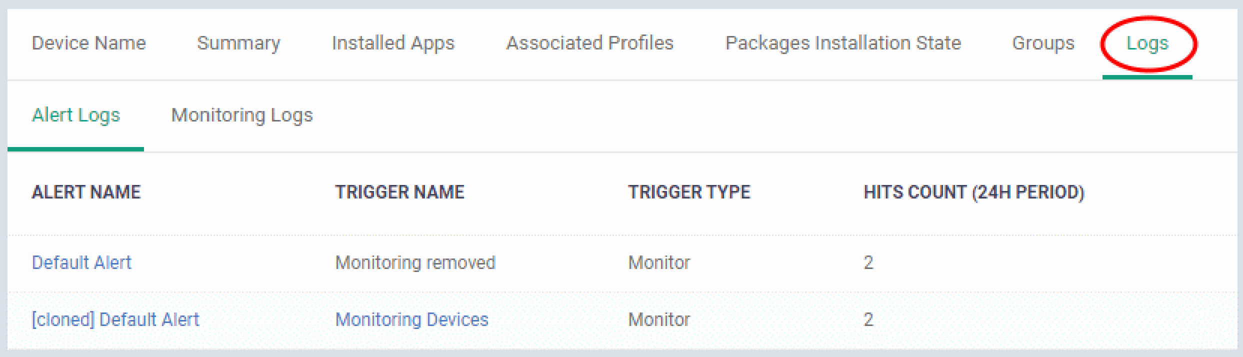
### 5.2.3.7. View Mac Device Logs

The 'Logs' tab shows all events that occurred on a specific device. This contrasts to 'Dashboard' > '**Audit Logs**', which shows events on all devices.

**View device logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    OR
  - Select 'Show all' to view every device enrolled to EM
- Click the name of a Mac OS device
- Click the 'Logs' tab



| ALERT NAME | TRIGGER NAME | TRIGGER TYPE | HITS COUNT (24H PERIOD) |
|---|---|---|---|
| Default Alert | Monitoring removed | Monitor | 2 |
| [cloned] Default Alert | Monitoring Devices | Monitor | 2 |

There are two types of logs, each shown on a different tab. Each row on these tabs is a specific event.

Click on the following for details about each type of log:

- **Alert Logs**
- **Monitoring Logs**

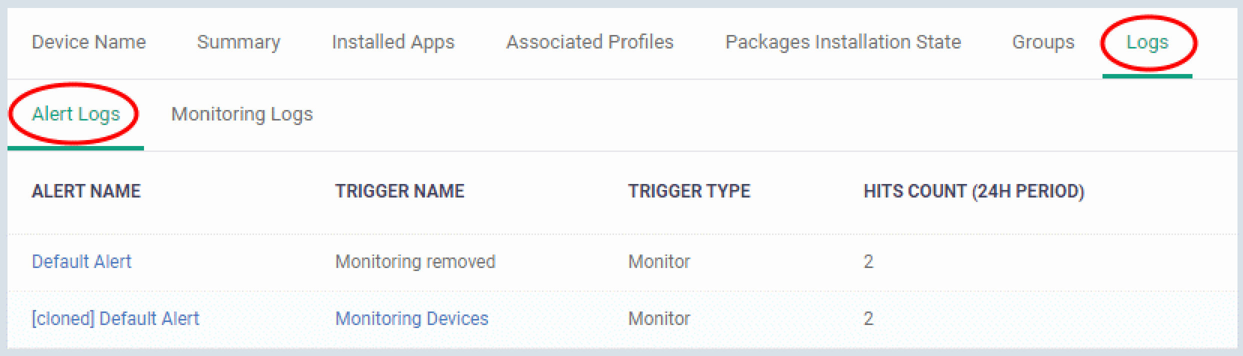
## View Alert Logs

A record of all events where an alert was generated on the endpoint. For example, logs are generated a breach of monitoring conditions.

View alert logs

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Mac OS device then select the 'Logs' tab
- Select 'Alert Logs'



| ALERT NAME | TRIGGER NAME | TRIGGER TYPE | HITS COUNT (24H PERIOD) |
|---|---|---|---|
| Default Alert | Monitoring removed | Monitor | 2 |
| [cloned] Default Alert | Monitoring Devices | Monitor | 2 |

| Alert Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Alert Name | The alert template used in the event.<br>• An alert template is just a collection of settings that determines alert recipients, information included, priority etc. The template does not specify the condition under which the alert is generated.<br>• The 'Trigger Name' is the actual monitor that generated the alert.<br>• In the standard workflow, all monitors have the 'Default Alert' template applied |

| | |
|---|---|
| | to them. Click 'Configuration' > 'Templates' > 'Alerts' > 'Default Alert' to view the settings in the default template.<br>• You can also create your own alert templates. See '**Manage Alerts**' for more details.<br>• Click the alert name to view and configure its settings. |
| Trigger Name | The monitor that generated the alert.<br>• You can create a monitor to watch activity on a device and alert you if certain conditions are met.<br>• For example, 'alert me if disk usage exceeds 90%' on a device.<br>• Click the monitor name to view and configure its settings<br>• See **Manage Monitors** for more details. |
| Trigger Type | The possible value is 'Monitor' |
| Hits Count (24 H Period) | The number of times this condition was triggered in the past 24 hours. |

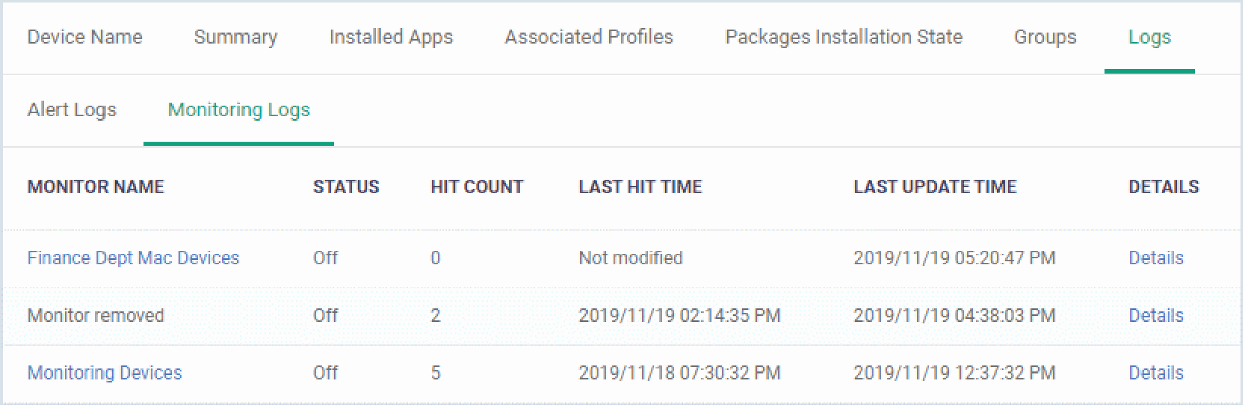
## View Monitoring Logs

- Monitors are scripts which keep track of specific items on a device. For example, you may set a monitor to track disk usage does not exceed a certain percentage.
- Monitors can be added to the 'Monitoring' section of a configuration profile
- Monitoring logs are shown for the past 24 hours.
  - See **Monitors for Mac OS Devices** for help to create monitors.
  - See **Monitor settings for Mac OS Profile** for help to add monitors to profiles

**View monitoring logs**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the Mac OS device then select the 'Logs' tab
- Click 'Monitoring Logs'

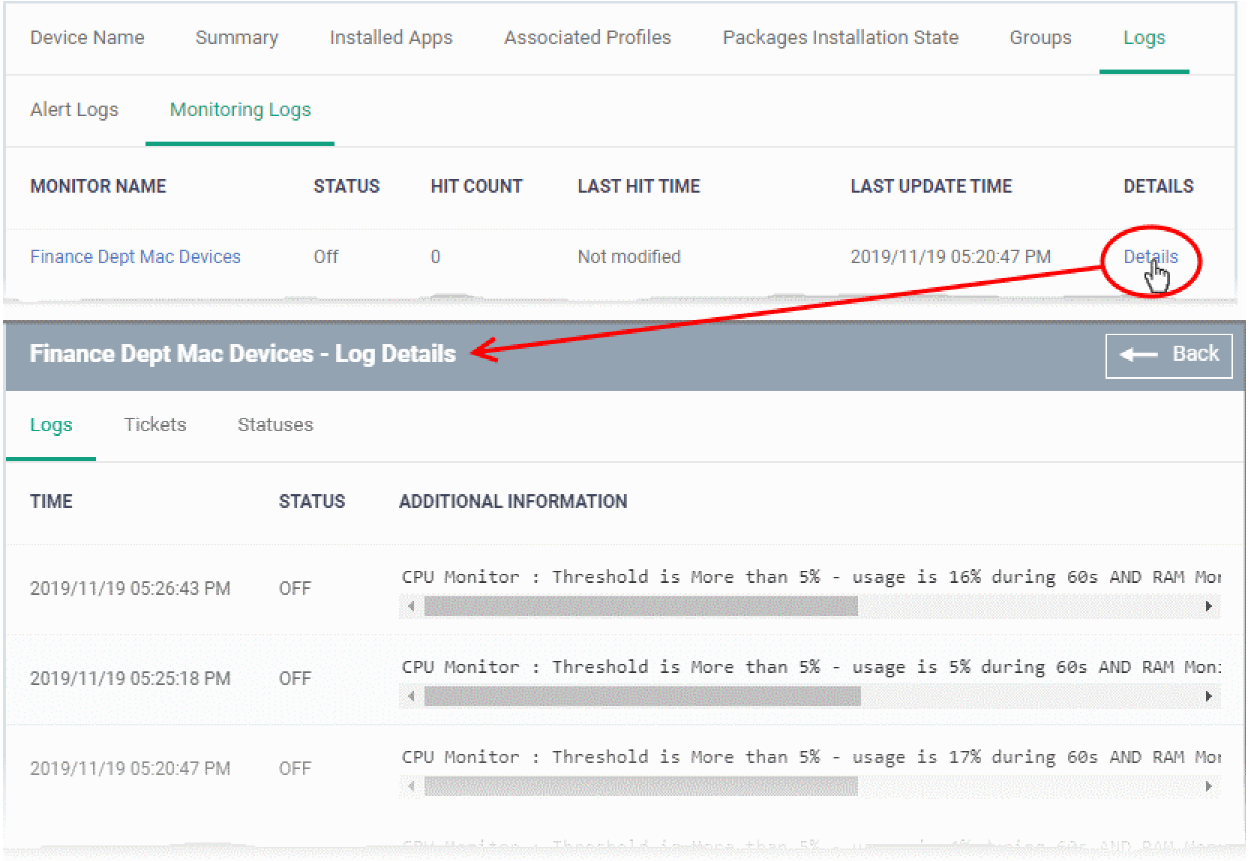


| MONITOR NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| Finance Dept Mac Devices | Off | 0 | Not modified | 2019/11/19 05:20:47 PM | Details |
| Monitor removed | Off | 2 | 2019/11/19 02:14:35 PM | 2019/11/19 04:38:03 PM | Details |
| Monitoring Devices | Off | 5 | 2019/11/18 07:30:32 PM | 2019/11/19 12:37:32 PM | Details |

| Monitoring Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The monitor that was triggered to create the log.<br>• Click the name to view and manage the conditions of the monitor.<br>• See **Manage Monitors** for more details. |
| Status | Whether or not the monitor is currently active on the device. |
| Hit Count | The number of times the monitored condition was breached in the last 24 hours. |
| Last Hit Time | Date and time the condition was last broken. |
| Last Update Time | Date and time when the information was last refreshed. |
| Details | • Click the 'Details' link to view a log of the breach events.<br>• See **View Details of Monitoring Logs** (given below) for more information. |

## View Details of Monitoring Logs

- Click the 'Details' link to view event information and the conditions of a monitor:



| MONITOR NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| Finance Dept Mac Devices | Off | 0 | Not modified | 2019/11/19 05:20:47 PM | Details |

Finance Dept Mac Devices - Log Details

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/11/19 05:26:43 PM | OFF | CPU Monitor : Threshold is More than 5% - usage is 16% during 60s AND RAM Mor |
| 2019/11/19 05:25:18 PM | OFF | CPU Monitor : Threshold is More than 5% - usage is 5% during 60s AND RAM Mon: |
| 2019/11/19 05:20:47 PM | OFF | CPU Monitor : Threshold is More than 5% - usage is 17% during 60s AND RAM Mor |

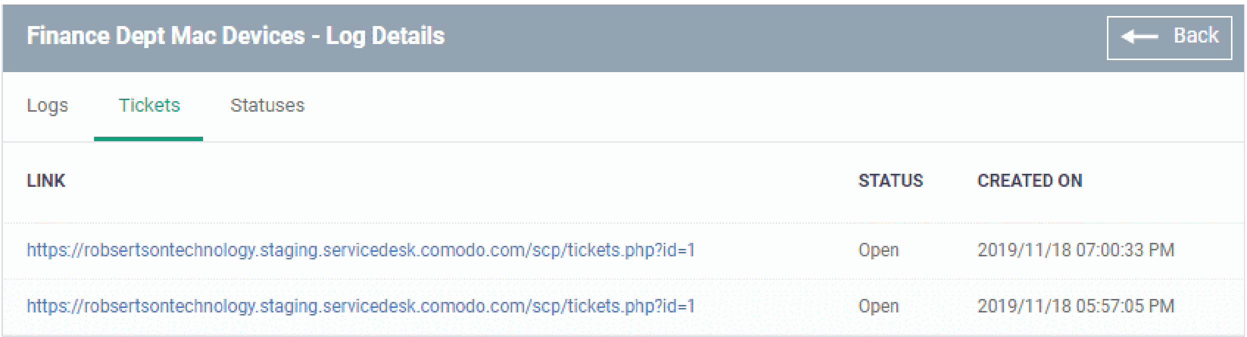
Details are shown under three tabs:

**Logs -** The date and time when the event occurred. Also shows details about the monitoring rule that detected the event.

| Monitoring Log Details - 'Logs' tab - Table of Column Descriptions |
|---|

| Column Heading | Description |
|---|---|
| Time | Date and time of the event. |
| Status | The current status of the monitored condition on the device. |
| Additional Information | Details on the condition monitored and the breach |

**Tickets** - Shows any service desk tickets created by the events.

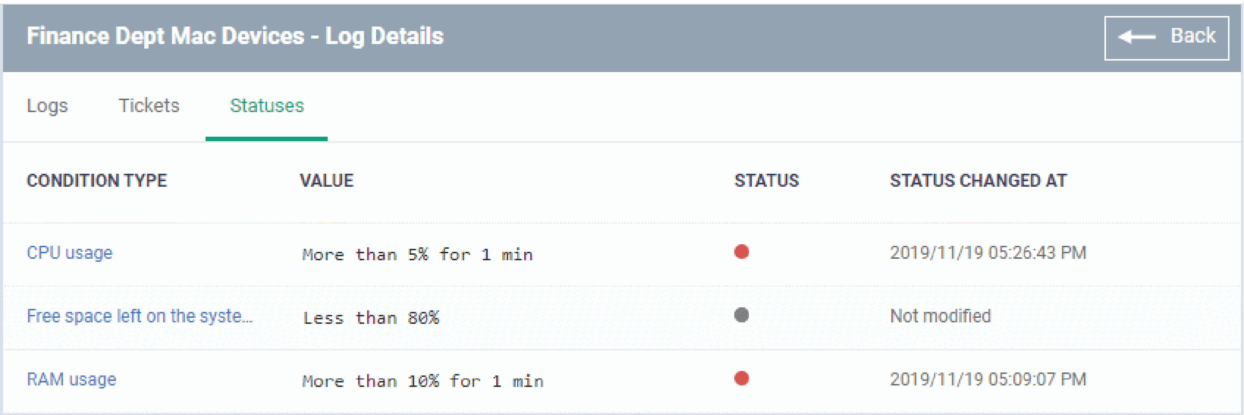


Finance Dept Mac Devices - Log Details

| LINK | STATUS | CREATED ON |
|---|---|---|
| https://robsertsontechnology.staging.servicedesk.comodo.com/scp/tickets.php?id=1 | Open | 2019/11/18 07:00:33 PM |
| https://robsertsontechnology.staging.servicedesk.comodo.com/scp/tickets.php?id=1 | Open | 2019/11/18 05:57:05 PM |

| Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

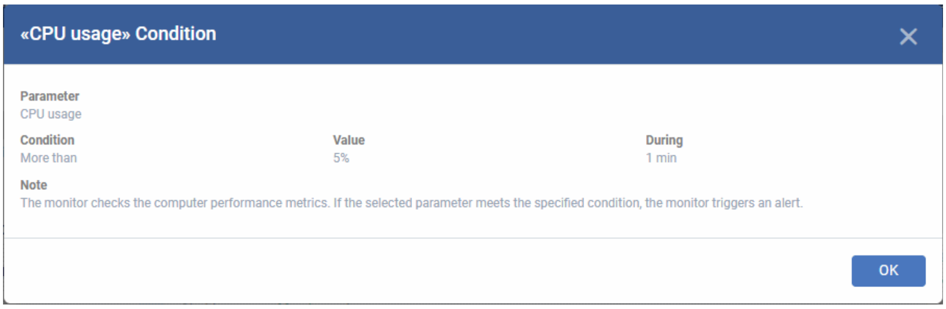
**Statuses** - Shows the current status of all conditions monitored on the device.



Finance Dept Mac Devices - Log Details

| CONDITION TYPE | VALUE | STATUS | STATUS CHANGED AT |
|---|---|---|---|
| CPU usage | More than 5% for 1 min | ● | 2019/11/19 05:26:43 PM |
| Free space left on the syste... | Less than 80% | ● | Not modified |
| RAM usage | More than 10% for 1 min | ● | 2019/11/19 05:09:07 PM |

| Monitoring Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Condition Type | The observed parameter of the monitor.<br>Click the condition to view the details of the monitored parameter and configured |

| | |
|---|---|
| | thresholds. An example is shown below:<br><br>«CPU usage» Condition<br>Parameter: CPU usage<br>Condition: More than<br>Value: 5%<br>During: 1 min<br>Note: The monitor checks the computer performance metrics. If the selected parameter meets the specified condition, the monitor triggers an alert.<br>OK |
| Value | The thresholds set for the parameter. |
| Status | Current state of the monitored parameter.<br>• Green - The device is operating within the thresholds of the monitored condition.<br>• Grey - Unknown<br>• Red - The device is exceeding the thresholds of the monitored condition. |
| Status Changed at | The date and time of the most recent change to the monitor status. |

## 5.2.4. Manage Linux Devices

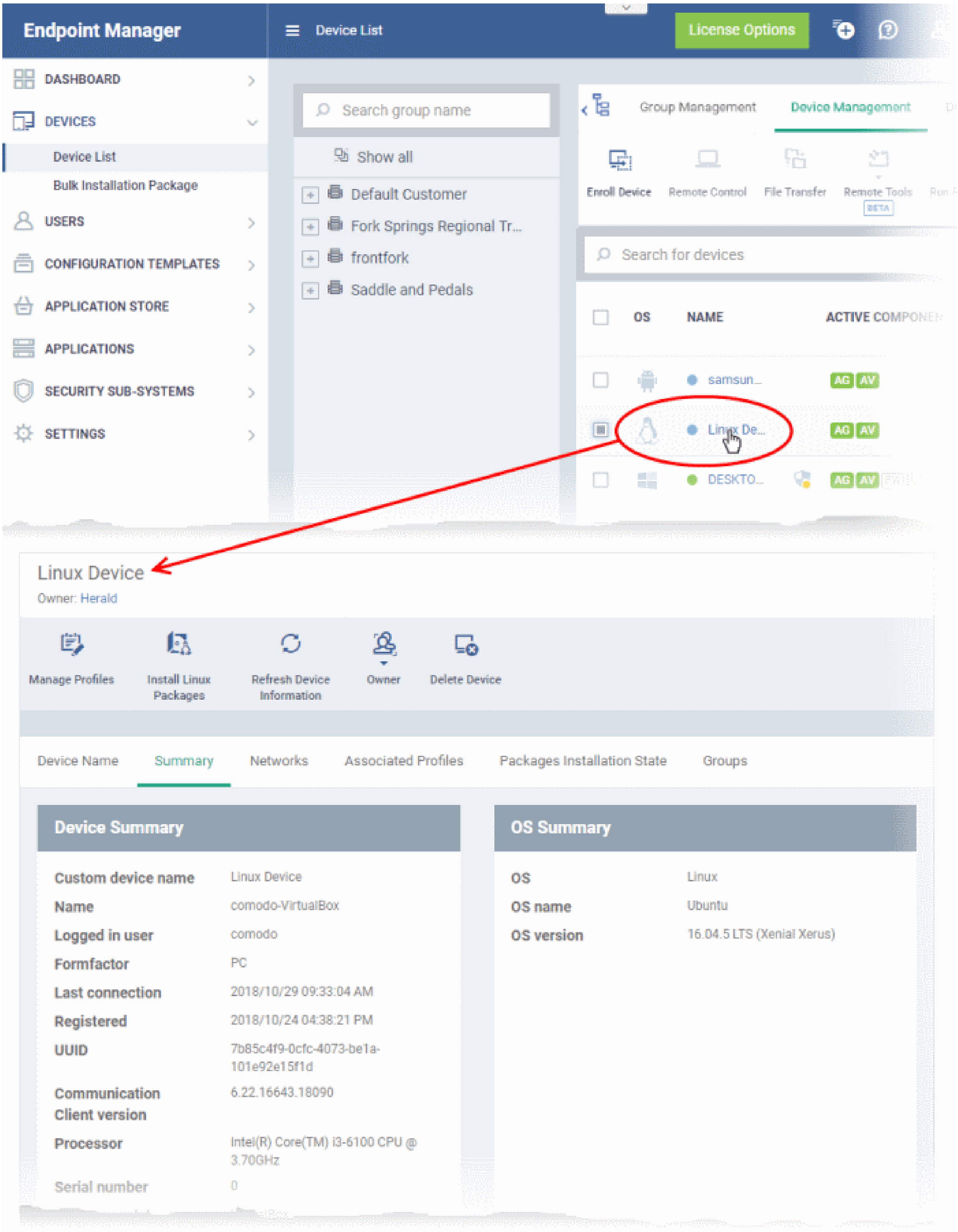
The details page of a Linux device shows OS and software data, security info from Comodo Client Security and other information. The screen also lets you manage endpoint profiles, remotely install Linux packages and configure group membership.

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

**To view and manage a Linux device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group in the middle column to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of any Linux device to open its 'Device Details' pane:



**Device Summary**

| | |
|---|---|
| Custom device name | Linux Device |
| Name | comodo-VirtualBox |
| Logged in user | comodo |
| Formfactor | PC |
| Last connection | 2018/10/29 09:33:04 AM |
| Registered | 2018/10/24 04:38:21 PM |
| UUID | 7b85c4f9-0cfc-4073-be1a-101e92e15f1d |
| Communication Client version | 6.22.16643.18090 |
| Processor | Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz |
| Serial number | 0 |

**OS Summary**

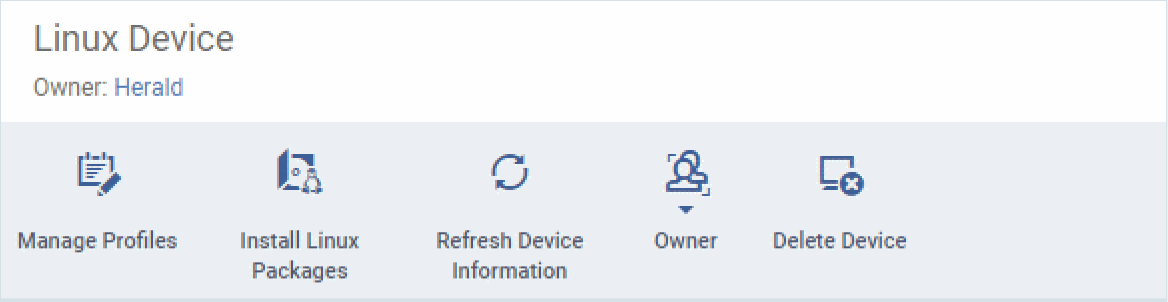
| | |
|---|---|
| OS | Linux |
| OS name | Ubuntu |
| OS version | 16.04.5 LTS (Xenial Xerus) |

Device details are shown in six tabs:

- **Device Name** - The device label. You can change this as per your preferences. See **View and Edit Linux Device Name** for more details.
- **Summary** - General details of the device, including device information, OS details and security configuration. See **View Summary Information of Linux Device** for more details.

- **Networks** - Information about the network to which the device is connected, MAC address, IP address, and more. See **View Network Information of a Linux Device** for more details.
- **Associated Profiles** - Profiles deployed on the device. See **View and Manage Profiles Associated with a Linux Device** for more details.
- **Packages Installation State** - Linux packages that have been installed on the device via Endpoint Manager. See **View Linux Packages Installed on a Device through Endpoint Manager** for more details.
- **Groups** - Device groups to which the device belongs. You can manage group membership from here. See **View and Manage Device Group Memberships** for more details

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



- **Manage Profiles** - Add or remove device profiles. See **Assign Configuration Profiles to Selected Devices** for more details.
- **Install Linux Packages** - Remotely install Comodo Client Security for Linux package. See **Remotely Install Packages on Linux Devices** for more details.
- **Refresh Information** - Contacts the device and updates displayed information. See **Update Device Information** for more details.
- **Owner** - Change the user with whom the device is associated. You can also change the type of device to corporate or personal. See **Change a Device's Owner** and **Change the Ownership Status of a Device** for more details.
- **Delete Device** - Removes the device from Endpoint Manager. See **Remove a Device** for more details.

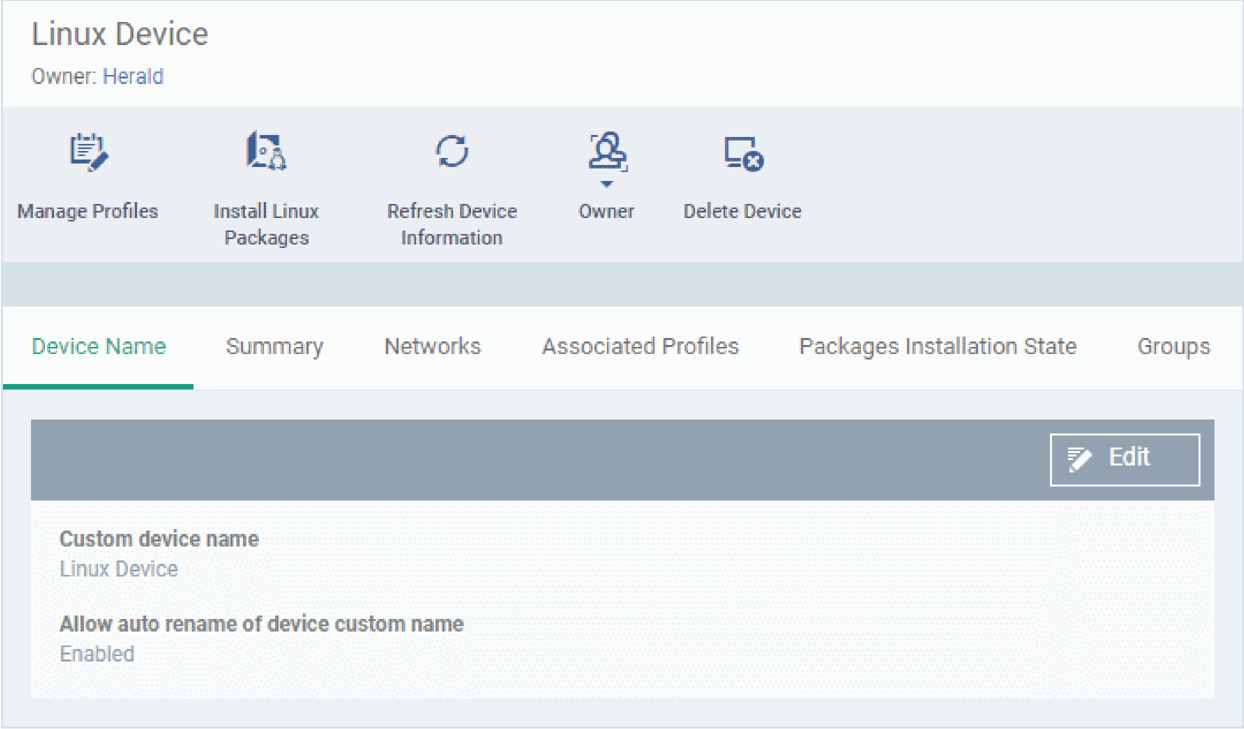
### 5.2.4.1. View and Edit Linux Device Name

- Enrolled devices are listed by the name assigned to them by their owner.
- If no name was assigned then the actual device name or model number is used.
- Admins can change the device name as required. Name changes apply only in Endpoint Manager. The name will not change on the endpoint itself.
- 'Allow Auto Rename of Device Custom Name' - If enabled, the custom name will be replaced by the device name/model number during the next sync. Disable this option if you want to keep the custom name.

**To change a device name**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' on the left to view every device enrolled to EM
- Click on any Linux device then select the 'Device Name' tab

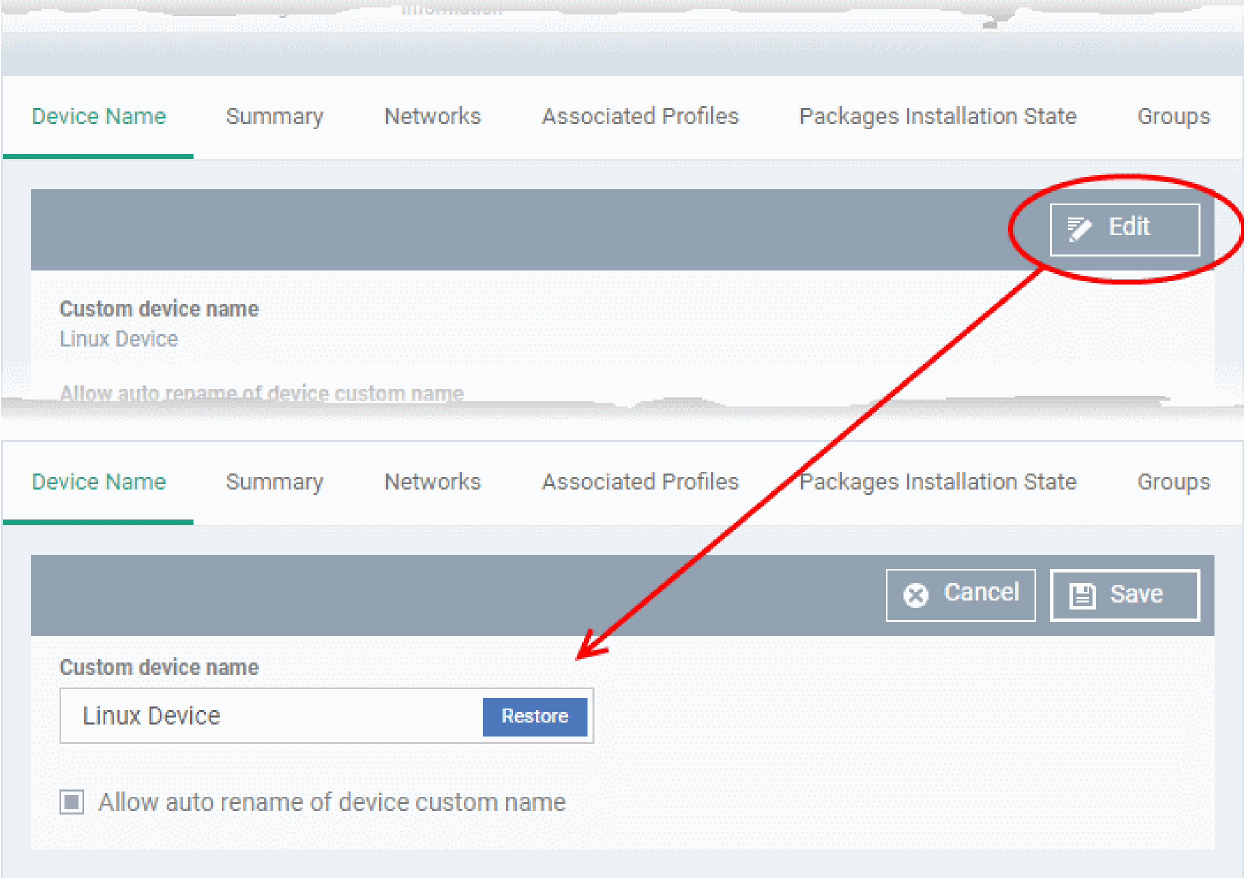


Custom device name
Linux Device

Allow auto rename of device custom name
Enabled

- **Custom device name** - The current name of the device.
- **Allow auto rename of device custom name -** Enabled - The device's real name will automatically replace the custom name in this list during the next sync. Disabled - the custom name is kept in EM

- Click the 'Edit' button at the right to change the name of the device.



Custom device name
Linux Device

Allow auto rename of device custom name

Custom device name
Linux Device

□ Allow auto rename of device custom name

- Enter the new name in the 'Custom Device Name' field

  - Make sure the 'Allow Auto Rename of Device Custom Name' is disabled to retain the custom name in the list. If this is enabled, the custom name will be automatically replaced with the original device's name or model number during the next sync with the communication client on the device.
- Click 'Save' for your changes to take effect.

The device will be listed with its new name.

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

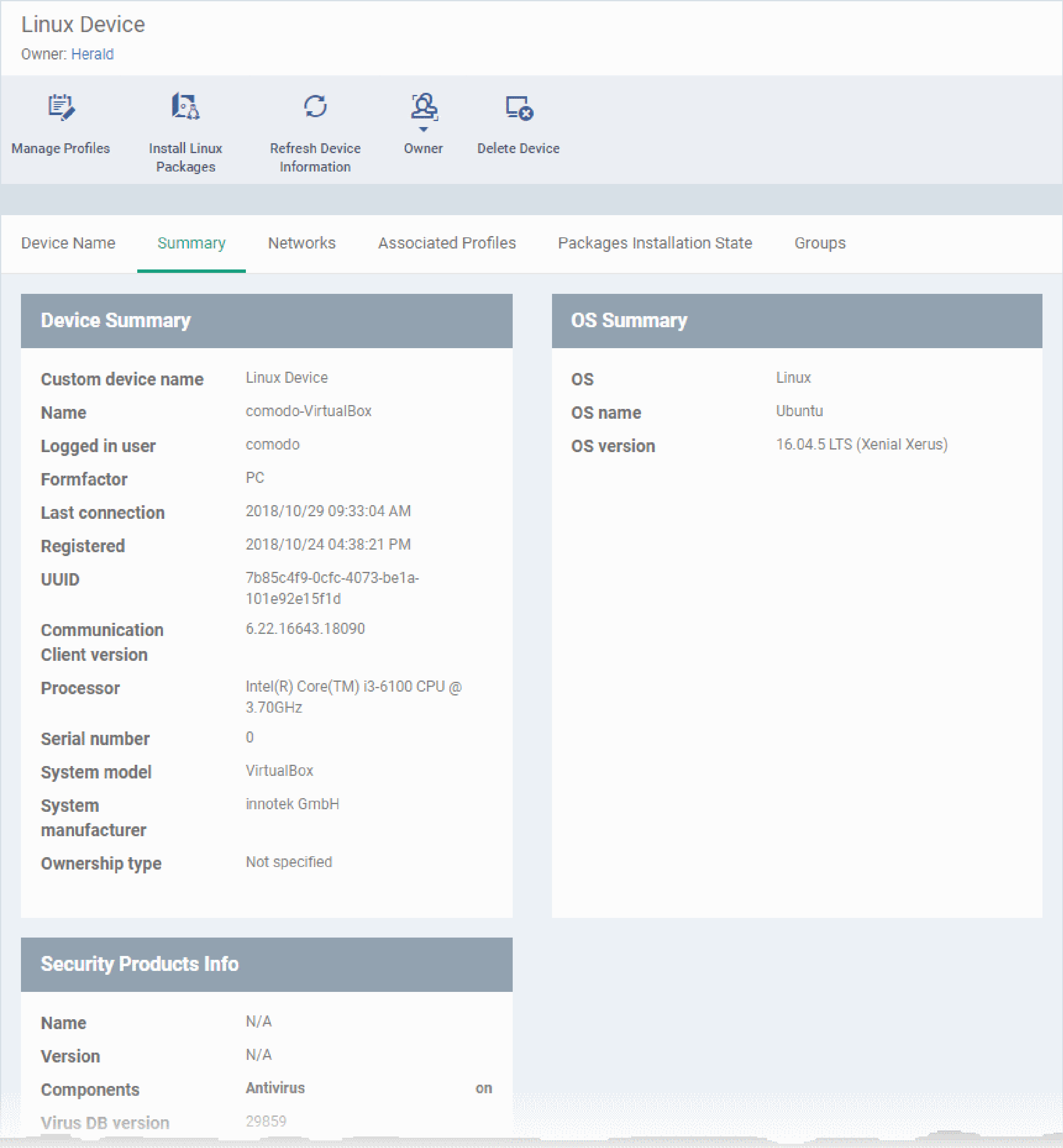
### 5.2.4.2. Summary Information of Linux Device

The 'Summary' tab contains information about the device, its operating system and Comodo Client Security (CCS) version.

**To view the device summary**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Linux device then select the 'Summary' tab (if it is not already open).



**Device Summary**

| | |
|---|---|
| Custom device name | Linux Device |
| Name | comodo-VirtualBox |
| Logged in user | comodo |
| Formfactor | PC |
| Last connection | 2018/10/29 09:33:04 AM |
| Registered | 2018/10/24 04:38:21 PM |
| UUID | 7b85c4f9-0cfc-4073-be1a-101e92e15f1d |
| Communication Client version | 6.22.16643.18090 |
| Processor | Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz |
| Serial number | 0 |
| System model | VirtualBox |
| System manufacturer | innotek GmbH |
| Ownership type | Not specified |

**OS Summary**

| | |
|---|---|
| OS | Linux |
| OS name | Ubuntu |
| OS version | 16.04.5 LTS (Xenial Xerus) |

**Security Products Info**

| | | |
|---|---|---|
| Name | N/A | |
| Version | N/A | |
| Components | Antivirus | on |
| Virus DB version | 29859 | |

- **Device Summary -** Device name, user, type, model, last sync time with the client, device ownership status and more.
- **OS Summary -** Details about the operating system of the device, including version and build.
- **Security Products Info -** Details about Comodo Client Security (CCS) on the device, including version number, database version and update status.

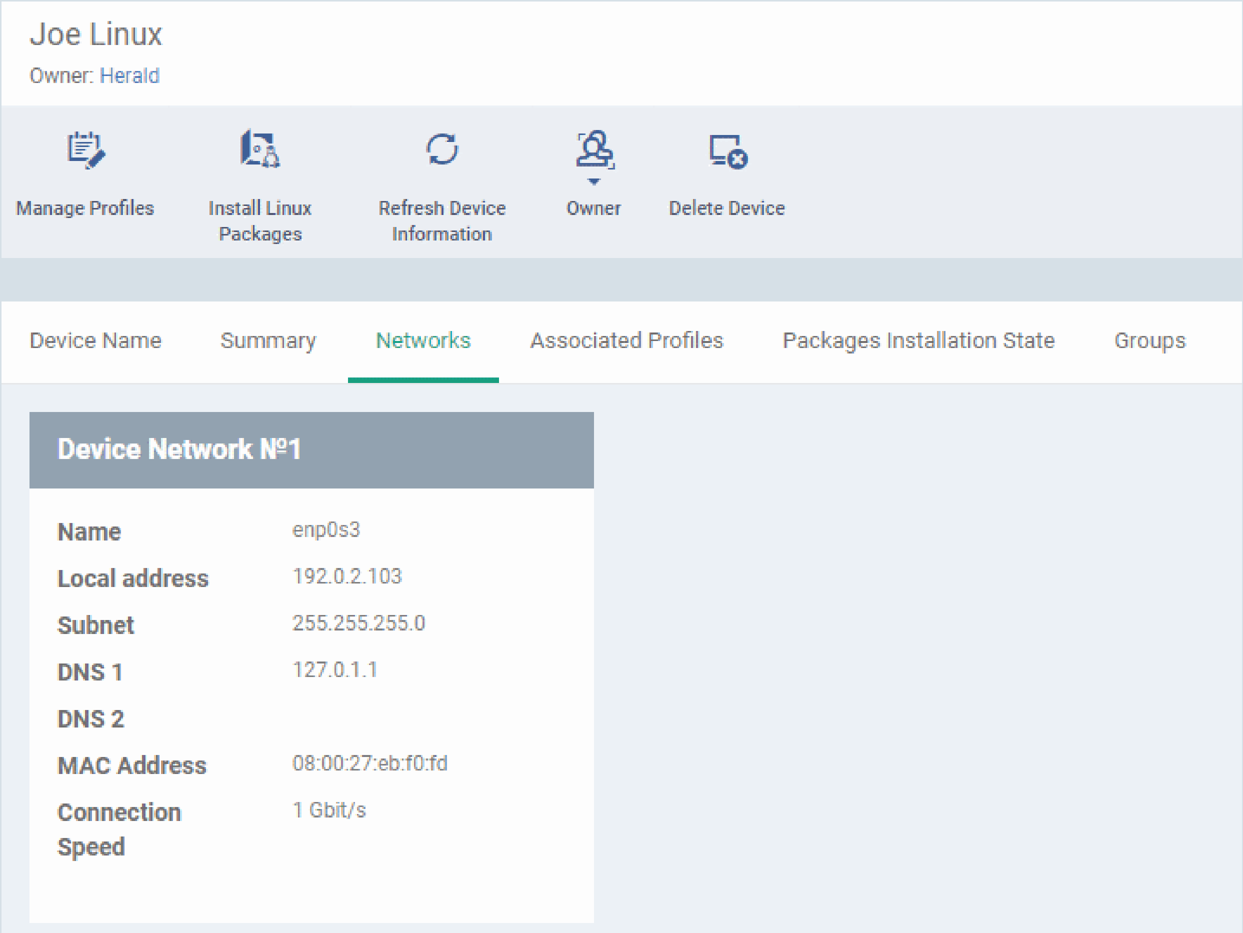
### 5.2.4.3. View Network Information of a Linux Device

- The 'Networks' tab shows information about the networks to which the device is connected. This includes the MAC address of the device and more.
- Each network is shown in a separate box

**To view a device's network details**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu

  - Select a company or a group to view just their devices
    Or
  - Select 'Show all' to view every device added to EM
- Click on any Linux device then select the 'Networks' tab



Device Network №1

| | |
|---|---|
| Name | enp0s3 |
| Local address | 192.0.2.103 |
| Subnet | 255.255.255.0 |
| DNS 1 | 127.0.1.1 |
| DNS 2 | |
| MAC Address | 08:00:27:eb:f0:fd |
| Connection Speed | 1 Gbit/s |

### 5.2.4.4. View and Manage Profiles Associated with a Linux Device

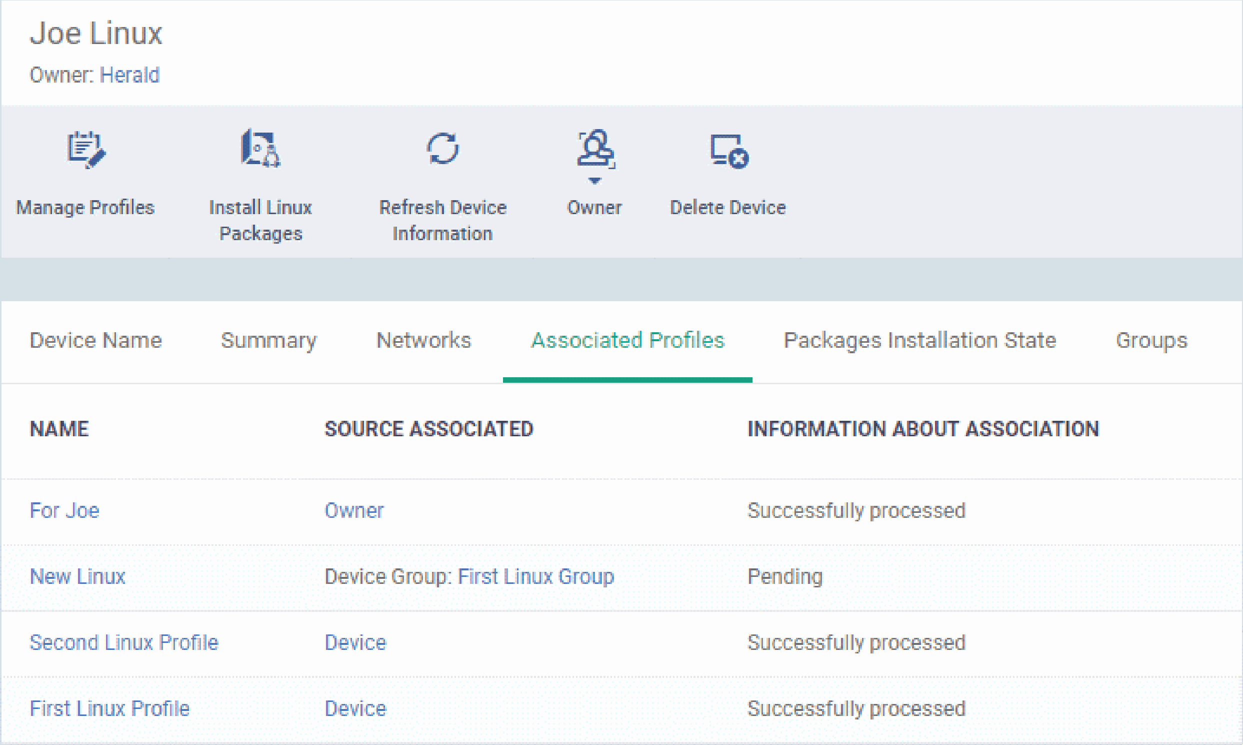
The 'Associated Profiles' tab lists all configuration profiles currently active on an endpoint. A profile may have been applied to a device because:

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

See **Profiles for Linux Devices** for more details on configuration profiles

**To view and manage profiles associated with a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices
    Or
  - Select 'Show all' to view every device added to EM
- Click on any Linux device then select the 'Associated Profiles' tab


Joe Linux

Owner: Herald

| NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSOCIATION |
|---|---|---|
| For Joe | Owner | Successfully processed |
| New Linux | Device Group: First Linux Group | Pending |
| Second Linux Profile | Device | Successfully processed |
| First Linux Profile | Device | Successfully processed |

| Associated Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The profile label.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Source Associated | How the profile was applied to the device. Profiles can be applied to a device in different ways:<br>• **Profile was directly applied to a device**. See **View and Manage Profiles Associated with a Device** for more details<br>• **Profile was applied to a user**. These profiles are in-turn deployed to all devices belonging to the user. See **Assign Configuration Profiles to a Users' Devices** for more details<br>• **Profile was applied to a user group**. These profiles are deployed to all devices owned by group members. See **Assign Configuration Profile to a User Group** for more details<br>• **Profile was applied to a device group**. These profiles are deployed to all devices in the group. See **Assign Configuration Profile to a Device Group** for more details<br>• Click the source to view and manage profiles associated with that source. |
| Information about Association | Whether the profile has been successfully applied to the device or is pending. |

- Click the 'Name' column header to sort the items in the alphabetical order of the names of the items

Click the 'Manage Profiles' button to add or remove profiles. See **View and Manage Profiles Associated with a Device** for a full overview of this interface.

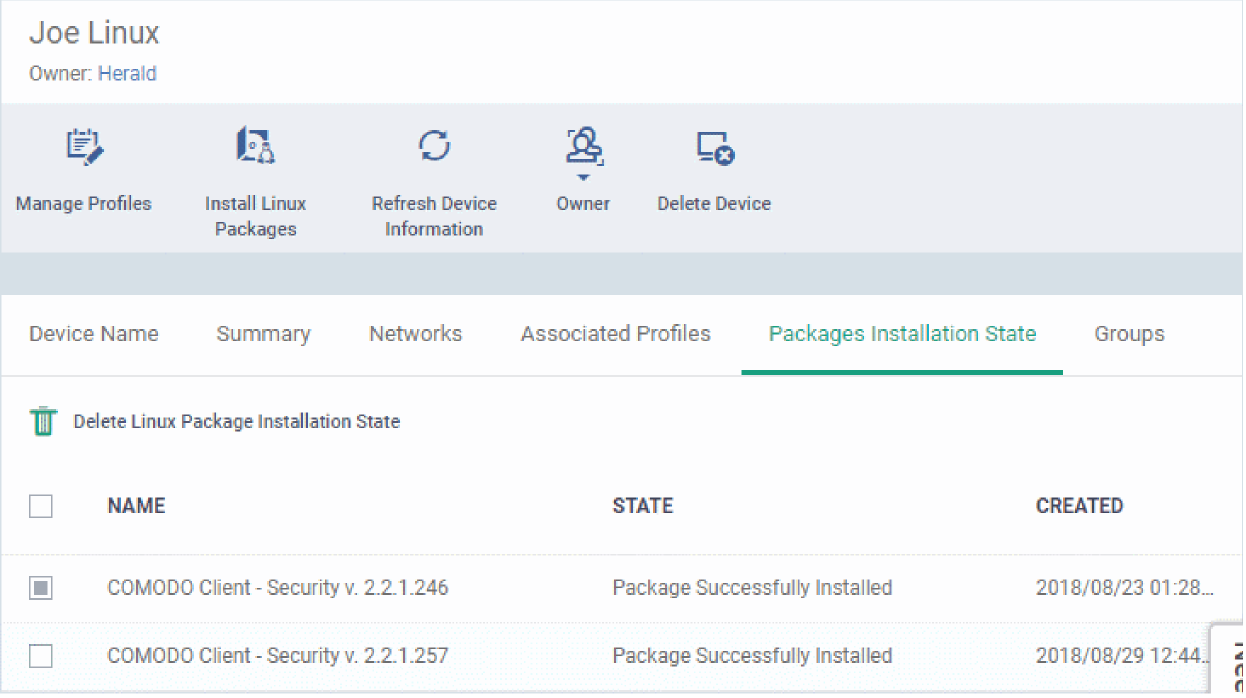
### 5.2.4.5. View Linux Packages Installed on a Device through Endpoint Manager

- Endpoint Manager lets you remotely install packages on managed Linux endpoints.

**To view Linux packages installed on a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Linux device
- Click the 'Packages Installation State' tab:

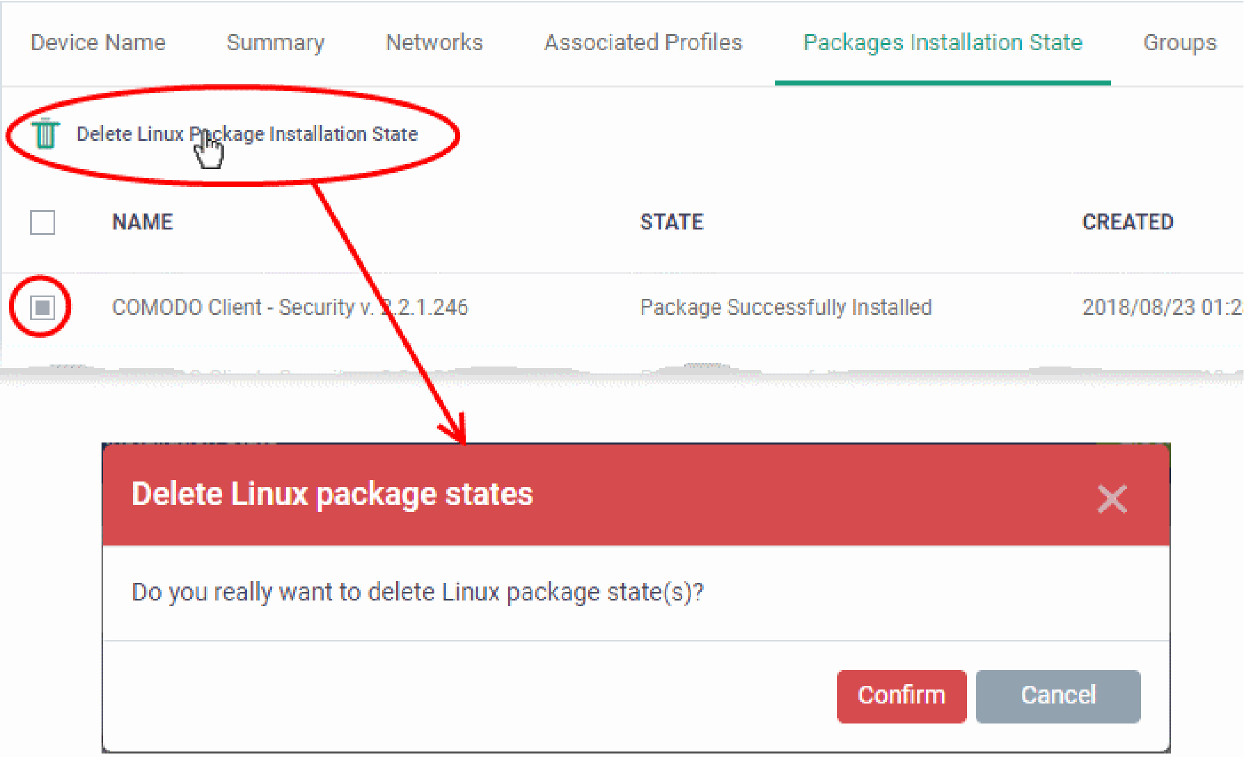

Joe Linux

Owner: Herald

| ☐ | NAME | STATE | CREATED |
|---|---|---|---|
| ☒ | COMODO Client - Security v. 2.2.1.246 | Package Successfully Installed | 2018/08/23 01:28... |
| ☐ | COMODO Client - Security v. 2.2.1.257 | Package Successfully Installed | 2018/08/29 12:44... |

| Package Installation State - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The URL/filename of the package. |
| State | Whether the installation was successful or not |
| Created | The date and time at which the installation command was sent. |

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Select an entry and click 'Delete Linux Package Installation State' to remove it from the list.



Device Name
Summary
Networks
Associated Profiles
Packages Installation State
Groups
Delete Linux Package Installation State

| □ | NAME | STATE | CREATED |
|---|---|---|---|
| ■ | COMODO Client - Security v. 2.2.1.246 | Package Successfully Installed | 2018/08/23 01:2 |

Delete Linux package states

Do you really want to delete Linux package state(s)?

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

Note - the entry will be removed from the list but the package will not be uninstalled from the device.

More reading - see **Remotely Install Packages on Linux Devices**.

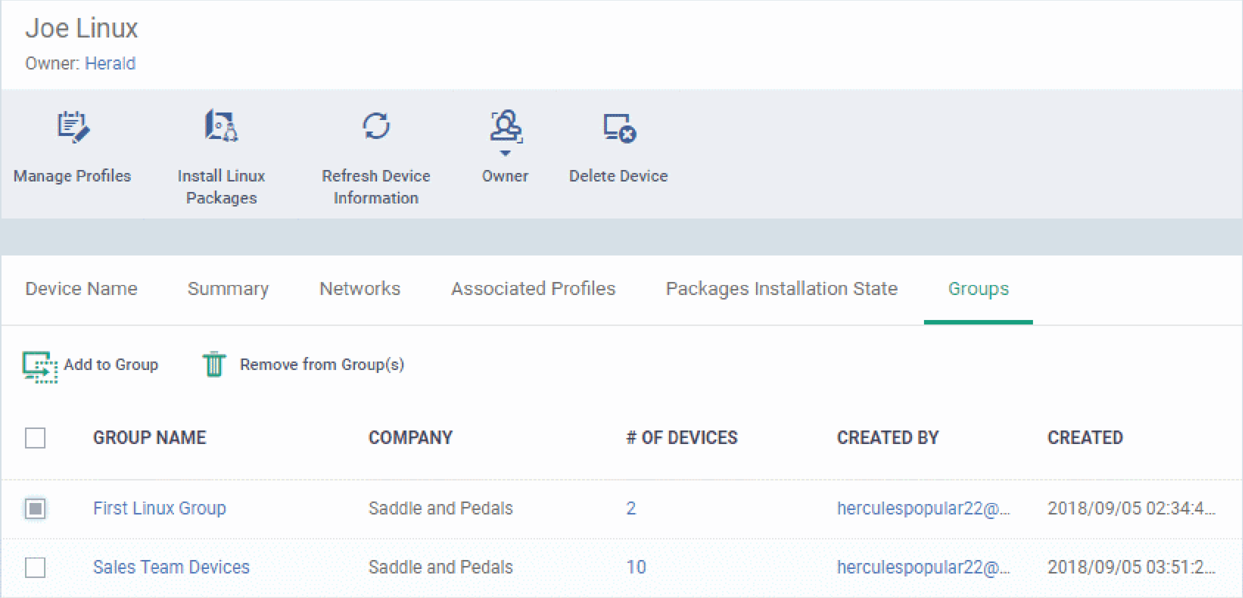
### 5.2.4.6. View and Manage Device Group Memberships

- Device groups let you deploy policies to multiple devices at once.

**To manage device group membership**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of a Linux device then select the 'Groups' tab:



Joe Linux
Owner: Herald

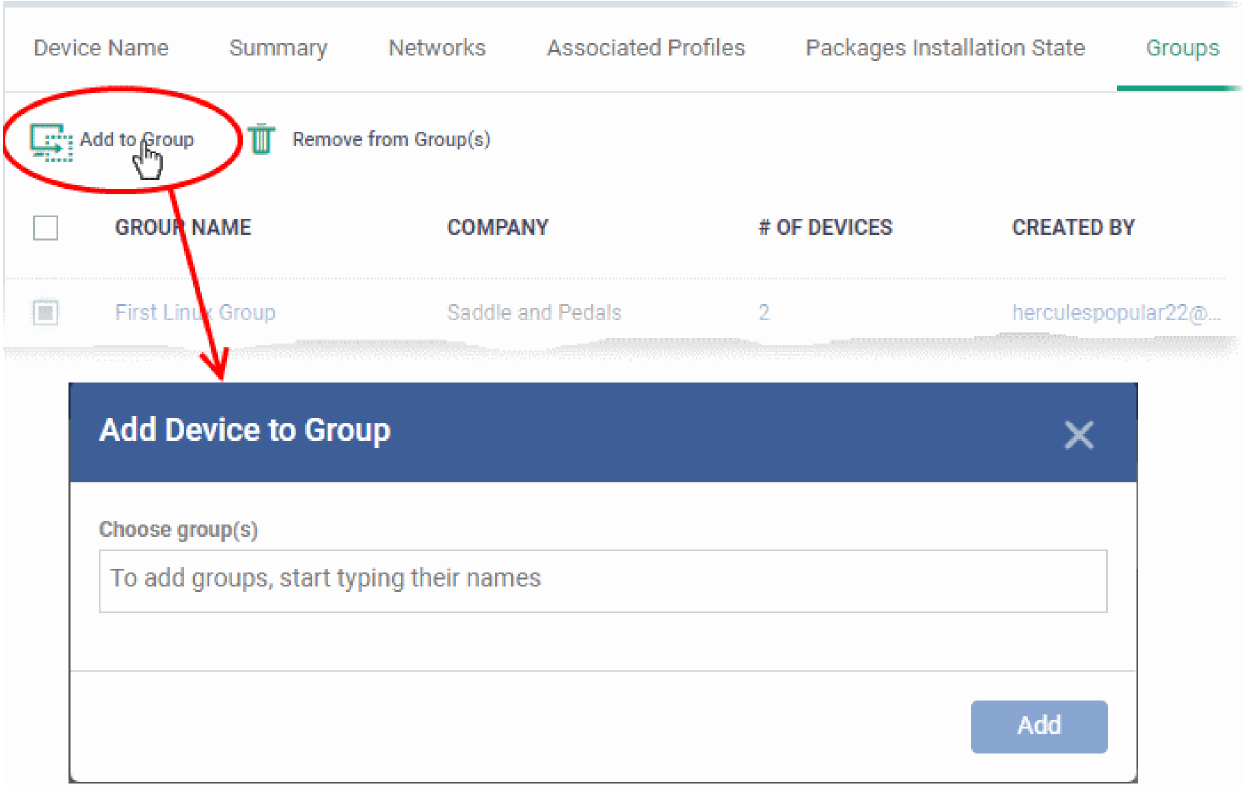
| □ | GROUP NAME | COMPANY | # OF DEVICES | CREATED BY | CREATED |
|---|---|---|---|---|---|
| ☑ | First Linux Group | Saddle and Pedals | 2 | herculespopular22@... | 2018/09/05 02:34:4... |
| □ | Sales Team Devices | Saddle and Pedals | 10 | herculespopular22@... | 2018/09/05 03:51:2... |

- The interface lists all groups of which the device is a member.
- Group profiles are applied to all endpoints in the group.
  - See **Assign Configuration Profiles to a Device Group** if you want to learn more about this process.

| Device Groups - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Group | The group label.<br>• Click the group name to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Customer | The name of the company for which the group was created. |
| Number of Devices | The total count of devices in the group.<br>• Click the number to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Created By | Name of the admin who created the group.<br>• Click the name to view the admin's details.<br>• See **View the Details of a User** for more details. |
| Created | The date and time at which the group was created. |

**To add a device to a new group**

- Click the 'Add to Group' button
- Select the group to which you want to add the device:



| GROUP NAME | COMPANY | # OF DEVICES | CREATED BY |
|---|---|---|---|
| First Linux Group | Saddle and Pedals | 2 | herculespopular22@... |

Add Device to Group

Choose group(s)

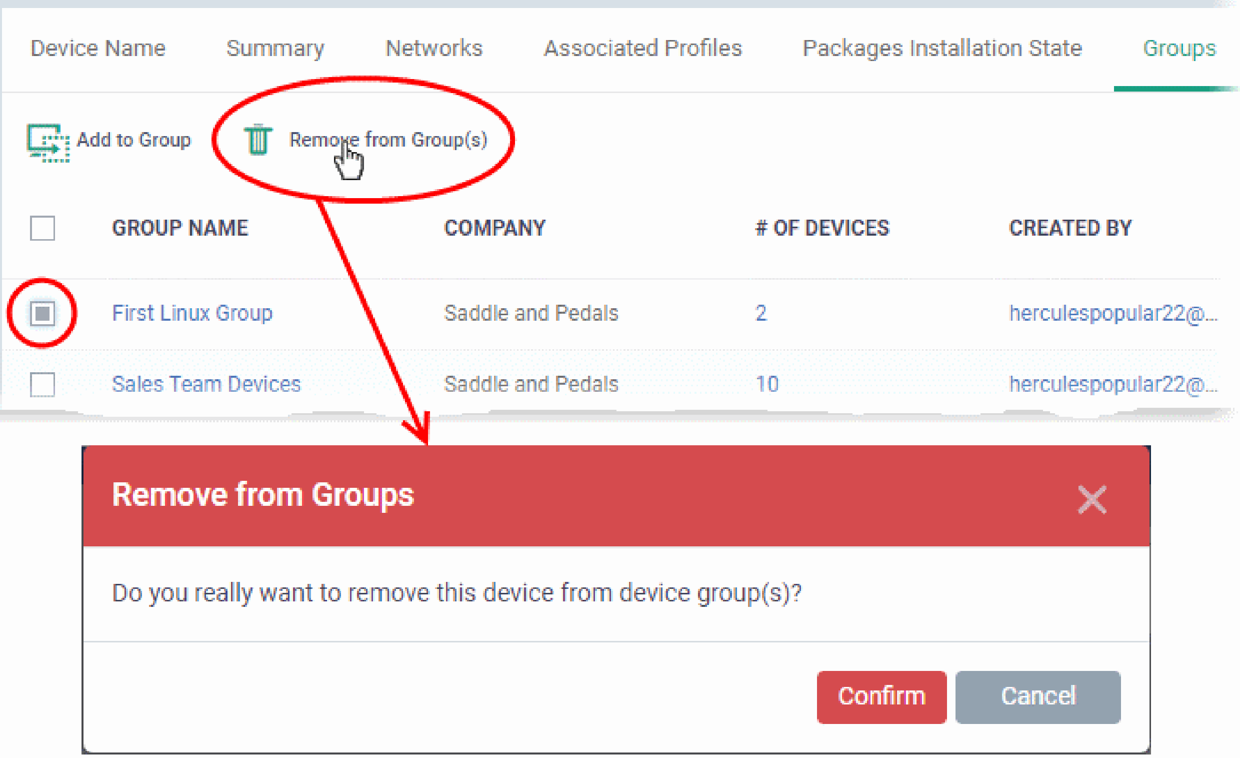
To add groups, start typing their names

- Start typing the name of the group to see a list of suggestions.
- Repeat the process to add the device to other groups.
- Click the 'Add' button.

The device will be added to the group.

**To remove a device from a group**

- Select the groups from which you want to remove the device
- Click the 'Remove from Group(s)' button:



| GROUP NAME | COMPANY | # OF DEVICES | CREATED BY |
|---|---|---|---|
| First Linux Group | Saddle and Pedals | 2 | herculespopular22@... |
| Sales Team Devices | Saddle and Pedals | 10 | herculespopular22@... |

Remove from Groups

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

- Click 'Confirm' to remove the device from the selected groups.

Note - Any group profiles will also be removed from the device.

## 5.2.5. Manage Android/iOS Devices

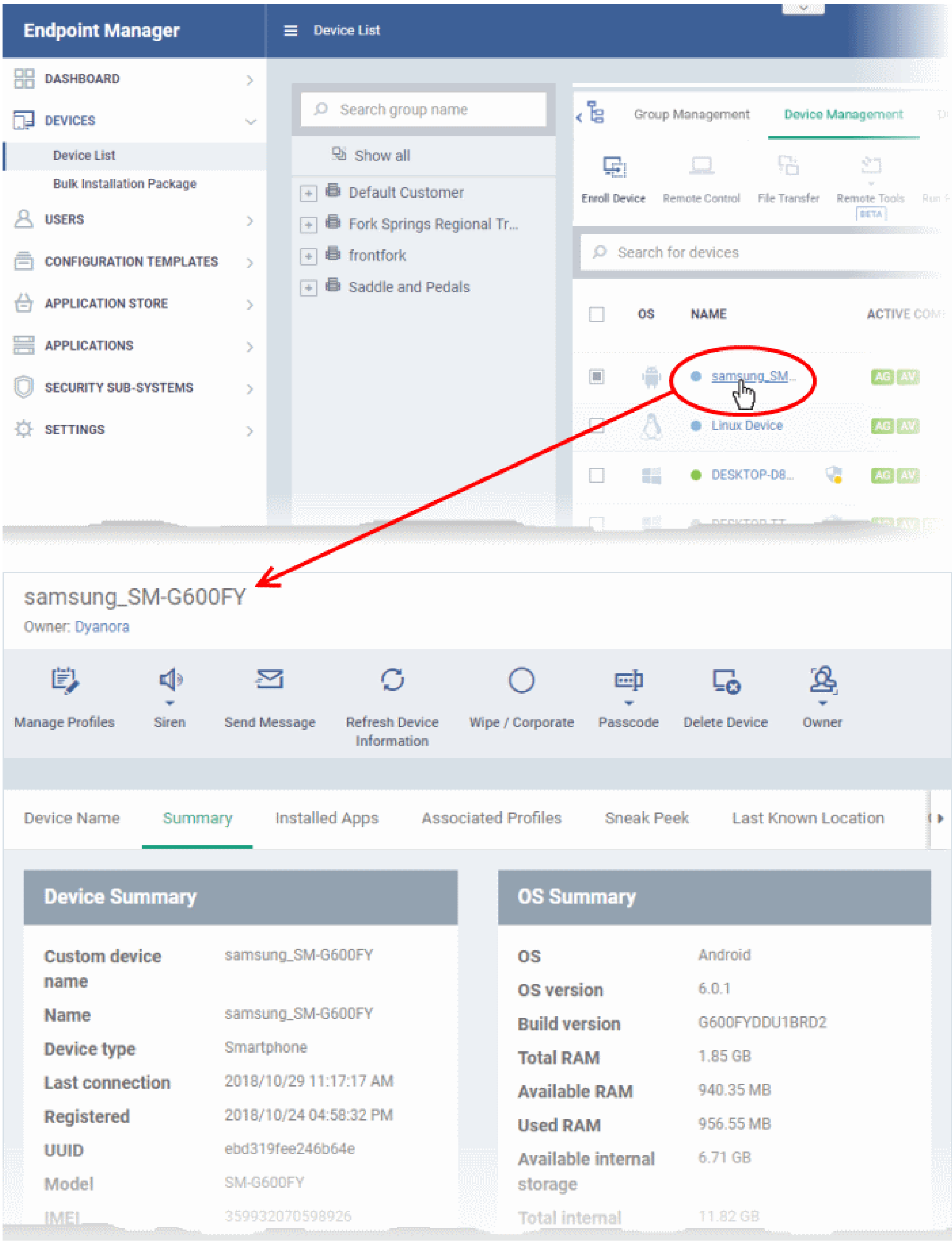
- The device details page lets you view hardware/software details, manage profiles and manage installed apps.
- You can also send messages to or sound an alarm on the device, remotely lock the device, track device location and more.

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

**To view and manage an individual device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of any Android or iOS device to open the 'Device Details' pane:



**Device Summary**

| | |
|---|---|
| Custom device name | samsung_SM-G600FY |
| Name | samsung_SM-G600FY |
| Device type | Smartphone |
| Last connection | 2018/10/29 11:17:17 AM |
| Registered | 2018/10/24 04:58:32 PM |
| UUID | ebd319fee246b64e |
| Model | SM-G600FY |
| IMEI | 359932070598926 |

**OS Summary**

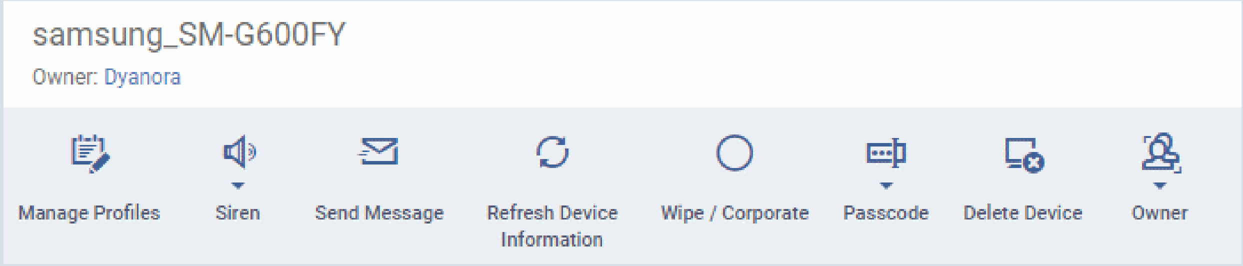
| | |
|---|---|
| OS | Android |
| OS version | 6.0.1 |
| Build version | G600FYDDU1BRD2 |
| Total RAM | 1.85 GB |
| Available RAM | 940.35 MB |
| Used RAM | 956.55 MB |
| Available internal storage | 6.71 GB |
| Total internal | 11.82 GB |

The device details screen has seven tabs:

- **Device Name** - Device label. Click the 'Edit' button if you wish to change the device name. See **View and Edit Device Name** for more details.
- **Summary** - General information about the device. Includes basic device information, operating system details, network details and security configuration. See **View Summary Information** for more details.
- **Installed apps** - Details of applications installed on the device. You can remotely block/release apps or uninstall applications. See **Manage Installed Applications** for more details.
- **Associated Profiles** - Profiles which have been deployed to the device. You can add new profiles or remove existing profiles on the device. See **View and Manage Profiles Associated with a Device** for more details.

- **Sneak Peek** - Pictures captured by the 'Sneak Peek' feature of Endpoint Manager. The 'Sneak Peek' feature photographs the person holding the device if they enter the wrong passcode too many times. You must enable sneak peek on a profile to use the feature. See **View Sneak Peek Pictures to Locate Lost Devices** for more details.
- **Last Known Location** - The map location of the device when it last connected to Endpoint Manager. See **View the Location of the Device** for more details.
- **Groups** - Shows all groups of which the Android/iOS device is a member. You can manage group membership from this tab. See **View and Manage Device Group Memberships** for more details.

Device tasks are shown along the top of the interface:


samsung_SM-G600FY

Owner: Dyanora

- **Manage Profiles** - Add or remove device profiles. See **Assign Configuration Profiles to Selected Devices** for more details.
- **Siren** - Sound an alarm on the device to locate it. See **Generate Alarm on Devices** for more details.
- **Send Message** - Send a text message to the user. See **Send Text Message to Devices** for more details
- **Refresh Information** - Obtain updated details from the device. See **Update Device Information** for more details.
- **Wipe / Corporate** - Delete all data stored in the device if it is lost or stolen. See **Wipe Data from Devices** for more details.
- **Passcode** - Create a new screen lock passcode for selected devices. You can also remotely lock or unlock the device. See **Set / Reset Screen Lock Password for Selected Devices** and **Lock / Unlock Selected Devices** for more details.
- **Delete Device** - Remove the device from Endpoint Manager. See **Remove a Device** for more details.
- **Owner** - Change the user with whom the device is associated. You can also change the type of device to corporate or personal. See **Change a Device's Owner** and **Change the Ownership Status of a Device** for more details.

### 5.2.5.1. View and Edit Device Name

- Enrolled devices are listed by the name assigned to them by their owner.
- If no name was assigned then the actual device name or model number is used.
- Admins can change the device name according to their preferences. Name changes apply only in Endpoint Manager. The name will not change on the device itself.
- 'Allow Auto Rename of Device Custom Name' - If enabled, the custom name will be replaced automatically by the device name/model number during the next sync..

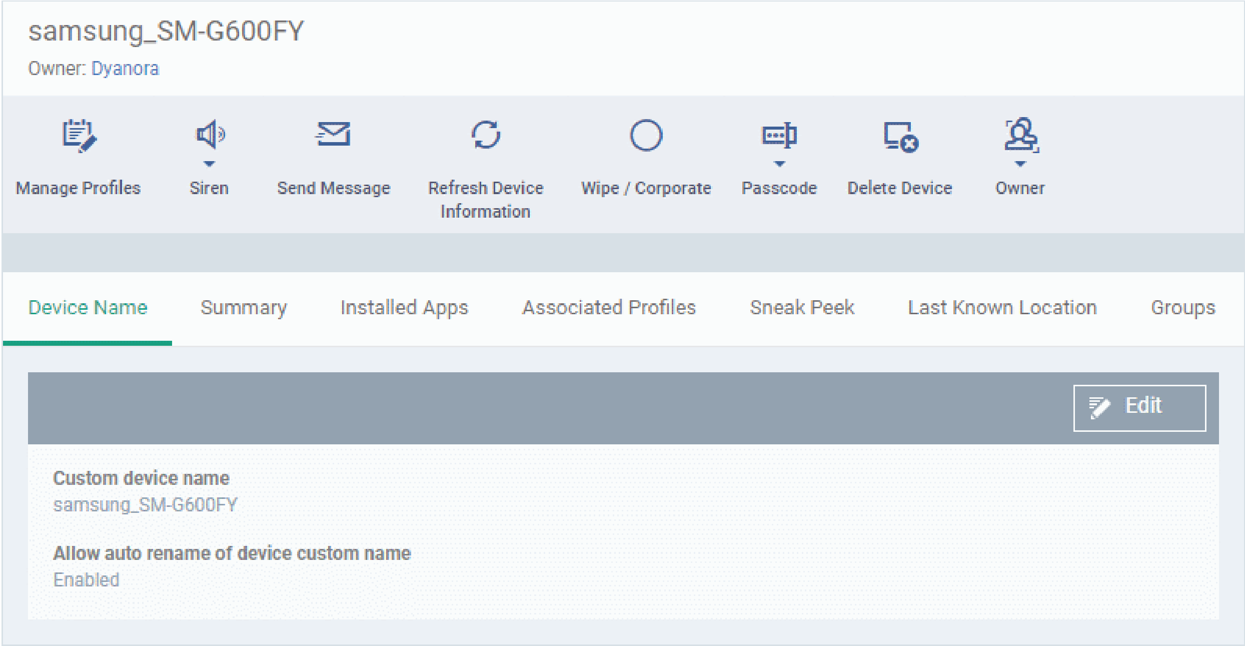
**To change the device's name**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

  Or

  - Select 'Show all' on the left to view every device enrolled to EM

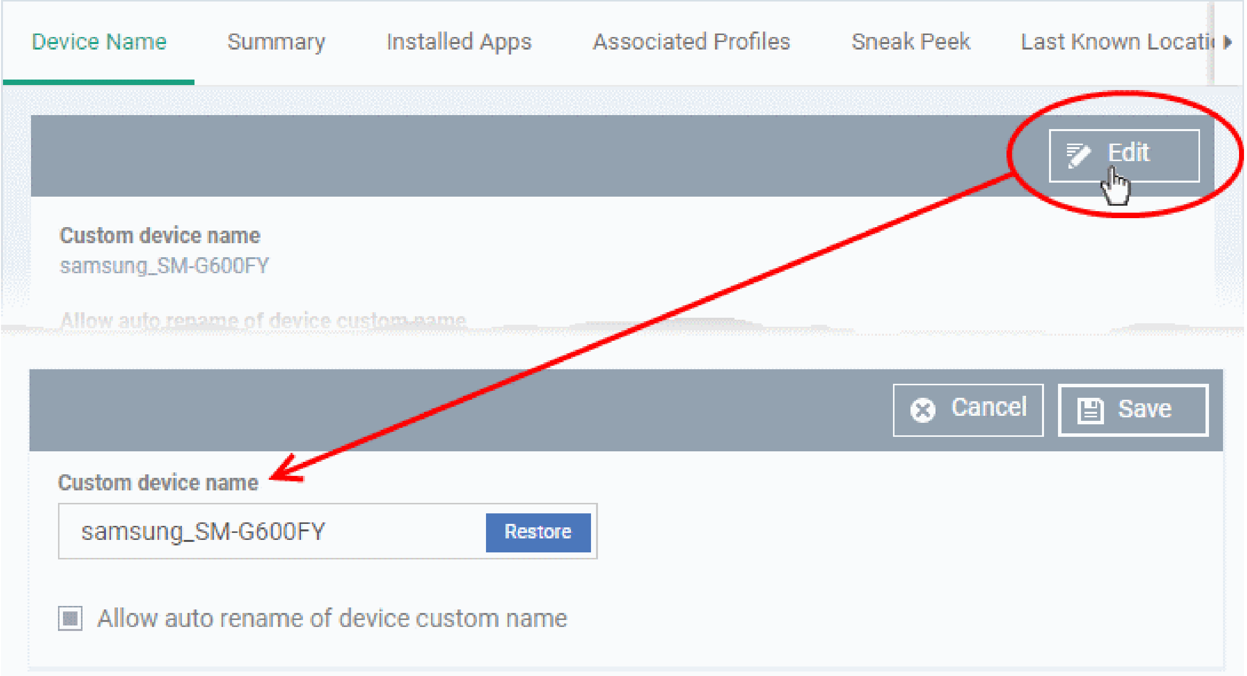
- Click on any Android or iOS device then select the 'Device Name' tab



Custom device name
samsung_SM-G600FY

Allow auto rename of device custom name
Enabled

- Custom device name - The current name of the device.
- Allow auto rename of device custom name - Indicates whether the device's name will automatically replace the custom name in the list during the next sync with communication client.
- To change the name of the device, click the 'Edit' button at the right.



Custom device name
samsung_SM-G600FY

Allow auto rename of device custom name

Custom device name
samsung_SM-G600FY

□ Allow auto rename of device custom name

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

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

The device will be listed with its new name.

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

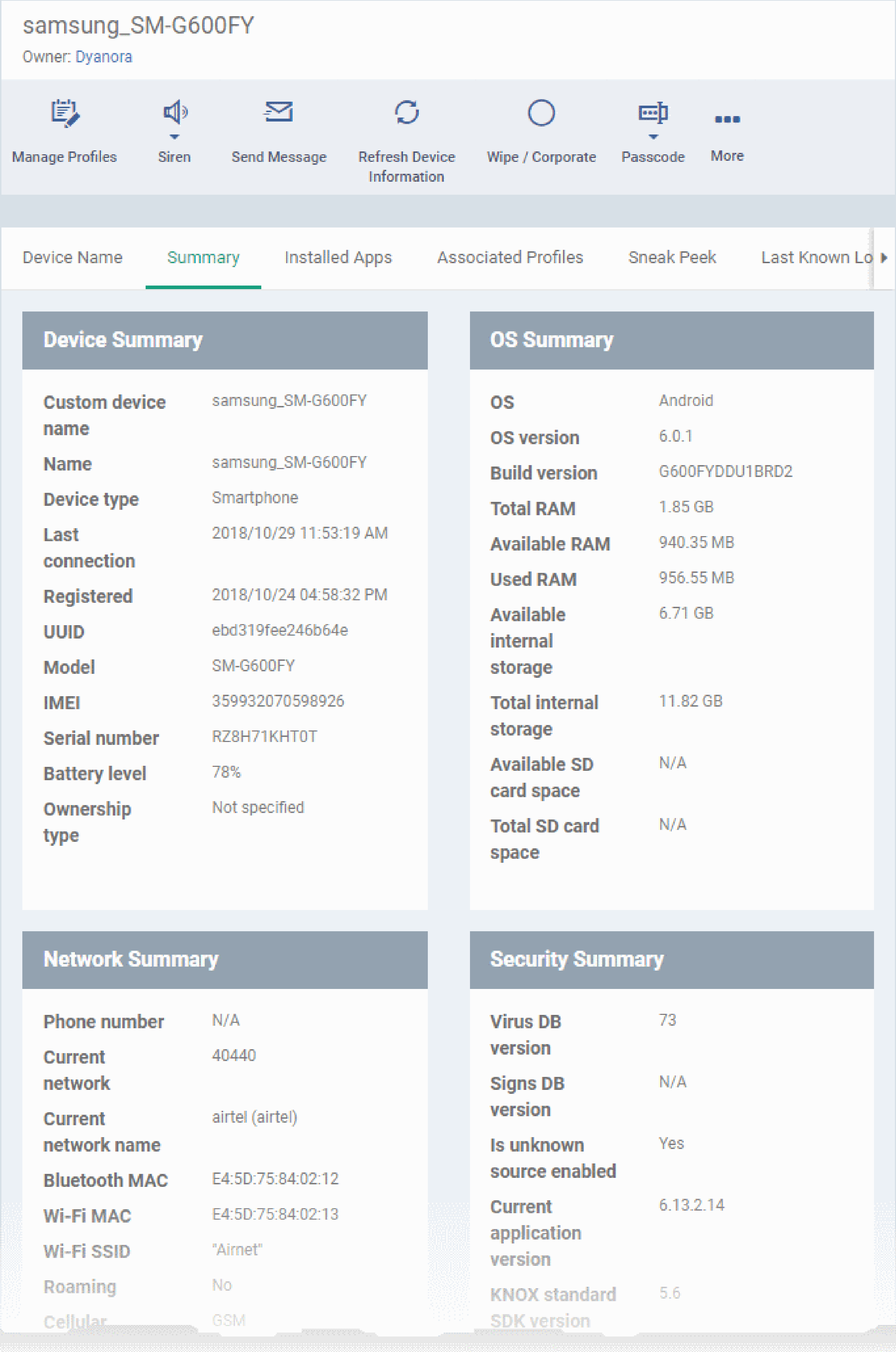
### 5.2.5.2. View Summary Information

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

**To view device information summary**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Android or iOS device then open the 'Summary' tab (if it is not already open).



samsung_SM-G600FY

Owner: Dyanora

**Device Summary**

| | |
|---|---|
| Custom device name | samsung_SM-G600FY |
| Name | samsung_SM-G600FY |
| Device type | Smartphone |
| Last connection | 2018/10/29 11:53:19 AM |
| Registered | 2018/10/24 04:58:32 PM |
| UUID | ebd319fee246b64e |
| Model | SM-G600FY |
| IMEI | 359932070598926 |
| Serial number | RZ8H71KHT0T |
| Battery level | 78% |
| Ownership type | Not specified |

**OS Summary**

| | |
|---|---|
| OS | Android |
| OS version | 6.0.1 |
| Build version | G600FYDDU1BRD2 |
| Total RAM | 1.85 GB |
| Available RAM | 940.35 MB |
| Used RAM | 956.55 MB |
| Available internal storage | 6.71 GB |
| Total internal storage | 11.82 GB |
| Available SD card space | N/A |
| Total SD card space | N/A |

**Network Summary**

| | |
|---|---|
| Phone number | N/A |
| Current network | 40440 |
| Current network name | airtel (airtel) |
| Bluetooth MAC | E4:5D:75:84:02:12 |
| Wi-Fi MAC | E4:5D:75:84:02:13 |
| Wi-Fi SSID | "Airnet" |
| Roaming | No |
| Cellular | GSM |

**Security Summary**

| | |
|---|---|
| Virus DB version | 73 |
| Signs DB version | N/A |
| Is unknown source enabled | Yes |
| Current application version | 6.13.2.14 |
| KNOX standard SDK version | 5.6 |

- **Device Summary -** Provides device details such as brand, model, International Mobile Equipment Identification (IMEI) number, last connection time, device battery level (at last connection time) and Ownership type of the device.
- **OS Summary -** Provides details about the device's Operating System, including version number, memory usage and available internal and external storage space.
- **Network Summary -** Provides details about the mobile and WiFi networks to which the device is connected, including the MAC addresses of the device for connection through Bluetooth and WiFi.
- **Security Summary -** Provides details about important security settings of the device. For Android devices, details from **Comodo Mobile Security** (CMS) like Virus Signature Database version and update status are displayed.

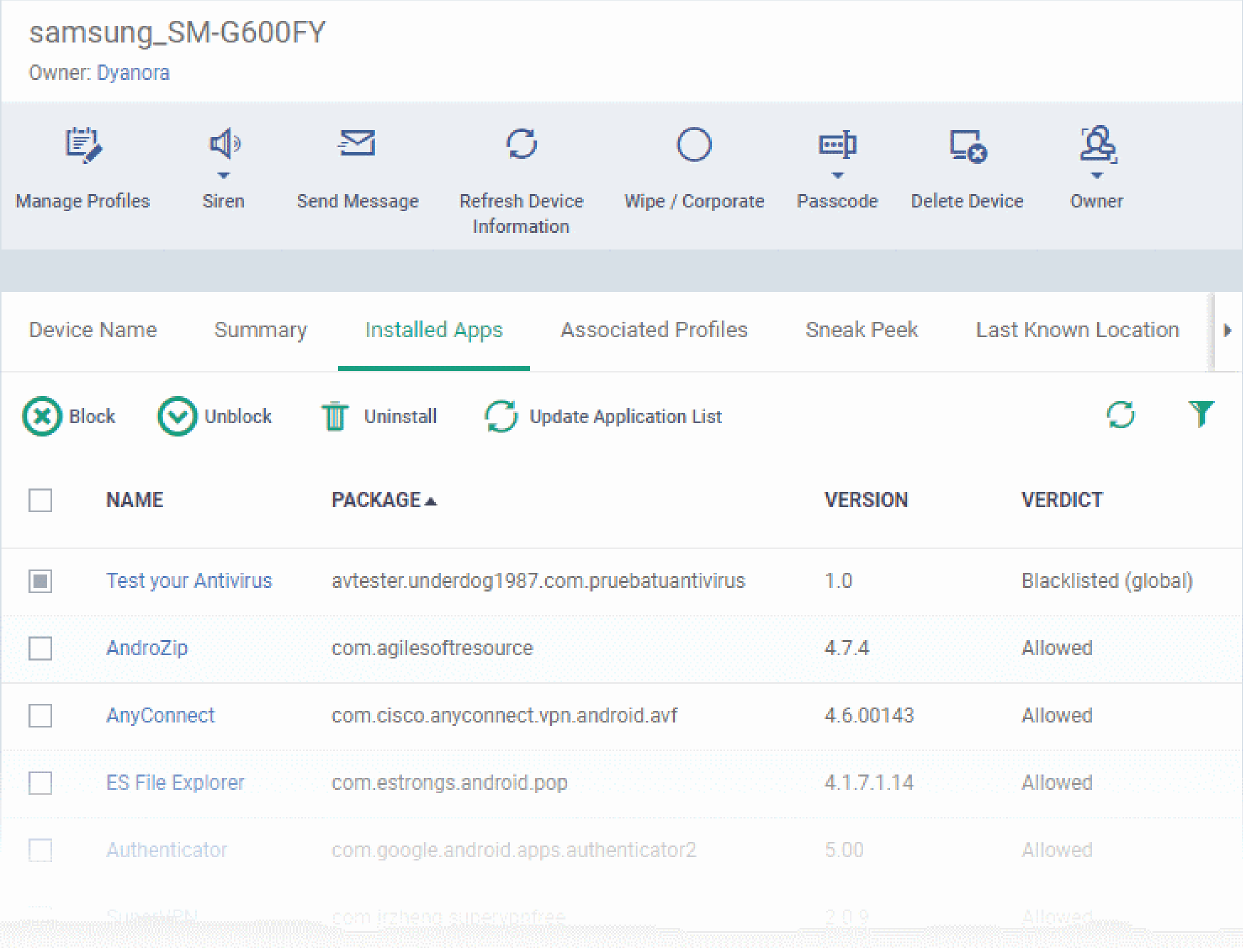
### 5.2.5.3. Manage Installed Applications

- The 'Installed Apps' tab shows all applications installed on a device with their package names and version numbers.
- You can block, unblock or remove apps as required.
- You can also see which other devices have the same applications installed.

**To manage installed apps**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on any Android or iOS device then open the 'Installed Apps' tab


samsung_SM-G600FY
Owner: Dyanora

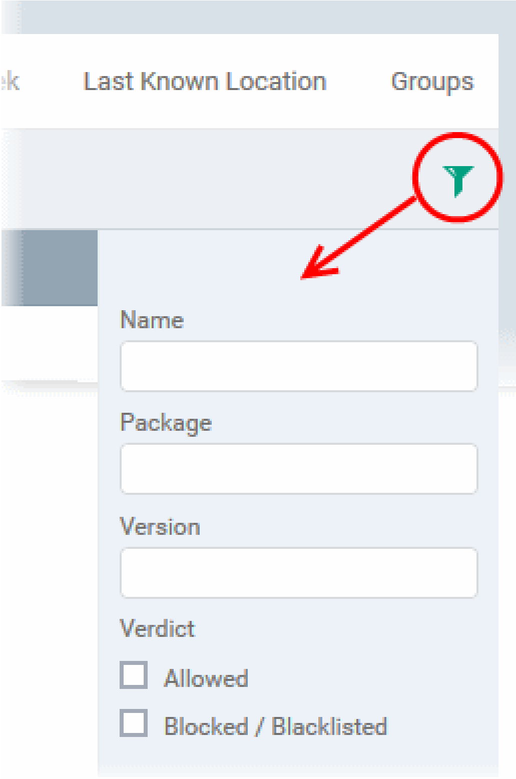
| ☐ | NAME | PACKAGE ▲ | VERSION | VERDICT |
|---|---|---|---|---|
| ▣ | Test your Antivirus | avtester.underdog1987.com.pruebatuantivirus | 1.0 | Blacklisted (global) |
| ☐ | AndroZip | com.agilesoftresource | 4.7.4 | Allowed |
| ☐ | AnyConnect | com.cisco.anyconnect.vpn.android.avf | 4.6.00143 | Allowed |
| ☐ | ES File Explorer | com.estrongs.android.pop | 4.1.7.1.14 | Allowed |
| ☐ | Authenticator | com.google.android.apps.authenticator2 | 5.00 | Allowed |
| ☐ | SuperVPN | com.jrzheng.supervpnfree | 2.0.9 | Allowed |

| Installed Apps - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of the application.<br>• Click the application name to view all devices which have this app installed.<br>This is useful if you want to apply an action to all devices which have a certain app installed. |
| Package | The application ID on the vendor app store. For example, 'cn.wps.moffice_i18n' can be found at **https://play.google.com/store/apps/details?id=cn.wps.moffice_i18n**. |
| Version | The version number of the application. |
| Verdict | Whether the application is allowed, blocked or blacklisted by EM. |

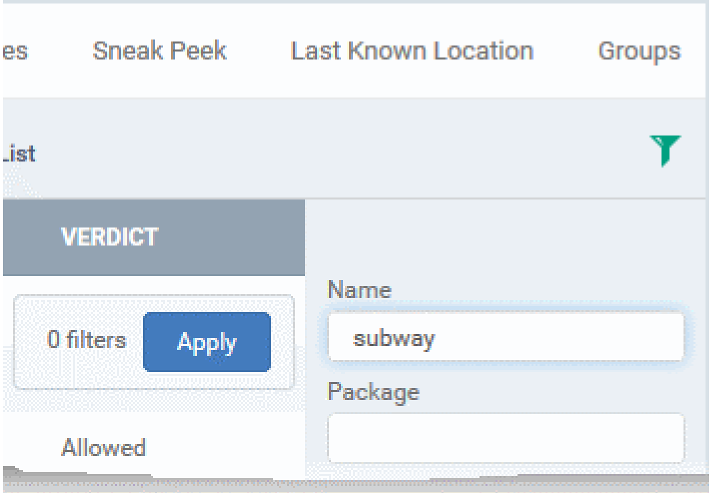
- The list of apps on a device is updated in Endpoint Manager every 24 hrs. To refresh the list immediately, click 'Update Application List'.

## Sorting and Filtering Options

- Click any column header to sort the items in alphabetical order.
- Click the funnel icon at the right to open the filter interface:



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



Name: subway

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

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

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

## Block Unwanted Apps

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

**To block selected apps**

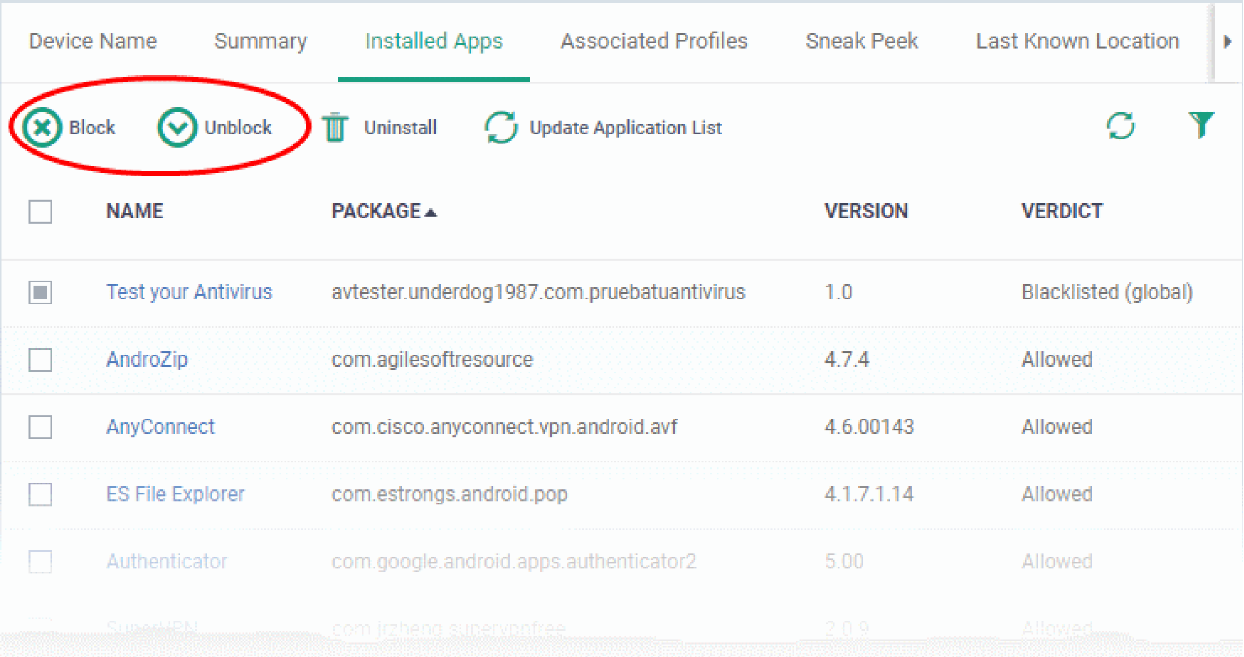
- Choose the app(s) that you wish to block and simply click the 'Block' button.

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

**To release blocked apps**

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

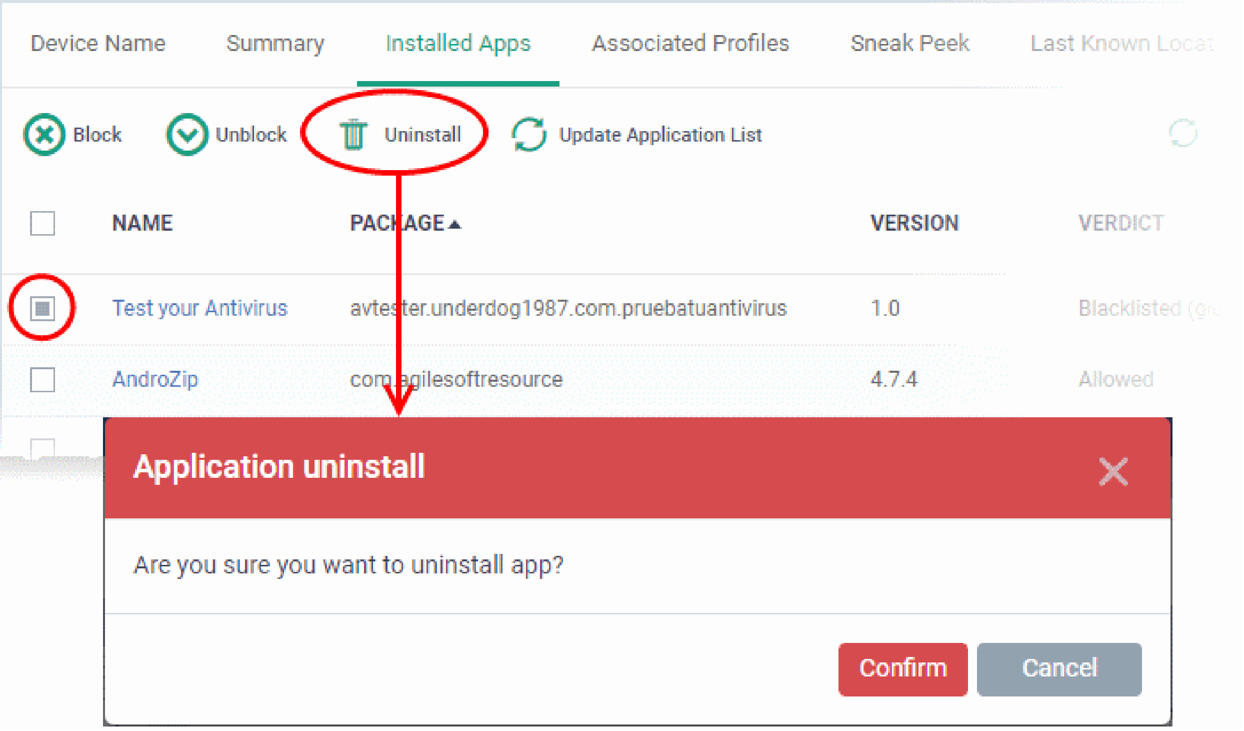
The verdict of the app(s) will change to 'Allowed' and they will be allowed to run on the device.



| ☐ | NAME | PACKAGE ▲ | VERSION | VERDICT |
|---|---|---|---|---|
| ☒ | Test your Antivirus | avtester.underdog1987.com.pruebatuantivirus | 1.0 | Blacklisted (global) |
| ☐ | AndroZip | com.agilesoftresource | 4.7.4 | Allowed |
| ☐ | AnyConnect | com.cisco.anyconnect.vpn.android.avf | 4.6.00143 | Allowed |
| ☐ | ES File Explorer | com.estrongs.android.pop | 4.1.7.1.14 | Allowed |
| ☐ | Authenticator | com.google.android.apps.authenticator2 | 5.00 | Allowed |
| ☐ | SuperVPN | com.jrzheng.supervpnfree | 2.0.9 | Allowed |

## Uninstall applications

- Select the app(s) and click 'Uninstall'.



| ☐ | NAME | PACKAGE ▲ | VERSION | VERDICT |
|---|---|---|---|---|
| ☒ | Test your Antivirus | avtester.underdog1987.com.pruebatuantivirus | 1.0 | Blacklisted (gl |
| ☐ | AndroZip | com.agilesoftresource | 4.7.4 | Allowed |

Application uninstall

Are you sure you want to uninstall app?

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

### 5.2.5.4. View and Manage Profiles Associated with a Device

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

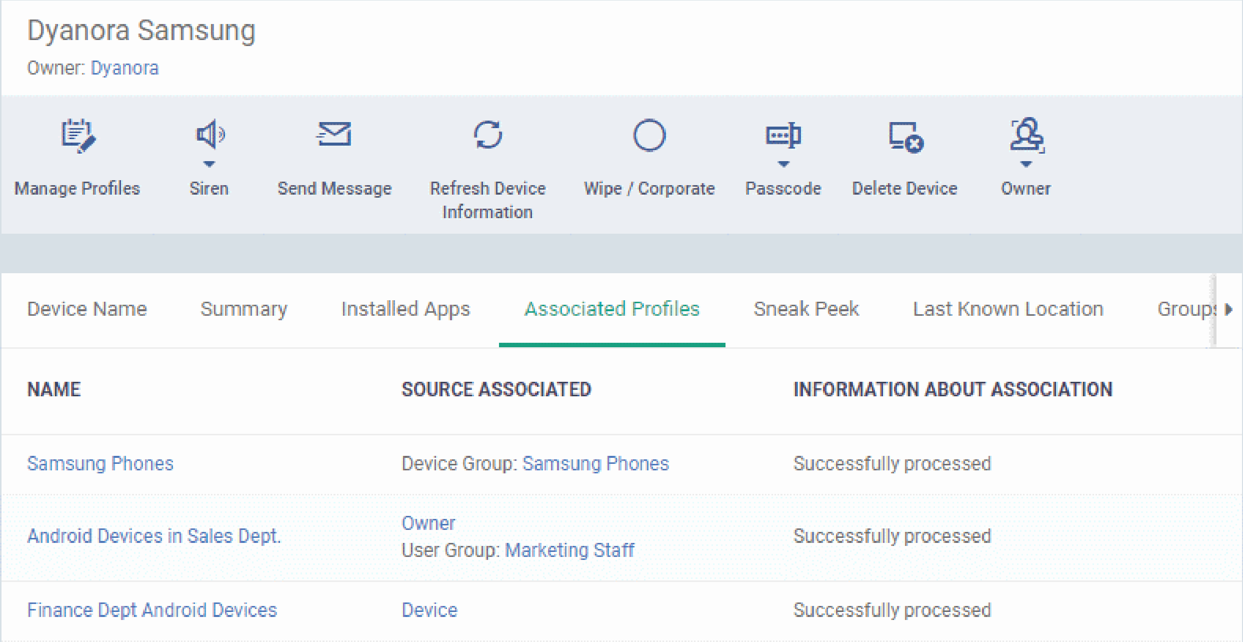
- It is a default profile
- It was specifically applied to the device
- It was specifically applied to the user
- The device belongs to one or more device groups and inherited profiles from the group
- The user belongs to one or more user groups and inherited profiles from the group

See '**Profiles for Android Devices**', '**Profiles for iOS Devices**', '**Viewing and Managing Profiles**' and '**Managing Default Profiles**', for more details on profiles and default profiles.

**To view and manage associated profiles**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Click on any Android or iOS device then open the 'Associated Profiles' tab



| NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSOCIATION |
|---|---|---|
| Samsung Phones | Device Group: Samsung Phones | Successfully processed |
| Android Devices in Sales Dept. | Owner<br>User Group: Marketing Staff | Successfully processed |
| Finance Dept Android Devices | Device | Successfully processed |

| Associated Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The profile label.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Source Associated | The channel through which the profile was applied to the device. Configuration profiles can be applied to a device in different ways:<br>• Profiles can be directly applied to the device. See **Assign Configuration** |

| | |
|---|---|
| | Profiles to Selected Devices for more details.<br>• Profiles applied to a user are deployed to all devices belonging to them. See Assign Configuration Profiles to User Devices for more details.<br>• Profiles applied to a user group are deployed to all devices owned by group members. See Assign Configuration Profiles to a User Group for more details.<br>• Profiles applied to a device group are deployed to all member devices in the group. See Assign Configuration Profiles to a Device Group for more details.<br>• Click a source to open the respective details interface. |
| Information about Association | The status of profile application to the device. |

### Add or Remove Profiles

Click 'Manage Profiles' at the top to add or remove profiles. See **Assign Configuration Profiles to Selected Devices** for more details.

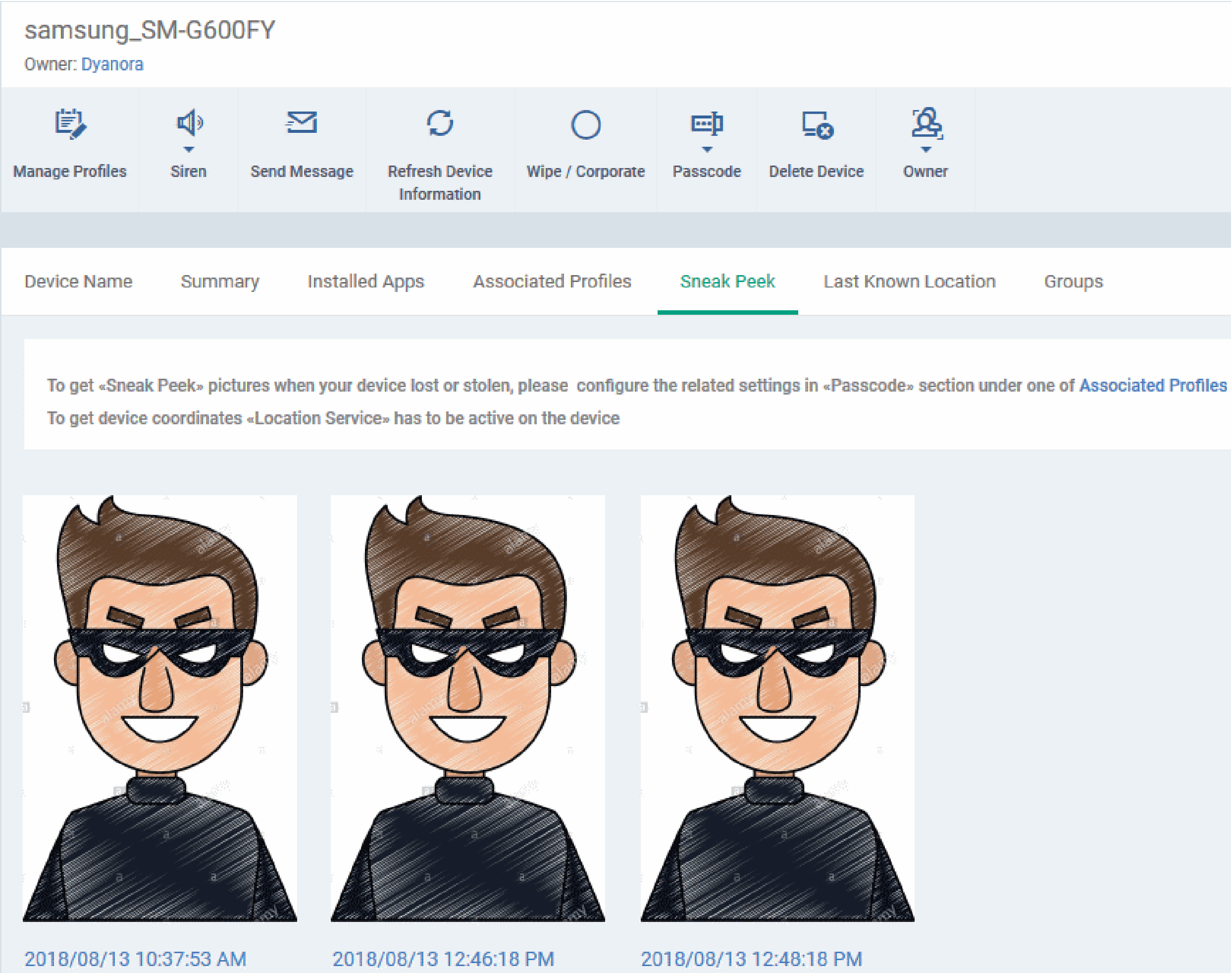
## 5.2.5.5. View Sneak Peek Pictures to Locate Lost Devices

- Click 'Devices' > 'Device List' > click a device name > 'Sneak Peek'
- 'Sneak Peek' takes a photo of the device holder if the wrong password is entered a certain number of times. This helps you to recover mislaid or stolen Android devices.
- The photo is sent to Endpoint Manager along with the location and time it was taken.
- The feature can be enabled on a device profile. You can specify how many incorrect attempts should be allowed.
- If a front camera is not available, a photograph is taken using the rear-facing camera.

**To view Sneak Peek pictures**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click on the name of any Android device then open the 'Sneak Peek' tab:



samsung_SM-G600FY

Owner: Dyanora

To get «Sneak Peek» pictures when your device lost or stolen, please configure the related settings in «Passcode» section under one of Associated Profiles

To get device coordinates «Location Service» has to be active on the device

2018/08/13 10:37:53 AM

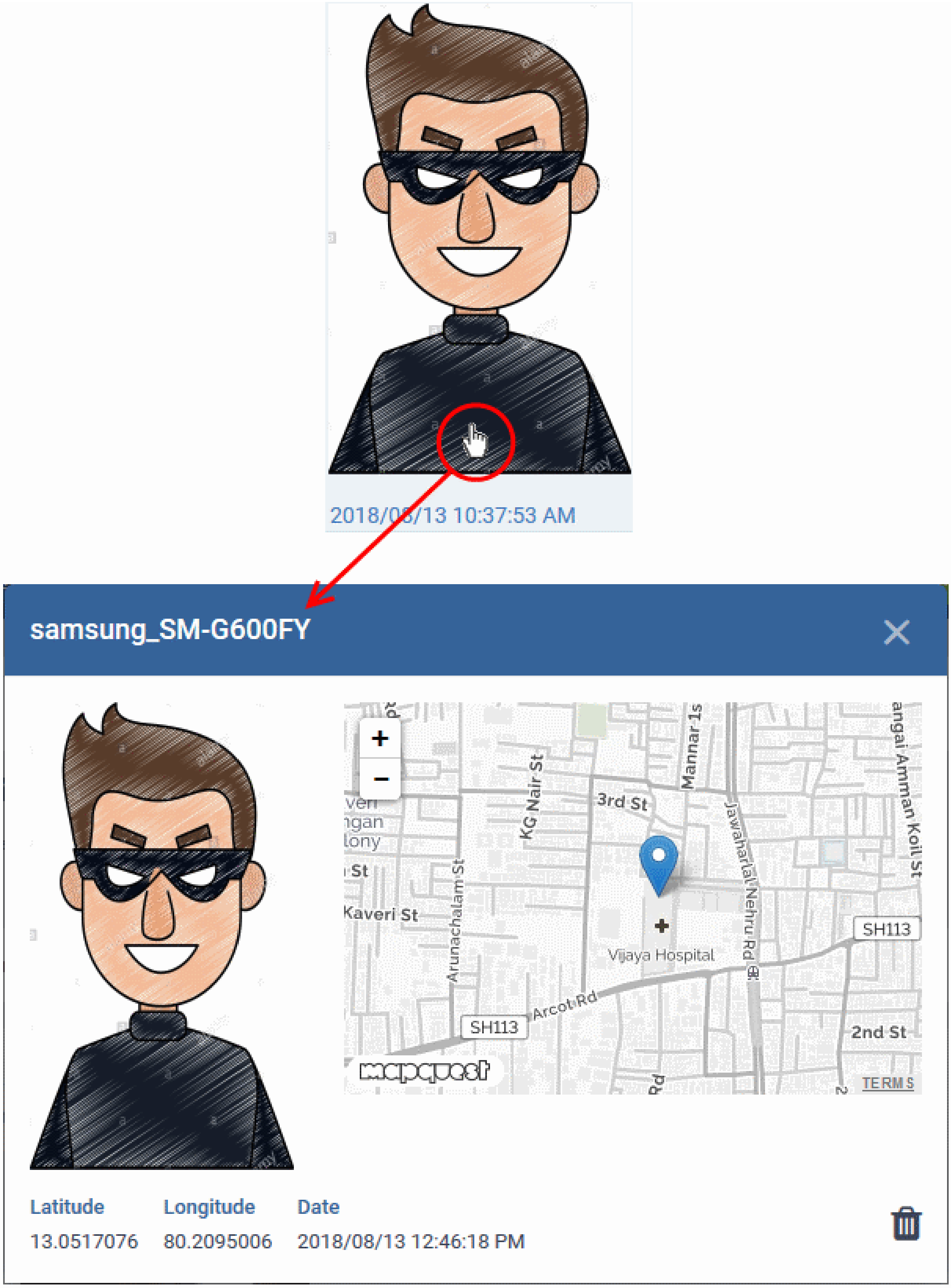
2018/08/13 12:46:18 PM

2018/08/13 12:48:18 PM

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

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

- Click on a picture to view see an enlarged view of the photograph and the location of the device at the time the photo was taken.



2018/08/13 10:37:53 AM

samsung_SM-G600FY

| Latitude | Longitude | Date |
|---|---|---|
| 13.0517076 | 80.2095006 | 2018/08/13 12:46:18 PM |

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

### 5.2.5.6. View the Location of the Device

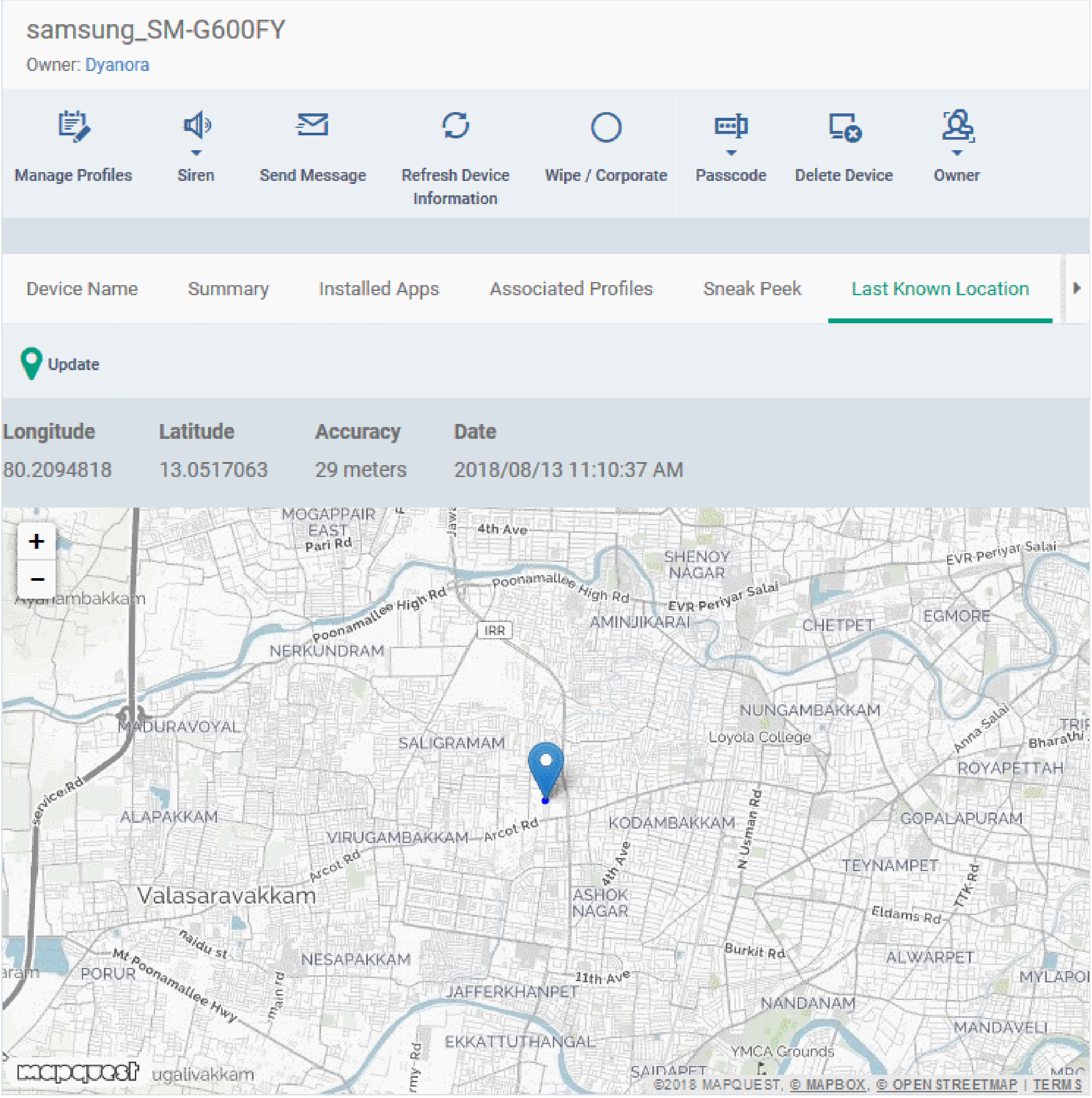
- The 'Last Known Location' tab shows from where the device most recently contacted Endpoint Manager.

- You can refresh the location by clicking the 'Update' link.

**To view the location**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices
    Or
  - Select 'Show all' to view every device added to EM
- Click on the name of any Android or iOS device then open the 'Last Known Location' tab:

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



samsung_SM-G600FY

Owner: Dyanora

| Longitude | Latitude | Accuracy | Date |
|---|---|---|---|
| 80.2094818 | 13.0517063 | 29 meters | 2018/08/13 11:10:37 AM |

The map shows the location of the device the last time it contacted EM.

- To view the current location of the device, click 'Update'.

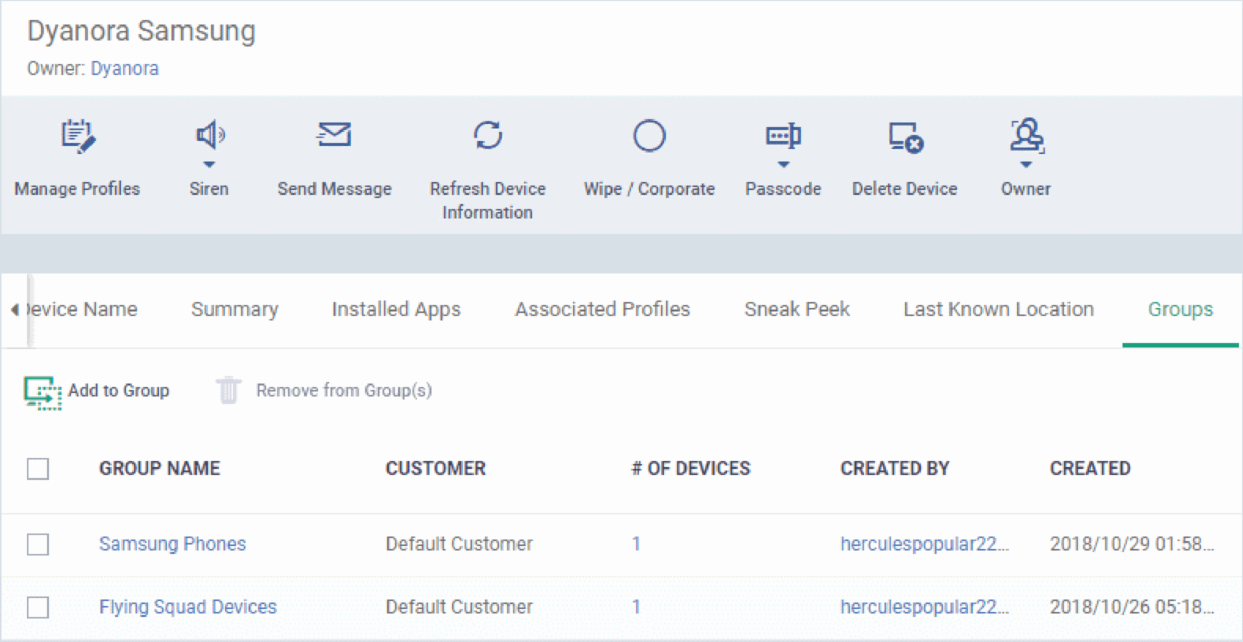
## 5.2.5.7. View and Manage Device Group Memberships

- 'Device Details' > 'Groups' shows all groups of which the device is a member.
- You can remove the device from a group or add it to a new group.

**To view and manage device group membership**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of any Android or iOS device then select the 'Groups' tab


Dyanora Samsung

Owner: Dyanora

| □ | GROUP NAME | CUSTOMER | # OF DEVICES | CREATED BY | CREATED |
|---|---|---|---|---|---|
| □ | Samsung Phones | Default Customer | 1 | herculespopular22... | 2018/10/29 01:58... |
| □ | Flying Squad Devices | Default Customer | 1 | herculespopular22... | 2018/10/26 05:18... |

- The interface lists all groups of which the device is a member.
- Any device group profiles will also be applied to the endpoint.

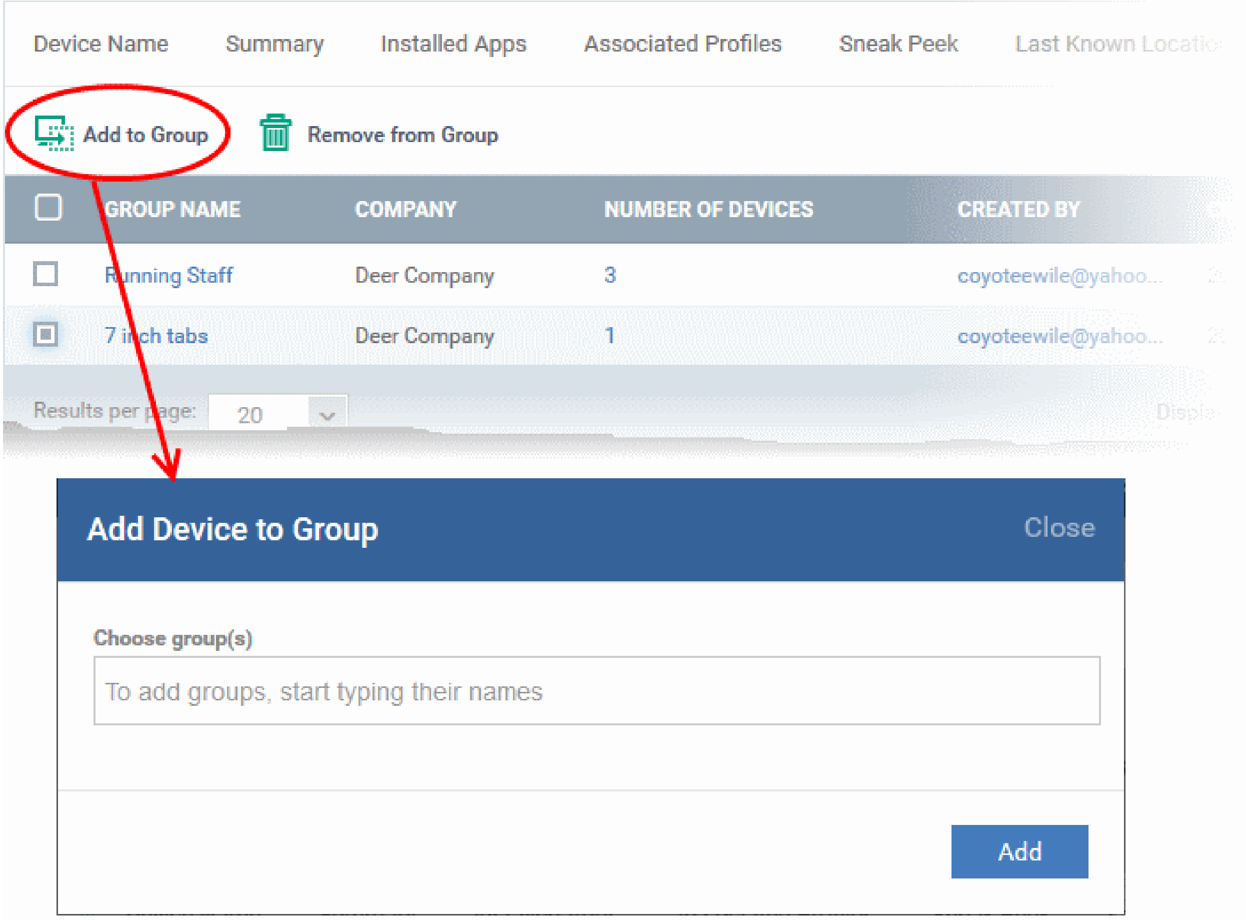
For more details about applying configuration profiles to device groups, see **Assign Configuration Profiles to a Device Group**.

| Device Groups - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Group | The group label.<br>• Click the group name to view and edit group details.<br>• See **Edit a Device Group** for more details. |
| Customer | The name of the company for which the group was created. |
| Number of Devices | The total count of devices in the group.<br>• Click the number to view and edit group details.<br>• See **Edit a Device Group** for more details. |

|  |  |
|---|---|
| Created By | Name of the admin who created the group.<br>• Click the name to view the admin's details.<br>• See **View the Details of a User** for more details. |
| Created | The date and time at which the group was created. |

### To add the device to a new group

- Click 'Add to Group'



| ☐ | GROUP NAME | COMPANY | NUMBER OF DEVICES | CREATED BY |
|---|---|---|---|---|
| ☐ | Running Staff | Deer Company | 3 | coyoteewile@yahoo... |
| ☐ | 7 inch tabs | Deer Company | 1 | coyoteewile@yahoo... |

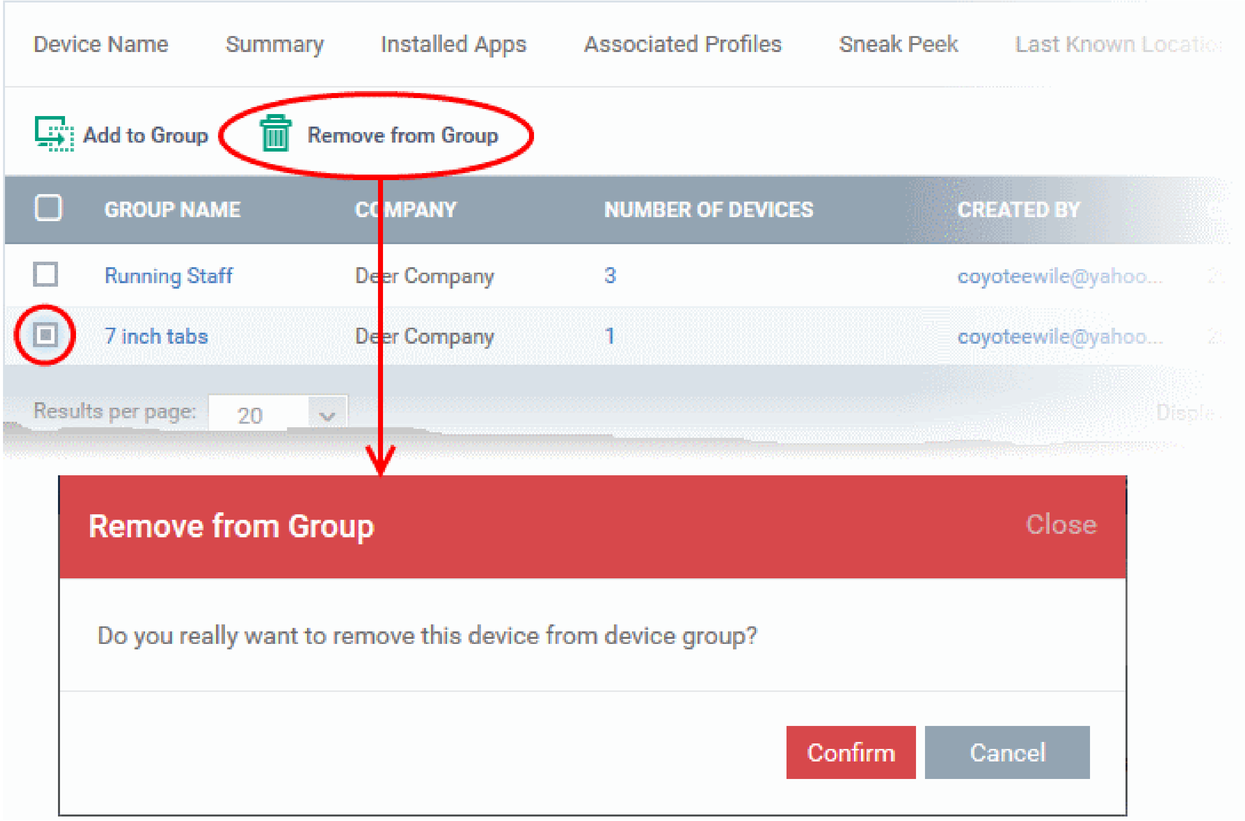
The 'Add Device to Group' dialog will appear.

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

The device will be added to the group.

### To remove the device from a group

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



| □ | GROUP NAME | COMPANY | NUMBER OF DEVICES | CREATED BY |
|---|---|---|---|---|
| □ | Running Staff | Deer Company | 3 | coyoteewile@yahoo... |
| ▣ | 7 inch tabs | Deer Company | 1 | coyoteewile@yahoo... |

Remove from Group

Do you really want to remove this device from device group?

A confirmation dialog will appear.

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

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

## 5.2.6. View User Information

- User information tells you about the owner of a device. Details include email address and phone number.

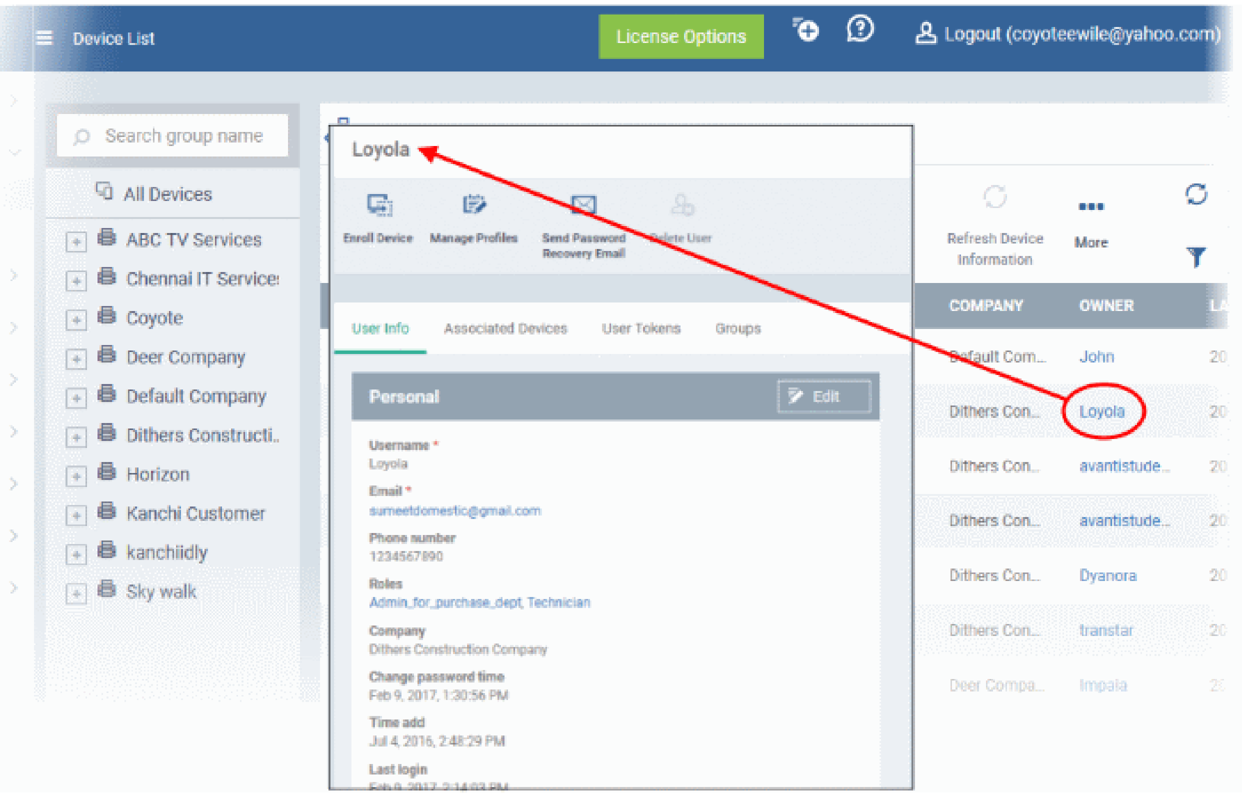
**To view the user information of a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM

The 'Owner' column shows the user of each device.

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



Loyola

Username *
Loyola

Email *
sumeetdomestic@gmail.com

Phone number
1234567890

Roles
Admin_for_purchase_dept, Technician

Company
Dithers Construction Company

Change password time
Feb 9, 2017, 1:30:56 PM

Time add
Jul 4, 2016, 2:48:29 PM

Last login
Feb 9, 2017, 2:14:03 PM

| COMPANY | OWNER |
|---|---|
| Default Com... | John |
| Dithers Con... | Loyola |
| Dithers Con... | avantistude... |
| Dithers Con... | avantistude... |
| Dithers Con... | Dyanora |
| Dithers Con... | transtar |
| Deer Compa... | Impala |

## 5.2.7. Remove a Device

- Click 'Devices' > 'Device List'
- Select target devices
- Click 'Delete Device'.

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

**Windows Devices** - You have the option to also uninstall the communication and/or security client when removing the device.

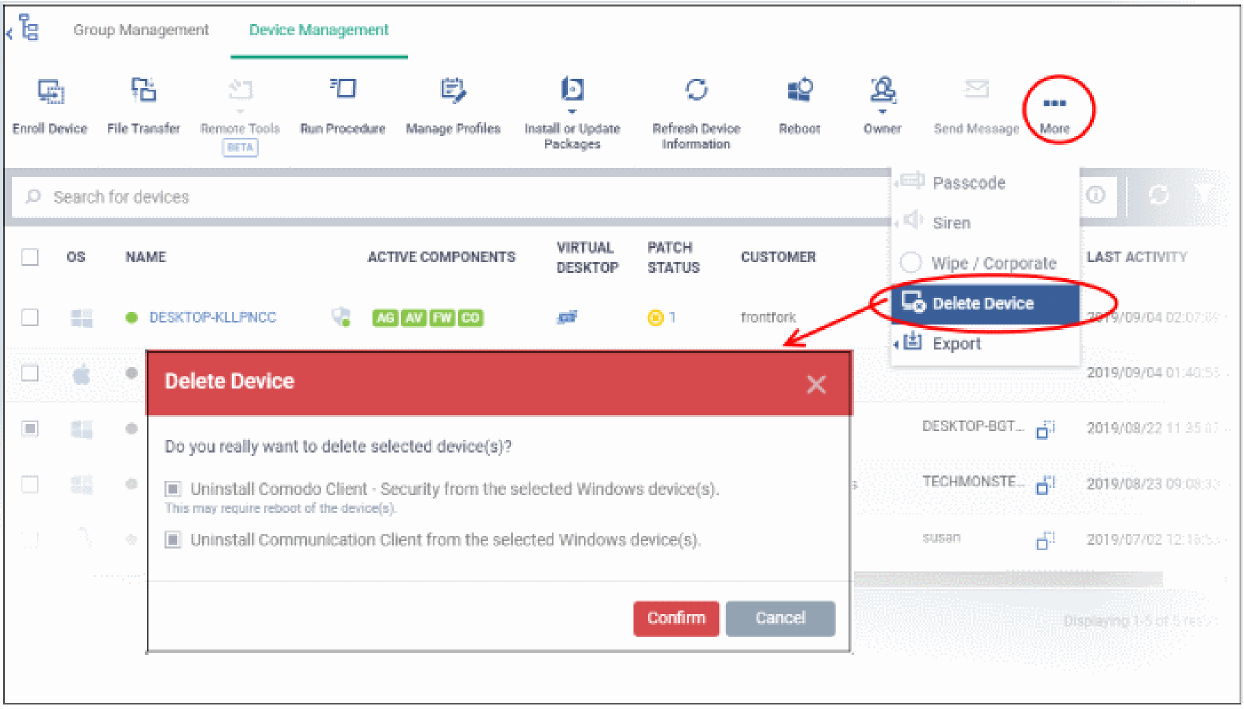
**Android, iOS, Mac OS and Linux devices** - Users can manually uninstall the clients and iOS profile from their device. **Instructions for uninstalling the agent/software** are available at the end of this section.

If you wish to reinstate the device in future then you need to re-enroll it. Device enrollment is explained in **Enroll User Devices for Management**.

### Remove a device from Endpoint Manager

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Select the devices you want to remove
- Click 'Delete Device' from the options at the top. If 'Delete Device' is not available, click 'More' at top-right then 'Delete Device' from the options.



Delete Device

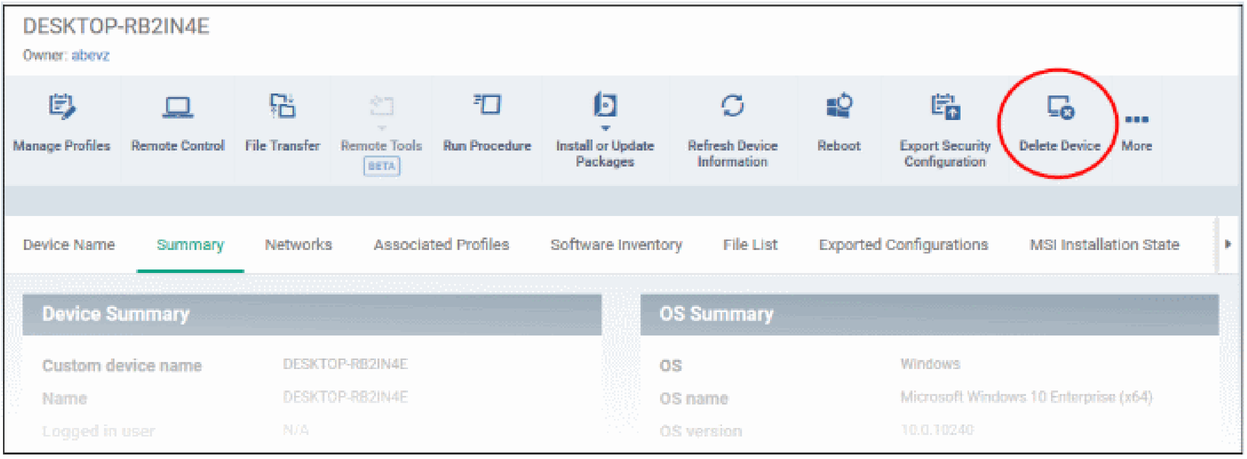
Do you really want to delete selected device(s)?

☐ Uninstall Comodo Client - Security from the selected Windows device(s).
This may require reboot of the device(s).

☐ Uninstall Communication Client from the selected Windows device(s).

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

- Click 'Devices' and choose 'Device List'.
- Click on the name of the device to be removed to open the device details interface.



DESKTOP-RB2IN4E
Owner: abevz

Device Summary

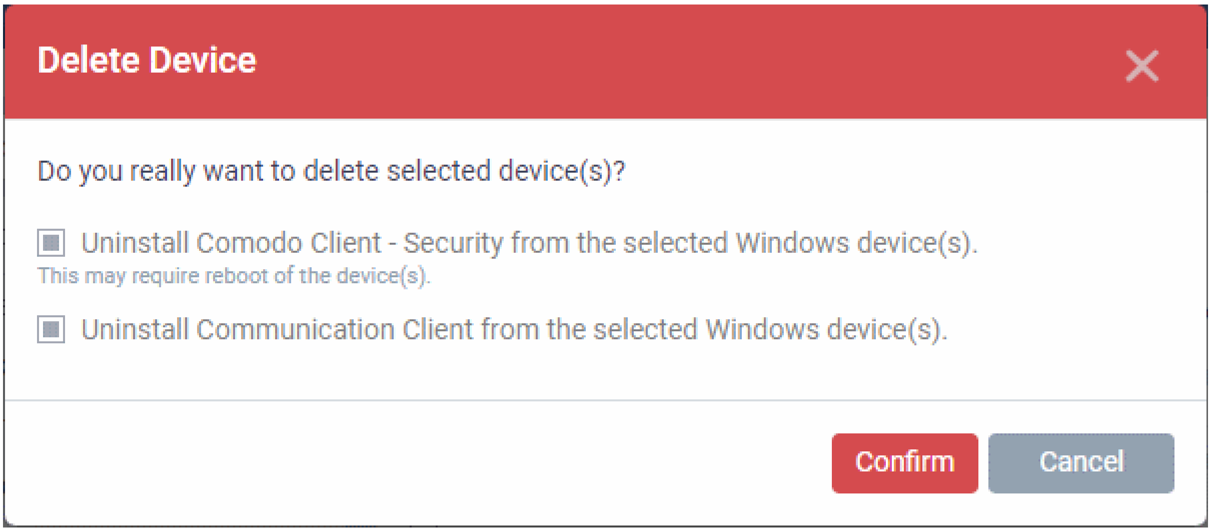
| | |
|---|---|
| Custom device name | DESKTOP-RB2IN4E |
| Name | DESKTOP-RB2IN4E |
| Logged in user | N/A |

OS Summary

| | |
|---|---|
| OS | Windows |
| OS name | Microsoft Windows 10 Enterprise (x64) |
| OS version | 10.0.10240 |

- Click 'Delete Device' from the options at the top. If 'Delete Device' is not available here, click 'More' at the top right and choose 'Delete Device' from the options.

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



Do you really want to delete selected device(s)?

▣ Uninstall Comodo Client - Security from the selected Windows device(s).
This may require reboot of the device(s).

▣ Uninstall Communication Client from the selected Windows device(s).

- Click 'Confirm' to remove the device from Endpoint Manager.

**Remove the communication client app from an Android device**

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

The communication client app will be removed from the device.

**Remove the EM profile from an iOS device**

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

The EM profile will be removed from the device.

**Remove the EM profile from Mac devices**

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

The Endpoint Manager profile will be removed from the device.

**Remove the communication client from Linux devices**

- Open the console terminal
- Enter the following command:

```
$ sudo systemctl stop itsm && sudo systemctl disable itsm && sudo rm -f /etc/systemd/system/itsm.service
&& sudo rm -rf /opt/COMODO.
```

## 5.2.8. Remote Management of Windows and Mac OS Devices

- Click 'Settings' > 'Portal Setup' > 'Extensions Management' to enable remote control for your account.
- The remote control feature lets you remotely access Windows and Mac devices to solve issues, install third party software, and run system maintenance.
- You can also transfer files and folders between the local and remote computers.

You can manage Windows and Mac devices with the following tools:

- **Remote Control** - Windows and Mac OS devices. Recommended for most users.
- **Comodo Remote Monitoring and Management (RMM)** - Windows only. This is a legacy tool for Comodo RMM and is not recommended for most users.

## Remote Control

- First, install the remote control application on your admin computer:
    - Click 'Devices' > 'Bulk Installation Package'
    - Click the 'Remote Control by ITarian' tab
    - Choose the operating system of your admin machine
    - Click 'Download'
- After installation, there are two ways you can take over devices:
    - Use the standalone remote control application

      OR
    - Use Endpoint Manager - Click 'Devices' > 'Device List' > 'Device Management' > select a device > click the 'Remote Control' button.
- For additional security, you can assign custom ports on the device to handle the remote connection. You can configure the ports by adding a 'Remote Control' section to the device profile.
    - See **Remote Control Settings** for Windows devices and **Remote control Settings for Mac OS Profile** if you want to read more about this.
- The viewer supports clip-board sharing between your computer and the managed device.
- You can also use key combinations such as 'Ctrl+Alt+Del', 'Alt+F4' and 'Ctrl+C' on the remote machine.
- You can view individual or all monitors if the target has a multi-monitor setup

See the following sections for more help:

- **Download and install the viewer**
- **Use the viewer**
- **Transfer files and folders to / from remote computer**

## Download and install the viewer

- Click 'Devices' > 'Bulk Installation Package'
- Select the 'Remote Control by ITarian' tab
- Choose the operating system of your admin machine
- Click 'Download'.
- Install on your local machine

Comodo Dragon / C1 customers - You can also download the app from the Dragon / C1 portal.

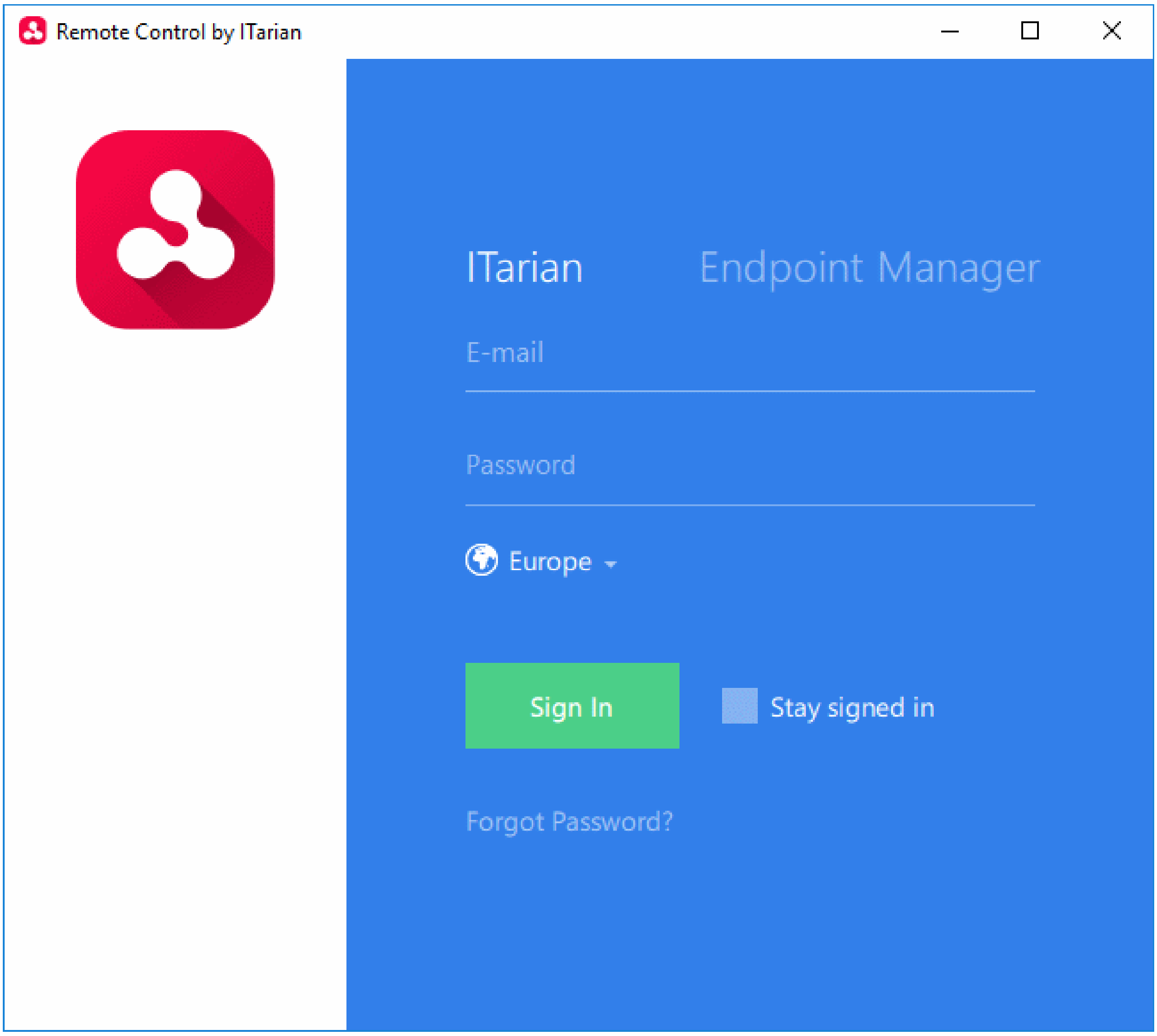
- Login to C1 / Dragon
- Click 'Tools' on the menu bar
- Locate the 'Remote Control by ITarian' tile
- Click 'Download'
- Install on your local machine

## Use the viewer

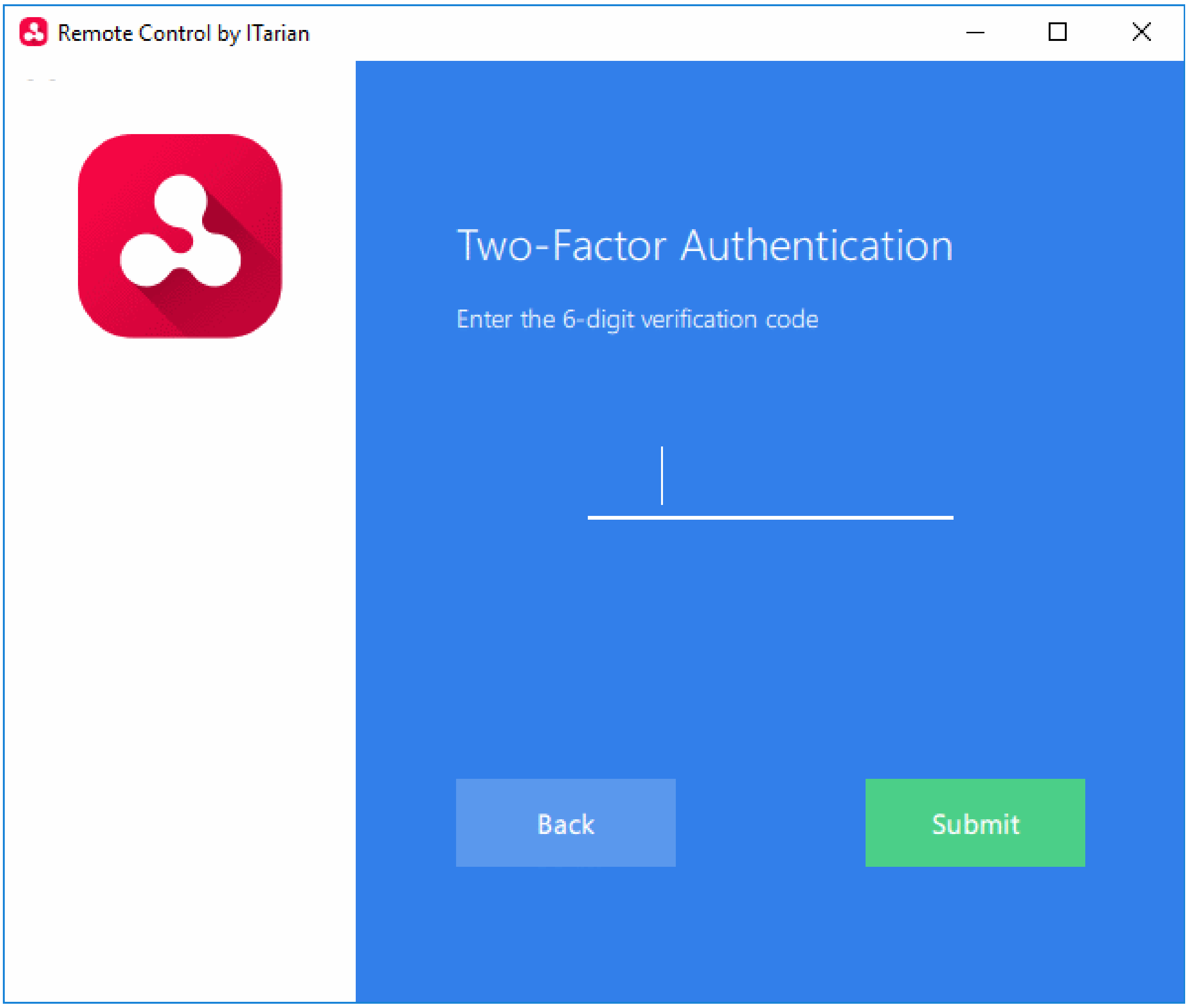
- Once installed, you can launch the remote control viewer from your desktop
- You can also take control direct from the EM interface:
    - Click 'Devices' > 'Device List' > 'Device Management' > select a Windows / Mac OS device > Click the 'Remote Control' button.
        - Note - A warning message is shown for Windows devices if you attempt remote control outside of a **maintenance window**. This is shown if you access via EM interface.

**Access the remote control viewer**

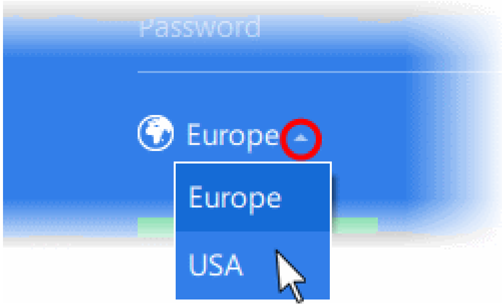
- Double click the desktop shortcut or the system tray icon to open the login screen:



- **Comodo Dragon and Comodo One customers** - Click the 'ITarian' tab then login with your Comodo Dragon / Comodo One portal username and password
    - If 'Two-Factor Authentication' is enabled for your account, then you have to enter the authentication code generated in the 'Google Authenticator' app on your mobile device. **Click here** to find out how to configure two-factor login settings.

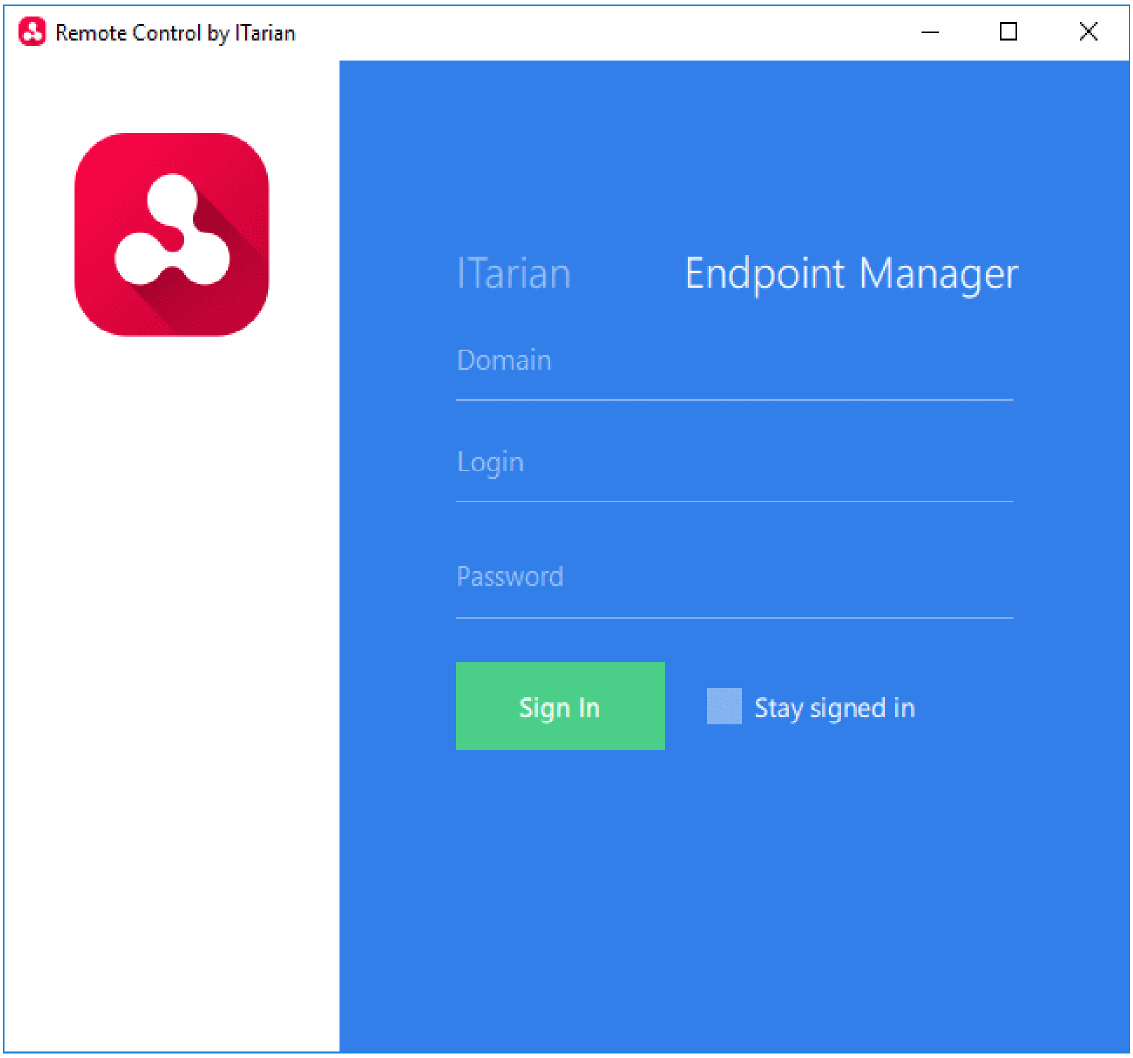

Remote Control by ITarian
Two-Factor Authentication
Enter the 6-digit verification code
Back
Submit

- Enter the code and click 'Submit'
  - The region selector allows you to choose the CD or C1 hosted service closest to your location. Select the location nearest to you for the best performance / fastest connection.



  - Select 'Stay Signed in' if you want the RC application to store your login credentials. The application will not ask for your credentials to login in future.
  - Click 'Sign In'

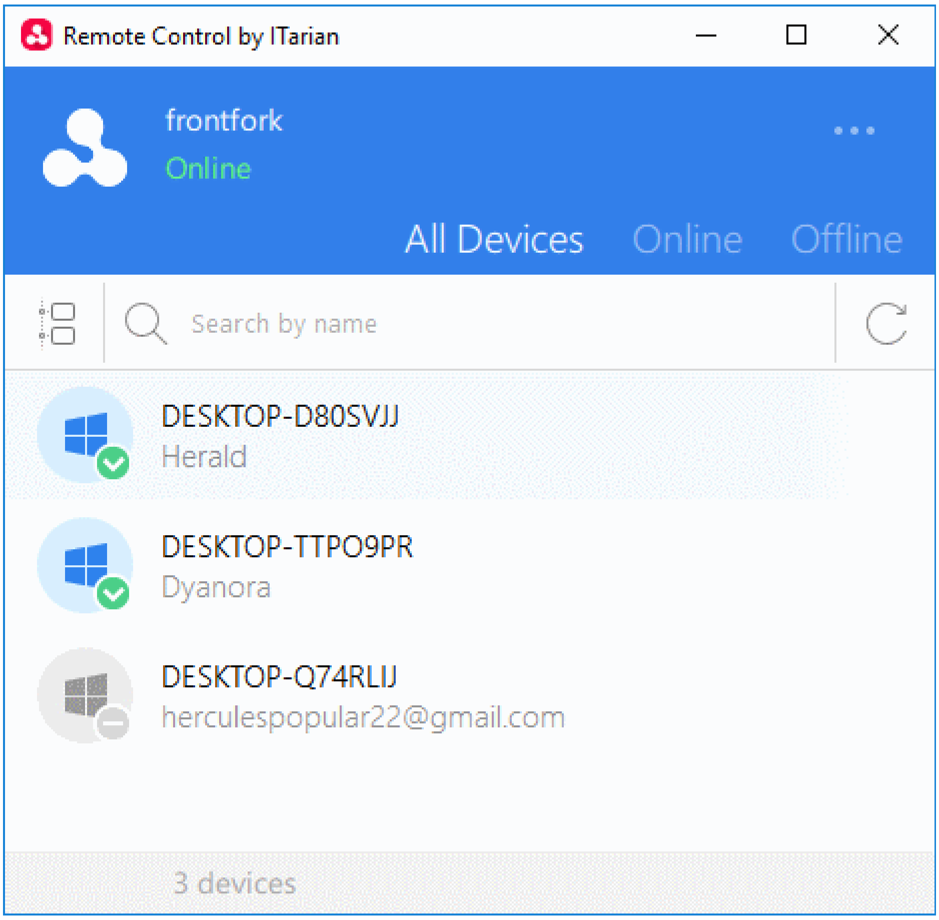
- **Stand-alone Endpoint Manager customers -** Click the 'Endpoint Manager' tab then enter your Endpoint Manager URL and your login credentials. Your EM URL will use the format https://<your company name>.cmdm.comodo.com, where <your company name> is your EM company name.



- Select 'Stay Signed in' if you want the RC application to store your login credentials. The application will not ask for your credentials to login in future.
- Click 'Sign In'

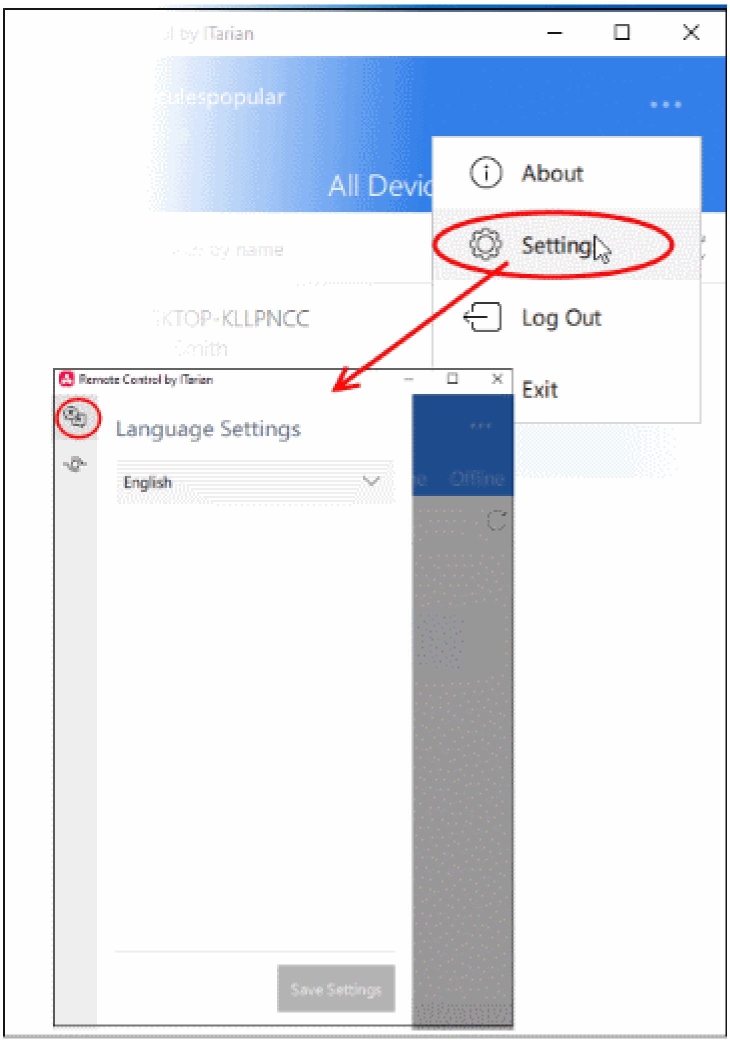
**Tip**: The remote control application will save your login credentials even if you forget to enable 'Stay Signed in'.

The viewer application will open with a list of enrolled Windows / Mac OS endpoints:



**Language Settings**

- Click the ellipsis button at top-right of the app
- Click 'Settings' to open language options:

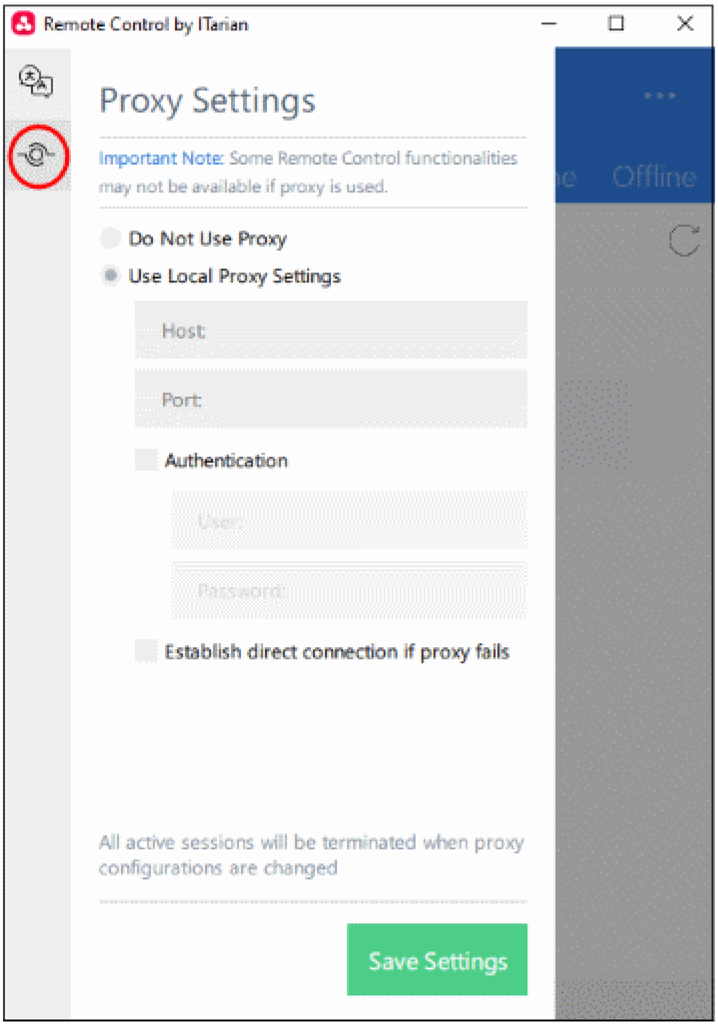


- Choose the language you require from the drop-down then click 'Save Settings'. This determines the language you see in the remote control application.
  - A notification box is shown on endpoints when you take over their machine. This box states the name of the person connected and the session duration etc.
  - The notification is in the language of the operating system IF the OS is English, Russian, Spanish, German, French, Portuguese or Chinese.
  - English is used if the OS is of any other language.
  - Examples:
    - You choose 'Russian' but connect to a Spanish PC - Notification is shown in Spanish.
    - You choose 'Russian' but connect to a Bulgarian PC - Notification is shown in English
    - You choose 'Russian' and connect to a Russian PC - Notification is shown in Russian

### Proxy Server Settings

You can configure a proxy through which you want to connect to managed endpoints.

- Click the ellipsis button then 'Settings'
- Click the proxy server icon on the left of the settings page:



Proxy Settings

Important Note: Some Remote Control functionalities may not be available if proxy is used.

● Do Not Use Proxy
● Use Local Proxy Settings

Host:

Port:

□ Authentication

User:

Password:

□ Establish direct connection if proxy fails

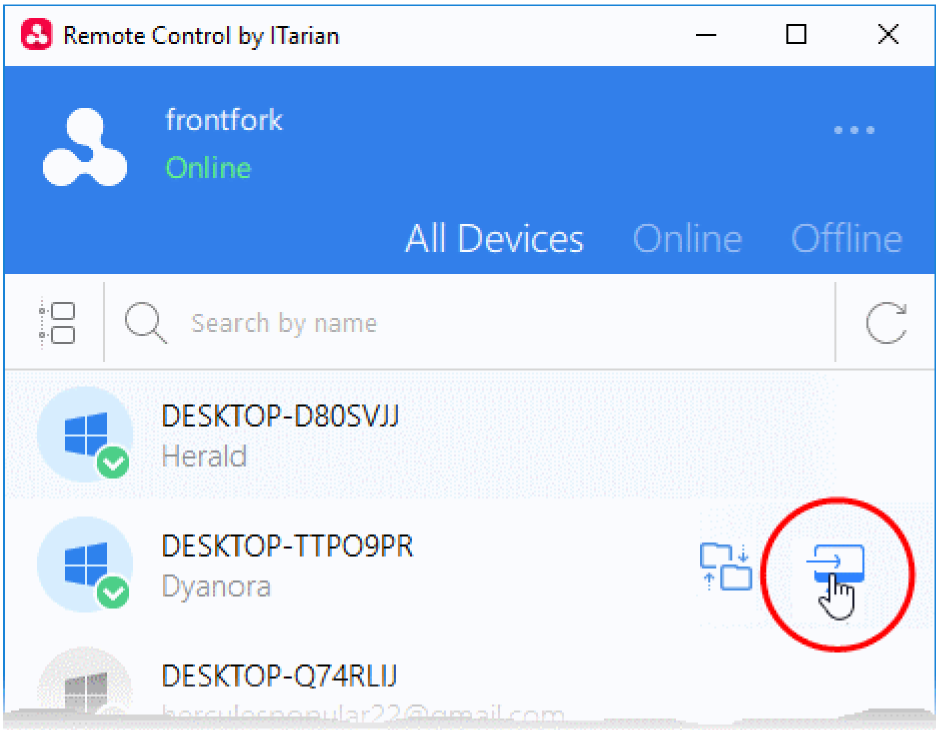
All active sessions will be terminated when proxy configurations are changed

Save Settings

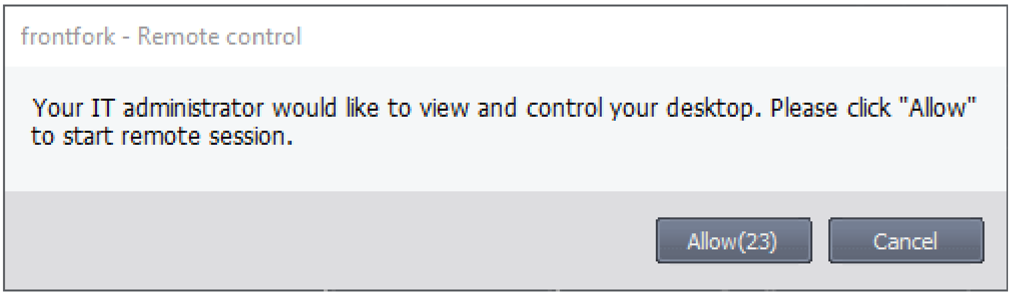
- **Do Not Use Proxy -** The remote control tool will establish a direct connection to the endpoint
- **Use Local Proxy Settings -** Use a proxy to connect to endpoints.
  - **Host -** Enter the IP address or the hostname of your proxy server
  - **Port -** The port on your proxy server that the remote control tool should connect to.
- **Authentication -** If your proxy server requires authentication, enter the UN/PW here.
- **Establish direct connection if proxy fails -** Allow the remote control tool to fallback to a direct internet connection if the proxy fails.
  - If you specify a proxy *but* disable direct connection, then the remote control tool will not be able to connect to endpoints if the proxy fails
  - Leave the direct connection option enabled to ensure you can access endpoints at all times
- Click 'Save Settings'

### Remotely manage an endpoint

- Move your mouse over an endpoint and click the remote desktop icon on the right:



The following message is shown to end-users if configured appropriately:

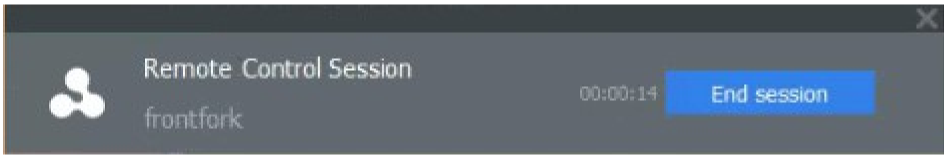

frontfork - Remote control

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

You have the following options:

- Take remote control of the device without permission from the user
- Ask for permission and take control if the user allows. Automatically take control if the user does not respond.
- Disable remote control entirely
- See **Remote Control Settings** for more details.

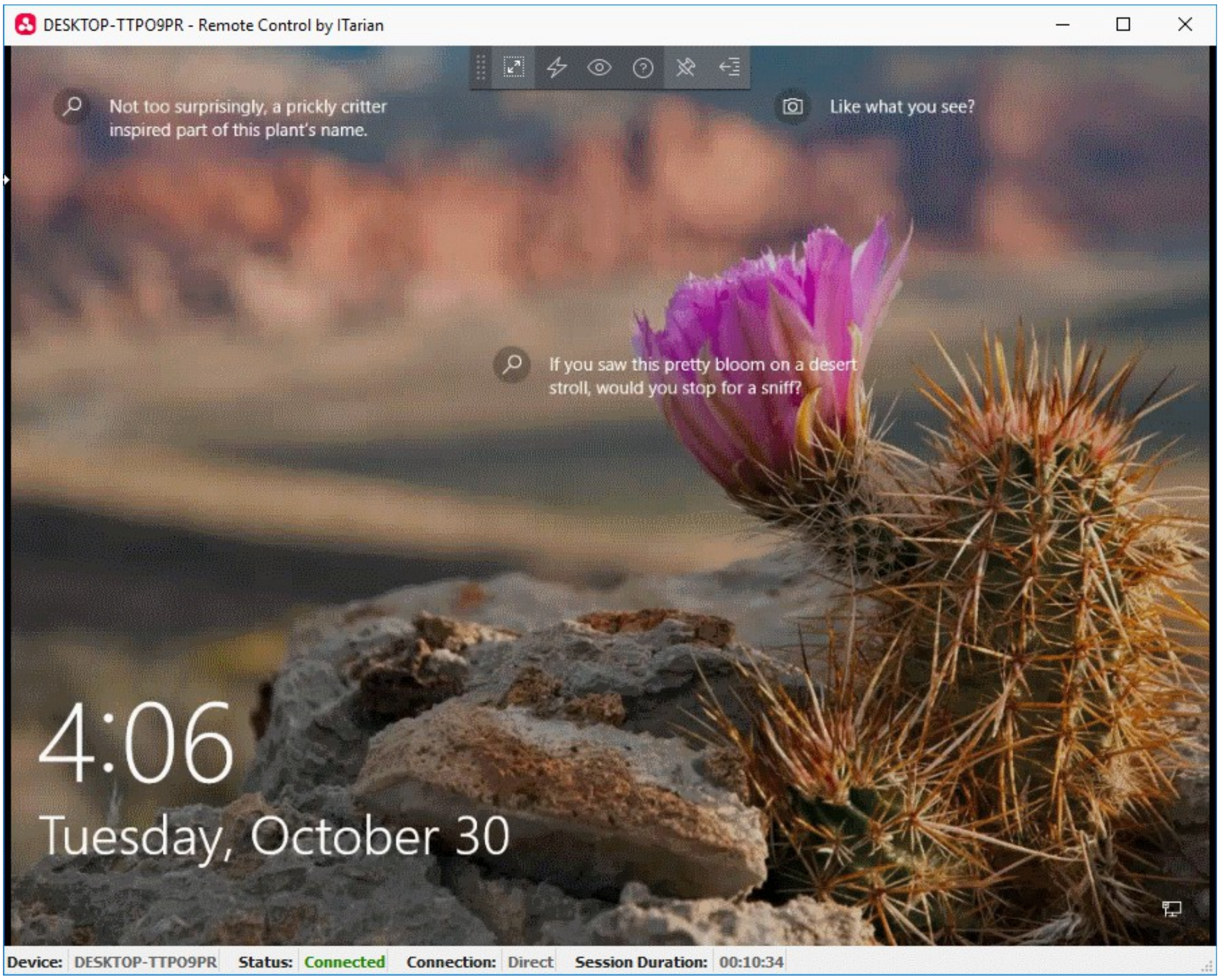
The following notification appears on the endpoint when you have established control:



You can configure the endpoint notification box in the 'Remote Control' section of a profile.

- Click 'Configuration Templates' > 'Profiles' > 'Add Profile Section' > 'Remote Control'

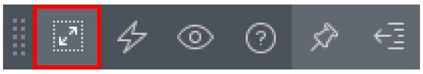
You can now access the desktop of the remote computer:


DESKTOP-TTPO9PR - Remote Control by ITarian

Not too surprisingly, a prickly critter inspired part of this plant's name.
Like what you see?
If you saw this pretty bloom on a desert stroll, would you stop for a sniff?
4:06
Tuesday, October 30

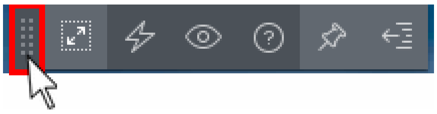
**Device:** DESKTOP-TTPO9PR **Status:** Connected **Connection:** Direct **Session Duration:** 00:10:34

- You can interact with the target device to perform tasks as required.
- Use the toolbar at the top of the interface to perform the following actions:

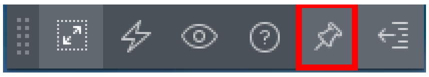


Full Screen - The remote desktop will cover your entire display, without the operating system's window-framing interface.

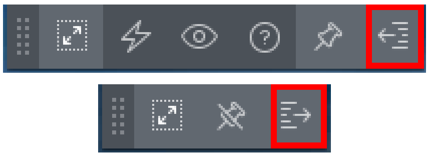
- Click the same icon to exit full screen mode



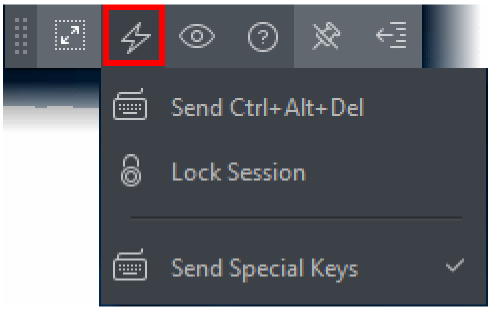
Position - Click and drag the tool bar to your preferred location.



Pin - Lock or unlock the tool bar to the title bar in full screen view.

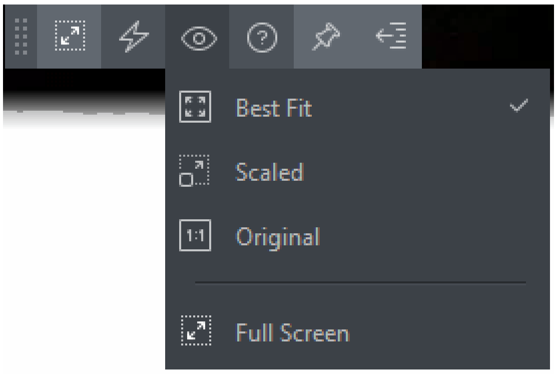


Minimize/Maximize - Show/hide tool bar options.



Actions - Send control commands to the endpoint.

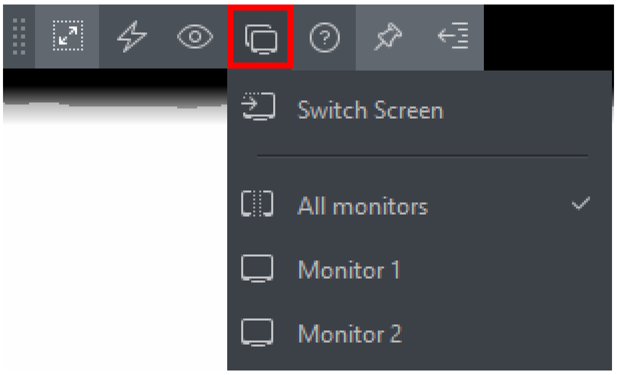
- **Send Ctrl + Alt + Del** - (Available only for Windows devices) Opens the Windows security screen. This allows you to lock the computer, log the current user out of the remote machine, change passwords, view the local task manager or shut down/restart/hibernate the machine.
- **Lock Session** - Locks the managed endpoint. A password will be required to unlock the endpoint.
- **Send Special Keys** - If enabled, allows you to send key combination commands such as Ctrl+C, Windows + R and so on.
  - The special key combinations are dependent on the operating systems of the local (admin) device and the managed remote device. See the **list of available special key combinations** given below.



View - Change the display size of the remote desktop. The available options are:

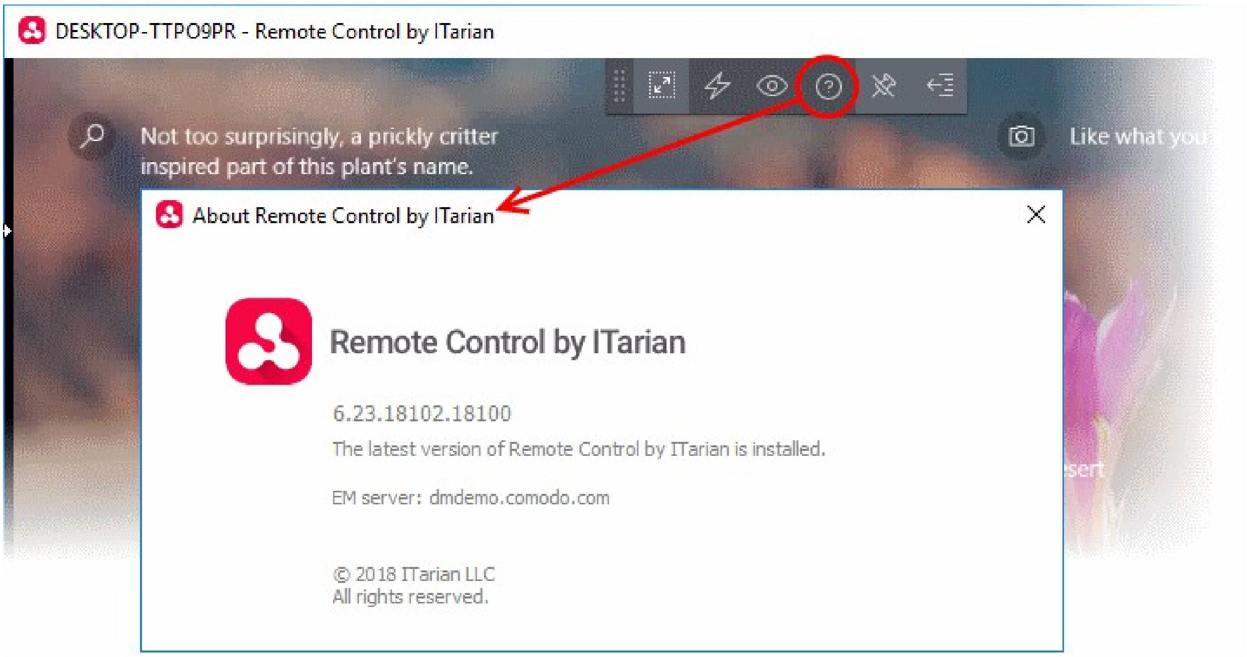
- **Best Fit** - Automatically adjusts the screen resolution for the best visual experience.
- **Scaled** - Displays the target desktop with the resolution of the admin computer
- **Original** - Displays the target desktop at its own resolution
- **Full screen** - Displays the remote desktop in full screen view

**Multi-Screen** - The multi-screen icon only appears if the target point endpoint has a multi-monitor setup. The drop-down shows all monitors connected to the endpoint and allows you to choose which to view.



- Select 'Switch Screen' to move to the next screen on the list
- Select 'All Monitors' to view all connected screens simultaneously
- Select an individual monitor to view it in stand-alone mode

**Help** - Shows the 'About Remote Control' dialog which shows version number and copyright information.


DESKTOP-TTPO9PR - Remote Control by ITarian

Not too surprisingly, a prickly critter inspired part of this plant's name.
Like what you

About Remote Control by ITarian

Remote Control by ITarian

6.23.18102.18100

The latest version of Remote Control by ITarian is installed.

EM server: dmdemo.comodo.com

© 2018 ITarian LLC
All rights reserved.

## Special Key Combinations

| Admin Device | Managed Remote Device | |
|---|---|---|
| | **Windows** | **Mac OS** |
| **Windows** | 'Windows' key is sent only to the remote device<br>Shortcuts in combination with 'Windows' key are applied only to the remote device | 'Windows'/'Command' key is sent only to the remote device. Exceptions:<br>• Ctrl+Alt+Del<br>• Win+L<br>PRINT SCREEN and NUMLOCK are not sent to remote device<br>NumPad digit keys always behave as arrow-keys on Mac OS<br>'Context Menu' key is sent as zero scan code and appears as key 'a'. |
| **Mac OS** | All Shortcuts with 'Windows'/'Command' key are applied to the remote device, except 'Windows'/'Command' key+Esc<br>Command+Tab - Switches between applications<br>F11 - Shows desktop<br>Ctrl +Up Arrow - Shows all Windows<br>Ctrl+Down Arrow - Shows active application Window | If Apple is keyboard used:<br>Media buttons (e.g. PLAY , STOP, MISSION CONTROL), POWER, EJECT keys and all system shortcuts with these keys are applied only to the local device.<br>Shortcuts with COMMAND are applied to the remote device, except 'COMMAND' key+Esc<br>• Command+Tab - Switches between applications<br>• Ctrl +Up Arrow - Shows all Windows<br>• Ctrl+Down Arrow - Shows active application Window<br>• Fn+F11 - Shows desktop |

| | | |
|---|---|---|
| | | • Fn+F12 - Shows Dashboard or enable standard key in Keyboard settings<br>• If non-Apple keyboard is used:<br>• Shortcuts with WIN are applied to the remote device, except 'WIN' key+Esc<br>• Command+Tab - Switches between applications<br>• Ctrl +Up Arrow - Shows all Windows<br>• Ctrl+Down Arrow - Shows active application Window<br>• F11 - Shows desktop<br>• F12 - Shows Dashboard |

- Full list of Windows keyboard shortcuts - **https://support.microsoft.com/en-us/help/12445/windows-keyboard-shortcuts**.
- Full list of MAC keyboard shortcuts - **https://support.apple.com/en-us/HT201236**.

### Use the RMM Console for Remote Control

Comodo's Remote Monitoring and Management (RMM) grants MSPs complete visibility and control over the systems they manage. C1 customers can use RMM to takeover Windows devices.

**Prerequisite** - You should have already installed the legacy RMM Technician Console on your admin computer and RMM plugins on the managed endpoints.

- Click 'Devices' > 'Device List' > 'Device Management'
- Select a Windows device then click the 'Remote Control' button
- Select 'With RMM Plugin' from the drop-down
- See **https://help.comodo.com/topic-289-1-719-8569-Support-Sessions-Interface-%E2%80%93-An-Overview.html** for more details.

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

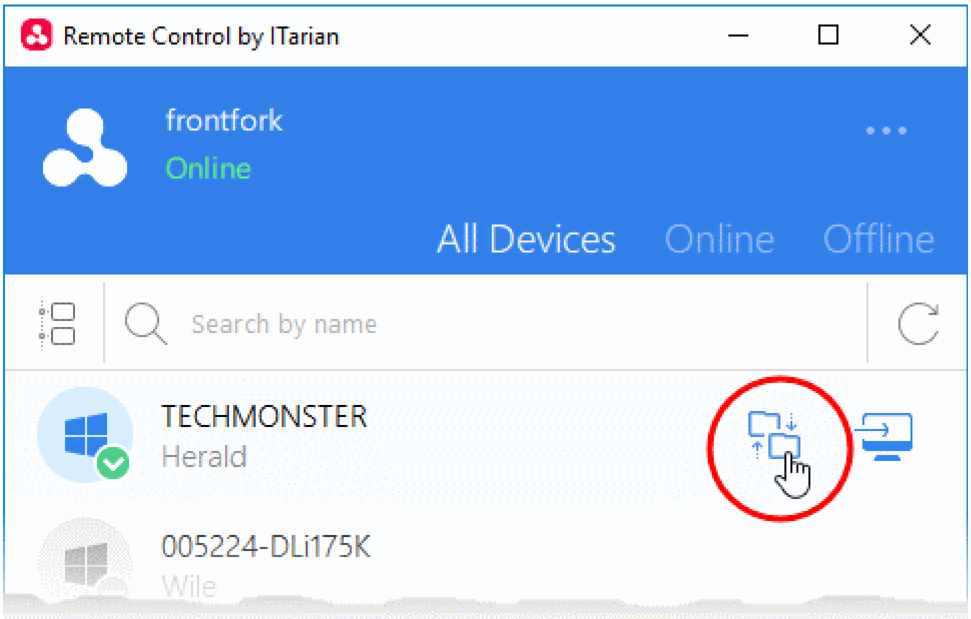
## 5.2.8.1. Transfer Items to / from the Remote Computer

There are two ways you can manage files on remote Windows devices:

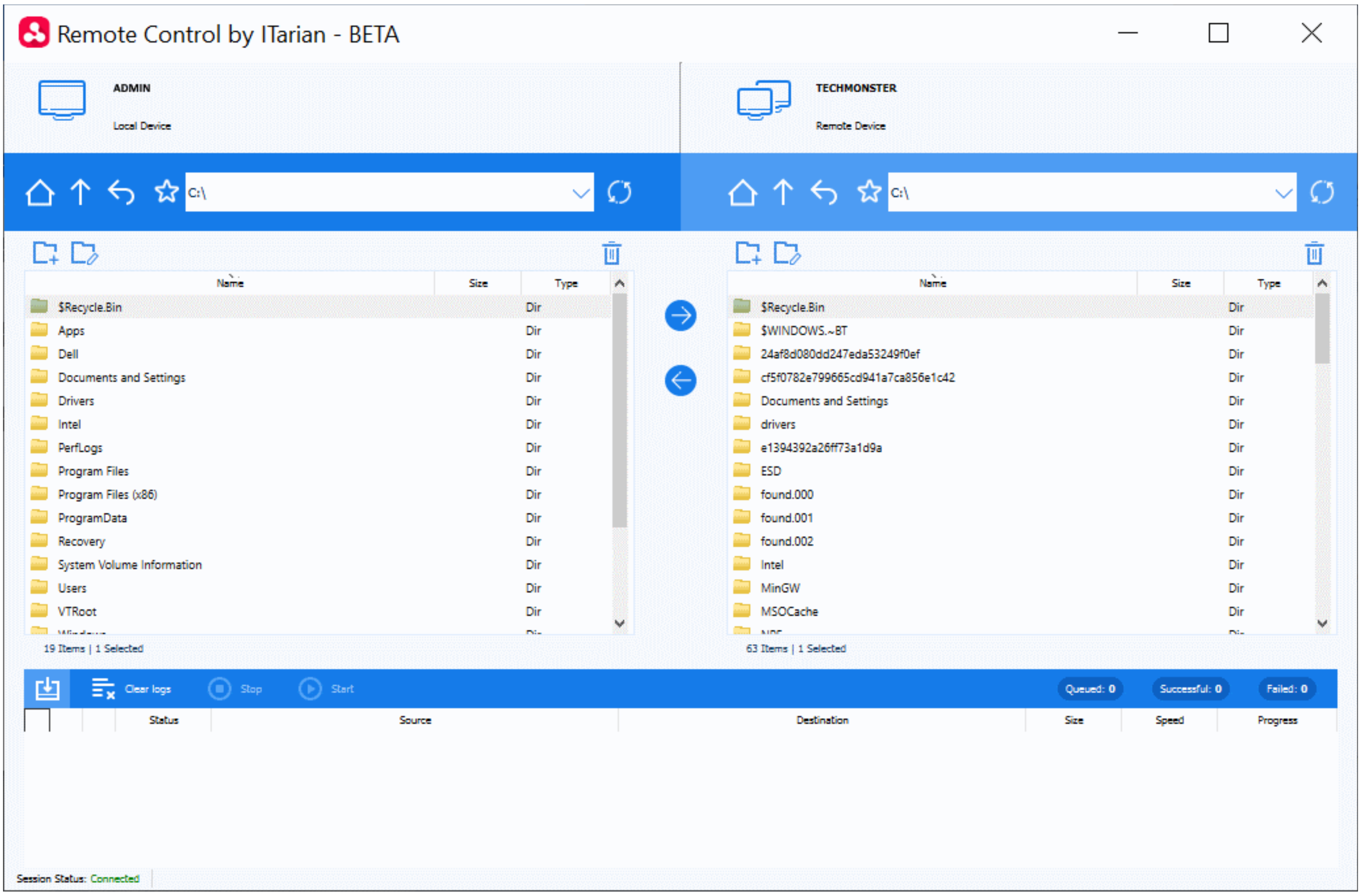
- **Endpoint Manager** - Click 'Devices' > 'Device List' > select a running Windows device > Click 'Remote Tools' > 'File Explorer'.
- **Remote Control application** - Click 'Devices' > 'Device List' > 'Device Management' > select a Windows device > Click the 'File Transfer' button.

This section explains how to transfer files using the remote control tool.

- Download and install the remote control app.
  - See **the previous section** for a list of steps if you haven't yet done this.
- Open and login to the remote control app.
- Move your mouse over an endpoint and click the file transfer icon on the right:



The interface shows the file systems of the local and remote computers in adjacent panes:



| Name | Size | Type |
|---|---|---|
| $Recycle.Bin | | Dir |
| Apps | | Dir |
| Dell | | Dir |
| Documents and Settings | | Dir |
| Drivers | | Dir |
| Intel | | Dir |
| PerfLogs | | Dir |
| Program Files | | Dir |
| Program Files (x86) | | Dir |
| ProgramData | | Dir |
| Recovery | | Dir |
| System Volume Information | | Dir |
| Users | | Dir |
| VTRoot | | Dir |

19 Items | 1 Selected

| Name | Size | Type |
|---|---|---|
| $Recycle.Bin | | Dir |
| $WINDOWS.~BT | | Dir |
| 24af8d080dd247eda53249f0ef | | Dir |
| cf5f0782e799665cd941a7ca856e1c42 | | Dir |
| Documents and Settings | | Dir |
| drivers | | Dir |
| e1394392a26ff73a1d9a | | Dir |
| ESD | | Dir |
| found.000 | | Dir |
| found.001 | | Dir |
| found.002 | | Dir |
| Intel | | Dir |
| MinGW | | Dir |
| MSOCache | | Dir |

63 Items | 1 Selected

| | | Status | Source | Destination | Size | Speed | Progress |
|---|---|---|---|---|---|---|---|

Session Status: Connected

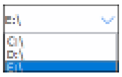
You can transfer files, create folders, rename folders and more:

⌂ - Go to the root folder of the selected drive/partition

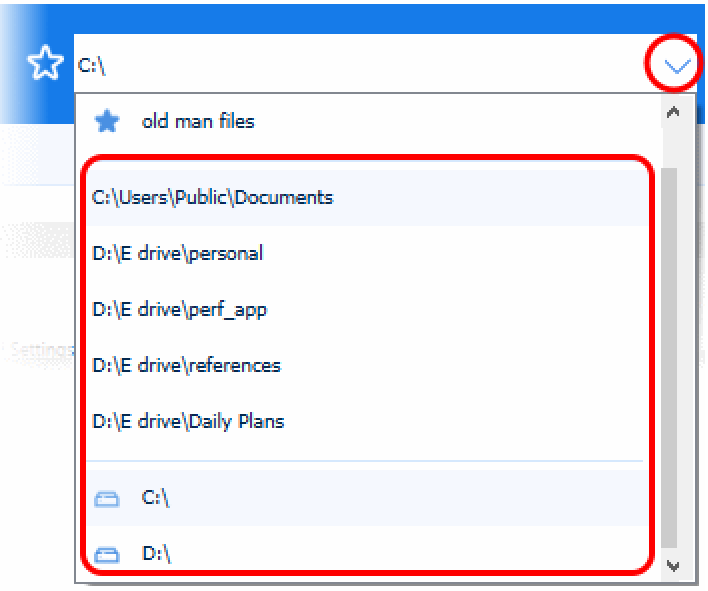
↑ - Go one level up

- Return to the previous location

- Add current folder to favorites.
  - You can add folders you often access to favorites
  - Click the address bar to access your favorite folders.
  - See **Add and manage favorites** if you need more help.



- Folder address bar
  - Use the drop-down to view recently accessed items and your favorites.
  - Recent folders shows the last five folders you accessed.



C:\

old man files

C:\Users\Public\Documents

D:\E drive\personal

D:\E drive\perf_app

D:\E drive\references

D:\E drive\Daily Plans

C:\

D:\

- Refresh the content

- Remove files / folders

- Create a new folder

- Rename a file / folder

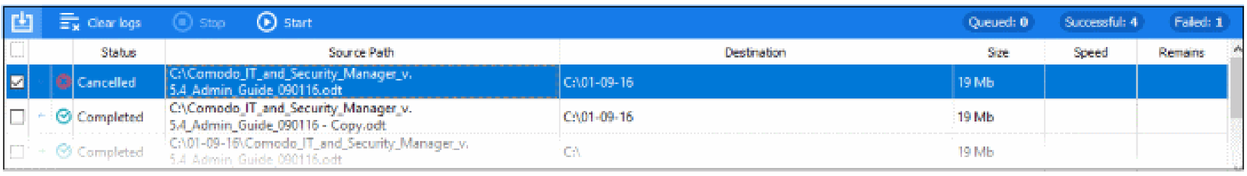
Send

- Transfer files from the local device to the remote device

Receive

- Transfer files from the remote device to the local device

- The lower pane shows the progress of your transfers:



| □ | Status | Source Path | Destination | Size | Speed | Remains |
|---|---|---|---|---|---|---|
| ☑ | Cancelled | C:\Comodo_IT_and_Security_Manager_v.<br>5.4_Admin_Guide_090116.odt | C:\01-09-16 | 19 Mb | | |
| □ | Completed | C:\Comodo_IT_and_Security_Manager_v.<br>5.4_Admin_Guide_090116 - Copy.odt | C:\01-09-16 | 19 Mb | | |
| □ | Completed | C:\01-09-16\Comodo_IT_and_Security_Manager_v.<br>5.4_Admin_Guide_090116.odt | C:\ | 19 Mb | | |

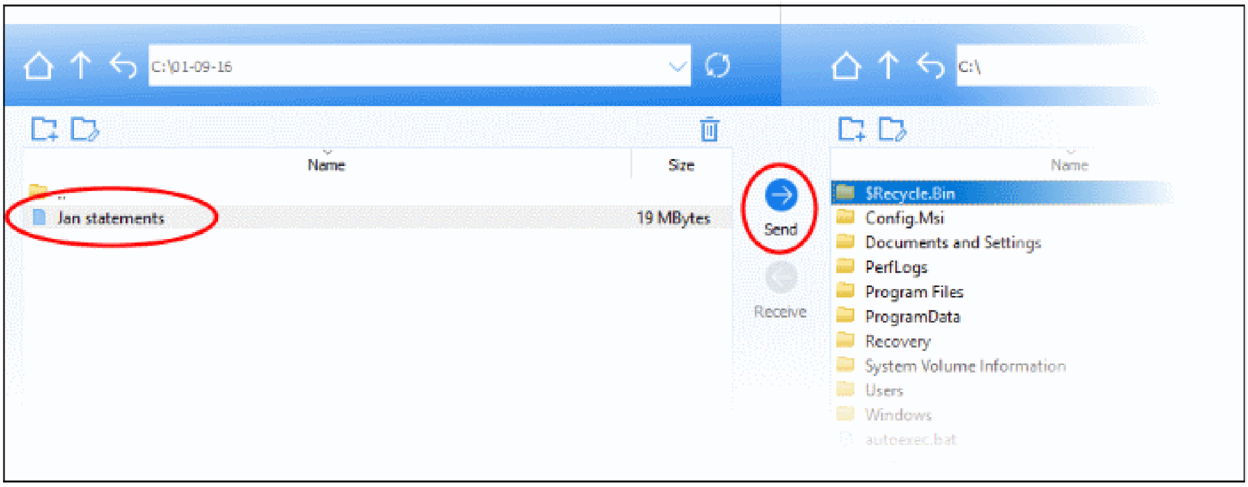
| File Transfer Tool Lower Pane - Column Descriptions | |
|---|---|
| **Column Header** | **Descriptions** |
| Status | The progress of the transfer. Possible statuses include 'Completed', 'In-progress', 'Canceled' or 'Failed'. |
| Source | Location of the file on the origin machine |
| Destination | Location to which the file is being copied. |
| Size | File size |
| Speed | The rate of the file transfer |
| Remains | Time left to complete the transfer |
| **Controls** | |
| ⤓ | Expand / collapse the pane |
| ≡× | Clears the transfer entries in the table |
| ▶ | Resume the canceled, failed file transfers |
| ■ | Stop a file transfer |
| **File transfer statuses shown on top-right** | |
| Queued | Number of files pending transfer |
| Successful | Number of files that completed transfer between devices |
| Failed | Number of files that did not complete the transfer |

From the remote control tool you can:

- **Copy files between the local and remote device**
- **Create a folder**
- **Edit a folder / file name**
- **Delete a folder / file**
- **Stop a file transfer**
- **Resume a file transfer**
- **Add folders to favorites**

## Transfer Files between Local and Remote Device

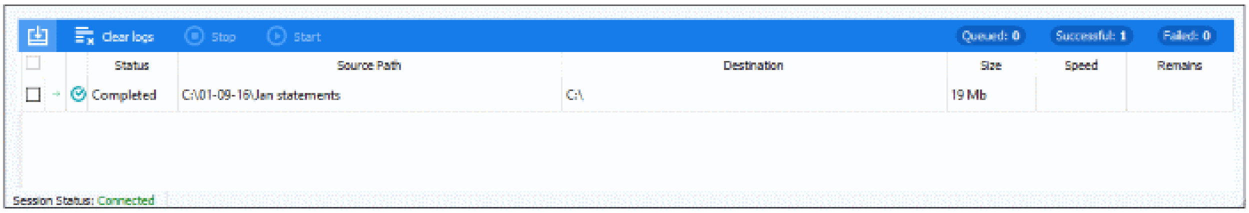
- Browse and select the file that you want to transfer and click 'Send' / 'Receive'
  - You can select multiple items to transfer



| Name | Size |
|---|---|
| .. | |
| Jan statements | 19 MBytes |

| Name |
|---|
| $Recycle.Bin |
| Config.Msi |
| Documents and Settings |
| PerfLogs |
| Program Files |
| ProgramData |
| Recovery |
| System Volume Information |
| Users |
| Windows |
| autoexec.bat |

- You can view the status of the transfer in the lower pane.



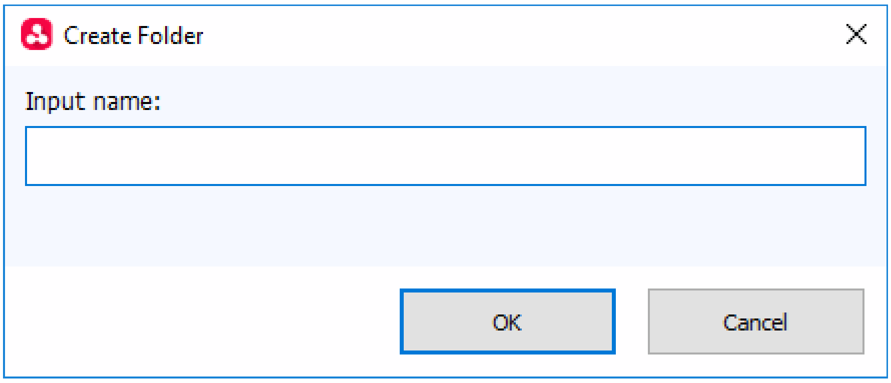
| | Status | Source Path | Destination | Size | Speed | Remains |
|---|---|---|---|---|---|---|
| □ | Completed | C:\01-09-16\Jan statements | C:\ | 19 Mb | | |

Session Status: Connected

- Note - You can send and receive files at the same time. Select a file in local device and in remote device. Click 'Send' and 'Receive' buttons.

## Create a Folder

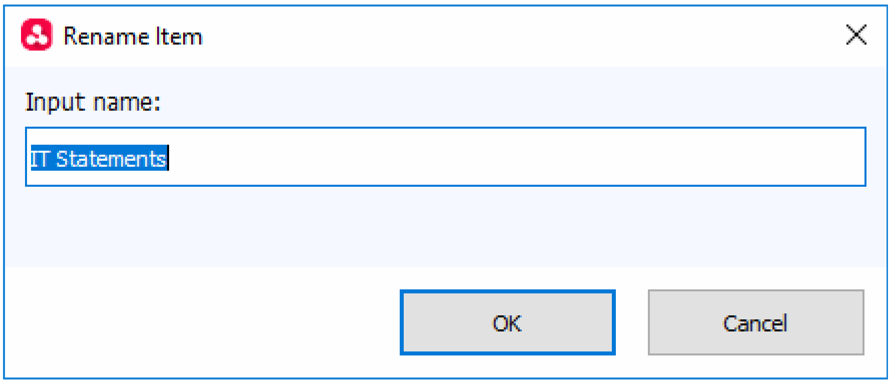
- Click the folder icon in the local or remote device



- Enter folder name and click 'OK'

## Edit a Folder / File Name

- Select a folder / file and click the edit icon in the local or remote device



Rename Item

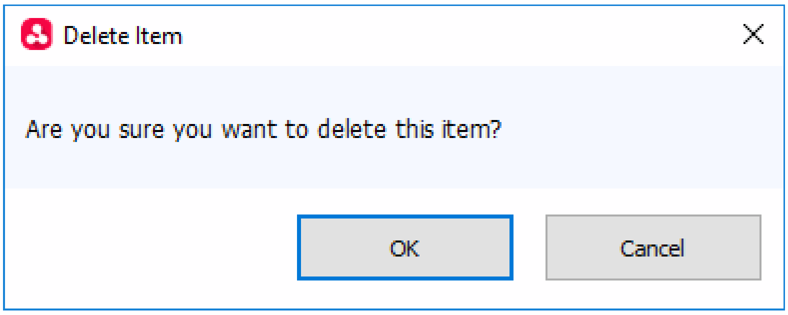
Input name:

IT Statements

- Update the name of the folder / file and click 'OK'
  - Alternatively, just click on an item and rename it.

## Delete a Folder / File

- Select a folder / file and click the trash can icon in the local or remote device



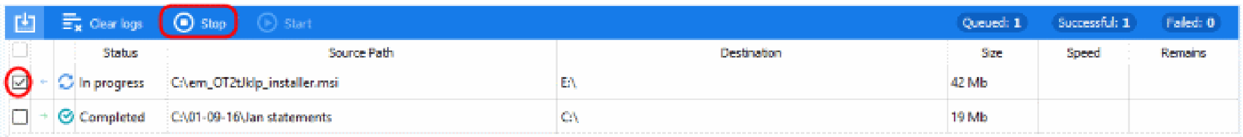
Delete Item

Are you sure you want to delete this item?

- Click 'OK' to confirm

## Stop a File Transfer

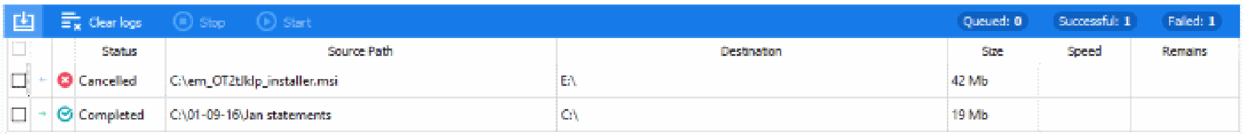
- To stop a file transfer that is in progress, select it from the status pane below and click 'Stop'



Queued: 1 Successful: 1 Failed: 0

| | Status | Source Path | Destination | Size | Speed | Remains |
|---|---|---|---|---|---|---|
| ☑ | In progress | C:\em_OT2tJklp_installer.msi | E:\ | 42 Mb | | |
| □ | Completed | C:\01-09-16\Jan statements | C:\ | 19 Mb | | |

- The file transfer process is canceled



Queued: 0 Successful: 1 Failed: 1

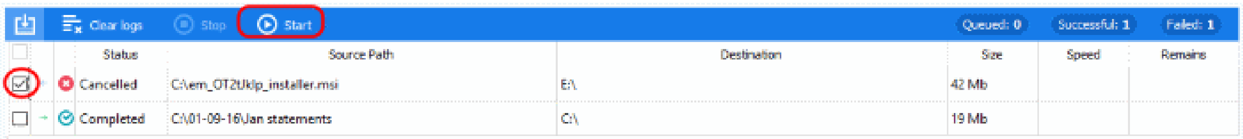
| | Status | Source Path | Destination | Size | Speed | Remains |
|---|---|---|---|---|---|---|
| □ | Cancelled | C:\em_OT2tJklp_installer.msi | E:\ | 42 Mb | | |
| □ | Completed | C:\01-09-16\Jan statements | C:\ | 19 Mb | | |

You can **resume the transfer** or remove from the status list.

- Click 'Clear Logs' at the top to remove all entries

## Resume a File Transfer

- Select a stopped file transfer and click 'Start' at the top



| ☐ | Status | Source Path | Destination | Size | Speed | Remains |
|---|---|---|---|---|---|---|
| ☑ | Cancelled | C:\em_OT2Uklp_installer.msi | E:\ | 42 Mb | | |
| ☐ | Completed | C:\01-09-16\Jan statements | C:\ | 19 Mb | | |

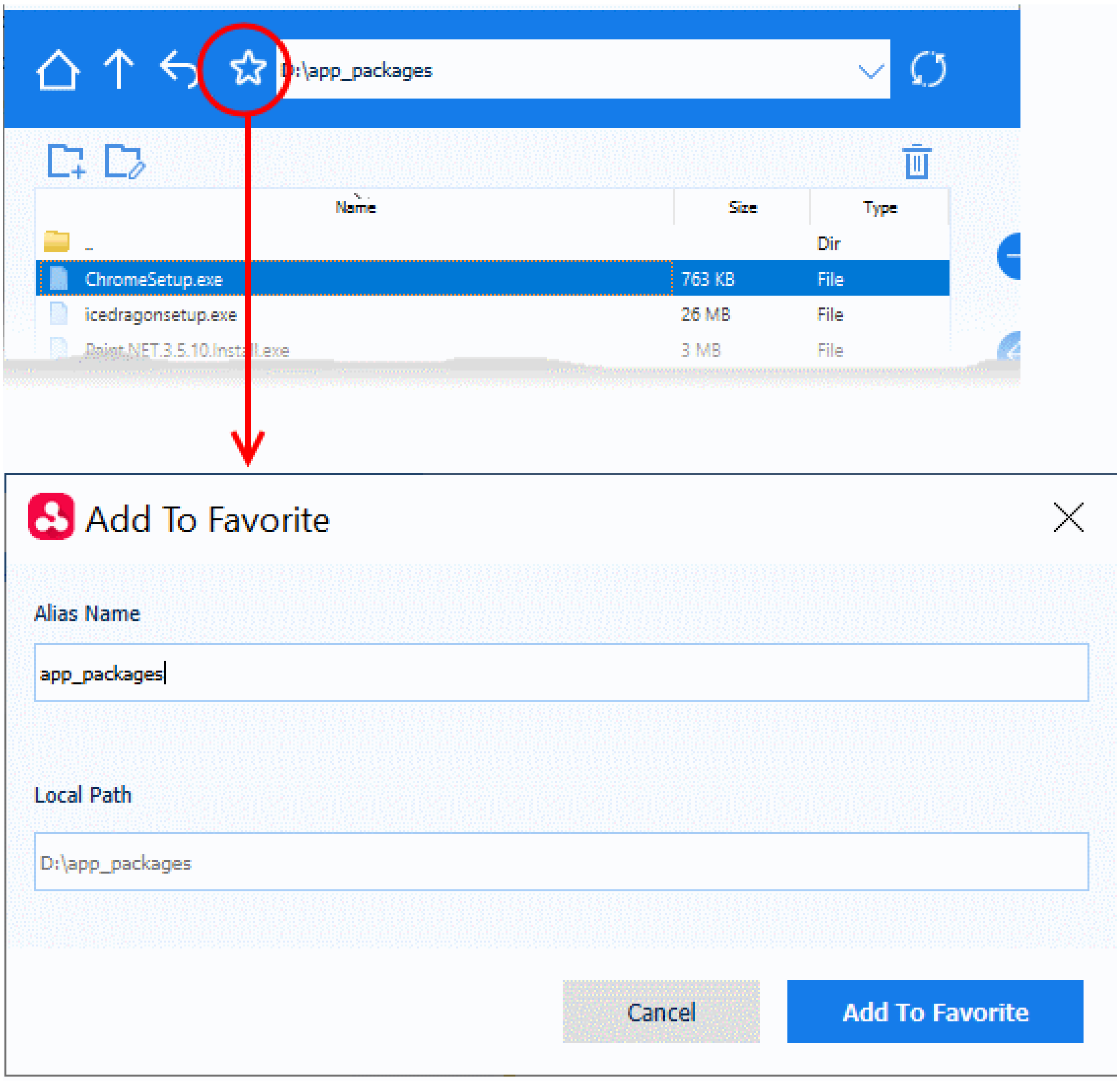
- The transfer will resume and show as completed when done.

## Add and manage favorites

- You can add folders you access often to your favorites for quick access
- Click the address bar to view your favorite folders.
- You can add up to five folders to favorites

### Add favorites

- Browse to the folder you want to favorite. The folder path is shown in the address bar.
- Click the start icon ☆ at the left of the address bar:



| Name | Size | Type |
|---|---|---|
| .. | | Dir |
| ChromeSetup.exe | 763 KB | File |
| icedragonsetup.exe | 26 MB | File |
| Paint.NET.3.5.10.Install.exe | 3 MB | File |

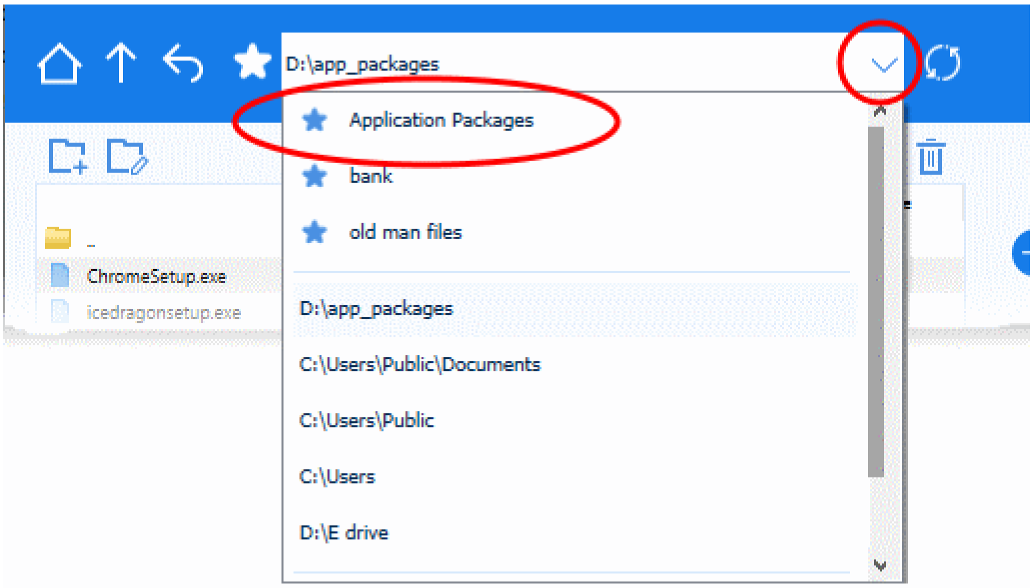
Add To Favorite

Alias Name: app_packages

Local Path: D:\app_packages

  - **Alias Name -** Enter a friendly name for the folder to easily identify it in the drop-down
  - **Local path -** Auto-populated with the path of the chosen folder
- Click 'Add to Favorite'

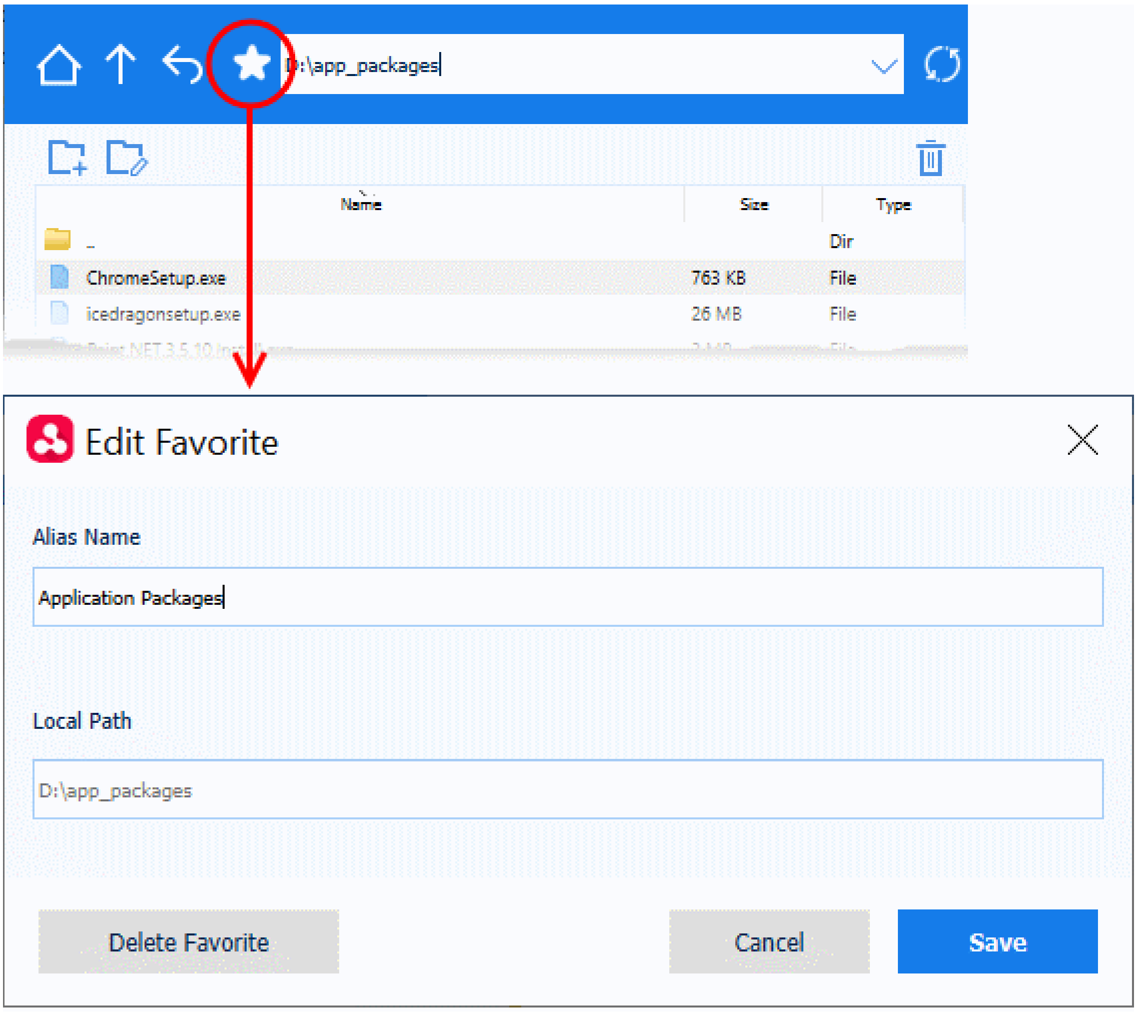
The folder will be added and available for quick access from the address bar drop-down:



- Repeat the process to add more favorites
- Note: You can add maximum of five folders to the favorites list.

**Edit a favorite**

- Open the favorite folder and click the star icon



Edit Favorite

Alias Name: Application Packages

Local Path: D:\app_packages

- Edit the name and path as required

- Click Save for your changes to take effect

**Remove a favorite**

- Open the favorite folder and click the star icon
- Click Delete Favorite in the 'Edit Favorite' dialog

## 5.2.9. Remotely Manage Folders and Files on Windows Devices

- Click 'Devices' > 'Device List'
- Select a running Windows device
- Click 'Remote Tools' > 'File Explorer'

The file explorer interface lets you remotely access files/folders on any managed Windows device.

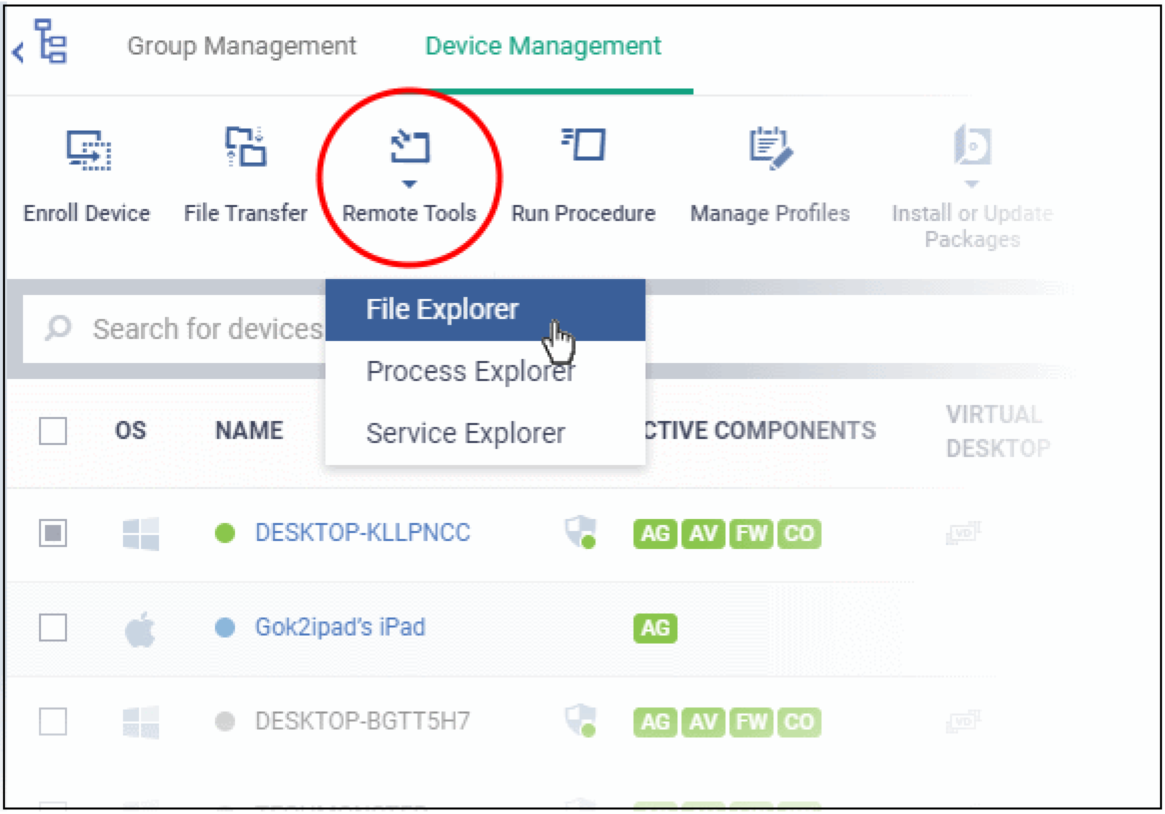
You can transfer files / folders back and forth between your machine and the remote device. You can also create / rename / delete items on the remote device.

- Note - You can also use the stand-alone remote control utility to manage files on Windows Devices. **Click here** find out more.

**View files on a managed Windows device**

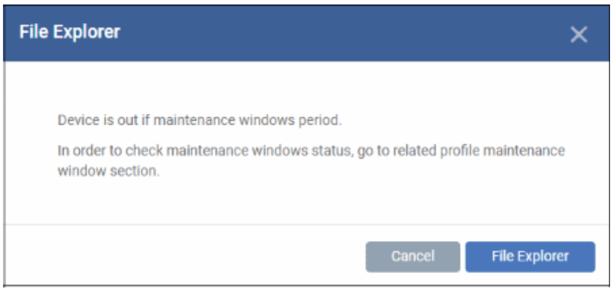
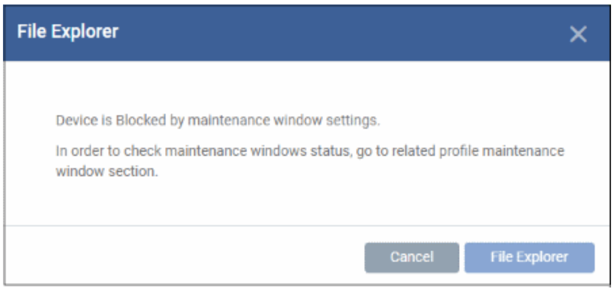
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to Endpoint Manager
- Select the Windows device you want to view
- Click 'Remote Tools' > 'File Explorer':

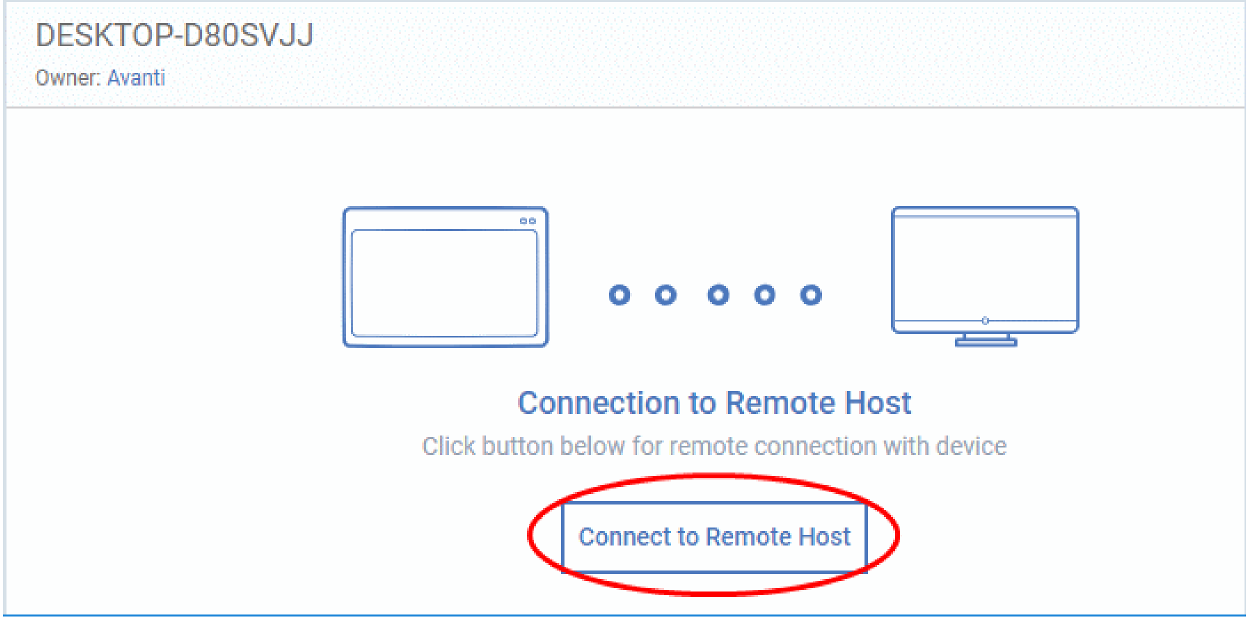


- Alternatively, click the name of the device to open 'Device Details' > select 'Remote Tools' > 'File Explorer' from the options at the top.

Note - you might see an alert if you try to use this feature outside of a maintenance window:

| Warning message | Blocked message |
|---|---|
| <br>File Explorer<br>Device is out if maintenance windows period.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br> <br>- Click 'File Explorer' to continue. | <br>File Explorer<br>Device is Blocked by maintenance window settings.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br> <br>- Click 'Cancel' to return to device management screen |

- Click 'Connect to Remote Host' in the confirmation screen to establish the connection:



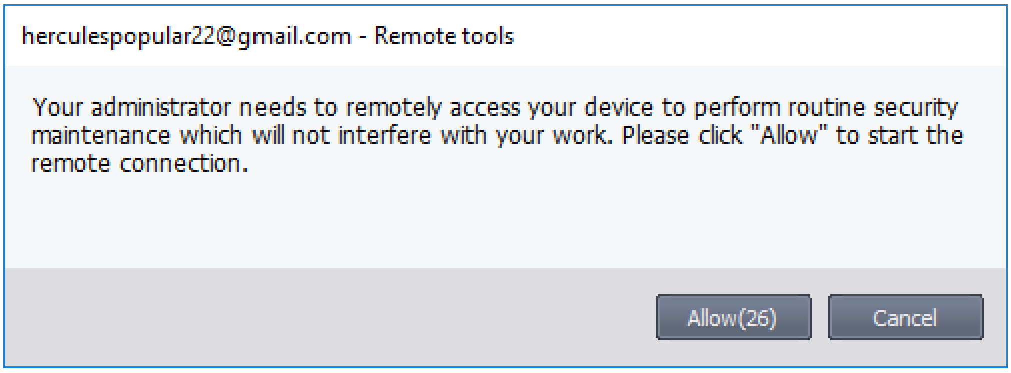
DESKTOP-D80SVJJ

Owner: Avanti

Connection to Remote Host

Click button below for remote connection with device

- Click 'Cancel Connection' to terminate immediately.
- A request message may be shown to the end-user if so configured:

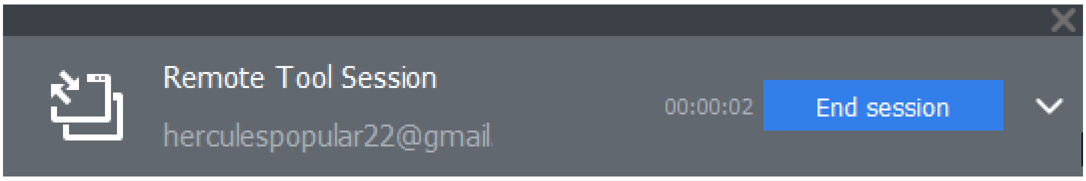


herculespopular22@gmail.com - Remote tools

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work. Please click "Allow" to start the remote connection.

- You can configure these request messages by adding a **Remote Tools Settings** section to a profile.
- Click 'Configuration Templates' > open the correct profile for the target endpoints > Click 'Add Profile Section' > Select 'Remote Tools'.
- You have the following choices:
    - **Silent control** - Take control without notifying the end-user
    - **Ask then allow** - Ask end-user permission but take control anyway if they don't respond within a set time
    - **Ask then deny access** - Ask end-user permission but close the connection if they don't respond within a set time.
    - **Do not allow** - Prohibit remote take-over of target devices associated with this profile.

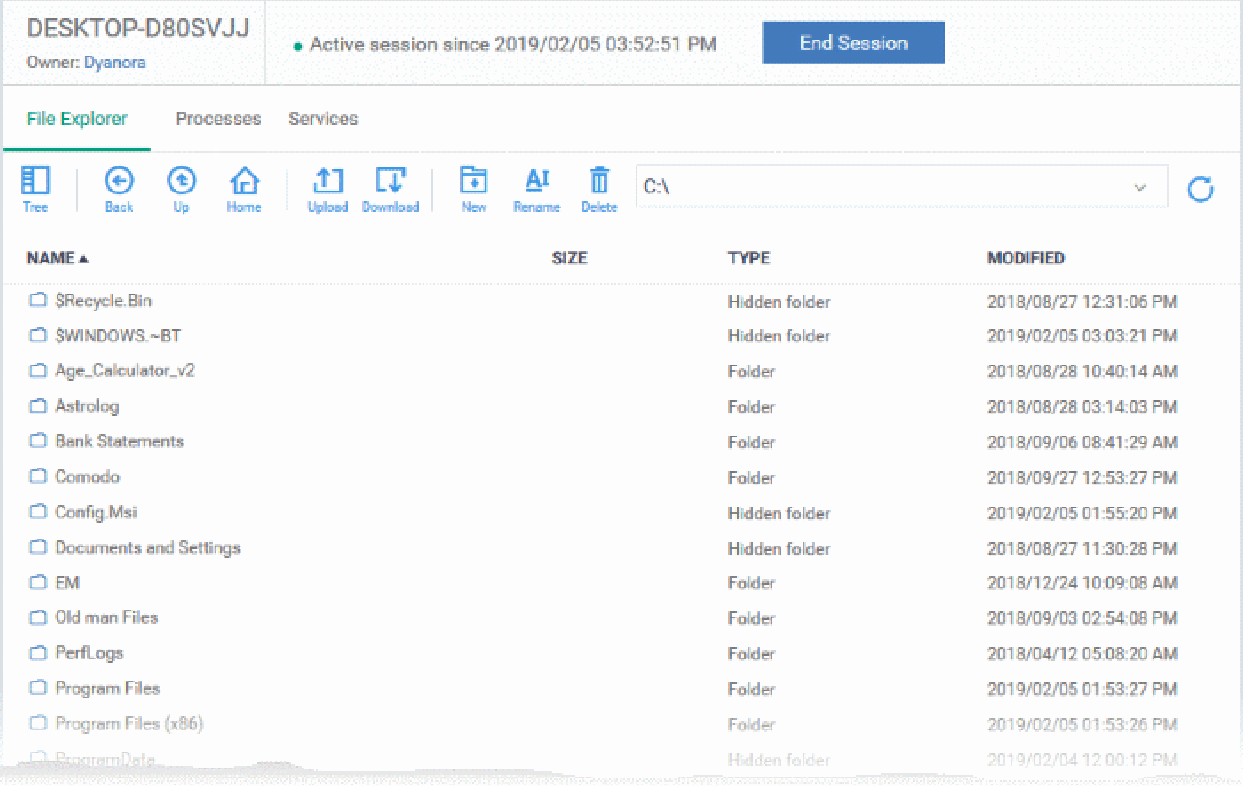
- The following notification is shown on the endpoint during a remote session:


Remote Tool Session

herculespopular22@gmail

00:00:02

- The file explorer interface will open after connecting to the device:


DESKTOP-D80SVJJ

Owner: Dyanora

● Active session since 2019/02/05 03:52:51 PM

| NAME ▲ | SIZE | TYPE | MODIFIED |
|---|---|---|---|
| $Recycle.Bin | | Hidden folder | 2018/08/27 12:31:06 PM |
| $WINDOWS.~BT | | Hidden folder | 2019/02/05 03:03:21 PM |
| Age_Calculator_v2 | | Folder | 2018/08/28 10:40:14 AM |
| Astrolog | | Folder | 2018/08/28 03:14:03 PM |
| Bank Statements | | Folder | 2018/09/06 08:41:29 AM |
| Comodo | | Folder | 2018/09/27 12:53:27 PM |
| Config.Msi | | Hidden folder | 2019/02/05 01:55:20 PM |
| Documents and Settings | | Hidden folder | 2018/08/27 11:30:28 PM |
| EM | | Folder | 2018/12/24 10:09:08 AM |
| Old man Files | | Folder | 2018/09/03 02:54:08 PM |
| PerfLogs | | Folder | 2018/04/12 05:08:20 AM |
| Program Files | | Folder | 2019/02/05 01:53:27 PM |
| Program Files (x86) | | Folder | 2019/02/05 01:53:26 PM |
| ProgramData | | Hidden folder | 2019/02/04 12:00:12 PM |

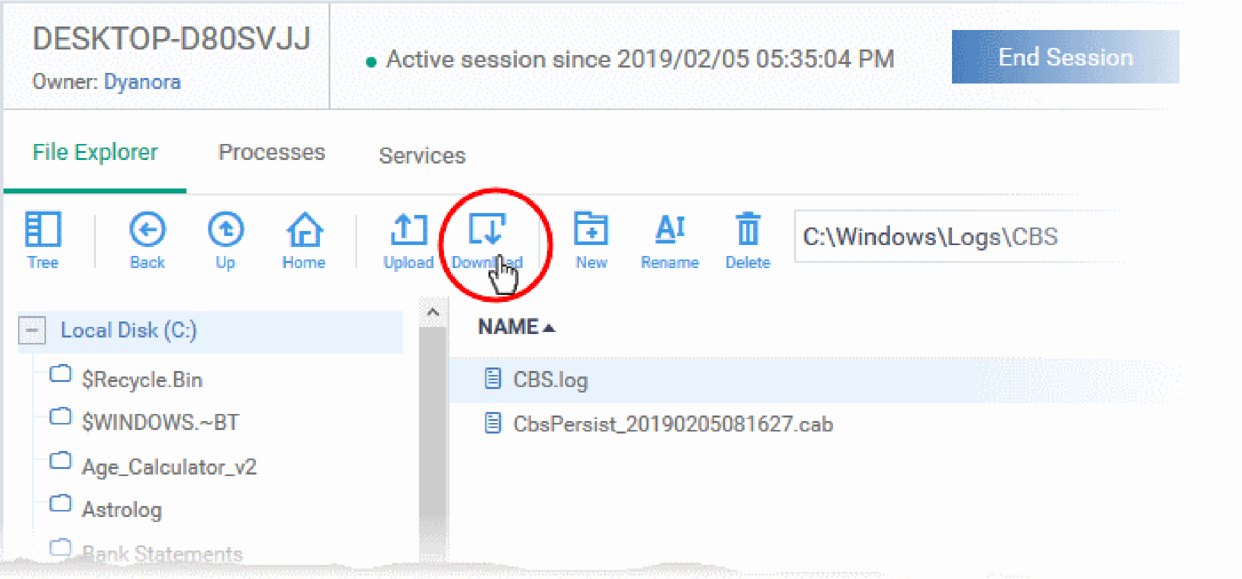
- Use the drop-down at upper-right to choose a drive/partition on the remote device.
- Folders and files, including hidden items, are shown in list view
    - Click the tree icon Tree at top-left to change to tree view.
- You can browse to any path by double-clicking on a folder

**Tip** - You can also enter a path in the field at the top of the interface.

- The controls at the top let you navigate the remote file system:
  - Tree - Switch between tree view and list view
  - Back - Return to the previous location
  - Up - Go one level up the folder tree
  - Home - Go to the root folder of the selected drive/partition
  - Upload - Transfer files / folders from your computer to the remote device.
    - See **Upload Files / Folders to Remote Device** for more details.
  - Download - Copy selected files/folders to your computer from the remote device.
    - See **Download Files / Folders from Remote Device to your Computer** for more details.
  - New - Create a new folder on the remote device.
    - See **Create New Folder on Remote Device** for more details
  - Rename - Set a new name for a file/folder on the remote device.
    - See **Rename File / Folder on Remote Device** for more details.
  - Delete - Remove unwanted items from the remote device.
    - See **Delete Folder / File from Remote Device** for more details
  - ↻ - Refresh the content of the current folder.

## Download Files / Folders from a Remote Device to your Computer

- Browse to the file / folder you want to download from the remote device
- Select the file / folder and click the download icon (right-click and select multiple files / folders):



DESKTOP-D80SVJJ
Owner: Dyanora

Active session since 2019/02/05 05:35:04 PM

C:\Windows\Logs\CBS

Local Disk (C:)
- $Recycle.Bin
- $WINDOWS.~BT
- Age_Calculator_v2
- Astrolog
- Bank Statements

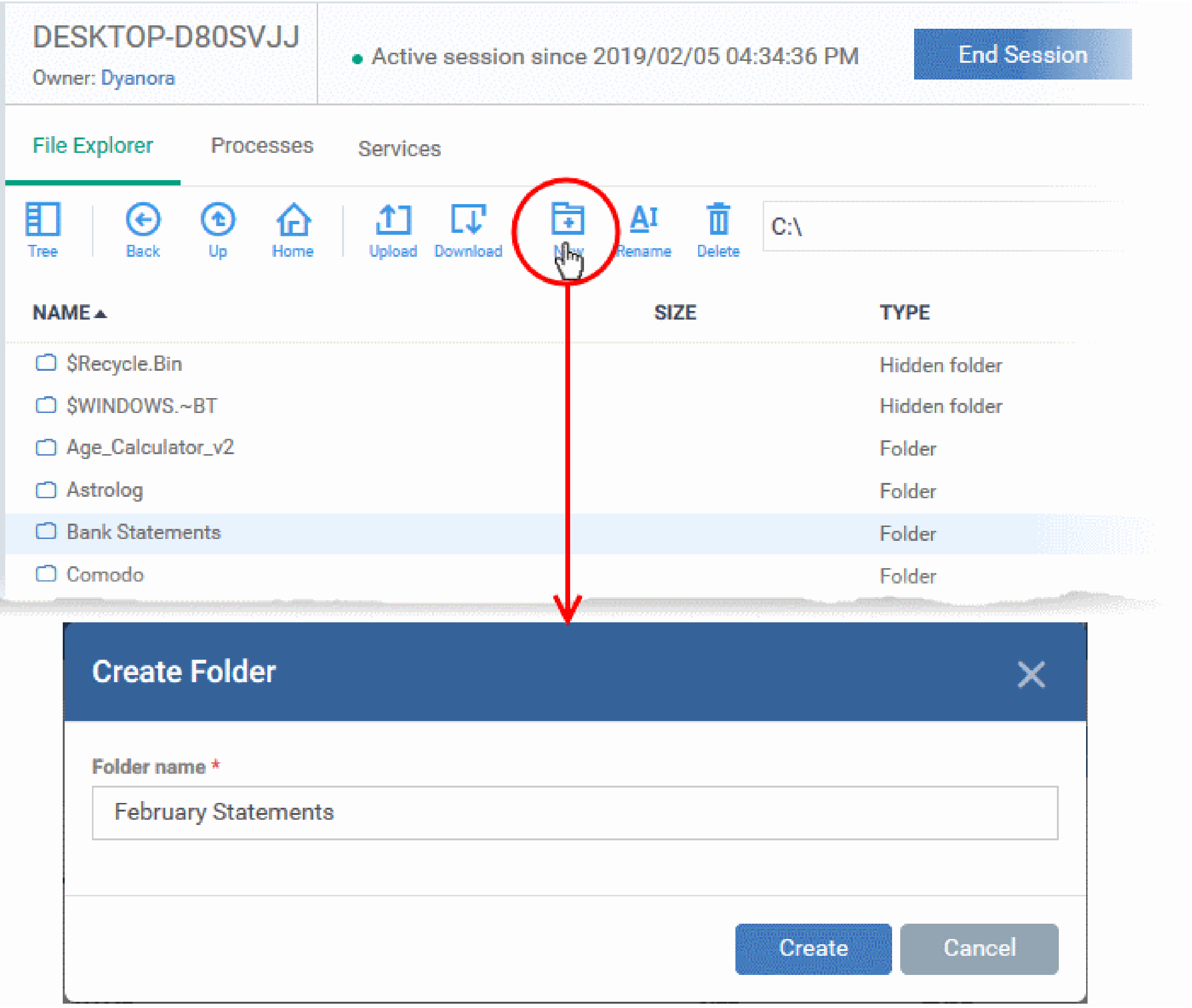
| NAME ▲ |
|---|
| CBS.log |
| CbsPersist_20190205081627.cab |

- The file will be copied to your computer.

Note: Only files of size up to 50 MB can be downloaded.

### Create a New Folder on Remote Device

- Browse to the location on the remote device where you want to create the new folder
- Click the 'New folder' icon:



| NAME | SIZE | TYPE |
|---|---|---|
| $Recycle.Bin | | Hidden folder |
| $WINDOWS.~BT | | Hidden folder |
| Age_Calculator_v2 | | Folder |
| Astrolog | | Folder |
| Bank Statements | | Folder |
| Comodo | | Folder |

Create Folder

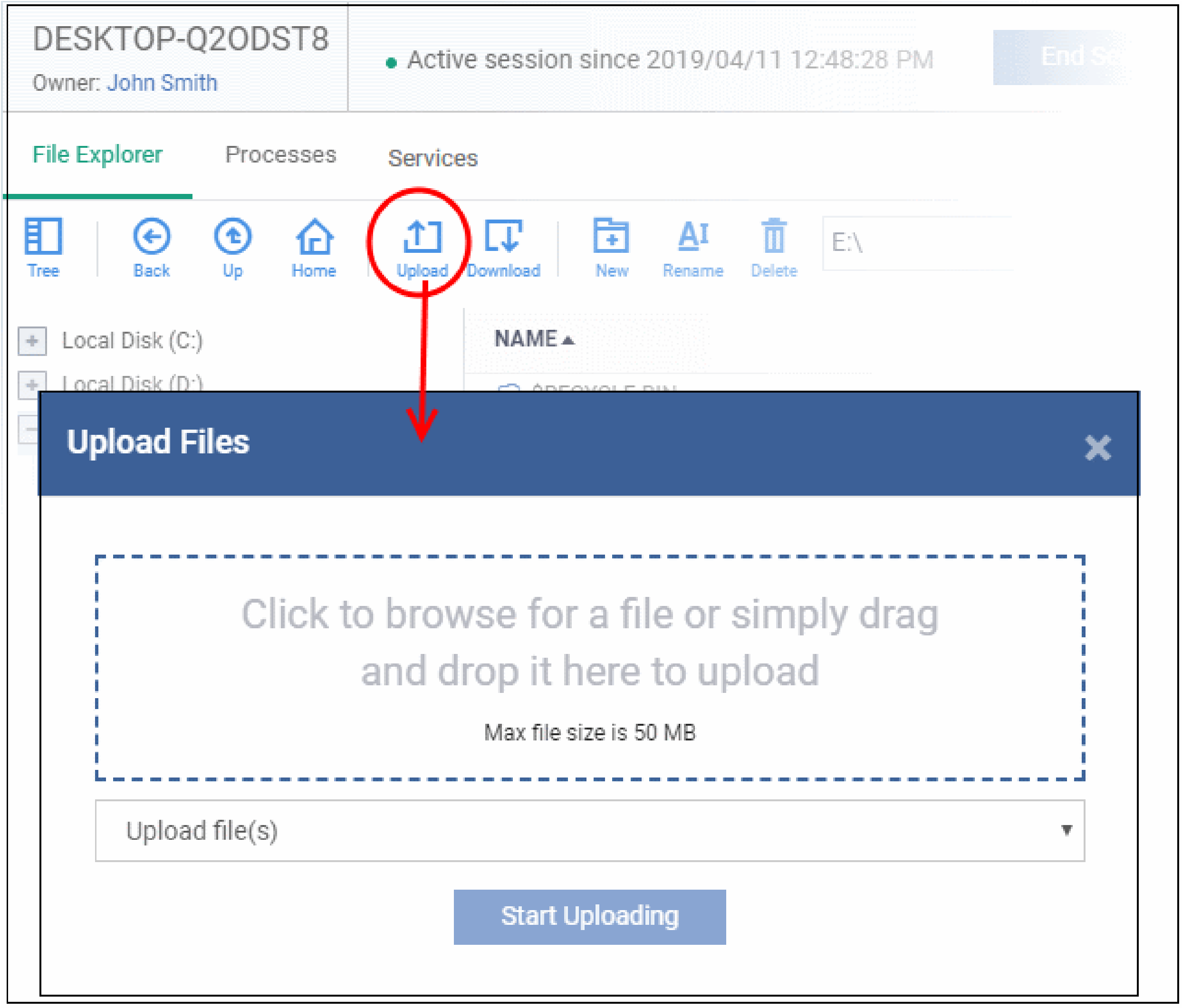
Folder name * February Statements

- Enter a name for the folder and click 'Create'.

The folder will be added at the location you chose. You can upload files from your computer to the new folder. The user can also save files in the new folder.

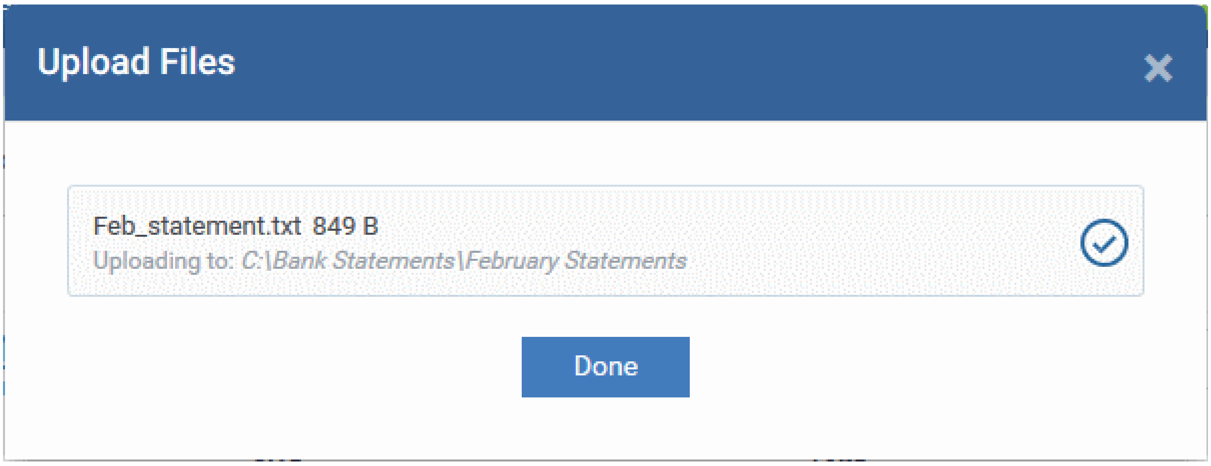
## Upload Files / Folders to a Remote Device

- Click the 'Upload' icon in the control bar:



- Select 'Upload file(s)' or 'Upload folder(s)' from the drop-down

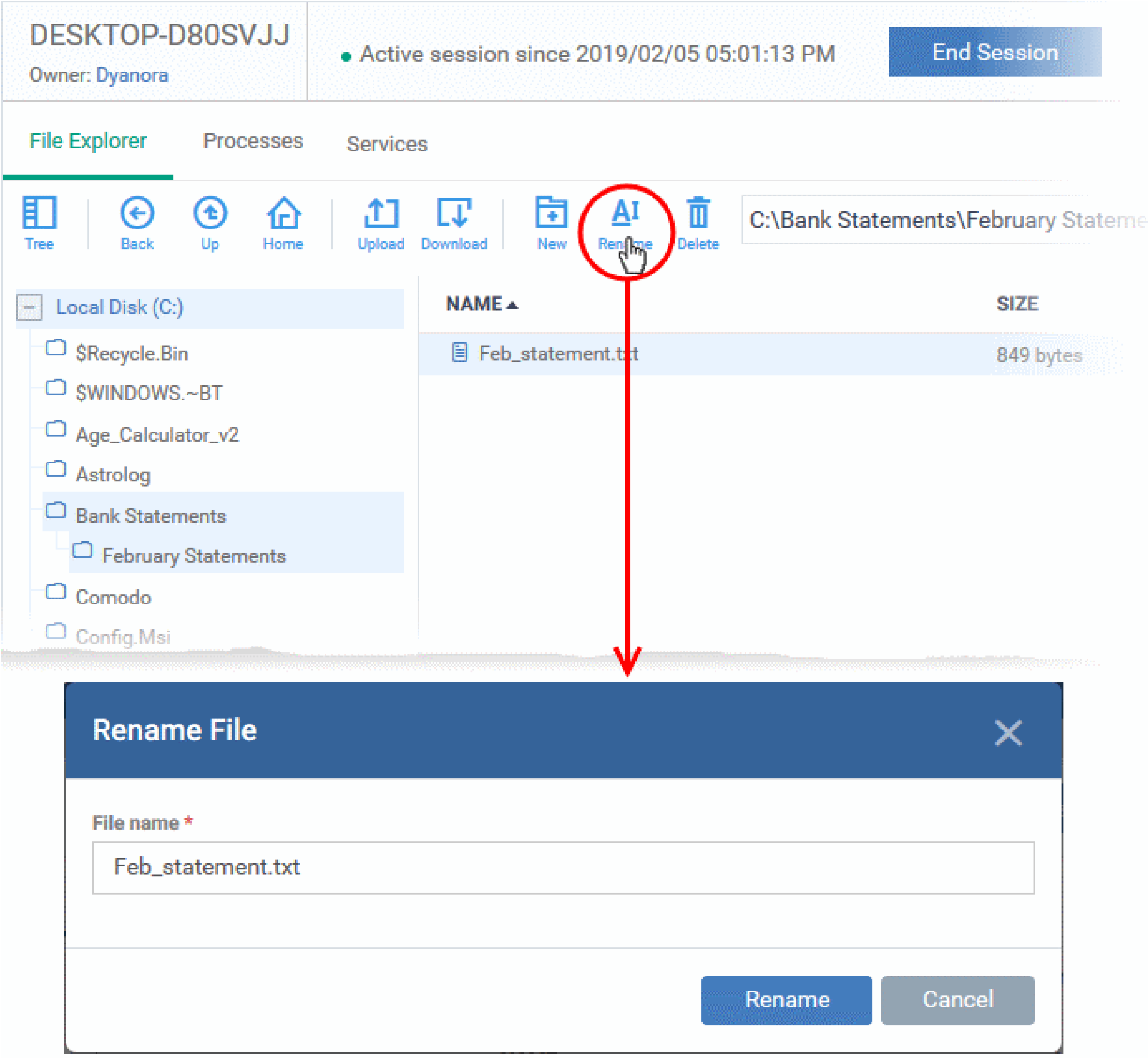
- Drag-and-drop files / folders into the box, or click inside the box to navigate to an item
- Click 'Start Uploading'



**Note**: The max. file / folder size you can upload is 50 MB

### Rename Files and Folders on the Remote Device

- Navigate to and select the item you want to rename
- Click the 'Rename' icon in the control bar:



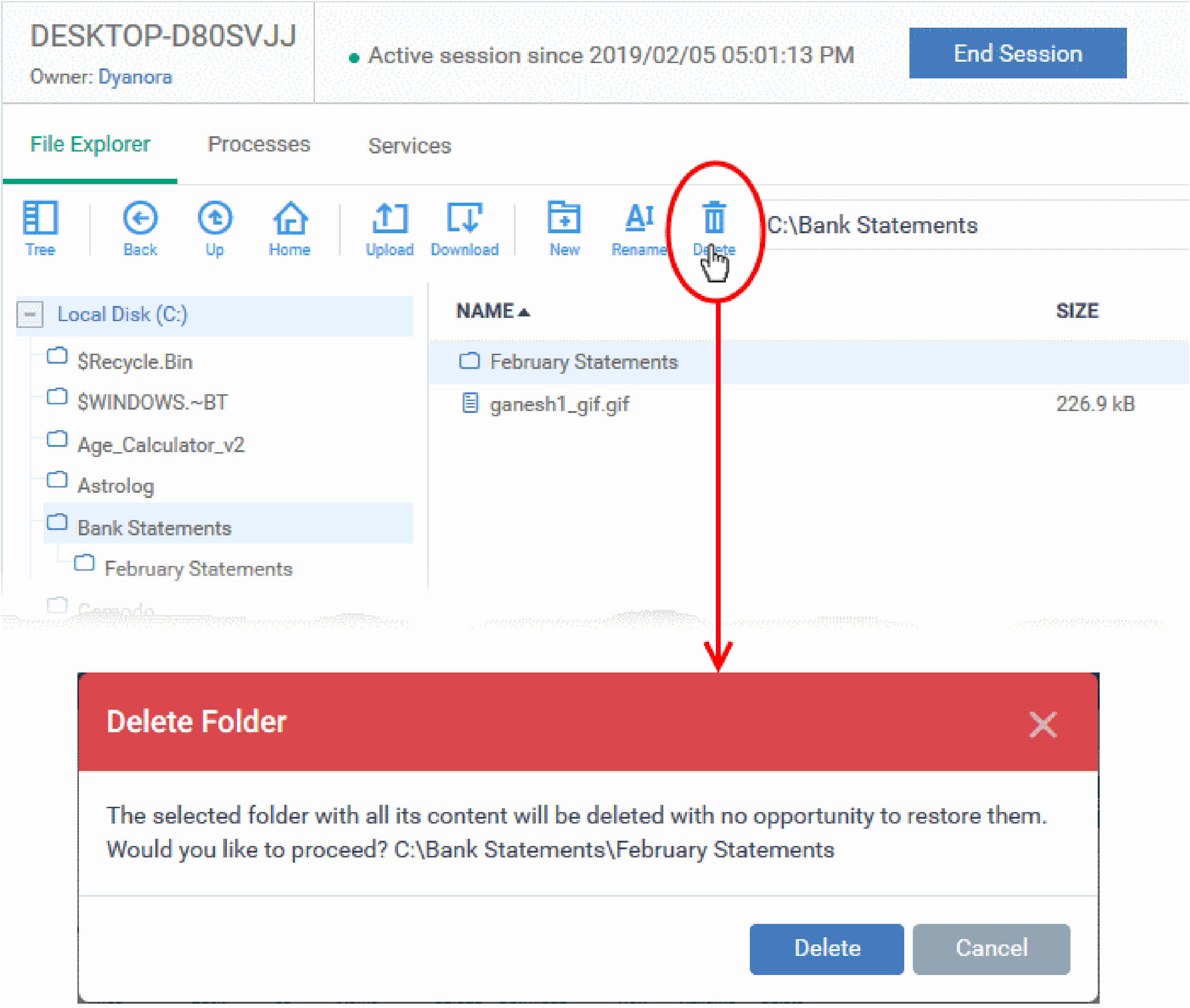
File name *

Feb_statement.txt

- Enter a new name for the item
- Click 'Rename'

## Delete Folder / File from Remote Device

- Navigate to and select the item you want to remove
- Click the 'Delete' icon in the control bar:



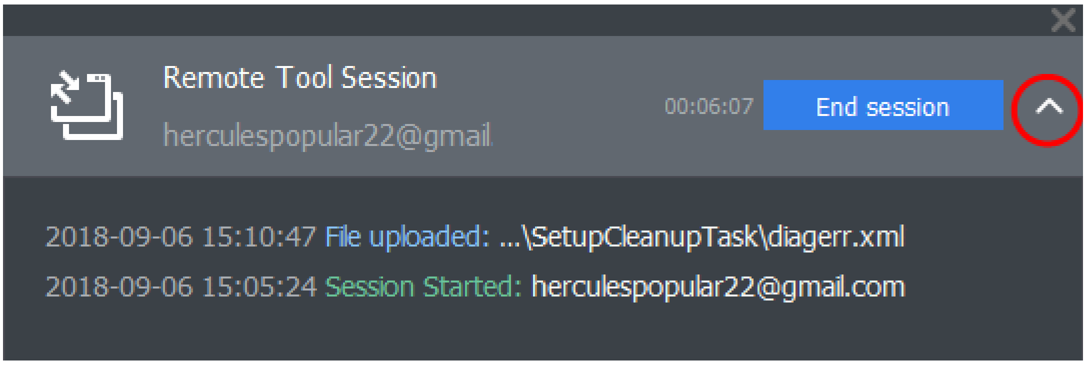
The selected folder with all its content will be deleted with no opportunity to restore them. Would you like to proceed? C:\Bank Statements\February Statements

- Click 'Delete' in the confirmation dialog

**Note**: Items deleted cannot be restored on the remote device.

## Notification

The device user can view your file activities by clicking the down arrow in the notification:



```
2018-09-06 15:10:47 File uploaded: ...\SetupCleanupTask\diagerr.xml
2018-09-06 15:05:24 Session Started: herculespopular22@gmail.com
```

- Click the 'End Session' to close the remote connection.

Endpoint Manager logs your remote browsing sessions in 'Dashboard' > 'Audit Logs'. See **Audit Logs** in **The Dashboard** for more details.

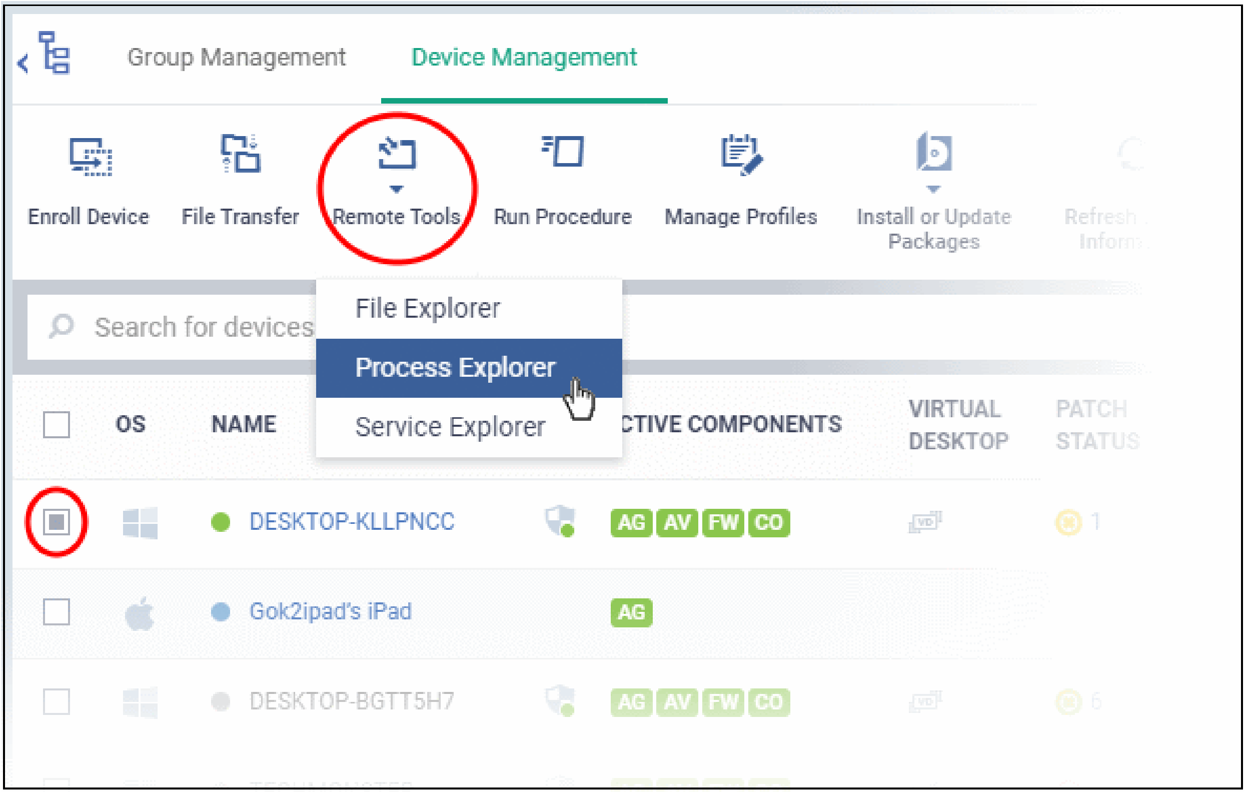
### 5.2.10. Remotely View and Manage Processes Running on Windows Devices

- The 'Processes' interface lets you remotely view running processes on any managed Windows device.
- You can also terminate any unwanted processes.

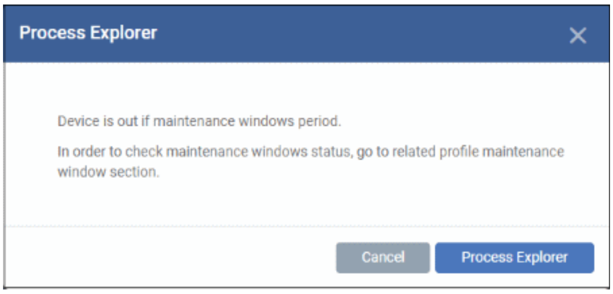
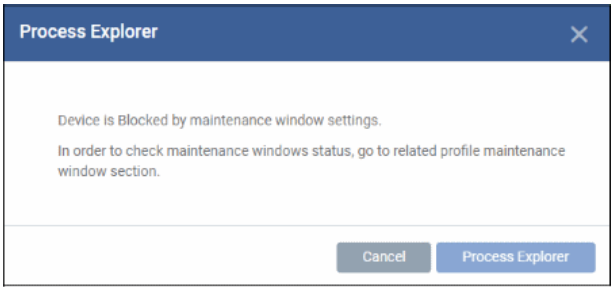
**View running processes on a Windows device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

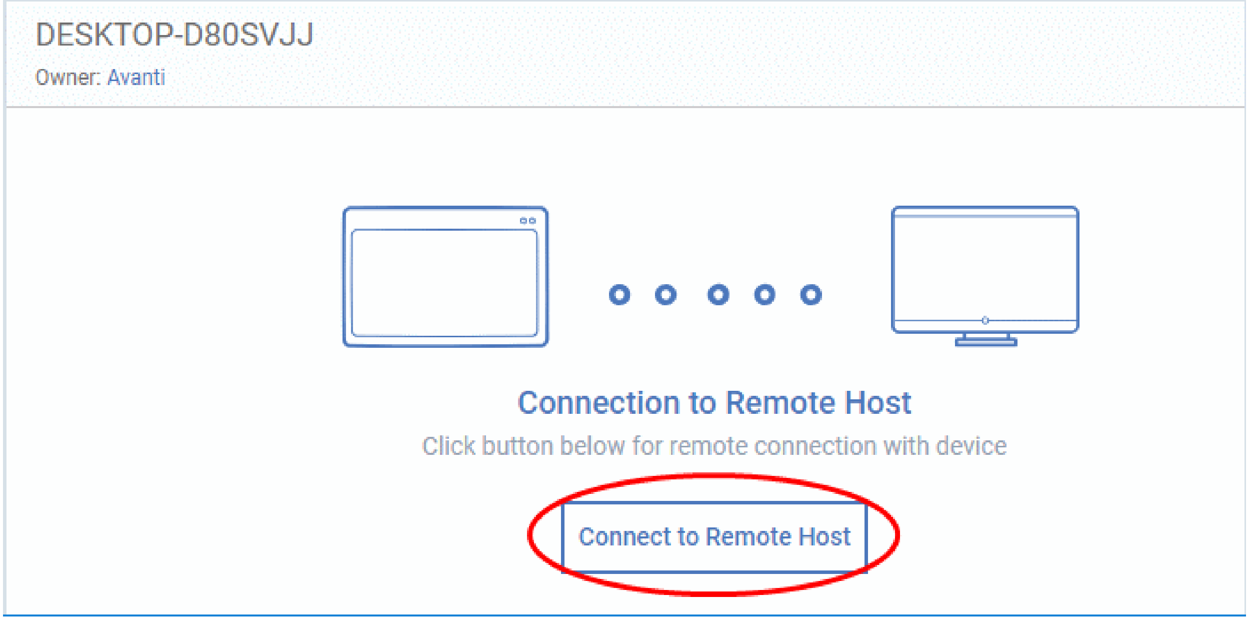
      Or
    - Select 'Show all' to view every device enrolled to EM
- Select the target Windows device
- Click 'Remote Tools' > 'Process Explorer':



You might see an alert if you try to access this feature outside of a maintenance window:

| Warning message | Blocked message |
|---|---|
| <br>Process Explorer<br>Device is out if maintenance windows period.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br> | <br>Process Explorer<br>Device is Blocked by maintenance window settings.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br> |
| • Click 'Process Explorer' to continue. | • Click 'Cancel' to return to device management screen |

- Click 'Connect to Remote Host' to establish the connection:



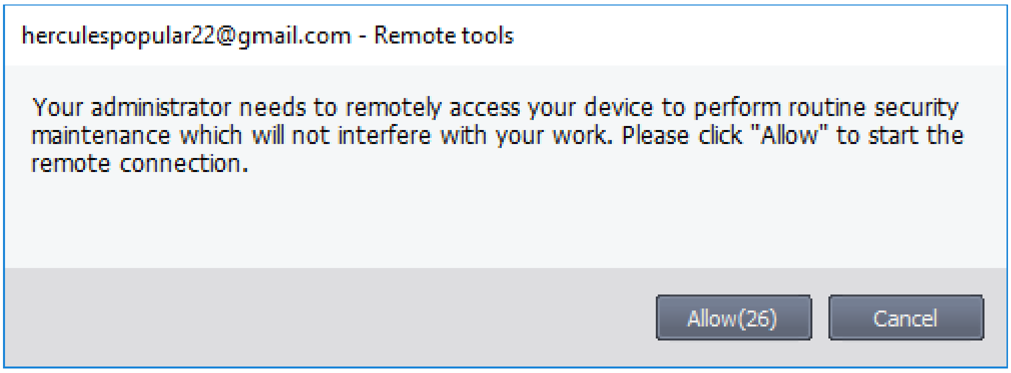
DESKTOP-D80SVJJ

Owner: Avanti

Connection to Remote Host

Click button below for remote connection with device

- Click 'Cancel Connection' to terminate immediately.
- A request message is shown to end-user if configured appropriately:



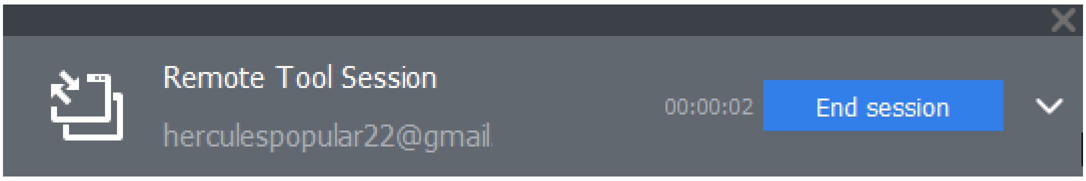
herculespopular22@gmail.com - Remote tools

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work. Please click "Allow" to start the remote connection.

- You have the following configuration options:
  - **Silent control** - Take control without notifying the end-user

- **Ask then allow** - Ask end-user permission but take control anyway if they don't respond within a set time
- **Ask then deny access** - Ask end-user permission but close the connection if they don't respond within a set time
- **Do not allow** - Prohibit remote take-over of target devices associated with this profile.
- See **Remote Tools Settings** for more details.

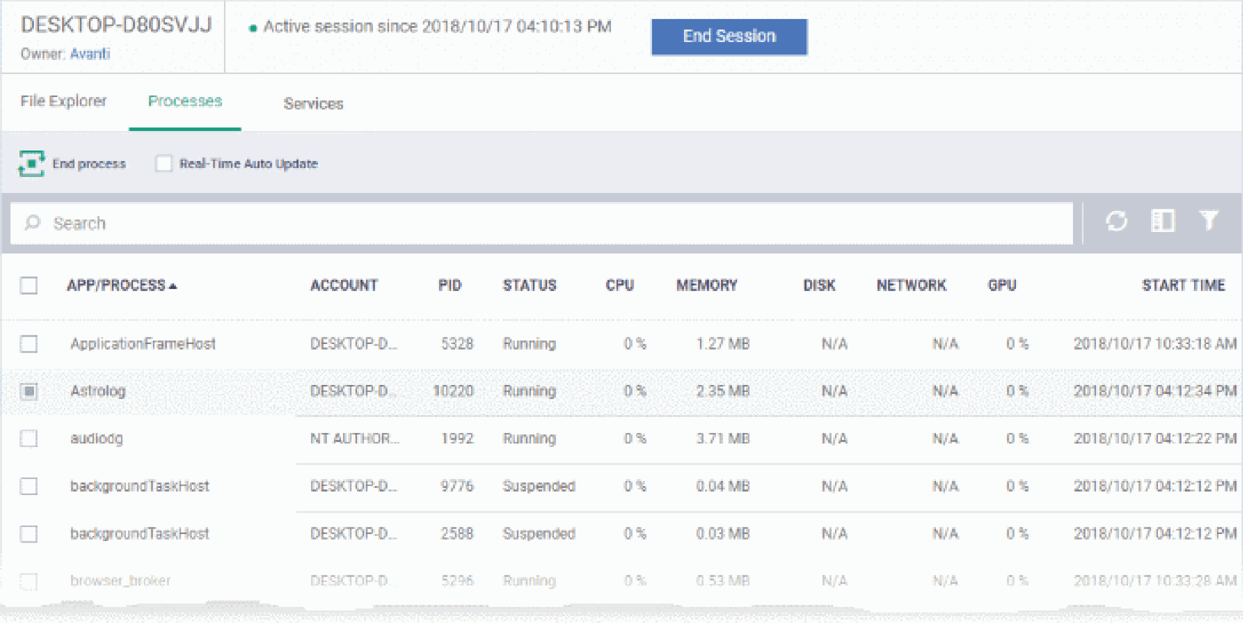
- The user is shown a notification during remote connections:



Remote Tool Session
herculespopular22@gmail
00:00:02

Users can click 'End session' to terminate the connection.

The 'Processes' interface for the selected device appears:



DESKTOP-D80SVJJ
Owner: Avanti
Active session since 2018/10/17 04:10:13 PM

| | APP/PROCESS | ACCOUNT | PID | STATUS | CPU | MEMORY | DISK | NETWORK | GPU | START TIME |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | ApplicationFrameHost | DESKTOP-D... | 5328 | Running | 0 % | 1.27 MB | N/A | N/A | 0 % | 2018/10/17 10:33:18 AM |
| ☑ | Astrolog | DESKTOP-D... | 10220 | Running | 0 % | 2.35 MB | N/A | N/A | 0 % | 2018/10/17 04:12:34 PM |
| □ | audiodg | NT AUTHOR... | 1992 | Running | 0 % | 3.71 MB | N/A | N/A | 0 % | 2018/10/17 04:12:22 PM |
| □ | backgroundTaskHost | DESKTOP-D... | 9776 | Suspended | 0 % | 0.04 MB | N/A | N/A | 0 % | 2018/10/17 04:12:12 PM |
| □ | backgroundTaskHost | DESKTOP-D... | 2588 | Suspended | 0 % | 0.03 MB | N/A | N/A | 0 % | 2018/10/17 04:12:12 PM |
| □ | browser_broker | DESKTOP-D... | 5296 | Running | 0 % | 0.53 MB | N/A | N/A | 0 % | 2018/10/17 10:33:28 AM |

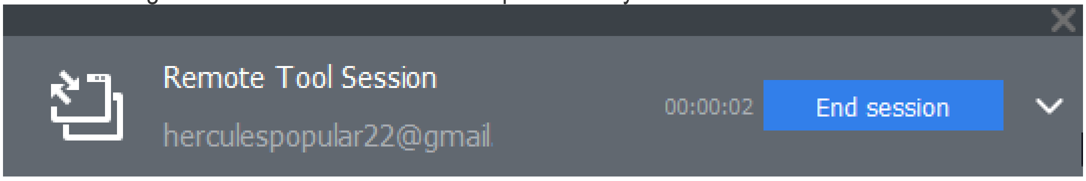
All processes that are currently running on the device are shown in the EM interface.

- Use the button ◧ at top-right to toggle between flat list and tree list views
- Click the funnel icon to filter processes by various criteria
- Click the right arrow beside a process name to view its child-processes.
- Terminate running processes by selecting them then clicking the 'End Process' button
- 'Real Time Auto-Update' - gets the latest information about a process from an endpoint every few seconds
- Start typing the process name in the search field. Matching results will be shown for the letters entered.

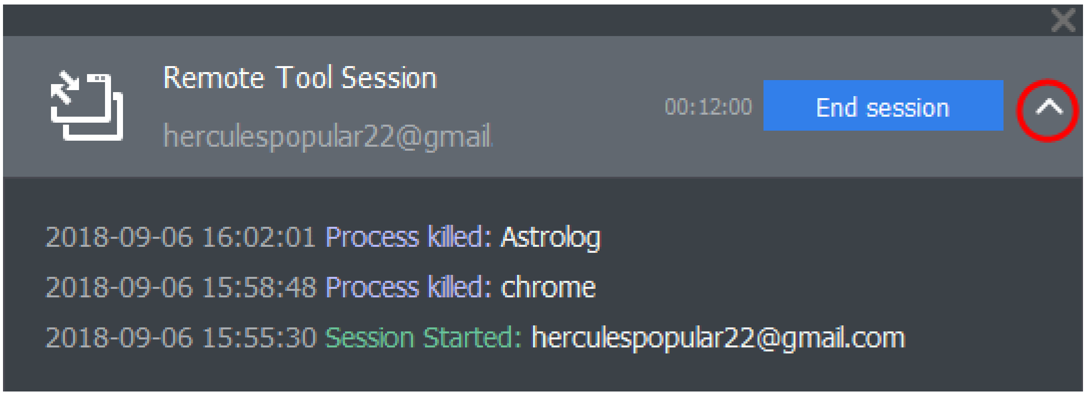
| Processes - Column Descriptions | |
|---|---|
| **Column Header** | **Descriptions** |
| App/Process | The label of the process or the parent application that triggered the process. |
| Account | The user account with which the process the running. The system access |

| | |
|---|---|
| | privileges for the process are limited by the user account. |
| PID | The process identification number. |
| Status | Whether the process is running or suspended. |
| CPU<br>Memory<br>Disk<br>Network<br>GPU | Indicates the resource usage of the respective hardware/connection bandwidth by the process. |
| Start time | The date and time the process commenced. |

- The following notification is shown on the endpoint while you are connected:



- The endpoint user can view your activities by clicking the arrow on the left:



```
2018-09-06 16:02:01 Process killed: Astrolog
2018-09-06 15:58:48 Process killed: chrome
2018-09-06 15:55:30 Session Started: herculespopular22@gmail.com
```

### 5.2.11. Remotely View and Manage Services Running on Windows Devices

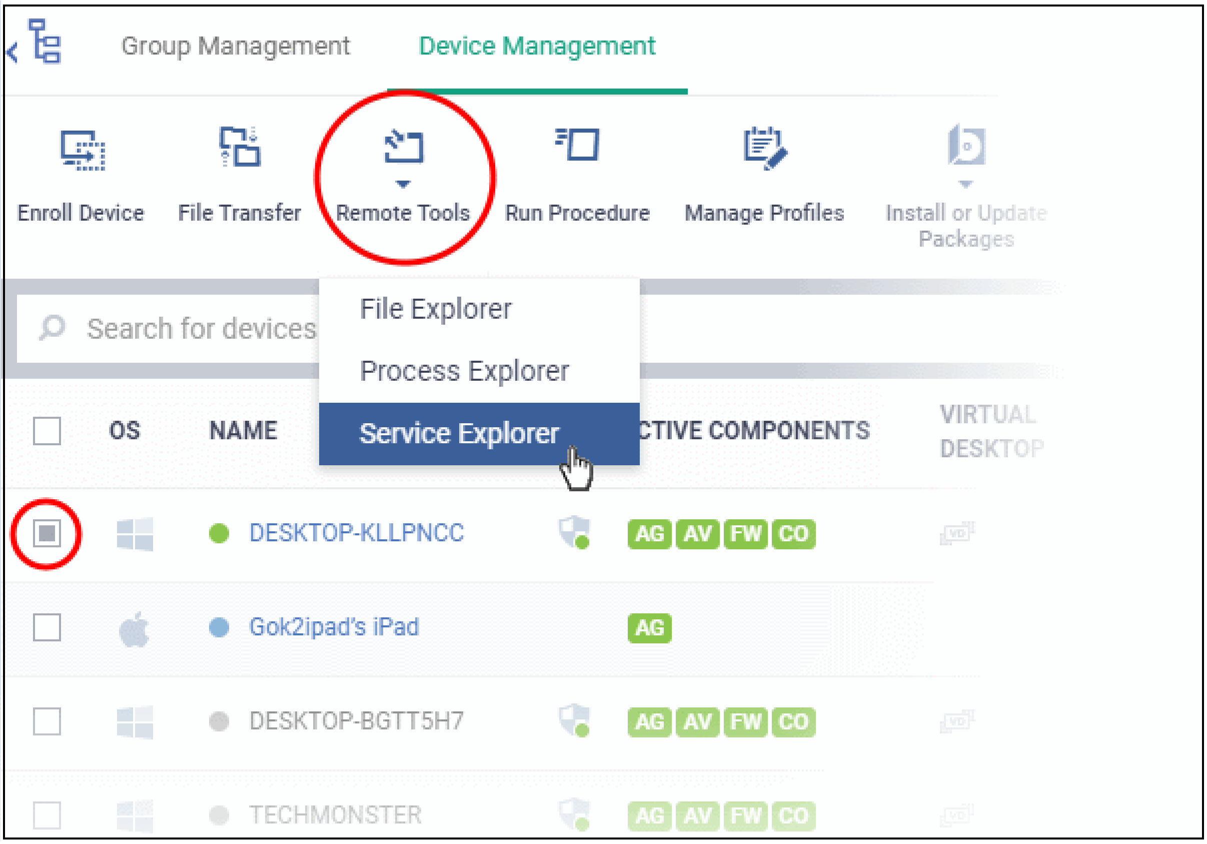
- The services area lets you remotely view all running services on a managed Windows device.
- You can also terminate any unwanted services.

**View running services on a Windows device**

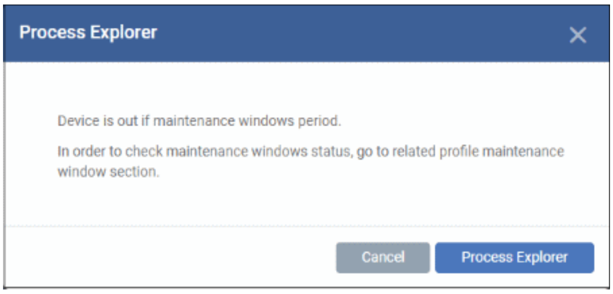
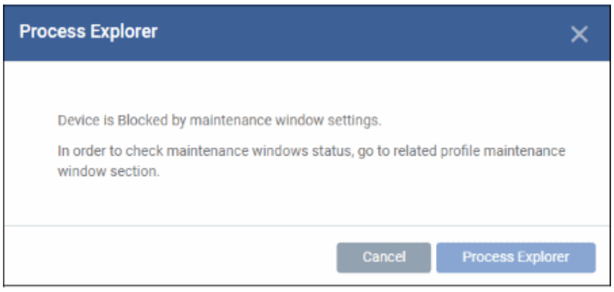
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM

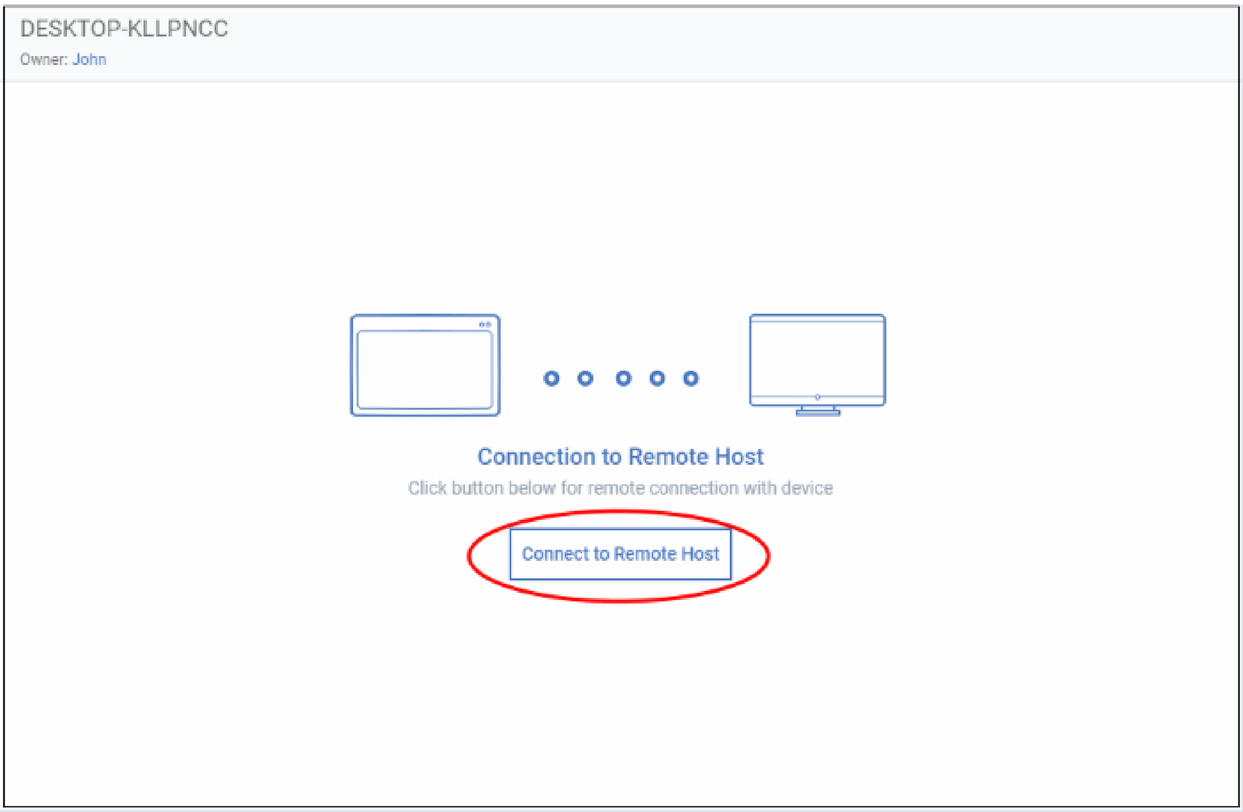
- Select the target Windows device
- Click 'Remote Tools' > 'Service Explorer':



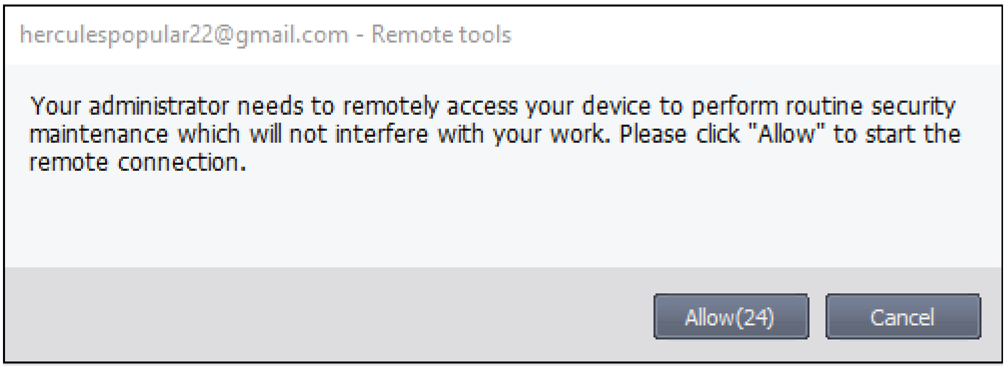
You might see an alert if you try to access this feature outside of a **maintenance window**:

| Warning message | Blocked message |
|---|---|
| <br>Process Explorer<br>Device is out if maintenance windows period.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br>Cancel Process Explorer | <br>Process Explorer<br>Device is Blocked by maintenance window settings.<br>In order to check maintenance windows status, go to related profile maintenance window section.<br>Cancel Process Explorer |
| • Click 'Service Explorer' to continue anyway. | • Click 'Cancel' to return to device management screen |

- Click 'Connect to Remote Host' to establish the connection:


DESKTOP-KLLPNCC
Owner: John
Connection to Remote Host
Click button below for remote connection with device
Connect to Remote Host

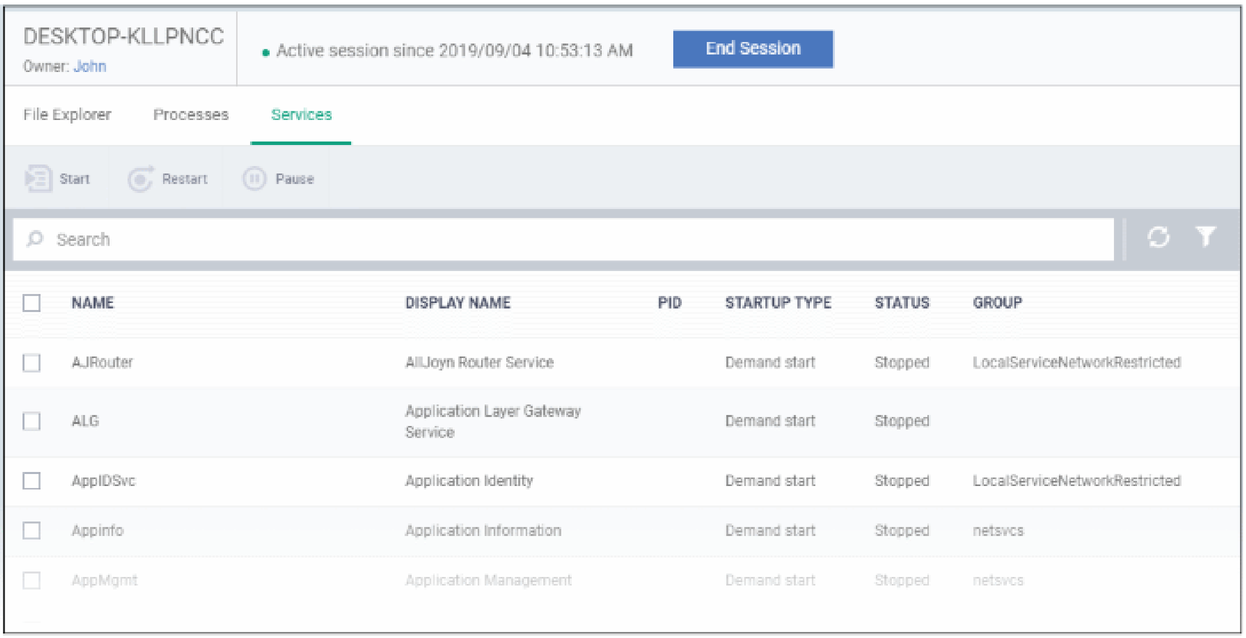
- A request message is shown to the end-user if notifications are enabled:



Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work. Please click "Allow" to start the remote connection.

- Note. You can configure these notices in **remote tool settings**. You have the following options:
  - **Silent control** - Take control without notifying the user
  - **Ask then allow** - Ask user permission, but take control anyway if they don't respond within a set time
  - **Ask then deny access** - Ask end-user permission, and close the connection if they don't respond within a set time
  - **Do not allow** - Prohibit remote take-over of devices that use this profile.

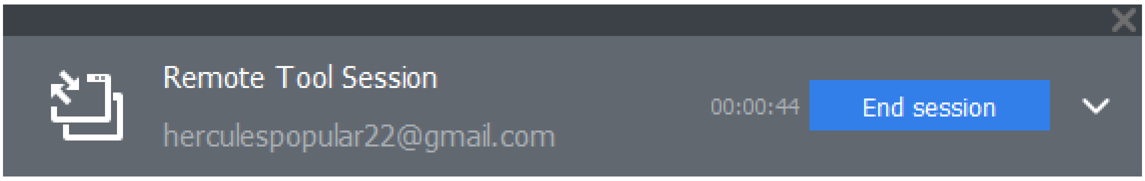
Once the connection has been established, Endpoint Manager shows all running services on the remote device:



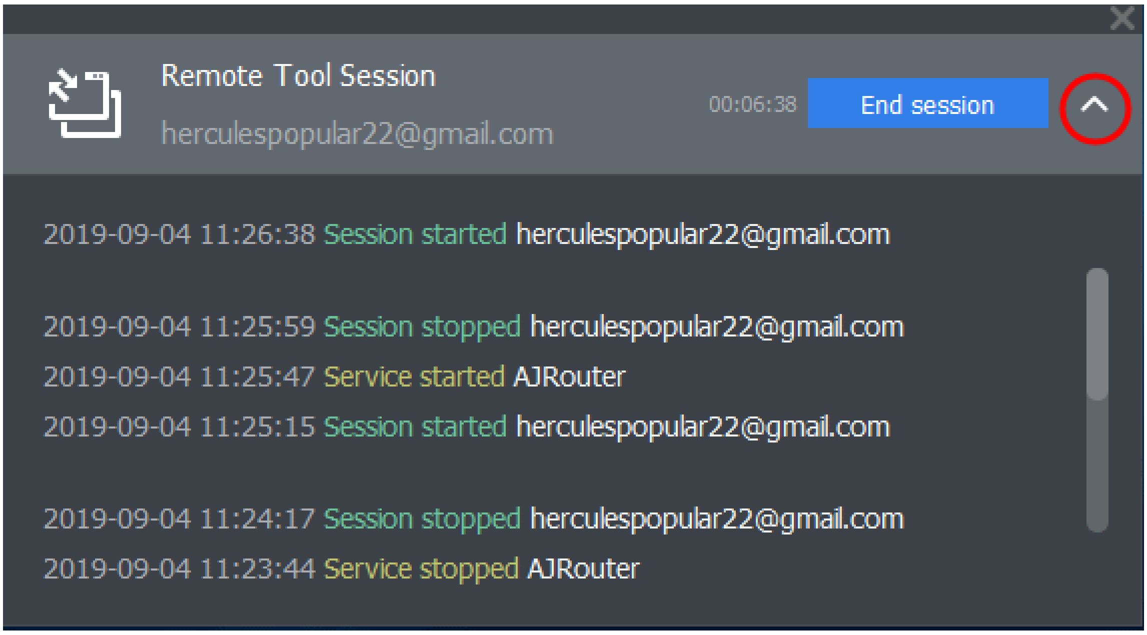
| □ | NAME | DISPLAY NAME | PID | STARTUP TYPE | STATUS | GROUP |
|---|---|---|---|---|---|---|
| □ | AJRouter | AllJoyn Router Service | | Demand start | Stopped | LocalServiceNetworkRestricted |
| □ | ALG | Application Layer Gateway Service | | Demand start | Stopped | |
| □ | AppIDSvc | Application Identity | | Demand start | Stopped | LocalServiceNetworkRestricted |
| □ | Appinfo | Application Information | | Demand start | Stopped | netsvcs |
| □ | AppMgmt | Application Management | | Demand start | Stopped | netsvcs |

- Use the buttons above the table to start, pause and restart selected services
- Click the funnel icon to filter services by various criteria
- Search for a service by typing its name in the search field. Matching results are shown for the letters entered.

- The following notification is shown on the endpoint while you are connected:



- The users can view your activities by clicking the arrow on the left:



```
2019-09-04 11:26:38 Session started herculespopular22@gmail.com

2019-09-04 11:25:59 Session stopped herculespopular22@gmail.com
2019-09-04 11:25:47 Service started AJRouter
2019-09-04 11:25:15 Session started herculespopular22@gmail.com

2019-09-04 11:24:17 Session stopped herculespopular22@gmail.com
2019-09-04 11:23:44 Service stopped AJRouter
```

## 5.2.12. Apply Procedures to Windows Devices

- Procedures are instruction sets designed to accomplish a specific task on target devices. There are two types - script procedures and patch procedures.
- Procedures can be run on single or multiple devices from the 'Devices' > 'Device List' screen.
    - You can also run them on an ad-hoc basis in 'Configuration Templates' > 'Procedures', or by adding them to a profile.
    - See **Directly Apply Procedures to Devices** and **Procedure Settings** for details about these methods.

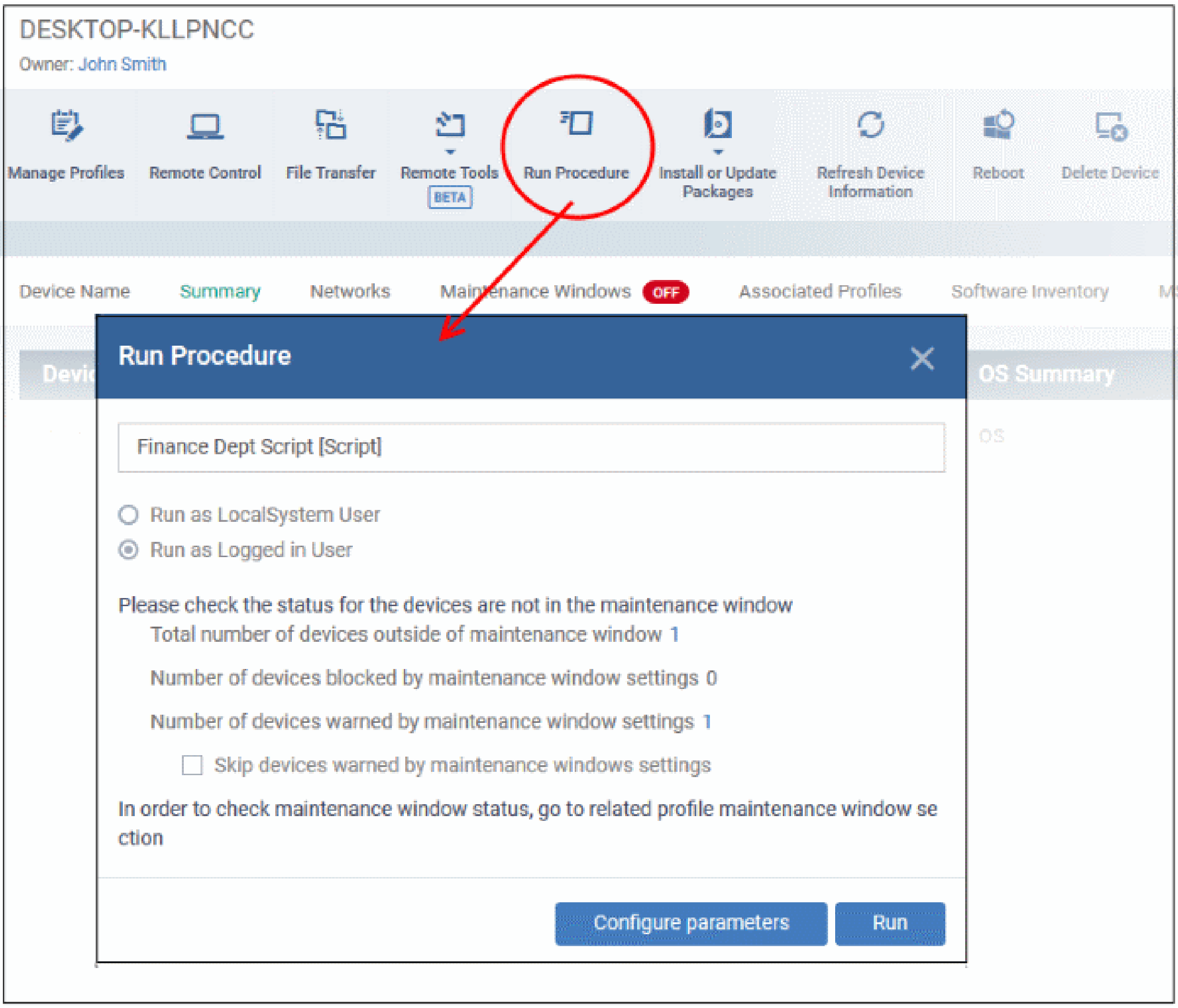
This section explains how to run procedures from the 'Device Management' interface.

- **Apply procedures on a single device**
- **Apply procedures on multiple devices at once**

**Run a procedure on a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Select your target Windows devices then click the 'Run Procedure' button



Run Procedure

Finance Dept Script [Script]

○ Run as LocalSystem User
● Run as Logged in User

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 1

Number of devices blocked by maintenance window settings 0

Number of devices warned by maintenance window settings 1

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window se ction

Configure parameters | Run

- Type the first few characters of procedure name in the search field.
  - If you don't know the name of the script, try experimenting with a single keyword to narrow the list. For example, 'Install', 'Remove', 'Activate', 'Windows', 'Backup', 'Logs', 'Client', 'Firewall' etc.
- Select the procedure you want to run from the recommendations. Only approved procedures are listed.
- Only one procedure can run at a time.

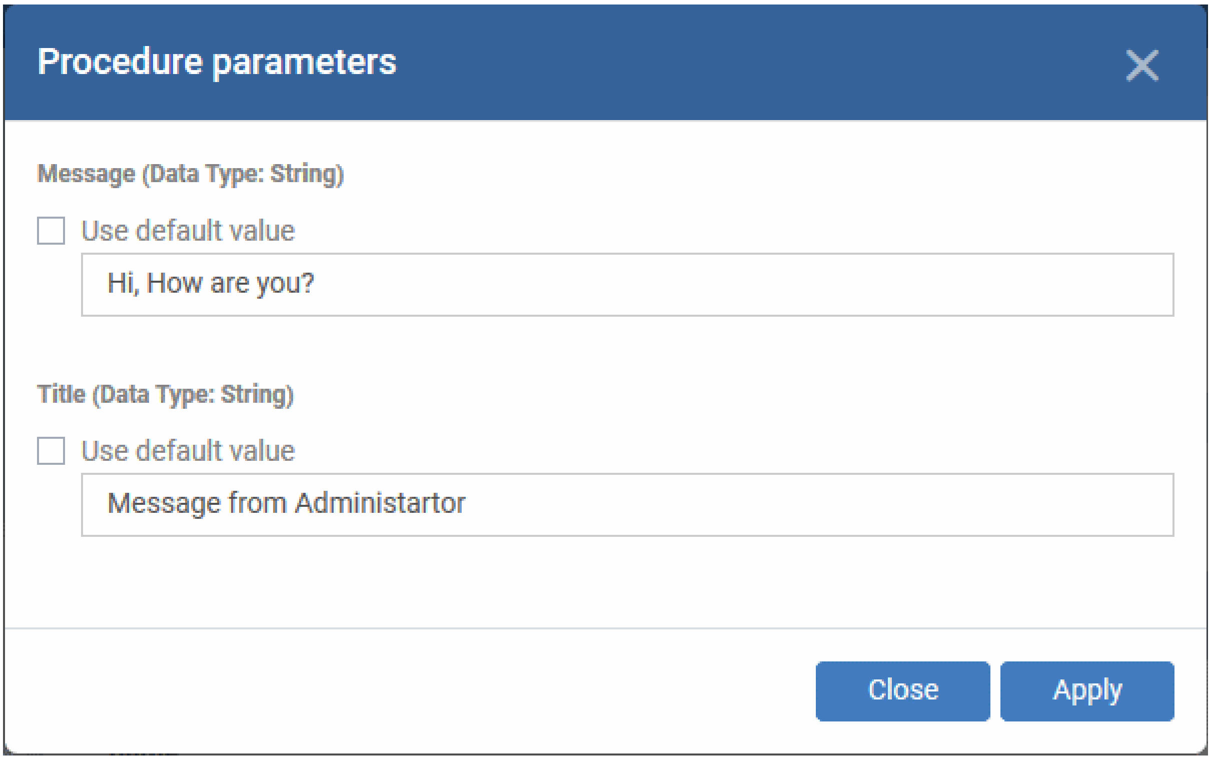
  - **Run as Local System User** / **Run as Logged in user** - Choose the user account with which the procedure has to be run on the device based on the access rights required for the procedure. Please note this option will not be available for a patch procedure.
  - **Maintenance window** status - Details of any maintenance windows in the device's profile.
    - **Total number of devices outside of maintenance window -** The number of devices that are not part of a maintenance window. The procedure can run on these devices.
    - **Number of devices blocked by maintenance windows settings -** The number of devices on which you cannot run the procedure because the admin has blocked procedures outside the maintenance window.
    - **Number of devices warned by maintenance window settings -** The number of devices that are part of a maintenance window and have warnings enabled. You can still run the procedure on these devices.
      - **Skip devices warned by maintenance windows settings -** A maintenance window is a time-slot reserved for running procedures on target devices. Admins can enable a warning if somebody attempts to run a procedure outside of the window. This setting will

skip those devices which have been added to a maintenance window with warnings enabled.

- **Configure parameters -** Available only for script procedures defined with variable parameters and allows you to enter the values for them.

**To specify values for variable parameters**

- Click 'Configure Parameters'



Procedure parameters

Message (Data Type: String)

□ Use default value

Hi, How are you?

Title (Data Type: String)

□ Use default value

Message from Administartor

A list of variable parameters will appear with their default values pre-populated.

- Enter the value for each parameter in the appropriate text box
- Select 'Use default value' if you want the default value to be applied for a parameter,
- Click 'Apply'

Tip: You can skip this step If you want to use default values for all parameters. For more info on default values, see **Create a Custom Procedure**.

- Click the 'Run' button in the 'Run Procedure' dialog.

The command will sent to the device and the selected procedure run. An alert will be generated if the procedure fails (presuming alerts have been configured). The process will be logged. You can view the procedure execution logs in two ways:

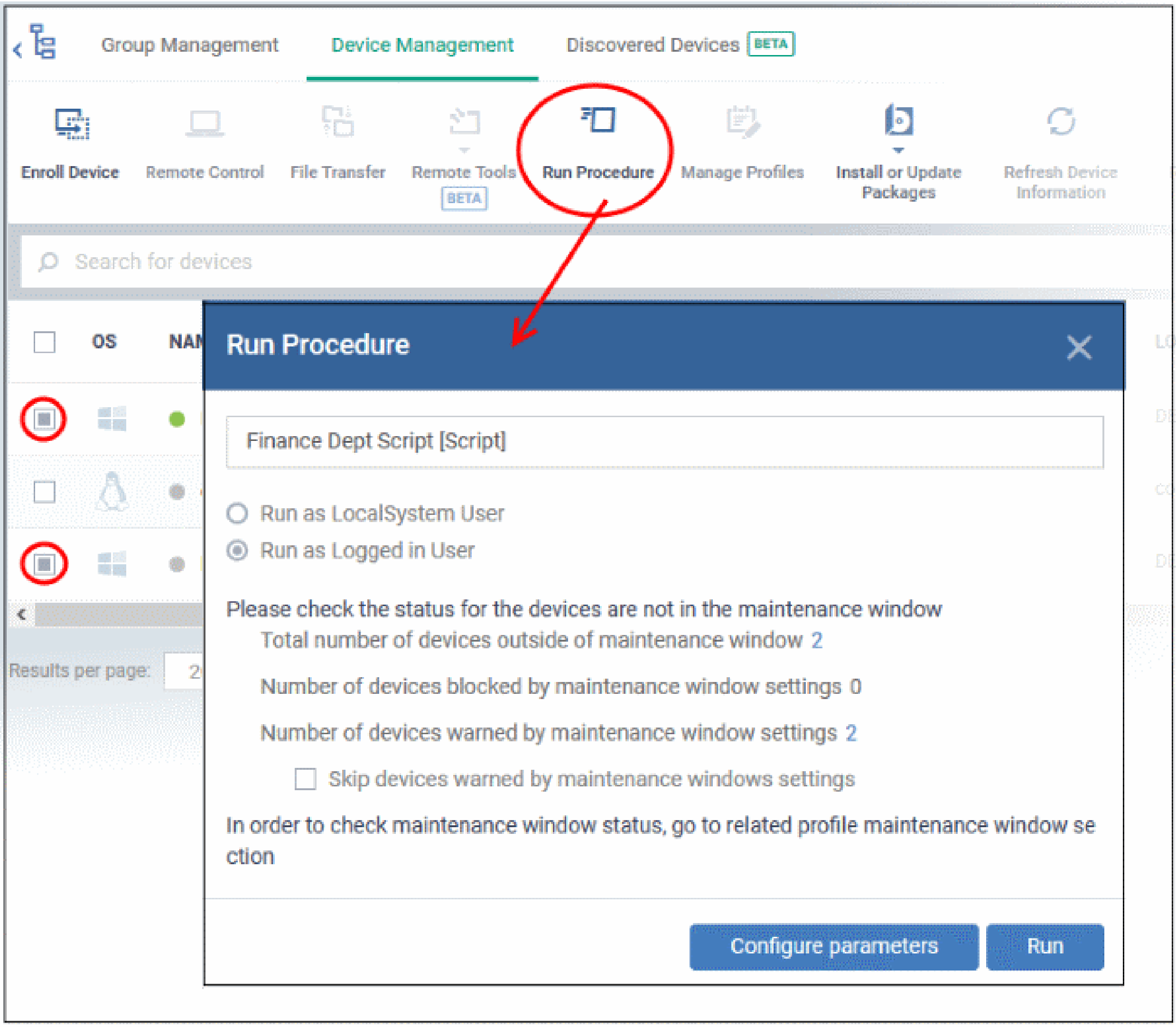
- From 'Device Logs' interface:
  - Click 'Devices' > 'Device List' > 'Device Management'
  - Click the device name to open its 'Device Details' interface
  - Select the 'Logs' tab and select 'Script Logs', 'Patch Logs' or 'Third Party Patch logs' depending on the type of the procedure
  - See **View Device Logs** for more details.
- From the 'Procedures' interface
  - Click 'Configuration Templates' > 'Procedures'
  - Click the name of the procedure to open the procedure configuration interface

- Select the 'Execution Log' tab
- See **View Procedure Results** for more details.

**Run a procedure on multiple devices at once**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Select the Windows devices on which you want to run a procedure
- Click 'Run Procedure'. ( or click 'More...' and choose 'Run Procedure' from the options)



Finance Dept Script [Script]

○ Run as LocalSystem User
● Run as Logged in User

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 2

Number of devices blocked by maintenance window settings 0

Number of devices warned by maintenance window settings 2

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window se ction

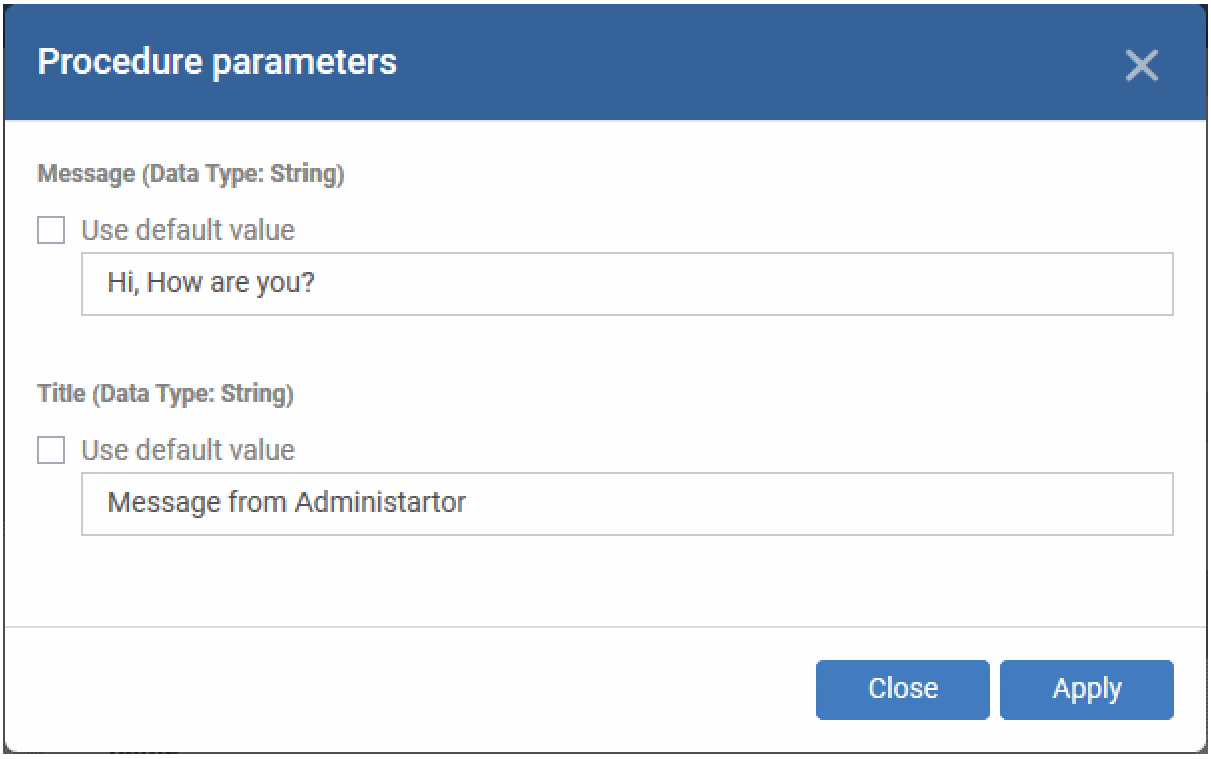
- Type the first few characters of the name of the procedure in the 'Choose Procedure' text box. Select the procedure you want to apply from the search suggestions. Only one procedure can be run at a time. Please note only **approved** procedures will be listed.
  - **Run as Local System User / Run as Logged in user -** Choose the user account with which the procedure has to be run on the device based on the access rights required for the procedure. Please note this option will not be available for a patch procedure.
  - **Maintenance window status -** Details of any **maintenance windows** in the device's profile.

- **Total number of devices outside of maintenance window -** The number of devices that are not part of a maintenance window. The procedure can run on these devices.
- **Number of devices blocked by maintenance windows settings -** The number of devices on which you cannot run the procedure because the admin has blocked procedures outside of maintenance window.
- **Number of devices warned by maintenance window settings -** The number of devices that are part of a maintenance window and have warnings enabled. You can still run the procedure on these devices.
    - **Skip devices warned by maintenance windows settings -** A maintenance window is a time-slot reserved for running procedures on target devices. Admins can enable a warning if somebody attempts to run a procedure outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.

- **Configure parameters -** Applicable only for script procedures defined with variable parameters and allows you to enter the values for them.

  **To specify values for variable parameters**

  - Click 'Configure Parameters'



Procedure parameters

Message (Data Type: String)

□ Use default value

Hi, How are you?

Title (Data Type: String)

□ Use default value

Message from Administartor

The list of variable parameters will appear with their default values pre-populated in their respective text fields

- Enter the value for each parameter in the respective text box
- Select 'Use default value' if you want the default value to be applied for a parameter,
- Click 'Apply'

**Tip**: You can skip this step If you want to use default values for all parameters. For more info on default values, see **Create a Custom Procedure**.

- Click the 'Run' button in the 'Run Procedure' dialog.

The command will sent to the devices and the selected procedure will be run on them. An alert will be generated if the procedure fails (presuming alerts have been configured). The process will be logged. You can view the procedure execution logs in two ways:

- From 'Device Logs' interface:
    - Click 'Devices' > 'Device List' > 'Device Management'
    - Click the name of a device on which the procedure was run, to open its 'Device Details' interface
    - Select the 'Logs' tab and select 'Script Logs', 'Patch Logs' or 'Third Party Patch logs' depending on the type of the procedure
    - See **View Device Logs** for more details.
- From the 'Procedures' interface
    - Click 'Configuration Templates' > 'Procedures'
    - Click the name of the procedure to open the procedure configuration interface
    - Select the 'Execution Log' tab
    - See **View Procedure Results** for more details.

## 5.2.13. Remotely Install and Update Packages on Windows Devices

- Click 'Devices' > 'Device List' > select a target device > Click 'Install or Updates Packages' button.

The device management screen lets you install/update Comodo applications and third-party packages on Windows endpoints. You have the following options:

- **Additional Comodo Packages** - Install Comodo Client Security (CCS) and Comodo Client Endpoint Detection and Response (EDR)
- **Custom MSI/Packages** - Install a package of your choice by specifying the URL of the package.
- **Update Additional Comodo Packages** - Install the latest versions of CCS, EDR and/or the communication client.

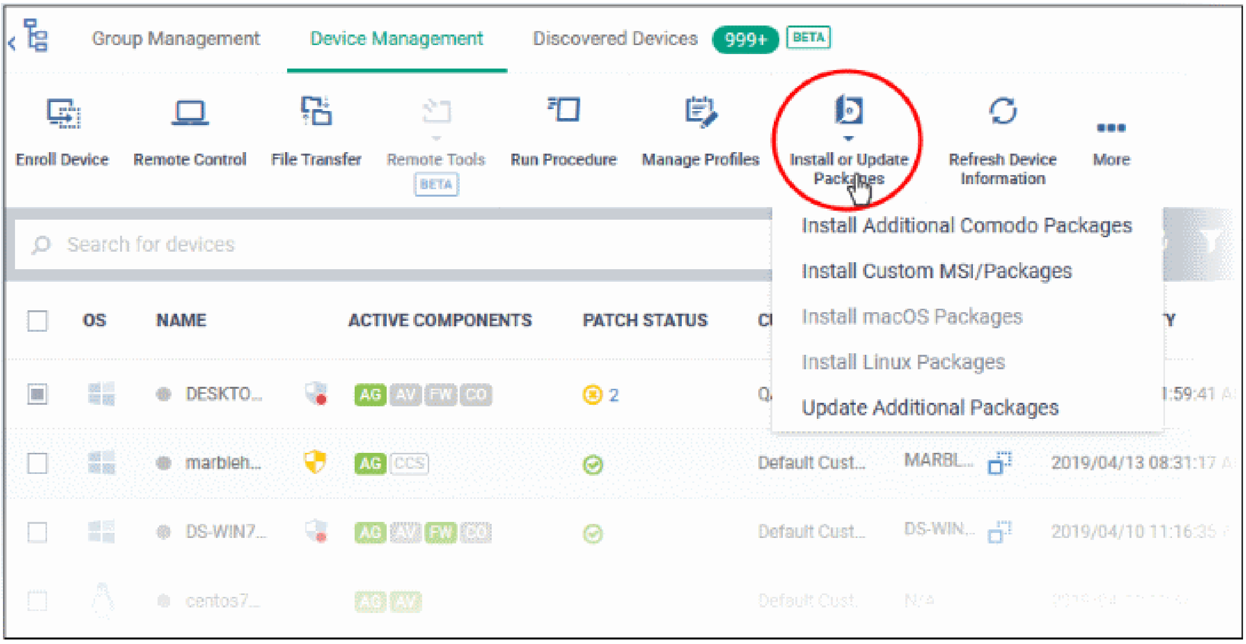
You can choose the following reboot options:

- Force reboot after 5, 10, 15 or 30 minutes
- Suppress the reboot entirely
- Warn the end-user about the reboot and allow them to postpone it. You can also send a message to the end-user.

**Install MSI / EM packages**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device in EM
- Select your target Windows devices using the check-boxes on the left
- Click 'Install or Update Packages':



- Alternatively, click on the name of the device > select 'Install or Update Packages'.

The drop-down contains the following options:

- Install Additional Comodo Packages
- Update Additional Comodo Packages
- Install Custom MSI/Packages

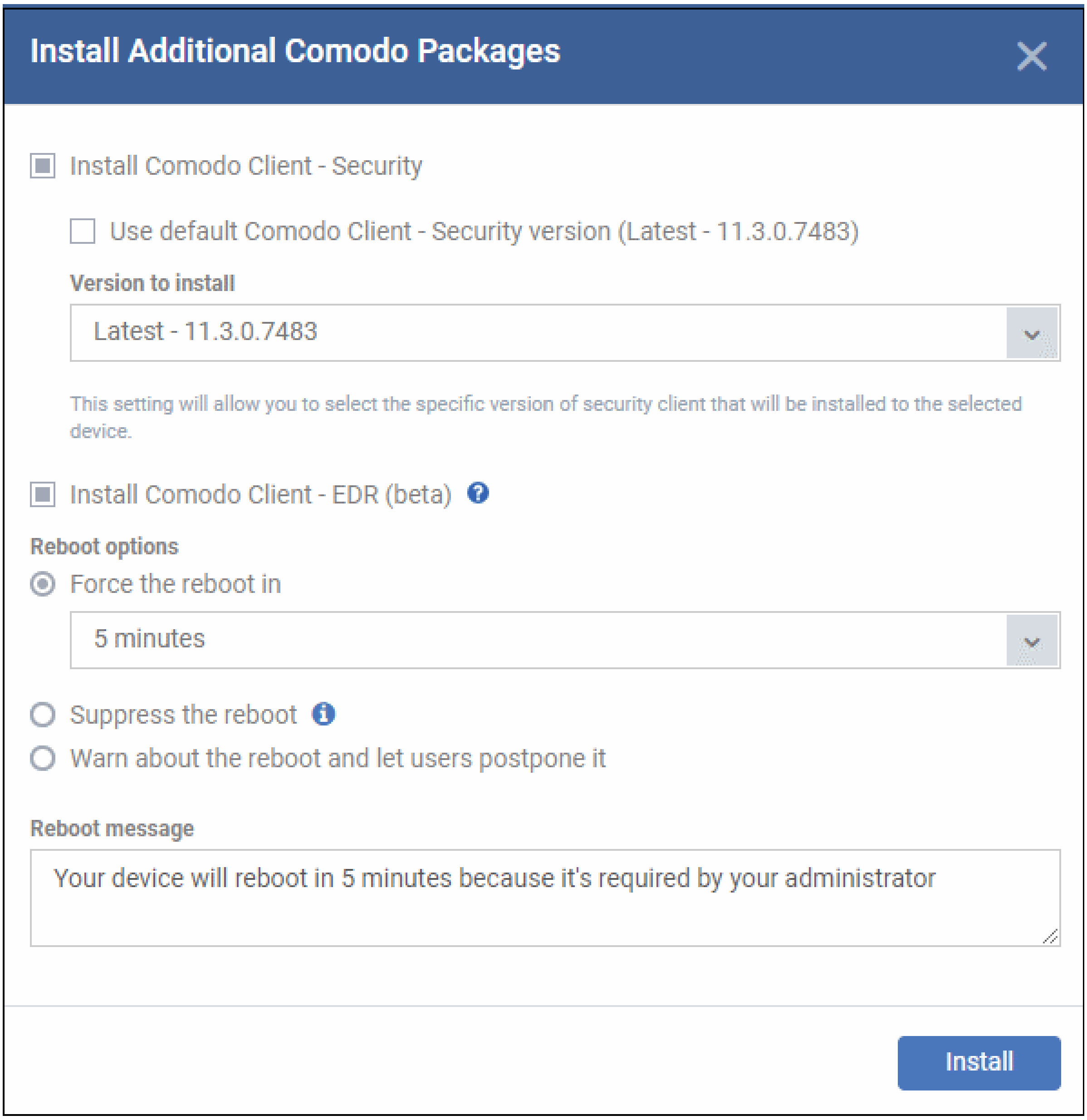
Tip: You can remotely install CCS on a Windows endpoint by clicking the shield icon next to the device name.

### Install Comodo packages

- Click 'Install or Update Packages'
- Select 'Install Additional Comodo packages'

Note:

- The packages must be enabled in 'Extensions Management' to appear in this screen.
- Click 'Settings' > 'Portal Set-up' > 'Extensions Management' to enable or disable packages.
- See 'Manage Endpoint Manager Extensions' if you wish to read more about extensions.



☑ Install Comodo Client - Security

□ Use default Comodo Client - Security version (Latest - 11.3.0.7483)

Version to install: Latest - 11.3.0.7483

This setting will allow you to select the specific version of security client that will be installed to the selected device.

☑ Install Comodo Client - EDR (beta)

Reboot options

● Force the reboot in: 5 minutes

○ Suppress the reboot

○ Warn about the reboot and let users postpone it

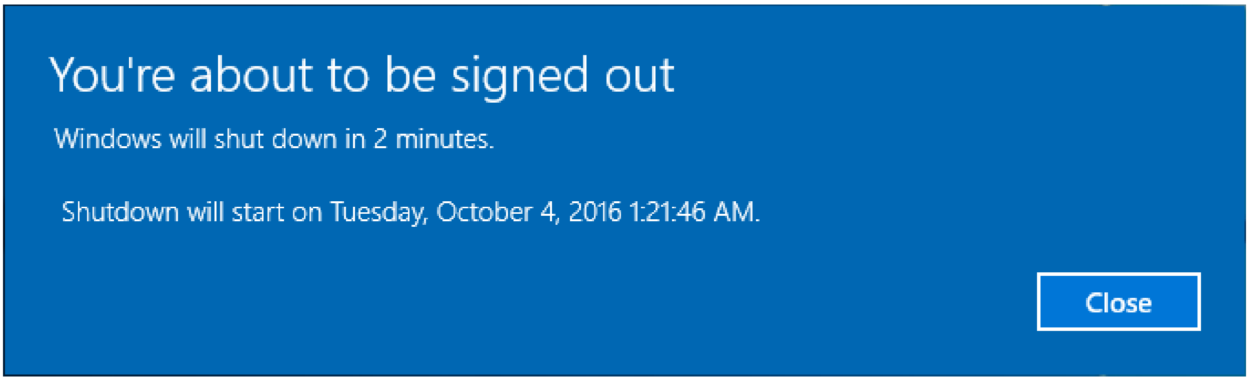
Reboot message: Your device will reboot in 5 minutes because it's required by your administrator

- **Install Comodo Client - Security** - Available for endpoints that do not have CCS installed. CCS is a complete endpoint security suite which features a powerful antivirus, enterprise class firewall, advanced host intrusion prevention and automatic containment of unknown files. You can configure which CCS components are installed by applying a configuration profile.
    - Note - The option to change the CCS version is only visible if enabled in **portal settings**. If not enabled then the 'Default version' is deployed.
- **Install Comodo Client EDR** - Installs the Comodo Endpoint Detection and Response (EDR) client. EDR is a powerful event analysis tool that provides real-time monitoring and detection of malicious events on Windows endpoints.
    - Note -You must first have added EDR to your CD / C1 account. Click 'Store' in CD / C1 to do so.

You need to restart the endpoint to complete the agent installation. You have the following reboot options:

- '**Force the reboot in...**' - restart the end-point a certain period of time after installation. Choice of 5, 10, 15 or 30 minutes

The following message will be displayed on the device:



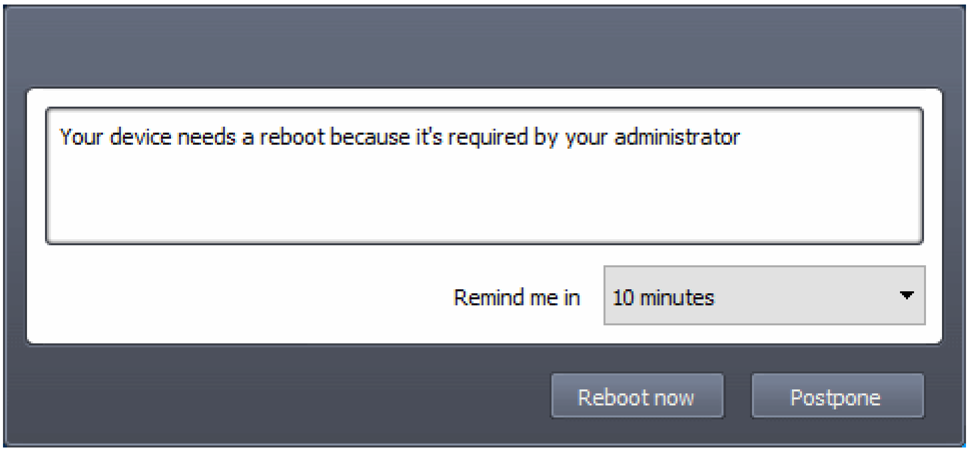
You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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

- '**Suppress the reboot**' - Do not restart the machine after installation. CCS will only become fully functional after the device is restarted.
- '**Warn about the reboot and let users postpone it**' - Show an alert to the user which advises them that their computer needs to be restarted. You can enter a custom message which is shown to the user:



Your device needs a reboot because it's required by your administrator

Remind me in: 10 minutes

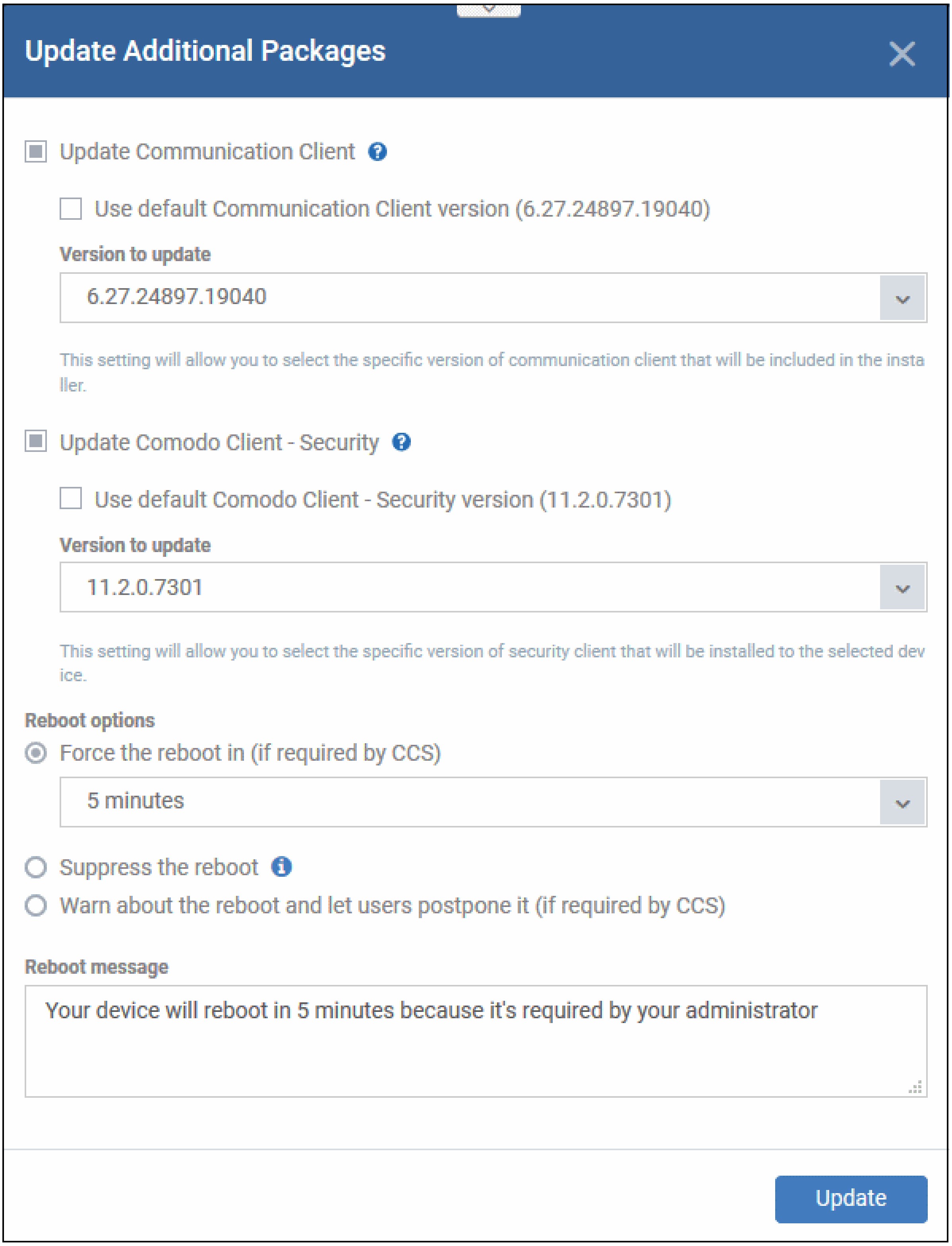
Users can restart the endpoint immediately by clicking 'Reboot now', or postpone it by picking a time in the 'Remind me in' drop-down.

Note: the CCS components which are active depends on the profile applied to the device. Components include firewall, antivirus, auto-containment, HIPS, Valkyrie and more.

- Click 'Devices' > 'Device List' > click device name > 'Associated Profiles', to see the profiles active on a device.
- Click 'Configuration Templates' > 'Profiles' to view and configure profiles
- See **View and Manage Profiles Associated with a Device**, **Assign Configuration Profile(s) to a User's Devices**, **Assign Configuration Profiles to a User Group** and **Assign Configuration Profiles to a Device Group** for help with profiles.

## Update EM Packages

- Select 'Update Additional Comodo packages' from the 'Install or Update Packages' drop-down
- The 'Update Additional Comodo packages' dialog lists all packages with available updates:



Update Additional Packages

☒ Update Communication Client

□ Use default Communication Client version (6.27.24897.19040)

Version to update: 6.27.24897.19040

This setting will allow you to select the specific version of communication client that will be included in the installer.

☒ Update Comodo Client - Security

□ Use default Comodo Client - Security version (11.2.0.7301)

Version to update: 11.2.0.7301

This setting will allow you to select the specific version of security client that will be installed to the selected device.

Reboot options

● Force the reboot in (if required by CCS)

5 minutes

○ Suppress the reboot

○ Warn about the reboot and let users postpone it (if required by CCS)

Reboot message: Your device will reboot in 5 minutes because it's required by your administrator

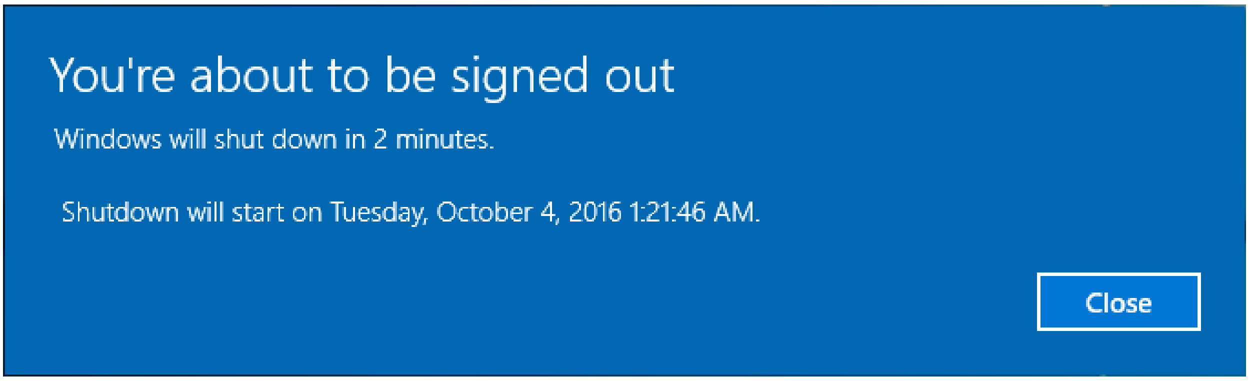
- **Update Communication Client -** Only available for devices with an out-dated version of the the communication client. As the name suggests, the communication client allows EM to send and receive updates to/from devices.
- **Update Comodo Client - Security -** Install database and software updates for CCS on the device. Only available for endpoints with out-dated versions of CCS.
  - Note 1 - The option to choose CC and CCS versions will be available if configured in **portal settings**. If the option is not selected, then the default version configured in **portal settings** will be updated.

- Note 2 - Make sure to upgrade to a higher version. Deployment of a lower version than the existing client is not supported.

CCS requires the endpoint to be restarted in order for the installation to take effect. You have the following reboot options:

- '**Force the reboot in...**' - restart the end-point a certain period of time after installation. Choice of 5, 10, 15 or 30 minutes

The following message will be displayed on the device:



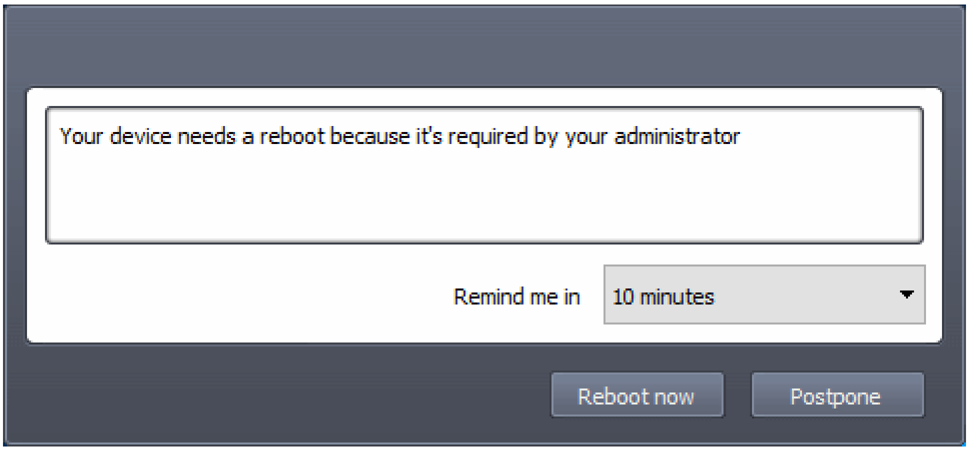
You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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

- '**Suppress the reboot**' - Do not restart the machine after installation. CCS will only become fully functional after the device is restarted.
- '**Warn about the reboot and let users postpone it**' - Show an alert to the user which advises them that their computer needs to be restarted. You can enter a custom message which is shown to the user:



Your device needs a reboot because it's required by your administrator

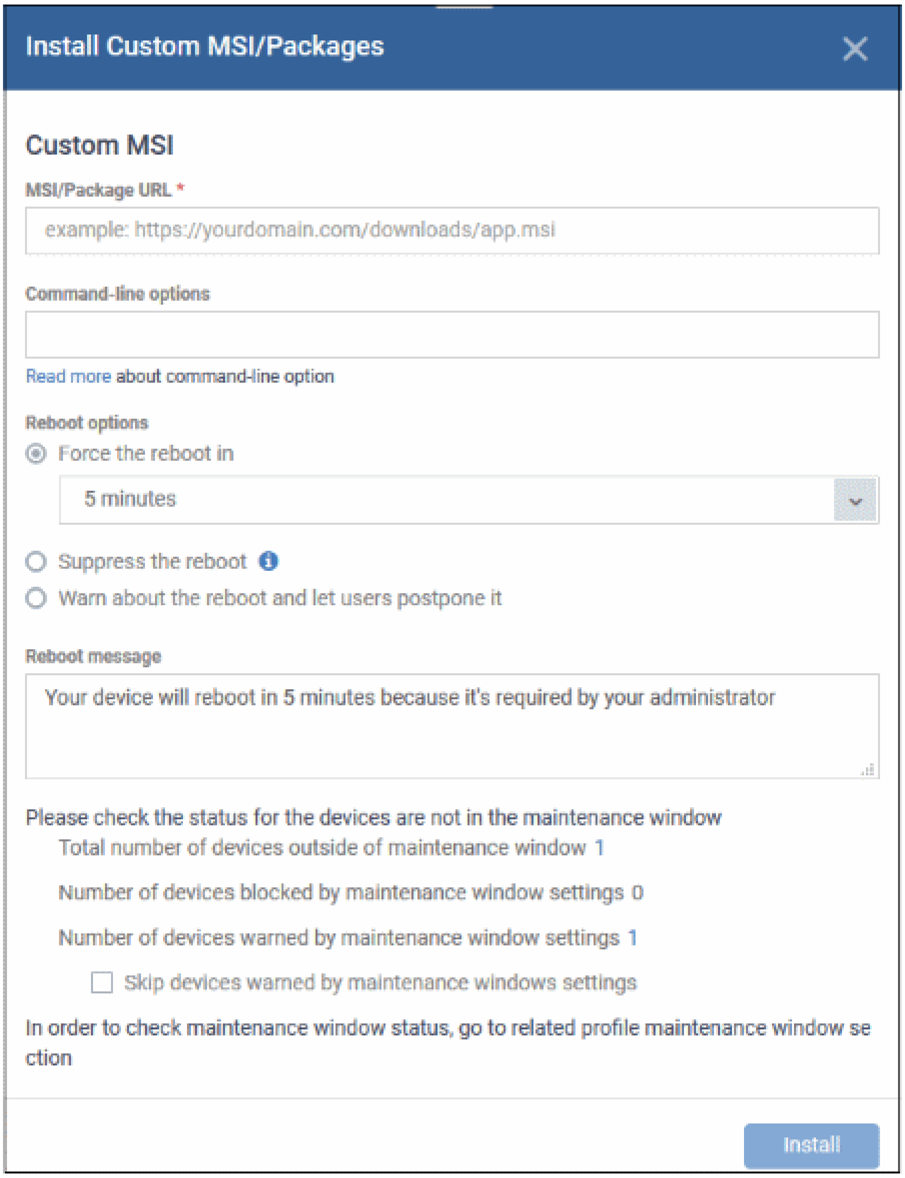
Remind me in: 10 minutes

Users can restart the endpoint immediately by clicking 'Reboot now', or postpone it by picking a time in the 'Remind me in' drop-down.

## Install third-party MSI packages

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

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



Install Custom MSI/Packages

Custom MSI

MSI/Package URL *

example: https://yourdomain.com/downloads/app.msi

Command-line options

Read more about command-line option

Reboot options

● Force the reboot in

5 minutes

○ Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message

Your device will reboot in 5 minutes because it's required by your administrator

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 1

Number of devices blocked by maintenance window settings 0

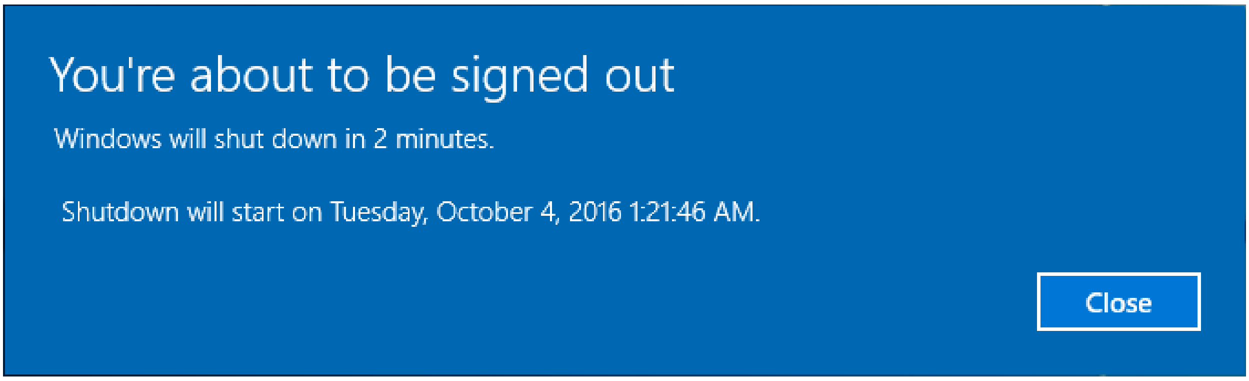
Number of devices warned by maintenance window settings 1

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window se ction

- **MSI/Package URL** - enter the location of the installer. Make sure it is from a https site. For example, https://www.hass.de/files/nodes/story/45/npp.6.8.4.installer.msi
- **Command-line Options** - Enter any required installation switches (optional).
    - You need only enter the command here. E.g. /L or /quiet
    - Click the 'Read more' link to read more about command-line options.
- Choose the reboot option you prefer:
    - '**Force the reboot in...**' - restart the end-point a certain period of time after installation. Choice of 5, 10, 15 or 30 minutes

The following message will be displayed on the device:



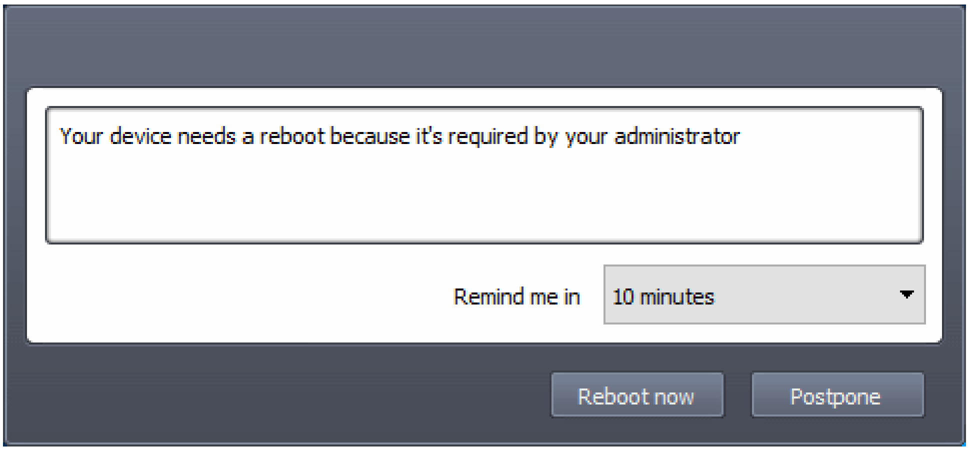
You're about to be signed out

Windows will shut down in 2 minutes.

Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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

- '**Suppress the reboot'** - Do not restart the machine after installation. CCS will only become fully functional after the device is restarted.
- '**Warn about the reboot and let users postpone it'** - Show an alert to the user which advises them that their computer needs to be restarted. You can enter a custom message which is shown to the user:



Your device needs a reboot because it's required by your administrator

Remind me in: 10 minutes

Users can restart the endpoint immediately by clicking 'Reboot now', or postpone it by picking a time in the 'Remind me in' drop-down.

- **Maintenance window status** - Details of any maintenance windows in the device's profile.
  - **Total number of devices outside of maintenance window** - The number of devices that are not part of a maintenance window. The installation can run on these devices.
  - **Number of devices blocked by maintenance windows settings** - The number of devices on which you cannot run the installation because the admin has blocked installs outside of maintenance window.
  - **Number of devices warned by maintenance window settings** - The number of devices that are part of a maintenance window and have warnings enabled. You can still install on these devices.
    - **Skip devices warned by maintenance windows settings** - A maintenance window is a time-slot reserved for running important tasks on target devices. Admins can enable a warning if somebody attempts an installation task outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.
- Click 'Install'

## 5.2.14. Remotely Install Packages on Mac OS Devices

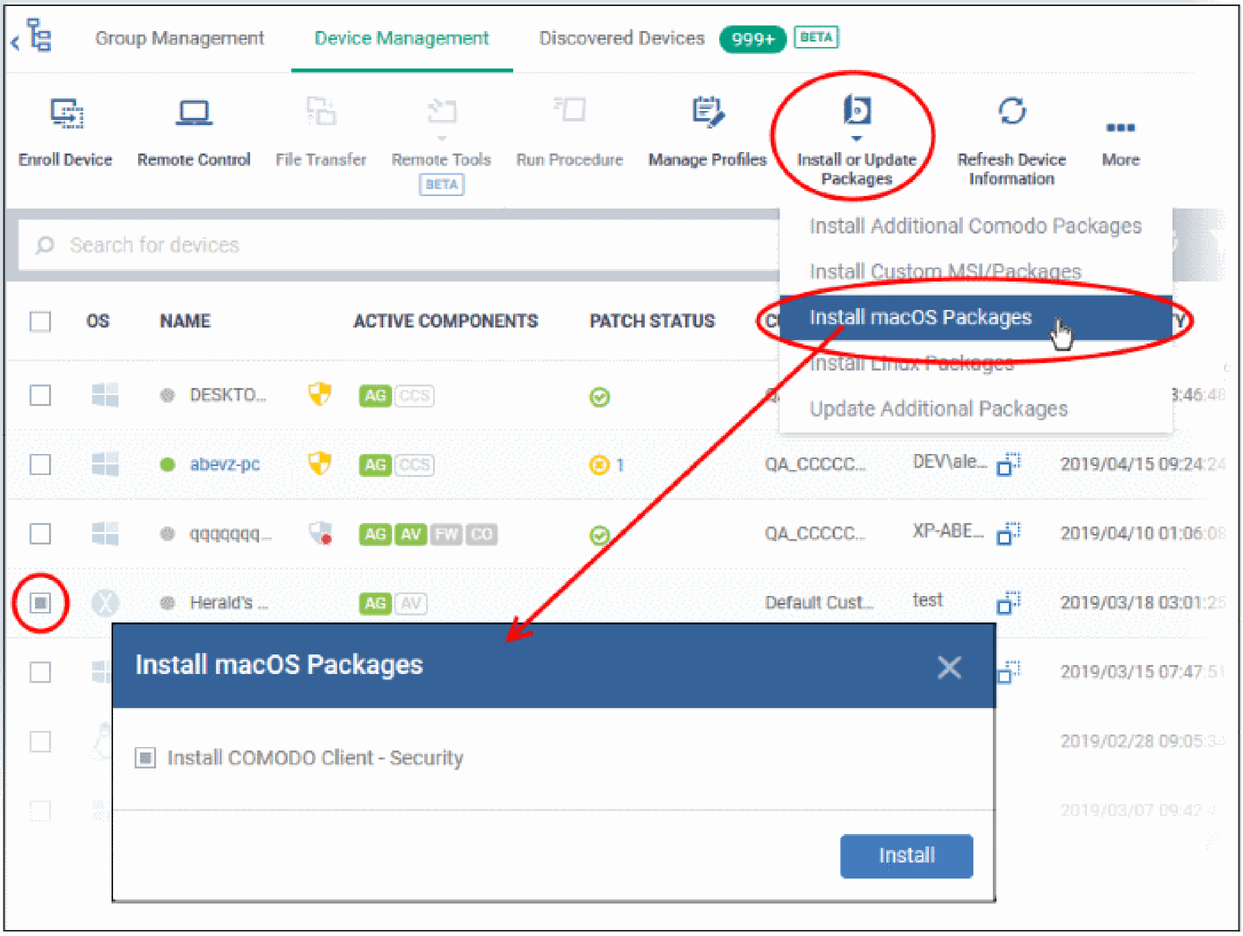
Admins can remotely install CCS onto Mac OS devices from the 'Device Management' interface.

**To install Mac OS packages**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
  - Select a company or a group to view just their devices

    Or

  - Select 'Show all' to view every device in EM
- Select the target Mac OS devices using the check-boxes on the left
- Click 'Install or Update Packages' from the options at the top then choose 'Install macOS Packages'



  - Alternatively, click on the name of the device > select 'Install mac OS Packages'.
- Choose 'Install Comodo Client - Security'
- Click 'Install'
- A command will be sent to target endpoints to install CCS. The application will become effective immediately after installation.
- You can view the installation status as follows:
  - Click 'Devices' > 'Device List'
  - Click on the name of the device > select 'Packages Installation State'.
  - See **View Mac OS Packages Installed on a Device through Endpoint Manager** for more details.

**Note**: The actual settings of CCS depends on the profile applied to the device:

- Click 'Devices' > 'Device List' > click device name > 'Associated Profiles', to see the profiles active on a device.
- Click 'Configuration Templates' > 'Profiles' to view and configure profiles

The following sections contain more help on profiles:

- **View and Manage Profiles Associated with a Device**
- **Assign Configuration Profile(s) to a User's Devices**
- **Assign Configuration Profiles to Selected Devices**
- **Assign Configuration Profiles to a User Group**
- **Assign Configuration Profiles to a Device Group**

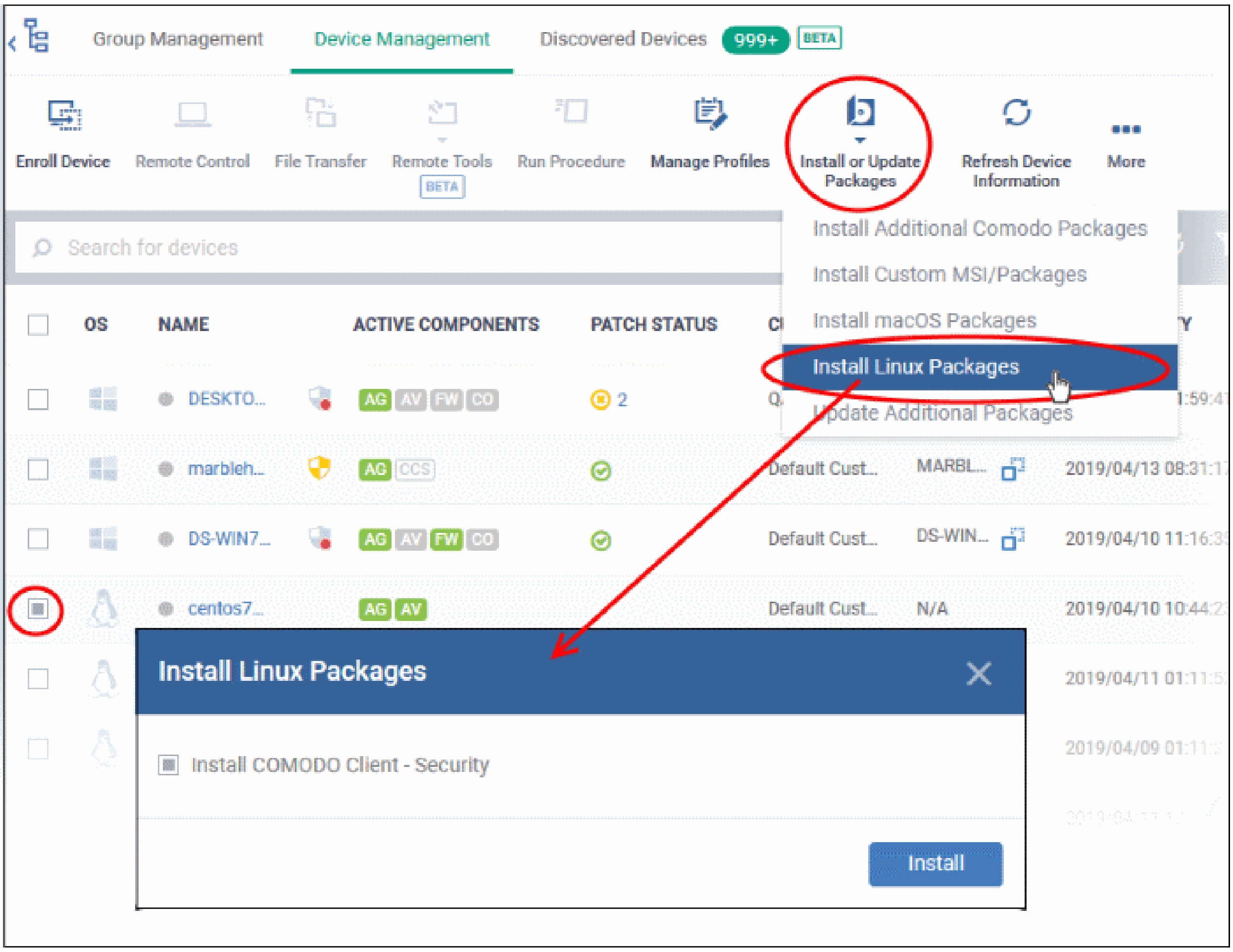
## 5.2.15. Remotely Install Packages on Linux Devices

Admins can remotely install CCS onto Linux devices from the 'Device Management' interface.

**To install Mac OS packages**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device in EM
- Select the target Linux devices using the check-boxes on the left
- Click 'Install or Update Packages' from the options at the top and choose 'Install Linux Packages'



  - Alternatively, click on the name of the device > select 'Install Linux Packages'.
- Choose 'Install Comodo Client - Security'
- Click 'Install':
- A command will be sent to target endpoints to install CCS. The application will become effective immediately after installation.
- You can view the installation status as follows:
  - Click 'Devices' > 'Device List'
  - Click on the name of the device > select 'Packages Installation State'.
  - See **View Linux Packages Installed on a Device through Endpoint Manager** for more details.

**Note**: The actual settings of CCS depends on the profile applied to the device:

- Click 'Devices' > 'Device List' > click device name > 'Associated Profiles', to see the profiles active on a device.
- Click 'Configuration Templates' > 'Profiles' to view and configure profiles

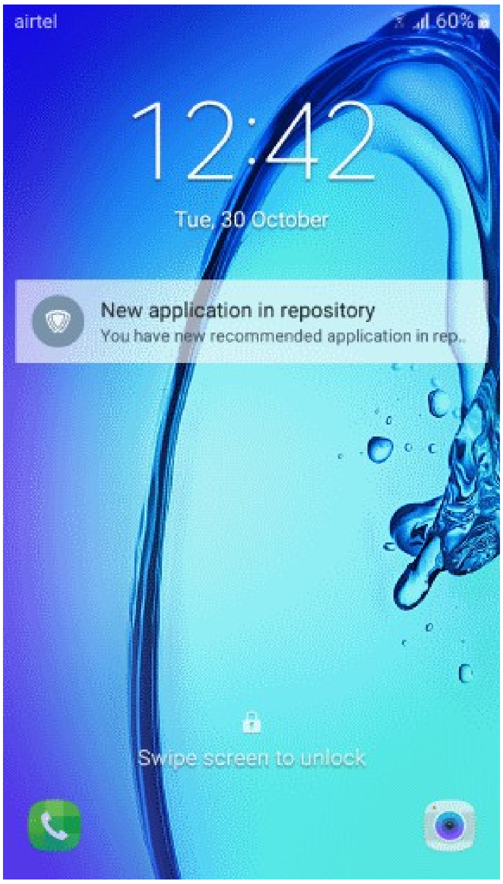
The following sections contain more help on profiles:

- **View and Manage Profiles Associated with a Device**
- **Assign Configuration Profile(s) to a User's Devices**
- **Assign Configuration Profiles to a User Group**
- **Assign Configuration Profiles to a Device Group**

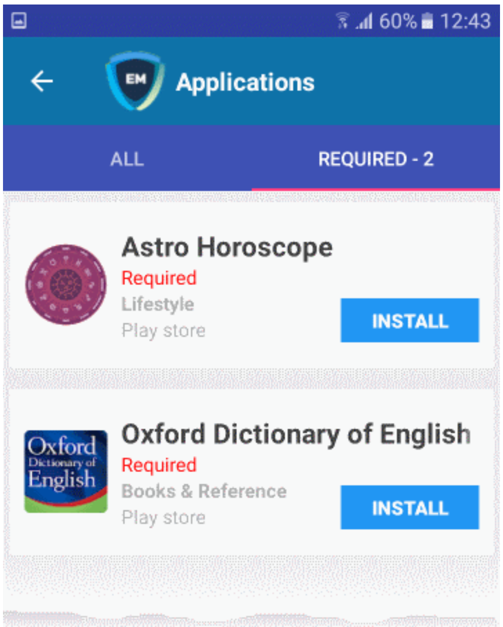
## 5.2.16. Install Apps on Android/iOS Devices

- Endpoint Manager allows you to push applications to all enrolled mobile devices
- You can add apps that you intend to distribute to devices to the EM **Application Store**.
  - Click 'Application Store' > 'iOS Store' or 'Android Store'
  - See **Application Store** for help to upload apps
- The sync between the EM server and the devices takes place every 24 hours. Alternatively, you can sync immediately by clicking 'Inform Devices Now' in the Android / iOS application store interface.

Managed devices are sent notifications about newly added apps:


airtel
12:42
Tue, 30 October
New application in repository
You have new recommended application in rep..
Swipe screen to unlock

Users should tap the notification to open the 'Applications' page:



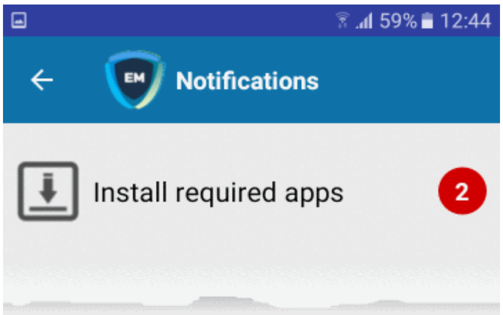
Astro Horoscope
Required
Lifestyle
Play store
INSTALL

Oxford Dictionary of English
Required
Books & Reference
Play store
INSTALL

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

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

Endpoint Manager also sends notification to devices if a mandatory or recommended app is uploaded to the **Application Store**.



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

## 5.2.17. Generate an Alarm on Devices

- If a device is mislaid, lost or stolen, you can make it sound an alarm to help locate it. The alarm will sound at full volume, even if it is set to silent mode.
- You 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.

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

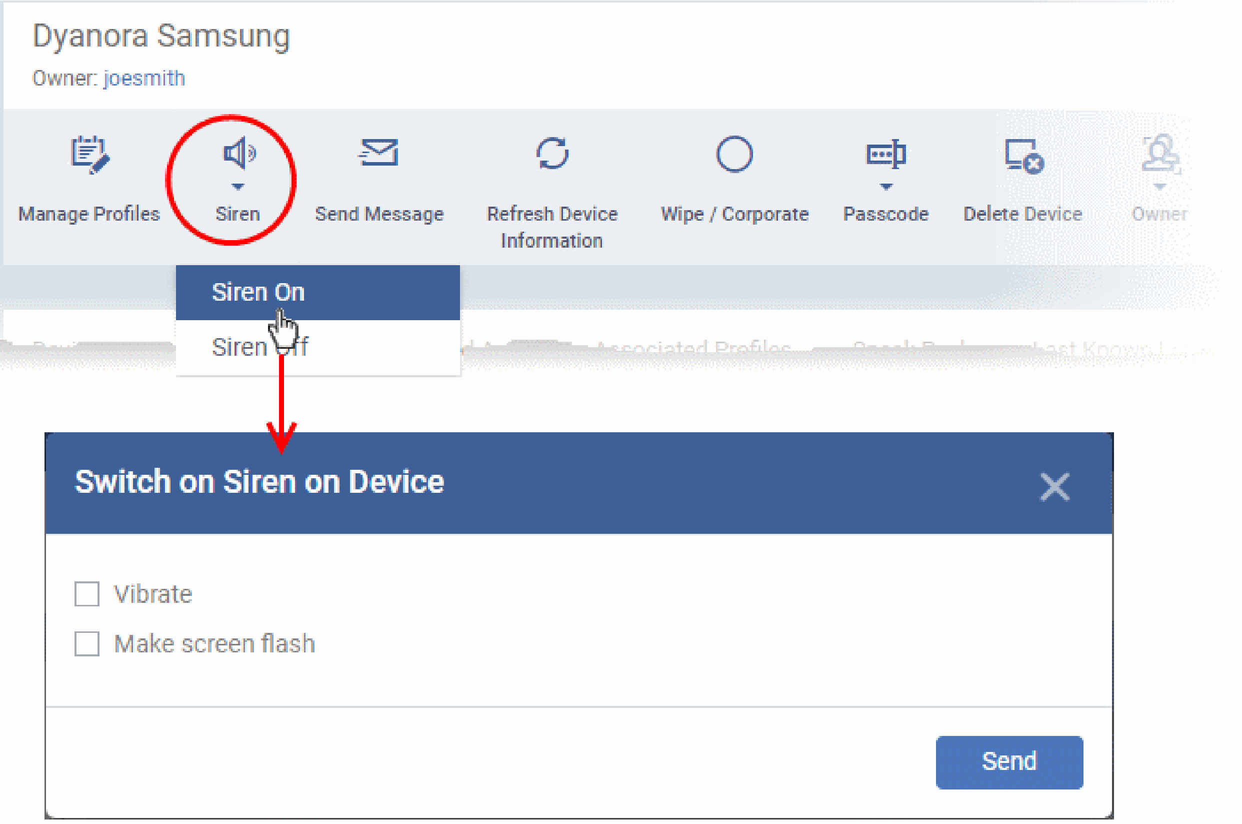
**To generate alarm on a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Click the name of the device on which you want to sound an alarm

The device details interface opens.

- Click 'Siren' on the top then choose 'Siren On'



Switch on Siren on Device

□ Vibrate

□ Make screen flash

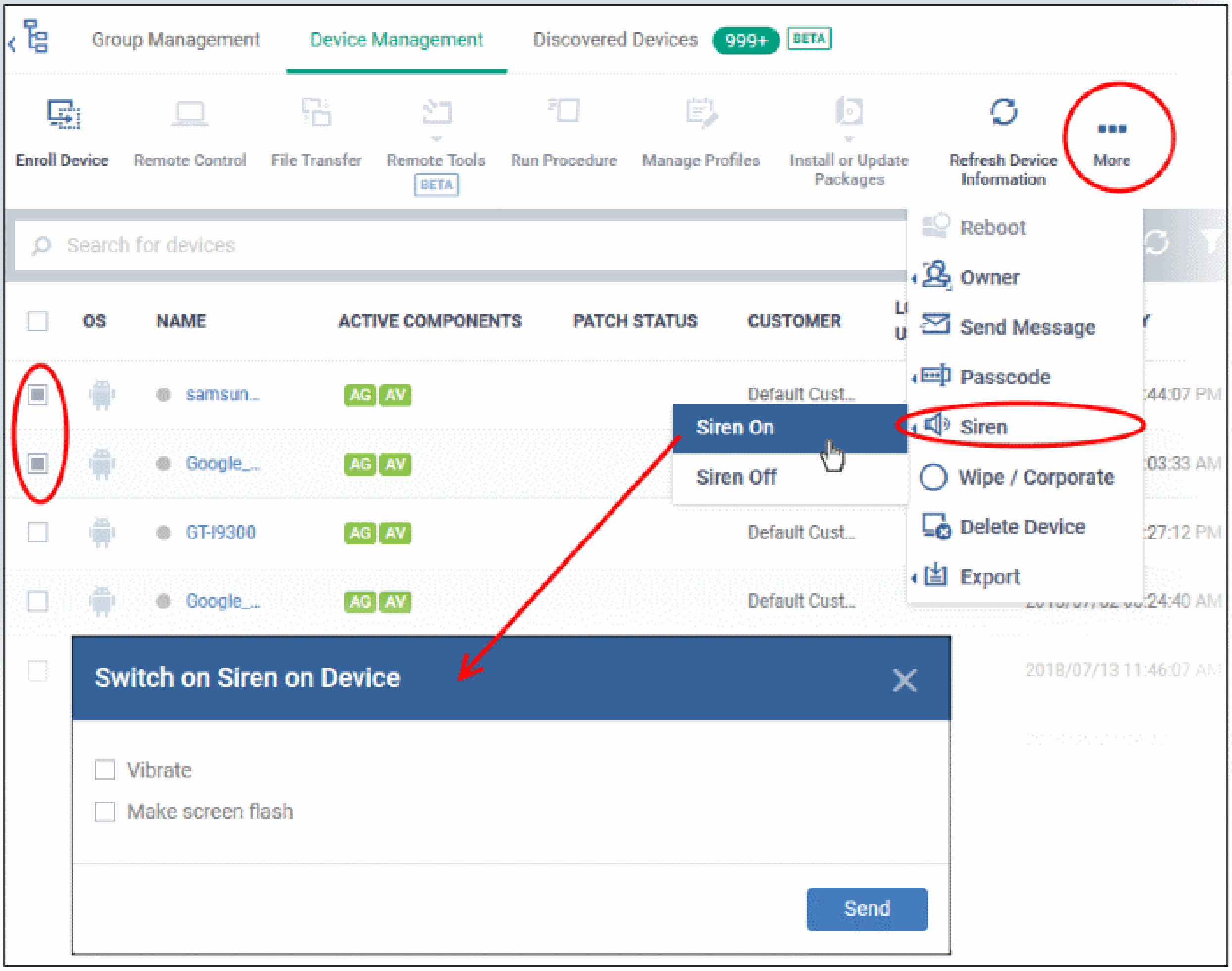
You can also choose the following extras:

  - Vibrate - The device will vibrate along with the siren
  - Make screen flash - The device screen will flash intermittently along with the siren
- Click the 'Send' button to issue the alarm.
- To switch off the alarm, click 'Siren' > 'Siren Off' from the same interface.

**To generate alarm on several devices**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Select the devices on which you want to sound an alarm
- Click 'Siren' at the top and choose Siren On' or click 'More...', select 'Siren' and choose 'Siren On'



You can also choose the following extras:

  - Vibrate - The devices will vibrate along with the siren
  - Make screen flash - The devices' screen will flash intermittently along with the siren
- Click the 'Send' button to issue the alarm

**To stop the alarm**

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

## 5.2.18. Lock / Unlock Selected Devices

- Admins can remotely lock devices to prevent them being accessed by unauthorized persons, or to generally block access to the device.
- Locked devices can only be opened by entering a passcode on the device.

The following sections contain more information on:

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

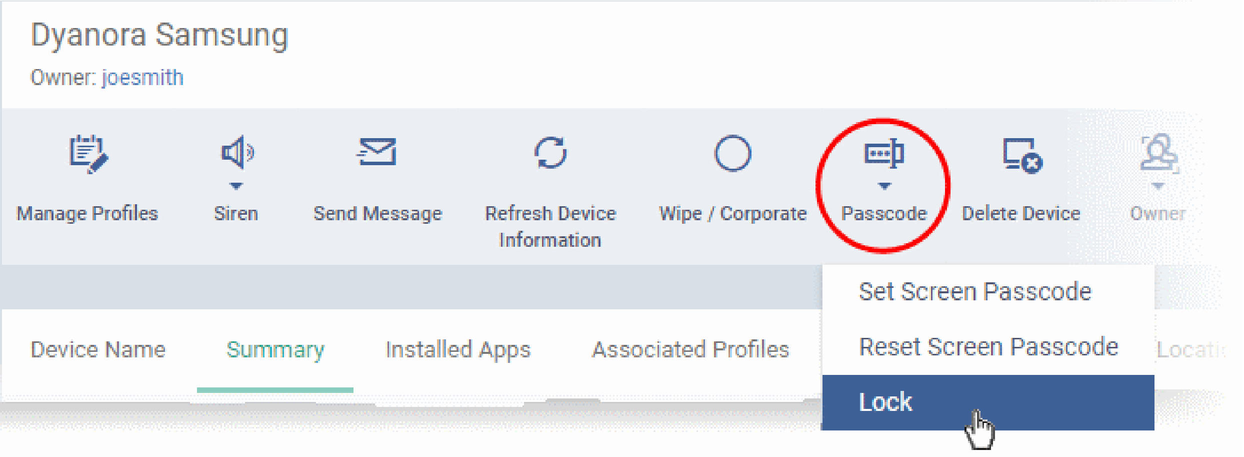
**To remotely lock a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

Or

- Select 'Show all' to view every device added to EM

- Click the name of the device you want to lock. This opens the device details interface.
- Click the 'Passcode' button at the top and choose 'Lock'.
  - If 'Passcode' is not displayed, click 'More...' , select 'Passcode' and choose 'Lock' from the options



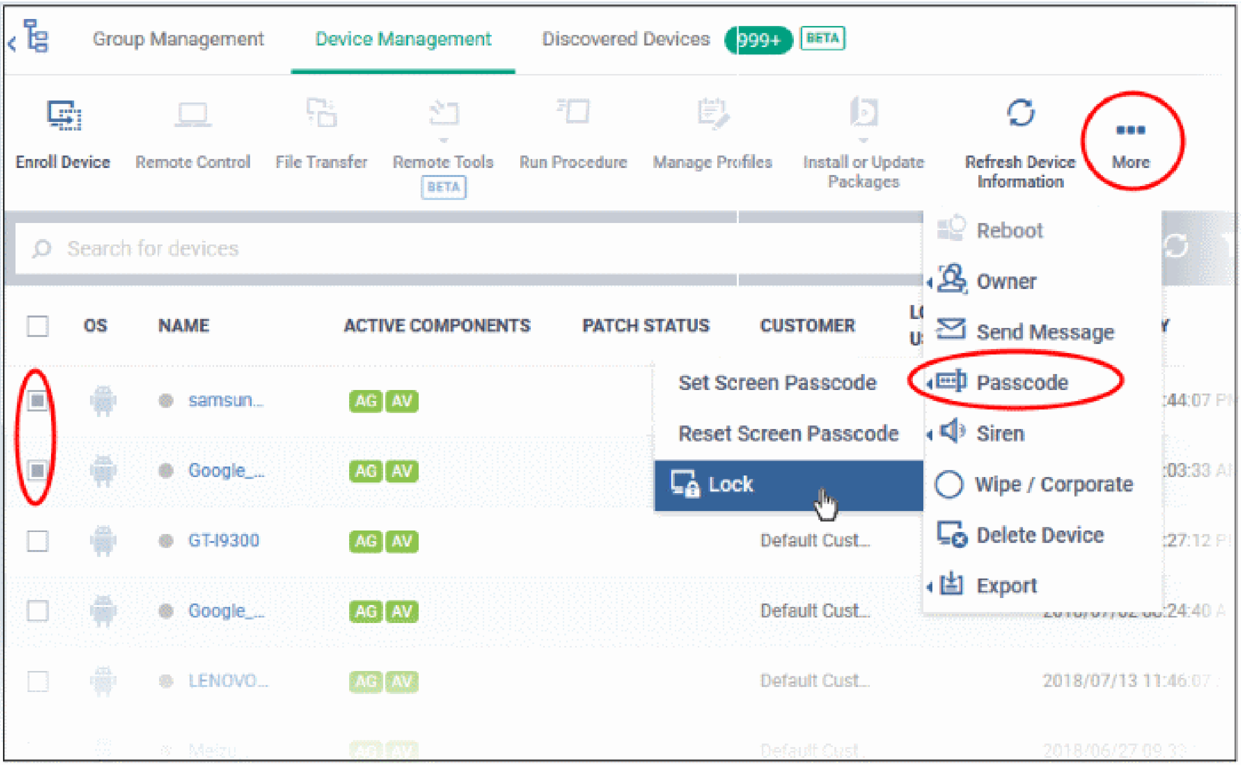
A command to lock the device is sent immediately. The device can only be unlocked by entering the screen lock password.

**To remotely lock several devices at-once**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

  Or

  - Select 'Show all' to view every device added to EM
- Select all devices that you want to lock
- Click the 'Passcode' button at the top
  - Or click 'More...' and select 'Passcode' from the drop-down.
- Choose 'Lock' from the options



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

## 5.2.19. Wipe Selected Devices

- Click 'Devices' > 'Device List' > select a device > Click 'More' > 'Wipe/Corporate'
- Confidential documents and sensitive information can be stolen from a lost or stolen device.
- To prevent such data loss, admins can remotely erase the contents of a lost device.
    - Additionally, you can configure a profile to wipe a device if the wrong password is entered a set number of times.
    - Click 'Configuration Templates' > 'Profiles' > click on an iOS/Android profile > 'Add Profile Section' > 'Passcode', to set this feature.

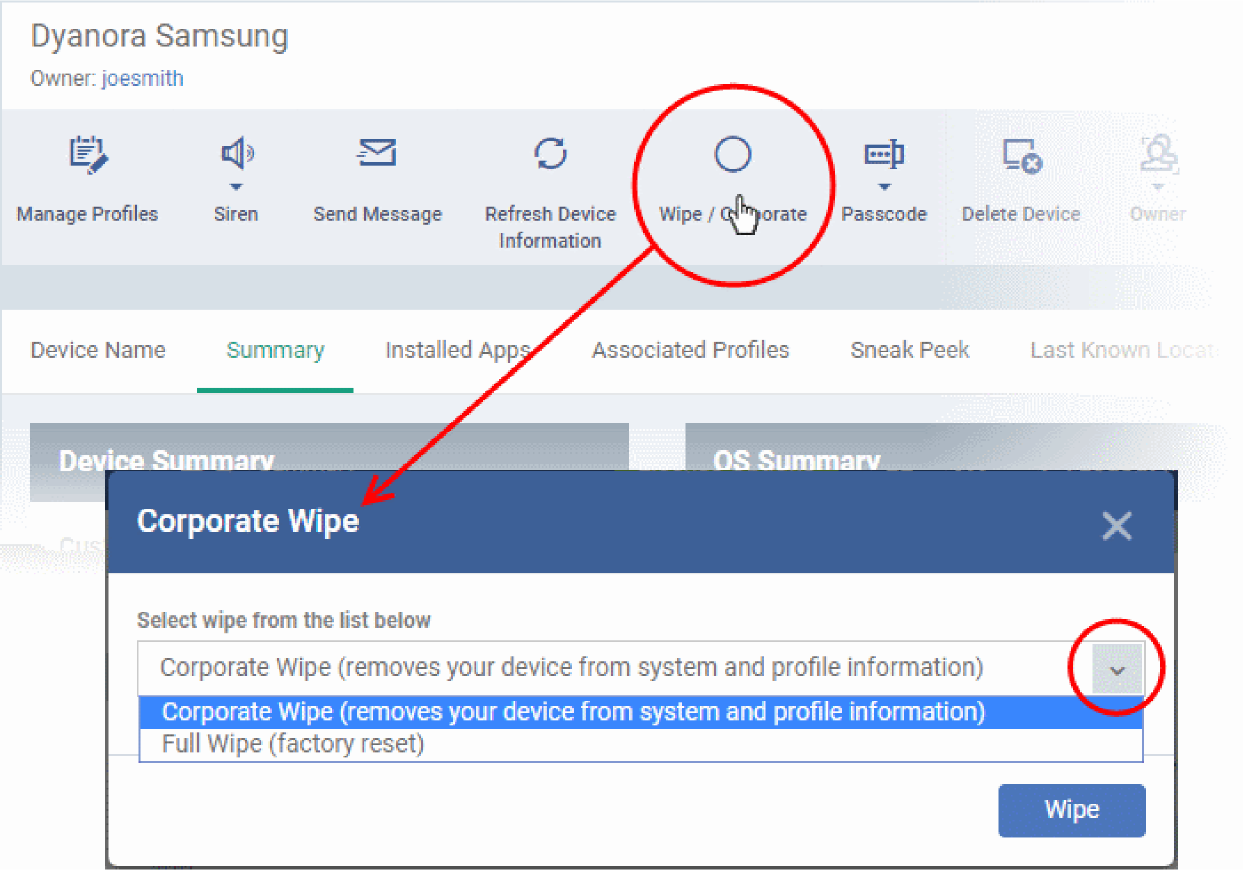
The following sections explain how to:

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

### Wipe a single device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Click on the name of the device you want to wipe. This will open the device details page.
- Click the 'Wipe / Corporate' button from the options at the top
    - or click 'More...' and choose 'Wipe / Corporate' from the options



Select wipe from the list below

Corporate Wipe (removes your device from system and profile information)

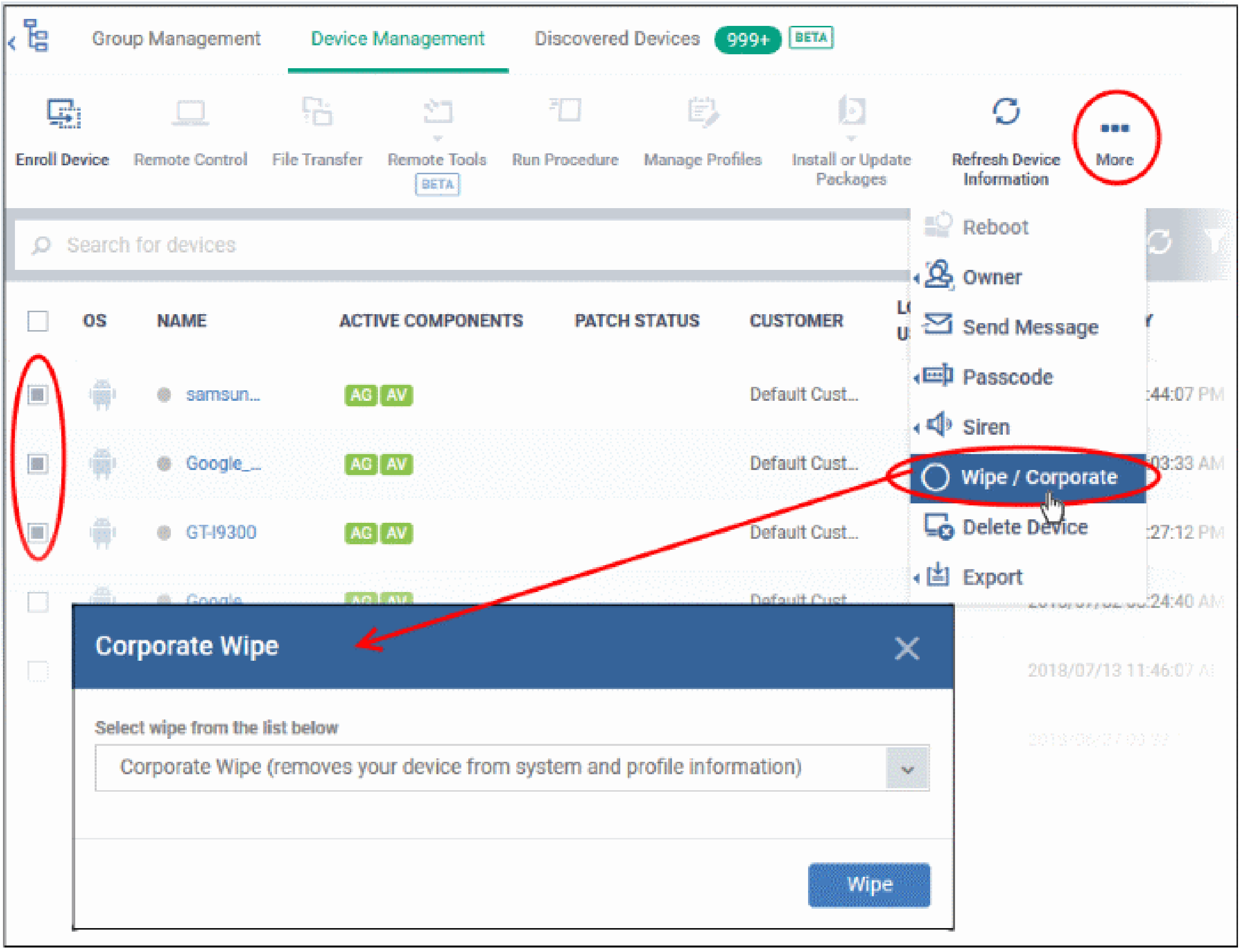
Corporate Wipe (removes your device from system and profile information)
Full Wipe (factory reset)

- Choose the type of wipe:
  - **Corporate Wipe -** Removes only the Endpoint Manager communication client and configuration profiles
  - **Full Wipe** - Erases all data from the device and the SD card. The device will be returned to default factory settings.
- Click the 'Wipe' button to send the command.

## Wipe several devices

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Select the target devices to be wiped
- Click 'Wipe / Corporate' from the options at the top or click 'More...' and choose 'Wipe / Corporate' from the options.



Corporate Wipe

Select wipe from the list below

Corporate Wipe (removes your device from system and profile information)

- Choose the type of wipe:
    - **Corporate Wipe -** Removes only the Endpoint Manager communication client and configuration profiles
    - **Full Wipe -** Erases all data from the device and the SD card. The device will be returned to default factory settings.
- Click the 'Wipe' button to send the command.

## 5.2.20. Assign Configuration Profiles to Selected Devices

- The 'Device Management' interface lets you view the configuration profiles in effect on selected devices. You can also apply new configuration profiles or remove profiles.
- Profiles applied from this interface will be added to any existing profiles on the device (such as profiles from a device group or user group).
- If the settings in a profile clash with those in another profile, Endpoint Manager follows the 'Most Restrictive' policy. For example, if a profile allows the use of the camera and another restricts its use, the device will not be able to use the camera.

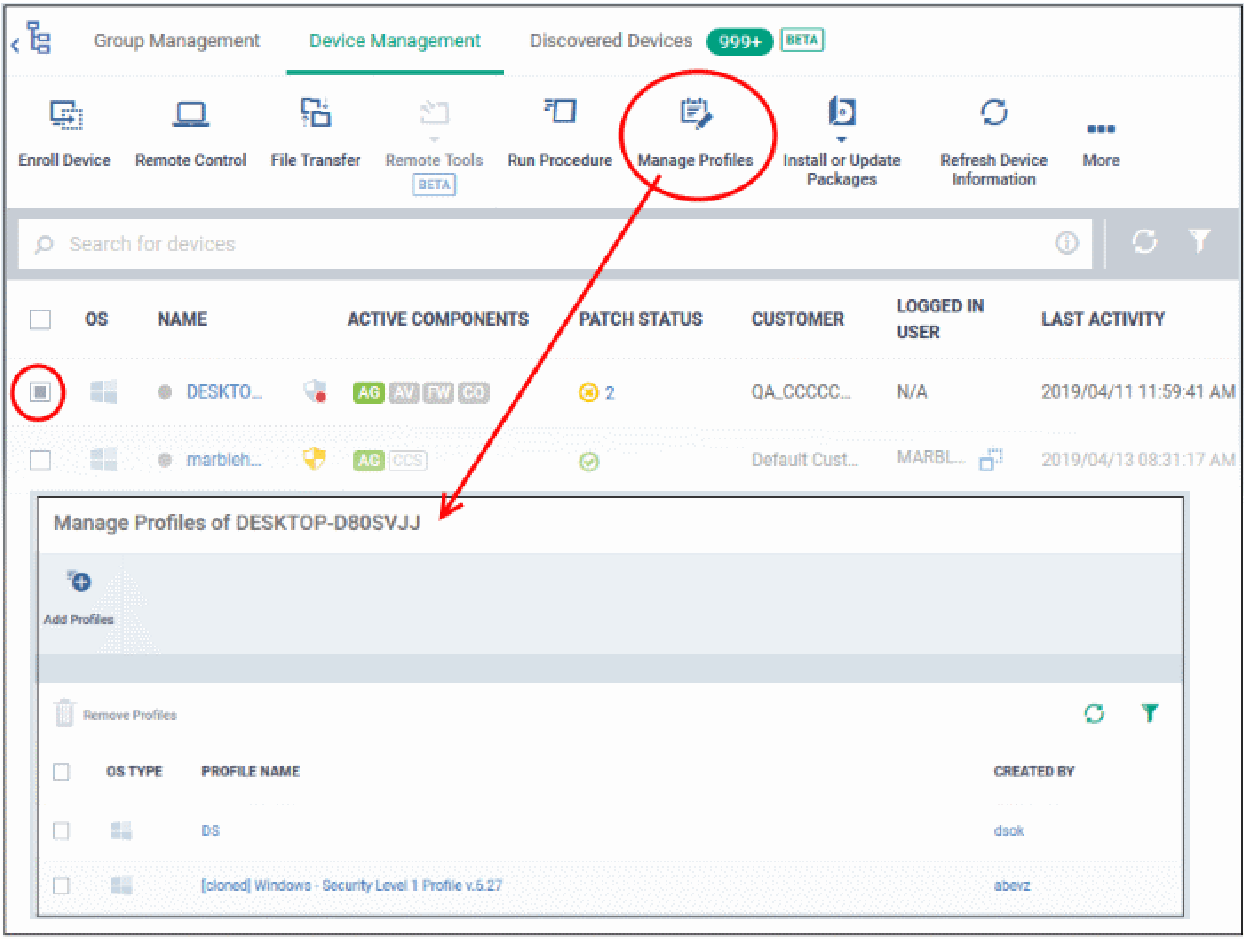
See **Create Configuration Profiles**, for more details on profiles.

**To manage profiles applied to a device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or

- Select 'Show all' to view every device added to EM
- Select the device you want to manage and click 'Manage Profiles' from the options at the top



| ☐ | OS | NAME | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LOGGED IN USER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|
| ☒ |  | DESKTO... | AG AV FW CO | 2 | QA_CCCCC... | N/A | 2019/04/11 11:59:41 AM |
| ☐ |  | marbleh... | AG CCS | ✓ | Default Cust... | MARBL... | 2019/04/13 08:31:17 AM |

Manage Profiles of DESKTOP-D80SVJJ

| ☐ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| ☐ |  | DS | dsok |
| ☐ |  | [cloned] Windows - Security Level 1 Profile v.6.27 | abevz |

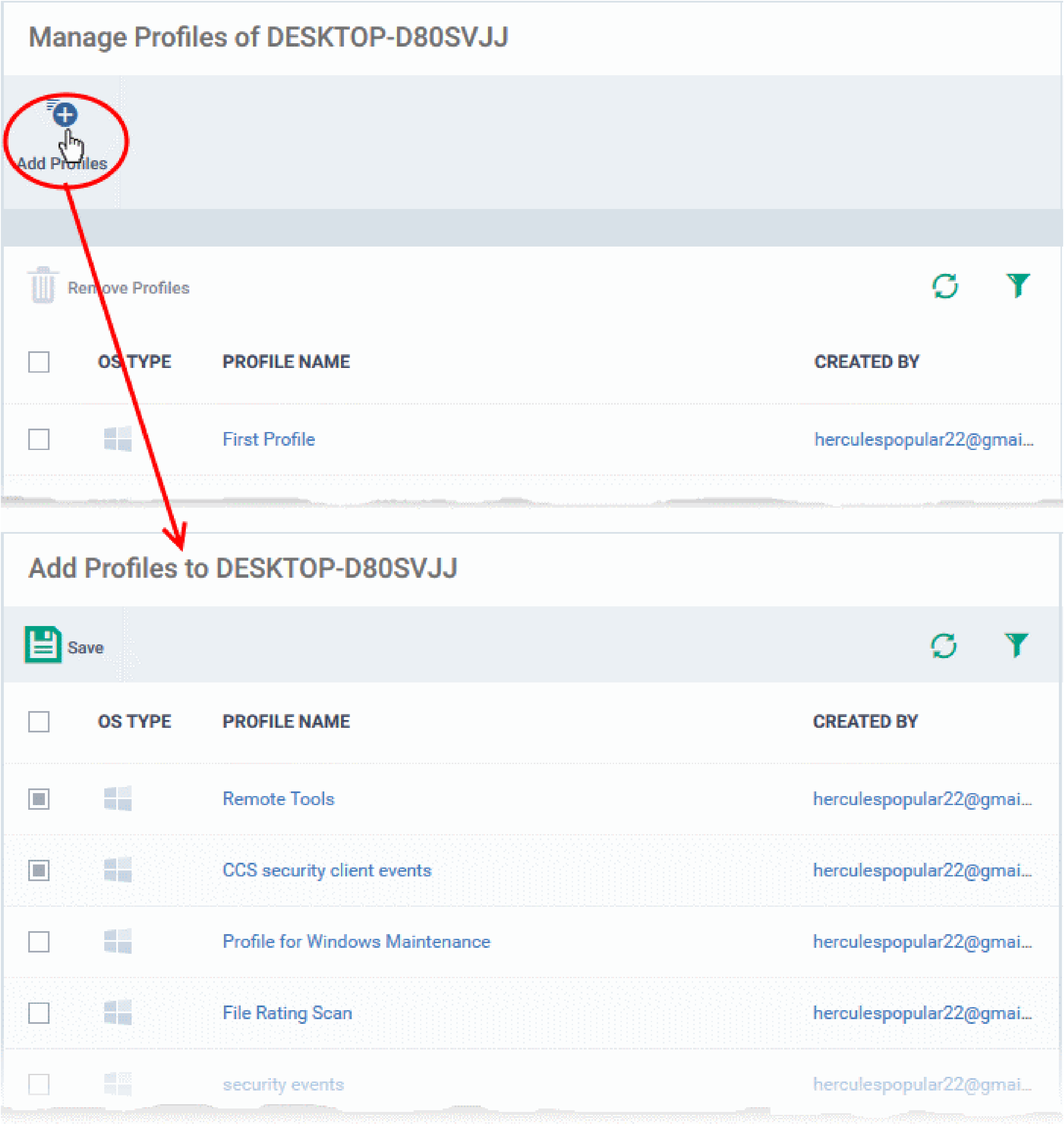
- Alternatively, click the name of the device to be managed to open its 'Device Details' interface and choose 'Manage Profiles' from the options at the top

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

| Manage Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS Type | Indicates the operating system of the device. |
| Profile Name | The profile label.<br>• Click the name of a profile to open the 'Edit Profile' interface.<br>• See **Edit Configuration Profiles** for more details. |
| Created By | The admin who added the profile.<br>• Click the name to open the user information interface of the admin.<br>• See **View User Details** for more details. |

**Note**: Device group and user group profiles applied to the device will not be shown here. Profiles applied to a device through different channels can be viewed from the respective 'Device Details' interface. See **View and Manage Profiles Associated with a Device** for more details.

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



Manage Profiles of DESKTOP-D80SVJJ

| | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | | First Profile | herculespopular22@gmai... |

Add Profiles to DESKTOP-D80SVJJ

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| ☒ | | Remote Tools | herculespopular22@gmai... |
| ☒ | | CCS security client events | herculespopular22@gmai... |
| □ | | Profile for Windows Maintenance | herculespopular22@gmai... |
| □ | | File Rating Scan | herculespopular22@gmai... |
| □ | | security events | herculespopular22@gmai... |

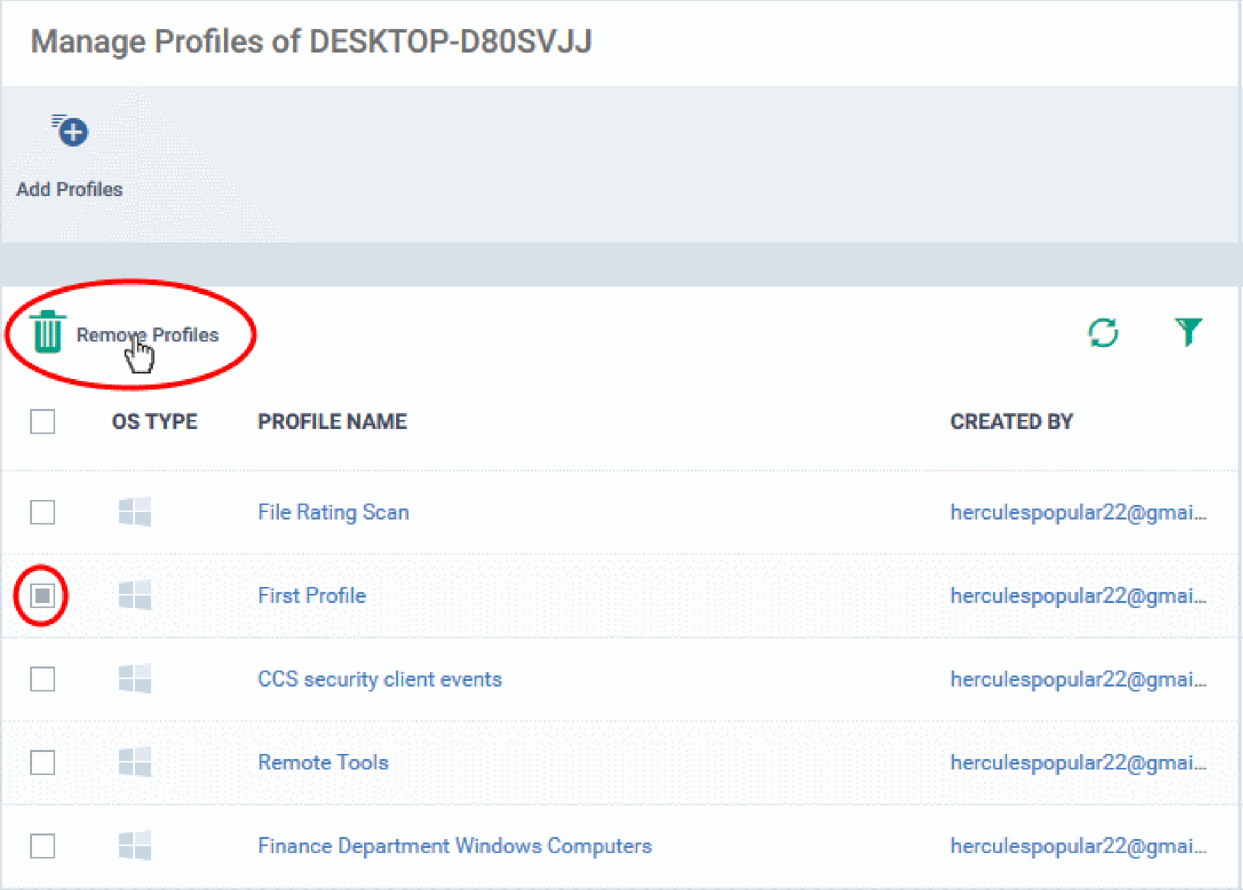
A list of all profiles applicable to the chosen device, excluding those that are already applied to the device is shown.

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

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

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

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



Manage Profiles of DESKTOP-D80SVJJ

| □ | OS TYPE | PROFILE NAME | CREATED BY |
|---|---|---|---|
| □ | ⊞ | File Rating Scan | herculespopular22@gmai... |
| ☒ | ⊞ | First Profile | herculespopular22@gmai... |
| □ | ⊞ | CCS security client events | herculespopular22@gmai... |
| □ | ⊞ | Remote Tools | herculespopular22@gmai... |
| □ | ⊞ | Finance Department Windows Computers | herculespopular22@gmai... |

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

### 5.2.21. Set / Reset Screen Lock Password for Selected Devices

- Endpoint Manager lets you remotely set a new screen lock passcode (or reset the existing code) for enrolled Android devices from the 'Device Management' interface.

**Note**: This feature is available only for Android devices.

The following sections explain more about:

- **Setting and resetting password for a single device**
- **Setting and resetting password for several devices at-once**

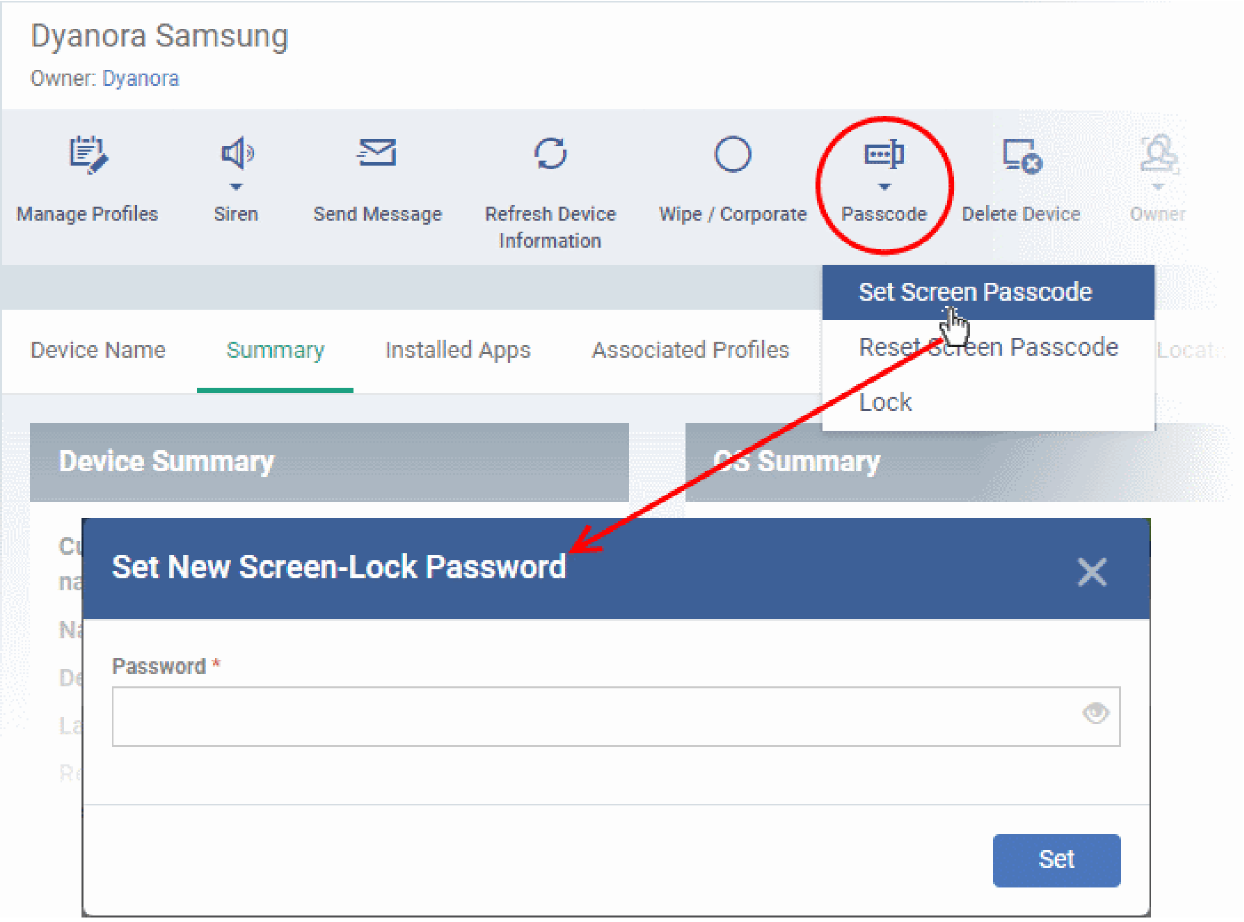
**To set a new screen lock password or remove password for a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of the device for which a new passcode is to be created or existing passcode is to be reset

This opens the 'Device Details' interface for the device.

- To set a new password:
  - Click the 'Passcode' button at the top and choose 'Set Screen Passcode'.
    - If 'Passcode' is not displayed, click 'More...' , select 'Passcode' and choose 'Set Screen Passcode' from the options



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

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

- Click 'Set'.

The command is sent to the device. This new password should be entered on the device to unlock it.

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

- To clear the existing password on the device:
    - Click the 'Passcode' button at the top and choose 'Reset Screen Passcode'.
        - If 'Passcode' is not displayed, click 'More...' , select 'Passcode' and choose 'Reset Screen Passcode' from the options

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

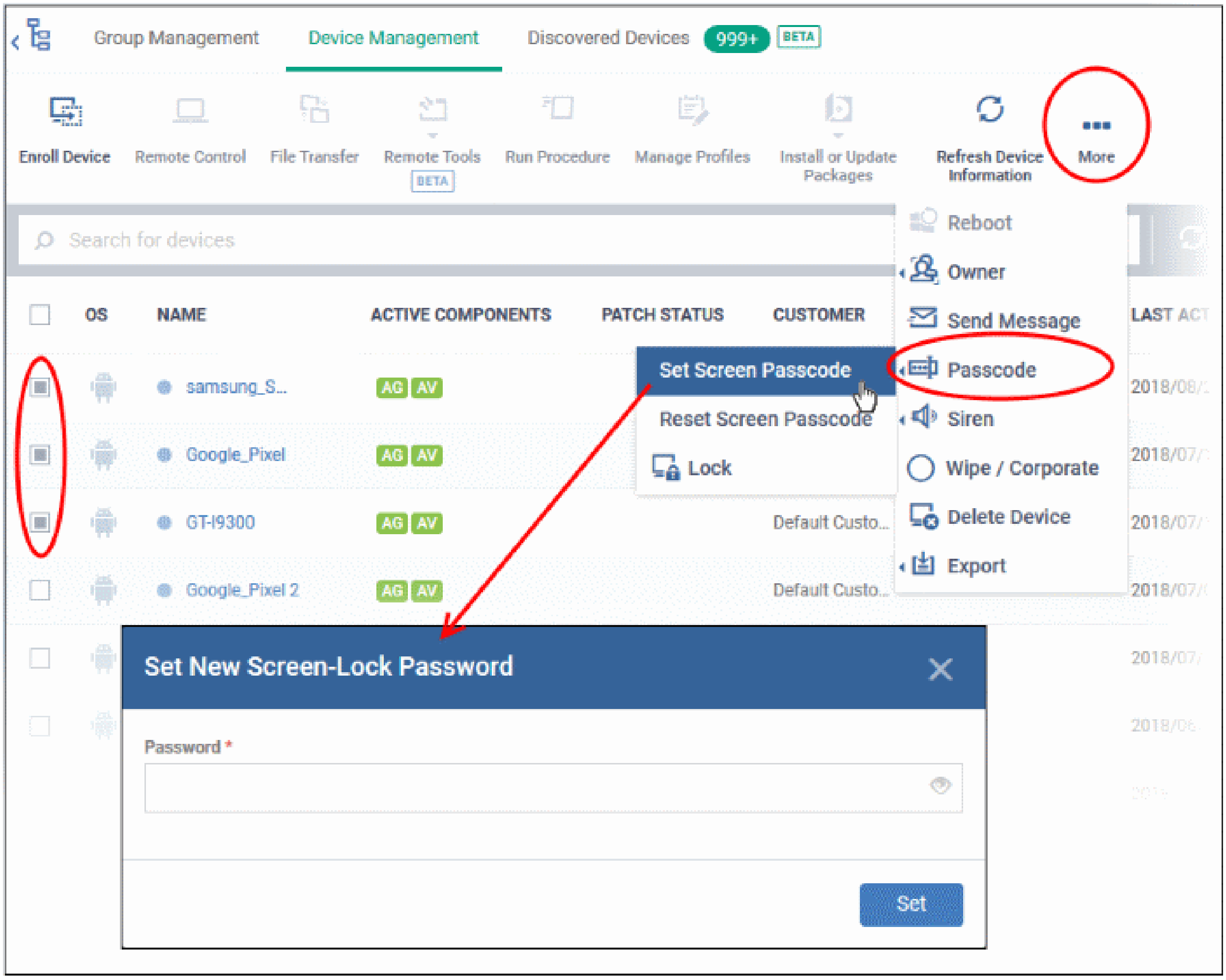
**To set a new screen lock password or remove password for several devices**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

Or

- Select 'Show all' to view every device added to EM

- Select the devices to set/reset their password.
- To set a new password:
  - Click the 'Passcode' button at the top and choose 'Set Screen Passcode'.
    - If 'Passcode' is not displayed, click 'More...' , select 'Passcode' and choose 'Set Screen Passcode' from the options



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

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

- Click 'Set'.

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

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

- To clear the existing passwords:
    - Click the 'Passcode' button at the top and choose 'Reset Screen Passcode'.
        - If 'Passcode' is not displayed, click 'More...' , select 'Passcode' 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.

## 5.2.22. Update Device Information

- The communication client on an enrolled device sends information about the device to Endpoint Manager.
- This includes OS version, memory status, network details, IMEI number, location, MAC address of Bluetooth, MAC address of WiFi and so on.
- The interval at which the device sends this information can be configured in the 'Settings' interface.
- Device information can also be fetched in real time by opening device details then clicking 'Refresh Device Information'.

The following sections explain more about:

- **Getting updated information from a single device**
- **Getting updated information from several devices at once**

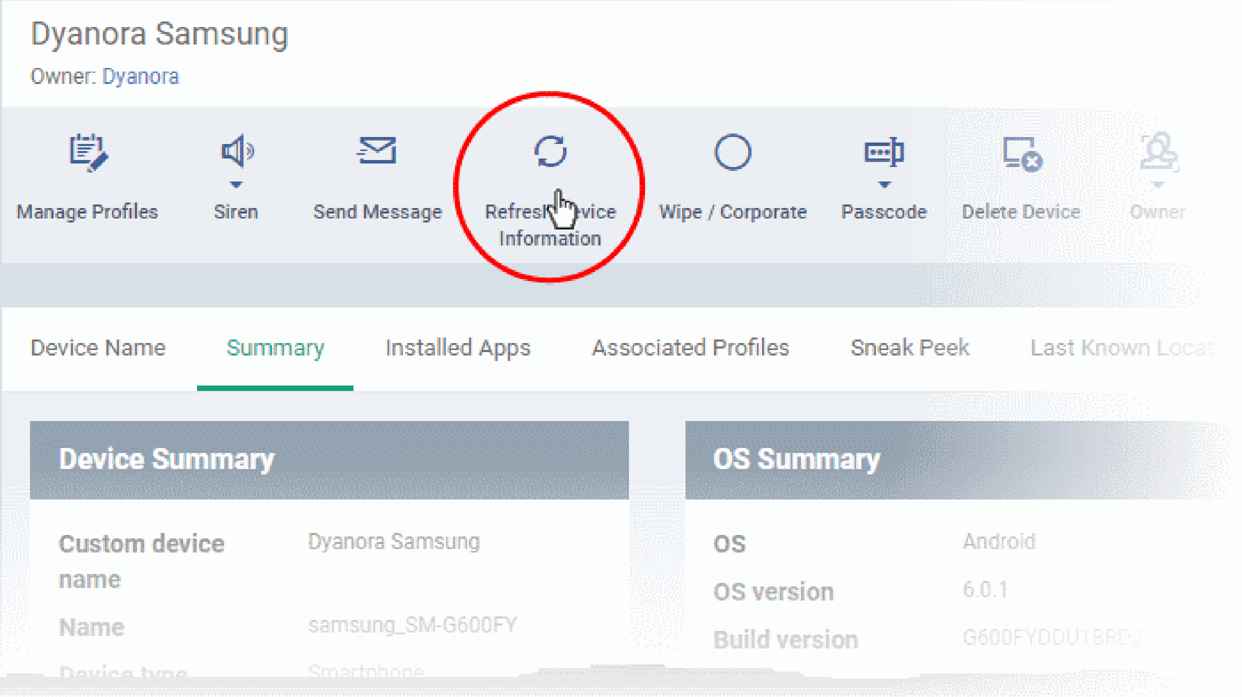
**To get updated information from a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Click the name of the device to refresh the information from

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

- Click 'Refresh Information' from the options at the top


Dyanora Samsung
Owner: Dyanora

**Device Summary**

| | |
|---|---|
| Custom device name | Dyanora Samsung |
| Name | samsung_SM-G600FY |
| Device type | Smartphone |

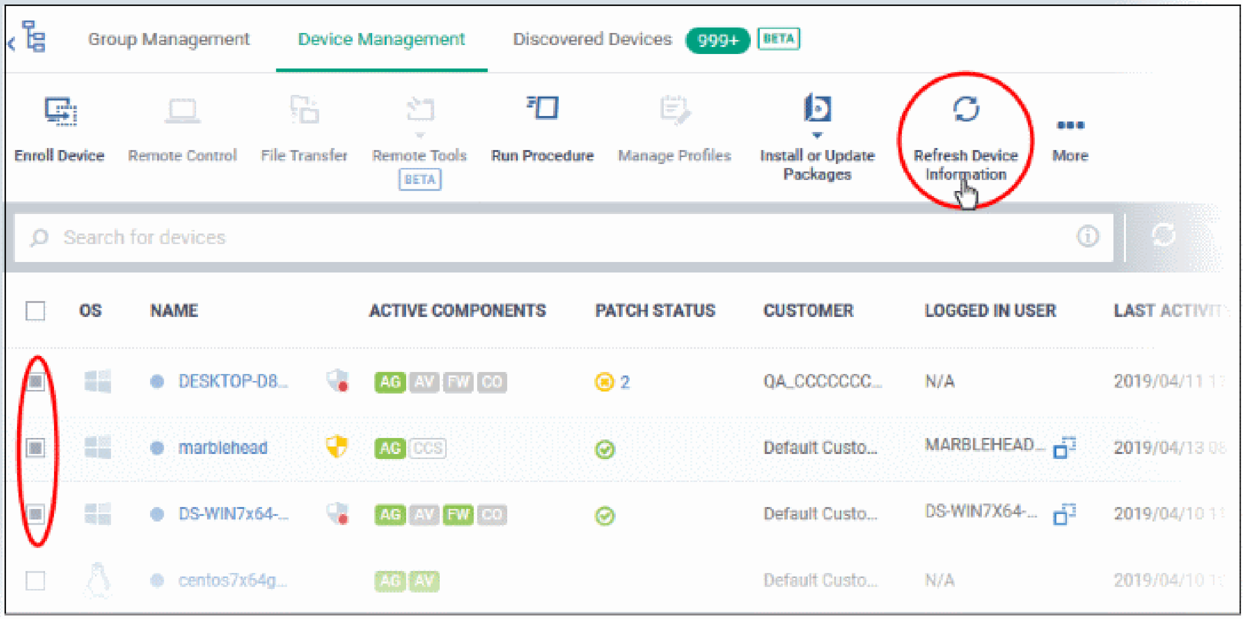
**OS Summary**

| | |
|---|---|
| OS | Android |
| OS version | 6.0.1 |
| Build version | G600FYDDU1SRD2 |

**To get updated information from several devices**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Select the devices to refresh information from.
- Click 'Refresh Device Information' from the options at the top
    - If 'Refresh Device Information' is not displayed, click 'More...' , and choose 'Refresh Device Information' from the options



| | OS | NAME | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LOGGED IN USER | LAST ACTIVIT |
|---|---|---|---|---|---|---|---|
| ■ | | DESKTOP-D8... | AG AV FW CO | 2 | QA_CCCCCCC... | N/A | 2019/04/11 1 |
| ■ | | marblehead | AG CCS | ✓ | Default Custo... | MARBLEHEAD... | 2019/04/13 0 |
| ■ | | DS-WIN7x64-... | AG AV FW CO | ✓ | Default Custo... | DS-WIN7X64-... | 2019/04/10 1 |
| □ | | centos7x64g... | AG AV | | Default Custo... | N/A | 2019/04/10 1 |

## 5.2.23. Send Text Message to Devices

Endpoint Manager lets you send text messages to enrolled Android and iOS devices. This comes in handy if you need to send important notifications to all users.

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

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

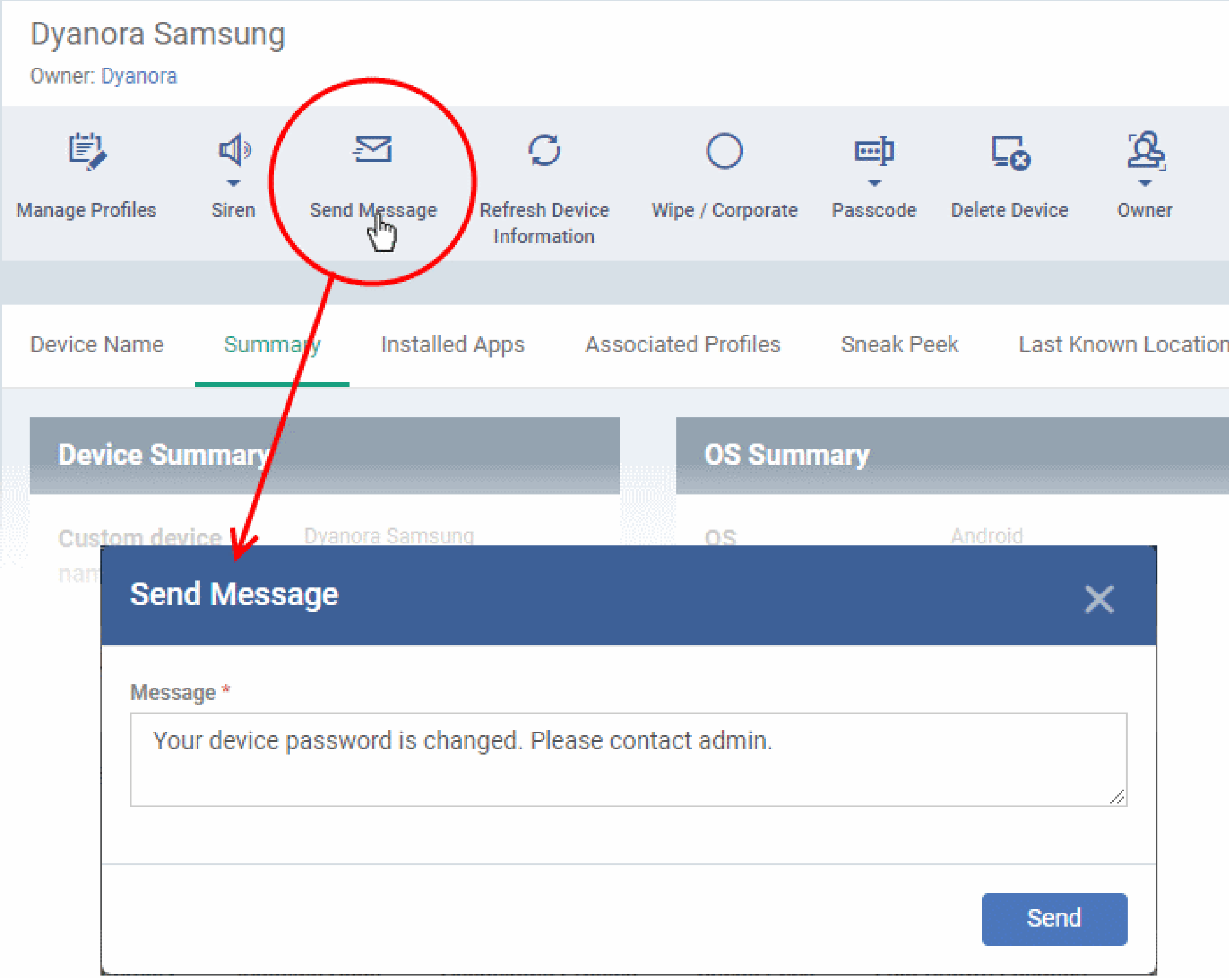
**To send a text message to a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Click the name of the target device to which the message should be sent

The 'Device Details' interface opens.

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



Your device password is changed. Please contact admin.

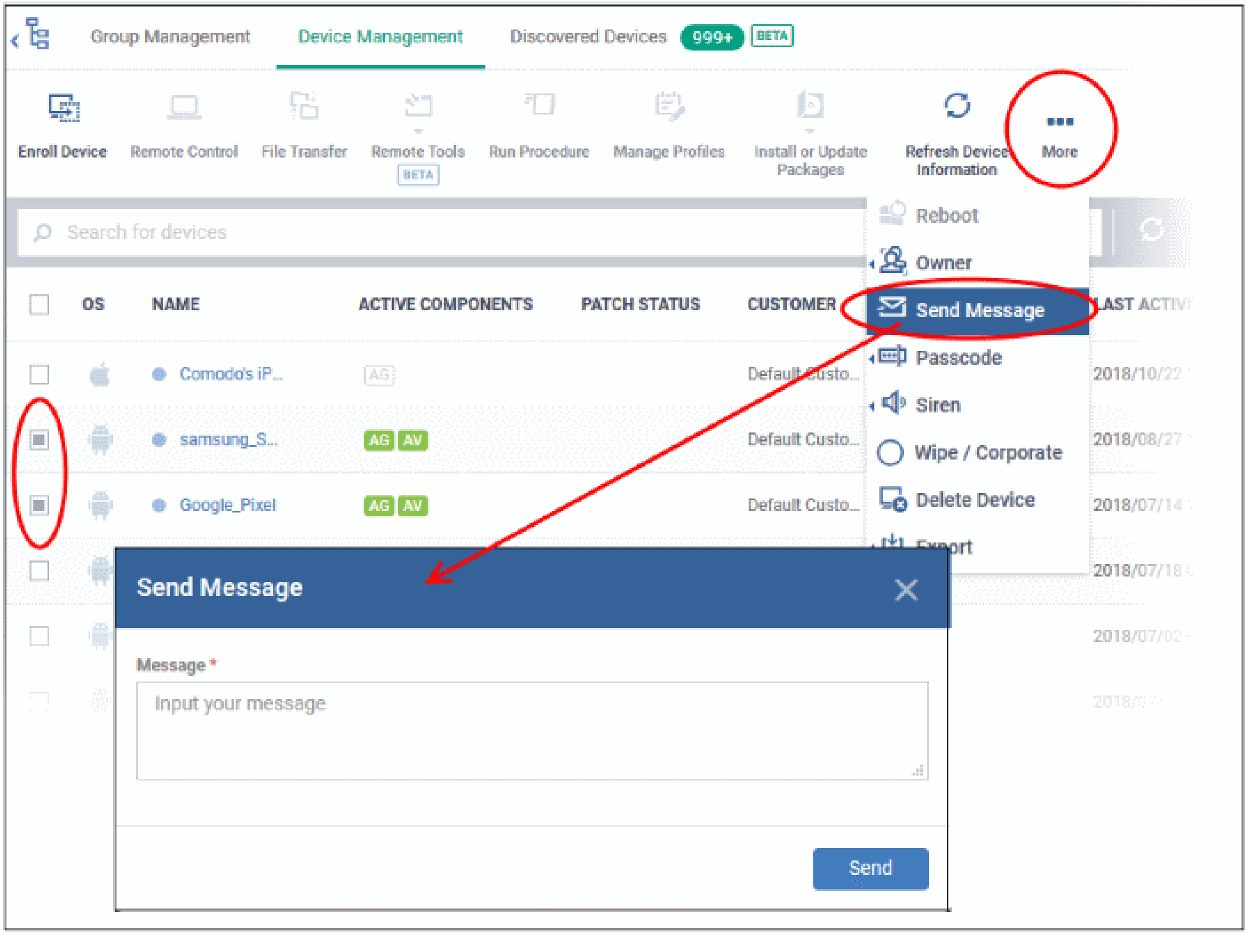
- Enter the text message in the 'Message' field.
- Click the 'Send' button.

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' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Select the target devices to which you wish to send messages
- Click 'Send Message' from the options at the top or click 'More...' and choose 'Send Message' from the drop-down



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

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

## 5.2.24. Restart Selected Windows Devices

Endpoint Manager allows you to remotely restart Windows machines as required. You can also specify how long to delay the restart, add a warning message to be displayed to users and allow them to postpone the restart.

**Note**: The reboot option is only available for Windows devices.

The following sections explain more about:

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

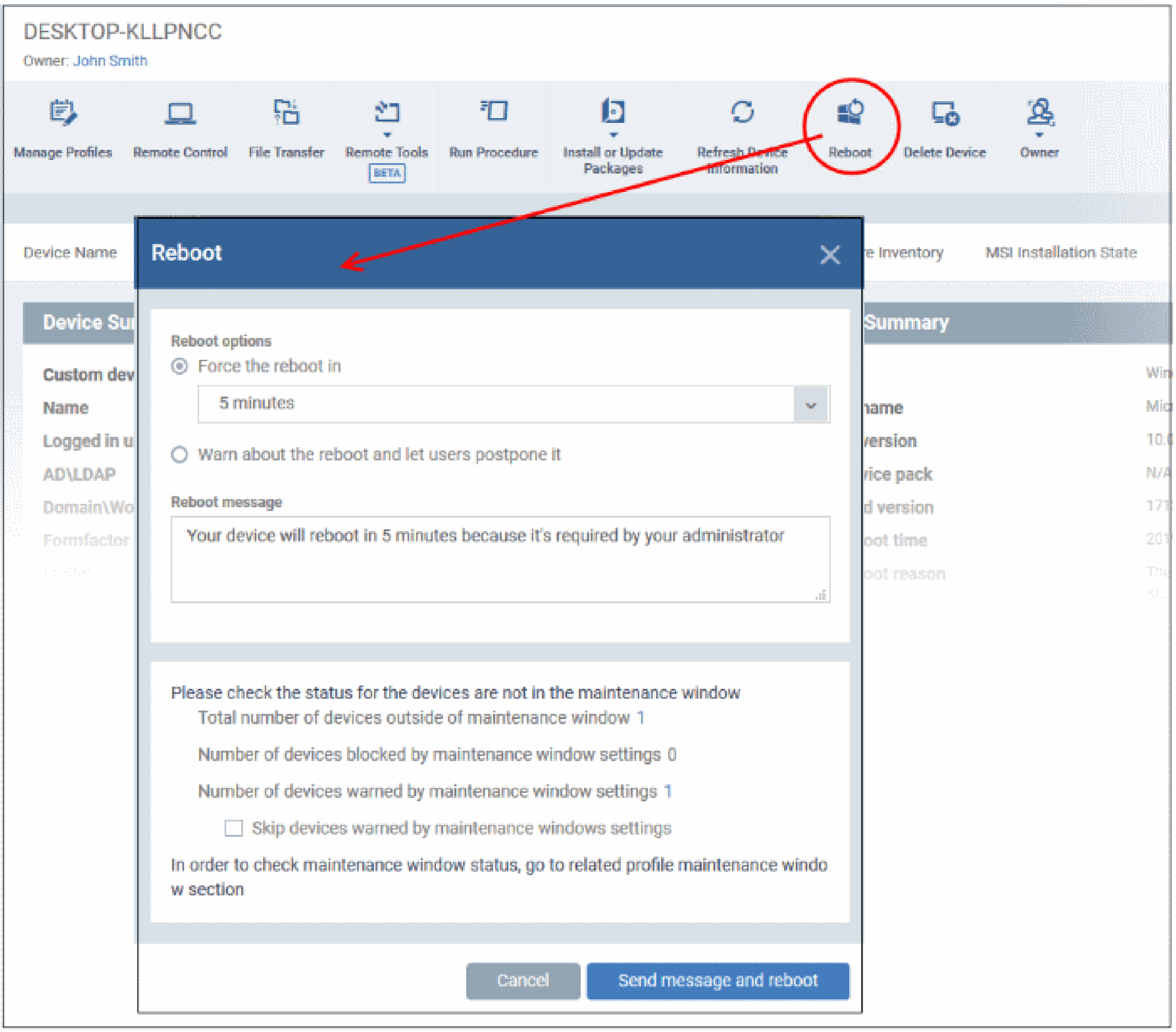
**To restart a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of the Windows device to be restarted

The device details interface opens.

- Click the 'Reboot' option at the top.



Reboot

Reboot options

● Force the reboot in

5 minutes

○ Warn about the reboot and let users postpone it

Reboot message

Your device will reboot in 5 minutes because it's required by your administrator

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 1

Number of devices blocked by maintenance window settings 0

Number of devices warned by maintenance window settings 1

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance windo w section

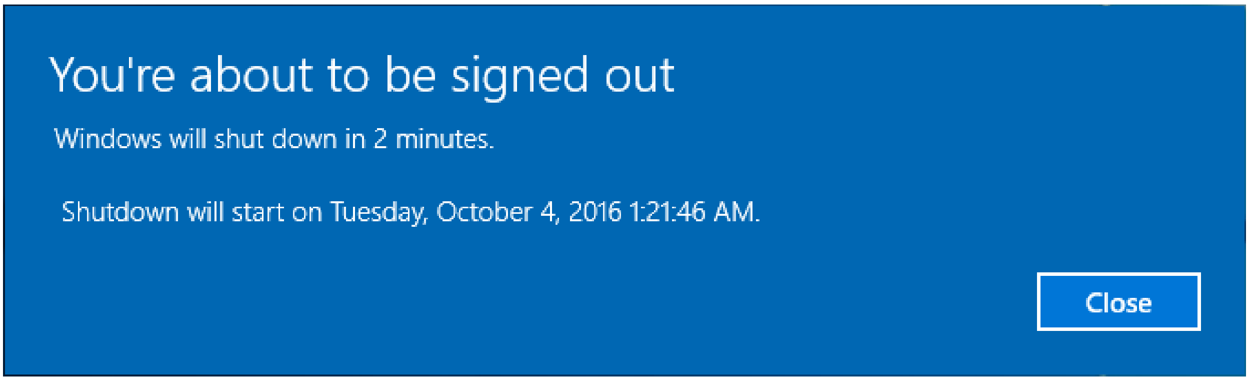
Cancel | Send message and reboot

- Configure your reboot options in the 'Reboot' dialog
- Maintenance window status - Details of any maintenance windows in the device's profile.
  - **Total number of devices outside of maintenance window** - The number of devices that are not part of a maintenance window. The reboot can proceed on these devices.
  - **Number of devices blocked by maintenance windows settings** - The number of devices that you cannot reboot because the admin has blocked reboots outside of the maintenance window.
  - **Number of devices warned by maintenance window settings** - The number of devices that are part of a maintenance window and have warnings enabled. You can still reboot these devices.
    - **Skip devices warned by maintenance windows settings** - A maintenance window is a time-slot reserved for running important tasks on target devices. Admins can enable a warning if somebody attempts to reboot outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.

**Restart the end-point after a certain period of time**

- Choose 'Force the reboot in' and select the delay period.
- Click 'Send message and reboot'

The message will be displayed at the device as shown below:



You're about to be signed out

Windows will shut down in 2 minutes.

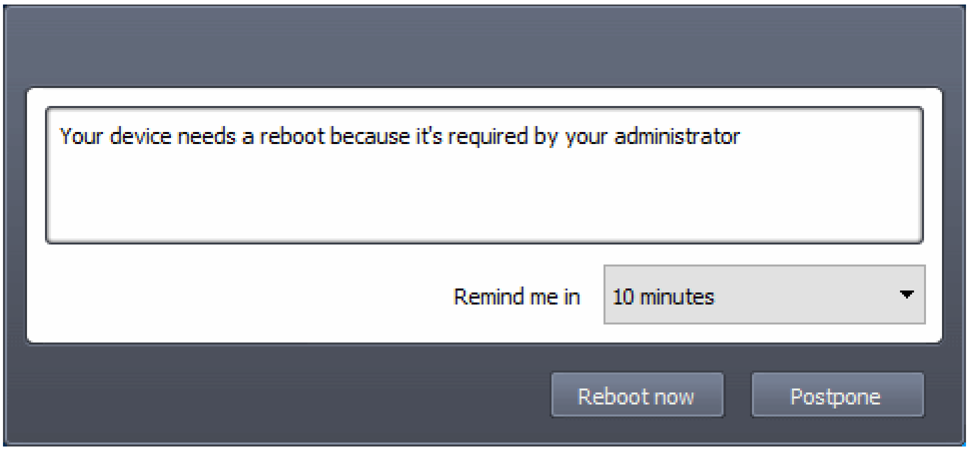
Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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

**Restart the end-point at user's convenience**

- Choose 'Warn about the reboot and let users postpone it.
- Enter the message to be displayed to the user in the 'Reboot message' field.
- Click 'Send message and reboot'

The message will be displayed at the device as shown below:



Your device needs a reboot because it's required by your administrator

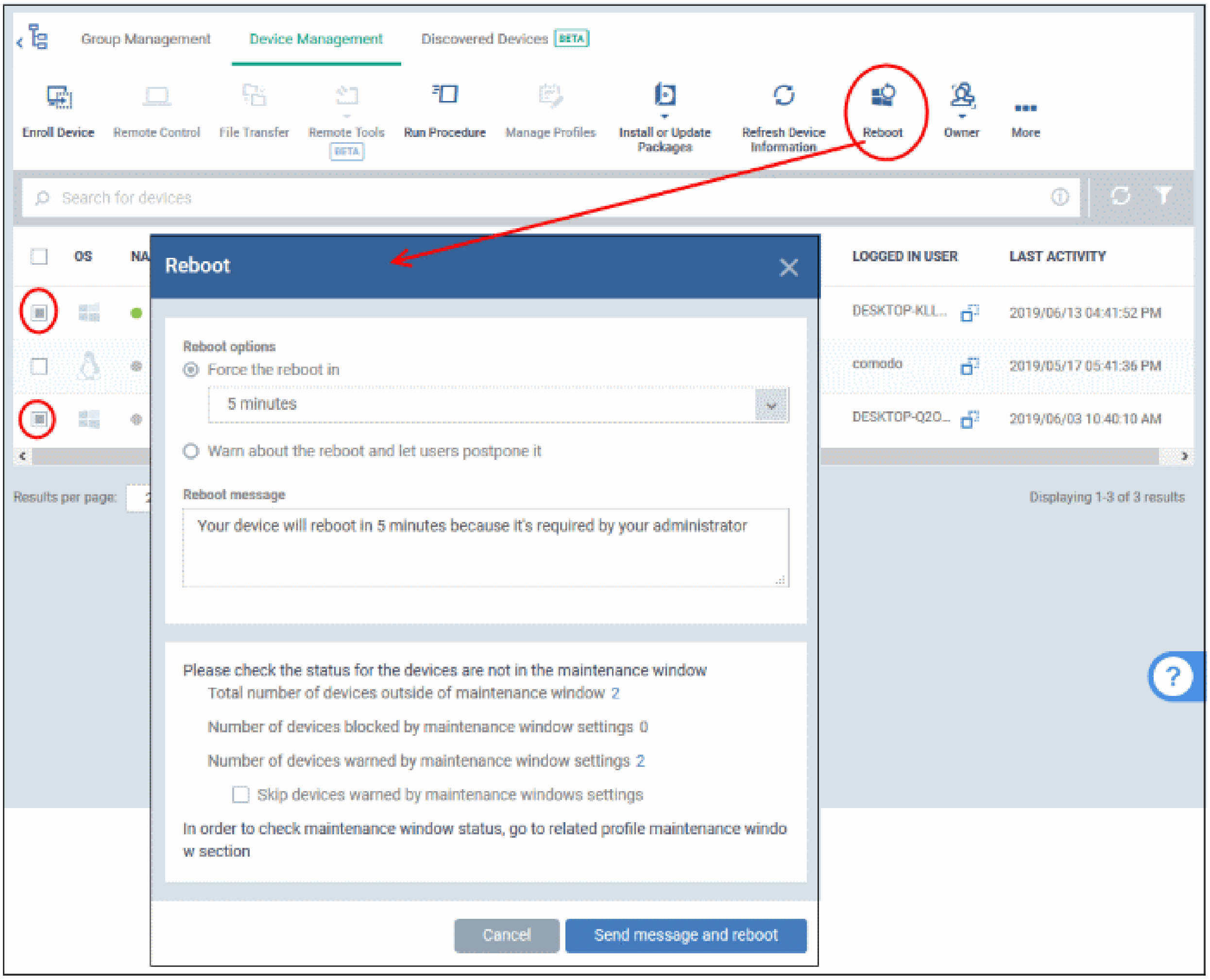
Remind me in 10 minutes

- The user can choose to restart the endpoint immediately by clicking 'Reboot now' or postpone the restart operation by selecting the period from the 'Remind me in' drop-down and clicking 'Postpone'.

**To restart several devices at once**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Select the target Windows devices to be restarted
- Click 'Reboot' from the options at the top or click 'More' and choose 'Reboot' from the options



| LOGGED IN USER | LAST ACTIVITY |
|---|---|
| DESKTOP-KLL... | 2019/06/13 04:41:52 PM |
| comodo | 2019/05/17 05:41:36 PM |
| DESKTOP-Q2O... | 2019/06/03 10:40:10 AM |

Reboot

Reboot options

● Force the reboot in

5 minutes

○ Warn about the reboot and let users postpone it

Reboot message

Your device will reboot in 5 minutes because it's required by your administrator

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 2

Number of devices blocked by maintenance window settings 0

Number of devices warned by maintenance window settings 2

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance windo w section

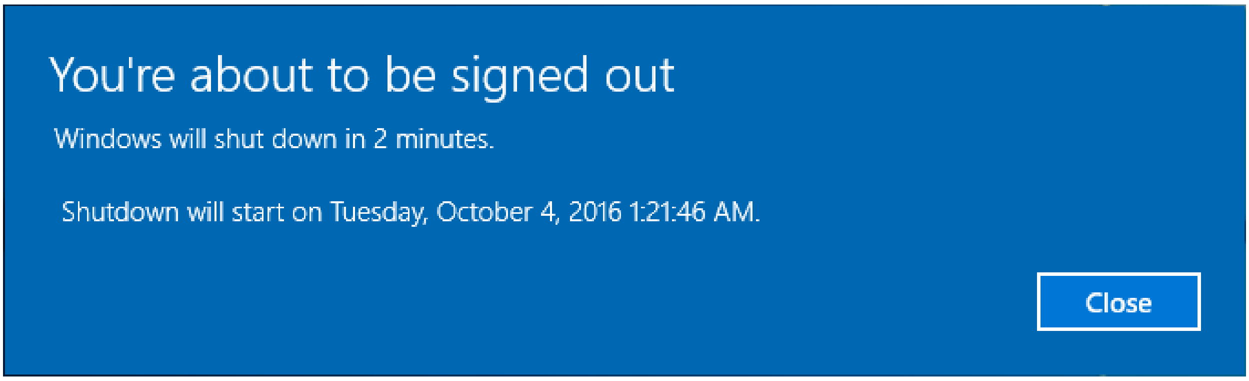
Cancel | Send message and reboot

- Configure your reboot options in the 'Reboot' dialog
- **Maintenance window status -** Details of any maintenance windows in the device's profile.
  - **Total number of devices outside of maintenance window -** The number of devices that are not part of a maintenance window. The reboot can proceed on these devices.
  - **Number of devices blocked by maintenance windows settings -** The number of devices that you cannot reboot because the admin has blocked reboots outside of the maintenance window.
  - **Number of devices warned by maintenance window settings -** The number of devices that are part of a maintenance window and have warnings enabled. You can still reboot these devices.
    - **Skip devices warned by maintenance windows settings -** A maintenance window is a time-slot reserved for running important tasks on target devices. Admins can enable a warning if somebody attempts to reboot outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.

**Restart the end-points after a certain period of time**

- Choose 'Force the reboot in' and select the delay period.
- Click 'Send message and reboot'

The message will be displayed at the device as shown below:



You're about to be signed out

Windows will shut down in 2 minutes.

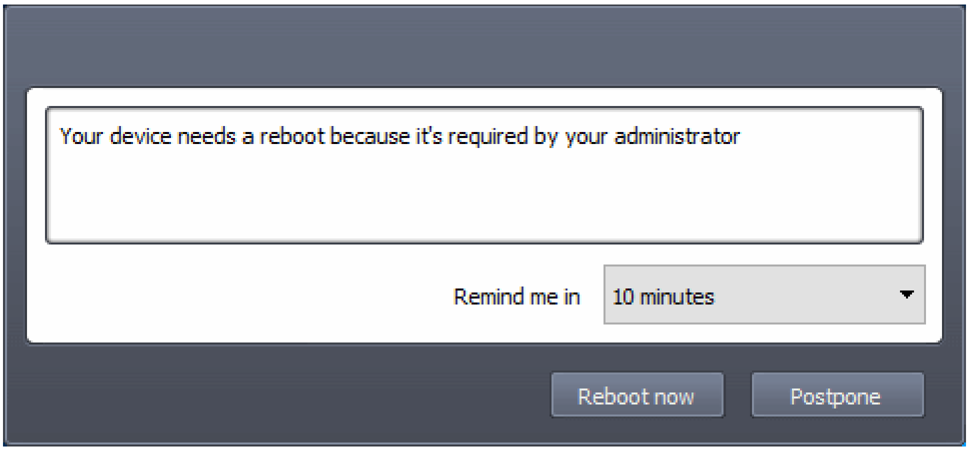
Shutdown will start on Tuesday, October 4, 2016 1:21:46 AM.

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

**Restart the end-point at user's convenience**

- Choose 'Warn about the reboot and let users postpone it'.
- Enter the message to be displayed to the users in the 'Reboot message' field.
- Click 'Send message and reboot'

The message will be displayed at the devices as shown below:



Your device needs a reboot because it's required by your administrator

Remind me in: 10 minutes

- Users can choose to restart their endpoints immediately by clicking 'Reboot now'. They can delay the restart by selecting a time-period from the 'Remind me in...' drop-down and clicking 'Postpone'.

## 5.2.25. Change a Device's Owner

Endpoint Manager allows you to assign device ownership from one user to another user.

- **Change ownership of a single device**
- **Assign multiple devices to single owner at-once**

**To change the device ownership of a single device**

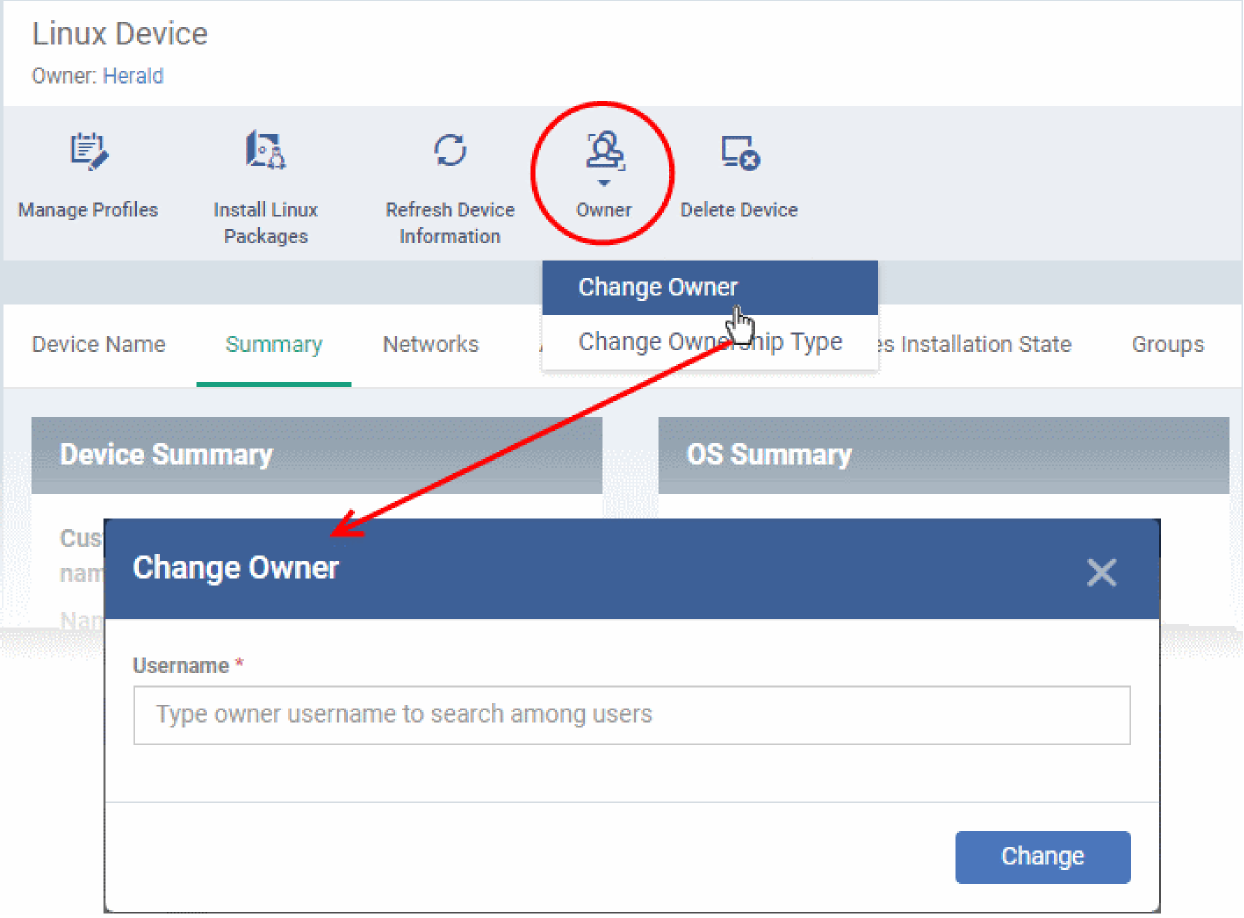
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of the device whose ownership is to be changed

The 'Device Details' interface opens.

- Click 'Owner' from the options at the top or click 'More' and choose 'Owner' from the drop-down
- Select 'Change Owner' from the options

- Start typing the first few characters of the name of the new user to whom the device is to be assigned and choose the user from the options
- Click 'Change'



The ownership of the device will be changed to the new user. The configuration profiles in effect on the device, associated with the previous user and the user group to which the previous user is a member, will be removed and the profiles, pertaining to the new user and the user group to which the new user is a member, will be applied to the device.

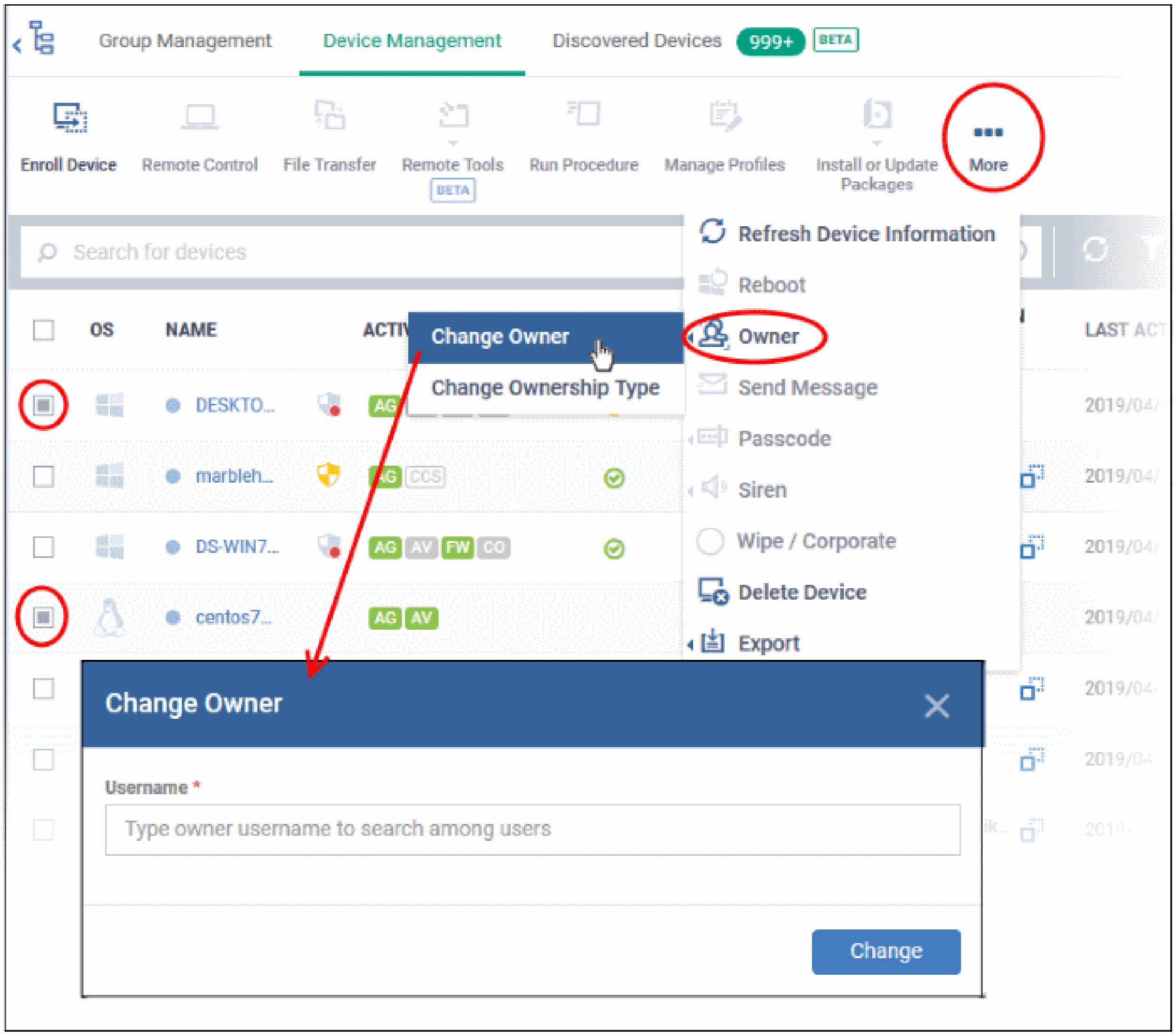
**To assign several devices to a user at-once**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
    - Select a company or group on the left to view only their devices

      Or
    - Select 'Show all' to view every device added to EM
- Select the target devices to be associated with a new user

**Tip**: You can change devices pertaining to different users to be assigned to a single new user.

- Click 'Owner' from the options at the top or click 'More' and choose 'Owner' from the drop-down
- Select 'Change Owner' from the options



- Start typing the first few characters of the name of the new user to whom the device is to be assigned and choose the user from the options
- Click 'Change'

All selected devices will be assigned to the new user. The configuration profiles in effect on the device, associated with the previous users and the user groups to which the previous users are members, will be removed and the profiles, pertaining to the new user and the user group to which the new user is a member, will be applied to the device.

## 5.2.26. Change the Ownership Status of a Device

- Admins can set the ownership status of a device depending on whether it belongs to a user or to the company.
- There are three ownership types - 'Personal', 'Corporate' and 'Not Specified'. The ownership type is listed in the 'Summary' tab of the device configuration area.
- By default, any new device enrolled to Endpoint Manager will have an ownership status of 'Not Specified'.
- Ownership types do not have any impact on device security policy or how the device is treated by EM. It is a just a descriptive label which allows admins to more easily identify and group devices.

The following sections explain more about:

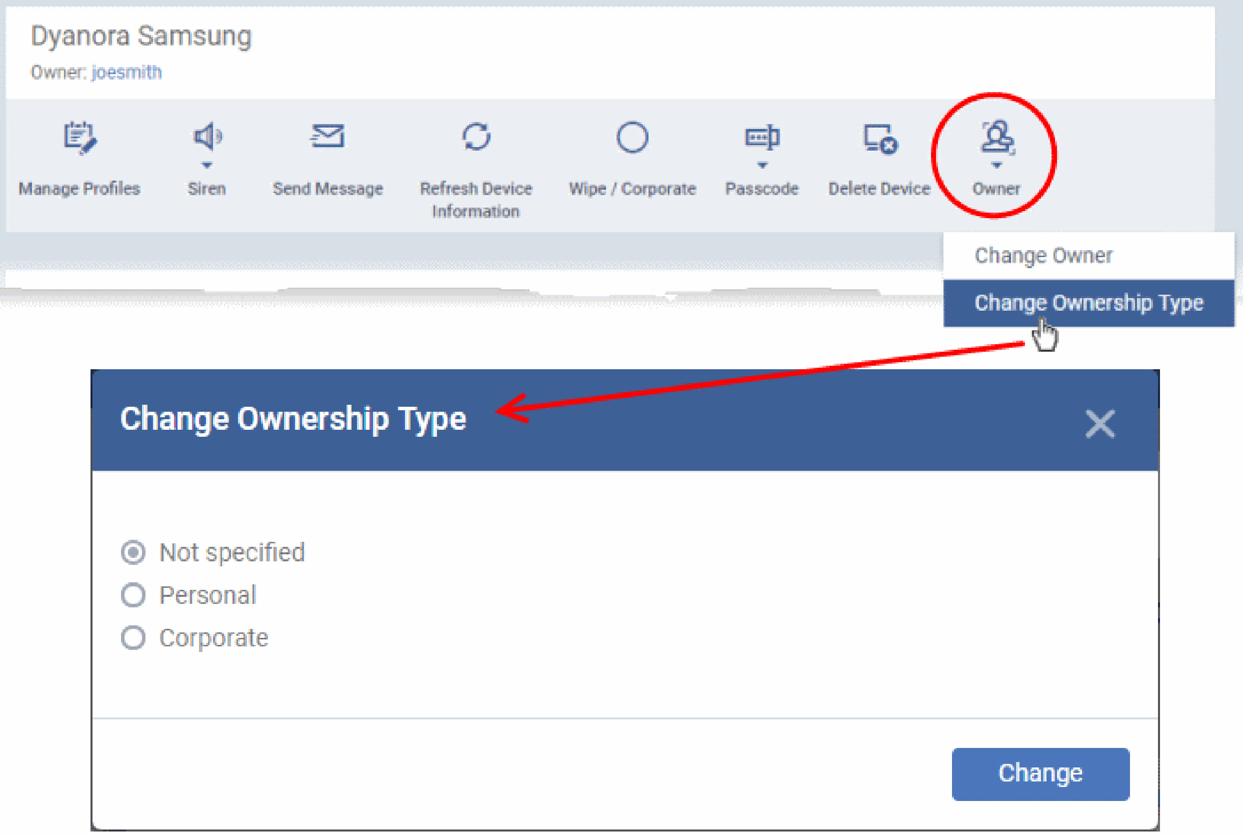
- **Changing ownership status of a single device**
- **Changing ownership status of several devices at-once**

**To set the ownership status of a single device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Click the name of the target device whose ownership status you wish to change.

The device details interface opens.



● Not specified
○ Personal
○ Corporate

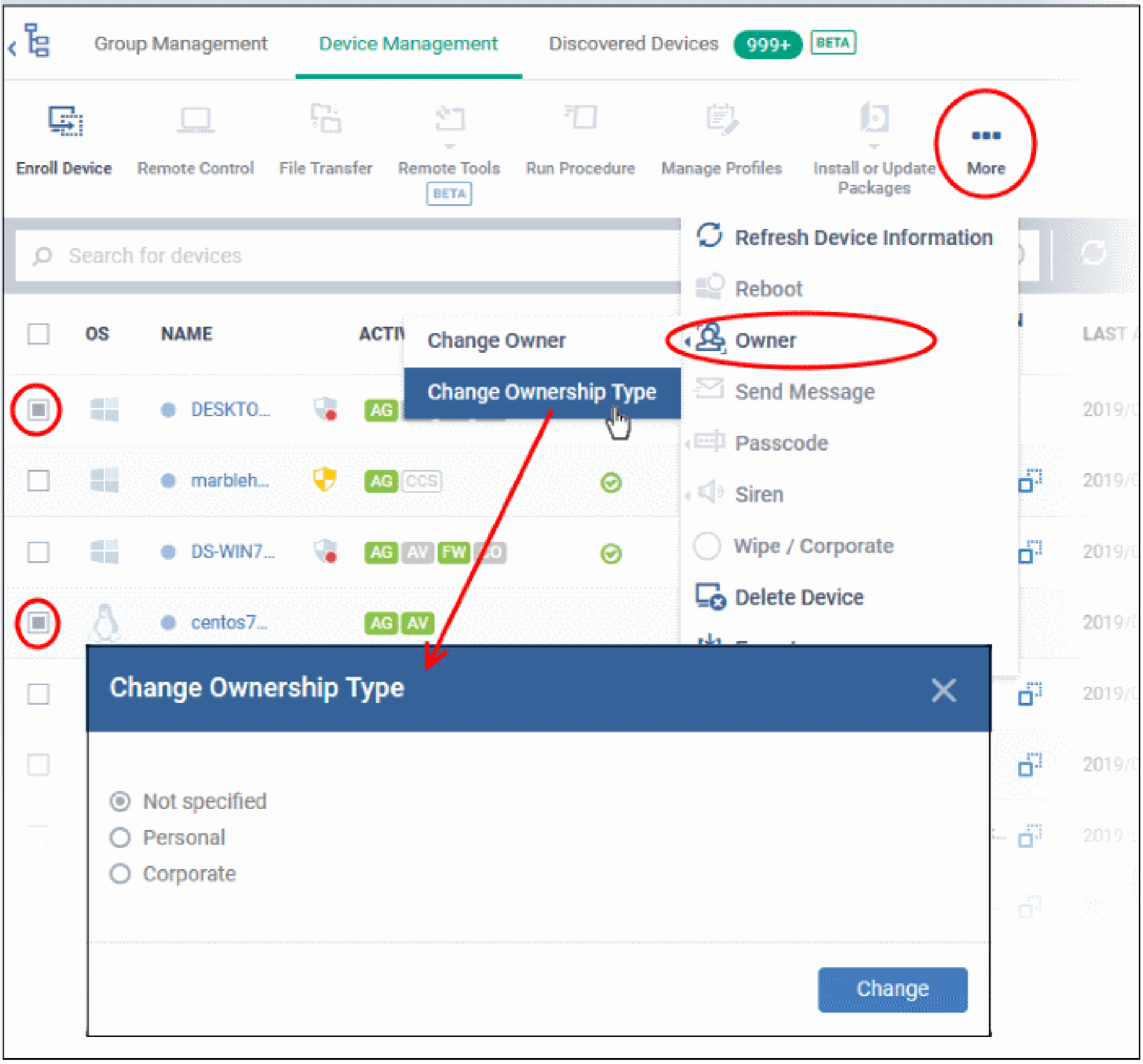
- Click 'Owner' from the options at the top or click 'More' and choose 'Owner' from the drop-down
- Select 'Change Ownership Type' from the options
- Choose the ownership type from the following options:
  - Personal
  - Corporate
  - Not Specified
- Click 'Change'.

**To set the ownership status of several devices at-once**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab above the control buttons
  - Select a company or group on the left to view only their devices

    Or
  - Select 'Show all' to view every device added to EM
- Select the devices whose ownership status you wish to change.

- Click 'Owner' from the options at the top or click 'More...' and choose 'Owner' from the drop-down
- Select 'Change Ownership Type' from the options



Change Ownership Type

● Not specified
○ Personal
○ Corporate

Change

- Choose the ownership type to be assigned to the selected devices and click 'Change'. The available options are:
  - Personal
  - Corporate
  - Not Specified

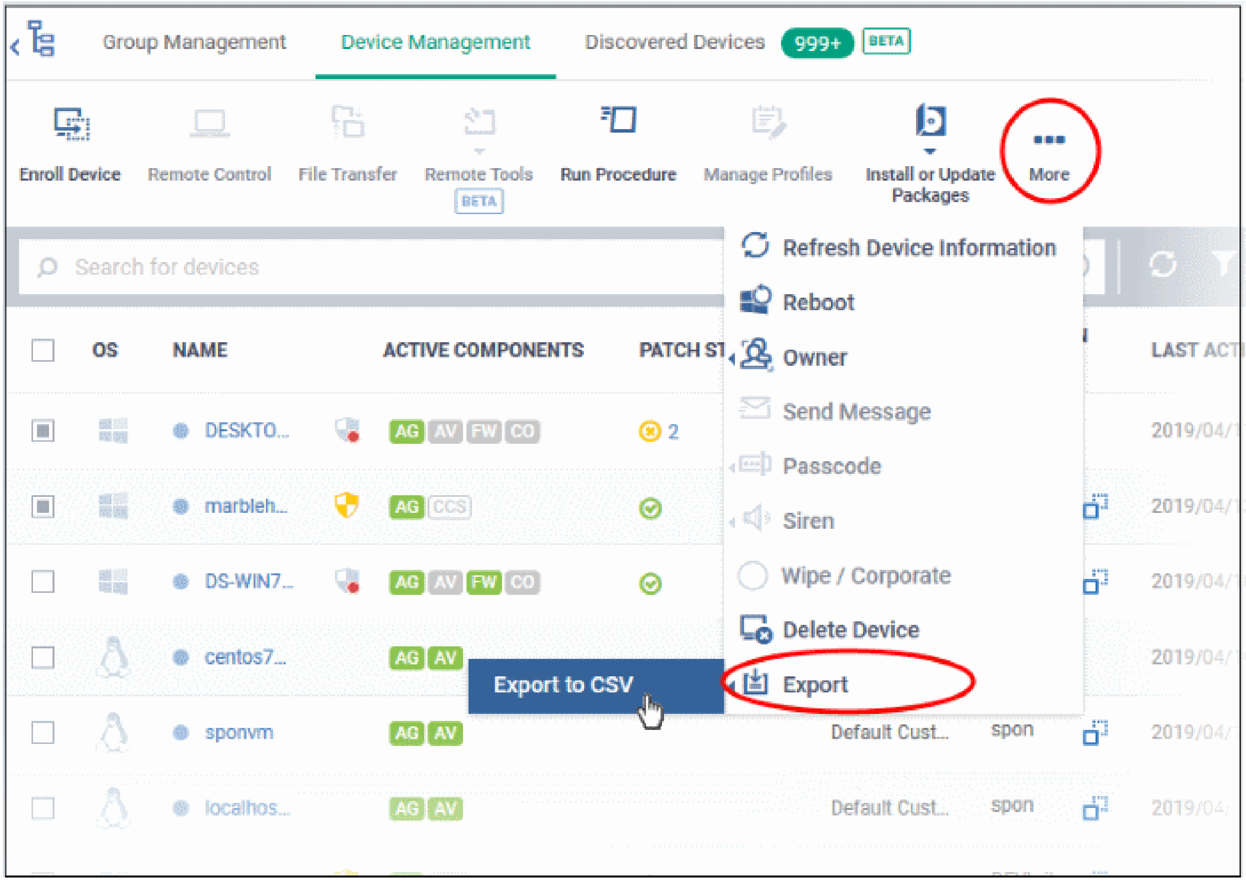
## 5.2.27. Generate Device List Report

- You can create a report on all managed devices listed in the 'Device Management' table.
- The report contains operating system details, hardware details, last activity, CCS configuration, resource usage and more for each device.

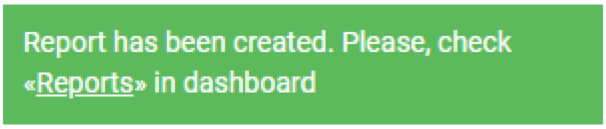
**Generate device list report**

- Click 'Devices' > 'Device List' > 'Device Management'
- Apply any filters that you require.

- Click 'Export' > 'Export to CSV' or click 'More' > 'Export' > 'Export to CSV':



A confirmation message is shown:


Report has been created. Please, check «Reports» in dashboard

See 'Reports' in 'Dashboard' for more information on how to view and download reports.

## 5.3. Bulk Enrollment of Devices

### Windows, MAC and Linux

- Click 'Devices' > 'Bulk Installation Package' > 'Bulk Installation Package' tab.

The bulk installation area lets you download the communication client package. You need to install this client on target devices to enroll them to Endpoint Manager.

After downloading the installation package, you can deploy it to target devices using any of the following methods:

**Windows**

- **Active Directory group policy object (GPO)**
- **Auto Discovery and Deployment Tool (ADDT)**
- **Manual installation**

**Mac OS and Linux:**

- **Manual installation**

**Android and iOS:**

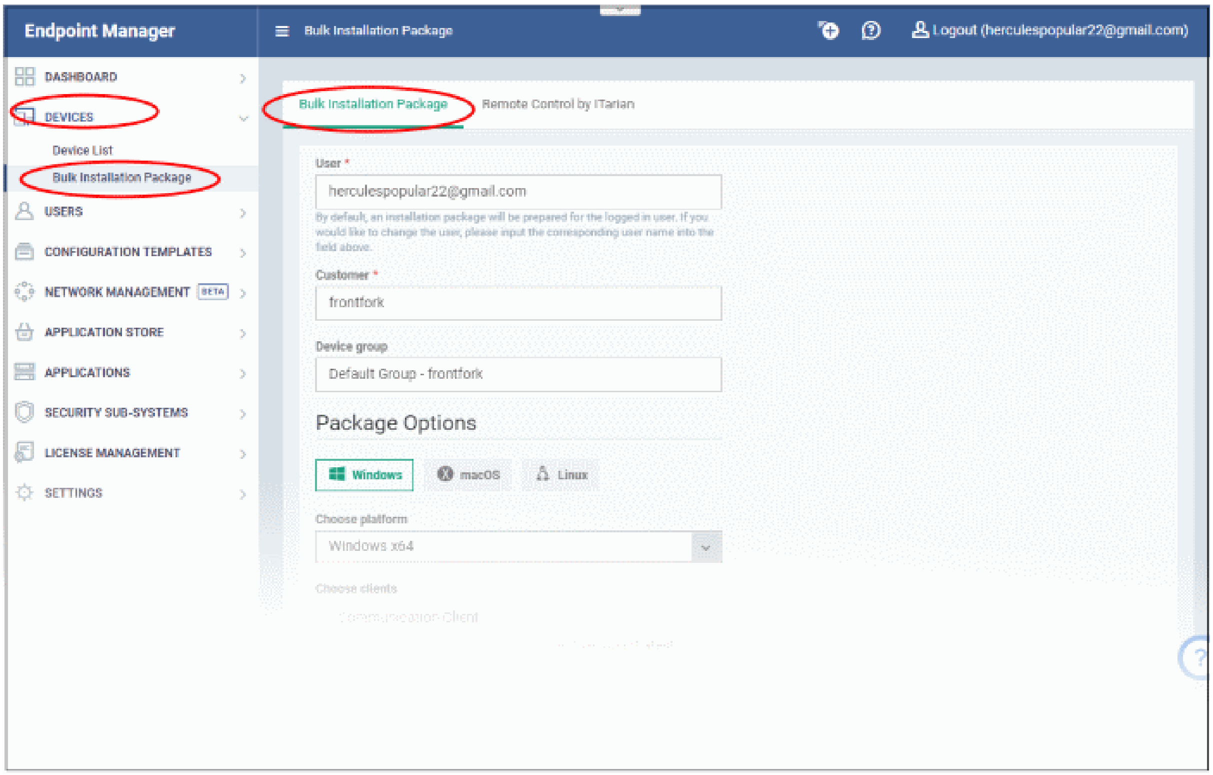
You can bulk enroll iOS and Android devices belonging to users that were imported from Active Directory.

- See **Import User Groups from LDAP** for help to import users from AD.
- After importing users, Android devices can be enrolled by installing the agent. iOS devices can be enrolled by deploying a configuration profile.
- See **Enroll Android and iOS Devices of AD Users** for help with this.

## 5.3.1. Enroll Windows, Mac OS and Linux Devices by Installing the Communication Client

You need to install the communication client on Windows, Mac OS and Linux devices to enroll them to endpoint manager.

- Click 'Devices' > 'Bulk Installation Package' > 'Bulk Installation Package' tab



User * herculespopular22@gmail.com

By default, an installation package will be prepared for the logged in user. If you would like to change the user, please input the corresponding user name into the field above.

Customer * frontfork

Device group Default Group - frontfork

Choose platform Windows x64

- Select the 'Bulk Installation Package' tab.

See the following sections for more details:

- **Enrollment of Windows Devices Via AD Group Policy**.
- **Enrollment of Windows, Mac OS and Linux Devices by Offline Installation of Agent**
- **Enrollment of Windows Devices using Auto Discovery and Deployment**

### 5.3.1.1. Enroll Windows Devices Via AD Group Policy

- You can enroll devices in bulk by creating an Active Directory (AD) group policy
- You need to download the communication client package and, if required, the transformed MST file. You then need to add these items to the GPO.
    - The MST file includes information about the proxy that the client should use to connect to Endpoint Manager and other Comodo servers.
    - By default, all devices enrolled via AD are assigned to the currently logged-in admin. You can change the person to whom the devices are assigned during the package download process.
    - After enrollment, you can assign devices to their correct owners in the 'Devices' interface. See **Change a Device's Owner** for help.

**Download the installation package**

- Click 'Devices' > 'Bulk Installation Package'
- Select the 'Bulk Installation Package' tab
- Create your custom installer by completing the form. Scroll down for **a table that explains the form fields.**
- **Download Installer -** Download the setup file for installation via Group Policy Object (GPO),
    - The installer package is created in .msi format. You can transfer the file to the required network location and create a software installation policy for deployment to your endpoints. Once the agent is installed, it establishes communication with the EM server and begins importing devices.
- **Download MST File** - Download an installer that includes proxy server information for client communication with Endpoint Manager.
    - As above, save the file on the AD server from where you want to enroll the endpoints, and add to the GPO created for the .msi file. After the agent is installed, it will establish communications with EM via the proxy servers and begin importing devices.
- For help to create a GPO for bulk enrollment, see **https://help.comodo.com/topic-399-1-856-11229-EM---Bulk-Enrollment-via-Active-Directory.html**.
- Imported devices inherit the configuration profile of the device owner. The configuration profile of the device user is automatically applied to the device.

| Bulk Installation Package - Form Parameters | |
|---|---|
| **Parameter** | **Description** |
| User | Devices enrolled by AD GPO are assigned to the currently logged-in admin by default.<br>Specify a different user if required.<br>• Start typing the name of a user and choose from the suggestions that appear. |
| Customer | Choose the company to which the endpoints should be assigned.<br>• This field only applies to CD MSP and C1 MSP customers. It does not apply to CD Enterprise, C1 Enterprise, or EM stand-alone customers. |
| Device Group | The device group to which the enrolled devices should be added (optional).<br>Any group profiles will also be applied to the devices you add.<br>See **Assign Configuration Profiles to a Device Group** if you want more help with this. |
| Package Options | **Operating system -** Select Window OS version (64 bit, 32 bit or hybrid package)<br>**Clients**:<br>• **Communication Client (CC) -** Mandatory. This client enrolls the endpoint.<br>• **Comodo Client Security (CCS) -** Optional. This client installs security software such as antivirus, firewall and auto-containment.<br>• Note - The option to choose CC and CCS versions is only available if enabled in **portal settings**. If the option is not enabled, then the 'Default version' is deployed.<br>If CCS is selected, you can also configure the following:<br>**Additional Options**:<br>• **Database -** Choose whether to include the latest virus database with the installation package. This increases file size. If disabled, the client will download the latest database anyway when you run the first scan.<br>• **Profile -** Default is 'Windows - Security Level 1' profile. Choose a different profile if required.<br>• Type the first few characters of a profile and choose from the suggestions that appear. |
| Restart Control Options | CCS only. Endpoints need to be restarted to complete CCS installation. You have the following restart options:<br>• **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message will be shown to the user prior to the restart.<br>• **Suppress reboot -** Endpoint is not auto-restarted. The installation will be finalized when the user next restarts the endpoint.<br>• **Warn about reboot and let users postpone it -** Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.<br>Optional. Type a custom message in the 'Reboot Message' field. |
| UI Options | Configure which messages are shown to the user regarding the installation.<br>• **Show error messages if installation failed -** Notifies the user if the installation is not successful. |

| | |
|---|---|
| | • **Show a confirmation message upon completion of installation -** Notifies the user if the installation is successful. Type your message in the box provided. |
| Proxy Settings | Specify a proxy server through which the clients should connect to Endpoint Manager and other Comodo servers. If you do not set a proxy then the clients will connect directly as per network settings.<br>• Enter the IP address/hostname of the proxy server and port in the respective fields.<br>• Enter the user-name and password of an administrative account on the proxy server in the Proxy Login and Proxy Password fields<br>Note: If you specify a proxy here then you must also configure the same proxy settings in the profile on the device:<br>• Click 'Configuration Templates' > 'Profiles' > *open the device profile* > 'Add Profile Section' > 'Clients Proxy' |

**Tip**: For more help on using GPO for remote installation of software, please see **https://support.microsoft.com/en-us/kb/816102**.

### 5.3.1.2. Enroll Windows, Mac OS and Linux Devices by Offline Installation of Agent

- Click 'Devices' > 'Bulk Installation Package' > 'Bulk Installation Package'
- You can download a custom Windows, MAC or Linux installer for offline installation of the client.
- You can specify the user to whom the enrolled device is assigned, and the initial configuration profile applied to the device.
- You must already have added the user of the device to EM. You can only create installation packages for existing users.

**Download the installation package**

- Click 'Devices' > 'Bulk Installation Package'
- Select the 'Bulk Installation Package' tab
- Create your custom installer by completing the form. Scroll down for **a table that explains the form fields.**
- **Download Installer -** Download the installation file for your chosen operating system. Once the agent is installed, it establishes communication with the EM server and begins importing devices.
  - Windows - Creates a .msi file if only the communication client is selected. Creates a .exe file if both communication and security client are selected.
  - MAC OS - Creates a .pkg installer file.
  - Linux - Creates a .run file.
- **Download MST File** - Windows only. Download a .mst installer that includes proxy server information for client communication with Endpoint Manager. File should be installed by command line.

**Bulk Installation Package - Form Parameters**

| Parameter | Description |
|---|---|
| User | Specify the user to whom the target endpoints should be assigned. By default, this is the currently logged in user. You can always can this later if required.<br>• Start typing the name of a user and choose from the suggestions that appear. |
| Customer | Choose the company to which the endpoints should be assigned.<br>• This field only applies to CD MSP and C1 MSP customers. It does not apply to CD Enterprise, C1 Enterprise, or EM stand-alone customers. |
| Device Group | The device group to which the enrolled devices should be added (optional).<br>Any group profiles will also be applied to the devices you add.<br>See **Assign Configuration Profiles to a Device Group** if you want more help with this. |
| Package Options | **Operating system**<br>Choose the target OS and package type you want. The options are:<br>**Windows**<br>• Windows X64 - For 64-bit Windows OS<br>• Windows X86 - For 32-bit Windows OS<br>• Windows X86 & X64 (hybrid package) - Suitable for both 64-bit and 32-bit Window OS. Select if your network has a mixture of 64-bit and 32-bit versions.<br>**Mac OS (Recommended)**<br>• Installs both the communication client and the configuration profile on the Mac device.<br>• Choose this option if you want to use Endpoint Manager for both MAC security (antivirus etc) AND for general MAC management.<br>• If you select this option, you must install an Apple Push Notification (APN) certificate on your portal to communicate with the devices.<br>  • Apple only allow one portal to control a MAC device via APN. If you want to use a different portal to manage WIFI, VPN, device permissions etc, then choose 'MAC OS without MDM Profile' instead.<br>  • See **Add Apple Push Notification Certificate** for help to install the certificate.<br>**Mac OS without MDM Profile**<br>• Installs just the communication client on the Mac device.<br>• Choose this option if you only want to use Endpoint Manager for security on Mac devices.<br>• This option lets you continue to use a different portal for general MAC management while using Endpoint Manager to manage security.<br>• This option means you cannot use Endpoint Manager to manage the following profile items:<br>  • Certificates<br>  • Restrictions<br>  • VPN |

| | |
|---|---|
| | • Wi-Fi<br>• To help you make a decision, you can see what is included the items above by checking the 'Profiles' area.<br>◦ Click 'Configuration Templates' > 'Profiles' > *open a MAC profile OR create a new MAC profile* > 'Add Profile Section'<br>◦ Add, for example, a 'Restrictions' section to see what is covered.<br>• See **Profiles for Mac OS Devices** if you want more help on MAC profiles.<br>**Linux**<br>• Ubuntu / Debian (Hybrid Package) - Suitable for both 64-bit and 32-bit<br>• RHEL / CentOS (Hybrid Package) - Suitable for both 64-bit and 32-bit<br>**Clients**<br>**Communication Client (CC) -** Mandatory. This client enrolls the endpoint and handles communication between the endpoint and endpoint manager.<br>**Comodo Client Security (CCS) -** Optional. This client installs the security software, including antivirus, firewall and auto-containment.<br>**Additional Options** (Windows only)<br>**Database -** Choose whether to include the latest virus database with the installer. This increases file size. If disabled, the client will download the latest database anyway when you run the first scan.<br>**Profile -** Choose a configuration profile for the endpoints (optional).<br>• Type the first few characters of a profile and choose from the suggestions that appear.<br>**Profile**<br>Select the configuration profile you want to apply to the target devices.<br>• If you do not choose a profile then the default OS profile is applied.<br>• Click 'Configuration Templates' > 'Profiles' to view and configure endpoint profiles. You can review the default OS profiles in here.<br>• Tip: You can always add or remove profiles later. The default OS profile will implement good, baseline settings for security and usability.<br>• See **View and Manage Profiles Associated with a Device** if you want to read more about profiles. |
| Restart Control Options (For Windows only) | CCS only. Endpoints need to be restarted to complete CCS installation. You have the following restart options:<br>• **Force the reboot in... -** Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message will be shown to the user prior to the restart.<br>• **Suppress reboot -** Endpoint is not auto-restarted. The installation will be finalized when the user next restarts the endpoint.<br>• **Warn about reboot and let users postpone it -** Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.<br>Optional. Type a custom message in the 'Reboot Message' field. |

|  |  |
|---|---|
| UI Options (For Windows only) | Configure which messages are shown to the user regarding the installation.<br>• **Show error messages if installation failed** - Notifies the user if the installation is not successful.<br>• **Show a confirmation message upon completion of installation** - Notifies the user if the installation is successful. Type your message in the box provided. |
| Proxy Settings (For Windows only) | Specify a proxy server through which the clients should connect to Endpoint Manager and other Comodo servers. If you do not set a proxy then the clients will connect directly as per network settings.<br>• Enter the IP address/hostname of the proxy server and port in the respective fields.<br>• Enter the user-name and password of an administrative account on the proxy server in the Proxy Login and Proxy Password fields<br>Note: If you specify a proxy here then you must also configure the same proxy settings in the profile on the device:<br>• Click 'Configuration Templates' > 'Profiles' > *open the device profile* > 'Add Profile Section' > 'Clients Proxy' |

### 5.3.1.3. Enroll Windows Devices using Auto Discovery and Deployment Tool

- You can use the auto-deployment tool to install the Endpoint Manager communication and security clients on target endpoints.
- By installing the clients you will enroll the endpoints to Endpoint Manager.
- You first need to create client installation files using the 'Bulk Installation Package' interface in 'Devices'

| |
|---|
| Note - The user of the device should already have been added to Endpoint Manager. You can download installation packages only for existing users. |

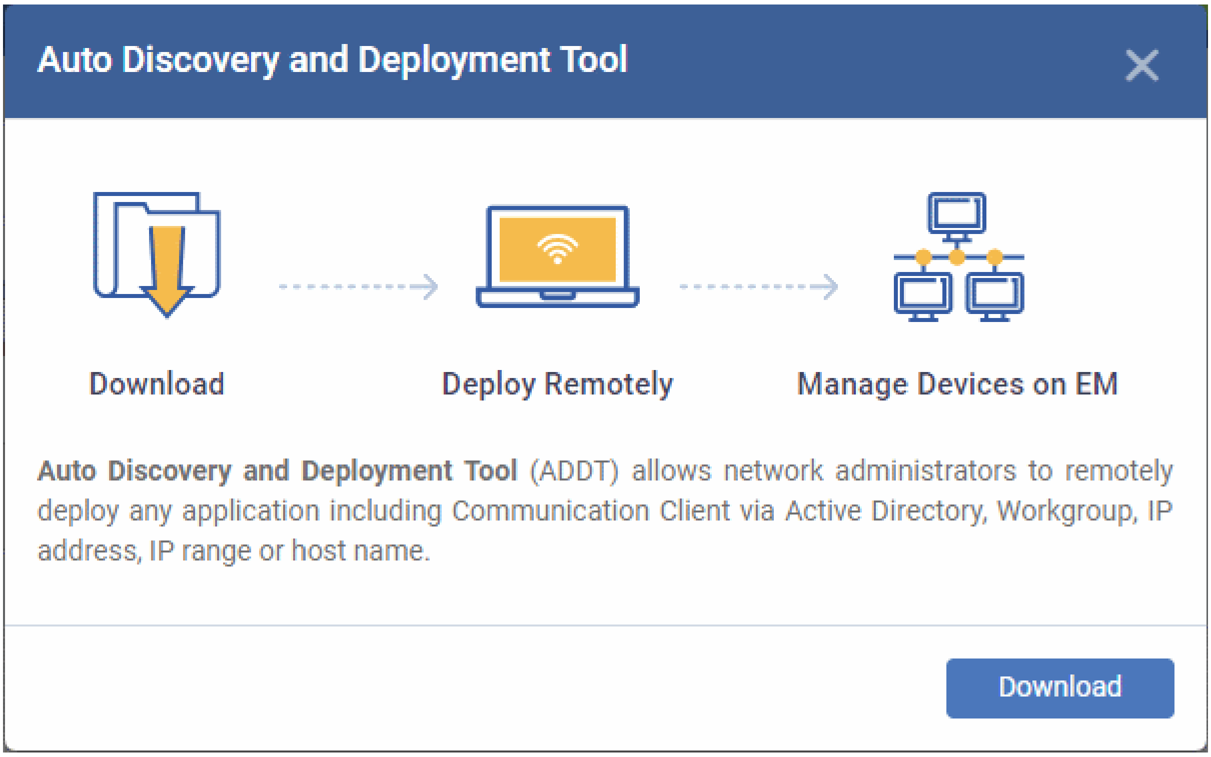
**Download ADDT and installation packages**

- Click 'Devices' > 'Bulk Installation Package'
- Each installation package is custom-created for a specific user, customer, group, operating system etc.
- Complete the fields in the form to generate your custom package:

| Bulk Installation Package - Form Parameters | |
|---|---|
| **Parameter** | **Description** |
| User | Specify the user to whom the target endpoints are assigned.<br>- Start typing the name of a user and choose from the suggestions that appear. |
| Customer | Choose the company to which the endpoints should be assigned.<br>- This field only applies to CD MSP and C1 MSP customers. It does not apply to CD Enterprise, C1 Enterprise, or EM stand-alone customers |
| Device Group | The device group to which the enrolled devices should be added (optional).<br>Any group profiles will also be applied to the devices you add.<br>See **Assign Configuration Profiles to a Device Group** if you want more help with this. |
| Package Options | **Operating system** - Select 'Windows'<br>- Choose platform - Select Windows OS version (64 bit, 32 bit or hybrid package)<br>**Clients**:<br>- **Communication Client (CC)** - Mandatory. This client enrolls the endpoint.<br>- **Comodo Client Security (CCS)** - Optional. This client installs security software such as antivirus, firewall and auto-containment.<br>**Additional Options**:<br>- **Database** - Choose whether to include the latest virus database with the installation package. This increases file size. If disabled, the client will download the latest database anyway when you run the first scan.<br>- **Profile** - Choose a configuration profile for the endpoints (optional).<br>  - Type the first few characters of a profile and choose from the suggestions that appear.<br>If you do not choose a profile then the default profiles for the operating system will be applied.<br>**Tip**: You can add or remove profiles later. See **View and Manage Profiles Associated with a Device** for more details. |
| Restart Control Options | CCS only. Endpoints need to be restarted to complete CCS installation. You have the following restart options:<br>- **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message will be shown to the user prior to the restart.<br>- **Suppress reboot** - Endpoint is not auto-restarted. The installation will be finalized when the user next restarts the endpoint.<br>- **Warn about reboot and let users postpone it** - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.<br>Optional. Type a custom message in the 'Reboot Message' field. |
| UI Options | Configure which messages are shown to the user regarding the installation. |

| | |
|---|---|
| | - **Show error messages if installation failed -** Notifies the user if the installation is not successful.<br>- **Show a confirmation message upon completion of installation -** Notifies the user if the installation is successful. Type your message in the box provided. |
| Proxy Settings | Leave these blank as these settings are not required for offline installation packages. |

- Click 'Download Installer' when you have completed the form.
- You will now download TWO items:
  1. The installation package. This will have a name like 'installer_2dr846534e83.exe'
  2. The Auto-Deployment tool (ADDT). This tool helps you deploy the installation package to your network:


Auto Discovery and Deployment Tool

**Auto Discovery and Deployment Tool** (ADDT) allows network administrators to remotely deploy any application including Communication Client via Active Directory, Workgroup, IP address, IP range or host name.

ADDT is a portable app which does not require installation. ADDT lets you deploy the clients via Active Directory, Workgroup or network address.

- Comodo Dragon customers - For more details about how to deploy applications via ADDT, visit **https://help.comodo.com/topic-457-1-978-14553-Introduction-to-Comodo-Auto-Discovery-and-Deployment-Tool.html**.
- Comodo One customers - For more details about how to deploy applications via ADDT, visit **https://help.comodo.com/topic-289-1-851-11043-Introduction-to-Comodo-Auto-Discovery-and-Deployment-Tool.html**.

## 5.3.2. Enroll the Android and iOS Devices of AD Users

- This section explains how to enroll the devices of users who were imported from Active Directory. See **Import User Groups from LDAP** if you need help to import users first.
- Setup involves installing the communication client on the user's device. After installation, the user should login to the client using their domain username and password.
- Please follow the steps below to import the devices:

  **Get the enrollment links**

  **Import Android devices**

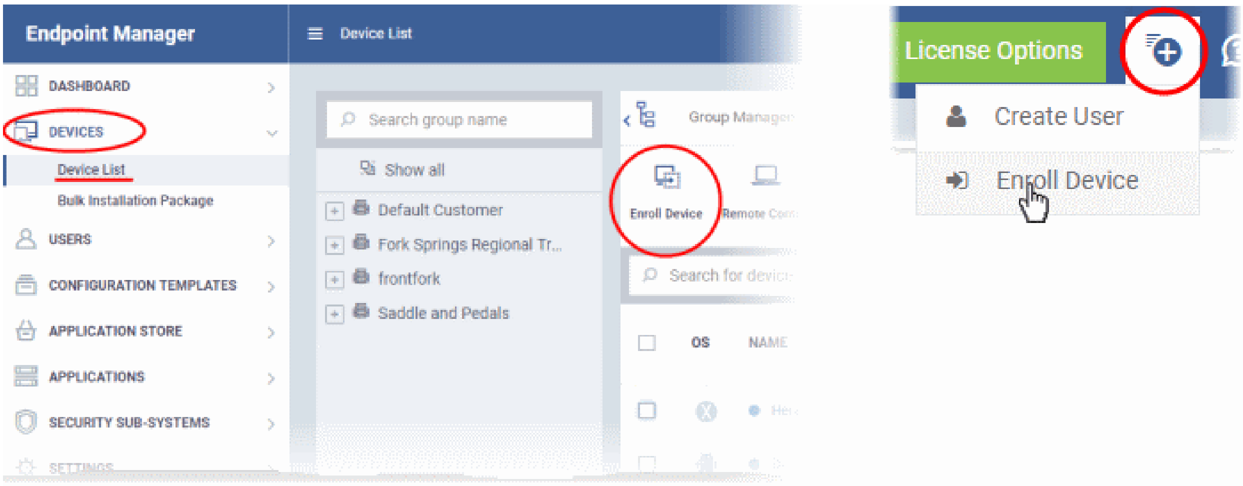
  **Import iOS devices**

### Get the enrollment links

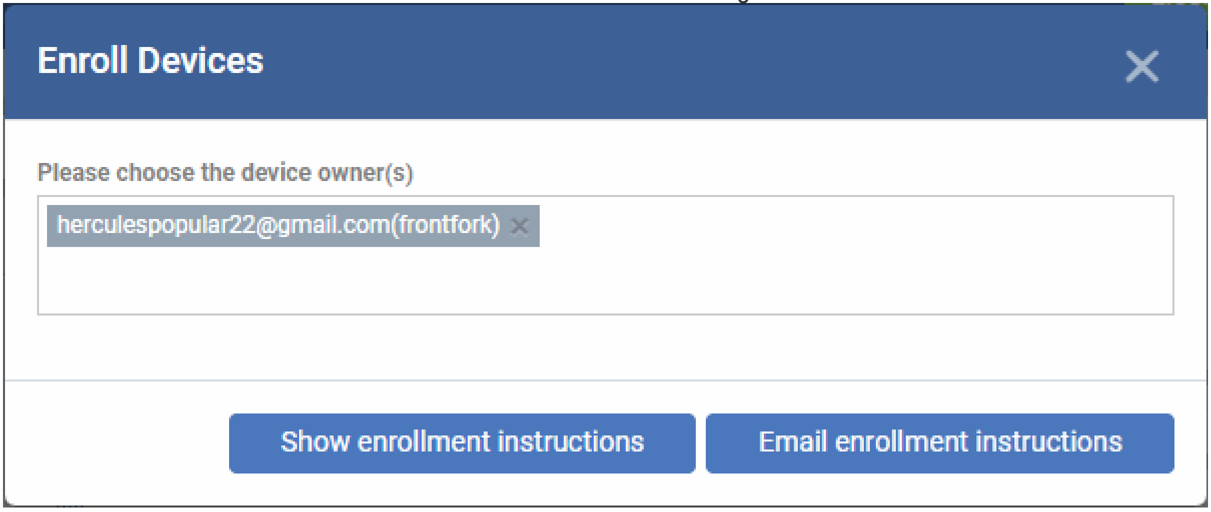
- Click 'Devices' > 'Device List' on the left
- Click the 'Enroll Device' button above the table

  Or

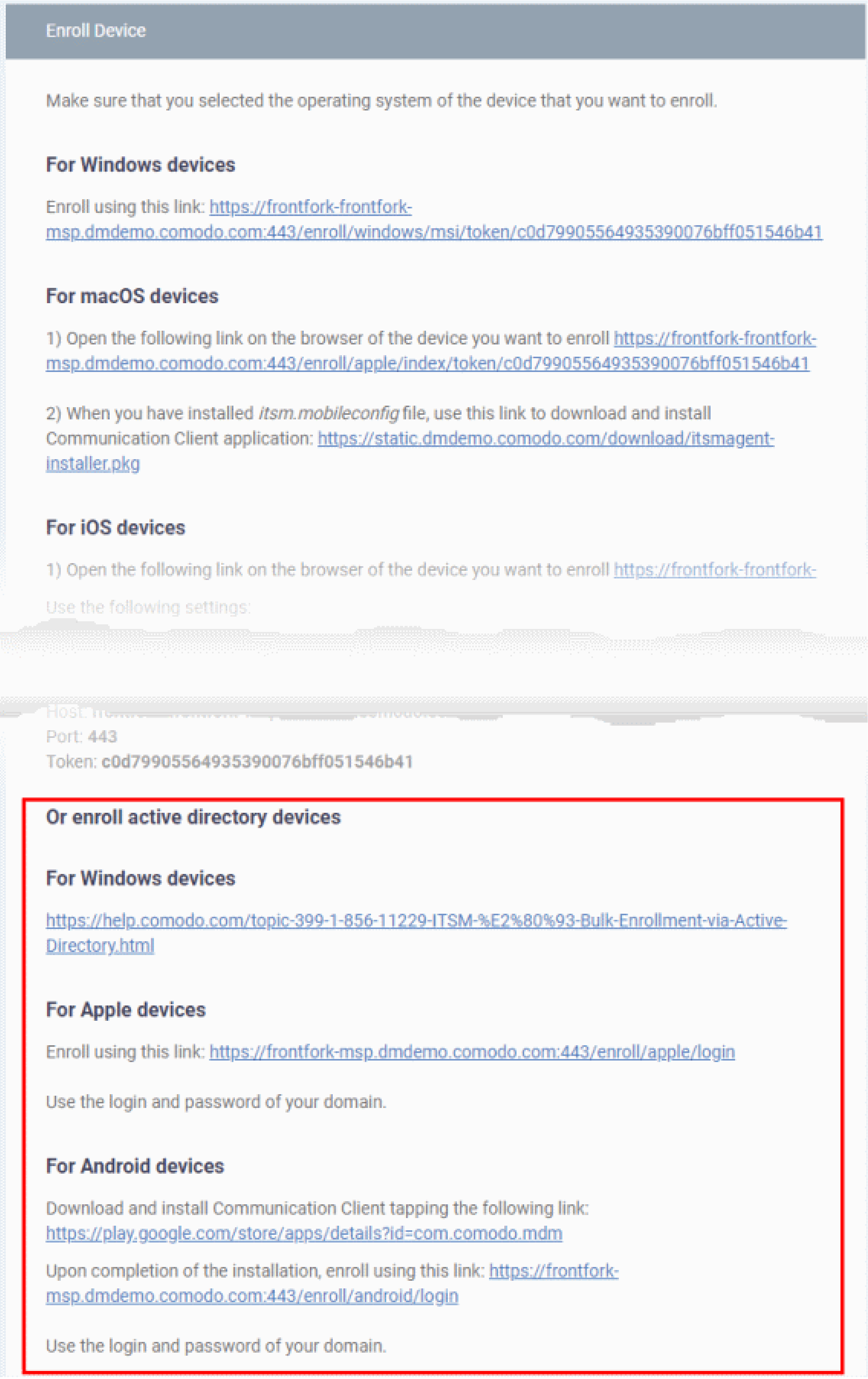
- Click the 'Add' button on the menu bar and choose 'Enroll Device'.



- Click 'Show Enrollment Instructions' in the enroll devices dialog:


Enroll Devices
Please choose the device owner(s)
herculespopular22@gmail.com(frontfork)
Show enrollment instructions
Email enrollment instructions

- Scroll down the section 'Or enroll Active Directory Services':



Enroll Device

Make sure that you selected the operating system of the device that you want to enroll.

For Windows devices

Enroll using this link: https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/c0d79905564935390076bff051546b41

For macOS devices

1) Open the following link on the browser of the device you want to enroll https://frontfork-frontfork-msp.dmdemo.comodo.com:443/enroll/apple/index/token/c0d79905564935390076bff051546b41

2) When you have installed *itsm.mobileconfig* file, use this link to download and install Communication Client application: https://static.dmdemo.comodo.com/download/itsmagent-installer.pkg

For iOS devices

1) Open the following link on the browser of the device you want to enroll https://frontfork-frontfork-

Use the following settings:

Host: [illegible]
Port: 443
Token: c0d79905564935390076bff051546b41

Or enroll active directory devices

For Windows devices

https://help.comodo.com/topic-399-1-856-11229-ITSM-%E2%80%93-Bulk-Enrollment-via-Active-Directory.html

For Apple devices

Enroll using this link: https://frontfork-msp.dmdemo.comodo.com:443/enroll/apple/login

Use the login and password of your domain.

For Android devices

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

Upon completion of the installation, enroll using this link: https://frontfork-msp.dmdemo.comodo.com:443/enroll/android/login

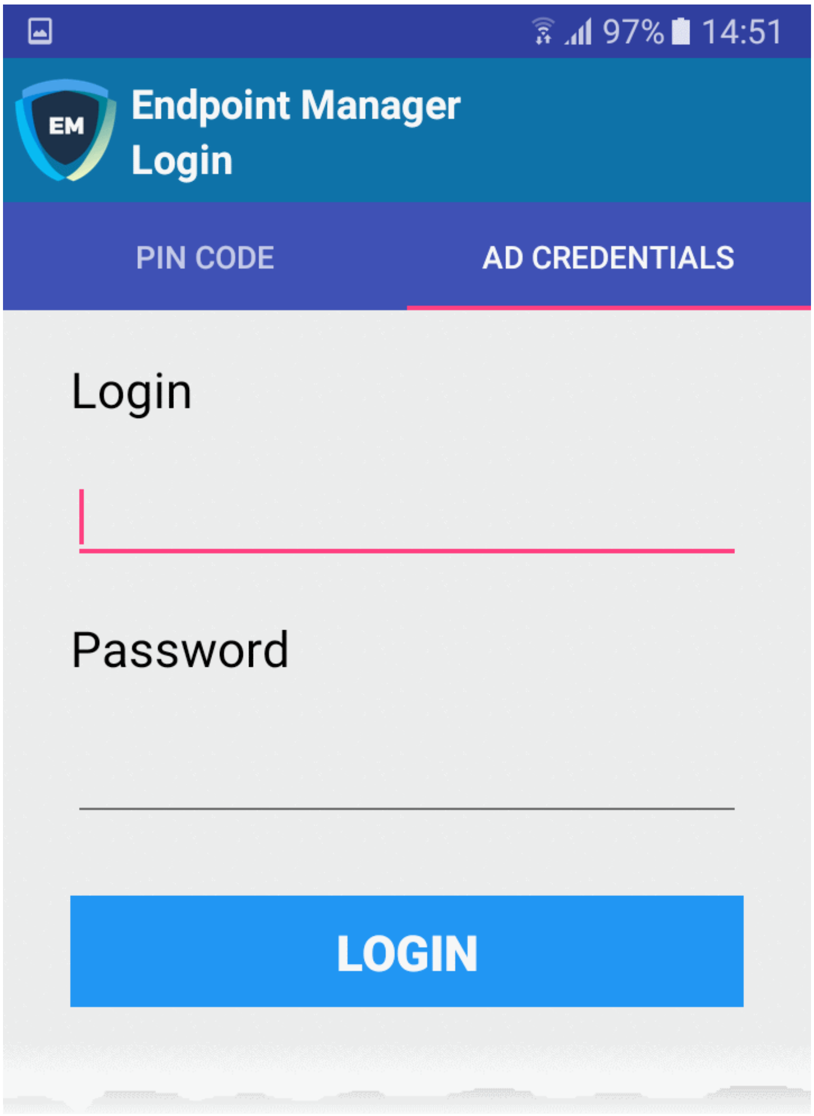
Use the login and password of your domain.

- You next need to send your target users the appropriate setup links for their device operating system.
- Users should open the links on the target device itself

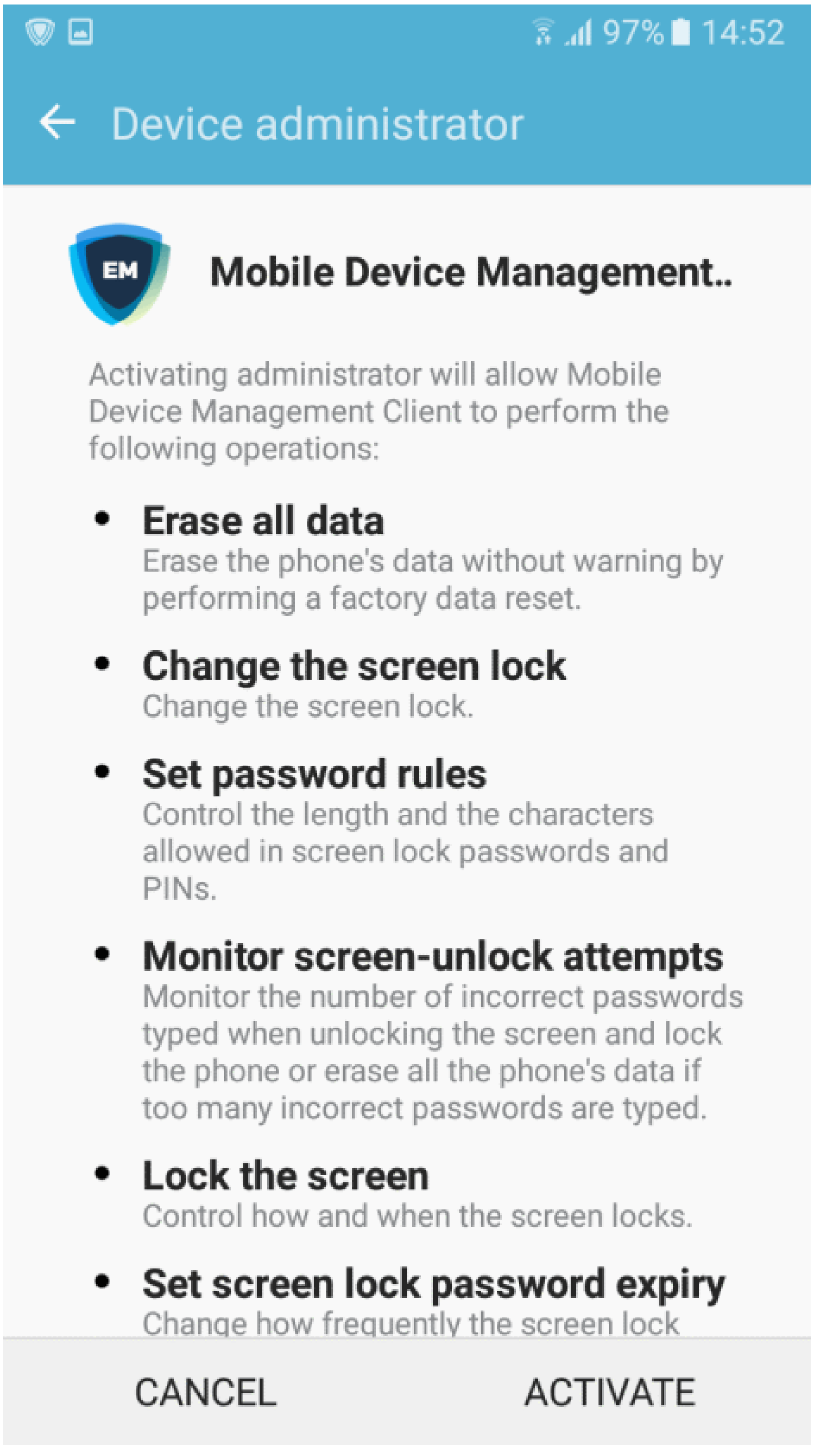
- See **Import Android devices** or **Import iOS devices** as required.

## Android Devices:

- Email the Android client download and enrollment links to target users
- Users should open the mail on the device you want to enroll
- First click the agent download link then install the client on the device.
- After installation is complete, the user should next open the enrollment link.
- This will open the Endpoint Manager login page. Users can login with their domain username and password:



- After agreeing to the EULA, the user should hit 'Activate' to grant admin privileges to the communication client:

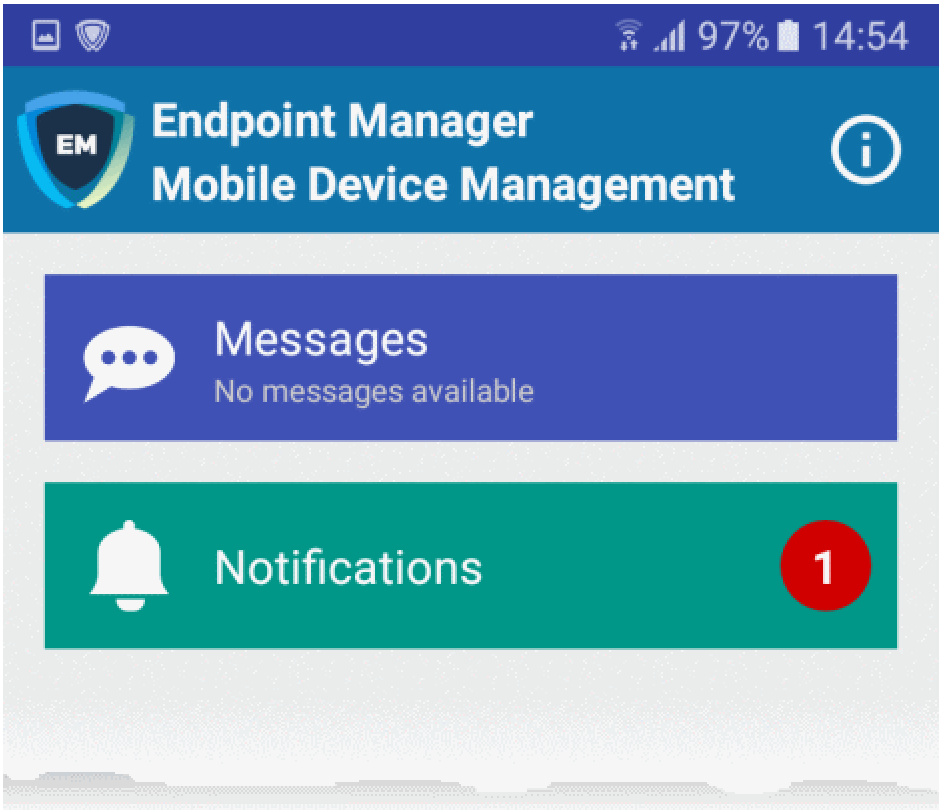


**Mobile Device Management..**

Activating administrator will allow Mobile Device Management Client to perform the following operations:

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

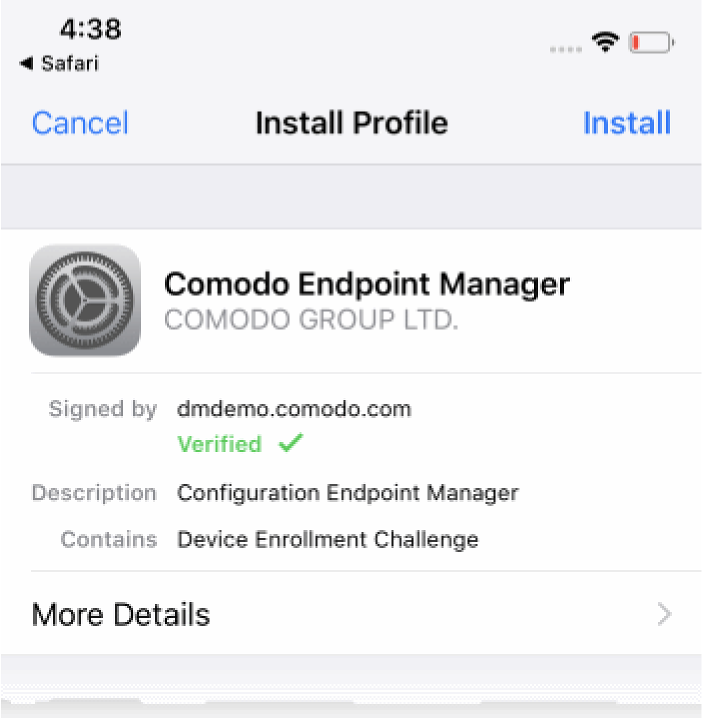
- After activation, the client will open at the home screen :



- The device is now enrolled and can be remotely managed from the Endpoint Manager console.

### iOS Devices:

- iOS users first need to install a device profile, then install the Endpoint Manager app.
- Email the Apple enrollment link to all target users. Users should open the mail on the device you want to enroll.
- Users should open the link to download and install the enrollment profile:



Comodo Endpoint Manager
COMODO GROUP LTD.

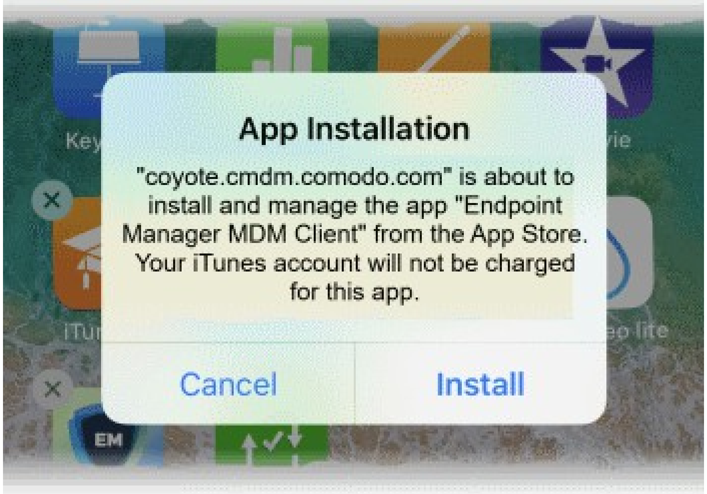
Signed by dmdemo.comodo.com
Verified ✓

Description Configuration Endpoint Manager

Contains Device Enrollment Challenge

- Users should follow the wizard to complete profile installation.

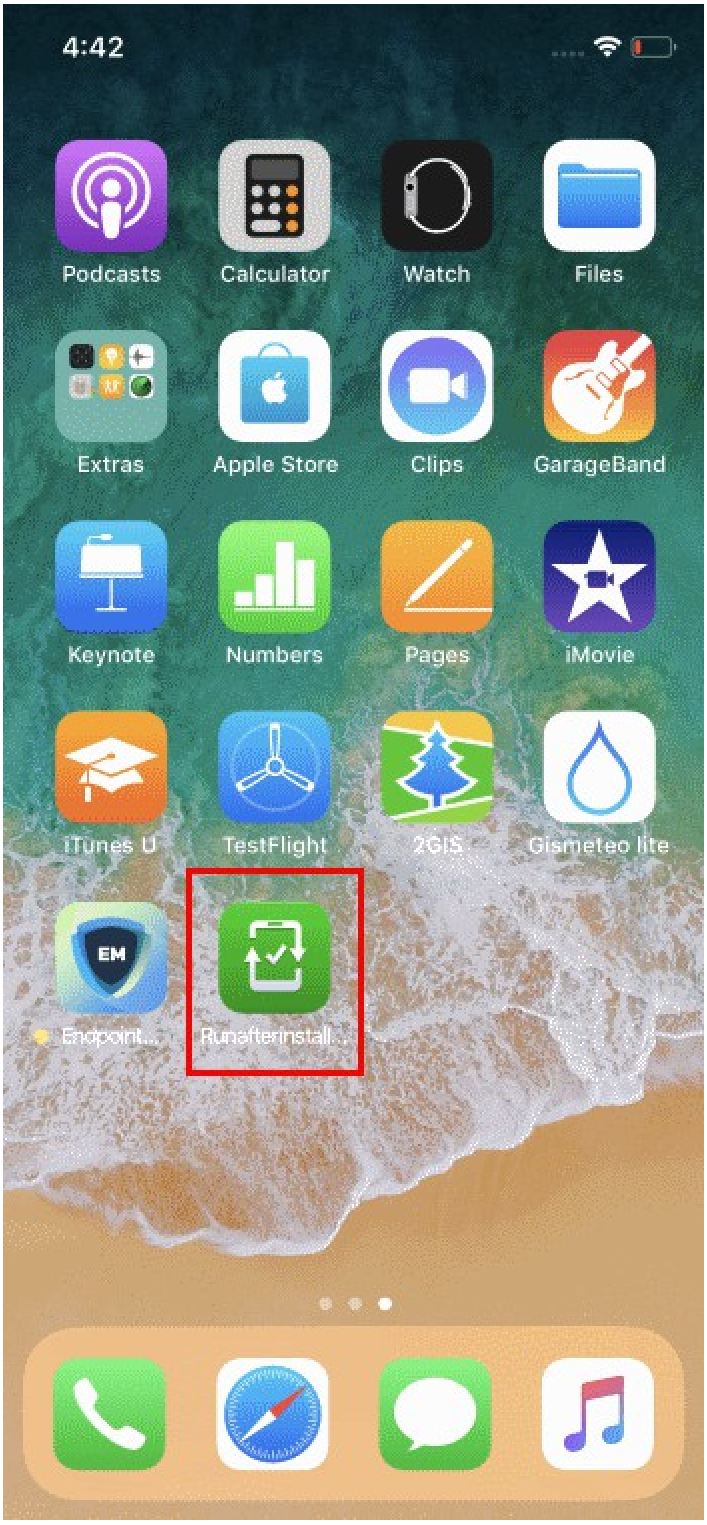
- The Endpoint Manager login page will appear when installation is complete. Users should login with their domain username / password.
- The device will connect to Endpoint Manager and commence the app installation process:



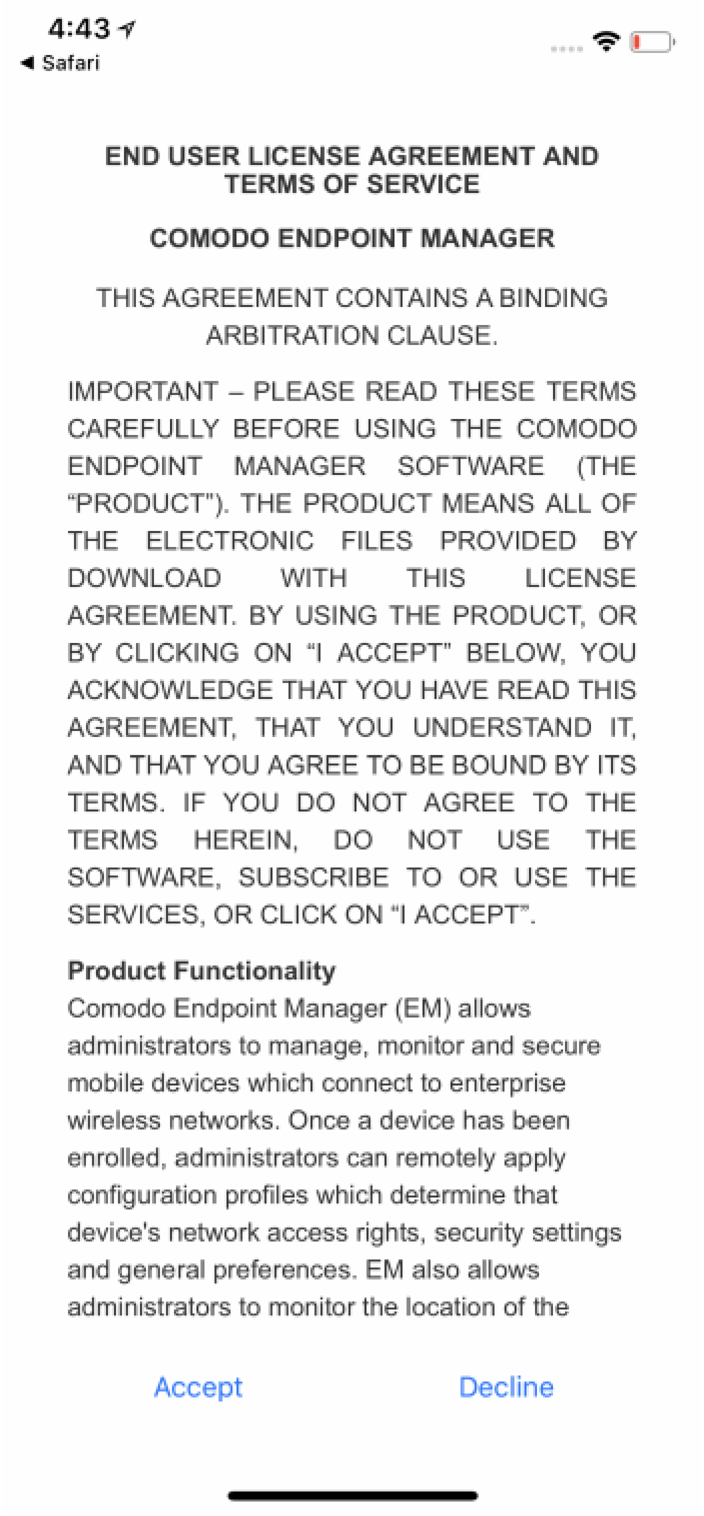
App Installation

"coyote.cmdm.comodo.com" is about to install and manage the app "Endpoint Manager MDM Client" from the App Store. Your iTunes account will not be charged for this app.

- User should select 'Install'. The app is downloaded from their iTunes store account. Users may need to login with their Apple account.
- After installation, users should open the green 'Run After Install' icon:



- User should next accept the EULA to complete device enrollment:



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

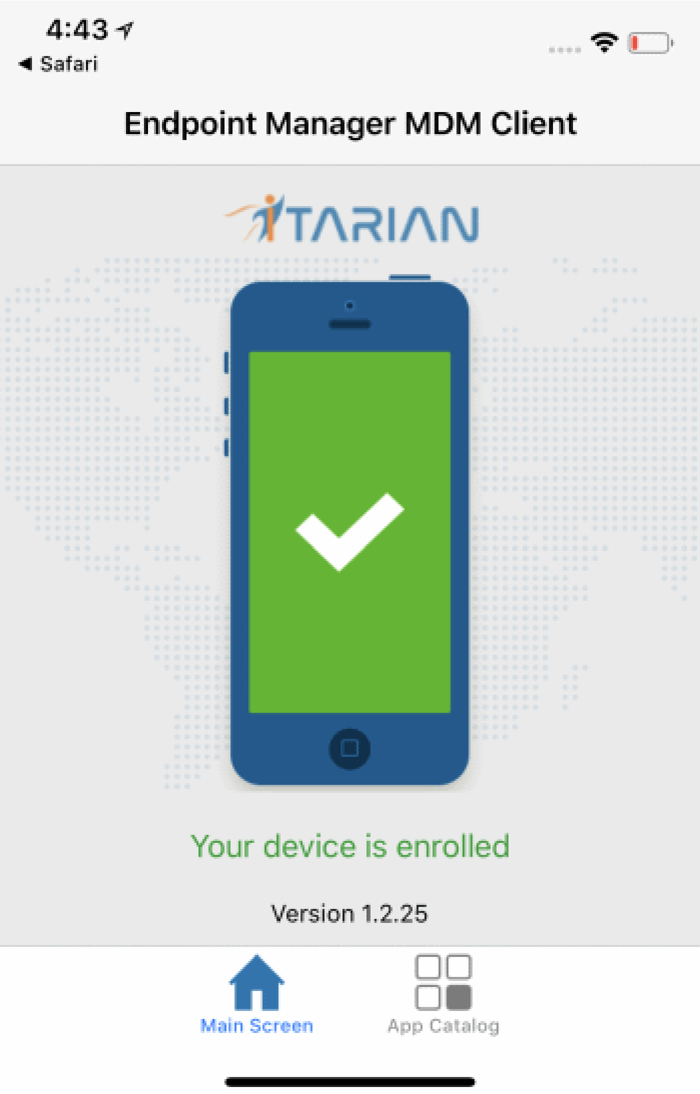
COMODO ENDPOINT MANAGER

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

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

**Product Functionality**
Comodo Endpoint Manager (EM) allows administrators to manage, monitor and secure mobile devices which connect to enterprise wireless networks. Once a device has been enrolled, administrators can remotely apply configuration profiles which determine that device's network access rights, security settings and general preferences. EM also allows administrators to monitor the location of the

- The device will be successfully enrolled to Endpoint Manager once the client is installed:



4:43

◀ Safari

Endpoint Manager MDM Client

Your device is enrolled

Version 1.2.25

**App Catalog** - Shows Endpoint Manager apps that are ready to be installed:

## 5.4. Download and Install the Remote Control Tool

- The remote control tool allows admins and staff to take remote control of Windows and Mac OS endpoints.
- This is useful in a number of circumstances, including troubleshooting, running system maintenance and providing training to users.
- You can download the tool from Endpoint Manager, or from the Comodo Dragon / Comodo One consoles:
    - **Endpoint Manager** - Click 'Devices' > 'Bulk Enrollment Package' > 'Remote Control by ITarian'.
    - **CD or C1 console** - Click 'Tools' > Click 'Download' in the 'Remote Control by ITarian' tile.
- The tool should be installed on your admin computer (the computer from which you want to control the remote endpoints).
- Once installed, the tool can be started from the desktop application or from the EM admin console.
- See **Remote Management of Windows and Mac OS Devices** for more help to takeover Windows and Mac OS devices

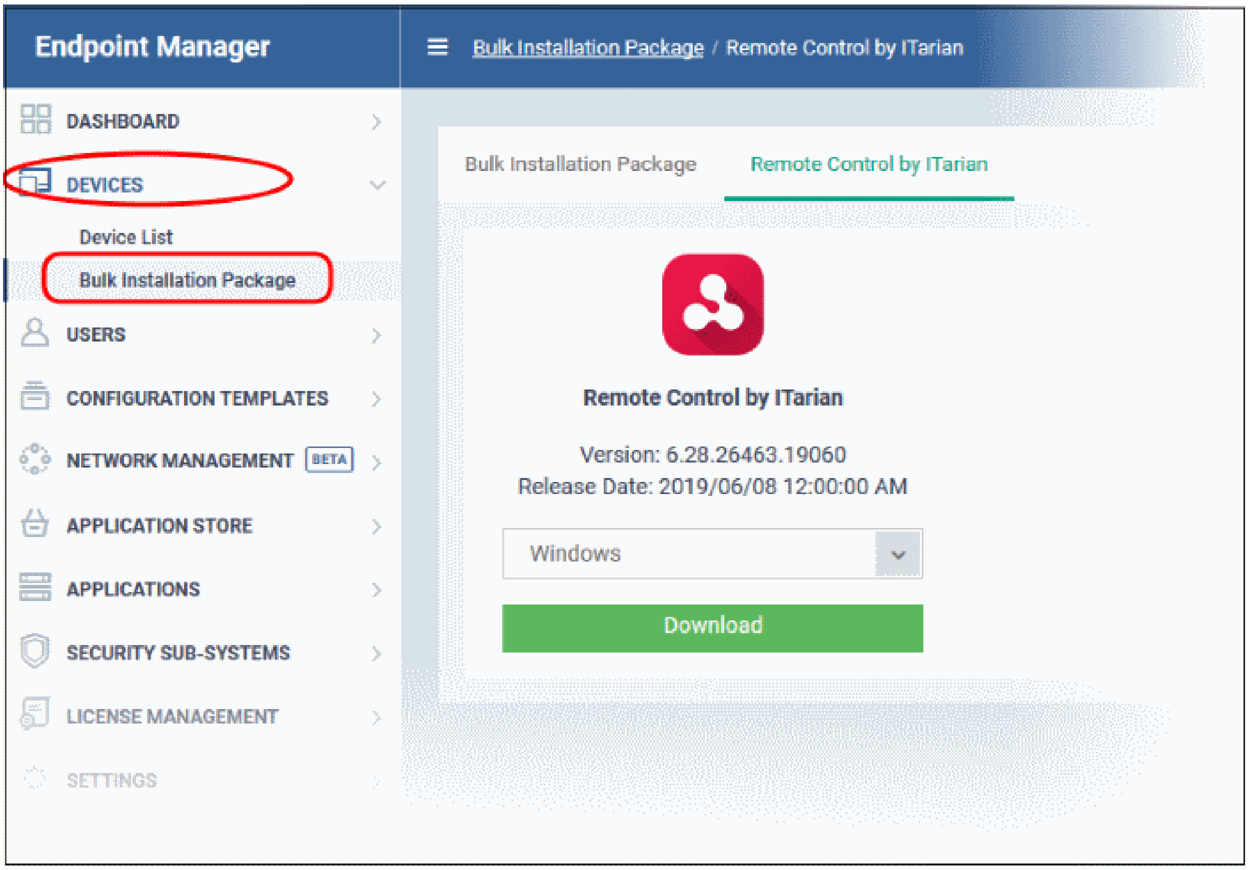
**Limitations**:

- The remote control tool uses WebRTC and Chromoting protocols to connect to Windows devices. It uses the Chromoting protocol alone to connect to Mac OS devices.

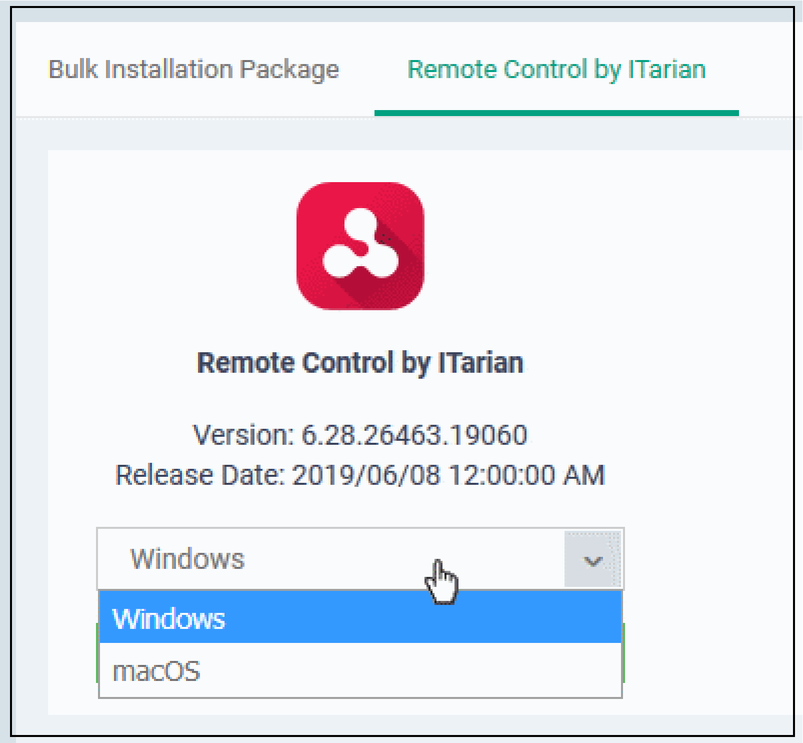
- Chromoting is supported by MAC OS and by Windows 7, 8/8.1, 10. It is not support by Windows XP.
- WebRTC is not supported by Mac OS

## Download RC from EM interface

- Click 'Devices' > 'Bulk Installation Package'.
- Select the 'Remote Control by ITarian' tab


Endpoint Manager
Bulk Installation Package / Remote Control by ITarian
DASHBOARD
DEVICES
Device List
Bulk Installation Package
USERS
CONFIGURATION TEMPLATES
NETWORK MANAGEMENT BETA
APPLICATION STORE
APPLICATIONS
SECURITY SUB-SYSTEMS
LICENSE MANAGEMENT
SETTINGS
Bulk Installation Package
Remote Control by ITarian
Remote Control by ITarian
Version: 6.28.26463.19060
Release Date: 2019/06/08 12:00:00 AM
Windows
Download

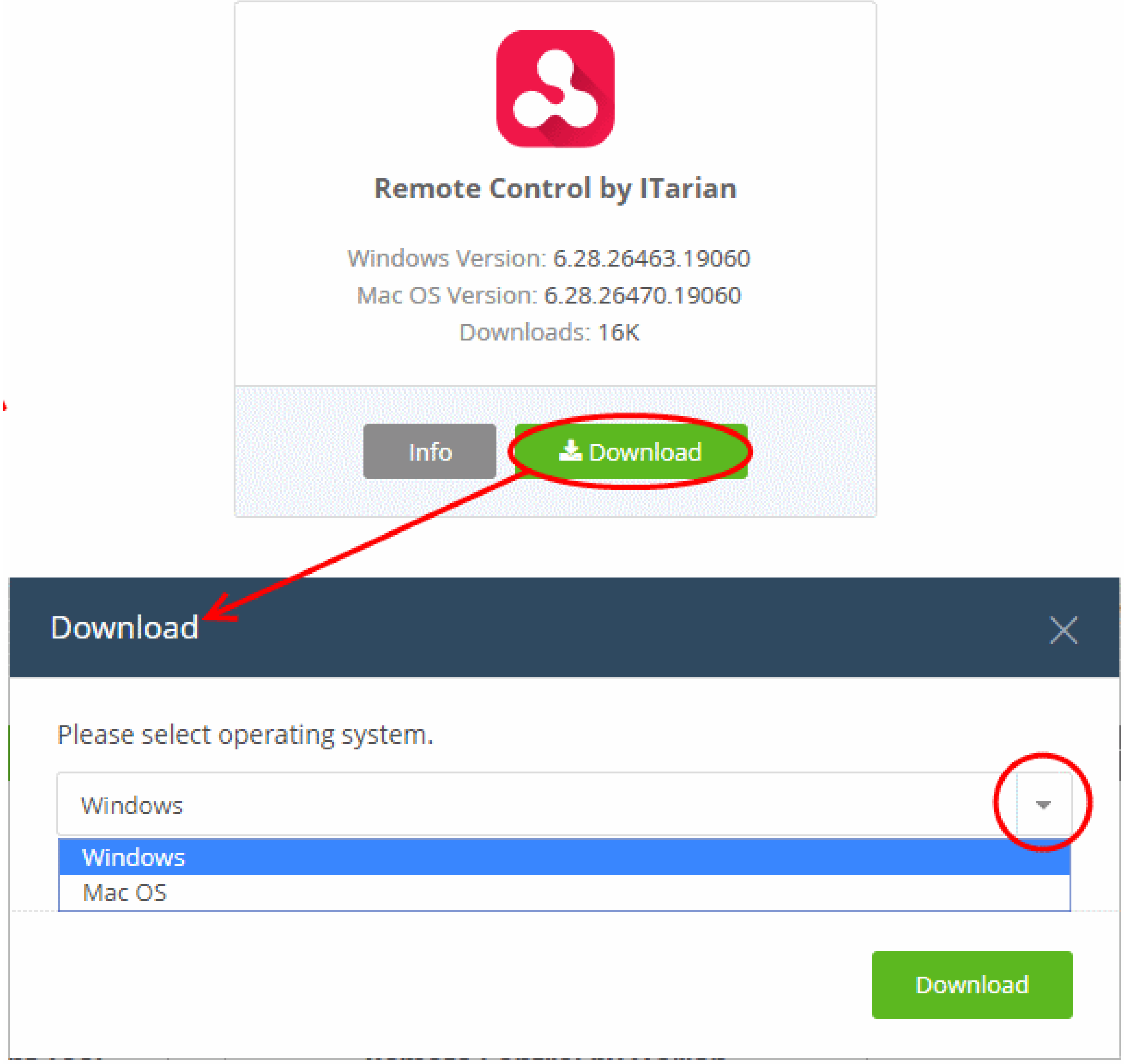
- Select the OS of the computer on which you want to install the tool.


Bulk Installation Package
Remote Control by ITarian
Remote Control by ITarian
Version: 6.28.26463.19060
Release Date: 2019/06/08 12:00:00 AM
Windows
Windows
macOS

- Click 'Download' and save the setup file.

### Download RC from Comodo Dragon or Comodo One Console

- **Comodo Dragon customers** - Login at **https://platform.comodo.com/app/login**
- **Comodo One customers** - Login at **https://one.comodo.com/app/msp/login**
- Click 'Tools' in the top-menu
  - The 'Tools' area is a repository of enterprise productivity and security tools
- Click the 'Download' button in the 'Remote Control for ITarian' tile



Remote Control by ITarian

Windows Version: 6.28.26463.19060

Mac OS Version: 6.28.26470.19060

Downloads: 16K

Download

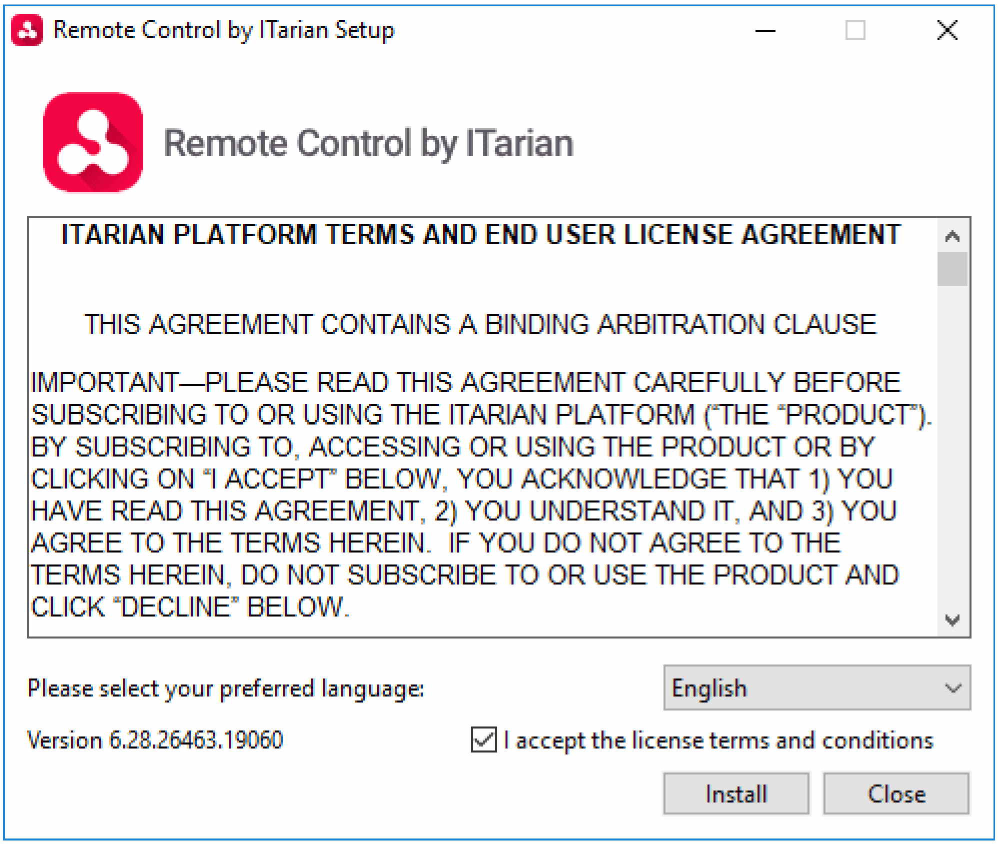
Please select operating system.

Windows

- Select the operating system of your admin machine.
- Click 'Download' and save the file.

**Install the tool**

- Launch the set up file to start the installation wizard:



Remote Control by ITarian Setup

Remote Control by ITarian

ITARIAN PLATFORM TERMS AND END USER LICENSE AGREEMENT

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE

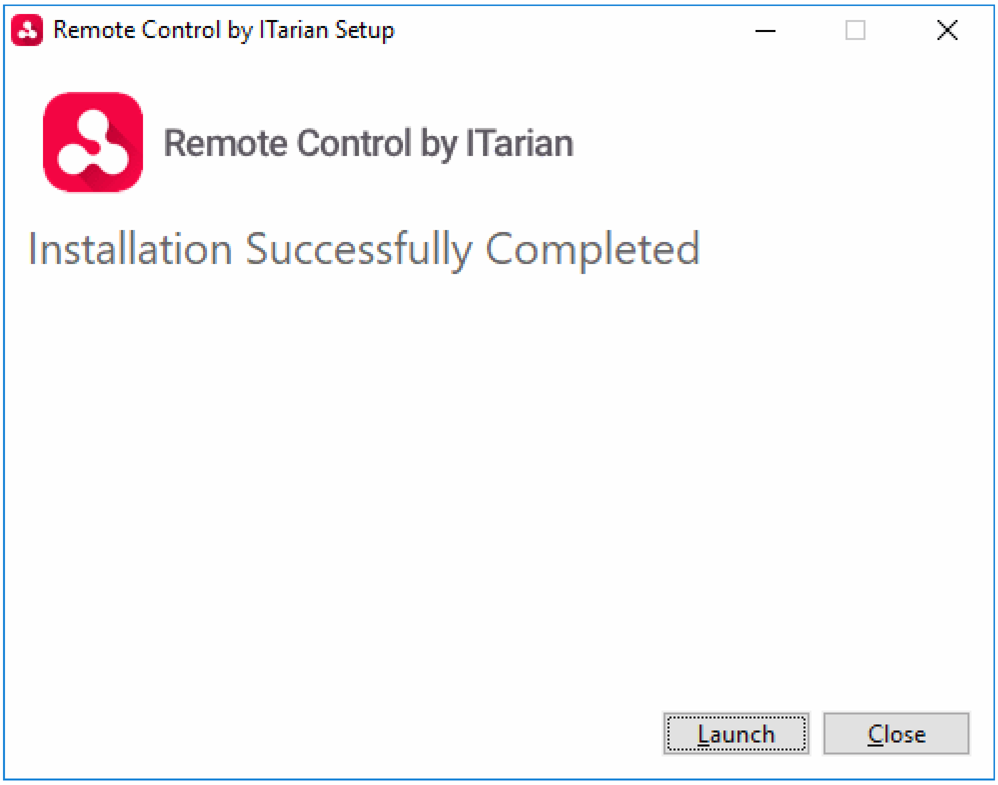
IMPORTANT—PLEASE READ THIS AGREEMENT CAREFULLY BEFORE SUBSCRIBING TO OR USING THE ITARIAN PLATFORM ("THE "PRODUCT"). BY SUBSCRIBING TO, ACCESSING OR USING THE PRODUCT OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT 1) YOU HAVE READ THIS AGREEMENT, 2) YOU UNDERSTAND IT, AND 3) YOU AGREE TO THE TERMS HEREIN. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT SUBSCRIBE TO OR USE THE PRODUCT AND CLICK "DECLINE" BELOW.

Please select your preferred language: English

Version 6.28.26463.19060

☑ I accept the license terms and conditions

- Language - Select your preferred language. Options available are English, Spanish and Russian.
- EULA - You must read and accept the End User License Agreement before continuing. After doing so, click 'Install' to start the installation.

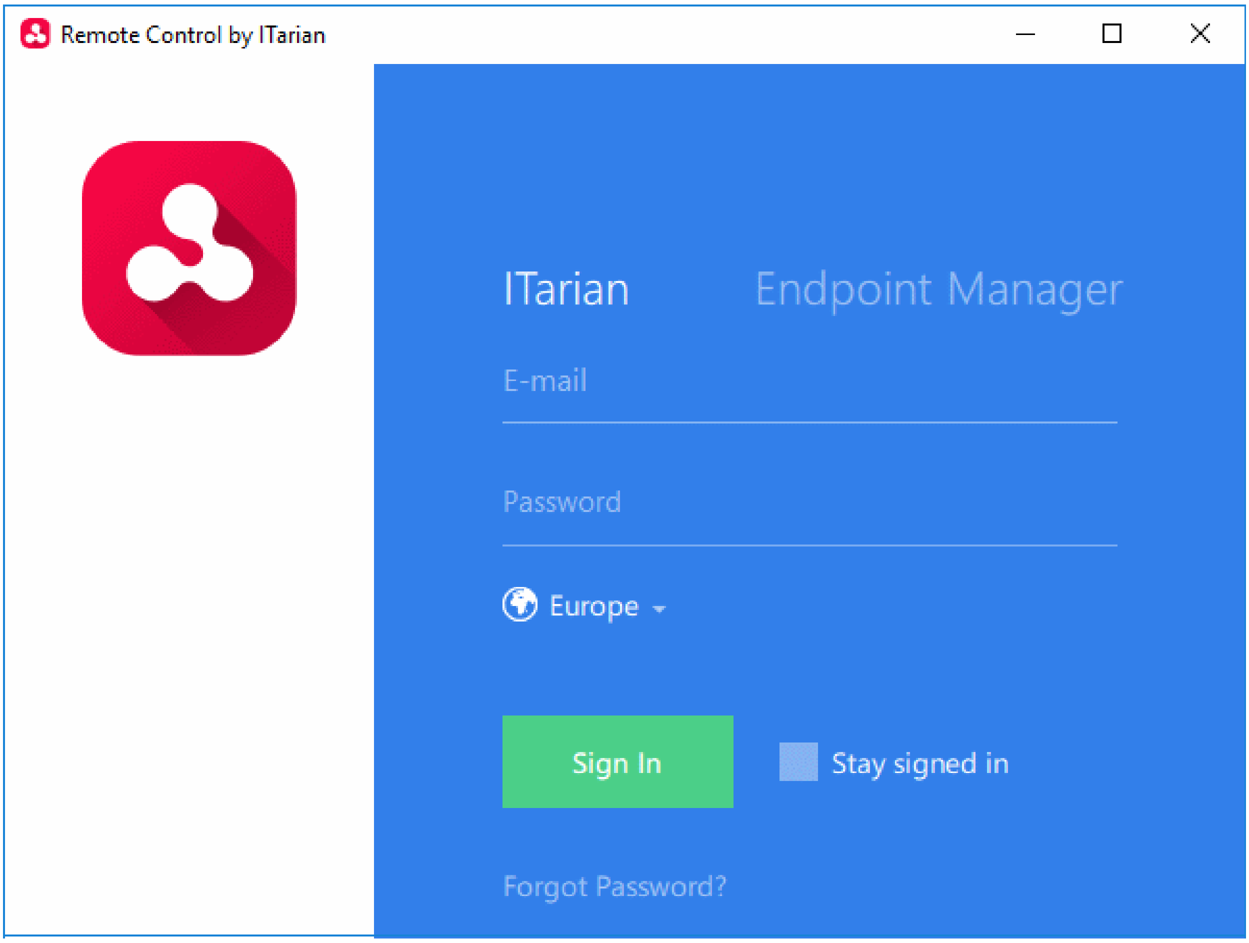


Remote Control by ITarian Setup

Remote Control by ITarian

Installation Successfully Completed

- After installation is complete, click 'Launch' to start the application.

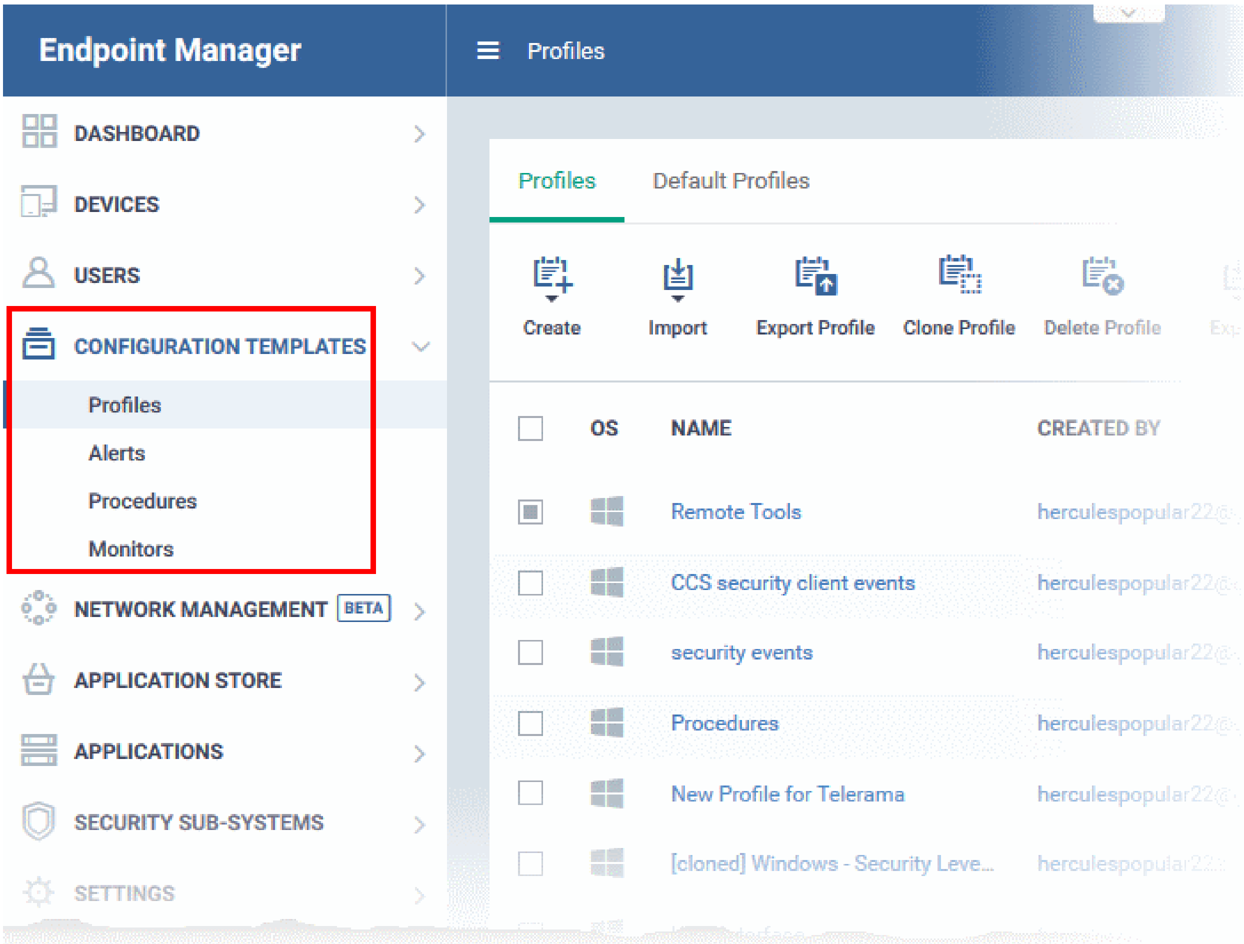


- Login to the application to start managing Windows or Mac OS endpoints.
    - **Comodo Dragon and Comodo One customers** - Click the 'ITarian' tab then login with your Comodo Dragon / Comodo One portal username and password
    - **Stand-alone Endpoint Manager customers** - Click the 'Endpoint Manager' tab then enter your Endpoint Manager URL and login details. The URL will have the format https://<your-company--name>.cmdm.comodo.com, where <your-company-name> is your Endpoint Manager company.
- See **Remote Management of Windows and Mac OS Devices** if you need help to use the remote application.

# 6.Configuration Templates

The 'Configuration Templates' section lets you create and manage profiles for Android, iOS, Mac, Windows and Linux devices.

- Each profile lets you to specify a device's network access rights, overall security policy, antivirus scan schedule and other settings.
- Once created, profiles can be applied to devices/device groups and users/user groups.
- You can also add procedures and monitors to a profile (Windows devices only).
    - **Procedures** let you automate a range of tasks on your protected endpoints. Example procedures include patch installation, disk de-fragmentation and so on. Procedures can also be deployed as stand-alone instructions.
    - **Monitors** are scripts which track events on your endpoints and take specific actions if their conditions are met. For example, 'Alert me when a USB removable disk is connected to the system', or 'Create a log entry if CPU usage goes above 75% for a certain length of time'.
- **Alerts** - You can configure monitors to generate alerts if their conditions are met.
    - The 'Alerts' area contains templates which specify general settings for those alerts.
    - For example, 'Create a ticket on service desk', 'Create a notification in the portal', 'Send a notification to the following users'.
    - You can create different alert templates and apply them to different monitors as required.



| | OS | NAME | CREATED BY |
|---|---|---|---|
| ☒ | | Remote Tools | herculespopular22@ |
| □ | | CCS security client events | herculespopular22@ |
| □ | | security events | herculespopular22@ |
| □ | | Procedures | herculespopular22@ |
| □ | | New Profile for Telerama | herculespopular22@ |
| □ | | [cloned] Windows - Security Leve... | herculespopular22 |

The 'Configuration Templates' tab contains four sub sections:

- **Profiles** - A list of every profile added to Endpoint Manager.

- A profile lets you define a device's security policy, network access rights, antivirus scan schedule and other settings.
- 'Default Profiles' are applied to newly added devices if no user or user group profile exists. Default profiles are available for iOS, Android, Mac OS, Windows and Linux devices
- You can mark custom profiles as 'default' if you wish.
- Profiles can be applied to individual devices/users, device groups and user groups. You can add new profiles, export profiles, and import profiles.

- **Alerts -** Alert templates govern what happens when you receive an alert from a procedure/monitor. For example, an alert template can tell EM to send you a notification if the conditions of a monitor are met.

  Unless you change it, the 'Default Alert' settings are applied to new monitors/procedures. Click 'Configuration Templates' > 'Alerts' then click on 'Default Alert' to view these settings. You can also create custom alert templates as required.

  See '**Manage Alerts**' for more details.
- **Procedures -** Contains a list of predefined and custom procedures that can be executed on enrolled devices. Procedures can be run ad-hoc on selected devices or scheduled in a profile to run at set intervals. See '**Manage Procedures**' for more details.
- **Monitors -** A monitor is a script which tracks events on your network and takes specific actions if its conditions are met. For example, 'Alert me when a USB removable disk is connected to the system', or 'Create a log entry if CPU usage goes above 75% for a certain length of time'.

  You can add a monitor to a Windows profile by adding a 'Monitoring' section. See **Manage Monitors** for more details.

The interface allows the administrator to:

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

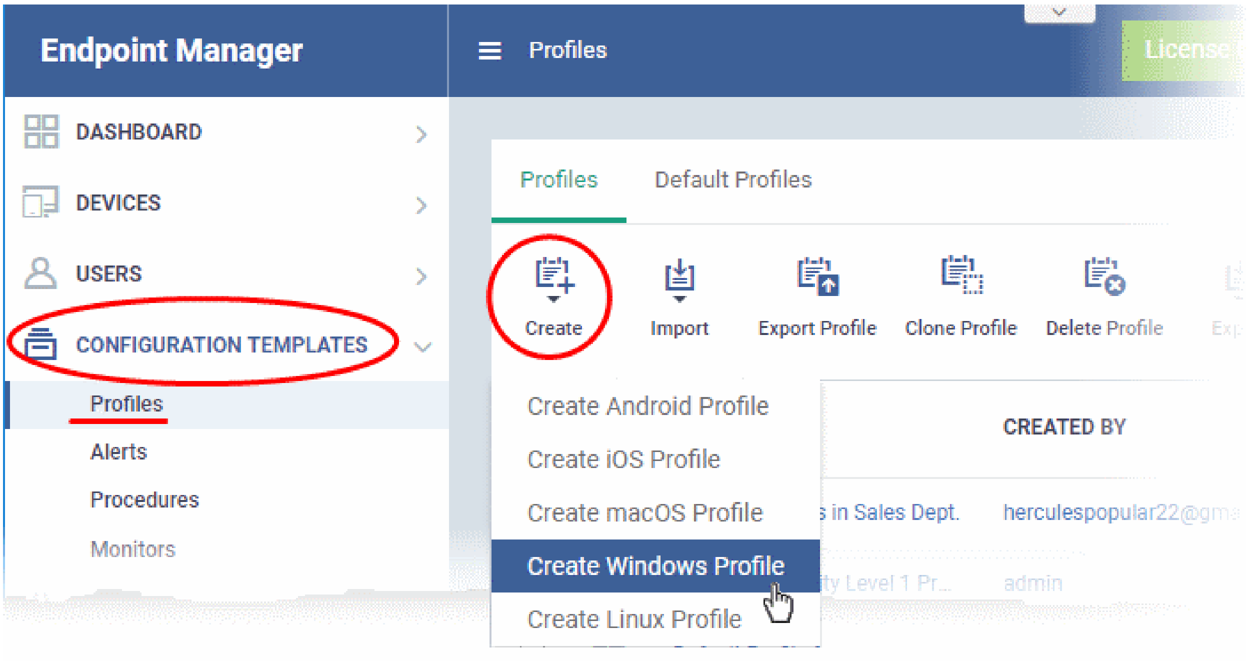
# 6.1. Create Configuration Profiles

- Click 'Configuration Templates' > 'Profiles'
- A configuration profile is a collection of settings which can be applied to devices managed by Endpoint Manager.
- Each profile lets you specify a device's network access rights, overall security policy, antivirus scan schedule and other settings.
- Profiles can be created and managed separately for iOS, Android, Mac OS, Windows and Linux devices.
- Once created, a profile can be applied to an individual device, to a group of devices, to a user, to a user group, or designated as a 'default' profile.
- You can also create new profiles by cloning or importing a profile.
  - Note - Please don't confuse Endpoint Manager profiles with **Apple DEP profiles**. DEP profiles are only for enrolling devices to Apple's Device Enrollment Program. Endpoint Manager profiles are for day-to-day device management.

**Create a configuration profile**

- Click the 'Configuration Templates' > 'Profiles'

- Click 'Create' from the options at the top



The 'Create' drop-down lets you add new profiles for Android, iOS Mac OS, Windows and Linux devices.

- You can create as many profiles as you want for different use-cases.
- You can apply multiple profiles to a single device. The most restrictive policy will prevail if there is a conflict in settings.
    - For example, if one profile allows the use of camera and another restricts its use, the device will not be able to use the camera.
- You can create a new Windows profile by defining security settings for each component of Comodo Client Security (CCS). In addition, you can import the current CCS configuration from an endpoint to use as a profile for other endpoints.
- The interface also allows you to export an existing Windows profile in .cfg format. You can import the profile at a later time for re-use or modification.

See the following sections for help with OS-specific profiles:

- **Profiles for Android Devices**
- **Profiles for iOS Devices**
- **Profiles for Mac OS Devices**
- **Profiles for Linux Devices**
- **Profiles for Windows Devices**
- **Import Windows Profiles**

## 6.1.1. Profiles for Android Devices

Android profiles let you configure a device's network access rights, security restrictions, scan schedule and other settings.

**Process in brief:**

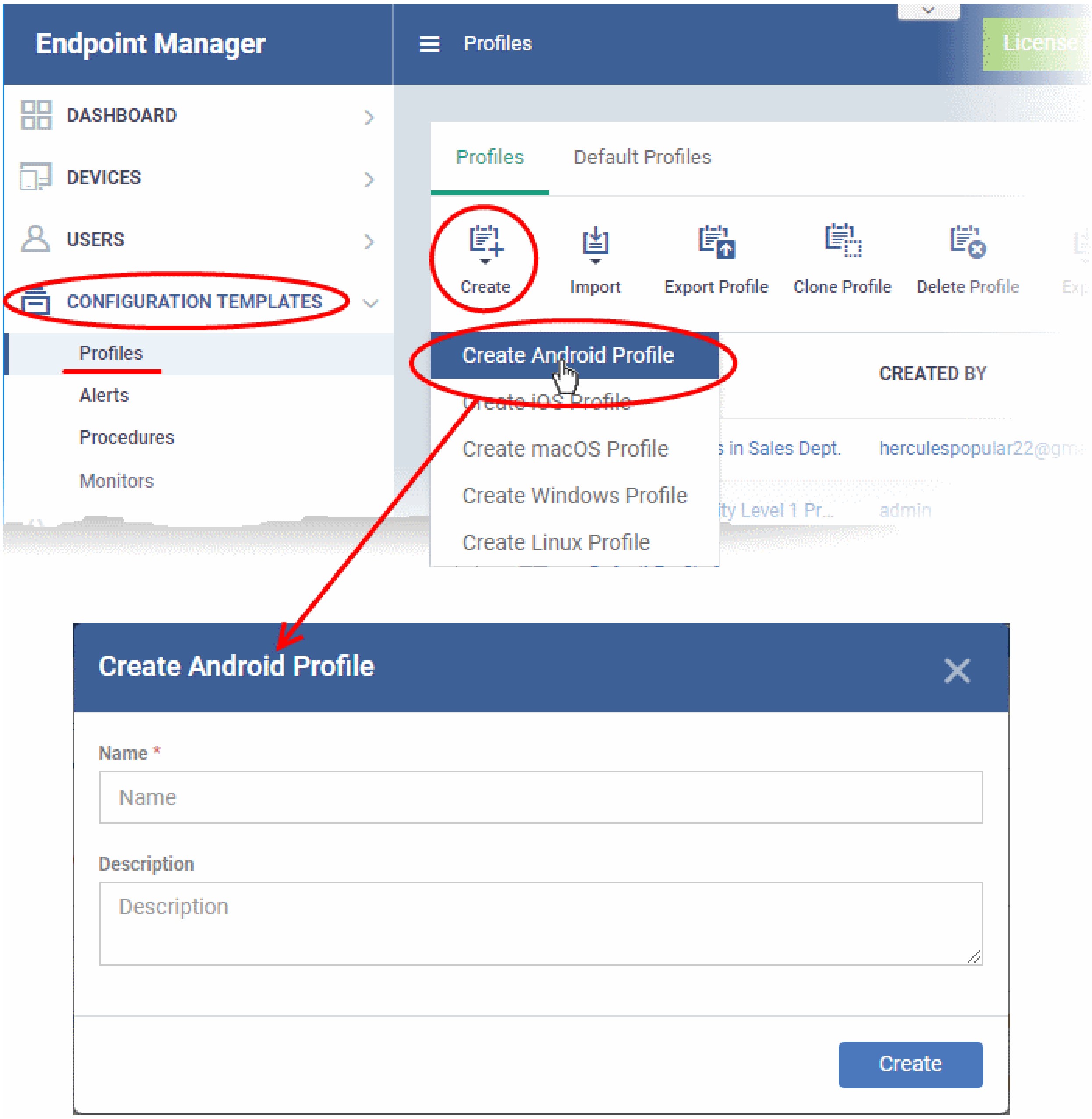
- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create Android Profile'
- Type a name and description for your profile then click the 'Create' button. The profile now appears in 'Configuration Templates' > 'Profiles'.

- New profiles have only one section - 'General'. Click 'Add Profile Section' to add settings for various security and management features. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices, device groups, users and user groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

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

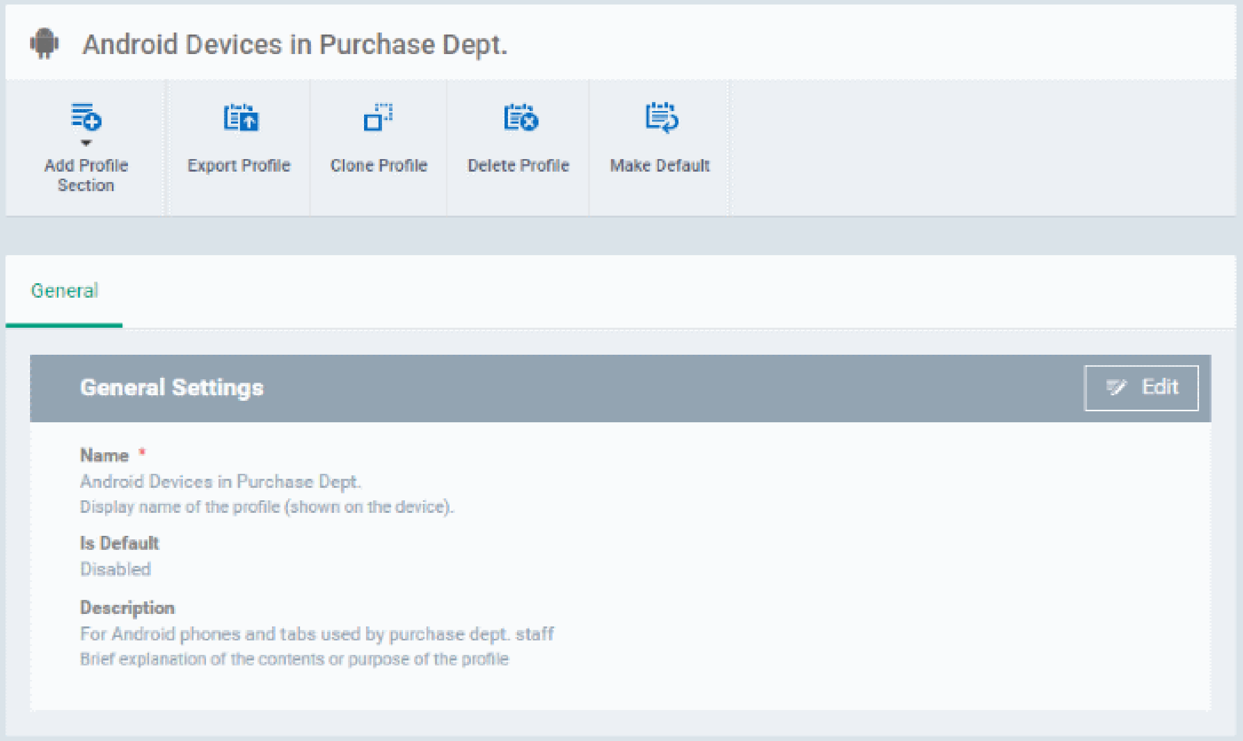
**Create an Android profile**

- Click 'Configuration Templates' > 'Profiles'
- Click the 'Create' button > 'Create Android Profile':



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

The Android profile is created and the 'General Settings' section is displayed. The new profile is not a 'Default Profile' by default.



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

Is Default
Disabled

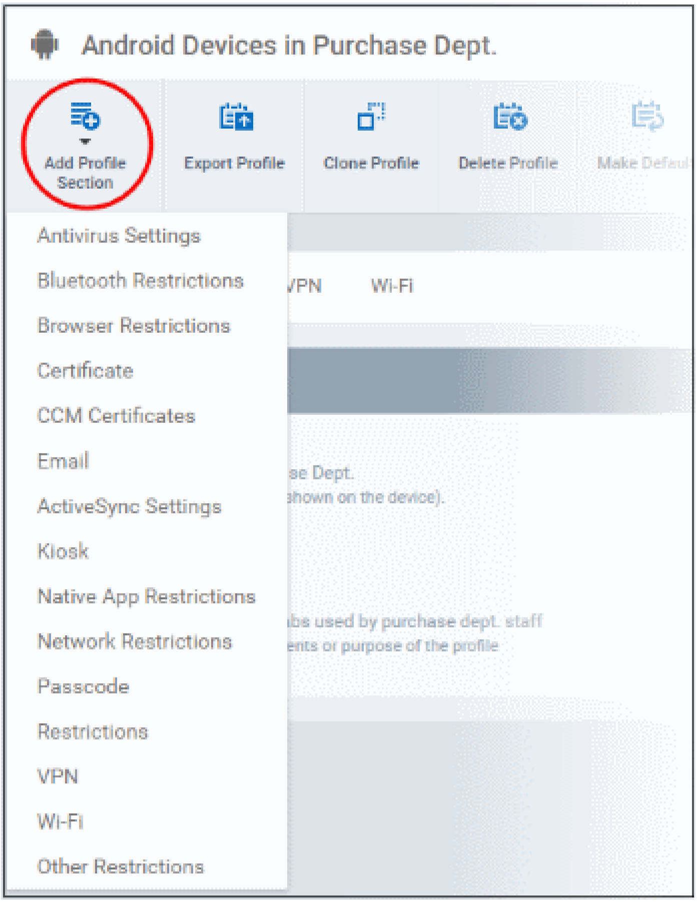
Description
For Android phones and tabs used by purchase dept. staff
Brief explanation of the contents or purpose of the profile

- A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- Click the 'Make Default' button if you want this profile to be a default.
  - Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable 'Is Default'.
- Click 'Save'.

**Tip**: You can set any profile as a default in the 'Profiles' screen. See **Edit Configuration Profiles** for more details.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific security or management feature.
- For example, there are profile sections for 'Browser Restrictions', 'Antivirus Settings', 'Network Restrictions', 'VPN' and so on.
- You can add as many different sections as you want when building your device profile.
- To get started:
  - Click 'Add Profile Section'
  - Select the security component that you want to include in the profile:

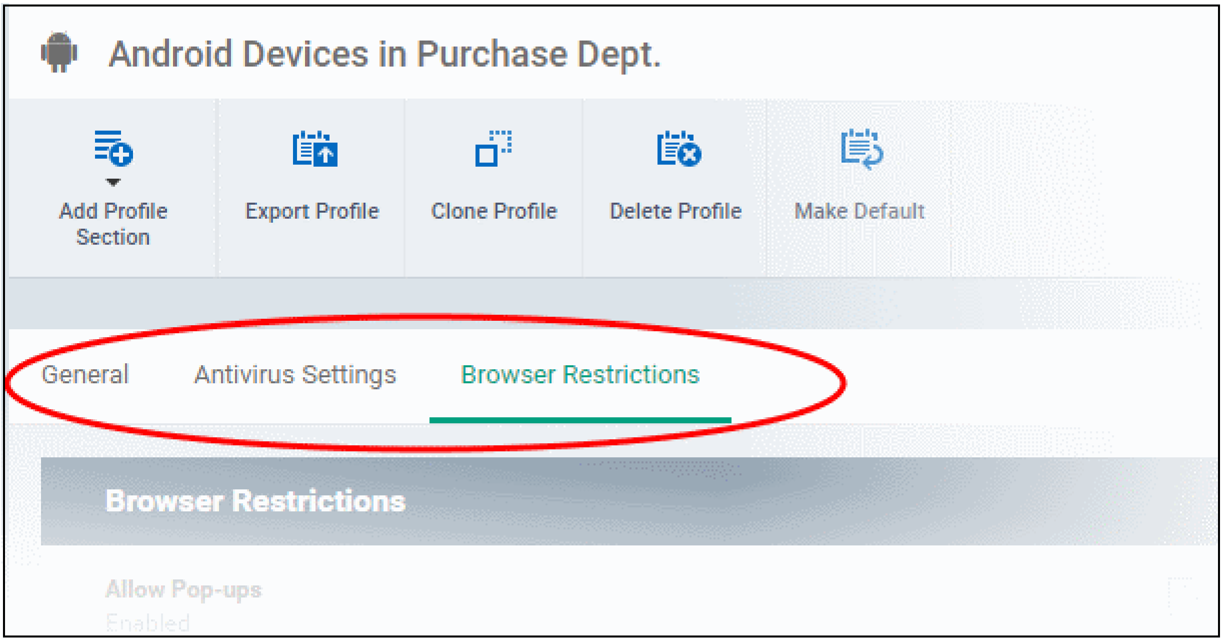


**Note**: Many Android profile settings have small information boxes next to them which indicate the OS and/or device required for the setting to work correctly.

For example, the following box indicates that the setting supports KNOX 2.0+ (Samsung For Enterprises) devices and tablets only

KNOX 2.0+/Tablets only

The settings screen for the selected component is shown. After saving, it is available as a link at the top.

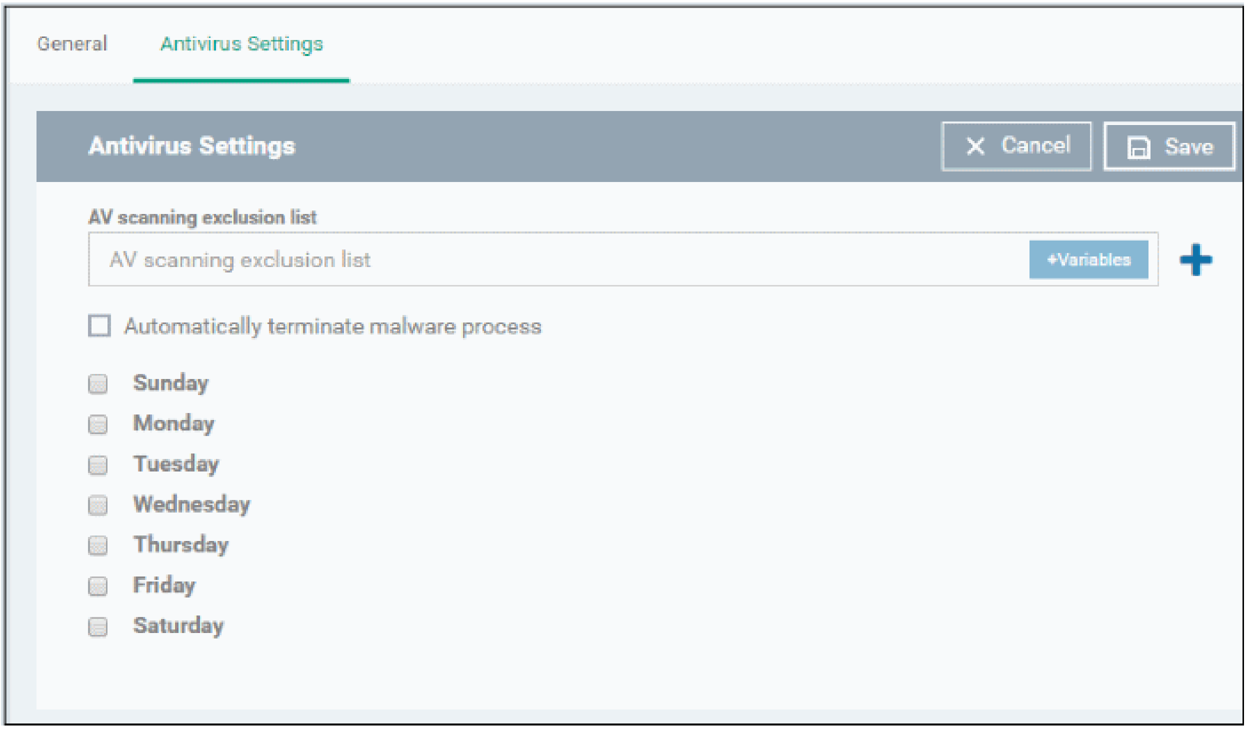


The following sections explain more about each of the sections:

- Antivirus
- Bluetooth Restrictions
- Browser Restrictions
- Certificate
- Email
- Active Sync
- Kiosk
- Native App Restrictions
- Network Restrictions
- Passcode
- Restrictions
- VPN
- Wi-Fi
- Other Restrictions

### Configure Antivirus settings

- Click 'Antivirus Settings' in the 'Add Profile Section' drop-down



AV scanning exclusion list

AV scanning exclusion list

□ Automatically terminate malware process

□ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

| Antivirus Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| AV scanning exclusion list | Text Field | Lets you add trusted apps.<br>Trusted apps are excluded from real-time, on-demand and scheduled antivirus scans run on the devices. You can add apps installed from the Google Play Store and apps installed through the EM App store.<br>• Enter the bundle identifier of the app that you want to exclude from antivirus scanning.<br>For more details on getting the bundle identifier for an app, see the **explanation** given below this table.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>• Click + to add more 'AV scanning exclusions list' fields.<br>• Click − to remove an item from the 'AV scanning exclusion list ' field. |
| Automatically terminate malware process | Checkbox | If enabled, any malware found is stopped from running.<br>From this point it might be ignored (allowed to remain on the device) or uninstalled, depending on the settings in **Android client antivirus settings**.<br>To view these settings, click:<br>'Settings' > 'Portal Set-Up' > 'Client Settings' > 'Android' > 'Antivirus' |
| Schedule scan | Checkbox | Select if you want to automate the process of antivirus scanning. Select the checkbox beside the day(s) that you want the scheduled scan to run. |

- Click the 'Save' button.

The settings are saved and shown under the 'Antivirus Settings' tab. You can edit settings or remove the 'Antivirus Settings' section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## Obtain Bundle/Package Identifier

The bundle identifier is a string that identifies the .apk package used to install the app.

**For Google Play Apps**:

The bundle identifier can be found at the end of the app's Google Play download URL.

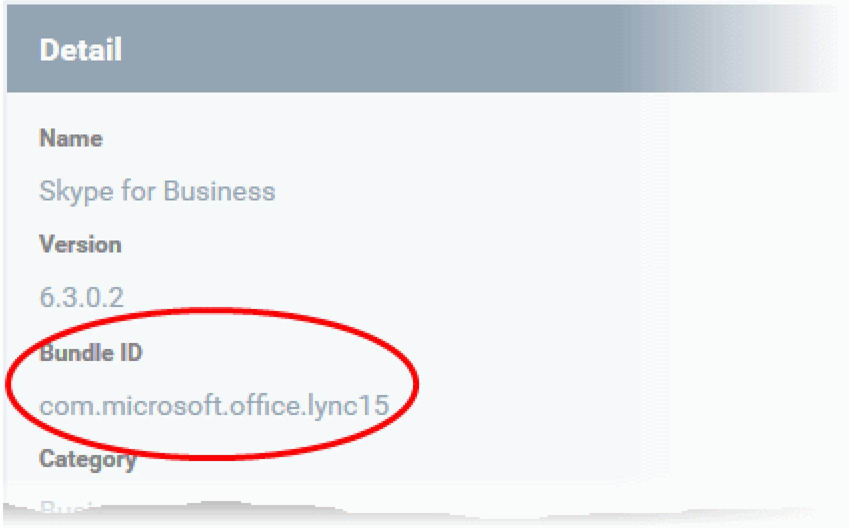
For example, 'com.comodo.batterysaver' is the Comodo Battery Saver app id in the URL

**https://play.google.com/store/apps/details?id=com.comodo.batterysaver**

**For Enterprise Apps installed through EM App Store:**

The bundle identifier can be viewed from the App Details screen of the App.

- Click 'App Store' from the left and choose Android
- Click on the app from the list displayed at the right



Detail

Name

Skype for Business

Version

6.3.0.2

Bundle ID

com.microsoft.office.lync15

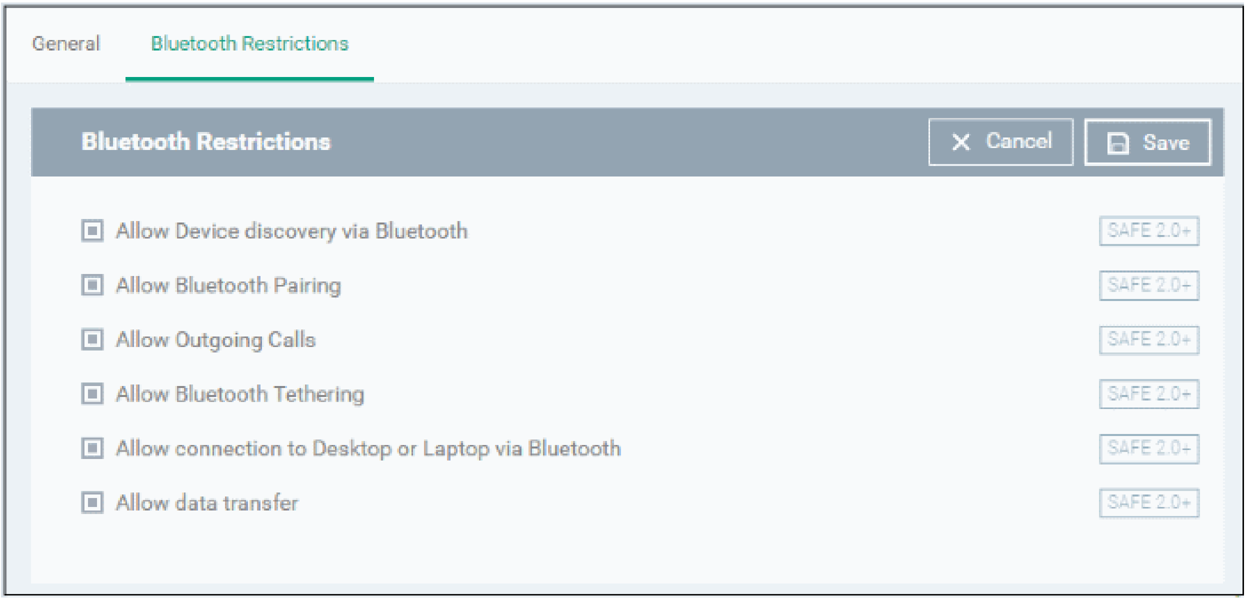
Category

The bundle identifier is displayed in the 'Bundle ID' field.

### Configure Bluetooth Restrictions settings

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

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



- ▣ Allow Device discovery via Bluetooth SAFE 2.0+
- ▣ Allow Bluetooth Pairing SAFE 2.0+
- ▣ Allow Outgoing Calls SAFE 2.0+
- ▣ Allow Bluetooth Tethering SAFE 2.0+
- ▣ Allow connection to Desktop or Laptop via Bluetooth SAFE 2.0+
- ▣ Allow data transfer SAFE 2.0+

| Bluetooth Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow Device discovery via Bluetooth | Checkbox | Allows discovery of other devices via Bluetooth. |
| Allow Bluetooth Pairing | Checkbox | Allows users' devices to pair with other their devices via Bluetooth. |
| Allow Outgoing Calls | Checkbox | Allows users to make calls using Bluetooth enabled devices (eg. hands-free devices) |
| Allow Bluetooth Tethering | Checkbox | Allows users to enable/disable Bluetooth tethering option. |
| Allow connection to Desktop or Laptop via Bluetooth | Checkbox | Allow users to enable/disable Bluetooth connection with Desktop or Laptop. |

| Bluetooth Restrictions Settings - Table of Parameters | | |
|---|---|---|
| Allow data transfer | Checkbox | Allows data transfer between devices via Bluetooth. |

- Click the 'Save' button.

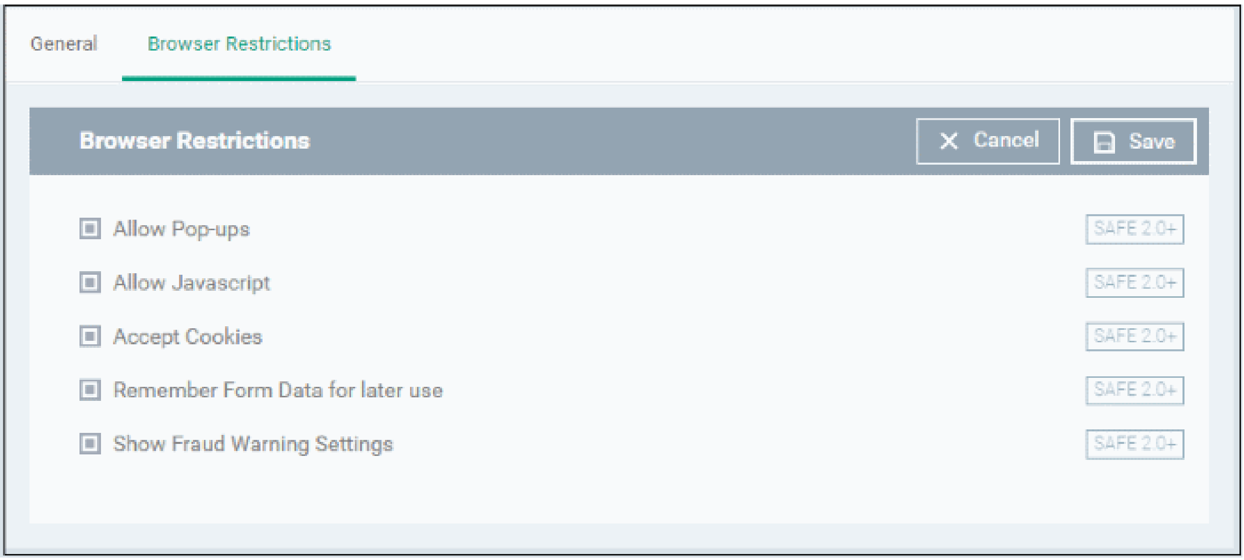
The settings are saved and shown under the 'Bluetooth Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Browser Restrictions settings

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

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

The 'Browser Restrictions' settings screen will be displayed.



□ Allow Pop-ups SAFE 2.0+
□ Allow Javascript SAFE 2.0+
□ Accept Cookies SAFE 2.0+
□ Remember Form Data for later use SAFE 2.0+
□ Show Fraud Warning Settings SAFE 2.0+

| Browser Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow Pop-ups | Checkbox | Pop-ups in browsers will be allowed on user devices. |
| Allow Javascript | Checkbox | Java scripts will be allowed on user devices |
| Accept Cookies | Checkbox | Users will be allowed to modify Cookies settings on their devices. |
| Remember Form Data for later use | Checkbox | Users will be allowed to use Auto Fill settings on their devices. |
| Show Fraud Warning Settings | Checkbox | Users will be allowed to view Fraud Warning Settings on their devices. |

- Click the 'Save' button.

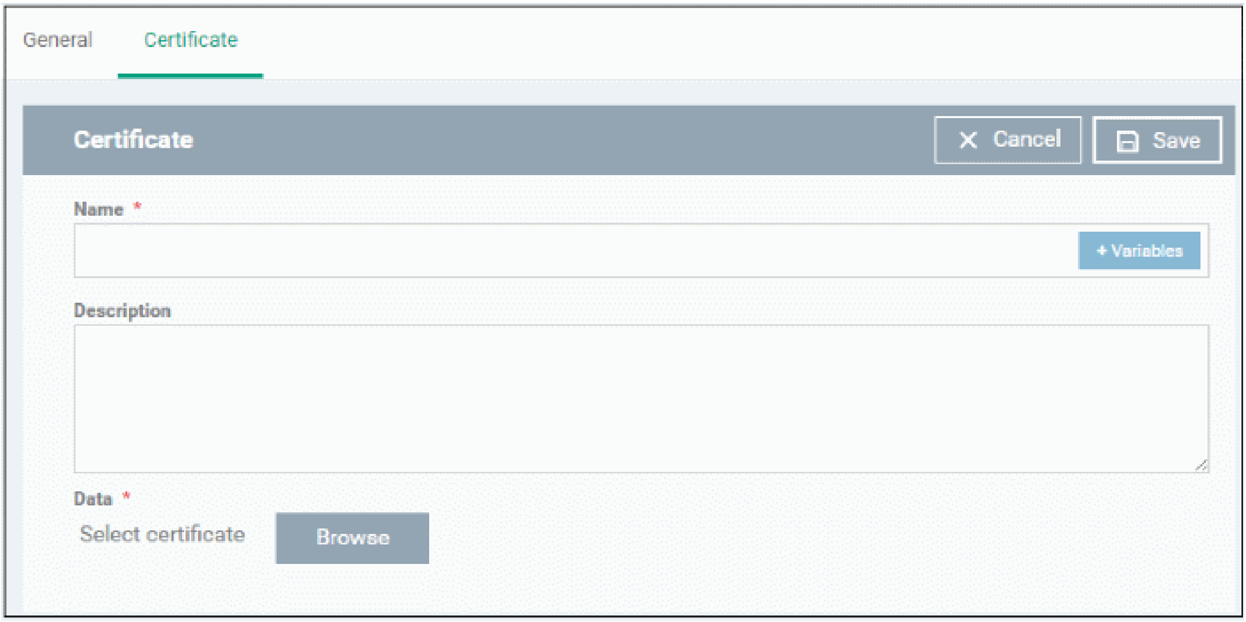
The settings are saved and shown under the 'Browser Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Certificate settings

The 'Certificate' settings section is used to upload certificates and will act as a repository from which certificates can be selected for use in other areas like 'Wi-Fi, 'Exchange Active Sync' and 'VPN'.

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

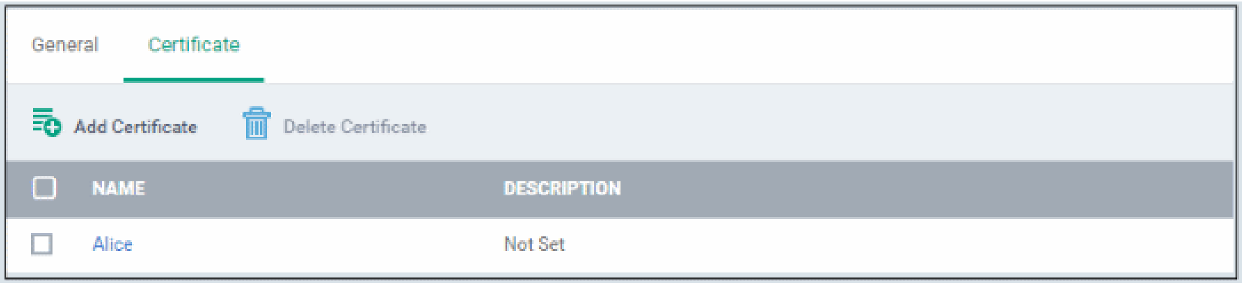
The 'Certificate' settings screen will be displayed.



| Certificate Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text Field | Enter the label of the certificate.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Description | Text Field | Enter an appropriate description for the certificate. |
| Data | Browse button | Browse to the location of the stored certificate and select the certificate.<br>**Note**: Only certificate files with extensions 'pub', 'crt' or 'key' can be uploaded. |

- Click the 'Save' button.

The certificate will be added to the certificate store.



| ☐ | NAME | DESCRIPTION |
|---|---|---|
| ☐ | Alice | Not Set |

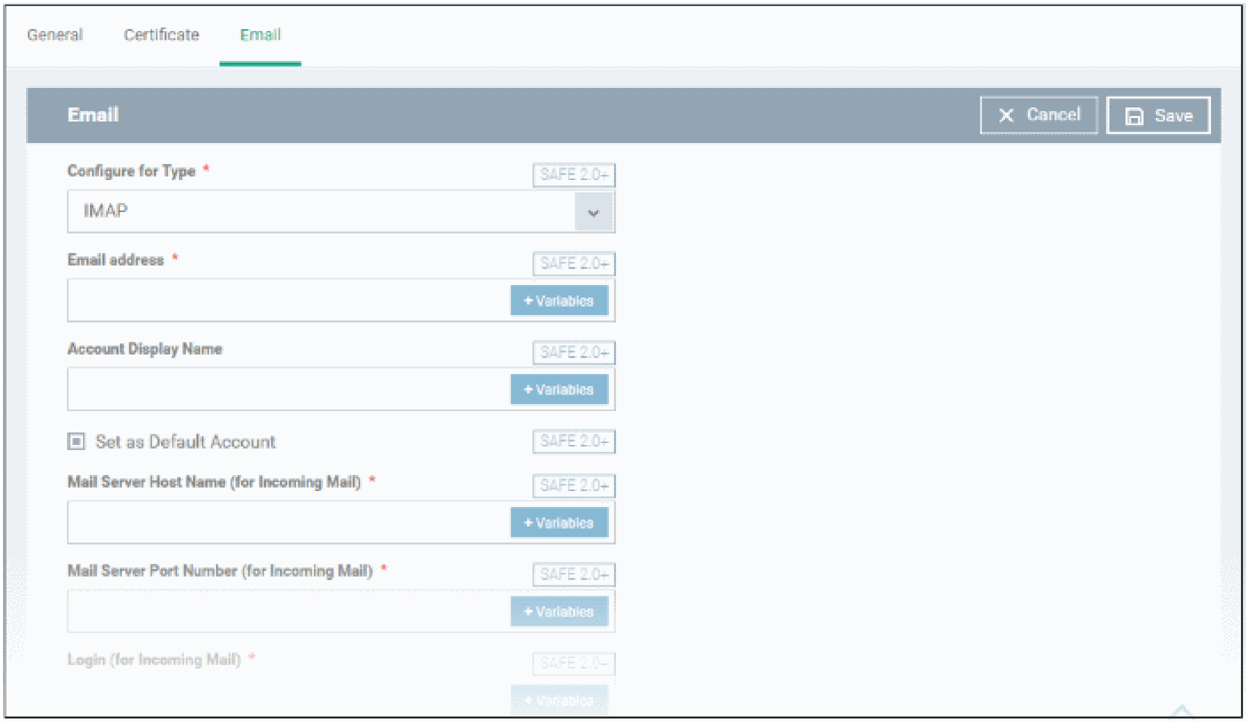
- Click 'Add Certificate' and repeat the process to add more certificates.
- Click on the name of the certificate to view the certificate key and edit the name

You can add any number of certificates to the profile and remove certificates at anytime. See **Edit Configuration Profiles** for more details.

## Configure Email settings

**Note**: The feature is supported for Samsung for Enterprise (SAFE) devices only. This area allows administrators to configure email settings on devices.

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



Configure for Type *: IMAP

Email address *

Account Display Name

□ Set as Default Account

Mail Server Host Name (for Incoming Mail) *

Mail Server Port Number (for Incoming Mail) *

Login (for Incoming Mail) *

| 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 | Enter the email address of the user at the incoming mail server If the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>The email address of the users to whom the profile is associated are automatically added to the profile while rolling out the same to the devices.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Account Display Name | Text Field | Enter a label to identify the user's email account at the incoming mail server, if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |

| Email Settings - Table of Parameters | | |
|---|---|---|
| | | The email address of the users to whom the profile is associated are automatically added to the profile while rolling out the same to the devices. |
| Set as Default Account | Checkbox | The email account is set as default for the users. |
| Mail Server Host Name (for Incoming Mail) * | Text Field | Enter the host name or IP address of the incoming mail server, if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Mail Server Port Number (for Incoming Mail) * | Text Field | Enter the server port number used for incoming mail service for a single user,<br>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.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Login (for Incoming Mail)* | Text Field | Enter the username for the email account of the user at the incoming mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>The email usernames of the users to whom the profile is associated are automatically added to the profile while rolling out to the devices. |
| Password (for Incoming Mail)* | Text Field | Enter the password for the email account of the user at the incoming mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>The email passwords of the users to whom the profile is associated are automatically added to the profile while rolling out to the devices. |
| Use SSL Incoming | Checkbox | Communication between incoming mail server and devices is encrypted using SSL (Secure Socket Layer Protocol). |
| Accept All Certificates (for Incoming Mail) | Checkbox | The device automatically accepts all SSL certificates from the incoming mails. |
| Accept TLS Certificates (for Incoming Mail) | Checkbox | The device automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol) from the incoming mails. |
| Mail Server Host Name (for Outgoing mail)* | Text box | Enter the host name or IP address of the outgoing (SMTP) mail server for a single user.<br>Click the variables button + Variables to insert dynamic values if the |

| Email Settings - Table of Parameters | | |
|---|---|---|
| | | profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Mail Server Port Number (for Outgoing Mail) * | Text box | Enter the server port number used for outgoing (SMTP) mail service, if the profile is for single user.<br>If no port number is specified then ports 25, 587 and 465 are used in the given order.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Login (for outgoing Mail)* | Text Field | Enter the username for the email account of the user at the outgoing (SMTP) mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>The email usernames of the users to whom the profile is associated are automatically added to the profile while rolling out to the devices. |
| Password (for outgoing Mail)* | Text Field | Enter the password for the email account of the user at the outgoing (SMTP) mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>The email passwords of the users to whom the profile is associated are automatically added to the profile while rolling out to the devices. |
| Use SSL (for Outgoing Mail) | Checkbox | Communication between outgoing mail server and devices is encrypted using SSL. |
| Accept All Certificates (for Outgoing Mail) | Checkbox | The device automatically accepts all SSL certificates from outgoing mails. |
| Accept TLS Certificates (for Outgoing Mail) | Checkbox | The device  automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol) from outgoing mails. |
| Sender Name | Text Field | Enter the name that should appear in the 'From' field of the sent emails from the device if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Set Signature | Text Field | Enter the signature and other details that appears at the end of the mails sent from the device.<br>Click the variables button + Variables to insert dynamic values if the |

| Email Settings - Table of Parameters | | |
|---|---|---|
| | | profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Prevent Moving Mail to other Accounts | Checkbox | The user cannot move sent or received mails to another account. |
| Always Vibrate on New Email Notification | Checkbox | The device vibrates in addition to sound alert when a new email is received. |
| Vibrate on New Email Notification if device is silent | Checkbox | The device vibrates when a new email is received, when the device is in silent mode. |

- Click the 'Save' button.

The settings are saved and shown under the 'Email' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

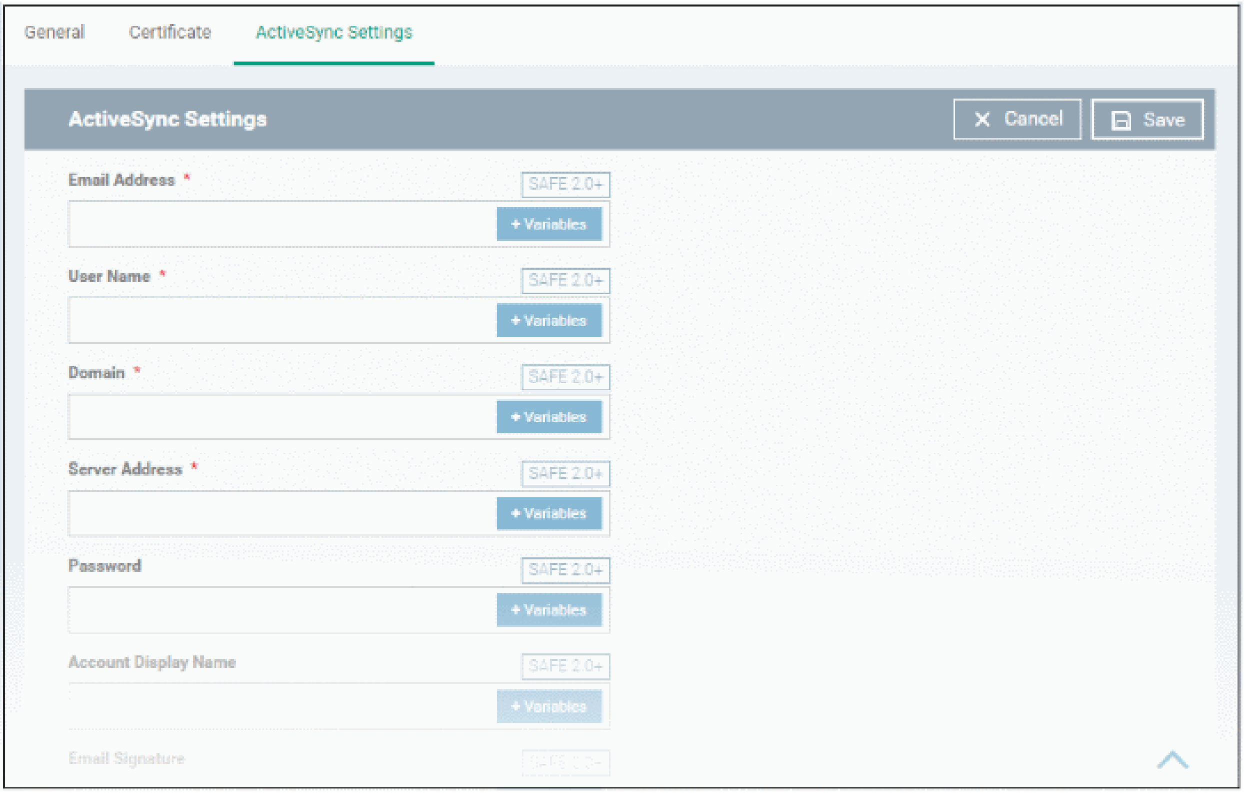
### Configure ActiveSync settings

ActiveSync settings allows you to configure user access to Exchange Server mail accounts.

**Note**: Please make sure users are not blocked from using the email client on their devices in **Native App Restrictions**

- Click 'ActiveSync Settings' from the 'Add Profile Section' drop-down

The 'ActiveSync Settings' screen will be displayed.



| ActiveSync Settings - Table of Parameters | | |
|---|---|---|
| Form Element | Type | Description |

| ActiveSync Settings - Table of Parameters | | |
|---|---|---|
| Email Address * | Text Field | Click the 'Variables' button + Variables and click + beside '%u.mail' from the User Variables' list. The email address of the users to whom the profile is associated are automatically filled. For more details on variables, see **Create and Manage Custom Variables**. |
| User Name * | Text Field | Click the 'Variables' button + Variables and click + beside '%u.login' from the User Variables' list. The username of the users to whom the profile is associated are automatically filled. For more details on variables, see **Create and Manage Custom Variables**. |
| Domain * | Text Field | Enter the domain name in the field.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Server Address * | Text Field | Enter the server address of the ActiveSync.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Password | Text Field | Leave the field blank. The user needs 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 | Enter a label to identify the user's email account at the exchange server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Email Signature | Text Field | Enter the signature and other details that appears at the end of the mails sent from the device.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on 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.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on 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 | Communication between the device and the exchange server is encrypted using SSL (Secure Socket Layer Protocol). |
| As default account | Checkbox | The email address is used as default for sending out emails. |
| Accept all certificates | Checkbox | The device automatically accepts all SSL certificates. |
| Can sync contacts | Checkbox | Allows synchronization of user contacts between device and exchange server. |

| ActiveSync Settings - Table of Parameters | | |
|---|---|---|
| Can sync calendar | Checkbox | Allows synchronization user created calendar events between the device and the exchange server. |
| Can sync tasks | Checkbox | Allows synchronization of user scheduled tasks between the device and the exchange server. |
| Manual roaming sync | Checkbox | The user can use the sync feature manually while away from the home network. |
| Always vibro on new email | Checkbox | The device will vibrate when a new email is received. |

Fields with * are mandatory.

- Click the 'Save' button.

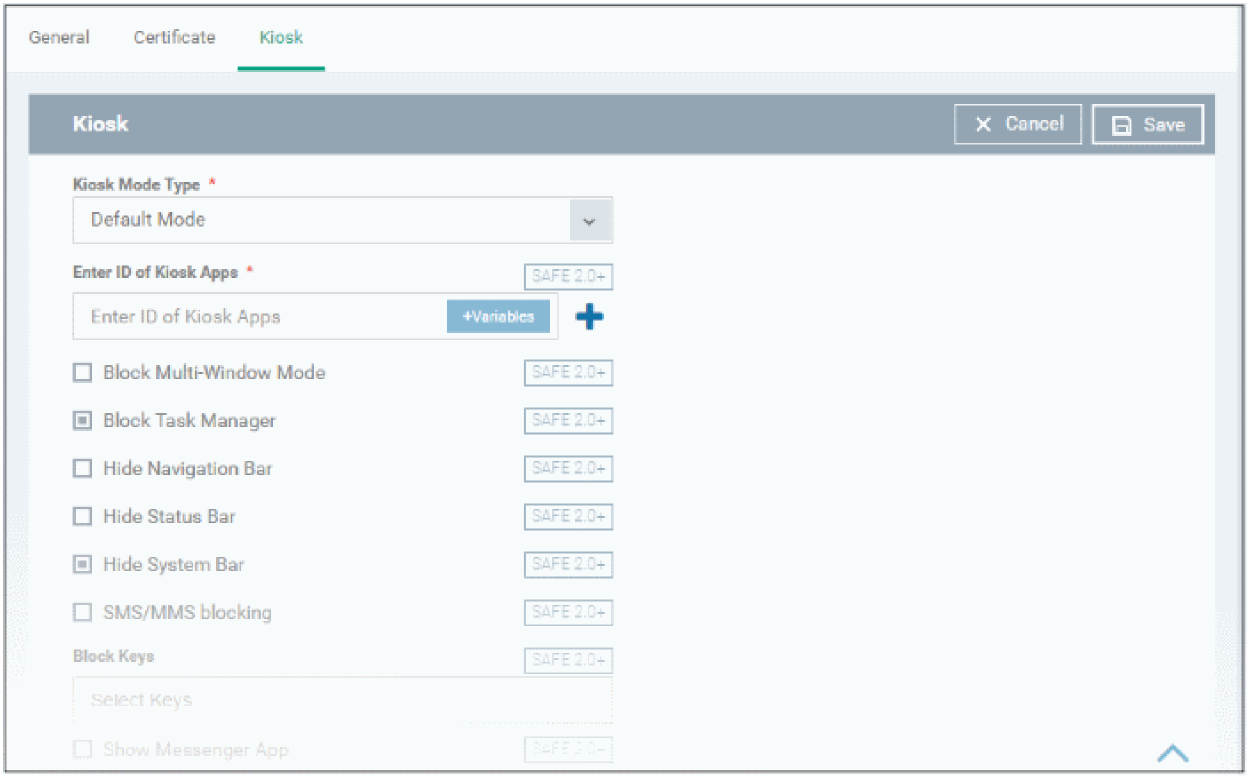
The settings are saved and shown under the 'ActiveSync Settings' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Kiosk settings

**Note**: This feature is only supported by Samsung for Enterprise (SAFE) devices.

**Background**: Kiosk mode is a feature intended to help administrators lock-down mobile devices by limiting the applications that are able to run on a device. 'Locking' a device to particular applications can prevent users from opening other applications or straying into important device configuration areas. You can also block aspects of the OS should you wish. An example is a retail or school environment where only certain apps should be used on the device.

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



Kiosk Mode Type *: Default Mode

Enter ID of Kiosk Apps * SAFE 2.0+: Enter ID of Kiosk Apps

□ Block Multi-Window Mode SAFE 2.0+

☑ Block Task Manager SAFE 2.0+

□ Hide Navigation Bar SAFE 2.0+

□ Hide Status Bar SAFE 2.0+

☑ Hide System Bar SAFE 2.0+

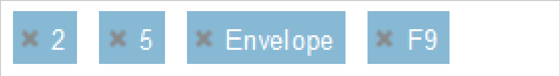
□ SMS/MMS blocking SAFE 2.0+

Block Keys SAFE 2.0+: Select Keys

□ Show Messenger App SAFE 2.0+

| Kiosk Settings - Table of Parameters | | |
|---|---|---|
| Form Element | Type | Description |

| Kiosk Settings - Table of Parameters | | |
|---|---|---|
| Kiosk Mode Type | Drop-down | The two Kiosk modes are:<br>- 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.<br>- 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 EM console.<br>Restrictions on access to other device functions, such as task manager and the status bar, can also be configured for either mode. |
| If 'Single App' is selected as Kiosk Mode Type: | | |
| Enter ID of Kiosk Apps | Text Field | Enter the Package ID of the app that will run in Kiosk mode.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>See **Obtain Bundle/Package Identifier** ror more details on Package ID. |
| If 'Default mode' is selected as Kiosk Mode Type: | | |
| Enter ID of Kiosk Apps | Text Field | Enter the package IDs of the apps that will run in Kiosk mode.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>See **Obtain Bundle/Package Identifier** ror more details on Package ID.<br>Click ✚ to add more app IDs.<br>Click the ▬ button to remove an item from the list |
| Block Multi-Window Mode | Checkbox | Users cannot open multiple windows. |
| Block Task Manager | Checkbox | Users cannot access task manager screen. |
| Hide Navigation Bar | Checkbox | The navigation bar is not shown on the devices. |
| Hide System Bar | Checkbox | The system bar is not shown on the devices. |
| SMS/MMS blocking | Checkbox | All SMSs and MMSs to the device are blocked. |
| Block Keys | Drop-down | This feature lets you selectively block touch keys and icons available on device screen.<br>For example, if you do not want the device owners to use 'Caps Lock' key you can block it.<br>Click in the 'Block Keys' field:<br> <br>Select Keys<br>Scroll down to view the full list and select the key. |

| Kiosk Settings - Table of Parameters | | |
|---|---|---|
| | |  ✖ 2 ✖ 5 ✖ Envelope ✖ F9<br>Repeat the process to add more keys to the blocked keys list. |
| The following features are visible if 'Default mode' is selected as Kiosk Mode Type: | | |
| Show messenger App | Checkbox | Allows the messenger app on the device. |
| Show email App | Checkbox | Allows the email app on the device. |
| Show dialer App | Checkbox | Allows the phone dialer app on the device. |
| Show admin bypass button | Checkbox | Adds the 'Admin bypass' button to the device screen. The user can tap the button and enter the password to exit from the Kiosk mode. |
| Admin bypass password | Text Field | Enter the password required to exit the Kiosk mode.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

- Click the 'Save' button.

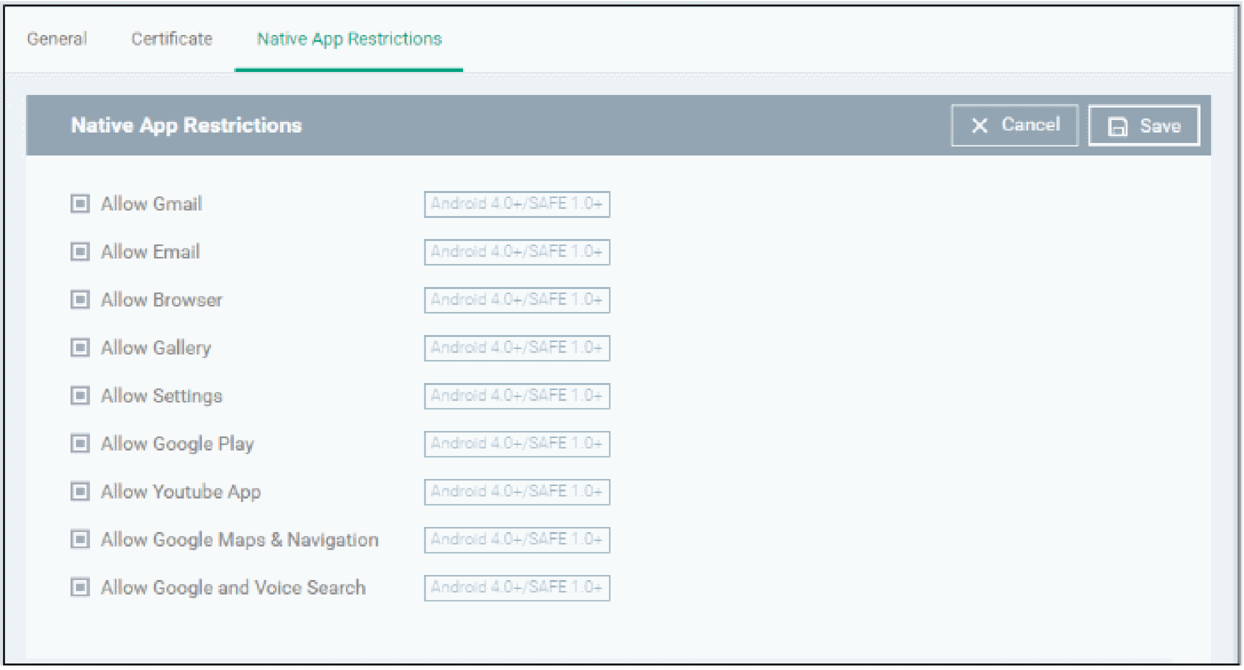
The settings are saved and shown under the 'Kiosk' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Native App Restriction settings

Native applications are those applications that come with the device operating system. Examples include the email and gallery apps. Admins can restrict users from accessing these native applications if required.

| **Note**: Native app restrictions are only available on Samsung which support KNOX 1.0 + |
|---|

- Click 'Add Profile Section' > 'Native App Restrictions'



☐ Allow Gmail Android 4.0+/SAFE 1.0+
☐ Allow Email Android 4.0+/SAFE 1.0+
☐ Allow Browser Android 4.0+/SAFE 1.0+
☐ Allow Gallery Android 4.0+/SAFE 1.0+
☐ Allow Settings Android 4.0+/SAFE 1.0+
☐ Allow Google Play Android 4.0+/SAFE 1.0+
☐ Allow Youtube App Android 4.0+/SAFE 1.0+
☐ Allow Google Maps & Navigation Android 4.0+/SAFE 1.0+
☐ Allow Google and Voice Search Android 4.0+/SAFE 1.0+

| Native Application Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow Gmail | Checkbox | Users can the access Gmail app. |
| Allow Email | Checkbox | Users can the access the default email app. |
| Allow Browser | Checkbox | Users can access the default Android browser on their devices. |
| Allow Gallery | Checkbox | Users can access Gallery on their devices. |
| Allow Settings | Checkbox | Users can change their device settings. |
| Allow Google Play | Checkbox | Users can access Google Play on their mobile devices. |
| Allow YouTube App | Checkbox | Users can access the YouTube app. |
| Allow Google Maps & Navigation | Checkbox | Users can access Google Maps and Navigation app on their devices. |
| Allow Google and Voice Search | Checkbox | Users can use Google and Voice Search services. |

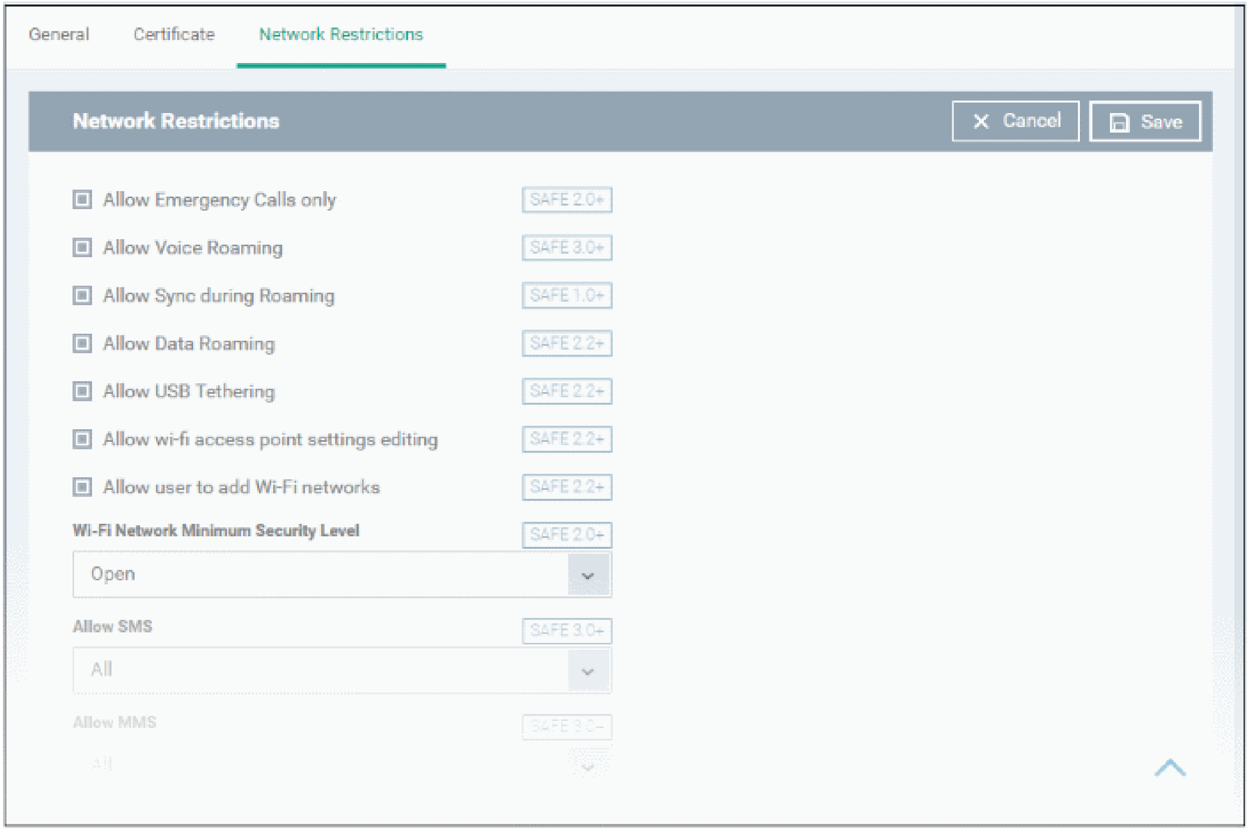
- Click the 'Save' button.

The settings are saved and shown under the 'Native App Restriction' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Network Restriction settings

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

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



▣ Allow Emergency Calls only SAFE 2.0+

▣ Allow Voice Roaming SAFE 3.0+

▣ Allow Sync during Roaming SAFE 1.0+

▣ Allow Data Roaming SAFE 2.2+

▣ Allow USB Tethering SAFE 2.2+

▣ Allow wi-fi access point settings editing SAFE 2.2+

▣ Allow user to add Wi-Fi networks SAFE 2.2+

Wi-Fi Network Minimum Security Level SAFE 2.0+

Open

Allow SMS SAFE 3.0+

All

Allow MMS SAFE 3.0+

All

| Network Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow Emergency Calls only | Checkbox | Allows users to make only emergency calls. |
| Allow Voice Roaming | Checkbox | Allows users to make/receive voice call during roaming. |
| Allow Sync during Roaming | Checkbox | Allows the use of Sync feature while roaming. |
| Allow Data Roaming | Checkbox | Allows users to enable 'Data Roaming' option on their devices to access data services during roaming. |
| Allow USB Tethering | Checkbox | Allows users to enable 'USB Tethering' option for sharing their data connection through USB tethering. |
| Allow Wi-Fi access point settings editing | Checkbox | Allows users to edit the Wi-Fi access point settings to create a Wi-Fi hotspot for sharing their data connection. |
| Allow user to add Wi-Fi networks | Checkbox | Allows users to add additional Wi-Fi networks. |
| Wi-Fi Network Minimum Security Level | Drop-down | Select the minimum security level required for the user to access the Wi-Fi network. The options available are:<br>• Open<br>• WEP<br>• WPA<br>• 802.1x EAP (LEAP)<br>• 802.1x EAP (FAST)<br>• 802.1x EAP (PEAP)<br>• 802.1x EAP (TTLS)<br>• 802.1x EAP (TLS) |
| Allow SMS | Drop-down | Allows text messages as per the option selected:<br>• All - Allows both incoming and outgoing text messages.<br>• Incoming Only - Allows incoming text messages only.<br>• Outgoing Only - Allows outgoing text messages only.<br>• None - Both incoming and outgoing text messages are blocked. |
| Allow MMS | Drop-down | Allows multimedia messages as per the option selected:<br>• All - Allows both incoming and outgoing multimedia messages.<br>• Incoming Only - Allows incoming multimedia messages only.<br>• Outgoing Only - Allows outgoing multimedia messages only.<br>• None - Both incoming and outgoing multimedia messages are blocked. |
| Blacklisted SSIDs | Text Field | Specify the name (SSID) of the wireless network that should be blacklisted.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>Click the + button to add more 'Blacklisted SSID' fields. |

| Network Restrictions Settings - Table of Parameters | | |
|---|---|---|
| | | Click the minus − button beside an SSID to remove it from the list |

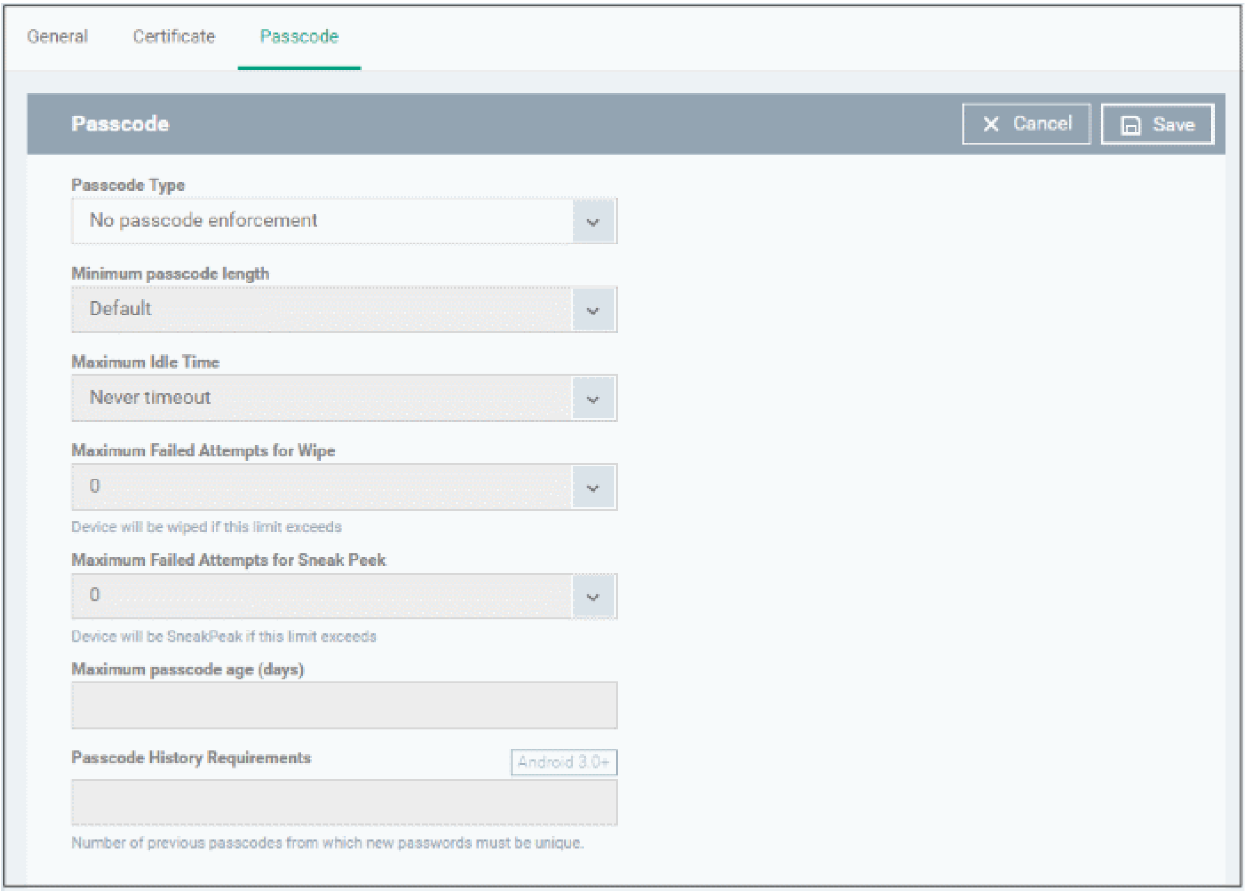
- Click the 'Save' button.

The settings are saved and shown under the 'Network Restrictions' tab. You can edit the settings or remove the section from the profile at anytime See **Edit Configuration Profiles** for more details.

### Configure Passcode settings

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

The Passcode settings screens will be displayed.



Passcode Type: No passcode enforcement

Minimum passcode length: Default

Maximum Idle Time: Never timeout

Maximum Failed Attempts for Wipe: 0

Device will be wiped if this limit exceeds

Maximum Failed Attempts for Sneak Peek: 0

Device will be SneakPeak if this limit exceeds

Maximum passcode age (days)

Passcode History Requirements (Android 3.0+)

Number of previous passcodes from which new passwords must be unique.

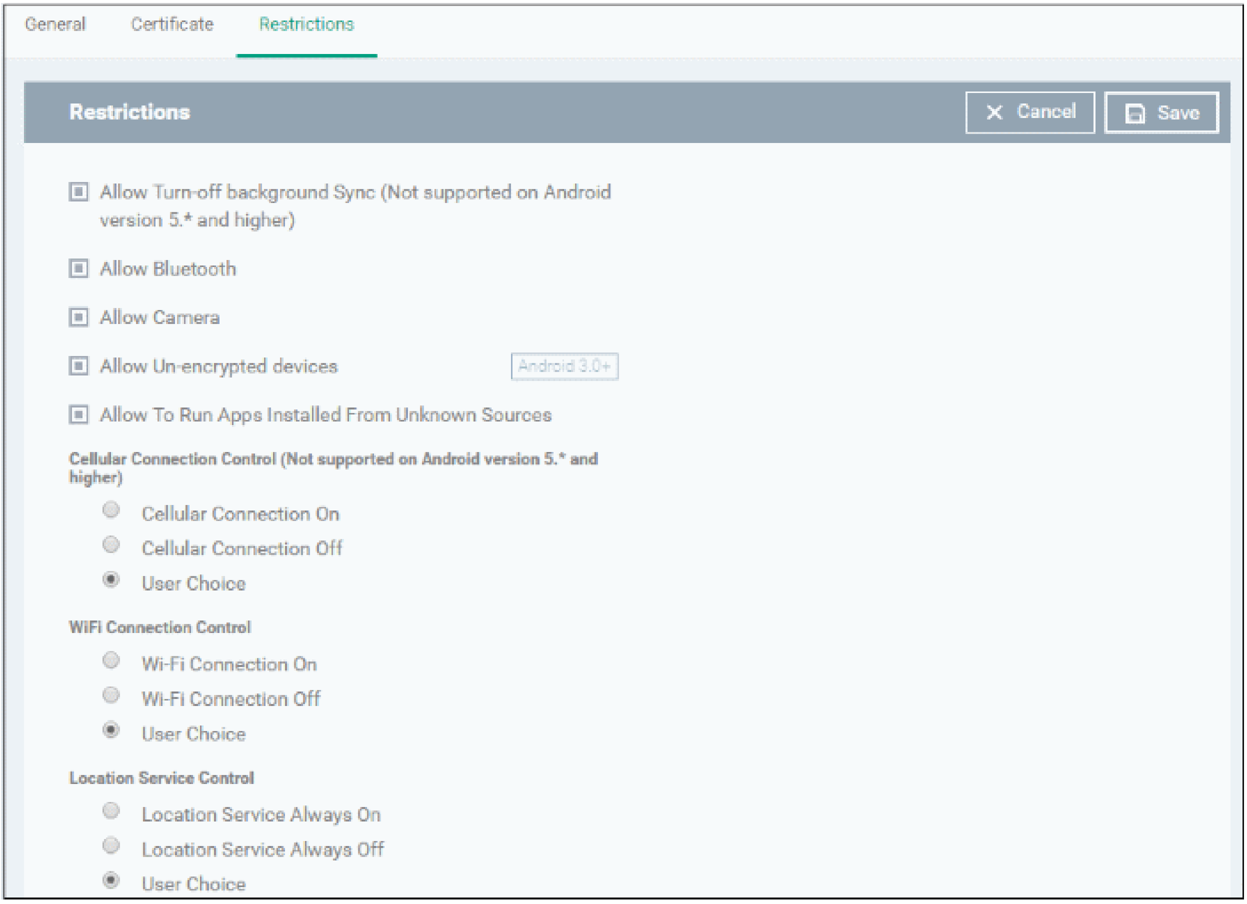
| Passcode Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Passcode Type | Drop-down | Select the type of passcode from the drop-down that the user should configure for unlocking screen lock. The options available are:<br>No passcode enforcement<br>Only letters<br>Letters and numbers<br>Only numbers<br>Letters, numbers and a special symbol<br>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.<br>If the number of failed attempts crosses this value, the data in the device will be automatically wiped off. This is useful to prevent the data from the device being stolen, if somebody, other than the user, tries to login to the device by entering guessed passcodes. |
| Maximum Failed Attempts for Sneak Peek | Drop-down | Select the maximum number of allowed unsuccessful login attempts for 'Sneak Peek' feature (4-16). Set the value as '0' for unlimited.<br>The 'Sneak Peek' feature makes the device take a photograph with the front-facing camera if the wrong passcode is entered a certain number of times - hopefully getting a picture of the person holding a lost/stolen device. Photographs are forwarded to the EM server.<br>The photograph(s) sent by the device can be viewed from the 'Device Details' interface that can be accessed by clicking 'Devices' > 'Device List' > the device name > 'Sneak Peek' tab. See **View Sneak Peek Pictures to Locate Lost Devices** for more details.<br>**Note**: If the device does not have a front camera, the rear camera will capture a photograph and forward to the EM server. |
| Maximum Passcode Age (days) | Text Field | Enter the maximum period in days for which a passcode can be valid. After the number of days specified in this field, the passcode will expire. The user needs to change the passcode before the current one expires. |
| Passcode History Requirements | Text Field | Set how many unique, new passcodes must be created before the user can re-use an old password.<br>This feature is available for Android 3.0 and later versions only. |

- Click the 'Save' button.

The settings are saved and shown under the 'Passcode' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## Configure Restriction settings

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



☑ Allow Turn-off background Sync (Not supported on Android version 5.* and higher)

☑ Allow Bluetooth

☑ Allow Camera

☑ Allow Un-encrypted devices Android 3.0+

☑ Allow To Run Apps Installed From Unknown Sources

Cellular Connection Control (Not supported on Android version 5.* and higher)

○ Cellular Connection On
○ Cellular Connection Off
● User Choice

WiFi Connection Control

○ Wi-Fi Connection On
○ Wi-Fi Connection Off
● User Choice

Location Service Control

○ Location Service Always On
○ Location Service Always Off
● User Choice

| Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow Turn-off background Sync | Checkbox | Select this to allow users to disable background synchronization setting on their devices. |
| Allow Bluetooth | Checkbox | Select this to allow users to enable/disable Bluetooth on their devices. |
| Allow Camera | Checkbox | Select this to allow users to use the camera |
| Allow Un-encrypted devices | Checkbox | Select this to enable users to use device without turning on the storage encryption feature. This feature is available for Android 3.0 and later versions only. |
| Allow to run Apps installed from unknown sources | Checkbox | Select this to allow users to run installed applications that were download from unknown sources |
| Cellular Connection Control | Radio Buttons | Choose whether or not to allow the device to connect to the internet through a cellular network (2G/3G/4G):<br>• Cellular Connection on - Maintains the data connection through cellular network enabled, irrespective of user settings under 'Settings' > 'Wireless and Network settings' in the device.<br>• Cellular Connection off - Maintains the data connection through cellular network disabled, irrespective of user settings under |

| Restrictions Settings - Table of Parameters | | |
|---|---|---|
| | | 'Settings' > 'Wireless and Network settings' in the device.<br>• User Choice - The connection is enabled or disabled as per the user's setting under 'Settings' > 'Wireless and Network settings' in the device. |
| WiFi Connection Control | Radio Buttons | Choose whether or not to allow the device to connect to WiFi networks and hotspots from the options.<br>• WiFi Connection on - Always maintains the WiFi connection enabled, irrespective of user's setting under 'Settings' > 'Wireless and Network settings' in the device.<br>• WiFi Connection off - Always maintains the WiFi connection disabled, irrespective of user's setting under 'Settings' > 'Wireless and Network settings' in the device.<br>• User Choice - The connection is enabled or disabled as per the user's setting under 'Settings' > 'Wireless and Network settings' in the device. |
| Location Service Control | Radio Buttons | Choose whether or not to allow the location services on the device from the options:<br>• Location Service Always On - Always maintains the location services enabled, irrespective of the user's setting on the device.<br>• Location Service Always Off - Always maintains the location services disabled, irrespective of the user's setting on the device.<br>• User Choice - The location service is enabled or disabled as per the user's setting on the device. |

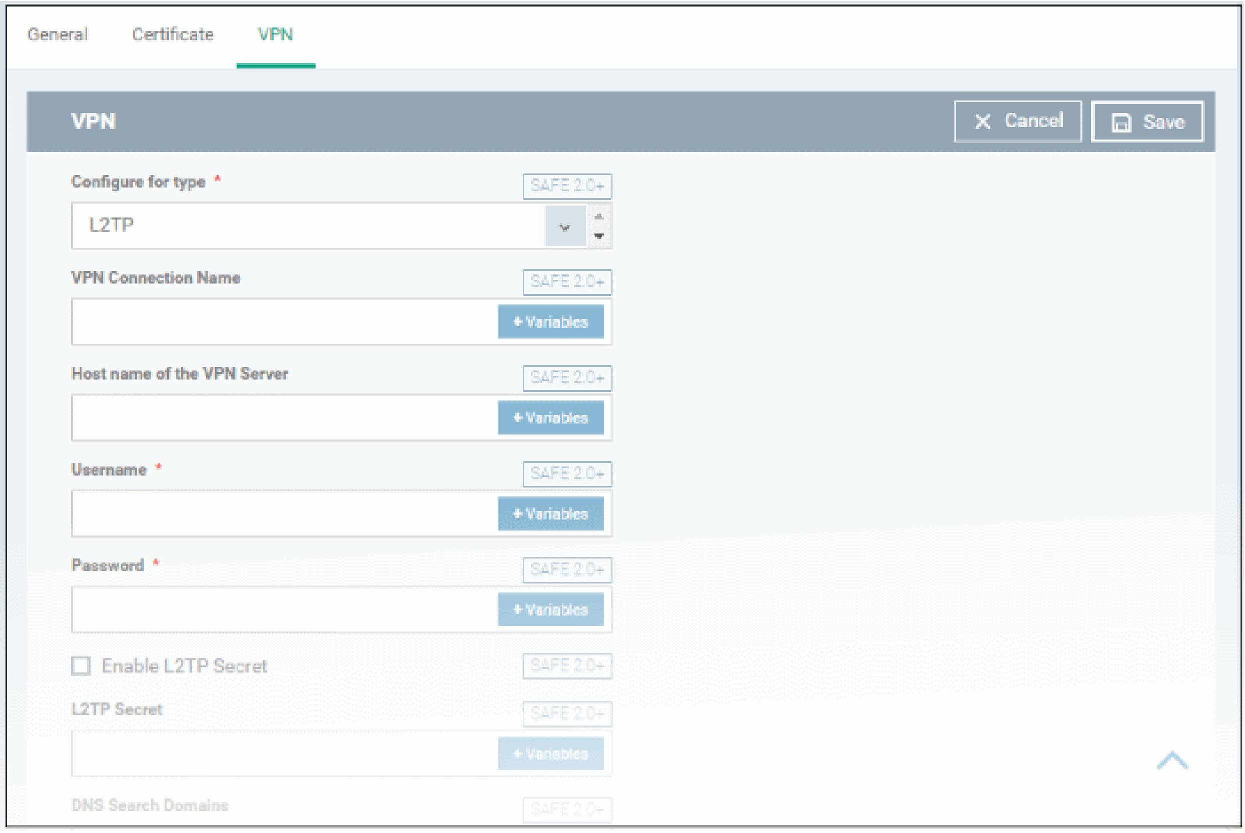
- Click the 'Save' button.

The settings are saved and shown under the 'Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure VPN settings

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

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



Configure for type *

L2TP

VPN Connection Name

Host name of the VPN Server

Username *

Password *

□ Enable L2TP Secret

L2TP Secret

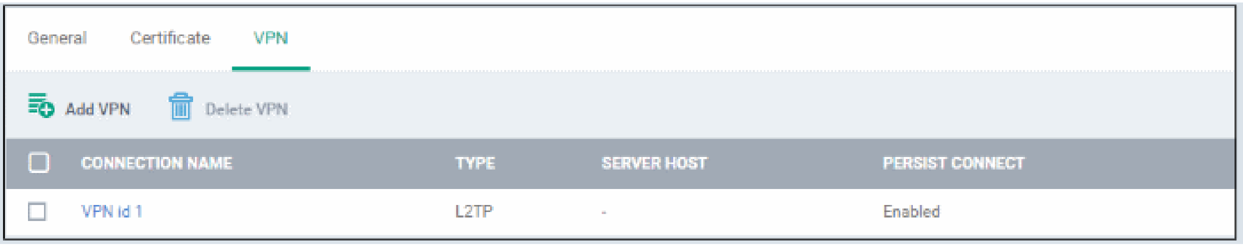
DNS Search Domains

| Form Element | Description |
|---|---|
| Configure for type | Choose the VPN connection type from drop-down. The options available are:<br>• L2TP,<br>• PPTP,<br>• L2TP/IPSec PSK,<br>• IPSec, XAuth PSK<br>• IPSec XAuth RSA. |
| VPN Connection Name | Enter a label for the connection. This is shown on the device.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Host name of the VPN Server | Enter the IP address or host name of the VPN server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Username / Password | Enter the login credentials for the device to connect to the VPN server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| DNS Search Domains | Enter the IP address or hostname of the DNS server that devices will use for searching domain names.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

| Form Element | Description |
|---|---|
| For **L2TP** | |
| • Enable L2TP Secret | If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret |
| • L2TP Secret | If L2TP Secret is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables' |
| For **PPTP** | |
| • Enable Encryption | If selected, the connection is encrypted between the devices and the VPN server. |
| For **L2TP/IPSec PSK** | |
| • Enable L2TP Secret | If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret |
| • L2TP Secret | If L2TP Secret is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables' |
| • IPSec Pre-Shared Key | If IP Sec Identifier is enabled, then the pre-shared key should be entered here by the user or selected from 'Variables' |
| For **IPSec Xauth PSK** | |
| • IP Sec Identifier | Enter the IPSec identifier in the field.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| • IPSec Pre-Shared Key | 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 | 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:<br>• 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. See **Edit Configuration Profiles** for more details.<br>• Suits to all VPN connections types, except PPTP<br>• The VPN server and the DNS server should have been specified by their IP addresses in IPv4. |

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

The VPN connection setting is added to the profile.



| □ | CONNECTION NAME | TYPE | SERVER HOST | PERSIST CONNECT |
|---|---|---|---|---|
| □ | VPN id 1 | L2TP | - | Enabled |

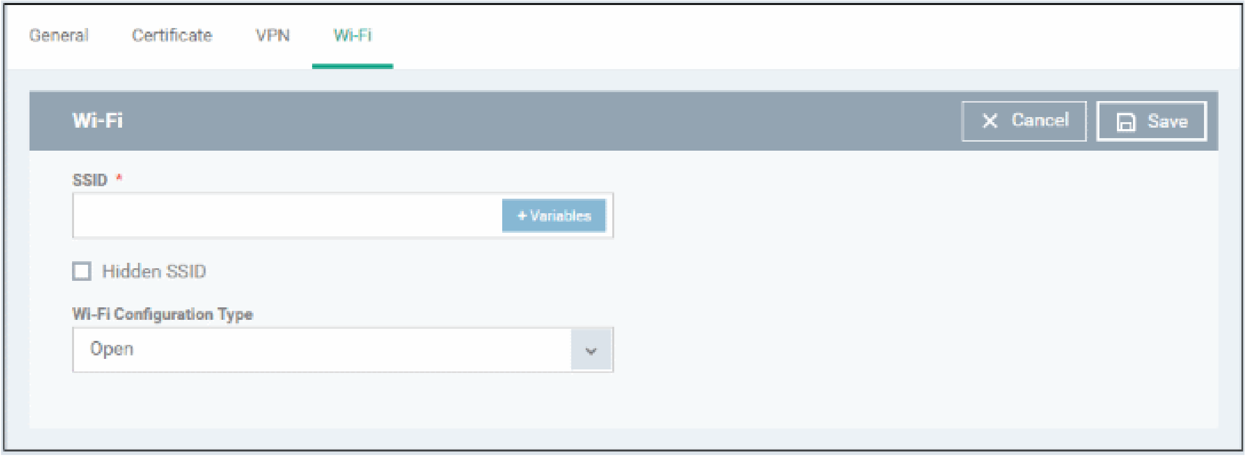
- Click 'Add VPN' and repeat the process to add more VPN connections.

- Click the name of a connection to view and edit its settings

You can add any number of VPN connection settings to the profile at anytime. See **Edit Configuration Profiles** for more details.

### Configure Wi-Fi settings

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



| 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.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Hidden SSID | Checkbox | If enabled, users will be able to access the hidden wireless network too. Users must know the hidden SSID details and the required credentials. |
| Wi-Fi Configuration Type | Drop-down | Select the type of encryption used by the wireless network from the drop-down. The options available are:<br>• Open<br>• WEP<br>• WPA / WPA2 - PSK<br>• 802.1x EAP<br>The settings for each type is explained in the next table **Wi-Fi configuration type settings**. |

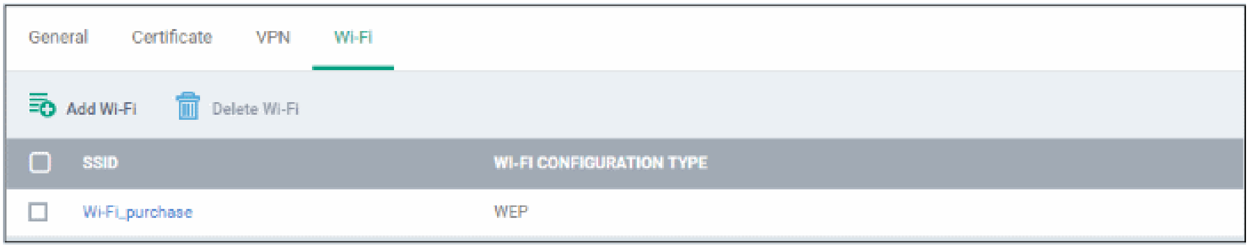
### Wi-Fi Configuration Type settings

| Wi-Fi Configuration Type Settings - Table of Parameters | |
|---|---|
| **Security Configuration Type** | **Description** |
| Open | No password is required for accessing the Wi-Fi network by the user. |
| WEP | Authentication Password - Enter the password to access the Wi-Fi network.<br>Click the variables button + Variables to insert dynamic values. See **Create and** |

| Wi-Fi Configuration Type Settings - Table of Parameters | |
|---|---|
| | Manage Custom Variables for more details on variables. |
| WPA / WPA2 - PSK | Authentication Password - Enter the password to access the Wi-Fi network.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| 802.1x EAP | **1. EAP Authentication Protocol** - Select the EAP authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.<br>• PEAP<br>• TLS<br>• TTLS<br>**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.<br>• None<br>• PAP<br>• MSCHAP<br>• MSCHAPV2<br>• GTC<br>**3. Certificate -** Select the user certificate from the drop-down or upload it using the 'Add New' button.<br>4. **CA Certificate** - Select the CA certificate from the drop-down or upload it using the 'Add New' button.<br>5. **Authentication Username -** Enter the username for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.<br>6. **Authentication Password -** Enter the password for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.<br>7. **Authentication Domain** - Enter the details for RADIUS Server authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.<br>8. **Anonymous Identity** - Enter the username that can be used for anonymous access. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.<br>9. **Encryption Key** - Enter the encryption key to access the Wi-Fi network.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

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

The 'Wi-Fi' network' is saved to the profile.



| □ | SSID | WI-FI CONFIGURATION TYPE |
|---|---|---|
| □ | Wi-Fi_purchase | WEP |

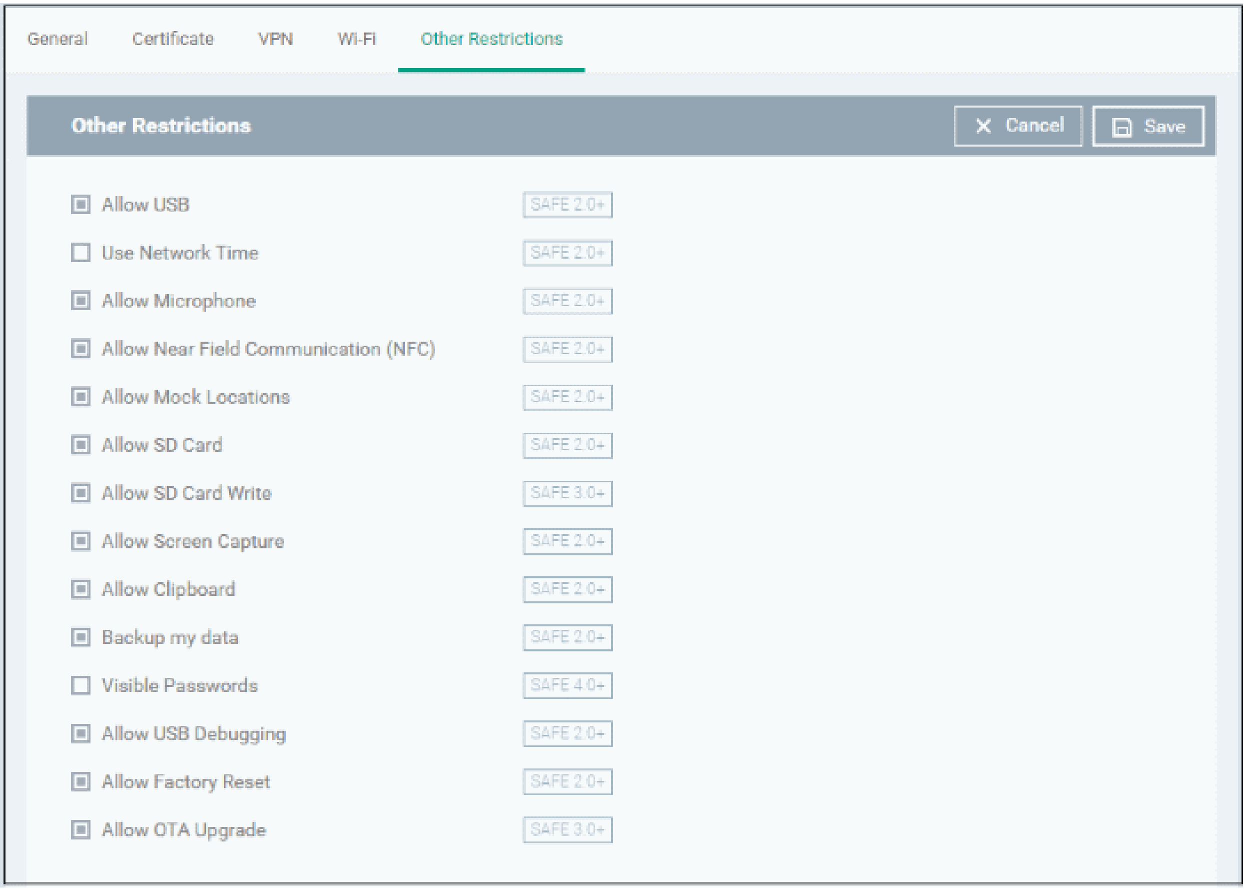
- Click 'Add Wi-Fi' and repeat the process to add more Wi-Fi networks.
- Click the SSID of the network  to view and edit its settings.

You can add or remove Wi-Fi networks at any time. See **Edit Configuration Profiles** for more details.

### Configure 'Other Restrictions' settings

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

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



☑ Allow USB SAFE 2.0+
□ Use Network Time SAFE 2.0+
☑ Allow Microphone SAFE 2.0+
☑ Allow Near Field Communication (NFC) SAFE 2.0+
☑ Allow Mock Locations SAFE 2.0+
☑ Allow SD Card SAFE 2.0+
☑ Allow SD Card Write SAFE 3.0+
☑ Allow Screen Capture SAFE 2.0+
☑ Allow Clipboard SAFE 2.0+
☑ Backup my data SAFE 2.0+
□ Visible Passwords SAFE 4.0+
☑ Allow USB Debugging SAFE 2.0+
☑ Allow Factory Reset SAFE 2.0+
☑ Allow OTA Upgrade SAFE 3.0+

| Other Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Allow USB | Checkbox | Allows users to establish connections via USB ports. |
| Use Network Time | Checkbox | Allows users to enable/disable network provided values in Date & Time settings. |
| Allow Microphone | Checkbox | Allows users to use microphone. If this is disabled, users can use microphone for receiving and making calls only. |

| Other Restrictions Settings - Table of Parameters | | |
|---|---|---|
| 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 | Allows users to reset the device to factory settings. |
| Allow OTA Upgrade | Checkbox | Allows devices to receive Over-the-air (OTA) upgrade for software updates. |

- Click the 'Save' button.

The settings are saved and shown under 'Other Restrictions' tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## 6.1.2. Profiles for iOS Devices

iOS profiles let you specify a device's network access rights, restrictions and other general settings.

**Process in Brief:**

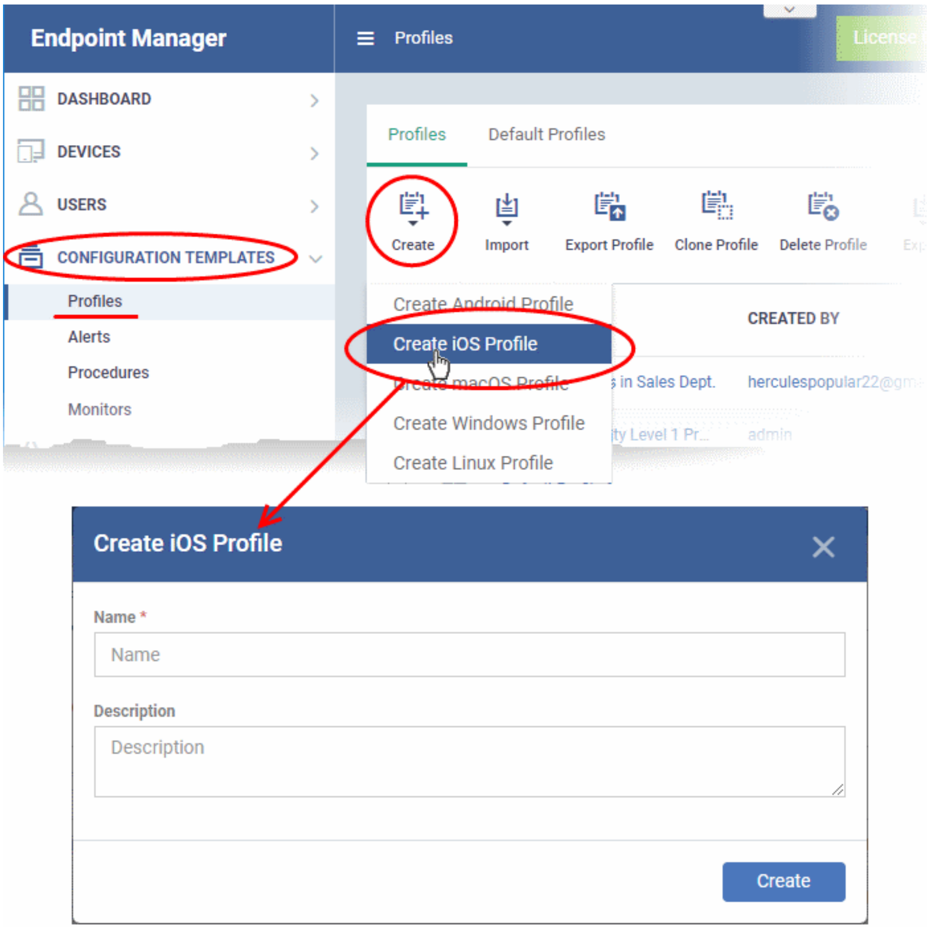
- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create iOS Profile'
- Type a name and description for your profile then click the 'Create' button. The profile will now appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - 'General'. Click 'Add Profile Section' to add settings for various security and management features. Each section you add will appear as a new tab.
- Once you have fully configured your profile you can apply it to devices, device groups, users and user groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.

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

**Create an iOS profile**

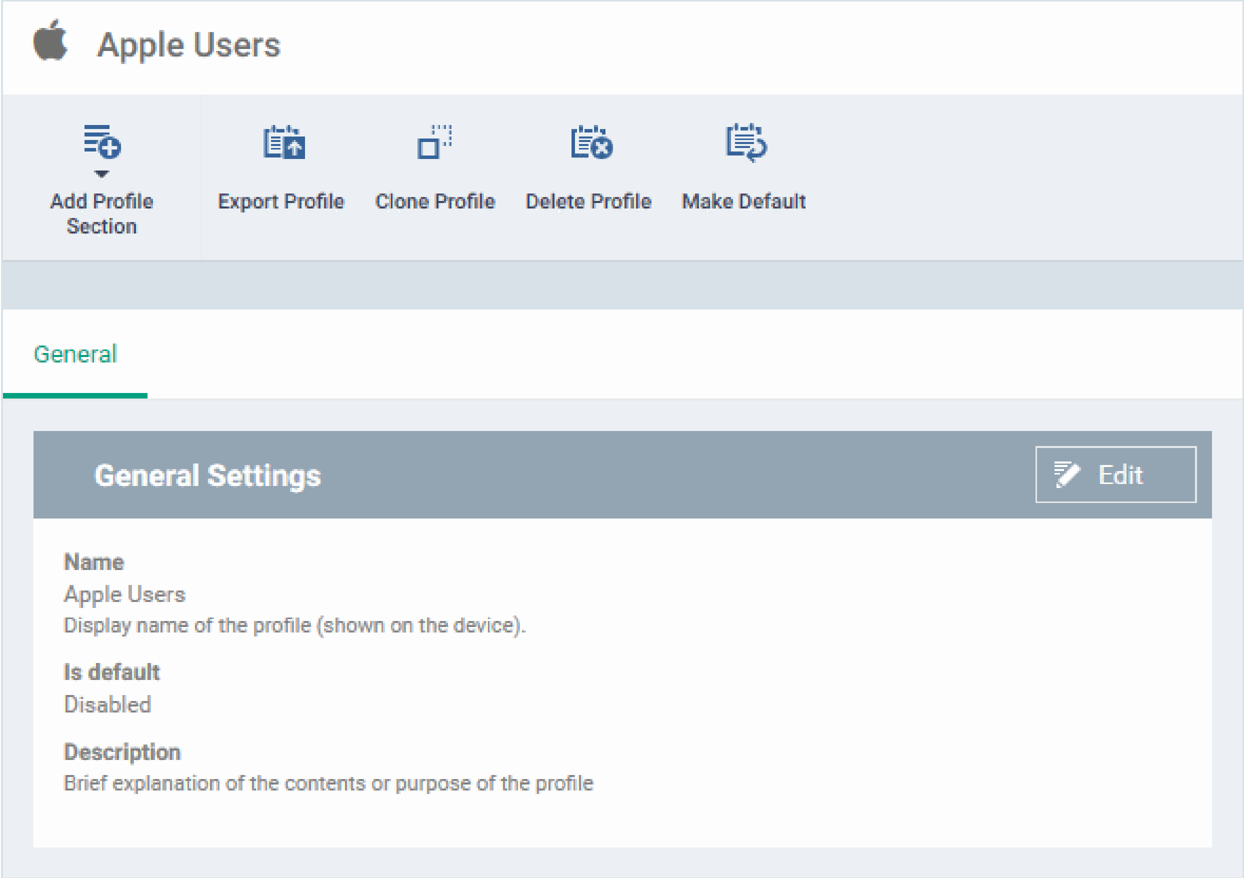
- Click 'Configuration Templates' > 'Profiles'

- Click the 'Create' button > 'Create iOS Profile':



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

The new profile will open at the 'General Settings' section:



Name
Apple Users
Display name of the profile (shown on the device).

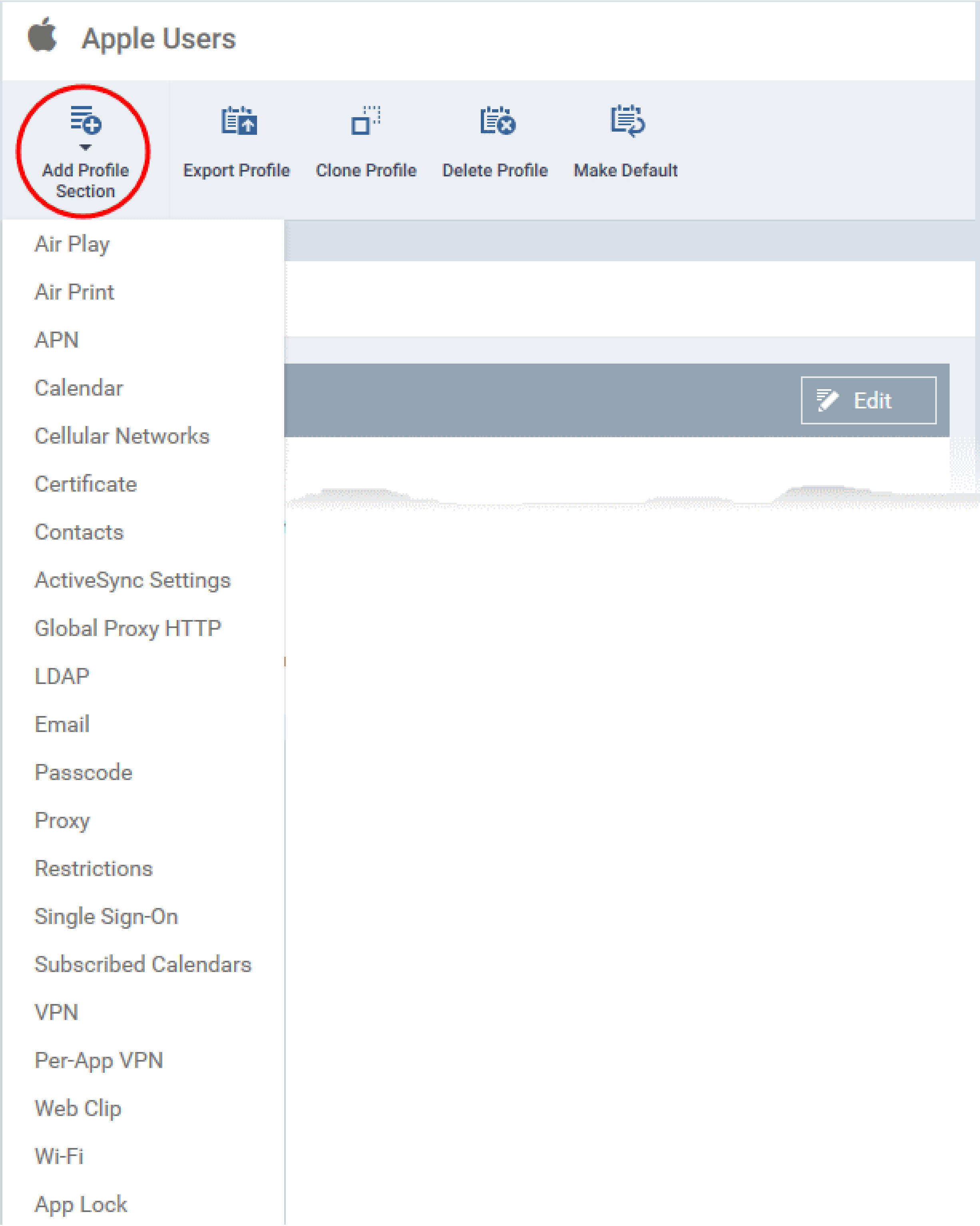
Is default
Disabled

Description
Brief explanation of the contents or purpose of the profile

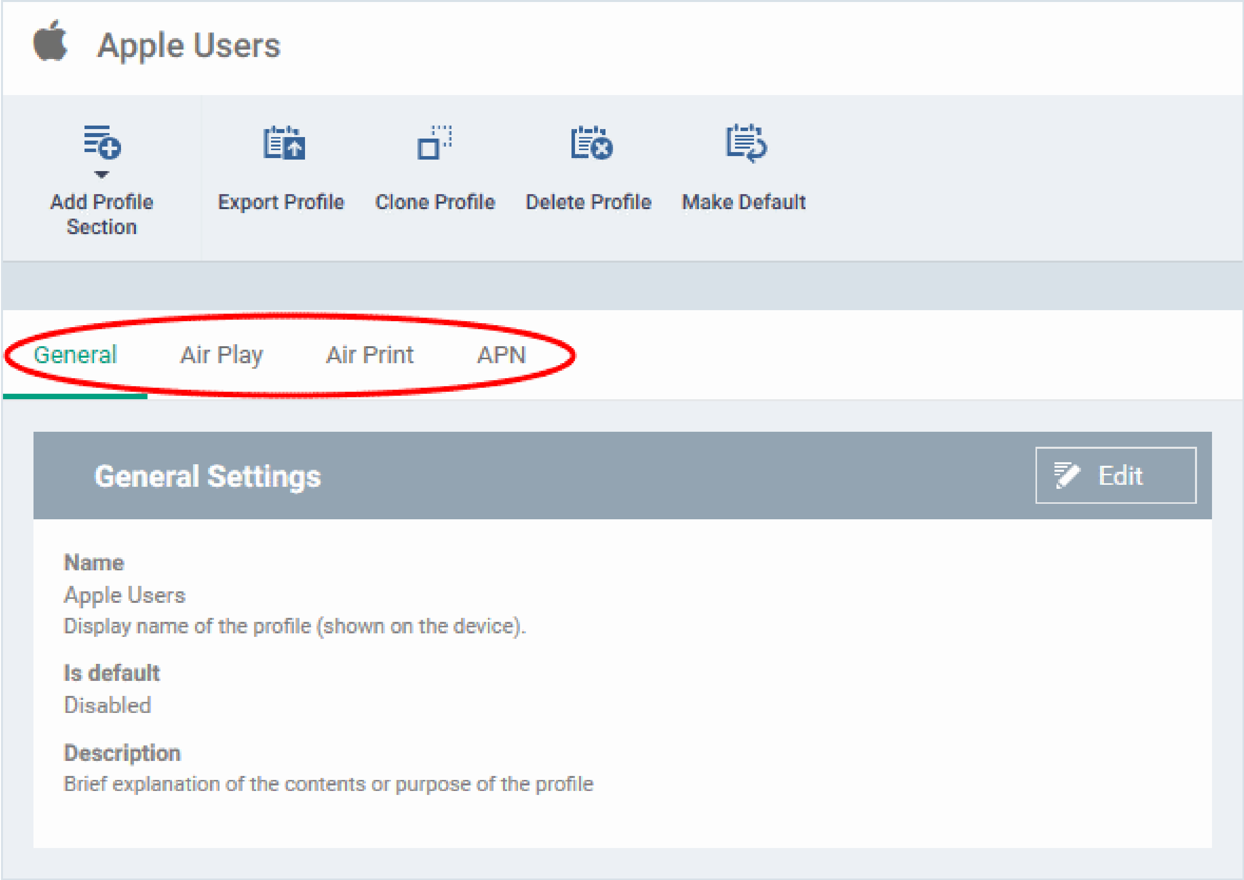
- The profile is not a 'default' profile at this stage. A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- Click the 'Make Default' button if you want this profile to be a default.
    - Alternatively, click the 'Edit' button on the right of the 'General' settings screen and enable 'Is Default'.
- Click 'Save'.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific management feature.
- For example, there are profile sections for 'Email', 'Single Sign-On', 'LDAP', 'Cellular Networks' and so on.
- You can add as many different sections as you want when building your device profile.
- To get started:
    - Click 'Add Profile Section'
    - Select the component that you want to include in the profile:



- Configure the component as required
- Click 'Save'
- This add a new tab for the component to the profile:



Name
Apple Users
Display name of the profile (shown on the device).

Is default
Disabled

Description
Brief explanation of the contents or purpose of the profile

The following links explain more about each section:

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

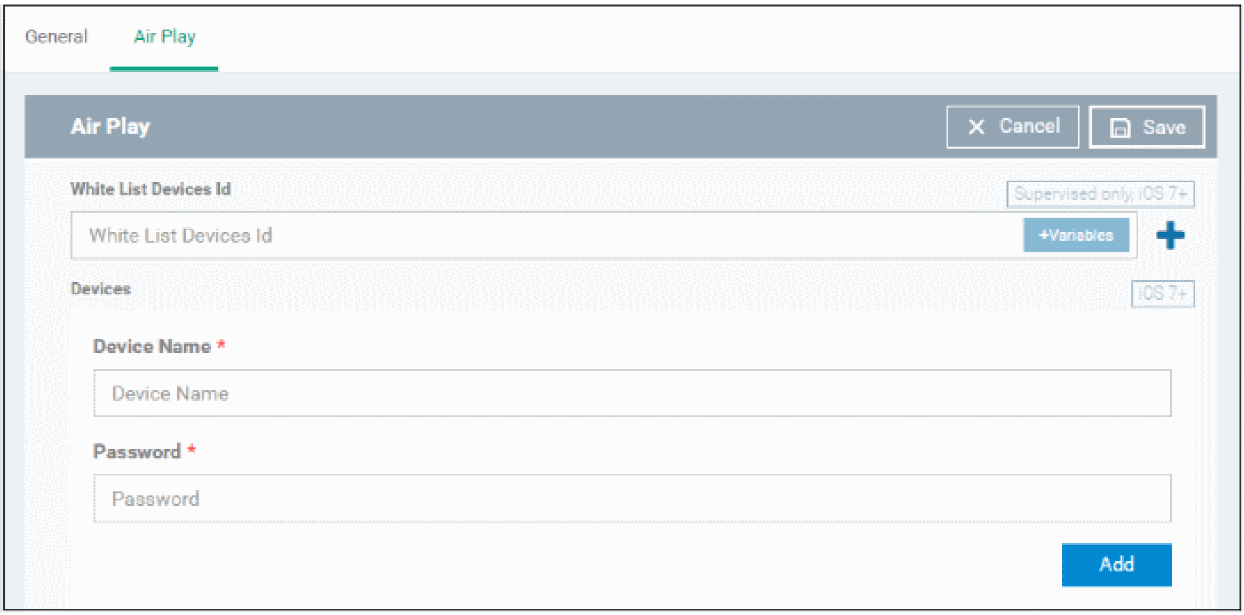
- App Lock

### Air Play settings

These settings let you whitelist devices which can play content from managed iOS devices via Apple Airplay. Example devices are televisions, monitors, stereo systems.

**Note**: If you do not create a whitelist then managed mobile devices will be able to broadcast to any Airplay capable device.

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

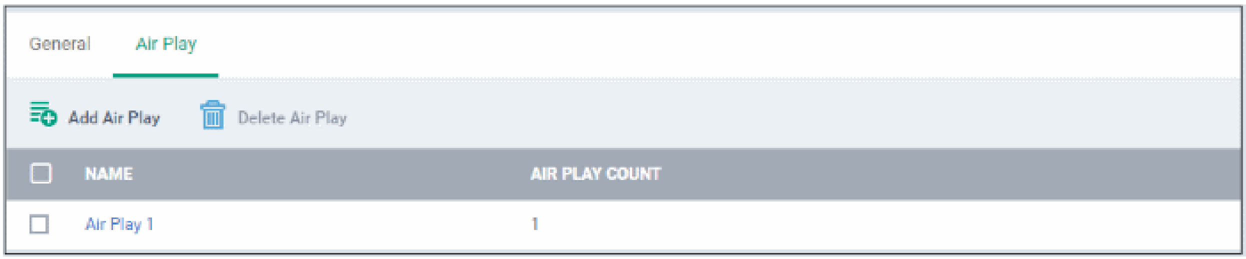


| AirPlay Settings Configuration - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| White List Devices ID | Text Field | Enter the identifier of the output device that you want to whitelist for Air Play. The ID numbers of the devices should be entered in the format as given below:<br>XX:XX:XX:XX:XX:XX<br>Note: The whitelist is applicable for supervised iOS 7+ devices and will not apply for all other devices.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>Click the + button to add more 'Device ID' fields.<br>Click − beside an item to remove it from the list. |
| Device Name | Text Field | Enter the name of the Air Play output device that you entered above.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>• Click the 'Add' button to add more devices<br>• Click the ✖ beside a device name to remove it from the list. |

| AirPlay Settings Configuration - Table of Parameters | | |
|---|---|---|
| Password | Text Field | Enter the password for the Air Play destination that you entered above. |
| Add | Button | Click this button to add another 'Devices' section. |

- Click the 'Save' button.

The 'Air Play' device is added to the list.



| NAME | AIR PLAY COUNT |
|---|---|
| Air Play 1 | 1 |

You can add multiple Air Play devices to the profile.

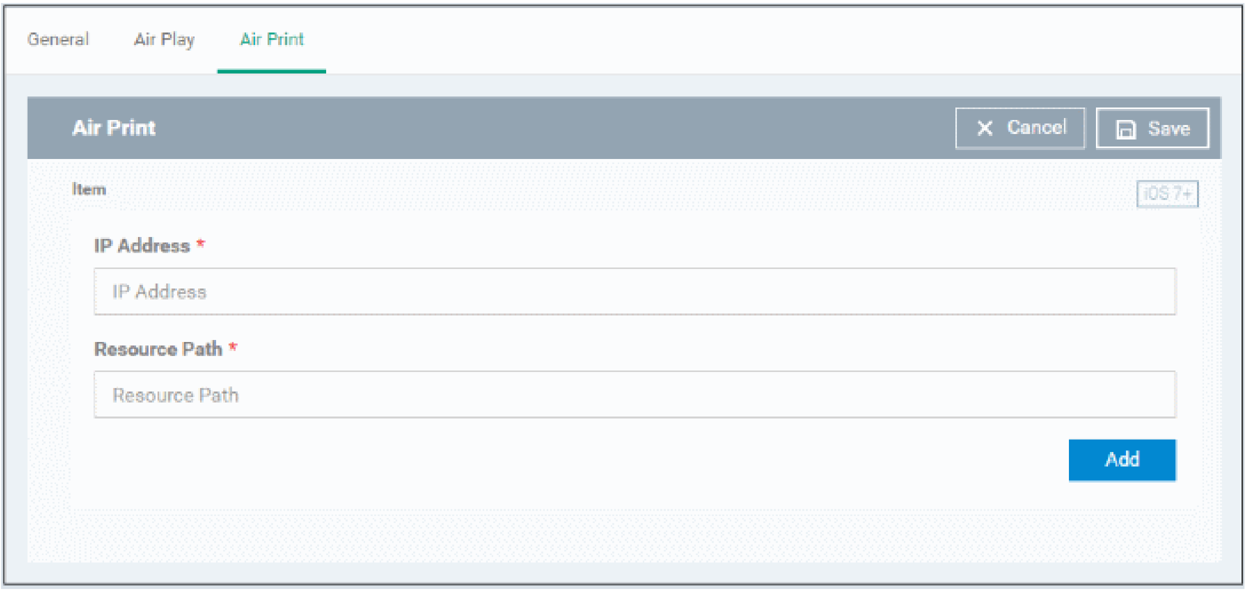
- Click 'Add Air Play' to add more devices
- Click a device name to edit its settings

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** if you want help with this.

### Air Print settings

These settings let you specify the default printer your devices use with the 'Air Print' feature.

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



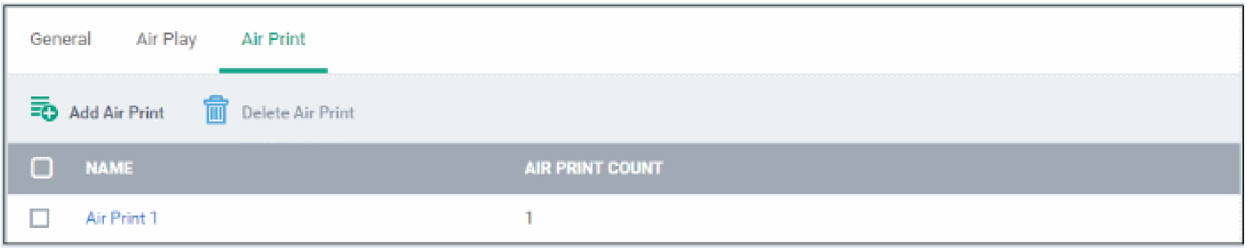
| Form Element | Type | Description |
|---|---|---|
| IP Address | Text Field | Enter the network address of the Air Print printer you wish to use. |
| Resource Path | Text Field | Enter the resource path of the printer.<br>For example: printers/Canon_MG5300_series |

| Form Element | Type | Description |
|---|---|---|
| Add | Button | Click this button to add another Air Print section. |

You can add more printers by repeating the process. To remove a printer, click the 'X' button beside the printer.

- Click the 'Save' button.

The printer will be added to the list.



| ☐ | NAME | AIR PRINT COUNT |
|---|---|---|
| ☐ | Air Print 1 | 1 |

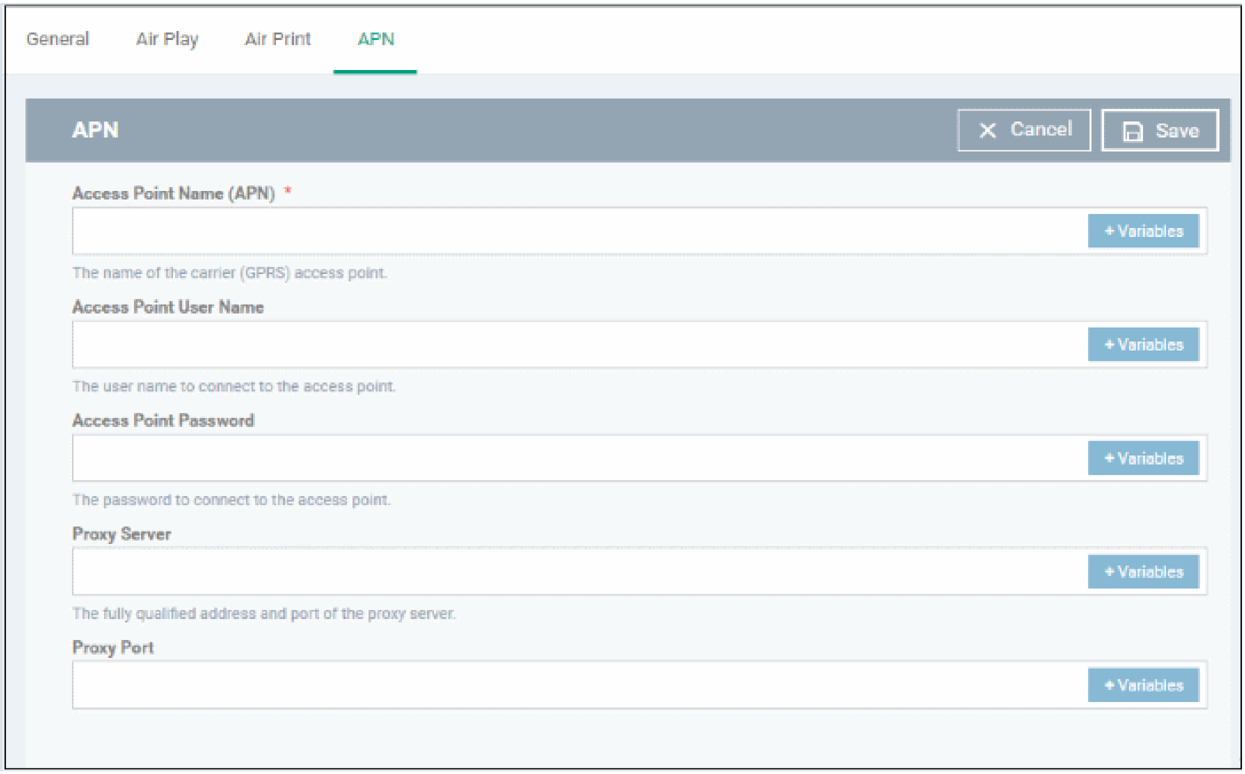
- Click 'Add Air Print' and repeat the process to add more printers,
- Click the name of a printer to view and edit its settings of a printer.

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## APN settings

**Note**: APN settings have been deprecated in favor of cellular settings in iOS 7 and above.

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



Access Point Name (APN) *

The name of the carrier (GPRS) access point.

Access Point User Name

The user name to connect to the access point.

Access Point Password

The password to connect to the access point.

Proxy Server

The fully qualified address and port of the proxy server.

Proxy Port

| Form Element | Type | Description |
|---|---|---|
| Access Point Name (APN)* | Text Field | Enter the name of the GPRS access point provided by the cellular |

| Form Element | Type | Description |
|---|---|---|
| | | service provider.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Access Point User Name / Access Point Password | Text Fields | Enter the login of the APN account to connect to the access point.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Proxy Server / Proxy Port | Text Field | Enter the host name and connection port of the proxy server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

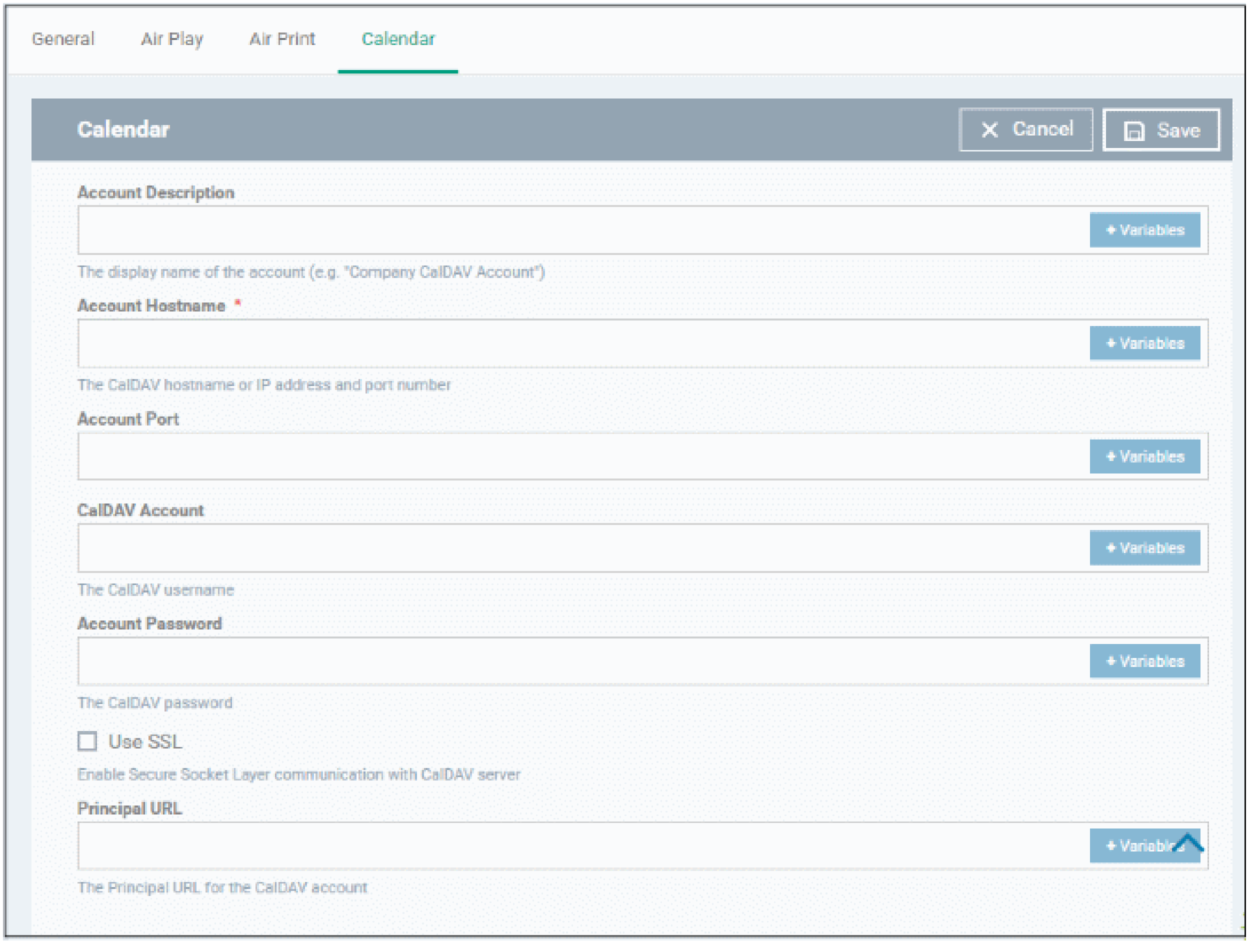
Fields marked * are mandatory.

- Click the 'Save' button.

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Calendar settings

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



Account Description

The display name of the account (e.g. "Company CalDAV Account")

Account Hostname *

The CalDAV hostname or IP address and port number

Account Port

CalDAV Account

The CalDAV username

Account Password

The CalDAV password

□ Use SSL

Enable Secure Socket Layer communication with CalDAV server

Principal URL

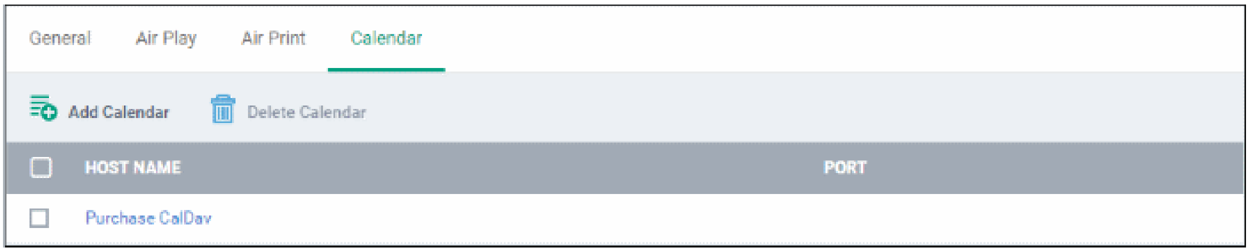
The Principal URL for the CalDAV account

| Form Element | Description |
|---|---|
| Account Description | Enter the display name of the CalDav account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Account Host Name* | Enter the CalDav host name or IP address.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Account Port | Enter the port number on which to connect to the server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| CalDav Account | The user name of the CalDav user.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Account Password | 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 | If enabled, SSL connection will be established with the CalDav server. |
| Principal URL | The URL of the CalDav account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

Fields marked * are mandatory.

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

The calendar account host will be added to the list.



| □ | HOST NAME | PORT |
|---|---|---|
| □ | Purchase CalDav | |

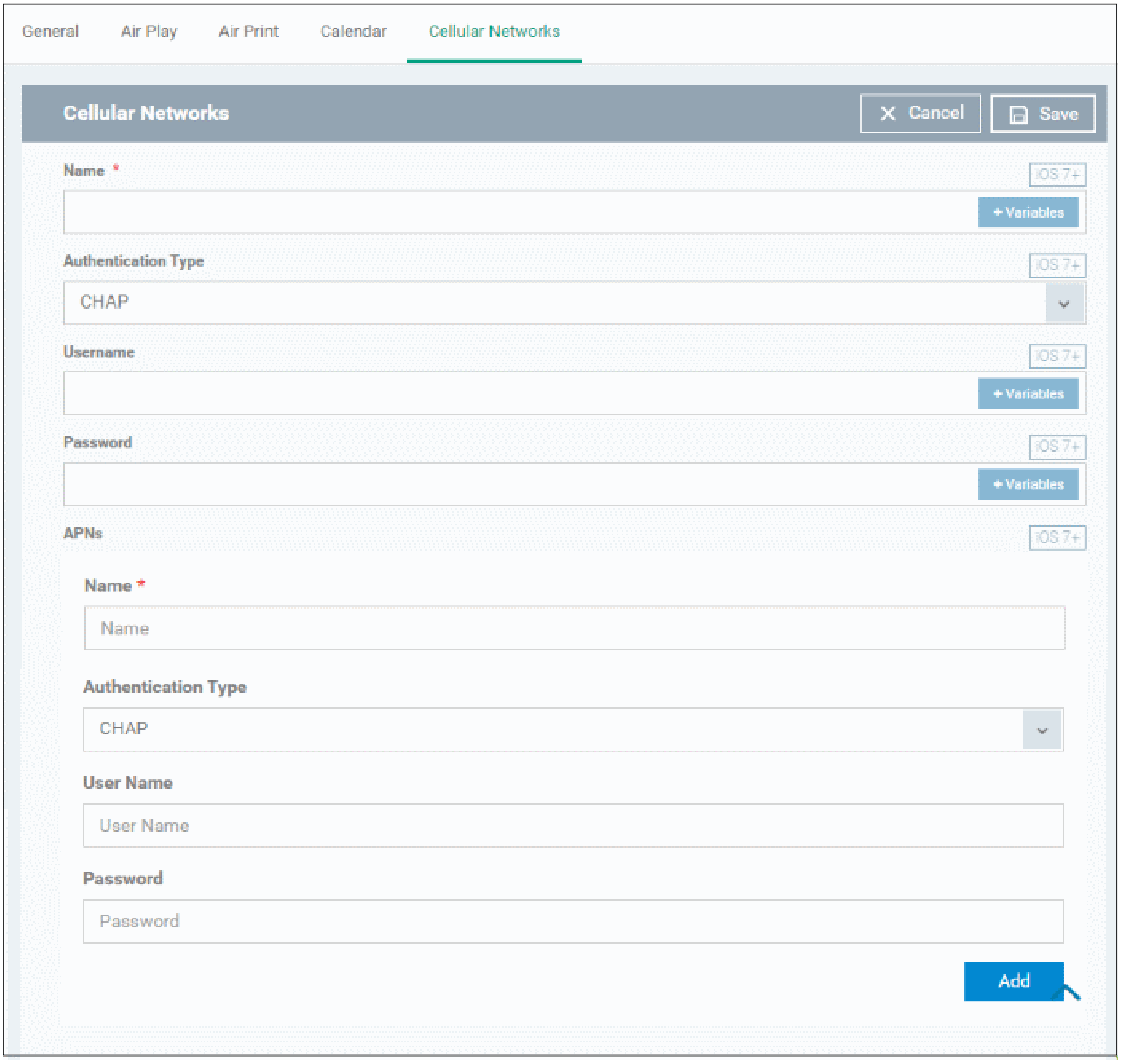
- Click 'Add Calendar' to add more calendar servers
- Click the host name of a calendar server to view and edit its settings

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Cellular network settings

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

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



| Form Element | Type | Description |
|---|---|---|
| Name | Text Field | Enter the name for this configuration, specifying the cellular service provider.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Authentication Type | Drop-down | Select the user authorization type used by the service provider. The options are CHAP or PAP. |
| Username / Password | Text Field | Enter login credentials for the provider network. This is required to authenticate the request. |

| Form Element | Type | Description |
|---|---|---|
| | | Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| **APNs** | | |
| **Note**: You can add more APN accounts for a single service provider by clicking the Add button at the bottom left. | | |

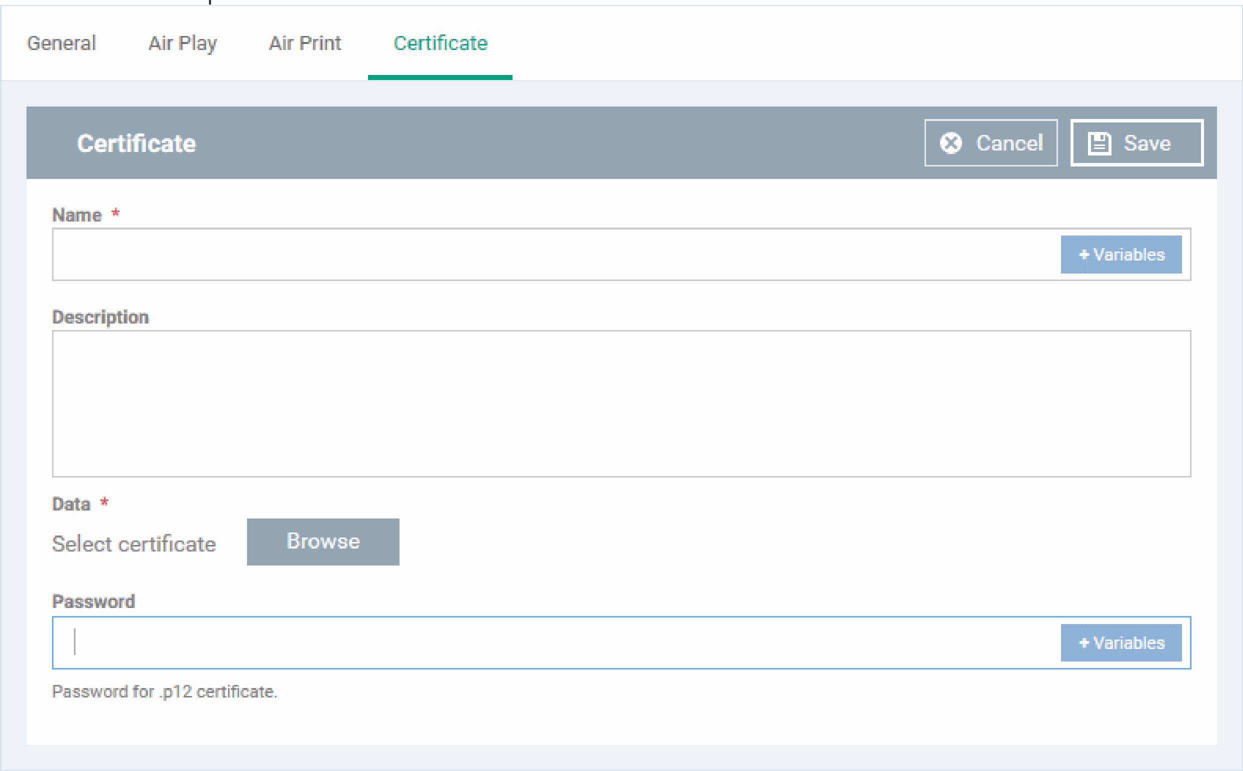
- Click 'Save'

This will add a 'Cellular Networks' tab to the profile. You can edit the settings or remove the section at anytime. See **Edit Configuration Profiles** if you want help with this.

### Certificate settings

The certificate settings area lets you upload certificates which can be used to secure other aspects of Endpoint Manager. For example, you can select your uploaded certificates in the 'Wi-Fi, 'Exchange Active Sync' and 'VPN' areas.

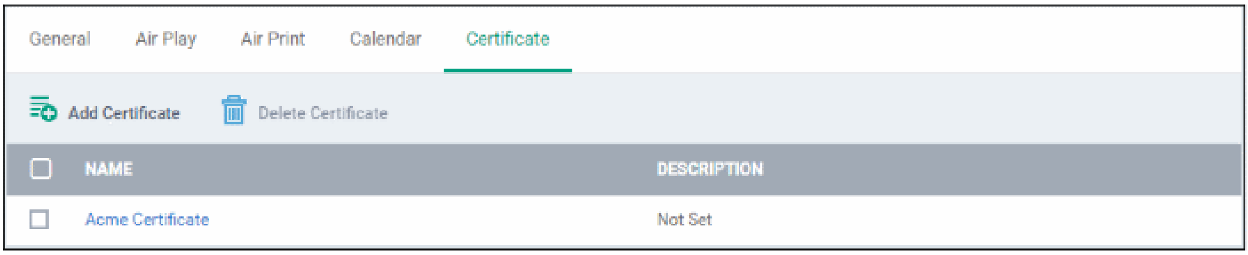
- Click 'Add profile section' > 'Certificate'



| Form Element | Description |
|---|---|
| Name | Enter a label for the certificate.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Description | Enter a brief description for the certificate. |
| Data | Click 'Browse' and upload you certificate. Supported extensions - 'p12'. 'pub', '.crt', '.key'. |
| Password | Enter the password for importing the certificate. |

- Click the 'Save' button.

The certificate will be added to the certificate store.



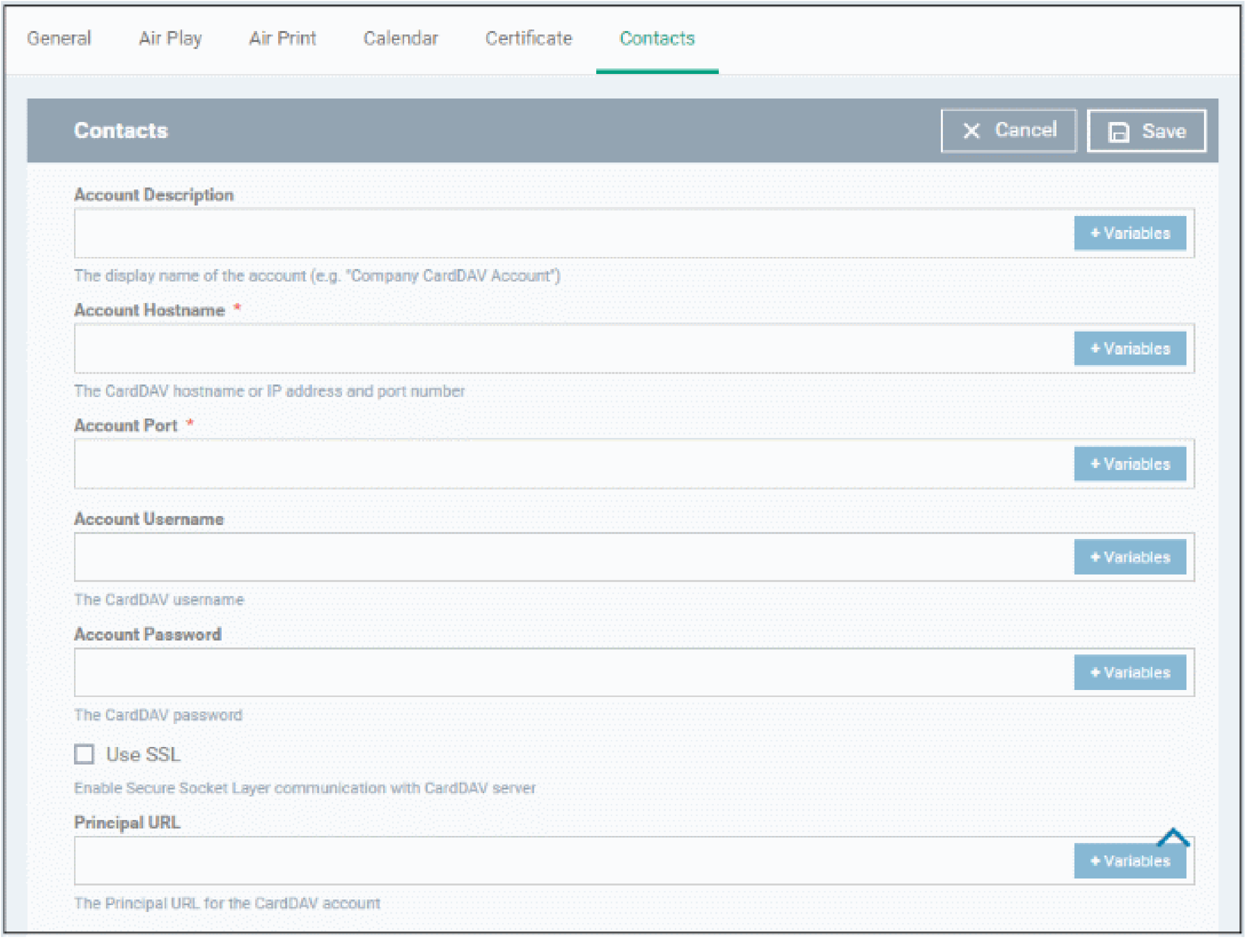
| ☐ | NAME | DESCRIPTION |
|---|---|---|
| ☐ | Acme Certificate | Not Set |

- Click 'Add Certificate' and repeat the process to add more certificates.
- Click on the name of a certificate to view the certificate key and edit its name.

You can add any number of certificates to the profile and remove certificates at anytime. See **Edit Configuration Profiles** for more details.

### Contacts settings

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



Account Description

The display name of the account (e.g. "Company CardDAV Account")

Account Hostname *

The CardDAV hostname or IP address and port number

Account Port *

Account Username

The CardDAV username

Account Password

The CardDAV password

☐ Use SSL

Enable Secure Socket Layer communication with CardDAV server

Principal URL

The Principal URL for the CardDAV account

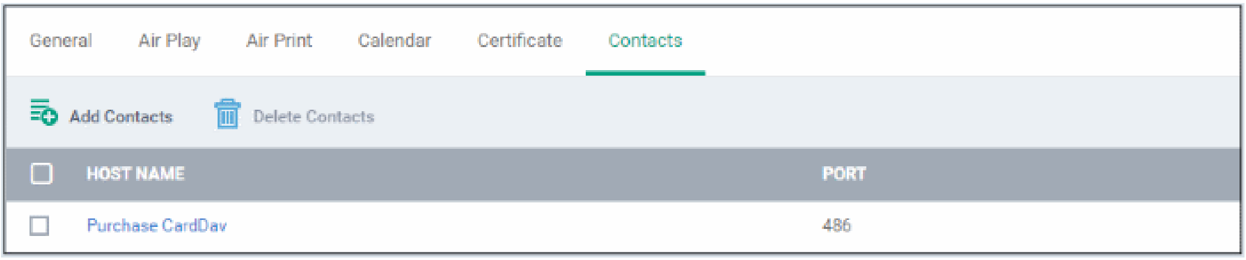
| Form Element | Description |
|---|---|
| Account Description | Enter the display name of the CardDav account.<br>Click the variables button + Variables to insert dynamic values. See **Create** |

| Form Element | Description |
|---|---|
| | and Manage Custom Variables for more details on variables. |
| Account Host Name* / Account Port* | Enter the CardDav server details. This includes hostname / IP address and server port.<br>Click the variables button + Variables to insert dynamic values. See Create and Manage Custom Variables for more details on variables. |
| Account Username / Account Password | The login credentials of the CardDav user account.<br>Click the variables button + Variables to insert dynamic values. See Create and Manage Custom Variables for more details on variables. |
| Use SSL | If enabled, a secure SSL connection will be used for communications with the CardDav server. |
| Principal URL | Enter the 'Principal URL' of the CardDav account. |

Fields marked * are mandatory.

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

The contact account is added to the list.



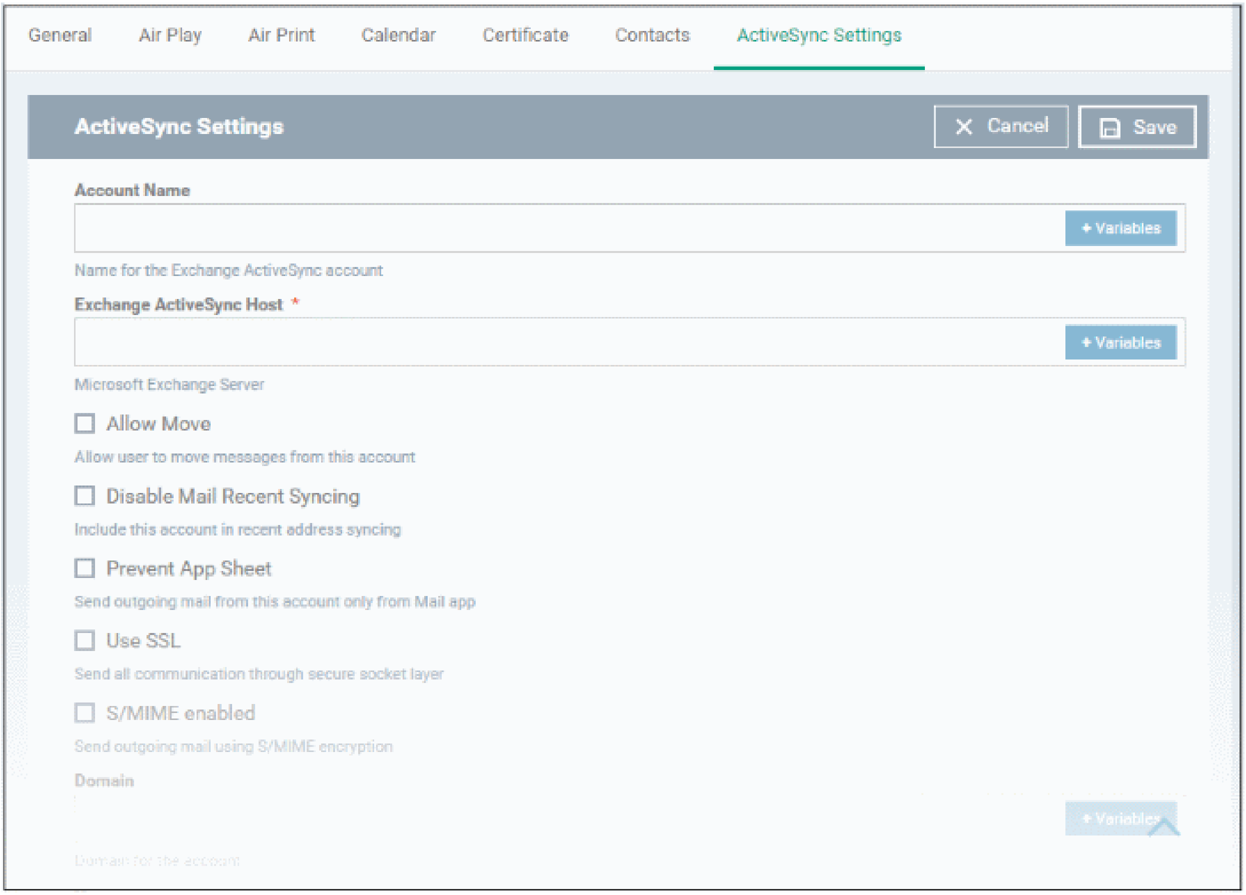
| □ | HOST NAME | PORT |
|---|---|---|
| □ | Purchase CardDav | 486 |

- Click 'Add Contacts' and repeat the process to add more accounts
- Click the hostname of the contact account to view or edit its details

The settings will be saved and shown under 'Contacts' tab. You can edit the contacts or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### ActiveSync settings

- Click 'Add Profile Section' > 'ActiveSync Settings'



ActiveSync Settings

Account Name

Name for the Exchange ActiveSync account

Exchange ActiveSync Host *

Microsoft Exchange Server

□ Allow Move

Allow user to move messages from this account

□ Disable Mail Recent Syncing

Include this account in recent address syncing

□ Prevent App Sheet

Send outgoing mail from this account only from Mail app

□ Use SSL

Send all communication through secure socket layer

□ S/MIME enabled

Send outgoing mail using S/MIME encryption

Domain

Domain for the account

| Form Element | Description |
|---|---|
| Account Name | Enter the Exchange ActiveSync account name.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Exchange ActiveSync host* | Enter the Exchange host name (Microsoft Exchange Server).<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Allow Move | If enabled, the user can move sent or received mails to another account. |
| Disable Mail Recent Syncing | If enabled, recently used emailed addresses are not synced with other devices via iCloud. |
| Prevent App Sheet | If enabled, mails cannot be sent using third-party applications. |
| Use SSL | If enabled, communication between Exchange server and devices will be encrypted using SSL. |
| S/MIME Enabled | 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 | Email domain name.<br>Click the 'Variables' button + Variables and click + beside '%u.mail' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, see **Create and Manage Custom Variables**. |

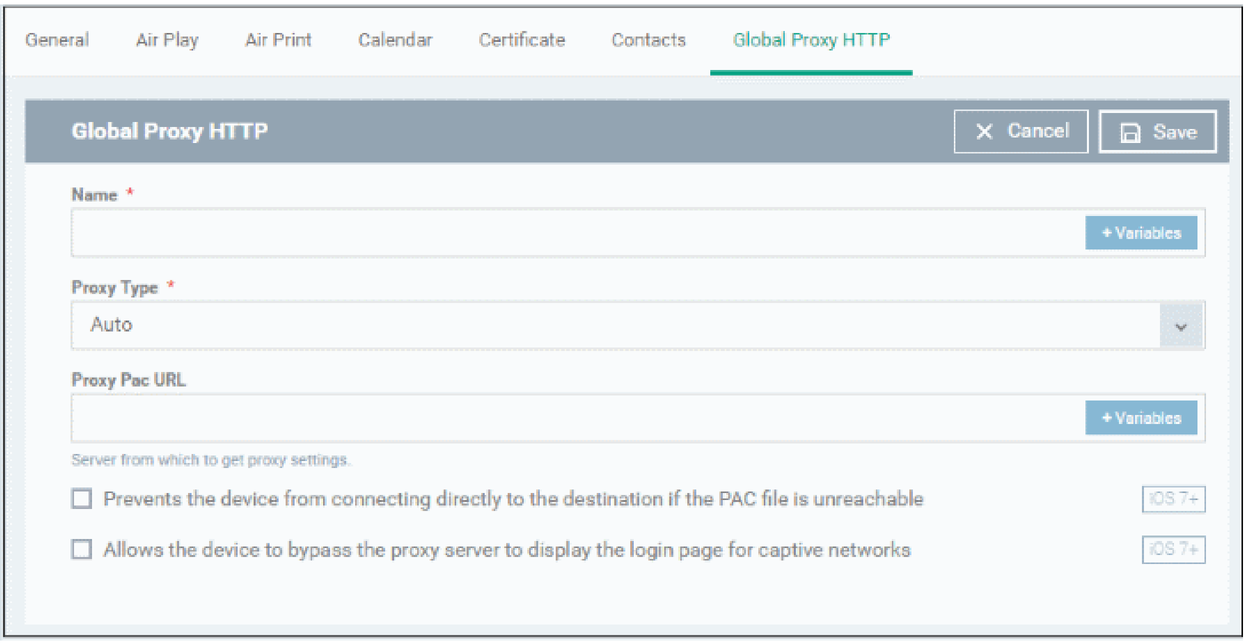
| Form Element | Description |
|---|---|
| User Name | User name for the account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Email Address | Address of the email account.<br>Click the 'Variables' button + Variables and click + beside '%u.mail' from the 'User Variables' list. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, see **Create and Manage Custom Variables**. |
| Password | 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 | 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 | Select the user client authentication certificate from the drop-down or upload it using the 'Add New' button. |

- Click the 'Save' button.

This adds the ActiveSync section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Global HTTP proxy settings

- Click 'Add Profile Section' > 'Global Proxy HTTP'



Name *

Proxy Type * Auto

Proxy Pac URL

Server from which to get proxy settings.

□ Prevents the device from connecting directly to the destination if the PAC file is unreachable

□ Allows the device to bypass the proxy server to display the login page for captive networks

| Form Element | Description |
|---|---|
| Name | Enter the host name of the proxy you want devices to use.<br>Click the variables button + Variables to insert dynamic values. See **Create** |

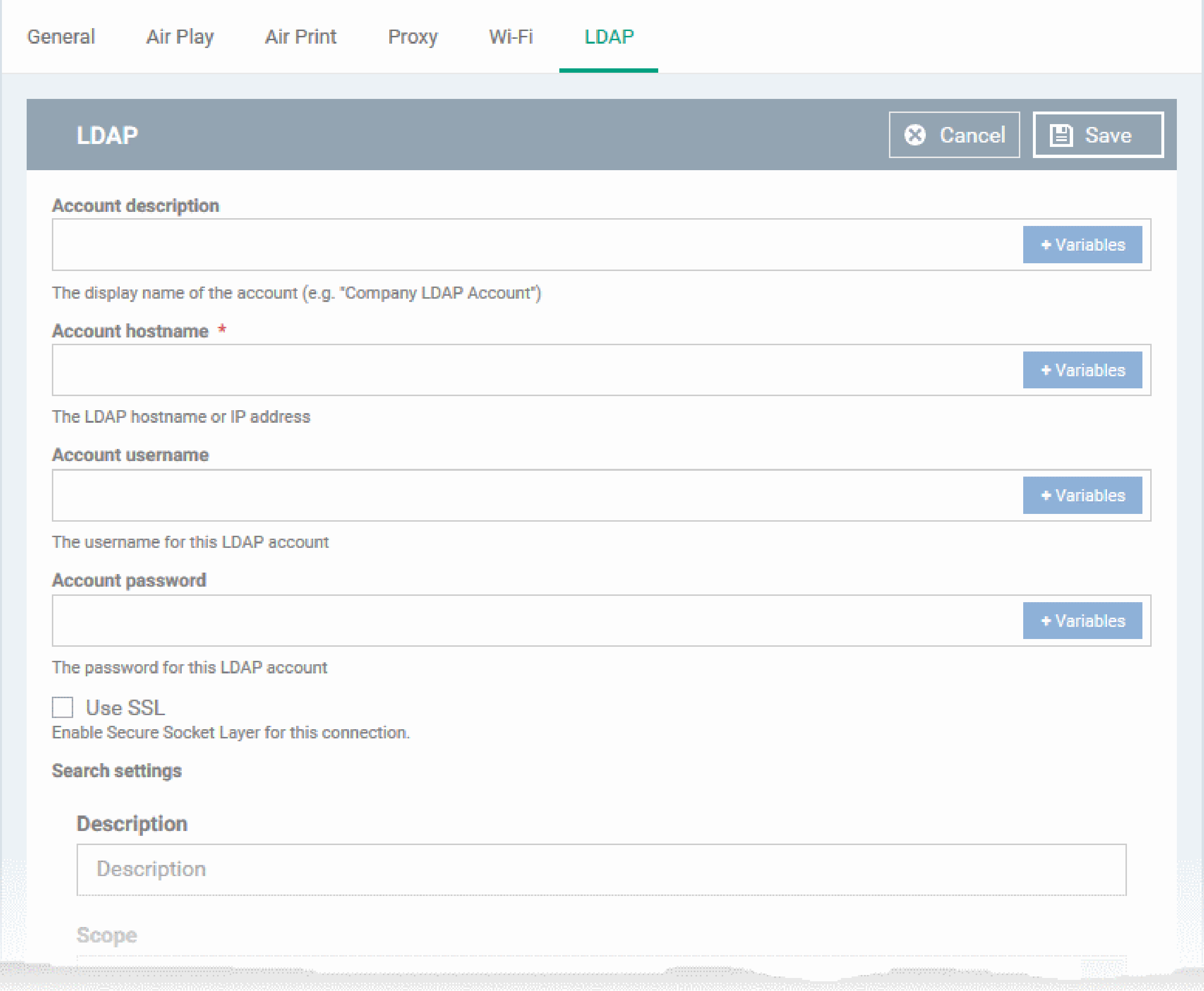
| Form Element | Description |
|---|---|
| | **and Manage Custom Variables** for more details on variables. |
| Proxy type | Select the proxy type from the drop-down. The options available are:<br>• None<br>• Manual<br>• Auto<br>If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields.<br>If you select 'Auto', enter the URL of the Proxy Pac, select whether or not the device can directly connect to the destination if Pac server is not reachable and whether or not the device can bypass the proxy server to display the login page for captive networks from the respective check box options.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables**. for more details on variables. |

- Click the 'Save' button.

This will add a ‘Global Proxy HTTP' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### LDAP settings

- Click 'Add Profile Section' > 'LDAP'



Account description

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

Account hostname *

The LDAP hostname or IP address

Account username

The username for this LDAP account

Account password

The password for this LDAP account

□ Use SSL

Enable Secure Socket Layer for this connection.

Search settings

Description

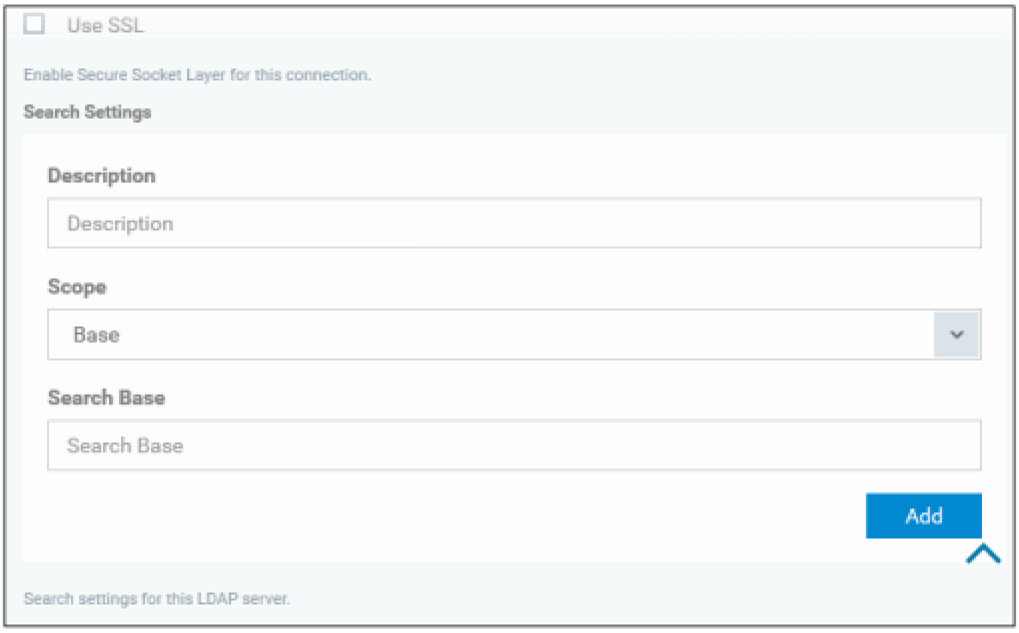
Description

Scope

| Form Element | Description |
|---|---|
| Account description | Enter the display name of the LDAP account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Account hostname | Enter the hostname or IP address of the AD server.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Account Username / Account Password | Login credentials for the LDAP account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Use SSL | If enabled, the communication will be encrypted. |
| Search settings | Configure the settings for searching email contacts from the LDAP server. See '**Search the LDAP directory**' below for more details. |

### Search the LDAP directory

Admins can search for email contacts in the domain using the search feature.



□ Use SSL

Enable Secure Socket Layer for this connection.

Search Settings

Description: Description

Scope: Base

Search Base: Search Base

Search settings for this LDAP server.

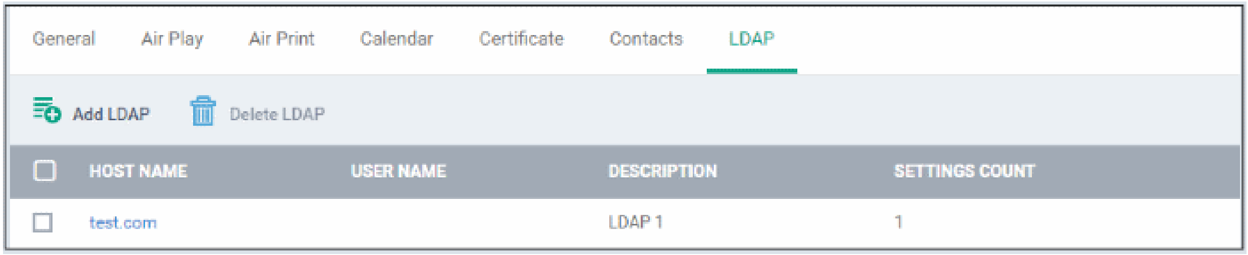
| Form Element | Description |
|---|---|
| Description | Enter a label for the search |
| Scope | Level of search on the LDAP tree structure.<br>• Base - Searches only the defined search base.<br>• One level - Searches the base and the first level below it.<br>• Subtree - Searches the base and all levels below. |
| Search base | Enter the search base for which the search will be restricted. For example, you |

| Form Element | Description |
|---|---|
| | might want to allow users to search only for other email users via LDAP. |

- You can add more searches by clicking the Add button
- To remove an item, click the ✖ button.

- Click the 'Save' button.

The LDAP account will be added to the list.



| □ | HOST NAME | USER NAME | DESCRIPTION | SETTINGS COUNT |
|---|---|---|---|---|
| □ | test.com | | LDAP 1 | 1 |

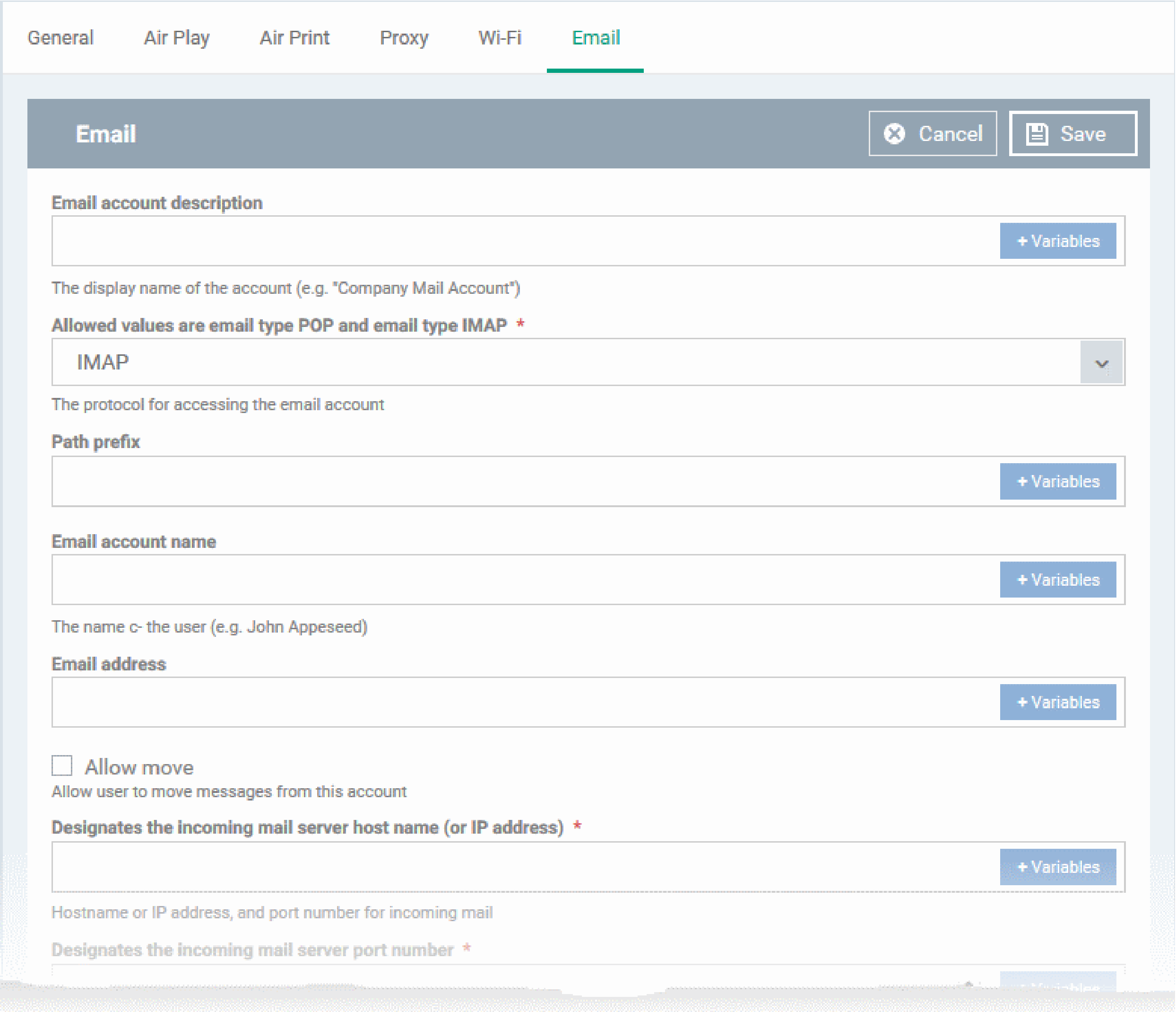
You can add multiple LDAP accounts.

- Click 'Add LDAP' and repeat the process to add more LDAP servers
- Click the hostname of an LDAP account to view and edit its settings

This will add a 'LDAP' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### E-Mail settings

- Click 'Add Profile Section' > 'E-mail'



Email account description

The display name of the account (e.g. "Company Mail Account")

Allowed values are email type POP and email type IMAP *

IMAP

The protocol for accessing the email account

Path prefix

Email account name

The name c- the user (e.g. John Appeseed)

Email address

□ Allow move

Allow user to move messages from this account

Designates the incoming mail server host name (or IP address) *

Hostname or IP address, and port number for incoming mail

Designates the incoming mail server port number *

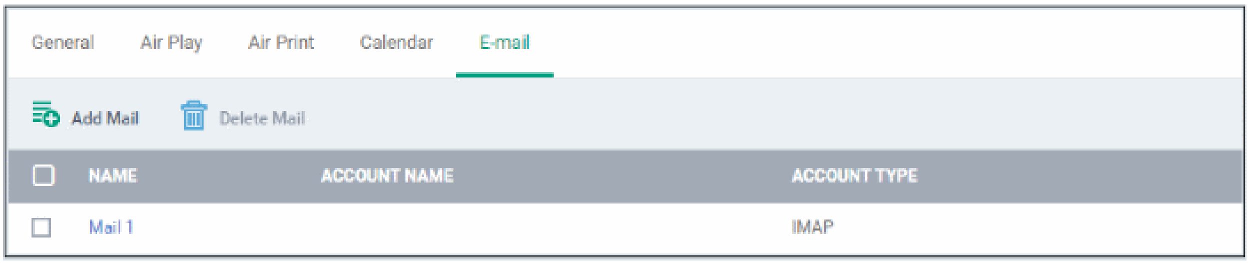
| Form Element | Description |
|---|---|
| Email account description | Enter a label for the email account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Allowed values are email type POP and email type IMAP * | Select the mail protocol. Possible values are IMAP and POP. |
| Path prefix | This will be visible if IMAP is chosen as Email Type in the previous step. Enter the path of the inbox in the field.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Email account name | Enter a label to identify the user's email account at the incoming mail server, if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>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. |

| Form Element | Description |
|---|---|
| Email address | Enter the email address of the user at the incoming mail server If the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>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.<br>See **Create and Manage Custom Variables** for more details on variables. |
| Allow move | If enabled, the user can move sent or received mails to another account. |
| Designates the incoming mail server host name (or IP address)* | Enter the host name of the incoming mail server or its IP address.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Designates the incoming mail server port number* | 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.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Incoming mail server username | Enter the username for the email account of the user at the incoming mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>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. |
| Allowed values are email auth password and email auth none * | Select the type of authentication method for the mail account from the drop-down. The options available are:<br>• None<br>• Password<br>• CRAM MD5<br>• NTLM<br>• HTTP MD5 |
| Incoming password | Leave the field blank. If authentication is chosen in the previous step, then user needs 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 | If enabled, communication between incoming mail server and devices is encrypted using SSL. |
| Outgoing mail server host name* | Enter the host name or IP address of the outgoing (SMTP) mail server for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables. |

| Form Element | Description |
|---|---|
| Designates the outgoing mail server port number* | 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.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Outgoing mail server username | Enter the username for the email account of the user at the outgoing (SMTP) mail server if the profile is for a single user.<br>Click the variables button + Variables to insert dynamic values if the profile is for several users.<br>See **Create and Manage Custom Variables** for more details on variables.<br>The email usernames of the users to whom the profile is associated are automatically added to the profile while rolling out to the devices. |
| Outgoing mail server authentication* | Select the type of authentication method for outgoing mail server from the drop-down. The options available are:<br>• None<br>• Password<br>• CRAM MD5<br>• NTLM<br>• HTTP MD5 |
| Outgoing password | Leave the field blank. If authentication is chosen in the previous step, then user needs 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 | If enabled, the password for incoming mail server will be used for outgoing mail server too. |
| Disable email recents syncing | If enabled, recently used emailed addresses are not synced with other devices via iCloud. |
| Signing and encryption per-message | If enabled, the device digitally signs and encrypts your mail per-message. |
| Prevent App Sheet | If enabled, outgoing mails can be sent from this account only via mail app. |
| Outgoing mail server Use SSL | If enabled, communication between outgoing mail server and devices is encrypted using SSL. |
| S/MIME enabled | If enabled, users can sign and encrypt email messages from their devices. Please note that certificates have to be installed in users' devices before this feature can be used. |

- Click the 'Save' button.

The e-mail account will be added to the profile.



| NAME | ACCOUNT NAME | ACCOUNT TYPE |
|---|---|---|
| Mail 1 | | IMAP |

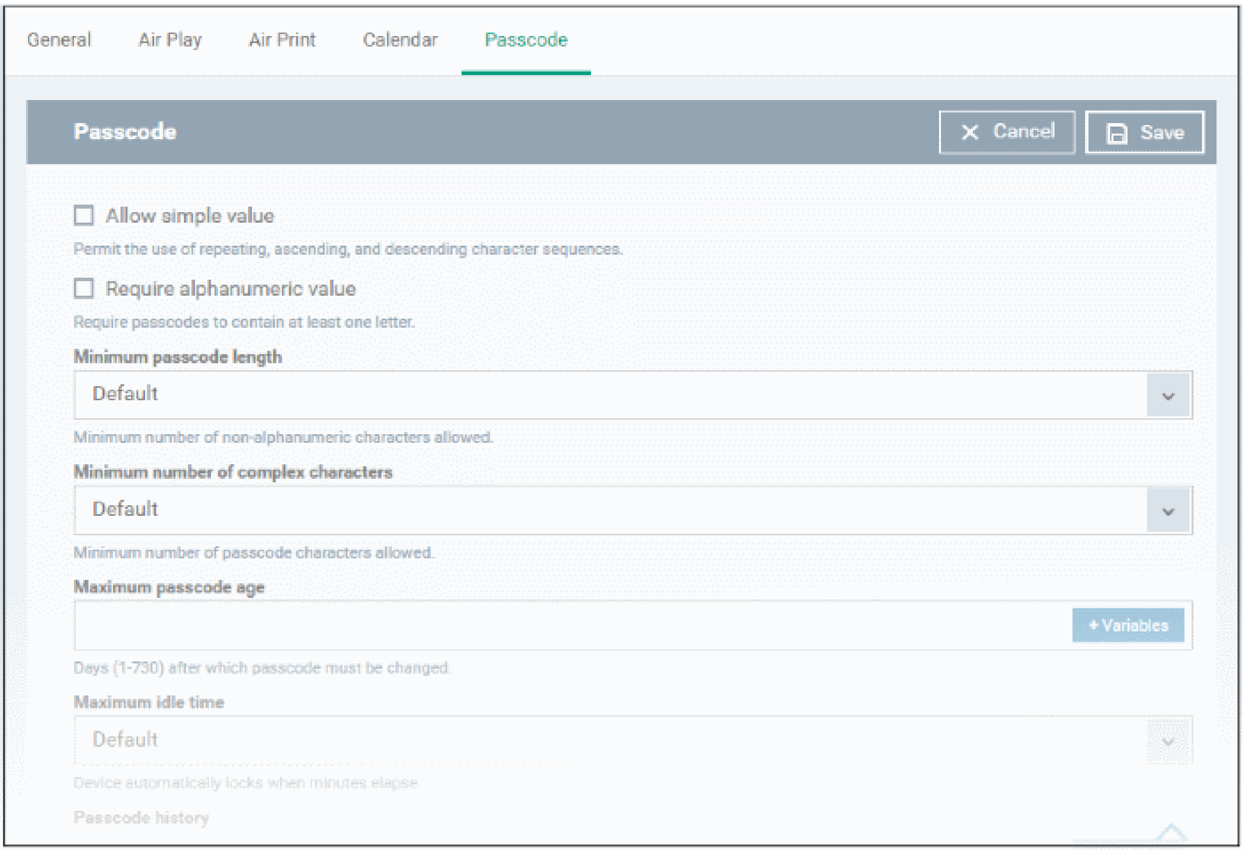
You can add several email accounts to the same profile.

- Cick 'Add Mail' and repeat the process to add more email accounts.
- Click the name of an email account to view and edit its settings

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Passcode settings

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



□ Allow simple value
Permit the use of repeating, ascending, and descending character sequences.

□ Require alphanumeric value
Require passcodes to contain at least one letter.

Minimum passcode length
Default
Minimum number of non-alphanumeric characters allowed.

Minimum number of complex characters
Default
Minimum number of passcode characters allowed.

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

Maximum idle time
Default
Device automatically locks when minutes elapse.

Passcode history

| Form Element | Description |
|---|---|
| Allow simple value | Allows users to use repeated or sequential characters in their passwords. For example, '9999' or ABCD. |
| Require alphanumeric value | Compels users to use at least one number or letter in their passwords. |
| Minimum passcode length | 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 | 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. |

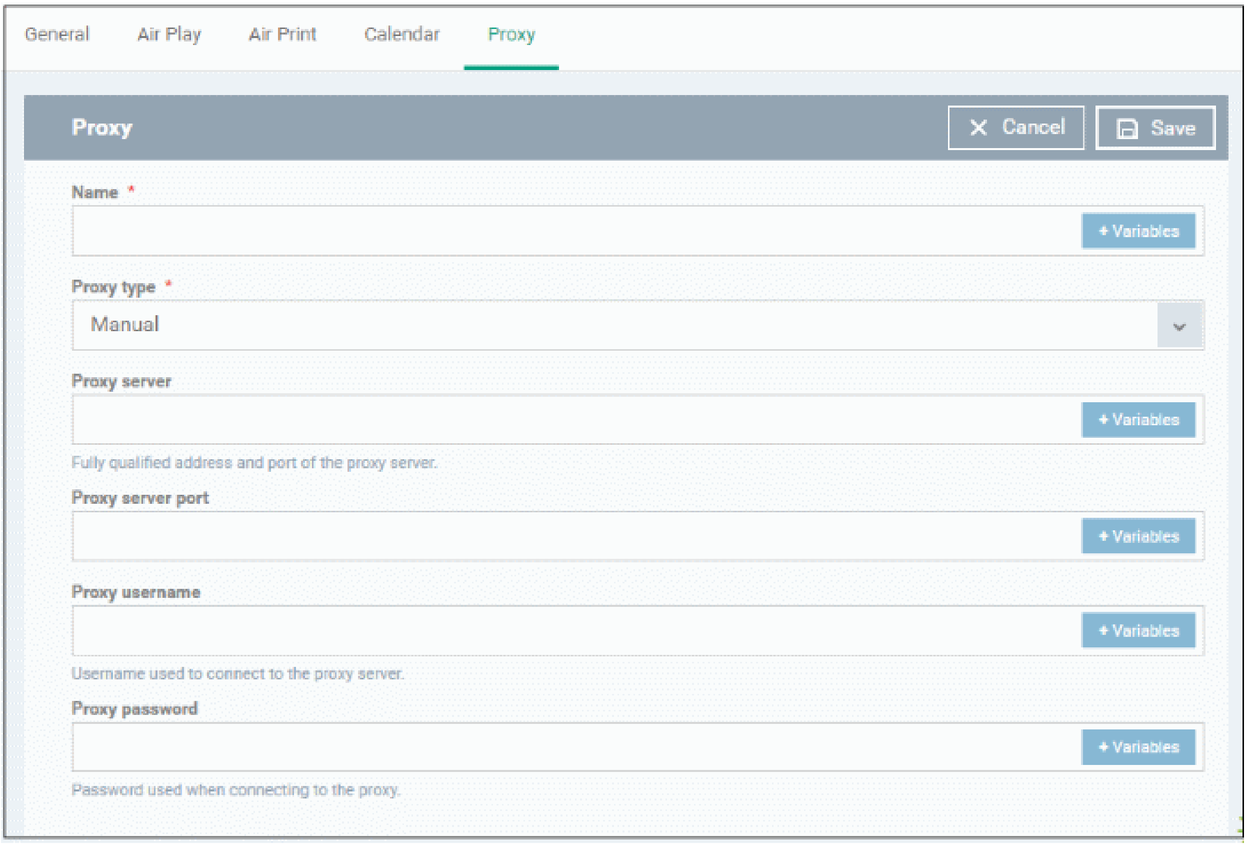
| Form Element | Description |
|---|---|
| Maximum passcode age | Enter the maximum number of days that a password can be valid. The availble option is from 1 day to 730 days.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Maximum idle time | Select the period of time in minutes that a device can be idle before it's screen is automatically locked. |
| Passcode history | New passwords should not match previously used passwords. Specify the number of last used passwords that should be stored for comparison.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Maximum grace period for device lock | 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 | Select the number of unsuccessful login attempts that can be tried by a user before the device is wiped clean of all its data and settings. The option is available to set from 4 to 10. After 6 unsuccessful login attempts, there will be a time delay before a password can be entered again and the time delay period increases with each failed login attempt. This time delay begins only after the sixth attempt, so if you select the period as 6 or lower, there will be no time delay and data will be erased after the final attempt. |
| Allows the user to modify Touch ID | If enabled, allows user you to modify the biometric authentication to unlock your device, make purchases and so on. |

- Click 'Save'.

You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Proxy settings

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



Name *

Proxy type *
Manual

Proxy server

Fully qualified address and port of the proxy server.

Proxy server port

Proxy username

Username used to connect to the proxy server.

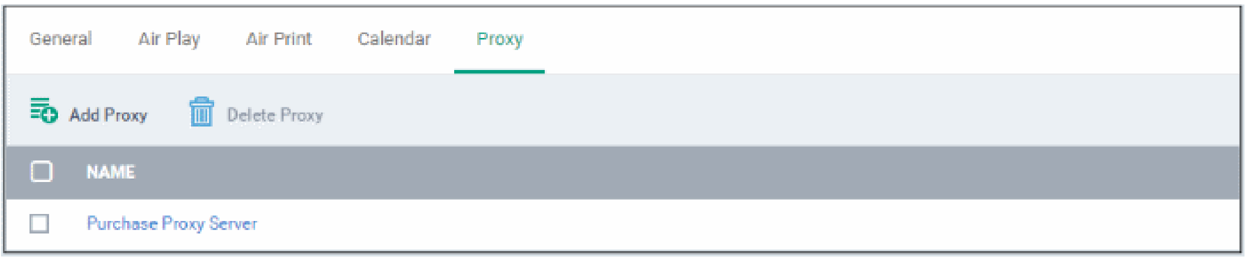
Proxy password

Password used when connecting to the proxy.

| Form Element | Description |
|---|---|
| Name | Enter a label for the proxy to be shown to the device users.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Proxy | Select the proxy type from the drop-down. The options available are:<br>• None<br>• Manual<br>• Auto<br>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.<br>If you select 'Auto', enter the URL of the Proxy Pac.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

- Click the 'Save' button.

The proxy server configuration is added to the profile.



□ Purchase Proxy Server

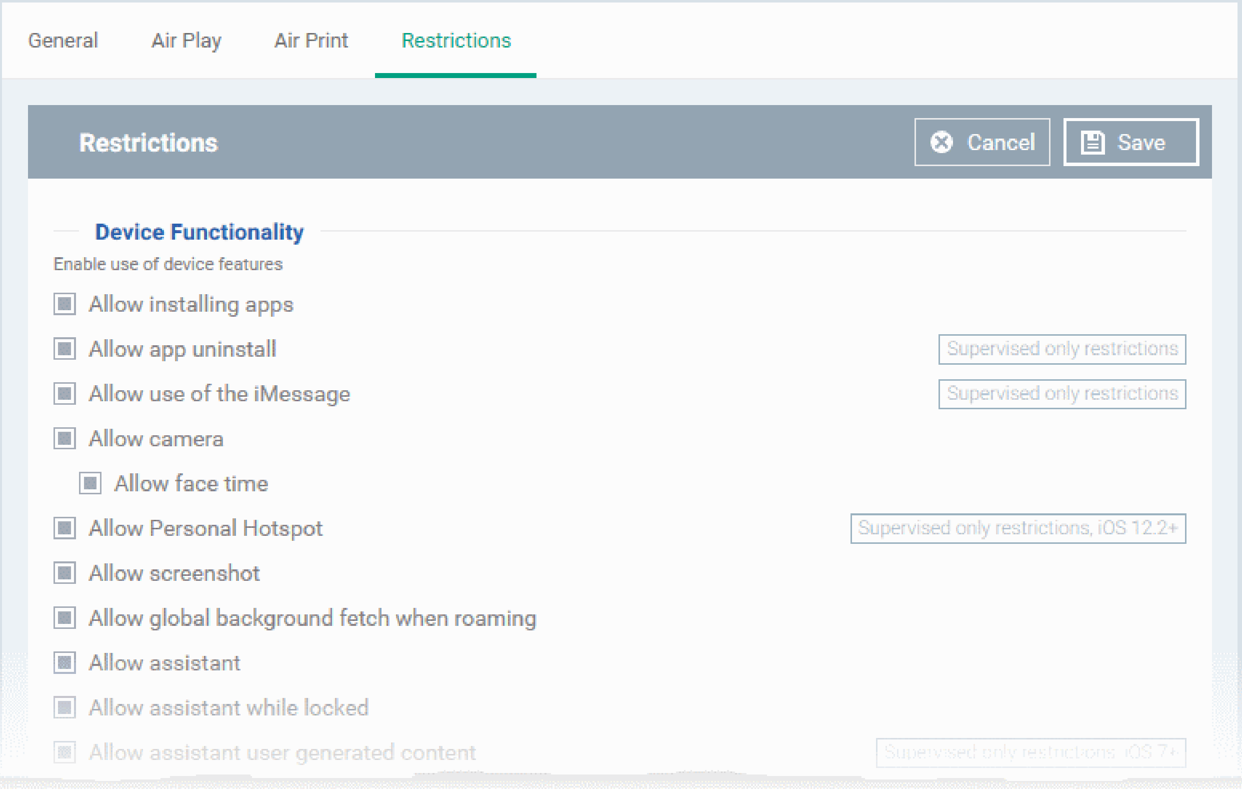
You can add more proxy server accounts to the profile.

- Click 'Add Proxy' and repeat the process to add more proxy server accounts.
- Click the name of a proxy server account to view or edit its details.

This will add a 'Proxy' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## Restriction settings

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



**Device Functionality**

Enable use of device features

☑ Allow installing apps
☑ Allow app uninstall — Supervised only restrictions
☑ Allow use of the iMessage — Supervised only restrictions
☑ Allow camera
☑ Allow face time
☑ Allow Personal Hotspot — Supervised only restrictions, iOS 12.2+
☑ Allow screenshot
☑ Allow global background fetch when roaming
☑ Allow assistant
☑ Allow assistant while locked
☑ Allow assistant user generated content — Supervised only restrictions, iOS 7+

| Device Functionality | |
|---|---|
| **Form Element** | **Description** |
| Allow installing apps | The user can install or update apps from the Apple App Store. If left unchecked, the App Store icon is removed from the device's home screen. |
| Allow app uninstall | The user can to uninstall applications. |
| Allow use of the iMessage | The user can quickly and easily chat over iMessage or SMS/MMS. |
| Allow camera | The user can 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 | The user can use FaceTime. Please note the 'Allow face time' can be enabled only if 'Allow Camera' is enabled. |
| Allow Personal Hotspot | Allows users to setup Wi-Fi hot-spots from their device, and allow other devices to connect. |
| Allow screen shot | Allows users to take screenshots on their device. |
| Allow global background fetch when roaming | Select this to allow the device to sync data when in roaming mode abroad. |
| Allow assistant | If enabled, users can use Siri voice commands and dictation. |
| Allow assistant while Locked | If enabled, users can use Siri even when the device is locked. The checkbox will be active only when 'Allow Assistant' is enabled. |
| Allow assistant user generated content | If enabled, users can use Siri to query user-generated content from the Internet or device. (Supervised mode only.) |
| Forces the use of the profanity filter assistant | If enabled, enforces profanity filter for Siri. |
| Allow voice dialing | Select this to allow the user to dial their phone using voice commands. |
| Allow passbook while locked | If enabled, Passbook notifications will be displayed even when the device is locked. |
| Allow in app purchases | Select this to allow the user to make in-app purchases from the device. |
| Force iTunes store password entry | If enabled, users have to enter their Apple ID to enter the iTunes store. |
| Allow multiplayer gaming | Select this to allow the user to play multiplayer games in Game Center. |
| Allow adding Game Center friends | If enabled, users can add friends in Game Center. |
| Allow account modification | Select this to allow user account modifications on devices.<br>Note: This feature is available for iOS 7+ and supervised devices only. |
| Allow air drop | Select this to allow Air Drop on devices.<br>Note: This feature is available for iOS 7+ and supervised devices only. |
| Allow find my friends modification | Select this to enable Find My Friends feature on devices.<br>Note: This feature is available for iOS 7+ and supervised devices only. |
| Allow fingerprint for unlock | Select this to enable Touch ID to unlock devices.<br>Note: This feature is available for iOS 7+ and supervised devices only. |
| Allow Game Center | 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 | Select this to allow host pairing on devices.<br>Note: This feature is available for iOS 7+ and supervised devices only. |
| Allow lock screen control center | 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 | Select this option to allow Notification Center to be displayed on the lock screen.<br>Note: This feature is available for iOS 7 and later versions. |
| Allow lock screen today view | Select this option to allow the Today View from Notification Center to be displayed in the lock screen.<br>Note: This feature is available for iOS 7 and later versions. |
| Allow OTAPKI updates | Select this option to allow over-the-air public key infrastructure (OTAPKI) updates on the device.<br>Note: This feature is available for iOS 7 and later versions. |
| Allow UI configuration profile installation | Select this option to allow users to install UI configuration profiles.<br>Note: This option is available for supervised devices only. |
| Force limit ad tracking | Select this to limit ad tracking on devices.<br>Note: This feature is available for iOS 7 and later versions. |
| Forces all devices receiving AirPlay requests from this device to use a pairing password | If enabled, forces the use of pairing password for all other devices sending AirPlay requests to the device. |
| Allow managed applications from using cloud sync | If enabled, users can restrict managed apps backing up any data to iCloud, while still allowing it for user downloaded apps. |
| Allow the "Erase All Content And Settings" option in the Reset UI | If enabled, users can remove his/her personal information: credit or debit card, photos, contacts, music, or apps.<br>Note: This feature is available for supervised devices only. |
| Spotlight will return Internet search results | If enabled, the spotlight features will provide suggestions from the Internet, iTunes, and the App Store for the user to quickly find any file, documents, emails, apps contacts and more on the device. (For supervised devices only.) |
| Allow the "Enable Restrictions" option in the Restrictions UI in Settings | If enabled, users can enable or disable 'Enable Restrictions' option in the 'Restrictions' user interface on the device. (For supervised devices only.) |
| Allow activity continuation | If enabled, user can control data flow through iCloud. |
| Allow backed up enterprise books | If enabled, users can backup iBooks and restrict synchronization to iCloud. |
| Enterprise books notes and highlights will be synced | If enabled, allows the user to to sync Enterprise books, notes and highlights to iCloud. |
| Allow podcasts | If enabled users can receive their favorite podcasts.<br>Note: This feature is available only for supervised devices with iOS 8 and later versions. |
| Allow definition lookup | If enabled, allows the user to enable or disable spell check and definition features on the device.<br>Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions. |
| Allow predictive keyboard | If enabled, users can enable or disable the predictive keyboard feature. |

| | |
|---|---|
| | Note: This feature is available only for supervised devices only with iOS 8.1.3 and later versions. |
| Allow keyboard auto-correction | If enabled, allows user to enable/disable keyboard auto-correct feature.<br>Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions. |
| Allow keyboard spell-check | If enabled, allows user to enable/disable keyboard spell check feature.<br>Note: This feature is available only for supervised devices with iOS 8.1.3 and later versions. |
| Paired Apple Watch will be forced to use wrist detection | If an Apple Watch is paired with the device, the device forces the Apple Watch to enable Wrist Detection.<br>Note: This feature is available for iOS 8.2 and later versions. |
| Allow music service and music | If enabled, it allows third-party apps to add music to user's iCloud music library.<br>Note: This feature is available for iOS 9.0 and later versions. |
| Allow iCloud Photo Library | If enabled, allows the user to upload photos and videos to iCloud photo library. |
| Allow News | If enabled, users can subscribe to news services.<br>Note: This feature is available only for supervised devices with iOS 9.0 and later versions. |
| Causes AirDrop to be considered an unmanaged drop target | If enabled, all targets specified for the AirDrop feature will be considered as unmanaged drop targets.<br>Note: This feature is available for iOS 9.0 and later versions. |
| Enable the App Store on the home screen | If enabled, displays the AppStore icon on the home screen of the device. |
| Allow keyboard shortcuts | If enabled, allows the user to create and use keyboard shortcuts for typing snippets.<br>Note: This feature is available only for Supervised devices with iOS 9.0 and later versions. |
| Allow pairing with an Apple Watch | If enabled, allows the user to pair the device with an Apple Watch.<br>Note: This feature is available only for Supervised devices with iOS 9.0 and later versions. |
| Allow device passcode from being added, changed, or removed | If enabled, users can create and modify screenlock passcodes for the device.<br>Note: This feature is available only for supervised devices with iOS 9.0 and later versions. |
| Allow device name modification | If enabled, allows users to change the device name.<br>Note: This feature is available for only Supervised devices with iOS 9.0 and later versions. |
| Allow wallpaper modification | If enabled, allows user to change wallpaper displayed on the device.<br>Note: This feature is available only for supervised devices with iOS 9.0 and later versions. |

| | |
|---|---|
| Allow automatic download applications | If enabled, allows applications in the device to automatically download and install apps and updates.<br>Note: This feature is available only for supervised devices with iOS 9.0 and later versions. |
| Allow enterprise application trust | If enabled, 'Trusted' status is automatically applied to enterprise applications.<br>Note: This feature is available for iOS 9.0 and later versions. |
| Allow enterprise application trust modification | If enabled, users can manually change the Trust status of enterprise applications.<br>Note: This feature is available only for Supervised devices with iOS 9.0 and later versions. |
| Allow radio service | If enabled, users can use Radio services on their device.<br>Note: This feature is available only for Supervised devices with iOS 9.3 and later versions. |
| Allow notifications modification | If enabled, user can modify 'Apple Push Notifications' settings on the device.<br>Note: This feature is available only for Supervised devices with iOS 9.3 and later versions. |
| Whitelisted application bundles | Add applications to the app whitelist. The applications in the whitelist will be skipped from security checks during installation and usage.<br>• Enter the App bundle ID of the application to be added to the whitelist.<br>For more details on obtaining the App bundle ID, see the **explanation** at the end of this section.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>• Click the + button to add more apps to the whitelist.<br>• Click − beside an app to remove it from the list.<br>Note: This feature is available only for supervised devices with iOS 9.3 and later versions. |
| Blacklisted application bundles | Add applications to the app blacklist. The applications in the blacklist will not be allowed to be installed or used.<br>• Enter the App bundle ID of the application to be added to the blacklist.<br>For more details on obtaining the App bundle ID, see the **explanation** at the end of this section.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>• Click the + button to add more apps to the blacklist.<br>• Click − beside an app to remove it from the list.<br>Note: This feature is available only for Supervised devices with iOS 9.3 and later versions. |
| **Security and privacy** | |

| | |
|---|---|
| Allow diagnostic submission | If enabled, the device will be enabled to submit its iOS diagnostic information to Apple. |
| Allow untrusted TLS prompt | If enabled, users will be prompted if they want to trust unverified certificates.<br>This setting applies to Calendar accounts, Contacts, Safari and to Mail. |
| Force encrypted backup | If left unchecked, users can select whether or not to encrypt backups from the device to iTunes in a local computer.<br>If this option is enabled, the backup data from the device to iTunes in local computer will be automatically encrypted. |
| **Content ratings** | |
| Allow explicit music and podcasts | Content providers of iTunes flag their explicit content for easy identification.<br>If enabled, explicit content including music and video will be displayed in iTunes store instead being hidden, in the device. |
| Allow iBookstore | If enabled, users can access iBookstore, an online bookstore from Apple.<br>Note: This option is available only for supervised devices. |
| Allow iBookstore erotica | If enabled, users can download media tagged as erotica from iBooks.<br>Note: This feature is available only for Supervised devices with versions prior to iOS 6.1. |
| Rating region | Select the region whose content ratings are to be followed, from the drop-down. |
| Rating movies | Choose the content rating to be allowed for watching movies. |
| Rating TV Shows | Choose the content rating to be allowed for watching the TV shows. |
| Rating apps | Choose the rating to be allowed for using apps. |
| **Applications** | |
| Allow use of iTunes Store | If enabled, users can access iTunes store. If left unchecked, iTune store is disabled and its icon will be removed from the home screen. |
| Allow Safari | If enabled, users can use Safari for browsing internet. If left unchecked, the Safari browser app will be disabled and its icon will be removed from the home screen. |
| Allow auto fill | If enabled, the 'auto-fill' feature will be enabled for Safari, to automatically fill details such as user name, password, credit card details and so on in web forms. |
| Allow java script | If enabled, java script features will be supported by Safari. |
| Allow popups | If enabled, popups will be allowed in Safari. |
| Force fraud warning | If enabled, Safari displays alerts to users when visiting websites that are identified as compromised or fraudulent. |
| Accept cookies | Select the option on when Safari can accept cookies, from the drop- |

| | |
|---|---|
| | down. The available options:<br>• Always<br>• Never<br>• From visited site |
| Allow app cellular data modification | If enabled, user can modify cellular data usage settings for individual apps on the device.<br>Note: This feature is available only for Supervised devices with iOS 7 or later versions. |
| Allow open from Managed to Unmanaged | If enabled, users can send data from managed apps to unmanaged apps.<br>Note: This feature is available for iOS 7 and later versions. |
| Allow open from Unmanaged to Managed | If enabled, users can send data from unmanaged apps to managed apps.<br>Note: This feature is available for iOS 7 and later versions. |
| Autonomous single app mode permitted app bundle IDs | iOS apps built with the functionality of single App Lock, can provoke App Lock for them under certain scenarios in Autonomous single app mode. Administrators can specify the apps for which the mode can be enabled, by entering their App bundle IDs.<br>• Enter the App bundle ID of the application to be permitted for autonomous single app mode.<br>For more details on obtaining the App bundle ID, see the **explanation** at the end of this section.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>• To add more apps, click + button.<br>• To remove an app, click the − beside it.<br>Note: This feature is applicable only for Supervised devices with iOS 7 or later versions. |
| **iCloud** | |
| Allow cloud keychain sync | If enabled, the Apple Keychain data on the device will be synced to iCloud.<br>Note: This feature is applicable only for iOS 7 and later versions. |
| Allow cloud backup | If enabled, users can backup their device data to iCloud.<br>Note: This feature is applicable only for iOS 7 and later versions. |
| Allow cloud document sync | If enabled, users can synchronize documents on their device with iCloud.<br>Note: This feature is applicable only for iOS 7 and later versions. |
| Allow photo stream | Users can use Photo Stream.<br>Note: This feature is applicable only for iOS 7 and later versions. |
| Allow shared stream | If enabled, users can share and view photos in Photo Stream.<br>Note: This feature is applicable only for iOS 7 and later versions. |

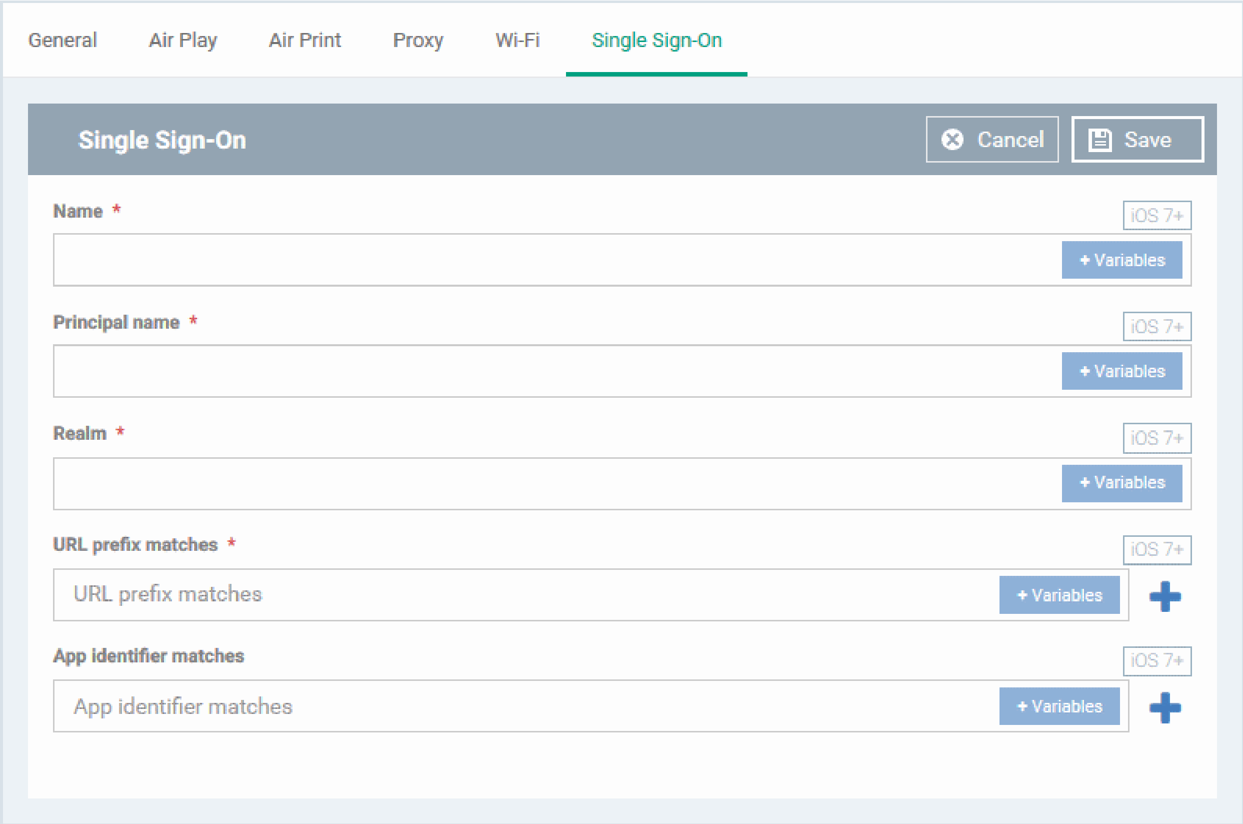
- Click the 'Save' button.

You can edit the settings or delete the section at any time. See **Edit Configuration Profiles** for more details.

### Single Sign-On settings

These settings are used to configure Kerberos authentication and are applicable for iOS 7 or later versions only. You can add several Single Sign On accounts to a profile.

- Click 'Single Sign-On' from the 'Add Profile Section' drop-down

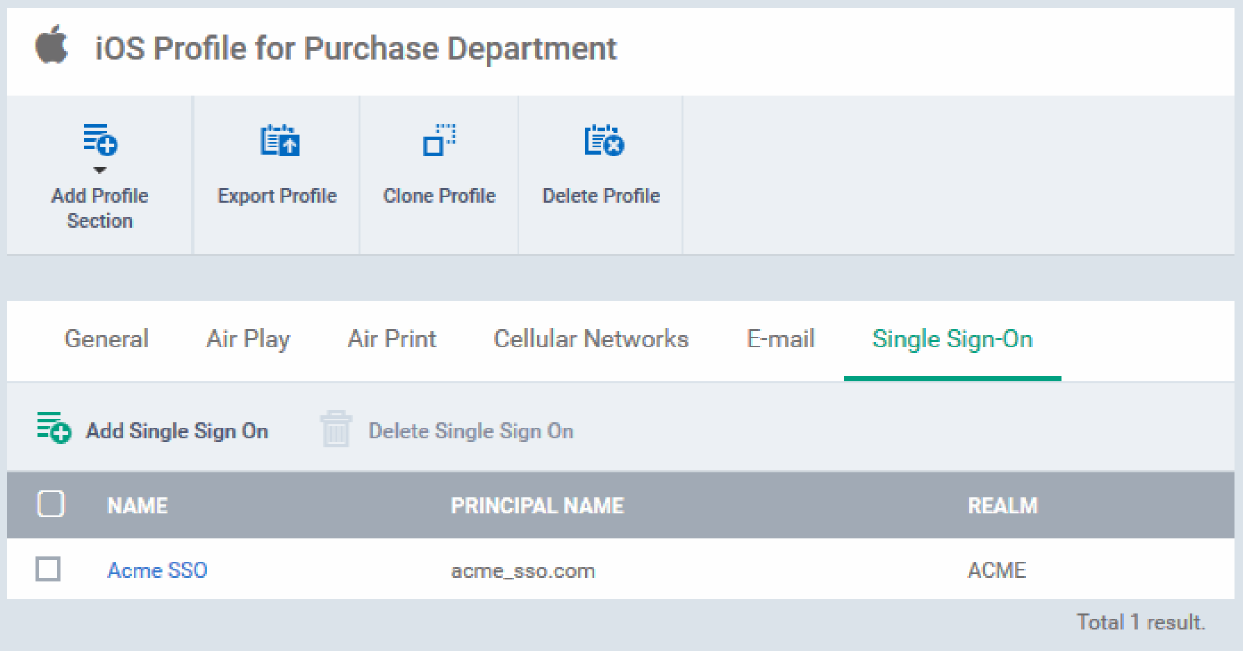


| Form Element | Description |
|---|---|
| Name* | Enter a label for the account.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Principal name* | Enter the Kerberos principal name.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Realm* | Enter the Kerberos realm name with upper-case characters.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| URL prefix matches* | Enter the URL prefix, which must be matched in order to use this account for Kerberos authentication over HTTP.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

| Form Element | Description |
|---|---|
| | Click the ➕ button to add more 'URL prefix matches' fields.<br>Click the ➖ button beside an item to remove it from the list. |
| App identifier matches | Enter the bundle IDs of apps that are allowed to use this Single Sign-On account for logging-in to respective account. If this field is left blank, this login matches all app bundle IDs.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>Click the ➕ button to add more 'URL prefix matches' fields.<br>Click the ➖ button beside an item to remove it from the list. |

- Click the 'Save' button.

The account will be added to the Single Sign-On section of the profile.



| □ | NAME | PRINCIPAL NAME | REALM |
|---|---|---|---|
| □ | Acme SSO | acme_sso.com | ACME |

Total 1 result.

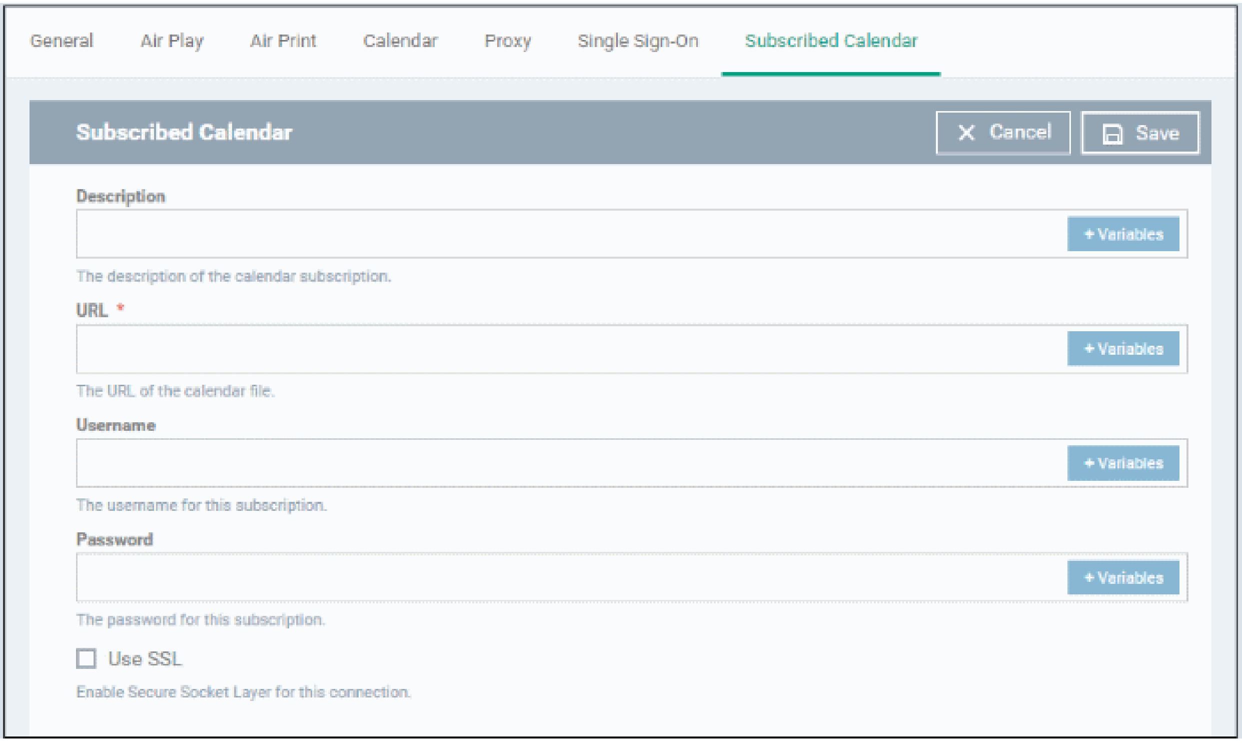
You can add several SSO accounts to the profile.

- Click 'Add Single Sign-On' and repeat the process to add more SSO accounts
- Click the name of an account to view and edit its details

This will add a 'Single Sign-On' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Subscribed Calendar settings

- Click 'Subscribed Calendars' from the 'Add Profile Section' drop-down



Description

The description of the calendar subscription.

URL *

The URL of the calendar file.

Username

The username for this subscription.

Password

The password for this subscription.

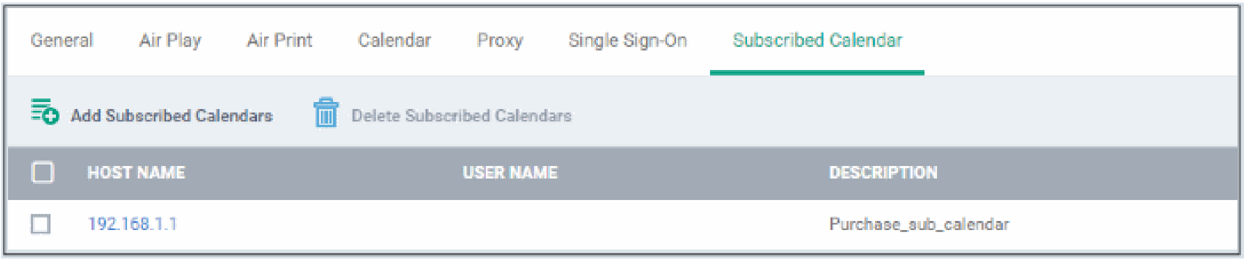
☐ Use SSL

Enable Secure Socket Layer for this connection.

| Form Element | Description |
|---|---|
| Description | Enter a description of the calendar subscription.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| URL* | Enter the URL of the calendar account to be subscribed.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Username | The user name for the subscription.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Password | 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 | If enabled, SSL connection will be established with the calendar server, if available. |

- Click the 'Save' button.

The calendar account will be added.



| ☐ | HOST NAME | USER NAME | DESCRIPTION |
|---|---|---|---|
| ☐ | 192.168.1.1 | | Purchase_sub_calendar |

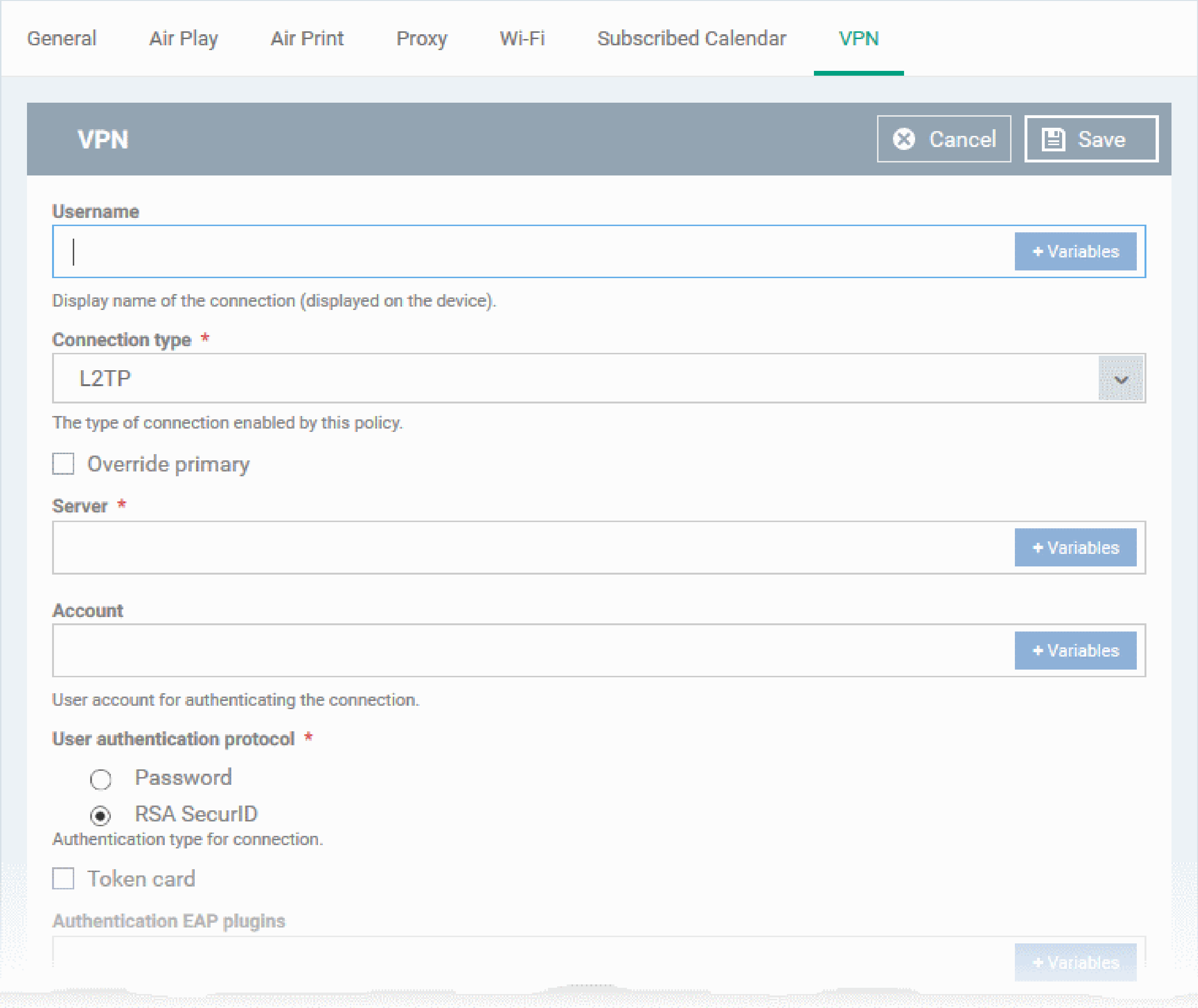
You can add several calendar accounts for a profile.

- Click 'Add Subscribed Calendars' and repeat the process to add more calendar accounts.
- Click the host name of a calendar account to view and edit its details.

This will add a 'Subscribed Calendar ' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### VPN settings

- Click 'Add Profile Section' > 'VPN'



VPN

Username

Display name of the connection (displayed on the device).

Connection type *

L2TP

The type of connection enabled by this policy.

□ Override primary

Server *

Account

User account for authenticating the connection.

User authentication protocol *

○ Password
● RSA SecurID

Authentication type for connection.

□ Token card

Authentication EAP plugins

| Form Element | Description |
|---|---|
| User name | Enter a label for the connection. This is shown on the device.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

| Form Element | Description |
|---|---|
| Connection type* | Options available are:<br>- L2TP<br>- PPTP<br>- IPSec<br>- Cisco Any Connection<br>- Juniper SSL<br>- F5 SSL<br>- Open VPN<br>The connection parameters for each type are explained in the **table below**. |
| Proxy | This drop-down shows any proxies you added to the **proxy settings section** of the profile.<br>- Choose the proxy you want the device to use.<br>See **Proxy settings** if you want help to add a new proxy. |

**VPN Connection Type settings**

| Connection Type | Description |
|---|---|
| L2TP | **Override primary -** Force VPN for all connections, including those to external domains:<br>- **Enabled -** All traffic to and from the device passes through the VPN.<br>- **Disabled -** The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Server -** Enter IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here.<br>**Account -** Enter the VPN account user name. Click the variables button + Variables to insert dynamic values here.<br>**User authentication protocol -** Select the authorization type the device uses to connect to the VPN server. The available options are 'Password' and 'RSA SecurID'.<br>- **Password -** If 'Password' is selected in 'User authentication protocol', enter the VPN account password. Click the variables button + Variables to insert dynamic values.<br>- **Token Card -** Select this if you have chosen 'RSA SecurID' in "User authentication protocol'.<br>- **Auth EAP plugins** – Applies only if RSA SecurID is being used. Enter the 'EAP-RSA' value. Click the variables button + Variables to insert dynamic values here<br>- **Shared secret -** Applies only i if RSA SecurID is being used. Click the variables button + Variables to insert dynamic values here<br>For more details on variables, see **Create and Manage Custom Variables**. |
| PPTP | **Override primary-** Force VPN for all connections, including those to external |

| Connection Type | Description |
|---|---|
| | domains:<br>• **Enabled** - All traffic to and from the device passes through the VPN.<br>• **Disabled** - The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Server** - Enter the IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here.<br>**Account** - Enter the VPN account user name. Click the variables button + Variables to insert dynamic values here<br><br>**User authentication protocol** - Select the authorization type the device uses to connect to the VPN server. The available options are 'Password' and 'RSA SecurID'<br>• **Password** - If 'Password' is selected, enter the VPN account password. Click the variables button + Variables to insert dynamic values here<br>• **Token Card** - Select this if you have chosen 'RSA SecurID' in 'Auth Protocol'.<br>• **Authentication EAP plugins** - Applies only if RSA SecurID is being used. Enter the 'EAP-RSA' value. Click the variables button + Variables to insert dynamic values here<br>• **Encryption Level** - Choose the encryption level you want to use for the VPN connection. The available options are:<br>    • None<br>    • Automatic<br>    • Maximum 128 bit encryption<br>• **Shared secret** - Applies only if RSA SecurID is used. Enter the shared secret string. Click the variables button + Variables to insert dynamic values here<br>For more details on variables, see **Create and Manage Custom Variables**. |
| IP SEC | **Override primary**- Force VPN for all connections, including those to external domains:<br>• **Enabled** - All traffic to and from the device passes through the VPN.<br>• **Disabled** - The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Server** - Enter the IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here<br>**Account** - Enter the VPN account name. Click the variables button + Variables to insert dynamic values here<br>**Password** - Enter the password for the account. Click the variables button + Variables to insert dynamic values here<br><br>**Authentication Method** - Select the authorization type the device uses to connect to the VPN server.<br>• **Shared secret** / **Group name** - Enter the shared secret string or the group name.<br>• **Certificate** - If you want client certificate type authentication, choose this |

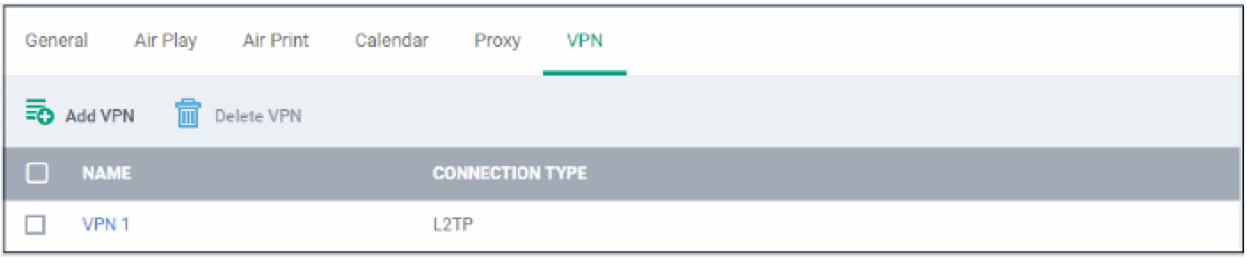
| Connection Type | Description |
|---|---|
| | option and configure the parameters as given below:<br>• **Password encryption** – Enter a password to be used as key to encrypt the communication.<br>• **Prompt for VPN PIN** – The user needs to enter the VPN PIN while connecting.<br>• **On demand enabled** - Create rules for auto-establish the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.<br>• **Certificate** - Shows certificates uploaded for the profile. Select the client certificate you want to use for authentication. See the explanation of adding certificates to the profile for more details. Click 'Add New' to upload the a new certificate.<br>• **Domain** and **Type** fields - Add a list of domains and specify VPN connection type for each domain, if 'On demand enabled' is selected.<br>• Enter a domain name in the domain field and choose the connection type:<br>**Always establish** - Initiates a VPN connection for the domain.<br>**Never establish** - No VPN connection is created for the domain.<br>**Establish if needed** - A VPN connection is created if domain name resolution fails.<br>• Click 'Add' to add the domain to the list<br>• Repeat the process to add more domains<br>For more details on variables, see **Create and Manage Custom Variables**. |
| Cisco Any Connection and F5 SSL | **Override primary**- Force VPN for all connections, including those to external domains:<br>• **Enabled** - All traffic to and from the device passes through the VPN.<br>• **Disabled** - The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Remote Address** - Enter the IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here<br>**Auth name** - Enter the VPN account name. Click the variables button + Variables to insert dynamic values here<br>**Authentication method** - Select the authorization type the device uses to connect to the VPN server.<br>• **Shared secret** / **Group name** - Enter the shared secret string or the group name.<br>• **Certificate** -<br>• **Id Certificate** - Shows certificates uploaded for the profile. Select the client certificate you want to use for authentication. See the explanation of adding certificates to the profile for more details.<br>• **On demand enabled** - Create rules to auto-establish the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.<br>• **Domain** and **Type** fields - Add a list of domains and specify VPN |

| Connection Type | Description |
|---|---|
| | connection type for each domain, if 'On demand enabled' is selected.<br>• Enter a domain name in the domain field and choose the connection type:<br>**Always establish** - Initiates a VPN connection for the domain.<br>**Never establish** - No VPN connection is created for the domain.<br>**Establish if needed** – A VPN connection is created if domain name resolution fails.<br>• Click 'Add' to add the domain to the list<br>• Repeat the process to add more domains.<br>For more details on variables, see **Create and Manage Custom Variables** |
| Juniper SSL | **Override primary** - Force VPN for all connections, including those to external domains:<br>• **Enabled** - All traffic to and from the device passes through the VPN.<br>• **Disabled** - The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Remote Address** - Enter the IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here.<br>**Auth name** - Enter the VPN account user name. Click the variables button + Variables to insert dynamic values here<br>**Realm** - Enter the name of the authentication server. Click the variables button + Variables to insert dynamic values here<br>**Role** - Enter the role of the user. Click the variables button + Variables to insert dynamic values here<br>**Authentication method** - Select the authorization type the device uses to connect to the VPN server.<br>• **Shared secret** / **Group name** - Enter the shared secret string or the group name.<br>• **Certificate** -<br>• **Certificate ID** - Shows certificates uploaded for the profile. Select the client certificate you want to use for authentication. See the explanation of adding certificates to the profile for more details.<br>• **On demand enabled** - Create rules to auto-establish the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.<br>• **Domain** and **Type** fields - Add a list of domains and specify VPN connection type for each domain, if 'On demand enabled' is selected.<br>• Enter a domain name in the domain field and choose the connection type:<br>**Always establish** - Initiates a VPN connection for the domain.<br>**Never establish** - No VPN connection is established for the domain.<br>**Establish if needed** - A VPN connection is created if domain name resolution fails.<br>• Click 'Add' to add the domain to the list |

| Connection Type | Description |
|---|---|
| | • Repeat the process to add more domains<br>For more details on variables, see **Create and Manage Custom Variables** |
| Open VPN | **Override primary-** Force VPN for all connections, including those to external domains:<br>• **Enabled** - All traffic to and from the device passes through the VPN.<br>• **Disabled** - The device accesses internal resources and intranet sites over the VPN, and external domains through a direct connection.<br>**Remote Address** - Enter the IP address or host name of the VPN server. Click the variables button + Variables to insert dynamic values here.<br>**Certificate ID** - The drop-down shows certificates uploaded for the profile. Select the client certificate you want to use for authentication. See the explanation of adding certificates to the profile for more details. Click 'Add New' to upload the a new certificate<br>• **Tip –** You can extract the certificate in .p12 format, from the Open VPN configuration file (in .ovpn format) in the VPN server.<br>• Use the command "sh split-ovpn.sh config.ovpn"<br>• Upload the certificate to the profile<br>**On demand enabled** - Create rules to auto-establish the VPN connection based on the domains accessed. You can create a list of domains and specify the VPN connection establishment type for each domain.<br>• **Domain** and **Type** fields - Add a list of domains and specify VPN connection type for each domain, if 'On demand enabled' is selected.<br>• Enter a domain name in the domain field and choose the connection type:<br>**Always establish** - Initiates a VPN connection for the domain.<br>**Never establish** - No VPN connection is created for the domain.<br>**Establish if needed** - A VPN connection is created if domain name resolution fails.<br>• Click 'Add' to add the domain to the list<br>• Repeat the process to add more domains<br>**Vendor config**<br>**Key** - The 'Key' string in the Open VPN server configuration file (in .ovpn format).<br>• Open the .ovpn file in a text editor like Notepad<br>• Copy the content between the <key> tags , excluding '-----BEGIN PRIVATE KEY-----' and '-----END PRIVATE KEY-----', and paste into the 'Key' field<br>**Value** - The 'Value' string in the Open VPN configuration file<br>• Copy the content from between the <value> tags, if present in the configuration file and paste into the 'Value' field similar to above. Else, leave this field blank.<br>• Click 'Add' to add the vendor config to the list<br>• Repeat the process to add more vendor configurations.<br>For more details on variables, see **Create and Manage Custom Variables**. |

- Click the 'Save' button.

The VPN connection is added to the profile.



| NAME | CONNECTION TYPE |
|---|---|
| VPN 1 | L2TP |

You can add several VPN accounts to the profile.

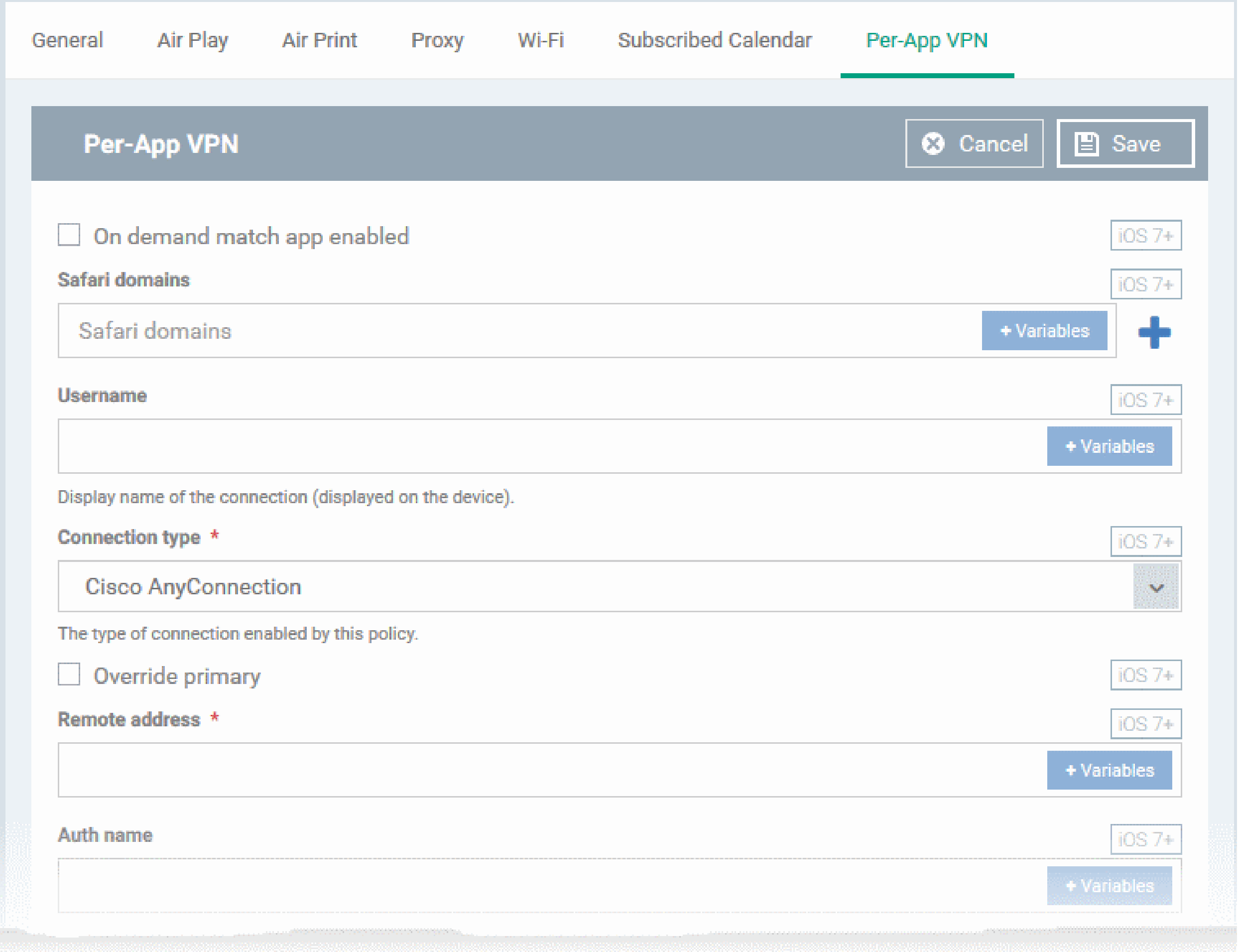
- Click 'Add VPN' and repeat the process to add more VPN accounts.
- Click the name of a VPN account to view and edit its settings

This will add a 'VPN' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Per-App VPN settings

**Note**: If you would like to connect only certain apps to VPN, then this feature allows you to configure the settings. This feature is available for iOS 7 and later versions.

- Click 'VPN Per App' from the 'Add Profile Section' drop-down



□ On demand match app enabled

Safari domains

Safari domains

Username

Display name of the connection (displayed on the device).

Connection type *

Cisco AnyConnection

The type of connection enabled by this policy.

□ Override primary

Remote address *

Auth name

- **On Demand Match App Enabled -** Select this checkbox to enable per-app VPN connection.
- **Safari domains -** Domains for which a VPN connection is established when visited through Safari browser.

Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.

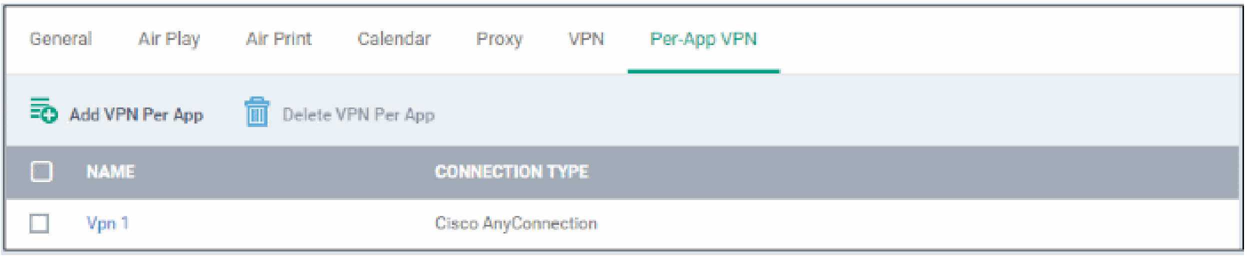
Click the ✚ button to add more domains in the field.

Click the ▬ button to remove a domain from the list

For details on other settings please see '**VPN settings**'.

- Click the 'Save' button.

The VPN per App settings for the specified VPN server will be saved and added to the list.



| □ | NAME | CONNECTION TYPE |
|---|---|---|
| □ | Vpn 1 | Cisco AnyConnection |

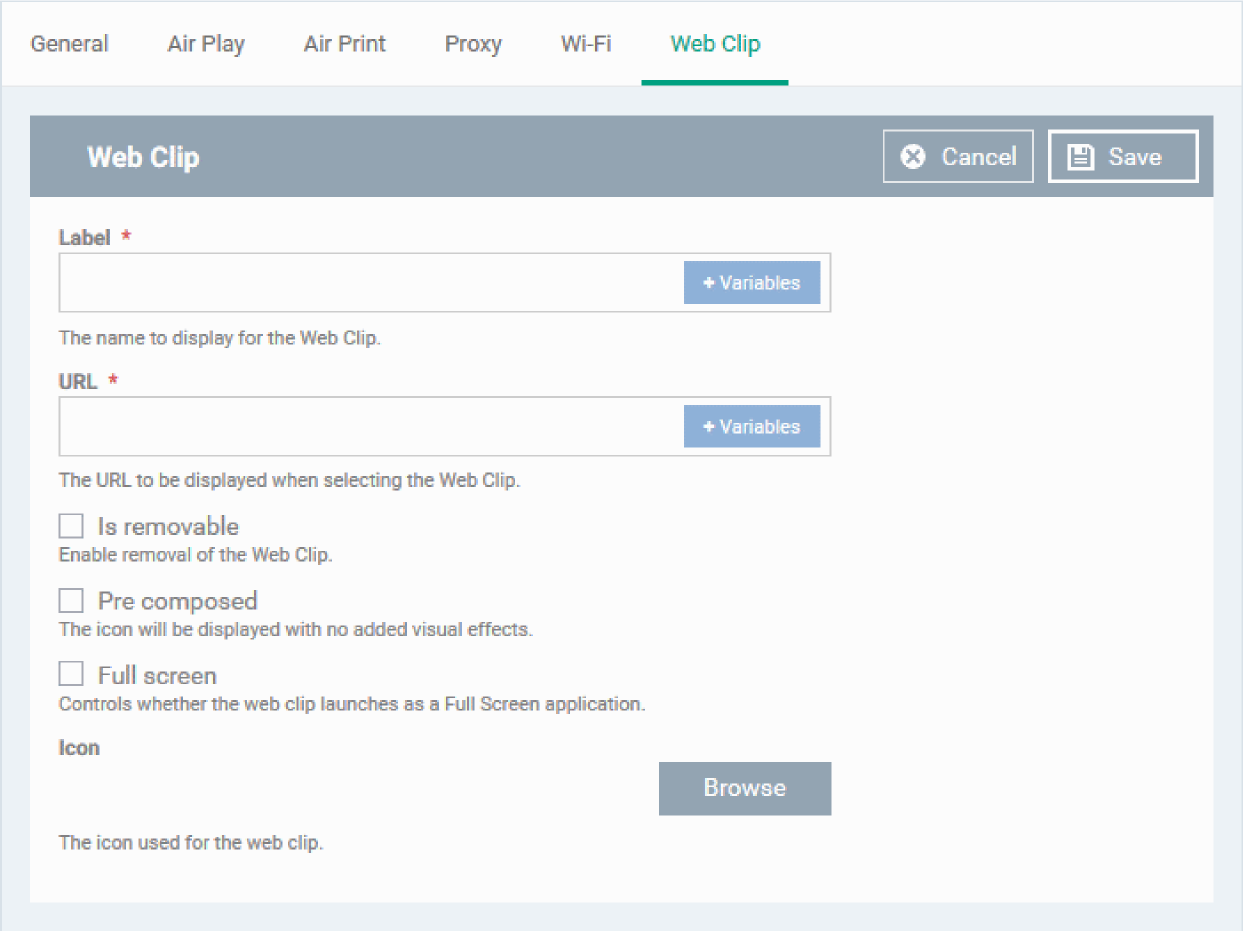
You can add multiple VPN servers for the profile.

- Click 'Add VPN per App' and repeat the process to add more VPN accounts
- Click on a VPN account name to view and edit its settings

This will add a 'Per-App VPN' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Web Clip settings

- Click 'Web Clip' from the 'Add Profile Section' drop-down



Web Clip

Label *

The name to display for the Web Clip.

URL *

The URL to be displayed when selecting the Web Clip.

□ Is removable
Enable removal of the Web Clip.

□ Pre composed
The icon will be displayed with no added visual effects.

□ Full screen
Controls whether the web clip launches as a Full Screen application.

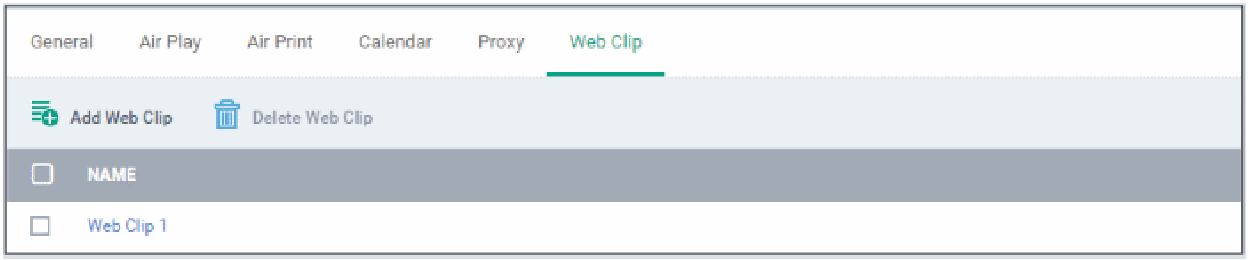
Icon

The icon used for the web clip.

| Form Element | Description |
|---|---|
| Label* | Enter a name for the web clip.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| URL* | The website address visited when the clip is opened.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Is removable | If enabled, users can remove the web clip from their devices. |
| Pre composed | If enabled, the web clip icon will be shown with no added visual effects. |
| Full screen | If enabled, the user can choose to view the web clip full screen mode. |
| Icon | Upload the image to be used as icon for the web clip. |

- Click the 'Save' button.

The web clip will be added to the list.



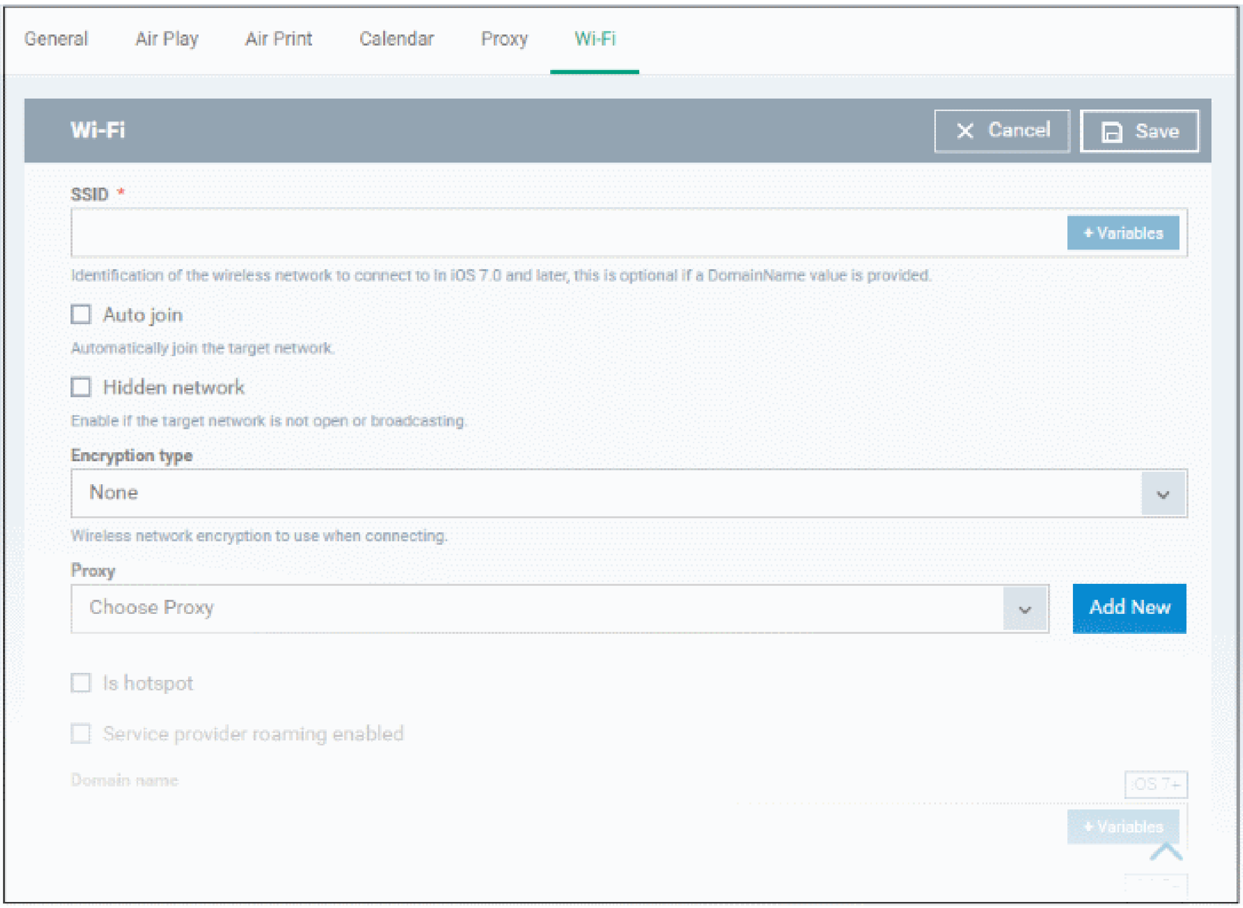
You can add multiple web clips for a profile.

- Click 'Add Web Clip' and repeat the process to add more webclips
- Click the name of a web clip to view and edit its settings

The settings will be saved and shown under the 'Web Clip' tab. You can add more web clips and edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

### Wi-Fi settings

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



SSID *

Identification of the wireless network to connect to In iOS 7.0 and later, this is optional if a DomainName value is provided.

□ Auto join

Automatically join the target network.

□ Hidden network

Enable if the target network is not open or broadcasting.

Encryption type

None

Wireless network encryption to use when connecting.

Proxy

Choose Proxy

□ Is hotspot

□ Service provider roaming enabled

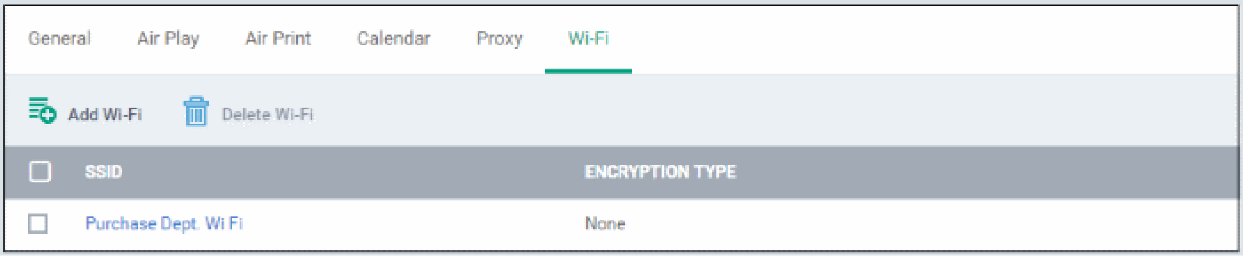
Domain name

| Form Element | Description |
|---|---|
| SSID* | Enter a unique identifier (Service Set Identifier) of the wireless network that the device should connect to.<br>Note: In iOS 7 and later versions, this is optional if the '**Domain Name**' value is set. |
| Auto join | The device will automatically connect to the configured wireless network. |
| Hidden network | Select this option if the specified wireless network is hidden and not visible to Wi-Fi scans. |
| Encryption type | Select the type of encryption used by the wireless network from the drop-down. The available options are:<br>• None<br>• WEP<br>• WPA / WPA2<br>• Any<br>• WEP Enterprise<br>• WPA / WPA2 Enterprise<br>• Any (Enterprise)<br>The Password field will appear if any of the options, 'WEP', 'WPA / WPA2' and 'Any' are chosen.<br>If any of the Enterprise encryption type is chosen, then select the supported protocols and configure authentication. The options available are: TLS, LEAP, |

| | |
|---|---|
| | TTLS, PEAP, EAP-FAST, Use Pac, Provision pac and Provision Pac Anonymously, PAP, CHAP, MS CHAP ans MS CHAP V2 |
| Password | Enter the password to connect to the Wi-Fi network. If left blank, the user will be prompted to enter the password when the device attempts to connect to the network. |
| Proxy | The proxy servers you added to the **proxy settings section** of the profile are available for selection in the 'Proxy' drop-down<br>- Choose the proxy to be used by the device for connecting to internet through the Wi-Fi connection.<br>You can also add new proxy servers:<br>- Click the 'Add New' and specify the proxy server settings.<br>- Repeat the process to add more proxies<br>- See '**Proxy settings**' for more help with this. |
| Is hotspot | If enabled, the network is treated as a hotspot. |
| Service provider roaming enabled | If enabled, devices can connect to roaming service providers. |
| Domain name | Enter the domain name of the Wi-Fi network to which the device has to connect.<br>This is optional and can be provided instead of SSID.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>Note: This feature is available for iOS 7 and later versions. |
| Displayed operator name | Enter the name of the Wi-Fi network provider, to be shown on the device to te user.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>Note: This feature is available for iOS 7 and later versions. |
| Roaming consortium OIs | Enter the Roaming Consortium Organization Identifier of the Wi-Fi network provider to which the devices will connect to.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>- Click the ➕ button to add more Roaming Consortium OIs fields.<br>- Click the ➖ to remove a field.<br>Note: This feature is available for iOS 7 and later versions. |
| NAI Realm Names | Enter the Network Access Identifier (NAI) realm names used for Wi-Fi hotspot 2.0.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>- Click the ➕ button to add more NAI Realm Names.<br>- Click the ➖ to remove a field.<br>Note: This feature is available for iOS 7 and later versions. |

- Click the 'Save' button.

The Wi-Fi network will be added to the list.



| □ | SSID | ENCRYPTION TYPE |
|---|---|---|
| □ | Purchase Dept. Wi Fi | None |

You can add multiple Wi-Fi networks to the profile.

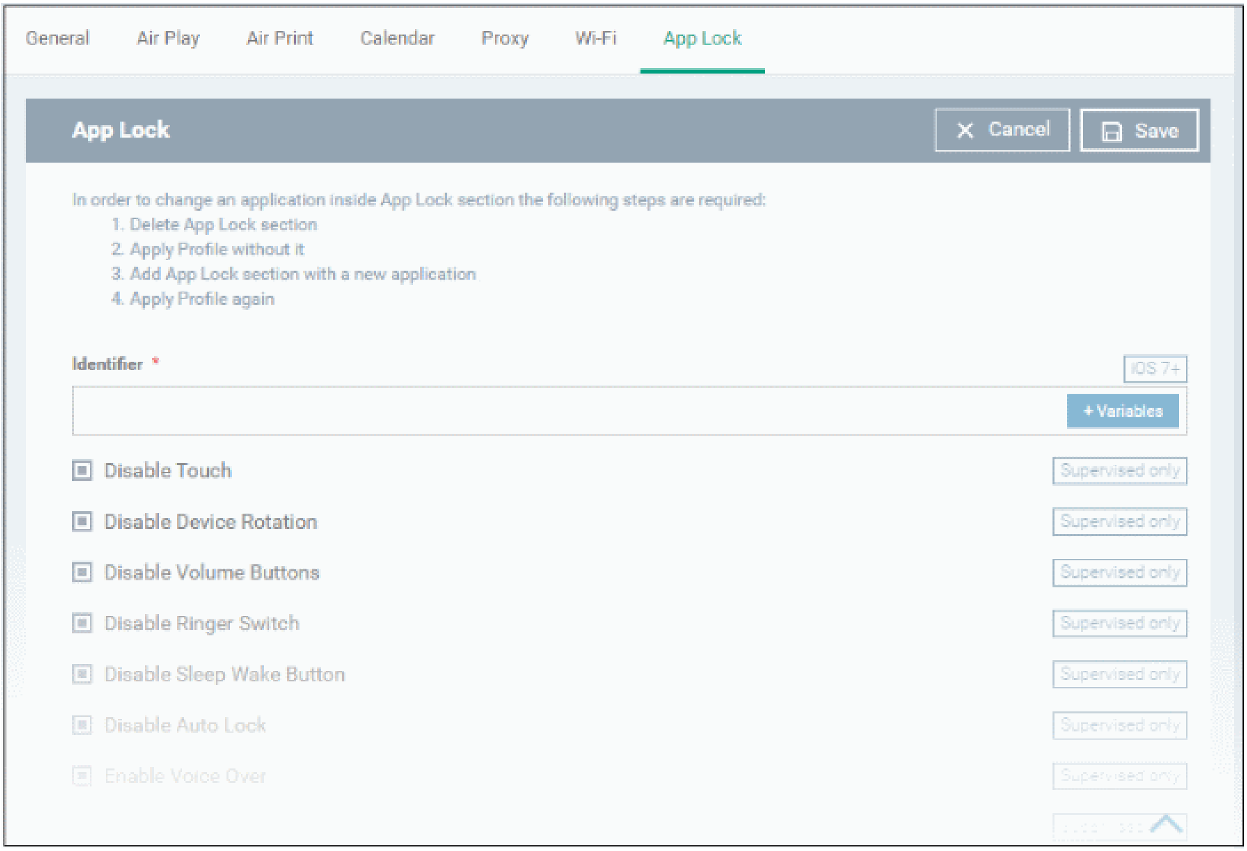
- Click 'Add Wi-Fi' and repeat the process to add more Wi-Fi networks
- Click the SSID of a WiFi network to view and edit its settings

This will add a 'Wi-Fi' section to the profile. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

## App Lock settings

The 'App Lock' section allows you to restrict the ability of specific applications to use device resources. You can add only one application with app restriction settings for a profile. If you want to impose restrictions on several applications, create a profile for each and apply those profiles to the managed devices, as required.

- Click 'App Lock' from the 'Add Profile Section' drop-down



In order to change an application inside App Lock section the following steps are required:

1. Delete App Lock section
2. Apply Profile without it
3. Add App Lock section with a new application
4. Apply Profile again

Identifier *

☐ Disable Touch

☐ Disable Device Rotation

☐ Disable Volume Buttons

☐ Disable Ringer Switch

☐ Disable Sleep Wake Button

☐ Disable Auto Lock

☐ Enable Voice Over

| Form Element | Description |
|---|---|
| Identifier | Specify the app to be included. You can add an Apple iTunes Store App or Enterprise App.<br>• Enter the App bundle ID of the application<br>For more details on getting the App bundle ID of an application, see the **explanation** given below this table.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables.<br>**Note**: This feature is available for iOS 7 and later versions only. |
| Disable touch | Touch screen inputs will be disabled for the app. |
| Disable device rotation | The app will not be able to change display orientation. |
| Disable volume buttons | The app will not be able to modify device volume. |
| Disable ringer switch | Inputs through the ringer switch will be disabled for the app. |
| Disable sleep wake button | Inputs through the power/lock/wake button will be disabled for the app. |
| Disable auto lock | The device will not auto-lock when this app is running. |
| Enable voice over | Allows the user to use the voice over feature on the device for this app. |
| Enable zoom | Allows the user to zoom-in/zoom-out the display for this app |
| Enable invert colors | Allows the user to invert the colors for the display screens of this app. |
| Enable assistive touch | Allows the user to use the 'Assistive Touch' feature on the device for this app. |
| Enable speak selection | Allows the user to use the 'Speak Selection' feature on the device for this app. |
| Enable mono audio | Allows the user to choose mono mode for audio output of this app. |
| VoiceOver | Automatically switches ON the 'Voice Over' feature for the app. |
| Zoom | Automatically switches ON the 'zoom-in' feature for the app. |
| Invert colors | Automatically switches ON the 'Invert Colors' feature when the app is used. |
| Assistive touch | Automatically switches ON the 'Voice Over' feature when the app is used. |

- Click Save after configuring the parameters and options

The settings will be saved and shown under 'App Lock' tab. You can edit the settings or remove the 'App Lock' section from the profile at anytime See **Edit Configuration Profiles** for more details.

## Obtain App Identifier

**App Store Application:**

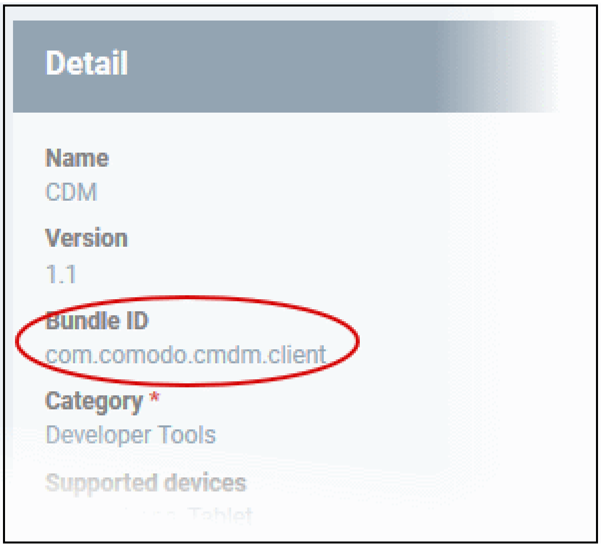
1. Find the iTunes Store download URL of the app. Example: https://itunes.apple.com/us/app/cmdm/id807480077?mt=8.
2. Copy the number after the id in the URL. (Here it is: 807480077).
3. Open https://itunes.apple.com/lookup?id=807480077 where you replace the ID with the one you looked up.

4. Search the output for "bundleID". In this example: "bundleId":"com.comodo.cmdm.client". So the Bundle ID is com.comodo.cmdm.client

**Enterprise Application:**

The App bundle ID can be viewed from the App Details screen of the App.

- Click 'Application Store' from the left and choose 'iOS Store'
- Click on the app from the list displayed at the right



Detail

Name
CDM

Version
1.1

Bundle ID
com.comodo.cmdm.client

Category *
Developer Tools

Supported devices

## 6.1.3. Profiles for Windows Devices

Windows profiles let you specify settings for Comodo Client Security (CCS) installed on managed Windows devices.

There are two ways you can add a Windows profile:

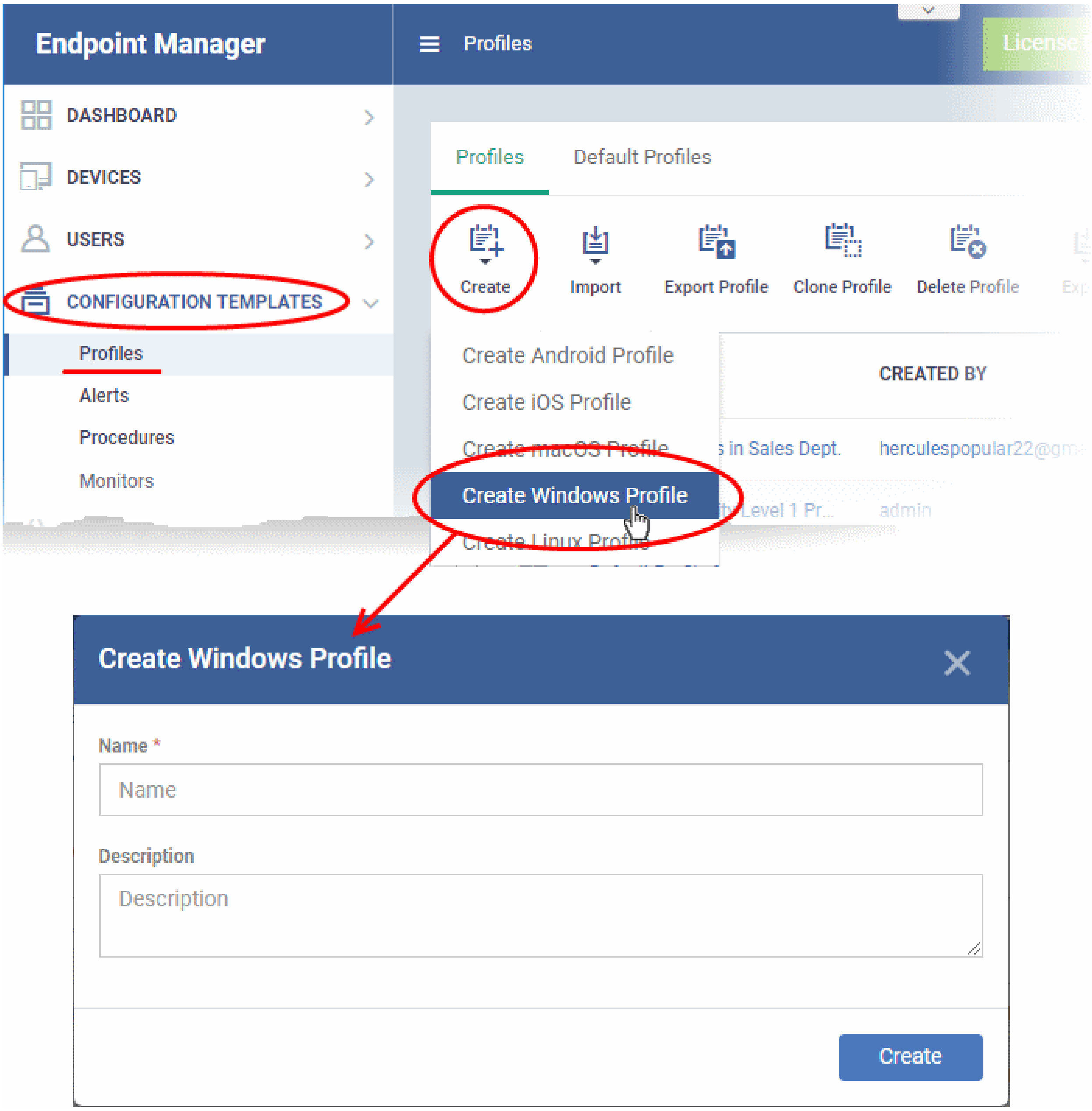
- Create a profile in the EM interface. See **Create Windows Profiles** for more details.
- Import a profile from an endpoint which is running CCS, or import from a stored configuration profile (.cfg file). See **Import Windows Profiles** for more details.

### 6.1.3.1. Create Windows Profiles

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' then 'Create Windows Profile'
- Type a name and description for your profile then click 'Create'
- The new profile will appear in 'Configuration Templates' > 'Profiles'. Click the profile name to open its configuration screen.
- New profiles have only one section - 'General'. Click 'Add Profile Section' to configure settings for other sections. Each section you add will appear as a new tab.
- After you have configured your profile you can apply it to devices, users and device groups/user groups.
- You can make any profile a 'Default' profile by selecting the 'General' tab then clicking the 'Edit' button.
    - A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- This part of the guide explains the processes above in more detail, and includes descriptions of each profile section.

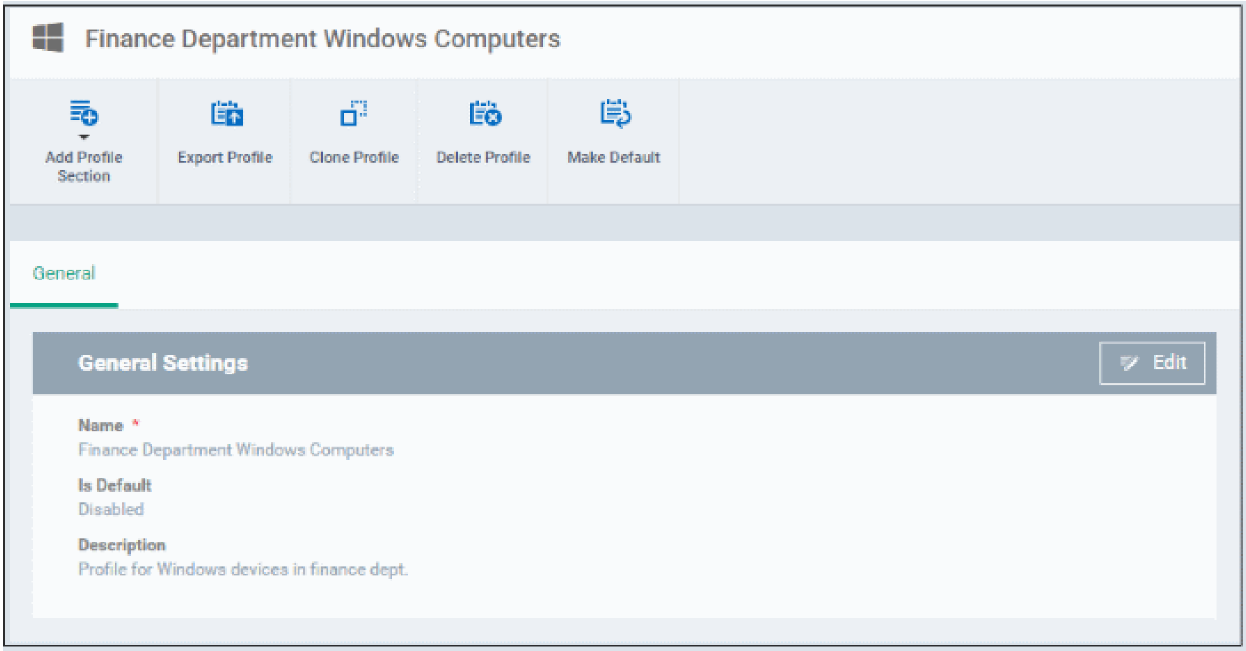
**Create a new profile**

- Click 'Configuration Templates' > 'Profiles' > 'Create' > 'Create Windows Profile':



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

Your profile will open at its configuration page:



Name *
Finance Department Windows Computers

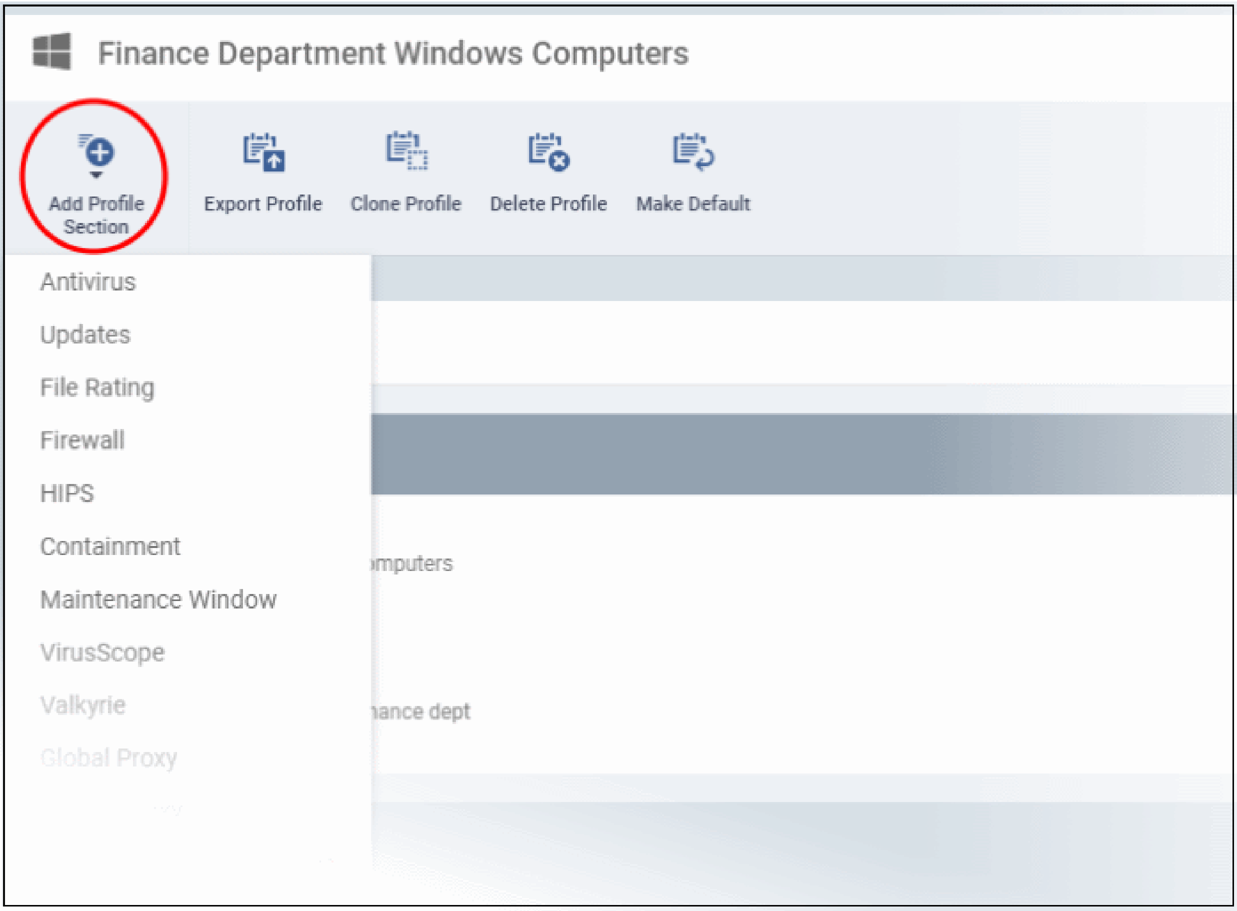
Is Default
Disabled

Description
Profile for Windows devices in finance dept.

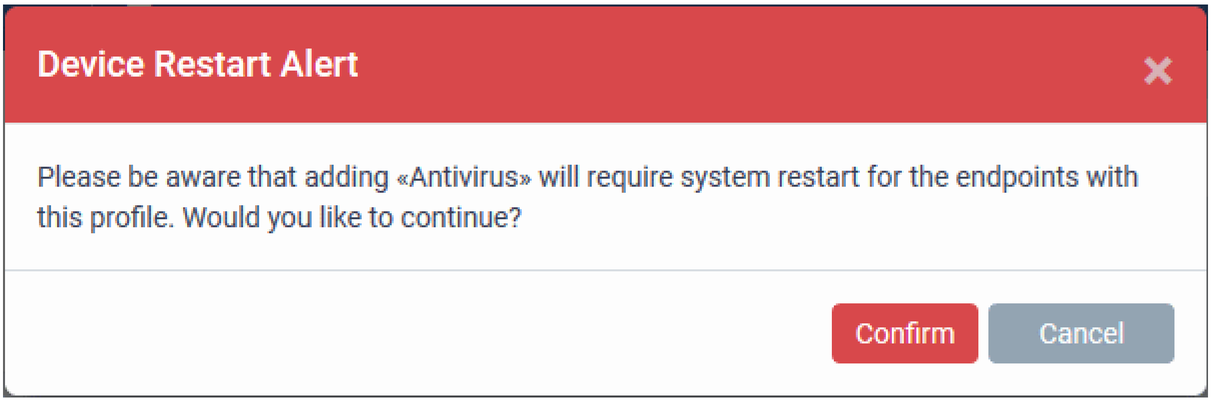
- Click 'Edit' if you wish to modify basic profile settings:
    - **'Is Default?'** - A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- Click 'Save'.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific security or management feature.
- For example, there are profile sections for 'Antivirus', 'External Device Control', 'Firewall', 'Procedures' and so on.
- You can add as many different sections as you want when building your profile.
- To get started:
    - Click 'Add Profile Section'
    - Select the component that you want to add to the profile:



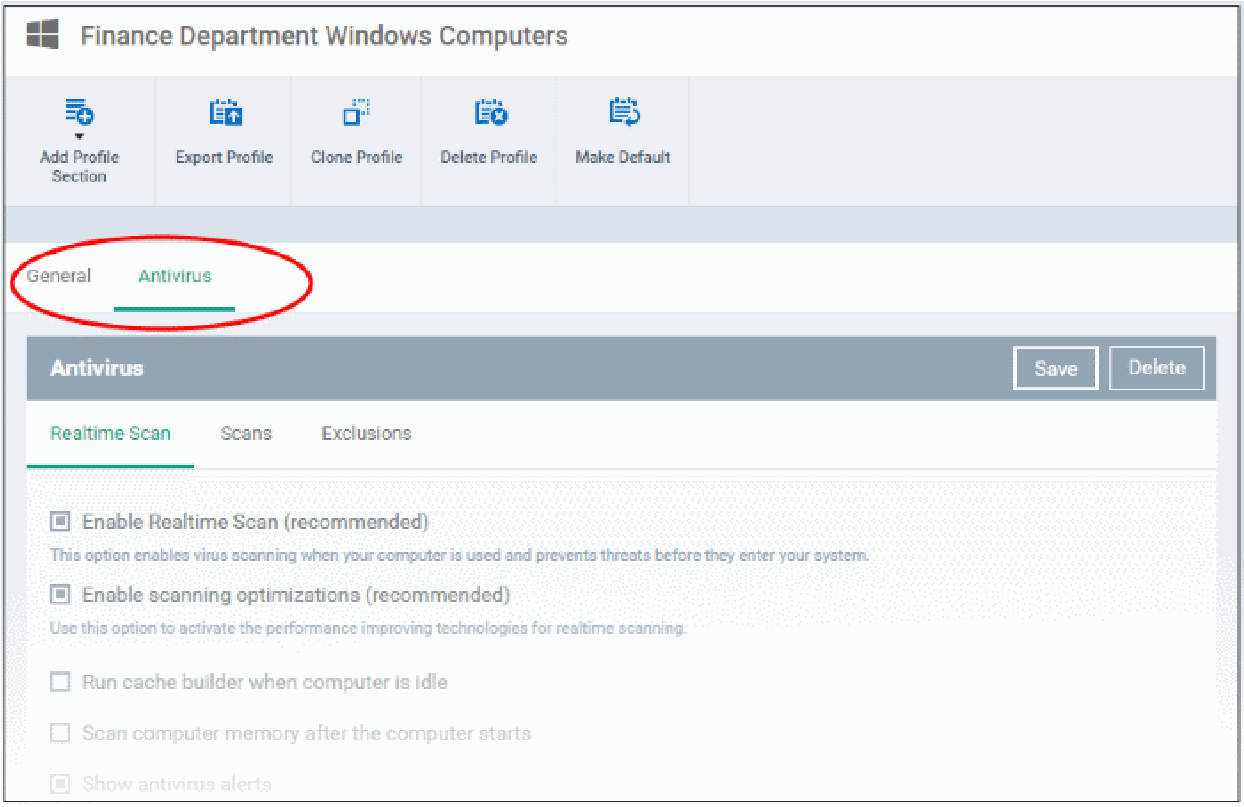
- Some sections require that target endpoints are restarted. You will see the following message if this is the case:



Please be aware that adding «Antivirus» will require system restart for the endpoints with this profile. Would you like to continue?

- Click 'Confirm' to continue.

The new section will be available as a tab in the profile configuration page:



☑ Enable Realtime Scan (recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (recommended)

Use this option to activate the performance improving technologies for realtime scanning.

☐ Run cache builder when computer is idle

☐ Scan computer memory after the computer starts

☑ Show antivirus alerts

Use the following links to learn more about each profile section:

- **Antivirus**
- **Update Settings**
- **File Rating**
- **Firewall**
- **HIPS**
- **Containment**
- **Maintenance Window**
- **VirusScope**
- **Valkyrie**
- **Global Proxy**
- **Clients Proxy**
- **Agent Discovery Settings**
- **UI Settings**
- **Logging Settings**
- **Client Access Control**
- **External Devices Control**
- **Monitors**
- **Procedures**
- **Remote Control**
- **Remote Tools**
- **Miscellaneous**

- **Script Analysis Settings**

### 6.1.3.1.1. Antivirus Settings

The antivirus settings screen lets you configure real-time monitoring, custom scans and scan exclusions.

- Tip. Add a 'Miscellaneous' section to the profile if you want to setup registry monitoring. See **Miscellaneous Settings** for more details.

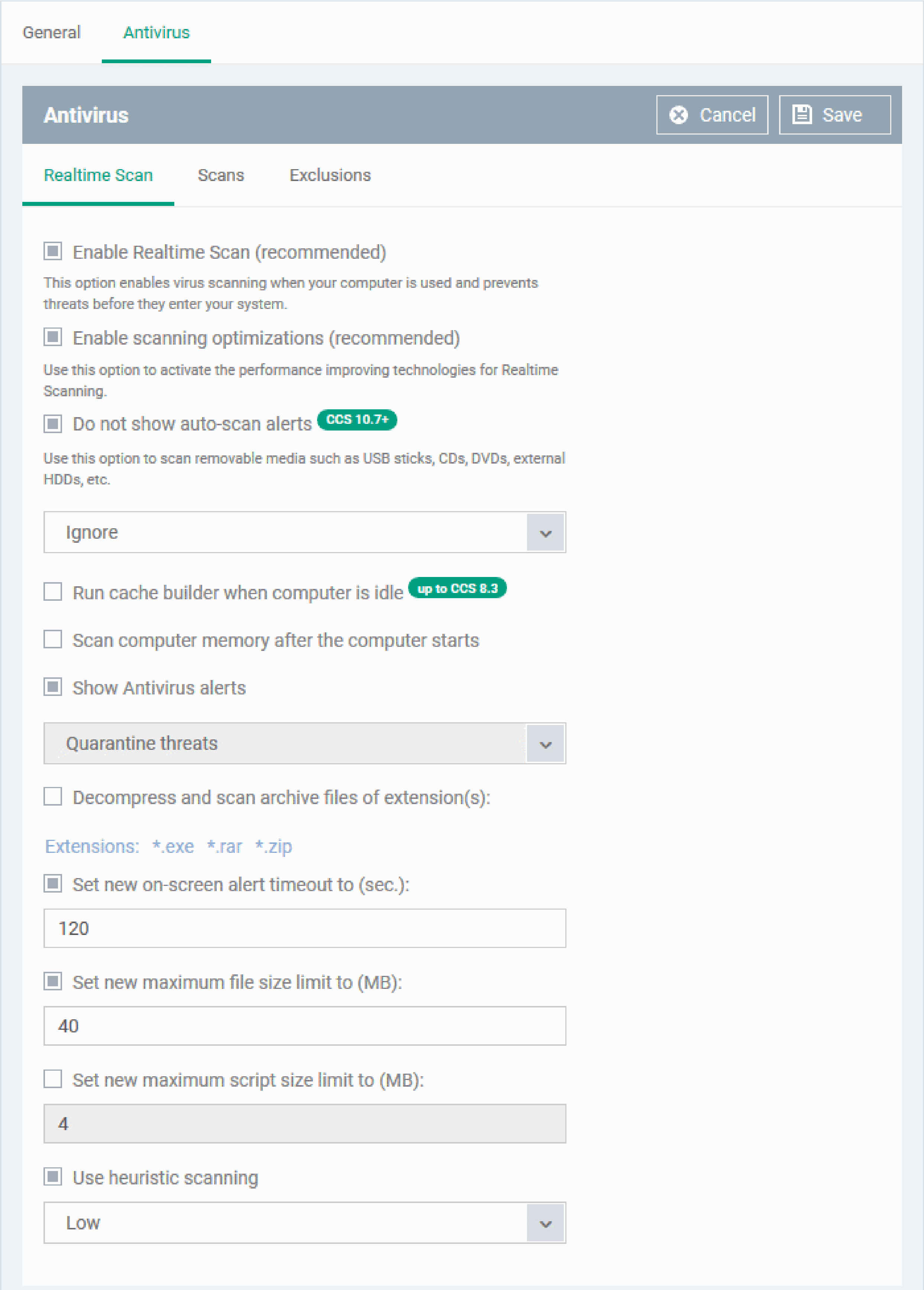
**Configure Antivirus settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you want to work on
- Click 'Add Profile Section' > 'Antivirus'

The AV settings screen will open:

- **Real Time Scan** - Configure the 'always-on' virus monitor. This is the core antivirus scanner that continuously protects your endpoints against malware.
- **Scans** - Create a custom scan profile. A custom profile lets you scan specific areas and configure other options. You can also create a schedule for the scan. Multiple scan profiles can be added to a device profile.
- **Exclusions** - Files and folders that should be skipped on devices to which the profile is applied. Items you add here are excluded from real-time scans and any custom scan profiles.

**Realtime Scan settings**



☑ Enable Realtime Scan (recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (recommended)

Use this option to activate the performance improving technologies for Realtime Scanning.

☑ Do not show auto-scan alerts CCS 10.7+

Use this option to scan removable media such as USB sticks, CDs, DVDs, external HDDs, etc.

Ignore

□ Run cache builder when computer is idle up to CCS 8.3

□ Scan computer memory after the computer starts

☑ Show Antivirus alerts

Quarantine threats

□ Decompress and scan archive files of extension(s):

Extensions: *.exe *.rar *.zip

☑ Set new on-screen alert timeout to (sec.):

120

☑ Set new maximum file size limit to (MB):

40

□ Set new maximum script size limit to (MB):

4

☑ Use heuristic scanning

Low

| Realtime Scan Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Realtime Scan | The realtime scanner ensures your devices are constantly protected from malware. The scanner inspects files whenever they are created, opened or copied.<br>• Choose whether of not to enable real time scanning.<br>(***Default = Enabled***) |
| Enable Scanning Optimizations | Various techniques to improve antivirus scan performance and reduce resource use.<br>• Choose whether or not to enable scan optimization.<br>(***Default = Enabled***) |
| Do not show auto-scan alerts | Choose whether or not to show a notification to end-users when an external device is connected to the endpoint.<br>• CCS can automatically scan external devices whenever they are connected. Example devices include external HDD's, USB sticks etc.<br>• Show alerts - End user can choose whether or not to scan the device from the alert<br>• Don't show alerts - You have a choice of default responses that CCS should take:<br>  • Ignore - The device will not be scanned<br>  • Scan - The device will be scanned for viruses<br>(***Default = Enabled with 'Ignore' option***) |
| Run cache builder when computer is idle | The antivirus cache builder runs whenever the computer is idle to boost the speed of real-time scans.<br>(***Default = Disabled***)<br>• Applies only to CCS versions 8.3 or lower. |
| Scan computer memory after the computer starts | If enabled, CCS will scan system memory for threats after a re-boot.<br>(***Default = Disabled***) |
| Show antivirus alerts | Configure whether or not to show alerts on the endpoints when malware is discovered.<br>Disabling will minimize disturbance to the end-user but at some loss of user awareness.<br>If you choose not to show alerts then you have a choice of default responses that CCS should automatically take:<br>• Quarantine threats - Moves detected threat(s) to quarantine for assessment.<br>• Block threats - Prevents the file from running<br>(***Default = Enabled with 'Quarantine threats' option***) |
| Decompress and scan archive files of extensions | The antivirus will open and scan archive files such as .jar, RAR, ZIP, ARJ, WinARJ and CAB.<br>If enabled, you can choose which types of archive should be decompressed and scanned. Click the 'Extensions' link to view existing extensions and add new extensions.<br>(***Default = Disabled***) |
| Set new on-screen alert timeout to (secs) | Specify how long an alert should stay on the screen at an endpoint.<br>(***Default = 120 seconds***) |

| | |
|---|---|
| Set new maximum file size to (MB) | Specify the maximum file size that the antivirus should attempt to scan.<br>Files larger than the size specified here will not be not scanned. (***Default = 40 MB***) |
| Set new maximum script size limit to (MB) | Specify the maximum size of a script that the antivirus should attempt to scan.<br>Files larger than the size specified here are not scanned. (***Default = 4 MB***) |
| Use heuristic scanning | Enable or disable heuristics scanning and define the scan level.<br>The scan level determines how likely the scanner is to classify an unknown file as a threat.<br>• Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)<br>• Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.<br>• High- Highest sensitivity to detecting unknown threats / increased possibility of false positives.<br>(***Default = Enabled with 'Low ' option***)<br>**Background Note**: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing a file to ascertain whether it contains code typical of a virus. It is about detecting attributes which resemble a virus, rather than looking for a signature that matches a signature on the virus blacklist. This allows the engine to predict the existence of new viruses - even if they are not in the current virus database. |

- Click the 'Save' button at the bottom.

**Custom Scans**

The 'Scans' pane allows you to view, edit, create and run custom scan profiles. Each scan profile is a collection of scanner settings that tell CCS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (options that let you specify the behavior of the scan engine when running this profile
- You can add multiple scan-profiles to a device profile.

Endpoint Manager ships with three pre-configured scan profiles:

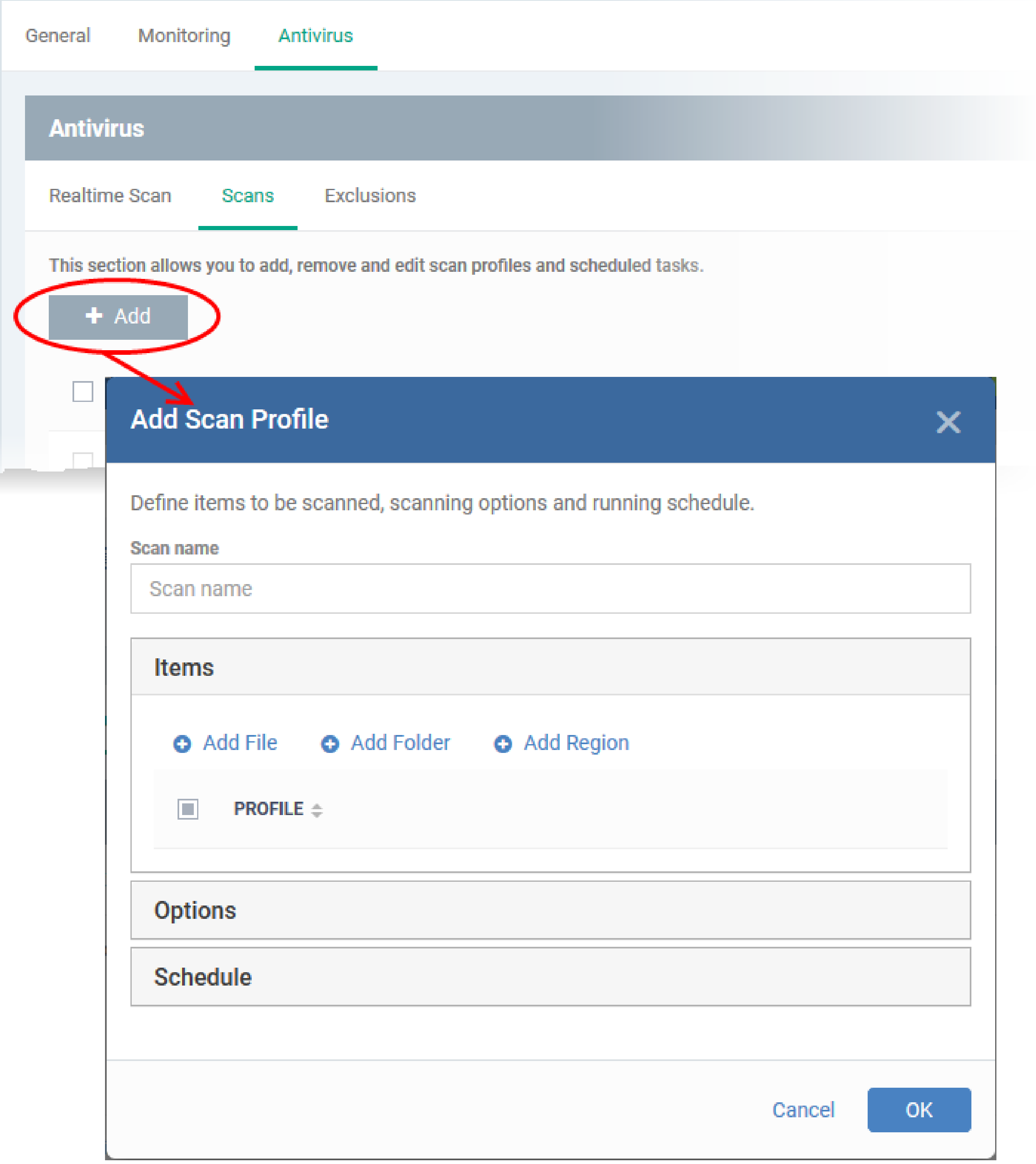
- Full Scan - CCS scans every drive, folder and file on the target device. External devices like USB drives and digital camera will also be scanned.
- Quick Scan - CCS scans critical areas which are most prone to attack from malware. Scanned areas include system memory, auto-run entries, hidden services, boot sectors and other significant areas.
- Unrecognized and Quarantined Files Scanning - CCS only scans quarantined files and files which have an 'unknown' trust rating. CCS will run a file-lookup to obtain their trust rating from the latest cloud database.

Click the 'Edit' icon ✎ beside a profile name to modify which items are scanned, and to set up a scan schedule. For details on the parameters, see the **explanation** below.

**Create a custom scan profile**

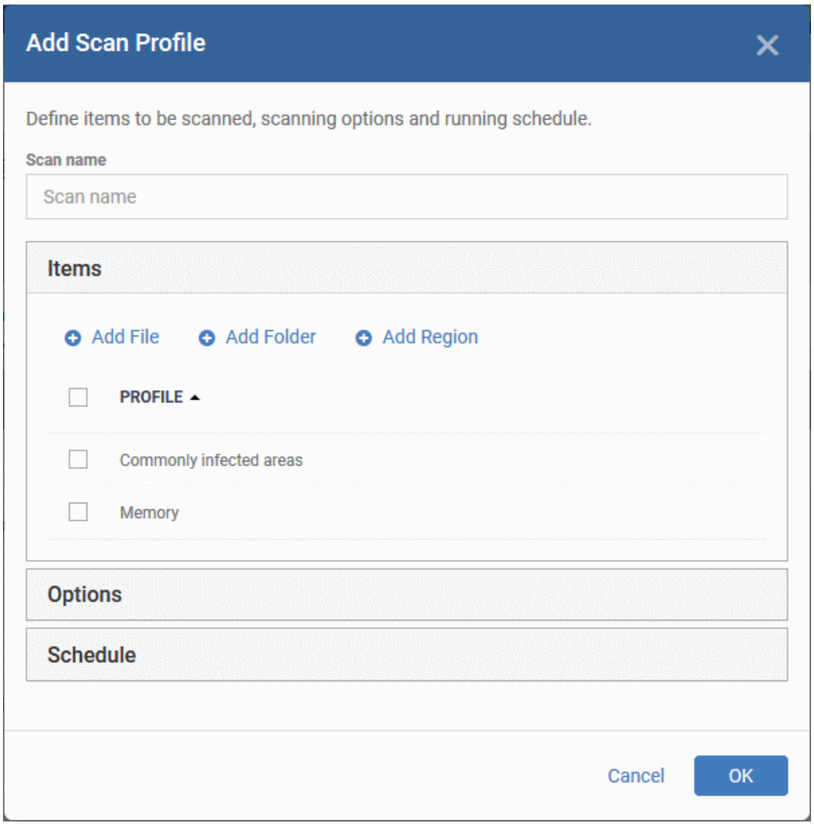
- Open the 'Antivirus' section of your profile.
  - 'Configuration Templates' > 'Profiles' > open the target profile
  - Open the 'Antivirus' section, or click 'Add Profile Section' > 'Antivirus'

- Click the 'Scans' tab.
- Click the 'Add' button:



- Enter the name of the custom scan in the 'Scan name' field
- Choose the files, folder or regions you want to scan

Target items are shown as follows:



Add Scan Profile

Define items to be scanned, scanning options and running schedule.

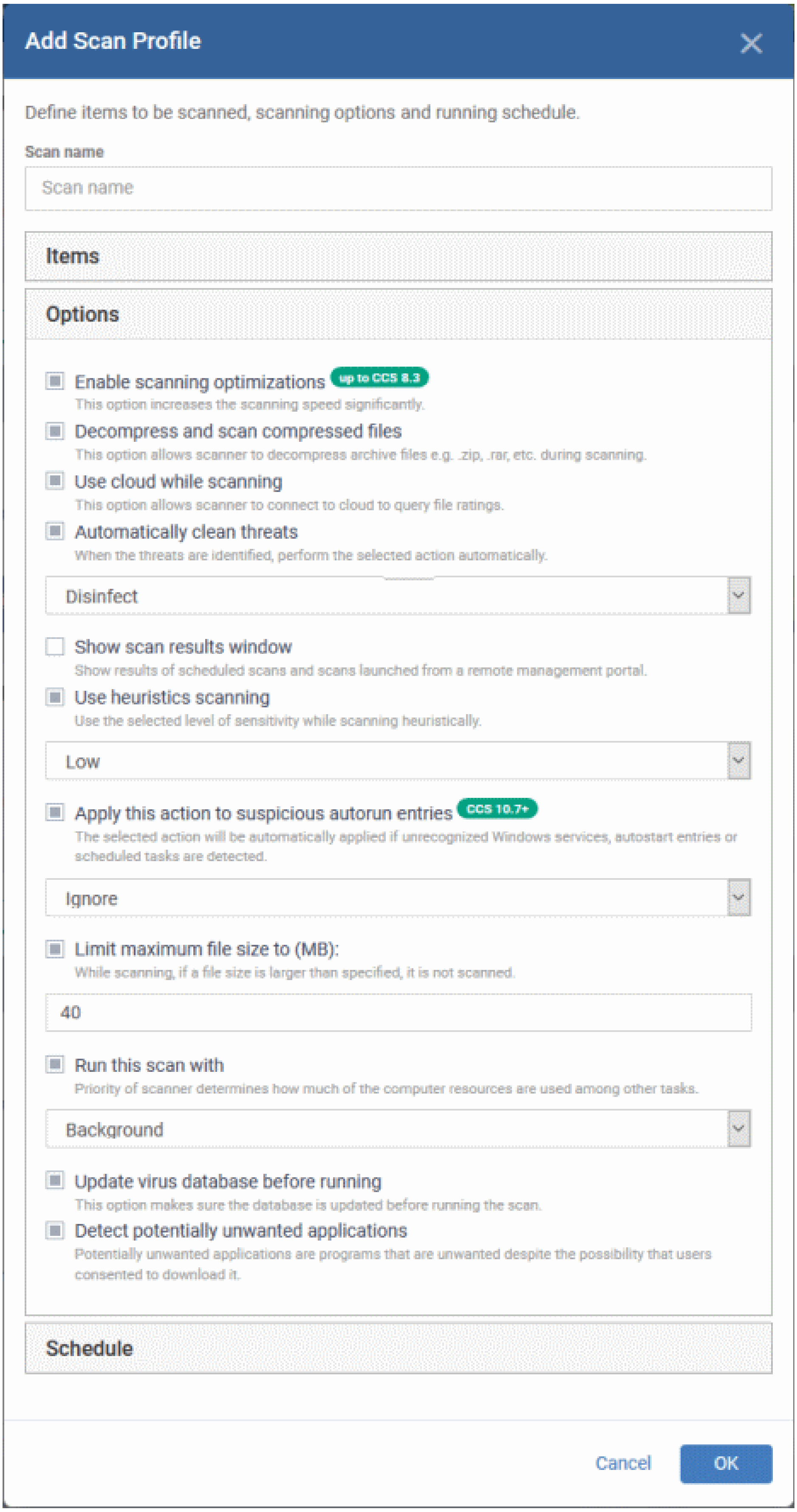
Scan name: Scan name

Items

| □ | PROFILE ▲ |
|---|---|
| □ | Commonly infected areas |
| □ | Memory |

Next, choose your scan options:

- Click the 'Options' bar
- See the table below the screenshot for a description of each option:



## Add Scan Profile

Define items to be scanned, scanning options and running schedule.

Scan name

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
This option allows scanner to connect to cloud to query file ratings.

☑ Automatically clean threats
When the threats are identified, perform the selected action automatically.

Disinfect

□ Show scan results window
Show results of scheduled scans and scans launched from a remote management portal.

☑ Use heuristics scanning
Use the selected level of sensitivity while scanning heuristically.

Low

☑ Apply this action to suspicious autorun entries
The selected action will be automatically applied if unrecognized Windows services, autostart entries or scheduled tasks are detected.

Ignore

☑ Limit maximum file size to (MB):
While scanning, if a file size is larger than specified, it is not scanned.

40

☑ Run this scan with
Priority of scanner determines how much of the computer resources are used among other tasks.

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

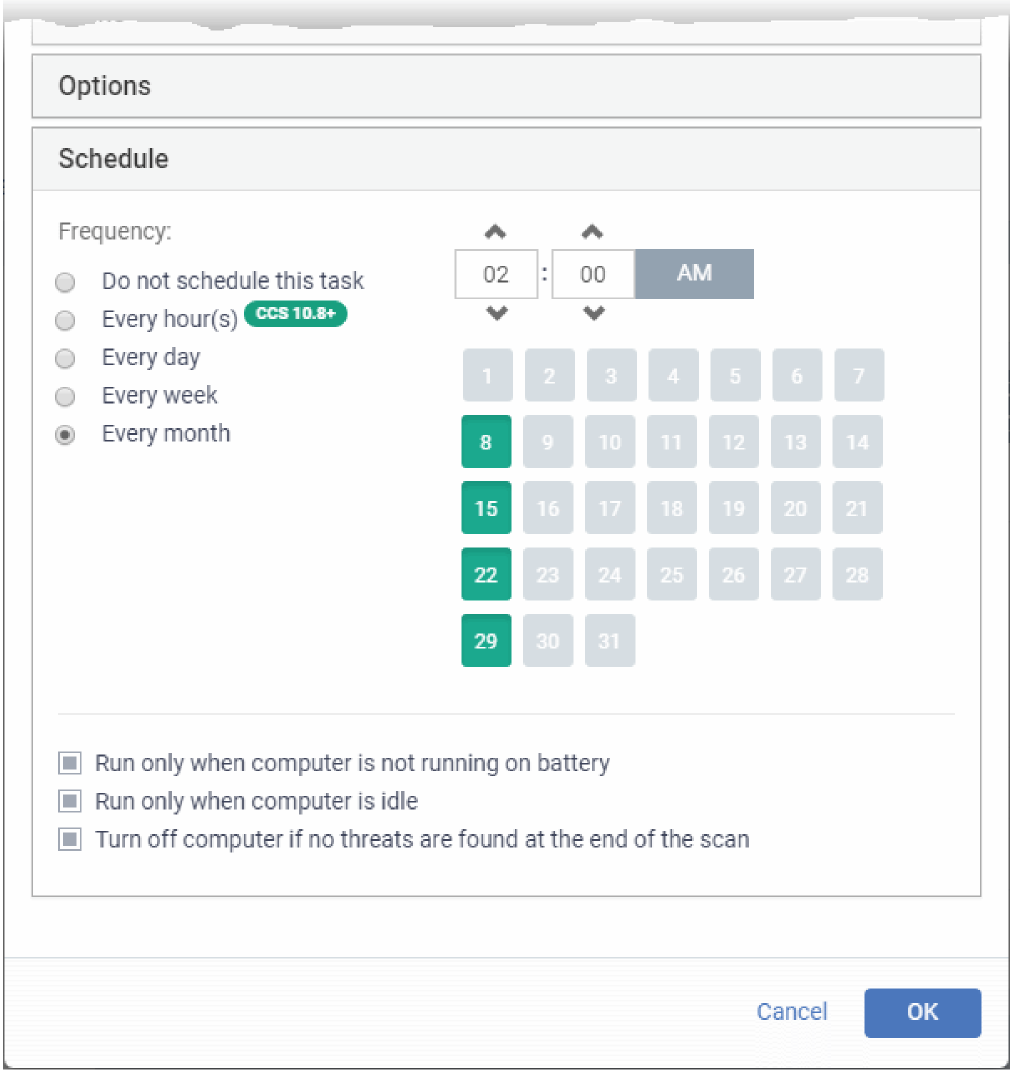
| Scan Options - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable scanning optimizations | The antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (***Default = Enabled***).<br>- Applies only to CCS versions 8.3 or lower. |
| Decompress and scan compressed files | The antivirus will open and scan archive files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***). |
| Use cloud while scanning | Augments the local scan with a real-time look-up of Comodo's online signature database. The cloud database is the most up-to-date version of our virus database, so antivirus scans are more accurate.<br>With 'Cloud Scanning' enabled, CCS is capable of detecting zero-day malware even if the local database is out-dated. (***Default = Enabled***). |
| Automatically clean threats | CCS will automatically take action against detected threats instead of showing the results screen with a list of threats. You can choose the action to be taken from the drop-down. The available options are:<br>- Disinfect<br>- Quarantine<br>(***Default = Enabled with Disinfect option***) |
| Show scan results window | Displays a results window at the end of a virus scan. The results windows shows all threats identified by the scan. (***Default = Disabled***) |
| Use heuristic scanning | Enable or disable heuristics scanning and define the scan level.<br>The scan level determines how likely the scanner is to classify an unknown file as a threat.<br>- Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (Default)<br>- Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.<br>- High- Highest sensitivity to detecting unknown threats / increased possibility of false positives.<br>(***Default = Enabled with 'Low ' option***)<br>**Background Note**: Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing a file to ascertain whether it contains code typical of a virus. It is about detecting attributes which resemble a virus, rather than looking for a signature that matches a signature on the virus blacklist. This allows the engine to predict the existence of new viruses - even if they are not in the current virus database |
| Apply this action to suspicious autorun entries | CCS will inspect auto-run entries, Windows services, startup items and scheduled tasks during each scan.<br>- You can apply one of the following actions to services started by unrecognized or malicious processes:<br>  - **Quarantine and Disable**: The service will be stopped and |

| Scan Options - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| | permanently disabled. The file that started the service will be quarantined on the device.<br>- **Terminate and Disable -** The service will be stopped and permanently disabled. If required, the service can be enabled manually. (***Default***)<br>- **Terminate -** The service will be stopped for the current session.<br>- **Ignore -**The detection will be logged but the service allowed to run normally.<br>- Applies only to CCS versions 10.7 or higher. |

| Scan Options - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Limit maximum file size to | Specify the maximum file size that the antivirus should attempt to scan.(***Default = 40 MB***). |
| Run this scan with | Set the Windows priority for the scan. Choices are high, medium, low and run in the background. (***Default = Enabled with Background option***) |
| Update virus database before running | Makes CCS to check for virus database updates before a scan. Available updates will be downloaded prior to the scan.<br>(***Default = Enabled***). |
| Detect potentially unwanted applications | CCS also scans for applications that<br>(i) a user may or may not be aware is installed on their computer and<br>(ii) may functionality and objectives that are not clear to the user.<br>Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (***Default = Enabled***). |

The next step is to schedule when the custom scan should be run.

- Click 'Schedule'



Options

Schedule

Frequency:

○ Do not schedule this task
○ Every hour(s)
○ Every day
○ Every week
● Every month

02 : 00 AM

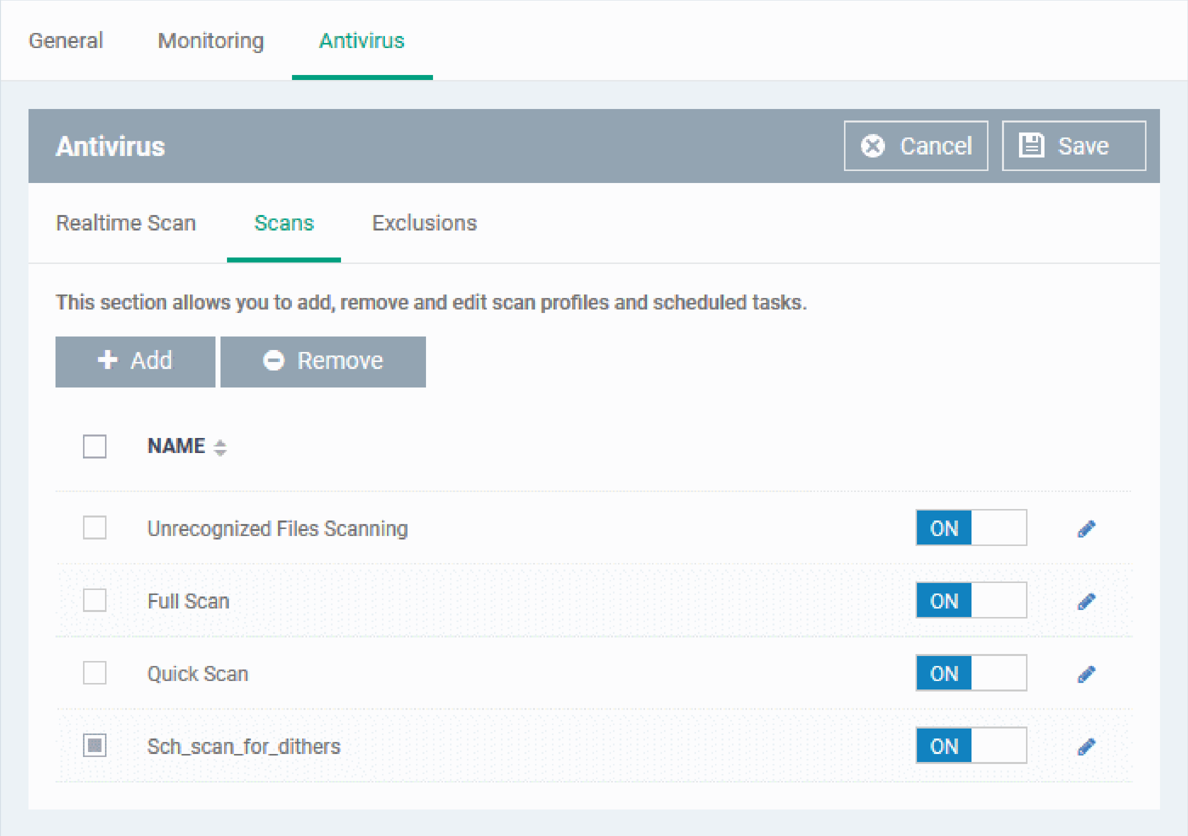
Selected days of the month: 8, 15, 22, 29

□ Run only when computer is not running on battery
□ Run only when computer is idle
□ Turn off computer if no threats are found at the end of the scan

| Schedule Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Frequency | - **Do not schedule this task -** The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning<br>- **Every hour(s)** - Run the scan once every n hours. For example, once every 3 hours.<br>  - Enter the number of hours between scans in the box provided.<br>- **Every Day** - Runs the scan every day at the time specified<br>- **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.<br>- **Every Month** - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them. |
| Run only when computer is not running on battery | Runs the scan only if the computer is connected to the mains supply. This is useful if you are using a laptop or any other battery driven portable computer. |

| Schedule Settings - Table of Parameters | |
|---|---|
| Run only when computer is idle | Scans will run only if the computer is in idle state. Select this if you do not want to be disturbed, or if you are running resource intensive programs and do not want the scan to take processing power. |
| Turn off computer if no threats are found at the end of the scan | Powers down your computer if no threats are found during the scan. For example, this is useful if you have scans which are scheduled to run at night. |

- Click 'OK' to save the custom scan settings



This section allows you to add, remove and edit scan profiles and scheduled tasks.

| | NAME | | |
|---|---|---|---|
| □ | Unrecognized Files Scanning | ON | ✎ |
| □ | Full Scan | ON | ✎ |
| □ | Quick Scan | ON | ✎ |
| ☑ | Sch_scan_for_dithers | ON | ✎ |

The added scan profile will be listed in the screen.

- Use the switches to enable or disable a scan-profile.
- To change the settings for the custom scan, click the edit button ✎ , edit the parameters and click 'OK'
- To remove a custom scan from the list, select it and click 'Remove'

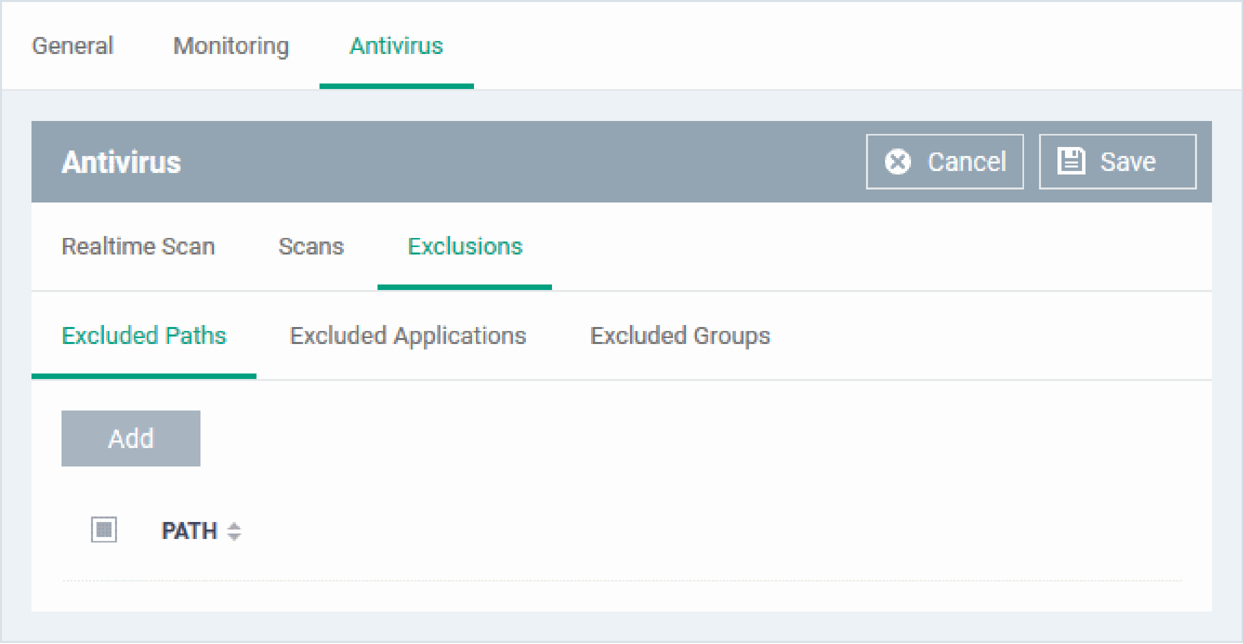
### Exclusions

The 'Exclusions' screen under the Antivirus setting has three sub sections that allow you to add a list of paths, list of applications/files and 'File Groups' which should be excluded from the antivirus scan.

- Click 'Exclusions'

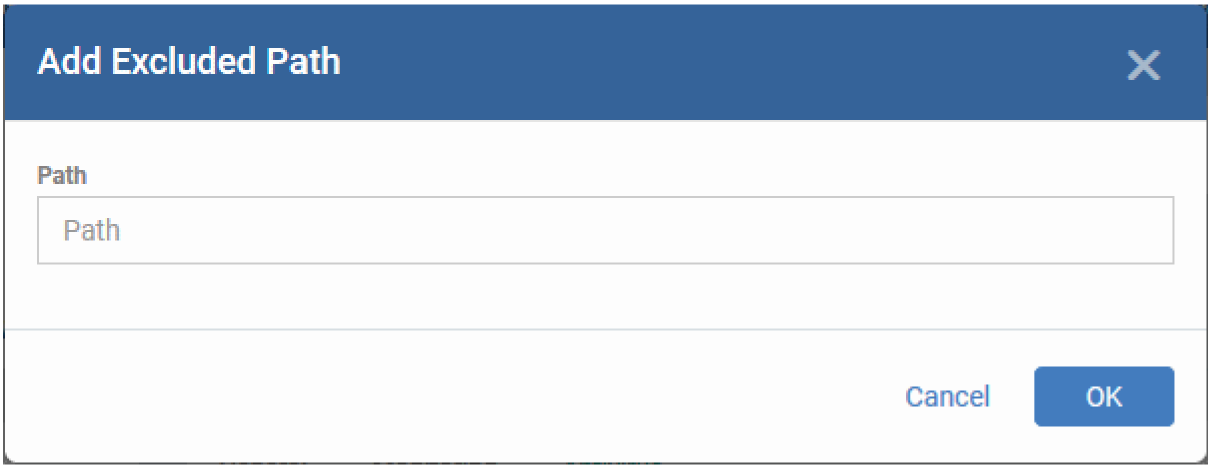
### To add excluded paths

By default the 'Excluded Paths' screen will be displayed:



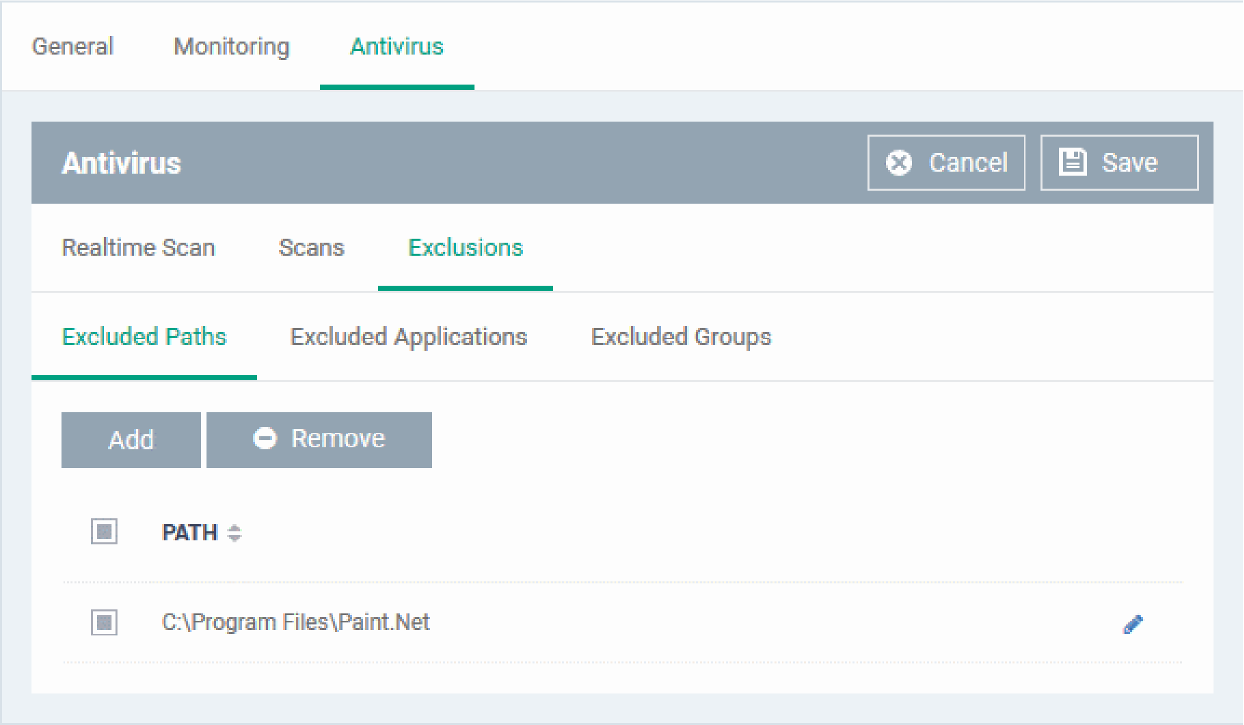
- Click 'Add'

The 'Add Excluded Path' dialog will appear:



- Enter the full path that should be excluded from scanning and click 'OK'.

The added excluded path will be added to the list.

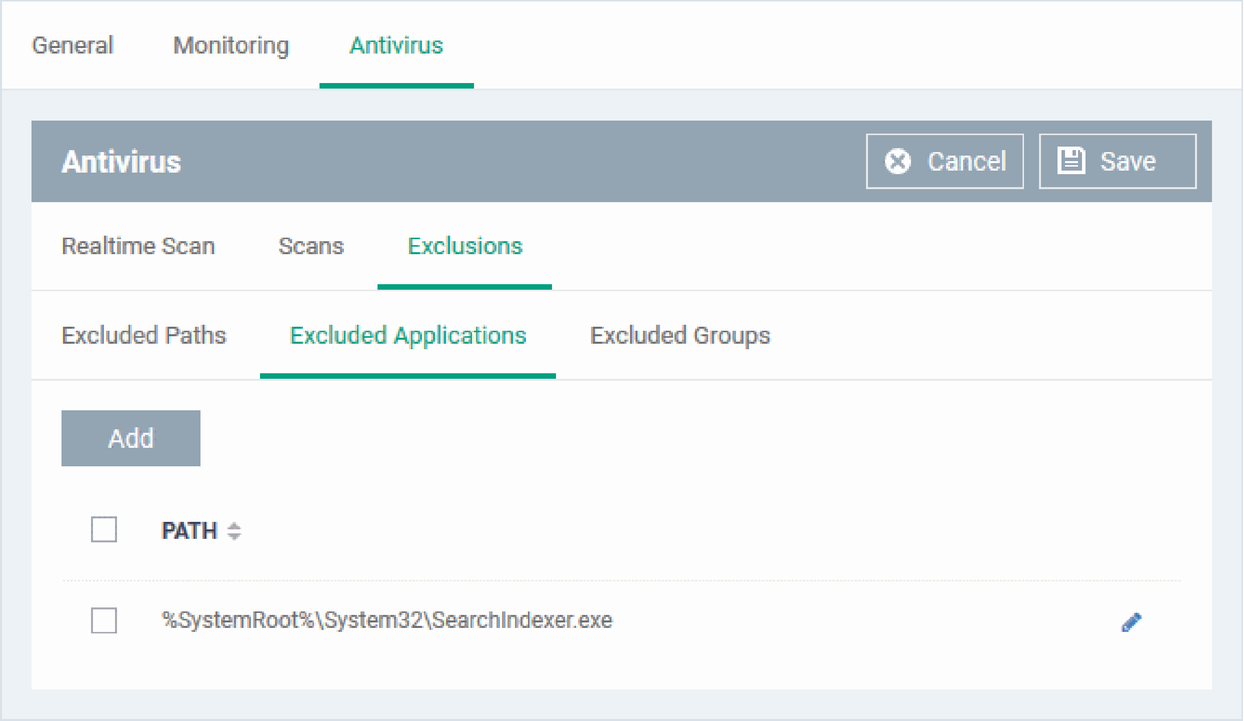


C:\Program Files\Paint.Net

- Repeat the process to include more paths
- To change the path, click the edit button ✎ , edit the parameters and click 'OK'
- To remove a path from the list, select it and click 'Remove'

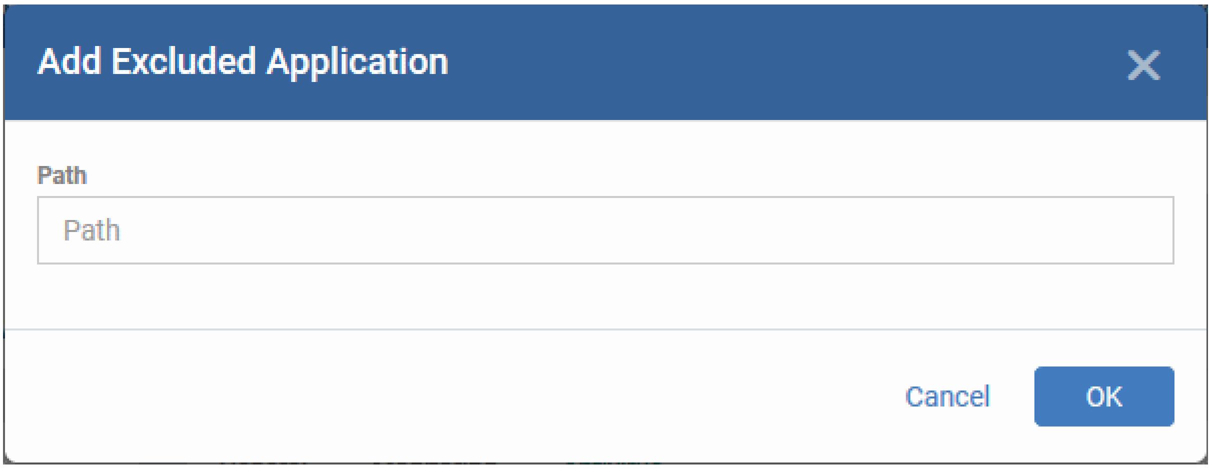
### To add excluded applications

- Click 'Excluded Applications'

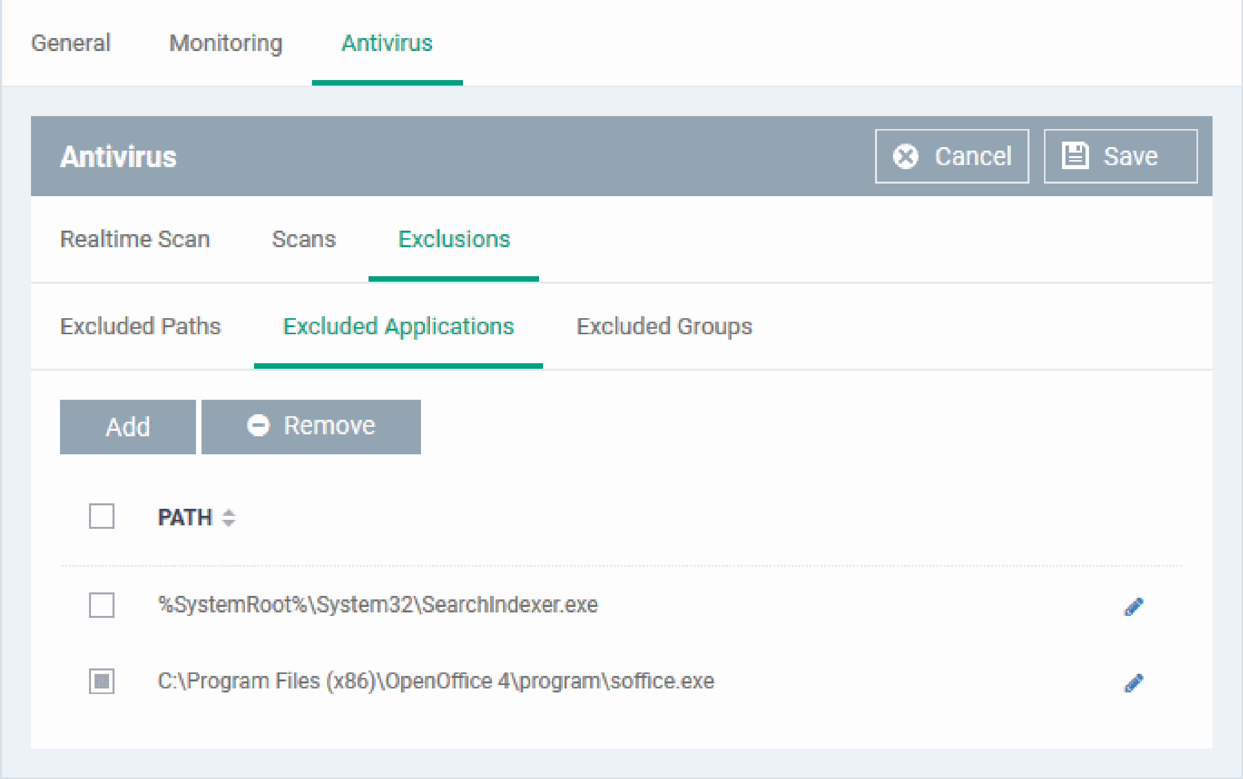


%SystemRoot%\System32\SearchIndexer.exe

- Click 'Add'



- Enter the full path including the application that should be excluded from scanning and click 'OK'
- Repeat the process to include more applications



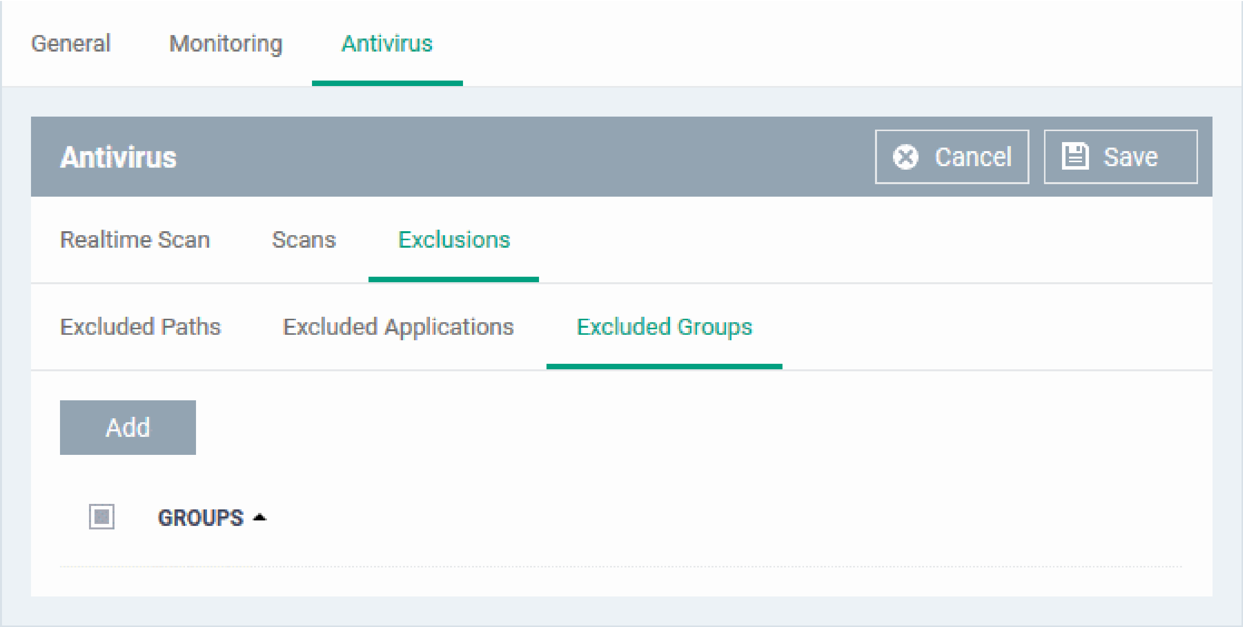
| □ | PATH |
|---|---|
| □ | %SystemRoot%\System32\SearchIndexer.exe |
| ■ | C:\Program Files (x86)\OpenOffice 4\program\soffice.exe |

- To change the application path, click the edit button ✎ , edit the parameters and click 'OK'
- To remove an application from the list, select it and click 'Remove'

**To add Excluded Groups**

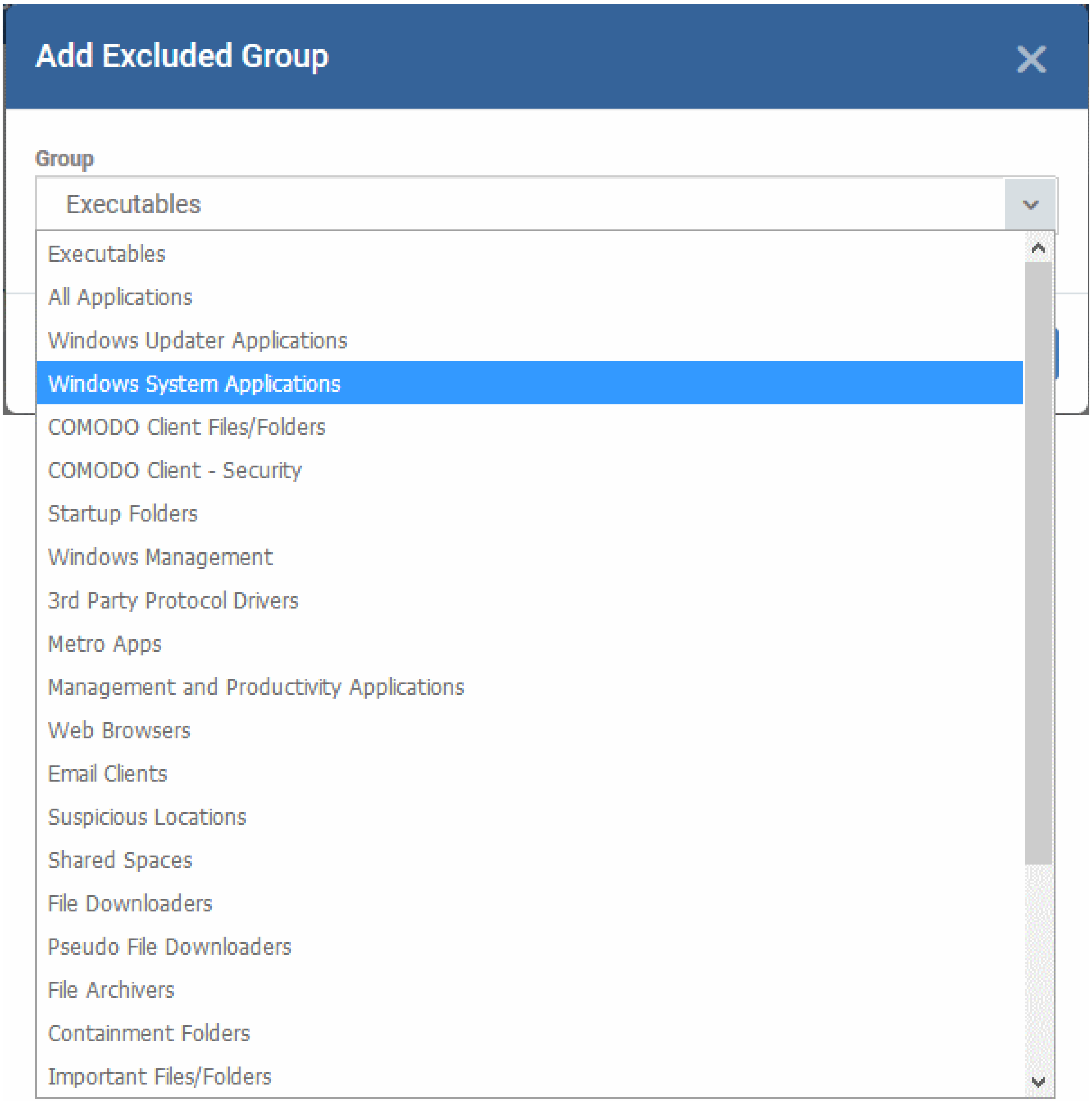
File groups are handy, predefined groupings of one or more file types. File groups make it easy to exclude an entire class of file types. EM ships with a set of predefined 'File Groups'. Users, can add new groups and edit existing groups. See '**File Groups**' under 'Settings' > 'System Templates' > 'File Groups Variables'.

- Click 'Excluded Groups'



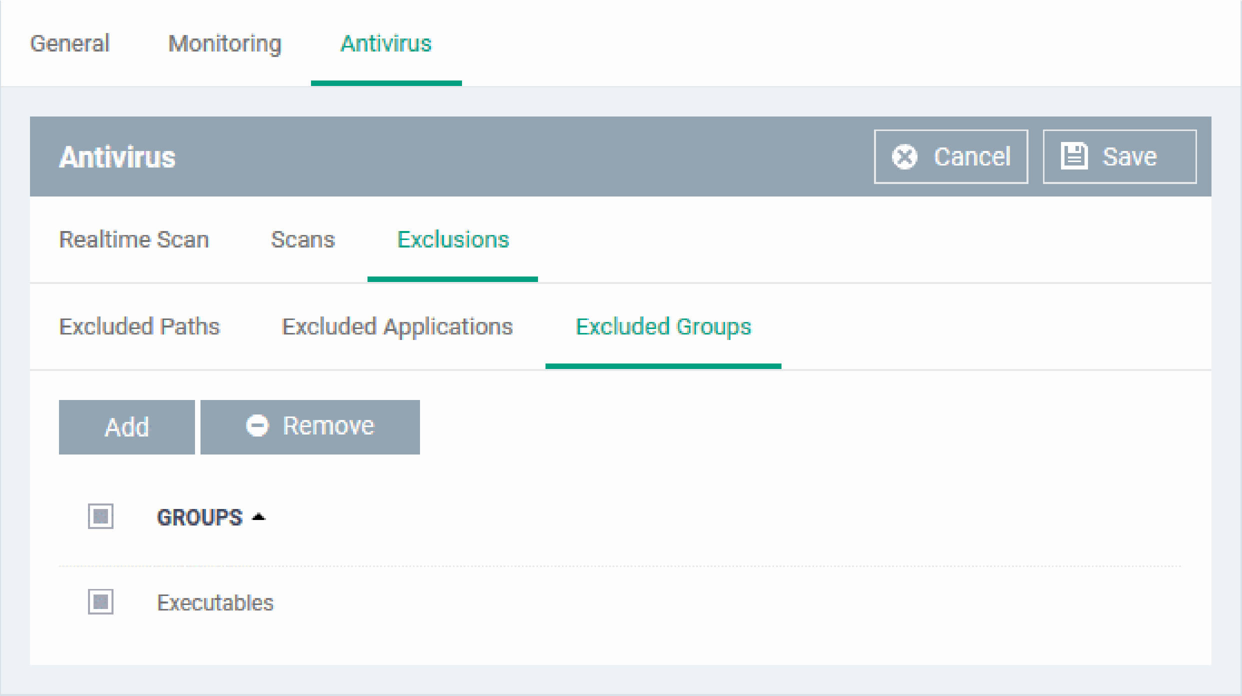
- Click 'Add'.

The 'Add Group' dialog will appear.



- Choose the group from the 'Group' drop-down and click 'OK'.

The group will be added to the exclusions.



- Repeat the process to add more file groups
- Click the 'Save' button at the bottom to save the antivirus settings.
- Click 'Delete' to remove the antivirus settings section. See **Edit Configuration Profiles** for more details about editing the parameters.

### 6.1.3.1.2. Communication Client and Comodo Client - Security Application Update Settings

- The updates section of a Windows profile lets you configure how and when managed devices should check for client updates.
- You can enable automatic updates, specify which version to install, choose update frequency, and enable local updates.

**Tip**: Alternatively, you can manually update clients as follows:

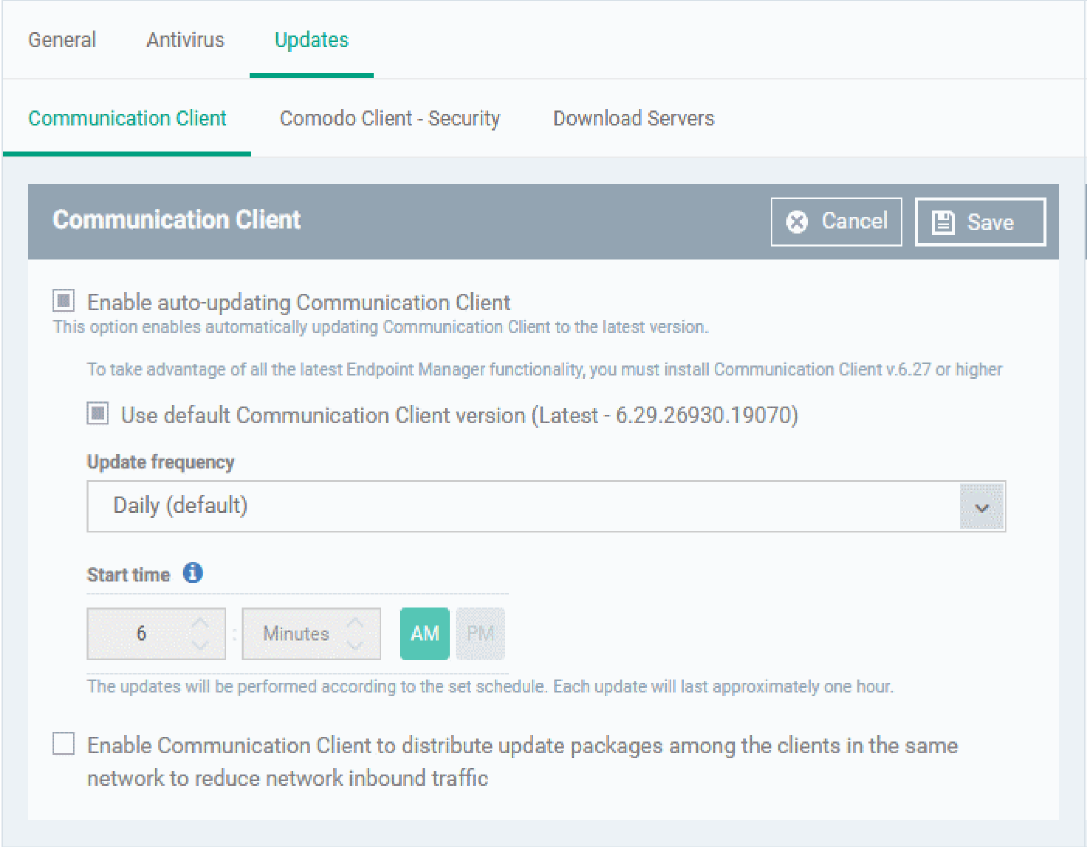
Click 'Devices' > 'Device List' > select target devices > Click 'Install or Update Packages' > 'Update Additional Packages'

See **Remotely Install and Update Packages on Windows Devices** if you want to know more about this method.

#### Configure update settings

- Open a device profile
- Click 'Add Profile Section' > 'Updates'

The section opens at the update configuration screen:



☒ Enable auto-updating Communication Client
This option enables automatically updating Communication Client to the latest version.

To take advantage of all the latest Endpoint Manager functionality, you must install Communication Client v.6.27 or higher

☒ Use default Communication Client version (Latest - 6.29.26930.19070)

Update frequency
Daily (default)

Start time
6 : Minutes AM PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

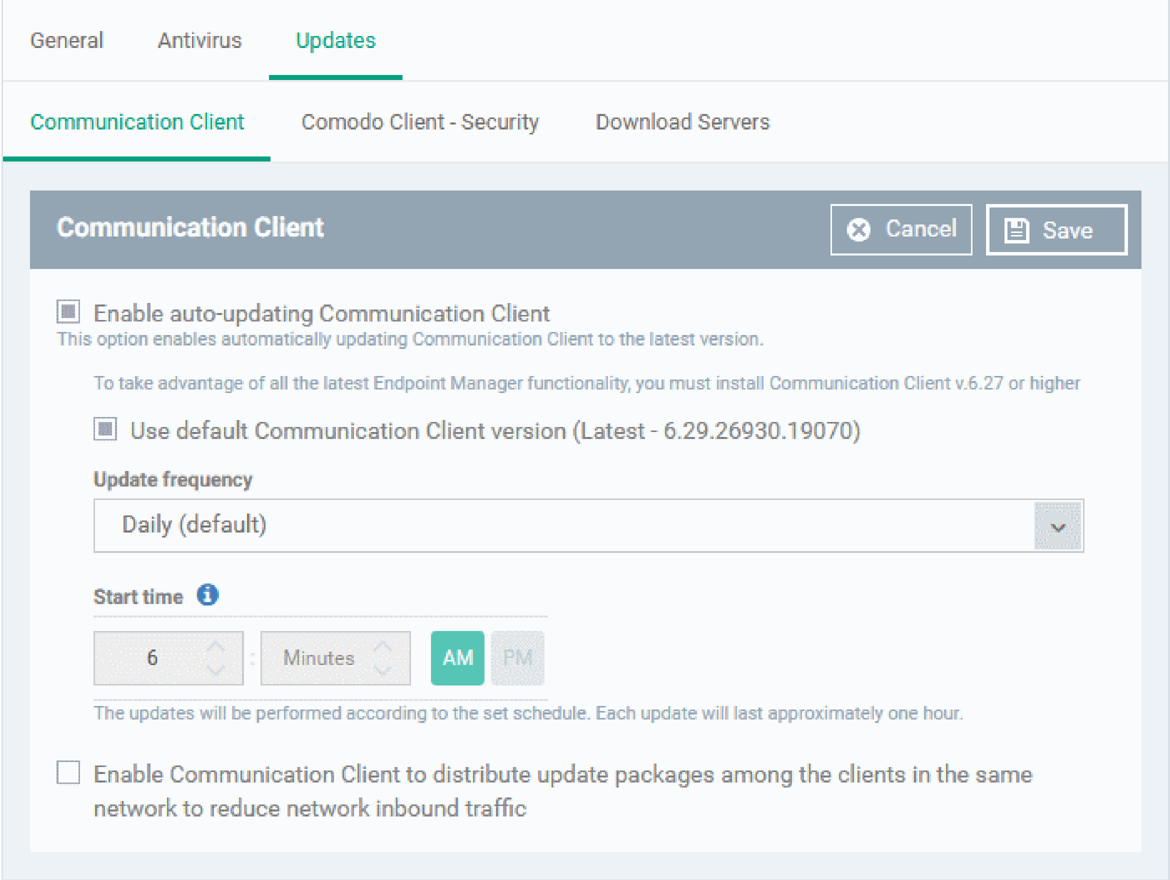
□ Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic

There are three tabs:

- **Communication Client** - Enable automatic program updates for CC and configure proxy server settings.
- **Comodo Client - Security** - Enable automatic program updates for CCS and configure a schedule.
- **Download Servers** - Specify the server from which managed endpoints should collect updates.

### Communication Client

- Open the 'Updates' section of a profile
- Click the 'Communication Client' tab:



☑ Enable auto-updating Communication Client
This option enables automatically updating Communication Client to the latest version.

To take advantage of all the latest Endpoint Manager functionality, you must install Communication Client v.6.27 or higher

☑ Use default Communication Client version (Latest - 6.29.26930.19070)

Update frequency
Daily (default)

Start time
6 : Minutes AM PM

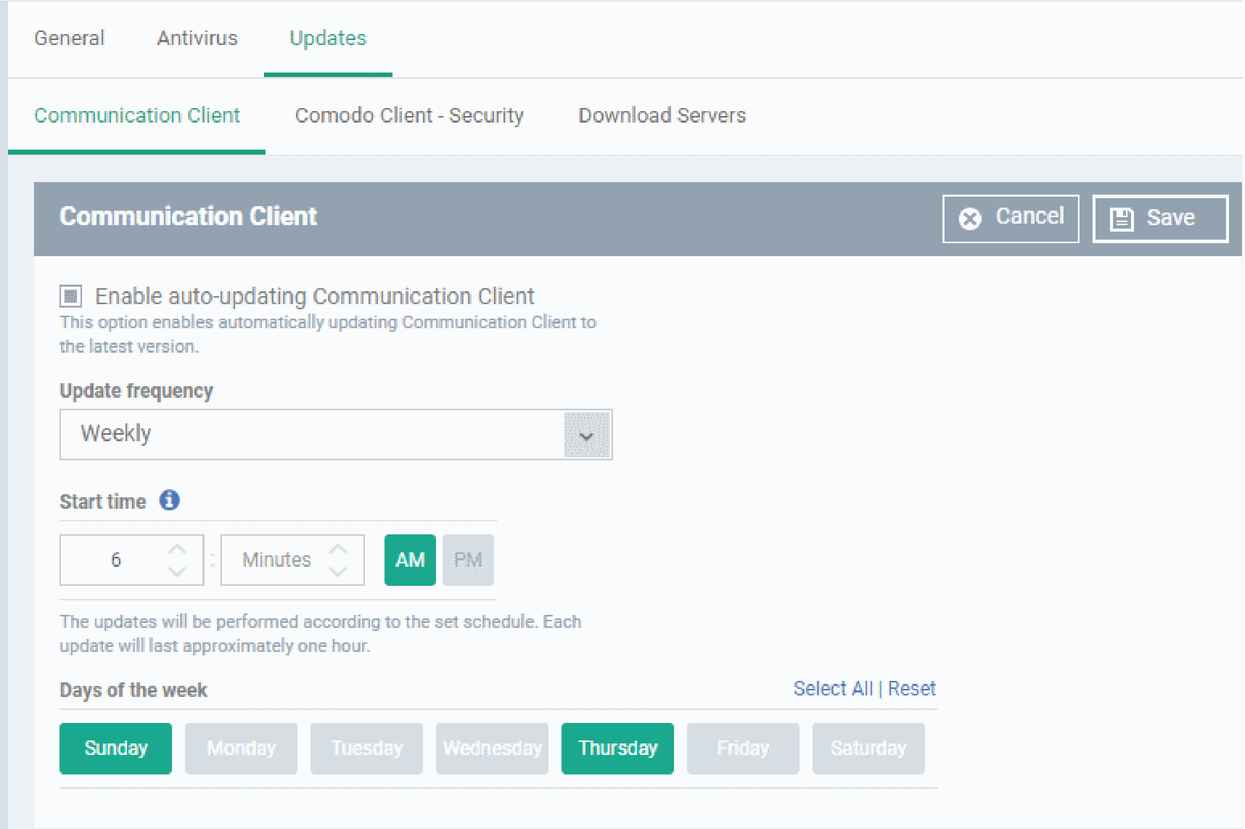
The updates will be performed according to the set schedule. Each update will last approximately one hour.

□ Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic

- **Enable auto-updating Communication Client -** Forces the endpoint to check for and install CC program updates at the selected frequency. You can set the location of the download server in the '**Download Servers**' tab. Deselect if you want to disable auto updates.
- **Use default Communication Client version -** Choose whether or not to always update to the 'default' version.
  - **Enabled** = The client will always update to the default version (***Default***)
  - **Disabled** = You can choose the version to which the client updates. Make sure you choose a higher version than already installed.

    Note 1. You can configure the default version in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'.

    Note 2. You can only change the version if 'Change of version while updating' is enabled in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'. If it is not enabled then the default version is automatically deployed.
- **Update Frequency -** Choose how often CC should check for updates. The available options are:
  - **Daily (Default) -** The client checks for updates everyday at 6:00 am.
  - **Daily (custom) -** The client checks for updates everyday at the time you specify
  - **Weekly -** Select the days and times that you want the client to check for updates
  - **On selected days -** Choose one or more days in a month to check for updates. For example, you might want to update on the first and third Wednesdays of every month.
  - **Monthly -** Select the date and time in a month to check for updates



☐ Enable auto-updating Communication Client
This option enables automatically updating Communication Client to the latest version.

Update frequency: Weekly

Start time: 6 : Minutes AM PM

The updates will be performed according to the set schedule. Each update will last approximately one hour.

Days of the week — Select All | Reset

Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

- **Enable Communication Client to distribute updates to clients in the same network -** Download updates to a managed endpoint, then use that endpoint as the source from which other endpoints collect their updates.

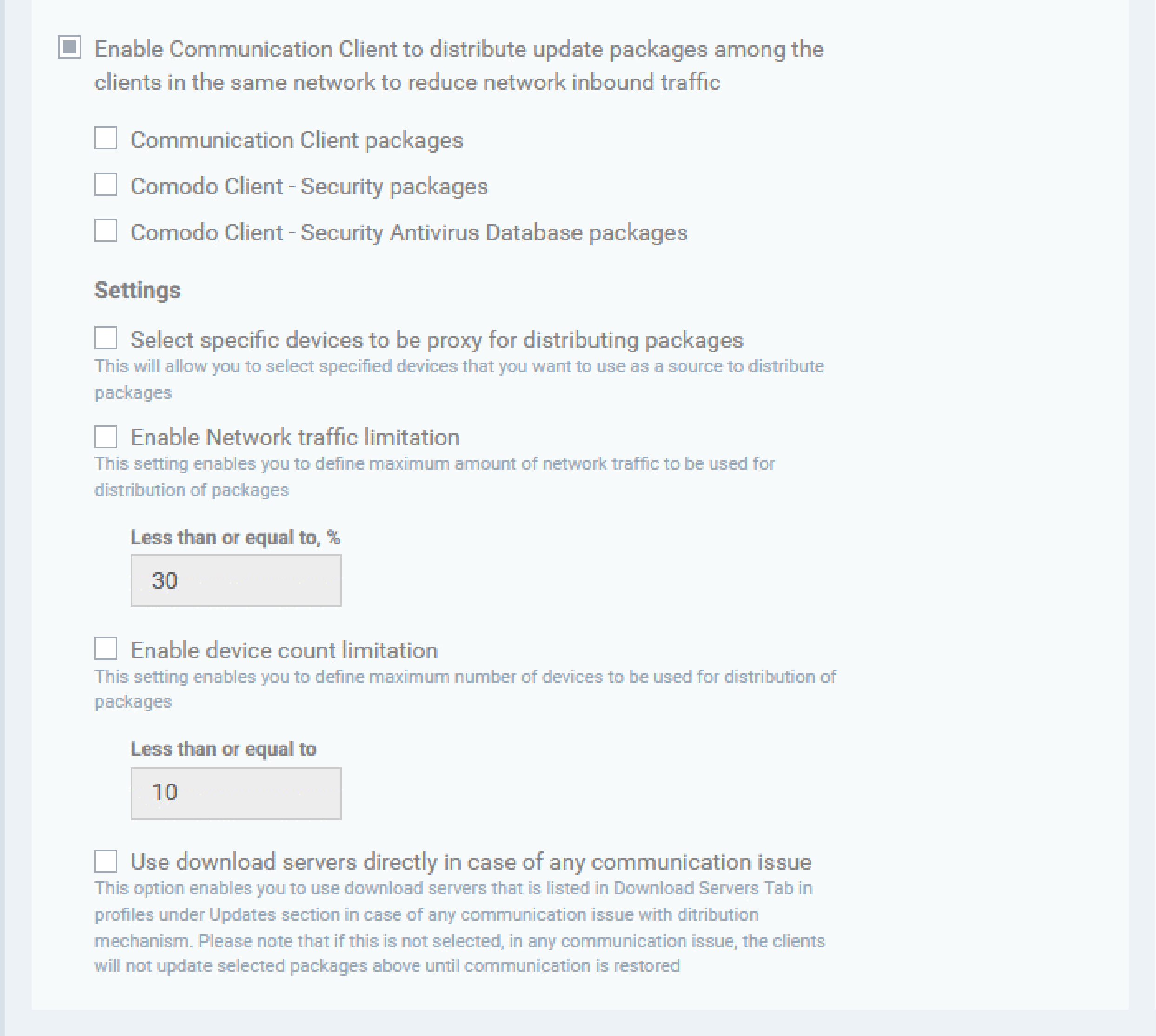
  This saves internet bandwidth usage and accelerates updates in large networks.

  If enabled, your endpoint clients will follow this process at update time:

  - The endpoint first checks other endpoints to see if the update is installed on them
  - If available, the client fetches the update from the local endpoint
  - If not available, the client downloads the update from the server set in the '**Download Servers**' tab
  - This endpoint then becomes the source from which other endpoints collect their updates.

  You can also choose the types of updates that use this mechanism:

  - **Communication Client updates** (Version 6.29 or higher)
  - **Comodo Client Security updates** (Version 11.4 or higher)
  - **Antivirus Database updates** (Version 11.4 or higher)



☑ Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic

□ Communication Client packages

□ Comodo Client - Security packages

□ Comodo Client - Security Antivirus Database packages

Settings

□ Select specific devices to be proxy for distributing packages
This will allow you to select specified devices that you want to use as a source to distribute packages

□ Enable Network traffic limitation
This setting enables you to define maximum amount of network traffic to be used for distribution of packages

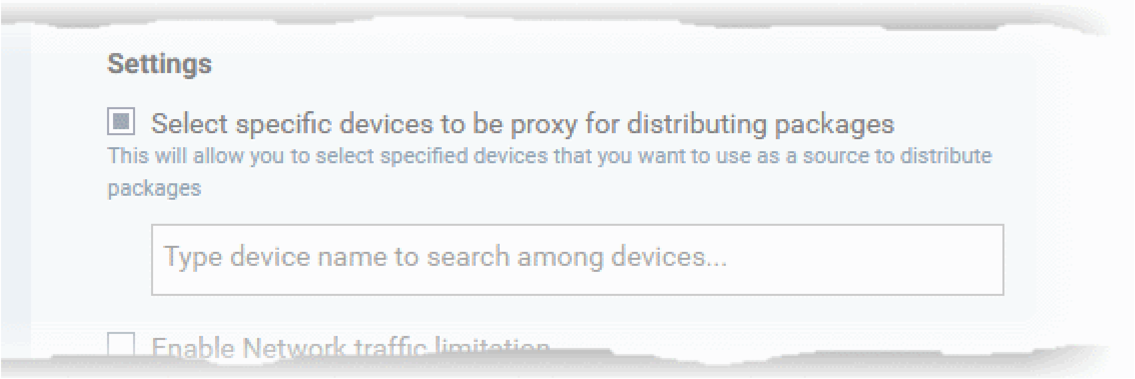
Less than or equal to, %
30

□ Enable device count limitation
This setting enables you to define maximum number of devices to be used for distribution of packages

Less than or equal to
10

□ Use download servers directly in case of any communication issue
This option enables you to use download servers that is listed in Download Servers Tab in profiles under Updates section in case of any communication issue with ditribution mechanism. Please note that if this is not selected, in any communication issue, the clients will not update selected packages above until communication is restored

- **Select specific devices to be proxy for distributing packages -** Choose specific devices from which endpoints should collect updates. If you do not enable this option then any device in the local network can act as a source.
    - Enter the names of the target devices in the field provided.
    - You can add multiple devices as sources. Endpoints will collect from the first source they find which has the update.



Settings

☑ Select specific devices to be proxy for distributing packages
This will allow you to select specified devices that you want to use as a source to distribute packages

Type device name to search among devices...

□ Enable Network traffic limitation

- **Enable Network traffic limitation -** The maximum % of network bandwidth that can be used to share updates. (***Default = 30%***)
- **Enable device count limitation -** The maximum number of devices with which the client is allowed to simultaneously share updates. (***Default = 10, Maximum = 20***).

- **Use download servers directly in case of any communication issue -** If the endpoint cannot contact other endpoints it will instead collect the update from the server in the 'Download Servers' tab.
- Click 'Save'.

The following table shows how clients will collect updates in different scenarios:

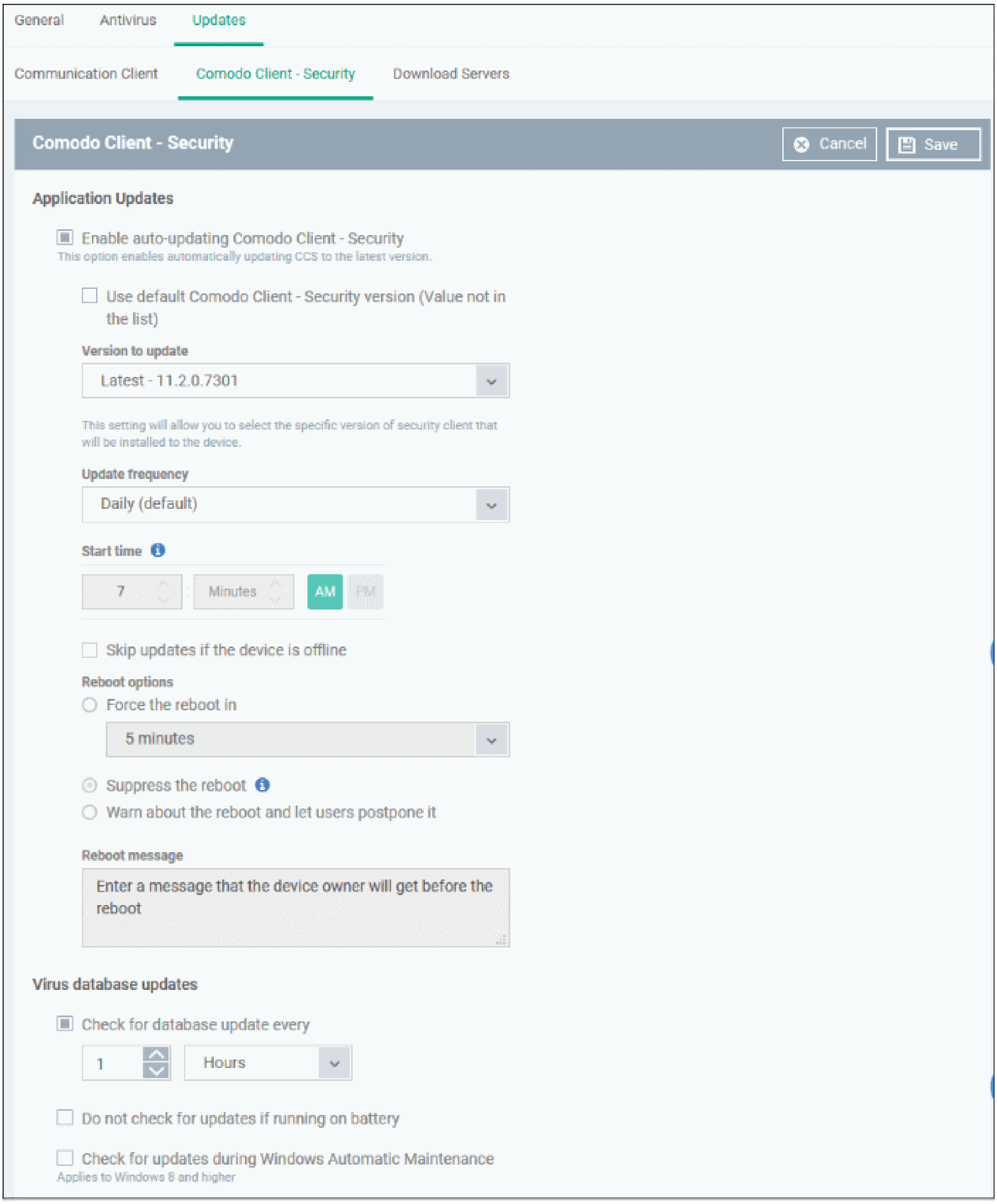
| | Option | | | Client fetches update from: |
|---|---|---|---|---|
| | Enable Communication Client to distribute ... | Select specific devices to be proxy ... | Use download servers directly in case ... | |
| Scenario 1 | ✓ | ✗ | ✗ | Any local device which already has the update |
| Scenario 2 | ✓ | ✓ | ✗ | Only from selected devices |
| Scenario 3 | ✓ | ✗ | ✓ | 1. Any device in the local network<br>2. Download servers |
| Scenario 4 | ✓ | ✓ | ✓ | 1. Selected devices<br>2. Download servers |

**Additional Notes**:

- You can also configure some 'global' settings for client updates at 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows'.
- There is one overlapping item in global settings - 'Enable the communication client to distribute packages to other clients in the network'.
- Endpoint Manager prioritizes this setting as follows:
  - If you *do not* add an update section to the profile, then the global settings apply
  - If you *do* add an update section, then Endpoint Manager will ignore the '...distribute...' settings in global settings
- See **Configure Communication Client Settings** for more details.

### Comodo Client - Security

- Open the 'Updates' section of a profile
- Click the 'Communication Client - Security' tab:



Comodo Client - Security

Application Updates

☒ Enable auto-updating Comodo Client - Security
This option enables automatically updating CCS to the latest version.

□ Use default Comodo Client - Security version (Value not in the list)

Version to update: Latest - 11.2.0.7301

This setting will allow you to select the specific version of security client that will be installed to the device.

Update frequency: Daily (default)

Start time: 7 : Minutes AM PM

□ Skip updates if the device is offline

Reboot options
○ Force the reboot in 5 minutes
● Suppress the reboot
○ Warn about the reboot and let users postpone it

Reboot message: Enter a message that the device owner will get before the reboot

Virus database updates

☒ Check for database update every 1 Hours

□ Do not check for updates if running on battery

□ Check for updates during Windows Automatic Maintenance
Applies to Windows 8 and higher

- **Enable auto-updating Comodo Client - Security** - Forces the endpoint to check for and install CCS program updates at the selected frequency. You can set the location of the download server in the '**Download Servers**' tab. Deselect if you want to disable auto updates.
- **Use default Comodo Client - Security version** - Choose whether or not to always update to the 'default' version.
  - **Enabled** = The client will always update to the default version (***Default***)
  - **Disabled** = You can choose the version to which the client updates. Make sure you choose a higher version than already installed. You cannot install a lower version than the current version.

Note 1. You can configure the default version in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'.

Note 2. You can only change the version if 'Change of version while updating' is enabled in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client - Security'.

If it is not enabled then the default version is automatically deployed.

- **Update Frequency** - Choose how often CCS should check for updates. The available options are:
  - **Daily (Default)** - The client checks for updates everyday at 6:00 am.
  - **Daily (custom)** - The client checks for updates everyday at the time you specify
  - **Weekly** - Select the days and times that you want the client to check for updates
  - **On selected days** - Choose one or more days in a month to check for updates. For example, you might want to update on the first and third Wednesdays of every month.
  - **Monthly** - Select the date and time in a month to check for updates
- **Skip updates if the device is offline** - Updates will not be installed if the endpoint is not connected to EM.
- **Reboot Options** - Configure how the endpoint should restart after the update is installed:
  - **Force the reboot in** - Restart the end-point a certain period of time after installation.
    - Choice of 5, 10, 15 or 30 minutes
    - Enter a message in the 'Reboot message' field to inform users about the reboot.
  - **Suppress the reboot** - Do not restart the machine after the updates. CCS will only become fully functional after the device is restarted.
  - **Warn about the reboot and let users postpone it** - Show an alert to the user which advises them that their computer needs to be restarted.
    - Enter a custom message which is shown to the user.
    - Users can restart the endpoint immediately by clicking 'Reboot now', or postpone it by picking a time in the 'Remind me in' drop-down.
- **Virus database Updates** - Configure when the endpoint should automatically check for virus signature database updates and apply them
  - **Check for database update every** - Specify how often CCS should check for, and automatically install, virus updates.
  - **Do not check for updates if running on battery** - Only check for updates if the computer is connected to the mains supply. Useful for laptops or other battery driven devices.
  - **Check for updates during Windows Automatic Maintenance** - CCS will check for virus updates when Windows enters maintenance mode. The update check will run at maintenance time in addition to the configured schedule. Only applies to Windows 8 and later.
- Click 'Save'.

## Download Servers

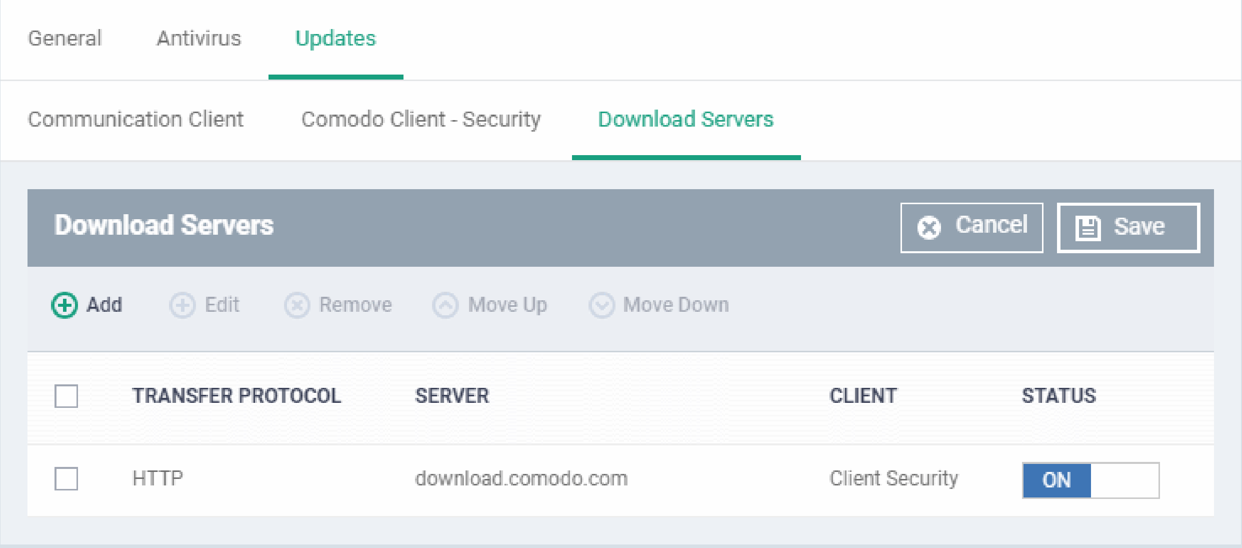
- The 'Download Servers' tab lets you add and select the servers from which endpoints should collect updates.
- You may wish to first download updates to a proxy/staging server and have endpoints collect updates from there. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.
- You can configure different proxy servers for Comodo Client Security and Comodo Client Communication.

**Note**: You need to install the 'ESM Update Mirror' utility on the proxy servers in order to get regular updates from Comodo.

- Download the setup file from **https://drive.google.com/file/d/0B4qKr5xfENWBS0FOUHM2VDFQMnc/view**.
- Run the setup file on a Windows server and follow the wizard to install the application.
- Ensure that the service has started:

- 'Run' > Enter 'services.msc' > locate 'Apache2.2'.
- Click the 'Start' link on the left if the service is not running.

- Click the 'Download Servers' tab

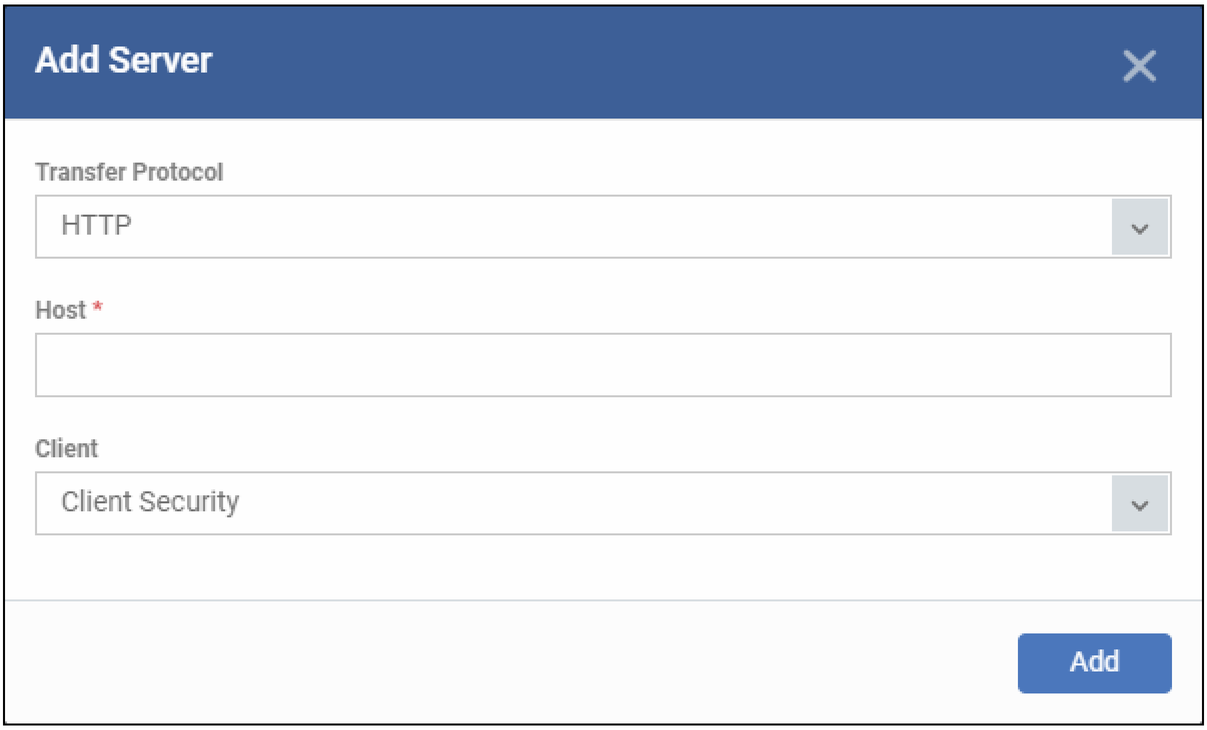


| □ | TRANSFER PROTOCOL | SERVER | CLIENT | STATUS |
|---|---|---|---|---|
| □ | HTTP | download.comodo.com | Client Security | ON |

By default, EM is set to download updates from the Comodo servers. You can add your local servers here, edit, reorder the list of servers and remove servers if required.

- Click 'Add' to add a server

The 'Add Server' dialog will be displayed.



Transfer Protocol: HTTP

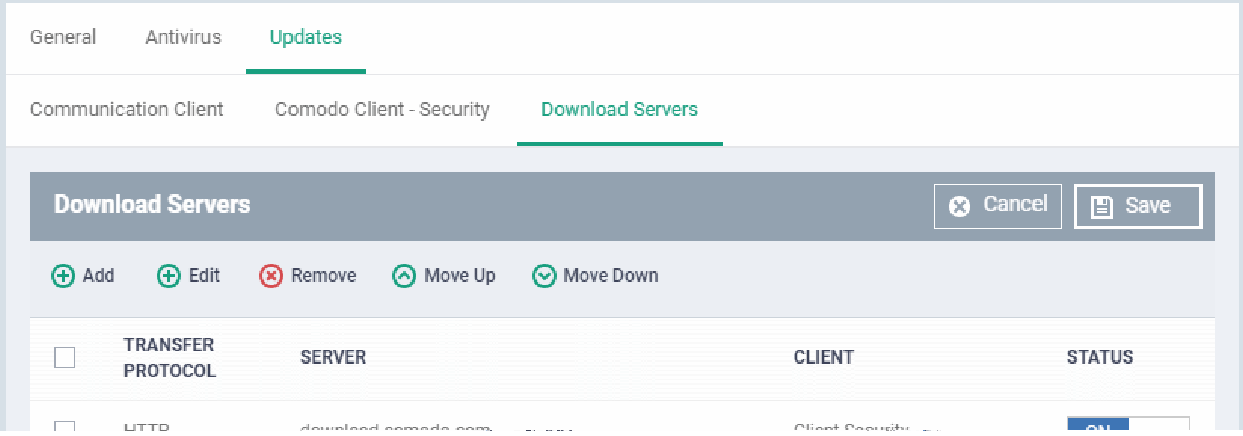
Host *:

Client: Client Security

- **Transfer Protocol -** Select HTTP or HTTPS
- **Host -** Enter the server details in the 'Host' field, either IP or the host name.
- **Client -** Select which items should be collected from the proxy:

        - **Communication Client -** Endpoints will collect communication client (CC) updates from the proxy server.
        - **Client Security -** Endpoints will collect security client (CCS) updates from the proxy server, including virus database updates.
        - **Communication Client + Client Security -** Endpoints will collect CC, CCS, and virus database updates from the proxy.

- Click 'Add'. Repeat the process to add more servers.



- Use the 'on-off' switch to enable or disable a server. You need to enable the server in order for endpoints to use it

You can edit, remove or reorder the list of servers.

    - To edit a server details, select it and click the 'Edit' button at the top.
        - Update the details as required and click the 'Set' button
    - To remove a server, select it and click 'Remove' at the top

The updates are checked from the server at the top and moves down the list. You can reorder the list of servers.

    - To reorder the server list, select the server(s) and click 'Move Up' or 'Move Down'

- Click 'Save' for the changes to updated in the profile.

### 6.1.3.1.3. File Rating Settings

- A file's trust rating determines how Comodo Client Security (CCS) handles the file on the endpoint.
- The ratings are obtained from Comodo's online file database, from the local CCS vendor list, and from the local CCS file list.
- Whenever a file is accessed, CCS does a lookup on the online database, and also consults the two local lists.

The file is classed as trusted if:

- The app is from a vendor who has a 'Trusted' status in the local vendor list in CCS
- The app is trusted in the online file database (aka, it is whitelisted)
- The application/file is trusted in the local CCS 'File List'

**Note**: CCS uses Ports 4446 and 4447 of the endpoint computers for TCP and UDP connections to the cloud. If this option is enabled, we advise you keep these ports free and do not assign them to other applications.

The interface lets you configure the overall behavior of the file rating system on Windows devices to which the profile is applied. You can also choose whether or not local file ratings should be consulted.

**Configure File rating settings**

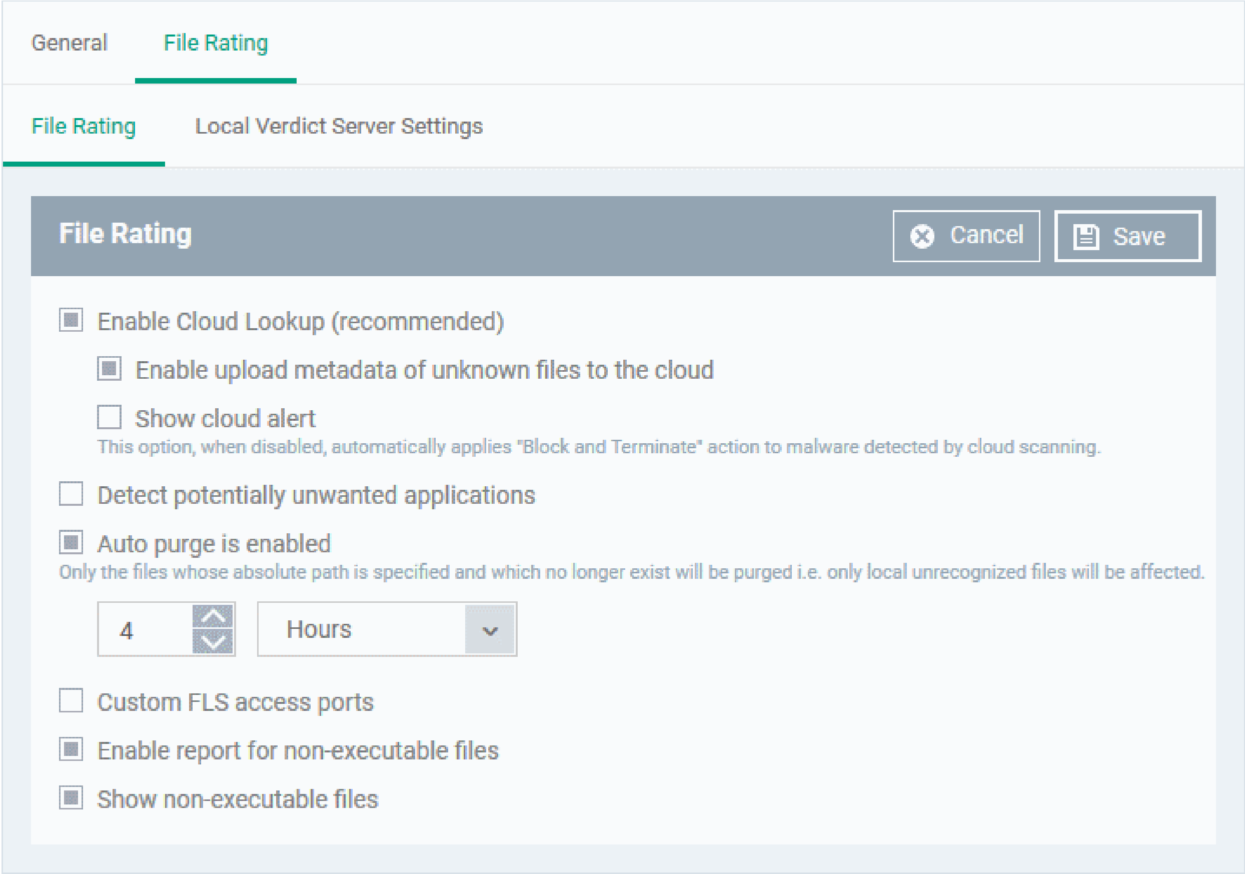
- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Windows profile to open it's details page
  - Click the 'File Rating' tab, if it has already been added to the profile

    OR
  - Click 'Add Profile Section' > 'File Rating'' if it hasn't yet been added

The file rating screen has two tabs:

- **File Rating** - Enable file rating and configure overall behavior.
- **Local Verdict Server Settings** - Choose whether CCS should obey or ignore admin trust ratings which have been assigned to a file. Admins can assign a trust rating to a file in Endpoint Manager at 'Security Sub-Systems' > 'Application Control'. If disabled, file rating scans will only consider the local and Comodo rating.

**File Rating Settings**



☑ Enable Cloud Lookup (recommended)

☑ Enable upload metadata of unknown files to the cloud

☐ Show cloud alert

This option, when disabled, automatically applies "Block and Terminate" action to malware detected by cloud scanning.

☐ Detect potentially unwanted applications

☑ Auto purge is enabled

Only the files whose absolute path is specified and which no longer exist will be purged i.e. only local unrecognized files will be affected.

4 Hours

☐ Custom FLS access ports

☑ Enable report for non-executable files

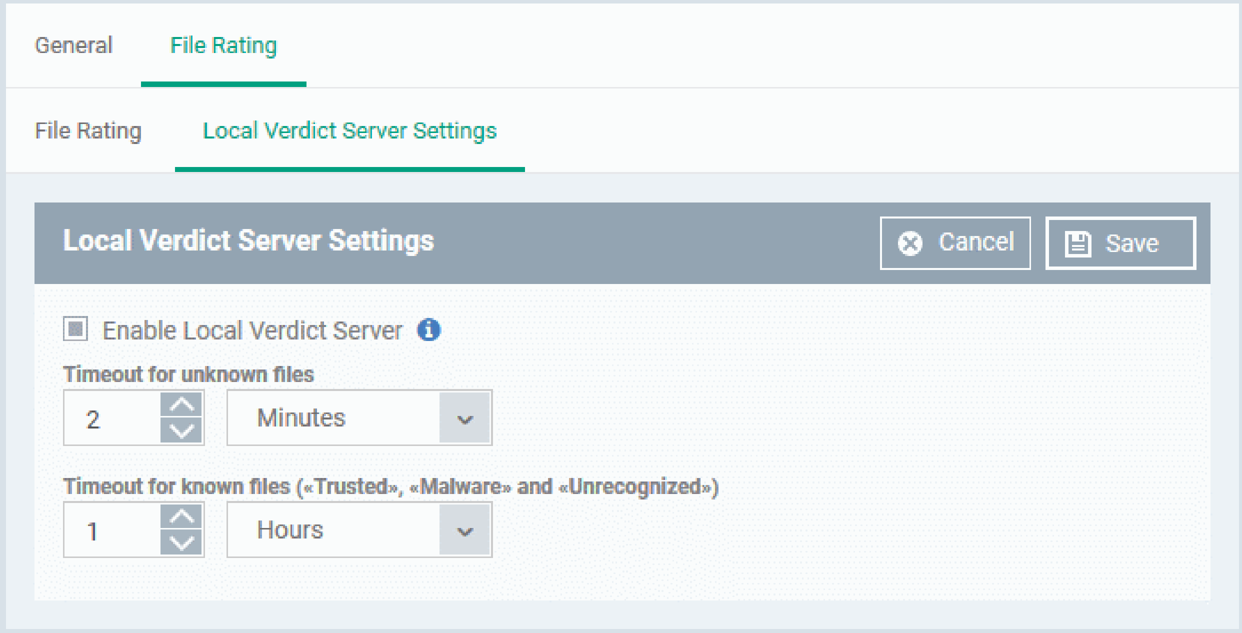
☑ Show non-executable files

| File Rating Configuration - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Cloud Lookup | CCS automatically checks the reputation of files on Comodo's file lookup service (FLS).<br>• Disable this option if you do not want CCS to use the cloud rating.<br>(***Default = Enabled***) |
| Enable upload metadata of unknown files to the cloud | CCS uploads anonymized information about unknown files to Comodo servers. This allows us to analyze and whitelist/blacklist files more effectively.<br>• Disable this option if you do not want CCS to send metadata to Comodo servers.<br>(***Default = Enabled***) |
| Show Cloud Alert | CCS can show an alert on the device when malware is found during a file rating scan. Users can block or allow the malware from the alert.<br>• Disable this option if you don't want users to see an alert. If disabled, CCS will automatically block and delete any discovered malware.<br>(***Default = Disabled***) |
| Detect potentially unwanted applications | A potentially unwanted application (PUA) is an app that:<br>• A user may or may not be aware is installed on their computer.<br>• May have functionality and objectives that are not clear to the user.<br>PUAs include adware and browser toolbars. They are often installed as an extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the software may not have been made clear to the end-user at the time |

| File Rating Configuration - Table of Parameters | |
|---|---|
| | of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet.<br>CCS will show an alert on the endpoint if it detects a PUA and a log entry is created.<br>(***Default = Disabled***) |
| Auto-Purge is enabled | CCS checks the file list and removes invalid and obsolete entries. You can specify the interval at which the check should take place.<br>(***Default = Enabled*** ) |
| Auto Purge Period | The time interval at which auto-purge operations are performed.<br>• Enter the time interval in hours.<br>(***Default = Four hours***) |
| Custom FLS access ports | Define custom ports through which the file lookup service will connect.<br>• Select the protocol(s) and enter the port details for UDP or TCP connections.<br>(***Default = Disabled***) |
| Enable report for non-executable files | If enabled, CCS sends a report on files identified as non-executable to EM on each file rating scan.<br>(***Default = Enabled*** ) |
| Show non-executable files | If enabled, non-executable files will also be added to the 'File List' interface of CCS on the endpoint.<br>To access the file list in CCS, click 'Tasks' > 'Advanced Tasks' > 'Advanced settings' > 'Security settings' > 'File Rating' > 'File list'.<br>(***Default = Enabled*** ) |

- Click 'Save' to apply your file rating settings.

## Local Verdict Server Settings



□ Enable Local Verdict Server

Timeout for unknown files

2 Minutes

Timeout for known files («Trusted», «Malware» and «Unrecognized»)

1 Hours

| Local Verdict Server Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Local Verdict Server | Choose whether CCS should consider the admin trust rating assigned to a file. ***(Default = Enabled)***<br>• Admins can change the trust rating of a file in Endpoint Manager at 'Security Sub-Systems' > 'Application Control'. |
| Timeout for Unknown Files | How often CCS should check Endpoint Manager for new ratings on files that are currently have no rating at all.<br>***(Default = 2 Minutes)*** |
| Timeout for known files (Trusted, malware and Unrecognized) | How often CCS should check Endpoint Manager for new ratings on files that are currently rated as 'Trusted', 'Malware' or 'Unrecognized'.<br>(***Default = 1 Hour***) |

- Click 'Save' to apply your changes.

### 6.1.3.1.4. Firewall Settings

The Firewall Settings area lets you configure the behavior of the CCS firewall on endpoints to which the profile is applied. You can also configure network zones, portsets and traffic filtering rules.

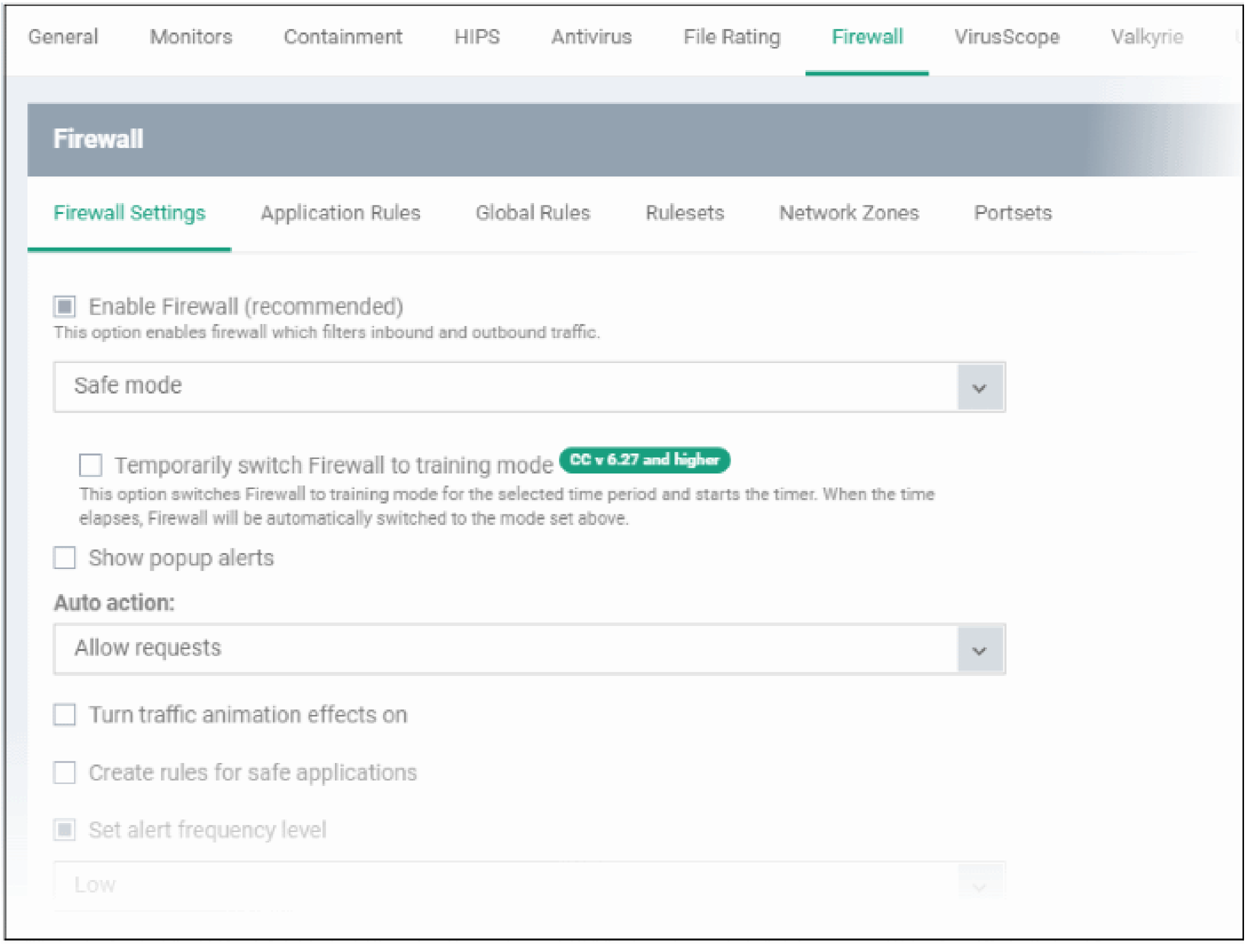
**Configure Firewall Settings and Traffic Filtering Rules**

- Click 'Firewall' from the 'Add Profile Section' drop-down

The Firewall settings screen is displayed. It has six tabs:

- **Firewall Settings** - Configure the general firewall behavior
- **Application Rules** - Define rules that determine the network access privileges of individual applications or specific types of applications at the endpoint
- **Global Rules** - Define rules that apply to all traffic flowing in and out of the endpoint
- **Rulesets** - Create and manage 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** - Create named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Define groups of regularly used ports that can used and reused when creating traffic filtering rules.

**Firewall Settings**



Firewall

☒ Enable Firewall (recommended)
This option enables firewall which filters inbound and outbound traffic.

Safe mode

□ Temporarily switch Firewall to training mode CC v 6.27 and higher
This option switches Firewall to training mode for the selected time period and starts the timer. When the time elapses, Firewall will be automatically switched to the mode set above.

□ Show popup alerts

Auto action:

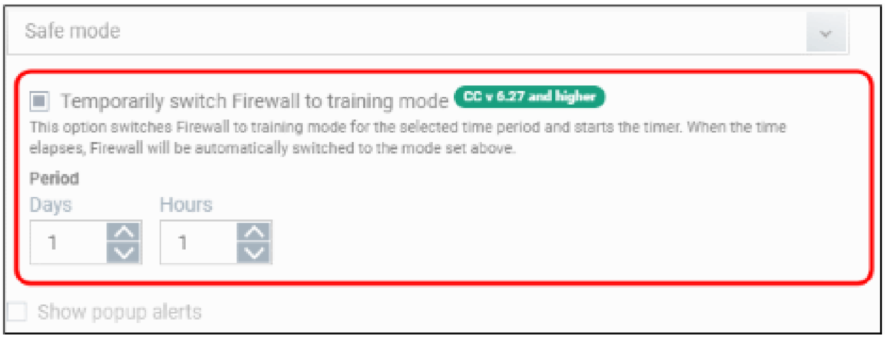
Allow requests

□ Turn traffic animation effects on

□ Create rules for safe applications

☒ Set alert frequency level

Low

| Firewall Configuration - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Traffic Filtering | Enable or disable Firewall protection at the endpoint. If enabled the following options are available:<br>• **Custom Ruleset** - The firewall applies ONLY the custom security configurations and network traffic policies specified by the administrator. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. The user will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, the administrator has specified rules and policies that instruct the firewall to trust the application's connection attempt).<br>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.<br>• **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.<br>'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.<br>• **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.<br>  • Note - If required you can enable training mode to work temporarily. To do that, select 'Temporarily switch Firewall to training mode' option and set the days / hours.<br><br>Safe mode<br>☑ Temporarily switch Firewall to training mode CC v 6.27 and higher<br>This option switches Firewall to training mode for the selected time period and starts the timer. When the time elapses, Firewall will be automatically switched to the mode set above.<br>Period<br>Days 1<br>Hours 1<br>□ Show popup alerts |

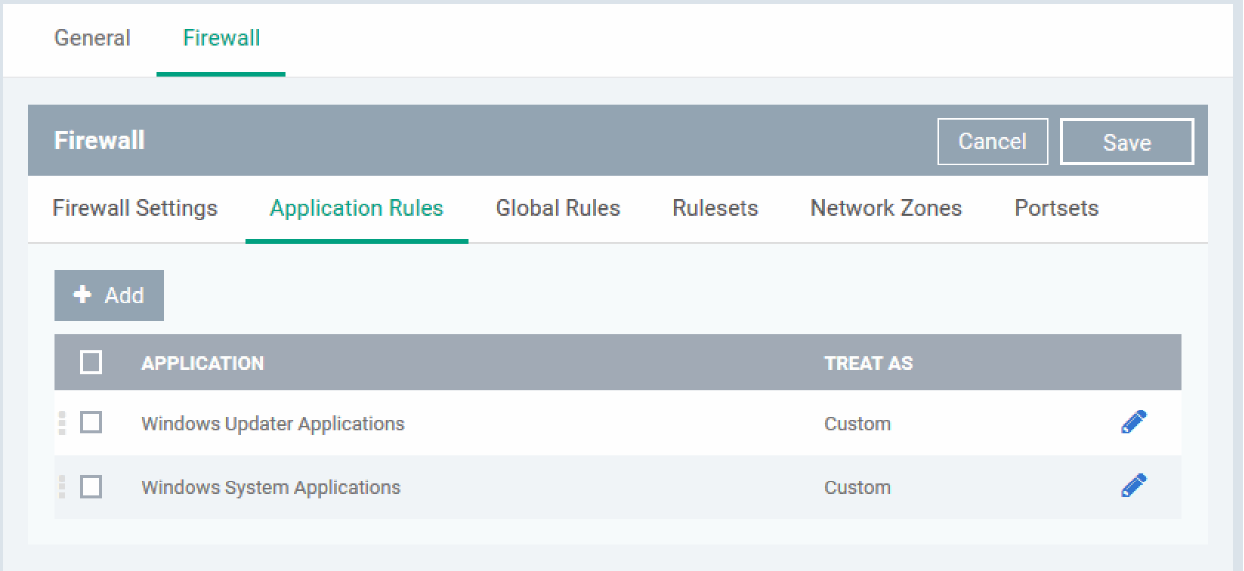
| Firewall Configuration - Table of Parameters | |
|---|---|
| | After the countdown is over, CCS will switch back to previous mode.<br>For more details on the Firewall Settings, see the of CCS - Firewall Settings online help page at **http://help.comodo.com/topic-399-1-790-10358-Firewall-Settings.html** . |
| Show popup alerts | Whether or not firewall alerts are to be displayed at the endpoint whenever the firewall encounters a request for network access, for the user to respond.<br>If you choose not to show the alerts, you can select the default responses from the 'Auto Action' drop-down. The available options are:<br>• Block Requests<br>• Allow Requests |
| Turn traffic animation effects on | The CCS tray icon can display a small animation whenever traffic moves to or from your computer.<br> <br>You can enable or disable the animation to be displayed at the endpoint. |
| Create rules for safe applications | Comodo Firewall trusts the application if:<br>• The app is from a vendor who has a 'Trusted' status in the local vendor list in CCS<br>• The app is trusted in the online file database (aka, it is whitelisted)<br>• The app is trusted in the local CCS 'File List'<br>• See **File Rating Settings** for more details.<br>By default, CCS does not automatically create 'allow' rules for safe applications. This saves resource usage and simplifies the rules interface by reducing the number of rules created.<br>Enabling this option instructs CCS to learn the behavior of safe applications so it can auto-create 'Allow' rules for them. These rules are listed in 'Settings' > 'Firewall Settings' > 'Application Rules'. Advanced users can edit/modify the rules as they wish. (***Default = Disabled***). |
| Set alert frequency level | Enabling this option allows you to configure the amount of alerts that Comodo Firewall generates, from the drop-down at the endpoint. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. (***Default=Disabled***)<br>The options available are:<br>• **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. |

| Firewall Configuration - Table of Parameters | |
|---|---|
| | - **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.<br>- **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.<br>- **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.<br>- **Very Low**: The firewall shows only one alert for an application.<br>The Alert Frequency settings refer only to connection attempts by applications or from IP addresses that you have not (yet) decided to trust. |
| Set new on-screen alert timeout to: | How long the Firewall shows an alert for, without any user intervention at the endpoint. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference by selecting this option and choosing the period from the drop-down combo-box. |
| Filter IPv6 traffic | If enabled, the firewall component of CCS at the endpoint will filter IPv6 network traffic in addition to IPv4 traffic.<br>**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.<br>IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets. |
| Filter loopback traffic | Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the Internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to, under its domain name of 'http://localhost', i.e. the address of your computer.<br>Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this option enabled means the firewall will filter traffic sent through this channel at the endpoints. (***Default = Enabled***). |
| Block fragmented IP traffic | When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. |

| Firewall Configuration - Table of Parameters | |
|---|---|
| | 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.<br>If you want the firewall component of CCS at the endpoint to block the fragmented datagrams, enable this option. (***Default = Enabled***0. |
| Do Protocol Analysis | Protocol Analysis is key to the detection of fake packets used in denial of service (DOS) attacks.<br>If you want firewall at the endpoint to check whether every packet conforms to that protocols standards, select this option. If not, then the packets are blocked (***Default = Enabled***). |
| Enable anti-ARP spoofing | A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update the machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in another machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update its ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in a small network. Enabling this setting helps to block such requests at the endpoints to which the profile is applied - protecting the ARP cache from potentially malicious updates (***Default = Enabled***). |

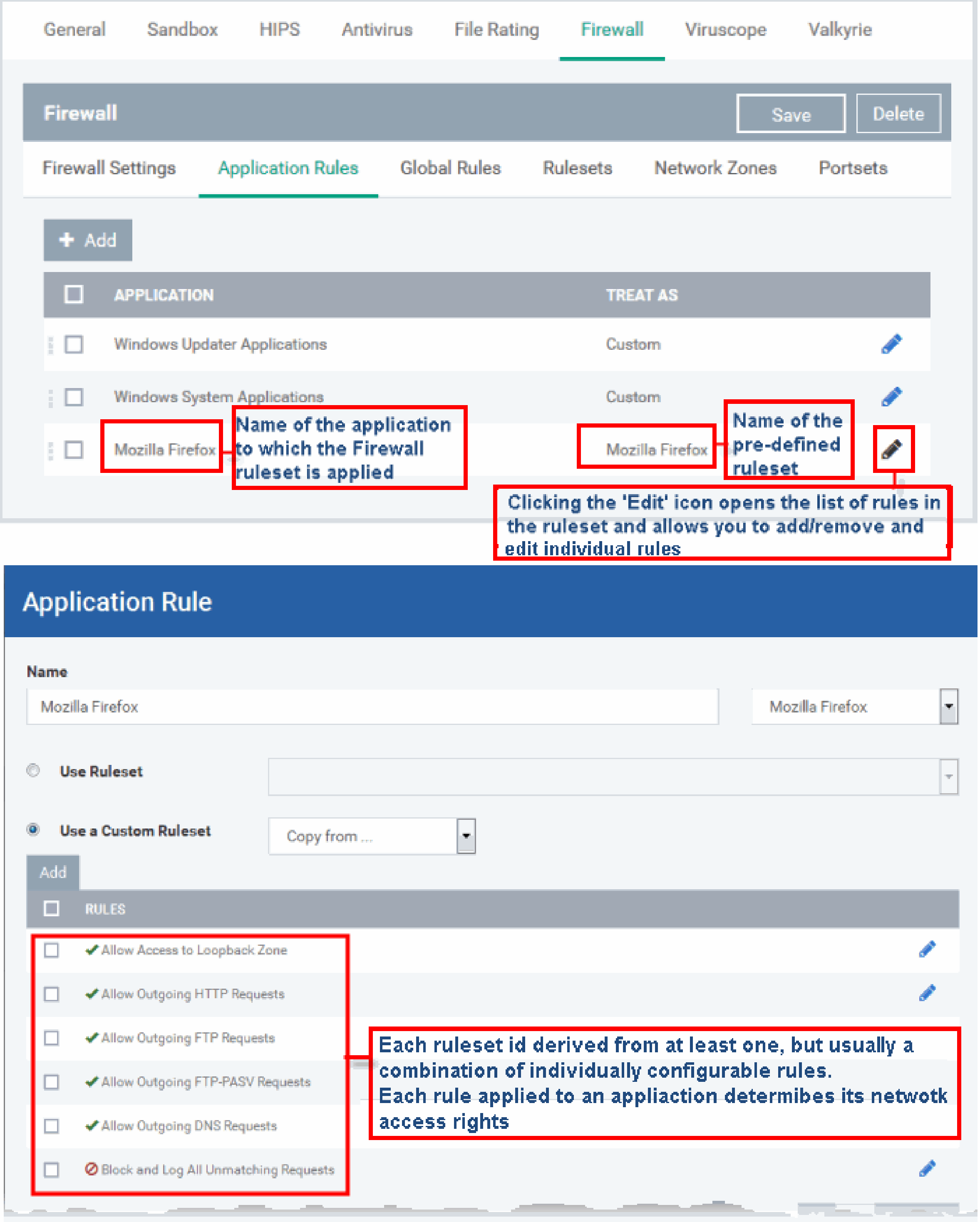
## Application Rules

Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network access rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.



| □ | APPLICATION | TREAT AS |
|---|---|---|
| □ | Windows Updater Applications | Custom |
| □ | Windows System Applications | Custom |

The 'Application Rules' interface allows you to create and manage application rules for regulating network access to individual applications at the endpoints to which the profile is applied.



| □ | APPLICATION | TREAT AS |
|---|---|---|
| □ | Windows Updater Applications | Custom |
| □ | Windows System Applications | Custom |
| □ | Mozilla Firefox | Mozilla Firefox |

Name of the application to which the Firewall ruleset is applied

Name of the pre-defined ruleset

Clicking the 'Edit' icon opens the list of rules in the ruleset and allows you to add/remove and edit individual rules

Name: Mozilla Firefox | Mozilla Firefox

○ Use Ruleset

● Use a Custom Ruleset | Copy from ...

| □ | RULES |
|---|---|
| □ | ✓ Allow Access to Loopback Zone |
| □ | ✓ Allow Outgoing HTTP Requests |
| □ | ✓ Allow Outgoing FTP Requests |
| □ | ✓ Allow Outgoing FTP-PASV Requests |
| □ | ✓ Allow Outgoing DNS Requests |
| □ | ⊘ Block and Log All Unmatching Requests |

Each ruleset id derived from at least one, but usually a combination of individually configurable rules.
Each rule applied to an appliaction determibes its netwotk access rights

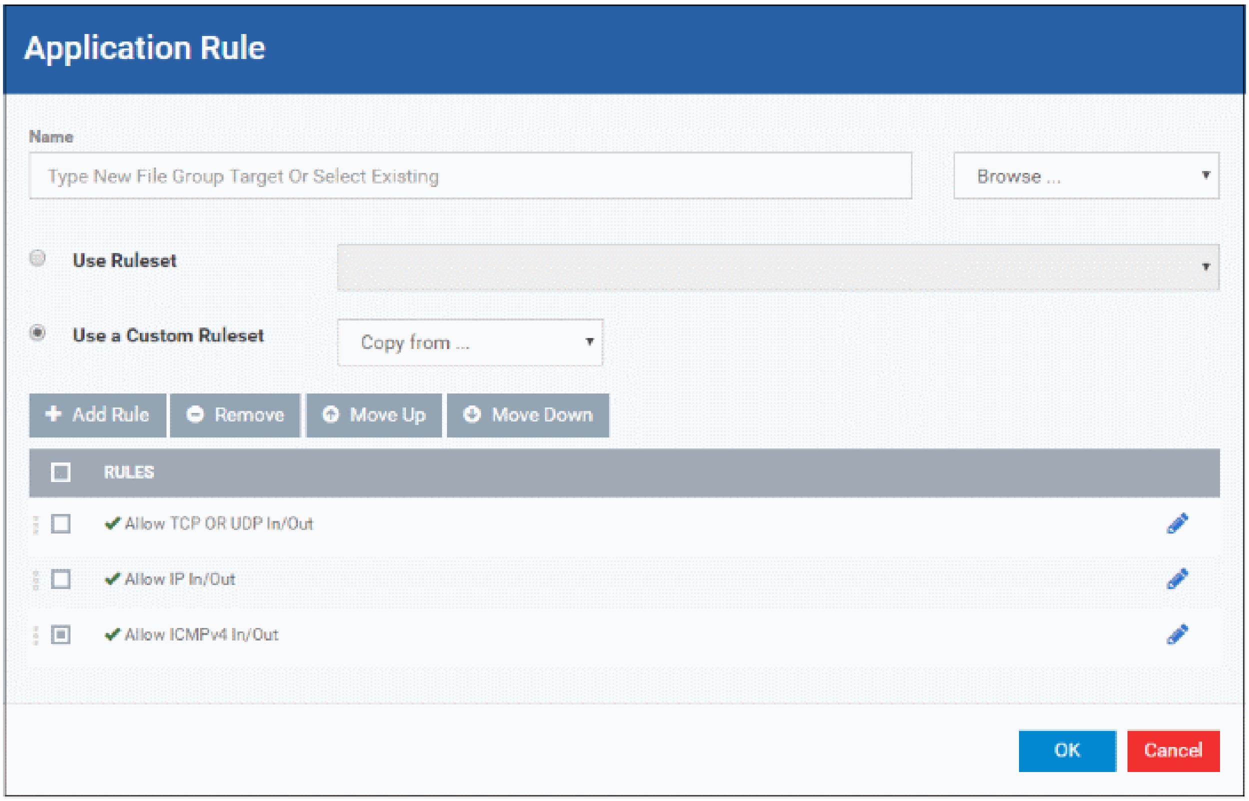
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Administrators can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets.**

- See **Application Rule interface** for an introduction to the rule setting interface
- See **Create and Modify 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 **Add and Edit a Firewall Rule** for an explanation of individual rule configuration.

**Application Rule interface**

- Click the 'Add' button **+ Add** or 'Edit' icon ✎ beside a ruleset in 'Application Rules' interface to open the 'Application Rule' interface.
- The rules in a Firewall ruleset can be added/modified/removed and re-ordered through the 'Application Rule' interface.
- You can also create new rules or edit existing rules in the ruleset in the 'Firewall Rule' interface (Click the 'Add' button or 'Edit' icon ✎ beside a rule in 'Application Rules' interface). See **Add and Edit a Firewall Rule** for guidance on this.



Comodo Firewall applies rules on a per packet basis and applies the first rule that matches that packet type to be filtered (see **Understanding Firewall Rules** for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied. Administrators can re-prioritize rules by uisng the 'Move Up' or 'Move Down' buttons.

**Create and Modify Firewall Rulesets**

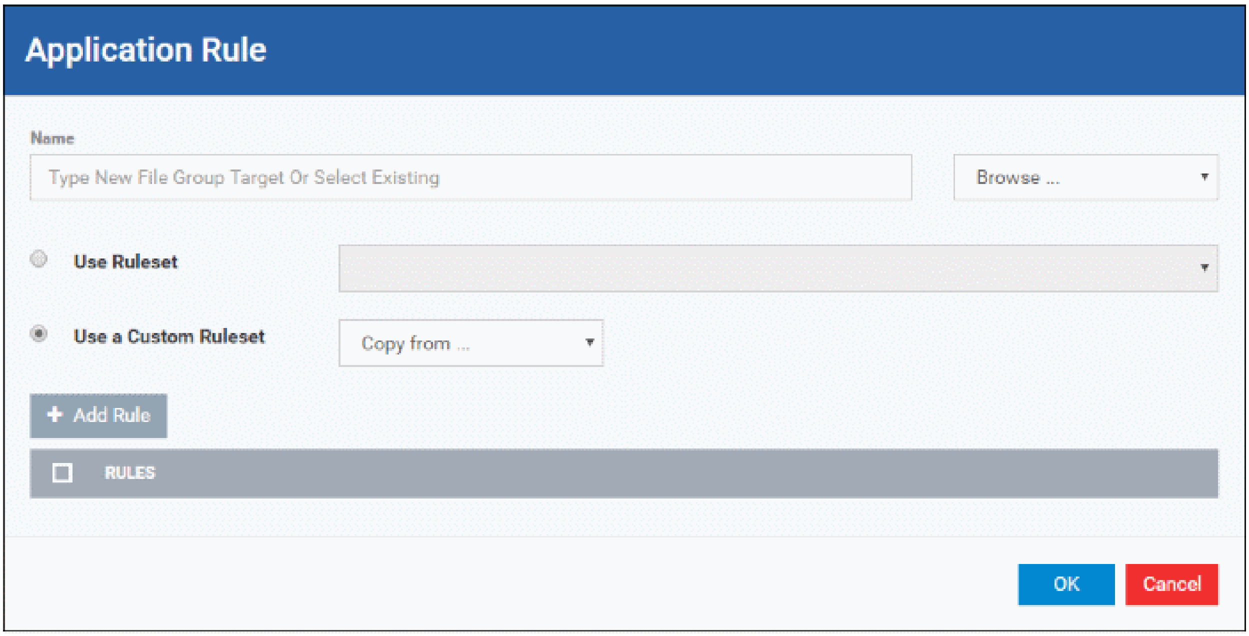
To begin defining an application's Firewall ruleset, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step 2 - **Configure the rules for this application's ruleset.**

**Step 1 - Select the application that you wish the ruleset is to be applied**

- To define a ruleset for a new application ( i.e. one that is not already listed), click the 'Add' button **+ Add** at the top of the list in the 'Application Rules' interface.

The 'Application Rule' interface will open as shown below:



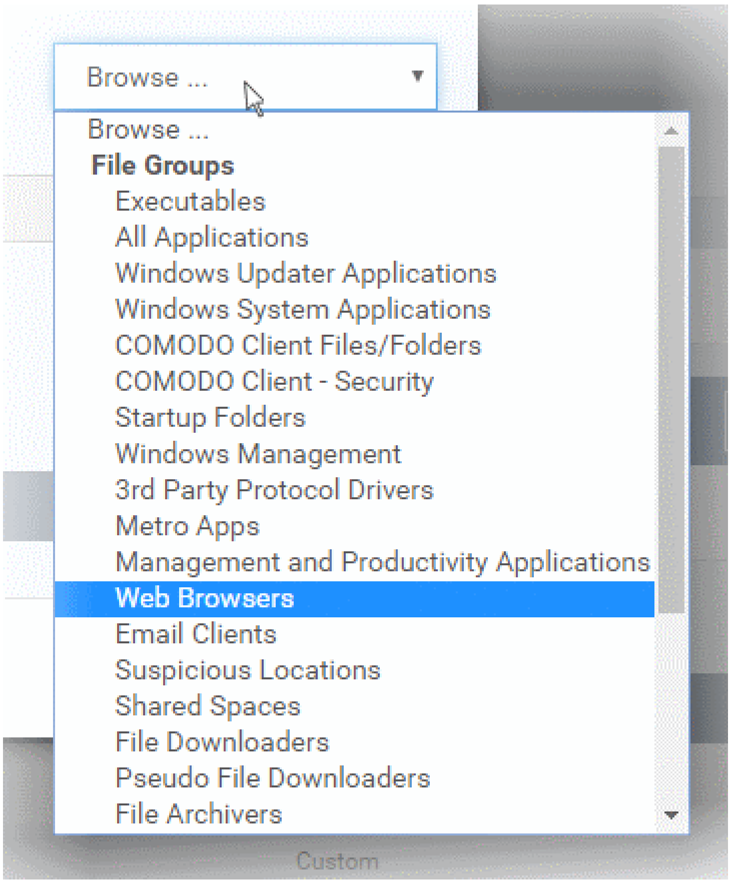
Because this is a new application, the 'Name' field is blank. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

You can enter the application(s) to which the rule set is to be applied in two ways:

- Enter the installation path of the application with the application file name in the Name field (For example, 'C:\Program Files\Mozilla Firefox\firefox.exe').

  Or

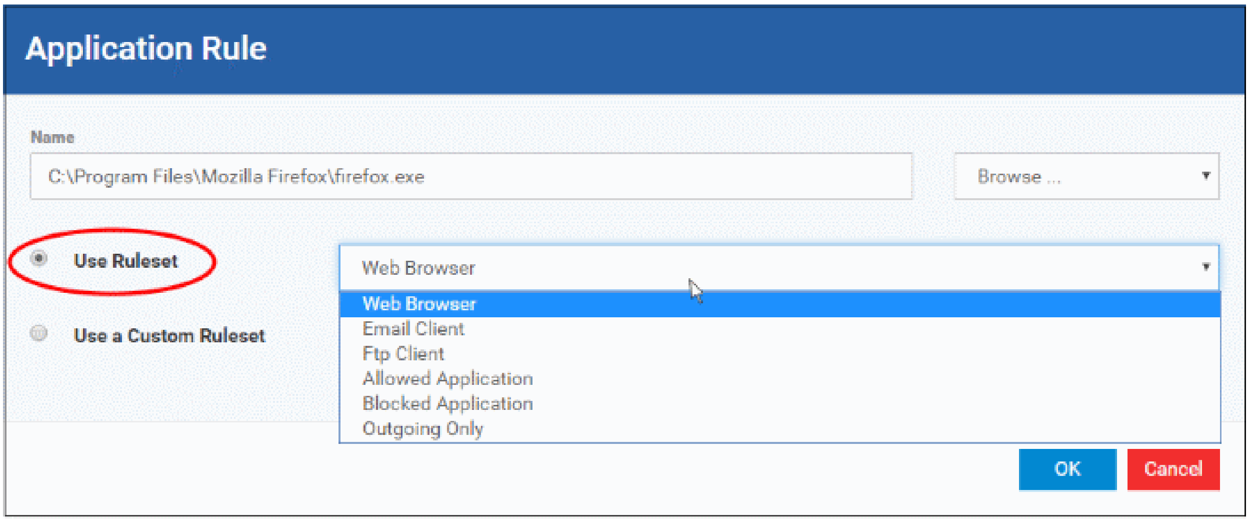
- Open the drop-down beside the 'Name' field and choose the application group to which the ruleset is to be applied. Choosing a 'File Group' allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders. Endpoint Manager ships with a set of predefined 'File Groups'. If required you can add new file groups and edit existing groups ('Settings' > 'System Templates' > 'File Groups Variables'). See **Create and Manage File Groups** for guidance on this.



**Step 2 - Configure the rules for this application's ruleset**

There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Allows you to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Firefox' browser. The name of the predefined ruleset you choose is displayed in the '**Treat As** ' column for that application in the '**Application Rules' interface** ***(Default = Disabled).***



Application Rule

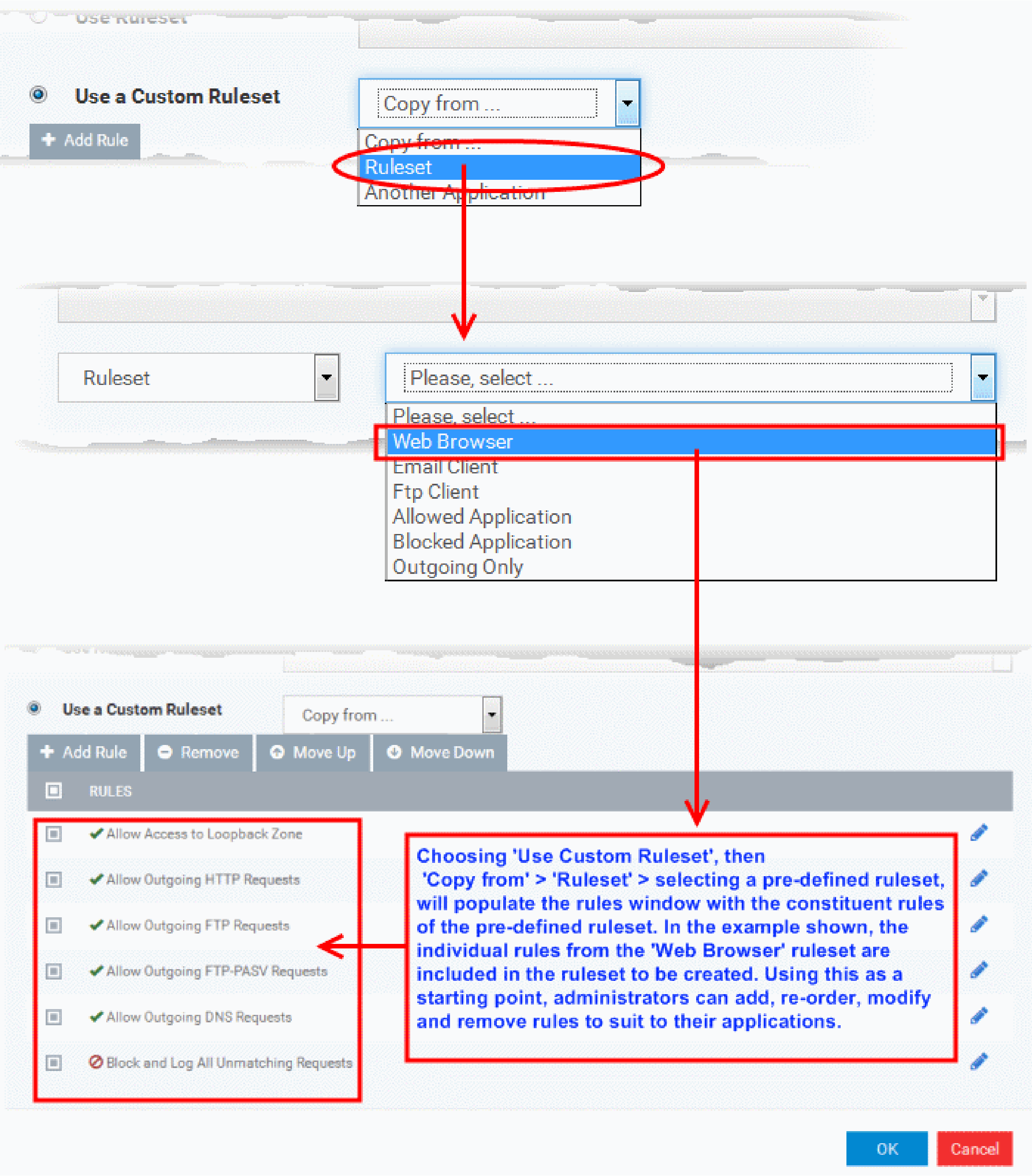
Name: C:\Program Files\Mozilla Firefox\firefox.exe

● Use Ruleset: Web Browser

○ Use a Custom Ruleset

**Note**: Predefined Rulesets, once chosen, cannot be modified ***directly*** from this interface - they can only be modified and defined using the **Application Rule** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - Designed for more experienced administrators, the Custom Ruleset option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset (***Default = Enabled***).



□ ✓ Allow Access to Loopback Zone
□ ✓ Allow Outgoing HTTP Requests
□ ✓ Allow Outgoing FTP Requests
□ ✓ Allow Outgoing FTP-PASV Requests
□ ✓ Allow Outgoing DNS Requests
□ ⊘ Block and Log All Unmatching Requests

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 '**Add and Edit 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 the 'Firewall Rule' interface. See **Add and Edit a Firewall Rule** for more details.

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 **Add and Edit 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 **Add and Edit a Firewall Rule** to see the list of available IP protocols that can be displayed here.

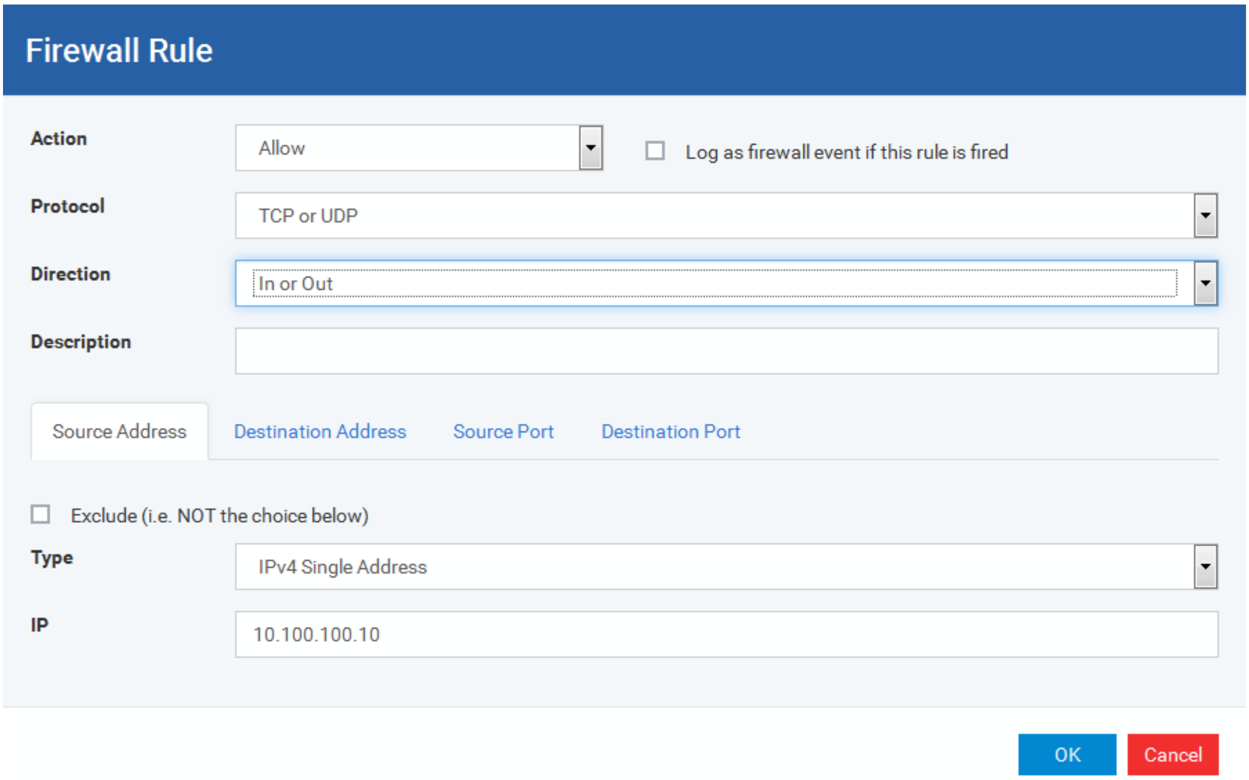
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

* 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, '**Add and Edit 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)

### Add and Edit 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 '**Create and Modify Firewall Rulesets**'.


Firewall Rule

Action: Allow
□ Log as firewall event if this rule is fired
Protocol: TCP or UDP
Direction: In or Out
Description:

□ Exclude (i.e. NOT the choice below)
Type: IPv4 Single Address
IP: 10.100.100.10

### General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' ***(Default)***, '**Block'** or '**Ask**'.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' ***(Default)***, '**ICMP**' or '**IP**' .

**Note:** Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

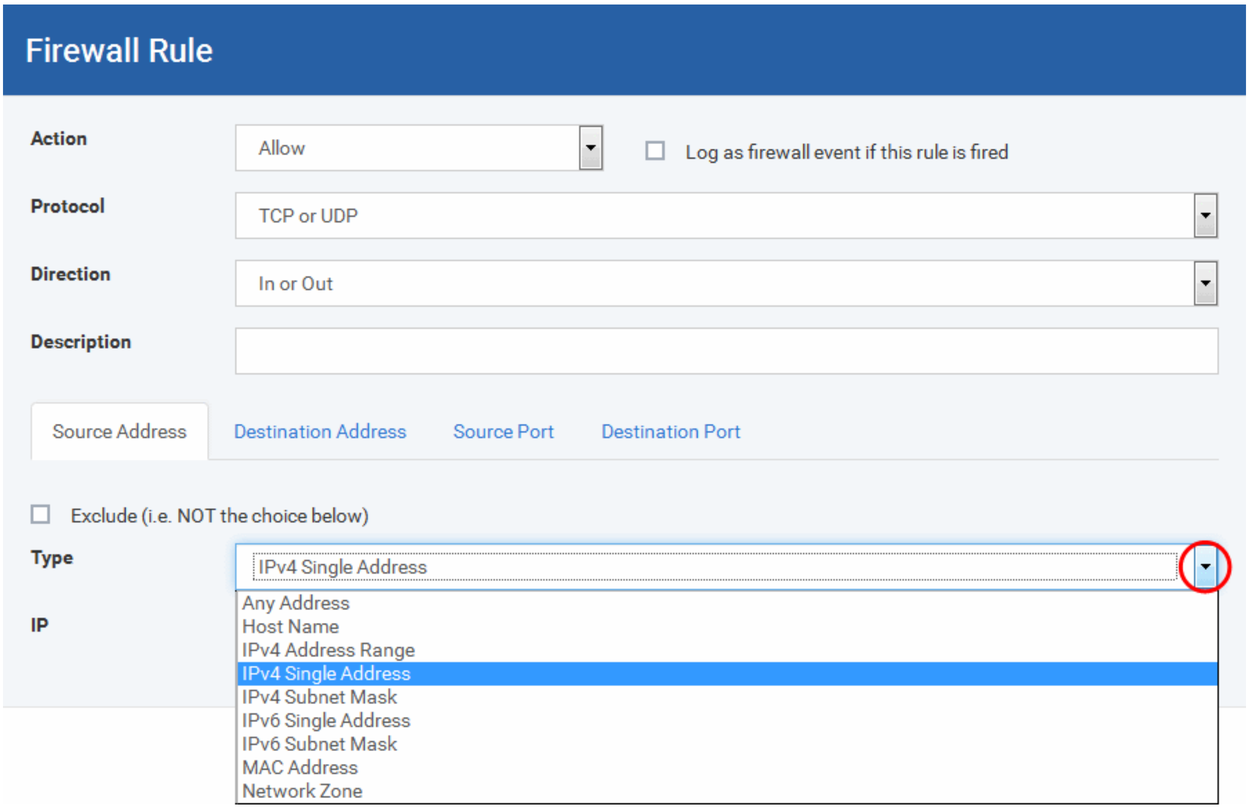
- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the firewall event log viewer whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ( 'Allow Outgoing HTTP requests'). If you create a friendly name, then this is

displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

**Protocol**

i. **'TCP,' 'UDP'** or **'TCP or UDP'**

If you select 'TCP', 'UDP' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information



Firewall Rule

| | |
|---|---|
| Action | Allow |
| Protocol | TCP or UDP |
| Direction | In or Out |
| Description | |

□ Log as firewall event if this rule is fired

Source Address | Destination Address | Source Port | Destination Port

□ Exclude (i.e. NOT the choice below)

Type: IPv4 Single Address

IP

**Source Address and Destination Address:**

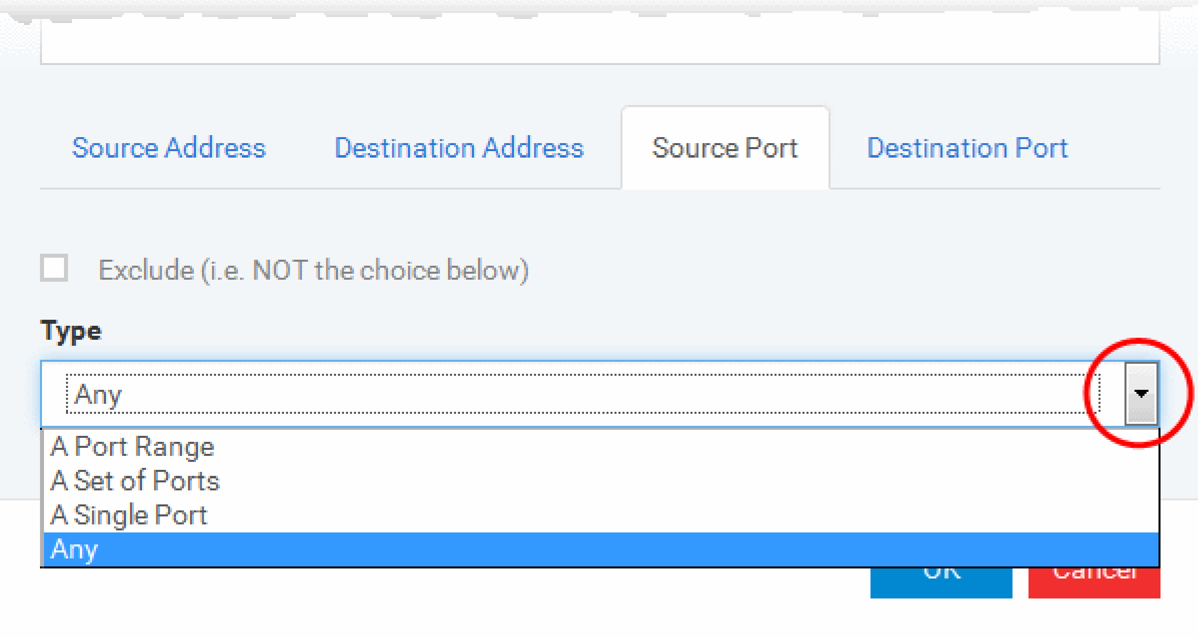
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

**Source Port and Destination Port:**

Enter the source and destination Port in the text box.



1. You can choose any port number by selecting Any - set by default , 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined **Port Set** by choosing A Set of Ports. If you wish to create a custom port set then please see the section '**Port Sets**'.

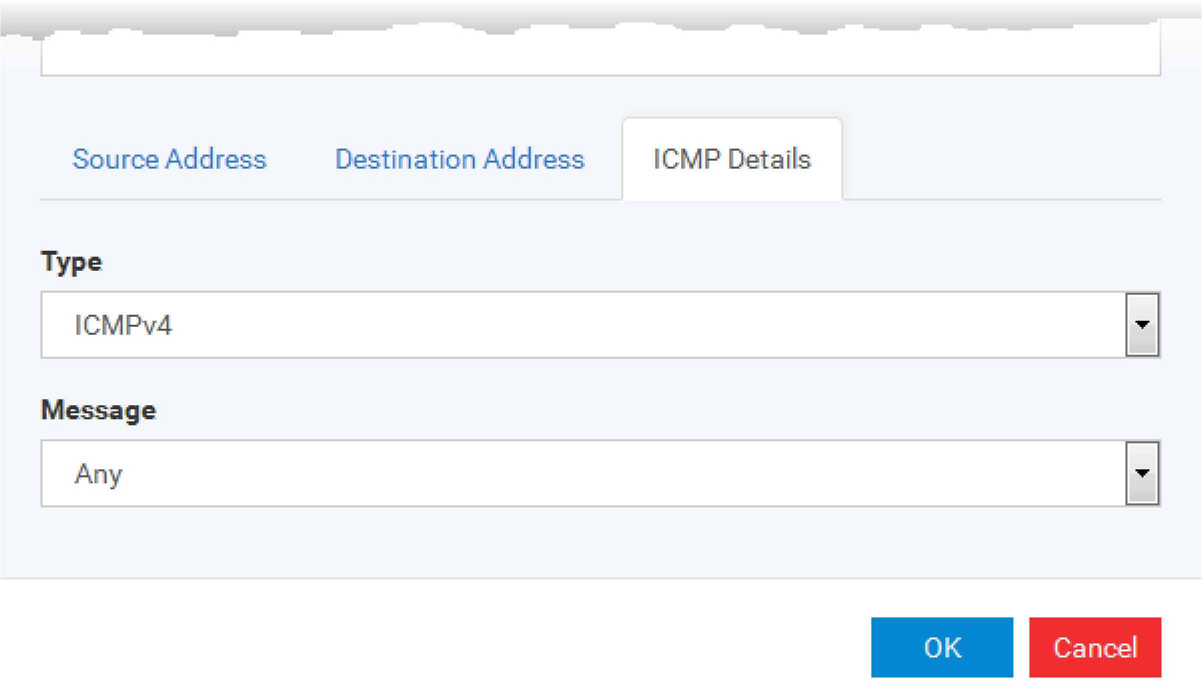
ii. **ICMP**

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

iii. **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.

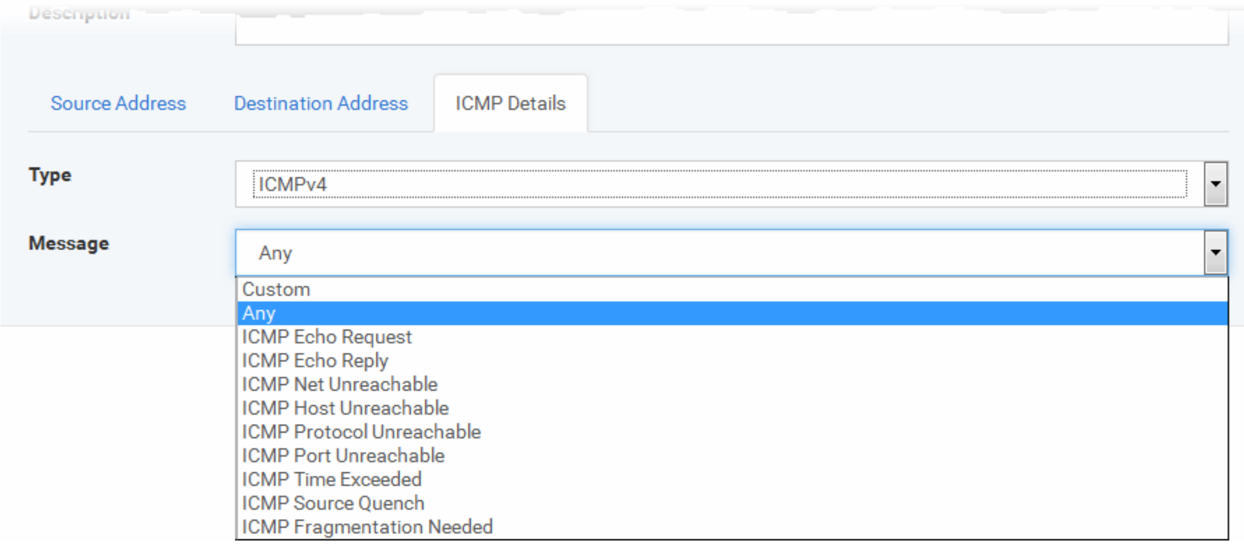
1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.



Type: ICMPv4

Message: Any

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.



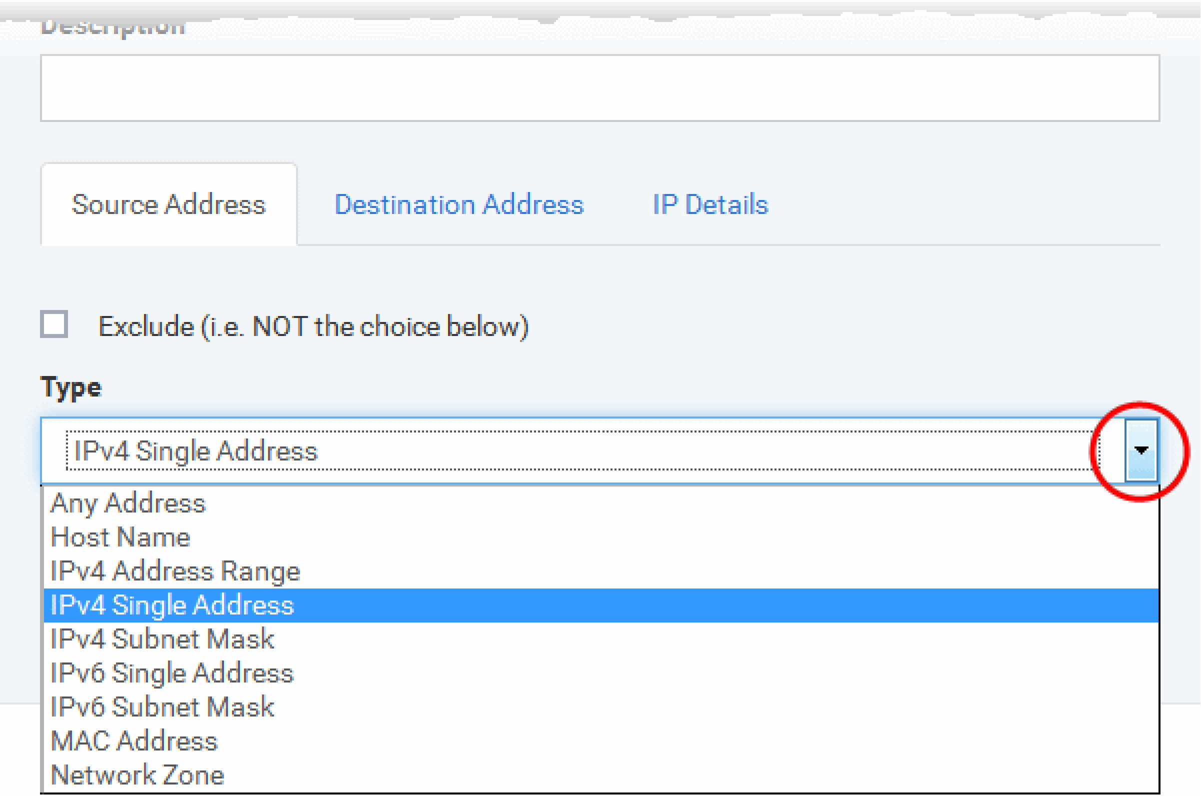
Type: ICMPv4

Message: Any

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.

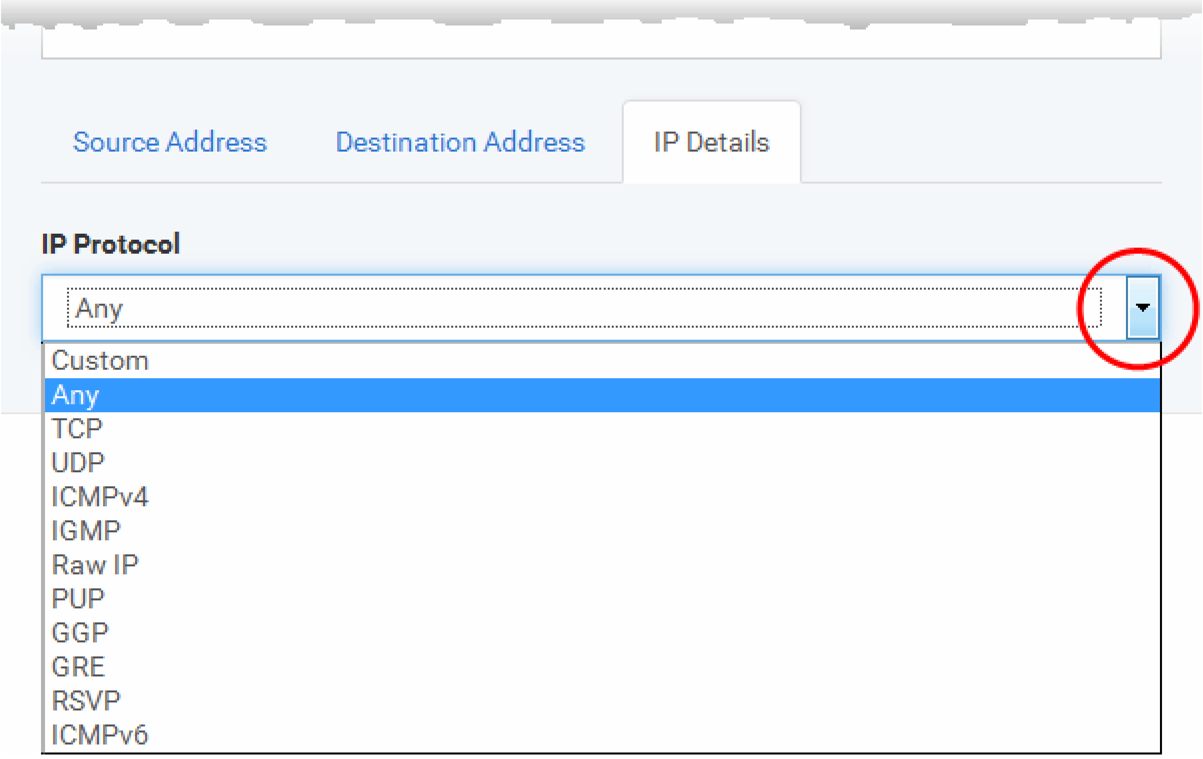
iv. **IP**

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.



v. **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.



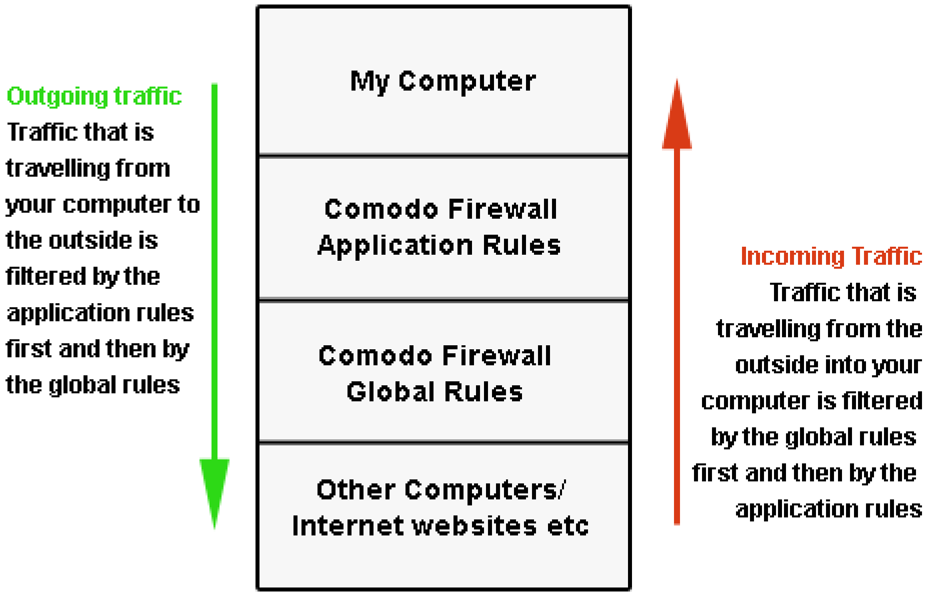
- Click 'OK' to save the firewall rule.

## Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied to all traffic traveling in and out of the computers applied with this profile.

Comodo Firewall analyzes every packet of data in and out of the computer using combination of Application and Global Rules.

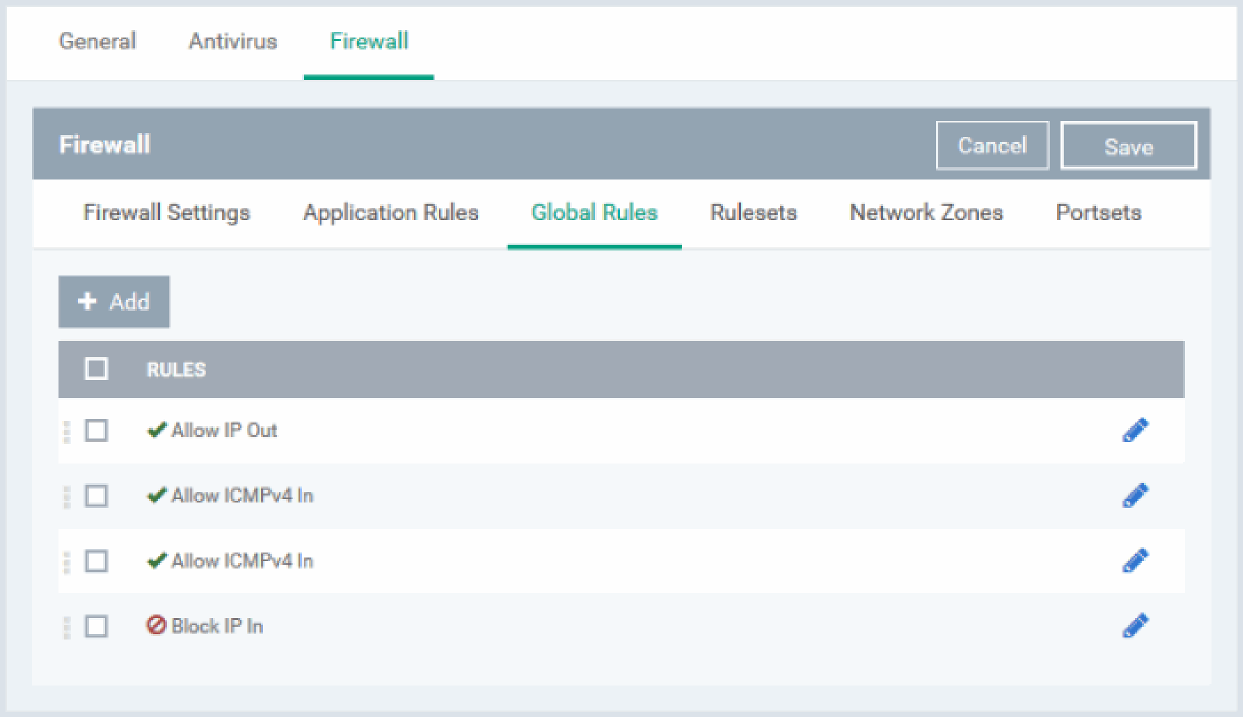
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.


Outgoing traffic
Traffic that is travelling from your computer to the outside is filtered by the application rules first and then by the global rules
My Computer
Comodo Firewall Application Rules
Comodo Firewall Global Rules
Other Computers/ Internet websites etc
Incoming Traffic
Traffic that is travelling from the outside into your computer is filtered by the global rules first and then by the application rules

Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

The 'Global Rules' panel in the under 'Firewall' tab allows you to view create and manage the global firewall rules.



| □ | RULES |
|---|---|
| □ | ✓ Allow IP Out |
| □ | ✓ Allow ICMPv4 In |
| □ | ✓ Allow ICMPv4 In |
| □ | ⊘ Block IP In |

The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add' button **+ Add** on the top. To edit an existing global rule, click the edit icon beside it.

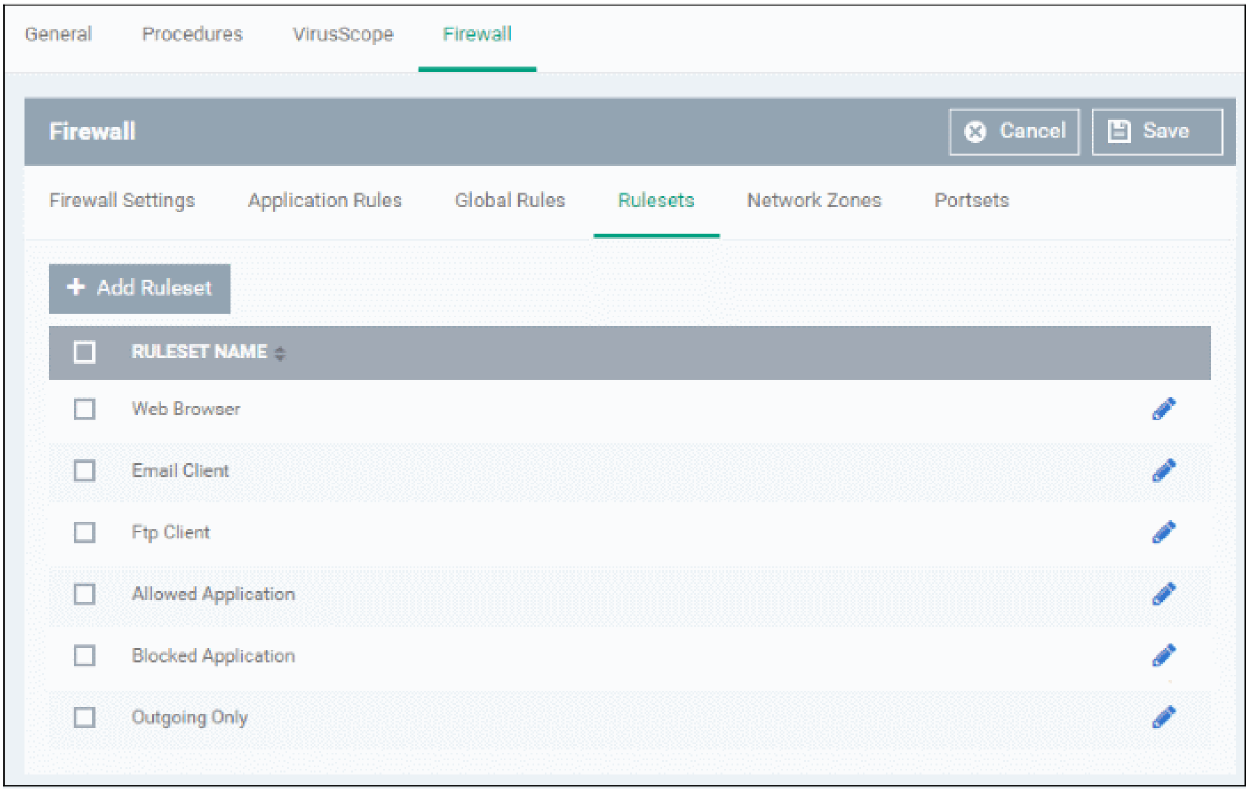
- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Add and Edit a Firewall Rule** for an explanation of individual rule configuration.

## 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. Endpoint Manager ships with six predefined rulesets and allows you to create and manage custom rulesets as required. This section contains advice on the following:

- **Predefined Rulesets**
- **Creating a new ruleset**

The 'Rulesets' panel under the 'Firewall' tab allows you to view, create and manage the firewall rulesets.



| □ | RULESET NAME |
|---|---|
| □ | Web Browser |
| □ | Email Client |
| □ | Ftp Client |
| □ | Allowed Application |
| □ | Blocked Application |
| □ | Outgoing Only |

The Rulesets panel displays a list of pre-defined and custom Firewall Rulesets.

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined policies to suit their environment and requirements. (for example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of it rules).

Endpoint Manager 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 see the explanation of **adding and editing firewall rules** in the section 'Application Rules'.

## Create a new ruleset

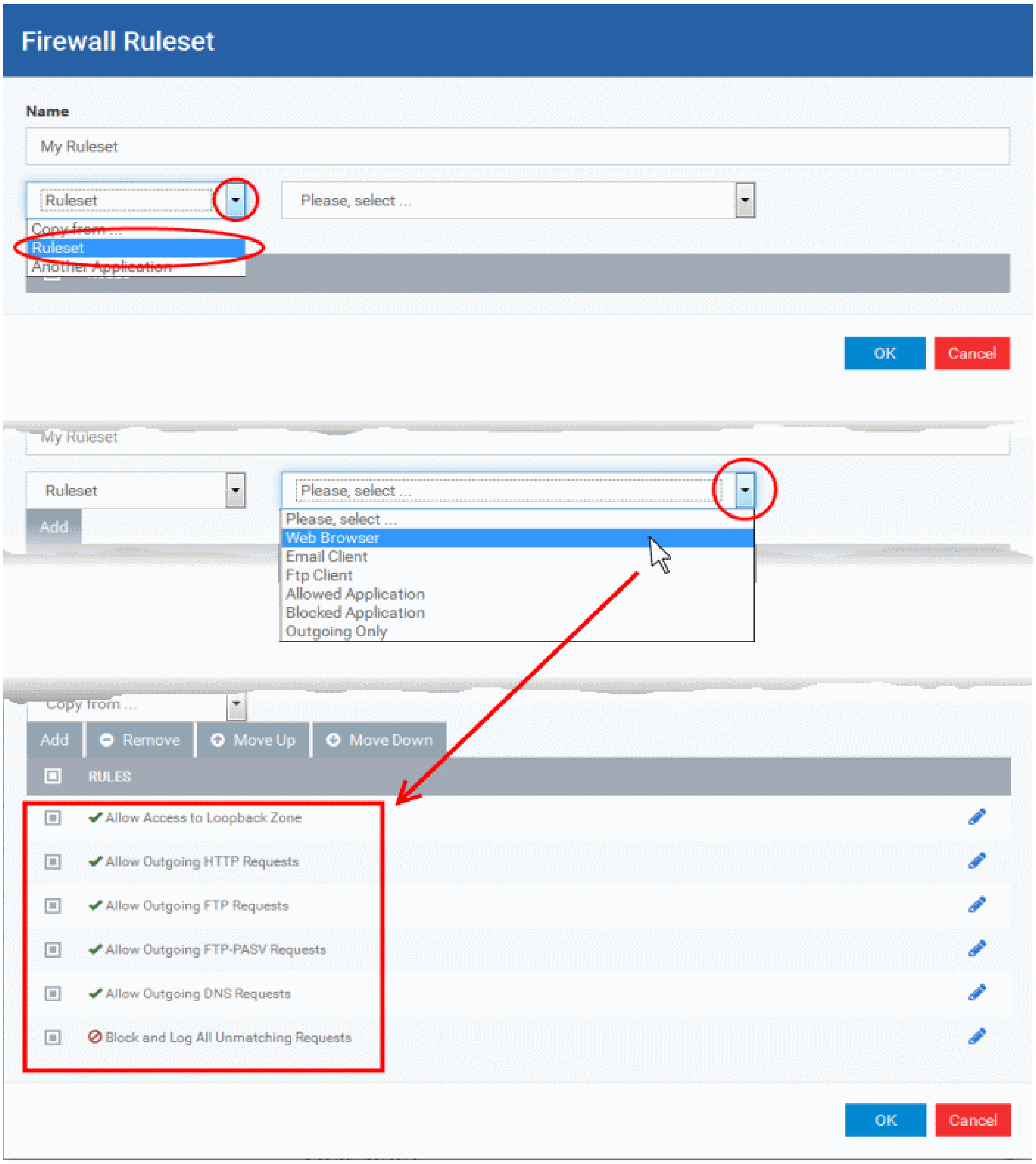
You can create new rulesets with network access control rules customized as per your requirements and can roll out them to required applications while **creating firewall ruleset** for the applications individually.

**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.



Name: My Ruleset

Ruleset

Please, select ...

Copy from ...

RULES
- Allow Access to Loopback Zone
- Allow Outgoing HTTP Requests
- Allow Outgoing FTP Requests
- Allow Outgoing FTP-PASV Requests
- Allow Outgoing DNS Requests
- Block and Log All Unmatching Requests

- 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 '**Add and Edit a Firewall Rule**' for more advice on this.

Once created, this ruleset can be quickly called from 'Use Ruleset' when **creating or modifying a Firewall ruleset**.

**To view or edit an existing predefined Ruleset**

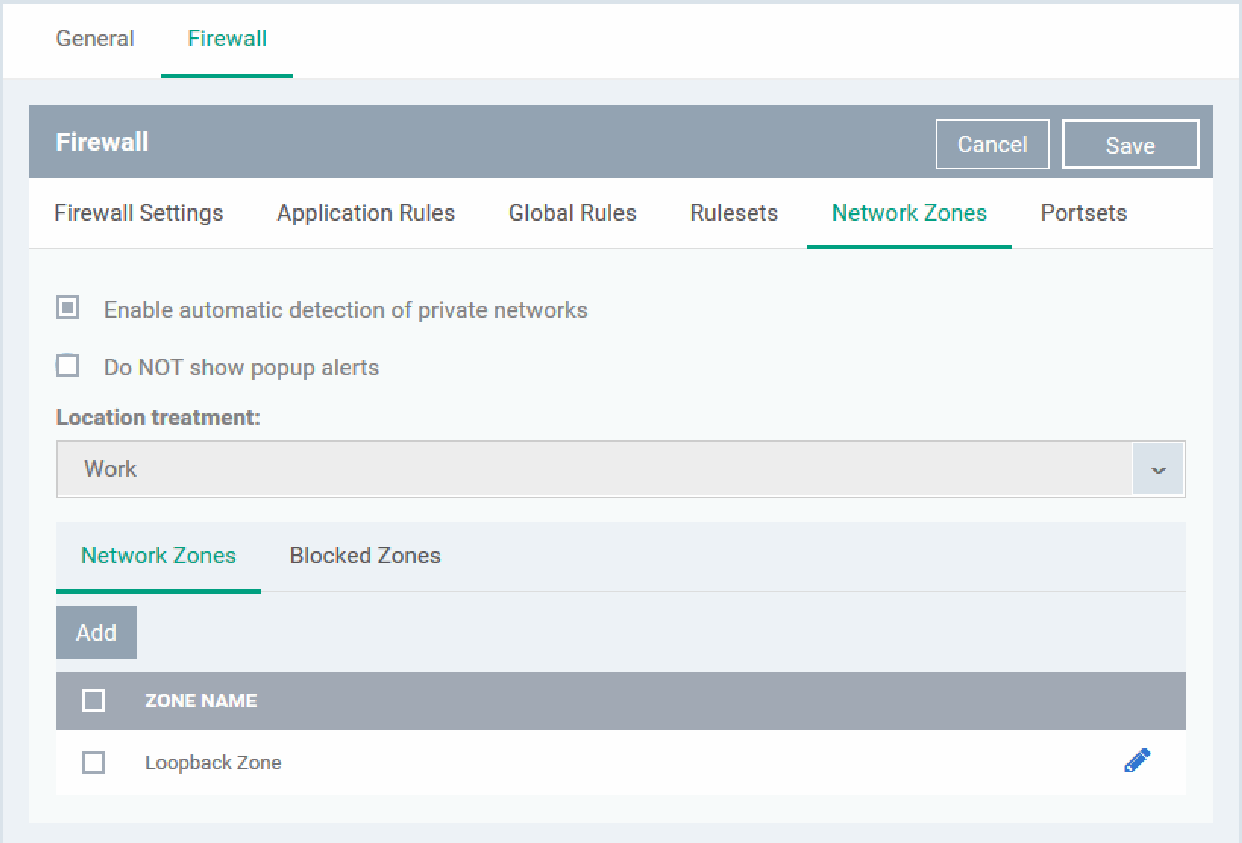
- Click on the 'Edit' icon beside Ruleset Name in the list.
- Details of the process from this point on can be found under '**Use Custom Rule Set.**'.

## Network Zones

The 'Network Zones' panel under the 'Firewall' tab allows you to:

- Configure to detect any new network (wired or wireless) that the computer applied with this profile is trying to connect and provide alerts for the same
- Define network zones that are trusted, and to specify access privileges to them

- Define network zones that are untrusted, and to block access to them



☒ Enable automatic detection of private networks

□ Do NOT show popup alerts

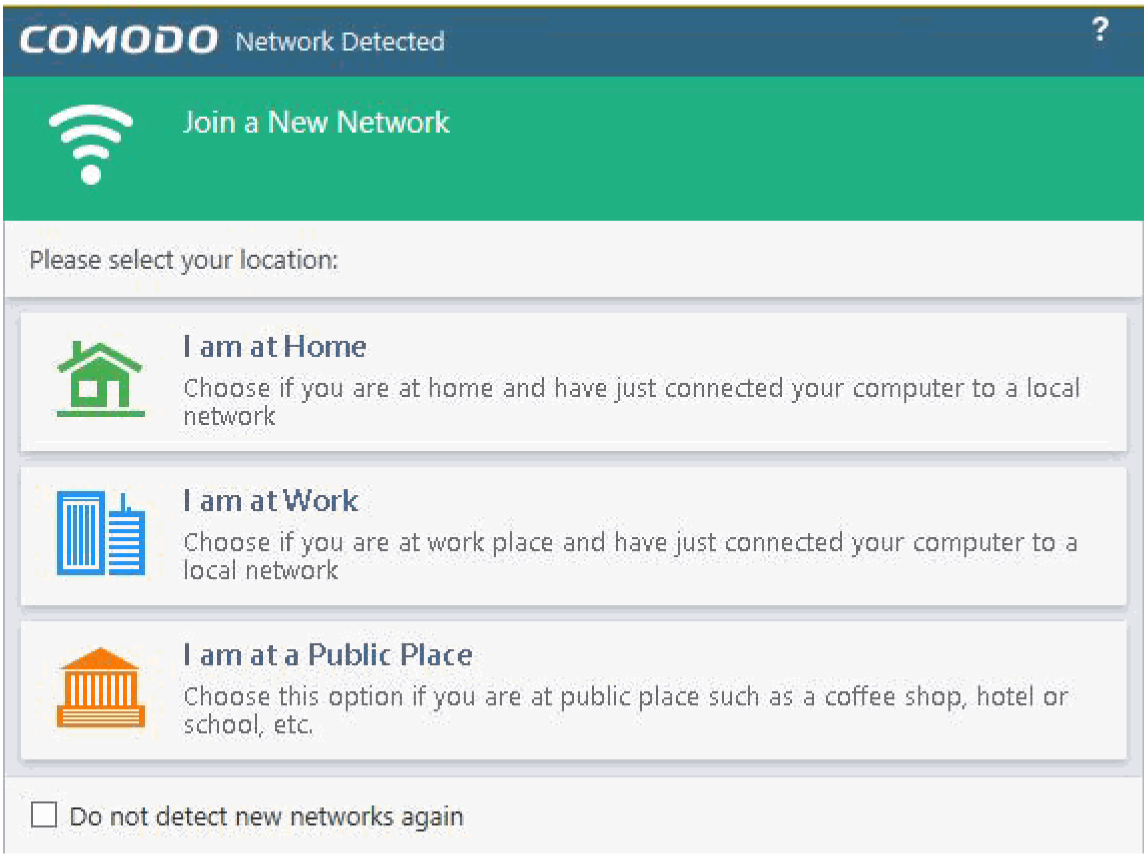
Location treatment: Work

| □ | ZONE NAME |
|---|---|
| □ | Loopback Zone |

The 'Network Zones' panel contains options for configuring the general network monitoring settings and lists of 'Allowed Network Zones' and 'Blocked Network Zones' under respective tabs. You can add and manage network zones to be allowed and blocked from this interface.

**Network Monitoring Settings**:

- **Enable automatic detection of private networks -** Instructs Comodo Firewall to keep monitoring whether the computer applied with this security profile is connected to any new wired or wireless network ***(Default = Enabled).*** Deselect this option if you do not want the new connection attempts is to be detected and/or wish to manually set-up their own trusted networks (this can be done in **'Network Zones**'.
- **Do Not show popup alerts -** By default, an alert will be displayed at the computer, if the computer attempts to connect to a new network, for the end-user to select the type of network. CCS will optimize its firewall settings for the new network, based on the selection. An example is shown below.



COMODO Network Detected ?

Join a New Network

Please select your location:

**I am at Home**
Choose if you are at home and have just connected your computer to a local network

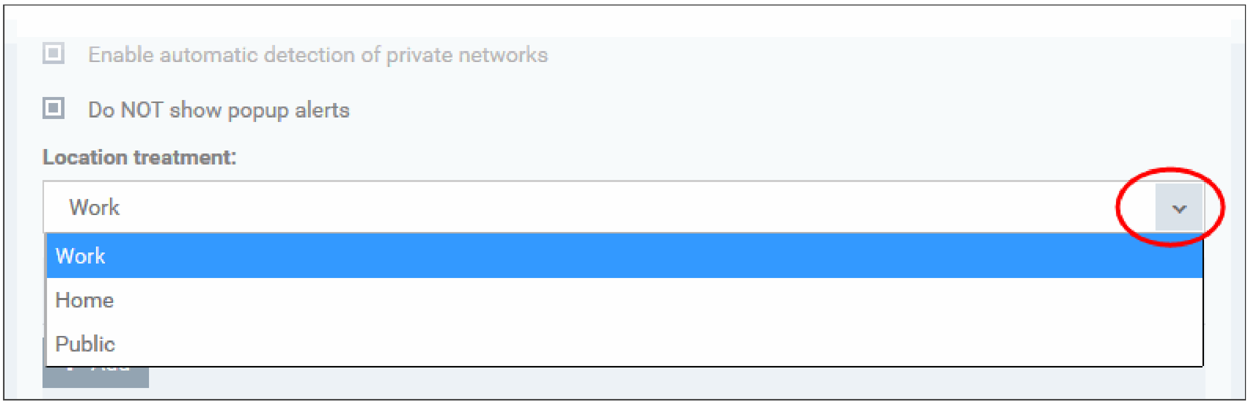
**I am at Work**
Choose if you are at work place and have just connected your computer to a local network

**I am at a Public Place**
Choose this option if you are at public place such as a coffee shop, hotel or school, etc.

□ Do not detect new networks again

If you do not want the alert to be displayed to the end-user and wish the CCS at the computer to decide on the type of network by default, deselect this option and choose the network type from the drop-down under Location Treatment. The available options are:

- Home
- Work
- Public



☐ Enable automatic detection of private networks

☐ Do NOT show popup alerts

Location treatment:

Work

Work<br>Home<br>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

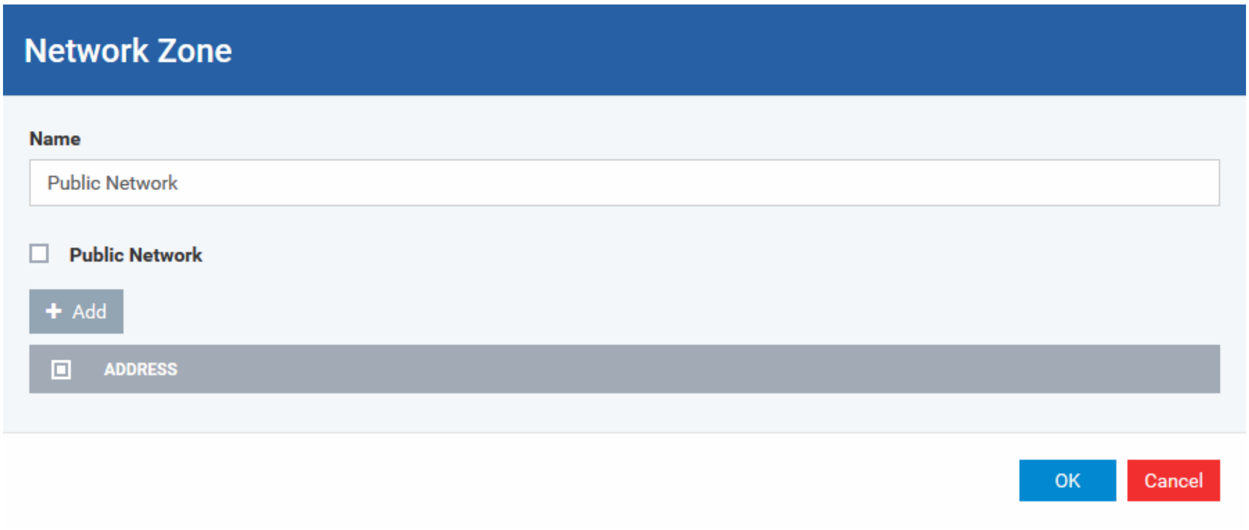
A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied.

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' **+ Add** button at the top of the list.

The 'Network Zone' dialog will open.

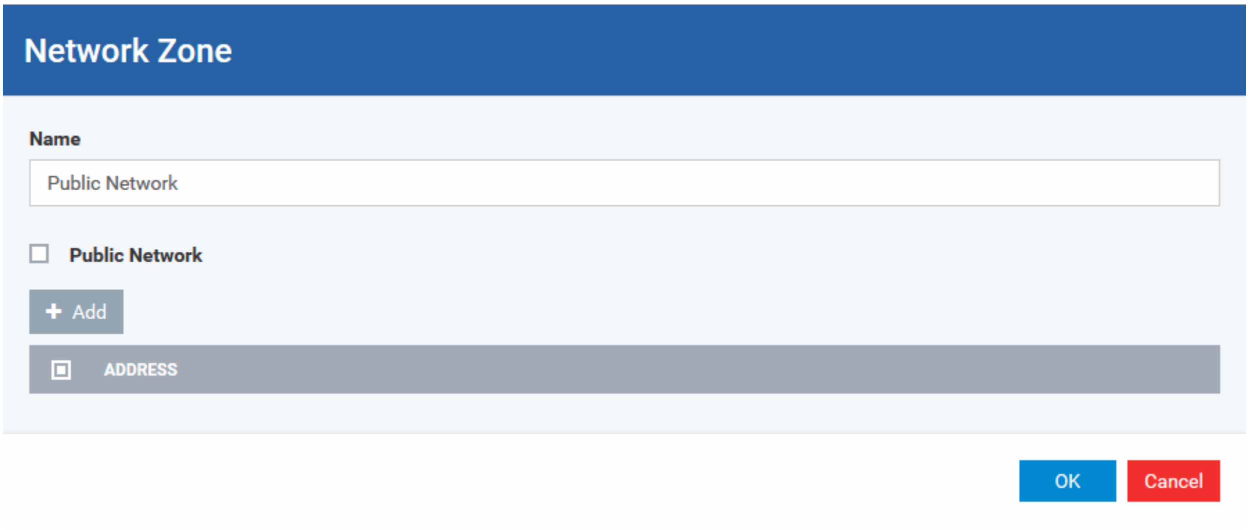


Network Zone

Name: Public Network

□ Public Network

- Enter a name for the new network zone in the 'Name' field.
- Select the checkbox 'Public Network' if you are defining a network zone for a network in a public place, for example, when you are connecting to a Wi-Fi network at an airport, restaurant etc., so that Comodo Firewall will optimize the configuration accordingly.
- Click 'Add' to add the computers in the new network zone



Network Zone

Name: Public Network

□ Public Network

The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below ***(Default = Any Address)***. The 'Exclude' check box will be enabled only if any other choice is selected from the drop-down box.

**Address Types:**

i. Any Address - Adds all the IP addresses (0.0.0.0- 255.255.255.255) to the zone.

ii. Host Name- Enter a named host which denotes an address on your network.

iii. IPv4 Range - Will include all the IPv4 addresses between the values you specify in the 'Start Range' and 'End Range' text boxes.

iv. IPv4 Single Address - Enter a single IP address to be added to the zone - e.g. 192.168.200.113.

v. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to add to the defined zone.

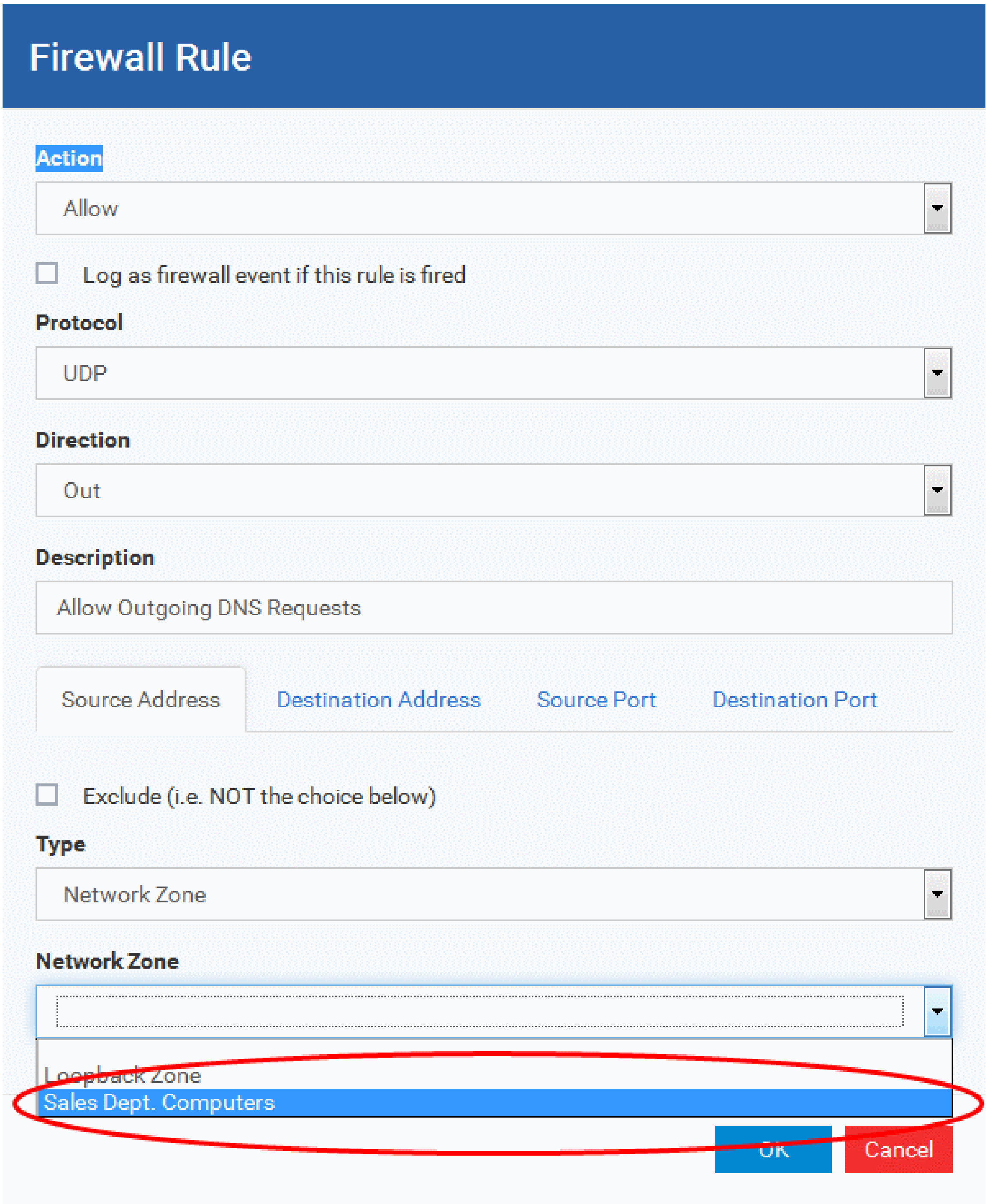
vi. IPv6 Single Address -Enter a single address to be added to the zone - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

vii. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

viii. MAC Address - Enter a specific MAC address to be added to the zone.

- Select/enter the Addresses to be included in the new network zone
- If you want to select all the other addresses to be included in the network zone, excluding those selected under the Type drop-down, select the 'Exclude' option.
- Click 'OK' in the 'Address' dialog.
- Click 'OK' in the 'Network Zone' dialog

The network zone will be added under Network Zones list and will be available to be quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**. Or when defining a **Blocked Zone**.



Firewall Rule

Action: Allow

□ Log as firewall event if this rule is fired

Protocol: UDP

Direction: Out

Description: Allow Outgoing DNS Requests

□ Exclude (i.e. NOT the choice below)

Type: Network Zone

Network Zone:

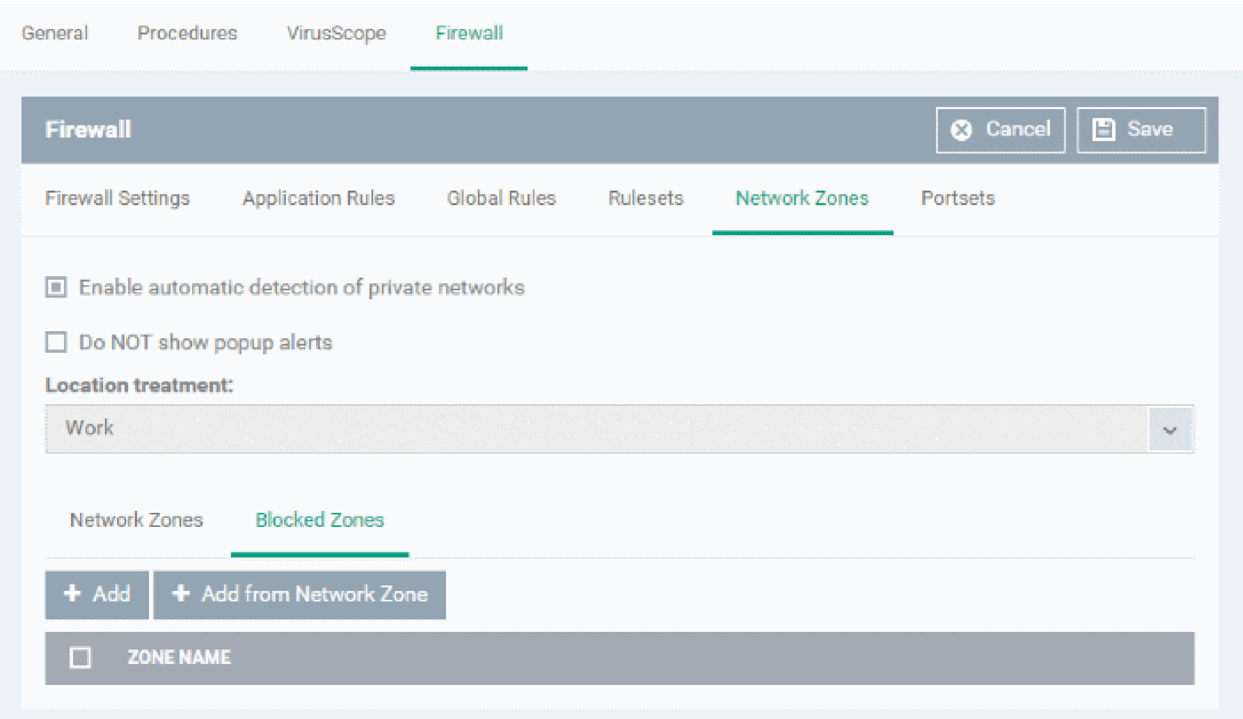
To edit a network zone, click the 'Edit' icon ✎ beside the network zone name. The 'Network Zone' dialog will appear populated with the name and the addresses of the network zone. Edit the details as required. The process is similar to **defining a new network zone** as explained above.

**Blocked Zones**

A computer network enables users to share information and devices between computers and other users within the network. There are certain networks that you'll want to 'trust' and grant access to - for example your work network. Conversely, there may be other networks that you do not trust and want to restrict communication with - or even block entirely.

The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not wish to trust and the computers applied with this profile will be blocked access to them.

The 'Blocked Zones' tab allows you to view the list of blocked network zones and add new blocked zones.



☒ Enable automatic detection of private networks

□ Do NOT show popup alerts

Location treatment: Work

The 'Blocked Zones' tab displays a list of zones that are currently blocked and allows you to:

- **Deny access to an existing network zone**
- **Deny access to a network by manually defining a new blocked zone**

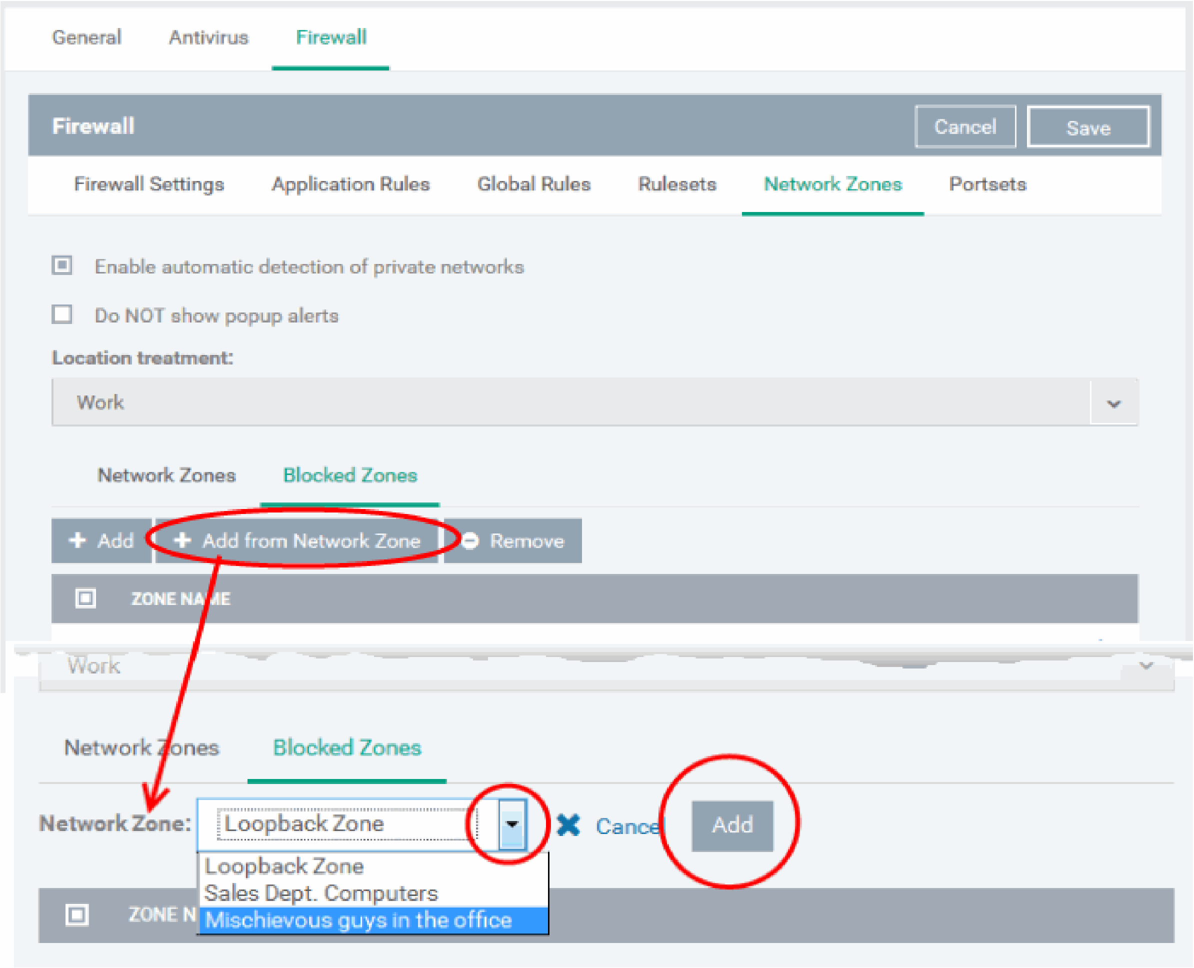
**Note 1**: You must create a zone before you can block it. There are two ways to do this;

1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

**Note 2**: You cannot reconfigure *existing* zones from this interface (e.g. to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

### To deny access to an existing network zone

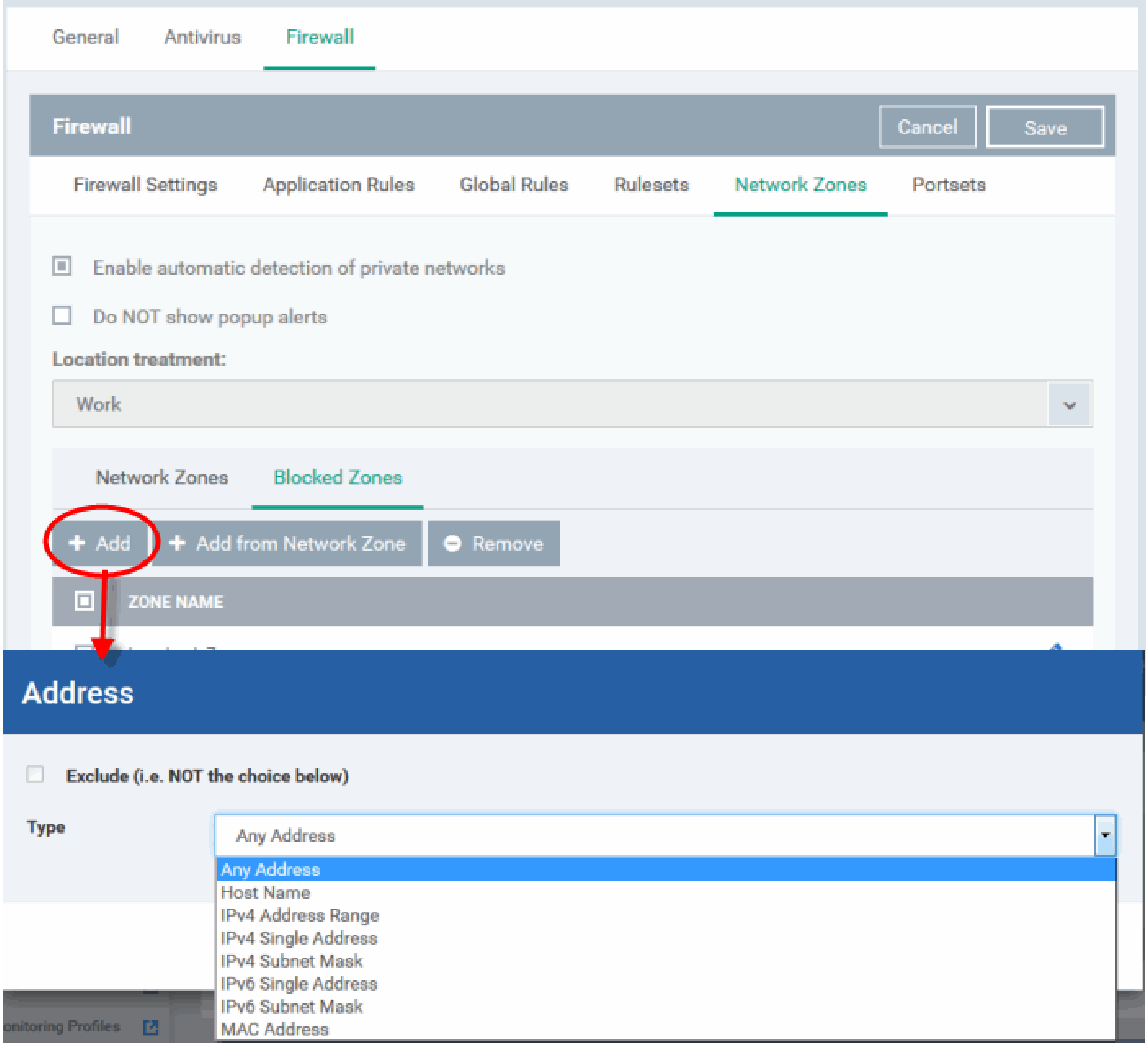
- Click 'Add from Network Zone' button from the top
- Choose the particular zone you wish to block from the 'Network Zone' drop-down.



- Click 'Add'
- Repeat the process to add more blocked network zones for the profile

**To deny access to a network by manually defining a new blocked zone**

- Click the 'Add' button from the top.



- Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

  **Address Types:**

  i. Any Address - Will block connections from all IP addresses (0.0.0.0- 255.255.255.255)

  ii. Host Name- Enter a named host which denotes an address on your network.

  iii. IPv4 Range - Will block access to the IPv4 addresses you specify in the 'Start Range' and 'End Range' text boxes.

  iv. IPv4 Single Address - Block access to a single address - e.g. 192.168.200.113.

  v. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to block.

  vi. IPv6 Single Address -Block access to a single address - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

  vii. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

  viii. MAC Address - Block access to a specific MAC address.

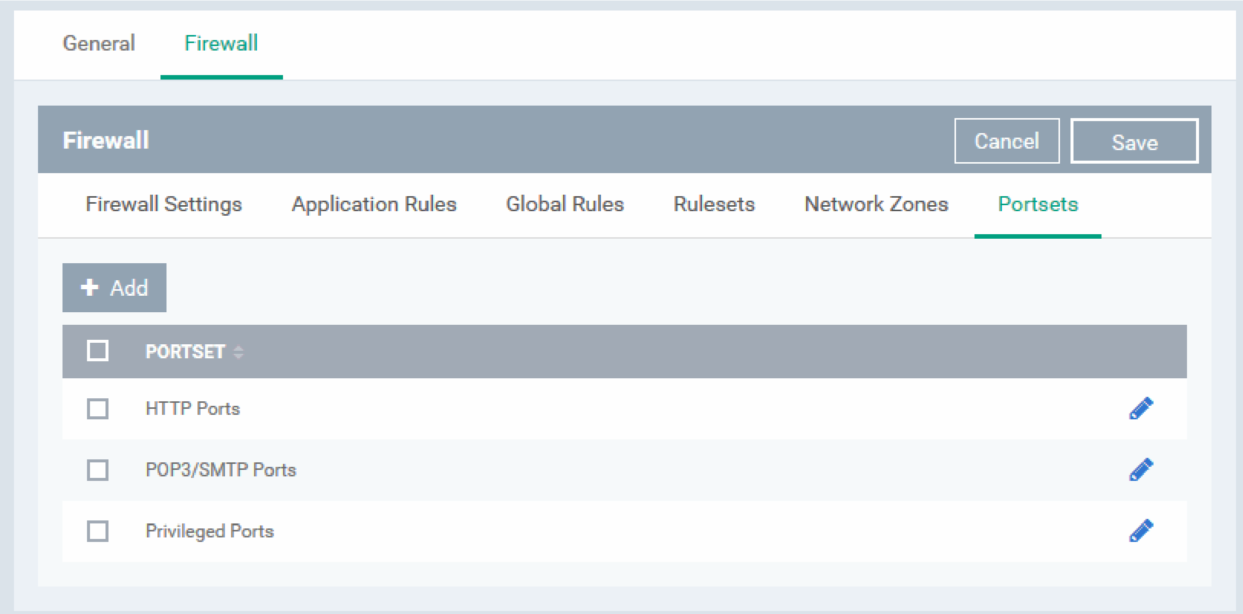
2. Select the address to be blocked and click 'OK'

The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

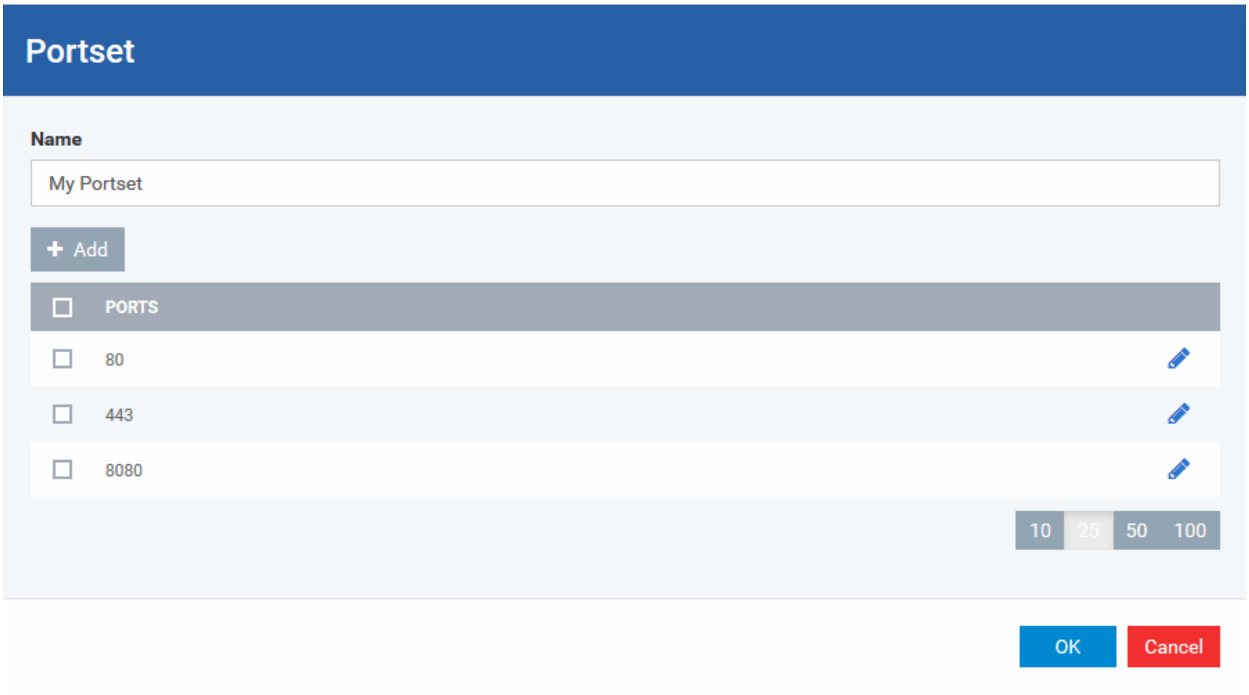
## Portsets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple **Application Rules** and **Global Rules**. The 'Port Sets' panel under the 'Firewall' tab allows you to view and manage pre-defined port sets and to add new port sets for the profile. The name of the port set is listed above the actual port numbers that belong to that set.



| □ | PORTSET |
|---|---|
| □ | HTTP Ports |
| □ | POP3/SMTP Ports |
| □ | Privileged Ports |

The panel lists all portsets that are defined for the profile. Clicking the 'Edit' icon ✎ beside a name reveals the ports included in the set.



Name

My Portset

| □ | PORTS |
|---|---|
| □ | 80 |
| □ | 443 |
| □ | 8080 |

Endpoint Manager 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.

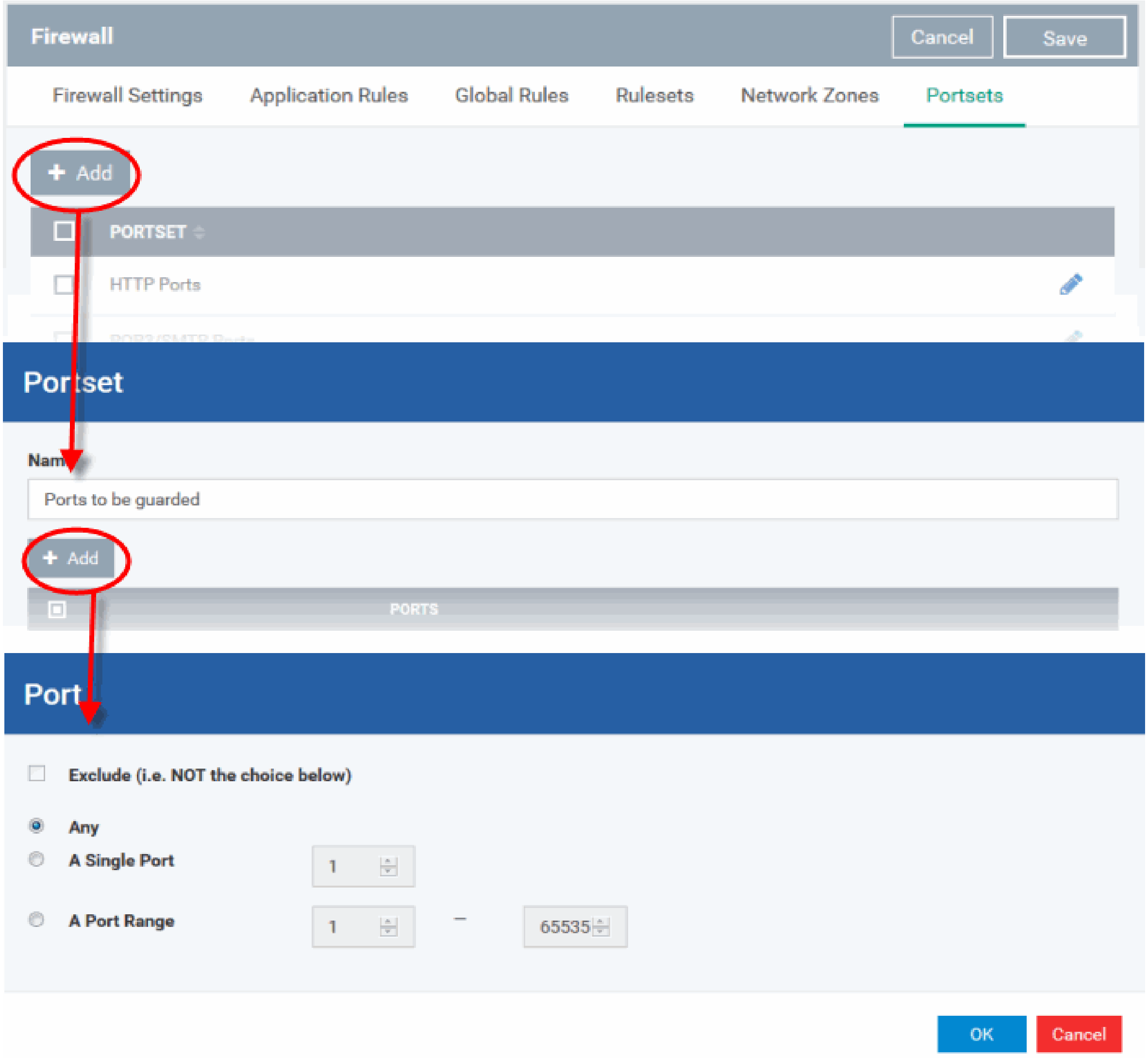
## Define a new Port Set

You can create new portsets and allow access to them for applications, with the access privileges specified through **Application Rule** interface. See '**Create or Modify Firewall Rules**' for more details.

### To add a new portset

- Click the 'Add' button from the top.

The 'Portset' dialog will open.

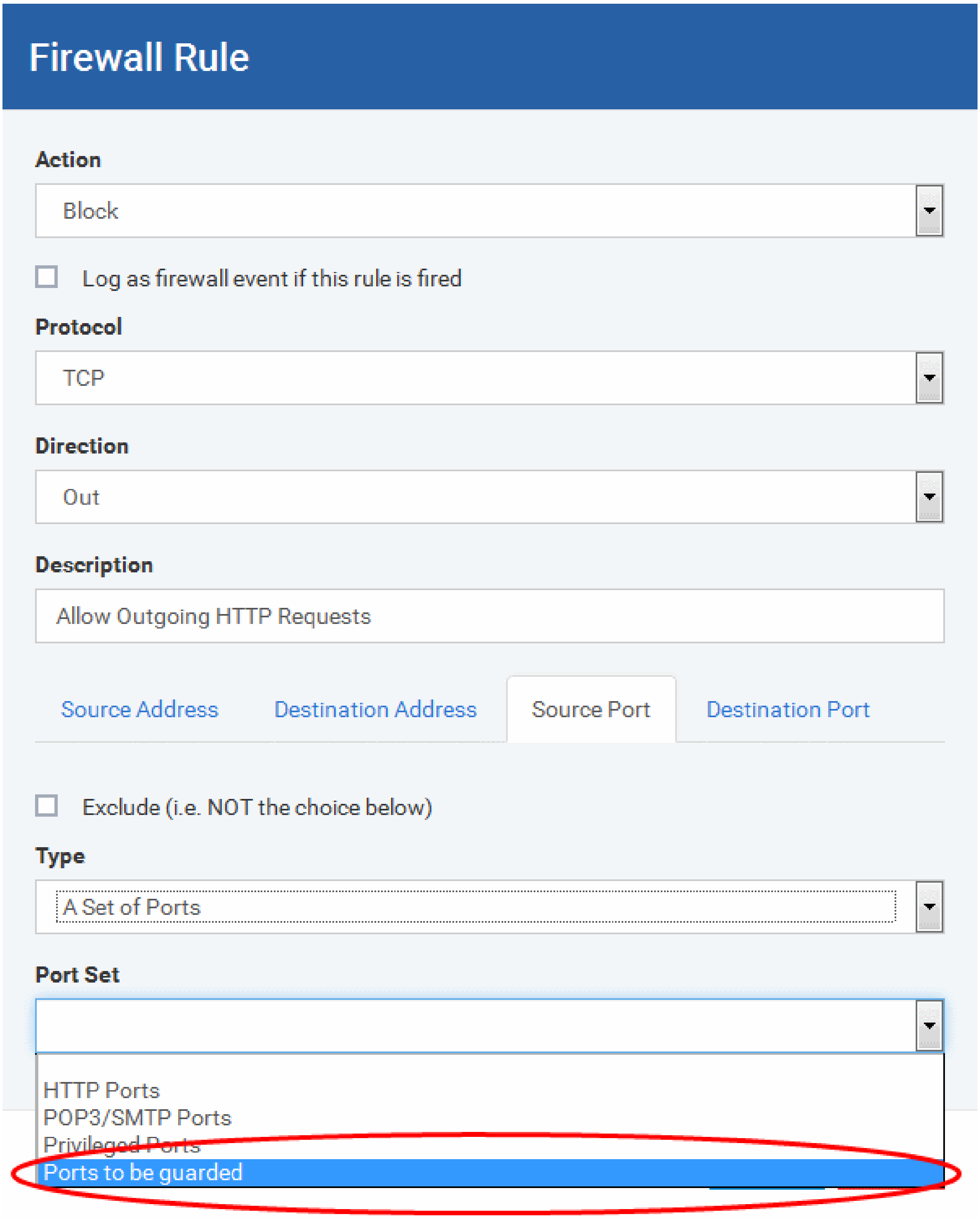


- Enter a name for the new portset in the 'Name' field.
- To add ports to the new portset, click the 'Add' button above the list of ports.
- Specify the ports to be included in the new portset:

  - **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

□ Exclude (i.e. NOT the choice below)

Type: A Set of Ports

Port Set:

**To edit an existing port set**

  - Click the 'Edit' icon ✎ beside the name of the portset. The 'Portset' dialog will appear with a list of port numbers in the port set.
  - The editing procedure is similar to **adding the portset** explained above.
- Click the 'Save' button at the top of 'Firewall' interface to sane your settings for the profile.

The saved 'Firewall' settings screen will be displayed with options to edit the settings or delete the section. See **Edit Configuration Profiles** for more details.

### 6.1.3.1.5. HIPS Settings

- The host intrusion prevention system (HIPS) constantly monitors system activity. It only allows processes to run if they comply with security rules in the Windows profile applied to the endpoint.
- For example, HIPS protects system-critical files and registry keys from unauthorized modification by malware.
- Comodo Client Security (CCS) ships with a default HIPS ruleset that provides extremely high levels of protection 'out of the box'. You can also create custom rulesets as required.
- You can configure the feature by adding a HIPS section to a Windows profile.

**Configure HIPS Settings and Rules**

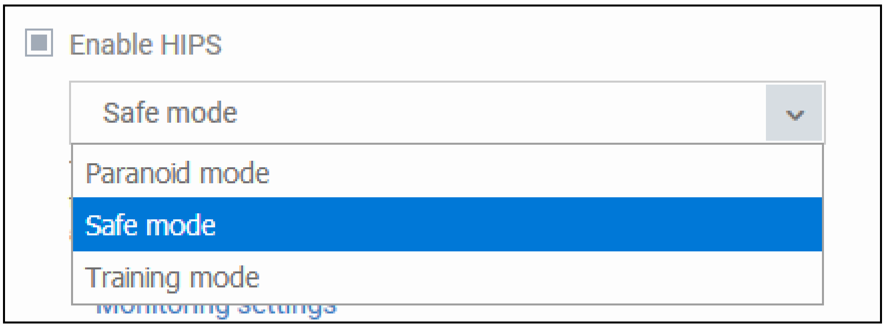
- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Windows profile to open it's details page
  - Click the 'HIPS' tab, if it has already been added to the profile

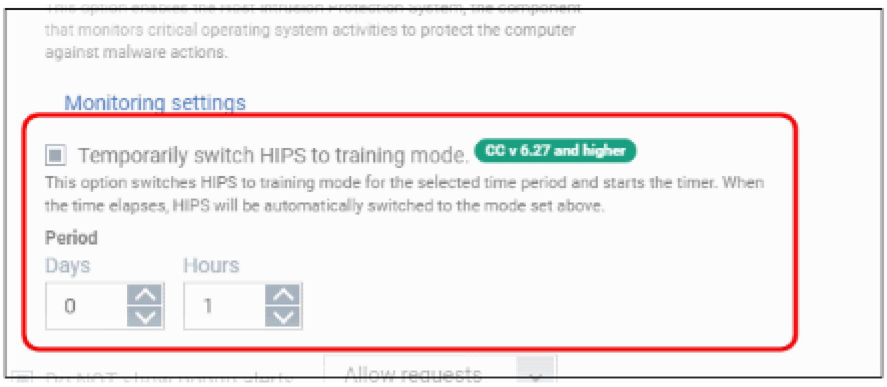
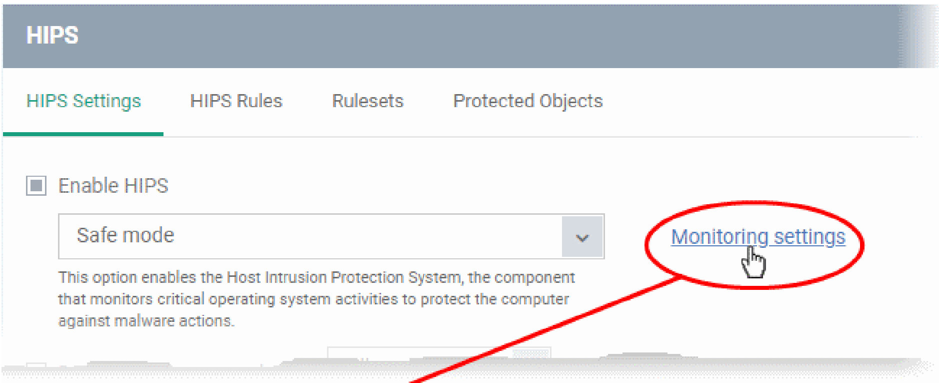
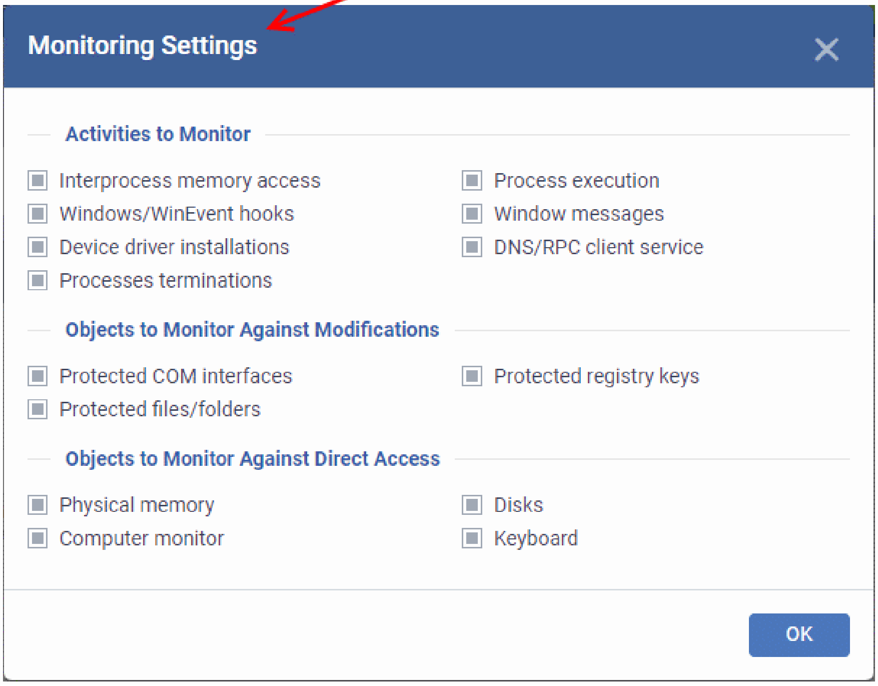
    OR
  - Click 'Add Profile Section' > 'HIPS' if it hasn't yet been added

The HIPS settings screen contains four tabs:

- **HIPS Settings** - Configure settings that govern the overall behavior of the HIPS component.
- **HIPS Rules** - View and create rules that control the behavior of applications on the managed computer.
- **Rulesets** - View predefined rulesets and create new rulesets. Rulesets can be applied to applications on managed computers.
- **Protected Objects** - A protected object is a collection of items which can be referenced as the target of a HIPS rule. For example 'Registry Keys' and 'COM Classes'. This interface lets you view and create new protected objects.

## HIPS Settings

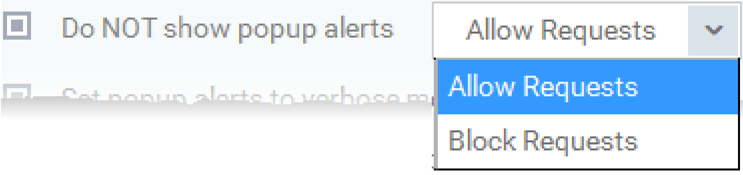
| HIPS Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable HIPS | Activate or deactivate HIPS protection on managed computers to which the profile is applied.<br>If enabled, you can configure the HIPS security level and monitoring settings.<br>(***Default=Enabled***) |
| 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'.<br><br>☑ Enable HIPS<br>Safe mode<br> Paranoid mode<br>Safe mode<br>Training mode<br>Monitoring settings<br>The available options are:<br>• **Paranoid Mode**: This is the highest security level setting and means that HIPS monitors and controls all executable files apart from those that you have deemed safe. Comodo Client Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Client Security does automatically create 'Allow' rules for any 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.<br>• **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 then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.<br>• **Training Mode**: HIPS monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. The end-user will not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on the endpoints are safe to run.<br>  • Note - If required you can enable training mode to work temporarily. To do that, select 'Temporarily switch HIPS to training mode' option and set the days / hours. |

| HIPS Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| | <br>that monitors critical operating system activities to protect the computer against malware actions.<br>Monitoring settings<br>☑ Temporarily switch HIPS to training mode. CC v 6.27 and higher<br>This option switches HIPS to training mode for the selected time period and starts the timer. When the time elapses, HIPS will be automatically switched to the mode set above.<br>Period<br>Days: 0<br>Hours: 1<br>Allow requests<br>After the countdown is over, CCS will switch back to previous mode. |
| Monitoring Settings | If HIPS is enabled, you can configure the activities, entities and objects that should monitored by it at the managed endpoint by clicking the 'Monitoring Settings' link.<br><br>HIPS<br>HIPS Settings \| HIPS Rules \| Rulesets \| Protected Objects<br>☑ Enable HIPS<br>Safe mode<br>This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.<br>Monitoring settings<br><br>Monitoring Settings<br>Activities to Monitor<br>☑ Interprocess memory access ☑ Process execution<br>☑ Windows/WinEvent hooks ☑ Window messages<br>☑ Device driver installations ☑ DNS/RPC client service<br>☑ Processes terminations<br>Objects to Monitor Against Modifications<br>☑ Protected COM interfaces ☑ Protected registry keys<br>☑ Protected files/folders<br>Objects to Monitor Against Direct Access<br>☑ Physical memory ☑ Disks<br>☑ Computer monitor ☑ Keyboard<br>OK<br>**Activities To Monitor:**<br>• **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 |

HIPS Settings - Table of Parameters

| Form Element | Description |
|---|---|
| | 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)***<br>• **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)***.<br>• **Device Driver Installations -** Device drivers are small programs that allow applications and/or operating systems to interact with hardware devices on the managed computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on the system. The installation of a malicious driver could, obviously, cause irreparable damage to the computer or even pass control of that device to a hacker. Leaving this option selected means HIPS generates alerts every time a device driver is installed on the computer by an untrusted application ***(Default = Enabled)***.<br>• **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)***.<br>• **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)***.<br>• **Windows Messages -** This setting means Comodo Client Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) ***(Default = Enabled)***.<br>• **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 |

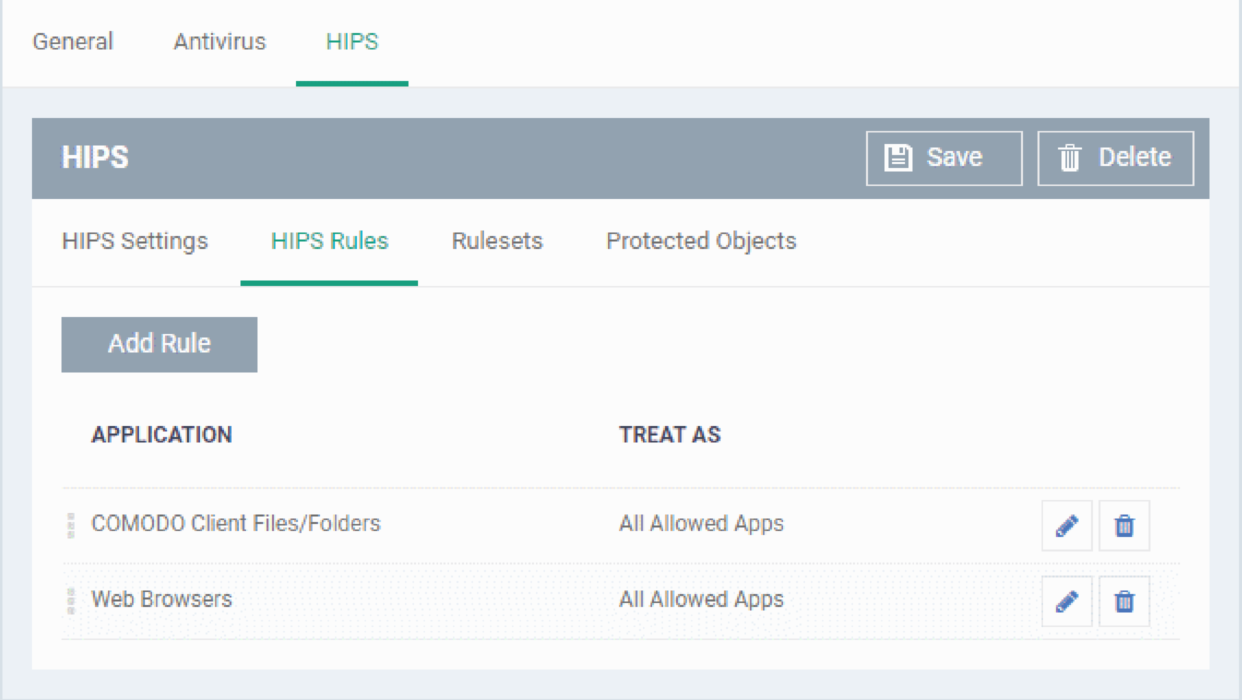
| HIPS Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| | the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack ***(Default = Enabled)***.<br>**Objects To Monitor Against Modifications:**<br>• **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. ***(Default = Enabled)***<br>• **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. ***(Default = Enabled)***.<br>• **Protected Files/Folders** enables monitoring of files and folders you specified from the **File Protection** pane. ***(Default = Enabled)***.<br>**Objects To Monitor Against Direct Access:**<br>Determines whether or not Comodo Client Security should monitor access to system critical objects on the managed computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:<br>• **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)***.<br>• **Computer Monitor:** Comodo Client Security raises an alert every time a process tries to directly access the computer monitor. Although legitimate applications sometimes require this access, spyware can also use such access to take screen shots of the current desktop, record browsing activities of the user and more ***(Default = Enabled).***<br>• **Disks:** Monitors the local disk drives at the managed computer, for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***.<br>• **Keyboard**: Monitors the keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke made on keyboard and can be used to steal passwords, credit card numbers and other personal data typed through the keyboard. With this setting is enabled, Comodo Client Security generates alerts every time an application attempts to establish direct access to the keyboard ***(Default = Enabled)***.<br>**Note**: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a global basis - effectively creating a universal 'Allow' rule for that activity . This 'Allow' setting over-rules any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface. |
| Do NOT show popup alerts | Configure whether or not the HIPS alerts are to be displayed at the managed computer for the end-user to respond. Choosing 'Do NOT show popup alerts' will minimize |

| HIPS Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| | disturbances but at some loss of user awareness (***Default = Enabled***).<br>If you choose not to show alerts then you have a choice of default responses that CCS should automatically take - either 'Block Requests' or 'Allow Requests'.<br><br>▣ Do NOT show popup alerts — Allow Requests<br>Allow Requests<br>Block Requests |
| Set popup alerts to verbose mode | Enabling this option instructs CCS to display HIPS alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests ***(Default = Enabled).*** |
| Create rules for safe applications | CCS will auto-create allow rules for known-safe applications. (***Default = Enabled***)<br>**Note**: HIPS trusts an application if:<br>• The app is from a vendor who has a 'Trusted' status in the local vendor list in CCS<br>• The app is trusted in the online file database (aka, it is whitelisted)<br>• The app is trusted in the local CCS 'File List'<br>See **File Rating Settings** for more details. |
| Set new on-screen alert timeout to | Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 60 seconds. You may adjust this setting to your own preference. |
| Enable adaptive mode under low system resources | Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems ***(Default = Enabled)***. |
| Block unknown requests when the application is not running | Selecting this option blocks all unknown execution requests if Comodo Client Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know the managed computer machine is already 'clean' and are looking just to enable the highest CCS security settings then it is OK to leave this option disabled. ***(Default = Disabled)*** |
| Enable enhanced protection mode (Requires a system restart) | 64 bit systems only. Activate additional protections which counteract sophisticated malware that tries to bypass regular HIPS protection. Because of limitations in Windows 7/8 x64 systems, some HIPS functions in previous versions of CCS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. The endpoint requires a restart to enable enhanced protection mode. (***Default = Disabled***) |

## HIPS Rules

The 'HIPS Rules' screen allows you to view the list of active HIPS rulesets applied to different groups of or individual applications and to create and manage rules for the profile. You can change the ruleset applied to a selected application or application group.

**Note**: HIPS Rulesets are to be created before applying them to an individual application or an application group. Refer to the next section **Rulesets** for details on creating new rulesets.



| APPLICATION | TREAT AS |
|---|---|
| COMODO Client Files/Folders | All Allowed Apps |
| Web Browsers | All Allowed Apps |

| HIPS Rules - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Application | Name of the individual application or the application group to which the ruleset is applied |
| Treat As | The ruleset applied. For more details on the rulesets, see the next section **Rulesets**. |
| Actions | Contains control buttons to edit or remove the rule |

## Create and Modify HIPS Rules

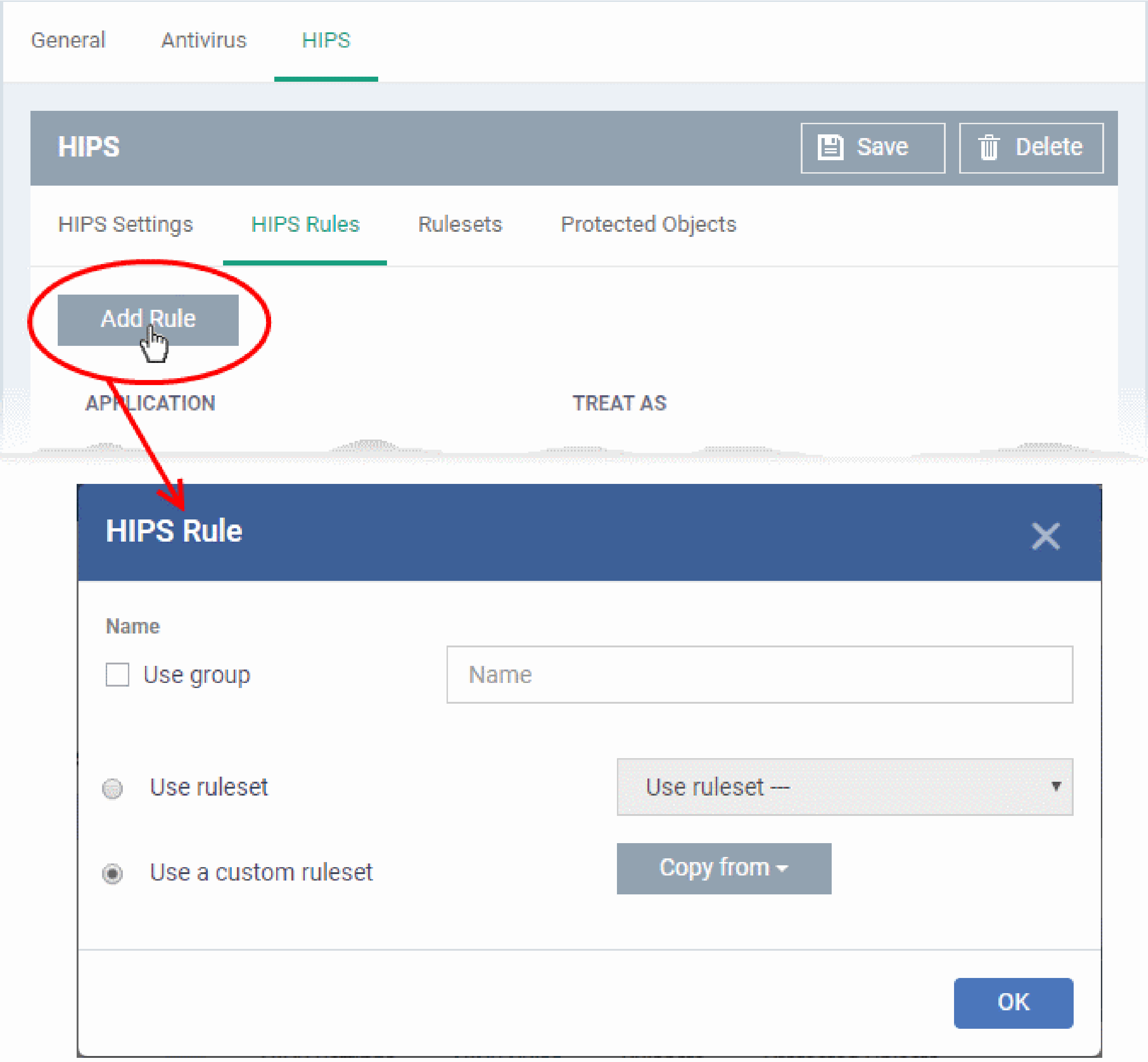
To begin defining an application's HIPS rule, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step2 - **Configure the rules for this application's ruleset.**

**Step 1 - Select the application that you wish the ruleset is to be applied**

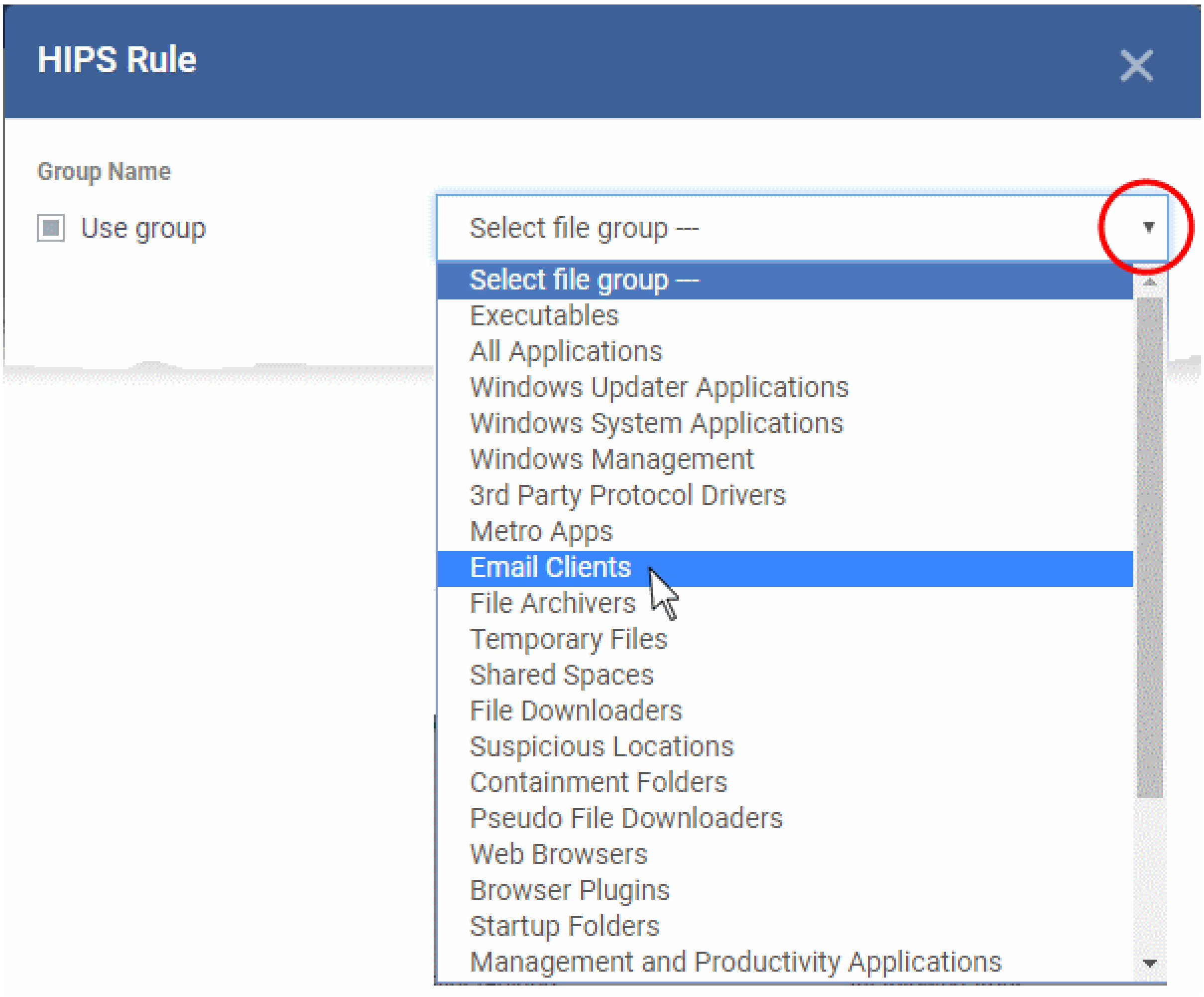
- To define a ruleset for a new application ( i.e. one that is not already listed), click the 'Add Rule' button at the top of the list in the 'HIPS Rules' interface.

The 'HIPS Rule' interface will open as shown below:



Because this is a new application, the 'Name' field is blank. (If you are modifying an existing rule, then this interface shows the individual rules for that application's ruleset).

- To create a rule for a single application enter the file name of it in the 'Name' field
- To create a rule for an application group, select 'Use Group' and choose the file group from the drop-down

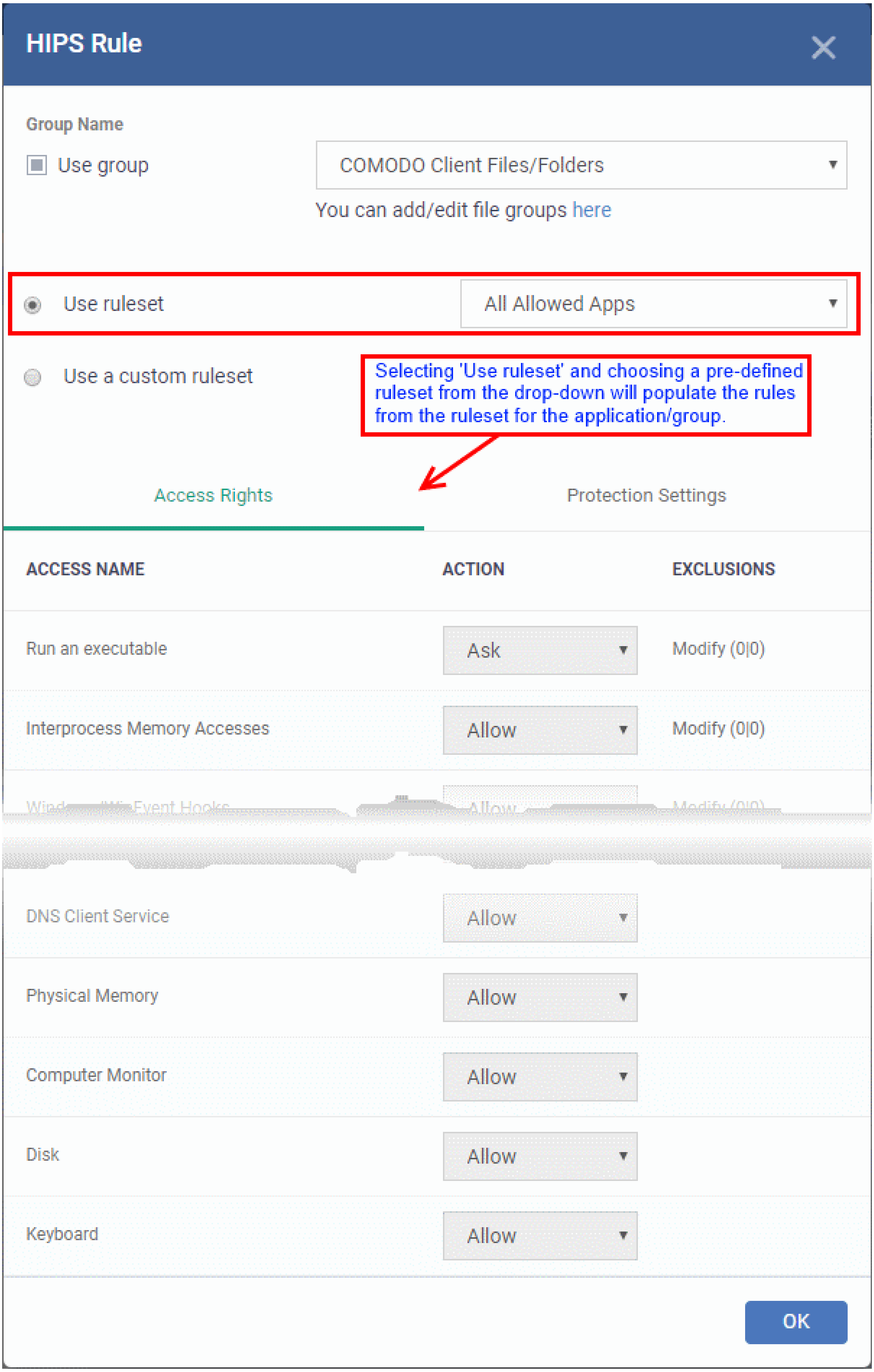


**Note**: Endpoint Manager ships with a set of predefined file groups containing collections of files under respective categories. Admins can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can be created under 'Settings' > 'System Templates' > 'File Groups Variables' interface. See **Create and Manage File Groups** for more details.

**Step 2 - Configure the rules for this application's ruleset**

There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset -** Allows you to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. The name of the predefined ruleset you choose is displayed in the '**Treat As** ' column for that application in the 'HIPS Rules' interface.



HIPS Rule

Group Name

☐ Use group — COMODO Client Files/Folders ▾

You can add/edit file groups here

● Use ruleset — All Allowed Apps ▾

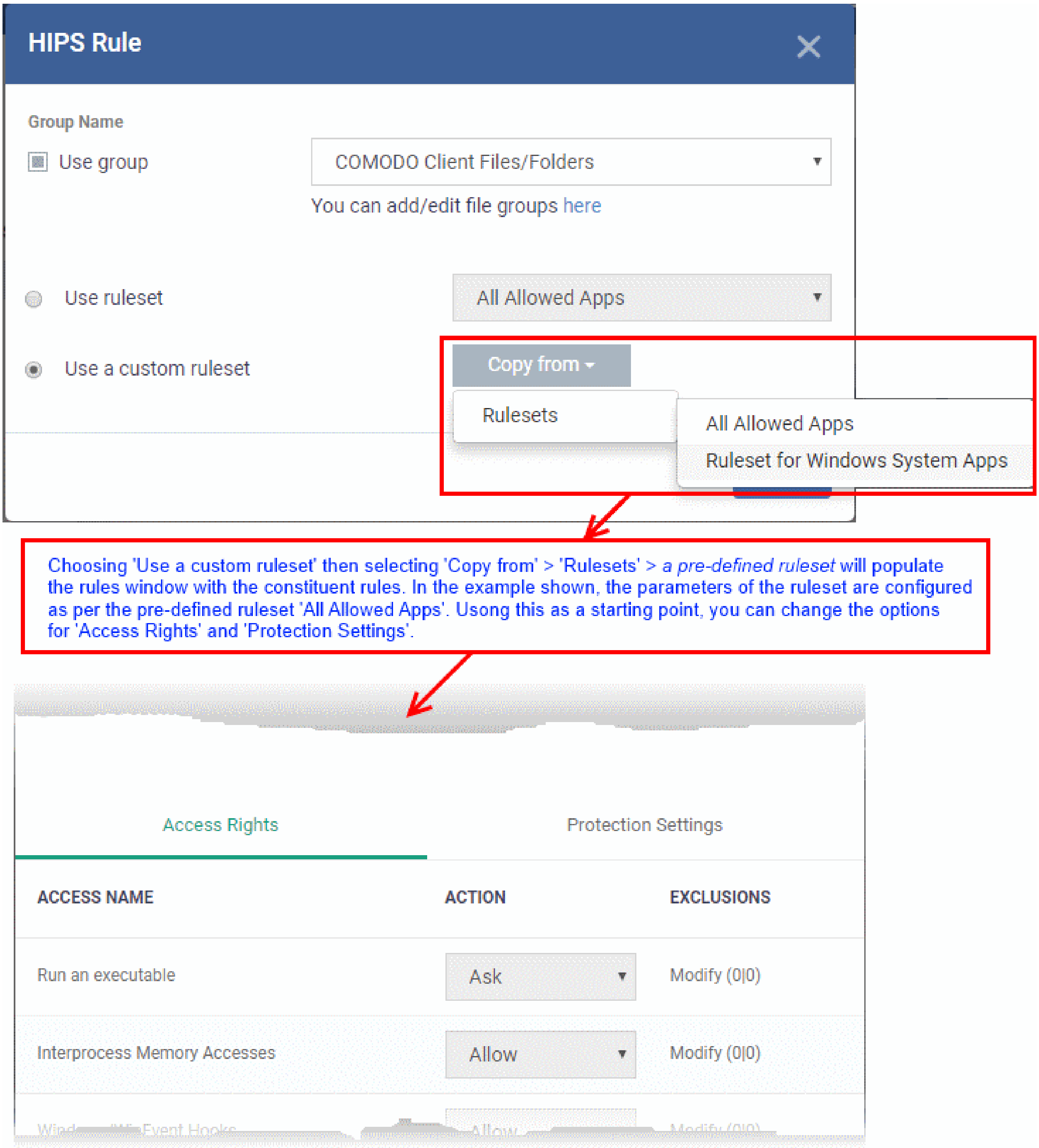
○ Use a custom ruleset

Selecting 'Use ruleset' and choosing a pre-defined ruleset from the drop-down will populate the rules from the ruleset for the application/group.

| ACCESS NAME | ACTION | EXCLUSIONS |
|---|---|---|
| Run an executable | Ask ▾ | Modify (0\|0) |
| Interprocess Memory Accesses | Allow ▾ | Modify (0\|0) |
| Windows/WinEvent Hooks | Allow | Modify (0\|0) |
| DNS Client Service | Allow ▾ | |
| Physical Memory | Allow ▾ | |
| Computer Monitor | Allow ▾ | |
| Disk | Allow ▾ | |
| Keyboard | Allow ▾ | |

**Note**: Predefined Rulesets, once chosen, cannot be modified ***directly*** from this interface - they can only be modified and defined using the **Ruleset** interface. If you require the ability to modify components of the rule set, then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset -** Designed for more experienced administrators, the 'Custom Ruleset' option grants full control over the configuration of each rule within that ruleset. The custom ruleset has two main configuration areas - Access Rights and Protection Settings. ***(Default = Enabled)***



HIPS Rule

Group Name

☒ Use group: COMODO Client Files/Folders ▾

You can add/edit file groups here

○ Use ruleset: All Allowed Apps ▾

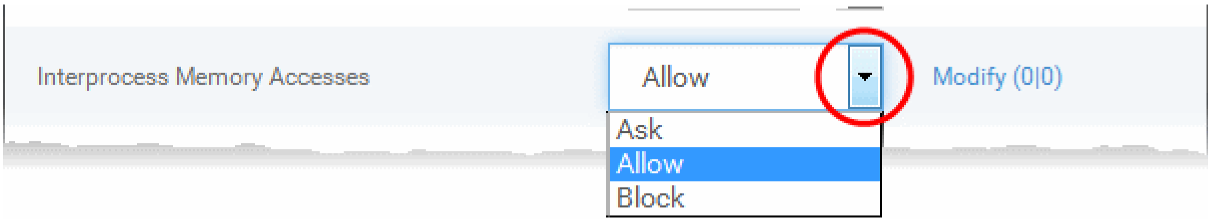
● Use a custom ruleset

Choosing 'Use a custom ruleset' then selecting 'Copy from' > 'Rulesets' > *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'. Usong this as a starting point, you can change the options for 'Access Rights' and 'Protection Settings'.

| ACCESS NAME | ACTION | EXCLUSIONS |
|---|---|---|
| Run an executable | Ask ▾ | Modify (0\|0) |
| Interprocess Memory Accesses | Allow ▾ | Modify (0\|0) |
| Wind... ...Win Event Hooks | Allow | Modify (0\|0) |

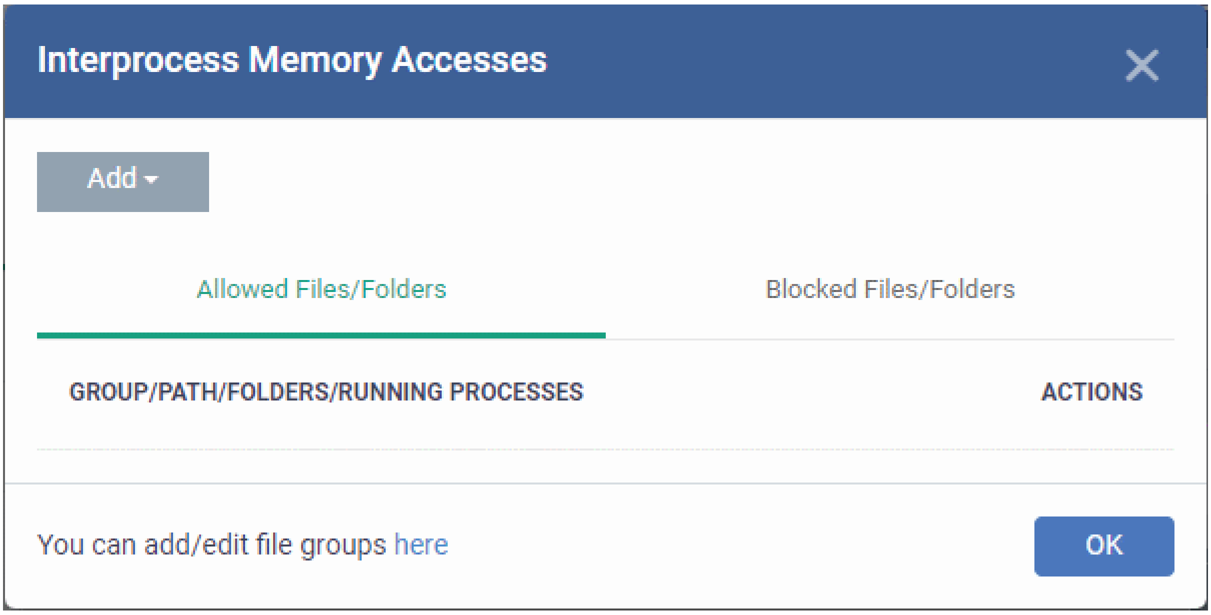
In simplistic terms 'Access Rights' determine what the application *can do to other processes and objects* whereas 'Protection Settings' determine what the application *can have done to it by other processes*.

i. **Access Rights -** The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset.



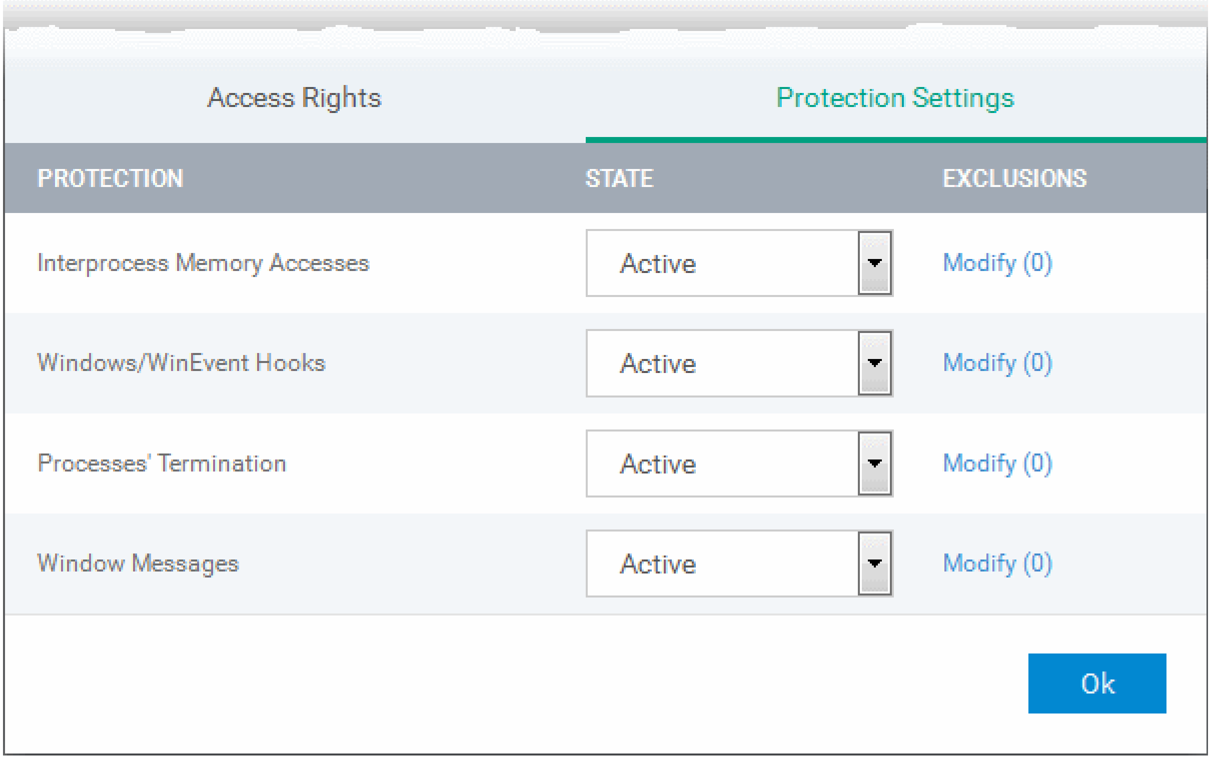
See **HIPS Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:

- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.


Interprocess Memory Accesses
Add
Allowed Files/Folders
Blocked Files/Folders
GROUP/PATH/FOLDERS/RUNNING PROCESSES
ACTIONS
You can add/edit file groups here
OK

- Click the 'Add' button at the top to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



| PROTECTION | STATE | EXCLUSIONS |
|---|---|---|
| Interprocess Memory Accesses | Active | Modify (0) |
| Windows/WinEvent Hooks | Active | Modify (0) |
| Processes' Termination | Active | Modify (0) |
| Window Messages | Active | Modify (0) |

- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection State' column. Select 'Inactive' to disable such protection.

**Click here** to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

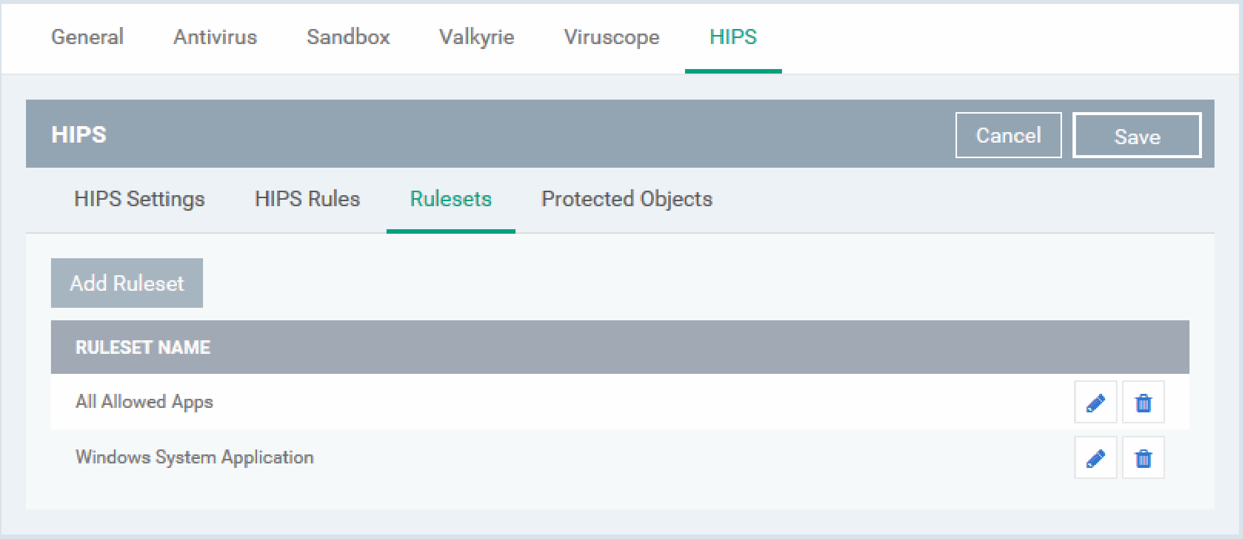
Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

5. Click 'OK' to confirm your settings.

## Rulesets

A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of rules and each of these rules is defined by a set of conditions/settings/parameters. Rulesets concern an application's access rights to memory, other programs, the registry etc.

The Rulesets screen under the the 'HIPS' tab displays the list of rulesets and allows you to add and manage new rulesets.

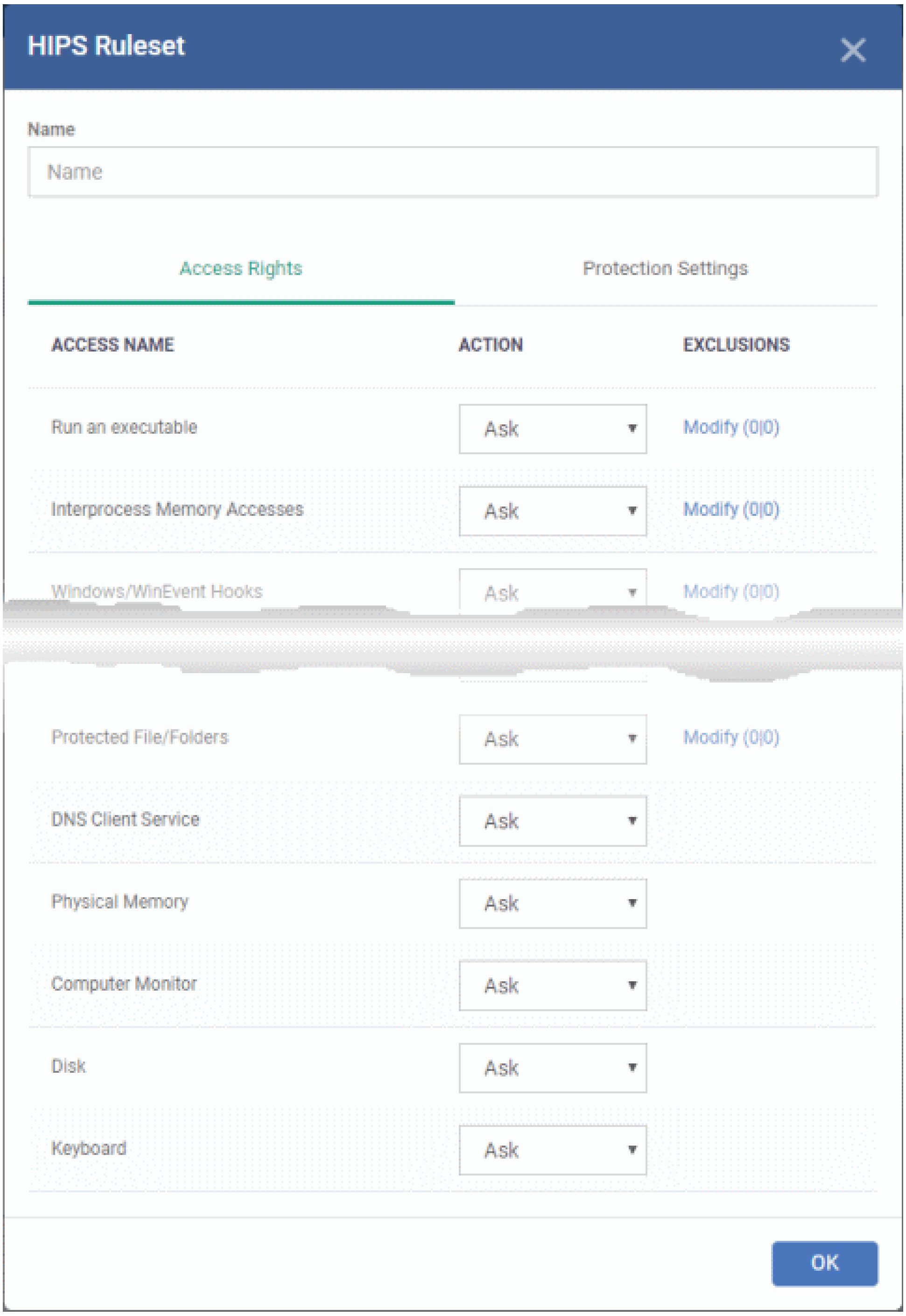


| RULESET NAME |
|---|
| All Allowed Apps |
| Windows System Application |

**Add a new ruleset**

- Click the 'Add Ruleset' button Add Ruleset above the list of rulesets.

The 'HIPS Ruleset' dialog will appear.



HIPS Ruleset

Name

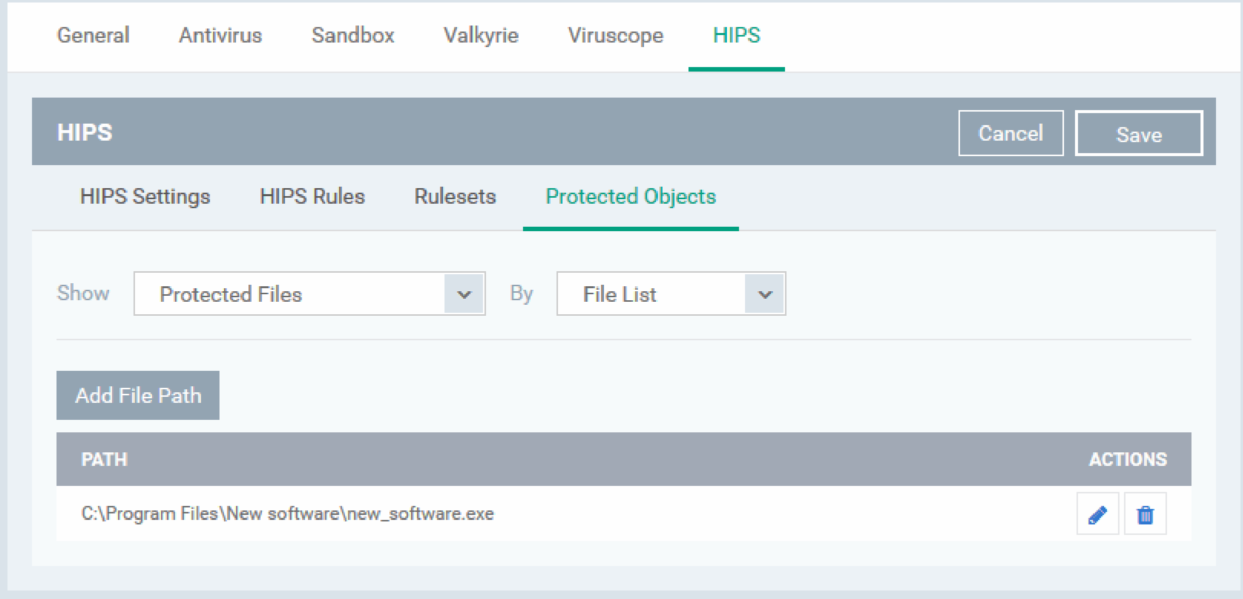
Name

| ACCESS NAME | ACTION | EXCLUSIONS |
|---|---|---|
| Run an executable | Ask | Modify (0\|0) |
| Interprocess Memory Accesses | Ask | Modify (0\|0) |
| Windows/WinEvent Hooks | Ask | Modify (0\|0) |
| Protected File/Folders | Ask | Modify (0\|0) |
| DNS Client Service | Ask | |
| Physical Memory | Ask | |
| Computer Monitor | Ask | |
| Disk | Ask | |
| Keyboard | Ask | |

- Enter a name for the ruleset
- Configure the Actions, states and exclusions for **'Access Rights' and 'Protection Settings'** as explained above. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset. The new ruleset will be available for deployment to HIPS rule for applications/application groups from the HIPS Rules interface.
- To edit a ruleset, click the Edit button under the Actions in the Rulesets interface. The Editing process is similar to the Ruleset creation process explained above.

## Protected Objects

The 'Protected Objects' panel under 'HIPS' tab lets you specify items at the managed computers to be protected against access or modification by unauthorized processes and services. These include files and folders, system critical registry keys and COM interfaces.



C:\Program Files\New software\new_software.exe

The 'Show' drop-down allows you to choose the category of protected objects to be displayed in the list and add and manage the protected objects of that category. You can add following categories of protected objects:

- **Protected Files** - Allows you to view and specify programs, applications, files an file groups that are to be protected from changes
- **Registry Keys** - Allows you to view and specify registry keys that are to be protected from changes
- **COM Interfaces** - Allows you to view and specify COM interfaces that are to be protected from changes

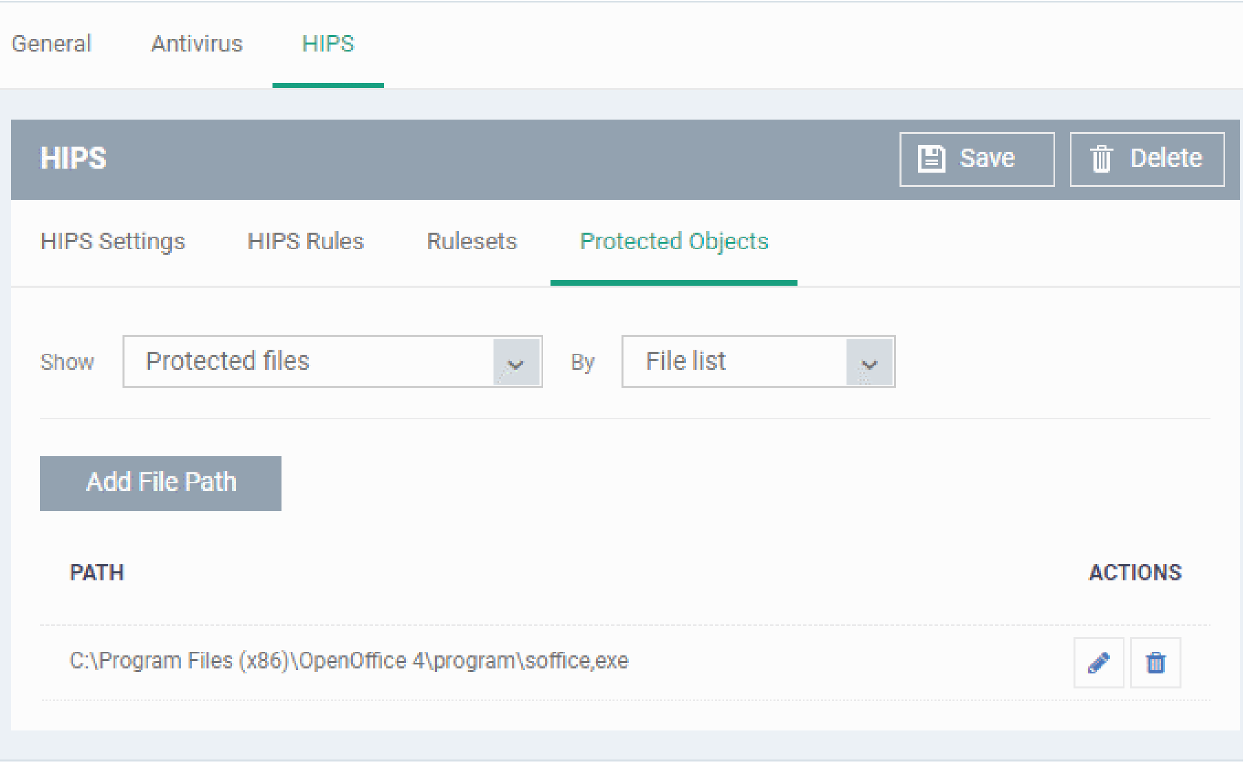
### Protected Files

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 any user and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Client Security blocks this attempt and produces a 'Protected File Access' pop-up alert.

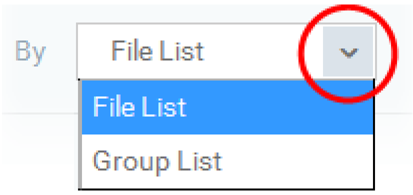
If you add a file to 'Protected Files', but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. See the explanation of **adding 'Exceptions' at the end of this section** for more details about how to allow access to files placed in Protected Files.

- To view the list of Protected Files, choose 'Protected Files' from the 'Show' drop-down in the 'Protected Objects' interface

The Protected File list is displayed under two categories, which can be selected from the drop-down at the right.



C:\Program Files (x86)\OpenOffice 4\program\soffice,exe

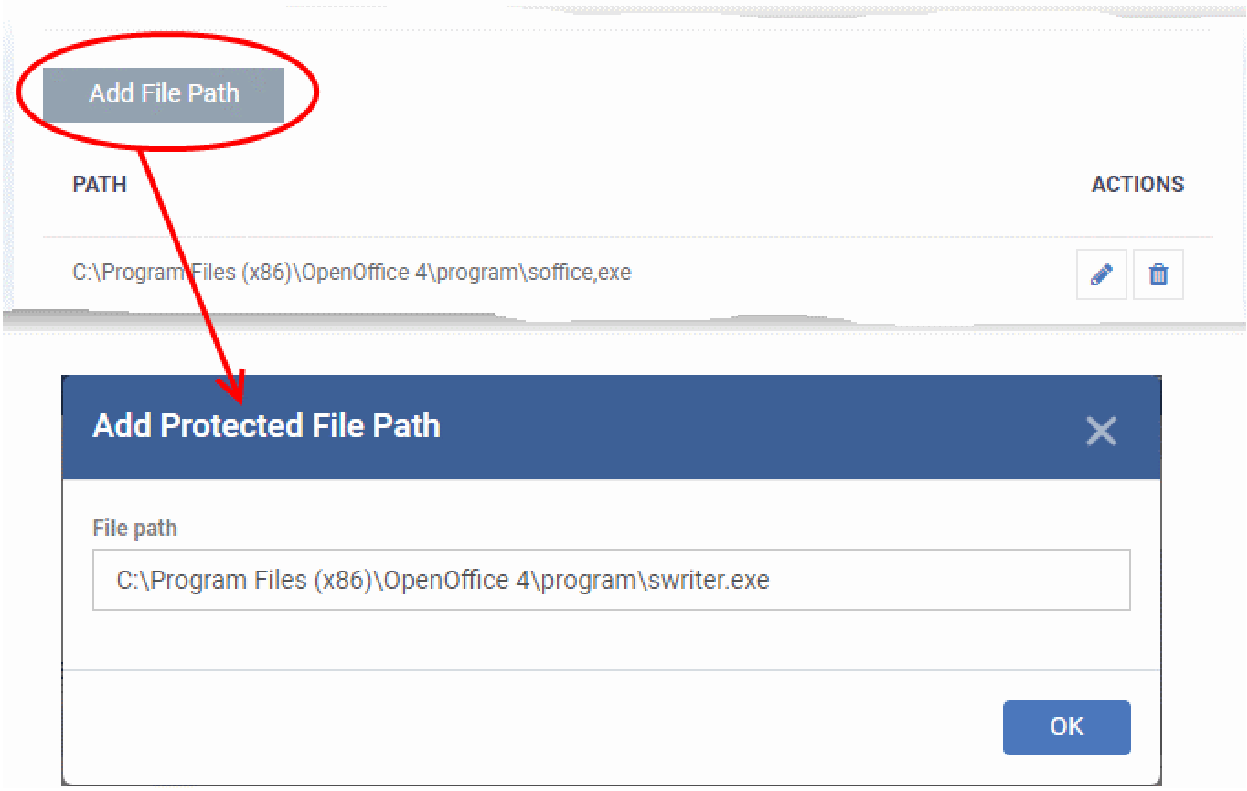


- To view the list of individual files, programs, applications added to the Protected Files list and manage them, choose 'File List'
- To view the File Groups added to the Protected File list, choose 'Group List'

You can add individual files, programs, applications or file/groups to 'Protected Files'.

**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.



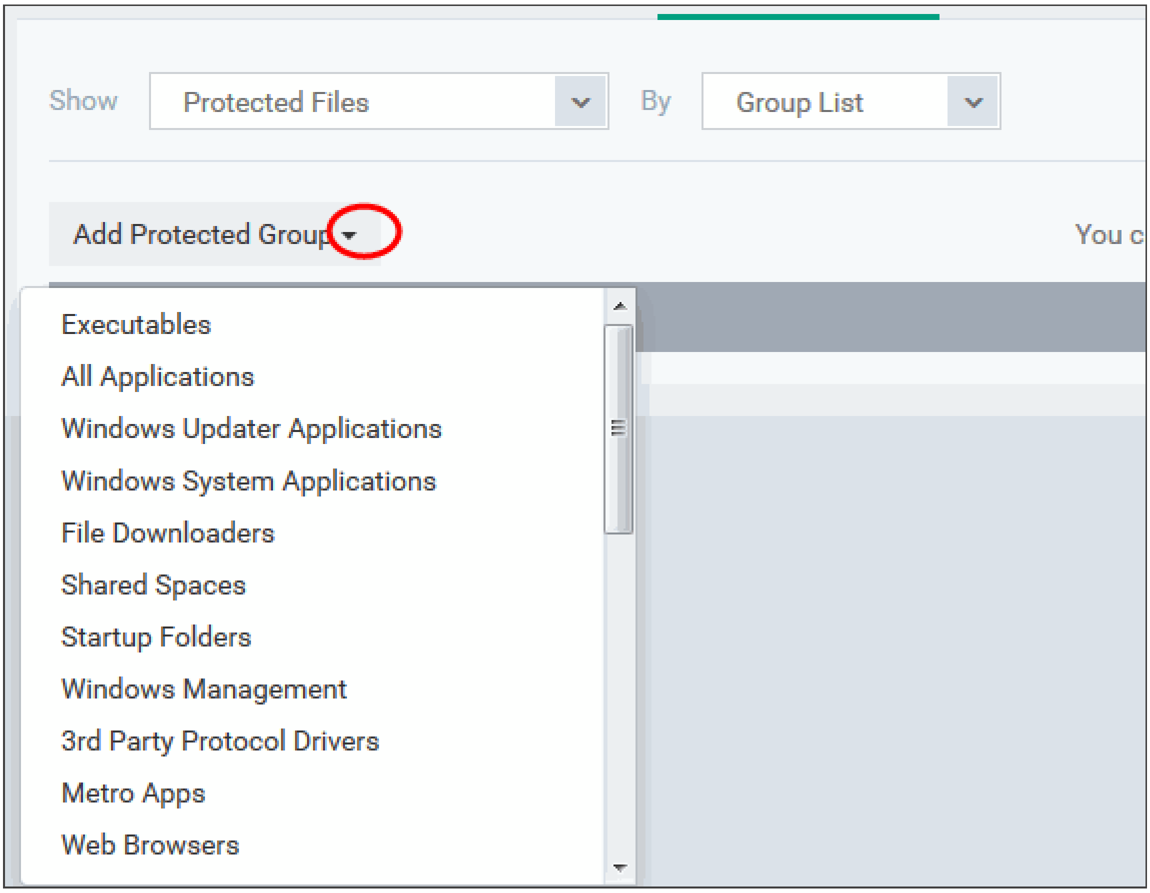
C:\Program Files (x86)\OpenOffice 4\program\soffice,exe

File path: C:\Program Files (x86)\OpenOffice 4\program\swriter.exe

- 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

**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'.

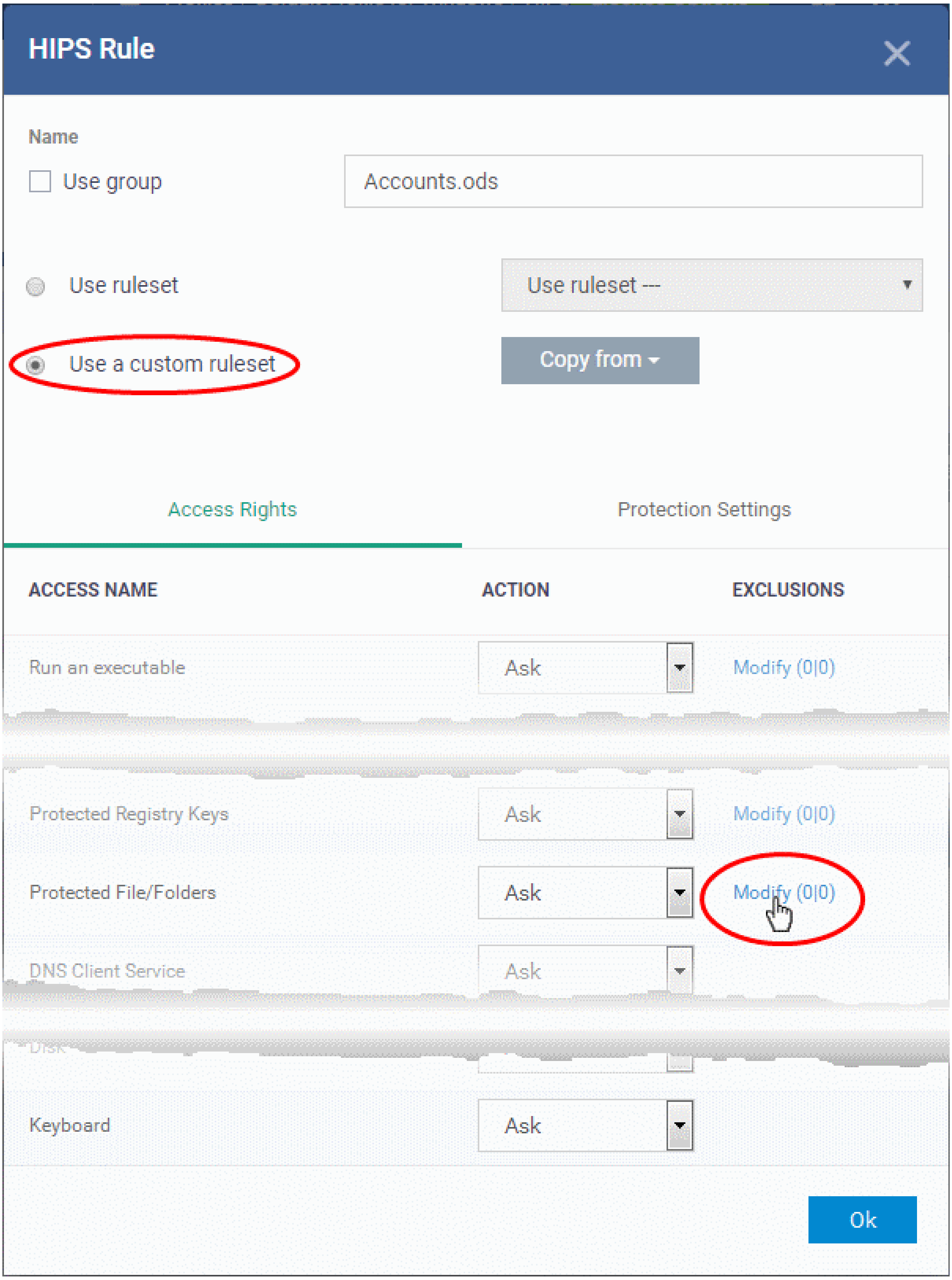
**Note**: Endpoint Manager ships with a set of predefined file groups containing collections of files under respective categories. You can also create custom file groups with required applications. All the pre-defined and the custom file groups will be available in the drop-down. The custom file groups can be created under 'Settings' > 'System Templates' > 'File Groups Variables' interface. See **Create and Manage File Groups** for more details.

- Repeat the process to add more file groups.
- To edit the path of an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

### Exceptions

You can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in '**HIPS Rules**' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the 'Open Office Calc' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first **add** the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**HIPS Rules**' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

- First add Accounts.ods to 'Protected Files' area as explained **above**.
- Then go to 'HIPS Rules' interface and add it to the list of applications.
- In the 'HIPS Rule' interface, enter the file name as Accounts.ods, choose 'Use a Custom Ruleset' and select a ruleset from the 'Copy From' drop-down.
- Under 'Access Rights' tab, set all the rules to 'Ask'



HIPS Rule

Name

□ Use group

Accounts.ods

○ Use ruleset

Use ruleset ---

● Use a custom ruleset

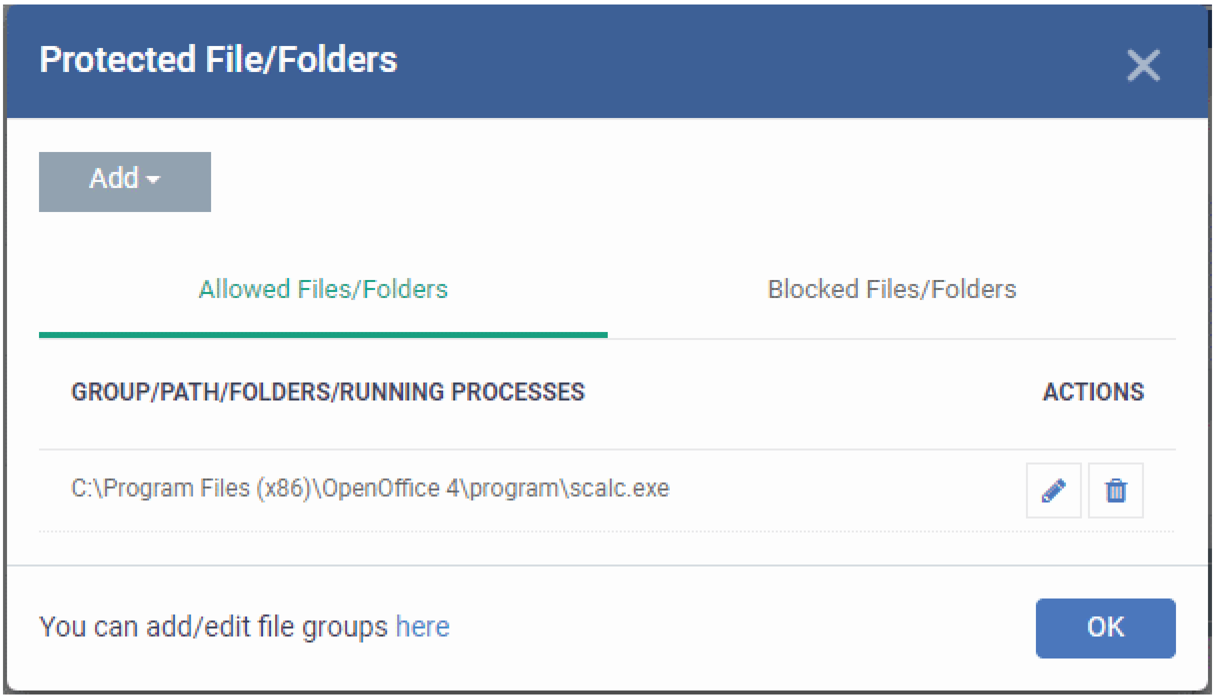
Copy from

| ACCESS NAME | ACTION | EXCLUSIONS |
|---|---|---|
| Run an executable | Ask | Modify (0\|0) |
| Protected Registry Keys | Ask | Modify (0\|0) |
| Protected File/Folders | Ask | Modify (0\|0) |
| DNS Client Service | Ask | |
| Disk | | |
| Keyboard | Ask | |

- Click the 'Modify' beside 'Protected File/Folders'
- Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'.

The 'Protected Files/Folders' interface will appear.

- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



C:\Program Files (x86)\OpenOffice 4\program\scalc.exe

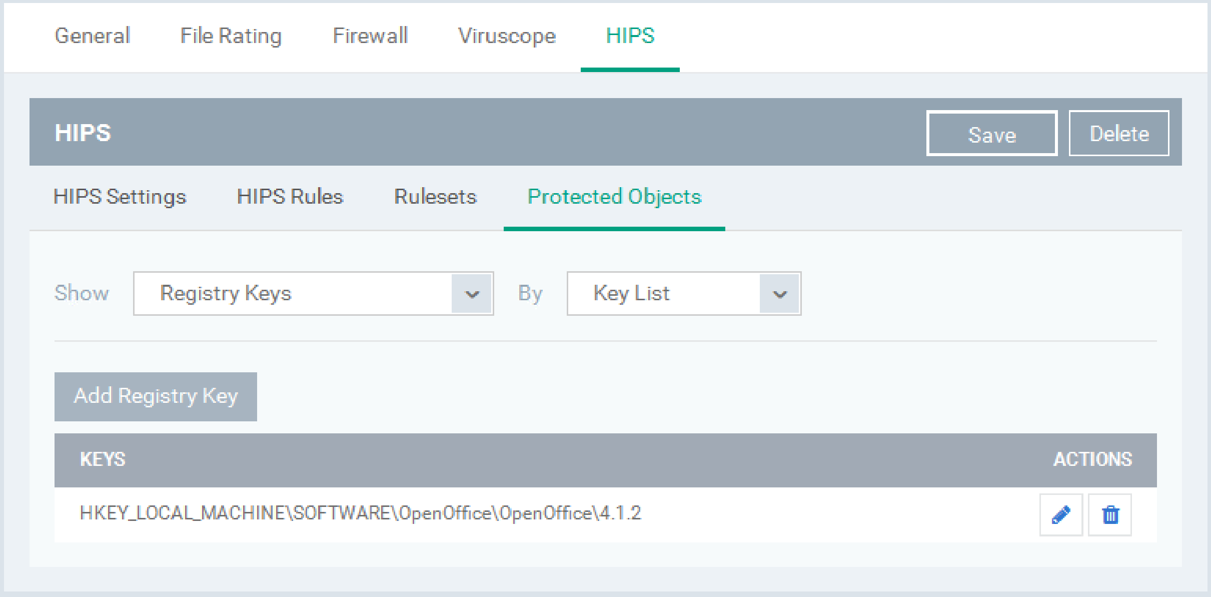
You can add/edit file groups here

Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32\* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

**Registry Keys**

The 'Registry Keys' list under 'Protected Objects' interface allows you to view and manage list of critical registry keys and registry groups to be protected against modification. Irreversible damage can be caused to the managed endpoint if important registry keys are corrupted or modified in any way. It is essential that the registry keys are protected against any type of attack.

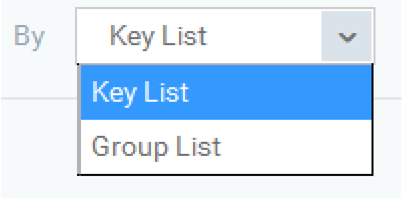
To view the list of Protected Registry Keys, choose 'Registry Keys' from the 'Show' drop-down in the 'Protected Objects' interface



Show: Registry Keys  By: Key List

HKEY_LOCAL_MACHINE\SOFTWARE\OpenOffice\OpenOffice\4.1.2

The Protected Registry Keys list is displayed under two categories, which can be selected from the drop-down at the right.

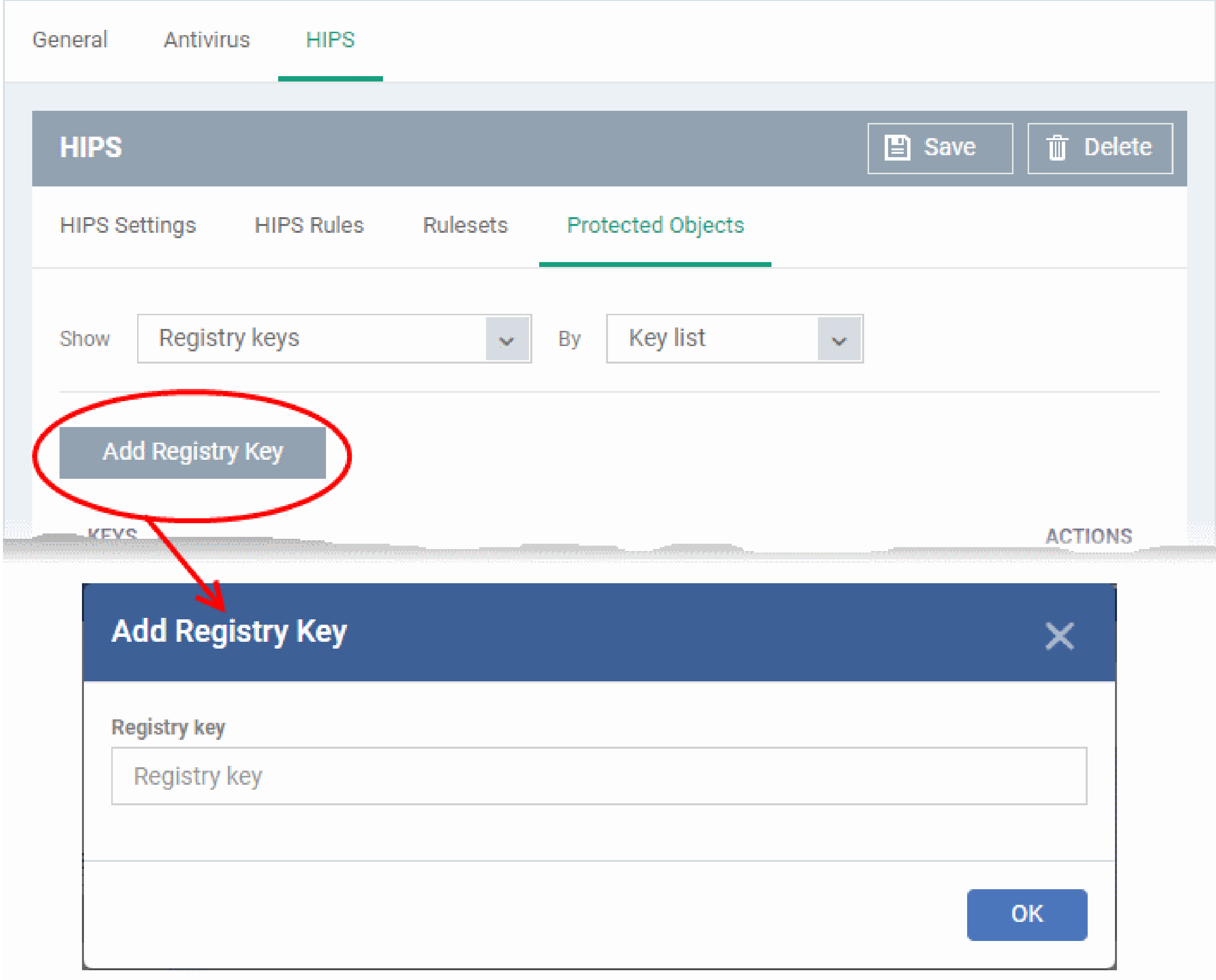


- To view the list of individual keys and values, and manage them, choose 'Key List'
- To view the Registry Groups, choose 'Group List'

You can add individual registry keys and Registry groups to Protected Registry Keys list.

**Add an individual key**

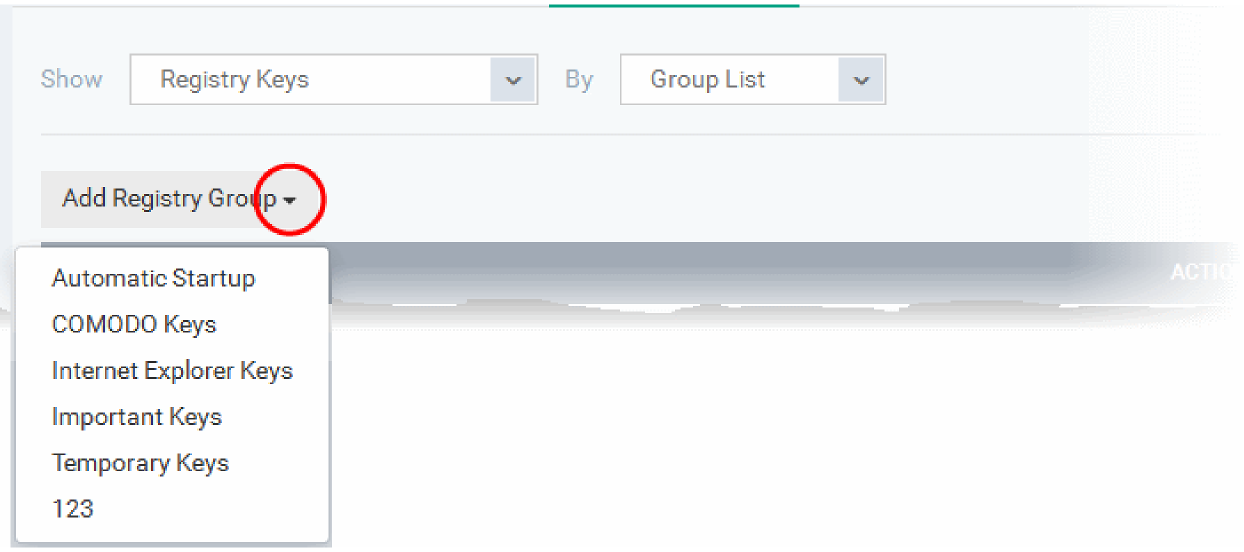
- Choose 'Key List' from the drop-down at the right and click the 'Add Registry Key' button.



- 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

**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**: Endpoint Manager ships with a set of predefined Registry groups containing collections of registry keys under respective categories. You can also create custom Registry groups with required key values. All the pre-defined and the custom Registry groups will be available in the drop-down. The custom Registry groups can be created under 'Settings' > 'System Templates' > 'Registry Variables' interface. See **Create and Manage Registry Groups** for more details.

- Repeat the process to add more Registry groups.
- To edit the an item in the list, click the Edit icon under the 'Actions' in the list.
- To remove an item from the list, click the trash can icon under 'Actions' in the list

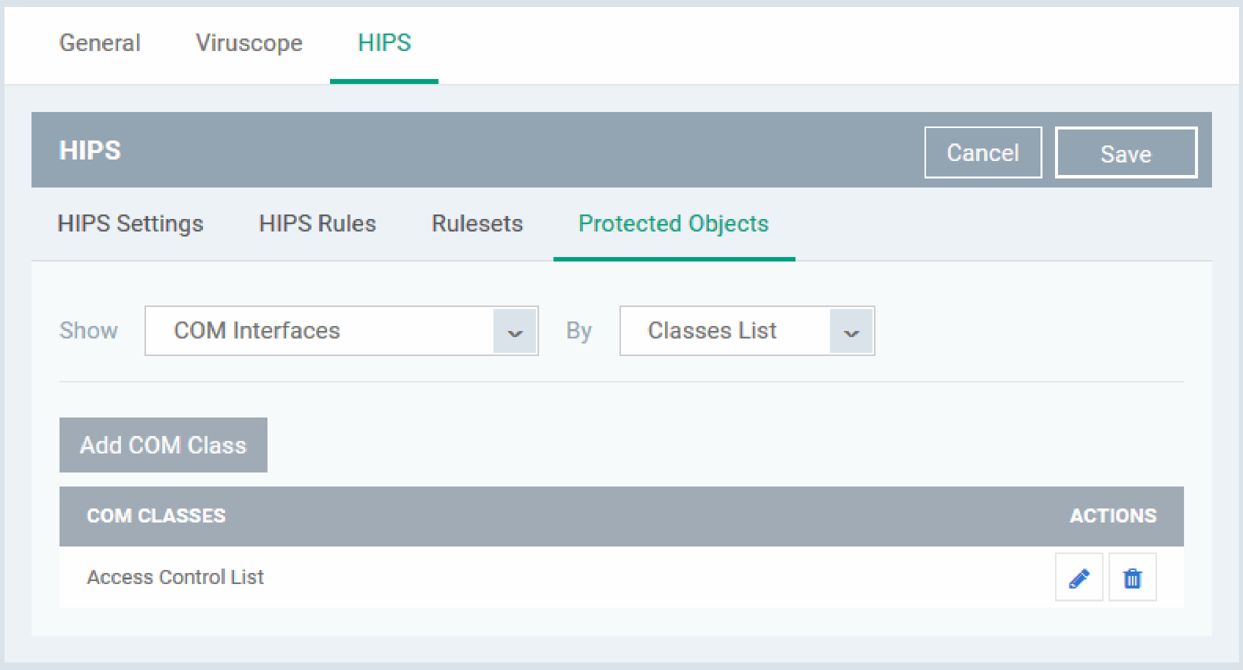
### COM Interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

The 'COM Interfaces' list under 'Protected Objects' interface allows you to view and manage list of individual COM classes and COM groups that are to be protected by the Comodo Client Security at the managed computer against modification, corruption and manipulation by malicious processes.

### View the list of Protected COM interfaces

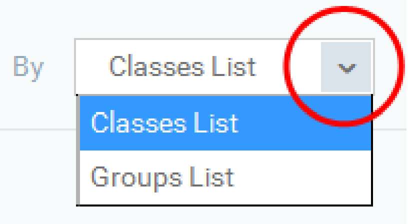
- Choose 'COM Interfaces' from the 'Show' drop-down in the 'Protected Objects' interface



Show: COM Interfaces
By: Classes List

| COM CLASSES | ACTIONS |
|---|---|
| Access Control List | |

The Protected COM Interfaces list is displayed under two categories, which can be selected from the drop-down at the right.

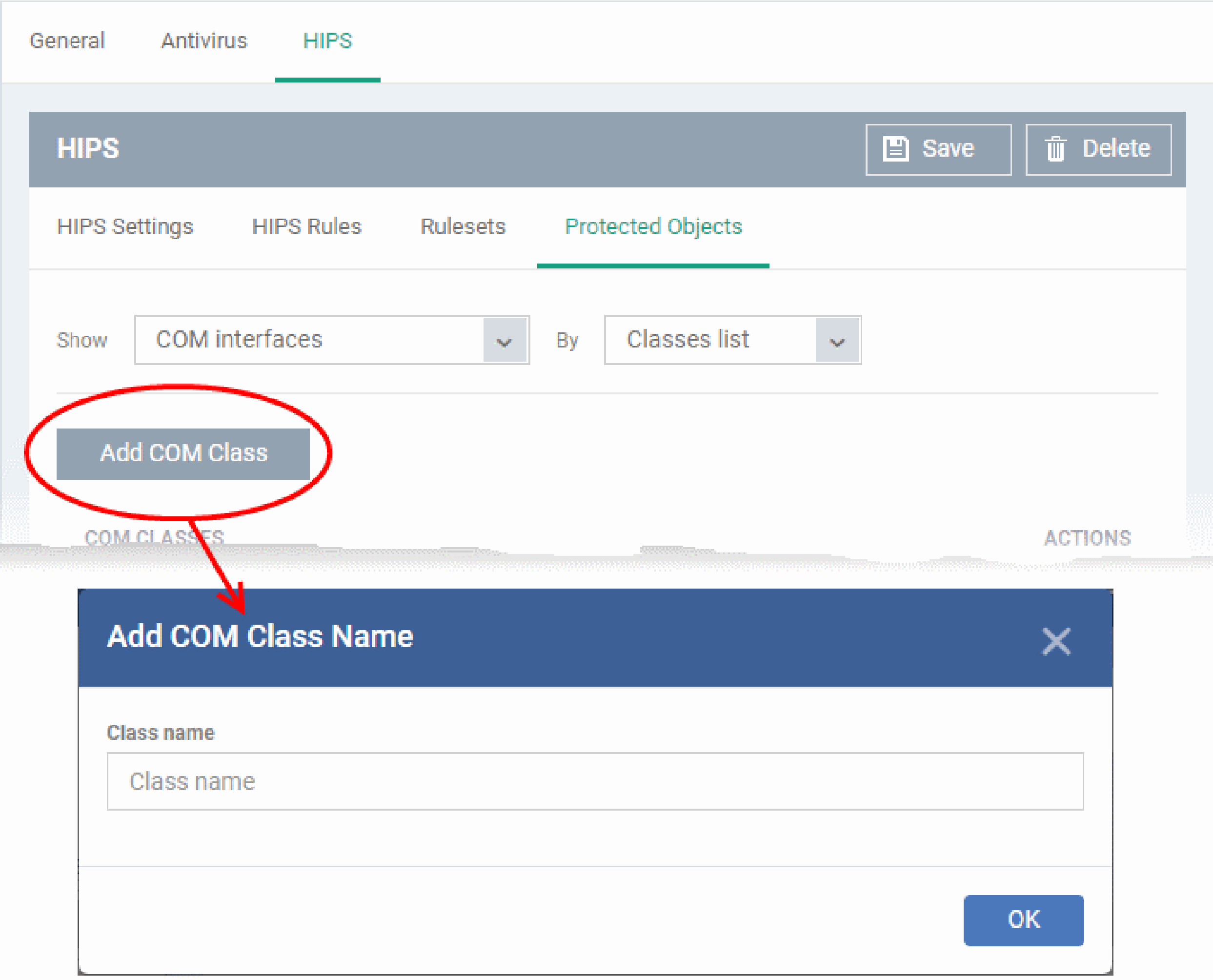


- To view the list of individual COM Interfaces/Classes and manage them, choose 'Classes List'
- To view the COM Groups and manage them, choose 'Group List'

You can add individual COM Interfaces/Classes and/or pre-defined COM groups to 'Protected COM Objects' list.

**Add an individual COM object**

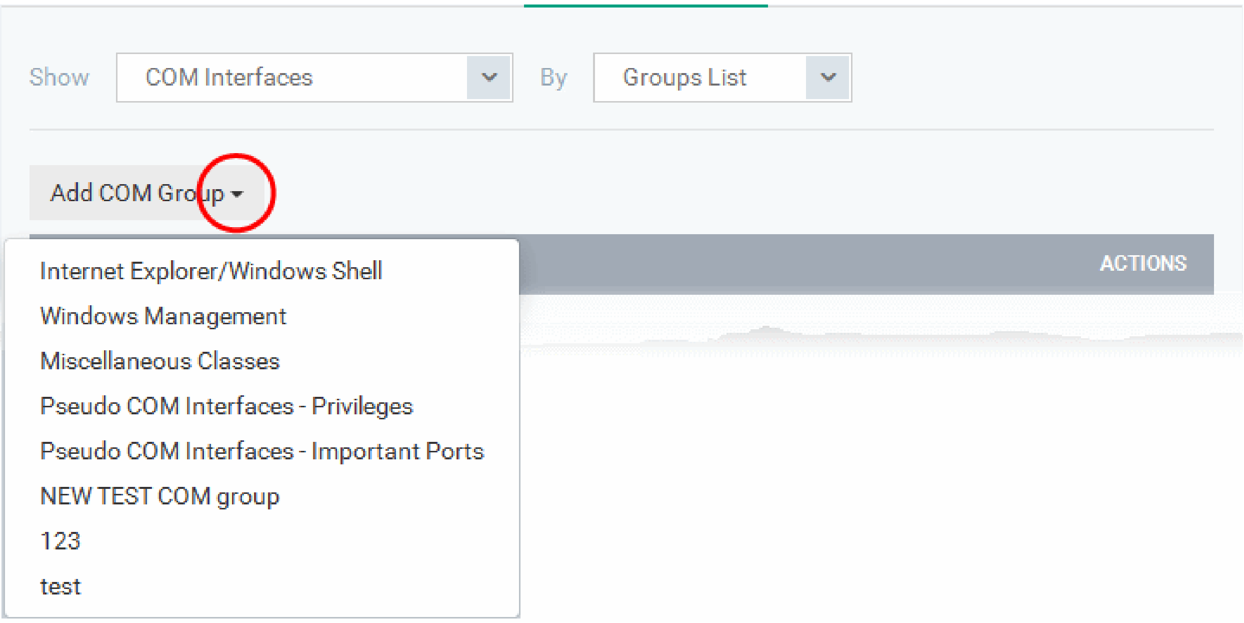
- Choose 'Classes List' from the drop-down at the right and click the 'Add COM Class' button



- 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

**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**: Endpoint Manager ships with a set of predefined COM groups containing collections of COM interfaces under respective categories. You can also create custom COM groups with required COM objects. All the pre-defined and the custom file groups will be available in the drop-down. The custom COM groups can be created under 'Settings' > 'System Templates' > 'COM Variables' interface. See **Create and Manage 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

### 6.1.3.1.6. Containment Settings

- Comodo Client Security (CCS) can be configured to run all unknown files in a security hardened environment known as the 'container'.
- Files in the container are prevented from causing damage because they are isolated from the OS, file system and user data.
- The containment settings area lets you configure the overall behavior of the containment component and the virtual desktop.
- You can create rules to define what types of files should be contained and at what restriction level.

  Restriction levels include:

  - **Run Virtually**. The file is completely isolated from your operating system and files on your computer
  - **Run Restricted**. The file is contained but has limited access to operating system resources
  - **Block**. The file is completely prevented from running
  - **Ignore**. The file is run outside the container without restrictions

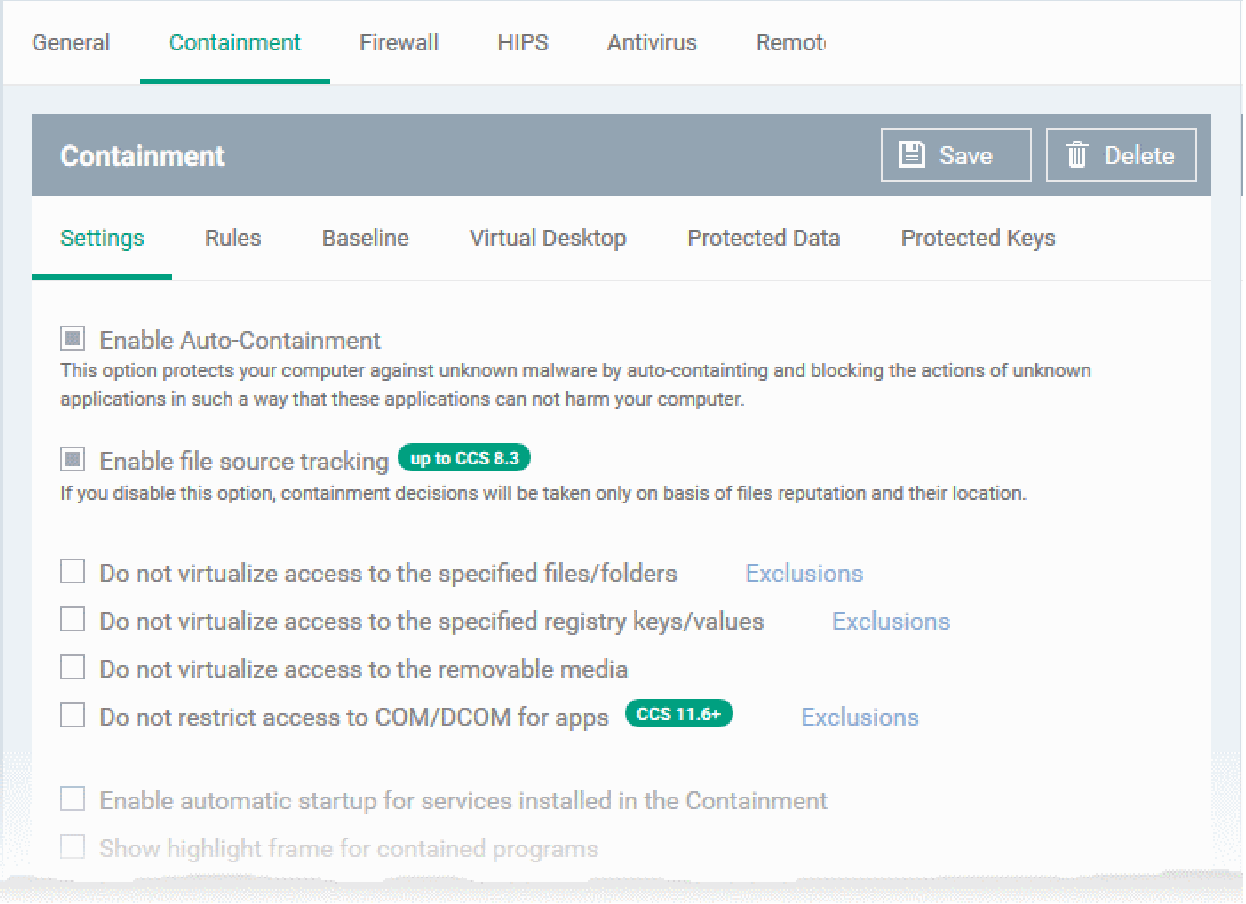
    See **Auto-Containment Rules** for more information about rules.
- You can also define files, folders and registry keys that programs in the container are blocked from accessing.
- The virtual desktop is separate, sandbox environment in which you can run Windows programs and internet browsers. Programs in the virtual desktop are isolated from the rest of the host, preventing them from potentially causing damage.

- Modifications to containment settings are automatically logged. You can view the old and new values in the 'Dashboard' > 'Audit Logs' screen. See '**Audit Logs**' in the '**Dashboard**' section for more information.

**Configure containment settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click 'Add Profile Section' > 'Containment'

The containment settings screen will open:



☑ Enable Auto-Containment
This option protects your computer against unknown malware by auto-containting and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

☑ Enable file source tracking
If you disable this option, containment decisions will be taken only on basis of files reputation and their location.

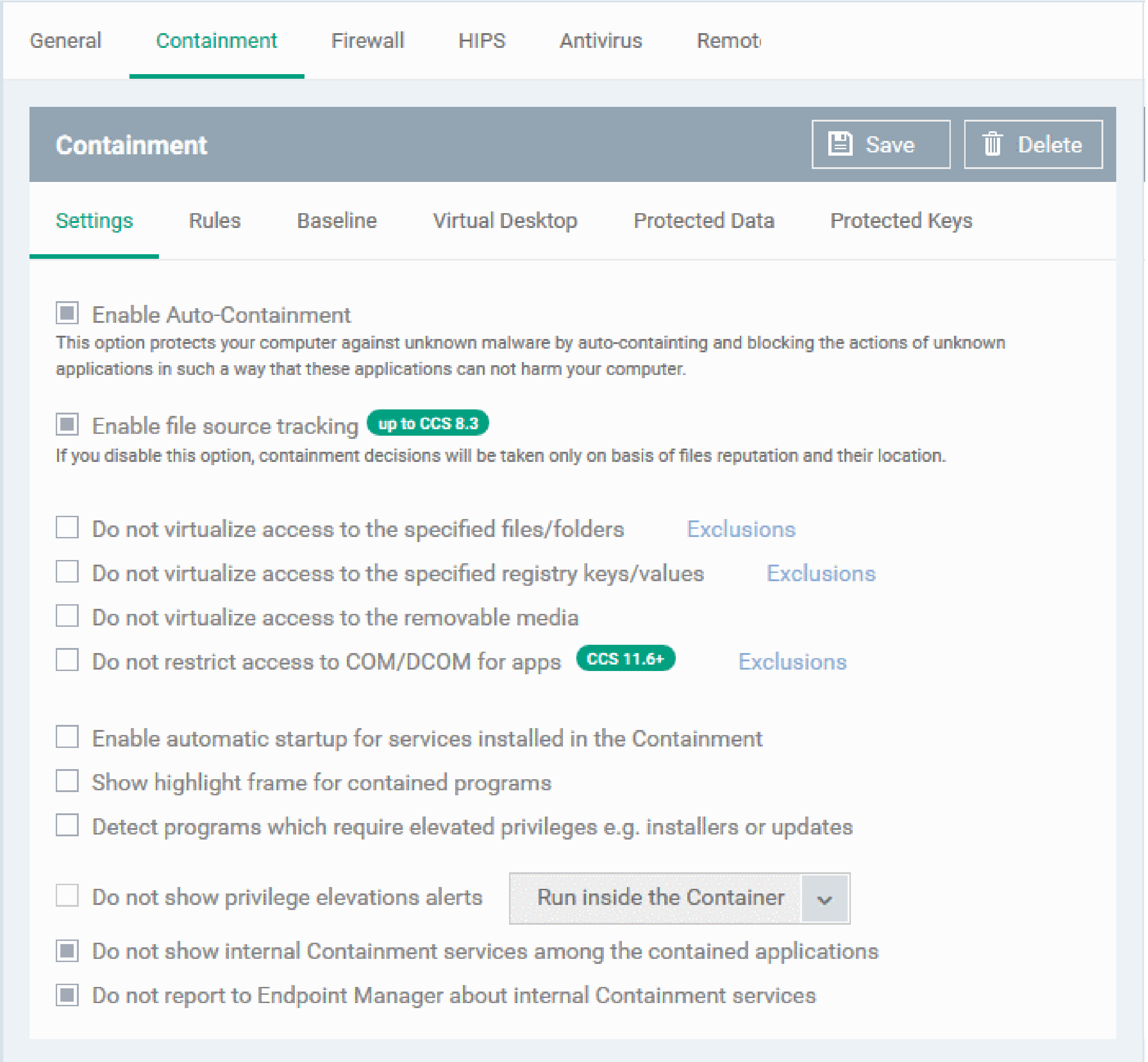
□ Do not virtualize access to the specified files/folders
□ Do not virtualize access to the specified registry keys/values
□ Do not virtualize access to the removable media
□ Do not restrict access to COM/DCOM for apps
□ Enable automatic startup for services installed in the Containment
□ Show highlight frame for contained programs

The containment section has four tabs:

- **Containment Settings**
- **Auto-Containment Rules**
- **Baseline Settings**
- **Virtual Desktop Settings**
- **Protected Data**
- **Protected Keys**

## Containment Settings

- Open the 'Containment' section of a profile
- Click the 'Settings' tab:



☑ Enable Auto-Containment
This option protects your computer against unknown malware by auto-containting and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

☑ Enable file source tracking up to CCS 8.3
If you disable this option, containment decisions will be taken only on basis of files reputation and their location.

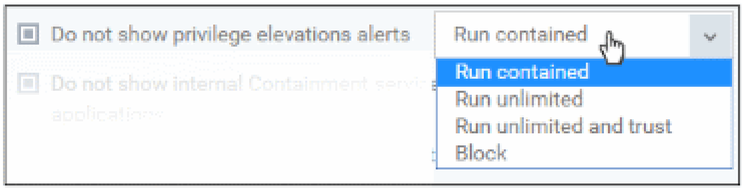
□ Do not virtualize access to the specified files/folders Exclusions
□ Do not virtualize access to the specified registry keys/values Exclusions
□ Do not virtualize access to the removable media
□ Do not restrict access to COM/DCOM for apps CCS 11.6+ Exclusions

□ Enable automatic startup for services installed in the Containment
□ Show highlight frame for contained programs
□ Detect programs which require elevated privileges e.g. installers or updates

□ Do not show privilege elevations alerts Run inside the Container
☑ Do not show internal Containment services among the contained applications
☑ Do not report to Endpoint Manager about internal Containment services

| Containment Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Auto-Containment | Activate or deactivate auto-containment on the endpoint. If enabled, CCS will automatically run unknown applications inside the container.<br>You can also create rules to fine-tune exactly which types of files are contained.<br>For more details on rules, see '**Configure Rules for Auto-Containment**'.<br>(***Default = Disabled***) |
| Enable file source tracking | If enabled, CCS will consider the origin of a file when deciding whether to contain it or not.<br>For example, if you only want to auto-contain files downloaded from the internet, then 'internet' is your source.<br>If this setting is disabled then the source is disregarded. Only the reputation and location of the file itself are considered.<br>• Applies only to CCS versions 8.3 or lower. |

| Containment Settings - Table of Parameters | |
|---|---|
| | (***Default = Disabled***) |
| Do not virtualize access to the specified files/folders | • Contained applications can access folders and files on the local system but cannot save any changes to them. However, you can define exceptions to this rule.<br>• (***Default = Disabled***)<br>• See **exclusions for files/tolders** (below this table) to find out how to add exclusions.<br><br>Note - This setting determines whether or not a contained application can access specific files/folders on your local system. It does not determine whether or not an application should run in the container in the first place. If you wish to exclude applications in their entirety from the container, see '**Configure Rules for Auto-Containment**' instead. |
| Do not virtualize access to the specified registry keys/values | • Contained applications can access registry keys and values on the local system but cannot save any changes to them.<br>• This setting lets you define exceptions to that rule. Contained applications will be able to access and save changes to registry items.<br>• Click the 'Exclusions' link to choose registry keys/values which contained files are allowed to modify.<br>(***Default = Disabled***)<br>See **exclusions for registry keys/values** (below this table) to find out how to add exclusions. |
| Do not virtualize access to the removable media | Allow contained applications to write to external storage devices like USB sticks and external hard disk drives. (***Default = Disabled***)<br><br>By default, applications in the container can only save data to a folder called 'Shared Space'. Users can save data to this folder if they want to access it from the host system.<br><br>This setting provides another way to export data from the container or virtual desktop. |
| Do not restrict access to COM/DCOM for apps | By default, contained applications cannot access the COM and DCOM components running on a Windows device.<br><br>This setting lets you specify applications that can access COM / DCOM components, even if the app is in the container.<br><br>(***Default = Disabled***)<br><br>See **Allow selected applications to access COM / DCOM components when run in container** to find out how to add applications. |
| Enable automatic startup for services installed in the Containment | By default, CCS does not permit contained services to run at Windows startup. Select this check-box to allow them to do so on target endpoints.<br>(***Default = Disabled***) |
| Show highlight frame for contained programs | Shows a green border around programs running in the container.<br>(***Default = Disabled***) |

| Containment Settings - Table of Parameters | |
|---|---|
| Detect programs which require elevated privileges e.g. installers or updates | CCS proactively tracks programs that require admin privileges to run.<br>A program that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry.<br>(***Default = Disabled***) |
| Do not show privilege elevation alerts | If 'Detect...' is enabled (see setting above) then an alert is shown to the end-user when a new or unrecognized program requires admin or elevated privileges to run. If you do not want these alerts to be shown, select this option and choose the action to be taken for unrecognized programs:<br><br>☑ Do not show privilege elevations alerts — Run contained<br>☑ Do not show internal Containment servi... applications<br>(***Default = Disabled***) |
| Do not show internal Containment services among the contained applications | Any processes started by CCC/CCS will not be shown in the 'Active Process List' in CCS.<br>You can view contained processes in CCS by clicking:<br>• Tasks' > 'General Tasks' > 'View Active Processes'<br>• Right-click anywhere in the interface > select 'Show Contained only'<br>(***Default = Enabled***) |
| Do not report to Endpoint Manager about internal Containment services | Info about Comodo client processes which are running in the container is not sent to Endpoint Manager. Client processes are those started by CCC or CCS themselves.<br>Click 'Security Sub-Systems' > 'Containment' in EM console to view a history of contained applications and processes.<br>(***Default = Enabled***) |

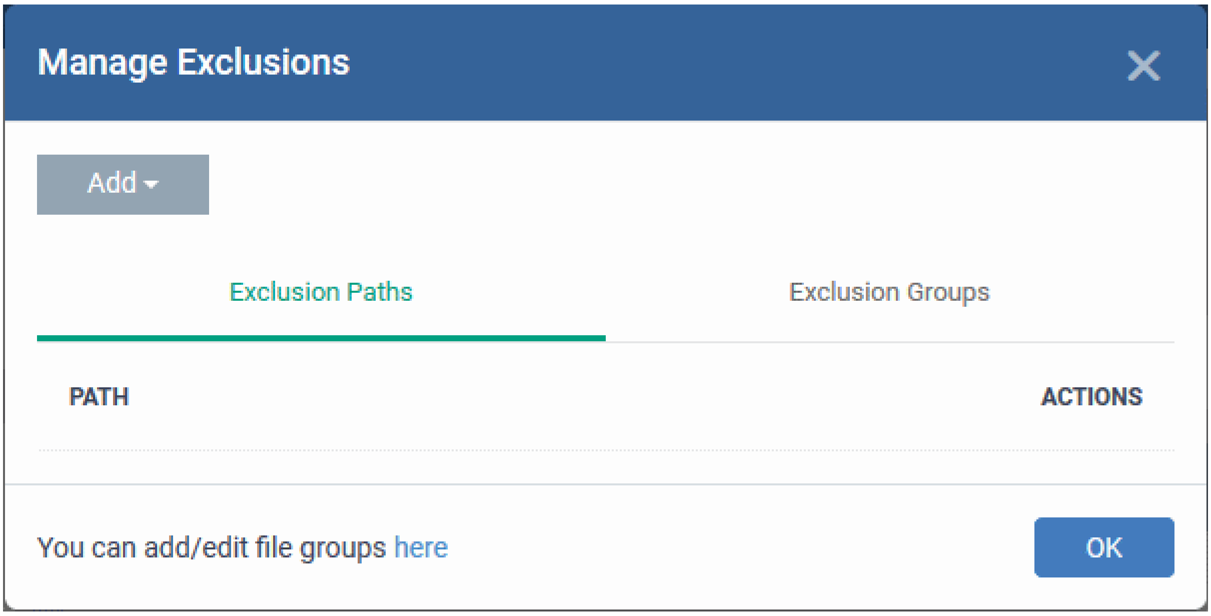
### Define exclusions for files and folders

**Note**. This section explains how to create an exclusion which allows an application in the container to access specific files and folders on the local system. If you want to entirely exclude an application from the container, then please see '**Configure Rules for Auto-Containment**' instead.

- Contained applications write to a virtual file system, preventing them from potentially damaging files on the host. This setting lets you define exceptions to that rule. You can specify folders or files on the host system which contained applications are allowed to access.

  Access scope if enabled:

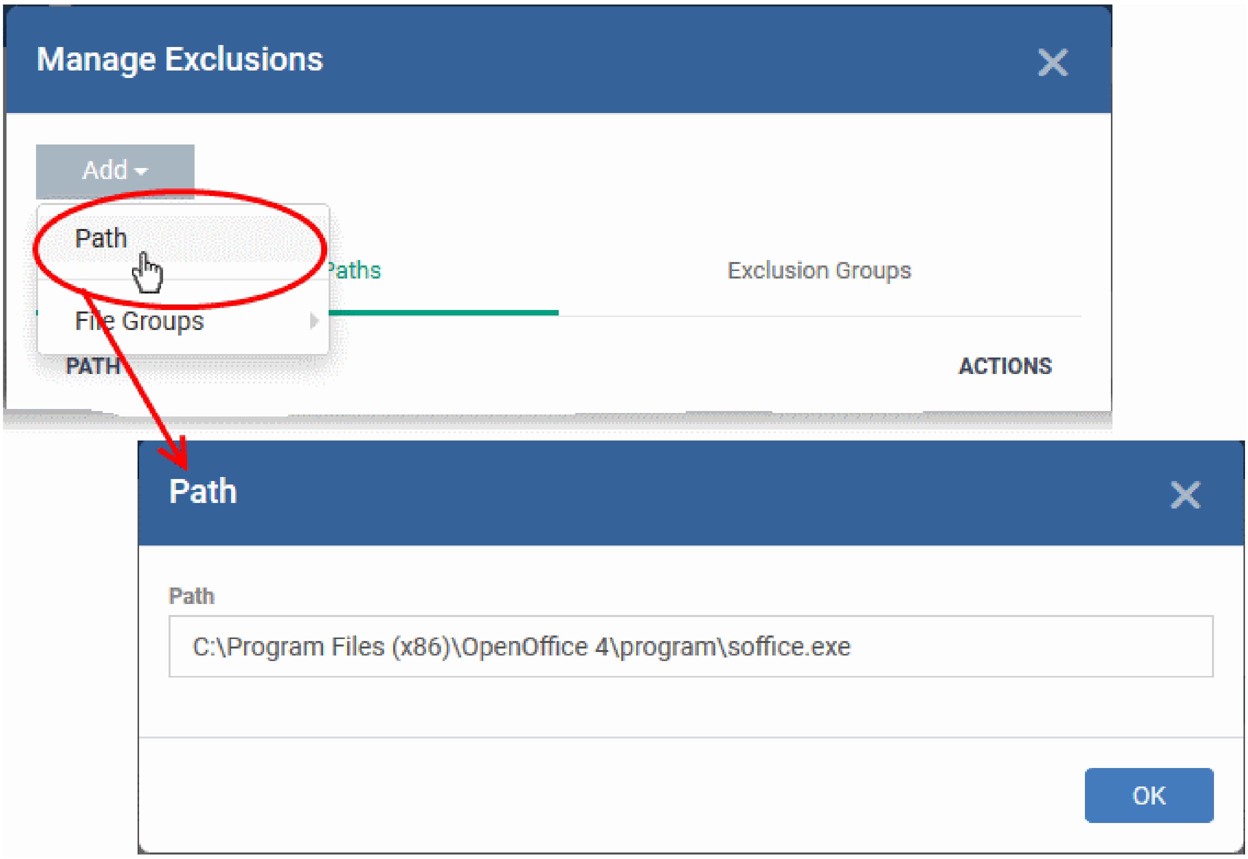
  - Data files (.doc, .txt etc) - Read/Write/Rename/Delete. Useful, for example, if you want MS Word in the container to save changes to a .doc file on the host file system.
  - Executable files (.exe, .msi etc) - Rename/Delete only.
- Enable 'Do not virtualize access to the specified files/folders', then click 'Exclusions':



Manage Exclusions

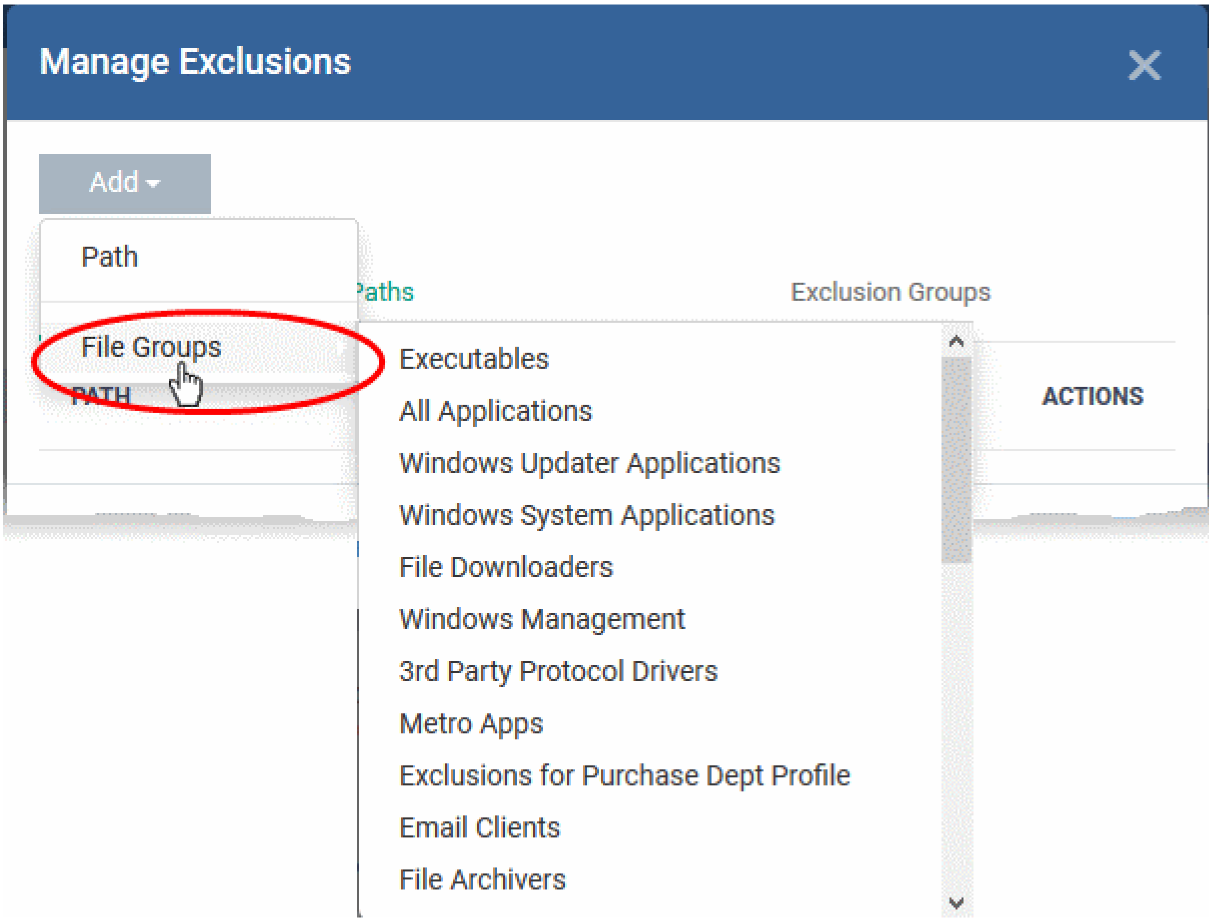
You can add/edit file groups here

- The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:
    - **Exclusion Paths -** Enter the location of an individual item that you want to exclude. Contained files can write to the files/folders you specify here. You can add multiple files by clicking 'Add' again.
    - **Exclusion Groups -** Allow contained apps to access apps and files in a particular group. A file group is a collection of file types which have similar attributes, scope, or functionality. For example, 'Executables', 'Metro Apps', or 'Windows System Applications'. Endpoint Manager ships with a set of pre-defined file groups. You can create custom file groups from the 'Settings' > 'System Templates' > 'File Groups Variables' interface. See **Create and Manage File Groups** for more details.
- Click 'Add' then 'Path' or 'File Group' as required:



Path

C:\Program Files (x86)\OpenOffice 4\program\soffice.exe

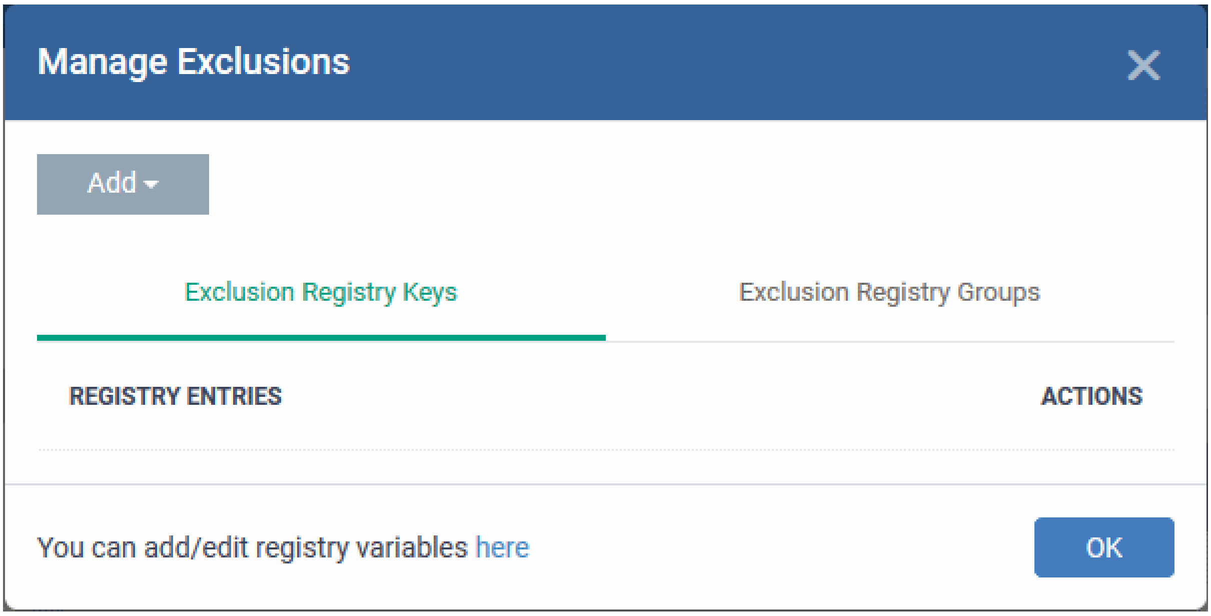


- Click 'OK' to save your settings.

- You can edit or remove the exclusions using the respective buttons in the 'Action' column in the File/Folders interface.

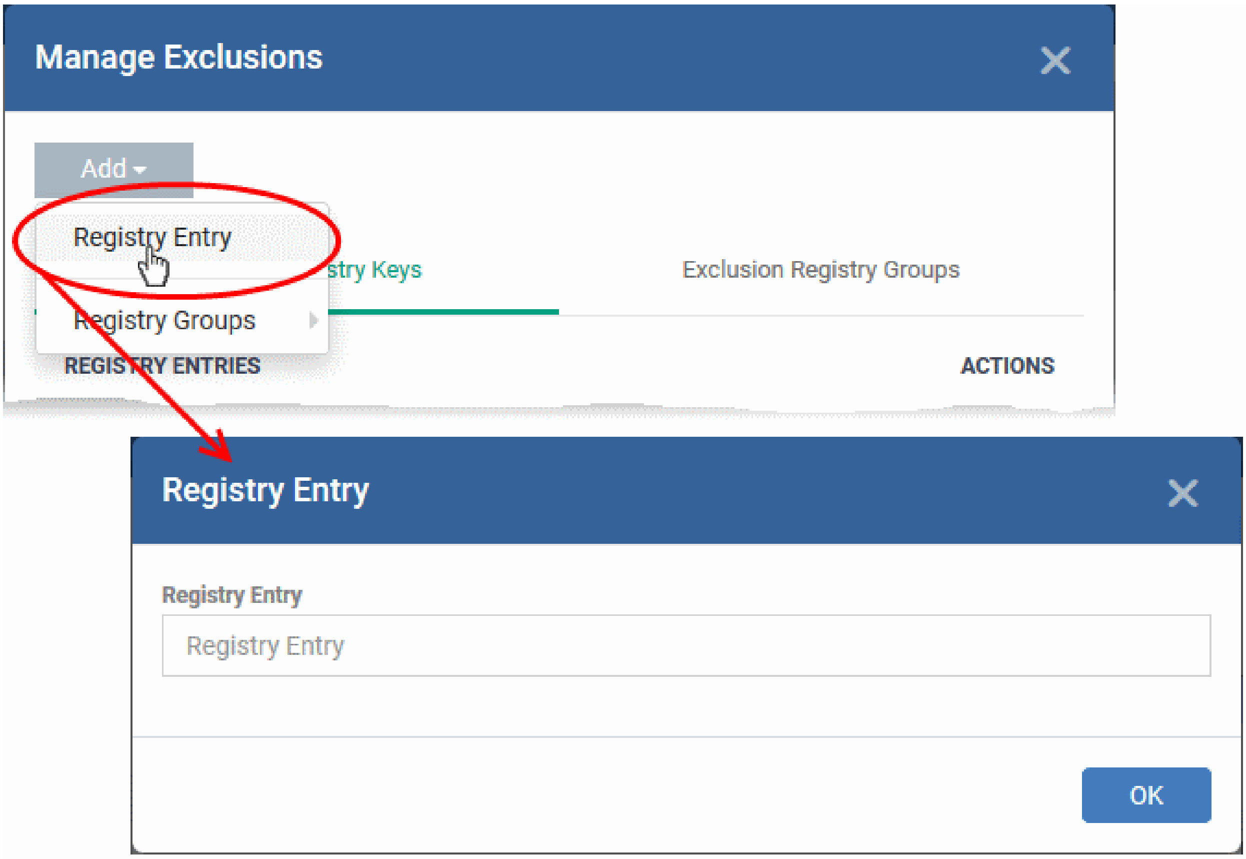
**Define exclusions for specific Registry keys and values**

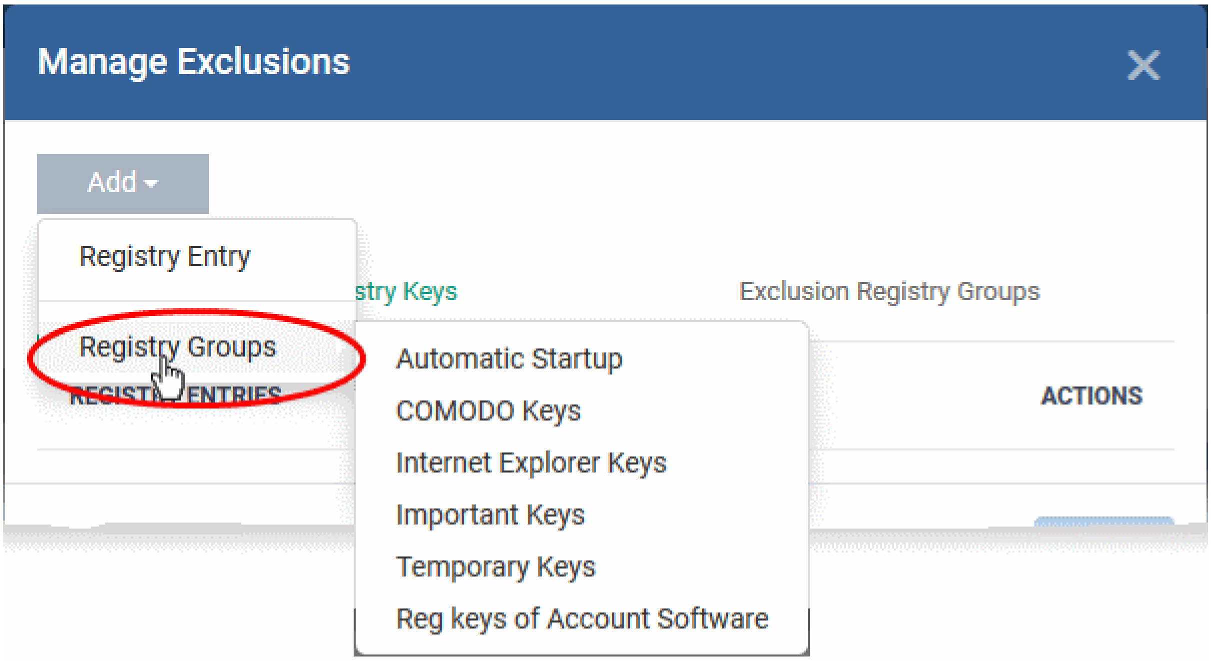
- Contained applications can access registry keys and values on the local system but cannot save any changes to them. This setting lets you define exceptions to that rule. Contained applications will be able to access and save changes to registry items.
- Enable 'Do not virtualize access to specified registry keys/values' and click 'Exclusions' beside it:



You can add/edit registry variables here

- **Exclusion Registry Keys -** Enter the location of an individual key that you want to exclude. Contained files can write to the keys you specify here. You can add multiple keys by clicking 'Add' again.
- **Exclusion Registry Groups -** Allow contained applications to access all keys in a particular group. A registry group is a collection keys with similar scope or functionality. Endpoint Manager ships with a set of registry groups. You can create custom registry groups from the 'Settings' > 'System Templates' > Registry Variables' interface. See **Create and Manage Registry Groups** for more details.
- Click 'Add' then 'Registry Entry' or 'Registry Group' as required:



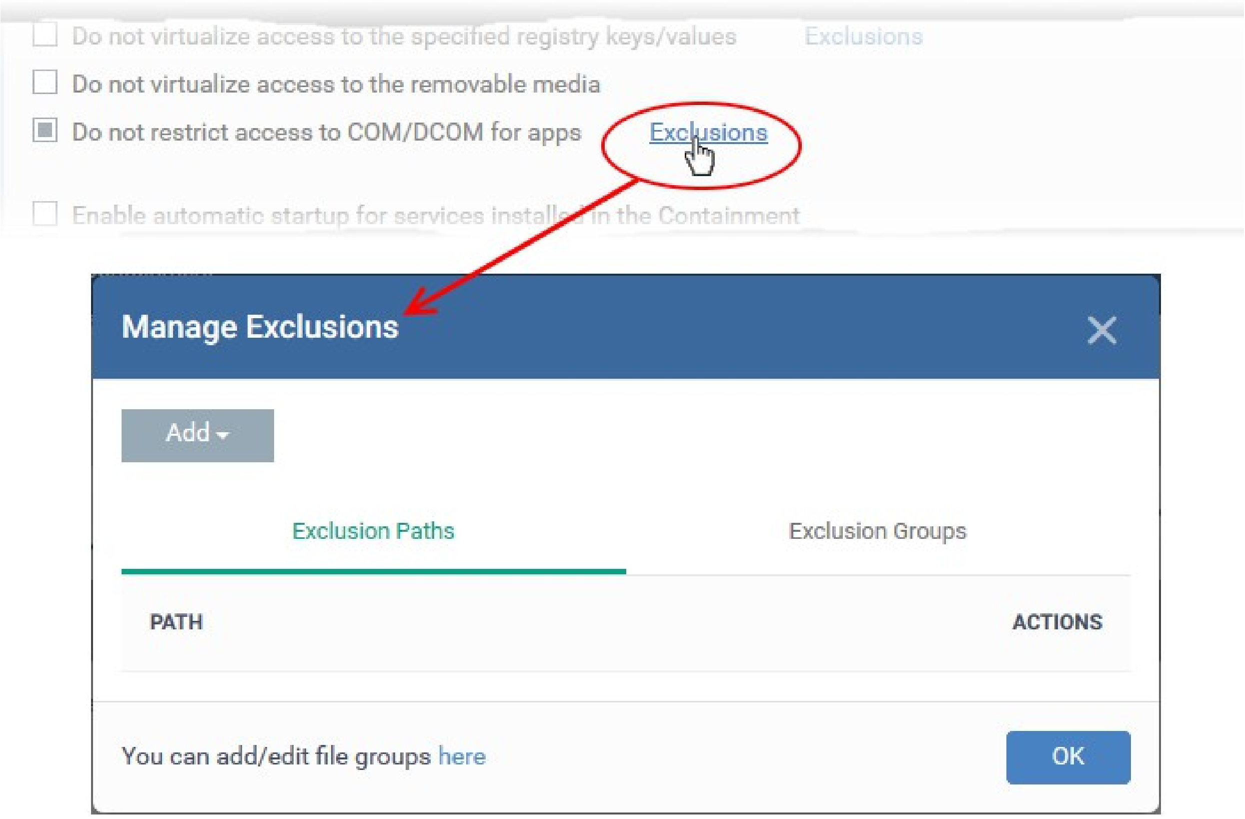


- Click 'OK' to save your settings.
- You can remove the exclusions using the trash can buttons in the 'Action' column in the 'Manage Exclusions' interface.

**Allow selected applications to access COM / DCOM components when run in container**

- 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.

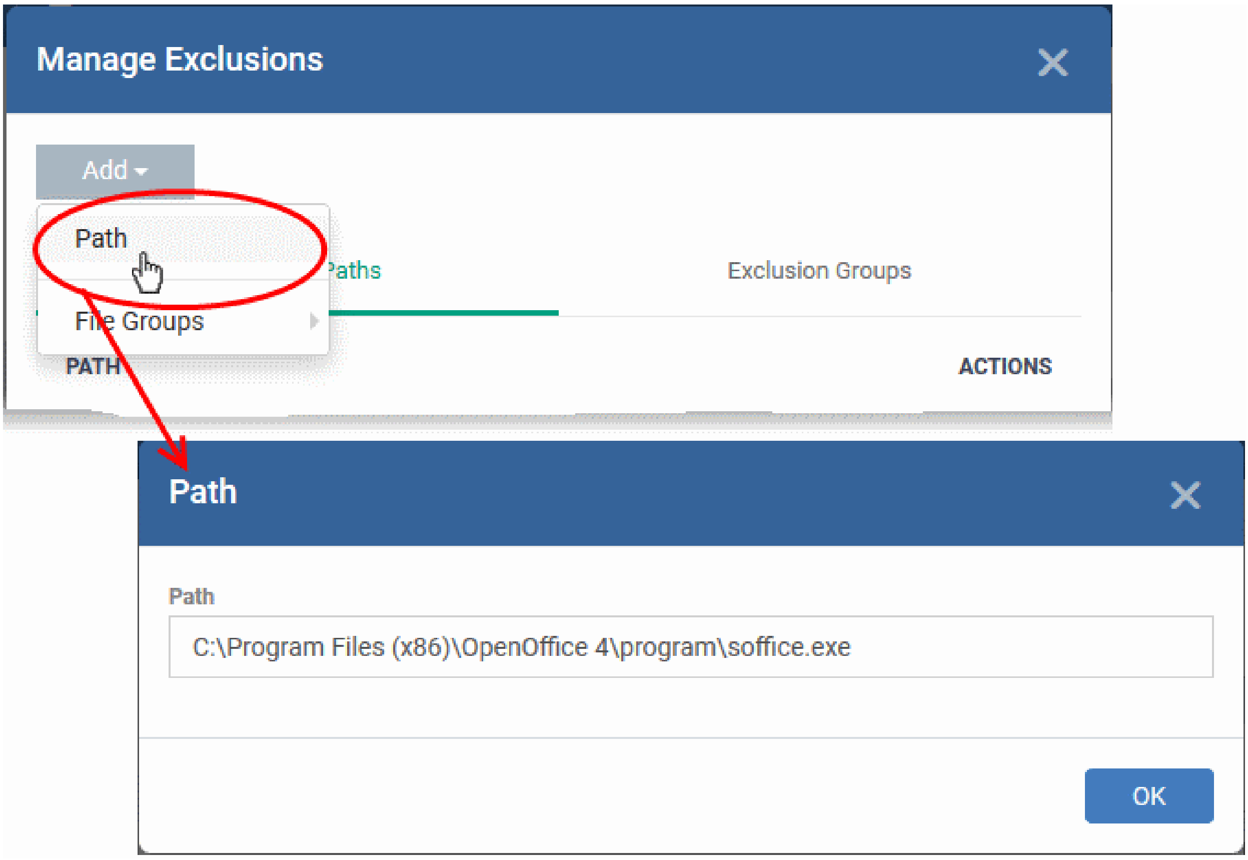
- By default, contained applications are prohibited from accessing the COM or Distributed COM (DCOM) components currently running on a device.
- If required, you can create a list of applications, that can access the COM and DCOM components, even if the application is run inside the container.
- Enable 'Do not restrict access to COM/DCOM for apps' and click 'Exclusions' beside it:



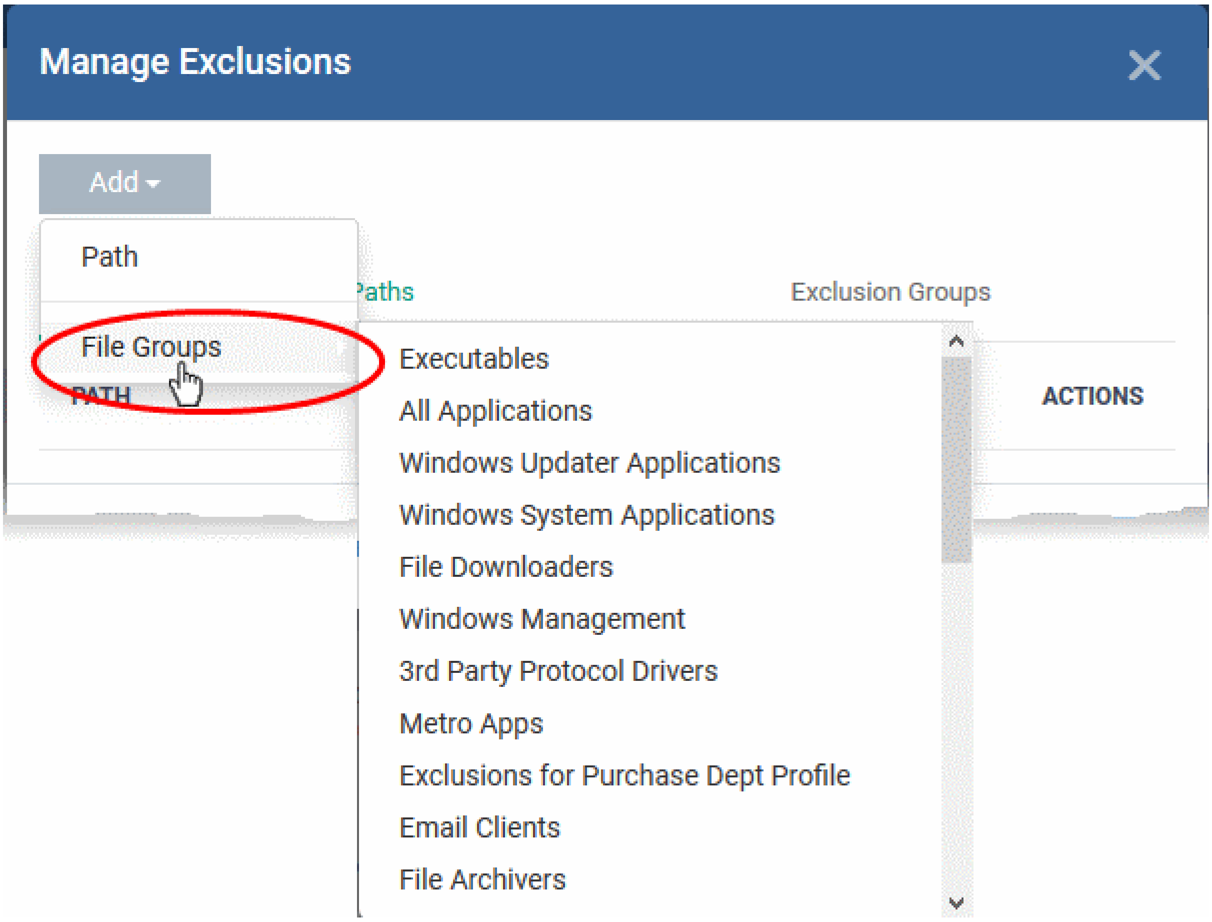
□ Do not virtualize access to the specified registry keys/values Exclusions
□ Do not virtualize access to the removable media
☑ Do not restrict access to COM/DCOM for apps Exclusions
□ Enable automatic startup for services installed in the Containment

You can add/edit file groups here

- The 'Manage Exclusions' dialog will appear with a list of defined exclusions under two tabs:
    - **Exclusion Paths** - Enter the location of an individual item that you want to add. The application you specify here can access COM / DCOM components, when run inside the containment.
    - **Exclusion Groups** - Allow applications in a particular group to access COM / DCOM interfaces. A file group is a collection of file types which have similar attributes, scope, or functionality. For example, 'Executables', 'Metro Apps', or 'Windows System Applications'. Endpoint Manager ships with a set of pre-defined file groups. You can create custom file groups from the 'Settings' > 'System Templates' > 'File Groups Variables' interface. See **Create and Manage File Groups** for more details.
- Click 'Add' then 'Path' or 'File Group' as required:



Path: C:\Program Files (x86)\OpenOffice 4\program\soffice.exe



- Click 'OK' to save your settings.

You can edit or remove the exclusions using the respective buttons in the 'Action' column in the Manage Exclusions interface.

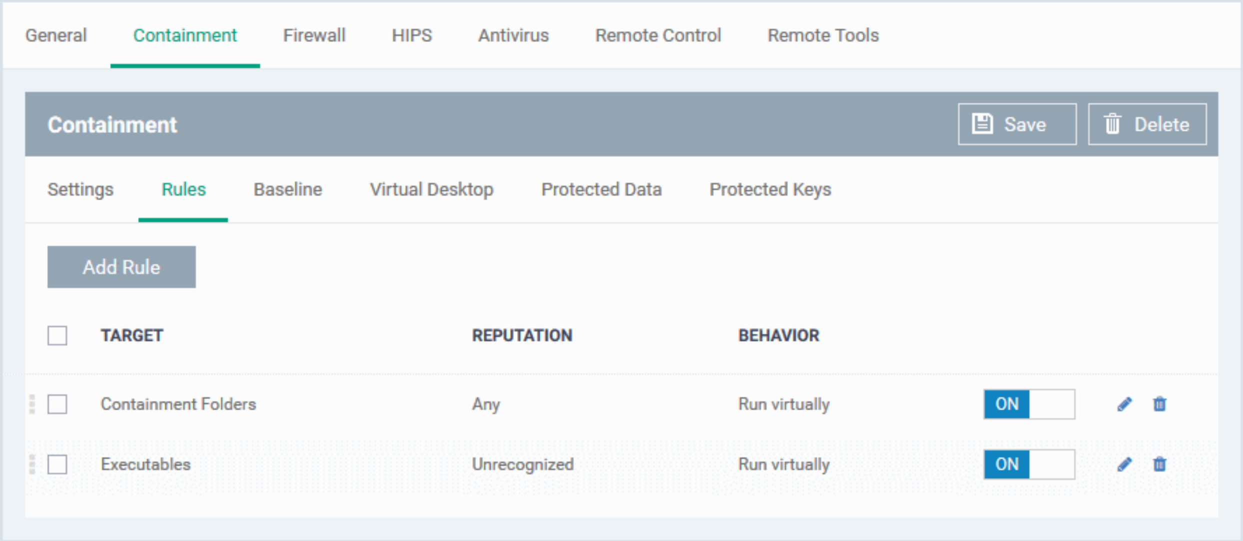
- Click the 'Save' button.

## Configure Auto-Containment Rules

- Containment rules determine whether a program should run as normal, run with restrictions, or run in the virtual environment. CCS consults these rules every time a program is opened on the endpoint.
- A contained application has much less opportunity to damage the endpoint because it is isolated from the operating system, system files and personal data.
- CCS shows a green border around contained programs if so configured in **containment settings**.

**Open the rules interface:**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you wish to work on
- Click the 'Containment' tab (click 'Add Profile Section' > 'Containment' if you haven't added it yet)
- Click the 'Rules' tab to view and manage auto-containment rules:



| □ | TARGET | REPUTATION | BEHAVIOR | |
|---|---|---|---|---|
| □ | Containment Folders | Any | Run virtually | ON |
| □ | Executables | Unrecognized | Run virtually | ON |

- The table lists all rules configured for the profile.
- Rules at the top of the table have a higher priority than those at the bottom. The setting in the rule nearer the top will prevail in the event of a conflict between rules.

| Containment Rules - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Target | The file, file group, or location on which the rule should run. |
| Reputation | The trust status of the files to which the rule should apply. The possible values are:<br>• 'Any'<br>• 'Malicious'<br>• 'Trusted'<br>• 'Unrecognized'. |
| Behavior | The action that will be taken on the targets if the rule criteria are met. Possible actions are:<br>• **Run virtually**. File is sandboxed inside a fully virtual environment. |

| | |
|---|---|
| | • **Run restricted**. File is sandboxed with limited access to device resources.<br>• **Block**. File is not allowed to run at all.<br>• **Ignore**. File is not sandboxed and is allowed to run on the host without restriction. |

- Use the slider to enable/disable a rule.
- Click the trash icon to remove a rule.
- Click the edit icon to modify a rule.

Target(s) can be filtered by numerous criteria. These are, however, optional, so admins can create a very simple rule to run an application in the container just by specifying the action and the target application.

Example:

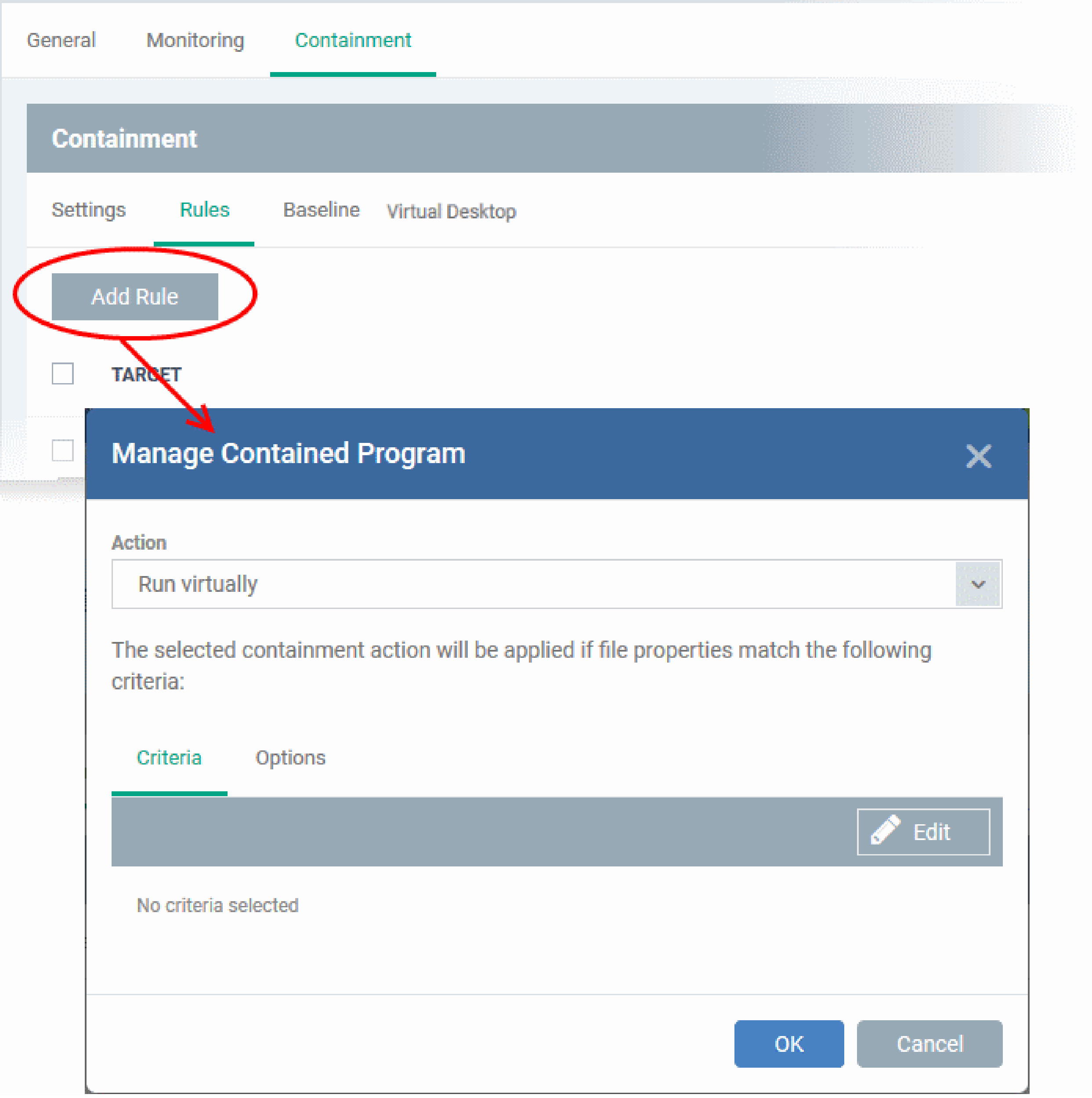
**Run an application outside the container**

- Open the containment tab and click 'Rules'
- Click 'Add Rule'
- Select 'Ignore' in the 'Action' drop-down
- Click 'Edit' in the 'Criteria' section to choose the application(s) you wish to exclude
- Choose the file, folder, file group or hash you want to exclude
- Click 'OK'
- Move the new rule to the top of the rules list (you can drag and drop rules)

### Add a new rule

- Open the profile you wish to add the rule to
- Click the 'Containment' tab. Click 'Add Profile Section' > 'Containment' if you haven't added it yet.
- Click the 'Rules' tab
- Click the 'Add Rule' button

- The 'Manage Contained Program' dialog will open:



The dialog shows the action at the top and contains two tabs:

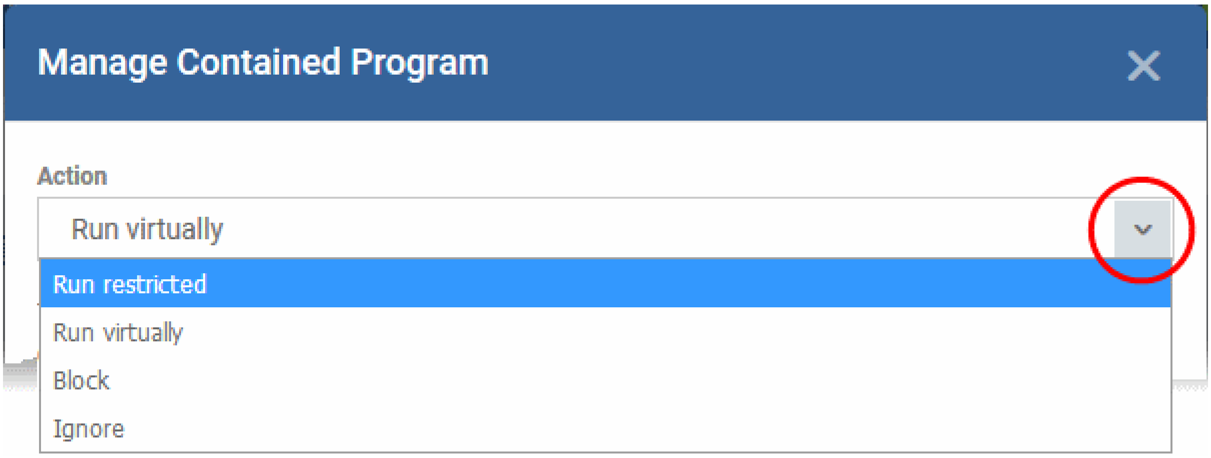
- Criteria - Define conditions upon which the rule should be applied.
- Options - Configure additional actions like logging, memory allowance and execution time restrictions.

Creating a new containment rule involves the following steps:

- **Step 1 - Choose the action**
- **Step 2 - Select the target file/group and set the filter criteria for the target files**
- **Step 3 - Select the options**

## Step 1 - Choose the action

- The setting in the 'Action' drop-down, and the restriction in the 'Options' tab, determine the privileges of an auto-contained application.



  - **Run Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
  - **Run Virtually -** The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
  - **Block -** The application is not allowed to run at all.
  - **Ignore -** The application will not be contained and allowed to run with all privileges.
- Choose the action from the options.

### Step 2 - Select the target file/group and set the filter criteria

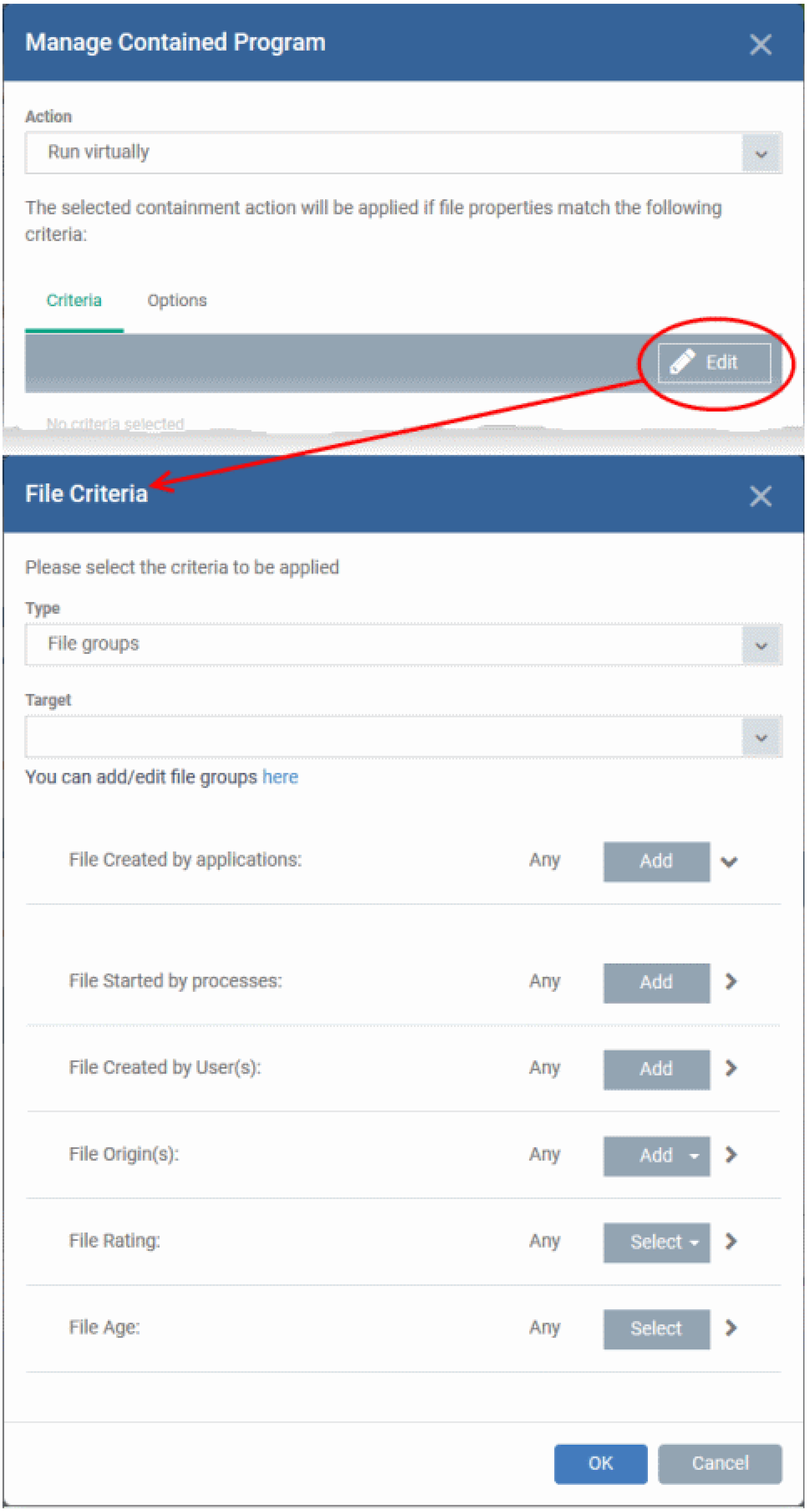
- The next step is to select the target files and configure filters.
- You can filter a rule so it applies to specific files.
  - For example, you can choose 'All executables' as the target, then add a filter so it only affects executables from the internet.
  - Another example is if you want to allow unrecognized files created by a certain user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target, then add 'Files created by a specific user' as the filter.

Select the target and set filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- Click the 'Edit' button at the far right to add new target and filter criteria



Manage Contained Program

Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

File Criteria

Please select the criteria to be applied

Type: File groups

Target:

You can add/edit file groups here

| | | |
|---|---|---|
| File Created by applications: | Any | Add |
| File Started by processes: | Any | Add |
| File Created by User(s): | Any | Add |
| File Origin(s): | Any | Add |
| File Rating: | Any | Select |
| File Age: | Any | Select |

The 'File Criteria' dialog will open. The file criteria dialog allows you:

- Select the target
- Configure the filter criteria

## Select the target

- Select the type of target item from the 'Type' drop-down. You can choose an application, file group, hash, or folder as your target:
    - **Files -** Apply the rule to a specific file.
        - Add an executable as the target by entering its installation path + file name.
    - **File Groups** - Apply the rule to predefined file groups.
            - File groups are handy, predefined groupings of one or more file types.
            - For example, selecting 'Executables' would include all files with the extensions .exe .dll .sys .ocx .bat .pif .scr. Other predefined categories include 'Windows System Applications' , 'Windows Updater Applications' and 'Start Up Folders'.
            - You can also create custom file groups in 'Settings' > 'System Templates' > 'File Groups Variables'. See '**Create and Manage File Groups**' for more details.
        - Select a predefined or custom file-group as required.
    - **Folder** - Apply the rule to all files in a folder or drive
        - Enter the path to the folder that contains the target files in the field provided.
    - **File Hash -** Apply the rule to all files that have a specific SHA1 hash value.
            - A hash value is a large number which is generated by passing the file through a hashing algorithm. The number uniquely identifies the file, and it is extremely unlikely that two files will ever generate the same hash value. The benefit of using a file hash is that the rule will still work even if the file name changes.
        - Enter the SHA1 hash value of the target executable file in the 'Target' field.
    - **Process Hash -** Apply the rule to files whose processes have a specific SHA1 hash value. Please see description above if required.
        - Enter the SHA1 hash value of the process created by the target file in the 'Target' field.

## Configure the Filter Criteria and File Rating

Filter criteria let you further refine which files are caught by the rule. The available filters are:

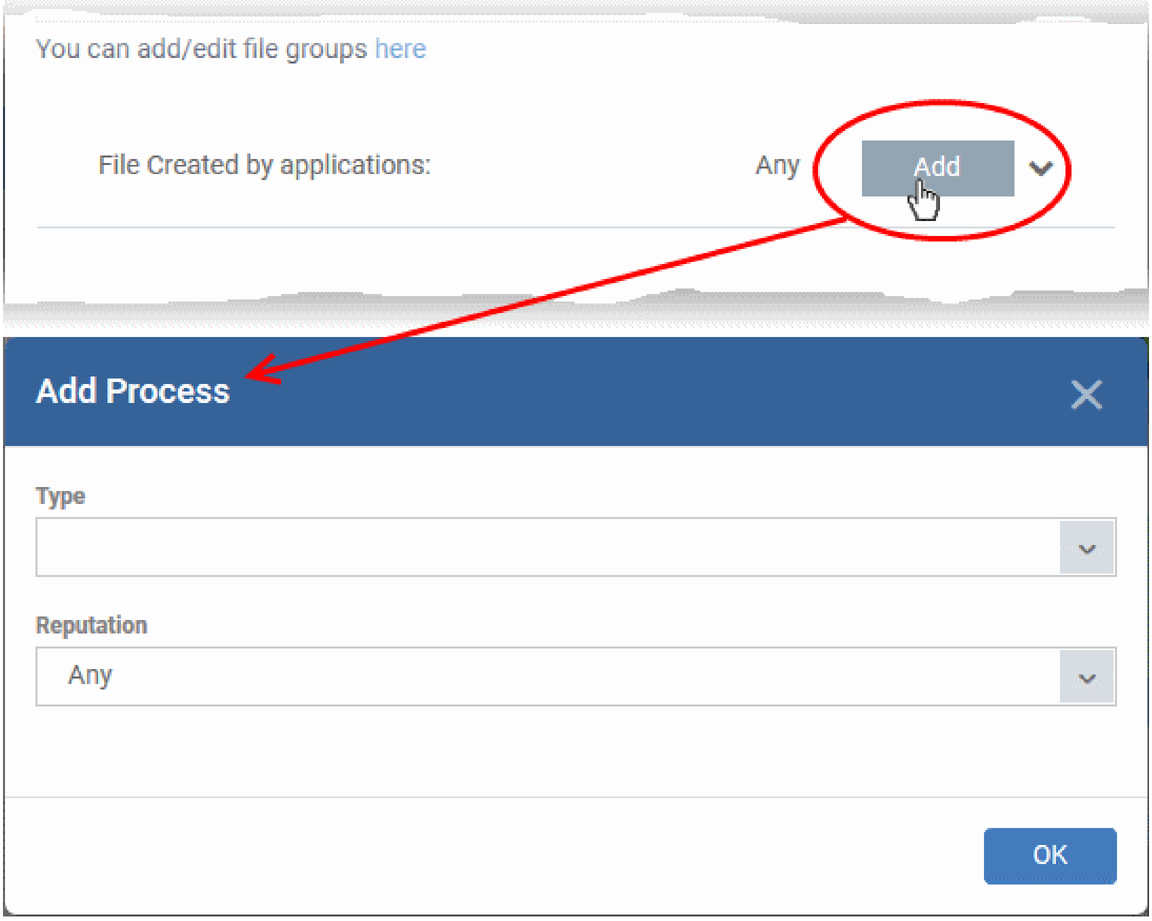
- By application that created the file
- By process that created the file
- By user that created the file
- By file origin
- By file rating
- By file age

## Auto-contain a file if it was created by a specific application

- Create a filter to apply an action to a file based on its parent application.
- You can also specify the file rating of the source application. The rule will then only contain a file if its parent has a certain trust rating.

Specify source applications

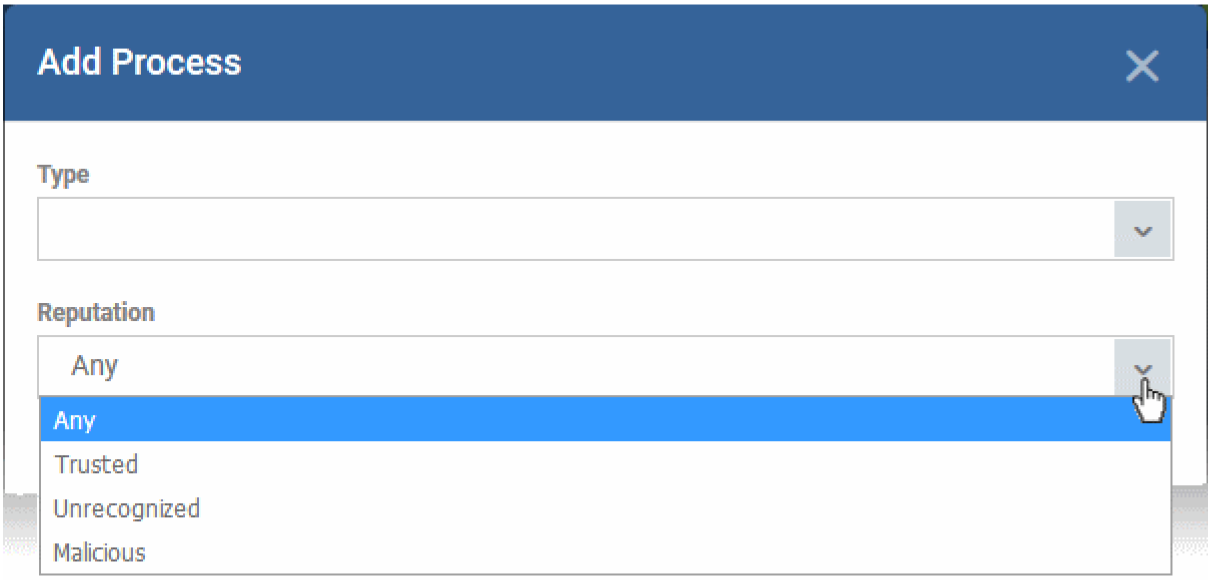
- Click the 'Add' button in the 'File Created by applications' stripe.


You can add/edit file groups here

File Created by applications: Any

The 'Action' you specified earlier will be applied to files matching the type and reputation you choose here:

- **Type** - See **target types** above for more details.
- **Reputation** - Choose the file rating of the source you specified in the 'Type' drop-down.



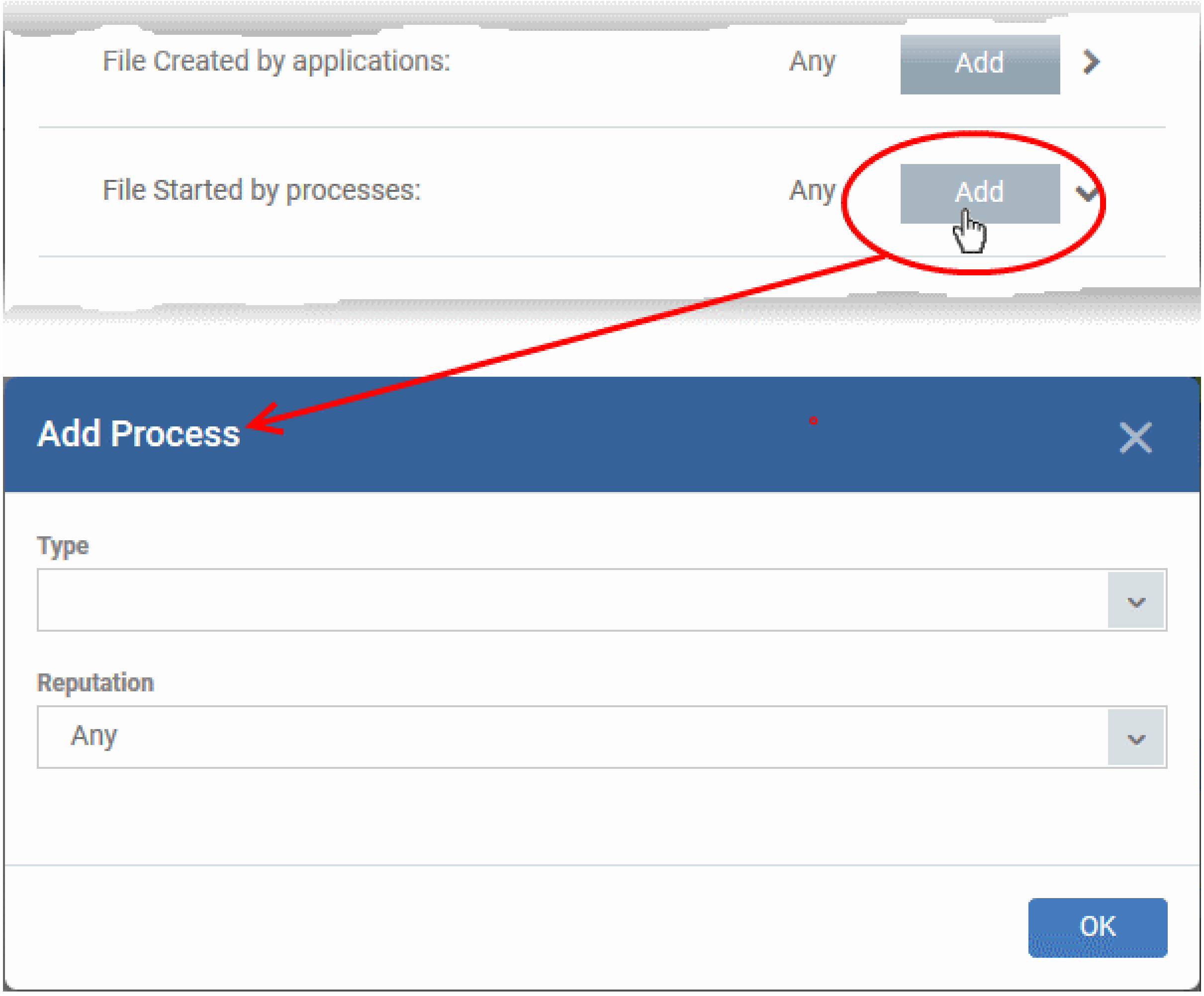
- Click 'OK' to save your settings
- Repeat the process to add more source applications
- To edit the source application items in the list, click the 'Edit' at the right of the item
- To remove an item, click 'Delete' at the right of the item

### Auto-contain a file if it was created by a specific process

- Create a filter to apply an action to a file based on its parent process.
- Optionally, you can also specify:
    - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
    - The number of levels in the process chain that should be inspected.

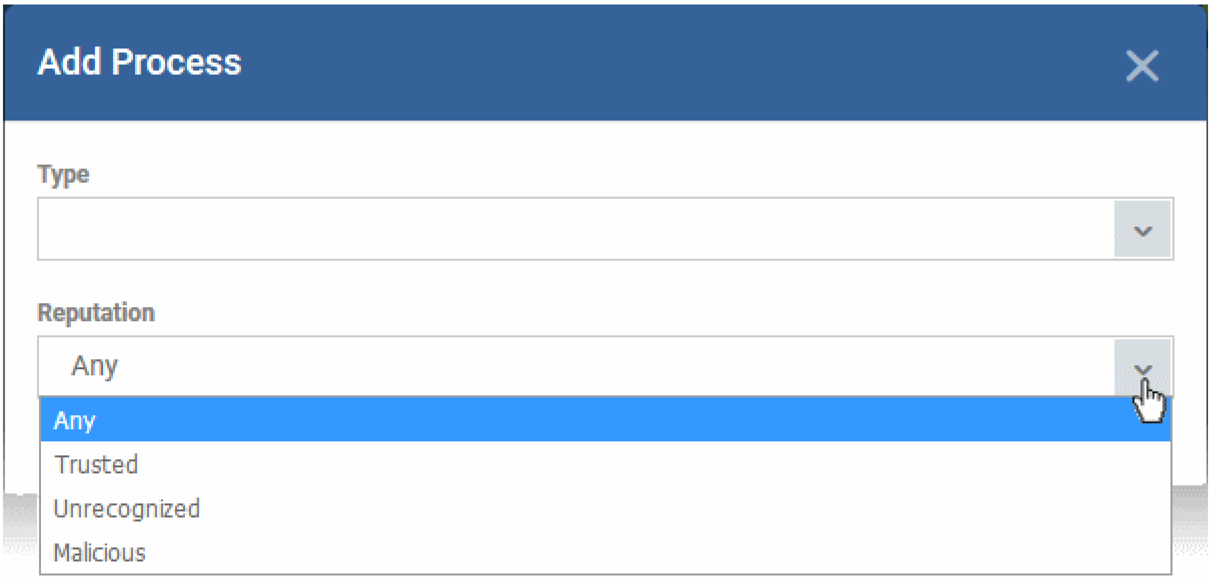
Specify source processes

- Click the 'Add' button in the 'File Created by Process(es)' stripe:



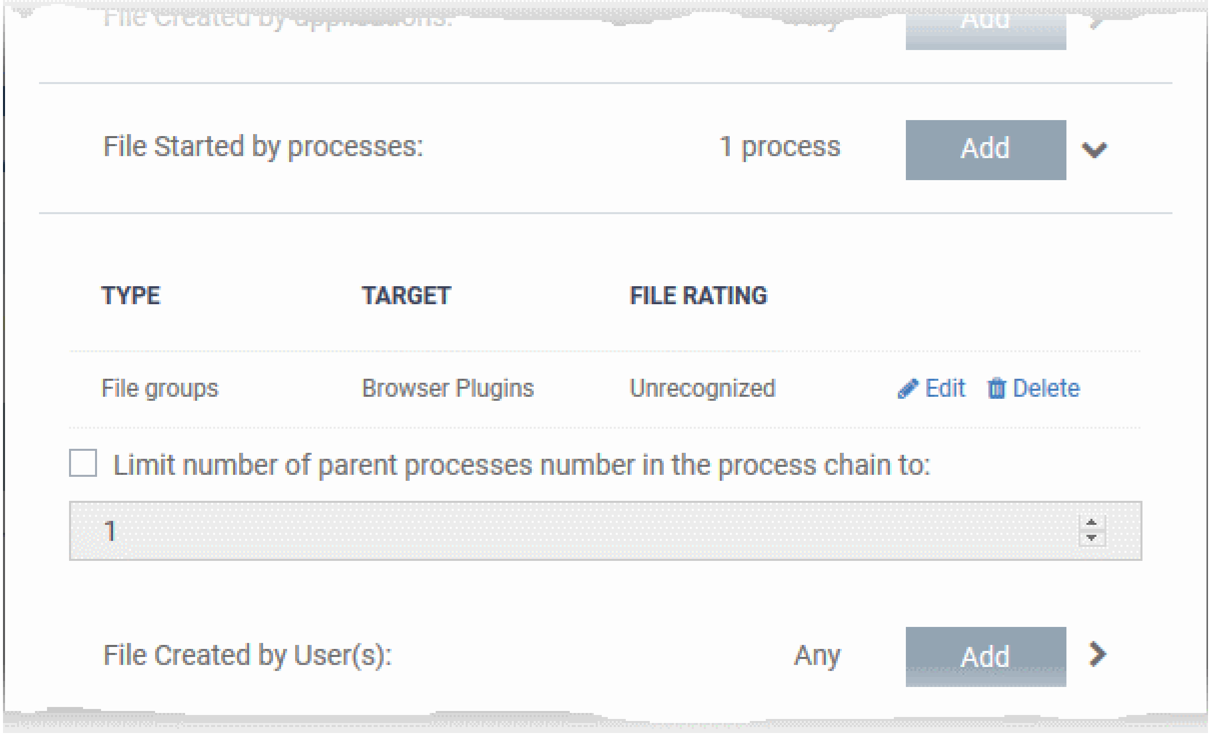
The 'Action' you chose earlier will be applied to files matching the type and reputation you pick here:

- **Type** - See **target types** above for more details.
- **Reputation** - Choose the file rating of the source you specified in the 'Type' drop-down.



- Click 'OK'

The source process type will be added.



| TYPE | TARGET | FILE RATING |
|---|---|---|
| File groups | Browser Plugins | Unrecognized |

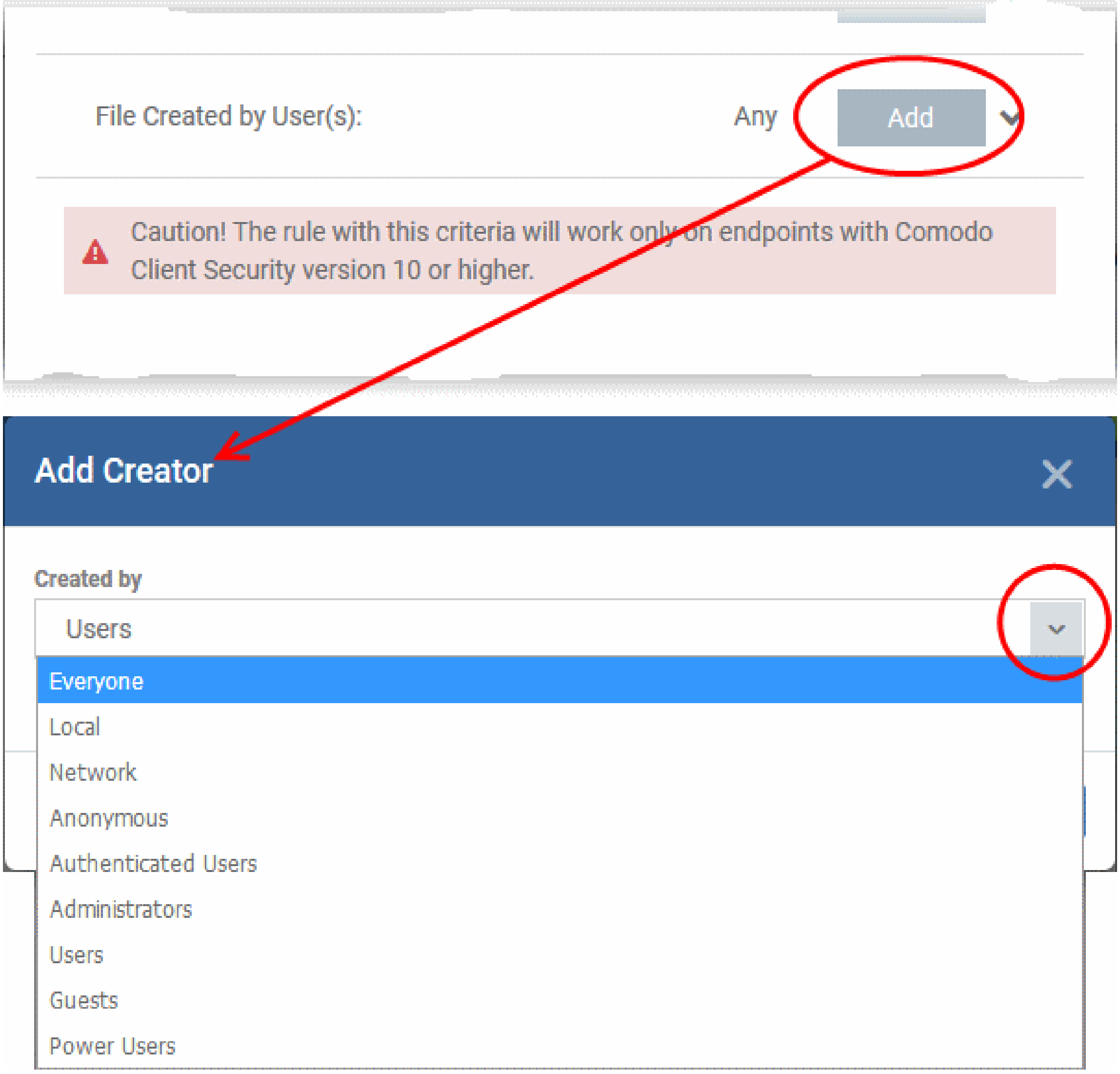
□ Limit number of parent processes number in the process chain to: 1

- **'Limit number of parent processes in the process chain to'** - Specify how far up the process tree CCS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.

- Repeat the process to add more source processes
- Click the 'Edit' if you want to modify the source process items.

## Auto-contain a file created by specific user(s)

- Click the 'Add' button in the 'File Created by User(s)' stripe.



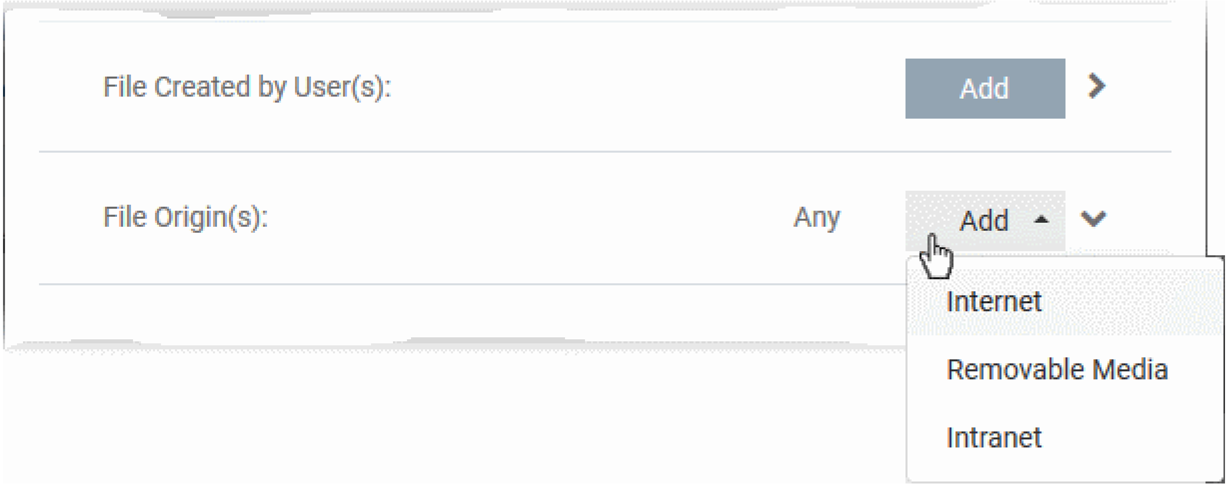
- The 'Add Creator' dialog will appear.
- Choose the pre-defined user group from the 'Created by' drop-down

The User Group will be added to the list of creators.

- Repeat the process to add more user groups
- Click 'X' at the right end of the user name to remove a group

### Auto-contain a file downloaded/copied from a specific source

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:

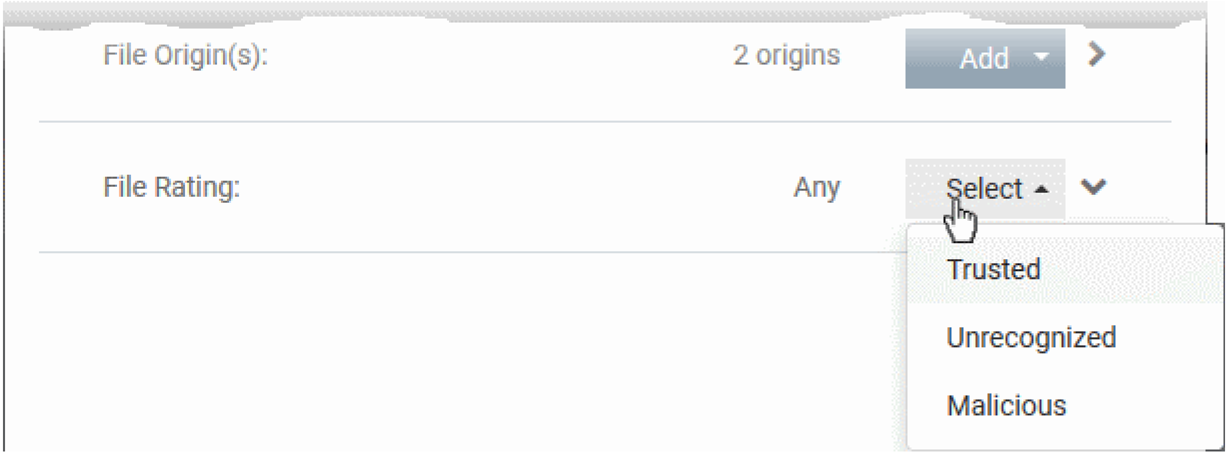


- **Internet** - The rule will only apply to files that were downloaded from the internet.
- **Removable Media** - The rule will only apply to items copied to the computer from removable devices. For example, from a USB drive, CD/DVD, or external storage.
- **Intranet** - The rule will only apply to files that were downloaded from the local intranet.

- Repeat the process to add more sources
- To remove a source added by mistake or no longer needed in the list, click 'X' at the right end of the item

### Select the file rating as filter criteria

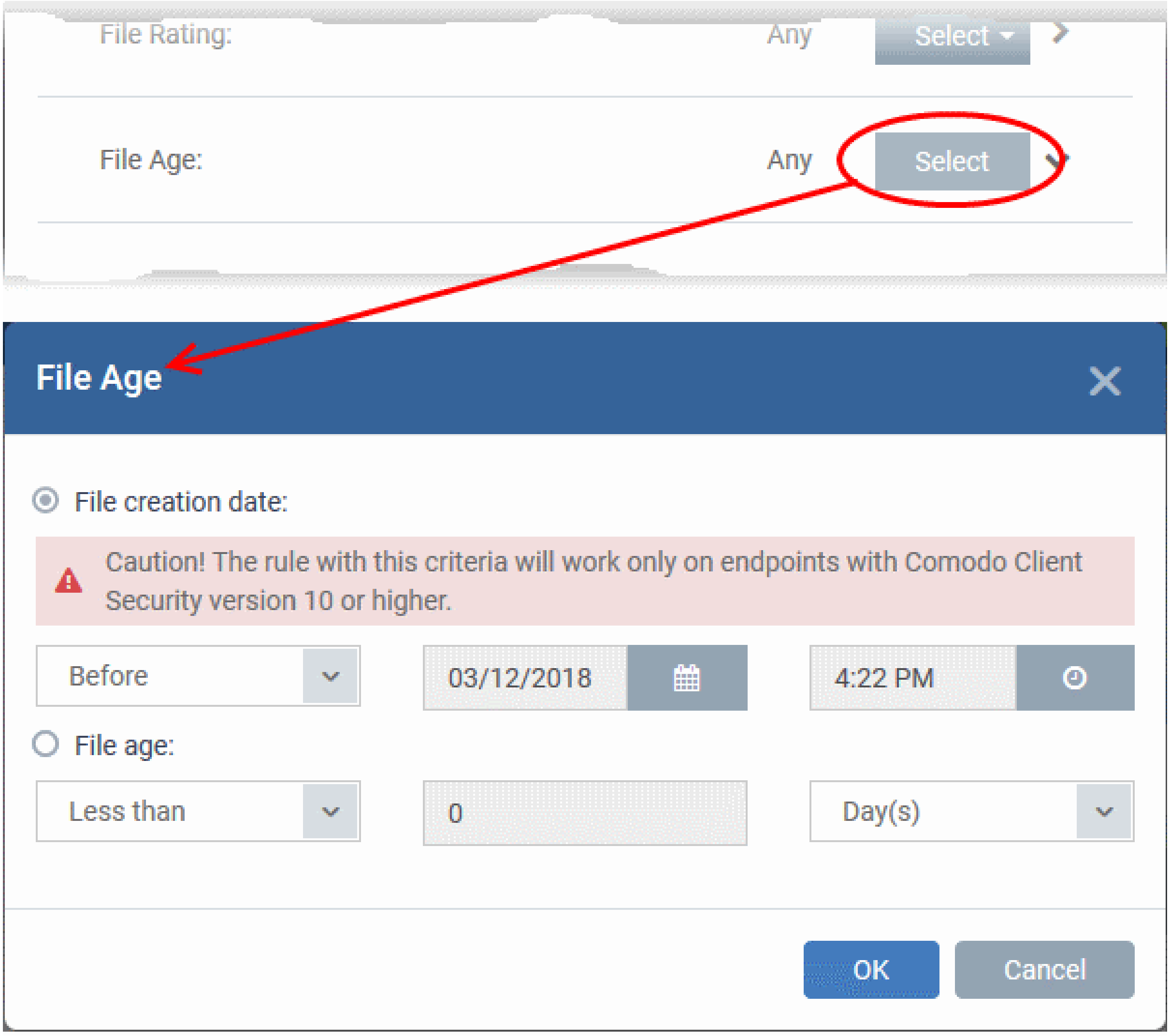
- Click the 'Select' button in the 'File Rating' stripe



- This will apply the rule to files which match the trust rating you set. You can choose from the following trust ratings:
  - **Trusted** - Applications are categorized as 'Trusted' if:
    - The file is on the global whitelist of safe files
    - The file is signed by a trusted vendor
    - The file was installed by a trusted installer
    - The file was given a trusted rating by an admin ('Settings' > 'Application Control')
    - See **Manage File Trust Ratings on Windows Devices** for more information.
  - **Unrecognized** - Files that do not have a current trust rating. The file is on neither the blacklist nor the safelist, so is given an 'unknown' trust rating.
  - **Malicious** - Malware files - those that are on the blacklist of known harmful files.

## Set the file age as filter criteria

- Click the 'Select' button in the 'File age' stripe.



File Rating: Any Select

File Age: Any Select

File Age

○ File creation date:

Caution! The rule with this criteria will work only on endpoints with Comodo Client Security version 10 or higher.

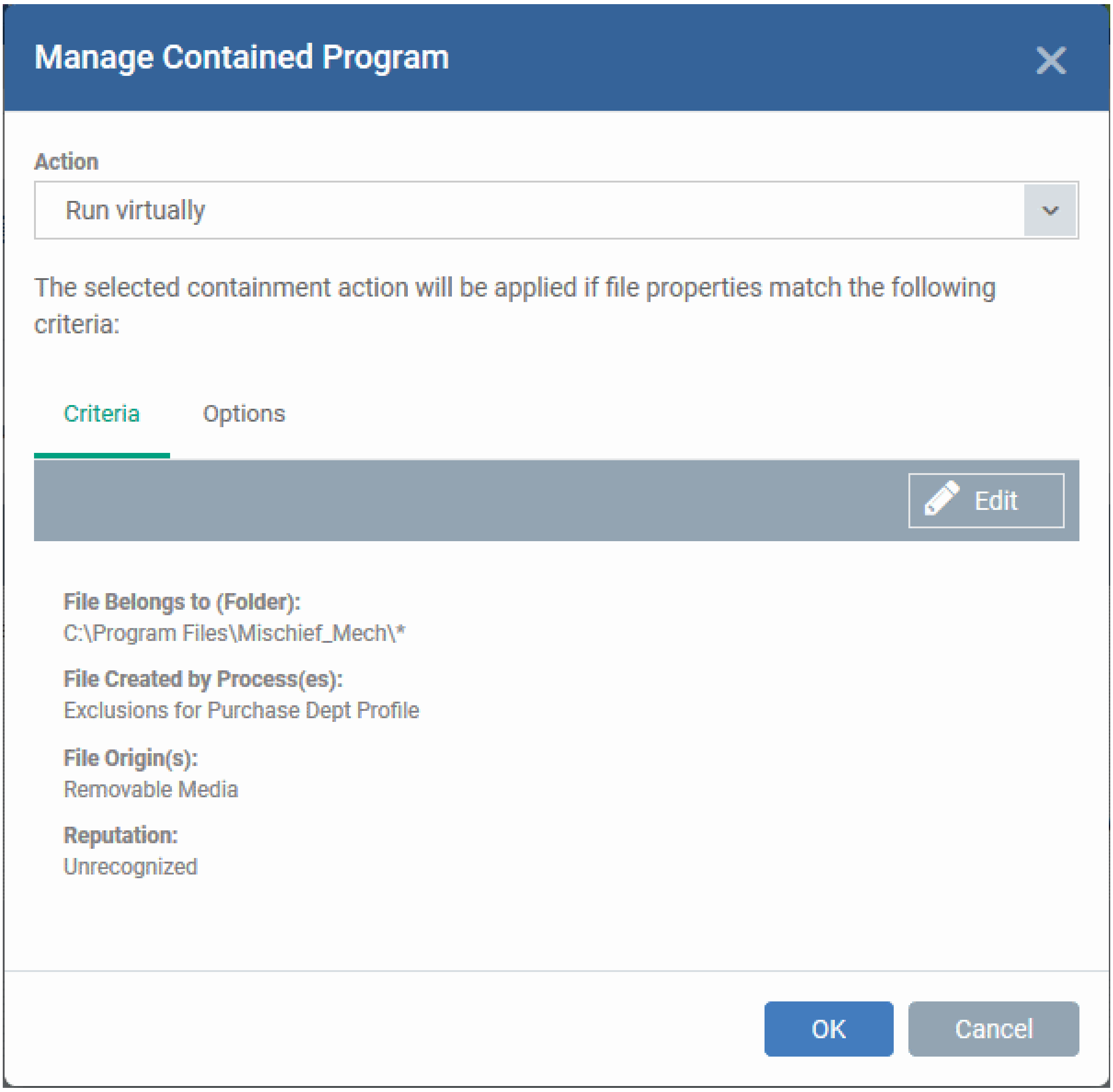
Before | 03/12/2018 | 4:22 PM

○ File age:

Less than | 0 | Day(s)

The 'File Age' dialog will appear. You can set the file age in two ways:

- **File Creation Date -** To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age -** To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than -** CCS will check the reputation of a file if it is younger than the age you set here.
  - **More Than -** CCS will check the reputation of a file ifit is older than the age you set here.
- Click 'OK' in the 'File Criteria' dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Manage Contained Program

Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

File Belongs to (Folder):
C:\Program Files\Mischief_Mech\*

File Created by Process(es):
Exclusions for Purchase Dept Profile

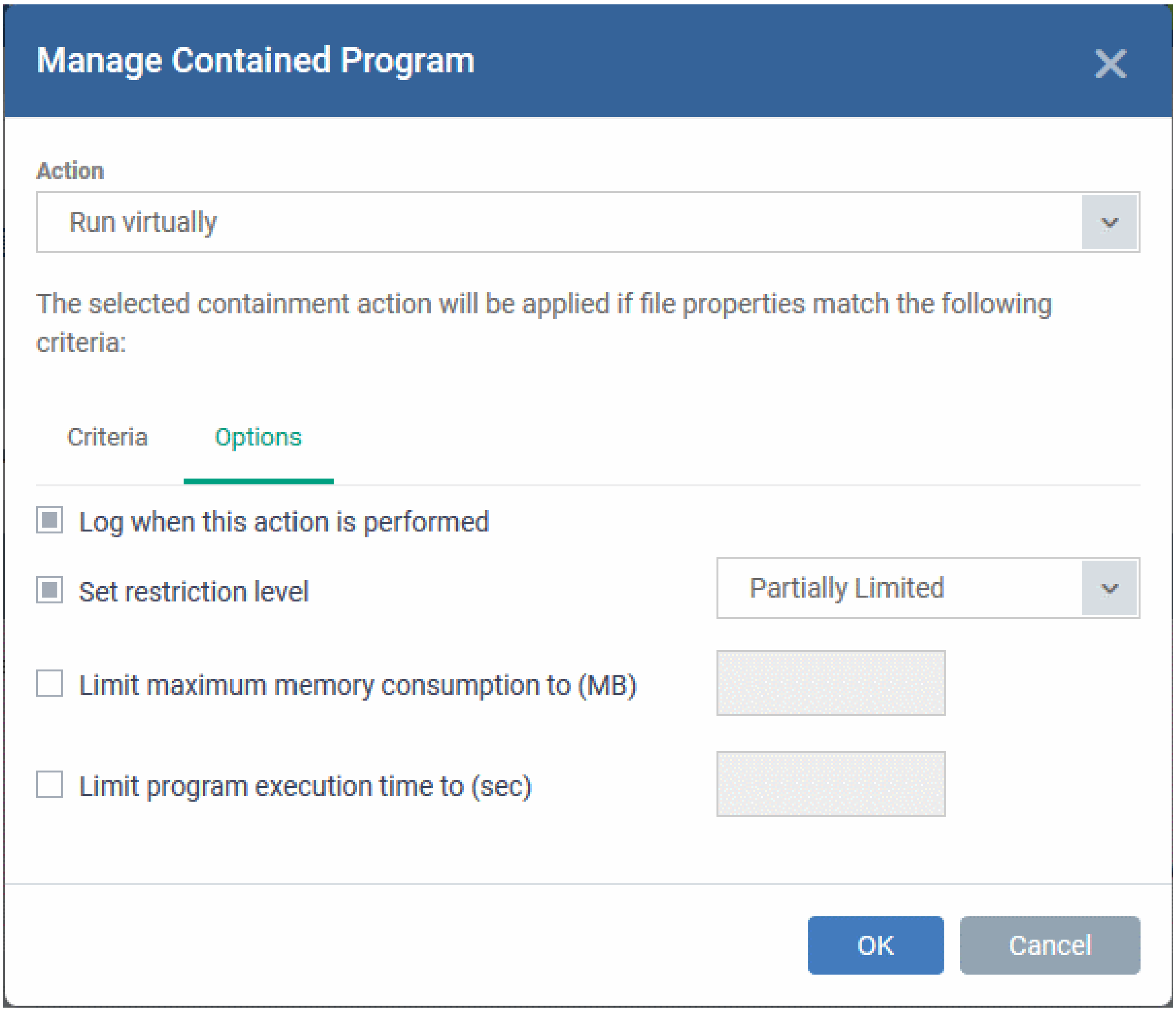
File Origin(s):
Removable Media

Reputation:
Unrecognized

## Step 3 - Select options

The next step is to choose additional options and restrictions on items contained by the rule.

- Click the 'Options' tab.



Manage Contained Program

Action: Run virtually

The selected containment action will be applied if file properties match the following criteria:

- ☑ Log when this action is performed
- ☑ Set restriction level: Partially Limited
- □ Limit maximum memory consumption to (MB)
- □ Limit program execution time to (sec)

The options available depend on the 'Action' chosen in **Step 1**.

The '**Ignore**' action has the following options:

- **Log when this action is performed** - Creates a containment log in CCS on the endpoint when the rule is triggered.
- **Don't apply the selected action to child processes** - Child processes are those started by the target application.
  - This option is disabled by default, so the ignore rule also applies to child processes.
  - If enabled, the ignore rule does not apply to child processes. Each child process will be inspected individually and all relevant rules applied.

The '**Run Restricted**' and '**Run Virtually**' actions have the following options:

- **Log when this action is performed** - Creates a containment log in CCS on the endpoint when the rule is triggered.
- **Set Restriction Level** - If the rule is triggered, CCS runs the file at the restriction level you set.

  You can choose from the following levels:

  - **Partially Limited** - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(Default)
  - **Limited** - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.

- **Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Untrusted** - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

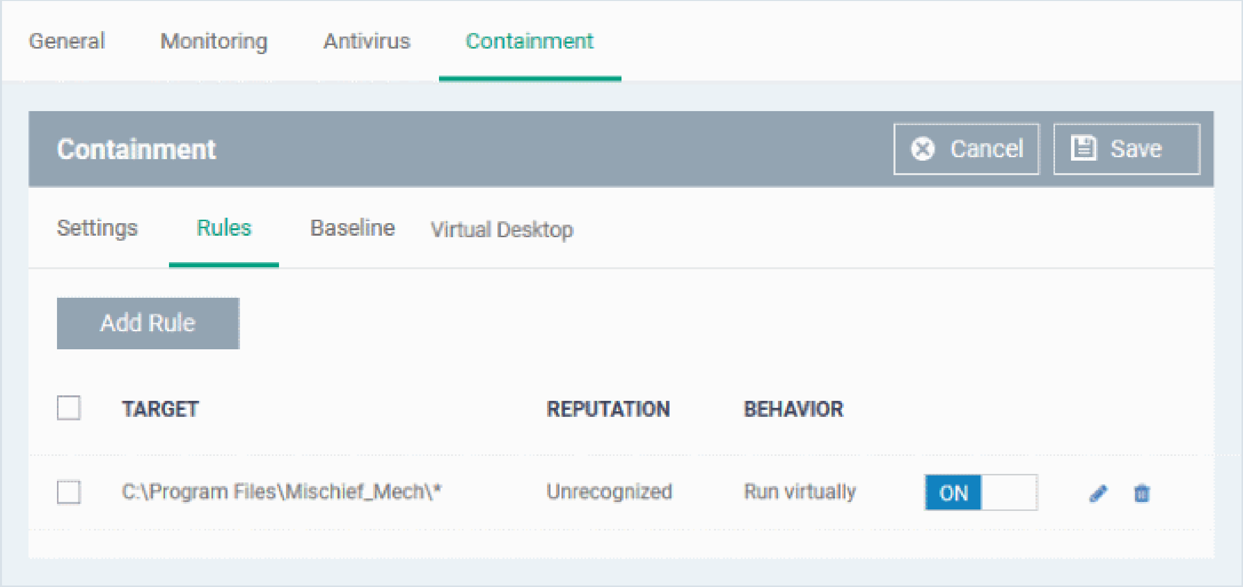
  Note. You must choose a restriction level if 'Run Restricted' is the action. However, you can disable 'Set Restriction Level' if the action is 'Run Virtually'.

- **Limit maximum memory consumption to** - Enter the maximum amount of memory that the application is allowed to use (in MB).
- **Limit program execution time to** - Specify how long the application is allowed to run. Enter the maximum time in seconds. The program is automatically terminated when the time limit expires.

The '**Block**' action has the following options:

- **Log when this action is performed** - Creates a containment log in CCS on the endpoint when the rule is triggered.
- **Quarantine program** - Applications satisfying the rule will be automatically quarantined. See **View and Manage Quarantined Items on Windows Devices** if you want to read more about the quarantine area.

Click 'OK' to save your choices. The rule will be added to the list of rules.



| □ | TARGET | REPUTATION | BEHAVIOR | | |
|---|---|---|---|---|---|
| □ | C:\Program Files\Mischief_Mech\* | Unrecognized | Run virtually | ON | |

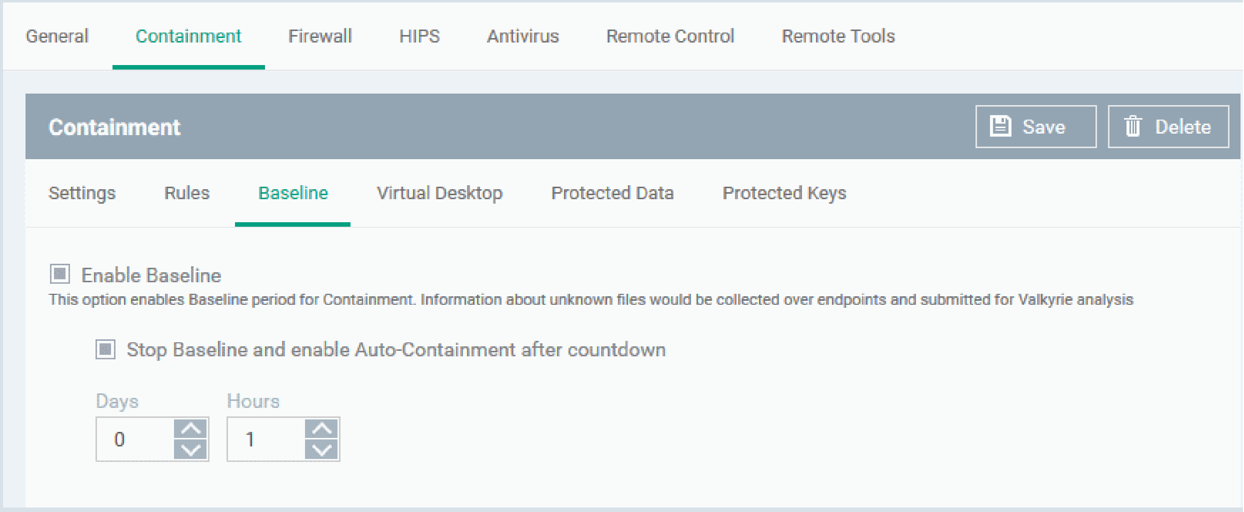
- Repeat the process to add more rules
- You can drag-and-drop the rules to re-prioritize them. Rules at the top of the table have a higher priority than those at the bottom. The setting in the rule nearer the top will prevail in the event of a conflict between rules.
- You can edit or remove rules at any time using the options at the right.

## Baseline Settings

- A baseline period is a window of time during which all unknown files are submitted to Valkyrie for analysis.
- Unknown files are not auto-contained during the baseline. This feature is best used during the initial setup period when, typically, many unknown files are discovered.
- You must enable 'Stop Baseline and enable...' if you want the baseline to last a specific length of time. If you don't then the baseline period runs indefinitely.

### Configure baseline settings

- Open the 'Containment' section of a profile
- Click the 'Baseline' tab:



☐ Enable Baseline

This option enables Baseline period for Containment. Information about unknown files would be collected over endpoints and submitted for Valkyrie analysis

☐ Stop Baseline and enable Auto-Containment after countdown

Days 0

Hours 1

| Baseline Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Baseline | A baseline is a period of time during which unknown files discovered on your network are sent to Valkyrie. Unknown files are not run in the container during the baseline period.<br>This can be useful if you want to create a whitelist of existing files on your network.<br>(***Default = Disabled***) |
| Stop Baseline and Enable Auto-Containment after countdown | **Enabled** - Baselining will last the length of time you set in the fields. Auto-containment will resume when this period expires.<br>**Disabled** - Baselining will continue until you disable it in the setting at the top.<br>The timer begins after you apply the profile to your network.<br>(***Default = Disabled***) |

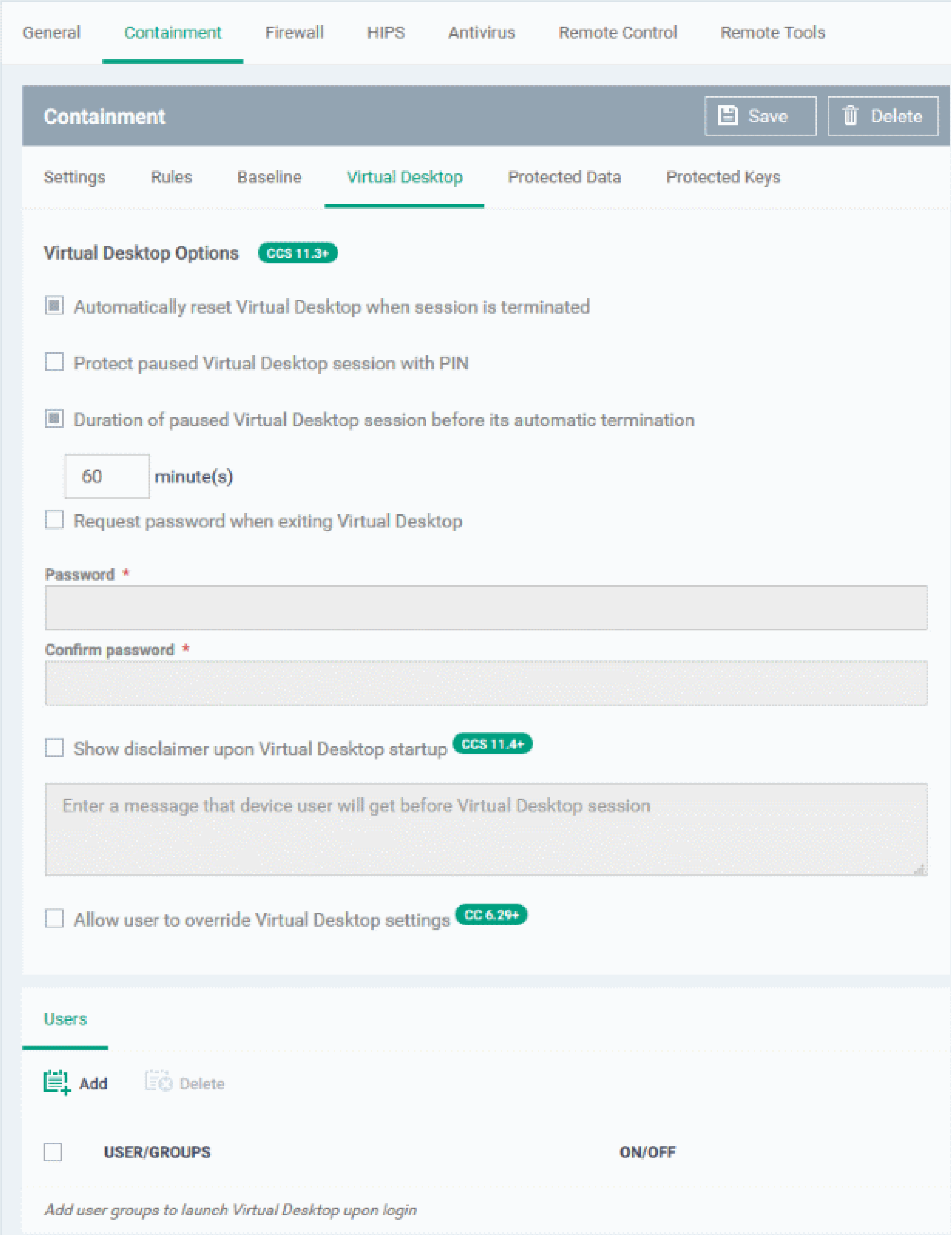
- Click 'Save' to apply your changes.

## Virtual Desktop Settings

- The 'Virtual Desktop' is a sandbox environment in which users can run programs and browse the internet without fear those activities will damage their computer.
- Applications in the virtual desktop are isolated from other processes, write to a virtual file system, and cannot access user data.
- This makes it ideal for risk-free internet surfing, beta-software, and general computer use. From the users point-of-view, programs in the virtual desktop run exactly as they would under Windows.
- Virtual desktop settings let you configure the behavior of the feature on endpoints.

### Configure virtual desktop settings

- Open the 'Containment' section of a profile
- Click the 'Virtual Desktop' tab:



Virtual Desktop Options CCS 11.3+

☒ Automatically reset Virtual Desktop when session is terminated

□ Protect paused Virtual Desktop session with PIN

☒ Duration of paused Virtual Desktop session before its automatic termination

60 minute(s)

□ Request password when exiting Virtual Desktop

Password *

Confirm password *

□ Show disclaimer upon Virtual Desktop startup CCS 11.4+

Enter a message that device user will get before Virtual Desktop session

□ Allow user to override Virtual Desktop settings CC 6.29+

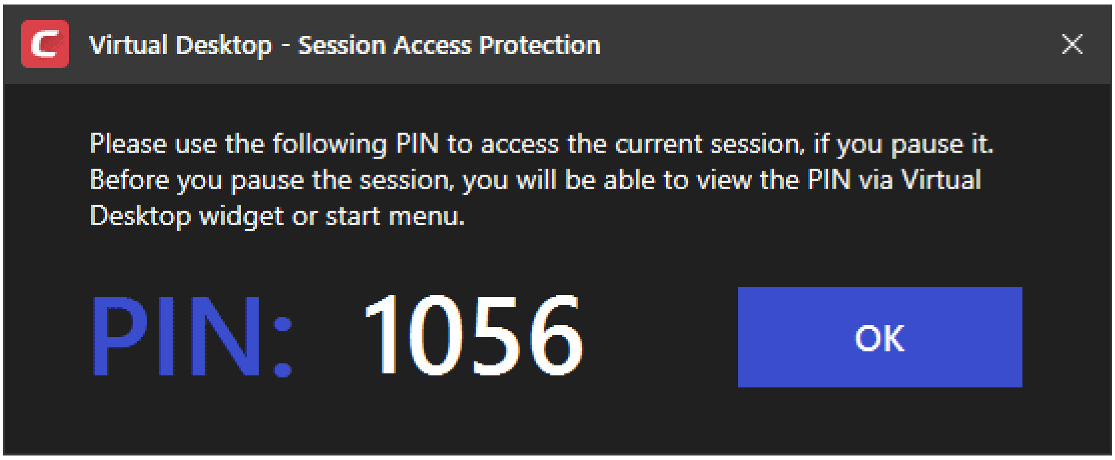
| □ | USER/GROUPS | ON/OFF |
|---|---|---|

*Add user groups to launch Virtual Desktop upon login*

- **Automatically reset Virtual Desktop when session is terminated -** All data saved in the virtual desktop is deleted when the desktop is closed. All changes are reversed. This includes any files downloaded from the internet and any system changes.

  Please use the 'Shared Space' folder to store files you want to keep. You can also enable external storage devices for use with the virtual desktop in **Containment Settings**.
- **Protect paused Virtual Desktop session with PIN -** Generates a session specific PIN number at virtual desktop startup. The PIN is required to resume the session from a paused state. This is useful

on shared computers as it prevents other users from accessing the session.



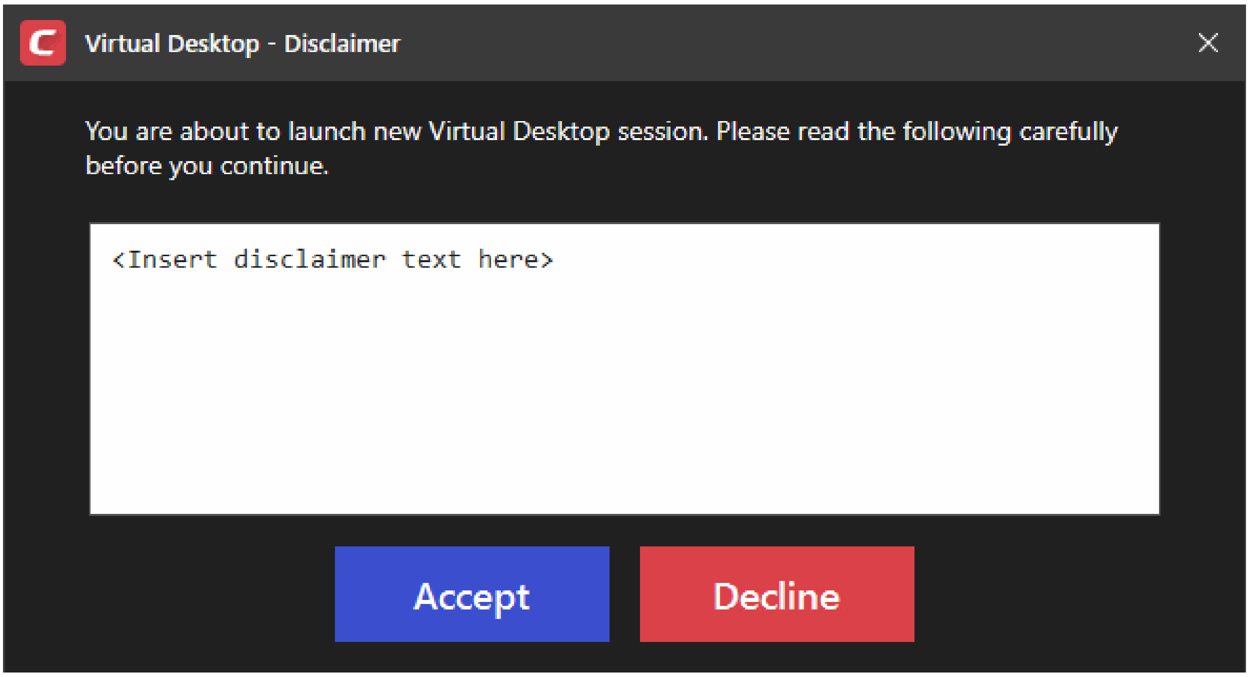
Virtual Desktop - Session Access Protection

Please use the following PIN to access the current session, if you pause it. Before you pause the session, you will be able to view the PIN via Virtual Desktop widget or start menu.

PIN: 1056

- **Duration of paused Virtual Desktop session before its automatic termination -** Set the maximum time that a virtual desktop session can be left in a paused state. The session gets automatically terminated when this period elapses.
- **Request password when exiting Virtual Desktop -** Create an 'exit' password for the virtual desktop. Users need to enter the password in order to close the virtual desktop.
  - This prevent users from closing the virtual desktop and accessing the host, potentially exposing the computer to danger.
  - Type a password that cannot easily be guessed. Passwords must be 8-16 characters and contain a mix of upper case letters, lower case letters, numbers, and special characters.
  - Re-enter the password for confirmation.
- **Show disclaimer upon Virtual Desktop startup -** Create a disclaimer which is shown when the virtual desktop starts. Users must accept the disclaimer before they can access the virtual desktop.

  Note - This setting is only of value if you are **rebranding the Comodo clients**. You can safely ignore this setting if you do not plan to rebrand.
  - Enter the disclaimer message
  - The message is shown when the virtual desktop starts.
  - Users should read the disclaimer and click 'Accept'. An example is shown below:



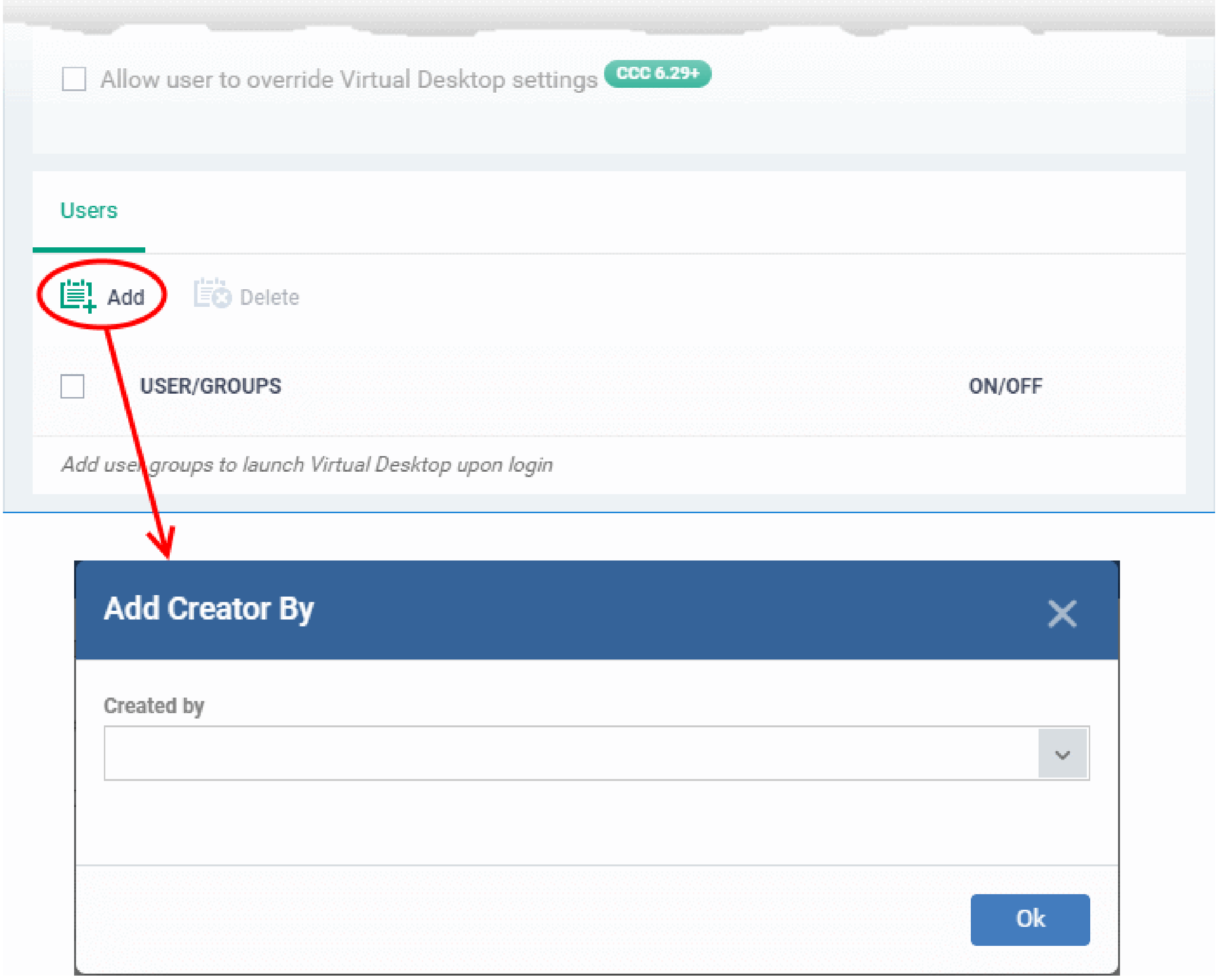
You are about to launch new Virtual Desktop session. Please read the following carefully before you continue.

```
<Insert disclaimer text here>
```

- **Allow user to override Virtual Desktop settings -** Changes to virtual desktop settings at the endpoint are not reversed by Endpoint Manager.
    - By default, EM checks devices to see if the local CCS settings match those in the profile. It will re-implement the profile settings if it detects any deviation.
    - Enabling this option stops the process described above. The EM profile does not apply any virtual desktop settings. Only the virtual desktop settings in CCS on the endpoint are applied to the device.
    - Note 1. This option complements the existing override option in the 'Client Access Control' section of a profile, which allows local changes to *every* CCS setting. You can allow local override of just the virtual desktop settings, while preventing changes to other CCS settings. See **Client Access Control** for help with this.
    - Note 2. If you enable this option, you effectively cancel all Virtual Desktop settings that come from the profile. For example, 'Exit Password', 'Reset Virtual Desktop' and 'Duration' settings will not get applied.
- **Users**

  Specify user groups for whom the virtual desktop should start automatically after login. This means the virtual desktop is the users' default environment, instead of the host operating system. This setting is especially useful for guest users and for public computers in libraries / class-rooms etc.

    - Click 'Add' under the 'Users' section:



□ Allow user to override Virtual Desktop settings CCC 6.29+

Users

Add Delete

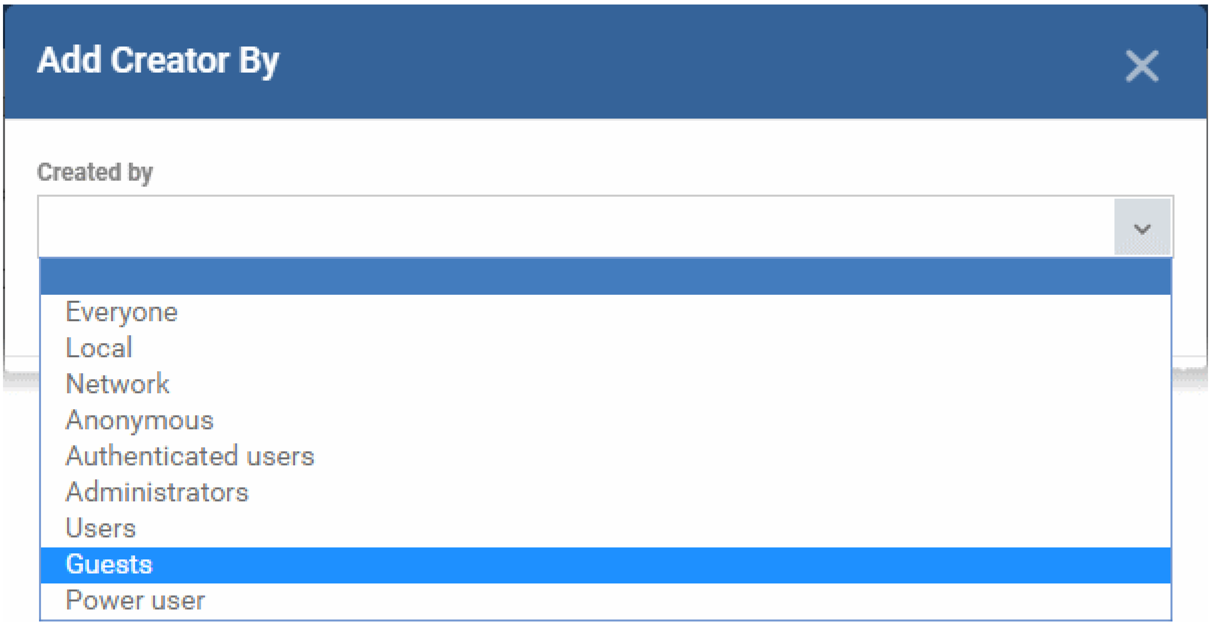
□ USER/GROUPS ON/OFF

*Add user groups to launch Virtual Desktop upon login*

Add Creator By

Created by

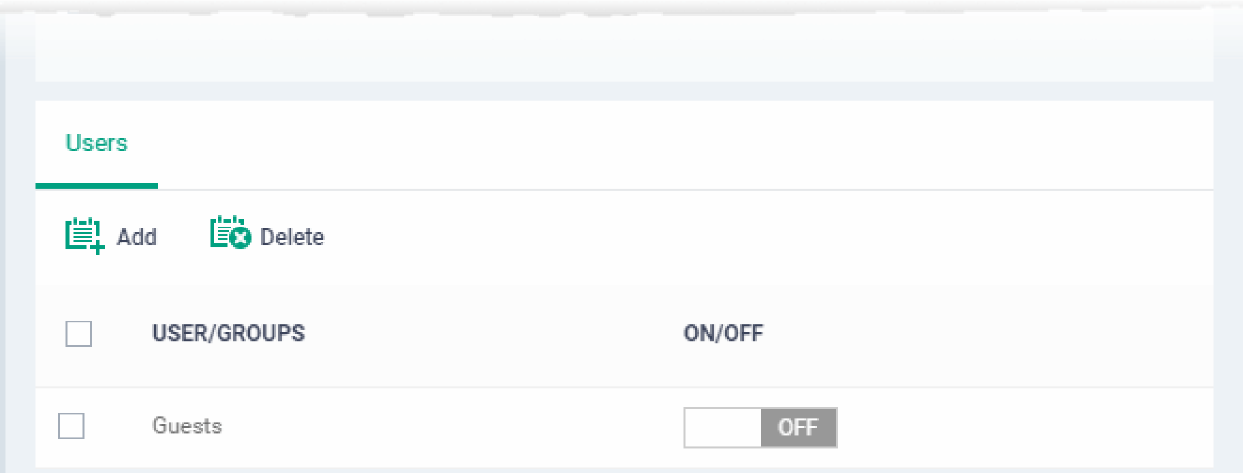
- Select a user group from the 'Created by' drop-down and click 'OK'.



Add Creator By

Created by

The selected user group is added to the list:

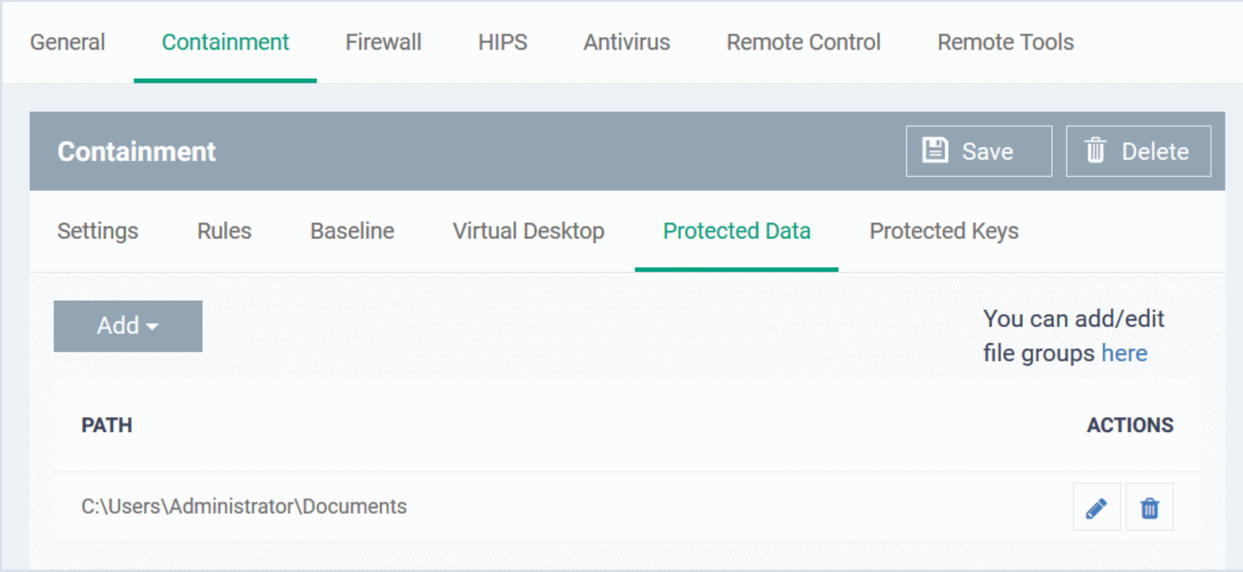


| □ | USER/GROUPS | ON/OFF |
|---|---|---|
| □ | Guests | OFF |

- Use 'ON/OFF' switches to enable or disable the feature for a particular group.
- Repeat the process to add more user groups
- Click 'Save' to apply your changes to the profile.

## Protected Data

- The 'Protected Data' tab lets you define files, folders and files in a file group that are to be denied access to the contained applications on the managed devices.
- Items in 'Protected Data' cannot be seen, accessed or modified by applications running in the container.
- This fortifies files containing sensitive data from unrecognized and potentially malicious programs.



You can add/edit file groups here

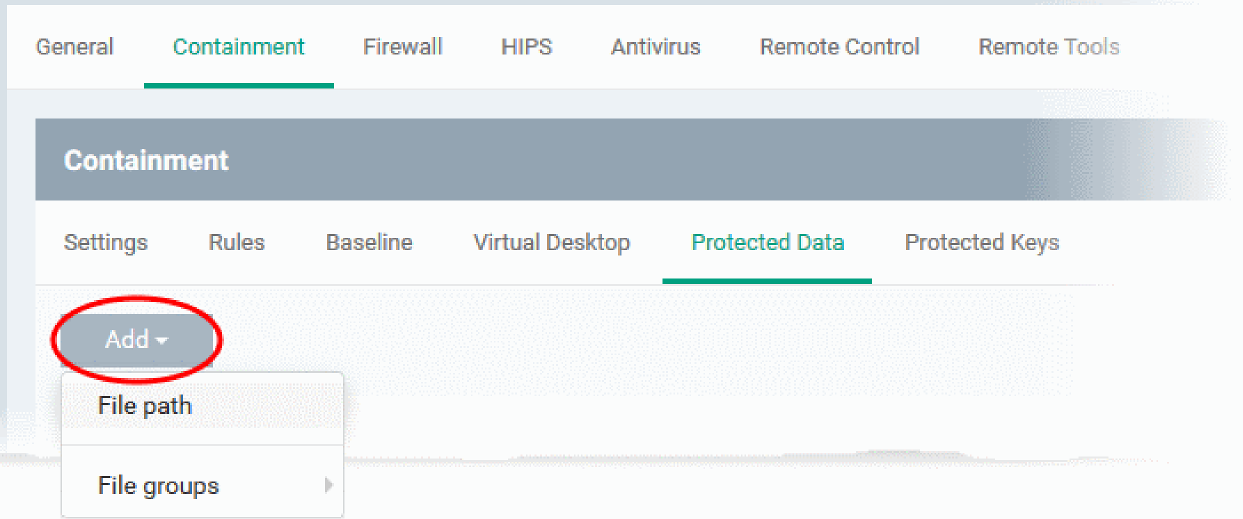
| PATH | ACTIONS |
|---|---|
| C:\Users\Administrator\Documents | |

### Protected Files and Protected Data

- Items in HIPS 'Protected Files' ('HIPS' > 'Protected Objects' > 'Protected Files') can be read by any program, but not modified by them. This contrasts to items in 'Protected Data' in containment settings, which are totally hidden to contained programs.
- If you want a file/folder to be read by other programs, but protected from modification, then add it to 'Protected Files' list.
- If you want to totally conceal an item from contained programs, but allow read/write access to trusted programs, then add it to 'Protected Data'.
- You can add the same item to both areas. This means trusted programs have read-only access to the file, and contained programs have no access rights.

**Add and manage protected data**

- Open the 'Containment' section of a profile
- Click the 'Protected Data' tab.
- Click 'Add'

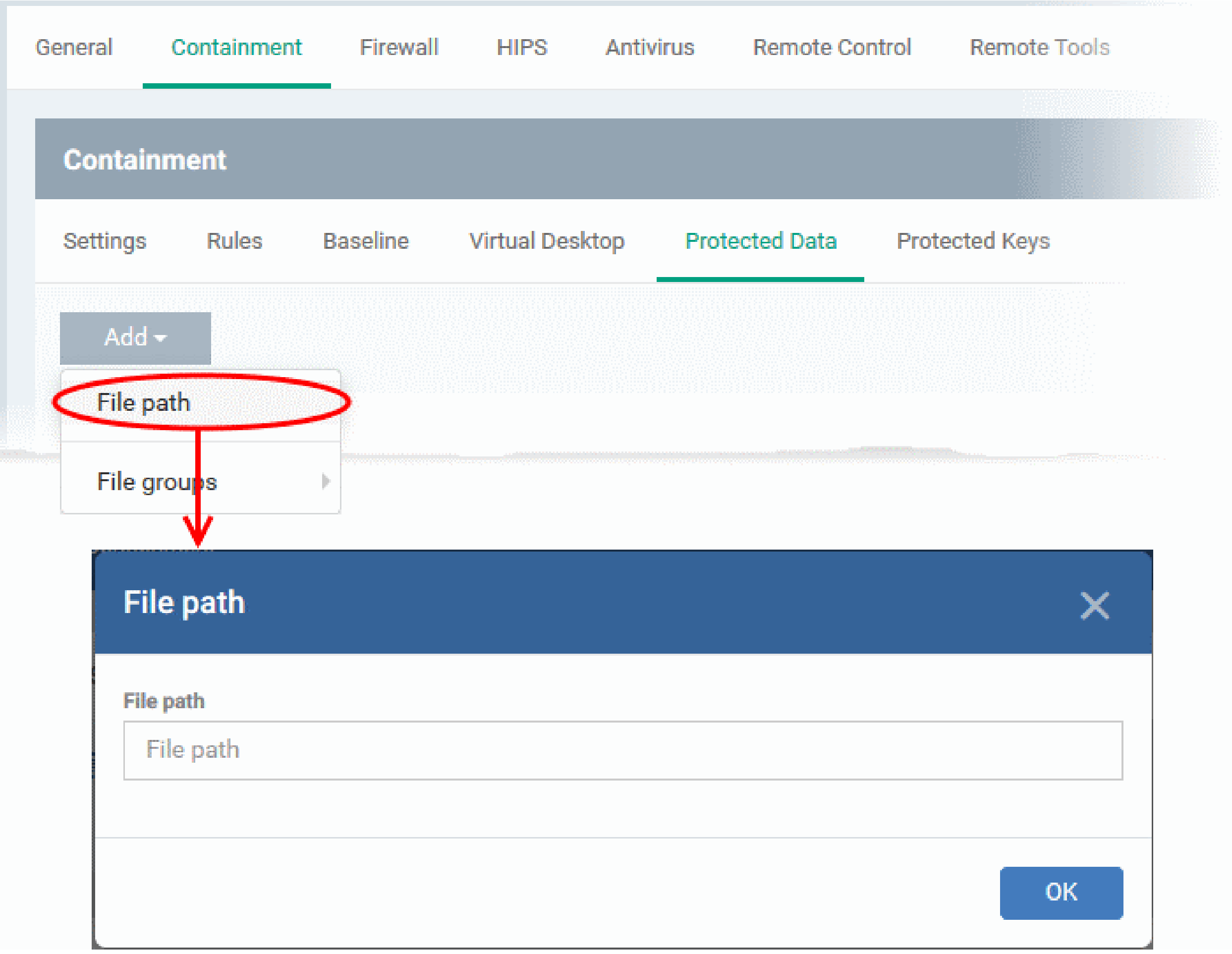


You add items in two ways:

- **File path** - Add individual files, applications, programs executables or folders
- **File groups** - Add a pre-defined group of files so that all member files in the group are blocked form contained applications

**Add files or folders**

- Choose 'File path' from the 'Add' drop-down

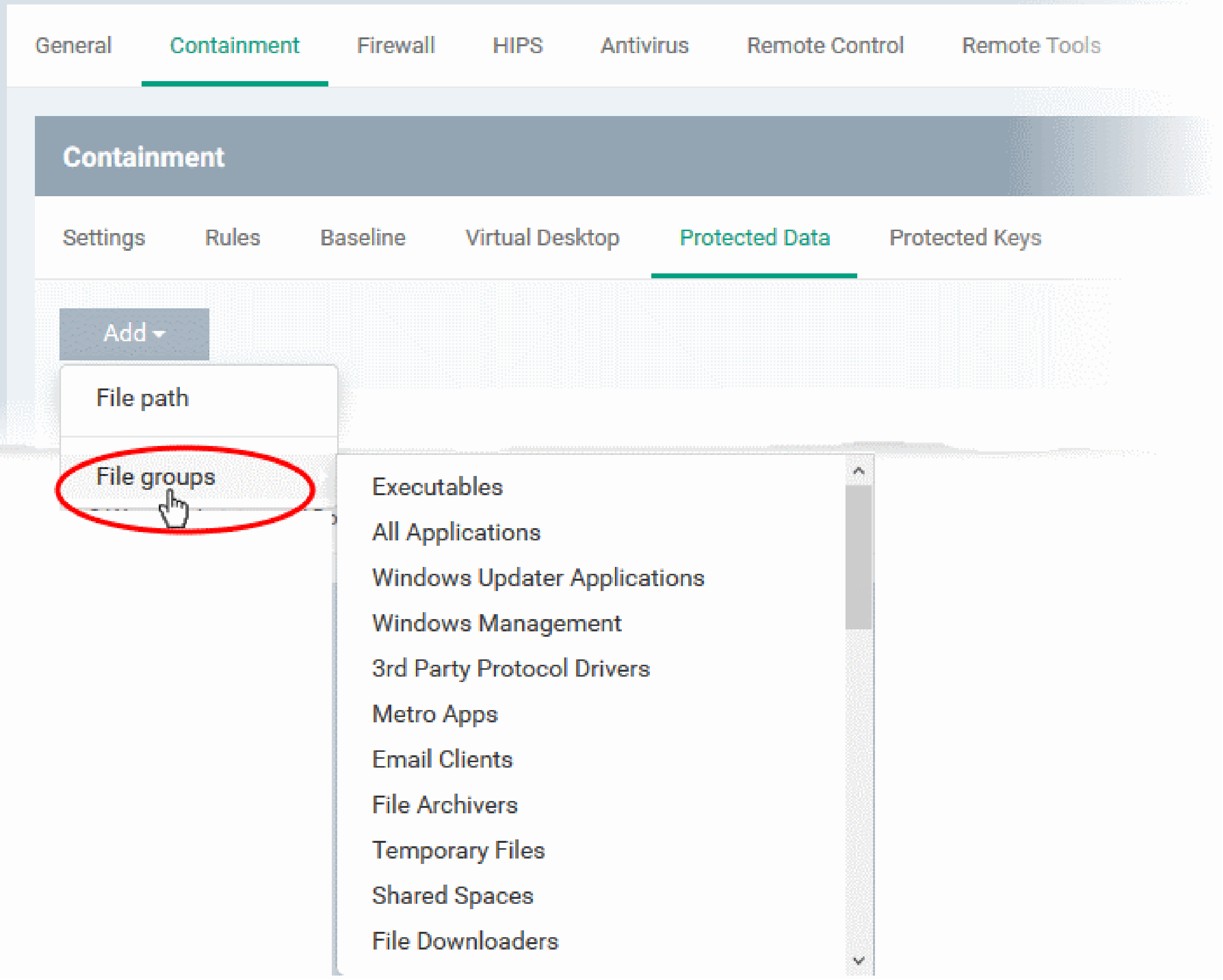


- Enter the installation path / storage location of the file to add an application or a file
- Enter the folder path to add a folder
- Click 'OK'
- Repeat the process to add more items

### Add file groups

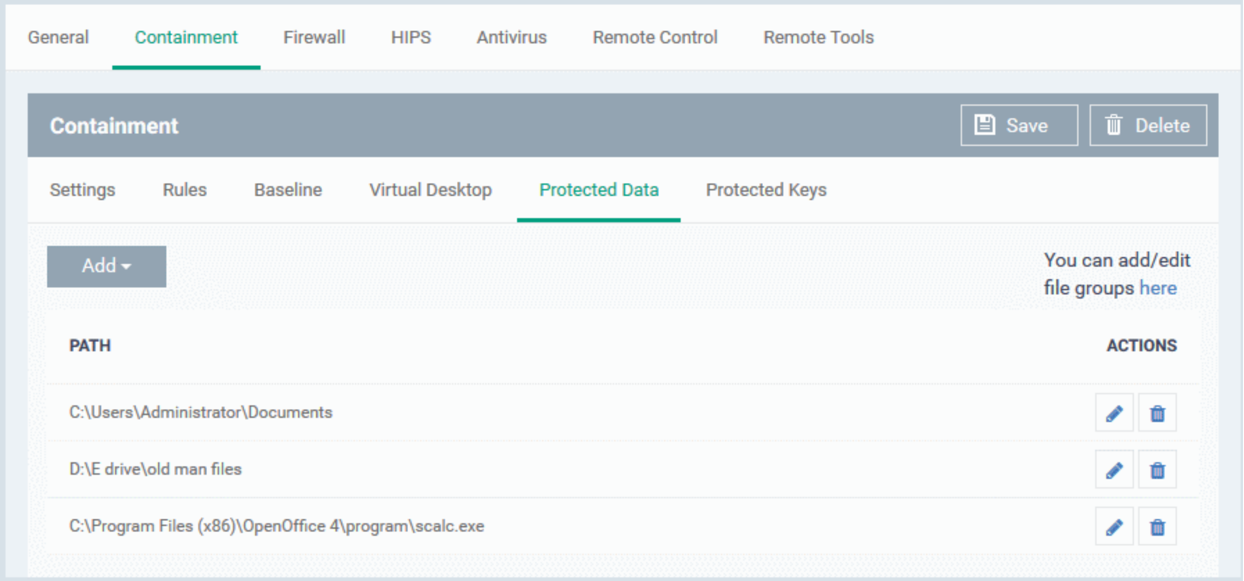
A file group is a collection of file types which have similar attributes, scope, or functionality. For example, 'Executables', 'Metro Apps', or 'Windows System Applications'. Endpoint Manager ships with a set of pre-defined file groups. You can create custom file groups from the 'Settings' > 'System Templates' > 'File Groups Variables' interface. See **Create and Manage File Groups** for more details.

- Choose 'File groups' from the 'Add' drop-down



- Select the file group from the drop-down
- Repeat the process to add more file groups

The items added are shown as a list under the 'Protected Data' tab.

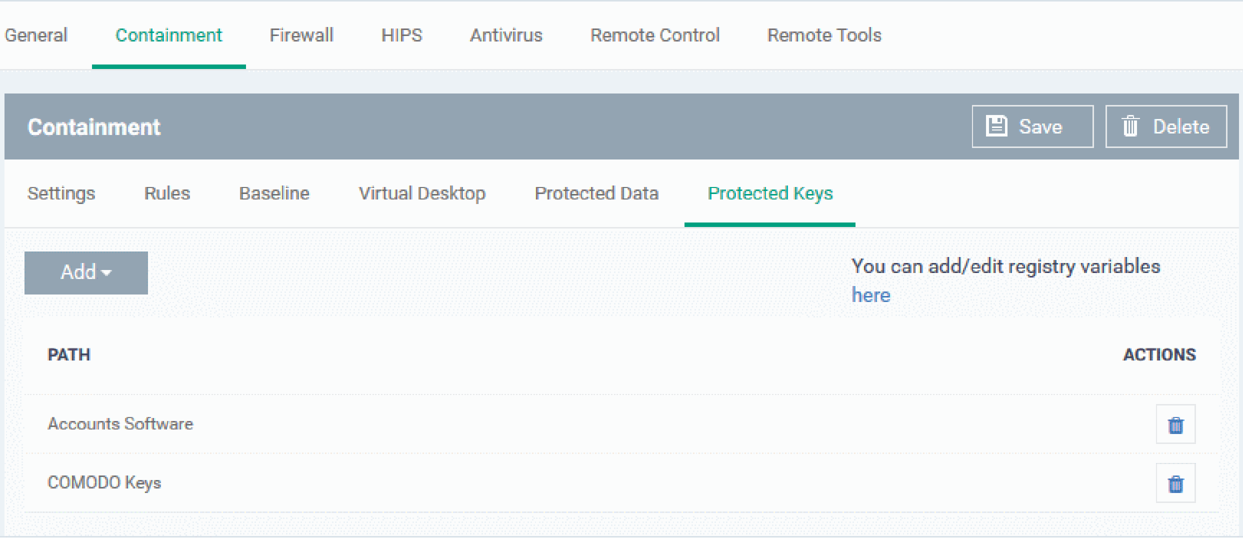


| PATH | ACTIONS |
|---|---|
| C:\Users\Administrator\Documents | |
| D:\E drive\old man files | |
| C:\Program Files (x86)\OpenOffice 4\program\scalc.exe | |

- You can edit or remove the items using the respective buttons in the 'Action' column in the 'Protected Data' interface.
- Click 'Save' for your settings to take effect.

## Protected Keys

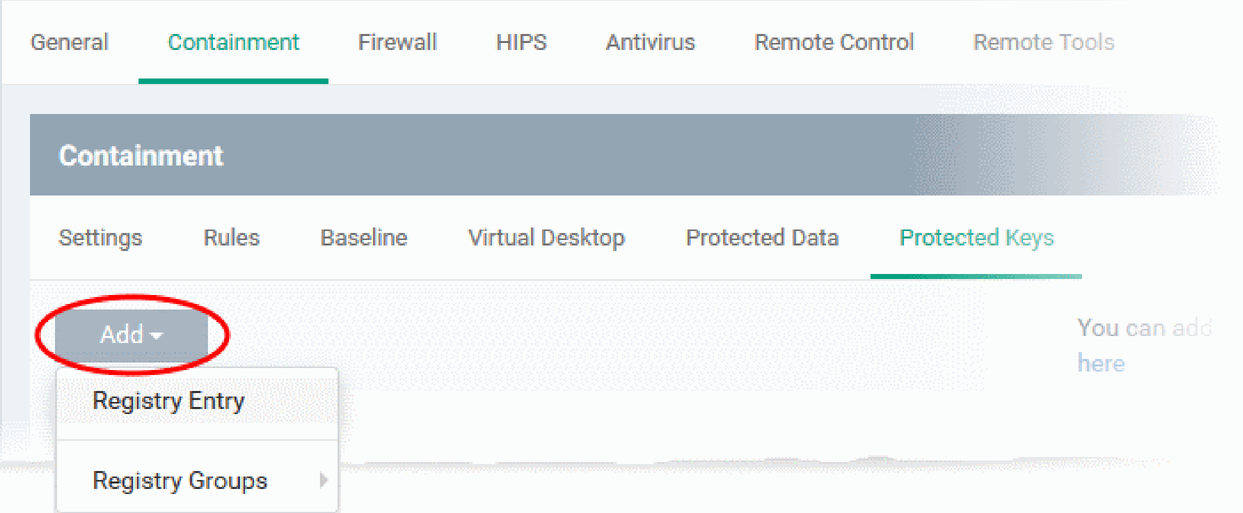
- The 'Protected Keys' tab lets you define Windows registry keys and key groups to be denied access to the contained applications on the managed devices.
- Adding important registry keys to this area will protect them from unknown and potentially malicious programs.



| PATH | ACTIONS |
|---|---|
| Accounts Software | 🗑 |
| COMODO Keys | 🗑 |

### Add and manage protected registry keys

- Open the 'Containment' section of a profile
- Click the 'Protected Data' tab.
- Click 'Add'

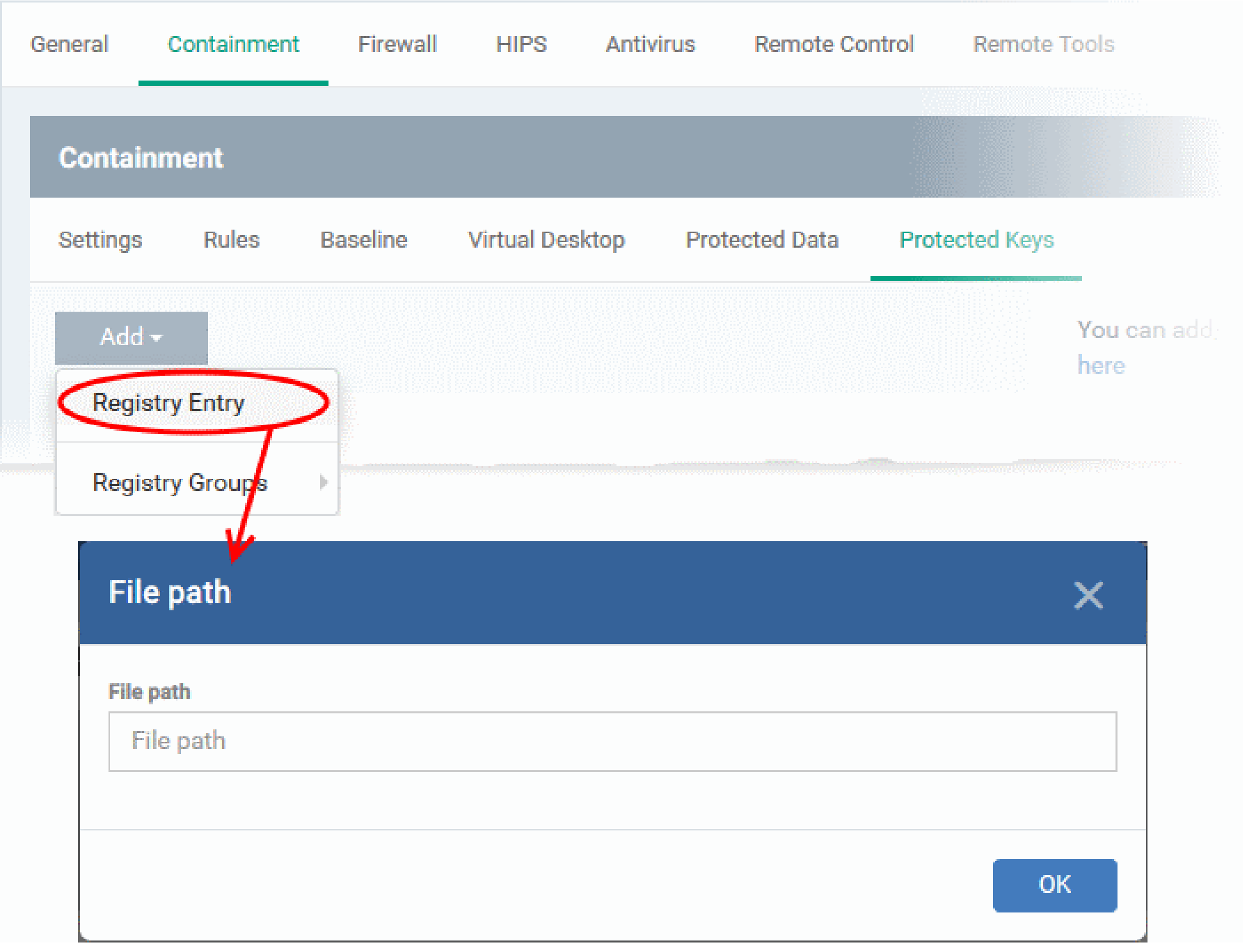


You add items in two ways:

- **Registry Entry** - Add individual keys
- **Registry Groups** - Add a pre-defined group of registry keys so that all member keys in the group are blocked form contained applications

### Add registry keys

- Choose 'Registry Entry' from the 'Add' drop-down

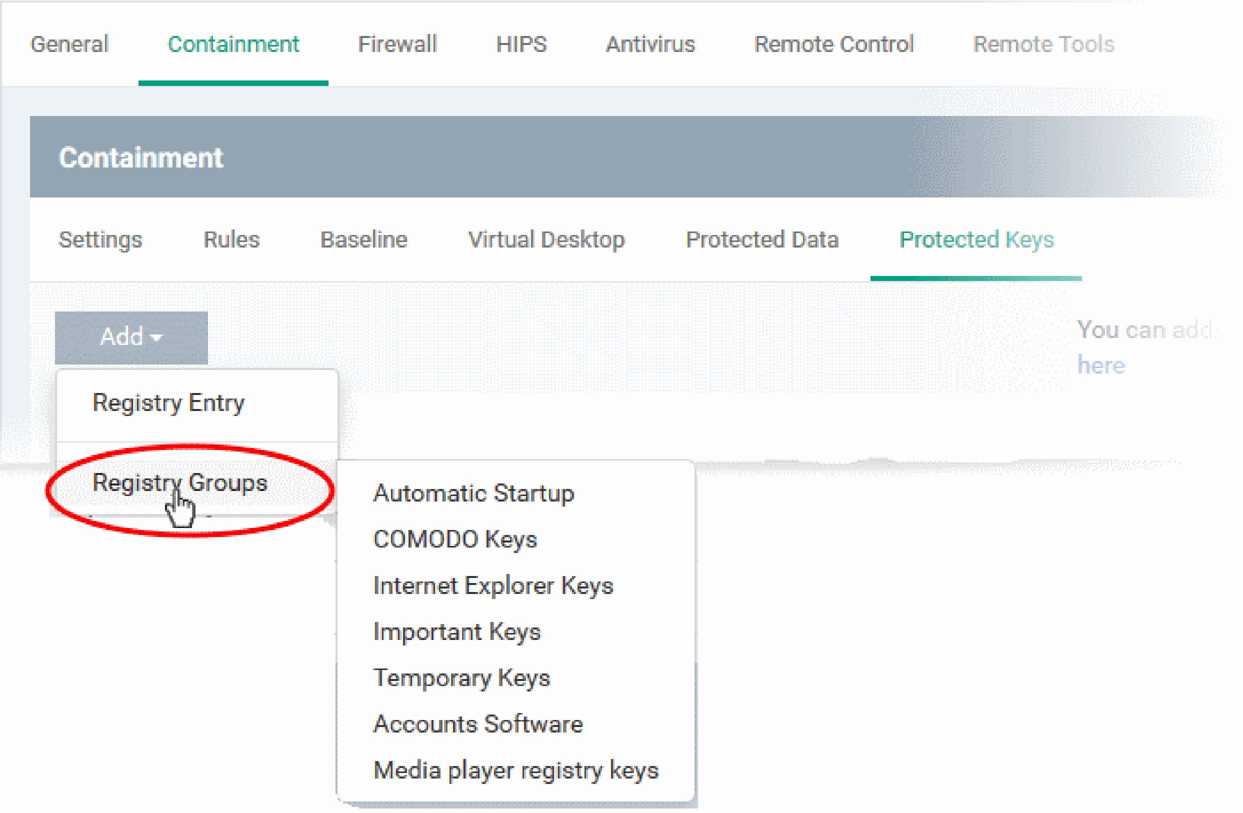


- Enter the location of an individual key that you want to protect and click 'OK'.
- Repeat the process to add more items

**Add registry groups**

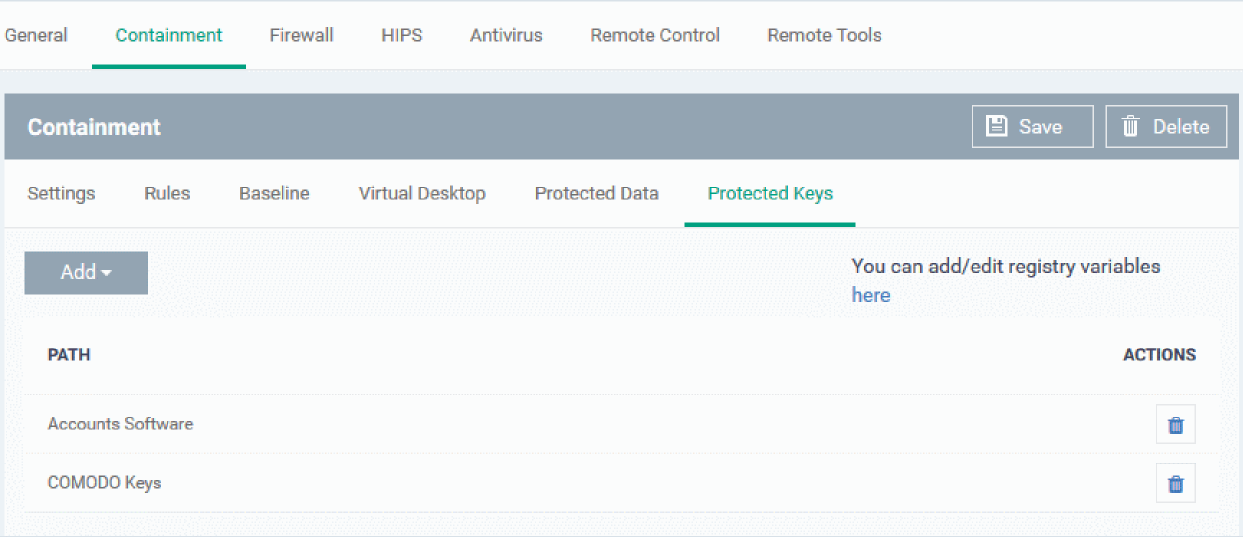
A registry group is a collection keys with similar scope or functionality.Endpoint Manager ships with a set of registry groups. You can create custom registry groups from the 'Settings' > 'System Templates' > Registry Variables' interface. See **Create and Manage Registry Groups** for more details.

- Choose 'Registry Group' from the 'Ádd' drop-down



- Choose a group to be protected
- Repeat the process to add more groups

The items added are shown as a list under the 'Protected Keys' tab.



| PATH | ACTIONS |
|---|---|
| Accounts Software | 🗑 |
| COMODO Keys | 🗑 |

- You can edit or remove the items using the respective buttons in the 'Action' column in the 'Protected Keys' interface.
- Click 'Save' for your settings to take effect.

### 6.1.3.1.7. Maintenance Window Settings

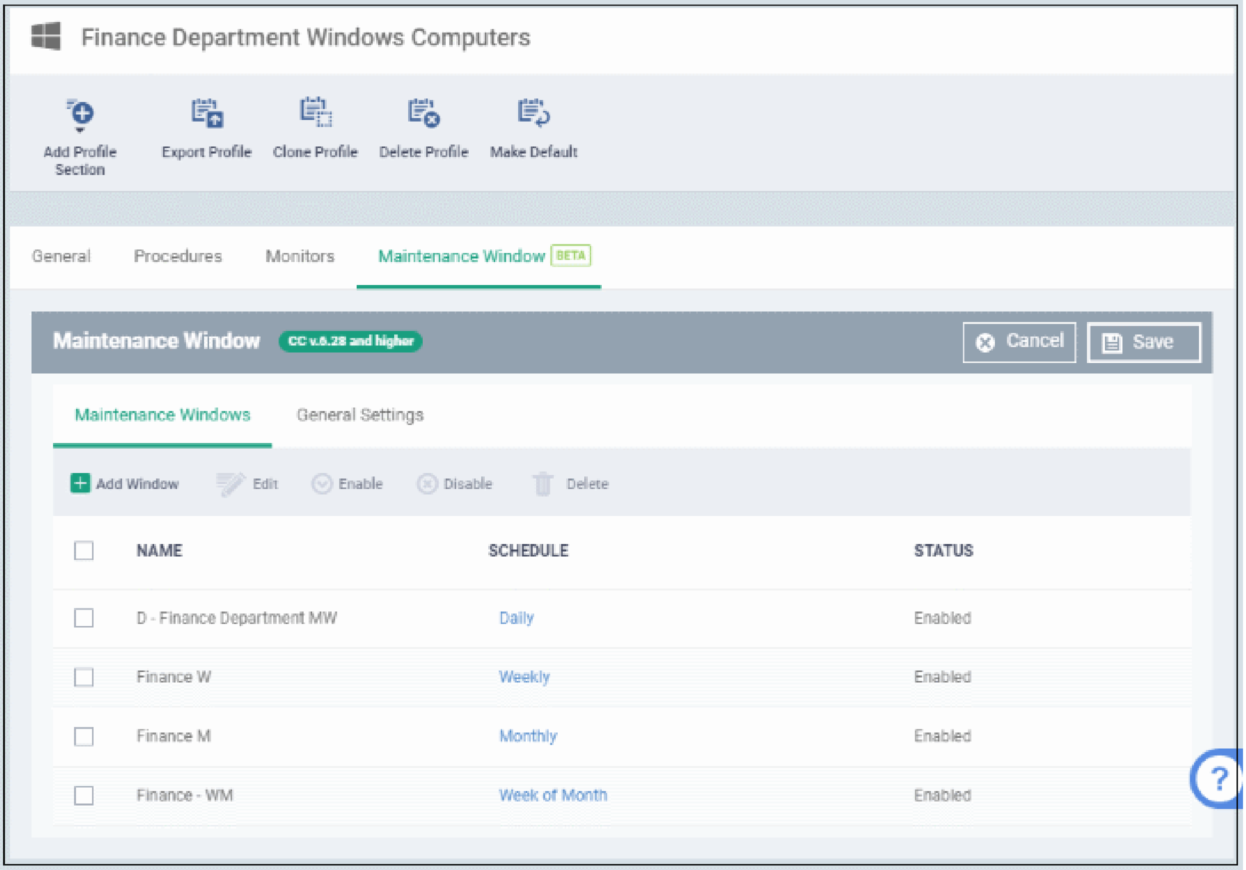
- A maintenance window is a scheduled time-slot when your Endpoint Manager procedures will run. You can create them by adding a 'Maintenance Window' section to a Windows profile.
- Once created, you can assign the maintenance window to a procedure in the **procedure settings**. You can assign multiple procedures to the same maintenance window.

- You can also add multiple maintenance windows to a profile. This lets you assign different procedures to different time-slots.
- You have the option to pause all running **monitors** while the maintenance window runs, and to randomize task start times to avoid system congestion.
- You can block certain tasks from running outside of a maintenance window. Example tasks include remote control sessions, patch installation and more.
    - Alternatively, you can show a warning to the admin which asks if they want to move the task to the maintenance window instead.
- You can define times when maintenance windows should not run. For example, holidays, weekends or other occasions.

### Create a maintenance window

- Click 'Configuration Templates' > 'Profiles'
- Click the name of a Windows profile
- Click 'Add Profile Section' > 'Maintenance Window'

The maintenance windows screen opens:



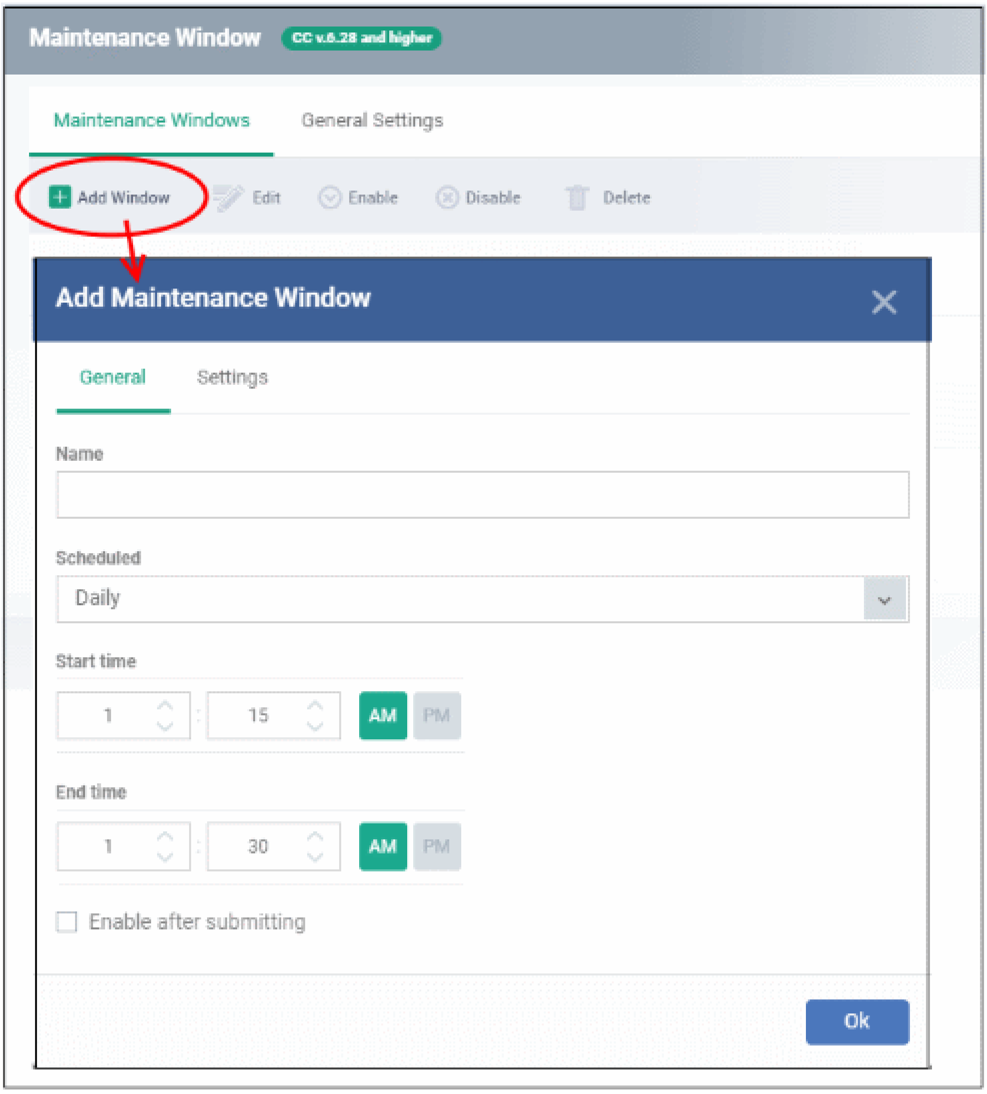
| | NAME | SCHEDULE | STATUS |
|---|---|---|---|
| □ | D - Finance Department MW | Daily | Enabled |
| □ | Finance W | Weekly | Enabled |
| □ | Finance M | Monthly | Enabled |
| □ | Finance - WM | Week of Month | Enabled |

Click the following links for more info on each tab:

- **Maintenance Window** (MW) - Configure the time-slot and settings you want to use.
- **General Settings** - Choose whether to randomize tasks and/or define no-maintenance times.

## Create a Maintenance Window

- Click 'Add Window' (or 'Edit' then 'Add Window')



Name

Scheduled: Daily

Start time: 1 : 15 AM

End time: 1 : 30 AM

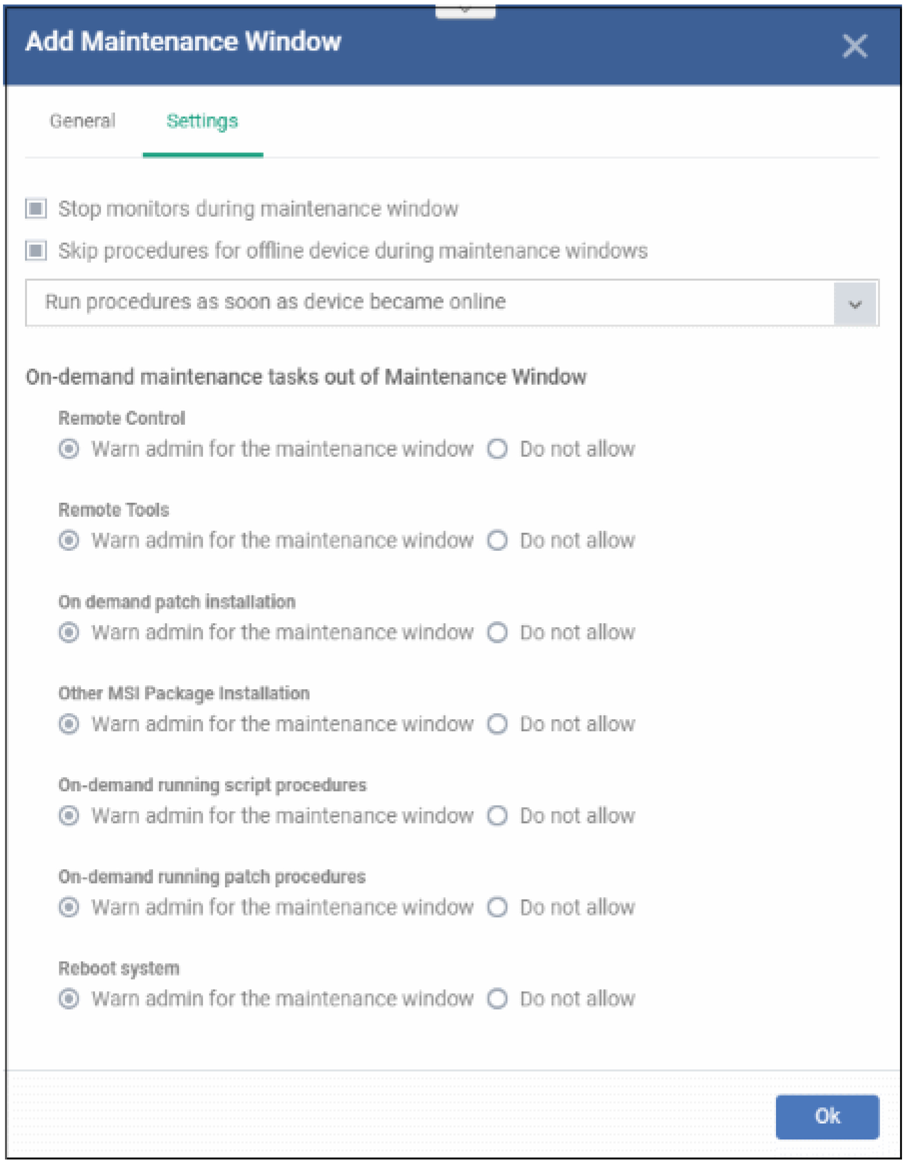
□ Enable after submitting

You can define a time-slot and additional settings for each maintenance window.

- **General** - Configure when the maintenance window should run.
    - **Name** - Create a label for the window. For example, 'Maintenance Window - 11 PM to 1 AM'

- **Scheduled -** Choose how often you want to run the maintenance:
  - Daily - Select the start and end time of the window. The window runs every day at the time you set.
  - Weekly - Select the start and end times, and the days of the week that the window should run.
  - Monthly - Select the start and end times, and the days of the month that the window should run.
  - Week of Month - Select the start and end times, the week number, and the days that the window should run. Use this, for example, if you want to run the window once every two weeks.
- **Enable after submitting -** Make the window available for use after clicking 'OK'. Only enabled windows are available for selection with procedures.

- **MW Settings -** Configure additional settings for the MW. Click the 'Settings' tab.



Add Maintenance Window

General | Settings

☑ Stop monitors during maintenance window

☑ Skip procedures for offline device during maintenance windows

Run procedures as soon as device became online

On-demand maintenance tasks out of Maintenance Window

Remote Control
● Warn admin for the maintenance window ○ Do not allow

Remote Tools
● Warn admin for the maintenance window ○ Do not allow

On demand patch installation
● Warn admin for the maintenance window ○ Do not allow

Other MSI Package Installation
● Warn admin for the maintenance window ○ Do not allow

On-demand running script procedures
● Warn admin for the maintenance window ○ Do not allow

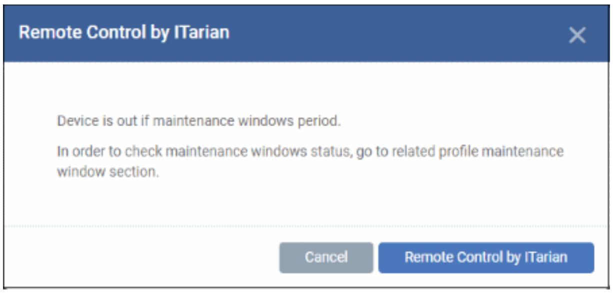
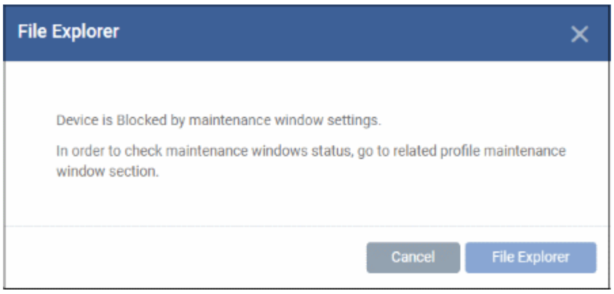
On-demand running patch procedures
● Warn admin for the maintenance window ○ Do not allow

Reboot system
● Warn admin for the maintenance window ○ Do not allow

- **Stop monitors during maintenance window -** Pause all monitors on a device for the duration of the maintenance window.
- **Skip procedures for offline device during maintenance windows:**

  - **Run procedure as soon as device became online** - The procedure is executed when the device is next connects to Endpoint Manager.
  - **Run procedure during the nearest maintenance window** - The procedure is executed in the next available window after the device comes online.
- **On-demand maintenance tasks out of Maintenance Window** - Endpoint Manager can block or show a warning if someone tries to run tasks outside of a maintenance window. You can warn/block the following tasks:
  - Remote control
  - Remote tools
  - On-demand patch installation
  - Other MSI package installation
  - On-demand running script procedures
  - On-demand running patch procedures
  - Reboot system

Example block/warn messages are shown below:

| Alert | Blocked |
|---|---|
| <br> Remote Control by ITarian<br>Cancel<br>Remote Control by ITarian<br>Device is out if maintenance windows period.<br>In order to check maintenance windows status, go to related profile maintenance window section. | <br> <br>Device is Blocked by maintenance window settings.<br>In order to check maintenance windows status, go to related profile maintenance window section. |

- Click 'OK'

Repeat the procedure to add more maintenance windows.

### Edit a MW

- Select a MW and click 'Edit' at the top. The procedure is similar to adding explained above.

### Enable / Disable

- Select a MW and click 'Enable / Disable' at the top. Note - Only active MWs are available for selection.

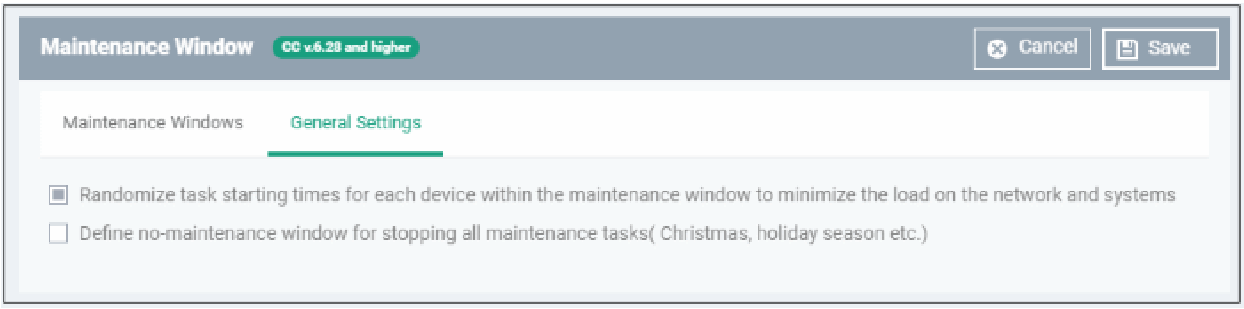
### Delete

- Select a MW and click 'Delete' at the top. Note - You cannot delete MWs that are in use.

## Configure MW General Settings

These settings apply to all maintenance windows in the profile.

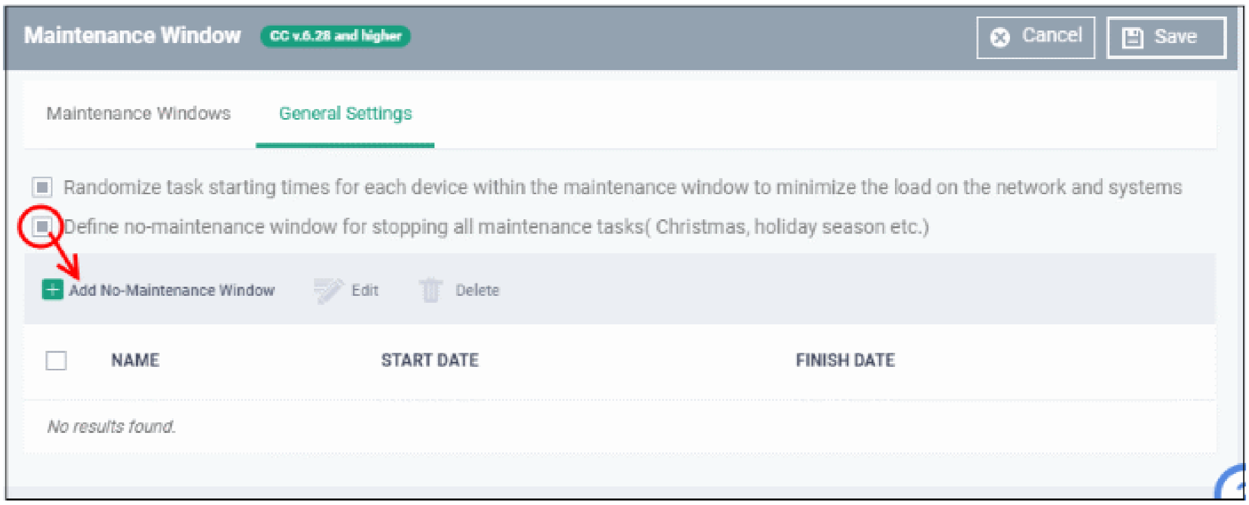
- Click the 'General Settings' tab



☑ Randomize task starting times for each device within the maintenance window to minimize the load on the network and systems

☐ Define no-maintenance window for stopping all maintenance tasks( Christmas, holiday season etc.)

- **Randomize task starting times for each device within the maintenance window to minimize the load on the network and systems** - Staggers task start-times to prevent several procedures running at the same time on each device. This can ease congestion and lead to a smoother roll-out of your procedures.
- **Define no-maintenance window for stopping all maintenance tasks** - Configure periods during which maintenance windows should not run. For example, during holidays.

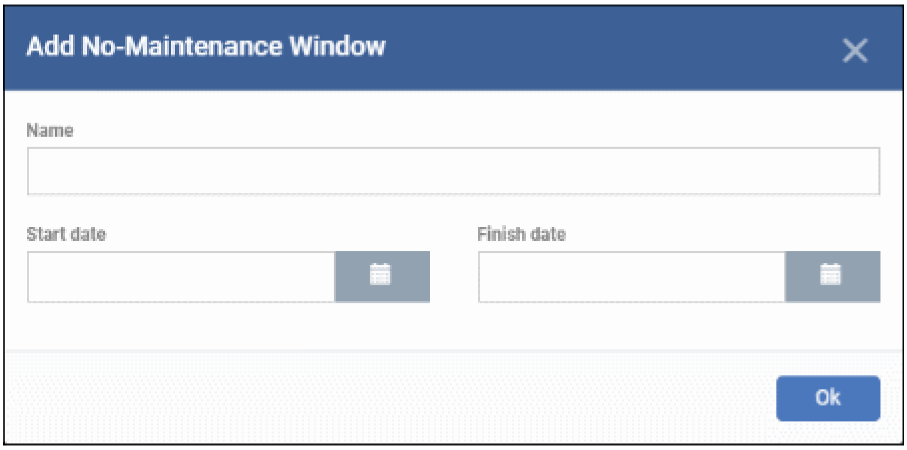


☑ Randomize task starting times for each device within the maintenance window to minimize the load on the network and systems

☑ Define no-maintenance window for stopping all maintenance tasks( Christmas, holiday season etc.)

| ☐ | NAME | START DATE | FINISH DATE |
|---|---|---|---|
| No results found. | | | |

- Click 'Add No-Maintenance Window'



- Name - Provide an appropriate label for the no-MW. For example, 'New year holiday'.
- Start and Finish dates - Select from the calendar or enter the start and end period.
- Click 'Ok'

Repeat the process to add more no-maintenance windows.

**Edit a no-MW**

- Select an item, click 'Edit' and update as explained above

**Delete a no-MW**

- Select an item and click 'Delete'

- Click 'Save' to apply your changes

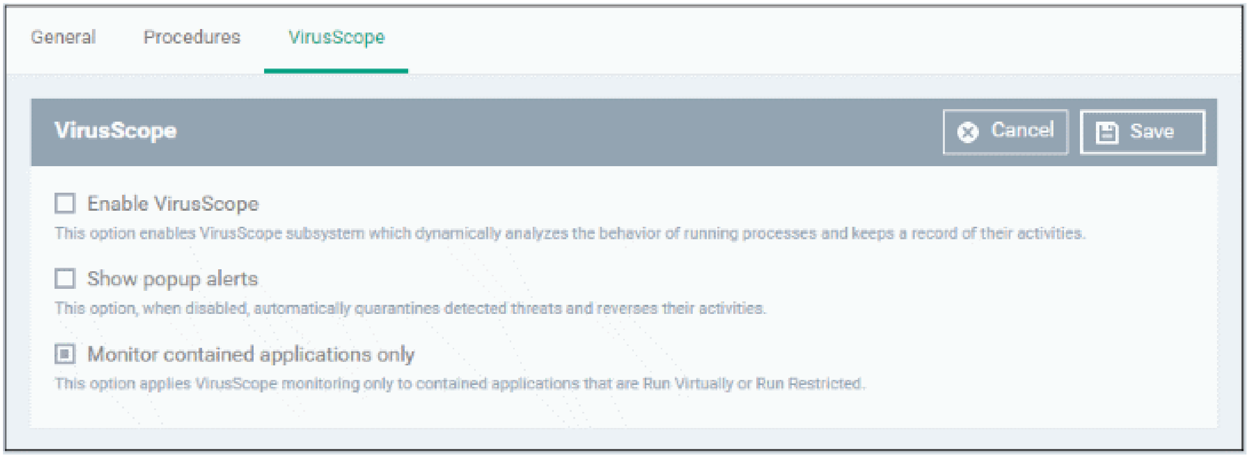
### 6.1.3.1.8. VirusScope Settings

- 'VirusScope' is a CCS feature which closely monitors the activities of running processes and generates alerts if they take threatening actions.
- The feature uses a system of 'recognizers' to detect malicious behavior and thus identify brand-new malware.
- VirusScope alerts offer the choice to quarantine the process & undo its changes, or let the process go ahead.
- You can choose whether VirusScope should monitor all processes, or only contained processes.

**To configure VirusScope settings**

- Click 'Configuration Templates' > 'Profiles'
- Click the name of a Windows profile
- Click 'Add Profile Section' > 'VirusScope'

The VirusScope settings screen will open:



□ Enable VirusScope

This option enables VirusScope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

□ Show popup alerts

This option, when disabled, automatically quarantines detected threats and reverses their activities.

☒ Monitor contained applications only

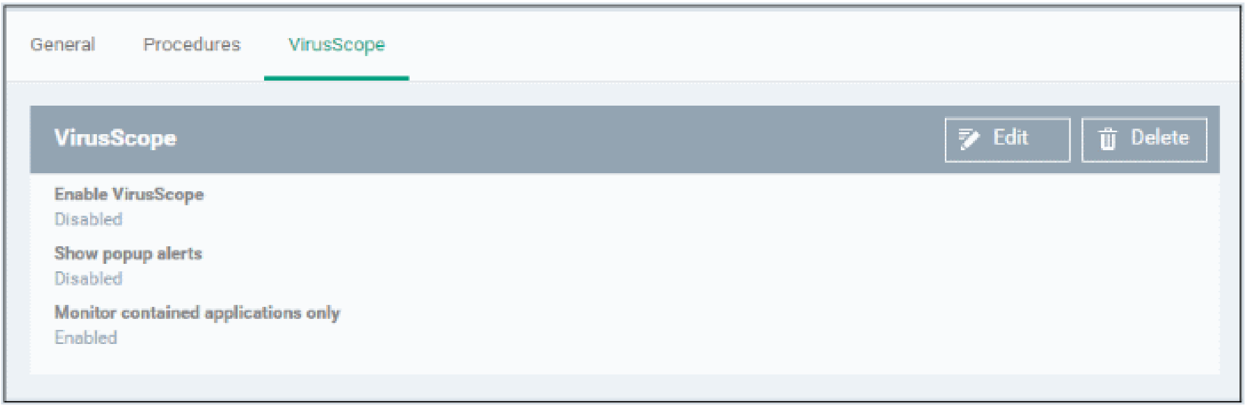
This option applies VirusScope monitoring only to contained applications that are Run Virtually or Run Restricted.

| VirusScope Configuration - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Enable Viruscope | Enable or disable Viruscope. If enabled, Viruscope monitors the activities of all running processes and generates alerts on suspicious activities |
| Show popup alerts | Configure whether or not alerts are shown to end-users when suspicious activity is detected.<br>• Disabling alerts will minimize disturbances but at some loss of user awareness.<br>• If you disable alerts then threats are automatically quarantined and their activities are reversed. |

| VirusScope Configuration - Table of Parameters | |
|---|---|
| Monitor contained applications only | Choose whether VirusScope should track every process on the host, or only processes which are running in the container. |

- Click the 'Save' button.

The VirusScope component will be added to the Windows profile.



Enable VirusScope
Disabled

Show popup alerts
Disabled

Monitor contained applications only
Enabled

The saved 'VirusScope' settings screen will be displayed with options to edit the settings or delete the section. See **Edit Configuration Profiles** for more details.

### 6.1.3.1.9. Valkyrie Settings

- Valkyrie is a cloud-based file verdict service that subjects unknown files to a range of tests in order to identify those that are malicious.
- Comodo Client Security can automatically submit unknown files to Valkyrie for analysis. When the tests are complete, Valkyrie will award a trust verdict to the file.
- You can view the verdicts at 'Security Sub-Systems' > 'Valkyrie'
  - See **View list of Valkyrie Analyzed Files** for more details.
- Click 'Dashboard' > 'Valkyrie' to view summary of all Valkyrie results.

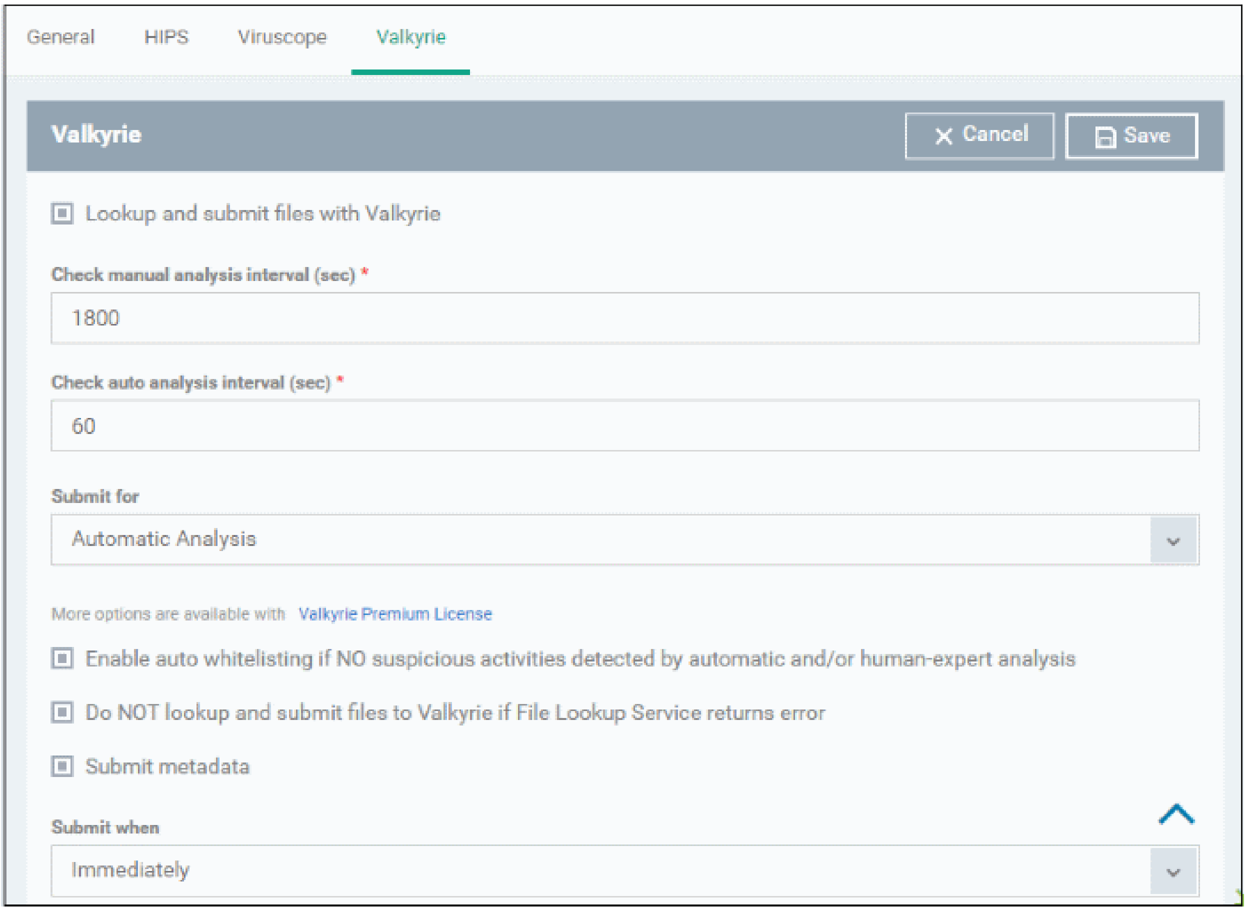
**Note**: The Valkyrie that comes with the free version of Endpoint Manager will only run automated tests on an unknown file. The Premium version also includes manual testing by Comodo research technicians.

You can configure general Valkyrie settings and create an analysis schedule in the Valkyrie component of a Windows profile.

**Configure Valkyrie Settings**

- Click 'Valkyrie' from the 'Add Profile Section' drop-down in the Windows Profile interface

The 'Valkyrie' settings screen will be displayed.



☐ Lookup and submit files with Valkyrie

Check manual analysis interval (sec) *
1800

Check auto analysis interval (sec) *
60

Submit for
Automatic Analysis

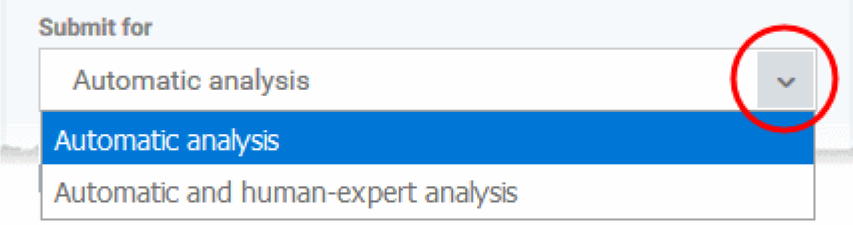
More options are available with Valkyrie Premium License

☐ Enable auto whitelisting if NO suspicious activities detected by automatic and/or human-expert analysis

☐ Do NOT lookup and submit files to Valkyrie if File Lookup Service returns error

☐ Submit metadata

Submit when
Immediately

| Valkyrie Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Lookup and Submit Files with Valkyrie | Choose this option if you want the files to be submitted to the cloud file lookup service |
| Check Manual Analysis Interval (sec)* | How often CCS should contact Valkyrie for the verdicts on files submitted for manual analysis. (Default=60) |
| Check Auto Analysis Interval (sec)* | How often CCS should contact Valkyrie for the verdicts on files submitted for automatic analysis. (Default=60) |
| Submit for | Choose the type of Valkyrie analysis.<br><br>Submit for<br>Automatic analysis<br>Automatic analysis<br>Automatic and human-expert analysis<br>- **Automatic analysis** - Unknown files are only tested by Valkyrie's automatic testing service. |

| Valkyrie Settings - Table of Parameters | |
|---|---|
| | - **Automatic and human-expert analysis -** Unknown files are tested by Valkyrie's automatic testing service, and then by Comodo research lab technicians. Available only for premium license holders. |
| Enable Auto Whitelisting if NO suspicious activities detected by Automatic and/or Human-Expert analysis | Choose this option if you wish the files identified as harmless by Valkyrie to be added to your local whitelist. |
| Do NOT lookup and submit files to Valkyrie if File Lookup Service returns error | Choose this option, if you don't want Valkyrie file analysis in case file look up service (FLS) failed. |
| 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 When | Choose when the unknown files are to be submitted. The options available are:<br>Immediately - CCS uploads the file to Valkyrie as soon as it encounters an Unknown file<br>Schedule Analysis - CCS accumulates the unknown files and uploads them as per the set schedule. Refer to **Valkyrie Analysis Schedule** about how to set analysis schedule. |

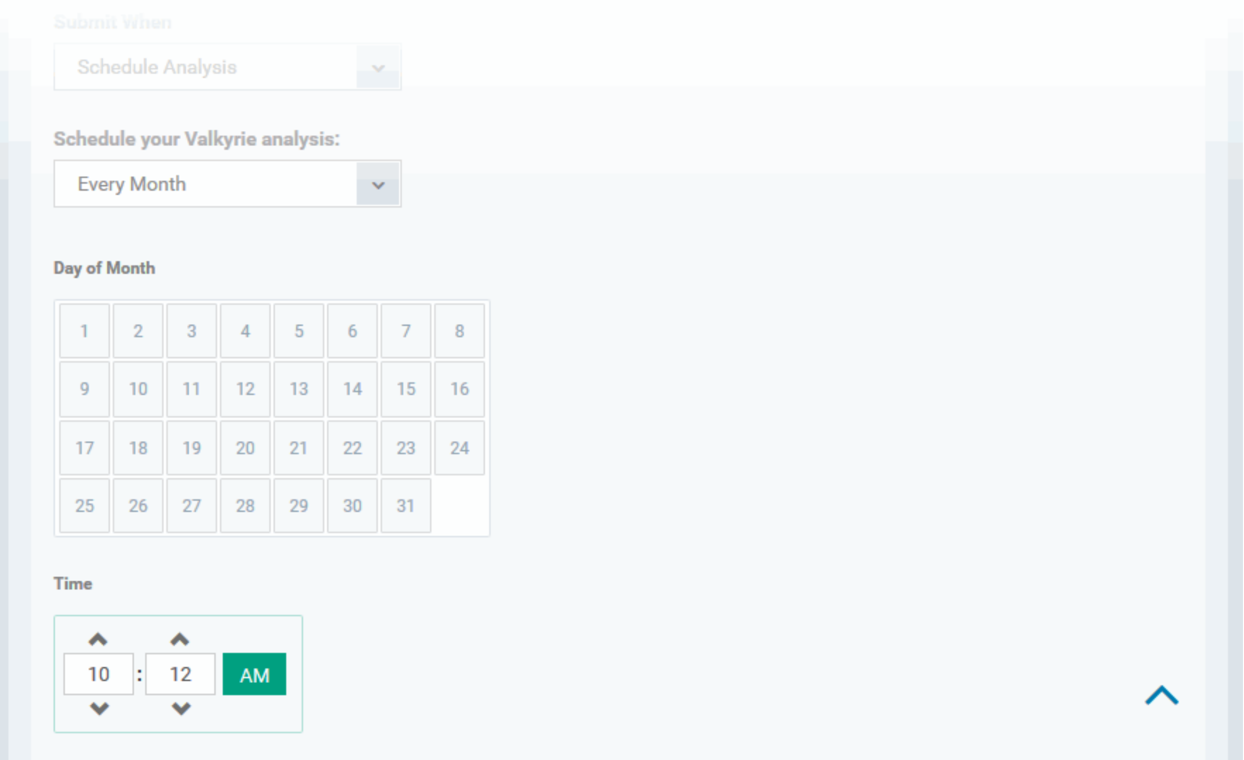
Fields marked * are mandatory.

- The 'Valkyrie Premium License' link takes to Valkyrie signup page for a full subscription.

## Valkyrie Analysis Schedule

The Valkyrie allows you to create a schedule for CCS to upload unknown files.

- Select 'Schedule Analysis' from the 'Submit When' drop-down.



Submit When

Schedule Analysis

Schedule your Valkyrie analysis:

Every Month

Day of Month

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |   |

Time

10 : 12 AM

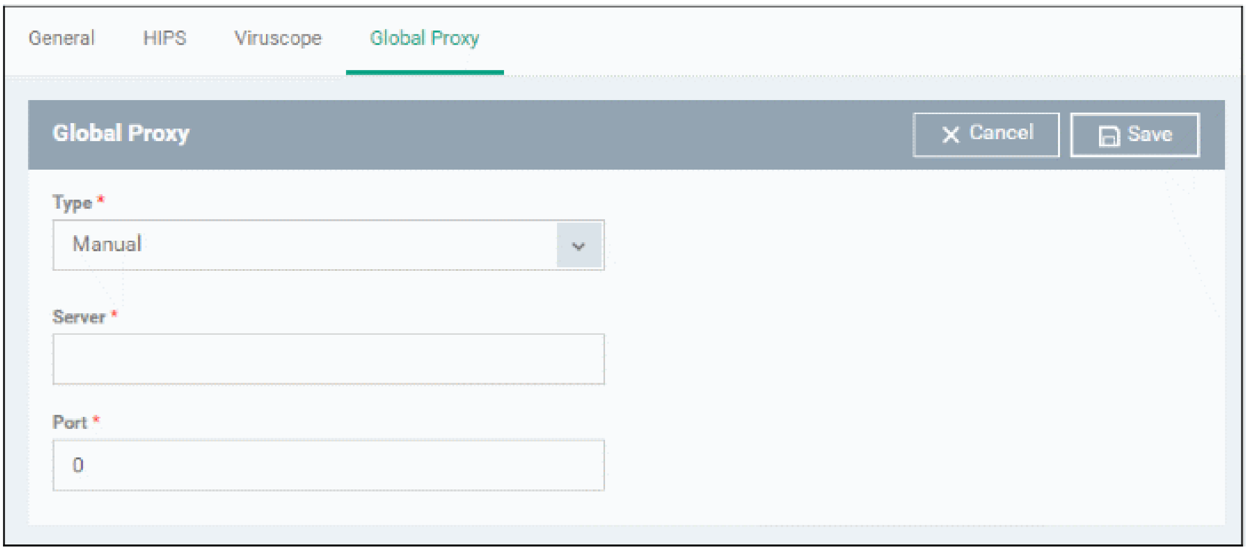
- To upload the unknown files daily choose 'Daily' from the drop-down at the top and set the time for upload in HH:MM format in the combo boxes under 'Time'.
- To upload the unknown files once per week, choose 'Every Week' from the drop-down at the top. Choose the day of the week from the 'Day of Week' options and set the time for upload in HH:MM format in the combo boxes under 'Time'.
- To upload the unknown files monthly, choose 'Every Month' from the drop-down at the top, choose the day of the month from the 'Day of month' options and set the time for upload in HH:MM format in the combo boxes under 'Time'.

### 6.1.3.1.10. Global Proxy Settings

The Global Proxy settings allows you to specify a proxy server through which applications in endpoints using this profile should connect to external network such as the internet. Please note the setting done here will not affect how Comodo Client Security (CCS) and the Communication Client (CC) in the endpoints connect to Endpoint Manager and Comodo servers. The proxy setting for CCS and CC are done in the **Client Proxy** section.

**Configure Global Proxy Settings**

- Click 'Global Proxy' from the 'Add Profile Section' drop-down in the Windows Profile interface



Type *
Manual

Server *

Port *
0

| Global Proxy Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Type * | Select the kind of the proxy setting. Choice = automatic or manual. |
| Pac Url* | This field is shown if 'Auto' is selected in the 'Type' field. Enter the path to your proxy auto-config file. |
| Server * | This field is shown if 'Manual' is selected in the 'Type' field. Enter the address of your proxy server. |
| Port * | This field is shown if 'Manual' is selected in the 'Type' field. Enter the port number of the proxy. If you do not have a set port number, port 8080 will work in many cases. |

* - options are mandatory.

- Click 'Save' in the title bar to save your update settings to the profile.

### 6.1.3.1.11. Client Proxy Settings

- The client proxy section lets you choose a proxy through which Comodo clients should connect to Endpoint Manager and other Comodo services. If you do not set a proxy then CCS and CC will use a direct connection.
- The proxy you set here only affects the connections of Endpoint Manager clients. It does not affect how other applications on the endpoint connect to the internet. If required, you can set a proxy for all other applications in the **Global Proxy** section of a profile.
- You can specify different proxies for CC and CCS if required.
- **Note**. If you use the **bulk enrollment wizard** to create an installer, make sure you specify the same proxy during the enrollment wizard. If the proxy settings used in the installer differ to those in the profile, then the connection to EM will be lost after first successful connection.

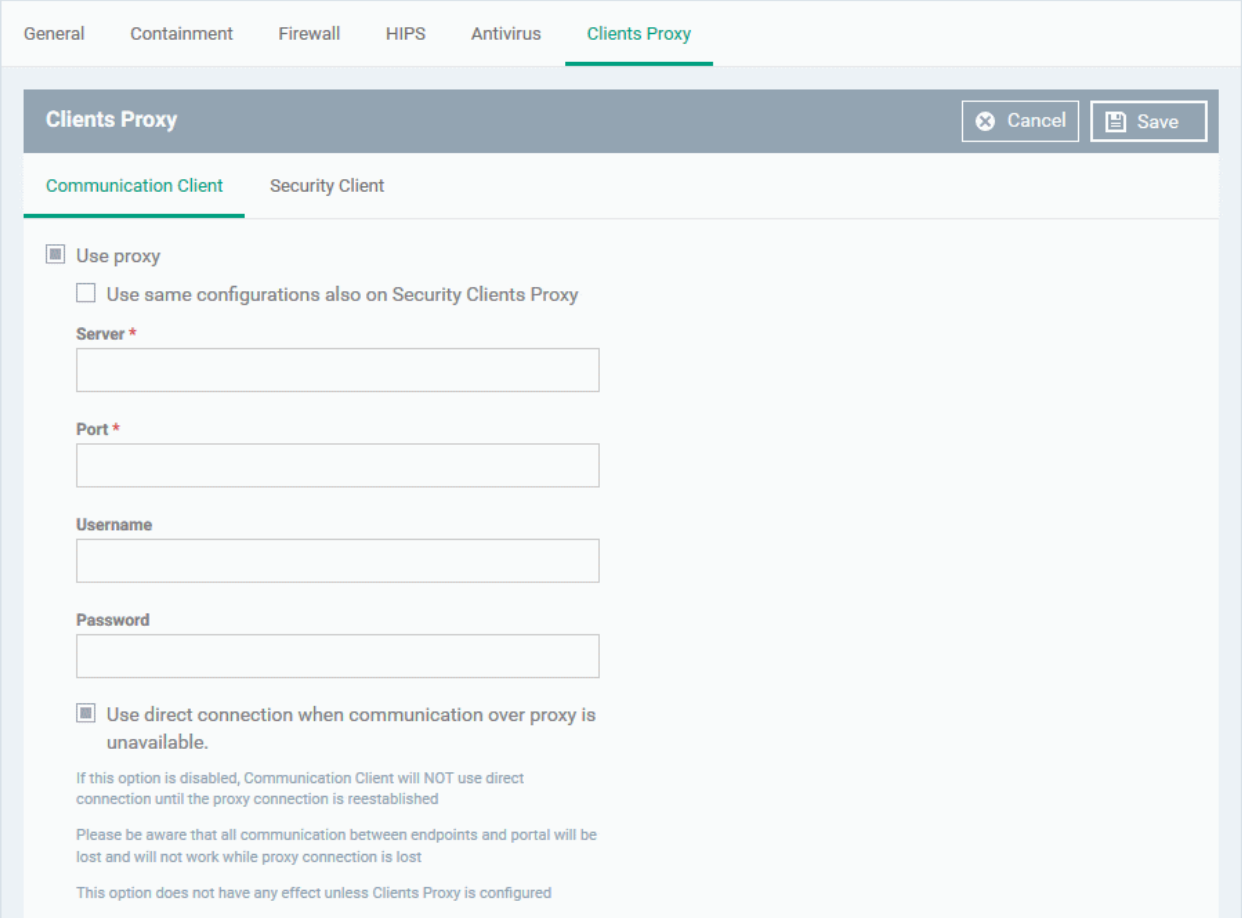
**Configure Client Proxy Settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile you want to work on

- Click the 'Clients Proxy' tab

  OR

- Click 'Add Profile Section' > 'Clients Proxy', if it hasn't yet been added
- Click 'Clients Proxy' from the 'Add Profile Section' drop-down in the Windows Profile interface



☒ Use proxy

□ Use same configurations also on Security Clients Proxy

Server *

Port *

Username

Password

☒ Use direct connection when communication over proxy is unavailable.

If this option is disabled, Communication Client will NOT use direct connection until the proxy connection is reestablished

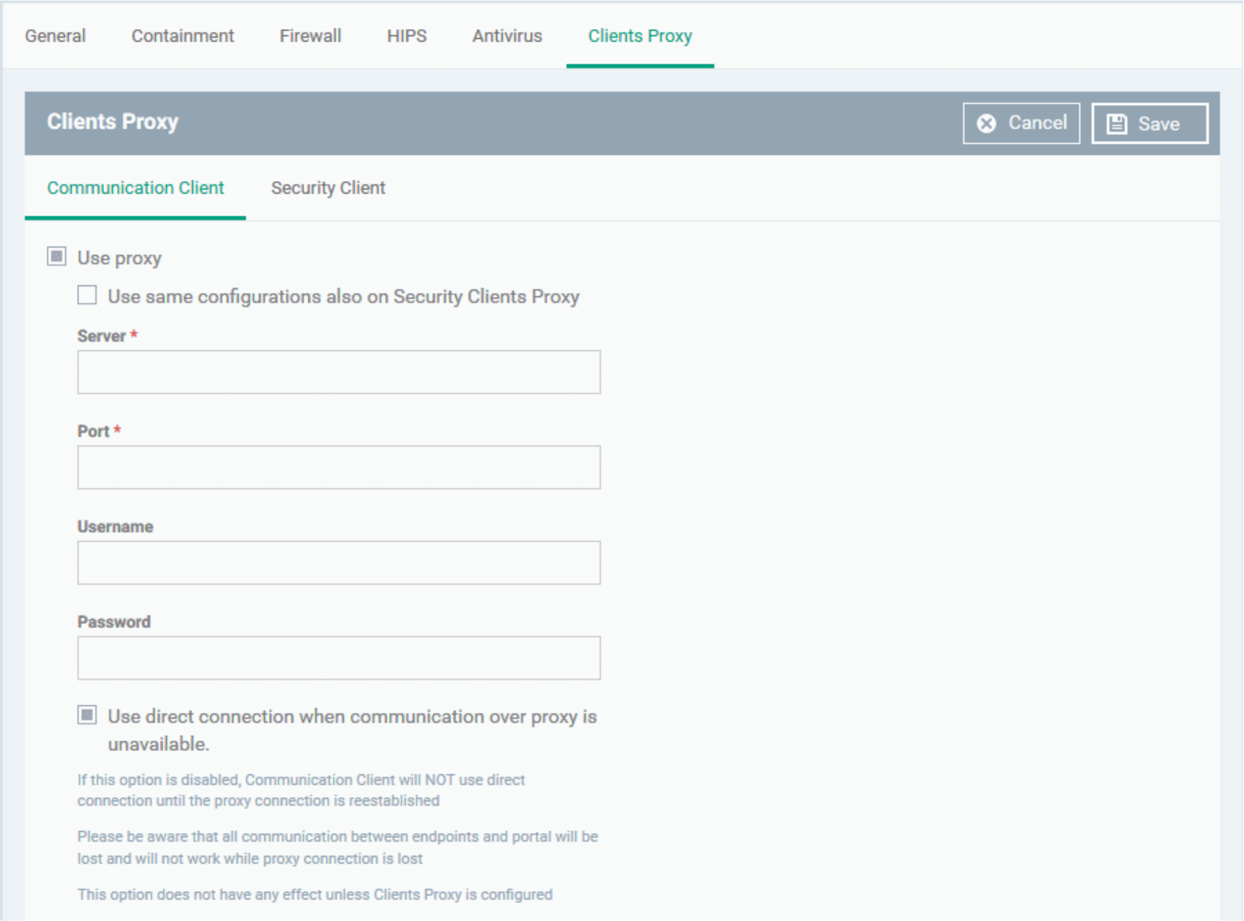
Please be aware that all communication between endpoints and portal will be lost and will not work while proxy connection is lost

This option does not have any effect unless Clients Proxy is configured

The settings screen has two tabs:

- **Communication client** - Specify the proxy for the communication client (CC). CC will use this proxy to connect to Endpoint Manager and other Comodo services.
- **Security client** - Specify the proxy server for Comodo Client Security (CCS). CCS will use this proxy to connect to Comodo servers for program and database updates.

**Communication Client**:



☒ Use proxy

□ Use same configurations also on Security Clients Proxy

Server *

Port *

Username

Password

☒ Use direct connection when communication over proxy is unavailable.

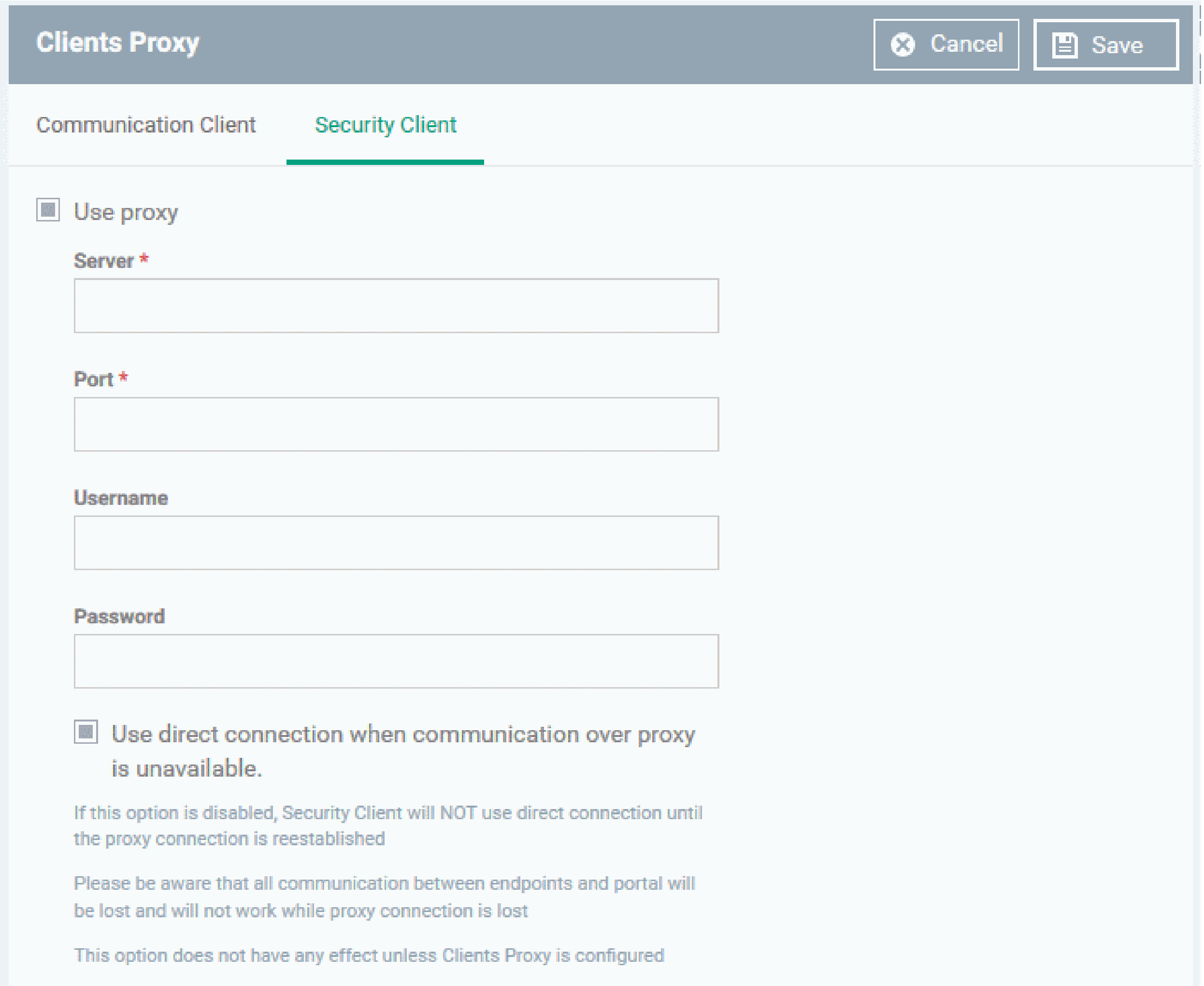
If this option is disabled, Communication Client will NOT use direct connection until the proxy connection is reestablished

Please be aware that all communication between endpoints and portal will be lost and will not work while proxy connection is lost

This option does not have any effect unless Clients Proxy is configured

- **Use Proxy** - The communication client will connect to EM and other Comodo services through a proxy server (***Default = Disabled***)
  - **Use same configurations also on Security Clients Proxy** - CCS will use the same proxy you configure for the communication client. (***Default = Disabled***)
- **Server** - Enter the IP address or hostname of your proxy server
- **Port** - The port on your proxy that CC should connect to. If you do not have a set port number, port 8080 will work in many cases.
- **Username/Password** - If your proxy requires authentication, enter the admin credentials here.
- **Use direct connection when communication over a proxy is unavailable** - Allow CC to fallback to a direct internet connection if the proxy fails.
  - If you specify a proxy BUT disable direct connections, then your endpoints will not be able to connect to EM if the proxy fails.
  - Leave the direct connection option enabled to ensure your devices are managed at all times.

**Security Client**:



☐ Use proxy

Server *

Port *

Username

Password

☐ Use direct connection when communication over proxy is unavailable.

If this option is disabled, Security Client will NOT use direct connection until the proxy connection is reestablished

Please be aware that all communication between endpoints and portal will be lost and will not work while proxy connection is lost

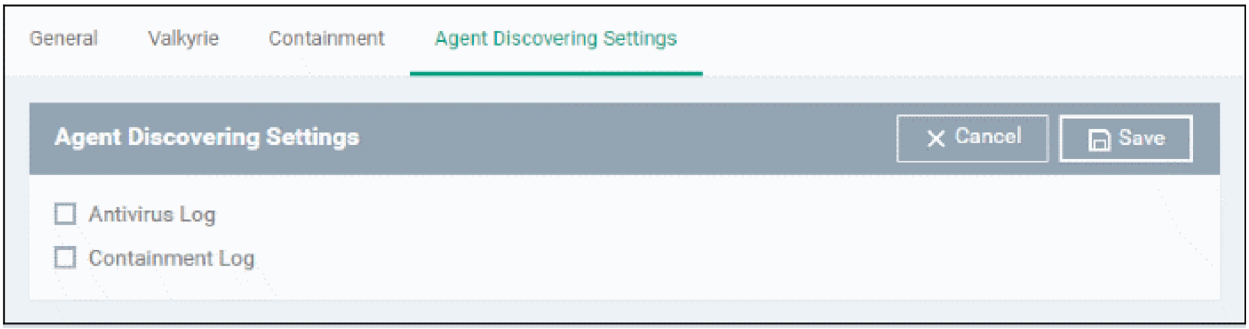
This option does not have any effect unless Clients Proxy is configured

- **Use Proxy -** Comodo Client Security (CCS) will connect to Endpoint Manager and update servers through a proxy.
- **Server -** Enter the IP address or hostname the proxy server
- **Port -** The port on your proxy that CCS should connect to. If you do not have a set port number, port 8080 will work in many cases.
- **Username/Password -** If your proxy requires authentication, enter the admin credentials here.
- **Use direct connection when communication over a proxy is unavailable -** Allow CCS to fallback to a direct internet connection if the proxy fails.
  - If you specify a proxy BUT disable direct connections, then CCS will not be able to connect if the proxy fails.
  - Leave the direct connection option enabled to ensure CCS is connected and up-to-date at all times.

Click 'Save' to apply your changes to the profile. The new settings will be automatically deployed to all endpoints on which the profile is active.

### 6.1.3.1.12. Agent Discovery Settings

The agent discovery Settings lets you specify whether or not CCS should log antivirus and containment events on the endpoint.



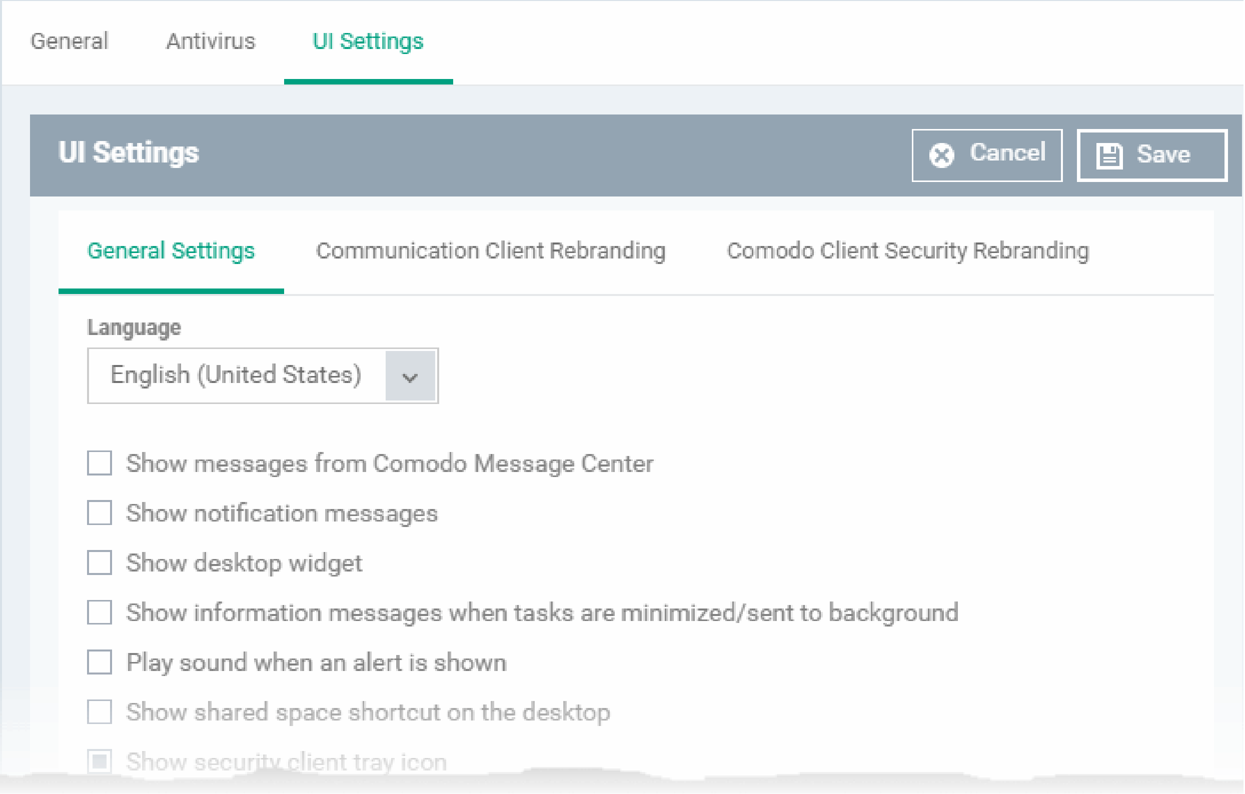
- Antivirus Log - Select this option if antivirus log is to be enabled
- Containment Log - Select this option if containment log is to be enabled
- Click 'Save' to apply your changes.

### 6.1.3.1.13. Communication Client and Comodo Client - Security Application UI Settings

- The UI settings screen lets you configure the appearance of Communication Client (CC), Comodo Client Security (CCS) and the Virtual Desktop.
- You can re-brand these items with your own company name, logo, product name and product logo. In addition, you can:
  - Add your support website, phone number and email to the GUI
  - Select which components of CCS should be visible to end-users in the GUI

**Configure UI settings**

- Click 'Configuration Templates' > 'Profiles'
- Click the Windows profile in which you want to configure UI appearance
  - Click 'Add Profile Section' > 'UI Settings'

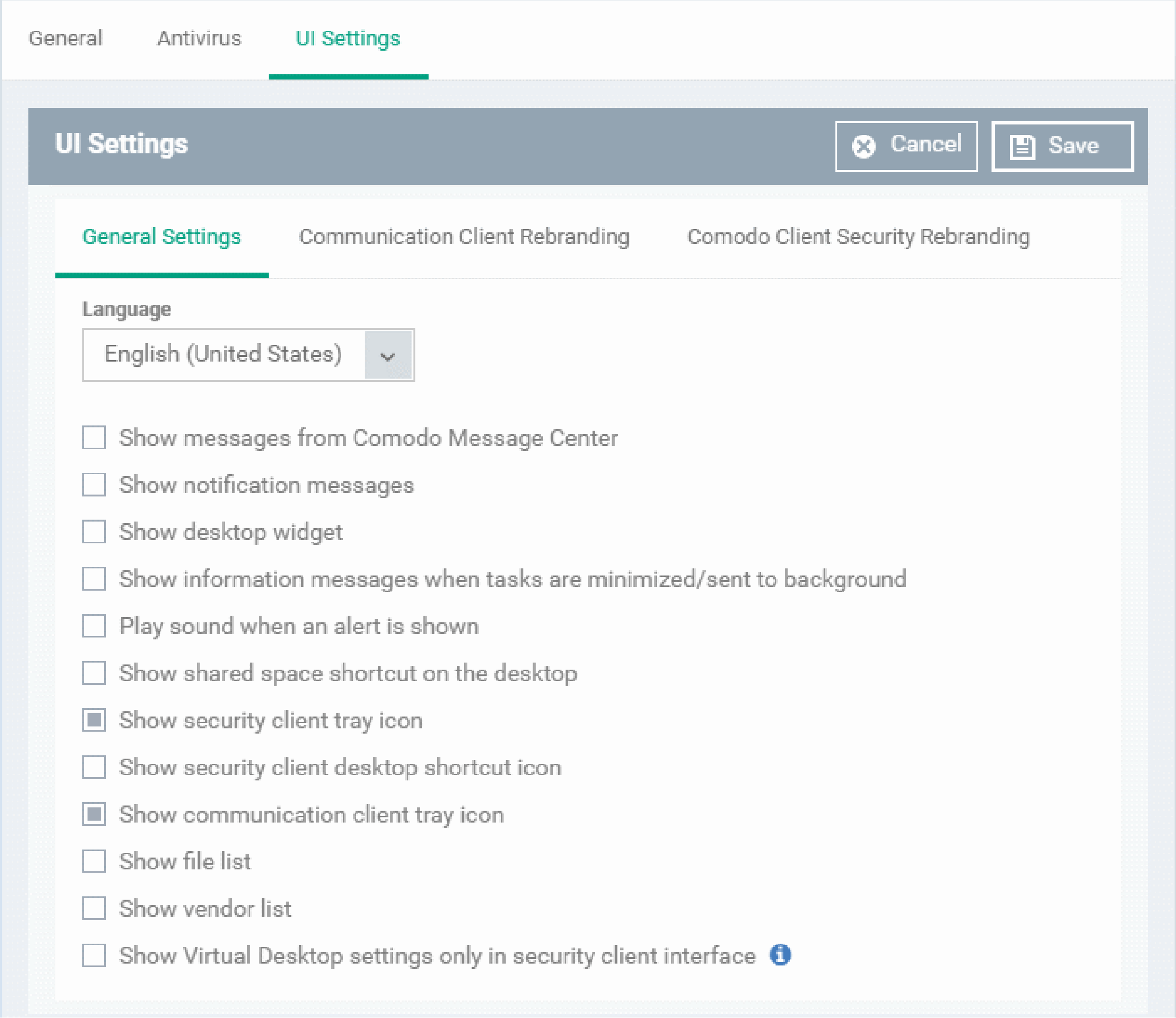

General
Antivirus
UI Settings
UI Settings
Cancel
Save
General Settings
Communication Client Rebranding
Comodo Client Security Rebranding
Language
English (United States)
Show messages from Comodo Message Center
Show notification messages
Show desktop widget
Show information messages when tasks are minimized/sent to background
Play sound when an alert is shown
Show shared space shortcut on the desktop
Show security client tray icon

The UI settings screen has three tabs:

- **General Settings** - Select GUI language and which components/shortcuts are shown in the interface to the end-user.
- **Communication Client Rebranding** - Customize CC with your own brand name, company logo and more.
- **Comodo Client Security Rebranding** - Customize CCS and VD with your own brand name, company logo and more.

## General Settings

- Open the 'UI Settings' section of a profile
- Click the 'General Settings' tab:



General
Antivirus
UI Settings
UI Settings
Cancel
Save
General Settings
Communication Client Rebranding
Comodo Client Security Rebranding

Language: English (United States)

□ Show messages from Comodo Message Center
□ Show notification messages
□ Show desktop widget
□ Show information messages when tasks are minimized/sent to background
□ Play sound when an alert is shown
□ Show shared space shortcut on the desktop
☑ Show security client tray icon
□ Show security client desktop shortcut icon
☑ Show communication client tray icon
□ Show file list
□ Show vendor list
□ Show Virtual Desktop settings only in security client interface

| General Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Language | The language which should be used in the Comodo Client Security interface.<br>(***Default = English (United States)***) |
| Show messages from Comodo Message Center | Message Center notifications appear as pop-ups at the bottom right-hand corner of the screen.<br>They contain news about updates, offers and other items of interest.<br>• Select whether or not the messages should be displayed to end-users..<br>(***Default = Disabled***) |
| Show notification messages | Notifications inform end-users about actions and status updates.<br>CCS notices appear in the bottom right hand corner of the screen (just above the tray icons).<br>• Select whether or not notifications should be shown to end-users.<br>(***Default = Disabled***) |
| Show desktop widget | The widget contains shortcuts to important CCS tasks and information about security levels, traffic and background tasks.<br>• Select whether or not the widget should be shown on endpoint desktops.<br>(***Default = Disabled***) |
| Show information messages when tasks are minimized/sent to background | These messages inform end-users of the effects of minimizing or moving a running task to the background. For example, when a virus scan task is moved to the background.<br>• Select whether or not information messages should be displayed to end-users.<br>(***Default = Disabled***) |
| Play sound when an alert is shown | If selected, CCS plays a chime whenever it raises a security alert.<br>(***Default = Disabled***) |
| Show shared space shortcut on the desktop | 'Shared Space' is the special folder on an endpoint where contained applications are allowed to save files. The shared space shortcut provides access to this folder.<br>• Select whether or not the shortcut should be shown to end-users.<br>(***Default = Disabled***) |
| Show security client tray icon | Select whether or not the CCS icon should be shown in the system tray.<br>(***Default = Enabled***) |
| Show security client desktop shortcut icon | Select whether or not the CCS desktop shortcut should be displayed.<br>(***Default = Disabled***) |
| Show communication client tray icon | Select whether or not the communication client shortcut icon should be available in the system tray.<br>(***Default = Enabled***) |
| Show file list | CCS can show a list of files on a device along with their trust ratings ('Trusted', 'Unrecognized' or 'Malicious'). This is available in 'Advanced Settings' > 'Security Settings' > 'File Rating' > 'File List'. |

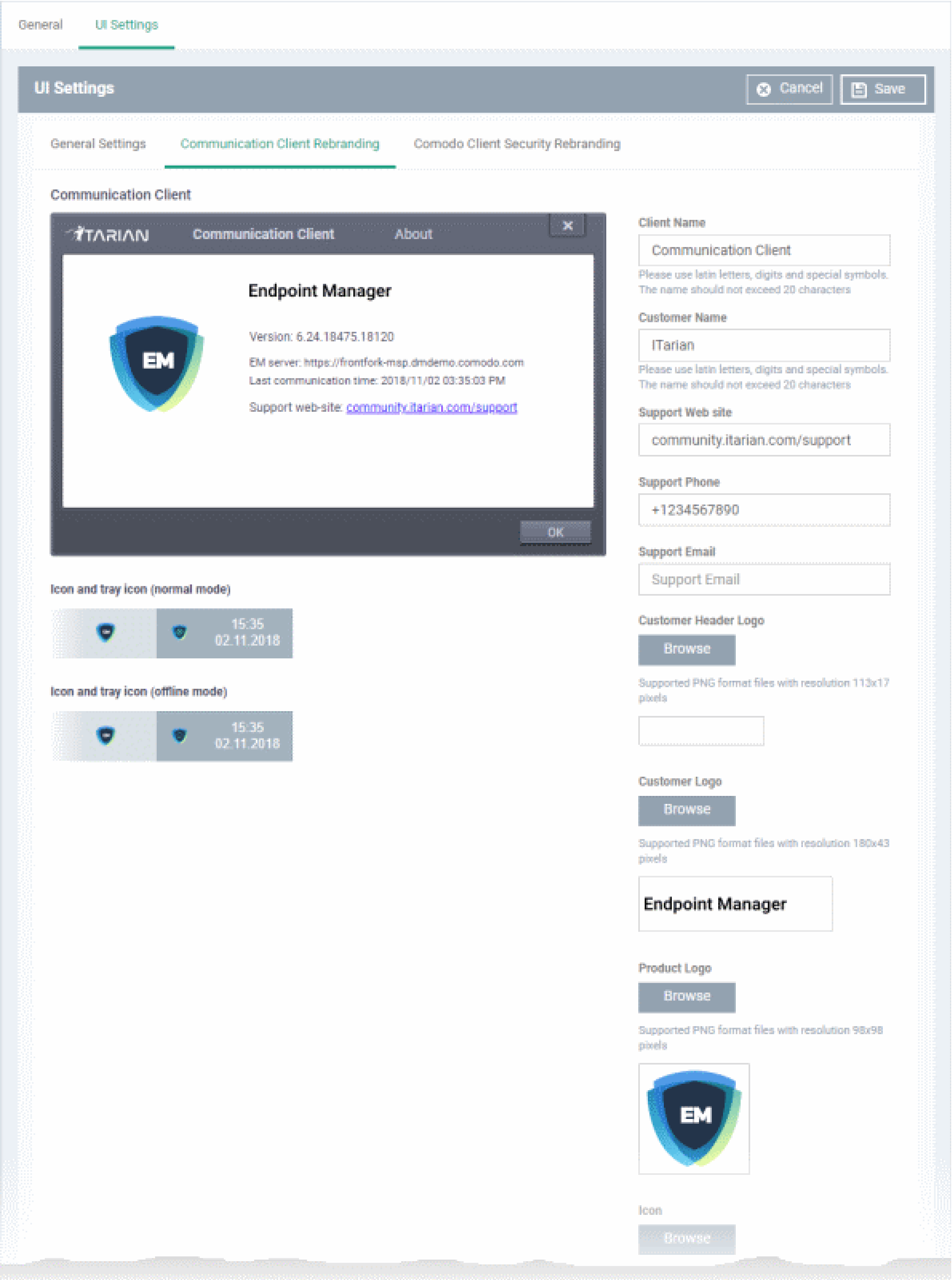
| General Settings - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| | For more details click the link https://help.comodo.com/topic-399-1-790-10397-File-List.html.<br>Select whether or not the file list should be available to end-users. (***Default = Disabled***) |
| Show vendor list | Enable to allow local users to open the vendor list area of Comodo Client Security on an endpoint.<br>CCS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CCS allows unknown files which are digitally signed by one of these vendors to run.<br>Users can also add new vendors, and change the rating of existing vendors.<br>Click 'Advanced Settings' > 'Security Settings' > 'File Rating' > 'Vendors List' in CCS to view the vendor list.<br>See https://help.comodo.com/topic-399-1-904-11879-Vendor-List.html if you want to read more. |
| Show Virtual Desktop settings only in security client interface | If enabled:<br>• The CCS tray icon and the widget are hidden on the endpoint.<br>• The CCS desktop and start menu shortcuts only show virtual desktop options:<br>• **Run Virtual Desktop** - Opens the virtual desktop<br>• **Open Virtual Desktop Settings** - Opens the virtual desktop settings area in CCS ('Settings' > 'Containment' > 'Virtual Desktop')<br>End-users cannot access any other area of CCS.<br>(***Default = Disabled***)<br>**Note**: This setting only works if 'Allow user to override Virtual Desktop settings' is disabled in the 'Containment' section of the profile. See **Virtual Desktop Settings** in **Containment Settings** for more details. |

- Click 'Save' to apply your changes to the profile.

## Communication Client Rebranding

The rebranding tab lets you change the appearance and interface texts of Communication Client .This is especially useful for customers who wish to white-label the CC interface for their clients.

- You can change the company name, support website, phone number and email.
- You can upload replacement images for company logo, header logo, product icons and product logo.
- The online editor lets you preview your changes in real-time.


General
UI Settings
UI Settings
Cancel
Save
General Settings
Communication Client Rebranding
Comodo Client Security Rebranding

Communication Client

Endpoint Manager

Version: 6.24.18475.18120

EM server: https://frontfork-msp.dmdemo.comodo.com

Last communication time: 2018/11/02 03:35:03 PM

Support web-site: community.itarian.com/support

Icon and tray icon (normal mode)

Icon and tray icon (offline mode)

Client Name: Communication Client

Please use latin letters, digits and special symbols. The name should not exceed 20 characters

Customer Name: ITarian

Please use latin letters, digits and special symbols. The name should not exceed 20 characters

Support Web site: community.itarian.com/support

Support Phone: +1234567890

Support Email: Support Email

Customer Header Logo

Supported PNG format files with resolution 113x17 pixels

Customer Logo

Supported PNG format files with resolution 180x43 pixels

Product Logo

Supported PNG format files with resolution 98x98 pixels

Icon

- Start typing in the fields to see your changes reflected in the example image
- Make sure all images you upload are the correct size and file format (.png).

| Communication Client Rebranding - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Client Name | Enter a custom name for the application.<br>You can use alphabetical, numeral and special characters. Maximum = 20 characters. |
| Company Name | Your company name. |
| Support Website | The URL of your support website.<br>The URL will be shown in the 'About' dialog of the CC application. |
| Support Phone | Your customer support phone number.<br>This number will be shown in the 'About' dialog of the CC application. |
| Support Email | Your customer support email address.<br>This address will be shown in the 'About' dialog of the CC application. |
| Company Header Logo | Logo shown at the top-left corner of the application window.<br>Accepted image size = 113 x 17 pixels<br>Accepted image file format = .png |
| Company Logo | Logo shown at the top of the CC 'About' dialog.<br>Accepted image size = 180 x 43 pixels<br>Accepted image file format = .png |
| Product Logo | Logo shown at the left of the CC 'About' dialog.<br>Accepted image size = 98 x 98 pixels<br>Accepted image file format = .png |
| Icon | Windows start menu and shortcut icon.<br>Accepted image sizes = 16 x 16, 20 x 20, 32 x 32, 40 x 40, 48 x 48 and 64 x 64 pixels<br>Accepted image format = .ico. http://www.dihav.com/view.php?id=png2icon is a free tool to convert .png files to .ico files.' |
| Tray Icon (normal mode) | Tray icon shown when the communication client is connected to Endpoint Manager.<br>Accepted image sizes = 16 x 16 pixels<br>Accepted image file format = .png |
| Tray Icon (offline mode) | Tray icon shown when the communication client is not connected to Endpoint Manager.<br>Accepted image sizes = 16 x 16 pixels<br>Accepted image file format = .png |

- Click 'Save' to apply your new design to the profile.

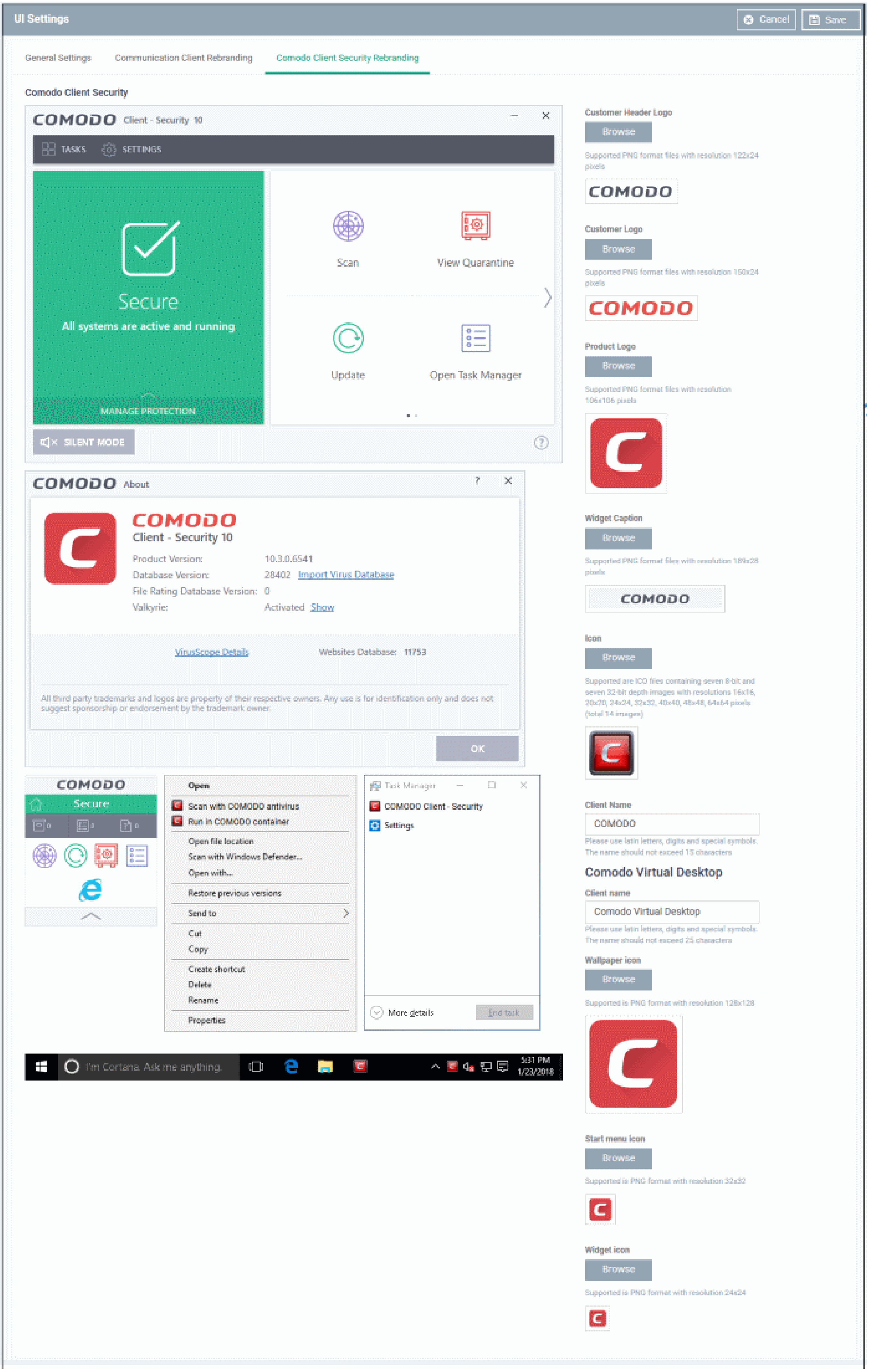
## Comodo Client Security Rebranding

- The rebranding tab lets you change the appearance of CCS and the Virtual Desktop. You can add you own company logos and texts to reinforce your brand in the eyes of your customers.

- Related. You can also create a disclaimer message which is shown to users when they start the virtual desktop. This is configured in the 'Containment' section of a profile. See **Virtual Desktop** in **Containment Settings** if you want to read more about this.

**Rebrand CCS interfaces**

- Open the 'UI settings' section of a profile
- Click the 'Comodo Client Security Rebranding' tab



Comodo Client Security

COMODO Client - Security 10

Product Version: 10.3.0.6541

Database Version: 28402 Import Virus Database

File Rating Database Version: 0

Valkyrie: Activated Show

VirusScope Details

Websites Database: 11753

All third party trademarks and logos are property of their respective owners. Any use is for identification only and does not suggest sponsorship or endorsement by the trademark owner.

Customer Header Logo

Supported PNG format files with resolution 122x24 pixels

Customer Logo

Supported PNG format files with resolution 150x24 pixels

Product Logo

Supported PNG format files with resolution 106x106 pixels

Widget Caption

Supported PNG format files with resolution 189x28 pixels

Icon

Supported are ICO files containing seven 8-bit and seven 32-bit depth images with resolutions 16x16, 20x20, 24x24, 32x32, 40x40, 48x48, 64x64 pixels (total 14 images)

Client Name: COMODO

Please use latin letters, digits and special symbols. The name should not exceed 15 characters

Comodo Virtual Desktop

Client name: Comodo Virtual Desktop

Please use latin letters, digits and special symbols. The name should not exceed 25 characters

Wallpaper icon

Supported is PNG format with resolution 128x128

Start menu icon

Supported is PNG format with resolution 32x32

Widget icon

Supported is PNG format with resolution 24x24

- Start typing in the fields to see your changes reflected in the example images.
- Make sure all images you upload are the correct size and file format (.png)
- The changes you make here will be rolled out to all interfaces in CCS.
- You cannot modify the UI in a default profile.

| Comodo Client Security Rebranding - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Company Header Logo | Logo shown at the top-left corner of the application window.<br>Accepted image size = 122 x 24 pixels<br>Accepted image file format = .png |
| Company Logo | Logo shown in various CCS interfaces.<br>Accepted image size = 150 x 24 pixels<br>Accepted image file format = .png |
| Product Logo | Logo shown on the left side of the CCS 'About' dialog.<br>Accepted image size = 106 x 106 pixels<br>Accepted image file format = .png |
| Widget Caption | Logo shown on the header of the CCS desktop widget.<br>Accepted image size = 189 x 28 pixels<br>Accepted image file format = .png |
| Icon | Windows start menu and shortcut icon. Also shown in various other interfaces of the application.<br>Accepted image sizes = 16 x 16, 20 x 20, 32 x 32, 40 x 40, 48 x 48 and 64 x 64 pixels<br>Accepted image format = .ico. http://www.dihav.com/view.php?id=png2icon is a free tool to convert .png files to .ico files.' |
| Client Name | Enter a custom name for the application. This will be shown in the interface and will be used as the product name in the Windows 'Start' menu.<br>You can use letters, numbers and special characters. Maximum = 20 characters. |
| **Comodo Virtual Desktop** | |
| Client Name | Enter a custom name for the application. This will be shown in the interface and will be used as the product name in the Windows 'Start' menu.<br>You can use letters, numbers and special characters. Maximum = 25 characters. |
| Wallpaper icon | Shown on the virtual desktop main screen.<br>Accepted image size = 128 x 128 pixels<br>Accepted image file format = .png |
| Start menu icon | Windows start menu and shortcut icon.<br>Accepted image size = 32 x 32 pixels<br>Accepted image file format = .png |
| Widget icon | Logo shown on the header of the virtual desktop widget.<br>Accepted image size = 24 x 24 pixels<br>Accepted image file format = .png |

- Click 'Save' to apply your settings to the profile.
- Click the 'Edit' button if you wish to modify a design that you have saved.

### 6.1.3.1.14. Logging Settings

- This area lets you specify how logs should be collected in CC (Communication Client) and CCS (Comodo Client - Security).
- For example, you can choose max. log size, log format and location, and extended log options.

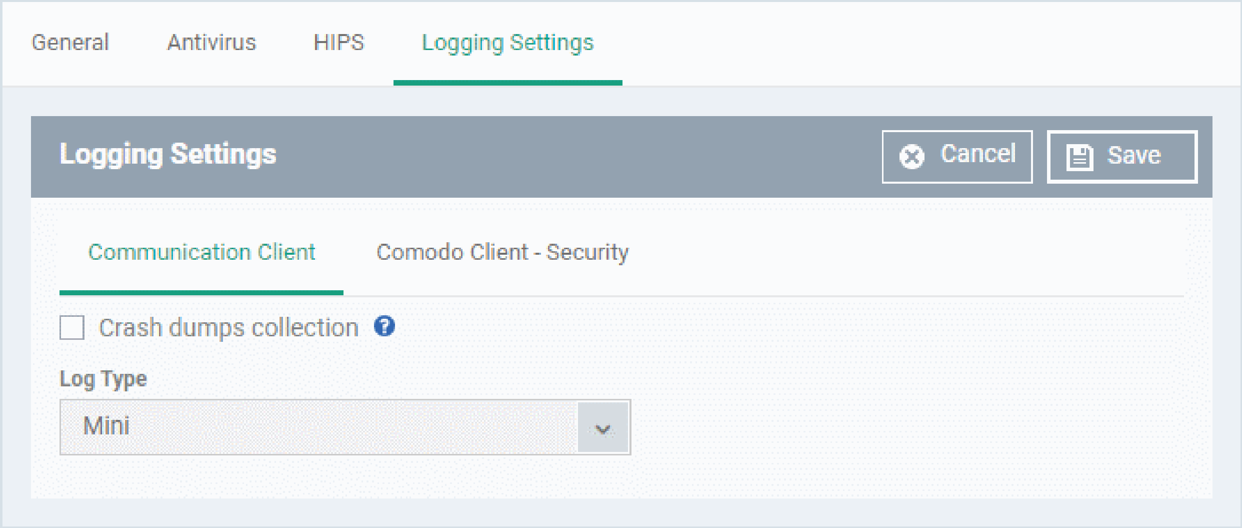
**To configure 'Logging' settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile that you want to configure
- Click 'Add Profile Section' > 'Logging Settings'

The settings screen contains two tabs:

- **Communication Client (CC)** - Choose whether a crash dump-file should be created when CC crashes on the endpoint. The dump file can help you to analyze and troubleshoot the issues.
- **Comodo Client - Security (CCS)** - Configure CCS log collection parameters, log file storage location and maximum size for the log file.

## Communication Client

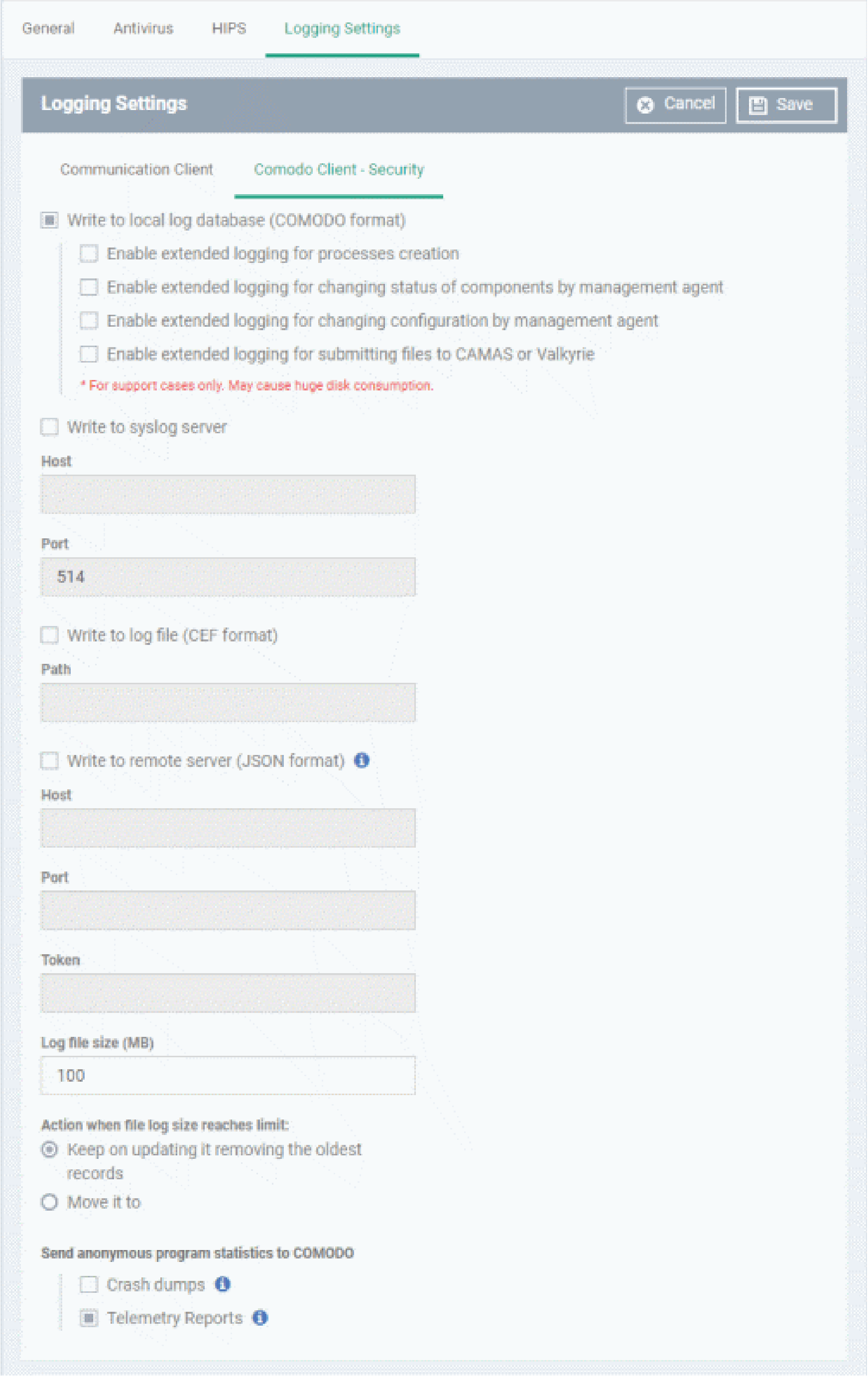


□ Crash dumps collection

Log Type: Mini

| Logging Settings - Comminucation Client - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Crash dump collection | Checkbox | Endpoint Manager creates a dump file if the communication client crashes on the endpoint. This is useful for analysis and troubleshooting.<br>You can also submit the file to Comodo for our technicians to assess.<br>(***Default = Disabled***) |
| Log Type | Drop-down | Choose the type of dump file you want. The options are:<br>**Mini** - The file only contains enough data to identify the conditions of the crash.<br>**Full** - A detailed log of all information related to the crash. Full logs let you analyze the crash in greater detail, but may take longer to generate than mini reports. |

## Comodo Client - Security



☒ Write to local log database (COMODO format)

- ☐ Enable extended logging for processes creation
- ☐ Enable extended logging for changing status of components by management agent
- ☐ Enable extended logging for changing configuration by management agent
- ☐ Enable extended logging for submitting files to CAMAS or Valkyrie

* For support cases only. May cause huge disk consumption.

☐ Write to syslog server

Host:

Port: 514

☐ Write to log file (CEF format)

Path:

☐ Write to remote server (JSON format)

Host:

Port:

Token:

Log file size (MB): 100

Action when file log size reaches limit:

● Keep on updating it removing the oldest records

○ Move it to

Send anonymous program statistics to COMODO

- ☐ Crash dumps
- ☒ Telemetry Reports

| Logging Settings - Comodo Client Security - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Write to Local Log Database (COMODO Format) | The log is saved in native Comodo format on the local endpoint.<br>You can enable extended logging for the following additional items:<br>• Process creation events<br>• CCS components are enabled/disabled by CC |

| | |
|---|---|
| | • Changes to CCS configuration made by CC<br>• Submitting files to CAMAS or Valkyrie |
| Write to Syslog Server | EM log events are written to a remote syslog server. If enabled you have to specify the hostname/IP address and port number settings for the server. |
| Host * | The host name or IP address of the syslog server. |
| Port * | The port number of the syslog server. |
| Write to Log File (CEF Format) | Logs are saved locally on the endpoint in Common Event Format (CEF) file format. If enabled, please specify the location of the CEF file. |
| Path | Enter the storage location path of the CEF file. |
| Write to remote server (JSON format) | Logs are saved in JavaScript Object Notation (JSON) format on a remote server. If enabled, please specify the hostname/IP address of the server, its connection port and the security token. |
| Host * | Enter the host name or IP address of the remote server. |
| Port * | Type the port number of the remote sever for EM to connect to. |
| Token* | Enter the security token to access the remote server. |
| Log file size (MB) | Specify the maximum limit for the size of the log file (Default = 100 MB). |
| Action when file log size reaches limit: | Specify behavior when the log file reaches a certain size. |
| Keep on updating it removing the oldest records | Once the log file reaches the maximum size, the file will be appended with the new log entries and the oldest entries will be deleted depending on the size of the new entries. |
| Move it to | Choose this option if you wish to move and save the log file when it reaches the maximum size. |
| The path to the folder for old log files * | If 'Move it to' is enabled, type a destination path for the log file. |
| Send anonymous program statistics to Comodo | If enabled, select the types of statistics sent from the following options: |
| Crash dumps | CCS sends dump files to Comodo if the application crashes or there is a BSOD (blue screen of death) on the endpoint.<br>This is useful for analysis and troubleshooting. |
| Telemetry Reports | Will send to Comodo a daily log about the files you scan with CCS. We use this data to improve EM and CCS.<br>The reports contain the following details:<br>• The hash value and path of the file<br>• The hash value(s) and path of the parent file that executed the file<br>• Size, certificate information, and attributes of the file |

Fields marked * are mandatory.

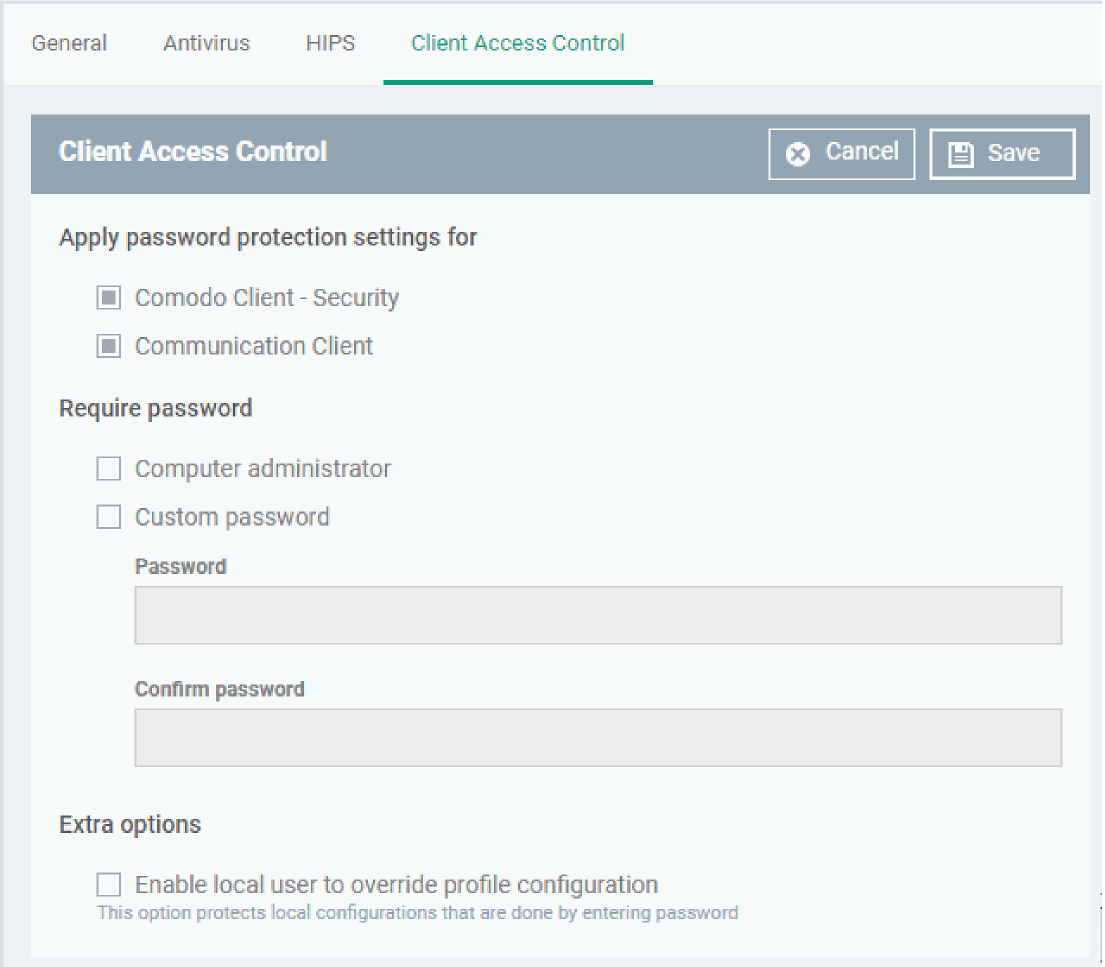
- Click the 'Save' button to apply your changes.
- Click 'Delete' or 'Edit' to remove / edit the logging settings section. See '**Edit Configuration Profiles**' for more details about editing the parameters

### 6.1.3.1.15. Client Access Control

- Client access control lets you password-protect Comodo Client Security (CCS) and the communication client (CC) on managed endpoints.
- Once set, users will need to enter a password to access important areas of the client interface.
- This stops users from opening the clients locally and making changes to important tasks and settings. Without password protection, the endpoint user can access the client interface and make changes.

**Implement access control**

- Click 'Configuration Templates' > 'Profiles'
- Click the name of the profile to which you want to add the section.
- Click 'Add Profile Section' > 'Client Access Control':



**Client Access Control**

Apply password protection settings for

☑ Comodo Client - Security

☑ Communication Client

Require password

□ Computer administrator

□ Custom password

Password

Confirm password

Extra options

□ Enable local user to override profile configuration

This option protects local configurations that are done by entering password

- **Apply password protection settings for -** Specify which clients you want to password protect.
  - Comodo Client - Security - Password protects the settings interface and the 'Task' interfaces for antivirus, firewall, HIPS and containment.

    Users can still run some limited tasks, including on-demand virus scans, open the virtual desktop, and run programs in the container.
  - Communication Client - Password protects important settings, including the ability to configure a proxy for the client to connect to the EM console.

Users can still submit support tickets to Service Desk from the tray icon without requiring the password.

- **Require Password** - select the type of password required to access CCS and/or CC:
    - **Computer administrator** - admins can access the local interfaces by providing their admin password. If the admin is already logged into the machine then they can open the interfaces without providing a password.
    - **Custom password** - specify a unique key to access the CCS / CC interfaces. The password will time-out and need to be re-entered after 15 minutes.
        - If you select 'Custom password' but not 'Computer administrator', then even admins will need to enter the custom password to access the clients.

The tables below summarize how the passwords work together for admins and regular users:

| Admin logged-in | | | |
|---|---|---|---|
| Admin password enabled | Yes | No | Yes |
| Custom password enabled | Yes | Yes | No |
| Requirements | No password needed | Custom password required | No password needed |

| Admin not logged-in / Standard user logged-in | | | |
|---|---|---|---|
| Admin password enabled | Yes | No | Yes |
| Custom password enabled | Yes | Yes | No |
| Requirements | Either password | Custom password required | Admin password required |

- **Enable local user to override profile configuration** - Endpoint Manager will not reverse local settings that are different to those in the endpoint's profile. You must enable password protection if you want to use this option.

  Background - Endpoint Manager periodically checks devices to see if the local CCS settings match those in the device's profile. It will undo any local changes unless you enable this setting.

  This is useful if you need to implement specific settings on a certain device.
- Click 'Save' to apply your changes to the profile.

**While you're here**

The following is a list of other settings you should consider if you want to lock-down CCS on endpoints:

**User Interface settings** - *'Configuration Templates'* > *'Profiles'* > *Add profile section* > *'UI Settings'*

- Hide the CCC and CCS tray icons
- Manage the visibility of other UI items

**Antivirus settings** - '*Configuration Templates*' > *'Profiles'* > *Add profile section* > *'Antivirus'*

- Disable 'Show Antivirus alerts' *
- Enable 'Do not show auto-scan alerts' *
- Enable 'Automatically clean threats' (when you create a scheduled scan) *

- Disable 'Show scan results' (when you create a scheduled scan)*

**Firewall settings** - *'Configuration Templates' > 'Profiles' > Add profile section > 'Firewall'*

- Disable 'Show popup alerts' *

**HIPS settings** - '*Configuration Templates' > 'Profiles' > Add profile section > 'HIPS'*

- Enable 'Do not show popup alerts' *

**Containment setttings** - *'Configuration Templates' > 'Profiles' > Add profile section > 'Containment'*

- Enable 'Do not show privilege elevations alerts' *

**VirusScope settings** - *'Configuration Templates' > 'Profiles' > Add profile section > 'VirusScope'*

- Disable 'Show popup alerts' *

**File rating Settings** - *'Configuration Templates' > 'Profiles' > Add profile section > 'File Rating'*

- Disable 'Show cloud alert' *

**External device control**: - *'Configuration Templates' > 'Profiles' > Add profile section > 'External Device Control'*

- Disable 'Show notifications when devices disabled or enabled' *

* This setting is already enforced in the 'Default' Windows profile that ships with Endpoint Manager.

### 6.1.3.1.16. External Devices Control Settings

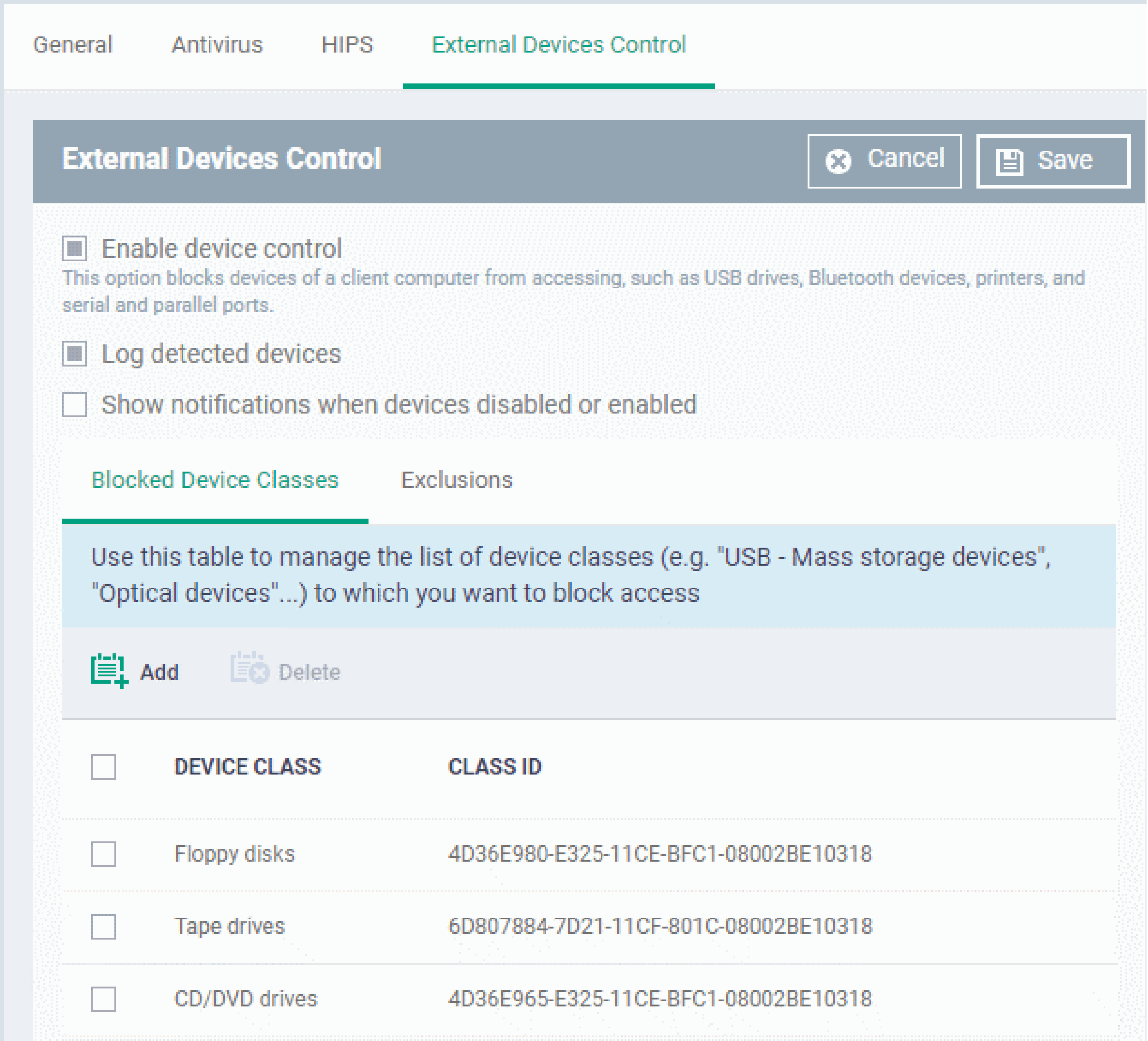
- Lets you to define a list of devices that should be blocked on endpoints using this profile.

For example, you can block access to USB storage devices, human interface devices, Bluetooth devices, infrared devices, IDE ATA/ATAPI controllers.

- Endpoint Manager blocks access to devices connected through both serial and parallel ports and creates a log of their connection activities.
- You can create exclusions for external devices which you want to allow to connect to managed endpoints. Devices can be added as exclusion by specifying their Device Ids. You can use wildcard characters in the device ID if you want to include a series of devices with similar device IDs.

**To configure External Devices Control Settings**

- Click 'Configuration Templates' > 'Profiles' then click the name of the profile to which you want to add the section.
- Click 'Add Profile Section' > 'External Devices Control'



☒ Enable device control

This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

☒ Log detected devices

☐ Show notifications when devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

| ☐ | DEVICE CLASS | CLASS ID |
|---|---|---|
| ☐ | Floppy disks | 4D36E980-E325-11CE-BFC1-08002BE10318 |
| ☐ | Tape drives | 6D807884-7D21-11CF-801C-08002BE10318 |
| ☐ | CD/DVD drives | 4D36E965-E325-11CE-BFC1-08002BE10318 |

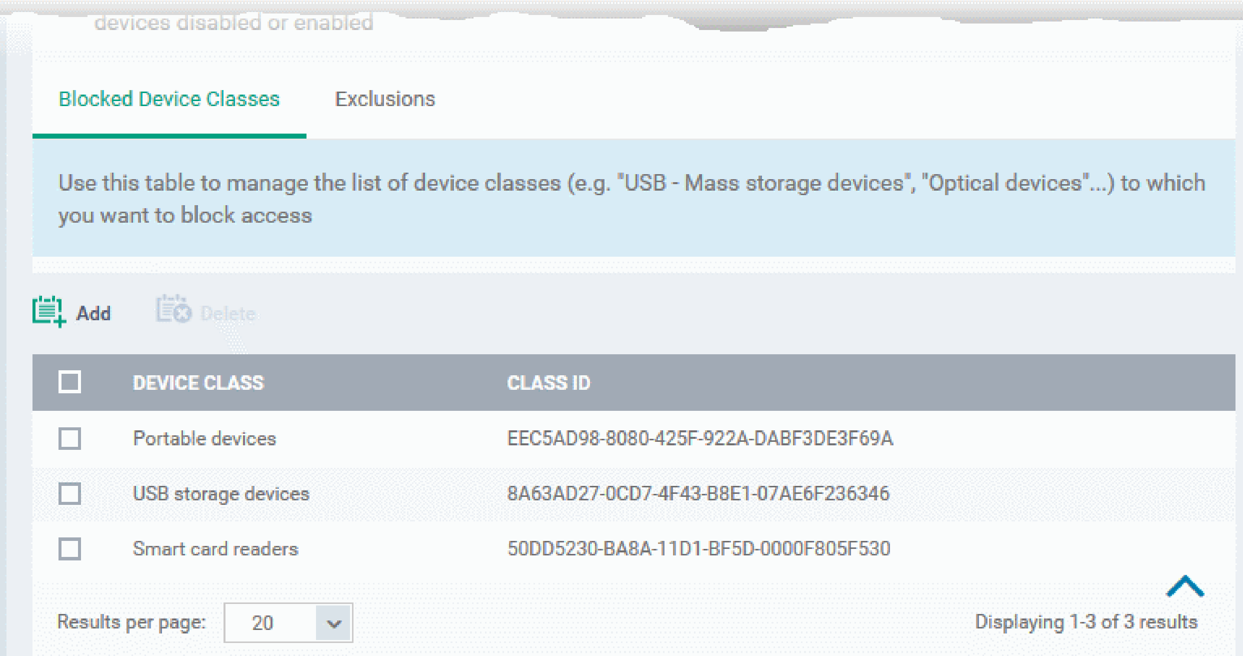
- **Enable Device Control** - Enable or disable the external device control feature. This is useful if you want to configure external device control settings for a profile during its creation and enable it at a later time
- **Log detected devices** - Enable or disable logging of external device connection attempts on endpoints that use this profile. The logs can be viewed from 'Security Sub Systems' > 'Device Control' interface. See **View History of External Device Connection Attempts** for more details.
- **Show notifications when devices disabled or enabled** - Select whether or not a notification is to be shown to end-user when a connected device is blocked or allowed.

The 'External Devices Control' settings interface contains two tabs:

- Blocked Device Classes - Define the list of types of external devices to be blocked at the endpoints
- Exclusions - Specify the devices that should be excluded from blocking and allowed access at the endpoints

## Blocked Device Classes

The 'Blocked Device Classes' tab displays a list of types of device that are blocked as per the profile and allows you to add/remove new device types.



devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

| □ | DEVICE CLASS | CLASS ID |
|---|---|---|
| □ | Portable devices | EEC5AD98-8080-425F-922A-DABF3DE3F69A |
| □ | USB storage devices | 8A63AD27-0CD7-4F43-B8E1-07AE6F236346 |
| □ | Smart card readers | 50DD5230-BA8A-11D1-BF5D-0000F805F530 |

Results per page: 20

Displaying 1-3 of 3 results

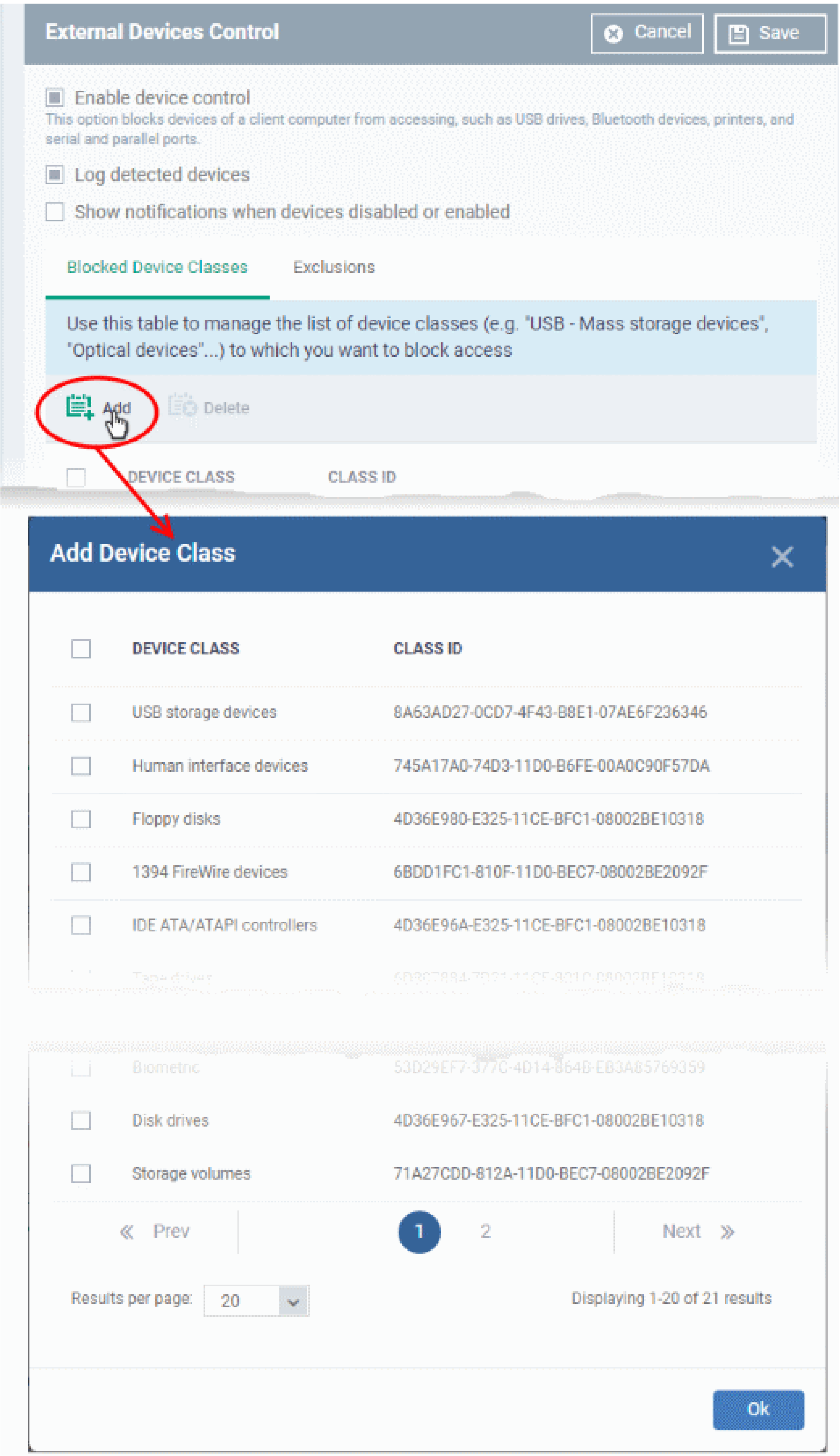
| Blocked Device Classes - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Device Class | The device type as per global hardware classification |
| Class ID | The Globally Unique Identifier (GUID) of the device class |

**Tip.** Block 'Portable Devices' in addition to 'USB storage devices' if you want to stop users connecting their phones to access the phone's memory card

**To add device types to be blocked**

- Click 'Add' at the top of the list

The 'Add Device Class' dialog appears with a list of device types.



External Devices Control

☑ Enable device control
This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

☑ Log detected devices

□ Show notifications when devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

□ DEVICE CLASS CLASS ID

Add Device Class

| □ | DEVICE CLASS | CLASS ID |
|---|---|---|
| □ | USB storage devices | 8A63AD27-0CD7-4F43-B8E1-07AE6F236346 |
| □ | Human interface devices | 745A17A0-74D3-11D0-B6FE-00A0C90F57DA |
| □ | Floppy disks | 4D36E980-E325-11CE-BFC1-08002BE10318 |
| □ | 1394 FireWire devices | 6BDD1FC1-810F-11D0-BEC7-08002BE2092F |
| □ | IDE ATA/ATAPI controllers | 4D36E96A-E325-11CE-BFC1-08002BE10318 |
| □ | Tape drives | 6D807884-7D21-11CF-801C-08002BE10318 |
| □ | Biometric | 53D29EF7-377C-4D14-864B-EB3A85769359 |
| □ | Disk drives | 4D36E967-E325-11CE-BFC1-08002BE10318 |
| □ | Storage volumes | 71A27CDD-812A-11D0-BEC7-08002BE2092F |

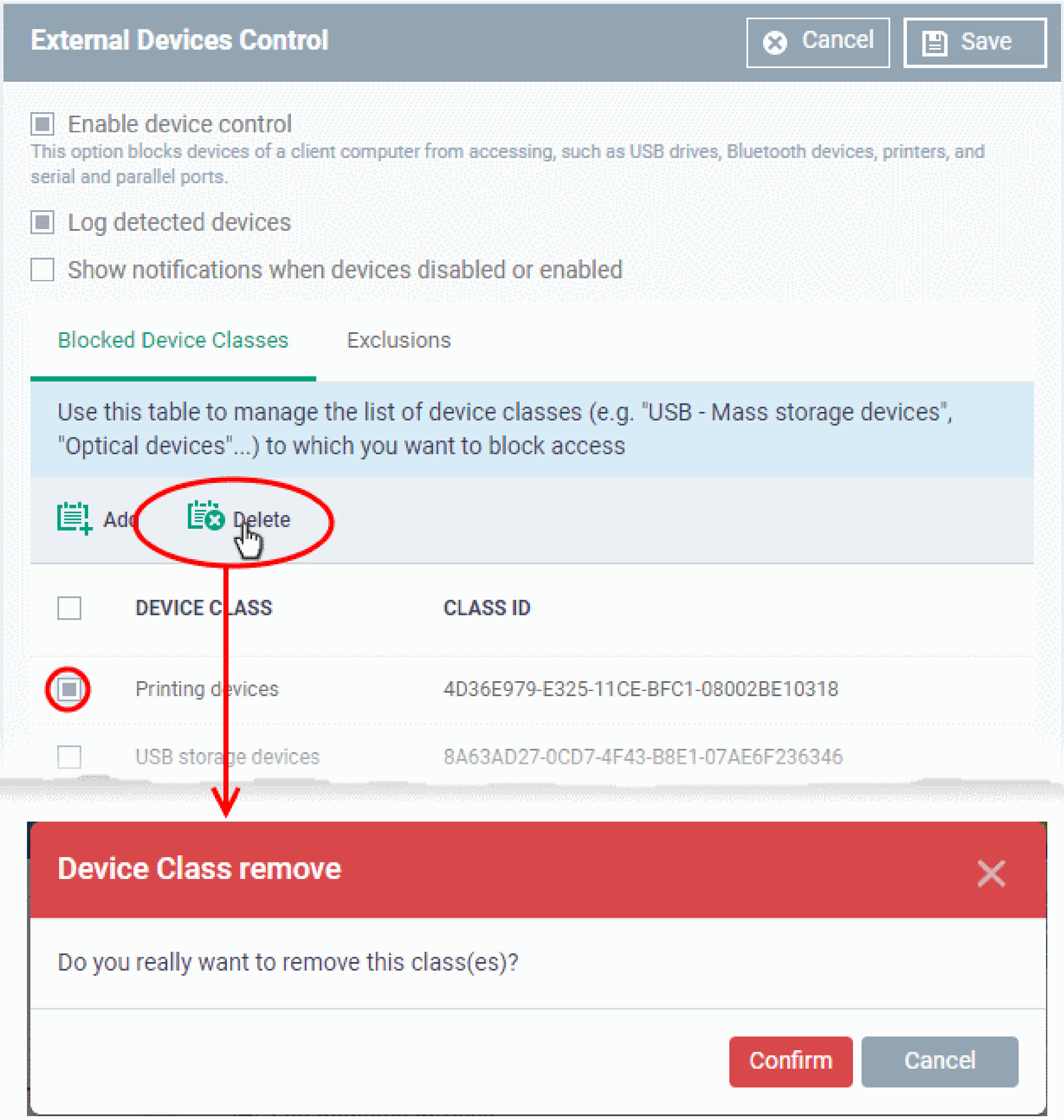
Results per page: 20

Displaying 1-20 of 21 results

- Select the device types to be added to the block list and click 'Ok'.
- Repeat the process to add more device types.

**To remove a device type from the list**

- Select the device type from the list and click 'Delete'


External Devices Control

☒ Enable device control

This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

☒ Log detected devices

□ Show notifications when devices disabled or enabled

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...) to which you want to block access

| | DEVICE CLASS | CLASS ID |
|---|---|---|
| ☒ | Printing devices | 4D36E979-E325-11CE-BFC1-08002BE10318 |
| □ | USB storage devices | 8A63AD27-0CD7-4F43-B8E1-07AE6F236346 |

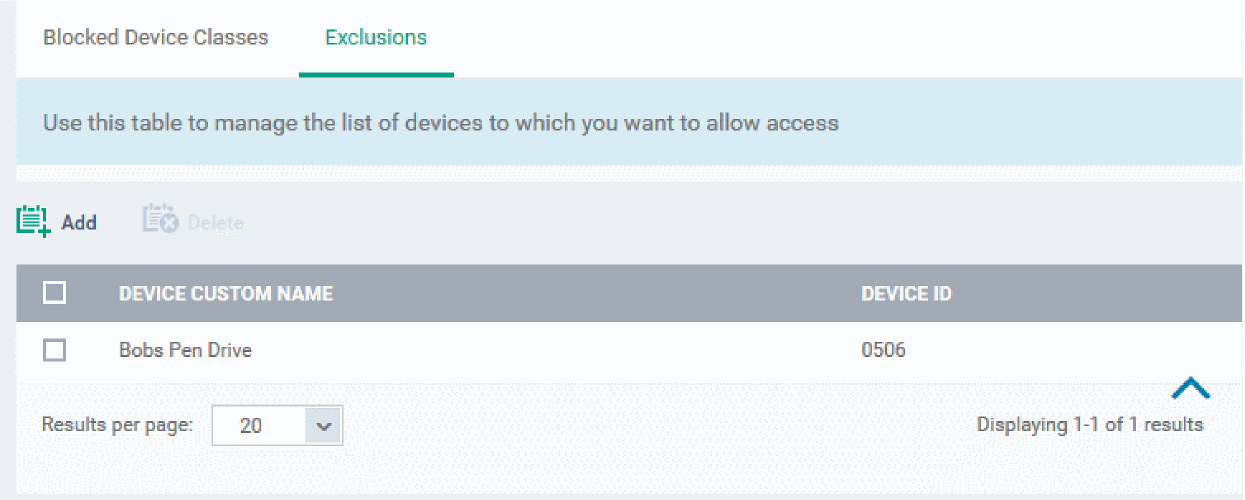
Device Class remove

Do you really want to remove this class(es)?

- Click 'Confirm' to remove the device type from the blocked list.

## Exclusions

The 'Exclusions' tab displays a list of external devices that are exempt from the block rule and so allowed access to the endpoint(s).



Use this table to manage the list of devices to which you want to allow access

| □ | DEVICE CUSTOM NAME | DEVICE ID |
|---|---|---|
| □ | Bobs Pen Drive | 0506 |

Results per page: 20

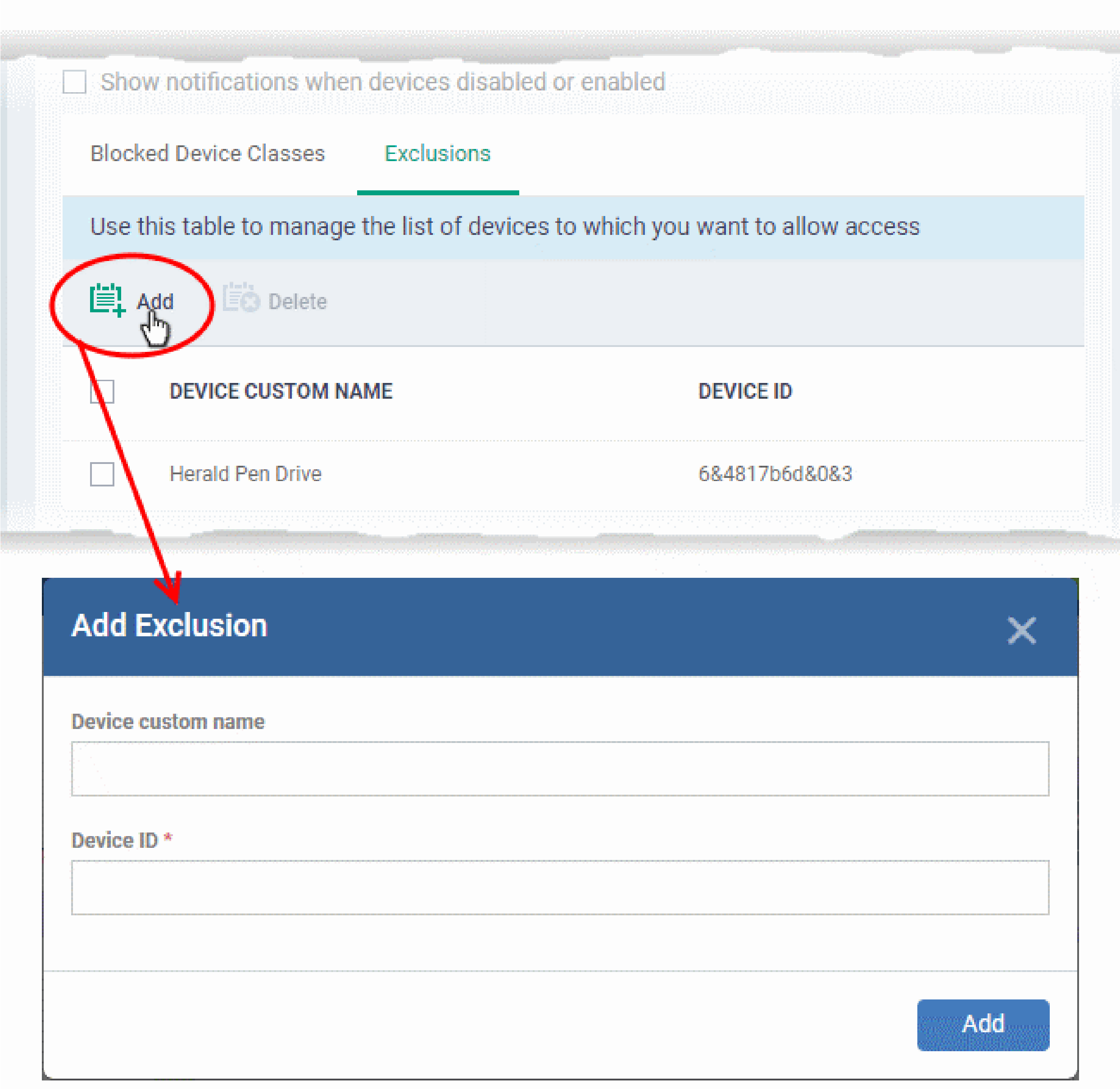
Displaying 1-1 of 1 results

| Exclusions - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Device Custom Name | Displays the name of the device. |
| Device ID | Displays the unique device identifier of the device. |

**To add a device to be excluded**

- Click 'Add' at the top of the list

The 'Add Device Class' dialog will appear with a list of device types.



□ Show notifications when devices disabled or enabled

Blocked Device Classes | Exclusions

Use this table to manage the list of devices to which you want to allow access

| □ | DEVICE CUSTOM NAME | DEVICE ID |
|---|---|---|
| □ | Herald Pen Drive | 6&4817b6d&0&3 |

**Add Exclusion**

Device custom name

Device ID *

- Enter a label for the device in the 'Device Custom Name' field (optional)
- Enter the unique device identifier in the 'Device ID' field

**Tip**: You can use a wildcard character '*' in the Device ID if you want to cover a range of devices with similar IDs. For example, to include all USB storage devices whose device IDs start with "4C5310", you could enter:

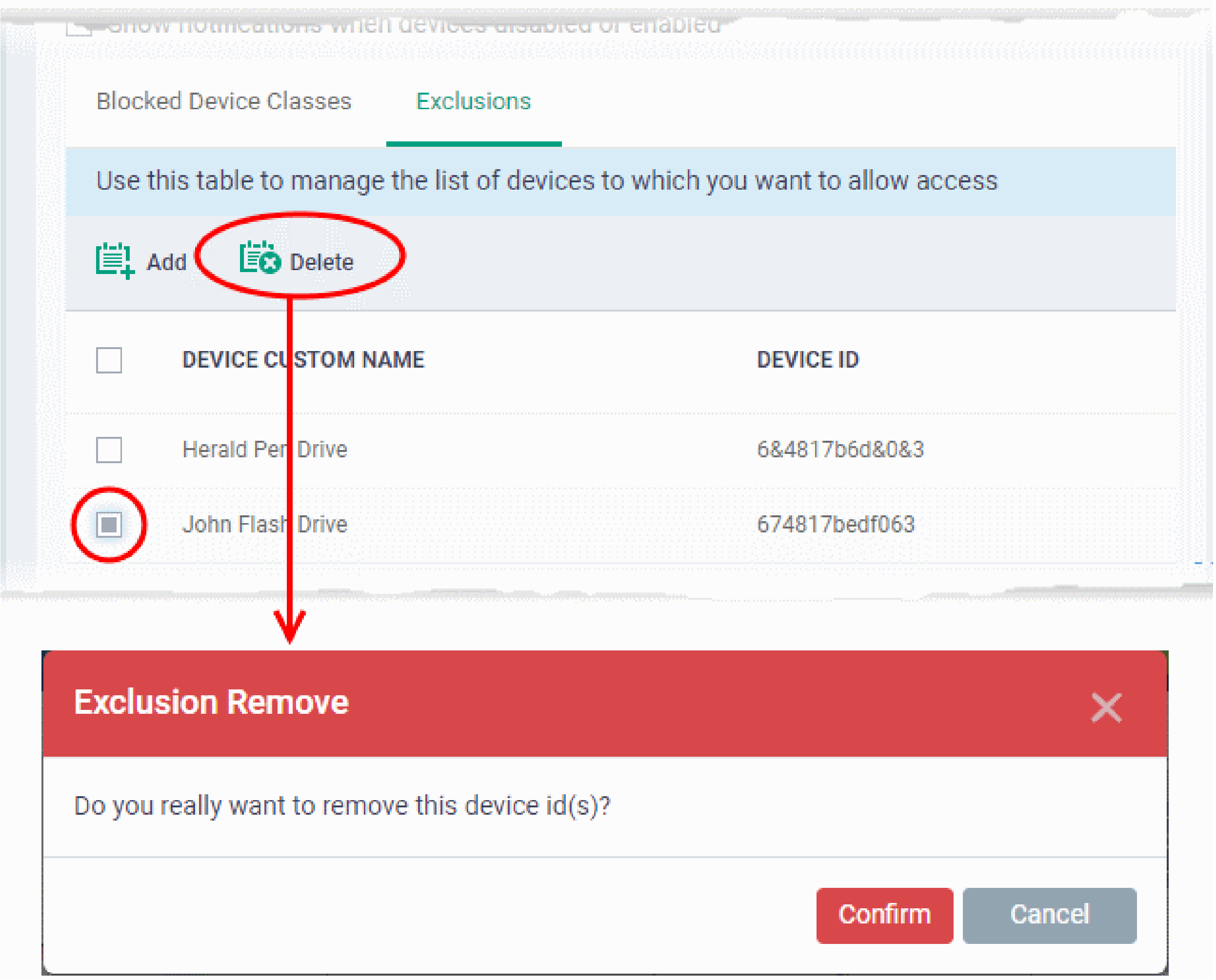
USBSTOR\DISK&VEN_SANDISK\4C5310*

- Click 'Add'

The device will be added to the exclusions list and will be allowed access at the endpoint(s).

**To remove a device from exclusions**

- Select the device and click 'Delete'



Use this table to manage the list of devices to which you want to allow access

| □ | DEVICE CUSTOM NAME | DEVICE ID |
|---|---|---|
| □ | Herald Pen Drive | 6&4817b6d&0&3 |
| ■ | John Flash Drive | 674817bedf063 |

**Exclusion Remove**

Do you really want to remove this device id(s)?

- Click 'Confirm' to remove the item from the list
- Click the 'Save' button save the 'External Devices Control' settings.
- Click 'Delete' to remove the 'External Devices Control' section from the profile. See **Edit Configuration Profiles** for more details about editing the parameters.

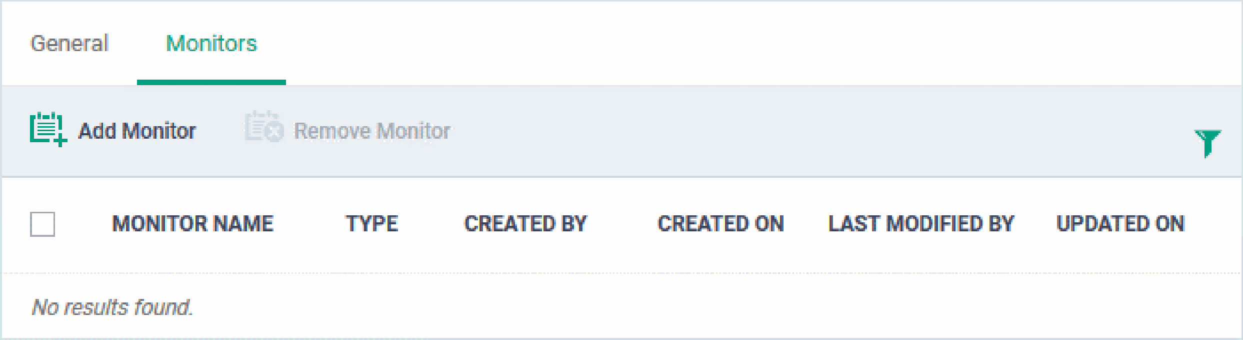
### 6.1.3.1.17. Monitors

- The monitors settings section lets you add performance and event monitors to a profile.
- A monitor is a script which tracks events on a managed endpoint and takes specific actions if its conditions are met.
    - For example, 'Alert me when a USB removable disk is connected to the system', or 'Create a log entry if CPU usage goes above 75% for a certain length of time'.
- You can also configure a monitor to run a procedure if its conditions are met.
- There are two types of monitor:
    - 'Predefined Monitors' - A collection of monitors from Comodo which perform a range of useful monitoring tasks. These can be used in custom profiles, but cannot be edited.
    - 'My Monitors' - Custom monitors that you create. You can configure custom monitors in the 'Monitors' inventory ('Configuration Templates' > 'Monitors'). See '**Manage Monitors**' for more details.
- Monitors added to the inventory can be added to a profile. You can add multiple monitors to a single profile.

**Add a monitor section to a profile**

- Click 'Configuration Templates' > 'Profiles'

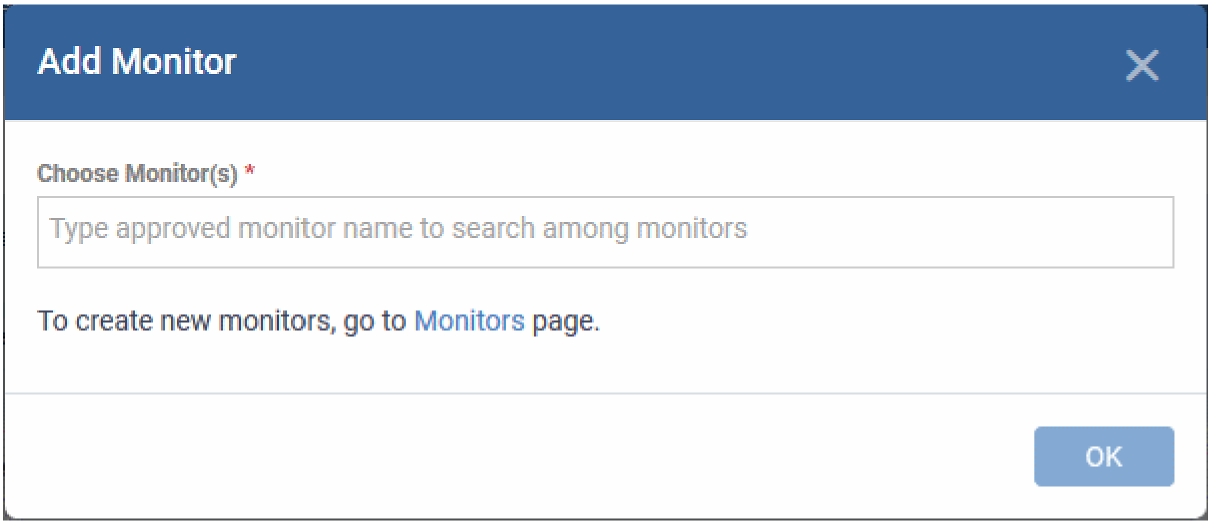
- Open the Windows profile you want to configure
- Click 'Add Profile Section' > 'Monitors'



| □ | MONITOR NAME | TYPE | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|---|

*No results found.*

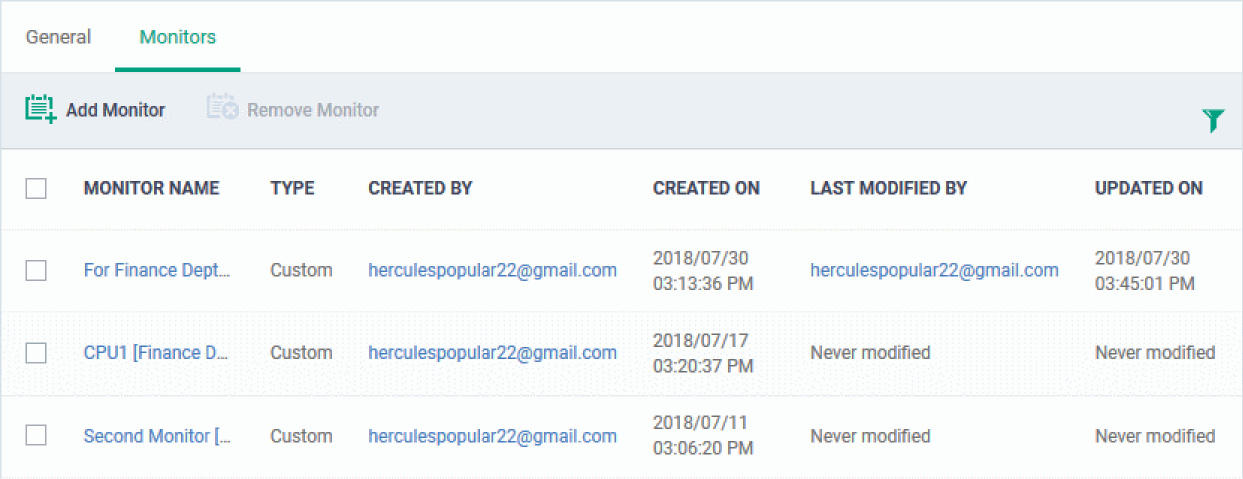
- Click 'Add Monitor'



To create new monitors, go to Monitors page.

- Choose Monitor(s) - Lets you add monitors to the profile
  - Start typing the first few letters of a monitor name then select from the suggestions
  - Repeat the process to add more monitors to the profile
  - See **Manage Monitors** for help to configure a monitor
- Click 'OK' to save your settings

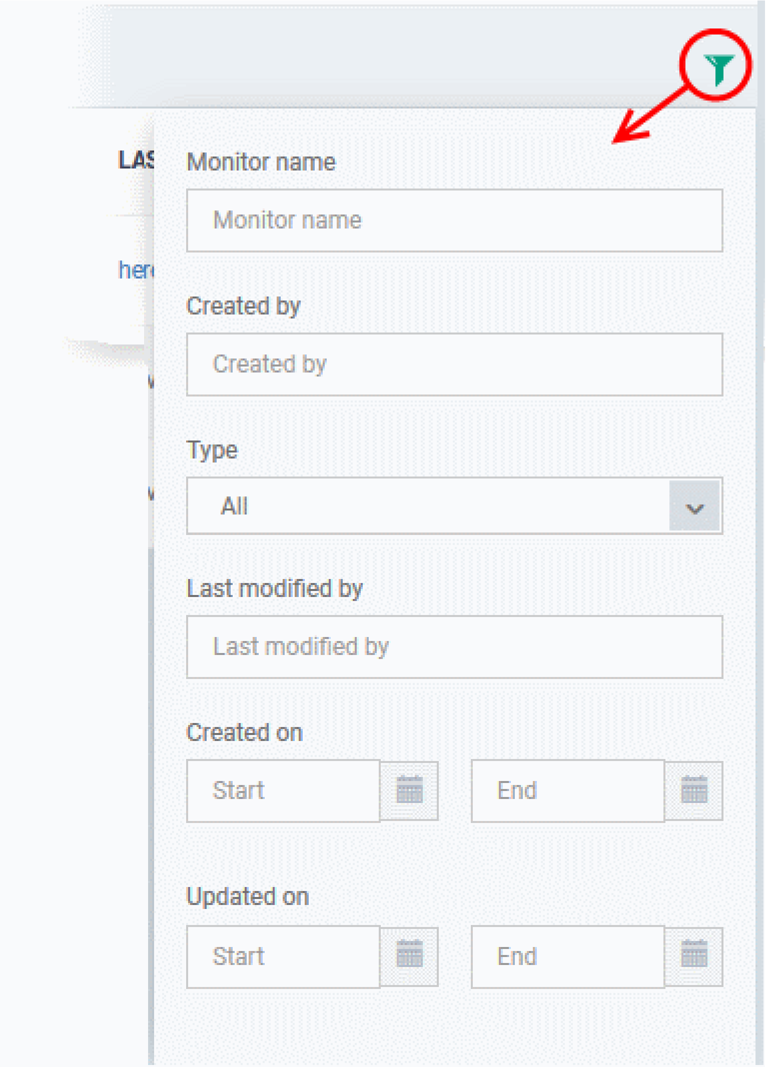
The list of monitors included in the profile will be displayed:



| □ | MONITOR NAME | TYPE | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|---|
| □ | For Finance Dept... | Custom | herculespopular22@gmail.com | 2018/07/30<br>03:13:36 PM | herculespopular22@gmail.com | 2018/07/30<br>03:45:01 PM |
| □ | CPU1 [Finance D... | Custom | herculespopular22@gmail.com | 2018/07/17<br>03:20:37 PM | Never modified | Never modified |
| □ | Second Monitor [... | Custom | herculespopular22@gmail.com | 2018/07/11<br>03:06:20 PM | Never modified | Never modified |

| Monitors - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The monitor label.<br>• Click the name of a monitor view and edit it. See **View and Edit Monitors** for more details. |
| Type | Whether the monitor is custom or predefined. |
| Created by | The administrator who created the custom monitor.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created On | Date and time the monitor was created. |
| Last Modified By | The admin who most recently edited the monitor. |
| Updated On | Date and time the monitor was last edited. |
| **Controls** | |
| Add Monitor | Add a monitor to the profile. See the explanation **above** for help with this. |
| Remove Monitor | Delete monitors from the profile Use the check-boxes to select the monitors you want to remove. |

- Click any column header to sort the items based on alphabetical or ascending/descending order of entries in the respective column.
- Click the funnel button at the right end to open the filter options.



Monitor name

Monitor name

Created by

Created by

Type

All

Last modified by

Last modified by

Created on

Start

End

Updated on

Start

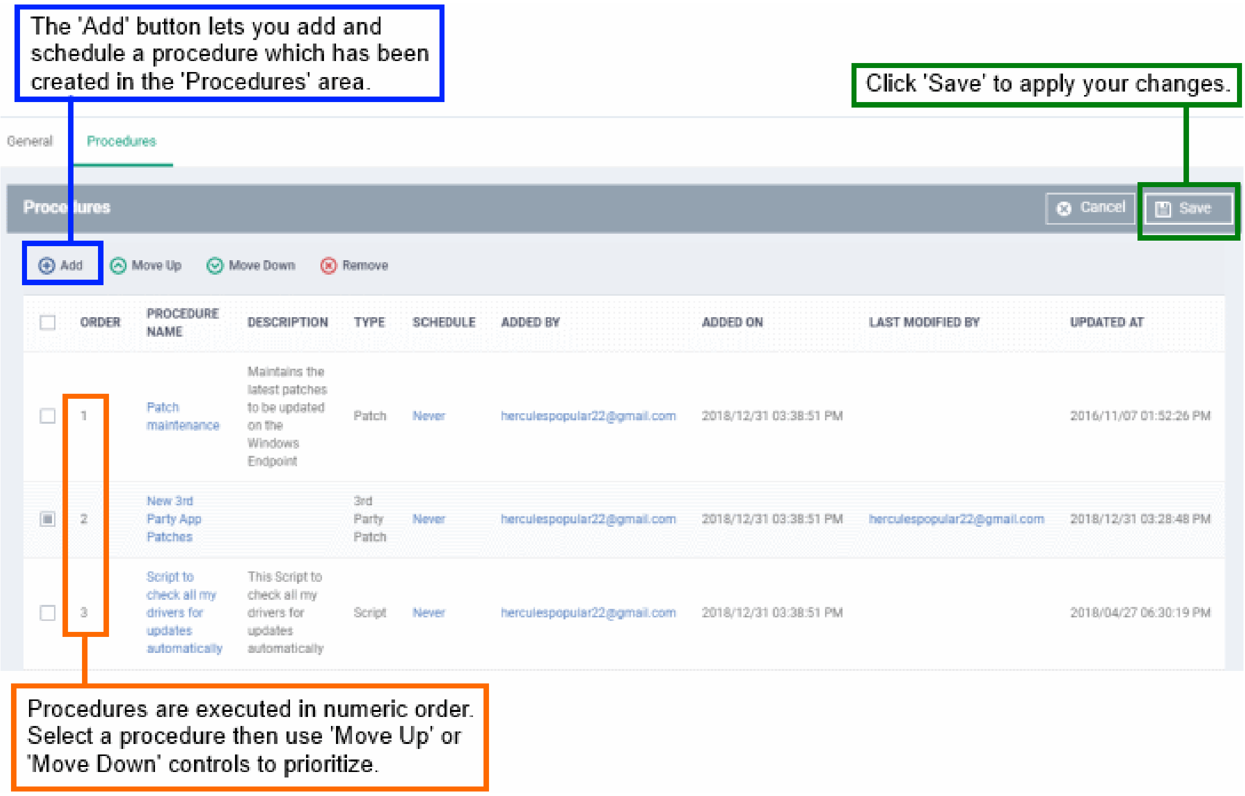
End

### 6.1.3.1.18. Procedure Settings

- You can run scripts and patches on Windows devices by adding a 'Procedures' section to a profile.
- Note - This section lets you *manage* the procedures on a specific profile. The procedures themselves are actually created at 'Configuration Templates' > 'Procedures'. **Click here** for help to configure a procedure.

**Add procedures to a profile**

- Click 'Configuration Templates' > 'Profiles'
- Open a Windows profile in the list
- Click 'Add Profile Section' > 'Procedures'



The 'Add' button lets you add and schedule a procedure which has been created in the 'Procedures' area.

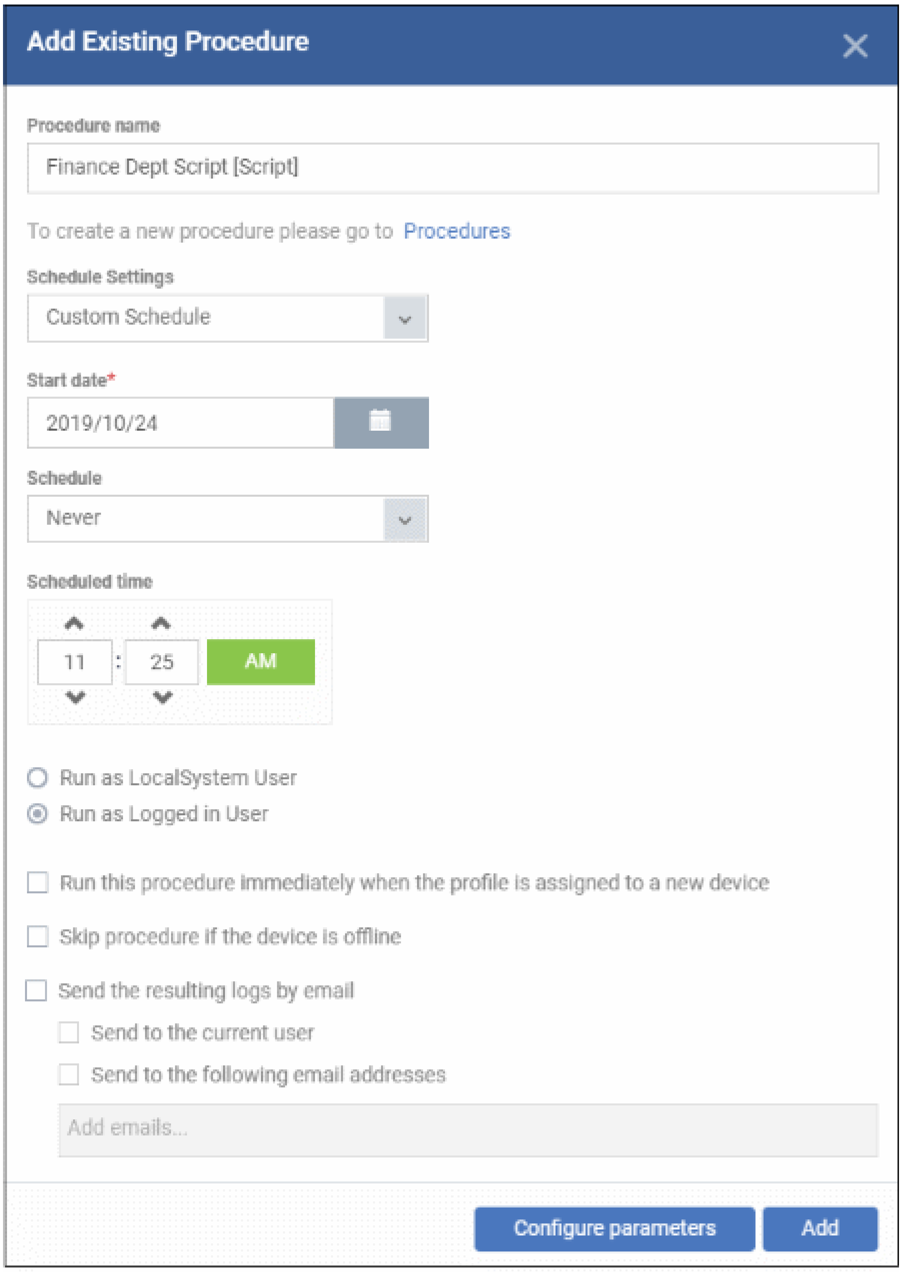
Click 'Save' to apply your changes.

| □ | ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | ADDED BY | ADDED ON | LAST MODIFIED BY | UPDATED AT |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Patch maintenance | Maintains the latest patches to be updated on the Windows Endpoint | Patch | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | | 2016/11/07 01:52:26 PM |
| ▣ | 2 | New 3rd Party App Patches | | 3rd Party Patch | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | herculespopular22@gmail.com | 2018/12/31 03:28:48 PM |
| □ | 3 | Script to check all my drivers for updates automatically | This Script to check all my drivers for updates automatically | Script | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | | 2018/04/27 06:30:19 PM |

Procedures are executed in numeric order. Select a procedure then use 'Move Up' or 'Move Down' controls to prioritize.

## Add a procedure

- Choose 'Procedures' from the 'Add Profile Section drop down' and click 'Add'.



Add Existing Procedure

Procedure name

Finance Dept Script [Script]

To create a new procedure please go to Procedures

Schedule Settings

Custom Schedule

Start date*

2019/10/24

Schedule

Never

Scheduled time

11 : 25 AM

○ Run as LocalSystem User

● Run as Logged in User

□ Run this procedure immediately when the profile is assigned to a new device

□ Skip procedure if the device is offline

□ Send the resulting logs by email

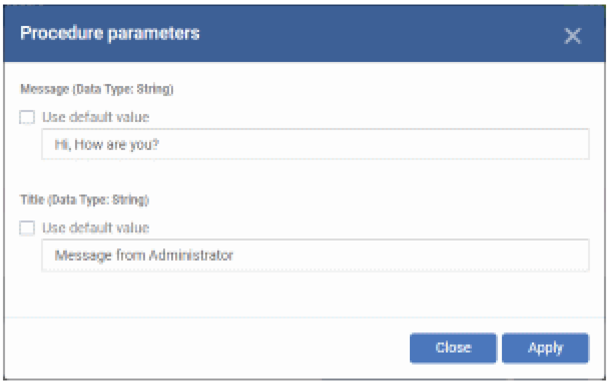
□ Send to the current user

□ Send to the following email addresses

Add emails...

| Add Existing Procedure to a Profile - Form Parameters | |
|---|---|
| **Parameter** | **Description** |
| Procedure Name | Choose an existing 'Script', 'Patch' or '3rd Party Patch procedure by typing the first few characters of the procedure name. Make sure you have already approved the procedure.<br>See **View and Manage Procedures** for help to configure procedures in EM. |
| Schedule Settings | Two options are available - 'Schedule on a maintenance window' and 'Custom schedule'.<br>**Custom Schedule**<br>Set a time-slot for the procedure to run on devices which use this profile (optional).<br>• Select the 'Start date' for the procedure by clicking the calendar icon beside 'Start Date'..<br>• Select the period for the schedule from the 'Schedule' drop-down. The |

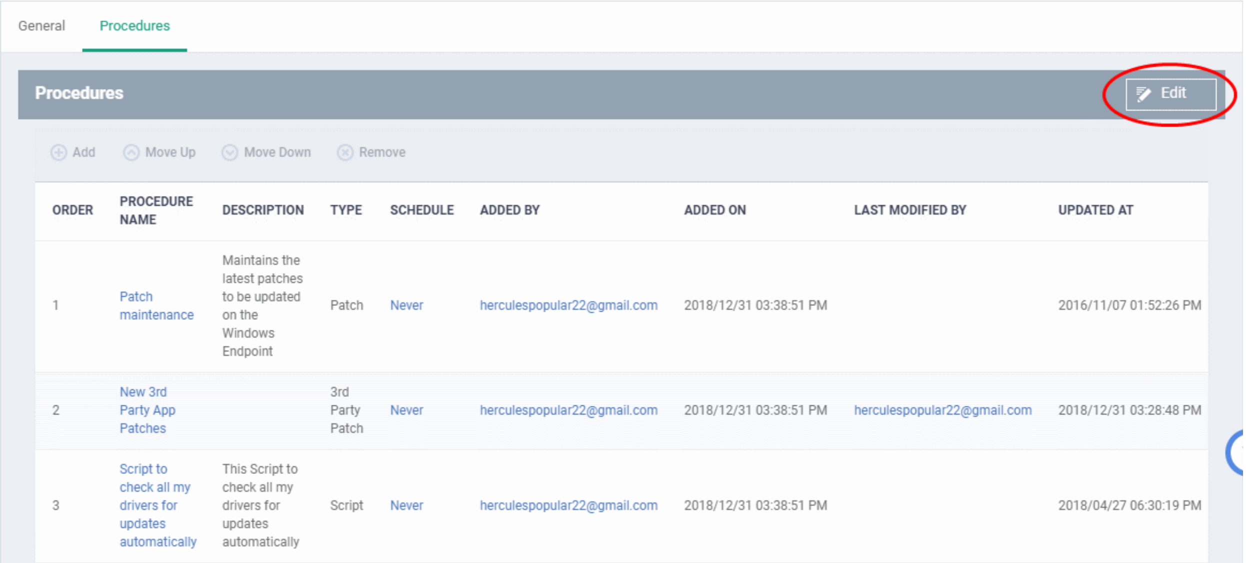
| | |
|---|---|
| | available options are:<br>• Never<br>• Daily<br>• Weekly - Select the days of the week that the procedure should run.<br>• Monthly - Select the dates of a month that the procedure should run.<br>• Set the time at which the procedure should run.<br>• If you select 'Daily', 'Weekly', 'Monthly' then specify the end-time settings for the procedure:<br>• No end settings - All procedures will run to completion.<br>• Run until - Chose a cut-off time from the calendar.<br>• Run no more than - Specify how long the procedure should run.<br>• Run until the end of the closest maintenance window - The procedure will start at the time you set, and must finish by the end of the first maintenance window after schedule start.<br>• Note - For the last three settings, any procedure that does not finish by the cut-off time is aborted and all changes undone.<br>**Schedule on a maintenance window**<br>• **Maintenance Window Type** - Choice of 'Daily', 'Weekly', 'Monthly' and 'Week of month'. This is the frequency you selected when you created the maintenance window. See '**Maintenance Window**' if you have not yet created a maintenance window.<br>• **Maintenance Window Name** - Shows a list of maintenance windows which have the frequency you chose in the 'Window Type' box above. Select the window you want to add to the procedure.<br>• **End Time Settings:**<br>• No end settings - All procedures will run to completion.<br>• Run until - Chose a cut-off time from the calendar.<br>• Run no more than - Specify how long the procedure should run.<br>• Note - For the last two settings, any procedure that does not finish by the cut-off time is aborted and all changes undone. |
| User Account Options | • Choose 'Run as system user' or 'Run as logged in user' based on the access rights required for the procedure to run at the endpoint.<br>• This applies only to 'Script' procedure |
| Execution Options | **Run this procedure immediately when the profile is assigned to a new device**<br>The procedure will run on target devices as soon as the profile is applied to the device, in addition to any schedule.<br>**Skip procedure if the device is offline**<br>The procedure will be aborted is the device is not connected to EM at the time of execution.<br>By default, procedures are queued for later deployment if the device is not connected to EM. The task will be executed as soon as it comes online.<br>• Select this option If you do not want the task to be added to the queue. |
| **Report Options** | Script procedures only |

| | |
|---|---|
| | - **Send to current user -** Procedure results are sent to the admin who is currently logged into Endpoint Manager.<br>- **Send to the following email addresses -** Add email addresses to whom log results should be sent. |
| **Configure parameters** | Only for script procedures with variable parameters.<br>- Click 'Configure parameters'<br><br>Procedure parameters<br>Message (Data Type: String)<br>□ Use default value<br>Hi, How are you?<br>Title (Data Type: String)<br>□ Use default value<br>Message from Administrator<br> <br>- Use the default values or choose a new value.<br>- Click 'Apply' |

- Click 'Add'
- Repeat the process to add multiple procedures to the profile
- Click 'Save' to add the procedures to the profile

**Edit a procedure:**

- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile containing the procedures component to be edited
- Click the 'Procedures' tab
- Click 'Edit' and select the procedure that needs to be modified.
- Modify the procedure as required and save it



| ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | ADDED BY | ADDED ON | LAST MODIFIED BY | UPDATED AT |
|---|---|---|---|---|---|---|---|---|
| 1 | Patch maintenance | Maintains the latest patches to be updated on the Windows Endpoint | Patch | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | | 2016/11/07 01:52:26 PM |
| 2 | New 3rd Party App Patches | | 3rd Party Patch | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | herculespopular22@gmail.com | 2018/12/31 03:28:48 PM |
| 3 | Script to check all my drivers for updates automatically | This Script to check all my drivers for updates automatically | Script | Never | herculespopular22@gmail.com | 2018/12/31 03:38:51 PM | | 2018/04/27 06:30:19 PM |

- Then click either 'Add', 'Move Up', 'Move down', or 'Remove' based on the changes that need to take effect.

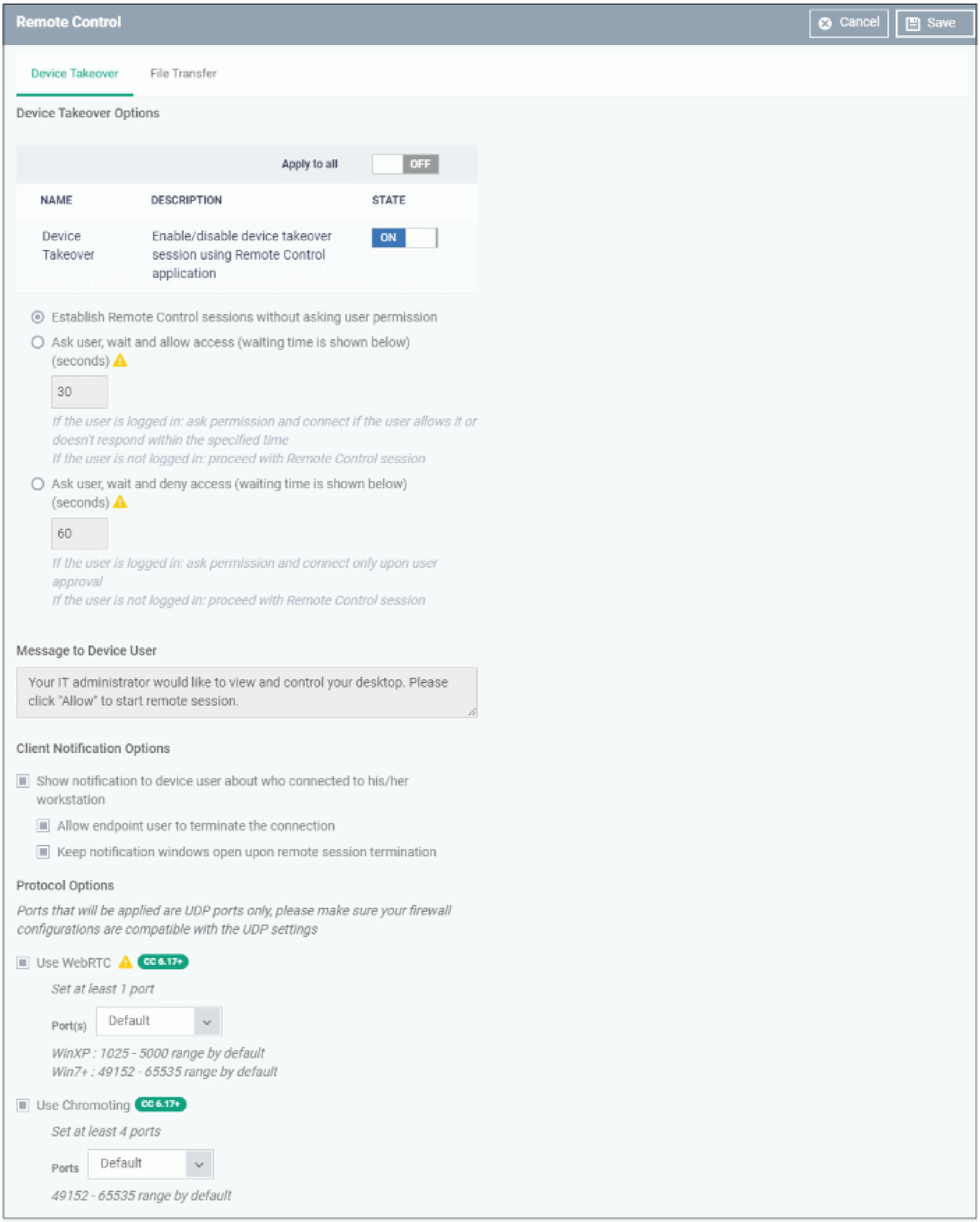
- Click 'Add' to add another procedure to the existing list
    - Click 'Move Up' to increase the priority of the procedure.
    - Click 'Move Down' to decrease the priority of the procedure.
    - Click 'Remove' to delete the procedure.
- Click 'Save'.

### 6.1.3.1.19. Remote Control Settings

- 'Remote Control' settings let you choose the protocol and ports used for remote connections.
- You can also configure takeover requests, endpoint notifications, and file transfer operations

**Configure Remote Control Settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile that you want to configure (click the profile name to do this)
- Click 'Add Profile Section' > Choose 'Remote Control' from the drop-down.
    - If 'Remote Control' is not available then it has already been added to the profile.
- Click the 'Remote Control' tab on the profile file-menu:



Device Takeover Options

| | Apply to all | OFF |
|---|---|---|
| NAME | DESCRIPTION | STATE |
| Device Takeover | Enable/disable device takeover session using Remote Control application | ON |

● Establish Remote Control sessions without asking user permission

○ Ask user, wait and allow access (waiting time is shown below) (seconds) ⚠

30

*If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time*
*If the user is not logged in: proceed with Remote Control session*

○ Ask user, wait and deny access (waiting time is shown below) (seconds) ⚠

60

*If the user is logged in: ask permission and connect only upon user approval*
*If the user is not logged in: proceed with Remote Control session*

Message to Device User

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

☑ Show notification to device user about who connected to his/her workstation

☑ Allow endpoint user to terminate the connection

☑ Keep notification windows open upon remote session termination

Protocol Options

*Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings*

☑ Use WebRTC ⚠ CC 6.17+

*Set at least 1 port*

Port(s) Default

*WinXP : 1025 - 5000 range by default*
*Win7+ : 49152 - 65535 range by default*

☑ Use Chromoting CC 6.17+

*Set at least 4 ports*

Ports Default

*49152 - 65535 range by default*

There are two tabs, 'Device Takeover' and 'File Transfer'. These two are independent of each other. You can disable device takeover and still enable file transfer operations.

- Configure device takeover
- Configure file transfer

## Device Takeover Options:

Click the 'Device Takeover' tab if not already open.

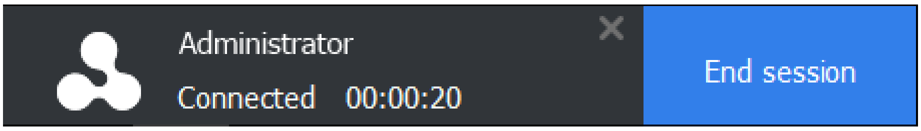
- **Apply to all** - Master switch to control the options below. The 'On/Off' switch currently only applies to the device takeover option.
- **Device Takeover** - Enable or disable the ability to take remote control of endpoints
- **Establish Remote Control sessions without asking user permission** - The remote connection is established without showing a request to the user.
- **Ask user, wait and allow access (waiting time is shown below)** - A message is shown to the user which requests them to accept the connection. The connection is established if the user does not respond within the timeout period.
  - Enter the timeout period (in seconds) in the text box
- **Ask user, wait and deny access (waiting time is shown below)** - A message is shown to the user which requests them to accept the connection. The connection attempt is abandoned if the user does not respond within the timeout period.
  - Enter the timeout period (in seconds) in the text box

### Message to Device User

- Enter the text of the request message. For example, 'Your administrator would like to take control of your desktop. Click 'Allow' to accept the connection request.'
- Please note that you can enter the message only on choosing the second or third notification options from the remote control settings.

### Client Notification Options

This area lets you configure the notification box which is shown on the endpoint when a remote session is active:



- Show notification to device user about who... - Enable or disable the notification box
  - Allow endpoint user to terminate the connection - Choose whether or not the 'End Session' button is shown in the notification box. If enabled, the end-user will be able to close the connection.
  - **Keep notification windows open upon termination** - The notification box will stay open on the endpoint even after the session is over. Users can close the box at their discretion.

### Protocol Options

These options let you configure the protocol used for the remote session.

- These settings apply to RC version 6.17 and above.
- You can also specify custom ports to be used by the protocol for an additional layer of safety. This allows you to keep only the specified ports open and block other ports for security.

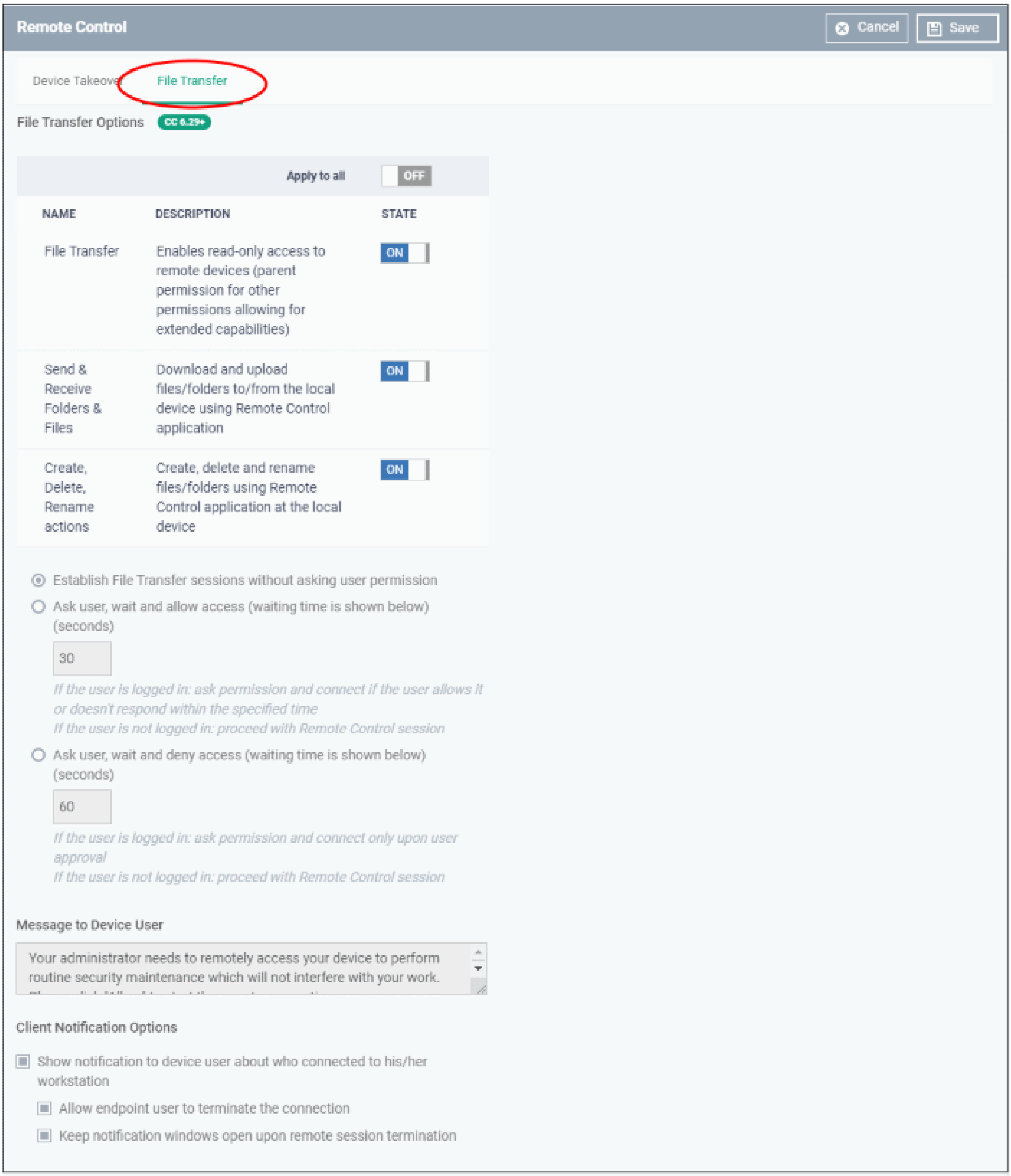
**Note**: Please make sure you do not assign well-known special ports. We recommend the following port range for custom use: 49152-65535.

- Use WebRTC - RC uses WebRTC protocol to connect to the device. This option is mandatory and cannot be deselected.
- Ports - Select the port type to be used by WebRTC protocol and specify the ports. The available options are:
  - Default - WebRTC will use port range 1025 - 5000 for Windows XP and port range 49152 - 65535 for Windows 7 and later versions
  - Custom - Allows you to specify a single custom port to be used by WebRTC
  - Custom Range - Allows you to specify a port range to be used by WebRTC

  - Use Chromoting - Chromoting provides a better quality of remote control and experience and is supported only by Windows 7 and later.
    - If selected, RC uses Chromoting to connecting to devices Windows 7 and later and use WebRTC for Windows XP devices.
    - If not selected, RC will use only WebRTC to connect to devices with any Windows version.
  - Ports - Select the port type to be used by Chromoting protocol and specify the ports. The available options are:
    - Default - Chromoting will use the port range 49152 - 65535
    - Custom Range - Allows you to specify a port range to be used by Chromoting. Enter a range covering at least 4 ports.
- Click 'Save' to apply your changes to the profile.

### File Transfer Options

- Click the 'File Transfer' tab



File Transfer Options CC 6.29+

Apply to all OFF

| NAME | DESCRIPTION | STATE |
|---|---|---|
| File Transfer | Enables read-only access to remote devices (parent permission for other permissions allowing for extended capabilities) | ON |
| Send & Receive Folders & Files | Download and upload files/folders to/from the local device using Remote Control application | ON |
| Create, Delete, Rename actions | Create, delete and rename files/folders using Remote Control application at the local device | ON |

● Establish File Transfer sessions without asking user permission

○ Ask user, wait and allow access (waiting time is shown below) (seconds)

30

*If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time*
*If the user is not logged in: proceed with Remote Control session*

○ Ask user, wait and deny access (waiting time is shown below) (seconds)

60

*If the user is logged in: ask permission and connect only upon user approval*
*If the user is not logged in: proceed with Remote Control session*

Message to Device User

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work.

Client Notification Options

☒ Show notification to device user about who connected to his/her workstation

☒ Allow endpoint user to terminate the connection

☒ Keep notification windows open upon remote session termination

- **Apply to all -** Master switch to the control options below.
- **File Transfer -** Allows admins to view files/folders on remote devices. You can enable this setting in isolation if you only want admins to have read-access to the remote device.
- You must enable this setting in order to enable the two more powerful settings below:
- **Send & Receive Folders & Files -** Enable admins to transfer files/folders between the admin computer and the remote computer.
- **Create, Delete, Rename actions -** Enable admins to perform file operations on the remote computer.

The user permission settings are the same, or very similar, to those described in the 'Device Takeover' section above.

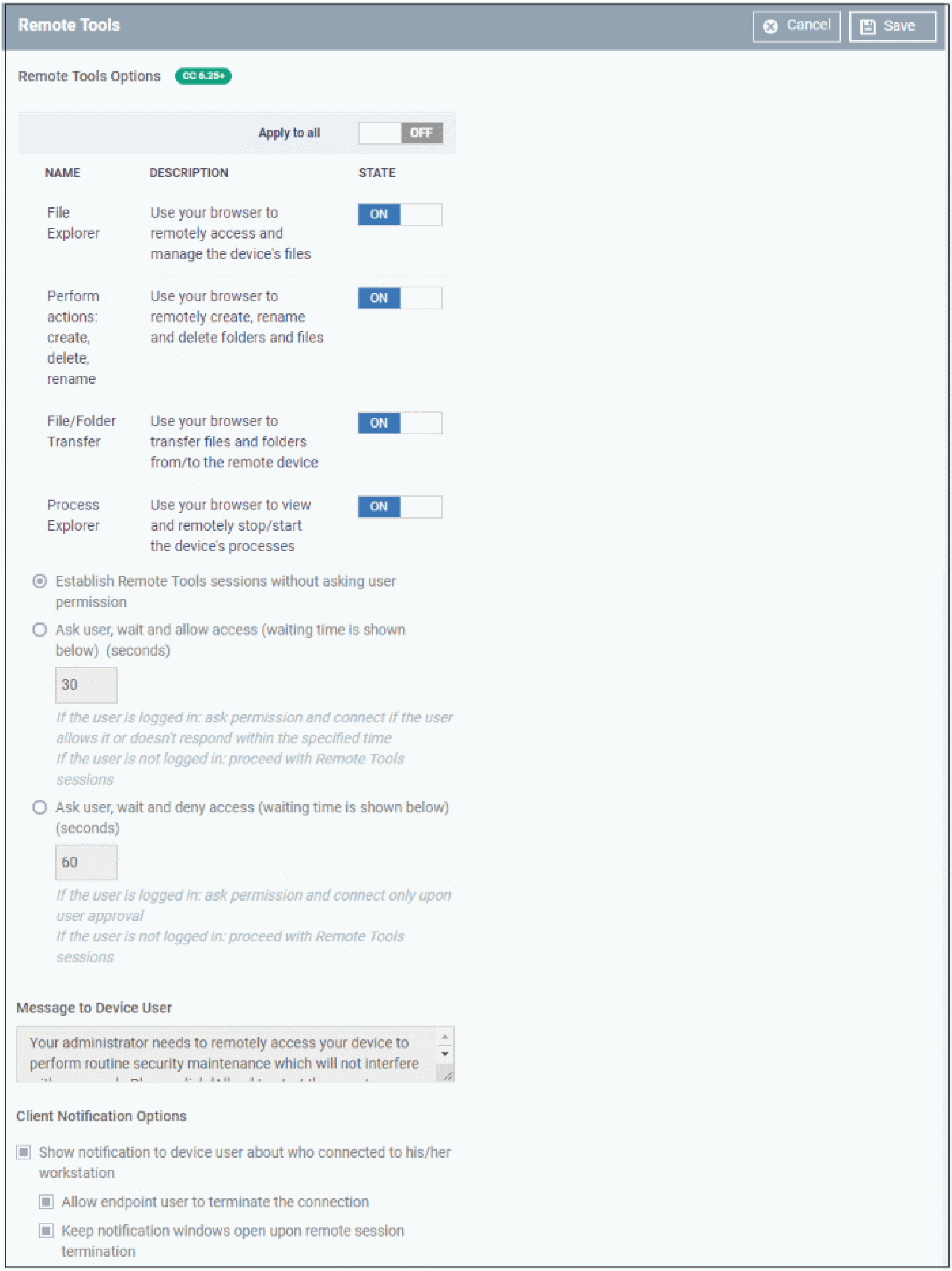
- Click 'Save' to apply your changes to the profile.

### 6.1.3.1.20. Remote Tools Settings

- Remote tool settings let you configure how you connect to managed endpoints
- There are two ways you can remotely connect:
    - **Remote Tools -** View and manage remote computers via the EM console. Click 'Devices' > 'Device List' > select a running Windows device > click 'Remote Tools' > 'File Explorer' / 'Process Explorer' / 'Service Explorer'.
    - **Remote Control -** Take-over the remote device like a traditional RDP connection. Click 'Devices' > 'Device List' > select a running Windows device > Click 'Remote Control'.
- The endpoint must have communication client v. 6.25 or higher installed to configure remote tool settings.

**Configure Remote Tools Settings**

- Click 'Configuration Templates' > 'Profiles'
- Open the profile that you want to configure (click the profile name to do this)
- Click 'Add Profile Section' and choose 'Remote Tools' from the drop-down.
    - If 'Remote Tools' is not in the 'Add...' menu then it has already been added to the profile.
    - Click the 'Remote Tools' tab on the profile file-menu:



Remote Tools Options

Apply to all OFF

| NAME | DESCRIPTION | STATE |
|---|---|---|
| File Explorer | Use your browser to remotely access and manage the device's files | ON |
| Perform actions: create, delete, rename | Use your browser to remotely create, rename and delete folders and files | ON |
| File/Folder Transfer | Use your browser to transfer files and folders from/to the remote device | ON |
| Process Explorer | Use your browser to view and remotely stop/start the device's processes | ON |

● Establish Remote Tools sessions without asking user permission

○ Ask user, wait and allow access (waiting time is shown below) (seconds)

30

*If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time*
*If the user is not logged in: proceed with Remote Tools sessions*

○ Ask user, wait and deny access (waiting time is shown below) (seconds)

60

*If the user is logged in: ask permission and connect only upon user approval*
*If the user is not logged in: proceed with Remote Tools sessions*

Message to Device User

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere

Client Notification Options

☑ Show notification to device user about who connected to his/her workstation

☑ Allow endpoint user to terminate the connection

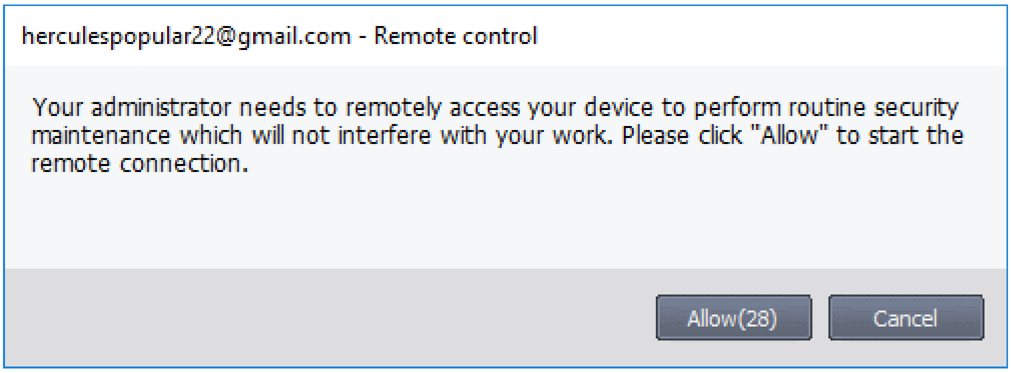
☑ Keep notification windows open upon remote session termination

**Remote Tools Options**:

- **File Explorer** - Enable the ability to view files on the remote system.
- **Perform actions** - Enable the ability to create / rename / move / delete files on the remote system.
- **File / Folder Transfer** - Enable the ability to copy files to and from the remote system.

- **Process Explorer** - Enable the ability to view and manage running processes and services on the remote system.
    - Alternatively, use the 'Apply to all' switch at the top to enable or disable all at-once.

- **Establish Remote Tools sessions without asking user permission** - The remote connection will be established without showing a request to the user.
- **Ask user, wait and allow access** - A message is shown to the user which requests them to accept the connection. The connection is established if the user does not respond within the timeout period.
    - Enter the timeout period (in seconds) in the text box
    - An example request message is shown below:



herculespopular22@gmail.com - Remote control

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work. Please click "Allow" to start the remote connection.

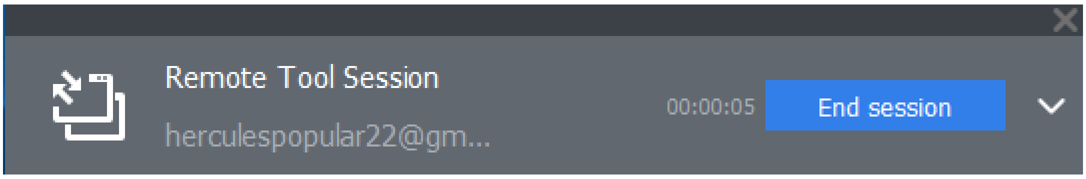
- **Ask user, wait and deny access** - A message is shown to the user which requests them to accept the connection. The connection attempt is abandoned if the user does not respond within the timeout period.
    - Enter the timeout period (in seconds) in the text box

**Message to Device User**

- Enter the text of the request message. For example, 'Your administrator needs to remotely access your device to perform routine maintenance. Please click "Allow" to start the remote connection.'
- Note - You can only enter a message if you choose one of the 'Ask...' settings.

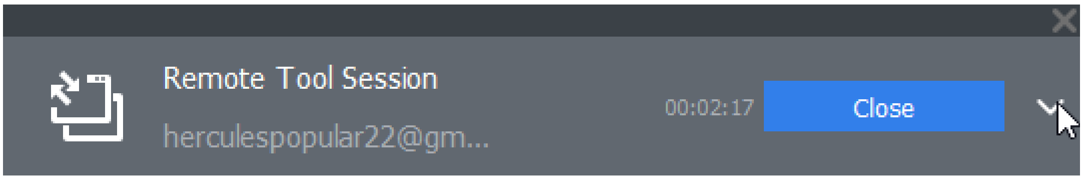
**Client Notification Options**

This area lets you configure the notification box which is shown on the endpoint when a remote session is active. An example is shown below:



The end-user can view the actions taken on the endpoint by clicking the down arrow at the right of the notification box.

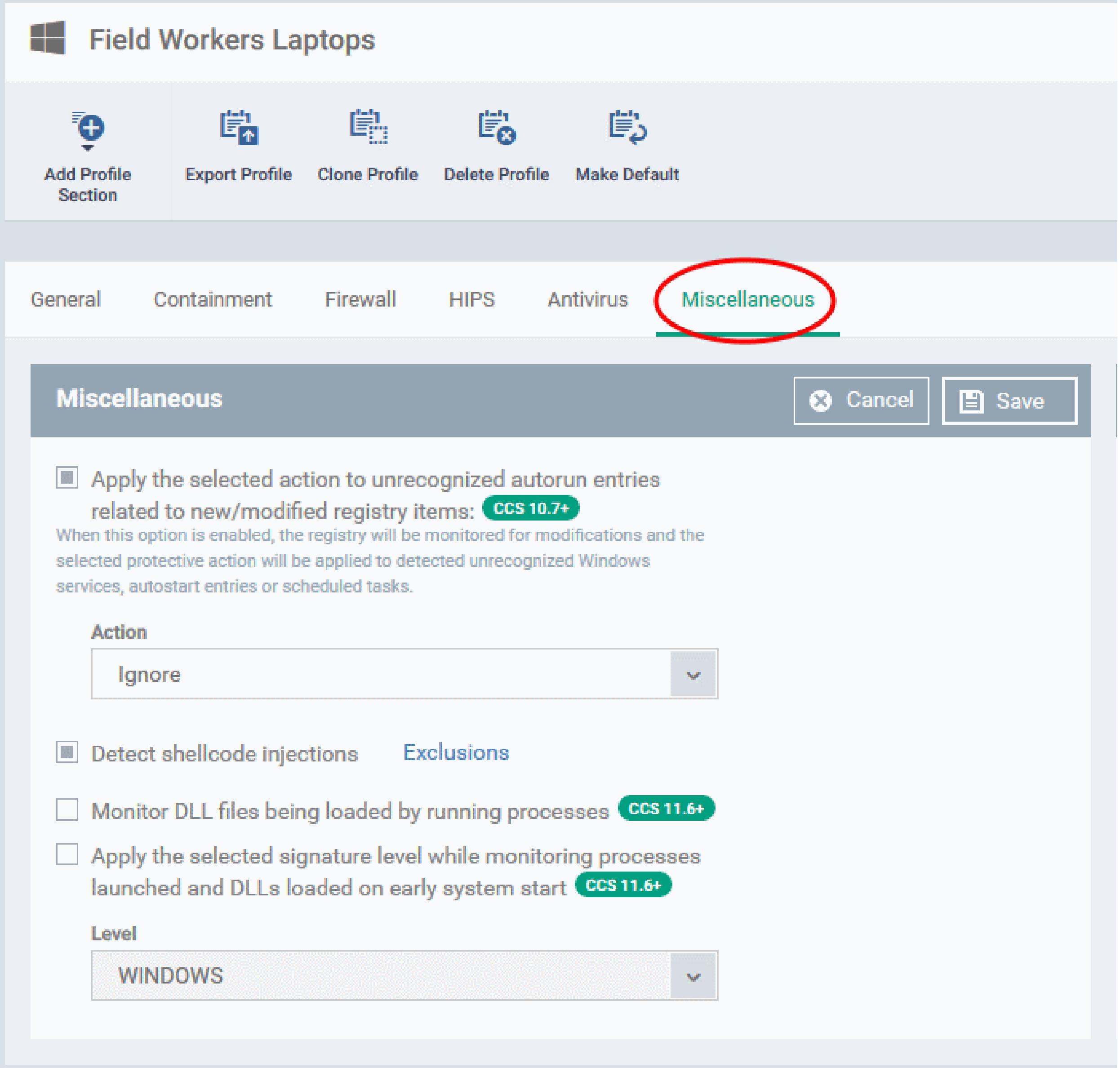
- **Show notification to device user about who connected to his/her workstation** - Enable or disable the notification box
    - **Allow endpoint user to terminate the connection** - Choose whether or not the 'End Session' button is shown in the notification box. If enabled, the end-user will be able to close the connection.
    - **Keep notification windows open upon remote session termination** - Choose whether or the notification box should be shown on the endpoint after the session is completed.



### 6.1.3.1.21. Miscellaneous Settings

- Click 'Configuration Templates' > 'Profiles'
- Click the name of a Windows profile
- Click 'Add Profile Section' > 'Miscellaneous'

The 'Miscellaneous' settings screen opens:



☑ Apply the selected action to unrecognized autorun entries related to new/modified registry items: CCS 10.7+

When this option is enabled, the registry will be monitored for modifications and the selected protective action will be applied to detected unrecognized Windows services, autostart entries or scheduled tasks.

Action: Ignore

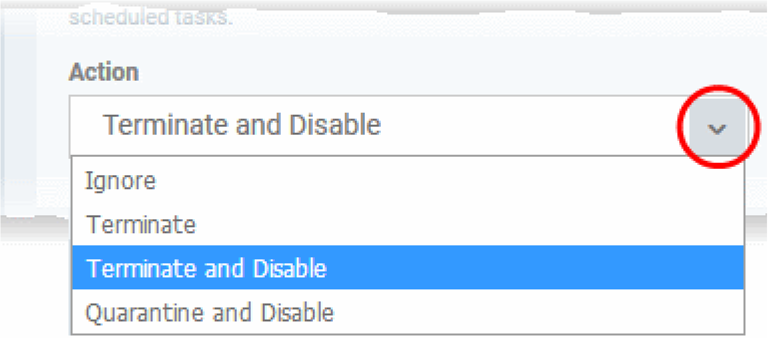
☑ Detect shellcode injections   Exclusions

☐ Monitor DLL files being loaded by running processes CCS 11.6+

☐ Apply the selected signature level while monitoring processes launched and DLLs loaded on early system start CCS 11.6+

Level: WINDOWS

- **Apply the selected action to...**' - CCS will monitor registry entries related to Windows services, auto-run items and scheduled tasks. If any entries are created or modified by unrecognized files/scripts, they will handled per the action chosen. (***Default = Enabled***)



scheduled tasks.

Action

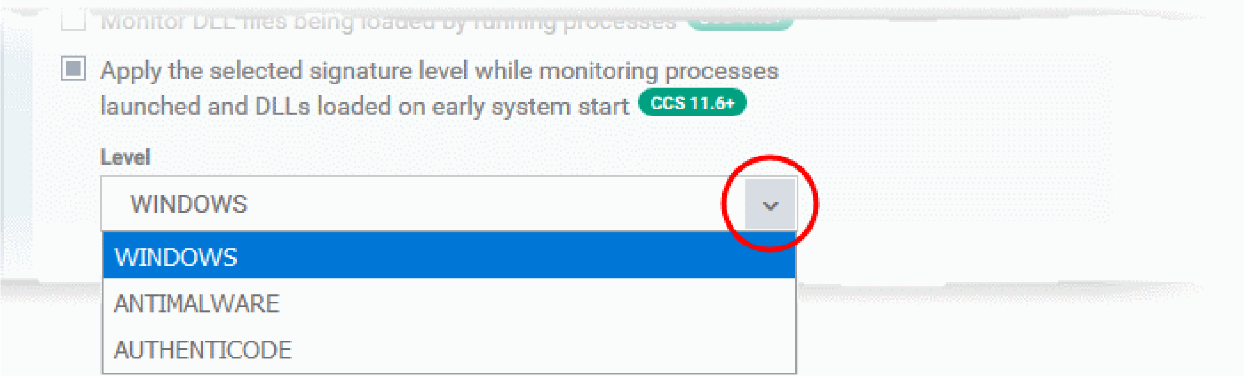
Terminate and Disable

- **Detect shellcode injections:**
    - A shellcode injection is an attack which exploits software vulnerabilities to give attackers control of a compromised machine.
    - For example, shellcode attacks are often used to create buffer-overflows on victim machines. Enable this setting to turn-on buffer overflow protection.
    - By default, Comodo Client Security (CCS) monitors all applications to make sure they do not suffer shellcode attacks.
    - However, you may want to omit certain applications from protection for compatibility reasons. Click the 'Exclusions' link to do this.
    - The process to **add exclusions** is similar to that explained in **Containment Settings**.

  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. As such, buffer overflows cause many software vulnerabilities and are the basis of many exploits.

  Comodo recommends this setting is left enabled (***Default* = *Enabled***).

- **Monitor DLL files being loaded by running processes** - CCS monitors the DLL files loaded to system memory, by processes that are currently running on the endpoint (***Default* = *Disabled***).
    - If enabled, CCS runs a file rating scan on each DLL loaded to identify its trust rating.
    - The trust rating is reported to Endpoint Manager. Files with an Unrecognized' rating are submitted to Valkyrie for analysis.
    - You can view these details at 'Security Sub-Systems' > 'Application Control'. See **Manage File Trust Ratings on Windows Devices** for more details.
- **Apply the selected signature level while....** - CCS identifies untrusted DLLs, apps, portable executables (PE) and autoruns launched before CCS starts on the endpoint. These may expose the endpoint to a danger if those items turn to be malicious. (***Default* = *Disabled***)
    - CCS checks whether startup items are signed by a trusted authority and marks them as trusted or untrusted. The flag is used at next restart to allow or block the item.
    - You can choose how strict the certificate check should be:



☐ Monitor DLL files being loaded by running processes

☑ Apply the selected signature level while monitoring processes launched and DLLs loaded on early system start CCS 11.6+

Level

WINDOWS

  - **Windows**- Only items signed by Microsoft certificates are marked as trusted
  - **Antimalware** - Trusts files signed by either Microsoft or Antimalware certificates
  - **Authenticode** - Flags all signed files as trusted
- Click 'Save' to apply your changes to the profile.

### 6.1.3.1.22. Script Analysis Settings

- CCS can analyze code in executable files in two ways:
  - Heuristic command line analysis
  - Embedded Code Detection
- You can enable these features and select the programs you want to monitor by adding a 'Script Analysis' section to a profile.
- You can also monitor programs which try to make changes to auto-run entries, Windows services and scheduled tasks

**Background**:

**Heuristic command line analysis:**

- Heuristic techniques identify previously unknown viruses and Trojans.
- Files are analyzed to ascertain whether they contain code typical of a virus.
- In other words, heuristics identifies files which have virus-like attributes, instead of looking for a signature that matches a signature on the blacklist.
- This allows the engine to predict the existence of new viruses - even if they are not in the current virus database.

**Embedded code detection:**

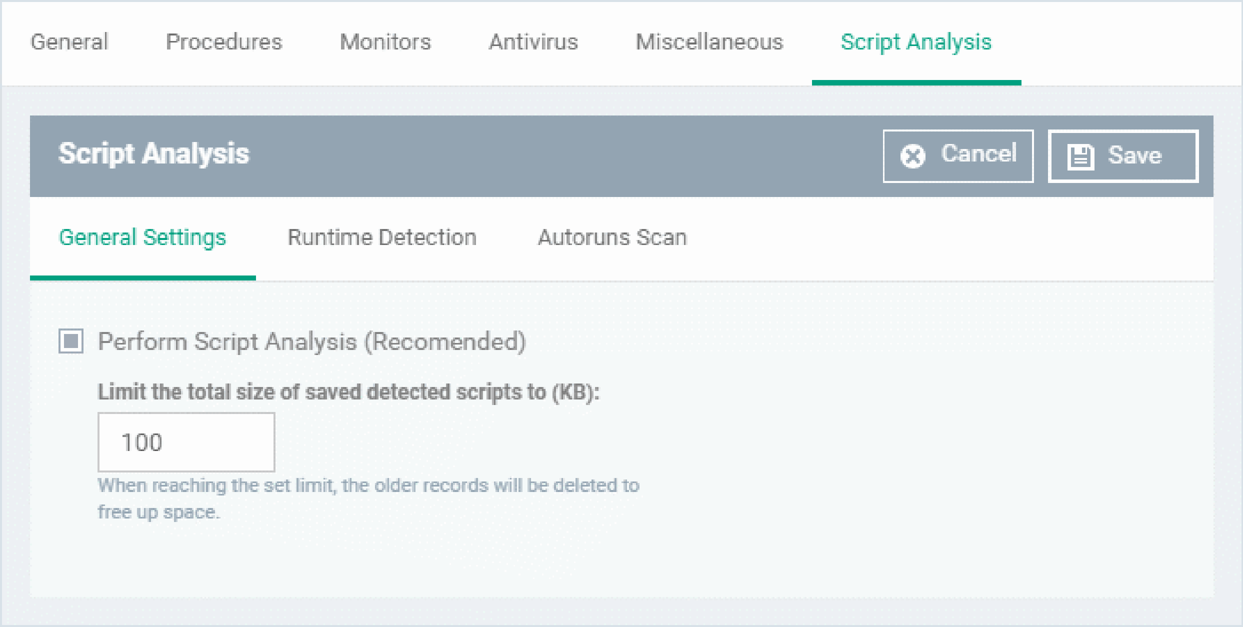
- Embedded code detection protects you against file-less malware attacks.
- File-less malware attacks allow malicious actors to directly execute powershell commands on your system.
- These commands can be used to take control of endpoints, install ransomware, steal confidential data and more.
- File-less scripts reside in memory so no trace of them remains after the computer is restarted.
- Example programs affected by 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, CCS detects c:/tests/test.vbs from the command-line and applies all security checks to this file.

  - Enabled - If test.vbs attempts to connect to the internet, the alert will state 'test.vbs' is attempting to connect to the internet
  - Disabled - The alert will only state 'wscript.exe' is trying to connect to the internet'.

**To configure 'Script Analysis' Settings**

- Click 'Configuration Templates' > 'Profiles'
- Click the name of a Windows profile
- Click 'Add Profile Section' > 'Script Analysis'



□ Perform Script Analysis (Recomended)

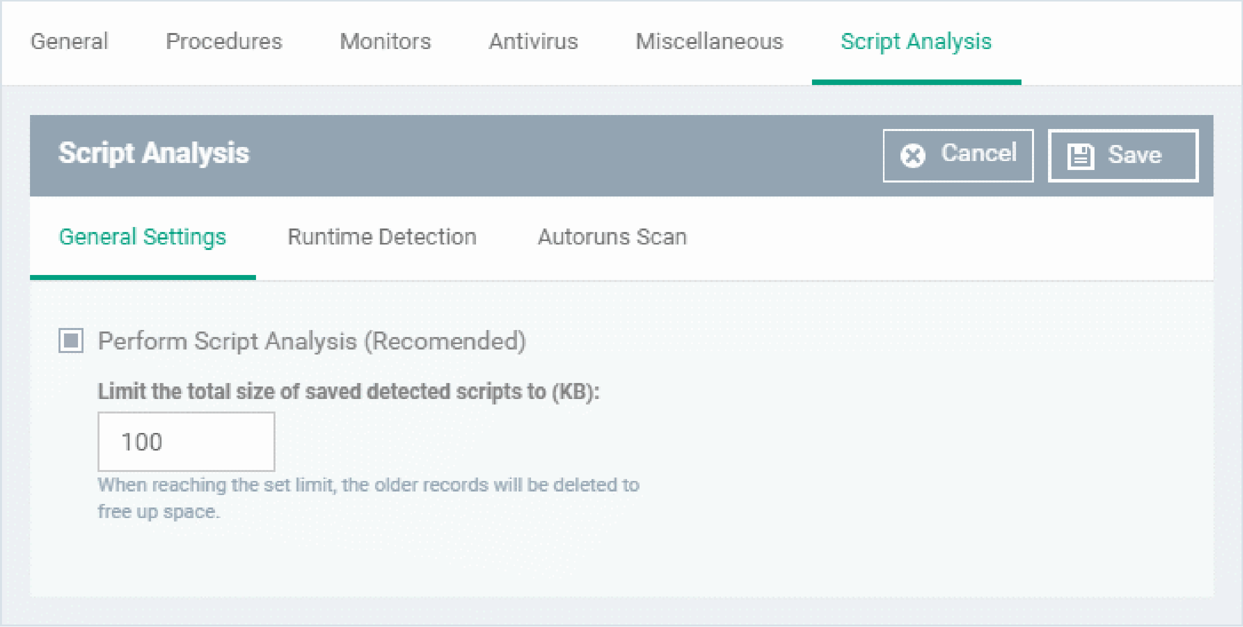
Limit the total size of saved detected scripts to (KB): 100

When reaching the set limit, the older records will be deleted to free up space.

The 'Script Analysis' settings screen contains three tabs:

- **General Settings** - Enable script analysis and set the maximum file size which should be checked.
- **Runtime Detection** - Select which programs are monitored throughout their operation.
- **Autoruns Scan** - Choose programs that you want to monitor to see if they make changes to auto-run entries, Windows services and scheduled tasks.

## General Settings



□ Perform Script Analysis (Recomended)

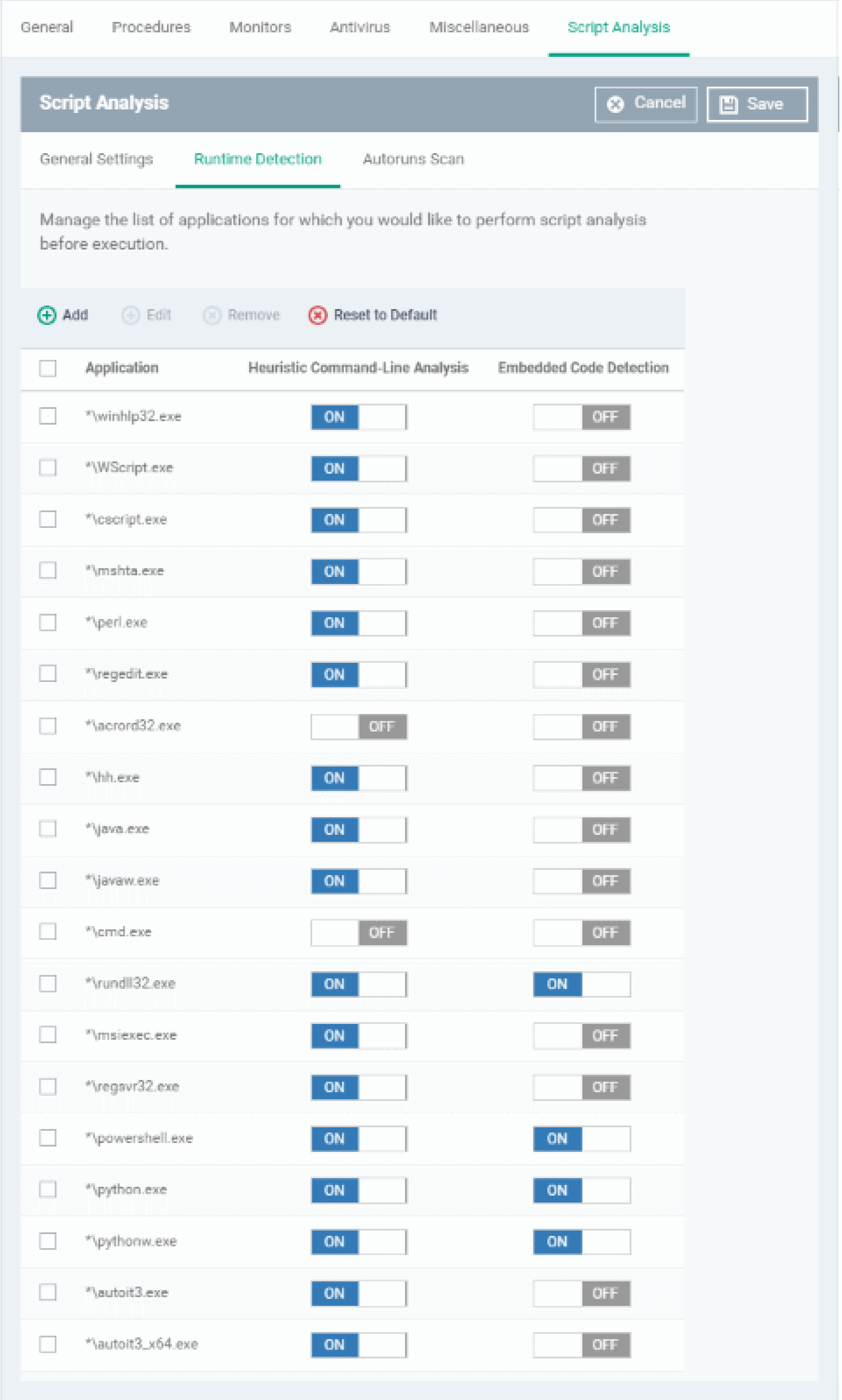
Limit the total size of saved detected scripts to (KB): 100

When reaching the set limit, the older records will be deleted to free up space.

- **Perform Script Analysis** - Enable/Disable script analysis. CCS will only analyze the applications selected in the 'Runtime Detection' tab if this option is enabled. An alert is generated if malicious code is found in any item. (***Default = Enabled***)
- **Limit the total size of saved detected scripts to** - CCS stores scripts run by managed applications for analysis. This option lets you specify the total size of stored scripts. When the set limit is reached, the older scripts are deleted automatically. (***Default = 100 KB***)

## Runtime Detection

- Lets you select executables which should be analyzed during their execution.
- You can also add custom applications which you want to protect.
- Click the 'Runtime Detection' tab in the 'Script Analysis' settings interface

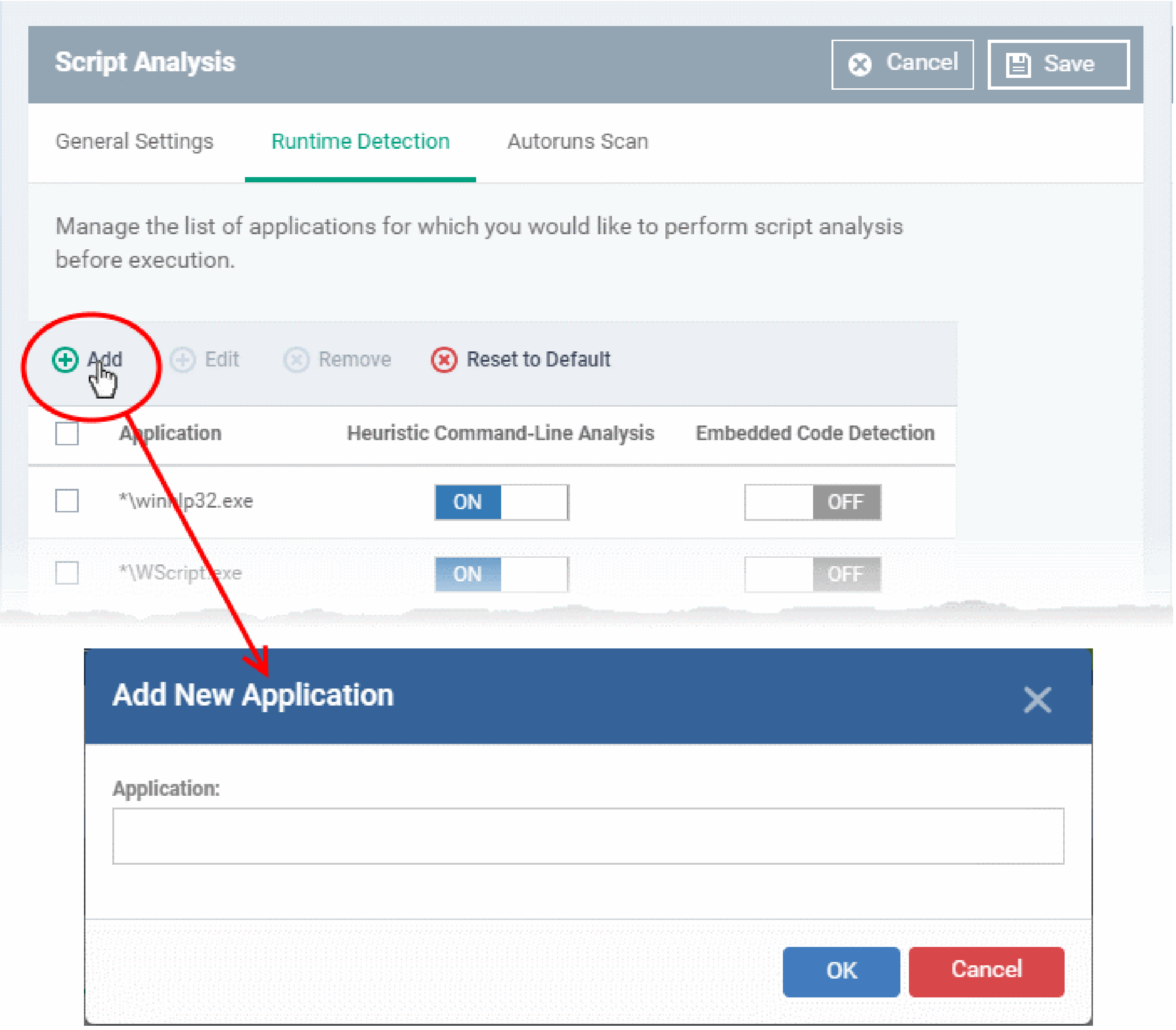


Manage the list of applications for which you would like to perform script analysis before execution.

| □ | Application | Heuristic Command-Line Analysis | Embedded Code Detection |
|---|---|---|---|
| □ | *\winhlp32.exe | ON | OFF |
| □ | *\WScript.exe | ON | OFF |
| □ | *\cscript.exe | ON | OFF |
| □ | *\mshta.exe | ON | OFF |
| □ | *\perl.exe | ON | OFF |
| □ | *\regedit.exe | ON | OFF |
| □ | *\acrord32.exe | OFF | OFF |
| □ | *\hh.exe | ON | OFF |
| □ | *\java.exe | ON | OFF |
| □ | *\javaw.exe | ON | OFF |
| □ | *\cmd.exe | OFF | OFF |
| □ | *\rundll32.exe | ON | ON |
| □ | *\msiexec.exe | ON | OFF |
| □ | *\regsvr32.exe | ON | OFF |
| □ | *\powershell.exe | ON | ON |
| □ | *\python.exe | ON | ON |
| □ | *\pythonw.exe | ON | ON |
| □ | *\autoit3.exe | ON | OFF |
| □ | *\autoit3_x64.exe | ON | OFF |

- Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command line analysis for each application.
- Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.

- Select an application and click the edit button to update its details.
- Select an application and click the trash can icon to remove it from the list.
- Click 'Add' at the top to include a new application to the list.



Manage the list of applications for which you would like to perform script analysis before execution.

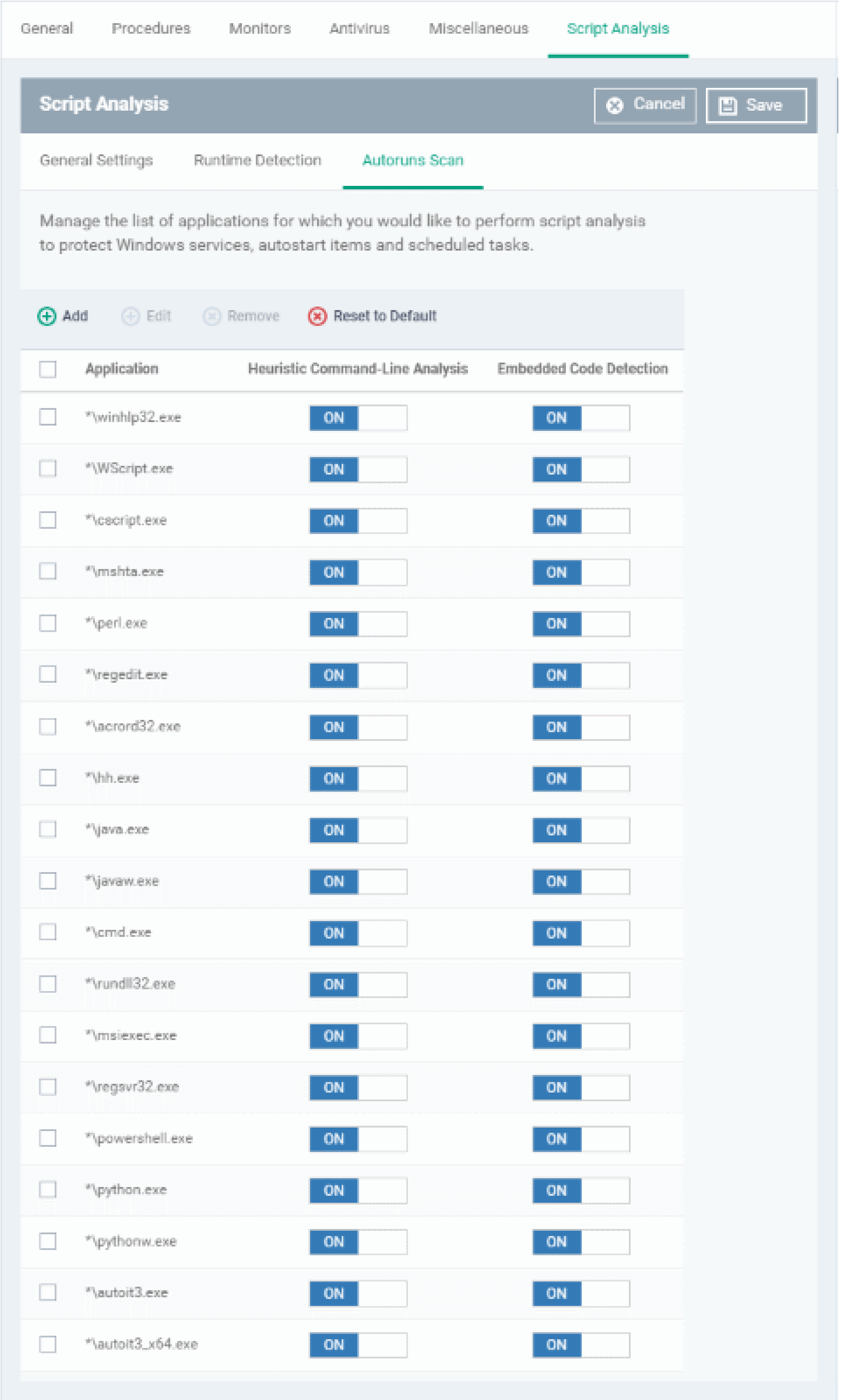
| □ | Application | Heuristic Command-Line Analysis | Embedded Code Detection |
|---|---|---|---|
| □ | *\winhlp32.exe | ON | OFF |
| □ | *\WScript.exe | ON | OFF |

- Enter the name of the application in the 'Add Application' dialog and click 'Add'.
- The new application will be added to the list and will be selected by default. You can use the toggle switch beside it to enable/disable it at any time.
- Repeat the process to add more applications

- To reset the list to the default list of applications, click 'Reset to Default' on the top
- Click 'OK' to apply your changes.

## Autoruns Scan

- Select applications which should be monitored in case they make changes to autoruns, Windows services or scheduled tasks.
- You can also add custom applications which you want to monitor.
- Click the 'Autoruns Scan' tab in the 'Script Analysis' settings interface

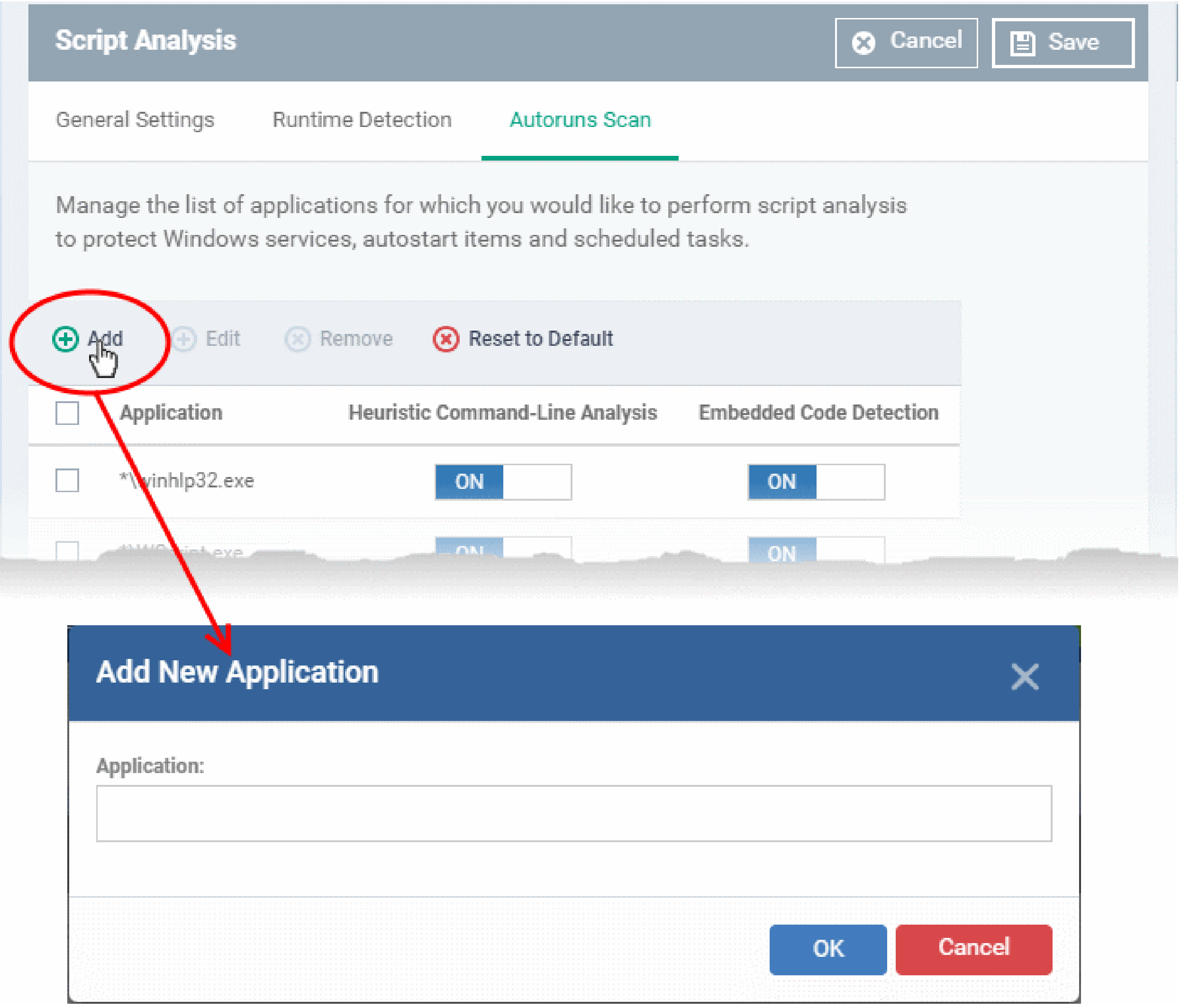


Manage the list of applications for which you would like to perform script analysis to protect Windows services, autostart items and scheduled tasks.

| □ | Application | Heuristic Command-Line Analysis | Embedded Code Detection |
|---|---|---|---|
| □ | *\winhlp32.exe | ON | ON |
| □ | *\WScript.exe | ON | ON |
| □ | *\cscript.exe | ON | ON |
| □ | *\mshta.exe | ON | ON |
| □ | *\perl.exe | ON | ON |
| □ | *\regedit.exe | ON | ON |
| □ | *\acrord32.exe | ON | ON |
| □ | *\hh.exe | ON | ON |
| □ | *\java.exe | ON | ON |
| □ | *\javaw.exe | ON | ON |
| □ | *\cmd.exe | ON | ON |
| □ | *\rundll32.exe | ON | ON |
| □ | *\msiexec.exe | ON | ON |
| □ | *\regsvr32.exe | ON | ON |
| □ | *\powershell.exe | ON | ON |
| □ | *\python.exe | ON | ON |
| □ | *\pythonw.exe | ON | ON |
| □ | *\autoit3.exe | ON | ON |
| □ | *\autoit3_x64.exe | ON | ON |

- Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command line analysis for each application.
- Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.

- Select an application and click the edit button to update its details.
- Select an application and click the trash can icon to remove it from the list.
- Click 'Add' at the top to include a new application to the list.



Manage the list of applications for which you would like to perform script analysis to protect Windows services, autostart items and scheduled tasks.

| □ | Application | Heuristic Command-Line Analysis | Embedded Code Detection |
|---|---|---|---|
| □ | *\winhlp32.exe | ON | ON |
| □ | *\WScript.exe | ON | ON |

- Enter the name of the application in the 'Add Application' dialog and click 'Add'.
- The new application will be added to the list and will be selected by default. You can use the toggle switch beside it to enable/disable it at any time.
- Repeat the process to add more applications

- To reset the list to the default list of applications, click 'Reset to Default' on the top
- Click 'OK' to apply your changes.

### 6.1.3.2. Import Windows Profiles

In addition to creating a new Windows profile from the Endpoint Manager interface, you can create new profiles for rolling out to endpoints or endpoint group(s) in the following ways:

- Import the security configuration of CCS from a managed endpoint and save it as a new profile
- Export a profile from EM in .cfg format then import it as a new profile
- Clone an existing profile and edit it to create a new profile

This section explains more about **importing CCS configuration from a selected endpoint**.

- For more details on **importing configurtion from an exported profile**, see **Export and Import Configuration Profiles**.
- For more details on creating a new profile by using an existing profile as base, see **Clone a Profile**.

#### Import CCS Configuration from a Managed Device

By importing the configuration of Comodo Client Security from an existing endpoint, you can create a Windows profile which can be deployed to similar machines on your network.

- **Step 1 - Export the current configuration from the selected device as an .xml file**
- **Step 2 - Import the .xml file as a profile to required endpoints or endpoint group(s).**

## Step 1 - Export the current configuration from the selected device as an .xml file

The current security configuration of the CCS installation on the endpoints depends on:

- The configuration profiles applied o the endpoint
- Manual configuration of the parameters at the endpoint.

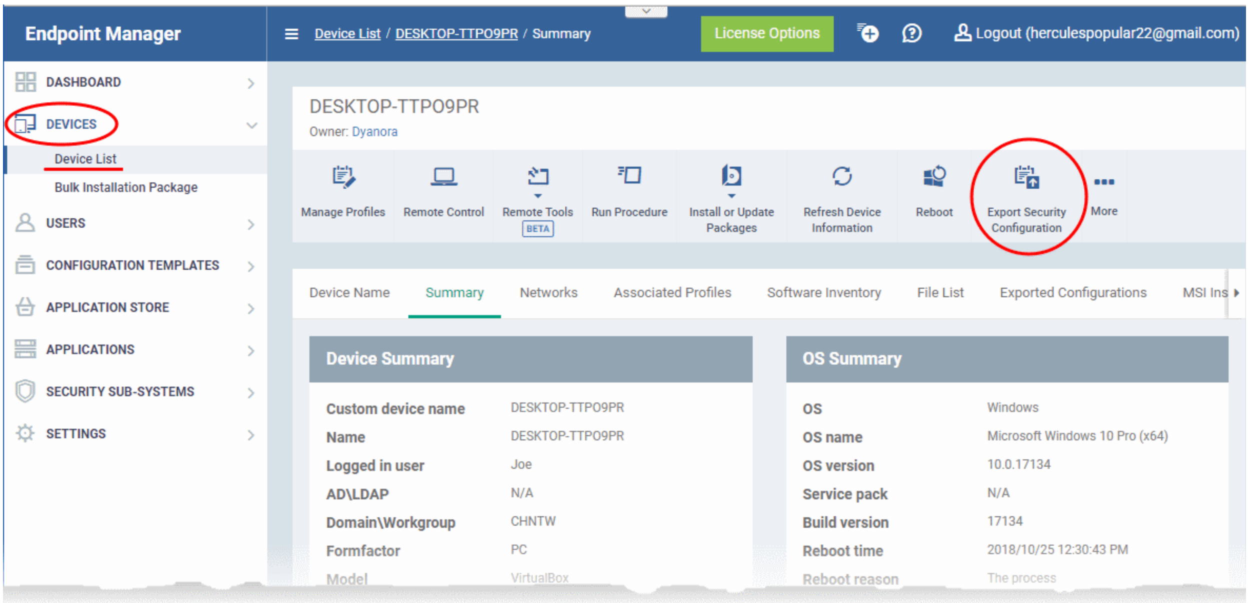
> **Note**: If you are manually configuring the security parameters, ensure that the option 'Enable local user to override profile configuration' is selected in the 'Client Access Control' section in the profile(s) in action on the endpoint. Otherwise your manual settings will be reverted and the security parameters will be automatically set as per the configuration profile(s) effective on the endpoint during the next polling cycle of the communication client. See **Client Access Control** for more details.

You can export the CCS configuration from a managed Windows device in two ways:

- **Export configuration of a selected device from EM interface**
- **Manually export the CCS configuration from the selected device**

## Export Configuration from EM interface

- Open the 'Device List' interface from the EM console by clicking 'Devices' > 'Device List' on the left
- Click the name of the device whose configuration you wish to export to open its 'Device Details'
- Click the 'Export Security Configuration' button:



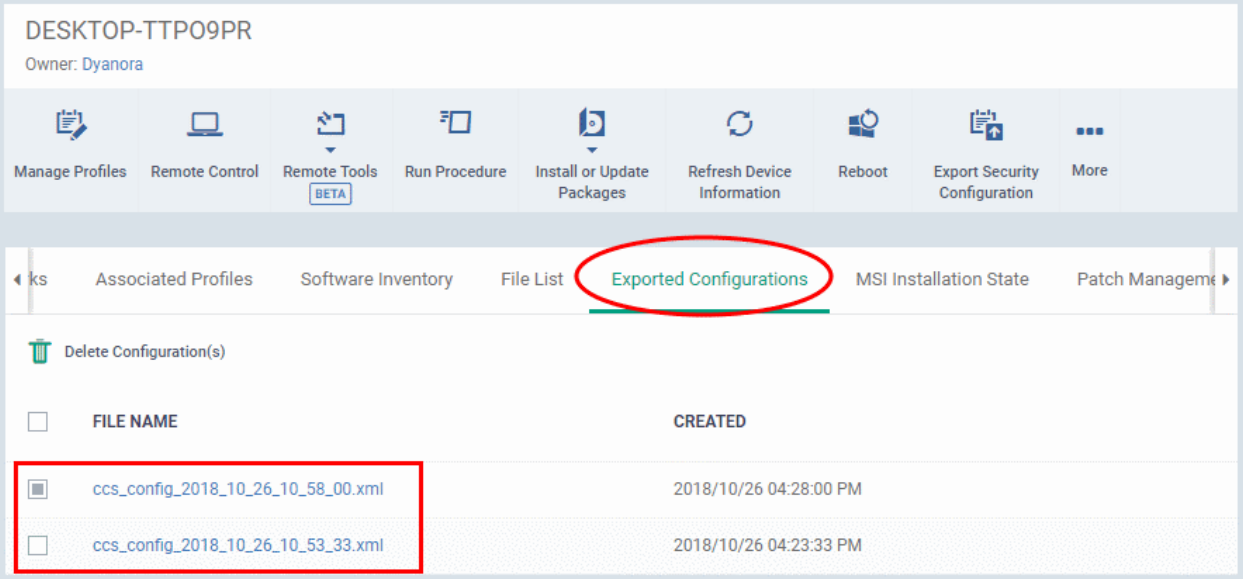
**Device Summary**

| | |
|---|---|
| Custom device name | DESKTOP-TTPO9PR |
| Name | DESKTOP-TTPO9PR |
| Logged in user | Joe |
| AD\LDAP | N/A |
| Domain\Workgroup | CHNTW |
| Formfactor | PC |
| Model | VirtualBox |

**OS Summary**

| | |
|---|---|
| OS | Windows |
| OS name | Microsoft Windows 10 Pro (x64) |
| OS version | 10.0.17134 |
| Service pack | N/A |
| Build version | 17134 |
| Reboot time | 2018/10/25 12:30:43 PM |
| Reboot reason | The process |

- The CCS configuration will be exported as a .xml file and saved in EM.
- You can view all configuration files exported from this device under the 'Exported Configurations' tab in 'Device Details':



| | FILE NAME | CREATED |
|---|---|---|
| ☐ | ccs_config_2018_10_26_10_58_00.xml | 2018/10/26 04:28:00 PM |
| ☐ | ccs_config_2018_10_26_10_53_33.xml | 2018/10/26 04:23:33 PM |

- Click the name of the file that you want to import as a profile and save it in a safe location.
- Then move on to **Step 2 - Import the .xml file as a profile to required endpoints or endpoint group(s)**.

**Manually export CCS configuration from a selected device**

- If you haven't done so already, configure the security settings of CCS at an endpoint to your requirements. See 'Advanced Settings' in the CCS guide if you need help with this - **https://help.comodo.com/topic-399-1-904-11732-CCS-Advanced-Settings.html**,
- To export the current configuration as an xml file, the following command locally on the endpoint:

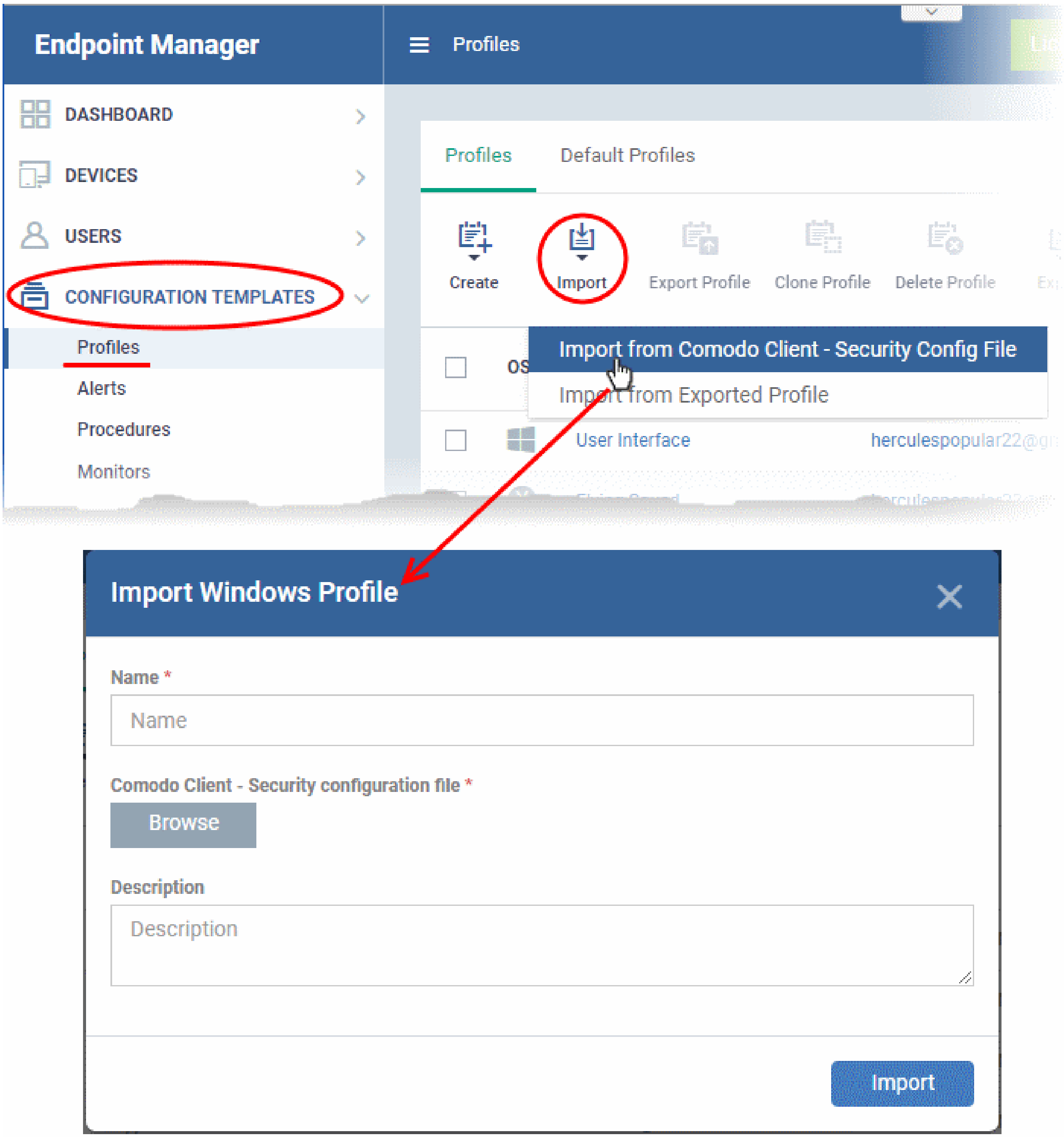
  ```
  C:\[installation folder of CCS]\cfpconfg.exe --xcfgExport="C:\<filename>.xml" --filter=""
  ```

  For example, C:\Program Files\COMODO\COMODO Internet Security\cfpconfg.exe --xcfgExport="C:\winconfigprofile.xml" --filter=""

- Copy the .xml file from the endpoint to the computer from which the EM console is accessed.
- Then move on to **Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)**.

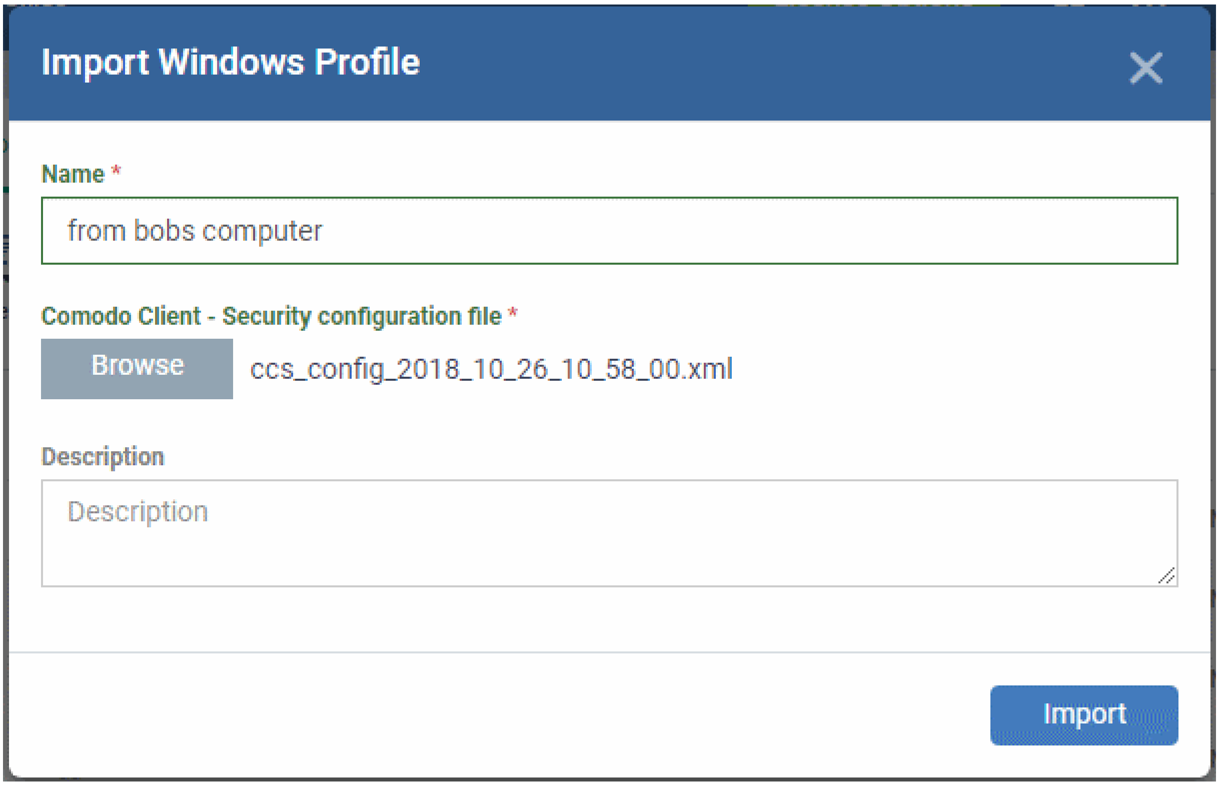
## Step 2 - Import the .xml file as a profile for application to required endpoints or endpoint group(s)

- Click 'Configuration Templates' > 'Profiles'
- Click 'Import' > 'Import from 'Comodo Client Security Config file'



The 'Import Windows Profile' opens.

- Enter a name and description for the profile.
- Click 'Browse', navigate to the location in your computer where the .xml file is saved, select the file and click 'Open'.


Import Windows Profile

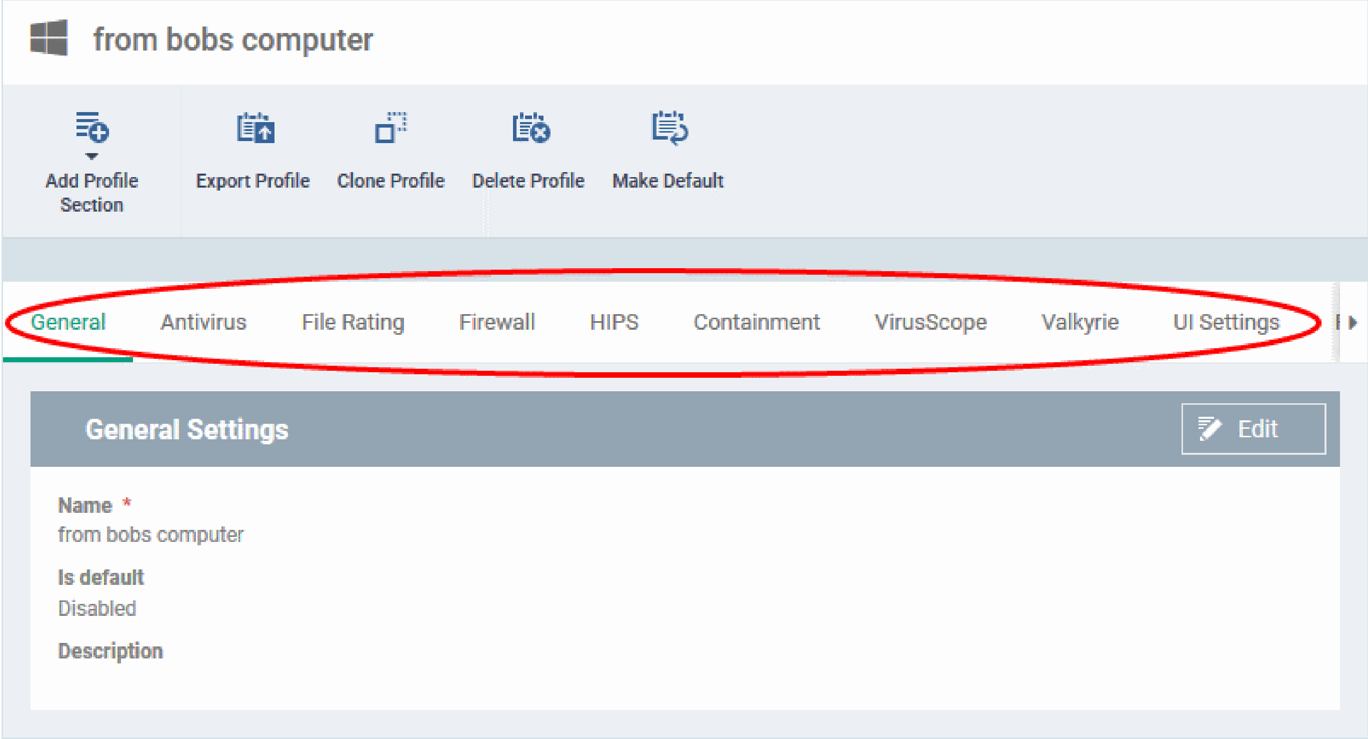
Name *
from bobs computer

Comodo Client - Security configuration file *
Browse ccs_config_2018_10_26_10_58_00.xml

Description
Description

- Click the 'Import' button.

The Windows Profile interface will open, with the security components pre-configured as per the settings in the configuration file.


from bobs computer

General Settings

Name *
from bobs computer

Is default
Disabled

Description

- The imported profile will not be set as 'Default Profile' by default.
- To change the name of the profile and/or to enable it as a default profile, click on the 'Edit' button at the top right of the 'General' settings screen, edit the settings and click the 'Save' button.

- You can now deploy this profile to endpoints and endpoint groups. You can add new profile components by clicking 'Add Profile Section' and can edit the settings for any security component by clicking the relevant tab. For more details on the options available under each component, see the **explanation of the component settings** in **Create Windows Profiles**.

## 6.1.4. Profiles for Mac OS Devices

Mac OS profiles let you specify the general settings and configuration of Comodo Client - Security (CCS) on Mac OS devices.

There are two ways you can add a MAC OS profile:

- Create a brand new profile. See **Create Mac OS Profiles** for more details.
- Clone an existing profile and modify its settings. See **Clone a Profile**, for more details.

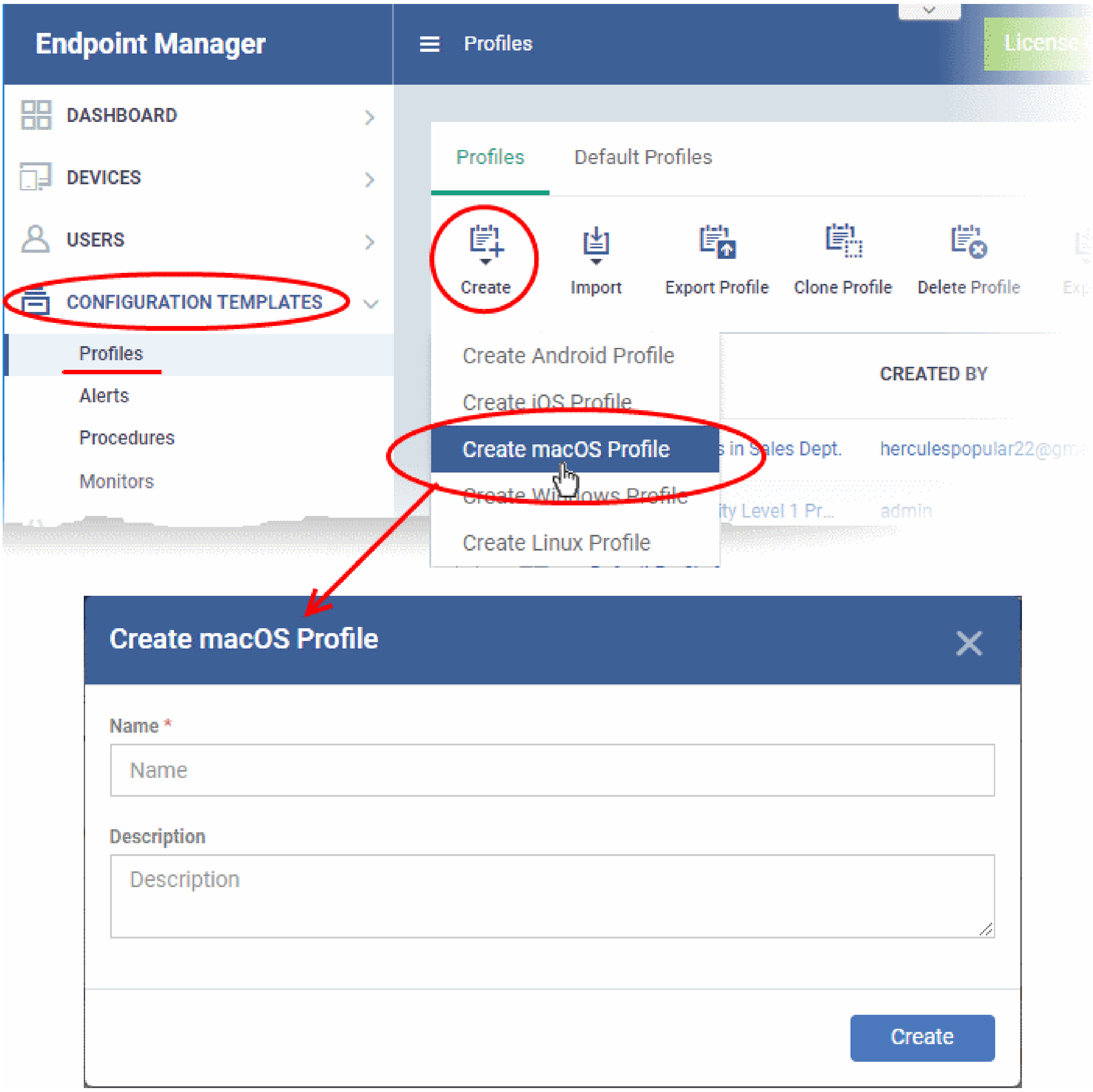
### 6.1.4.1. Create a Mac OS Profile

Process in brief:

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create Mac OS Profile'
- Type a name and description for your profile then click the 'Create' button. The new profile will appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - 'General'. Click 'Add Profile Section' to add settings for various security and management features. Each section you add will appear as a new tab.
- Once configured, you can apply the profile to users, devices, and groups of users or devices.
- Click the 'General' tab then 'Edit' to make it a 'Default' profile.
  - A 'default' profile is one that is applied automatically to any device which matches its operating system. You can have multiple 'default' profiles per operating system.
- This part of the guide explains the processes above in more detail, and includes descriptions of each section.

**Create a new profile**

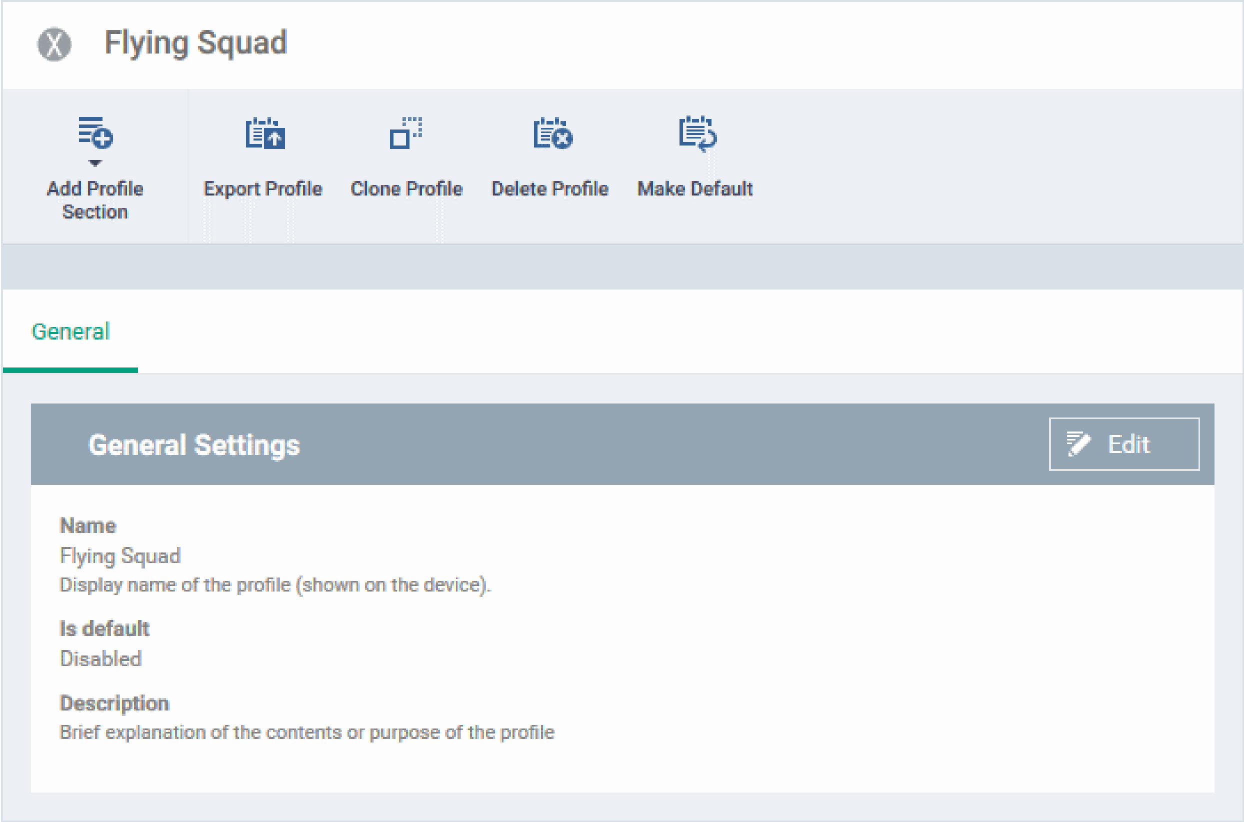
- Click 'Configuration Templates' > 'Profiles' > 'Create' > 'Create Mac OS Profile'



- Name - Enter a label for the profile
- Description - Enter appropriate short notes for the profile

- Click the 'Create' button

The new profile will open at the general settings page:



Name
Flying Squad
Display name of the profile (shown on the device).

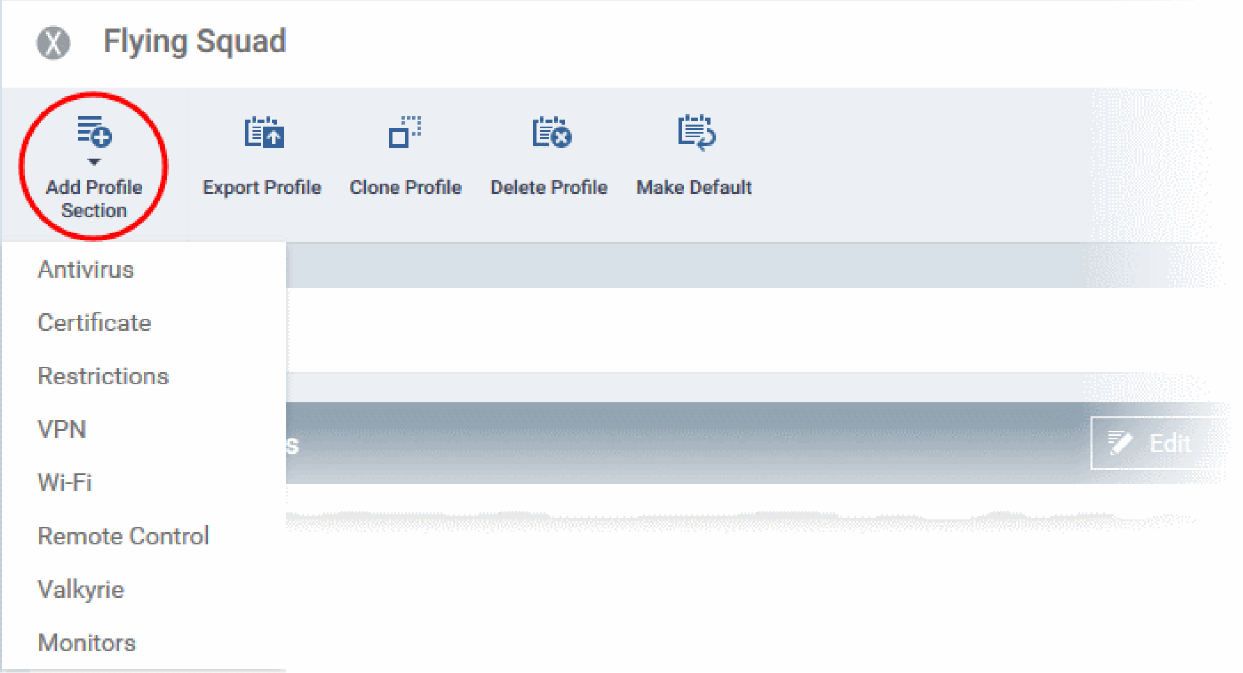
Is default
Disabled

Description
Brief explanation of the contents or purpose of the profile

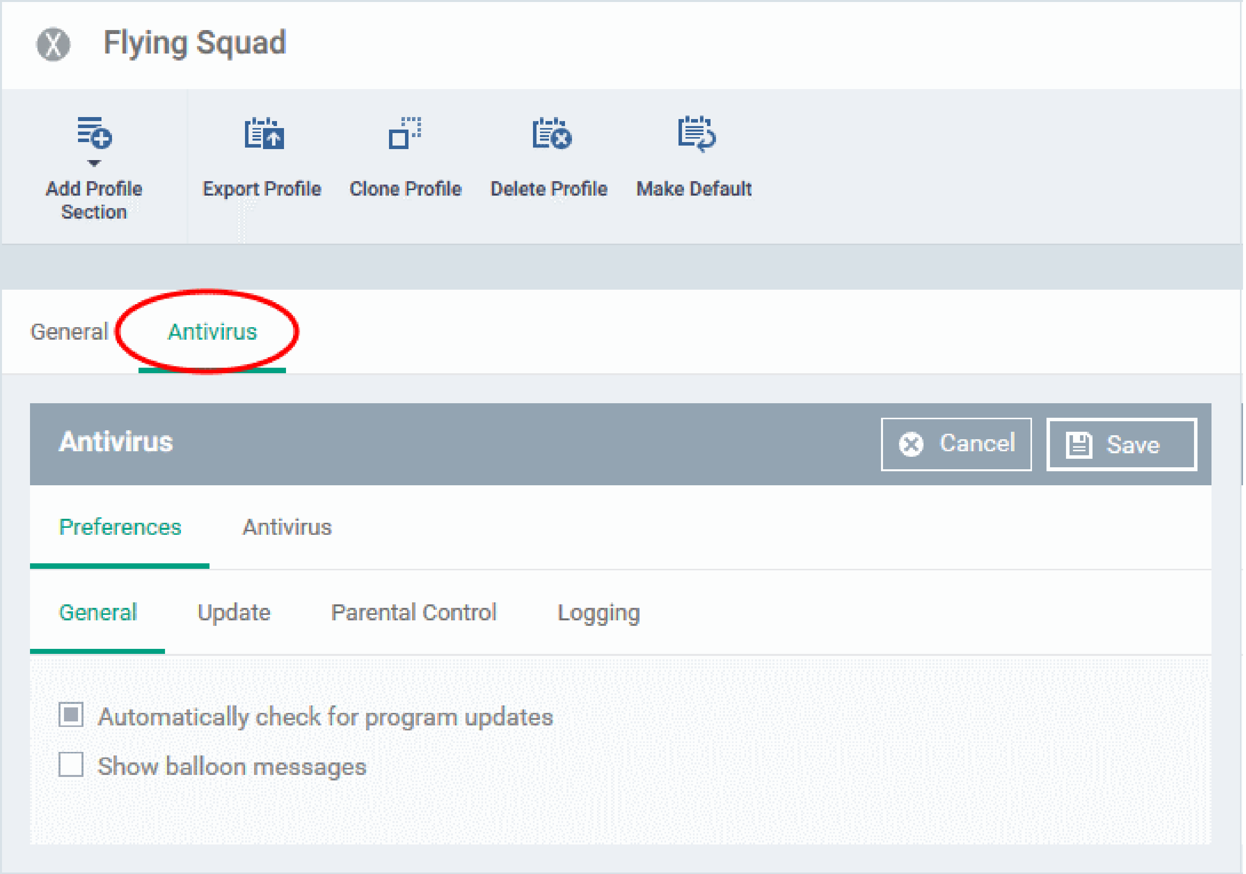
- **Make Default -** A 'default' profile is one that is automatically applied to every device that matches its operating system. Click this button if you want all MAC OS devices to receive this profile. Do not select if you only want to apply the profile to selected MACs.
- Click 'Save'.

The next step is to add sections to the profile. Each section lets you define settings for a particular security or management feature.

- Click 'Add Profile Section' then select the section you want to add from the list:



The new section will appear as a tab under the profile name. You can add as many sections as required to a profile.



☒ Automatically check for program updates

□ Show balloon messages

Following sections explain more about each of the settings:

- **Antivirus**
- **Certificate**
- **Restrictions**
- **VPN**
- **Wi-Fi**
- **Remote control**
- **Valkyrie Settings**
- **Monitors**

### 6.1.4.1.1. Antivirus Settings for Mac OS Profile

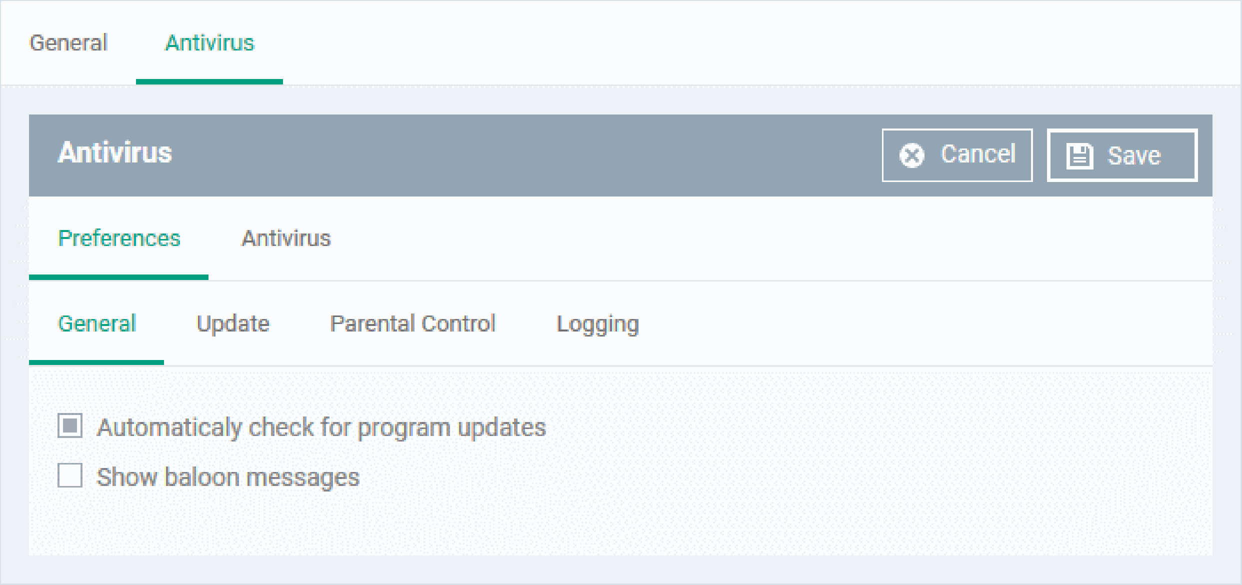
The antivirus section lets you configure real-time monitoring, custom scans, scan schedules, exclusions and more.

**Configure antivirus settings in a Mac OS profile**

- Click 'Configuration Templates' > 'Profiles'
- Click the name of a Mac OS profile
- Click 'Add Profile Section' then 'Antivirus' (if you haven't yet added the AV section)

  OR
- Open the 'Antivirus' tab if it was already added

The antivirus settings screen has two tabs:



▣ Automaticaly check for program updates

□ Show baloon messages

- **Preferences** - Configure general behavior, updates, parental control and log settings
- **Antivirus** - Configure settings for all scan types, create custom scan profiles and schedule AV scans.

## Preferences

The preferences tab lets you configure the following settings:

- **General**
- **Update**
- **Parental Control**
- **Logging**

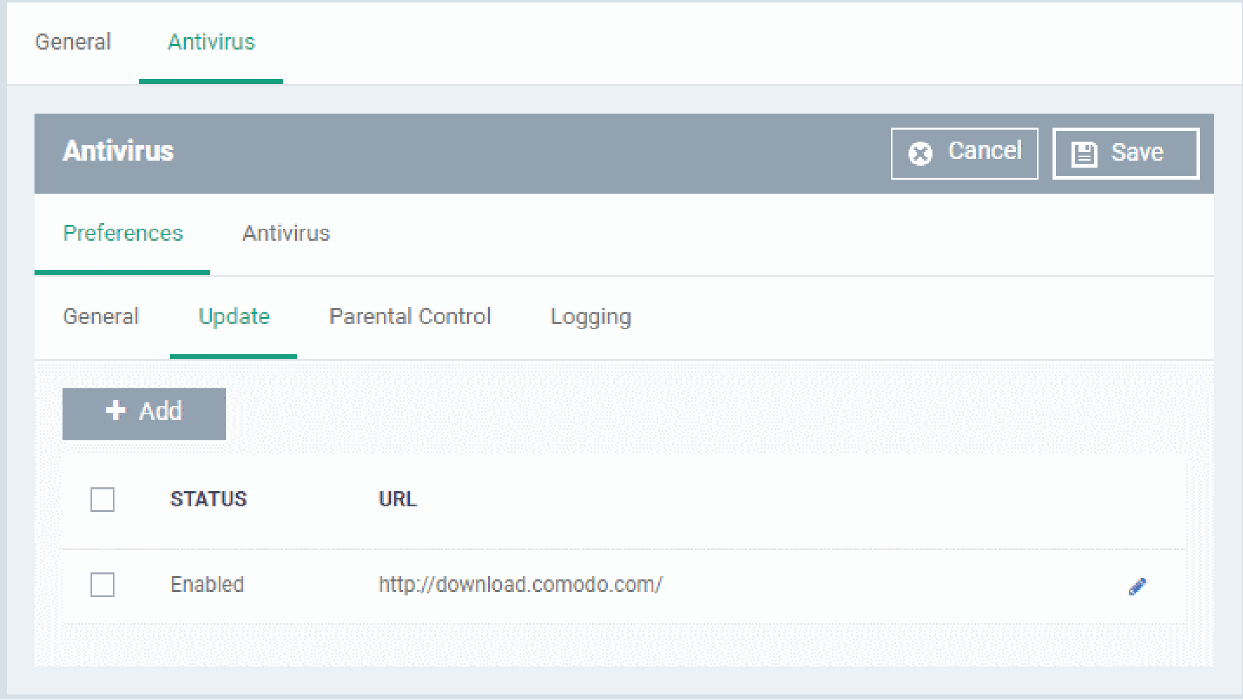
## General

- **Automatically check for program updates** - Choose whether CCS should periodically contact Comodo servers for new product versions and patches. If enabled, CCS checks for updates every 24 hours AND every time users start their computers. If updates are found, they are automatically downloaded and installed. (***Default = Enabled***).
- **Show balloon messages** - If enabled, notifications from CCS will appear in the bottom-right hand corner of the computer screen - just above the tray icons. Balloon messages are usually generated when CCS is learning the activity of previously unknown components of trusted applications. (***Default = Disabled***).

## Update Settings

The update tab lets you specify an alternate host from which endpoints should collect updates. The default download server is https://download.comodo.com

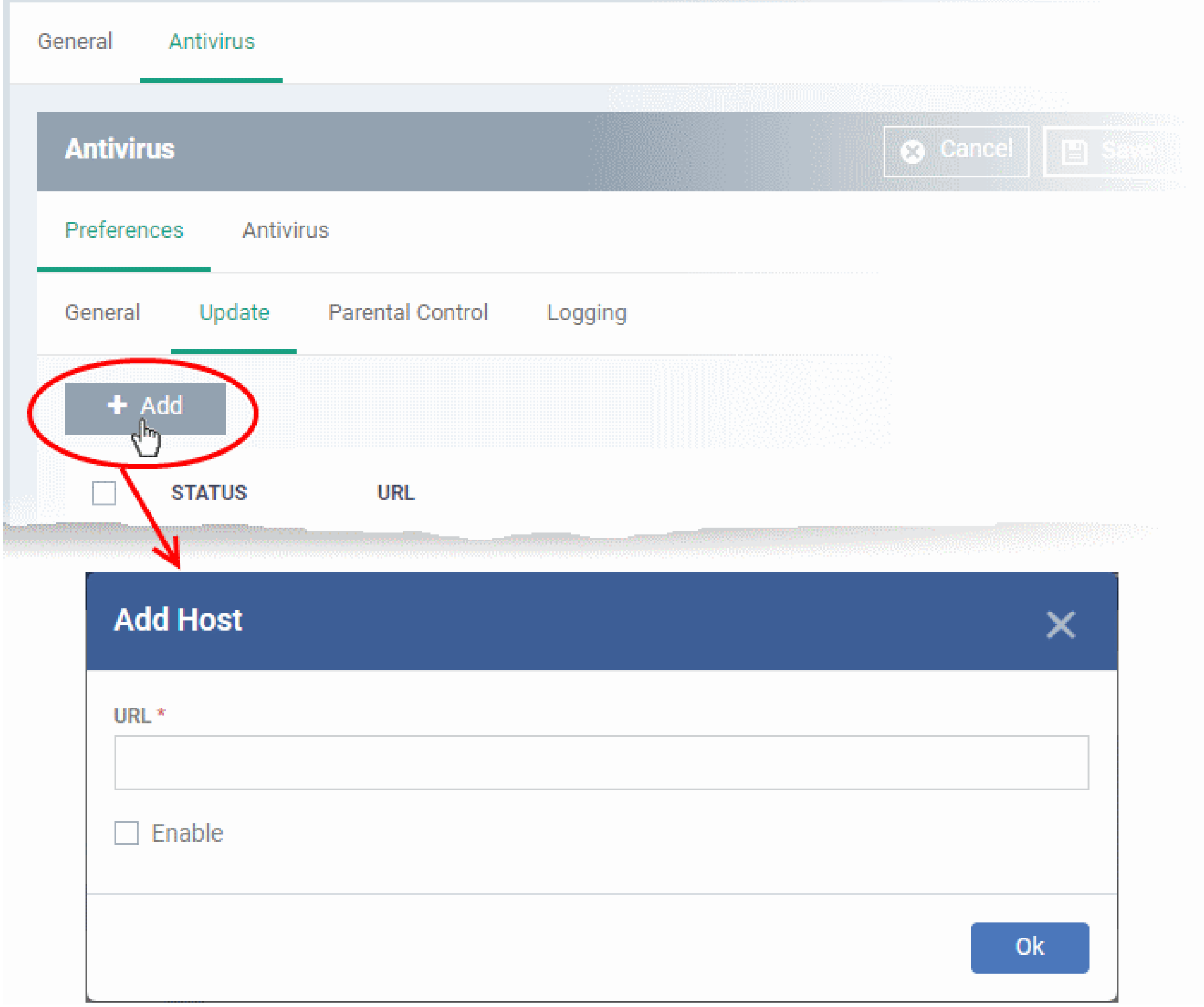
- Click 'Preferences' > 'Update'



| □ | STATUS | URL |
|---|---|---|
| □ | Enabled | http://download.comodo.com/ |

You can add the URL of an alternative download host if required. For example, you may want to distribute the updates from a local server to conserve bandwidth.

- Click 'Add'

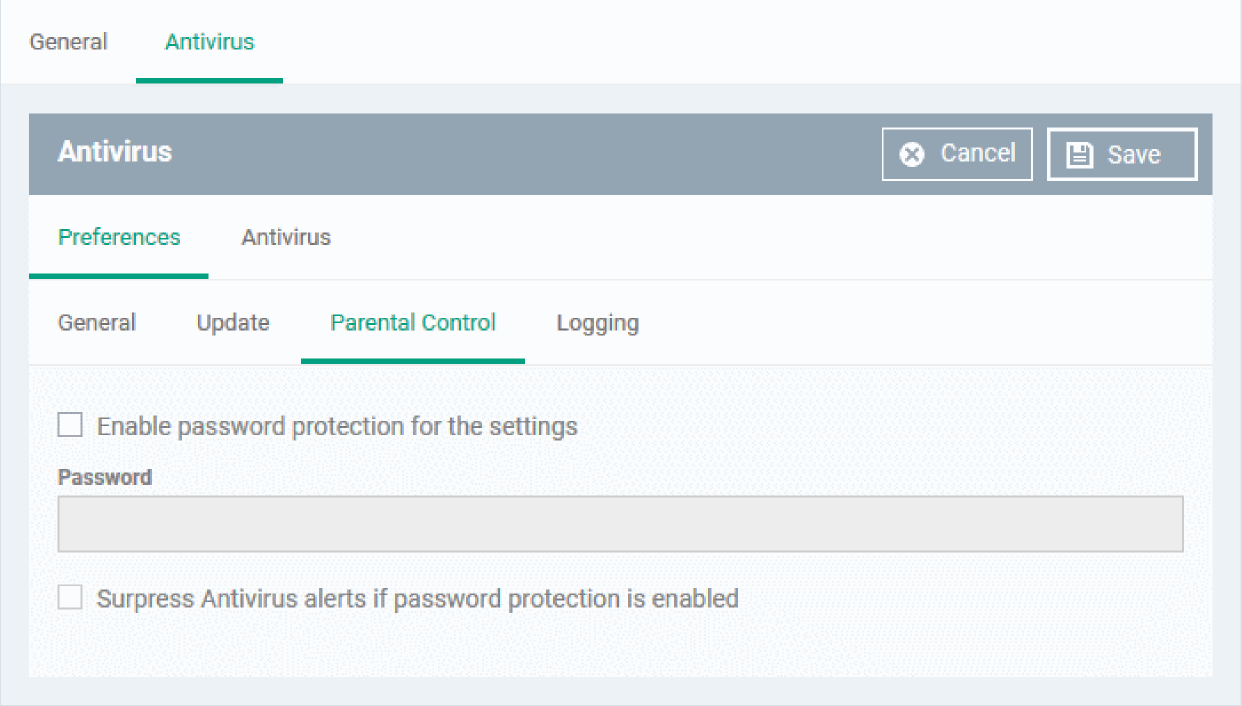


- Enter the URL or IP of the host from which endpoints should collect updates
- Select 'Enable' to activate the host
- Click 'Ok' to apply your changes
- Repeat the process to add multiple hosts.
- Click the pencil icon ✎ to edit the host

## Parental Control Settings

Parental controls let you password protect access to CCS settings. This helps prevent unauthorized personnel from making changes which could compromise the endpoint.

- Click the 'Parental Control' tab under 'Preferences'



□ Enable password protection for the settings

Password

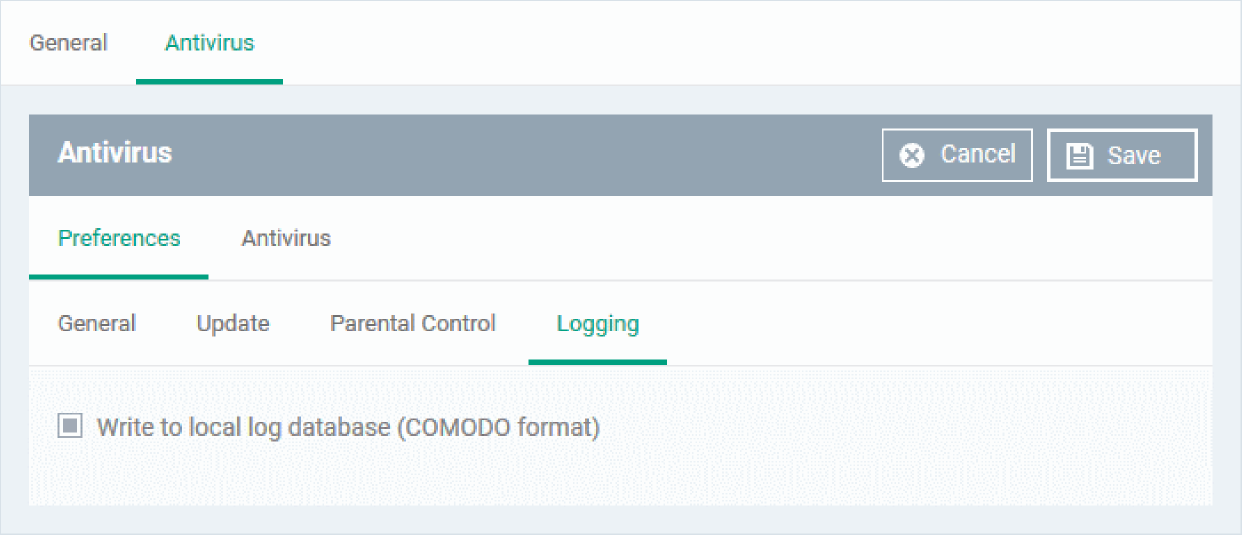
□ Surpress Antivirus alerts if password protection is enabled

- **Enable password protection for the settings -** Activates password protection for all important CCS settings. End-users will need to provide a password to access the settings area in the local CCS UI.

  Please type the password in the field provided.
- **Suppress Antivirus alerts if password protection is enabled -** If selected, threats on the device are automatically blocked but no alert is shown to the end-user. This avoids the situation where a user dangerously clicks 'Allow' just to make an alert go away.

## Log Settings

- Click the 'Logging' tab under 'Preferences'



☑ Write to local log database (COMODO format)

By default, CCS logs all antivirus (AV) events locally on the device. Users can view the logs by clicking 'View Antivirus Events' in the tasks interface.

- **Write to local log database (COMODO format) -** Deselect if you don't want CCS to store logs on the local device.

## Configure Antivirus Settings

The antivirus tab lets you configure settings for all types of scan, view/create scan profiles, and to schedule scans.

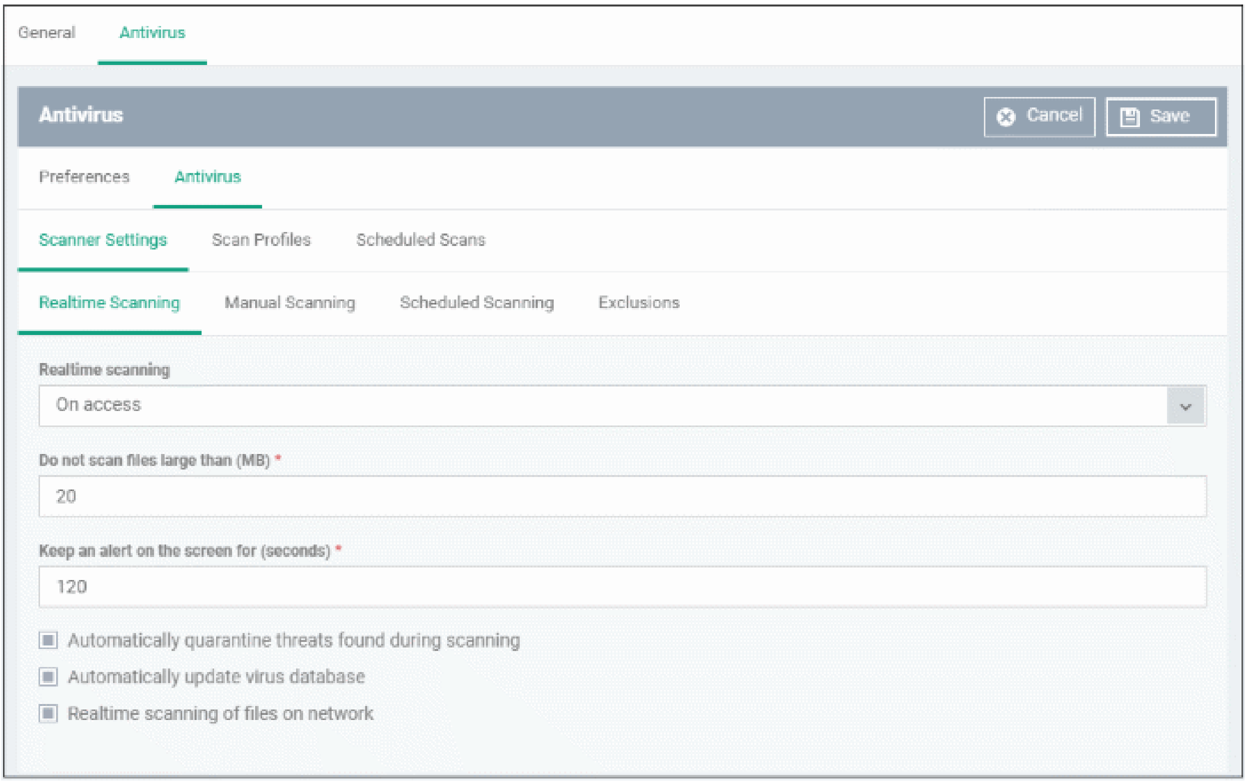
It has three sub-tabs:

- Scanner Settings
- Scan Profiles
- Scheduled Scans

## Scanner Settings

You can configure the following in the scanner settings area:

- Realtime Scanning
- Manual Scanning
- Scheduled Scanning
- Exclusions



Realtime scanning: On access

Do not scan files large than (MB) *: 20

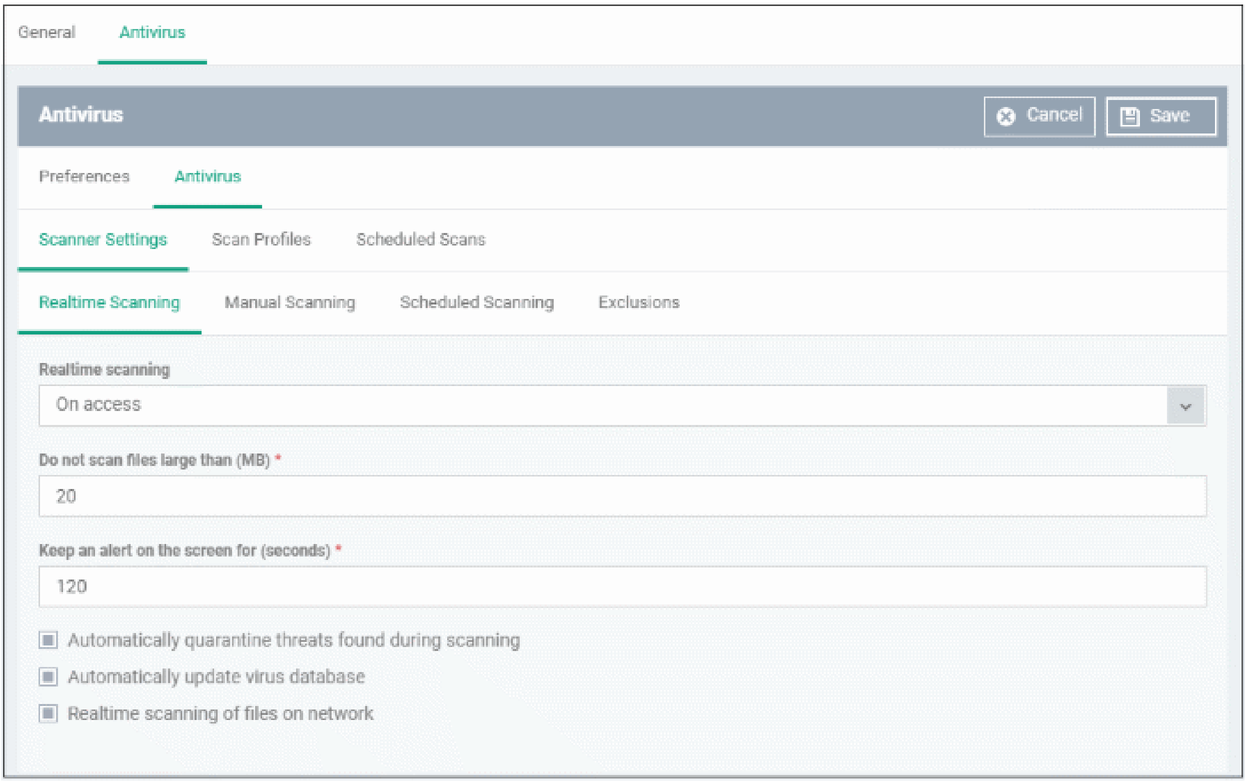
Keep an alert on the screen for (seconds) *: 120

☐ Automatically quarantine threats found during scanning

☐ Automatically update virus database

☐ Realtime scanning of files on network

## Realtime Scanning



Realtime scanning: On access

Do not scan files large than (MB) *: 20

Keep an alert on the screen for (seconds) *: 120

☐ Automatically quarantine threats found during scanning

☐ Automatically update virus database

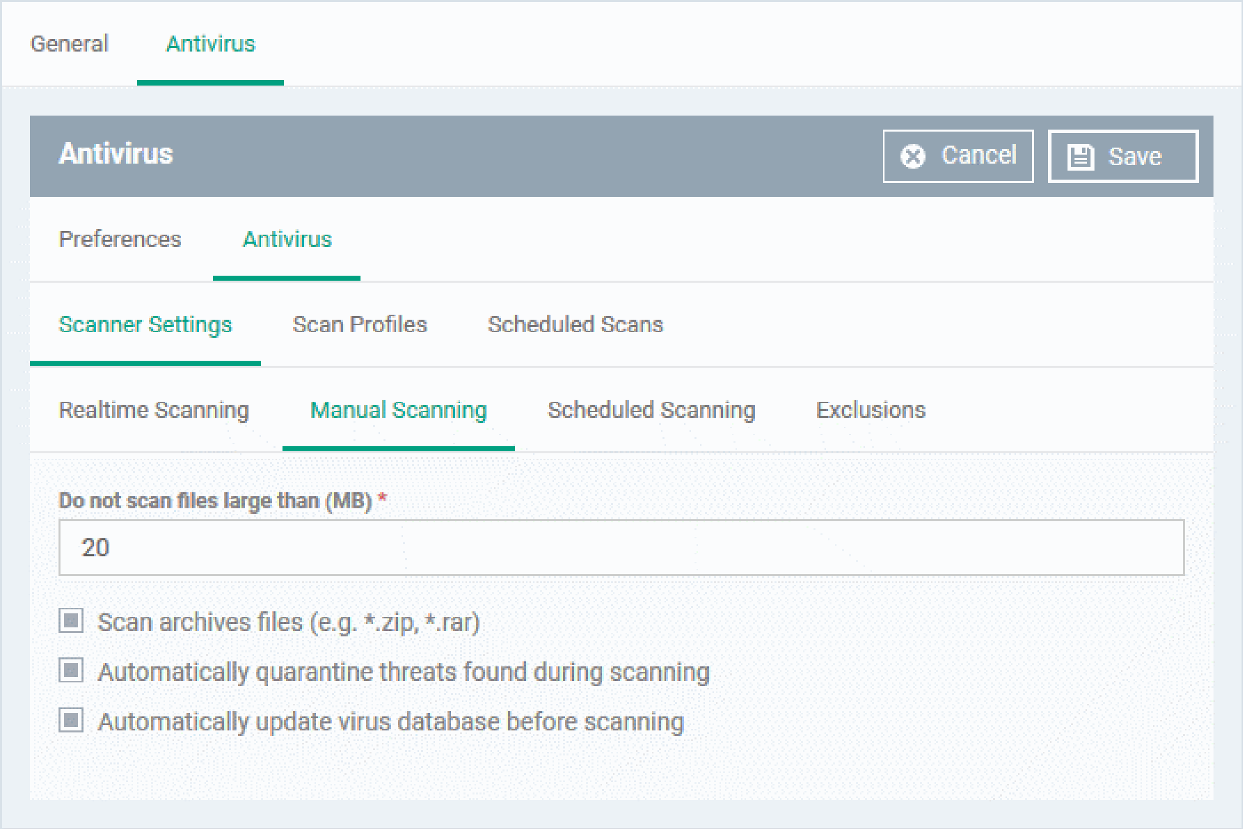
☐ Realtime scanning of files on network

| Form Element | Description |
|---|---|
| Real time scanning | Enable or disable realtime scans.<br>• **On Access -** Any file opened is scanned before it is allowed to run. Threats are detected before they get a chance to execute |

| Form Element | Description |
|---|---|
| | - Disabled - Real-time protection is switched off. Files are allowed to run without first being checked for threats. |
| Do not scan files larger than (MB) | Files larger than the size specified here will not be scanned (***Default =20MB***). |
| Keep an alert on the screen for (seconds) | How long threat notifications should stay on-screen if not dismissed by the end-user. (***Default = 120 seconds***) |
| Automatically quarantine threats found during scanning | Threats will be encrypted and moved to a secure holding area where they can cause no harm. You can review quarantined items and delete, ignore, or restore them.<br>- Disable this option if you do not want threats to be moved to quarantine.<br>(***Default = Enabled***) |
| Automatically update virus database | CCS checks for and downloads database updates at system start-up, and subsequently at regular intervals.<br>- Disable this option if you do not want CCS to automatically check for updates.<br>(***Default = Enabled***). |
| Realtime scanning of files on network | Activate or deactivate automatic scans of files on network drives.<br>- **Enabled** - CCS checks every file that the user interacts with on a network drive, even if it is not copied to the local machine.***(Default)***<br>- **Disabled** - Network files are not checked unless they are copied to the local machine. |

## Manual Scanning

- A manual scan is one you run 'on-demand' on selected files, folder or drives. Manual scans can be launched from 'Security Sub-Systems' > 'Antivirus'.
- For more details on running on-demand scans on selected devices, see **Run Antivirus and/or File Rating Scans on Devices**.



Do not scan files large than (MB) *

20

☑ Scan archives files (e.g. *.zip, *.rar)

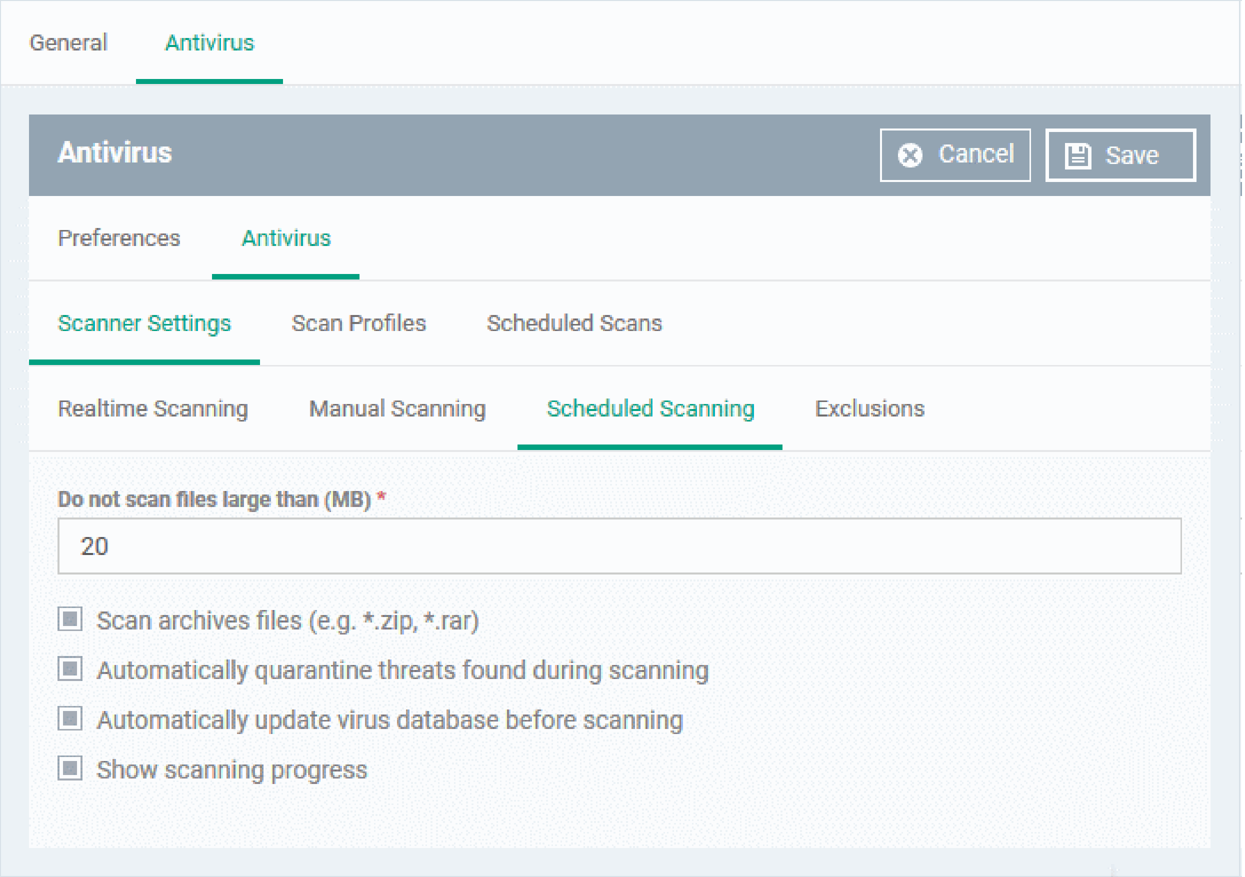
☑ Automatically quarantine threats found during scanning

☑ Automatically update virus database before scanning

| Manual Scanning Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Do not scan files large than (MB) | Text box | Files larger than the size specified here, will not be scanned (***Default =20MB***). |
| Scan archive files | Checkbox | CCS scans archive files such as .ZIP and .RAR files.<br>• Disable this option if you don't want archive files to be scanned.<br>(***Default = Enabled***). |
| Automatically quarantine threats found during scanning | Checkbox | Threats will be encrypted and moved to a secure holding area where they can cause no harm. You can review quarantined items and delete, ignore or restore them.<br>• Disable this option if you do not want threats to be moved to quarantine.<br>(***Default = Enabled***) |
| Automatically update virus database before scanning | Checkbox | CCS will check for and download the latest virus database updates on system start-up, and subsequently at regular intervals.<br>• Disable this option if you do not want CCS to automatically check for updates.<br>(***Default = Enabled***). |

## Scheduled Scanning

- Specify general settings which will apply to all scheduled scans you create
    - Note. You actually create schedules in the 'Scheduled Scans' area. See **create a scheduled scan** if you need help with this.



Do not scan files large than (MB) *

20

□ Scan archives files (e.g. *.zip, *.rar)

□ Automatically quarantine threats found during scanning

□ Automatically update virus database before scanning

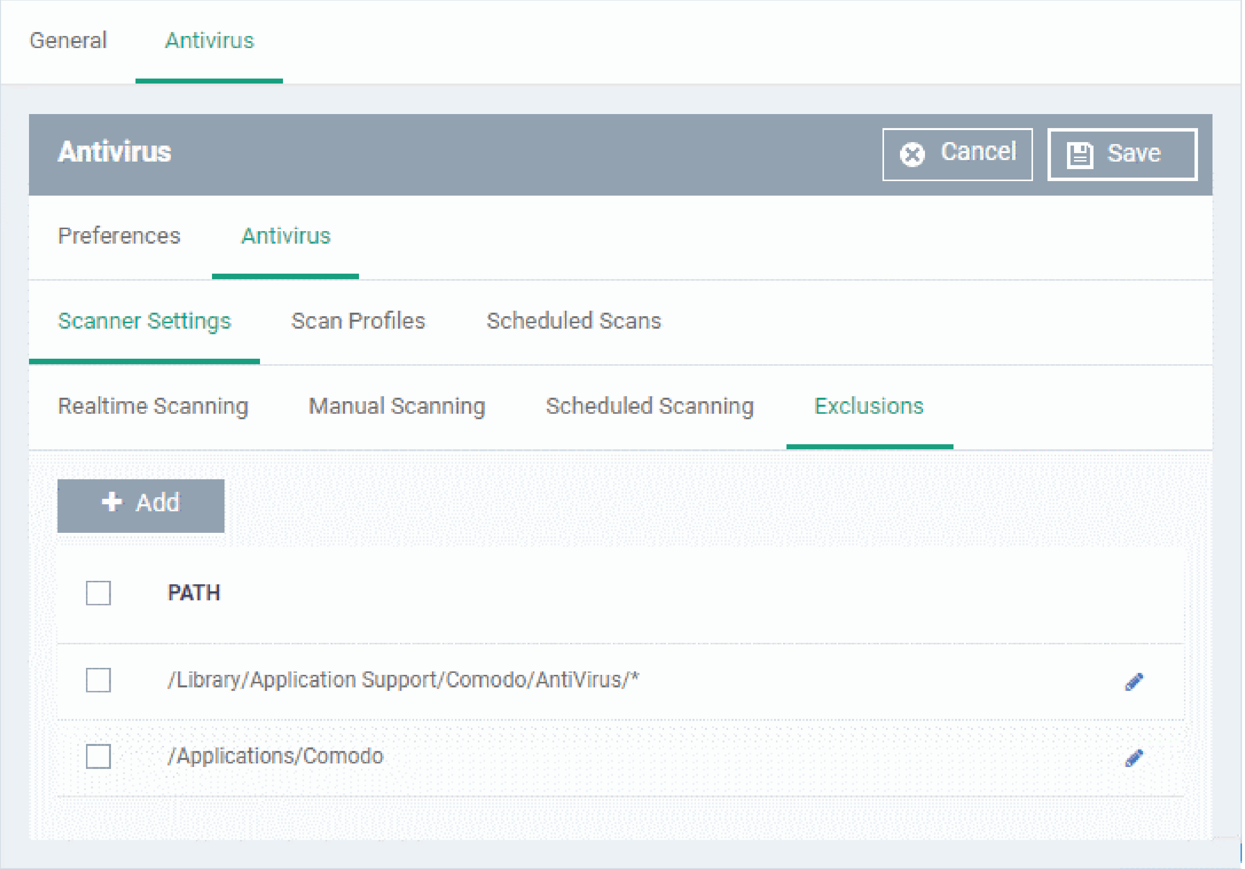
□ Show scanning progress

| Scheduled Scanning Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Do not scan files large than (MB) | Text box | Files larger than the size specified here will not be scanned. (***Default =20MB***). |
| Scan archives files | Checkbox | CCS scans archive files such as .ZIP and .RAR files.<br>• Disable this option if you don't want to scan archive files.<br>(***Default = Enabled***). |
| Automatically quarantine threats found during scanning | Checkbox | Threats will be encrypted and moved to a secure holding area where they can cause no harm. You can review quarantined items and delete, ignore or restore them.<br>• Disable this option if you do not want threats to be moved to quarantine.<br>(***Default = Enabled***) |
| Automatically update virus database before scanning | Checkbox | CCS will check for and download the latest virus database updates on system start-up, and subsequently at regular intervals.<br>• Disable this option if you do not want CCS to |

| Scheduled Scanning Settings - Table of Parameters | | |
|---|---|---|
| | | automatically check for updates.<br>(***Default = Enabled***). |
| Show scanning progress | Checkbox | Enabled - End-users will see a scan progress bar when the scan is running.<br>Disable this option if you don't want CCS to show the progress bar.<br>(***Default = Enabled***) |

## Exclusions

Note. Any item you exclude will be skipped by ALL types of scan - real-time, on-demand and scheduled.

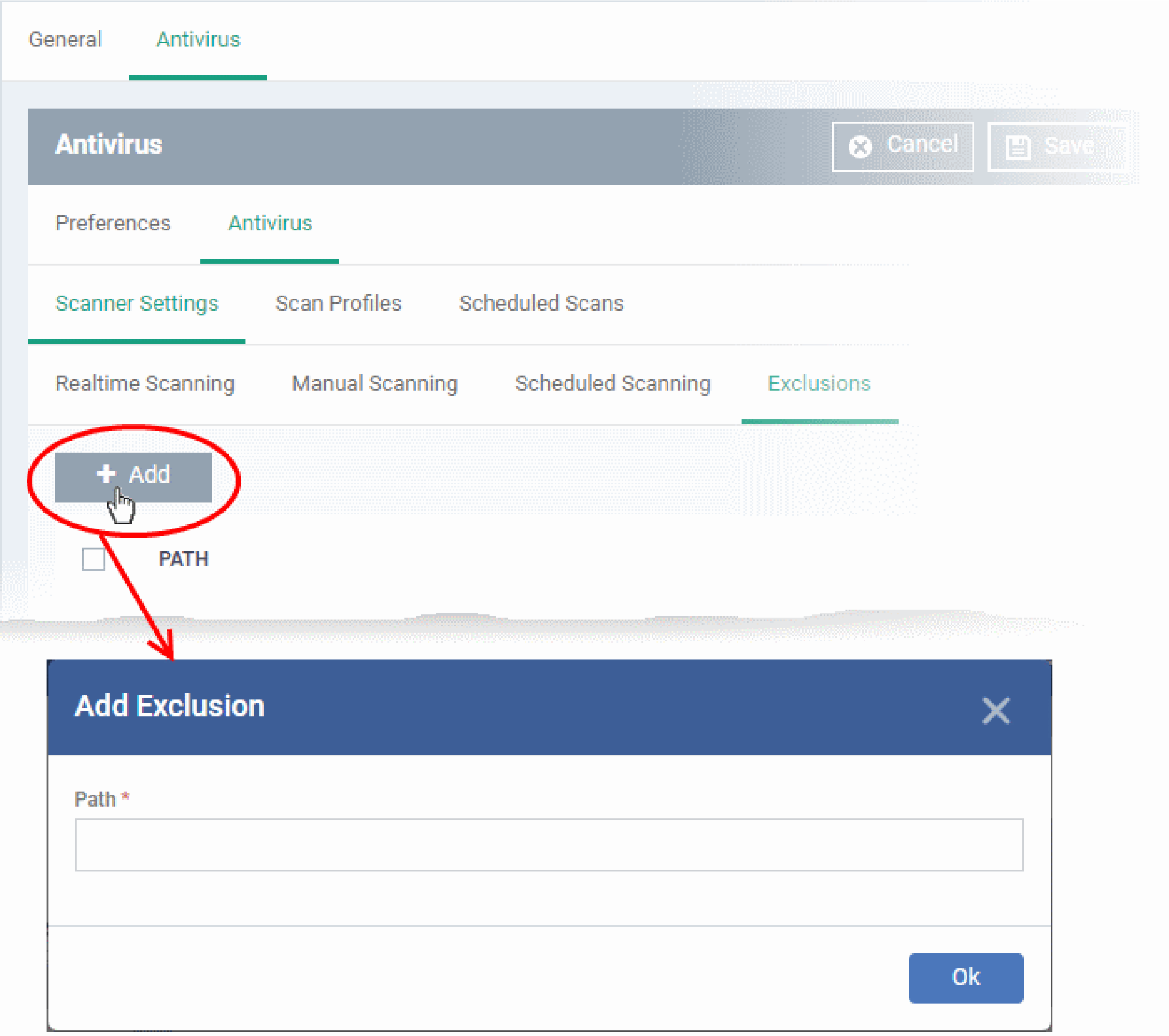


| □ | PATH |
|---|---|
| □ | /Library/Application Support/Comodo/AntiVirus/* |
| □ | /Applications/Comodo |

A list of excluded items will be displayed.

### Add an item to the 'Exclusions' list

- Click 'Add'



- Enter the location of the item to be excluded in the 'Path' field and click 'Ok'
- Repeat the process to add more items

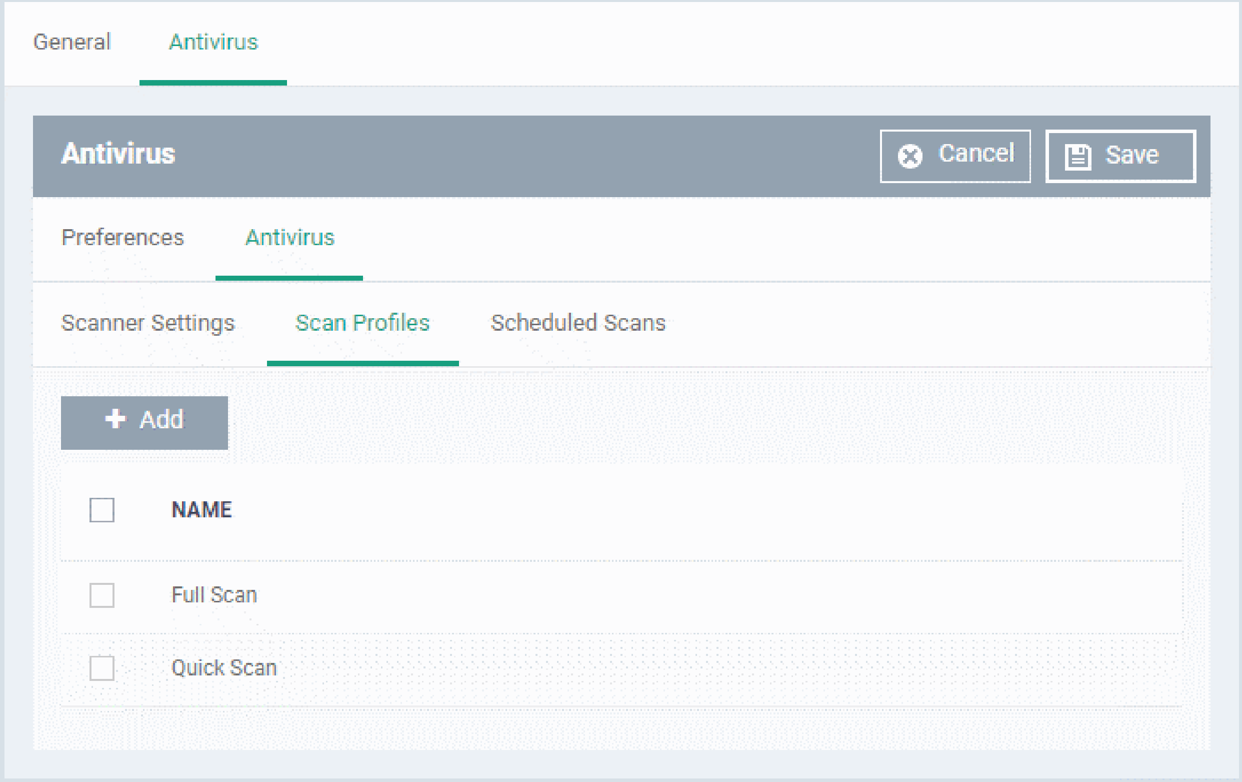
- To edit the path of an item, click the pencil icon ✎ beside it

## Scan Profiles

- Scan profiles instruct CCS to scan selected areas, folders or drives on a the device.
- You can add a scan profile to:
  - A scheduled scan
  - An on-demand scan

**To create a scan profile**

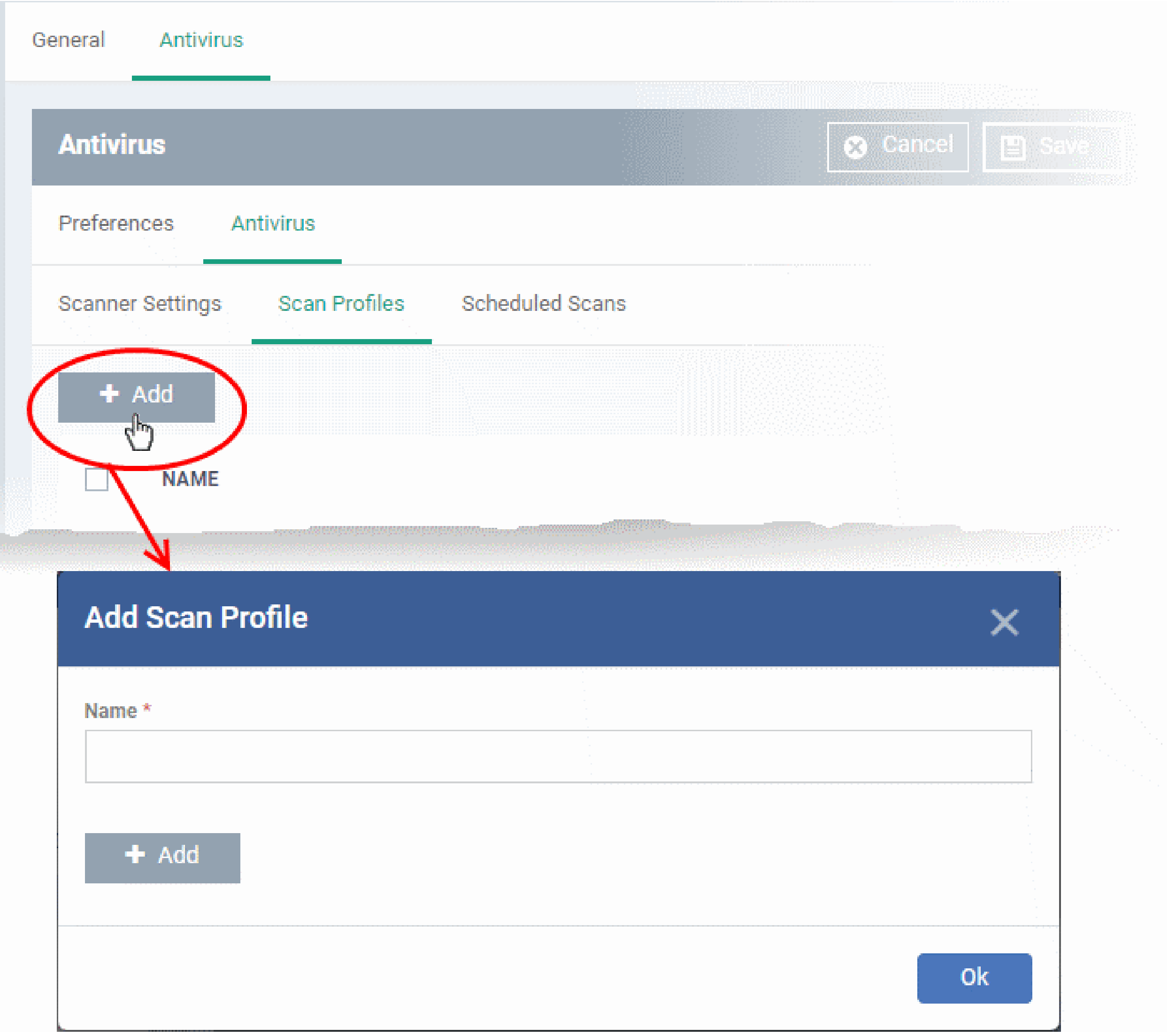
- Click the 'Scan Profiles' tab under 'Antivirus'



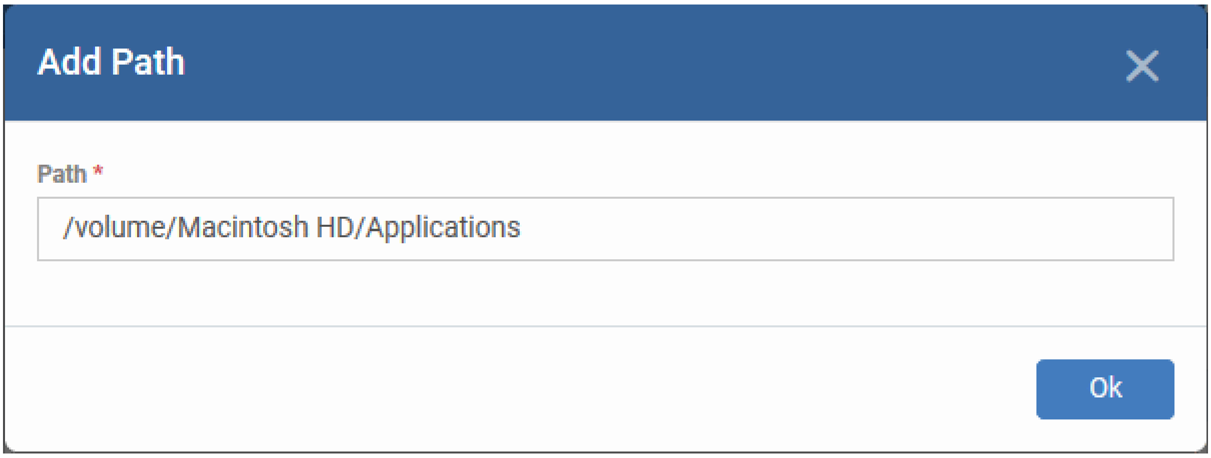
| □ | NAME |
|---|---|
| □ | Full Scan |
| □ | Quick Scan |

The list of pre-defined scan profiles will be displayed.

- Click 'Add'



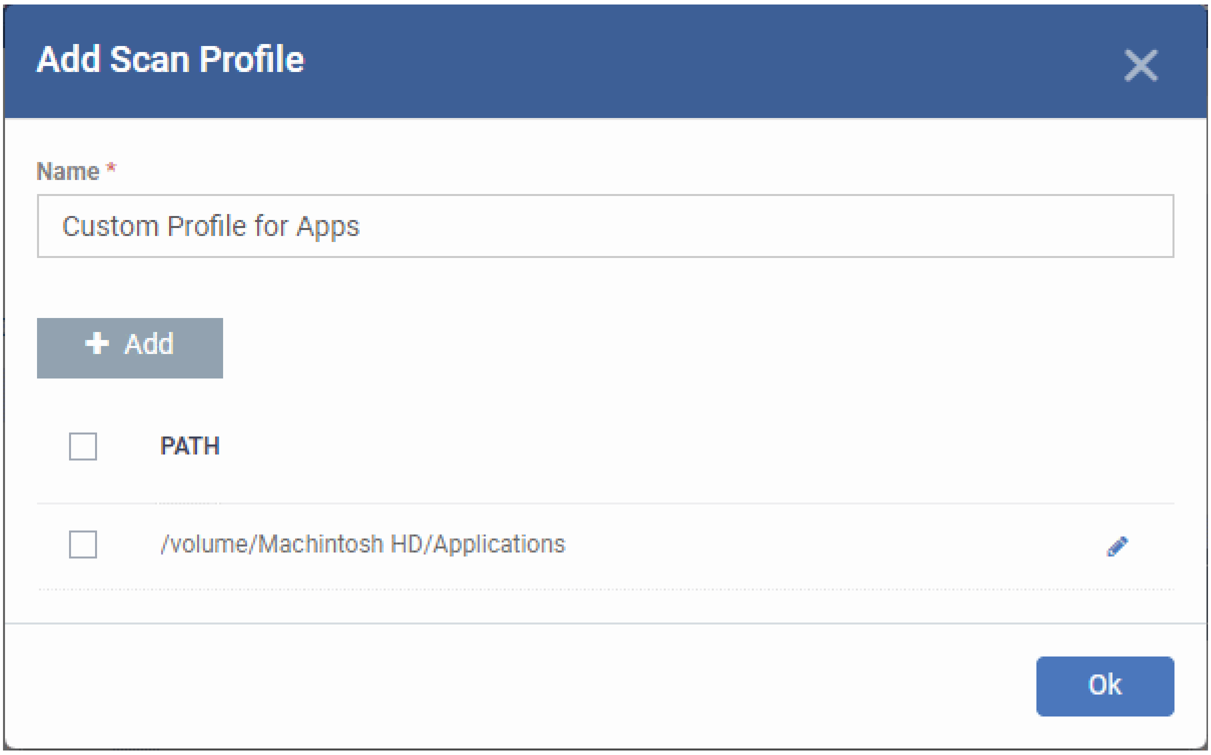
- Enter a name for the scan profile
- Click 'Add' to add the locations to be scanned as per the custom profile



Path *: /volume/Macintosh HD/Applications

- Enter the path of the location to be scanned as per the custom profile and click 'Ok'

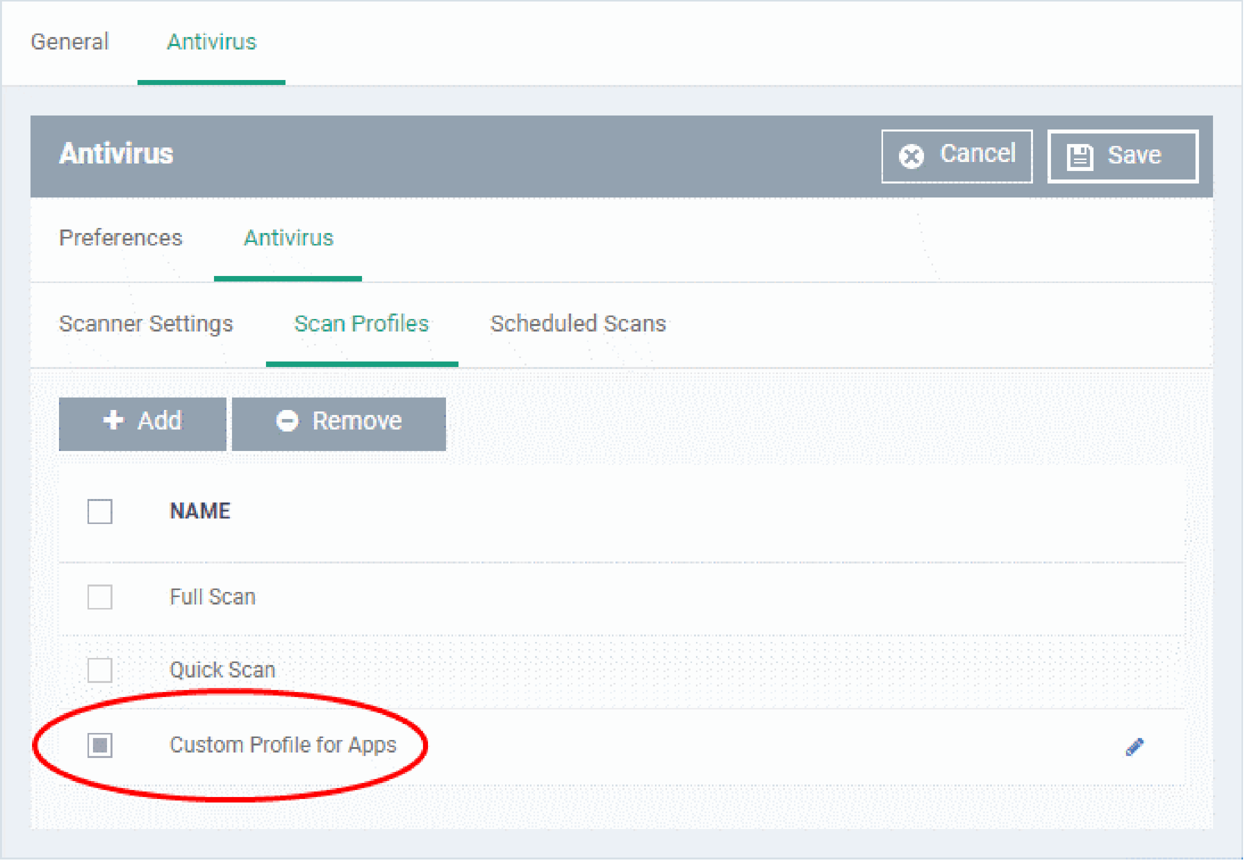
The path will be added to the profile.



Name * Custom Profile for Apps

| ☐ | PATH |
|---|---|
| ☐ | /volume/Machintosh HD/Applications |

  - To add more paths, click 'Add' and repeat the process
  - To edit the path, click the pencil icon ✎ beside it
  - Click 'Ok' in the 'Add Scan Profile' dialog.
- The profile will be added to the list of 'Scan Profiles'.



| ☐ | NAME |
|---|---|
| ☐ | Full Scan |
| ☐ | Quick Scan |
| ☑ | Custom Profile for Apps |

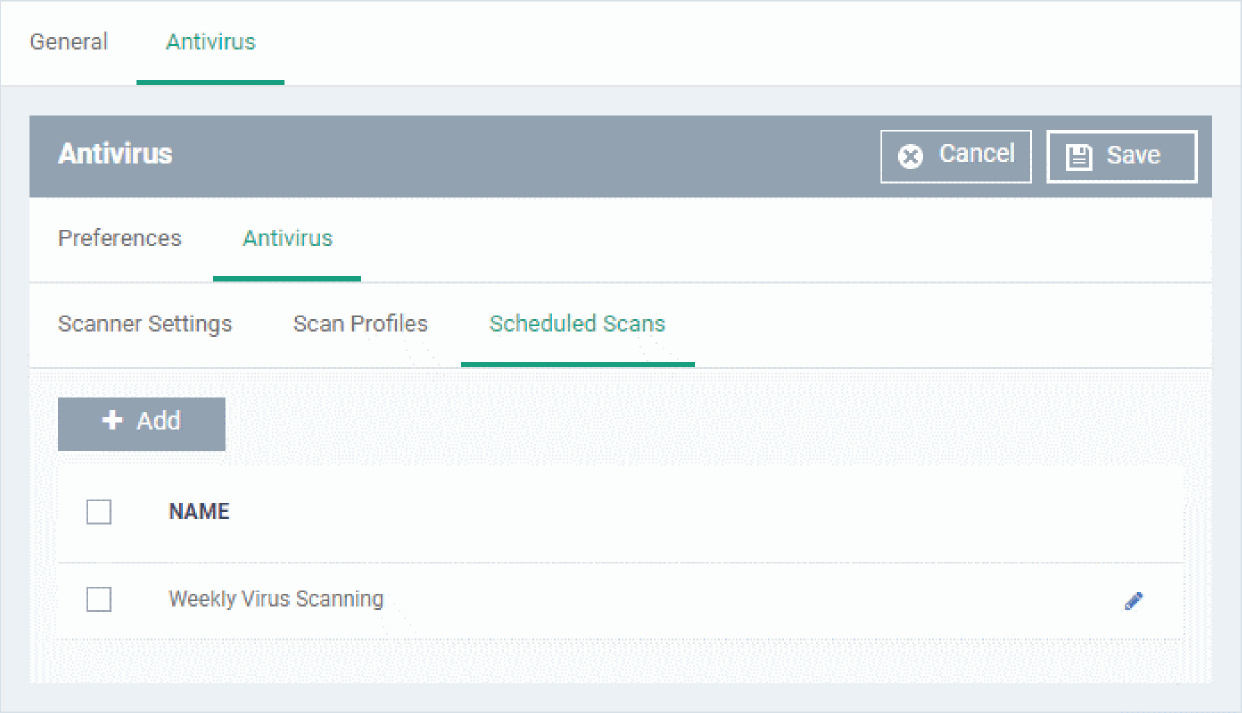
- Click 'Add' and repeat the process to add more custom scan profiles
- Click the pencil icon ✎ beside a custom profile to edit its details.

## Scheduled Scans

- The highly customizable scan scheduler lets you timetable scans to be run on managed devices according to your preferences. CCS automatically starts scanning the entire system or the disks or folders contained in the profile selected for that scan.
- You can add any number of scheduled scans for a profile to run at a time that suits your preference. A scheduled scan may contain any scan profile of your choice.

### Create a scan schedule

- Click the 'Scheduled Scans' tab under 'Antivirus'

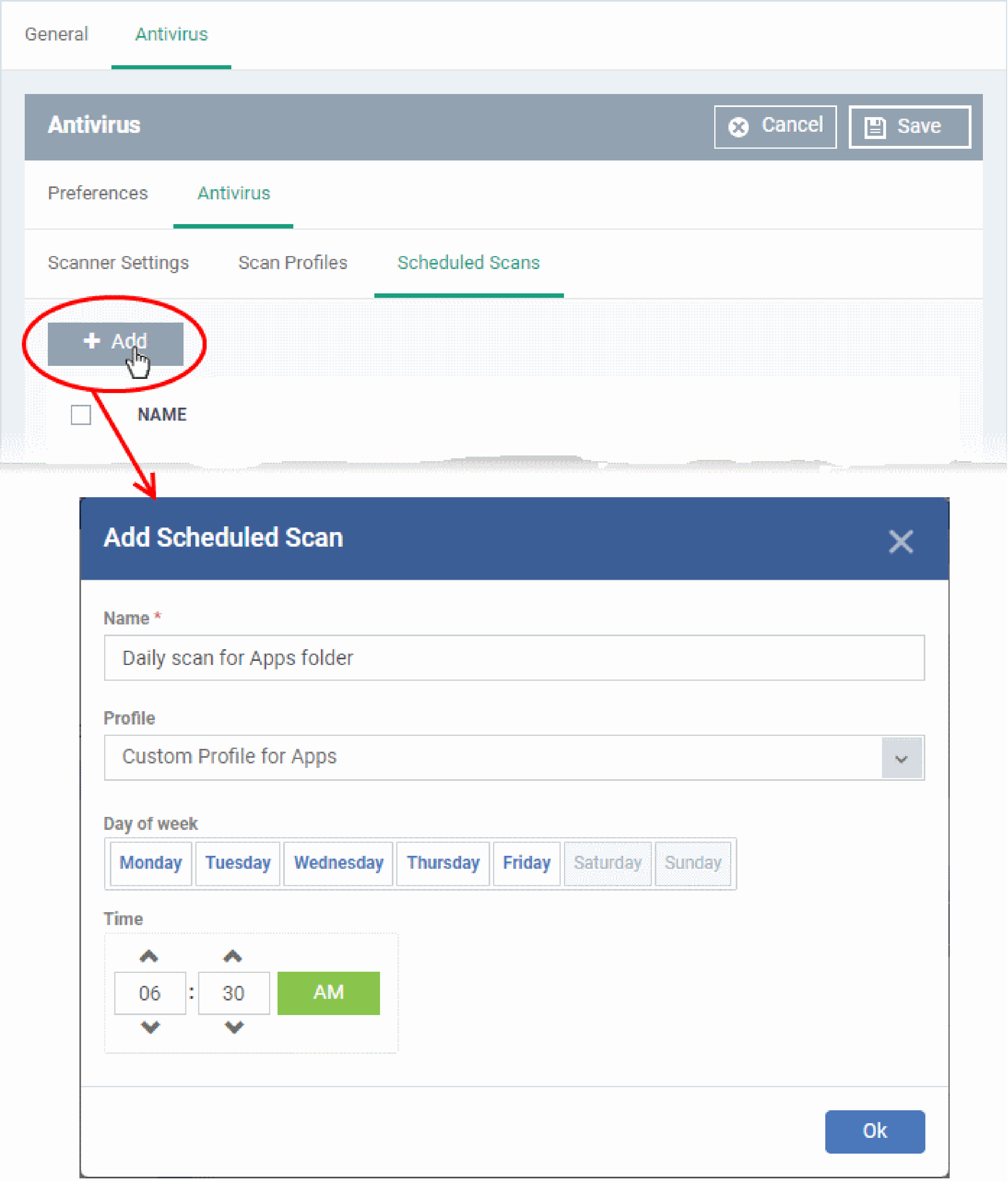


| □ | NAME |
|---|---|
| □ | Weekly Virus Scanning |

A list of pre-configured scheduled scans will be displayed.

### Add a new scheduled scan

- Click 'Add'



Name *

Daily scan for Apps folder

Profile

Custom Profile for Apps

Time

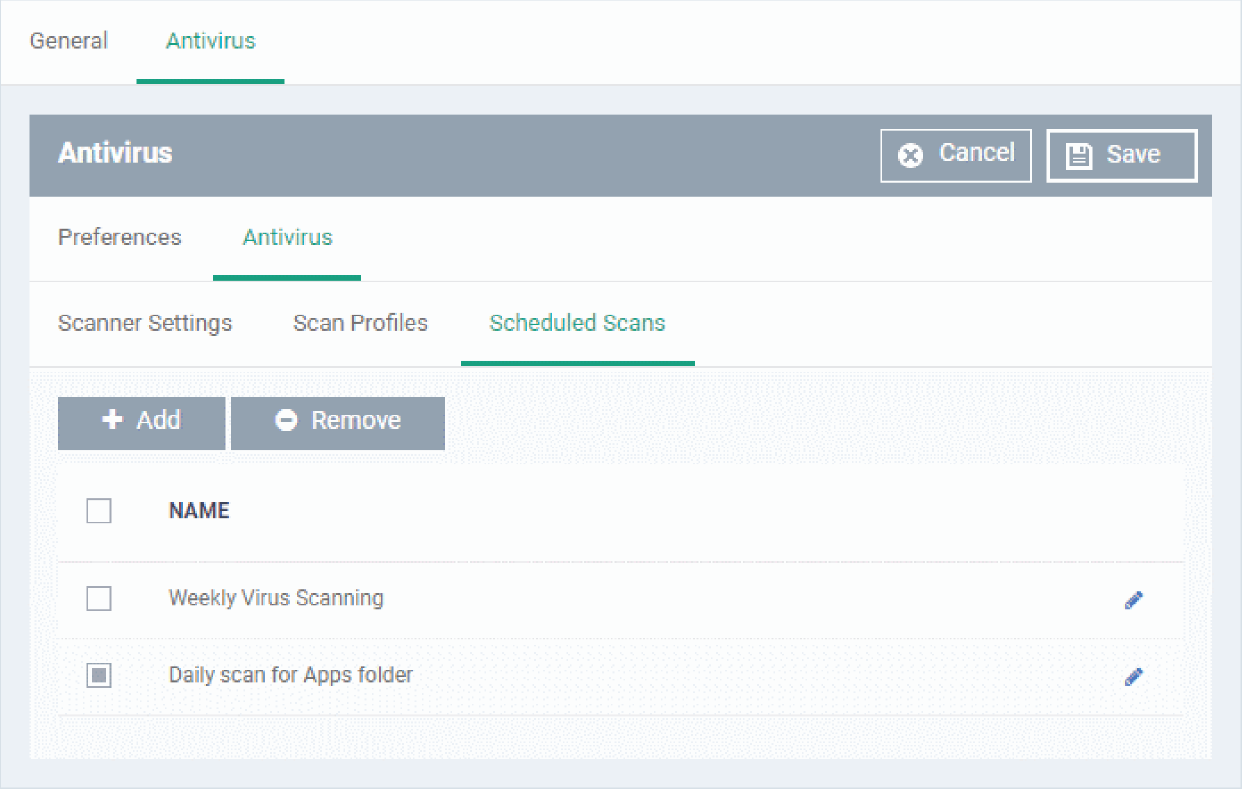
06 : 30 AM

| Add Scheduled Scan - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text box | Label for the scheduled scan |
| Profile | Drop-down | Choose the pre-defined or custom scan profile to be applied for the scheduled scan. The scan profiles included under the 'Scan Profiles' tab will be available in the drop-down. |
| Day of the Week | Buttons | Select the day(s) of the week on which the scan has to run |

| Add Scheduled Scan - Table of Parameters | | |
|---|---|---|
| Time | HH:MM drop-down combo boxes | Set the time at which the scans are to run on the selected days. |

- Click 'Ok'

The scheduled scan will be added to the list.



| □ | NAME |
|---|---|
| □ | Weekly Virus Scanning |
| ☒ | Daily scan for Apps folder |

- Click 'Add' and repeat the process to add more scheduled scans to the configuration profile.
- Click the pencil icon beside a scheduled scan to it edit its settings.

- Click 'Save' for your settings to take effect for the profile.

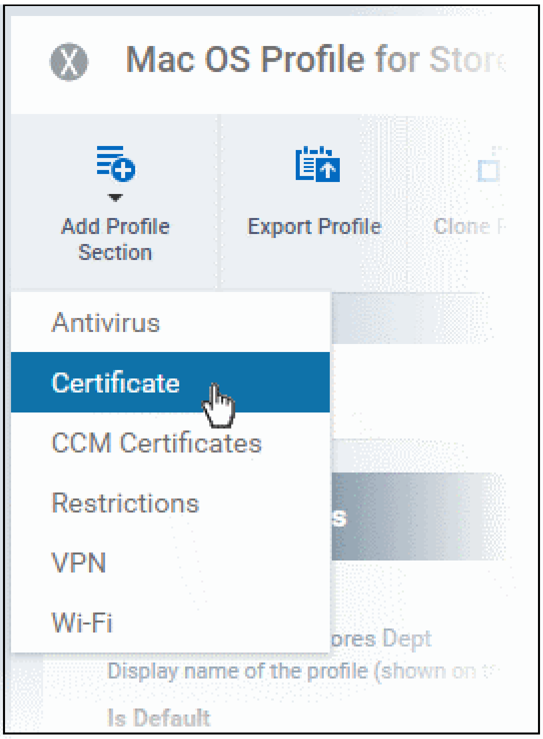
The settings will be saved and shown in the 'Antivirus' tab. You can edit the settings or remove the section at anytime. See **Edit Configuration Profiles** for more details.

### 6.1.4.1.2. Certificate Settings for Mac OS Profile

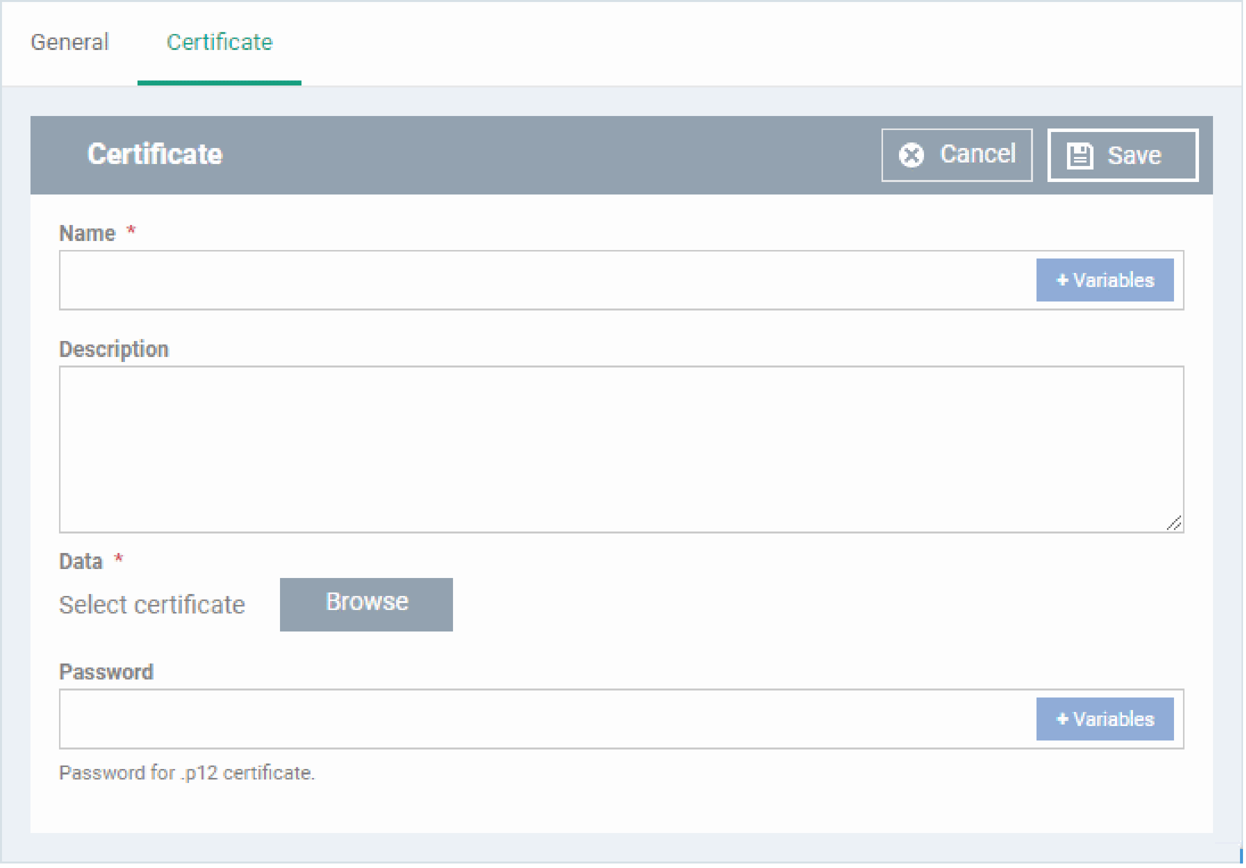
- The 'Certificate Settings' section lets you upload certificates for use in 'Wi-Fi', 'Exchange Active Sync', 'VPN' and other areas of EM.

#### Configure certificate settings for Mac OS profile

- Click 'Configuration Templates' > 'Profiles'
- Open the Mac OS profile you want to configure
- Click 'Add Profile Section' > 'Certificate'



The certificate settings screen will open:



Name *

Description

Data *

Select certificate

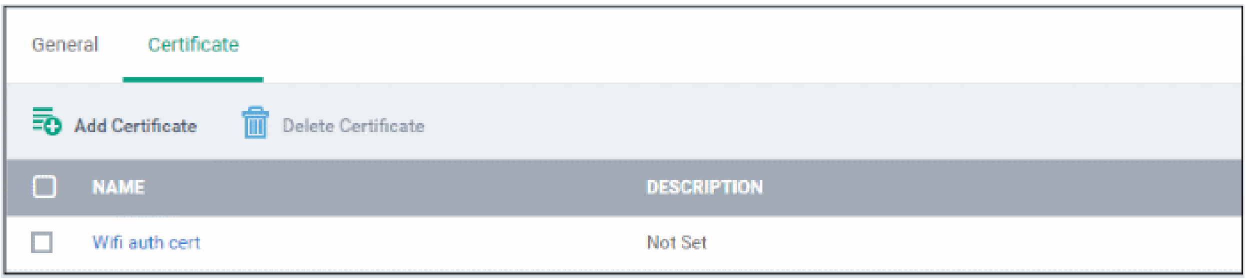
Password

Password for .p12 certificate.

| Certificate Settings | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text Field | Enter the label of the certificate.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |
| Description | Text Field | Enter an appropriate description for the certificate. |
| Data | Browse button | Browse and upload the required certificate. Only certificate files with extensions 'pub', 'crt', 'key' or 'p12' can be uploaded. |
| Password | Text Field | Enter the password used for exporting a .p12 certificate.<br>Click the variables button + Variables to insert dynamic values. See **Create and Manage Custom Variables** for more details on variables. |

- Click the 'Save' button.

The certificate will be added to the certificate store.



| ☐ NAME | DESCRIPTION |
|---|---|
| ☐ Wifi auth cert | Not Set |

- To add more certificates, click 'Add Certificate' and repeat the process.
- To view the certificate key and edit the name, click on the name of the certificate
- To remove an unwanted certificate, select it and click 'Delete Certificate'

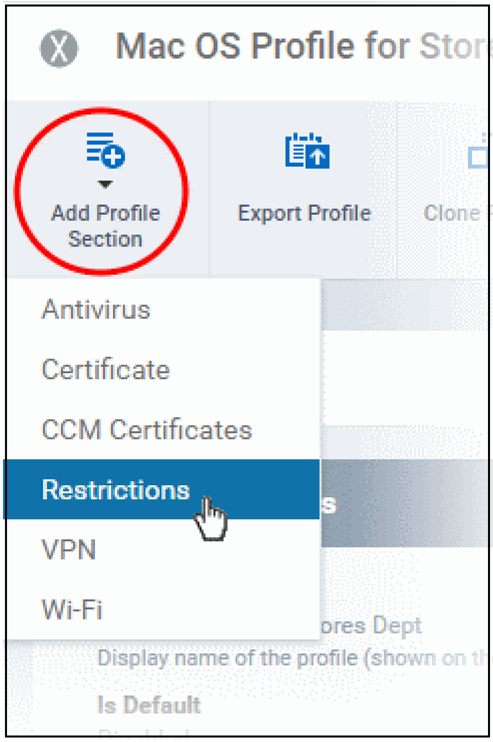
You can add any number of certificates to the profile and remove certificates at anytime. See **Edit Configuration Profiles** for more details.

### 6.1.4.1.3. Restrictions Settings for Mac OS Profile

The 'Restrictions' section allows you to modify the profile to enable or disable selected device features:

#### Configure Restrictions settings

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



The 'Restrictions' settings screen will be displayed.

| Restrictions Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Device Functionality | | |
| Allow Camera | Checkbox | Allows the user to take photos or videos (if enabled). If left unchecked, the camera icon is removed from the device and camera is disabled.<br>Note: This feature is applicable only for OS X 10.11 and later versions. |
| Spotlight will return Internet search results | Checkbox | If enabled, the spotlight features will provide suggestions from the Internet, iTunes, and the App Store for the user to quickly find any file, documents, emails, apps contacts and more on the device.<br>Note: This feature is applicable only for Supervised devices with OS X 10.11 and later versions. |
| iCloud | | |
| Allow cloud document sync | Checkbox | If enabled, users can synchronize documents on their device with iCloud.<br>Note: This feature is applicable only for OS X 10.11 and later versions. |

- Click the 'Save' button.

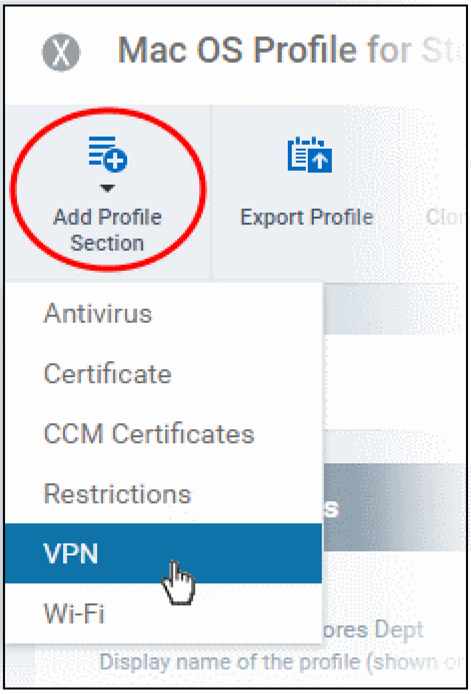
The saved 'Restrictions Settings' screen will be displayed with options to edit the settings or delete the section. See **Edit Configuration Profiles** for more details.

#### 6.1.4.1.4. VPN Settings for Mac OS Profile

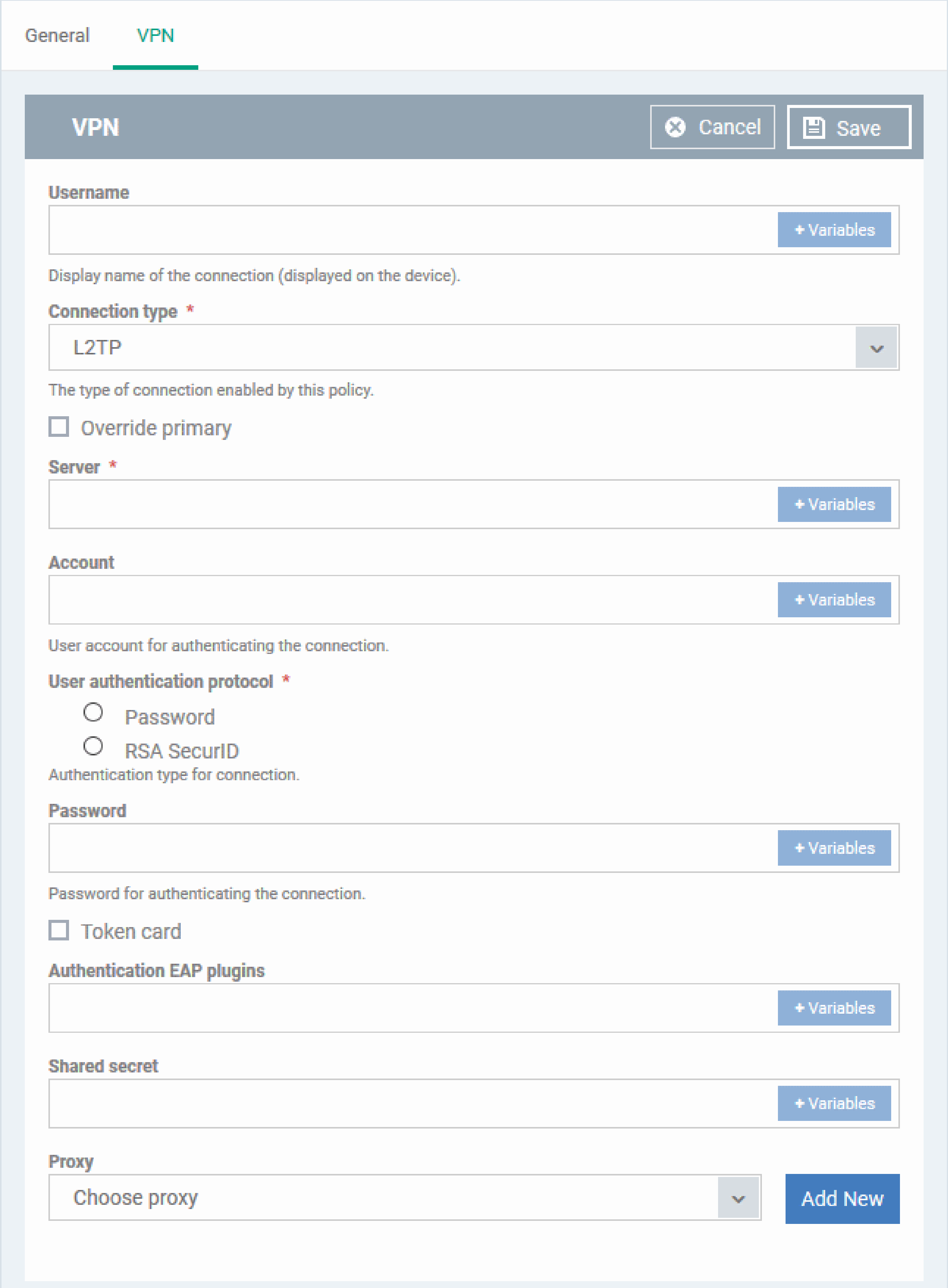
The 'VPN' section allows you to configure the VPN connection settings for the profile.

### Configure VPN settings

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



The settings screen for VPN will be displayed.



Username

Display name of the connection (displayed on the device).

Connection type *

L2TP

The type of connection enabled by this policy.

□ Override primary

Server *

Account

User account for authenticating the connection.

User authentication protocol *

○ Password

○ RSA SecurID

Authentication type for connection.

Password

Password for authenticating the connection.

□ Token card

Authentication EAP plugins

Shared secret

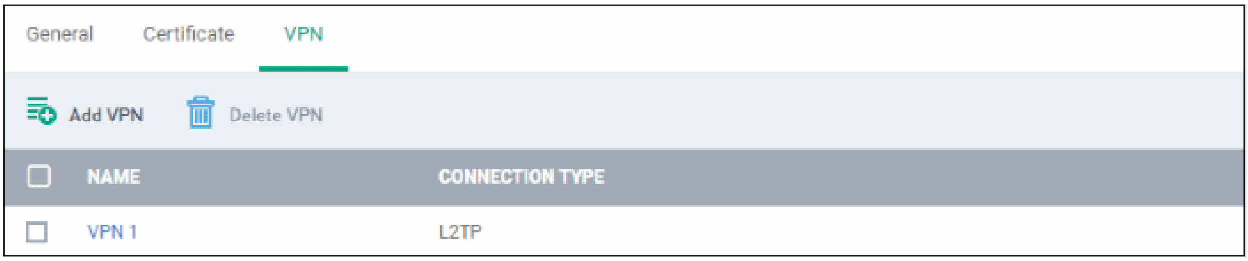
Proxy

Choose proxy

The connection setting parameters are similar to the VPN settings for an iOS profile. See **VPN settings** section for an iOS profile for details.

- Click the 'Save' button after configuring the settings.

The VPN connection will be added to the profile.



| □ | NAME | CONNECTION TYPE |
|---|---|---|
| □ | VPN 1 | L2TP |

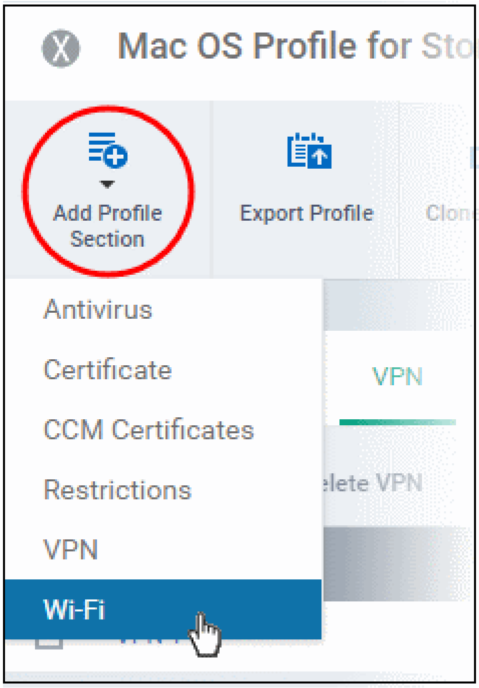
- Click 'Add VPN' and repeat the process to add more VPN connections
- Click the name of a VPN connection to edit its details

The settings will be saved and displayed under the VPN tab. You can edit the settings or remove the section from the profile at anytime. See **Edit Configuration Profiles** for more details.

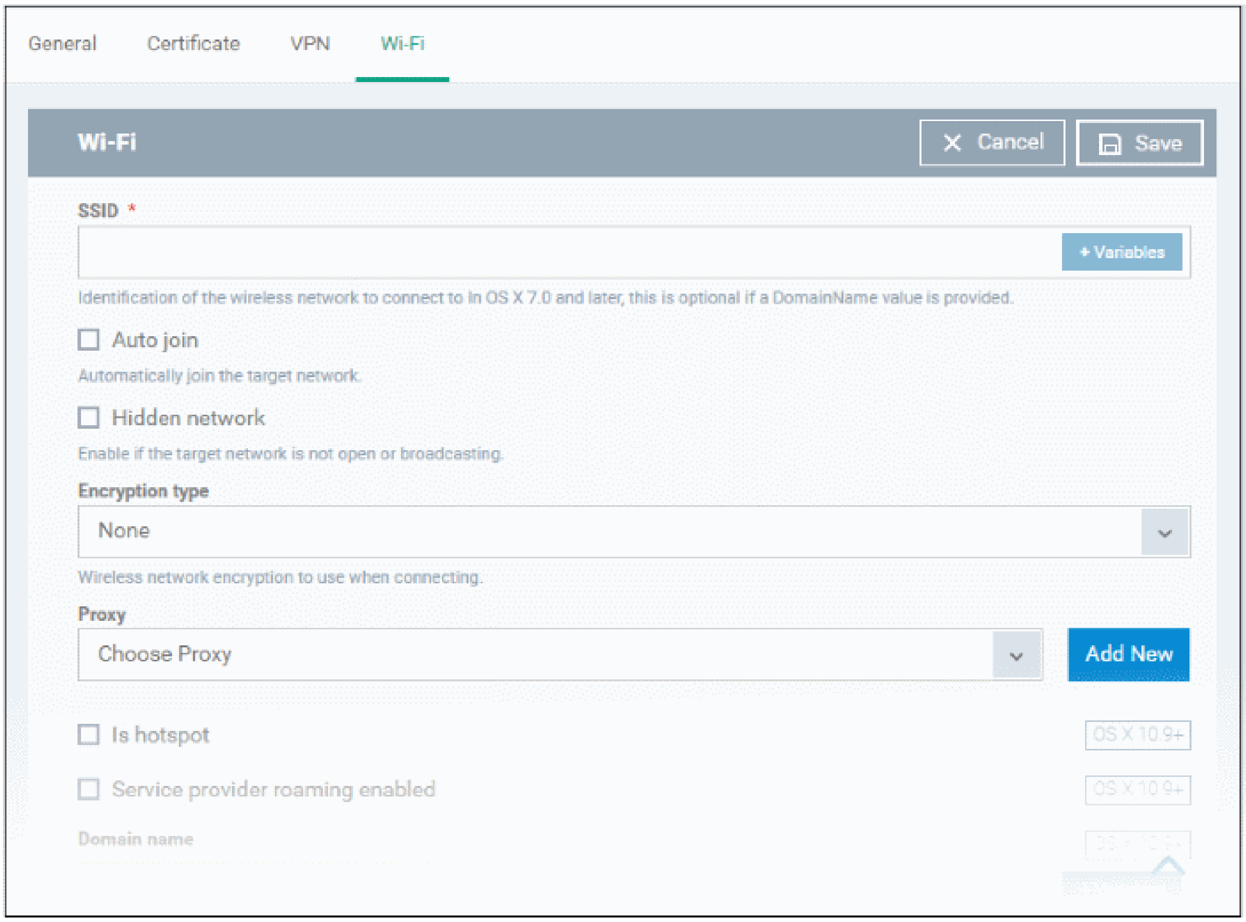
### 6.1.4.1.5. Wi-Fi Settings for Mac OS Profile

The 'Wi-Fi' section allows you to configure Wi-Fi connection settings for the profile.

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



The 'Wi-Fi' settings screen will be displayed.



SSID *

Identification of the wireless network to connect to In OS X 7.0 and later, this is optional if a DomainName value is provided.

□ Auto join

Automatically join the target network.

□ Hidden network

Enable if the target network is not open or broadcasting.

Encryption type

None

Wireless network encryption to use when connecting.

Proxy

Choose Proxy

□ Is hotspot

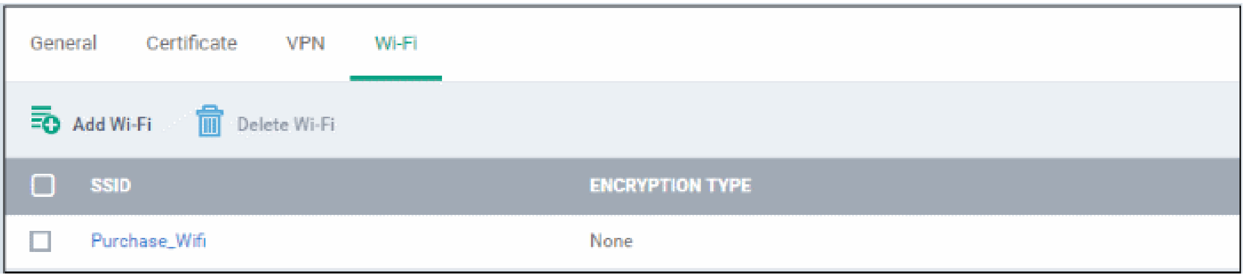
□ Service provider roaming enabled

Domain name

The connection setting parameters are similar to the Wi-Fi settings for an iOS profile. See the **Wi-Fi settings** section for an iOS profile for details.

- Click the 'Save' button after configuring the settings.

The Wi-Fi network will be added to the list.



| □ | SSID | ENCRYPTION TYPE |
|---|---|---|
| □ | Purchase_Wifi | None |

- Click 'Add Wi-Fi' and repeat the process to add more Wi-Fi networks
- Click on SSID of a network to edit its details.

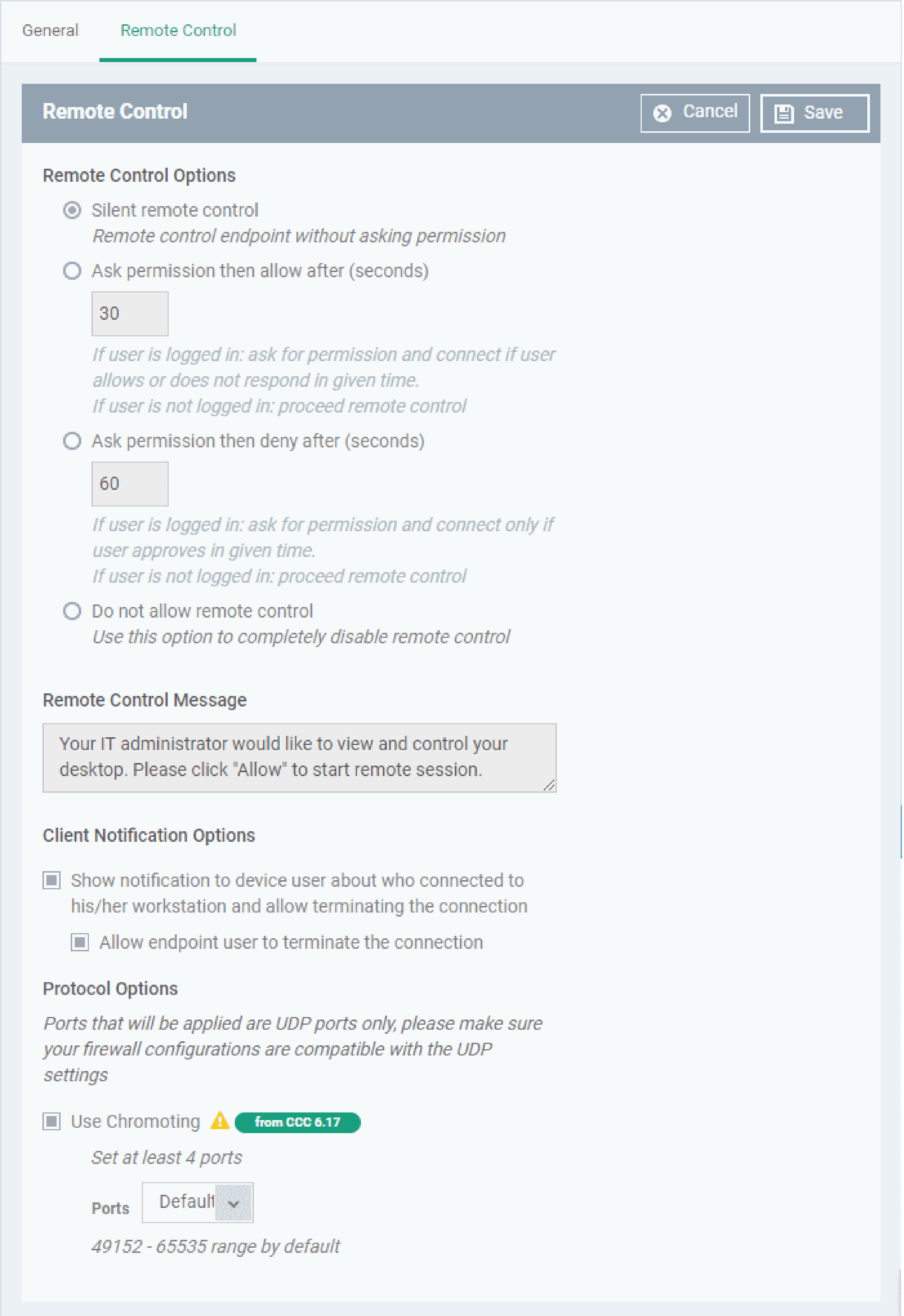
The settings is saved and shown under the Wi-Fi tab. You can edit the settings, add or remove Wi-Fi networks or remove the Wi-Fi networks at anytime. See **Edit Configuration Profiles** for more details.

### 6.1.4.1.6. Remote control Settings for Mac OS Profile

- 'Remote Control' settings let you configure protocol used during remote control sessions.
- You can also customize the message which is shown to Mac OS end-users when you make a remote connection to their computer.
- See **Remote Management of Windows and Mac OS Devices** if you need help to setup the remote control service.

### Configure Remote Control Settings for MAC OS

- Click 'Configuration Templates' > 'Profiles'
- Select a Mac OS profile that you want to configure
- Click 'Add Profile Section' at the top and choose 'Remote Control' from the drop-down.
    - Note: If 'Remote Control' is not in the 'Add...' menu then it has already been added to the profile.
- The 'Remote Control' tab will open:



Remote Control

Remote Control Options

● Silent remote control
*Remote control endpoint without asking permission*

○ Ask permission then allow after (seconds)

30

*If user is logged in: ask for permission and connect if user allows or does not respond in given time.*
*If user is not logged in: proceed remote control*

○ Ask permission then deny after (seconds)

60

*If user is logged in: ask for permission and connect only if user approves in given time.*
*If user is not logged in: proceed remote control*

○ Do not allow remote control
*Use this option to completely disable remote control*

Remote Control Message

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

☑ Show notification to device user about who connected to his/her workstation and allow terminating the connection

☑ Allow endpoint user to terminate the connection

Protocol Options

*Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings*

☑ Use Chromoting ⚠ from CCC 6.17

*Set at least 4 ports*

Ports: Default

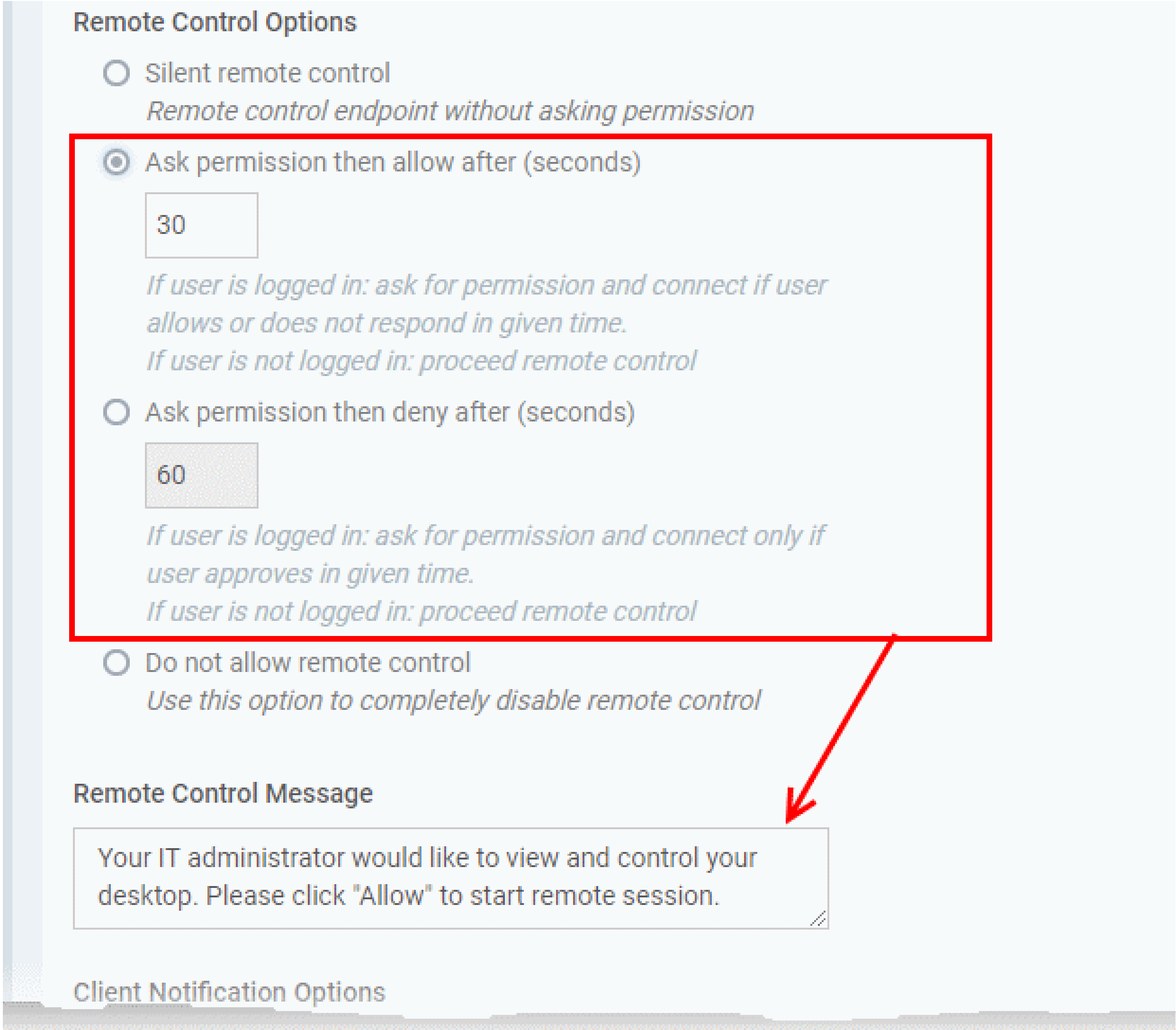
*49152 - 65535 range by default*

**Remote Control Options:**

- Silent remote control -The remote connection will start without requesting permission from the user.
- Ask permission then allow after NN seconds:
  - A message will be shown to the user which requests them to accept the connection. The connection will be automatically established if the user does not respond within the specified time.
  - Specify the timeout period (in seconds) in the text box
- Ask permission then deny after NN seconds:
  - A message will be shown to the user which requests them to accept the connection. The connection attempt will be terminated automatically if the user does not respond within the specified time.
  - Specify the timeout period (in seconds) in the text box.
- Do not allow remote control**:** Disable the ability to take remote control of the endpoint.

**Remote Control Message**

- Enter the text of the request message. For example, 'Your administrator would like to take control of your desktop. Click 'Allow' to accept the connection request.'
  - Please note that you can enter the message only if you choose the second or third notification options.



Remote Control Options

○ Silent remote control

*Remote control endpoint without asking permission*

● Ask permission then allow after (seconds)

30

*If user is logged in: ask for permission and connect if user allows or does not respond in given time.*
*If user is not logged in: proceed remote control*

○ Ask permission then deny after (seconds)

60

*If user is logged in: ask for permission and connect only if user approves in given time.*
*If user is not logged in: proceed remote control*

○ Do not allow remote control

*Use this option to completely disable remote control*

Remote Control Message

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

**Client Notification Options**

This area lets you configure the notification box which is shown on the endpoint when a remote session is active:

- Show notification to device user about who connected to his/her workstation and allow terminating the connection - Let the end user know which EM admin/technician is connected to their machine.

- Allow endpoint user to terminate the connection - Choose whether the 'End Session' button should be shown in the notification box or not. If enabled, the end-user will be able to close the connection.

**Protocol Options**

These settings let you choose the protocol used to connect to Mac OS devices.

- These settings apply to RC version 6.17 and above.
- You can also specify custom ports to be used by the protocol for an additional layer of safety. This allows you to keep only the specified ports open and block other ports for security.

**Note**:Please make sure you do not assign well-known special ports. We recommend the following port range for custom use: 49152-65535.

- Use Chromoting - RC uses Chromoting protocol to connect to the device. This option is mandatory and cannot be deselected.
- Ports - Select the port type to be used by Chromoting protocol and specify the ports. The available options are:
  - Default - Chromoting will use the port range 49152 - 65535
  - Custom Range - Allows you to specify a port range to be used by Chromoting. Enter a range covering at least 4 ports.

**Note**: Chromoting is supported by Windows 7 and later versions. If RC is installed on a Windows XP admin machine, it will not be able to connect to a Mac OS device.

- Click 'Save' to apply your changes to the profile.

### 6.1.4.1.7. Valkyrie Settings for MacOS Profile

- Valkyrie is a cloud-based file verdict service that subjects unknown files to a range of tests in order to identify those that are malicious.
- Comodo Client Security for Mac can automatically submit unknown files to Valkyrie for analysis. When the tests are complete, Valkyrie will award a trust verdict to the file.
  - Note - 'Cloud Scanning' should be enabled in Antivirus section of CCS for Mac on the endpoints.
- The verdicts can be viewed in 'Security Sub-Systems' > 'Valkyrie' interface.
  - See **View list of Valkyrie Analyzed Files** for more details.
- Click 'Dashboard' > 'Valkyrie' to view summary of all Valkyrie results.

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

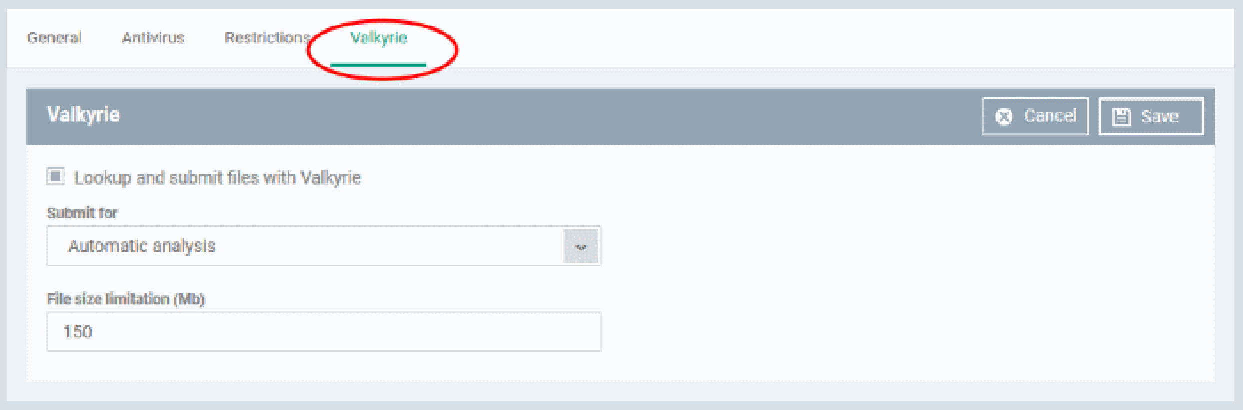
You can configure general Valkyrie settings and create an analysis schedule in the Valkyrie component of a Mac OS profile.

**Configure Valkyrie Settings**

- Click 'Valkyrie' from the 'Add Profile Section' drop-down in the Mac OS Profile interface

The 'Valkyrie' settings screen will be displayed.

- Click 'Edit'



Valkyrie

□ Lookup and submit files with Valkyrie

Submit for: Automatic analysis

File size limitation (Mb): 150

| Valkyrie Settings for Mac OS Profile - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Lookup and submit files with Valkyrie | Choose this option if you want the files to be submitted to the cloud file lookup service |
| 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. |
| File size limitations (MB) | Specify the maximum file size for upload to Valkyrie. The default value is 150 MB. |

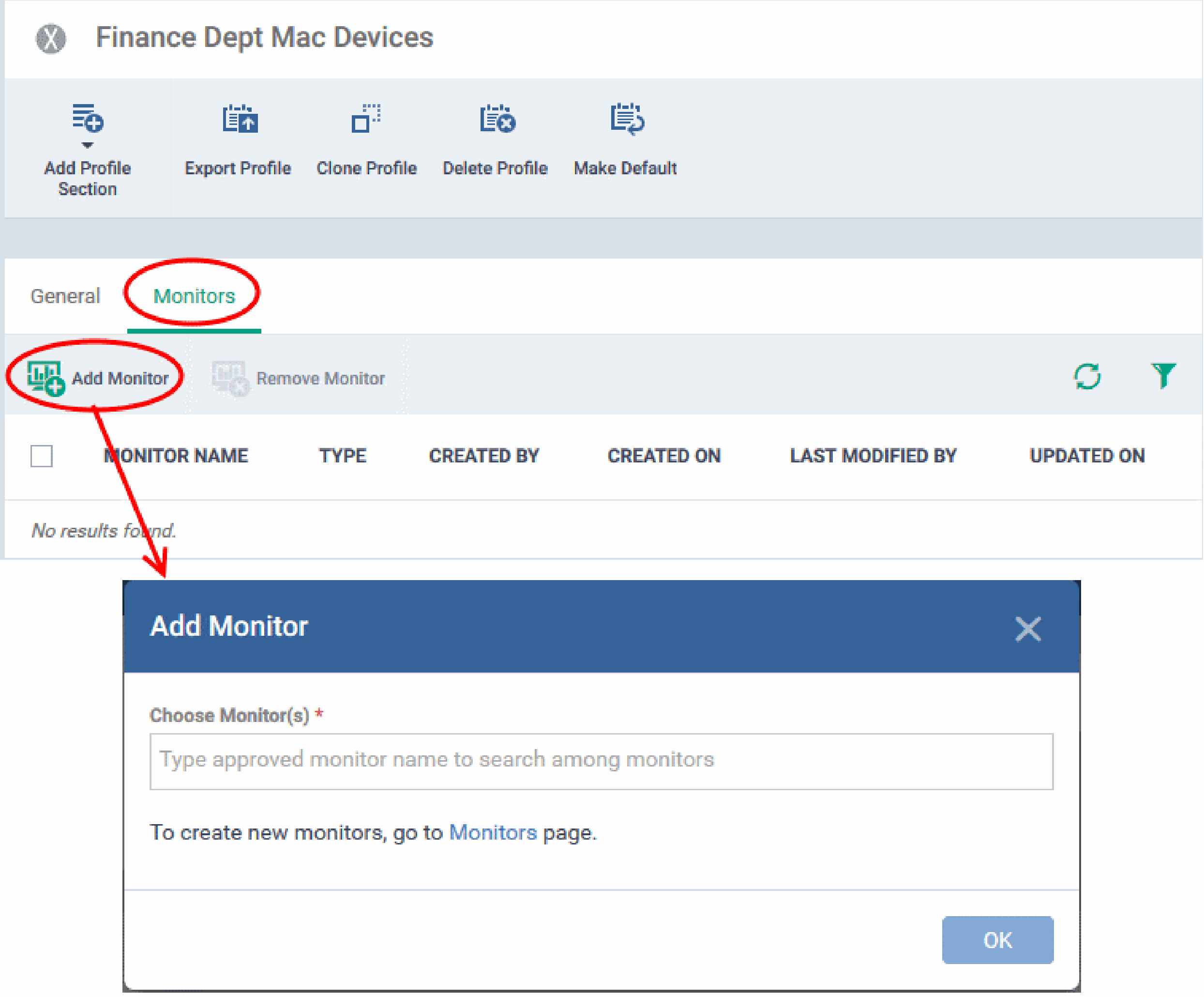
- Click 'Save'

### 6.1.4.1.8. Monitor settings for Mac OS Profile

- The monitors settings section lets you add performance and event monitors to a Mac OS profile.
- A monitor is a script which tracks events on a managed endpoint and generates alerts if its conditions are met.
  - For example, 'Alert me when a certain process is running on the device', or 'Alert me if CPU usage goes above 75% for a certain length of time'.
- There are two types of monitor:
  - **Predefined Monitors -** A collection of monitors from Comodo which perform a range of useful monitoring tasks. These can be used in custom profiles, but cannot be edited.
  - **My Monitors -** Custom monitors that you create. You can configure custom monitors in the 'Monitors' inventory ('Configuration Templates' > 'Monitors'). See '**Manage Monitors**' for more details.
- Monitors added to the inventory can be added to a profile. You can add multiple monitors to a single profile.

**Add a monitor section to a profile**

- Click 'Configuration Templates' > 'Profiles'
- Open the Mac OS profile you want to configure
- Click 'Add Profile Section' > 'Monitors'
- Click 'Add Monitor'



*No results found.*

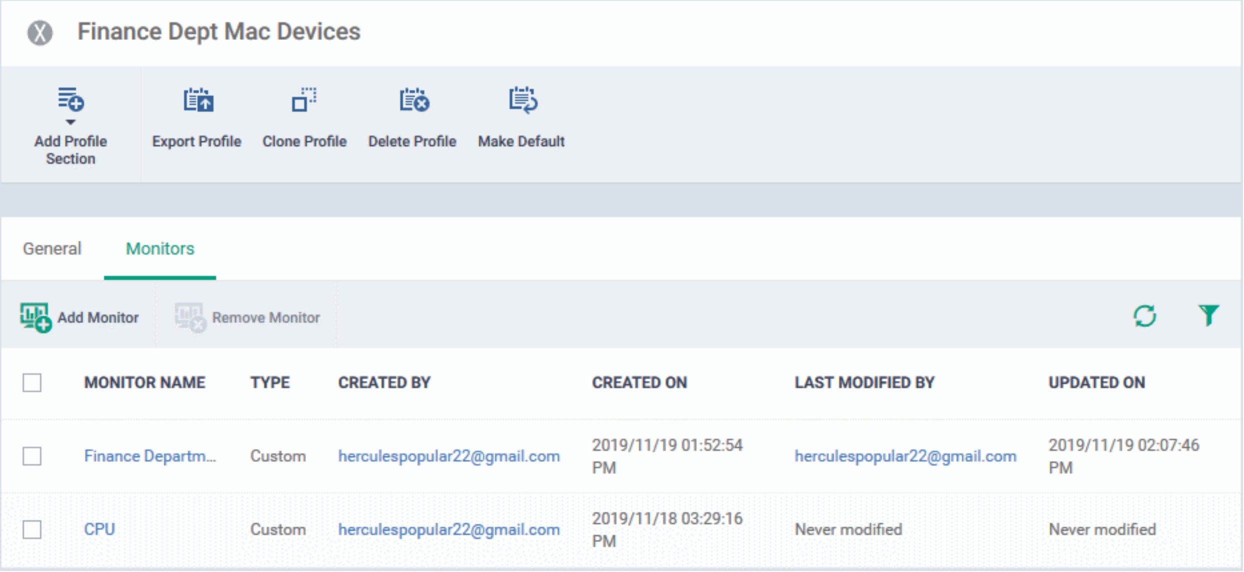
Choose Monitor(s) *

Type approved monitor name to search among monitors

To create new monitors, go to Monitors page.

- Choose Monitor(s) - Add monitors to the profile
  - Start typing the first few letters of the name of a Mac OS then select from the suggestions
  - Repeat the process to add more monitors to the profile
  - See **Monitors for Mac OS Devices** for help to configure a monitor
- Click 'OK' to save your settings

The list of monitors included in the profile is shown:



| □ | MONITOR NAME | TYPE | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|---|
| □ | Finance Departm... | Custom | herculespopular22@gmail.com | 2019/11/19 01:52:54 PM | herculespopular22@gmail.com | 2019/11/19 02:07:46 PM |
| □ | CPU | Custom | herculespopular22@gmail.com | 2019/11/18 03:29:16 PM | Never modified | Never modified |

| Monitors - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The monitor label.<br>• Click the name of a monitor view and edit it. See **View and Edit Monitors** for more details. |
| Type | Whether the monitor is custom or predefined. |
| Created by | The administrator who created the custom monitor.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created On | Date and time the monitor was created. |
| Last Modified By | The admin who most recently edited the monitor. |
| Updated On | Date and time the monitor was last edited. |
| **Controls** | |
| Add Monitor | Add a monitor to the profile. See the explanation **above** for help with this. |
| Remove Monitor | Delete monitors from the profile Use the check-boxes to select the monitors you want to remove. |

- Click any column header to sort the items based on alphabetical or ascending/descending order of entries in the respective column.
- Click the funnel button at the right end to open the filter options.

## 6.1.5. Profiles for Linux Devices

Linux profiles let you configure Comodo Client Security (CCS) on Linux endpoints.

There are two ways you can add a new Linux profile to Endpoint Manager:

- Create a new Linux profile. See **Create Linux a Profile** for more details.
- Clone an existing profile and modify its settings to your requirements. See **Clone a Profile**, for more details.

### 6.1.5.1. Create a Linux Profile

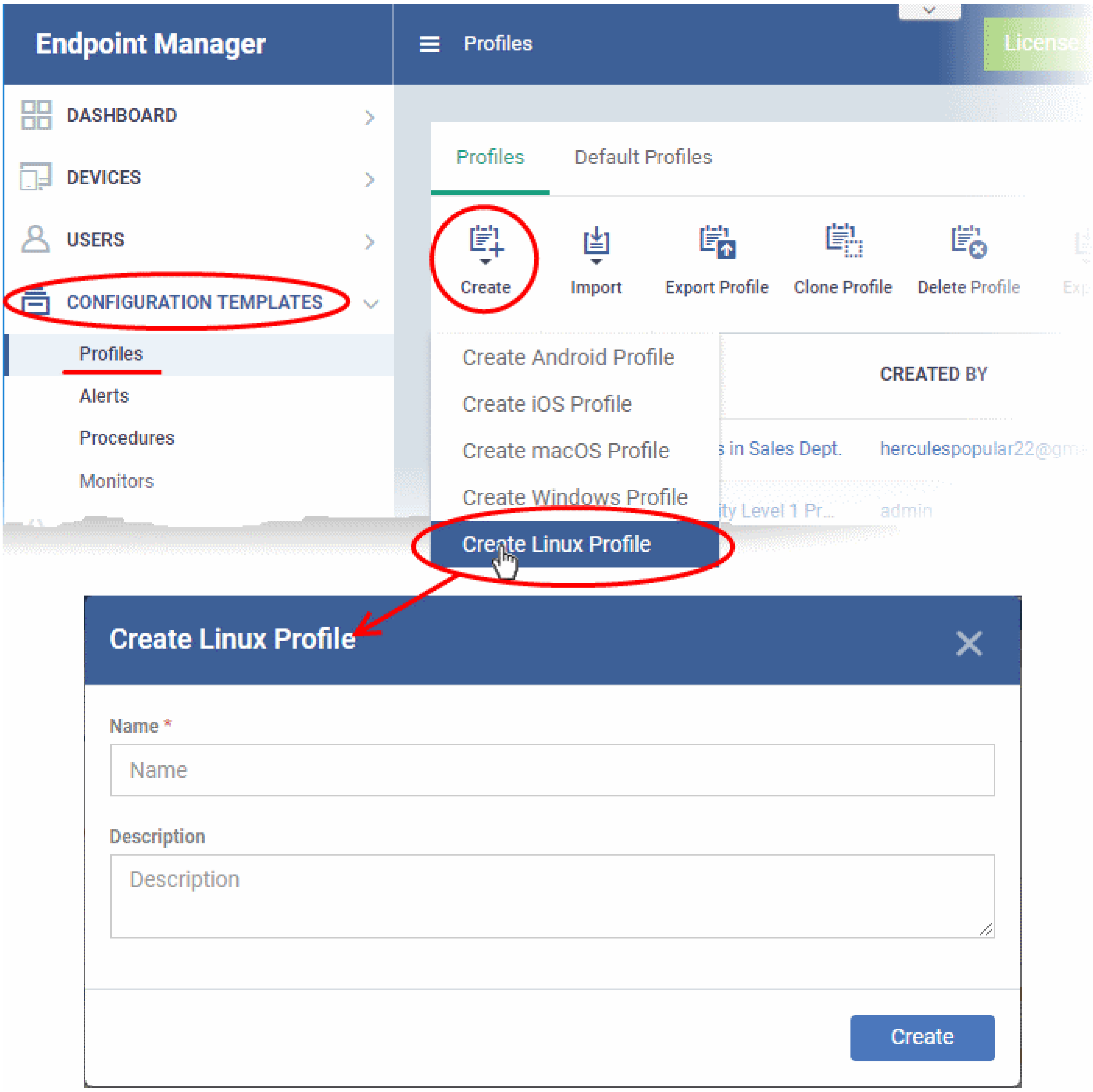
Process in brief:

- Click 'Configuration Templates' > 'Profiles'
- Click 'Create' > 'Create Linux Profile'
- Type a name and description for your profile then click the 'Create' button. The profile will now appear in 'Configuration Templates' > 'Profiles'.
- New profiles have only one section - 'General'. Click 'Add Profile Section' to add settings for various security and management features. Each section you add will appear as a new tab.
- Once configured, you can apply your profile to devices and device groups.
- You also have the option to make it a 'Default' profile. A 'default' profile is one that is automatically applied to any device which matches its operating system.

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

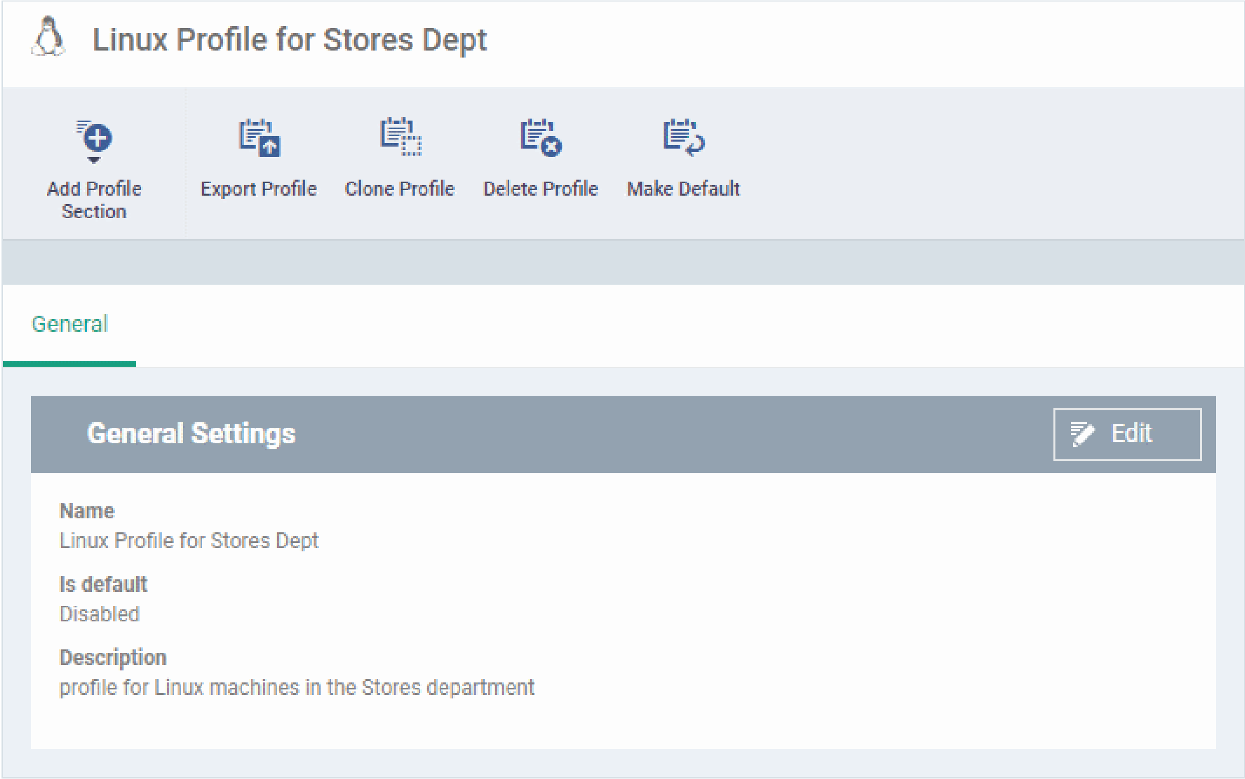
**Create a new profile**

- Click 'Configuration Templates' > 'Profiles' > 'Create' > 'Create Linux Profile'



- Name - Enter a label for the profile
- Description - Enter appropriate short notes for the profile
- Click the 'Create' button

The profile will open at the 'General Settings' section:



Name
Linux Profile for Stores Dept

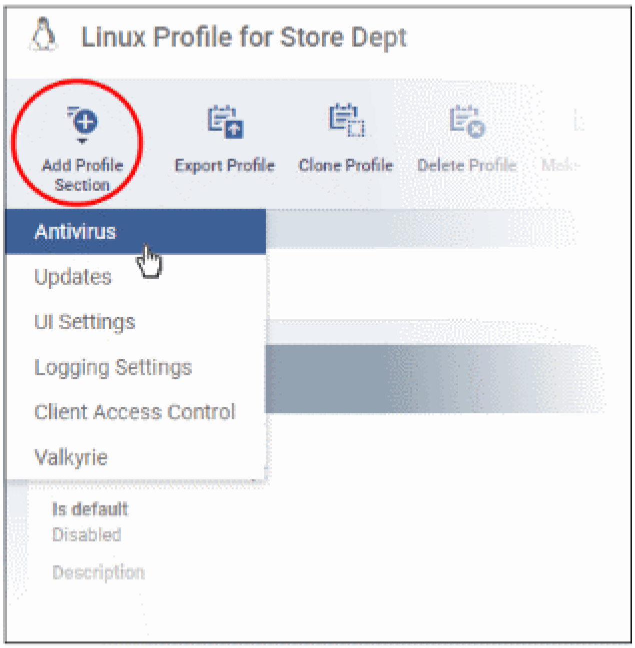
Is default
Disabled

Description
profile for Linux machines in the Stores department

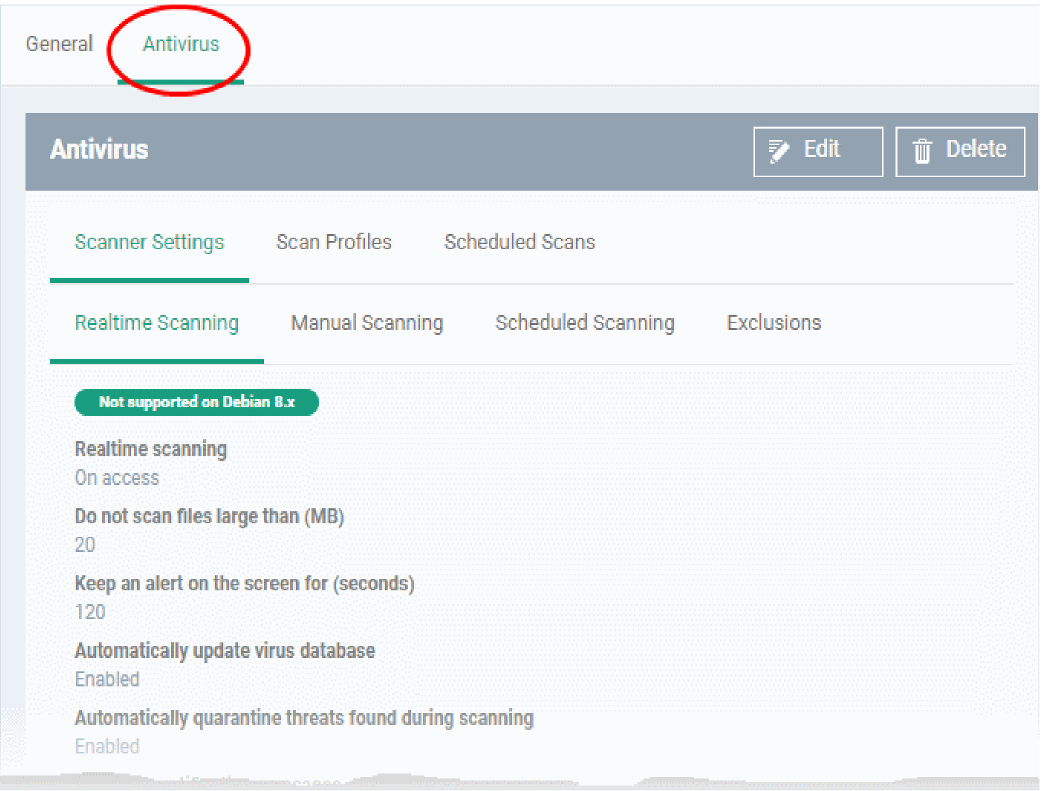
- 'Make Default' - A 'default' profile is one that is applied automatically to any device which matches its operating system. Click this button if you want this profile to be applied to every Linux device. Do not select this if you only want to apply the profile to certain Linux endpoints.
- Click 'Save'.

The next step is to add profile sections.

- Each profile section contains a range of settings for a specific security or management feature.
- For example, there are profile sections for 'Antivirus', 'Logging', 'UI' and so on.
- You can add as many different sections as you want when building your profile.
- To get started:
    - Click 'Add Profile Section'
    - Select the section that you want to add to the profile:



This will open the settings screen of the component:



Realtime scanning
On access

Do not scan files large than (MB)
20

Keep an alert on the screen for (seconds)
120

Automatically update virus database
Enabled

Automatically quarantine threats found during scanning
Enabled

Click the following links to find out more about each section:

- **Antivirus**
- **Updates**
- **UI Settings**
- **Logging Settings**
- **Client Access Control**
- **Valkyrie Settings**

### 6.1.5.1.1. Antivirus Settings for Linux Profile

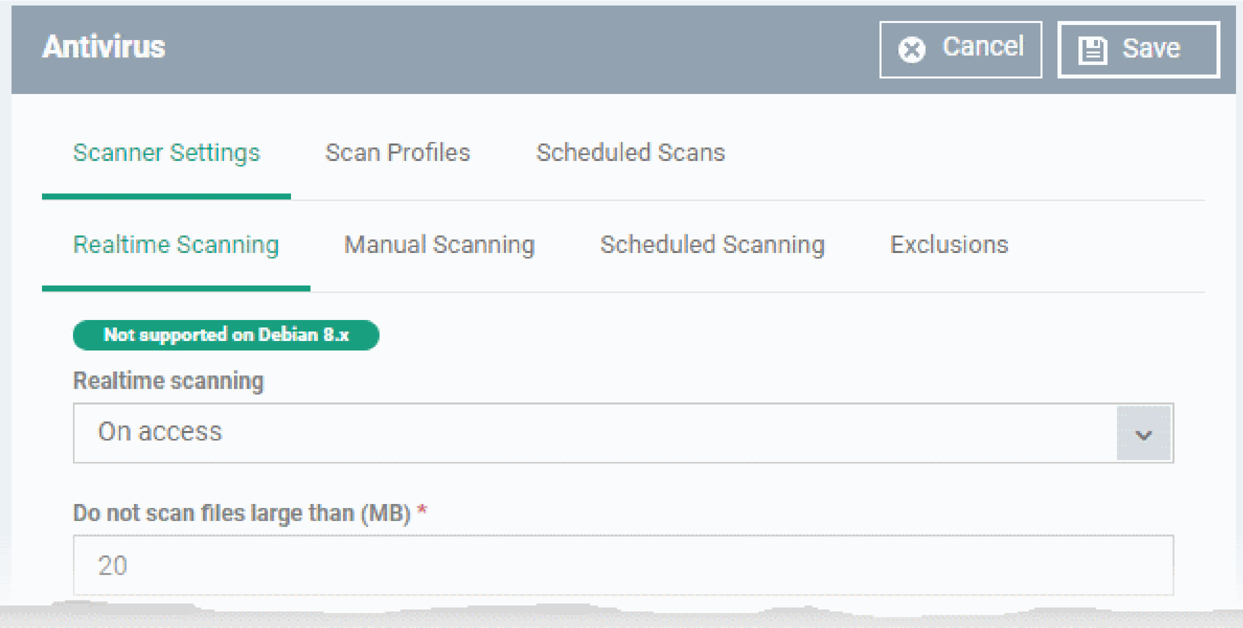
The antivirus section lets you configure real-time monitoring, custom scans, scan schedules, exclusions and more.

#### Configure antivirus settings in a Linux profile

- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Linux profile
- Click 'Add Profile Section' then 'Antivirus' (if you haven't yet added the AV section)

  OR
- Open the 'Antivirus' tab and click 'Edit' if it was already added

The antivirus settings screen will open:



Realtime scanning: On access

Do not scan files large than (MB) *: 20

It contains three tabs:

- **Scanner Settings** - Configure real-time scans, manual scans, scheduled scans and exclusions.
- **Scan Profiles** - Create antivirus scan profiles that define specific folders, drives or areas to scan. Once saved, you can apply a scan profile to scheduled scans.
- **Scheduled Scans** - Timetable scans to be run on managed devices according to a selected scan profile.

#### Configure Scanner Settings for CCS for Linux

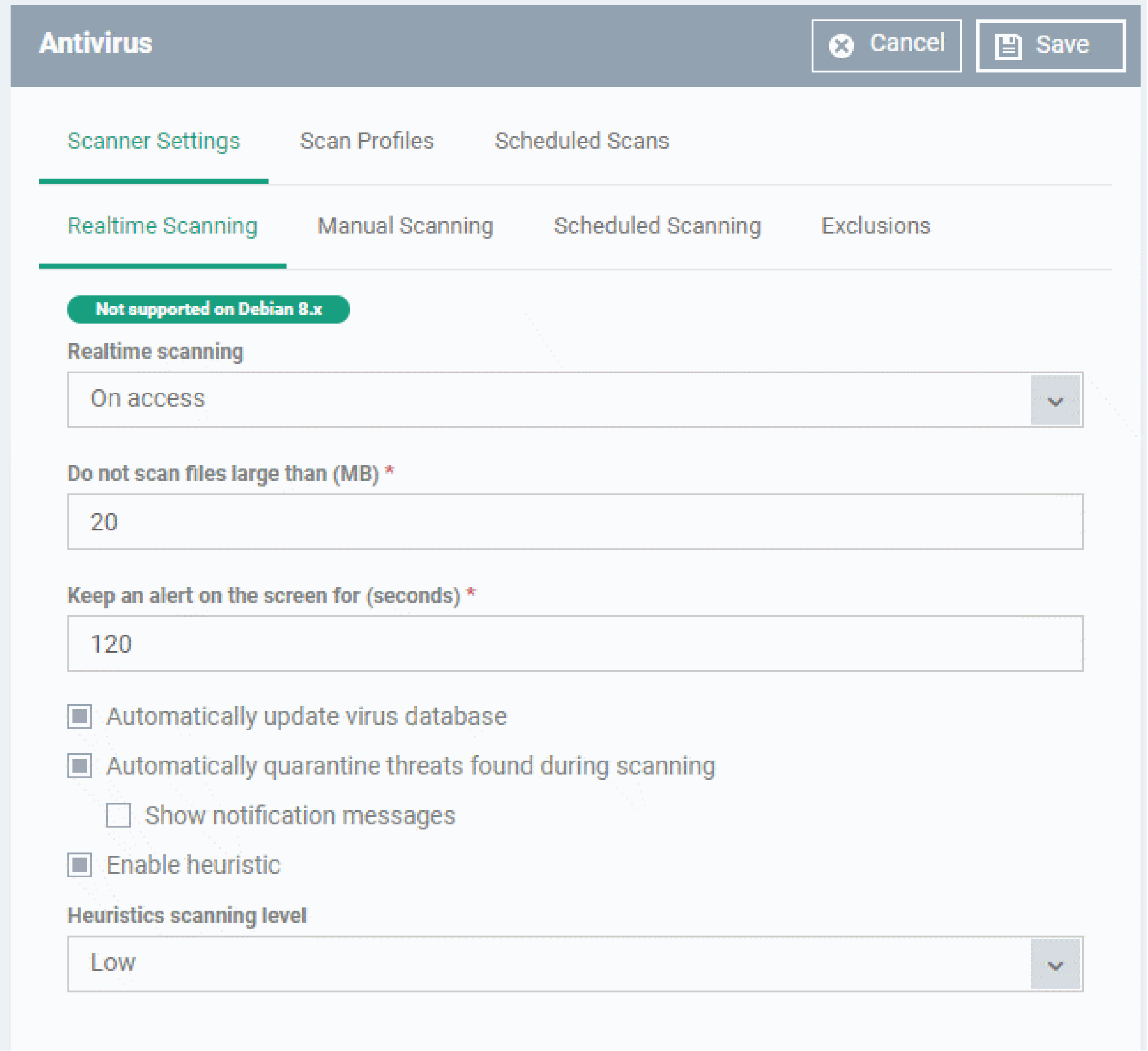
The 'Scanner Settings' area contains four sub-tabs:

- **Realtime Scanning** - Set parameters for the 'always-on' virus monitor
- **Manual Scanning** - Set parameters for on-demand scans
- **Scheduled Scanning** - Set parameters for scheduled scans
- **Exclusions** - View and manage items which will be skipped by virus scans.

#### Realtime Scanning

- Click the 'Realtime Scanning' sub-tab under 'Scanner Settings'

**Please note**: The real-time virus scanner is not supported on Debian. The settings in this screen do not apply to Debian devices.



Realtime scanning: On access

Do not scan files large than (MB) *: 20

Keep an alert on the screen for (seconds) *: 120

☑ Automatically update virus database

☑ Automatically quarantine threats found during scanning

☐ Show notification messages

☑ Enable heuristic

Heuristics scanning level: Low

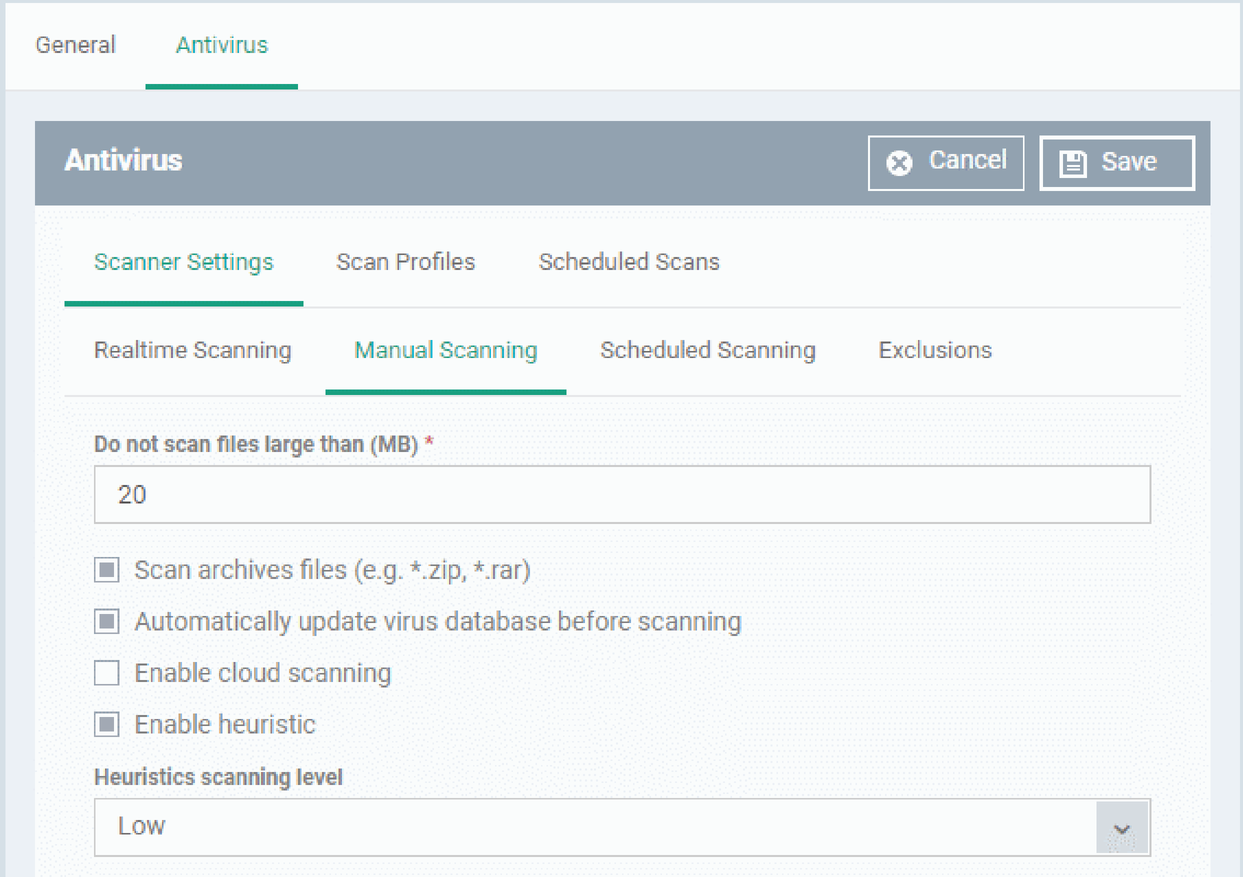
| Real Time Scanning Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Real time scanning | Drop-down | Enable or disable the background virus monitor.<br>• On Access - Files are scanned before they are allowed to run. Threats are detected before they get a chance to execute (***Default***)<br>• Disabled - Real-time protection is switched off. Files are allowed to run without first being checked for threats. |
| Do not scan files larger than (MB) | Text box | Maximum file size that the antivirus should attempt to scan. Files larger than the size specified here are not scanned. ***(Default = 20 MB)***. |

| Real Time Scanning Settings - Table of Parameters | | |
|---|---|---|
| Keep an alert on the screen for (seconds) | Text box | How long threat notifications should stay on-screen if not dismissed by the end-user. (***Default = 120 seconds***) |
| Automatically update virus database | Checkbox | CCS will check for and download the latest virus database updates on system start-up, and subsequently at regular intervals.<br>• Disable this option if you do not want CCS to automatically check for updates.<br>(***Default = Enabled***). |
| Automatically quarantine threats found during scanning | Checkbox | Threats will be encrypted and moved to a secure holding area where they can cause no harm. You can review quarantined items and delete, ignore or restore them.<br>• Disable this option if you do not want threats to be moved to quarantine.<br>(***Default = Enabled***) |
| Show notification messages | Checkbox | Choose whether or not a notification is to be shown to the end-user, whenever CCS identifies a threat and moves it to quarantine.<br>(***Default = Disabled***) |
| Enable heuristic scanning | Checkbox | Enable or disable heuristics scanning and define the scan level.<br>The scan level determines how likely the scanner is to classify an unknown file as a threat.<br>• Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)<br>• Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.<br>• High- Highest sensitivity to detecting unknown threats / increased possibility of false positives.<br>(***Default = Enabled with 'Low ' option***)<br>**Background Note**: Background. Heuristics identify previously unknown malware by checking 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.<br>Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current database. |

## Manual Scanning

- Click the 'Manual Scanning' sub-tab under 'Scanner Settings'

- The options you set here will apply to manual scans on the endpoints on which the profile is active.
- A manual scan is one you run 'on-demand' on selected files, folder or drives. Manual scans can be launched from 'Security Sub-Systems' > 'Antivirus'.
- For more details on running on-demand scans on selected devices, see **Run Antivirus and/or File Rating Scans on Devices**.



Do not scan files large than (MB) *
20

☑ Scan archives files (e.g. *.zip, *.rar)
☑ Automatically update virus database before scanning
☐ Enable cloud scanning
☑ Enable heuristic

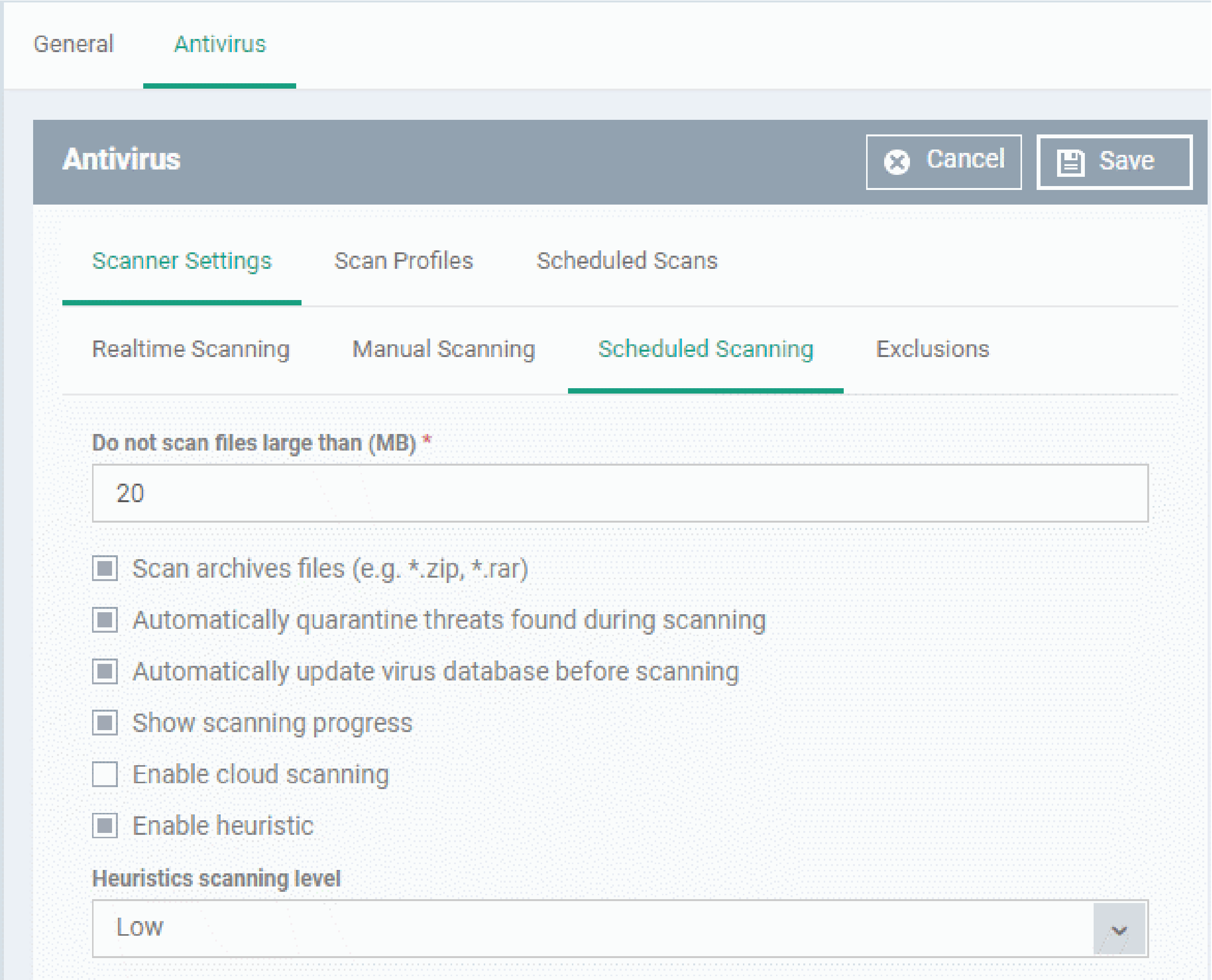
Heuristics scanning level
Low

| Manual Scanning Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Do not scan files large than (MB) | Text box | Maximum file size that the antivirus should attempt to scan. Files larger than the size specified here are not scanned. ***(Default = 20 MB).*** |
| Scan archive files | Checkbox | CCS scans archive files such as .ZIP and .RAR files.<br>• Disable this option if you don't want archive files to be scanned.<br>(***Default = Enabled***). |
| Automatically update virus database before scanning | Checkbox | CCS will check for and download the latest virus database before starting an on-demand scan<br>• Disable this option if you do not want CCS to automatically check for updates.<br>(***Default = Enabled***). |
| Enable cloud scanning | Checkbox | CCS detects the very latest viruses more accurately because |

| Manual Scanning Settings - Table of Parameters | | |
|---|---|---|
| | | the local scan is augmented with a real-time look-up of Comodo's online signature database. This makes it possible to detect zero-day malware even if your local virus database is outdated. (***Default = Disabled***). |
| Enable heuristic scanning | Checkbox | Enable or disable heuristics scanning and define the scan level.<br>The scan level determines how likely the scanner is to classify an unknown file as a threat.<br>• Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)<br>• Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.<br>• High- Highest sensitivity to detecting unknown threats / increased possibility of false positives.<br>(***Default = Enabled with 'Low ' option***)<br>**Background Note**: Background. Heuristics identify previously unknown malware by checking 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.<br>Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current database. |

## Scheduled Scanning

- Click the 'Scheduled Scanning' sub-tab under 'Scanner Settings'
- The options you set will apply to scheduled scans created for the profile. See **Create and Manage Scheduled Scans for the Profile** if you need help with this.



Do not scan files large than (MB) *

20

☒ Scan archives files (e.g. *.zip, *.rar)

☒ Automatically quarantine threats found during scanning

☒ Automatically update virus database before scanning

☒ Show scanning progress

☐ Enable cloud scanning

☒ Enable heuristic

Heuristics scanning level

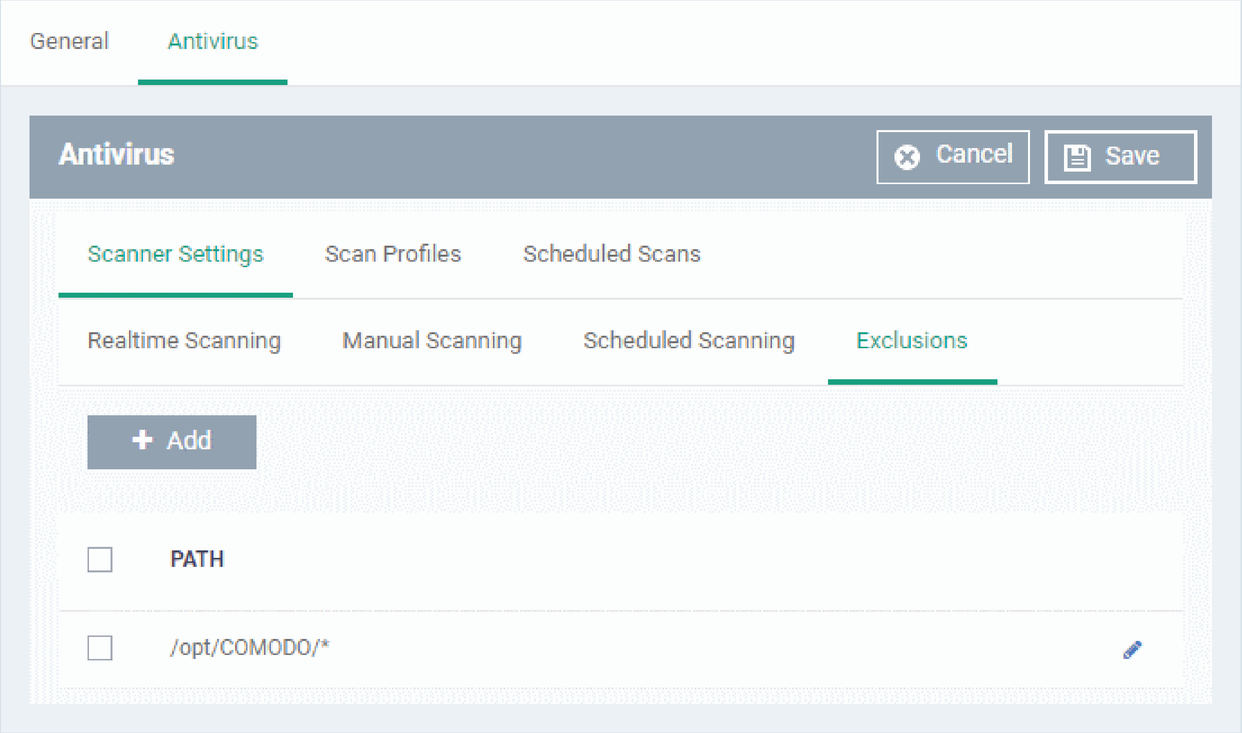
Low

| Scheduled Scanning Settings - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Do not scan files large than (MB) | Text box | Maximum file size that the antivirus should attempt to scan. Files larger than the size specified here are not scanned. **(Default = 20 MB).** |
| Scan archives files | Checkbox | CCS scans archive files such as .ZIP and .RAR files.<br>• Disable this option if you don't want to scan archive files.<br>(***Default = Enabled***). |
| Automatically quarantine threats found during scanning | Checkbox | Threats identified by scheduled scans will be encrypted and moved to a secure holding area where they can cause no harm. You can review quarantined items and delete, ignore or restore them.<br>• Disable this option if you do not want threats to be moved to quarantine.<br>(***Default = Enabled***) |
| Automatically update virus database before scanning | Checkbox | CCS will check for and download the latest virus database updates on system start-up, and subsequently at regular intervals.<br>• Disable this option if you do not want CCS to automatically check for updates. (***Default = Enabled***). |
| Show scanning progress | Checkbox | End-users will see a scan progress bar when the scan is running.<br>• Disable this option if you don't want CCS to show the progress bar. (***Default = Enabled***) |
| Enable cloud scanning | Checkbox | CCS detects the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. This makes it possible to detect zero-day malware even if your local virus database is outdated. (***Default = Disabled***). |
| Enable heuristic scanning | Checkbox | Enable or disable heuristics scanning and define the scan level.<br>The scan level determines how likely the scanner is to classify an unknown file as a threat.<br>• Low - Lowest sensitivity to detecting unknown threats / generates fewest false positives. The 'low' setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)<br>• Medium - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.<br>• High- Highest sensitivity to detecting unknown threats / increased possibility of false positives.<br>(***Default = Enabled with 'Low ' option***)<br>**Background Note**: Background. Heuristics identify previously unknown malware by checking 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.<br>Heuristics is about detecting 'virus-like' attributes rather than |

| Scheduled Scanning Settings - Table of Parameters | | |
|---|---|---|
| Form Element | Type | Description |
| | | looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current database. |

## Exclusions

- Click the 'Exclusions' sub-tab under 'Scanner Settings'
- You can add files to be ignored by CCS during virus scans.
- Note. Any item you exclude will be skipped by ALL types of scan - real-time, on-demand and scheduled.

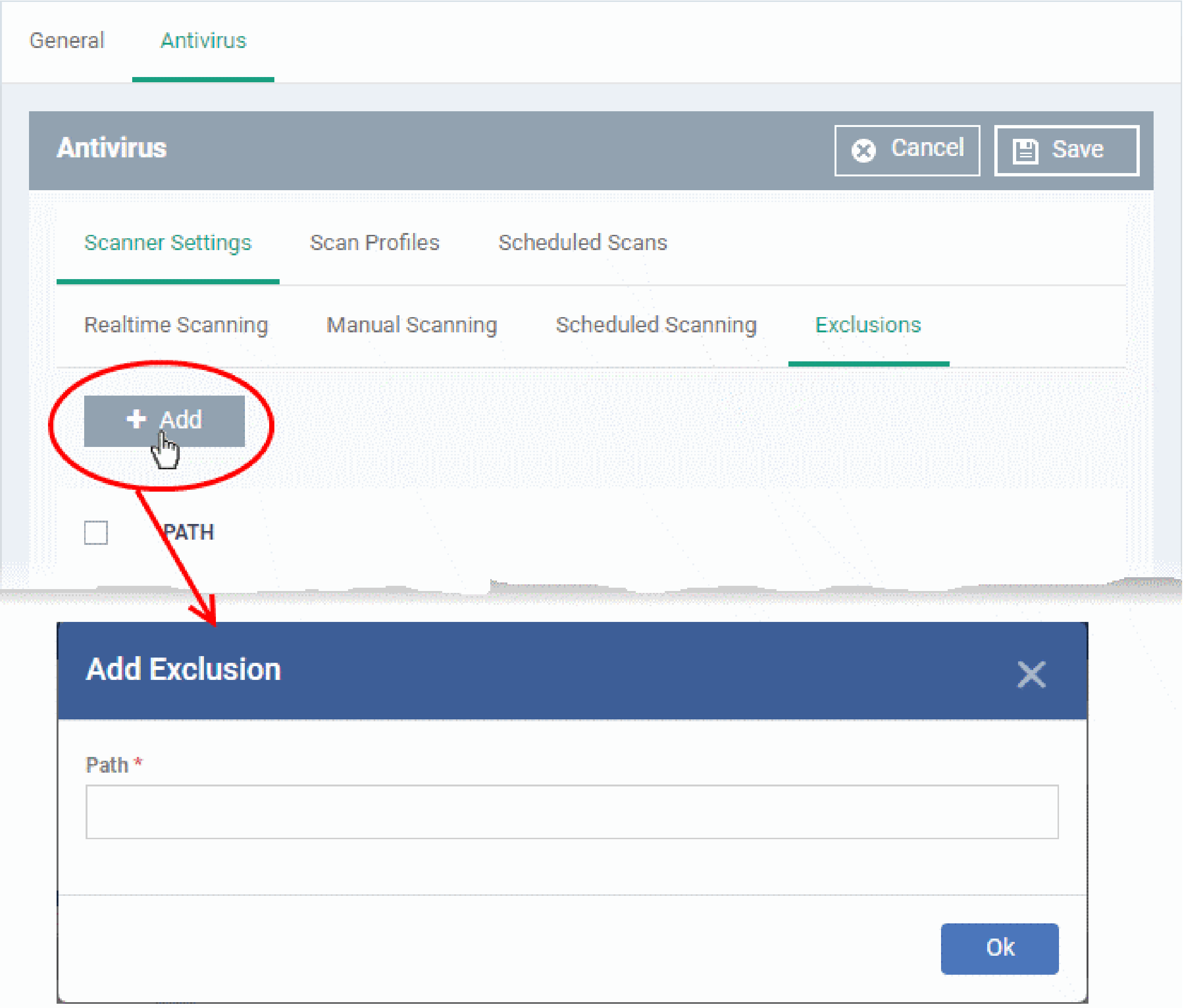


| □ | PATH |
|---|---|
| □ | /opt/COMODO/* |

A list of excluded items will be displayed.

**To add an item to the 'Exclusions' list**

- Click 'Add'

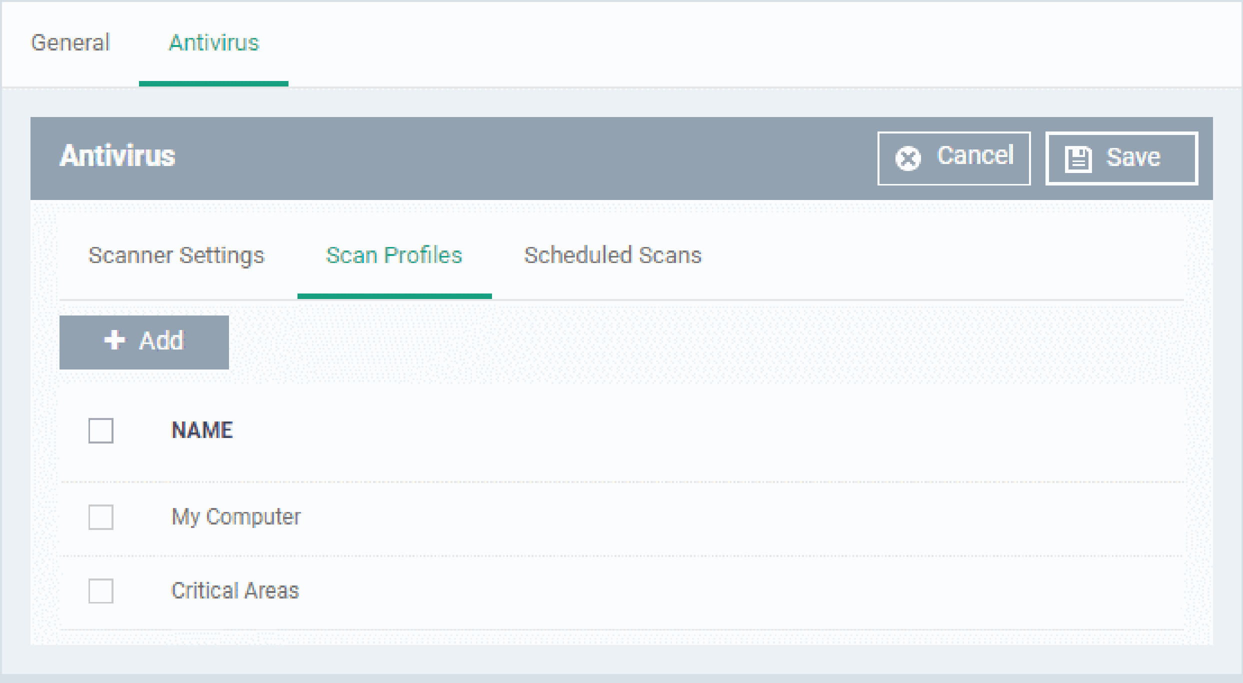


- Enter the location of the item to be excluded in the 'Path' field and click 'Ok'
- Repeat the process to add more items

- To edit the path of an item, click the pencil icon ✎ beside it

### Create and Manage Scan Profiles for the Profile

- Click the 'Scan Profiles' tab under 'Antivirus'
- Scan profiles instruct CCS to scan selected areas, folders or drives on a the device.
- The scan profiles you create here will be available when you configure a scheduled scan.

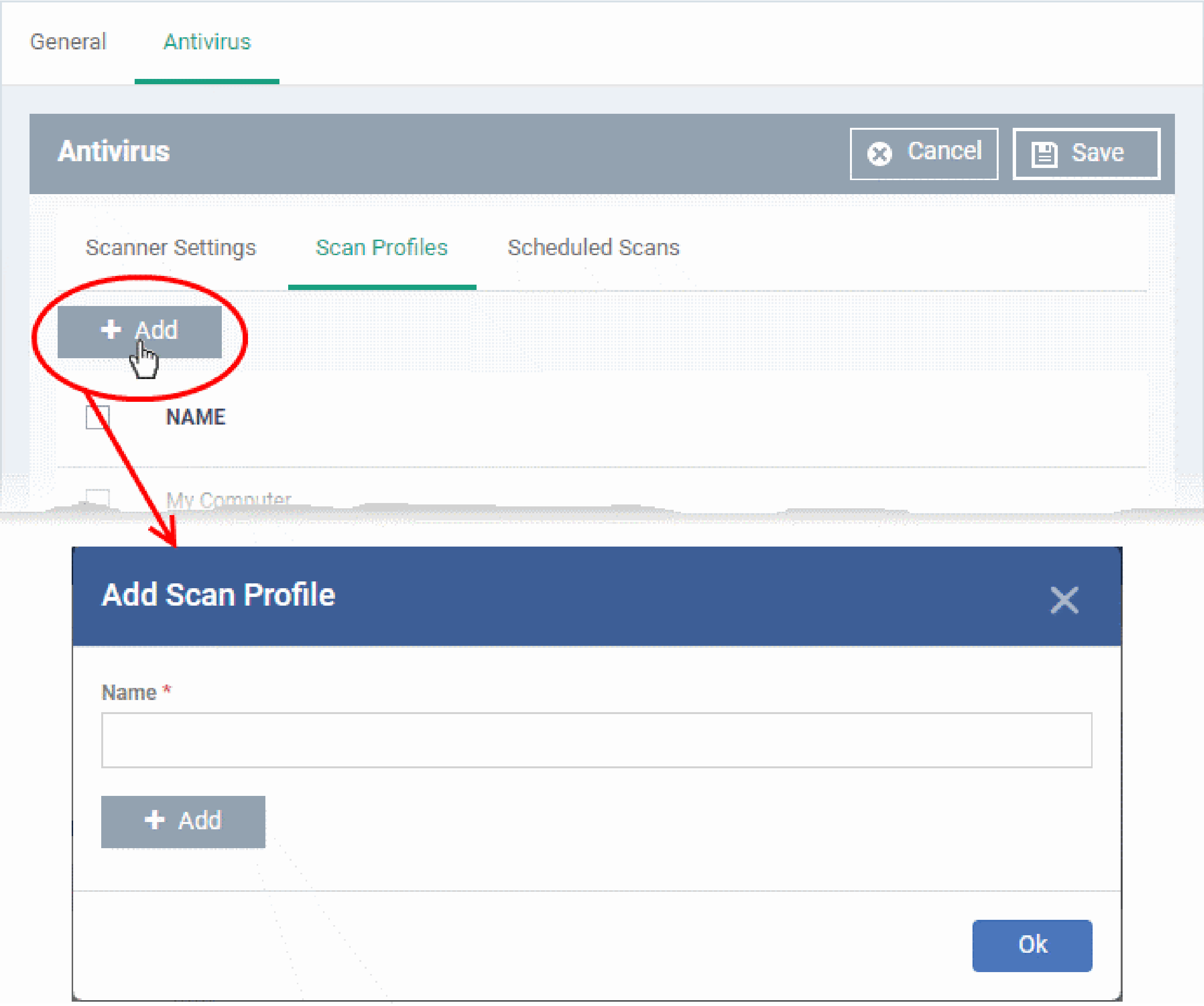


| □ | NAME |
|---|---|
| □ | My Computer |
| □ | Critical Areas |

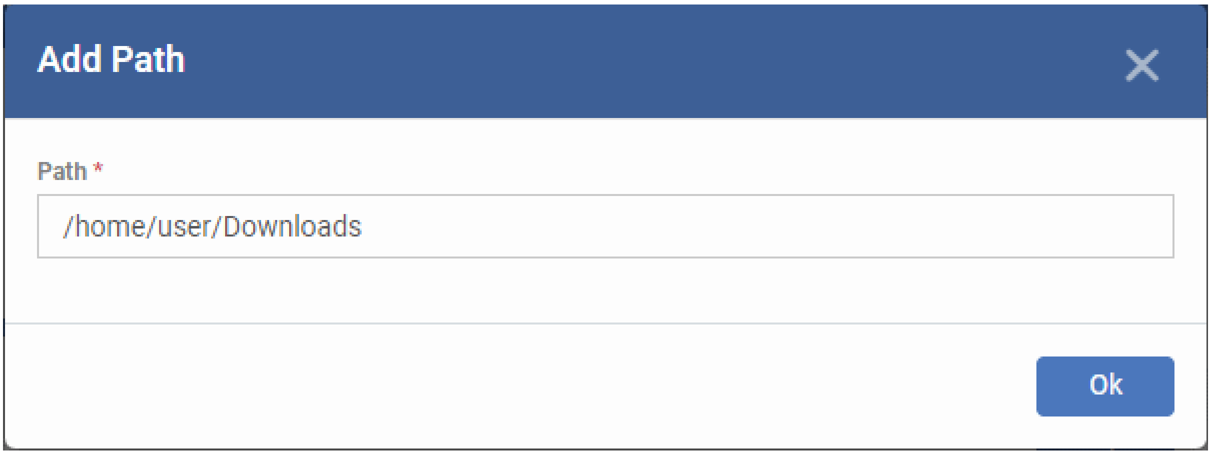
The list of pre-defined scan profiles will be displayed.

**Add a new scan profile**

- Click 'Add'



- Enter a name for the scan profile
- Click 'Add' to specify the locations to be scanned as per the custom profile

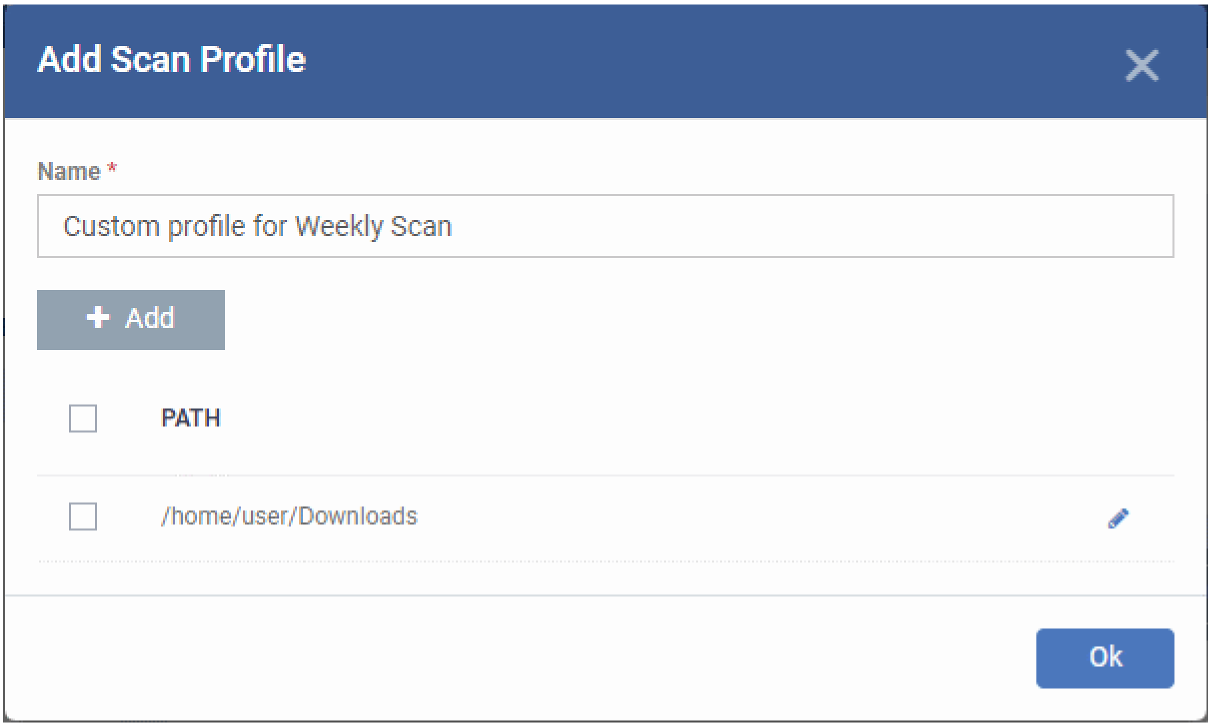


Path *

/home/user/Downloads

- Enter the path of the location to be scanned as per the custom profile and click 'Ok'

The path will be added to the profile.


Add Scan Profile

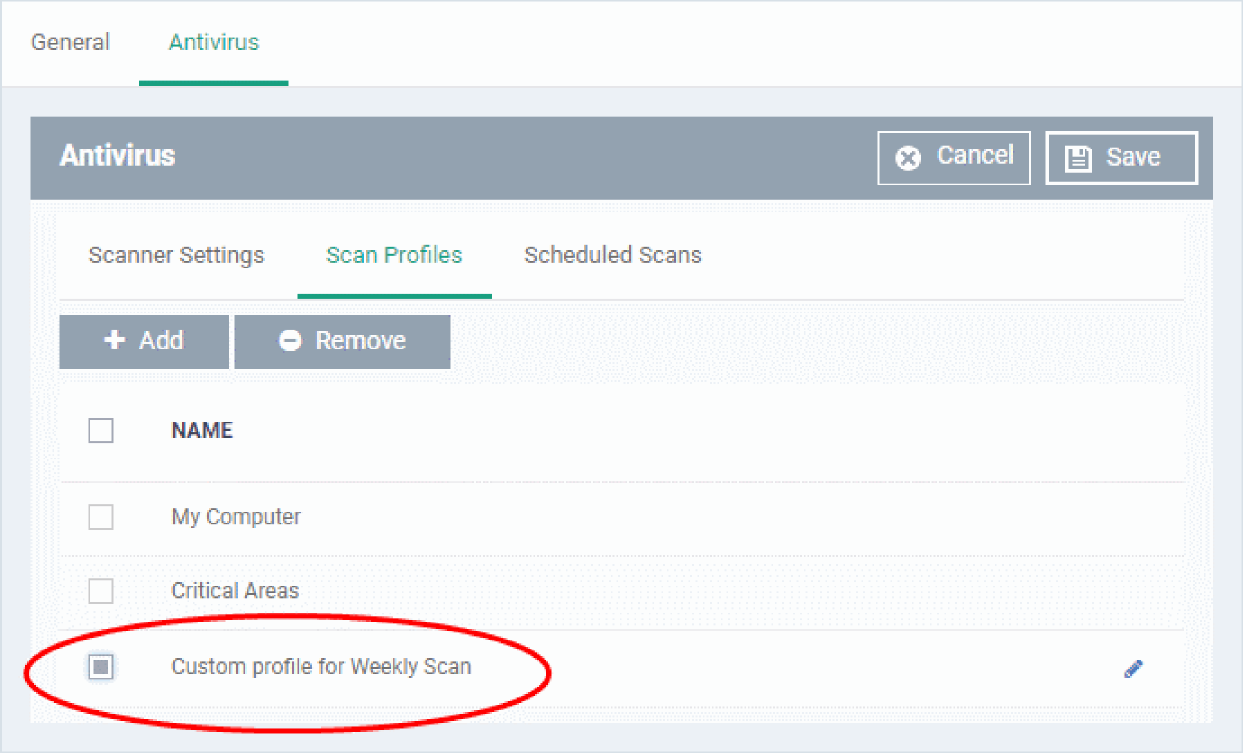
Name *

Custom profile for Weekly Scan

| □ | PATH |
|---|---|
| □ | /home/user/Downloads |

- To add more paths, click 'Add Path' and repeat the process
- To edit the path, click the pencil icon beside it
- Click 'Ok' in the 'Add Scan Profile' dialog.

- The profile will be added to the list of 'Scan Profiles'.



| □ | NAME |
|---|---|
| □ | My Computer |
| □ | Critical Areas |
| ■ | Custom profile for Weekly Scan |

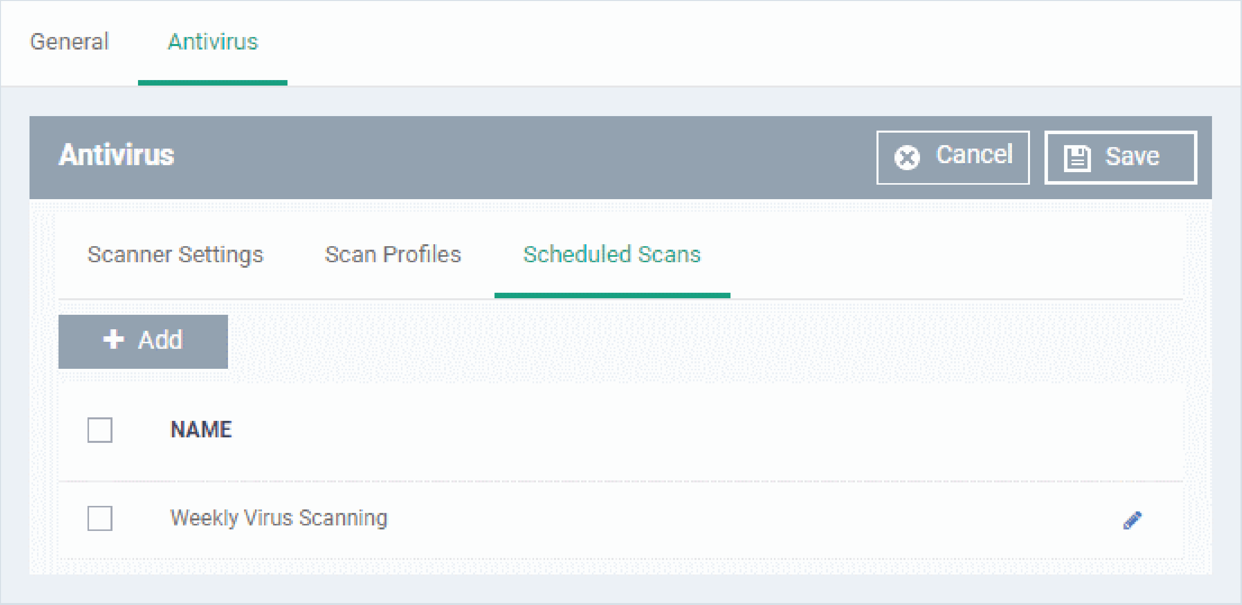
The custom profile will be added to the list.

- To add more custom scan profiles, click 'Add' and repeat the process
- To edit a custom scan profile, click the pencil icon beside it

- To remove a custom scan profile, select it and click 'Remove'

## Create and Manage Scheduled Scans for the Profile

- Click the 'Scheduled Scans' tab under 'Antivirus'
- The highly customizable scan scheduler lets you timetable scans to be run on managed devices according to your preferences. CCS automatically starts scanning the entire system or the disks or folders contained in the scan profile selected for that scan.
- You can add any number of scheduled scans for a profile to run at a time that suits your preference. A scheduled scan may contain any scan profile of your choice.

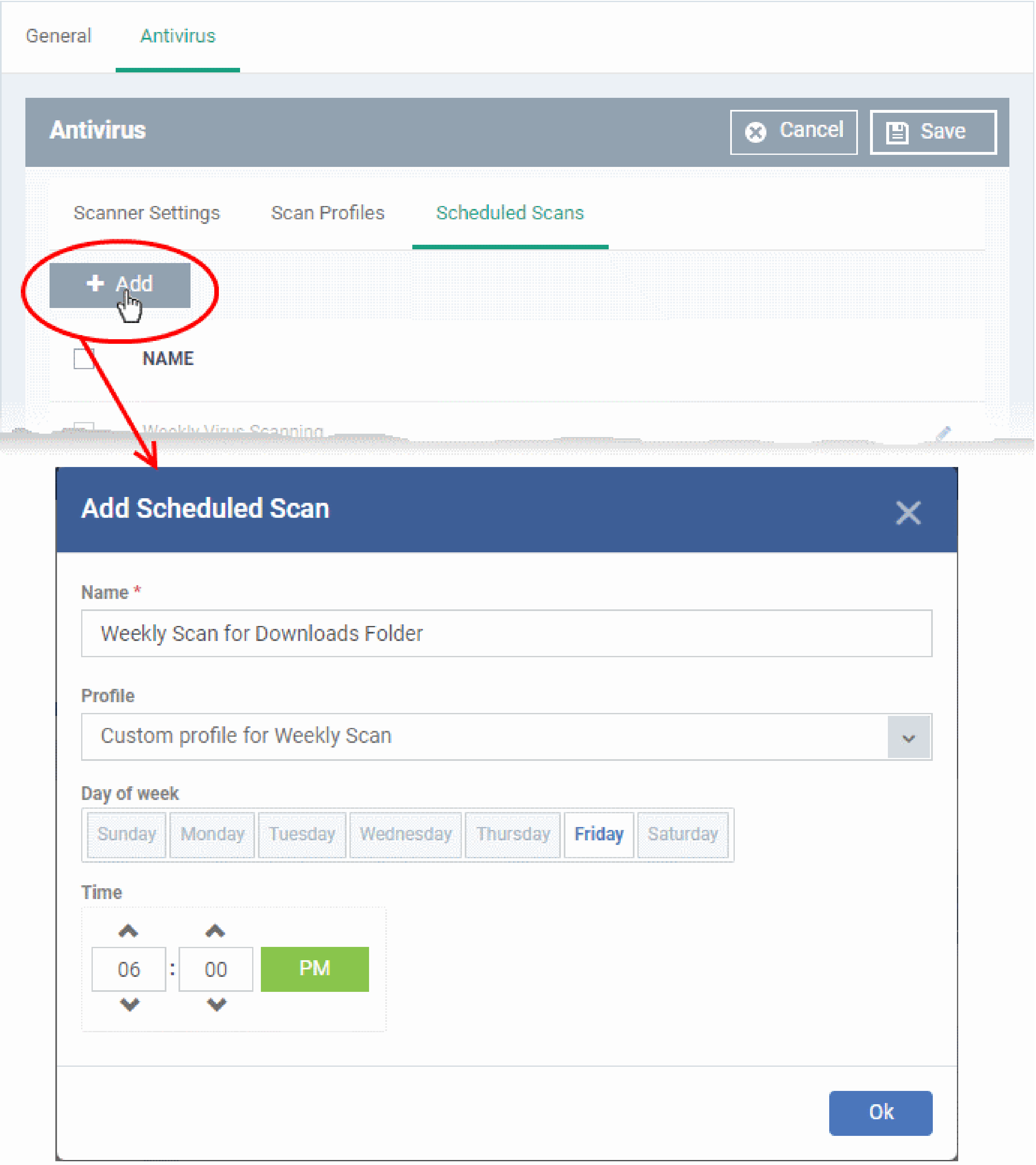


| □ | NAME |
|---|---|
| □ | Weekly Virus Scanning |

A list of pre-configured scheduled scans will be displayed.

**To add a new scheduled scan**

- Click 'Add'



Name *: Weekly Scan for Downloads Folder

Profile: Custom profile for Weekly Scan

Day of week: Friday

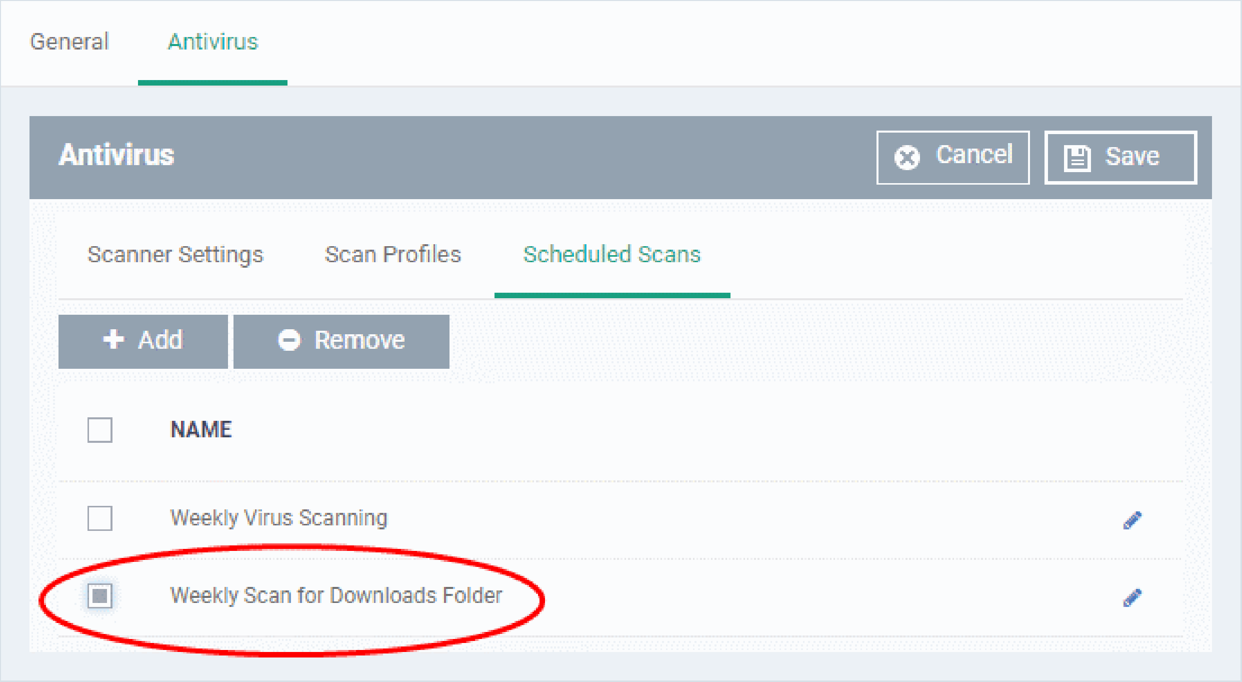
Time: 06 : 00 PM

| Add Scheduled Scan - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text box | Label for the scheduled scan |
| Profile | Drop-down | Choose the pre-defined or custom scan profile to be applied for the scheduled scan. The scan profiles included under the 'Scan Profiles' tab will be available in the drop-down. |
| Day of the Week | Buttons | Select the day(s) of the week on which the scan has to run |
| Time | HH:MM drop- | Set the time at which the scans are to run on the selected |

| Add Scheduled Scan - Table of Parameters | | |
|---|---|---|
| | down combo boxes | days. |

- Click 'Ok'

The scheduled scan will be added to the list.



- To add more scheduled scans to the configuration profile, click 'Add' and repeat the process
- To edit the settings of a scheduled scan, click the pencil icon ✎ beside it
- To remove a scheduled scan, select it and click 'Remove'

- Click 'Save' on the top right for your settings to take effect for the profile.

The settings will be saved and displayed under the 'Antivirus' tab. You can edit the settings or remove the section at anytime. See **Edit Configuration Profiles** for more details.

### 6.1.5.1.2. Communication Client and Comodo Client - Security Application Update Settings for Linux Profile

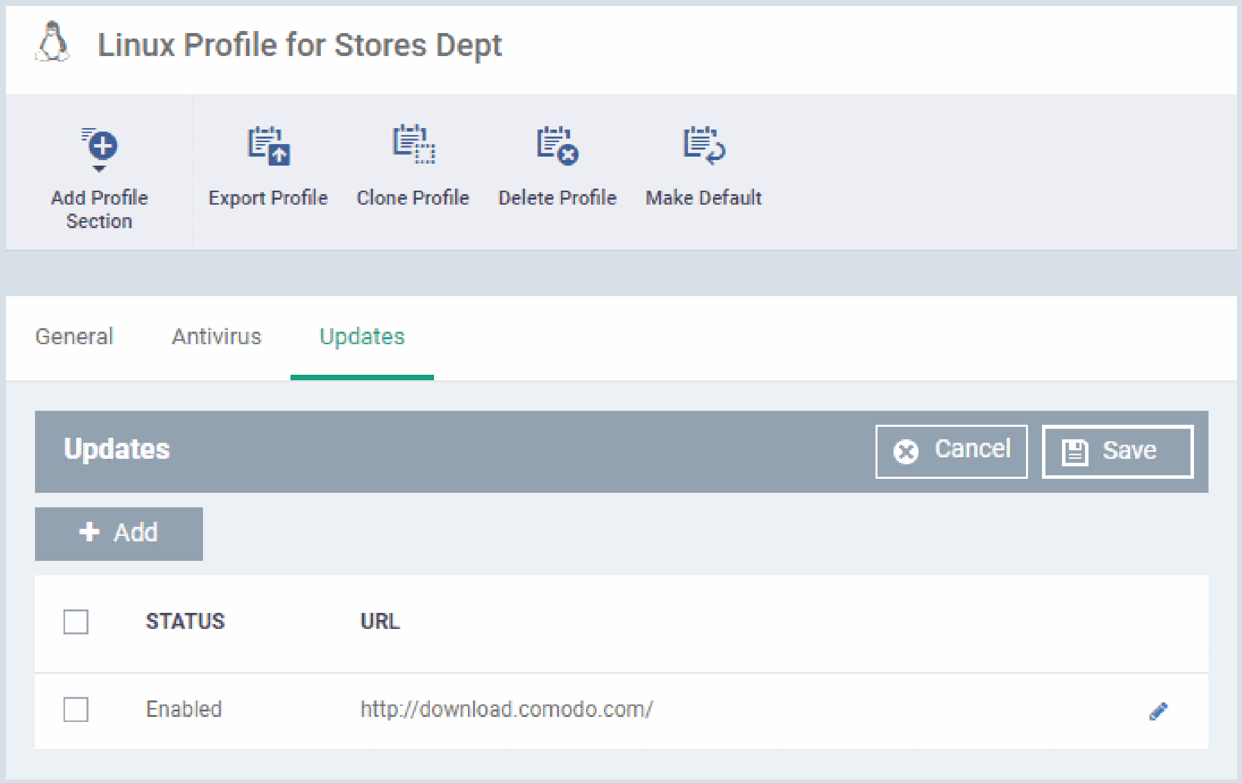
This section lets you enable or disable automatic updates and specify an alternate host from which endpoints should collect updates. By default, updates are downloaded from **https://download.comodo.com**.

**Configure updates settings in a Linux profile**

- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Linux profile
- Click 'Add Profile Section' then 'Updates' (if you haven't yet added the 'Updates' section)

  OR
- Open the 'Updates' tab and click 'Edit' if it was already added

The 'Updates' settings screen will open:



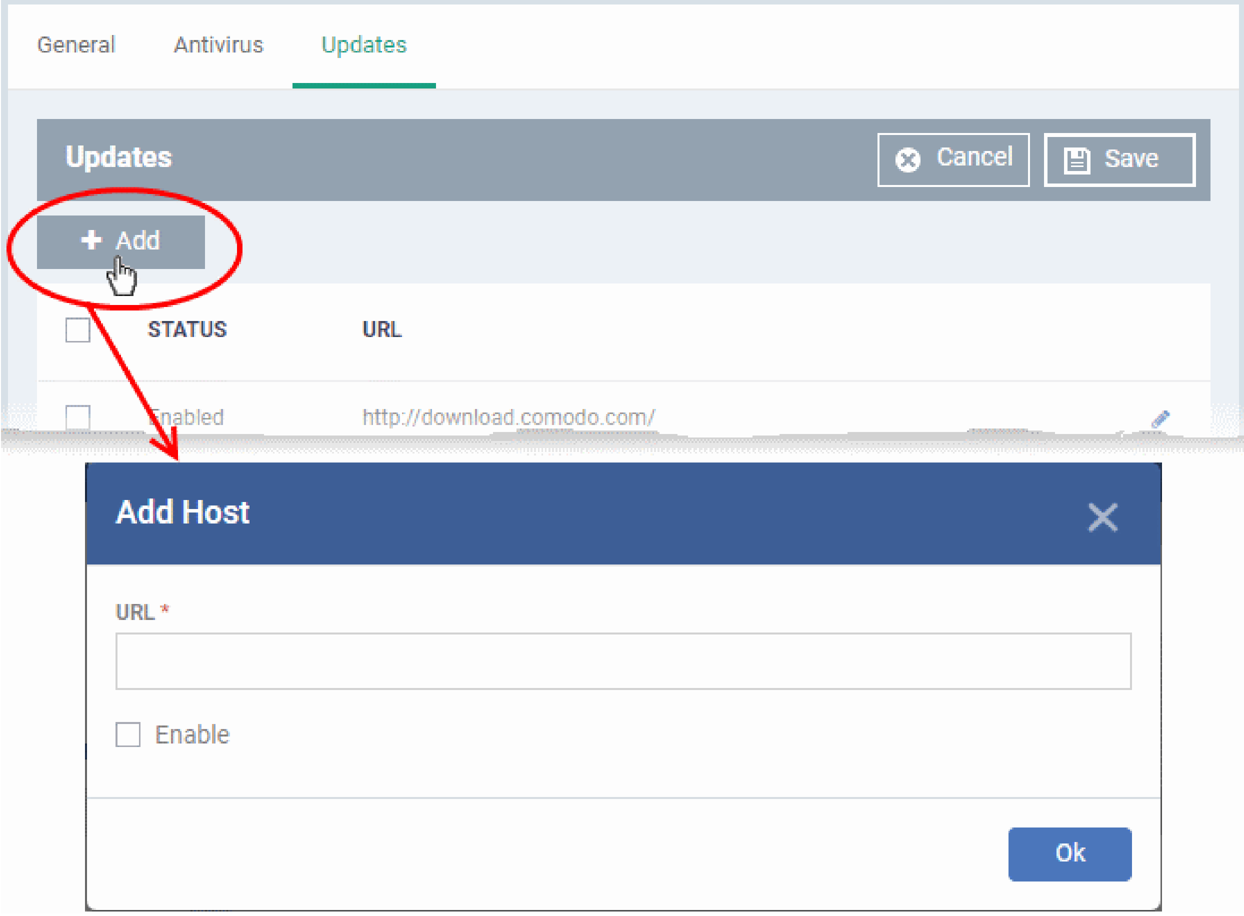
| □ | STATUS | URL |
|---|---|---|
| □ | Enabled | http://download.comodo.com/ |

- Use the checkbox beside 'Enabled' to enable or disable downloading updates from the URL specified beside it.

You can add the URL of an alternative download host if required. For example, you may want to distribute the updates from a local server to conserve bandwidth.

**To add a host in the local network**

- Click 'Add'



- Enter the URL or IP of the host from which updates should be downloaded in the 'URL' field
- Select the 'Enable' to activate the host
- Click 'Ok' to apply your changes
- Repeat the process to add multiple hosts.

- To edit a host, click the pencil icon ✎ beside the host name in the list
- Click 'Save' for your settings to take effect in the profile

### 6.1.5.1.3. User Interface Settings for Linux Profile

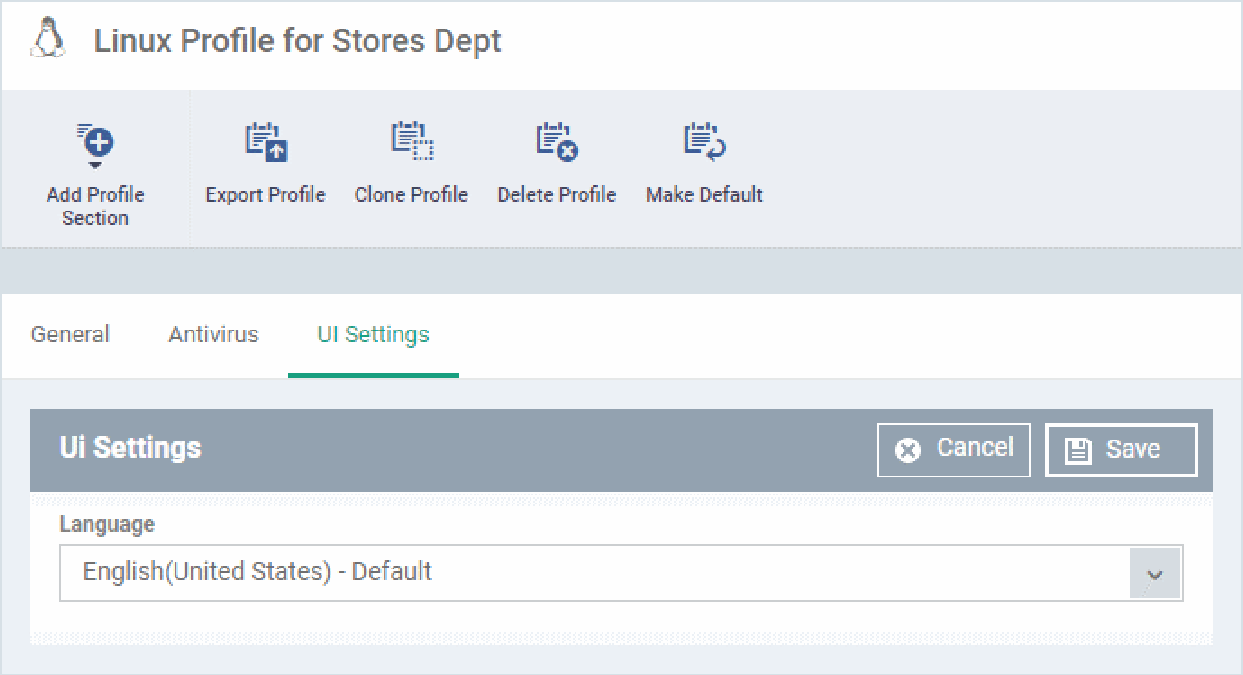
The 'UI Settings' section lets you choose the interface language for the CCS application on the endpoint.

#### Configure Language Settings in a Linux Profile

- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Linux profile
- Click 'Add Profile Section' then 'UI Settings' (if you haven't yet added the 'UI Settings' section)

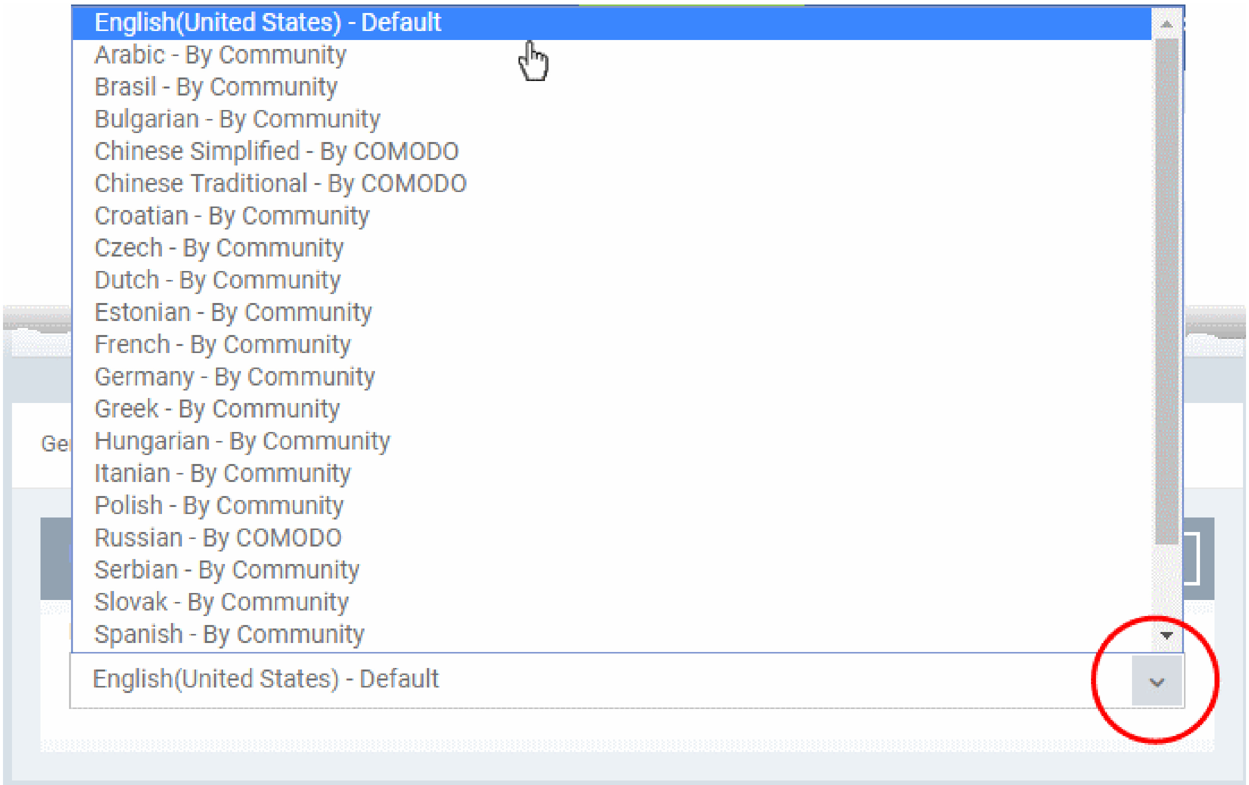
  OR
- Open the 'UI Settings' tab and click 'Edit' if it was already added

The 'UI Settings' screen will open:



Language: English(United States) - Default

- Select the language which should be used in the Comodo Client Security interface from the Language drop-down. (***Default = English (United States)***)



English(United States) - Default
Arabic - By Community
Brasil - By Community
Bulgarian - By Community
Chinese Simplified - By COMODO
Chinese Traditional - By COMODO
Croatian - By Community
Czech - By Community
Dutch - By Community
Estonian - By Community
French - By Community
Germany - By Community
Greek - By Community
Hungarian - By Community
Itanian - By Community
Polish - By Community
Russian - By COMODO
Serbian - By Community
Slovak - By Community
Spanish - By Community

- Click 'Save' to apply your changes to the profile.

### 6.1.5.1.4. Logging Settings for Linux Profile

- The 'Logging' area lets you specify how logs should be collected in CCS

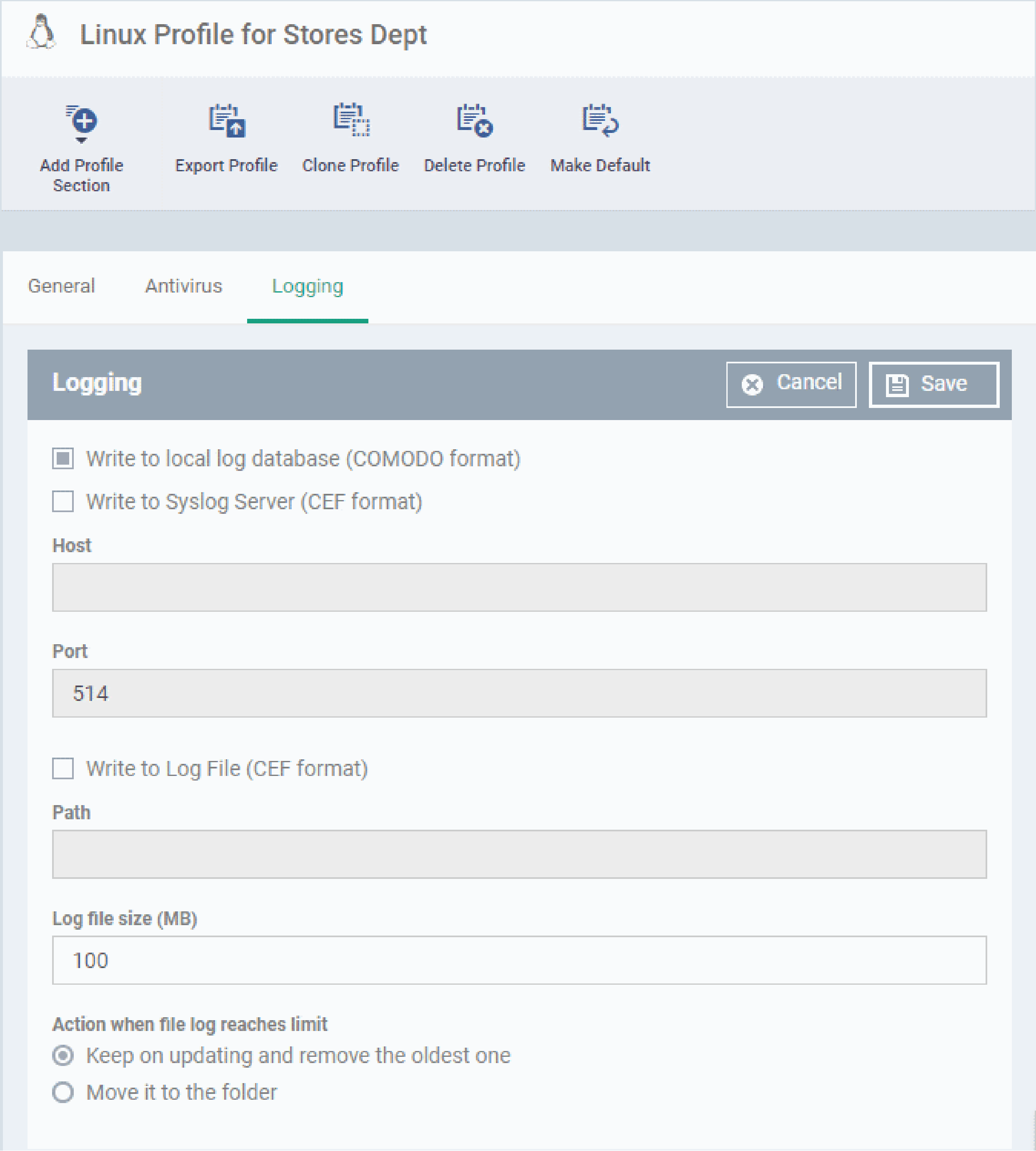
- For example, you can choose max. log size, log format and location, and extended log options.

## Configure 'Logging' Settings in a Linux Profile

- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Linux profile
- Click 'Add Profile Section' then 'Logging Settings' (if you haven't yet added the 'Logging' section)

  OR
- Open the 'Logging' tab and click 'Edit' if it was already added

The 'Logging' settings screen will open:



☑ Write to local log database (COMODO format)

□ Write to Syslog Server (CEF format)

Host

Port: 514

□ Write to Log File (CEF format)

Path

Log file size (MB): 100

Action when file log reaches limit

● Keep on updating and remove the oldest one

○ Move it to the folder

| Logging Settings - Form Parameters | |
|---|---|
| **Parameters** | **Description** |
| Write to Local Log Database (COMODO Format) | The log is saved in native Comodo format on the local endpoint. |
| Write to Syslog Server | Endpoint Manager log events are written to a remote syslog server. If enabled you have to specify the hostname/IP address and port number settings for the server. |
| Host * | The host name or IP address of the syslog server. |
| Port * | The port number of the syslog server. |
| Write to Log File (CEF Format) | Logs are saved locally on the endpoint in Common Event Format (CEF) file format. If enabled, please specify the location of the CEF file. |
| Path | Enter the location of the CEF file. |
| Log file size (MB) | Specify the maximum size of the log file (default = 100 MB). |
| Action when file log size reaches limit: | Specify behavior when the log file reaches the max. size. |
| Keep on updating it removing the oldest records | Once the log file reaches the maximum size, the file will be appended with the new log entries and the oldest entries will be deleted. |
| Move it to | Move and save the log file when it reaches the maximum size. |
| The path to the folder for old log files * | If 'Move it to' is enabled, type a destination path for the log file. |

Fields marked * are mandatory.

- Click the 'Save' button to apply your changes.

### 6.1.5.1.5. Clients Access Control Settings for Linux Profile

- Access control lets you password-protect the antivirus settings area on Comodo Client Security on managed endpoints.
- Once set, users will need to enter a password to access the antivirus settings area ('Antivirus' > 'Scanner Settings').
- This stops users from opening the clients locally and making potentially dangerous changes. Without password protection, any user can modify AV settings and options.
- Users can still run some simple tasks without the password, including on-demand scans and database updates.

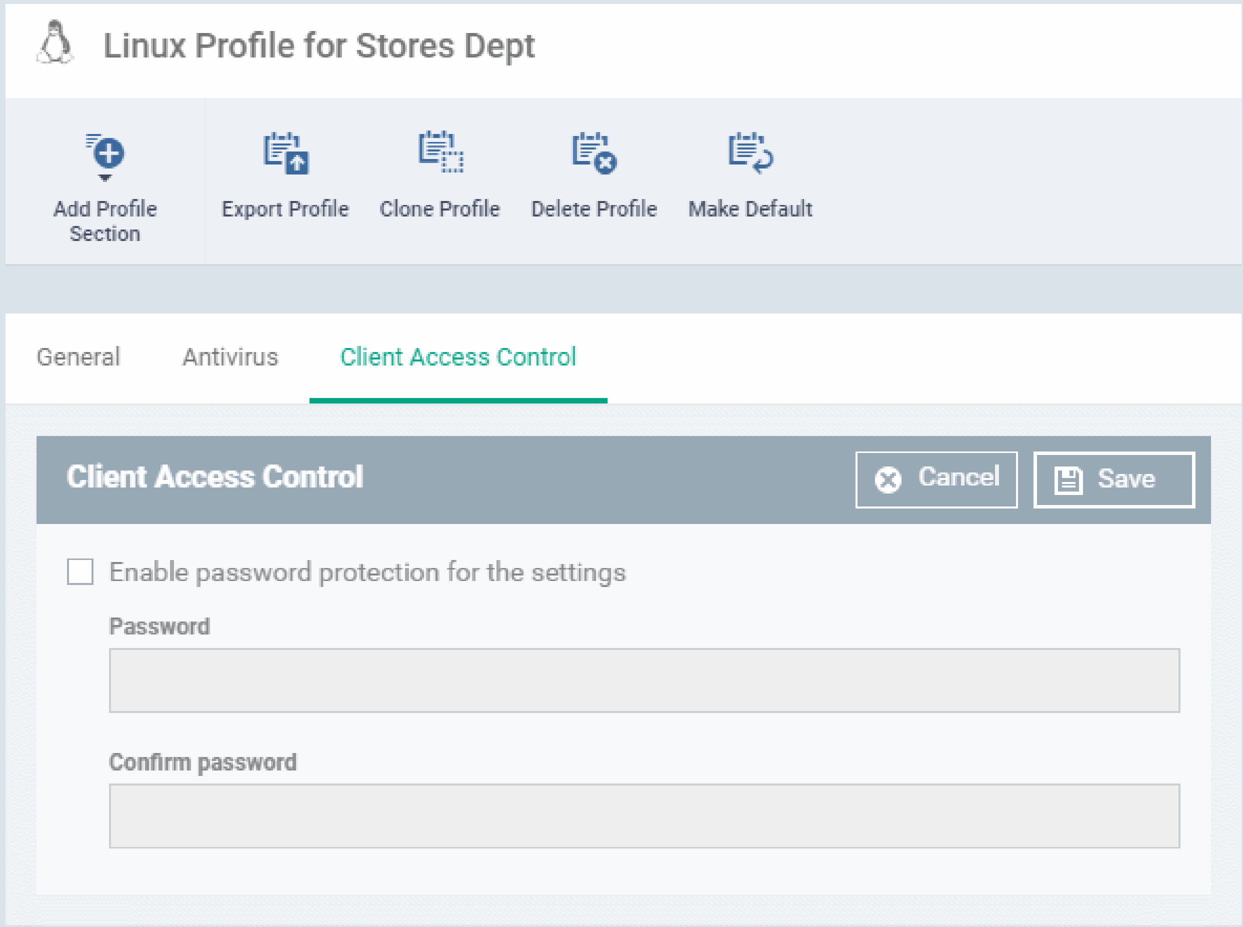
**Implement access control**

- Click 'Configuration Templates' > 'Profiles'
- Click on the name of a Linux profile
- Click 'Add Profile Section' then 'Client Access Control' (if you haven't yet added the section)

  OR

- Open the 'Client Access Control' tab and click 'Edit' if it was already added

The 'Client Access Control' settings screen will open:



□ Enable password protection for the settings

Password

Confirm password

- **Enable password protection for the settings -** Make users enter a password before they can access the AV settings area in the CCS interface.
  - Enter and confirm the password in the fields provided
  - Click 'Save' for your changes to take effect

### 6.1.5.1.6. Valkyrie Settings for Linux Profile

- Valkyrie is a cloud-based file verdict service that subjects unknown files to a range of tests in order to identify those that are malicious.
- Comodo Client Security for Linux can automatically submit unknown files to Valkyrie for analysis. When the tests are complete, Valkyrie will award a trust verdict to the file.
  - Note - 'Cloud Scanning' should be enabled in Antivirus section of CCS for Linux on the endpoints.
- The verdicts can be viewed in 'Security Sub-Systems' > 'Valkyrie' interface.
  - See **View list of Valkyrie Analyzed Files** for more details.
- Click 'Dashboard' > 'Valkyrie' to view summary of all Valkyrie results.

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

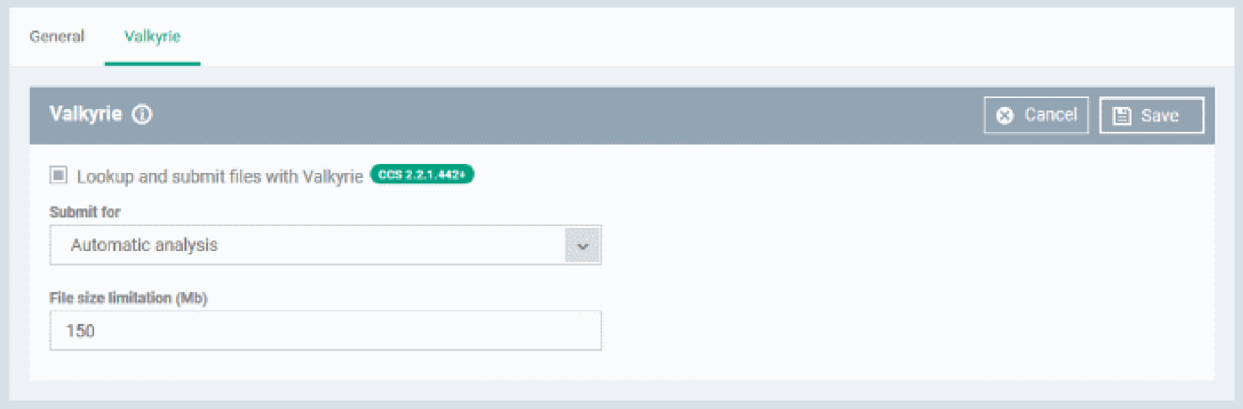
You can configure Valkyrie and create an analysis schedule by adding a 'Valkyrie' section to a profile.

### Configure Valkyrie Settings

- Click 'Configuration Templates' > 'Profiles'
- Open the Linux profile that you want to work on
- Click 'Add Profile Section'
- Select 'Valkyrie' from the menu

The 'Valkyrie' settings screen will open.

- Click 'Edit'



□ Lookup and submit files with Valkyrie CCS 2.2.1.442+

Submit for: Automatic analysis

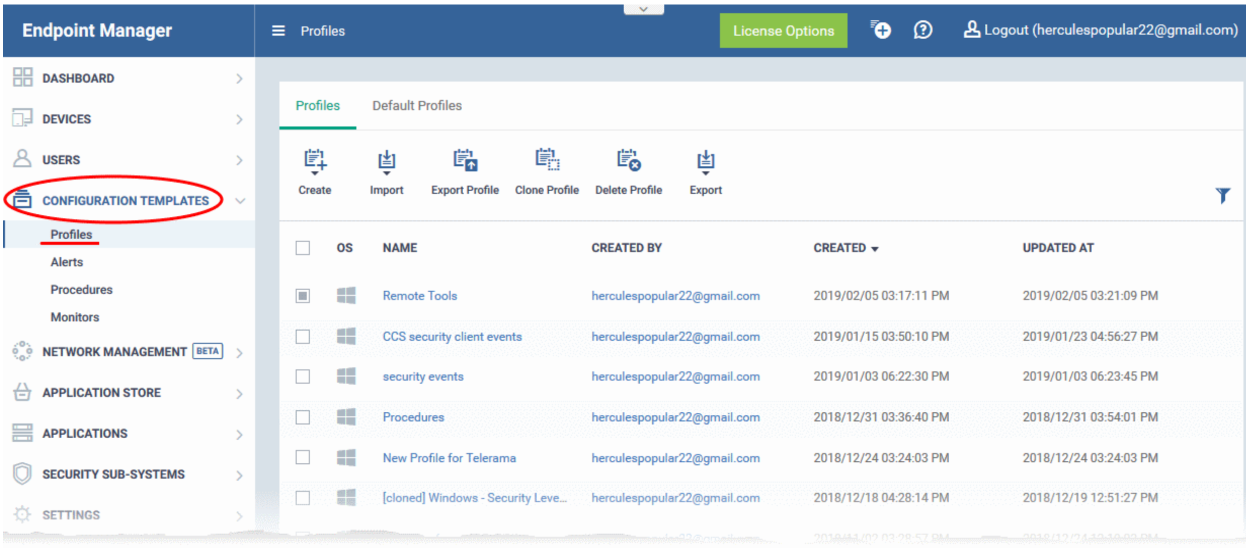
File size limitation (Mb): 150

| Valkyrie Settings for Linux Profile - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Lookup and submit files with Valkyrie | Choose this option if you want the files to be submitted to the cloud file lookup service |
| 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. |
| File size limitations (MB) | Specify the maximum file size for upload to Valkyrie. The default value is 150 MB. |

- Click 'Save'

## 6.2. View and Manage Profiles

- Click 'Configuration Templates' > 'Profiles' to open this interface
- The 'Profiles' screen shows all available configuration profiles for Android, iOS, Mac OS, Windows and Linux devices.
- You can create, deploy, import/export, and clone profiles from this interface.



| OS | NAME | CREATED BY | CREATED | UPDATED AT |
|---|---|---|---|---|
| | Remote Tools | herculespopular22@gmail.com | 2019/02/05 03:17:11 PM | 2019/02/05 03:21:09 PM |
| | CCS security client events | herculespopular22@gmail.com | 2019/01/15 03:50:10 PM | 2019/01/23 04:56:27 PM |
| | security events | herculespopular22@gmail.com | 2019/01/03 06:22:30 PM | 2019/01/03 06:23:45 PM |
| | Procedures | herculespopular22@gmail.com | 2018/12/31 03:36:40 PM | 2018/12/31 03:54:01 PM |
| | New Profile for Telerama | herculespopular22@gmail.com | 2018/12/24 03:24:03 PM | 2018/12/24 03:24:03 PM |
| | [cloned] Windows - Security Leve... | herculespopular22@gmail.com | 2018/12/18 04:28:14 PM | 2018/12/19 12:51:27 PM |

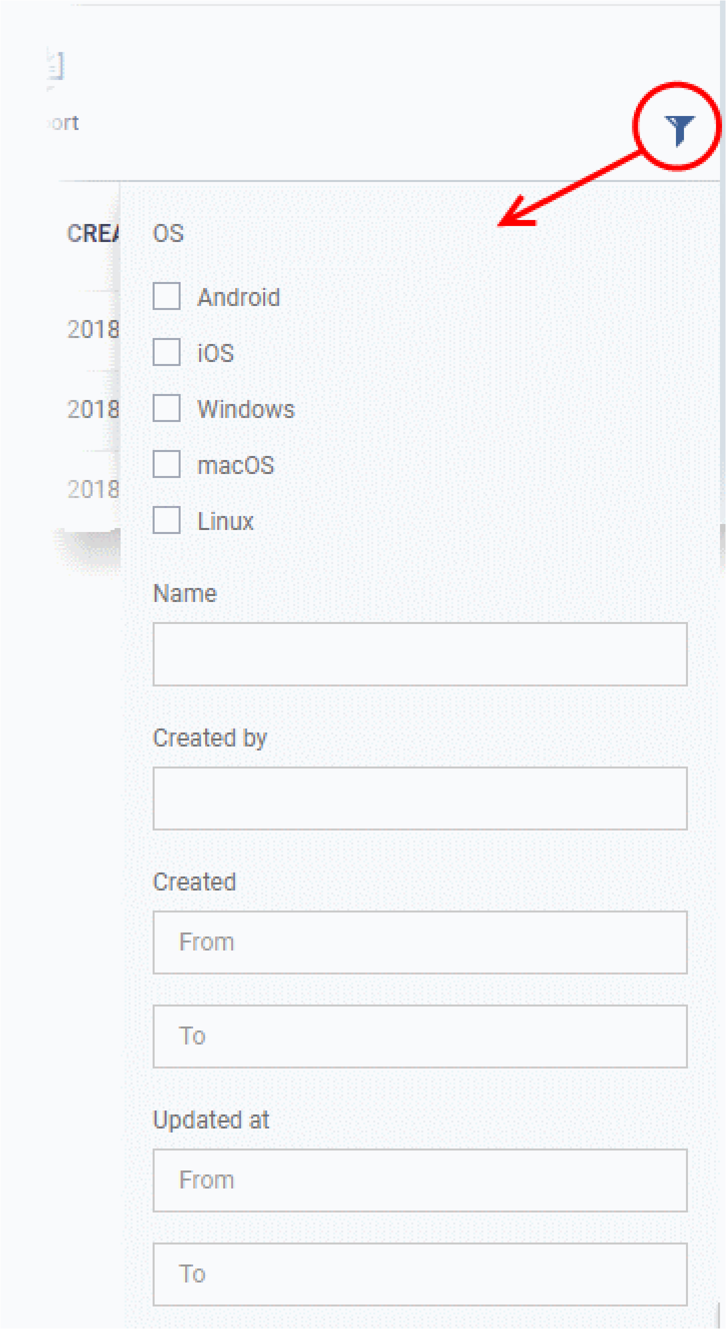
The interface has two tabs:

- Profiles - A list of all profiles added to Endpoint Manager.
- Default Profiles - A default profile is one that is automatically applied to any device that matches its operating system. See **Manage Default Profiles** for more details.

| The 'Profiles' interface | | |
|---|---|---|
| **Column** | | **Description** |
| OS | | The operating system that the profile supports. |
| Name | | Label of the profile.<br>• Click the profile name to open the profile settings and configuration interface. See **Edit Configuration Profiles** for more details. |
| Created by | | The administrator who created the profile.<br>• Click the name of an administrator to view their user details. See **View the details of the User** for more details. |
| Created | | The date and time at which the profile was created. |
| Updated at | | The date and time at which the profile was last updated. |
| **Controls** | | |
| Create | Create Android profile | Add a new Android profile. See '**Profiles for Android Devices**' for more details. |
| | Create iOS profile | Add a new iOS profile. See '**Profiles for iOS Devices**' for more details. |
| | Create Mac OS profile | Add a new Mac OS profile. See '**Profiles for Mac OS Devices**' for more details. |
| | Create Windows profile | Add a new Windows profile. See '**Create Windows Profiles**' for more details. |
| | Create Linux profile | Add a new Linux profile. See '**Profiles for Linux Devices**' for more details. |
| Import | Import from Comodo Client Security Config file | Import the security configuration of CCS from a .cfg configuration file as a Windows profile. The configuration file will usually have been exported from a managed endpoint with CCS installed. See '**Import Windows Profiles**' for more details. |
| | Import from Exported Profile | Import a configuration profile from a previously exported and saved profile. See **Export and Import Configuration Profiles** for more details. |
| Clone Profile | | Create a new profile by cloning an existing profile and modifying its settings as required. See **Clone a Profile** for more details. |
| Export profile | | Export the selected configuration as a .cfg file and save it for future implementation. See **Export and Import Configuration Profiles** for more details.<br>The control will appear only if a single profile is selected from the list. |
| Delete profile | | Remove selected profile(s).<br>The control will appear only if one or more profiles are selected. |
| Export | | Save the list of profiles as a comma separated values (CSV) file. See **Export the List of Profiles** for more details. |

## Sorting, Search and Filter Options

- Click any column header to sort items in ascending/descending order
- Click the funnel icon to filter profiles by various criteria:



OS

□ Android
□ iOS
□ Windows
□ macOS
□ Linux

Name

Created by

Created

From

To

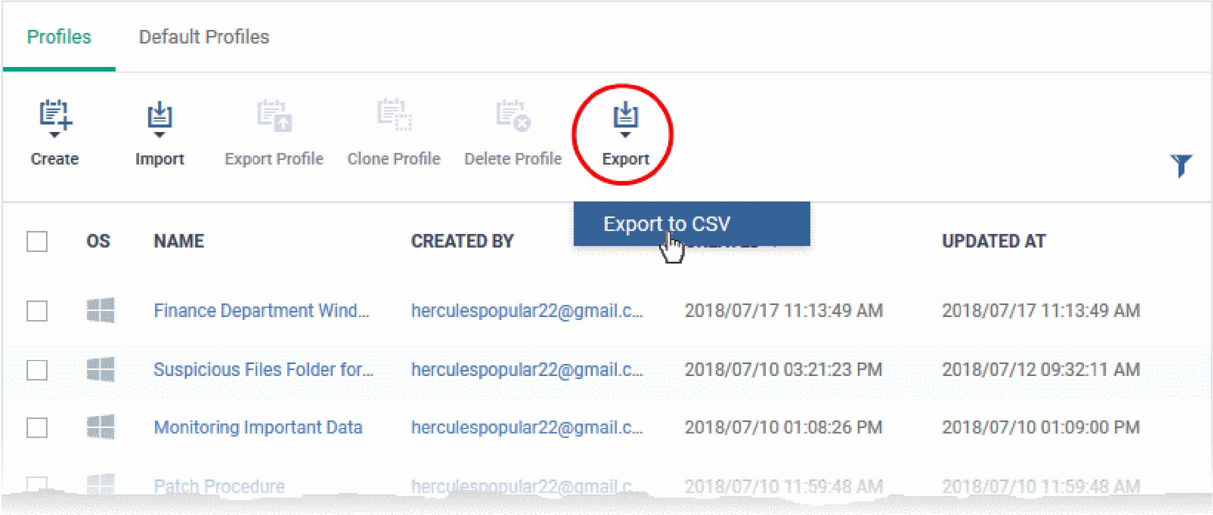
Updated at

From

To

## Export the List of Profiles

- Click 'Configuration Templates' > 'Profiles'
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | OS | NAME | CREATED BY | | UPDATED AT |
|---|---|---|---|---|---|
| □ | | Finance Department Wind... | herculespopular22@gmail.c... | 2018/07/17 11:13:49 AM | 2018/07/17 11:13:49 AM |
| □ | | Suspicious Files Folder for... | herculespopular22@gmail.c... | 2018/07/10 03:21:23 PM | 2018/07/12 09:32:11 AM |
| □ | | Monitoring Important Data | herculespopular22@gmail.c... | 2018/07/10 01:08:26 PM | 2018/07/10 01:09:00 PM |
| □ | | Patch Procedure | herculespopular22@gmail.c... | 2018/07/10 11:59:48 AM | 2018/07/10 11:59:48 AM |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

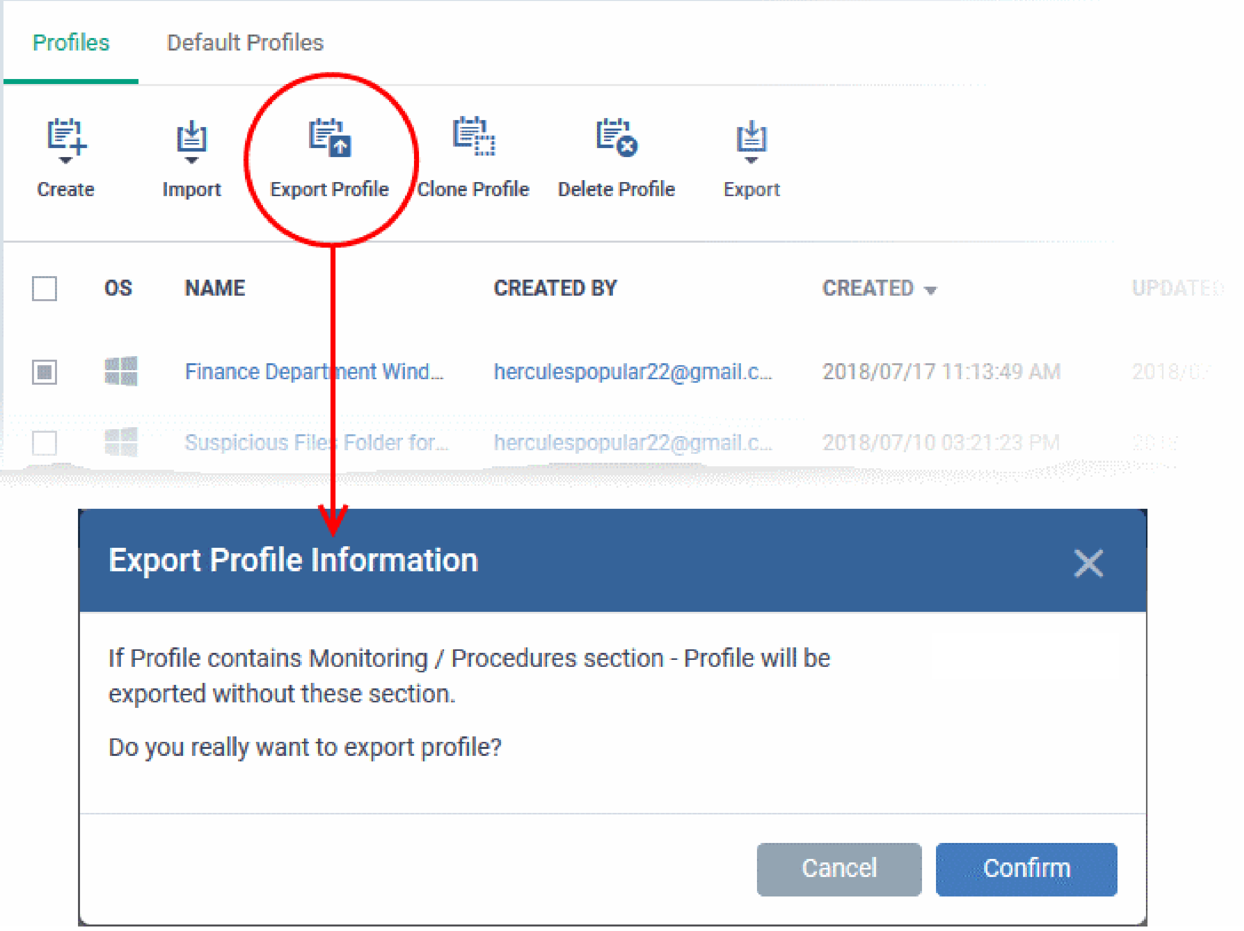
## 6.2.1. Export and Import Configuration Profiles

You can export and import profiles for re-deployment to other devices and groups.

**Note**: 'Monitor Settings' and 'Procedure Settings' are not included in exported profiles. You will need to reconfigure these sections before deploying, if you require them.

**Export a profile**

- Click 'Configuration Templates' > 'Profiles'
- Select the 'Profiles' tab.
- Select the profile you want to export then click the 'Export profile' button:



If Profile contains Monitoring / Procedures section - Profile will be exported without these section.

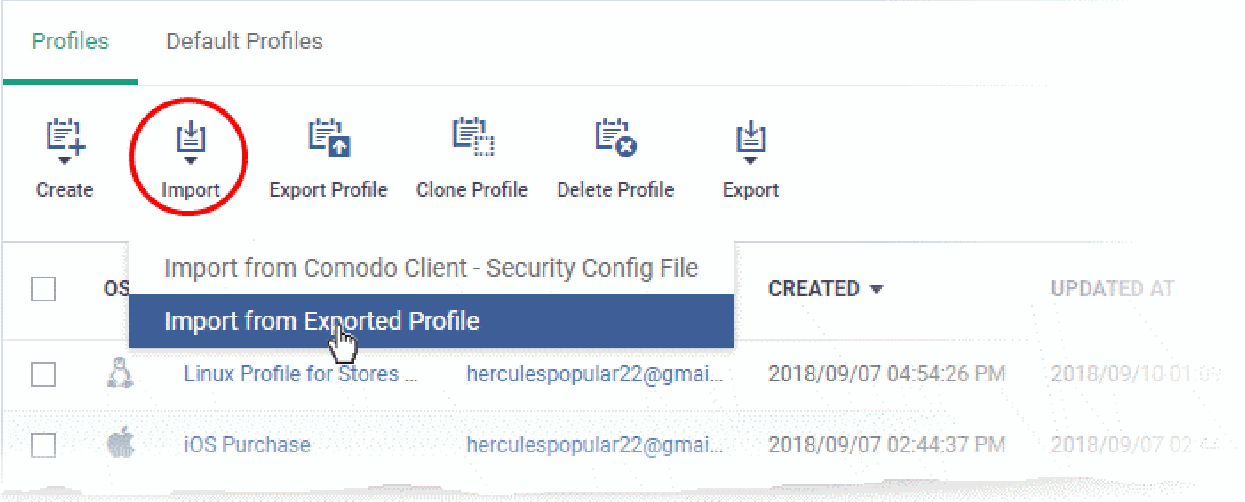
Do you really want to export profile?

You will see a prompt stating that the monitoring and procedures sections will be omitted from exported profiles.

- Click 'Confirm' to export the profiles to .cfg file
- Exported files can be imported back into Endpoint Manager as a profile at any time.

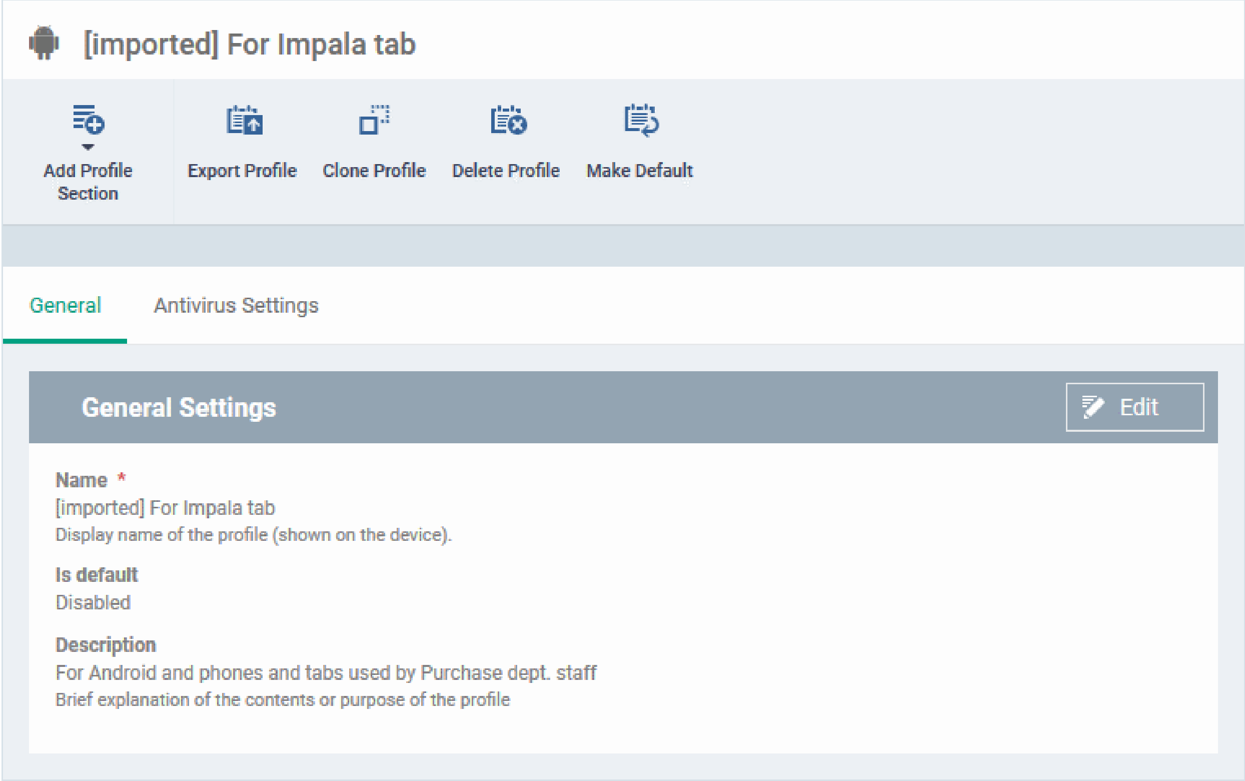
**Import a profile from a saved .cfg file**

- Open the 'Profiles' interface by clicking 'Configuration Template' from the left and choosing 'Profiles' from the options.



- Click 'Import' > 'Import from Exported Profile'.
- Navigate to the location in your computer where the .cfg file is stored, select the file and click 'Open'.

- The 'Profile' interface will open, with the prefix [Imported] in the file name and security components pre-configured as per the source profile.



Name *
[imported] For Impala tab
Display name of the profile (shown on the device).

Is default
Disabled

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

The imported profile is not set as a 'Default Profile' by default.

- Click the 'Edit' button in 'General Settings' to change the profile name and/or make it a default profile.
- Click 'Add Profile Section' to add a new component
- Click the name of an existing component name to view/edit its settings

See the following sections for help with profiles:

**Profiles for Android Devices**

**Profiles for iOS Devices**

**Profiles for Mac OS Devices**

**Profiles for Windows Devices**.

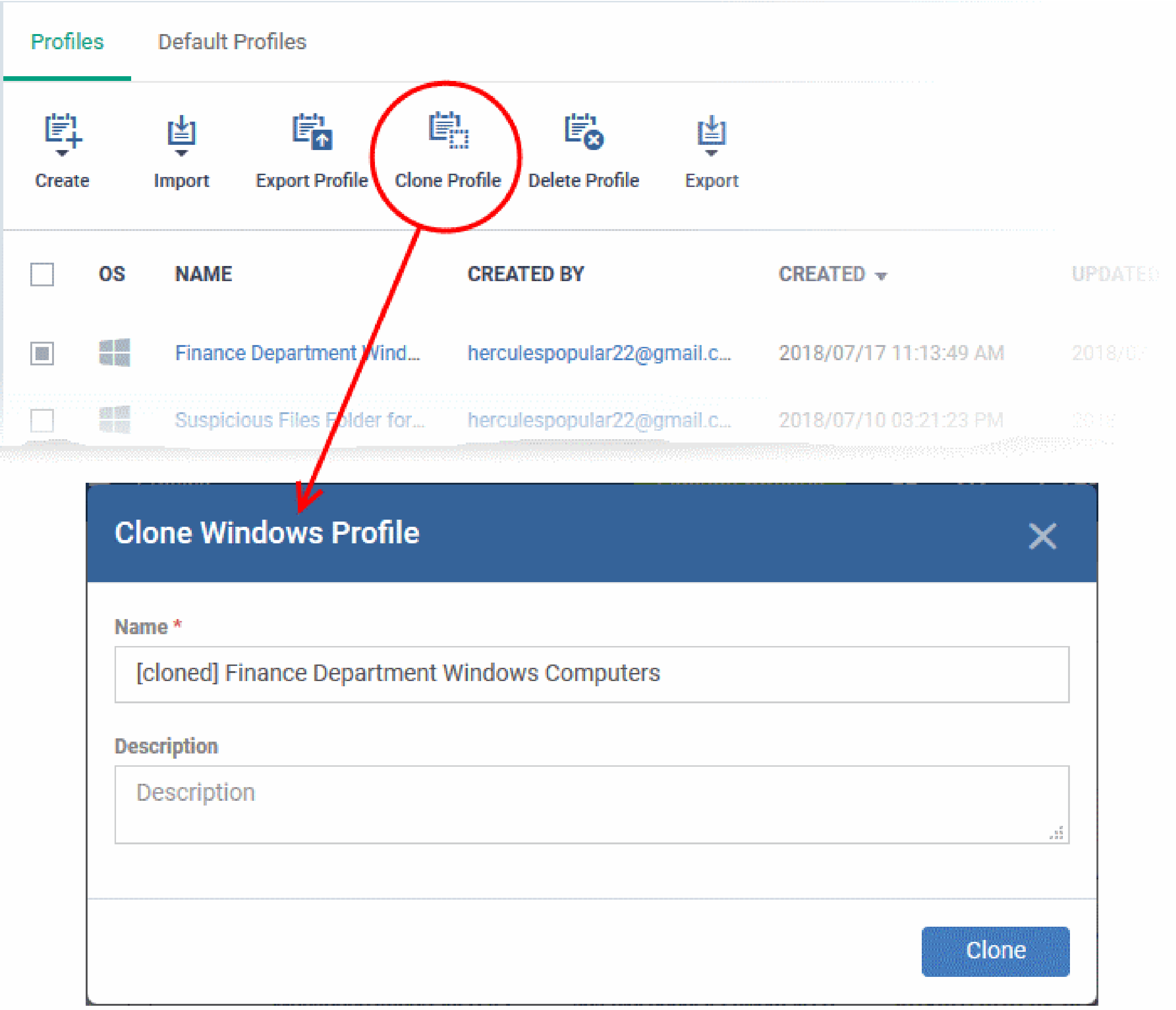
**Profiles for Linux Devices**

## 6.2.2. Clone a Profile

- Cloning then modifying a profile is an easy way to set up a new profile with custom settings.
- You can edit the cloned profile according to the requirements of your target devices or group.

**To clone a profile**

- Click 'Configuration Templates' > 'Profiles'
- Select the 'Profiles' tab.
- Click on the name of the profile you want to clone.
- Click 'Clone Profile' in the profile details page
  - Alternatively, select the profile in the 'Profiles' interface and click 'Clone Profile' at the top.



| ☐ | OS | NAME | CREATED BY | CREATED | UPDATED |
|---|---|---|---|---|---|
| ☒ | | Finance Department Wind... | herculespopular22@gmail.c... | 2018/07/17 11:13:49 AM | 2018/0... |
| ☐ | | Suspicious Files Folder for... | herculespopular22@gmail.c... | 2018/07/10 03:21:23 PM | 2018 |

Clone Windows Profile

Name *: [cloned] Finance Department Windows Computers

Description: Description

The name of the new profile is the same as the source profile with the prefix [cloned].

- Enter a new name for the profile (if required) and a short description
- Click 'Clone'.

The new profile has identical settings to the source profile at this stage. To configure the profile:

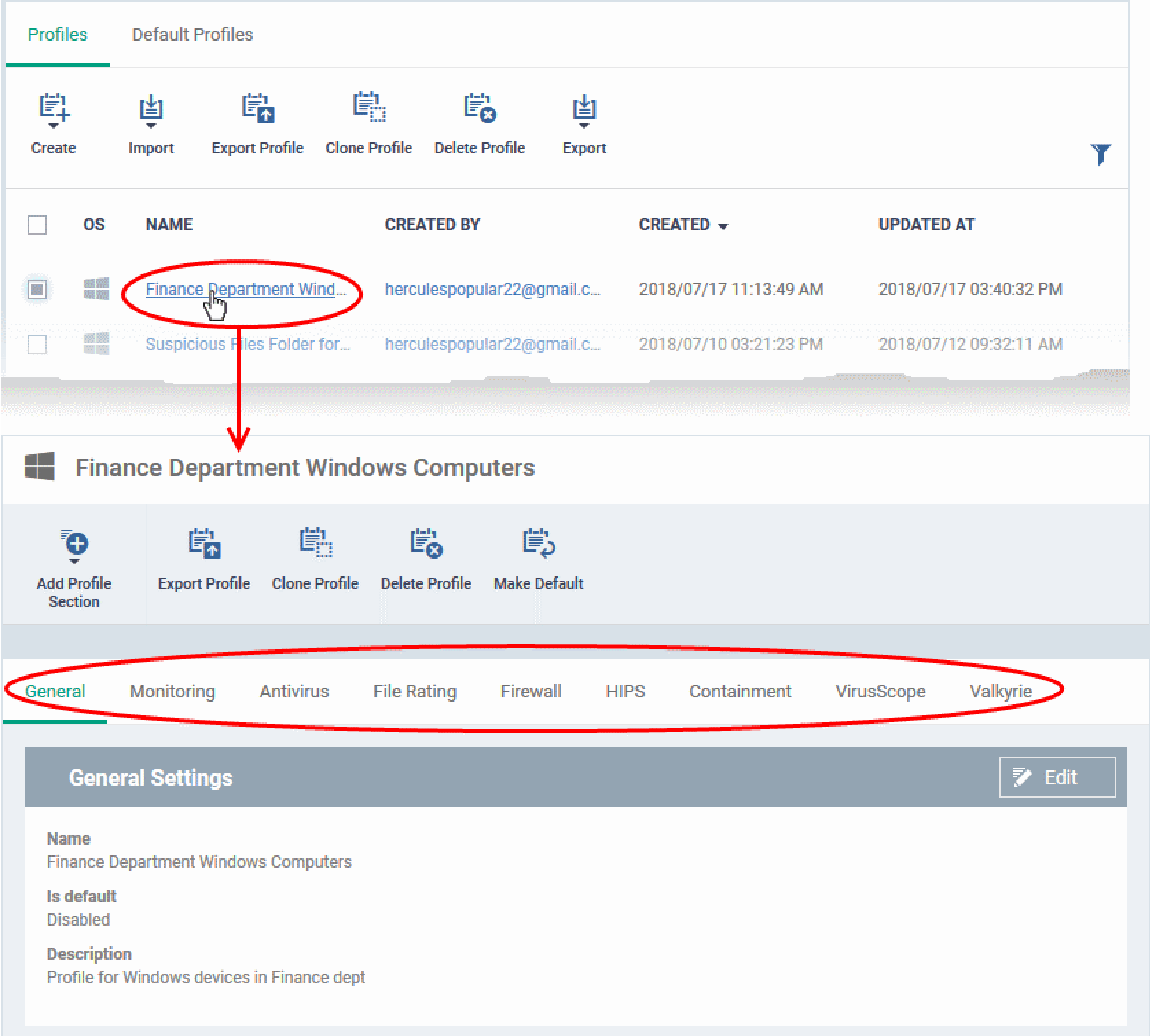
- Click 'Configuration Templates' > 'Profiles'
- Click on the name of the cloned profile
  - Click 'Add Profile Section' to configure settings that were not included in the original
  - Click a section name then 'Edit' to change existing settings. Each existing section is shown as a tab underneath the profile name
- For more details on the options available under each component, see the following sections for more details:
  - **Profiles for Android Devices**
  - **Profiles for iOS Devices**
  - **Profiles for Mac OS Devices**
  - **Profiles for Windows Devices**.
  - **Profiles for Linux Devices**

# 6.3. Edit Configuration Profiles

- You can edit an existing configuration profile to modify settings as required.
- For example, you might want to enable or disable certain security components or add a procedure to the profile.
- The updated profile is automatically deployed to endpoints after you save.

**Edit a profile**

- Click 'Configuration Templates' > 'Profiles'
- Select the 'Profiles' tab
- Click on the name of the profile that you want edit.
- This will open the profile details screen:



| ☐ | OS | NAME | CREATED BY | CREATED | UPDATED AT |
|---|---|---|---|---|---|
| ☒ | | Finance Department Wind... | herculespopular22@gmail.c... | 2018/07/17 11:13:49 AM | 2018/07/17 03:40:32 PM |
| ☐ | | Suspicious Files Folder for... | herculespopular22@gmail.c... | 2018/07/10 03:21:23 PM | 2018/07/12 09:32:11 AM |

Finance Department Windows Computers

Name
Finance Department Windows Computers

Is default
Disabled

Description
Profile for Windows devices in Finance dept

The tabs let you configure various Endpoint Manager modules. Click 'Add Profile Section' if you want to add a new module.

- Click the tab of the section you want to edit. For example, 'General', 'Monitoring', 'Antivirus', 'Firewall'.
- Some tabs let you directly edit the parameters. In others, you will need to click the 'Edit' button: Edit

  - See the following sections for in-depth help on the settings in a profile:

  - **Profiles for Android Devices**
  - **Profiles for iOS Devices**
  - **Profiles for Mac OS Devices**
  - **Profiles for Windows Devices**.
  - **Profiles for Linux Devices**
- Click 'Save' for your changes to take effect
- Click the 'Delete Profile' button if you want to entirely remove a profile. The profile will be automatically uninstalled from devices on which it is active.

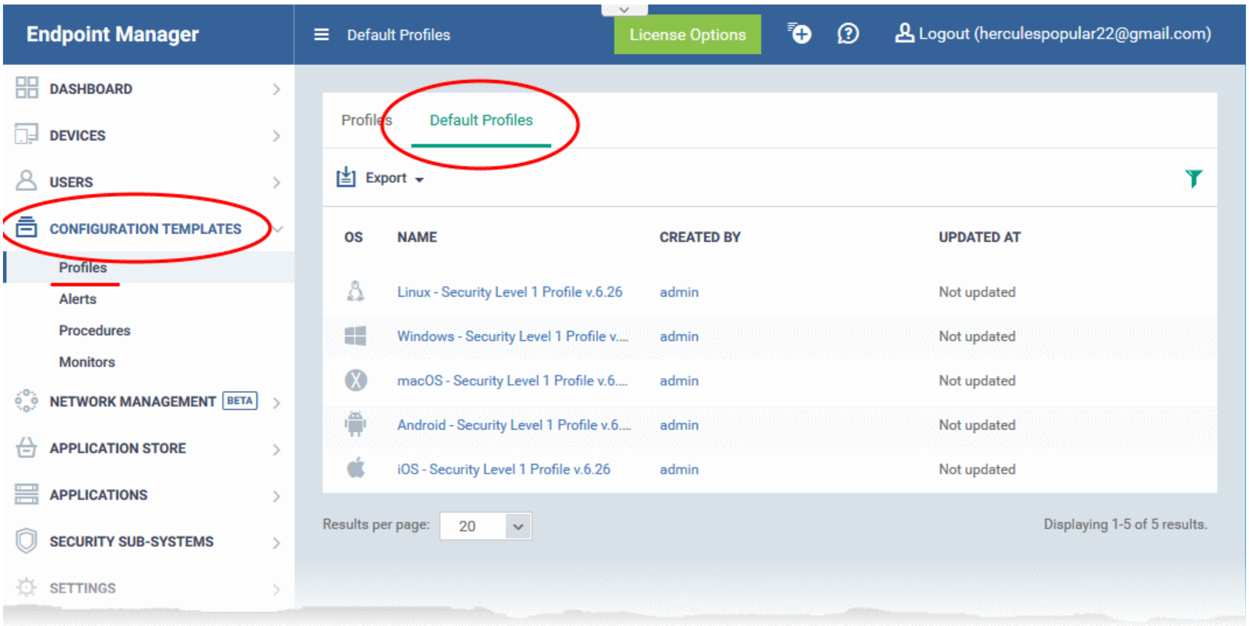
## 6.4. Manage Default Profiles

- 'Default' profiles are automatically assigned to new devices which match their operating system IF no user / user-group profile exists for the OS.
  - Default profiles are only applied if no user or user-group profile exists for the operating system.
  - If you remove all user profiles from a device then they will be replaced by the appropriate default profiles.
  - You can mark any profile you want as a 'default' profile. You can also apply multiple default profiles to the same devices.
- Endpoint Manager ships with the following default profiles:
  - Windows - Security Level 1 Profile
  - Mac OS - Security Level 1 Profile
  - Android - Security Level 1 Profile
  - iOS - Security Level 1 Profile
  - Linux - Security Level 1 Profile

  Each of the profiles above provides good, baseline security for managed devices. These profiles cannot be modified or deleted, but may be replaced on devices by another profile.
- Endpoint Manager also ships with three, non-default, profiles for Windows:
  - Windows - Security Level 1 Profile [Former Standard Profile]
  - Windows - Security Level 2 Profile
  - Windows - Security Level 3 Profile
- You can remove 'default' status from any profile, including the 'built-in' profiles mentioned above. However, it is mandatory to have at least one default profile per operating system.
- You can turn any profile you want into a default profile. You can also clone a default profile to use as a template for a new profile.

### View and manage default profiles

- Click 'Configuration Templates' > 'Profiles'
- Select the 'Default Profiles' tab at the top.



| OS | NAME | CREATED BY | UPDATED AT |
|---|---|---|---|
| | Linux - Security Level 1 Profile v.6.26 | admin | Not updated |
| | Windows - Security Level 1 Profile v.... | admin | Not updated |
| | macOS - Security Level 1 Profile v.6.... | admin | Not updated |
| | Android - Security Level 1 Profile v.6.... | admin | Not updated |
| | iOS - Security Level 1 Profile v.6.26 | admin | Not updated |

The image above shows the default profiles shipped with Endpoint Manager.

Click the following links for more help:

- Create a default profile
- View and manage default profiles
- Assign default profiles to devices
- Remove default profiles
- Cancel default profiles
- Export the list of Default Profiles to a CSV file

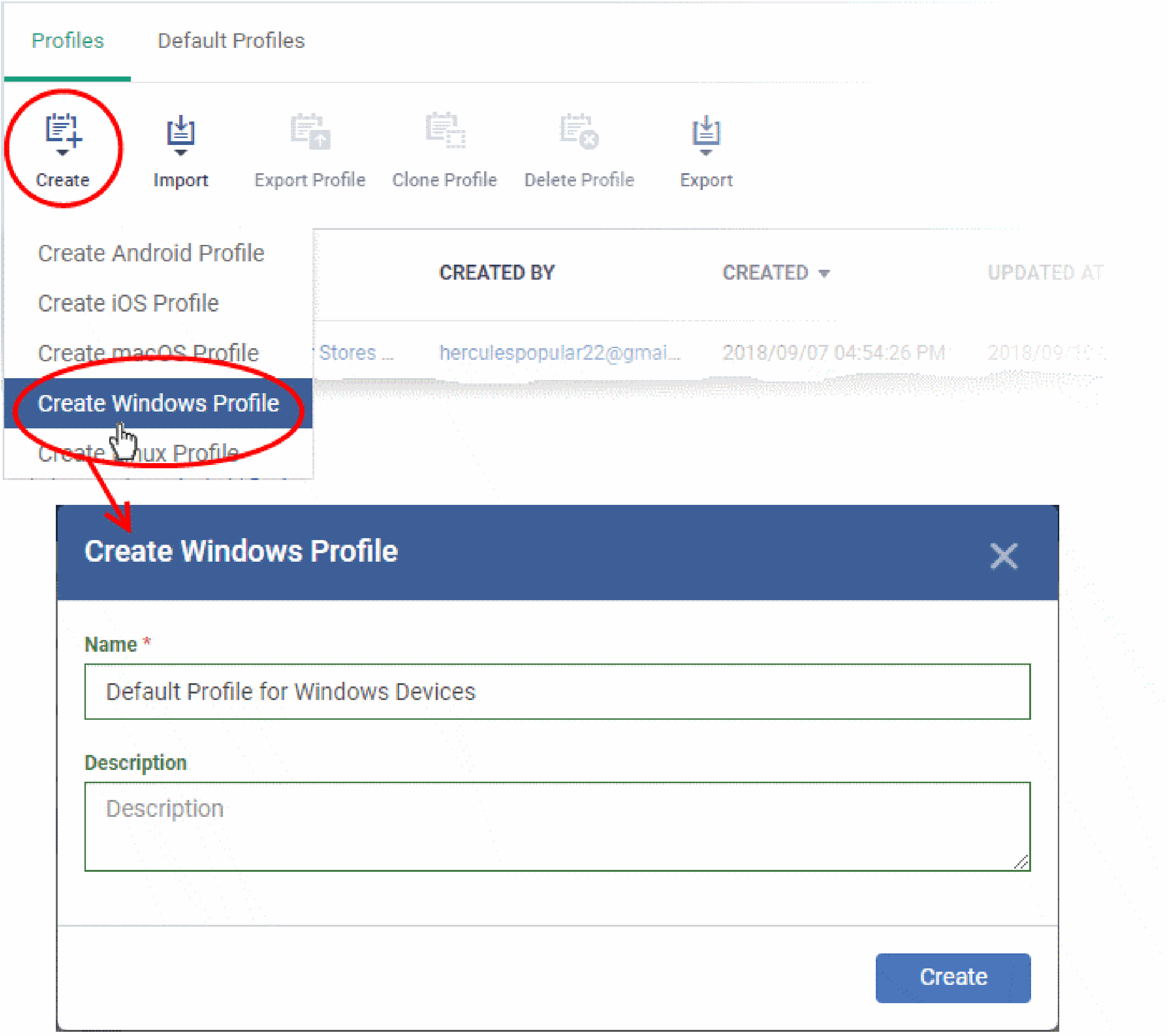
## Create a default profile

You can turn any profile into a 'default' profile. You can do this when you create a new profile, or by editing an existing profile.

- Create a new default profile
- Turn an existing profile into a default profile

## Create a new default profile

- Click 'Configuration Templates' > 'Profiles'
- Click the 'Profiles' tab
- Click 'Create' and choose the OS of the profile:



Create Windows Profile

Name *

Default Profile for Windows Devices

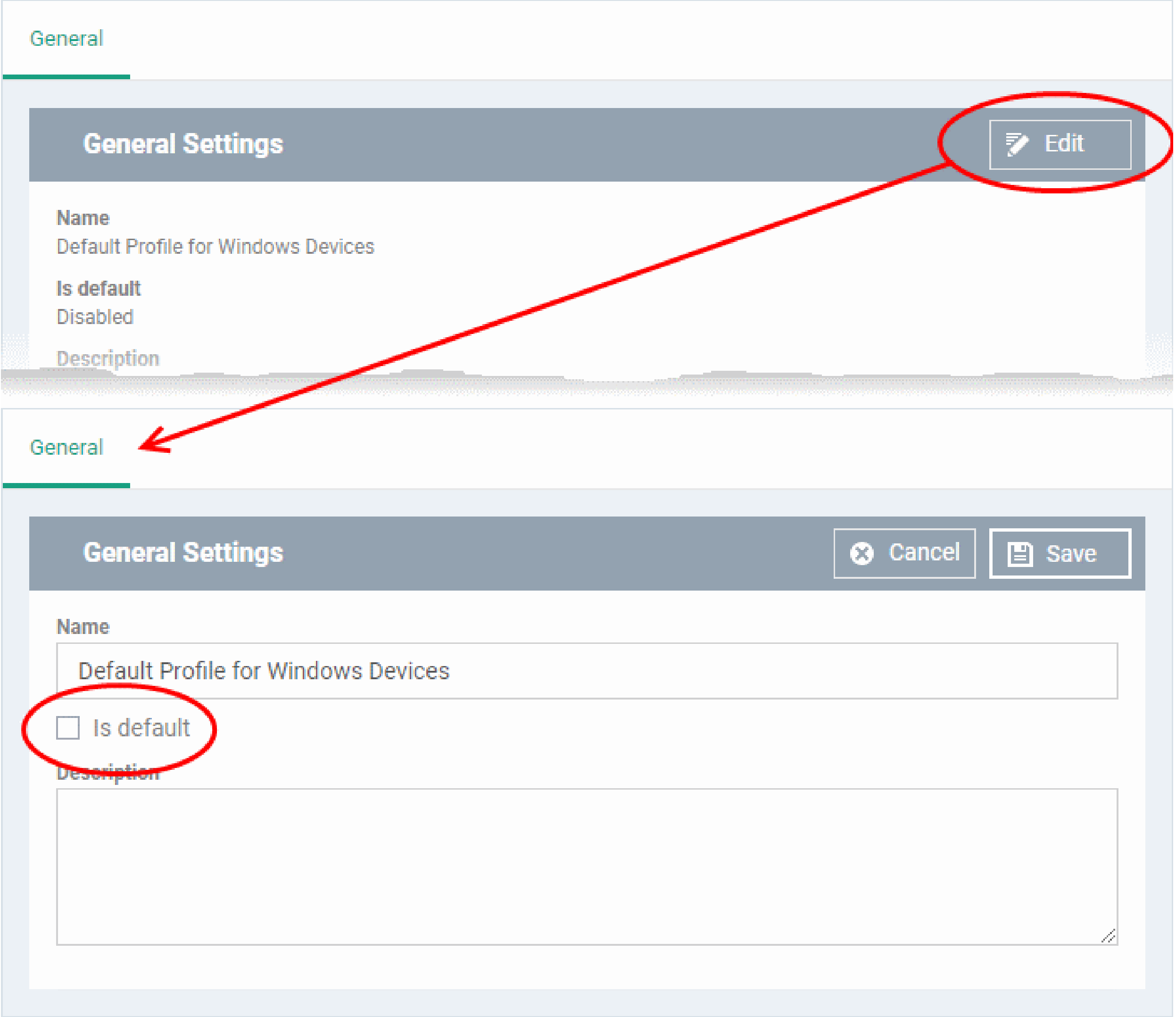
Description

Description

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

The profile will open at the 'General Settings' screen.

- Click 'Edit' at the top right and enable 'Is Default':



Name
Default Profile for Windows Devices

Is default
Disabled

Description

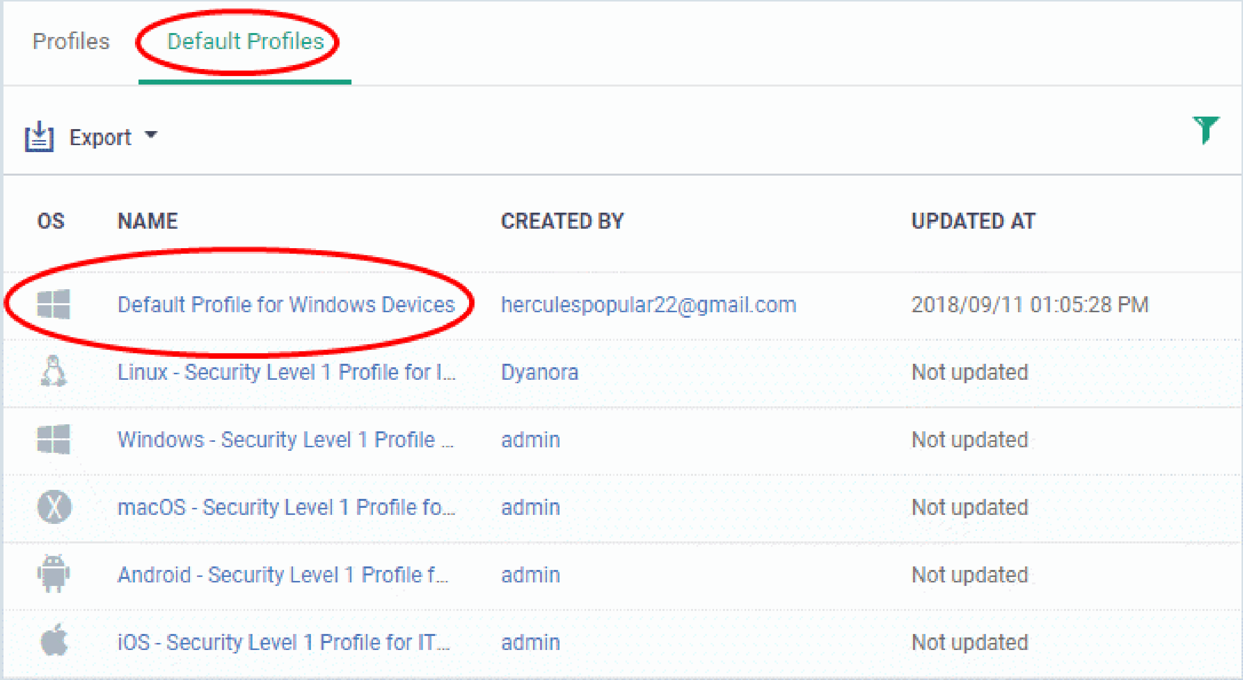
Name
Default Profile for Windows Devices

□ Is default

Description

- Click 'Save'.

The new profile will be listed in the 'Default Profiles' area:

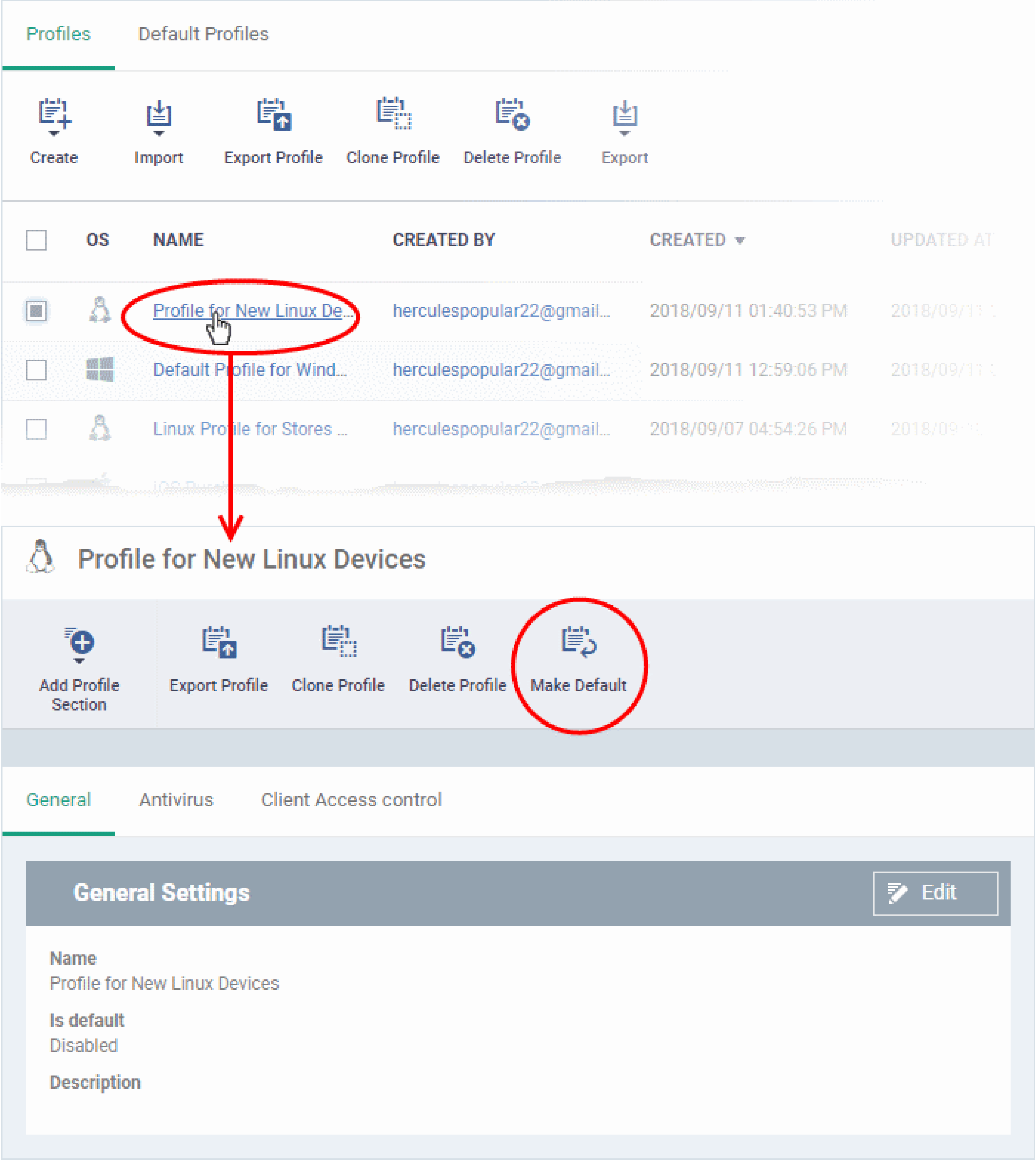


| OS | NAME | CREATED BY | UPDATED AT |
|---|---|---|---|
| ⊞ | Default Profile for Windows Devices | herculespopular22@gmail.com | 2018/09/11 01:05:28 PM |
|  | Linux - Security Level 1 Profile for I... | Dyanora | Not updated |
| ⊞ | Windows - Security Level 1 Profile ... | admin | Not updated |
| Ⓧ | macOS - Security Level 1 Profile fo... | admin | Not updated |
|  | Android - Security Level 1 Profile f... | admin | Not updated |
|  | iOS - Security Level 1 Profile for IT... | admin | Not updated |

You can edit the profile and add profile components (sections) as required. See **Edit Configuration Profiles** for more details.

### Turn an existing profile into a default profile

- Click 'Configuration Templates' > 'Profiles'
- Click the 'Profiles' tab
- Click the name of the profile that you want to set as a default:



| □ | OS | NAME | CREATED BY | CREATED ▾ | UPDATED AT |
|---|---|---|---|---|---|
| ▣ | | Profile for New Linux De... | herculespopular22@gmail... | 2018/09/11 01:40:53 PM | 2018/09/11 |
| □ | | Default Profile for Wind... | herculespopular22@gmail... | 2018/09/11 12:59:06 PM | 2018/09/11 |
| □ | | Linux Profile for Stores ... | herculespopular22@gmail... | 2018/09/07 04:54:26 PM | 2018/09/ |

**Name**
Profile for New Linux Devices

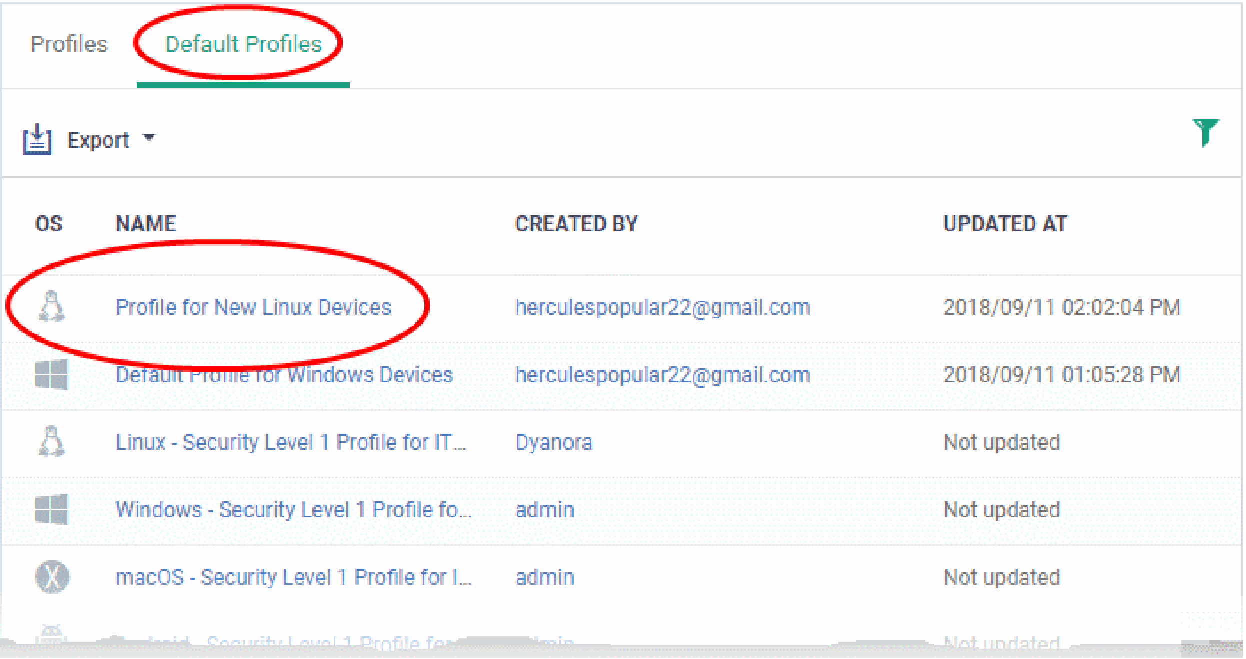
**Is default**
Disabled

**Description**

- Click the 'Make Default' button in the profile details screen.

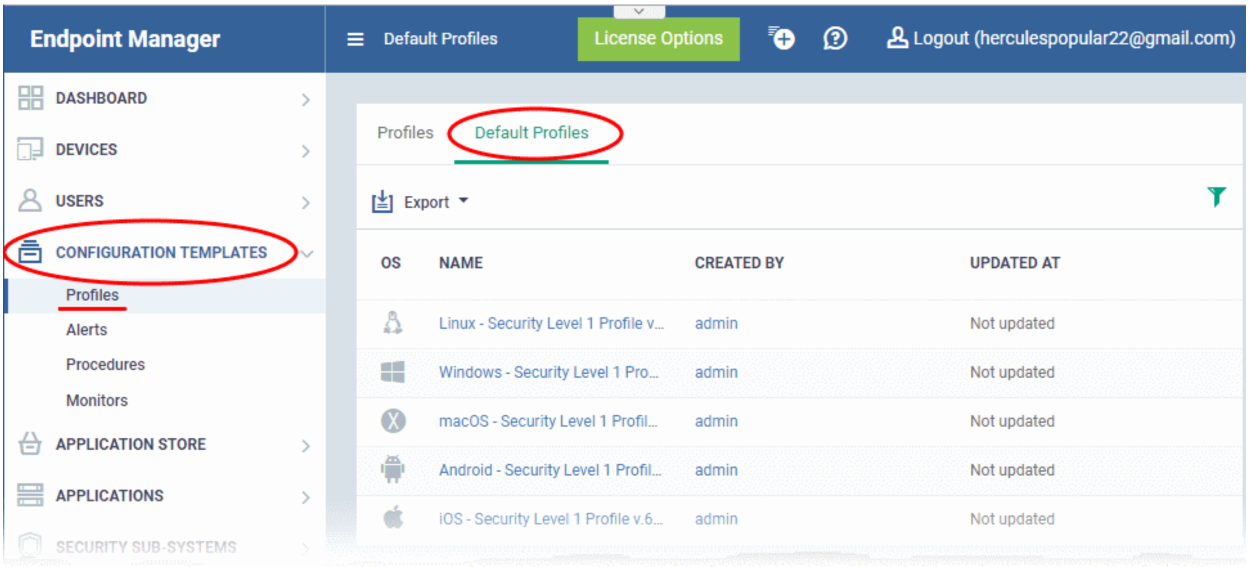
  Or
- Click the 'Edit' button then enable 'Is Default'
- Click 'Save'.

The profile will be listed in the 'Default Profiles' screen:



| OS | NAME | CREATED BY | UPDATED AT |
|---|---|---|---|
|  | Profile for New Linux Devices | herculespopular22@gmail.com | 2018/09/11 02:02:04 PM |
|  | Default Profile for Windows Devices | herculespopular22@gmail.com | 2018/09/11 01:05:28 PM |
|  | Linux - Security Level 1 Profile for IT... | Dyanora | Not updated |
|  | Windows - Security Level 1 Profile fo... | admin | Not updated |
|  | macOS - Security Level 1 Profile for I... | admin | Not updated |
|  | Android - Security Level 1 Profile fo... | admin | Not updated |

## The 'Default Profiles' interface

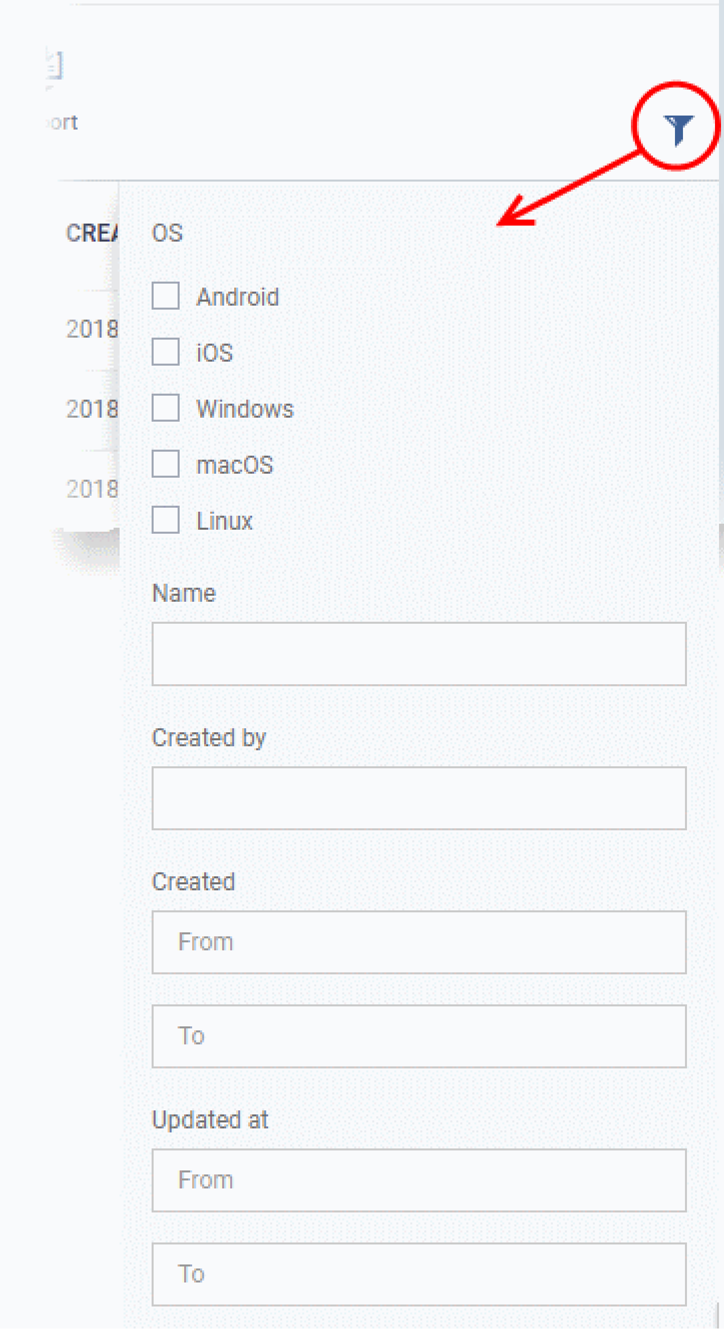


| OS | NAME | CREATED BY | UPDATED AT |
|---|---|---|---|
|  | Linux - Security Level 1 Profile v... | admin | Not updated |
|  | Windows - Security Level 1 Pro... | admin | Not updated |
|  | macOS - Security Level 1 Profil... | admin | Not updated |
|  | Android - Security Level 1 Profil... | admin | Not updated |
|  | iOS - Security Level 1 Profile v.6... | admin | Not updated |

| Default Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the devices to which the profile is applied. |
| Name | The label of the profile<br>• Click the profile name to open its details interface. This area lets you view and edit profile settings.<br>• See **Edit Configuration Profiles** for help with this. |
| Created by | The admin who created the profile. |

| | |
|---|---|
| | • Click the admin name to view their details. See **View the details of the User** if you want help with the user details screen. |
| Updated at | Date and time the profile was most recently edited. |

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Click the funnel icon to filter by OS, profile name, author or date:

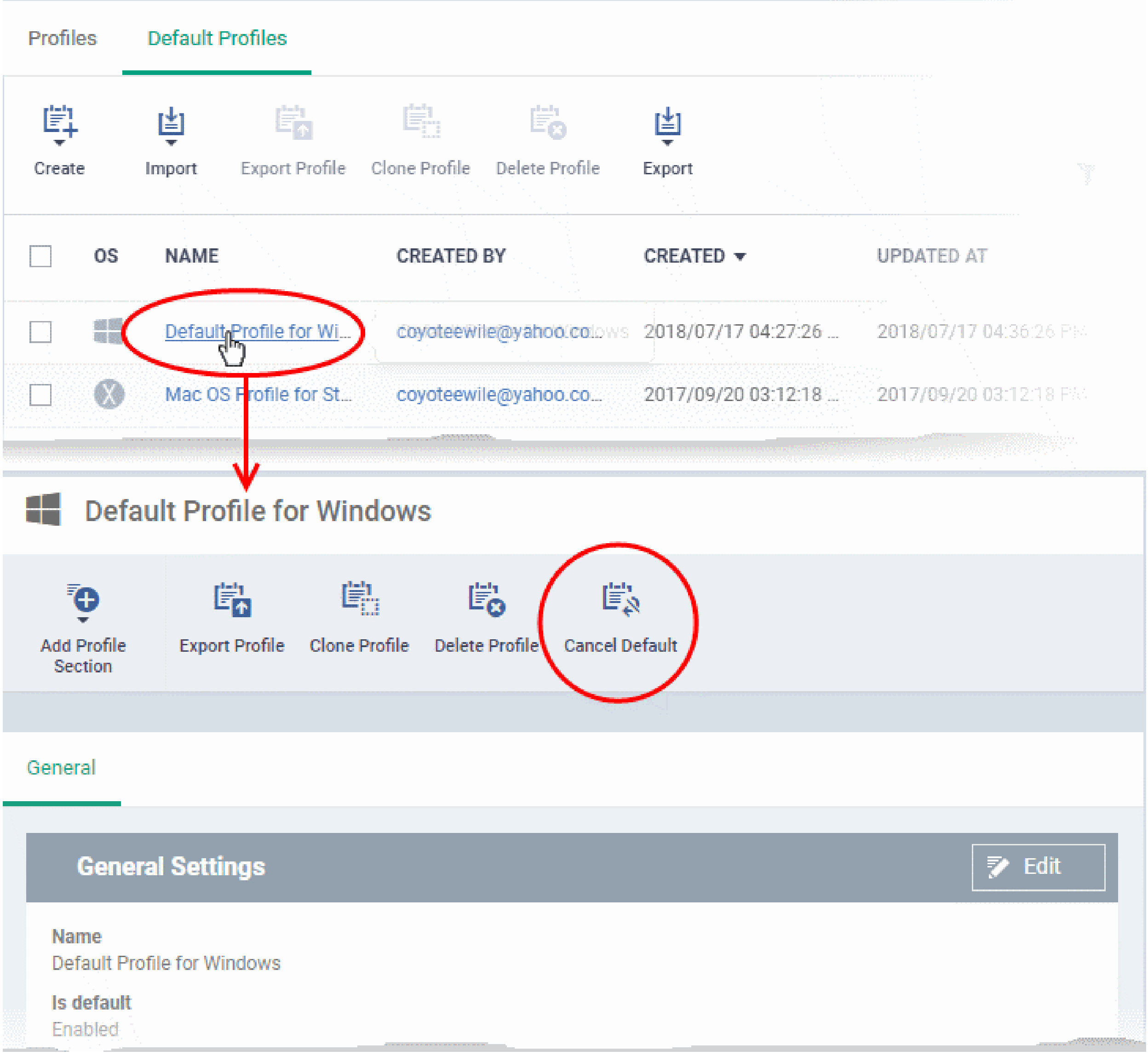


## Assign default profiles to devices

- New devices are automatically given the default profiles for their operating system IF there are no user/user group profiles for the device owner.
- Conversely, if you remove all user/user-group profiles from a device, then the default profiles are automatically deployed to take their place.

## Cancel default profiles

- You can cancel the default status of built-in profiles so they are not applied to new devices on enrollment. They will also be removed from any existing devices.
- For devices with no profiles applied, you can carry out on-demand functions such as run antivirus scans, run a procedure and so on. For Windows devices with CCS installed, when there are no profiles applied, the default CCS settings will apply.
- To open the default profiles screen, click 'Configuration Templates' > 'Profiles' on the left then choose the 'Default Profiles' tab.



| □ | OS | NAME | CREATED BY | CREATED ▼ | UPDATED AT |
|---|---|---|---|---|---|
| □ | | Default Profile for Wi... | coyoteewile@yahoo.co... | 2018/07/17 04:27:26 ... | 2018/07/17 04:36:26 PM |
| □ | | Mac OS Profile for St... | coyoteewile@yahoo.co... | 2017/09/20 03:12:18 ... | 2017/09/20 03:12:18 PM |

General Settings

Name
Default Profile for Windows

Is default
Enabled

- Click the name of the default profile from the list
- Click 'Cancel Default' button at the top

  Or
- Click 'Edit' on the right, deselect 'Is Default' check box and click 'Save'

The 'Edit' button is not available for built-in default profiles. You can remove default status only by clicking the 'Cancel Default' button at the top.

**Notes**:

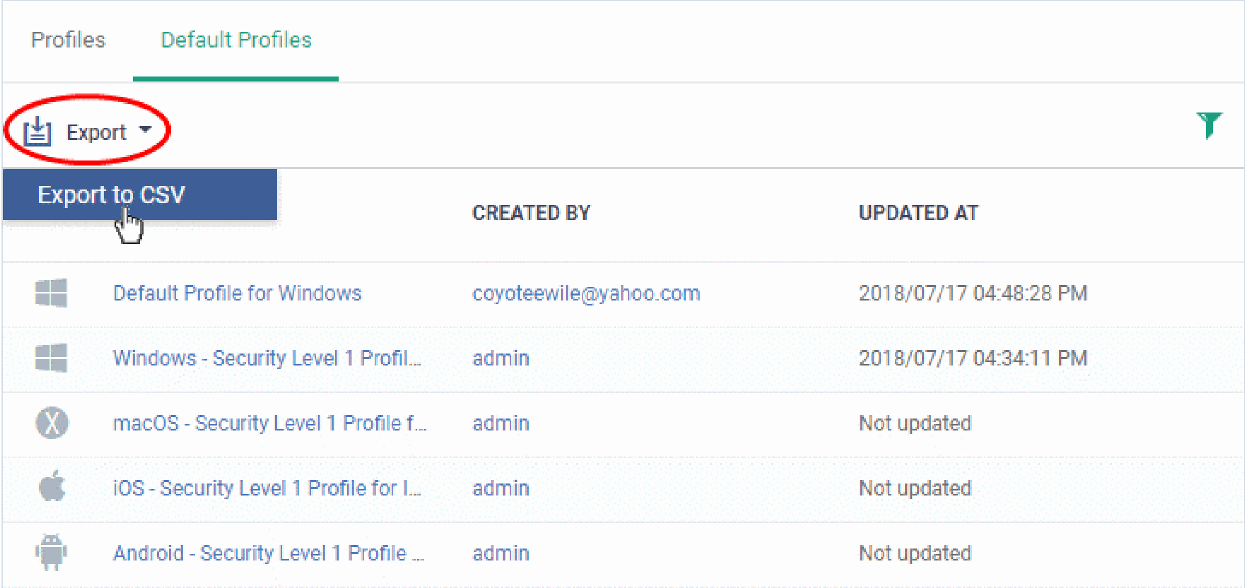
- It is mandatory to have at least one default profile for each operating system.

- You cannot cancel a default profile if it is the only default available for an OS.
    - Workaround - Assign a different profile as a default, then go back and cancel the first profile.

### Export the list of Default Profiles to a CSV file

You can export the list of default profiles to a comma-separated values (CSV) file as follows:

- Click the 'Export' button above the table then choose 'Export to CSV':



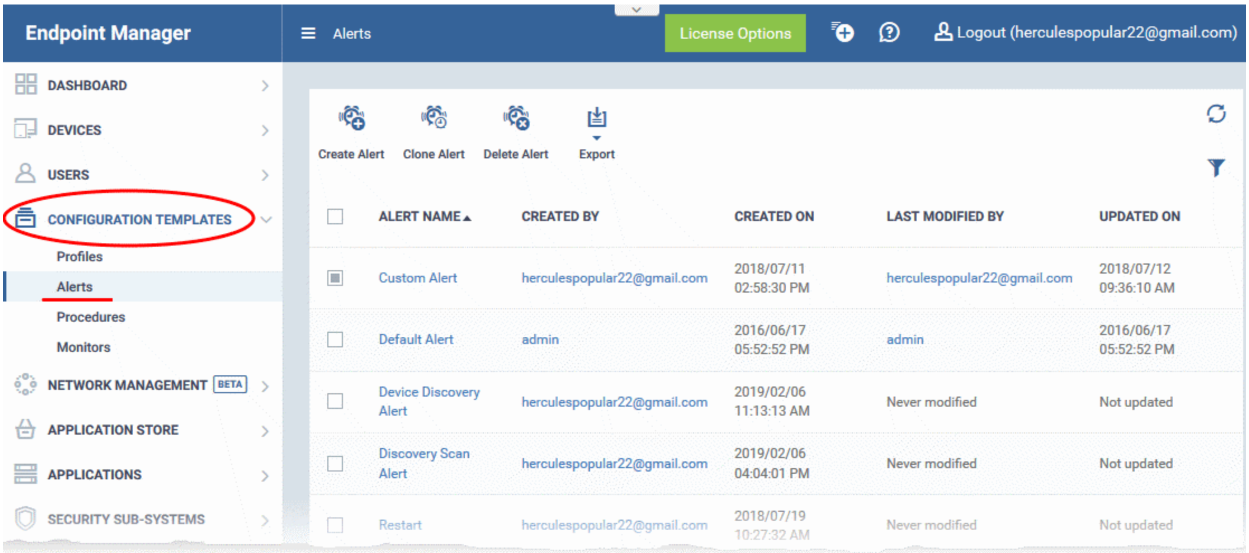
| | CREATED BY | UPDATED AT |
|---|---|---|
| Default Profile for Windows | coyoteewile@yahoo.com | 2018/07/17 04:48:28 PM |
| Windows - Security Level 1 Profil... | admin | 2018/07/17 04:34:11 PM |
| macOS - Security Level 1 Profile f... | admin | Not updated |
| iOS - Security Level 1 Profile for I... | admin | Not updated |
| Android - Security Level 1 Profile ... | admin | Not updated |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

# 6.5. Manage Alerts

- Click 'Configuration Templates' > 'Alerts' to view this interface.
- You can create procedures and monitors to track certain activities, and generate an alert when their conditions are met. For example, 'Generate an alert if CPU usage exceeds 90%', or 'Alert me when all Windows patches have been installed.'
- You can also configure network discovery scan tasks to generate alerts. For example, when a new device is found or if a device IP address changes.
- The 'Alerts' section contains templates of settings for these alerts. For example 'Send a notification to these recipients...', or 'Create a service desk ticket from the issue'.
- You apply the alert template to the procedure, monitor or discovery scan. You can have multiple templates to address different types of events. For example, you might want the alert for a failed patch to be different to the alert for a system restart.
- In the standard workflow, all procedures, monitors and discovery scan tasks have the 'Default Alert' template applied to them.
    - Click 'Configuration Templates' > 'Alerts' > 'Default Alert' to view these settings.
- If you want different alert settings for a specific event then you must create a new alert in this interface. For example, you may want an alert to be sent to specific recipients, or certain metrics to be included in the alert.
- Example. Click 'Procedures' > 'Predefined Procedures' > 'Monitors' > 'Alert if a new scheduled Task is Created'. You will notice the 'Default Alert' is used if the procedure fails. If you want to implement different alert settings then:

- Click 'Clone' to make a copy of the procedure. The procedure will be saved in the 'My Procedures' section as '[cloned] Alert if a new scheduled task is created'.
- Go to the alerts section and click 'Create Alert'. Name the alert and configure its settings as required.
- Next, open your cloned procedure and click 'Edit'. Type the name of the alert settings you want to use in the 'Use alert settings...' field. Click 'Save'.
- You can also specify that your new alert settings are used in the 'Monitoring' section of a profile.



| | ALERT NAME ▲ | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|
| ☒ | Custom Alert | herculespopular22@gmail.com | 2018/07/11 02:58:30 PM | herculespopular22@gmail.com | 2018/07/12 09:36:10 AM |
| ☐ | Default Alert | admin | 2016/06/17 05:52:52 PM | admin | 2016/06/17 05:52:52 PM |
| ☐ | Device Discovery Alert | herculespopular22@gmail.com | 2019/02/06 11:13:13 AM | Never modified | Not updated |
| ☐ | Discovery Scan Alert | herculespopular22@gmail.com | 2019/02/06 04:04:01 PM | Never modified | Not updated |
| ☐ | Restart | herculespopular22@gmail.com | 2018/07/19 10:27:32 AM | Never modified | Not updated |

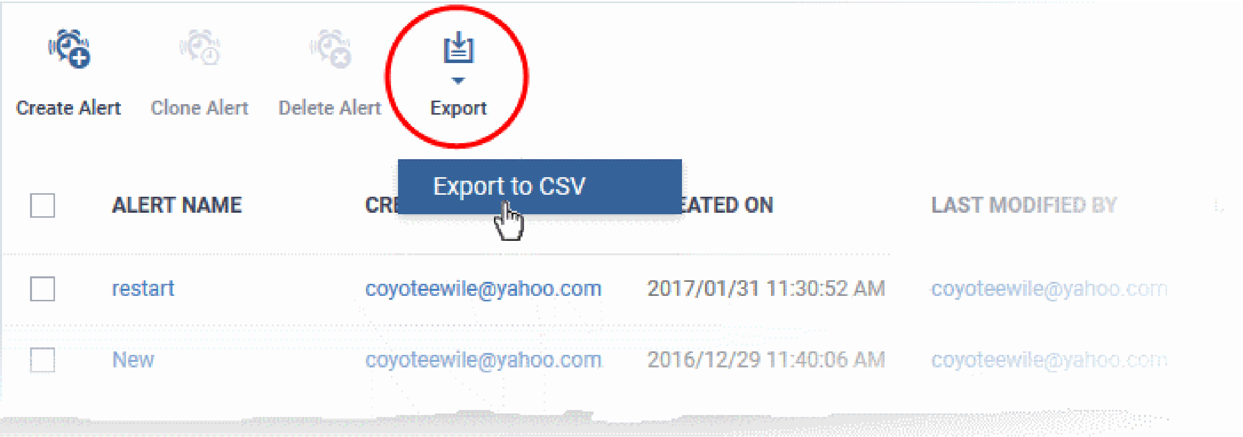
| Alerts - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Alert Name | Label of the alert.<br>• Click the alert name to open the alert configuration interface. See **Edit / Delete an Alert** for more details. |
| Created by | The administrator who created the alert.<br>• Click the name of an administrator to view their user details. See **View the details of the User** for more details. |
| Created on | The date and time at which the profile was created. |
| Last Modified by | The administrator who recently edited the alert.<br>• Click the name of an administrator to view their user details. See **View the details of the User** for more details. |
| Updated on | The date and time at which the alert was last updated. |
| **Controls** | |
| Create Alert | Add a new alert. See '**Create a New Alert**' for more details. |
| Clone Alert | Create a new alert by cloning an existing alert and modifying its settings as required. See '**Create a New Alert**' for more details. |
| Delete Alert | Remove selected alert(s).<br>The control will appear only if one or more alerts are selected. See **Edit / Delete an Alert** for more details. |

| | |
|---|---|
| Export | Save the list of alerts as a comma separated values (CSV) file. See **Export the List of Alerts** for more details. |

## Export the List of Alerts

Export the list of alerts to a .csv file as follows:

- Click 'Configuration Templates' on the left then choose 'Alerts'.
- Click the 'Export' button above the table then choose 'Export to CSV':

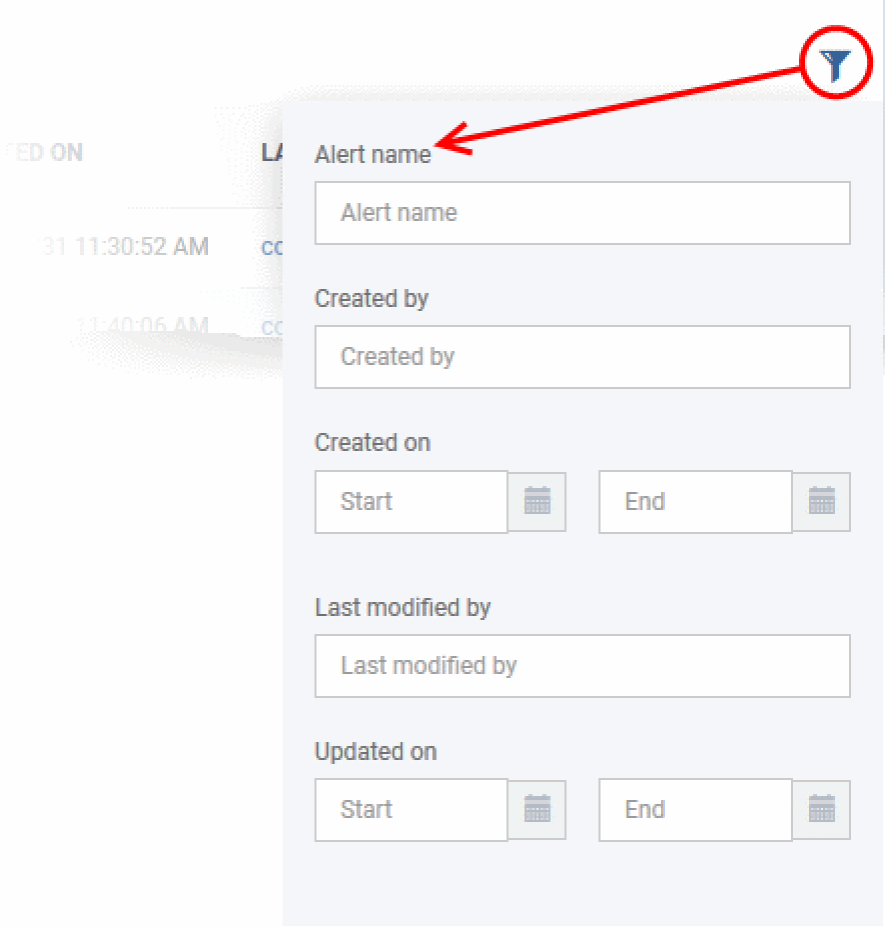


| ALERT NAME | CRE…EATED ON | | LAST MODIFIED BY |
|---|---|---|---|
| restart | coyoteewile@yahoo.com | 2017/01/31 11:30:52 AM | coyoteewile@yahoo.com |
| New | coyoteewile@yahoo.com | 2016/12/29 11:40:06 AM | coyoteewile@yahoo.com |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Sorting, Search and Filter Options

- Click on any of the column headers to sort the items in ascending/descending order of entries in that column.
- Click the funnel icon to search for alerts based on the filter parameters



- To filter the alerts based on name, author and admin who last edited the alert, enter the text partially or fully in the respective fields and click the 'Apply' button.
- To filter the alerts based on the period at which they were created or last modified, enter the date range in the specified fields, and click the 'Apply' button.
- You can use these filters in combination to search for specific alert.

Alerts which match the search parameters will be displayed in the screen.

- To display all alerts again, clear all filters and click the 'Apply' button.
- Click the funnel icon again to close filter options

Click the following links for more details:

- **Create a new alert**
- **Edit / delete an alert**

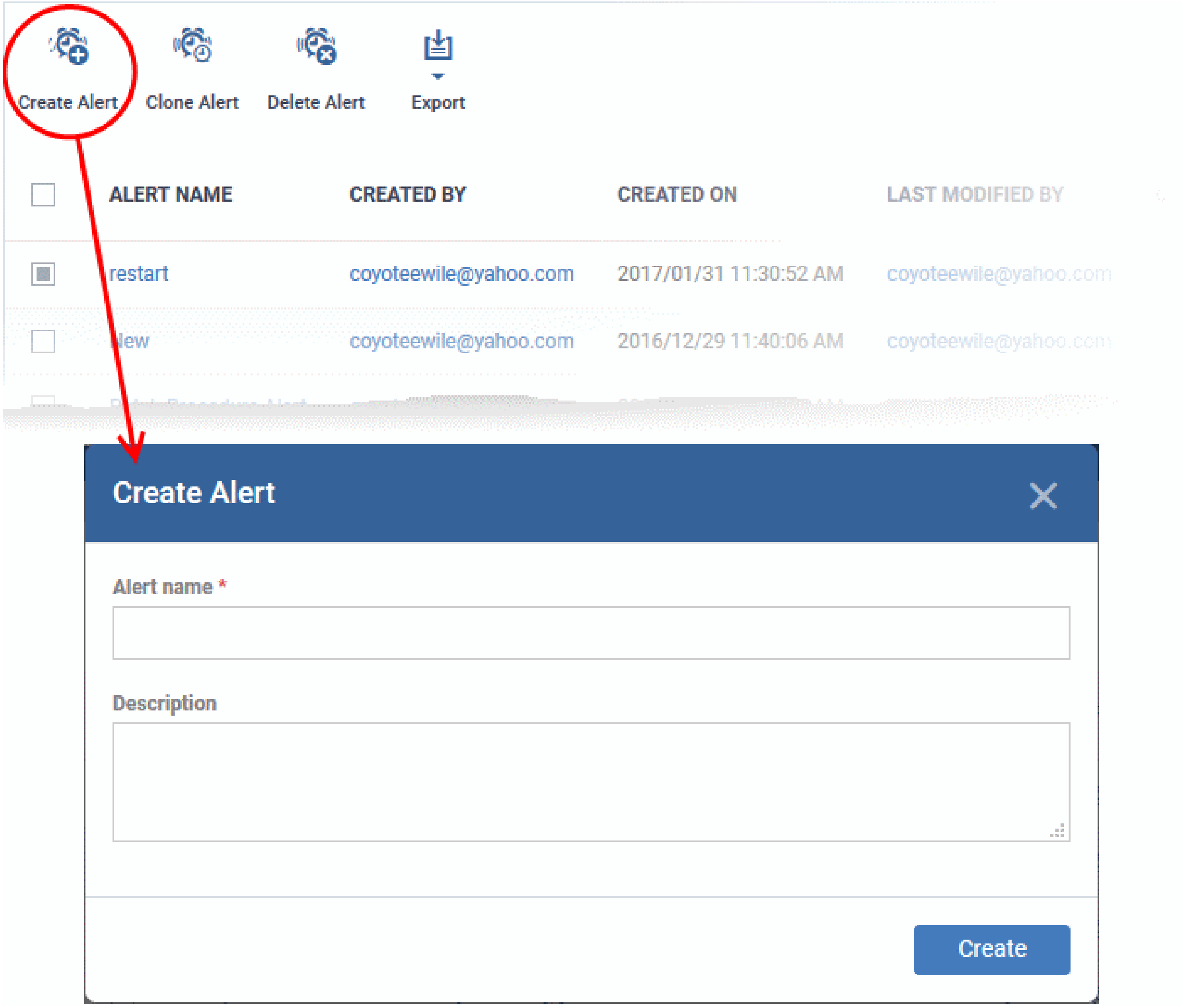
## 6.5.1. Create a New Alert

Alerts can be created in two ways:

- **Create new alert**
- **Clone an existing alert and edit its configuration as required**

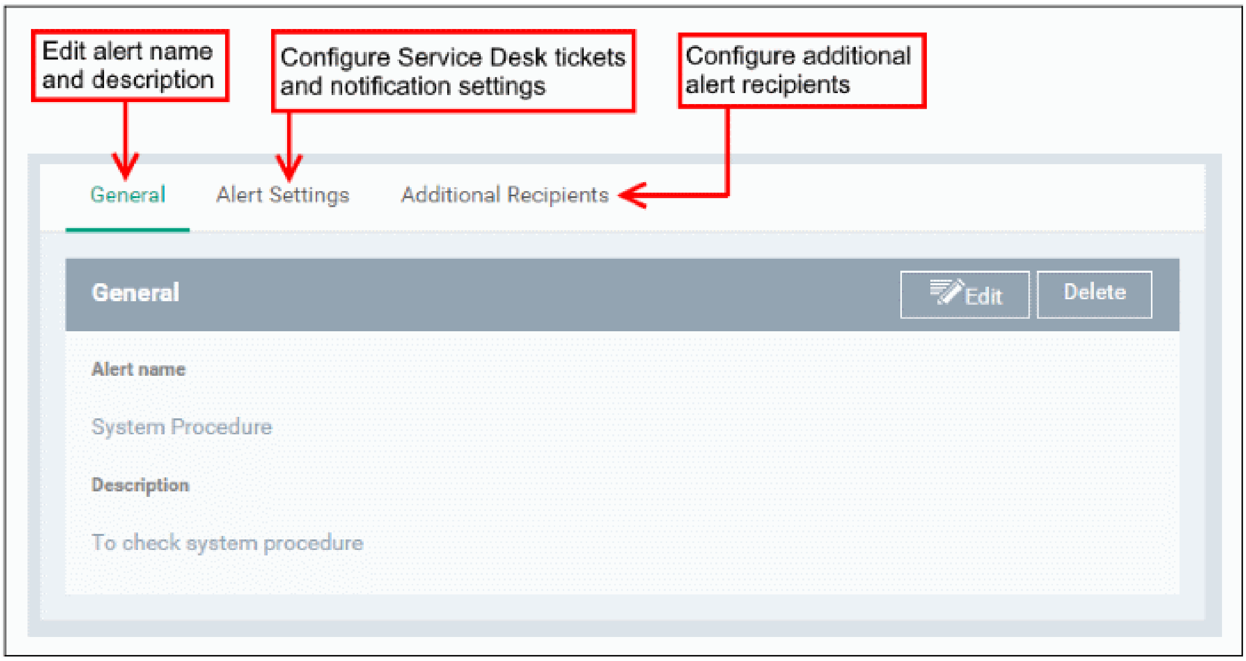
**To create a new alert**

- Click 'Configuration Templates' > 'Alerts'
- Click 'Create Alert'



| | ALERT NAME | CREATED BY | CREATED ON | LAST MODIFIED BY |
|---|---|---|---|---|
| ☒ | restart | coyoteewile@yahoo.com | 2017/01/31 11:30:52 AM | coyoteewile@yahoo.com |
| □ | new | coyoteewile@yahoo.com | 2016/12/29 11:40:06 AM | coyoteewile@yahoo.com |

- Enter a name and description for your alert and click 'Create'
- After saving, you will be taken to the alert configuration screen. The 'General' section allows you to modify basic settings:


Edit alert name and description
Configure Service Desk tickets and notification settings
Configure additional alert recipients
General
Alert Settings
Additional Recipients
General
Edit
Delete

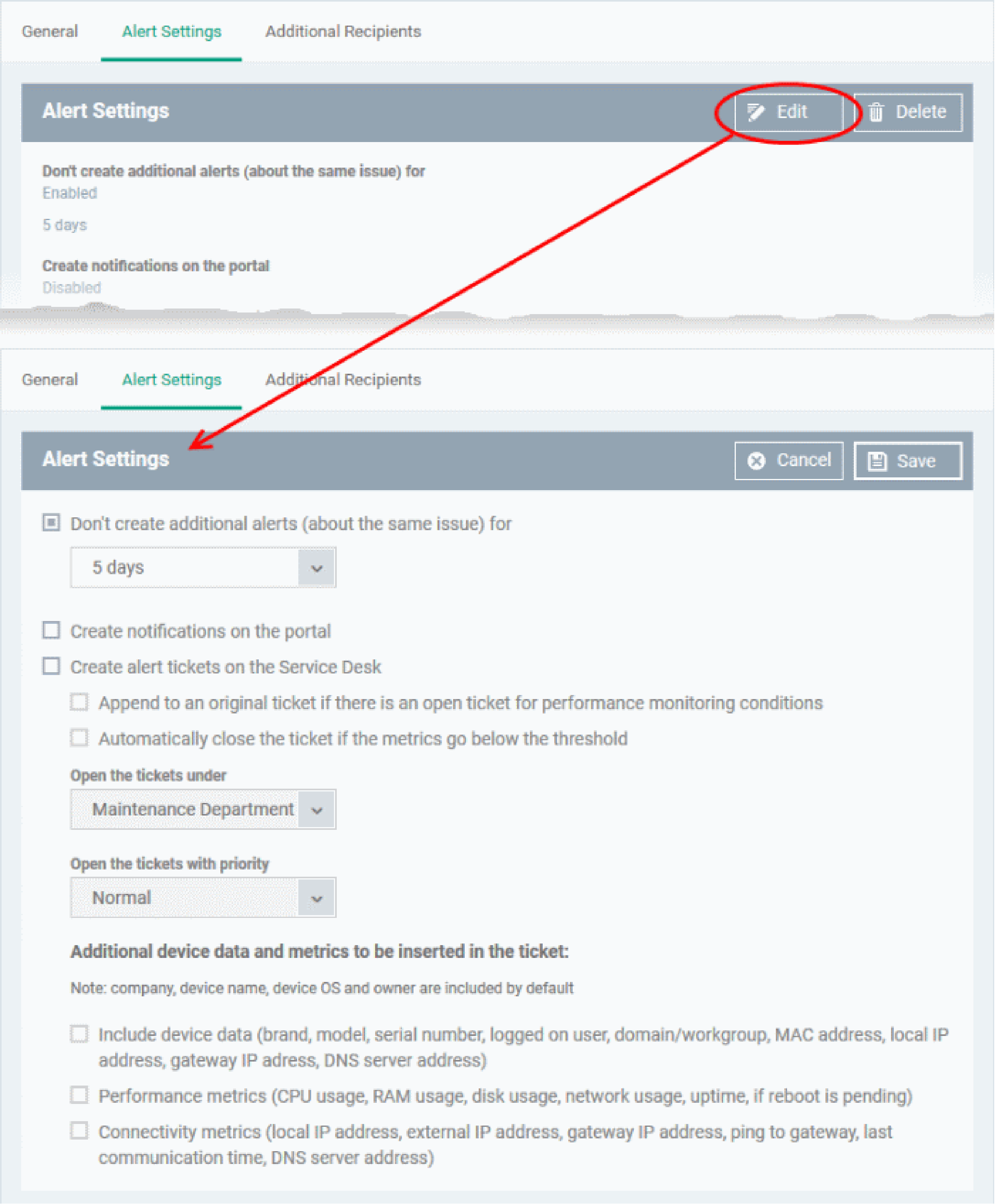
Alert name

System Procedure

Description

To check system procedure

- To configure alert settings, click 'Alert Settings' tab and then 'Edit'



Don't create additional alerts (about the same issue) for
Enabled
5 days

Create notifications on the portal
Disabled

☒ Don't create additional alerts (about the same issue) for

5 days

□ Create notifications on the portal

□ Create alert tickets on the Service Desk

□ Append to an original ticket if there is an open ticket for performance monitoring conditions

□ Automatically close the ticket if the metrics go below the threshold

Open the tickets under
Maintenance Department

Open the tickets with priority
Normal

Additional device data and metrics to be inserted in the ticket:

Note: company, device name, device OS and owner are included by default

□ Include device data (brand, model, serial number, logged on user, domain/workgroup, MAC address, local IP address, gateway IP adress, DNS server address)

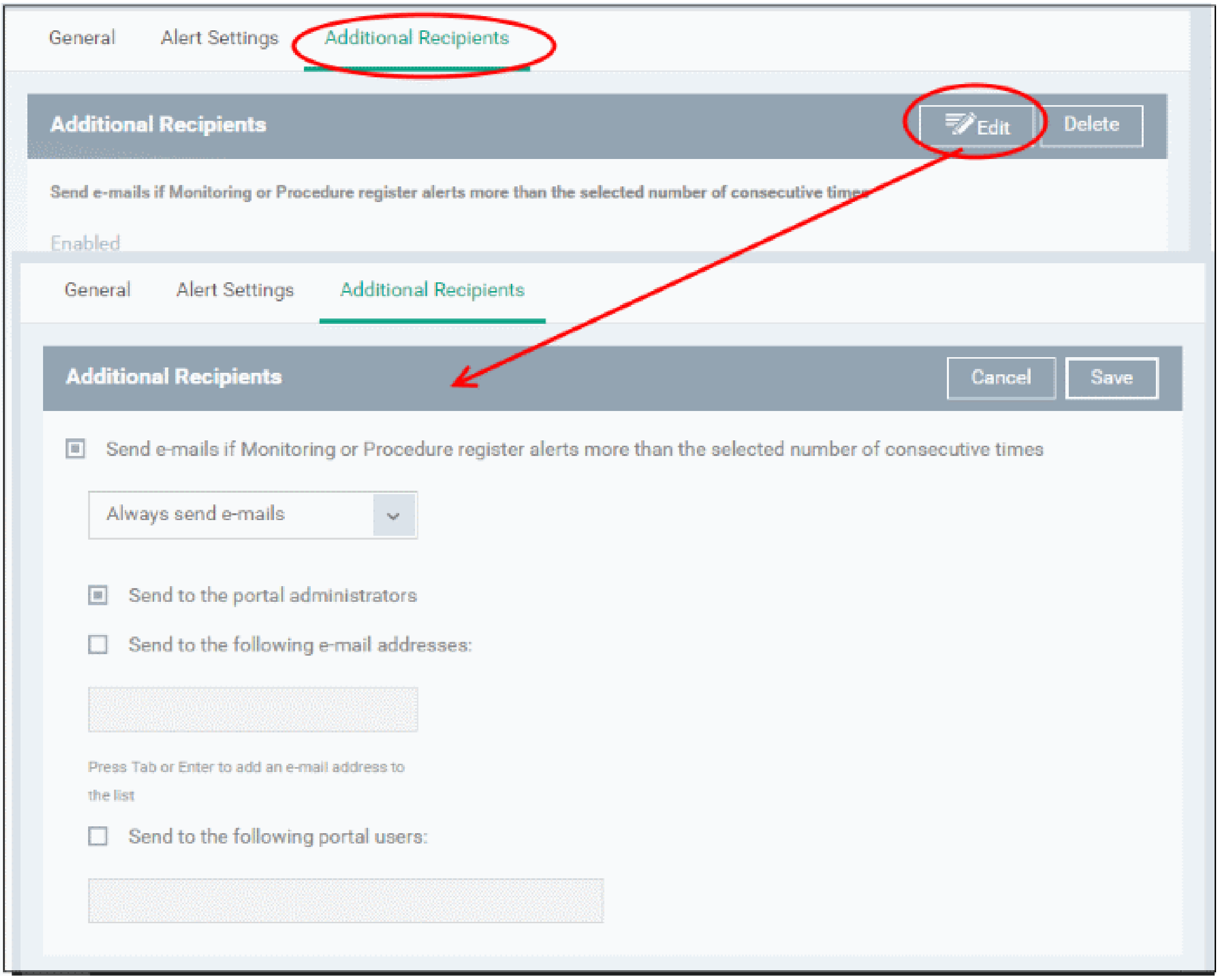
□ Performance metrics (CPU usage, RAM usage, disk usage, network usage, uptime, if reboot is pending)

□ Connectivity metrics (local IP address, external IP address, gateway IP address, ping to gateway, last communication time, DNS server address)

- **Don't create additional alerts (about the same issue) for -** Determines whether additional alerts should be generated if same issue occurs within the specified period. The field below this allows you to select the period which ranges from 5 minutes to 5 days. By default, this is selected with a specified period of 5 days.
- **Create notifications on the portal -** Alerts will be generated and displayed on the **Notifications** screen.
- **Create alert tickets on the Service Desk -** If enabled, tickets will be raised automatically on Service Desk application and allotted to specified departments.

- **Append to an original ticket if there is an open ticket for performance monitoring conditions** - Determines whether a new ticket should be raised for an issue even if a ticket is open for the same issue in Service Desk.
- **Automatically close the ticket if the metrics go below the threshold** - Determines whether the open tickets for an issue should be closed automatically if the monitoring parameter goes below the set threshold.
- **Open the tickets under** - Select the the department from the drop-down to which the tickets should be allotted.
- **Open the tickets with priority** - Select the ticket priority, whether normal, high or critical from the drop-down.
- **Additional device data and metrics to be inserted in the ticket** - By default, the name of the company, device type, device OS and the owner information are included in the ticket. To add additional device data and metrics to the ticket, select the respective options.
  - **Device Data** - Adds device information like brand, model. IP address and so on
  - **Performance Metrics** - Adds device performance information like CPU usage, RAM usage, disk usage, network usage and more
  - **Connectivity Metrics** - Adds information on network to which the device is connected, like local IP address, external IP address, gateway IP address and more

- To configure 'Additional Recipients' settings, click 'Additional Recipients' tab and then 'Edit'.



☒ Send e-mails if Monitoring or Procedure register alerts more than the selected number of consecutive times

Always send e-mails

☒ Send to the portal administrators

☐ Send to the following e-mail addresses:

Press Tab or Enter to add an e-mail address to the list

☐ Send to the following portal users:

- **Send e-mails if Monitoring or Procedure register alerts more than the selected number of consecutive times** - Determines when email alerts should be sent for an issue. For example, if you select 5 from the drop-down, email alert will be sent only if the same issue is generated 5 consecutive times.

- **Send to the portal administrators -** Emails alerts will be sent to users with 'Administrative' roles.
- **Send to the following e-mail addresses -** Allows you to add external recipients. Enter the email address and press either 'Tab' or 'Enter' button. You can add multiple recipients. To remove a recipient, click the 'X' beside the recipient.
- **Send to the following portal users -** Allows you to add users with 'User' roles. Type the username fully or partly and select from the list. You can add multiple users. To remove a user, click the 'X' beside the name.

- Click 'Save' to apply your changes. The alert will be created and displayed in the list. The alerts will be available for selection in the **Procedure** section and while configuring **Monitor Settings** for a Windows profile.

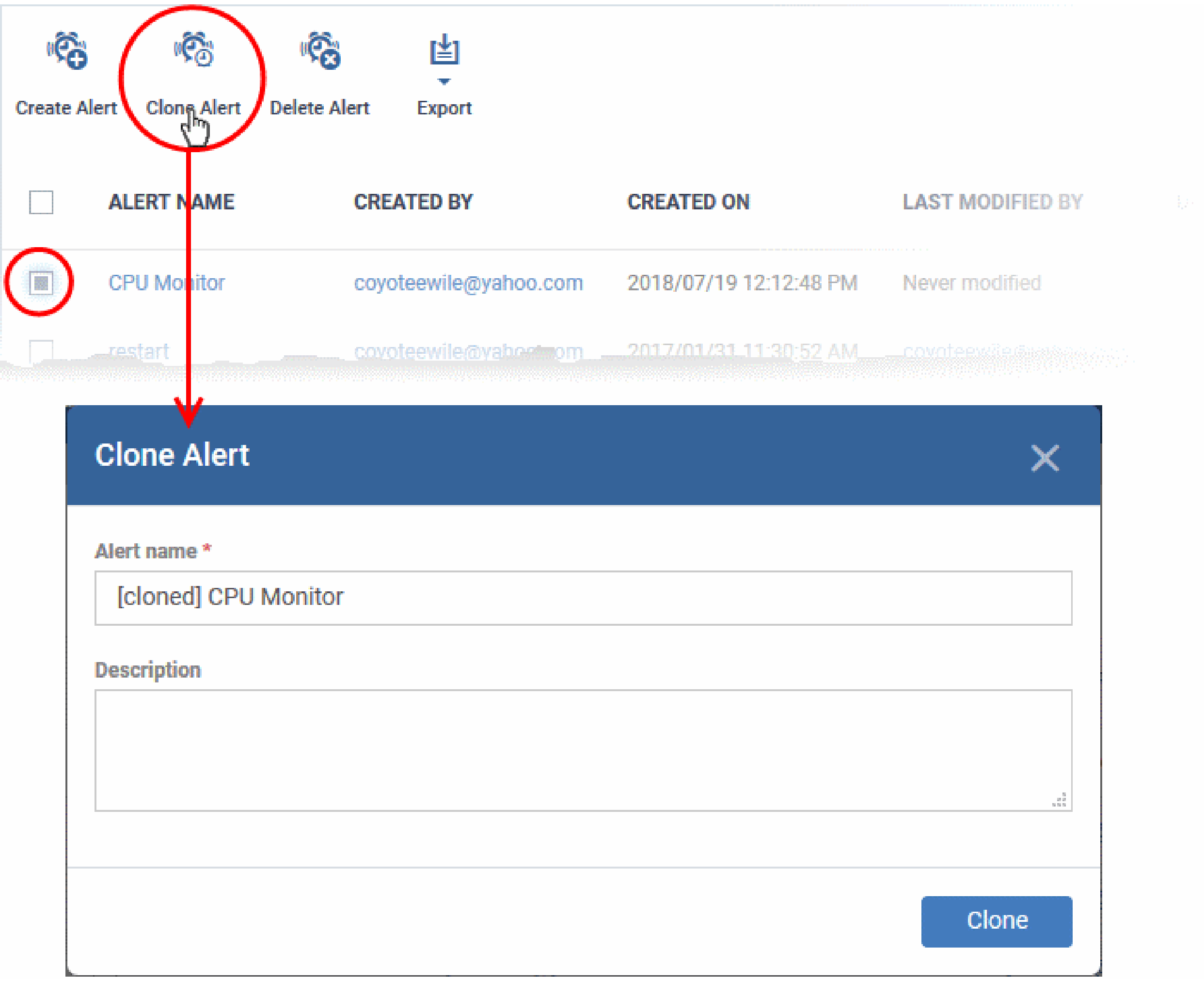
**To create an alert by cloning an existing alert**

- Click 'Configuration Templates' > 'Alerts'
- Click on the name of the alert you want to clone.

The alert configuration interface will open

- Click 'Clone Alert' from the top

Alternatively, select the alert from the 'Alerts' interface and click 'Clone Alert' at the top.



| □ | ALERT NAME | CREATED BY | CREATED ON | LAST MODIFIED BY |
|---|---|---|---|---|
| ▣ | CPU Monitor | coyoteewile@yahoo.com | 2018/07/19 12:12:48 PM | Never modified |
| □ | restart | coyoteewile@yahoo.com | 2017/01/31 11:30:52 AM | coyoteewile |

Clone Alert

Alert name *

[cloned] CPU Monitor

Description

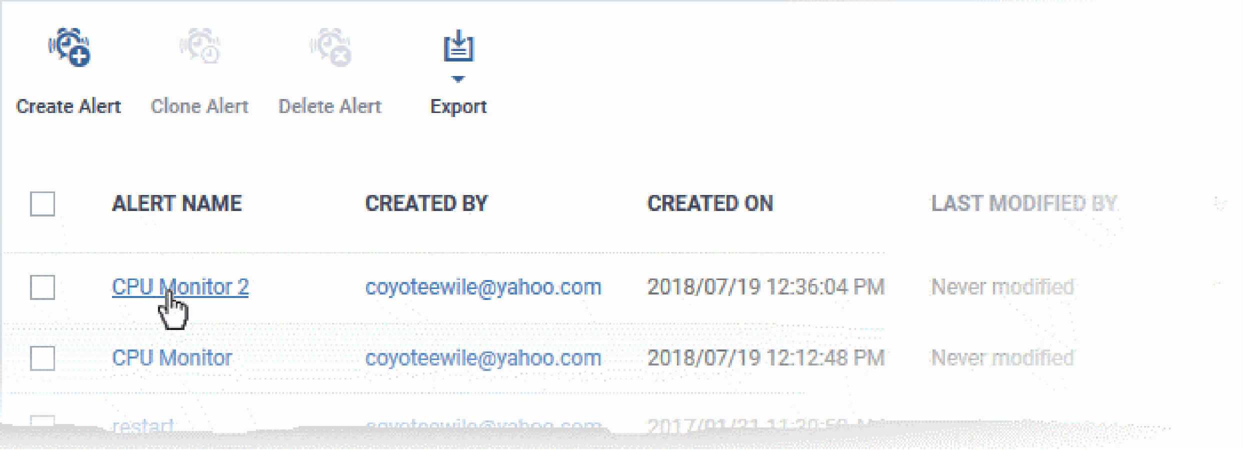
The 'Clone Alert' dialog will open. The name of the new alert will be the same as the source alert with the prefix [cloned].

- If required, enter a new name for the alert and a short description

- Click 'Clone'.

A new alert will be created with configuration parameters identical to the source alert and added to the list.

- Click the name of the alert



| □ | ALERT NAME | CREATED BY | CREATED ON | LAST MODIFIED BY |
|---|---|---|---|---|
| □ | CPU Monitor 2 | coyoteewile@yahoo.com | 2018/07/19 12:36:04 PM | Never modified |
| □ | CPU Monitor | coyoteewile@yahoo.com | 2018/07/19 12:12:48 PM | Never modified |
| □ | restart | coyoteewile@yahoo.com | 2017/01/21 11:20:5 | |

The configuration screen for the alert will open with the settings identical to the source alert

- Edit the parameters as required. See the **explanation above** for more details
- Click 'Save' to apply your changes

## 6.5.2. Edit / Delete an Alert

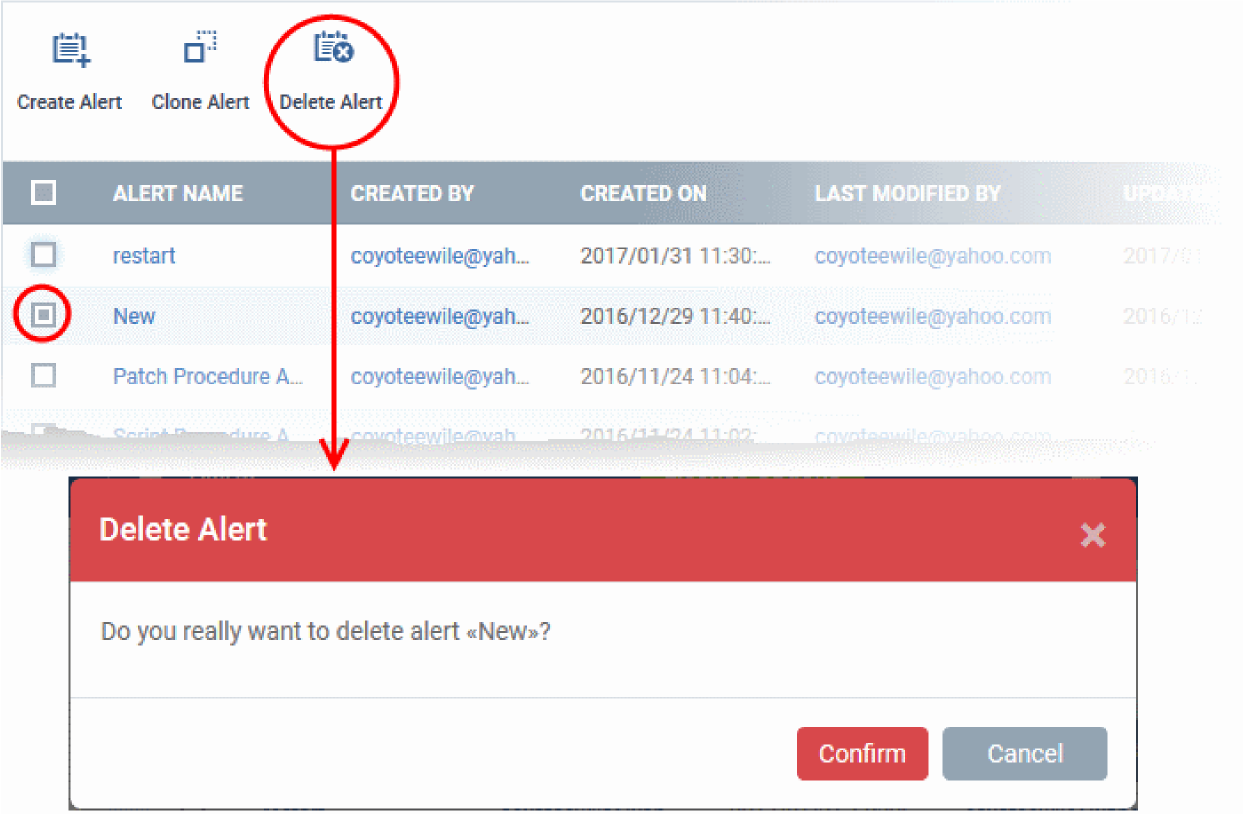
To edit an alert:

- Click 'Configuration Templates' > 'Alerts'
- Click the name of the alert you wish to modify
- Click the 'Edit' button on the right
- You can edit settings in the 'General', 'Alert Settings' and 'Additional Recipients' areas
- See '**Create a New Alert**' for more information on the settings in these areas
- Click 'Save' to apply your changes

Before deleting an alert, please consider whether it is currently being used on any **Procedures** or **Monitor Settings** for a Windows profile. Please also investigate whether the alert could be edited rather than deleted.

**To delete an alert:**

- Click 'Configuration Templates' > 'Alerts'
- Click the name of the alert you wish to delete
- Click the 'Delete' button on the right.
- Click 'Confirm' in the confirmation dialog:



| □ | ALERT NAME | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATE |
|---|---|---|---|---|---|
| □ | restart | coyoteewile@yah... | 2017/01/31 11:30:... | coyoteewile@yahoo.com | 2017/0 |
| ▣ | New | coyoteewile@yah... | 2016/12/29 11:40:... | coyoteewile@yahoo.com | 2016/12 |
| □ | Patch Procedure A... | coyoteewile@yah... | 2016/11/24 11:04:... | coyoteewile@yahoo.com | 2016/1 |
| □ | Script Procedure A... | coyoteewile@yah... | 2016/11/24 11:02:... | coyoteewile@yahoo.com | |

Delete Alert

Do you really want to delete alert «New»?

## 6.6. Manage Procedures

- Click 'Configuration Templates' > 'Procedures'

Procedures are standalone instruction scripts and patches for Windows devices. Procedures can be run on an ad-hoc basis or added to a profile. You can create procedures to identify and fix issues, monitor resources, and run patches.

Features include:

- Select a predefined or custom procedure to execute on endpoint
- Easily modify procedure variables.
- Compose script instructions in Python
- Update Windows and third party apps with a patch procedure
- Combine procedures to build broader procedures.
- Show procedure results in the execution log as well as inside a particular device
- Import procedures from JSON.
- Export and clone procedures.
- Run procedures on demand by selecting 'Run Over Device'.
- Add predefined procedures to Windows device profiles and create schedules for them.

Please use the following links to learn more about procedures:

- **View and Manage Procedures**
- **Create a Custom Procedure**
- **Combine Procedures to Build Broader Procedures**
- **Review / Approve / Decline New procedures**
- **Add a Procedure to a Profile / Procedure Schedules**

- **Import / Export / Clone Procedures**
- **Change Alert Settings**
- **Directly Apply Procedures to Devices**
- **Edit / Delete Procedures**
- **View Procedure Results**

## 6.6.1. View and Manage Procedures

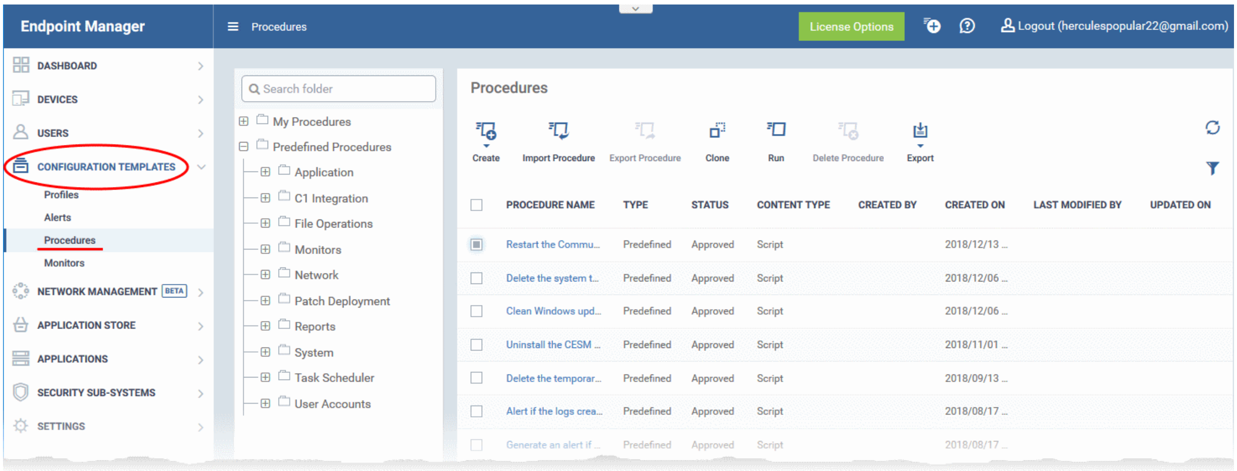
- Click 'Configuration Templates' > 'Procedures' to open the procedures interface.

There are two categories of procedures:

1. 'Predefined Procedures- two types: 'Script' and 'Patch' procedures
2. 'My Procedures' - custom procedures that you create.

Predefined procedures cannot be edited. However, you can clone a procedure and modify it to create a custom procedure. See **Create a Custom Procedure** for help with this.

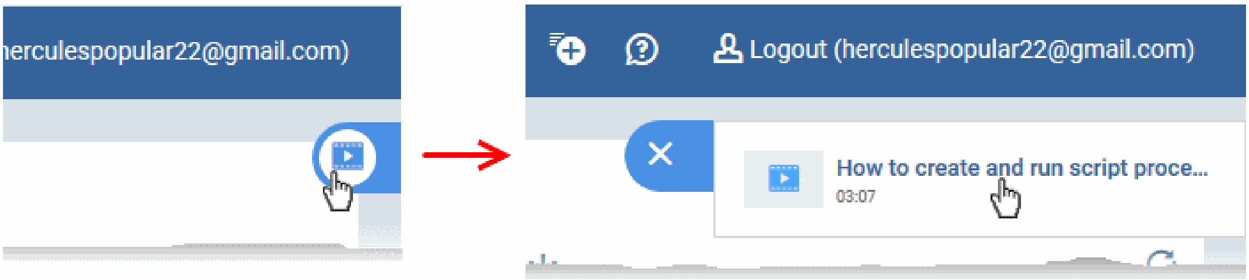
- The following folders contain scripts to execute many useful tasks - 'Application', 'System', 'File Operations', 'Task Scheduler', 'Reports', 'Monitors', 'Network' and 'User Accounts'.
- The 'Patch Deployment' folder contains procedures to install Windows OS patches onto Windows endpoints.



| □ | PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|---|---|---|
| ■ | Restart the Commu... | Predefined | Approved | Script | | 2018/12/13 ... | | |
| □ | Delete the system t... | Predefined | Approved | Script | | 2018/12/06 ... | | |
| □ | Clean Windows upd... | Predefined | Approved | Script | | 2018/12/06 ... | | |
| □ | Uninstall the CESM ... | Predefined | Approved | Script | | 2018/11/01 ... | | |
| □ | Delete the temporar... | Predefined | Approved | Script | | 2018/09/13 ... | | |
| □ | Alert if the logs crea... | Predefined | Approved | Script | | 2018/08/17 ... | | |
| □ | Generate an alert if ... | Predefined | Approved | Script | | 2018/08/17 ... | | |

| Procedures - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Procedure Name | The procedure label.<br>• Click the name of a procedure to view, edit review, schedule or approve/decline it. See **Review / Approve / Decline New Procedures** and **Edit / Delete Procedures** for more details. |
| Type | Whether the procedure is a custom or a predefined procedure. |
| Status | The current status of the procedure. The possible statuses are:<br>• Created<br>• Edited<br>• Ready to review<br>• Approved<br>• Declined |
| Content Type | Whether the procedure is script procedure or patch procedure. |
| Created by | The administrator who created the custom procedure.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created On | Date and time the procedure was created. |
| Last Modified By | The admin who most recently edited the procedure. |
| Updated On | Date and time the procedure was last edited. |
| **Controls** | |
| Create | Configure a new script or patch procedure. See '**Create a Custom Procedure**' for help with this. |
| Import / Export / Clone | Import a saved procedure, export and save a procedure, and clone an existing procedure.<br>Cloned procedures can be modified to create a new, custom procedure.<br>See '**Import / Export / Clone Procedure**' for more details. |
| Run | Execute a procedure on target Windows devices. See '**Directly Apply Procedures to Devices**' for more details. |
| Delete Procedure | Remove procedures from Endpoint Manager. Use the check-boxes to select the procedures. |
| Export | Save the list of currently displayed procedures as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of Procedures** for more details. |

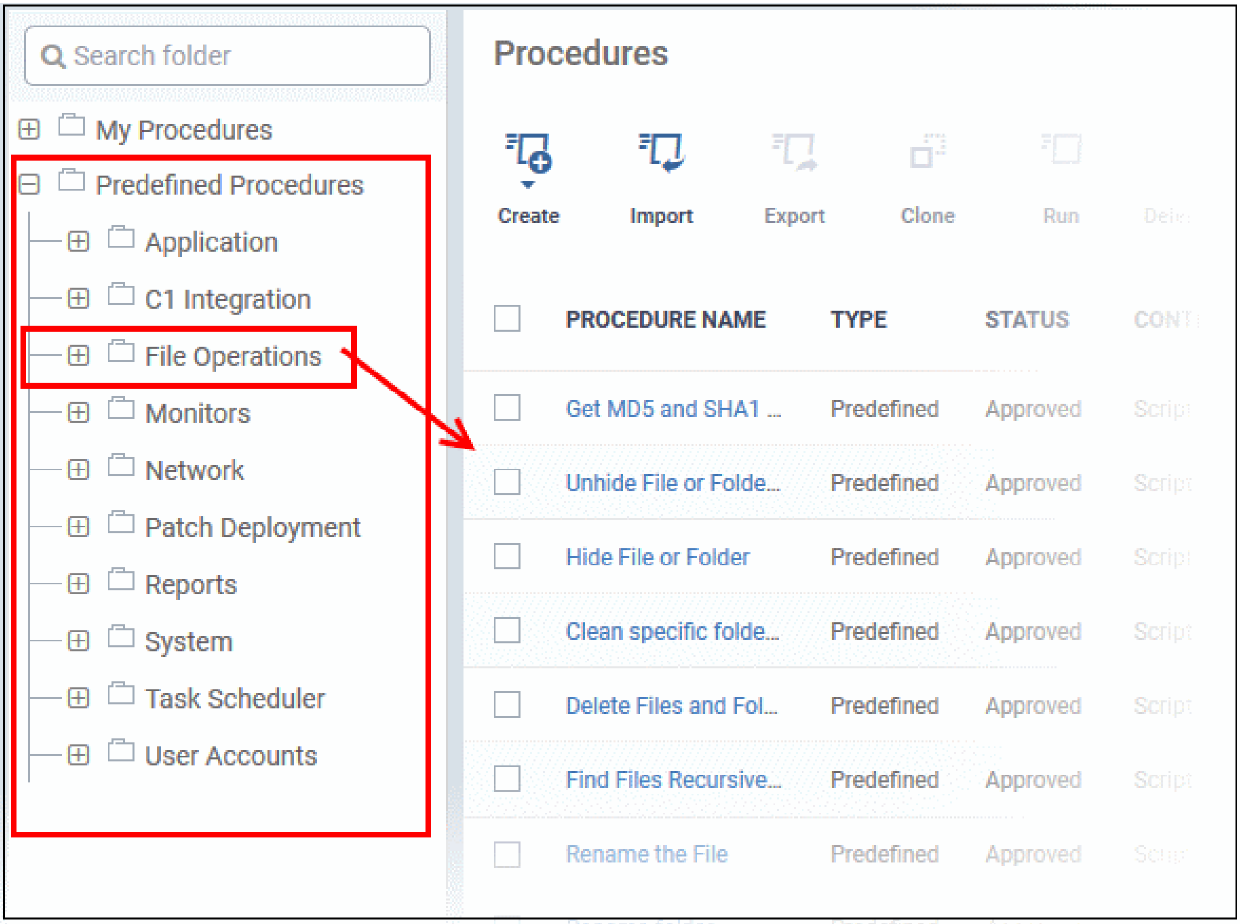
The slider at top-right contains links to help videos on procedures:


herculespopular22@gmail.com)
Logout (herculespopular22@gmail.com)
How to create and run script proce...
03:07

- Use the video guide to quickly learn about creating and running procedures.

### View sub-categories of 'Predefined Procedures':

- Click 'Configuration Templates' > 'Predefined Procedures'
- Click the 'Predefined Procedures' folder
- Open a category folder to view related procedures
- Procedures are shown on the right:



| | PROCEDURE NAME | TYPE | STATUS | CONT |
|---|---|---|---|---|
| □ | Get MD5 and SHA1 ... | Predefined | Approved | Script |
| □ | Unhide File or Folde... | Predefined | Approved | Script |
| □ | Hide File or Folder | Predefined | Approved | Script |
| □ | Clean specific folde... | Predefined | Approved | Script |
| □ | Delete Files and Fol... | Predefined | Approved | Script |
| □ | Find Files Recursive... | Predefined | Approved | Script |
| □ | Rename the File | Predefined | Approved | Script |

The following table lists all predefined categories and procedures:

| Category | Procedures |
|---|---|
| Application | Scripts to run tasks on Comodo and 3rd party applications.<br>Examples include install/uninstall applications, kill running applications, get details on running applications/processes/servers + many other useful scripts. |
| C1 Integration | Scripts to ensure your CD or C1 environment runs smoothly. Examples include |

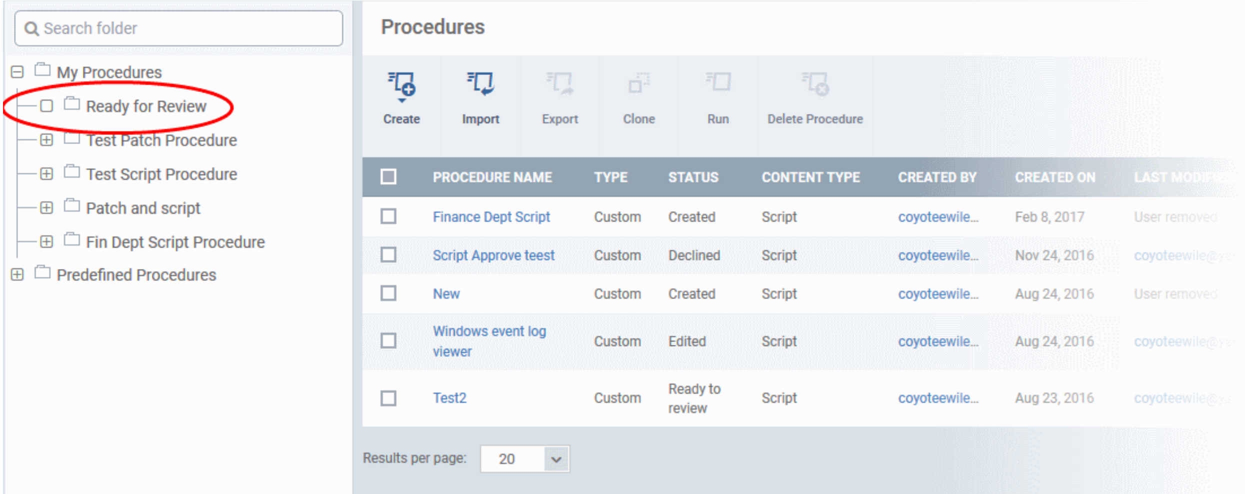
| | |
|---|---|
| | generate a patch report, run a backup operation, and restart the communication client. |
| File Operations | Copy, move/delete files/folders, find and remove duplicate files, compress/decompress folders, clean up temporary files and downloaded files and more. |
| Monitors | Scripts to generate alerts or run specific tasks if a condition is met. For example, 'Alert when USB removable disk is connected to the system'.<br>These can be used in the **monitor settings** of a Windows profile. See **Add Custom Monitoring Conditions** for more details. |
| Network | Scripts to run tasks on, or get information about, your network.<br>For example, view TCP/IP settings, save/restore network configurations, clear DNS cache and more |
| Patch Deployment | Installation and update of OS patches of different categories. |
| Reports | Contains procedures for obtaining various system logs. |
| System | Reboot devices, create restore point, enable/disable USB ports, mapping network drives, running disk defragmentation, fixing disk errors and more. |
| Task Scheduler | Create new tasks and schedule them, run tasks and more. |
| User Accounts | Add/remove domain user to a group, enable/disable user access control (UAC), get UAC status and more. |

Any predefined procedure can be cloned and edited to create a custom procedure. See the following sections for more details.

- **Import / Export / Clone Procedures**
- **Edit Procedures**
- **Add a Procedure to a Profile / Procedure Schedules**

**To view 'My Procedures':**

- Click 'Configuration Templates' > 'Procedures'. Expand the 'My Procedures' folder. Each folder has sub-folders which display procedures under specific categories (for example, 'Ready for review').

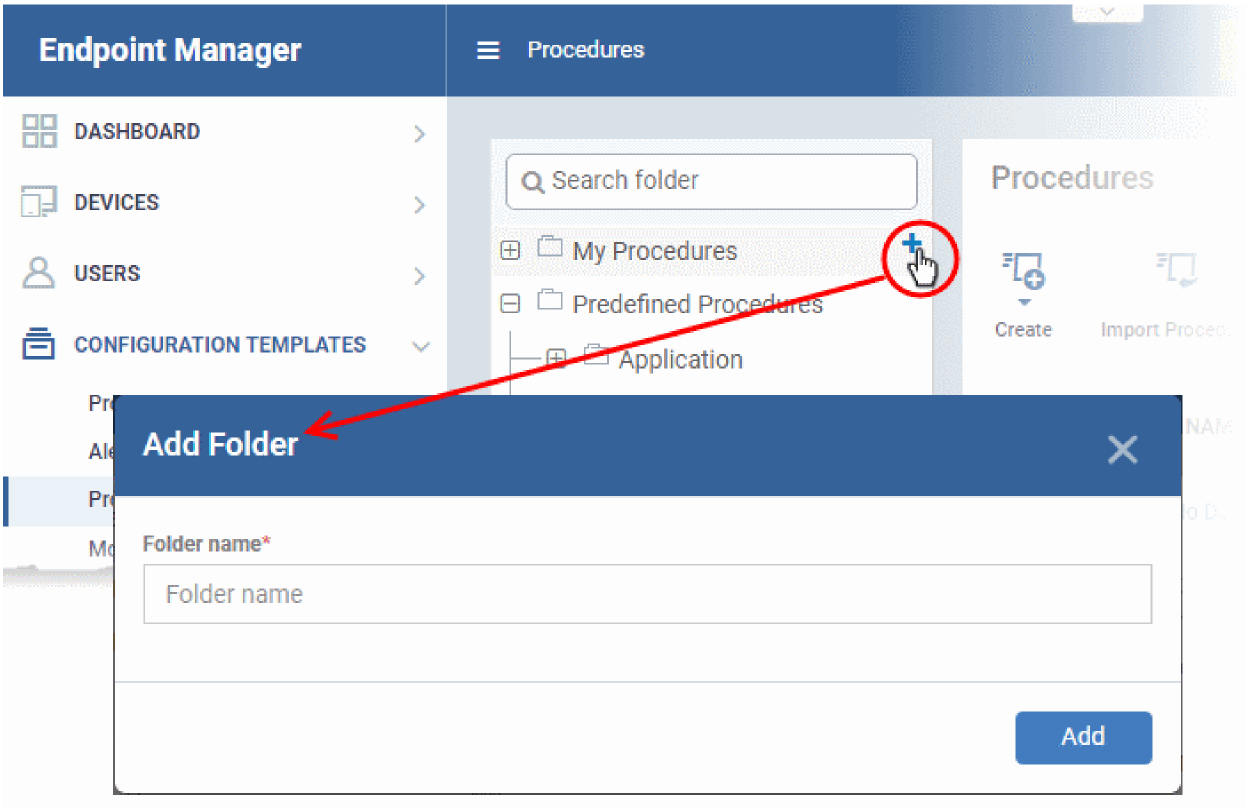


| ☐ | PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON | LAST MODIF |
|---|---|---|---|---|---|---|---|
| ☐ | Finance Dept Script | Custom | Created | Script | coyoteewile... | Feb 8, 2017 | User removed |
| ☐ | Script Approve teest | Custom | Declined | Script | coyoteewile... | Nov 24, 2016 | coyoteewile@y |
| ☐ | New | Custom | Created | Script | coyoteewile... | Aug 24, 2016 | User removed |
| ☐ | Windows event log viewer | Custom | Edited | Script | coyoteewile... | Aug 24, 2016 | coyoteewile@y |
| ☐ | Test2 | Custom | Ready to review | Script | coyoteewile... | Aug 23, 2016 | coyoteewile@y |

Results per page: 20

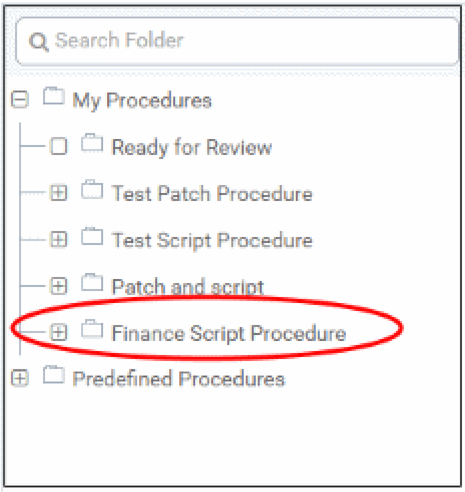
**To add a sub folder to the My Procedures folder:**

- Place your mouse on the 'My Procedures' folder and click '+' beside it



- Enter a name for the sub-folder to be created in the 'Add Folder' dialog and click 'Add'

The sub-folder will be created and displayed under 'My Procedures'



You can also add sub-folders of a sub-folder. Once sub folders are created, you can create new procedures inside them or import/clone predefined procedures.

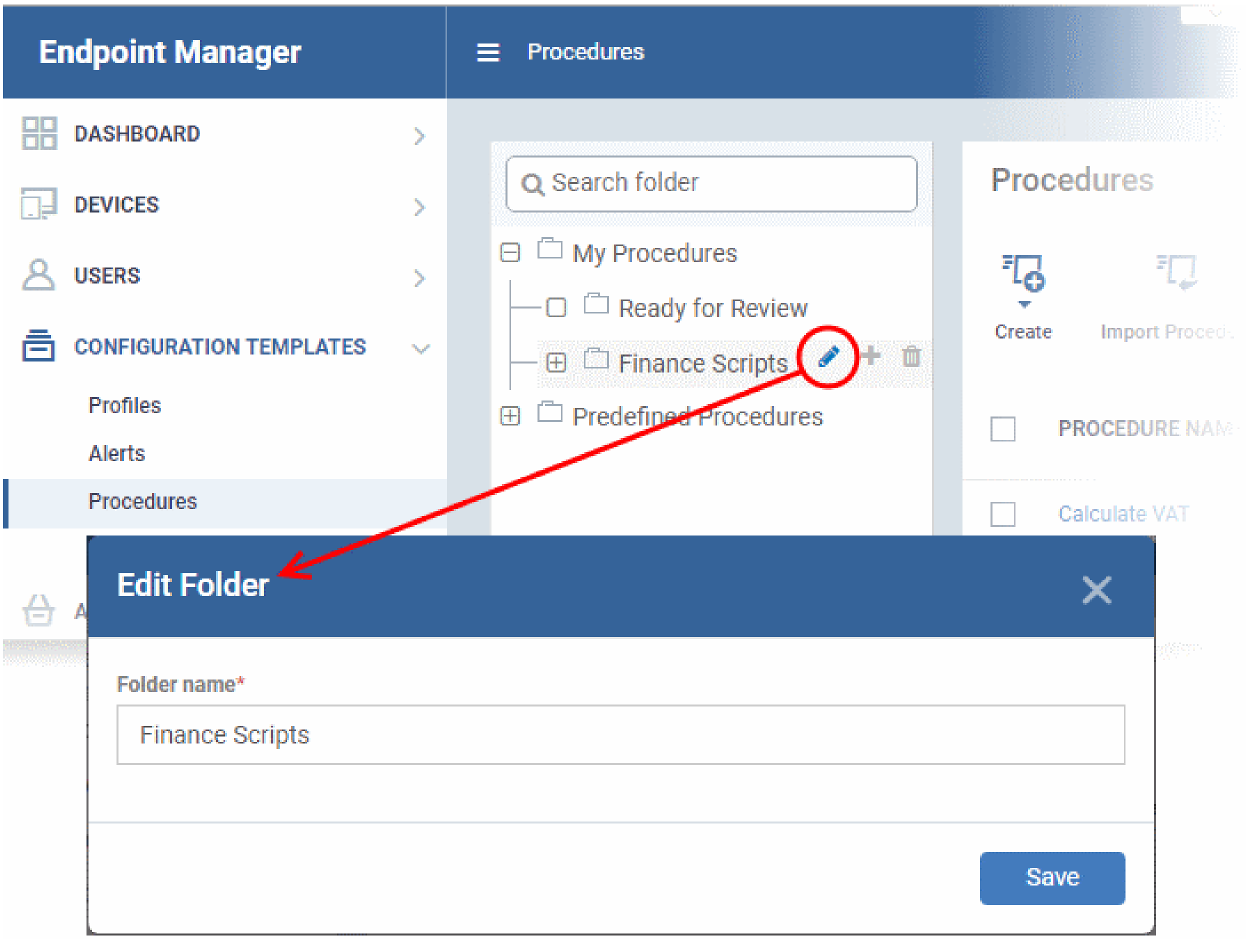
See the following sections for more details about:

- Create a new procedure
- Import / Export / Clone a procedure
- Edit a Procedures

**To edit the name of a sub folder under 'My Procedures'**

- Place your mouse on the sub folder and click the pencil symbol beside it

- Enter a new name for the sub-folder in the 'Edit Folder' dialog and click 'Save'



Folder name*

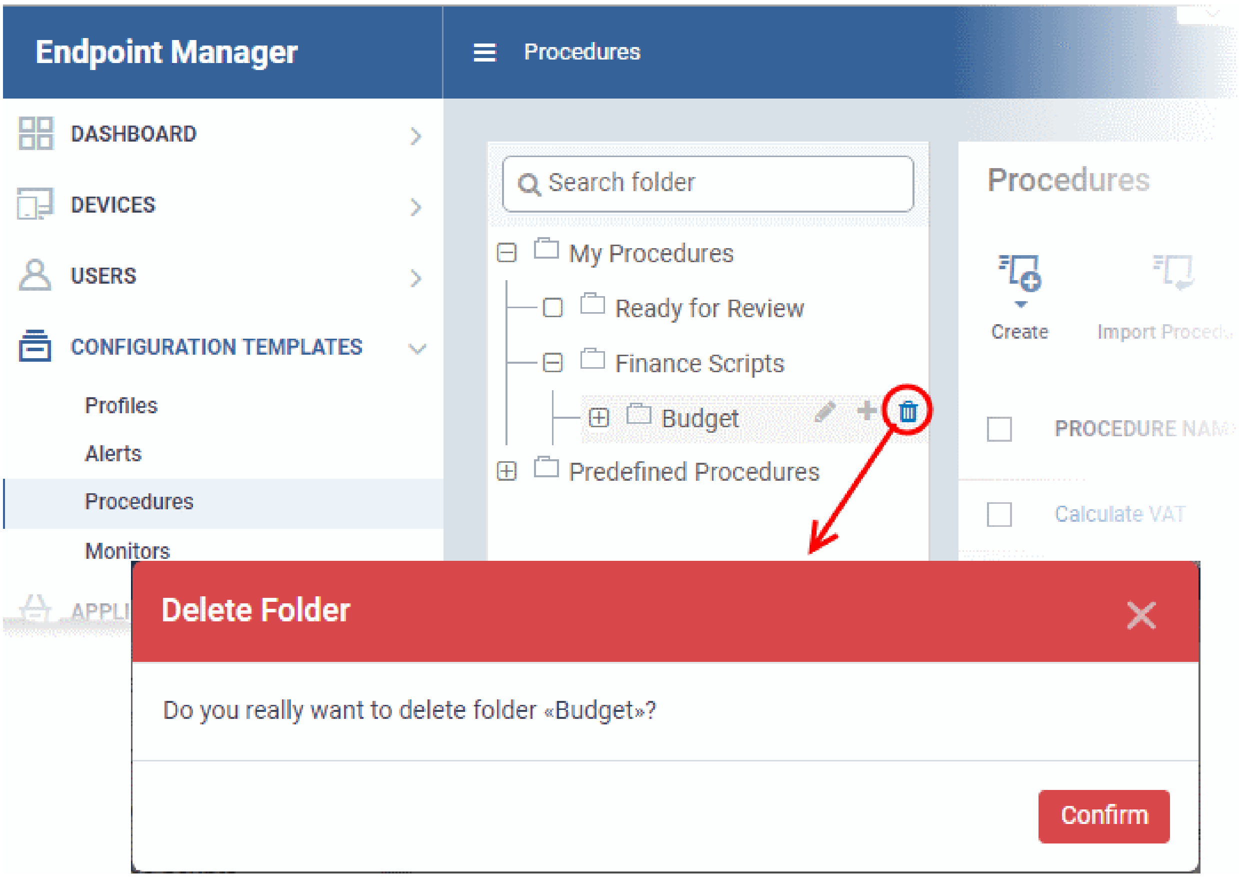
Finance Scripts

The folder name will be updated in folder tree.

**Note**: You cannot edit or delete the 'Ready for Review' folder.

**To delete a sub folder under 'My Procedures' folder:**

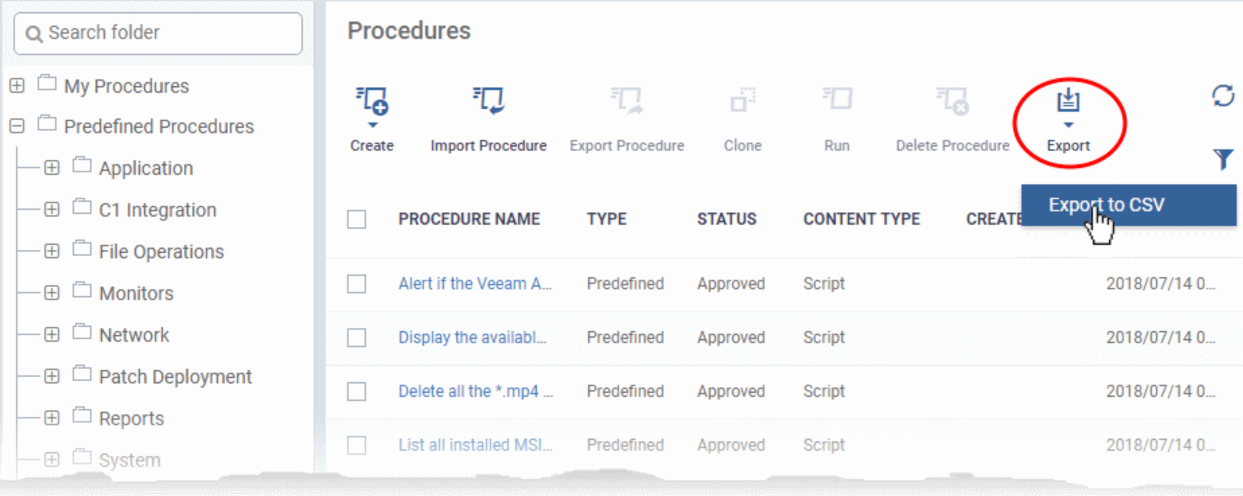
- Place your mouse on the sub folder and click the trash can symbol beside it



- Click 'Confirm' to update the tree.

## Export the Procedure List

- Click 'Configuration Templates' > 'Procedures'.
- Click 'My Procedures' or 'Predefined Procedures'
- Click the 'Export' button then choose 'Export to CSV':



| PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATE |
|---|---|---|---|---|
| Alert if the Veeam A... | Predefined | Approved | Script | 2018/07/14 0... |
| Display the availabl... | Predefined | Approved | Script | 2018/07/14 0... |
| Delete all the *.mp4 ... | Predefined | Approved | Script | 2018/07/14 0... |
| List all installed MSI... | Predefined | Approved | Script | 2018/07/14 0... |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

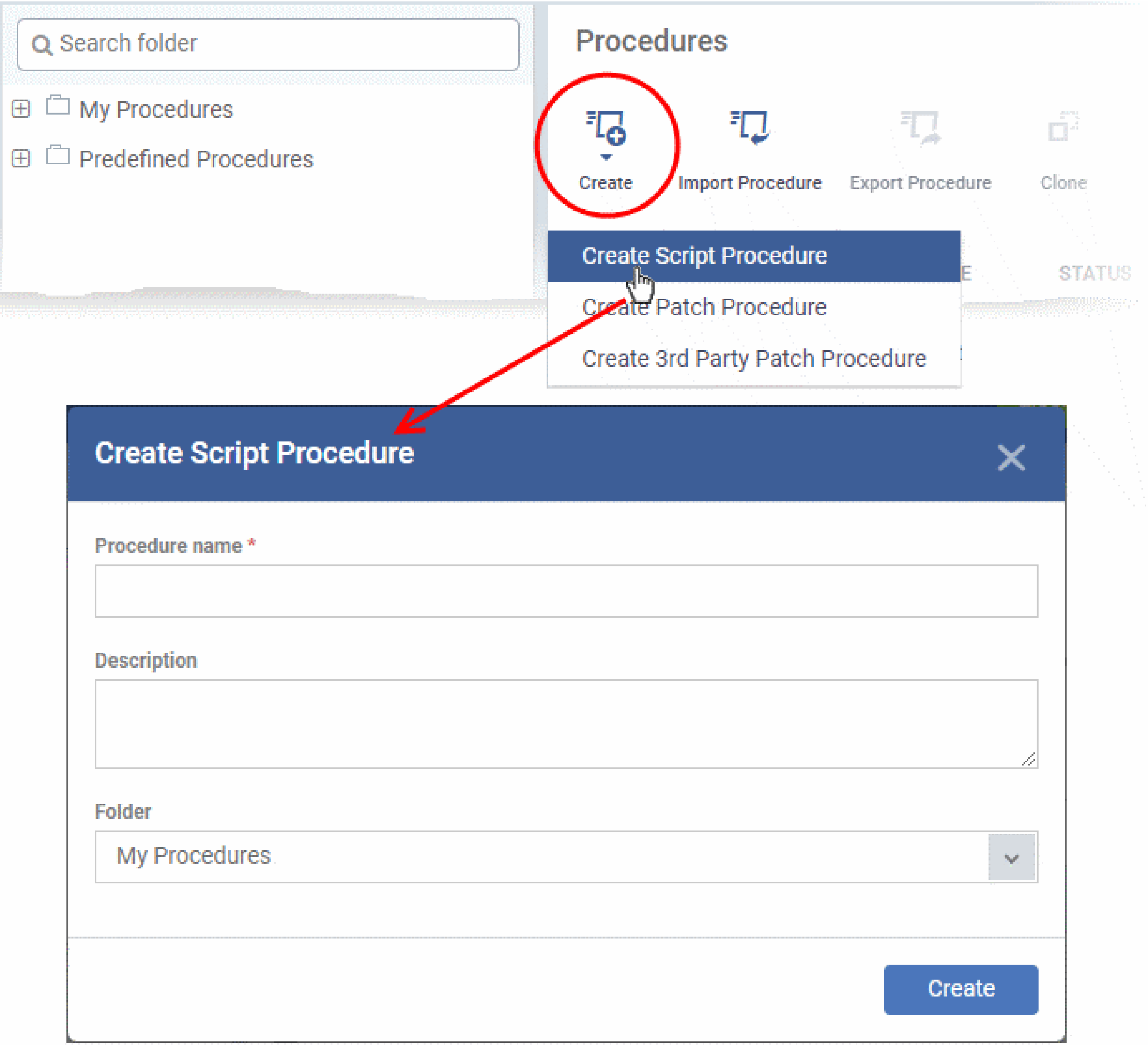
## 6.6.2. Create a Custom Procedure

Endpoint Manager lets you create custom script/patch procedures to achieve specific tasks. Click the following links to find out more:

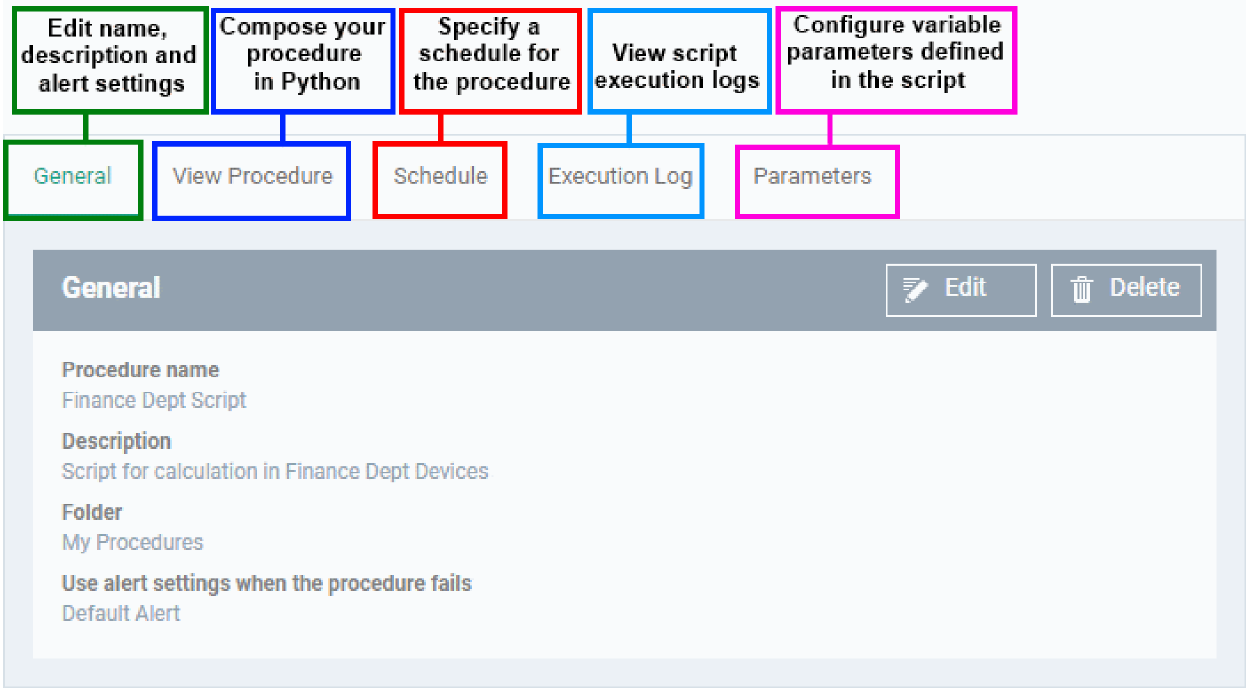
- Create a custom script procedure
- Create a custom patch procedure
- Create a custom 3rd Party application patch procedure

### To create a custom script procedure

- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create Script Procedure'



- Enter a name and description and specify the folder where it should be saved. If required, you can create new sub-folders under 'My Procedures' in the 'Procedures' area.
- After saving, you will be taken to the procedure configuration screen:


Edit name, description and alert settings
Compose your procedure in Python
Specify a schedule for the procedure
View script execution logs
Configure variable parameters defined in the script
General
View Procedure
Schedule
Execution Log
Parameters
General
Edit
Delete

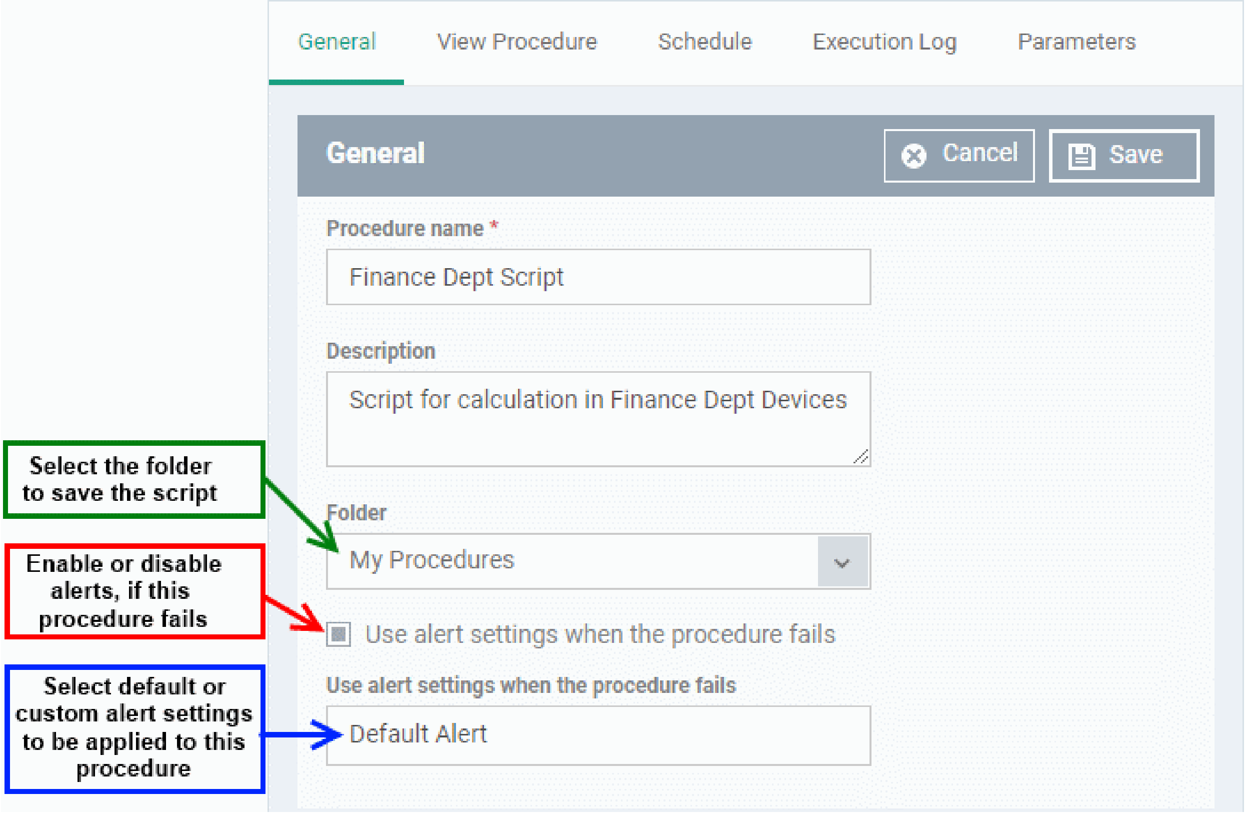
Procedure name
Finance Dept Script

Description
Script for calculation in Finance Dept Devices

Folder
My Procedures

Use alert settings when the procedure fails
Default Alert

- Click 'Edit' to modify the basic settings:


General
View Procedure
Schedule
Execution Log
Parameters
General
Cancel
Save
Select the folder to save the script
Enable or disable alerts, if this procedure fails
Select default or custom alert settings to be applied to this procedure

Procedure name *
Finance Dept Script

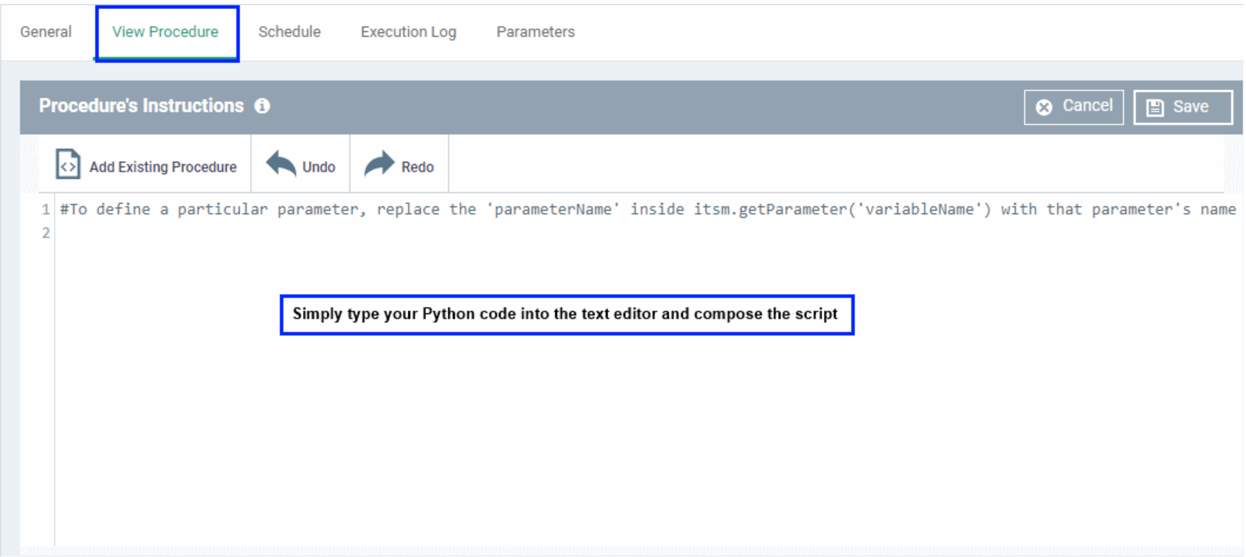
Description
Script for calculation in Finance Dept Devices

Folder
My Procedures

☑ Use alert settings when the procedure fails

Use alert settings when the procedure fails
Default Alert

- Default Alert - You can view the settings of the default alert in 'Configuration Templates' > 'Alerts'. You can create custom alert settings if required from this interface.
- Click 'Save' to save your settings.
- Click the 'View Procedure' tab followed by 'Edit' to define a Python script for your procedure. The built-in text editor lets you to compose your script:

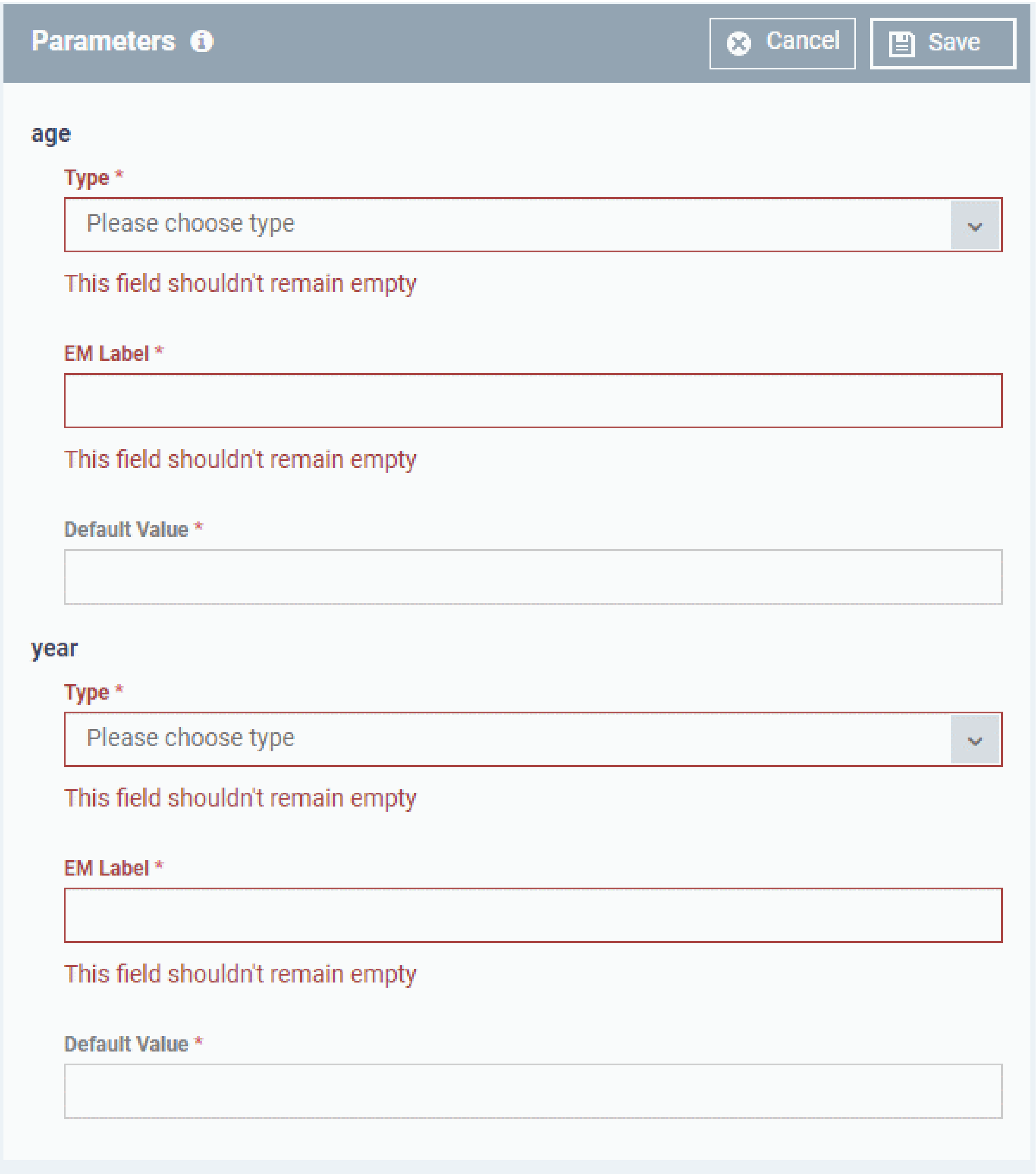


```
#To define a particular parameter, replace the 'parameterName' inside itsm.getParameter('variableName') with that parameter's name
```

Simply type your Python code into the text editor and compose the script

- You can include variable parameters whose values are populated when the procedure runs.
- To define variable parameters in the script:
  - Click the 'View Procedure' tab followed by 'Edit'
  - In the text editor, type the parameter name and enter the value as itsm.getParameter('parameter name'). Examples:
    - Age = itsm.getParameter('age')
    - Year = itsm.getParameter('year')
  - The specified variables will become available in the 'Parameters' tab. You can define the type, label and default values for them.
  - Click the 'Parameters' tab after completing the script under the 'View Procedure' tab

An example is shown below:



age

Type *

Please choose type

This field shouldn't remain empty

EM Label *

This field shouldn't remain empty

Default Value *

year

Type *

Please choose type

This field shouldn't remain empty

EM Label *

This field shouldn't remain empty

Default Value *

For each parameter you should configure the following:

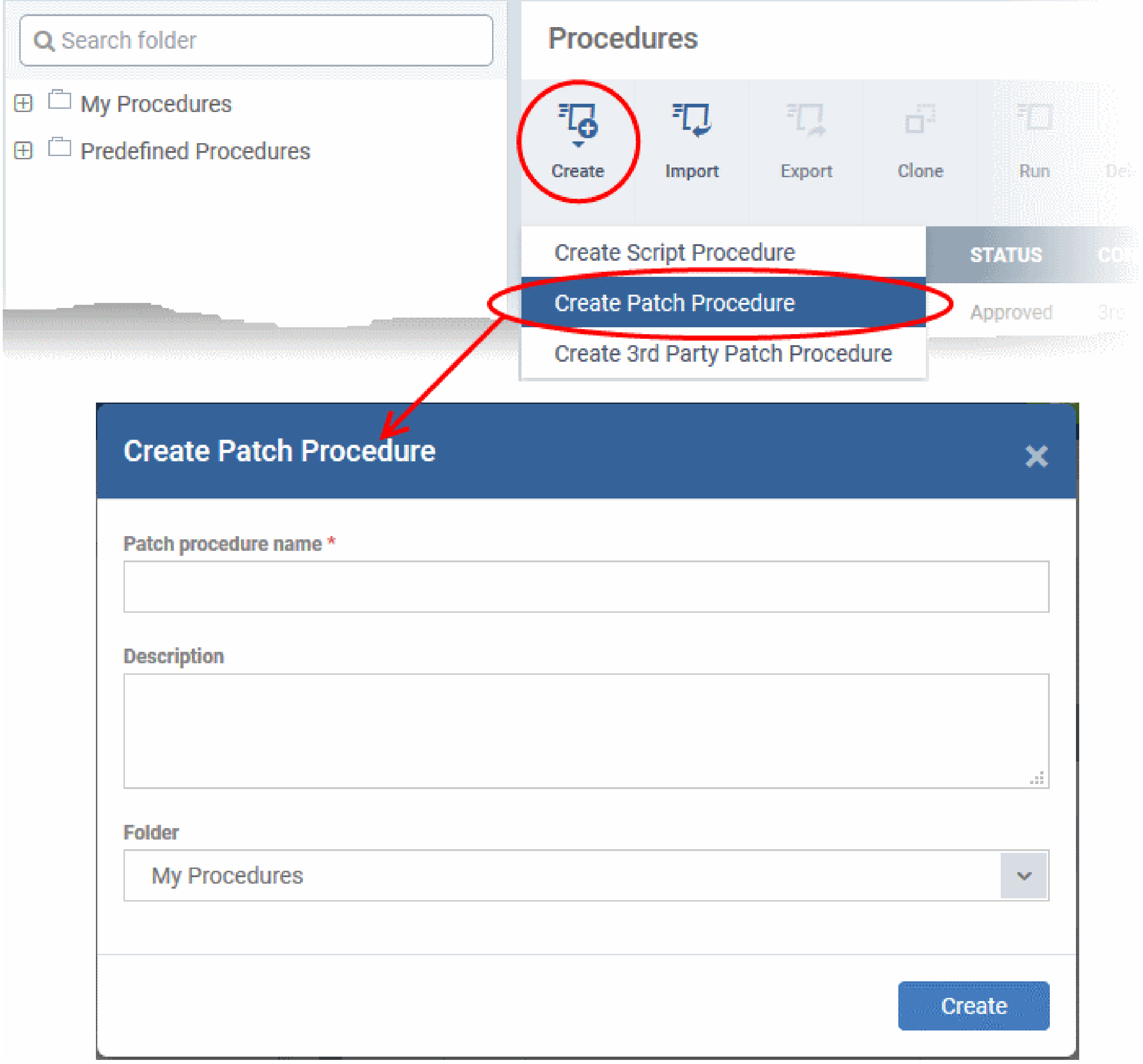
- **Type** - Choose the category of variable. The supported types are:
  - Integer
  - Double
  - String
  - List
- **EM Label** - Enter a name for the variable.
- **Default Value** - Enter a value for the parameter to be taken when no value is input during run-time

- Click 'Save' to save the script.
- After saving your script you need to **approve** it before it can be deployed in a profile.
- The 'Schedule' tab will be auto-populated once you deploy the procedure to a configuration profile and create a schedule for the procedure to run in the profile. Refer to the section **Add a Procedure to a Profile / Procedure Schedules** for more details.

- The 'Execution Log' tab will be populated after the procedure has successfully run on end-points. You can view the history of execution of this procedure at anytime by selecting this procedure from the Procedures interface and clicking the 'Execution Log' tab.
- Note 1. Comodo runs a free script library at https://scripts.comodo.com/ which contains Python scripts covering a wide range of tasks. Feel free to try any script that fits your needs. You can also use this site to request a new script for a particular task you think will be useful. You can contribute your own scripts to the MSP forum at https://forum.mspconsortium.com/forum/script-library
- Note 2. You can also use the Import and Clone features if you wish to create a new procedure using an existing procedure as a starting point

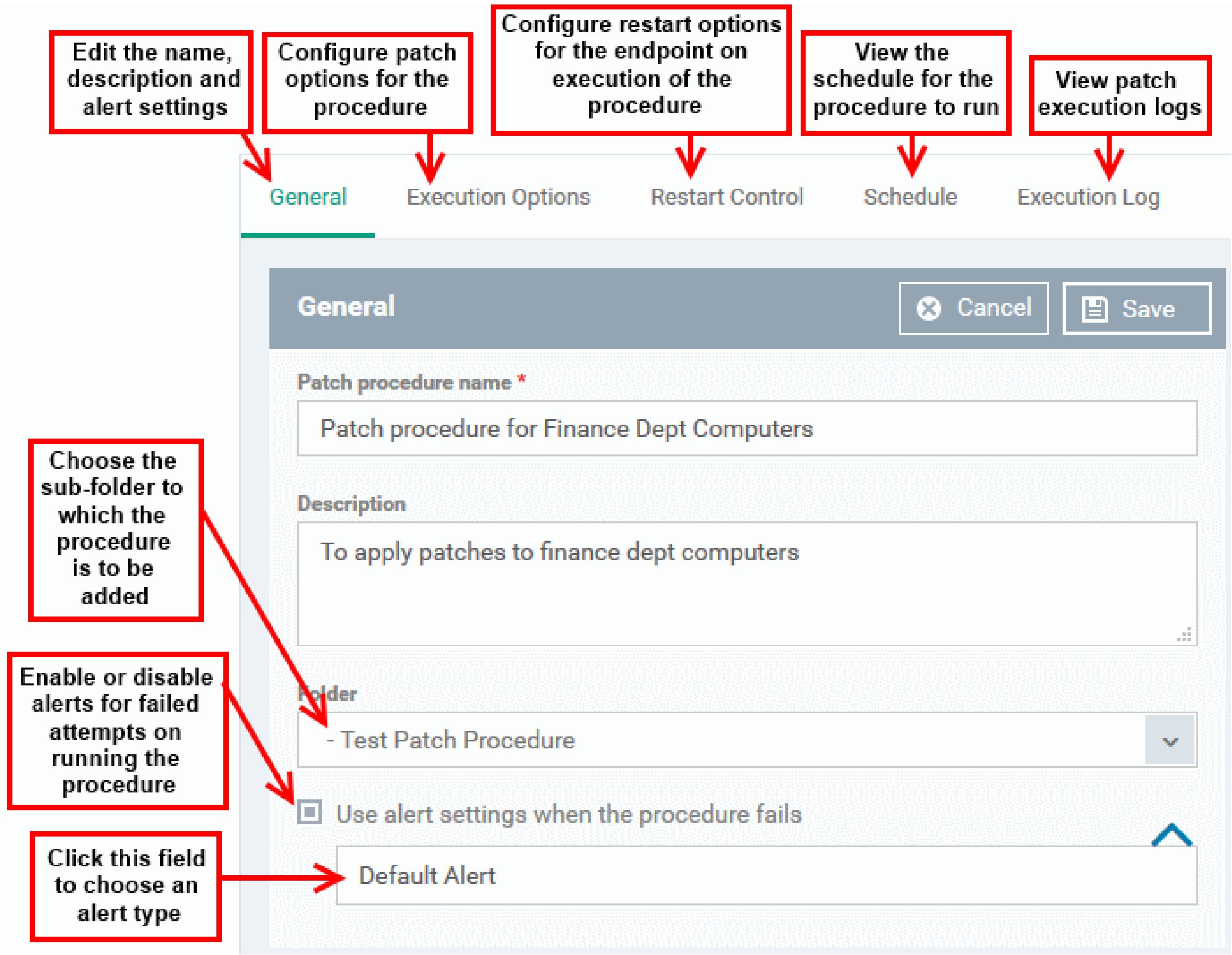
### To create a custom patch procedure

- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create Patch Procedure'



- Enter a name and description and specify the folder where it should be saved. If required, you can create new sub-folders under 'My Procedures' in the 'Procedures' area.
- After saving, you will be taken to the procedure configuration screen:

## Procedure Configuration


Edit the name, description and alert settings
Configure patch options for the procedure
Configure restart options for the endpoint on execution of the procedure
View the schedule for the procedure to run
View patch execution logs
General
Execution Options
Restart Control
Schedule
Execution Log
General
Cancel
Save
Choose the sub-folder to which the procedure is to be added
Enable or disable alerts for failed attempts on running the procedure
Click this field to choose an alert type

Patch procedure name *

Patch procedure for Finance Dept Computers

Description

To apply patches to finance dept computers

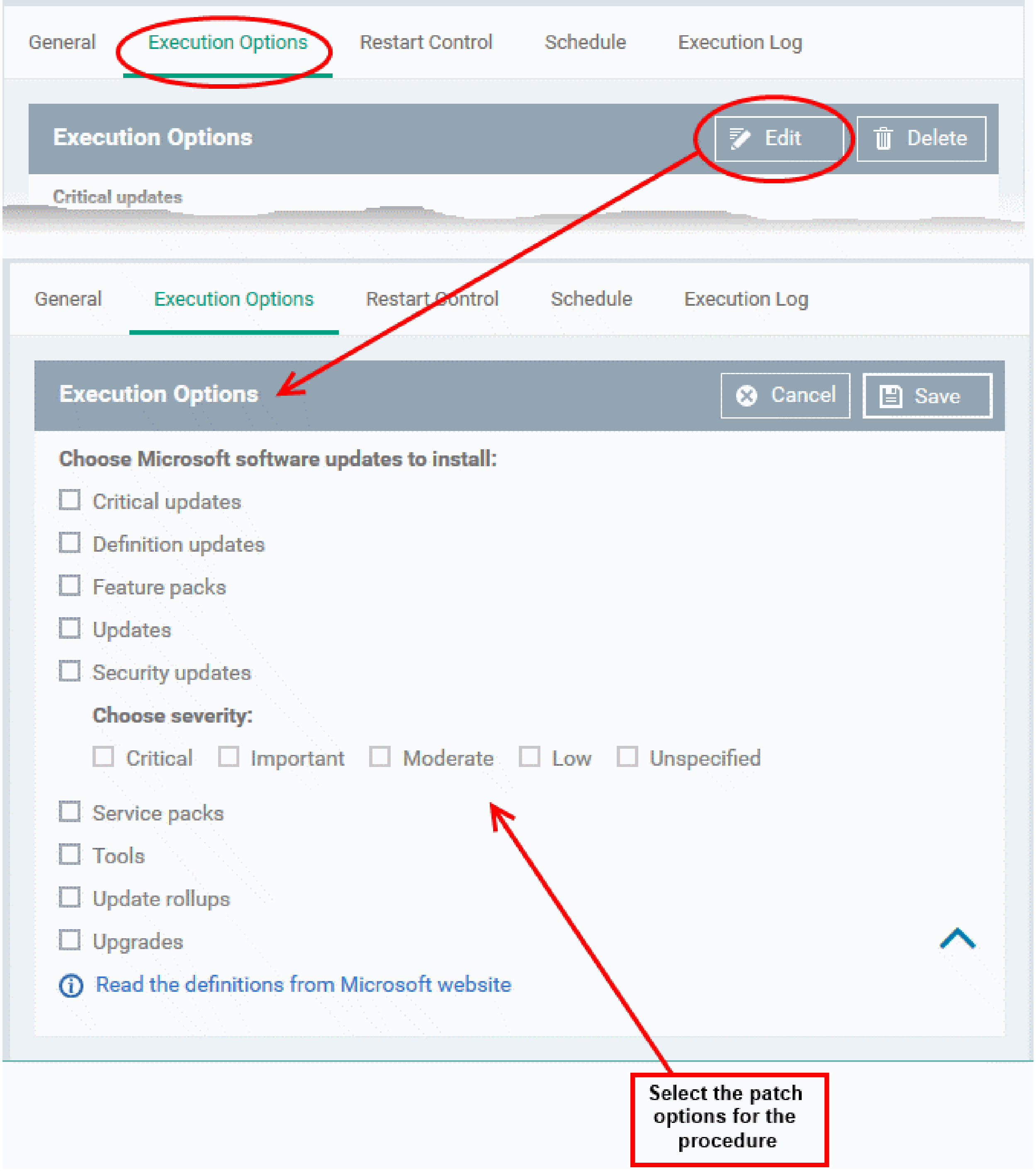
Folder

- Test Patch Procedure

☑ Use alert settings when the procedure fails

Default Alert

- To configure patch options for your procedure, click the 'Execution Options' tab followed by the 'Edit' button. You can select the Microsoft software updates required for the procedure from the options.



Choose Microsoft software updates to install:

- □ Critical updates
- □ Definition updates
- □ Feature packs
- □ Updates
- □ Security updates

Choose severity:

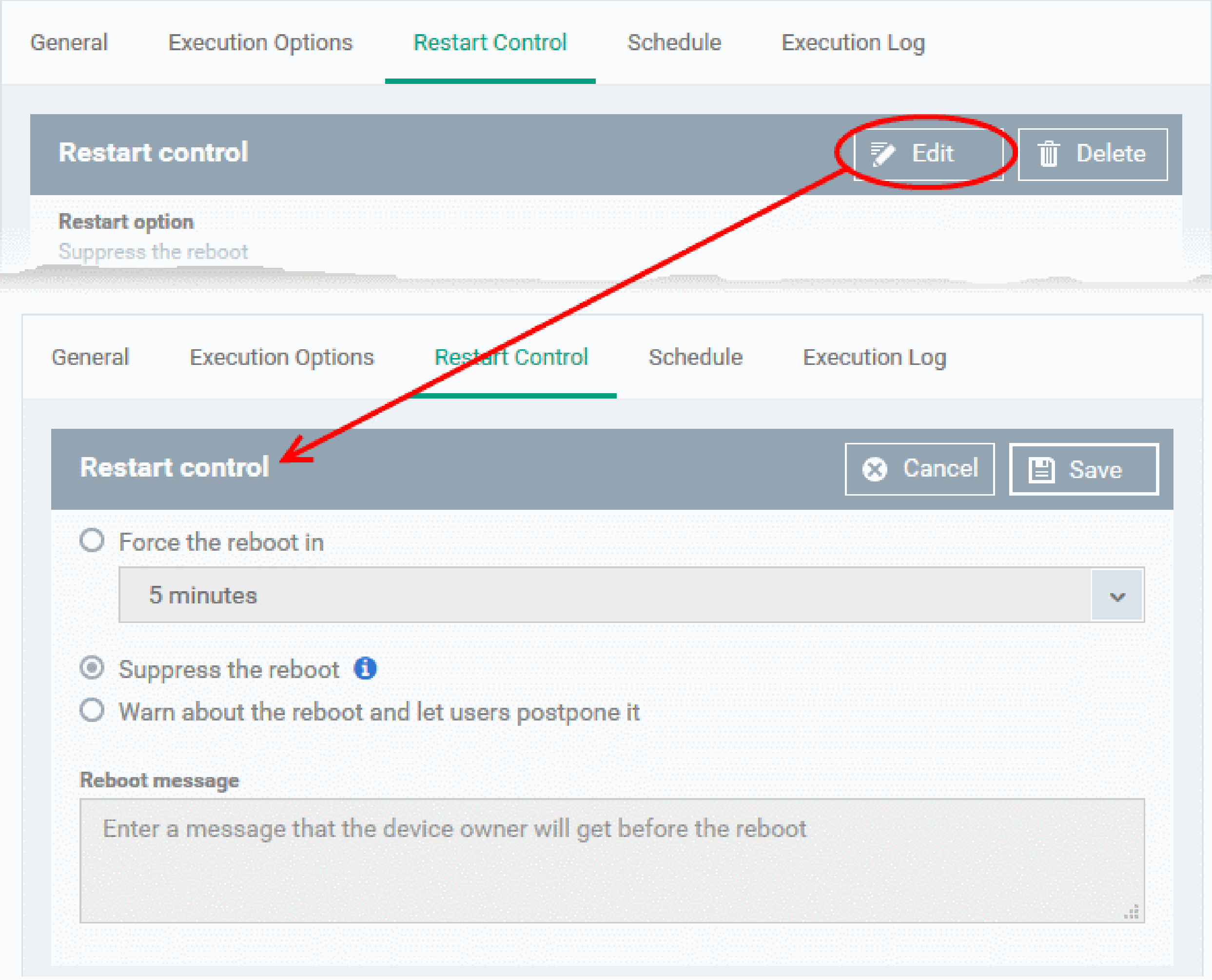
□ Critical □ Important □ Moderate □ Low □ Unspecified

- □ Service packs
- □ Tools
- □ Update rollups
- □ Upgrades

Read the definitions from Microsoft website

Select the patch options for the procedure

- Click the link 'Read the definitions from Microsoft website' link to view patch details.
- Choose which types of patch the procedure should install and click 'Save'
- Click the 'Restart Control' tab followed by the 'Edit' button to configure restart options for the endpoint after the procedure has run successfully.



Restart control

Restart option
Suppress the reboot

Restart control

○ Force the reboot in

5 minutes

● Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message

Enter a message that the device owner will get before the reboot

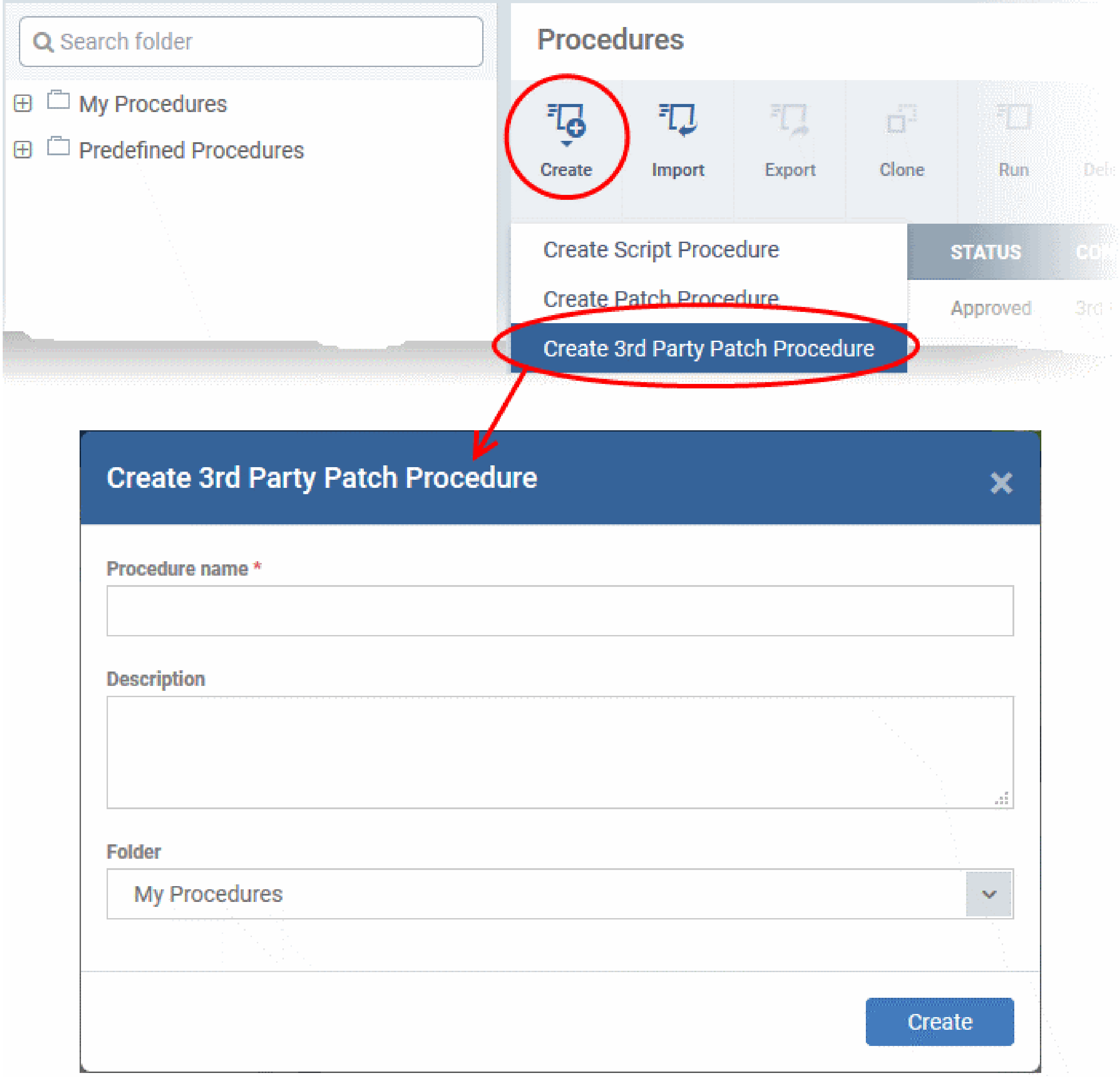
- You can choose to:
  - Continue the operation of the endpoint without restart by selecting 'Suppress the reboot'
  - Force restart the endpoint a certain period of time after the procedure has completed.

    OR
  - Display a warning to the user and let them postpone the restart. Type a message for the user if you choose this option.
- The 'Schedule' tab will be auto-populated once you add the procedure to a configuration profile and schedule its execution. See **Add a Procedure to a Profile / Procedure Schedules** for more details.
- The 'Execution Log' will be auto-populated after the procedure has been successful executed as part of a profile. You can view a history of executions at anytime by selecting this procedure in the 'Procedures' interface and clicking the 'Execution Log' tab.
- After saving, your patch procedure will be automatically approved, added to the 'Procedures' list and can be deployed in a profile.

Important Note: Patches that are hidden by administrators will not be executed. Refer to the section ' **Installing OS Patches on Windows Endpoints**' for more details.

### To create a custom 3rd party patch procedure

- Click 'Configuration Templates' > 'Procedures' > 'Create' > 'Create 3rd Party Patch Procedure'



Create 3rd Party Patch Procedure

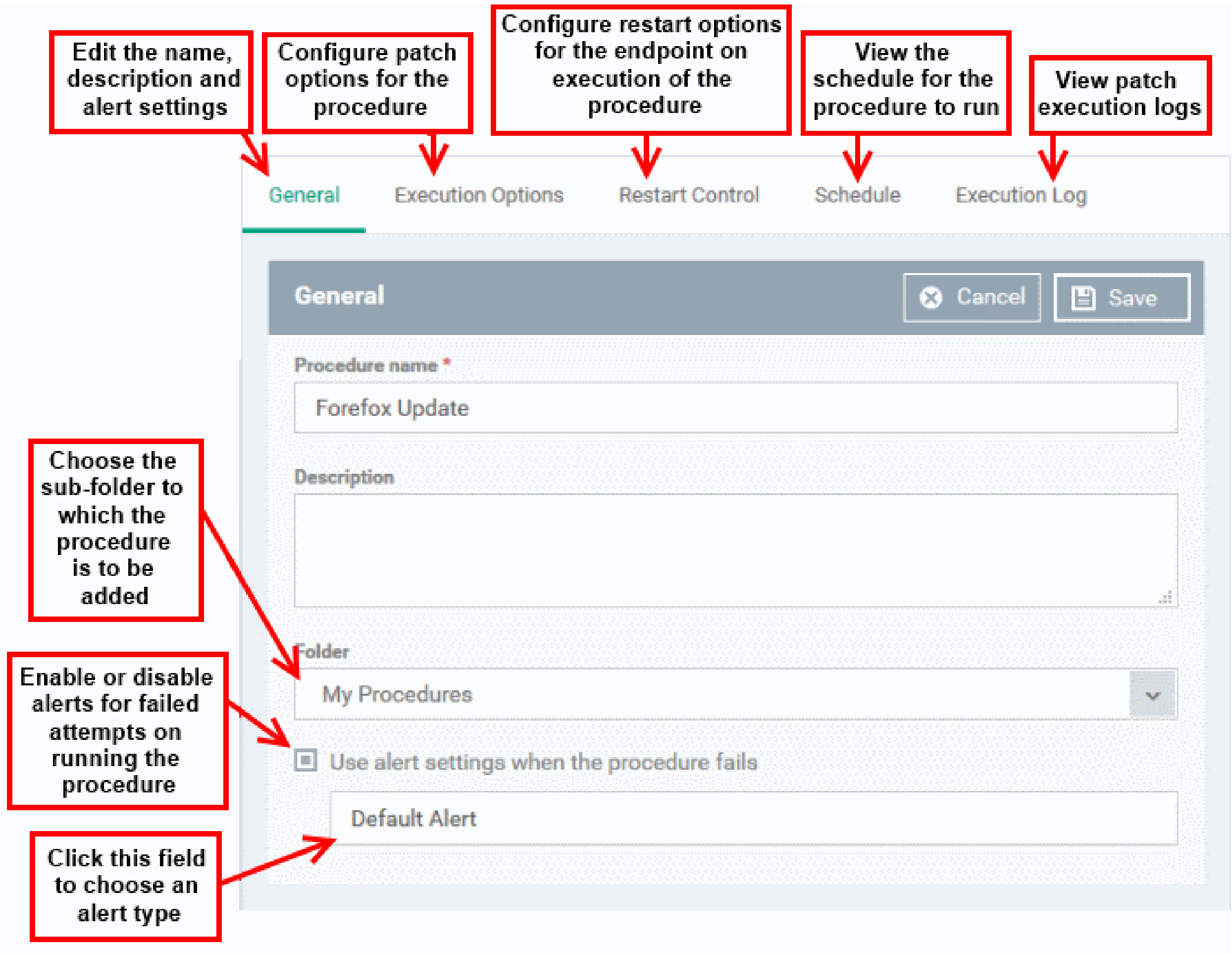
Procedure name *

Description

Folder

My Procedures

- Enter a name and description for your 3rd party patch procedure and specify the folder in which you want to save it. After saving, you will be taken to the procedure configuration screen with the 'General' section open
- Click 'Edit' if you want to change the general parameters.


Edit the name, description and alert settings
Configure patch options for the procedure
Configure restart options for the endpoint on execution of the procedure
View the schedule for the procedure to run
View patch execution logs
General
Execution Options
Restart Control
Schedule
Execution Log
General
Cancel
Save
Choose the sub-folder to which the procedure is to be added
Enable or disable alerts for failed attempts on running the procedure
Click this field to choose an alert type

Procedure name * Forefox Update

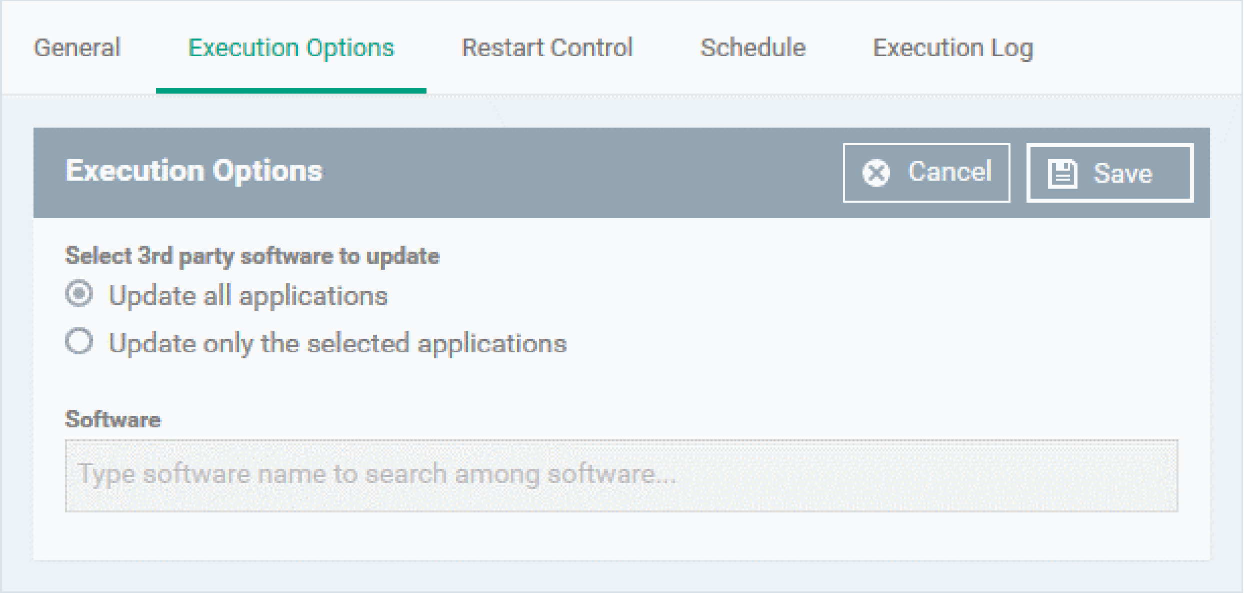
Description

Folder My Procedures

☐ Use alert settings when the procedure fails

Default Alert

- To configure patch options for your procedure, click the 'Execution Options' tab followed by the 'Edit' button. You can select the applications to be updated from the options.



Select 3rd party software to update

● Update all applications

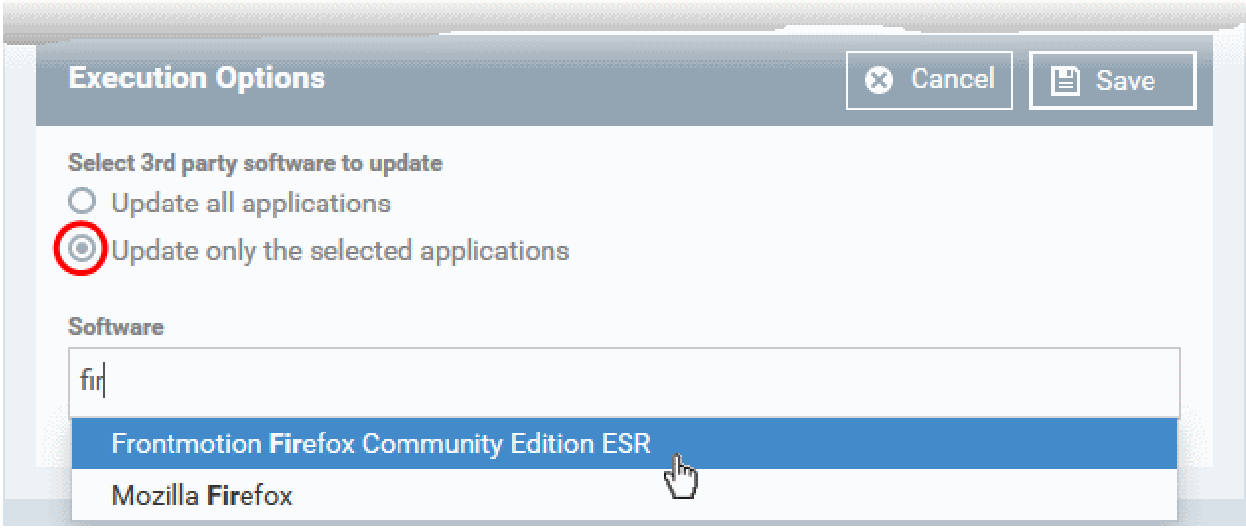
○ Update only the selected applications

Software

Type software name to search among software...

- **Select 3rd party software to update -** Allows you to choose whether all upgradable applications identified at the endpoint to be updated or only specific application(s) is/are to be updated.
  - **Update all applications -** Select this option if you want all outdated applications in the endpoint to be updated on running the procedure

- **Update only the selected applications -** Select this option if you want only specified applications are to be updated on the endpoint, then specify the applications to be updated.
    - Start entering the first few characters of the application. The upgradable applications identified from all managed endpoints and matching the search criteria will be displayed as options
    - Select the application from the list



Select 3rd party software to update

○ Update all applications

● Update only the selected applications

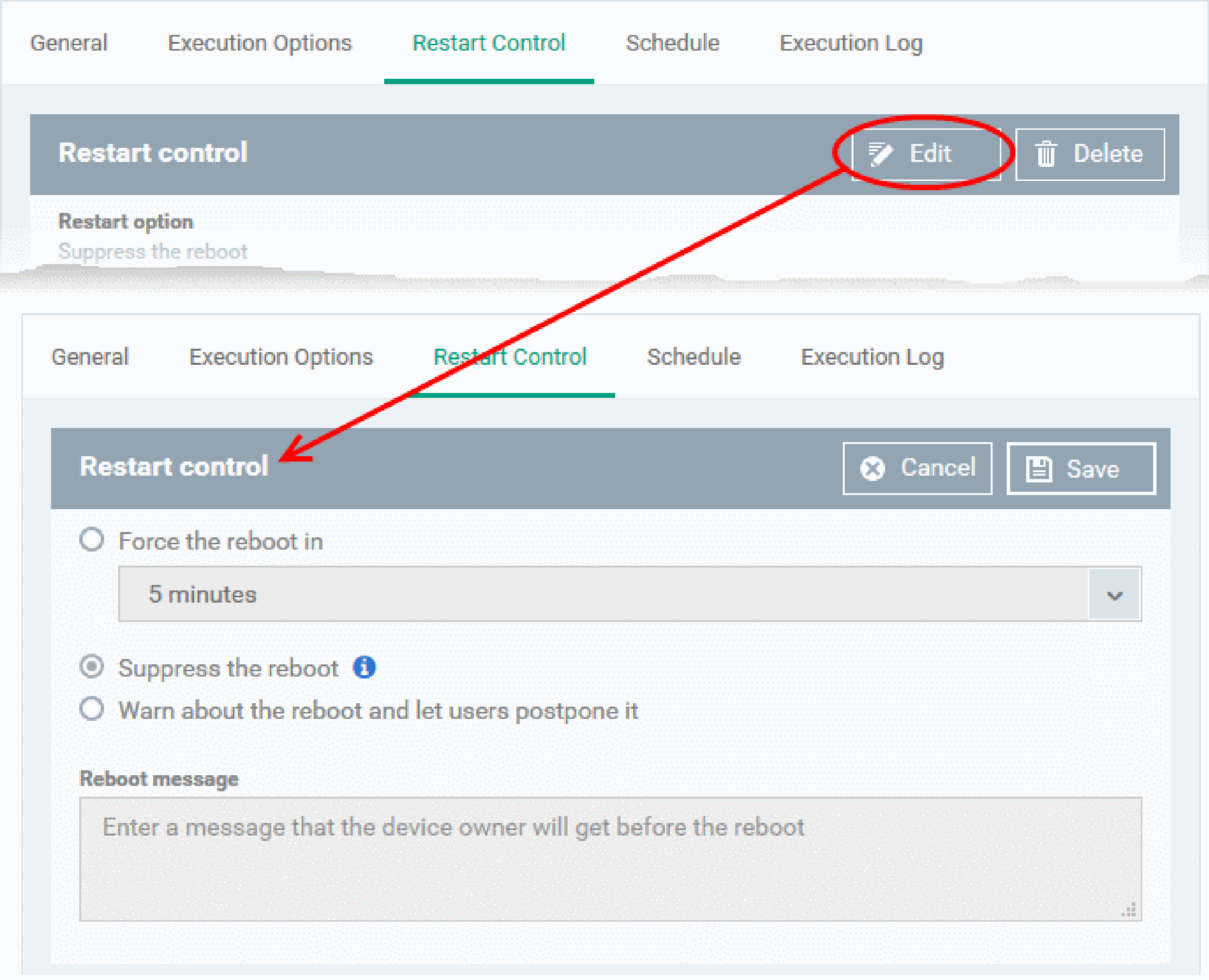
Software

fir

Frontmotion Firefox Community Edition ESR

Mozilla Firefox

- Click 'Save'
- Click the 'Restart Control' tab followed by the 'Edit' button to configure restart options for the endpoint after the procedure has run successfully.



Restart option

Suppress the reboot

○ Force the reboot in

5 minutes

● Suppress the reboot

○ Warn about the reboot and let users postpone it

Reboot message

Enter a message that the device owner will get before the reboot

- You can choose to:
    - Continue the operation of the endpoint without restart by selecting 'Suppress the reboot'
    - Force restart the endpoint a certain period of time after the procedure has completed.

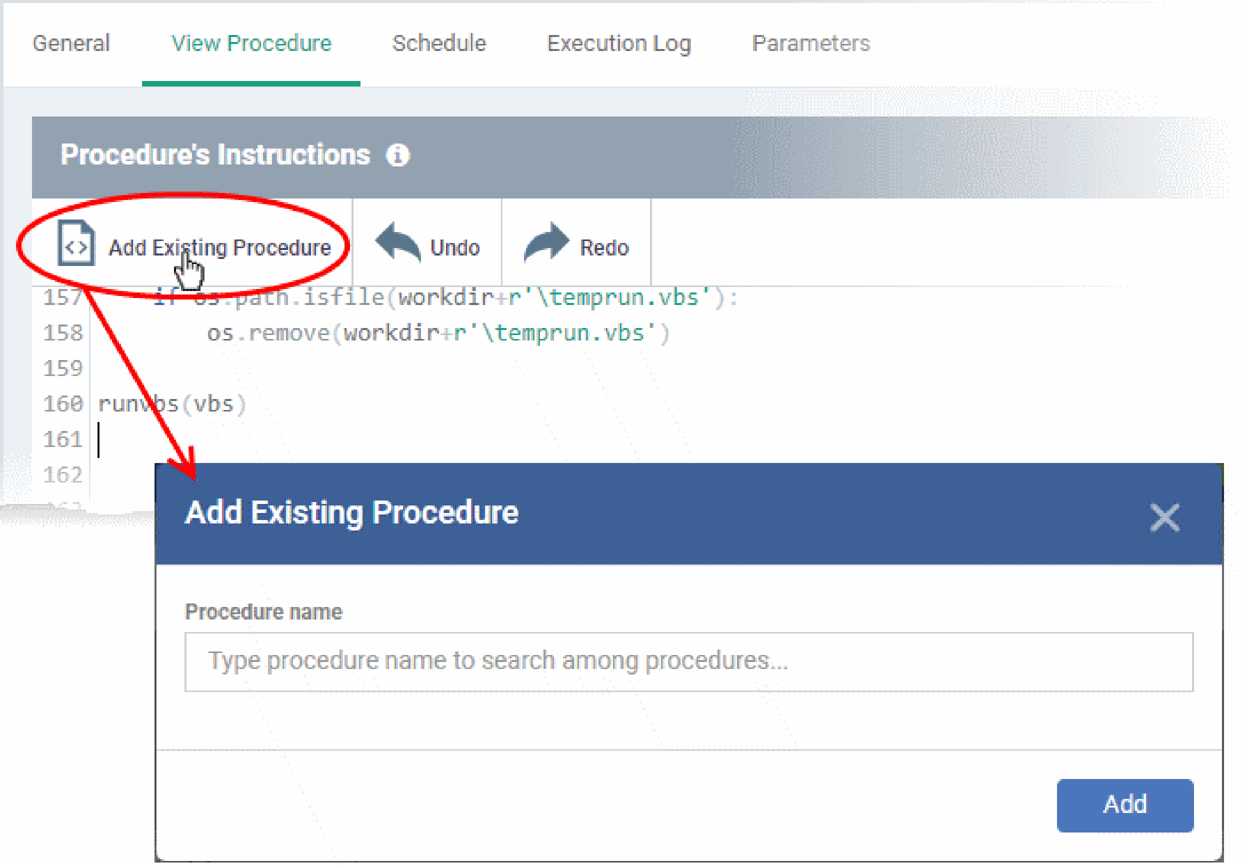
      OR
    - Display a warning to the user and let them postpone the restart. Type a message for the user if you choose this option.
- The 'Schedule' tab will be auto-populated once you add the procedure to a configuration profile and schedule its execution. See **Add a Procedure to a Profile / Procedure Schedules** for more details.
- The 'Execution Log' will be auto-populated after the procedure has been successful executed as part of a profile. You can view a history of executions at anytime by selecting this procedure in the 'Procedures' interface and clicking the 'Execution Log' tab.
- After saving, your patch procedure will be automatically approved, added to the 'Procedures' list and can be deployed in a profile.

## 6.6.3. Combine Procedures to Build Broader Procedures

Note - this section only applies to script procedures, not patch procedures.

**To incorporate a script from another procedure:**

- Open your **custom procedure** and click the 'View Procedure' tab, then click 'Edit' on the right
- Position your mouse cursor at the place in your script where you wish to add the new code
- Click 'Add Existing Procedure'
- Type the name of the procedure whose script you want to import
- Click 'Add'. The code will be added to your existing script at the place you specified.
- You can, of course, subsequently modify the script as required.



```
    if os.path.isfile(workdir+r'\temprun.vbs'):
        os.remove(workdir+r'\temprun.vbs')

runvbs(vbs)
```

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

## 6.6.4. Review / Approve / Decline New Procedures

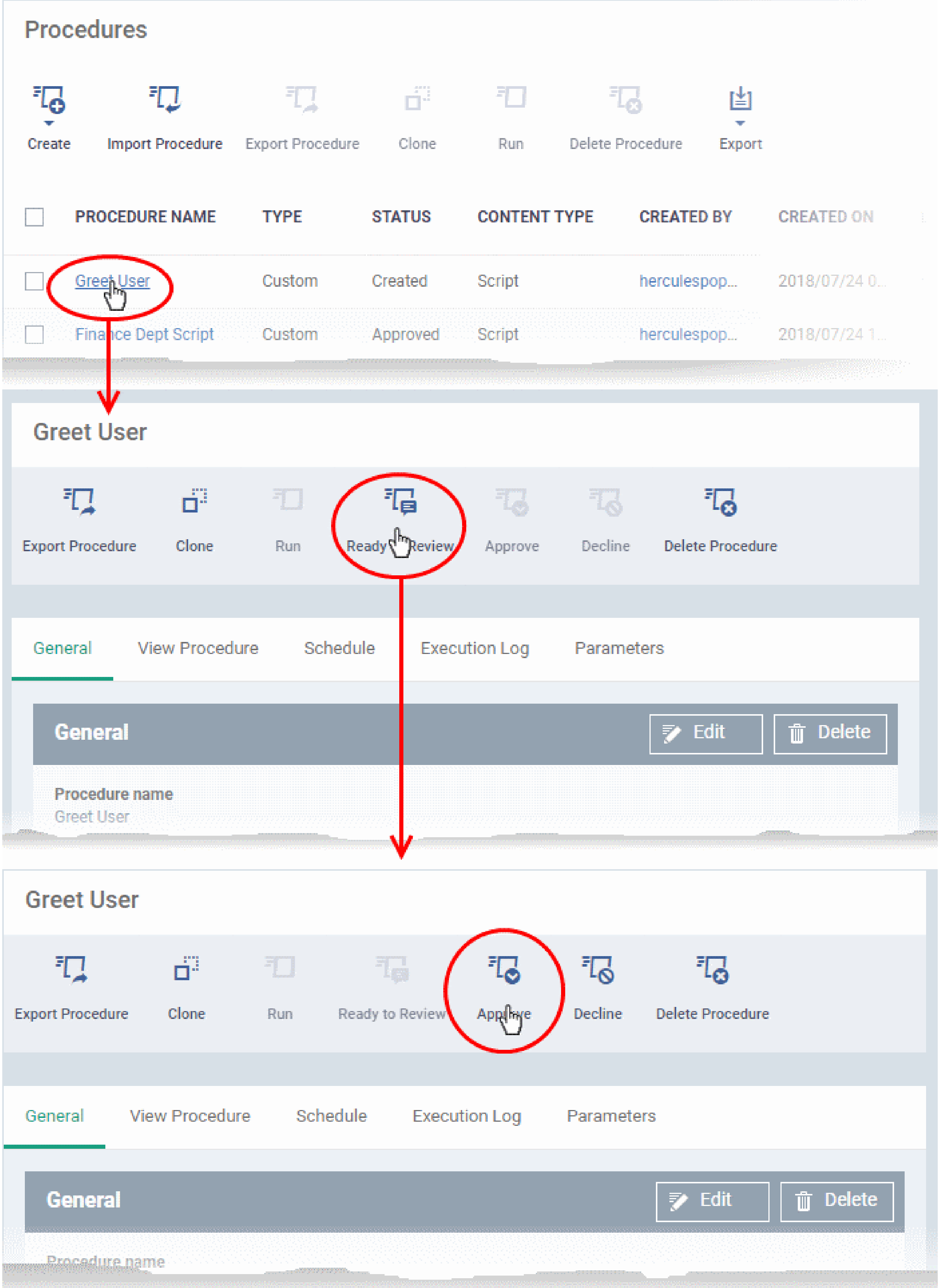
- New custom script procedures are given an initial status of 'Created'.
- Custom script procedures must be approved before they can be added to a profile.
- Custom patch procedures do not require approval.

**The review/approval process:**

- **Script writer -**
    - Go to 'Configuration Templates' > 'Procedures' and create a new script procedure.
    - Save the procedure in 'My Procedures' (or a sub-folder).
    - The procedure will have a status of 'Created'.
    - Click the name of the new procedure to open its configuration screen.
    - Click the 'Ready to Review' button
- **Approver -**
    - Receives a notification that a procedure requires approval
    - Goes to 'Configuration Templates' > 'Procedures' and opens the procedure details page
        - Clicks 'Approve' to commit the script and make it available for selection in profiles
        - Clicks 'Decline' to reject the script

**Notes:**

- The writer and approver in the example above can be the same person.
- The specific permissions required to approve a procedure are:
    - 'manage.procedures' and 'manage.procedures.manage'
    - Both these permissions are enabled in the 'admin' and 'technician' roles
    - Make sure these permissions are enabled in a custom role if its members are to approve procedures



| □ | PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON |
|---|---|---|---|---|---|---|
| □ | Greet User | Custom | Created | Script | herculespop... | 2018/07/24 0... |
| □ | Finance Dept Script | Custom | Approved | Script | herculespop... | 2018/07/24 1... |

Procedure name
Greet User

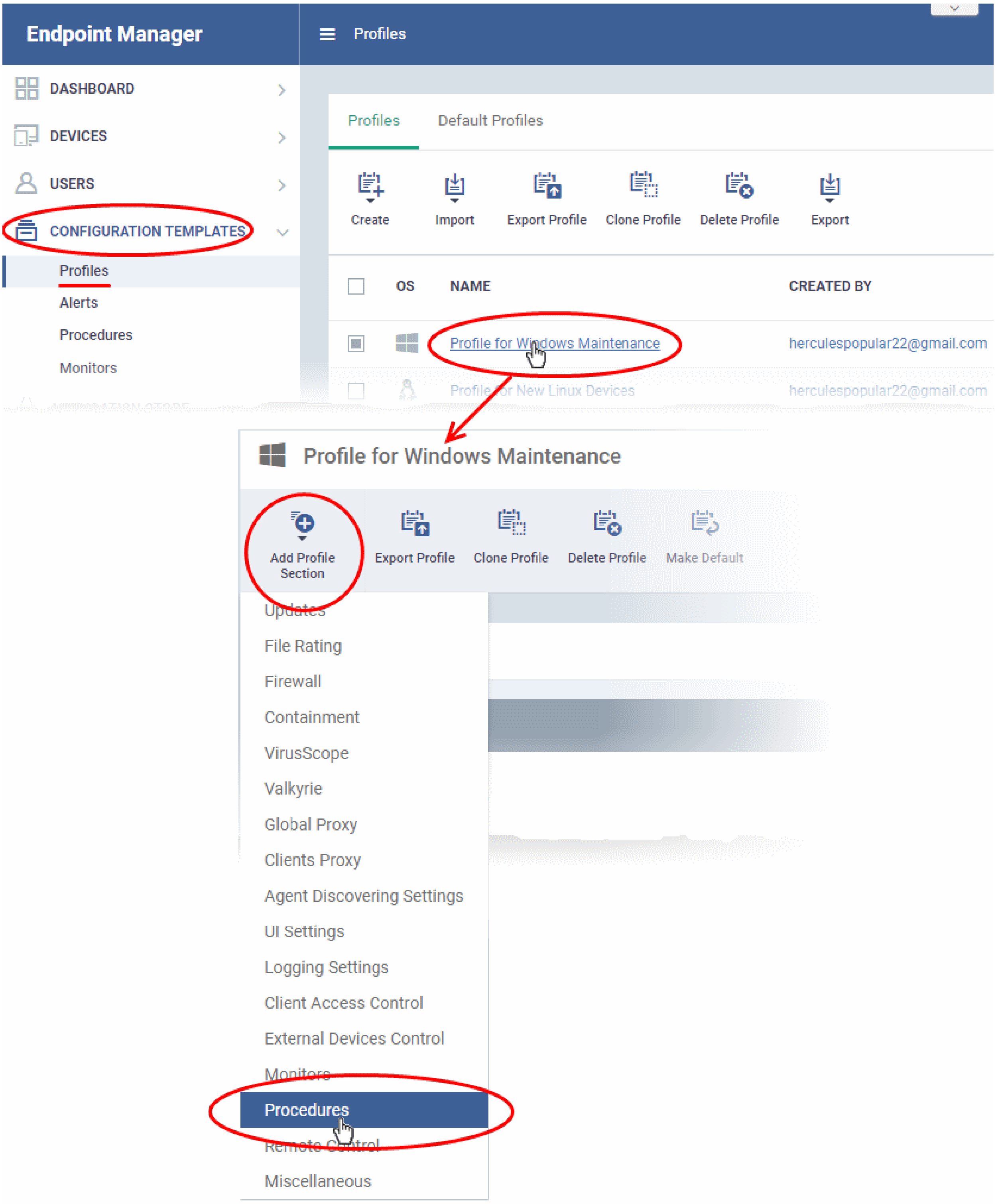
- Approved procedures can be selected and added to a profile.

## 6.6.5. Add a Procedure to a Profile / Procedure Schedules

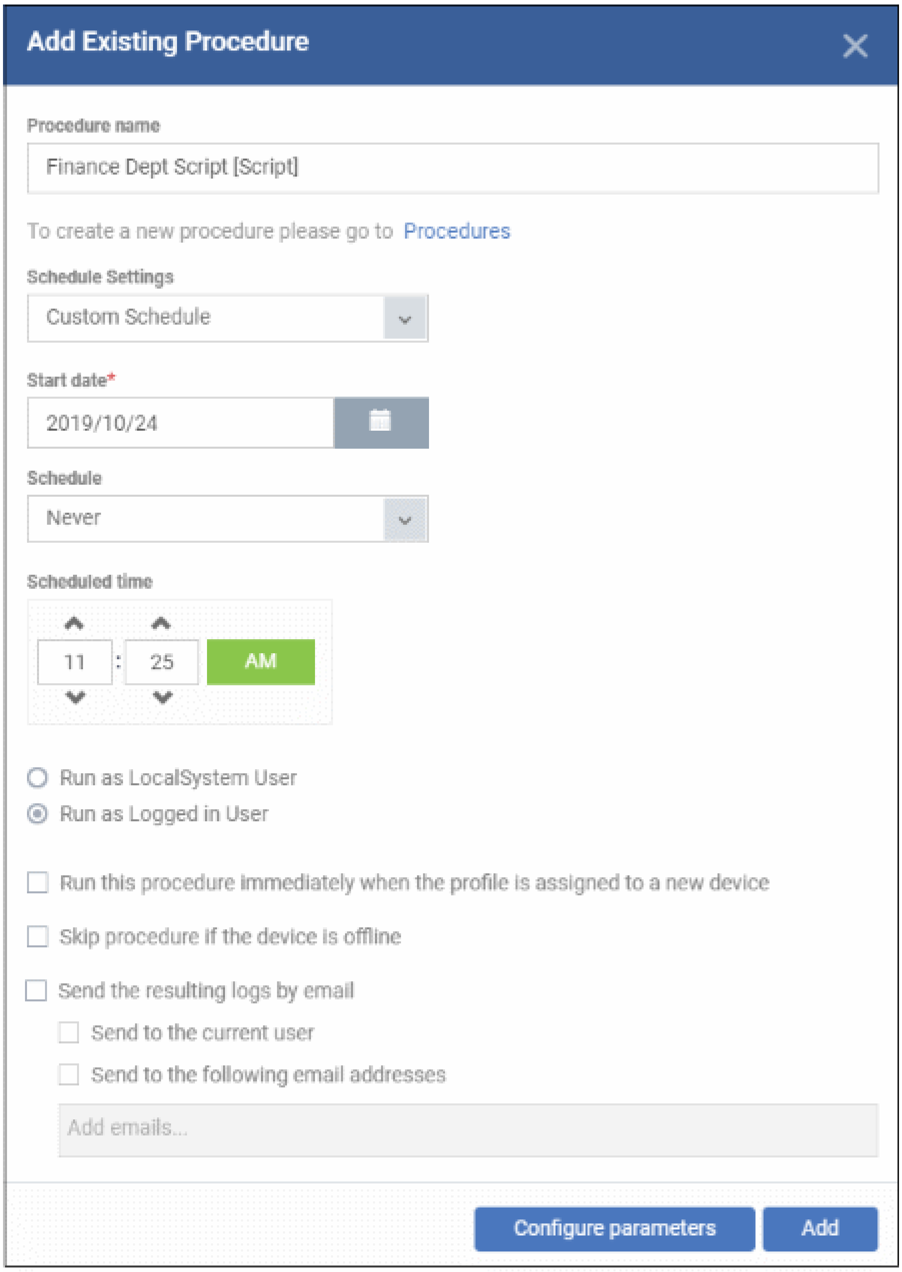
**FYI**. Procedure schedules are configured in the 'Profiles' area. You create the schedule when you add the procedure to the profile. The 'Schedule' tab in the procedures area just shows you which profiles are using the procedure.

**Add and schedule a procedure:**

- Click 'Configuration Templates' > 'Profiles'
- Click the profile to which you want to add a procedure
- Click 'Add Profile Section' > 'Procedures':



- This adds a 'Procedures' tab to the profile.
- Click the 'Add button' to open the procedure configuration screen



Add Existing Procedure ✕

Procedure name

Finance Dept Script [Script]

To create a new procedure please go to Procedures

Schedule Settings

Custom Schedule

Start date*

2019/10/24

Schedule

Never

Scheduled time

11 : 25 AM

○ Run as LocalSystem User

● Run as Logged in User

□ Run this procedure immediately when the profile is assigned to a new device

□ Skip procedure if the device is offline

□ Send the resulting logs by email

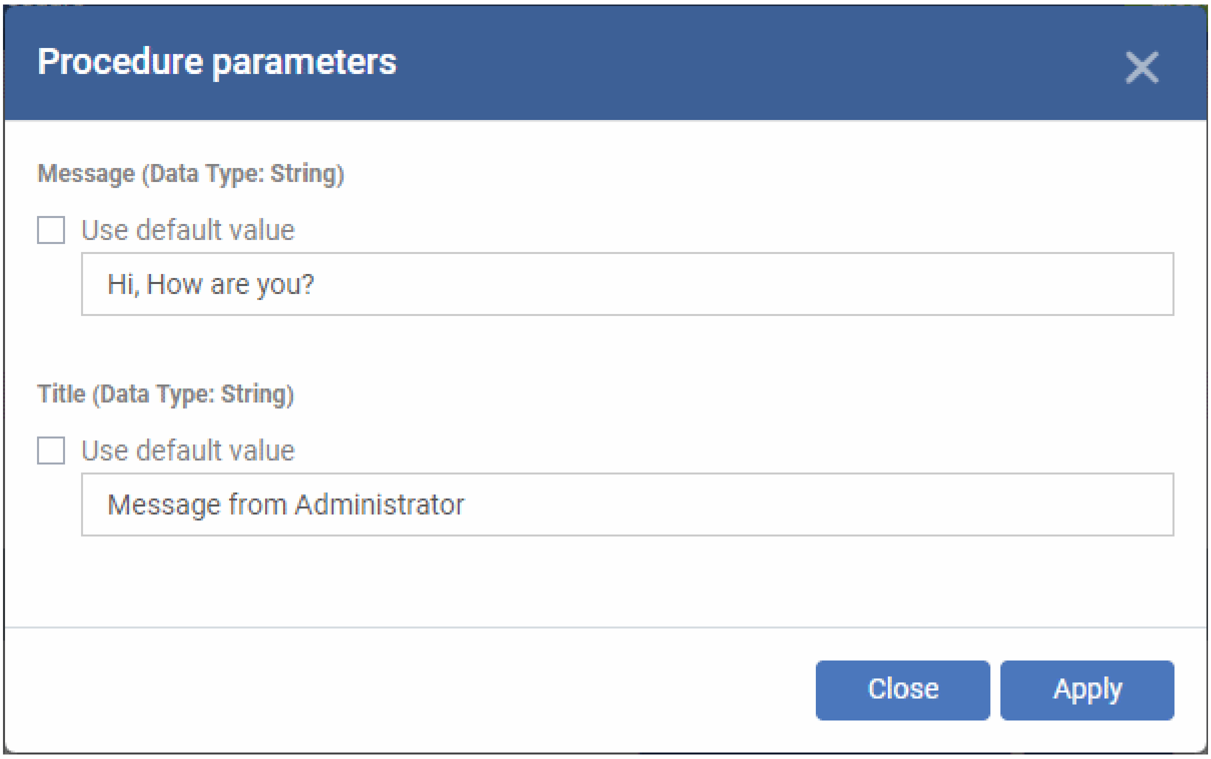
□ Send to the current user

□ Send to the following email addresses

Add emails...

- **Procedure Name -** Type the name of the procedure that you want to add to the profile (make sure you have **approved the procedure**)
- **Schedule Settings -** Create a custom schedule, or add it to an existing **maintenance window**
  - Custom schedule - Choose the start date, start time and frequency of the schedule.
  - Maintenance window:
    - Select the maintenance window type from 'Daily', 'Weekly', 'Monthly', or 'Week of month'.
    - You will then see a list of available windows of that type. Choose the window in which you want the schedule to run.
    - You can create new windows by adding a 'Maintenance Window' section to a profile.
      - Click 'Add Profile Section' > 'Maintenance Window'

- **Run as Local System User / Run as Logged in user -** Choose the user account under which the procedure should run. This option is not available for patch procedures.
- **Run this procedure immediately when the profile is assigned to a new device -** The procedure is executed instantly on devices which use the profile. Thereafter it will run as per scheduled.
- **Skip procedure if the device is offline -** The procedure is not executed on devices that are not connected to EM
- **Send the resulting logs by email -** Script procedures only.
    - **Send to current user -** Procedure results are sent to the admin who is currently logged into Endpoint Manager.
    - **Send to the following email addresses -** Add email addresses to whom log results should be sent.
- **Configure parameters -** Specify values for script variables. This is only available for scripts that have variables associated with them:



Procedure parameters

Message (Data Type: String)

□ Use default value

Hi, How are you?

Title (Data Type: String)

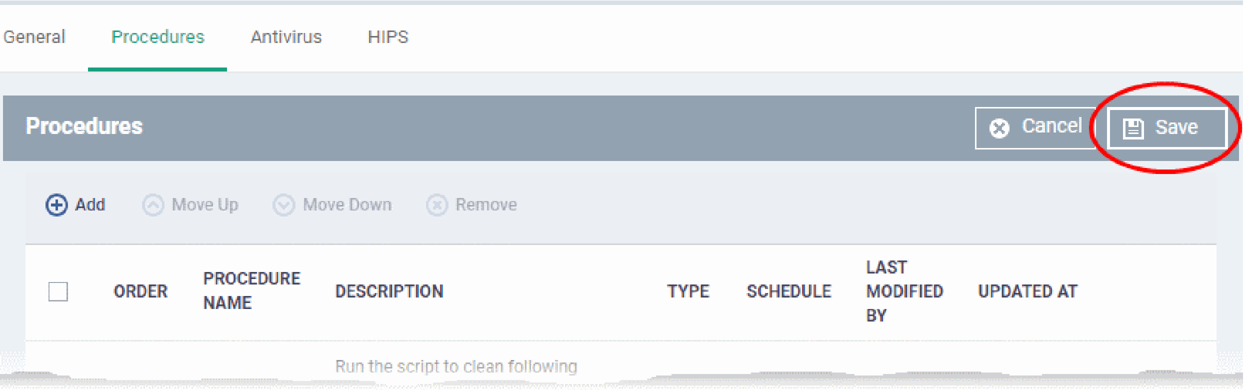
□ Use default value

Message from Administrator

Each variable is pre-populated with its default value

- You can change these variables as required, or leave it at use default value.
- Click 'Apply'.

- Click 'Add'.
- Finally, click 'Save' to apply the procedure and the schedule to the profile:



| □ | ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | LAST MODIFIED BY | UPDATED AT |
|---|---|---|---|---|---|---|---|
| | | | Run the script to clean following | | | | |

- The 'Schedule' tab of the procedure interface lists all profiles which have this procedure scheduled:

**Important Note**: Patches that are hidden by administrators will not be executed. See **Manage OS Patches on Windows Endpoints** for more details.

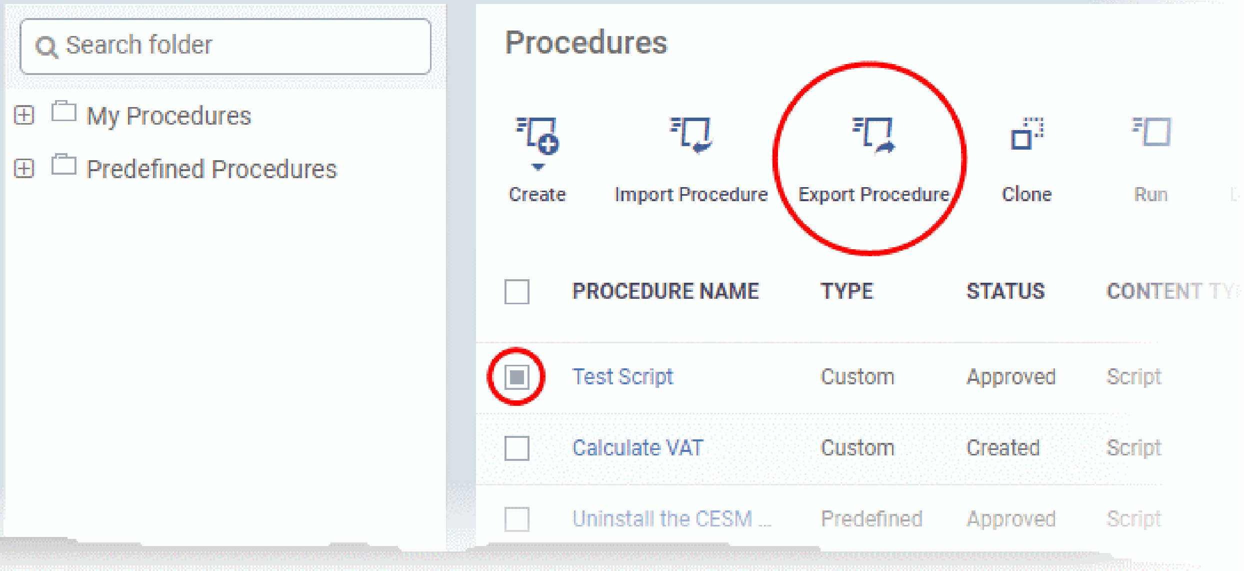
## 6.6.6. Import / Export / Clone Procedures

Endpoint Manager allows you to export or import procedures in order to use them in profiles. The procedure files are saved in .json format. You can also clone a procedure and use it as a starting point to create a new procedure according to your requirements. Click the following links to find out more:

- **Export a procedure**
- **Import a procedure**
- **Clone a procedure**

**To export a procedure**

- Click 'Configuration Templates' > 'Procedures'
- Navigate to the folder containing the procedure to be exported
- Select the procedure and click 'Export' at the top. Please note you can export only custom procedures.

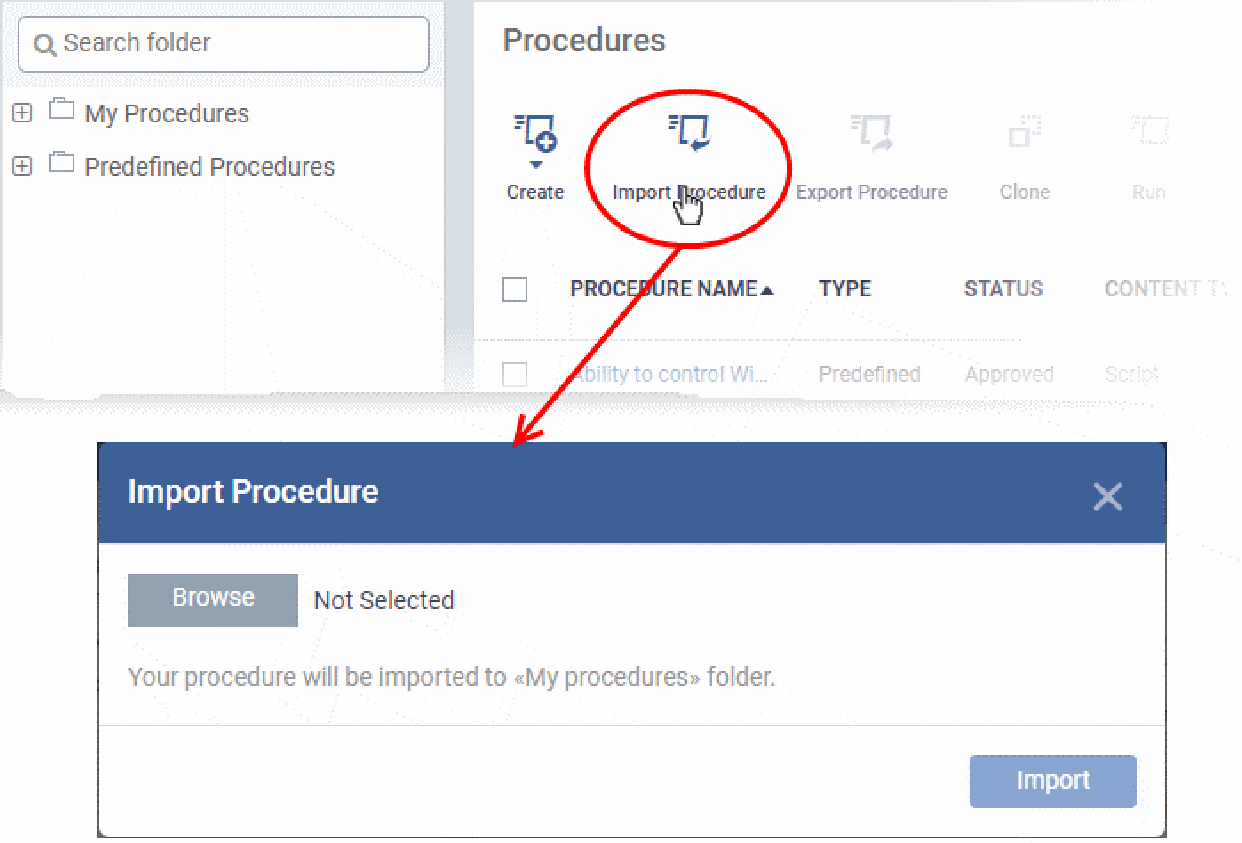


| □ | PROCEDURE NAME | TYPE | STATUS | CONTENT TY |
|---|---|---|---|---|
| ▣ | Test Script | Custom | Approved | Script |
| □ | Calculate VAT | Custom | Created | Script |
| □ | Uninstall the CESM ... | Predefined | Approved | Script |

The selected procedure file will be saved in your default download location.

**To import a procedure**

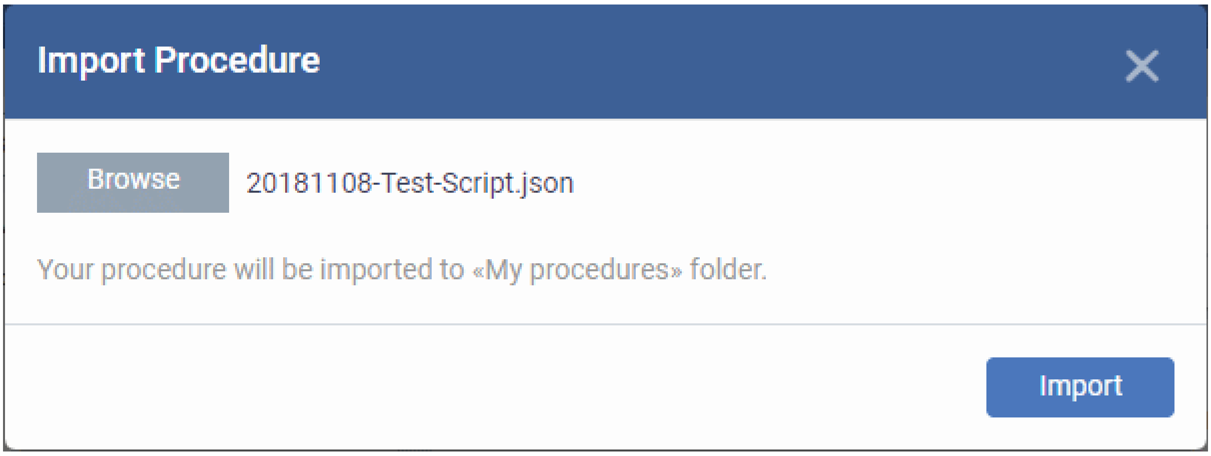
- Click 'Configuration Templates' > 'Procedures'
- Click 'Import' at the top



Your procedure will be imported to «My procedures» folder.

- Click 'Browse', navigate to the location where the procedure file is saved and click 'Open'

The selected file will be displayed on the 'Import Procedure' dialog.



Import Procedure

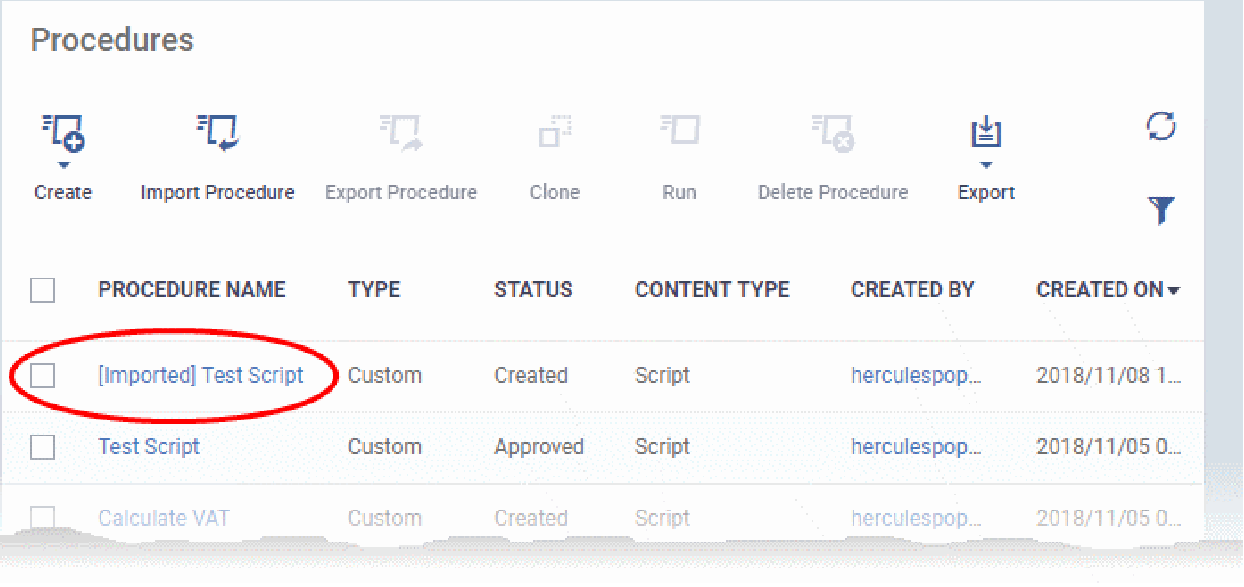
20181108-Test-Script.json

Your procedure will be imported to «My procedures» folder.

- Click 'Import'

The procedure is imported and placed in the 'My Procedures' folder. The procedure name is prefixed with "Imported" to distinguish it from other procedures.

You can save the procedure in a different folder by editing it. See **Edit / Delete Procedures** for guidance on this.



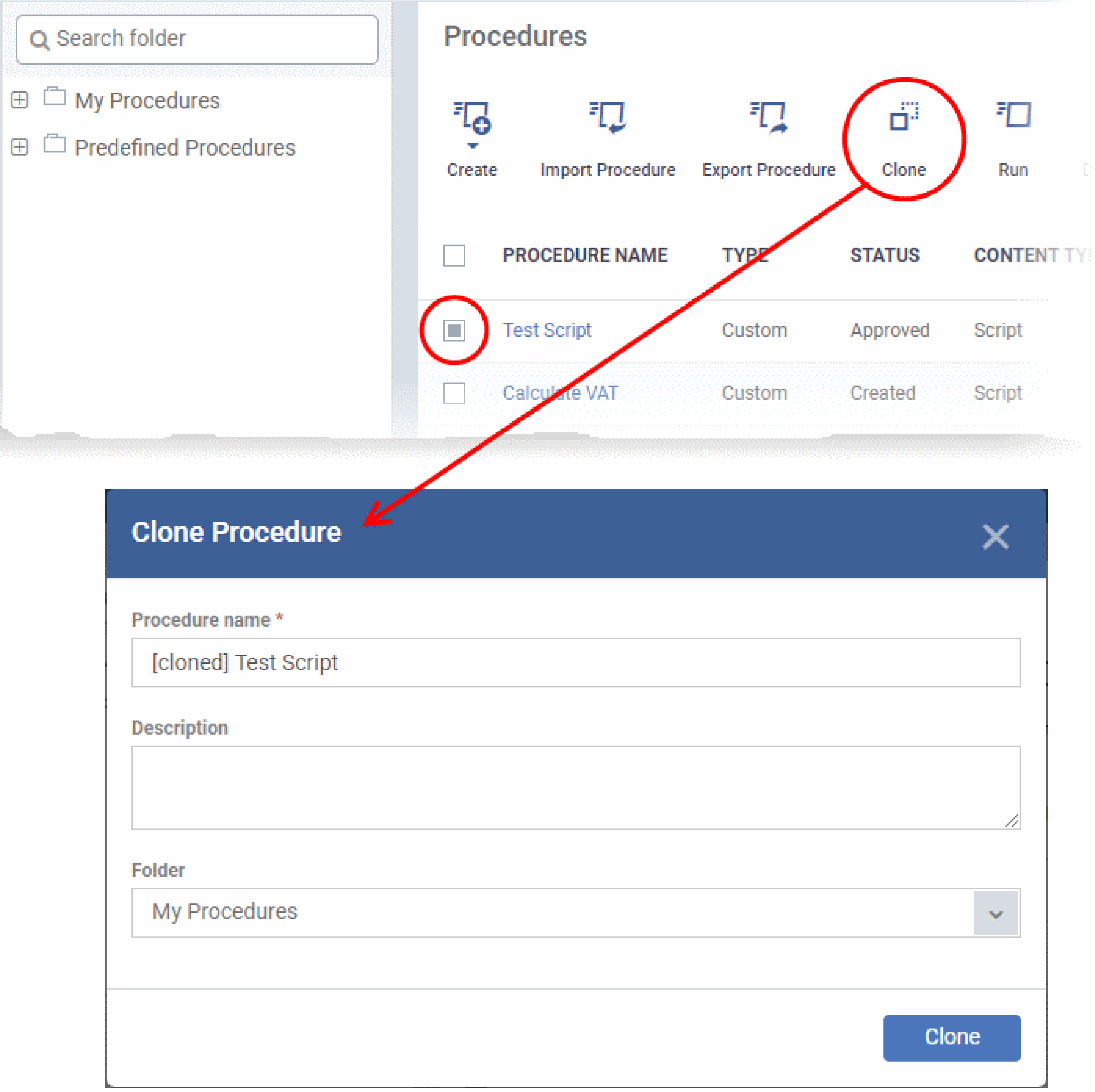
Procedures

| □ | PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON |
|---|---|---|---|---|---|---|
| □ | [Imported] Test Script | Custom | Created | Script | herculespop... | 2018/11/08 1... |
| □ | Test Script | Custom | Approved | Script | herculespop... | 2018/11/05 0... |
| □ | Calculate VAT | Custom | Created | Script | herculespop... | 2018/11/05 0... |

Please note you have to **approve** the imported procedure in order to deploy it in profiles. To change the name and/or edit the script, click on the procedure and then click 'Edit' button on the right. Refer to the section '**Edit / Delete Procedures**' for more details.

### To clone a procedure

- Click 'Configuration Templates' > 'Procedures'
- Navigate to the folder containing the procedure to be cloned
- Select the procedure and click 'Clone' at the top.



| PROCEDURE NAME | TYPE | STATUS | CONTENT TY |
|---|---|---|---|
| Test Script | Custom | Approved | Script |
| Calculate VAT | Custom | Created | Script |

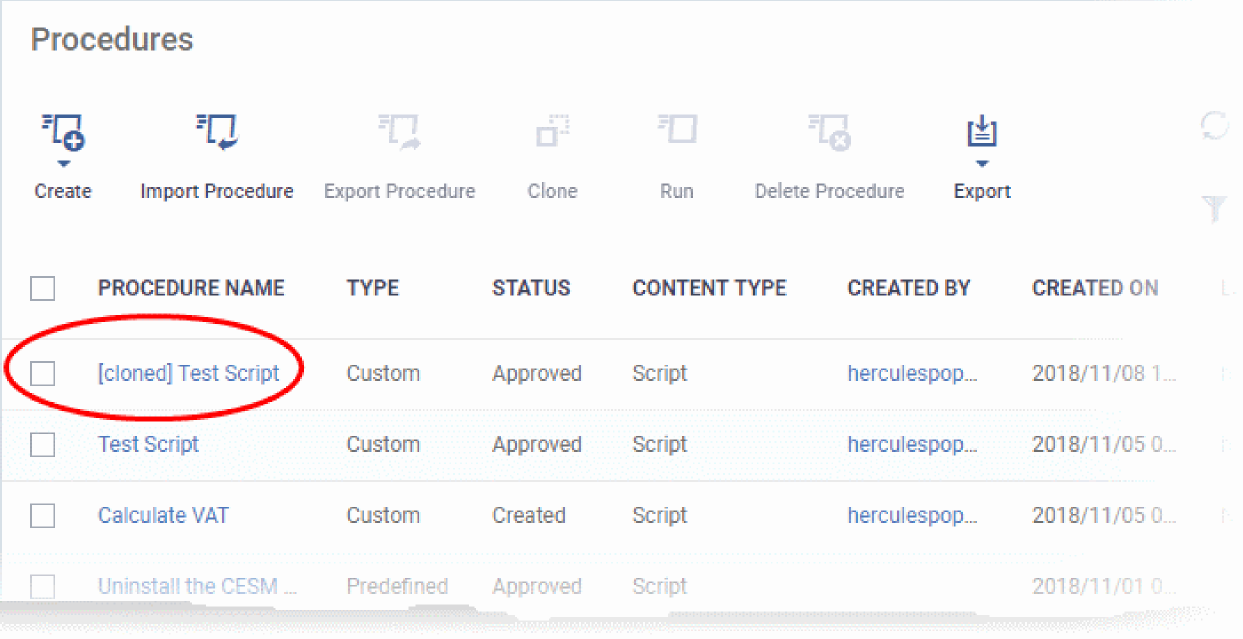
Procedure name *: [cloned] Test Script

Description:

Folder: My Procedures

- Change the name, if required, and provide an appropriate description of the profile
- Select the folder in which the cloned procedure is to be placed
- Click 'Clone'

The procedure will be added to the list:



Procedures

| ☐ | PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON |
|---|---|---|---|---|---|---|
| ☐ | [cloned] Test Script | Custom | Approved | Script | herculespop... | 2018/11/08 1... |
| ☐ | Test Script | Custom | Approved | Script | herculespop... | 2018/11/05 0... |
| ☐ | Calculate VAT | Custom | Created | Script | herculespop... | 2018/11/05 0... |
| ☐ | Uninstall the CESM ... | Predefined | Approved | Script | | 2018/11/01 0... |

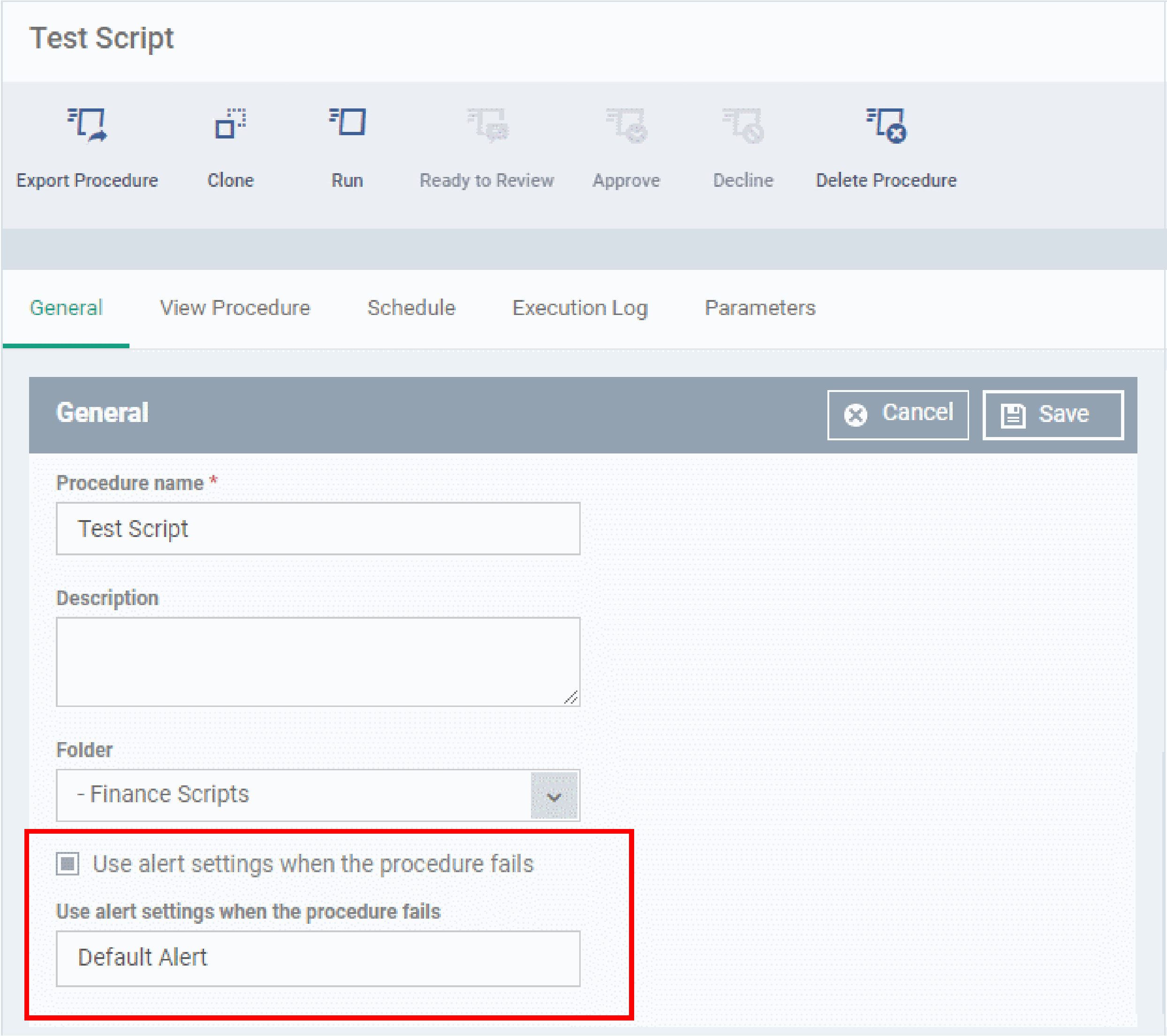
Please note the status of the cloned procedure will be same as that of the procedure that was cloned. For example, if the status was approved then the cloned procedure will also be of the same status.

## 6.6.7. Change Alert Settings

Endpoint Manager is capable of issuing alerts when procedures fail to execute as intended. You can set the type of alert shown while you are creating a new procedure, or by editing an existing procedure. Please note you can only select alerts that are already created in the 'Alerts' interface ('Configuration Templates' > 'Alerts'). See '**Manage Alerts**' for more details.

**To change alert settings**

- Click 'Configuration Templates' > 'Procedures'
- Navigate to the folder containing the procedure to be configured for alert
- Click the name of the procedure to open its details interface and select the 'General' tab.
- Click 'Edit' on the top right



Procedure name *

Test Script

Description

Folder

- Finance Scripts

☑ Use alert settings when the procedure fails

Use alert settings when the procedure fails

Default Alert

- Make sure the 'Use alert settings when the procedure fails' check box is selected.
- The current alert name is displayed in the 'Use alert settings when the procedure fails' field.
- Start typing the name of the alert in the field and choose the alert to be used, from the options.
- Click 'Save' at the top right.

## 6.6.8. Directly Apply Procedures to Devices

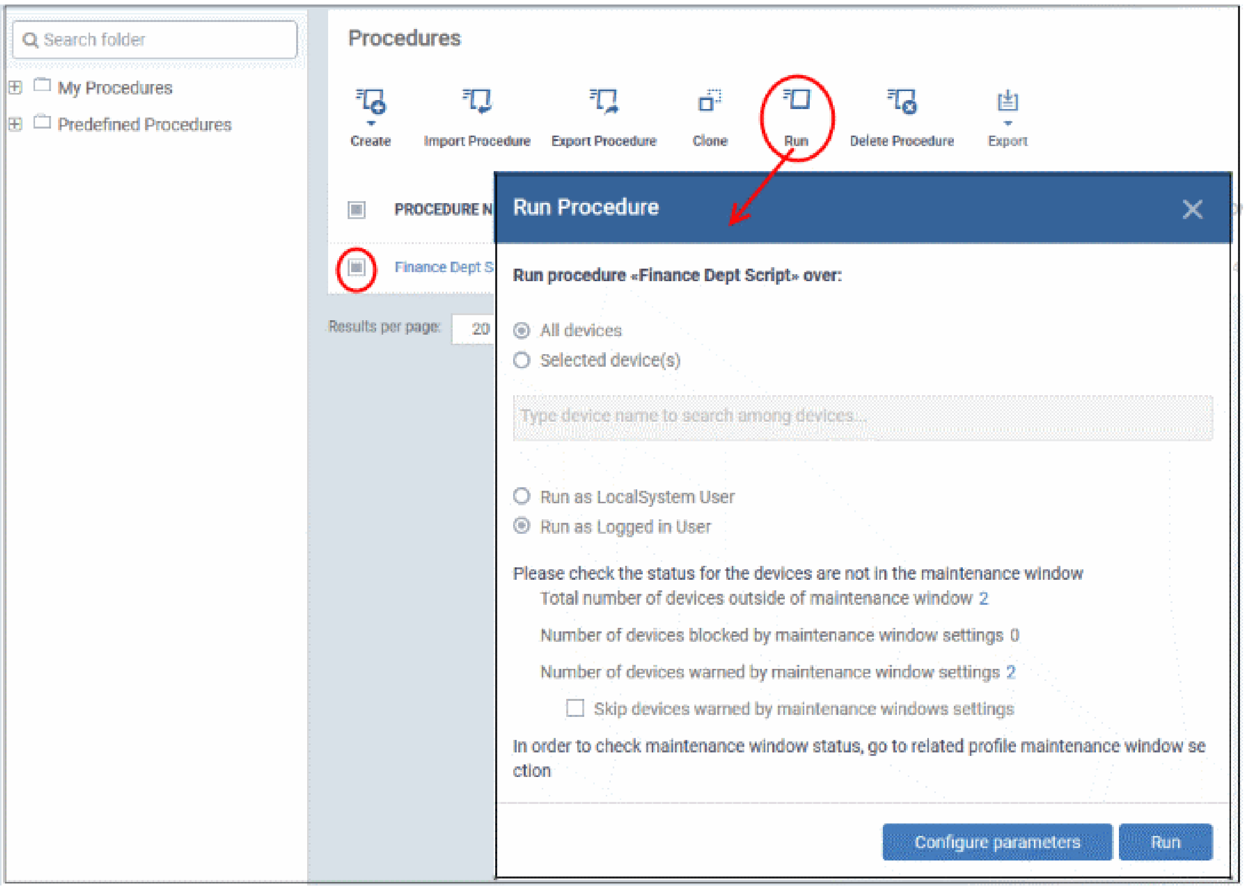
There are three ways you can run a procedure:

- **From the procedures interface**
- **From the device list interface**
- **Via profiles according to a schedule**

The following section describes how to apply procedures to devices from the procedures interface.

**Run a procedure**

- Click 'Configuration Templates' > 'Procedures'
- Browse the folder tree to locate the procedure you want to run
- Select the procedure and click 'Run' at the top. Note - only **approved** procedures can be applied. You can also run only one procedure at a time.



Run procedure «Finance Dept Script» over:

● All devices
○ Selected device(s)

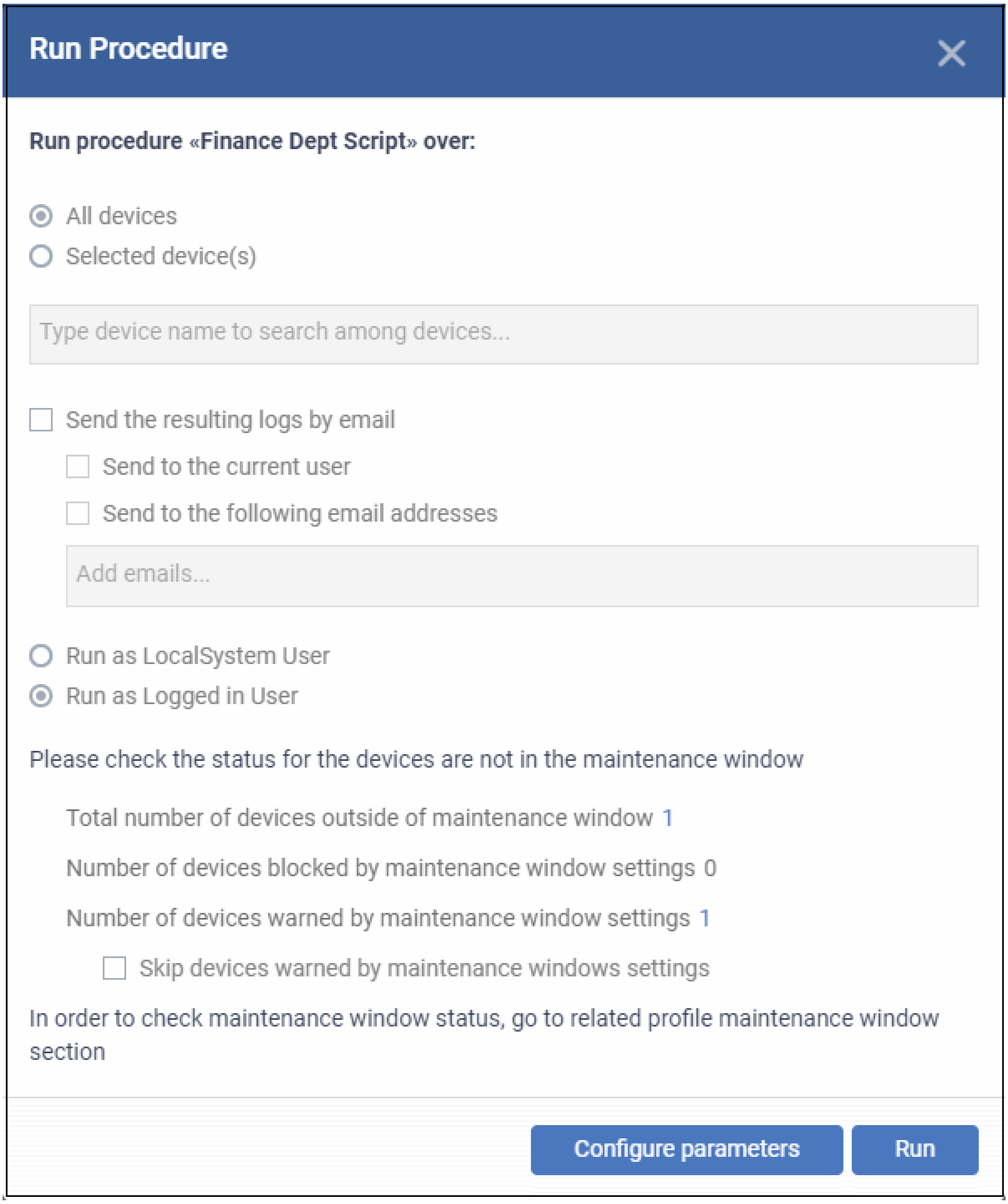
Type device name to search among devices...

○ Run as LocalSystem User
● Run as Logged in User

Please check the status for the devices are not in the maintenance window
Total number of devices outside of maintenance window 2
Number of devices blocked by maintenance window settings 0
Number of devices warned by maintenance window settings 2
□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window se ction

- Choose the execution options from the 'Run Procedure' dialog
  - **All Devices -** The procedure will be applied to all Windows devices.
  - **Selected Device(s) -** Enter the name of the Windows device partly or fully and select the device from the list. You can also add multiple devices in the field.



Run Procedure

Run procedure «Finance Dept Script» over:

● All devices
○ Selected device(s)

Type device name to search among devices...

□ Send the resulting logs by email
□ Send to the current user
□ Send to the following email addresses

Add emails...

○ Run as LocalSystem User
● Run as Logged in User

Please check the status for the devices are not in the maintenance window

Total number of devices outside of maintenance window 1

Number of devices blocked by maintenance window settings 0

Number of devices warned by maintenance window settings 1

□ Skip devices warned by maintenance windows settings

In order to check maintenance window status, go to related profile maintenance window section

- **Send the resulting logs by email** - Script procedures only.
  - **Send to current user** - Procedure results are sent to the admin who is currently logged into Endpoint Manager.
  - **Send to the following email addresses** - Add email addresses to whom log results should be sent.

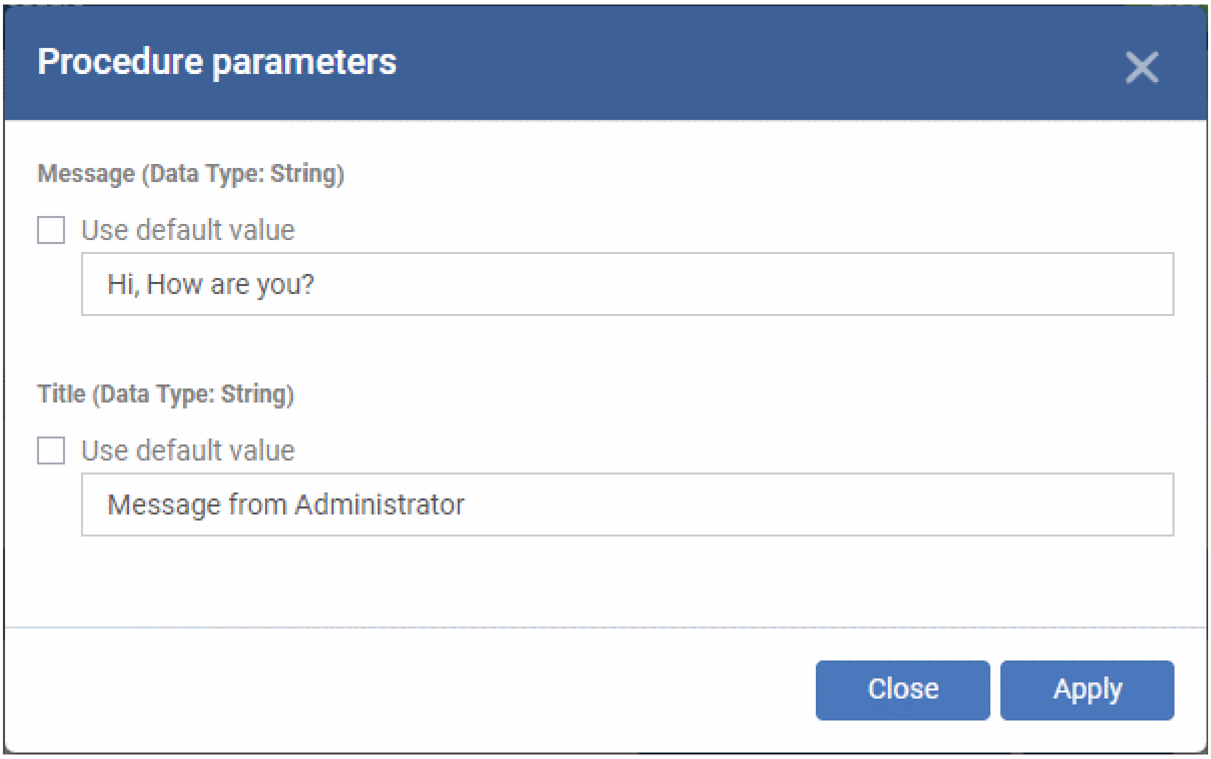
- **Run as Local System User** / **Run as Logged in user** - Choose the user account with which the procedure has to be run on the devices based on the access rights required for the procedure. Please note this option will not be available for a patch procedure.
- **Maintenance window status** - Details of any **maintenance windows** in the device's profile.
  - **Total number of devices outside of maintenance window** - The number of devices that are not part of a maintenance window. The procedure can run on these devices.

- **Number of devices blocked by maintenance windows settings -** The number of devices on which you cannot run the procedure because the admin has blocked procedures outside the maintenance window.
- **Number of devices warned by maintenance window settings -** The number of devices that are part of a maintenance window and have warnings enabled. You can still run the procedure on these devices.
    - **Skip devices warned by maintenance windows settings -** A maintenance window is a time-slot reserved for running important tasks on target devices. Admins can enable a warning if somebody attempts to run a procedure outside of the window. This setting will skip those devices which have been added to a maintenance window with warnings enabled.

- **Configure parameters -** Available only for script procedures defined with variable parameters and allows you to enter the values for them.

**To specify values for variable parameters**

- Click 'Configure Parameters'



Procedure parameters

Message (Data Type: String)

□ Use default value

Hi, How are you?

Title (Data Type: String)

□ Use default value

Message from Administrator

The list of variable parameters will appear with their default values pre-populated in their respective text fields

- Enter the value for each parameter in the respective text box
- Select 'Use default value' if you want the default value to be applied for a parameter,
- Click 'Apply'

**Tip**: You can skip this step If you want to use default values for all parameters. For more info on default values, see **Create a Custom Procedure**.

- Click the 'Run' button in the 'Run Procedure' dialog.

The procedure is applied to the selected devices. A confirmation dialog is displayed and the process is logged. You can view the details in the **Procedure Logs** screen for script procedures. **Patch procedure logs** will be available in the respective patch procedure itself.

**Important Note**: Patches that are hidden by administrators will not be executed. See **Manage OS Patches on Windows Endpoints** for more details.

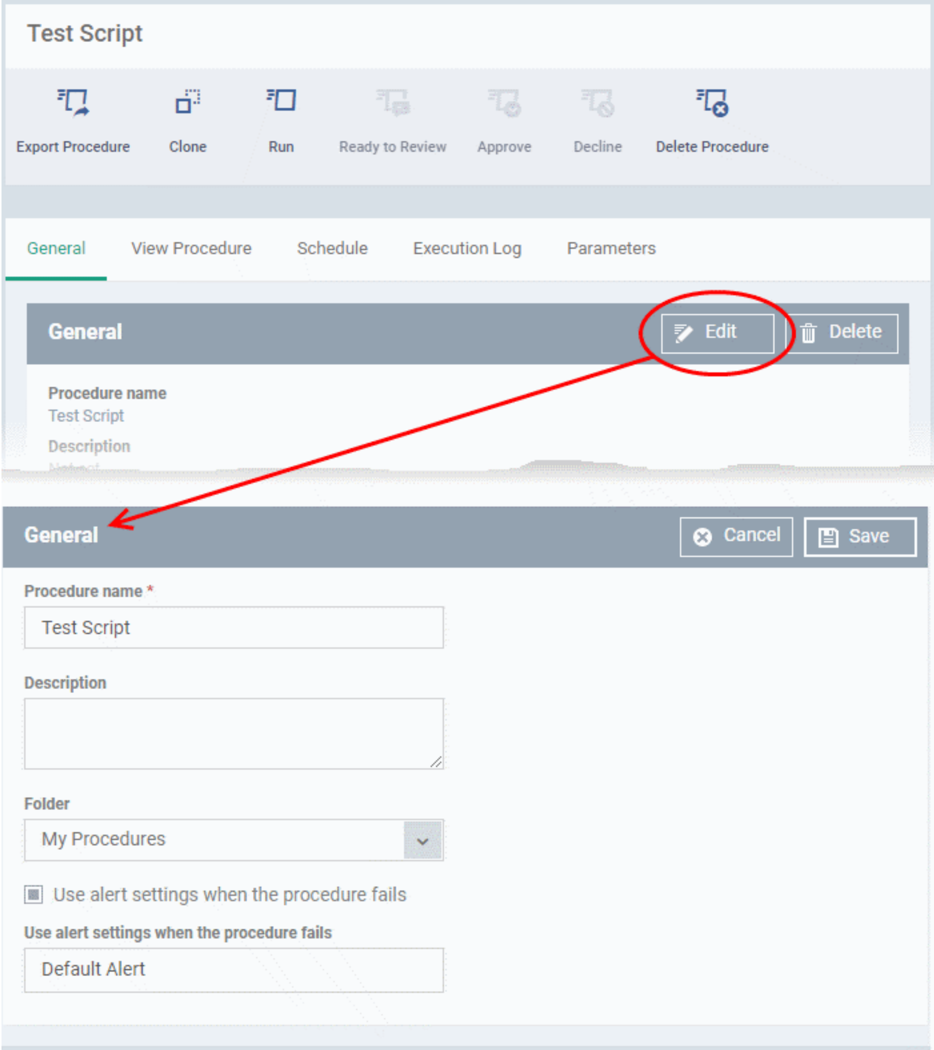
## 6.6.9. Edit / Delete Procedures

Custom procedures can be edited or deleted according to your requirements. Please note that if you edit a script procedure, it has to be **approved** again. Predefined procedures cannot be edited or deleted. Click the following links for more details:

- **Edit / delete a script procedure**
- **Edit / delete a patch procedure**

### Edit a Script Procedure

- Click 'Configuration Templates' > 'Procedures'
- Browse the folder tree to locate the procedure you want to edit
- Click on the script procedure to open its details interface
- Select a tab and click 'Edit' to modify its details



Test Script

Procedure name *: Test Script

Description:

Folder: My Procedures

☑ Use alert settings when the procedure fails

Use alert settings when the procedure fails: Default Alert

**General**

- Modify the procedure name, description, the folder in which the procedure is saved and / or alert settings

**View Procedure**

- Modify the script and / or add another existing procedure

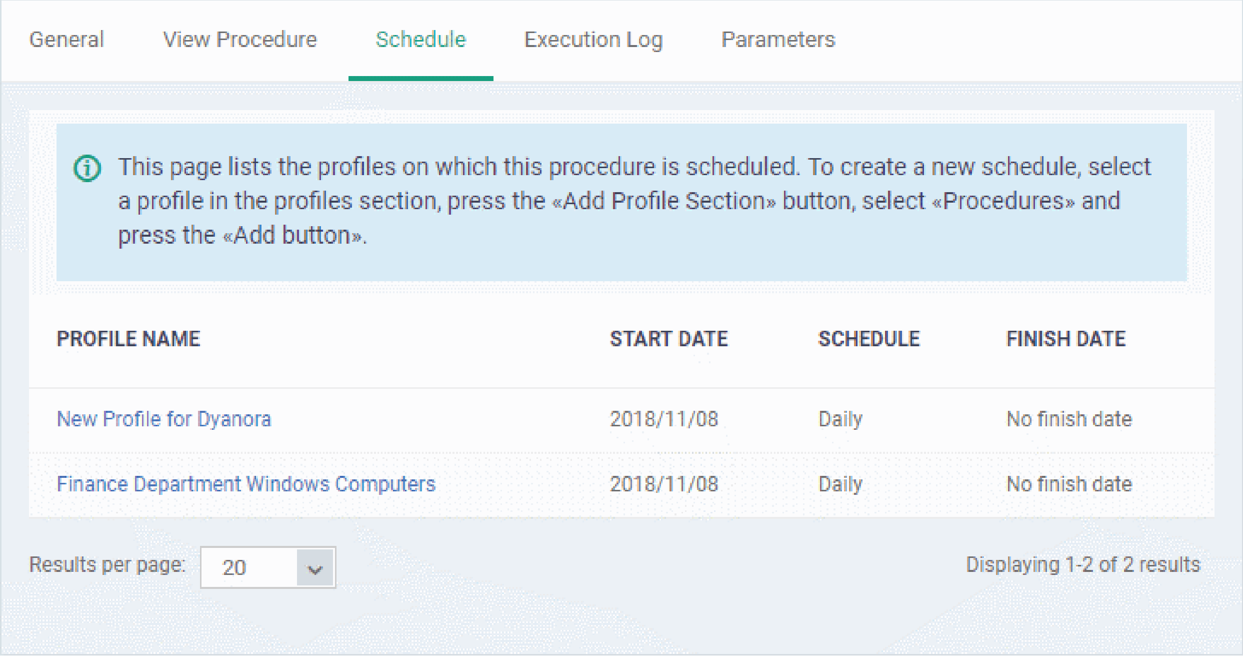
**Execution Log**

- Displays the results of the script procedure that was executed, both manually and scheduled on Windows profiles.

**Schedule**

The schedule can be edited only in the profile(s) that the procedure is deployed.

- Click the 'Schedule' tab to view the profile(s) in which the procedure is being used.



This page lists the profiles on which this procedure is scheduled. To create a new schedule, select a profile in the profiles section, press the «Add Profile Section» button, select «Procedures» and press the «Add button».

| PROFILE NAME | START DATE | SCHEDULE | FINISH DATE |
|---|---|---|---|
| New Profile for Dyanora | 2018/11/08 | Daily | No finish date |
| Finance Department Windows Computers | 2018/11/08 | Daily | No finish date |

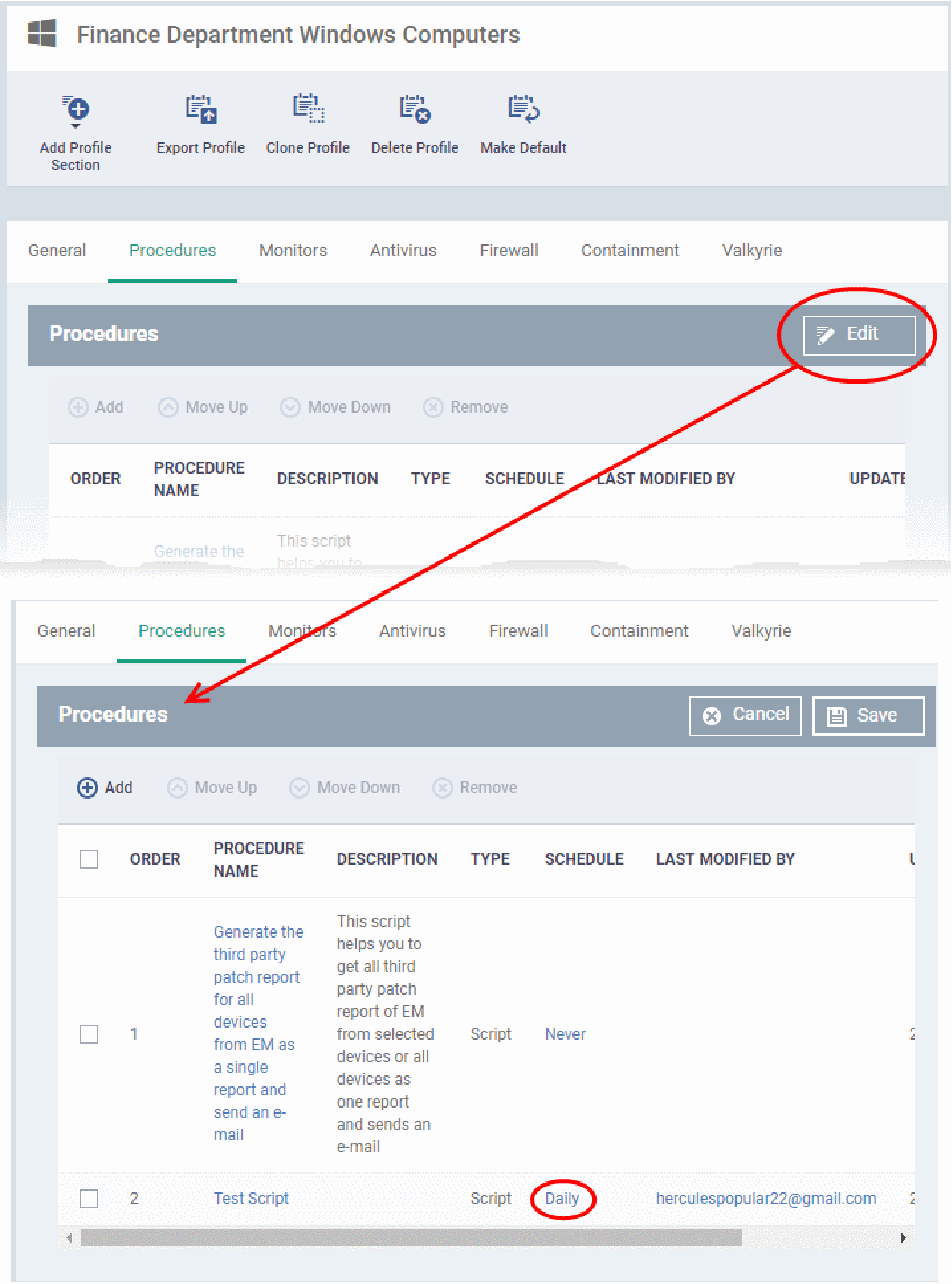
Results per page: 20

Displaying 1-2 of 2 results

- Click the profile for which you want to edit the procedure schedule.

The selected profile is displayed with the 'Procedure' tab opened.

- Click 'Edit' at the top right.



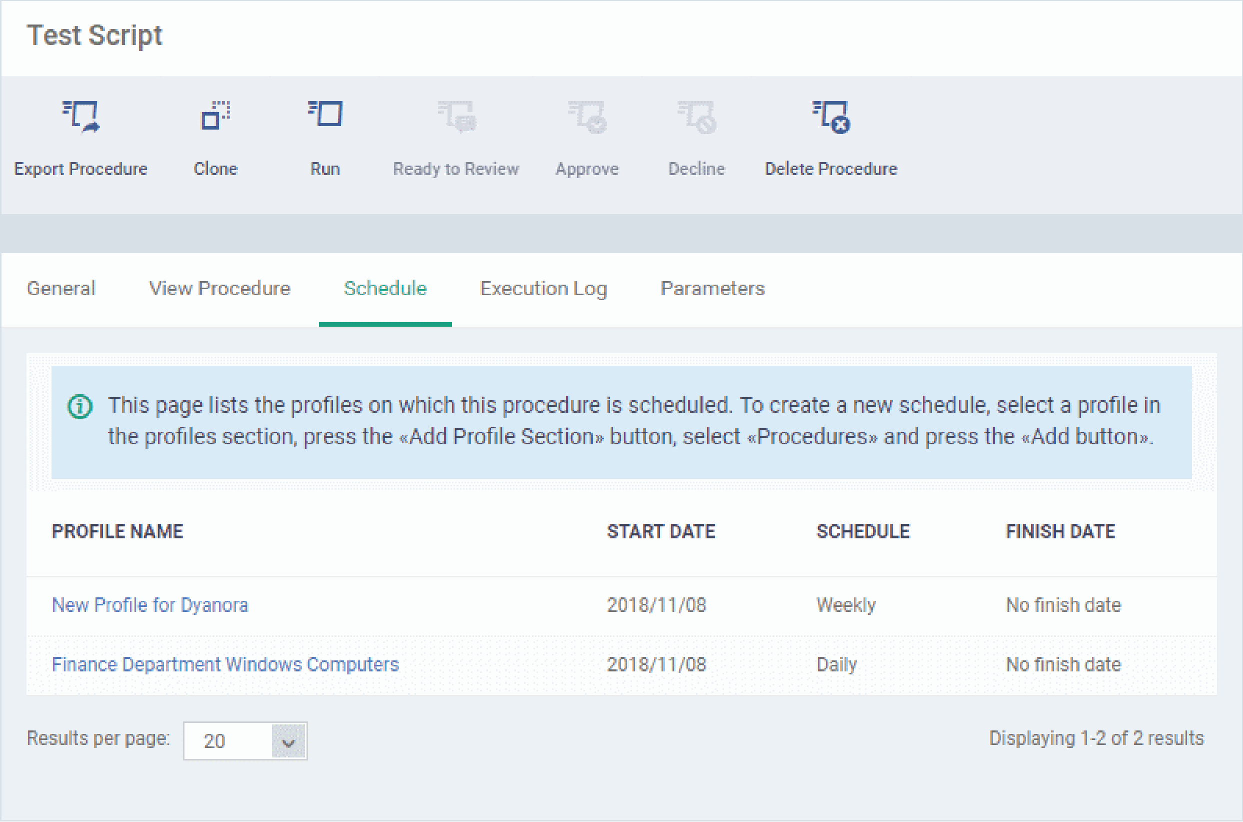
| □ | ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | LAST MODIFIED BY | U |
|---|---|---|---|---|---|---|---|
| □ | 1 | Generate the third party patch report for all devices from EM as a single report and send an e-mail | This script helps you to get all third party patch report of EM from selected devices or all devices as one report and sends an e-mail | Script | Never | | 2 |
| □ | 2 | Test Script | | Script | Daily | herculespopular22@gmail.com | 2 |

You can find the procedure type, whether script or patch, under the 'Type' column.

- Click the schedule parameter under 'Schedule' column beside the procedure.
- The 'Procedure Schedule' dialog will be displayed. Modify the schedule per your requirement and click 'Set'.
- The schedule will be modified for the profile. Please note the procedure schedule will impact only the profile that you modify. The schedule for the same procedure deployed onto other profiles will not be affected.

- Click 'Save'

The changes for the procedure will be saved. The following image shows the same procedure having different schedule for different profiles.



This page lists the profiles on which this procedure is scheduled. To create a new schedule, select a profile in the profiles section, press the «Add Profile Section» button, select «Procedures» and press the «Add button».

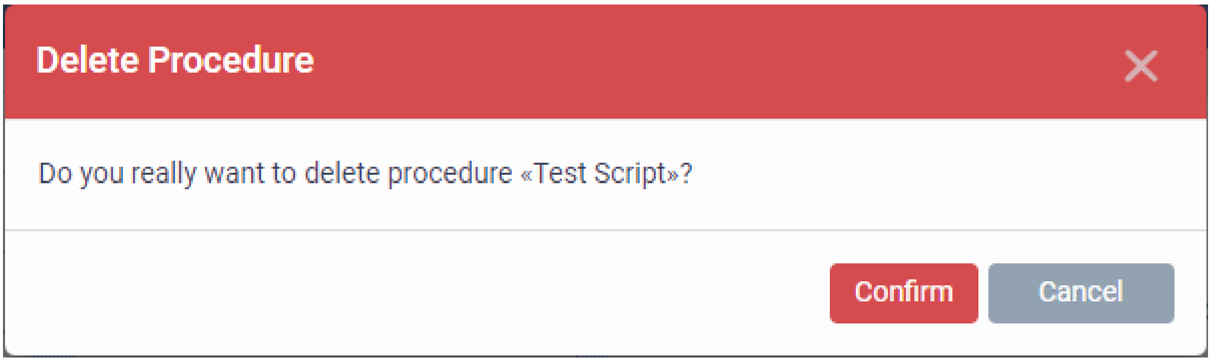
| PROFILE NAME | START DATE | SCHEDULE | FINISH DATE |
|---|---|---|---|
| New Profile for Dyanora | 2018/11/08 | Weekly | No finish date |
| Finance Department Windows Computers | 2018/11/08 | Daily | No finish date |

Results per page: 20

Displaying 1-2 of 2 results

### To delete a script procedure

- Click 'Configuration Templates' > 'Procedures'
- Browse the folder tree to locate the procedure you want to edit
- Select the check box beside the procedure and click 'Delete Procedure' at the top.
- Alternatively, click on the procedure that you want to delete and click 'Delete' on the top right



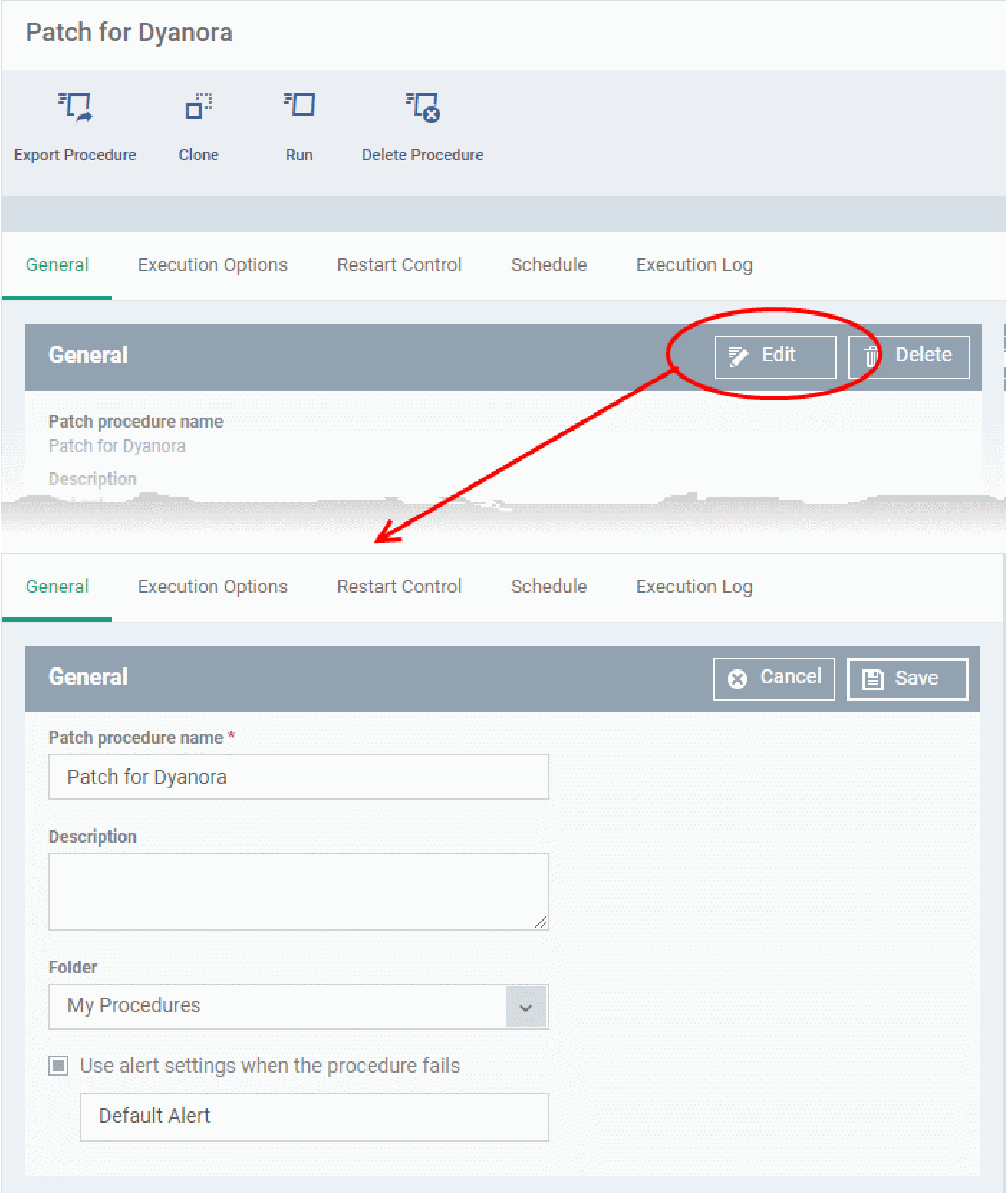
Do you really want to delete procedure «Test Script»?

- Click 'Confirm'. The procedure is removed from the list as well as from the profiles on which it is deployed.

## Edit a patch procedure

- Click 'Configuration Templates' > 'Procedures'
- Browse the folder tree to locate the procedure you want to edit

- Click on the patch procedure to open its details interface
- Select a tab and click 'Edit' to modify its details



**General**

- Modify the procedure name, description, the folder in which the procedure is saved and / or alert settings

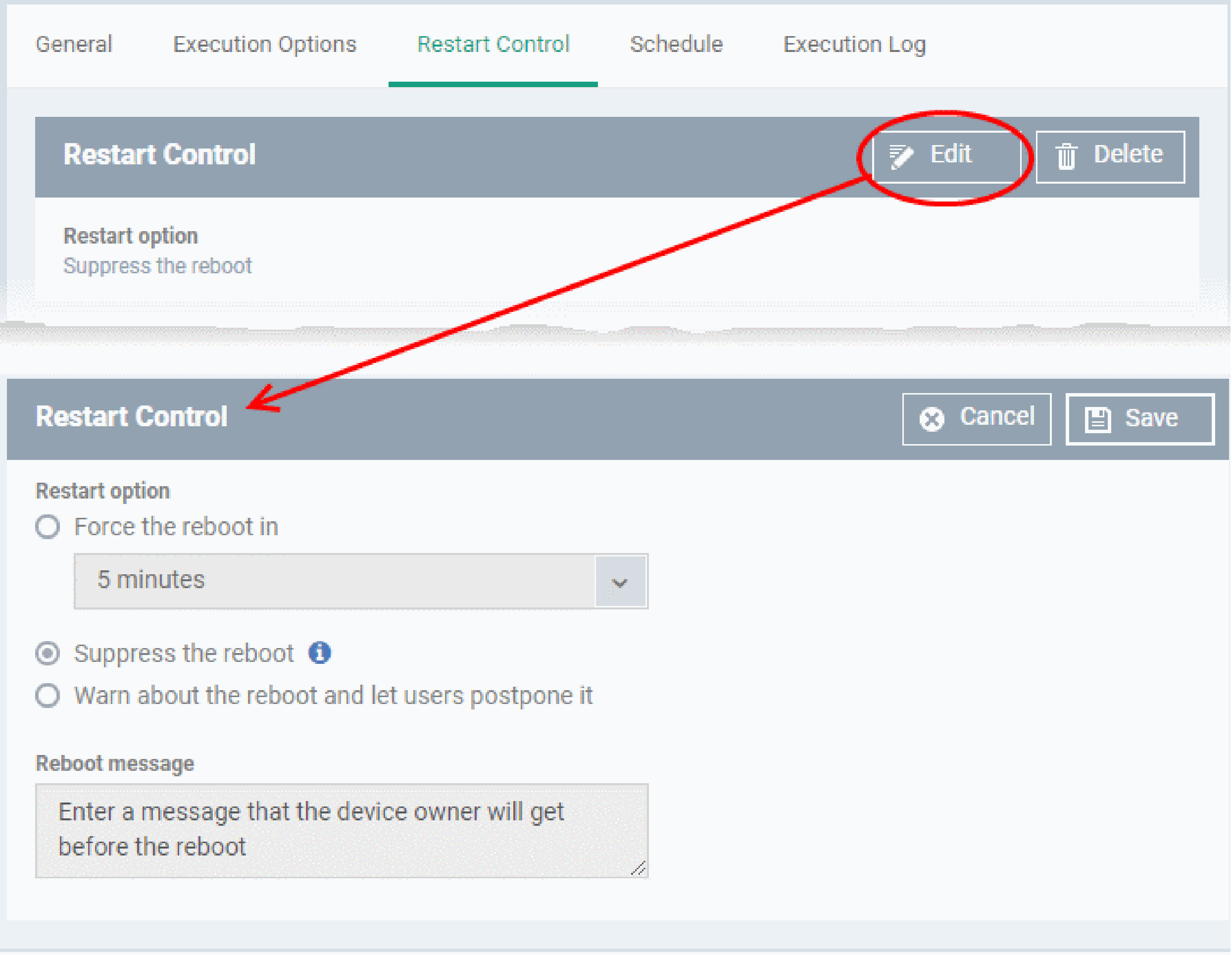
**Execution Options**

- Modify the patch options. See the explanation of **Procedure Configuration** in **Create a Custom Procedure** for help on configuring the execution settings.

- Click 'Save' when done

**Restart Control**

- Modify the restart options for the endpoint after the procedure has run successfully.



Restart option
Suppress the reboot

Restart option
○ Force the reboot in
5 minutes
● Suppress the reboot
○ Warn about the reboot and let users postpone it

Reboot message
Enter a message that the device owner will get before the reboot

- See the explanation of **Procedure Configuration** in **Create a Custom Procedure** for help on configuring the restart control settings.
- Click 'Save' when done

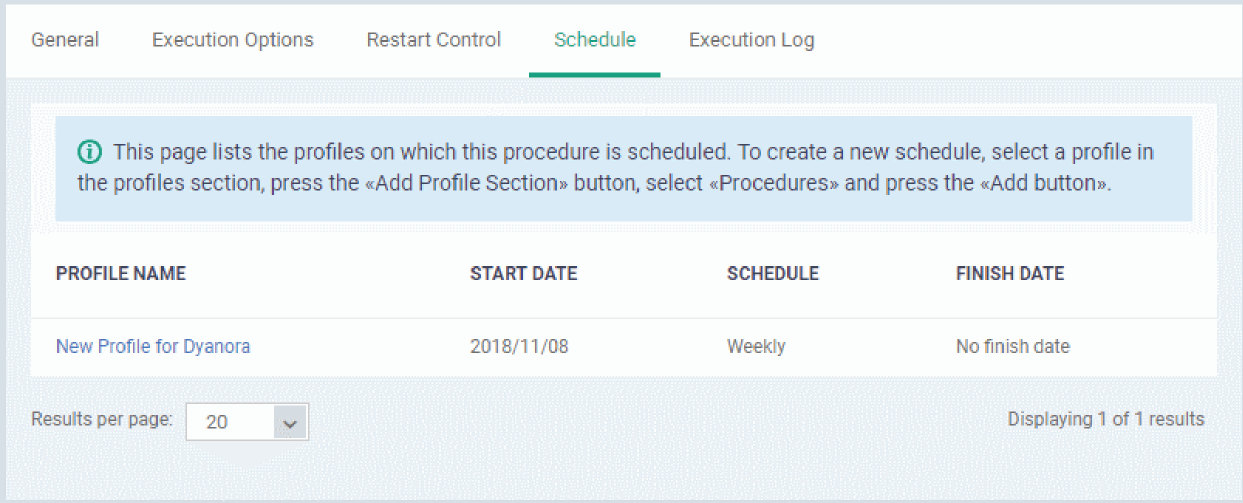
**Execution Log**

- Displays the results of the patch procedure that was executed, both manually and scheduled on Windows profiles.

**Schedule**

The schedule can be edited only in the profile(s) that the procedure is deployed.

- Click the 'Schedule' tab to view the profile(s) in which the procedure is being used.



This page lists the profiles on which this procedure is scheduled. To create a new schedule, select a profile in the profiles section, press the «Add Profile Section» button, select «Procedures» and press the «Add button».

| PROFILE NAME | START DATE | SCHEDULE | FINISH DATE |
|---|---|---|---|
| New Profile for Dyanora | 2018/11/08 | Weekly | No finish date |

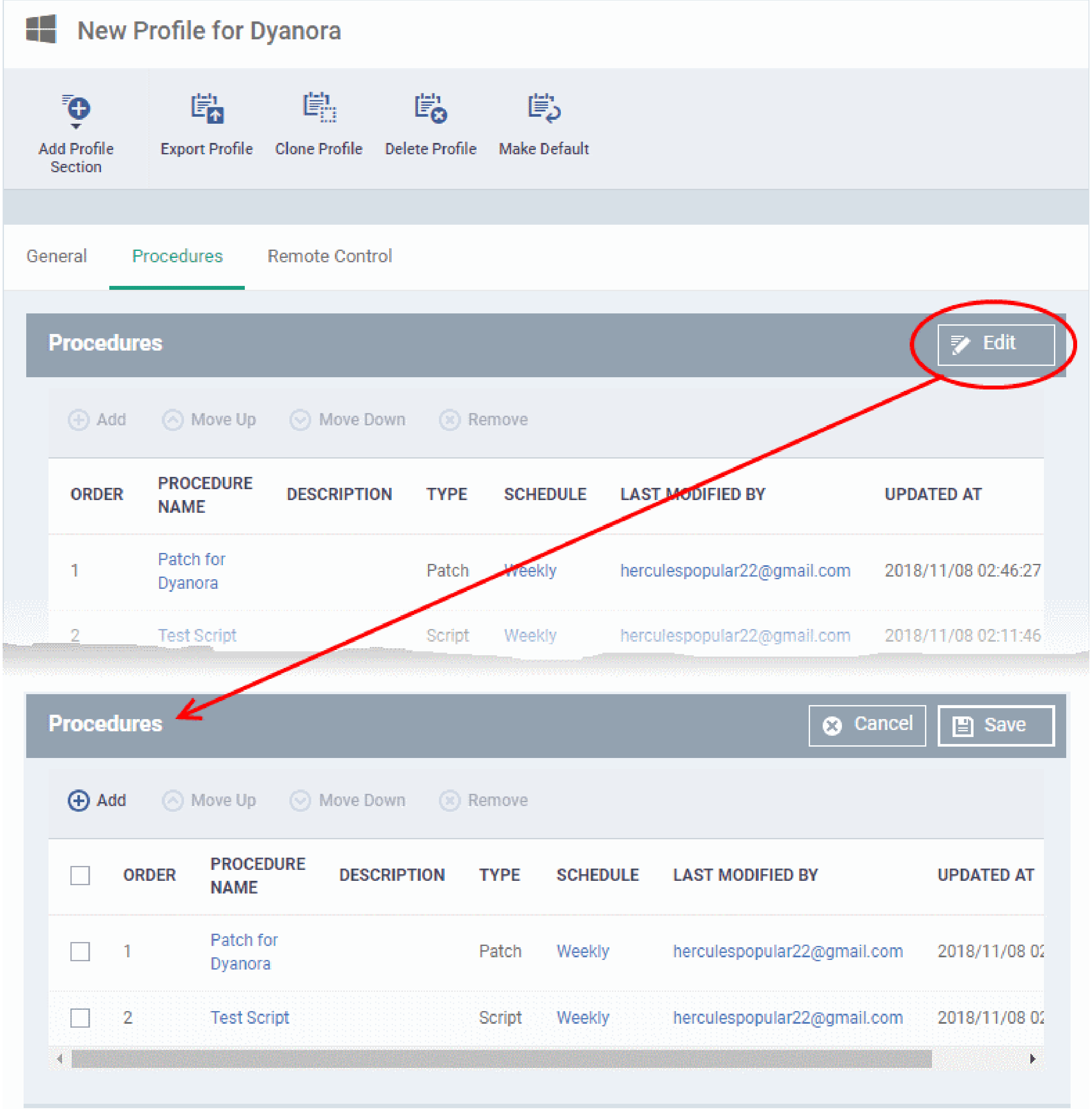
Results per page: 20

Displaying 1 of 1 results

- Click the profile for which you want to edit the procedure schedule.

The selected profile is displayed with the 'Procedure' tab opened.

- Click 'Edit' at the top right.



| ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | LAST MODIFIED BY | UPDATED AT |
|---|---|---|---|---|---|---|
| 1 | Patch for Dyanora | | Patch | Weekly | herculespopular22@gmail.com | 2018/11/08 02:46:27 |
| 2 | Test Script | | Script | Weekly | herculespopular22@gmail.com | 2018/11/08 02:11:46 |

| □ | ORDER | PROCEDURE NAME | DESCRIPTION | TYPE | SCHEDULE | LAST MODIFIED BY | UPDATED AT |
|---|---|---|---|---|---|---|---|
| □ | 1 | Patch for Dyanora | | Patch | Weekly | herculespopular22@gmail.com | 2018/11/08 02 |
| □ | 2 | Test Script | | Script | Weekly | herculespopular22@gmail.com | 2018/11/08 02 |

You can find the procedure type, whether script or patch, under the 'Type' column.

- Click the schedule parameter under 'Schedule' column beside the patch procedure.
- The 'Procedure Schedule' dialog will be displayed. Modify the schedule per your requirement and click 'Set'.
- The schedule will be modified for the profile. Please note the procedure schedule will be impacted for only the profile that you modify. The schedule for the same procedure deployed onto other profiles will not be affected.
- Click 'Save'

The changes for the patch procedure will be saved.

**Important Note:** Patches that are hidden by administrators will not be executed. See **Manage OS Patches on Windows Endpoints** for more details.

## 6.6.10. View Procedure Results

The results of any script or patch procedure can be viewed in the '**Logs**' section of a device. The results can also be found in the 'Procedures' interface.

Click the following links for more details:

- **View script procedure results**
- **View patch procedure results**

### View Script Procedure Results

Script procedure logs can be viewed in two places:

- **Device List** - 'Devices' > 'Device List' > Open a Windows device > 'Logs' > 'Script Logs' - Shows results for all scripts run on a selected device.
- **Procedures area** - 'Configuration Templates' > 'Procedures' > Open a script procedure > 'Execution Log' - Shows all devices on which a selected script was run.

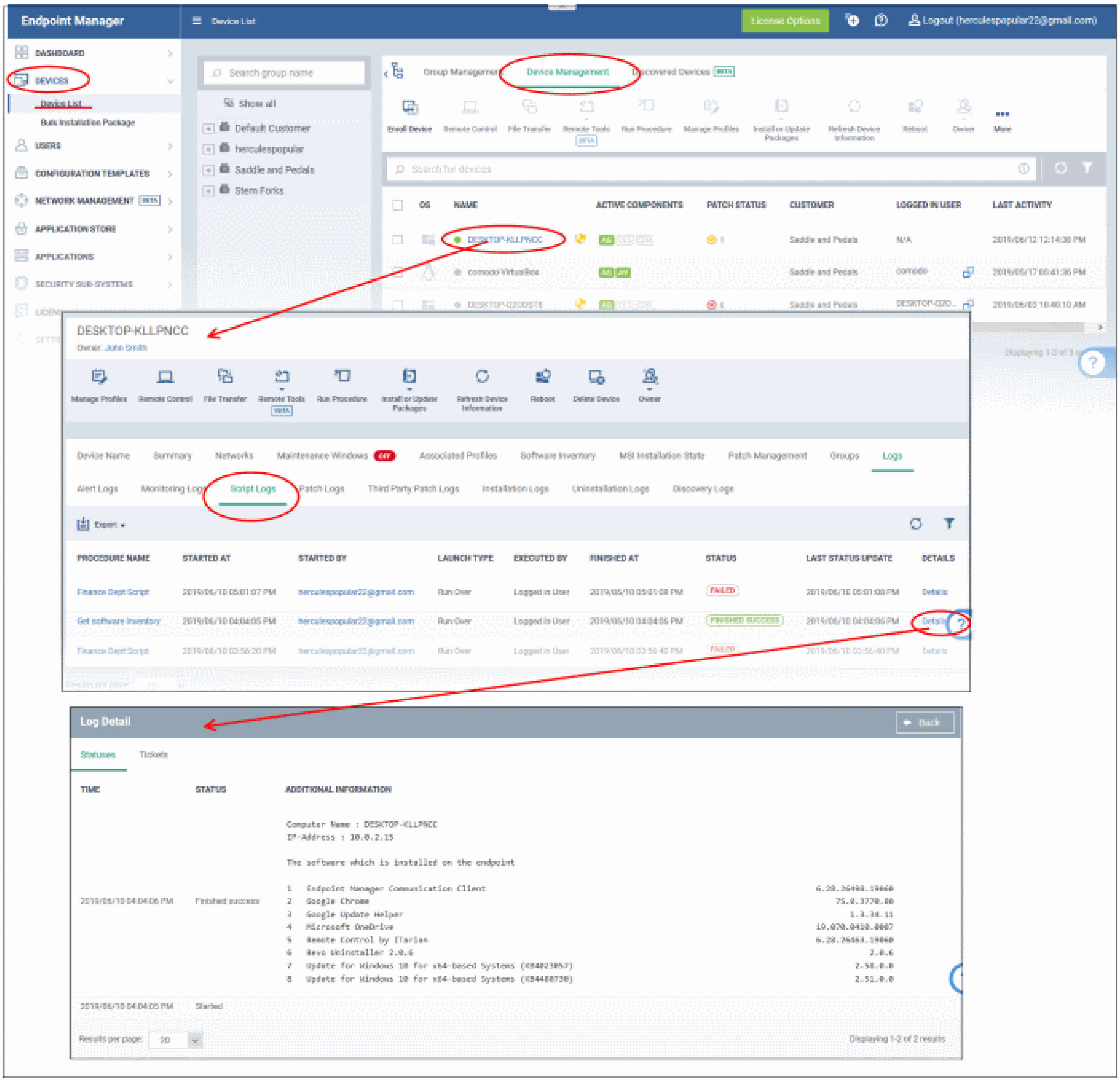
**Script procedures results on a particular device**

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
    - Select a company or a group to view just their devices

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Logs' tab in the device details interface
- Select the 'Script Logs' sub-tab

This opens the list of all script procedures run on the device. You can also see the scripts start/end time and whether or not it was successful.

- To view the results of a particular procedure, click 'Details' in the row of the procedure name.



| OS | NAME | ACTIVE COMPONENTS | PATCH STATUS | CUSTOMER | LOGGED IN USER | LAST ACTIVITY |
|---|---|---|---|---|---|---|
| | DESKTOP-KLLPNCC | AS | 1 | Saddle and Pedals | N/A | 2019/06/12 12:14:38 PM |
| | comodo-VirtualBox | AS AV | | Saddle and Pedals | comodo | 2019/05/17 05:41:36 PM |
| | DESKTOP-O20DS18 | AS | 6 | Saddle and Pedals | DESKTOP-O20... | 2019/06/03 10:40:10 AM |

| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| Finance Dept Script | 2019/06/10 05:01:07 PM | herculespopular22@gmail.com | Run Over | Logged in User | 2019/06/10 05:01:08 PM | FAILED | 2019/06/10 05:01:08 PM | Details |
| Get software inventory | 2019/06/10 04:04:05 PM | herculespopular22@gmail.com | Run Over | Logged in User | 2019/06/10 04:04:06 PM | FINISHED SUCCESS | 2019/06/10 04:04:06 PM | Details |
| Finance Dept Script | 2019/06/10 03:56:20 PM | herculespopular22@gmail.com | Run Over | Logged in User | 2019/06/10 03:56:40 PM | FAILED | 2019/06/10 03:56:40 PM | Details |

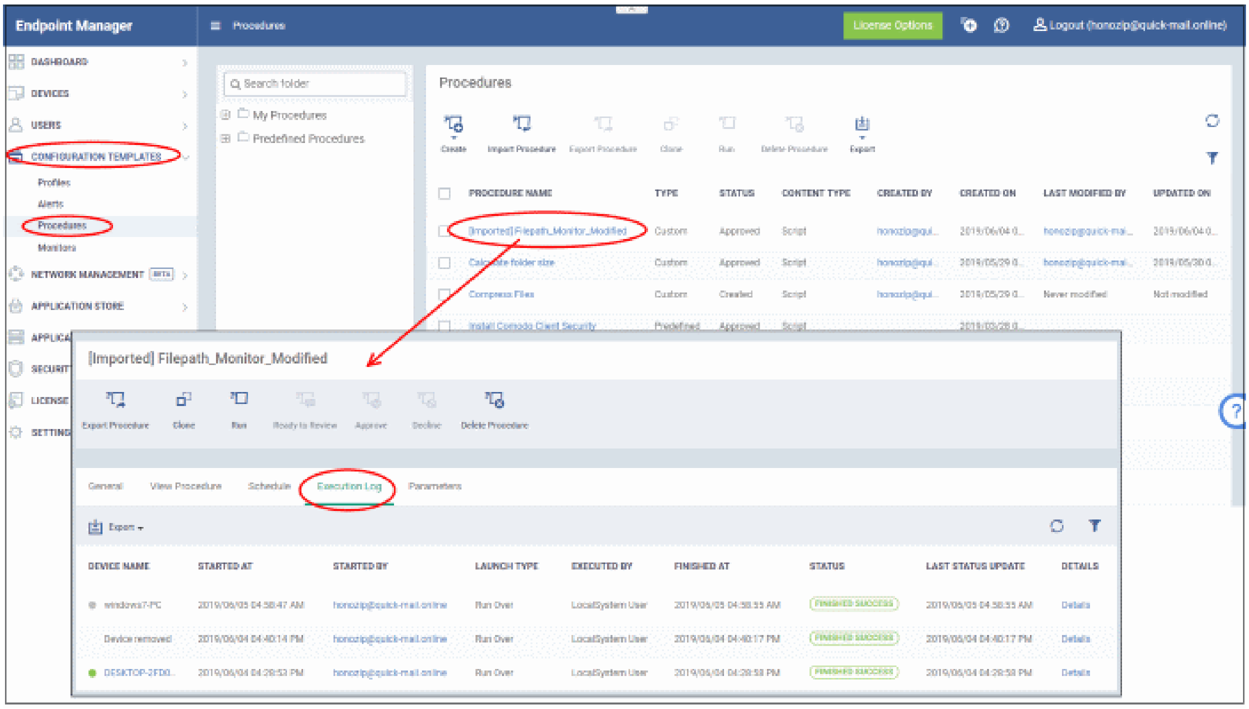
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/06/10 04:04:06 PM | Finished success | (see output below) |
| 2019/06/10 04:04:05 PM | Started | |

```
Computer Name : DESKTOP-KLLPNCC
IP-Address : 10.0.2.15

The software which is installed on the endpoint

1   Endpoint Manager Communication Client                          6.28.26498.19060
2   Google Chrome                                                   75.0.3770.80
3   Google Update Helper                                            1.3.34.11
4   Microsoft OneDrive                                             19.070.0410.0007
5   Remote Control by ITarian                                      6.28.26463.19060
6   Revo Uninstaller 2.0.6                                          2.0.6
7   Update for Windows 10 for x64-based Systems (KB4023057)         2.58.0.0
8   Update for Windows 10 for x64-based Systems (KB4480730)         2.51.0.0
```

- The 'Tickets' tab lists tickets which were created as a result of a failed procedure. Clicking the ticket link will open the ticket in service desk.

### Results of a selected script on all devices

- Click 'Configuration Templates' > 'Procedures'.
- Browse the folder tree to locate the procedure for which you want to view results
- Click the name of the script procedure then click 'Execution Log'
- This will open a list of all devices on which the script was run



| PROCEDURE NAME | TYPE | STATUS | CONTENT TYPE | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|---|---|
| [Imported] Filepath_Monitor_Modified | Custom | Approved | Script | honozip@qui... | 2019/06/04 0... | honozip@quick-mai... | 2019/06/04 0... |
| Calculate folder size | Custom | Approved | Script | honozip@qui... | 2019/05/29 0... | honozip@quick-mai... | 2019/05/30 0... |
| Compress Files | Custom | Created | Script | honozip@qui... | 2019/05/29 0... | Never modified | Not modified |
| Install Comodo Client Security | Predefined | Approved | Script | | 2019/03/28 0... | | |

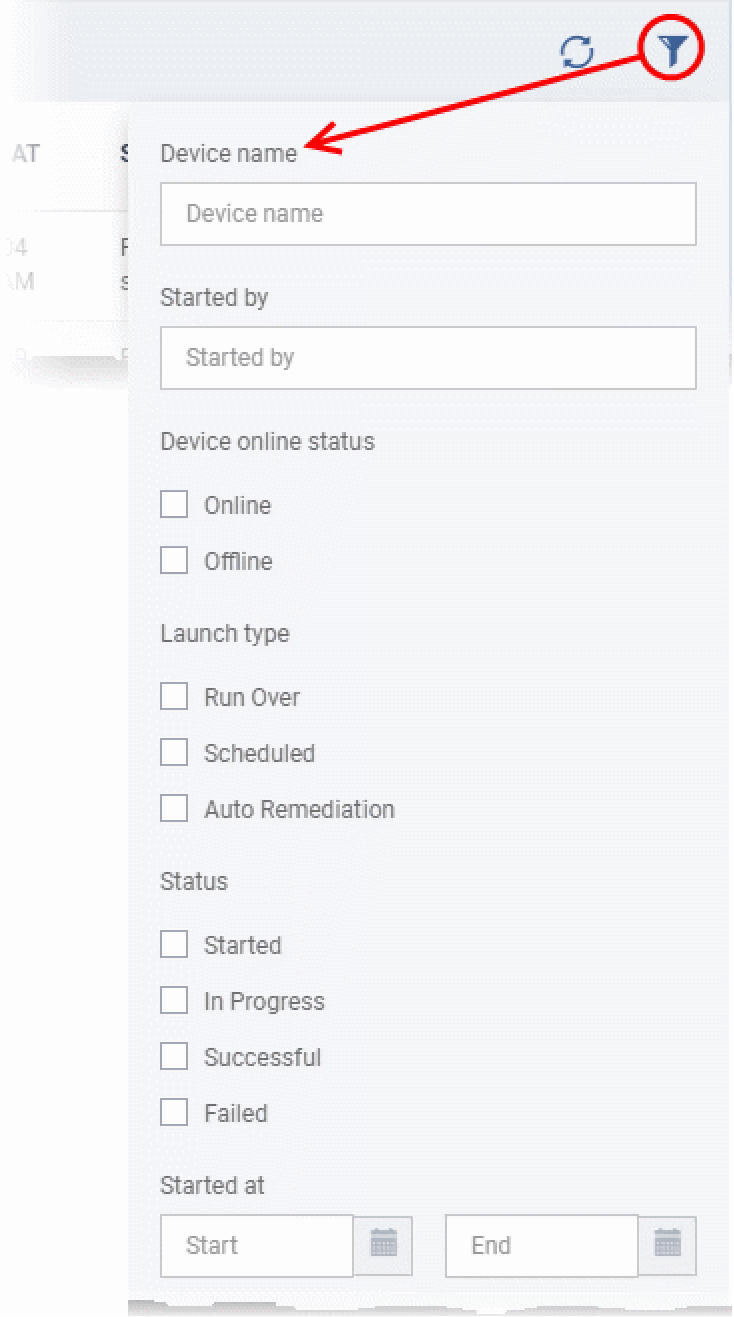
| DEVICE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| windows7-PC | 2019/06/05 04:58:47 AM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/05 04:58:55 AM | FINISHED SUCCESS | 2019/06/05 04:58:55 AM | Details |
| Device removed | 2019/06/04 04:40:14 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:40:17 PM | FINISHED SUCCESS | 2019/06/04 04:40:17 PM | Details |
| DESKTOP-2FD0... | 2019/06/04 04:28:53 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:28:58 PM | FINISHED SUCCESS | 2019/06/04 04:28:58 PM | Details |

| Script Procedure Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Device Name | The label of the Windows device on which the script procedure was run.<br>• Click the device name to open the device details interface of the respective device.<br>• See **Manage Windows Devices** for more details. |
| Started At | The date and time when the procedure commenced on the device. |
| Started By | Who or what launched the procedure.<br>• A profile name will be shown here if the procedure was scheduled in a profile which is active on the device.<br>• An admins name or email address will be shown if the procedure was run manually.<br>  • Click the name/email address to view the details of the admin. |
| Launch Type | Whether the procedure was scheduled or run manually. |
| Executed By | The user account type used by Endpoint Manager to execute the procedure. |
| Finished At | The date and time when the procedure was completed. |
| Status | Whether the script successfully executed or not. Each status is color coded:<br>• Started - Blue<br>• In progress - Blue<br>• Finished Success - Green<br>• Failed - Red |

| | |
|---|---|
| | You can configure an alert if a procedure deployment fails. See '**Manage Procedures**' for more details. |
| Last Status Update | The date and time when the information was last updated. |
| Details | • Click the 'Details' link to view a log of the procedure's execution.<br>• See the explanation of **View results of script procedure execution on a device** given below. |

**Sorting and Filtering**

- Click any column header except 'Device Name' and 'Started By' to sort the items in alphabetical order of entries in that column.
- Click the funnel icon on the right to open the filter options.



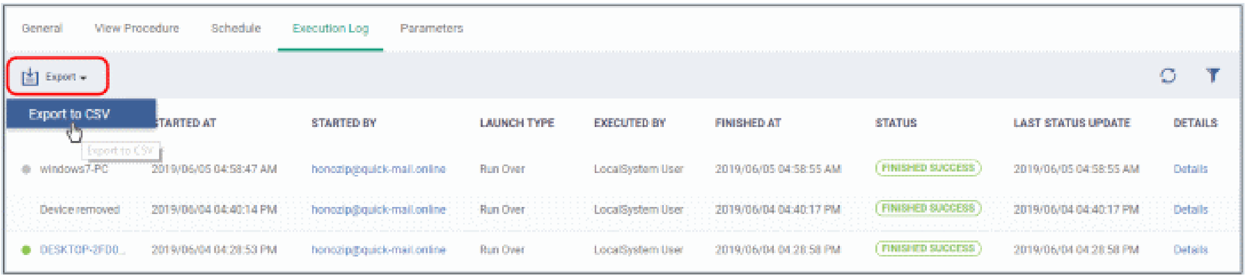
- To filter the items or search for a specific item, enter and/or select the search criteria and click 'Apply'

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'.
- EM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.
- To reload the list with latest results, click the 'Refresh' icon.

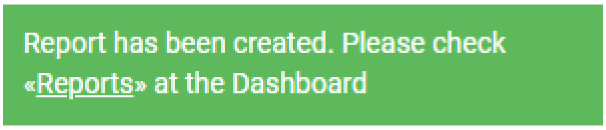
**Export script procedure execution records as a CSV file**

- Click 'Configuration Templates' > 'Procedures' > click on a script procedure
- Click the 'Execution Log' sub-tab
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| | TARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| windows7-PC | 2019/06/05 04:58:47 AM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/05 04:58:55 AM | FINISHED SUCCESS | 2019/06/05 04:58:55 AM | Details |
| Device removed | 2019/06/04 04:40:14 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:40:17 PM | FINISHED SUCCESS | 2019/06/04 04:40:17 PM | Details |
| DESKTOP-2FD0... | 2019/06/04 04:28:53 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:28:58 PM | FINISHED SUCCESS | 2019/06/04 04:28:58 PM | Details |

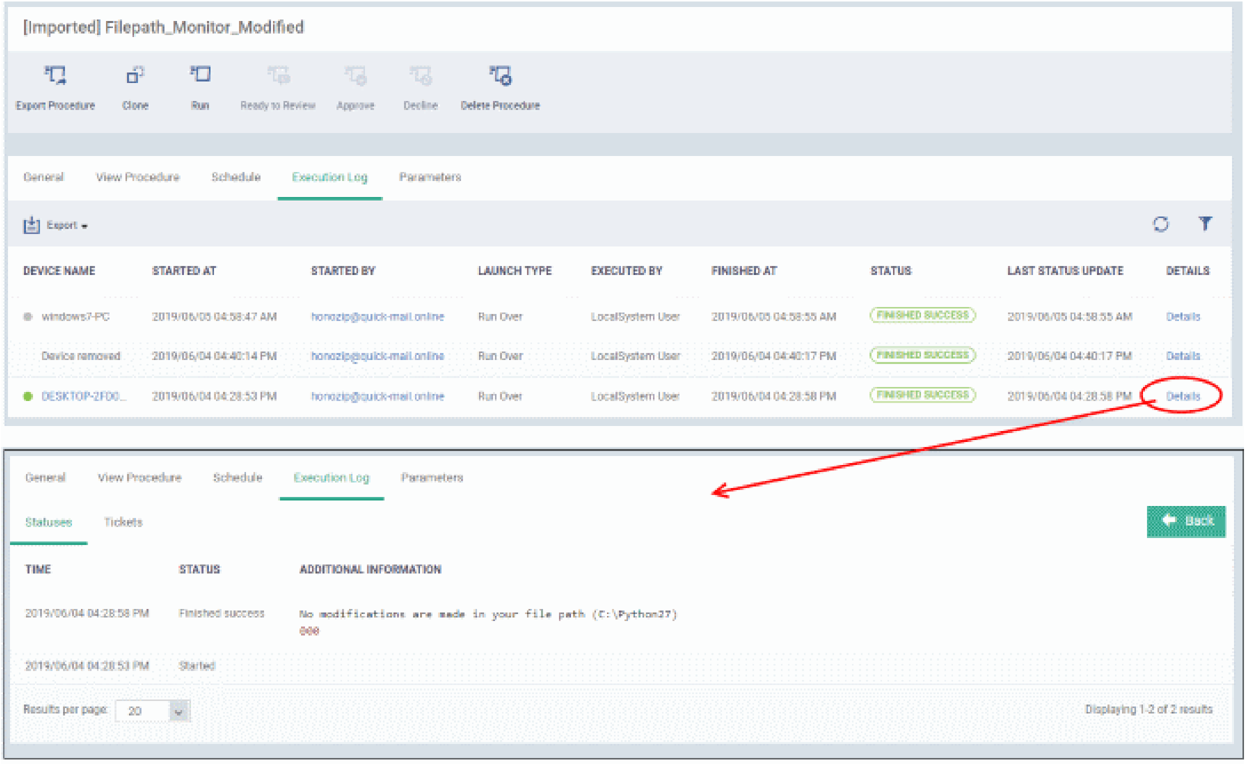
The report is generated in .csv file format.


Report has been created. Please check «Reports» at the Dashboard

Click 'Dashboard' > 'Reports' to view the report. See **Reports** if you need more help with this interface.

**View results of script procedure execution on a device**

- Click 'Details' in the row of a device to view specific results:



| DEVICE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | EXECUTED BY | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|---|
| windows7-PC | 2019/06/05 04:58:47 AM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/05 04:58:55 AM | FINISHED SUCCESS | 2019/06/05 04:58:55 AM | Details |
| Device removed | 2019/06/04 04:40:14 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:40:17 PM | FINISHED SUCCESS | 2019/06/04 04:40:17 PM | Details |
| DESKTOP-2F00... | 2019/06/04 04:28:53 PM | honozip@quick-mail.online | Run Over | LocalSystem User | 2019/06/04 04:28:58 PM | FINISHED SUCCESS | 2019/06/04 04:28:58 PM | Details |

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/06/04 04:28:58 PM | Finished success | No modifications are made in your file path (C:\Python27)<br>000 |
| 2019/06/04 04:28:53 PM | Started | |

Results per page: 20

Displaying 1-2 of 2 results

The details are shown under two tabs:

- **Statuses -** The date and time at which successive stages in the procedure were run, their success status and results.

  For example, the 'Get Running Processes' results show a list of all processes found running on the device.
- **Tickets -** Shows tickets raised for any failed procedures.
  - Click the ticket link to open the ticket in service desk.

## View Patch Procedure Results

Patch procedure results can be viewed in two interfaces - 'Device List' and 'Procedures'.

- **Device List -** 'Devices' > 'Device List' > *Open a Windows device* > 'Logs' > 'Patch Logs' - Displays results for all patch procedures run on a selected device.
- **Procedures area -** 'Configuration Templates' > 'Procedures' > *Open a patch procedure* > 'Execution Log' - Displays all devices on which the selected patch procedure was run.

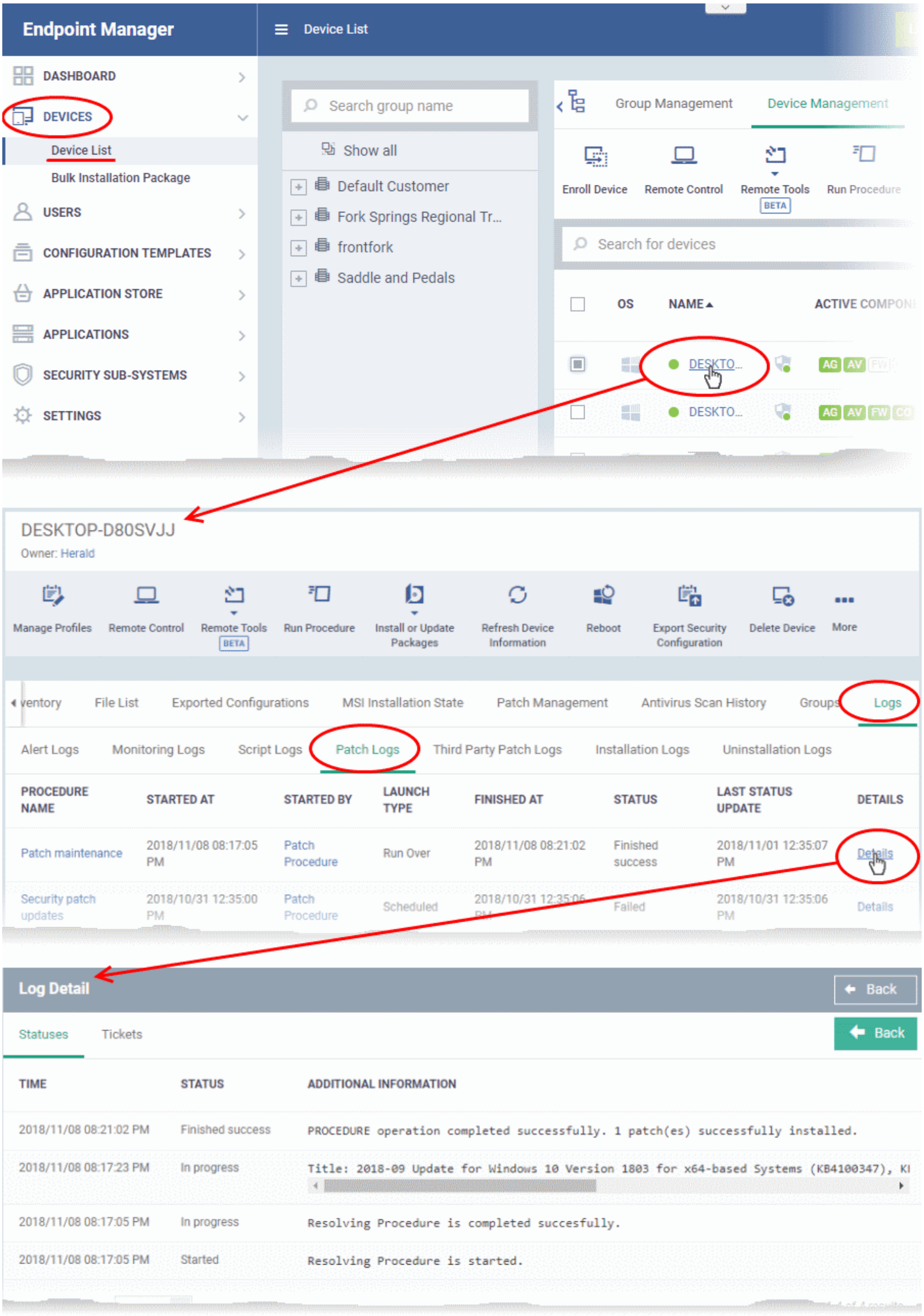
### Patch procedure results on a specific device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top-menu
  - Select a company or a group to view just their devices

    Or
  - Select 'Show all' to view every device enrolled to EM
- Click on any Windows device then select the 'Logs' tab in the device details interface
- Select the 'Patch Logs' sub-tab

This opens a list of all patch procedures run on the device along with their status (success/failure), their start/finish time and time of last status update.

- Click 'Details' in the row of a procedure to view specific results:



| PROCEDURE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| Patch maintenance | 2018/11/08 08:17:05 PM | Patch Procedure | Run Over | 2018/11/08 08:21:02 PM | Finished success | 2018/11/01 12:35:07 PM | Details |
| Security patch updates | 2018/10/31 12:35:00 PM | Patch Procedure | Scheduled | 2018/10/31 12:35:06 PM | Failed | 2018/10/31 12:35:06 PM | Details |

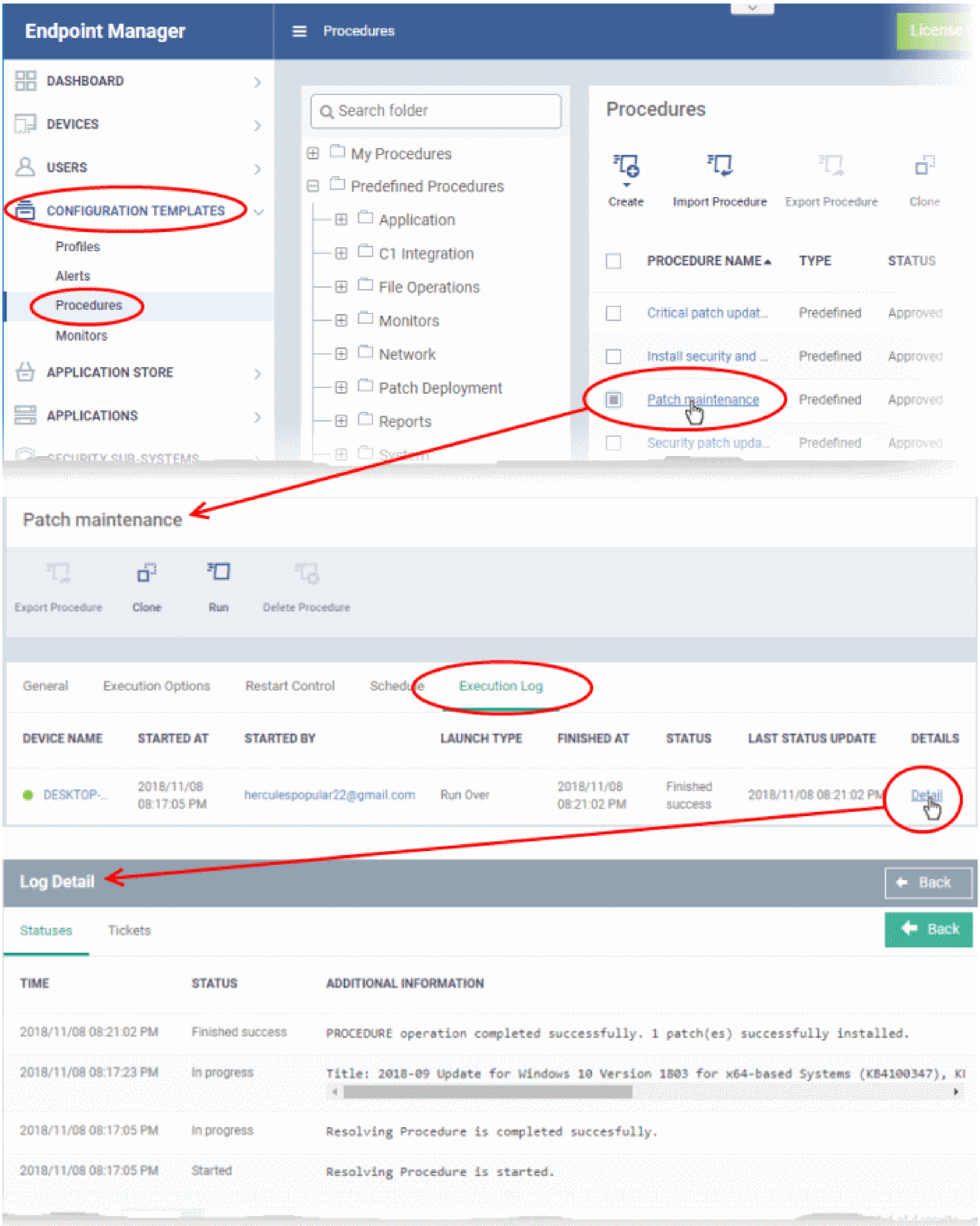
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/11/08 08:21:02 PM | Finished success | `PROCEDURE operation completed successfully. 1 patch(es) successfully installed.` |
| 2018/11/08 08:17:23 PM | In progress | `Title: 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347), KI` |
| 2018/11/08 08:17:05 PM | In progress | `Resolving Procedure is completed succesfully.` |
| 2018/11/08 08:17:05 PM | Started | `Resolving Procedure is started.` |

- The 'Tickets' tab shows tickets which were created as a result of a failed procedure. Click the ticket link to open the ticket in service desk.

**Results of a selected patch procedure run on all devices**

- Click 'Configuration Templates' > 'Procedures'.

- Click the name of the patch procedure under 'My Procedures' or 'Predefined Procedures' for which you want to view results, then click 'Execution Log' in the Procedure Details screen.
- This will open a list of all devices on which the script procedure was run along with their status (success/failure), their start/finish time and time of last status update.
- Click 'Details' in the row of a device to view specific results:



| DEVICE NAME | STARTED AT | STARTED BY | LAUNCH TYPE | FINISHED AT | STATUS | LAST STATUS UPDATE | DETAILS |
|---|---|---|---|---|---|---|---|
| ● DESKTOP-... | 2018/11/08 08:17:05 PM | herculespopular22@gmail.com | Run Over | 2018/11/08 08:21:02 PM | Finished success | 2018/11/08 08:21:02 PM | Detail |

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/11/08 08:21:02 PM | Finished success | PROCEDURE operation completed successfully. 1 patch(es) successfully installed. |
| 2018/11/08 08:17:23 PM | In progress | Title: 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347), KI |
| 2018/11/08 08:17:05 PM | In progress | Resolving Procedure is completed succesfully. |
| 2018/11/08 08:17:05 PM | Started | Resolving Procedure is started. |

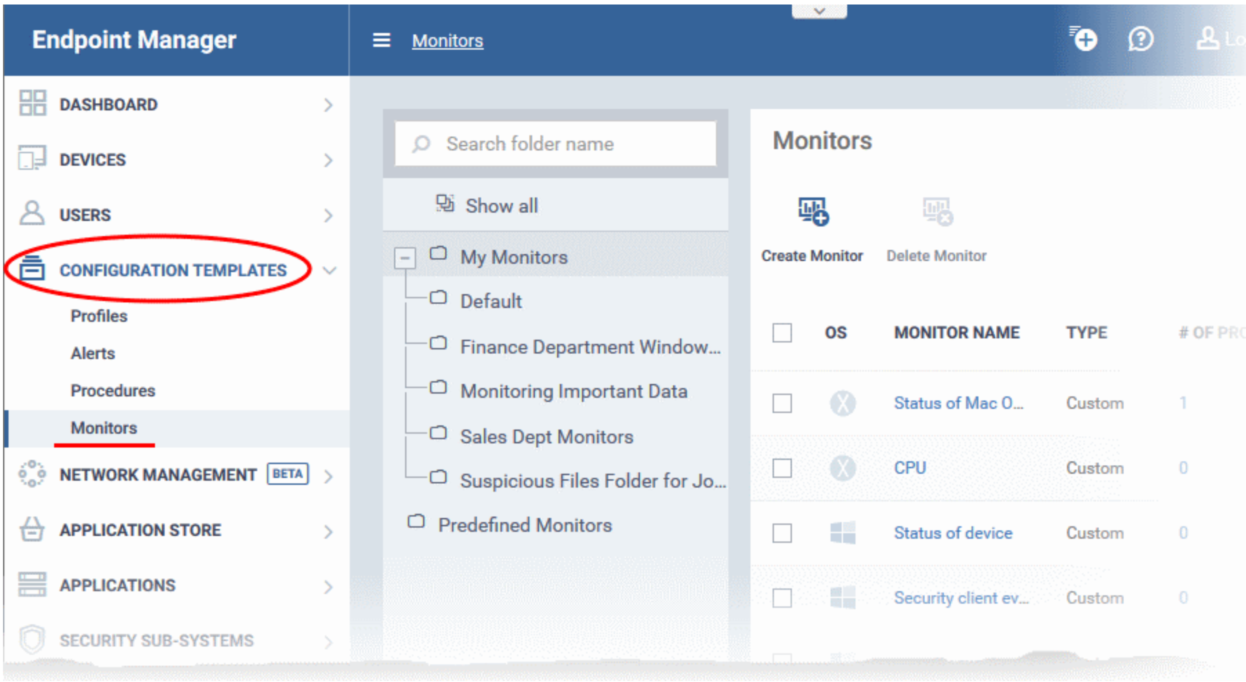
- The 'Tickets' tab displays a list of tickets which were created as a result of a failed procedure. Clicking the ticket link will open the ticket in service desk.
- Note - Sorting, filtering and exporting is similar to that for script procedure results explained above.

# 6.7. Manage Monitors

- Click 'Configuration Templates' > 'Monitors'
- A monitor is a script which tracks events on managed Windows and Mac OS devices. You can instruct the monitor to take specific actions if its conditions are met.
- For example, 'Alert me when a USB removable disk is connected to the system', or 'Create a log entry if CPU usage goes above 75% for a certain length of time'.
- You can also tell a monitor to run a procedure to remediate issues.
- Monitors are added to configuration profiles which are in-turn applied to a devices. To add a monitor to a profile:
    - Click 'Configuration Templates' > 'Profiles'
    - Open an existing profile or create a new profile
    - Click 'Add Profile Section' > 'Monitoring'
- A single monitor can be used in multiple profiles. A single profile can include any number of monitors.
- There are two types of monitors:
    - **Predefined Monitors -** A collection of monitors from Comodo which perform a range of useful monitoring tasks. These can be used in custom profiles, but cannot be edited.
    - **My Monitors -** Custom monitors that you create. These monitors are saved in the 'My Monitors' folder. You can add custom sub-folders as required.

**View and manage monitors**

- Click 'Configuration Templates' > 'Monitors'



| OS | MONITOR NAME | TYPE | # OF PR |
|---|---|---|---|
| | Status of Mac O... | Custom | 1 |
| | CPU | Custom | 0 |
| | Status of device | Custom | 0 |
| | Security client ev... | Custom | 0 |

| Monitors - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system that the monitor supports. |
| Monitor Name | The monitor label.<br>• Click the name of a monitor view and edit it. See **View and Edit Monitors** for |

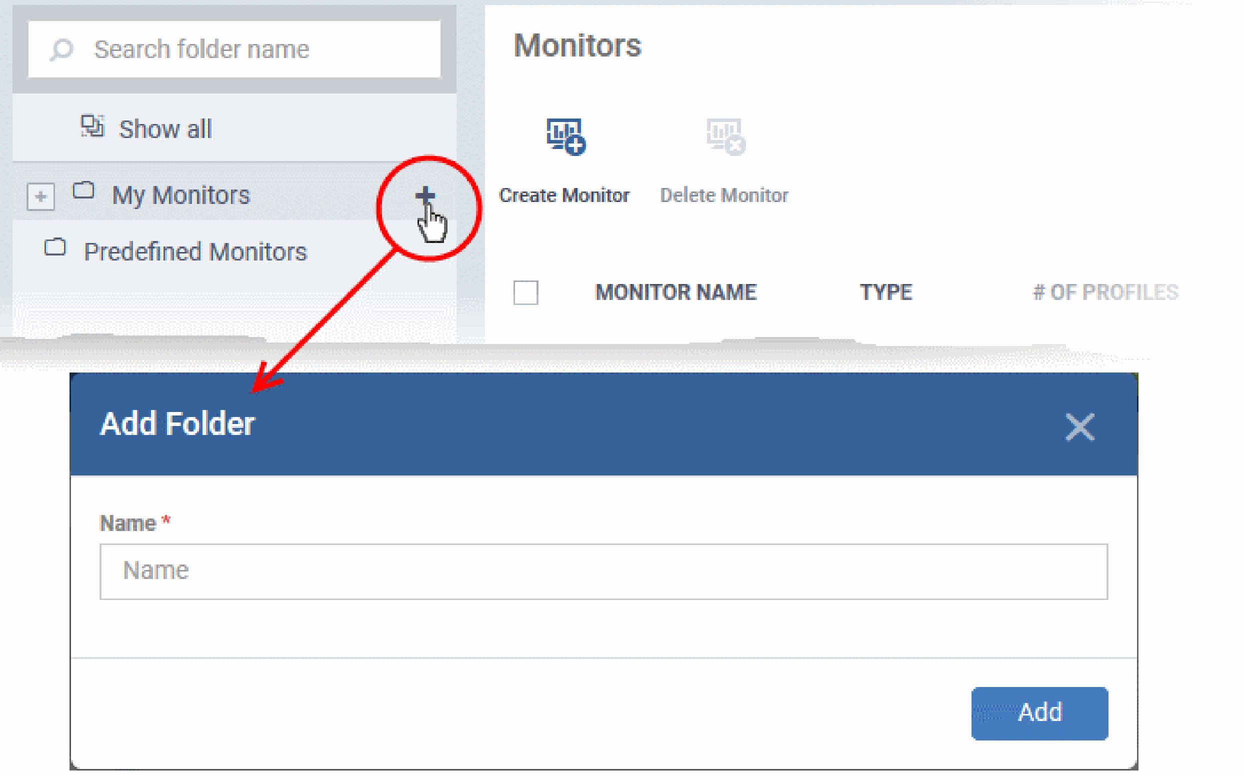
| | |
|---|---|
| | more details. |
| Type | Whether the monitor is custom or predefined |
| Number of profiles | The quantity of profiles on which the monitor is active. |
| Created by | The administrator who created the custom monitor.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created On | Date and time the monitor was created. |
| Last Modified By | The admin who most recently edited the monitor. |
| Updated On | Date and time the monitor was last edited. |
| **Controls** | |
| Create Monitor | Configure a new monitor. See '**Create Monitors and Add them to Profiles**' for help with this. |
| Delete Monitor | Remove monitors from Endpoint Manager. Use the check-boxes to select the monitors to be removed. |

- Click any column header to sort the items in ascending/descending order of entries in that column.
- Click the funnel icon on the right to search for monitors

Next, see **Create a monitor and add it to a profile**

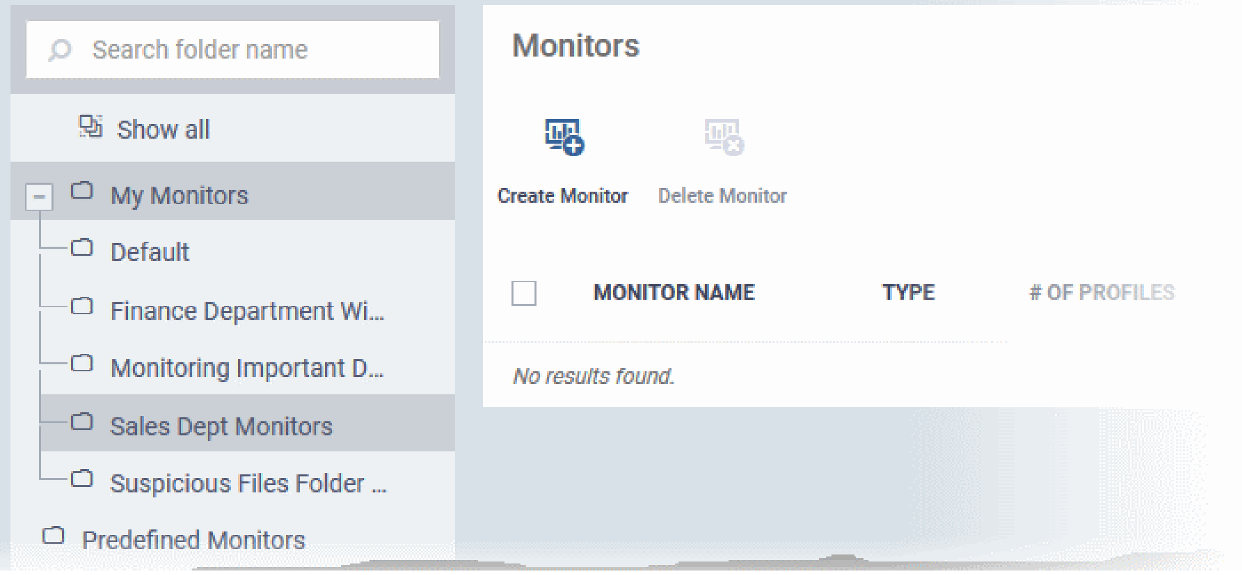
### Add a sub folder to the 'My Monitors' folder

- Click 'Configuration Templates' > 'Monitors'
- Place your mouse on the 'My Monitors' folder and click '+' beside it



- Enter a name for the sub-folder to be created in the 'Add Folder' dialog and click 'Add'

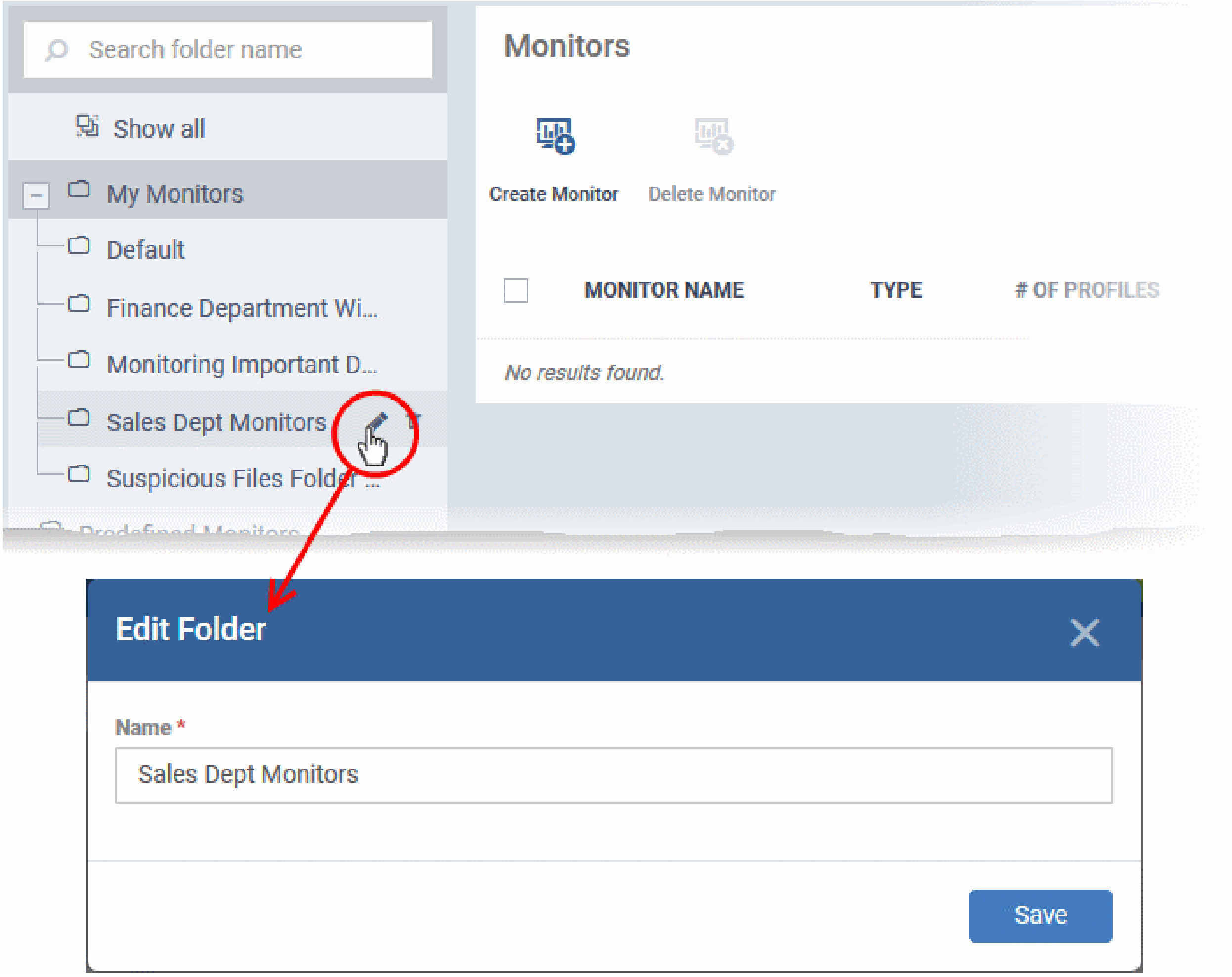
The sub-folder will be created and displayed under 'My Monitors'



You can also add sub-folders of a sub-folder. Once sub folders are created, you can create new monitors inside them. See **Create Monitors and Add them to Profiles** for more details about adding new monitors.

### Edit the name of a sub folder under 'My Monitors'

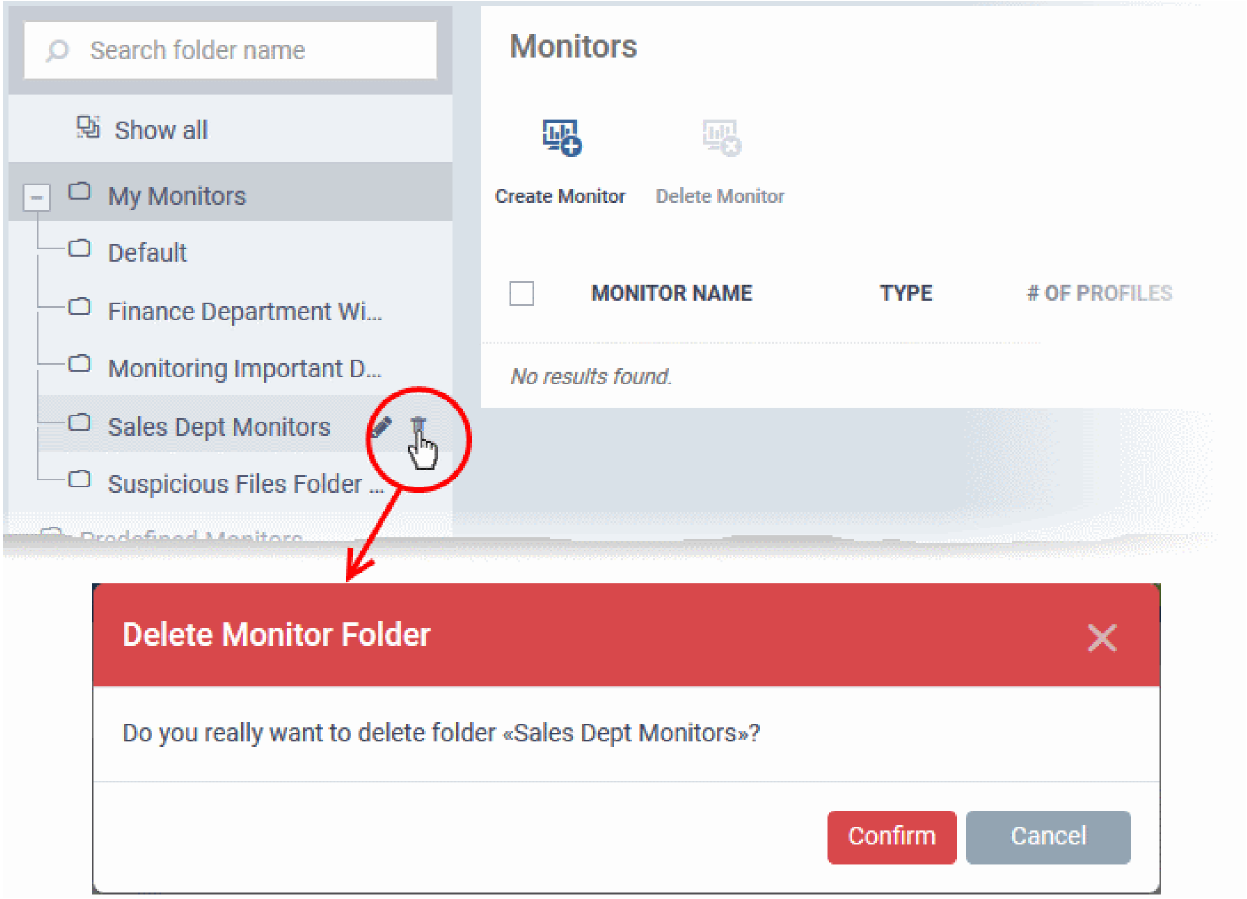
- Click 'Configuration Templates' > 'Monitors'
- Expand the 'My Monitors' folder (or the parent folder of the sub-folder)
- Place your mouse on the sub folder and click the pencil symbol beside it
- Enter a new name for the sub folder in the 'Edit Folder' dialog and click 'Save'



The folder name will be updated in folder tree.

**Remove a sub folder under 'My Monitors' folder**

- Click 'Configuration Templates' > 'Monitors'
- Expand the 'My Monitors' folder (or the parent folder of the sub-folder)
- Place your mouse on the sub folder and click the trash can symbol beside it



Do you really want to delete folder «Sales Dept Monitors»?

- Click 'Confirm' to remove the folder.

**Note**: You can only remove empty folders. Delete all monitors in a folder before attempting to delete the folder.

Following sections explain more about:

- **Create Monitors and Add them to Profiles**
- **View and Edit Monitors**

## 6.7.1. Create Monitors and Add them to Profiles

Custom monitors let you track and respond to events of your choice. For example, you may create a monitor to alert you if disk space on a device falls below 10%.

- You can set a monitor to run a specific procedure if its conditions are met. For example, you could run a disk-defrag procedure when free space falls below a set threshold. (Windows only)

- You can also configure custom notifications by modifying the alert template on the procedure. Click 'Configuration Templates' > 'Alerts' to view alert templates.

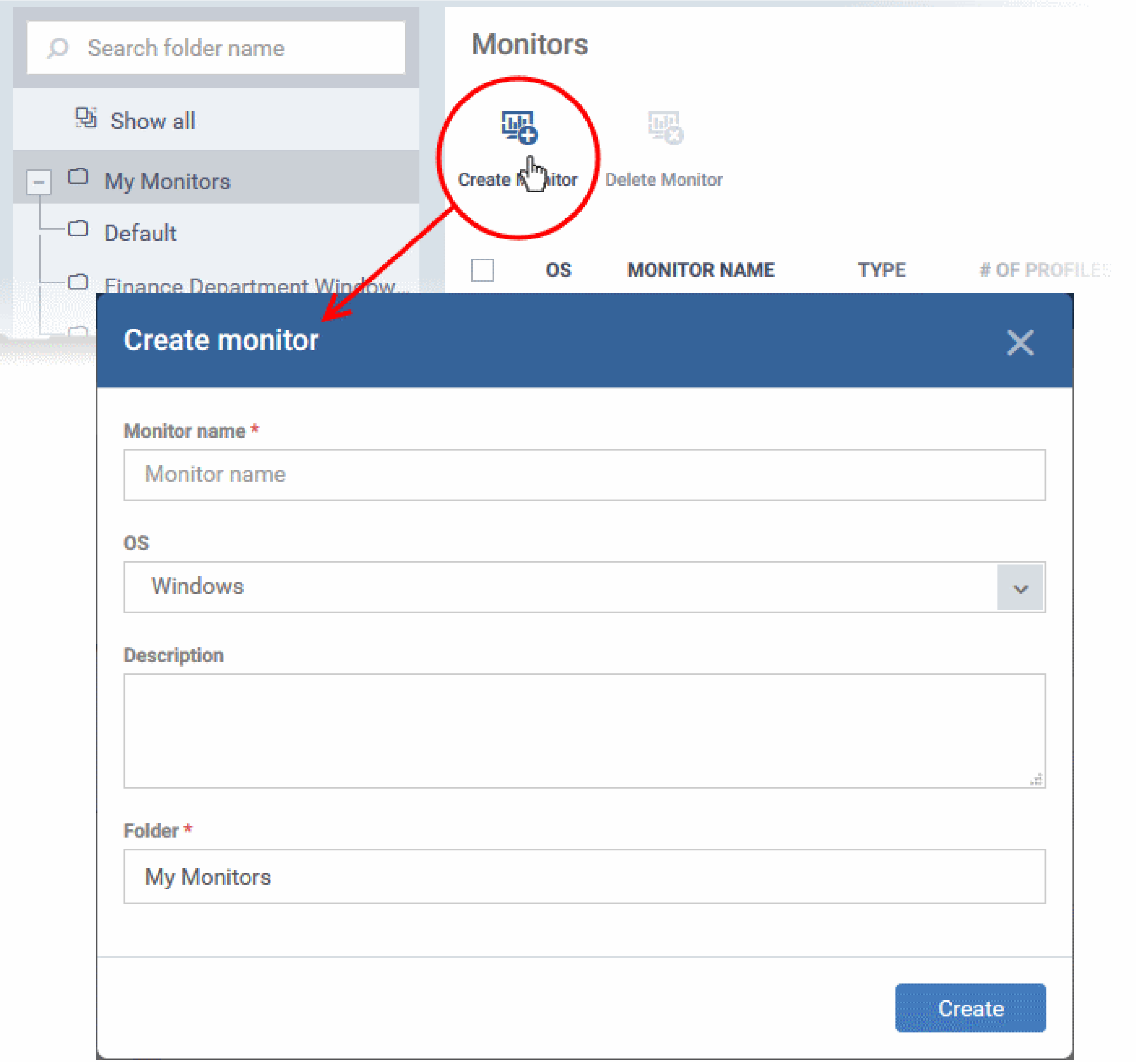
Monitors are added to security profiles which, in-turn, are deployed to devices. You need to add a 'Monitors' section to a profile to add your monitor.

See the following sections for help with creating OS-specific monitors:

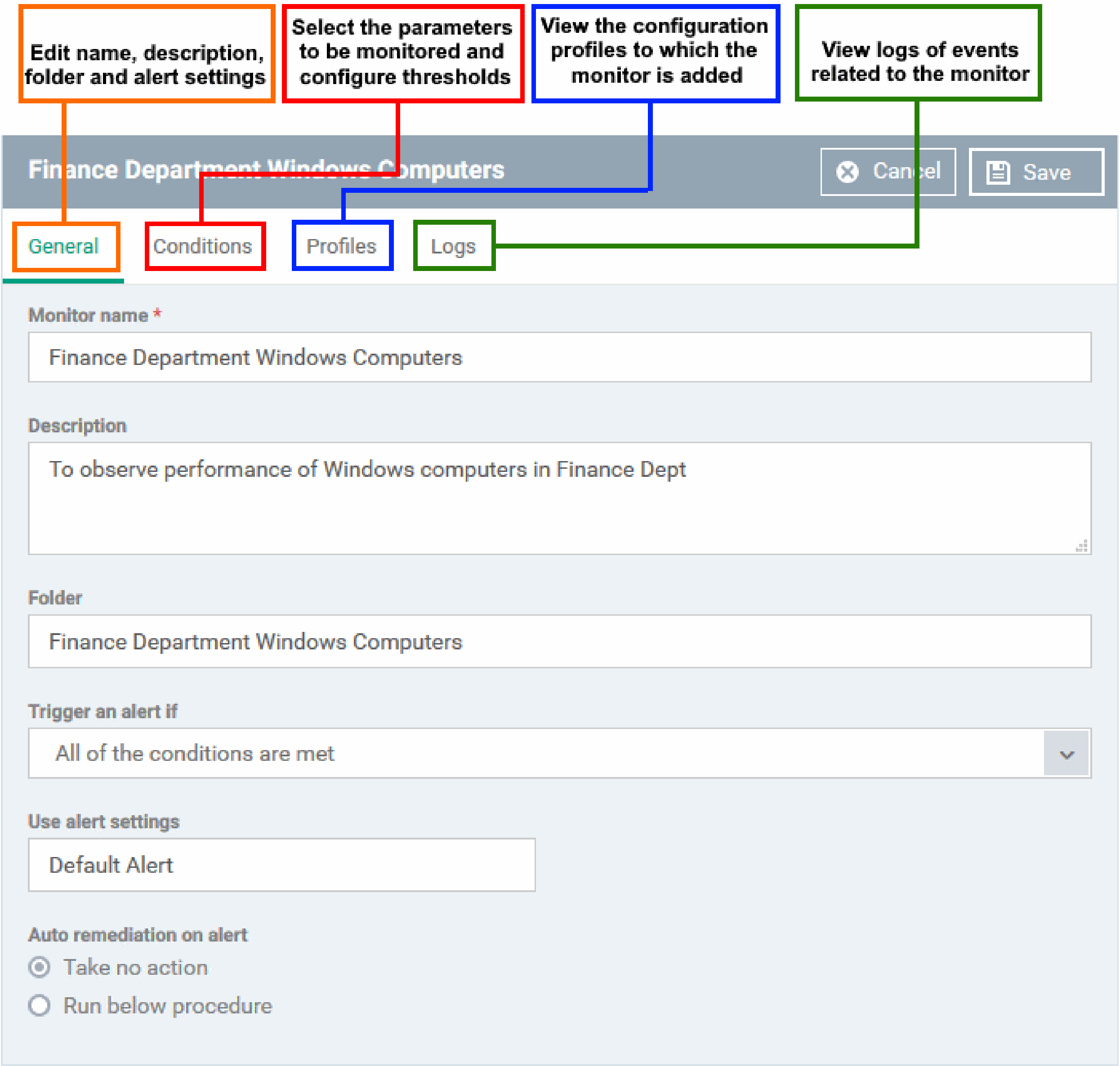
- **Monitors for Windows Devices**
- **Monitors for Mac OS Devices**

### 6.7.1.1. Monitors for Windows Devices

- Click 'Configuration Templates' > 'Monitors'
- Click 'Create Monitor'



- Enter a label and description for the monitor
- Select 'Windows' in the OS drop-down
- Specify where to save the new monitor. You can create new sub-folders under 'My Monitors' if required.
- Click 'Create'.
- You will be taken to the monitor configuration screen:



Edit name, description, folder and alert settings
Select the parameters to be monitored and configure thresholds
View the configuration profiles to which the monitor is added
View logs of events related to the monitor
Finance Department Windows Computers
Cancel
Save
General
Conditions
Profiles
Logs

Monitor name *: Finance Department Windows Computers

Description: To observe performance of Windows computers in Finance Dept

Folder: Finance Department Windows Computers

Trigger an alert if: All of the conditions are met

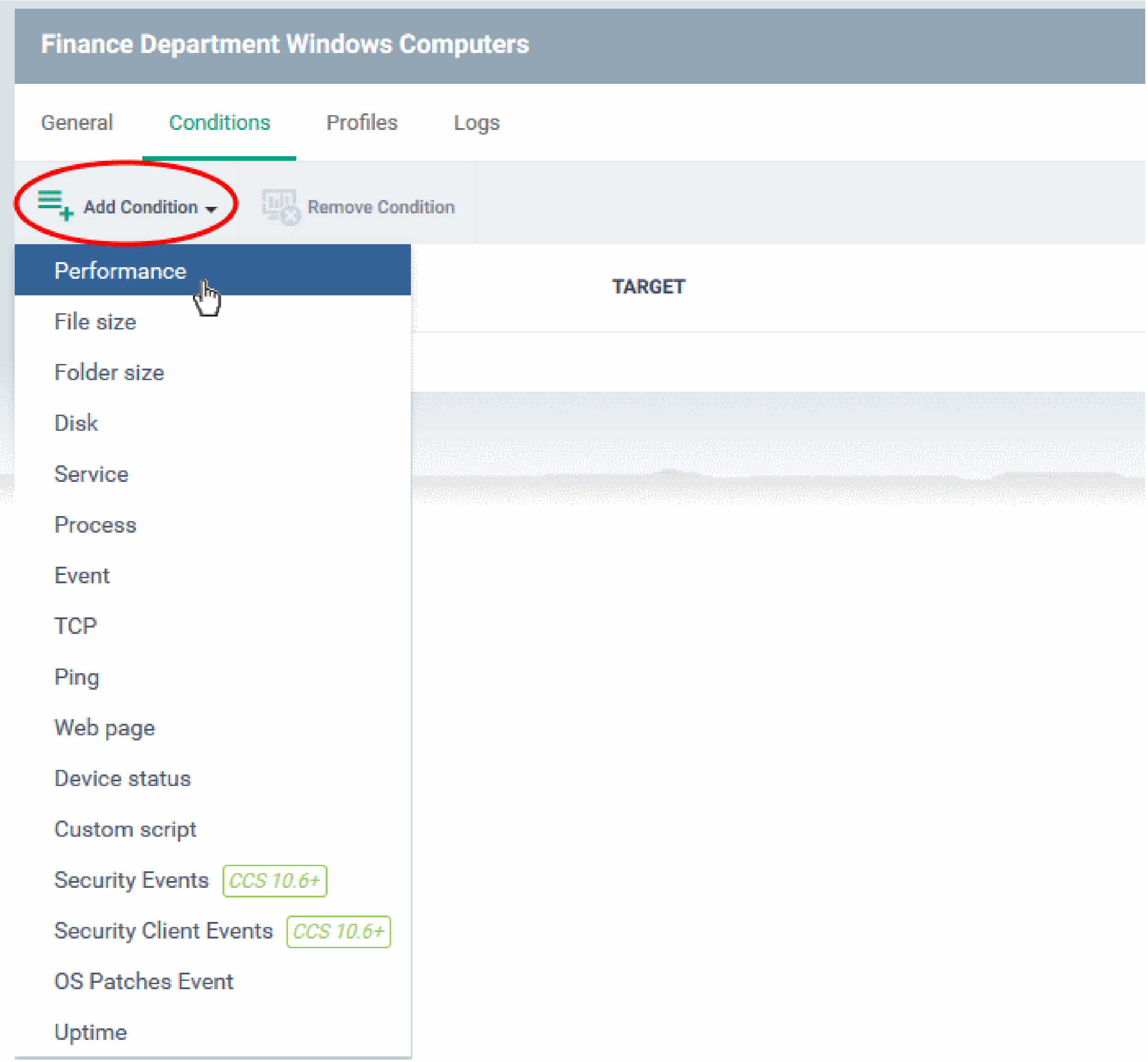
Use alert settings: Default Alert

Auto remediation on alert

● Take no action

○ Run below procedure

- Modify the following settings if required:
- **Trigger an alert if -** Select when the alert should be sent to admins. The options are send alert when all conditions are met or when any condition is met.
- **Use Alert Settings -** Select the alert that should be generated. The alert types listed here are defined in the 'Alerts' section. See '**Manage Alerts**' for more details.
- **Auto Remediation on alert -** Choose how you want to respond to the alert:
  - **Taken no action -** No automatic response is made to the alert. You can, of course, manually run a procedure in response to the alert.
  - **Run below procedure -** Select a procedure to run on affected endpoints in response to the alert. The procedures listed here are defined in the **Procedures** interface. Type the first few characters of the procedure and select from the list.
- Click 'Save'.
- Click the 'Conditions' tab followed by 'Edit' to define monitor thresholds
- Click 'Add Condition'



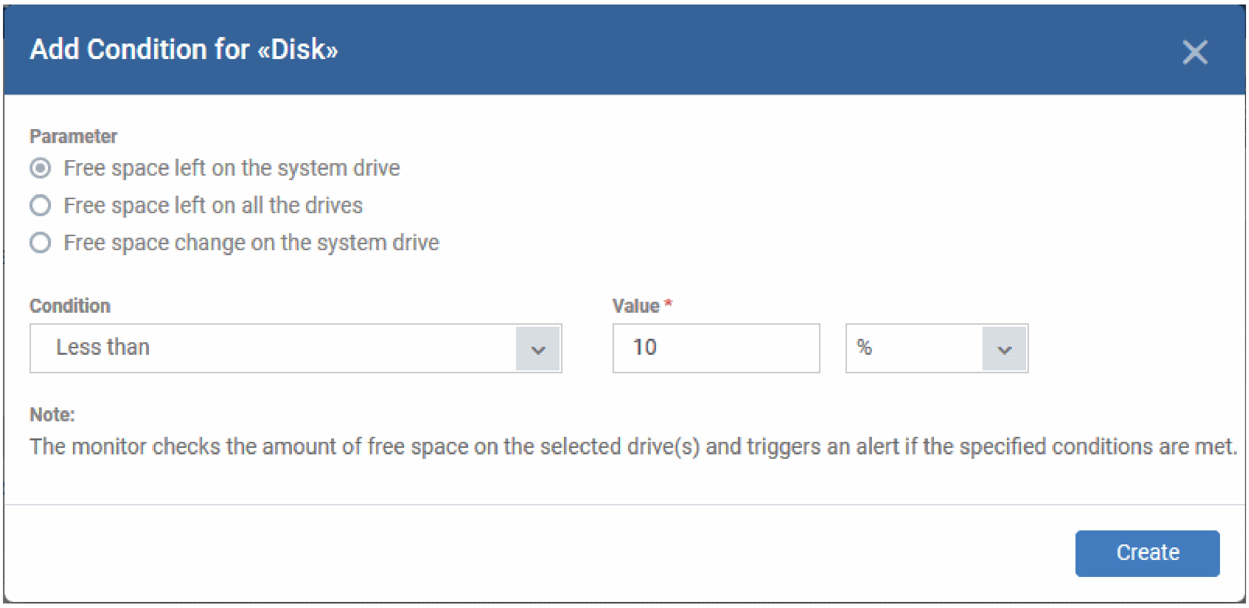
- Choose the parameter you want to monitor:

| Available Monitors | |
|---|---|
| Performance | Checks CPU, RAM and network usage and triggers an alert if certain conditions are met. |
| File Size | Checks the disk space used by a specific file. Triggers an alert if the file size is less or more than a specific size. |
| Folder Size | Checks the disk space used by a directory. Triggers an alert if the folder size is less or more than a specific size. |
| Disk | Checks free disk space, or for large changes to free disk space in short periods. Trigger an alert if disk space falls below a certain level, or if there are large alterations to disk space in a short time period. |
| Service | Checks whether or not a named service is running. Triggers an alert if the condition is met. |
| Process | Checks whether or not a named process is running. Triggers an alert if the condition is met. |
| Event | Checks if a specific event occurs and alerts you accordingly. The condition monitors |

| | |
|---|---|
| | Windows event logs. You must specify the event ID, the criticality of the event, and the source of the event. |
| TCP | Checks whether a specific port is open or closed and alerts you accordingly. This is useful for important ports that need to remain open/closed for operational reasons.<br>You need to specify the host name/ IP of the target port, the port number, the polling interval (in seconds), and whether you want to test for an open or closed state. |
| Ping | Checks whether a host is online or not. You need to specifiy the host name, the polling interval (in seconds), and whether you want to test for an online or offline status. |
| Web Page | Checks whether specific content is present or not present on a webpage. You need to specify the URL, the content you want to search for, the polling interval (in minutes), and the present/not present status. You are alerted if the condition is met. |
| Device Status | Checks every managed device to see whether it has been online or offline for a certain length of time. You will receive an alert if the device has been offline/online for the length of time you specify.<br>Background. Every minute, managed devices send a message to Endpoint Manager to signal they are online. If EM does not receive this signal for three minutes straight then the device status is set to 'Offline'. This condition will alert you if a device has been continuously 'Offline' (or 'Online') for the total length of time you specify. |
| Custom Script | Create a python script to monitor for your own set of conditions. Paste your script in the space provided. See **Add Custom Monitoring Conditions** if you need help with this. |
| Security Events | Checks for significant security related events on the managed endpoint. Example events monitored are:<br>• Malware detected and handled<br>• Malware detected and not handled<br>• Unknown application is placed in the container<br>• An external device was blocked by device control<br>You can receive an alert when the condition is met, or automatically run a procedure. |
| Security Client Events | Alerts you when there are errors with Comodo Client Security (CCS).<br>CCS is the endpoint application which provides the antivirus, firewall and containment services. This monitor checks for any failure in those processes, including:<br>• Antivirus scan failed or interrupted<br>• Antivirus database update failed<br>• Antivirus scan interrupted<br>• Another antivirus is installed<br>You can receive an alert when the condition is met, or automatically run a procedure. |
| OS Patches Event | Alerts you on events when various types of Windows patches are installed. You can monitor the installation of:<br>• Critical Updates<br>• Definition Updates<br>• Upgrades<br>• Feature Packs<br>• Update Rollups |

|  |  |
|---|---|
|  | • Service Packs<br>• Tools<br>• Updates<br>• Security updates |

- Define the specifics of the condition. The type of information you need to provide depends on the condition. For example, if you select 'Disk' monitor, you have the option to specify conditions for three values. See the example image below.



Add Condition for «Disk»

Parameter

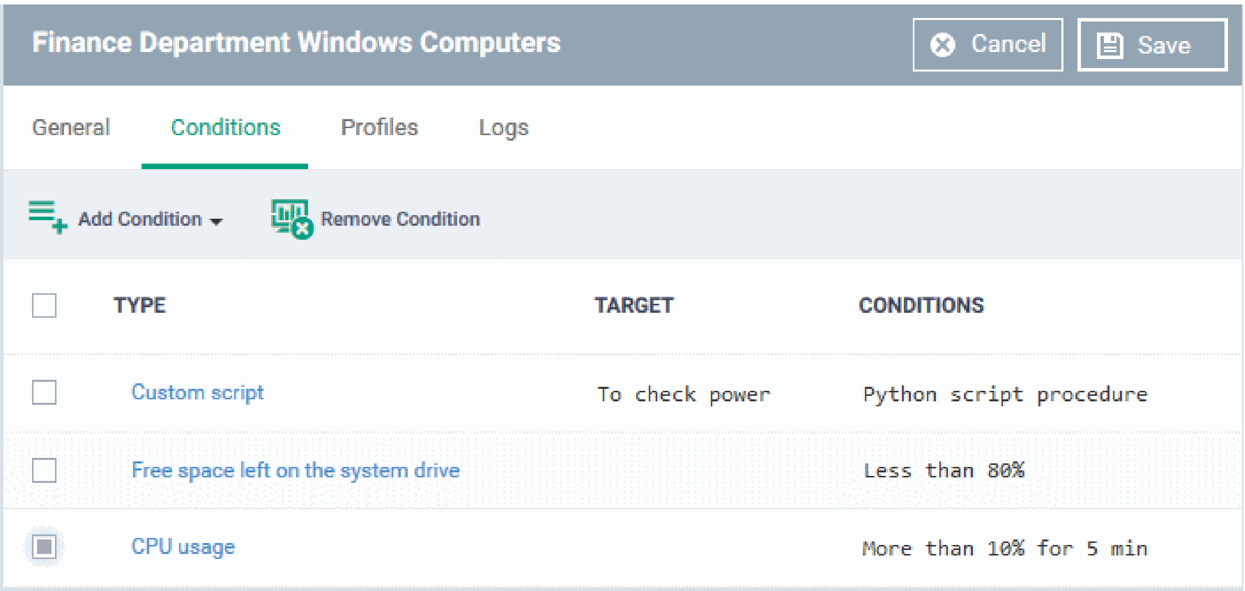
● Free space left on the system drive
○ Free space left on all the drives
○ Free space change on the system drive

Condition: Less than

Value *: 10 %

Note:
The monitor checks the amount of free space on the selected drive(s) and triggers an alert if the specified conditions are met.

- Repeat the process to add more parameters and monitoring conditions.



Finance Department Windows Computers

| □ | TYPE | TARGET | CONDITIONS |
|---|---|---|---|
| □ | Custom script | To check power | Python script procedure |
| □ | Free space left on the system drive |  | Less than 80% |
| ☑ | CPU usage |  | More than 10% for 5 min |

- To remove a monitoring condition, select the check box beside it and click 'Remove Condition' at the top.
- Click 'Save' to apply your changes.

## Add Custom Monitoring Conditions

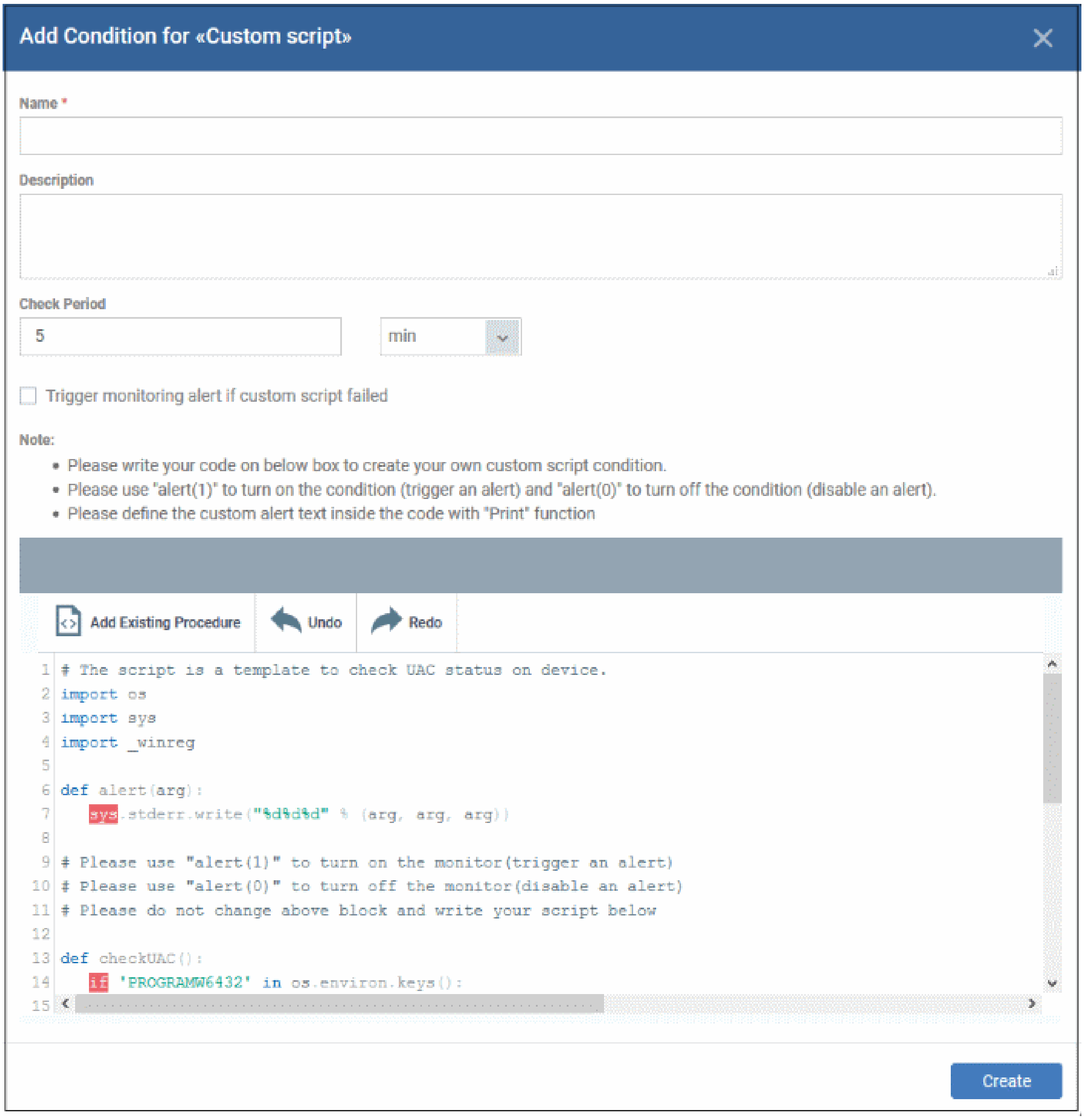
- Endpoint Manager allows you to create custom monitoring conditions per your business requirements.

- You can create custom scripts in python and can define which items should be monitored. You can also define the threshold before an alert is generated.
- You can use custom script with parameters when creating a monitor
- Predefined script monitors are available in 'Configuration Templates' > 'Procedures' > 'Predefined Procedures' > 'Monitors'. These are available for selection in the 'Add Existing Procedure' >'Procedure name' drop-down.

### Add a custom script to the monitoring conditions

- Choose 'Custom script' from the 'Add Condition' drop-down

The 'Add Condition for Custom Script' form will appear.



Name *

Description

Check Period

5 min

□ Trigger monitoring alert if custom script failed

Note:

- Please write your code on below box to create your own custom script condition.
- Please use "alert(1)" to turn on the condition (trigger an alert) and "alert(0)" to turn off the condition (disable an alert).
- Please define the custom alert text inside the code with "Print" function

```
# The script is a template to check UAC status on device.
import os
import sys
import _winreg

def alert(arg):
    sys.stderr.write("%d%d%d" % (arg, arg, arg))

# Please use "alert(1)" to turn on the monitor(trigger an alert)
# Please use "alert(0)" to turn off the monitor(disable an alert)
# Please do not change above block and write your script below

def checkUAC():
    if 'PROGRAMW6432' in os.environ.keys():
```

| Add Condition for Custom Script - Table of Parameters | |
|---|---|
| **Form Element** | **Description** |
| Name | Enter a label for the script, shortly describing its purpose. |

| Add Condition for Custom Script - Table of Parameters | |
|---|---|
| | |
| Description | Enter a short description for the script. |
| Check Period | Enter the time interval at which the script should be run on the endpoints to which the profile is applied.<br>**Tip**: Ensure that the check period is greater than the time taken for the script to run and complete, so that successive executions of the script do not overlap. |
| Trigger monitoring alert if custom script failed | Select this if you want to generate a warning notice if the custom script did not run successfully. |
| Script | Enter your Python script in the text editor.<br>**Note 1**: Keep the following lines intact in the editor and enter your script below these:<br>`import os`<br>`import sys`<br>`import _winreg`<br>`def alert(arg):`<br>`    sys.stderr.write("%d%d%d" % (arg, arg, arg))`<br>`# Please use "alert(1)" to turn on the monitor(trigger an alert)`<br>`# Please use "alert(0)" to turn off the monitor(disable an alert)`<br>`# Please do not change above block and write your script below`<br>**Note 2**: If you want an alert to be triggered if the condition is met set the argument to alert parameter to 1, i.e. 'alert(1)'.<br>If you do not want an alert to be triggered even if the condition is met set the argument to alert parameter to 0, i.e. 'alert(0)'.<br>**Note 3**: You can import an existing script procedure in EM if you wish to create a new custom monitor script using an existing procedure as a starting point. To do so, click 'Add Existing Procedure' and choose the existing procedure. Edit the script as per your requirement as per Note 1. For more details on procedures, See **Manage Procedures**.<br>**Note 4**: In addition to the above, Python script monitors by the Comodo development team are available in the 'Monitors' folder under 'Configuration Templates' > 'Procedures' > 'Predefined Procedures'. You can add these predefined scripts by clicking 'Add Existing Procedure' and select from the 'Procedure name' drop-down and can be used directly without any changes. Feel free to try any script that fits your needs. If you require custom scripts from Comodo, please raise a request at **https://c1forum.comodo.com/forum/script-library/4460-script-requests-comodo-will-write-the-scripts-for-you-for-free**<br>**Note 5:** You can add parameters to your custom scripts. **Click here** to know how. |

- Complete the form and click 'Create'

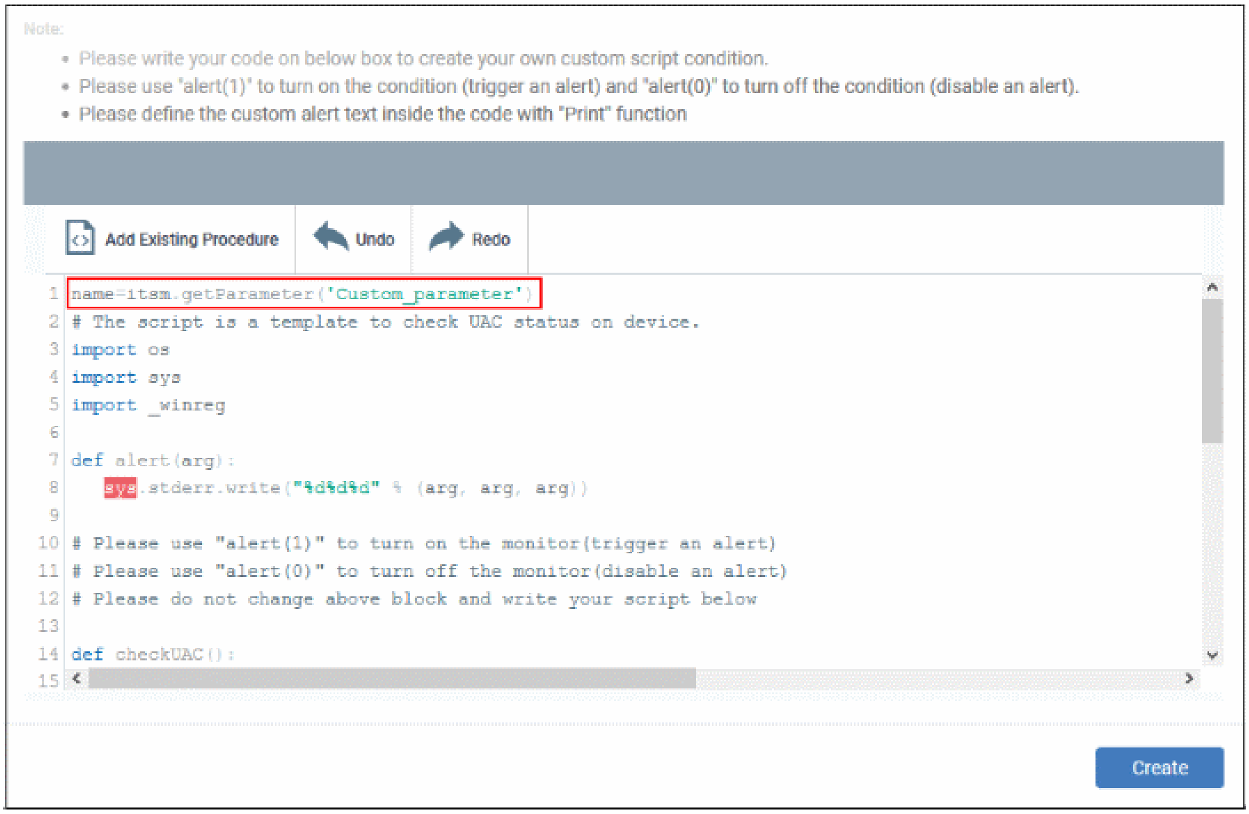
The custom monitor will be added to the list of monitors under the 'Monitors' tab.

### Add parameters to custom scripts

You can add parameter types such as integer, list, unicode and float to your custom script in the monitor condition form.

- Click 'Configuration Templates' > 'Monitors'
- Click 'Create Monitors'
- Complete the form as explained above.
- Click 'Add Condition' and select 'Custom script'
  - See '**Add Custom Monitoring Conditions**' explained above.
- Scroll down to the script area and enter the following code:

name=itsm.getParameter('parameterName')



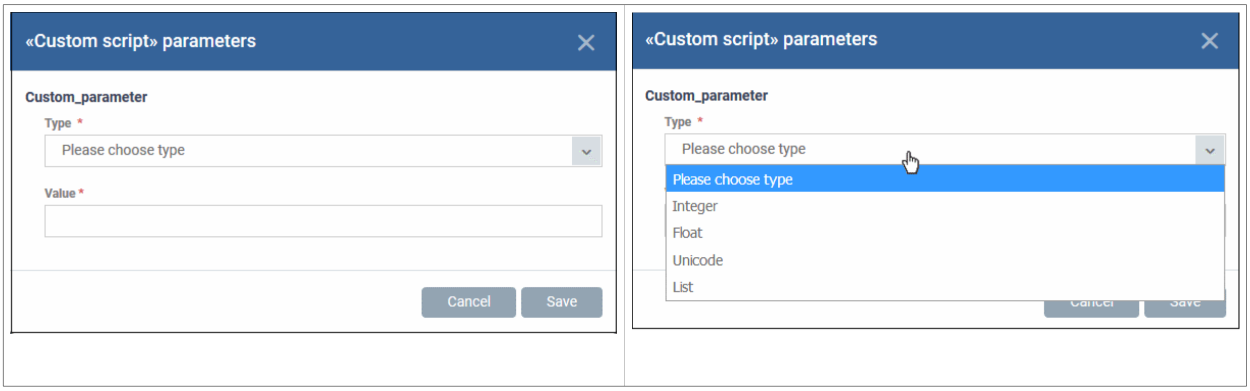
Note:

- Please write your code on below box to create your own custom script condition.
- Please use "alert(1)" to turn on the condition (trigger an alert) and "alert(0)" to turn off the condition (disable an alert).
- Please define the custom alert text inside the code with "Print" function

```
name=itsm.getParameter('Custom_parameter')
# The script is a template to check UAC status on device.
import os
import sys
import _winreg

def alert(arg):
    sys.stderr.write("%d%d%d" % (arg, arg, arg))

# Please use "alert(1)" to turn on the monitor(trigger an alert)
# Please use "alert(0)" to turn off the monitor(disable an alert)
# Please do not change above block and write your script below

def checkUAC():
```

- Click 'Create'

Custom script parameters dialog box appears:



«Custom script» parameters

Custom_parameter

Type * Please choose type

Value *

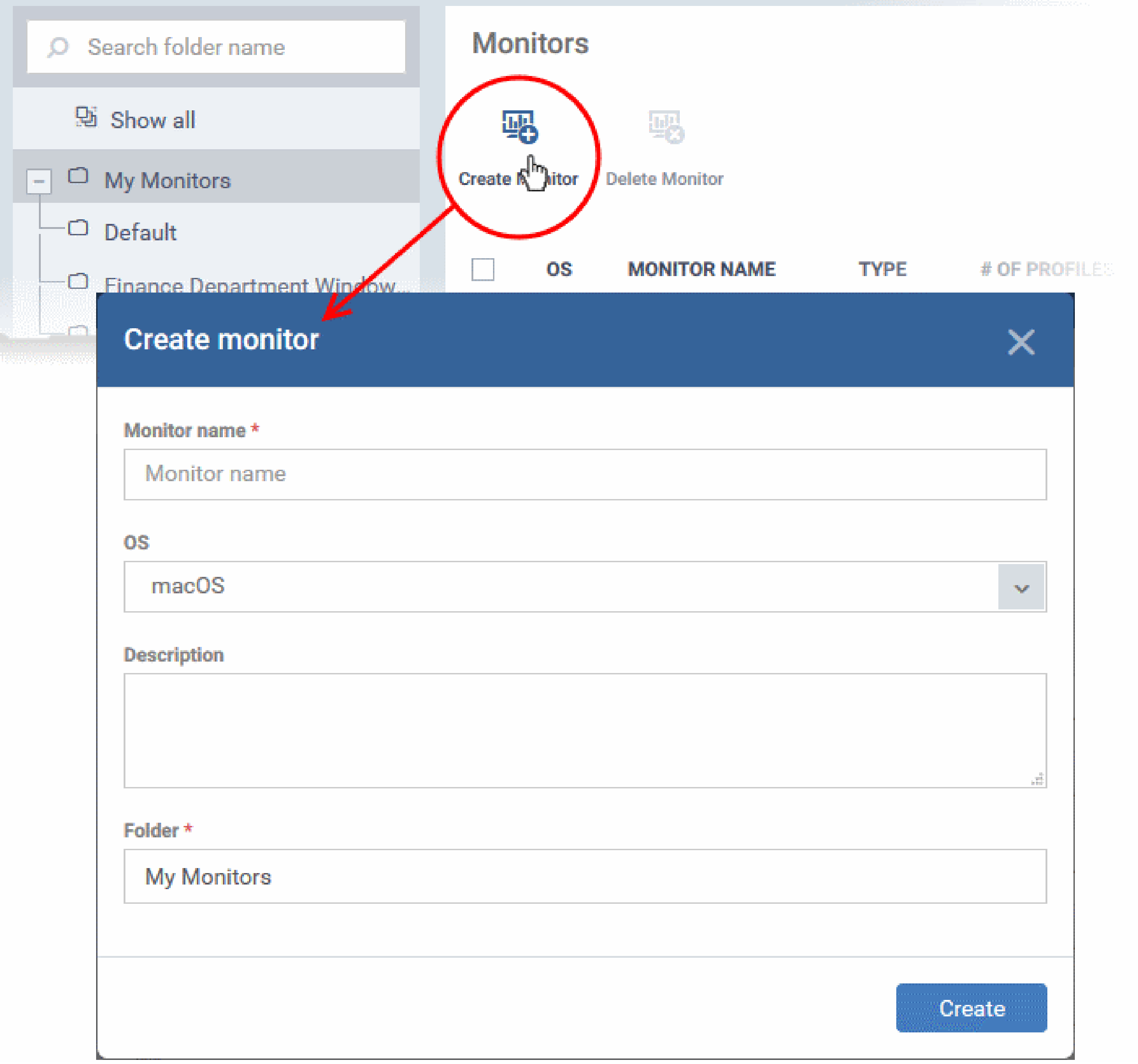
- Type - Select the parameter type from the drop-down. Available types are:
  - Integer
  - Float
  - Unicode

    - List
  - Value - Enter appropriate parameter value.
- Click 'Save'

The monitor will be available for selection under 'Add Monitor' when configuring the 'Monitors' section of a Windows profile. For more details on adding a monitor to a profile, see **Monitors** in **Create Windows Profiles**.

### 6.7.1.2. Monitors for Mac OS Devices

- Click 'Configuration Templates' > 'Monitors'
- Click 'Create Monitor'



Create monitor

Monitor name *

Monitor name

OS

macOS

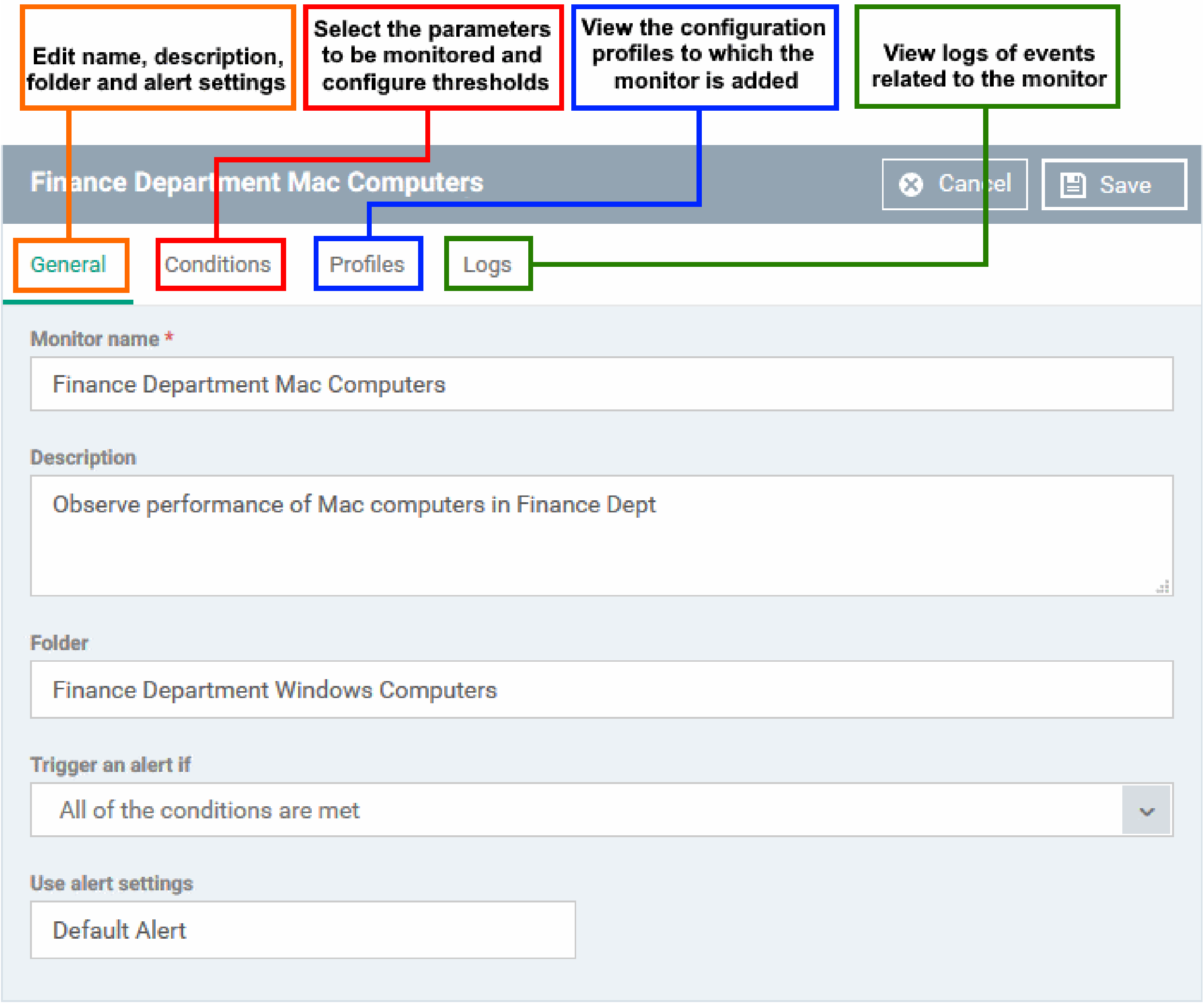
Description

Folder *

My Monitors

Create

- Enter a label and description for the monitor
- Select 'macOS' in the OS drop-down
- Specify where to save the new monitor. You can create new sub-folders under 'My Monitors' if required.
- Click 'Create'.
- You will be taken to the monitor configuration screen:


Edit name, description, folder and alert settings
Select the parameters to be monitored and configure thresholds
View the configuration profiles to which the monitor is added
View logs of events related to the monitor
Finance Department Mac Computers
Cancel
Save
General
Conditions
Profiles
Logs

Monitor name *
Finance Department Mac Computers

Description
Observe performance of Mac computers in Finance Dept

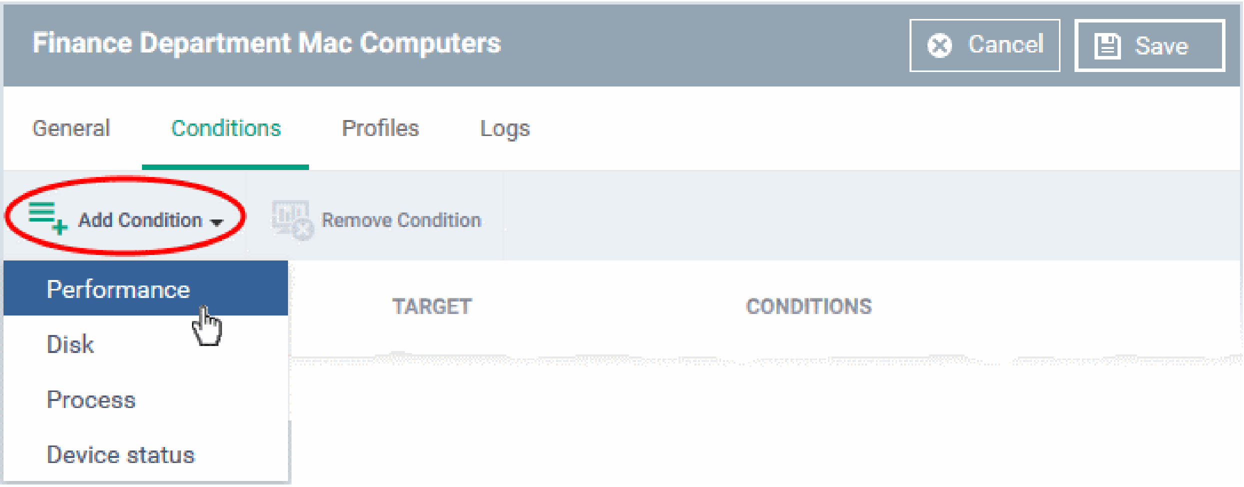
Folder
Finance Department Windows Computers

Trigger an alert if
All of the conditions are met

Use alert settings
Default Alert

Modify the following settings if required:

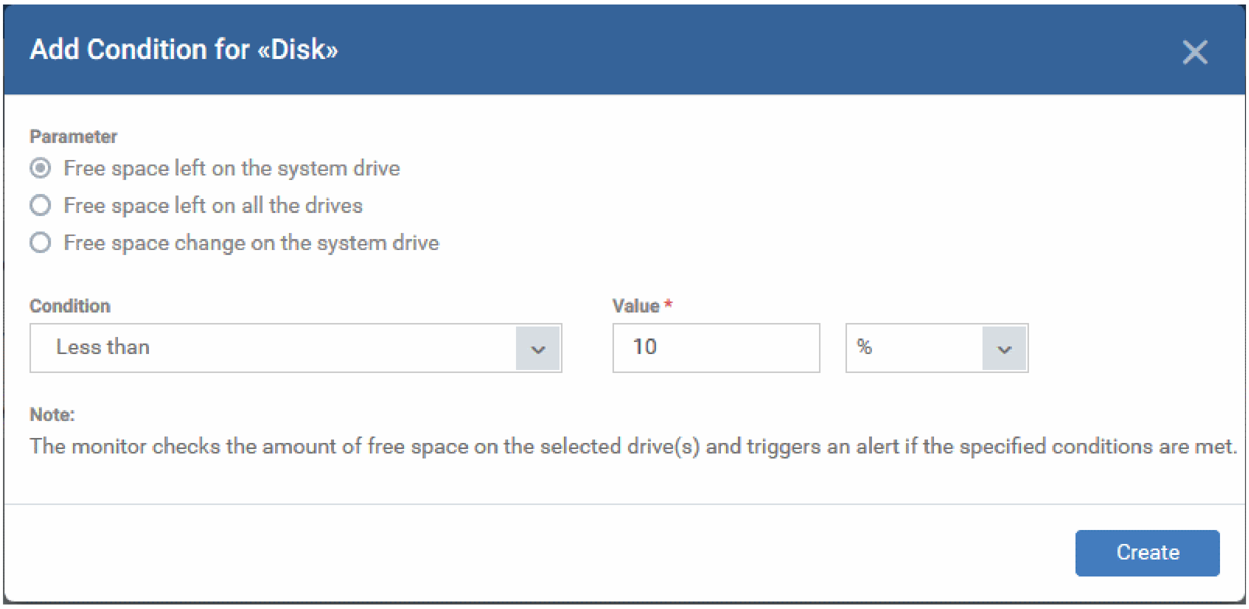
- **Trigger an alert if -** Select when the alert should be sent to admins. The options are send alert when all conditions are met or when any condition is met.
- **Use Alert Settings -** Select the alert that should be generated. The alert types listed here are defined in the 'Alerts' section. See '**Manage Alerts**' for more details.
- Click 'Save'
  - Click the 'Conditions' tab followed by 'Edit' to define monitor thresholds
  - Click 'Add Condition'



- Choose the parameter you want to monitor

| Available Monitors | |
|---|---|
| Performance | Checks CPU, RAM and network usage and triggers an alert if certain conditions are met.<br>You can specify thresholds for these parameters and the length of time the threshold can be continuously exceeded, before triggering an alert. |
| Disk | Checks free disk space, or for large changes to free disk space in short periods.<br>• Triggers an alert if disk space falls below a certain level, or if there are large alterations to disk space in a short time period. |
| Process | Checks whether or not a named process is running.<br>• Triggers an alert if the condition is met. |
| Device Status | Checks every managed device to see whether it has been online or offline for a certain length of time. You will receive an alert if the device has been offline/online for the length of time you specify.<br>Background. Every minute, managed devices send a message to Endpoint Manager to signal they are online. If EM does not receive this signal for three minutes straight then the device status is set to 'Offline'. This condition will alert you if a device has been continuously 'Offline' (or 'Online') for the total length of time you specify. |

- Define the specifics of the condition. The type of information you need to provide depends on the condition. For example, if you select 'Disk' monitor, you have the option to specify conditions for three values. See the example image below.



Add Condition for «Disk»

Parameter

● Free space left on the system drive

○ Free space left on all the drives

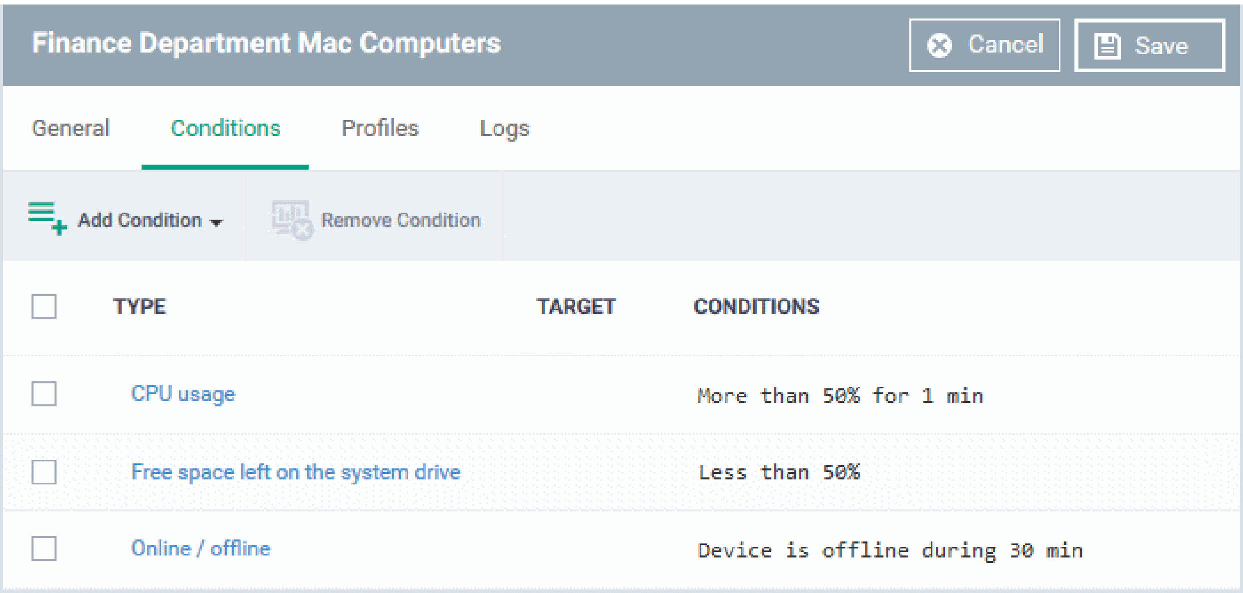
○ Free space change on the system drive

Condition: Less than

Value *: 10 %

Note:
The monitor checks the amount of free space on the selected drive(s) and triggers an alert if the specified conditions are met.

- Click 'Create' after specifying the conditions.
- Repeat the process to add more conditions



| □ | TYPE | TARGET | CONDITIONS |
|---|---|---|---|
| □ | CPU usage | | More than 50% for 1 min |
| □ | Free space left on the system drive | | Less than 50% |
| □ | Online / offline | | Device is offline during 30 min |

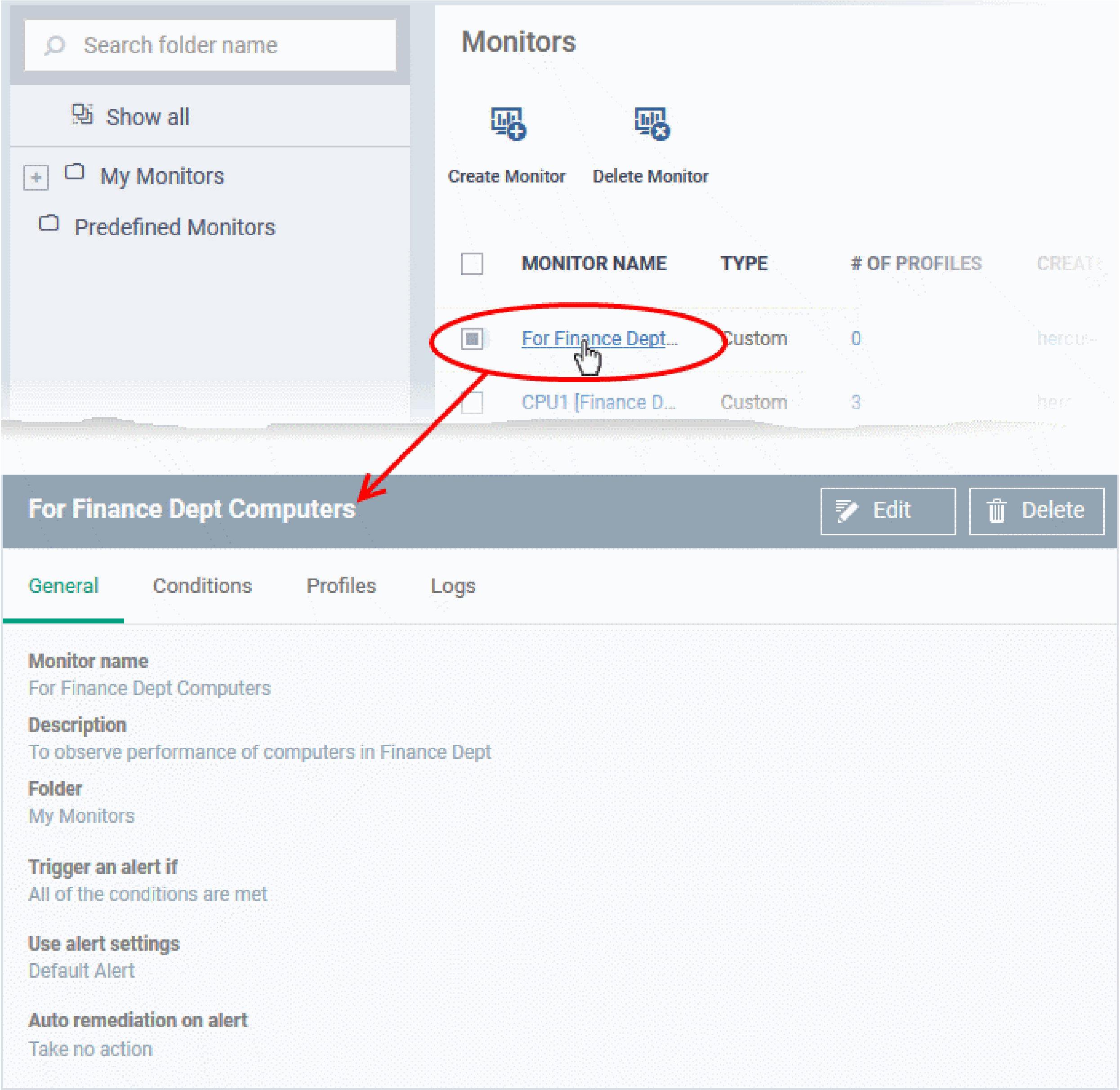
- To remove a monitoring condition, select the check box beside it and click 'Remove Condition' at the top.
- Click 'Save' to apply your changes.

## 6.7.2. View and Edit Monitors

- You can view the details of predefined and custom monitors, but you can only edit custom monitors.
- You can also view profiles in which a monitor is active, and events generated by the monitor.

**View details of a monitor**

- Click 'Configuration Templates' > 'Monitors'
- Click the name of a monitor to open its configuration interface



For Finance Dept Computers

Monitor name
For Finance Dept Computers

Description
To observe performance of computers in Finance Dept

Folder
My Monitors

Trigger an alert if
All of the conditions are met

Use alert settings
Default Alert

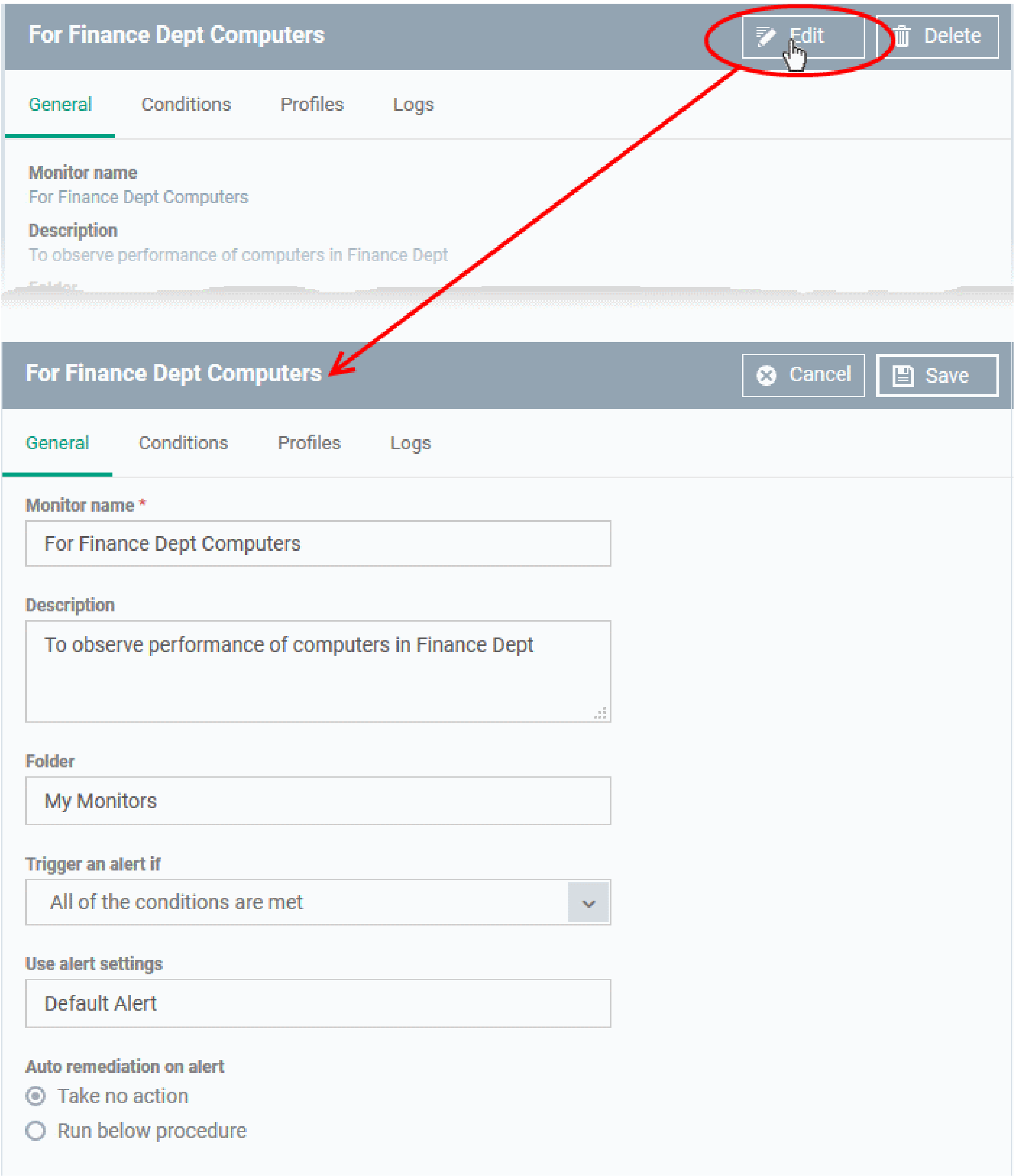
Auto remediation on alert
Take no action

The configuration interface allows you to:

- **Edit general settings and monitoring conditions**
- **View all profiles which use a particular monitor**
- **View the log of events related to the monitor. from all devices on which profiles with the monitor is applied**

## Edit a Monitor

- Click 'Configuration Templates' > 'Monitors'
- Click on the name of a monitor. The monitor configuration interface will open at the 'General' tab.
- Click the 'Edit' button to modify the details.



Monitor name
For Finance Dept Computers

Description
To observe performance of computers in Finance Dept

Monitor name *
For Finance Dept Computers

Description
To observe performance of computers in Finance Dept

Folder
My Monitors

Trigger an alert if
All of the conditions are met

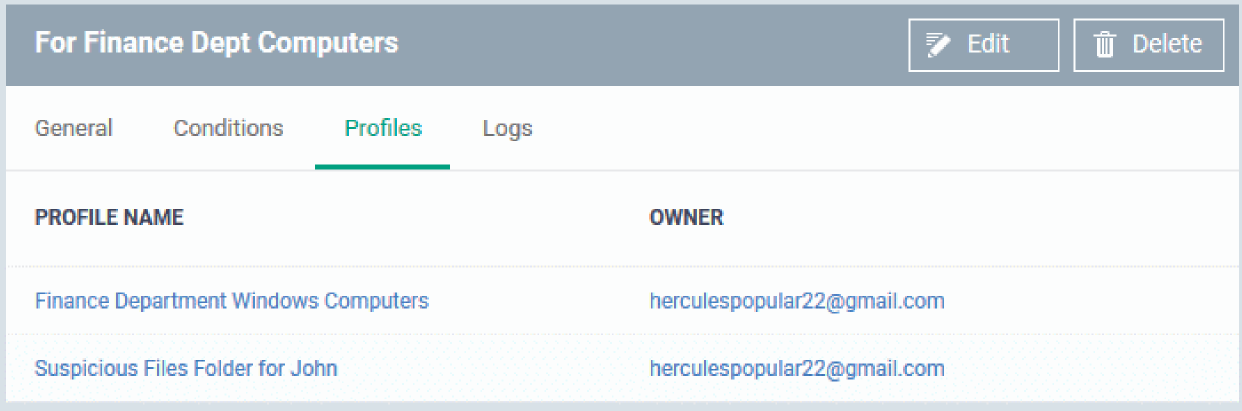
Use alert settings
Default Alert

Auto remediation on alert
● Take no action
○ Run below procedure

- **General** - Modify the name, description, location, alert settings and more
- **Conditions** - Modify the items which are tracked by the monitor
  - Editing the conditions is similar to adding conditions to a monitor. See **Monitors for Windows Devices** / **Monitors for Mac OS Devices** for more details.
- Click 'Save' for your changes to take effect.
- The changes are immediately implemented in all profiles which use the monitor.

### View all profiles which use a particular monitor

- Click 'Configuration Templates' > 'Monitors'
- Click the name of a monitor to open its configuration interface.
- Click the 'Profiles' tab.



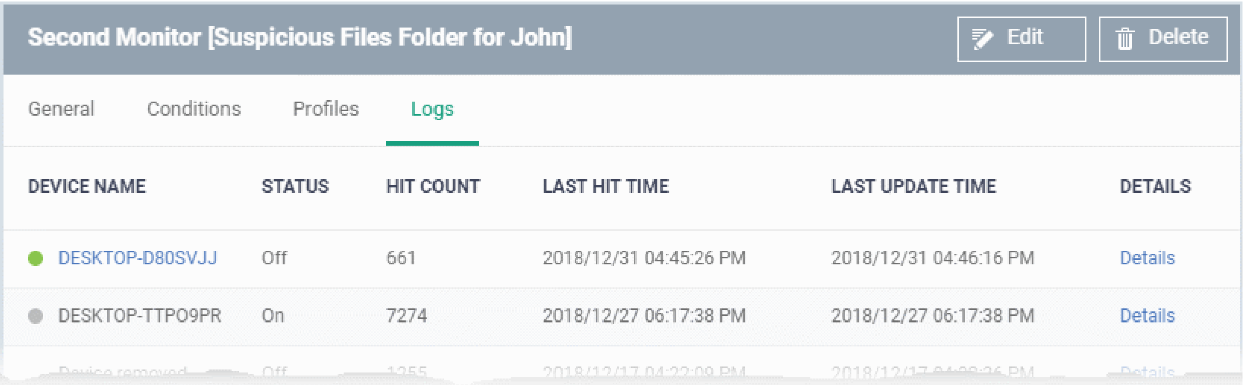
| PROFILE NAME | OWNER |
|---|---|
| Finance Department Windows Computers | herculespopular22@gmail.com |
| Suspicious Files Folder for John | herculespopular22@gmail.com |

| Monitors - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Profile Name | The profile in which the monitor is active.<br>• Click the profile name to open its configuration screen. See **Edit Configuration Profiles** for more details. |
| Owner | The administrator who created the profile.<br>• Click the name to view their user details. See **View the details of the User** for more details. |

## View Monitor Logs

- Click 'Configuration Templates' > 'Monitors'
- Click the name of a monitor to open its configuration interface.
- Click the 'Logs' tab.

The 'Logs' tab shows all instances where the conditions of the monitor were breached:



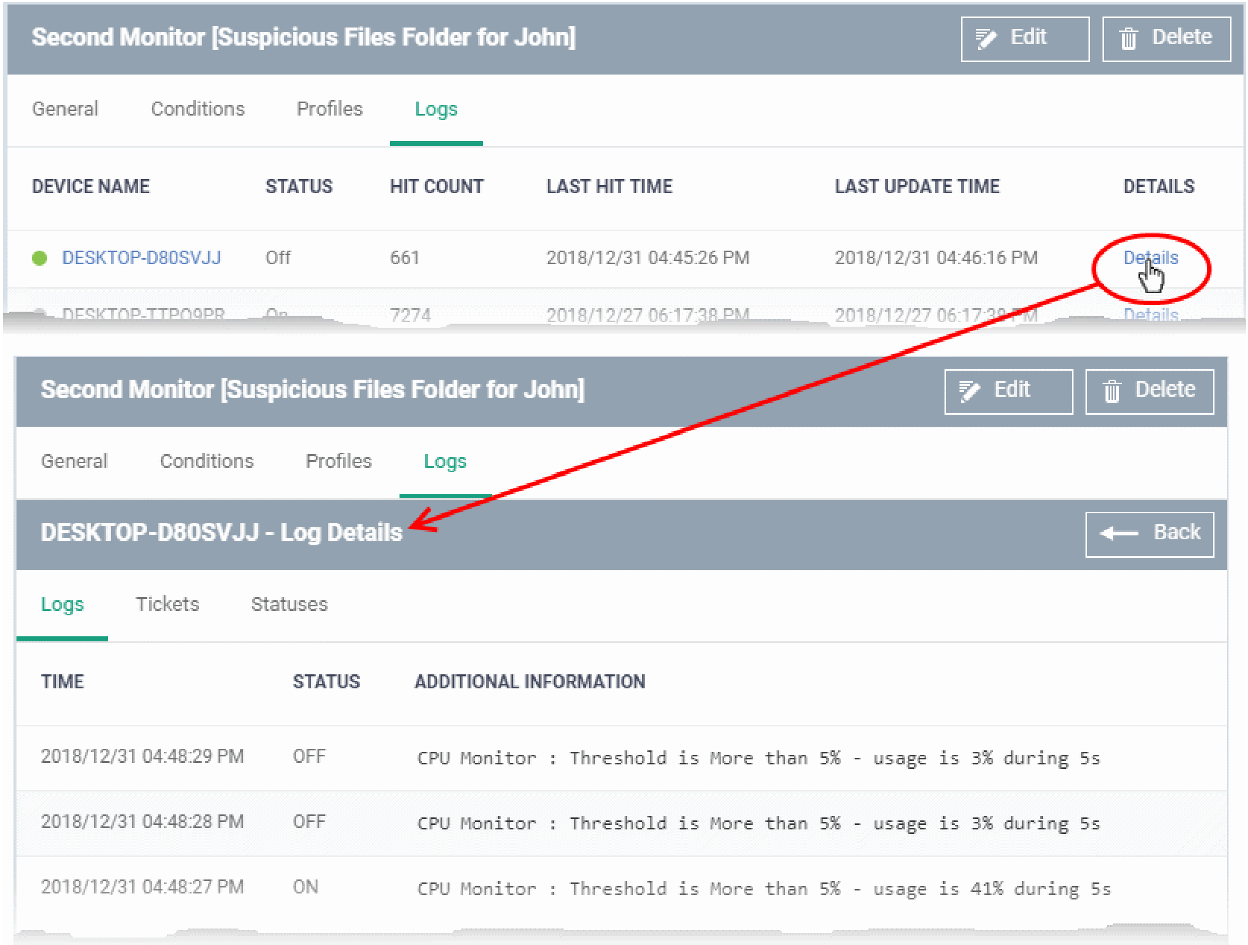
| DEVICE NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| ● DESKTOP-D80SVJJ | Off | 661 | 2018/12/31 04:45:26 PM | 2018/12/31 04:46:16 PM | Details |
| ● DESKTOP-TTPO9PR | On | 7274 | 2018/12/27 06:17:38 PM | 2018/12/27 06:17:38 PM | Details |
| Device removed | Off | 1255 | 2018/12/17 04:22:09 PM | 2018/12/17 04:[illegible]:36 PM | Details |

| Monitoring Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Device Name | The Windows or Mac OS device on which the violation occurred.<br>• Click the name of the device to open its details interface. |

| | |
|---|---|
| | • See **Manage Windows Devices** / **Manage Mac OS Devices** for more details. |
| Status | Whether or not the monitor is currently active on the device. |
| Hit Count | Number of times the monitored conditions were breached in the last 24 hours. |
| Last Hit Time | Date and time the monitoring rule was last broken. |
| Last Update Time | Date and time when the information was last refreshed. |
| Details | • Click the 'Details' link to view a log of the breach events.<br>• See **View Details of Monitor Logs** (given below) for more information. |

## View Details of Monitor Logs

- Click the 'Details' link to view the details of the violations of the monitoring conditions:



Second Monitor [Suspicious Files Folder for John]

| DEVICE NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| DESKTOP-D80SVJJ | Off | 661 | 2018/12/31 04:45:26 PM | 2018/12/31 04:46:16 PM | Details |
| DESKTOP-TTPO9PR | On | 7274 | 2018/12/27 06:17:38 PM | 2018/12/27 06:17:39 PM | Details |

Second Monitor [Suspicious Files Folder for John]

DESKTOP-D80SVJJ - Log Details

| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2018/12/31 04:48:29 PM | OFF | CPU Monitor : Threshold is More than 5% - usage is 3% during 5s |
| 2018/12/31 04:48:28 PM | OFF | CPU Monitor : Threshold is More than 5% - usage is 3% during 5s |
| 2018/12/31 04:48:27 PM | ON | CPU Monitor : Threshold is More than 5% - usage is 41% during 5s |

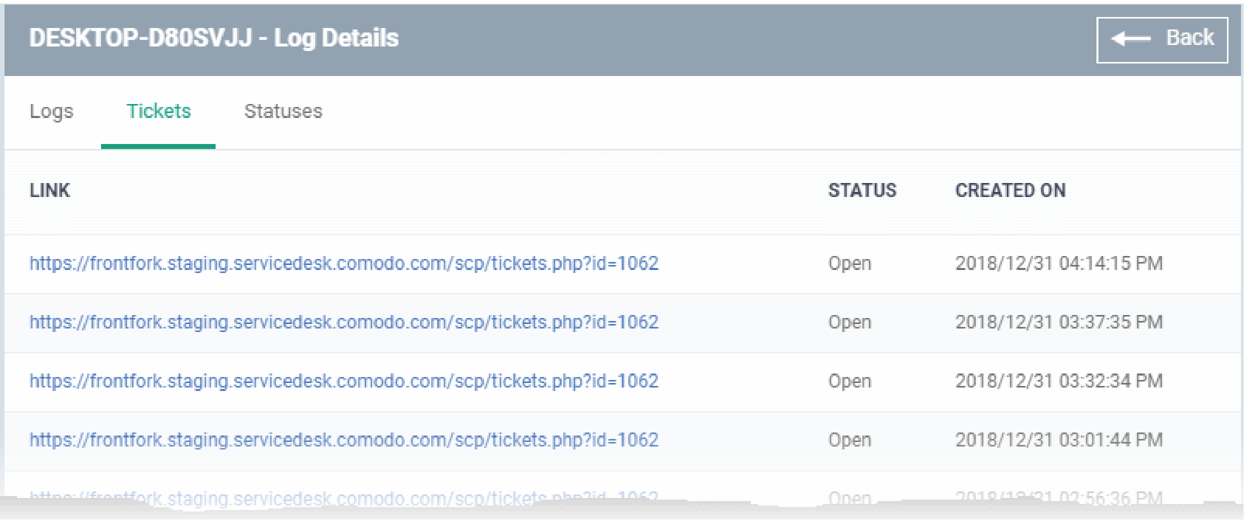
Details are shown under three tabs:

**Logs** - The date and time when the event occurred. Also shows the details of the monitoring rule that detected the event.

| Monitoring Log Details - 'Logs' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time of the event. |

| | |
|---|---|
| Status | The current state of the monitor on the device:<br>• On - The device is exceeding the thresholds of the monitor<br>• Off - The device is operating within the thresholds of the monitor |
| Additional Information | Details on the condition monitored and the breach |

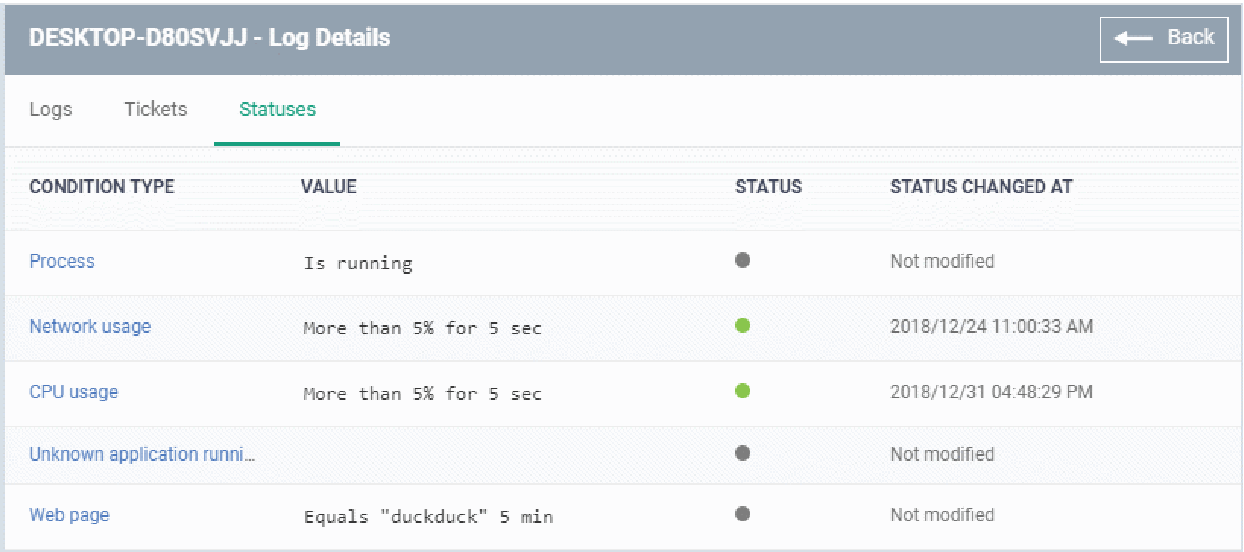
**Tickets** - Shows any service desk tickets which were automatically generated by the alert.


DESKTOP-D80SVJJ - Log Details

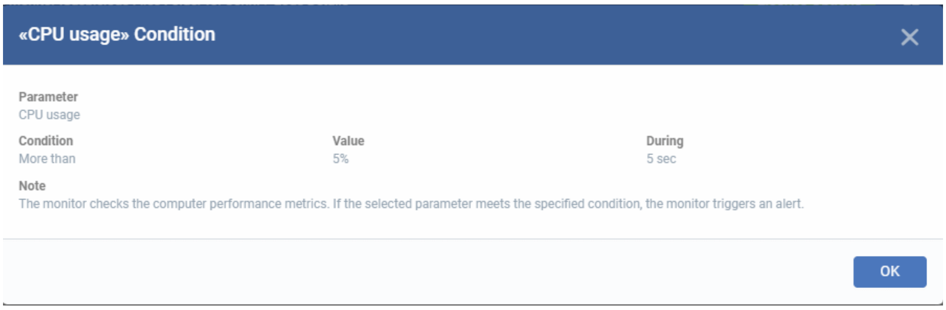
| LINK | STATUS | CREATED ON |
|---|---|---|
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2018/12/31 04:14:15 PM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2018/12/31 03:37:35 PM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2018/12/31 03:32:34 PM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2018/12/31 03:01:44 PM |
| https://frontfork.staging.servicedesk.comodo.com/scp/tickets.php?id=1062 | Open | 2018/12/31 02:56:36 PM |

| Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was created. |

**Statuses** - Shows the current status of each condition in the monitor:

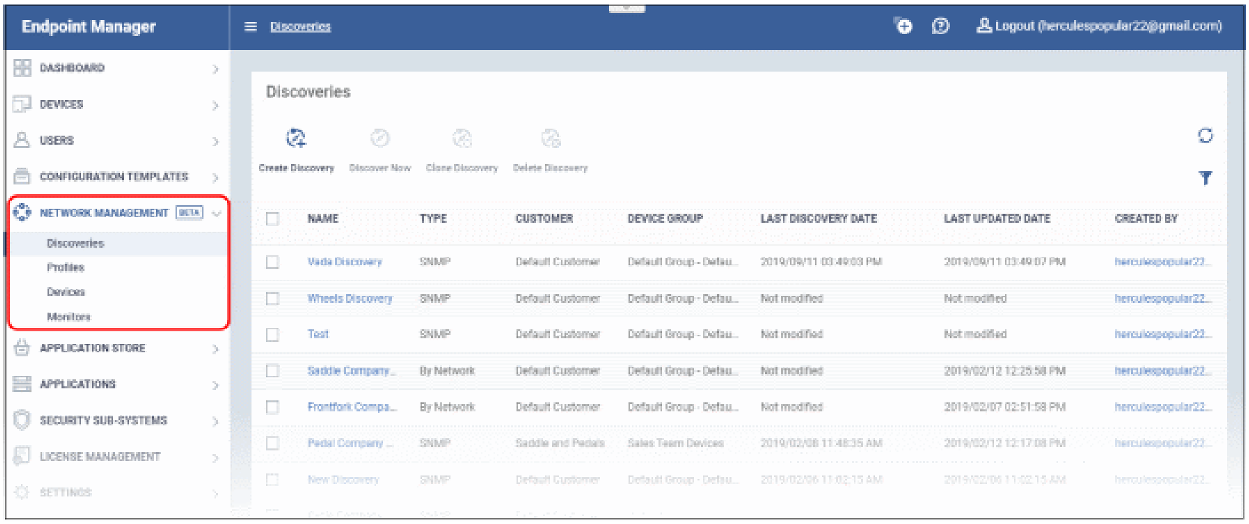

DESKTOP-D80SVJJ - Log Details

| CONDITION TYPE | VALUE | STATUS | STATUS CHANGED AT |
|---|---|---|---|
| Process | Is running | ● | Not modified |
| Network usage | More than 5% for 5 sec | 🟢 | 2018/12/24 11:00:33 AM |
| CPU usage | More than 5% for 5 sec | 🟢 | 2018/12/31 04:48:29 PM |
| Unknown application runni... | | ● | Not modified |
| Web page | Equals "duckduck" 5 min | ● | Not modified |

| Monitoring Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Condition Type | The category of monitor.<br>Click the type to view its exact conditions and thresholds. An example is shown below:<br><br>«CPU usage» Condition<br>Parameter: CPU usage<br>Condition: More than<br>Value: 5%<br>During: 5 sec<br>Note: The monitor checks the computer performance metrics. If the selected parameter meets the specified condition, the monitor triggers an alert.<br> |
| Value | The thresholds set for the parameter. |
| Status | The current state of the monitored parameter on the device.<br>• Green - The device is operating within the thresholds of the monitor<br>• Grey - Unknown<br>• Red - The device is exceeding the conditions of the monitor. |
| Status Changed at | The date and time of the last change in state of the monitored parameter. |

# 7.Network Management

- Click 'Network Management' > 'Discoveries' to open this interface.
- The discovery feature lets you scan networks and active directory (AD) servers to identify all devices on the network.
- The scan will identify both managed and unmanaged devices. You can configure EM to alert you if a scan finds new devices.
- You can run simple network scans from a 'probe device' situated in the target network. The probe device must be a managed Windows endpoint which has already been added to Endpoint Manager.
- You can scan Active Directory servers either with or without the use of a probe device.
- All discovered devices are shown in 'Network Management' > 'Devices' > 'Discovered Devices':



| | NAME | TYPE | CUSTOMER | DEVICE GROUP | LAST DISCOVERY DATE | LAST UPDATED DATE | CREATED BY |
|---|---|---|---|---|---|---|---|
| □ | Vada Discovery | SNMP | Default Customer | Default Group - Defau... | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:07 PM | herculespopular22... |
| □ | Wheels Discovery | SNMP | Default Customer | Default Group - Defau... | Not modified | Not modified | herculespopular22... |
| □ | Test | SNMP | Default Customer | Default Group - Defau... | Not modified | Not modified | herculespopular22... |
| □ | Saddle Company... | By Network | Default Customer | Default Group - Defau... | Not modified | 2019/02/12 12:25:58 PM | herculespopular22... |
| □ | Frontfork Compa... | By Network | Default Customer | Default Group - Defau... | Not modified | 2019/02/07 02:51:58 PM | herculespopular22... |
| □ | Pedal Company ... | SNMP | Saddle and Pedals | Sales Team Devices | 2019/02/08 11:48:35 AM | 2019/02/12 12:17:08 PM | herculespopular22... |
| □ | New Discovery | SNMP | Default Customer | Default Group - Defau... | 2019/02/06 11:02:15 AM | 2019/02/06 11:02:15 AM | herculespopular22... |

### Enroll discovered devices to EM

- All newly discovered devices are 'Unmanaged', so you cannot control them with Endpoint Manager yet. You need to install the communication client on the devices to enroll them.
- EM can auto-enroll discovered Windows devices. Auto-enrollment of other discovered devices is coming in later releases.
- You can also create a client install package for discovered devices, then use Comodo's auto-deployment tool to install the package. You can change the owner and group of these devices after they have been enrolled.

### Manage device over SNMP

- The SNMP (Simple Network Management Protocol) scan identifies devices such as printers, routers, switches, UPS etc.
- Click 'Manage Device over SNMP' to apply an SNMP profile to these devices. SNMP profiles are quite simple, offering to alert you if the device is powered on or off for a certain length of time.
- However, this still gives you some management of devices that do not run on a supported operating system (Windows / Android / Linux / Mac / iOS).
- You can view these devices in 'Network Management' > 'Devices' > 'Managed Devices' tab.

Please see the following sections:

- **Create and Run Network Discovery Tasks**

- Manage Profiles for Network Devices
- Manage Network Devices
- Manage Network Monitors

## 7.1. Create and Run Network Discovery Tasks

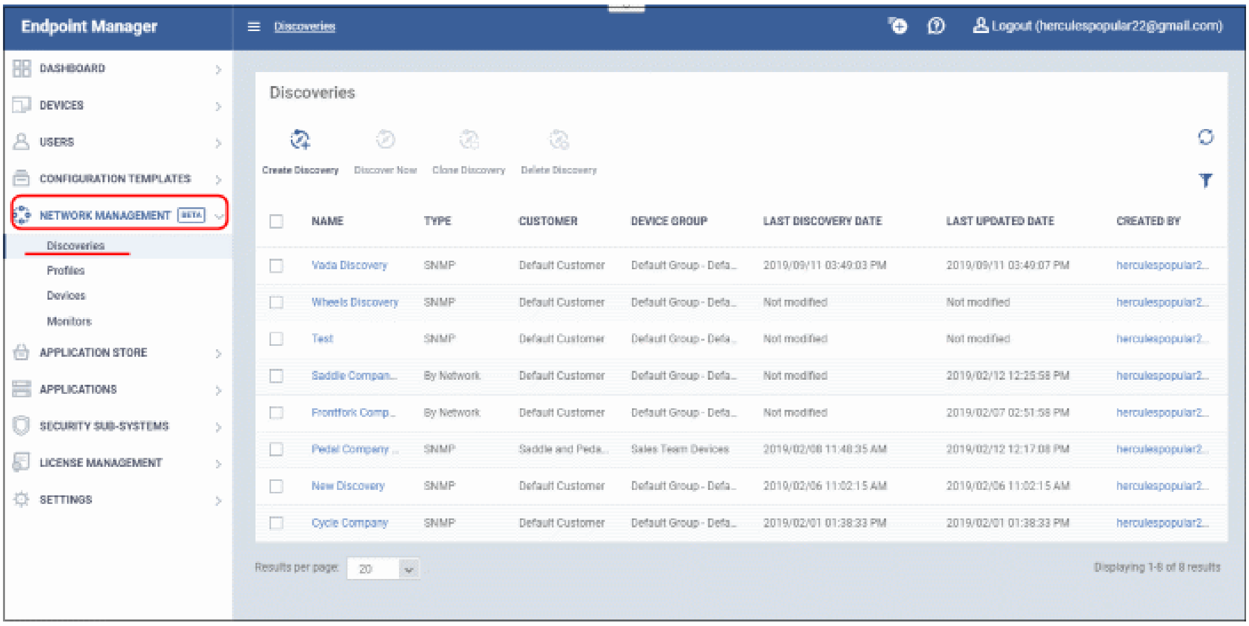
- Click 'Network Management' > 'Discoveries' in the left menu

Discovery scans consist of the IP range you want to scan, a probe device, and a destination group for discovered devices.

- The Discoveries Area
- Example Deployment Process
- Create a Discovery Task
- Run a Discovery Task
- View Discovery Logs
- Manage a Discovery Task
- Remove Discovery Tasks

### The Discoveries Area

The discoveries area lets you manage, create and run discovery scans:



Discoveries

| NAME | TYPE | CUSTOMER | DEVICE GROUP | LAST DISCOVERY DATE | LAST UPDATED DATE | CREATED BY |
|---|---|---|---|---|---|---|
| Vada Discovery | SNMP | Default Customer | Default Group - Defa... | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:07 PM | herculespopular2... |
| Wheels Discovery | SNMP | Default Customer | Default Group - Defa... | Not modified | Not modified | herculespopular2... |
| Test | SNMP | Default Customer | Default Group - Defa... | Not modified | Not modified | herculespopular2... |
| Saddle Compan... | By Network | Default Customer | Default Group - Defa... | Not modified | 2019/02/12 12:25:58 PM | herculespopular2... |
| Frontfork Comp... | By Network | Default Customer | Default Group - Defa... | Not modified | 2019/02/07 02:51:58 PM | herculespopular2... |
| Pedal Company ... | SNMP | Saddle and Peda... | Sales Team Devices | 2019/02/08 11:48:35 AM | 2019/02/12 12:17:08 PM | herculespopular2... |
| New Discovery | SNMP | Default Customer | Default Group - Defa... | 2019/02/06 11:02:15 AM | 2019/02/06 11:02:15 AM | herculespopular2... |
| Cycle Company | SNMP | Default Customer | Default Group - Defa... | 2019/02/01 01:38:33 PM | 2019/02/01 01:38:33 PM | herculespopular2... |

Results per page: 20

Displaying 1-8 of 8 results

| Column Heading | Description |
|---|---|
| Name | The label of the discovery task.<br>Ideally, the label should help you identify the target or purpose of the task in future. For example, 'Discovery Task on Company X network'.<br>Click the discovery name to open its configuration screen. See **Create a Discovery Task** for more details |
| Type | The kind of scan used to audit the network. The three possible types are:<br>• Active Directory |

| | |
|---|---|
| | • Network<br>• SNMP<br>You enable SNMP scans within the network scan type. They run simultaneously with the network scan. SNMP results are reported separately to Endpoint Manager and may find additional devices. |
| Customer | The company that owns/controls the target network. |
| Device Group | The group to which identified devices are assigned. You can specify the target device group when you configure the scan. |
| Last Discovery Date | Date and time the scan was most recently run. |
| Last Updated Date | Date and time the scan task was most recently edited. |
| Created by | The admin who created the discovery task.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| **Controls** | |
| Create Discovery | Add a new discovery task.<br>• See **Create a Discovery Task** for more details |
| Discover Now | Run an on-demand scan to identify all devices connected to the target network.<br>• See **Run a Discovery Task** for more details. |
| Clone Discovery | Create a new scan by copying an existing scan and modifying its settings as required.<br>• See **Create a Discovery Task** for more details. |
| Delete Discovery | Remove selected discovery tasks. The control will appear only if a discovery task is selected.<br>• See **Remove Discovery Tasks** for more details. |

## Example Deployment Process

- Optional - Make sure your probe device is in place. The probe is required for network and SNMP scans, but is optional for Active Directory scans.
- Create a new group for discovered devices under the company of your choice: 'Devices' > 'Device List' > 'Group Management' > 'Create Group'.
  - Name the group, for example, 'Discovered Devices - Company X'.
  - Do not add any existing devices to this group. Leave it empty. The group is purely to segment the discovered devices. You can move devices to different groups after they have been enrolled.
- Click 'Network Management' > 'Discoveries' > 'Create Discovery' > 'Discovery by Network' > create a name for the discovery task. E.g 'Discovery Task on Company X network'.
- Click 'OK' to open the task configuration screen. Click 'Edit' to actually configure the scan.
  - Specify the customer / target device group.
  - See **Network discovery scan** if you need help to configure a network/snmp scan
  - See **AD discovery scan** for help to configure an AD scan
- Save your task then select it in the 'Discoveries' screen. Click 'Discover Now' to run the scan.
- The scan will take around 10 minutes. All discovered devices will go into your new group. You can view discovered devices in 'Network Management' > 'Devices' > 'Discovered Devices'.

- Auto-enrolled Windows devices can be viewed in 'Devices' > 'Device List'
- Next, we will create a package to install the communication client on Windows devices, then use the auto-deployment tool to deploy the package.
- Click 'Devices' > 'Device List' > 'Bulk Installation Package'. Configure the package as required.
  - Remember to specify the correct company and the group you just created.
  - Do not change the filename of the .msi. It is unique to this deployment.
- Click 'Download Installer' and save the file to your local machine.
- Next, download and install the 'Auto Discovery and Deployment Tool' (ADDT). You can do this at the prompt, or download it from the Comodo Dragon / Comodo One portal (click 'Tools' in the top-menu).
- In ADDT, choose the .msi you just created as the 'Deployment Package'.
- Deployment options - Choose 'Network Addresses' then enter the same IP range as you used in your discovery scan.
- Click 'Start Deployment' to install the .msi on the target devices. This will enroll the devices to Endpoint Manager in the customer/group you created earlier.
  - See the ADDT user guide at **https://help.comodo.com/topic-289-1-851-11045-Deploy-Applications---Packages-.html** if you want help with the utility
- In Endpoint Manager, click 'Devices' 'Device List' > 'Group Management' > Company/Group to view the enrolled devices.
- You can now assign the devices to new users, or move them to new groups, as required.
- See '**Bulk Enrollment of Devices**' for more information about enrolling Windows, Mac and Linux devices.

## Create a Discovery Task

There are two ways you can create a discovery task:

- **Create new discovery task**
- **Clone an existing task and edit it as required**

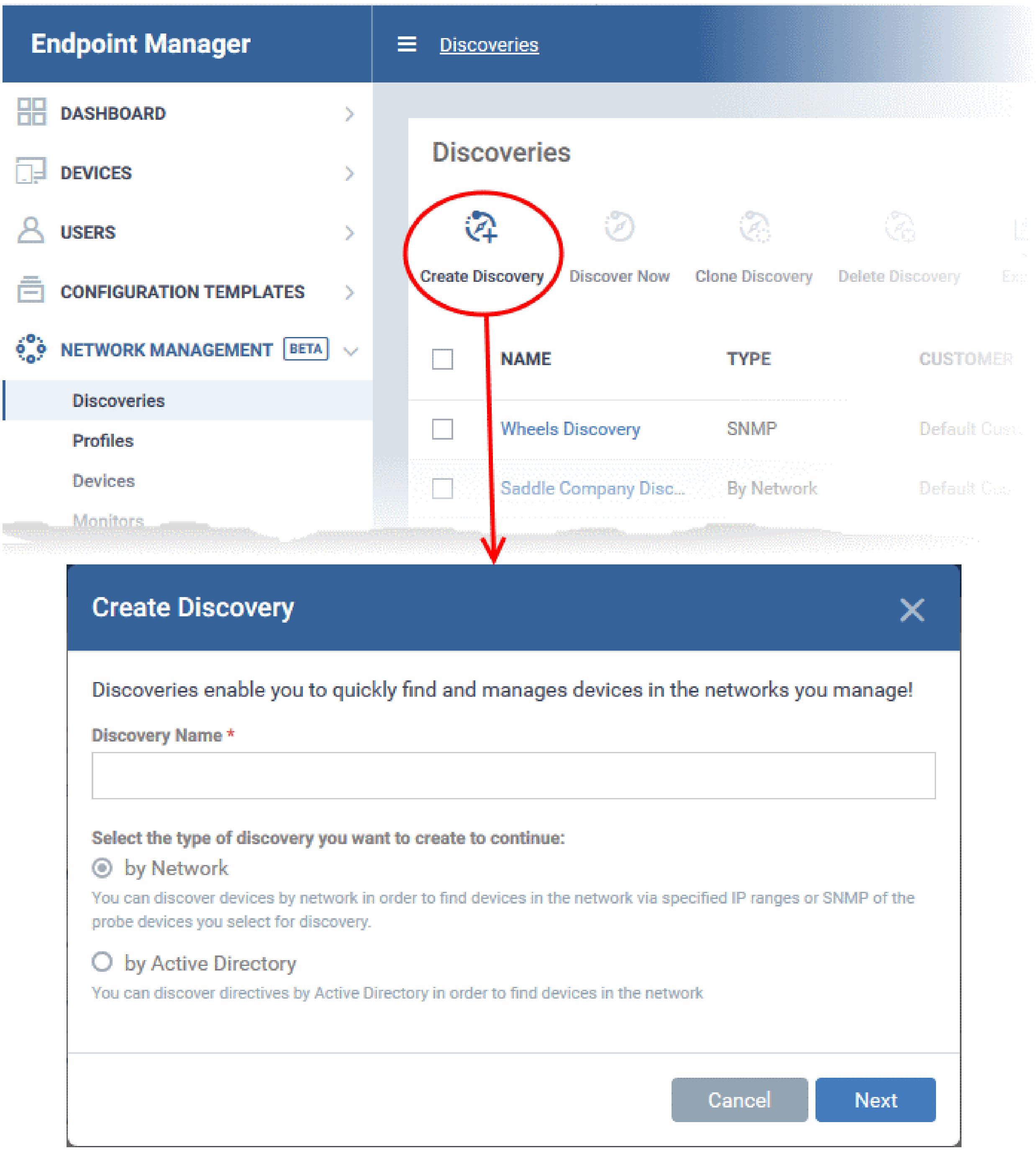
### Create a new discovery task

There are two types of discovery task:

- **Network** - Scan an IP range using a probe device. The probe must be a managed Windows device connected to the network. You can run a concurrent SNMP scan when you run a network scan.
- **Active Directory** - Scan an Active Directory domain for devices. You can configure the scan with or without a probe device. If not specified, EM will directly scan the AD server.

### Network discovery scan

- Click 'Network Management' > 'Discoveries'
- Click 'Create Discovery'



| ☐ | NAME | TYPE | CUSTOMER |
|---|---|---|---|
| ☐ | Wheels Discovery | SNMP | Default Cust.. |
| ☐ | Saddle Company Disc... | By Network | Default Cu... |

Create Discovery

Discoveries enable you to quickly find and manages devices in the networks you manage!

Discovery Name *

Select the type of discovery you want to create to continue:

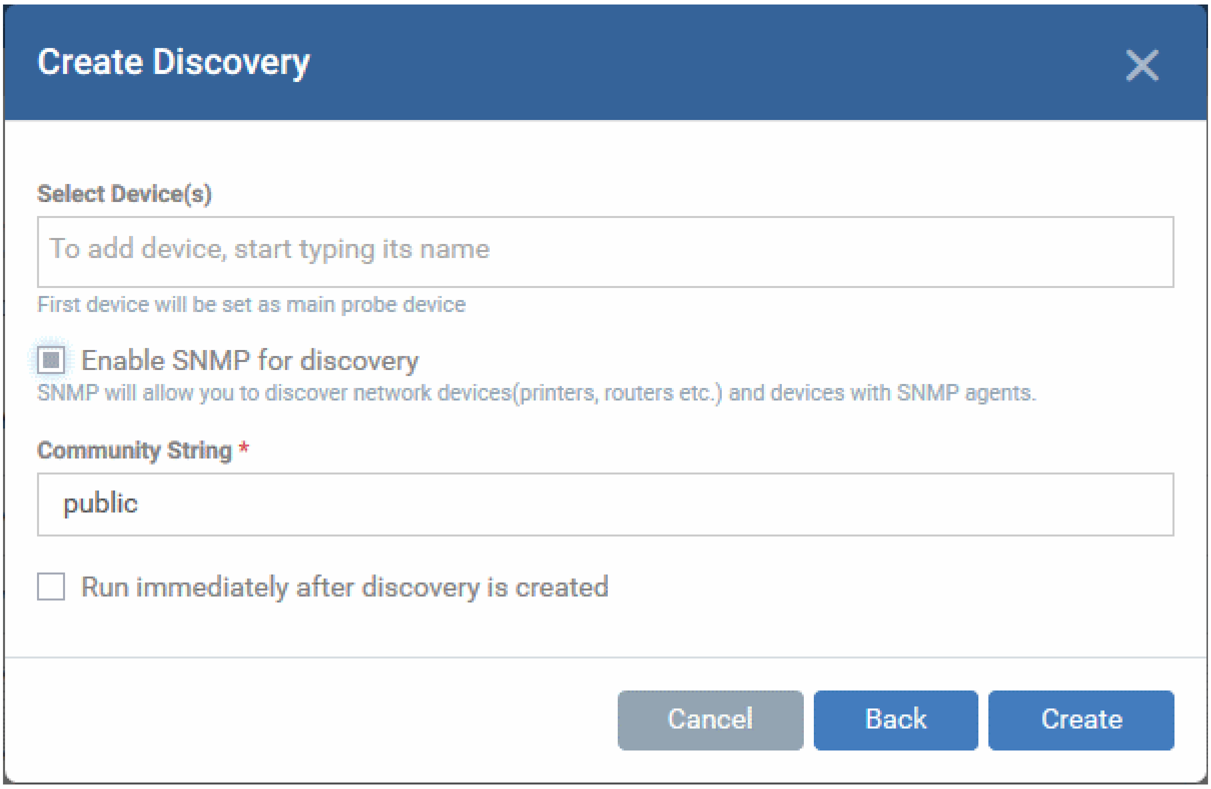
● by Network

You can discover devices by network in order to find devices in the network via specified IP ranges or SNMP of the probe devices you select for discovery.

○ by Active Directory

You can discover directives by Active Directory in order to find devices in the network

- **Discovery Name -** Create a label for the discovery task. Ideally, the label should help you identify the target or purpose of the task in future.
- Select 'by Network'
- Click 'Next' to add probe devices.


Create Discovery

Select Device(s)

To add device, start typing its name

First device will be set as main probe device

☒ Enable SNMP for discovery

SNMP will allow you to discover network devices(printers, routers etc.) and devices with SNMP agents.

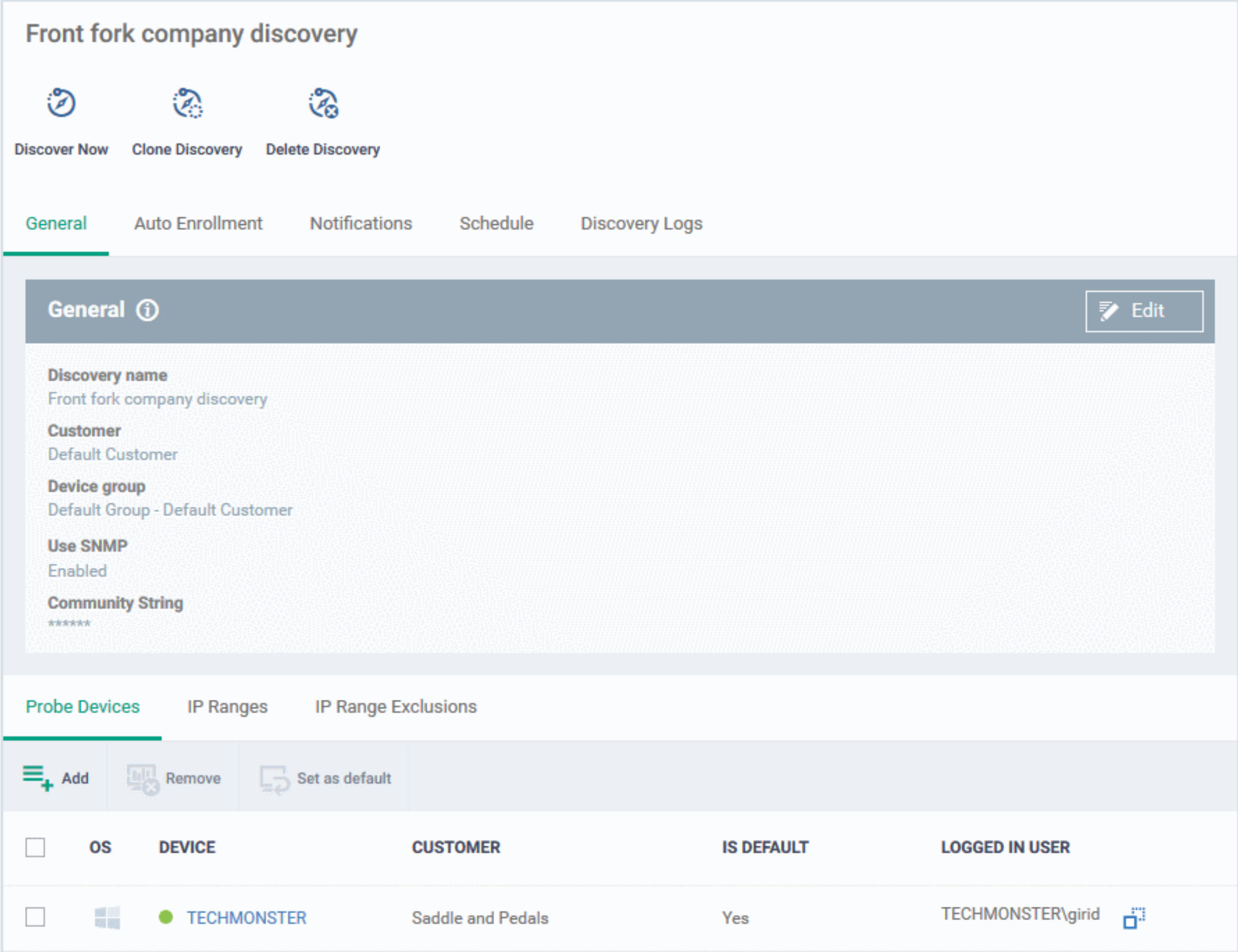
Community String *

public

□ Run immediately after discovery is created

- **Select Device(s)** - Start typing the name of the device you want to use as probe and select from the suggestions.
  - A probe device is a managed Windows endpoint inside the network that you want to scan. The device must already be enrolled to Endpoint Manager and have communication client (CC) 6.32 or higher installed. This device will launch the scans you request on the target network.
  - You can also add additional devices for fail-over. The device added first will be used as the probe. If the first device is offline then EM will use the next device for the scan.
- **Enable SNMP for discovery** - Run a simple network management protocol (SNMP) scan alongside the network scan.
  - If enabled, the SNMP scan will run simultaneously with the IP range scan.
  - The SNMP results are shown as separate row in the 'Network Management' > 'Devices' > 'Discovered Devices' interface.
  - Community String - This is a passcode sent with each SNMP Get-Request to authenticate access to a router or other device. If the community string is correct, then the device responds with the requested information.
- Run immediately after discovery is created - The discovery scan will start after it is saved.

- Click 'Create'
- The discovery task configuration screen opens:



Front fork company discovery

Discovery name
Front fork company discovery

Customer
Default Customer

Device group
Default Group - Default Customer

Use SNMP
Enabled

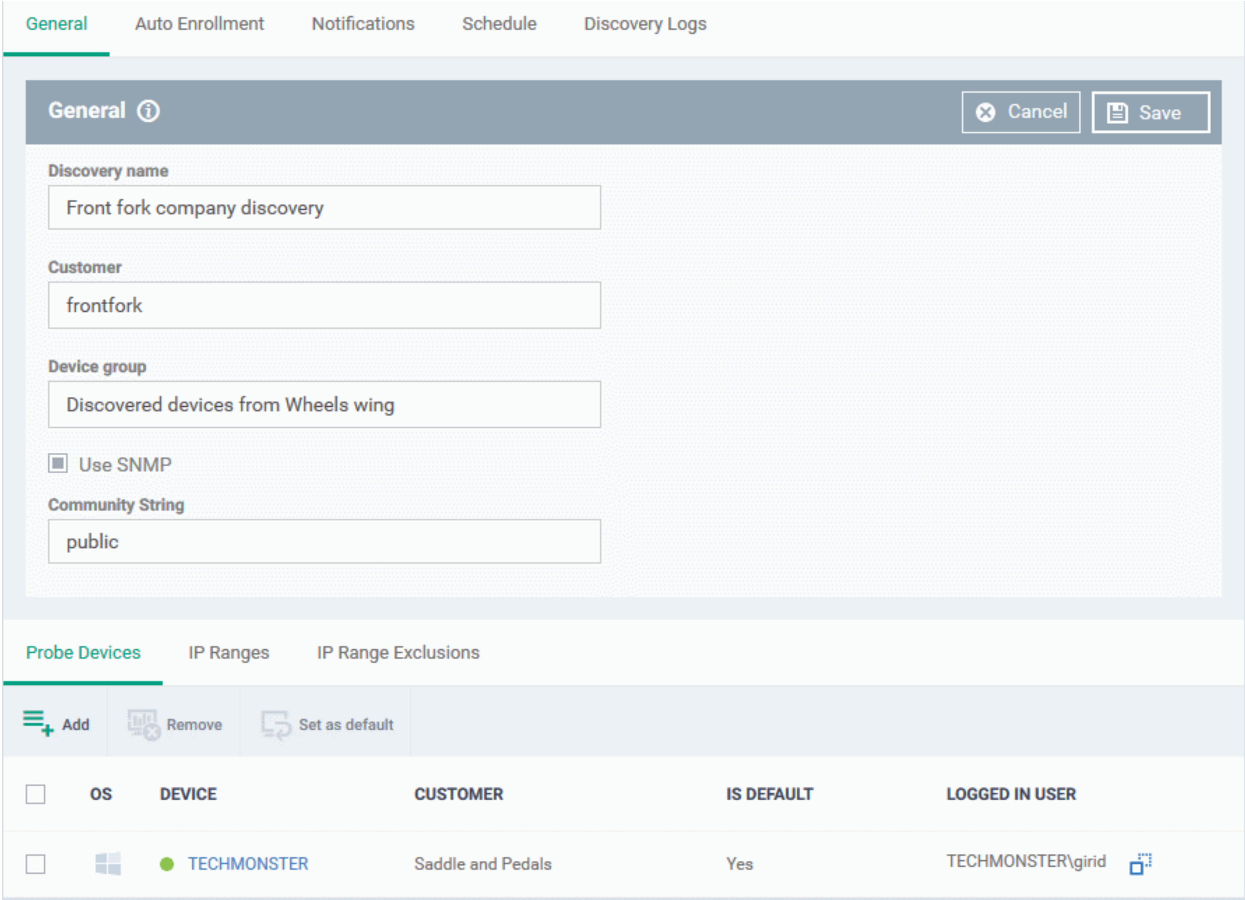
Community String
******

| □ | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|
| □ | | ● TECHMONSTER | Saddle and Pedals | Yes | TECHMONSTER\girid |

Next, click 'Edit' on the right to configure scan targets and options. Click the following sub-headers if you need help with a particular tab:

- **General** - Specify the IP addresses you want to scan. Set the customer and device group to which new devices should be assigned. Choose your probe device.
- **Auto Enrollment** - Windows devices only. Set the customer and device group to which you want to assign discovered Windows devices. Complete the instructions in the 'Auto Enrollment' tab on the probe and target devices.
- **Notifications** - Select which events you want to be notified about. Events include when the scan ends, when a new device is found, and when a new IP is found.
- **Schedule** - You can automate the discovery scans by scheduling them to run daily, weekly or monthly.
- **Discovery Logs** - View the results of previous scans run under this task. You can see the date, type and other general details about a scan. Click 'Details' then 'Click Here' to view a list of devices found by the scan.

### General Settings



Discovery name: Front fork company discovery

Customer: frontfork

Device group: Discovered devices from Wheels wing

☒ Use SNMP

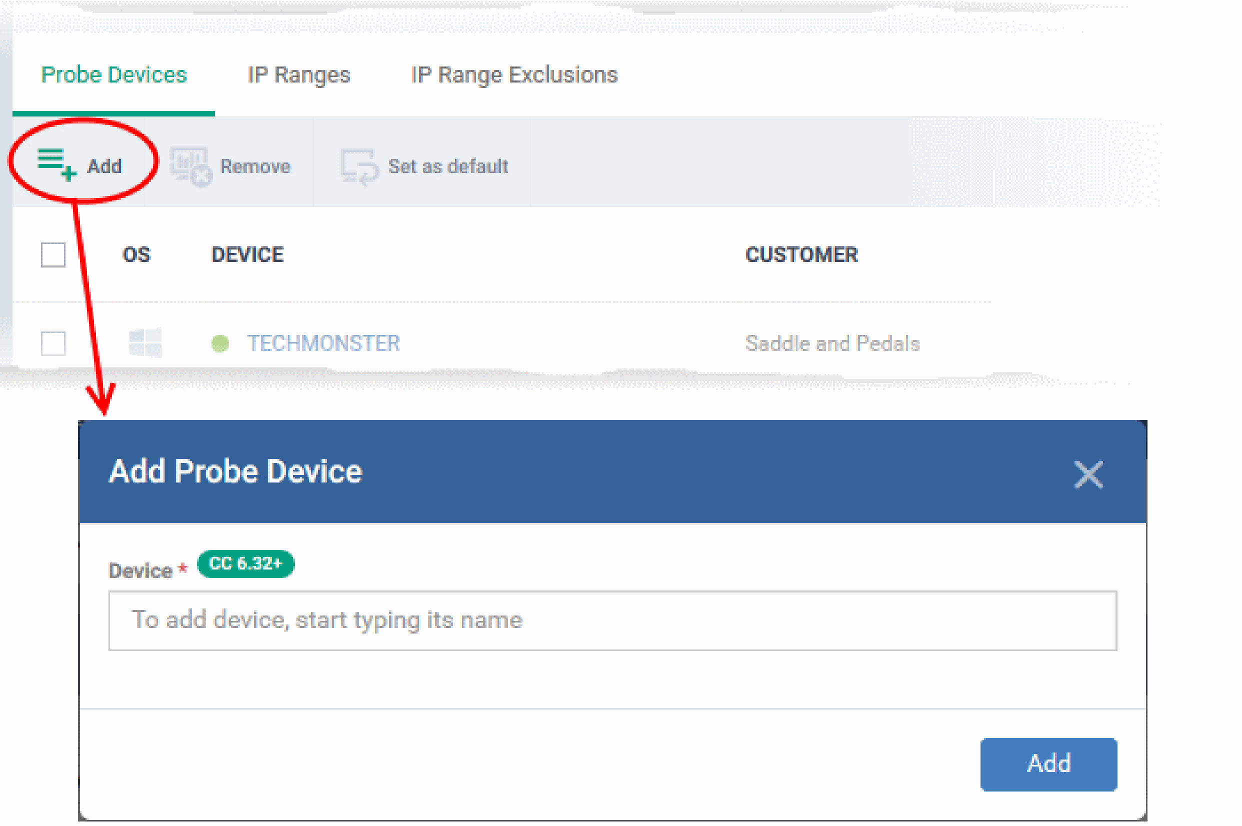
Community String: public

| | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|
| □ | | ● TECHMONSTER | Saddle and Pedals | Yes | TECHMONSTER\girid |

- **Discovery name -** This is pre-populated with the label you created in the previous step. Edit the name, if required.
- **Customer -** Specify the company that owns/controls the target network.
  - Enter first few letters of a company name and select from the suggestions.
- **Device group -** Specify the group to which discovered devices should be assigned. The device group must belong the 'Customer' named in the previous row.
  - Enter the first few letters of the device group and select from the suggestions.
- **SNMP -** Pre-populated with the choice you made in the previous step. Change the choice if required.
  - If enabled, the SNMP scan will run simultaneously with the IP range scan.
  - SNMP results are shown as a separate row in the 'Network Management' > 'Devices' > 'Discovered Devices' interface.
  - **Community String -** This is a passcode sent with each SNMP Get-Request to authenticate access to a router or other device. If the community string is correct, then the device responds with the requested information.

    Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string".

- **Probe Devices -** Pre-populated with the list of probe devices you specified in the previous step. You can add a new probe as follows:
  - Click 'Add' at top-left:



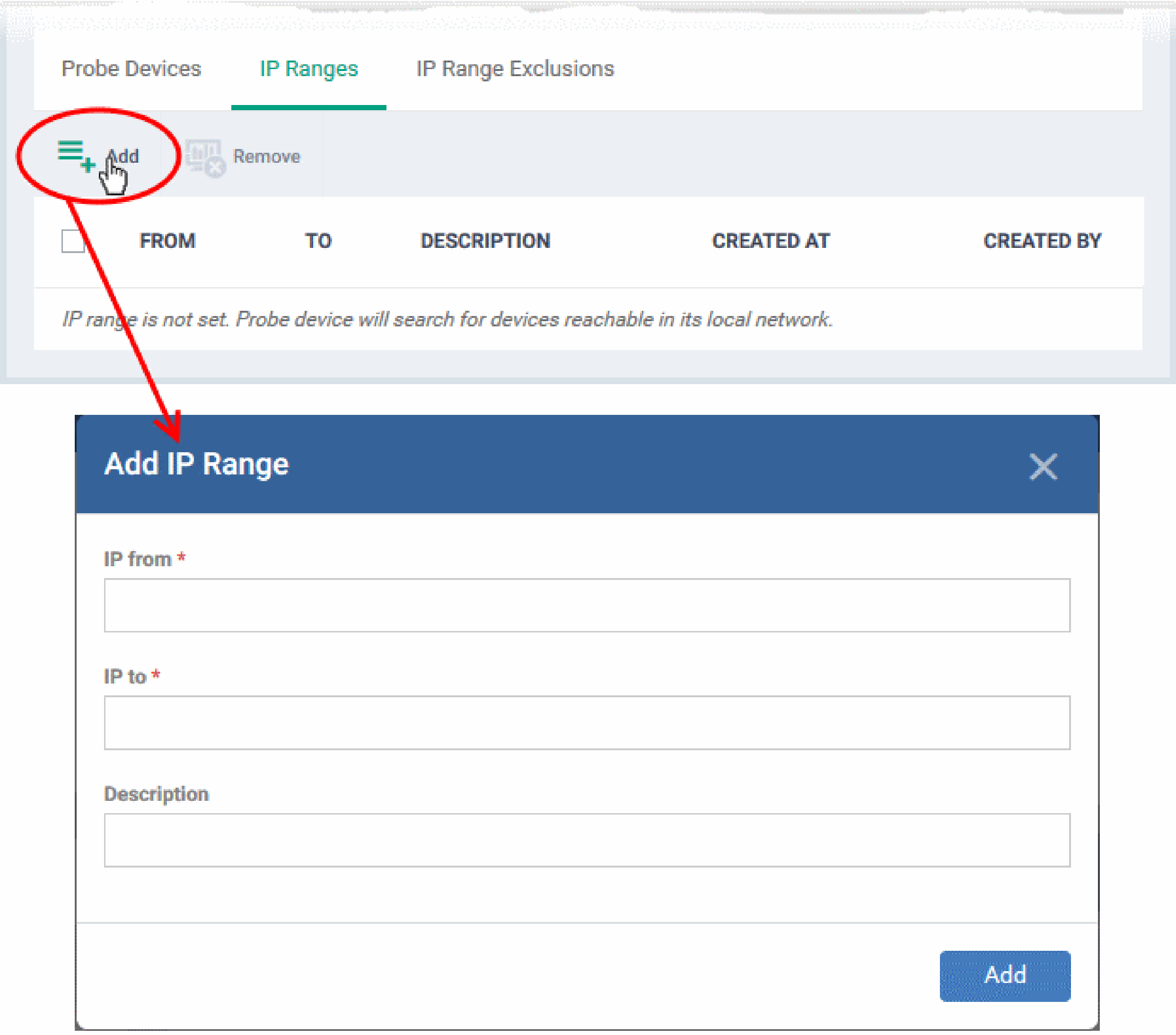
| OS | DEVICE | CUSTOMER |
|---|---|---|
|  | TECHMONSTER | Saddle and Pedals |

Add Probe Device

Device * CC 6.32+

To add device, start typing its name

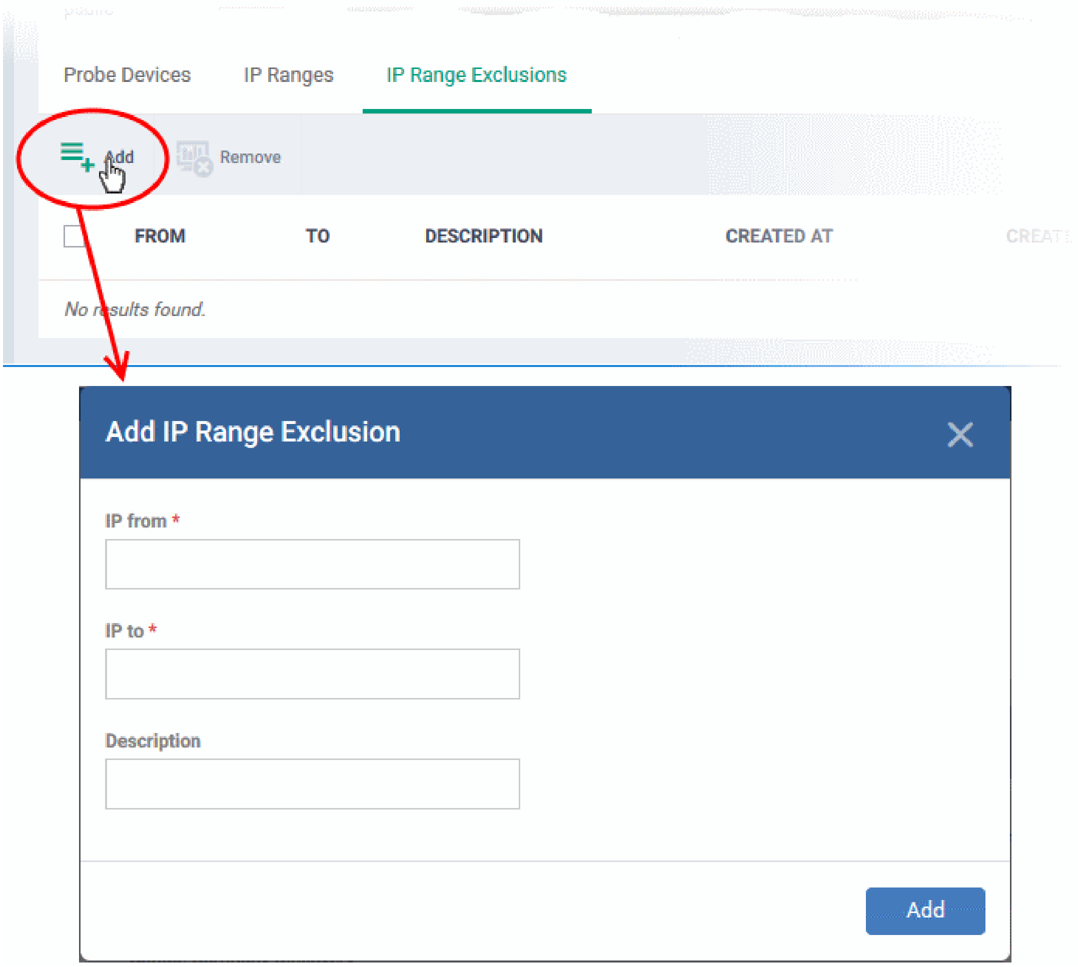
  - Start typing the name of the device you want to use as probe. Select from the suggestions.
  - You can add multiple devices for fail-over, if required. You must choose a default probe if you add multiple probes. The other probes are only used if the default is not available.
- **IP Ranges -** Specify the IP address range that you want to scan for connected devices. You can add any number of IP ranges within the network for a single discovery task. You can also specify addresses to be skipped as exclusions.
- Leave this blank if you want to scan the entire network to which the probe is connected.



*IP range is not set. Probe device will search for devices reachable in its local network.*

  - **IP from -** Start address of the IP range
  - **IP to -** End address of the IP range
  - **Description -** A brief description of the IP range (optional). Use this if there are different IP segments which you want to identify. You can enable or disable ranges as required in any scan task.
- Click 'Add' to add the IP range to the list
- Repeat the process to add more IP address ranges
- Select an IP range and click 'Remove' to delete the IP range from the list

- **IP Range Exclusions -** Specify IP addresses that should not be scanned.



No results found.

IP from *

IP to *

Description

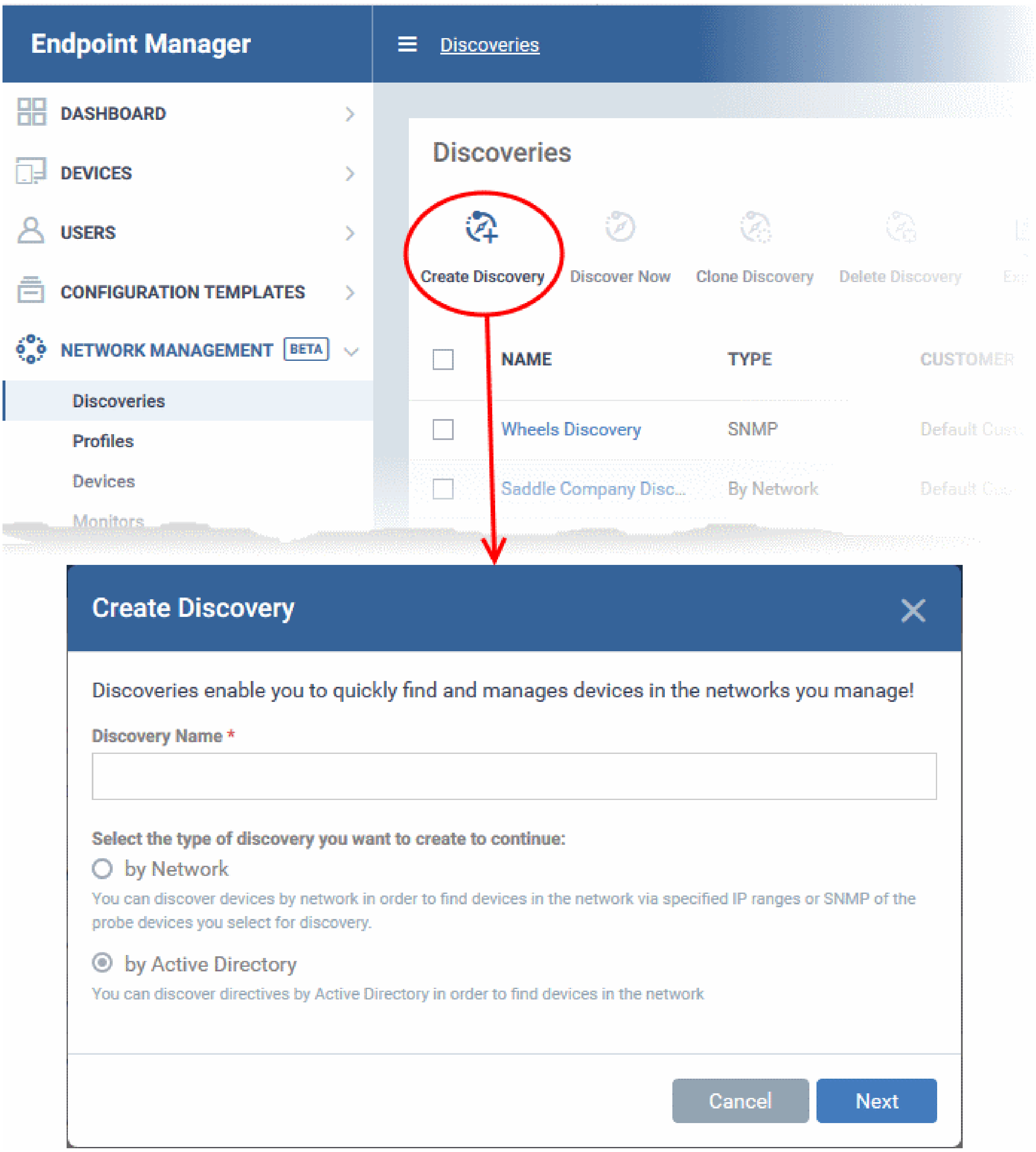
Next:

- Click the 'Auto Enrollment' tab to configure the scan to auto-enroll Windows devices. See **Auto Enrollment** for help with this.
- Click the 'Notifications' tab to configure alerts. See **Notification Settings** for help with this.
- Click the 'Schedule' to run the scan at a set time. See **Schedule the discovery task** for help with this.

**AD discovery scan**

- Click 'Network Management' > 'Discoveries'
- Click 'Create Discovery'

The 'Create Discovery' wizard starts:



Discoveries enable you to quickly find and manages devices in the networks you manage!

Discovery Name *

Select the type of discovery you want to create to continue:

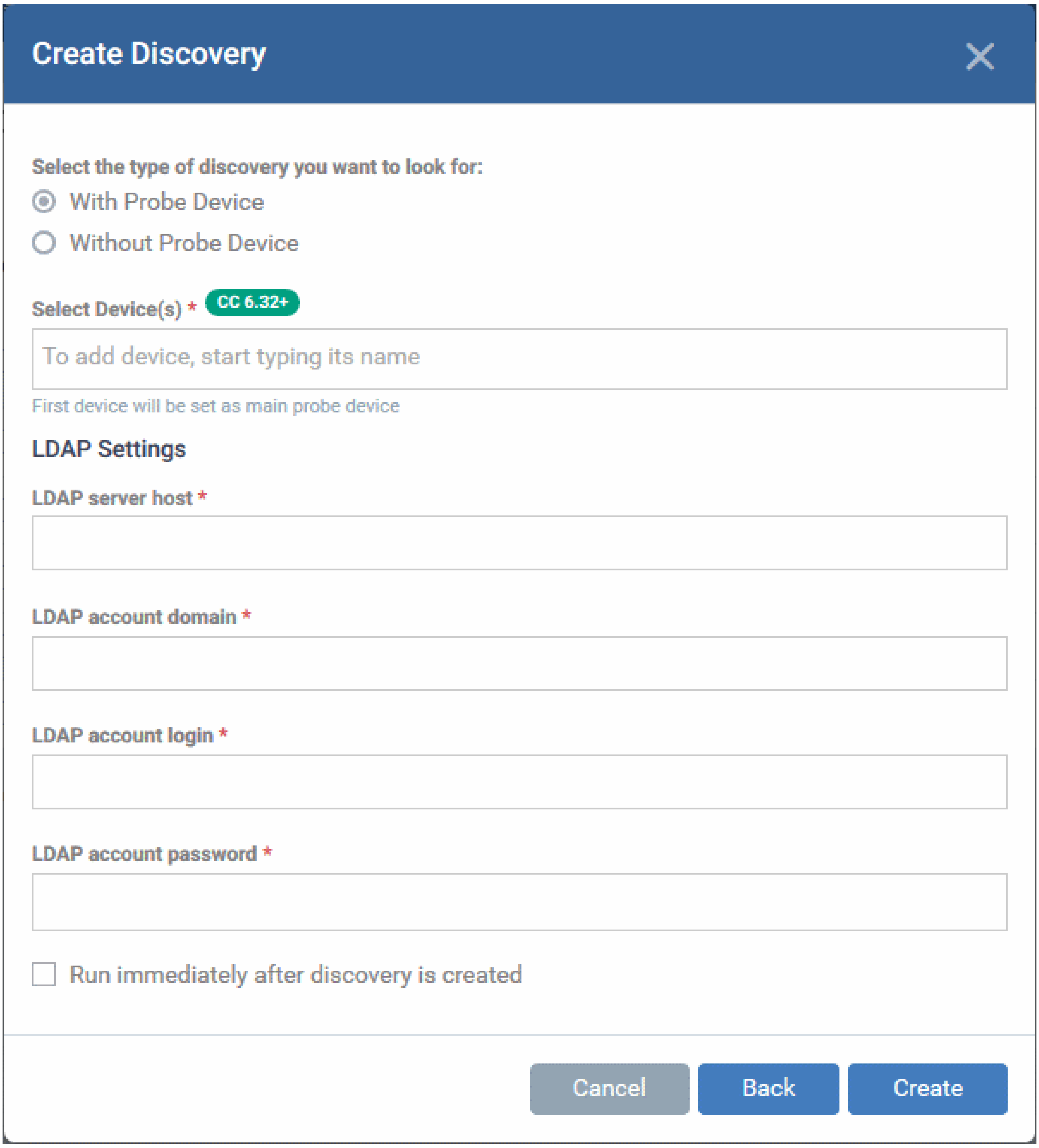
○ by Network

You can discover devices by network in order to find devices in the network via specified IP ranges or SNMP of the probe devices you select for discovery.

● by Active Directory

You can discover directives by Active Directory in order to find devices in the network

- **Discovery Name -** Enter a label for the new discovery task. Ideally, the label should help you identify the target or purpose of the task in future.
- Select 'by Active Directory'
- Click 'Next'.



Create Discovery

Select the type of discovery you want to look for:

● With Probe Device

○ Without Probe Device

Select Device(s) * CC 6.32+

To add device, start typing its name

First device will be set as main probe device

LDAP Settings

LDAP server host *

LDAP account domain *

LDAP account login *

LDAP account password *

□ Run immediately after discovery is created

- **Select the type of discovery**: There are two options:
    - **With Probe Device -** Specify a probe device to run the discovery scan on the AD domain.
        - Select this option if the AD server is not directly accessible through the internet.
        - A probe device is a managed Windows endpoint on the same network to which the AD server is connected.
        - The device must already be enrolled to Endpoint Manager and installed with communication client (CC) version 6.32 or higher. This device will launch the scans you request on the target network.
        - The probe device need not be a member of the AD domain
        - If selected, specify the probe device to be used in the 'Select Devices' field
    - **Without Probe Device -** The discovery scan will be run directly by EM
        - Select this option if the AD server is accessible through the internet.
        - You need not specify a probe device to run the scan.

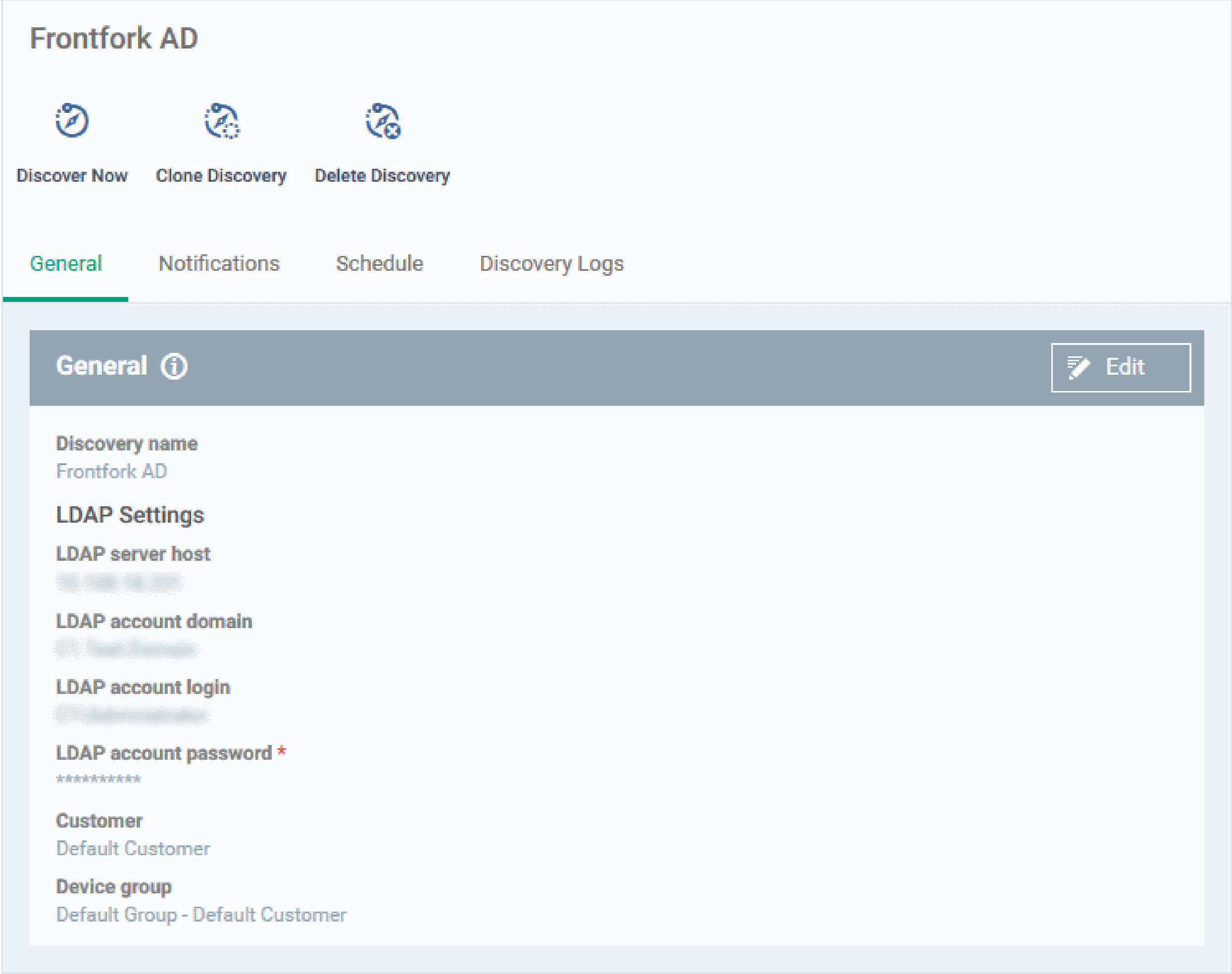
- **Select Device(s) -** Applicable only if 'With Probe Device' is chosen.
  - Start typing the name of the device you want to use as probe and select from the suggestions.
  - You can also add additional devices for fail-over. The device added first will be used as the probe. If the first device is offline at the time of discovery, EM will use the next device and so on.

**LDAP Settings**:

- **LDAP server host -** Enter the IP address or hostname of the AD server that hosts the AD domain
- **LDAP account domain -** Enter the domain name of the AD domain
- **LDAP account login** and **LDAP account password -** The admin username and password required to access the AD server.

- **Run immediately after discovery is created -** The discovery scan will start after it is saved.

- Click 'Create'
- The discovery task configuration screen opens:



Discovery name
Frontfork AD

LDAP Settings

LDAP server host
[redacted]

LDAP account domain
[redacted]

LDAP account login
[redacted]

LDAP account password *
**********

Customer
Default Customer

Device group
Default Group - Default Customer

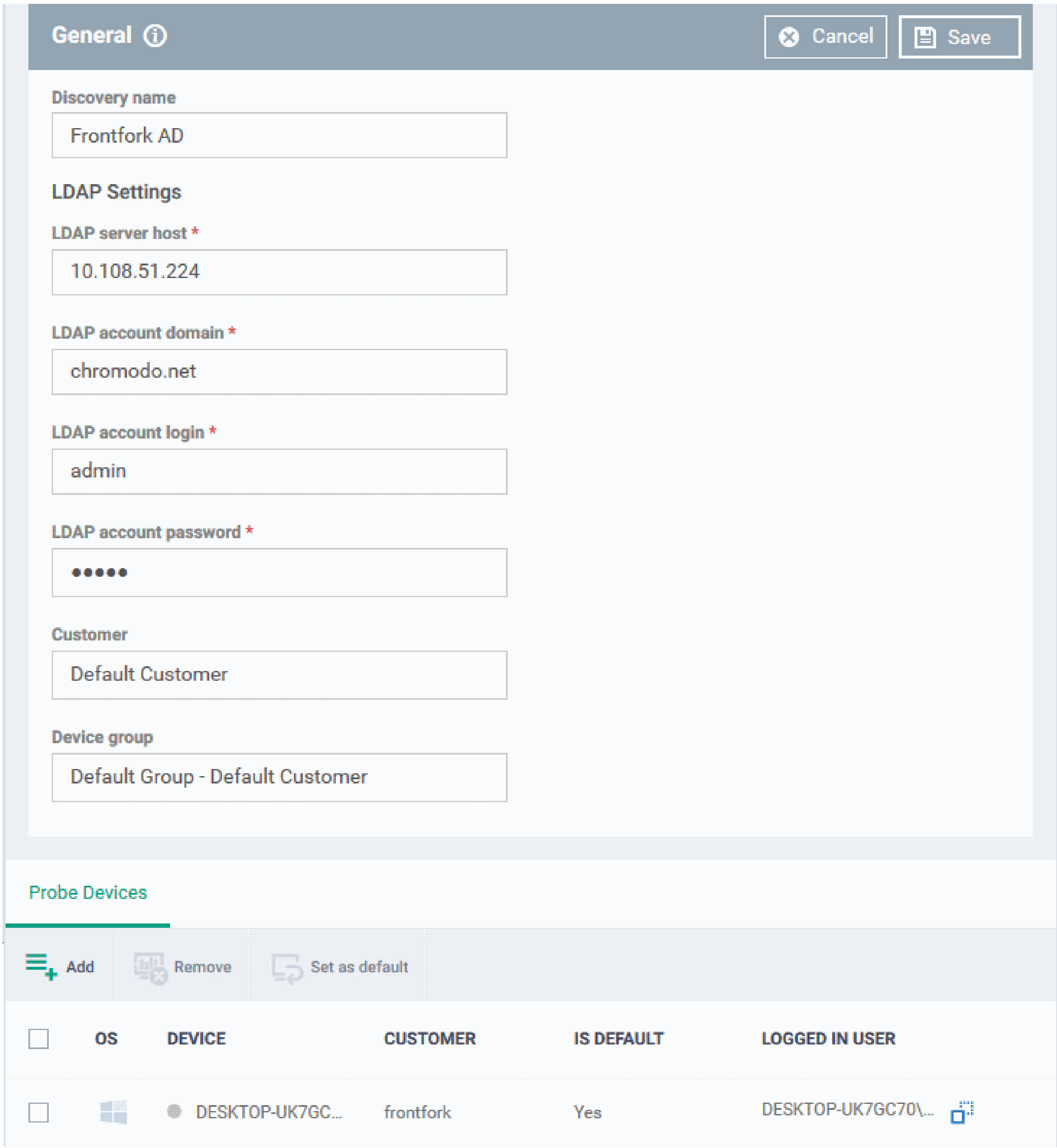
Click 'Edit' on the right to get started. Click the following sub-headers if you need help with a particular tab:

- **General** - Edit the LDAP details of the AD server you want to scan. Set the customer and device group to which new devices should be assigned. Choose your probe device.
- **Notifications** - Select which events you want to be notified about. Events include when the scan ends and when a new device is found.
- **Schedule** - You can automate the discovery scans by scheduling them to run daily, weekly or monthly.

- **Discovery Logs** - View the results of previous scans run under this task. You can see the date, type and other general details about a scan. Click 'Details' then 'Click Here' to view a list of devices found by the scan.

**General Settings**

- Click the 'General' tab (if it is not already open)
- Click the 'Edit' button at the top-right



Discovery name
Frontfork AD

LDAP Settings

LDAP server host *
10.108.51.224

LDAP account domain *
chromodo.net

LDAP account login *
admin

LDAP account password *
●●●●●

Customer
Default Customer

Device group
Default Group - Default Customer

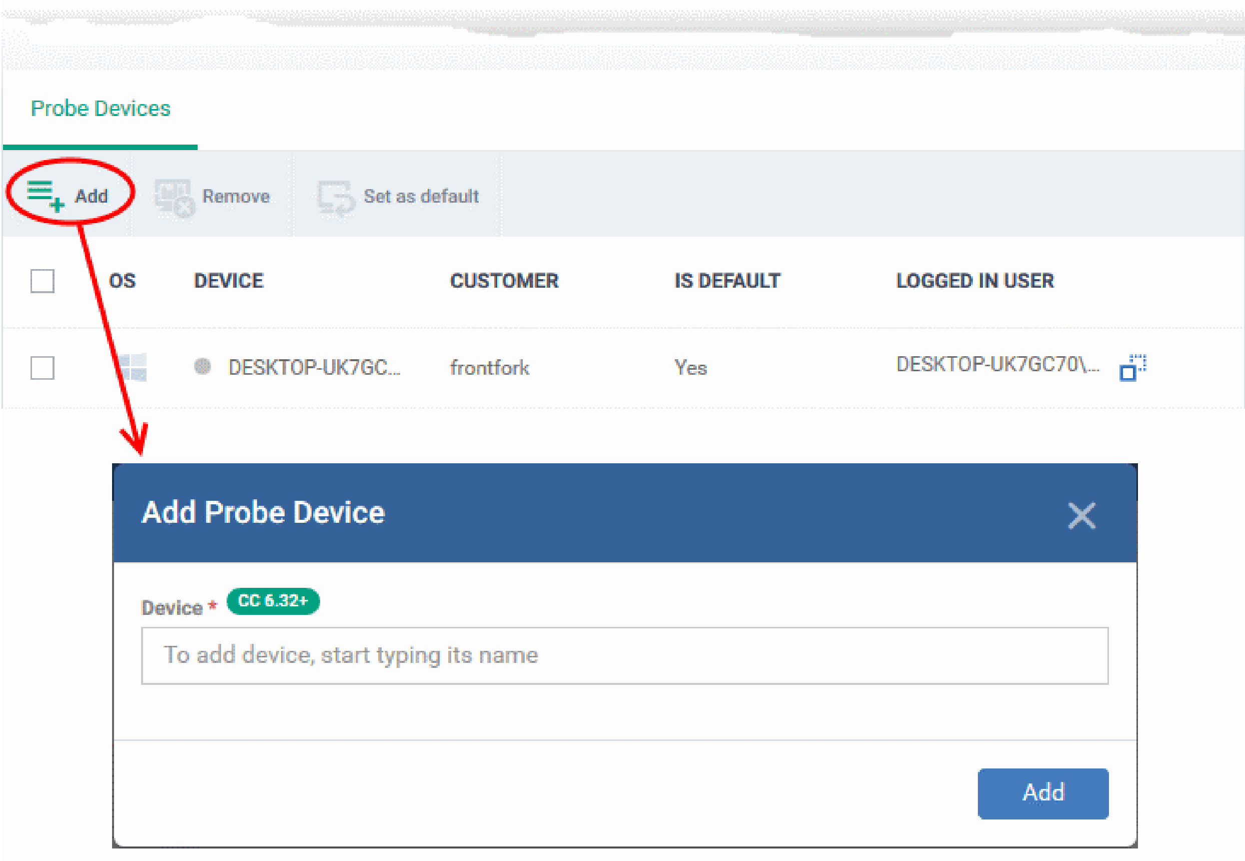
| □ | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|
| □ | | DESKTOP-UK7GC... | frontfork | Yes | DESKTOP-UK7GC70\... |

- **Discovery name** - This field is pre-populated with the label you created in the previous step. Edit the name, if required.
- **LDAP Settings** - The hostname of the AD server, AD domain name, AD admin username and password are pre-populated from the details you entered in the previous step. Modify them if required.
- **Customer** - Specify the company that owns/controls the target AD network.
  - Enter first few letters of a company name and select from the suggestions.

  - **Device group -** Specify the device group to which identified devices will be assigned. The device group must belong the 'Customer' named in the previous row.
    - Enter the first few letters of the device group and select from the suggestions.
- **Probe Devices -** Applies only if you have chosen 'With Probe Devices' in the previous step. The list is pre-populated with the probe devices you specified in the previous step. You can add or remove devices if required.

  **Add a probe device:**

  - Click 'Add' at the top-left:



| | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|
| □ | | DESKTOP-UK7GC... | frontfork | Yes | DESKTOP-UK7GC70\... |

  - Start typing the name of the device you want to use as the probe then select from the suggestions.
  - You can also add additional devices for fail-over. The device added first will be used as the probe. if the first device is offline at the time of discovery, EM will use the next device and so on.
- Click 'Add'.
- Repeat the process to add more probes. Multiple probes act as fail-overs for each other.
- You must select a default probe for scans if you add multiple probes. The other probes will only run the scan if the default probe is not available
- Click 'Save'

Next:

- Click the 'Notifications' tab to configure the alerts. See **Notification Settings** for help with this.
- Click the 'Schedule' tab to create a schedule to periodically run the scans. See **Schedule the discovery task** for help with this.

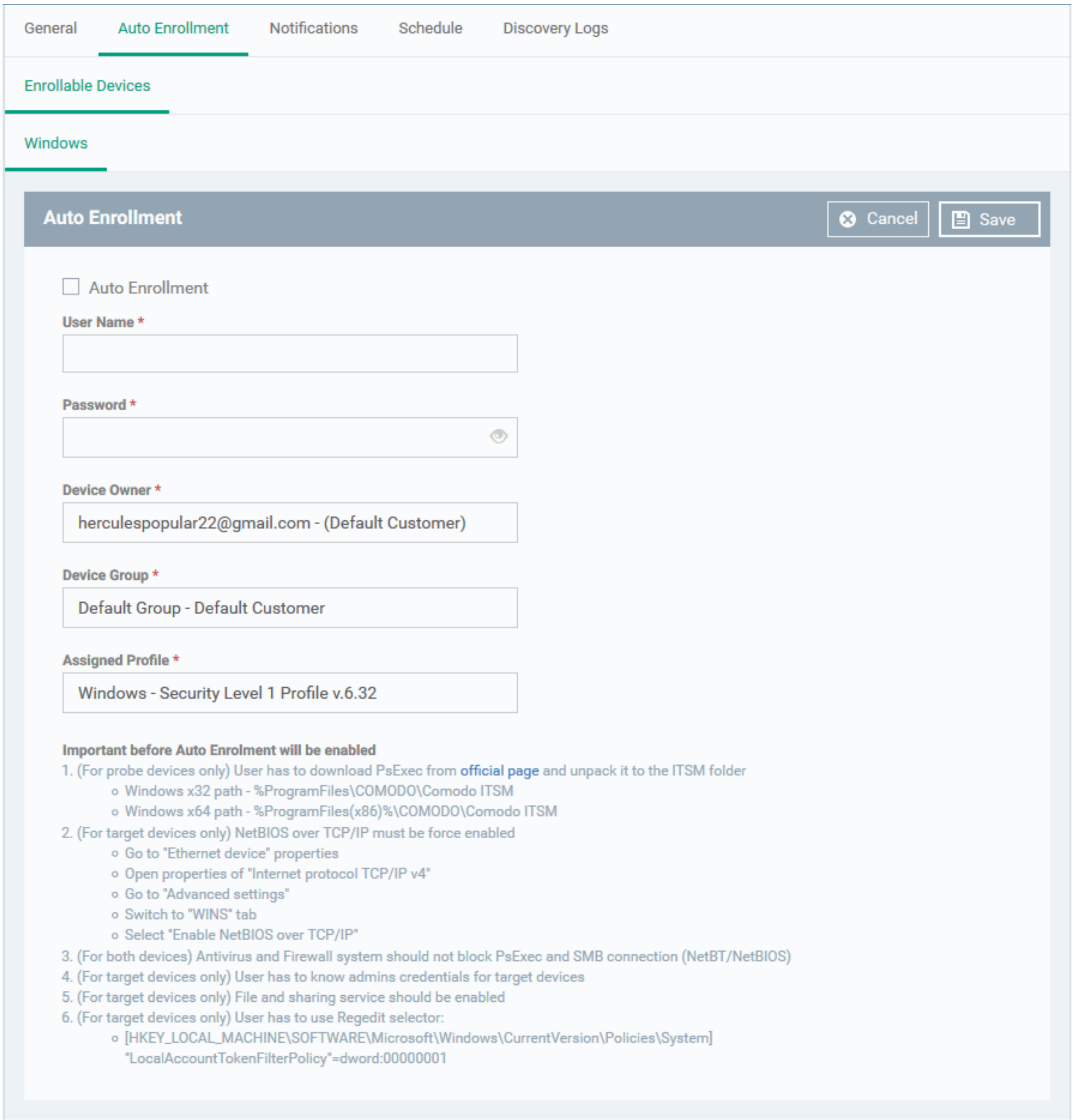
### Auto Enrollment

- You must download and install PsTools on the probe device before you can use the auto-enrollment feature.
- You also need to enable NetBIOS over TCP/IP on target devices.

- Read the full instructions on the 'Auto Enrollment' page and complete the steps therein.

Auto-enroll devices:

- Click the 'Auto Enrollment' tab
- Click the 'Edit' button at the top-right



□ Auto Enrollment

User Name *

Password *

Device Owner *
herculespopular22@gmail.com - (Default Customer)

Device Group *
Default Group - Default Customer

Assigned Profile *
Windows - Security Level 1 Profile v.6.32

**Important before Auto Enrolment will be enabled**

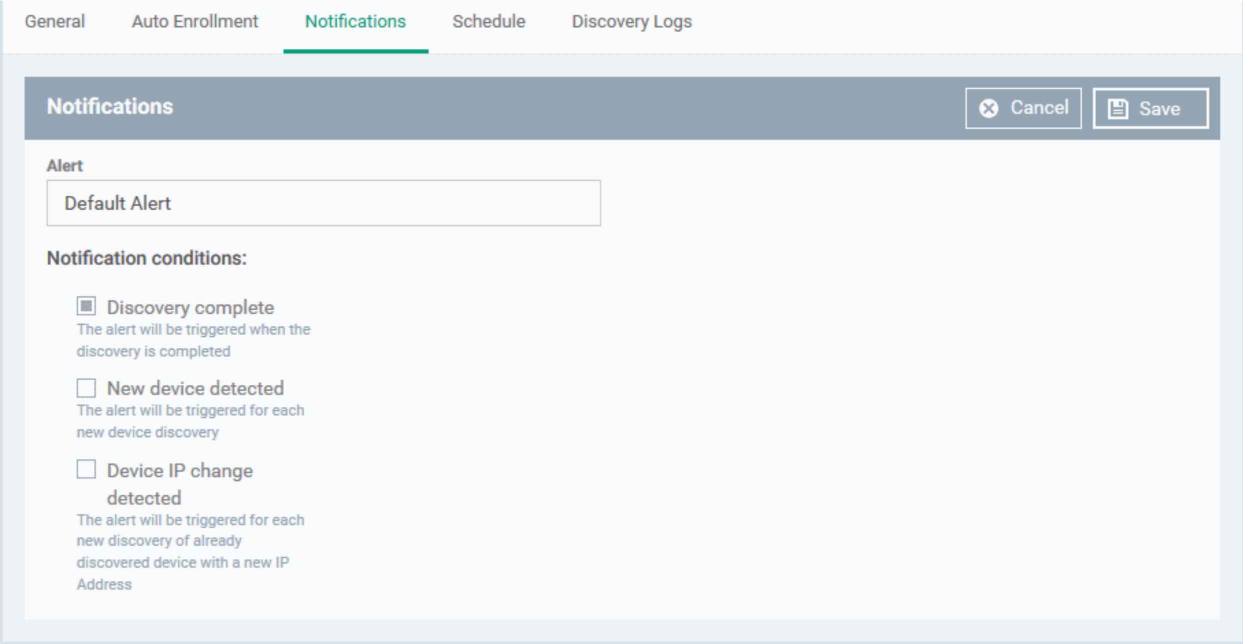
1. (For probe devices only) User has to download PsExec from official page and unpack it to the ITSM folder
   - Windows x32 path - %ProgramFiles\COMODO\Comodo ITSM
   - Windows x64 path - %ProgramFiles(x86)%\COMODO\Comodo ITSM
2. (For target devices only) NetBIOS over TCP/IP must be force enabled
   - Go to "Ethernet device" properties
   - Open properties of "Internet protocol TCP/IP v4"
   - Go to "Advanced settings"
   - Switch to "WINS" tab
   - Select "Enable NetBIOS over TCP/IP"
3. (For both devices) Antivirus and Firewall system should not block PsExec and SMB connection (NetBT/NetBIOS)
4. (For target devices only) User has to know admins credentials for target devices
5. (For target devices only) File and sharing service should be enabled
6. (For target devices only) User has to use Regedit selector:
   - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "LocalAccountTokenFilterPolicy"=dword:00000001

- **Auto Enrollment** - Enable this to auto-enroll discovered Windows devices to EM
- **User Name / Password** - Admin credentials for the target devices.
- **Device Owner** - Select the admin of the customer that you selected in the general tab. The devices are assigned to this admin after enrollment. You can assign the device to the appropriate user later. Start typing a name and select from the suggestions.
- **Device Group** - Choose the group to which you want to assign auto-enrolled devices. Start typing the group name and select from the suggestions.
- **Assigned Profile** - Choose the profile you want to apply to discovered devices. Start typing a profile name and select from the suggestions. Note - The security client has to be installed for the profile to take effect.

- Click 'Save' to apply your changes

### Notification Settings

- Click the 'Notifications' tab
- Click the 'Edit' button at the top-right



Alert

Default Alert

Notification conditions:

☒ Discovery complete
The alert will be triggered when the discovery is completed

□ New device detected
The alert will be triggered for each new device discovery

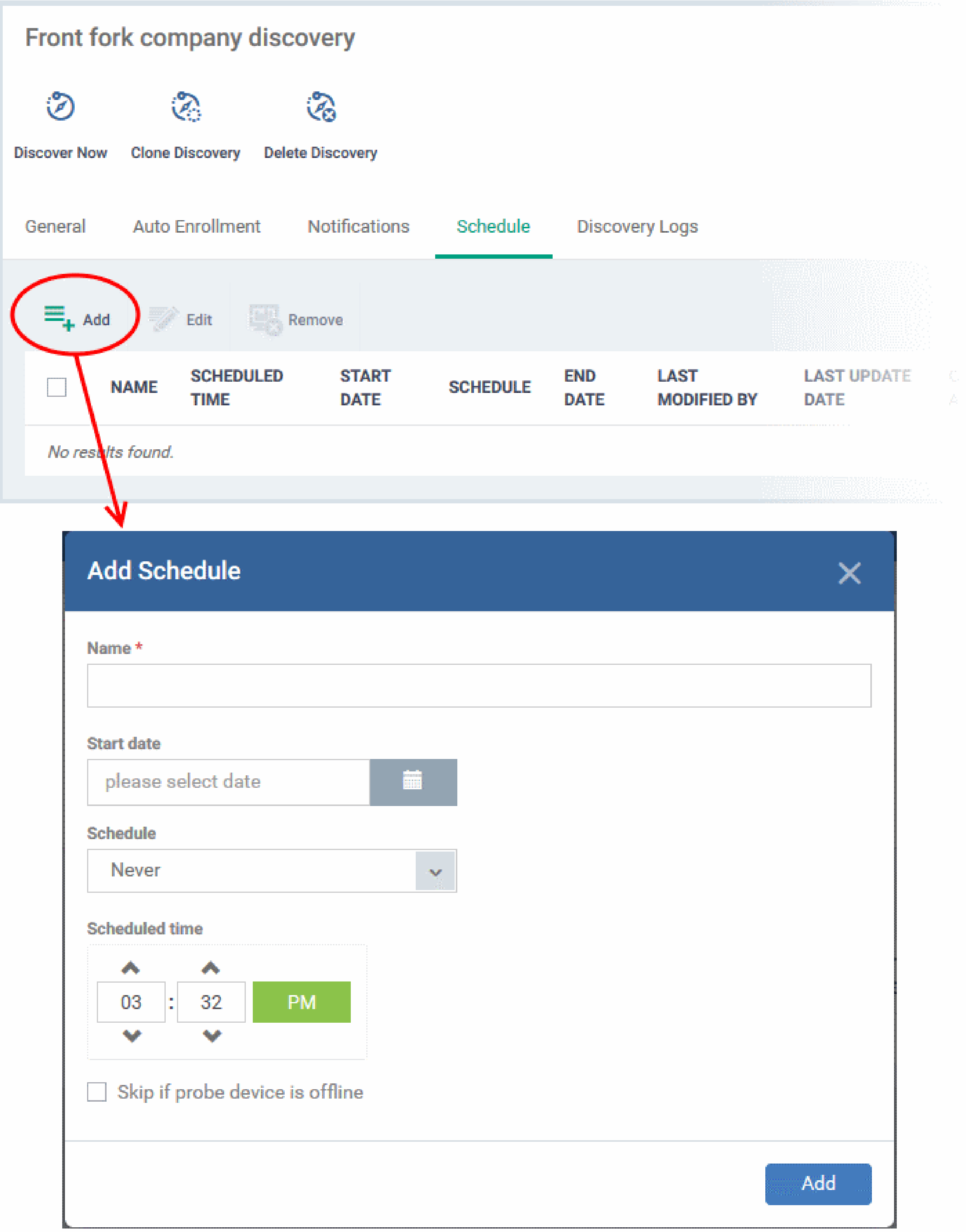
□ Device IP change detected
The alert will be triggered for each new discovery of already discovered device with a new IP Address

- **Alert -** Choose the alert template for your notification. An alert template contains general settings of your alert and specifies its recipients. Alert templates are configured in 'Configuration Templates' > 'Alerts'. See **Manage Alerts** for more details.
- Select which events generate an alert:
  - **Discovery complete -** Get an alert when a discovery scan finishes
  - **New device detected -** Get an alert when a device is identified for the first time
  - **Device IP change detected -** Get an alert if the IP address of a device changes (Available only for network scans)
- Click 'Save' for your settings to take effect

### Schedule the discovery task

The 'Schedule' tab lets you configure daily, weekly or monthly scans to run at specific times.

- Click the 'Schedule' tab
- Click 'Add' to create a schedule



Schedule: Never

Scheduled time: 03 : 32 PM

□ Skip if probe device is offline

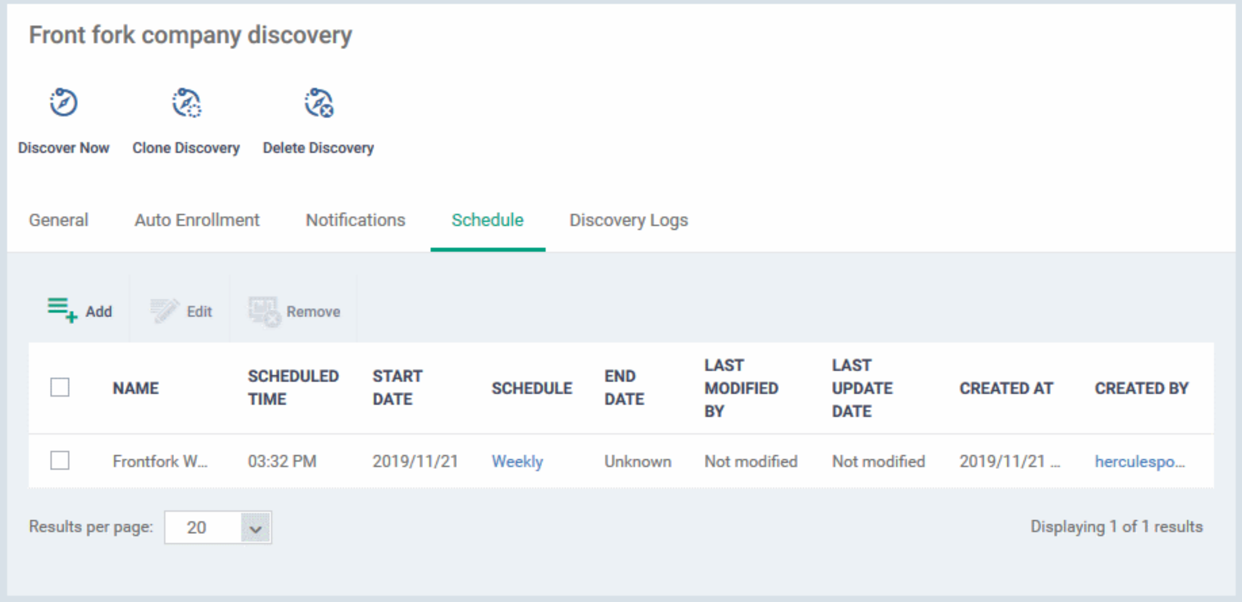
- **Name -** Enter a label for the discovery scan schedule
- **Start date** - Select what date the scan should start
- **Schedule -** Specify whether the scan should run daily, weekly, monthly, or never.
  - For weekly, specify the days of the week
  - For monthly, specify the days of the month
- **Scheduled time -** Specify the scan start time
- **Finish date -** The options are:

- No end date
- End date - Select the date on which the schedule will end.

- **Skip if probe device is offline -** The scan will be aborted if all probe devices are offline at the scheduled time. If disabled, the scan will be queued until the device comes online.

- Click 'Add'

The schedule will be saved and added to the list.



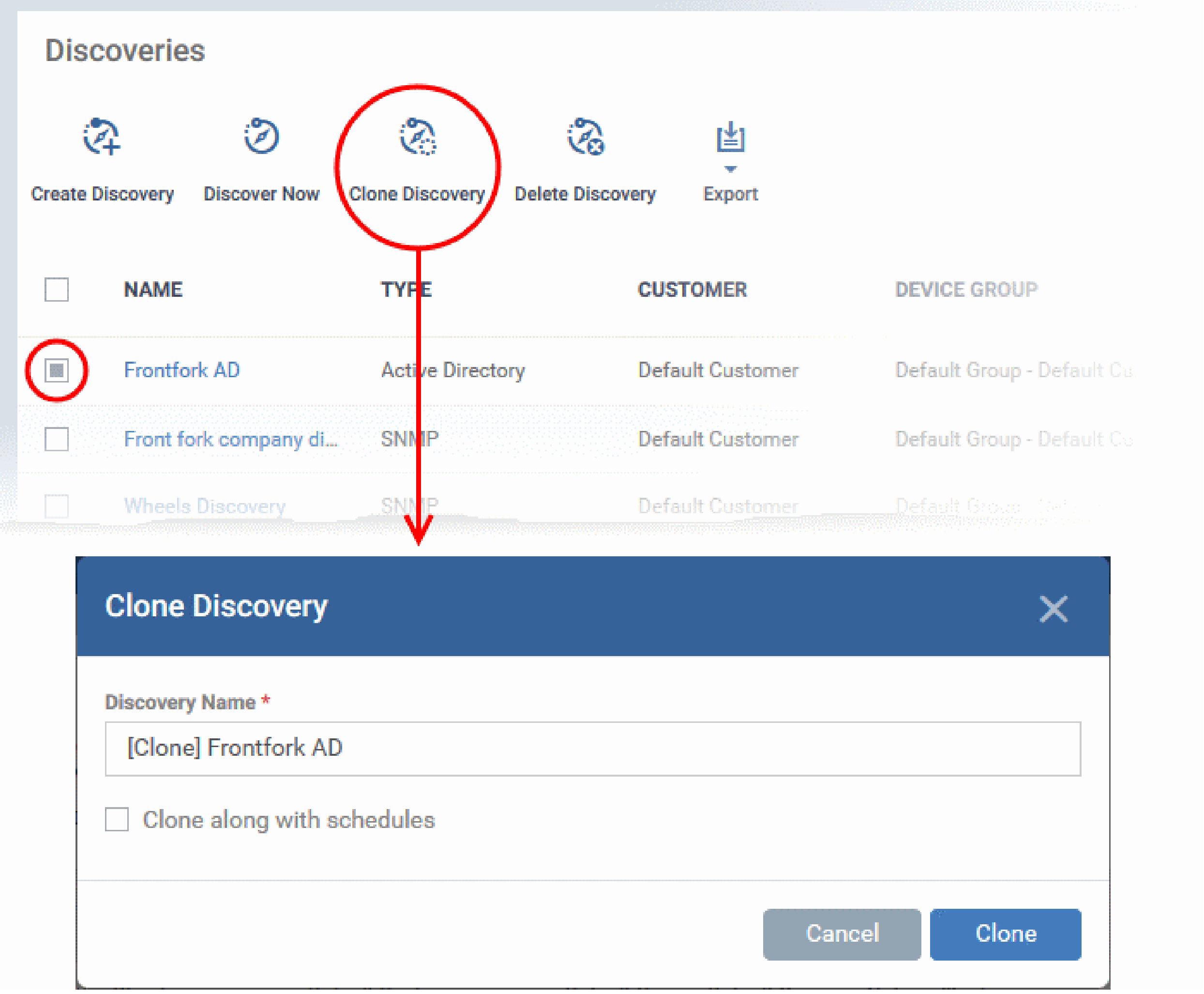
| □ | NAME | SCHEDULED TIME | START DATE | SCHEDULE | END DATE | LAST MODIFIED BY | LAST UPDATE DATE | CREATED AT | CREATED BY |
|---|---|---|---|---|---|---|---|---|---|
| □ | Frontfork W... | 03:32 PM | 2019/11/21 | Weekly | Unknown | Not modified | Not modified | 2019/11/21 ... | herculespo... |

Results per page: 20 Displaying 1 of 1 results

- Repeat the process to add more schedules
- Select a schedule and click the Edit button on the top to modify it
- Select a schedule and click the 'Remove' button at the top to delete it

## Create a new discovery task by cloning an existing task

- Click 'Network Management' > 'Discoveries'
- Select the discovery task you want to use as the base and click 'Clone Discovery'
- Alternatively, click the name of the discovery scan task and click 'Clone Discovery' on the top of the configuration screen.



| □ | NAME | TYPE | CUSTOMER | DEVICE GROUP |
|---|---|---|---|---|
| ☒ | Frontfork AD | Active Directory | Default Customer | Default Group - Default Cu |
| □ | Front fork company di... | SNMP | Default Customer | Default Group - Default Cu |
| □ | Wheels Discovery | SNMP | Default Customer | Default Group - |

[Clone] Frontfork AD

□ Clone along with schedules

- **Discovery Name -** The label of the discovery task. This is auto-populated with the name of the source discovery task wit the prefix '[Clone]'. Create a new name for the task, if required.
- **Clone along with schedules -** Select if you want to use the same schedule as the source task.
- Click 'Clone'.

The new discovery scan task is created with the parameters of the source task.

- Edit the task as required in the confirmation screen. See above if you need help.
- Click 'Save' to apply your changes

## Run a Discovery Task

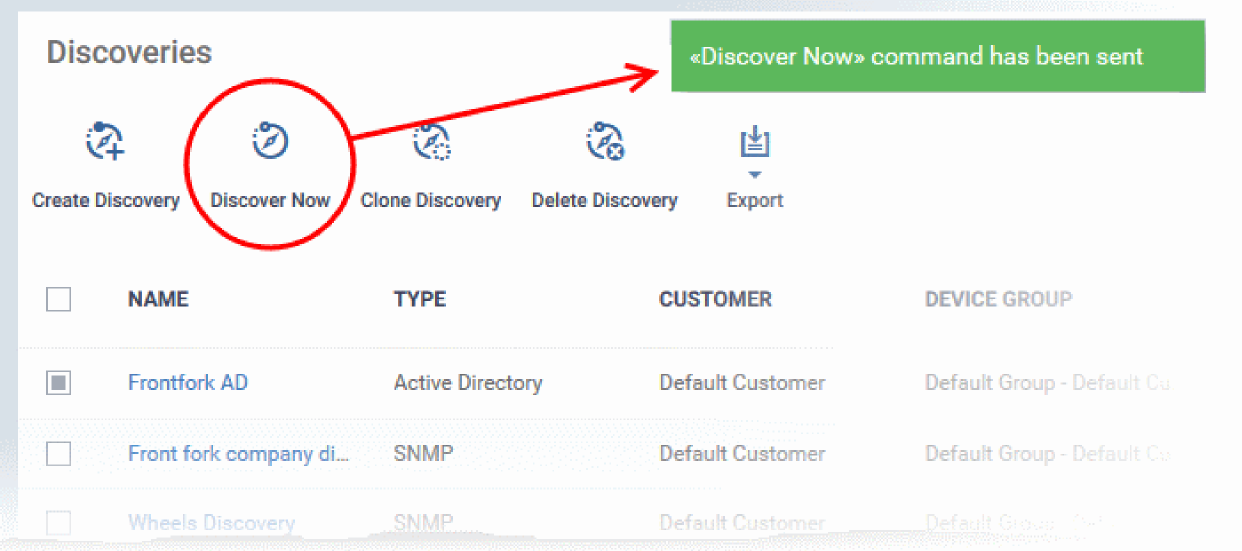
There are two ways you can run a discovery task:

- From 'Network Management' > 'Discoveries'
- From 'Network Management' > 'Devices' .

The following section explains how to run a scan from the 'Discoveries' interface.

**Run an on-demand network discovery scan**

- Click 'Network Management' > 'Discoveries'
- Select the discovery scan task from the list and click 'Discover Now' on the top
- Alternatively, click the name of the discovery task and click 'Discover Now':



Discoveries

«Discover Now» command has been sent

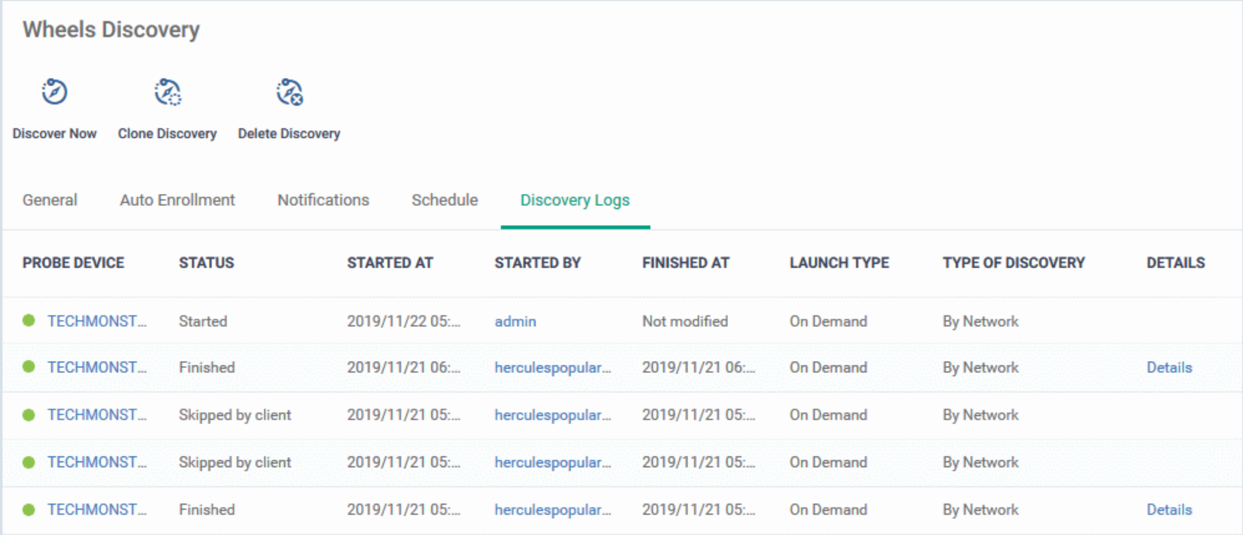
| | NAME | TYPE | CUSTOMER | DEVICE GROUP |
|---|---|---|---|---|
| ☒ | Frontfork AD | Active Directory | Default Customer | Default Group - Default Cu |
| □ | Front fork company di... | SNMP | Default Customer | Default Group - Default Cu |
| □ | Wheels Discovery | SNMP | Default Customer | Default Group - Def |

- The scan will start and will run for ten minutes. Any SNMP scans will start simultaneously.
- All discovered devices will appear in 'Network Management' >'Devices' > 'Discovered Devices'
    - See **Discovered Devices** for more details.

## View Discovery Logs

The 'Discovery Logs' tab in the discovery scan task configuration screen lets you view the history of scans run by the task and their details.

- Click 'Network Management' > 'Discoveries'
- Click the name of a discovery scan task to open its configuration interface
- Click the 'Discovery Logs' tab



Wheels Discovery

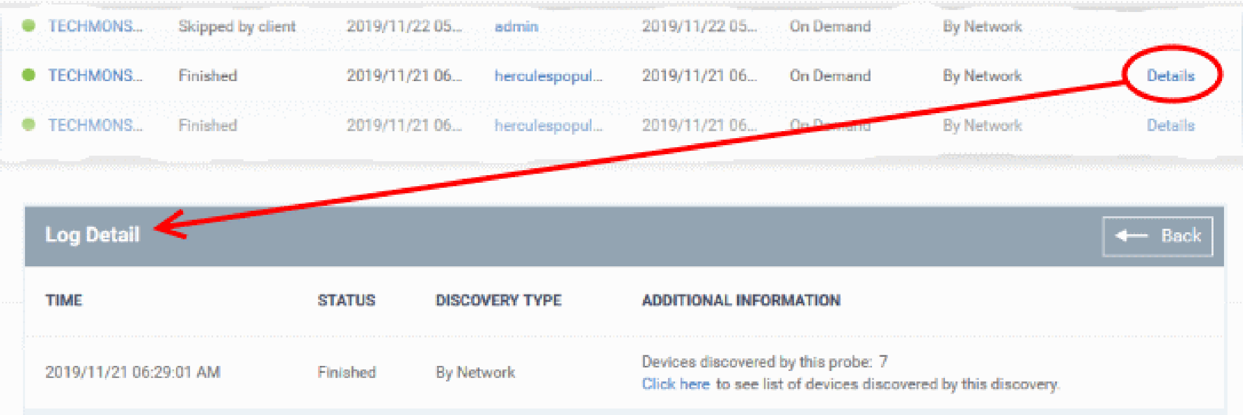
| PROBE DEVICE | STATUS | STARTED AT | STARTED BY | FINISHED AT | LAUNCH TYPE | TYPE OF DISCOVERY | DETAILS |
|---|---|---|---|---|---|---|---|
| ● TECHMONST... | Started | 2019/11/22 05:... | admin | Not modified | On Demand | By Network | |
| ● TECHMONST... | Finished | 2019/11/21 06:... | herculespopular... | 2019/11/21 06:... | On Demand | By Network | Details |
| ● TECHMONST... | Skipped by client | 2019/11/21 05:... | herculespopular... | 2019/11/21 05:... | On Demand | By Network | |
| ● TECHMONST... | Skipped by client | 2019/11/21 05:... | herculespopular... | 2019/11/21 05:... | On Demand | By Network | |
| ● TECHMONST... | Finished | 2019/11/21 05:... | herculespopular... | 2019/11/21 05:... | On Demand | By Network | Details |

| Discovery Scan Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Probe Device | The Windows device that ran the scan. Shown only for network discovery scans and AD discovery scans configured with a probe device. |

| | |
|---|---|
| | • Click the device name to view device's details. |
| Status | Current progress of the scan. The possible values are:<br>• Queued<br>• Started<br>• Skipped<br>• Finished |
| Started At | Date and time when the scan commenced. |
| Started By | Email address of the admin who launched the scan.<br>• Click the email address to view the details of the admin. See **View User Details** if you need help with this. |
| Finished At | Date and time the scan completed. |
| Launch Type | Whether the scan was scheduled or started manually. |
| Type of Discovery | The kind of the scan. The possible types are:<br>• Active Directory<br>• SNMP<br>• Network |
| Details | • Click the 'Details' link to view information such as the names and number of devices found.<br>• See **View Details of a Discovery Scan** for more info on the details screen. |

### View Discovery Scan Details

- Click 'Details' in the row of a scan to view additional information:



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ● TECHMONS... | Skipped by client | 2019/11/22 05... | admin | 2019/11/22 05... | On Demand | By Network | |
| ● TECHMONS... | Finished | 2019/11/21 06... | herculespopul... | 2019/11/21 06... | On Demand | By Network | Details |
| ● TECHMONS... | Finished | 2019/11/21 06... | herculespopul... | 2019/11/21 06... | On Demand | By Network | Details |

| TIME | STATUS | DISCOVERY TYPE | ADDITIONAL INFORMATION |
|---|---|---|---|
| 2019/11/21 06:29:01 AM | Finished | By Network | Devices discovered by this probe: 7<br>Click here to see list of devices discovered by this discovery |

- Click the 'Click here' link to view the devices found by the scan. See **Discovered Devices** for more details.

### Edit a Discovery Task

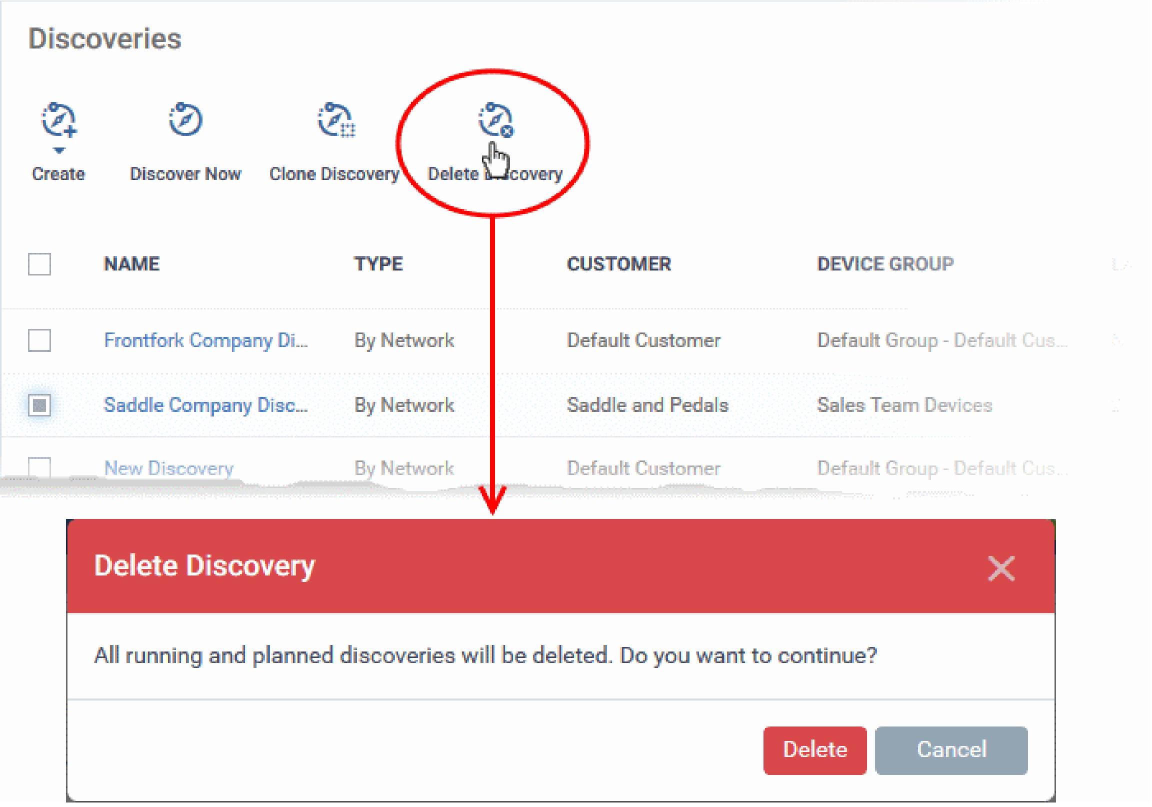
- Click 'Network Management' > 'Discoveries'
- Click the name of a discovery scan task to open its configuration interface
- Click the 'Edit' button on the right
- You can edit settings in the 'General', 'Auto Enrollment', 'Notifications' and 'Schedule' areas

- Edit the parameters as required. See the explanations of configuration screens of **network discovery task** and **AD discovery task** for more details.
- Click 'Save' to apply your changes

### Remove Discovery Tasks

Discovery scan tasks that are no longer required can be removed from Endpoint Manager

- Click 'Network Management' > 'Discoveries'
- Select the discovery task to be removed and click 'Delete Discovery' on the top
- Alternatively click the name of the discovery task and click 'Delete Discovery' on the top of the configuration screen



| □ | NAME | TYPE | CUSTOMER | DEVICE GROUP |
|---|---|---|---|---|
| □ | Frontfork Company Di... | By Network | Default Customer | Default Group - Default Cus... |
| ☑ | Saddle Company Disc... | By Network | Saddle and Pedals | Sales Team Devices |
| □ | New Discovery | By Network | Default Customer | Default Group - Default Cus... |

Delete Discovery

All running and planned discoveries will be deleted. Do you want to continue?

- Click 'Delete' in the confirmation dialog to remove the task.

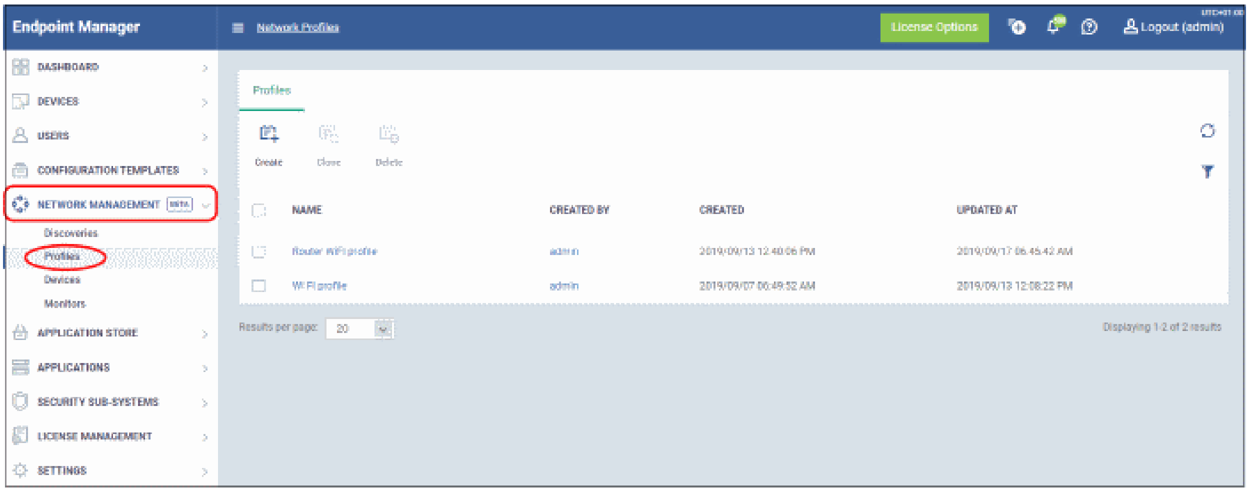
# 7.2. Manage Profiles for Network SNMP Devices

Click 'Network Management' > 'Profiles'

- Network profiles are used on SNMP compliant devices that don't run a supported operating system (Windows, Linux, iOS etc). Example devices include routers, switches and printers.
- The profiles let you track events on SNMP devices and receive alerts if certain conditions are met.
- You first create a monitor to track events, then you add the monitor to a network profile. You then deploy the profile to your SNMP devices.
  - You must have run at least one **discovery scan** to find your SNMP devices.
  - You should also have created at least one network monitor. See '**Manage Network Monitors**'

**Open the Network Profiles interface**

- Click 'Network Management' > 'Profiles'



| NAME | CREATED BY | CREATED | UPDATED AT |
|---|---|---|---|
| Router WiFi profile | admin | 2019/09/13 12:40:06 PM | 2019/09/17 06:45:42 AM |
| WiFi profile | admin | 2019/09/07 06:49:52 AM | 2019/09/13 12:08:22 PM |

Results per page: 20

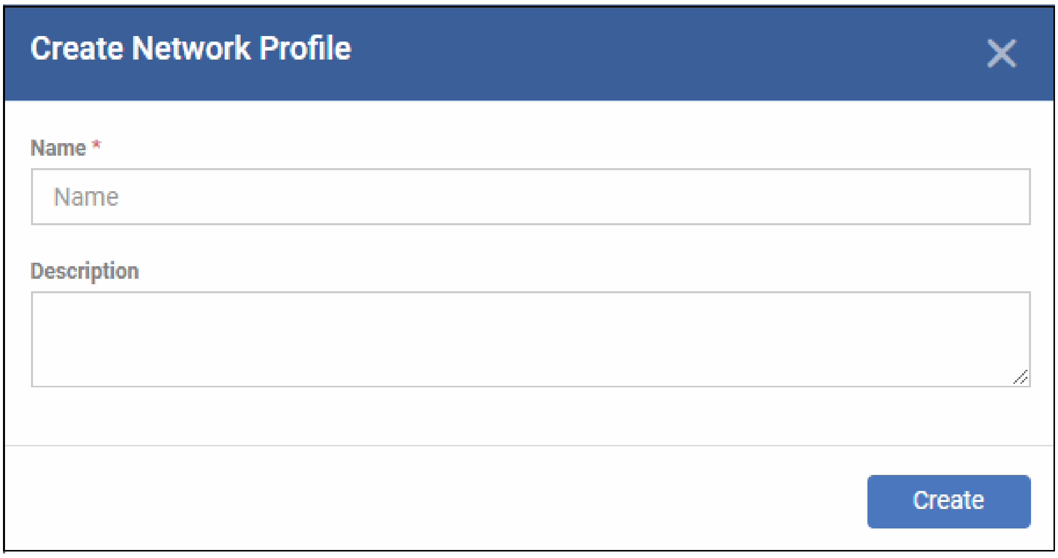
Displaying 1-2 of 2 results

Click the following links to learn more about each task:

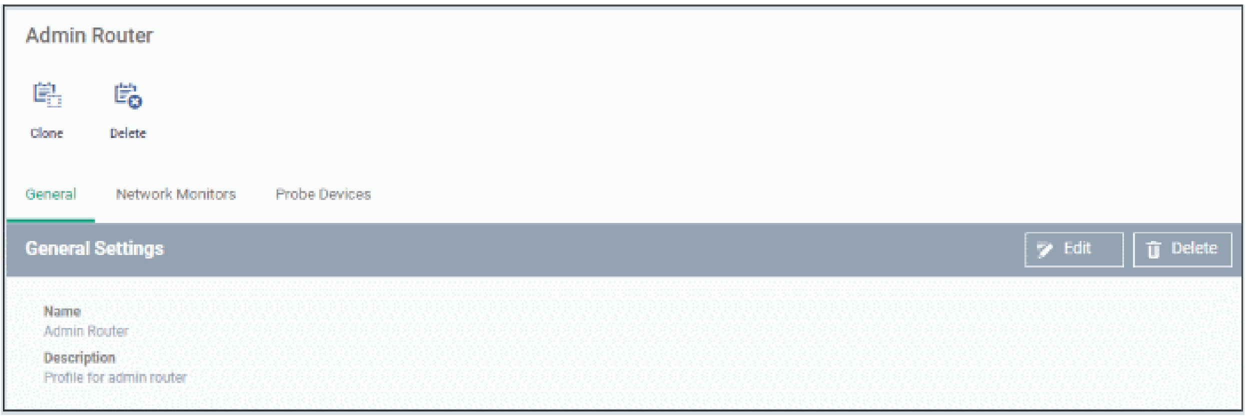
- **Create Network Profile**
- **Clone a Network Profile**
- **Delete a Network Profile**

## Create a Network Profile

- Click 'Network Management' > 'Profiles'
- Click 'Create' at top-left

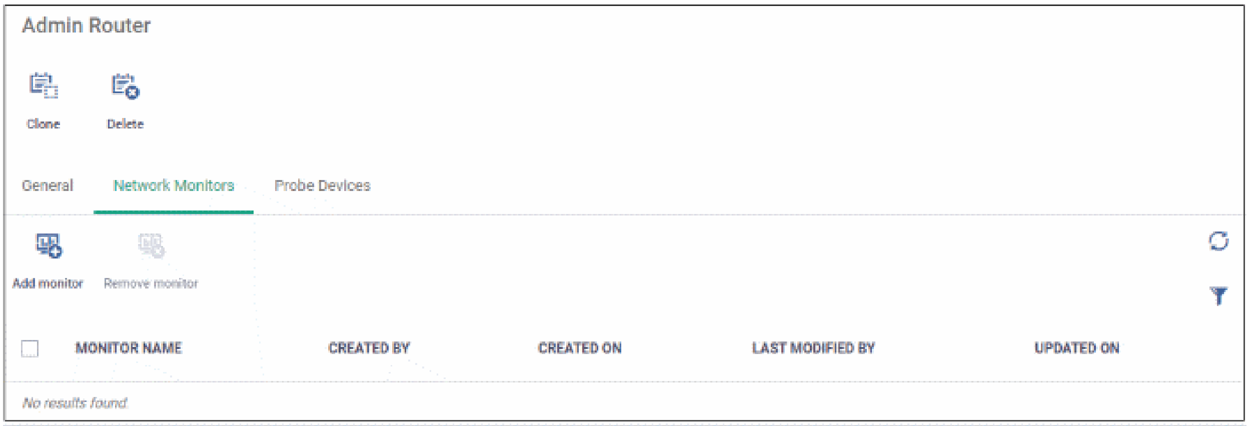


  - **Name -** Create a label for the profile. For example, 'Profile for routers'.
  - **Description-** Add any short notes you think are required.
- Click 'Create'. This opens the profile, ready for you to configure.
- Click 'Edit' on the right:



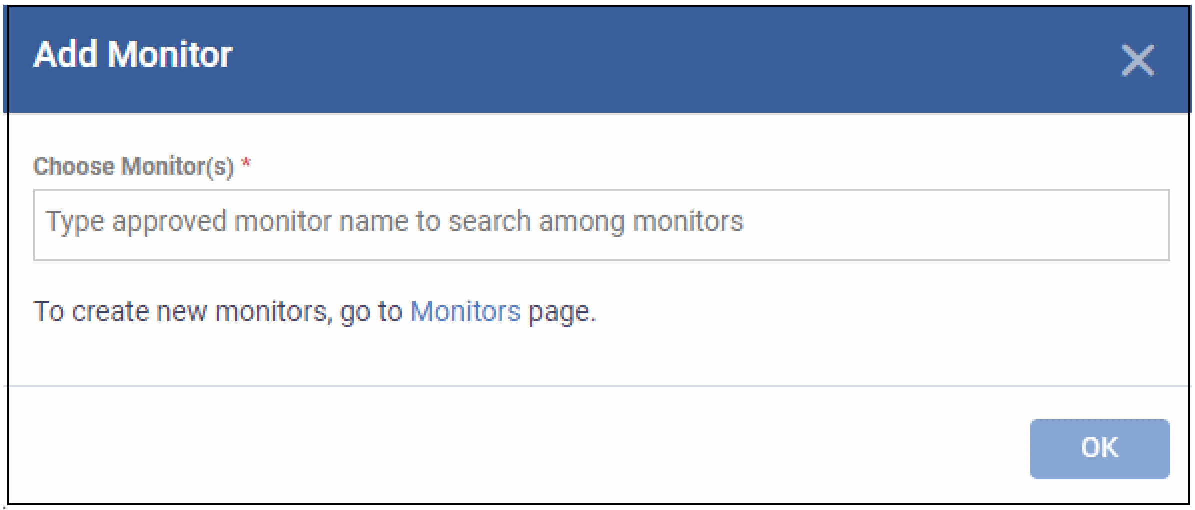
Name
Admin Router
Description
Profile for admin router

- Click the 'Network Monitors' tab:



| MONITOR NAME | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|
| No results found | | | | |

- Click 'Add monitor'
- A network monitor tracks activity on your devices and generate an alert if certain conditions are met.



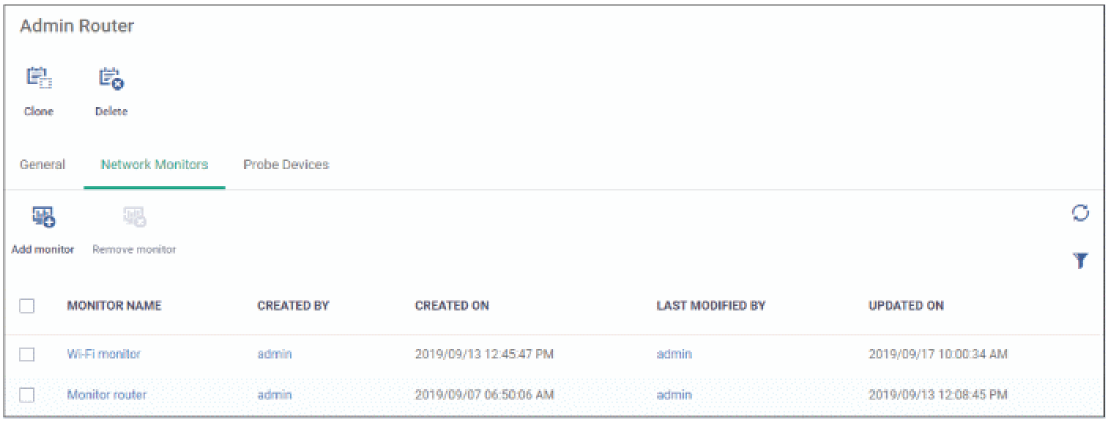
Choose Monitor(s) *

Type approved monitor name to search among monitors

To create new monitors, go to Monitors page.

- **Choose Monitors** - Start typing the monitor name and select from the suggestions. You can add multiple monitors.
  - See '**Manage Network Monitors**' if you have not yet saved a monitor.
- Click 'OK'

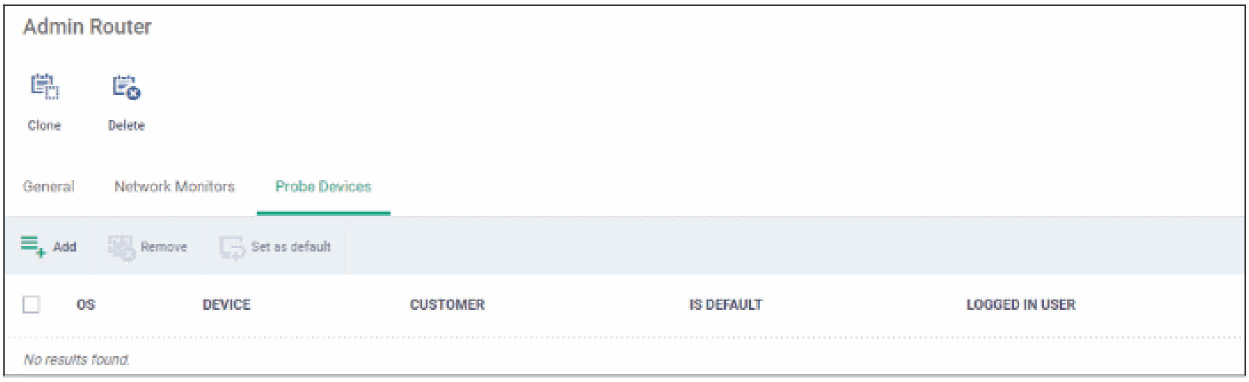
The page shows all monitors on the profile:



| □ | MONITOR NAME | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|
| □ | Wi-Fi monitor | admin | 2019/09/13 12:45:47 PM | admin | 2019/09/17 10:00:34 AM |
| □ | Monitor router | admin | 2019/09/07 06:50:06 AM | admin | 2019/09/13 12:08:45 PM |

- Click 'Probe Devices'
- Choose the device you want to use to keep track of SNMP devices.

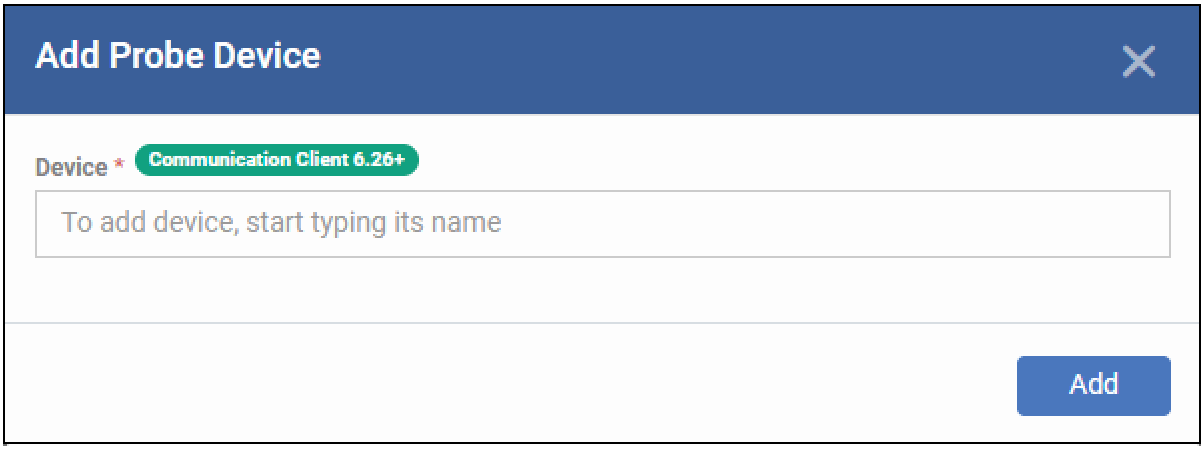
A probe device is a managed Windows endpoint inside your target network. The device must already be enrolled to Endpoint Manager and have the communication client installed. This device will run the monitors on your target SNMP devices.



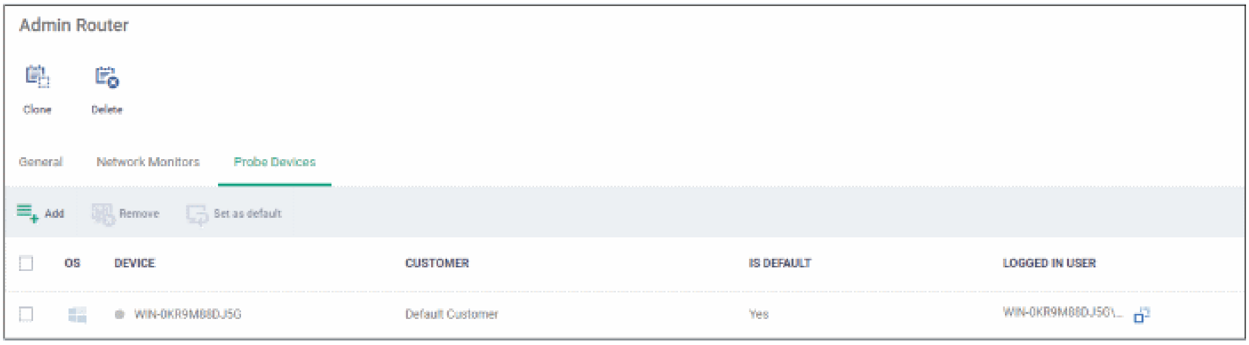
| □ | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|

No results found.

- Click 'Add'


Add Probe Device
Device *
Communication Client 6.26+
To add device, start typing its name
Add

- **Device** - Start typing the managed Windows device name and select from the suggestions.
- Click 'Add'



| □ | OS | DEVICE | CUSTOMER | IS DEFAULT | LOGGED IN USER |
|---|---|---|---|---|---|
| □ | | WIN-0KR9M88DJ5G | Default Customer | Yes | WIN-0KR9M88DJ5G\... |

- Repeat the process to add more probe devices. More devices act as fail-overs for each other.
- Note - The first device that you add will be default probe device. If you want to change, select the probe device and click 'Set as default'.

The profile is now configured. You can deploy the profile to discovered SNMP devices as follows:

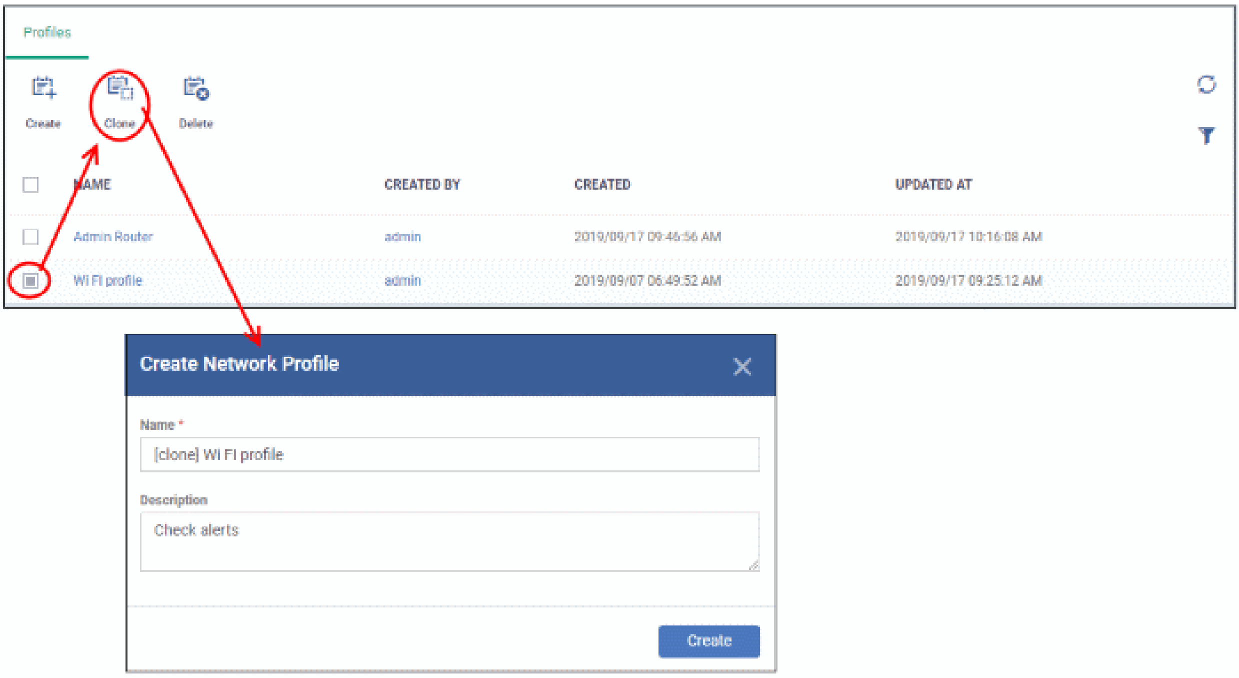
- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab
- Select your target SNMP devices
- Click 'Add Profile'
- Type the name of the profile you just created
- Click 'Add'

**Click here** for an illustrated walk-through of the profile deployment process.

## Clone a Network Profile

You can add a new profile by using the settings of an existing network profile.

- Click 'Network Management' > 'Profiles'
- Click 'Clone' at top-left



Profiles

| NAME | CREATED BY | CREATED | UPDATED AT |
|---|---|---|---|
| Admin Router | admin | 2019/09/17 09:46:56 AM | 2019/09/17 10:16:08 AM |
| Wi FI profile | admin | 2019/09/07 06:49:52 AM | 2019/09/17 09:25:12 AM |

Create Network Profile

Name * [clone] Wi FI profile

Description Check alerts

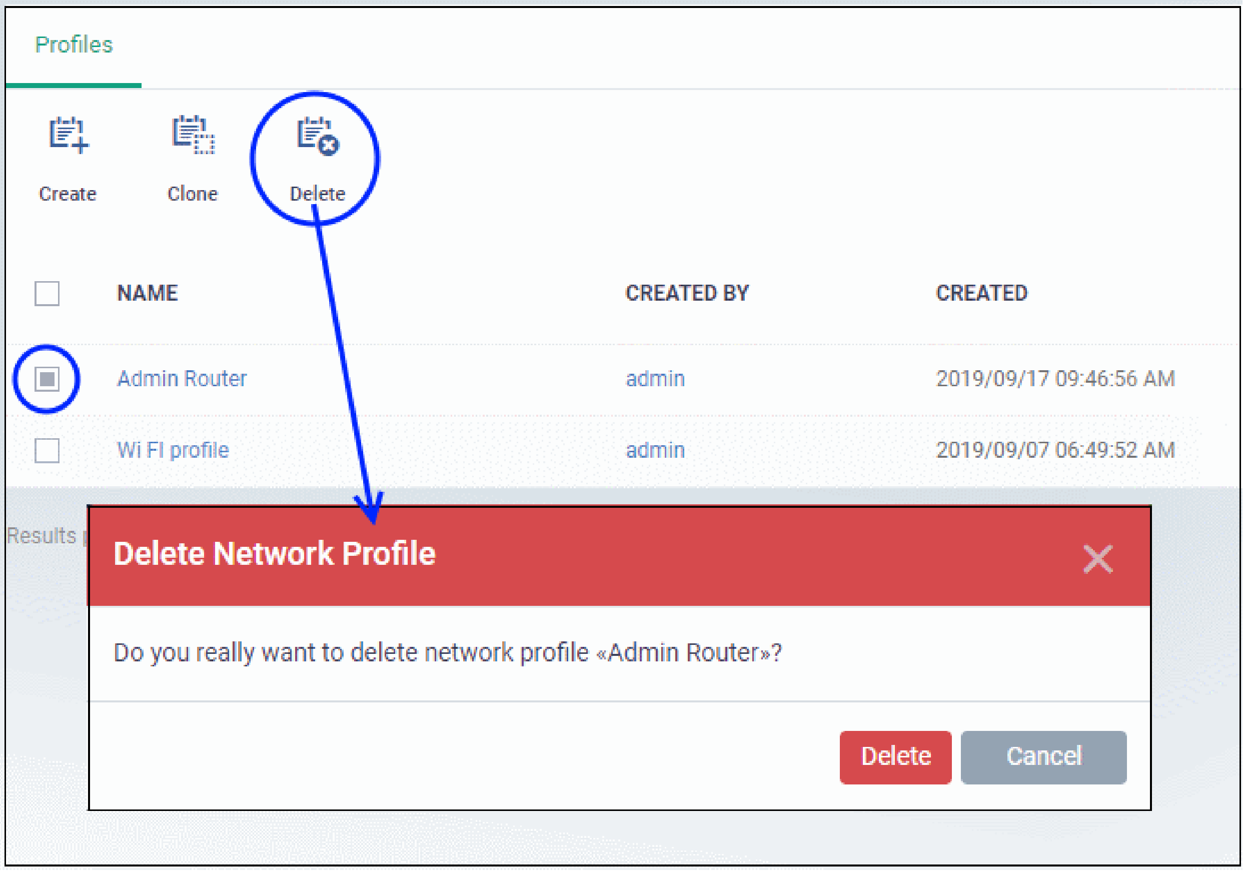
The cloning process is similar to creating a new profile explained above. Edit the settings as required.

**Click here** for an illustrated walk-through of the profile deployment process.

## Delete a Network Profile

You will no longer get alerts if a network profile is deleted.

- Click 'Network Management' > 'Profiles'
- Click 'Delete' at top-left



|  | NAME | CREATED BY | CREATED |
|---|---|---|---|
| ☐ | Admin Router | admin | 2019/09/17 09:46:56 AM |
| ☐ | Wi FI profile | admin | 2019/09/07 06:49:52 AM |

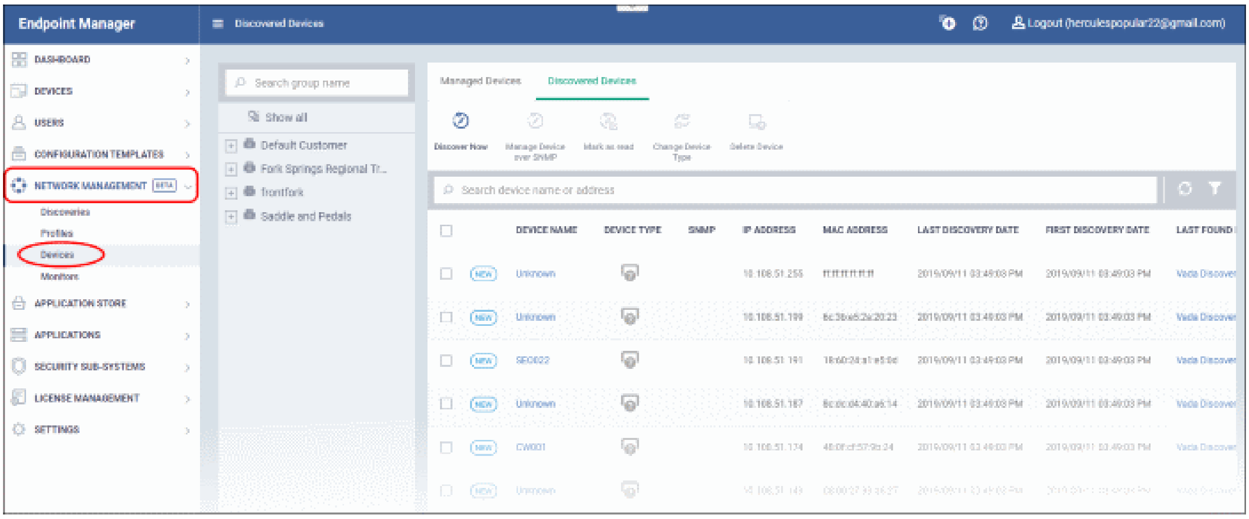
**Delete Network Profile** ✕

Do you really want to delete network profile «Admin Router»?

- Click 'Delete' to confirm

# 7.3. Manage Network Devices

- Click 'Network Management' > 'Devices'
- This interface lets you view the results of all discovery scans. You can also manage Simple Network Management Protocol (SNMP) compliant devices.
- **Managed devices tab -** Monitor and apply profiles to SNMP compliant devices
- **Discovered devices tab -** View all discovered devices. Select SNMP devices for management.



| ☐ |  | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISCOVERY DATE | LAST FOUND |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | NEW | Unknown |  |  | 10.108.51.255 | ff:ff:ff:ff:ff:ff | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:03 PM | Vada Discover |
| ☐ | NEW | Unknown |  |  | 10.108.51.199 | 6c:3b:e5:2a:20:23 | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:03 PM | Vada Discover |
| ☐ | NEW | SEO022 |  |  | 10.108.51.191 | 18:60:24:a1:e5:0e | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:03 PM | Vada Discover |
| ☐ | NEW | Unknown |  |  | 10.108.51.187 | 6c:dc:d4:40:a6:14 | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:03 PM | Vada Discover |
| ☐ | NEW | CW001 |  |  | 10.108.51.174 | 48:0f:cf:57:9b:24 | 2019/09/11 03:49:03 PM | 2019/09/11 03:49:03 PM | Vada Discover |
| ☐ | NEW | Unknown |  |  | 10.108.51.143 | 08:00:27:33:a6:27 | 2019/09/11 03:49:03 PM | [illegible] | [illegible] |

Click the following links for details:

- **Manage SNMP Devices**

- SNMP Device Details Interface
- Discovered Devices

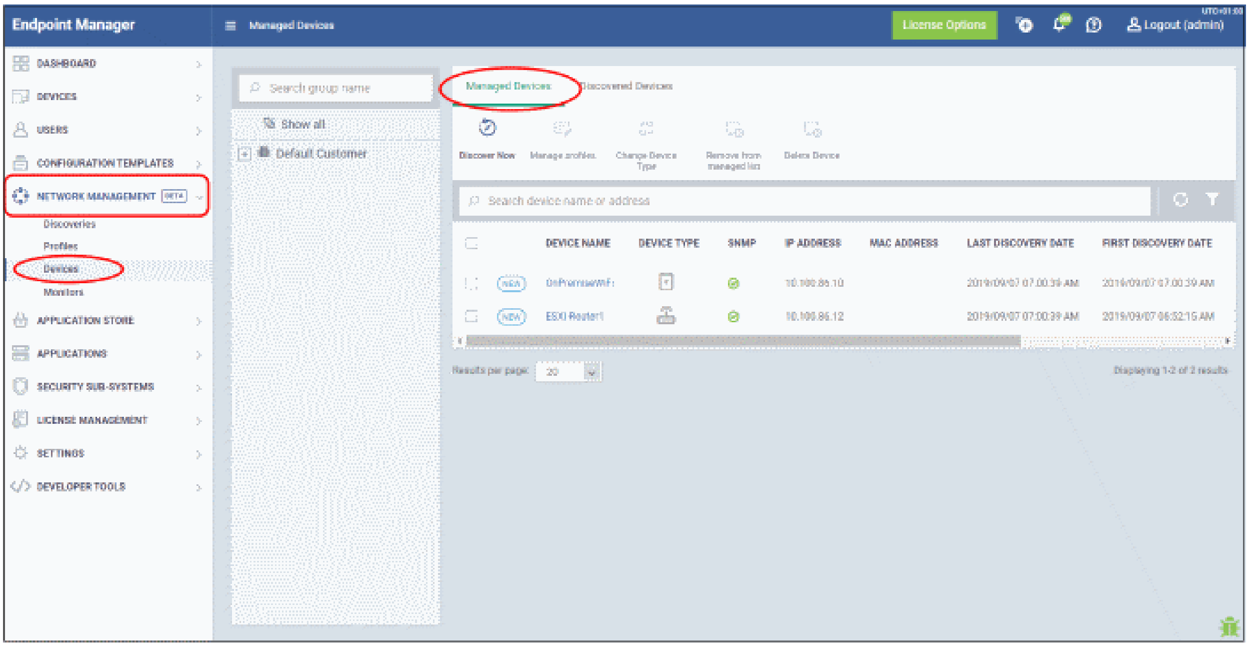
## 7.3.1. Manage SNMP Devices

- Click 'Network Management' > 'Devices' > 'Managed Devices'
- This area lets you apply network profiles to SNMP compliant devices.
- Network profiles provide limited management of devices that don't run a supported operating system (Windows, Linux, iOS etc). In other words, devices that you cannot apply a regular configuration profile to.
  - For example - routers, printers, switches, UPS devices, etc.

**Open the Managed Devices interface**

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
  - Select a company or a group to view managed SNMP devices assigned to that group

    Or
  - Select 'Show all' to view every managed SNMP device



| | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISCOVERY DATE |
|---|---|---|---|---|---|---|---|
| NEW | OnPremiseWiFi | | ✓ | 10.100.86.10 | | 2019/09/07 07:00:39 AM | 2019/09/07 07:00:39 AM |
| NEW | ESXI Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM | 2019/09/07 06:52:15 AM |

| Managed Devices - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Device Name | The label assigned to the device by the user.<br>• NEW - Endpoint Manager has not seen this device before. Click 'Mark as read' to remove this tag.<br>• Click a device name to open its details screen. |
| Device Type | The category to which the device belongs. For example, endpoint, router, printer and so on. The icon indicates the device's category. |
| SNMP | Shows whether the device responded to SNMP requests during the scan.<br>SNMP devices are usually items like routers, printers, switches etc. These devices don't run a supported operating system (Windows, Mac etc), so you cannot enroll them as you |

| | |
|---|---|
| | would a regular endpoint. |
| IP Address | The unique network address of the device |
| MAC Address | The address of the machine's network card |
| Last Discovery Date | Date and time the device was most recently identified |
| First Discovery Date | Date and time when the device was first identified |
| Last Found By | The discovery scan task that most recently identified the device<br>• Click the task name to view its details<br>• See **Create, Manage and Run Network Discovery Tasks** for more details on the discovery scan tasks |
| Customer | The company that owns/controls the target network. |
| Device Group | The device group to which the device belongs. |
| **Controls** | |
| Discover Now | Select a discovery scan task then click this button to run the associated discovery scan.<br>• See **Run a Discovery Scan** in '**Discovered Devices**' section for more details |
| Manage Profiles | Select a SNMP device and deploy profiles in order to monitor it.<br>• See **Deploy Profile on SNMP Device** |
| Change Device Type | Update device category type<br>• See '**Change Device Type**' in '**Discovered Devices**' section for more details |
| Remove from Managed List | Move the SNMP device back to Discovered Devices section. |
| Delete Device | Remove selected devices from the list |

- Use the funnel on the right to filter devices by name, customer, IP address and more.

The interface lets you:

- **Run a Discovery Scan**
- **Deploy Profile on SNMP Device**
- **Change Device Type**
- **Move SNMP Devices to Discovered Devices**
- **Remove SNMP Devices**

## Run a Discovery Scan

This task is same as described in the discovered devices section. **Click here** for help with this.

## Deploy Profiles on SNMP Device

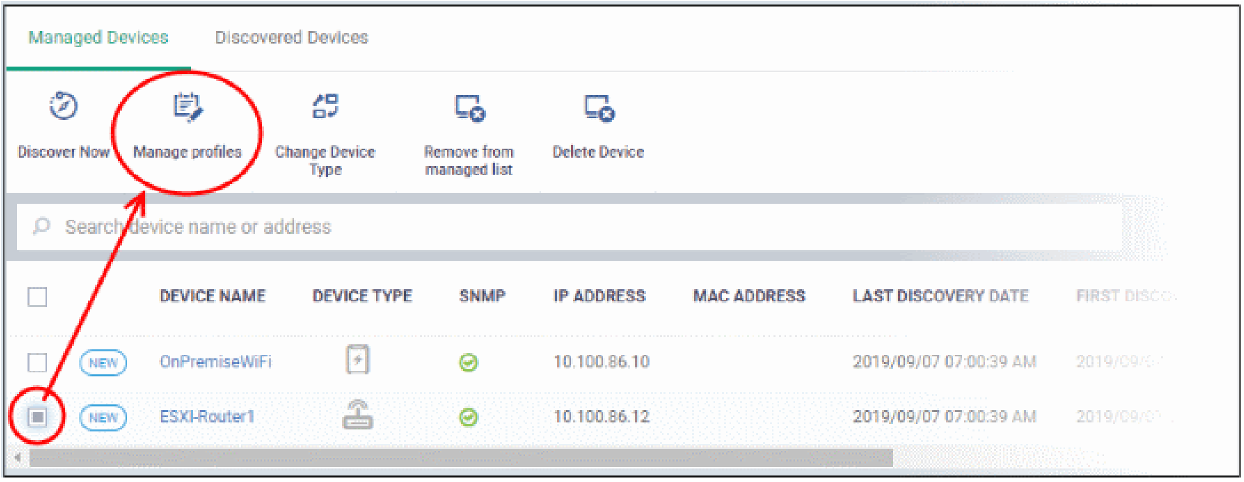
- Network profiles are created and managed in 'Network Management' > 'Profiles'. See **Manage Profiles for Network SNMP Profiles**
- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open

- Select a company or a group to view managed SNMP devices assigned to that group

  Or

- Select 'Show all' to view every managed SNMP device

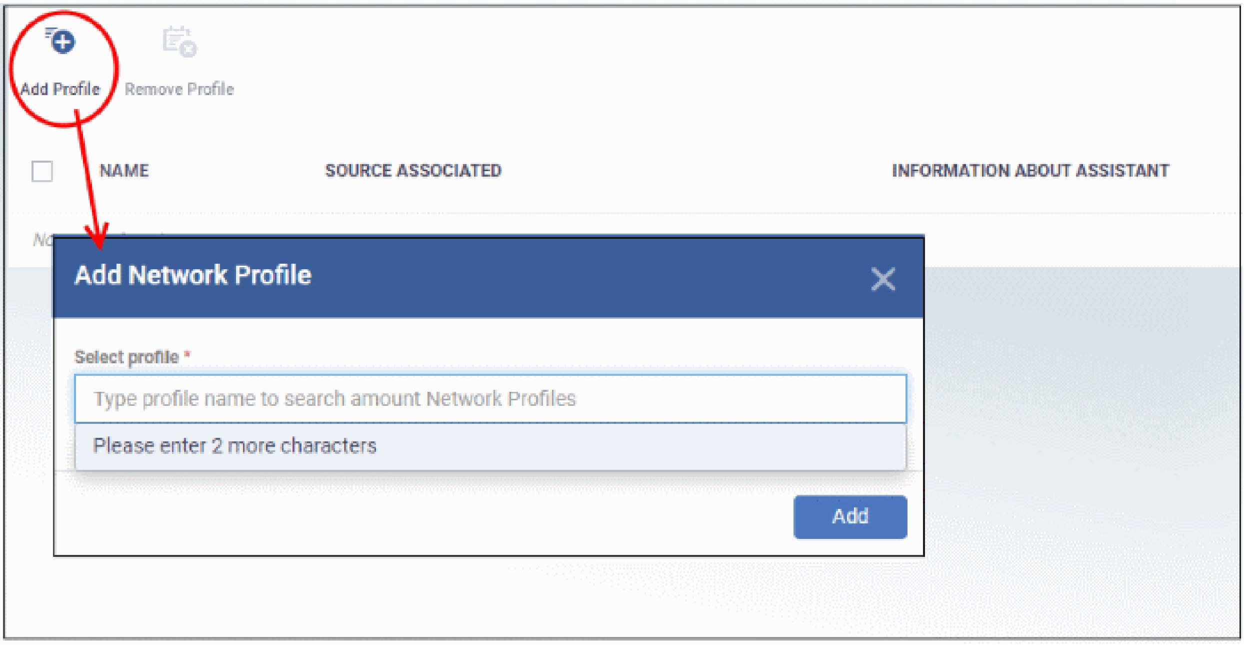
- Select the device and click 'Manage Profiles'



| ☐ | | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISCO... |
|---|---|---|---|---|---|---|---|---|
| ☐ | NEW | OnPremiseWiFi | | ✓ | 10.100.86.10 | | 2019/09/07 07:00:39 AM | 2019/09/... |
| ☑ | NEW | ESXI-Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM | 2019/09/... |

- Alternatively, click the device name then 'Manage Profiles' in the device details screen.

- Click 'Add Profile'



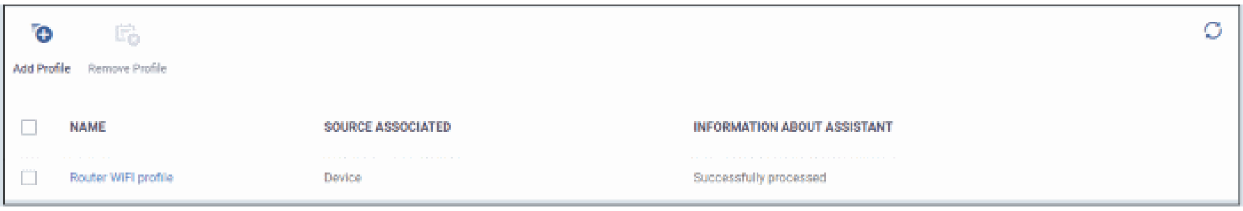
Select profile *

Type profile name to search amount Network Profiles

Please enter 2 more characters

- In the add network profile dialog, start typing the profile name and select from the suggestions.
- Click 'Add'

The profile is added to the selected device and confirmation message is shown:



| ☐ | NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSISTANT |
|---|---|---|---|
| ☐ | Router WIFI profile | Device | Successfully processed |

- Repeat the process to add more profiles, if required.
- Clicking a profile name will take you to the profile details screen.
- To remove a profile, select it and click 'Remove Profile'

## Change Device Type

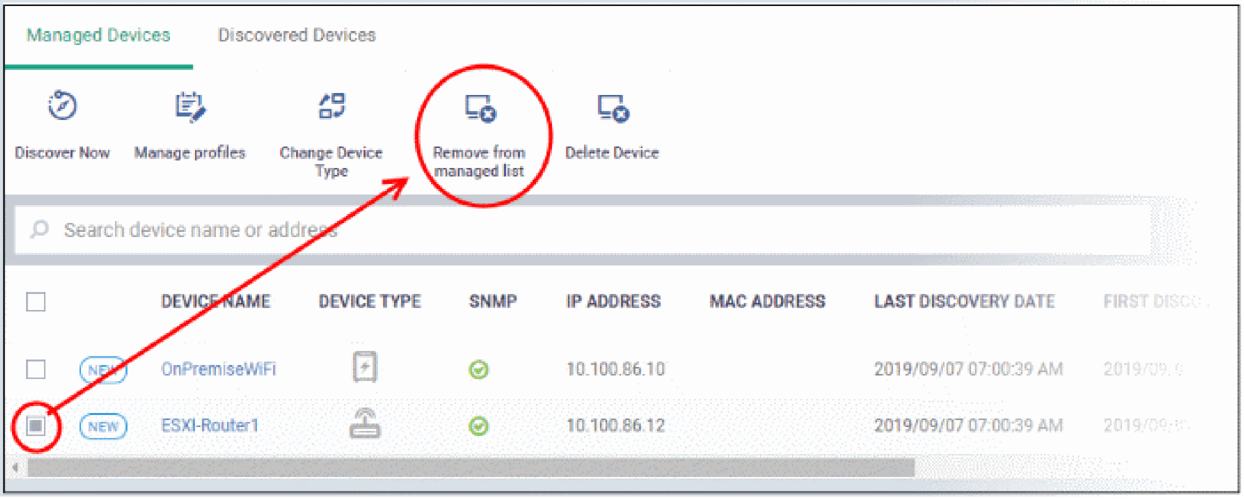
This task is same as described in the discovered devices section. **Click here** for help with this.

## Move SNMP Devices to Discovered Devices

You can move SNMP devices back to discovered devices if required. Note - Profiles associated with the SNMP device is removed if you move it to discovered devices section.

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
  - Select a company or a group to view managed SNMP devices assigned to that group

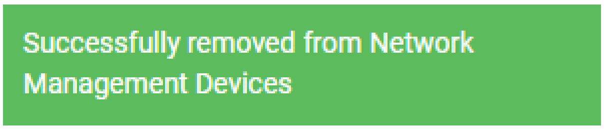
    Or
  - Select 'Show all' to view every managed SNMP device
- Select a device and click 'Remove from managed list'



| ☐ | | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISC |
|---|---|---|---|---|---|---|---|---|
| ☐ | NEW | OnPremiseWiFi | | ✓ | 10.100.86.10 | | 2019/09/07 07:00:39 AM | 2019/09 |
| ☑ | NEW | ESXI-Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM | 2019/09 |

- Alternatively, click the device name then 'Remove from managed list' in the device details screen.

A confirmation message is shown:


Successfully removed from Network Management Devices

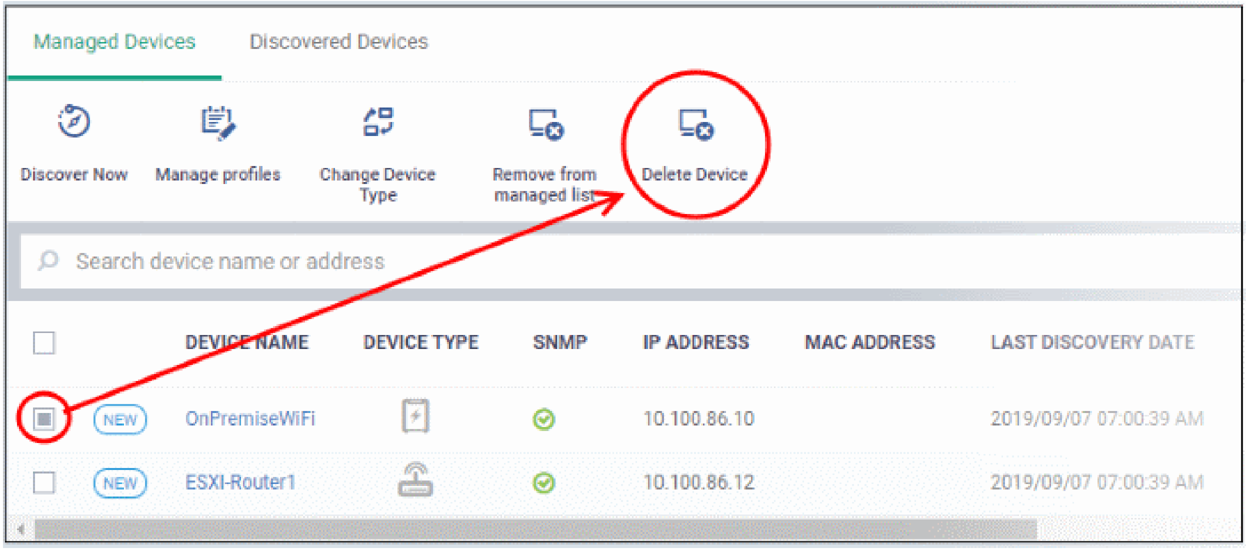
## Remove SNMP Devices

If you delete a device from the managed devices interface, it will be removed from this screen and also from the discovered devices section. It will be however added to discovered devices screen during the next discovery scan.

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
  - Select a company or a group to view managed SNMP devices assigned to that group

    Or
  - Select 'Show all' to view every managed SNMP device

- Select a device and click 'Delete Device'



| □ | | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE |
|---|---|---|---|---|---|---|---|
| ■ | NEW | OnPremiseWiFi | | ✓ | 10.100.86.10 | | 2019/09/07 07:00:39 AM |
| □ | NEW | ESXI-Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM |

- Alternatively, click the device name then 'Delete Device' in the device details screen.

A confirmation message is shown.

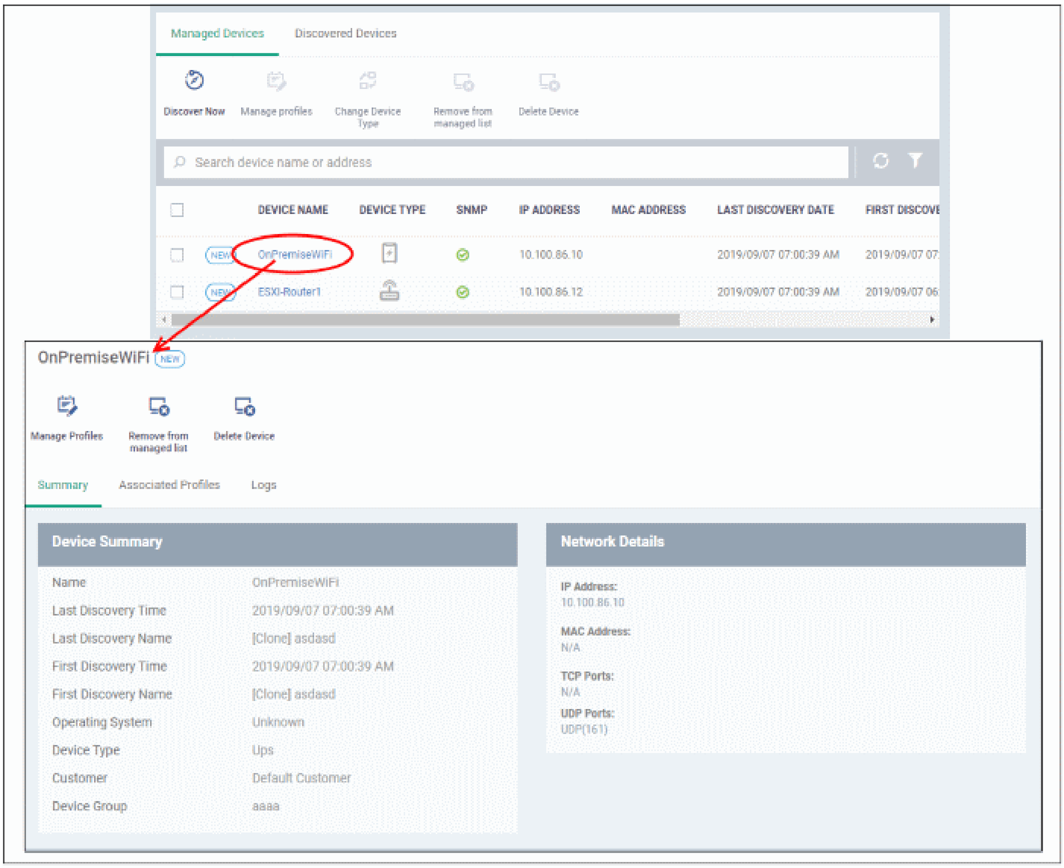
## 7.3.1.1. SNMP Device Details Interface

- The device details page lets you view an SNMP device's hardware and software, profiles, and event logs.
- You can also manage profiles, remove it from the managed list, and delete the device.

**Open SNMP Device Details**

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
    - Select a company or a group to view managed SNMP devices assigned to that group

      Or
    - Select 'Show all' to view every managed SNMP device
- Click the name of any SNMP device to view its details:



| □ | | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISCOVE |
|---|---|---|---|---|---|---|---|---|
| □ | NEW | OnPremiseWiFi | | ✓ | 10.100.86.10 | | 2019/09/07 07:00:39 AM | 2019/09/07 07: |
| □ | NEW | ESXI-Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM | 2019/09/07 06 |

Device Summary

| | |
|---|---|
| Name | OnPremiseWiFi |
| Last Discovery Time | 2019/09/07 07:00:39 AM |
| Last Discovery Name | [Clone] asdasd |
| First Discovery Time | 2019/09/07 07:00:39 AM |
| First Discovery Name | [Clone] asdasd |
| Operating System | Unknown |
| Device Type | Ups |
| Customer | Default Customer |
| Device Group | aaaa |

Network Details

IP Address:
10.100.86.10

MAC Address:
N/A

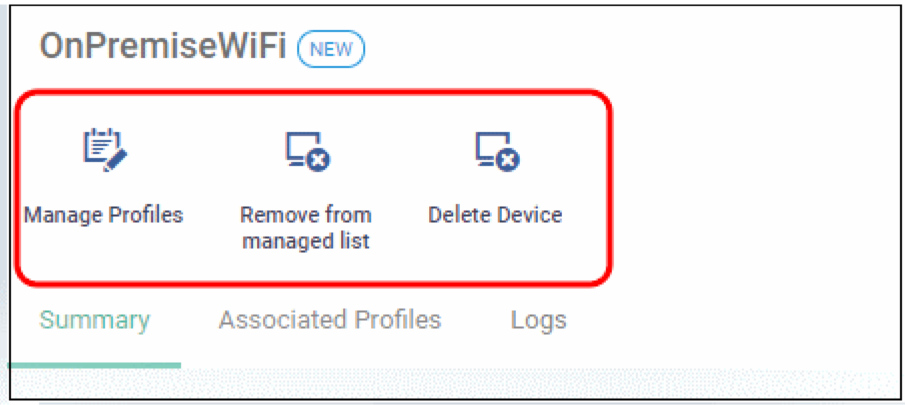
TCP Ports:
N/A

UDP Ports:
UDP(161)

The details screen contains three tabs:

- **Summary** - General hardware and network details.
- **Associated Profiles** - Network profiles deployed on the device.
- **Logs** - Device event logs

The buttons above the table let you perform various tasks:



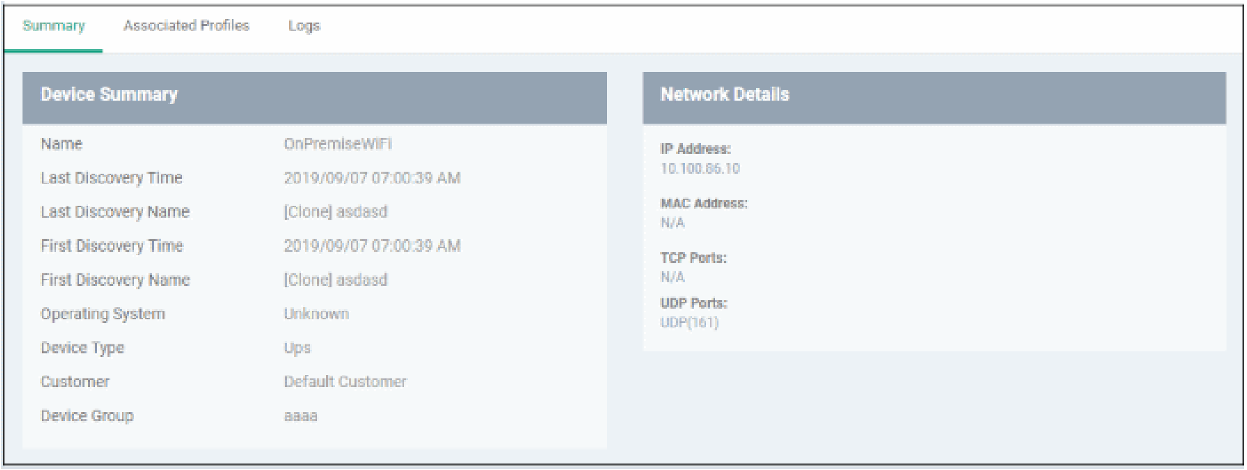
- **Manage Profiles -** Add / remove network profiles to / from the SNMP device. See **Deploy Profile on SNMP Device**
- **Remove from managed list -** The device is moved back to the 'Discovered Devices' section.. See **Move SNMP Devices to Discovered Devices**
- **Delete Device -** The SNMP device is removed from the list. See **Remove SNMP Devices**

## SNMP Device Summary

The summary page contains general information about the device. This includes IP / MAC address, discovery times, and device type.

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
    - Select a company or a group to view managed SNMP devices assigned to that group

      Or
    - Select 'Show all' to view every managed SNMP device
- Click the name of any SNMP device to open its details pane:



Device Summary

| | |
|---|---|
| Name | OnPremiseWiFi |
| Last Discovery Time | 2019/09/07 07:00:39 AM |
| Last Discovery Name | [Clone] asdasd |
| First Discovery Time | 2019/09/07 07:00:39 AM |
| First Discovery Name | [Clone] asdasd |
| Operating System | Unknown |
| Device Type | Ups |
| Customer | Default Customer |
| Device Group | aaaa |

Network Details

IP Address:
10.100.86.10

MAC Address:
N/A

TCP Ports:
N/A

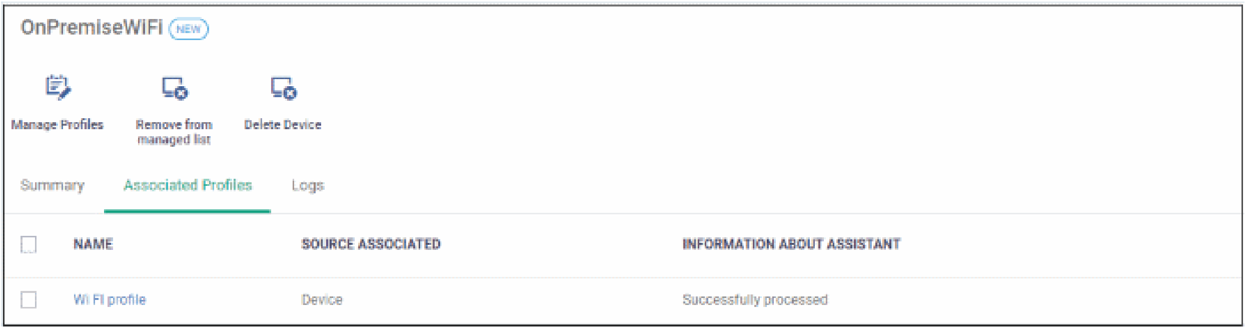
UDP Ports:
UDP(161)

## Manage Profiles Associated with the Device

The profile tab shows all profiles which have been applied to the device. Profiles contain **monitors** which track events on the device and alert you when certain conditions are met. For example, you can set up a monitor to alert you if a device has been switched off for a certain length of time.

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
    - Select a company or a group to view managed SNMP devices assigned to that group

      Or
    - Select 'Show all' to view every managed SNMP device
- Click the name of any SNMP device to open its details pane
- Click 'Associated Profiles':



| ☐ | NAME | SOURCE ASSOCIATED | INFORMATION ABOUT ASSISTANT |
|---|---|---|---|
| ☐ | Wi Fi profile | Device | Successfully processed |

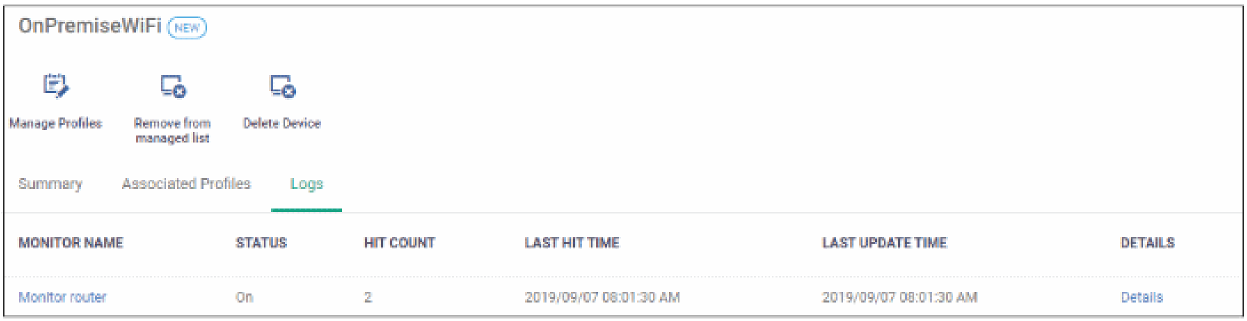
| SNMP Device's Associated Profiles - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | Label of the profile.<br>• Click the profile name to view and edit it. See **Create a Network Profile**. |
| Source Associated | The type of object to which the profile is applied. This column will always say 'Device' for SNMP profiles. |
| Information about Association | The current status of profile deployment. For example, successfully processed, deployment failed, etc. |

## SNMP Device Event Logs

The logs tab shows all activity on a specific SNMP device.

- Click 'Network Management' > 'Devices'
- Click the 'Managed Devices' tab if not already open
  - Select a company or a group to view managed SNMP devices assigned to that group

    Or
  - Select 'Show all' to view every managed SNMP device
- Click the name of any SNMP device to open its details pane then click 'Logs' tab



| MONITOR NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| Monitor router | On | 2 | 2019/09/07 08:01:30 AM | 2019/09/07 08:01:30 AM | Details |

| SNMP Device Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The monitor that recorded the event. |

| | |
|---|---|
| | • Click the name of the network monitor to open its details interface. See '**View Monitor Details**' |
| Status | Whether or not the monitor is currently active on the device |
| Hit Count | Number of times the monitor's conditions have been triggered. |
| Last Hit Time | Date and time the monitor's conditions were most recently triggered. |
| Last Update Time | Date and time when the information was last refreshed |
| Details | • View a log of the breach events<br>• This is similar to network monitor logs except here it shows logs associated with the device. See **View Details of Network Monitor Logs** for more information |

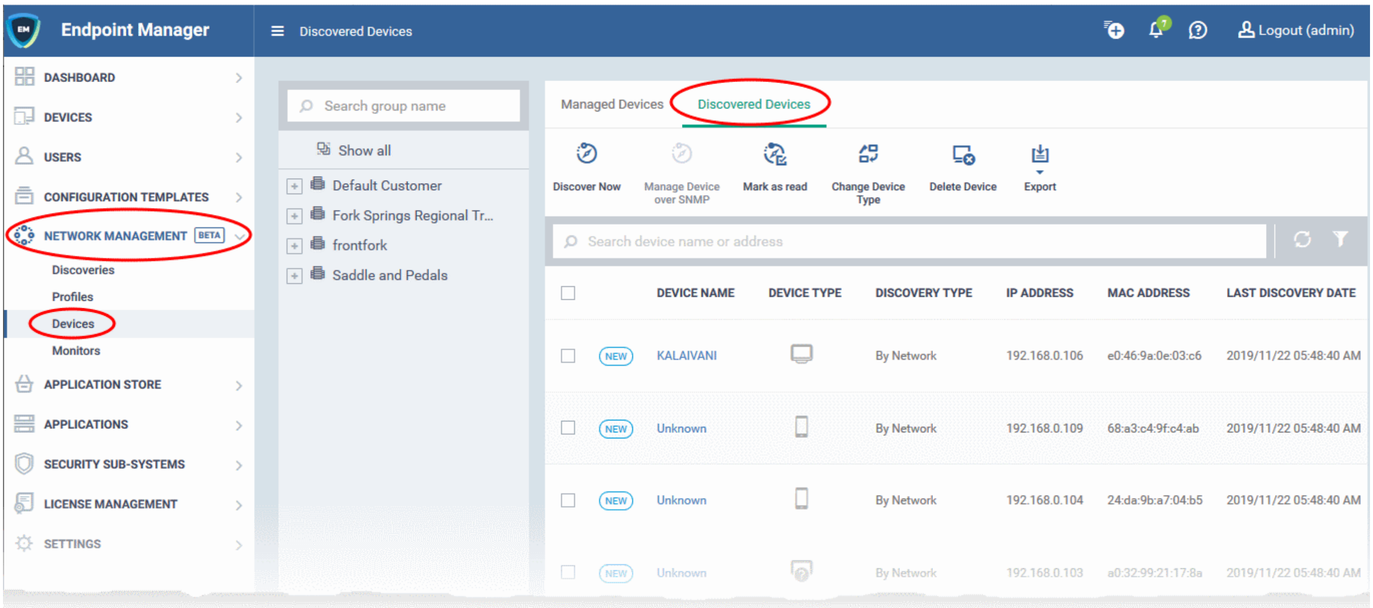
## 7.3.2. Discovered Devices

- Click 'Network Management' > 'Devices' > 'Discovered Devices'
- This is the results screen for devices found by the discovery scans. Discovery scans help identify all devices connected to a specific IP range or AD domain.
- You can configure and run a discovery scan in 'Network Management' > 'Discoveries'. **Click here** if you want help on this.

### Open Discovered Devices

- Click 'Network Management' > 'Devices' > 'Discovered Devices'
    - Select a company or a group to view discovered devices assigned to that group

      Or
    - Select 'Show all' to view every discovered device



| □ | | DEVICE NAME | DEVICE TYPE | DISCOVERY TYPE | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE |
|---|---|---|---|---|---|---|---|
| □ | NEW | KALAIVANI | | By Network | 192.168.0.106 | e0:46:9a:0e:03:c6 | 2019/11/22 05:48:40 AM |
| □ | NEW | Unknown | | By Network | 192.168.0.109 | 68:a3:c4:9f:c4:ab | 2019/11/22 05:48:40 AM |
| □ | NEW | Unknown | | By Network | 192.168.0.104 | 24:da:9b:a7:04:b5 | 2019/11/22 05:48:40 AM |
| □ | NEW | Unknown | | By Network | 192.168.0.103 | a0:32:99:21:17:8a | 2019/11/22 05:48:40 AM |

| Column Heading | Description |
|---|---|
| Device Name | The label assigned to the device by the user.<br>• NEW - Endpoint Manager has not seen this device before. 'New' devices can |

| | |
|---|---|
| | be enrolled to EM if required.<br>• Alternatively, select the device and click 'Manage Device over SNMP' if it is a printer, router etc.<br>• Select a device and click 'Mark as read' to remove the 'New' tag.<br>• Click a device name to open its details screen. |
| Device Type | The category to which the device belongs. For example, endpoint, router, printer and so on. The icon indicates the device's category. |
| Discovery Type | The kind of discovery scan by which the device was identified. The possible types are:<br>• Active Directory<br>• Network<br>• SNMP |
| IP Address | The unique network address of the device |
| MAC Address | The address of the machine's network card |
| Last Discovery Date | Date and time the device was most recently identified |
| First Discovery Date | Date and time when the device was first identified |
| Last Found By | The discovery scan task that most recently identified the device<br>• Click the task name to view its details<br>• See **Create, Manage and Run Network Discovery Tasks** for more details on the discovery scan tasks |
| Customer | The company that owns/controls the target network. |
| Device Group | The group to which the device is assigned. |
| **Controls** | |
| Discover Now | Select a discovery scan task then click this button to run the associated discovery scan.<br>• See **Run a Discovery Scan** for more details |
| Manage Device over SNMP | Select a SNMP device and move to 'Managed Devices' for applying network profiles.<br>• See '**Move SNMP Devices for Management**' |
| Mark as read | Removes the 'New' status of selected devices<br>• See **Mark Recognized Devices as Known Devices** for more details |
| Change Device Type | Update device category type<br>• See '**Change Device Type**' |
| Delete Device | Remove selected devices from the list |

- Use the funnel on the right to filter devices by name, customer, IP address and more.

The interface lets you:

- **Run a Discovery Scan**
- **Move SNMP Devices for Management**
- **Mark Recognized Devices as Known Devices**

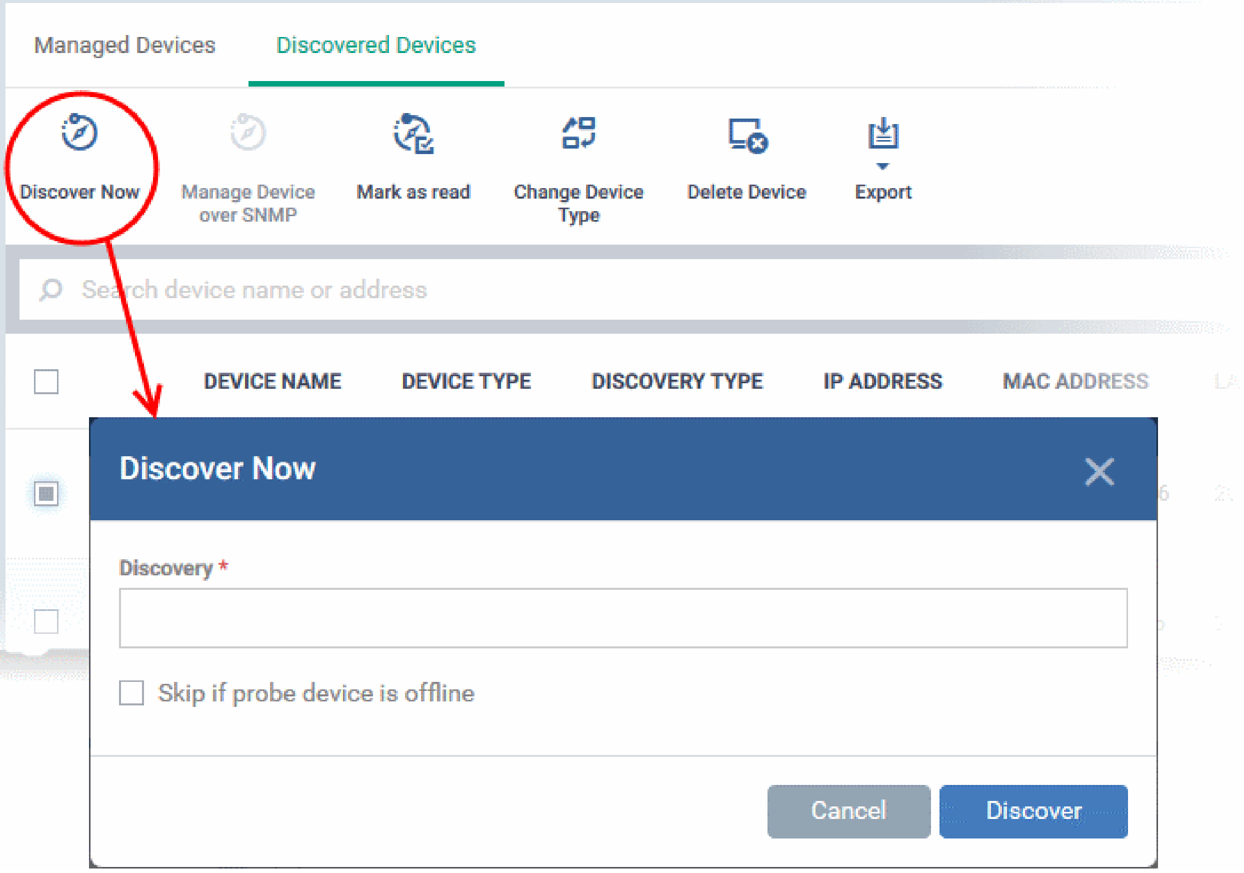
- Change Device Type
- Remove Selected Devices

## Run a Discovery Scan

- Discovery scans are configured and run in 'Network Management' > 'Discoveries'. Chapter 7.1 covers this in more detail.
- You can also run existing scans from the results screen ('Network Management' > 'Devices' > 'Discovered Devices')

### Run a scan

- Click 'Network Management' > 'Devices'
- Click the 'Discovered Devices' tab
- Click the 'Discover Now' button above the table



- **Discovery -** Select the pre-configured discovery task you want to run.
  - Enter the first few letters of the scan name and select from the suggestions
- **Skip if probe device is offline -** The scan will be aborted if all probe devices are offline.
  - The command is queued if this option is not selected. The scan will start once the probe device comes online.
- Click 'Discover' to run the scan. The scan will run for ten minutes and report all discovered devices found at the end of this period. If selected, the SNMP scan will run simultaneously.
- You can see discovered devices in 'Network Management' > 'Devices' > 'Discovered Devices'.
- Results include SNMP, managed and unmanaged devices. Managed devices = already enrolled to Endpoint Manager. Unmanaged = not enrolled to Endpoint Manager.

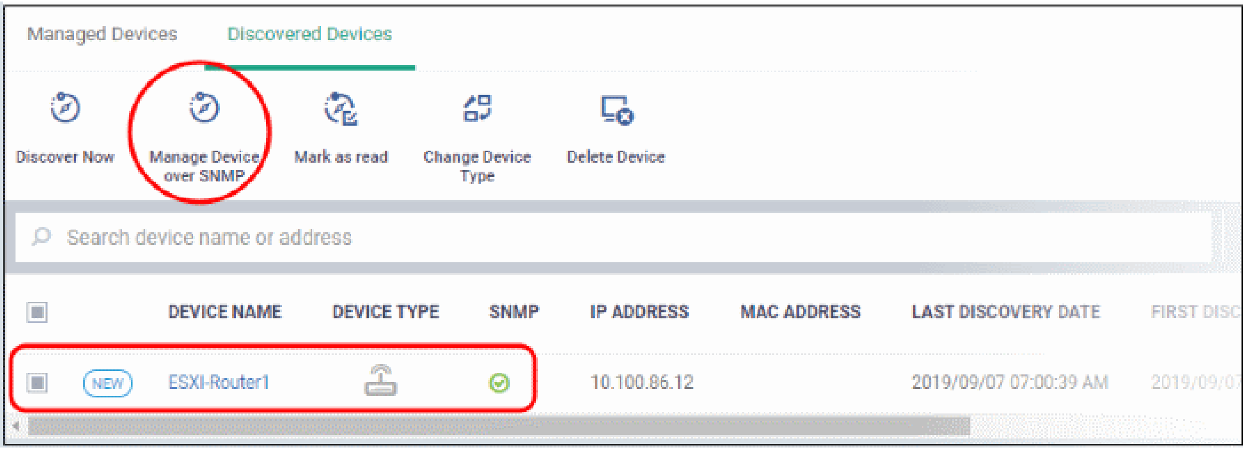
## Manage SNMP Devices

- Endpoint Manager is capable of detecting SNMP devices in a discovery scan. You should have enabled SNMP detection when setting up the network scan.
- The SNMP feature provides simple management of devices which don't run a supported operating system (Windows, Mac, Linux etc). SNMP devices are usually items like UPS, printers, routers, switches etc.
- You can apply a simple network profile to these devices which alerts you if the device has been powered on or off for a certain period of time.
  - See **Manage Profiles for Network SNMP Devices** for more on this.

**Move SNMP devices to management**

- Click 'Network Management' > 'Devices'
- Click the 'Discovered Devices' tab
  - Select a company or a group to view the list of devices identified in that group

    Or
  - Select 'Show all' to view every discovered device
- Select an SNMP compliant device then click 'Manage Device over SNMP'



| | | DEVICE NAME | DEVICE TYPE | SNMP | IP ADDRESS | MAC ADDRESS | LAST DISCOVERY DATE | FIRST DISC |
|---|---|---|---|---|---|---|---|---|
| □ | NEW | ESXI-Router1 | | ✓ | 10.100.86.12 | | 2019/09/07 07:00:39 AM | 2019/09/0 |

- You can move one device at a time
- A confirmation message is shown:

Successfully added to Network Management Devices

## Mark Recognized Devices as Known Devices

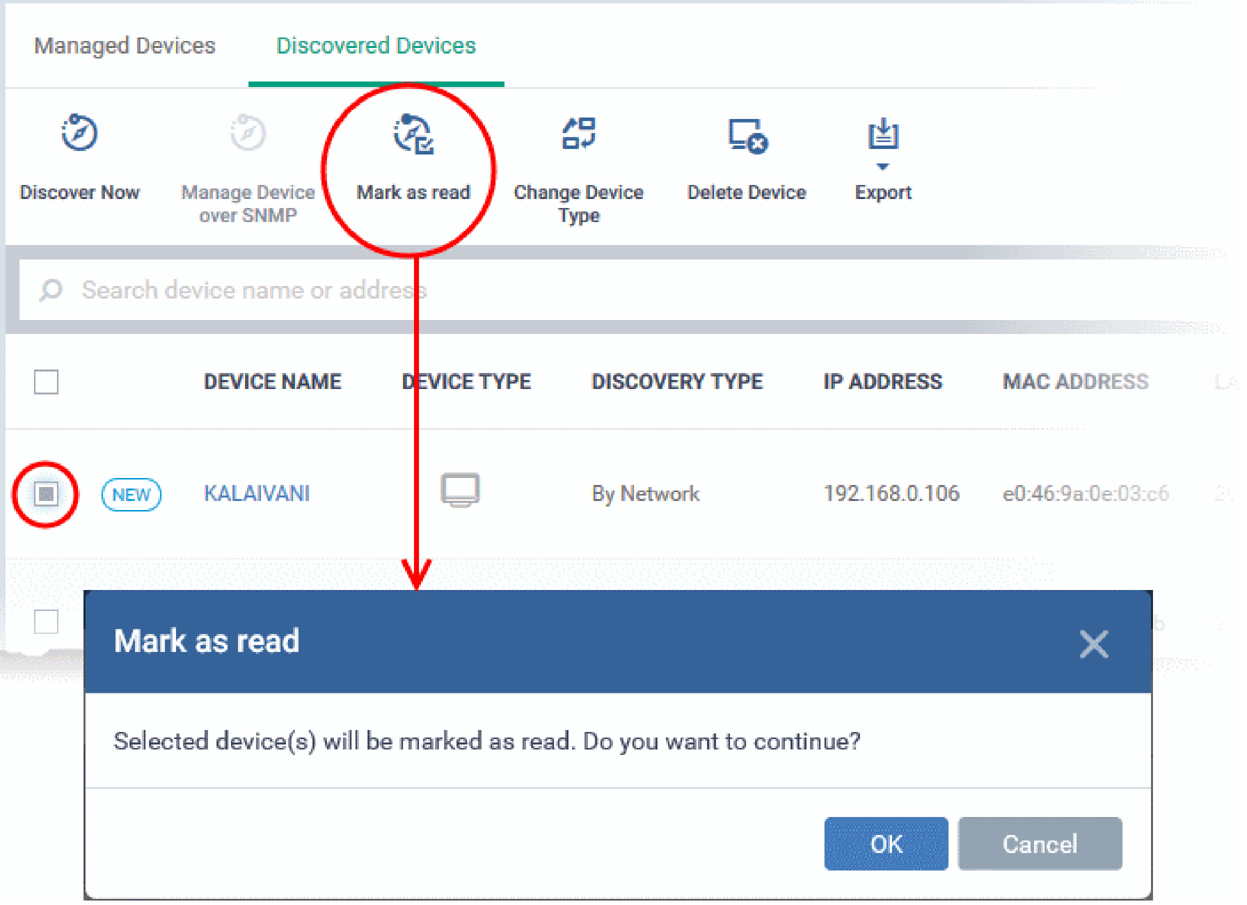
- Unmanaged devices identified for the first time are marked 'New'.
  - You can enroll discovered devices to Endpoint Manager. See **Example Deployment Process** in **chapter 7.1** for a quick guide on this.
  - After enrolling devices you may want to remove the 'New' tag.
  - If you remove the 'New' tag the device will not be flagged as new in subsequent scans.

**Mark new devices as known**

- Click 'Network Management' > 'Devices'
- Click the 'Discovered Devices' tab

- Select a company or a group to view the list of devices identified in that group
  Or
- Select 'Show all' to view every discovered device

- Select the new devices that are to be marked as known devices and click 'Mark as read'.



| | | DEVICE NAME | DEVICE TYPE | DISCOVERY TYPE | IP ADDRESS | MAC ADDRESS |
|---|---|---|---|---|---|---|
| ☒ | NEW | KALAIVANI | | By Network | 192.168.0.106 | e0:46:9a:0e:03:c6 |

Mark as read

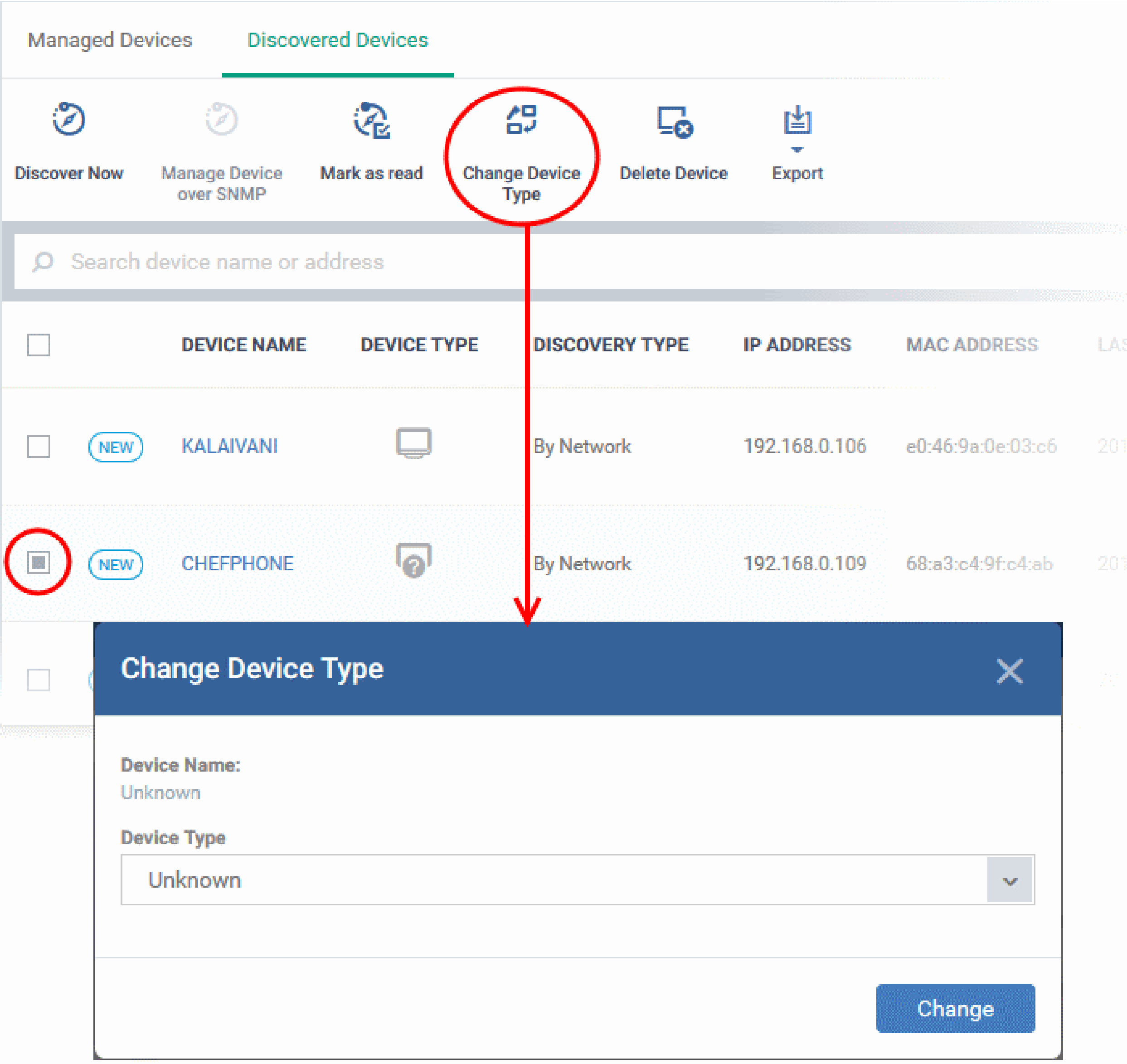
Selected device(s) will be marked as read. Do you want to continue?

- Click 'OK' in the confirmation dialog. The 'New' tag NEW beside the device will disappear

## Change Device Type

You can change the device category in case it was detected incorrectly after a scan.

- Click 'Network Management' > 'Devices'
- Click the 'Discovered Devices' tab
  - Select a company or a group to view the list of devices identified in that group
    Or
  - Select 'Show all' to view every discovered device
- Select the devices that you want to change the category



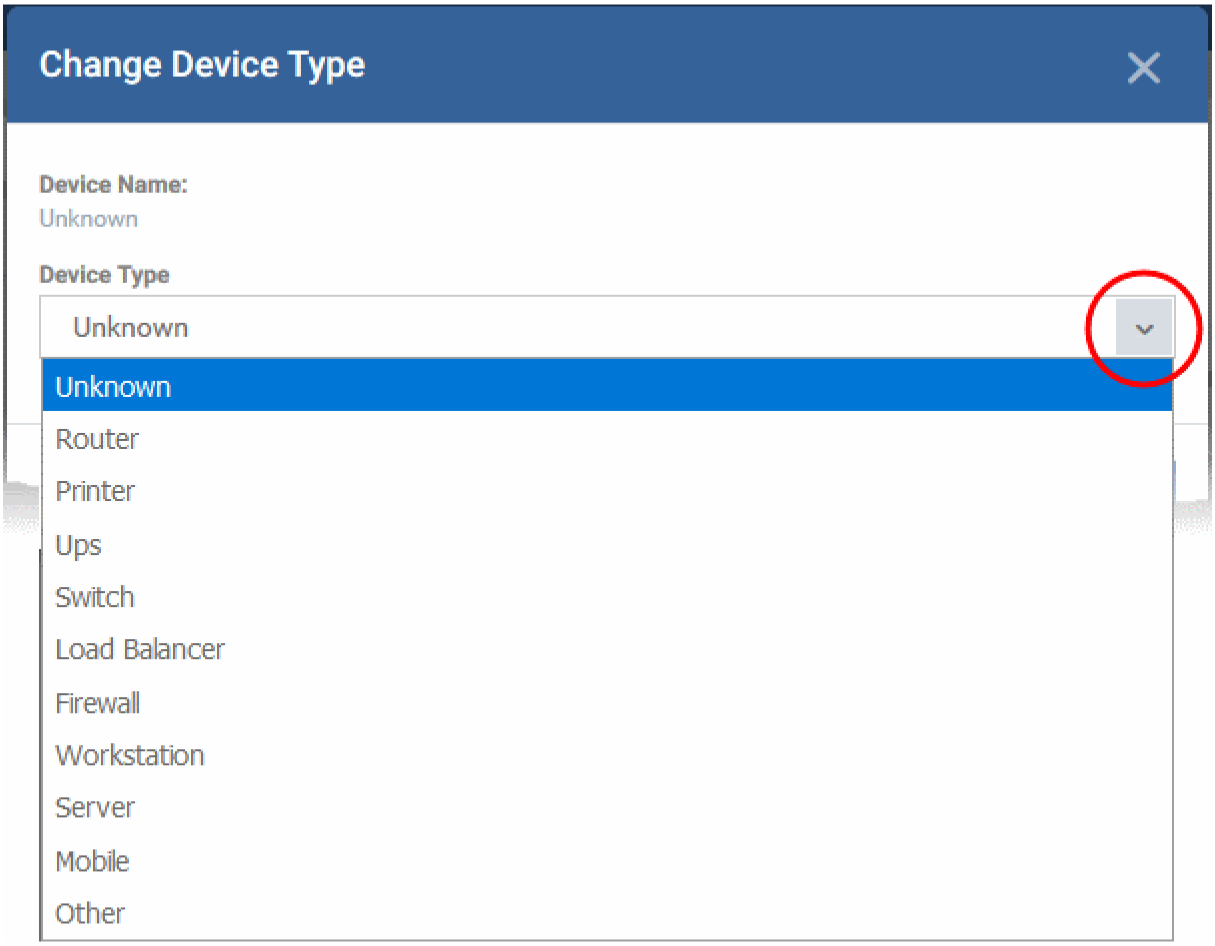
| □ | | DEVICE NAME | DEVICE TYPE | DISCOVERY TYPE | IP ADDRESS | MAC ADDRESS | LAS |
|---|---|---|---|---|---|---|---|
| □ | NEW | KALAIVANI | | By Network | 192.168.0.106 | e0:46:9a:0e:03:c6 | 20 |
| ■ | NEW | CHEFPHONE | | By Network | 192.168.0.109 | 68:a3:c4:9f:c4:ab | 20 |

**Change Device Type**

Device Name:
Unknown

Device Type
Unknown

- Select the device type from the drop-down



Change Device Type

Device Name:
Unknown

Device Type

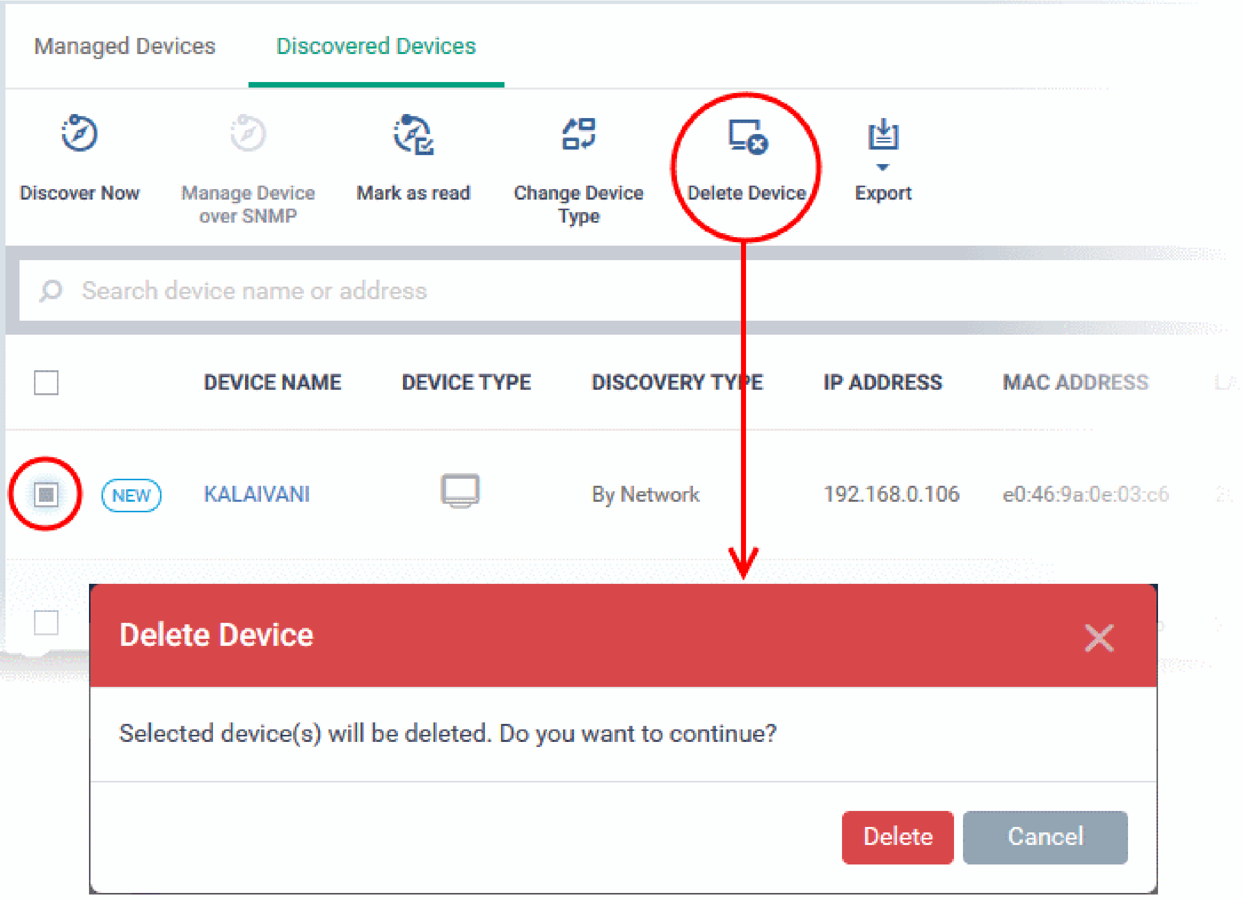
- Click 'Change'

The category will change with appropriate icon in the device type column.

### Remove Selected Devices from the 'Discovered Devices' list

- Click 'Network Management' > 'Devices'
- Click the 'Discovered Devices' tab
    - Select a company or a group to view the list of devices identified in that group

      Or
    - Select 'Show all' to view every discovered device
- Select the devices to be removed and click 'Delete Device'.



| | | DEVICE NAME | DEVICE TYPE | DISCOVERY TYPE | IP ADDRESS | MAC ADDRESS |
|---|---|---|---|---|---|---|
| ☒ | NEW | KALAIVANI | | By Network | 192.168.0.106 | e0:46:9a:0e:03:c6 |

Delete Device

Selected device(s) will be deleted. Do you want to continue?

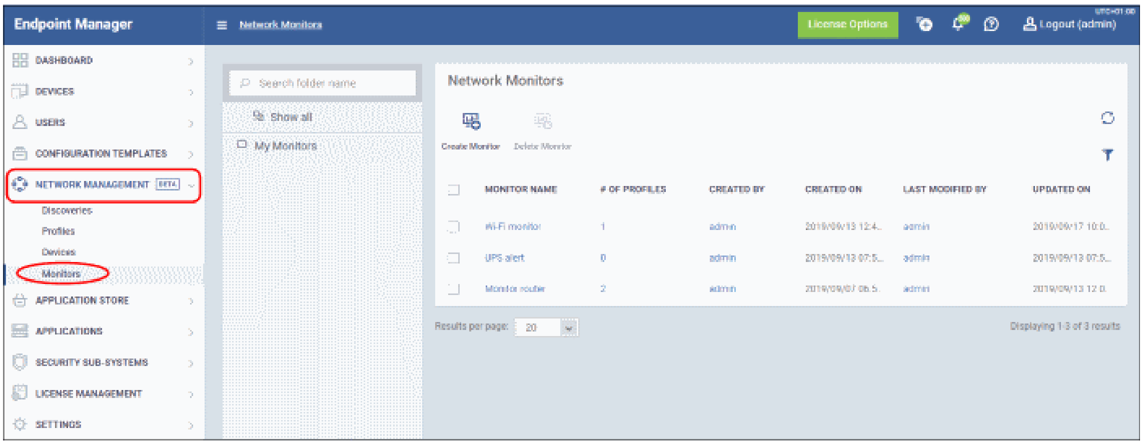
- Click 'Delete' in the confirmation dialog. The device will be removed from the list.
- If a deleted device is discovered again in subsequent scans, it will be shown as a new device.

## 7.4. Manage Network Monitors

- Click 'Network Management' > 'Monitors'
- A monitor is a script which tracks events on SNMP devices on the network and takes specific actions if its conditions are met. For example, a monitor could alert you if a device is switched off for a certain length of time.
- Network monitors are added to network profiles, which are in-turn applied to your SNMP devices.
- A single network monitor can be used in multiple network profiles. A single profile can include multiple monitors.

**View and manage monitors**

- Click 'Network Management' > 'Monitors'



| MONITOR NAME | # OF PROFILES | CREATED BY | CREATED ON | LAST MODIFIED BY | UPDATED ON |
|---|---|---|---|---|---|
| Wi-Fi monitor | 1 | admin | 2019/09/13 12:4... | admin | 2019/09/17 10:0... |
| UPS alert | 0 | admin | 2019/09/13 07:5... | admin | 2019/09/13 07:5... |
| Monitor router | 2 | admin | 2019/09/07 06:5... | admin | 2019/09/13 12:0... |

Results per page: 20

Displaying 1-3 of 3 results

| Network Monitors - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Monitor Name | The label of the network monitor |
| No. of Profiles | Show how many network profiles are using the monitor. Click the number to view a list of the profiles. |
| Created By | Admin that added the network profile |
| Created On | Date and time the profile was added |
| Last Modified By | Admin that most recently edited the profile |
| Updated On | Date and time the profile was most recently modified. |
| **Controls** | |
| Create Monitor | Configure a new monitor<br>• See **Create a Network Monitor** |
| Delete | Remove a monitor |

- Use the funnel on the right to filter monitors by various criteria.
- Click a column header to sort items by ascending / descending/ alphabetical order

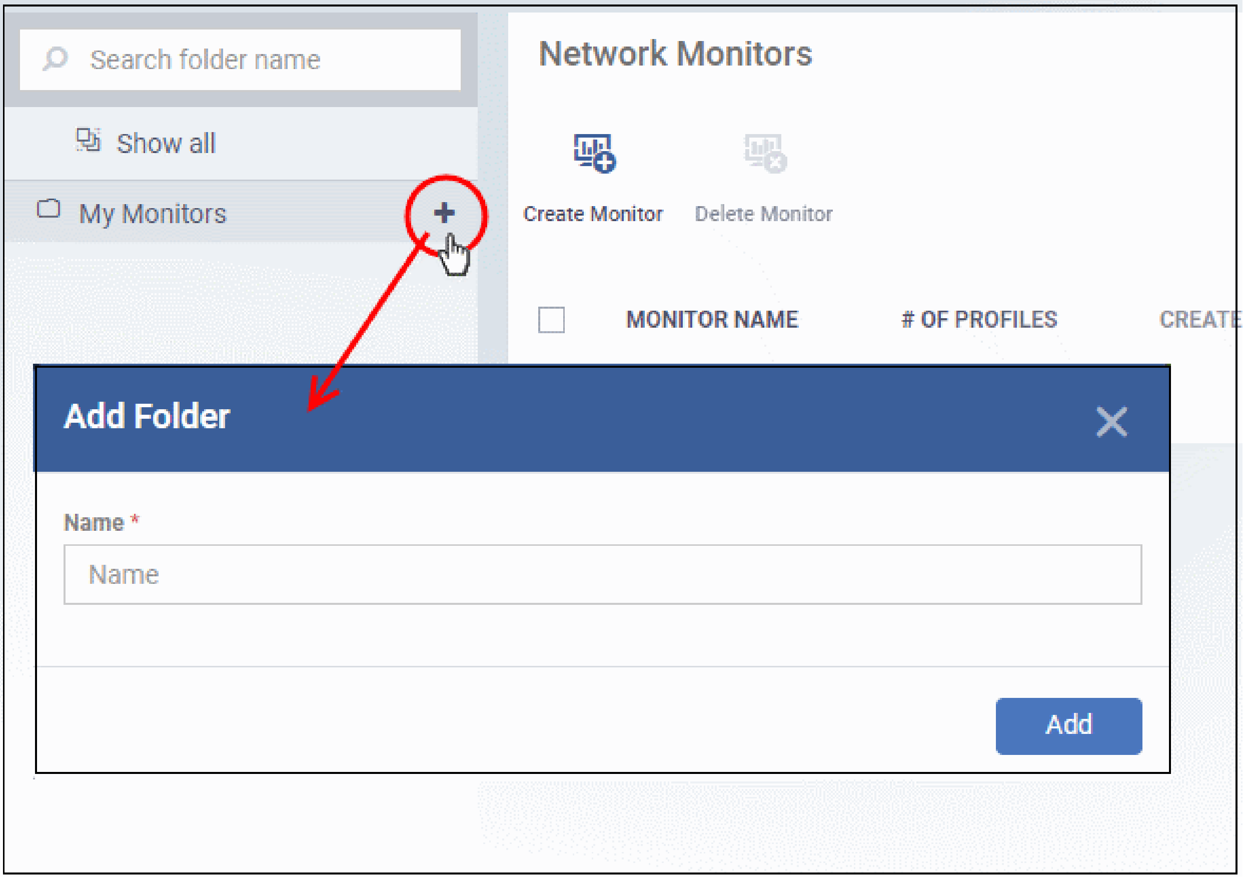
See the following links for more help:

- **Optional - Create a sub-folder in the My Monitors folder**
- **Create a network monitor**
- **Edit a monitor**
- **Delete a monitor**
- **View monitor details**

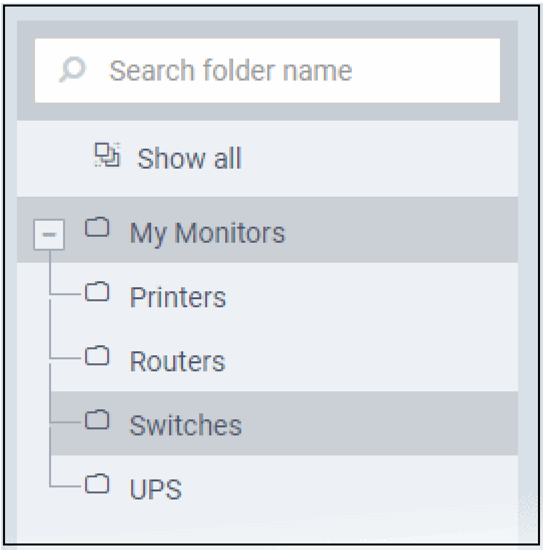
## Optional - Create a sub-folder in the My Monitors folder

- Click 'Network Management' > 'Monitors'
- To keep things organized, it is a good idea to create a sub-folder to house your SNMP monitors. You can create individual folders named after your target SNMP devices, or simply create a single folder for all SNMP monitors.

- Place your mouse on the 'My Monitors' folder and click '+'



- **Name -** Enter an appropriate label for the sub-folder and click 'Add'
- Repeat the process to add more folders as required.

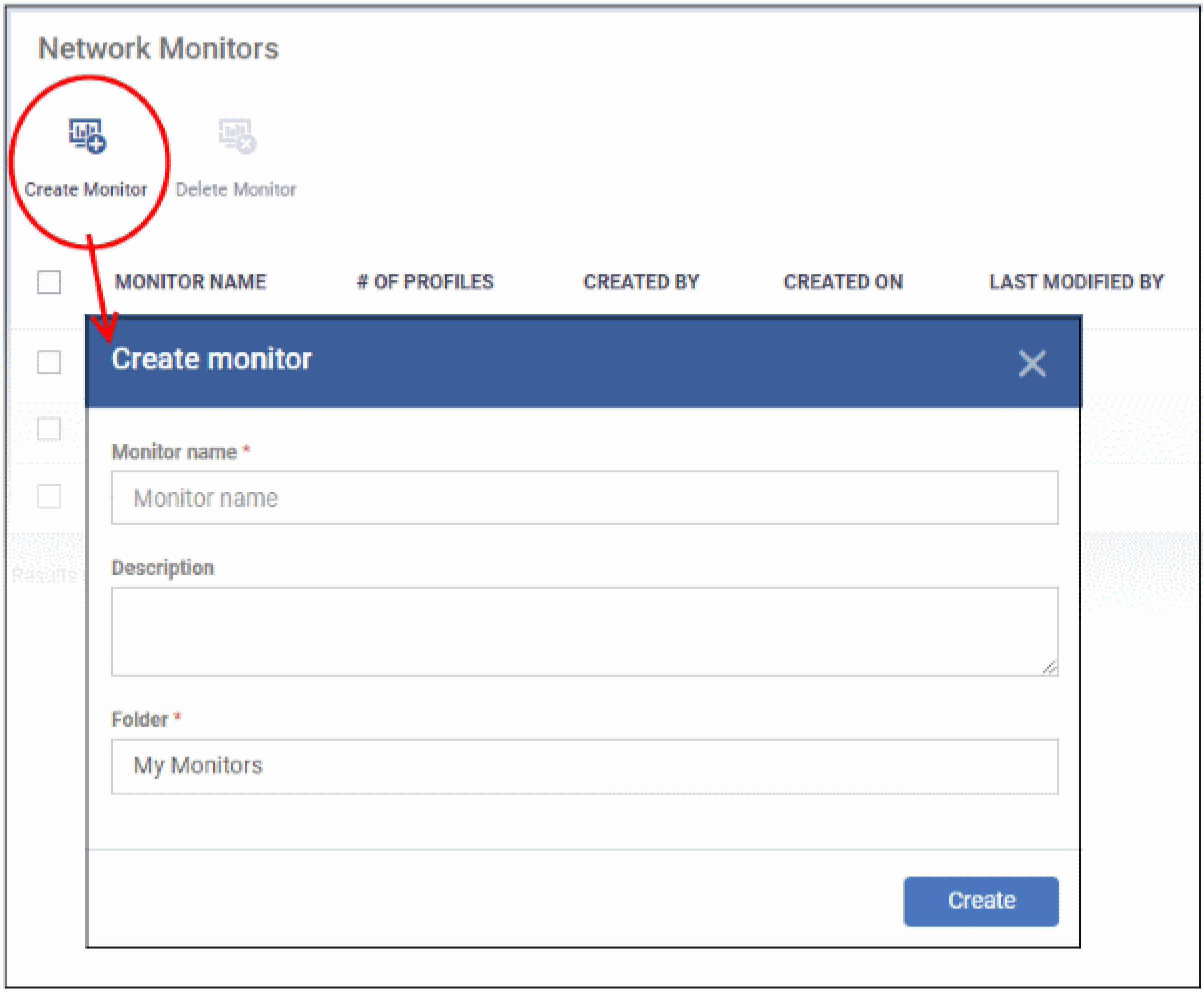


You can also add sub-folders to a sub-folder. You can now save **network monitors** in your new folders.

- **Rename a sub-folder -** Place your mouse over it, click the pencil icon, enter a new name and click 'Save'
- **Delete a sub-folder -** Place your mouse over it, click the trash can icon and confirm removal in the delete folder dialog.

### Create a Network Monitor

- Click 'Network Management' > 'Monitors'
- Select the folder on the left in which you want save the monitor. All monitors are shown in 'My Monitors' irrespective of which you folder save them.
- Click 'Create Monitor'



Monitor name *

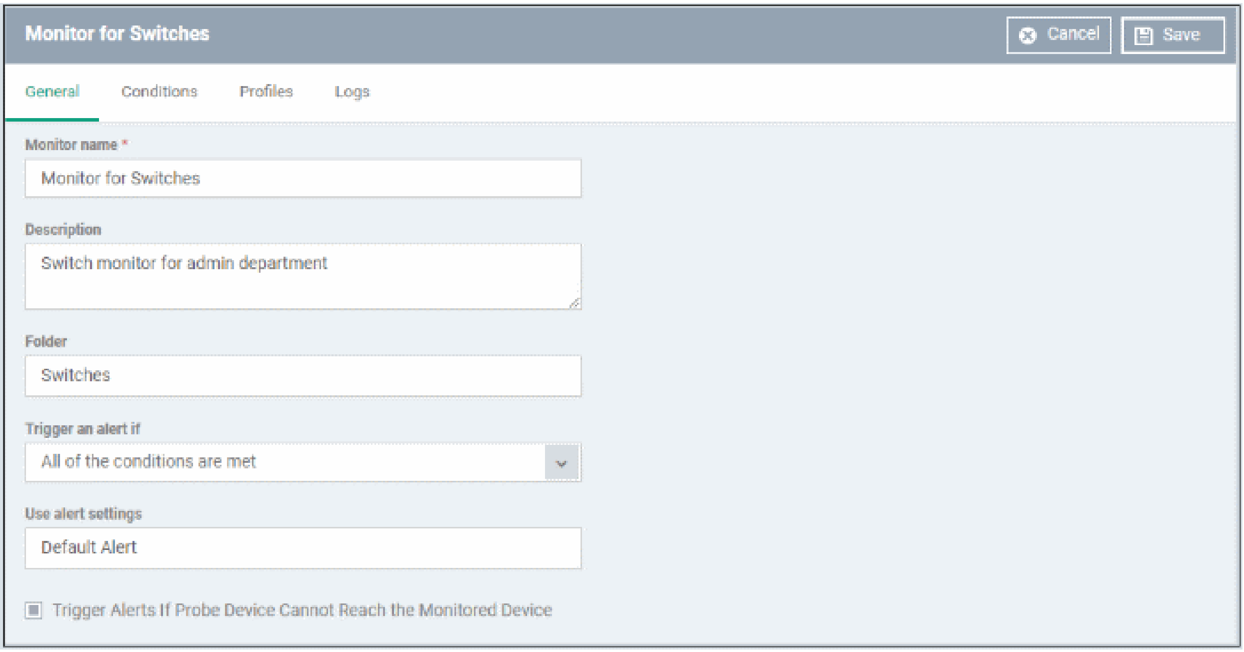
Monitor name

Description

Folder *

My Monitors

- **Monitor name -** Enter an appropriate label for the monitor, for example, 'Monitor for Switches'
- **Description -** Any short notes about the monitor, if required.
- **Folder -** Select which folder you want to save the monitor. Default is 'My Monitor'. Start typing the folder name and select from the suggestions.
- Click 'Create'. This opens the monitor, ready for you to configure.



Monitor name *
Monitor for Switches

Description
Switch monitor for admin department

Folder
Switches

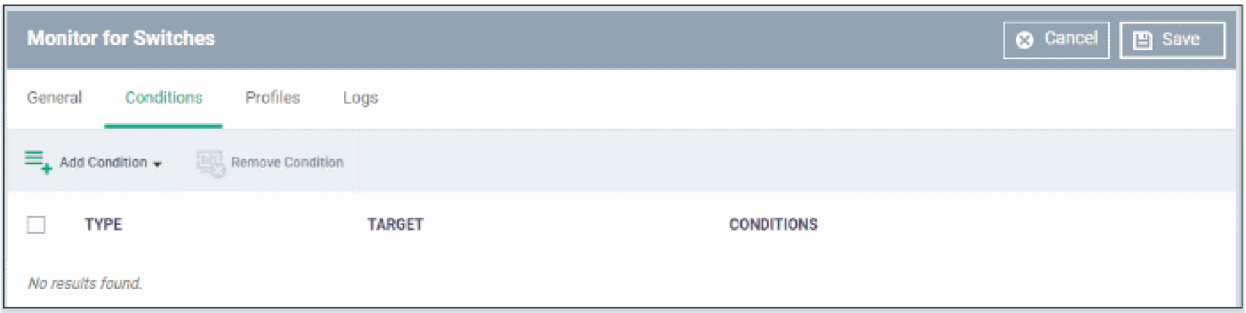
Trigger an alert if
All of the conditions are met

Use alert settings
Default Alert

☒ Trigger Alerts If Probe Device Cannot Reach the Monitored Device

- Monitor name, description and folder are what you configured in the previous step. Update if required.
- **Trigger an alert if** - If the conditions that you configure in the 'Conditions' tab is breached, select when alert should be activated. The options are:
  - All of the conditions are met - All rules that you configure in 'Conditions' tab is met.
  - Any of the conditions are met - Any of the rules that you configure is met.
- **Use alert settings** - Select the alert type that should be triggered. See '**Manage Alerts**' to configure custom alerts and manage them.
- **Trigger Alerts if Probe Device Cannot Reach the Monitored Device** - Alert is activated if the probe device(s) is not able to establish communication with the SNMP device.

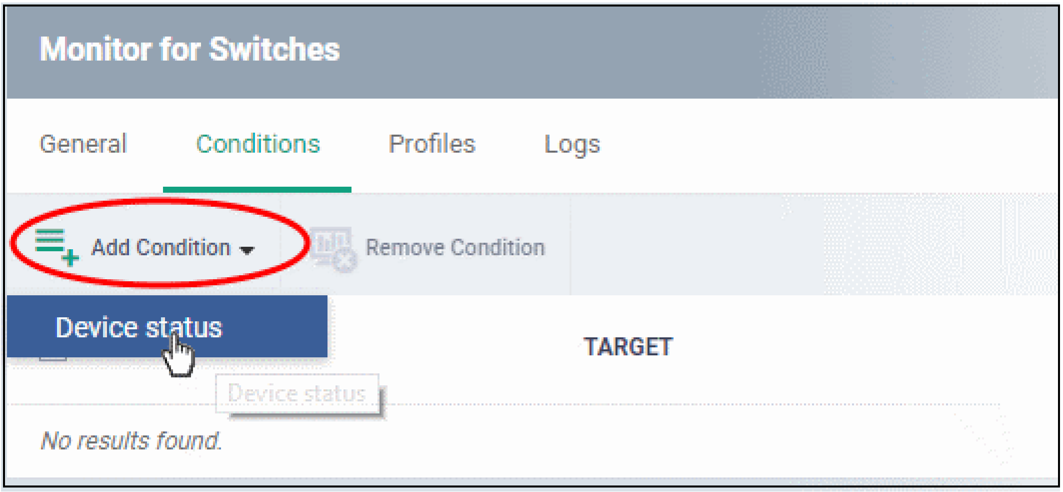
- Click the 'Conditions' tab. This is where you can configure rules for the monitor.



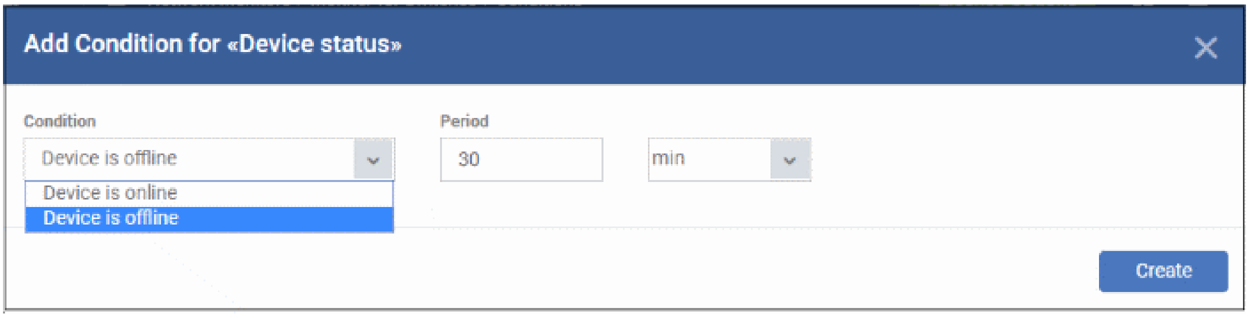
| □ | TYPE | TARGET | CONDITIONS |
|---|---|---|---|

*No results found.*

- Click 'Add Condition' and select 'Device status'

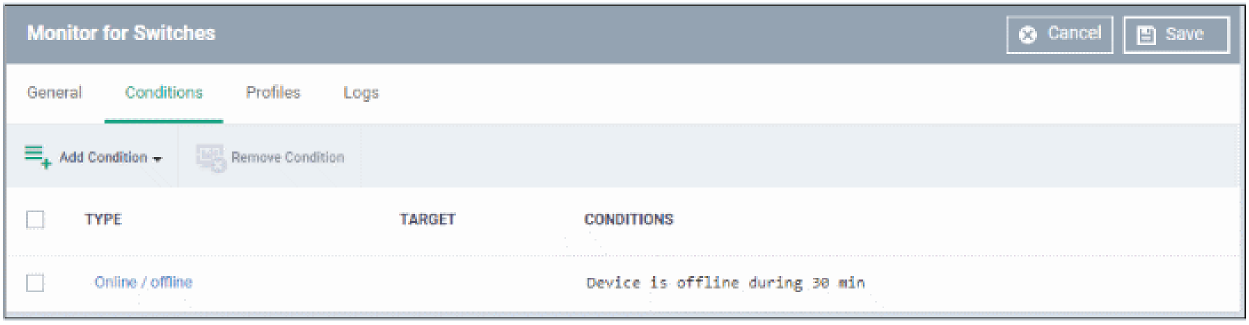


The 'Add Condition' dialog is shown:



- **Condition** - Select the parameter. The options are:
  - Device is offline
  - Device is online
- **Period** - Enter the amount of time (in hours or minutes) for the condition.

- Click 'Create'



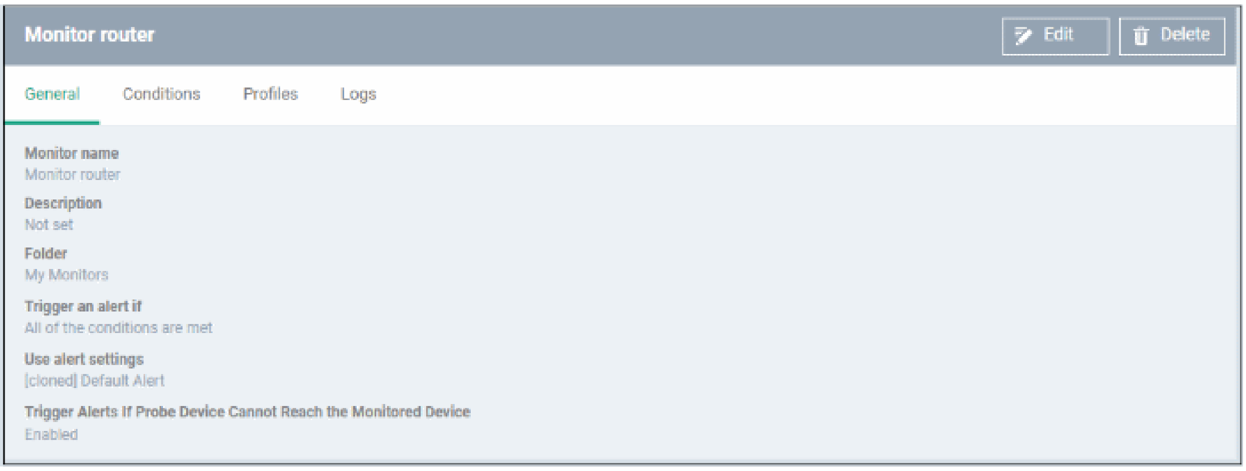
| □ | TYPE | TARGET | CONDITIONS |
|---|---|---|---|
| □ | Online / offline | | Device is offline during 30 min |

- Repeat the process to add more conditions.
- To delete a condition, select it and click 'Remove Condition'

- 'Profiles' and 'Logs' screens are populated after the monitor is added to profiles. See '**View Monitor Details**'
- Click 'Save'. The monitor will be available for selection while **creating a network profile**.

## Edit a Monitor

- Click 'Network Management' > 'Monitors'
- Click the monitor name



Monitor name
Monitor router

Description
Not set

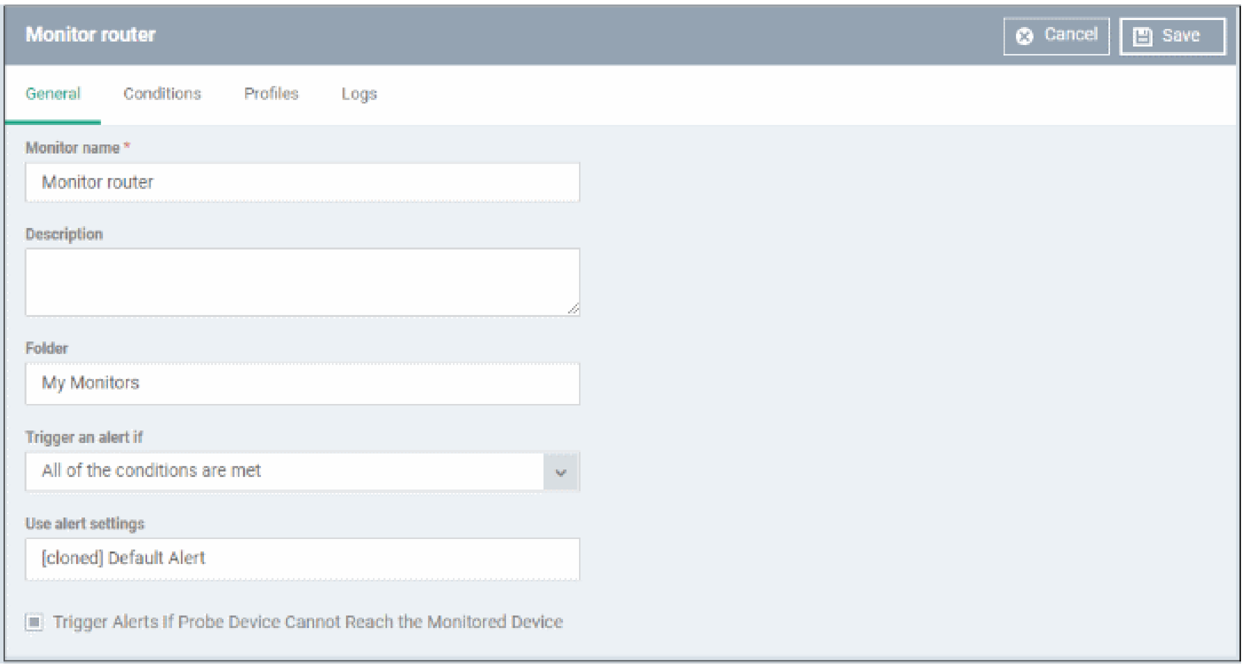
Folder
My Monitors

Trigger an alert if
All of the conditions are met

Use alert settings
[cloned] Default Alert

Trigger Alerts If Probe Device Cannot Reach the Monitored Device
Enabled

- Click 'Edit' at top-right



Monitor name *
Monitor router

Description

Folder
My Monitors

Trigger an alert if
All of the conditions are met

Use alert settings
[cloned] Default Alert

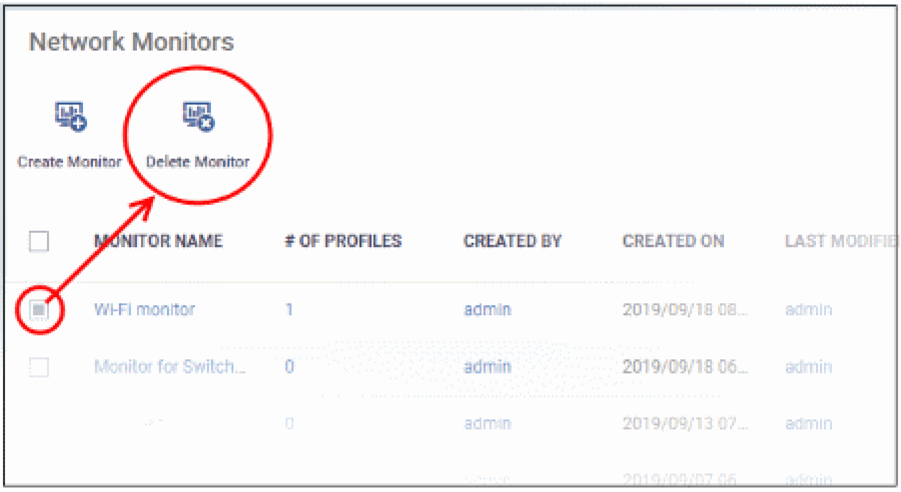
☒ Trigger Alerts If Probe Device Cannot Reach the Monitored Device

- The monitor update process is similar to creating a monitor explained above.
    - 'Profiles' and 'Logs' screens are populated after the monitor is added to profiles. See '**View Monitor Details**'
- Click 'Save' to apply your changes.

## Delete a Monitor

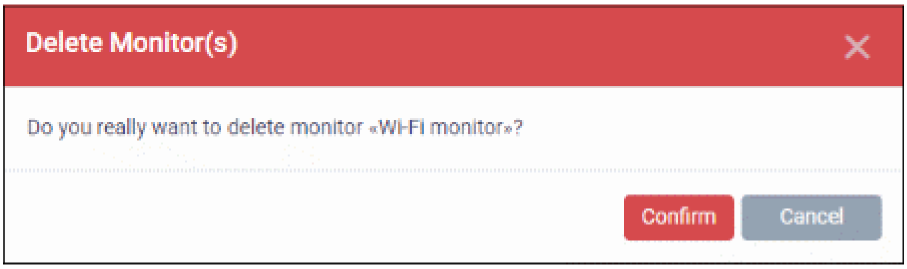
If you delete a monitor, it will be removed from the applicable profiles also.

- Click 'Network Management' > 'Monitors'
- Select the monitor and click 'Delete Monitor'



| □ | MONITOR NAME | # OF PROFILES | CREATED BY | CREATED ON | LAST MODIFIE |
|---|---|---|---|---|---|
| ☑ | Wi-Fi monitor | 1 | admin | 2019/09/18 08... | admin |
| □ | Monitor for Switch... | 0 | admin | 2019/09/18 06... | admin |
| | | 0 | admin | 2019/09/13 07... | admin |

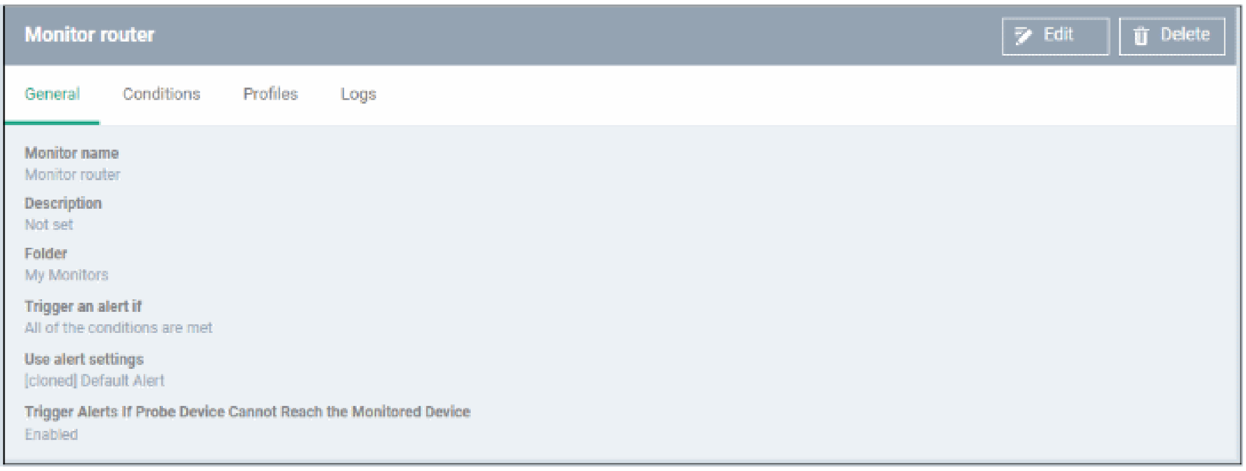
- Click 'Confirm'



Do you really want to delete monitor «Wi-Fi monitor»?

## View Monitor Details

- Click 'Network Management' > 'Monitors'
- Click the name of a network monitor. The monitor configuration interface will open at the 'General' tab



Monitor name
Monitor router

Description
Not set

Folder
My Monitors

Trigger an alert if
All of the conditions are met

Use alert settings
[cloned] Default Alert

Trigger Alerts If Probe Device Cannot Reach the Monitored Device
Enabled

The configuration interface lets you to:

- **Edit the general settings and monitoring conditions**
- **View all profiles that use the monitor**
- **View the log of events related to the monitor from all SNMP devices on which the profiles with the monitor is applied**

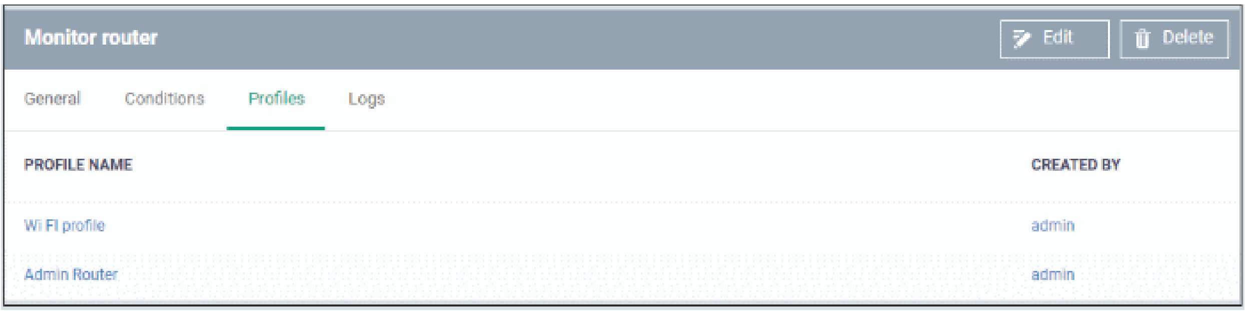
**Edit a Monitor**

- See **Edit Monitor** section above.

**View all Profiles that use the Monitor**

- Click 'Network Management' > 'Monitors'

- Click the name of a network monitor.
- Click the 'Profiles' tab


Monitor router

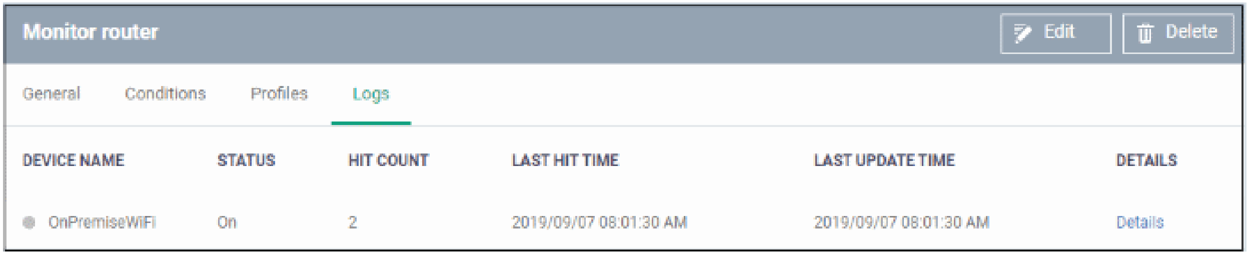
| PROFILE NAME | CREATED BY |
|---|---|
| Wi FI profile | admin |
| Admin Router | admin |

| Network Profile - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Profile Name | The profile in which the monitor is active.<br>• Click the profile name to open its configuration interface. See **Create a Network Profile**. |
| Created By | The admin that created the profile<br>• Click the name to view user details. See **View User Details**. |

### View Network Monitor Logs

- Click 'Network Management' > 'Monitors'
- Click the name of a network monitor.
- Click the 'Logs' tab

The logs tab shows all instances where the conditions of the monitor were breached:

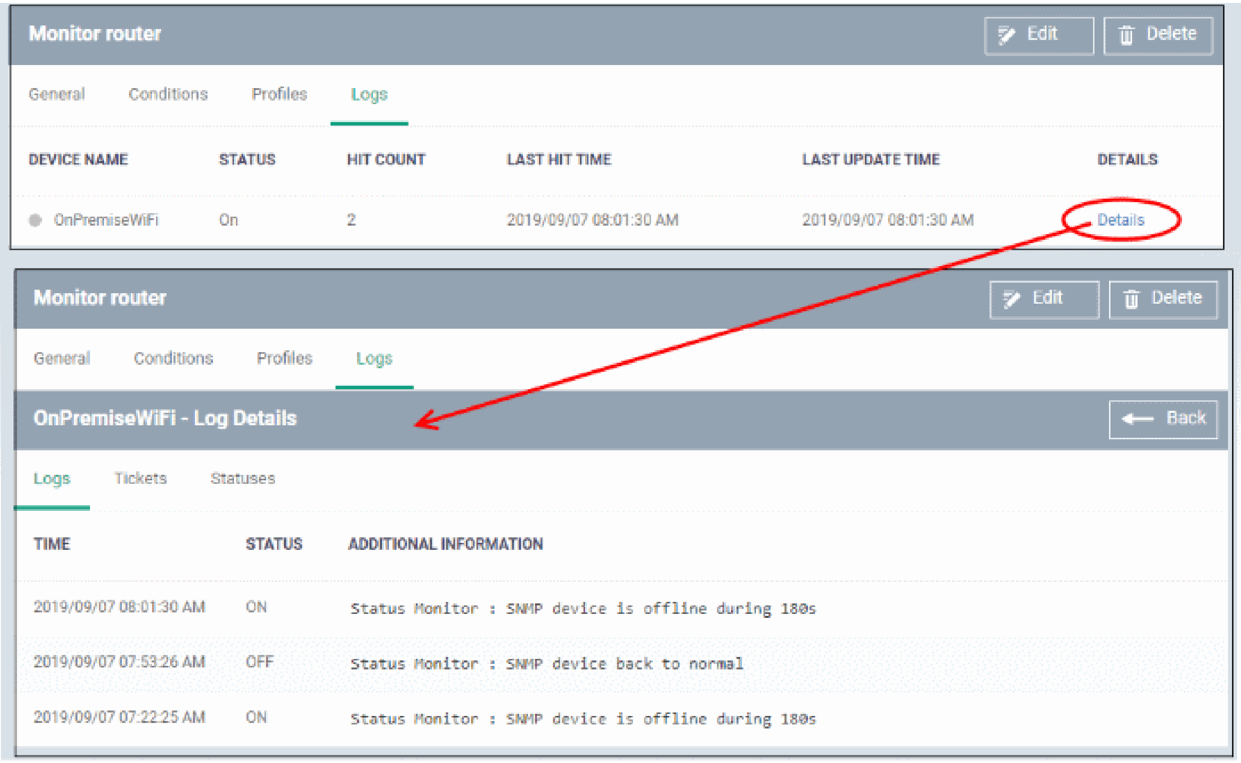

Monitor router

| DEVICE NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| OnPremiseWiFi | On | 2 | 2019/09/07 08:01:30 AM | 2019/09/07 08:01:30 AM | Details |

| Network Monitor Logs - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Device Name | The SNMP device on which the breach occurred.<br>• Click the name of the SNMP device to open its details interface. See **SNMP Device Details Interface** |
| Status | Whether or not the monitor is currently active for the device |
| Hit Count | Number of times the monitored conditions were breached |
| Last Hit Time | Date and time the monitoring rule was last breached |
| Last Update Time | Date and time when the information was last refreshed |
| Details | • Click the 'Details' link to view a log of the breach events<br>• See **View Details of Network Monitor Logs** (given below) for more information |

### View Details of Network Monitor Logs

- Click the 'Details' link to view the details of the breaches of the monitoring conditions:



| DEVICE NAME | STATUS | HIT COUNT | LAST HIT TIME | LAST UPDATE TIME | DETAILS |
|---|---|---|---|---|---|
| OnPremiseWiFi | On | 2 | 2019/09/07 08:01:30 AM | 2019/09/07 08:01:30 AM | Details |

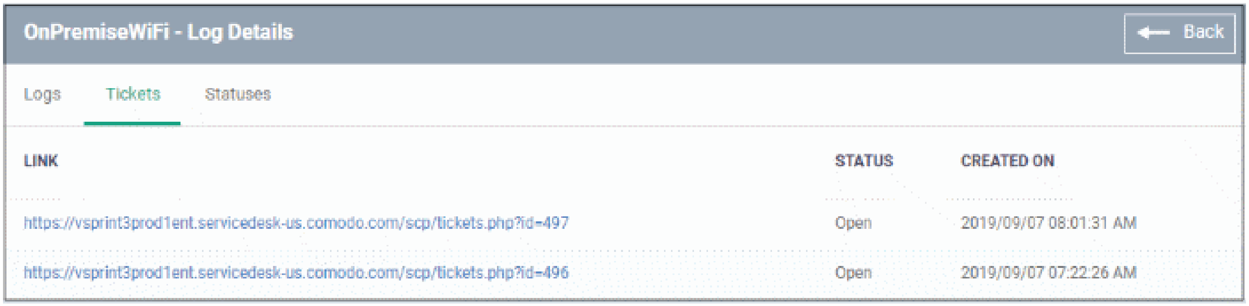
| TIME | STATUS | ADDITIONAL INFORMATION |
|---|---|---|
| 2019/09/07 08:01:30 AM | ON | Status Monitor : SNMP device is offline during 180s |
| 2019/09/07 07:53:26 AM | OFF | Status Monitor : SNMP device back to normal |
| 2019/09/07 07:22:25 AM | ON | Status Monitor : SNMP device is offline during 180s |

Details are shown under three tabs:

**Logs** - The date and time when the event occurred. Also shows the details of the monitoring rule that detected the event.

| Network Monitoring Log Details - 'Logs' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Time | Date and time of the event. |
| Status | The current state of the monitor on the device:<br>• On - The device is exceeding the thresholds of the monitor<br>• Off - The device is operating within the thresholds of the monitor |
| Additional Information | Details on the condition monitored and the breach |

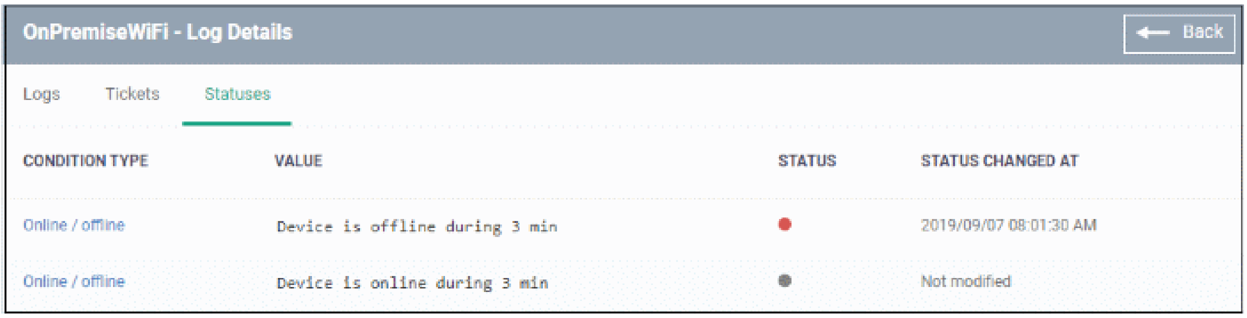
**Tickets** - Shows any service desk tickets which were automatically generated by the alert.



| LINK | STATUS | CREATED ON |
|---|---|---|
| https://vsprint3prod1ent.servicedesk-us.comodo.com/scp/tickets.php?id=497 | Open | 2019/09/07 08:01:31 AM |
| https://vsprint3prod1ent.servicedesk-us.comodo.com/scp/tickets.php?id=496 | Open | 2019/09/07 07:22:26 AM |

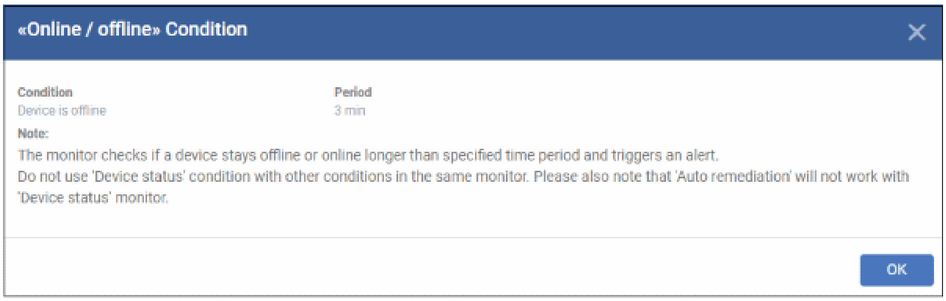
| Network Monitoring Log Details - 'Tickets' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Link | A link to the support ticket created for the breach event.<br>• Click the link to open the ticket in service desk. |
| Status | Indicates whether the ticket is open or closed |
| Created On | The date and time at which the ticket was raised. |

**Statuses** - Shows the current status of each condition in the monitor:



OnPremiseWiFi - Log Details

| CONDITION TYPE | VALUE | STATUS | STATUS CHANGED AT |
|---|---|---|---|
| Online / offline | Device is offline during 3 min | ● | 2019/09/07 08:01:30 AM |
| Online / offline | Device is online during 3 min | ● | Not modified |

| Network Monitoring Log Details - 'Statuses' tab - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Condition Type | The category of monitor.<br>Click the type to view its exact conditions and thresholds. An example is shown below:<br><br>«Online / offline» Condition<br>Condition: Device is offline<br>Period: 3 min<br>Note:<br>The monitor checks if a device stays offline or online longer than specified time period and triggers an alert.<br>Do not use 'Device status' condition with other conditions in the same monitor. Please also note that 'Auto remediation' will not work with 'Device status' monitor.<br>OK |
| Value | Condition set in the monitor |
| Status | The current state of the monitored parameter on the device.<br>• Green - The device is operating within the thresholds of the monitor<br>• Grey - Unknown<br>• Red - The device is exceeding the conditions of the monitor. |
| Status Changed at | The date and time of the last change in state of the monitored parameter. |

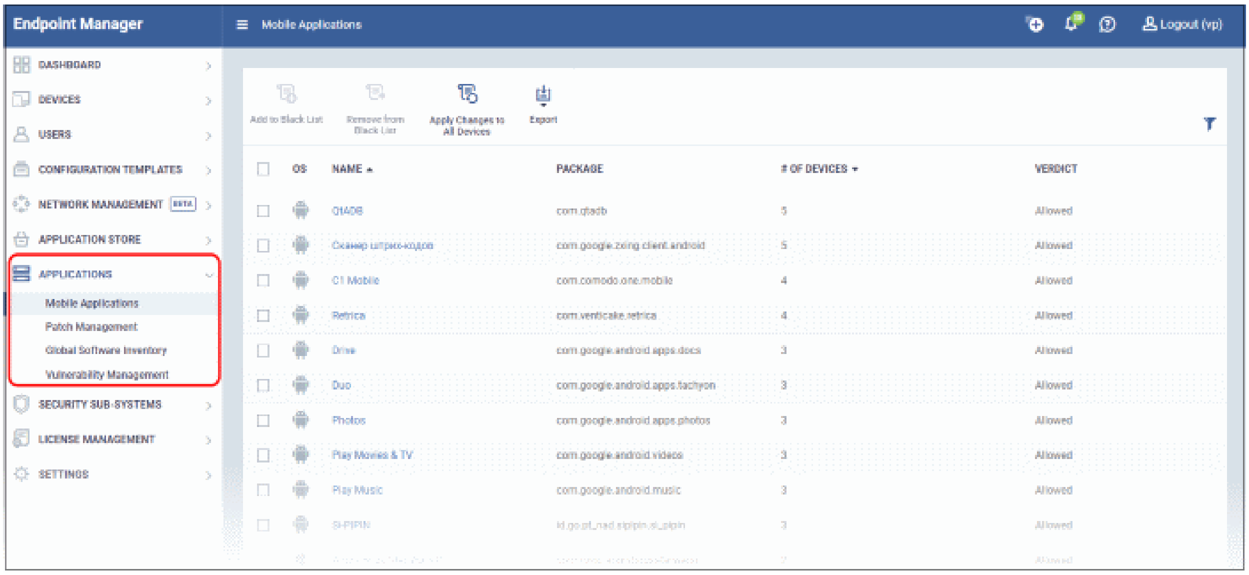
# 8.Applications

- Click 'Applications' in the left-menu to view this section.

Endpoint Manager provides visibility and control over the applications which are installed on user devices.

The applications area has the following sections:

- **Mobile Applications -** View all applications installed on enrolled Android and iOS devices. Block any application identified as malicious. Once blacklisted, the application is not allowed to run on any device on which it is installed.
- **Patch Management -** View a constantly updated list of OS and third party application patches available for managed Windows devices. The area lets you install or uninstall patches/updates as required.
- **Global Software Inventory -** View all applications installed on your Windows devices. You can uninstall unwanted applications as required.
- **Vulnerability Management -** Shows known weaknesses on your devices along with their common vulnerabilities and exposures (CVE) listing. You can run patches on affected devices.



| ☐ | OS | NAME ▲ | PACKAGE | # OF DEVICES ▼ | VERDICT |
|---|---|---|---|---|---|
| ☐ | | Q1408 | com.qtadb | 5 | Allowed |
| ☐ | | Сканер штрих-кодов | com.google.zxing.client.android | 5 | Allowed |
| ☐ | | C1 Mobile | com.comodo.one.mobile | 4 | Allowed |
| ☐ | | Retrica | com.venticake.retrica | 4 | Allowed |
| ☐ | | Drive | com.google.android.apps.docs | 3 | Allowed |
| ☐ | | Duo | com.google.android.apps.tachyon | 3 | Allowed |
| ☐ | | Photos | com.google.android.apps.photos | 3 | Allowed |
| ☐ | | Play Movies & TV | com.google.android.videos | 3 | Allowed |
| ☐ | | Play Music | com.google.android.music | 3 | Allowed |
| ☐ | | SI-PIPIN | id.go.pt_nad.sipipin.si_pipin | 3 | Allowed |

Click the following links for more help:

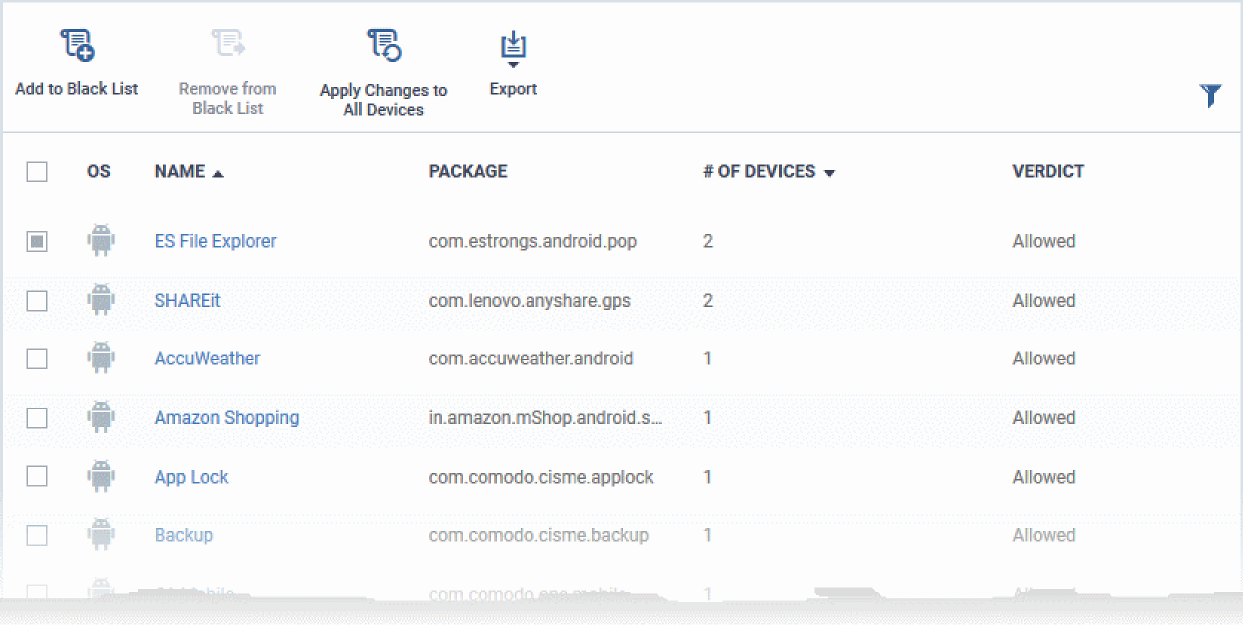
- View Applications Installed on Android and iOS Devices
  - Blacklist and Whitelist Applications
- Patch Management
- View and Manage Applications Installed on Windows Devices
- Vulnerability Management

## 8.1.View Applications Installed on Android and iOS Devices

- Click 'Applications' > 'Mobile Applications'
- The 'Mobile Applications' interface shows all applications identified on enrolled Android and iOS devices. Additional details include the package name and the number of devices on which the app was found.
- You can blacklist application you feel are suspicious or not trustworthy.
- Blacklisted apps are blocked on any devices on which they are installed. EM also prevents them from being installed on other devices in future.

### To access the 'Mobile Applications' interface

- Click 'Applications' > 'Mobile Applications'.



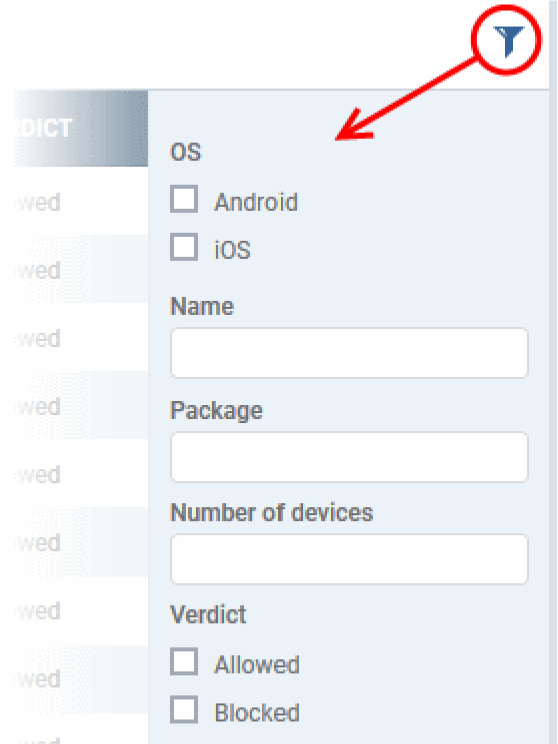
| □ | OS | NAME ▲ | PACKAGE | # OF DEVICES ▼ | VERDICT |
|---|---|---|---|---|---|
| ☒ | | ES File Explorer | com.estrongs.android.pop | 2 | Allowed |
| □ | | SHAREit | com.lenovo.anyshare.gps | 2 | Allowed |
| □ | | AccuWeather | com.accuweather.android | 1 | Allowed |
| □ | | Amazon Shopping | in.amazon.mShop.android.s... | 1 | Allowed |
| □ | | App Lock | com.comodo.cisme.applock | 1 | Allowed |
| □ | | Backup | com.comodo.cisme.backup | 1 | Allowed |

| Mobile Applications - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system on which the application runs. |
| Name | Application label.<br>• Click the name of an application to open the '**Devices**' interface that shows the list of only those devices on which the app is installed.<br>• This enables you 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 | The count of devices on which the app is found installed. |
| Verdict | Whether the application is allowed or blacklisted. |
| **Controls** | |
| Add to Black List | Add selected applications to the global black list.<br>Blacklisted apps are blocked on any devices on which they are installed. EM also prevents them from being installed on other devices in future.<br>See **Blacklist and Whitelist Applications** the next section for more details. |
| Remove from Black List | Release an application from the global black list.<br>Released applications are allowed to run on devices on which they are installed. They can also be installed in future on other devices.<br>See **Blacklist and Whitelist Applications** the next section for more details. |
| Apply Changes to All Devices | Deploy the new settings to all devices. |
| Export | Save the list of mobile applications as a comma separated values (CSV) file. See **Export** |

| | |
|---|---|
| | the List of Mobile Applications for more details. |

## Sorting, Search and Filter Options

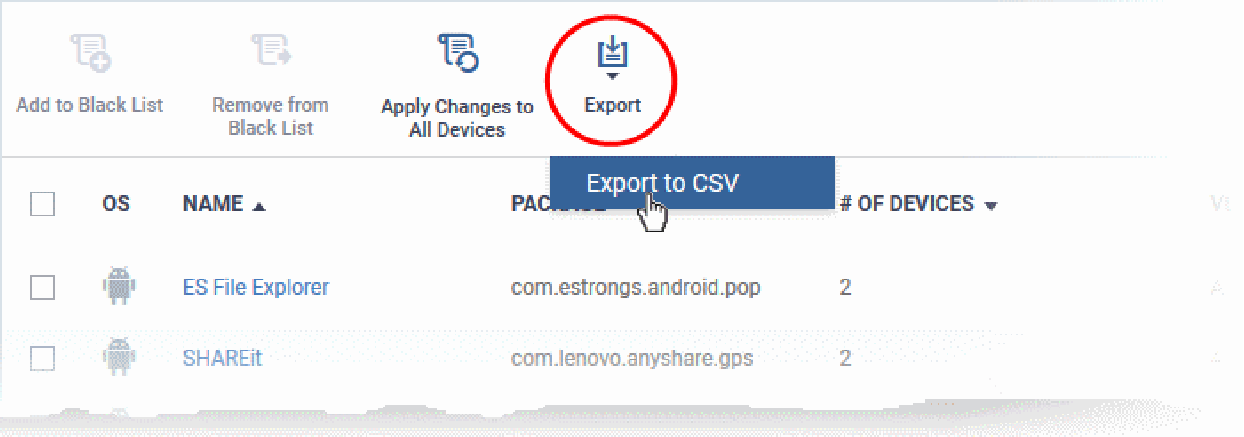
- Click any column header to sort the items based on alphabetical order of entries in that column.
- Click the funnel button at the right end to open filter options.



## Export the List of Mobile Applications

Export the list of mobile applications to a .csv file as follows:

- Click 'Applications' > 'Mobile Applications'.
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | OS | NAME ▲ | PAC | # OF DEVICES ▼ | V |
|---|---|---|---|---|---|
| □ | | ES File Explorer | com.estrongs.android.pop | 2 | |
| □ | | SHAREit | com.lenovo.anyshare.gps | 2 | |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See Reports in The Dashboard for more details.

## 8.1.1. Blacklist and Whitelist Applications

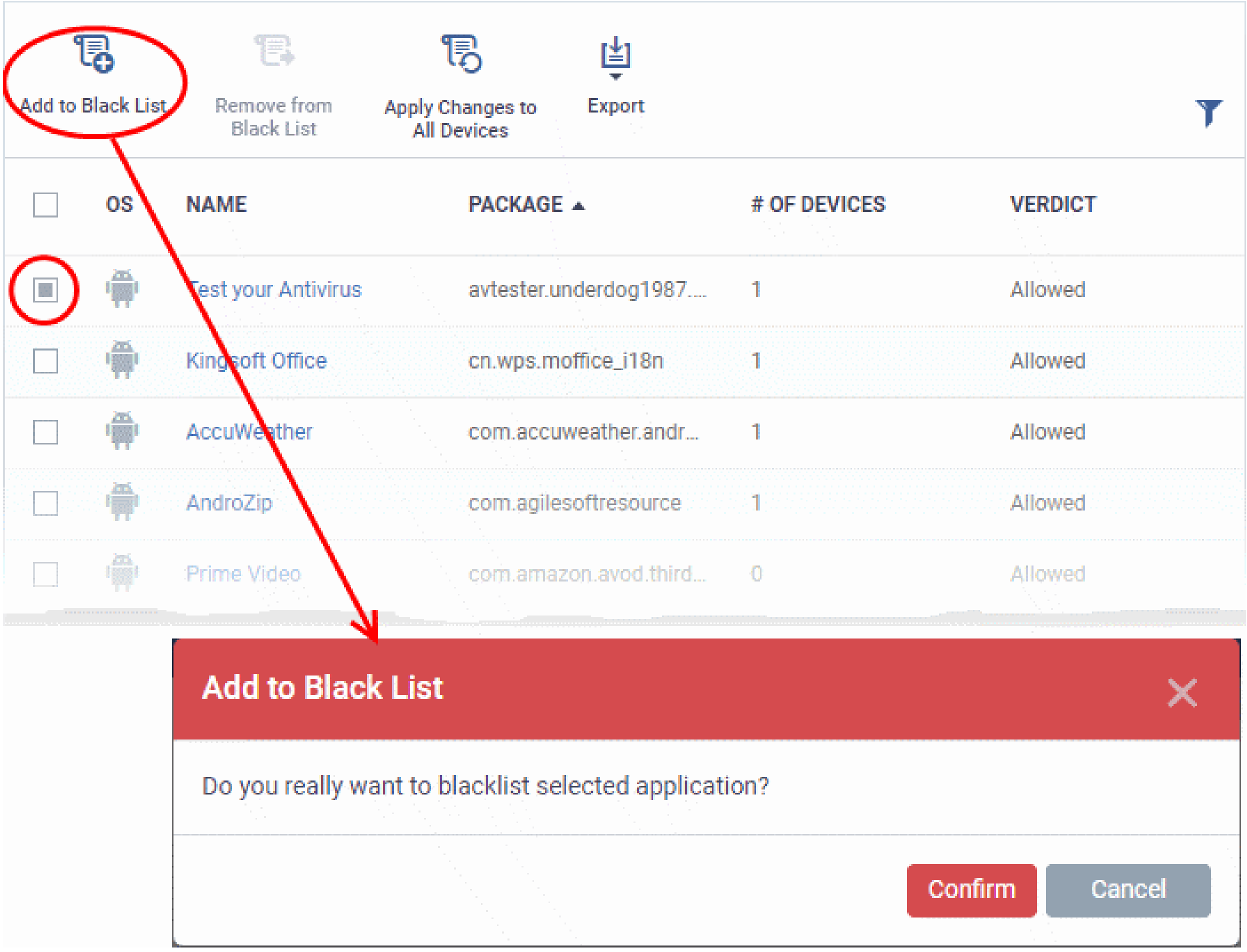
- Click 'Applications' > 'Mobile Applications'

- The mobile applications area shows a list of applications installed on all enrolled Android and iOS devices.
- You can review the list and decide which apps should be allowed or blocked.
- If a suspicious or malicious application is identified then it can be moved to the blacklist. This blocks the application on all devices and prevents other devices from installing the application in future.
- Blacklisted files that are subsequently found to be trustworthy can be moved to the whitelist.

**To move selected apps to blacklist**

- Click 'Applications' > 'Mobile Applications'.
- Select the apps to be blocked.

**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.



| | OS | NAME | PACKAGE ▲ | # OF DEVICES | VERDICT |
|---|---|---|---|---|---|
| ☑ | | Test your Antivirus | avtester.underdog1987.... | 1 | Allowed |
| ☐ | | Kingsoft Office | cn.wps.moffice_i18n | 1 | Allowed |
| ☐ | | AccuWeather | com.accuweather.andr... | 1 | Allowed |
| ☐ | | AndroZip | com.agilesoftresource | 1 | Allowed |
| ☐ | | Prime Video | com.amazon.avod.third... | 0 | Allowed |

Add to Black List

Do you really want to blacklist selected application?

- Click 'Add to Black List' on the top.
- Click 'Confirm' in the confirmation dialog.

The selected apps will be added to the 'Black List' and their status will change to 'Blocked'. The apps will be blocked at the devices on which they are currently installed, during the next polling cycle of the device.

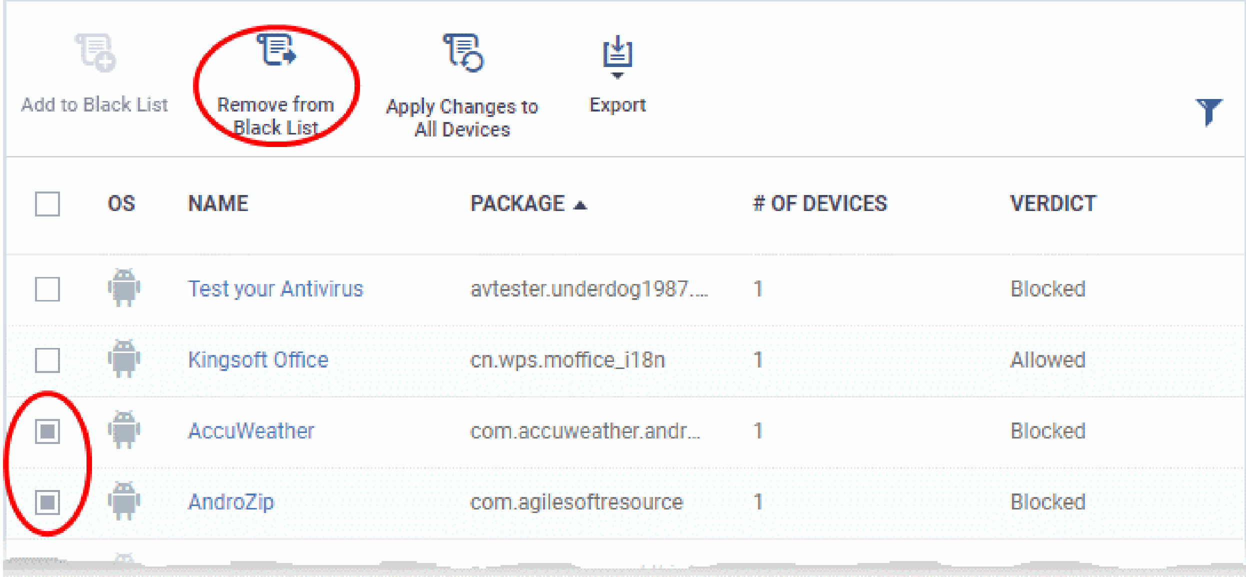
- Click 'Apply Changes to All Devices' to instantly block the apps on the devices on which they are currently installed.

## Unblocking Blacklisted Apps

- Applications that were blocked by mistake can be released from blacklist and allowed to be installed or run on the devices.

### To remove trustworthy apps from blacklist

- Click 'Applications' > 'Mobile Applications'.
- Select the apps with 'Blocked' status, to be whitelisted.



| □ | OS | NAME | PACKAGE ▲ | # OF DEVICES | VERDICT |
|---|---|---|---|---|---|
| □ | | Test your Antivirus | avtester.underdog1987.... | 1 | Blocked |
| □ | | Kingsoft Office | cn.wps.moffice_i18n | 1 | Allowed |
| ☑ | | AccuWeather | com.accuweather.andr... | 1 | Blocked |
| ☑ | | AndroZip | com.agilesoftresource | 1 | Blocked |

- Click 'Remove From Black List' at the top.

The status of the apps will change to 'Allowed'. The apps will be allowed to run on the devices on which they are currently installed, during the next polling cycle of the device.

- Click 'Apply Changes to All Devices' to instantly change the status of the apps in the devices and allow them to run.

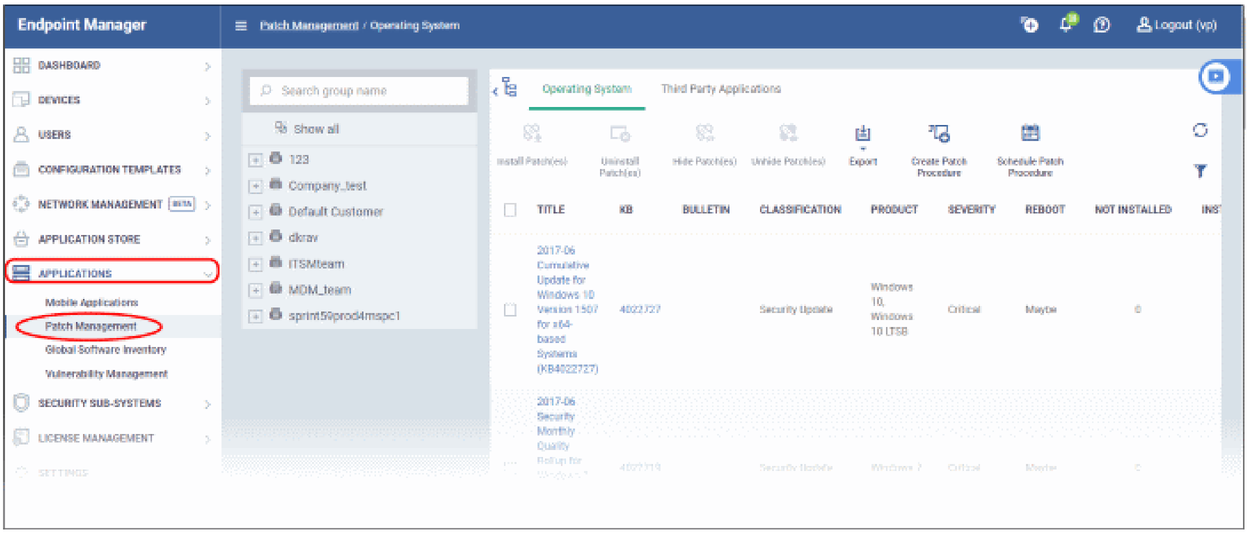
## 8.2. Patch Management

- Click 'Applications' > 'Patch Management' to open this interface
- The patch management area lets you install OS updates and patches for 3rd party applications on managed Windows devices.
- The area also lets you uninstall Windows updates and patches if you want to roll back to the previous version.
- You can also create procedures to deploy operating system and 3rd party application patches. The procedures can be added to profiles to automatically install any new patches.
- All available patches are displayed by default. You can filter patches by company and device group.

**Tip**: This area lets you manage patches across all devices in your network. As an alternative, you can manage patches on *individual* devices by clicking 'Devices' > 'Device List' > 'Device Management' > *Click on a device* > 'Patch Management'. See **View and Manage Patches for Windows and 3rd Party Application** to find out more.

### To open the 'Patch Management' interface

- Open Endpoint Manager
- Click 'Applications' > 'Patch Management':

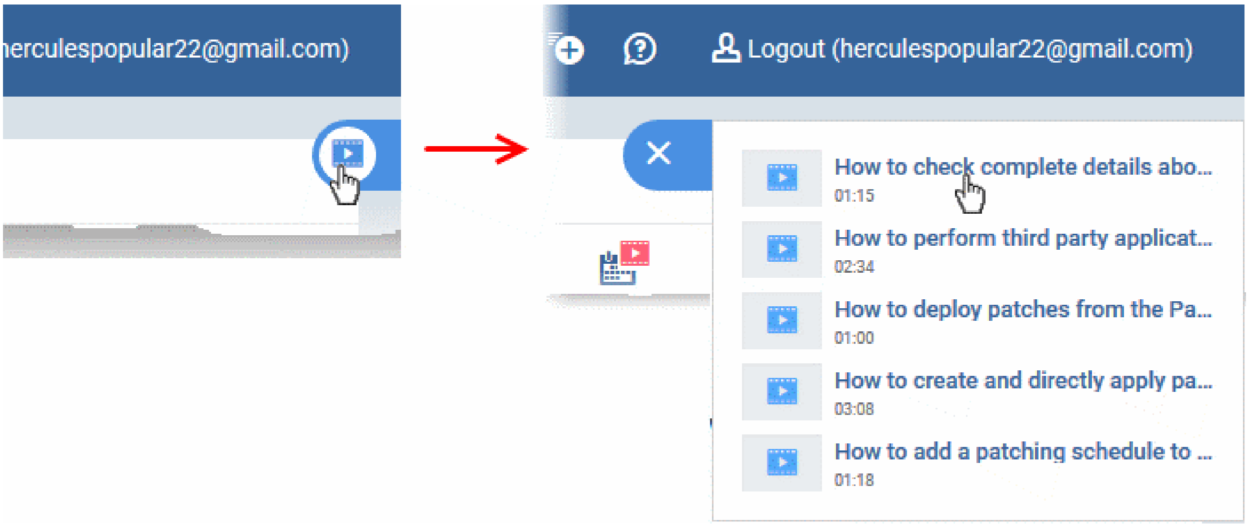


| | TITLE | KB | BULLETIN | CLASSIFICATION | PRODUCT | SEVERITY | REBOOT | NOT INSTALLED | INS |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2017-06 Cumulative Update for Windows 10 Version 1507 for x64-based Systems (KB4022727) | 4022727 | | Security Update | Windows 10, Windows 10 LTSB | Critical | Maybe | 0 | |
| | 2017-06 Security Monthly Quality Rollup for Windows 7 | 4022719 | | Security Update | Windows 7 | Critical | Maybe | 0 | |

The interface has two tabs:

- **Operating System** - All OS patches available for deployment through Endpoint Manager.
  - Each patch has additional details such as classification, the Windows component to which the patch applies, severity, release date, installation status and links to knowledgebase articles.
  - The interface lets you install or uninstall selected patches on multiple devices. You can also generate a report on overall patch status.
  - See **Manage OS Patches on Windows Endpoints** for more details.
- **Third Party Applications** - All updates available for 3rd party applications installed on managed Windows endpoints.
  - You can update selected applications on all required endpoints. See **Install 3rd Party Application Patches on Windows Endpoints** for more details.
  - See **EM Supported 3rd Party Applications** for a list of applications that we support for patching.

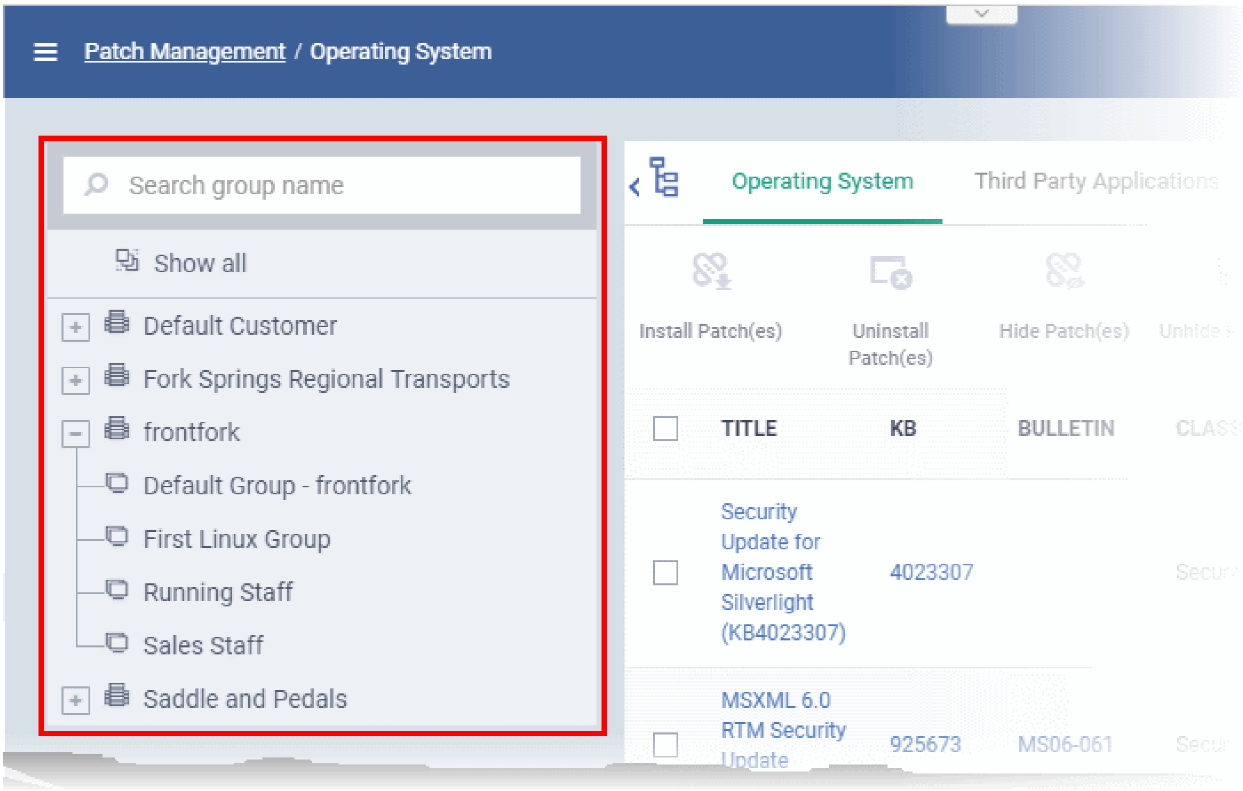
The slider at top-right contains links to help videos on various patch management tasks:


herculespopular22@gmail.com)
Logout (herculespopular22@gmail.com)
How to check complete details abo...
01:15
How to perform third party applicat...
02:34
How to deploy patches from the Pa...
01:00
How to create and directly apply pa...
03:08
How to add a patching schedule to ...
01:18

- Use the videos to quickly learn about patch deployment tasks.

## View patches by company / device group

- The tree structure on the left shows all enrolled organizations and device groups:



- Type a company or group name in the search field to look for a specific entity
- Click a company name to view patches for all device groups under it
- Click '+' beside a company to view device groups under it
- Click a device group to view patches for devices belonging to that group
- Click 'Show all' to clear any selections and view all patches

## 8.2.1. Manage OS Patches on Windows Endpoints

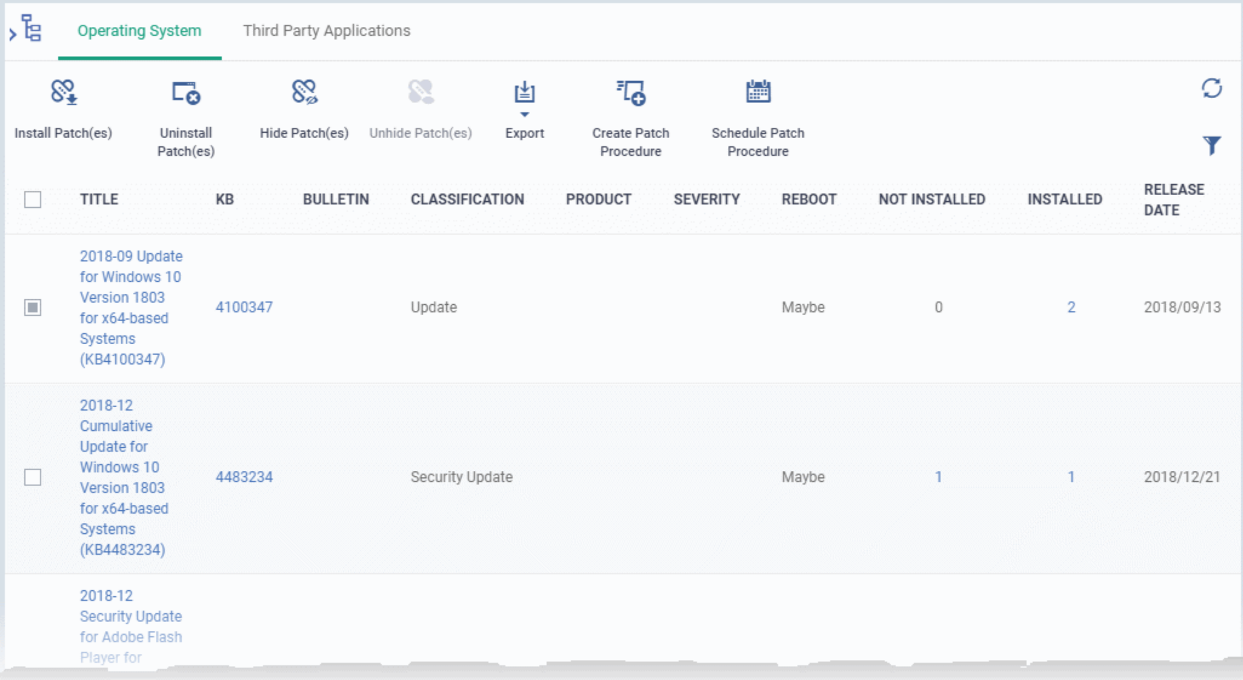
- Click 'Applications' > 'Patch Management' > 'Operating System' tab
- The 'Operating System' tab lets you deploy and manage OS updates on Windows devices.
- Endpoint Manager checks Microsoft update servers for available Windows patches and lists them in the interface. You can deploy patches to devices as require. You can also uninstall patches from devices if required.
- The interface shows details about each patch, including patch classification, the Windows component to which it applies, release date, severity, previous versions, Microsoft bulletins and number of endpoints which require the patch.
- You can filter patches by company and device group.
- You can hide patches if you do not want to deploy them. Hidden patches will not be available for deployment in the '**Device Management**' screen and will not be executed if added to a **patch procedure**.
- You can also create procedures to deploy operating system and 3rd party application patches. The procedures can be added to profiles to automatically install any new patches.
- You can also **generate reports** on the current patch status of your Windows devices.

**Manage operating system patches**

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
  - Select a company or group to view updates for that entity's devices

Or

- Select 'Show all' to view every available Windows update



| | TITLE | KB | BULLETIN | CLASSIFICATION | PRODUCT | SEVERITY | REBOOT | NOT INSTALLED | INSTALLED | RELEASE DATE |
|---|---|---|---|---|---|---|---|---|---|---|
| ▣ | 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347) | 4100347 | | Update | | | Maybe | 0 | 2 | 2018/09/13 |
| □ | 2018-12 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4483234) | 4483234 | | Security Update | | | Maybe | 1 | 1 | 2018/12/21 |
| | 2018-12 Security Update for Adobe Flash Player for | | | | | | | | | |

| 'Operating System' Patch Management - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Title | The descriptive name of the patch.<br>• Click the name to view patch details. See **View Patch Details** for more information on this interface. |
| KB | The knowledgebase article number that describes the patch.<br>• Click the number to view the Microsoft Knowledgebase article on the patch. |
| Bulletin | The Microsoft Bulletin number that contains details about the patch release.<br>• Click the number to view the patch bulletin. |
| Classification | The category of the patch. The possible values are:<br>• **Update -** Fixes a specific non-critical problem, but not a security-related bug.<br>• **Definition update -** Contains updates to a product's definition database. For example, an update to the virus signature database for Windows Defender.<br>• **Critical Update** - Fixes a specific, critical OS problem or a critical security-related bug<br>• **Security update** - Fixes a version specific, security related vulnerability<br>• **Update rollup -** Contains a collection of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. These updates generally target a specific Windows component.<br>• **Driver -** Adds software for controlling peripherals or add-on devices that could be connected to the endpoint<br>• **Feature pack -** Adds new functionality distributed after an OS release. |

| 'Operating System' Patch Management - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| | • **Service pack** - Contains a collection of hotfixes, security updates, critical updates, updates, and additional fixes.<br>• **Tool** - Installs a utility or feature for a specific task or a set of tasks.<br>• **Upgrades** - Updates the Windows OS version on the endpoint to the latest build. |
| Product | The Windows component to which the patch applies. |
| Severity | The criticality of the patch. The possible levels are:<br>• Critical<br>• Important<br>• Low<br>• Moderate<br>• Unspecified |
| Reboot | Whether or not the endpoint requires a restart to complete the patch installation. |
| Not Installed | The number of managed endpoints on which the patch is yet to be installed.<br>• Click the number to view the patch details screen at the 'Device List' tab. See the explanation of **View Details of a Patch** for more details on the 'Patch Details' screen.<br>• The 'Device List' tab shows devices to which the patch is relevant. You can deploy the patch to those devices which need it.<br>• See **Install a patch on selected endpoints** for more details. |
| Installed | The number of managed endpoints on which the patch has already been installed.<br>• Click the number to view the patch details screen at the 'Device List' tab. See **View Details of a Patch** for more details on the 'Patch Details' screen.<br>• The 'Device List' tab shows devices along with the installation status of the selected patch.<br>• You can select devices on which the patch is required and start the installation process. See the explanation of **Install a patch on selected endpoints** for more details. |
| Release Date | The date on which the patch was released by Microsoft. |
| **Controls** | |
| Install Patch(es) | Deploy selected patches to all devices on which they are yet to be installed.<br>See **Install selected patches on all managed endpoints at once** for more details. |
| Uninstall Patch(es) | Remove selected patches from all devices on which they are installed.<br>See **Uninstall selected patches from all managed endpoints at once** for more details. |
| Hide Patch(es) | Conceal selected patches that you do not want to be deployed onto enrolled |

| 'Operating System' Patch Management - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| | endpoints.<br>Hidden patches will not be visible in the '**Device Management**' screen and will not be executed as well if added to a **patch procedure**. |
| Unhide Patch(es) | Reveal all hidden patches. |
| Export | Generate current patch statuses for the devices. See **Generate Patch Statuses Report**. |
| Create Patch Procedure | Add a new procedure capable of auto-installing patches on your endpoints.<br>The procedure can be added to a profile and scheduled to install specific updates at specific times. See **Create a New Patch Procedure** for more. |
| Schedule Patch Procedure | Takes you to the 'Profiles' interface in Endpoint Manager.<br>You can add a procedure to a profile which will install your selected updates onto your endpoints. See **Procedure Settings** in **Profiles for Windows Devices** for guidance on this. |
| Show hidden patch(es) | Reveal all hidden patches so they can be potentially deployed. |

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

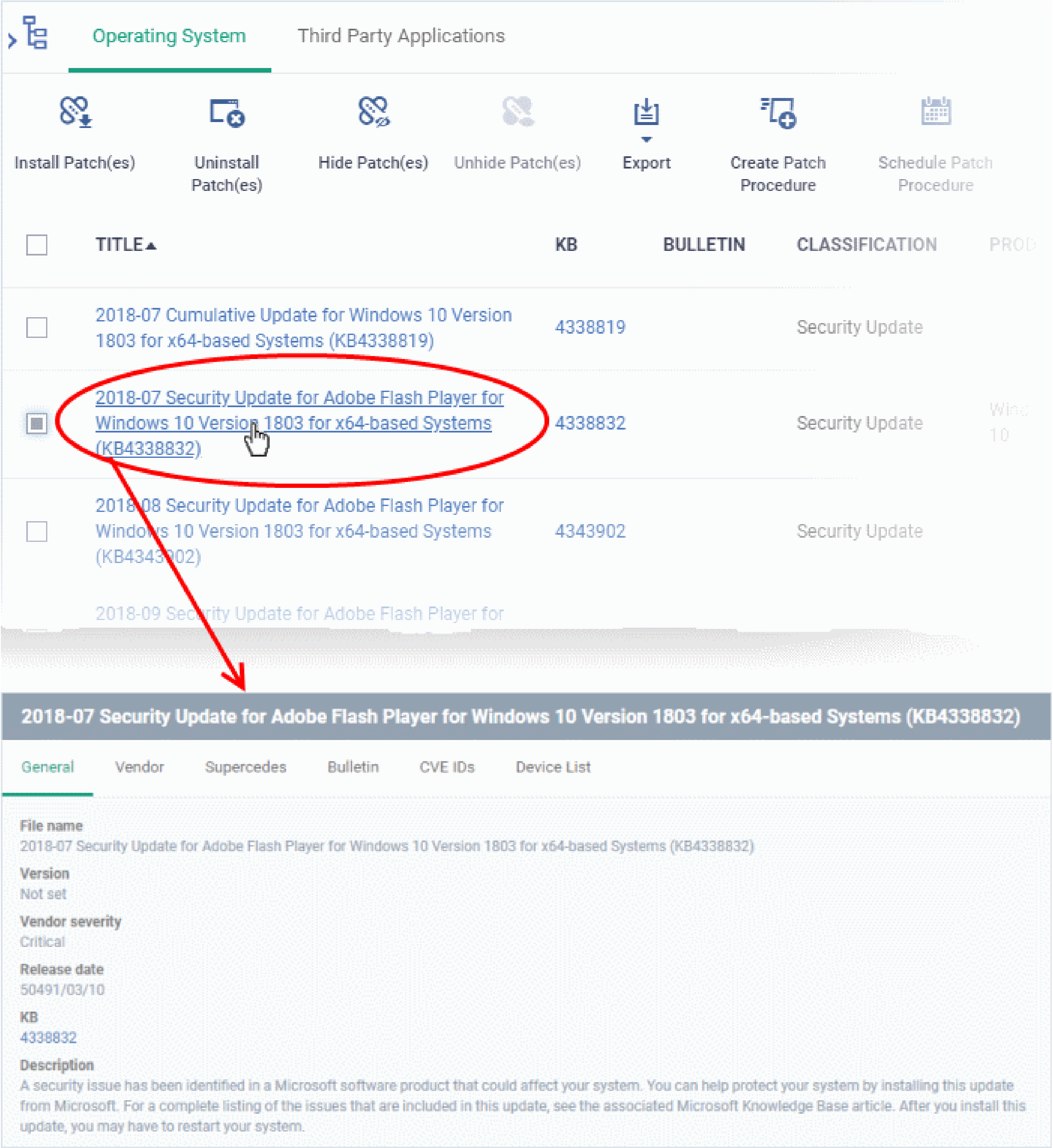
The 'Operating System Patch Management' interface allows you to:

- **View Details of a Patch**
- **Hide Patches**
- **Restore Hidden Patches**
- **Install selected patches on all managed endpoints at once**
- **Install a patch on selected endpoints**
- **Uninstall selected patches from all managed endpoints at once**
- **Create a New Patch Procedure**
- **Search specific patches in the Patch Management interface**
- **Generate Patch Statuses Report**

## View Details of a Patch

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
    - Select a company or a group to view the list of patches and Windows updates available for its devices

      Or
    - Select 'Show all' to view a list of all available patches and Windows updates
- Click the name of a patch to open its patch details screen.



| | TITLE▲ | KB | BULLETIN | CLASSIFICATION | PROD |
|---|---|---|---|---|---|
| □ | 2018-07 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4338819) | 4338819 | | Security Update | |
| ▣ | 2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832) | 4338832 | | Security Update | Wind 10 |
| □ | 2018-08 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4343902) | 4343902 | | Security Update | |
| | 2018-09 Security Update for Adobe Flash Player for | | | | |

2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832)

File name
2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832)

Version
Not set

Vendor severity
Critical

Release date
50491/03/10

KB
4338832

Description
A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.

The details of the patch are displayed under six tabs:

- **General** - Shows the name and general description, version number, severity as set by the vendor, release date and a link to the knowledgebase (KB) article for the patch release.
- **Vendor** - Indicates the publisher of the patch, with a link to the support page for the patch from the vendor
- **Security Patch Info** - Contains information on previous patches that are superseded by this patch
- **Bulletin** - Contains the Bulletin ID and a short summary of the bulletin published by the vendor for the patch
- **CVE IDs** - Displays the Common Vulnerabilities and Exposure (CVE) Identity numbers set for the patch by the vendor.
- **Device List** - The list of managed Windows endpoints with the installation status of the patch on them. You can install the patch on selected the endpoints from the list. See **Install a patch on selected endpoints** for more details.

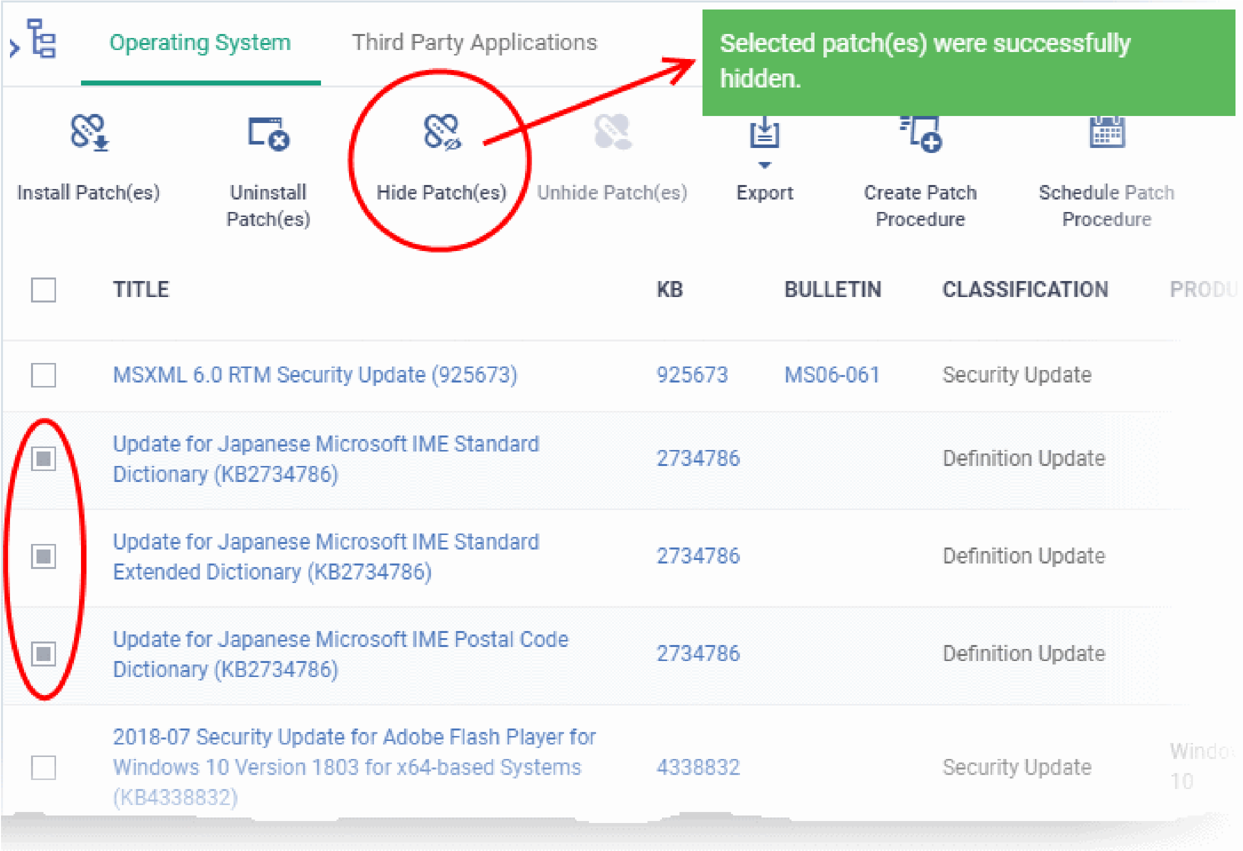
## Hide Patches

- You can hide those patches that you do not want to be rolled out to the endpoints, from the list.
- These patches will also be not available for deployment from the '**Device Management**' screen and will not be executed as well if added to a **patch procedure**.
- You can view the hidden patches by using the 'Show hidden patch(es) toggle button and install these patches onto endpoints.

**To hide unwanted patch(es)**

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
  - Select a company or a group to view the list of patches and Windows updates available for its devices

    Or
  - Select 'Show all' to view a list of all available patches and Windows updates
- Select the patch(es) you want to hide and click 'Hide Patch(es)'



Selected patch(es) were successfully hidden.

| ☐ | TITLE | KB | BULLETIN | CLASSIFICATION | PRODU |
|---|---|---|---|---|---|
| ☐ | MSXML 6.0 RTM Security Update (925673) | 925673 | MS06-061 | Security Update | |
| ☑ | Update for Japanese Microsoft IME Standard Dictionary (KB2734786) | 2734786 | | Definition Update | |
| ☑ | Update for Japanese Microsoft IME Standard Extended Dictionary (KB2734786) | 2734786 | | Definition Update | |
| ☑ | Update for Japanese Microsoft IME Postal Code Dictionary (KB2734786) | 2734786 | | Definition Update | |
| ☐ | 2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832) | 4338832 | | Security Update | Windo 10 |

To view the hidden patches again, you have to **unhide** them.

## Restore Hidden Patches

- Restored patches will also be available for installation in the **Device Management** interface and can be added to a **patch procedure.**

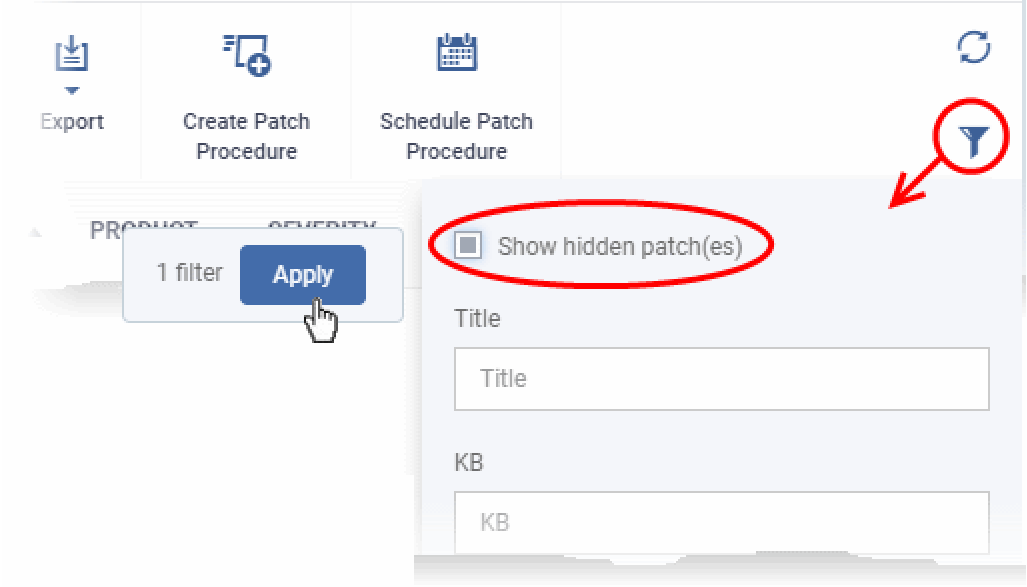
**To view hidden patches and restore them**

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
  - Select a company or a group to view the list of patches and Windows updates available for its devices

Or

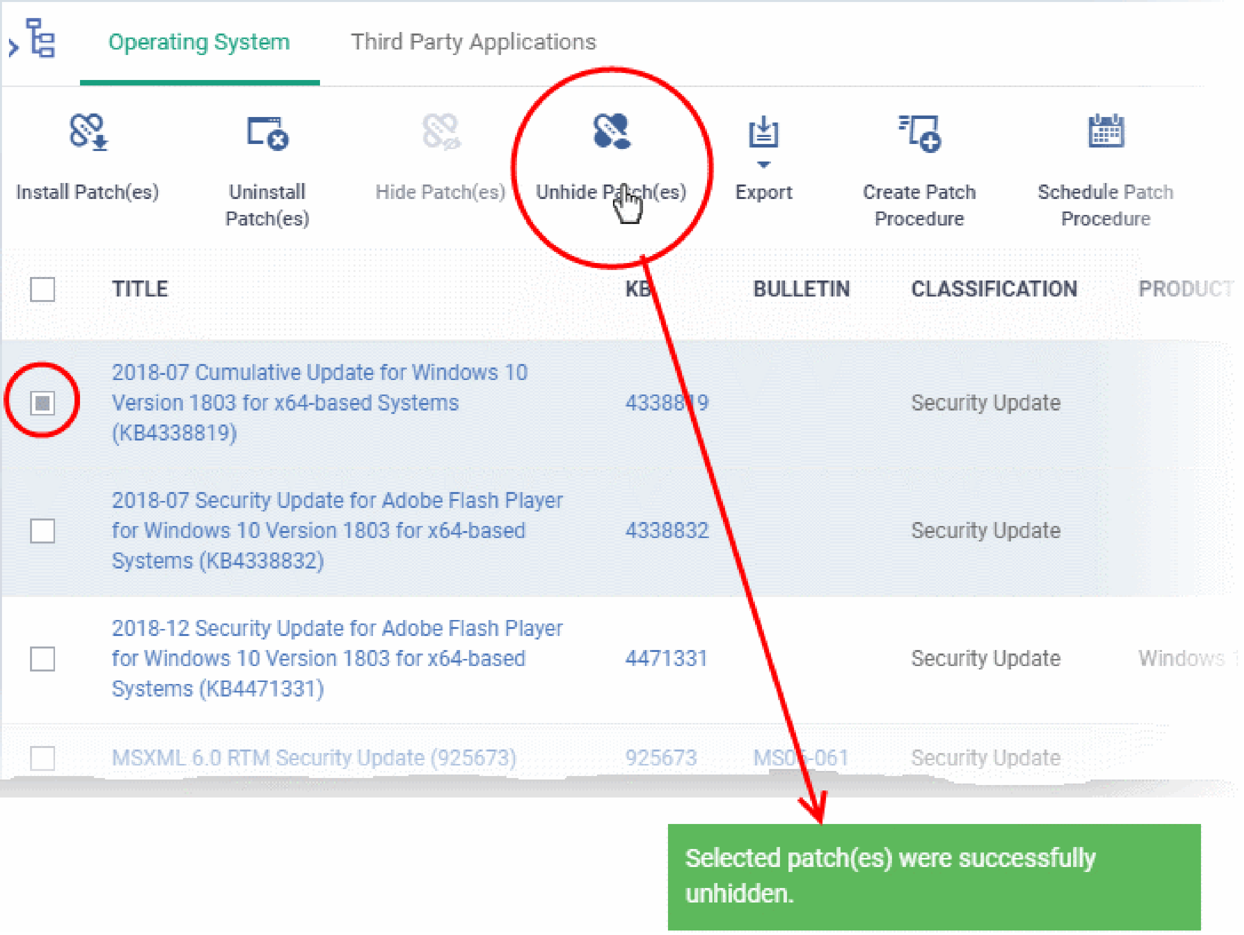
- Select 'Show all' to view a list of all available patches and Windows updates

- Click the funnel icon on the right, select 'Show hidden patch(es)' and click 'Apply'



The hidden patches are shown with dark gray background stripe.

- Select the hidden patch(es) from the list and click 'Unhide Patch(es)'



| ☐ | TITLE | KB | BULLETIN | CLASSIFICATION | PRODUCT |
|---|---|---|---|---|---|
| ☒ | 2018-07 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4338819) | 4338819 | | Security Update | |
| ☐ | 2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832) | 4338832 | | Security Update | |
| ☐ | 2018-12 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4471331) | 4471331 | | Security Update | Windows 1 |
| ☐ | MSXML 6.0 RTM Security Update (925673) | 925673 | MS06-061 | Security Update | |

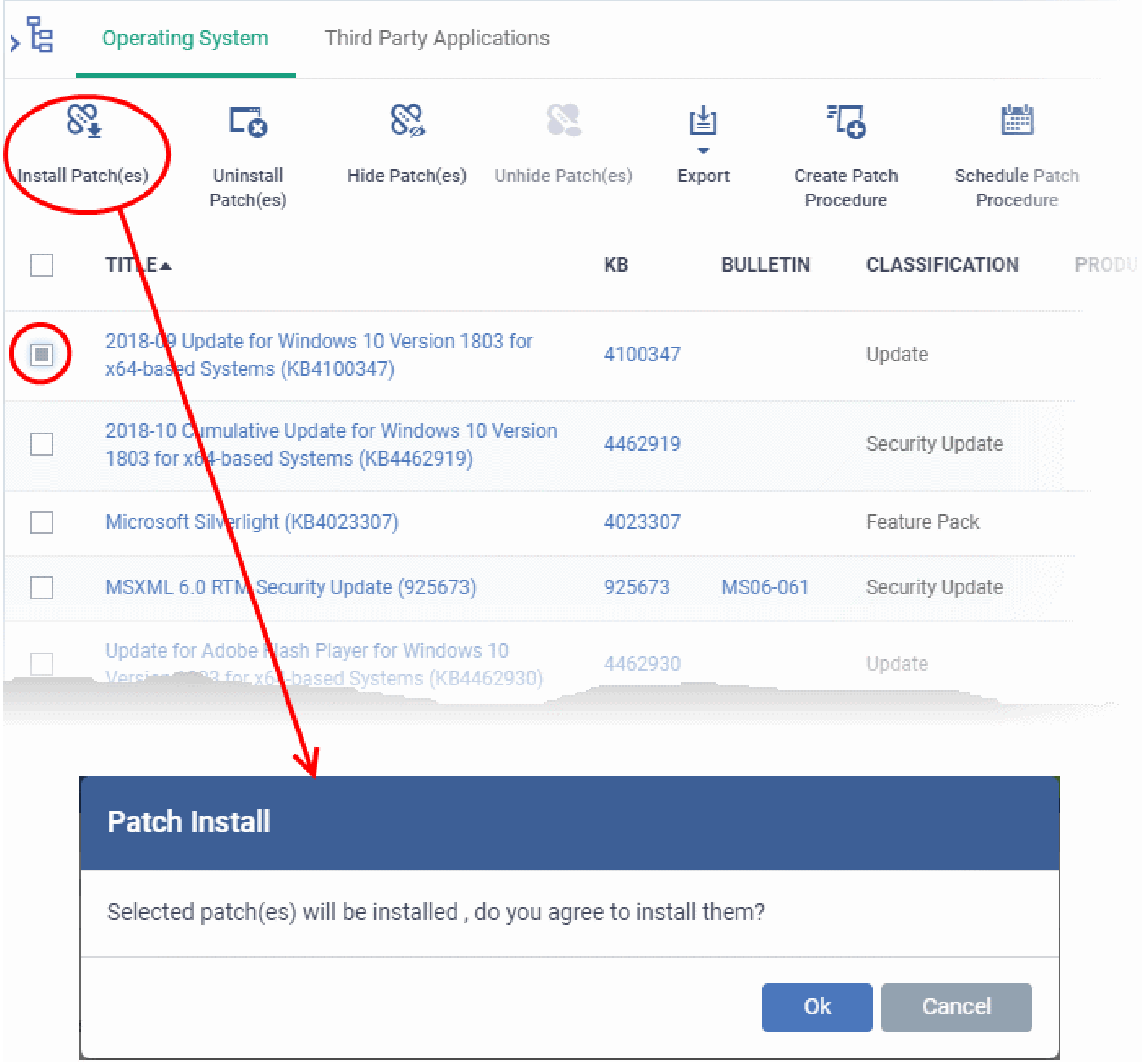
Selected patch(es) were successfully unhidden.

A confirmation message is displayed. The patches are re-added to the list.

## Install patch(es) on all managed endpoints at-once

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
    - Select a company or a group to view the list of patches and Windows updates available for its devices

      Or
    - Select 'Show all' to view a list of all available patches and Windows updates
- Select the patch(es) to be installed and click 'Install Patch(es)'



| | TITLE ▲ | KB | BULLETIN | CLASSIFICATION | PRODU |
|---|---|---|---|---|---|
| ▣ | 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347) | 4100347 | | Update | |
| □ | 2018-10 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4462919) | 4462919 | | Security Update | |
| □ | Microsoft Silverlight (KB4023307) | 4023307 | | Feature Pack | |
| □ | MSXML 6.0 RTM Security Update (925673) | 925673 | MS06-061 | Security Update | |
| □ | Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4462930) | 4462930 | | Update | |

**Patch Install**

Selected patch(es) will be installed , do you agree to install them?

- Click 'OK' in the confirmation dialog

The command will be sent and the selected patch(es) will be installed on all endpoint(s) in which the patch is not already installed.

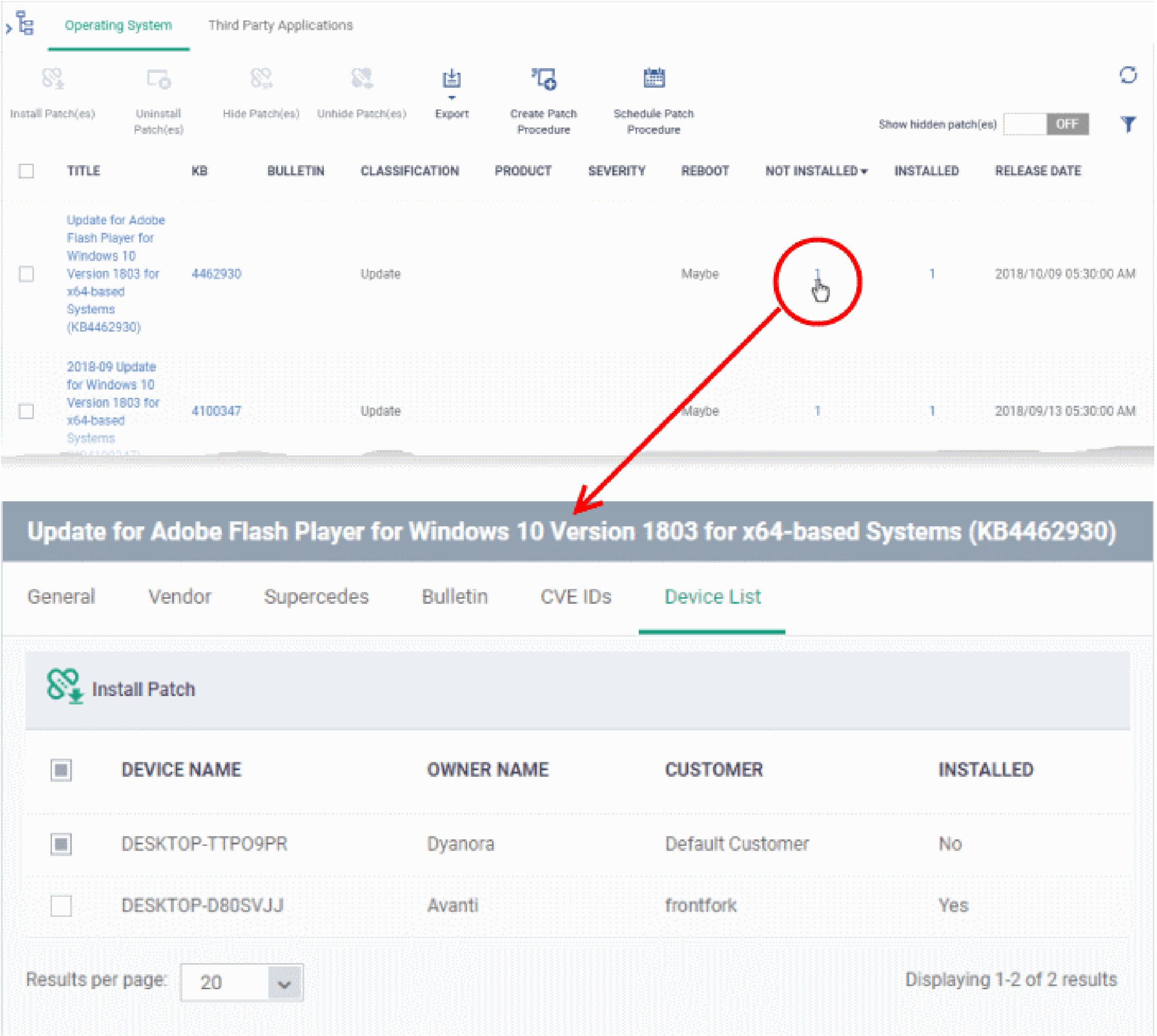
## Install a patch on selected endpoints

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
    - Select a company or a group to view the list of patches and Windows updates available for its devices

Or

- Select 'Show all' to view a list of all available patches and Windows updates

- Click the number in the 'Not Installed' column of the patch you want to install.



| TITLE | KB | BULLETIN | CLASSIFICATION | PRODUCT | SEVERITY | REBOOT | NOT INSTALLED | INSTALLED | RELEASE DATE |
|---|---|---|---|---|---|---|---|---|---|
| Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4462930) | 4462930 | | Update | | | Maybe | 1 | 1 | 2018/10/09 05:30:00 AM |
| 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347) | 4100347 | | Update | | | Maybe | 1 | 1 | 2018/09/13 05:30:00 AM |

Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4462930)

| DEVICE NAME | OWNER NAME | CUSTOMER | INSTALLED |
|---|---|---|---|
| DESKTOP-TTPO9PR | Dyanora | Default Customer | No |
| DESKTOP-D80SVJJ | Avanti | frontfork | Yes |

Results per page: 20

Displaying 1-2 of 2 results

The 'Patch Details' screen will open at the 'Device List' tab. The screen shows all managed devices to which the patch is relevant. The 'Installed' column tells whether the patch is installed on the device.

- Select the device(s) on which the patch is to be installed and click 'Install Patch'.

- A confirmation dialog will appear:

Patch(es) successfully added to install queue.

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

## Uninstall selected patches from all managed endpoints at-once

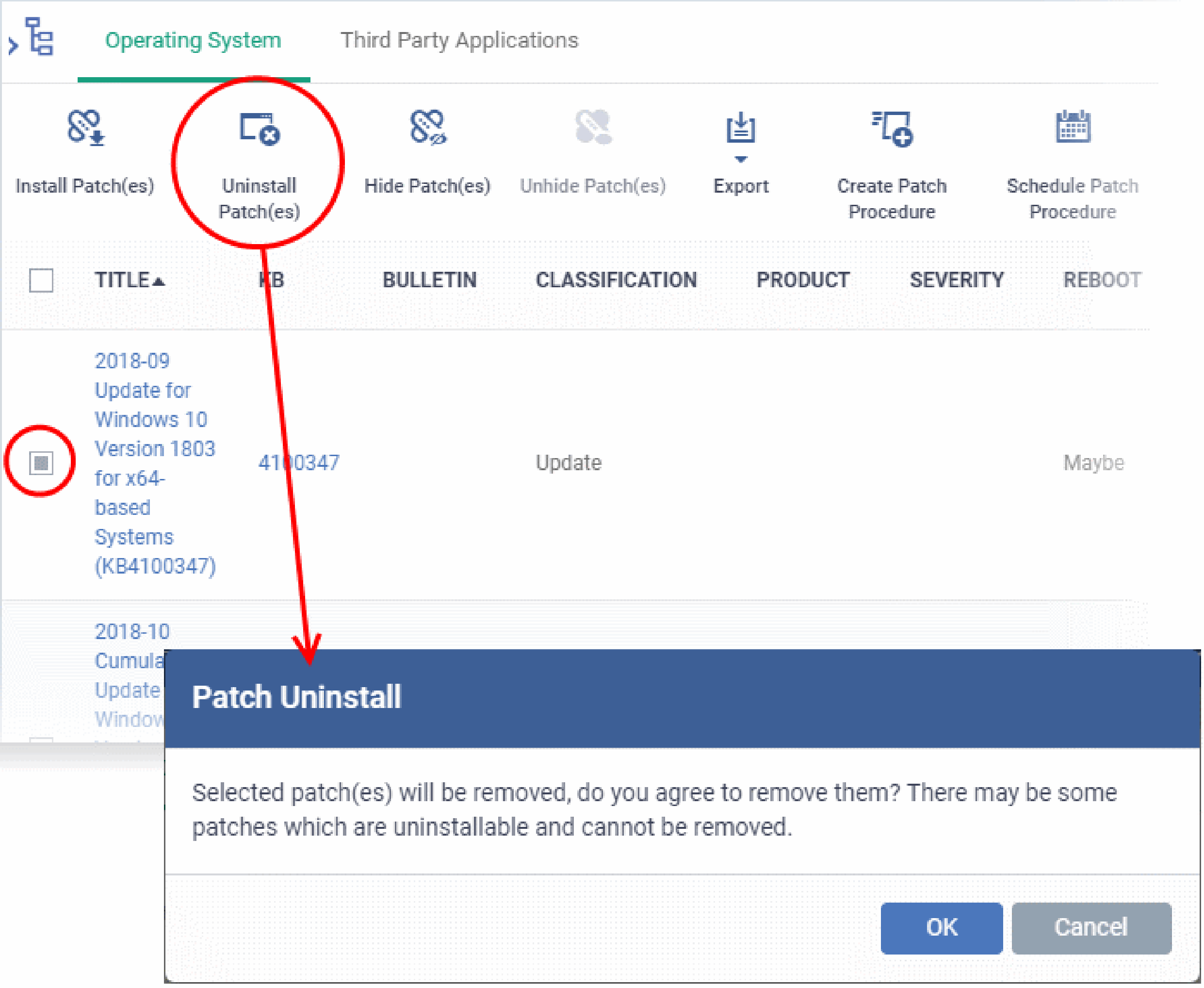
You can remove unwanted patches and Windows updates from the managed devices. This is useful if you want the managed endpoints to be rolled back to the previous build version of Windows component or the OS itself.

- Click 'Applications' > 'Patch Management'

- Select the 'Operating System' tab
    - Select a company or a group to view the list of patches and Windows updates available for its devices

    Or

    - Select 'Show all' to view a list of all available patches and Windows updates
- Select the patch(es) to be removed from the devices and click 'Uninstall Patch(es)'

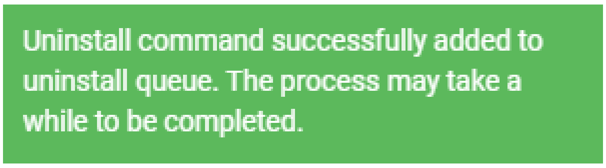


| □ | TITLE▲ | KB | BULLETIN | CLASSIFICATION | PRODUCT | SEVERITY | REBOOT |
|---|---|---|---|---|---|---|---|
| ▣ | 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347) | 4100347 | | Update | | | Maybe |
| | 2018-10 Cumula... Update... Window... | | | | | | |

Patch Uninstall

Selected patch(es) will be removed, do you agree to remove them? There may be some patches which are uninstallable and cannot be removed.

- Click 'OK ' in the confirmation dialog
- The command will be sent to the selected device(s) and a schedule will be created for uninstallation of the selected patch(es) on the devices.



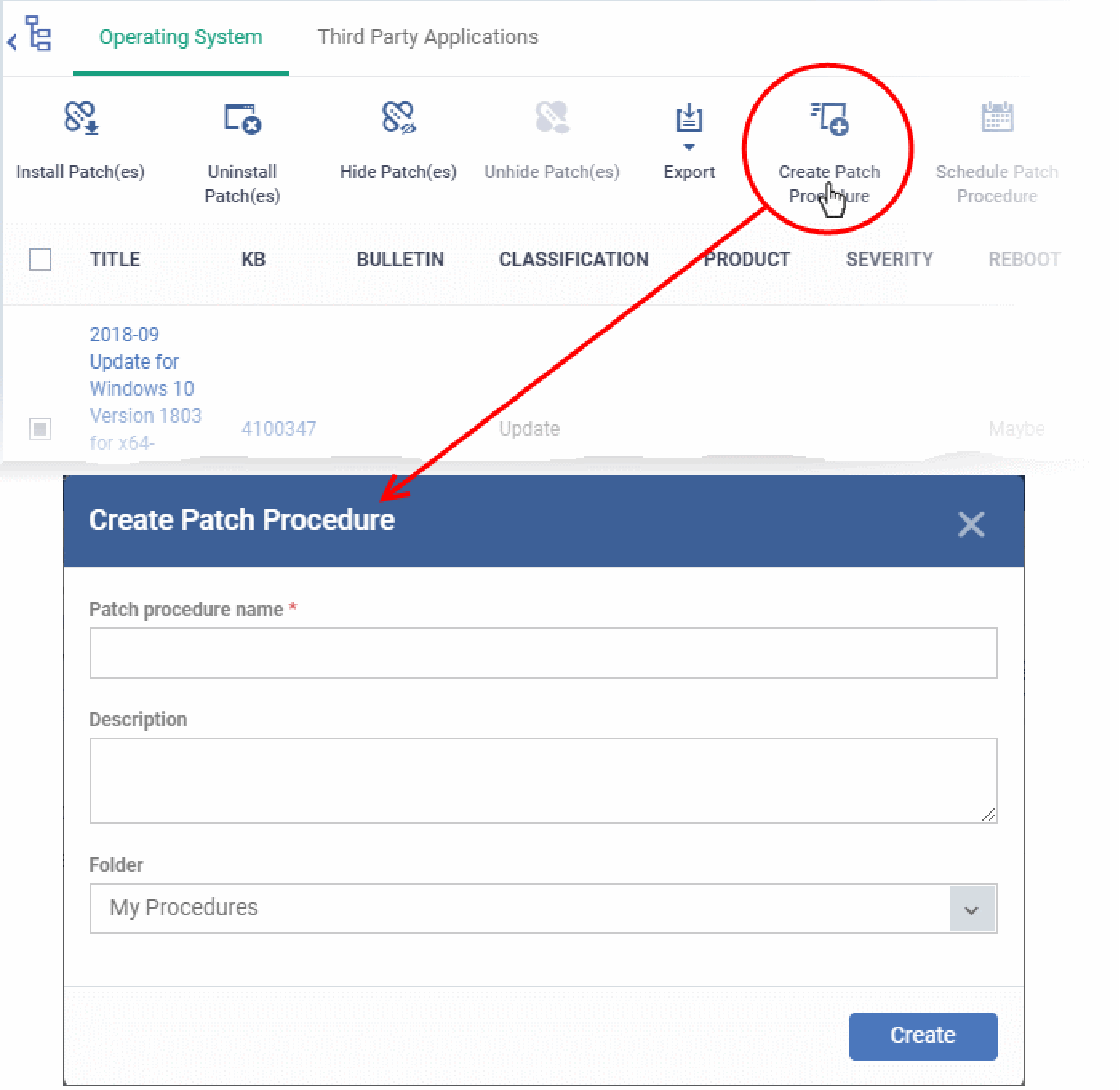
Uninstall command successfully added to uninstall queue. The process may take a while to be completed.

## Create a New Patch Procedure

- The 'Patch Management' > 'Operating System' interface lets you create a procedures to deploy OS patches.
- The procedures can be added to profiles and scheduled to run periodically.

**To create a new patch procedure**

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
- Click 'Create Patch Procedure' at the top



The 'Create Patch Procedure' wizard starts.

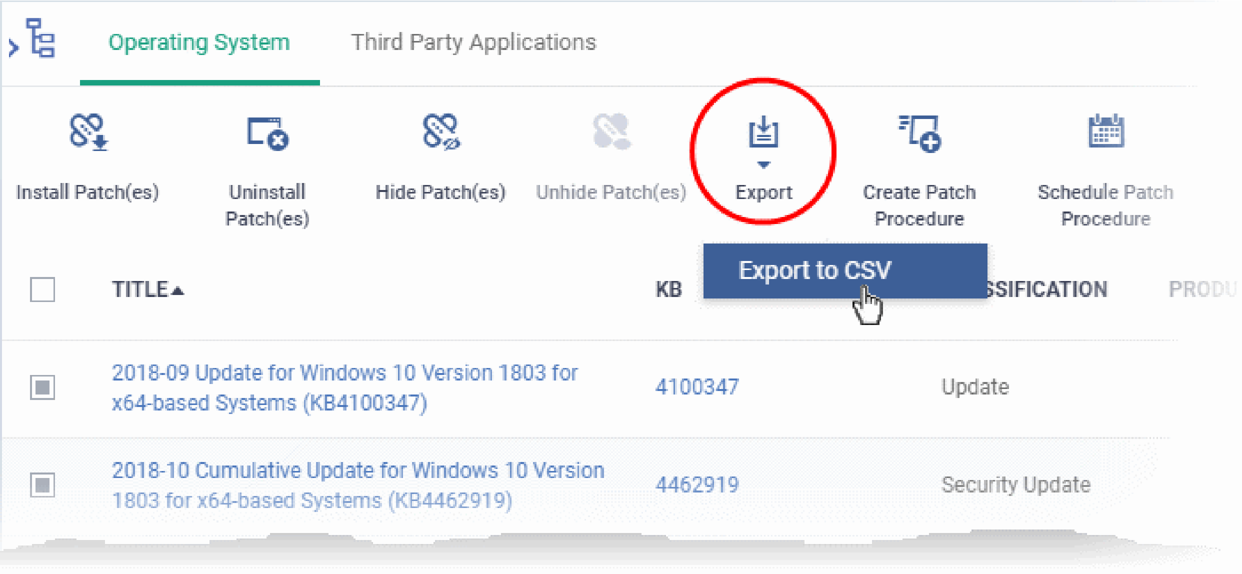
- Create a name and specify the storage folder for the procedure. Select the categories of OS patches you want to install and configure endpoint restart options.
- See **creating an OS patch procedure** for more help with the wizard.

### Search specific patches in the Patch Management interface

- Click the funnel icon on the right to filter patches by various criteria, including by name, by KB number, by bulletin number, by classification, by severity, and by whether a restart is required for the patches.
- Start typing the name of a patch in the search field to find a particular patch. Select the patch from the search suggestions and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.
- EM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

### Generate Patch Statuses Report

- Click 'Applications' > 'Patch Management'
- Select the 'Operating System' tab
- Click 'Export' at the top.



| TITLE | KB | SSIFICATION | PRODU |
|---|---|---|---|
| 2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347) | 4100347 | Update | |
| 2018-10 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4462919) | 4462919 | Security Update | |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See '**Reports**' in '**Dashboard**' for how to view and download reports.

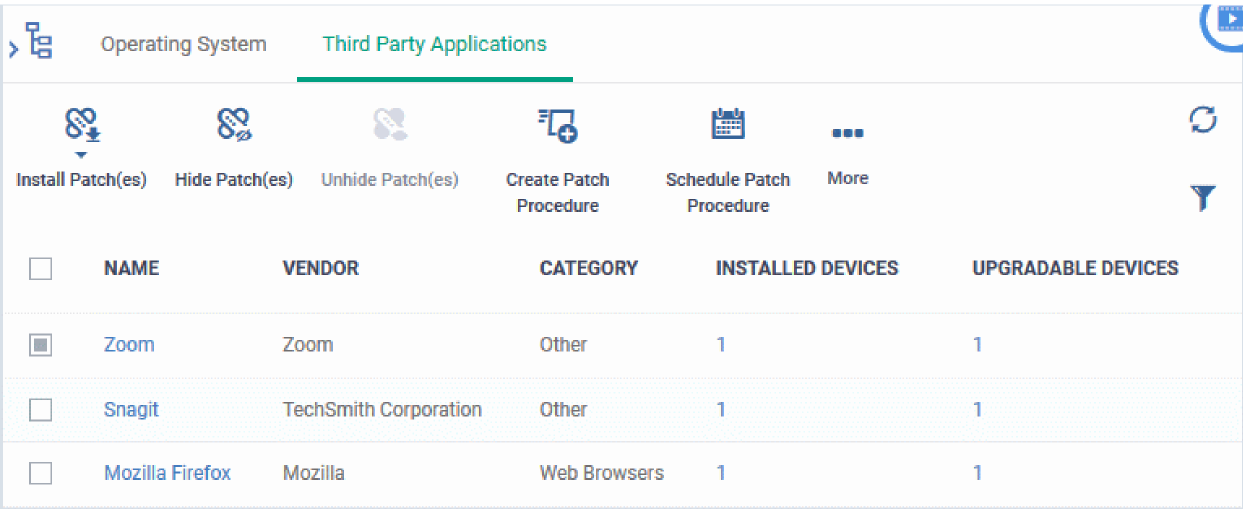
## 8.2.2. Install 3rd Party Application Patches on Windows Endpoints

- Click 'Applications' > 'Patch Management' > 'Third Party Applications'.
- This area lets you apply patches and updates to 3rd party applications on Windows devices.
- The interface lists all available patches along with details such as patch category, vendor name, and the number of devices which require the patch.
- You can filter patches by company and device group.
- You can hide those applications that you do not want to update.
  - Hidden applications will also not be available for update from the '**Device Management**' screen. They will also be skipped if named in a **patch procedure**.
  - Click 'Show hidden patch(es)' to view hidden items.
- You can also create new procedures to deploy updates and patches for all or selected 3rd party applications. The procedures can be added them to profiles with a schedule to periodically install new patches and updates available on every execution.

**To open the 'Third Party Applications' interface**

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
  - Select a company or a group to view the list of third party application patches and updates available for its devices

    Or
  - Select 'Show all' to view a list of all available third party application patches and updates



| ☐ | NAME | VENDOR | CATEGORY | INSTALLED DEVICES | UPGRADABLE DEVICES |
|---|---|---|---|---|---|
| ☑ | Zoom | Zoom | Other | 1 | 1 |
| ☐ | Snagit | TechSmith Corporation | Other | 1 | 1 |
| ☐ | Mozilla Firefox | Mozilla | Web Browsers | 1 | 1 |

- Each row shows the name of the software that needs to be updated. It also shows you how many devices have the software installed and how many of those require the update.
- You can apply updates to all devices or to individual devices:
  - Patch All - Use the check-boxes on the left to choose the software you want to patch. Click 'Install Patches' to apply the update to all devices which require patching.
  - Patch Individual - Click the number in the 'Upgradable Devices' row > Select the devices you want to update > Click 'Install Patches'

| Third Party Applications Table - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of the software.<br>• Click the name to view application details.<br>• See **View Details of an Application** for more details. |
| Vendor | The software publisher. |
| Category | The type of the application. Possible values include:<br>• Comodo Products<br>• Runtime applications<br>• Web Browsers<br>• Utilities<br>• Messaging<br>• File Compression utilities<br>• Developer Tools<br>• Documents<br>• Online Storage<br>• Other |
| Installed Devices | Total number of devices on which the application is installed. This figure includes devices with patched and unpatched versions of the software. |
| Upgradable Devices | Number of devices which need to be patched because they are using an older version |

| | |
|---|---|
| | of the software. |
| **Controls** | |
| Install Patch(es) | Allows you to install the patches/updates. |
| Hide Patch(es) | Allows you to hide selected patches that you do not want to update. Hidden patches will not be available for deployment on the 'Device Management' screen and will not be executed as well if added to a **patch procedure**. |
| Unhide Patch(es) | Allows you to unlock hidden patches. |
| Create Patch Procedure | Starts the wizard to create a new 3rd party application patch procedure.<br>You can create a new patch procedures to deploy updates and patches for all supported or selected 3rd party applications. The new procedures can be added to profiles and scheduled to install selected updates onto your endpoints. See **Create a New 3rd Party Application Patch Procedure** for more details. |
| Schedule Patch Procedure | Takes you to the 'Profiles' interface in Endpoint Manager. You create new or edit an existing Windows profile and add/edit the 'Procedures' component in it to create a schedule for running a patch installation procedure on endpoints on which the profile is active. See **Procedure Settings** in **Profiles for Windows Devices** for guidance on this. |
| Show hidden patch(es) | Allows you to view hidden patches and, if required, install them on endpoints. Use the toggle button to hide / view hidden applications. |

- Click any column header to sort items in ascending/descending order of entries in that column.
- Click the funnel icon on the right to search for applications by name, vendor and/or category.
- See '**EM Supported 3rd Party Applications**' for a full list of supported 3rd party applications.

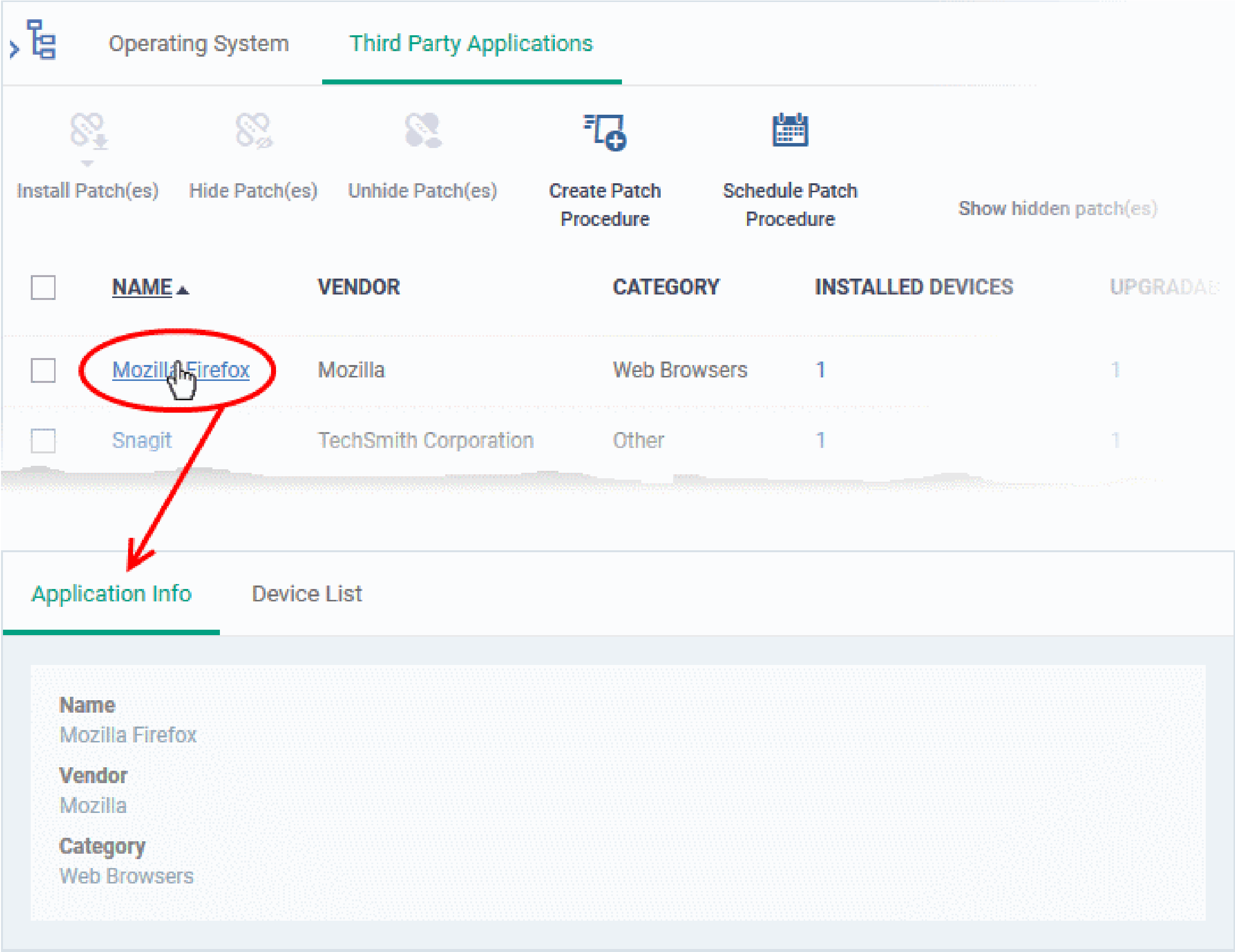
The 'Patch Management' > 'Third Party Applications' interface allows you to:

- **View Details of an Application**
- **Hide Applications**
- **Restore Hidden Applications**
- **Update selected applications on all upgradable devices at once**
- **Update an application on selected devices**
- **Create a New 3rd Party Application Patch Procedure**

## View Details of an Application

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
    - Select a company or a group to view the list of third party application patches and updates available for its devices

      Or
    - Select 'Show all' to view a list of all available third party application patches and updates
- Click the name of any application to open its application details screen



| □ | NAME ▲ | VENDOR | CATEGORY | INSTALLED DEVICES | UPGRADAB |
|---|---|---|---|---|---|
| □ | Mozilla Firefox | Mozilla | Web Browsers | 1 | 1 |
| □ | Snagit | TechSmith Corporation | Other | 1 | 1 |

Name
Mozilla Firefox
Vendor
Mozilla
Category
Web Browsers

The details of the application are displayed under two tabs:

- **General** - Displays the name, software publisher and the category of the application.
- **Device List** - Displays the list of managed devices on which the application is installed, with the details like the installed version, installation path and the device owner. You can update the application on the devices where required from this screen. See **Update an Application On Selected Devices** for more details.

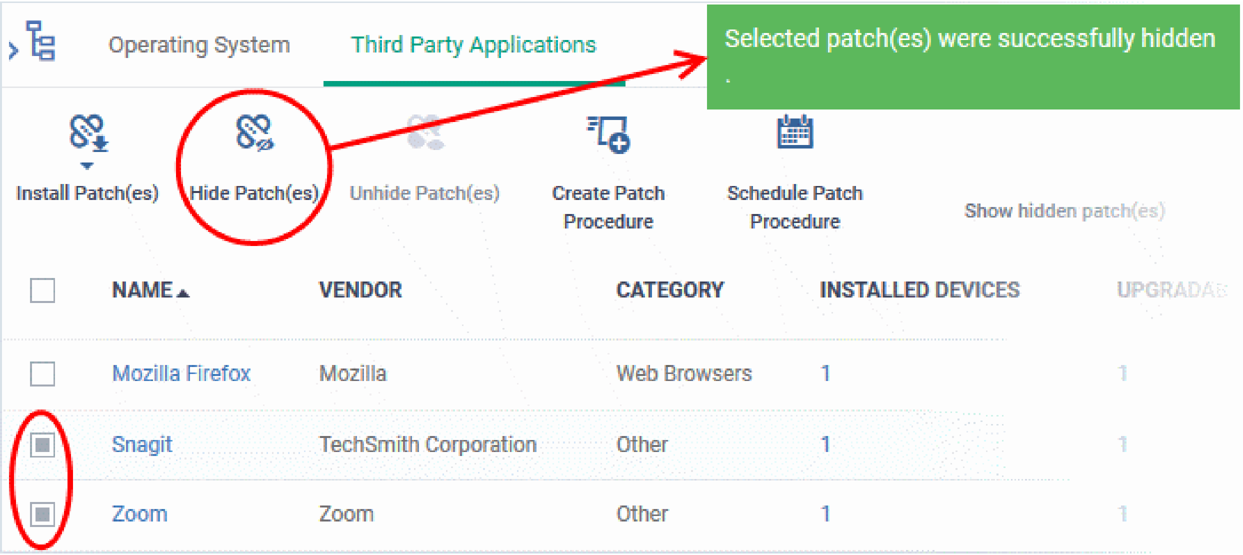
## Hide Applications

- You can hide those applications that you do not want to update
- These applications will also be not available for update from the '**Device Management**' screen and will not be executed as well if added to a **patch procedure**.
- You can view the hidden applications by using the 'Show hidden patch(es) toggle button and update these applications on selected on devices.

**To hide upgradable applications**

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
  - Select a company or a group to view the list of third party application patches and updates available for its devices

    Or
  - Select 'Show all' to view a list of all available third party application patches and updates
- Select the application(s) to be hidden from the list and click 'Hide Patch(es)'



| □ | NAME ▲ | VENDOR | CATEGORY | INSTALLED DEVICES | UPGRADAB |
|---|---|---|---|---|---|
| □ | Mozilla Firefox | Mozilla | Web Browsers | 1 | 1 |
| ▣ | Snagit | TechSmith Corporation | Other | 1 | 1 |
| ▣ | Zoom | Zoom | Other | 1 | 1 |

A confirmation is displayed. The selected applications are hidden from the list.

- To view the hidden applications, use the 'Show hidden patch(es)' switch on the top right
- To re-add the hidden applications to the list, you have to **unhide** them.

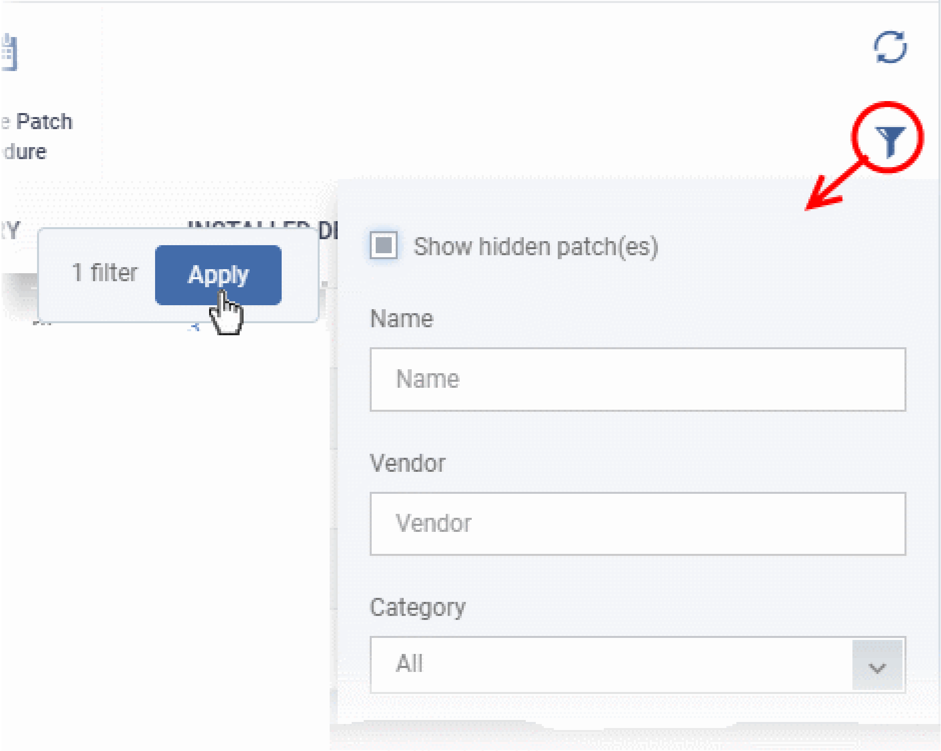
## Restore Hidden Applications

- You can make the hidden applications to be re-added to the 'Third Party Applications' interface.
- Restored applications will also be available for being updated from the **Device Management** interface and can be added to a **patch procedure.**

### View hidden upgradable applications and restore them

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
  - Select a company or a group to view the list of third party application patches and updates available for its devices

    Or
  - Select 'Show all' to view a list of all available third party application patches and updates
- Click the funnel icon on the right, select 'Show hidden patch(es)' and click 'Apply'



☐ Show hidden patch(es)

Name

Name

Vendor

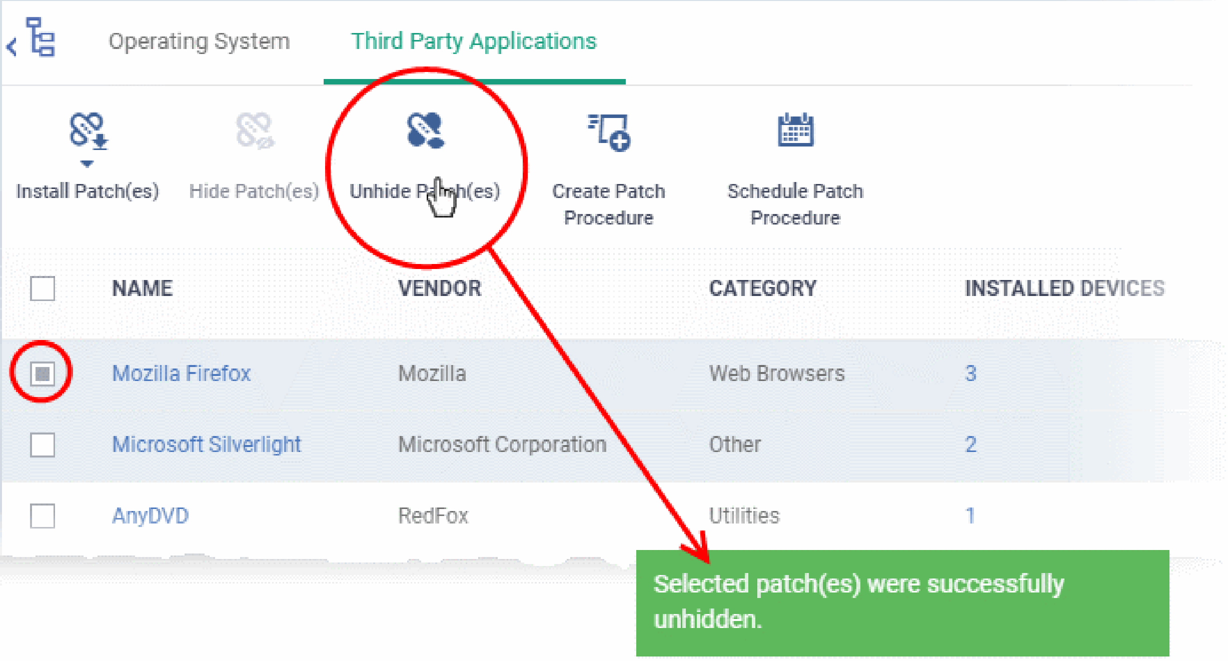
Vendor

Category

All

The hidden applications are shown with dark gray background stripe.

- Select the hidden app(s) from the list and click 'Unhide Patch(es)'



| ☐ | NAME | VENDOR | CATEGORY | INSTALLED DEVICES |
|---|---|---|---|---|
| ☐ | Mozilla Firefox | Mozilla | Web Browsers | 3 |
| ☐ | Microsoft Silverlight | Microsoft Corporation | Other | 2 |
| ☐ | AnyDVD | RedFox | Utilities | 1 |

Selected patch(es) were successfully unhidden.

A confirmation is displayed. The applications are re-added to the list.

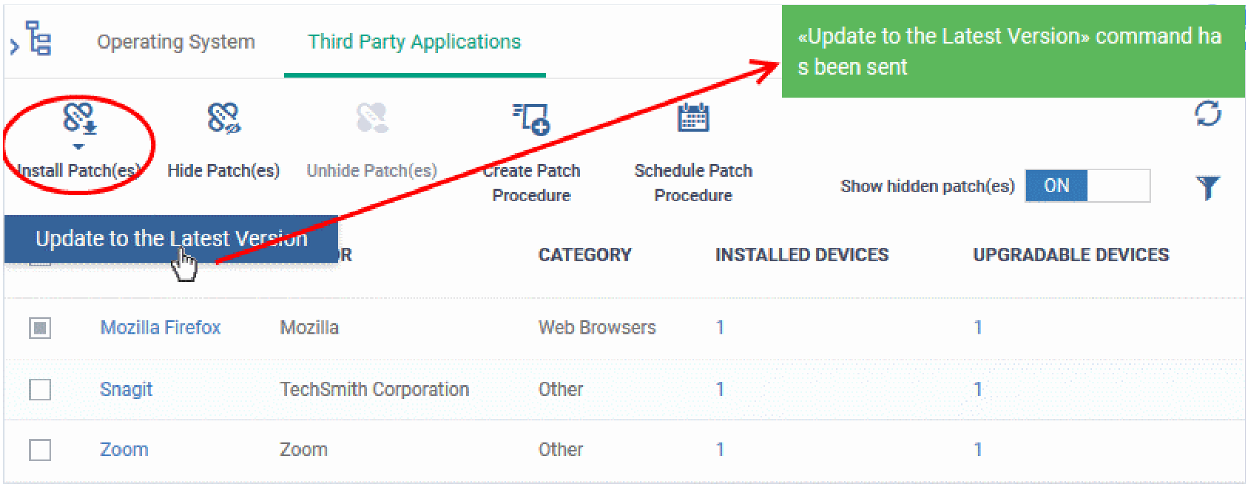
## Update Selected Applications on All Upgradable Devices at once

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
  - Select a company or a group to view the list of third party application patches and updates available for its devices

Or

  - Select 'Show all' to view a list of all available third party application patches and updates

- Select the application(s) to be updated, click 'Install Patch(es)' and choose 'Update to Latest Version'



| | | R | CATEGORY | INSTALLED DEVICES | UPGRADABLE DEVICES |
|---|---|---|---|---|---|
| ☒ | Mozilla Firefox | Mozilla | Web Browsers | 1 | 1 |
| □ | Snagit | TechSmith Corporation | Other | 1 | 1 |
| □ | Zoom | Zoom | Other | 1 | 1 |

A command is sent to Communication Client (CC) on the devices to commence the update.

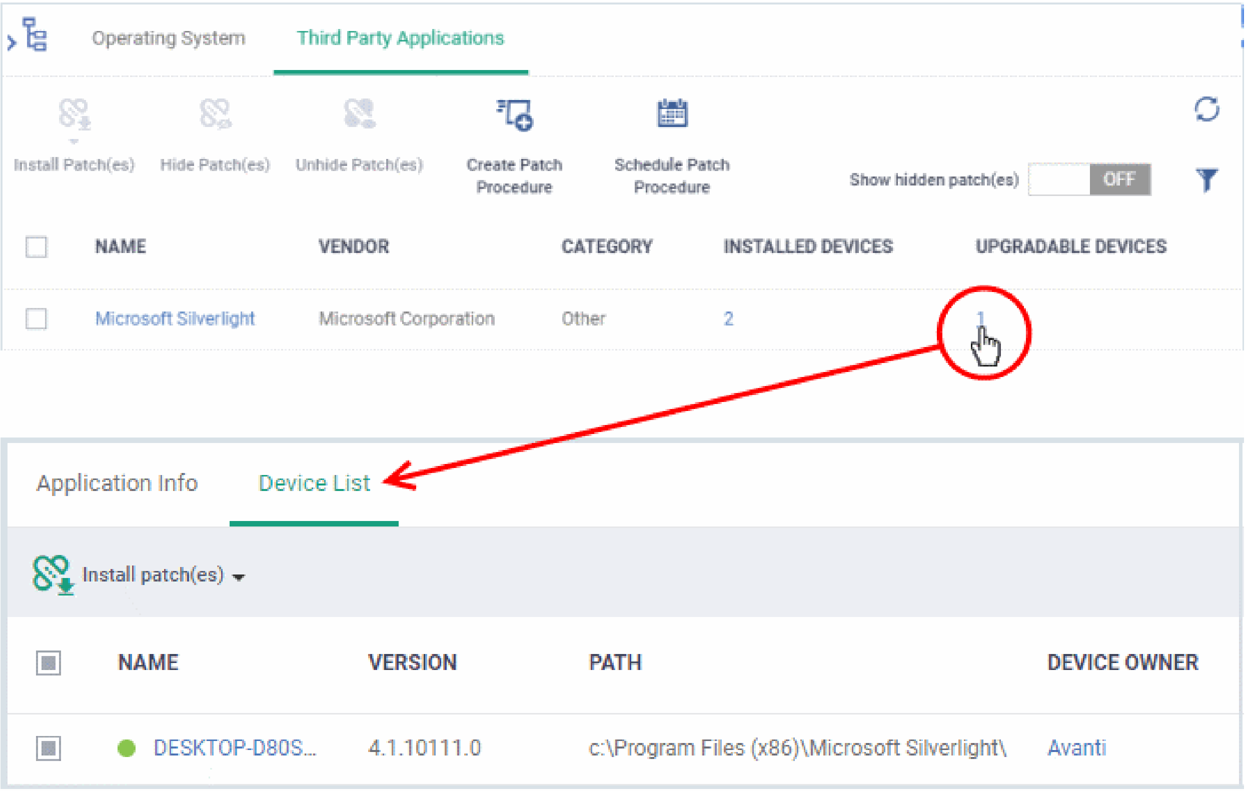
- Once the command is received, CC checks whether the update has already been downloaded by other devices in the network.
  - If the update is available, CC establishes a peer-to-peer network with the device and downloads the patch. This reduces bandwidth usage as the update is downloaded from the local network.
  - If the update is not available on any devices in the local network, CC downloads the update from the EM patch portal.

## Update an Application on Selected Devices

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
  - Select a company or a group to view the list of third party application patches and updates available for its devices

    Or

  - Select 'Show all' to view a list of all available third party application patches and updates
- Click the number in the 'Upgradable Devices' column of the application to be updated



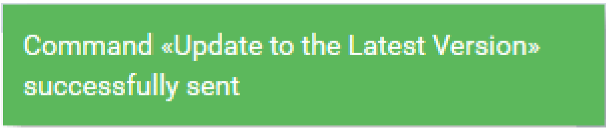
| □ | NAME | VENDOR | CATEGORY | INSTALLED DEVICES | UPGRADABLE DEVICES |
|---|---|---|---|---|---|
| □ | Microsoft Silverlight | Microsoft Corporation | Other | 2 | 1 |

| ■ | NAME | VERSION | PATH | DEVICE OWNER |
|---|---|---|---|---|
| ■ | ● DESKTOP-D80S... | 4.1.10111.0 | c:\Program Files (x86)\Microsoft Silverlight\ | Avanti |

The application details screen will appear with the 'Device List' tab open, with a list of devices on which the application can be updated.

- Select the device(s) on which the application is to be updated
- Click 'Install patch(es)' and choose 'Update to Latest Version'

A command will be sent to the endpoint(s) to schedule installation of the patch/update the application to the latest version.



Command «Update to the Latest Version» successfully sent

A command is sent to Communication Client (CC) on the devices to commence the update.

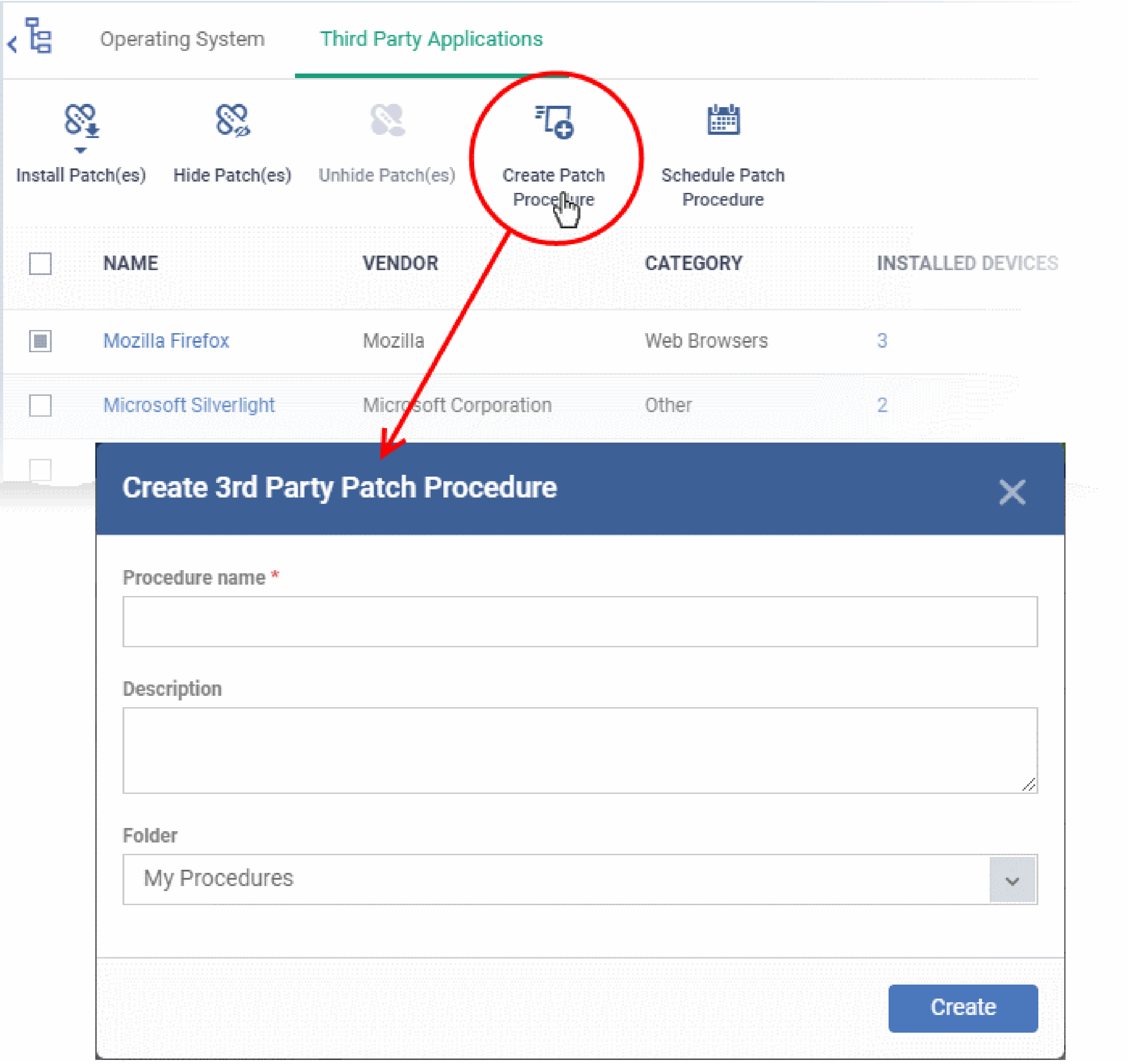
- Once the command is received, CC checks whether the update has already been downloaded by other devices in the network.
  - If the update is available, CC establishes a peer-to-peer network with the device and downloads the patch. This reduces bandwidth usage as the update is downloaded from the local network.
  - If the update is not available on any devices in the local network, CC downloads the update from the EM patch portal.

## Create a New 3rd Party Application Patch Procedure

- The 'Patch Management' > 'Third Party Applications' interface allows you to create a new patch procedures for periodical updates and deployment of patches for all or selected 3rd party applications.
- The procedures can be added to profiles and scheduled to run periodically.
- The new patches and updates available for the selected applications are deployed on the endpoints to which the profile is applied during every execution of the procedure.

**To create a new procedure**

- Click 'Applications' > 'Patch Management'
- Select the 'Third Party Applications' tab
- Click 'Create Patch Procedure' on the top



| NAME | VENDOR | CATEGORY | INSTALLED DEVICES |
|---|---|---|---|
| Mozilla Firefox | Mozilla | Web Browsers | 3 |
| Microsoft Silverlight | Microsoft Corporation | Other | 2 |

Create 3rd Party Patch Procedure

Procedure name *

Description

Folder: My Procedures

The 'Create 3rd Party Patch Procedure' wizard starts.

- The wizard allows you to set a name for the procedure, select the folder in which it is to be stored, select the applications to be updated and configure the restart options for the endpoints after the installation of the updates.
- Please see the **explanation of creating an 3rd party application patch procedure** in **Create a Custom Procedure** for detailed guidance on the wizard.

### 8.2.2.1. EM Supported 3rd Party Applications

The following table provides the names of third party applications that can be updated on enrolled Windows endpoints:

- 7-Zip
- ActivePresenter
- Glary Utilities PRO
- GlassWire
- PicPick
- PKZIP for Windows

- ActiveState Komodo Edit
- Adblock Plus for IE
- Adobe Acrobat Reader DC
- Adobe AIR
- Adobe Digital Editions
- Adobe Flash Player ActiveX
- Adobe Flash Player NPAPI
- Adobe Flash Player PPAPI
- Adobe Shockwave Player
- Advanced Installer
- Advanced IP Scanner
- AIMP
- AirDroid
- AirParrot
- AirServer Universal
- Ant Movie Catalog
- Ant Renamer
- AnyBurn
- AnyDVD
- AppGate Client
- AppInventor Setup
- Apple Application Support
- Apple Application Support (64-bit)
- Apple Mobile Device Support
- Apple Software Update
- Audacity
- Aurora Blu-ray Media Player
- Auslogics Browser Care
- Auslogics Disk Defrag
- Auslogics Duplicate File Finder
- Auslogics Registry Cleaner
- Auslogics Registry Defrag
- AutoIt
- Avant Browser
- AVS Document Converter
- AVS Image Converter
- AVS Media Player
- GlobalMapper
- GOM Audio
- GOM Player
- GoodSync
- Google Chrome
- Google Drive
- Google Earth
- Google Earth Pro
- GPL Ghostscript
- grepWin
- HardCopy Pro
- HeliosPaint
- HelpNDoc Personal Edition
- HipChat
- Honeycam
- Honeyview
- HttpWatch Basic
- Hugin
- IE7Pro
- IIS
- ImgBurn
- InfoSlips ForMe Viewer
- iReport
- IrfanView
- iTunes
- IZArc
- JabraDirect
- Java(TM) Update
- Java SE Development Kit
- jing
- Jitsi
- JRE
- K-Lite Codec Pack Basic
- K-Lite Codec Pack Full
- K-Lite Codec Pack Standard
- K-Lite Mega Codec Pack
- KeePass Password Safe 1
- KeePass Password Safe 2
- Kerio Outlook Connector
- Plantronics Hub Software
- Plex Media Server
- PNotes.NET
- Poedit
- PotPlayer
- PrimoPDF
- PrintKey-Pro
- proCertum CardManager
- Progress Telerik Fiddler
- PSPad editor
- PuTTY release
- qBittorrent
- QTranslate
- QuickBooks Desktop File DoctorQuickTime 7
- RD Tabs
- Recuva
- Reflector
- RenWeb.com
- Revo Uninstaller
- Revo Uninstaller Pro
- R for Windows
- RingCentral for Windows
- RJ TextEd
- RStudio
- Safari
- Sandboxie
- SciTE Text Editor
- ScreenConnect
- Screenpresso
- Scribus
- SeaMonkey
- ShadowCopy
- Silverjuke
- SimplySign Desktop
- Skype
- Slik Subversion
- SmartCam
- Smart Defrag

- AVS Video Editor
- AxCrypt
- AXIS Media Control Embedded Installer
- Bandicut
- Bandizip
- Belarc Advisor
- Beyond Compare
- Bing Desktop
- BitComet
- BitLord
- Blender
- Blio
- Bluebeam Vu
- Blue Jeans
- Bullzip PDF Printer
- Cabos
- calibre
- CCleaner
- CCleanerPro
- CDBurnerXP
- Chilkat ActiveX
- Citrix Group Policy Management
- Citrix Receiver
- Citrix ShareFile Sync
- Classic Shell
- Code42 server
- CollageIt
- Collagerator
- Combined Community Codec Pack
- Comodo IceDragon
- Remote Control by ITarian
- Converber
- CPUID CPU-Z
- CrashPlan
- CryptoPrevent
- CrystalDiskInfo
- CutePDF Writer
- Kingsoft Office 2013
- Kobo
- Krita
- LibreOffice
- Lightshot
- Linphone
- Logitech SetPoint
- LogMeIn Client
- LogMeIn Hamachi
- Malwarebytes
- MathType
- McAfee Security Scan Plus
- MediaInfo
- MediaMonkey
- Media Player Classic Home
- MeshLab_64b 2016
- Microsoft AntiXSS
- Microsoft Baseline Security Analyzer
- Microsoft Power BI Desktop
- Microsoft PowerPoint Viewer
- Microsoft Security Client
- Microsoft Silverlight
- Microsoft SQL Server 2008 R2 Native Client
- Microsoft SQL Server 2017 T-SQL Language Service
- Microsoft Sync Framework Runtime v1.0 SP1
- Microsoft Visio Viewer 2013
- Microsoft Visual C++ 2008 Redistributable
- Microsoft Visual C++ 2012 Redistributable
- Microsoft Visual C++ 2017 x86 Additional Runtime
- Microsoft Visual Studio Code
- Microsoft Web Deploy
- MimioStudio
- Miranda IM
- Spark
- Speccy
- Spiceworks Desktop
- SplashID Safe
- Splashtop Streamer
- Spybot - Search & Destroy
- Steam
- Sticky Password
- SugarSync
- SumatraPDF
- SyncBackFree
- Synology Surveillance Station Client
- Tableau Reader
- TeamSpeak Client
- TeamViewer
- TED Notepad
- Tekla BIMsight
- TenClips
- TeraCopy
- TestNav
- TextPad
- TIBCO Jaspersoft Studio final
- TightVNC
- TomTom HOME
- TortoiseSVN
- TortoiseGit
- TOSHIBA Password Utility
- TreeSize Free
- Trillian
- TSPrint Client
- TSR Watermark Image software version - Free version
- UltraVnc
- UniPDF
- Universal Extractor
- Unlocker
- Uplay

- Cyberduck
- D&D Interceptor
- DC++
- Defraggler
- Desktop Restore
- DisplayCAL
- DriveImage XML
- Druva inSync
- Dual Monitor Tools
- DU Meter
- Duplicate Cleaner Pro
- DVD Flick
- DYMO Label
- Easy 7-Zip
- Easy Thumbnails
- EditPad Lite
- eM Client
- eMuleTorrent
- EncryptOnClick
- EPI
- Epic Games Launcher
- EPIM-Outlook Sync
- EssentialPIM
- Evernote
- exacqVision Client
- Exact Audio Copy
- Exsate VideoExpress
- FastStone Capture
- FastStone Image Viewer
- FileZilla Client
- Firebird
- FlashGet
- Foobar
- Fotosizer
- Foxit Advanced PDF Editor
- Foxit PhantomPDF
- Foxit Reader
- FreeFixer
- Free RAR Extract Frog
- MobaXterm
- MongoDB
- Mozilla Firefox en-GB
- Mozilla Firefox en-US
- Mozilla Firefox ESR
- Mozilla Thunderbird
- MozyHome
- MozyPro
- Mp3tag
- MSXML 4.0 SP3 Parser
- Mumble
- MX5
- MyDefrag
- MySQL Connector/C
- MySQL Connector/ODBC
- MySQL Installer - Community
- MySQL Notifier
- MySQL Workbench 6.3 CE
- NeoLoad
- NetBeans IDE
- NetSetMan
- Nextcloud
- Nitro Pro
- Node.js
- NoMachine
- Notepad++
- NoteTab Light
- nPassword
- OCS Inventory NG Agent
- OpenOffice
- Opera Stable
- Oracle VM VirtualBox
- Origin
- ownCloud
- paint.net
- Pale Moon
- Parallels Client
- pCon.planner STD
- VirtualCloneDrive
- VitalSource Bookshelf
- VLC media player
- VMware Horizon Client
- VMware Player
- VMware vCenter Converter Standalone
- VNC Enterprise Edition
- VNC Server
- VNC Viewer
- VSDC Free Video Editor version
- VulkanSDK
- VyprVPN
- Waterfox
- Wave Editor
- WebStorage
- WildTangent Games App
- Winamp
- WinDjView
- Windows Live Sync
- Windows Movie Maker
- Windows Phone app for desktop
- WinHTTrack Website Copier
- WinMerge
- WinRAR
- WinSCP
- WinSnap
- WinZip
- Wireshark
- Wise AD Cleaner
- Wise Care 365
- Wise Disk Cleaner
- Wise Folder Hider
- Wise Force Deleter
- Wise Memory Optimizer
- Wise Registry Cleaner
- XAMPP
- XMind

- FrontMotion Firefox Community Edition (en-US)
- Frontmotion Firefox Community Edition ESR
- FSASecureBrowser
- GetGo Download Manager
- gImageReader
- GIMP
- Git version
- Glary Utilities
- PDF-Viewer
- PDF-XChange Editor
- PDF24 Creator
- PDFCreator
- PDFill FREE PDF Tools
- PDFsam Basic
- PDFTools Version
- PeaZip
- Personal Backup
- PhotoFilmStrip
- XnConvert
- XnView
- Xvid Video Codec
- Zimbra Connector for Microsoft Outlook
- Zimbra Desktop
- ZIPI
- Zoiper
- Zoom
- Zoom Player
- Zotero

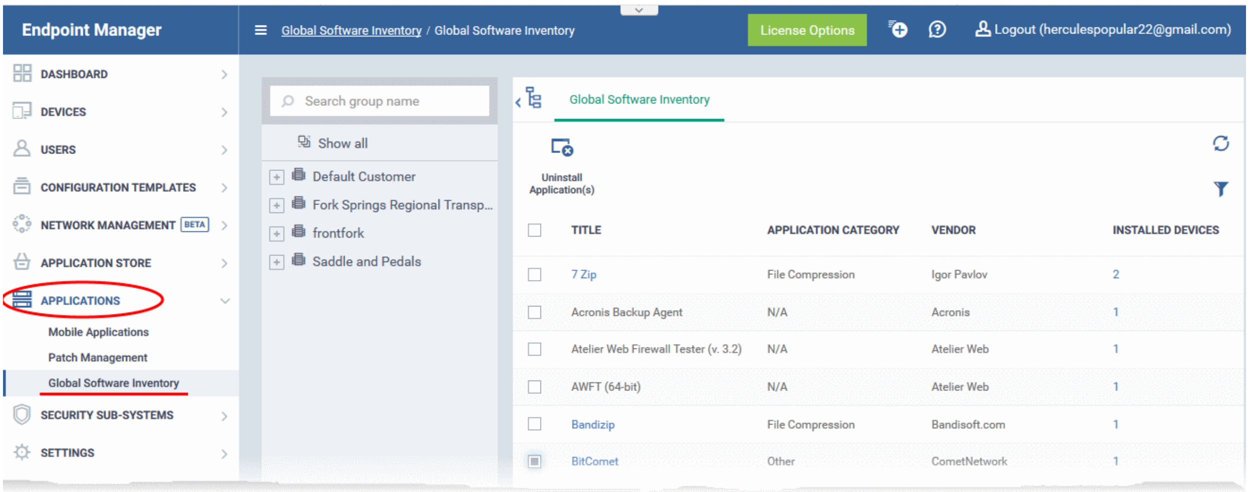
## 8.3. View and Manage Applications Installed on Windows Devices

- Click 'Applications' > 'Global Software Inventory'
- The global software inventory shows all applications installed on managed Windows devices.
- The interface also shows details about each application. Details include the software vendor and the number of devices on which the app is installed.
- You can have the option to uninstall applications from *all* Windows devices at-once

**To open the 'Global Software Inventory' interface**

- Click 'Applications' > 'Global Software Inventory'
  - Select a company or group on the left to view applications installed on devices in it

    Or
  - Select 'Show all' to view applications on every Windows device enrolled to Endpoint Manager



| TITLE | APPLICATION CATEGORY | VENDOR | INSTALLED DEVICES |
|---|---|---|---|
| 7 Zip | File Compression | Igor Pavlov | 2 |
| Acronis Backup Agent | N/A | Acronis | 1 |
| Atelier Web Firewall Tester (v. 3.2) | N/A | Atelier Web | 1 |
| AWFT (64-bit) | N/A | Atelier Web | 1 |
| Bandizip | File Compression | Bandisoft.com | 1 |
| BitComet | Other | CometNetwork | 1 |

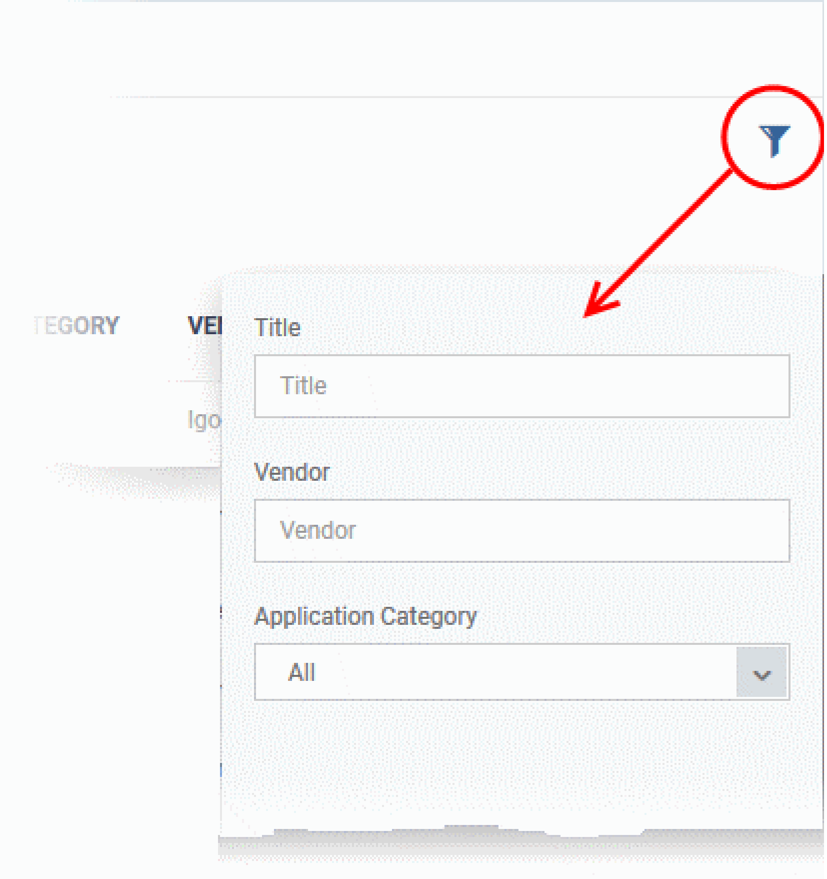
| Global Software Inventory - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Title | Label of the application.<br>• Click the name of an application to view its details and a list of endpoints on which it is installed.<br>• The app details screens also lets you uninstall the application from devices.<br>• See **View Details of an Application** for more details. |
| Application Category | The genre of the application. For example, 'Productivity', 'Security', 'Entertainment' etc. |
| Vendor | The publisher of the software/application |
| Installed Devices | The number of devices on which the app is installed currently. |
| **Controls** | |
| Uninstall | Uninstalls the selected application from all Windows devices at-once. See **Remotely Uninstall an Application from all Devices** for more details. |

The global software inventory lets you:

- **View details of an application**
- **Remotely uninstall an application from selected devices**
- **Remotely uninstall an application from all devices**

## Sorting and Filtering Options

- Click any column header to sort the items in ascending or descending order
- Click the funnel button at the right end to open the filter options.



## View Details of an Application

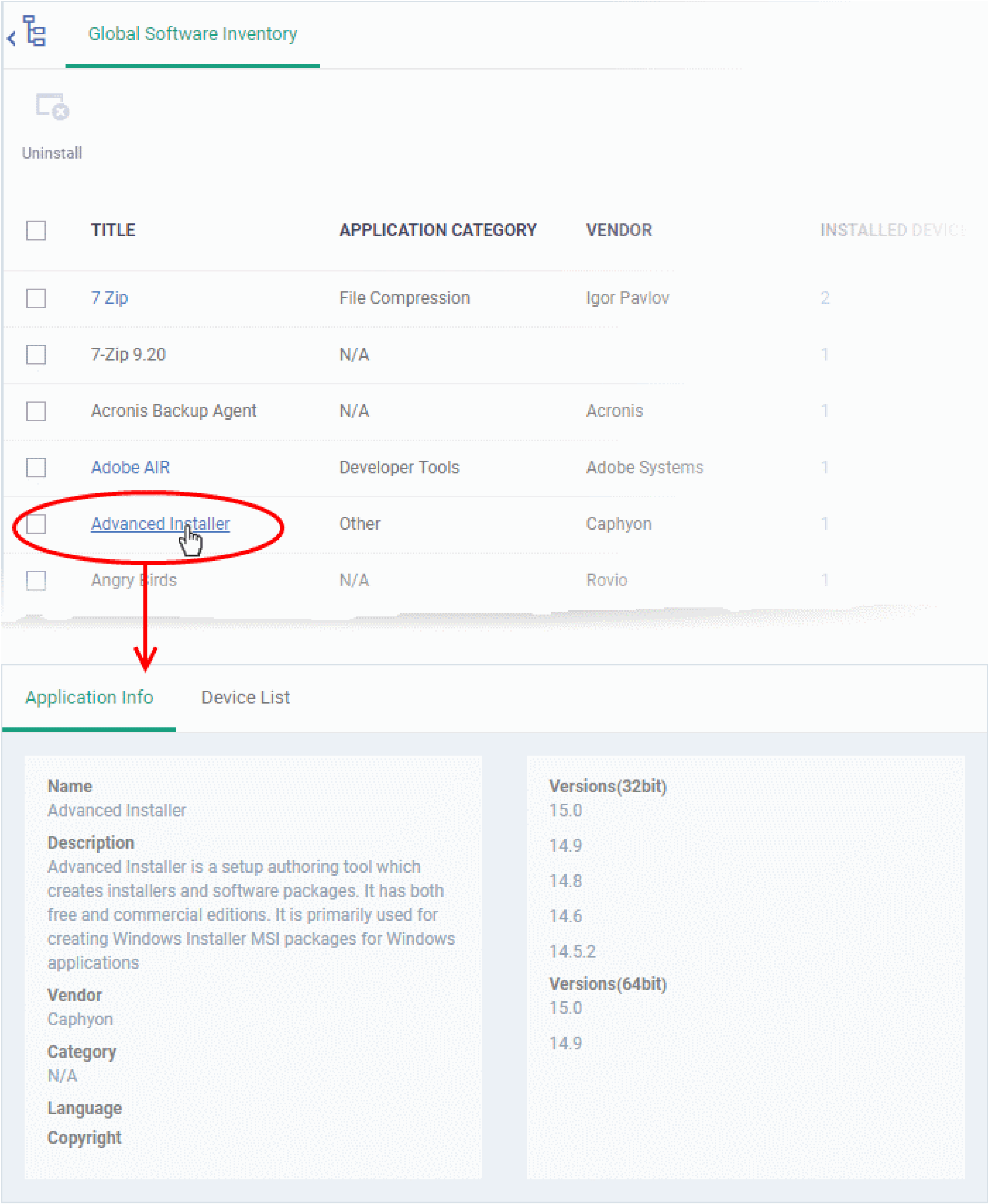
The 'Global Software Inventory' interface allows you to view the information about an application and the list of devices on which it is found. You can also remove the application from selected devices on which it is not required.

**Note**: The application details is available only for applications supported by EM. See **EM Supported 3rd Party Applications** to view the list of supported applications.

### View the details of an application

- Click 'Applications' > 'Global Software Inventory'
  - Select a company or group on the left to view applications installed on devices in it

    Or
  - Select 'Show all' to view applications on every Windows device enrolled to EM
- Click on the name of a supported application to view its details



| □ | TITLE | APPLICATION CATEGORY | VENDOR | INSTALLED DEVICE |
|---|---|---|---|---|
| □ | 7 Zip | File Compression | Igor Pavlov | 2 |
| □ | 7-Zip 9.20 | N/A | | 1 |
| □ | Acronis Backup Agent | N/A | Acronis | 1 |
| □ | Adobe AIR | Developer Tools | Adobe Systems | 1 |
| □ | Advanced Installer | Other | Caphyon | 1 |
| □ | Angry Birds | N/A | Rovio | 1 |

**Name**
Advanced Installer

**Description**
Advanced Installer is a setup authoring tool which creates installers and software packages. It has both free and commercial editions. It is primarily used for creating Windows Installer MSI packages for Windows applications

**Vendor**
Caphyon

**Category**
N/A

**Language**

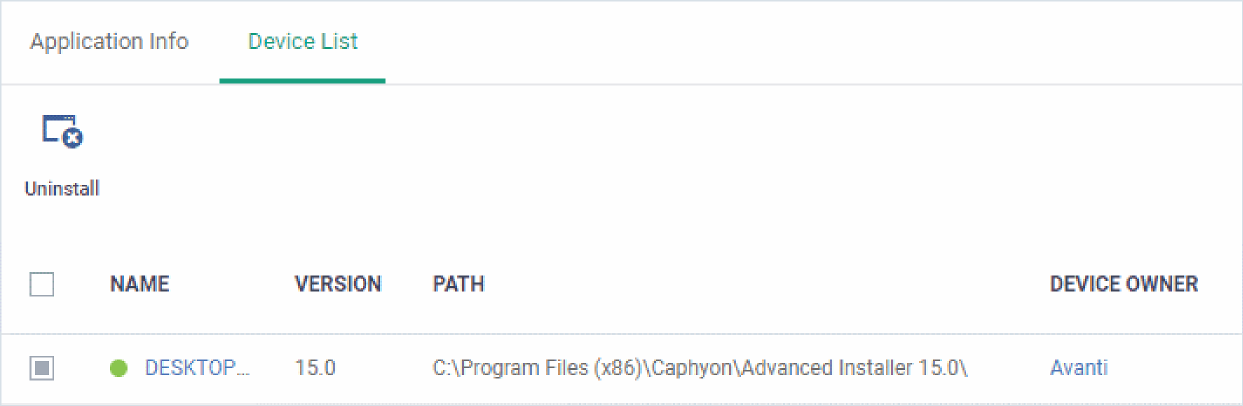
**Copyright**

**Versions(32bit)**
15.0
14.9
14.8
14.6
14.5.2

**Versions(64bit)**
15.0
14.9

The application details interface contains two tabs:

- **Application Info -** General information about the application. This includes a short description of the application, the vendor, category, the available versions and more.
- **Device List -** The devices on which the application was found installed. You can select the devices and uninstall the application from them.



| ☐ | NAME | VERSION | PATH | DEVICE OWNER |
|---|---|---|---|---|
| ☐ | ● DESKTOP... | 15.0 | C:\Program Files (x86)\Caphyon\Advanced Installer 15.0\ | Avanti |

| Device List - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of the Windows device.<br>• Click the name of a device to open its device details interface<br>• See **Manage Windows Devices** for more details |
| Version | The version number of the application installed in the device |
| Path | The installation location of the application |
| Owner | The device user.<br>• Click the user name to open the 'View User' interface. See **View User Information** for more details. |
| **Controls** | |
| Uninstall | Allows your to remotely uninstall the application from selected Windows devices. See **Uninstall a Windows Application from Selected Devices** for more details. |

## 8.3.1. Uninstall a Windows Application from Selected Devices

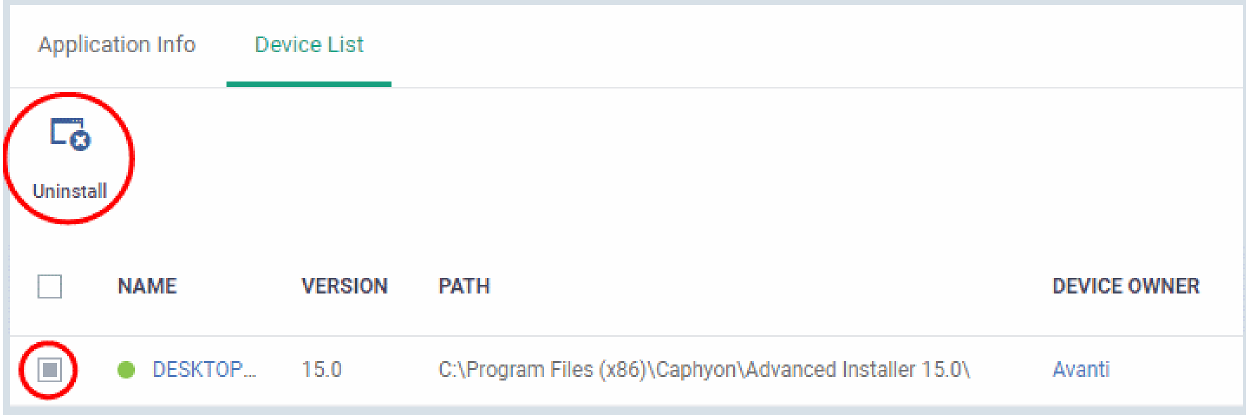
The global software inventory lets you remotely remove unwanted applications from selected Windows devices.

**Note**: You can only remove applications which are supported by EM. See the list at **EM Supported 3rd Party Applications**.

To uninstall an application from selected devices:

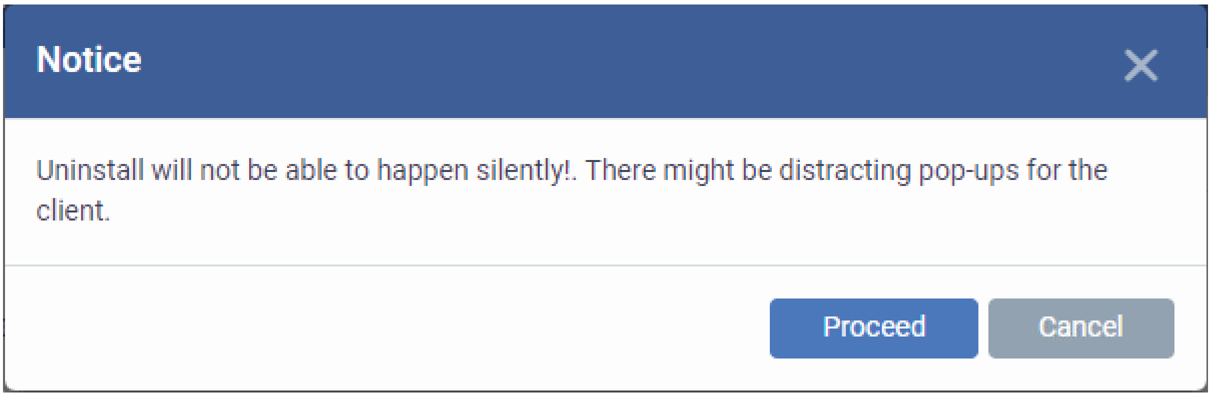
- Click 'Applications' > 'Global Software Inventory'
  - Select a company or group on the left

    Or
  - Select 'Show all' to view applications on every enrolled device
- Click the name of an application to open its details interface
- Click the 'Device List' tab



| □ | NAME | VERSION | PATH | DEVICE OWNER |
|---|---|---|---|---|
| ▣ | ● DESKTOP... | 15.0 | C:\Program Files (x86)\Caphyon\Advanced Installer 15.0\ | Avanti |

- Select the devices and click the 'Uninstall' button at the top
- An uninstall command will be sent to the selected devices.
- You will see the following message if the software cannot be uninstalled without notifying the device user:



Uninstall will not be able to happen silently!. There might be distracting pop-ups for the client.

- Click 'Proceed' to continue with the uninstall.

The application will be uninstalled from the selected devices.

**Tip**: You can remove apps from an individual device by using the device's details page. See **View and Manage Applications Installed on a Device** for more details.

## 8.3.2. Uninstall a Windows Application from All Devices

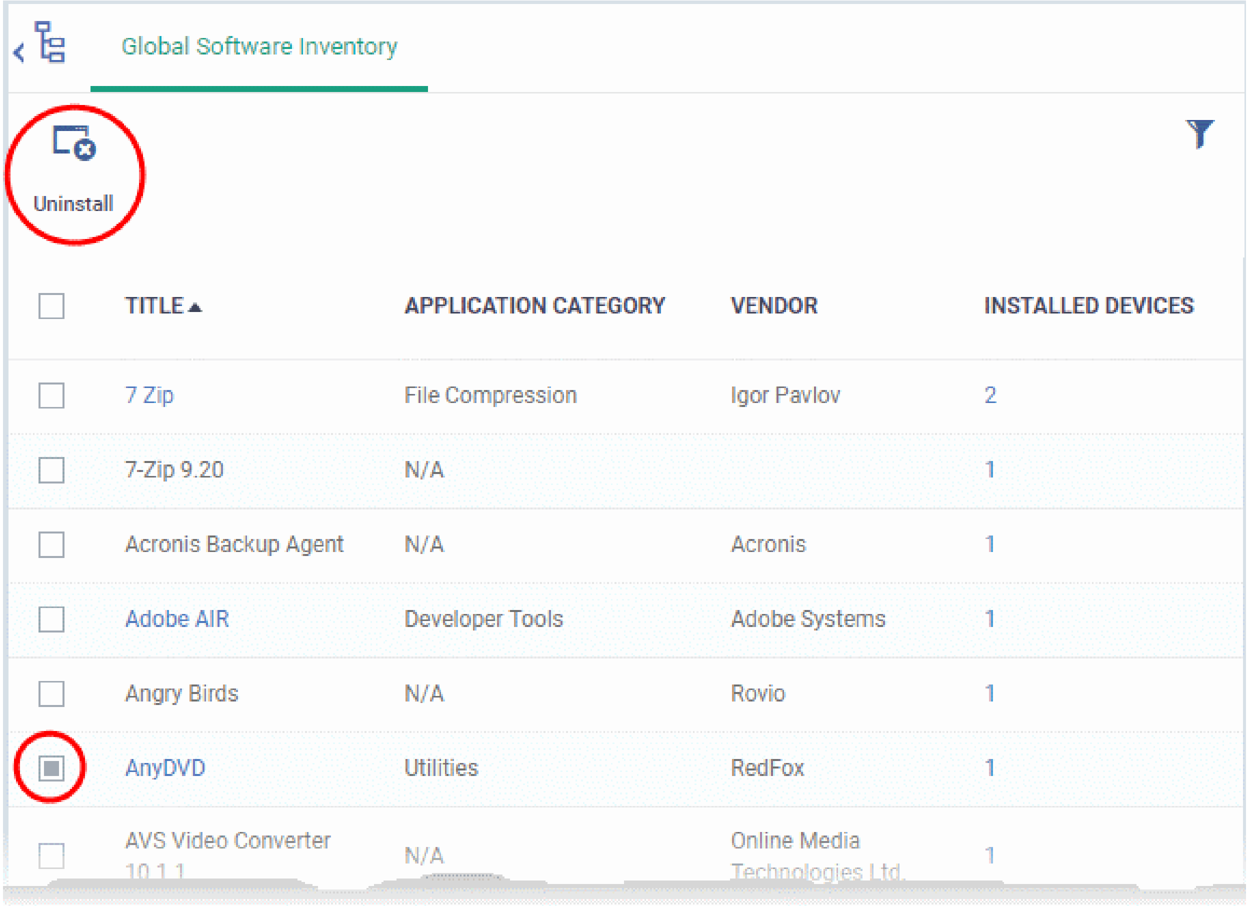
The global software inventory lets you remove unwanted applications from multiple Windows devices.

**Note**: You can only remove applications which are supported by EM. See the list at **EM Supported 3rd Party Applications**.

**To uninstall an application from all Windows devices**

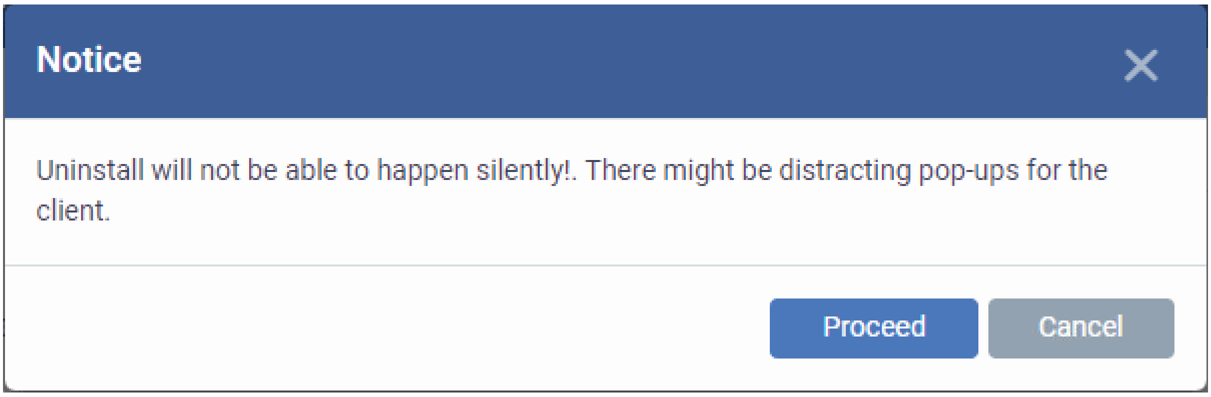
- Click 'Applications' > 'Global Software Inventory'
    - Select a company or group on the left

      Or
    - Select 'Show all' to view applications on every enrolled device
- Select the application and click the 'Uninstall' button



| □ | TITLE ▲ | APPLICATION CATEGORY | VENDOR | INSTALLED DEVICES |
|---|---|---|---|---|
| □ | 7 Zip | File Compression | Igor Pavlov | 2 |
| □ | 7-Zip 9.20 | N/A | | 1 |
| □ | Acronis Backup Agent | N/A | Acronis | 1 |
| □ | Adobe AIR | Developer Tools | Adobe Systems | 1 |
| □ | Angry Birds | N/A | Rovio | 1 |
| ☑ | AnyDVD | Utilities | RedFox | 1 |
| □ | AVS Video Converter 10.1.1 | N/A | Online Media Technologies Ltd. | 1 |

- The uninstall command is sent to all devices which have the application installed.
- You will see the following message if the software cannot be uninstalled without notifying the device user:



Uninstall will not be able to happen silently!. There might be distracting pop-ups for the client.

- Click 'Proceed' to continue with the uninstall.

The application will be uninstalled from the selected devices.

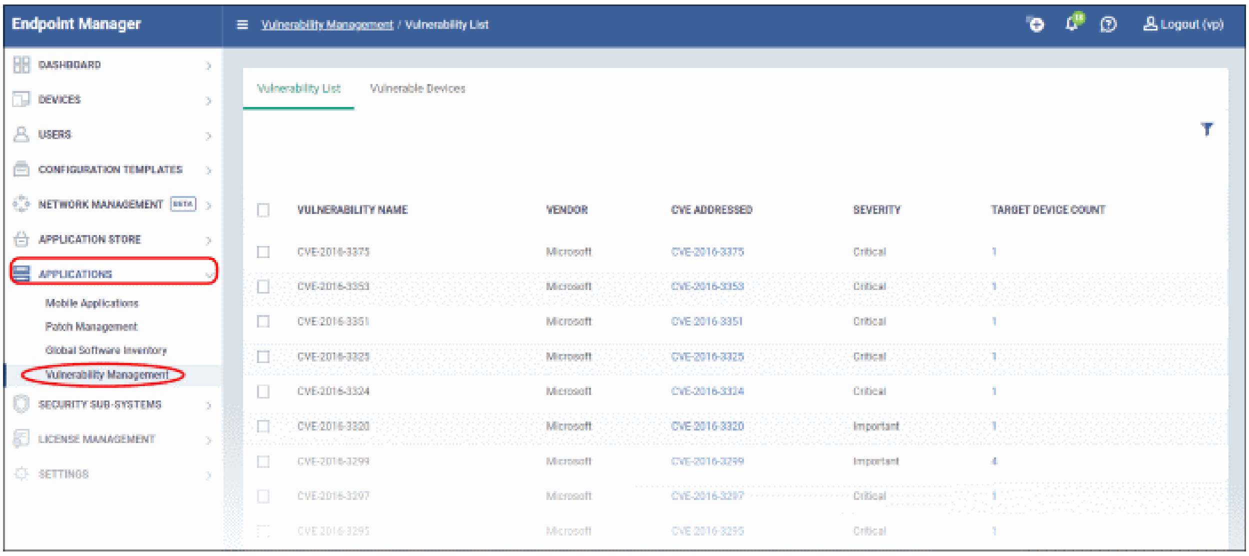
**Tip**: You can uninstall an application from an individual Windows device from its Device Details interface. See **View and Manage Applications Installed on a Device** for more details.

# 8.4. Vulnerability Management

- Click 'Applications' > 'Vulnerability Management' to open this interface.
- This area lets you view known weaknesses found on your devices, along with their CVE (common vulnerabilities and exposures) rating.
- You can view which devices are affected and install patches as required.

### Open the vulnerability management interface

- Click 'Applications' > 'Vulnerability Management'



| □ | VULNERABILITY NAME | VENDOR | CVE ADDRESSED | SEVERITY | TARGET DEVICE COUNT |
|---|---|---|---|---|---|
| □ | CVE-2016-3375 | Microsoft | CVE-2016-3375 | Critical | 1 |
| □ | CVE-2016-3353 | Microsoft | CVE-2016-3353 | Critical | 1 |
| □ | CVE-2016-3351 | Microsoft | CVE-2016-3351 | Critical | 1 |
| □ | CVE-2016-3325 | Microsoft | CVE-2016-3325 | Critical | 1 |
| □ | CVE-2016-3324 | Microsoft | CVE-2016-3324 | Critical | 1 |
| □ | CVE-2016-3320 | Microsoft | CVE-2016-3320 | Important | 1 |
| □ | CVE-2016-3299 | Microsoft | CVE-2016-3299 | Important | 4 |
| □ | CVE-2016-3297 | Microsoft | CVE-2016-3297 | Critical | 1 |
| □ | CVE-2016-3295 | Microsoft | CVE-2016-3295 | Critical | 1 |

There are two tabs, each of which offers a different view of the vulnerabilities:

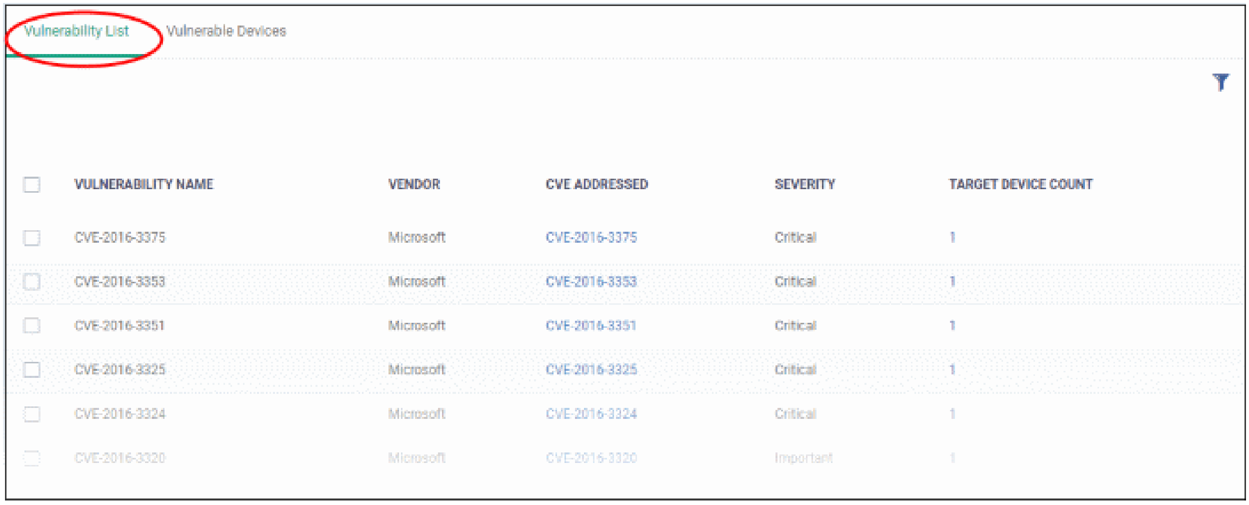
- **Vulnerability List** - A list of discovered vulnerabilities and the number of devices affected by each.

  Apply corrective patches:

  - Click the number in the 'Target Device Count' column
  - Select the devices you want to patch
  - Click the 'Install Patch' button above the table
- **Vulnerable Devices** - A list of devices affected by listed vulnerabilities. Allows you patch affected device with a single click.

## Vulnerability List

- Click 'Applications' > 'Vulnerability Management'
- Click the 'Vulnerability List' tab



| | VULNERABILITY NAME | VENDOR | CVE ADDRESSED | SEVERITY | TARGET DEVICE COUNT |
|---|---|---|---|---|---|
| □ | CVE-2016-3375 | Microsoft | CVE-2016-3375 | Critical | 1 |
| □ | CVE-2016-3353 | Microsoft | CVE-2016-3353 | Critical | 1 |
| □ | CVE-2016-3351 | Microsoft | CVE-2016-3351 | Critical | 1 |
| □ | CVE-2016-3325 | Microsoft | CVE-2016-3325 | Critical | 1 |
| □ | CVE-2016-3324 | Microsoft | CVE-2016-3324 | Critical | 1 |
| □ | CVE-2016-3320 | Microsoft | CVE-2016-3320 | Important | 1 |

| Vulnerability List - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Vulnerability Name | The vulnerability identifier. This is same as the CVE code. |
| Vendor | Developer of the affected software and the corresponding patch |
| CVE Addressed | Identification code of the security threat. Click this to view vulnerability details, vendor and affected devices. |
| Severity | Criticality of the vulnerability. The possible levels are:<br>• **Critical** - Vulnerabilities that can be exploited without warnings or prompts. Examples include remote elevation of privileges exploits that allow attackers to write to the file system, or execute arbitrary code without user interaction. You should patch critical vulnerabilities as soon as possible.<br>• **Important** - A vulnerability which could compromise the confidentiality, integrity, or availability of user data if exploited. The distinguishing factor between critical and important is that important vulnerabilities show some warning or prompt to the user. For example, local escalation of privilege exploits, or the execution of arbitrary code which requires extensive user action. Again, you should patch important vulnerabilities as soon as possible.<br>• **Moderate** - The likelihood of exploit is largely mitigated by factors such as default configuration, auditing, or difficulty of exploitation. Moderate vulnerabilities usually require specific scenarios, locations or other prerequisites. We recommend you consider patching moderate vulnerabilities.<br>• **Low** - A vulnerability whose exploitation is extremely difficult, or whose impact is minimal. We recommend applying low severity updates at your discretion.<br>• **Unspecified** - The patch was issued without a severity rating. |
| Target Device Count | Number of devices affected by the vulnerability. Click this to view device details and implement patches. |

- Click the funnel icon to filter vulnerabilities by various criteria
- Click a column header to sort in ascending / descending / alphabetical order

From this interface you can:

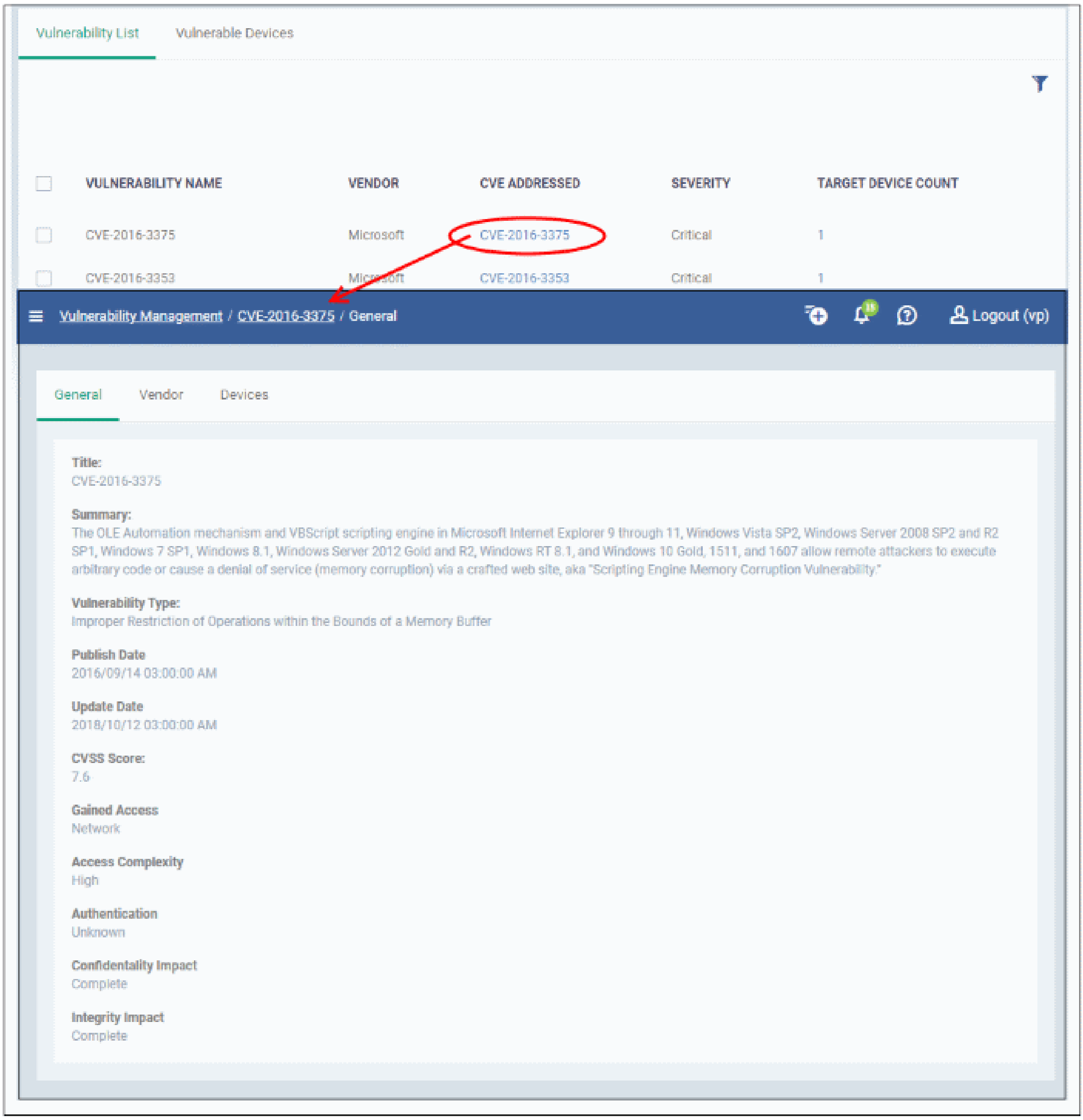
- View details of a vulnerability threat
- Run a security patch on devices

### View Details of a Vulnerability Threat

- Click 'Applications' > 'Vulnerability Management' then the 'Vulnerability List' tab
- Click the CVE ID number in the CVE Addressed column

The CVE details has three tabs, General, Vendor and Devices. By default the general tab is open in the CVE details screen.

- **General** - Provides the CVE details such as the name of the vulnerability type, published date and so on.



| ☐ | VULNERABILITY NAME | VENDOR | CVE ADDRESSED | SEVERITY | TARGET DEVICE COUNT |
|---|---|---|---|---|---|
| ☐ | CVE-2016-3375 | Microsoft | CVE-2016-3375 | Critical | 1 |
| ☐ | CVE-2016-3353 | Microsoft | CVE-2016-3353 | Critical | 1 |

Title:
CVE-2016-3375

Summary:
The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

Vulnerability Type:
Improper Restriction of Operations within the Bounds of a Memory Buffer

Publish Date
2016/09/14 03:00:00 AM

Update Date
2018/10/12 03:00:00 AM

CVSS Score:
7.6

Gained Access
Network

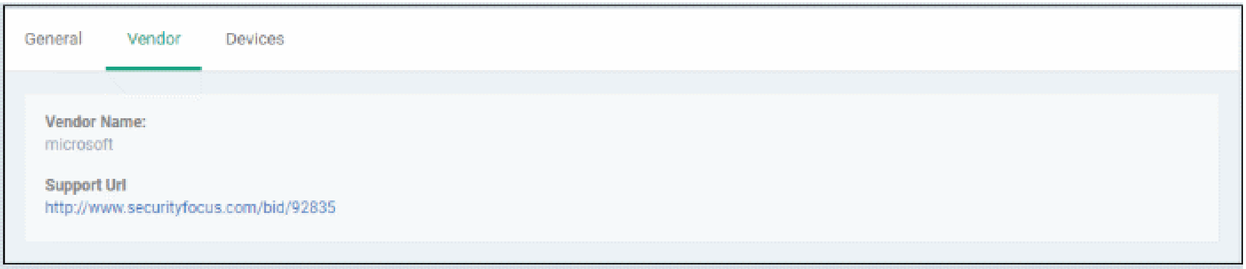
Access Complexity
High

Authentication
Unknown

Confidentiality Impact
Complete

Integrity Impact
Complete

Click the vendor tab.

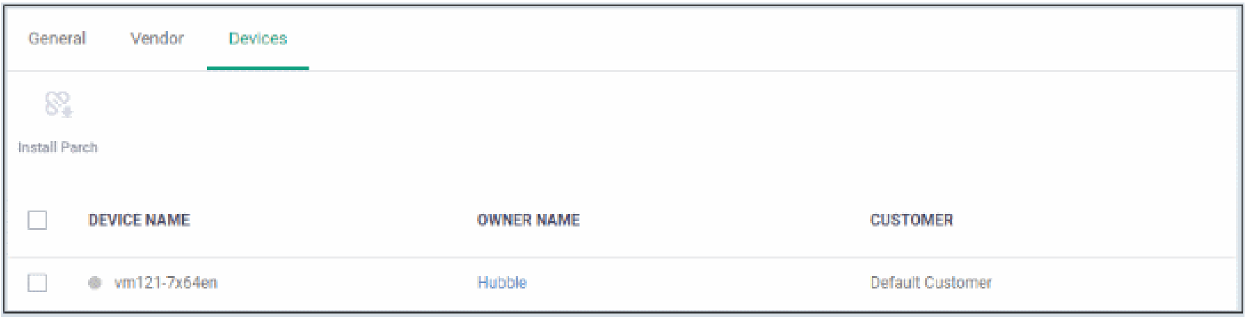


Vendor Name:
microsoft

Support Url
http://www.securityfocus.com/bid/92835

- **Vendor Name -** The software publisher's name
- **Support URL -** Clicking the link will take you to the technical community page that provides full information about the vulnerability, discussions, solutions and so on.

Click the devices tab.



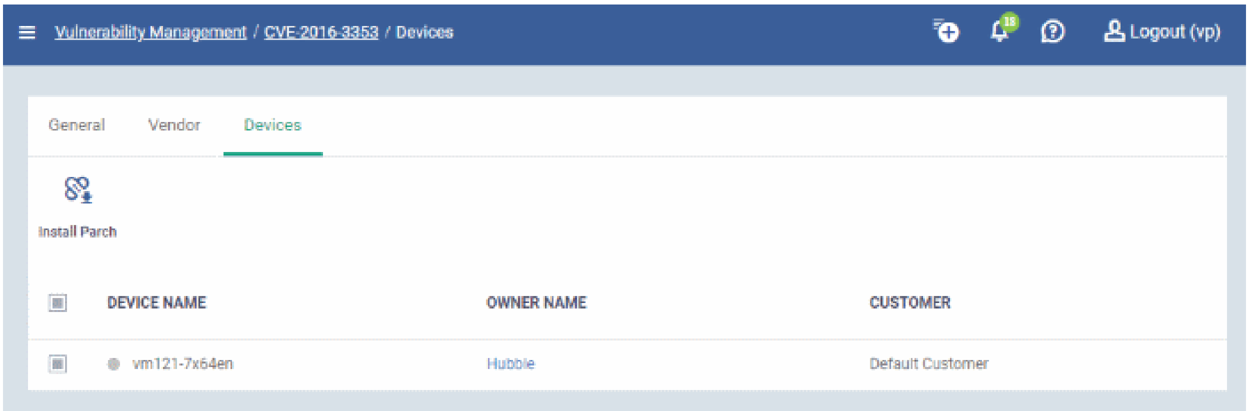
| □ | DEVICE NAME | OWNER NAME | CUSTOMER |
|---|---|---|---|
| □ | vm121-7x64en | Hubble | Default Customer |

- Shows the affected devices. You can run security patches for devices from here. See '**Run a Security Patch on Devices**'

### Run a Security Patch on Devices

You can run security patches targeted to address a particular CVE security threat.

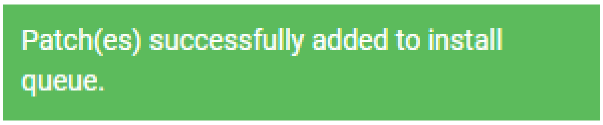
- Click 'Applications' > 'Vulnerability Management' then the 'Vulnerability List' tab
- Click the number in the target device count column or click the CVE ID number in the CVE Addressed column then the 'Devices' tab



| ☒ | DEVICE NAME | OWNER NAME | CUSTOMER |
|---|---|---|---|
| ☒ | vm121-7x64en | Hubble | Default Customer |

  - **Device Name -** Clicking the name will take you to the **patch management** section in the **device summary** page
  - **Owner Name -** Clicking the name will take you to **user information** page
  - **Customer -** The name of the organization the device is assigned to.
- Select the device and click 'Install Patch' above

A confirmation message is shown:

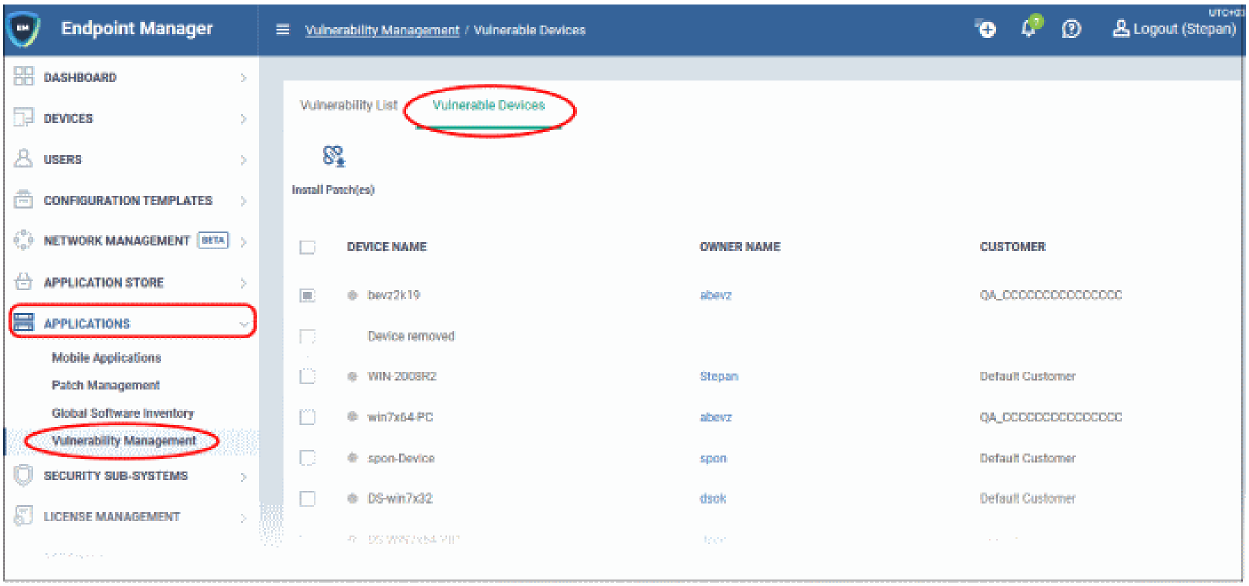


Patch(es) successfully added to install queue.

## Vulnerable Devices

This screen lets you view devices that are affected by vulnerabilities and install patches as required. The 'Install Patches' button will install every required patch.

- Click 'Applications' > 'Vulnerability Management' then the 'Vulnerable Devices' tab



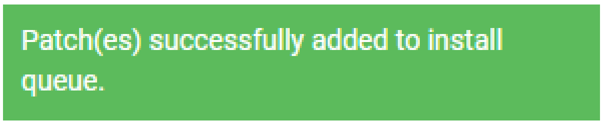
| | DEVICE NAME | OWNER NAME | CUSTOMER |
|---|---|---|---|
| ☒ | bevz2k19 | abevz | QA_CCCCCCCCCCCCCC |
| □ | Device removed | | |
| □ | WIN-2008R2 | Stepan | Default Customer |
| □ | win7x64-PC | abevz | QA_CCCCCCCCCCCCCC |
| □ | spon-Device | spon | Default Customer |
| □ | DS-win7x32 | dsok | Default Customer |

- **Device Name -** Affected device. Click the name to view the patches available for the device.
- **Owner Name -** User of the device. Click the name to view the user's details.
- **Customer -** The name of the organization to which the device is assigned.

**Install security patch(es)**

- Select the devices you want to patch then click the 'Install Patch(es)' button.

You will see the following confirmation message:



Patch(es) successfully added to install queue.

All available patches are installed.

# 9.Application Store

- The 'Application Store' is a repository of useful applications which can be pushed to iOS, Android and Windows devices.

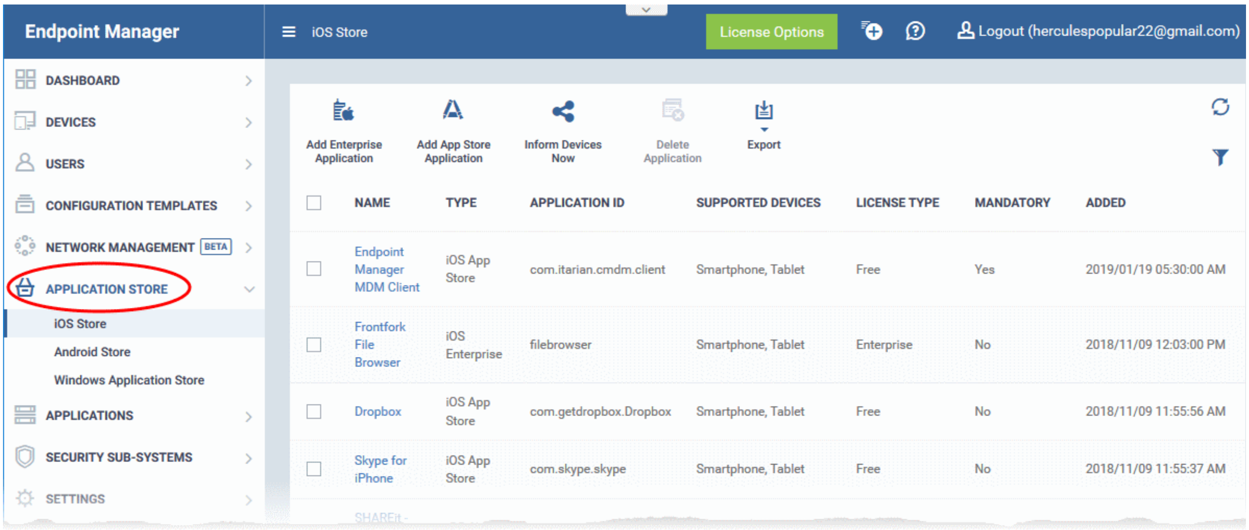
**Android and iOS Applications**

- You can add both mandatory and optional apps to the repository. You can update all devices with one-click of the 'Inform Devices Now' button.
    - **Google Play and Apple App Store -** Specify the app name or bundle identifier. Endpoint Manager will automatically fetch the app details. The device owner will be taken to the Google Play page/App Store page to install the app.
    - **Custom 'Enterprise' applications -** You can also upload your own .apk (Android) or .ipa (iOS) files to the app store. The communication client on the device collects the app from Endpoint Manager and installs it.
- Apps in the repository are automatically synchronized with enrolled devices every 24 hours. Notifications are sent to devices if new apps are ready to be installed. You can also manually sync apps if required. Users will be informed if there are new apps awaiting installation.

**Windows Applications**

- Endpoint Manager comes with a built-in list of popular Windows applications.
- Applications can be installed on all managed devices or selected devices.
- You cannot edit or remove applications from the list

The 'Application Store' tab contains three sub tabs, iOS Store, Android Store and Windows Application Store.



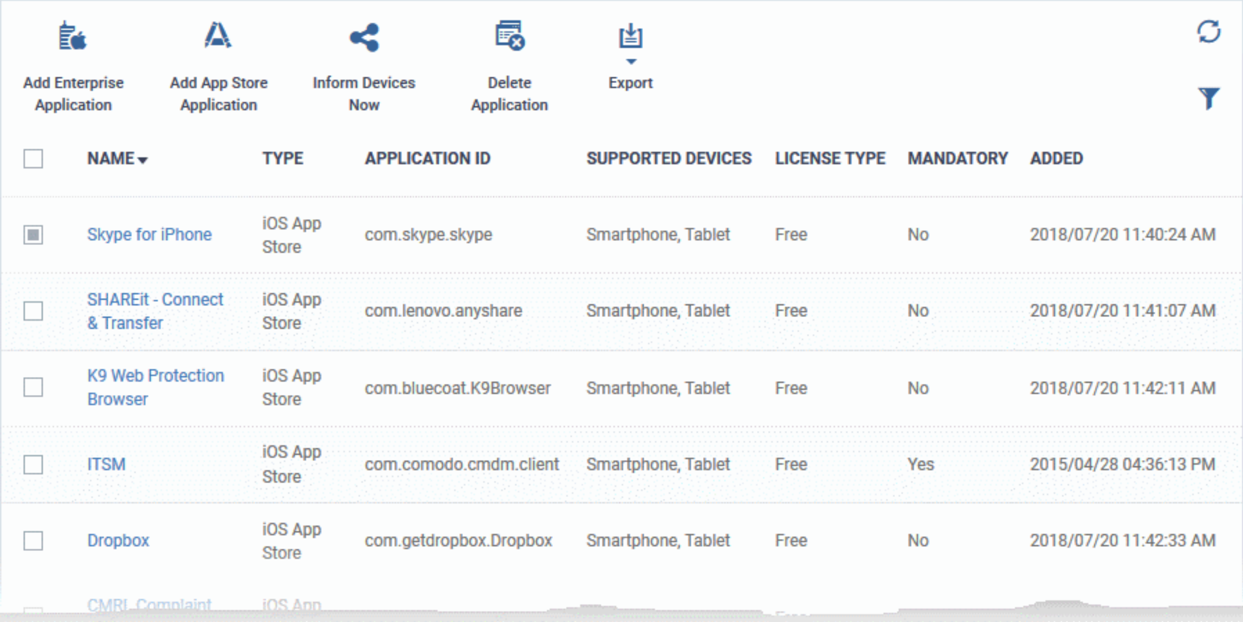
| □ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| □ | Endpoint Manager MDM Client | iOS App Store | com.itarian.cmdm.client | Smartphone, Tablet | Free | Yes | 2019/01/19 05:30:00 AM |
| □ | Frontfork File Browser | iOS Enterprise | filebrowser | Smartphone, Tablet | Enterprise | No | 2018/11/09 12:03:00 PM |
| □ | Dropbox | iOS App Store | com.getdropbox.Dropbox | Smartphone, Tablet | Free | No | 2018/11/09 11:55:56 AM |
| □ | Skype for iPhone | iOS App Store | com.skype.skype | Smartphone, Tablet | Free | No | 2018/11/09 11:55:37 AM |
|  | SHAREit - |  |  |  |  |  |  |

The following sections contain more details on each app type:

- iOS Apps
    - Add iOS Apps and Installing them on Devices
    - Manage iOS Apps
- Android Apps
    - Add Android Apps and Installing them on Devices
    - Manage Android Apps
- Windows Apps
    - Install Windows Apps on Devices

# 9.1.iOS Apps

- Click 'Application Store' > 'iOS Store'.
- The iOS store area contains all available iOS apps that have been uploaded to Endpoint Manager. You can deploy selected apps to all managed devices or specific devices.
- You can add new apps from the Apple store or upload your own custom enterprise apps. You can synchronize the app list with managed iOS devices and edit existing app parameters.
- You can specify whether an app is a mandatory install or an optional install.



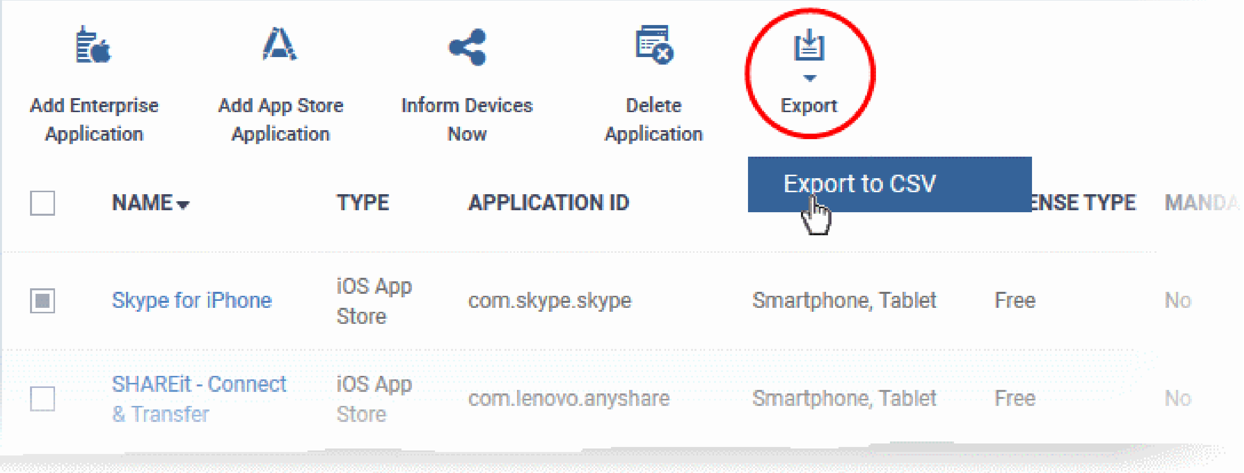
| □ | NAME ▾ | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| ☑ | Skype for iPhone | iOS App Store | com.skype.skype | Smartphone, Tablet | Free | No | 2018/07/20 11:40:24 AM |
| □ | SHAREit - Connect & Transfer | iOS App Store | com.lenovo.anyshare | Smartphone, Tablet | Free | No | 2018/07/20 11:41:07 AM |
| □ | K9 Web Protection Browser | iOS App Store | com.bluecoat.K9Browser | Smartphone, Tablet | Free | No | 2018/07/20 11:42:11 AM |
| □ | ITSM | iOS App Store | com.comodo.cmdm.client | Smartphone, Tablet | Free | Yes | 2015/04/28 04:36:13 PM |
| □ | Dropbox | iOS App Store | com.getdropbox.Dropbox | Smartphone, Tablet | Free | No | 2018/07/20 11:42:33 AM |
| □ | CMRL Complaint | iOS App | | | | | |

| 'iOS App Catalog' - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | Application label.<br>• Click on the name to view app description, version number, bundle ID, category, supported devices, mandatory/optional setting and download URL.<br>• You can also edit app details from here. See **Manage iOS Apps** for more details. |
| Type | App class as determined by the source of the app. Possible types are:<br>• iOS App Store<br>• iOS Enterprise (apps uploaded by an admin) |
| Application ID | The bundle identifier of the app. This is a unique id used by Apple to identify an app. |
| Supported Devices | Types of devices with which the app is compatible. |
| License Type | Whether the app is a free, paid or enterprise version. |
| Mandatory | Whether or not it is compulsory for managed devices to install the app. Admins can set if an app should be mandatory. See '**Add iOS Apps and Install them on Devices**' for more details. |
| Added | The date and time at which the app was added to repository. |

| | |
|---|---|
| **Controls** | |
| Add Enterprise Application | Add custom applications to Endpoint Manager by simply uploading the .ipa package files of the apps. See **Add iOS Apps and Install them on Devices** for more details. |
| Add App Store Application | Add applications from the Apple store by typing the app name. See **Add iOS Apps and Install them on Devices** for more details. |
| Inform Devices Now | Synchronize enrolled Android devices with the latest app list. |
| Delete Application | Remove an application from the iOS app repository. |
| Export | Save a copy of the app list as a comma separated values (csv) file. See **Export the List of iOS Applications** for more details. |

## Export the List of iOS Applications

- Click 'Application Store' > 'iOS Store'.
- Click the 'Export' button above the table then choose 'Export to CSV':

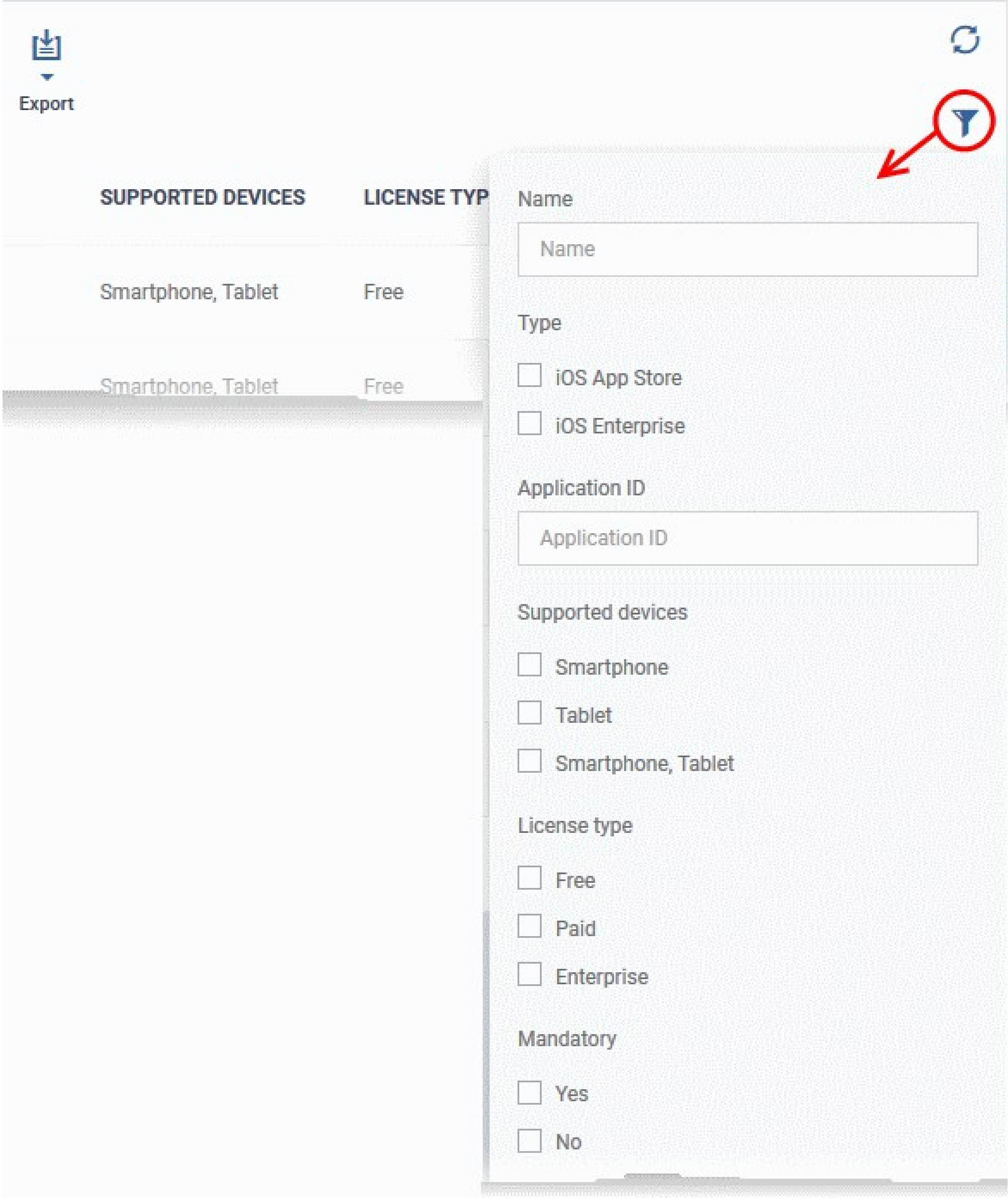


| □ | NAME | TYPE | APPLICATION ID | | ENSE TYPE | MANDA |
|---|---|---|---|---|---|---|
| ☒ | Skype for iPhone | iOS App Store | com.skype.skype | Smartphone, Tablet | Free | No |
| □ | SHAREit - Connect & Transfer | iOS App Store | com.lenovo.anyshare | Smartphone, Tablet | Free | No |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Sorting, Search and Filter Options

- Click a column header to sort items in alphabetical order of entries in the column.
- Click the funnel button to open the filter options.



Name

Name

Type

□ iOS App Store

□ iOS Enterprise

Application ID

Application ID

Supported devices

□ Smartphone

□ Tablet

□ Smartphone, Tablet

License type

□ Free

□ Paid

□ Enterprise

Mandatory

□ Yes

□ No

Click the following links for more help:

- **Add iOS Apps and Install them on Devices**
- **Manage iOS Apps**

## 9.1.1. Add iOS Apps and Install them on Devices

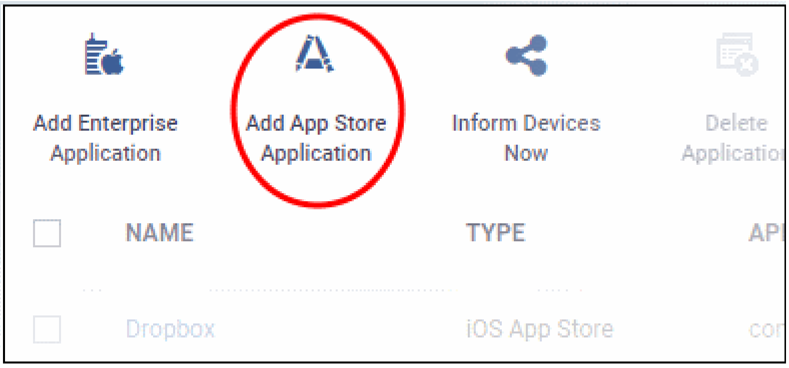
- You can add apps to Endpoint Manager directly from the Apple store or by uploading a custom app.
- Apps can be installed on all or selected iOS devices

Please see the following sections for more help:

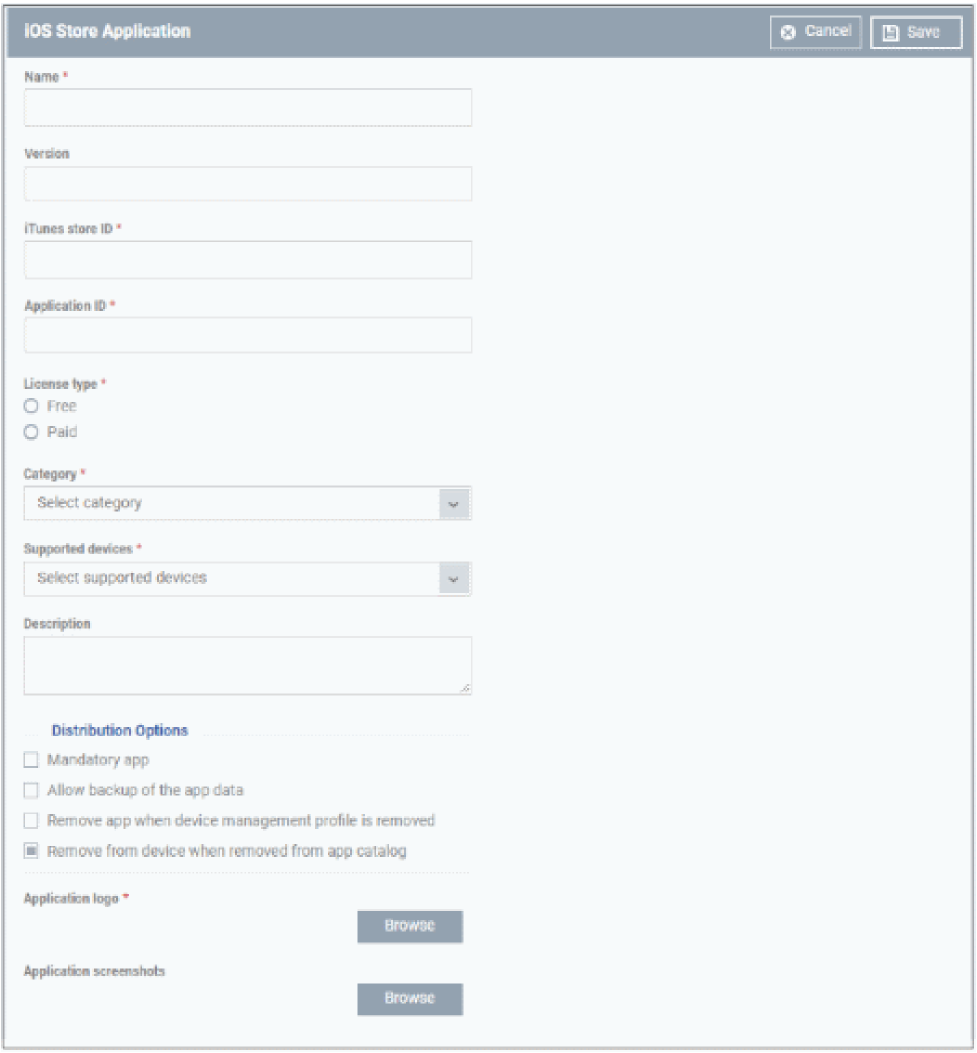
- **Add iOS Apps from the App Store**
- **Add Custom/Enterprise iOS Apps**

## Add iOS Apps from the App Store

- Click 'Application Store' > 'iOS Store'
- Click the 'Add App Store Application' button:



- Type the first few letters of the app in the 'Name' field on the form. Endpoint Manager will search for matching apps from the store.
- Select the correct app from the list of suggestions. The rest of the form will be auto-populated by the app details.



Name *

Version

iTunes store ID *

Application ID *

License type *
○ Free
○ Paid

Category *
Select category

Supported devices *
Select supported devices

Description

Distribution Options
□ Mandatory app
□ Allow backup of the app data
□ Remove app when device management profile is removed
☒ Remove from device when removed from app catalog

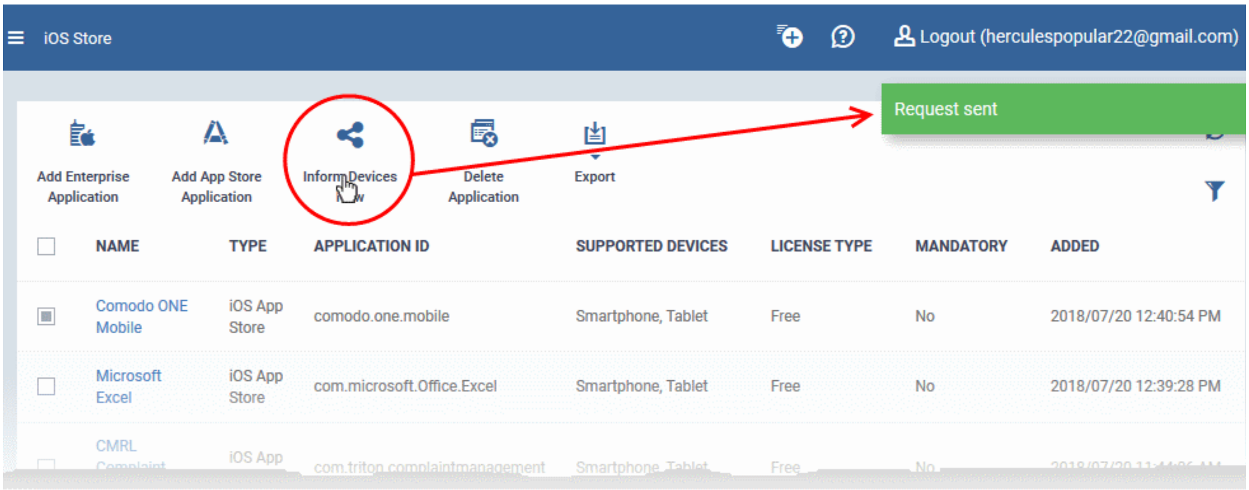
Application logo *
Browse

Application screenshots
Browse

| Apple Store Application - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text Field | The label of the application.<br>• Enter the first few letters of the app name.<br>• EM searches for matching apps in the app store |
| Version | Text Field | The version number of the application. This field is auto-populated after entering the app name. |
| iTunes Store ID | Text Field | The Apple identification number of the app. This field is auto-populated after entering the app name.<br>Usually, this number will appear after ID in the download URL of the app. For example, in the URL **https://itunes.apple.com/us/app/ITSM/id807480077**, the numbers after ID is the iTunes Store ID for this app. |
| Application ID | Text Field | The bundle ID of the app. This field is auto-populated after entering the app name.<br>For example, the bundle ID for EM client is com.comodo.ITSM.client |
| License Type | Radio Button | Specify whether the app is free or a paid version.<br>This option is pre-populated by the app chosen in the 'Name' field. |
| Category | Drop-down | The classification of the application. The category field will be auto-populated depending on the app chosen in the 'Name' field<br>The drop-down also enables you to choose the category to which the app belongs. |
| Supported devices | Drop-down | The category of devices on which the app can run.<br>The device type will be auto-selected depending on the app chosen in the 'Name' field.<br>The drop-down also enables you to choose the device types to which the app is compatible. |
| Description | Text Field | The 'Description' filed will be auto-populated with the description of the selected app, from the App Store page.<br>The text field also enables you to enter your description or edit the existing description. |
| Mandatory app | Checkbox | Specify whether or not it is compulsory that devices install this app. If enabled, all enrolled devices will get alerts automatically to install the app.<br>See **Install Apps on Android/iOS Devices** for more details. |
| Allow backup of the app data | Checkbox | Allows user to backup the application along with its user data to iTunes. |
| Remove app when device management profile is removed | Checkbox | The app will be deleted from devices if the profile applied to the device is removed. |
| Remove from device when removed from app catalog | Checkbox | The app will be deleted from devices if it is removed from 'iOS Store'. |

| 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 confirming the details.
- The app will be added to the repository and listed in the 'iOS Store' interface. It will be synced to devices during the next cycle.
- Click 'Inform Devices Now' if you want to immediately notify devices to install the app:


iOS Store
Logout (herculespopular22@gmail.com)
Add Enterprise Application
Add App Store Application
Inform Devices Now
Delete Application
Export

Request sent

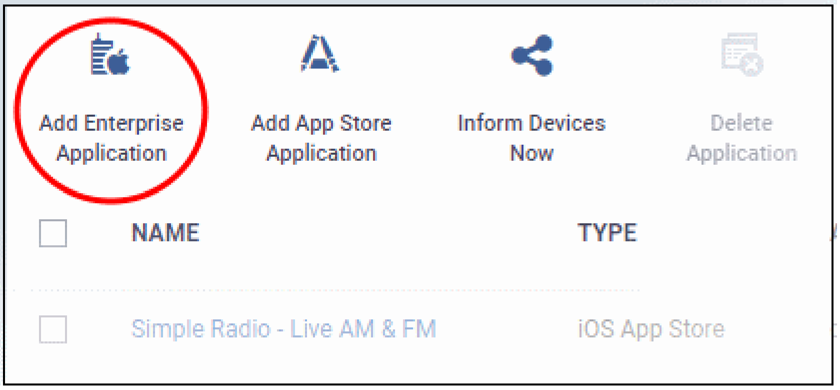
| ☐ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| ▣ | Comodo ONE Mobile | iOS App Store | comodo.one.mobile | Smartphone, Tablet | Free | No | 2018/07/20 12:40:54 PM |
| ☐ | Microsoft Excel | iOS App Store | com.microsoft.Office.Excel | Smartphone, Tablet | Free | No | 2018/07/20 12:39:28 PM |
| ☐ | CMRL Complaint | iOS App | com.triton.complaintmanagement | Smartphone, Tablet | Free | No | 2018/07/20 11:44:06 AM |

## Add Custom/Enterprise iOS Apps

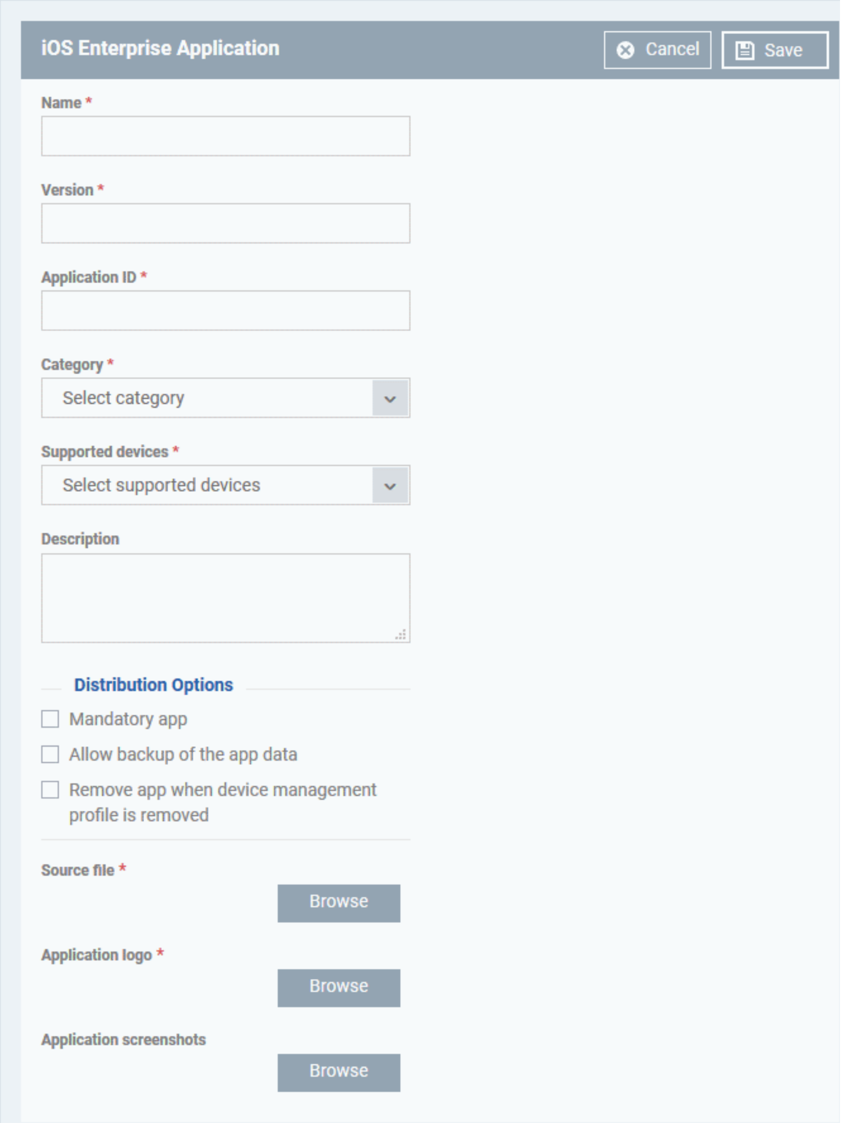
- Custom applications can be added to the repository by simply uploading the app .ipa file
- Most app details, such as name, version and ID, will be automatically fetched by parsing the file. You just need to manually enter some remaining details

### To add Custom/Enterprise iOS Apps

- Click 'Application Store' > 'iOS Store' to open the interface
- Click 'Add Enterprise Application' from the options at the top.


Add Enterprise Application
Add App Store Application
Inform Devices Now
Delete Application
NAME
TYPE
Simple Radio - Live AM & FM
iOS App Store

- Click 'Browse' beside 'Source File', select the .ipa file you want to upload and click 'Open'
- The file will be uploaded. Many form field details are auto-populated from the file itself:


iOS Enterprise Application

Cancel | Save

Name *

Version *

Application ID *

Category *
Select category

Supported devices *
Select supported devices

Description

Distribution Options

□ Mandatory app
□ Allow backup of the app data
□ Remove app when device management profile is removed

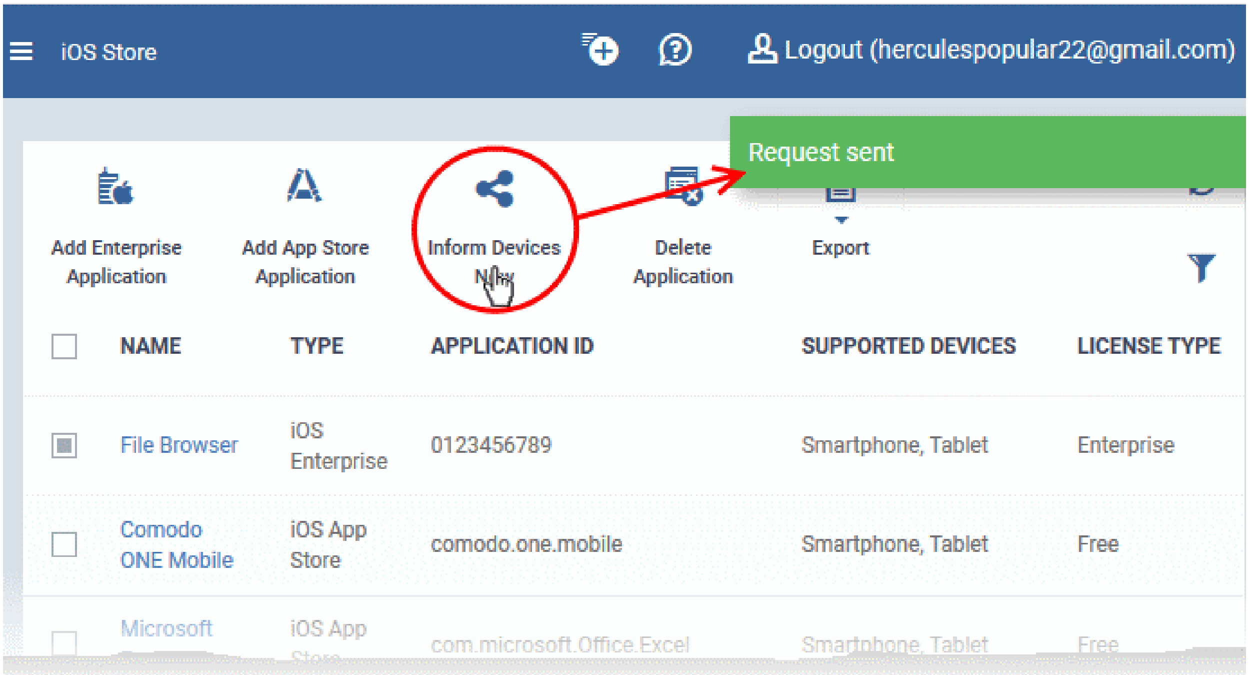
Source file * Browse

Application logo * Browse

Application screenshots Browse

| Add iOS Enterprise Application - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text Field | Application label. Auto-populated from the .ipa file<br>• Enter the name of the app if not auto-populated |
| Version | Text Field | The version of the application as obtained from the .ipa file.<br>• Enter the version number, if it is not auto-populated |
| Application ID | Text Field | The app's unique identifier as obtained from the .ipa file.<br>Usually, this number will appear after ID in the download URL of the app.<br>For example, in the URL https://itunes.apple.com/us/app/ITSM/id807480077, the numbers after ID is the iTunes Store ID for this app. |
| Category | Drop-down | Select the app classification. |
| Supported devices | Drop-down | Select the category of the devices to which the app is compatible. |
| Description | Text Field | Enter a description for the app. |
| Mandatory app | Checkbox | Specify whether the app should compulsorily be installed on devices. If enabled, all enrolled devices will be alerted to install the app.<br>See **Install Apps on Android/iOS Devices** for more details. |
| Allow backup of the app data | Checkbox | Allows to backup the application along with its user data to iTunes. |
| Remove app when device management profile Is removed | Checkbox | The app will be automatically uninstalled if the EM profile applied to the device is removed. |
| Source file | Browse button | Navigate to the storage location of the .ipa file to be uploaded and select the file. |
| Application logo | Browse button | Upload the logo image for the app. |
| Application screenshots | Browse button | Upload screenshots of the app, if required. |

- Click 'Save' after confirming all details.
- The app will be added to the repository and listed in the 'iOS Store' interface. It will be pushed to devices on the next sync-cycle.
- Click 'Inform Devices Now' if you want to push the app to devices immediately.


iOS Store
Logout (herculespopular22@gmail.com)
Add Enterprise Application
Add App Store Application
Inform Devices Now
Delete Application
Export

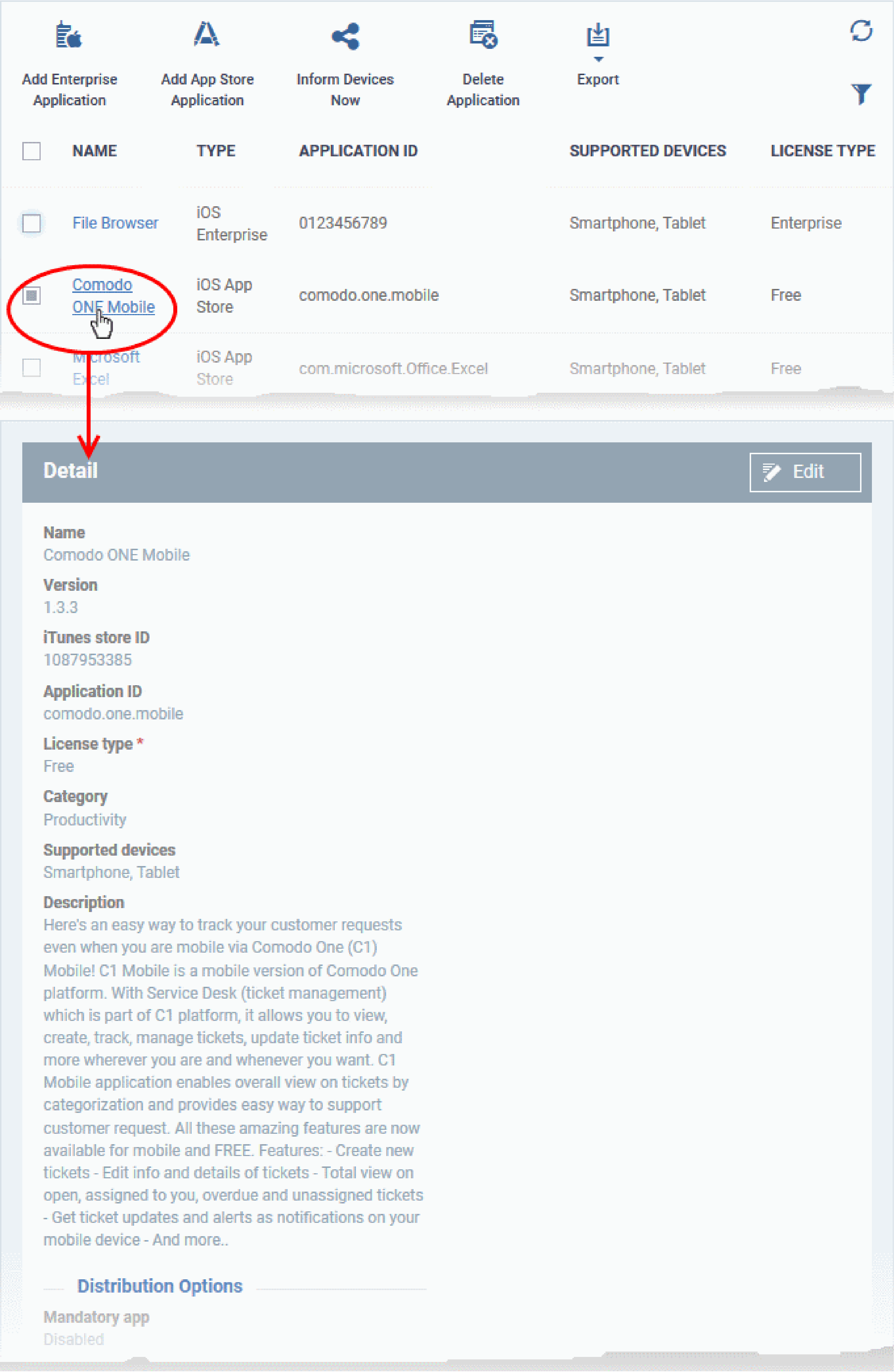
Request sent

| ☐ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE |
|---|---|---|---|---|---|
| ☑ | File Browser | iOS Enterprise | 0123456789 | Smartphone, Tablet | Enterprise |
| ☐ | Comodo ONE Mobile | iOS App Store | comodo.one.mobile | Smartphone, Tablet | Free |
| ☐ | Microsoft | iOS App Store | com.microsoft.Office.Excel | Smartphone, Tablet | Free |

## 9.1.2. Manage iOS Apps

The 'iOS Apps' interface lets you view and edit app details, and remove unwanted apps from the repository.

- Click 'Application Store' > 'iOS Store'
- Click the name of an app.



| □ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE |
|---|---|---|---|---|---|
| □ | File Browser | iOS Enterprise | 0123456789 | Smartphone, Tablet | Enterprise |
| ■ | Comodo ONE Mobile | iOS App Store | comodo.one.mobile | Smartphone, Tablet | Free |
| □ | Microsoft Excel | iOS App Store | com.microsoft.Office.Excel | Smartphone, Tablet | Free |

Detail

**Name**
Comodo ONE Mobile

**Version**
1.3.3

**iTunes store ID**
1087953385

**Application ID**
comodo.one.mobile

**License type** *
Free

**Category**
Productivity

**Supported devices**
Smartphone, Tablet

**Description**
Here's an easy way to track your customer requests even when you are mobile via Comodo One (C1) Mobile! C1 Mobile is a mobile version of Comodo One platform. With Service Desk (ticket management) which is part of C1 platform, it allows you to view, create, track, manage tickets, update ticket info and more wherever you are and whenever you want. C1 Mobile application enables overall view on tickets by categorization and provides easy way to support customer request. All these amazing features are now available for mobile and FREE. Features: - Create new tickets - Edit info and details of tickets - Total view on open, assigned to you, overdue and unassigned tickets - Get ticket updates and alerts as notifications on your mobile device - And more..

Distribution Options

Mandatory app
Disabled

The details page contains a product description and various other info about the app. You can edit app details from here too.

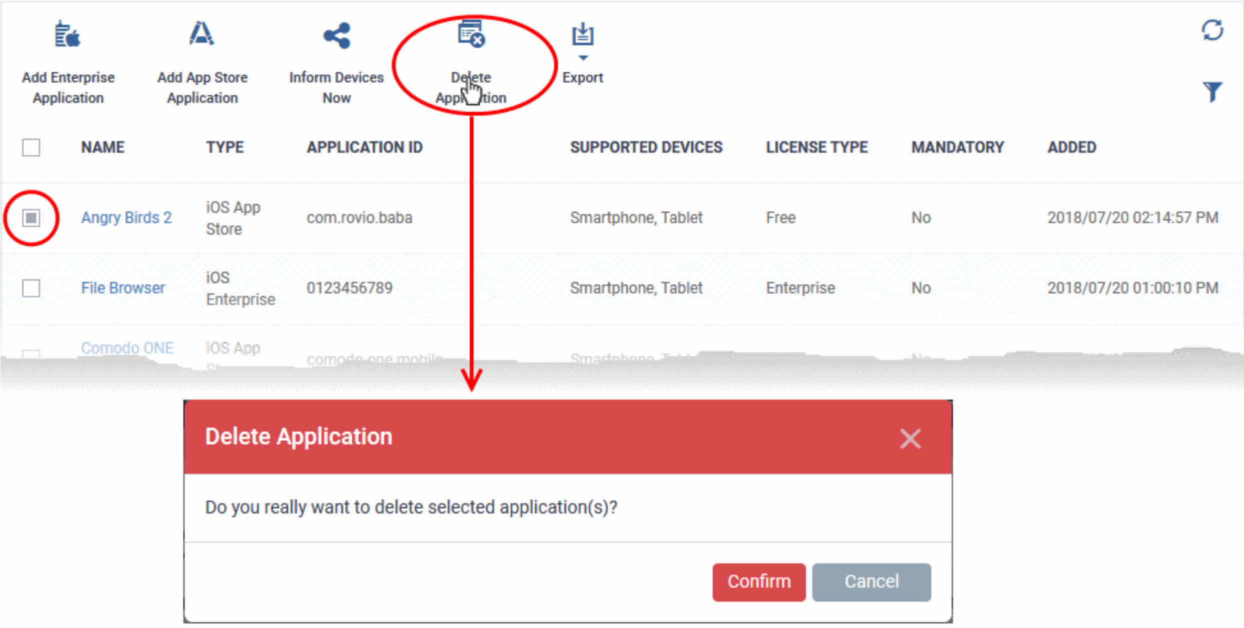
**To edit the details of an application**

- Click on the 'Edit' button Edit at top right.

The application details edit screen will open. This screen is similar to the interface for adding a new application. See **Add iOS Apps and Install them on Devices** if you need help with this.

### Remove Apps from the store

- Click 'Application Store' > 'iOS Store'
- Select the app(s) you want to remove and click 'Delete Application' above the table.
  - Note. If 'Remove from device when removed from app catalog' is enabled, then the app will also be removed from devices.



| ☐ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| ☑ | Angry Birds 2 | iOS App Store | com.rovio.baba | Smartphone, Tablet | Free | No | 2018/07/20 02:14:57 PM |
| ☐ | File Browser | iOS Enterprise | 0123456789 | Smartphone, Tablet | Enterprise | No | 2018/07/20 01:00:10 PM |
| ☐ | Comodo ONE | iOS App St | comodo.one.mobile | Smartphone, Tab | | No | |

**Delete Application** ×

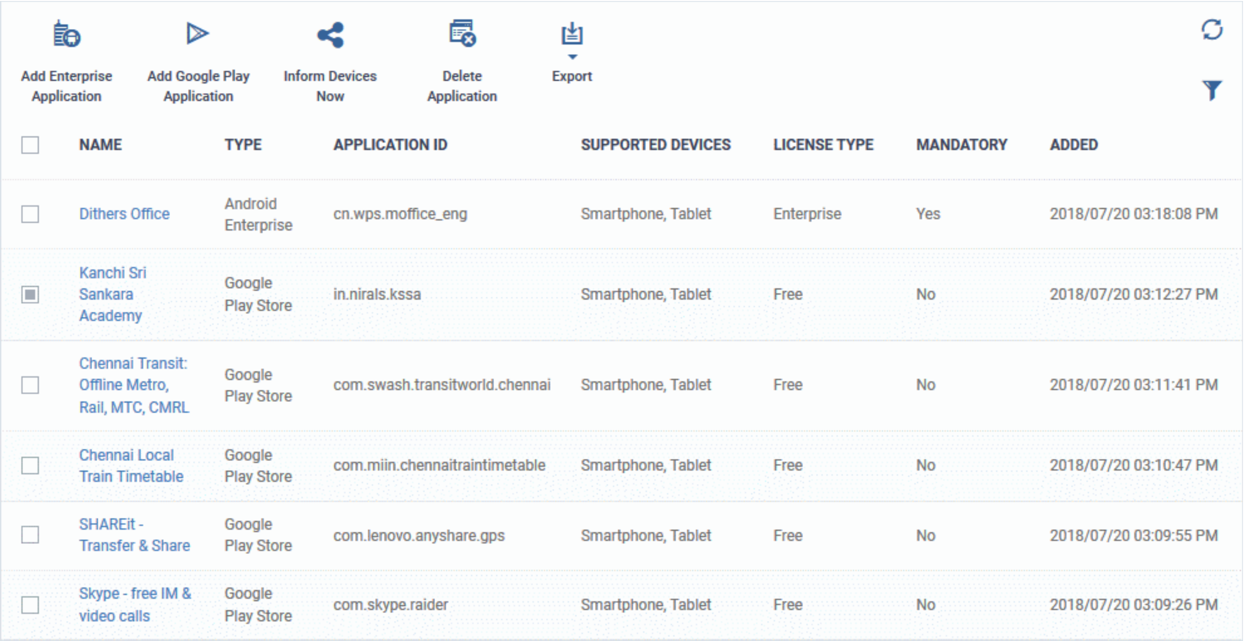
Do you really want to delete selected application(s)?

Confirm | Cancel

- Click 'Confirm' in the confirmation dialog to remove the app(s)

## 9.2. Android Apps

- Click 'Application Store' > 'Android Store'.
- The store contains all Android apps that have been uploaded to Endpoint Manager. You can deploy selected apps to all managed devices or to specific devices.
- You can add new apps from the Google Play Store or upload your own custom enterprise apps. You can synchronize the app list with managed Android devices and edit existing app parameters.
- You can specify whether an app is a mandatory install or an optional install.



| □ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| □ | Dithers Office | Android Enterprise | cn.wps.moffice_eng | Smartphone, Tablet | Enterprise | Yes | 2018/07/20 03:18:08 PM |
| ☑ | Kanchi Sri Sankara Academy | Google Play Store | in.nirals.kssa | Smartphone, Tablet | Free | No | 2018/07/20 03:12:27 PM |
| □ | Chennai Transit: Offline Metro, Rail, MTC, CMRL | Google Play Store | com.swash.transitworld.chennai | Smartphone, Tablet | Free | No | 2018/07/20 03:11:41 PM |
| □ | Chennai Local Train Timetable | Google Play Store | com.miin.chennaitraintimetable | Smartphone, Tablet | Free | No | 2018/07/20 03:10:47 PM |
| □ | SHAREit - Transfer & Share | Google Play Store | com.lenovo.anyshare.gps | Smartphone, Tablet | Free | No | 2018/07/20 03:09:55 PM |
| □ | Skype - free IM & video calls | Google Play Store | com.skype.raider | Smartphone, Tablet | Free | No | 2018/07/20 03:09:26 PM |

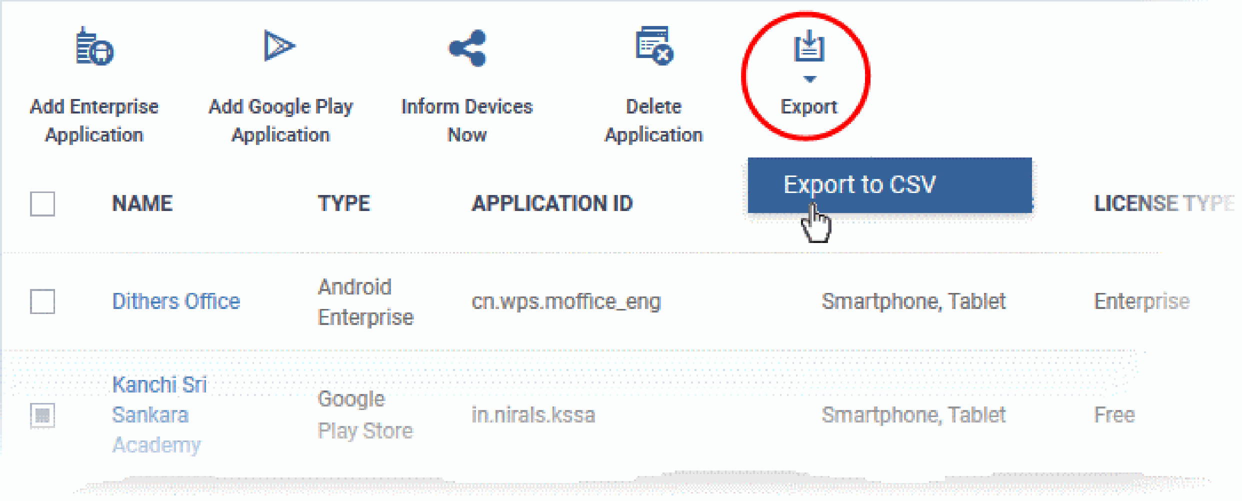
| 'Android Store' - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | Label of the application.<br>• Click the name to view details of the application.<br>• The screen also lets you edit app details. See **Manage Android Apps** for more details. |
| Type | The source type of the app. Possible types are:<br>• Google Play Store Application<br>• Android Enterprise Application uploaded by the administrator |
| Application ID | The bundle identifier of the app. |
| Supported Devices | The types of devices with which the application is compatible. |
| License Type | Whether the app is a free, paid or enterprise version. |
| Mandatory | Whether the app has been marked to be installed compulsorily on the devices. See '**Add Android Apps and Install them on Devices**' for more details |
| Added | The date and time at which the app was added to repository. |
| **Controls** | |
| Add Enterprise Application | Add custom applications to Endpoint Manager by uploading the .apk package files. See **Add Android Apps and Install them on Devices** for more details. |
| Add App Store Application | Add Android apps from the Play Store by entering the app name. See **Add Android Apps and Install them on Devices** for more details. |
| Inform Devices Now | Synchronize the app list with enrolled Android devices. |
| Delete Application | Remove an application from the Android app repository. |
| Export | Save the list of Android apps as a comma separated values (csv) file. See **Export the** |

| | |
|---|---|
| | List of Android Applications for more details. |

## Export the List of Android Applications

Export the list of Android applications to a .csv file as follows:

- Click 'Application Store' > 'Android Store'.
- Click the 'Export' button above the table then choose 'Export to CSV':

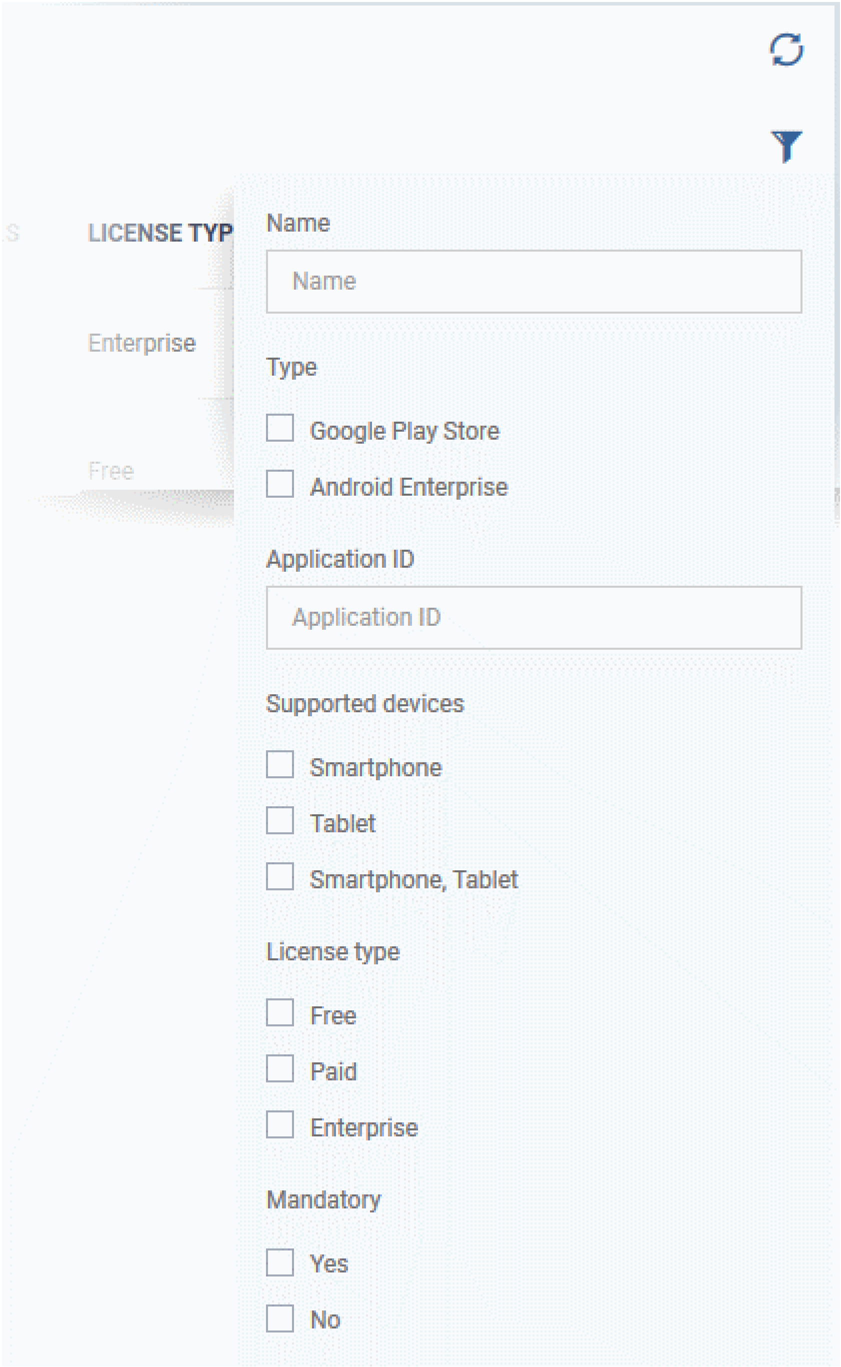


| □ | NAME | TYPE | APPLICATION ID | | LICENSE TYPE |
|---|---|---|---|---|---|
| □ | Dithers Office | Android Enterprise | cn.wps.moffice_eng | Smartphone, Tablet | Enterprise |
| ▣ | Kanchi Sri Sankara Academy | Google Play Store | in.nirals.kssa | Smartphone, Tablet | Free |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## Sort, Search and Filter Options

- Click a column header to sort items in alphabetical order of entries in the column.
- Click the funnel button ▼ to open the filter options.



Name

Name

Type

□ Google Play Store

□ Android Enterprise

Application ID

Application ID

Supported devices

□ Smartphone

□ Tablet

□ Smartphone, Tablet

License type

□ Free

□ Paid

□ Enterprise

Mandatory

□ Yes

□ No

Click the following links for more help:

- Add Android Apps and Install them on Devices
- Manage Android Apps

## 9.2.1. Add Android Apps and Install them on Devices

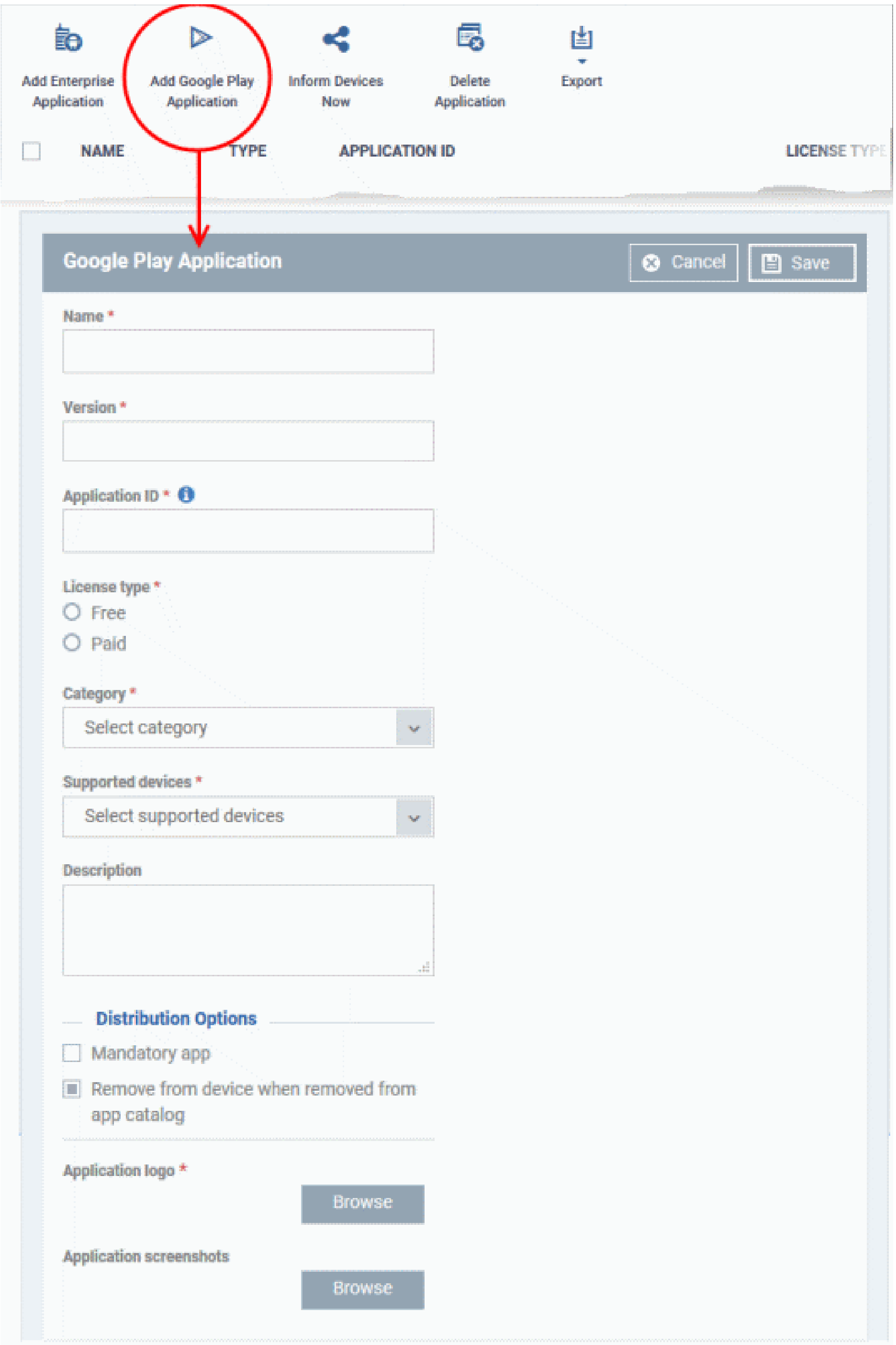
- You can add apps direct from the Google Play Store or by uploading custom apps
- Apps in the repository can be installed on all or specific managed Android devices.

See the following sections for more details:

- **Add an Android App from Google Play Store**
- **Add a Custom/Enterprise Android App**

## Add an App from the Google Play Store

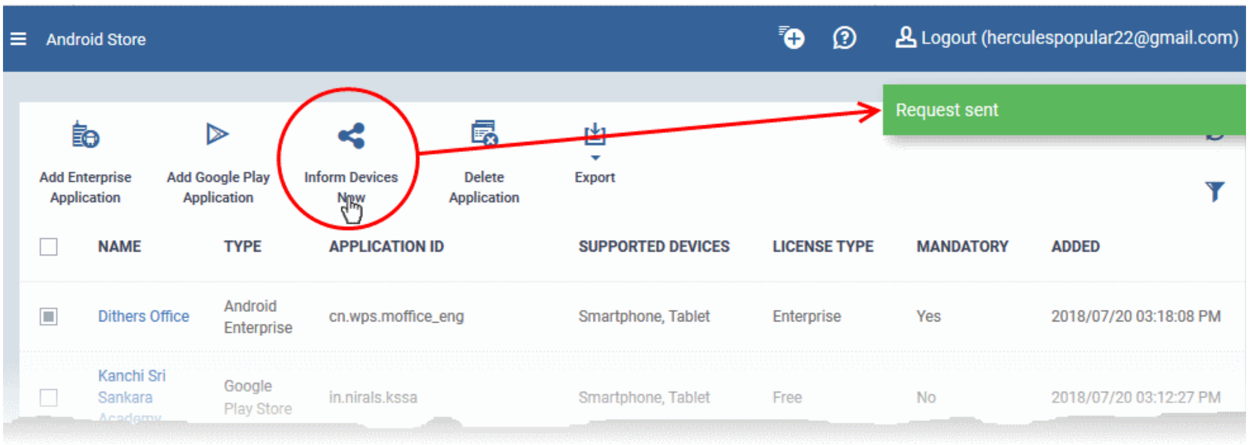
- Click 'Application Store' > 'Android Store'
- Click the 'Add Google Play Application' button
- Type the first few letters of the app in the 'Name' field on the form. Endpoint Manager will search for matching apps from the store.
- Select the correct app from the list of suggestions. Most of the form will then be auto-populated from the app details



| Google Play Application - Table of Parameters | | |
|---|---|---|
| **Form Element** | **Type** | **Description** |
| Name | Text Field | Enter the label of the application.<br>• Type the first few letters of the app name<br>• EM displays matching results<br>• Choose the app you want to add from the suggestions<br>• Once you have chosen the app, most other form fields will be auto-populated. |
| Version | Text Field | The version number of the application.<br>This field will be auto-populated after choosing an app in the 'Name' field.<br>• Enter the version number manually if the version number wasn't automatically fetched. |
| Application ID | Text Field | The application ID (bundle identifier) of the app. Usually this is in the reverse DNS format, for example, 'com.comodo.mobile.comodoantitheft'. 'In the Google Play store, the identifier is located after the '=' in the URL. An example is shown below:<br>**https://play.google.com/store/apps/details?id=com.comodo.mdm**<br>• Click the help icon beside the field displays how to retrieve the application ID for the Play Store Apps.<br>This field will be auto-populated on entering the correct app name in the 'Name' field. |
| License Type | Radio Button | Whether the app is free or paid.<br>This option will be pre-chosen depending on the app chosen in the 'Name' field. |
| Category | Drop-down | The classification of the application.<br>The category will be auto-selected depending on the app chosen in the 'Name' field.<br>• Select the category from the drop-down if it is not auto-populated. |
| Supported devices | Drop-down | The category of devices on which the app can be run.<br>This device type will be auto-selected depending on the app chosen in the 'Name' field.<br>• Select the device type from the drop-down if it is not auto-populated. |
| Description | Text Field | The 'Description' filed will be auto-populated with the description of the selected app, from the Google Play Store page.<br>The text field also enables you to edit the description or enter your own description of the app. |
| Mandatory app | Checkbox | Specify whether the app is a compulsorily install. If enabled, the app will be automatically pushed to all enrolled devices. |
| Remove from device when | Checkbox | The app will be uninstalled from devices if it is removed from the EM app |

| Google Play Application - Table of Parameters | | |
|---|---|---|
| removed from app catalog | | store. |
| 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 listed in the 'Android Store'. It will be synced to the devices during the next cycle.
- Click 'Inform Devices Now' if you want to push the app immediately.


Android Store
Logout (herculespopular22@gmail.com)
Request sent
Add Enterprise Application
Add Google Play Application
Inform Devices Now
Delete Application
Export

| | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| ☒ | Dithers Office | Android Enterprise | cn.wps.moffice_eng | Smartphone, Tablet | Enterprise | Yes | 2018/07/20 03:18:08 PM |
| □ | Kanchi Sri Sankara Academy | Google Play Store | in.nirals.kssa | Smartphone, Tablet | Free | No | 2018/07/20 03:12:27 PM |

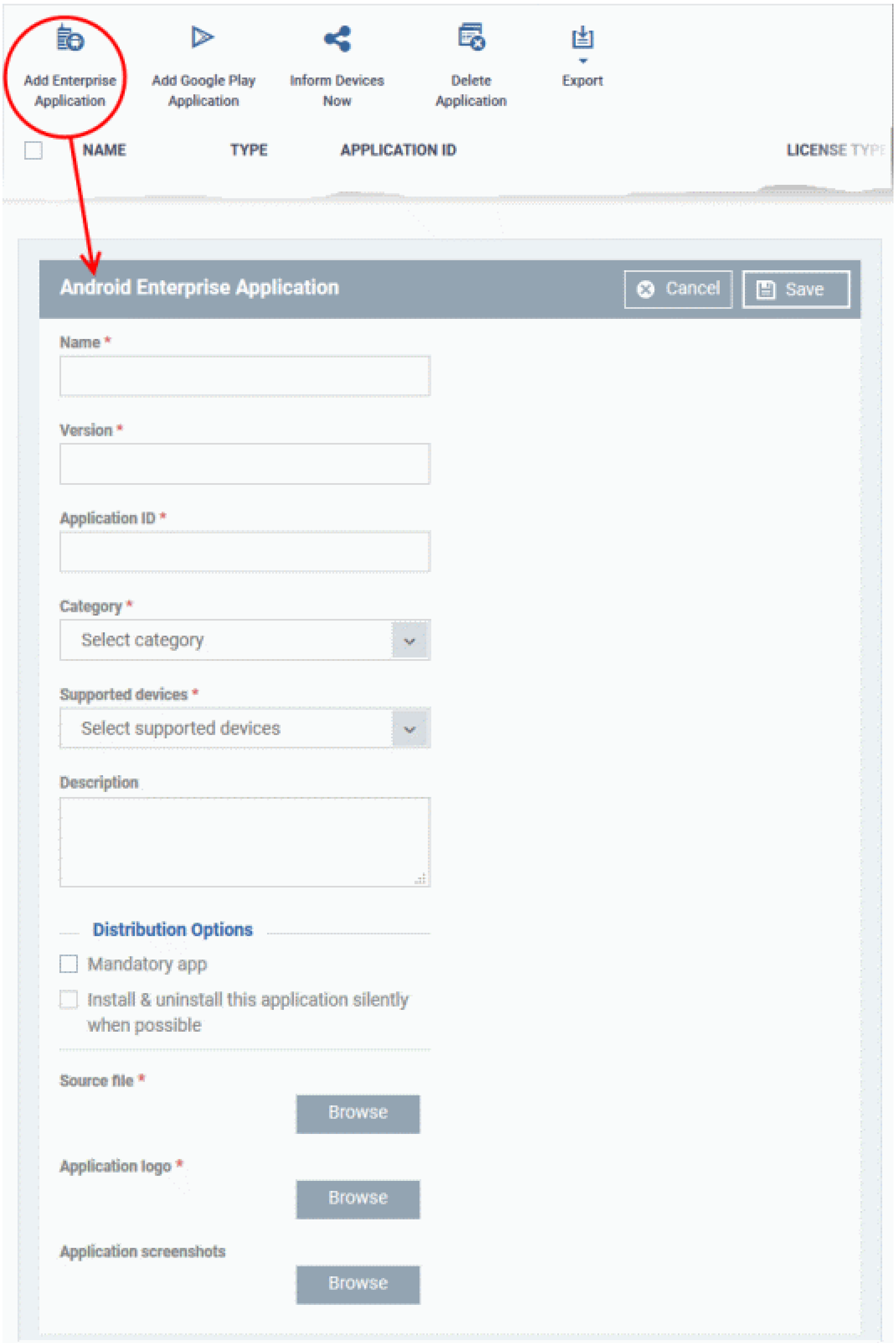
## Add a Custom/Enterprise Android App

- Custom apps can be added to the repository by uploading the app's .apk file.
- App details will be automatically fetched by parsing the file. You will need to manually enter 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 Endpoint Manager console is accessed.

### To add Custom/Enterprise Android Apps

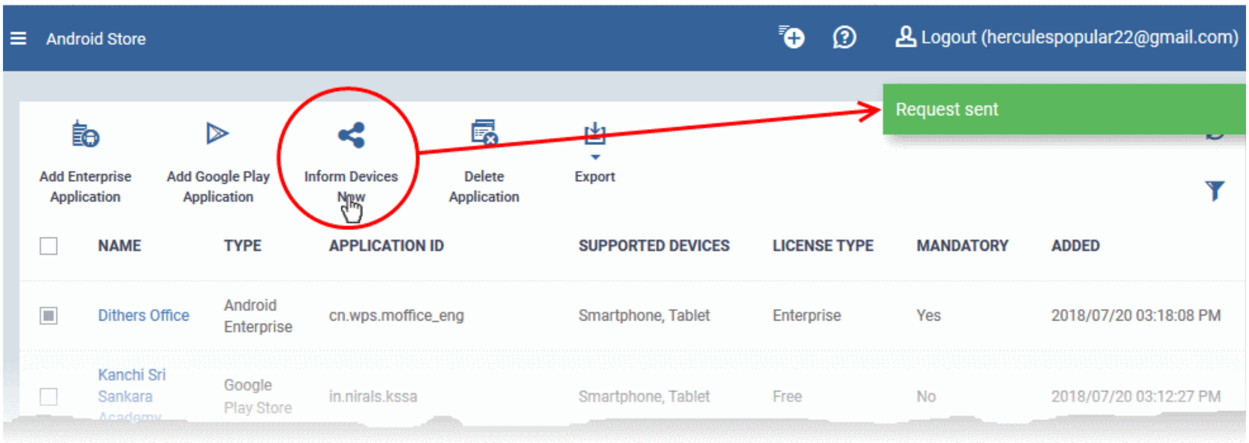
- Click 'Application Store' > 'Android Store'
- Click 'Add Enterprise Application' from the options at the top.



- 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 form details auto-populated. See the previous section if you need advice on the fields in this form.

- Click 'Save' after entering the details.
- The app will be added to the repository and listed in the 'Android Store' interface. It will be synced to enrolled devices during the next update cycle.
- Click 'Inform Devices Now' if you want to push the app out immediately.

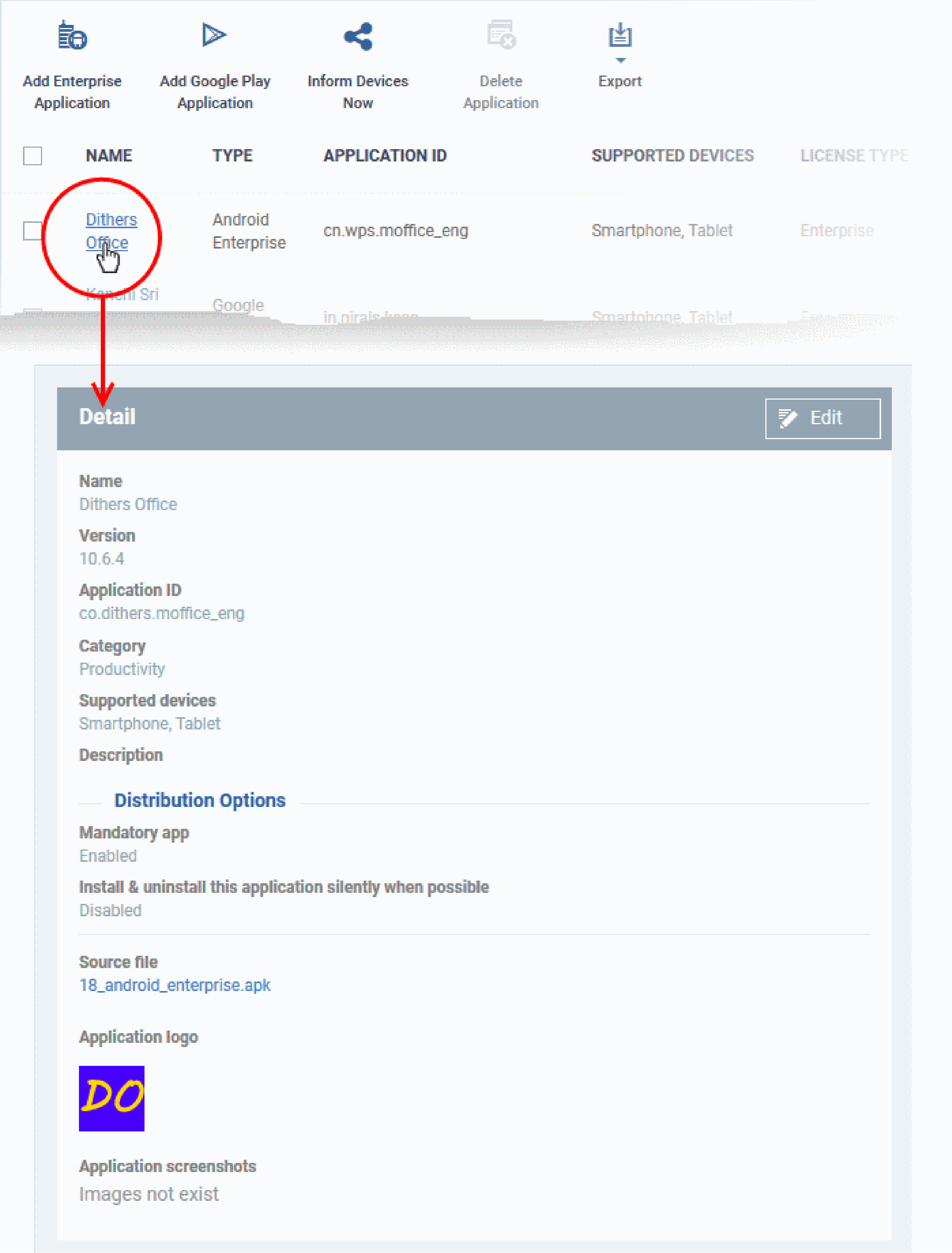

Android Store
Logout (herculespopular22@gmail.com)
Request sent
Add Enterprise Application
Add Google Play Application
Inform Devices Now
Delete Application
Export

| □ | NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE | MANDATORY | ADDED |
|---|---|---|---|---|---|---|---|
| ☒ | Dithers Office | Android Enterprise | cn.wps.moffice_eng | Smartphone, Tablet | Enterprise | Yes | 2018/07/20 03:18:08 PM |
| □ | Kanchi Sri Sankara Academy | Google Play Store | in.nirals.kssa | Smartphone, Tablet | Free | No | 2018/07/20 03:12:27 PM |

## 9.2.2. Manage Android Apps

The 'Android Apps' interface lets you view and edit app details, and remove unwanted apps from the repository.

- Click 'Application Store' > 'Android Store'
- Click the name of an app



| NAME | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE |
|---|---|---|---|---|
| Dithers Office | Android Enterprise | cn.wps.moffice_eng | Smartphone, Tablet | Enterprise |

**Detail**

**Name**
Dithers Office

**Version**
10.6.4

**Application ID**
co.dithers.moffice_eng

**Category**
Productivity

**Supported devices**
Smartphone, Tablet

**Description**

**Distribution Options**

**Mandatory app**
Enabled

**Install & uninstall this application silently when possible**
Disabled

**Source file**
18_android_enterprise.apk

**Application logo**

DO

**Application screenshots**
Images not exist

The 'Application Details' page contains a description of the app and various other identifying information. You can also edit app details from here.

**To edit the details of an application**

- Click on the 'Edit' button Edit at the top right .

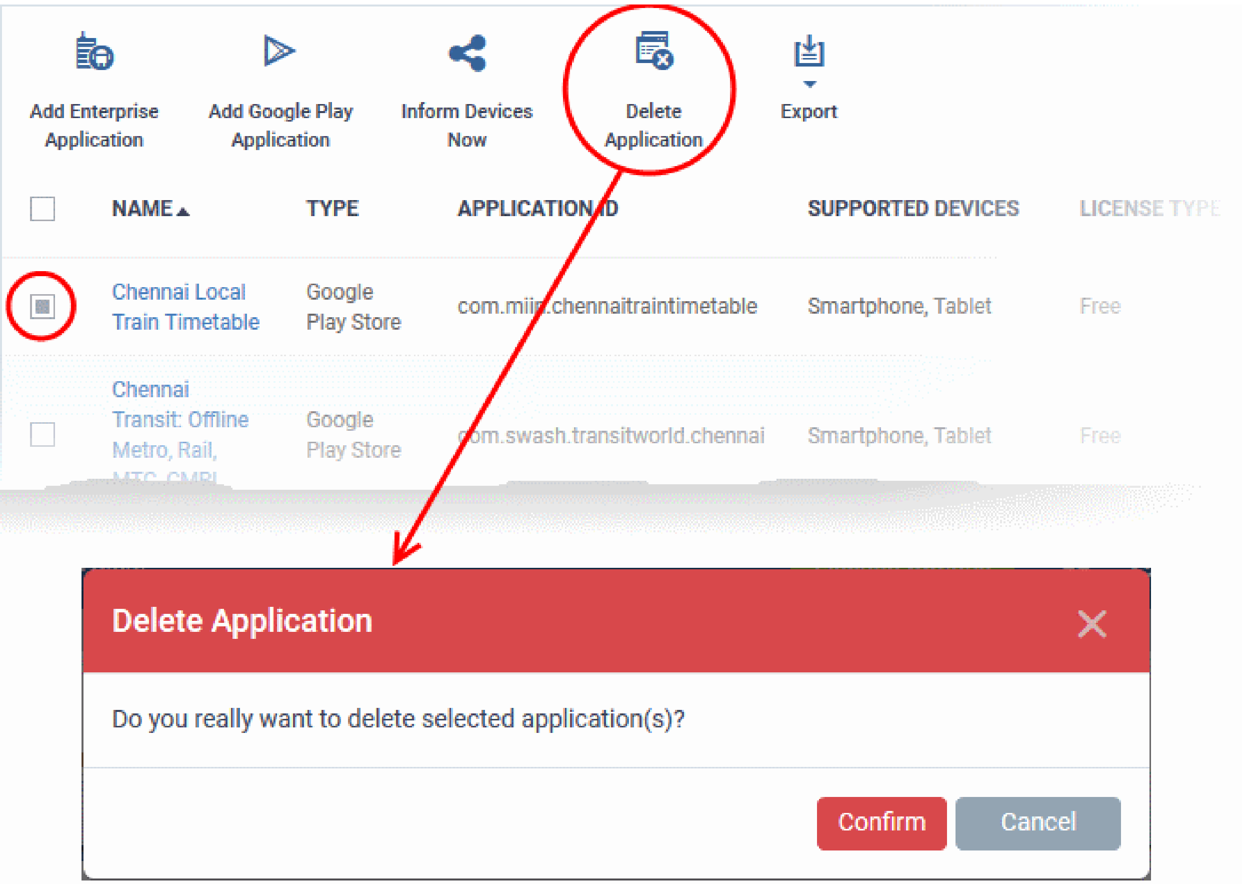
The application details edit screen will be displayed. This screen is similar to the interface for adding a new application. For more details on the parameters, see **Add Android Apps and Install them on Devices**.

### Remove Apps from the Android App Catalog

- You can remove unwanted applications from the repository at any time.
- If you also select 'Remove from device when removed from app catalog', the app will also be deleted from devices.

**To remove selected Apps**

- Click 'Application Store' > 'Android Store'
- Select the app(s) you want to remove and click the 'Delete Application' button:



| □ | NAME ▲ | TYPE | APPLICATION ID | SUPPORTED DEVICES | LICENSE TYPE |
|---|---|---|---|---|---|
| ☒ | Chennai Local Train Timetable | Google Play Store | com.miir.chennaitraintimetable | Smartphone, Tablet | Free |
| □ | Chennai Transit: Offline Metro, Rail, MTC, CMBT | Google Play Store | com.swash.transitworld.chennai | Smartphone, Tablet | Free |

**Delete Application**

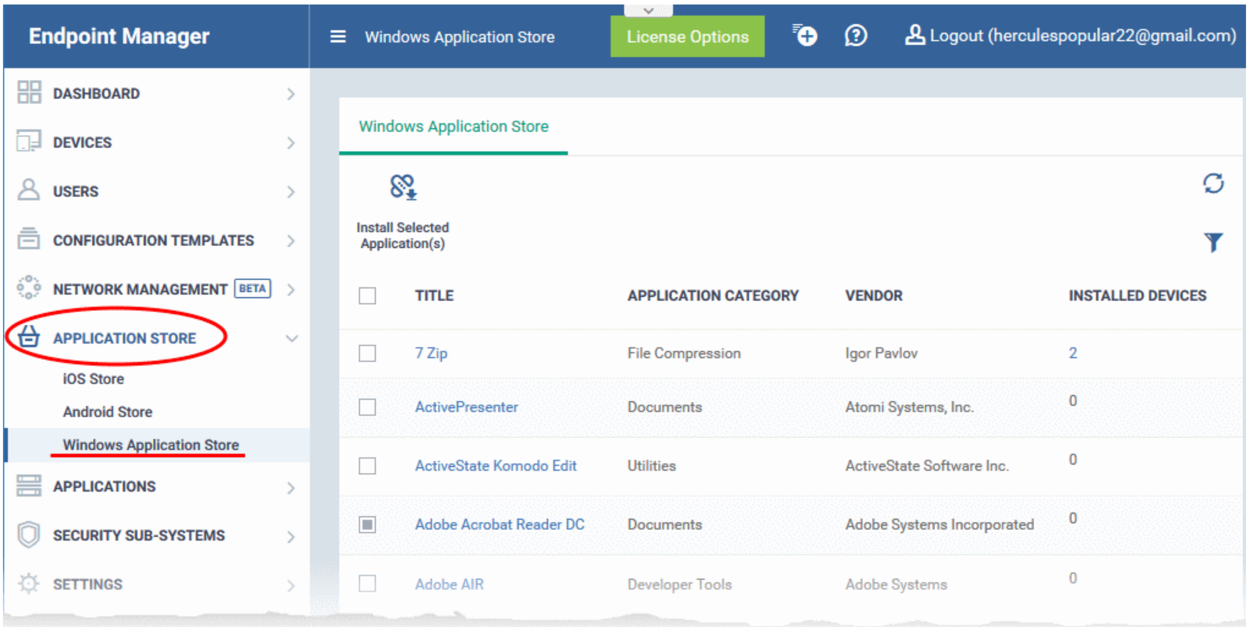
Do you really want to delete selected application(s)?

- Click 'Confirm' to remove the app(s).

# 9.3. Windows Apps

The 'Windows Application Store' is a library of applications which can be deployed to Windows devices. Applications you can install include Adobe Acrobat, CCleaner, Firefox, Thunderbird and more. The list is continuously updated by Comodo.

- Click 'Application Store' > 'Windows Application Store' to open the interface



| | TITLE | APPLICATION CATEGORY | VENDOR | INSTALLED DEVICES |
|---|---|---|---|---|
| □ | 7 Zip | File Compression | Igor Pavlov | 2 |
| □ | ActivePresenter | Documents | Atomi Systems, Inc. | 0 |
| □ | ActiveState Komodo Edit | Utilities | ActiveState Software Inc. | 0 |
| ☒ | Adobe Acrobat Reader DC | Documents | Adobe Systems Incorporated | 0 |
| □ | Adobe AIR | Developer Tools | Adobe Systems | 0 |

| Windows Application Store - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Title | The name of the application.<br>• Click the name to view application details, including version number and any devices on which it is installed.<br>• See **View Application Details**. |
| Application Category | The category under which the application is grouped. |
| Vendor | The name of the organization / person that distributes the application |
| Installed Devices | The number of devices on which the application is installed. Clicking the number will open the 'Device List' screen. See **View Application-Installed Devices List**. |
| **Controls** | |
| Install Selected Application(s) | Allows you to install selected application(s) on managed devices. See **Install Windows Apps on Devices** for more details. |

- Click any column header to sort items in ascending/descending order of entries in that column.
- Click the refresh icon ⟳ on the top-right to update the table list
- Click the funnel icon ▼ on the top-right to search for Windows applications by title, vendor and/or application category.
- To display all the items again, remove the search key from filter and click 'Apply'.
- EM returns 20 results per page when you perform a search. Click the arrow next to 'Results per page' to change the number of results shown.

From the interface you can:

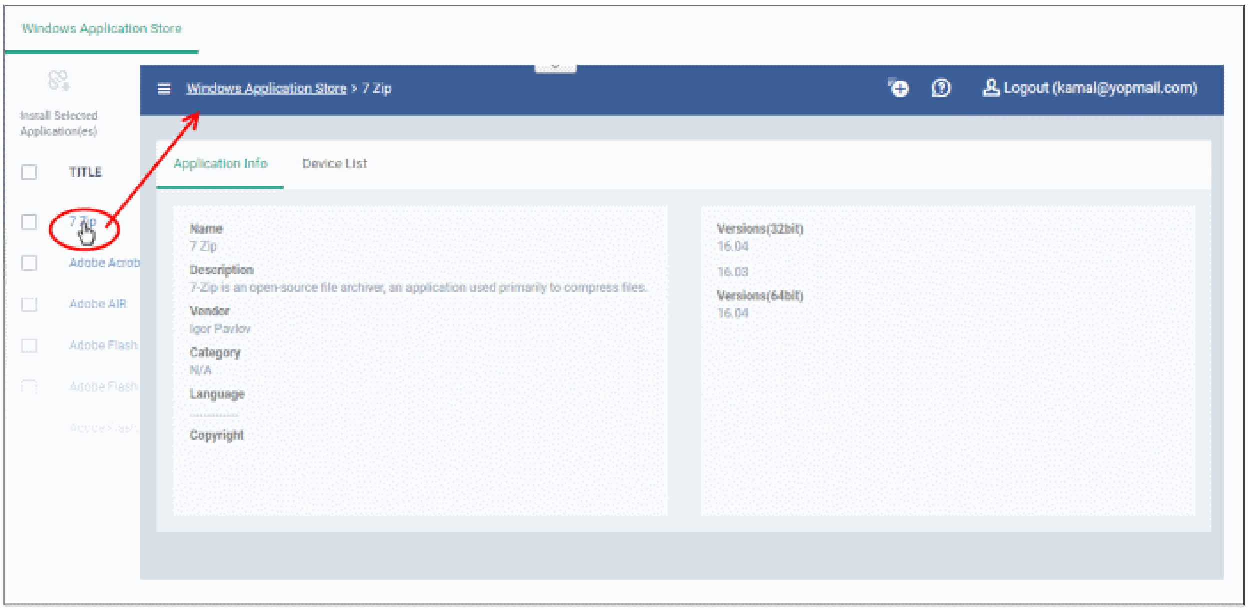
- **View Application Details**
- **View Application-Installed Devices List**

- Install Applications on Devices

## View Application Details

- Click an application's name in the list

A new screen with 'Application Info' and 'Device List' tabs will open.



Windows Application Store

Install Selected Application(es)

| □ | TITLE |
|---|---|
| □ | 7 Zip |
| □ | Adobe Acrob |
| □ | Adobe AIR |
| □ | Adobe Flash |
| □ | Adobe Flash |

Windows Application Store > 7 Zip

Logout (kamal@yopmail.com)

Application Info | Device List

Name
7 Zip
Description
7-Zip is an open-source file archiver, an application used primarily to compress files.
Vendor
Igor Pavlov
Category
N/A
Language

Copyright

Versions(32bit)
16.04
16.03
Versions(64bit)
16.04

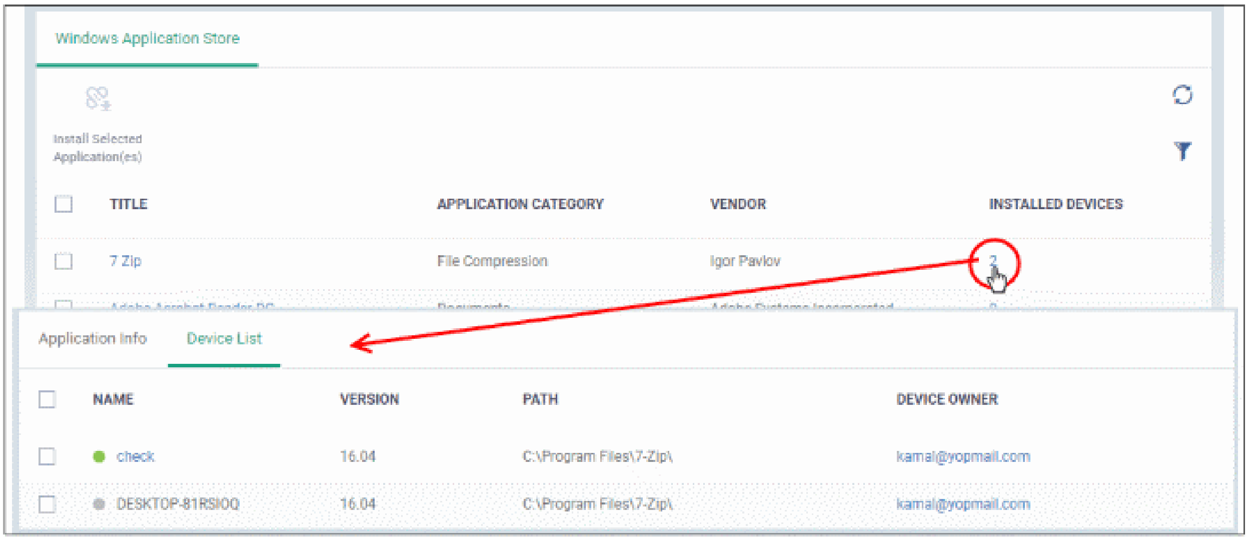
By default, the 'Application Info' tab will be displayed. The details of the application such as name, description, vendor, category including version number(s) will be available.

- The 'Device List' tab displays the device details on which the application is installed. This screen is same that is shown when the number in the 'Installed Devices' column is clicked. See View Application-Installed Devices List for details.

## View Application-Installed Devices List

- Click the number on the far right beside an application's name ('Installed Devices' column)

A new screen with 'Application Info' and 'Device List' tabs will open.



Windows Application Store

Install Selected Application(es)

| □ | TITLE | APPLICATION CATEGORY | VENDOR | INSTALLED DEVICES |
|---|---|---|---|---|
| □ | 7 Zip | File Compression | Igor Pavlov | 2 |

Application Info | Device List

| □ | NAME | VERSION | PATH | DEVICE OWNER |
|---|---|---|---|---|
| □ | ● check | 16.04 | C:\Program Files\7-Zip\ | kamal@yopmail.com |
| □ | ● DESKTOP-81RSI0Q | 16.04 | C:\Program Files\7-Zip\ | kamal@yopmail.com |

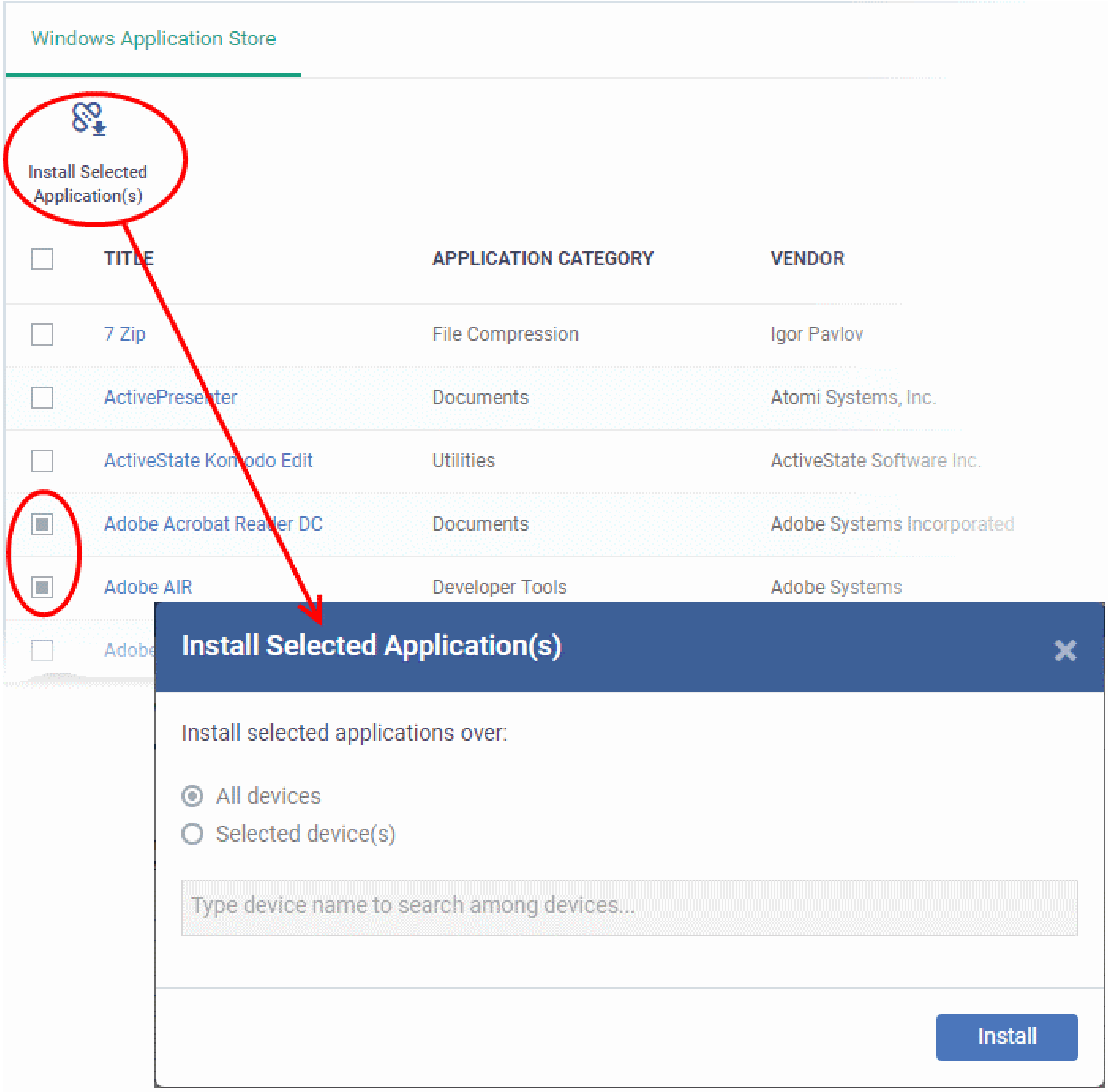
By default, the 'Device List' tab will be displayed. The details of the device such as name, application version, installation path and name of the device owner will be available.

- Click the name of a device to view its **summary** information. See '**Manage Windows Devices**' for more information about how to manage devices.

## 9.3.1. Install Windows Apps on Devices

The 'Windows Application Store' lets you install apps on managed Windows devices.

- Click 'Application Store' > 'Windows Application Store'
- Select the applications you want and click 'Install Selected Application(s)':



| □ | TITLE | APPLICATION CATEGORY | VENDOR |
|---|---|---|---|
| □ | 7 Zip | File Compression | Igor Pavlov |
| □ | ActivePresenter | Documents | Atomi Systems, Inc. |
| □ | ActiveState Komodo Edit | Utilities | ActiveState Software Inc. |
| ☑ | Adobe Acrobat Reader DC | Documents | Adobe Systems Incorporated |
| ☑ | Adobe AIR | Developer Tools | Adobe Systems |
| □ | Adobe | | |

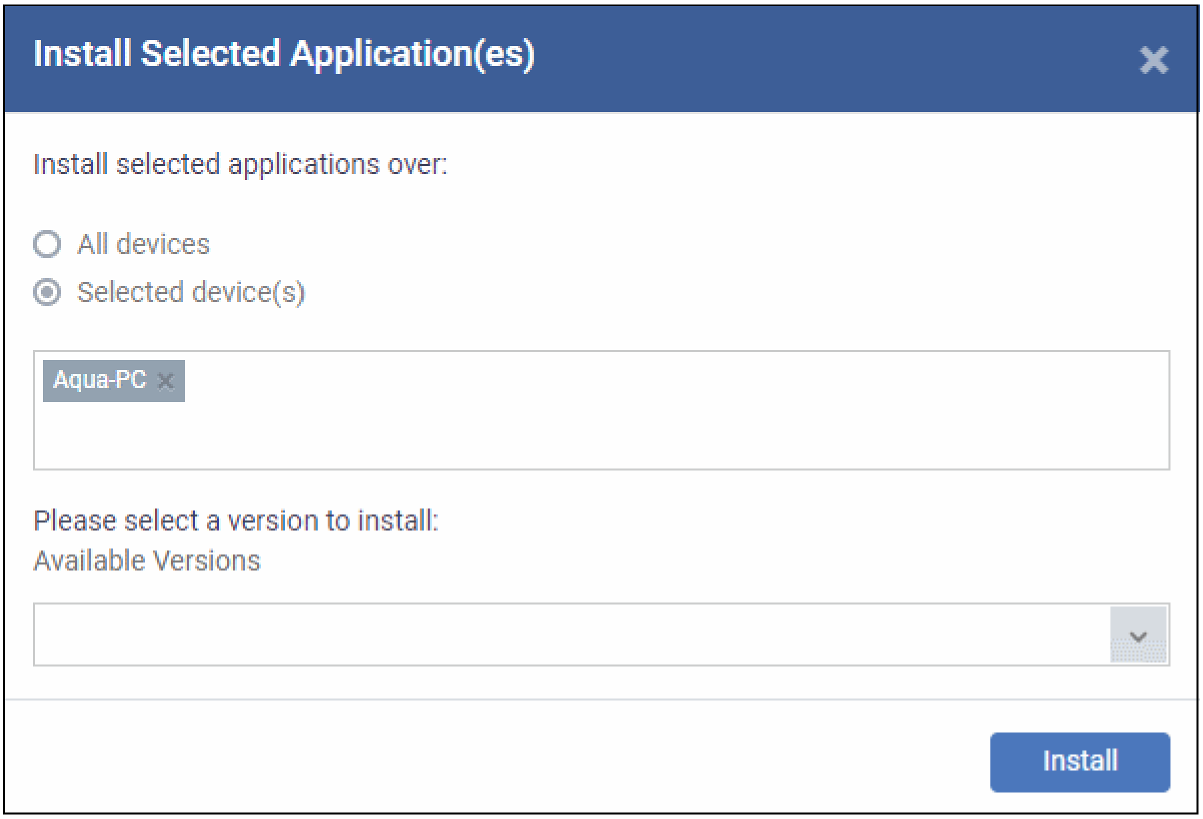
**Install Selected Application(s)**

Install selected applications over:

● All devices
○ Selected device(s)

Type device name to search among devices...

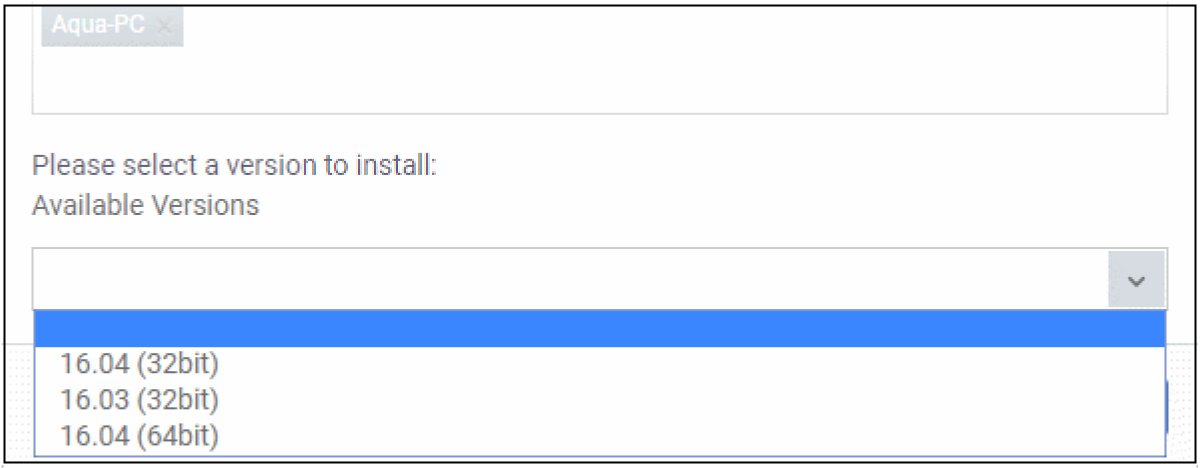
- **All Devices -** Install the latest version of the apps on every managed Windows device.
- **Selected Devices -** Install the apps on specific devices:
  - Choose 'Selected device(s)'


Install Selected Application(es)
Install selected applications over:
○ All devices
● Selected device(s)
Aqua-PC ×
Please select a version to install:
Available Versions
Install

- Enter first few letters of the device name and select from the suggestions.
- Repeat to add multiple devices.

Note - The version number drop-down is not available if you select 'All devices', multiple devices, or multiple apps.

- Select the application version (available for single application/ single device installs only)



- Click 'Install'

The install command is sent immediately. The 'Software Inventory' screen shows all apps installed on a particular device. See '**View Applications Installed on a Device**' for more information.

# 10. Security Sub Systems

The 'Security Sub systems' menu lets you:

- View the infection status of managed devices.
- Run antivirus and file-rating scan on devices.
- Update the virus database on devices.
- View and manage quarantined files.
- View and modify the trust rating of files discovered on devices
- View unknown files currently running in the container on an endpoint.
- View unknown files which were automatically submitted to Valkyrie for analysis
- View a consolidated list of all security events on all managed Windows endpoints.
- View a list of external connection attempts from devices.

The following sections contain more details on each area:

- **Security Dashboards**
  - **View Security Events by Time**
  - **View Security Events by File**
  - **View Security Events by Device**
- **View Contained Applications**
- **Manage File Trust Ratings on Windows Devices**
- **View Valkyrie Analyzed Files**
- **Antivirus and File Rating scans**
  - **Run Antivirus and/or File Rating Scans on Devices**
  - **Handle Malware on Scanned Devices**
  - **Update Virus Signature Database on Windows, Mac OS and Linux Devices**
- **View and Manage Identified Malware**
- **View and Manage Quarantined Items**
- **View Threat History**
- **View and Manage Autoruns Items**
- **View History of External Device Connection Attempts**

# 10.1. Security Dashboards

- Click 'Security Sub-Systems' > 'Security Dashboards'

The security dashboard is a list of all security events on managed endpoints. This includes events from the antivirus, containment, application-control, autorun control, and virtual desktop components.

Endpoint Manager retains security event logs for 12 months for PCI-DSS compliance.

Events that are captured include:

**Antivirus** - Windows, Mac OS, and Linux devices

- File blocked, moved to quarantine, or ignored
- File restored/removed from quarantine
- File skipped by a virus scan
- File rated as trusted, or submitted as a false positive, at the scan results screen
- File added to the exclusions list

**Containment** - Windows devices

- File blocked, ignored, or run in the container by:
    - Auto-containment rules in the profile on the device
    - A local user running the file in the container on a one-off basis

**Application Control** - Windows devices

- Unrecognized or malicious file added to, or removed from, the CCS 'File list'.
- Changes to the trust rating of a file
- See **Manage File Trust Ratings on Windows Devices** for more details.

**Autorun Control** - Windows devices

- Records the action taken by CCS on apps that try to modify Windows services, startup entries, and scheduled tasks.

  Recorded actions include:

    - Ignore
    - Terminate
    - Terminated and disabled
    - Quarantined and disabled
    - Restored
    - Deleted

**Virtual Desktop** - Windows devices

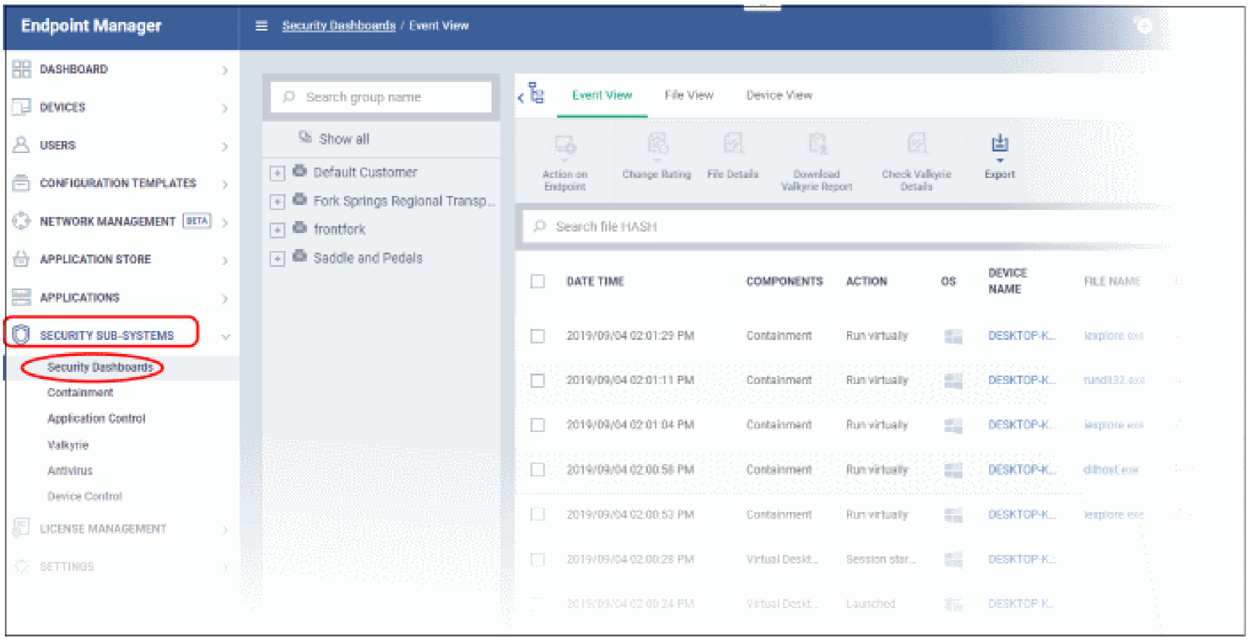
- Virtual desktop activity on endpoints. Recorded actions include:
    - Launched
    - Terminated
    - Session started
    - Session paused
    - Session continued
    - Session terminated
    - Switched to host

- Switched to virtual desktop

The interface also lets you rate files, view file details, and move files in or out of quarantine.

**Open the dashboard:**

- Click 'Security Sub-Systems' > 'Security Dashboards'
    - Select a company or group to view devices in that group
      Or
    - Select 'Show all' to view every device enrolled to Endpoint Manager



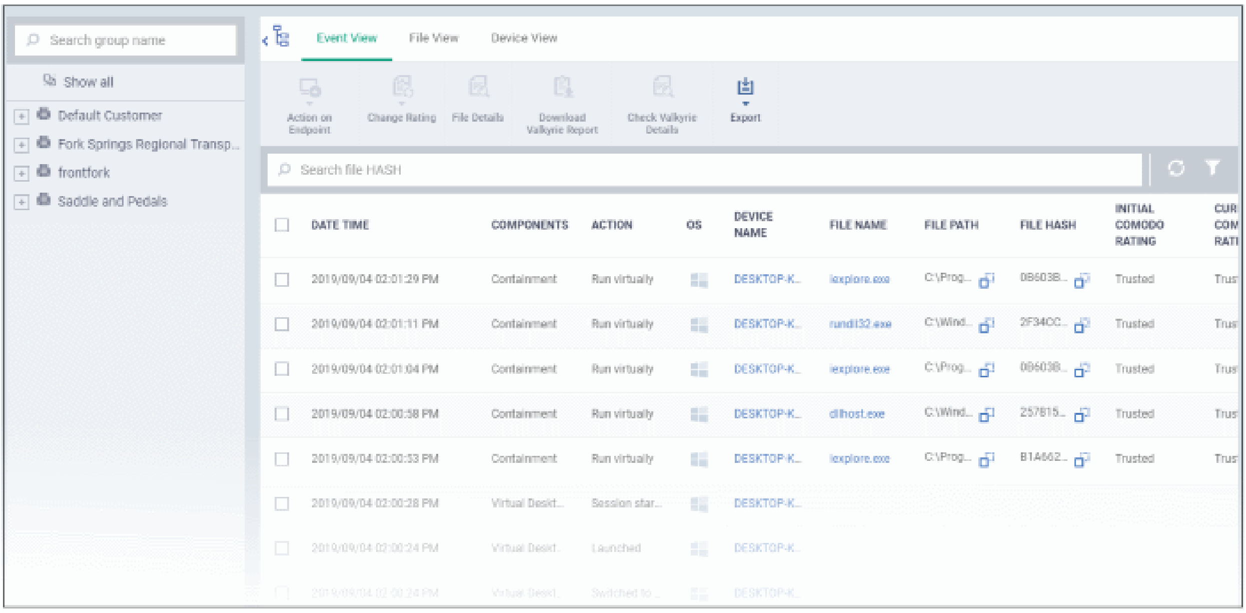
| DATE TIME | COMPONENTS | ACTION | OS | DEVICE NAME | FILE NAME |
|---|---|---|---|---|---|
| 2019/09/04 02:01:29 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe |
| 2019/09/04 02:01:11 PM | Containment | Run virtually | | DESKTOP-K... | rundll32.exe |
| 2019/09/04 02:01:04 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe |
| 2019/09/04 02:00:58 PM | Containment | Run virtually | | DESKTOP-K... | dllhost.exe |
| 2019/09/04 02:00:53 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe |
| 2019/09/04 02:00:28 PM | Virtual Deskt... | Session star... | | DESKTOP-K... | |
| 2019/09/04 02:00:24 PM | Virtual Deskt... | Launched | | DESKTOP-K... | |

The dashboard has three tabs:

- **Event View** - Shows events in chronological order. See **View Security Events by Time** for more details.
- **File View** - All events concerning a particular file are grouped together. See **View Security Events by File** for more details.
- **Device View** - Shows all events that occurred on a specific device. See **View Security Events by Device** for more information.

## 10.1.1. View Security Events by Time

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
    - Select a company or group to view events in that group
      Or
    - Select 'Show all' to view all events
- Event view shows security events from all managed endpoints in chronological order:



| □ | DATE TIME | COMPONENTS | ACTION | OS | DEVICE NAME | FILE NAME | FILE PATH | FILE HASH | INITIAL COMODO RATING | CUR COM RATI |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 2019/09/04 02:01:29 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe | C:\Prog... | 0B603B... | Trusted | Trus |
| □ | 2019/09/04 02:01:11 PM | Containment | Run virtually | | DESKTOP-K... | rundll32.exe | C:\Wind... | 2F34CC... | Trusted | Trus |
| □ | 2019/09/04 02:01:04 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe | C:\Prog... | 0B603B... | Trusted | Trus |
| □ | 2019/09/04 02:00:58 PM | Containment | Run virtually | | DESKTOP-K... | dllhost.exe | C:\Wind... | 257815... | Trusted | Trus |
| □ | 2019/09/04 02:00:53 PM | Containment | Run virtually | | DESKTOP-K... | iexplore.exe | C:\Prog... | B1A662... | Trusted | Trus |
| □ | 2019/09/04 02:00:28 PM | Virtual Deskt... | Session star... | | DESKTOP-K... | | | | | |
| □ | 2019/09/04 02:00:24 PM | Virtual Deskt... | Launched | | DESKTOP-K... | | | | | |
| □ | 2019/09/04 02:00:24 PM | Virtual Deskt... | Switched to ... | | DESKTOP-K... | | | | | |

| Security Dashboards - Event View - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date/Time | The time at which the event occurred. |
| Components | The CCS module that reported the event. This can be 'Antivirus', 'Containment', 'Application Control', 'Autorun Control' or 'Virtual Desktop'. |
| Action | The response to the event. This shows how the file was handled by the component mentioned above.<br>Here are the possible actions per module:<br>**Antivirus** - Windows, Mac OS, and Linux devices<br>• Malware detected<br>• Malware quarantined<br>• Malware removed from quarantine<br>• Malware restored from quarantine<br>• Malware removed from infected file<br>• The file was skipped by the scan<br>• Detected malware ignored<br>• Detected malware blocked<br>• File added to exclusions<br>• File added to trusted files list<br>• File reported as a false positive from the results screen<br>**Containment** - Windows devices<br>• File run inside container with different restriction levels:<br>  • Restricted |

| Security Dashboards - Event View - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| | • Virtually<br>• File blocked<br>• File ignored<br>**Application Control** - Windows devices<br>• File added to the file list<br>• File removed from the endpoint<br>• Trust rating updated for a file<br>**Autorun Control** - Windows devices<br>• Detected item ignored<br>• Process / service stopped<br>• Auto-run process stopped. Corresponding auto-run entry removed. In the case of a service, CCS disables the service.<br>• Auto-start process quarantined. Corresponding auto-start entry removed. In the case of a service, CCS disables the service.<br>• Processes restored from quarantine<br>• File deleted from the endpoint<br>**Virtual Desktop** - Windows devices<br>• Launched<br>• Terminated<br>• Session started<br>• Session paused<br>• Session continued<br>• Session terminated<br>• Switched to host<br>• Switched to virtual desktop |
| Device Name | The label of the endpoint on which the event occurred.<br>• Click the name of a device to open its 'Device Details' interface.<br>• See **Manage Devices** for more details on the interface. |
| File Name | The label of the executable file affected by the action<br>• Click the name of a file to open its 'File Details' interface.<br>• See **View the details of a file** for more details. |
| File Path | The installation location of the executable file on the endpoint<br>• Click the ⧉ icon to copy the path to the clipboard. |
| File Hash | The SHA 1 hash value of the executable file<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Initial Comodo Rating | The trust rating awarded by Comodo File Look-up Service (FLS) to the file before the |

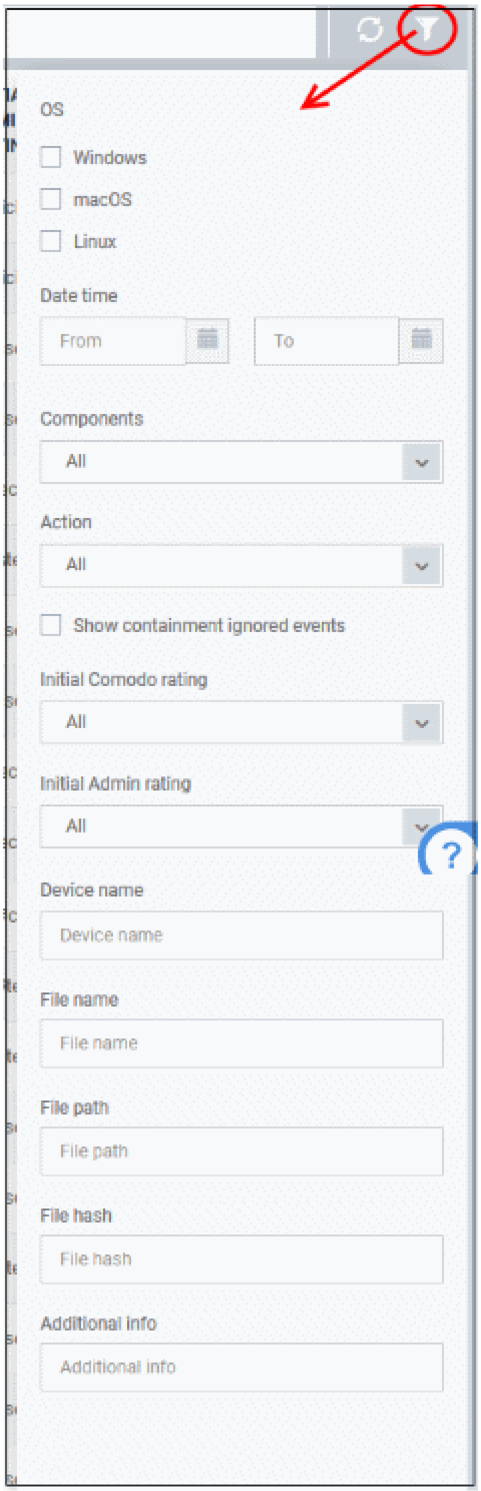
| Security Dashboards - Event View - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| | event. |
| Current Comodo Rating | The present trust rating of the file as per the Comodo FLS. |
| Initial Admin Rating | The trust rating of the file as manually set by the admin before the event, if any.<br>• See **Rate Files as Trusted, Malicious or Unrecognized** for more details. |
| Current Admin Rating | The most recent trust rating of the file as manually set by the admin after the event, if any.<br>• See **Rate Files as Trusted, Malicious or Unrecognized** for more details. |
| Additional Info | Provides the current status of the event or the action taken on the affected file. |
| **Controls** | |
| Action on Endpoints | Delete or restore a file from quarantine on the endpoint. Applies to events where malware or autorun items were quarantined.<br>• See **Handle Quarantined Items** for more details |
| Change rating | Assign a new admin rating to a file (trusted, malicious or unrecognized).<br>• See **Rate Files as Trusted, Malicious or Unrecognized** for more details. |
| File Details | View complete information about the file that caused the event. You can also view a history of actions taken by the file.<br>• See **View the details of a file** for more details. |
| Download Valkyrie Report | Get a detailed Valkyrie analysis report for the file as a PDF.<br>• See **Get Valkyrie Report of a file** for more details |
| Check Valkyrie Details | View the Valkyrie analysis on a file.<br>• See **View Valkyrie analysis details of file** for more details |
| Export | Save the list of events as a comma separated values (csv) file.<br>• See **Export the List of Events** for more details. |

The 'Event View' interface lets you to:

- **Handle Quarantined Items**
- **Rate Files as Trusted, Malicious or Unrecognized**
- **View the details of a file**
- **Get Valkyrie Report of a file**
- **View Valkyrie analysis details of a file**
- **Export the List of Events**

## Sorting, Search and Filter Options

- Click the 'Date/Time', 'File Name', 'File Path' or 'File Path' column header to sort events in ascending or descending order
- Enter the SHA 1 hash value of a file in the search box to filter the events involving the file.
- Click the funnel icon on the top right to open more filter options:



OS

□ Windows

□ macOS

□ Linux

Date time

From | To

Components

All

Action

All

□ Show containment ignored events

Initial Comodo rating

All

Initial Admin rating

All

Device name

Device name

File name

File name

File path

File path

File hash

File hash

Additional info

Additional info

- Use the search fields to filter events by OS, date/time, file rating and other criteria.
- By default, 'Security Dashboards' > 'Event View' does not show the files that are ignored by auto-containment rules.

  - Select 'Show containment ignored events' to include the files ignored by auto-containment rules in the events list
- To display all items again, clear any search filters then click 'OK'.

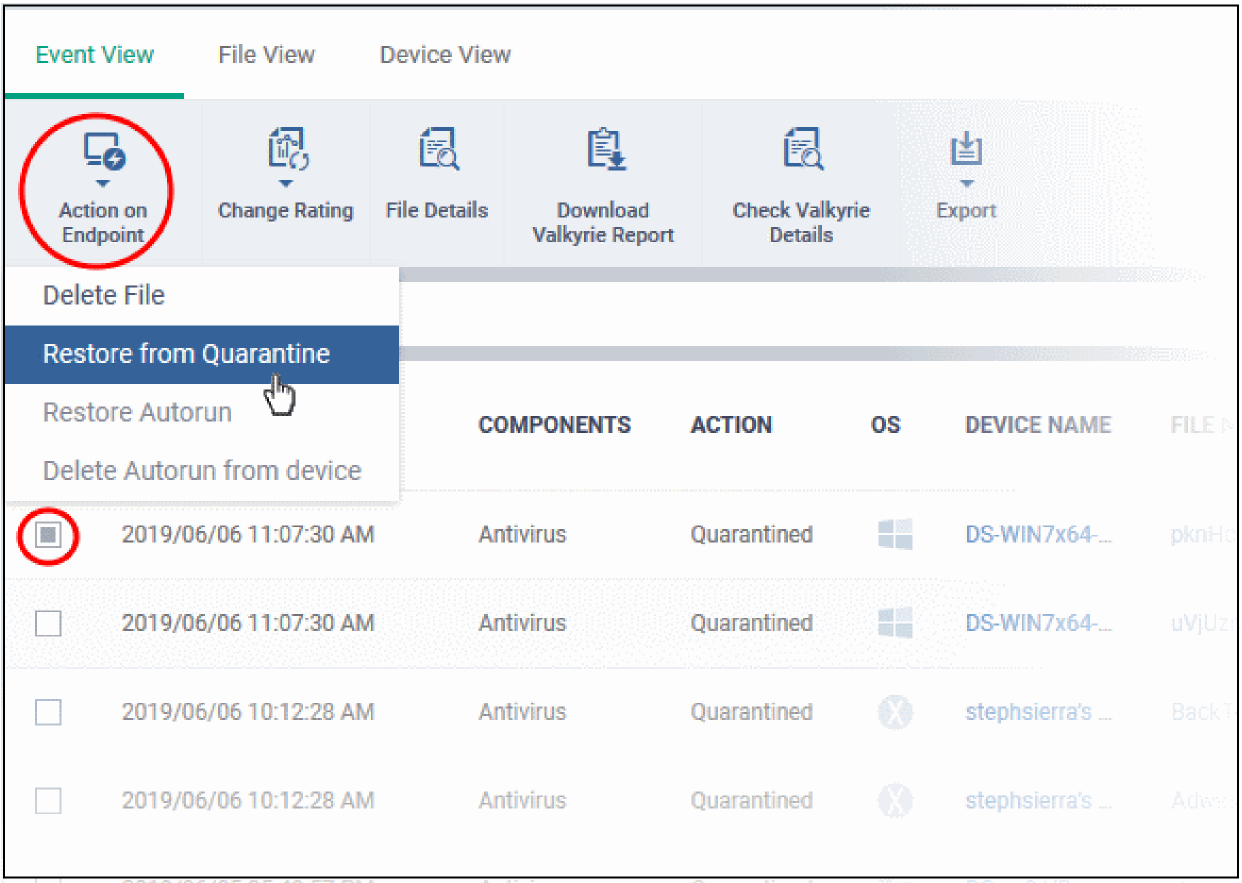
You can use any combination of filters simultaneously to search for specific apps.

## Handle Quarantined Items

You can delete or restore quarantined items from the 'Event View' tab of the security dashboard.

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
  - Select a company or group to view events in that group

    Or
  - Select 'Show all' to view all events
- Select the events where the files of interest were moved to quarantine.
- Click 'Action on Endpoint' button:



| | | COMPONENTS | ACTION | OS | DEVICE NAME | FILE |
|---|---|---|---|---|---|---|
| ■ | 2019/06/06 11:07:30 AM | Antivirus | Quarantined | | DS-WIN7x64-... | pknHa |
| □ | 2019/06/06 11:07:30 AM | Antivirus | Quarantined | | DS-WIN7x64-... | uVjUz |
| □ | 2019/06/06 10:12:28 AM | Antivirus | Quarantined | | stephsierra's ... | Back |
| □ | 2019/06/06 10:12:28 AM | Antivirus | Quarantined | | stephsierra's ... | Adw |

- Select 'Delete File / Delete Autorun from device' to remove the file from the device
- Select 'Restore from Quarantine' / 'Restore Autorun' to move the file(s) from quarantine to their original location on the device.

## Rate Files as Trusted, Malicious or Unrecognized

If required, you can manually rate files as unrecognized, trusted or malicious. The new rating will be sent to endpoints during the next sync.

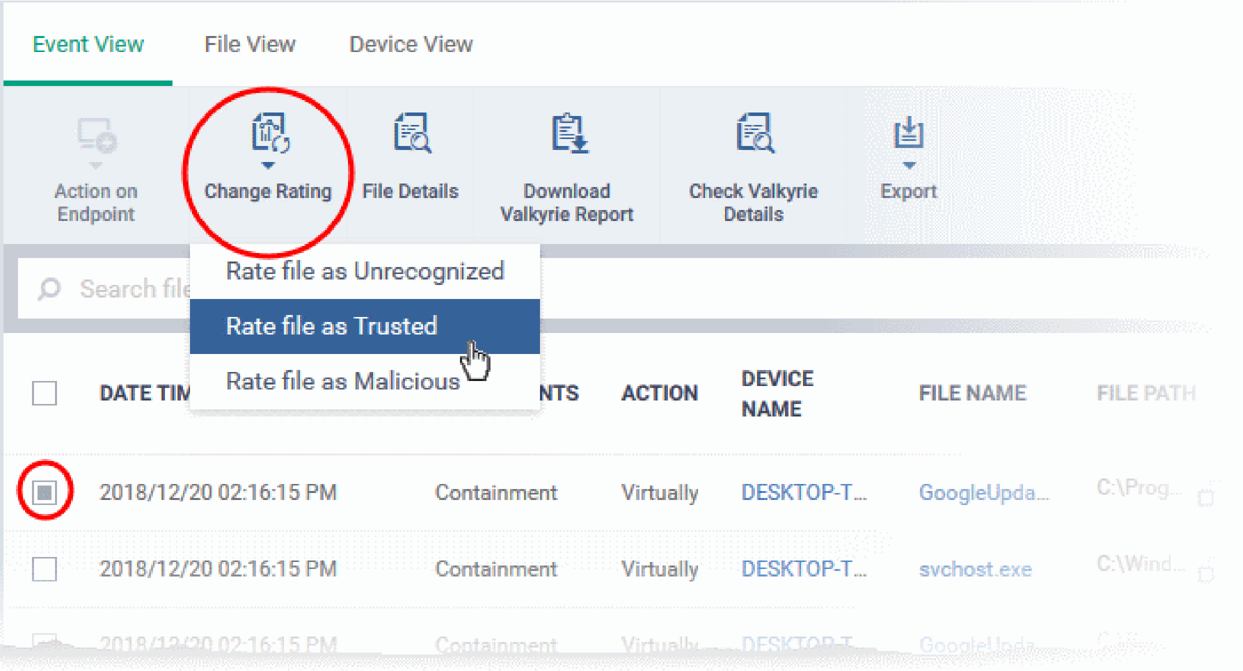
- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'

- Select a company or group to view events in that group

  Or

- Select 'Show all' to view all events

- Select the events involving the files of interest.
- Click the 'Change Rating' button
- Set your preferred rating from the options:



| ☐ | DATE TIM | NTS | ACTION | DEVICE NAME | FILE NAME | FILE PATH |
|---|---|---|---|---|---|---|
| ☒ | 2018/12/20 02:16:15 PM | Containment | Virtually | DESKTOP-T... | GoogleUpda... | C:\Prog... |
| ☐ | 2018/12/20 02:16:15 PM | Containment | Virtually | DESKTOP-T... | svchost.exe | C:\Wind... |
| ☐ | 2018/12/20 02:16:15 PM | Containment | Virtually | DESKTOP-T... | GoogleUpda... | C:\... |

The new rating will be propagated to all endpoints during the next synchronization.

## View the details of a file

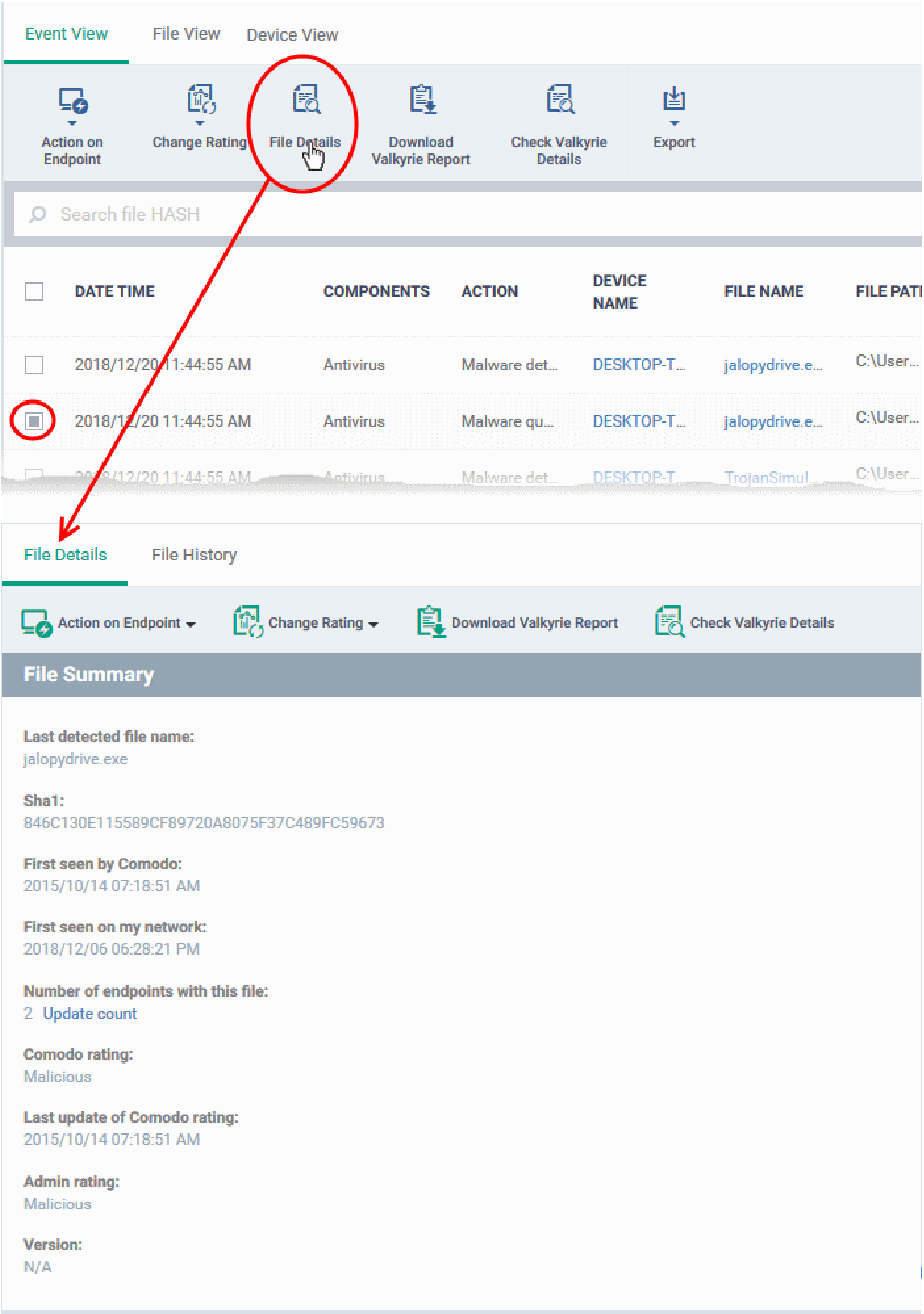
- You can view the complete details of the executable file that effected a security event on a managed endpoint from the 'Events View' interface.
- You can also view the history of actions taken on the file on all endpoints on which it was discovered.

**To view the details of a file that induced a security event**

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
  - Select a company or group to view events in that group

    Or

  - Select 'Show all' to view all events
- Select the event involving the file of interest.
- Click the 'File Details' button:
- Alternatively, click the label of the file in the 'File Name' column



| □ | DATE TIME | COMPONENTS | ACTION | DEVICE NAME | FILE NAME | FILE PATI |
|---|---|---|---|---|---|---|
| □ | 2018/12/20 11:44:55 AM | Antivirus | Malware det... | DESKTOP-T... | jalopydrive.e... | C:\User... |
| ☑ | 2018/12/20 11:44:55 AM | Antivirus | Malware qu... | DESKTOP-T... | jalopydrive.e... | C:\User... |
| □ | 2018/12/20 11:44:55 AM | Antivirus | Malware det... | DESKTOP-T... | TrojanSimul... | C:\User... |

File Summary

Last detected file name:
jalopydrive.exe

Sha1:
846C130E115589CF89720A8075F37C489FC59673

First seen by Comodo:
2015/10/14 07:18:51 AM

First seen on my network:
2018/12/06 06:28:21 PM

Number of endpoints with this file:
2 Update count

Comodo rating:
Malicious

Last update of Comodo rating:
2015/10/14 07:18:51 AM

Admin rating:
Malicious

Version:
N/A

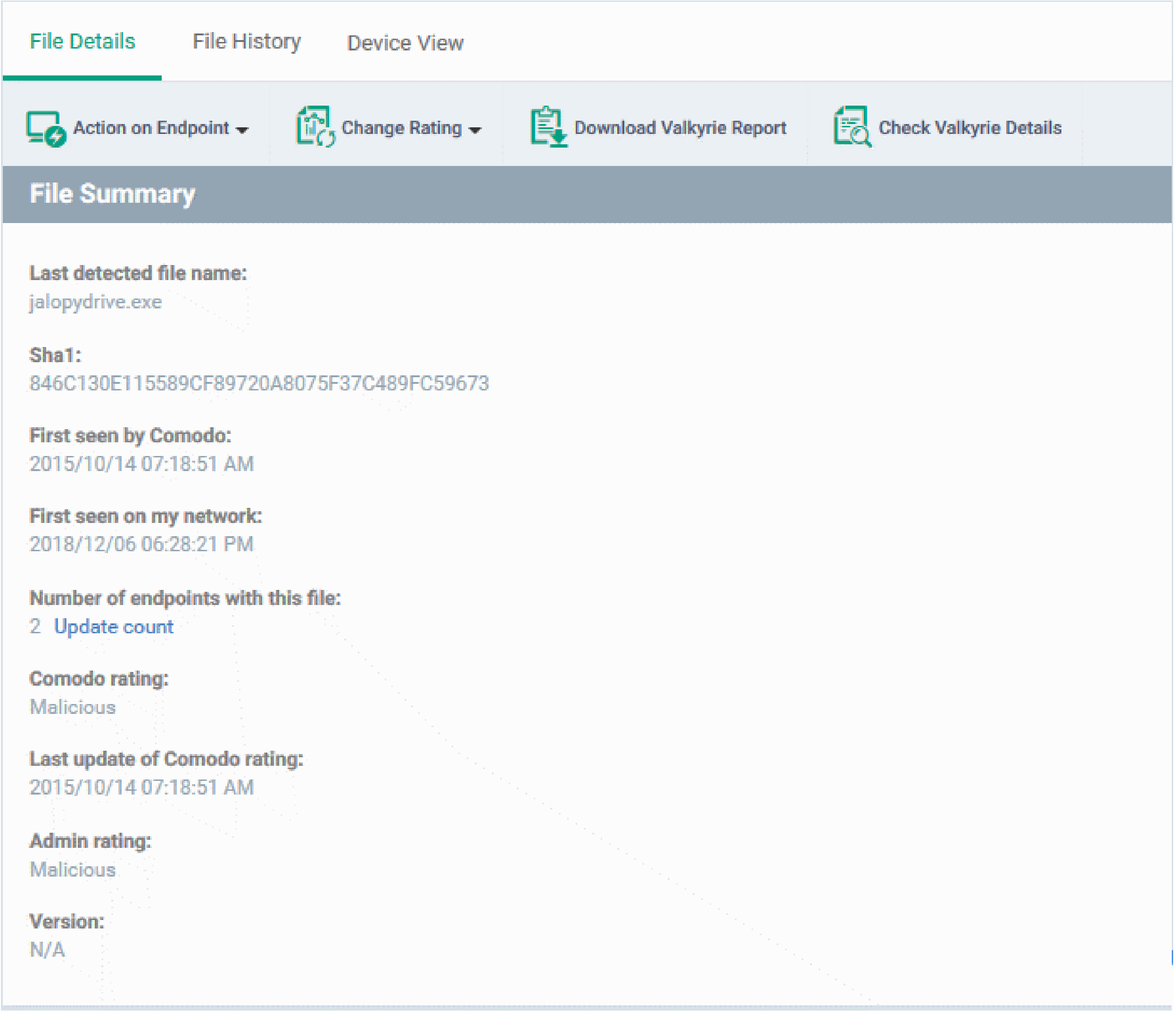
The information on the file are shown under two tabs:

- **File Details**

- File History

## File Details

- The 'File Details' tab shows the particulars of the file.
- The interface also allows you to:
  - Change the admin trust rating of the file
  - Delete the file from the endpoints or restore the file from quarantine, if the file has been moved to quarantine by antivirus on the endpoints.
  - Get a Valkyrie analysis report of the file as a PDF
  - View Valkyrie analysis details of the file



File Summary

Last detected file name:
jalopydrive.exe

Sha1:
846C130E115589CF89720A8075F37C489FC59673

First seen by Comodo:
2015/10/14 07:18:51 AM

First seen on my network:
2018/12/06 06:28:21 PM

Number of endpoints with this file:
2 Update count

Comodo rating:
Malicious

Last update of Comodo rating:
2015/10/14 07:18:51 AM

Admin rating:
Malicious

Version:
N/A

The 'File Summary' pane shows the following details:

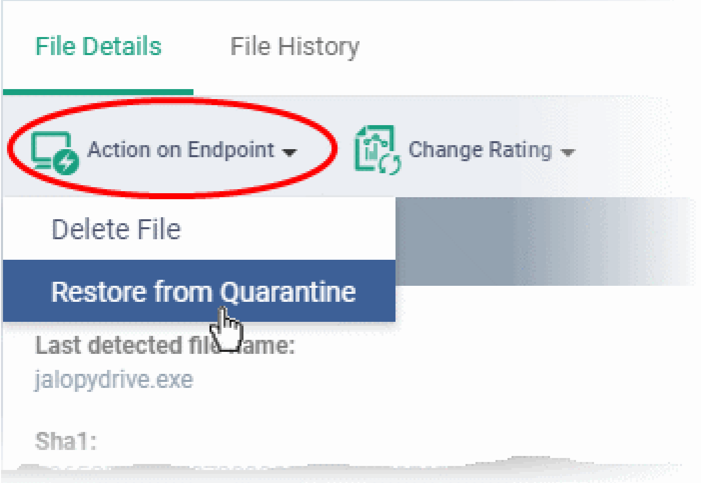
- **Last detected file name -** Label of the file when it was most recently scanned
- **SHA1** - SHA1 hash value of the file
- **First Seen by Comodo -** Date and time at which the file was first reported to Comodo threat labs
- **First Seen on my Network -** Date and time at which the file was first detected on one of your devices
- **Number of endpoints -** The count of Windows devices on which the file was found

    - Click 'Calculate' to update the number of devices on which the file is currently found

- **Comodo Rating -** The trust verdict on the file from Comodo threat labs
- **Last Update of Comodo Rating -** Date and time at which the Comodo rating last changed
- **Admin Rating -** The trust rating most recently assigned to the file by an administrator, if any.
- **Version -** The version number of the executable file

**To handle a quarantined file**

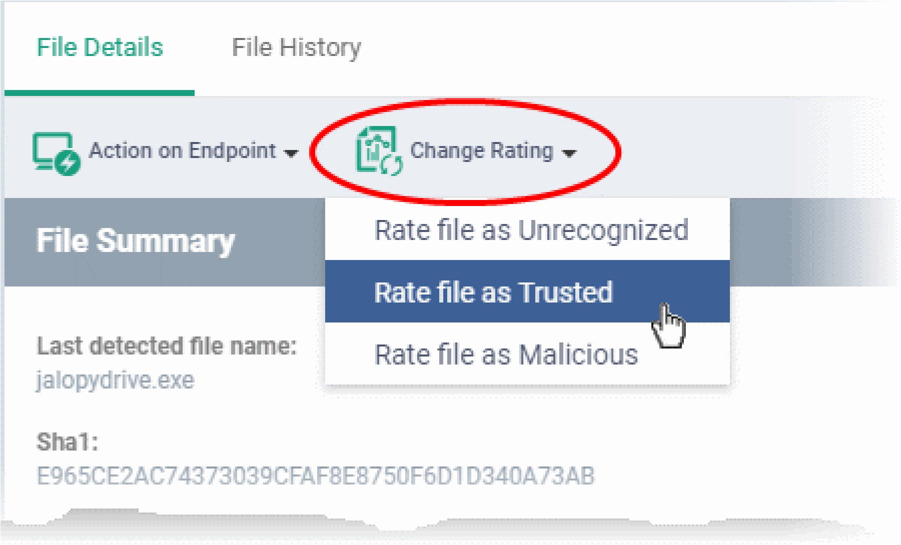
- Click 'Action on Endpoint' on the top



- Select 'Delete File' to remove the file the device, on which the selected event occurred.
- Select 'Restore from Quarantine' to move the file from quarantine to their original location on the device.

**To assign or change the admin rating of the file**

- Click 'Change Rating' on the top
- Set your preferred rating from the options:



The new rating will be propagated to all endpoints during the next synchronization.

**To download Valkyrie report of a file**

- Click the 'Download Valkyrie Report' button

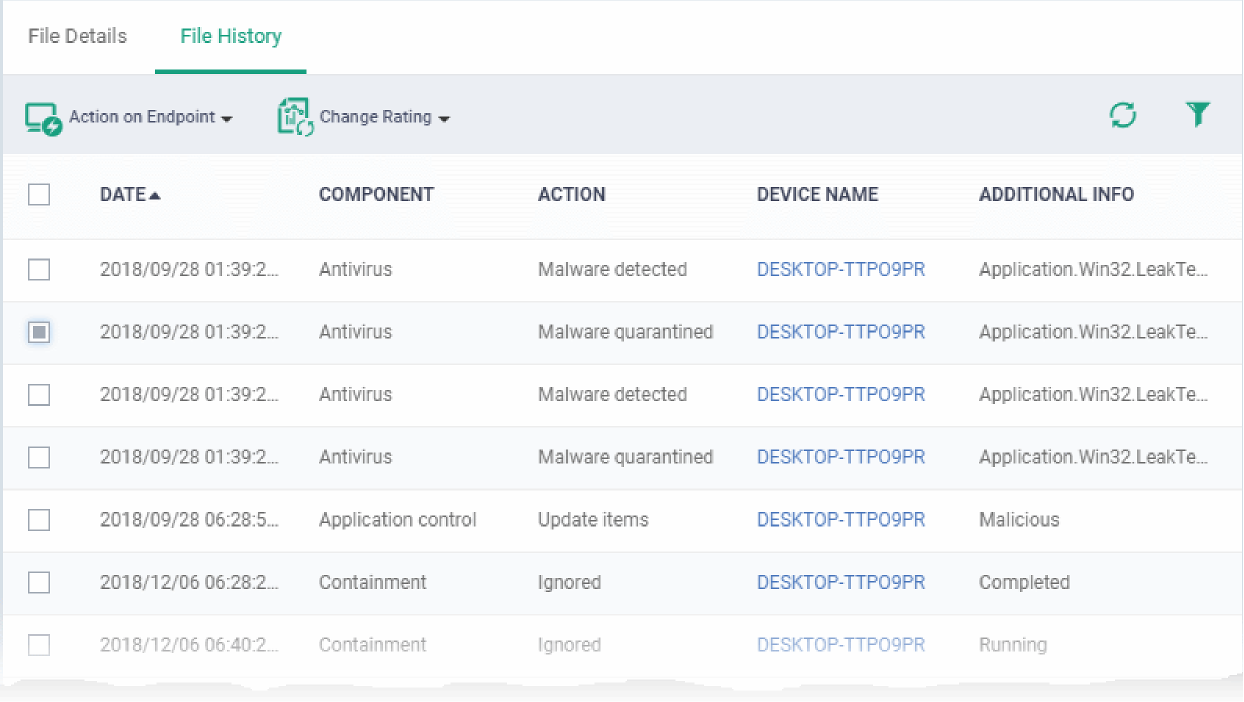
- See **Get Valkyrie Report of a file** for more details on the report

**To view the Valkyrie analysis results of the file**

- Click the 'Check Valkyrie Details' button
- See **View Valkyrie analysis details of file** for more details on the results

## File History

- This tab shows a timeline of events caused by the file. You can see the devices on which the file was found, the security module which detected the activity, and the action that was taken on the file
- The interface also allows you to:
  - Change the admin trust rating of the file
  - Delete the file from the endpoints or restore the file from quarantine, if the file has been moved to quarantine by antivirus on the endpoints.



| | DATE ▲ | COMPONENT | ACTION | DEVICE NAME | ADDITIONAL INFO |
|---|---|---|---|---|---|
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| ☒ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 06:28:5... | Application control | Update items | DESKTOP-TTPO9PR | Malicious |
| □ | 2018/12/06 06:28:2... | Containment | Ignored | DESKTOP-TTPO9PR | Completed |
| □ | 2018/12/06 06:40:2... | Containment | Ignored | DESKTOP-TTPO9PR | Running |

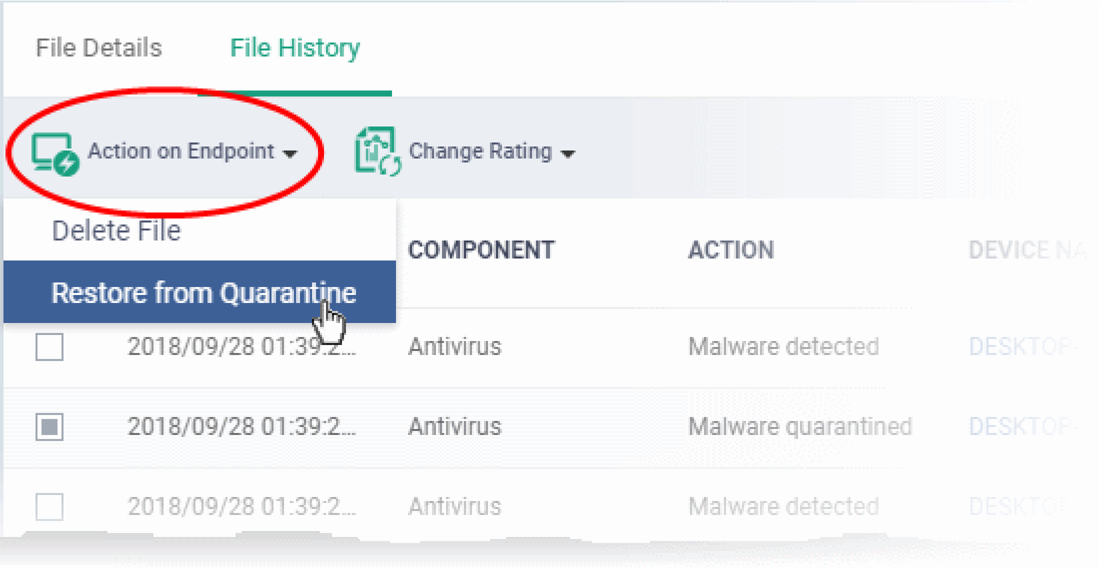
| Security Dashboards - Event View - File History - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date/Time | The time at which the event occurred. |
| Components | The module that reported the event. This can be 'Antivirus', 'Containment', 'Application Control' or 'Autorun Control'. |
| Action | The nature of the event showing the how the file was handled by the CCS component. The possible actions are:<br>Antivirus:<br>• Detection of malware<br>• Malware quarantined<br>• Malware removed from quarantine<br>• Malware restored from quarantine |

| Security Dashboards - Event View - File History - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| | • Malware removed from infected file<br>• Detected item ignored<br>• Detected file blocked<br>• File added to exclusions<br>• File added to trusted files list<br>• File reported as false positive from the results screen<br>Containment<br>• File run inside container with different restriction levels:<br>  • Restricted<br>  • Virtually<br>• File blocked<br>• File ignored<br>Application Control:<br>• File added to the file list<br>• File removed from the endpoint<br>• Trust rating updated for a file<br>Autorun Control:<br>• Detected item ignored<br>• Process / service stopped<br>• Auto-run process stopped. Corresponding auto-run entry removed. In the case of a service, CCS disables the service.<br>• Auto-start process quarantined. Corresponding auto-start entry removed. In the case of a service, CCS disables the service.<br>• Processes restored from quarantine<br>• File deleted from the endpoint |

| Security Dashboards - Event View - File History - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Device Name | The label of the Windows endpoint on which the event occurred.<br>• Click the name of a device to open its 'Device Details' interface.<br>• See **Manage Windows Devices** for more details on the interface. |
| Additional Info | Provides the current status of the event or the action taken on the affected file. |
| **Controls** | |
| Action on Endpoints | Allows you to delete a file or restore a file from quarantine on the endpoint. Applicable only for events involving 'Malware quarantined' action. |
| Change rating | Allows you to change the rating of the affected file to trusted, malicious or unrecognized. |

**Handle a quarantined file**

- Click 'Action on Endpoint' on the top

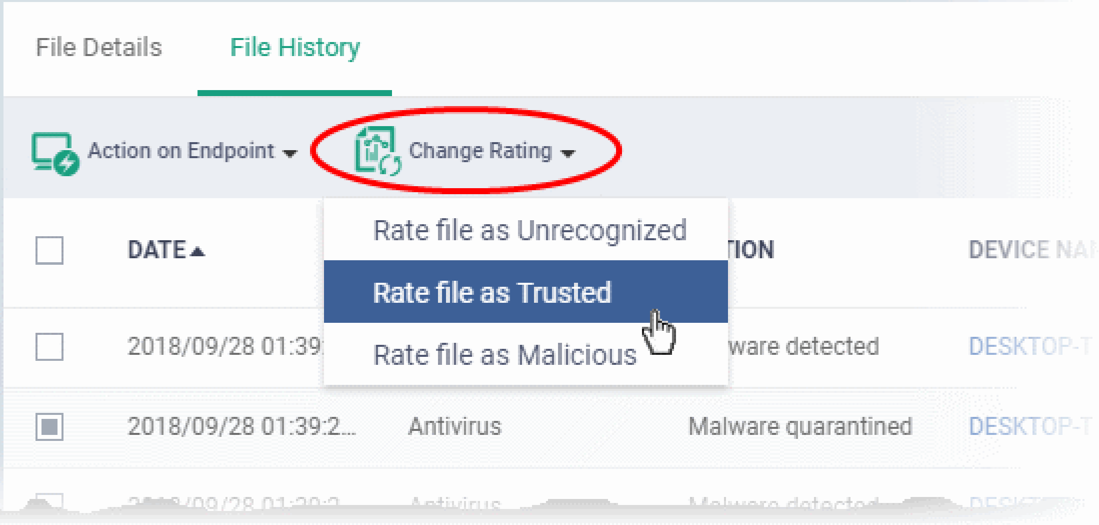


| | | COMPONENT | ACTION | DEVICE NA |
|---|---|---|---|---|
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP- |
| ☒ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP- |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP |

- Select 'Delete File' to remove the file the device, on which the selected event occurred.
- Select 'Restore from Quarantine' to move the file from quarantine to their original location on the device.

**Assign or change the admin rating of the file**

- Click 'Change Rating' on the top
- Set your preferred rating from the options:



The new rating will be propagated to all endpoints during the next synchronization.

## Get the Valkyrie Report on a file

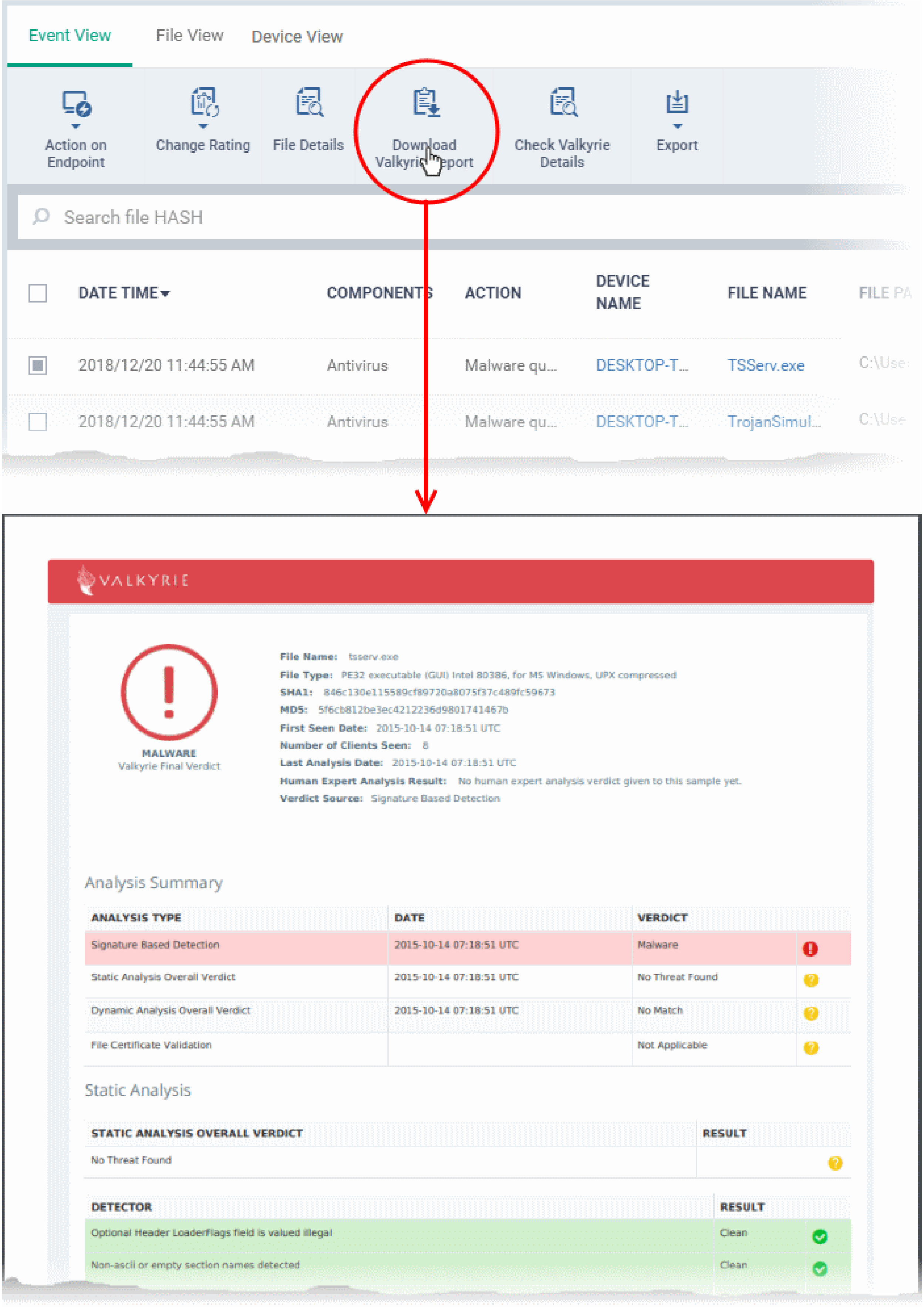
**Background**:

- Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks. The service helps Comodo establish whether an unknown file is malicious or safe
- You can configure Comodo Client Security on endpoints to automatically upload unknown files to Valkyrie
- You can schedule the upload of unknown files in the 'Valkyrie' section of a Windows profile. See **Valkyrie Settings** if you need help with this.

### Download a Valkyrie report

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
    - Select a company or group to view events in that group

      Or
    - Select 'Show all' to view all events
- Select the event involving the file of interest.
- Click the 'Download Valkyrie Report' button



| ☐ | DATE TIME ▾ | COMPONENTS | ACTION | DEVICE NAME | FILE NAME | FILE PA |
|---|---|---|---|---|---|---|
| ☒ | 2018/12/20 11:44:55 AM | Antivirus | Malware qu... | DESKTOP-T... | TSServ.exe | C:\Use |
| ☐ | 2018/12/20 11:44:55 AM | Antivirus | Malware qu... | DESKTOP-T... | TrojanSimul... | C:\Use |

**File Name:** tsserv.exe
**File Type:** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
**SHA1:** 846c130e115589cf89720a8075f37c489fc59673
**MD5:** 5f6cb812be3ec4212236d9801741467b
**First Seen Date:** 2015-10-14 07:18:51 UTC
**Number of Clients Seen:** 8
**Last Analysis Date:** 2015-10-14 07:18:51 UTC
**Human Expert Analysis Result:** No human expert analysis verdict given to this sample yet.
**Verdict Source:** Signature Based Detection

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---|---|---|---|
| Signature Based Detection | 2015-10-14 07:18:51 UTC | Malware | ! |
| Static Analysis Overall Verdict | 2015-10-14 07:18:51 UTC | No Threat Found | ? |
| Dynamic Analysis Overall Verdict | 2015-10-14 07:18:51 UTC | No Match | ? |
| File Certificate Validation | | Not Applicable | ? |

Static Analysis

| STATIC ANALYSIS OVERALL VERDICT | RESULT |
|---|---|
| No Threat Found | ? |

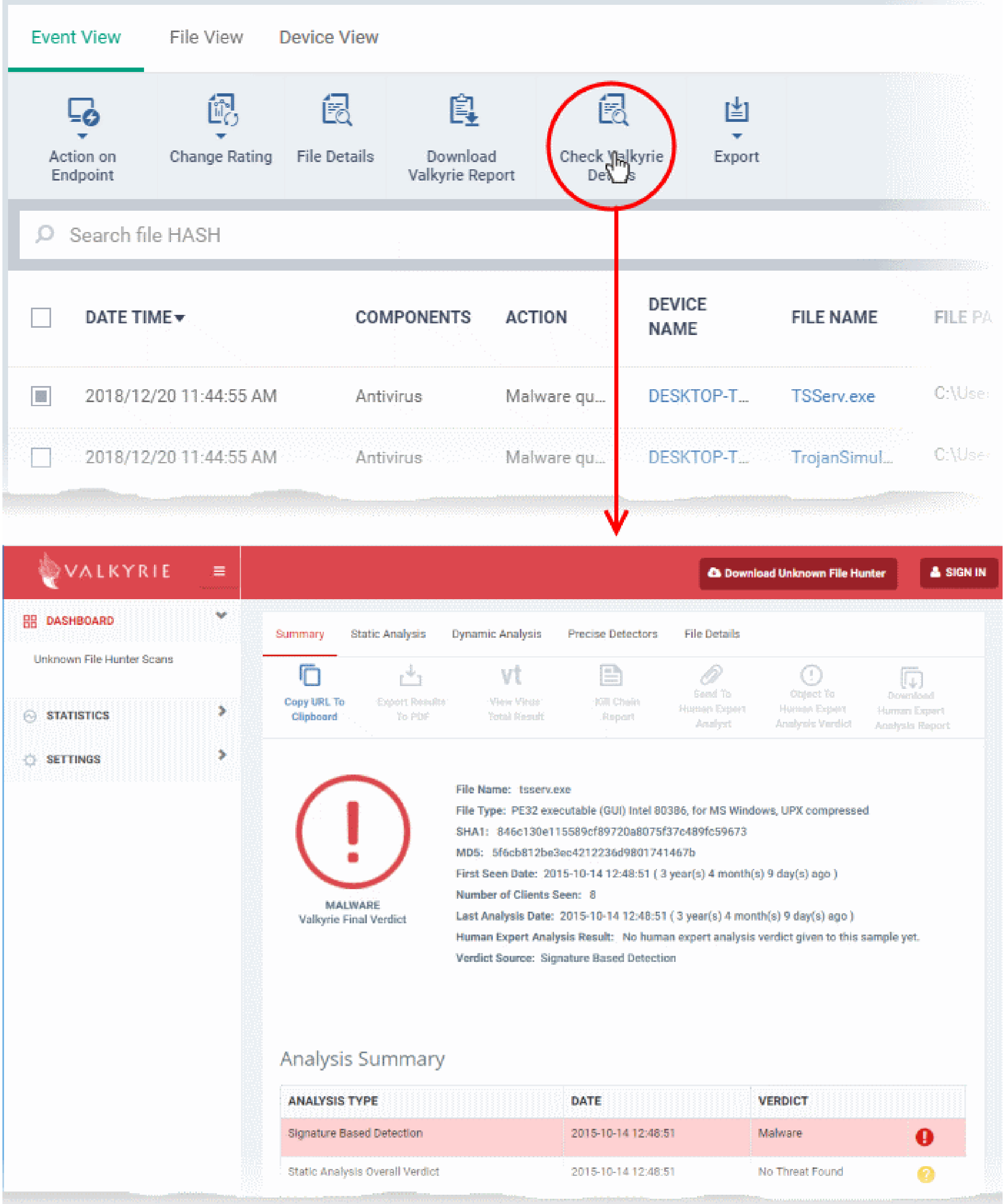
| DETECTOR | RESULT | |
|---|---|---|
| Optional Header LoaderFlags field is valued illegal | Clean | ✓ |
| Non-ascii or empty section names detected | Clean | ✓ |

- The PDF opens in a new browser tab.
- The report contains granular details of various tests on the file

## View Valkyrie analysis on a file

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
  - Select a company or group to view events in that group

    Or
  - Select 'Show all' to view all events
- Select the event involving the file of interest.
- Click the 'Check Valkyrie Details' button



| ☐ | DATE TIME ▾ | COMPONENTS | ACTION | DEVICE NAME | FILE NAME | FILE PA |
|---|---|---|---|---|---|---|
| ☒ | 2018/12/20 11:44:55 AM | Antivirus | Malware qu... | DESKTOP-T... | TSServ.exe | C:\Use |
| ☐ | 2018/12/20 11:44:55 AM | Antivirus | Malware qu... | DESKTOP-T... | TrojanSimul... | C:\Use |

File Name: tsserv.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 846c130e115589cf89720a8075f37c489fc59673
MD5: 5f6cb812be3ec4212236d9801741467b
First Seen Date: 2015-10-14 12:48:51 ( 3 year(s) 4 month(s) 9 day(s) ago )
Number of Clients Seen: 8
Last Analysis Date: 2015-10-14 12:48:51 ( 3 year(s) 4 month(s) 9 day(s) ago )
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---|---|---|---|
| Signature Based Detection | 2015-10-14 12:48:51 | Malware | ! |
| Static Analysis Overall Verdict | 2015-10-14 12:48:51 | No Threat Found | ? |

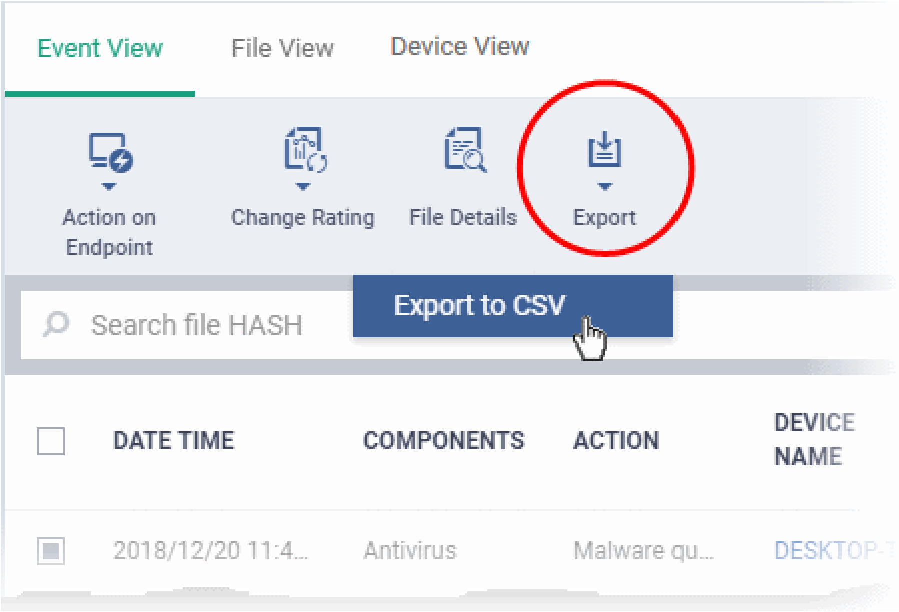
- The Valkyrie 'file verdict' page opens in a new tab.

- The page contains the results of various tests, and a trust verdict from each test.
- For more details on Valkyrie tests, see **http://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html**.

### Export the List of Events

You can save the list of events as a comma separated values (CSV) file for future analysis.

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Event View'
- Apply any filters that you require.
- Click 'Export' > 'Export to CSV'



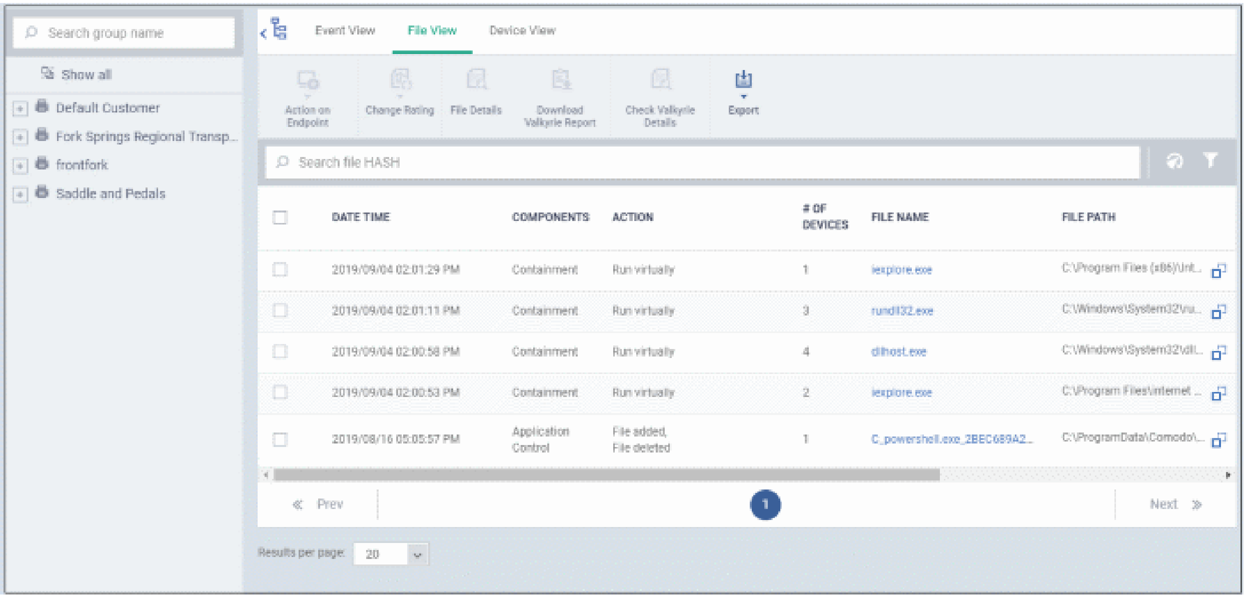
- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## 10.1.2. View Security Events by File

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'

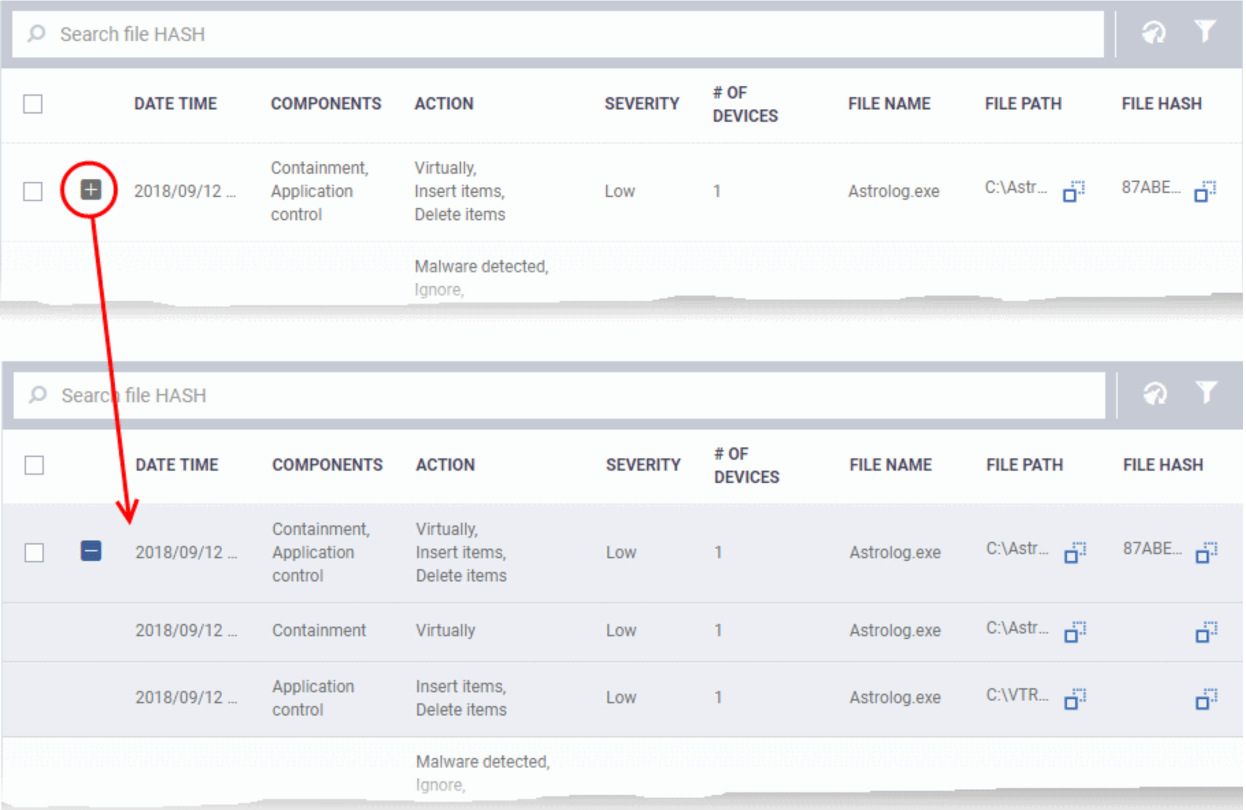
'File view' groups together all events that involve a particular file.

- A file can generate events in different security modules, on multiple devices, at different times.
- All these events are grouped together and shown as a single row:



| ☐ | DATE TIME | COMPONENTS | ACTION | # OF DEVICES | FILE NAME | FILE PATH |
|---|---|---|---|---|---|---|
| ☐ | 2019/09/04 02:01:29 PM | Containment | Run virtually | 1 | iexplore.exe | C:\Program Files (x86)\Int... |
| ☐ | 2019/09/04 02:01:11 PM | Containment | Run virtually | 3 | rundll32.exe | C:\Windows\System32\ru... |
| ☐ | 2019/09/04 02:00:58 PM | Containment | Run virtually | 4 | dllhost.exe | C:\Windows\System32\dll... |
| ☐ | 2019/09/04 02:00:53 PM | Containment | Run virtually | 2 | iexplore.exe | C:\Program Files\Internet ... |
| ☐ | 2019/08/16 05:05:57 PM | Application Control | File added,<br>File deleted | 1 | C_powershell.exe_2BEC689A2... | C:\ProgramData\Comodo\... |

- You can expand the row to view individual events:
- Click '+' at the left of the row to view all events related to the file:



| ☐ | | DATE TIME | COMPONENTS | ACTION | SEVERITY | # OF DEVICES | FILE NAME | FILE PATH | FILE HASH |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | + | 2018/09/12 ... | Containment, Application control | Virtually, Insert items, Delete items | Low | 1 | Astrolog.exe | C:\Astr... | 87ABE... |
| | | | | Malware detected, Ignore, | | | | | |

| ☐ | | DATE TIME | COMPONENTS | ACTION | SEVERITY | # OF DEVICES | FILE NAME | FILE PATH | FILE HASH |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | − | 2018/09/12 ... | Containment, Application control | Virtually, Insert items, Delete items | Low | 1 | Astrolog.exe | C:\Astr... | 87ABE... |
| | | 2018/09/12 ... | Containment | Virtually | Low | 1 | Astrolog.exe | C:\Astr... | |
| | | 2018/09/12 ... | Application control | Insert items, Delete items | Low | 1 | Astrolog.exe | C:\VTR... | |
| | | | | Malware detected, Ignore, | | | | | |

| Security Dashboards - File View - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date/Time | The time at which the event occurred. |
| Components | The security module that reported the event. This can be 'Antivirus', 'Containment', |

| | |
|---|---|
| | 'Application Control' or 'Autorun Control'. |
| Action | The response to the event. This shows how the file was handled by the CCS component mentioned above.<br>List of possible actions:<br>Antivirus:<br>• Detection of malware<br>• Malware quarantined<br>• Malware removed from quarantine<br>• Malware restored from quarantine<br>• The file was skipped by a virus scan<br>• Malware removed from infected file<br>• Detected item ignored<br>• Detected file blocked<br>• File added to exclusions<br>• File added to trusted files list<br>• File reported as false positive from the results screen<br>Containment:<br>• File run inside container with different restriction levels:<br>  • Restricted<br>  • Virtually<br>• File blocked<br>• File ignored<br>Application Control:<br>• File added - An unrecognized or malicious file was added to the 'File List' in CCS on the endpoint.<br>• File deleted - A file was removed from the 'File List' in CCS on the endpoint. This is because it rating was changed to 'Trusted', or because the file was deleted from the endpoint.<br>• File updated - A file's rating changed in the 'File List' in CCS on the endpoint. The rating may have changed from 'Unrecognized' to 'Malicious', or vice-versa.<br>Autorun Control:<br>• Detected item ignored<br>• Process / service stopped<br>• Auto-run process stopped. Corresponding auto-run entry removed. In the case of a service, CCS disables the service.<br>• Auto-start process quarantined. Corresponding auto-start entry removed. In the case of a service, CCS disables the service.<br>• Processes restored from quarantine<br>• File deleted from the endpoint |
| Number of devices | On how many devices the event was detected |
| File Name | The label of the executable file affected by the action |

| | |
|---|---|
| | • Click the name of a file to open its 'File Details' interface.<br>• See **View the details of a file** for more details. |
| File Path | The installation location of the executable file on the endpoint<br>• Click the ⧉ icon to copy the path to the clipboard. |
| File Hash | The SHA 1 hash value of the executable file<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Current Comodo Rating | The present trust rating of the file as per the Comodo File Look-up Service (FLS). |
| Current Admin Rating | The most recent trust rating of the file as manually set by the admin, if any.<br>• See **Rate Files as Trusted, Malicious or Unrecognized** for more details. |
| **Controls** | |
| Action on Endpoints | Delete or restore a file from quarantine on the endpoint. Applies only to 'Malware quarantined' events.<br>• See **Handle Quarantined Items** for more details |
| Change rating | Assign a new admin rating to a file (trusted, malicious or unrecognized).<br>• See **Rate Files as Trusted, Malicious or Unrecognized** for more details. |
| File Details | View complete information about the file that caused the event. You can also view a history of actions taken by the file.<br>• See **View the details of a file** for more details. |
| Download Valkyrie Report | Get a detailed Valkyrie analysis report for a file as a PDF.<br>• See **Get Valkyrie Report of a file** for more details |
| Check Valkyrie Details | View the Valkyrie analysis on a file.<br>• See **View Valkyrie analysis details of file** for more details |
| Export | Save the list of events as a comma separated values (csv) file.<br>• See **Export the List of Files** for more details. |

- Use the search fields to filter events by component, date, file name, and other criteria.
- Click the funnel icon at top-right to view more filter options:

The file view interface lets you:

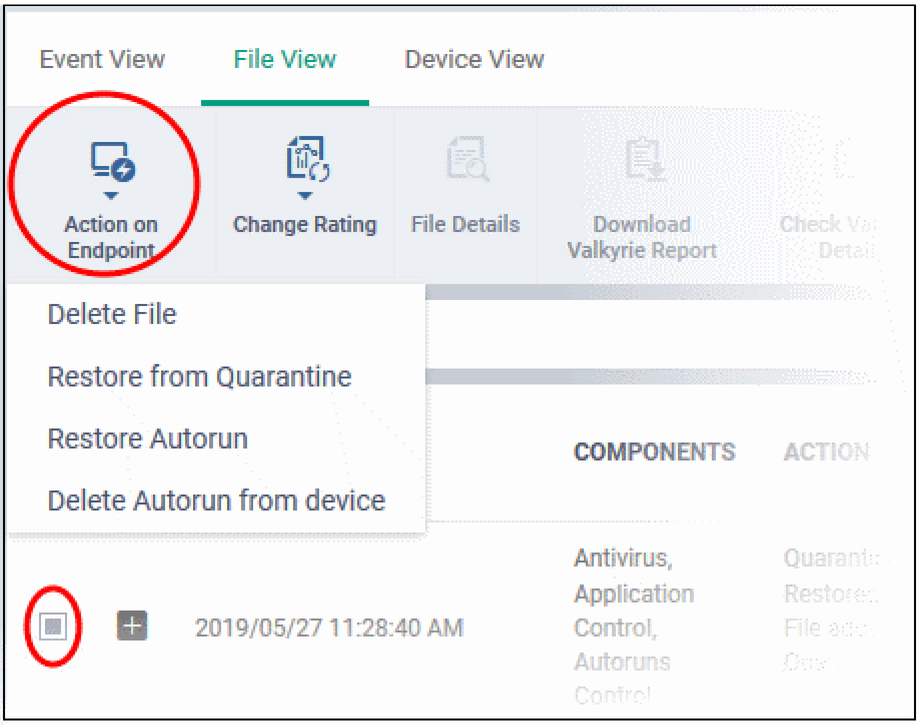
- **Handle Quarantined Items**
- **Rate Files as Trusted, Malicious or Unrecognized**
- **View the details of a file**
- **Get Valkyrie Report of a file**
- **View Valkyrie analysis details of file**
- **Export the List of Files**

## Handle Quarantined Items

- You can delete or restore quarantined items from the 'Security Dashboards' interface.

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
    - Select a company or group to view events in that group

      Or
    - Select 'Show all' to view all events
- Select the event(s) in which the file(s) of interest are moved to quarantine.
- Click 'Action on Endpoint' on top



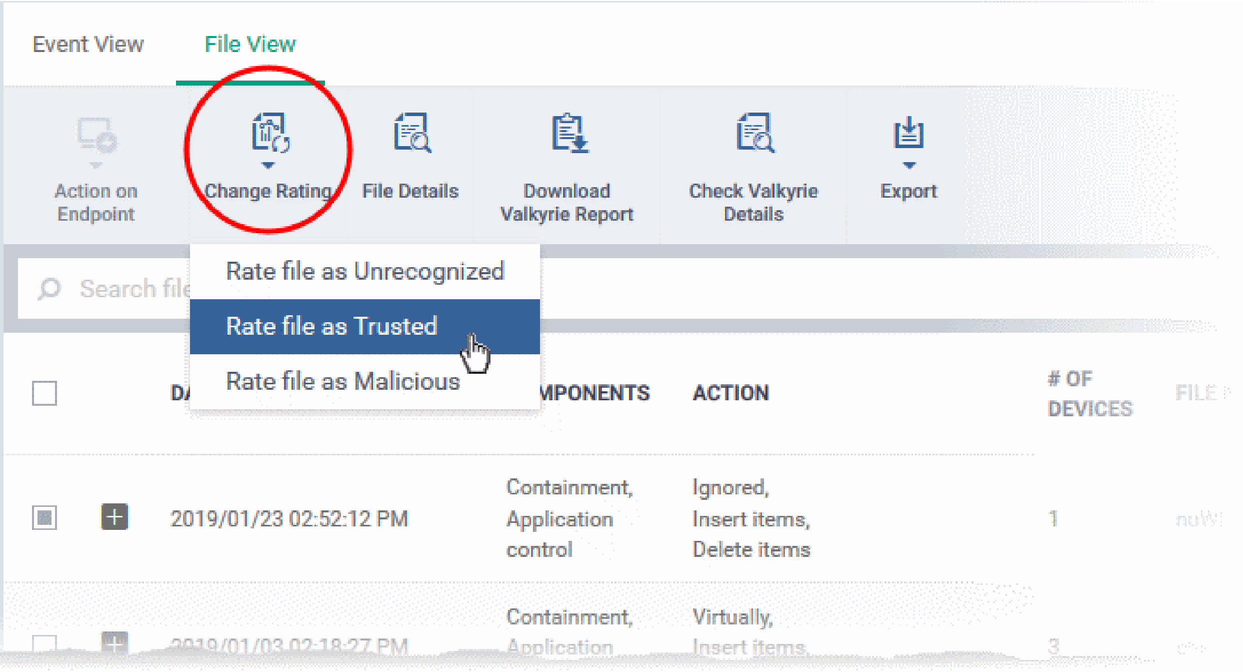
- Select 'Delete File' / 'Delete Autorun from device' to remove the file from the respective devices
- Select 'Restore from Quarantine' / 'Restore Autorun' to move the files back to their original location.

## Rate Files as Trusted, Malicious or Unrecognized

If required, you can rate the files affected by the events as unrecognized, trusted or malicious. Please make sure before marking a file as trusted. Any new file ratings will be sent to endpoints during the next sync.

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
    - Select a company or group to view events in that group

      Or
    - Select 'Show all' to view all events
- Select the event(s) involving the file(s) of interest.
- Click the 'Change Rating' button
- Set your preferred rating from the options:



| DA | MPONENTS | ACTION | # OF DEVICES |
|---|---|---|---|
| 2019/01/23 02:52:12 PM | Containment, Application control | Ignored, Insert items, Delete items | 1 |
| 2019/01/03 02:18:27 PM | Containment, Application | Virtually, Insert items | 3 |

The new rating will be propagated to all endpoints during the next synchronization.

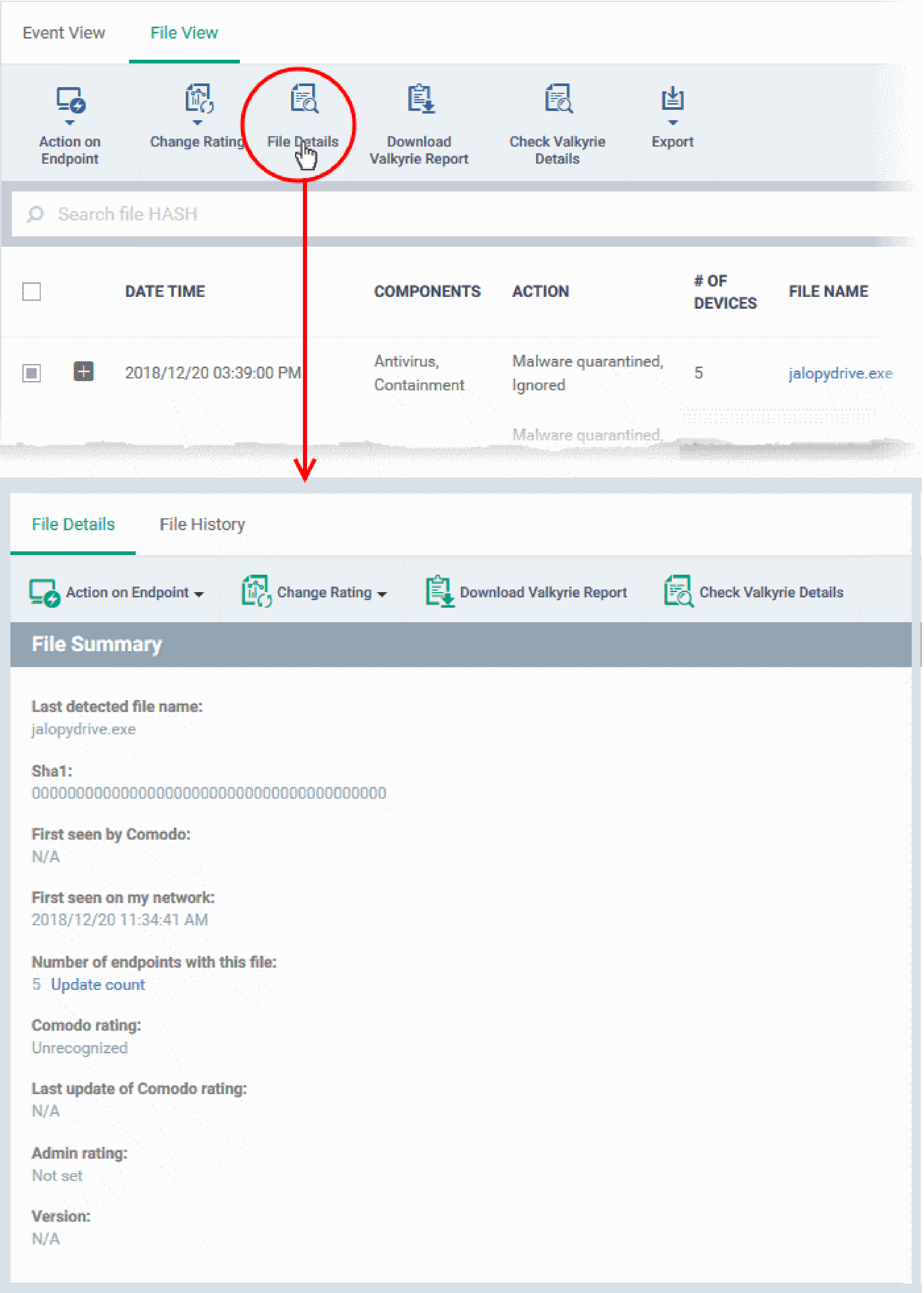
## View the details of a file

- You can view the complete details of the executable file that effected security events on managed endpoints from the 'File View' interface.
- You can also view the history of actions taken on the file on all endpoints on which it was discovered.

**View details about the file that caused an event**

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
  - Select a company or group to view events in that group

    Or
  - Select 'Show all' to view all events
- Select the event involving the file of interest.
- Click the 'File Details' button:
- Alternatively, click the label of the file in the 'File Name' column



| □ | | DATE TIME | COMPONENTS | ACTION | # OF DEVICES | FILE NAME |
|---|---|---|---|---|---|---|
| ▣ | ⊞ | 2018/12/20 03:39:00 PM | Antivirus, Containment | Malware quarantined, Ignored | 5 | jalopydrive.exe |
| | | | | Malware quarantined, | | |

**File Summary**

Last detected file name:
jalopydrive.exe

Sha1:
0000000000000000000000000000000000000000

First seen by Comodo:
N/A

First seen on my network:
2018/12/20 11:34:41 AM

Number of endpoints with this file:
5 Update count

Comodo rating:
Unrecognized

Last update of Comodo rating:
N/A

Admin rating:
Not set

Version:
N/A

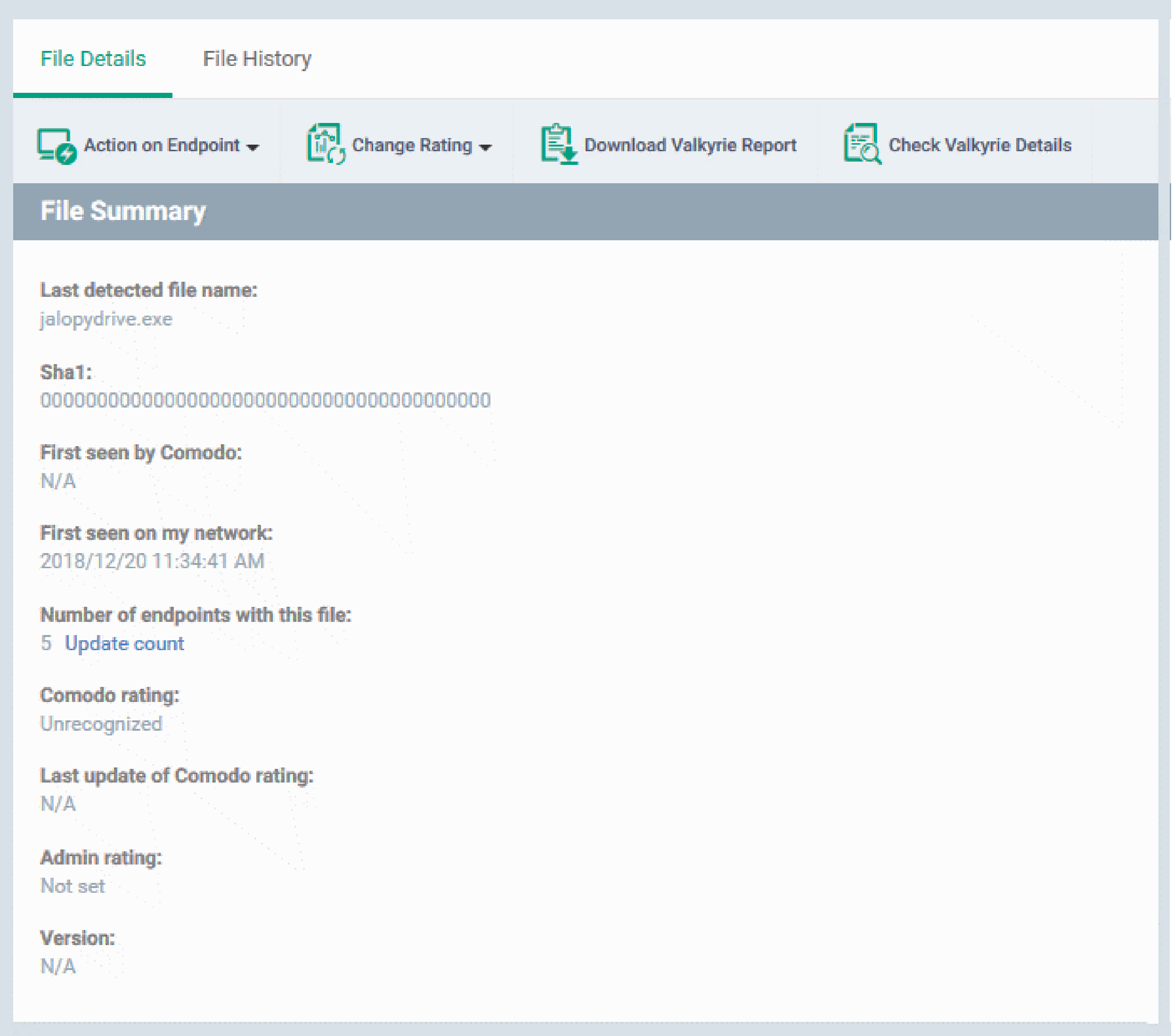
File information is shown in two tabs:

- **File Details**

- File History

## File Details

- The 'File Details' tab shows the particulars of the file.
- The interface also allows you to:
    - Change the admin trust rating of the file
    - Delete the file from the endpoints or restore the file from quarantine, if the file has been moved to quarantine by antivirus on the endpoints.
    - Get a Valkyrie analysis report of the file as a PDF
    - View Valkyrie analysis details of the file



Last detected file name:
jalopydrive.exe

Sha1:
0000000000000000000000000000000000000000

First seen by Comodo:
N/A

First seen on my network:
2018/12/20 11:34:41 AM

Number of endpoints with this file:
5 Update count

Comodo rating:
Unrecognized

Last update of Comodo rating:
N/A

Admin rating:
Not set

Version:
N/A

The 'File Summary' pane shows the following details:

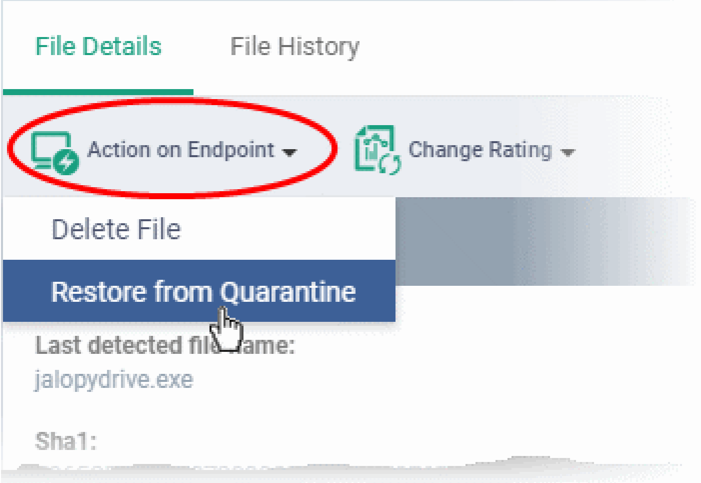
- **Last detected file name** - Label of the file when it was most recently scanned
- **SHA1** - SHA1 hash value of the file
- **First Seen by Comodo** - Date and time at which the file was first reported to Comodo threat labs
- **First Seen on my Network** - Date and time at which the file was first detected on one of your devices
- **Number of endpoints** - The count of Windows devices on which the file was found

- Click 'Calculate' to update the number of devices on which the file is currently found

- **Comodo Rating -** The trust verdict on the file from Comodo threat labs
- **Last Update of Comodo Rating -** Date and time at which the Comodo rating last changed
- **Admin Rating -** The trust rating most recently assigned to the file by an administrator, if any.
- **Version -** The version number of the executable file

**To handle a quarantined file**

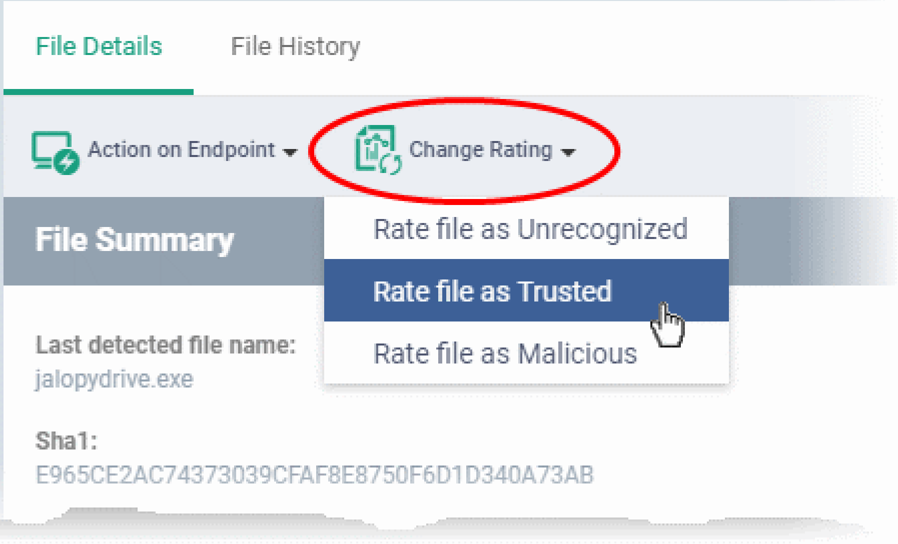
- Click 'Action on Endpoint' on the top



- Select 'Delete File' to remove the file the device, on which the selected events occurred.
- Select 'Restore from Quarantine' to move the file from quarantine to their original location on the device.

**To assign or change the admin rating of the file**

- Click 'Change Rating' on the top
- Set your preferred rating from the options:



The new rating will be propagated to all endpoints during the next synchronization.

**To download Valkyrie report of a file**

- Click the 'Download Valkyrie Report' button

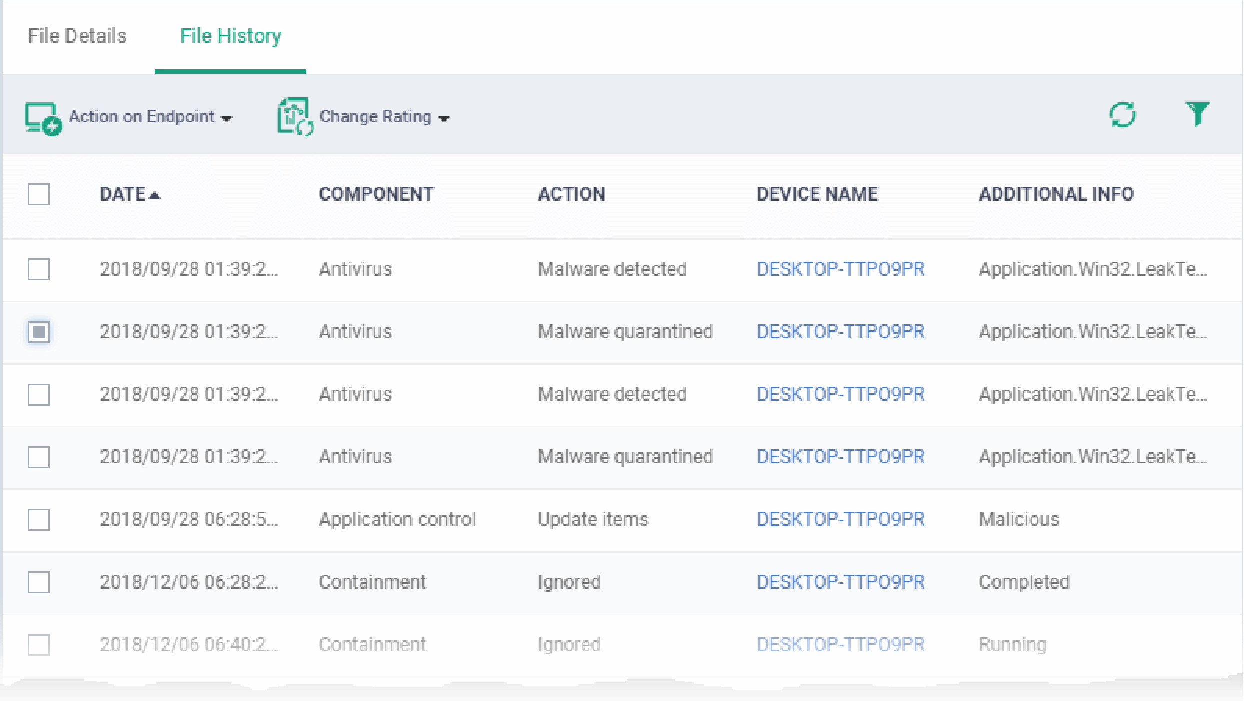
- See **Get Valkyrie Report of a file** for more details on the report

**To view the Valkyrie analysis results of the file**

- Click the 'Check Valkyrie Details' button
- See **View Valkyrie analysis details of file** for more details on the results

## File History

- The 'File History' tab shows the timeline of events induced by the file and actions taken on it at all devices in which it was found.
- The interface also allows you to:
  - Change the admin trust rating of the file
  - Delete the file from the endpoints or restore the file from quarantine, if the file has been moved to quarantine by antivirus on the endpoints.



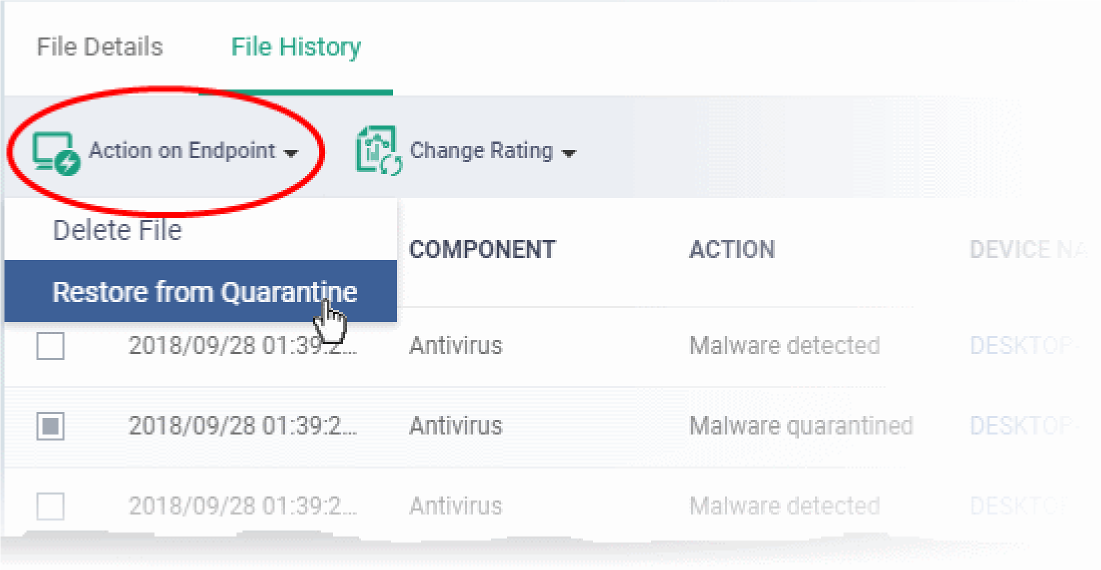
| □ | DATE ▲ | COMPONENT | ACTION | DEVICE NAME | ADDITIONAL INFO |
|---|---|---|---|---|---|
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| ☒ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP-TTPO9PR | Application.Win32.LeakTe... |
| □ | 2018/09/28 06:28:5... | Application control | Update items | DESKTOP-TTPO9PR | Malicious |
| □ | 2018/12/06 06:28:2... | Containment | Ignored | DESKTOP-TTPO9PR | Completed |
| □ | 2018/12/06 06:40:2... | Containment | Ignored | DESKTOP-TTPO9PR | Running |

| Security Dashboards - Event View - File History - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date/Time | The time at which the event occurred. |
| Components | Whether the 'Antivirus', 'Containment' or 'Application Control' that reported the event |
| Action | The nature of the event showing the how the file was handled by the CCS component. The possible actions are:<br>Antivirus:<br>• Detection of malware<br>• Malware quarantined<br>• Malware removed from quarantine<br>• Malware restored from quarantine |

| Security Dashboards - Event View - File History - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| | • Malware removed from infected file<br>• Detected item ignored<br>• Detected file blocked<br>• File added to exclusions<br>• File added to trusted files list<br>• File reported as false positive from the results screen<br>Containment<br>• File run inside container with different restriction levels:<br>    • Restricted<br>    • Virtually<br>• File blocked<br>• File ignored<br>Application Control:<br>• File added - An unrecognized or malicious file was added to the 'File List' in CCS on the endpoint.<br>• File deleted - A file was removed from the 'File List' in CCS on the endpoint. This is because it rating was changed to 'Trusted', or because the file was deleted from the endpoint.<br>• File updated - A file's rating changed in the 'File List' in CCS on the endpoint. The rating may have changed from 'Unrecognized' to 'Malicious', or vice-versa.<br>Autorun Control:<br>• Detected item ignored<br>• Process / service stopped<br>• Auto-run process stopped. Corresponding auto-run entry removed. In the case of a service, CCS disables the service.<br>• Auto-start process quarantined. Corresponding auto-start entry removed. In the case of a service, CCS disables the service.<br>• Processes restored from quarantine<br>• File deleted from the endpoint |
| Device Name | The label of the Windows endpoint on which the event occurred.<br>• Click the name of a device to open its 'Device Details' interface.<br>• See **Manage Windows Devices** for more details on the interface. |
| Additional Info | Provides the current status of the event or the action taken on the affected file. |
| **Controls** | |
| Action on Endpoints | Allows you to delete a file or restore a file from quarantine on the endpoint. Applicable only for events involving 'Malware quarantined' action. |
| Change rating | Allows you to change the rating of the affected file to trusted, malicious or unrecognized. |

**To handle a quarantined file**

- Click 'Action on Endpoint' on the top

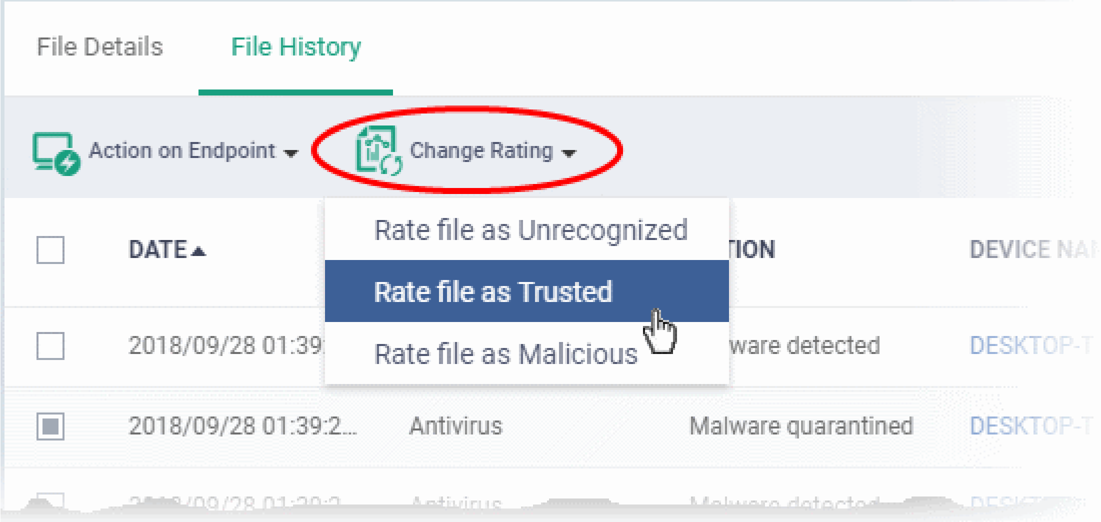


| □ | | COMPONENT | ACTION | DEVICE NA |
|---|---|---|---|---|
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTOP- |
| ■ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP- |
| □ | 2018/09/28 01:39:2... | Antivirus | Malware detected | DESKTO |

- Select 'Delete File' to remove the file the device, on which the selected event occurred.
- Select 'Restore from Quarantine' to move the file from quarantine to their original location on the device.

**To assign or change the admin rating of the file**

- Click 'Change Rating' on the top
- Set your preferred rating from the options:



| □ | DATE ▲ | | TION | DEVICE NA |
|---|---|---|---|---|
| □ | 2018/09/28 01:39 | | ware detected | DESKTOP-T |
| ■ | 2018/09/28 01:39:2... | Antivirus | Malware quarantined | DESKTOP-T |
| □ | 2018/09/28 01:39:2 | Antivirus | Malware detected | DESKT |

The new rating will be propagated to all endpoints during the next synchronization.

### Get the Valkyrie Report on a file

**Background**:

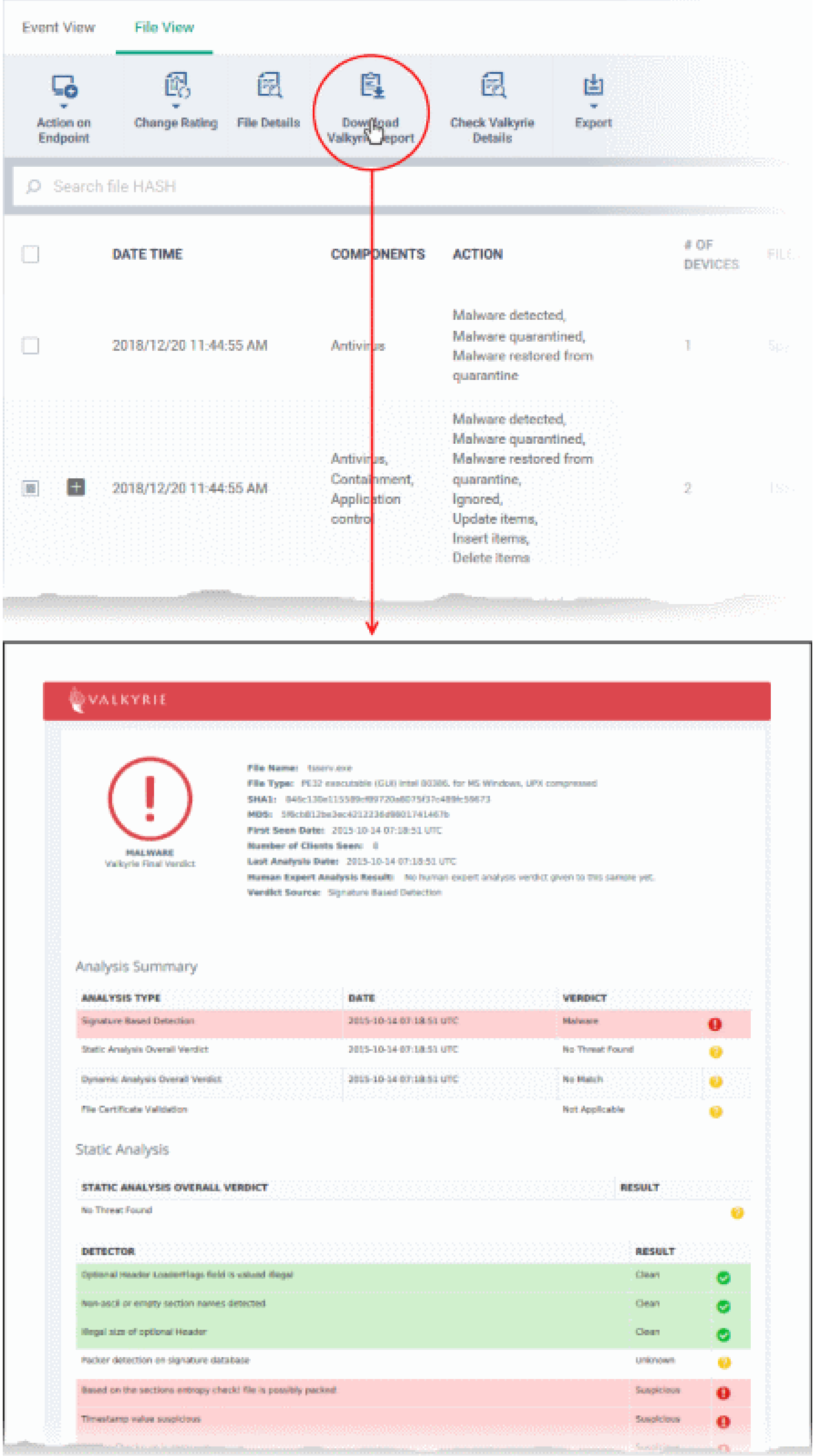
- Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks. The service helps Comodo establish whether an unknown file is malicious or safe

- You can configure Comodo Client Security on endpoints to automatically upload unknown files to Valkyrie
- You can schedule the upload of unknown files in the 'Valkyrie' section of a Windows profile. See **Valkyrie Settings** if you need help with this.

**Download the Valkyrie report on a file**

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
  - Select a company or group to view events in that group

    Or
  - Select 'Show all' to view all events
- Select the event involving the file of interest.
- Click the 'Download Valkyrie' button



| | | DATE TIME | COMPONENTS | ACTION | # OF DEVICES | FILE |
|---|---|---|---|---|---|---|
| □ | | 2018/12/20 11:44:55 AM | Antivirus | Malware detected,<br>Malware quarantined,<br>Malware restored from quarantine | 1 | Sp |
| ▣ | ⊞ | 2018/12/20 11:44:55 AM | Antivirus,<br>Containment,<br>Application control | Malware detected,<br>Malware quarantined,<br>Malware restored from quarantine,<br>Ignored,<br>Update items,<br>Insert items,<br>Delete items | 2 | Ts |

MALWARE
Valkyrie Final Verdict

**File Name:** tsserv.exe
**File Type:** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
**SHA1:** 040c130e115589c4f9720a8075f37c489fc59673
**MD5:** 5f6cb812be3ec4212236d9801741467b
**First Seen Date:** 2015-10-14 07:18:51 UTC
**Number of Clients Seen:** 0
**Last Analysis Date:** 2015-10-14 07:18:51 UTC
**Human Expert Analysis Result:** No human expert analysis verdict given to this sample yet.
**Verdict Source:** Signature Based Detection

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---|---|---|---|
| Signature Based Detection | 2015-10-14 07:18:51 UTC | Malware | ! |
| Static Analysis Overall Verdict | 2015-10-14 07:18:51 UTC | No Threat Found | ? |
| Dynamic Analysis Overall Verdict | 2015-10-14 07:18:51 UTC | No Match | ? |
| File Certificate Validation | | Not Applicable | ? |

Static Analysis

| STATIC ANALYSIS OVERALL VERDICT | RESULT |
|---|---|
| No Threat Found | ? |

| DETECTOR | RESULT | |
|---|---|---|
| Optional Header LoaderFlags field is valued illegal | Clean | ✓ |
| Non-ascii or empty section names detected | Clean | ✓ |
| Illegal size of optional Header | Clean | ✓ |
| Packer detection on signature database | Unknown | ? |
| Based on the sections entropy check! file is possibly packed | Suspicious | ! |
| Timestamp value suspicious | Suspicious | ! |

- The PDF opens in a new browser tab.
- The report contains granular details of various tests on the file

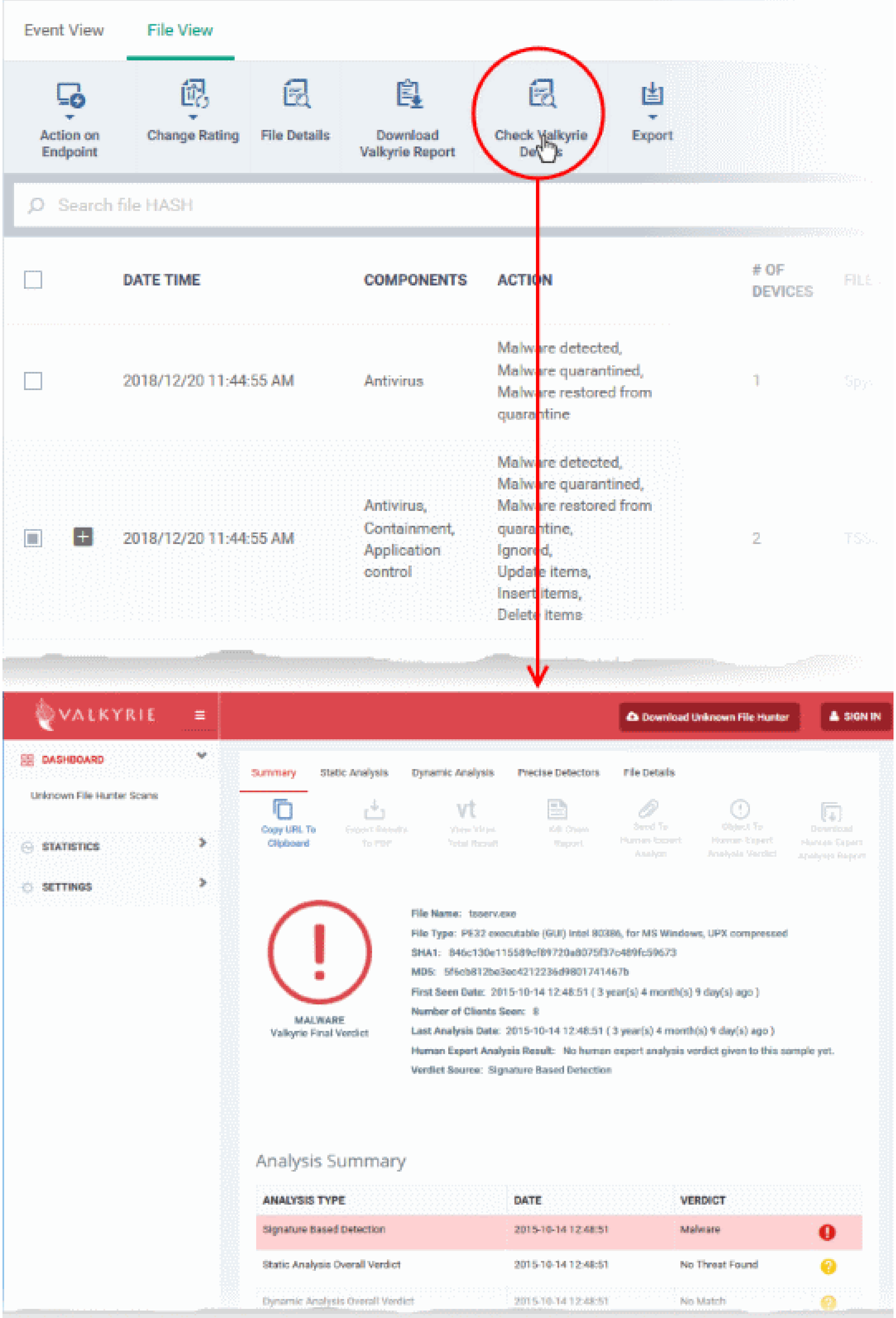
## View Valkyrie analysis of a file

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
    - Select a company or group to view events in that group

Or

- Select 'Show all' to view all events

- Select the event involving the file of interest.
- Click the 'Check Valkyrie Details' button



| ☐ | | DATE TIME | COMPONENTS | ACTION | # OF DEVICES | FILE |
|---|---|---|---|---|---|---|
| ☐ | | 2018/12/20 11:44:55 AM | Antivirus | Malware detected, Malware quarantined, Malware restored from quarantine | 1 | Spy |
| ☐ | + | 2018/12/20 11:44:55 AM | Antivirus, Containment, Application control | Malware detected, Malware quarantined, Malware restored from quarantine, Ignored, Update items, Insert items, Delete items | 2 | TSS |

File Name: tsserv.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 846c130e115589cf89720a8075f37c489fc59673
MD5: 5f6cb812be3ec4212236d9801741467b
First Seen Date: 2015-10-14 12:48:51 ( 3 year(s) 4 month(s) 9 day(s) ago )
Number of Clients Seen: 8
Last Analysis Date: 2015-10-14 12:48:51 ( 3 year(s) 4 month(s) 9 day(s) ago )
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---|---|---|---|
| Signature Based Detection | 2015-10-14 12:48:51 | Malware | ! |
| Static Analysis Overall Verdict | 2015-10-14 12:48:51 | No Threat Found | ? |
| Dynamic Analysis Overall Verdict | 2015-10-14 12:48:51 | No Match | ? |

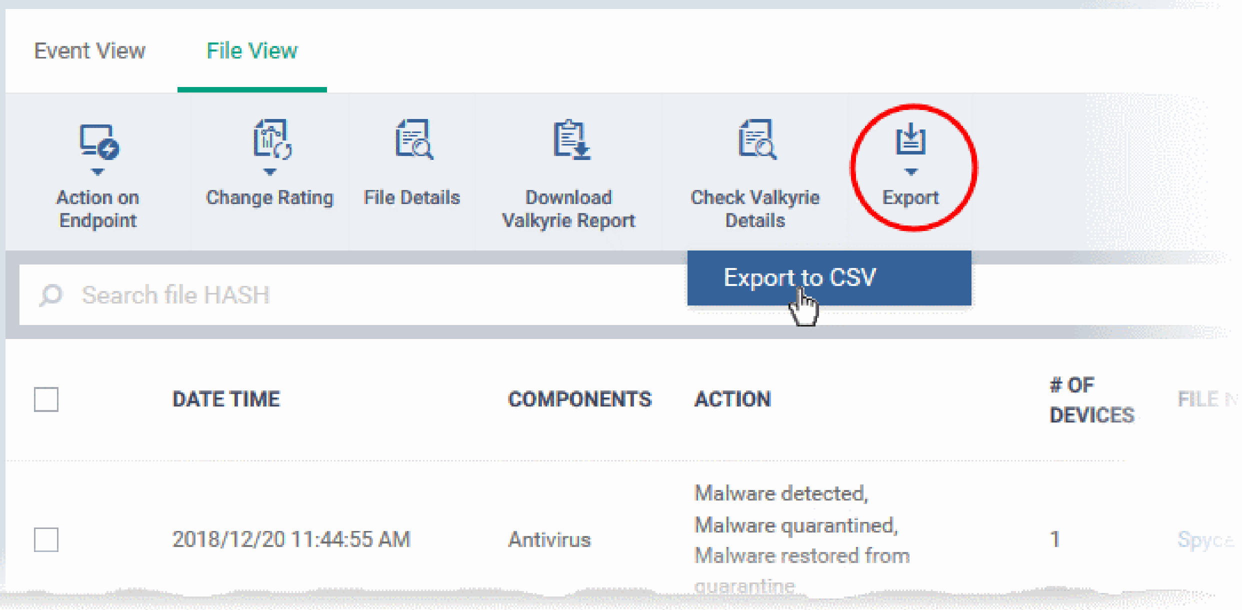
- The Valkyrie 'file verdict' page opens in a new tab.
- The page contains the results of various tests, and a trust verdict from each test.

- For more details on Valkyrie tests, see **http://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html**.

### Export the List of Files

You can save the list of events as a comma separated values (CSV) file for future analysis.

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'File View'
- Apply any filters that you require.
- Click 'Export' > 'Export to CSV'



| □ | DATE TIME | COMPONENTS | ACTION | # OF DEVICES | FILE N |
|---|---|---|---|---|---|
| □ | 2018/12/20 11:44:55 AM | Antivirus | Malware detected, Malware quarantined, Malware restored from quarantine | 1 | Spyca |

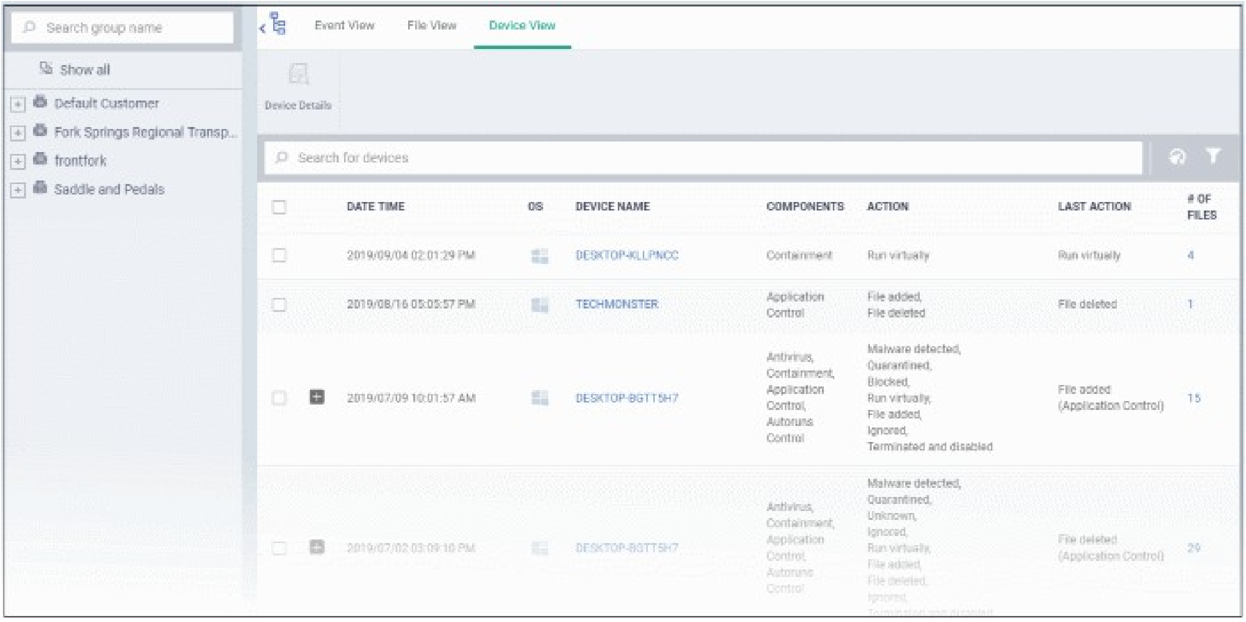
- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## 10.1.3. View Security Events by Device

- Click 'Security Sub-Systems' > 'Security Dashboards' > 'Device View'

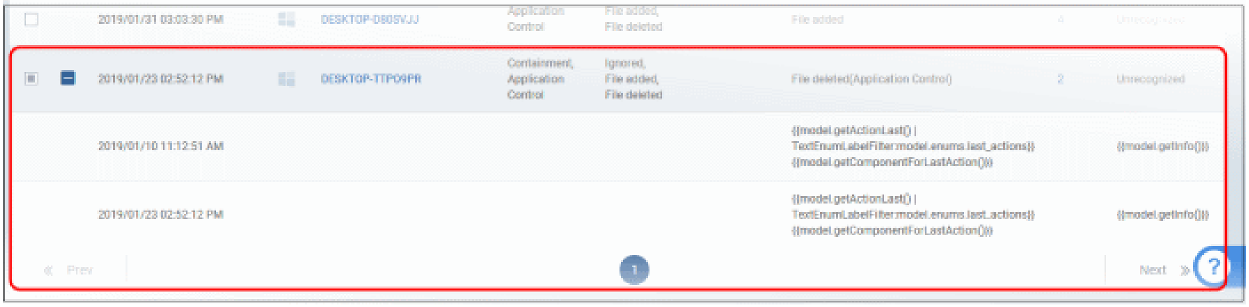
Device view shows all events that occurred on a particular device.

- Multiple security modules can create events on a device at different times. All these events are grouped together and shown as a single row:



| | DATE TIME | OS | DEVICE NAME | COMPONENTS | ACTION | LAST ACTION | # OF FILES |
|---|---|---|---|---|---|---|---|
| □ | 2019/09/04 02:01:29 PM | | DESKTOP-KLLPNCC | Containment | Run virtually | Run virtually | 4 |
| □ | 2019/08/16 05:05:57 PM | | TECHMONSTER | Application Control | File added,<br>File deleted | File deleted | 1 |
| □ + | 2019/07/09 10:01:57 AM | | DESKTOP-BGTT5H7 | Antivirus,<br>Containment,<br>Application Control,<br>Autoruns Control | Malware detected,<br>Quarantined,<br>Blocked,<br>Run virtually,<br>File added,<br>Ignored,<br>Terminated and disabled | File added (Application Control) | 15 |
| □ + | 2019/07/02 03:09:10 PM | | DESKTOP-BGTT5H7 | Antivirus,<br>Containment,<br>Application Control,<br>Autoruns Control | Malware detected,<br>Quarantined,<br>Unknown,<br>Ignored,<br>Run virtually,<br>File added,<br>File deleted,<br>Ignored,<br>Terminated and disabled | File deleted (Application Control) | 29 |

- Click '+' to view all events on the device



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| □ | 2019/01/31 03:03:30 PM | | DESKTOP-D80SVJJ | Application Control | File added,<br>File deleted | File added | 4 | Unrecognized |
| ▣ − | 2019/01/23 02:52:12 PM | | DESKTOP-TTPO9PR | Containment,<br>Application Control | Ignored,<br>File added,<br>File deleted | File deleted(Application Control) | 2 | Unrecognized |
| | 2019/01/10 11:12:51 AM | | | | | {{model.getActionLast() \| TextEnumLabelFilter:model.enums.last_actions}}<br>{{model.getComponentForLastAction()}} | | {{model.getInfo()}} |
| | 2019/01/23 02:52:12 PM | | | | | {{model.getActionLast() \| TextEnumLabelFilter:model.enums.last_actions}}<br>{{model.getComponentForLastAction()}} | | {{model.getInfo()}} |

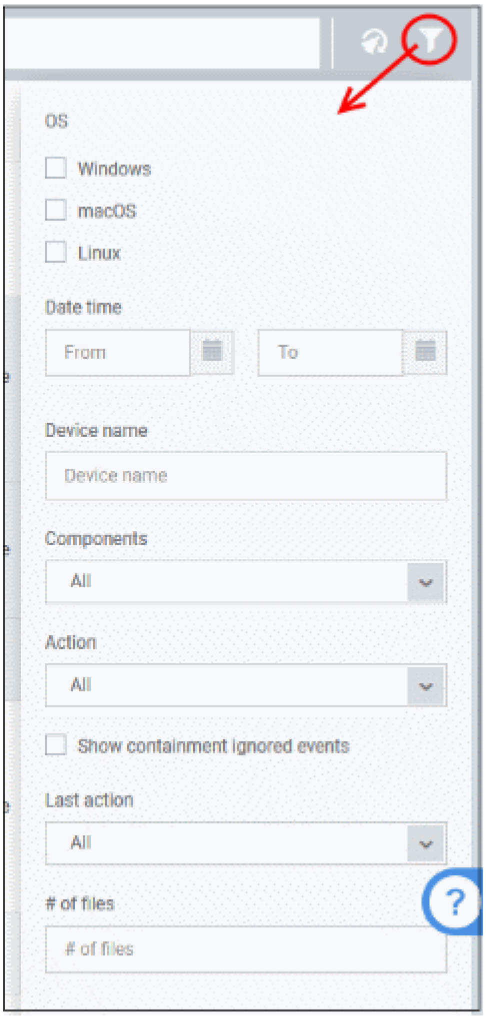
| Security Dashboards - Device View - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date/Time | The time at which the event occurred. |
| OS | The operating system of the device. |
| Device Name | The device label. Click a link to view its **device details**. |
| Components | The security module that reported the event. This can be 'Antivirus', 'Containment', 'Application Control' or 'Autorun Control'. |
| Action | The response to the event. This shows how the file was handled by the CCS component mentioned above.<br>List of possible actions:<br>**Antivirus** - Windows, Mac OS, and Linux devices<br>• Detection of malware<br>• Malware quarantined<br>• Malware removed from quarantine<br>• Malware restored from quarantine<br>• File was skipped by a virus scan |

| | |
|---|---|
| | • Malware removed from infected file<br>• Detected item ignored<br>• Detected file blocked<br>• File added to exclusions<br>• File added to trusted files list<br>• File reported as false positive from the results screen<br>**Containment** - Windows devices<br>• File run inside container with different restriction levels:<br>  • Restricted<br>  • Virtually<br>• File blocked<br>• File ignored<br>**Application Control** - Windows devices<br>• File added to the file list<br>• File removed from the endpoint<br>• Trust rating updated for a file<br>**Autorun Control** - Windows devices<br>• Detected item ignored<br>• Process / service stopped<br>• Auto-run process stopped. Corresponding auto-run entry removed. In the case of a service, CCS disables the service.<br>• Auto-start process quarantined. Corresponding auto-start entry removed. In the case of a service, CCS disables the service.<br>• Processes restored from quarantine<br>• File deleted from the endpoint |
| Last Action | Indicates what was done last on the device related to a security component, for example, file added, file deleted and so on. See above row for list of actions. |
| Number of Files | Shows how many file events were logged for the device. Click the number to view a list of the events. |
| Additional Info | Provides the current status of the event or the action taken on the affected file. |
| **Controls** | |
| Device Details | View general information about the device.<br>• Select a device and click 'Device Details' above.<br>• You will be taken to the 'Device List' screen of the device showing information such as device summary, operating system summary and so on.<br>• See '**View Summary Information**' for more details. |

### Sort, Search and Filter Options

- Click the 'Date/Time' column header to sort events in ascending or descending order

- Enter the device name in the search box to filter events involving the device
- Click the funnel icon at top-right to view more filters:



- Use the search fields to filter events by device, date/time, action and other criteria.
- By default, 'Security Dashboards' > 'Device View' does not show files which are ignored by auto-containment rules.
    - Select 'Show containment ignored events' to include these files.
- To display all items again, clear any search filters and click 'OK'.

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

## 10.2. View Contained Applications

- Click 'Security Sub-Systems' > 'Containment'
- The container is a secure environment in which files with an 'unknown' trust rating are run. 'Unknown' files have not yet been classified as either 'safe' or 'malware'.
- Contained applications are not permitted to modify files, user data or other processes on the host machine.
- You can also submit unknown applications to Valkyrie, Comodo's file analysis system. Valkyrie will test the file and attempt to classify it as 'safe' or 'malware'.

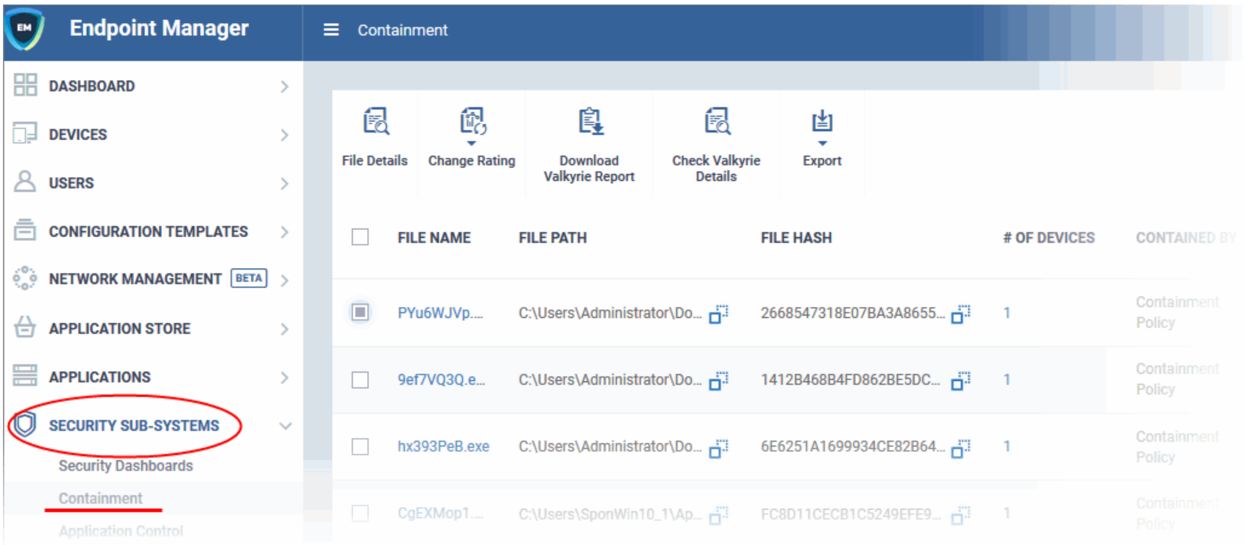
An application could be run inside the container because:

- It was auto-contained by rules in the EM configuration profile applied to the endpoint. See '**Containment Settings**' in **Create Windows Profiles** for more details about containment rules in a profile.
- It was auto-contained by local Comodo Client Security rules on the endpoint
- The endpoint user ran the program inside the container on a 'one-off' basis. This can be helpful to test the behavior of new executables that have they downloaded.

You can view all programs that ran inside the container from the 'Containment' interface. Admins can also view the activity of processes started by contained applications. Admins have the option to rate a contained file as trusted or malicious.

To open the 'Containment' file list interface:

- Click 'Security Sub-Systems' > 'Containment'



| FILE NAME | FILE PATH | FILE HASH | # OF DEVICES | CONTAINED BY |
|---|---|---|---|---|
| PYu6WJVp.... | C:\Users\Administrator\Do... | 2668547318E07BA3A8655... | 1 | Containment Policy |
| 9ef7VQ3Q.e... | C:\Users\Administrator\Do... | 1412B468B4FD862BE5DC... | 1 | Containment Policy |
| hx393PeB.exe | C:\Users\Administrator\Do... | 6E6251A1699934CE82B64... | 1 | Containment Policy |
| CgEXMop1.... | C:\Users\SponWin10_1\Ap... | FC8D11CECB1C5249EFE9... | 1 | Containment Policy |

| Containment - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| File Name | The executable that was run in the container.<br>• Click the name of the file to view its details.<br>• See **View details of a contained application** for more details. |
| File Path | The location of the contained file on the local endpoint.<br>• Click the ⧉ icon to copy the path to the clipboard. |
| File Hash | SHA1 hash value of the file.<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Number of Devices | The quantity of endpoints on which the item was identified.<br>• Click the number to view a list of endpoints on which the item was found.<br>• This also allows you to view the activities of processes started by the item. For more details, see **Device List Screen** below. |
| Contained By | The reason the file was contained. |
| Parent Process Name | The program or service that launched the contained application. |

| | |
|---|---|
| Action | The permission level at which the file was executed in the container, or the action that was taken upon it. The possible values are:<br>• Restricted - The file was run inside the container but had limited access to the operating system resources.<br>• Virtually - The file was completely isolated from the operating system and files on the computer.<br>• Blocked - The file was not allowed to run at all.<br>• Ignored - The file was allowed to run outside the container without any restrictions.<br>• Unknown - The containment status was not determined. |
| Status | The execution state of the file inside the container. The possible values are:<br>• Running<br>• Complete<br>• Failed |
| Admin Rating | The trust rating of the file as set by the administrator. Files can be rated as trusted, malicious or unrecognized. |
| Date Contained | Date and time the file ran in the contained environment. |
| **Controls** | |
| File Details | View full information of the contained file including the devices on which it was contained and its activity. |
| Change Rating | You can change the rating of the contained file as trusted, malicious or unrecognized. |
| Record | Hide or delete a contained file record from the list. |
| Export | Export the list of contained files to a .csv file.<br>The exported file can be viewed in 'Dashboard' > 'Reports'. |
| Download Valkyrie report | Valkyrie is Comodo's advanced file analysis and verdicting system. Each report contains an in-depth breakdown on the activity an unknown file, along with an overall verdict on its trustworthiness. |
| Check Valkyrie details | View Valkyrie file analysis of the contained file at **https://valkyrie.comodo.com** . |

- Click any column header to sort items in ascending/descending order of entries in that column.
- Click the funnel icon on the right to search for contained applications by name, file path, SHA1 file hash, admin rating, action, status and/or execution date.
- To display all the items again, remove / deselect the search key from filter and click 'Apply'.
- EM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down and choose the number.

### Manage Contained Items

The 'Containment' interface allows you to:

- **View details of a contained application**
- **Rate the files**
- **Export file records as CSV file**

- **Download Valkyrie report**
- **View Valkyrie fie analysis report online**

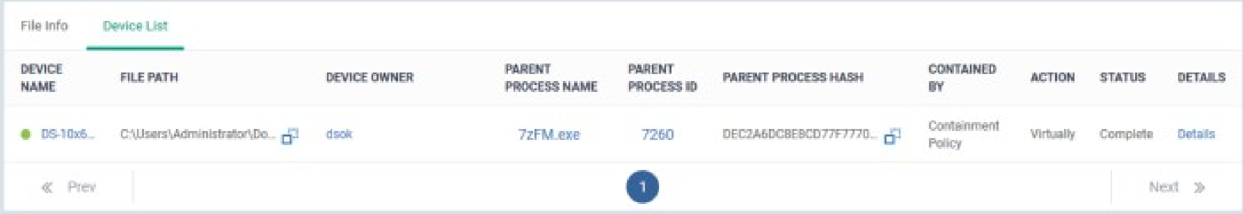
## View details of a contained application

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file-name in the list OR select a file and click file details
- This will open the file details interface which shows:
  - **File Info** - General information such as file-name, path, age, hash and file-size.
  - **Device List** - Shows endpoints upon which the file was found. This tab also tells you the device owner and lists any activities by the file. The next sections contain more info on these items:

## Device List Screen

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file name in the list OR select a file and click file details
- Click the 'Device List' tab

The 'Device List' shows endpoints on which the file was discovered and its activities. Admins can view processes executed by the file with details on data handled by each process.



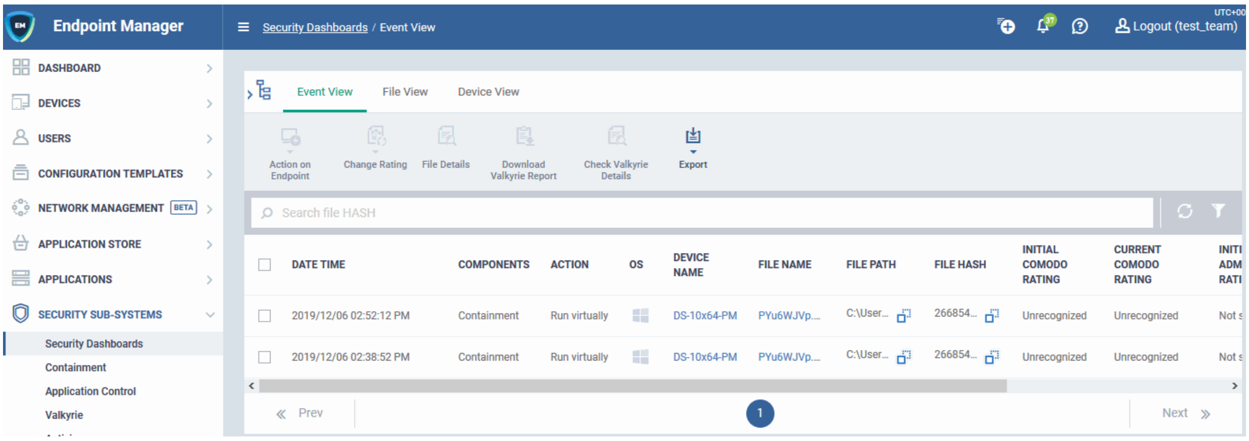
| DEVICE NAME | FILE PATH | DEVICE OWNER | PARENT PROCESS NAME | PARENT PROCESS ID | PARENT PROCESS HASH | CONTAINED BY | ACTION | STATUS | DETAILS |
|---|---|---|---|---|---|---|---|---|---|
| ● DS-10x6... | C:\Users\Administrator\Do... | dsok | 7zFM.exe | 7260 | DEC2A6DCBE8CD77F7770... | Containment Policy | Virtually | Complete | Details |

## View File Activities on Endpoints

- Click 'Security Sub-Systems' > 'Containment'
- Click on a specific file-name in the list OR select a file and click 'File Details'
- Click the 'Device List' tab

> **Note**: VirusScope must be enabled in the profile in effect on the endpoint for Endpoint Manager to collect file activity data. See **VirusScope Settings** in **Create Windows Profiles** for more details.

- To view the details of an activity, click the 'Details' link under the 'Details' column

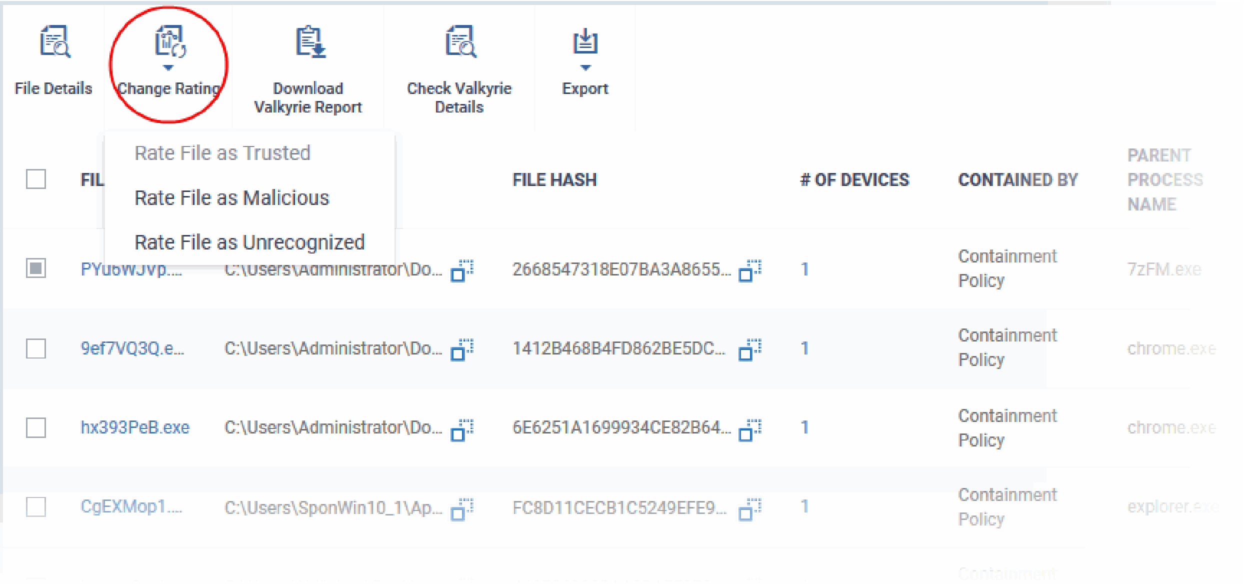


| □ | DATE TIME | COMPONENTS | ACTION | OS | DEVICE NAME | FILE NAME | FILE PATH | FILE HASH | INITIAL COMODO RATING | CURRENT COMODO RATING | INITI ADM RATI |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 2019/12/06 02:52:12 PM | Containment | Run virtually | ⊞ | DS-10x64-PM | PYu6WJVp.... | C:\User... | 266854... | Unrecognized | Unrecognized | Not s |
| □ | 2019/12/06 02:38:52 PM | Containment | Run virtually | ⊞ | DS-10x64-PM | PYu6WJVp.... | C:\User... | 266854... | Unrecognized | Unrecognized | Not s |

## Rate files as trusted / malicious

If required, admins can rate contained files as unrecognized, trusted or malicious. Please make sure before marking a file as trusted. Any new file ratings will be sent to endpoints during the next sync.

- Click 'Security Sub-Systems' > 'Containment'
- Select the file(s) whose rating you wish to change
- Click the 'Change Rating' button
- Set your preferred rating from the options:

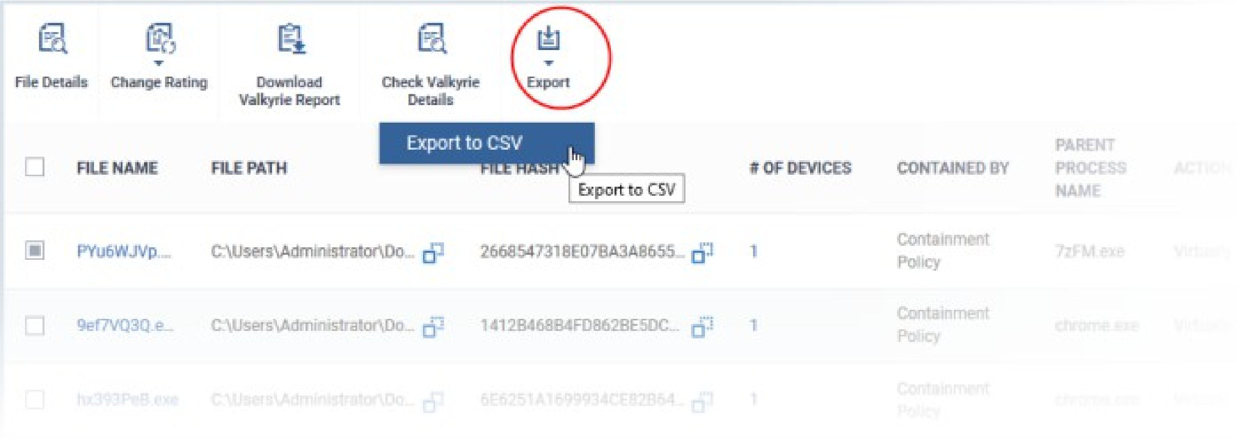


| ☐ | FIL |  | FILE HASH | # OF DEVICES | CONTAINED BY | PARENT PROCESS NAME |
|---|---|---|---|---|---|---|
| ☒ | PYu6WJVp.... | C:\Users\Administrator\Do... | 2668547318E07BA3A8655... | 1 | Containment Policy | 7zFM.exe |
| ☐ | 9ef7VQ3Q.e... | C:\Users\Administrator\Do... | 1412B468B4FD862BE5DC... | 1 | Containment Policy | chrome.exe |
| ☐ | hx393PeB.exe | C:\Users\Administrator\Do... | 6E6251A1699934CE82B64... | 1 | Containment Policy | chrome.exe |
| ☐ | CgEXMop1.... | C:\Users\SponWin10_1\Ap... | FC8D11CECB1C5249EFE9... | 1 | Containment Policy | explorer.exe |

The new rating will be propagated to all endpoints during the next synchronization.

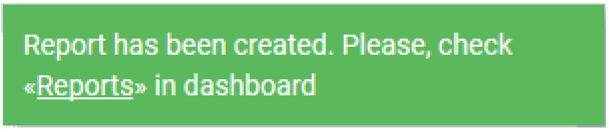
### Export file records as a CSV file

- Click 'Security Sub-Systems' > 'Containment'
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| ☐ | FILE NAME | FILE PATH | FILE HASH | # OF DEVICES | CONTAINED BY | PARENT PROCESS NAME | ACTION |
|---|---|---|---|---|---|---|---|
| ☒ | PYu6WJVp.... | C:\Users\Administrator\Do... | 2668547318E07BA3A8655... | 1 | Containment Policy | 7zFM.exe | Virtual |
| ☐ | 9ef7VQ3Q.e... | C:\Users\Administrator\Do... | 1412B468B4FD862BE5DC... | 1 | Containment Policy | chrome.exe | Virtual |
| ☐ | hx393PeB.exe | C:\Users\Administrator\Do... | 6E6251A1699934CE82B64... | 1 | Containment Policy | chrome.exe | Virtual |

The report will be generated in .csv file format.



Report has been created. Please, check «Reports» in dashboard

You can access the report in the 'Dashboard' > 'Reports' interface. See **Reports** if you need more help with this interface.

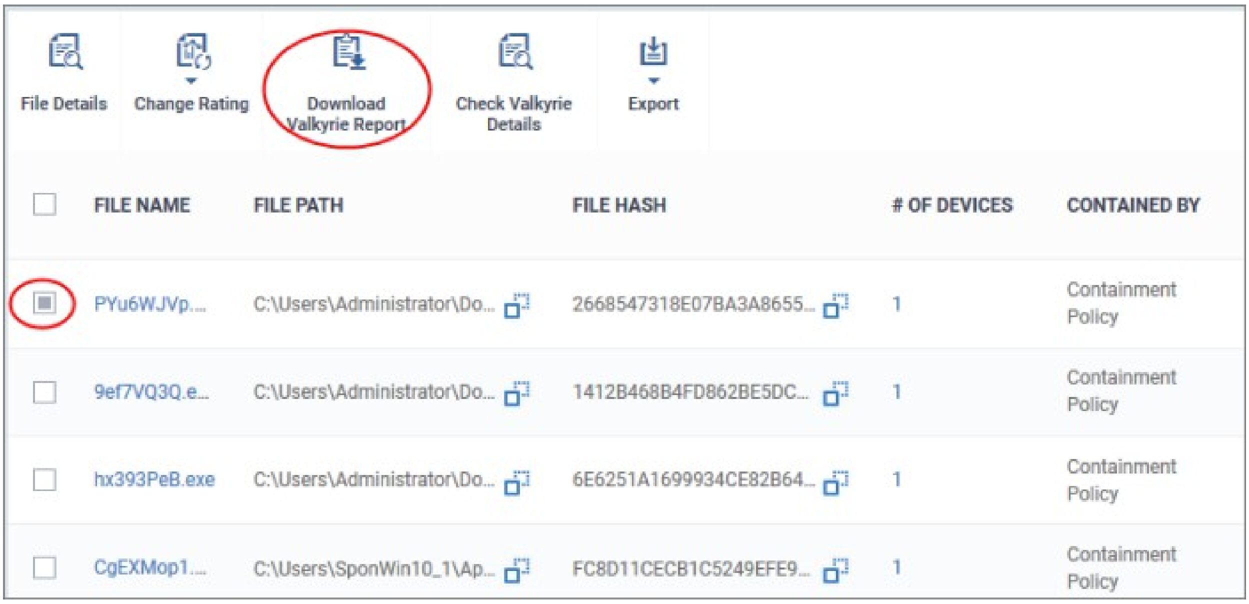
## Valkyrie Reports

Files running in the container are analyzed and rated by Comodo's behavior analysis system, Valkyrie. Valkyrie tests unknown files with a range of static and dynamic behavioral checks to identify whether they are malicious or safe.

You can view the file rating in the '**Application Control**' interface also. You can download a Valkyrie report or view it online at **https://valkyrie.comodo.com/**

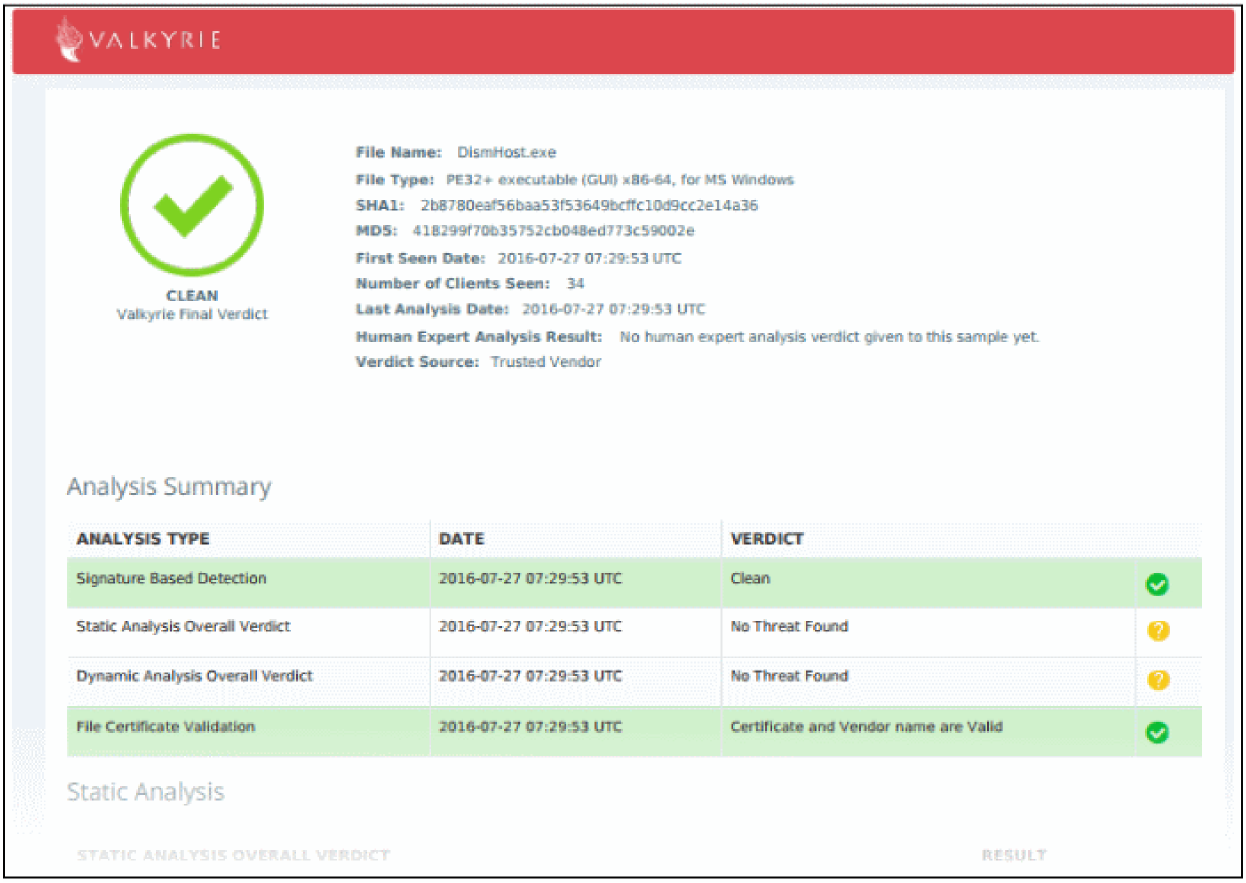
### Download Valkyrie report

- Click 'Security Sub-Systems' > 'Containment'
- Select any file
- Click 'Download Valkyrie report':



| □ | FILE NAME | FILE PATH | FILE HASH | # OF DEVICES | CONTAINED BY |
|---|---|---|---|---|---|
| ■ | PYu6WJVp.... | C:\Users\Administrator\Do... | 2668547318E07BA3A8655... | 1 | Containment Policy |
| □ | 9ef7VQ3Q.e... | C:\Users\Administrator\Do... | 1412B468B4FD862BE5DC... | 1 | Containment Policy |
| □ | hx393PeB.exe | C:\Users\Administrator\Do... | 6E6251A1699934CE82B64... | 1 | Containment Policy |
| □ | CgEXMop1.... | C:\Users\SponWin10_1\Ap... | FC8D11CECB1C5249EFE9... | 1 | Containment Policy |

This will open the Valkyrie report on the contained file in PDF format:



CLEAN
Valkyrie Final Verdict

**File Name:** DismHost.exe
**File Type:** PE32+ executable (GUI) x86-64, for MS Windows
**SHA1:** 2b8780eaf56baa53f53649bcffc10d9cc2e14a36
**MD5:** 418299f70b35752cb048ed773c59002e
**First Seen Date:** 2016-07-27 07:29:53 UTC
**Number of Clients Seen:** 34
**Last Analysis Date:** 2016-07-27 07:29:53 UTC
**Human Expert Analysis Result:** No human expert analysis verdict given to this sample yet.
**Verdict Source:** Trusted Vendor

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---|---|---|---|
| Signature Based Detection | 2016-07-27 07:29:53 UTC | Clean | ✓ |
| Static Analysis Overall Verdict | 2016-07-27 07:29:53 UTC | No Threat Found | ? |
| Dynamic Analysis Overall Verdict | 2016-07-27 07:29:53 UTC | No Threat Found | ? |
| File Certificate Validation | 2016-07-27 07:29:53 UTC | Certificate and Vendor name are Valid | ✓ |

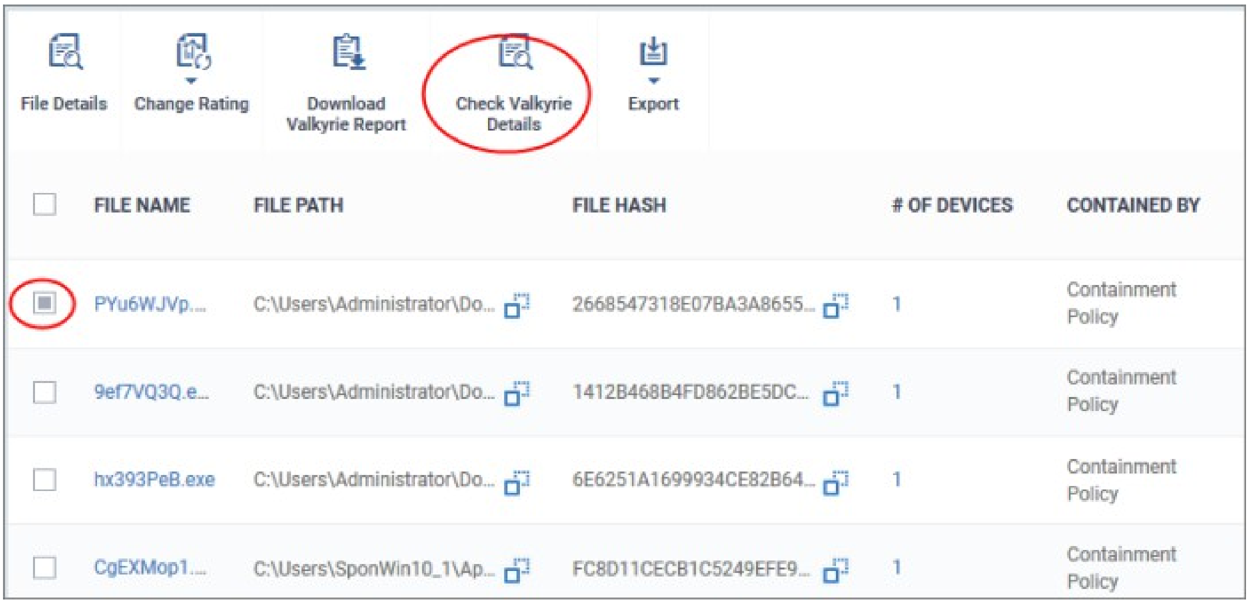
Static Analysis

STATIC ANALYSIS OVERALL VERDICT RESULT

You can also download and view the report at https://valkyrie.comodo.com/ after signing into your Valkyrie account.

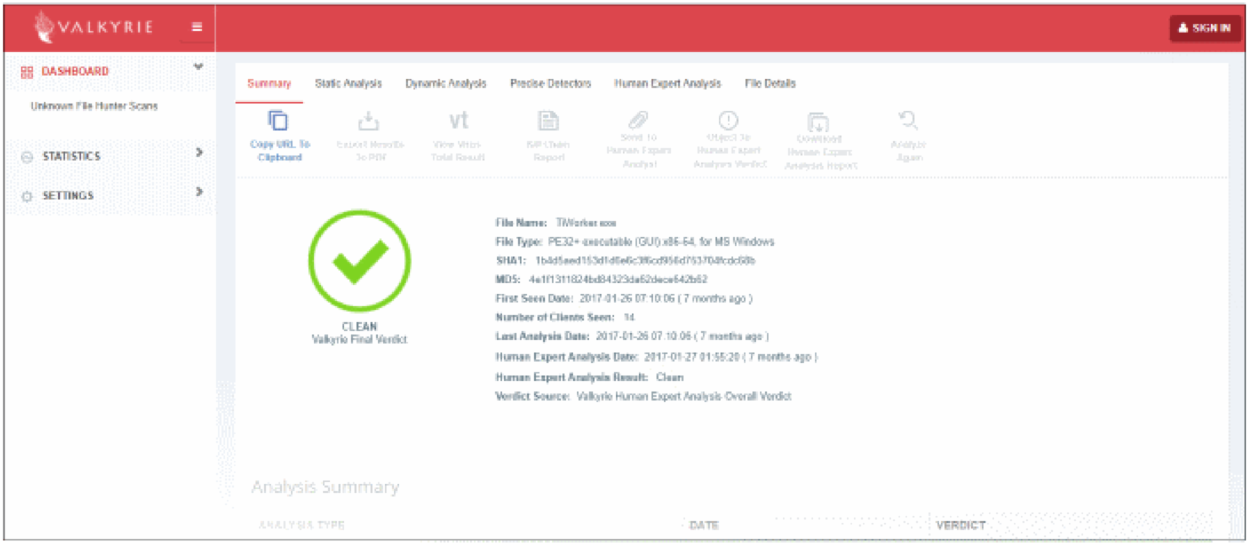
### View Valkyrie fie analysis report online

- Select the file from the list and click 'Check Valkyrie Details' at the top.



| □ | FILE NAME | FILE PATH | FILE HASH | # OF DEVICES | CONTAINED BY |
|---|---|---|---|---|---|
| ☑ | PYu6WJVp... | C:\Users\Administrator\Do... | 2668547318E07BA3A8655... | 1 | Containment Policy |
| □ | 9ef7VQ3Q.e... | C:\Users\Administrator\Do... | 1412B468B4FD862BE5DC... | 1 | Containment Policy |
| □ | hx393PeB.exe | C:\Users\Administrator\Do... | 6E6251A1699934CE82B64... | 1 | Containment Policy |
| □ | CgEXMop1.... | C:\Users\SponWin10_1\Ap... | FC8D11CECB1C5249EFE9... | 1 | Containment Policy |

You will be taken to the report summary page of the selected file at https://valkyrie.comodo.com/.



File Name: TiWorker.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 1b4d5aed153d1d6e6c3f6cd956d7537049cdc68b
MD5: 4e1f1311824bd84323da62dece642b62
First Seen Date: 2017-01-26 07:10:06 ( 7 months ago )
Number of Clients Seen: 14
Last Analysis Date: 2017-01-26 07:10:06 ( 7 months ago )
Human Expert Analysis Date: 2017-01-27 01:55:20 ( 7 months ago )
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

- View a more detailed version of the Valkyrie analysis by logging in at **https://valkyrie.comodo.com/**. You can use your Comodo One username and password to login.
- See **https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html** for help to use the Valkyrie online portal.

# 10.3. Manage File Trust Ratings on Windows Devices

- Click 'Security Sub-Systems' > 'Application Control' to open the 'Application Control' interface.
- Comodo Client Security (CCS) monitors all file activity on Windows devices. Every new executable is scanned against the Comodo white and blacklists then awarded a rating of '**Unrecognized**', '**Trusted**' or '**Malicious**'.
- Files that have a rating of 'Unrecognized' or 'Malicious' are reported to the 'Application Control' interface. Admins can change the rating of a file as required.
- You can configure file analysis in the 'File Rating settings' section of the configuration profile applied to the device. See **File Rating settings** in **Creating a Windows Profile** for more details.
- See **File Ratings Explained** for background information on file ratings.

## The Application Control Interface

The 'Application Control' interface lets you view the trust rating of files on an endpoint. Possible ratings are 'Unrecognized', 'Trusted' or 'Malicious', with 'Unrecognized' and 'Malicious' files being reported to this interface. You can manually set the rating of a file at your discretion.

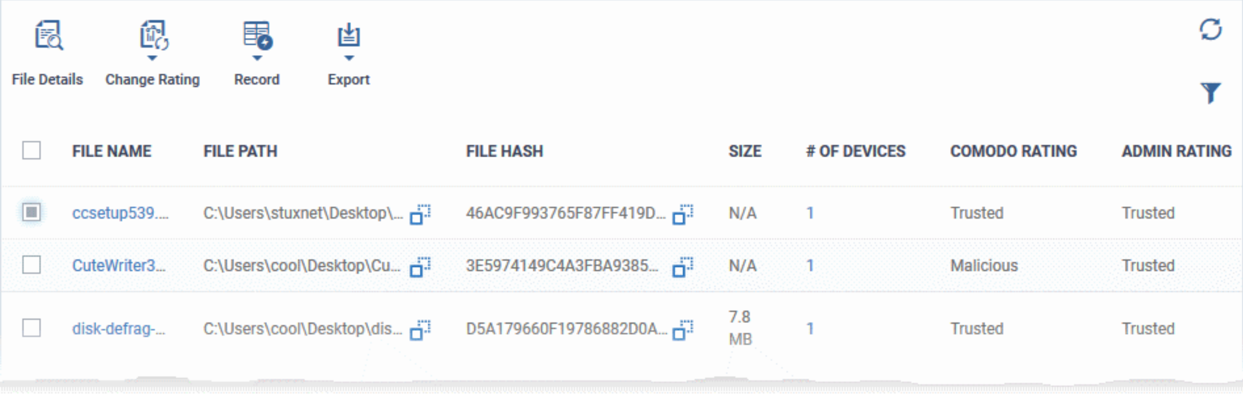
- Files rated as 'Trusted' are allowed to run as normal on the endpoint.
- Files rated as 'Malicious' are quarantined and not allowed to run.
- Files rated as 'Unrecognized' are run inside the container - an isolated operating environment. Contained applications are not permitted to access files or user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

Any rating you set for a file is pushed to all managed endpoints on which the file is installed.

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

You can also hide items as required.

- Click 'Security Sub-Systems' > Application Control' to open the application control interface:

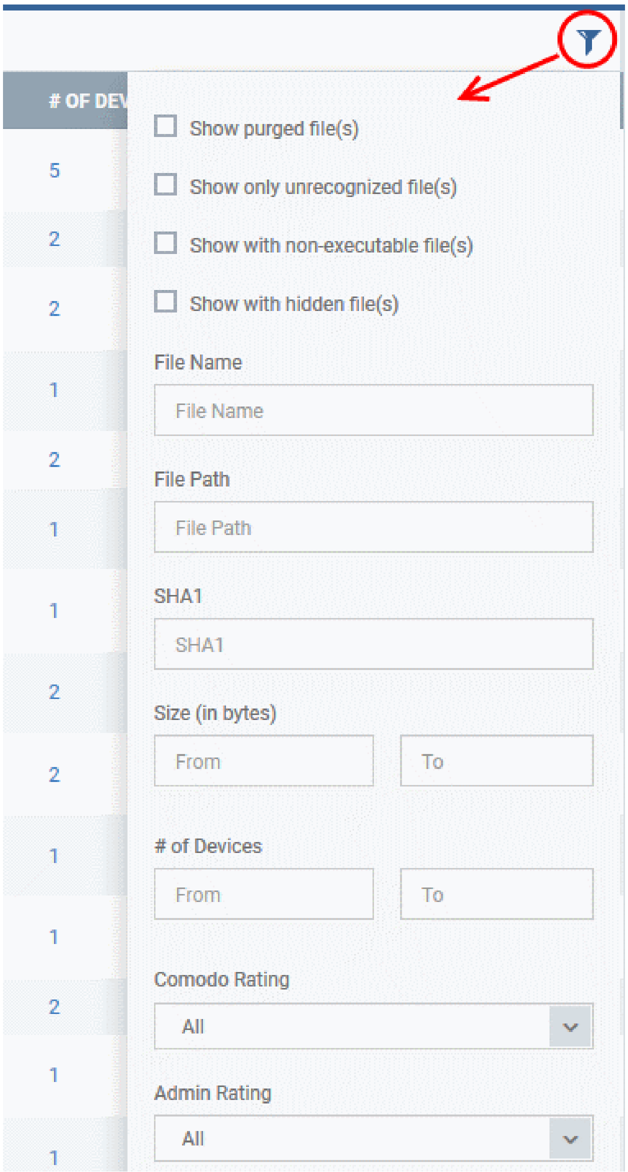


| □ | FILE NAME | FILE PATH | FILE HASH | SIZE | # OF DEVICES | COMODO RATING | ADMIN RATING |
|---|---|---|---|---|---|---|---|
| ▣ | ccsetup539.... | C:\Users\stuxnet\Desktop\... ⧉ | 46AC9F993765F87FF419D... ⧉ | N/A | 1 | Trusted | Trusted |
| □ | CuteWriter3... | C:\Users\cool\Desktop\Cu... ⧉ | 3E5974149C4A3FBA9385... ⧉ | N/A | 1 | Malicious | Trusted |
| □ | disk-defrag-... | C:\Users\cool\Desktop\dis... ⧉ | D5A179660F19786882D0A... ⧉ | 7.8 MB | 1 | Trusted | Trusted |

| Application Control - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| File Name | The label of the application/executable file.<br>• Click the name of a file to view its details.<br>• See **View file details** given below for more details. |
| File Path | The installation location of the application on the endpoint.<br>• Click the ⧉ icon to copy the path to the clipboard. |
| File Hash | The SHA1 hash value of the executable file.<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Size | The size of the executable file. |
| # of Devices | The count of endpoints on which the item was found.<br>• Click the number to view the the 'Device List' interface with a list of endpoints containing the item.<br>• You can also view the activities of the item from here. For more details, refer to the description under **Device List Screen** below. |
| Comodo Rating | The rating of the file as per the Comodo File Look-up service, reported by the CCS installations at the endpoints. See **File Ratings Explained** for more details. |
| Admin Rating | Indicates the rating of the file as manually set by the administrator, if any. |

## Sorting, Search and Filter Options

- Click any column header to sort items in alphabetical order
- Click the funnel icon ▼ to open more filter options:



□ Show purged file(s)

□ Show only unrecognized file(s)

□ Show with non-executable file(s)

□ Show with hidden file(s)

File Name: File Name

File Path: File Path

SHA1: SHA1

Size (in bytes): From To

# of Devices: From To

Comodo Rating: All

Admin Rating: All

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

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

## Manage Applications

The Applications Control interface allows you to:

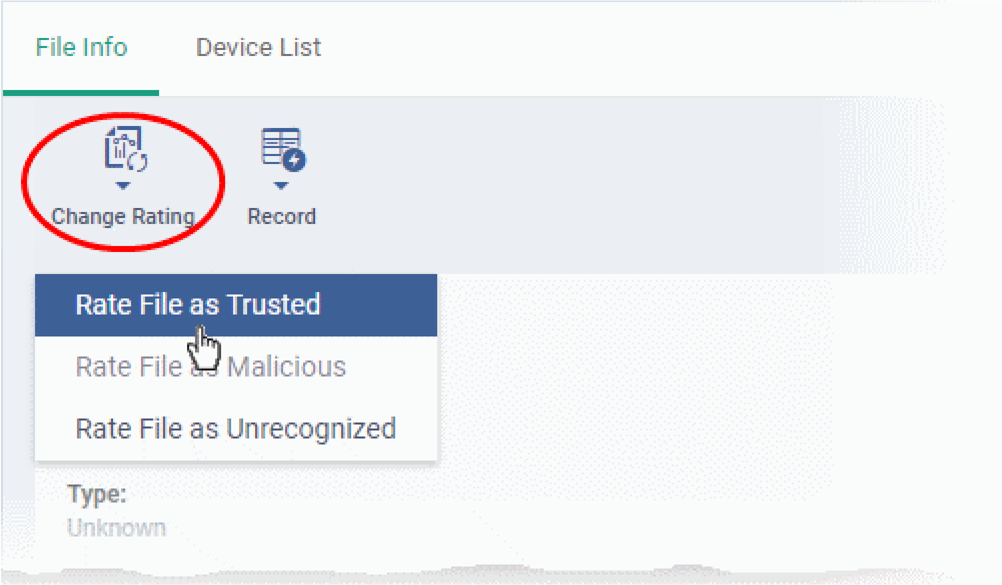
- **View the details of files in the list**
- **View Process Activities of a File**
- **Assign Admin rating to a file**
- **Hide/Display selected files in the list**
- **Export the list of selected files to a CSV file**
- **Remove files from the list**

## View file details

- Simply click on a file in the list or select a file and click 'File Details' at the top. The 'file info' screen shows basic file details and the devices on which the file is present. You can also change the trust rating of the file in this area.

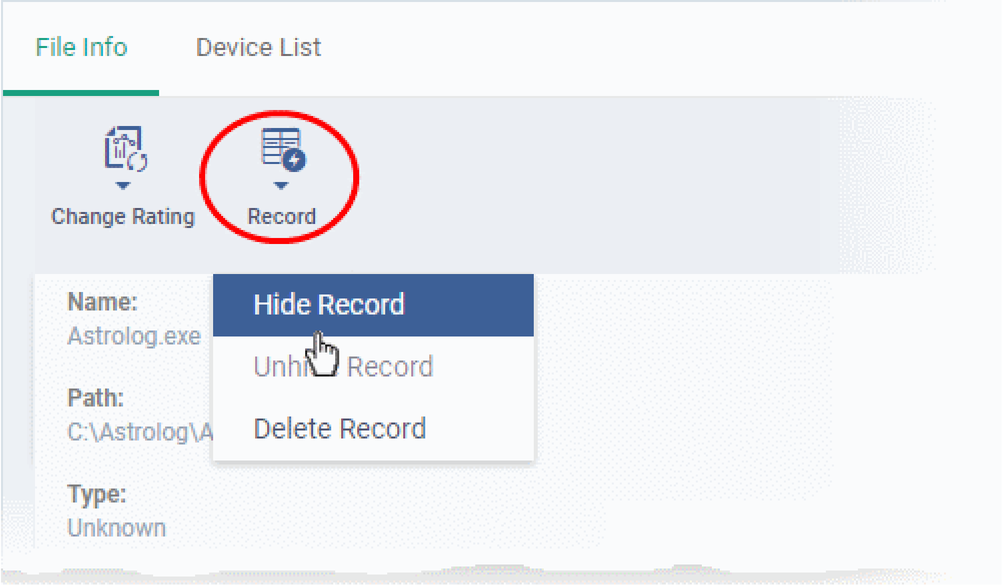
## File information

- The file info screen shows file name, installation path, file type, version, size, hash values and the date the file was first encountered. The screen also shows the file's trust rating and the number of endpoints on which the file is present.
- The 'Change Rating' button allows you to manually set the file's rating as 'Trusted', 'Malicious' or 'Unrecognized':



The new rating will be sent to all endpoints.

- The 'Record' button lets you hide, display or remove the file from the 'Application Control' list



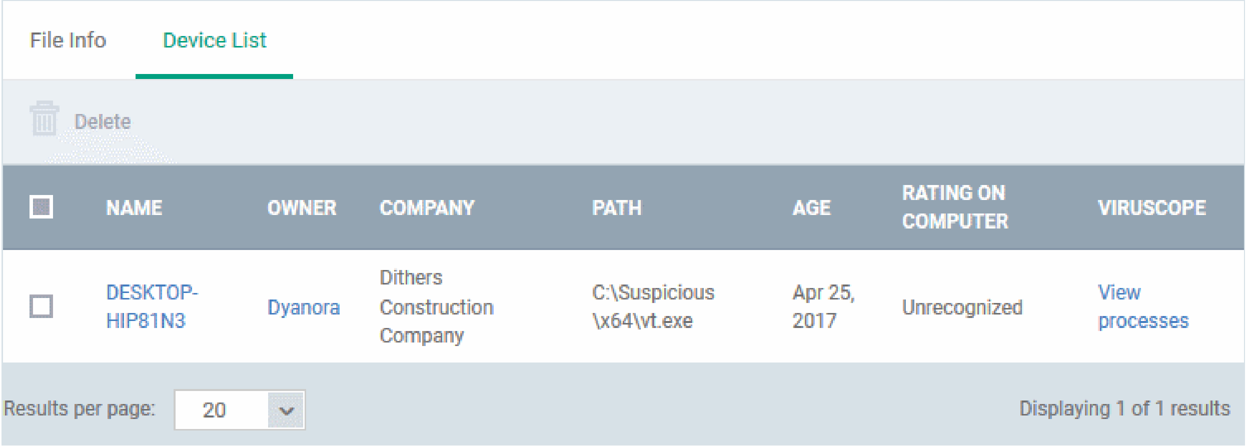
Name:
Astrolog.exe

Path:
C:\Astrolog\A

Type:
Unknown

## Device List Screen

- Click 'Security Sub-Systems' > 'Application Control' then click on a file in the list.
- Next, select the 'Device List' tab to see a list of all devices on which the file is present
- The 'Device List' Screen can also be opened by clicking on the number in the 'Number of Devices' column in the 'Application Control' table.
- The device list screen shows each endpoint on which the item was discovered. The screen also shows the installation path, the installation date and the file rating assigned by Comodo Client Security. The Viruscope column shows detailed info on processes started by the file.



| □ | NAME | OWNER | COMPANY | PATH | AGE | RATING ON COMPUTER | VIRUSCOPE |
|---|---|---|---|---|---|---|---|
| □ | DESKTOP-HIP81N3 | Dyanora | Dithers Construction Company | C:\Suspicious \x64\vt.exe | Apr 25, 2017 | Unrecognized | View processes |

Results per page: 20

Displaying 1 of 1 results

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

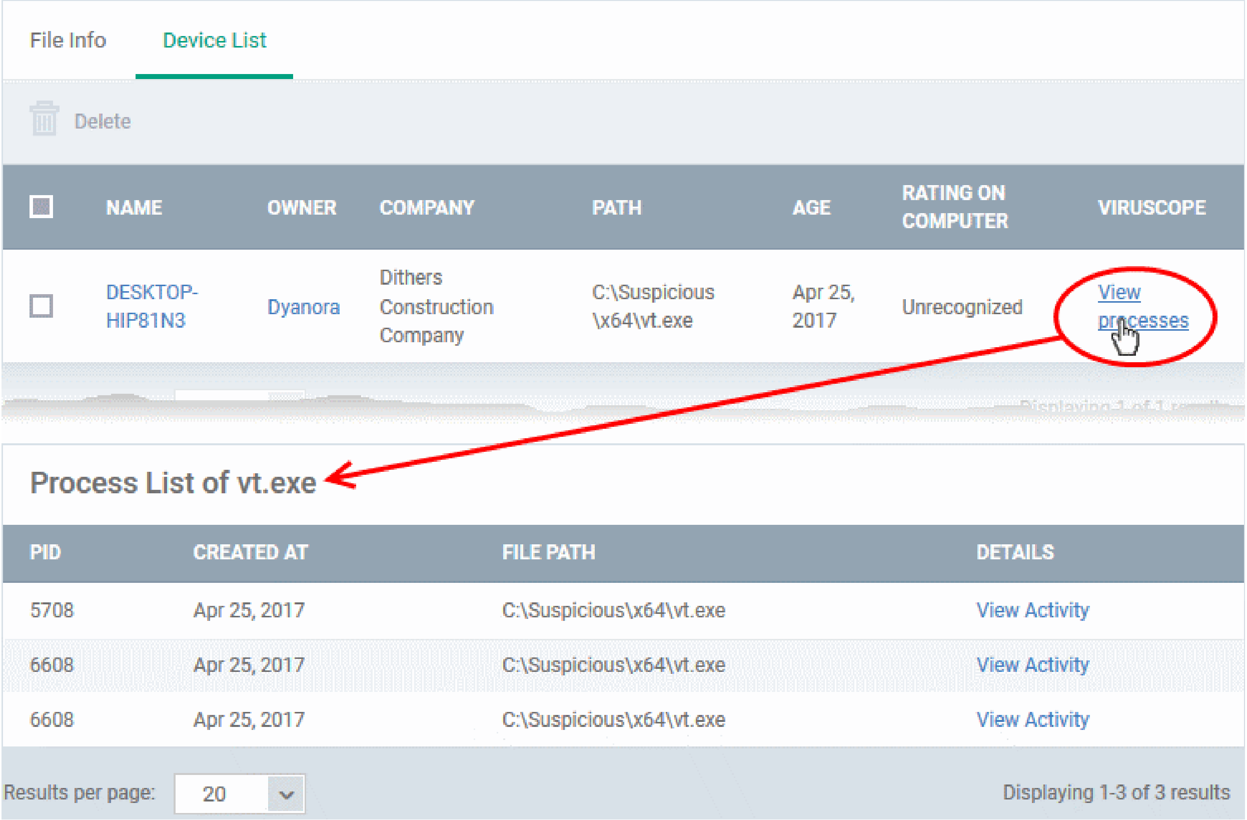
## View Process Activities of a File

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

### To view the activities of a file on an endpoint

- Open the 'Device List' screen by clicking the file name or the number in the 'Number of Devices' column

- Click the 'View Processes' link in the 'Activity' column in the row of the device name.
- This will open a list of processes executed by the file on the selected endpoint:



| ☐ | NAME | OWNER | COMPANY | PATH | AGE | RATING ON COMPUTER | VIRUSCOPE |
|---|---|---|---|---|---|---|---|
| ☐ | DESKTOP-HIP81N3 | Dyanora | Dithers Construction Company | C:\Suspicious \x64\vt.exe | Apr 25, 2017 | Unrecognized | View processes |

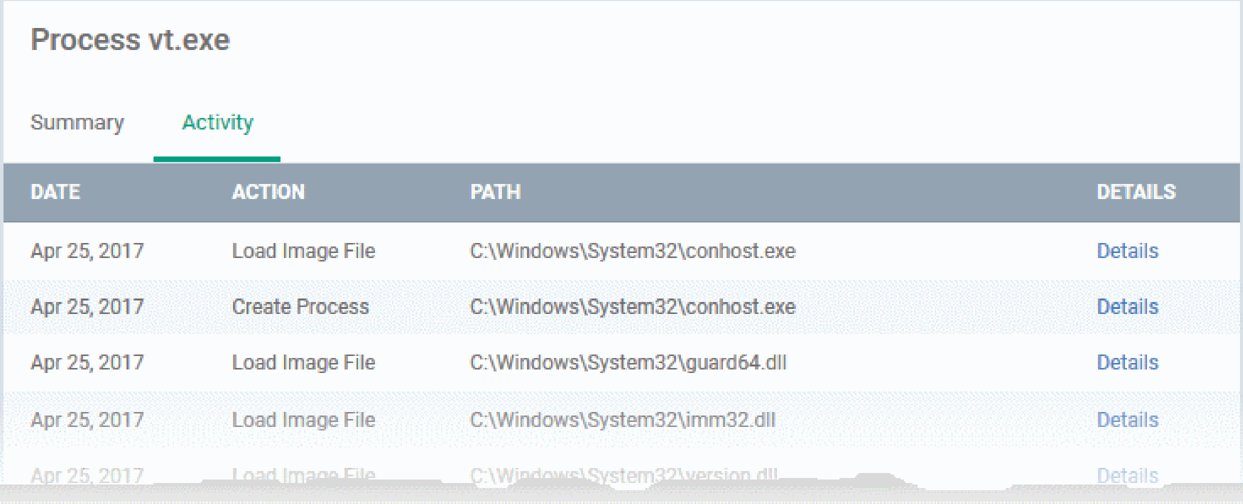
Process List of vt.exe

| PID | CREATED AT | FILE PATH | DETAILS |
|---|---|---|---|
| 5708 | Apr 25, 2017 | C:\Suspicious\x64\vt.exe | View Activity |
| 6608 | Apr 25, 2017 | C:\Suspicious\x64\vt.exe | View Activity |
| 6608 | Apr 25, 2017 | C:\Suspicious\x64\vt.exe | View Activity |

Results per page: 20

Displaying 1-3 of 3 results

- Click 'View Activity' to see detailed information about each process. The 'Process Activity' interface has two tabs:
  - **Summary -** Displays the name of the device and the installation path of the executable
  - **Activity -** Displays a chronological list of activities by the selected process, including details of files modified by the process.



Process vt.exe

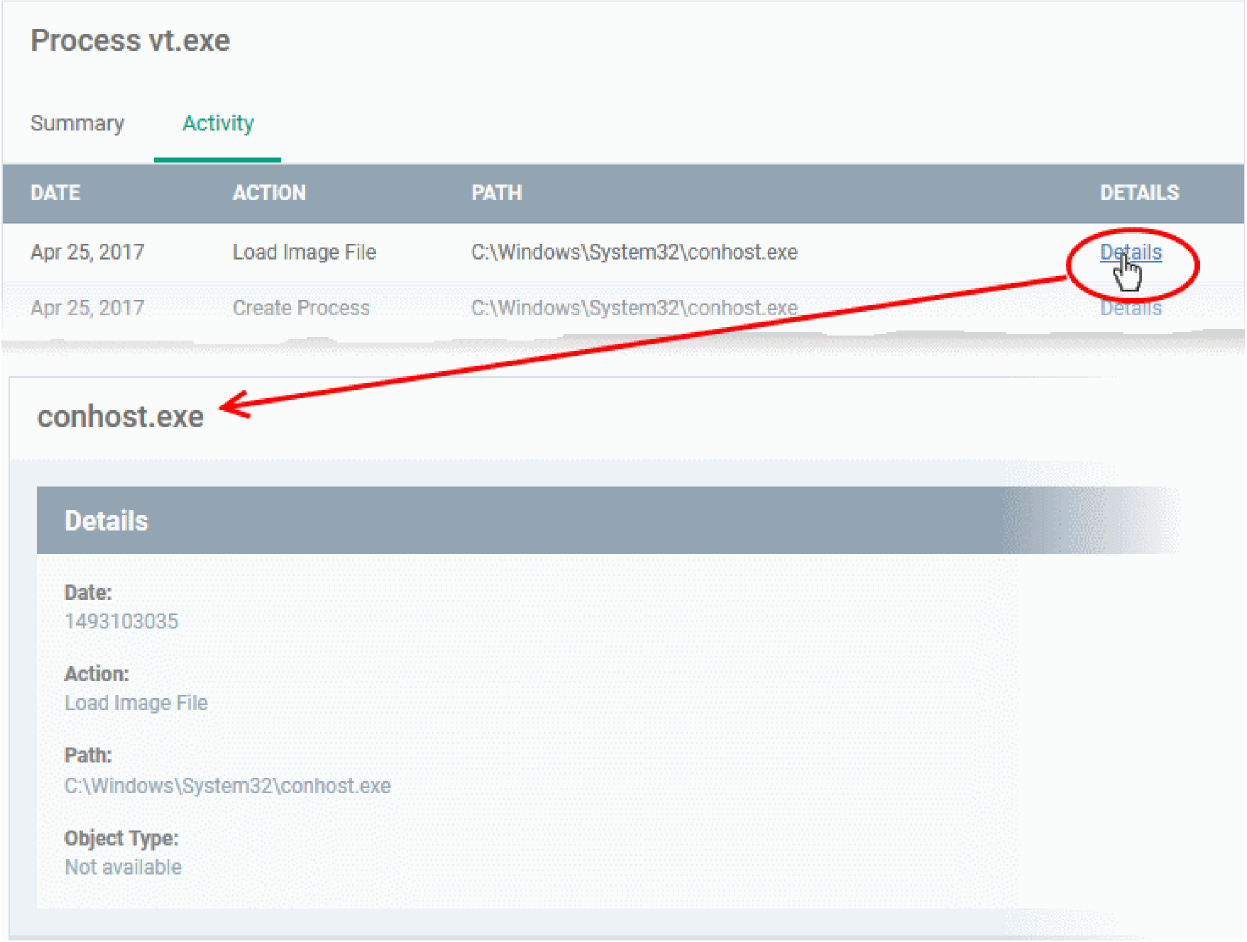
| DATE | ACTION | PATH | DETAILS |
|---|---|---|---|
| Apr 25, 2017 | Load Image File | C:\Windows\System32\conhost.exe | Details |
| Apr 25, 2017 | Create Process | C:\Windows\System32\conhost.exe | Details |
| Apr 25, 2017 | Load Image File | C:\Windows\System32\guard64.dll | Details |
| Apr 25, 2017 | Load Image File | C:\Windows\System32\imm32.dll | Details |
| Apr 25, 2017 | Load Image File | C:\Windows\System32\version.dll | Details |

The 'Activity' - Table of Column Descriptions

| Column Heading | Description |
|---|---|

| | |
|---|---|
| Date | Indicates the date and time of process execution |
| Action | Indicates the action executed by the process on the target file |
| Path | Indicates the path of the target file |
| Details | Contains a link to view details of the action |

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


Process vt.exe

| DATE | ACTION | PATH | DETAILS |
|---|---|---|---|
| Apr 25, 2017 | Load Image File | C:\Windows\System32\conhost.exe | Details |
| Apr 25, 2017 | Create Process | C:\Windows\System32\conhost.exe | Details |

conhost.exe

Details

Date:
1493103035

Action:
Load Image File

Path:
C:\Windows\System32\conhost.exe

Object Type:
Not available

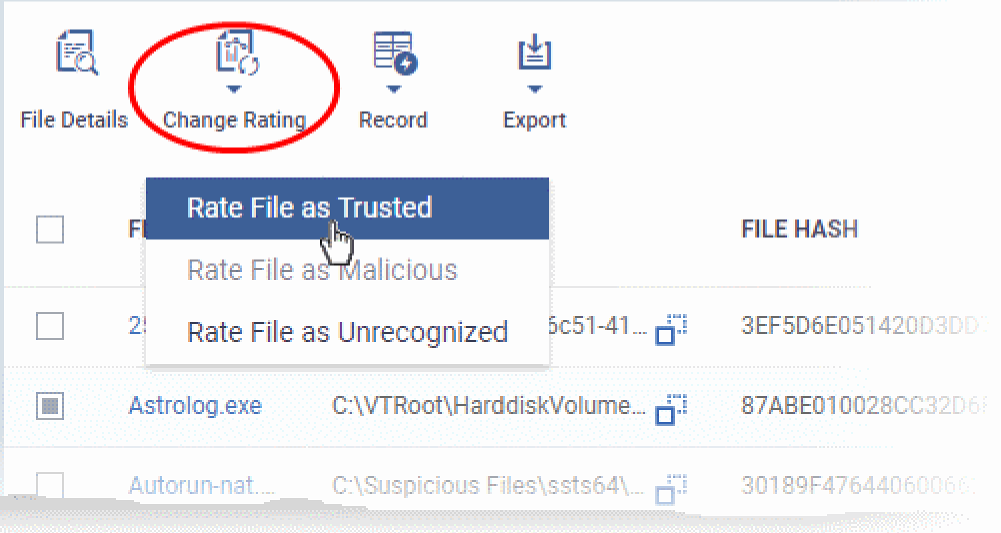
## Assign Admin Rating to a File

- Each file on an endpoint is automatically scanned and assigned a trust rating by Comodo Client Security on the endpoint.
- These ratings can be either '**Unrecognized**', '**Trusted**' or '**Malicious**'. The rating for each file is shown in the 'Comodo Rating' column of the 'Application Control' interface.
- The file rating determines whether or how the file is allowed to run:
    - **Trusted -** The file will be allowed to run normally. It will, of course, still be subject to the standard protection mechanisms of Comodo Client Security (behavior monitoring, host intrusion prevention etc).
    - **Malicious -** The file will not be allowed to run. It will be automatically quarantined or deleted depending on admin preferences.
    - **Unknown -** The file will be run inside the container. The container is a virtual operating environment which is isolated from the rest of the endpoint. Files in the container write to a virtual file system, use a virtual registry and cannot access user or operating system data.

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

**To assign a file rating to a file**

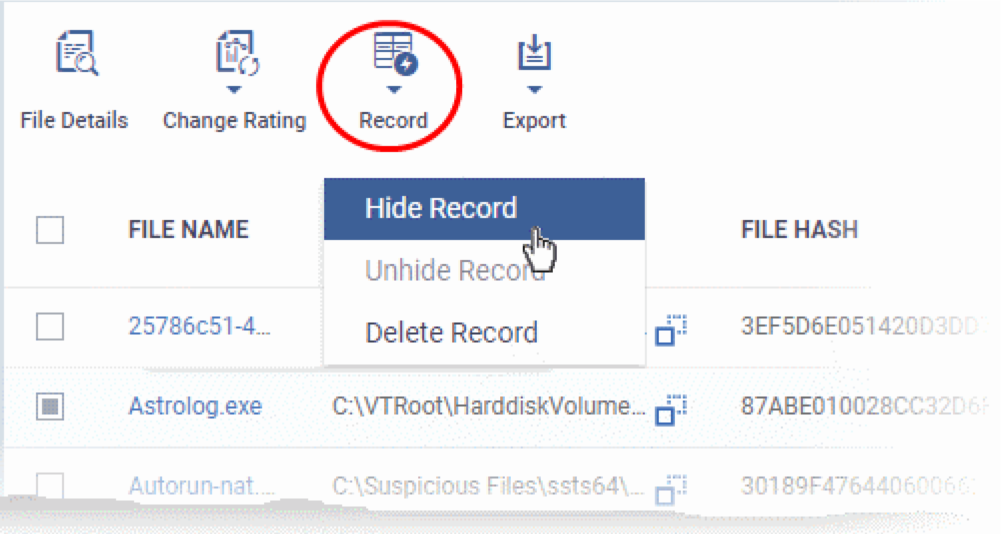
- Select the file(s) whose rating you want to change and click 'Change Rating'.
- Choose the rating you want to from the drop-down:



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

## Hide/Display Selected Files

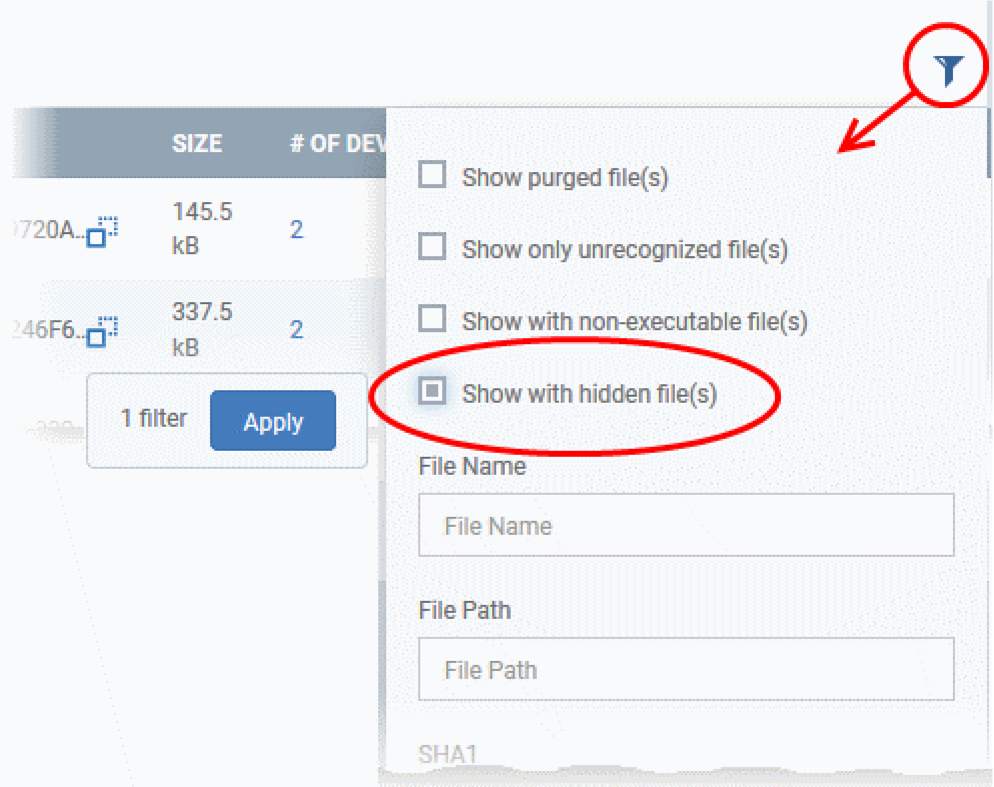
- Select the file(s) you want to hide and click 'Record' at the top



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

**To view hidden files**

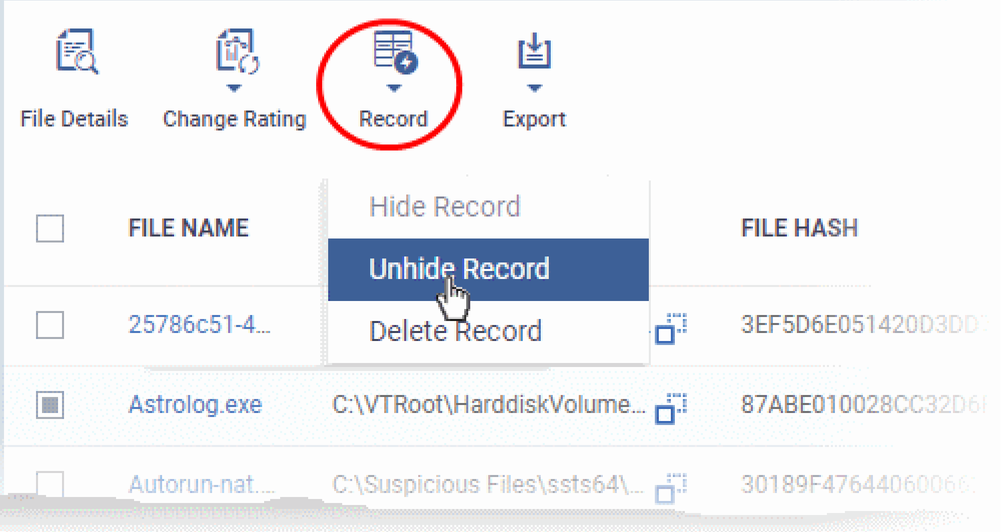
- Click the funnel icon at the top-right to open the filter options
- Select 'Show with hidden file(s)' and click 'Apply'



The hidden files will be included to the 'Application Control' interface. These files will be highlighted with a gray stripe.

**To restore hidden files**

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

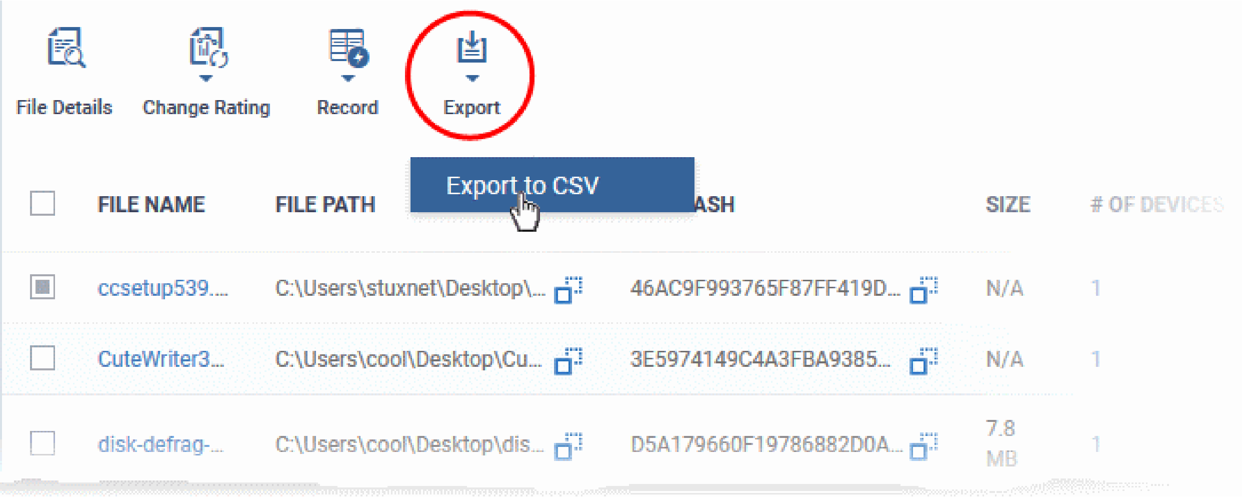


The files will be displayed in the file list permanently.

## Export a Report of the Files List

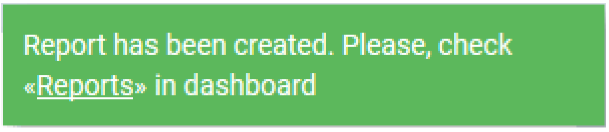
You can export a file-rating report in .csv format as follows:

- Click 'Security Sub-Systems' > 'Application Control'
- Click the funnel icon to apply any filters you require
- Click the 'Export' button and choose 'Export to CSV':



| ☐ | FILE NAME | FILE PATH | ASH | SIZE | # OF DEVICES |
|---|---|---|---|---|---|
| ☒ | ccsetup539.... | C:\Users\stuxnet\Desktop\... | 46AC9F993765F87FF419D... | N/A | 1 |
| ☐ | CuteWriter3... | C:\Users\cool\Desktop\Cu... | 3E5974149C4A3FBA9385... | N/A | 1 |
| ☐ | disk-defrag-... | C:\Users\cool\Desktop\dis... | D5A179660F19786882D0A... | 7.8 MB | 1 |

The report will be generated in .csv file format.



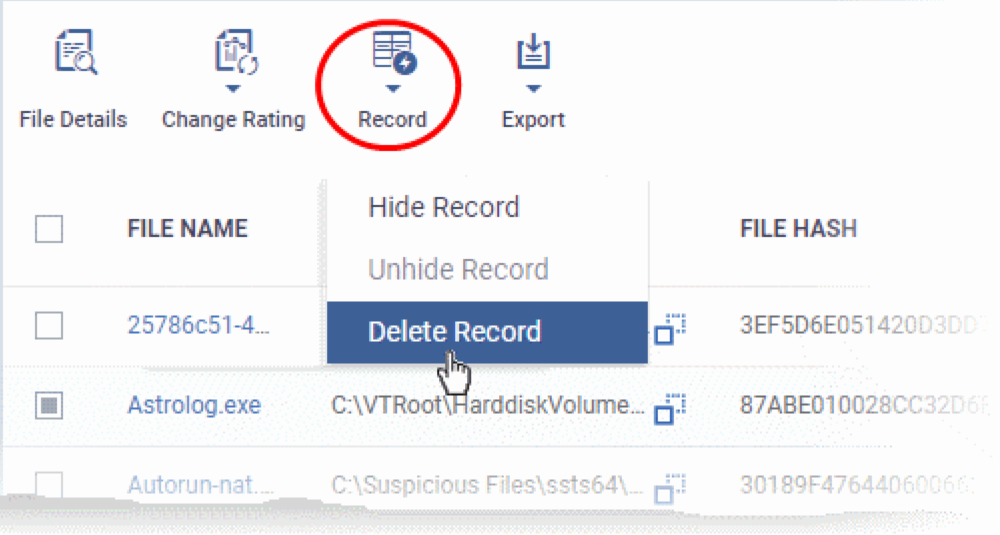
Report has been created. Please, check «Reports» in dashboard

The report will be available in the 'Dashboard' > 'Reports' interface. See **Reports** if you need more help with this interface.

## Remove files from the list

You can hide files that you no longer wish to see in the list. The files will be removed from the list but will not be deleted from the endpoints.

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



| ☐ | FILE NAME | | FILE HASH |
|---|---|---|---|
| ☐ | 25786c51-4... | | 3EF5D6E051420D3DD |
| ☒ | Astrolog.exe | C:\VTRoot\HarddiskVolume... | 87ABE010028CC32D6F |
| ☐ | Autorun-nat... | C:\Suspicious Files\ssts64\... | 30189F4764406006C |

### 10.3.1. File Ratings Explained

Comodo Client Security (CCS) rates files on Windows devices as follows:

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

**Trusted Files**
Files that are safe to run. Files can be classed as safe by the following:

- **File lookup service (FLS)** - Whenever a file is accessed, Comodo Client Security (CCS) checks the file's reputation on Comodo's online file database.
- **Vendor rating** - The app was created by a vendor who has a 'Trusted' status in the local vendor list. Open CCS > Click 'Settings' > 'File Rating' > 'Vendor List'.
- **Admin rating** - You can assign a trusted rating to files in Endpoint Manager at 'Security Sub-Systems > 'Application Control'.
- **User rating** - Users can assign a trusted rating to a file in the CCS interface. There are two ways to do this:
  - Security alert - If an executable is unknown then it may generate a HIPS alert on the local endpoint. Users could choose 'Treat this as a Trusted Application' at the alert
  - File List - From the CCS home screen, click 'Settings' > 'File Rating' > 'File List'

CCS creates a hash of all files that a user classifies as 'Trusted'. So, even if the file name is changed it will keep its trust status because the hash remains same. This is particularly useful for developers creating new applications which, by their nature, are unknown to the Comodo.

**Malicious Files**
Files on the Comodo blacklist will be quarantined or deleted by CCS. These files are reported to Endpoint Manager as malware.

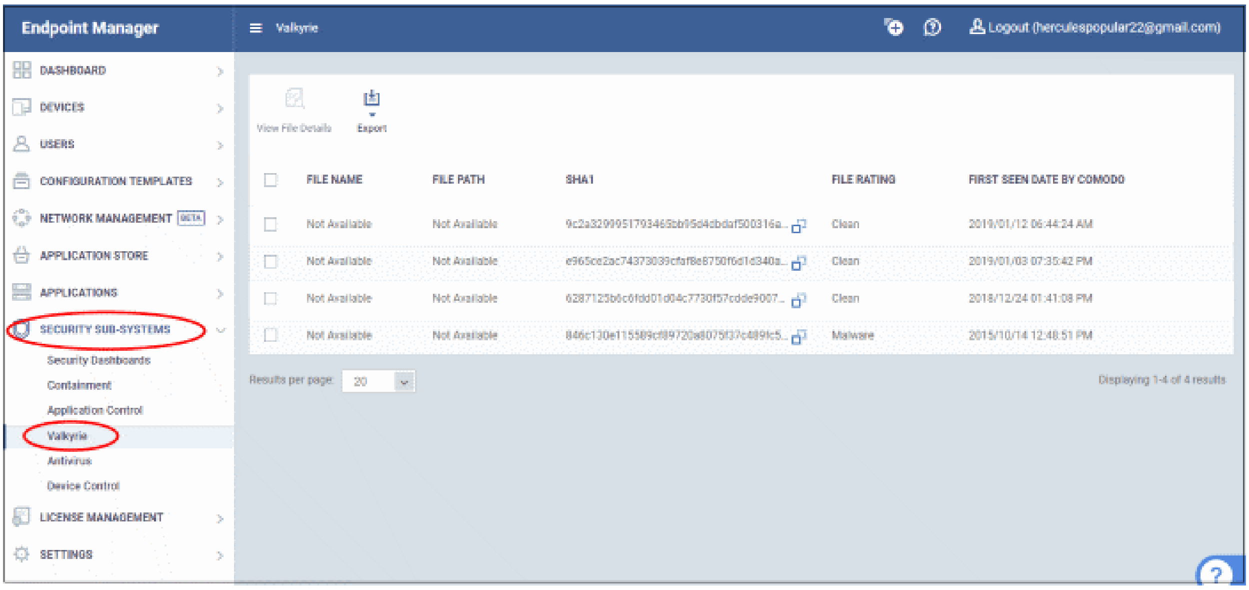
## 10.4. View List of Valkyrie Analyzed Files

- Click 'Security Sub-Systems' > 'Valkyrie'
- The 'Valkyrie' interface lists unknown files identified on all endpoints, along with their Valkyrie ratings.
  - Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks. The service helps Comodo establish whether an unknown file is malicious or safe.
  - You can configure Comodo Client Security on endpoints to automatically upload unknown files to Valkyrie.
- You can also view Valkyrie statistics by clicking 'Dashboard' > 'Valkyrie'.
- You can schedule the upload of unknown files in the 'Valkyrie' section of a Windows profile. See **Valkyrie Settings** if you need help with this.

**Note:** The version of Valkyrie that comes with the free version of Endpoint Manager is limited to the online testing service. The 'Premium' and 'Managed' versions of EM also includes manual file testing by Comodo research labs. This helps enterprises quickly create definitive whitelists of trusted files. Valkyrie is also available as a standalone service. Contact your Comodo account manager for further details.

**To open the 'Valkyrie' interface**

- Click 'Security Sub-Systems' > 'Valkyrie'



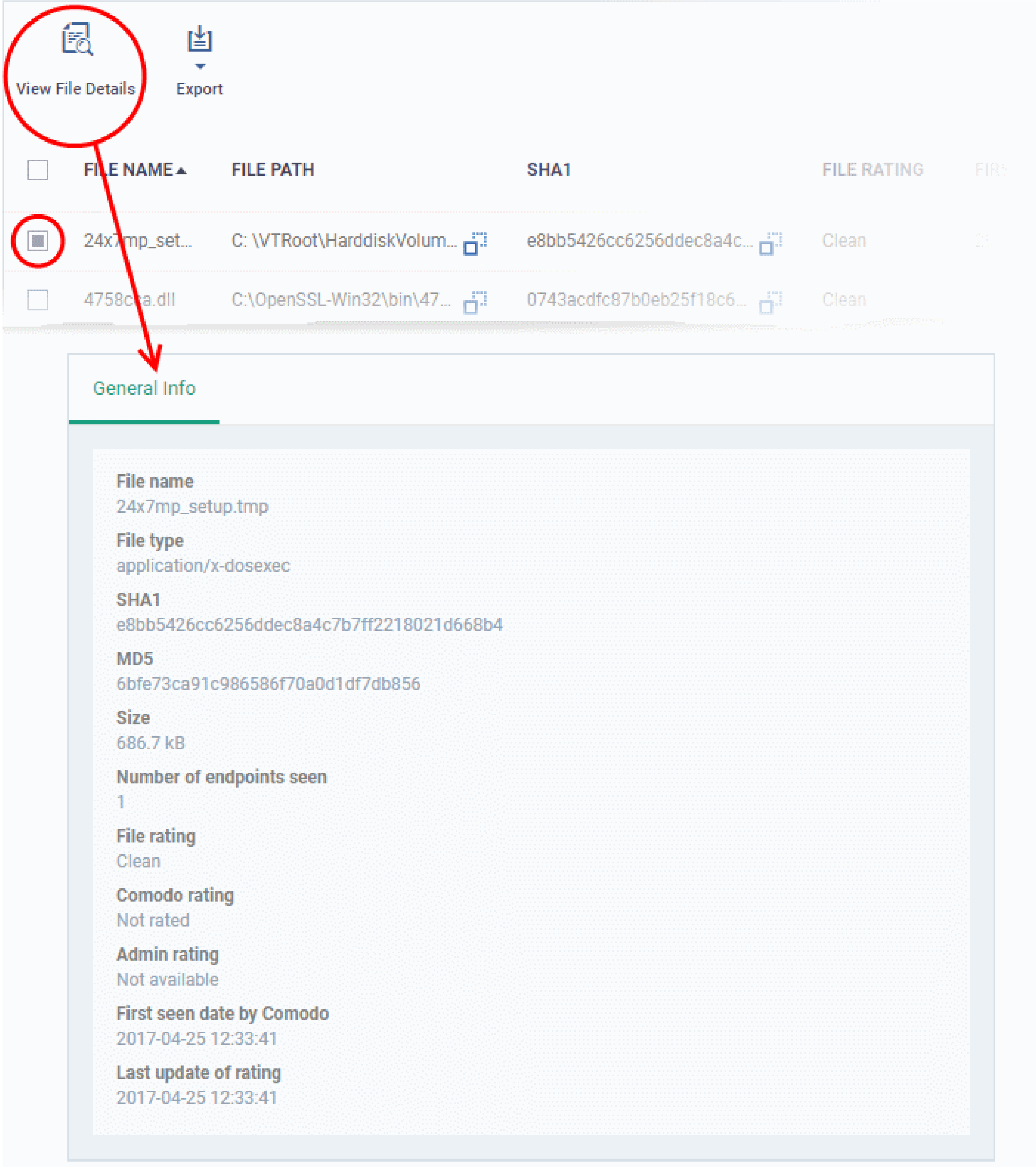
| □ | FILE NAME | FILE PATH | SHA1 | FILE RATING | FIRST SEEN DATE BY COMODO |
|---|---|---|---|---|---|
| □ | Not Available | Not Available | 9c2a3299951793465bb95d4cbdaf500316a... | Clean | 2019/01/12 06:44:24 AM |
| □ | Not Available | Not Available | e965ce2ac74373039cfaf8e8750f6d1d340a... | Clean | 2019/01/03 07:35:42 PM |
| □ | Not Available | Not Available | 6287123b6c6fdd01d04c7730f57cdde9007... | Clean | 2018/12/24 01:41:08 PM |
| □ | Not Available | Not Available | 846c130e115589cf89720a8075f37c489fc5... | Malware | 2015/10/14 12:48:51 PM |

| The 'Valkyrie' List - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of the unknown item |
| Path | The installation location of the file on the endpoint<br>• Click the ⧉ icon to copy the file path to the clipboard. |
| Hash | The SHA1 hash value of the unknown file<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| File Rating | The file's trust verdict from Valkyrie. The possible values are:<br>• Clean - The file is safe to run<br>• No Threat Found - No malware found in the file, but cannot say it is safe to run<br>• Malware - The file is malicious and should not be allowed to run.<br>• Potentially Unwanted Application - Applications such as adware, browser toolbars etc. These applications are often bundled as an 'extra utility' with freeware applications. Users might not be aware they are installed, or may not be aware of their full functionality. For example, a browser toolbar may also contain code that tracks a user's activity on the internet. |
| First Seen by Comodo | Date and time at which the file was first received by Valkyrie. |
| View File Details | Complete information about a selected item. See **View the details of files in the list** for more. |
| Export | Save the list of analyzed files as a comma separated values (csv) file. See **Export the List of Valkyrie Analyzed Files** for more details. |

## View the details of files in the list

Administrators can view complete details of files identified as 'Unknown' and uploaded to Valkyrie for analysis.

- Select a file and click the 'View File Details' button:



| ☐ | FILE NAME ▲ | FILE PATH | SHA1 | FILE RATING | FIRS |
|---|---|---|---|---|---|
| ▣ | 24x7mp_set... | C: \VTRoot\HarddiskVolum... | e8bb5426cc6256ddec8a4c... | Clean | |
| ☐ | 4758cca.dll | C:\OpenSSL-Win32\bin\47... | 0743acdfc87b0eb25f18c6... | Clean | |

General Info

File name
24x7mp_setup.tmp

File type
application/x-dosexec

SHA1
e8bb5426cc6256ddec8a4c7b7ff2218021d668b4

MD5
6bfe73ca91c986586f70a0d1df7db856

Size
686.7 kB

Number of endpoints seen
1

File rating
Clean

Comodo rating
Not rated

Admin rating
Not available

First seen date by Comodo
2017-04-25 12:33:41

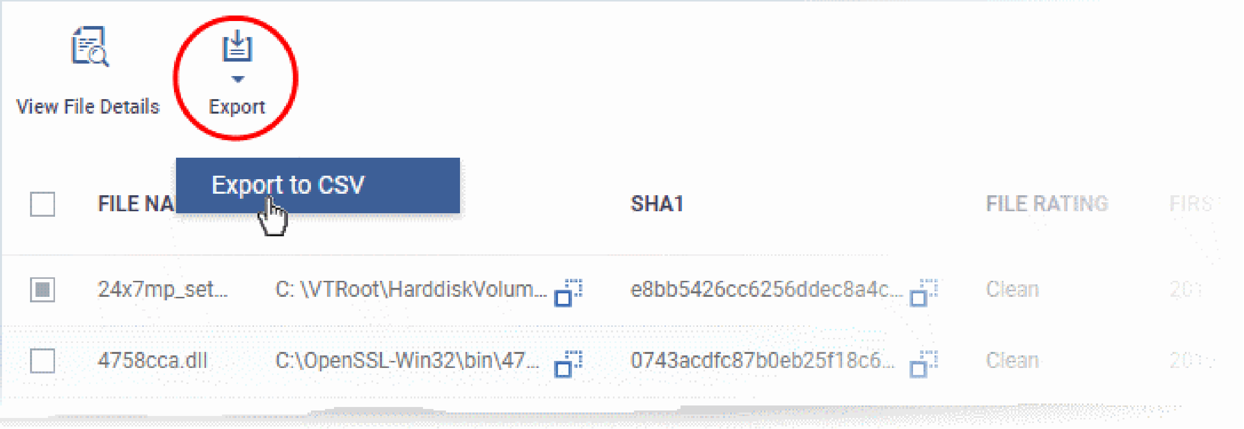
Last update of rating
2017-04-25 12:33:41

The 'General Info' screen displays file details like file name, installation path, file version, size, hash value and file ratings assigned by Comodo and by EM Administrator.

## Export the List of Valkyrie Analyzed Files

Export the list of files to a .csv file as follows:

- Click 'Security Sub-Systems' > 'Valkyrie'.
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | FILE NA | | SHA1 | FILE RATING | FIRS |
|---|---|---|---|---|---|
| ■ | 24x7mp_set... | C: \VTRoot\HarddiskVolum... | e8bb5426cc6256ddec8a4c... | Clean | 201 |
| □ | 4758cca.dll | C:\OpenSSL-Win32\bin\47... | 0743acdfc87b0eb25f18c6... | Clean | 201 |

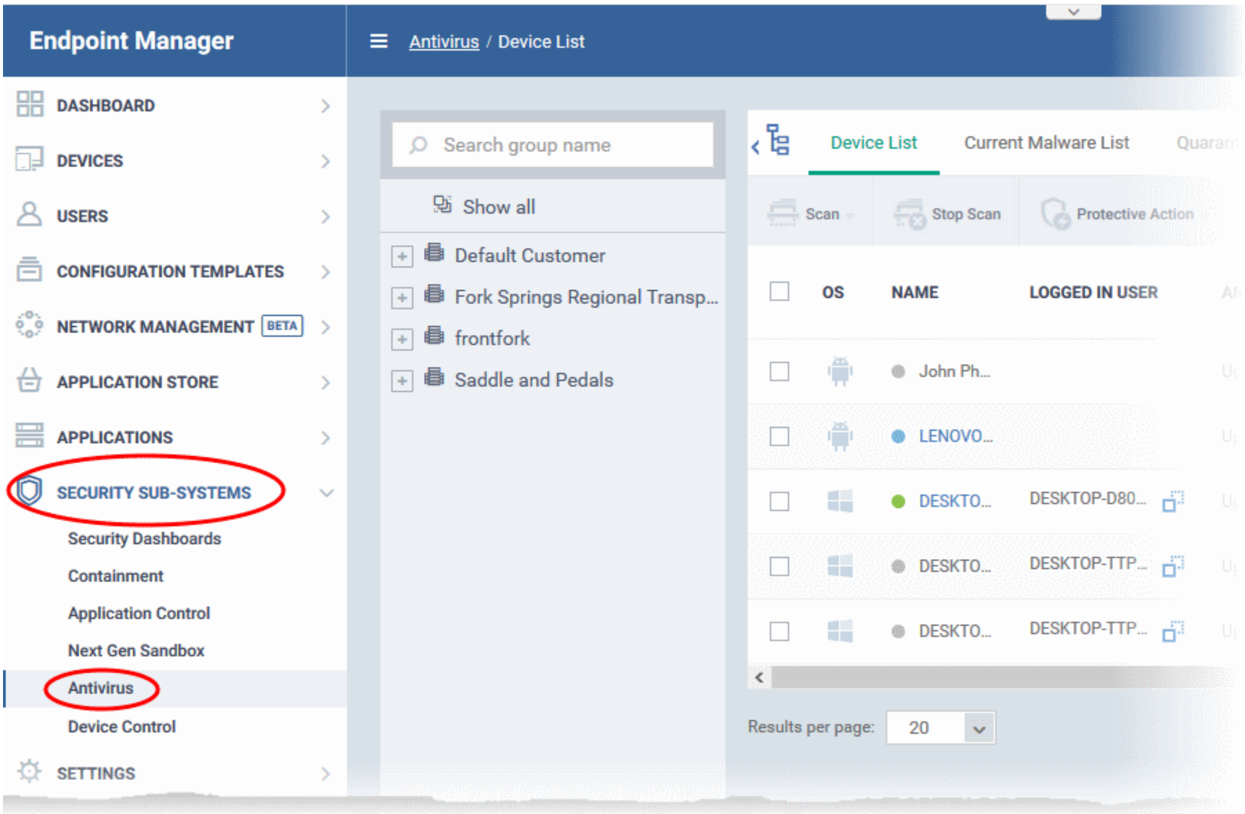
- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## 10.5. Antivirus and File Rating Scans

- Click 'Security Sub-systems' > 'Antivirus' to open this area.

This area allows you to:

- View the infection status of managed Windows, Mas OS, Linux and Android devices.
- Run antivirus and file rating scans on devices.
- View a consolidated list of all malware on all endpoints.
- View all quarantined files on Windows, Mac OS and Linux devices
- View an all-time history of threats discovered on all endpoints
- Manually delete, quarantine or ignore malicious files



| OS | NAME | LOGGED IN USER |
|---|---|---|
|  | John Ph... |  |
|  | LENOVO... |  |
|  | DESKTO... | DESKTOP-D80... |
|  | DESKTO... | DESKTOP-TTP... |
|  | DESKTO... | DESKTOP-TTP... |

The 'Antivirus' interface has five tabs:

- **Device List** - Shows the status of all managed devices with regards to antivirus health. The interface shows:
  - The date and type of the most recent virus scan
  - Whether or not the device is using the latest virus database
  - The malware status of the device (clean, infected or unknown)

  You can also run an on-demand scan on a device, and delete/quarantine/ignore threats.

  See **The Device List Interface** for more details.
- **Current Malware List** - Lists all unprocessed malware residing on managed devices. You can delete, ignore or quarantine specific pieces of malware on specific devices, or apply these actions to multiple threats at once. See **Viewing and Managing Identified Malware** for more details.
- **Quarantined Files** - Malware which has been quarantined by Comodo Client Security on Windows, Mac and Linux devices. You can delete or restore quarantined items, or assign a trust rating to items. See **View and Manage Quarantined Items** for more details.
- **Threat History** - A log of all malicious items found on Android, Windows, Mac OS and Linux devices over time. See **View Threat History** for more details.
- **Autorun Items** - List of files that tried to modify Windows services, auto-start entries or scheduled tasks. See **View and Manager Autorun Items** for more details.

## The Device List Interface

The 'Device List' screen displays the infection status of Android, Mac OS, Windows and Linux devices. From here you can:

- Run on-demand antivirus scans on selected devices
- Run file rating scans on Windows devices
- Choose the action to be taken on malware discovered by scans.
- Update the AV database on endpoints

- **Export device list data from the table**

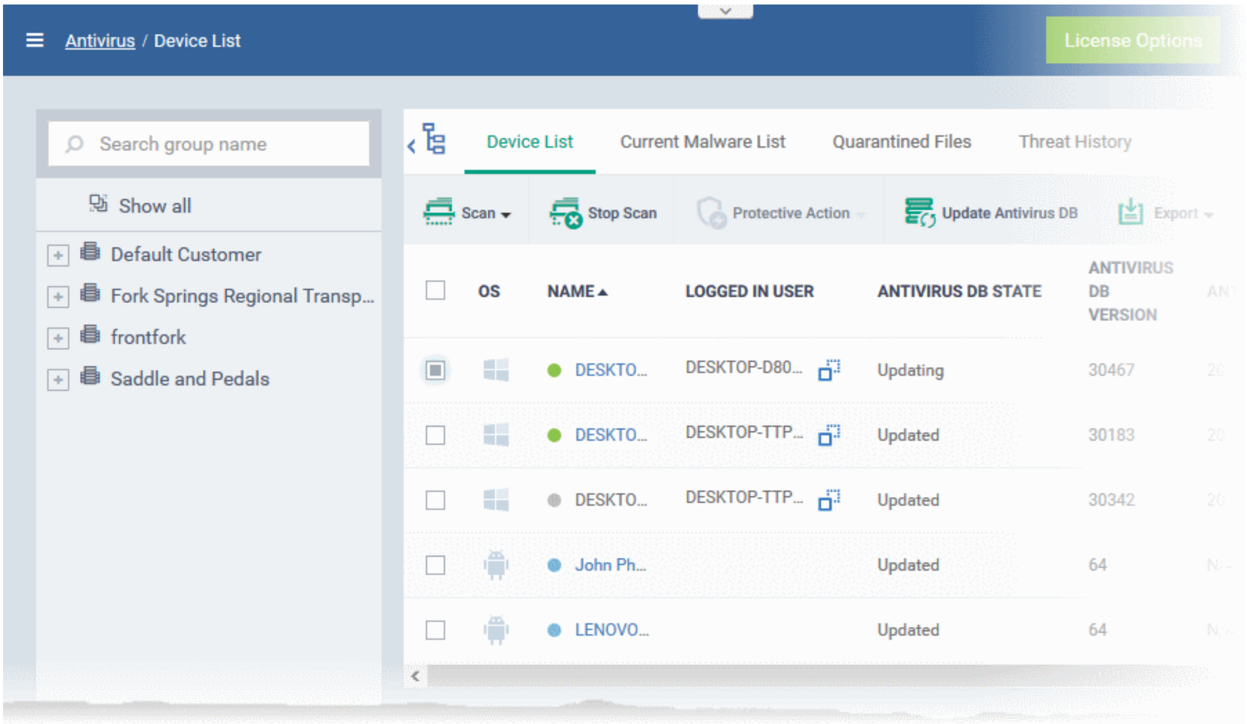
**Note**: You can run virus scans on specific areas of a device and setup ongoing, scheduled scans. These tasks are configured in the 'Antivirus' section of the device's configuration profile. See:

- **Windows** - see **Custom Scans** and **Create Windows Profiles**.
- **MAC** - see **Scan Profiles** and **Create a Mac OS Profile**.
- **Linux** - see **Create and Manage Scan Profiles** and **Create a Linux Profile**

**Open the 'Device List':**

- Click 'Security Sub-Systems' > 'Antivirus'
- Select the 'Device List' tab
- Select a company and group on the left to view all devices in it

  Or
- Select 'Show All' to view all devices enrolled to EM



| OS | NAME ▲ | LOGGED IN USER | ANTIVIRUS DB STATE | ANTIVIRUS DB VERSION |
|---|---|---|---|---|
| | DESKTO... | DESKTOP-D80... | Updating | 30467 |
| | DESKTO... | DESKTOP-TTP... | Updated | 30183 |
| | DESKTO... | DESKTOP-TTP... | Updated | 30342 |
| | John Ph... | | Updated | 64 |
| | LENOVO... | | Updated | 64 |

The list shows all Android, Windows, Mac OS and Linux devices along with their last scan details, infection status and antivirus database update state.

| Antivirus Device List - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the device. |
| Name | The label of the device on which the threat was found.<br>• If no name was assigned then the model number of the device is used.<br>• Gray text color shows the device has been offline for the past 24 hours.<br>• Click the name of the device to open its device details interface. |

| | |
|---|---|
| | • See **Manage Windows Devices**, **Manage Mac OS Devices**, **Manage Linux Devices** and **Manage Android / iOS Devices** for more details. |
| Logged in User | The name of the user currently signed-in to the device.<br>• The user name is prefixed with the active directory (AD) domain or workgroup that the user is currently logged-in to:<br>  ◦ Active Directory - Name is shown as <AD domain name>\<user name><br>  ◦ Workgroup - Name is shown as <workgroup name>\<user name><br>  ◦ No network - Name is shown as <device name>\<user name><br>• Click the ⧉ icon to copy the username to the clipboard. |
| Antivirus DB State | The update status of the virus signature database on the device. |
| Antivirus DB Version | The version number of the virus signature database on the device |
| Antivirus DB Date | The date and time at which the AV database was last updated |
| Run By | The source that initiated the last scan. An antivirus scan or a file rating scan can be initiated in the following ways:<br>• **Portal** - Manually run by an admin from the EM interface. See **Run Antivirus and/or File Rating Scans on Devices** for more details.<br>• **User** - Manually run by the end-user at the device itself.<br>• **Scheduled** - Automatically run as per the schedule defined in the configuration profiles effective on the device. |
| Scan Type | Indicates the kind of the last scan ran on the device. The possible types of scan are:<br>• Antivirus Full Scan - Applies to Windows, Mac OS and Android devices.<br>• Antivirus Quick Scan - Applies to Windows, Mac OS and Android devices.<br>• File Rating Quick Scan - Applies only to Windows devices.<br>• Custom Scan - Applies to Windows and Mac OS devices.<br>• Manual Scan - Applies to Windows and Mac OS devices<br>• SD Card Scan - Applies only to Android devices. |
| Scan State | Status of the last scan run on the device. Possible states are:<br>• Not scanned yet<br>• Complete<br>• Scanning<br>• Failed<br>• Viruses found<br>• Canceled<br>• Command sent |
| Scan Date | The date and time at which the last scan was run. |
| Malware Status | The infection status of the device.<br>• Devices with untreated malware are listed as 'Infected'.<br>• Click the 'Infected' link to view a list of malware on all managed devices.<br>  ◦ You can remove, quarantine or ignore the malware direct from this list. |

| | |
|---|---|
| | • See **View and Manage Identified Malware** if you want more help on this.<br>• Alternatively, you can also view/manage malware from the device details screen. Click "Security Sub-Systems' > 'Antivirus' > 'Device List'. See **Handle Malware on Scanned Devices** for more details. |
| **Controls** | |
| Scan | Run a manual scan on selected devices. See **Run Antivirus and/or File Rating Scans on Devices** for more details. |
| Stop Scan | Terminate any type of on-going scans on selected devices. This includes on-demand scans run from the EM console, scheduled scans run by the security profiles active on the device and any on-demand scan run by the local user from the Comodo Client - Security (CCS) application on the device.<br>See **Run Antivirus and/or File Rating Scans on Devices** for more details. |
| Protective Action | Remove, quarantine or ignore threats found on infected devices. See **Handle Malware on Scanned Devices** for more details. |
| Update Antivirus DB | Manually run a virus signature update on selected devices. See **Update virus signature database on Windows, Mac OS and Linux Devices** for more details. |
| Export | Save the device list, including current statuses, as a .csv file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of Devices** for more details. |

The 'Antivirus' > 'Device List' interface allows you to:

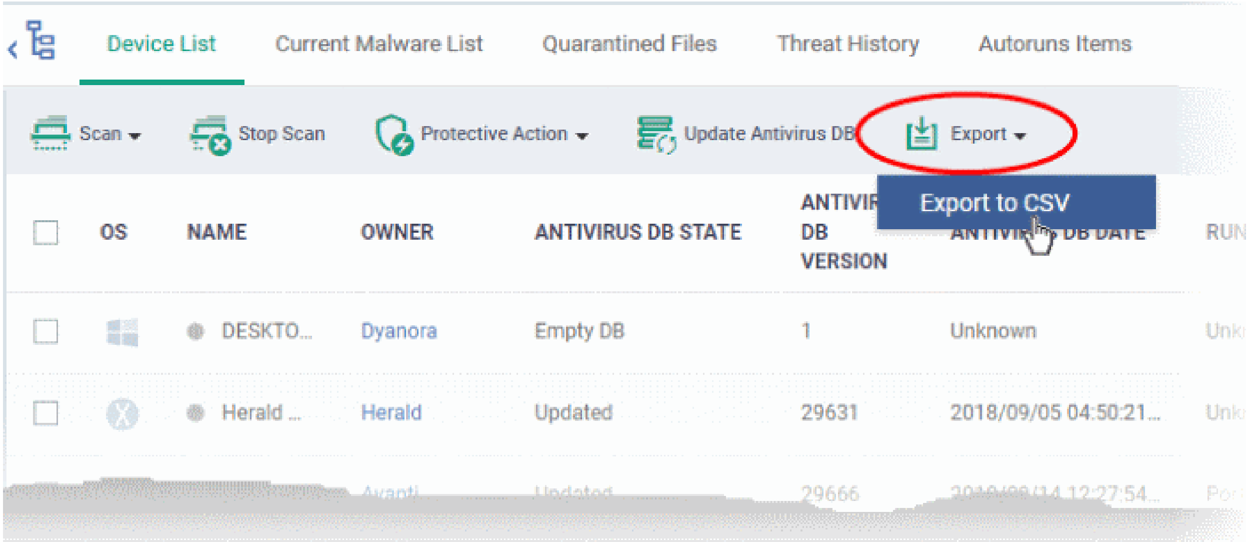
- **Run Antivirus and/or File Rating Scans on Devices**
- **Handle Malware on Scanned Devices**
- **Update virus signature database on Windows, Mac OS and Linux Devices**

## Sorting, Search and Filter Options

- Click any column header except 'Antivirus DB version' to sort items in ascending/descending order
- Click the funnel icon on the right to filter items by various criteria.
  - Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
  - To display all items again, clear any filters and search criteria and click 'Apply'.
- EM returns 20 results per page when you perform a search. Click the arrow next to the 'Results per page' drop-down to increase results up to a maximum of 200.
- Use the left and right arrows and the page numbers to navigate to the page you want to view.

## Export device list records as a CSV file

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List'
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| | OS | NAME | OWNER | ANTIVIRUS DB STATE | ANTIVIRUS DB VERSION | ANTIVIRUS DB DATE | RUN |
|---|---|---|---|---|---|---|---|
| □ | | DESKTO... | Dyanora | Empty DB | 1 | Unknown | Unk |
| □ | | Herald ... | Herald | Updated | 29631 | 2018/09/05 04:50:21... | Unk |
| | | | Avanti | Updated | 29666 | 2018/09/14 12:27:54... | Por |

- The .csv file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

### 10.5.1. Run Antivirus and/or File Rating Scans on Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List'.
- The interface lets you run virus and file rating scans on Android, Mac OS, Windows and Linux devices.

**Note**: The scans interface lets you manage on-demand scans only. For automated scans, please create a scan schedule in a configuration profile then push it to selected devices/groups. See **Create Configuration Profiles** for more details.

**To launch an on-demand scan**

- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Device List' tab
  - Select a company or a group to view their devices

    Or
  - Select 'Show All' to view all devices enrolled to EM
- Select the devices you wish to scan
- Choose a scan type from the 'Scan' drop-down
- The scan command will sent to the target devices and the scan will commence immediately

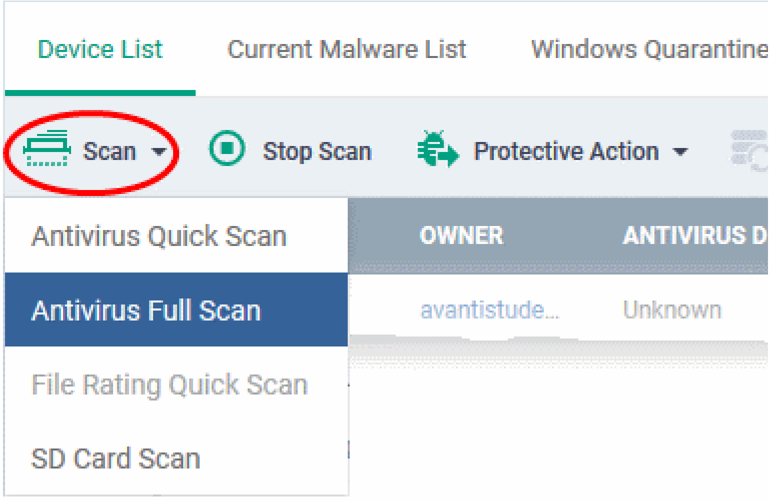
**Tip**: You can access filters by clicking the funnel icon at the top right. For example, you may want to display only devices with Last Scan States of 'Unknown', 'Scan Failed' and 'Scan Canceled'.

The scan types available depend on the OS of the selected device(s). The scan type defines the areas to be scanned on the selected device(s). The following sections explain the scan process for:

  - **Android Devices** (Quick Scan, Full Scan, SD Card Scan)
  - **Windows Devices** (Quick Scan, Full Scan, File Rating Quick Scan)
  - **Mac OS Devices** (Quick Scan, Full Scan)
  - **Linux Devices** (Quick Scan, Full Scan)

## Android Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

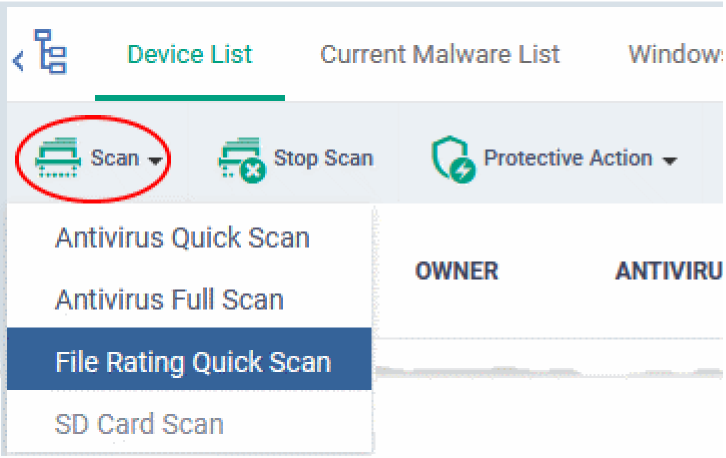
- **Antivirus Quick Scan -** Scans critical areas of the device which are highly prone to attack from viruses, rootkits and other malware. Areas scanned include RAM, hidden services and other significant areas like system files. These areas are of great importance to the health of the device so it is essential to keep them free of infection.
- **Antivirus Full Scan -** Scans all folders/files in both the system internal memory and the SD card.
- **SD Card Scan -** Scans all folders/files in the Secure Digital (SD) memory card mounted on the device.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

- If you want to terminate the scan, choose the devices and click 'Stop Scan' from the options at the top.
- If malware is found after the scan then the 'Last Scan State' will say 'Infected'. Infections identified after the scan will be treated according to settings in 'Settings' > 'Portal Set-Up' >Android Client Configuration' > 'Antivirus'. See **Configure Android Client Antivirus Settings** for more details.
- If 'Manual control' is chosen, then you have the option to uninstall or ignore from the 'Current Malware List'. See **View and Manage Identified Malware** for more details.
- You can also choose to uninstall or ignore the identified malware by clicking the respective buttons at the top. See **Handle Malware Identified from Scanned devices** section for more details.

## Windows Devices

- Click 'Scan Device' and choose the 'Scan type/Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan types/profiles are:

- **Antivirus Quick Scan** - Scans critical areas of the device which are highly prone to attack from viruses, rootkits and other malware. Areas scanned include. Areas scanned include include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of each computer so it is essential to keep them free of infection.
- **Antivirus Full Scan** - Scans every local drive, folder and file on each computer. Any external devices like USB drives, digital camera and so on are also scanned.
- **File Rating Quick Scan** - Runs a cloud-based assessment of files on the device to determine the trust rating of each file. The 'Quick' rating scan checks commonly infected areas and memory.

Files are rated as:

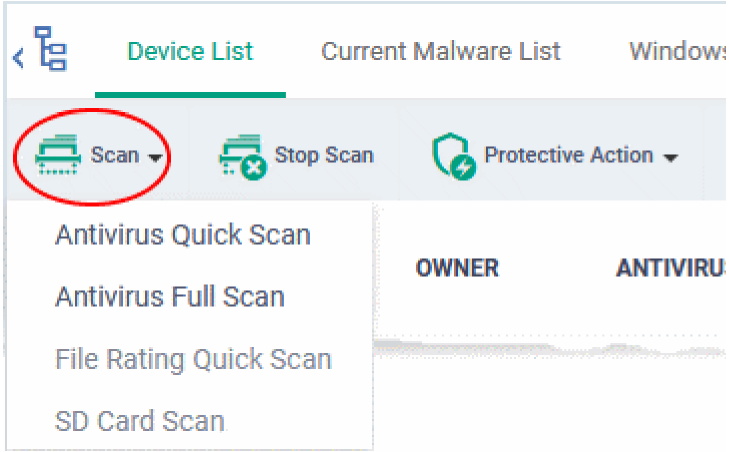
- **Trusted** - the file is safe
- **Unknown** - the trustworthiness of the file could not be assessed
- **Bad** - the file is unsafe and may contain malicious code

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Scan State' column for each device.

- If you want to terminate the scanning on selected devices, choose the devices and click 'Stop Scan' from the options at the top.
- If malware is found on completion of scan the Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. See **Handle Malware Identified from Scanned devices** for more details.
- Items moved to quarantine are encrypted and saved in the endpoint itself, so that they are isolated from the rest of the system.
- You view the quarantined items from the 'Quarantine' interface. The Quarantine interface allows you to:
  - Delete an item, if it is identified as malicious
  - Restore the file to its original location on the endpoint if the item is a false-positive. You can also rate a file as 'Trusted' to restore it to the endpoint. Doing so will effectively white-list the file by giving it a 'Trusted' rating in the local CCS database.
- See **View and Manage Quarantined Items** for more details.

## Mac OS Devices

- Click 'Scan Device' and choose the 'Scan Profile' from the drop-down to select the area to be scanned on the device.



The available scan profiles are:

- **Antivirus Quick Scan** - Scans important operating system files and folders including system memory, auto-run entries, hidden services.

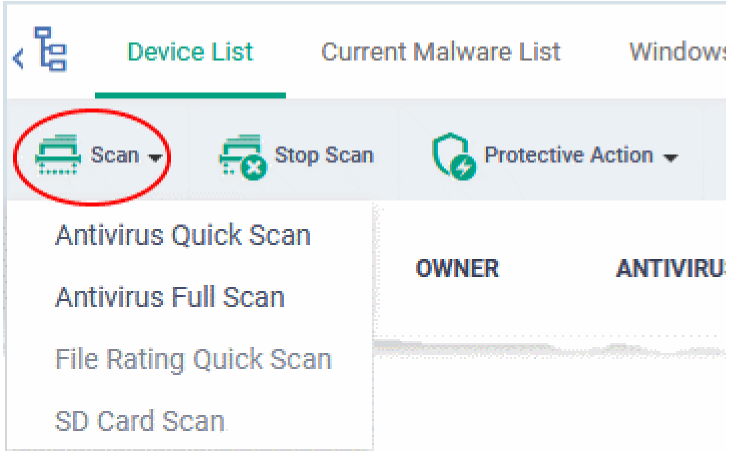
- **Antivirus Full Scan -** Scans every local drive, folder and file on your system including external devices, storage drives, digital cameras.

The scan command will be sent to the selected device(s) and the scan status will be displayed in the 'Last Scan State' column for each device.

- If you want to terminate the scan on certain devices, choose the devices and click 'Stop Scan' from the options at the top.
- If malware is found on completion of scan the Last Scan State will indicate 'Viruses Found'. You can choose to uninstall, ignore, delete the identified malware or to move them to quarantine at the endpoint for later analysis. See **Handle Malware Identified from Scanned devices** for more details.
- Items moved to quarantine are encrypted and saved in the device itself, so that they are isolated from the rest of the system.
- You view the quarantined items from the 'Quarantine' interface. The Quarantine interface allows you to:
  - Delete an item, if it is identified as malicious
  - Restore the file to its original location on the endpoint if the item is a false-positive.
- See **View and Manage Quarantined Items** for more details.

## Linux Devices

- Click 'Scan Device' and choose the scan type from the drop-down menu:



- **Antivirus Quick Scan -** Scans important areas which are frequently targeted by malware. Areas scanned include system memory, important registry keys, auto-run entries, operating system folders and hidden services.
- **Antivirus Full Scan -** Scans every local drive, folder and file on your system. Connected devices like USB sticks and external drives are also scanned.

The status of current, or previous, scans is shown in the 'Last Scan State' column.

- **Terminate a scan -** Select target devices then click 'Stop Scan' from the options at the top.
- **'Viruses Found' -** You can uninstall, ignore, quarantine or delete the identified malware. See **Handle Malware Identified on Scanned devices** for more details.

## 10.5.2. Handle Malware on Scanned Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List'
- Click the 'Protective Action' button to remove, ignore or quarantine the malware.

**Note**:

- This interface lets you apply actions to all malware found on specific devices.
- If you instead want to apply actions to individual malware, please use the 'Current Malware List'.

- Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List'.
- See **View and Manage Identified Malware** if you need more help with this interface.

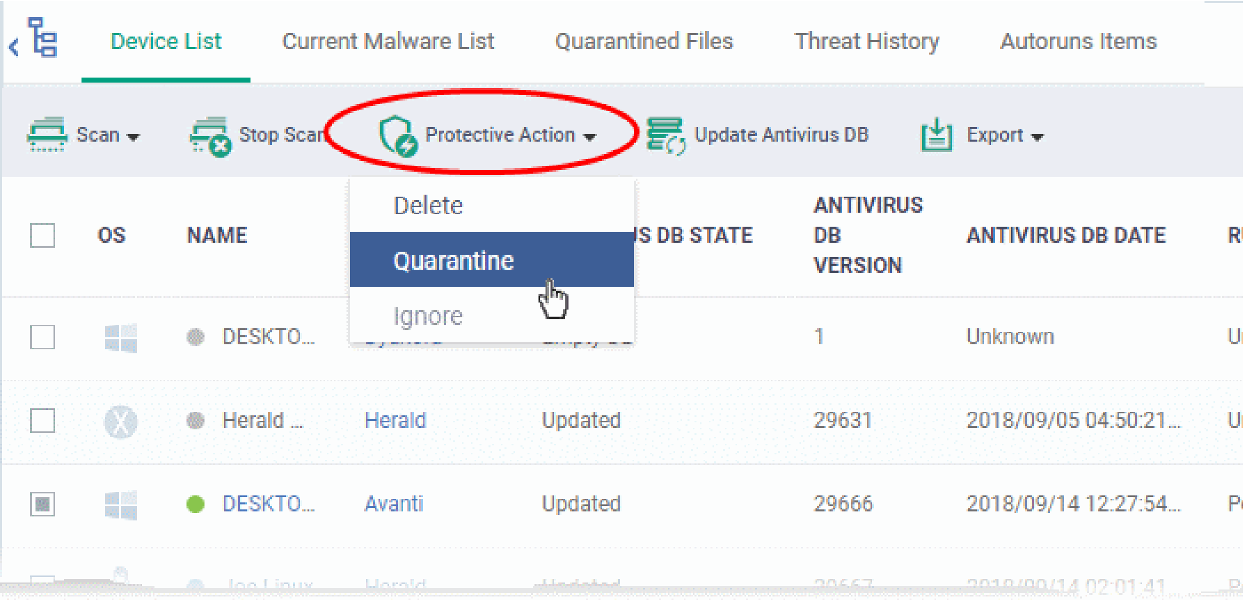
**Apply actions to ALL malware on selected devices**

- Click 'Security Sub-Systems' > 'Antivirus'
- Click the 'Device List' tab
    - Click a company name/group on the left to view their devices

      Or
    - Select 'Show All' on the left menu to view every device enrolled to EM
- Select device(s) with a malware status of 'Infected' using the check-box(es) on the left.

**Tip**: You can filter the list to search for specific devices by clicking the funnel icon at the top right of the table.

- Click 'Protective Action' above the table and select your desired action:



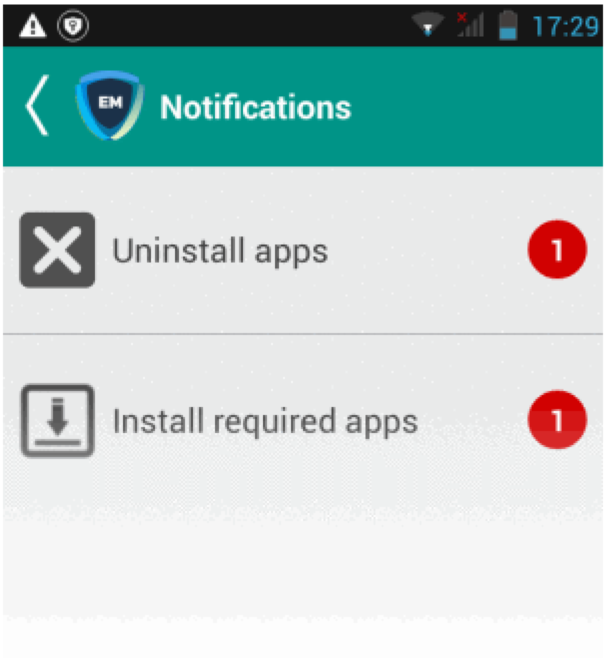
| ☐ | OS | NAME | | IS DB STATE | ANTIVIRUS DB VERSION | ANTIVIRUS DB DATE | R |
|---|---|---|---|---|---|---|---|
| ☐ | | ● DESKTO... | | | 1 | Unknown | U |
| ☐ | | ● Herald ... | Herald | Updated | 29631 | 2018/09/05 04:50:21... | U |
| ☒ | | ● DESKTO... | Avanti | Updated | 29666 | 2018/09/14 12:27:54... | P |
| ☐ | | ● Joe Linux | Herald | Updated | 29667 | 2018/09/14 02:01:41 | P |

The actions available depend on the OS of the device chosen:

**For Android Devices:**

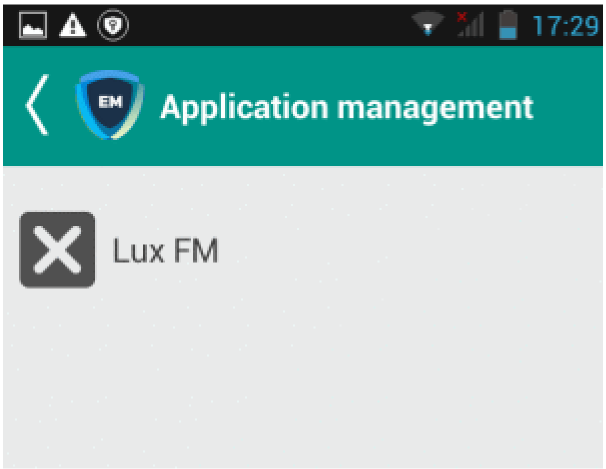
- **Delete** - Removes the malicious app
- **Ignore** - Ignores malware found by the last scan. The item will be identified as malware again on the next scan.

For the 'Delete' operation, a notification will be sent to the selected devices to uninstall the apps:

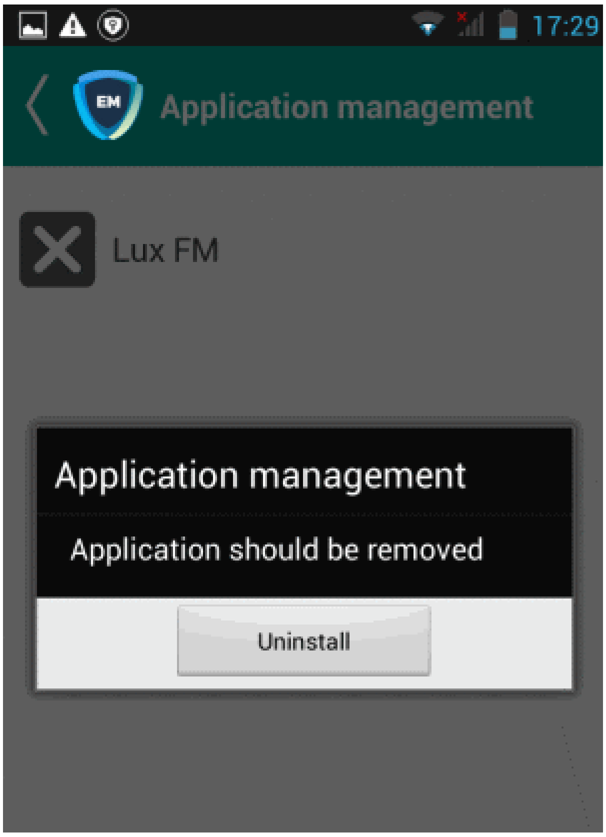


The notification shows the number of threats which will be removed from the device.

- Touch the alert to view all items which are ready for removal.



- Tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



Application management

Application should be removed

**For Windows. Mac OS and Linux Devices**

- **Delete -** Instructs CCS on the endpoint to clean the malware.
    - If a disinfection routine is available, CCS will disinfect it and retain the original file.
    - If a disinfection routine is not available, CCS will delete the application.
- **Quarantine** - Moves the malware to quarantine on the device.
    - Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files' to manage quarantined files.
    - Based on their trustworthiness, you can remove them from the device or restore them to their original locations. See **View and Manage Quarantined Items** for more details.

### 10.5.3. Update Virus Signature Database on Windows, Mac OS and Linux Devices

- Click 'Security Sub-Systems' > 'Antivirus' > 'Device List'
- Select a device using the check-boxes on the left > Click the 'Update Antivirus DB' button
- You can update the database manually or according to a schedule.

**Automatic Updates**

- **Windows devices** - Configure the 'Update' component of the Windows profile applied to a device. See **Client Security Update** in **Creating Windows Profiles** for more details.
- **MAC OS devices** - Configure the 'Antivirus' component of the Mac OS profile applied to a device. See **Configure Antivirus Settings** in **Antivirus Settings for Mac OS Profile** for more details.
- **Linux devices** - Configure the 'Antivirus' component of the Linux profile applied to a device. See **Antivirus Settings for Linux Profile** for more details.

**Manual Updates**

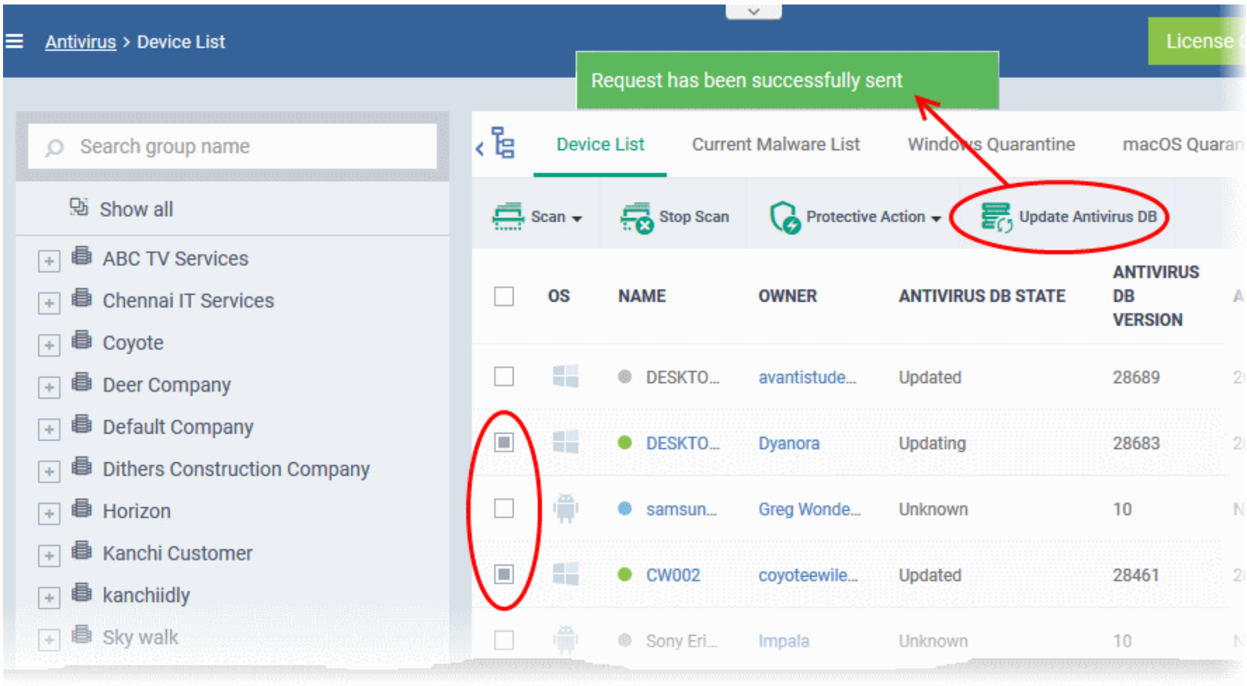
- Click 'Security Sub-Systems' on the left then select 'Antivirus'
- Click the 'Device List' tab

- Click a company or a group to view only their devices
  Or
- Select 'Show All' to view every device enrolled to EM

- Select the Windows, Mac OS and/or Linux device(s) on which you wish to update the virus database

**Tip**: You can filter the list or search for specific device(s) by clicking the funnel icon at the top right of the table.

- Click 'Update Antivirus DB' from the options at the top:



Request has been successfully sent

| | OS | NAME | OWNER | ANTIVIRUS DB STATE | ANTIVIRUS DB VERSION | A |
|---|---|---|---|---|---|---|
| □ | | DESKTO... | avantistude... | Updated | 28689 | 2 |
| ☑ | | DESKTO... | Dyanora | Updating | 28683 | 2 |
| □ | | samsun... | Greg Wonde... | Unknown | 10 | N |
| ☑ | | CW002 | coyoteewile... | Updated | 28461 | 2 |
| □ | | Sony Eri... | Impala | Unknown | 10 | N |

A command will be sent to target devices to start downloading the updates.

## 10.6. View and Manage Identified Malware

- Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List'
- The 'Current Malware List' shows malicious items on which no action has yet been taken.
- You can use this interface to clean (delete), ignore, or quarantine the items.
- You can also assign a 'Trusted' rating to an item. Use this option if you think the item is a false positive. The item will not be flagged by future scans.

**Background.** This box explains the conditions under which a file will appear in the current malware list.

**Windows Devices:**

**Real-time virus monitor**:

- Threats are shown in the list if:
  - 'Show antivirus alerts' is disabled and 'Block Threats' is chosen as the default action in the profile active on the device
    OR
  - 'Show antivirus alerts' is enabled and the user decides to block the threat at an alert.

- Threats are NOT shown in the list if:
    - 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action

      OR
    - 'Show antivirus alerts' is enabled and the user quarantines the threat at an alert.
- To view the settings above:
    - Click 'Configuration Templates' > 'Profiles' > *Click the name of any Windows profile* > 'Antivirus' tab > Open the 'Realtime Scan' tab.
- See **Realtime Scan settings** in **Antivirus Settings** if you need more help with this.

**Scheduled and manual scans**:

- Threats are shown in the list only if 'Automatically clean threats' is disabled in the profile active on the device.
- To view the setting above:
    - Click 'Configuration Templates' > 'Profiles' > *Click the name of any Windows profile* > 'Antivirus' tab > 'Scans' tab > Click the 'Edit' icon beside a profile > Click the 'Options' bar.
- See **Custom Scans** in **Antivirus Settings** if you need more help with this.

### Mac OS Devices:

- Threats only appear in this list if 'Auto-Quarantine' is disabled in the profile on the device.
- Threats will NOT appear in this list if:
    - 'Auto quarantine' is enabled in 'Realtime scanning', 'Manual Scanning' and 'Scheduled Scanning'
    - 'Auto quarantine' is disabled but the user chooses to quarantine the item from an alert
- See **Configure Antivirus Settings** in **Antivirus Settings for Mac OS Profile** under **Create a Mac OS Profile** for more details.

### Linux Devices:

- Threats only appear in this list if 'Auto-Quarantine' is disabled in the profile on the device.
- Threats will NOT appear in this list if:
    - 'Auto quarantine' is enabled in 'Realtime scanning' and 'Scheduled Scanning'
    - 'Auto quarantine' is disabled but the user chooses to quarantine the item from an alert
- See '**Configure Scanner Settings for CCS for Linux**' in **Antivirus Settings for Linux Profile** in **Create a Linux Profile** for more details.

### Android Devices:

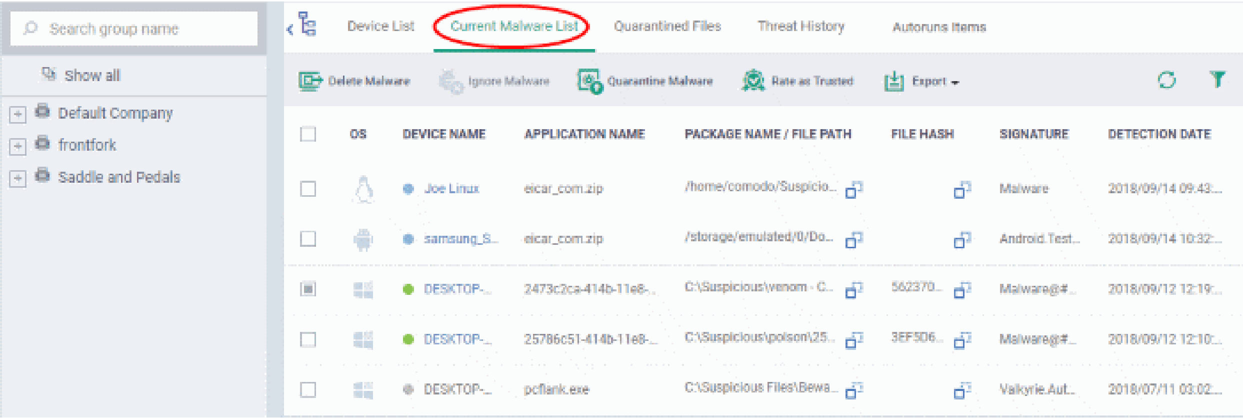
- Threats are shown in the list if the threat is ignored on the device. This can be because:
    - 'Manual control' is selected in Android client antivirus settings, or
    - 'Automatic response' is selected with 'Ignore' as the response in Android client antivirus settings.
- To view the settings above:
    - Click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'Android' > 'Antivirus'
    - **Click here** for more information on this setting

**View the malware list**

- Click 'Security Sub-Systems' > 'Antivirus'
- Click the 'Current Malware List' tab
    - Click a company or a group to view malware identified on their devices

      Or

- Select 'Show All' to view malware identified on every device in EM



| | OS | DEVICE NAME | APPLICATION NAME | PACKAGE NAME / FILE PATH | FILE HASH | SIGNATURE | DETECTION DATE |
|---|---|---|---|---|---|---|---|
| □ | | Joe Linux | eicar_com.zip | /home/comodo/Suspicio... | | Malware | 2018/09/14 09:43:... |
| □ | | samsung_S... | eicar_com.zip | /storage/emulated/0/Do... | | Android.Test... | 2018/09/14 10:32:... |
| ▣ | | DESKTOP-... | 2473c2ca-414b-11e8-... | C:\Suspicious\venom - C... | 562370... | Malware@#... | 2018/09/12 12:19:... |
| □ | | DESKTOP-... | 25786c51-414b-11e8-... | C:\Suspicious\poison\25... | 3EF5D6... | Malware@#... | 2018/09/12 12:10:... |
| □ | | DESKTOP-... | pcflank.exe | C:\Suspicious Files\Bewa... | | Valkyrie.Aut... | 2018/07/11 03:02:... |

| Current Malware List - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the device on which the malware was identified. |
| Device Name | The label of the device on which threats were found.<br>If no name was assigned then the model number of the device is used.<br>Gray text color shows the device has been offline for the past 24 hours.<br>• Click the name of the device to open its device details interface.<br>• See **Manage Windows Devices**, **Manage Mac OS Devices**, **Manage Linux Devices** and **Manage Android / iOS Devices** for more details. |
| Application Name | The label of the infected file. |
| Package Name / File Path | Windows, Linux and Mac OS devices - Shows the location of the malware<br>Android devices - Shows the package name or identifier.<br>• Click the ⧉ icon to copy the package name/ file path to the clipboard. |
| File Hash | The SHA1 hash value of the file.<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Signature | The malware signature.<br>• Signatures enable the scanner to identify viruses. Each malware signature represents a snippet of malicious code unique to a virus.<br>• The signatures of known-malware are stored in the local antivirus database. This is also known as the 'blacklist'.<br>• If the scanner finds a file with a signature that matches one on the blacklist then it raises a virus alert. |
| Detection Date | Date and time that the malware was discovered. |
| **Controls** | |

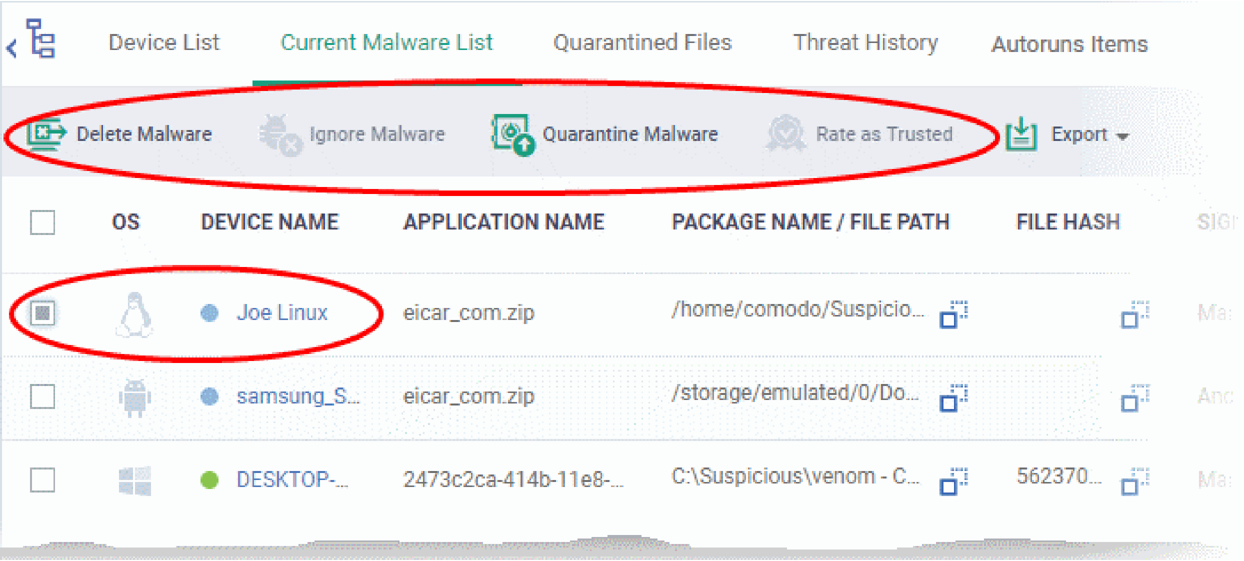
| | |
|---|---|
| Delete Malware | Uninstalls/removes the malware infected item from the device.<br>• Applies to items identified from devices of all operating systems. |
| Ignore Malware | The item will be allowed to remain on the device.<br>• Applies to items identified from Android devices only. |
| Quarantine Malware | Moves the selected items to quarantine on the respective devices.<br>• Applies to items identified from Windows, Mac OS and Linux devices. |
| Rate as Trusted | Awards 'Trusted' file rating to the selected items. Please make sure before marking a file as trusted. Use this option only for false positives and genuine items.<br>• Applies only to items identified from Windows devices. |
| Export | Save the list of currently displayed threats as a comma separated values (CSV) file.<br>The exported .csv is available in 'Dashboard' > 'Reports'<br>See **Export the List of Malware** for more details. |

- Click any column header to sort items in ascending/descending order.
- Click the funnel icon on the right to filter items by various criteria.
  - Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
  - To display all items again, clear any filters and search criteria and click 'Apply'.
- EM returns 20 results per page when you perform a search. You can increase results up to a maximum of 200.

## Take Actions on Identified Malware

- You can uninstall/delete malicious items from the devices on which they were found.
- Alternatively, if you think an item is a false positive, you have the following options:
  - Ignore malware - Applies to items identified on Android devices only. The item will not be uninstalled and will be skipped in the future scans.
  - Rate as 'Trusted' - Applies to items identified on Windows devices only. The item will be allowed to run and will be skipped in future scans.
- If an item is found to be suspicious, you can choose to move it to quarantine for later analysis and removal.

The options at the top of the table let you take actions on selected items. The available actions depend on the operating system of the device(s).



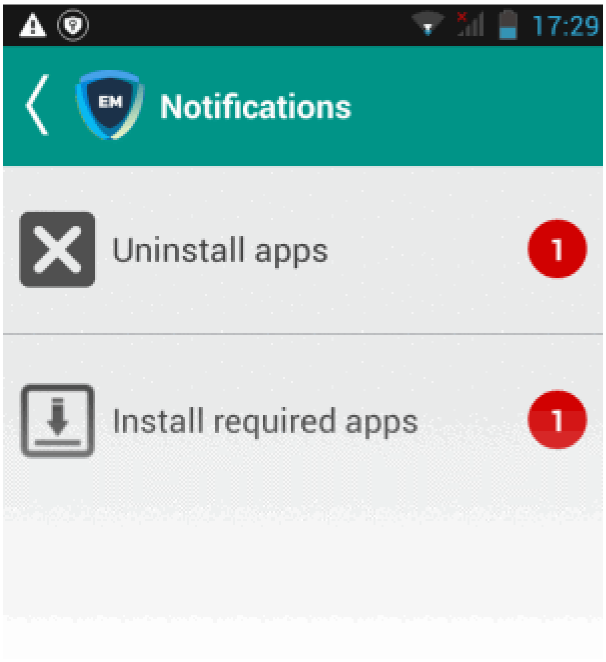
| ☐ | OS | DEVICE NAME | APPLICATION NAME | PACKAGE NAME / FILE PATH | FILE HASH | SIGI |
|---|---|---|---|---|---|---|
| ☒ | | Joe Linux | eicar_com.zip | /home/comodo/Suspicio... | | Ma |
| ☐ | | samsung_S... | eicar_com.zip | /storage/emulated/0/Do... | | Anc |
| ☐ | | DESKTOP-... | 2473c2ca-414b-11e8-... | C:\Suspicious\venom - C... | 562370... | Ma |

**Threats identified on Android Devices**

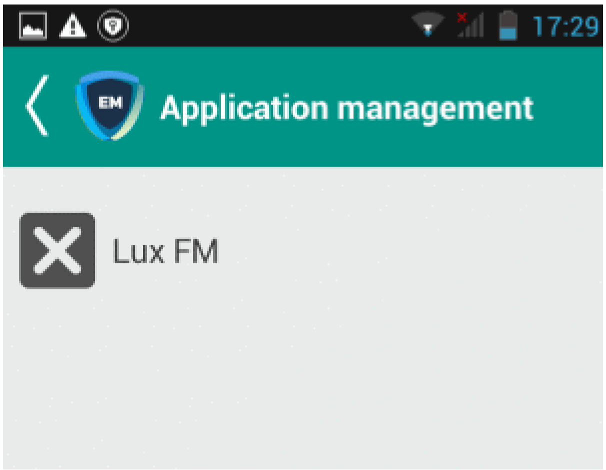
Action on malware depends on the Android device type. Knox and non-Knox devices. Knox is a security technology used by Samsung for its devices.

First, select the items on which you want to take the action. Then click one of the following:

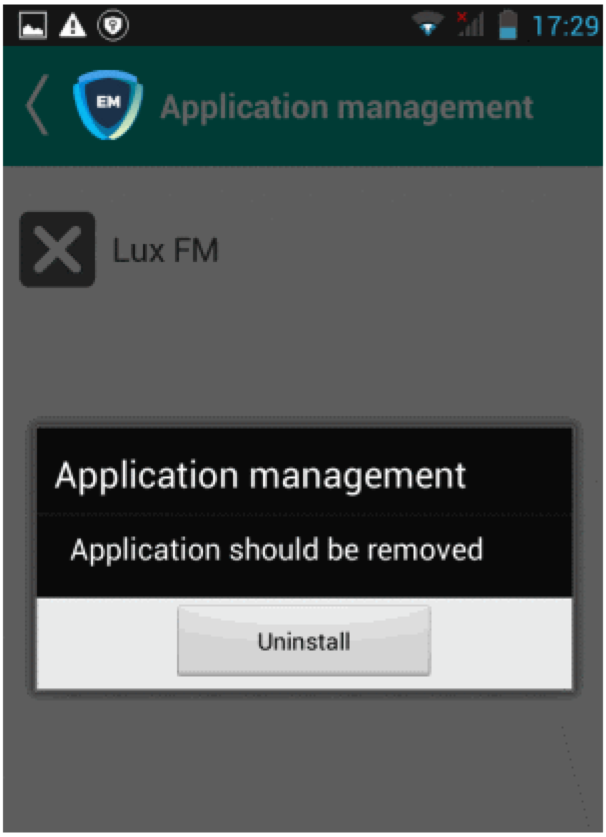
- **Ignore Malware** - Select if the item is a false positive. The item will remain on the device and skipped in future scans.
- **Delete Malware** - Select if you want to remove the malware from the device.
  - Knox devices - Applications with viruses or infected files on the devices and from the SD card are deleted without any alert on the device.
  - Non-Knox devices - Infected files on the SD card are deleted without any alert. The following notification is sent to the affected device for removal of malware on the device.



- Touch the alert to view a list of all items which are ready to be removed:



- Tap on the malware to be removed, confirm the removal in the next dialog and follow the uninstall wizard.



**Threats identified on Windows Devices:**

First, select the items on which you want to take the action. Then click one of the following:

- **Delete Malware** - Will remove the malware from the device.
- **Quarantine Malware** - The items will be moved to quarantine on the respective devices. You can delete the items from quarantine later, or restore them to their original locations. See **View and Manage Quarantined Items** for more details.
- **Rate as Trusted** - Trusted files are considered safe to run. Trusted items can run outside the container on devices and will be skipped in future scans. See **File Ratings Explained** for more details on trust ratings of files.

**Threats identified on Mac OS Devices:**

First, select the items on which you want to take the action. Then click one of the following:

- **Delete Malware** - Will remove the malware from the device.
- **Quarantine Malware** - The items will be moved to quarantine on the respective devices. You can delete the items from quarantine later, or restore them to their original locations. See **View and Manage Quarantined Items** for more details.

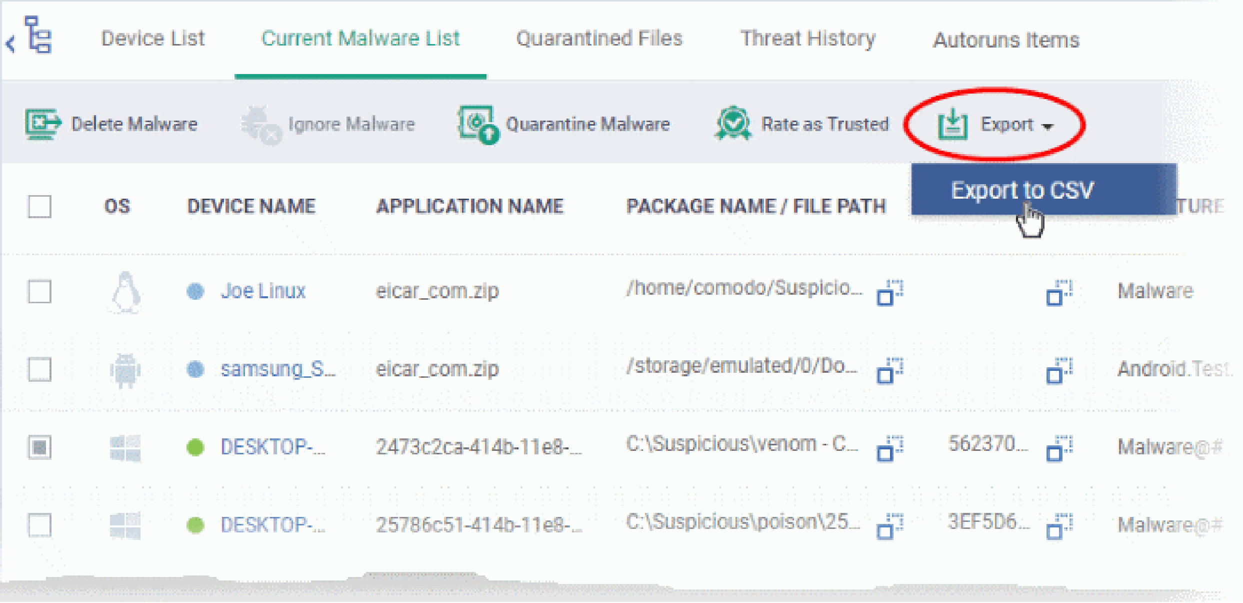
**Threats identified on Linux Devices:**

First, select the items on which you want to take the action. Then click one of the following:

- **Delete Malware** - Will remove the malware from the device.
- **Quarantine Malware** - The items will be moved to quarantine on the respective devices. You can delete the items from quarantine later, or restore them to their original locations. See **View and Manage Quarantined Items** for more details.

### Export the List of Malware

- Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List'
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button then choose 'Export to CSV':



| □ | OS | DEVICE NAME | APPLICATION NAME | PACKAGE NAME / FILE PATH | | TURE |
|---|---|---|---|---|---|---|
| □ | | Joe Linux | eicar_com.zip | /home/comodo/Suspicio... | | Malware |
| □ | | samsung_S... | eicar_com.zip | /storage/emulated/0/Do... | | Android.Test |
| ☑ | | DESKTOP-... | 2473c2ca-414b-11e8-... | C:\Suspicious\venom - C... | 562370... | Malware@# |
| □ | | DESKTOP-... | 25786c51-414b-11e8-... | C:\Suspicious\poison\25... | 3EF5D6... | Malware@# |

- The .csv file is available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## 10.7. View and Manage Quarantined Items

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files' to open the quarantine interface
- This interface lists all items moved to quarantine by CCS on managed Windows, Linux and Mac OS devices.
- Quarantine is a secure holding area for potentially dangerous files. Quarantined files pose no threat to your system.
- You can delete or restore quarantined items, or assign a file rating to them.

- File ratings determine how CCS handles the file:
  - Files rated as 'Malicious' will stay in quarantine on the device.
  - Files rated as 'Unrecognized' will be restored to their original location on the device. Future virus scans may flag them as malicious again.
  - Files rated as 'Trusted' will be restored to their original locations on the device. These files are skipped in future virus scans.

### How do threats get quarantined on a Windows device?

**Real time scans** - Threats are placed in quarantine if:

- 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action in the profile on the device. This setting is in the 'Realtime Scan Settings' area of the profile's antivirus section.
- 'Show antivirus alerts' is enabled and the end-user quarantined the threat at an alert.
- See **Realtime Scan settings** if you want to read more about the antivirus section of a profile.

**On-demand / Scheduled scans** - Threats are placed in quarantine if:

- 'Automatically clean threats' is enabled and 'Quarantine' is set as the action in the profile on the device.
- See **Custom Scans** in **Antivirus Settings** if you need more help with this.

**Manual quarantine:**

- Admins can move threats to quarantine from the 'Current Malware List' interface.
- End-users can move files to quarantine on their endpoint.
- See **View and Manage Identified Malware** for more details.

### How do threats get quarantined on a MAC?

**Real time scans** - Threats are placed in quarantine if:

- 'Automatically quarantine threats found during scanning' is enabled is enabled in the profile on the device. This setting is in the 'Realtime Scan Settings' area of the profile's antivirus section.
- The end-user chooses to quarantine the threat at an alert
- See the explanation of **Realtime Scanner** settings in the section **Antivirus Settings for Mac OS Profile** under **Create a Mac OS Profile**

**On-demand / Scheduled scans** - Threats are quarantined if:

- 'Automatically quarantine threats found during scanning' is enabled in the profile on the device
- See **Manual Scanner settings** and **Scheduled Scanner settings** for more help with this.

**Manual quarantine:**

- An administrator moved a threat to quarantine from the 'Current Malware List' interface
- An end-user moved a file to quarantine on the endpoint
- See **View and Manage Identified Malware** for more details.

### How do threats get quarantined on Linux?

**Real time scans** - Threats are quarantined if:

- 'Automatically quarantine threats found during scanning' is enabled in the profile on the device. This setting is in the 'Realtime Scan Settings' area of the profile's antivirus section.
- The end-user chooses to quarantine the threat at an alert
- See **Realtime Scanner** settings for more help with this.

**On-demand / Scheduled scans -** Threats will be placed in quarantine if:

- 'Automatically quarantine threats found during scanning' is enabled in the profile on the device
- See **Realtime Scanner settings** and **Scheduled Scanner settings** to view help on these settings.

**Manual quarantine:**

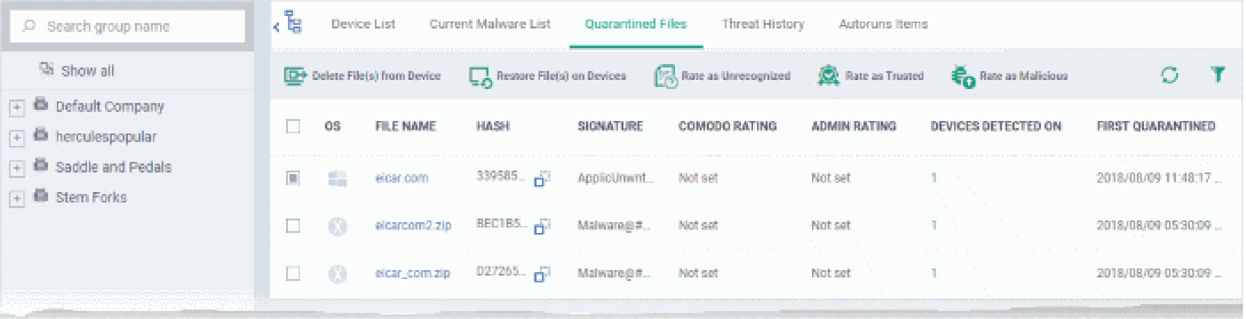
- An administrator moved a threat to quarantine from the 'Current Malware List' interface
- An end-user moved a file to quarantine on the endpoint
- See **View and Manage Identified Malware** for more details.

Items moved to quarantine are encrypted and not allowed to run.

### Open the quarantine interface

- Click 'Security Sub-Systems' > 'Antivirus'
- Click the 'Quarantined Files' tab
    - Select a company or a group to view malware identified on their devices

      Or
    - Select 'Show All' on the left menu to view malware identified on all devices enrolled to EM



| ☐ | OS | FILE NAME | HASH | SIGNATURE | COMODO RATING | ADMIN RATING | DEVICES DETECTED ON | FIRST QUARANTINED |
|---|---|---|---|---|---|---|---|---|
| ☐ | | eicar.com | 339585... | ApplicUnwnt... | Not set | Not set | 1 | 2018/08/09 11:48:17 ... |
| ☐ | | eicarcom2.zip | BEC1B5... | Malware@#... | Not set | Not set | 1 | 2018/08/09 05:30:09 ... |
| ☐ | | eicar_com.zip | D27265... | Malware@#... | Not set | Not set | 1 | 2018/08/09 05:30:09 ... |

| 'Quarantine Files' - Table of Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the device at which the item was quarantined. |
| File Name | The file that was moved to quarantine.<br>• Click the name of a file to view its details.<br>• See **View details of a quarantined item** for more details. |
| Hash | The SHA1 hash value of the quarantined file<br>• Click the ⧉ icon to copy the hash value to the clipboard. |
| Signature | The name of the identified malware. 'User Item' indicates the file was moved to quarantine manually by the user on the endpoint. |
| Comodo Rating | The file's trust level as rated by CCS. |
| Admin Rating | The trust rating of the file as set by the administrator. Files can be rated as trusted, |

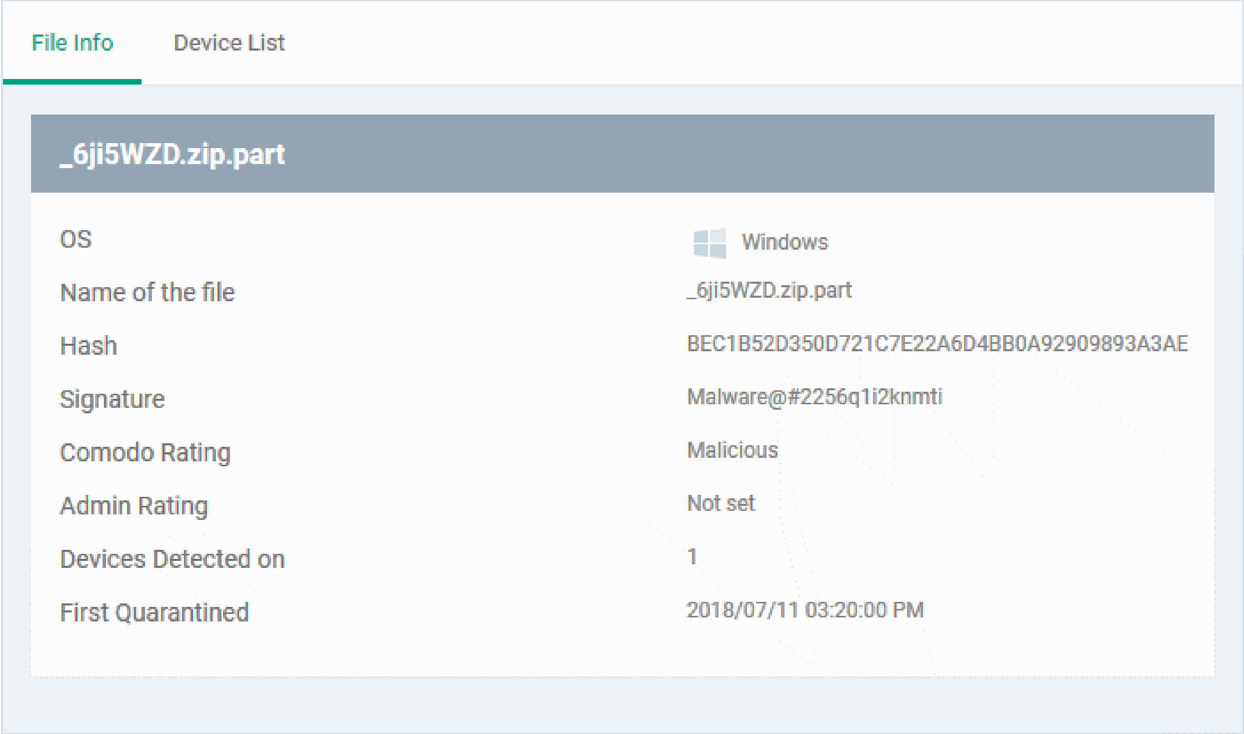
| | |
|---|---|
| | malicious or unrecognized. |
| Devices Detected On | The number of devices on which the item was quarantined.<br>• Click the number to view the list of devices on which the item was quarantined<br>• See the explanation of **Device Details** given below |
| First Quarantined | Date and time at which the malware was identified and quarantined the first time. |

The quarantine interface allows you to:

- **View details of a quarantined item**
- **Restore False Positives from Quarantine**
- **Remove Malware files from the devices**
- **Rate files as 'Unrecognized', 'Trusted' or 'Malicious'**
- **Export the list of quarantined files as a CSV file**

## View Details of a Quarantined Item

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files'
- Click on the file name of an item in the list:

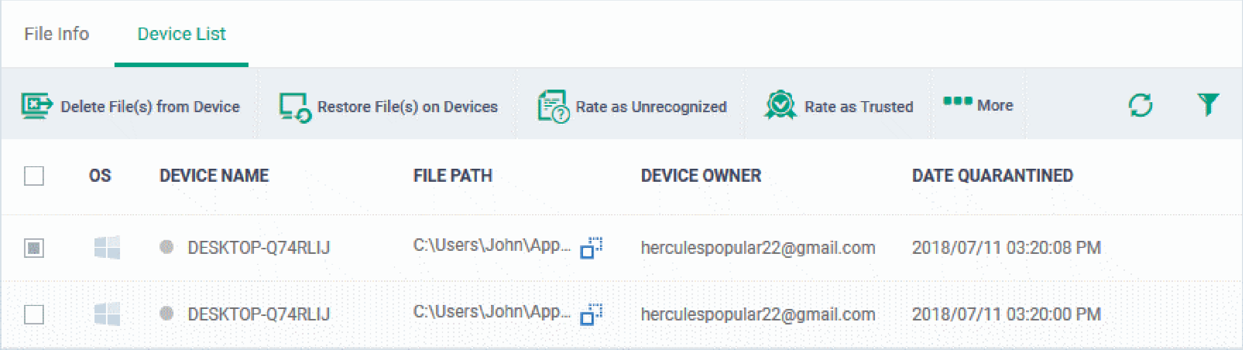


_6ji5WZD.zip.part

| | |
|---|---|
| OS | Windows |
| Name of the file | _6ji5WZD.zip.part |
| Hash | BEC1B52D350D721C7E22A6D4BB0A92909893A3AE |
| Signature | Malware@#2256q1i2knmti |
| Comodo Rating | Malicious |
| Admin Rating | Not set |
| Devices Detected on | 1 |
| First Quarantined | 2018/07/11 03:20:00 PM |

- This will open the file details interface which shows:
  - **File Info** - General information such as OS, file-name,hash, file ratings, number of devices on which the file was quarantined and more.
  - **Device List** - Shows list of endpoints upon which the file was found with heir details like installation path of the file on each device, the device owner and the date and time at which the file was quarantined.

**Device Details**



| ☐ | OS | DEVICE NAME | FILE PATH | DEVICE OWNER | DATE QUARANTINED |
|---|---|---|---|---|---|
| ☒ | | DESKTOP-Q74RLIJ | C:\Users\John\App... | herculespopular22@gmail.com | 2018/07/11 03:20:08 PM |
| ☐ | | DESKTOP-Q74RLIJ | C:\Users\John\App... | herculespopular22@gmail.com | 2018/07/11 03:20:00 PM |

The options on the top let you to:

- Restore False Positives from Quarantine on a device
- Remove the item from a device
- Rate files as 'Unrecognized', 'Trusted' or 'Malicious'
- See the following sections for more details

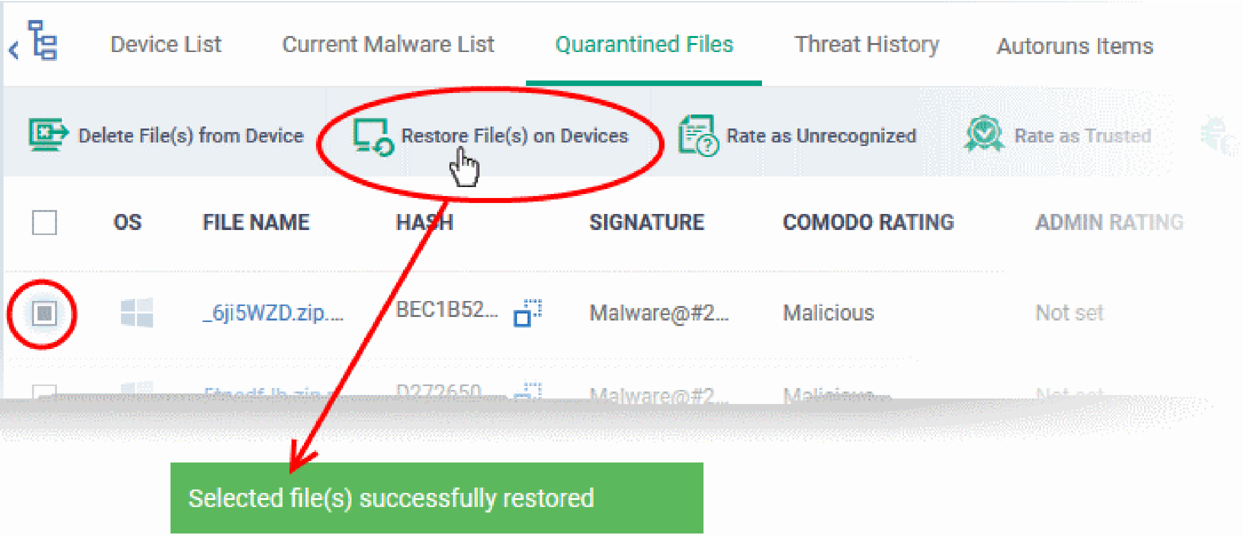
## Manage Quarantined Items

- If your review confirms that a quarantined item is a genuine threat then it can be deleted from endpoints.
- Conversely, if an item is is found to be a false positive, you can restore it to its original location.
- You can also rate a file as unrecognized, trusted or malicious based on your assessment. The new verdict will be sent to all endpoints and will be reflected in the 'Unrecognized' and 'Trusted' interfaces.

## Restore False Positives from Quarantine

- If the identified item is a false positive, select the item from the list and click 'Restore File(s) on Devices' from the options at the top.

The item will be restored to its original location on all devices and removed from the list.

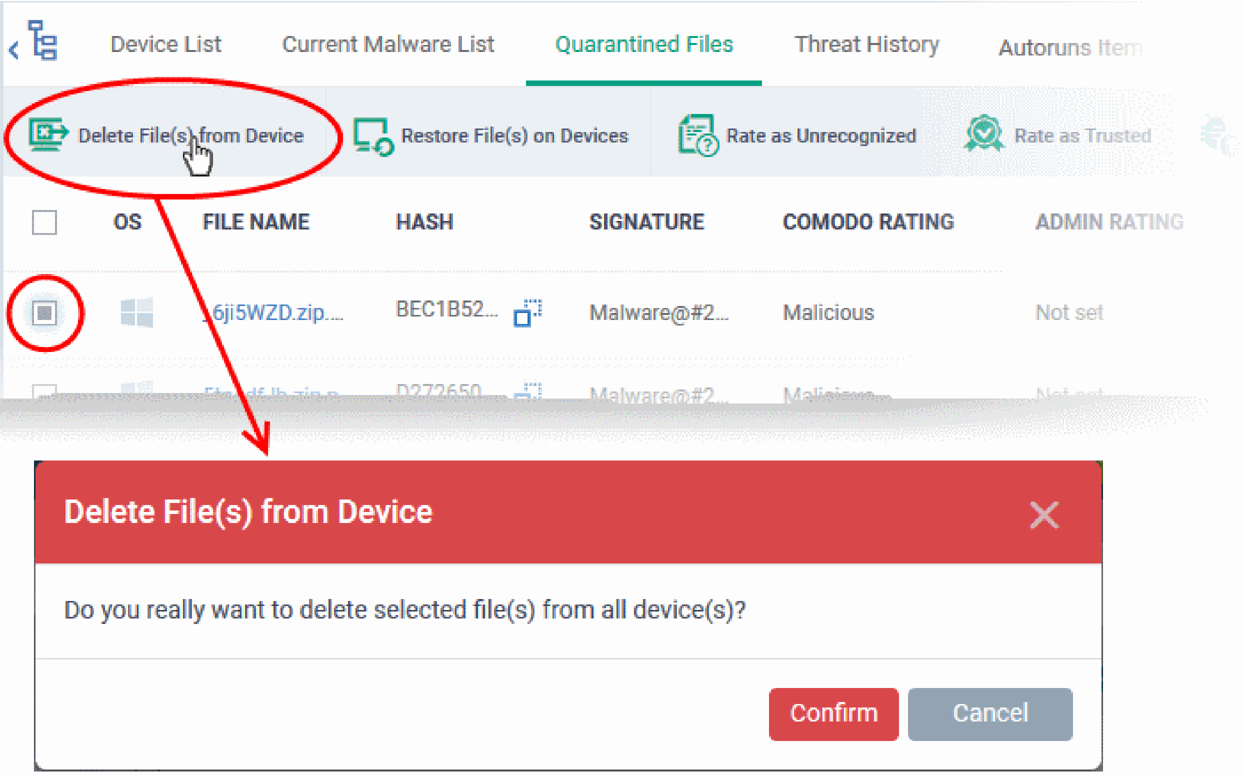


| ☐ | OS | FILE NAME | HASH | SIGNATURE | COMODO RATING | ADMIN RATING |
|---|---|---|---|---|---|---|
| ☒ | | _6ji5WZD.zip.... | BEC1B52... | Malware@#2... | Malicious | Not set |

Selected file(s) successfully restored

## Remove Malware files from the devices

- Select the item(s) from the list and click 'Delete File(s) From Device' from the options at the top.



| ☐ | OS | FILE NAME | HASH | SIGNATURE | COMODO RATING | ADMIN RATING |
|---|---|---|---|---|---|---|
| ☑ | | _6ji5WZD.zip.... | BEC1B52... | Malware@#2... | Malicious | Not set |
| ☐ | | 5tnedfJb.zip.p... | D272650... | Malware@#2... | Malicious | Not set |

**Delete File(s) from Device**

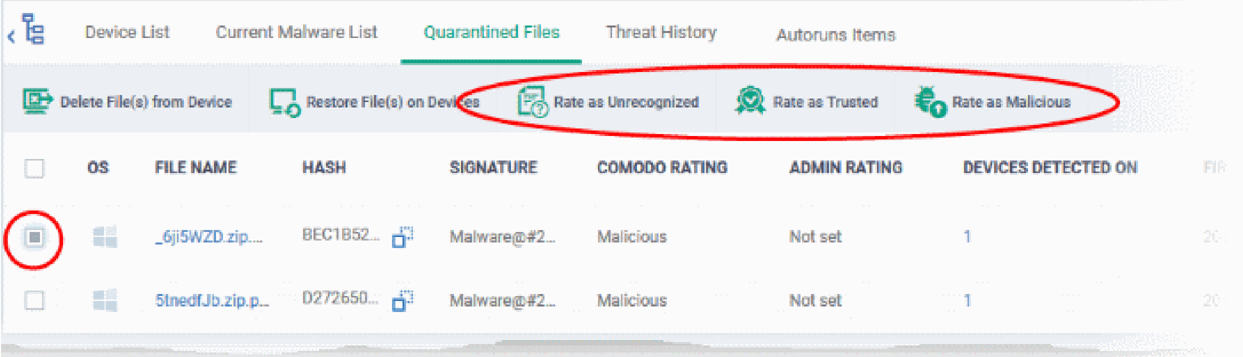
Do you really want to delete selected file(s) from all device(s)?

- Click 'Confirm' in the confirmation dialog.

The file will be deleted from all devices at which it was quarantined and removed from the list.

## Rate files as 'Unrecognized', 'Trusted' or 'Malicious'

- If the rating of a quarantined file is changed to 'Trusted' or 'Unrecognized', the file is restored to its original location. The new rating is also stored in the CCS database on the devices.
- To change the rating of a quarantined file, select it and click the appropriate button at the top:



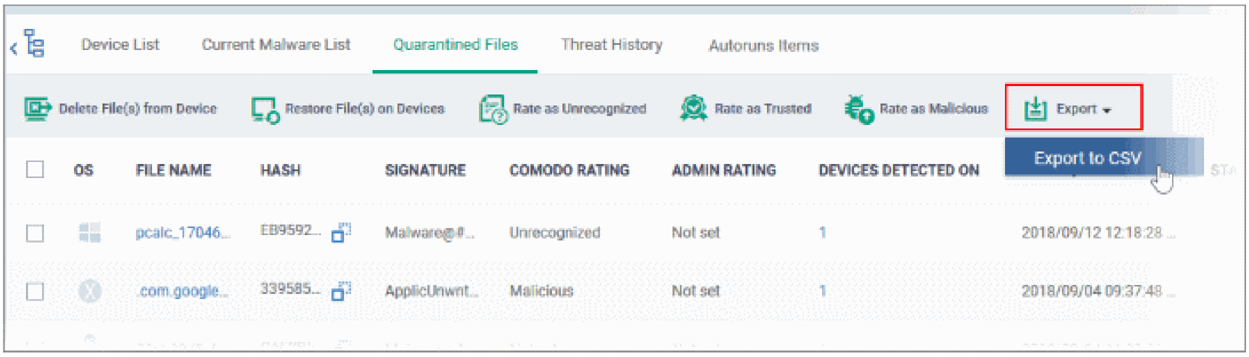
| ☐ | OS | FILE NAME | HASH | SIGNATURE | COMODO RATING | ADMIN RATING | DEVICES DETECTED ON |
|---|---|---|---|---|---|---|---|
| ☑ | | _6ji5WZD.zip.... | BEC1B52... | Malware@#2... | Malicious | Not set | 1 |
| ☐ | | 5tnedfJb.zip.p... | D272650... | Malware@#2... | Malicious | Not set | 1 |

A confirmation will be displayed and the information will also be sent to the devices.

- Files rated as 'Malicious' will stay in quarantine on the device.
- Files rated as 'Unrecognized' will be restored to their original locations on the device. Future AV scans may flag them as 'malicious' again.
- Files rated as 'Trusted' will be restored to their original locations in the device. These files will be white-listed and skipped by future antivirus scans.

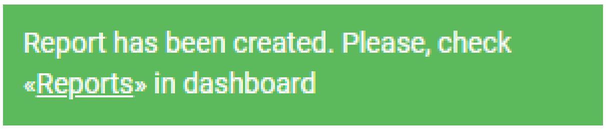
### Export quarantined files records as a CSV file

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files' tab
- Click the funnel ▼ icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| □ | OS | FILE NAME | HASH | SIGNATURE | COMODO RATING | ADMIN RATING | DEVICES DETECTED ON | STA |
|---|---|---|---|---|---|---|---|---|
| □ | | pcalc_17046... | EB9592... | Malware@#... | Unrecognized | Not set | 1 | 2018/09/12 12:18:28 ... |
| □ | | com.google... | 339585... | ApplicUnwnt... | Malicious | Not set | 1 | 2018/09/04 09:37:48 ... |

The report will be generated in .csv format.


Report has been created. Please, check «Reports» in dashboard

The file will be available in 'Dashboard' > 'Reports'. See **Reports** if you need more help with this interface.

## 10.8. View Threat History

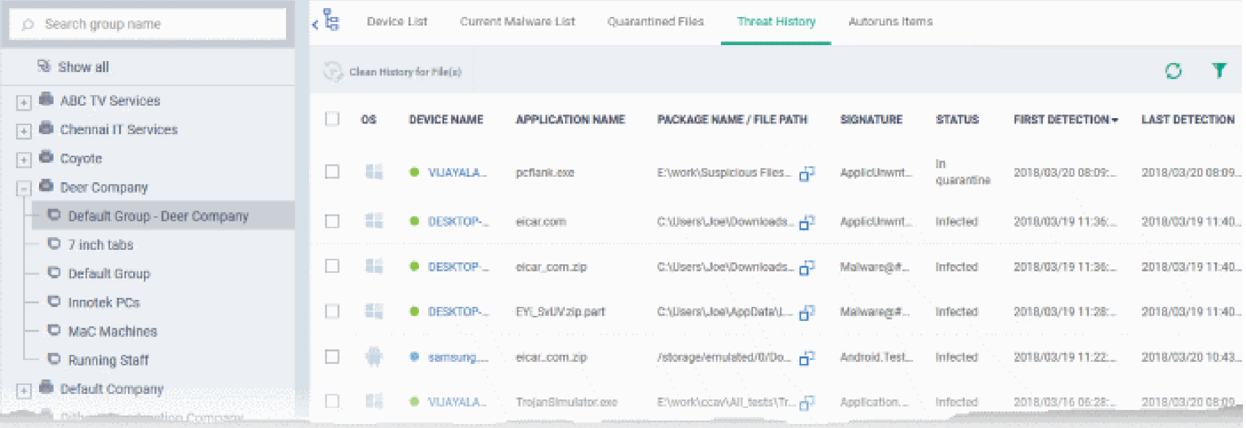
Click 'Security Sub-Systems' > 'Antivirus' > 'Threat History'

- The threat history area is a record of all malicious events on your devices since you deployed Endpoint Manager.
- The list shows old events caused by malware which has been removed, and new events by malware which is still present.
- Endpoint Manager retains logs of malicious events for 12 months for PCI-DSS compliance.
- You can remove unnecessary entries from the list as required

**View threat history**

- Click 'Security Sub-systems' > 'Antivirus'.
- Click the 'Threat History' tab.
  - Select a company or a group to view events on their devices

    Or
  - Select 'Show All' on to view events on all devices added to EM

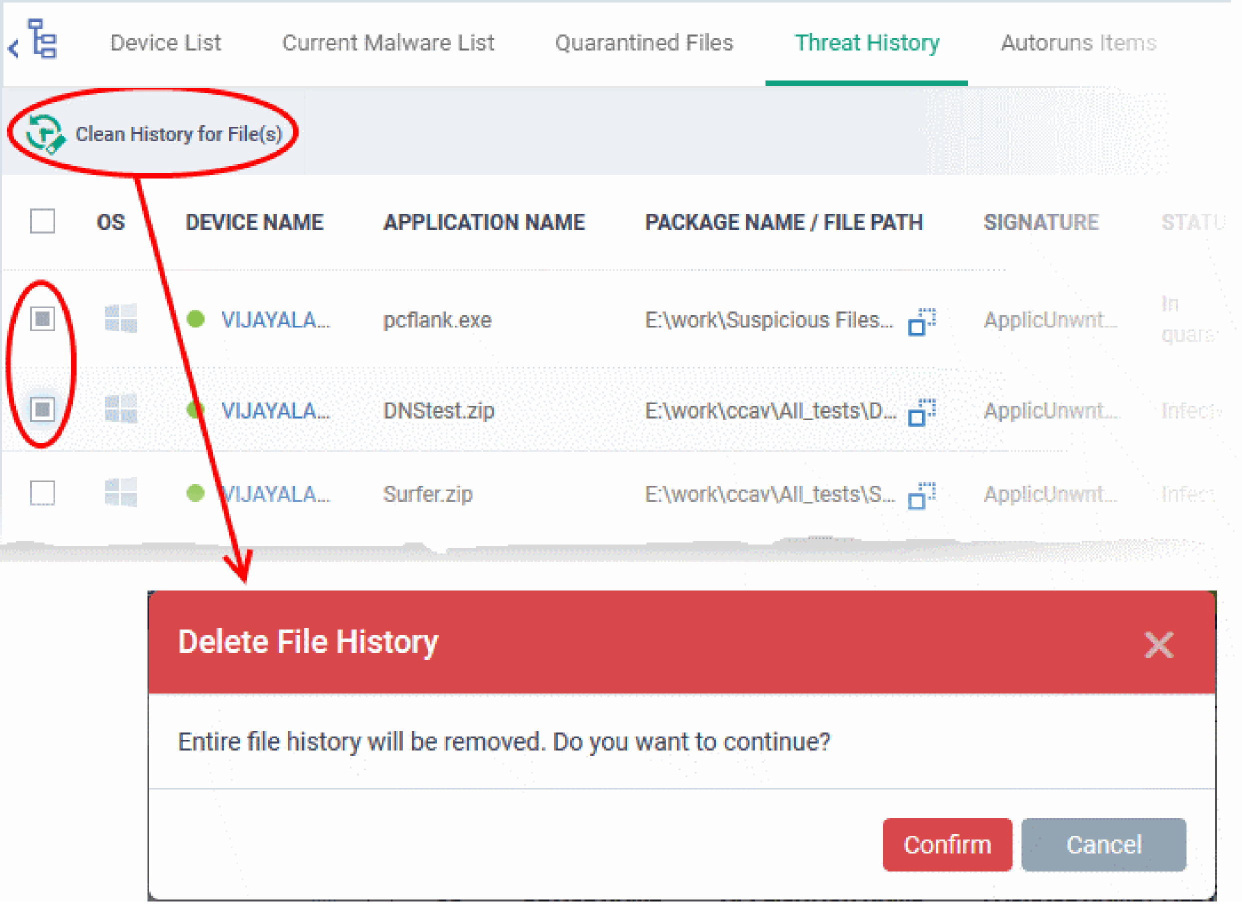


| □ | OS | DEVICE NAME | APPLICATION NAME | PACKAGE NAME / FILE PATH | SIGNATURE | STATUS | FIRST DETECTION ▾ | LAST DETECTION |
|---|---|---|---|---|---|---|---|---|
| □ | | ● VIJAYALA... | pcflank.exe | E:\work\Suspicious Files... | ApplicUnwnt... | In quarantine | 2018/03/20 08:09:... | 2018/03/20 08:09... |
| □ | | ● DESKTOP-... | eicar.com | C:\Users\Joe\Downloads... | ApplicUnwnt... | Infected | 2018/03/19 11:36:... | 2018/03/19 11:40... |
| □ | | ● DESKTOP-... | eicar_com.zip | C:\Users\Joe\Downloads... | Malware@#... | Infected | 2018/03/19 11:36:... | 2018/03/19 11:40... |
| □ | | ● DESKTOP-... | EYI_SvUV.zip.part | C:\Users\Joe\AppData\L... | Malware@#... | Infected | 2018/03/19 11:28:... | 2018/03/19 11:40... |
| □ | | ● samsung... | eicar_com.zip | /storage/emulated/0/Do... | Android.Test... | Infected | 2018/03/19 11:22:... | 2018/03/20 10:43... |
| □ | | ● VIJAYALA... | TrojanSimulator.exe | E:\work\ccav\All_tests\Tr... | Application... | Infected | 2018/03/16 06:28:... | 2018/03/20 08:09... |

| Antivirus Threat History - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| OS | The operating system of the device on which the malware was found. |
| Device Name | The label assigned to the device. If no name was assigned by the end-user, the model number of the device is used. A gray text color indicates the device has been offline for the past 24 hours.<br>• Click the device name to view granular details about the device.<br>• See **Manage Windows Devices**, **Manage Mac OS Devices**, **Manage Linux Devices** and **Manage Android / iOS Devices** for more details. |
| Application Name | The name of the infected application. |
| Package Name / File Path | The Android package name or identifier of the package from which the app was installed. For Windows, Linux and Mac OS devices, the file path of the detected malware is shown. |
| Signature | The name of the identified malware. |
| Status | Whether the malware was uninstalled or is yet to be uninstalled. |
| First Detection | Date and time of the scan which first discovered the malware on the device. |
| Last Detection | Date and time of the last scan to discover the malware. |

**Remove unwanted entries from the 'Threat History' interface**

- Select the log entries you want to remove then click 'Clean History for File(s)' at the top



| □ | OS | DEVICE NAME | APPLICATION NAME | PACKAGE NAME / FILE PATH | SIGNATURE | STATU |
|---|---|---|---|---|---|---|
| ☑ | | VIJAYALA... | pcflank.exe | E:\work\Suspicious Files... | ApplicUnwnt... | In quara |
| ☑ | | VIJAYALA... | DNStest.zip | E:\work\ccav\All_tests\D... | ApplicUnwnt... | Infect |
| □ | | VIJAYALA... | Surfer.zip | E:\work\ccav\All_tests\S... | ApplicUnwnt... | Infect |

**Delete File History**

Entire file history will be removed. Do you want to continue?

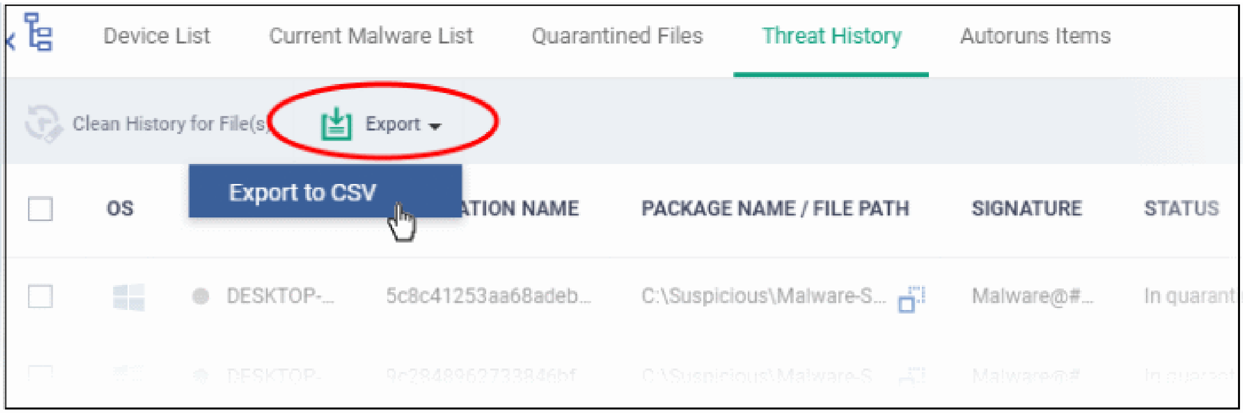
- Click 'Confirm' to remove the entries from the list
- Deleting file history will only remove the log entry. The file will not be removed from the device or from any other interfaces in which it is listed (for example, the quarantine list).

## Sorting, Search and Filter Options

- Click any column header to sort items in ascending/descending order of the entries in that column
- Click the funnel icon on the right to filter items by various criteria, including by OS, device name, application name, package name/file path, signature, status and first/last detection dates.
- Start typing or select the search criteria in the search field to find a particular item and click 'Apply'
- To display all items again, clear any filters and search criteria and click 'Apply'.
- EM returns 20 results per page when you perform a search. Click the arrow next to the 'Results per page' drop-down to increase results up to a maximum of 200.
- Use the left and right arrows and the page numbers to navigate to the page you want to view.

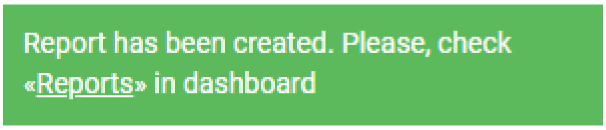
### Export threat history records as a CSV file

- Click 'Security Sub-Systems' > 'Antivirus' > 'Threat History' tab
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| | OS | | ...ATION NAME | PACKAGE NAME / FILE PATH | SIGNATURE | STATUS |
|---|---|---|---|---|---|---|
| □ | | DESKTOP-... | 5c8c41253aa68adeb... | C:\Suspicious\Malware-S... | Malware@#... | In quarant |
| □ | | DESKTOP- | 9c2848962733846bf | C:\Suspicious\Malware-S | Malware@# | In quarant |

The report will be generated in .csv file format.



Report has been created. Please, check «Reports» in dashboard

Click 'Dashboard' > 'Reports' to view the report. See **Reports** if you need more help with this interface.

## 10.9. View and Manage Autorun Items

- Click 'Security Sub-Systems' > 'Antivirus' > Click the 'Autoruns Items' tab
- This area lets you view and take action on items blocked by the boot protection feature of Comodo Client Security (CCS).
- This includes unrecognized Windows services, auto-start entries and scheduled tasks.

From this interface, you can:

- Assign a rating to quarantined auto-run items (trusted, malicious or unrecognized)
- Delete them permanently
- Restore them to their original location

**How do unrecognized autoruns items get terminated?**

Unrecognized auto-runs will be terminated if:

- 'Apply this action to suspicious auto-run processes' is enabled

  with

  'Terminate', 'Terminate and Disable' or 'Quarantine and Disable' set as the action.

You can implement this setting in two places:

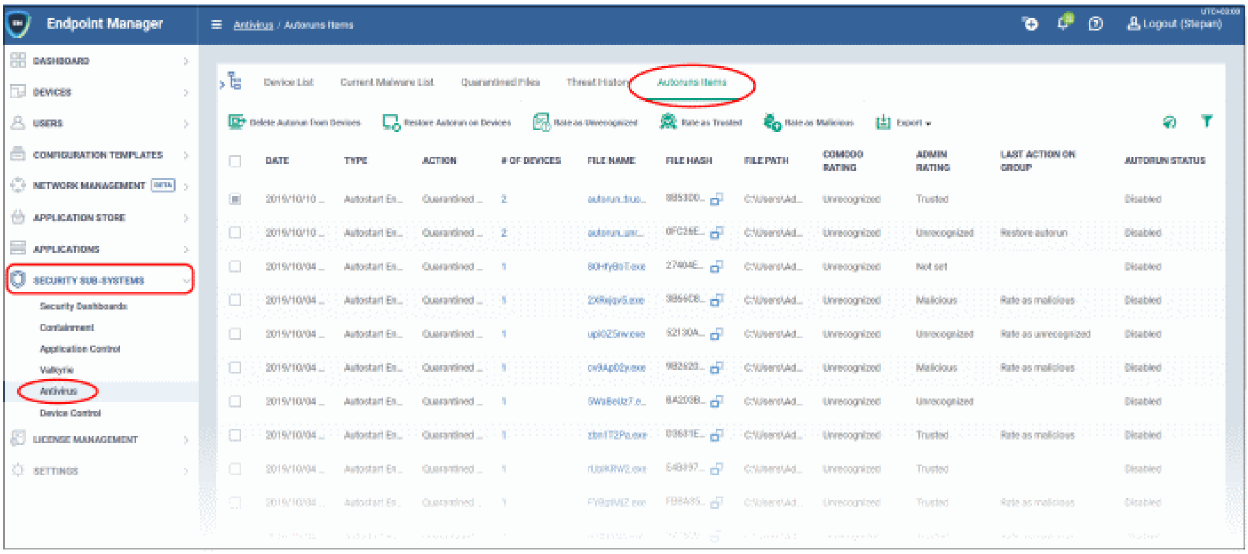
1) The 'miscellaneous' section of a profile. This applies the action to the real-time virus scanner. See **Miscellaneous Settings**

2) The 'Options' section when you create a custom virus scan. See **custom scans** in **Antivirus Settings** **https://help.comodo.com/topic-399-1-786-10202-antivirus-settings.html#custom_scans**.

**Open the interface**

- Click 'Security Sub-Systems' > 'Antivirus'
- Click the 'Autoruns Items' tab
  - Select a company or a group to view auto-runs on their devices

    Or
  - Select 'Show All' to view all terminated auto-runs



| DATE | TYPE | ACTION | # OF DEVICES | FILE NAME | FILE HASH | FILE PATH | COMODO RATING | ADMIN RATING | LAST ACTION ON GROUP | AUTORUN STATUS |
|---|---|---|---|---|---|---|---|---|---|---|
| 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_true... | 8B53D0... | C:\Users\Ad... | Unrecognized | Trusted | | Disabled |
| 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_unr... | 0FC26E... | C:\Users\Ad... | Unrecognized | Unrecognized | Restore autorun | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 80HfyBbT.exe | 27404E... | C:\Users\Ad... | Unrecognized | Not set | | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 2XRejqv5.exe | 3B66C8... | C:\Users\Ad... | Unrecognized | Malicious | Rate as malicious | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | upl0Z5rw.exe | 52130A... | C:\Users\Ad... | Unrecognized | Unrecognized | Rate as unrecognized | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | cv9Ap02y.exe | 9B2620... | C:\Users\Ad... | Unrecognized | Malicious | Rate as malicious | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 5WaBeUz7.e... | 8A203B... | C:\Users\Ad... | Unrecognized | Unrecognized | | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | zbn1T2Pa.exe | 03631E... | C:\Users\Ad... | Unrecognized | Trusted | Rate as malicious | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | rUbkRW2.exe | E4B897... | C:\Users\Ad... | Unrecognized | Trusted | | Disabled |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | FY8gIMZ.exe | FB8A85... | C:\Users\Ad... | Unrecognized | Trusted | Rate as malicious | Disabled |

| Column Heading | Description |
|---|---|
| Date | The date and time the auto-run was terminated on the device |
| Type | The auto-run category:<br>• Windows Services<br>• Scheduled Task<br>• Autostart Entry |
| Action | How the unrecognized autorun was treated on the endpoints:<br>• Terminated<br>• Terminated and Disabled<br>• Quarantined and Disabled |
| # of Devices | The number of devices on which the item was terminated<br>• Click the number to view the list of devices on which the item was terminated<br>• See the explanation of **Device Details** given below |
| File Name | The file whose auto-run entry was terminated<br>• Click the name of a file to view its details<br>• See **View details of a terminated autorun item** for details |
| File Hash | The SHA1 hash value of the quarantined file. The hash value uniquely identifies the item even if its filename is changed. |

| | |
|---|---|
| | • Click the ⧉ icon to copy the hash value to the clipboard. |
| File Path | The location of the file on the endpoint |
| Comodo Rating | The file's trust level as rated by CCS. |
| Admin Rating | The trust rating of the file as set by the administrator. Files can be rated as trusted, malicious or unrecognized. |
| Last Action Group | Indicates the latest action taken by the admin. |
| Autorun Status | Shows whether the auto-run is enabled or disabled on the endpoint |

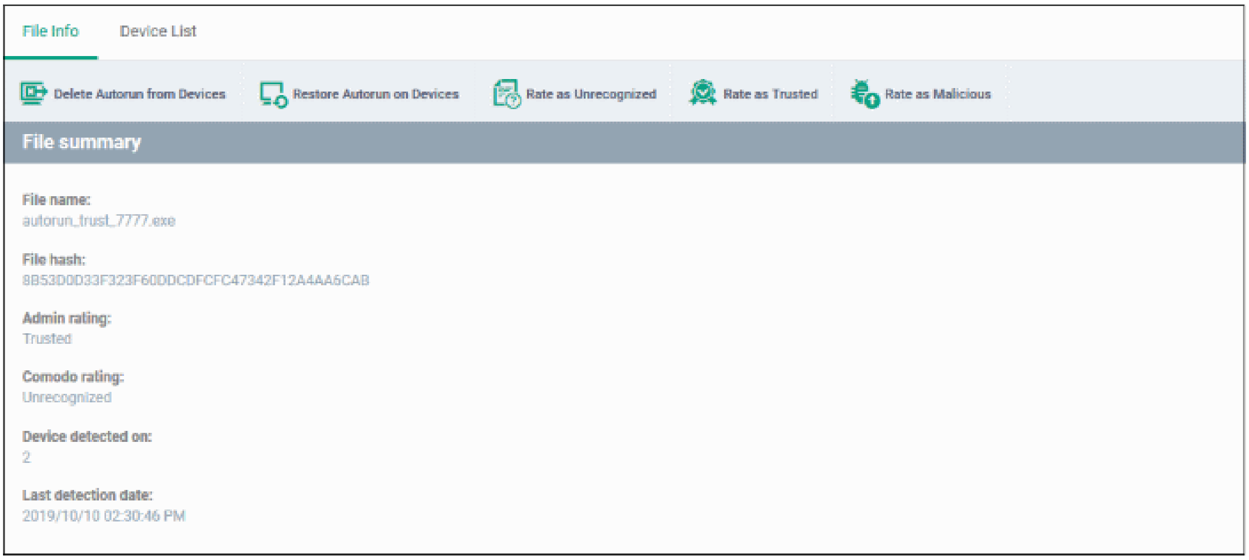
- Click a column header to sort items in ascending / descending / alphabetical order
- Click the funnel icon at top-right and search by various parameters

You can perform the following tasks from the auto-runs page:

- **View details of a terminated autorun item**
- **Restore autorun item on devices**
- **Delete autorun item from devices**
- **Rate autorun items as unrecognized, trusted or malicious**
- **Export the list of autorun items as a CSV file**

## View Details of a Terminated Autorun Item

- Click 'Security Sub-Systems' > 'Antivirus' > 'Autoruns Items'
- Click the file name of an item in the list:



File summary

File name:
autorun_trust_7777.exe

File hash:
8B53D0D33F323F60DDCDFCFC47342F12A4AA6CAB

Admin rating:
Trusted

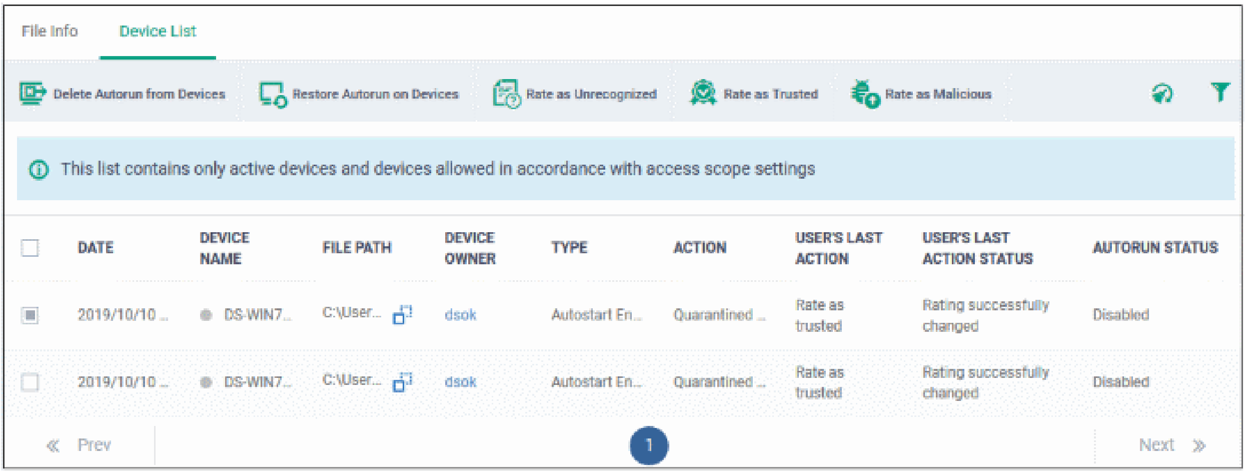
Comodo rating:
Unrecognized

Device detected on:
2

Last detection date:
2019/10/10 02:30:46 PM

- This will open the file details interface which shows:
  - **File Info** - General information such as file-name, hash, file rating, number of devices on which the file was terminated, and more.
  - **Device List** - Shows a list of the endpoints on which the file was found, along with details like file installation path.

### Device Details



This list contains only active devices and devices allowed in accordance with access scope settings

| □ | DATE | DEVICE NAME | FILE PATH | DEVICE OWNER | TYPE | ACTION | USER'S LAST ACTION | USER'S LAST ACTION STATUS | AUTORUN STATUS |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | 2019/10/10 ... | DS-WIN7... | C:\User... | dsok | Autostart En... | Quarantined ... | Rate as trusted | Rating successfully changed | Disabled |
| □ | 2019/10/10 ... | DS-WIN7... | C:\User... | dsok | Autostart En... | Quarantined ... | Rate as trusted | Rating successfully changed | Disabled |

The options on the top let you to:

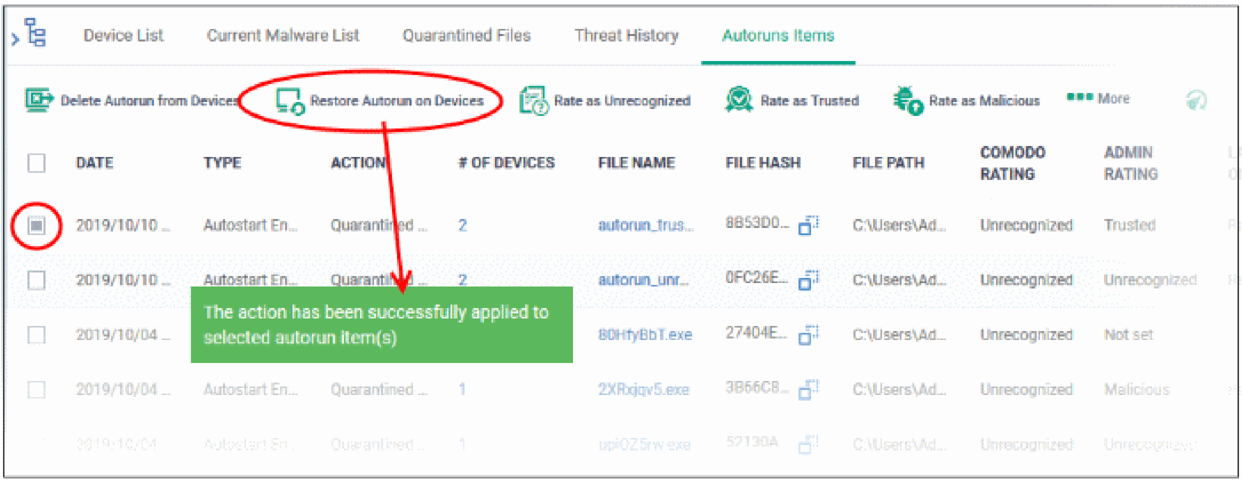
- Restore terminated autorun on a device
- Remove the item from a device
- Rate files as 'Unrecognized', 'Trusted' or 'Malicious'
- See the following sections for more details

### Manage Terminated Autorun Items

- If your review confirms that an autorun item is a genuine threat then it can be deleted from endpoints.
- Conversely, if an item is is found to be a false positive, you can restore it to its original location.
- You can also rate a file as unrecognized, trusted or malicious based on your assessment. The new verdict will be sent to all endpoints and will be reflected in the 'Unrecognized' and 'Trusted' interfaces.

## Restore Autorun Items on Devices

- If the identified item is a false positive, select the item from the list and click 'Restore Autorun on Devices' from the options at the top.

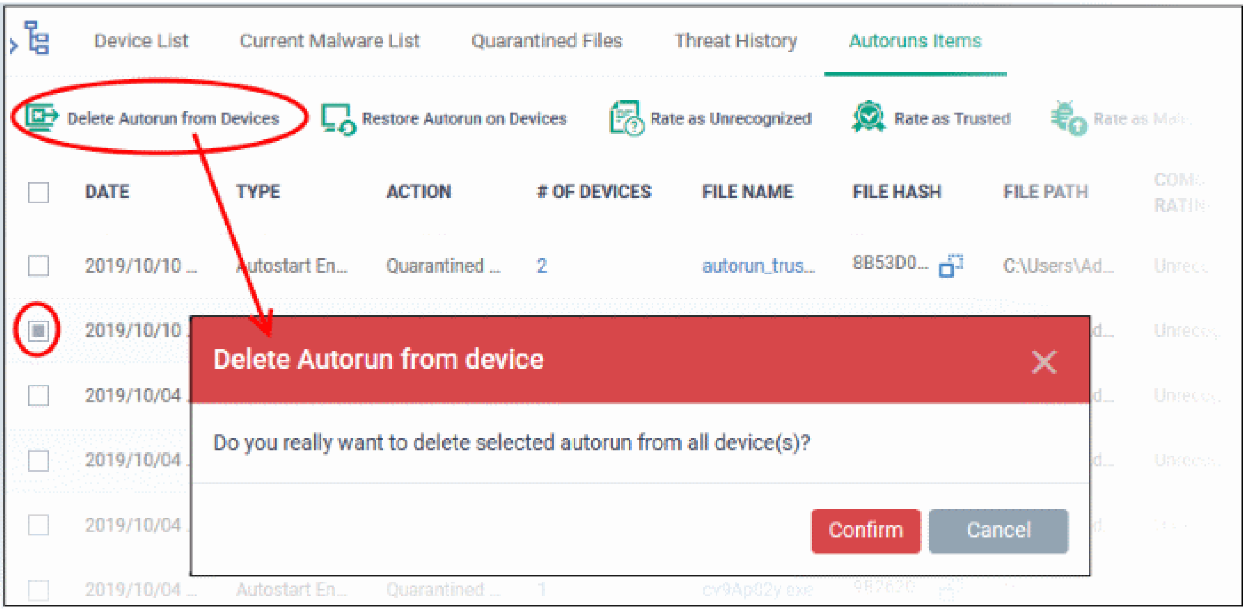


| □ | DATE | TYPE | ACTION | # OF DEVICES | FILE NAME | FILE HASH | FILE PATH | COMODO RATING | ADMIN RATING |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_trus... | 8B53D0... | C:\Users\Ad... | Unrecognized | Trusted |
| □ | 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_unr... | 0FC26E... | C:\Users\Ad... | Unrecognized | Unrecognized |
| □ | 2019/10/04 ... |  |  |  | 80HfyBbT.exe | 27404E... | C:\Users\Ad... | Unrecognized | Not set |
| □ | 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 2XRxjqv5.exe | 3B66C8... | C:\Users\Ad... | Unrecognized | Malicious |
|  | 2019/10/04 | Autostart En... | Quarantined ... | 1 | upiOZ5rw.exe | 52130A... | C:\Users\Ad... | Unrecognized | Unrecognized |

The action has been successfully applied to selected autorun item(s)

## Delete Autorun Items from Devices

- Select the item(s) from the list and click 'Delete Autorun from Device' from the options at the top.



| DATE | TYPE | ACTION | # OF DEVICES | FILE NAME | FILE HASH | FILE PATH | COM... RATIN... |
|---|---|---|---|---|---|---|---|
| 2019/10/10 ... | utostart En... | Quarantined ... | 2 | autorun_trus... | 8B53D0... | C:\Users\Ad... | Unrec... |
| 2019/10/10 | | | | | | ...d... | Unrec... |
| 2019/10/04 | | | | | | ...d... | Unrec... |
| 2019/10/04 | | | | | | ...d... | Unrec... |
| 2019/10/04 | | | | | | | |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | cv9Ap02y.exe | 9B262C... | | |

**Delete Autorun from device**

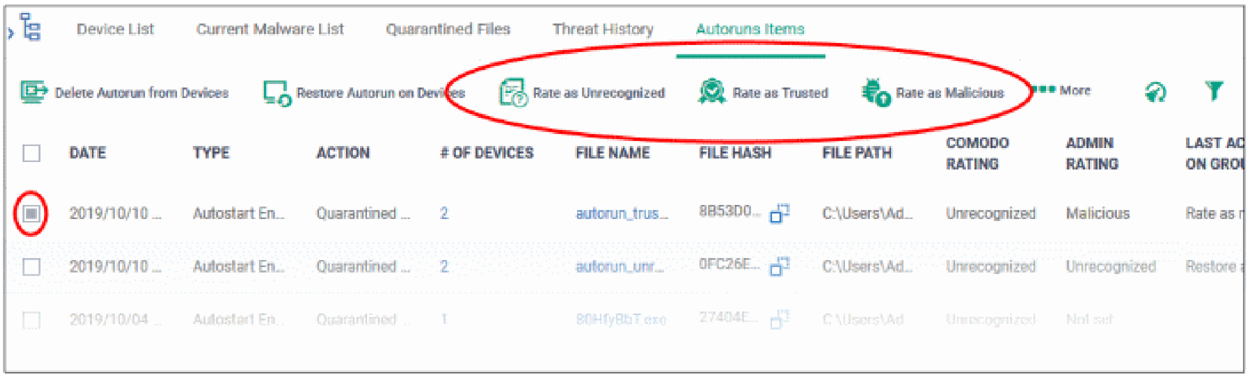
Do you really want to delete selected autorun from all device(s)?

- Click 'Confirm' to remove the files

The file will be deleted from all devices on which it was terminated and removed from the list.

## Rate Autorun Items as 'Unrecognized', 'Trusted' or 'Malicious'

- To change the rating of a file, select it and click the appropriate button at the top:



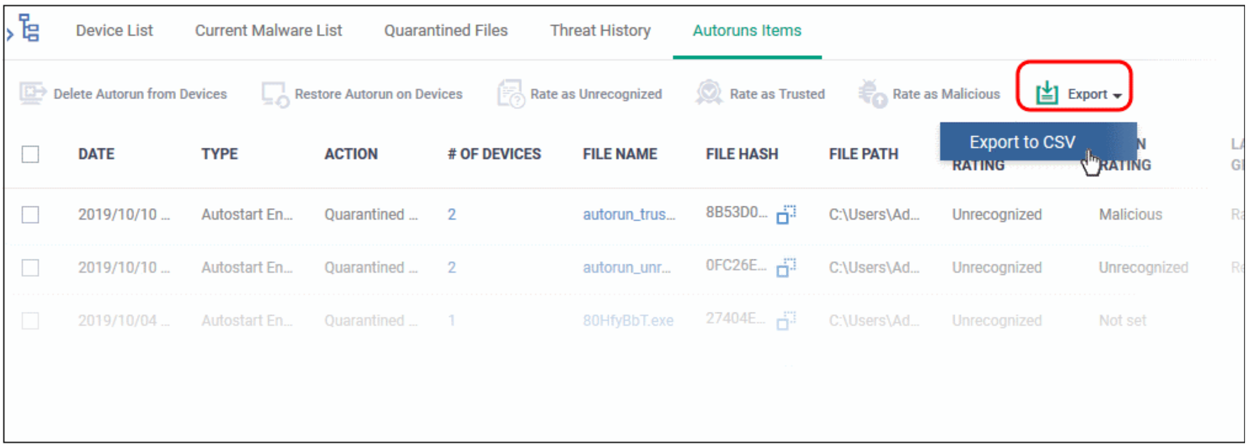
| DATE | TYPE | ACTION | # OF DEVICES | FILE NAME | FILE HASH | FILE PATH | COMODO RATING | ADMIN RATING | LAST AC ON GROU |
|---|---|---|---|---|---|---|---|---|---|
| 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_trus... | 8B53D0... | C:\Users\Ad... | Unrecognized | Malicious | Rate as r |
| 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_unr... | 0FC26E... | C:\Users\Ad... | Unrecognized | Unrecognized | Restore a |
| 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 80HfyBbT.exe | 27404E... | C:\Users\Ad... | Unrecognized | Not set | |

A confirmation will be displayed and the information sent to the devices.

- Files rated as 'Trusted' will be restored to their original locations in the device. These files will be white-listed and skipped by future antivirus scans.
- Files rated as 'Unrecognized' or 'Malicious' will be quarantined or their processes will be terminated per the profile settings.

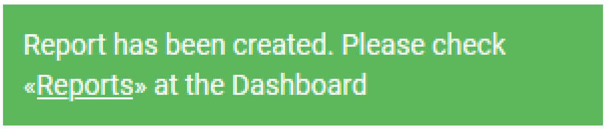
## Export Terminated Autorun Items as a CSV File

- Click 'Security Sub-Systems' > 'Antivirus' > 'Autoruns Items' tab
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



| □ | DATE | TYPE | ACTION | # OF DEVICES | FILE NAME | FILE HASH | FILE PATH | RATING | N RATING | LA GI |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_trus... | 8B53D0... | C:\Users\Ad... | Unrecognized | Malicious | Ra |
| □ | 2019/10/10 ... | Autostart En... | Quarantined ... | 2 | autorun_unr... | 0FC26E... | C:\Users\Ad... | Unrecognized | Unrecognized | Re |
| □ | 2019/10/04 ... | Autostart En... | Quarantined ... | 1 | 80HfyBbT.exe | 27404E... | C:\Users\Ad... | Unrecognized | Not set | |

The report will be generated in .csv format.



Report has been created. Please check «Reports» at the Dashboard

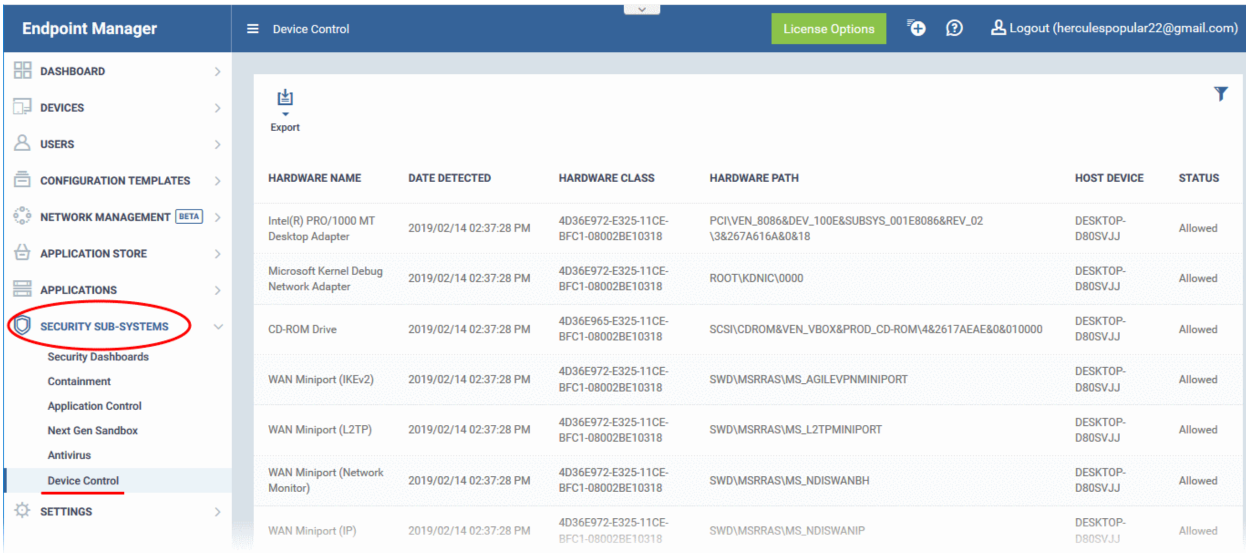
The file will be available in 'Dashboard' > 'Reports'. See **Reports** if you need more help with this interface.

## 10.10. View History of External Device Connection Attempts

- Click 'Security Sub-Systems' > 'Device Control' to view all connection attempts from external devices to your Windows endpoints
- Endpoint Manager can create a log entry when an external device attempts to connect to a Windows endpoint. External devices include USB devices, DVD drives, printers, Bluetooth devices etc.
- These logs are created when the Windows profile contains the 'External Devices Control' section. See **External Devices Control Settings** for more details.
- You can also generate a report of external device connection attempts.

**To view a history of device connections:**

- Click 'Security Sub-Systems' > 'Device Control'



| HARDWARE NAME | DATE DETECTED | HARDWARE CLASS | HARDWARE PATH | HOST DEVICE | STATUS |
|---|---|---|---|---|---|
| Intel(R) PRO/1000 MT Desktop Adapter | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | PCI\VEN_8086&DEV_100E&SUBSYS_001E8086&REV_02 \3&267A616A&0&18 | DESKTOP-D80SVJJ | Allowed |
| Microsoft Kernel Debug Network Adapter | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | ROOT\KDNIC\0000 | DESKTOP-D80SVJJ | Allowed |
| CD-ROM Drive | 2019/02/14 02:37:28 PM | 4D36E965-E325-11CE-BFC1-08002BE10318 | SCSI\CDROM&VEN_VBOX&PROD_CD-ROM\4&2617AEAE&0&010000 | DESKTOP-D80SVJJ | Allowed |
| WAN Miniport (IKEv2) | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | SWD\MSRRAS\MS_AGILEVPNMINIPORT | DESKTOP-D80SVJJ | Allowed |
| WAN Miniport (L2TP) | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | SWD\MSRRAS\MS_L2TPMINIPORT | DESKTOP-D80SVJJ | Allowed |
| WAN Miniport (Network Monitor) | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | SWD\MSRRAS\MS_NDISWANBH | DESKTOP-D80SVJJ | Allowed |
| WAN Miniport (IP) | 2019/02/14 02:37:28 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | SWD\MSRRAS\MS_NDISWANIP | DESKTOP-D80SVJJ | Allowed |

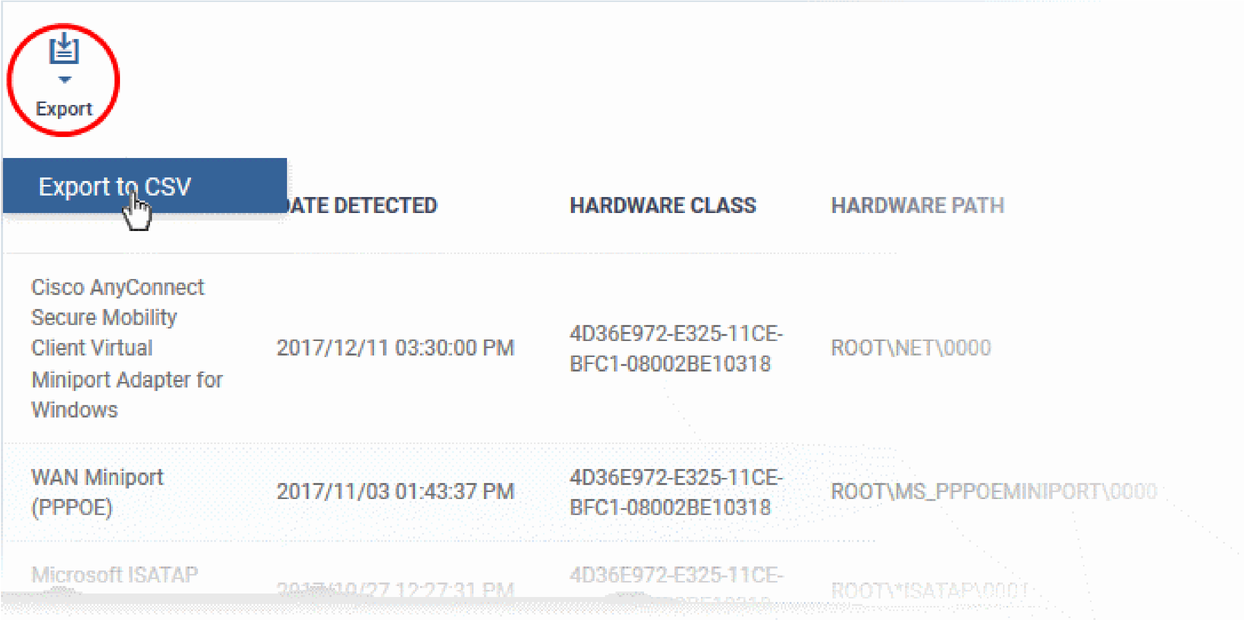
| Device Control - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Hardware Name | Displays the name of the external device which attempted to connect to a managed Windows device |
| Date Detected | The date and time at which the device was first detected |
| Hardware Class | The Globally Unique Identifier (GUID) of the device class which attempted to connect. |
| Hardware Path | The Device Instance Identifier of the external device which attempted to connect. |
| Host Device | The name of the Windows device to which the connection attempt was made. This column also shows the host's current connection status (connected or removed) |
| Status | Indicates whether the connection was allowed or blocked. This depends on the settings in the 'External Devices Control' section of the profile active on the host device. |

## Sorting, Search and Filter Options

- Click any of the 'Hardware Name', 'Hardware Class', 'Host Device' or 'Status' column headers to sort the items based on alphabetical order of entries in that column.
- Click the funnel button at the right end to filter the items based on device name, hardware class, hardware path, host, status and/or detection date.
    - Enter the search criteria in the respective field and click 'Apply'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- EM 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.
- Use the left and right arrows and the page numbers at the bottom to navigate to the page you want to view.

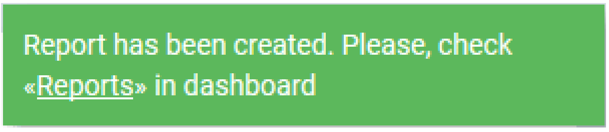
## Generate a report containing log of device connection attempts

- Click 'Security Sub-Systems' > 'Device Control'
- Click the funnel icon to apply filters to the report.
- Click the 'Export' button and choose 'Export to CSV':



| | ATE DETECTED | HARDWARE CLASS | HARDWARE PATH |
|---|---|---|---|
| Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows | 2017/12/11 03:30:00 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | ROOT\NET\0000 |
| WAN Miniport (PPPOE) | 2017/11/03 01:43:37 PM | 4D36E972-E325-11CE-BFC1-08002BE10318 | ROOT\MS_PPPOEMINIPORT\0000 |
| Microsoft ISATAP | 2017/10/27 12:27:31 PM | 4D36E972-E325-11CE- | ROOT*ISATAP\0001 |

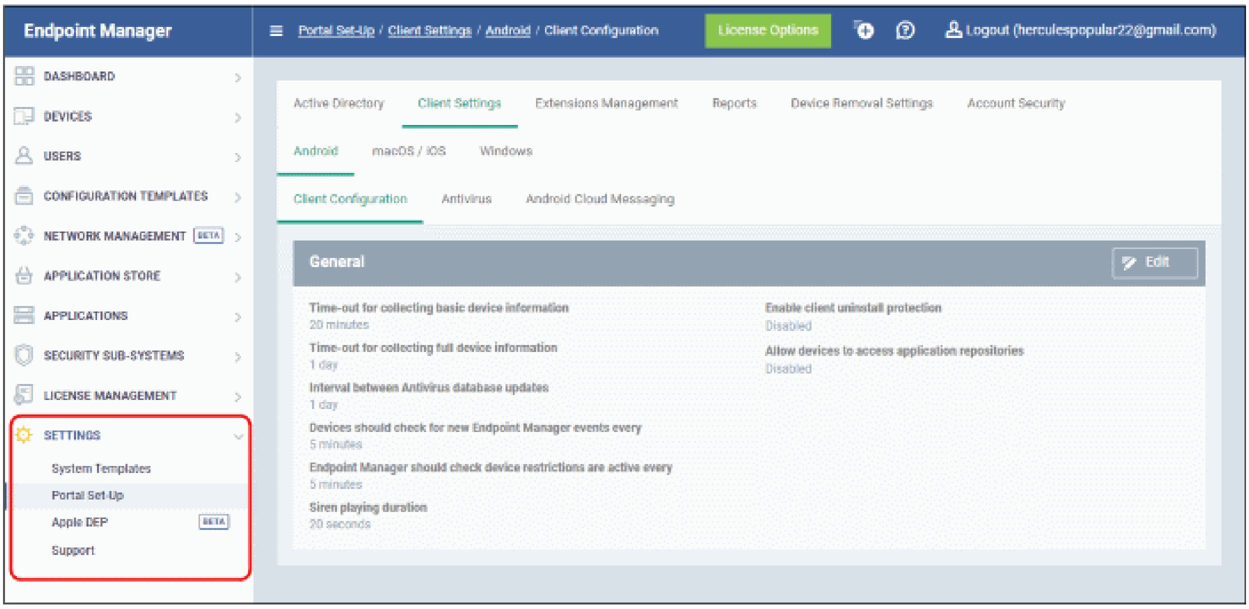
The report will be generated in .csv file format.


Report has been created. Please, check «Reports» in dashboard

The report can be accessed in the 'Dashboard' > 'Reports' interface. See **Reports** in **The Dashboard** if you need more help with this interface.

# 11. Configure Endpoint Manager

- The 'Settings' area lets you configure email notifications, active directory, Google and Apple device certificates, and more.
- You can also manage subscriptions, renew/upgrade licenses and view support information.



Time-out for collecting basic device information
20 minutes

Time-out for collecting full device information
1 day

Interval between Antivirus database updates
1 day

Devices should check for new Endpoint Manager events every
5 minutes

Endpoint Manager should check device restrictions are active every
5 minutes

Siren playing duration
20 seconds

Enable client uninstall protection
Disabled

Allow devices to access application repositories
Disabled

The following sections provide more details on each area:

- Email Notifications, Templates and Custom Variables
    - Configure Email Templates
    - Configure Email Notifications
    - Create and Manage Custom Variables
    - Create and Manage Registry Groups
    - Create and Manage COM Groups
    - Create and Manage File Groups
- Endpoint Manager Portal Configuration
  - Import User Groups from LDAP
  - Configure Communication and Security Client Settings
    - Configure the EM Android Client
      - Configure Android General Settings
      - Configure Android Client Antivirus Settings
      - Add Google Cloud Messaging (GCM) Token
    - Add Apple Push Notification Certificate
    - Configure EM Windows Client
      - Configure Communication Client Settings
      - Configure Client Security Settings
  - Manage Endpoint Manager Extensions
  - Configure Endpoint Manager Reports
  - Configure Device Removal Settings

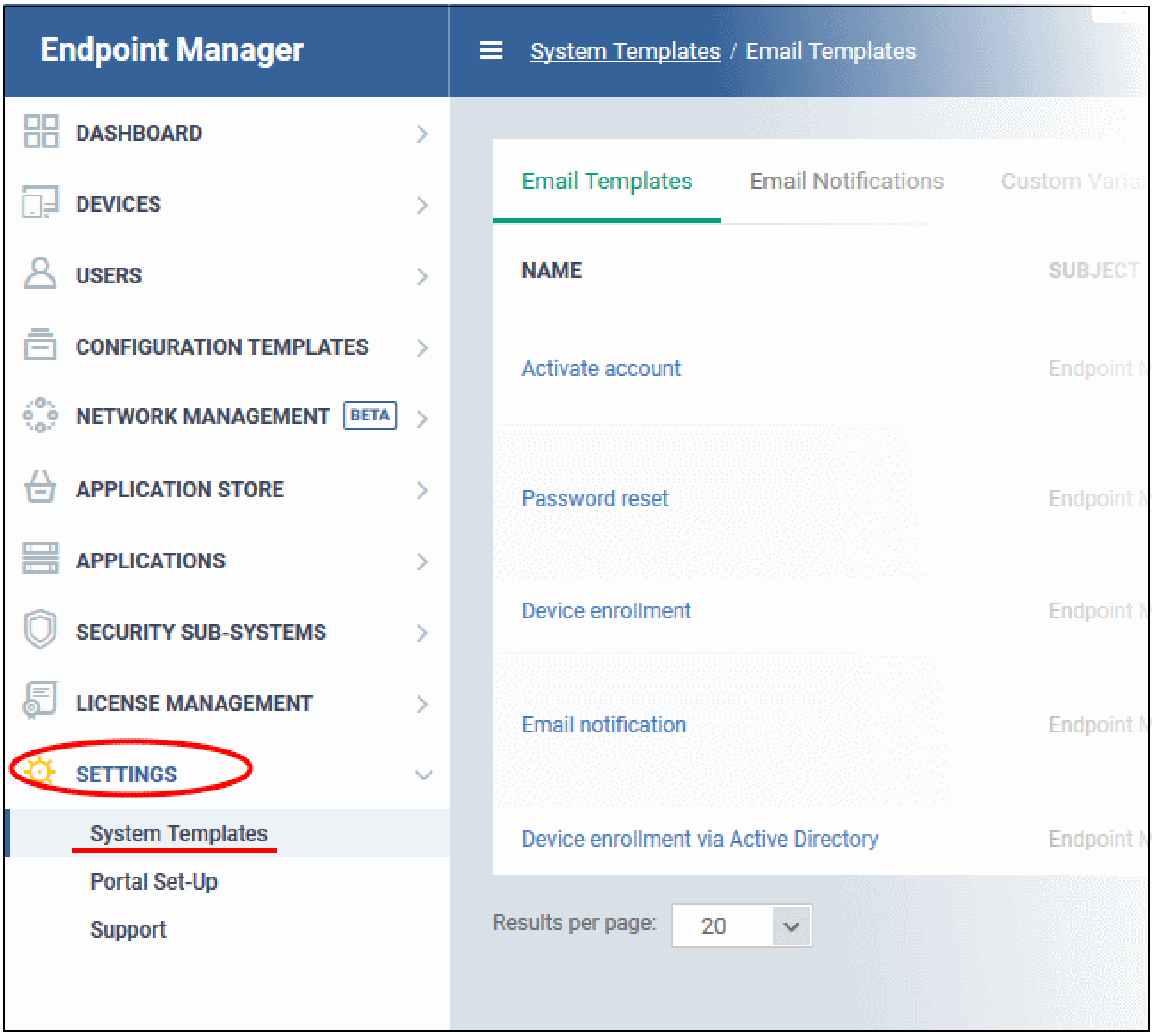
- Configure Two-Factor Authentication Settings
- Set-up Administrator's Time Zone and Language

- Integrate Apple DEP with Endpoint Manager
- View Version and Support Information

# 11.1.Email Notifications, Templates and Custom Variables

- Click 'Settings' > 'System Templates'

The templates, variables and file groups in this section are used / referenced by various Endpoint Manager modules. For example, a custom variable which represents a user's name can be inserted into an email template. The notifications tab lets you choose the recipients of alerts, and the events upon which they should be sent.



| NAME | SUBJECT |
|---|---|
| Activate account | Endpoint M |
| Password reset | Endpoint M |
| Device enrollment | Endpoint M |
| Email notification | Endpoint M |
| Device enrollment via Active Directory | Endpoint M |

The following sections explain how to:

- Configure Email Templates
- Configure Email Notifications
- Create and Manage Custom Variables
- Create and Manage Custom Variables

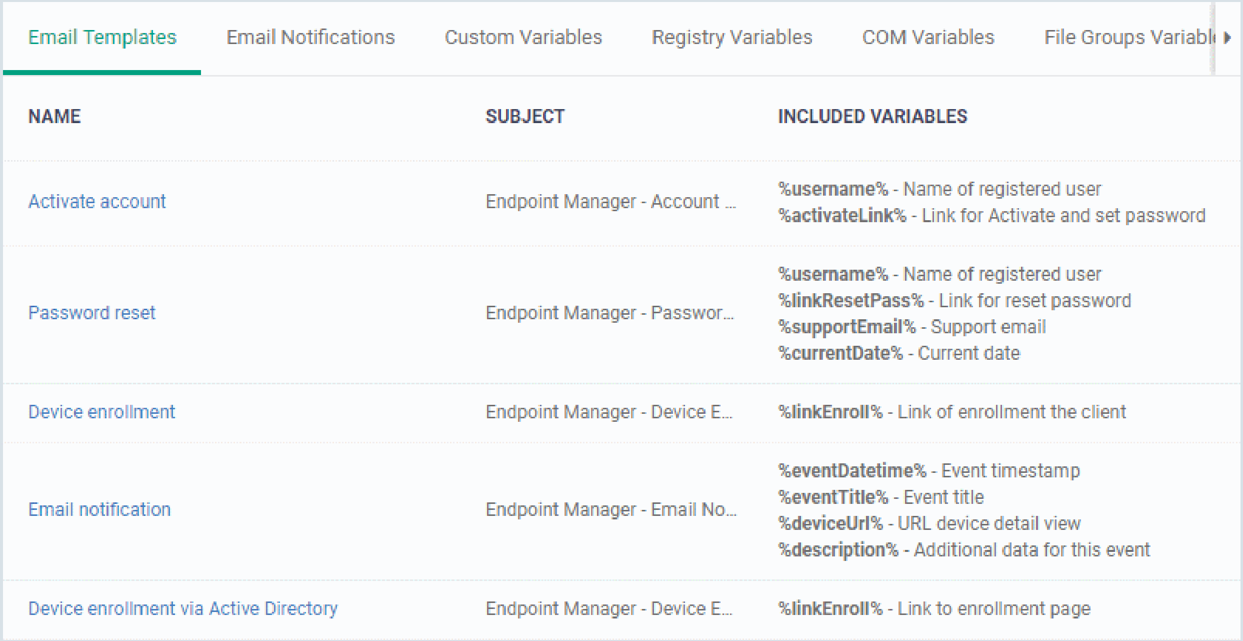
- Create and Manage COM Groups
- Create and Manage File Groups

### 11.1.1. Configure Email Templates

- Click 'Settings' > 'System Templates' > 'Email Templates'
- Email templates contain the content for Endpoint Manager's system emails. Examples include templates for account activation, device enrollment and password resets.
- Due to their importance, you cannot delete these templates or create new templates. You can, however, modify the contents of a template. The preset email templates are:
    - **Activate account** - Sent only to new admins to activate their account. These mails are not sent to people with the 'User' role (your end-users/device owners). Users receive a different enrollment mail which you can disable during the csv user import process if required.
    - **Password reset** - Sent to any user that requests a new password.
    - **Device enrollment** - Sent to end-users. Contains instructions on how to add their device to Endpoint Manager.
    - **Email notification** - Sent on the occurrence of certain events. You can configure the recipients of these mails, and the events that generate them, in the 'Email Notifications' tab.
    - **Device enrollment via Active Directory** - Sent to users imported from Active Directory when you enroll their devices. You can enable or disable this mail in 'Settings' > 'Portal Set-Up' > 'Active Directory' > click the name of an LDAP domain > 'Enroll' > 'Edit'.

## View and manage email templates

- Click 'Settings' > 'System Templates'.
- Click the 'Email Templates' tab



| NAME | SUBJECT | INCLUDED VARIABLES |
|---|---|---|
| Activate account | Endpoint Manager - Account ... | **%username%** - Name of registered user<br>**%activateLink%** - Link for Activate and set password |
| Password reset | Endpoint Manager - Passwor... | **%username%** - Name of registered user<br>**%linkResetPass%** - Link for reset password<br>**%supportEmail%** - Support email<br>**%currentDate%** - Current date |
| Device enrollment | Endpoint Manager - Device E... | **%linkEnroll%** - Link of enrollment the client |
| Email notification | Endpoint Manager - Email No... | **%eventDatetime%** - Event timestamp<br>**%eventTitle%** - Event title<br>**%deviceUrl%** - URL device detail view<br>**%description%** - Additional data for this event |
| Device enrollment via Active Directory | Endpoint Manager - Device E... | **%linkEnroll%** - Link to enrollment page |

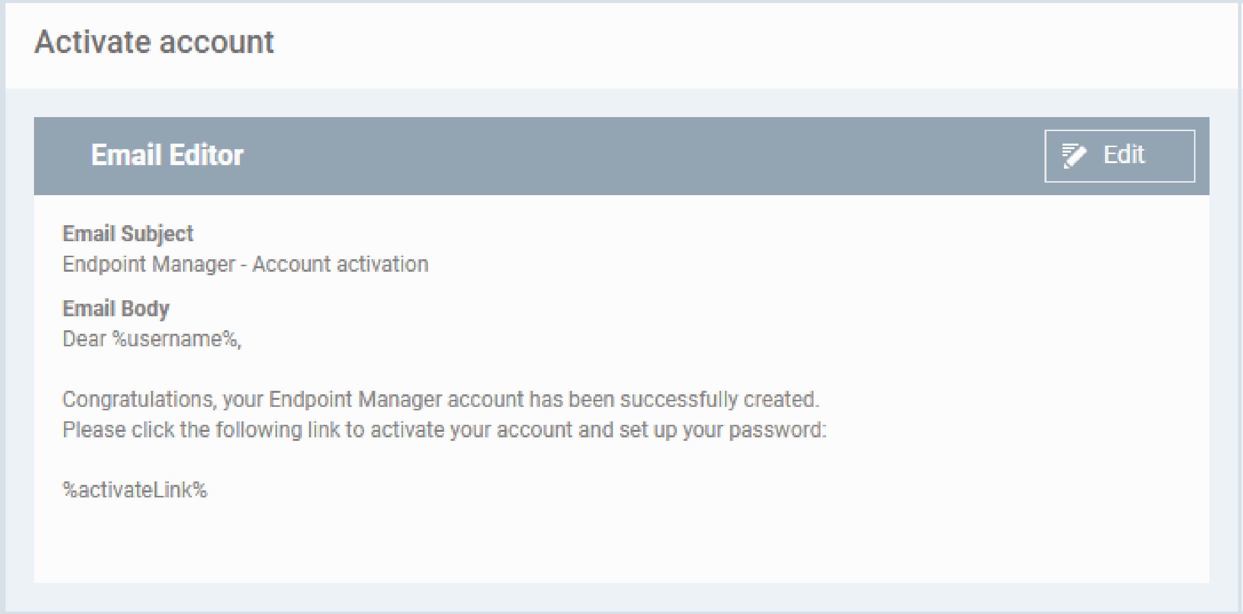
| Email Templates- Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Name | The label of email template. This cannot be changed. |

| | |
|---|---|
| | • Click the name of a email template to view and edit its content and variables.<br>• See **View and Manage an Email Template** for more details |
| Subject | The email subject. You can modify this as required. |
| Included Variables | Email variables are dynamic fields which reference data held elsewhere. For example, the %username% variable will actually show the real username of the email recipient.<br>• The 'Included Variables' column tells you the name and purpose of each variable in a template.<br>• You can add or remove variables if you edit the template.<br>• You can create your own variables in 'Settings' > 'System Templates' > 'Custom Variables'<br>• You can view other variables in the 'Registry variables', 'COM variables' and 'File Group variables' tabs. |

## View and Manage an Email Template

- Click 'Settings' > 'System Templates'
- Click the 'Email Templates' tab
- Click the name of the template that you want to edit

This opens the full email text. The 'Activate Account' template is shown below:



Activate account

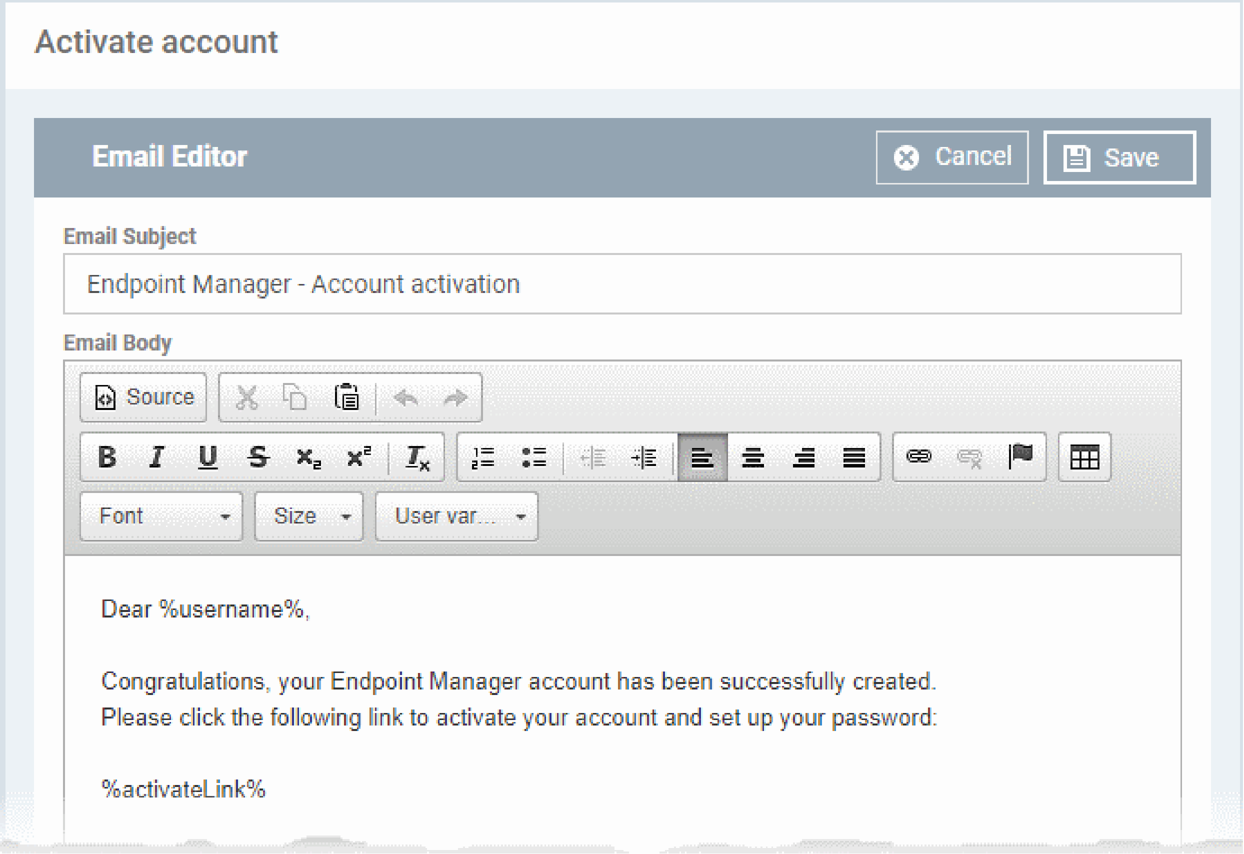
**Email Subject**
Endpoint Manager - Account activation

**Email Body**
Dear %username%,

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

%activateLink%

- Click the edit button if you want to modify the subject line, body text or variables.



Email Subject

Endpoint Manager - Account activation

Email Body

Dear %username%,

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

%activateLink%

- Edit the subject line and/or email content as required
- You can remove variables by simply deleting the %variable% from the body text.
- Insert a variable - Place your mouse cursor where you want the variable to appear. Click the 'User Variables' button to insert the variable.

**Note**: Each email template has a limited selection of user and device variables.

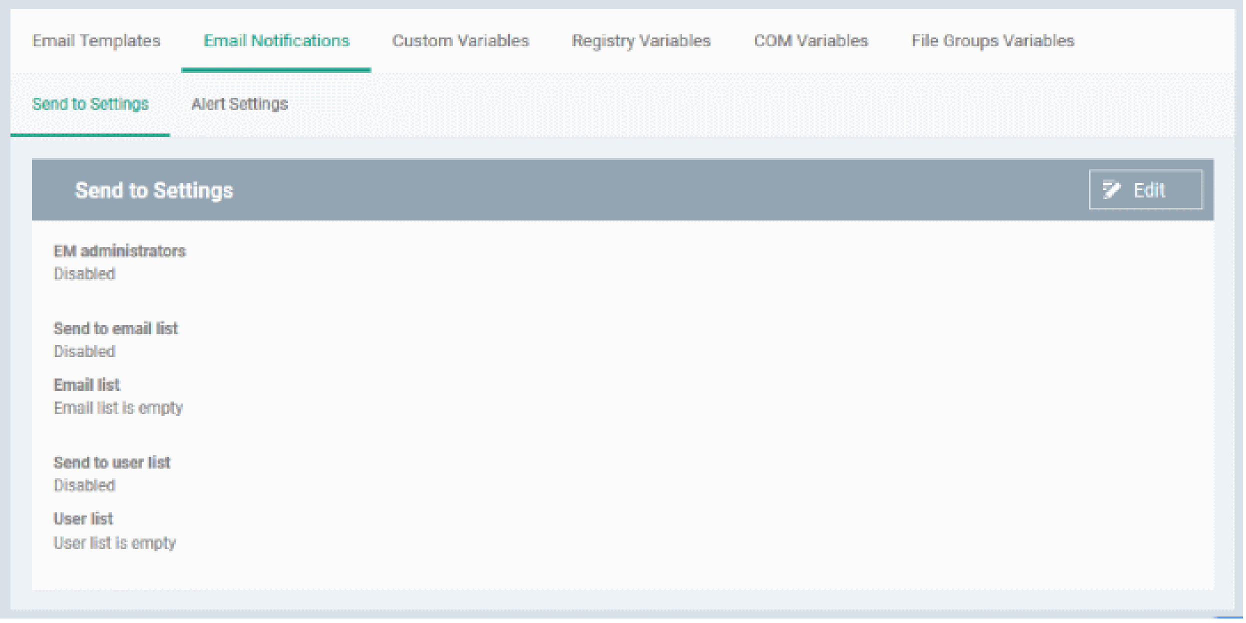
- Click 'Save'. You changes will take effect immediately.

### 11.1.2. Configure Email Notifications

- Click 'Settings' > 'System Templates' > 'Email Notifications'
- Endpoint Manager can send alert emails to admins and users when certain events happen.
- Example events include detection of a new threat, or when a mobile device is removed from management.
- The 'Email Notifications' tab lets you set alert recipients and specify which events are covered.
  - The 'Email Notification' template contains the actual content of the mail. Click 'Settings' > 'System Templates' > 'Email Templates' to view and edit this content.

**Configure email notifications**

- Click 'Settings' > 'System Templates'.
- Click the 'Email Notifications' tab



EM administrators
Disabled

Send to email list
Disabled

Email list
Email list is empty

Send to user list
Disabled

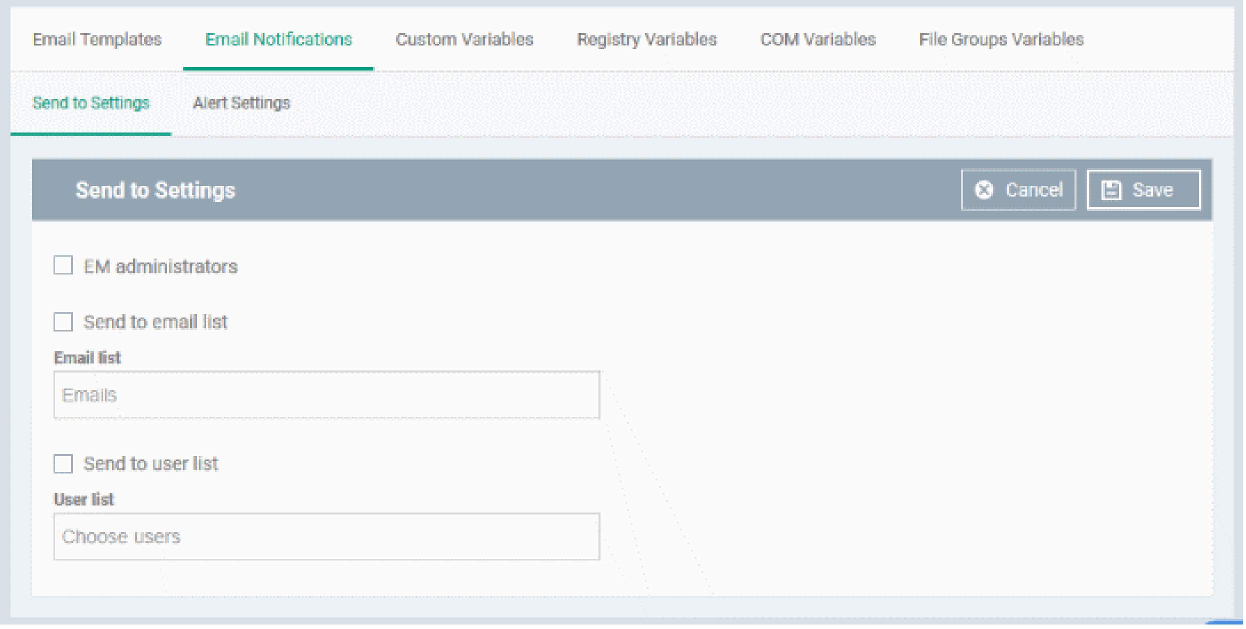
User list
User list is empty

The interface has two tabs:

- **Send to Settings** - Configure alert recipients
- **Alert Settings** - Select which events generate an alert

### Send to Settings

- Click the 'Edit' button at top-right to modify the list of recipients



□ EM administrators

□ Send to email list

Email list

Emails

□ Send to user list

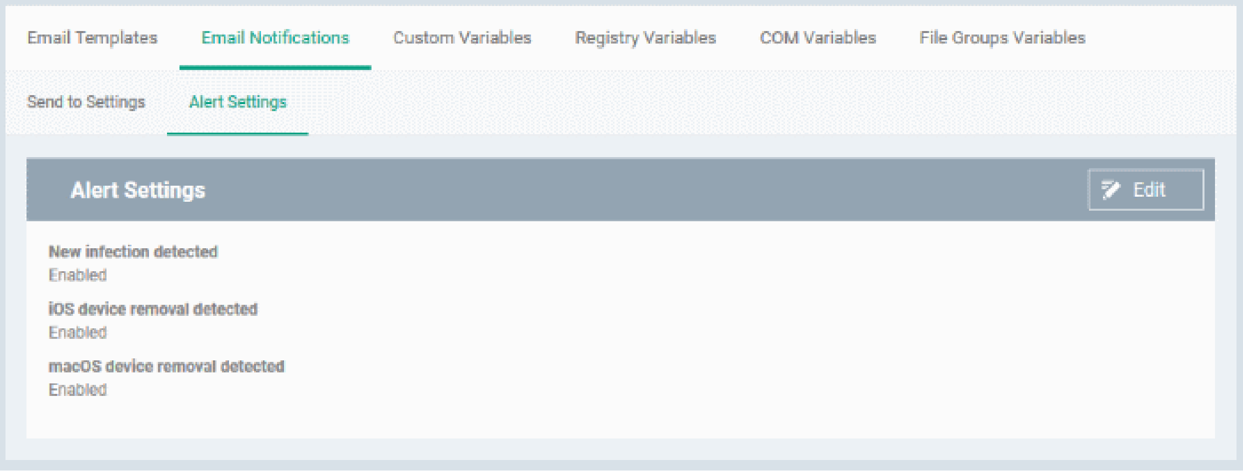
User list

Choose users

- **EM Administrators** - Send alerts to every Endpoint Manager admin
- **Send to Email List** - Type the email addresses of additional recipients. Press space after each address to enter another email address.
- **Send to User List** - Select users that have been added to endpoint manager. You can view a list of current users in 'Users' > 'User List'.

### Alert Settings

The alerts interface lets you select the events for which alerts are sent.



New infection detected
Enabled

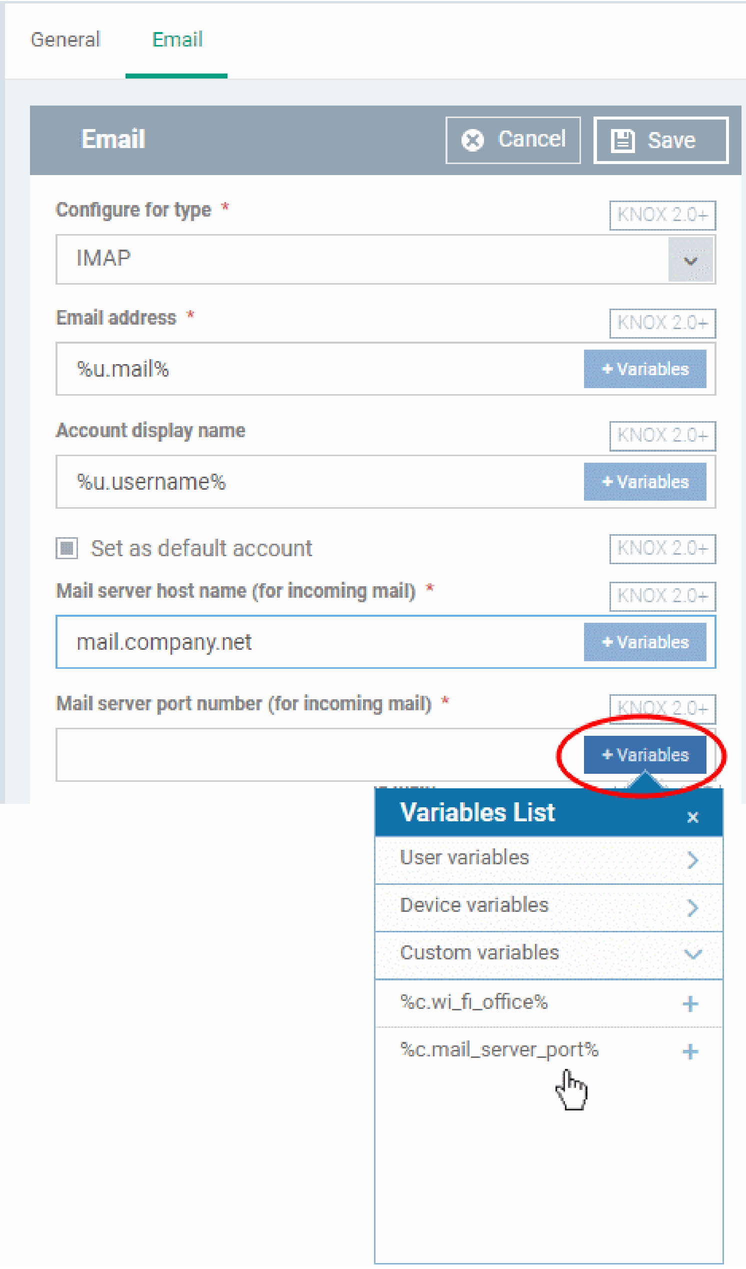
iOS device removal detected
Enabled

macOS device removal detected
Enabled

  - **New Infection Detected** - Sends an alert if malware is found on a managed device
  - **iOS Device Removal Detected** - Sends an alert if an iOS device is removed from management.
  - **Mac OS Device Removal Detected** - Sends an alert if a MAC is removed from management.
- Click the 'Edit' button at top-right to enable/disable specific alerts.

### 11.1.3. Create and Manage Custom Variables

- Click 'Settings' > 'System Templates' > 'Custom Variables'
- A variable is a string of text which references a piece of data. For example, '%u.mail% is the variable for a user's email address.
- Variables can be added to email templates and profiles. They will dynamically populate the field with the piece of data requested.
- There are three types of variable - 'User', 'Device' and 'Custom'. The first two types, 'user' and 'device', are preset and cannot be edited.
  - **User variables** - Fetch data about a specific user. For example, the user's login name or email address.
  - **Device variables** - Fetch data about a specific device. For example, the IMEI number or phone number of a mobile device.
  - **Custom variables** - Fetch data about an item of your choice. For example, you could create a custom variable called 'secure_mail_port' with a value of '2525'. You can then use this variable in the 'Email' section of an Android or iOS profile. If you decide to change the port number in future, you can easily update all devices by changing the variable value instead of editing multiple profiles.
- Illustration - Click 'Configuration Templates' > 'Profiles' > open an Android profile > Click 'Add Profile Section' > 'Email'. Click the 'Variables' button in any field to view available variables:



Configure for type *: IMAP

Email address *: %u.mail%

Account display name: %u.username%

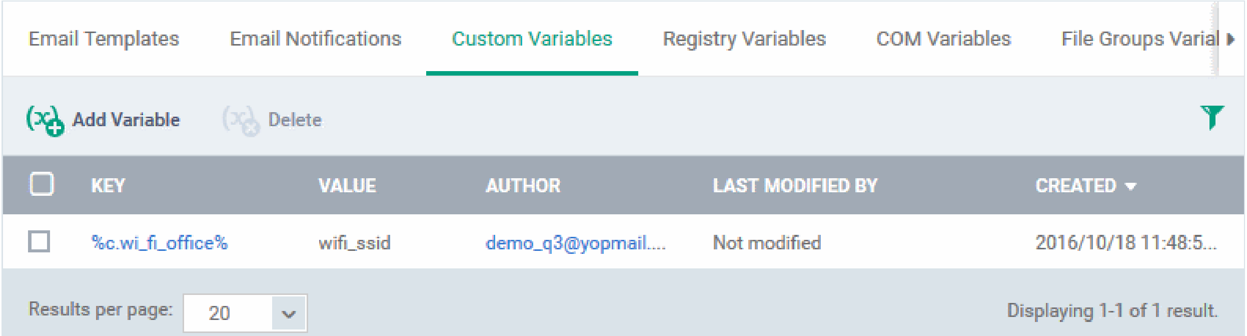
□ Set as default account

Mail server host name (for incoming mail) *: mail.company.net

Mail server port number (for incoming mail) *

## View, manage and create custom variables

- Click 'Settings' > 'System Templates'
- Click the 'Custom Variables' tab



| □ | KEY | VALUE | AUTHOR | LAST MODIFIED BY | CREATED |
|---|---|---|---|---|---|
| □ | %c.wi_fi_office% | wifi_ssid | demo_q3@yopmail.... | Not modified | 2016/10/18 11:48:5... |

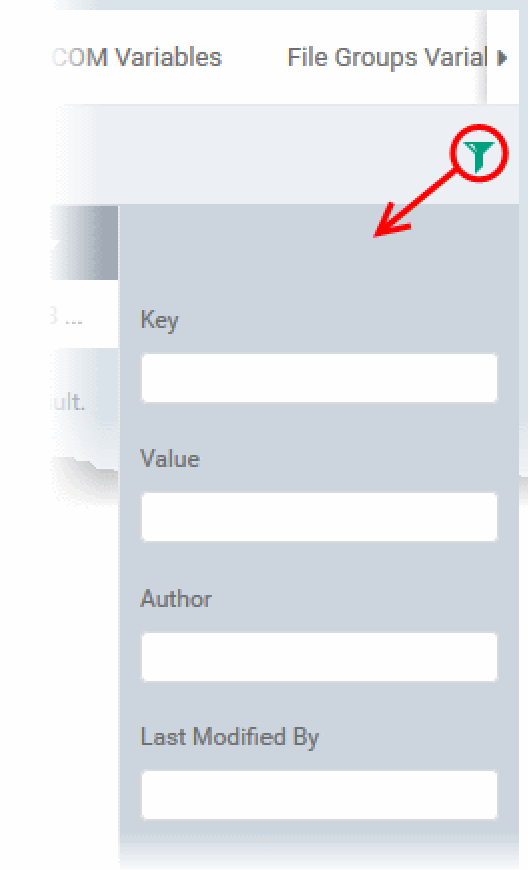
Results per page: 20

Displaying 1-1 of 1 result.

| Custom Variables - Column Descriptions | |
|---|---|
| **Column Heading** | **Description** |
| Key | Friendly name which identifies the variable.<br>• You select a variable you want to use by choosing the key name.<br>• Click the key name to edit the key value. |
| Value | The value to be substituted for the key |
| Author | The admin who created the custom variable.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Last Modified By | The admin who most recently edited the variable.<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |
| Created | The date and time the custom variable was added. |

## Sorting, Search and Filter Options

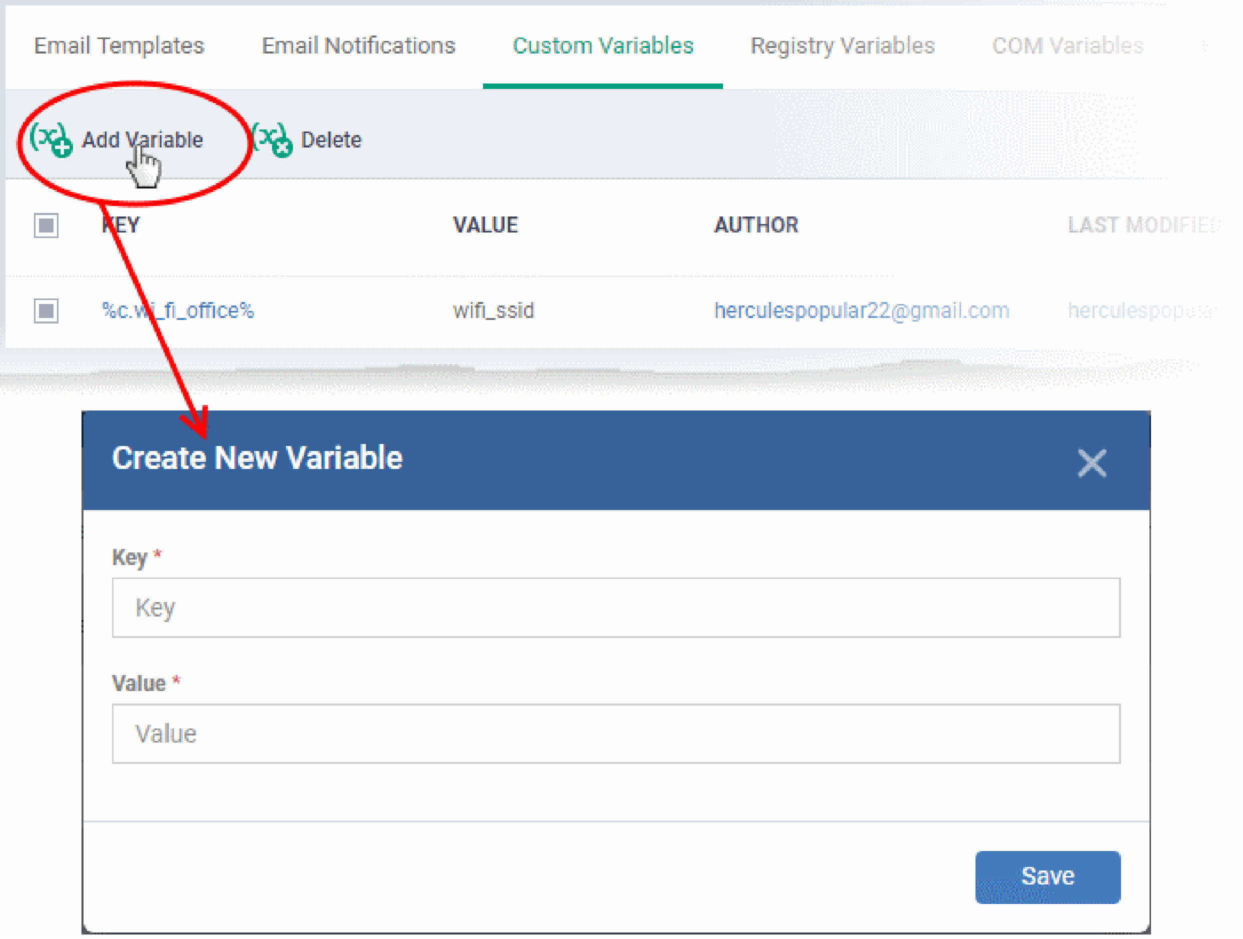
- Click on any of the column headers to sort the items in ascending/descending order of entries in that column
- Click the funnel icon to search for custom variables based on filter parameters



**To create a new custom variable**

- Click 'Settings' > 'System Templates' > 'Custom Variables' tab

- Click 'Add Variable'

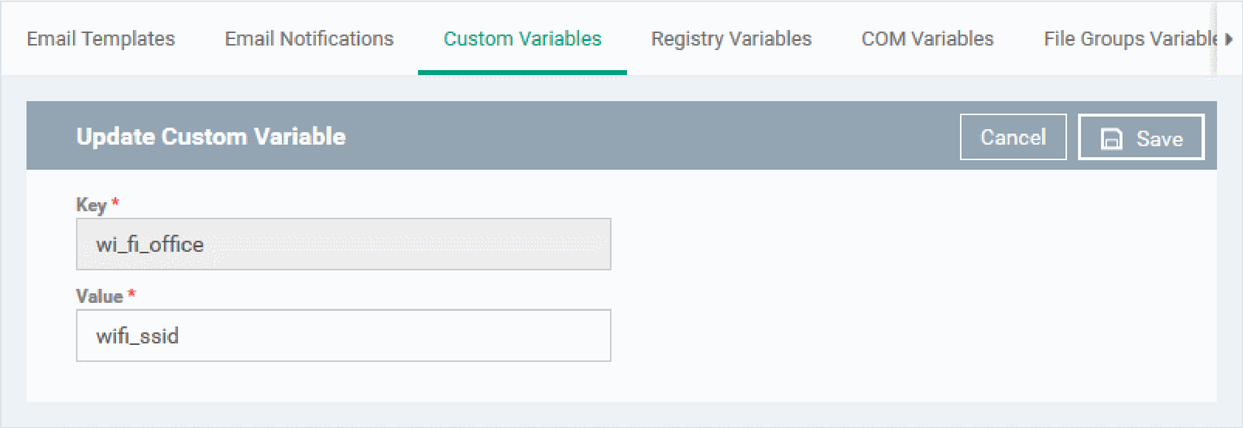


  - **Key** - Enter a name for variable as it should appear in the Variables drop-down
  - **Value** - Enter the value to be fetched for the key
- Click 'Save' to add the variable to EM.
- Repeat the process to add more variables.

**To edit a Custom Variable**

- Click on the name of the 'Custom Variable' to be edited.

The 'Update Custom Variable' screen will appear.



Key *
wi_fi_office

Value *
wifi_ssid

- Edit the 'Key' and 'Value' as required and click the 'Save' button.

**To remove a Custom Variable**

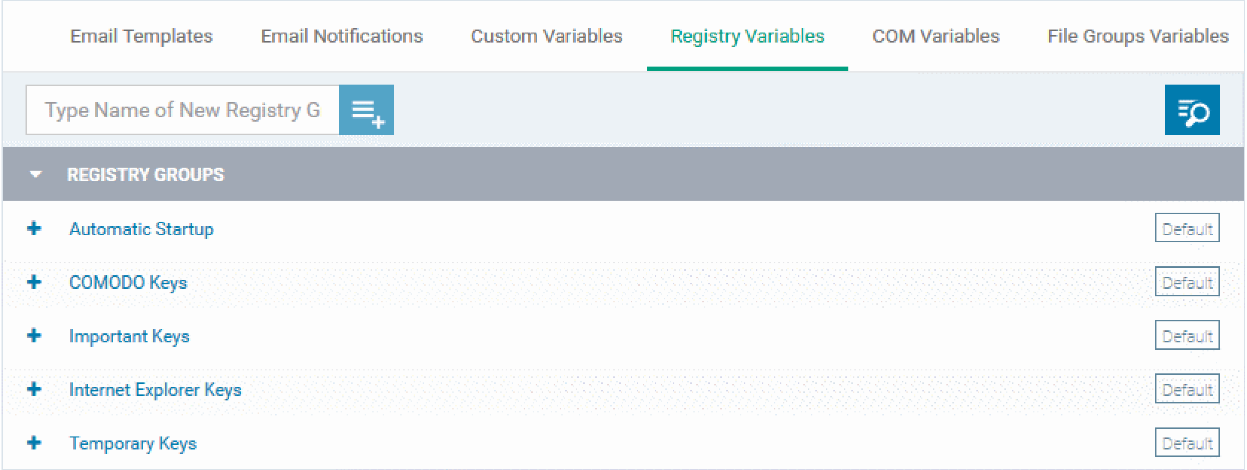
- Select the custom variable to be removed from the list and click the 'Delete' button at the top

## 11.1.4. Create and Manage Registry Groups

- Click 'Settings' > 'System Templates' > 'Registry Variables'
- The 'Registry Variables' tab contains references to pre-defined and custom registry groups.
  - A registry group is a collection of registry keys with similar attributes or scope.
  - For example, the 'Important Keys' group contains keys which are essential to the security and stability of the operating system. The 'Automatic Startup' group contains keys which load at Windows boot.
- Registry groups are useful when you want to apply an action to an entire class of keys. For example, you can exclude a registry group from containment when creating a profile.
- You can add new groups and edit existing groups as required.
- Groups in this interface are available for selection when configuring a Windows profile.

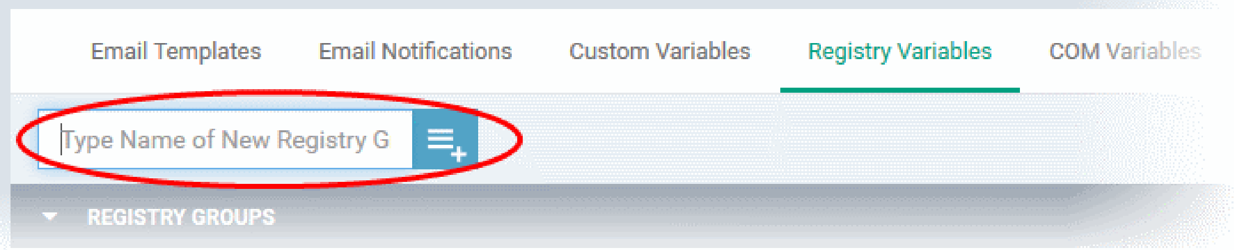
**Open the 'Registry Groups' interface**

- Click 'Settings' > 'System Templates'
- Click the 'Registry Variables' tab



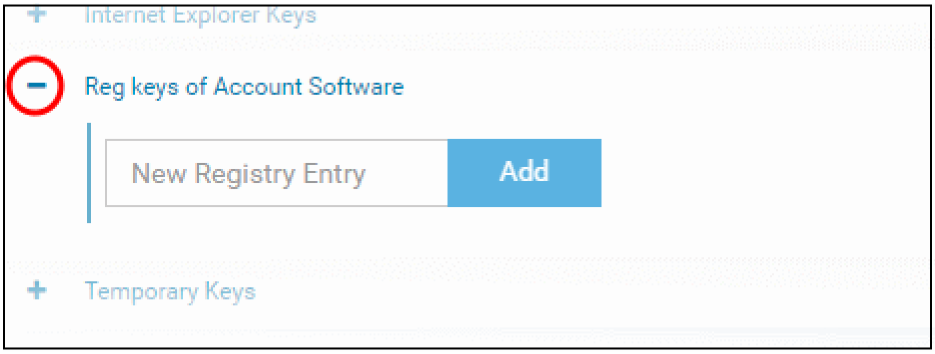
**Add a new Registry group**

- Enter the name of the group in the 'New Registry Group' field and click the '+' button.

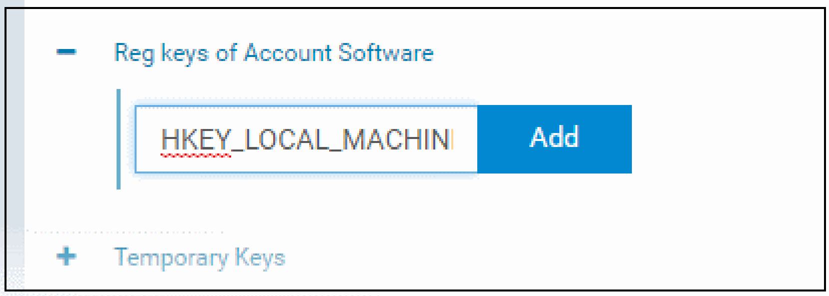


The new group will be added to the list. The next step is to add registry keys to the group.

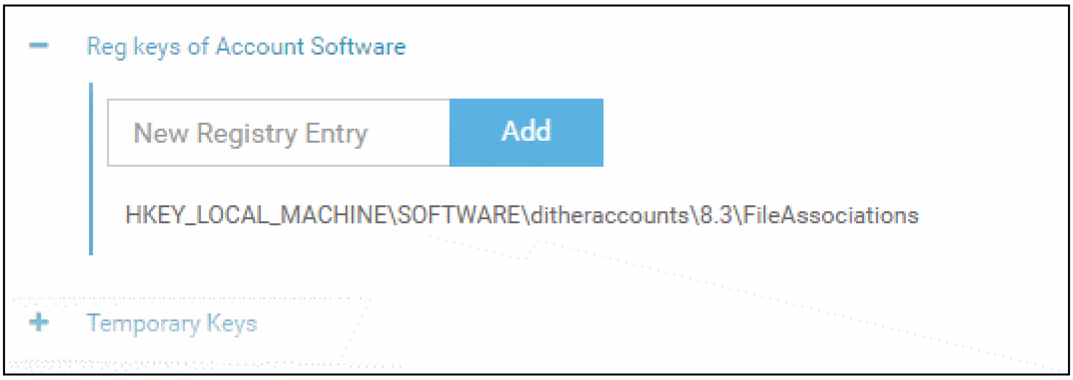
- Click the '+' at the left of the group name



- Enter the path of the registry key/value in the New Registry Entry field and click 'Add'

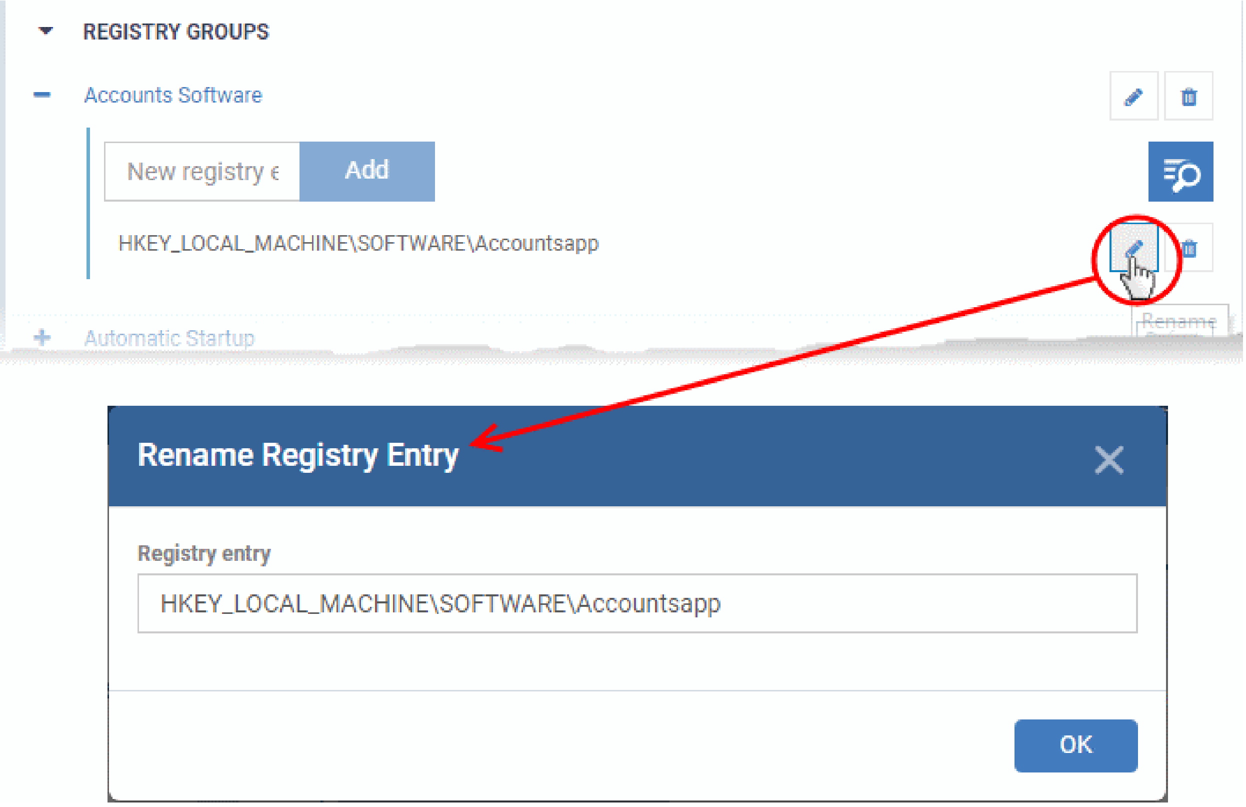


The key will be added to the group.



HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations

- Repeat the process to add more keys and values to the group.
- Click the 'Edit' icon if you want to modify the value:



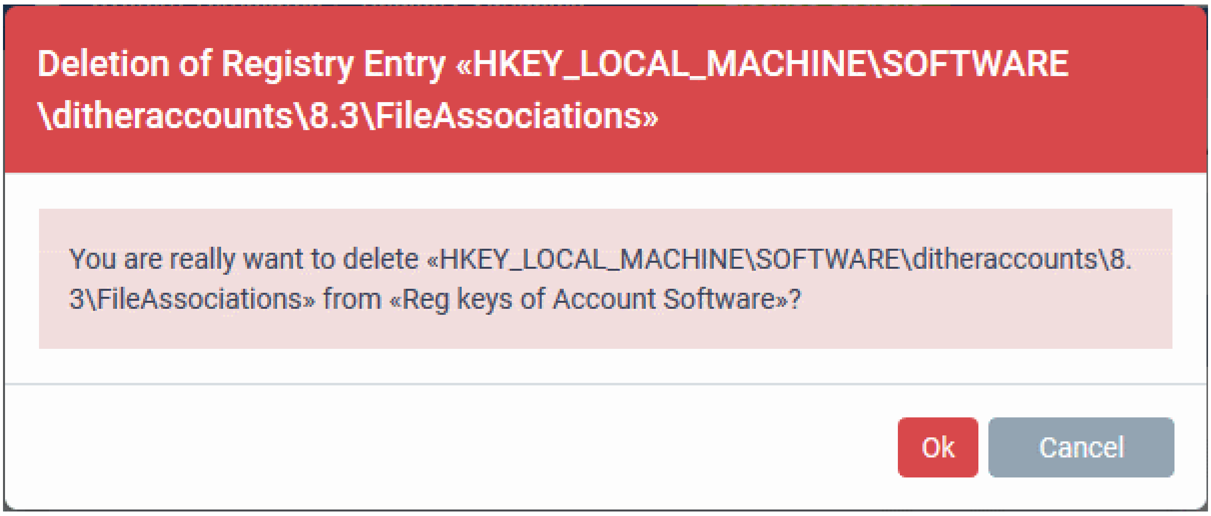
HKEY_LOCAL_MACHINE\SOFTWARE\Accountsapp

Rename Registry Entry

Registry entry: HKEY_LOCAL_MACHINE\SOFTWARE\Accountsapp

  - Edit the entry and click 'OK' to save your changes

- Click the trash can icon to remove a key:

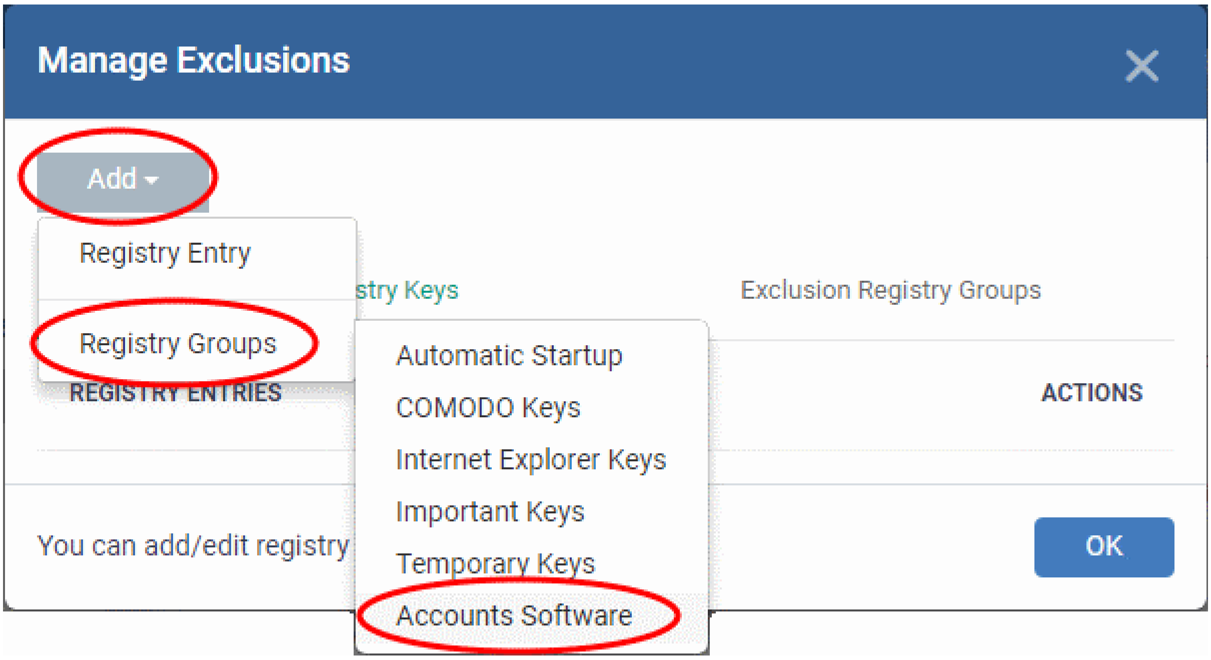


Deletion of Registry Entry «HKEY_LOCAL_MACHINE\SOFTWARE \ditheraccounts\8.3\FileAssociations»

You are really want to delete «HKEY_LOCAL_MACHINE\SOFTWARE\ditheraccounts\8.3\FileAssociations» from «Reg keys of Account Software»?

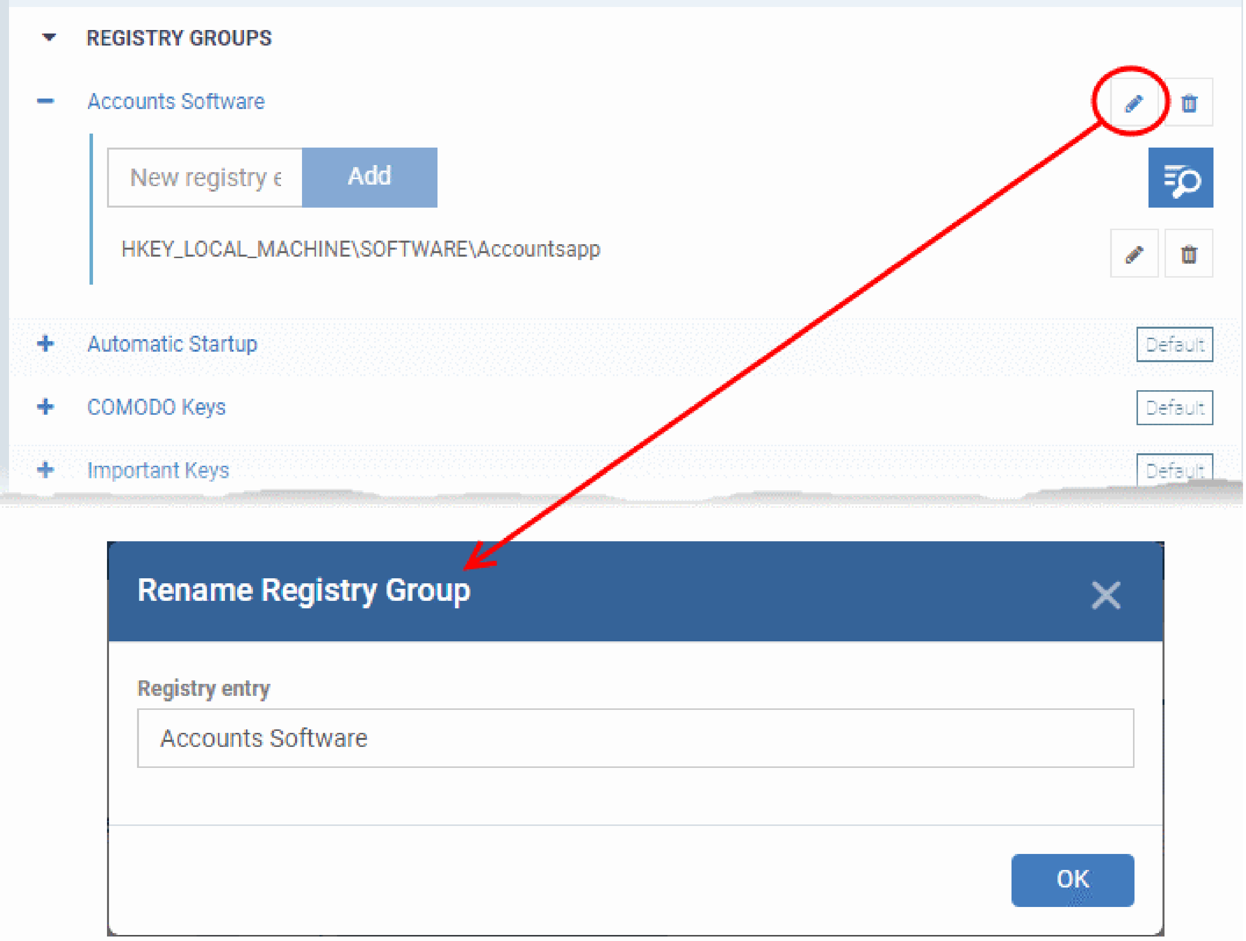
- Click 'OK' in the confirmation dialog.

The new registry group is now available for selection when configuring a Windows Profile. For example, in 'Containment' > 'Settings' > 'Do not virtualize access to the specified registry keys/values' > 'Exclusions'.



**Edit the name of a Registry Group**

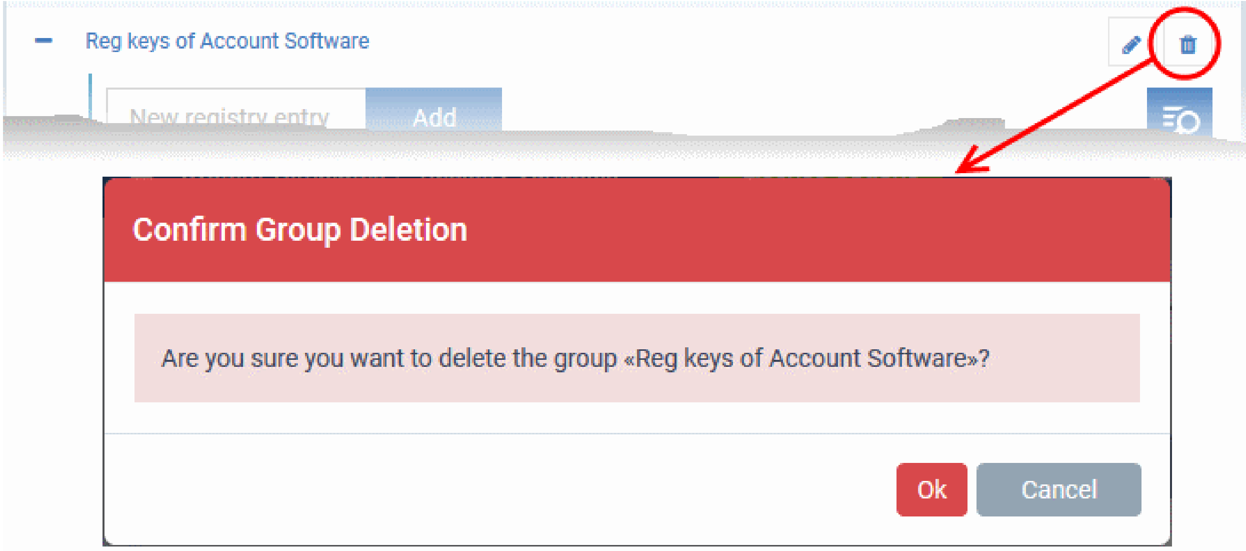
- Click the 'Edit' icon beside the Registry Group



- Enter the new name for the group in the 'Rename Registry Group' dialog and click 'OK'

**Remove a Registry Group**

- Click the trash can icon beside the Registry Group



Confirm Group Deletion

Are you sure you want to delete the group «Reg keys of Account Software»?

A confirmation dialog will appear.

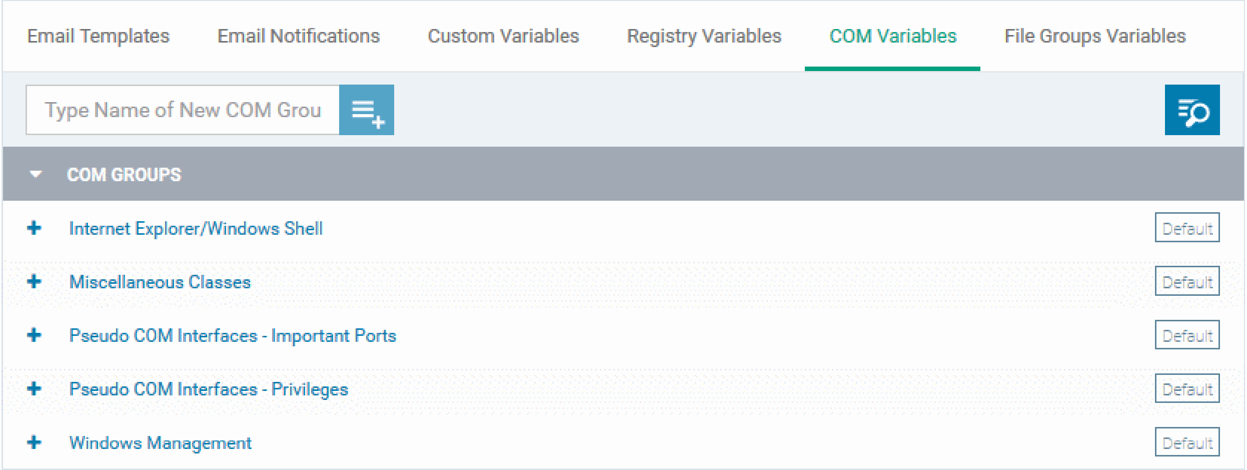
- Click OK in the confirmation dialog.

## 11.1.5. Create and Manage COM Groups

- Click 'Settings' > 'System Templates' > 'COM Variables'
- Each COM group is a handy collection of COM interfaces falling under a certain category.
- Endpoint Manager ships with a set of predefined COM Groups that are available for use in configuration profiles, for example to add a COM group to the 'Protected Objects' list in the HIPS settings of a Windows profile. If required, You administrators can add new COM Groups, edit and manage them.
- The 'COM Variables' tab in the 'System Templates' interface lets you 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.

**Open the 'COM Groups' interface**

- Click 'Settings' > 'System Templates'
- Click the 'COM Variables' tab



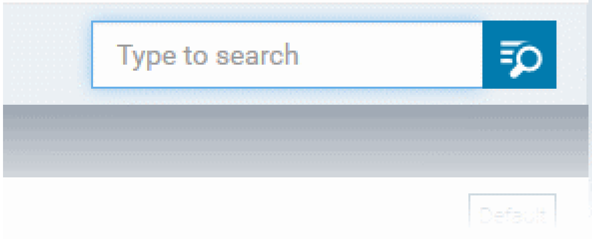
COM GROUPS

| | |
|---|---|
| Internet Explorer/Windows Shell | Default |
| Miscellaneous Classes | Default |
| Pseudo COM Interfaces - Important Ports | Default |
| Pseudo COM Interfaces - Privileges | Default |
| Windows Management | Default |

The list of pre-defined and user-defined COM groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

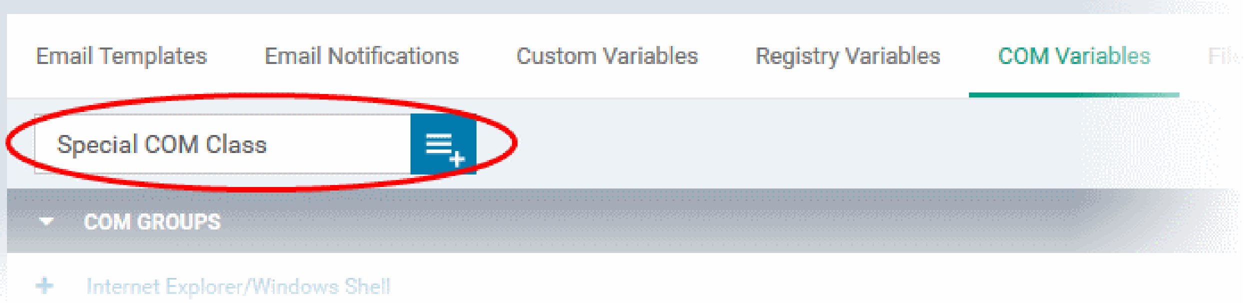
## Sorting, Search and Filter Options

- Click 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



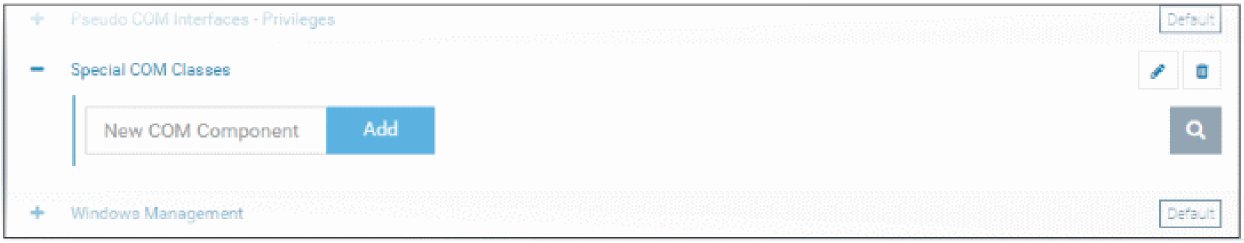
### Add a new COM group

- Enter the name of the new COM group and click the '+ ' button:

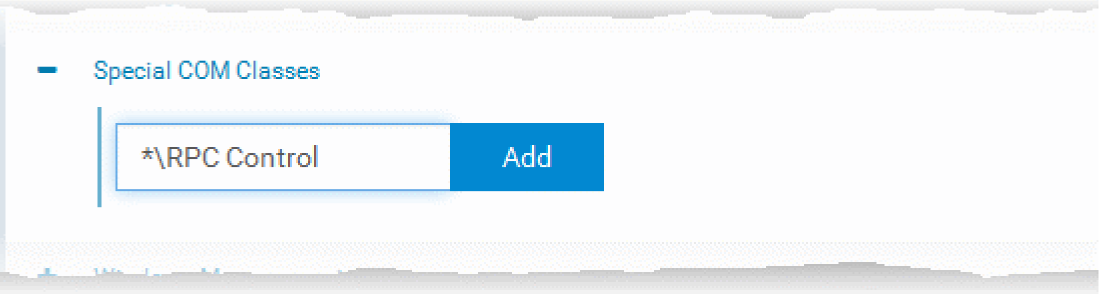


The new group will be added to the list. The next step is to add COM classes to the group.

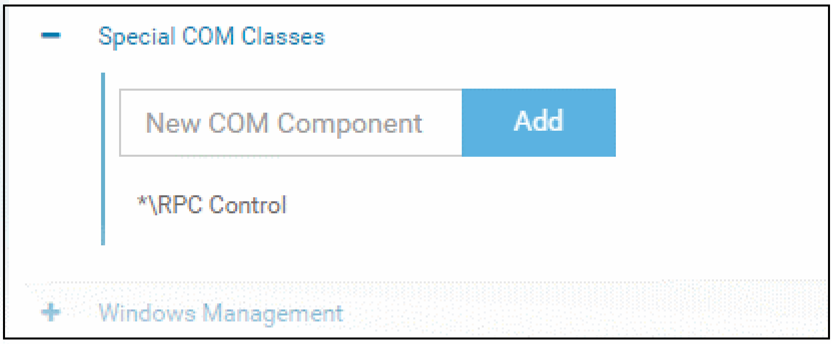
- Click the '+' at the left of the group name



- Enter the COM classes to be added to the group, in the 'New COM Component' field and click 'Add'

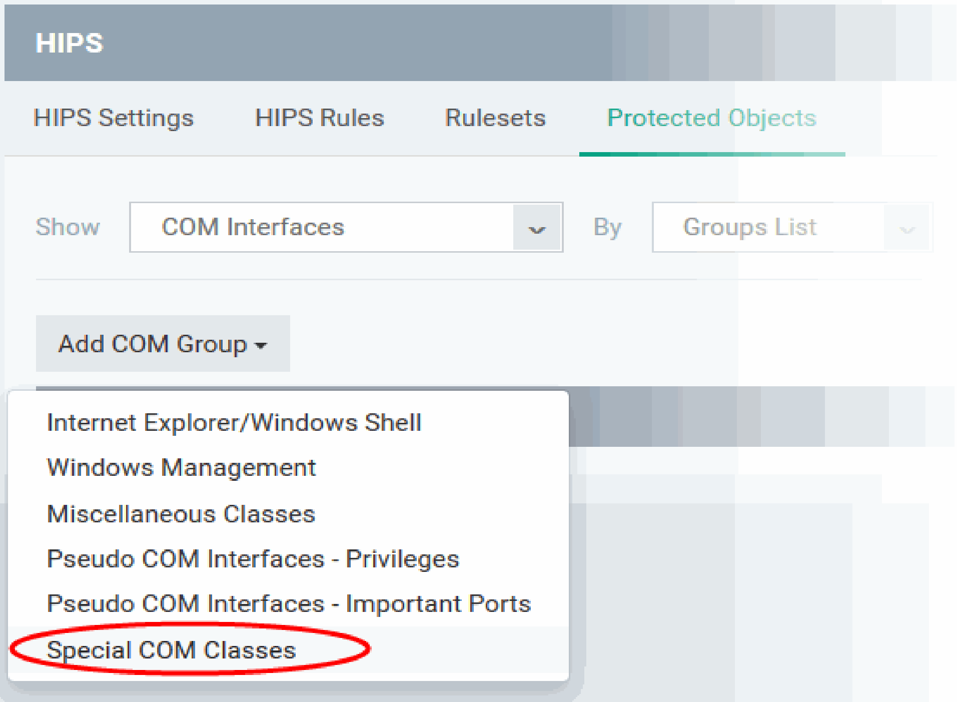


The COM class will be added to the group.

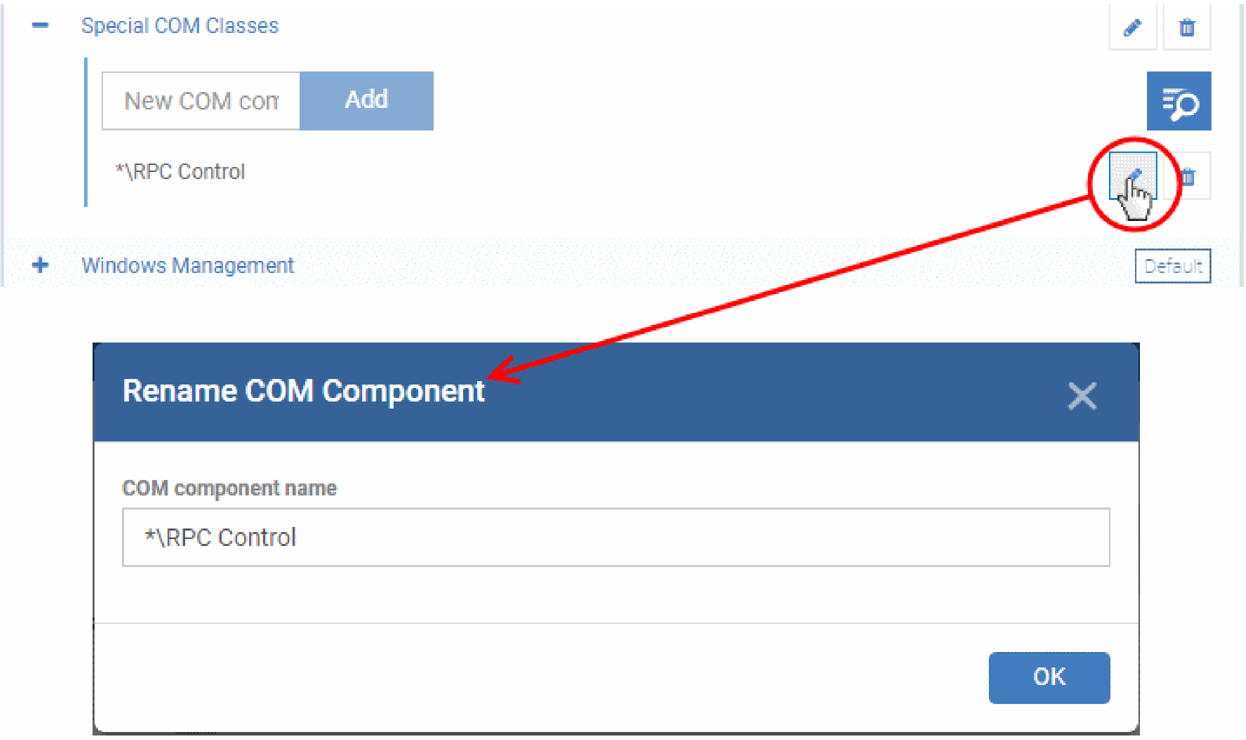


- Repeat the process to add more COM classes to the group.

Once a COM group is added, it will be available for selection while configuring a Windows Profile, for example in the 'HIPS' > 'Protected Objects' > 'Groups List' interface.



- Click the pencil icon beside the class name to edit a class in the group,



*\RPC Control

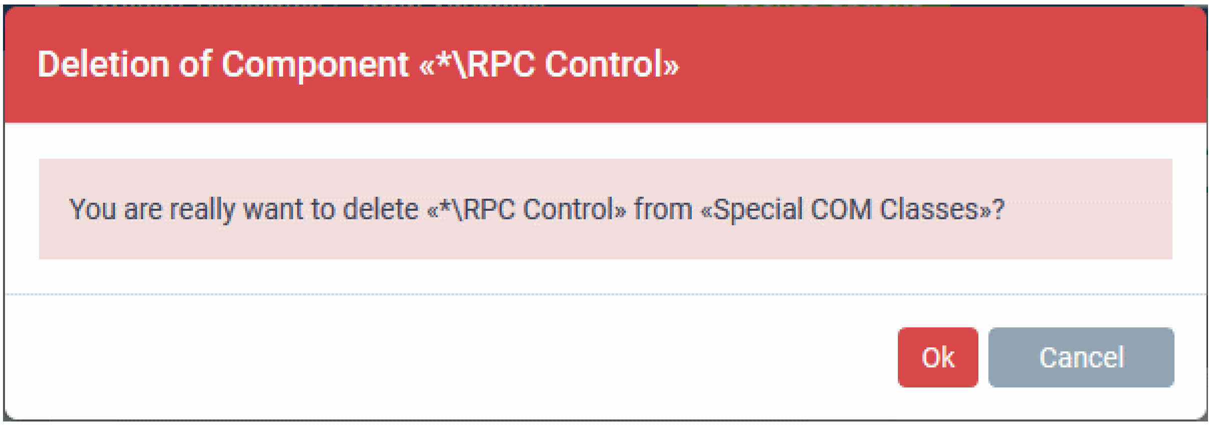
Rename COM Component

COM component name

*\RPC Control

- Edit the entry and click 'OK' to save your changes

- Click the trash can icon beside the COM component name to remove the COM class added by mistake or an unwanted class



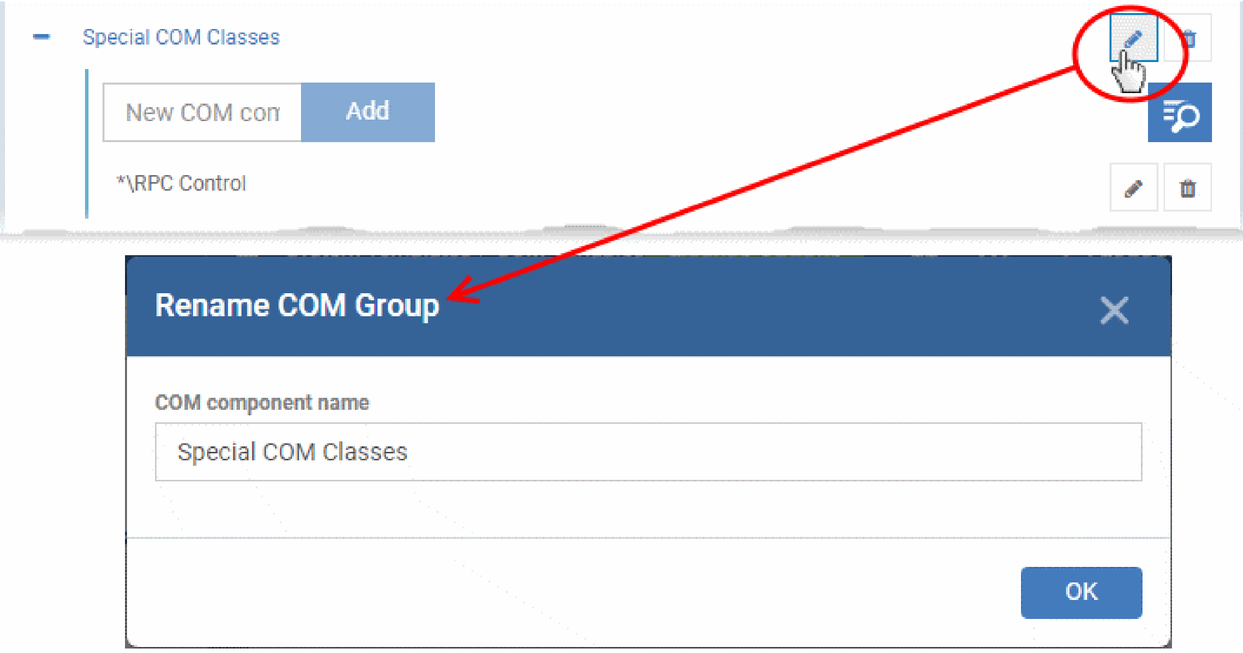
Deletion of Component «*\RPC Control»

You are really want to delete «*\RPC Control» from «Special COM Classes»?

- Click 'OK' in the confirmation dialog.

**Edit the name of a COM Group**

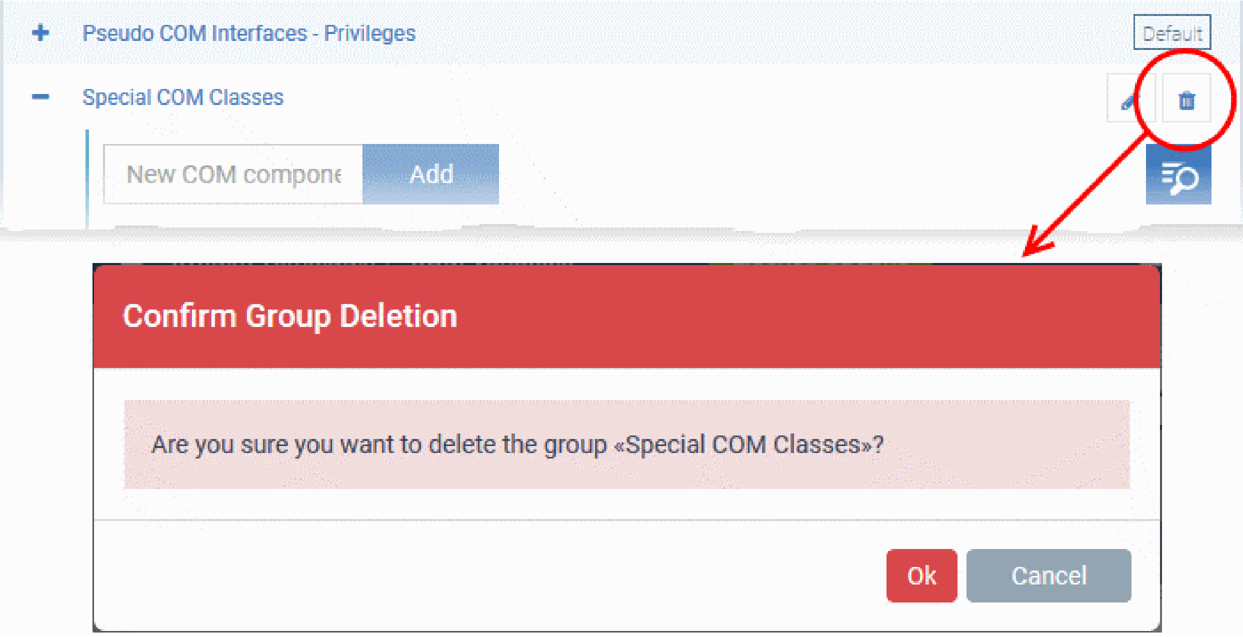
- Click the pencil icon beside the COM Group



- Enter the new name for the group in the Rename COM Group dialog and click 'OK'

**Remove a COM Group**

- Click the Trash can icon beside the COM Group



Are you sure you want to delete the group «Special COM Classes»?

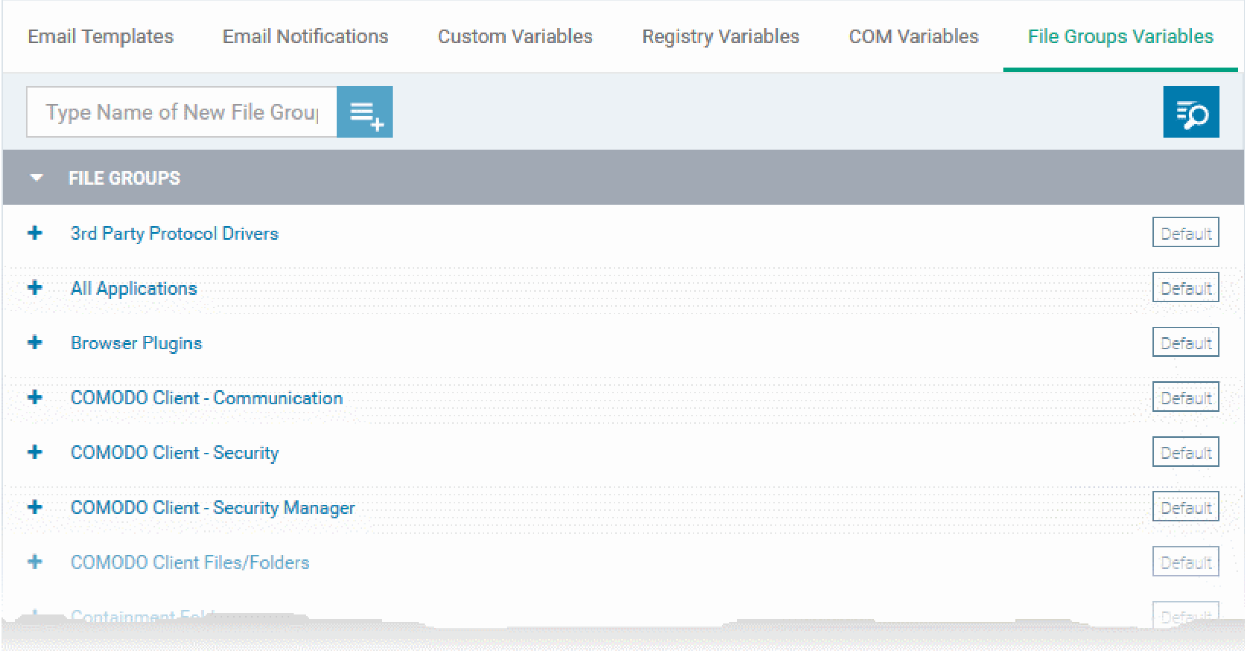
- Click 'OK' in the confirmation dialog.

## 11.1.6. Create and Manage File Groups

- Click 'Settings' > 'System Templates' > 'File Groups Variables'
- File groups are handy, predefined groupings of one or more file types. You can select a file group as the target of various functions and rules. For example, you scan specify that a file group is excluded from AV scans, or that everything in a file group is auto-contained when run.
- Endpoint Manager ships with a set of predefined file groups, and allows you to create your own.
- After creating a group, it becomes available for selection when configuring a Windows profile.

**Open the 'File Groups' interface**

- Click 'Settings' > 'System Templates'
- Click the 'File Groups Variables' tab

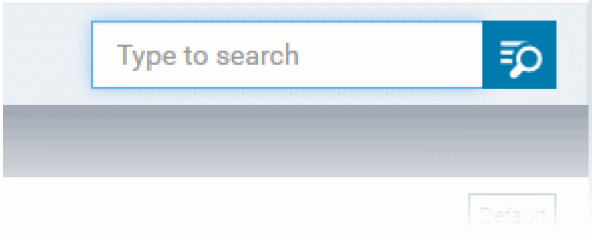


| FILE GROUPS | |
|---|---|
| 3rd Party Protocol Drivers | Default |
| All Applications | Default |
| Browser Plugins | Default |
| COMODO Client - Communication | Default |
| COMODO Client - Security | Default |
| COMODO Client - Security Manager | Default |
| COMODO Client Files/Folders | Default |
| Containment Fold | Default |

'Default' groups cannot be edited or deleted.

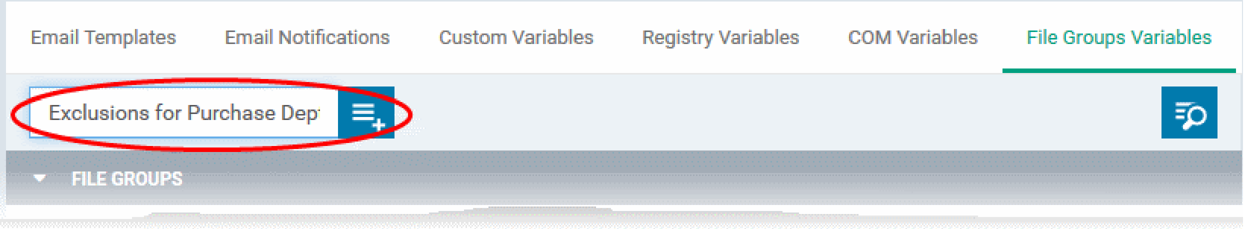
### Sort, Search and Filter Options

- Click the 'File Groups' column header to 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



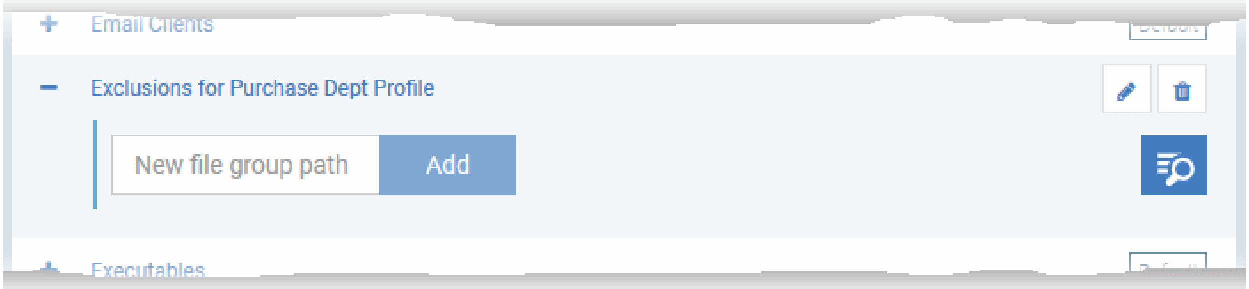
**Add a new File group**

- Enter a name for the group and click the '+'.button. The group name should ideally identify the content or purpose of the group:



The new group will be added to the list. The next step is to add files to the group.

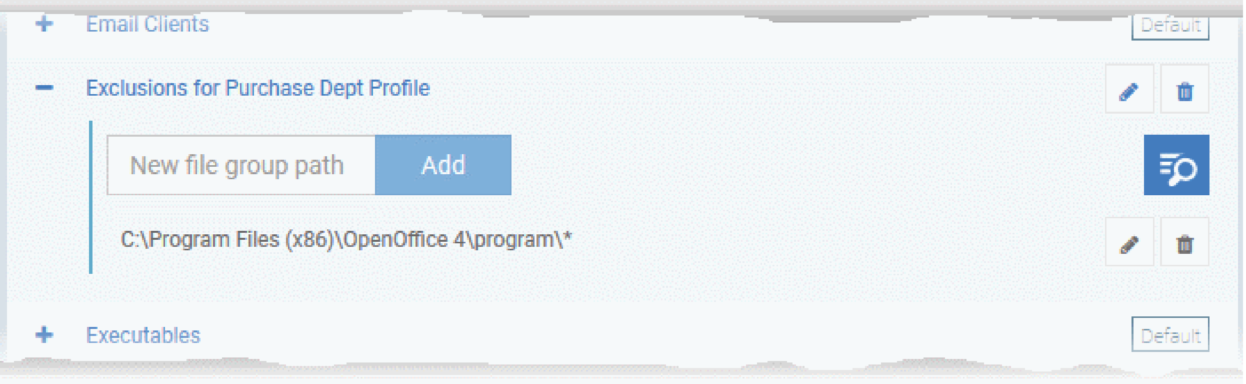
- Click the '+' at the left of the group name



- Enter the full standard folder/file path of the file to be added to the group in the 'New File Group Path' field and click 'Add'

**Tip**: To include all the files in a folder, place the wildcard character in the place of file name in the folder path. For example: " C:\My Files* "

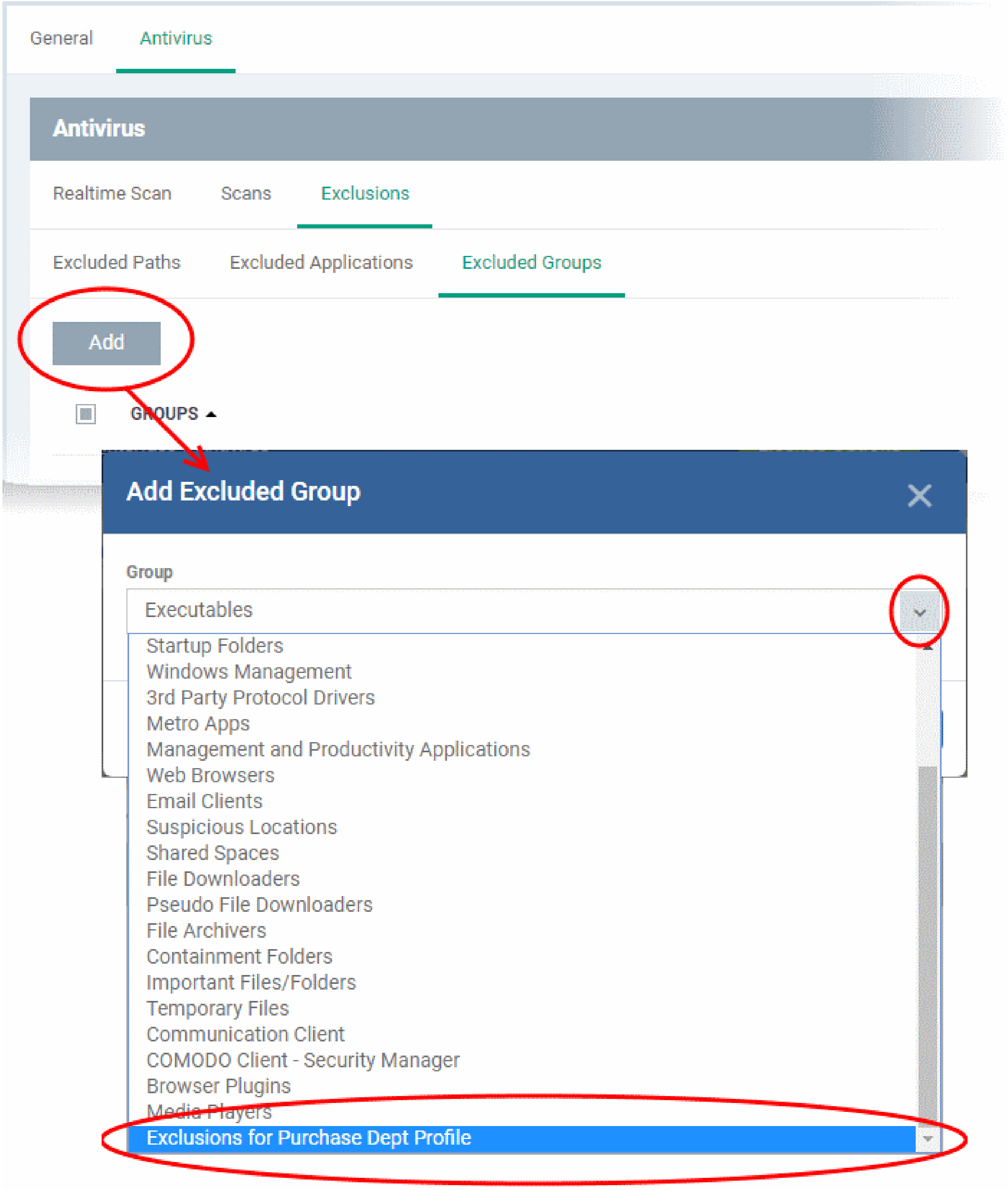
The file(s) will be added to the group.



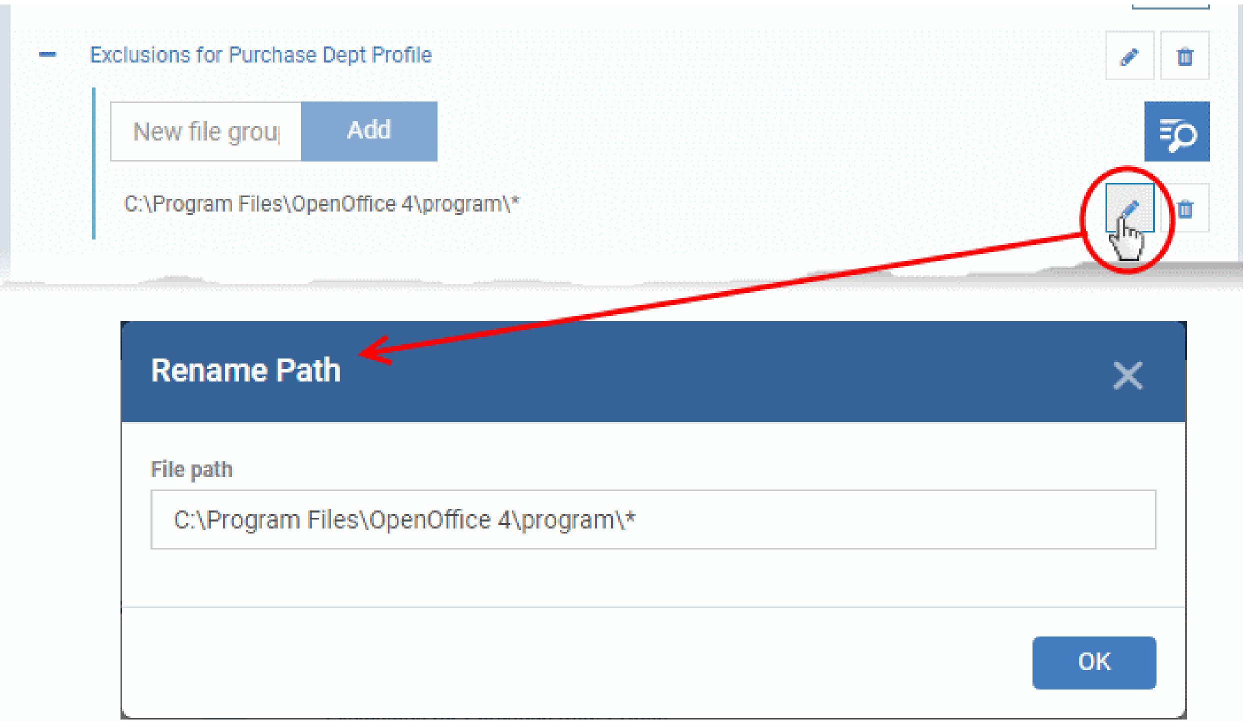
C:\Program Files (x86)\OpenOffice 4\program\*

- Repeat the process to add more files to the group.

Once a File Group is added, it will be available for selection in applicable settings interfaces for defining the File Groups, example, for adding to 'Exclusions' list in 'Antivirus Settings' panel in the 'Windows Profile' interface.



- Click the pencil icon beside the file name to edit the files in the group



Exclusions for Purchase Dept Profile

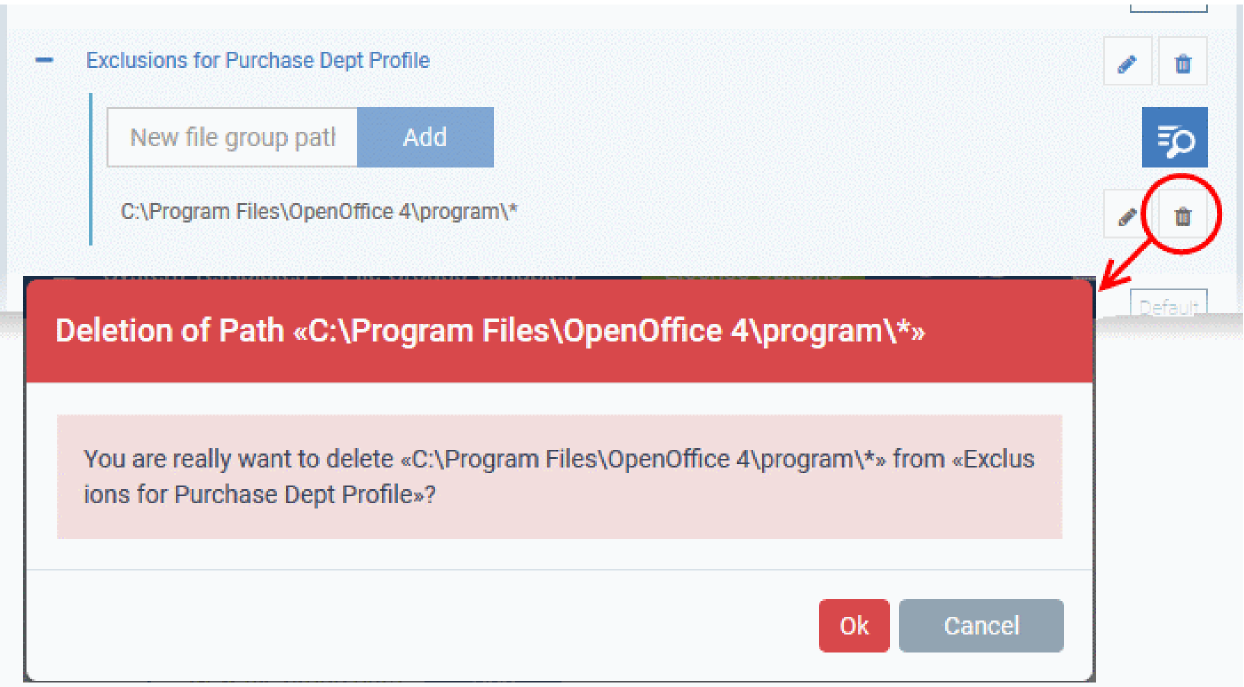
C:\Program Files\OpenOffice 4\program\*

Rename Path

File path: C:\Program Files\OpenOffice 4\program\*

- Edit the file path in the 'Rename Path' dialog and click 'OK'.

- Click the trash can icon beside the file name to remove the file added by mistake or an unwanted file from the group.



Exclusions for Purchase Dept Profile

C:\Program Files\OpenOffice 4\program\*

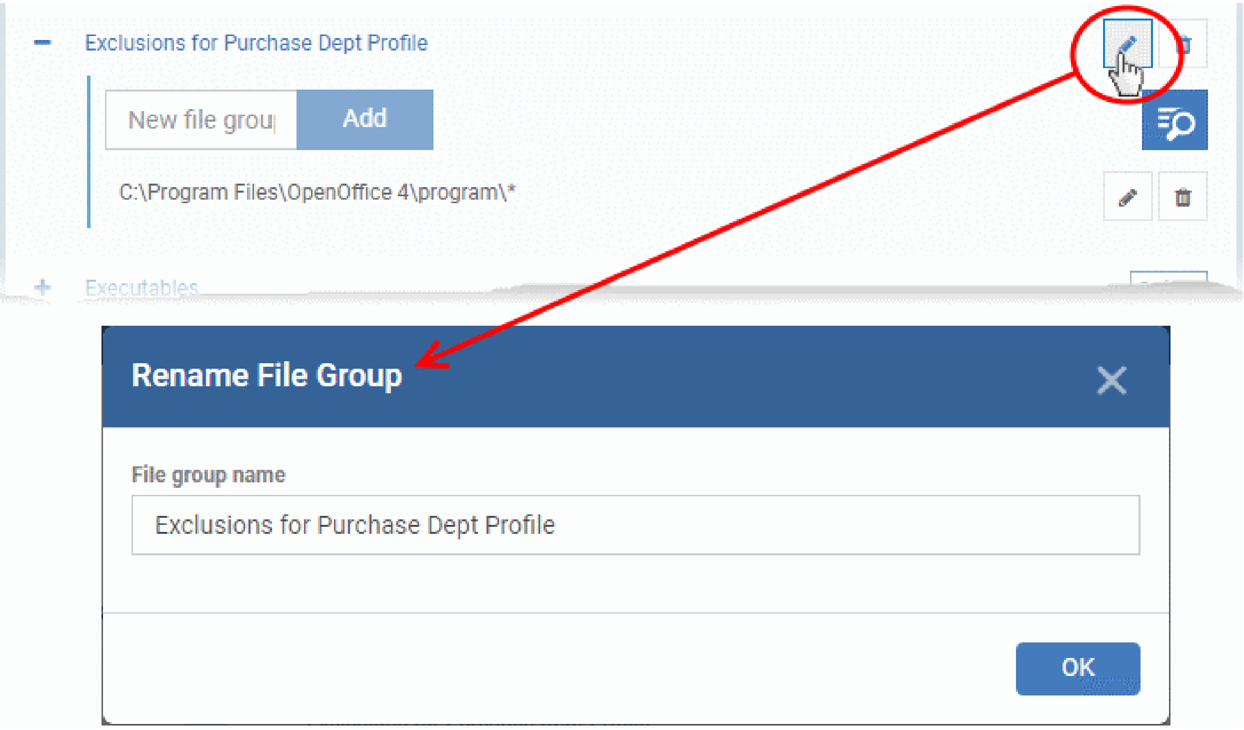
Deletion of Path «C:\Program Files\OpenOffice 4\program\*»

You are really want to delete «C:\Program Files\OpenOffice 4\program\*» from «Exclusions for Purchase Dept Profile»?

- Click OK in the confirmation dialog

**Edit the name of a File Group**

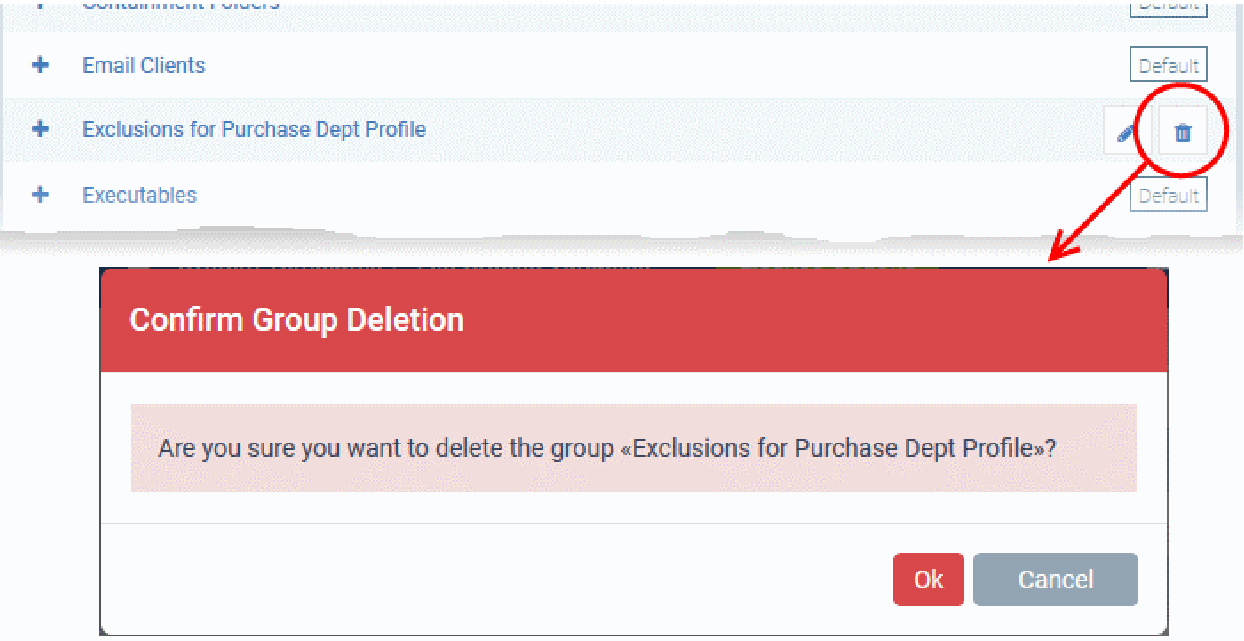
- Click the 'Edit' icon beside the file group


Exclusions for Purchase Dept Profile
New file grou
Add
C:\Program Files\OpenOffice 4\program\*
Executables
Rename File Group
File group name
Exclusions for Purchase Dept Profile
OK

- Enter the new name for the group in the 'Rename File Group' dialog and click 'OK'

**Remove a File Group**

- Click the trash can icon in the group row:


Email Clients
Default
Exclusions for Purchase Dept Profile
Executables
Default
Confirm Group Deletion
Are you sure you want to delete the group «Exclusions for Purchase Dept Profile»?
Ok
Cancel

A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

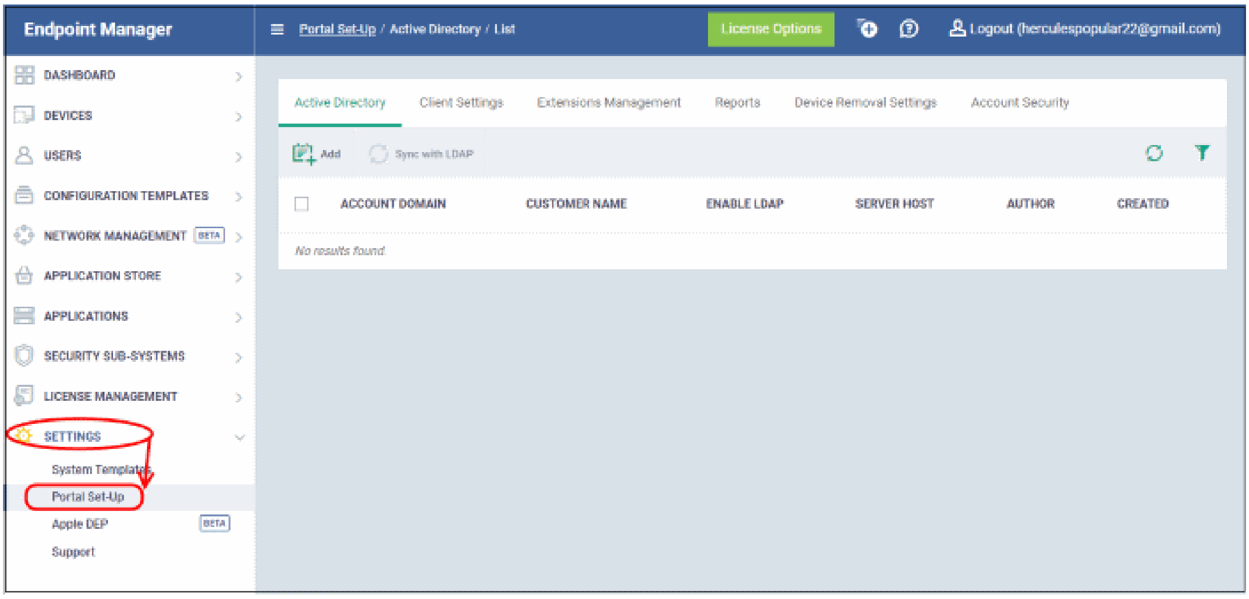
# 11.2. Endpoint Manager Portal Configuration

- Click 'Settings' > 'Portal Set-up'

The portal set-up area lets you configure core settings which are important to the operation of Endpoint Manager.

From here you can:

- Integrate Active Directory so you can import users and devices from your domain
- Add Apple and Google certificates so Endpoint Manager can communicate with iOS and Android devices
- Configure client settings, reports, two-factor logins, admin time-zones, and more.



| □ | ACCOUNT DOMAIN | CUSTOMER NAME | ENABLE LDAP | SERVER HOST | AUTHOR | CREATED |
|---|---|---|---|---|---|---|

*No results found.*

Use the following links to learn more about each setting:

- Import User Groups from LDAP
- Configure Communication and Security Client Settings
  - Configure the EM Android Client
    - Configure Android General Settings
    - Configure Android Client Antivirus Settings
    - Add Google Cloud Messaging (GCM) Token
  - Add Apple Push Notification Certificate
  - Configure EM Windows Client
    - Configure Communication Client Settings
    - Configure Client Security Settings
- Manage Endpoint Manager Extensions
- Configure Endpoint Manager Reports
- Set-up Administrators Time Zone and Language

## 11.2.1. Import User Groups from LDAP

There are two ways to add users to Endpoint Manager:

1. Manually add users:
    - Enroll one user at a time

- Import multiple users from a .csv file

2. Import user groups from Active Directory (AD) servers

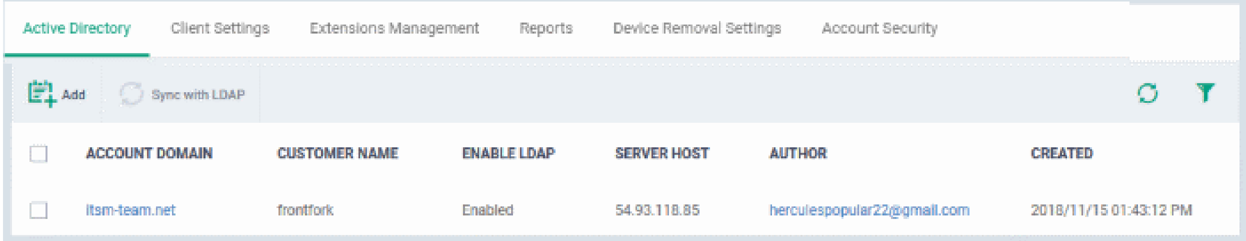
Endpoint Manager can be configured to access your AD server through the Lightweight Directory Access Protocol (LDAP). You can add multiple LDAP accounts.

**Process in brief:**

- Add an LDAP server by specifying its IP address, domain and the login credentials of the AD server:
  - Click 'Settings' > 'Portal Set-Up' > select the 'Active Directory' tab > Click 'Add'
- Once added, users and user groups in the AD directory will be visible in the 'Active Directory' interface:
  - Click 'Settings' > 'Portal Set-Up' > select the 'Active Directory' tab > Click on an AD domain name > Click the 'User Groups' tab
- Select the users and groups you wish to import
- Assign roles to users/user groups as required
- Synchronize LDAP with Endpoint Manager
- The selected users/user groups will be imported and placed into respective groups in EM
- The 'User List' and 'User Groups' interfaces let you view/manage users and enroll user devices. See **Users and User Groups** for more details.

**To open the Active Directory interface**

- Click 'Settings' > 'Portal Set-Up'
- Click the 'Active Directory' tab



| □ | ACCOUNT DOMAIN | CUSTOMER NAME | ENABLE LDAP | SERVER HOST | AUTHOR | CREATED |
|---|---|---|---|---|---|---|
| □ | itsm-team.net | frontfork | Enabled | 54.93.118.85 | herculespopular22@gmail.com | 2018/11/15 01:43:12 PM |

| LDAP Accounts - Column Description | |
|---|---|
| **Column Heading** | **Description** |
| Account Domain | The Active Directory domain name.<br>• Click the domain name to:<br>• View and import user groups<br>• Configure device enrollment for imported users<br>• Configure the connection between the AD server and Endpoint Manager<br>See **Manage LDAP Accounts** for more details. |
| Customer Name | The organization associated with the AD domain |
| Enable LDAP | Whether or not the LDAP account is active |
| Server Host | The LDAP hostname or IP address of the AD server |
| Author | The admin who added the LDAP account<br>• Click the admin name to view their details. See **View User Details** if you need help with this. |

| | |
|---|---|
| Created | The date and time at which the LDAP account was added |

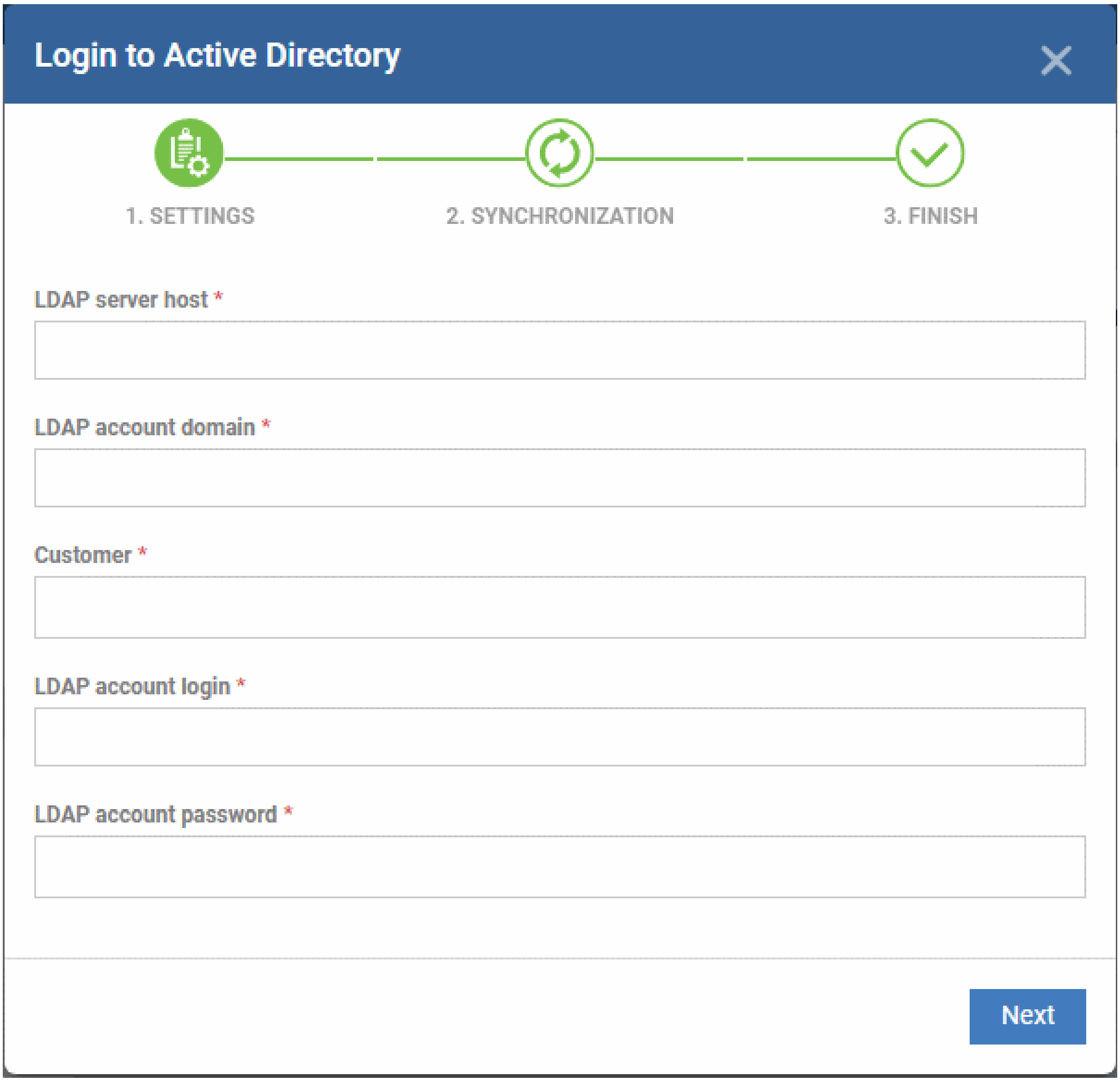
**Note**: Endpoint Manager communicates with Comodo servers and managed devices in order to update data, deploy profiles, synchronize LDAP server via devices and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in **Appendix 1**.

**To add an LDAP account**

- Click 'Add' at the top

The 'Login to Active Directory' wizard opens:

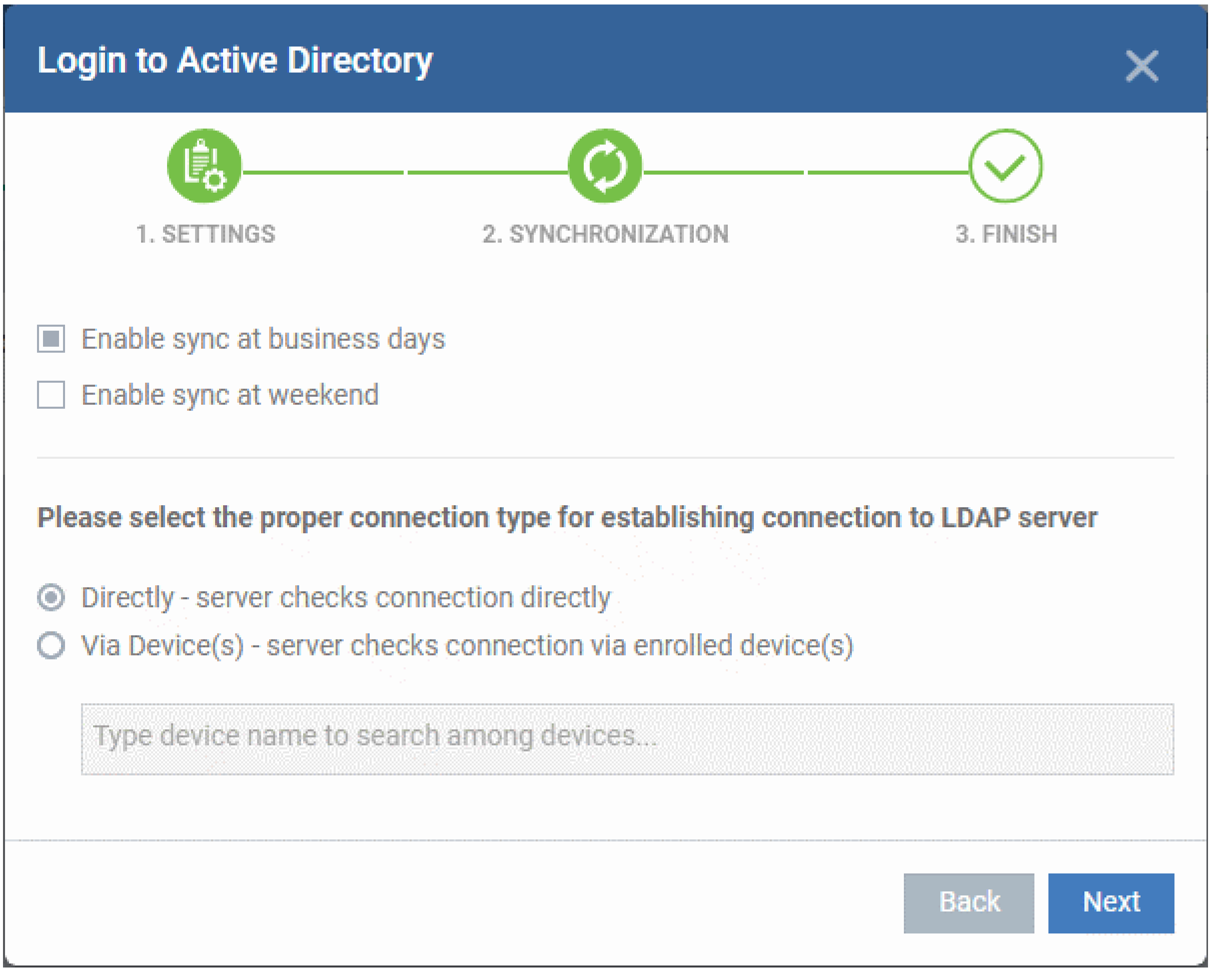
**Step 1 - Enter LDAP account details**



| 'Login to Active Directory - Settings' Form - Table of Parameters | |
|---|---|
| **Form Element Type** | **Description** |
| LDAP Server Host | The IP address or hostname of the Active Directory (AD) server |
| LDAP Account Domain | The Active Directory domain name. |
| Company | Choose the company to which the AD server belongs.<br>• Comodo Dragon MSP and Comodo One MSP customers can add AD servers for multiple companies.<br>• Type the first few characters of the company name and select from options.<br>• Comodo Dragon Enterprise, Comodo One Enterprise and EM stand-alone customers can only select the default company. |
| LDAP Account Login | The admin username and password required to access the AD server. |
| LDAP Account Password | |

- Click 'Next' after completing the settings form.

**Step 2 - Configure Synchronization Settings**



☑ Enable sync at business days

☐ Enable sync at weekend

Please select the proper connection type for establishing connection to LDAP server

● Directly - server checks connection directly

○ Via Device(s) - server checks connection via enrolled device(s)

Type device name to search among devices...

**Sync Settings**

- Enable Sync at Business Days - Endpoint Manager will automatically sync with the LDAP server once per day Monday through Friday to check for and import new users
- Enable Sync At Weekend - Endpoint Manager will automatically sync with the LDAP server once a day on Saturdays and Sundays to check for and import new users on weekends.

Note - you can manually sync at any time by clicking the 'Sync with LDAP' button.

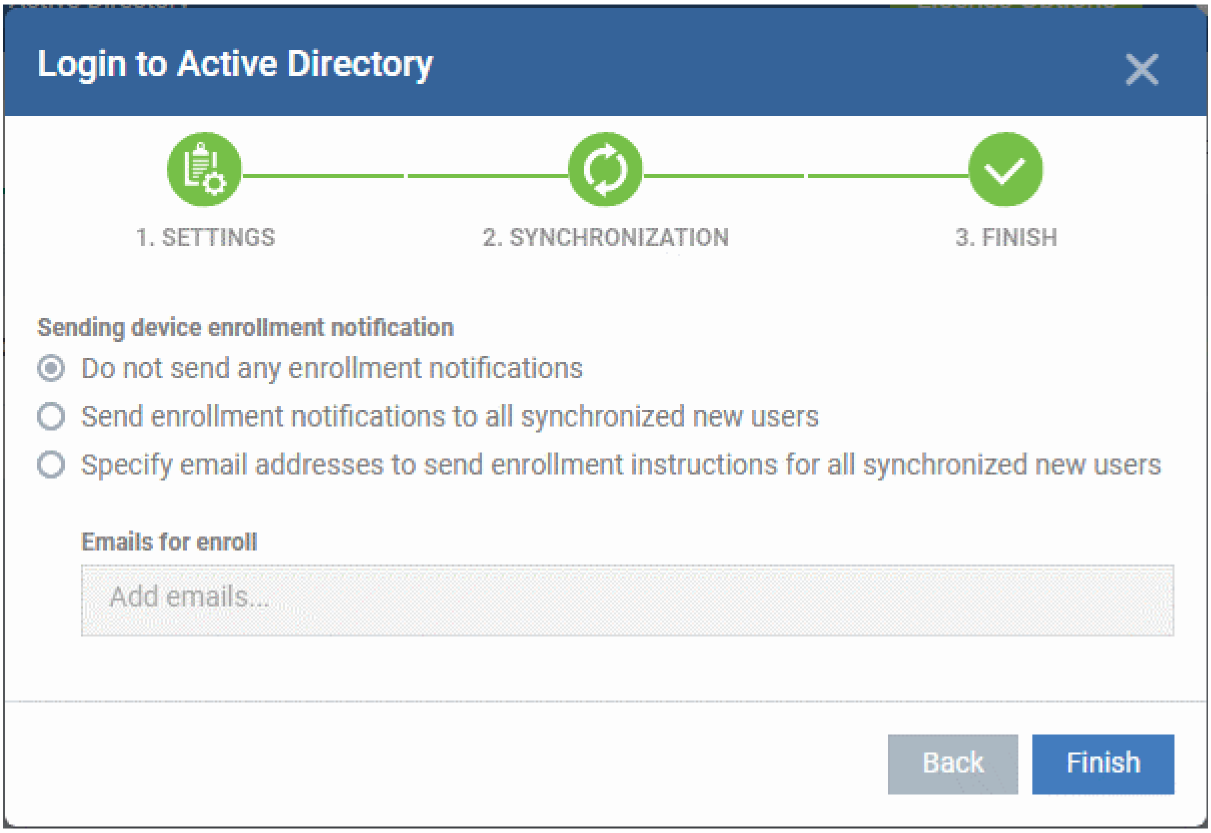
**Connection Type**

The connections setting determine how Endpoint Manager connects to the LDAP server. You can connect directly from the EM server or via the enrolled devices.

If you choose the second option, you should specify the names of enrolled Windows devices which are in the same network as the AD server.

- Click 'Next'

**Step 3 - Finish**



Sending device enrollment notification

● Do not send any enrollment notifications

○ Send enrollment notifications to all synchronized new users

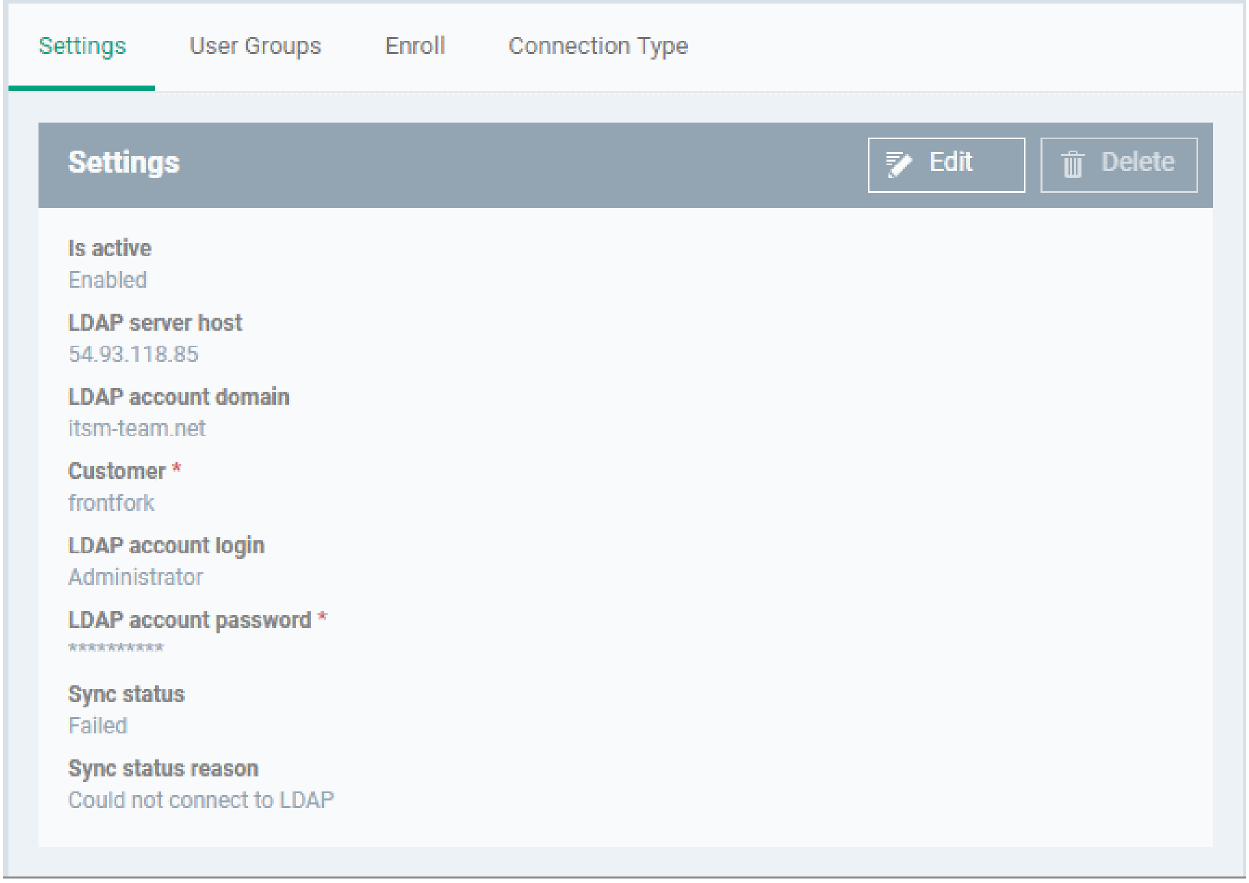
○ Specify email addresses to send enrollment instructions for all synchronized new users

Emails for enroll

Add emails...

- **Do not send any enrollment notifications** - No notification mails are sent to imported users
- **Send enrollment notifications to all synchronized new users** - Device enrollment emails are sent to imported users. These mails include instructions which tell the user how to add their device to Endpoint Manager.
- **Specify email address to send enrollment notifications for all synchronized new users** - Add the recipients who should receive a notification mail when new users are added. Usually sent to an administrator, the mail contains instructions on how to enroll devices for the new users. You can add multiple email addresses here.
- Click 'Finish'

Endpoint Manager will connect to the LDAP server per the configuration. A summary of account settings is shown if the connection is successful:



Is active
Enabled

LDAP server host
54.93.118.85

LDAP account domain
itsm-team.net

Customer *
frontfork

LDAP account login
Administrator

LDAP account password *
***********

Sync status
Failed

Sync status reason
Could not connect to LDAP

- Click 'Edit' if you want to change any details, edit the details and click 'Save' to save your settings.

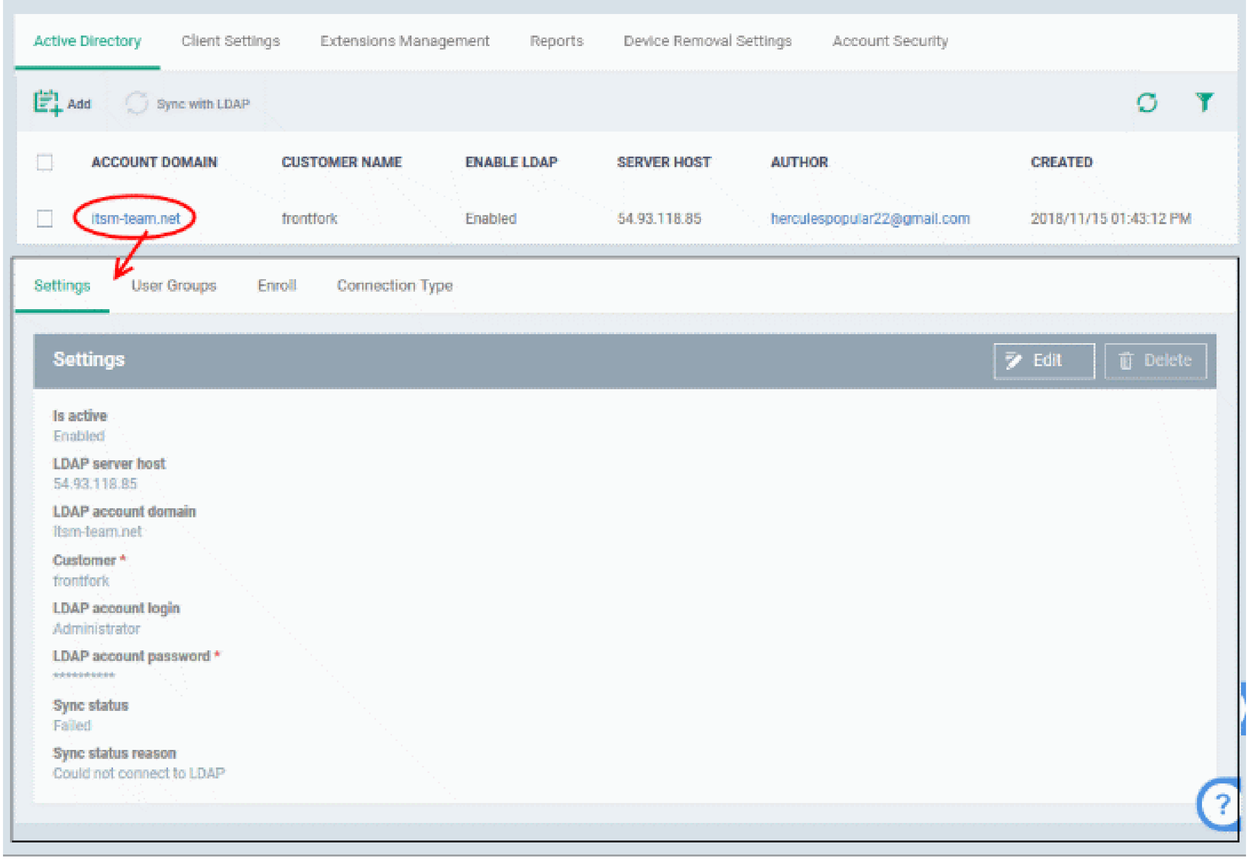
The synchronization task will run as scheduled in step - 2, and the user groups will be added.

- Click 'Sync with LDAP' to instantly sync the user groups between the AD server and EM
- Repeat the process to add more AD servers to import user groups from.

## Manage LDAP Accounts

The Active Directory interface lets you view and edit the details of integrated AD servers, synchronize users between AD and EM, and more.

- Click 'Settings' > 'Portal Set-up' > 'Active Directory'
- Click the AD domain name from the list of LDAP accounts to view or edit its details



| ACCOUNT DOMAIN | CUSTOMER NAME | ENABLE LDAP | SERVER HOST | AUTHOR | CREATED |
|---|---|---|---|---|---|
| itsm-team.net | frontfork | Enabled | 54.93.118.85 | herculespopular22@gmail.com | 2018/11/15 01:43:12 PM |

Is active
Enabled

LDAP server host
54.93.118.85

LDAP account domain
itsm-team.net

Customer *
frontfork

LDAP account login
Administrator

LDAP account password *
**********

Sync status
Failed

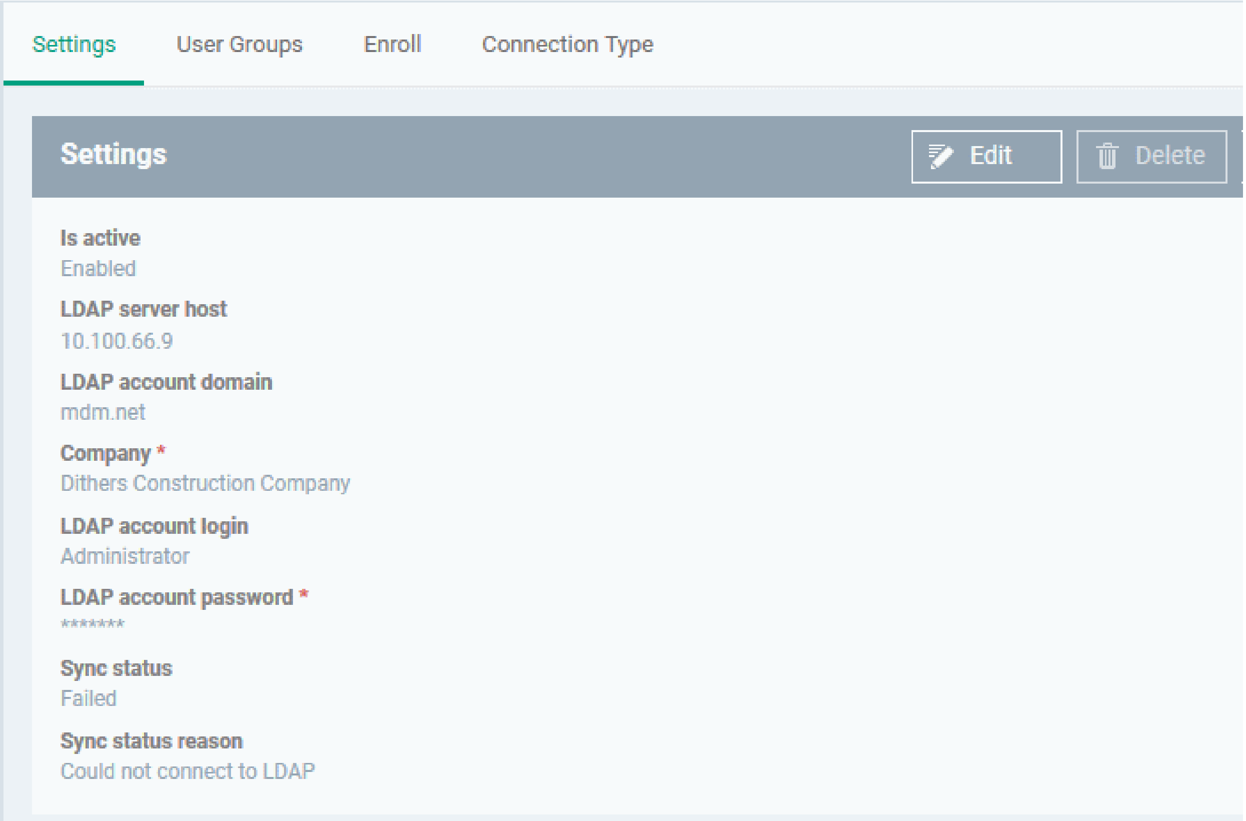
Sync status reason
Could not connect to LDAP

The Active Directory details will be displayed under four tabs:

- Settings
- User Groups
- Enroll
- Connection Type

### Settings tab

The 'Settings' tab displays AD configuration details:



Is active
Enabled

LDAP server host
10.100.66.9

LDAP account domain
mdm.net

Company *
Dithers Construction Company

LDAP account login
Administrator

LDAP account password *
*******

Sync status
Failed

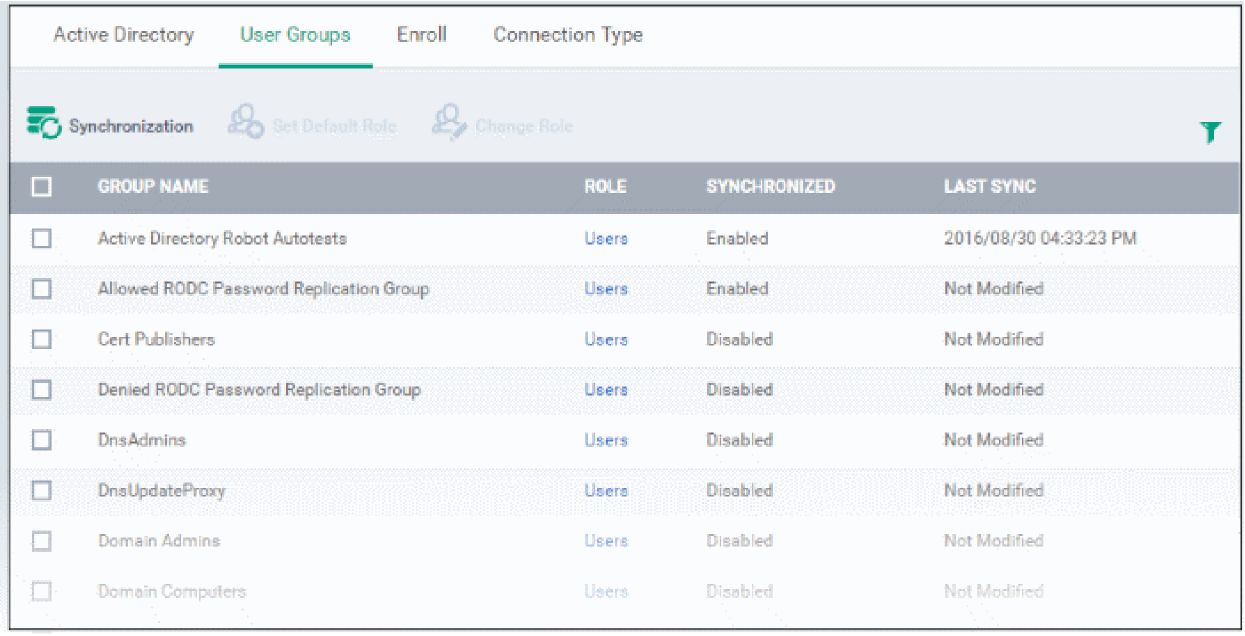
Sync status reason
Could not connect to LDAP

- Click 'Edit' to update any LDAP details and click the 'Save' button

### User Groups tab

The 'User Groups' tab shows groups that were identified on the AD server. This includes users/groups created in the root folder and all sub-folders/custom folders on the AD server. This interface allows you to:

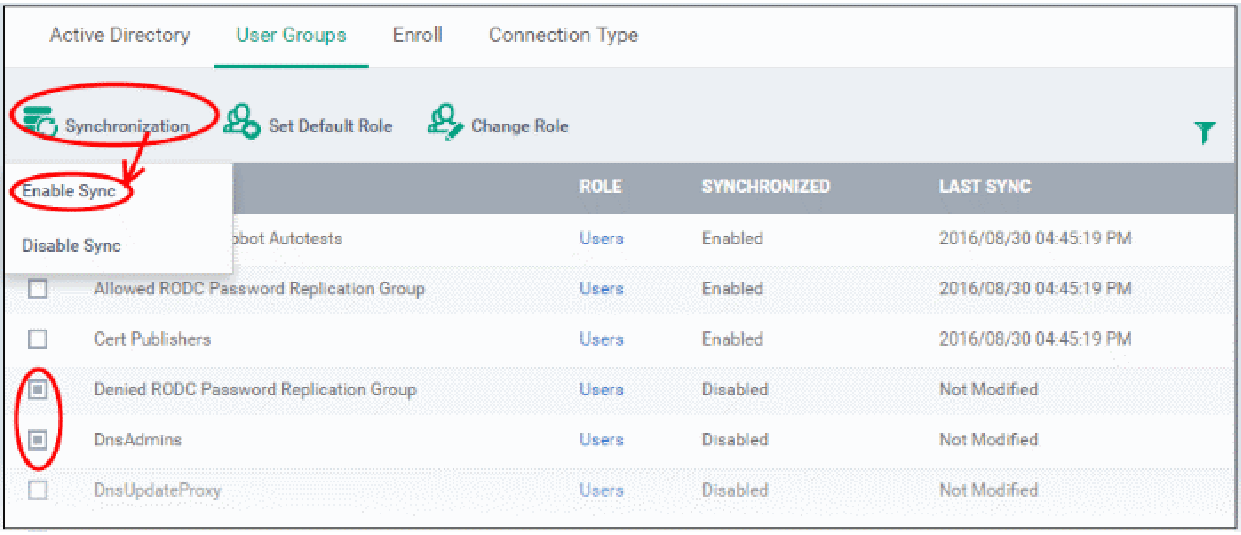
- Selectively enable/disable AD synchronization for groups. Synchronization allows EM to update its user list whenever users are added/removed from the AD sever.
- Select the roles to be applied to users in each AD group.
- Manually synchronize groups before importing to EM



| ☐ | GROUP NAME | ROLE | SYNCHRONIZED | LAST SYNC |
|---|---|---|---|---|
| ☐ | Active Directory Robot Autotests | Users | Enabled | 2016/08/30 04:33:23 PM |
| ☐ | Allowed RODC Password Replication Group | Users | Enabled | Not Modified |
| ☐ | Cert Publishers | Users | Disabled | Not Modified |
| ☐ | Denied RODC Password Replication Group | Users | Disabled | Not Modified |
| ☐ | DnsAdmins | Users | Disabled | Not Modified |
| ☐ | DnsUpdateProxy | Users | Disabled | Not Modified |
| ☐ | Domain Admins | Users | Disabled | Not Modified |
| ☐ | Domain Computers | Users | Disabled | Not Modified |

### Enable/disable synchronization

- Select user group(s) from the list and click 'Synchronization' at the top:

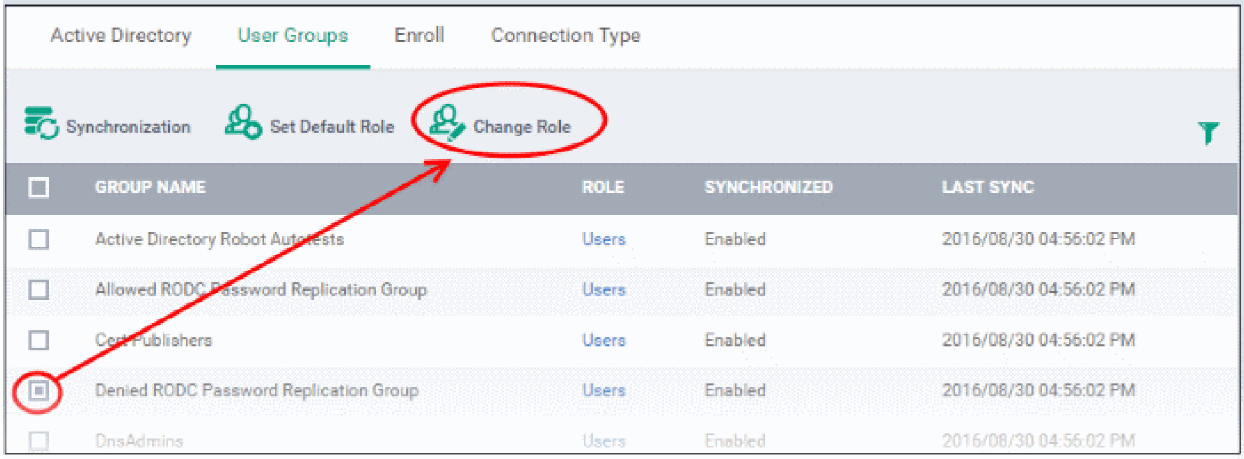


|  |  | ROLE | SYNCHRONIZED | LAST SYNC |
|---|---|---|---|---|
|  | ...bot Autotests | Users | Enabled | 2016/08/30 04:45:19 PM |
| □ | Allowed RODC Password Replication Group | Users | Enabled | 2016/08/30 04:45:19 PM |
| □ | Cert Publishers | Users | Enabled | 2016/08/30 04:45:19 PM |
| ☑ | Denied RODC Password Replication Group | Users | Disabled | Not Modified |
| ☑ | DnsAdmins | Users | Disabled | Not Modified |
| □ | DnsUpdateProxy | Users | Disabled | Not Modified |

- Select whether synchronization should be enabled or not from the drop-down. If enabled, EM will periodically synchronize with the group to import new users and remove deleted users.

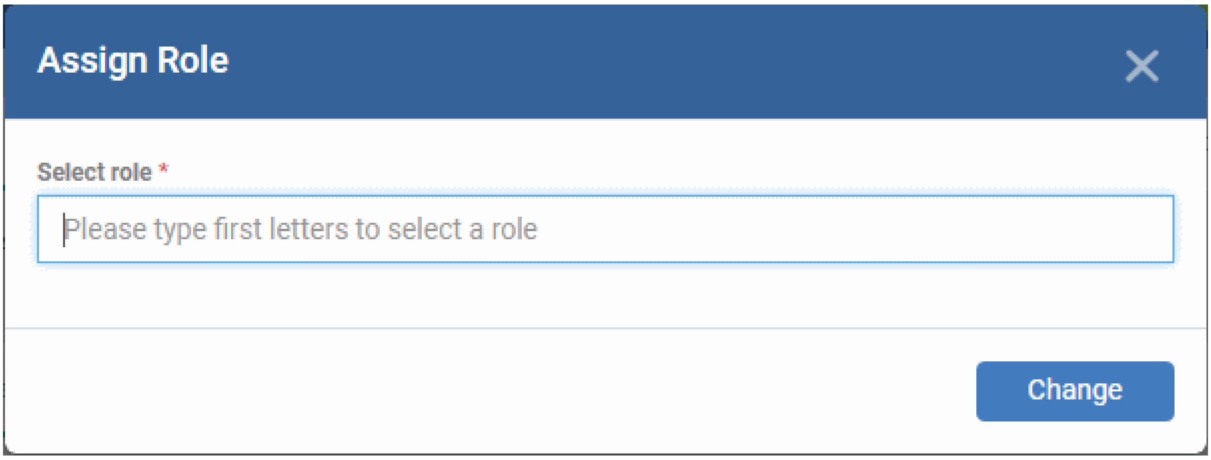
### Assign roles to imported users

- Select the user(s)/user group(s).
- Select 'Set Default Role' to assign the default EM user role to the users. See **Set a role as the default role** if you need help with this.



| □ | GROUP NAME | ROLE | SYNCHRONIZED | LAST SYNC |
|---|---|---|---|---|
| □ | Active Directory Robot Autotests | Users | Enabled | 2016/08/30 04:56:02 PM |
| □ | Allowed RODC Password Replication Group | Users | Enabled | 2016/08/30 04:56:02 PM |
| □ | Cert Publishers | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☑ | Denied RODC Password Replication Group | Users | Enabled | 2016/08/30 04:56:02 PM |
| □ | DnsAdmins | Users | Enabled | 2016/08/30 04:56:02 PM |

- Select 'Change Role' if you want to assign a different role to imported users.



- Type the first few characters of the name of the role to be assigned and select the role from the options.

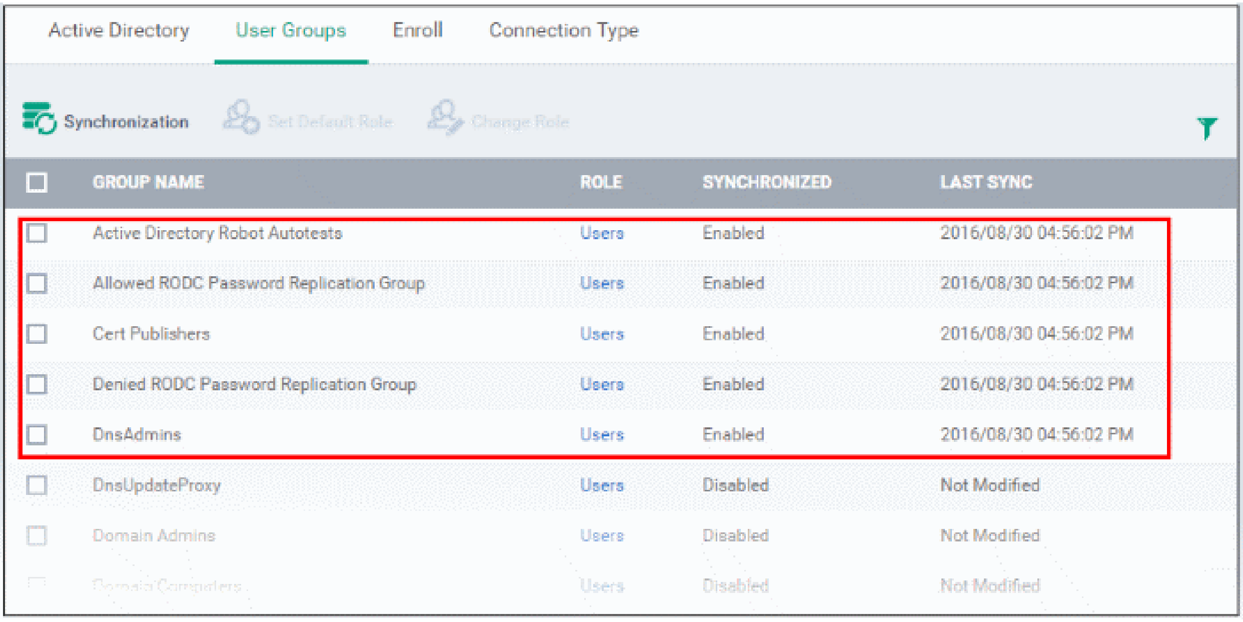
The selected role will be displayed in the 'Role' column for the users/user groups.

- Repeat the process to apply different roles to different users/user groups.

See '**Manage Roles Assigned to a User**' for more details on roles.

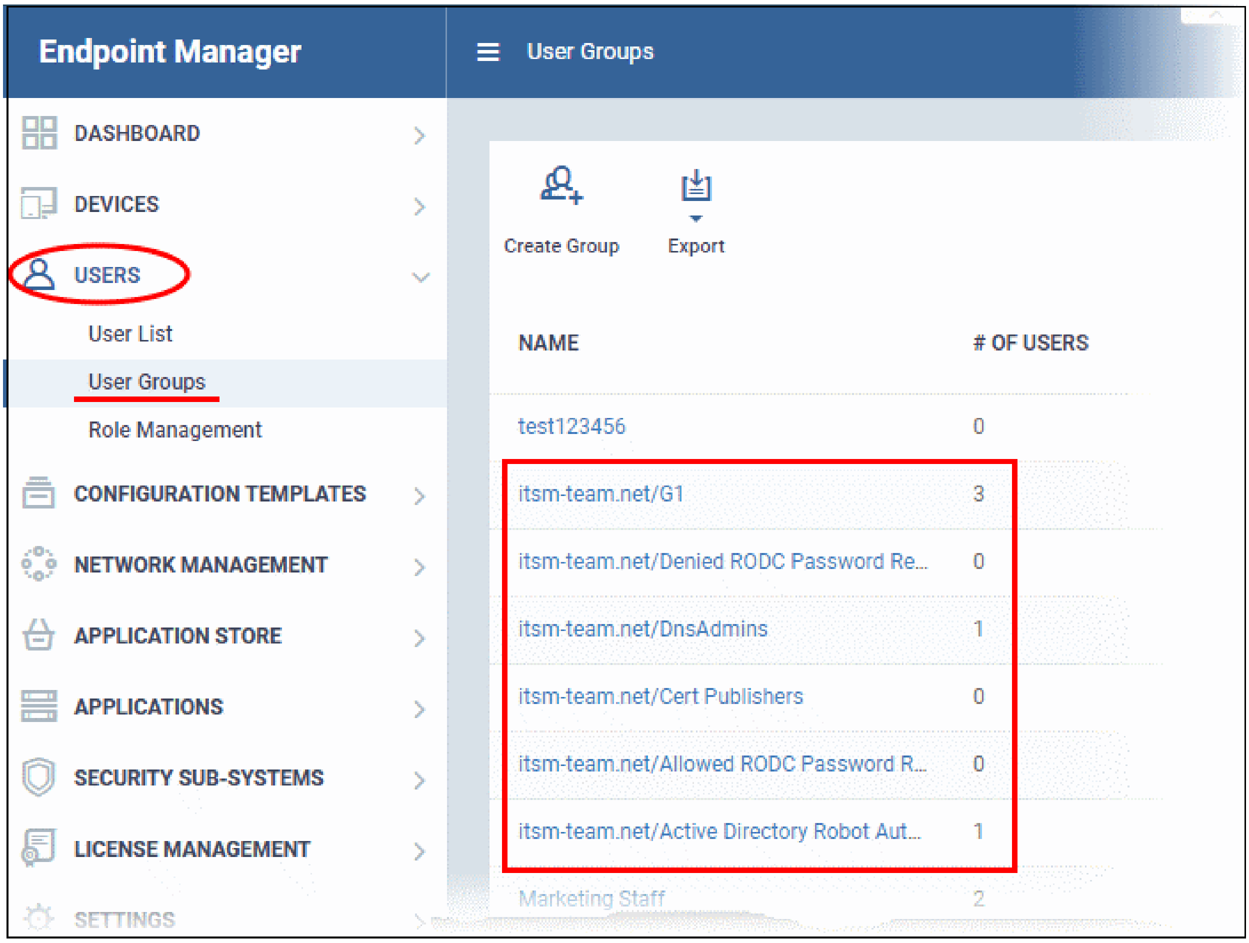
**To import users from selected user group**

- Click 'Sync with LDAP'



| ☐ | GROUP NAME | ROLE | SYNCHRONIZED | LAST SYNC |
|---|---|---|---|---|
| ☐ | Active Directory Robot Autotests | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☐ | Allowed RODC Password Replication Group | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☐ | Cert Publishers | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☐ | Denied RODC Password Replication Group | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☐ | DnsAdmins | Users | Enabled | 2016/08/30 04:56:02 PM |
| ☐ | DnsUpdateProxy | Users | Disabled | Not Modified |
| ☐ | Domain Admins | Users | Disabled | Not Modified |
| ☐ | Domain Computers | Users | Disabled | Not Modified |

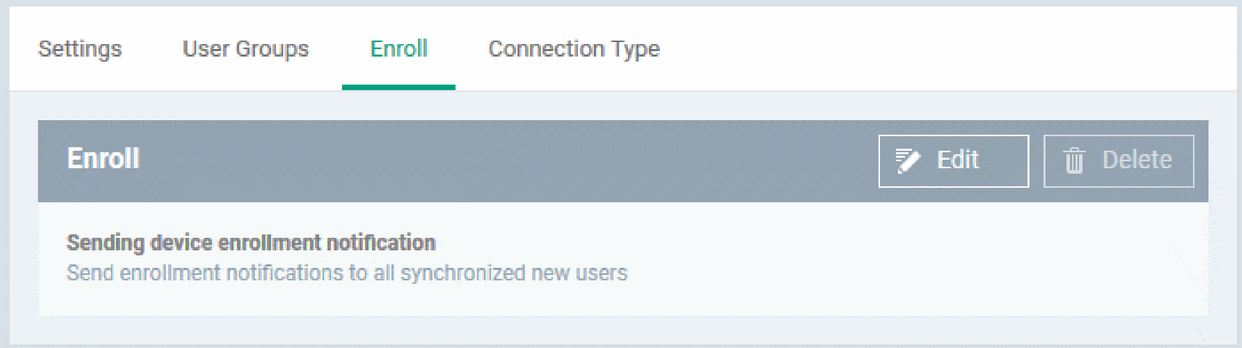
- The LDAP user/user groups are synchronized with EM and new users are imported. The 'User List'/'User Groups' interfaces will update appropriately. See '**Users and User Groups**' if you need more help with users and groups.



| NAME | # OF USERS |
|---|---|
| test123456 | 0 |
| itsm-team.net/G1 | 3 |
| itsm-team.net/Denied RODC Password Re... | 0 |
| itsm-team.net/DnsAdmins | 1 |
| itsm-team.net/Cert Publishers | 0 |
| itsm-team.net/Allowed RODC Password R... | 0 |
| itsm-team.net/Active Directory Robot Aut... | 1 |
| Marketing Staff | 2 |

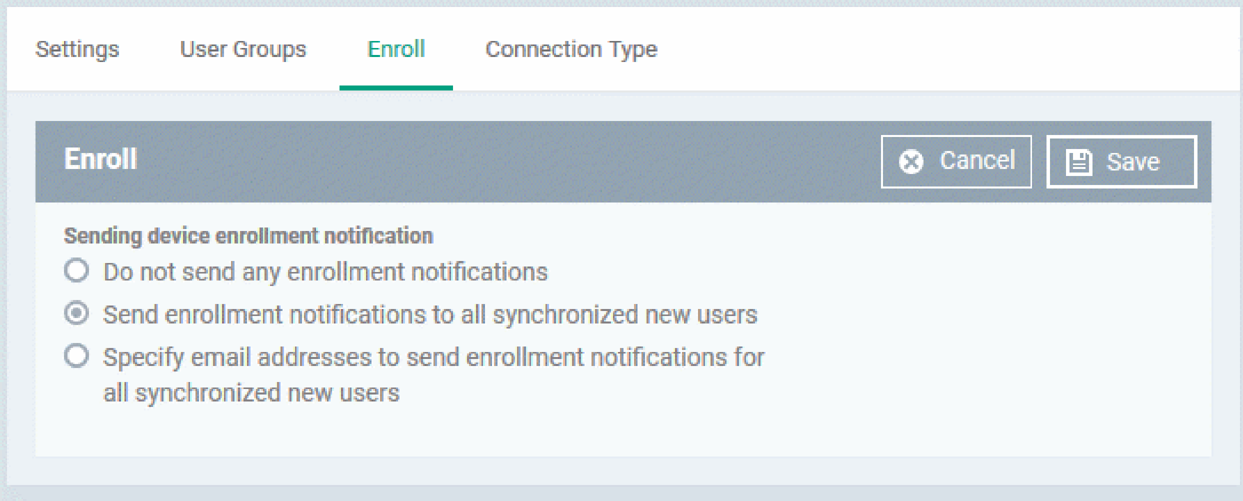
### Enroll tab

The 'Enroll' tab displays the current setting of enrollment notification sent to imported users.



**Sending device enrollment notification**
Send enrollment notifications to all synchronized new users

- Click 'Edit' to change the enrollment notification type



Settings | User Groups | Enroll | Connection Type

Sending device enrollment notification

○ Do not send any enrollment notifications

● Send enrollment notifications to all synchronized new users

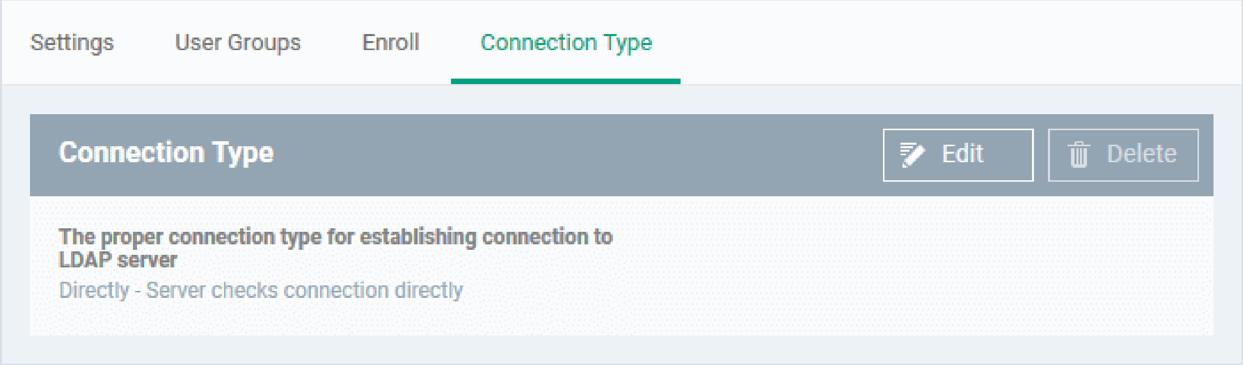
○ Specify email addresses to send enrollment notifications for all synchronized new users

- **Do not send any enrollment notifications -** No enrollment mails will be sent to users imported via LDAP
- **Send enrollment notifications to all synchronized new users -** Device enrollment emails will be sent to new users enrolled via LDAP.
- **Specify email address to send enrollment notifications for all synchronized new users -** Specify email recipients who should receive a notification mail when new users have been added. Usually sent to an administrator, the mail will contain instructions on how to enroll devices for the new users. You can add multiple email addresses here.

- Update the notification type from the options and click 'Save'

### Connection Type Tab

The 'Connection Type' tab displays how the AD server currently connects to Endpoint Manager.

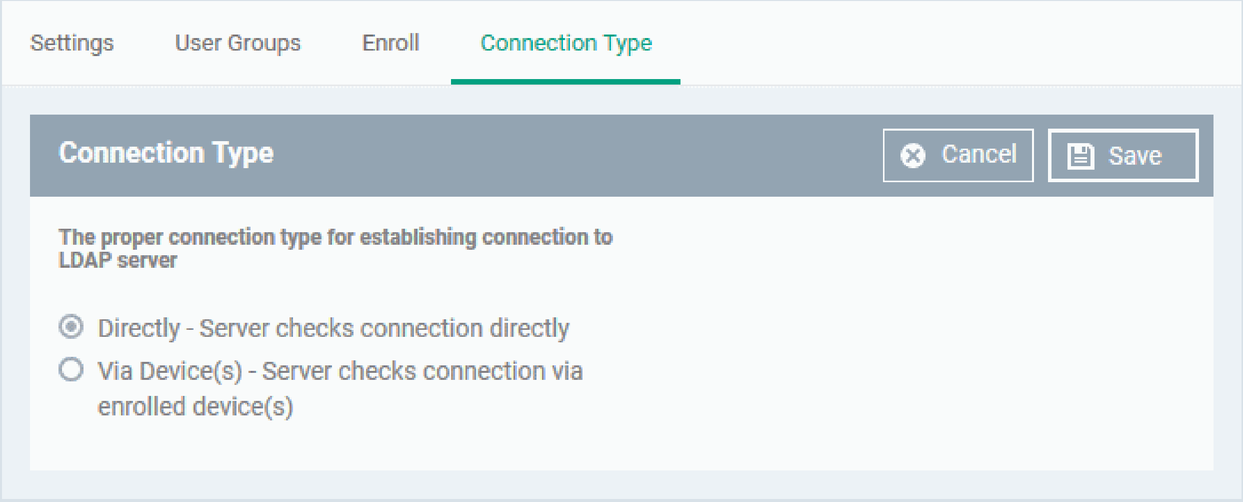


Settings | User Groups | Enroll | Connection Type

The proper connection type for establishing connection to LDAP server

Directly - Server checks connection directly

- Click the 'Edit' button to change the connection type.



Connection Type

The proper connection type for establishing connection to LDAP server

● Directly - Server checks connection directly

○ Via Device(s) - Server checks connection via enrolled device(s)

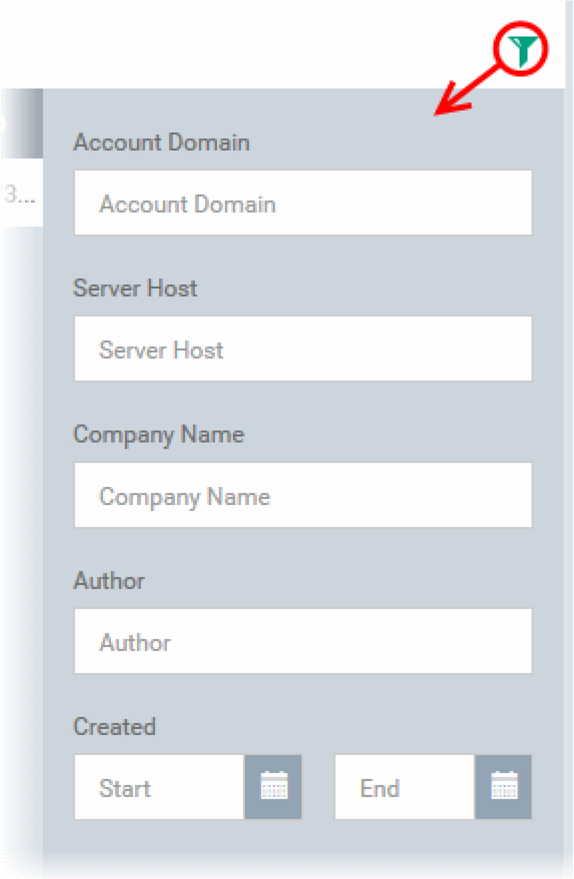
If the first option is selected, EM will connect to the configured LDAP server directly. The second option enables the EM server to connect to the LDAP server via enrolled devices. Multiple devices can be configured for the second option.

- Click 'Save' after selecting the option.

You can add multiple LDAP servers for the account from the Active Directory interface. Click 'Add' and follow the same procedure explained above.

### Active Directory Interface - Sorting, Search and Filter Options

- Click on the column headers sorts items in alphabetical, ascending/descending order
- Click the funnel button ▼ to open filter options:



Account Domain

Account Domain

Server Host

Server Host

Company Name

Company Name

Author

Author

Created

Start

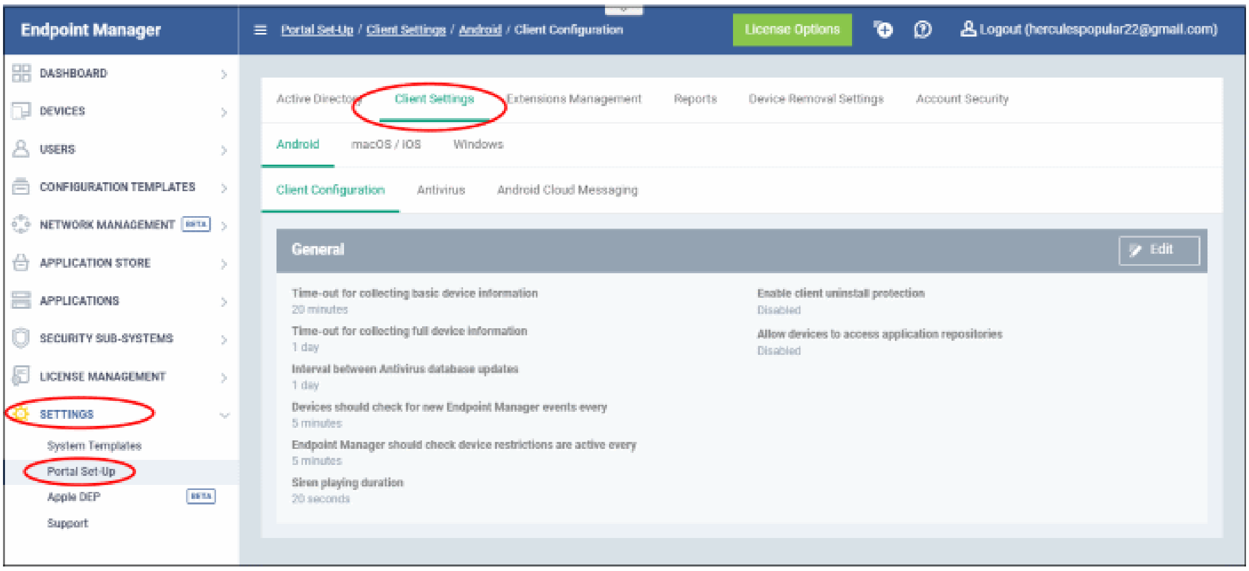
End

- You can search for a specific LDAP account based by domain name, host, company and/or author. Enter your search criteria in the respective text boxes and click 'Apply'.
- You can also filter by the date the account was created. Use the calendar buttons at the bottom to select start and end dates then click 'Apply'.

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

### 11.2.2. Configure Communication and Security Client Settings

- Click 'Settings' > 'Portal Set-up' > 'Client Settings'
- This section allows you to configure Android, Windows communication clients and install Apple Push Notification (APN) certificates on your Endpoint Manager.
- Configure default Windows communication and security clients that will be deployed on endpoints



Time-out for collecting basic device information
20 minutes

Time-out for collecting full device information
1 day

Interval between Antivirus database updates
1 day

Devices should check for new Endpoint Manager events every
5 minutes

Endpoint Manager should check device restrictions are active every
5 minutes

Siren playing duration
20 seconds

Enable client uninstall protection
Disabled

Allow devices to access application repositories
Disabled

Use the following links to learn more about each setting:

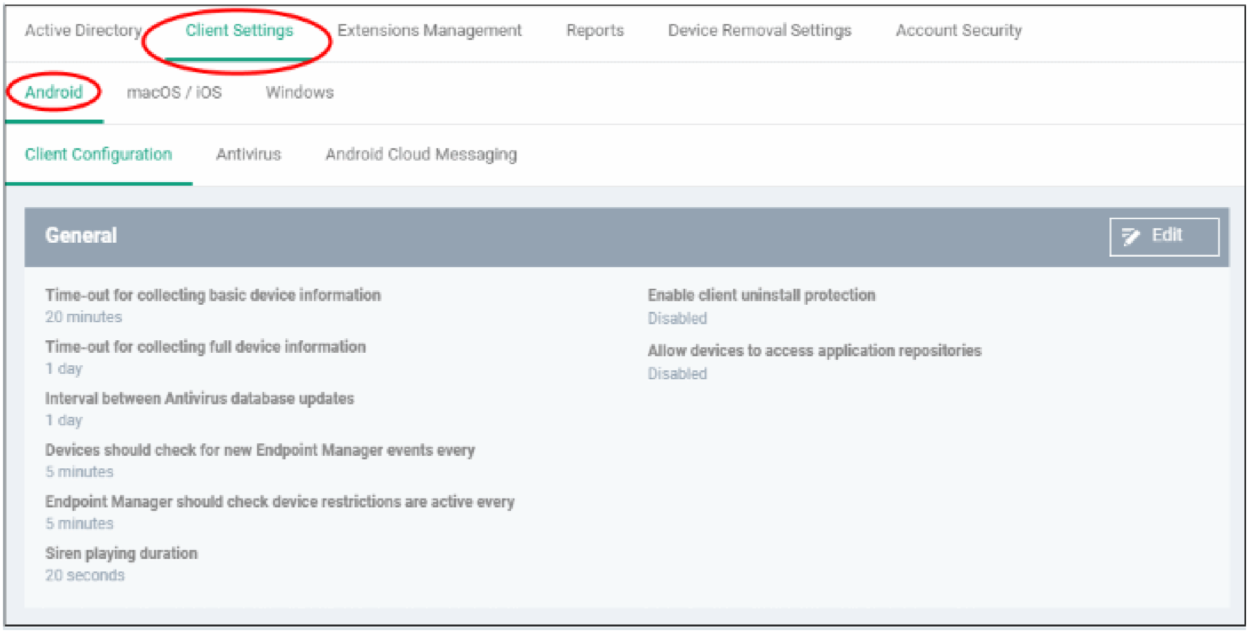
- **Configure the EM Android Client**
  - **Configure General Settings**
  - **Configure Android Client Antivirus Settings**
  - **Add Google Cloud Messaging (GCM) Token**
- **Add Apple Push Notification Certificate**
- **Configure EM Windows Clients**
  - **Configure Communication Client Settings**
  - **Configure Comodo Client Security (CCS) Settings**

## 11.2.2.1. Configure the EM Android Client

- Click 'Settings' > 'Portal Set-up' > 'Client Settings' > Open the 'Android' tab.
- You need to install the communication client on each Android device that you want to manage. The client allows Endpoint Manager to pass updates and commands to the device, and to run antivirus scans.
- You also need to add a Google Cloud Messaging (GCM) token for the EM server to communicate with the clients.
- This area also lets you configure client general settings and antivirus settings.

**Open the Android Client Config Screen**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click the 'Android' tab



General

Time-out for collecting basic device information
20 minutes

Time-out for collecting full device information
1 day

Interval between Antivirus database updates
1 day

Devices should check for new Endpoint Manager events every
5 minutes

Endpoint Manager should check device restrictions are active every
5 minutes

Siren playing duration
20 seconds

Enable client uninstall protection
Disabled

Allow devices to access application repositories
Disabled

The interface has three tabs:

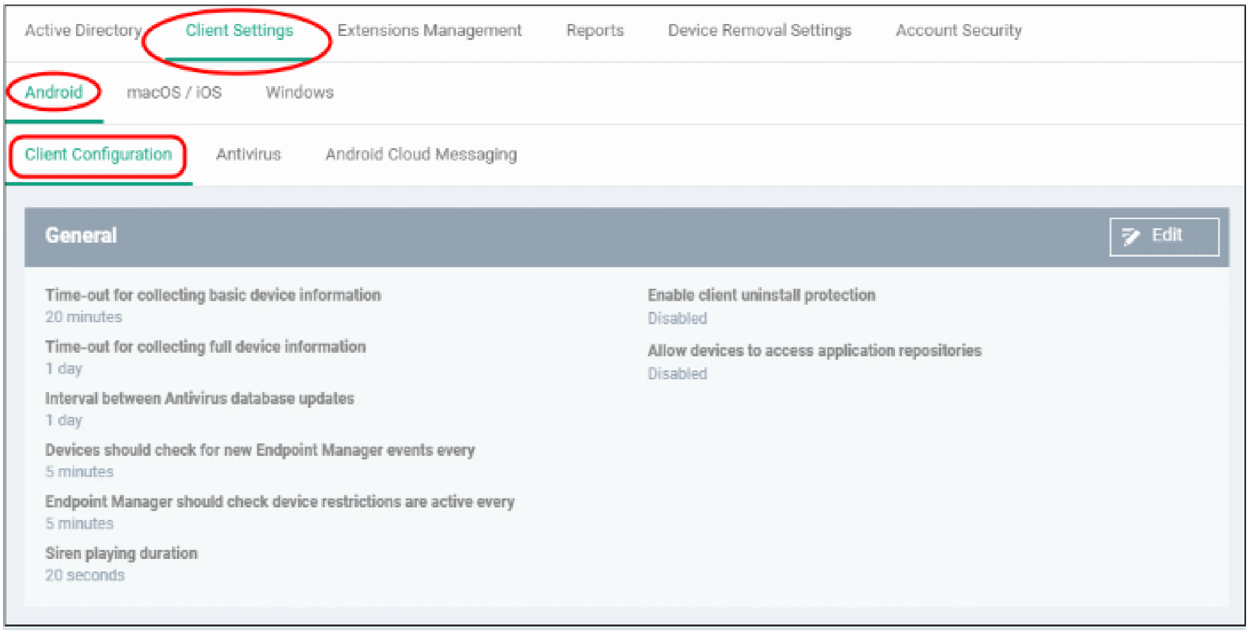
- **Client Configuration** - General settings like client and AV database updates, polling intervals, client uninstall protection and more. See **Configure Android Client General Settings**.
- **Antivirus** - Specify how viruses identified by client should be dealt with. If 'Automatic' is chosen you can also specify whether the AV should remove the threat or ignore it. See **Configure Android Client Antivirus Settings**.
- **Android Cloud Messaging** - Create a Google Cloud Messaging (GCM) token to facilitate communications between EM and Android devices. See **Add Google Cloud Messaging (GCM) Token**.

## 11.2.2.1.1. Configure Android Client General Settings

- Click 'Settings' > 'Portal Set-up' > 'Client Settings'
- Open the 'Android' tab then click 'Client Configuration'
- This area lets you configure various settings for the Endpoint Manager Android client. Settings include update frequency, device alarms, uninstall protection and more.

**Configure the Android client**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click 'Android' > 'Client Configuration'



Time-out for collecting basic device information
20 minutes

Time-out for collecting full device information
1 day

Interval between Antivirus database updates
1 day

Devices should check for new Endpoint Manager events every
5 minutes

Endpoint Manager should check device restrictions are active every
5 minutes

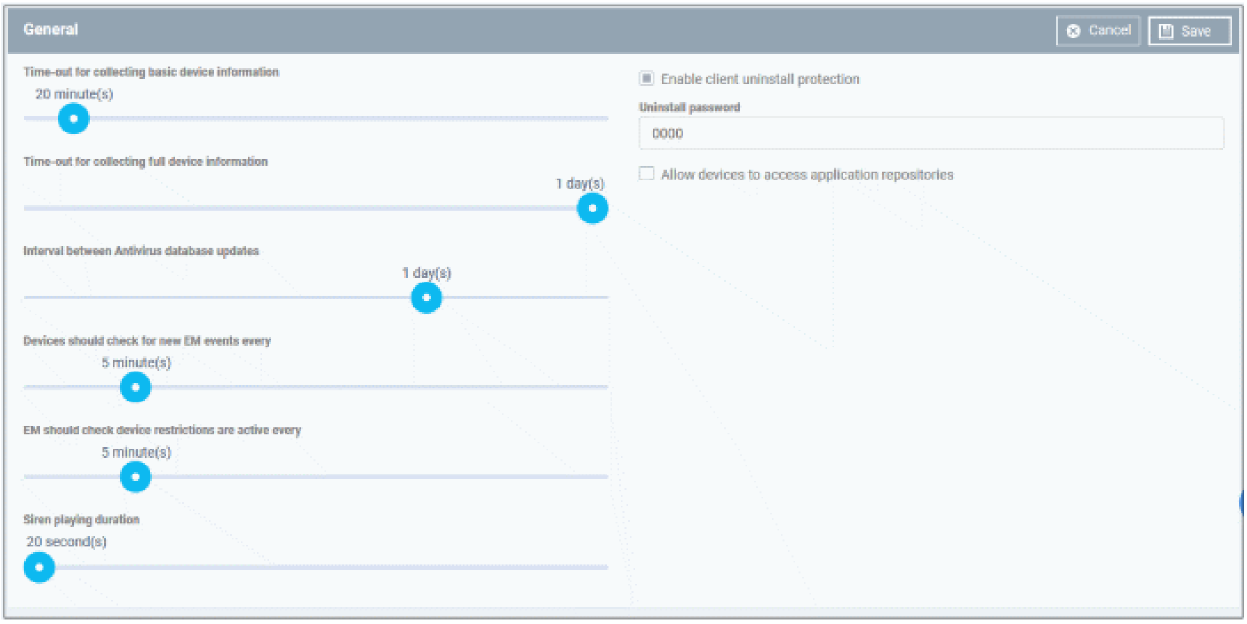
Siren playing duration
20 seconds

Enable client uninstall protection
Disabled

Allow devices to access application repositories
Disabled

The current settings for various parameters of Client Configuration is displayed.

- Click the edit button to modify settings:



Time-out for collecting basic device information
20 minute(s)

Time-out for collecting full device information
1 day(s)

Interval between Antivirus database updates
1 day(s)

Devices should check for new EM events every
5 minute(s)

EM should check device restrictions are active every
5 minute(s)

Siren playing duration
20 second(s)

☑ Enable client uninstall protection

Uninstall password
0000

□ Allow devices to access application repositories

| Android Client Configuration - Table of parameters | |
|---|---|
| **Parameter** | **Description** |
| Time-out for collecting basic device information | The maximum time allowed for EM to collect essential information such as battery level, CPU usage, GPS location and WiFI SSID. |
| Time-out for collecting full device information | The maximum time allowed for EM to collect all device information. This includes memory status, device name, IMEI number, roaming status, bluetooth MAC address and WiFi MAC address. |
| Interval between antivirus database | The frequency at which the antivirus database should be updated on the device. |

| | |
|---|---|
| update | |
| Devices should check for new EM events every | The frequency at which the device should contact Endpoint Manager to receive new push notifications. |
| EM should check device restrictions are active every | The frequency at which the client should confirm that its device restrictions (as per the applied profile) are in place. |
| Siren Playing Duration | Length of time that the device alarm will play for when remotely activated by an admin. |
| Enable client uninstall protection | Whether or not a password is required in order to remove the client from a device.<br>• Select the 'Enable client uninstall protection' check box and specify a password in the text box.<br>The EM client can be uninstalled from any enrolled device only after entering the password. |
| Allow devices to access application repositories | If enabled, an 'Applications' bar will be visible on Android devices which will open a list of Android apps in the 'Application Store'. |

- Click 'Save' to apply your changes.

### 11.2.2.1.2. Configure Android Client Antivirus Settings

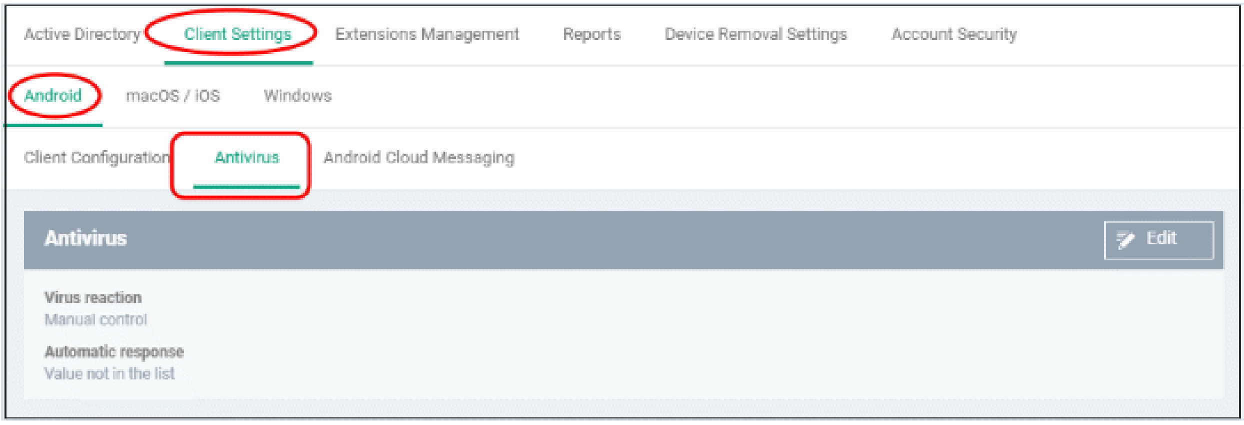
The Android antivirus provides real-time protection against malware and malicious apps. You can also launch on-demand scans on Android devices from Endpoint Manager.

The antivirus settings area lets you configure whether threats are automatically removed or handled manually.

- **Automatic Response -** You have the choice to auto-uninstall or ignore the threat. If you choose 'Ignore' then the item will appear in the current malware list ('Security Sub-Systems' > 'Antivirus' > 'Current Malware List').
- **Manual Control -** All threats are ignored on the device. You can manage these ignored threats at 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List'.

**Configure antivirus settings**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click 'Android' > 'Antivirus'

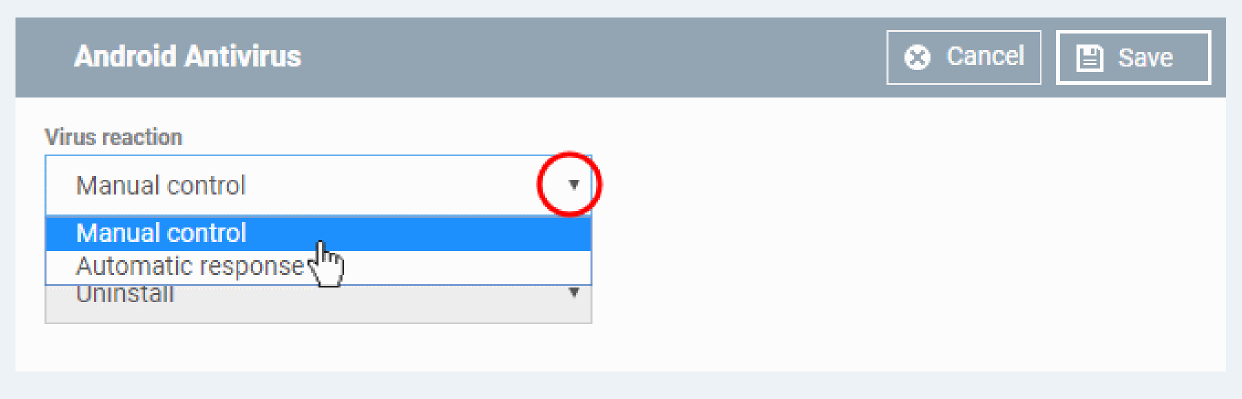


Virus reaction
Manual control

Automatic response
Value not in the list

The current antivirus settings are displayed.

- Click the edit button Edit at the top to modify settings.



| Android Client Antivirus Settings - Table of Parameters | |
|---|---|
| **Parameter** | **Description** |
| Virus Reaction | Choose the type of action taken if malware is discovered on the device. The options are:<br>**1) Manual control** - Discovered malware is ignored and its details are sent to Endpoint Manager (**current malware list** and **threat history**). No alerts are shown on the device.<br>• You must enable 'Terminate Malware' in the Android profile if you also want stop the malware running.<br>• Click 'Configuration Templates' > 'Profiles' > open your Android profile > Open or add the 'Antivirus' section.<br>• **Click here** to view help on this in the online guide<br>**2) Automatic response** - Two options are available.<br>• Uninstall:<br>◦ Knox devices - Applications with viruses or infected files on the devices and from the SD card are deleted without any alert on the device.<br>◦ Non-Knox devices - An alert is shown to the user on the device for removal of malware. Infected files on the SD card are deleted without any alert.<br>• Ignore:<br>◦ No action is taken on malware files and details are sent to portal (**current malware list** and **threat history**). You can manage the threats in the **current malware list** screen. |

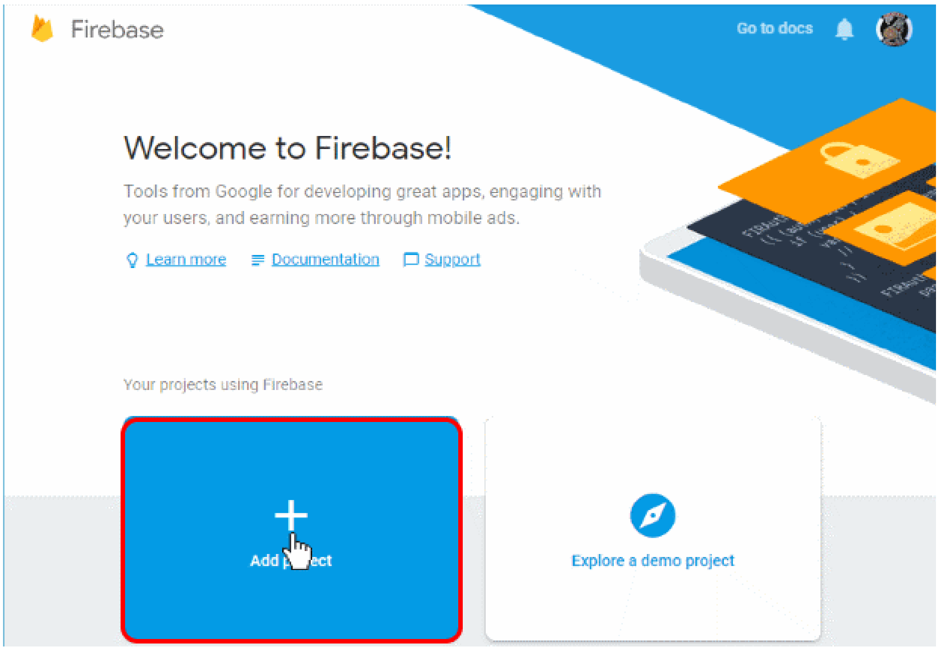
- Click 'Save' for your settings to take effect.

### 11.2.2.1.3. Add Google Cloud Messaging (GCM) Token

- Endpoint Manager requires a Google Cloud Messaging (GCM) token in order to communicate with enrolled Android devices.
- EM ships with a default token. However, you can also generate a unique Android GCM token for your EM portal.
- To get a token, you must first create a project in the Google Developers console.
- Please follow the steps given below to create a project and upload a token.

**Step 1 - Create a New Project**

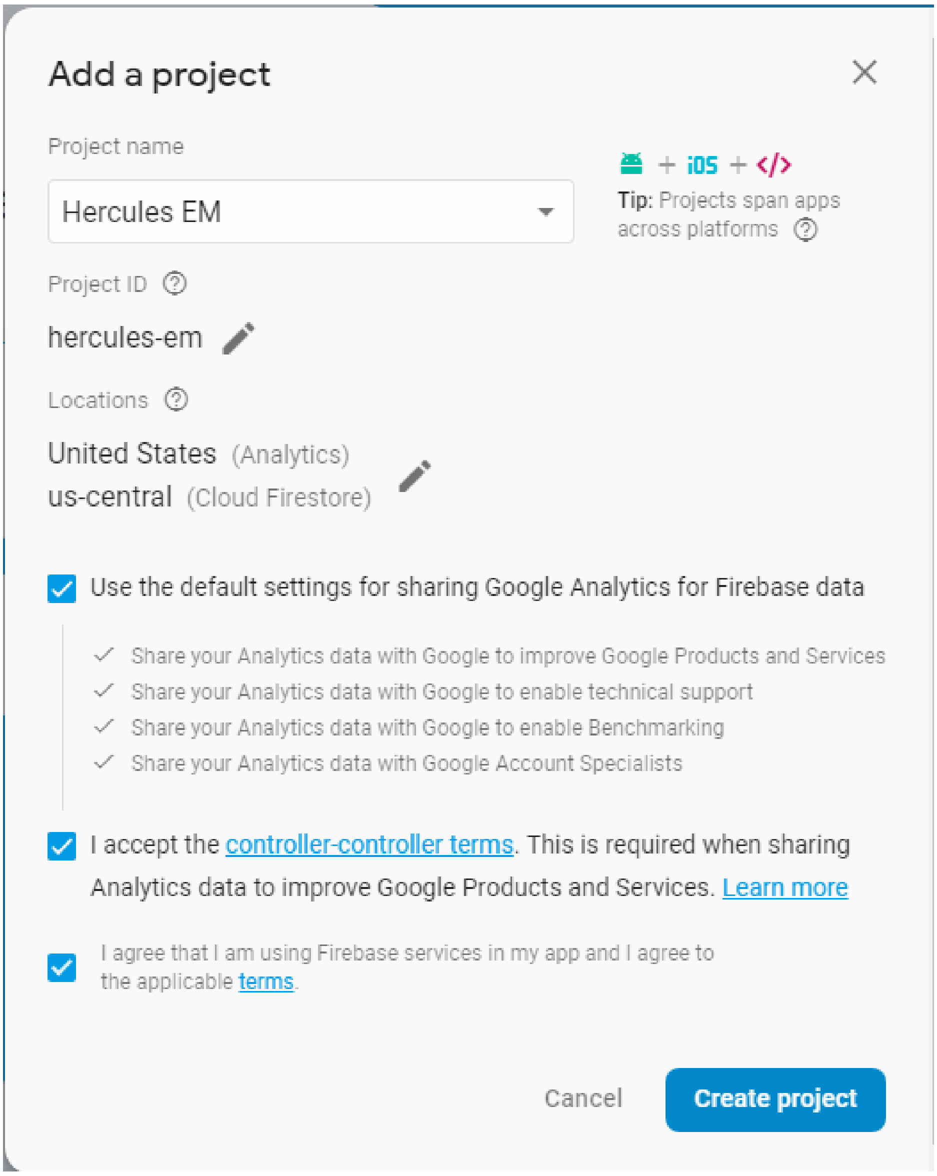
- Login to the Google Firebase API Console at **https://console.firebase.google.com**, using your Google account.



Welcome to Firebase!

Tools from Google for developing great apps, engaging with your users, and earning more through mobile ads.

- Click 'Add Project'



Add a project

Project name

Hercules EM

Tip: Projects span apps across platforms

Project ID

hercules-em

Locations

United States (Analytics)
us-central (Cloud Firestore)

☑ Use the default settings for sharing Google Analytics for Firebase data

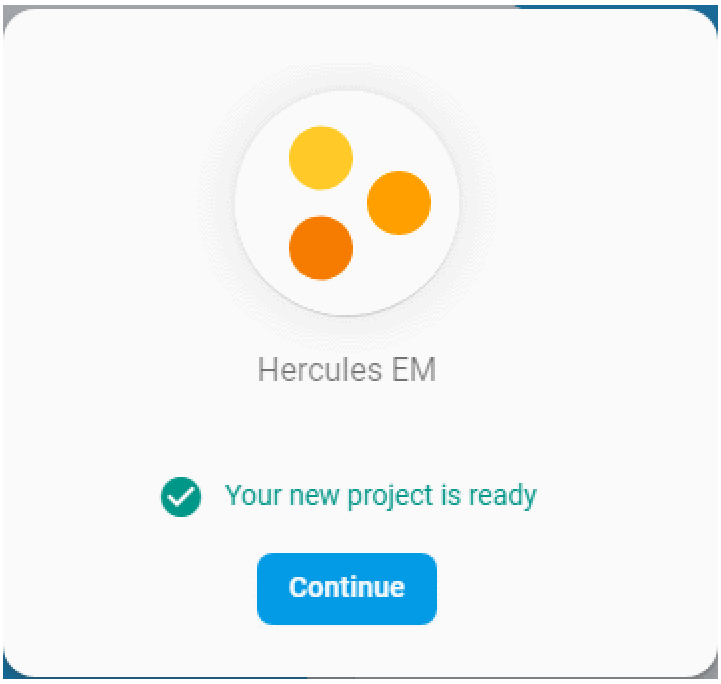
- ✓ Share your Analytics data with Google to improve Google Products and Services
- ✓ Share your Analytics data with Google to enable technical support
- ✓ Share your Analytics data with Google to enable Benchmarking
- ✓ Share your Analytics data with Google Account Specialists

☑ I accept the controller-controller terms. This is required when sharing Analytics data to improve Google Products and Services. Learn more

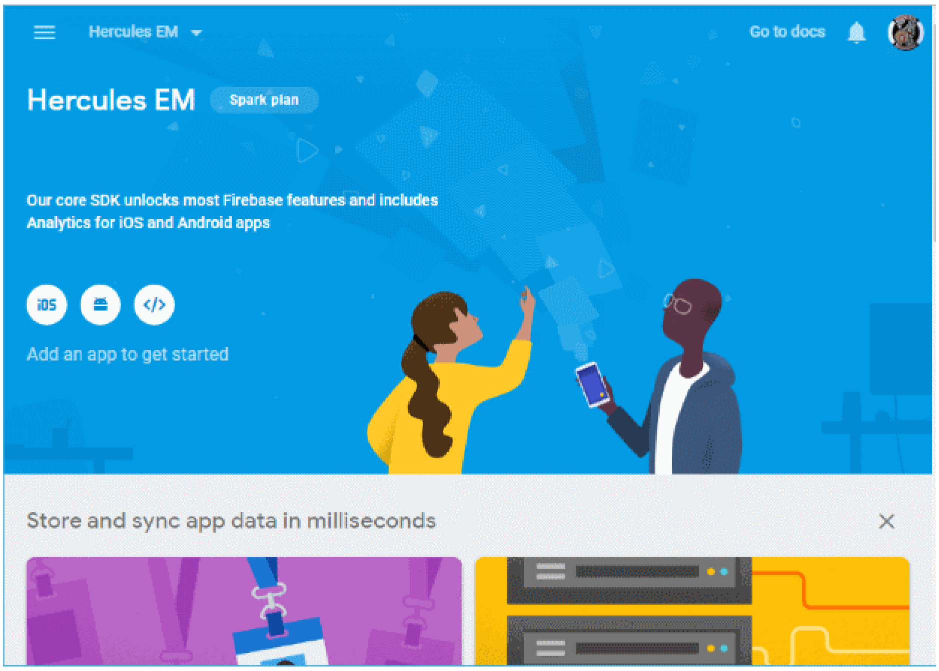
☑ I agree that I am using Firebase services in my app and I agree to the applicable terms.

- Type a name for the new project in the 'Project name' field
- Click the pencil icon beside the 'Locations' field and select your country and Google Cloud Firestore server location nearest to you.
- Leave 'Use the default settings for sharing Google Analytics for Firebase data' selected
- Read Agree to the terms and conditions by selecting respective checkboxes
- Click 'Create Project'.

Your project is created.

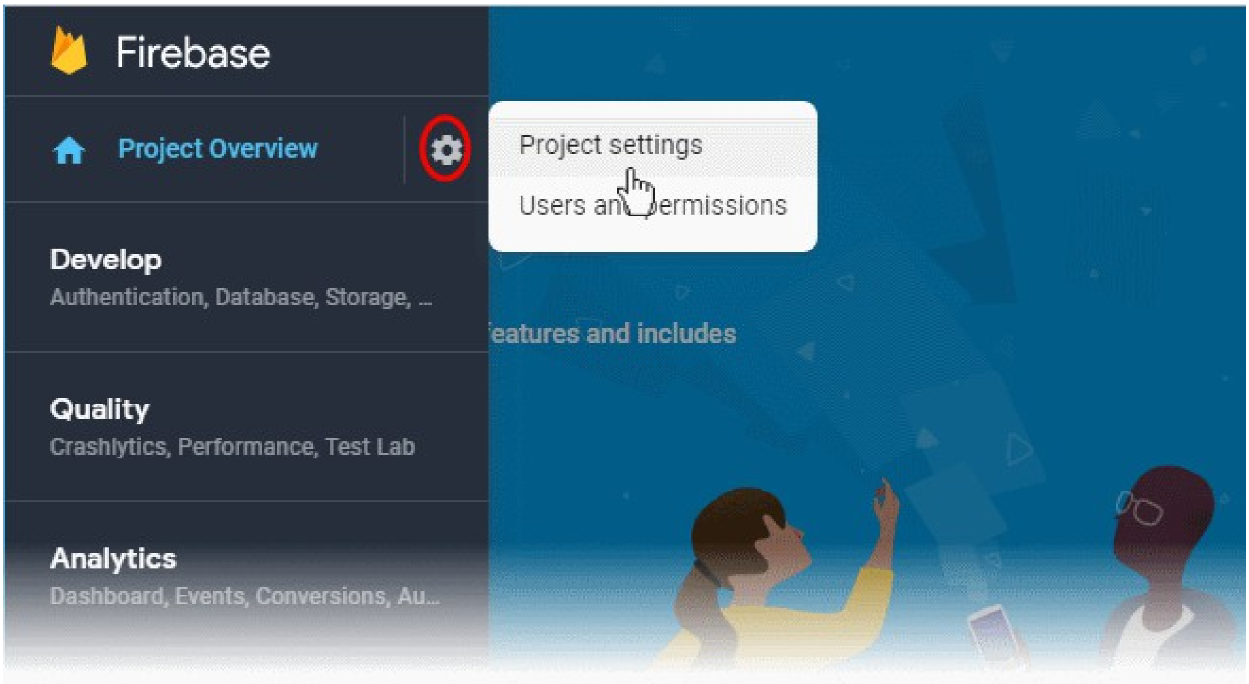


- Click 'Continue' to go to the project dashboard


Hercules EM
Go to docs
Hercules EM
Spark plan
Our core SDK unlocks most Firebase features and includes Analytics for iOS and Android apps
iOS
</>
Add an app to get started
Store and sync app data in milliseconds

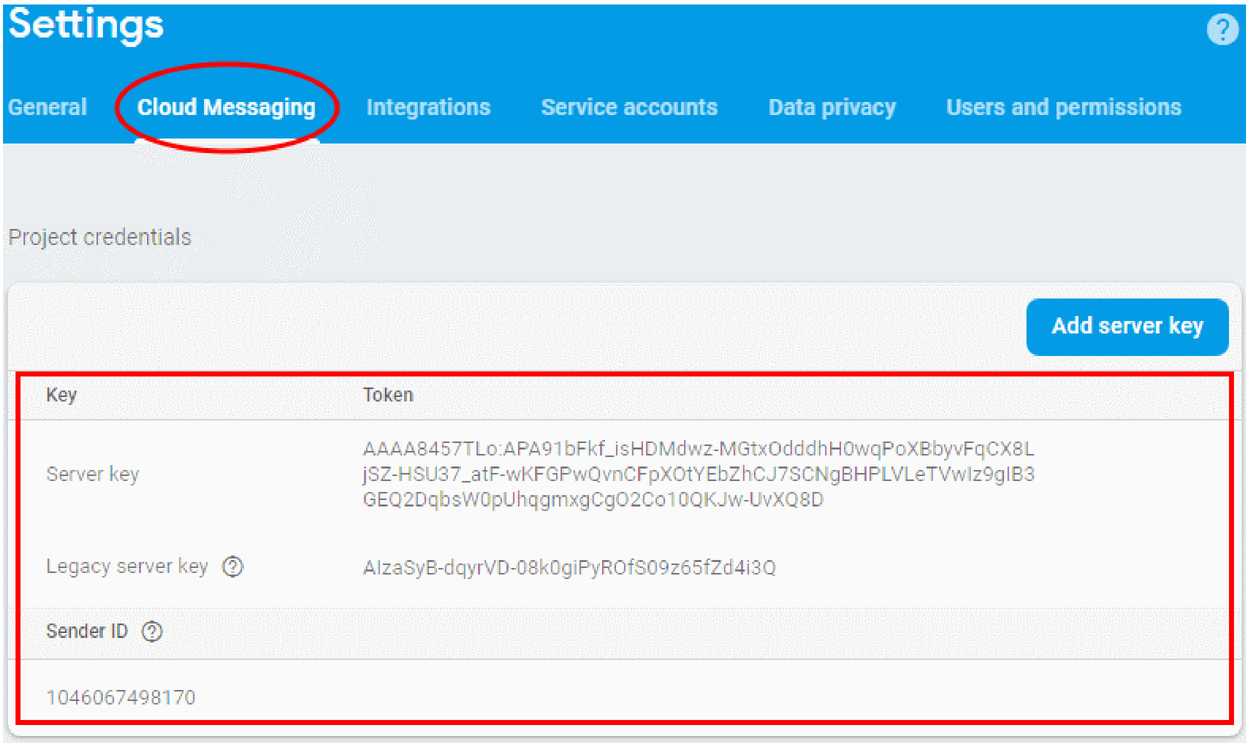
## Step 2 - Obtain GCM Token and Project number

- Click the hamburger button
- Click the gear icon beside 'Project Overview' and choose 'Project settings' from the options.


Firebase
Project Overview
Project settings
Users and permissions
Develop
Authentication, Database, Storage, ...
Quality
Crashlytics, Performance, Test Lab
Analytics
Dashboard, Events, Conversions, Au...
features and includes

The 'Settings' screen for the project appears.

- Click the 'Cloud Messaging' tab.



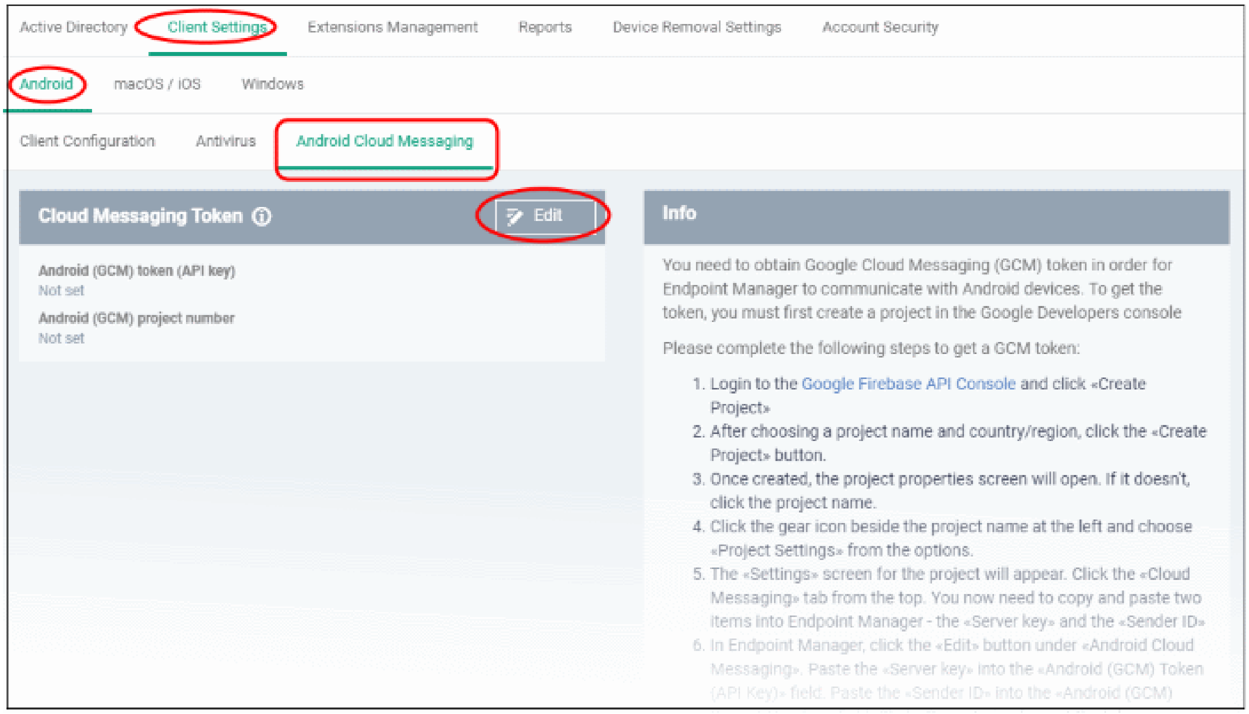
Project credentials

| Key | Token |
|---|---|
| Server key | AAAA8457TLo:APA91bFkf_isHDMdwz-MGtxOdddhH0wqPoXBbyvFqCX8L jSZ-HSU37_atF-wKFGPwQvnCFpXOtYEbZhCJ7SCNgBHPLVLeTVwlz9glB3 GEQ2DqbsW0pUhqgmxgCgO2Co10QKJw-UvXQ8D |
| Legacy server key | AIzaSyB-dqyrVD-08k0giPyROfS09z65fZd4i3Q |
| Sender ID | |
| 1046067498170 | |

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

## Step 3 - Enter GCM Token and Project number

- Login to Endpoint Manager
- Click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'Android' > 'Android Cloud Messaging' tab



Android (GCM) token (API key)
Not set

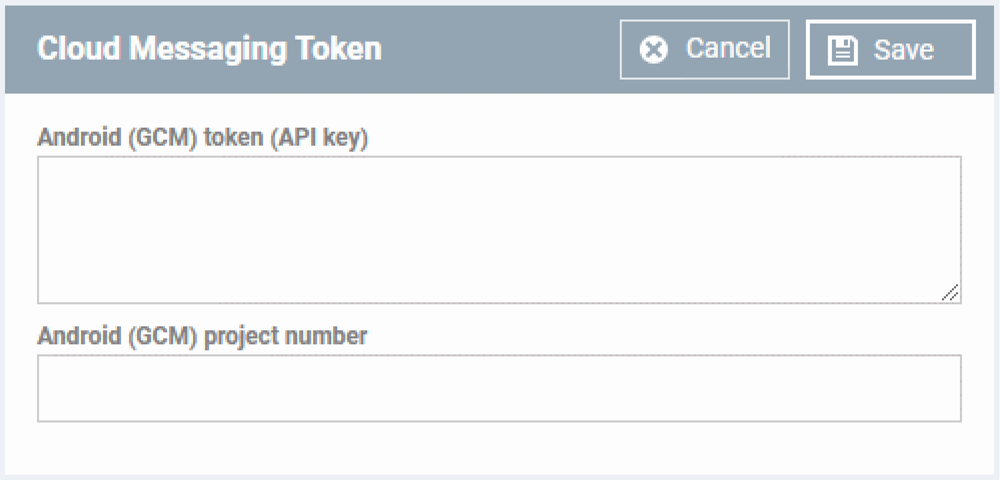
Android (GCM) project number
Not set

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

Please complete the following steps to get a GCM token:

1. Login to the Google Firebase API Console and click «Create Project»
2. After choosing a project name and country/region, click the «Create Project» button.
3. Once created, the project properties screen will open. If it doesn't, click the project name.
4. Click the gear icon beside the project name at the left and choose «Project Settings» from the options.
5. The «Settings» screen for the project will appear. Click the «Cloud Messaging» tab from the top. You now need to copy and paste two items into Endpoint Manager - the «Server key» and the «Sender ID»
6. In Endpoint Manager, click the «Edit» button under «Android Cloud Messaging». Paste the «Server key» into the «Android (GCM) Token (API Key)» field. Paste the «Sender ID» into the «Android (GCM)

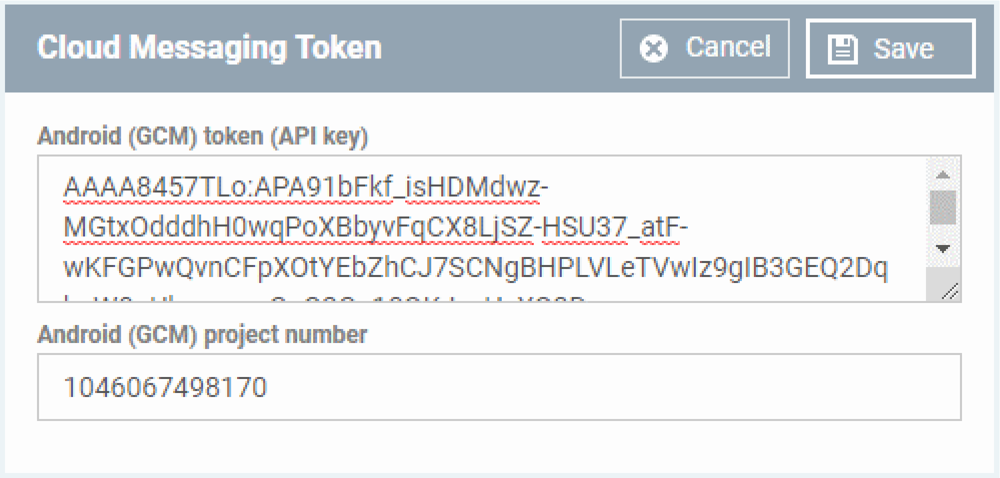
- Click the edit button at the top right of the 'Cloud Messaging Token' column, to view the GCM token and project number fields



Android (GCM) token (API key)

Android (GCM) project number

- Paste the 'Server key' into 'Android (GCM) Token' field.
- Paste the 'Sender ID' into 'Android (GCM) Project Number' field.



Android (GCM) token (API key)

AAAA8457TLo:APA91bFkf_isHDMdwz-MGtxOdddhH0wqPoXBbyvFqCX8LjSZ-HSU37_atF-wKFGPwQvnCFpXOtYEbZhCJ7SCNgBHPLVLeTVwIz9gIB3GEQ2Dq

Android (GCM) project number

1046067498170

- Click 'Save'.

Your settings will be updated and the token/project number will be displayed in the same interface.

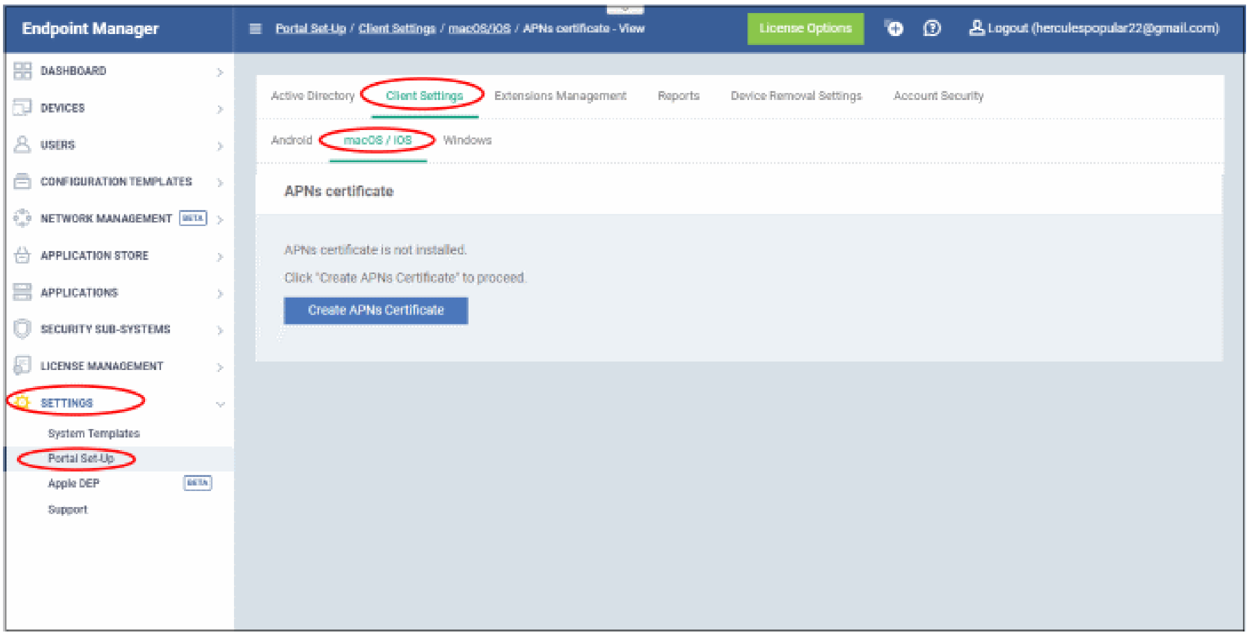
Your EM Portal will be now be able to communicate with Android devices using the unique token generated for your EM portal.

### 11.2.2.2. Add Apple Push Notification Certificate

- You need to install an Apple Push Notification (APN) certificate on your Endpoint Manager portal in order to communicate with iOS and Mac devices.
- You can enroll for an APN certificate using your Apple account. If you do not have an Apple account then please create one at **https://appleid.apple.com**. A free account is enough.
- The certificate is valid for one year. EM will remind you when your certificate is nearing expiry. It is free to renew the certificate each year
- Please follow the steps below to obtain and implement an APN certificate:

**Step 1- Generate your PLIST**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click the 'macOS / iOS' tab.

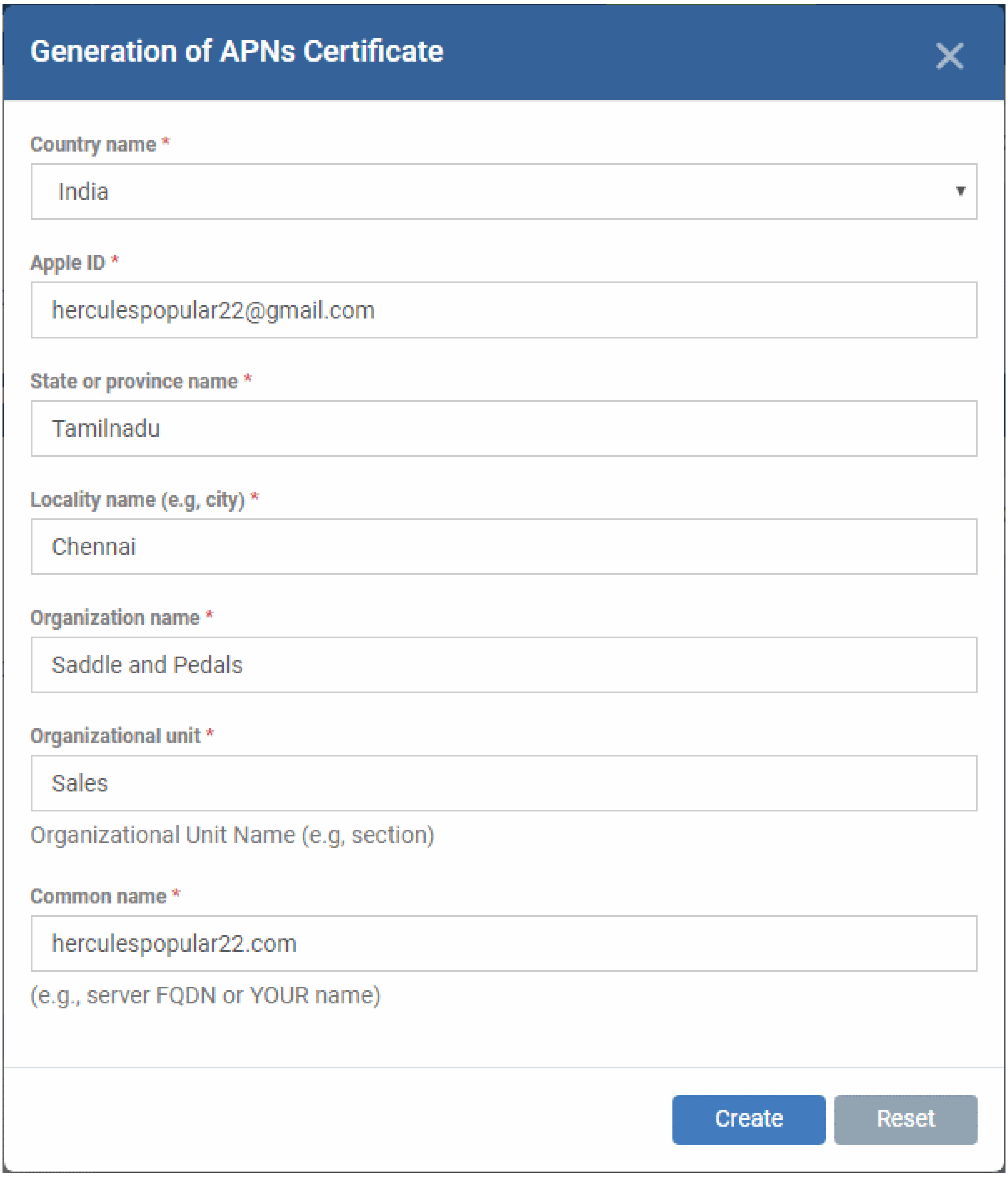


APNs certificate is not installed.

Click "Create APNs Certificate" to proceed.

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

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



Generation of APNs Certificate

Country name *: India

Apple ID *: herculespopular22@gmail.com

State or province name *: Tamilnadu

Locality name (e.g, city) *: Chennai

Organization name *: Saddle and Pedals

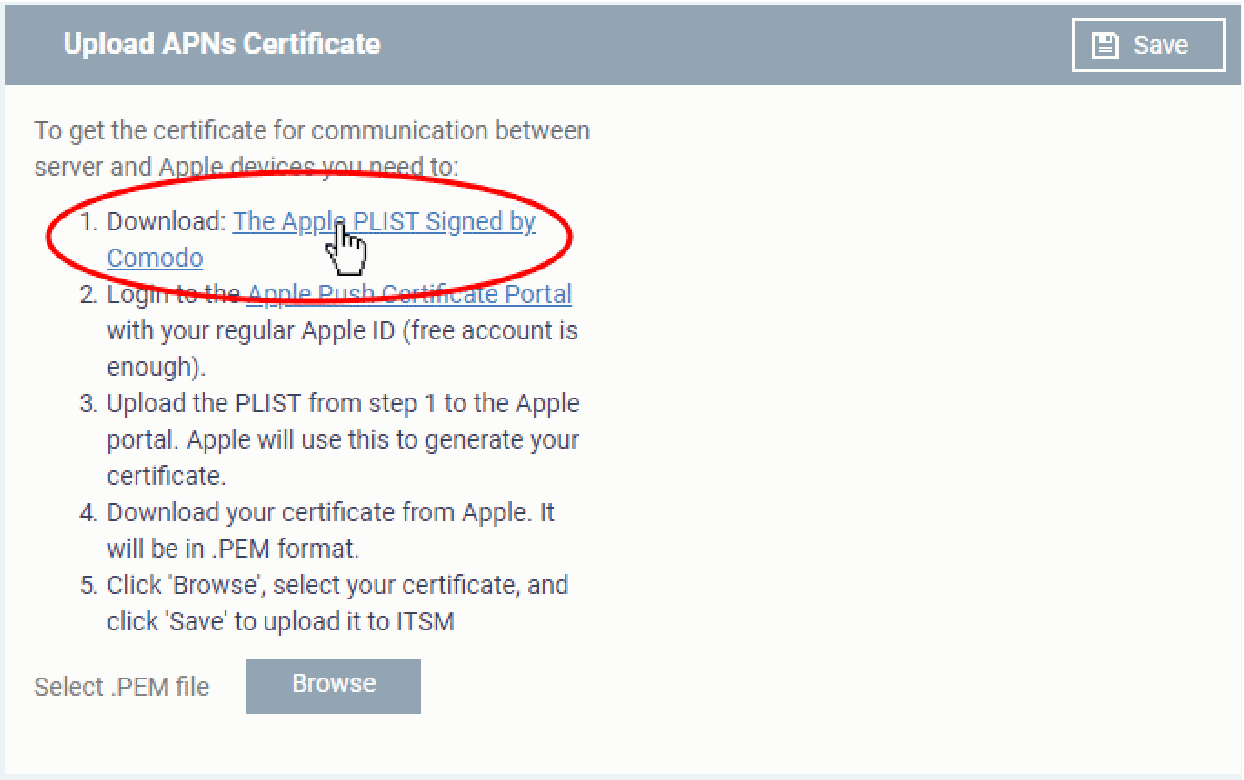
Organizational unit *: Sales

Organizational Unit Name (e.g, section)

Common name *: herculespopular22.com

(e.g., server FQDN or YOUR name)

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



Upload APNs Certificate

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

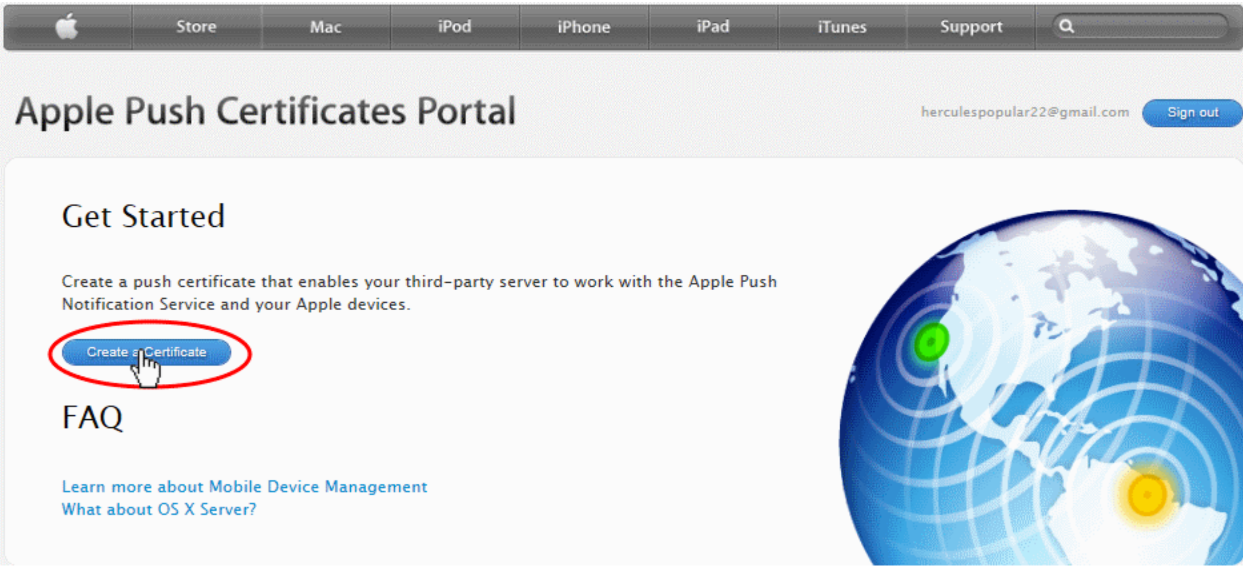
1. Download: The Apple PLIST Signed by Comodo
2. Login to the Apple Push Certificate Portal with your regular Apple ID (free account is enough).
3. Upload the PLIST from step 1 to the Apple portal. Apple will use this to generate your certificate.
4. Download your certificate from Apple. It will be in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

Select .PEM file

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

**Step 2 -Obtain Your Certificate From Apple**

- Login to the 'Apple Push Certificates Portal' with your Apple ID at **https://identity.apple.com/pushcert/**.
- Once logged in, click 'Create a Certificate'.



Apple Push Certificates Portal

herculespopular22@gmail.com

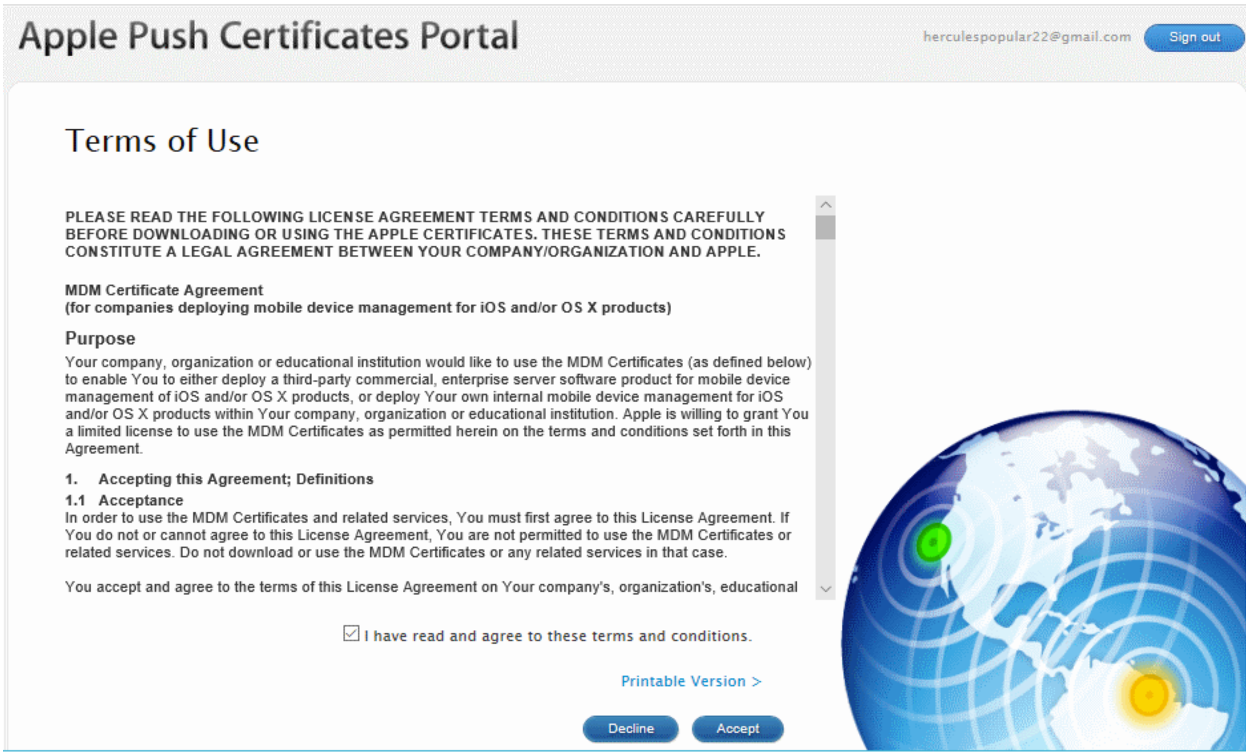
Get Started

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

FAQ

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

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



Apple Push Certificates Portal

Terms of Use

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

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

Purpose

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

1. Accepting this Agreement; Definitions

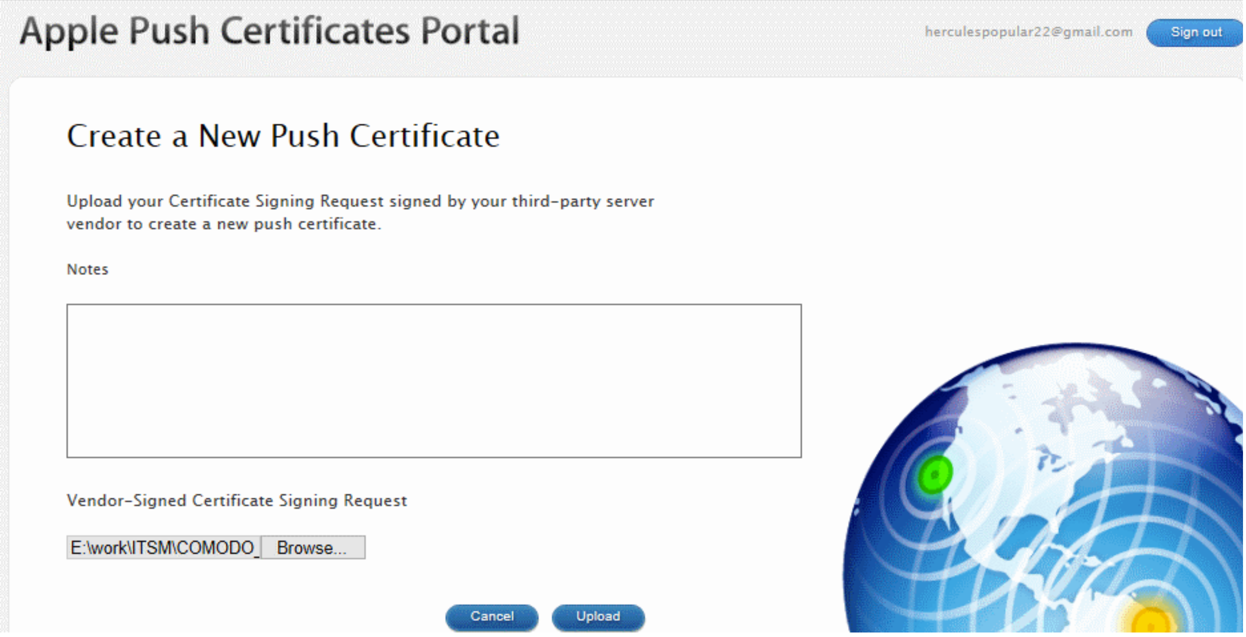
1.1 Acceptance

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

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational

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

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



Apple Push Certificates Portal

Create a New Push Certificate

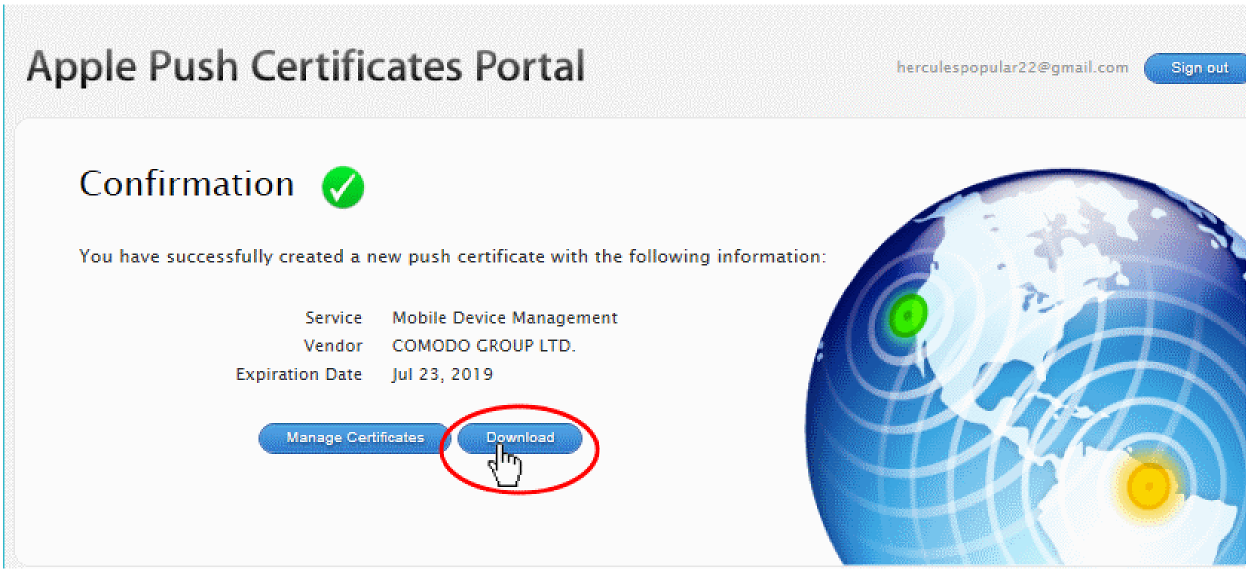
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

E:\work\ITSM\COMODO_ Browse...

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



Apple Push Certificates Portal

Confirmation

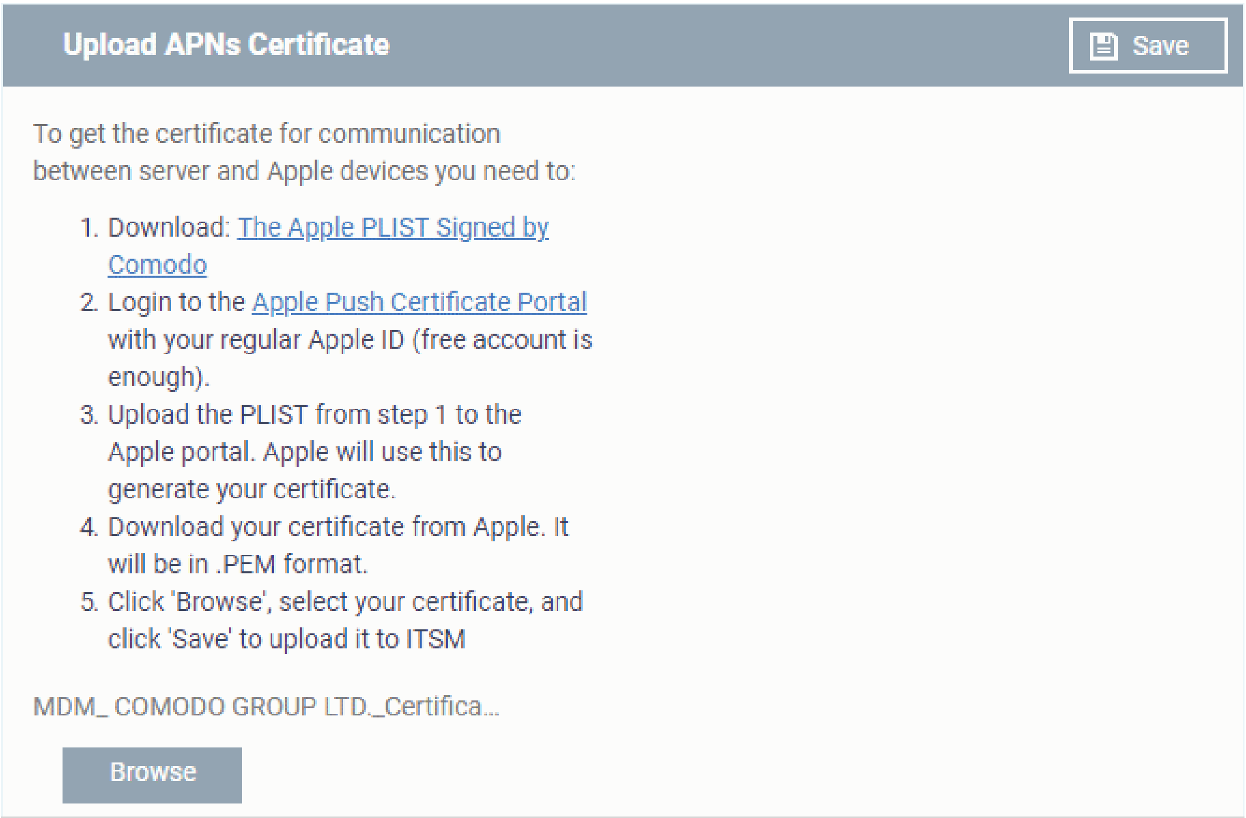
You have successfully created a new push certificate with the following information:

| | |
|---|---|
| Service | Mobile Device Management |
| Vendor | COMODO GROUP LTD. |
| Expiration Date | Jul 23, 2019 |

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

**Step 3 - Upload your certificate to Endpoint Manager**

- Return to EM, click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'macOS / iOS'
- Click the 'Browse' button, locate your certificate file and select it.



Upload APNs Certificate

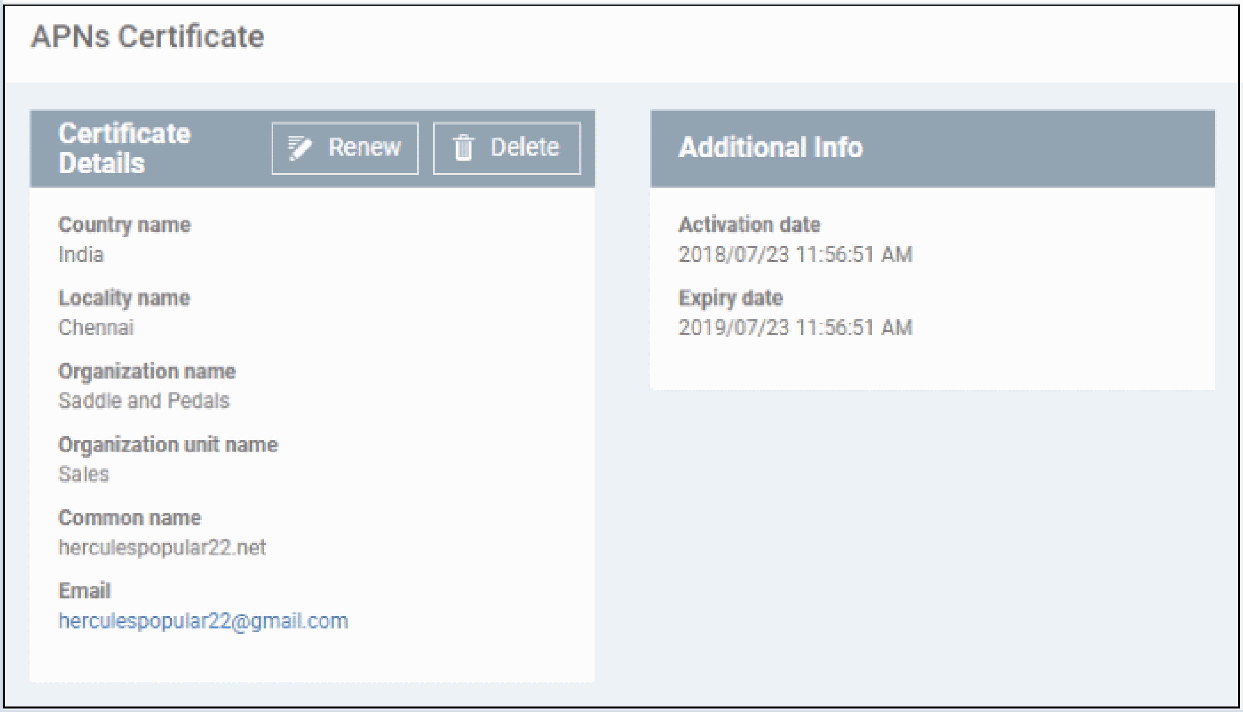
To get the certificate for communication between server and Apple devices you need to:

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

MDM_ COMODO GROUP LTD._Certifica...

- Click 'Save' to upload your certificate.

The APNs Certificate details interface opens:



APNs Certificate

Country name
India

Locality name
Chennai

Organization name
Saddle and Pedals

Organization unit name
Sales

Common name
herculespopular22.net

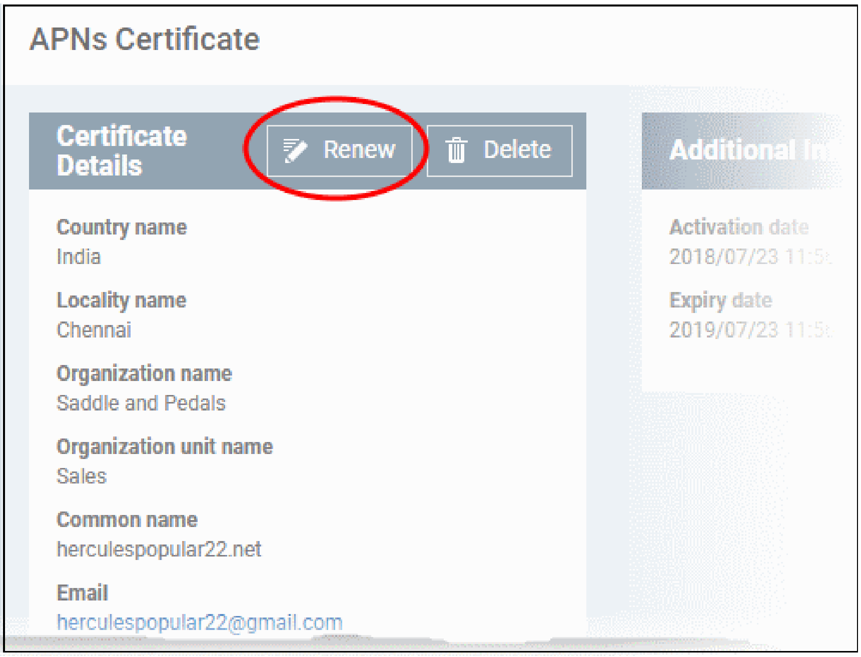
Email
herculespopular22@gmail.com

Activation date
2018/07/23 11:56:51 AM

Expiry date
2019/07/23 11:56:51 AM

Endpoint Manager can now communicate with iOS and Mac OS devices. You can enroll iOS devices and Mac OS devices for management.

- The certificate is valid for 365 days. EM will remind you when your certificate is due to expire.
- 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 and Mac devices.
    - Click 'Renew' in the APNs certificate details interface to renew the cert:



APNs Certificate

Country name
India

Locality name
Chennai

Organization name
Saddle and Pedals

Organization unit name
Sales

Common name
herculespopular22.net

Email
herculespopular22@gmail.com

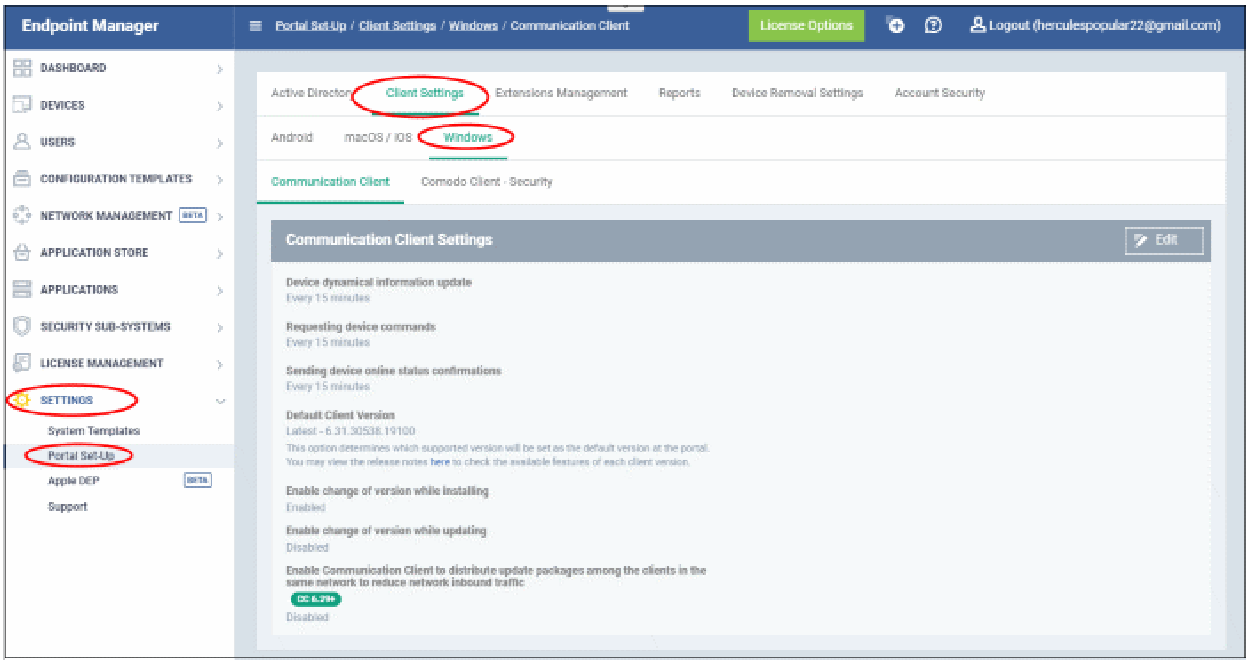
Activation date
2018/07/23 11:5

Expiry date
2019/07/23 11:5

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

### 11.2.2.3. Configure Windows Clients

- Click 'Settings' > 'Portal Set-up' > 'Client Settings' then open the 'Windows' tab
- This area lets you configure settings such as the interval between device updates, the default client version and more.



Communication Client Settings

Device dynamical information update
Every 15 minutes

Requesting device commands
Every 15 minutes

Sending device online status confirmations
Every 15 minutes

Default Client Version
Latest - 6.31.30538.19100
This option determines which supported version will be set as the default version at the portal.
You may view the release notes here to check the available features of each client version.

Enable change of version while installing
Enabled

Enable change of version while updating
Disabled

Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic
CC 6.29+
Disabled

Click the following links for help with each client's settings:

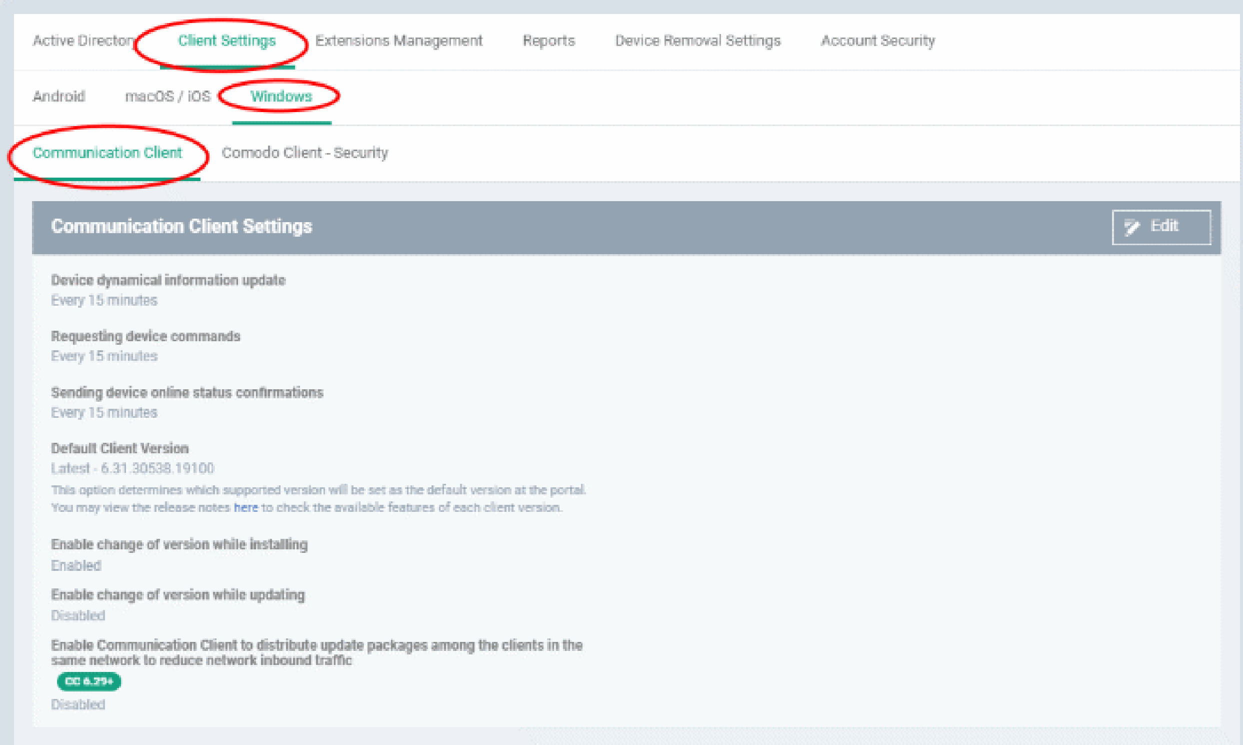
- **Configure Communication Client Settings**
- **Configure Client Security Settings**

### 11.2.2.3.1. Configure Communication Client Settings

- The communication client is an agent installed on your managed devices. It receives commands and tasks from Endpoint Manager and implements them on those devices. The client also informs Endpoint Manager of the endpoint's status.
- The settings area lets you:
  - Configure update intervals
  - Set the 'Default client version' which is installed on your endpoints. This is set to always fetch and install the latest version unless you specify otherwise.
  - Specify whether admins can change the version of the client installed on an endpoint.
  - Choose whether to use an endpoint as the source from which other endpoints collect their updates. This can save time / bandwidth over each endpoint downloading direct from the server.

**Configure the Windows communication client**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click the 'Windows' tab > 'Communication Client'



Communication Client Settings

Device dynamical information update
Every 15 minutes

Requesting device commands
Every 15 minutes

Sending device online status confirmations
Every 15 minutes

Default Client Version
Latest - 6.31.30538.19100
This option determines which supported version will be set as the default version at the portal.
You may view the release notes here to check the available features of each client version.

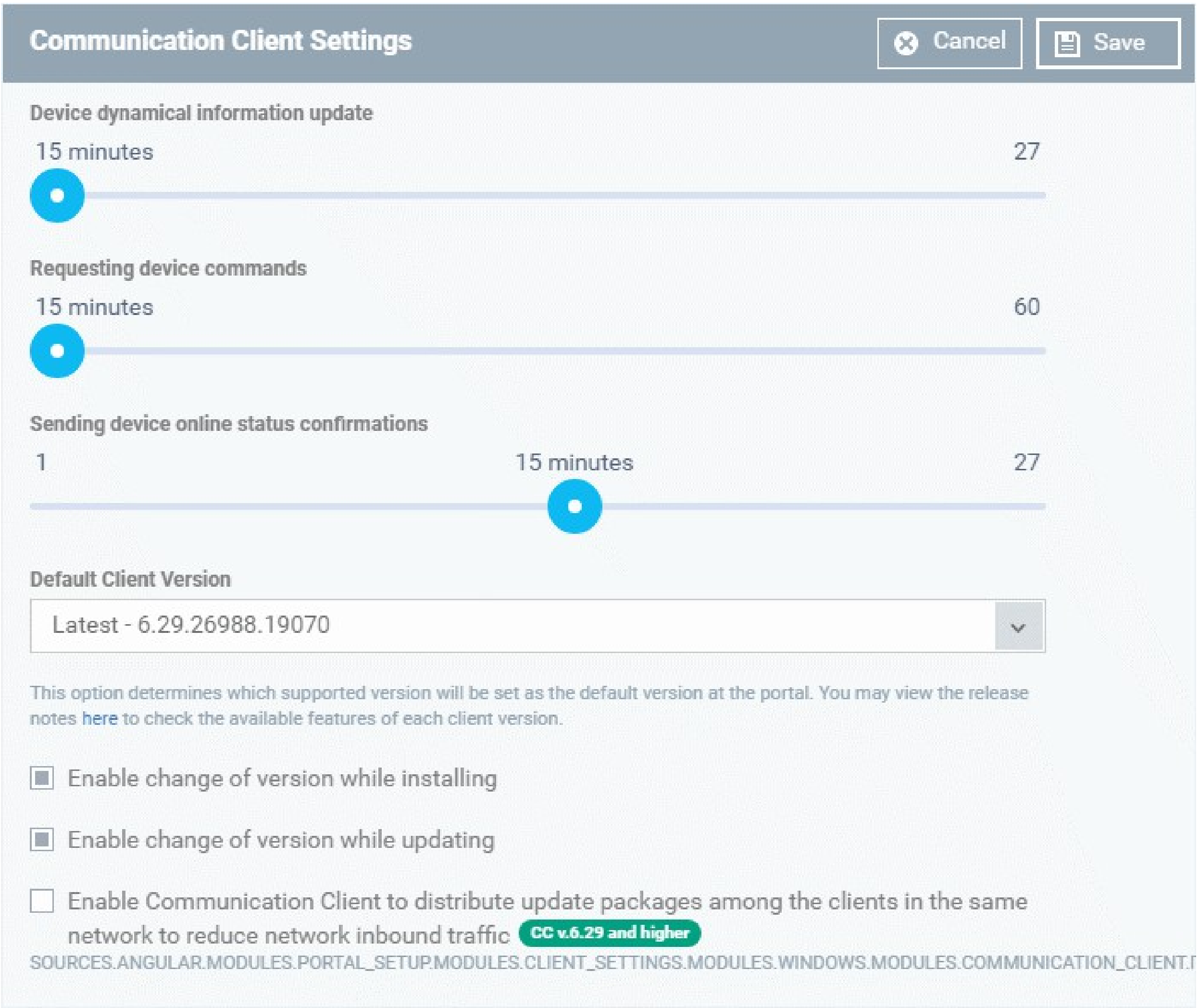
Enable change of version while installing
Enabled

Enable change of version while updating
Disabled

Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic
CC 6.29+
Disabled

The default values of the settings are displayed.

- Click the edit button Edit on the top right to modify these settings



Communication Client Settings

Device dynamical information update

15 minutes 27

Requesting device commands

15 minutes 60

Sending device online status confirmations

1 15 minutes 27

Default Client Version

Latest - 6.29.26988.19070

This option determines which supported version will be set as the default version at the portal. You may view the release notes here to check the available features of each client version.

☒ Enable change of version while installing

☒ Enable change of version while updating

☐ Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic CC v.6.29 and higher

SOURCES.ANGULAR.MODULES.PORTAL_SETUP.MODULES.CLIENT_SETTINGS.MODULES.WINDOWS.MODULES.COMMUNICATION_CLIENT.I

- **Device dynamical information update -** How often the client should provide Endpoint Manager with device status updates. This includes, for example, available memory, name of the device, OS summary, CCS configuration, and network information.
  - Use the slider to set the update interval. (***Default = 15 minutes***)
- **Requesting device commands -** The frequency at which the client should query Endpoint Manager for new tasks and updates.
  - Use the slider to set the update interval. (***Default = 15 minutes***)
- **Sending device online status confirmations -** The frequency at which the client should send a message confirming the device is online and connected. Endpoint Manager changes the device status to 'Offline' if it does not receive a confirmation in the set time period.
  - Use the slider to set the update interval. (***Default = 15 minutes***)
- **Default Client Version -** Determines which agent version should be installed on endpoints.
  - Choose the default agent version from the drop down. (***Default = 'Latest'***).
- **Enable change of version while installing -** Whether admins can install a version of the client that is different to the 'Default client version'. (Default = Disabled)

  If enabled, admins can choose the version of the client they want to install in the following interfaces:
  - **Enroll devices -** 'Devices' > 'Device List' > 'Enroll Device'
  - **Bulk installation -** 'Devices' > 'Bulk Installation Package'

- **Enable change of version while updating -** Whether admins can update a client to a version that is different to the 'Default client version'. (***Default = Disabled***)

  If enabled, admins can choose the version of the client they want to update to in the following interfaces:

  - **Update additional packages -** 'Devices' > 'Device List' > 'Install or Update Packages' > 'Update Additional Packages'
  - **Updates section of Windows profile -** 'Configuration Templates' > 'Profiles' > 'Windows Profile' > 'Updates' profile section

  **Note -** Make sure to upgrade to a higher version. Installing a lower version than the existing agent is not supported.

- **Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic -** Download updates to a managed endpoint, then use that endpoint as the source from which other endpoints collect their updates.

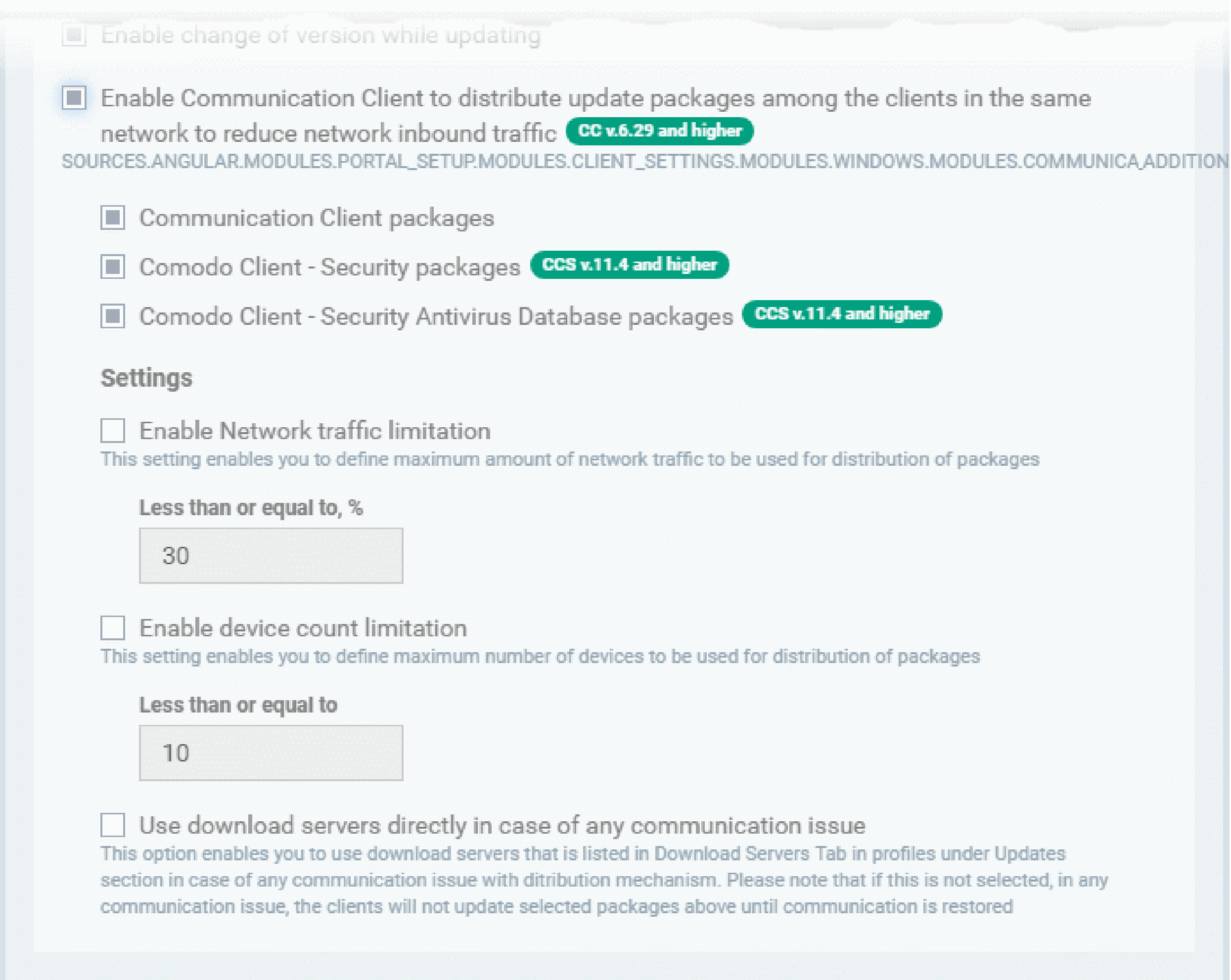
  This saves internet bandwidth usage and accelerates updates in large networks.

  If enabled, your endpoint clients will follow this process at update time:

  - The endpoint first checks other endpoints to see if the update is installed on them
  - If available, the client fetches the update from the local endpoint
  - If not available, the client downloads the update from the default download servers
  - This endpoint then becomes the source from which other endpoints collect their updates.

  You can choose the type of updates that use this mechanism:

  - **Communication Client updates** (Version 6.29 or higher)
  - **Comodo Client Security updates** (Version 11.4 or higher)
  - **Antivirus Database updates** (Version 11.4 or higher)



☐ Enable change of version while updating

☑ Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic CC v.6.29 and higher

SOURCES.ANGULAR.MODULES.PORTAL_SETUP.MODULES.CLIENT_SETTINGS.MODULES.WINDOWS.MODULES.COMMUNICA.ADDITION

☑ Communication Client packages

☑ Comodo Client - Security packages CCS v.11.4 and higher

☑ Comodo Client - Security Antivirus Database packages CCS v.11.4 and higher

Settings

☐ Enable Network traffic limitation

This setting enables you to define maximum amount of network traffic to be used for distribution of packages

Less than or equal to, %

30

☐ Enable device count limitation

This setting enables you to define maximum number of devices to be used for distribution of packages

Less than or equal to

10

☐ Use download servers directly in case of any communication issue

This option enables you to use download servers that is listed in Download Servers Tab in profiles under Updates section in case of any communication issue with ditribution mechanism. Please note that if this is not selected, in any communication issue, the clients will not update selected packages above until communication is restored

- **Enable Network traffic limitation** - The maximum % of network bandwidth that can be used to share updates. (***Default = 30%***)
- **Enable device count limitation** - The maximum number of devices with which the client is allowed to share updates. Default = 10.
- **Use download servers directly in case of any communication issue** - If the endpoint cannot contact other endpoints it will collect the update from the main server.

- Click 'Save' to apply your changes.

The following table shows how clients will collect updates in different scenarios:

| | Enable Communication Client to distribute ... | Select specific devices to be proxy ... | Use download servers directly in case ... | Will download from: |
|---|---|---|---|---|
| Scenario 1 | ✓ | ✗ | ✗ | Any local device which already has the update |
| Scenario 2 | ✓ | ✓ | ✗ | Only from selected devices |
| Scenario 3 | ✓ | ✗ | ✓ | 1. Any device in the |

| | | | | |
|---|---|---|---|---|
| | | | | local network<br>2. Download servers |
| Scenario 4 | ✓ | ✓ | ✓ | 1. Selected devices<br>2. Download servers |

**Additional Notes**:

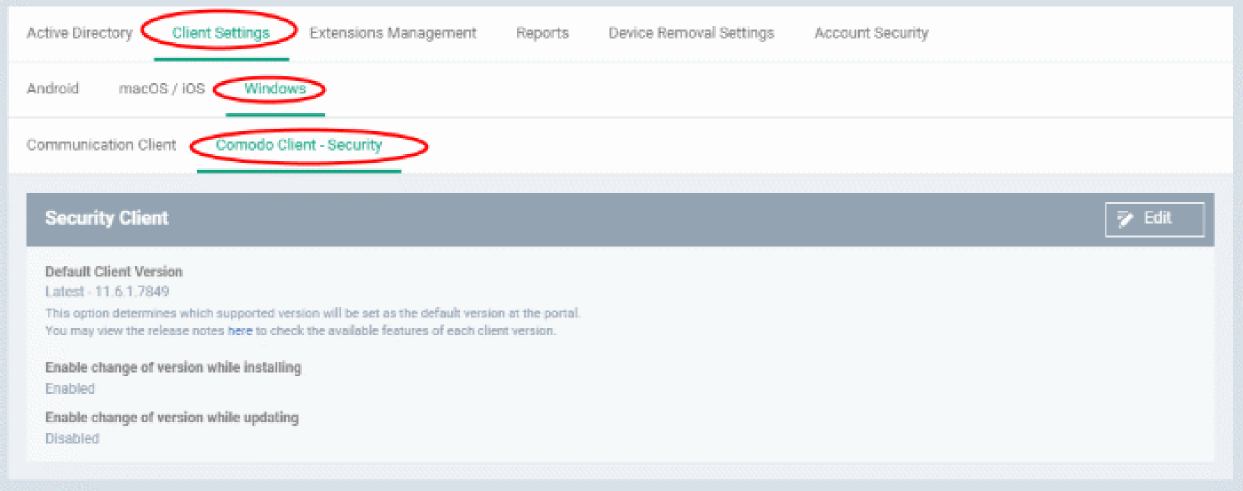
- The settings described in this section are 'global' settings which apply to all endpoint clients. However, you can also configure client update settings by adding an 'Updates' section to profile.
- There is one overlapping item between these two - 'Enable the communication client to distribute packages to other clients in the network'.
- Endpoint Manager prioritizes this setting as follows:
  - If you *do not* add an update section to the profile, then the global settings apply
  - If you *do* add an update section, then Endpoint Manager will ignore the '...distribute...' settings in global settings

### 11.2.2.3.2. Configure Client Security Settings

- Comodo Client Security (CCS) provides advanced endpoint protection such as antivirus, firewall and more
- The client security settings area lets you:
  - Set the default client version which should be installed on your endpoints. This is set to always fetch and install the latest version, unless you specify otherwise.
  - Specify whether admins can change the installed version of the client from a command elsewhere in Endpoint Manager.
    - In other words, can admins choose to install a different version of the client in a 'Bulk Installation Package', for example?
    - If you leave the ' Enable change...' options deselected, then admins will not have the option to install a different client version when installing or updating the client.

**Configure the Windows client security**

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'
- Click the 'Windows' tab > 'Client Security'



Default Client Version

Latest - 11.6.1.7849

This option determines which supported version will be set as the default version at the portal.
You may view the release notes here to check the available features of each client version.

Enable change of version while installing

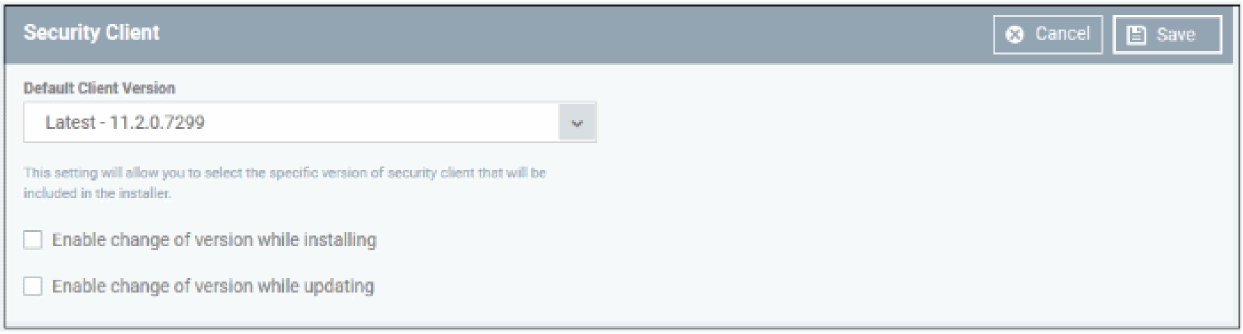
Enabled

Enable change of version while updating

Disabled

The default values of the settings are displayed.

- Click the edit button Edit on the top right to modify these settings



Default Client Version

Latest - 11.2.0.7299

This setting will allow you to select the specific version of security client that will be included in the installer.

□ Enable change of version while installing

□ Enable change of version while updating

.

| Windows Client Security Settings | |
|---|---|
| **Parameter** | **Description** |
| Default Client Version | Determines which security client should be installed or updated on endpoints. You can choose the default security client version from the drop down.<br>Default security client version is 'Latest' |
| Enable change of version while installing | Can admins install a version of the client that is different to the 'Default client version'?<br>If enabled, admins can choose the version of the client they want to install in the following interfaces:<br>• **Enroll devices** - 'Devices' > 'Device List' > 'Enroll Device'<br>• **Bulk installation** - 'Devices' > 'Bulk Installation Package'<br>• **Install additional packages** - 'Devices' > 'Device List' > 'Install or Update Packages' > 'Update Additional Packages'<br>**Default = Disabled** |
| Enable change of version while updating | Can admins update to a client version that is different to the 'Default client version'?<br>If enabled, admins can choose the version of the client they want to update to in the following interfaces:<br>• **Update additional packages** - 'Devices' > 'Device List' > 'Install or Update Packages' > 'Update Additional Packages'<br>• **Updates section of Windows profile** - 'Configuration Templates' > 'Profiles' > 'Windows Profile' > 'Updates' profile section<br>**Default = Disabled**<br>Note - Make sure to upgrade to a higher version. Deployment of a lower version than the existing security agent is not supported. |

- Click 'Save' to apply your changes.

### 11.2.3. Manage Endpoint Manager Extensions

- Click 'Settings' > 'Portal Set-up' > 'Extensions Management'
- Endpoint Manager Extensions are additional software modules which administrators can add to EM to expand its functionality. Once added, each extension can be controlled and managed from the EM interface.
- The 'Extensions Management' interface lets you enable or disable modules.

The extension currently available is:

- **Comodo Client Security** - Comodo Client Security is the remotely managed Client Security software installed on managed Windows devices. It offers complete protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, an advanced host intrusion prevention system (HIPS) and Containment feature that runs unknown and unrecognized applications in an isolated environment at the endpoints. CCS can be installed on the endpoints from the 'Devices' interface. See **Remotely Install and Update Packages on Windows Devices** for more details.

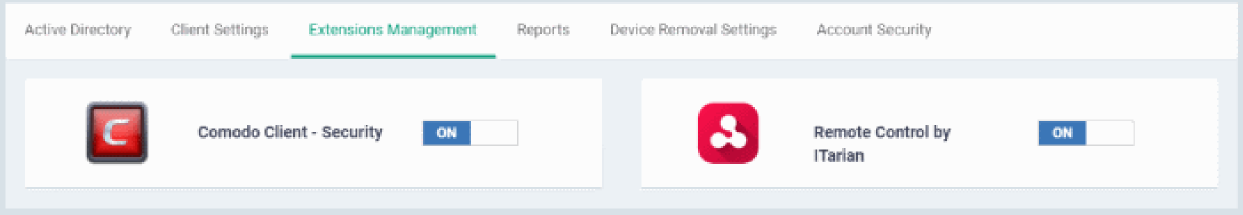
  Once installed, CCS can be configured for optimal security by applying configuration profiles. See **Profiles for Windows Devices** for more details.

- **Remote Control by ITarian** - 'Remote Control by ITarian' lets you to take control of managed Windows and Mac OS endpoints through remote desktop connection. This allows you to solve issues, install third party software, run system maintenance and more. There are two ways to remote control of a device:
  - **Remote Control by ITarian** (recommended) - Install the client viewer software on your Windows or Mac OS admin computer to take control of any managed Windows endpoint.
  - **Comodo Remote Monitoring and Management** (RMM) - Customers using our legacy RMM product can connect to Windows endpoints using the remote desktop feature built into that product.

You can take remote control of a Windows or Mac OS device from the 'Device Management' interface. For more details, see **Remote Management of Windows and Mac OS Devices**.

**Enable or disable EM extensions**

- Click 'Settings' > 'Portal Set-Up'
- Click the 'Extensions Management' tab



- Use the toggle switch in a tile to enable or disable an extension. Only extensions which are enabled will be available in the 'Device Management' interface.
- See **Remotely Install and Update Packages on Windows Devices** and **Remote Management of Windows and Mac OS Devices** for more details.

### 11.2.4. Configure Endpoint Manager Reports

Endpoint Manager undergoes rigorous Quality Assurance testing before release to ensure that the software is as stable and reliable as possible. However, in rare situations, EM may run into an exception which needs to be addressed. If the report setting is enabled, an exception report will automatically be sent to Comodo if EM encounters a problem.

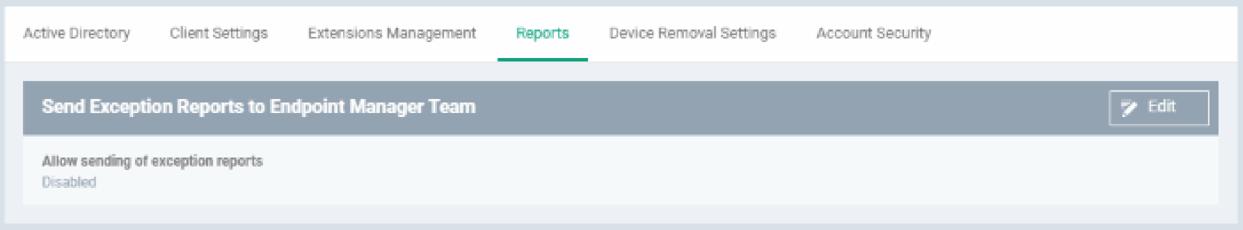
Exception reports are a valuable and constructive means of feedback that help Comodo to debug our products and improve the service we provide to our customers.

These reports contain only the line of code that failed with additional information about the circumstances of the exception. They do not contain any private information about your company or your users.

The 'Reports' interface allows you to enable or disable automated sending of exception reports. Automatic report submission is disabled by default.

**Configure exception reporting**

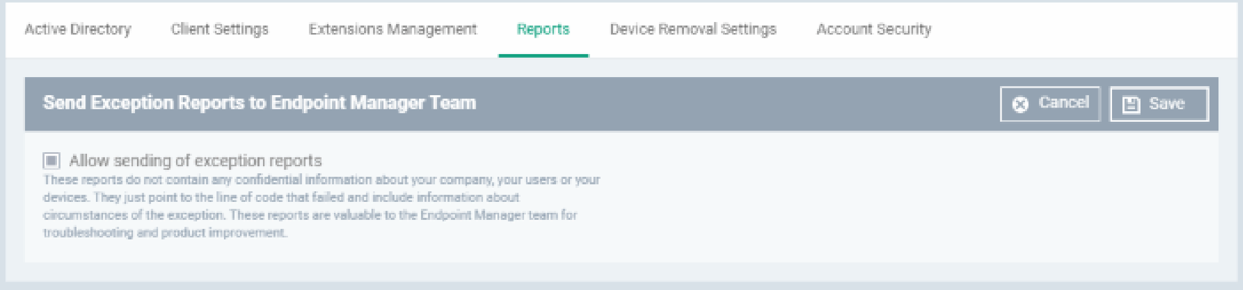
- Click 'Settings' > 'Portal Set-Up'
- Click the 'Reports' tab



Send Exception Reports to Endpoint Manager Team

Allow sending of exception reports
Disabled

- To edit the settings click the edit button Edit at the top right.



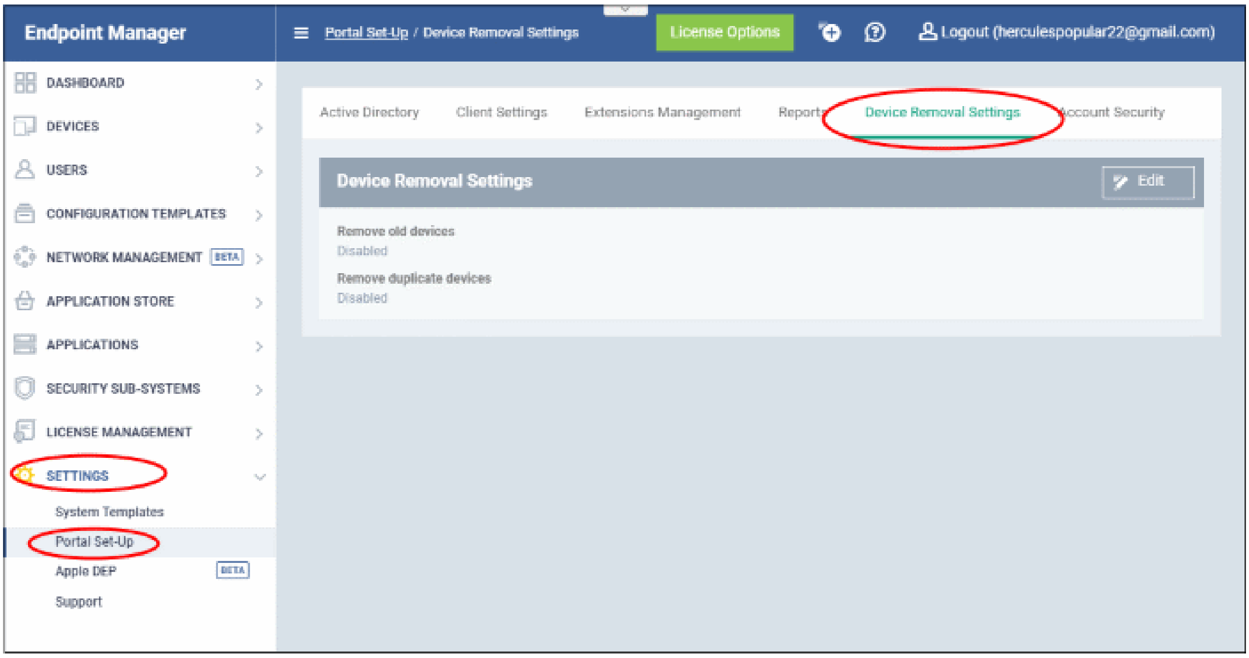
Send Exception Reports to Endpoint Manager Team

▣ Allow sending of exception reports
These reports do not contain any confidential information about your company, your users or your devices. They just point to the line of code that failed and include information about circumstances of the exception. These reports are valuable to the Endpoint Manager team for troubleshooting and product improvement.

  - **Allow sending of exception reports -** Send anonymous reports to the Endpoint Manager team if the application encounters errors
- Click 'Save' for your settings to take effect.

## 11.2.5. Configure Device Removal Settings

- Click 'Settings' > 'Portal Set-up'
- Select the 'Device Removal Settings' tab:



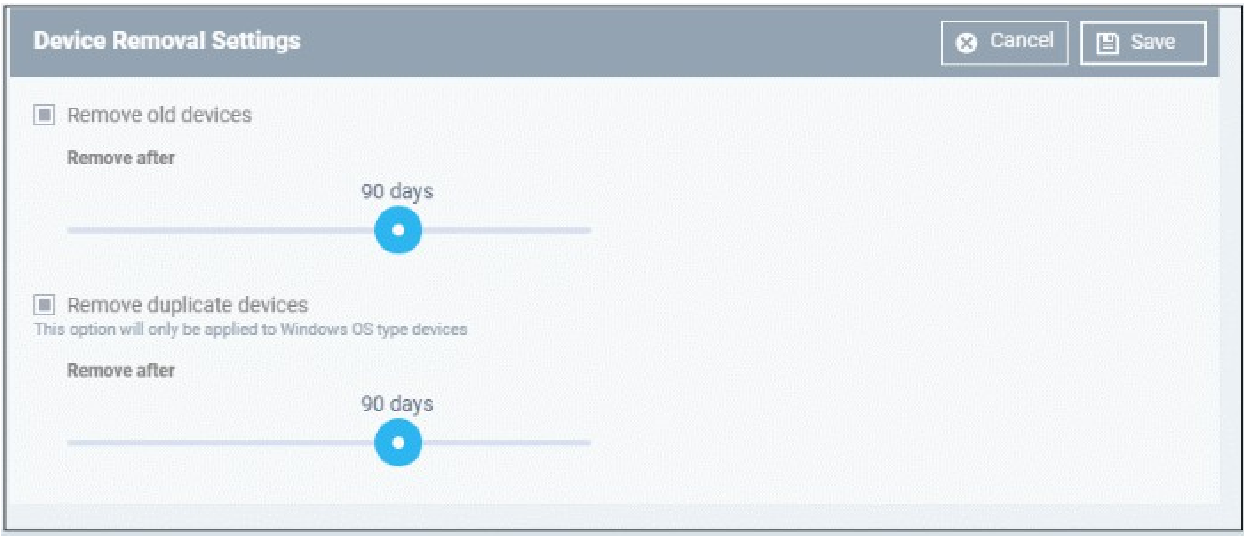
Device Removal Settings

Remove old devices
Disabled

Remove duplicate devices
Disabled

This area lets you specify whether old (inactive) and duplicate devices should be auto-removed from Endpoint Manager after a certain length of time.

- Click the 'Edit' button at top-right



Device Removal Settings

□ Remove old devices

Remove after

90 days

□ Remove duplicate devices

This option will only be applied to Windows OS type devices

Remove after

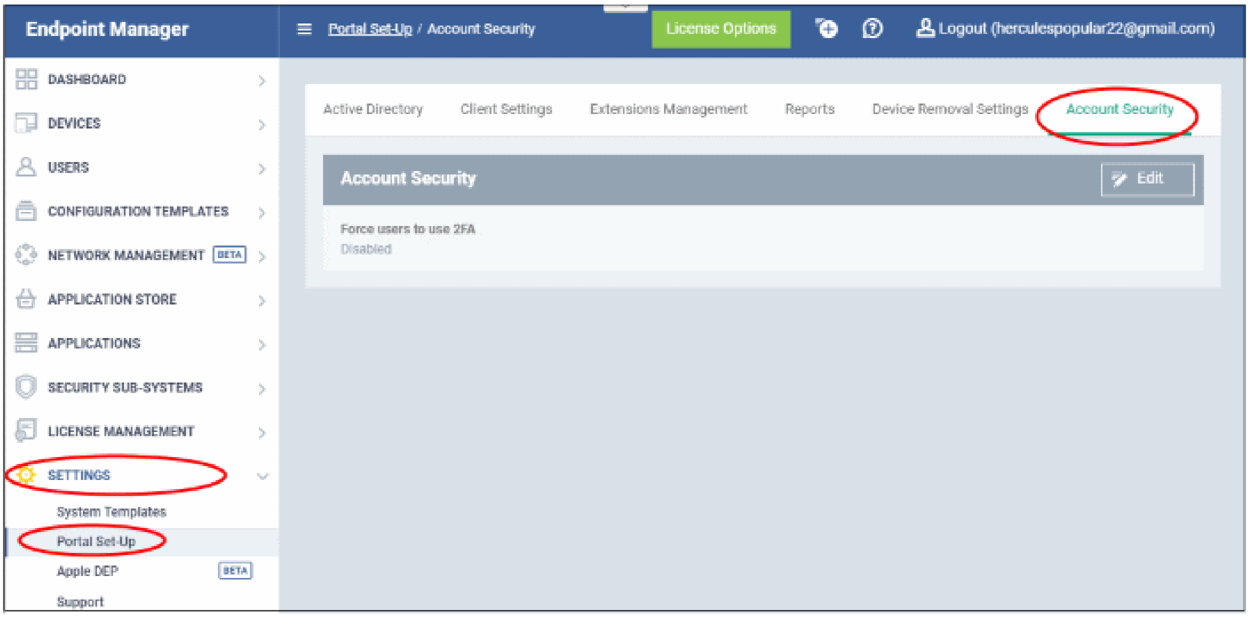
90 days

- **Remove old devices -** An 'old' device is an inactive device - one that has not connected to Endpoint Manager for 24 hours. Use the slider to choose how many consecutive days of inactivity must pass before EM removes a device from the device list. Applies to devices that use any operating system.
  - The timer only counts inactive days from the moment you enable the option. Inactive days prior to this are not retroactively added to the count.
- **Remove duplicate devices -** A 'duplicate' is a device that has been enrolled more than once.
  - If you enable this option, EM will delete the duplicate which is currently inactive, or has been inactive for the longest period of time.
  - Use the slider to set the period after which duplicates are removed.
  - This setting applies to Windows devices only.

- Click 'Save'

### 11.2.6. Configure Two-Factor Authentication Settings

Click 'Settings' > 'Portal Set-up' then the 'Account Security' tab

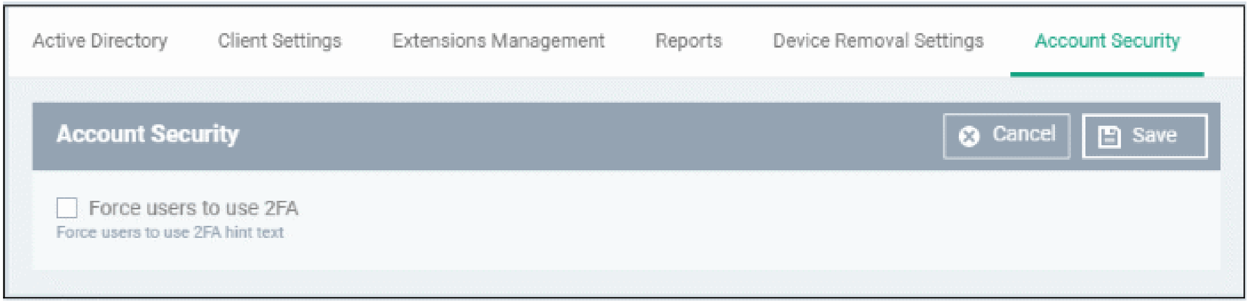


Account Security

Force users to use 2FA
Disabled

- Two-factor authentication adds additional security by requiring admins to present two forms of authentication before they can login to endpoint manager. They will need to enter their regular UN/PW + a unique code generated on their mobile device.
- This area lets you enable two-factor authentication (2FA) for admins that were created in Endpoint Manager itself ('Users' > 'User List' > 'Create User').
  - This area does not implement 2FA for C1 logins. If you created your admins in the C1 portal, then please enable 2FA in C1 instead ('Management' > 'Account' > 'Account Security Details').
  - You can create roles which allow users to login to Endpoint Manager if required. You can view and edit the privileges in each role at 'Users' > 'Role Management'. **Click here** if you want help with roles.

Click 'Edit' at top-right:



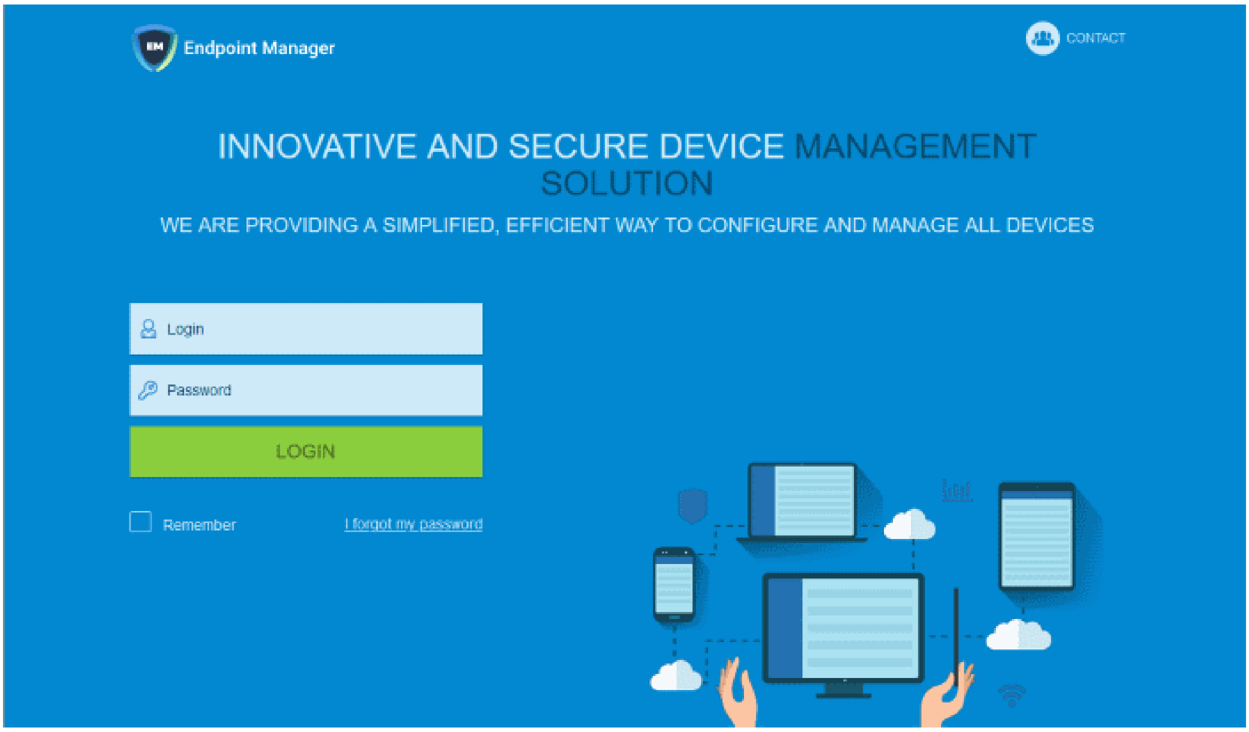
Account Security

☐ Force users to use 2FA
Force users to use 2FA hint text

- **Force user to use 2FA** - If enabled, admins will need to set-up 2FA on their next login to the EM console. Setup involves installing the Google Authenticator app on their device. This app generates the codes that form the 2nd layer of authentication.
- Click 'Save' to apply your changes

The following explains the admin user-experience to configure 2FA at first login:

- Admin enters his UN/PW in the EM login screen and clicks 'Login':



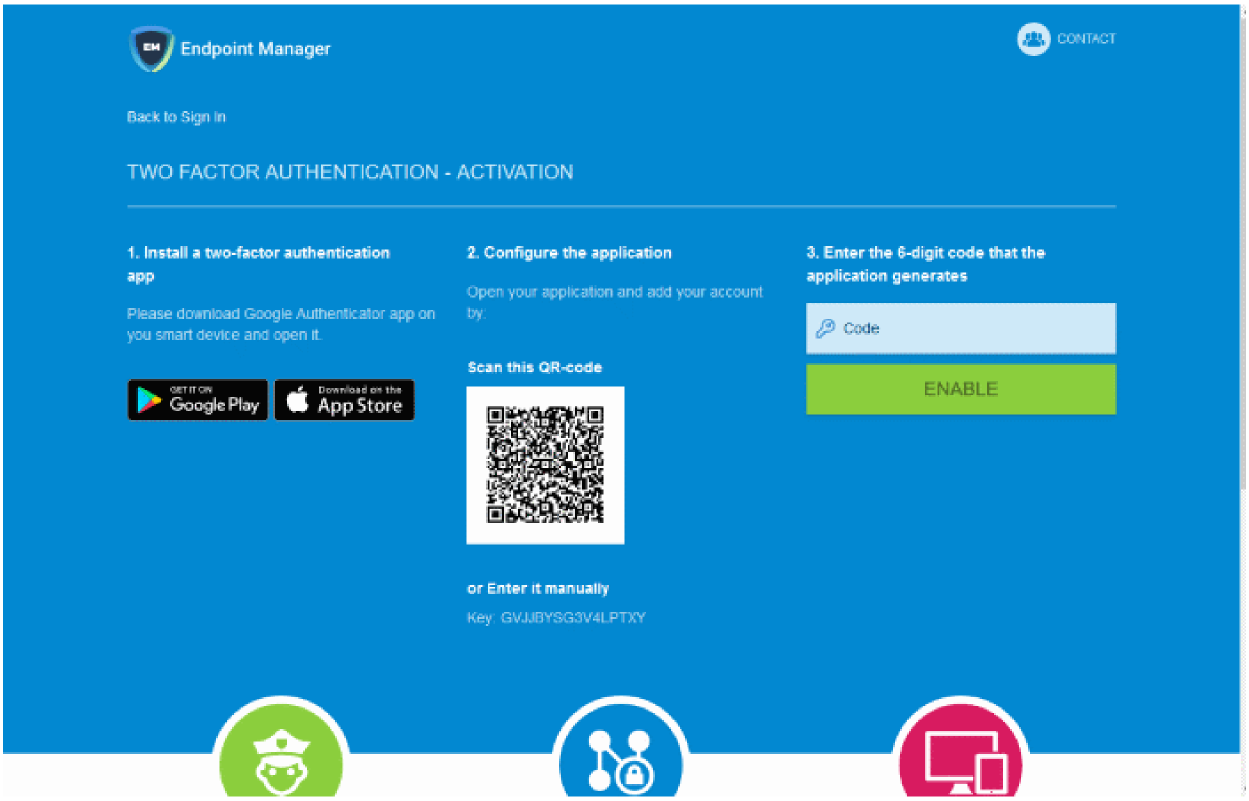
Endpoint Manager

CONTACT

INNOVATIVE AND SECURE DEVICE MANAGEMENT SOLUTION

WE ARE PROVIDING A SIMPLIFIED, EFFICIENT WAY TO CONFIGURE AND MANAGE ALL DEVICES

The two factor authentication activation screen is shown:



Endpoint Manager

CONTACT

Back to Sign In

TWO FACTOR AUTHENTICATION - ACTIVATION

1. Install a two-factor authentication app

Please download Google Authenticator app on you smart device and open it.

2. Configure the application

Open your application and add your account by:

Scan this QR-code

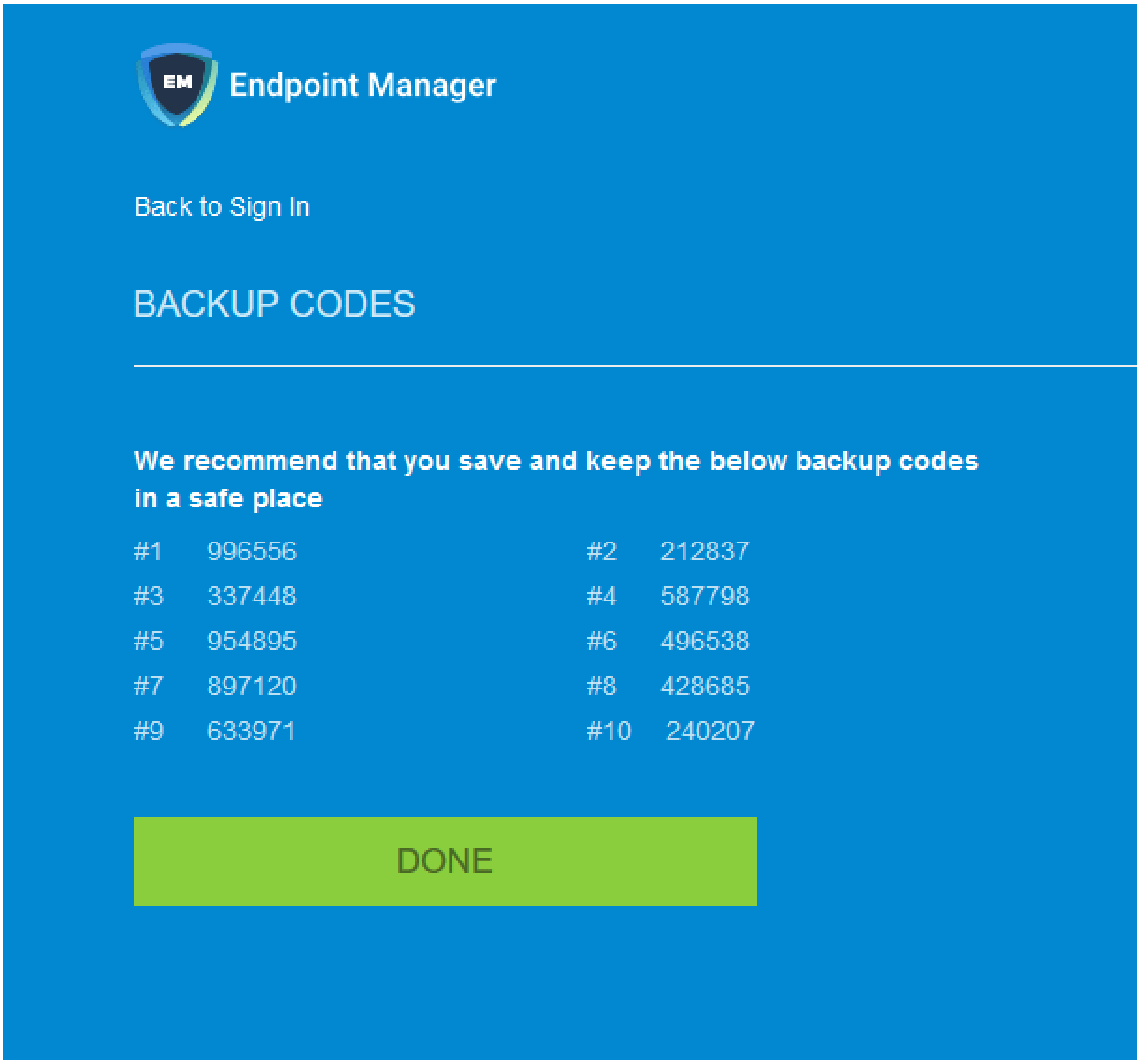
or Enter it manually

Key: GVJJBYSG3V4LPTXY

3. Enter the 6-digit code that the application generates

- **Step 1 -** Download the 'Google Authenticator' app and install it on your iOS or Android device
    - Open the 'Authenticator' app and tap the '+' icon
- **Step 2 -** Scan the QR code with the device camera. This will cause the Google app to generate the six digit code you need to complete pairing.
    - Alternatively, enter the key shown below the QR code in the Google Authenticator app.

- **Step 3 -** After completing steps 1 and 2, a six digit authentication code is generated in the Google app. This code changes frequently and is unique to your account.
    - Enter the verification code in the field provided
- Click 'Enable'
- A success message is shown along with 10 backup codes



BACKUP CODES

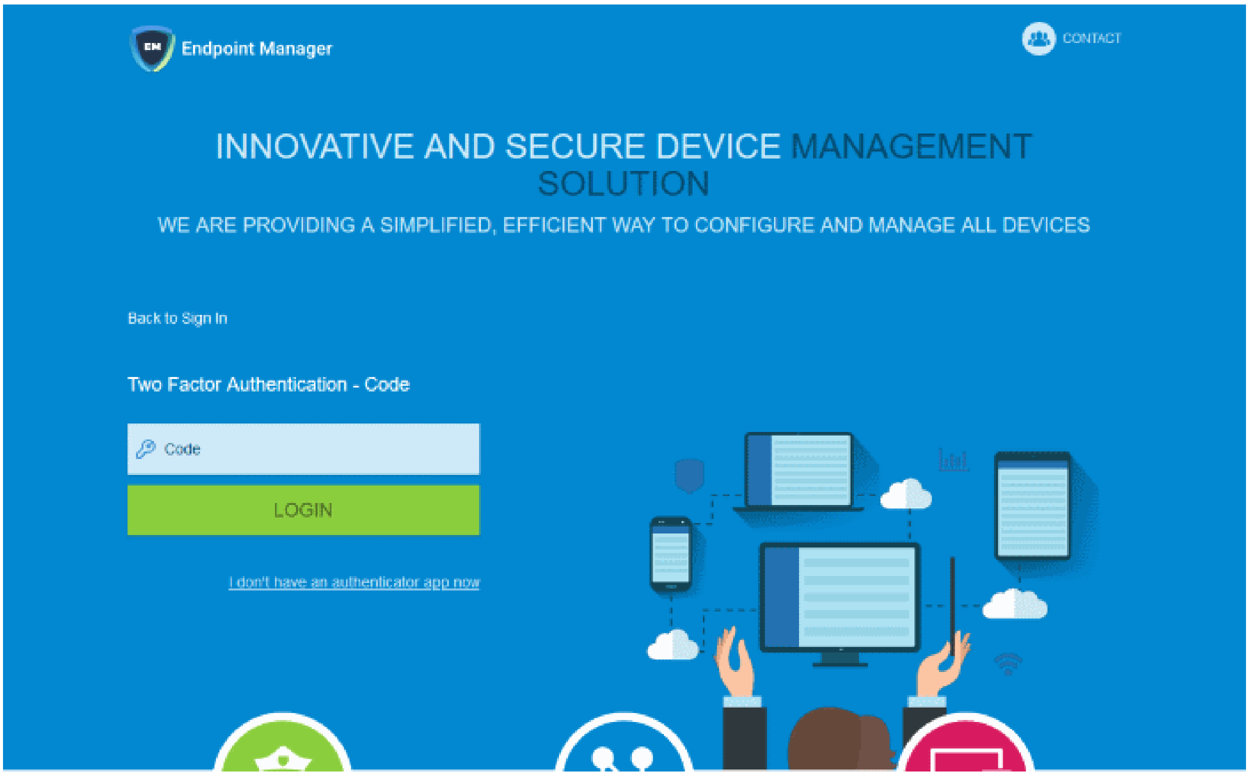
We recommend that you save and keep the below backup codes in a safe place

| | | | |
|---|---|---|---|
| #1 | 996556 | #2 | 212837 |
| #3 | 337448 | #4 | 587798 |
| #5 | 954895 | #6 | 496538 |
| #7 | 897120 | #8 | 428685 |
| #9 | 633971 | #10 | 240207 |

- You can use the backup codes to complete two-factor authentication if you do have the authentication device with you. Please make a copy of the codes. Each code can only be used once.
- Click 'Done'. You will be logged in to your account.

Two-factor authentication is now configured.

- During next login to EM console, the two-factor authentication screen is shown after entering your username and password

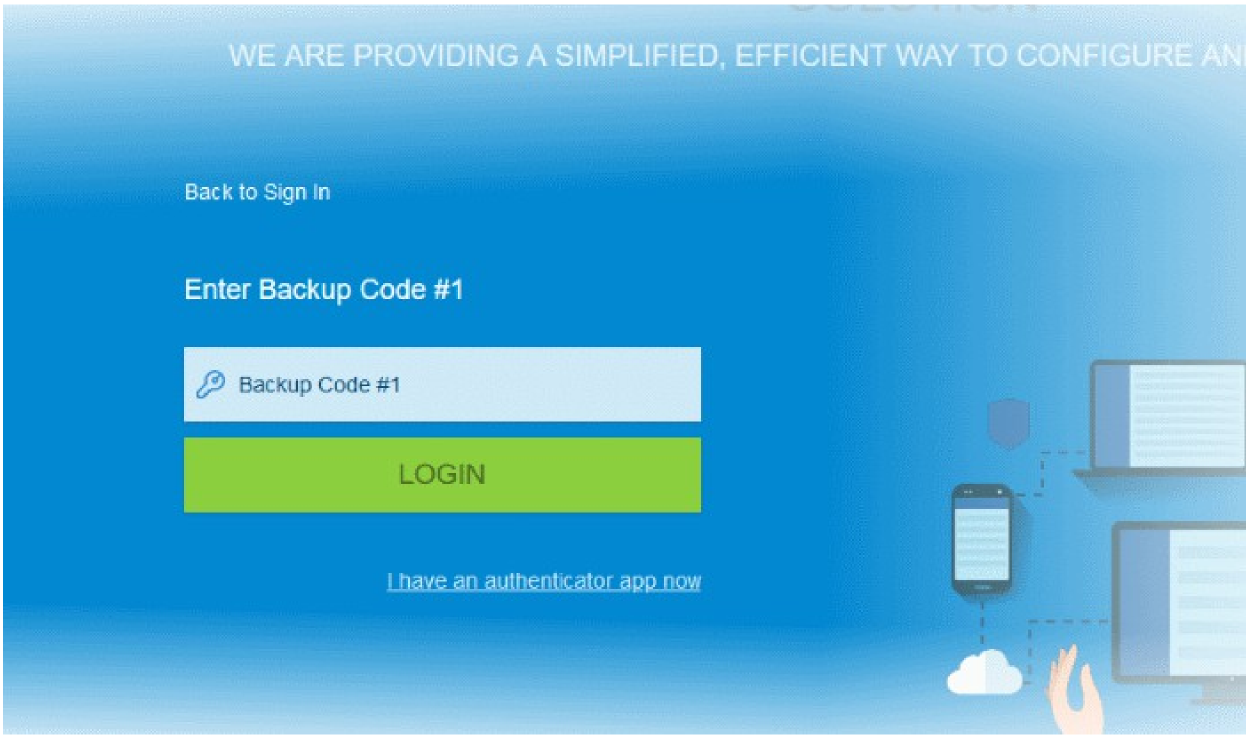

Endpoint Manager
CONTACT
INNOVATIVE AND SECURE DEVICE MANAGEMENT SOLUTION
WE ARE PROVIDING A SIMPLIFIED, EFFICIENT WAY TO CONFIGURE AND MANAGE ALL DEVICES
Back to Sign In
Two Factor Authentication - Code
Code
LOGIN
I don't have an authenticator app now

- **Code** - Open the Google Authenticator app on your paired device and enter the displayed code. Please note the code changes frequently.
- Click 'Login'

### Use Backup Codes

Endpoint Manager two-factor authentication allows you to use your backup codes in case you do not have your paired device with you during a login attempt.

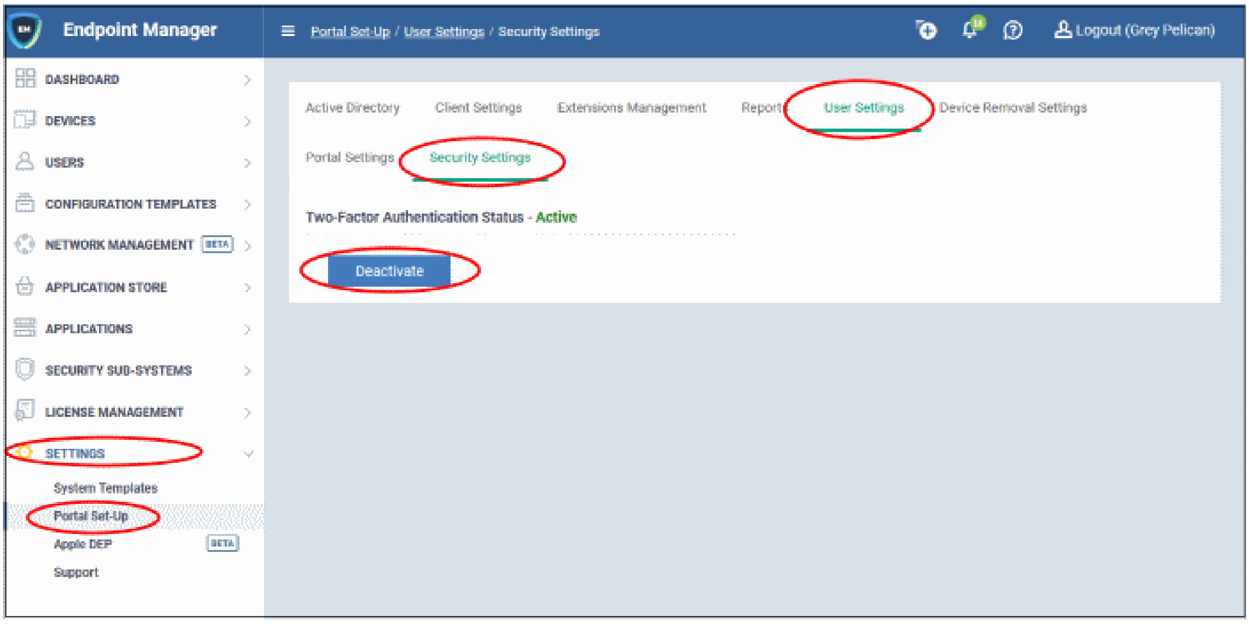
- Click 'I don't have an authenticator app now' link


WE ARE PROVIDING A SIMPLIFIED, EFFICIENT WAY TO CONFIGURE AN
Back to Sign In
Enter Backup Code #1
Backup Code #1
LOGIN
I have an authenticator app now

- Enter backup code 1 from the saved backup codes when you paired your device
- Click 'Login'

**Disable Two-Factor Authentication**

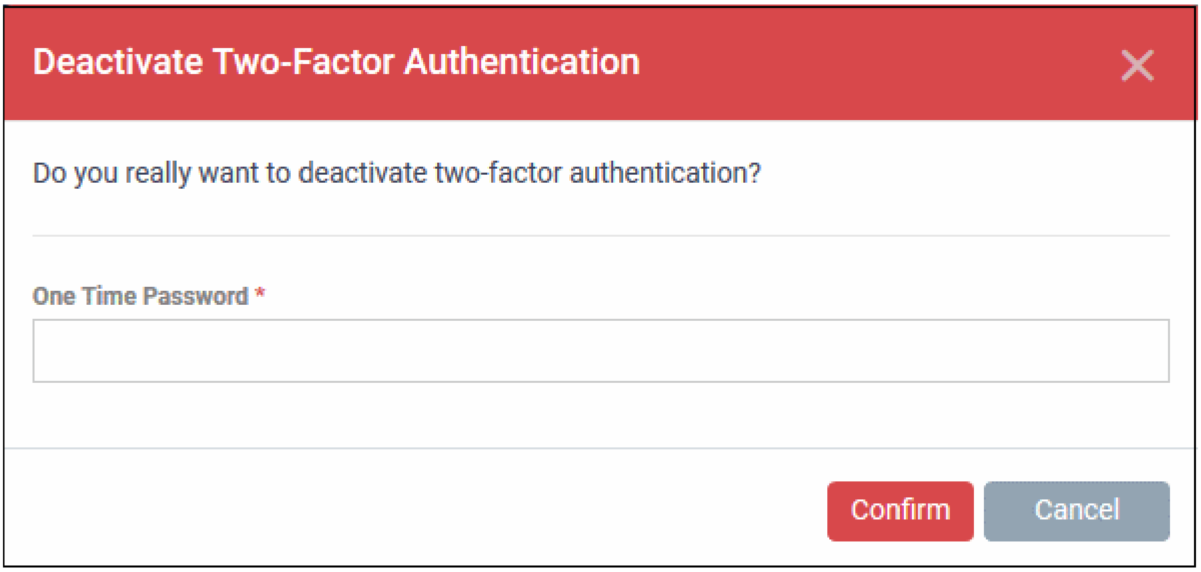
- Individual admins cannot disable two-factor authentication on their own account as long as it is enabled by the account manager in EM
- If 2FA is disabled by the account manager in EM, then you can deactivate it after logging in to your EM account.
- Login to your account by providing credentials and 2FA code.
- Click 'Settings' > 'Portal Set-Up' then 'User Settings' tab
- Click 'Security Settings'



Two-Factor Authentication Status - Active

- Click 'Deactivate'

A confirmation dialog is shown:



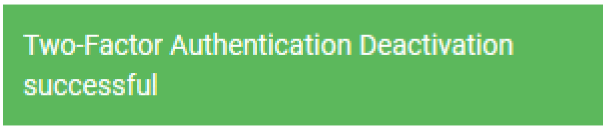
Deactivate Two-Factor Authentication

Do you really want to deactivate two-factor authentication?

One Time Password *

- **One Time Password -** Enter the code from your paired device
- Click 'Confirm'

A success message is shown:

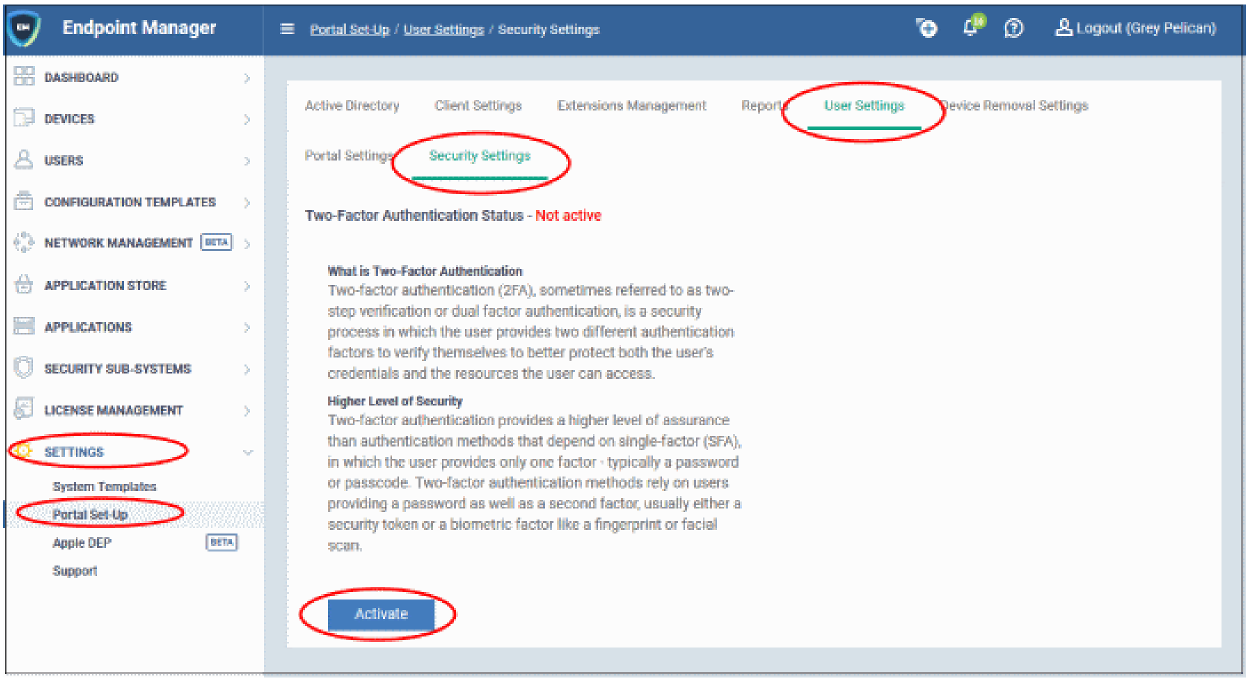


Two-Factor Authentication Deactivation successful

### Two Factor Authentication Activation by Admins

If 2FA is not enabled by your account manager in EM, you can enable it for yourself as follows:

- Login to your EM account
- Click 'Settings' > 'Portal Set-Up' then the 'User Settings' tab
- Click 'Security Settings'



Two-Factor Authentication Status - Not active

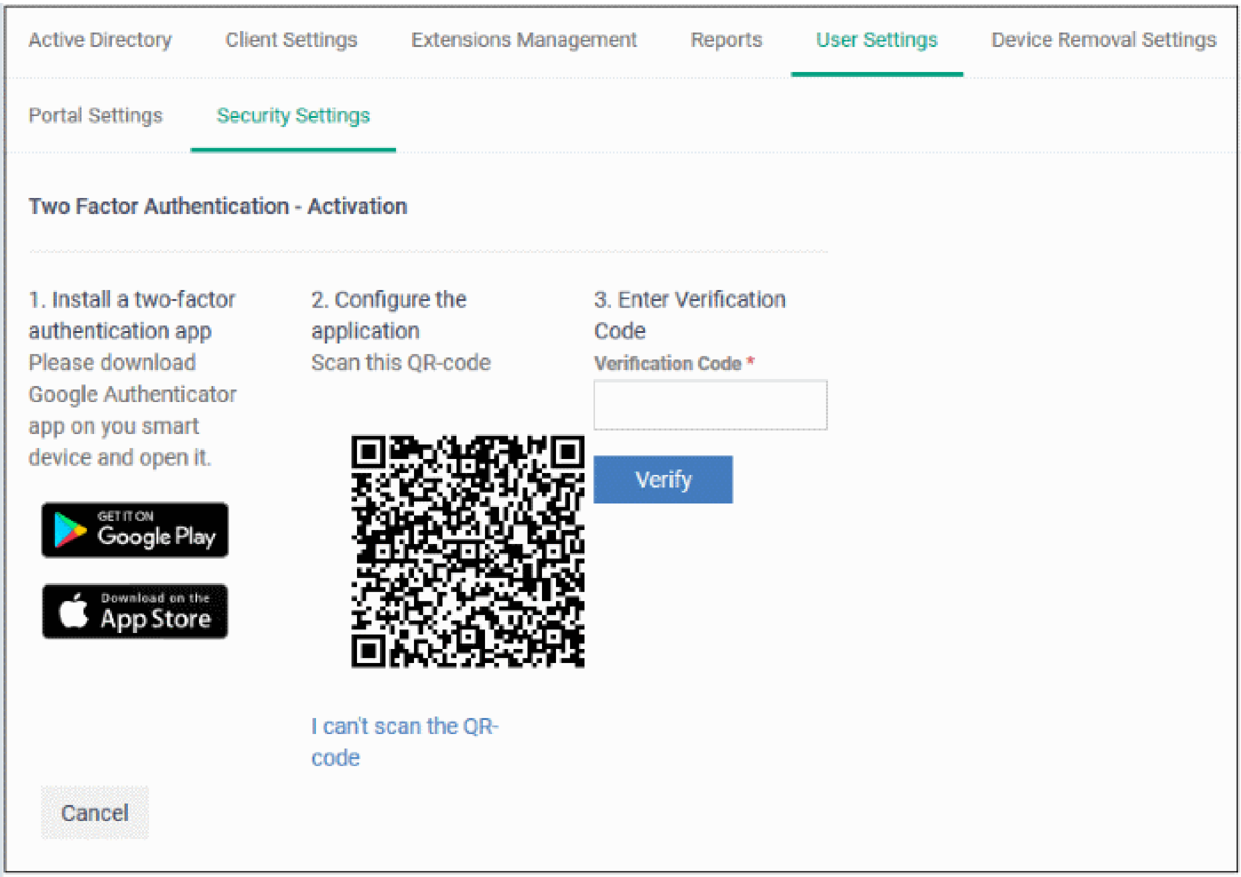
**What is Two-Factor Authentication**

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

**Higher Level of Security**

Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor (SFA), in which the user provides only one factor - typically a password or passcode. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan.

- Click 'Activate'



Two Factor Authentication - Activation

1. Install a two-factor authentication app
Please download Google Authenticator app on you smart device and open it.

2. Configure the application
Scan this QR-code

3. Enter Verification Code
Verification Code *

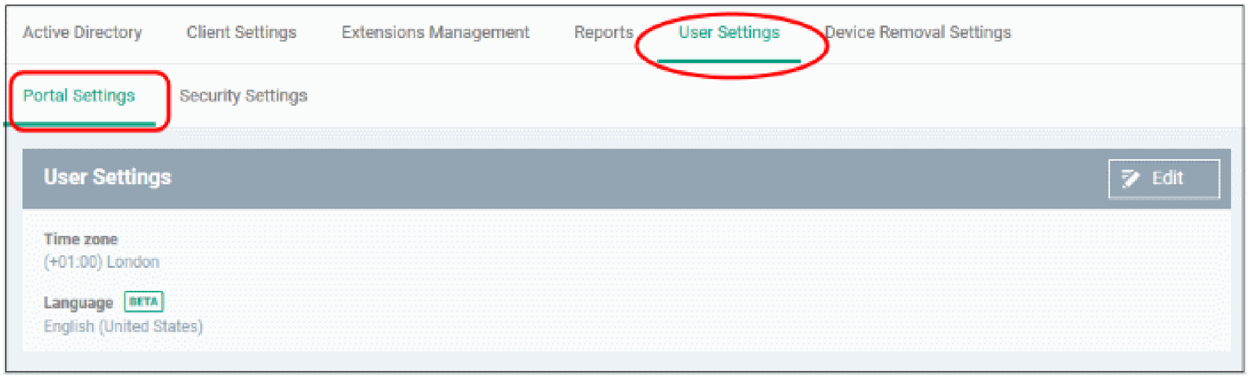
- The device pairing procedure is similar as explained in the section above.

## 11.2.7. Set-up Administrator's Time Zone and Language

**Note:**

- Admins added through Comodo Dragon or Comodo One must set their time zone in the CD / C1 console.
- Only admins added directly to Endpoint Manager can set their time and language in the EM console.
- The 'User Settings' tab is only available if you login to EM through your dedicated URL. It is not available if you login through CD / C1.

- Click 'Settings' > 'Portal Set-Up'
- Click the 'User Settings' tab then 'Portal Settings'

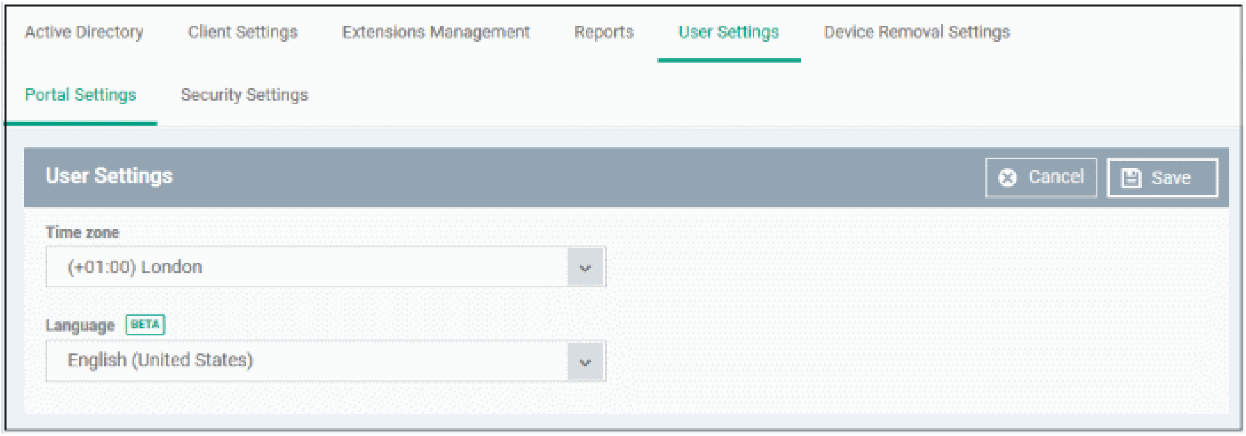


User Settings

Time zone
(+01:00) London

Language BETA
English (United States)

- Click 'Edit' at the top-right



User Settings

Time zone
(+01:00) London

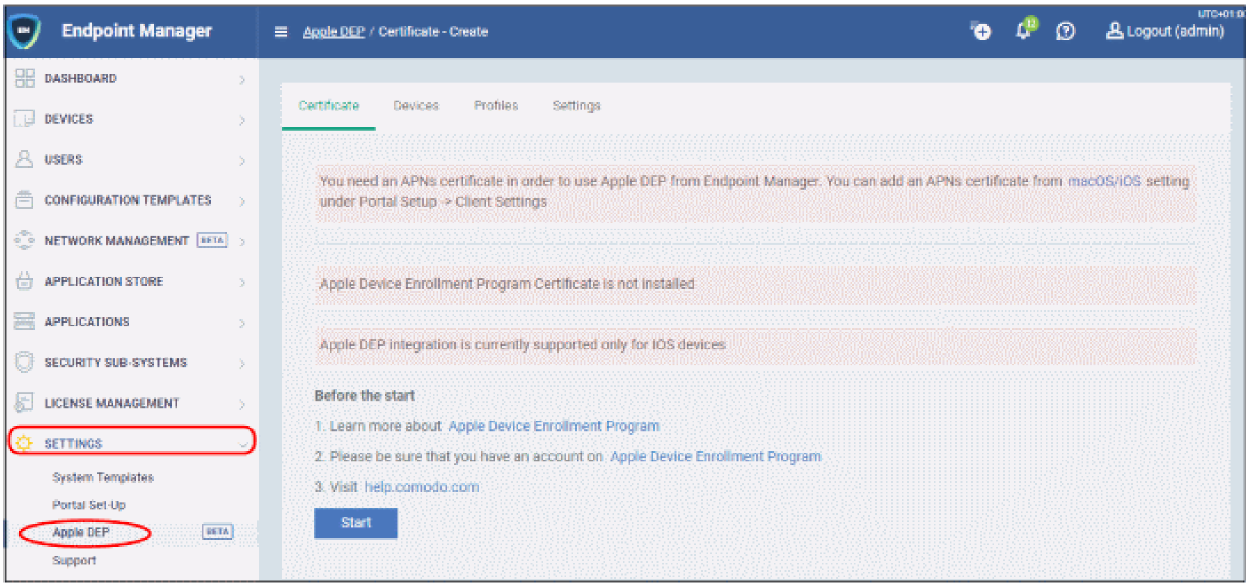
Language BETA
English (United States)

- Choose your time zone and interface language from the drop-down menus
- Click 'Save'.

Your time zone and language selection will be updated. All logs and interface time indicators will use the set time zone.

## 11.3. Integrate Apple DEP with Endpoint Manager

- Click 'Settings' > 'Apple DEP'



You need an APNs certificate in order to use Apple DEP from Endpoint Manager. You can add an APNs certificate from macOS/iOS setting under Portal Setup -> Client Settings

Apple Device Enrollment Program Certificate is not installed

Apple DEP integration is currently supported only for IOS devices

Before the start

1. Learn more about Apple Device Enrollment Program

2. Please be sure that you have an account on Apple Device Enrollment Program

3. Visit help.comodo.com

Apple's Device Enrollment Program (DEP) simplifies the activation and management of iOS and Mac devices in an enterprise network. While you will continue to use Endpoint Manager for day-to-day device management, DEP makes the initial setup process far easier for both admins and users.

After integrating EM with DEP:

- Admins no longer have to manually configure each device, nor individually enroll each device with EM. All devices you register with DEP will automatically become managed by Endpoint Manager as soon as they are turned on.
- All setup tasks, including EM enrollment, are carried out over-the-air (OTA) at device start-up. You can even choose to skip the various setup wizards that usually appear when a device is first turned on.
- Devices can never become unmanaged without your consent, even if the device is factory reset. Admins have to remove them from Endpoint Manager to unmanage them.
- Endpoint Manager (EM) currently supports iOS devices only.

See **https://www.apple.com/business/docs/site/DEP_Guide.pdf** for more information about Apple DEP

**Process in brief**

- Add Apple devices to your DEP account
- Create a virtual MDM server in your DEP account and link it to Endpoint Manager (EM)
  - Once linked, devices in your DEP account are synced with EM
  - Click 'Settings' > 'Apple DEP' > 'Devices' to view them
- Create a DEP profile and assign it to your devices. The DEP profile lets you enable supervisor mode and skip setup wizards
- User activates the device
- Once activated, EM profiles are applied to the device and it is enrolled into EM
  - You can view the devices at 'Devices' > 'Device List'
- If you remove a device from your DEP account, it remains enrolled in Endpoint Manager.
- If you remove a device from EM, it remains enrolled in DEP. You will have to reapply the DEP profile or manually enroll it again to return it to EM.

Click the following links for help to integrate Endpoint Manager with DEP:

- **Link Endpoint Manager with Apple DEP**
- **Manage Apple DEP Devices**

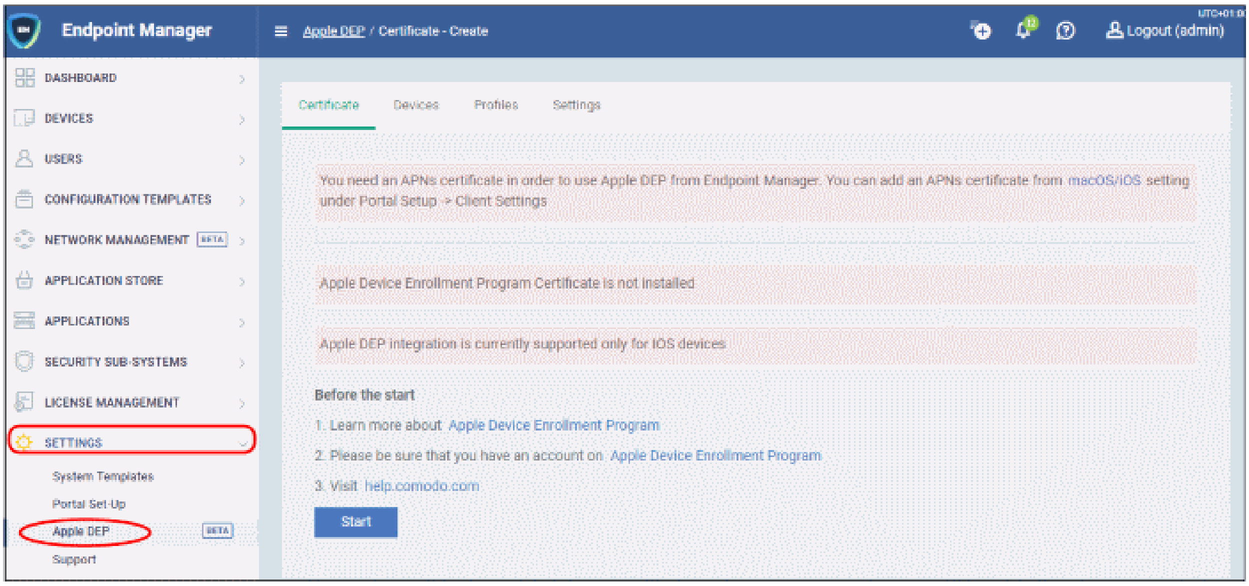
- **Manage Apple DEP Profiles**
- **Configure Apple DEP Notification Settings**

### 11.3.1. Link Endpoint Manager with Apple DEP

- You first need to complete the following steps with Apple:
  - Enroll in the Apple Device Enrollment Program (DEP) program if you haven't done so already.
  - Link Endpoint Manager (EM) to your DEP account. EM is the 'MDM solution' referred to in Apple's docs (see link below).
  - Assign devices to your DEP account.
- Please follow the steps in **Apple's help documentation** to complete the processes above.
- Completing these steps will establish a virtual Endpoint Manager server in DEP. The virtual server is synchronized with your physical EM account.

Next, you need configure settings in Endpoint Manager to complete the link to DEP.

- Click 'Settings' > 'Apple DEP'
- Click the 'Certificate' tab:



You need an APNs certificate in order to use Apple DEP from Endpoint Manager. You can add an APNs certificate from macOS/iOS setting under Portal Setup -> Client Settings

Apple Device Enrollment Program Certificate is not installed

Apple DEP integration is currently supported only for IOS devices

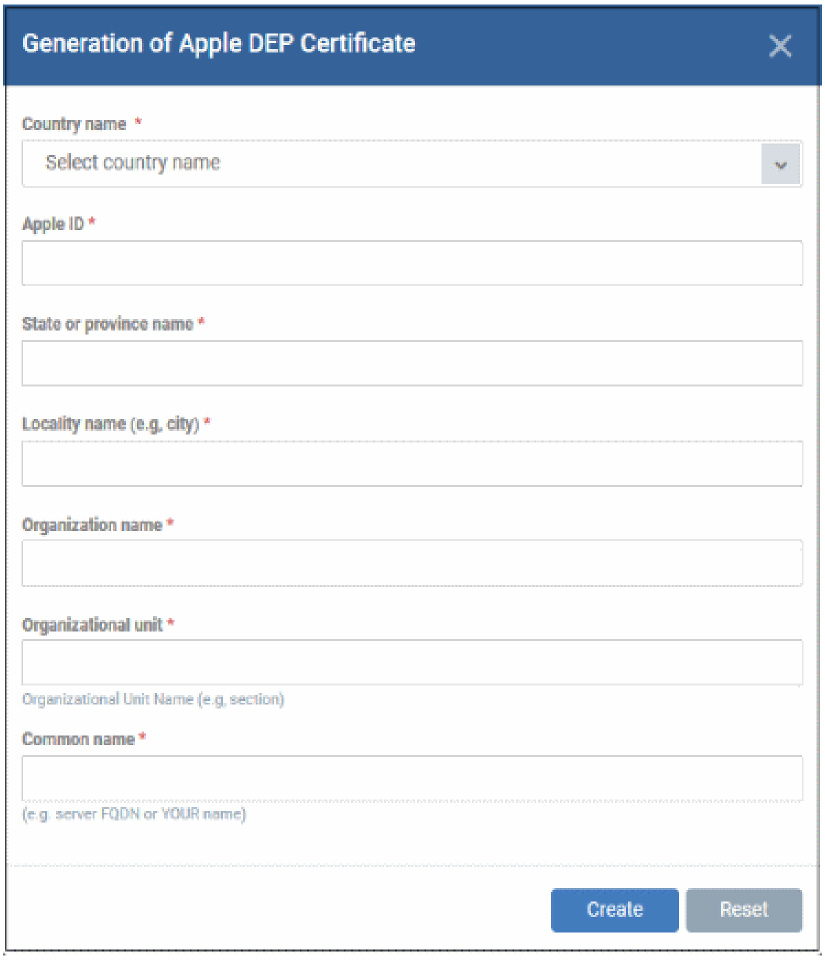
Before the start

1. Learn more about Apple Device Enrollment Program
2. Please be sure that you have an account on Apple Device Enrollment Program
3. Visit help.comodo.com

- First, you need to install an Apple Push Notification (APN) certificate on your EM portal. This certificate allows Endpoint Manager to communicate with iOS and Mac devices.
- You may already have done this if you are currently using EM to manage iOS devices. If not, then:
  - Click 'Settings' > 'Portal Set-up' > 'Client Settings' > 'mac OS/iOS' > 'Create APN certificate'
  - Complete the certificate application form then click 'Create'.
  - See '**Add Apple Push Notification Certificate**' if you need help with this.

- After installing the APN cert, you need to install a DEP certificate. This certificate allows Endpoint Manager to communicate with Apple's DEP servers.
- Click 'Settings' > 'Portal Set-up' > 'Apple DEP'

- Click the 'Start' button



Generation of Apple DEP Certificate

Country name *

Select country name

Apple ID *

State or province name *

Locality name (e.g, city) *

Organization name *

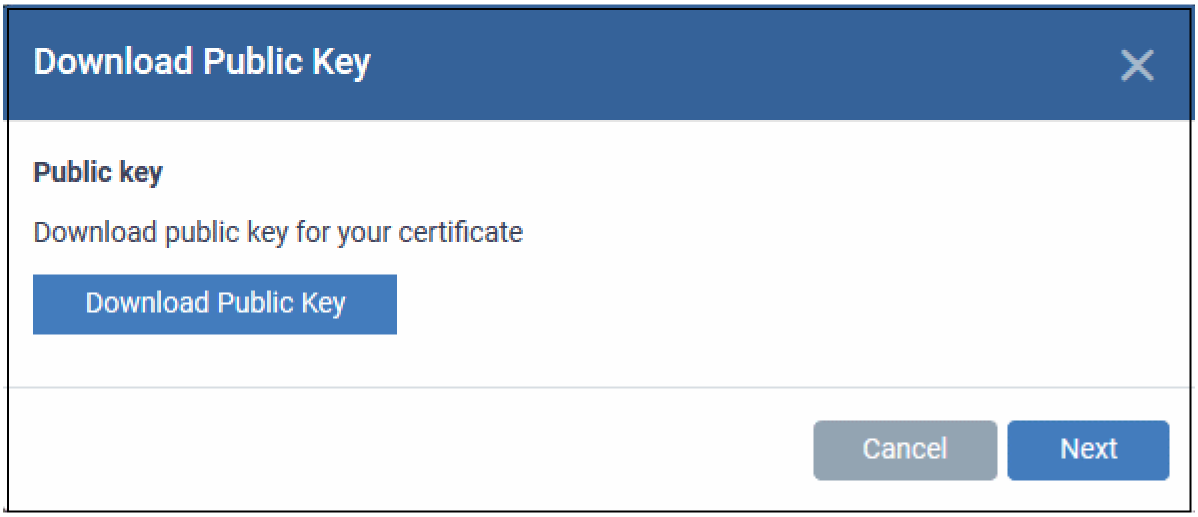
Organizational unit *

Organizational Unit Name (e.g, section)

Common name *

(e.g. server FQDN or YOUR name)

- Complete all fields on the certificate request form. Enter your Apple ID and your company details.
- Click 'Create' to submit the form, then 'Download Public Key':



Download Public Key

Public key

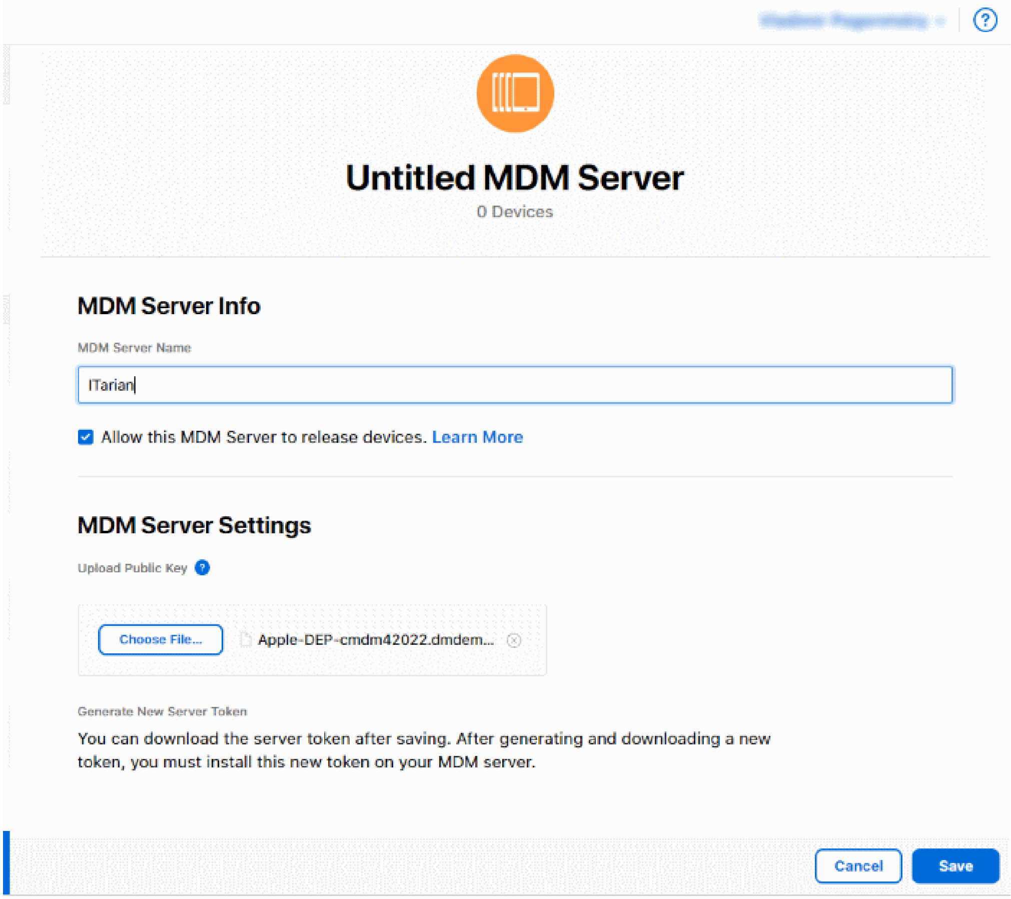
Download public key for your certificate

- Save the key in a safe place as you will need to upload it to the DEP server later.
- Click 'Next' after you have saved the key.

Next, you need to create a virtual EM server on Apple's DEP server:

- Click 'Go to DEP Portal' and login to your DEP account

- Open the 'Device Management Settings' page then click 'Add MDM Server'
- Create a name for your virtual server in the 'MDM Server Info' field. This can be anything you choose.
- Make sure 'Allow this MDM server to release devices' is enabled
- Click 'Choose File...' to upload the public key you saved.
- Click 'Save':



[redacted]

## Untitled MDM Server

0 Devices

### MDM Server Info

MDM Server Name

ITarian

☑ Allow this MDM Server to release devices. Learn More

### MDM Server Settings

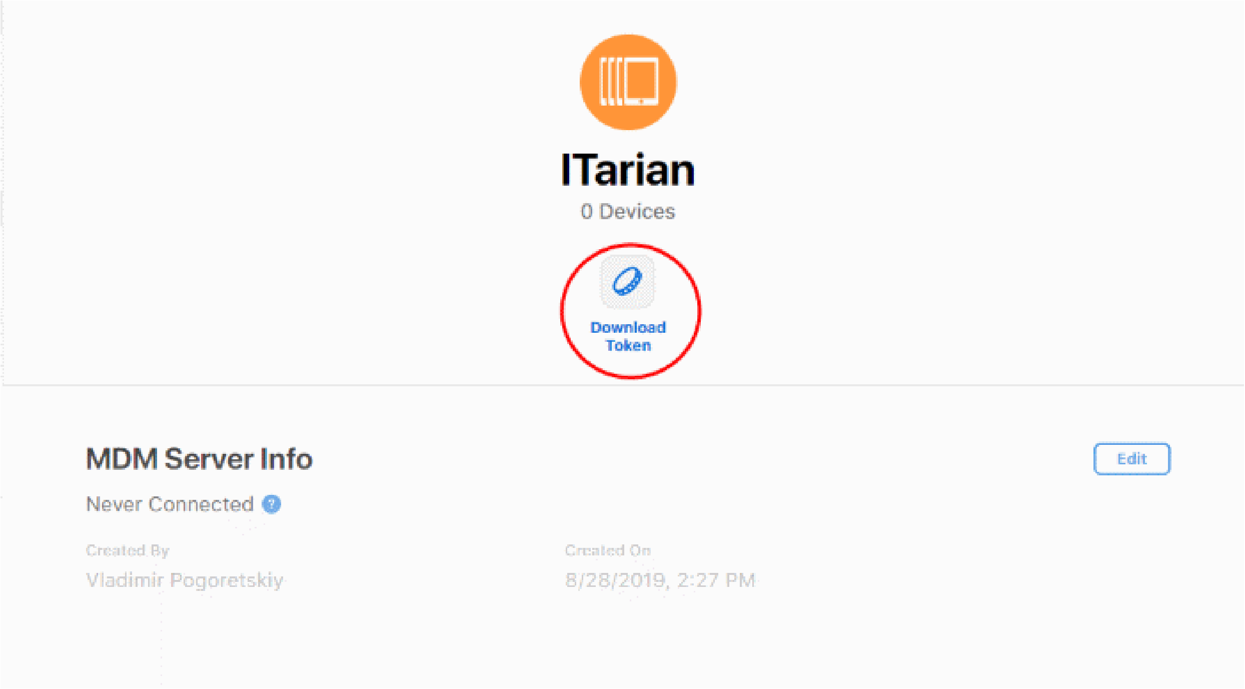
Upload Public Key

Choose File... Apple-DEP-cmdm42022.dmdem...

Generate New Server Token

You can download the server token after saving. After generating and downloading a new token, you must install this new token on your MDM server.

- After authenticating your request, DEP will generate a token which you need to upload to Endpoint Manager:



ITarian

0 Devices

MDM Server Info

Never Connected

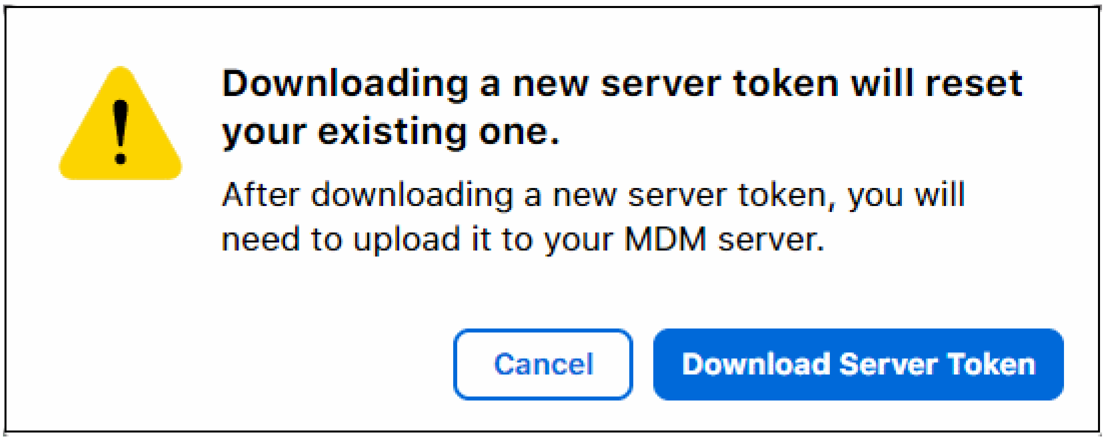
Created By

Vladimir Pogoretskiy

Created On

8/28/2019, 2:27 PM

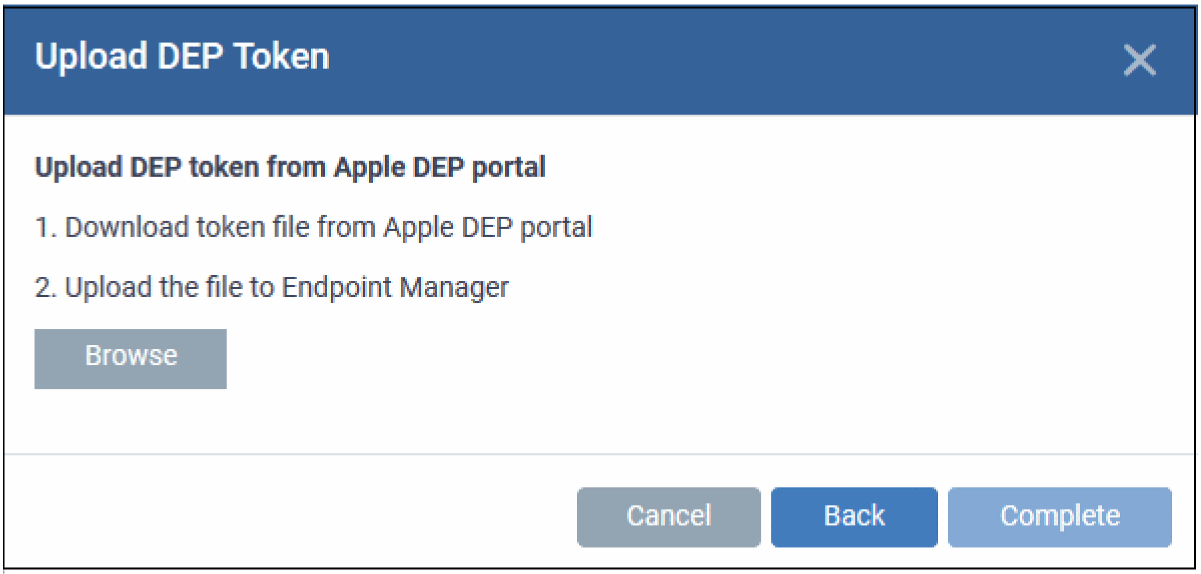
- Click 'Download Token'



Downloading a new server token will reset your existing one.

After downloading a new server token, you will need to upload it to your MDM server.

- Click 'Download Server Token' and save it.
- Go back to Endpoint Manager and upload the token
  - Click 'Settings' > 'Apple DEP' > 'Certificate'
  - Click 'Browse', locate your token then click 'Open':



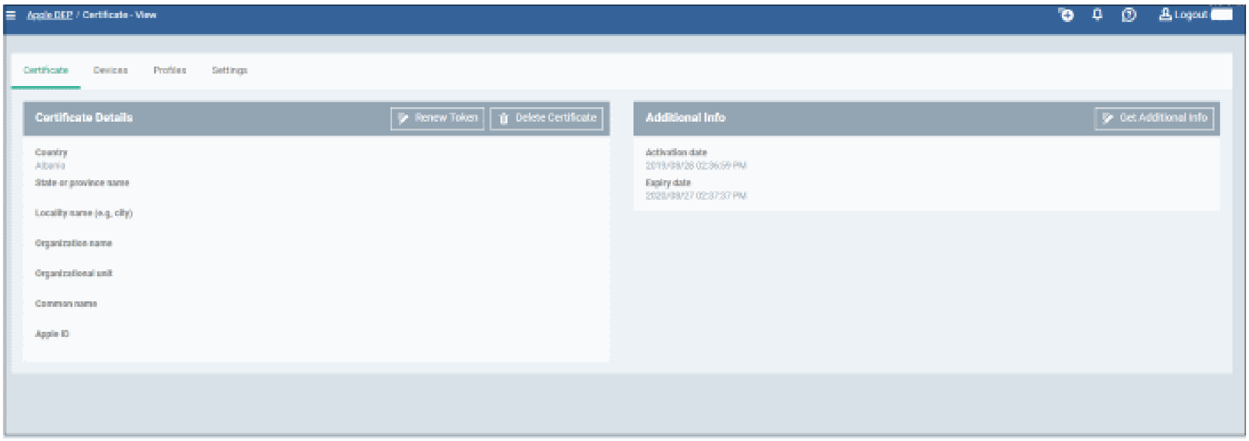
Upload DEP Token

**Upload DEP token from Apple DEP portal**

1. Download token file from Apple DEP portal
2. Upload the file to Endpoint Manager

- Click 'Complete'

The 'Certificates' tab will now show your DEP certificate details:



**Certificate Details**

Country
Albania
State or province name
Locality name (e.g, city)
Organization name
Organizational unit
Common name
Apple ID

**Additional Info**

Activation date
2019/09/28 02:36:59 PM
Expiry date
2020/09/27 02:37:37 PM

- Your Endpoint Manager and Apple DEP accounts are now synced. You can now add devices and configure your DEP profile.

## 11.3.2. Manage Apple DEP Devices

- Click 'Settings' > 'Apple DEP' then the 'Devices' tab
- DEP registered devices are automatically synced with EM after you have **linked your account**
- After enrollment, the devices will appear in two places:

  i. **Settings > Apple DEP > Devices -** Device identified by serial number.

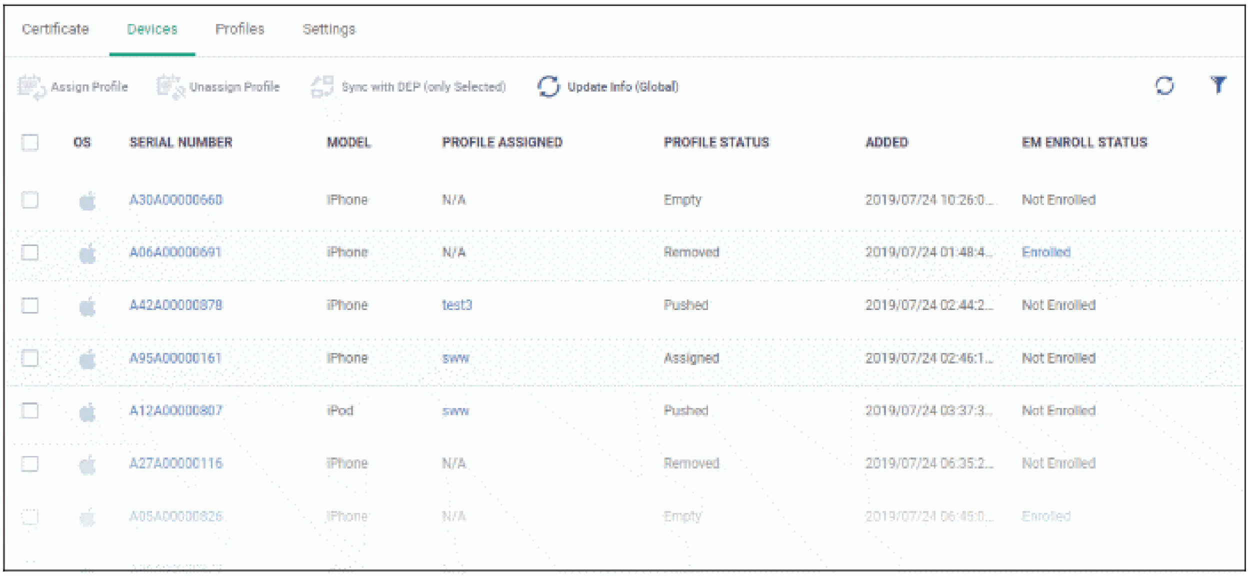
  ii. **Devices > Devices List -** Device identified by name. Open device details to view the serial number.
- DEP enrolled devices will have two profiles:

  i. **DEP Profile -** Created during enrollment to the DEP program. You can create and assign new DEP profiles in the 'Profiles' tab. See **Manage Apple DEP Profile**

  ii. **Endpoint Manager Profile -** The default OS profile is applied by default. You can change this as required.

The DEP 'devices' area allows you to:

- Assign DEP profiles to devices
- Remove profiles
- Update device information from DEP
- Update DEP information



| ☐ | OS | SERIAL NUMBER | MODEL | PROFILE ASSIGNED | PROFILE STATUS | ADDED | EM ENROLL STATUS |
|---|---|---|---|---|---|---|---|
| ☐ |  | A30A00000660 | iPhone | N/A | Empty | 2019/07/24 10:26:0... | Not Enrolled |
| ☐ |  | A06A00000691 | iPhone | N/A | Removed | 2019/07/24 01:48:4... | Enrolled |
| ☐ |  | A42A00000878 | iPhone | test3 | Pushed | 2019/07/24 02:44:2... | Not Enrolled |
| ☐ |  | A95A00000161 | iPhone | sww | Assigned | 2019/07/24 02:46:1... | Not Enrolled |
| ☐ |  | A12A00000807 | iPod | sww | Pushed | 2019/07/24 03:37:3... | Not Enrolled |
| ☐ |  | A27A00000116 | iPhone | N/A | Removed | 2019/07/24 06:35:2... | Not Enrolled |
| ☐ |  | A05A00000826 | iPhone | N/A | Empty | 2019/07/24 06:45:0... | Enrolled |

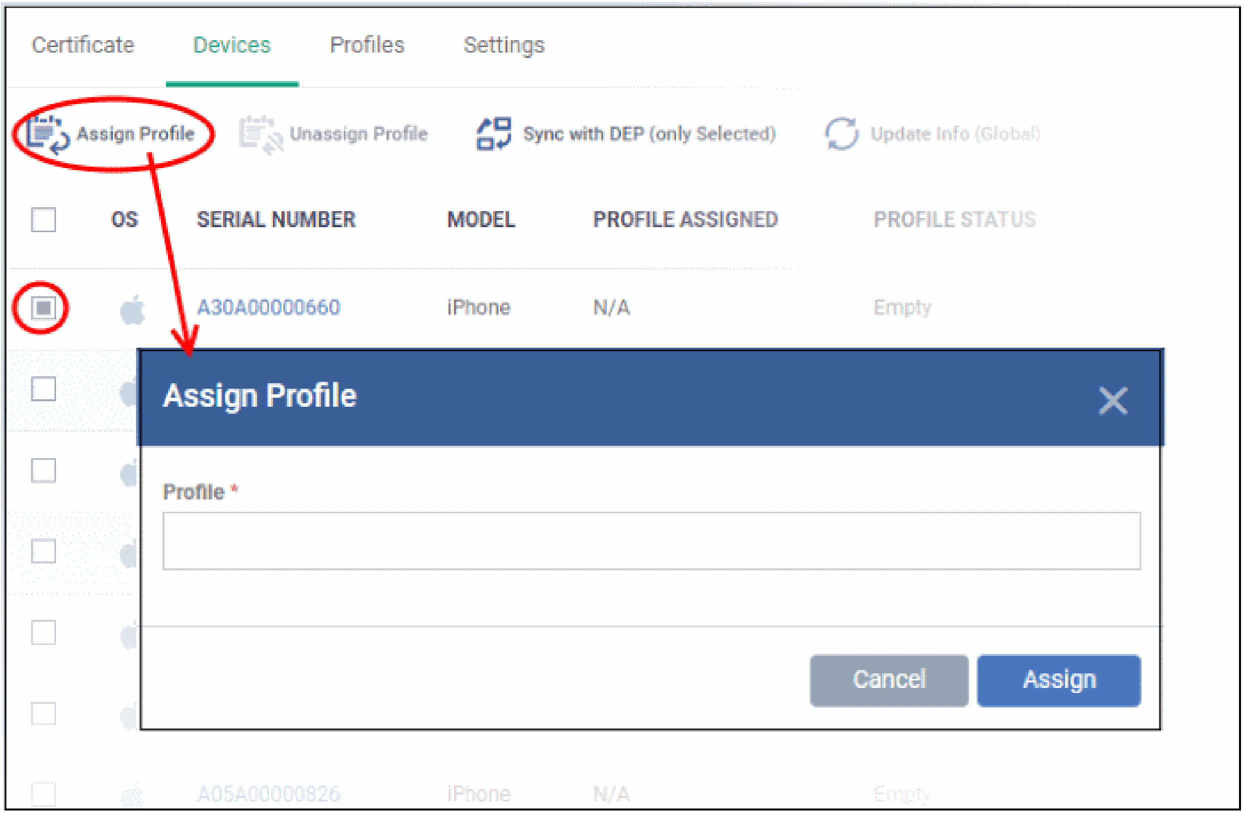
| Column Heading | Description |
|---|---|
| OS | Operating system of the registered device. Currently only iOS is supported. |
| Serial Number | Apple assigned device identification number |
| Model | Type of Apple device |
| Profile Assigned | The DEP profile delegated to the device. See 'Profile Status' below for more info: |
| Profile Status | • **Empty -** No profile is assigned to the device<br>• **Assigned -** Profile is ready for deployment, but the user has not yet activated the device.<br>• **Pushed -** User has activated the device and the DEP profile is installed<br>• **Removed -** DEP profile was installed then deleted from the device |
| Added | Date and time the device was registered in DEP |
| EM Enroll Status | 'EM enrolled' means that the endpoint manager profile has been installed on the device. This means you can manage the device via the Endpoint Manager console.<br>• User has completed the device setup process and installed the DEP profile.<br>• The EM iOS profile is installed right afterwards to bring the device under MDM control<br>• You can view enrolled devices at 'Devices' > 'Device List'<br>Not Enrolled - User has not started the device setup process. |
| **Control buttons:** | |
| Assign Profile | Delegate a DEP profile to the device. The profile will be installed when the device is |

| | |
|---|---|
| | activated. See **Assign Profiles to Device** |
| Unassign Profile | Removes the selected profile from a device. See **Remove Profiles** |
| Sync with DEP (only selected) | Update profile information for the device from DEP. See **Update Device Information from DEP** |
| Update info (Global) | Checks DEP server the status of all devices. See **Update DEP Information** |

- Click the funnel icon to filter devices by various criteria
- Click a column header to sort by ascending / descending order

## Assign DEP Profiles to Devices

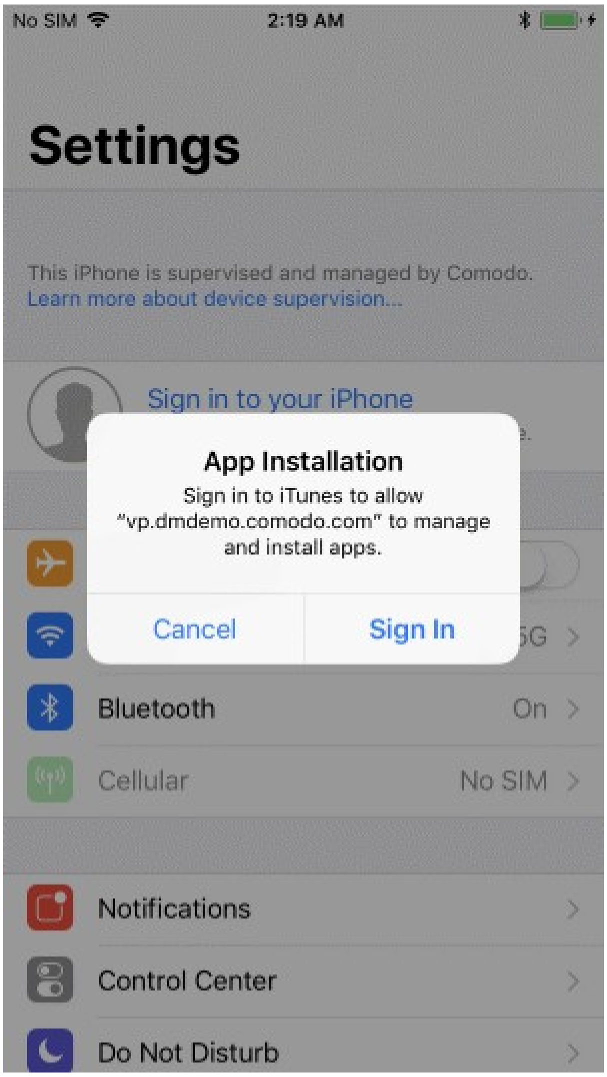
- Select target devices then click 'Assign Profile':



- Start typing the name of a profile and select from the suggestions
- Click 'Assign'
- The following confirmation is shown:

Device(s) assigned successfully

Users are asked to install the profile when the device is activated:



No SIM 2:19 AM

Settings

This iPhone is supervised and managed by Comodo.
Learn more about device supervision...

Sign in to your iPhone

App Installation

Sign in to iTunes to allow "vp.dmdemo.comodo.com" to manage and install apps.

Cancel | Sign In

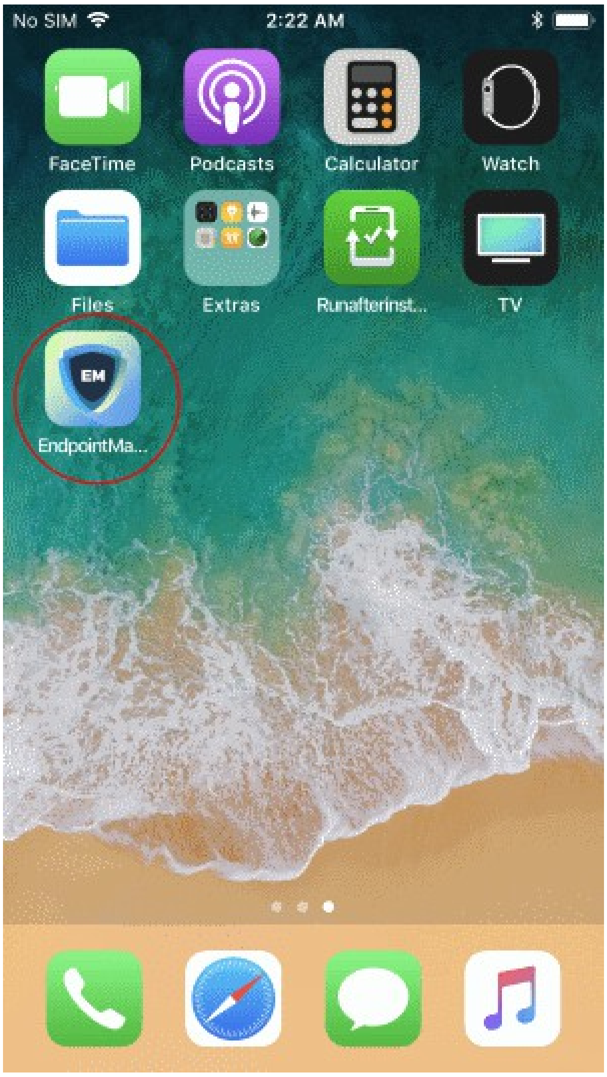
Bluetooth On

Cellular No SIM

Notifications

Control Center

Do Not Disturb

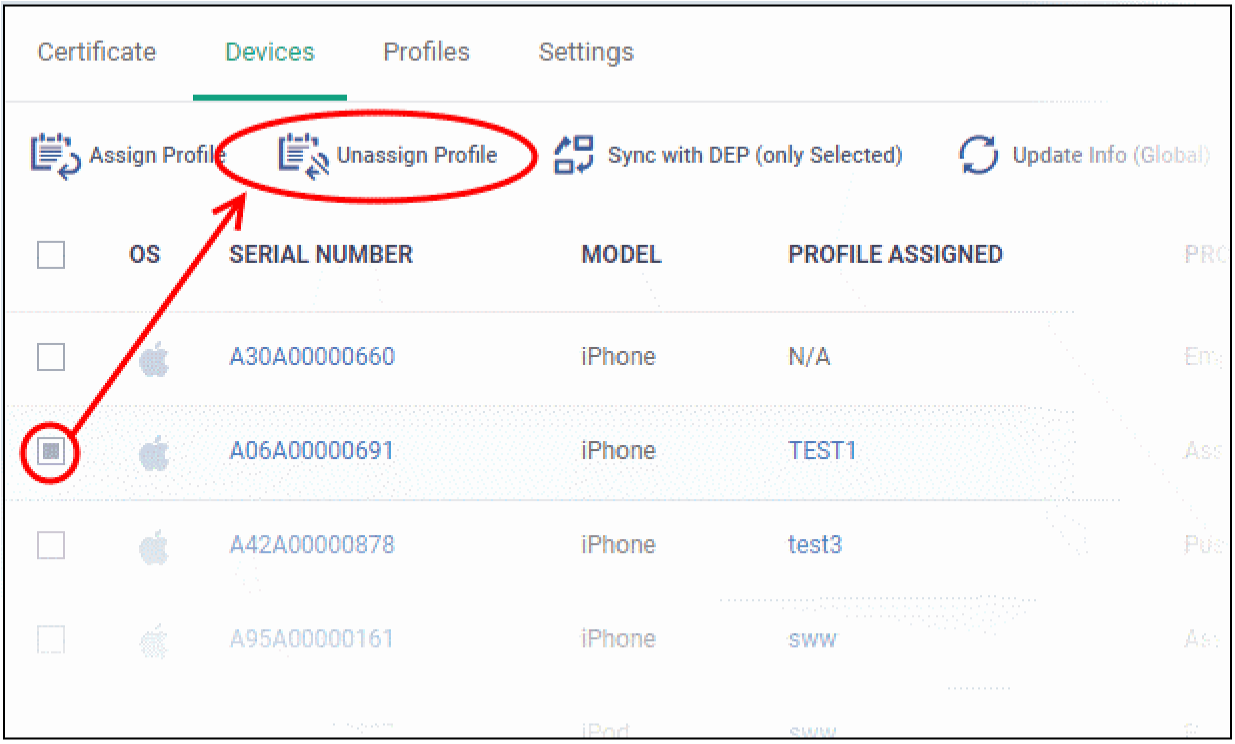


Endpoint Manager profiles are applied as follows:

- Custom device profiles are assigned if they exist.
  - See **Assign Configuration Profiles to User Devices**, and **Assign Configuration Profiles to a User Group**
- The 'default' profiles are applied if no custom profiles exist.
  - See **Manage Default Profiles** if you want help with default EM profiles.

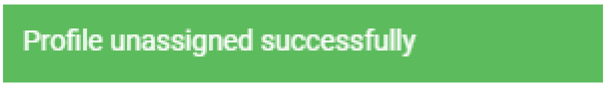
## Remove DEP Profiles

- Select target devices then click 'Unassign Profile':



| | OS | SERIAL NUMBER | MODEL | PROFILE ASSIGNED | PRO |
|---|---|---|---|---|---|
| □ | | A30A00000660 | iPhone | N/A | Em |
| ☒ | | A06A00000691 | iPhone | TEST1 | Ass |
| □ | | A42A00000878 | iPhone | test3 | Pus |
| □ | | A95A00000161 | iPhone | sww | As |
| | | | iPod | sww | |

The following confirmation is shown:



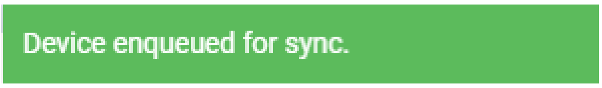
Profile unassigned successfully

- Note - The device stays enrolled to Endpoint Manager, and all EM profiles remain in place.

## Update Device Information from DEP

Endpoint Manager periodically contacts the DEP server to update the status of device profiles. You can manually run this update as follows:

- Select the target devices then click 'Sync with DEP (only Selected)'



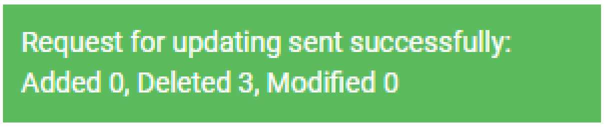
Device enqueued for sync.

- The device profile status is refreshed.

## Update DEP Information

Device information from DEP is updated periodically. You can update in real-time if required.

- Click 'Update Info (Global) at the top



Request for updating sent successfully:
Added 0, Deleted 3, Modified 0

## 11.3.3. Manage Apple DEP Profiles

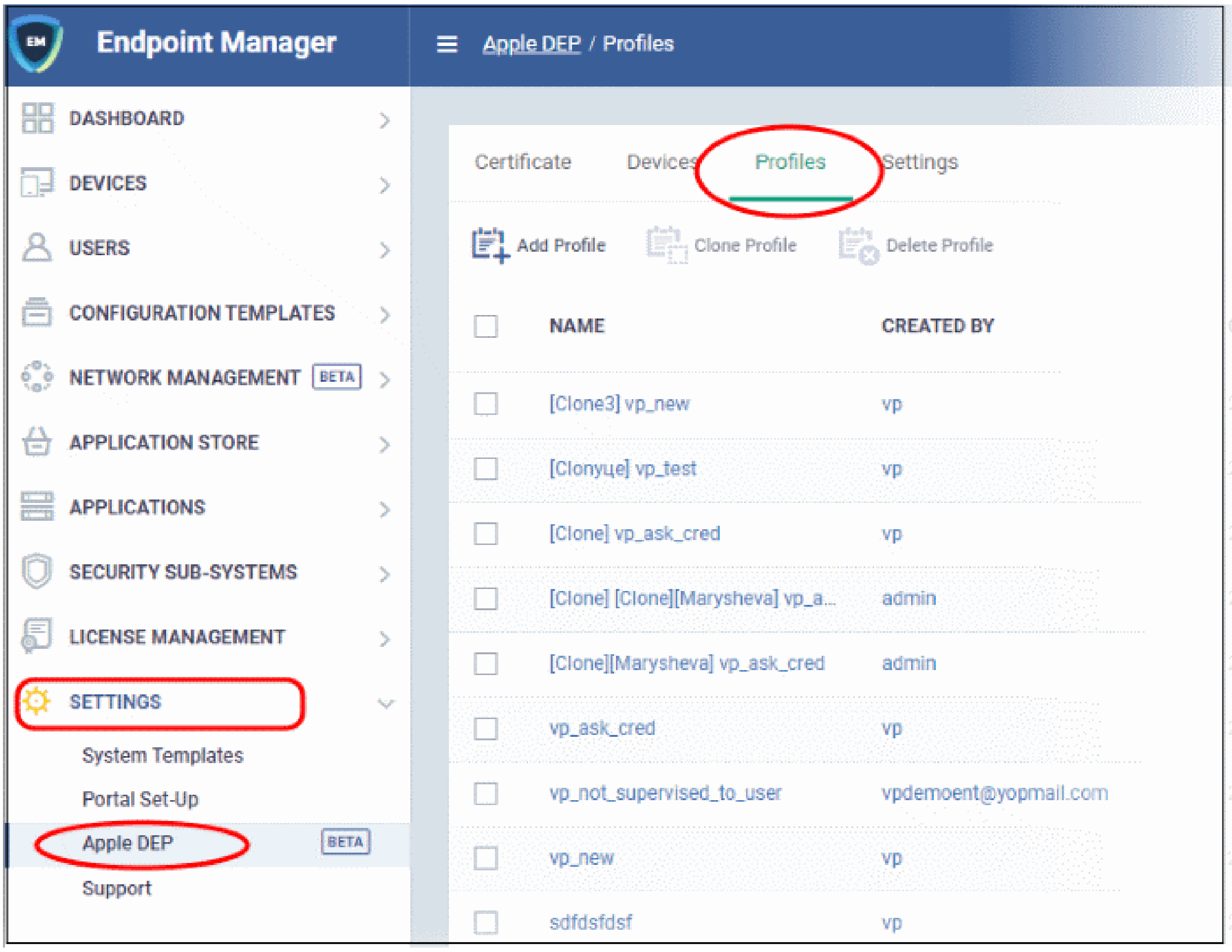
Click 'Settings' > 'Apple DEP' > 'Profiles'

- A DEP profile is assigned to target devices when you enroll them to Apple's Device Enrollment Program.
- Each profile lets you enable supervisor mode and other top-level management settings. Profiles also let you skip the setup wizards that appear when a user first activates a device.
- The profile is enabled right after the user activates the device. Activated profiles are listed as 'Pushed' in the 'Devices' tab.
- After enrollment, the device will appear in two places:
  - **Settings > Apple DEP > Devices** - Device identified by serial number.
  - **Devices > Devices List** - Device identified by name. Open device details to view the serial number.

The profiles area lets you:

- Create, clone and remove profiles
- Specify profile details:
  - Top-level device management settings
  - Enable / disable various setup wizards
  - Enable / disable various iOS features
- Publish the profile to the DEP server. Only published profiles can be assigned to devices.

Click 'Settings' > 'Apple DEP' then the 'Profiles' tab:

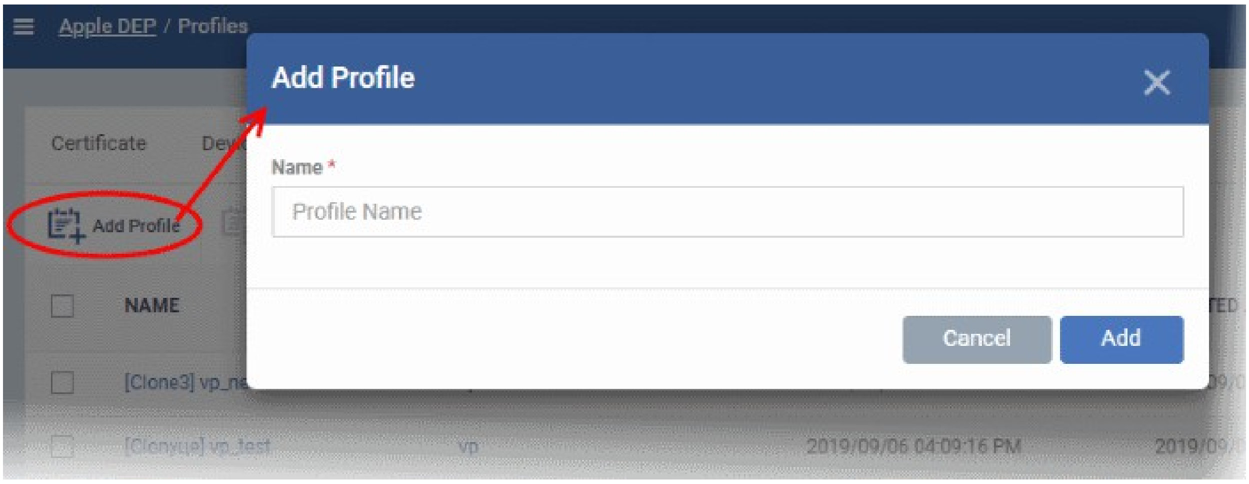


| □ | NAME | CREATED BY |
|---|---|---|
| □ | [Clone3] vp_new | vp |
| □ | [Clonyце] vp_test | vp |
| □ | [Clone] vp_ask_cred | vp |
| □ | [Clone] [Clone][Marysheva] vp_a... | admin |
| □ | [Clone][Marysheva] vp_ask_cred | admin |
| □ | vp_ask_cred | vp |
| □ | vp_not_supervised_to_user | vpdemoent@yopmail.com |
| □ | vp_new | vp |
| □ | sdfdsfdsf | vp |

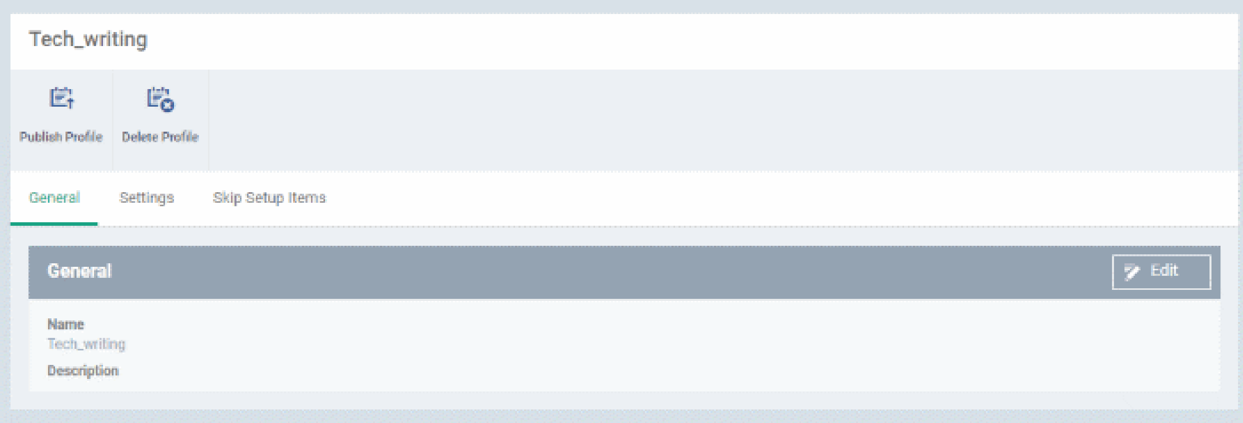
| Column Heading | Description |
|---|---|
| Name | DEP profile label |
| Created By | Name of the admin that configured the profile |
| Created At | Date and time the profile was configured |
| Updated At | Date and time the profile was modified |
| Published | Published means the profile has been submitted to, and accepted by, the DEP server. |

## Add a DEP profile

- Click 'Settings' > 'Apple DEP' > 'Profiles'
- Click 'Add Profile'
- Type a label for the profile then click 'Add':



- You will go straight to the profile configuration screen
- Click the 'Edit' button to review and modify profile settings:



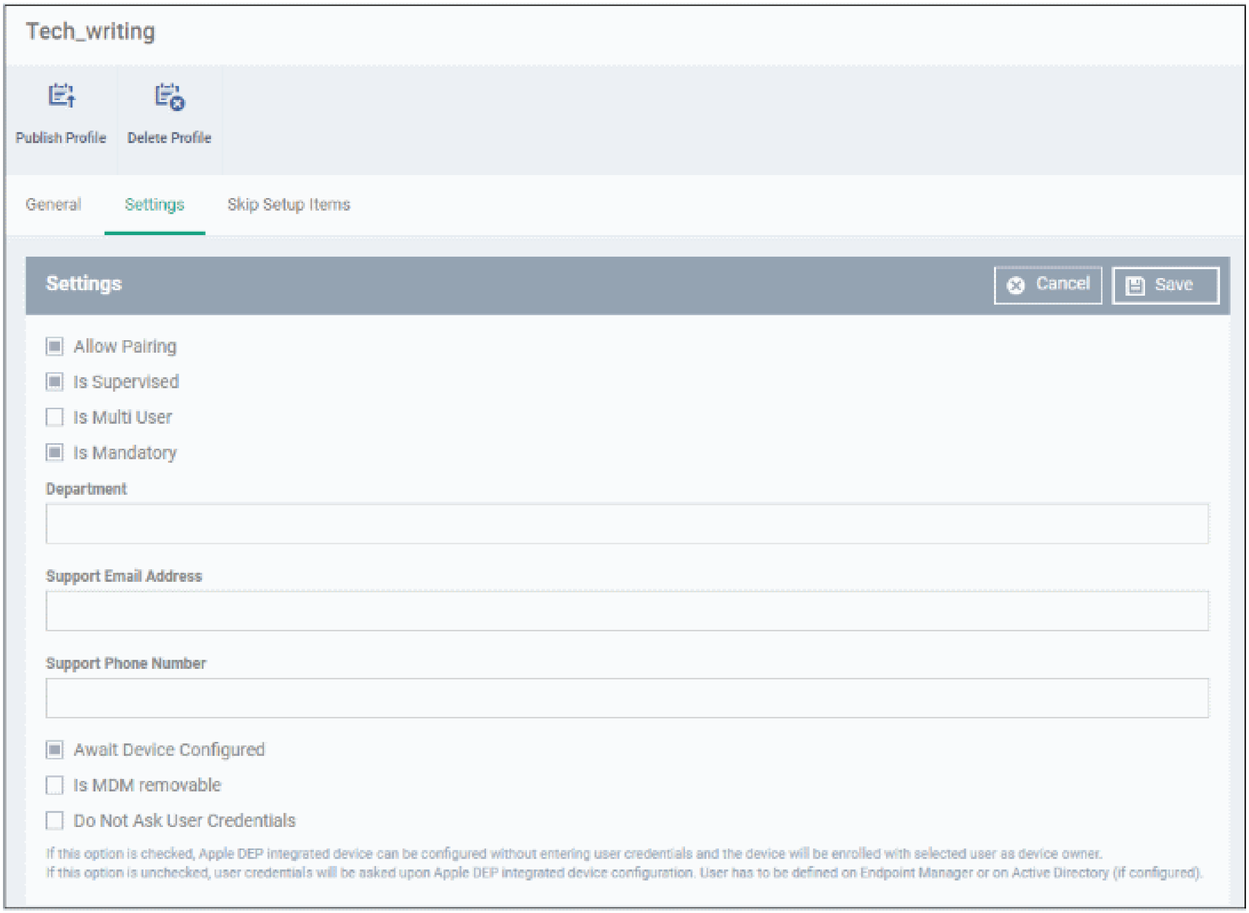
Name
Tech_writing
Description

### General

- Change the profile name and general description.

### Settings

Specify top-level device management settings, contact details and device department.:



☒ Allow Pairing

☒ Is Supervised

☐ Is Multi User

☒ Is Mandatory

Department

Support Email Address

Support Phone Number

☒ Await Device Configured

☐ Is MDM removable

☐ Do Not Ask User Credentials

If this option is checked, Apple DEP integrated device can be configured without entering user credentials and the device will be enrolled with selected user as device owner.
If this option is unchecked, user credentials will be asked upon Apple DEP integrated device configuration. User has to be defined on Endpoint Manager or on Active Directory (if configured).

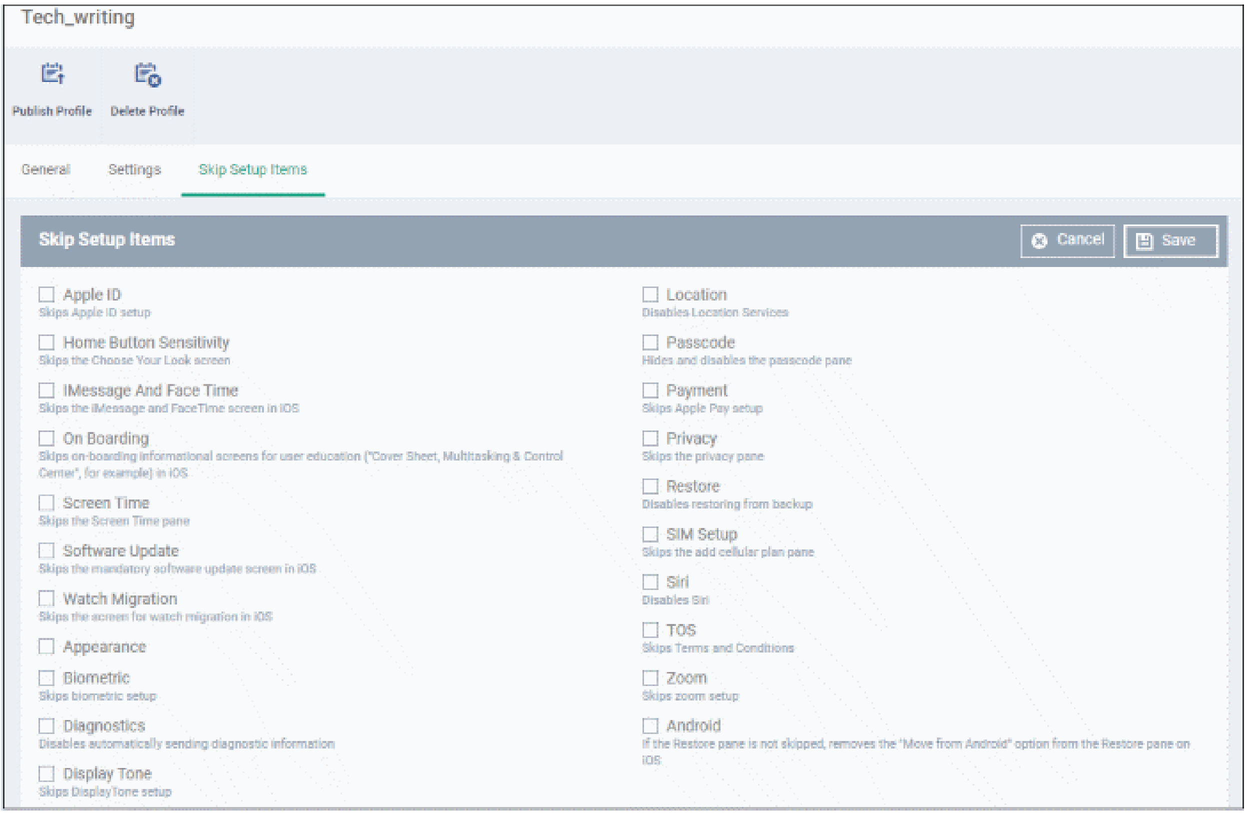
- **Allow Pairing -** Specify whether the device can pair with other devices. For example, with Apple watches, earphones and other Bluetooth devices.
- **Is Supervised -** Puts the target device in supervised mode. You must enable this setting to manage the device.
- **Is Multi User -** More than one user account can be stored on the device. This lets multiple users share a single device, while maintaining the privacy of all users. This is required for education functionality such as Apple School Manager.
- **Is Mandatory -** If enabled, the user must enroll the device to EM at device activation. The user cannot skip installation of the EM profile.
- **Department -** The department of your company that they device belongs to.
  - Comodo One / Dragon users - This is not connected to Service Desk departments programmatically. However, you can use a Service Desk department name here for the sake of identification.
- **Support Email Address -** The address at which device users can contact your IT staff.
- **Support Phone Number -** The number at which device users can contact your IT staff.
- **Await Device Configured -** If enabled, users will not be able to proceed in the setup assistant until Endpoint Manager sends a command that states the device is configured. This setting only applies if the devised is in supervised mode.
- **Is MDM removable -** If enabled, the Endpoint Manager (EM) profile can be removed from the device. This removes it from EM control. Note - The EM profile cannot be removed if the device is in supervised mode.
- **Do Not Ask User Credentials**
  - Enabled - The device can be activated without a user authentication. The admin can assign the device to any user.
  - Disabled - The user has to login to the device at activation. Note - The user should be already have be added to Endpoint Manager.

- Click 'Save'

### Skip Setup Items

Specify which setup wizards should be shown during device activation. User can configure these items later if allowed by the Endpoint Manager profile.

- Click 'Skip Setup Items'. All setup items are enabled/shown by default.
- Click 'Edit' to disable specific items.



□ Apple ID
Skips Apple ID setup

□ Home Button Sensitivity
Skips the Choose Your Look screen

□ IMessage And Face Time
Skips the iMessage and FaceTime screen in iOS

□ On Boarding
Skips on-boarding informational screens for user education ("Cover Sheet, Multitasking & Control Center", for example) in iOS

□ Screen Time
Skips the Screen Time pane

□ Software Update
Skips the mandatory software update screen in iOS

□ Watch Migration
Skips the screen for watch migration in iOS

□ Appearance

□ Biometric
Skips biometric setup

□ Diagnostics
Disables automatically sending diagnostic information

□ Display Tone
Skips DisplayTone setup

□ Location
Disables Location Services

□ Passcode
Hides and disables the passcode pane

□ Payment
Skips Apple Pay setup

□ Privacy
Skips the privacy pane

□ Restore
Disables restoring from backup

□ SIM Setup
Skips the add cellular plan pane

□ Siri
Disables Siri

□ TOS
Skips Terms and Conditions

□ Zoom
Skips zoom setup

□ Android
If the Restore pane is not skipped, removes the "Move from Android" option from the Restore pane on iOS

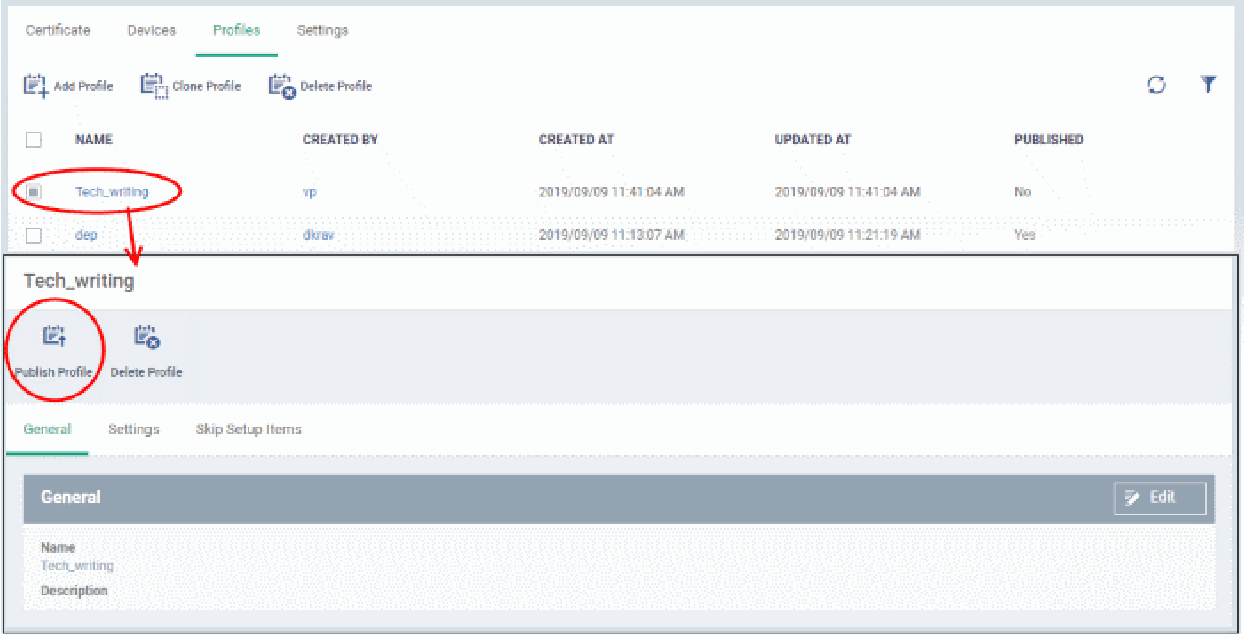
- Click 'Save' to apply your changes.

The next step is to publish the profile to the DEP server.

## Publish Profile

You have to submit the profile to the DEP server in order to push it to devices.

- Click 'Settings' > 'Apple DEP' > 'Profiles'
- Click the name of a profile. Note - Published profiles cannot be re-published or deleted.



| □ | NAME | CREATED BY | CREATED AT | UPDATED AT | PUBLISHED |
|---|---|---|---|---|---|
| ■ | Tech_writing | vp | 2019/09/09 11:41:04 AM | 2019/09/09 11:41:04 AM | No |
| □ | dep | dkrav | 2019/09/09 11:13:07 AM | 2019/09/09 11:21:19 AM | Yes |

Tech_writing

General

Name
Tech_writing
Description

- Click Publish Profile at top-left

A confirmation message is shown:

Profile successfully published

You can assign a published profile to devices. See **Manage Apple DEP Devices**.

## Edit a Profile

- Click on the name of a profile then click 'Edit' at top-left
- The process is the same as explained above for adding a profile
- You cannot modify a published profile

## Clone a Profile

- Select a profile and click the 'Clone Profile' button
- You can create a new profile by copying an existing profile making changes as required
- You can clone both published and unpublished profiles

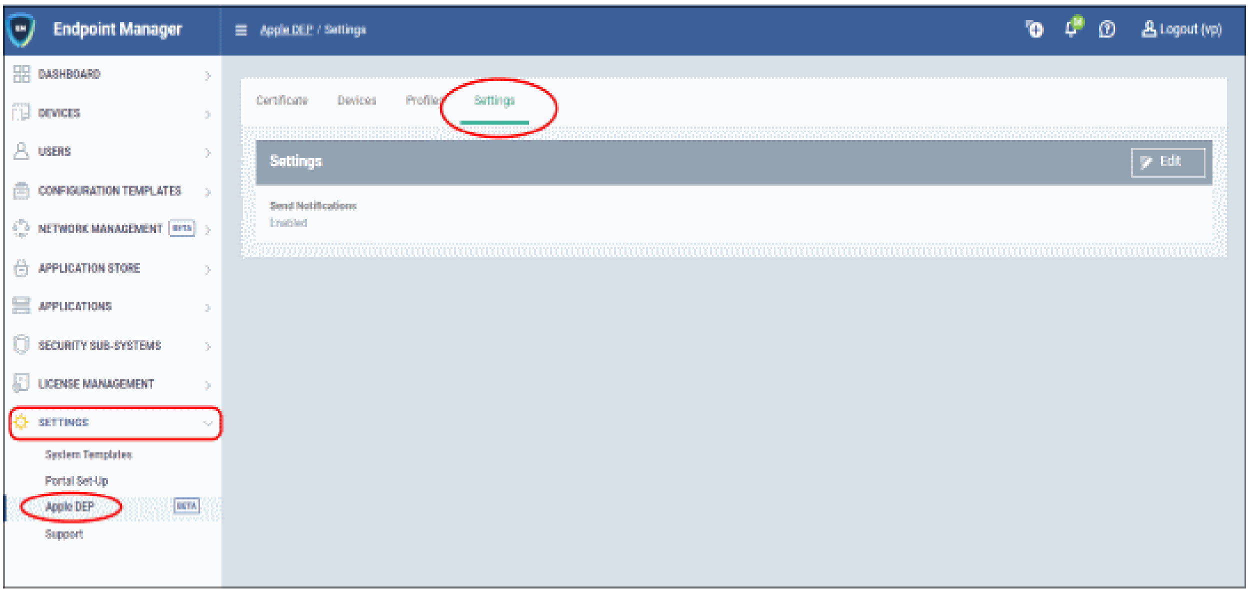
## Delete a Profile

- Select a profile and click 'Delete Profile'

  OR
- Click the name of the profile and click 'Delete Profile'
- You cannot delete a published profile

### 11.3.4. Configure Apple DEP Notifications

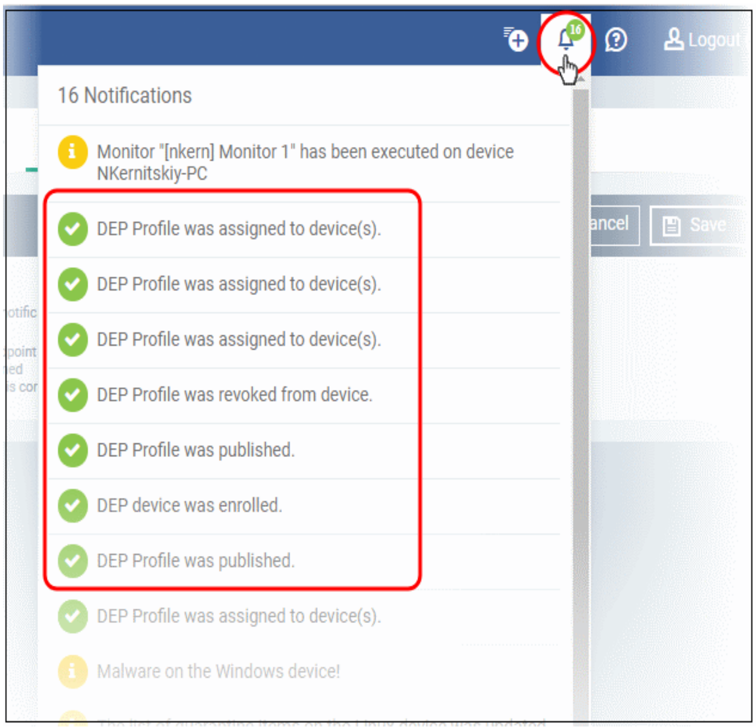
- Click 'Settings' > 'Apple DEP' > 'Settings'
- Click 'Edit':



Settings

Send Notifications
Enabled

- **Send Notifications -** Choose whether or not you want to see alerts from DEP in the notifications area:



16 Notifications

Monitor "[nkern] Monitor 1" has been executed on device NKernitskiy-PC

DEP Profile was assigned to device(s).

DEP Profile was assigned to device(s).

DEP Profile was assigned to device(s).

DEP Profile was revoked from device.

DEP Profile was published.

DEP device was enrolled.

DEP Profile was published.

DEP Profile was assigned to device(s).

Malware on the Windows device!

If enabled, you will see alerts when:

- A DEP profile is published (submitted to the DEP server)
- A DEP profile is unassigned or unassigned ('Settings' > 'Apple DEP' > 'Devices')
- A device is enrolled to DEP, or removed from DEP.

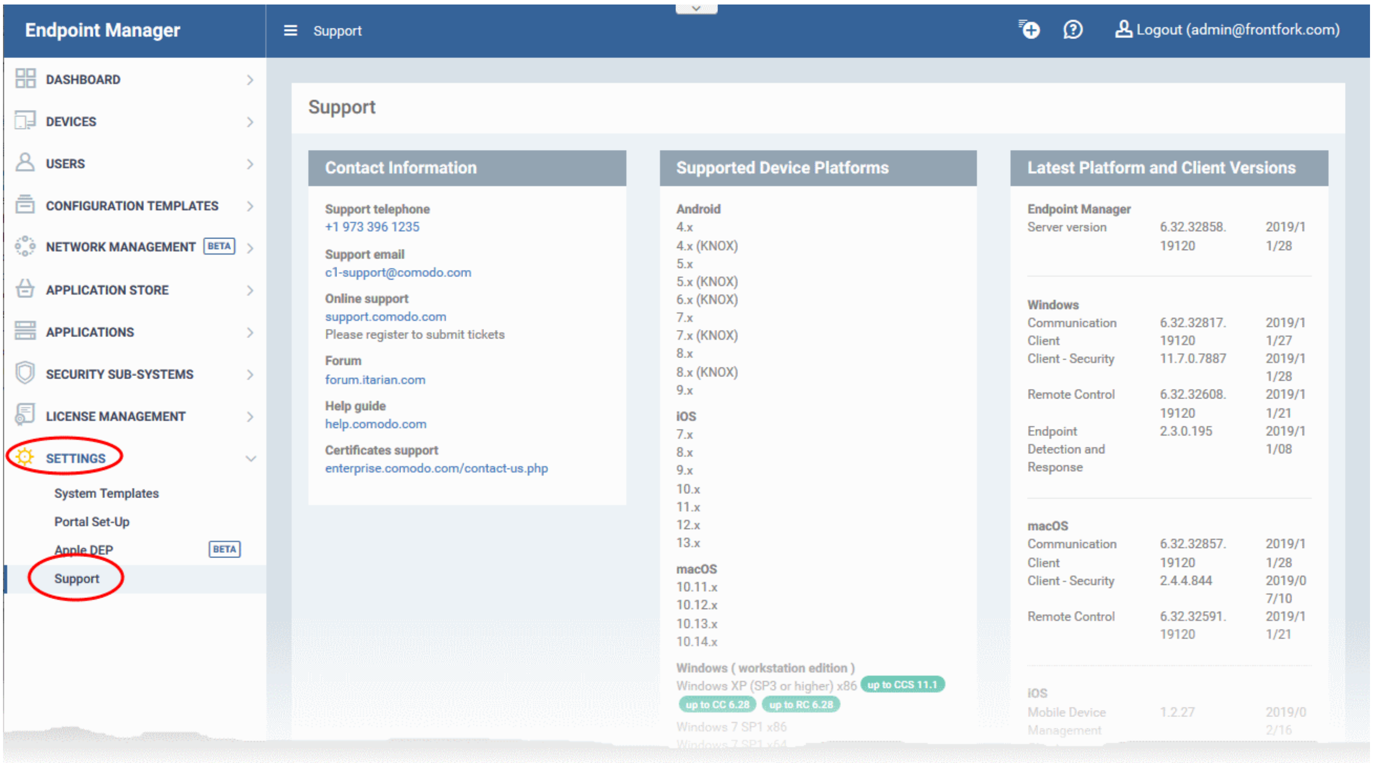
# 11.4. View Version and Support Information

- Click 'Settings' > 'Support'

The support panel shows contact information, the Endpoint Manager version number, and a list of platforms supported by this version.

**View the version and support details**

- Click 'Settings' > 'Support'



Support

**Contact Information**

**Support telephone**
+1 973 396 1235

**Support email**
c1-support@comodo.com

**Online support**
support.comodo.com
Please register to submit tickets

**Forum**
forum.itarian.com

**Help guide**
help.comodo.com

**Certificates support**
enterprise.comodo.com/contact-us.php

**Supported Device Platforms**

**Android**
4.x
4.x (KNOX)
5.x
5.x (KNOX)
6.x (KNOX)
7.x
7.x (KNOX)
8.x
8.x (KNOX)
9.x

**iOS**
7.x
8.x
9.x
10.x
11.x
12.x
13.x

**macOS**
10.11.x
10.12.x
10.13.x
10.14.x

**Windows ( workstation edition )**
Windows XP (SP3 or higher) x86 up to CCS 11.1 up to CC 6.28 up to RC 6.28
Windows 7 SP1 x86
Windows 7 SP1 x64

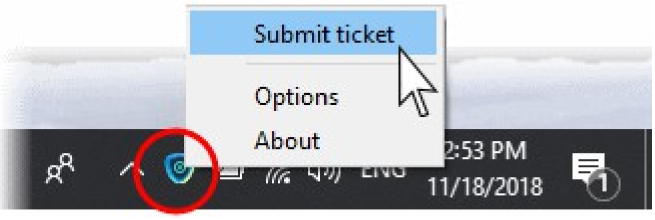
**Latest Platform and Client Versions**

| | | |
|---|---|---|
| **Endpoint Manager** | | |
| Server version | 6.32.32858.19120 | 2019/11/28 |
| **Windows** | | |
| Communication Client | 6.32.32817.19120 | 2019/11/27 |
| Client - Security | 11.7.0.7887 | 2019/11/28 |
| Remote Control | 6.32.32608.19120 | 2019/11/21 |
| Endpoint Detection and Response | 2.3.0.195 | 2019/11/08 |
| **macOS** | | |
| Communication Client | 6.32.32857.19120 | 2019/11/28 |
| Client - Security | 2.4.4.844 | 2019/07/10 |
| Remote Control | 6.32.32591.19120 | 2019/11/21 |
| **iOS** | | |
| Mobile Device Management | 1.2.27 | 2019/02/16 |

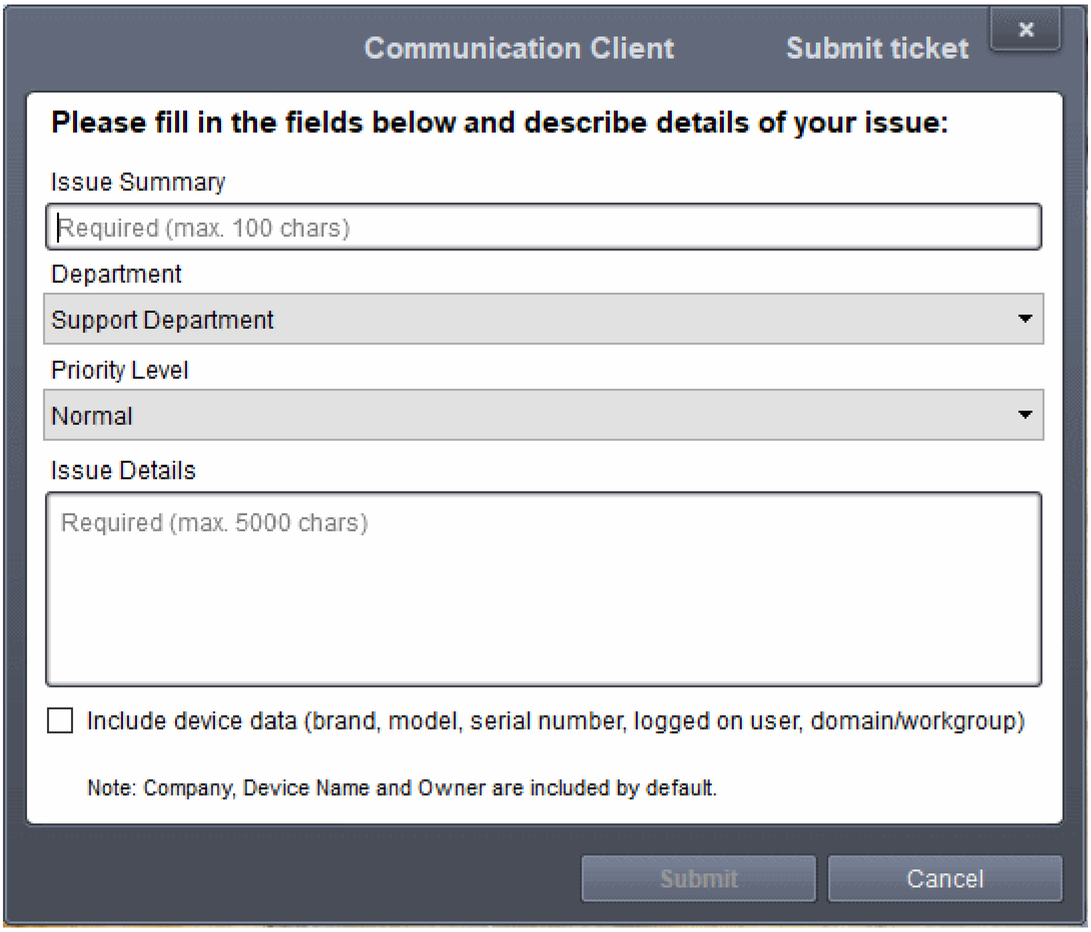
- **Contact Information -** Support telephone numbers and email addresses
- **Supported Device Platforms -** The devices and operating systems supported by this version of Endpoint Manager.
- **Latest Platform and Client Versions -** Version numbers of the Endpoint Manager server, communication clients and client security software.

**Submit Ticket -** Your end-users can submit a ticket to your Service Desk module for your technicians to handle.

- Right-click on the communication client tray icon and select 'Submit ticket'



The 'Submit ticket' dialog opens:



Please fill in the fields below and describe details of your issue:

Issue Summary

Required (max. 100 chars)

Department

Support Department

Priority Level

Normal

Issue Details

Required (max. 5000 chars)

□ Include device data (brand, model, serial number, logged on user, domain/workgroup)

Note: Company, Device Name and Owner are included by default.

Tip: You can rebrand the dialog shown above as required. See Communication Client and Comodo Client - Security Application UI Settings in Create Windows Profiles for help with this.

- Issue Summary - Provide a short description of the issue.
- Department - Select the department to whom the ticket should be assigned.
- Priority Level - Select the priority from the drop-down. The levels are: Low, Normal, High and Critical.
- Issue Details - Provide detailed description of the issue.

- Click 'Submit'.

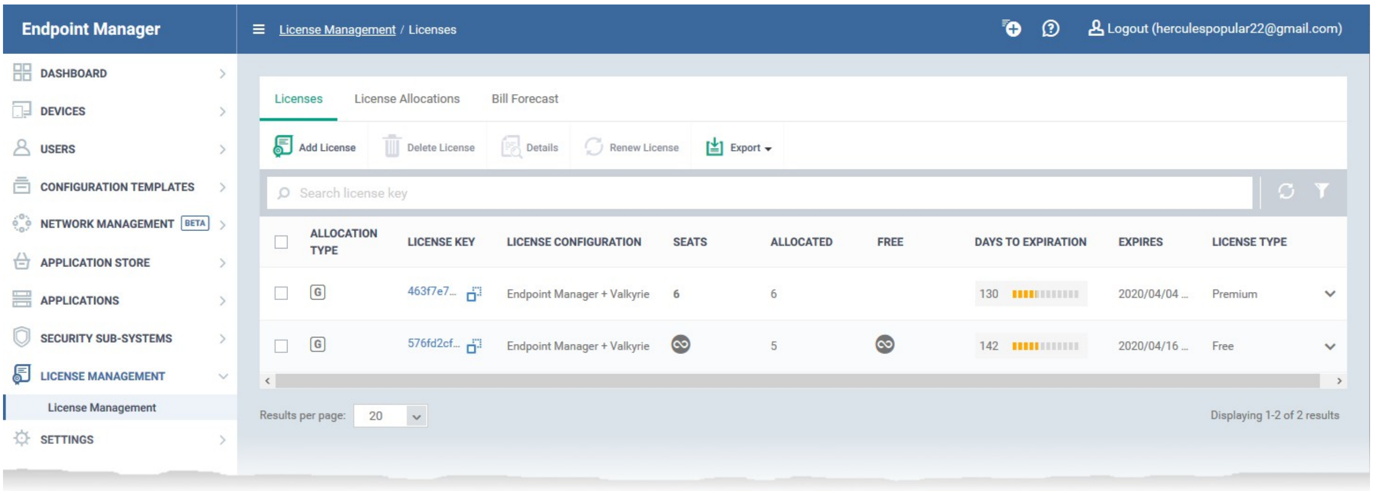
A support ticket will be created in the Service Desk module of the Comodo Dragon or Comodo One account based on your subscription and assigned to the selected department.

# 12. License Management

- Click 'License Management' > 'License Management'

This section allows you to:

- View license details
- Add a new license
- Delete a license
- Renew a license
- Use a single license to enroll devices for multiple customers (MSPs only)
- Assign multiple licenses to a single customer (MSPs only)
- Configure license usage reports



| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE | DAYS TO EXPIRATION | EXPIRES | LICENSE TYPE |
|---|---|---|---|---|---|---|---|---|---|
| □ | G | 463f7e7... | Endpoint Manager + Valkyrie | 6 | 6 | | 130 | 2020/04/04 ... | Premium |
| □ | G | 576fd2cf... | Endpoint Manager + Valkyrie | ∞ | 5 | ∞ | 142 | 2020/04/16 ... | Free |

Results per page: 20

Displaying 1-2 of 2 results

See the following sections for help with each tab:

- **Licenses** - View and manage your licenses
- **License Allocation**- Use your licenses for multiple customers
- **Bill Forecast** - View estimated future charges

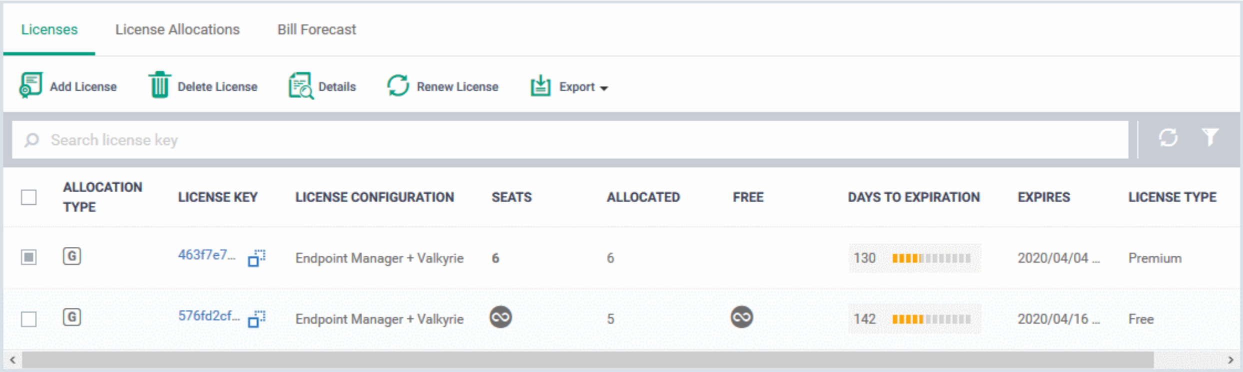
# 12.1. Manage your Licenses

- Click 'License Management' > 'License Management'
- This area lets you add, delete and renew licenses, view license details, change license allocation, configure reports, and more.

See the following for more help:

- **License table columns**
- **Add a license**
- **Delete a license**
- **View license details, change allocation type**
- **Renew a license**
- **Configure usage report settings**
- **Export list of licenses**

### License table columns

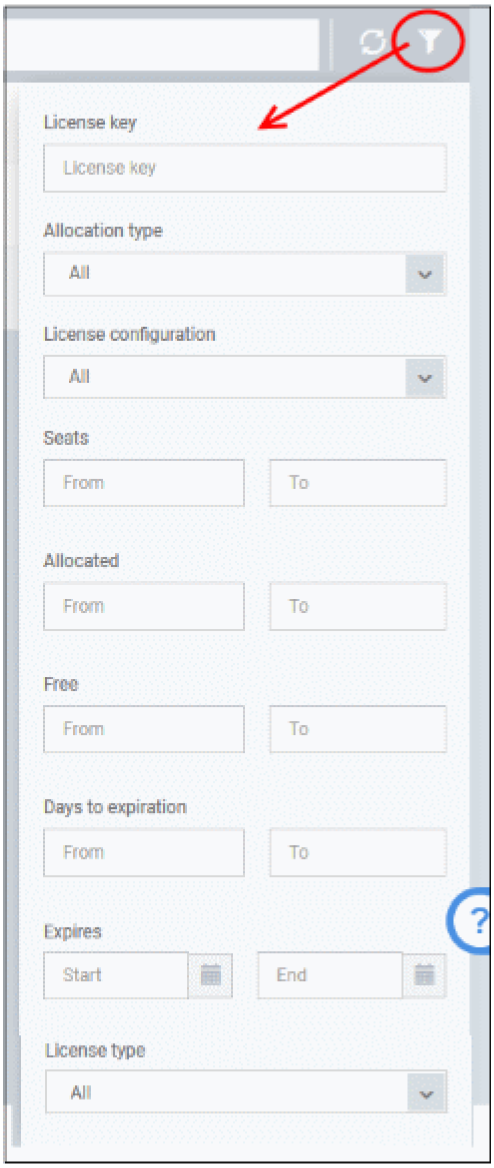


| ☐ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE | DAYS TO EXPIRATION | EXPIRES | LICENSE TYPE |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | G | 463f7e7... | Endpoint Manager + Valkyrie | 6 | 6 | | 130 | 2020/04/04 ... | Premium |
| ☐ | G | 576fd2cf... | Endpoint Manager + Valkyrie | ∞ | 5 | ∞ | 142 | 2020/04/16 ... | Free |

| Column | Description |
|---|---|
| Allocation Type | States whether you can use the license for multiple customers or a single customer.<br>• **Global (G)** - You can use the license for multiple customers<br>• **Allocated (A)** - You can use the license on a single customer<br>You can change the allocation type of a license as follows:<br>• Select a license<br>• Click the 'Details' button at the top<br>• Click the 'Edit' button<br>• Select 'Global' or 'Customer' in the 'Allocation type' drop-down.<br>• Click 'Save'<br>See '**View License Details and Change Allocation Type**' if you need more help. |
| License Key | Unique identifier for the license. |
| License Configuration | The security features which are included on the license. |
| Seats | Number of devices covered by the license.<br>• The infinity symbol icon indicates unlimited seats.<br>• These licenses support unlimited devices, but are limited to a one month term. |

| | |
|---|---|
| Allocated | The number of seats that you have already assigned to devices.<br>Seats can be assigned to a single customer or multiple customers. |
| Free | Number of seats remaining on the license. |
| Days to Expiration | Number of days left on the license. |
| Expires | License period end date and time |
| License Type | Indicates whether the subscription is free, premium or managed. |

- Click column headers to sort items in ascending or descending order
- You can enter license keys in the search box to locate specific licenses.
- Click the funnel at top-right to open more filters:



License key

License key

Allocation type

All

License configuration

All

Seats

From | To

Allocated

From | To

Free

From | To

Days to expiration

From | To

Expires

Start | End

License type

All

## Add a License

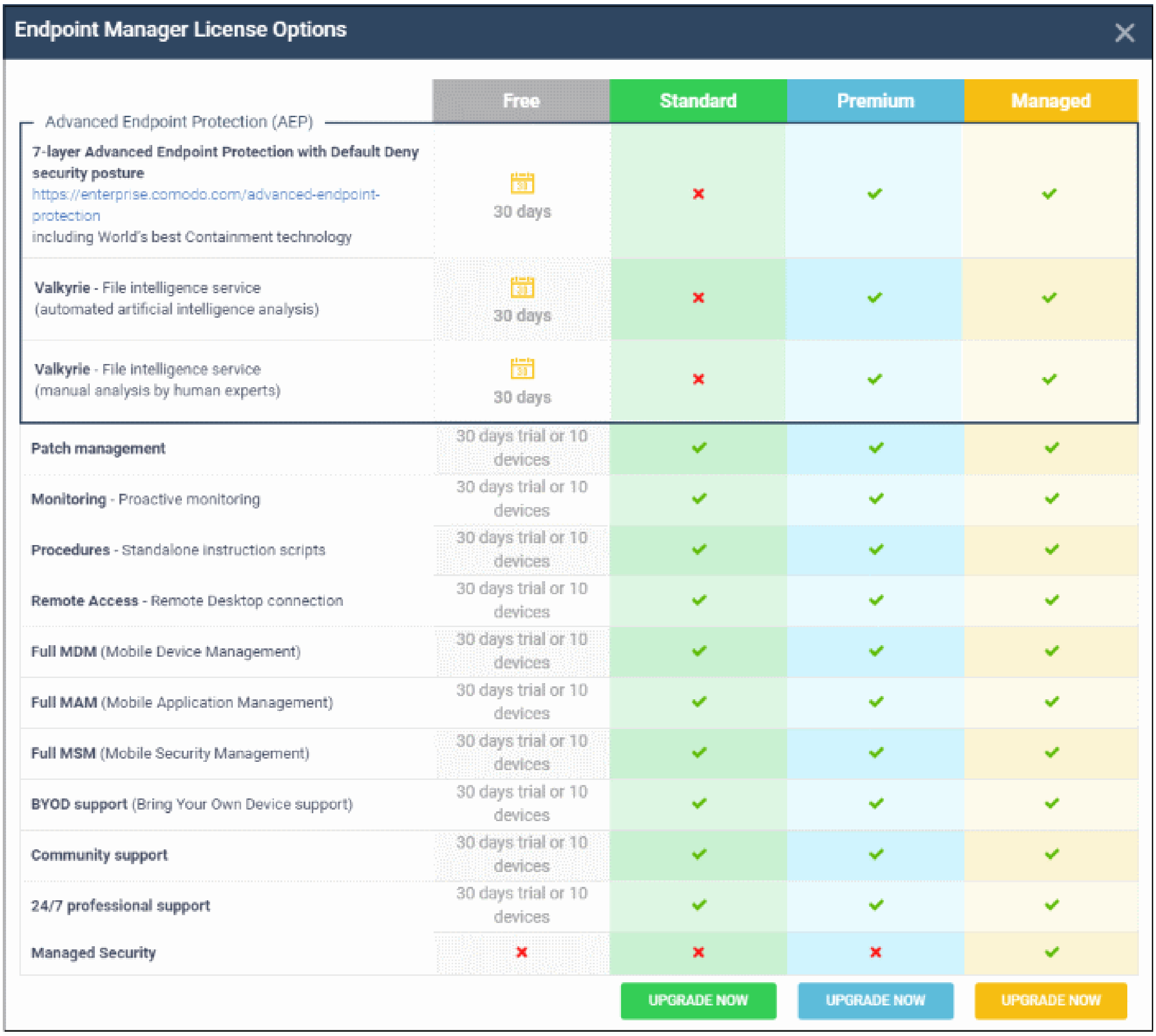
You can purchase new licenses from Comodo Account Manager (CAM) at **https://accounts.comodo.com**.

- Log in at https://accounts.comodo.com with your Comodo username and password
- Select 'Endpoint Manager' and complete the purchase process.

Your license key will be sent to your registered email address.

### Upgrade a license

- Alternatively, click 'License Options' at the top of the Endpoint Manager interface.
- This opens a comparison of available license types:



Endpoint Manager License Options

| Advanced Endpoint Protection (AEP) | Free | Standard | Premium | Managed |
|---|---|---|---|---|
| **7-layer Advanced Endpoint Protection with Default Deny security posture** https://enterprise.comodo.com/advanced-endpoint-protection including World's best Containment technology | 📅 30 days | ✗ | ✓ | ✓ |
| **Valkyrie** - File intelligence service (automated artificial intelligence analysis) | 📅 30 days | ✗ | ✓ | ✓ |
| **Valkyrie** - File intelligence service (manual analysis by human experts) | 📅 30 days | ✗ | ✓ | ✓ |
| **Patch management** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Monitoring** - Proactive monitoring | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Procedures** - Standalone instruction scripts | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Remote Access** - Remote Desktop connection | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MDM** (Mobile Device Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MAM** (Mobile Application Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MSM** (Mobile Security Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **BYOD support** (Bring Your Own Device support) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Community support** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **24/7 professional support** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Managed Security** | ✗ | ✗ | ✗ | ✓ |
| | | UPGRADE NOW | UPGRADE NOW | UPGRADE NOW |

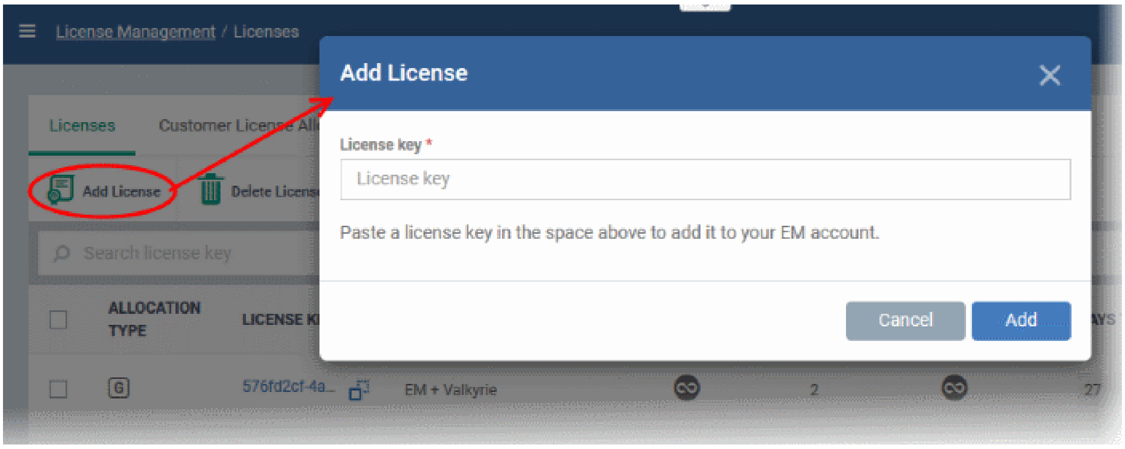
- Click 'Upgrade Now' under the license type you want.

You will be taken to the order forms to complete the purchase.

### Register the license

Once you have obtained a new license, you need to register it in Endpoint Manager.

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Click 'Add New License' at the top left.



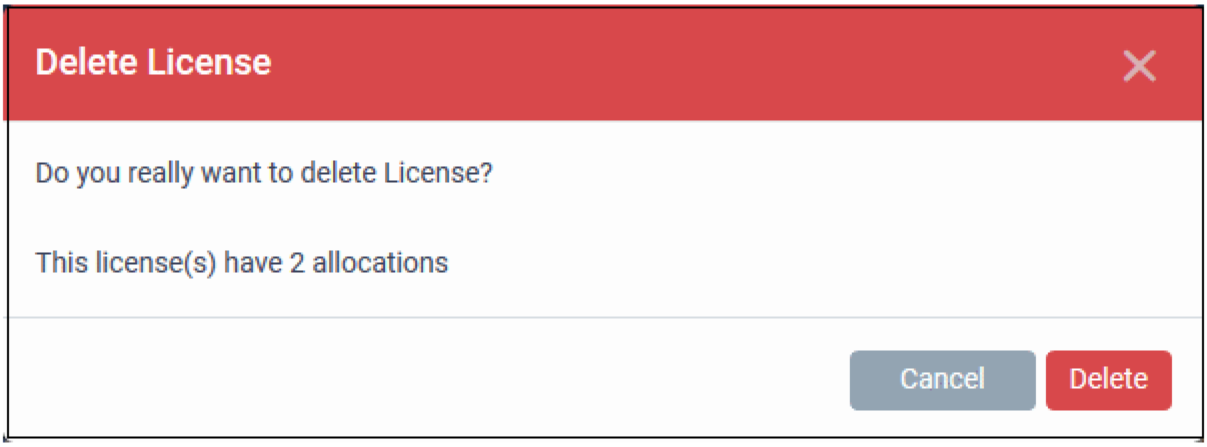
Paste a license key in the space above to add it to your EM account.

- Enter the license key from your confirmation email.
- Click 'Add'.

Your new license is shown in the 'License Key' column.

## Delete a License

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Select the license and click 'Delete License' at the top



Do you really want to delete License?

This license(s) have 2 allocations

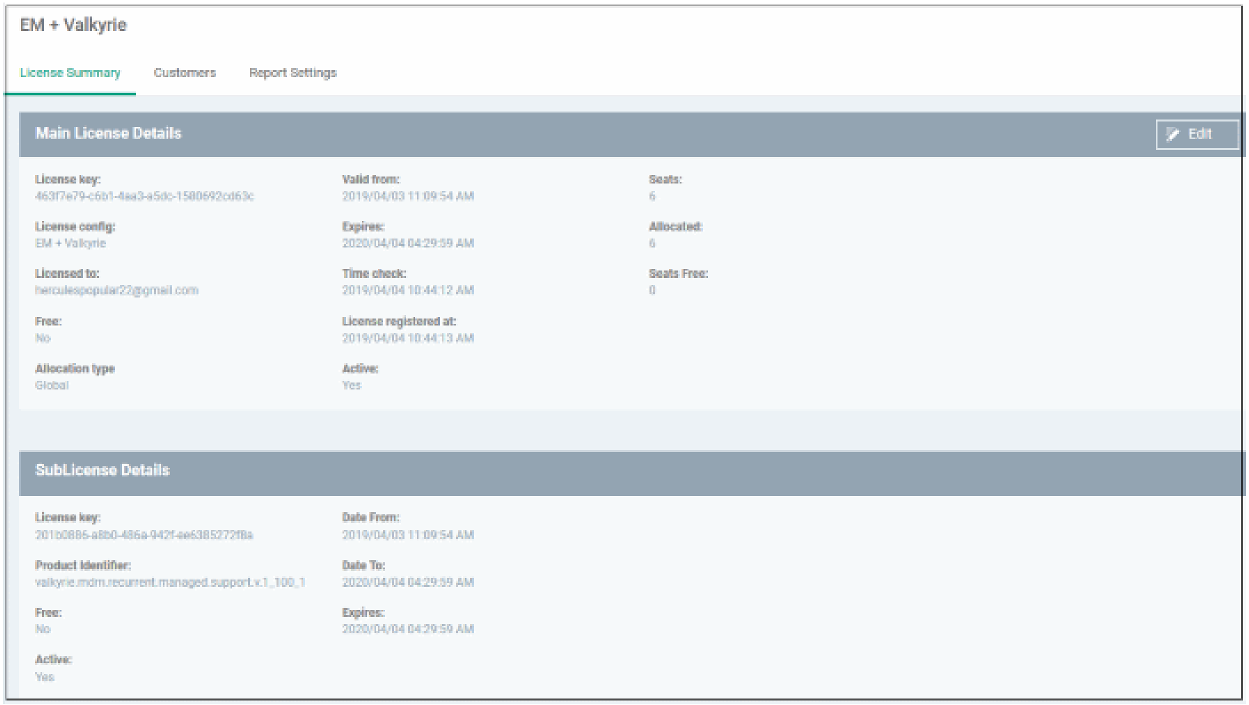
- Click 'Delete' to remove the license from the list.

Note - You can add the license again if required. See above how to add a license.

## View License Details and Change Allocation Type

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Select the license and click 'Details' at the top.

The license details screen opens:



Main License Details

License key:
463f7e79-c6b1-4aa3-a5dc-1580692cd63c

License config:
EM + Valkyrie

Licensed to:
herculespopular22@gmail.com

Free:
No

Allocation type
Global

Valid from:
2019/04/03 11:09:54 AM

Expires:
2020/04/04 04:29:59 AM

Time check:
2019/04/04 10:44:12 AM

License registered at:
2019/04/04 10:44:13 AM

Active:
Yes

Seats:
6

Allocated:
6

Seats Free:
0

SubLicense Details

License key:
201b0886-a8b0-486a-942f-ee6385272f8a

Product Identifier:
valkyrie.mdm.recurrent.managed.support.v.1_100_1

Free:
No

Active:
Yes

Date From:
2019/04/03 11:09:54 AM

Date To:
2020/04/04 04:29:59 AM

Expires:
2020/04/04 04:29:59 AM

The license details screen has three tabs:

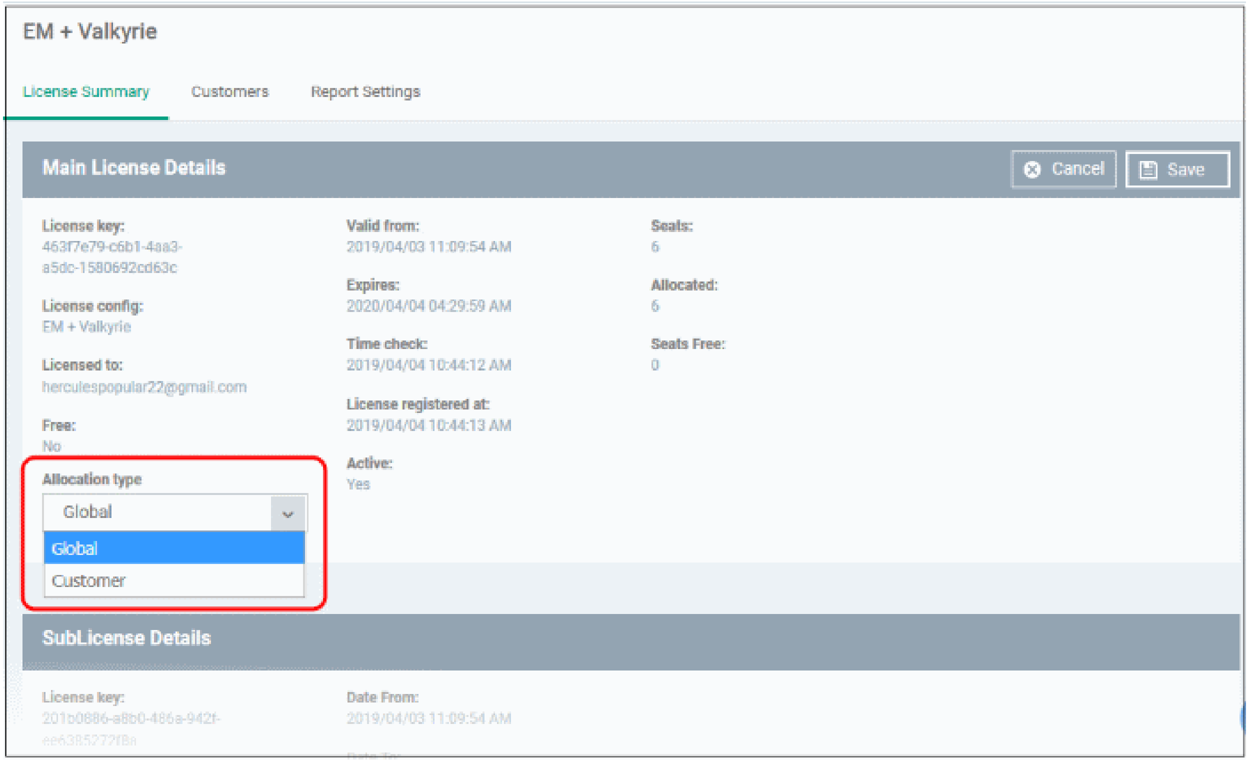
- **License Summary** - Details of your subscriptions for Endpoint Manager and other Comodo products. You can change the license allocation type from here too.
- **Customers** - Shows how your license seats are allocated among your customers. You can change seat allocation from here.
- **Report Settings** - Configure license usage reports.

## License Summary

- **Main License Details** - Info about your Endpoint Manager subscriptions.
- **Sub License Details** - Info about additional subscriptions included with the main license. These licenses are for other Comodo products such as Valkyrie.

### Change License Allocation Type

- Click on a license key to open its details screen
- Click the 'Edit' button on the right
- Use the drop-down menu to change the allocation type:
  - **Global (G)** - You can use the license for multiple customers
  - **Allocated (A)** - You can use the license on a single customer


EM + Valkyrie

License key: 463f7e79-c6b1-4aa3-a5dc-1580692cd63c

License config: EM + Valkyrie

Licensed to: herculespopular22@gmail.com

Free: No

Allocation type: Global

Valid from: 2019/04/03 11:09:54 AM

Expires: 2020/04/04 04:29:59 AM

Time check: 2019/04/04 10:44:12 AM

License registered at: 2019/04/04 10:44:13 AM

Active: Yes

Seats: 6

Allocated: 6

Seats Free: 0

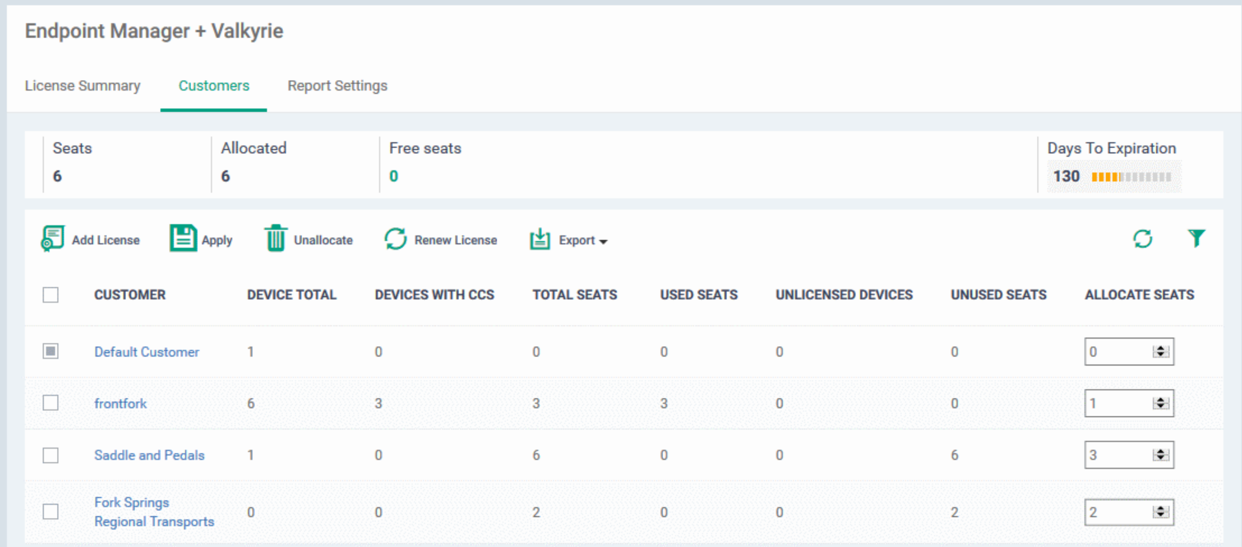
License key: 201b0886-a8b0-486a-942f-ee6385272f8a

Date From: 2019/04/03 11:09:54 AM

- Click 'Save'.
- You can assign seats to specific customers in the 'Customers' tab.

## Customers

The customers area shows how your seats are distributed among your customers. You can reallocate seats, add new licenses to a customer, renew licenses, and more.


Endpoint Manager + Valkyrie

Seats 6 | Allocated 6 | Free seats 0 | Days To Expiration 130

| □ | CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS | ALLOCATE SEATS |
|---|---|---|---|---|---|---|---|---|
| ☒ | Default Customer | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | frontfork | 6 | 3 | 3 | 3 | 0 | 0 | 1 |
| □ | Saddle and Pedals | 1 | 0 | 6 | 0 | 0 | 6 | 3 |
| □ | Fork Springs Regional Transports | 0 | 0 | 2 | 0 | 0 | 2 | 2 |

The top row shows the total number of seats covered by the license, total seats assigned to customers and the number of seats remaining.

| Column Heading | Description |
|---|---|
| Customer | Name of your client. Click the name to view their **license usage**. |
| Device Total | Number of endpoints you have assigned to the customer in Endpoint Manager. |

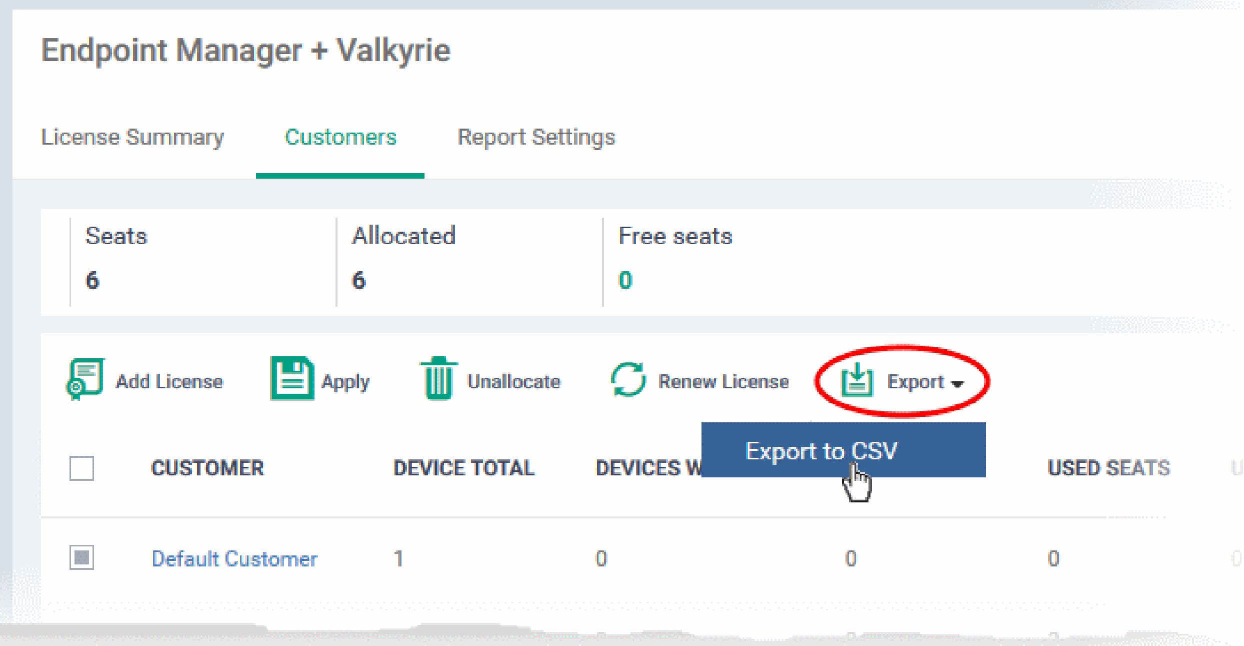
| | |
|---|---|
| Device with CCS | Number of endpoints which have Comodo Client Security (CCS) installed |
| Total Seats | Number of seats available on all licenses assigned to the customer |
| Used Seats | Number of seats currently assigned to the customer's endpoints |
| Unlicensed Devices | Number of devices enrolled for the customer and have CCS installed, exceeding the total number of seats allotted for the customer. |
| Unused Seats | Number of seats remaining on the license<br>• Unused seats = Total seats - Used seats |
| Allocate Seats | Add or remove seats to/from the customer |
| Controls | • **Add License** - Import a new license to a your account. See **Add a License** for more details.<br>• **Apply** - Save your settings.<br>• **Unallocate** - Remove licenses from a customer<br>• **Renew** - Renew a license for a customer. |

The interface allow you to:

- **Redistribute seats to customers** - See '**Select a license and assign it to different customers**' for more help with this.
- **Generate a report of seat distribution**

**Export the seat distribution report for a license**

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Select the license and click 'Details' at the top
- Click the 'Customers' tab
- Click the 'Export' button above the table then choose 'Export to CSV':



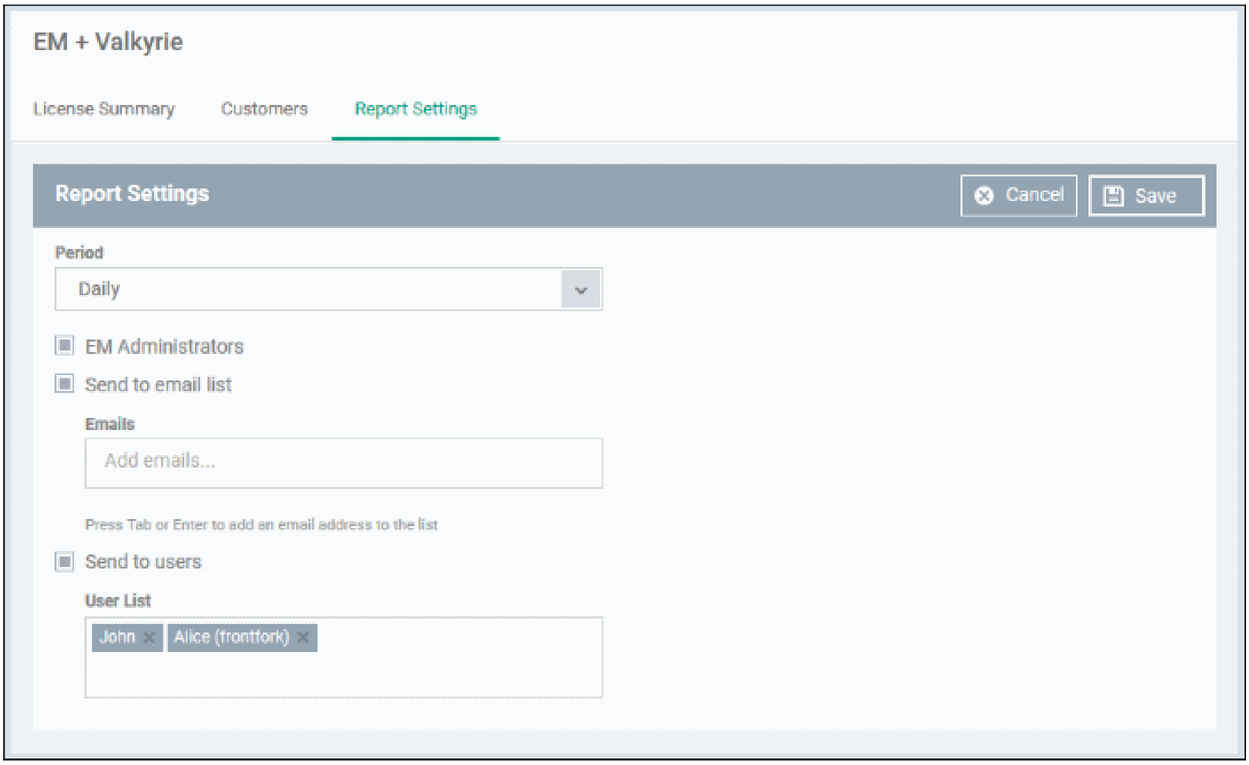
- The CSV file will be available in 'Dashboard' > 'Reports'

- See **Reports** in **The Dashboard** for more details.

## Configure Usage Report Settings

The report contains details on the license period, allocation type, customers covered by the license, total devices used, and so on.

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Select the license and click 'Details' at the top
- Open the 'Report Settings' tab and click 'Edit' at top-right



Period: Daily

□ EM Administrators

□ Send to email list

Emails: Add emails...

Press Tab or Enter to add an email address to the list

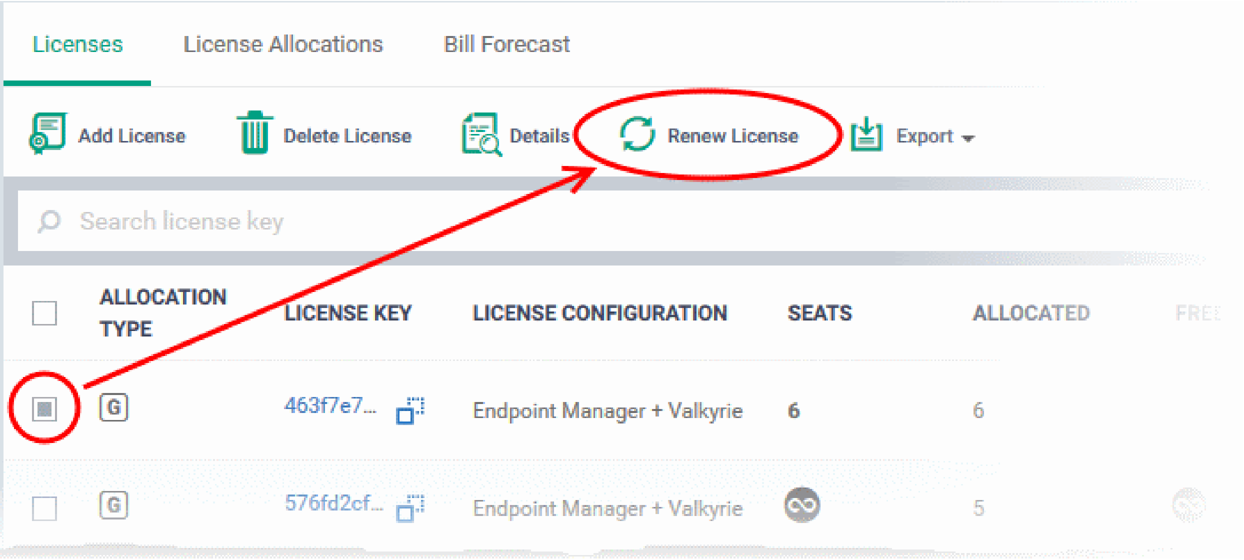
□ Send to users

User List: John ×, Alice (frontfork) ×

- **Period -** How frequently the report is generated.
- **EM Administrators -** Send the report to users with the admin role
- **Send to email list -** Add the mail addresses of people to whom the report should be sent.
  - Enter an email address then press 'Enter'. Repeat the process to add more addresses.
- **Send to users -** Add enrolled users to whom the report should be sent.
  - Enter the first few letters of a username then select from the suggestions.
- Click 'Save'

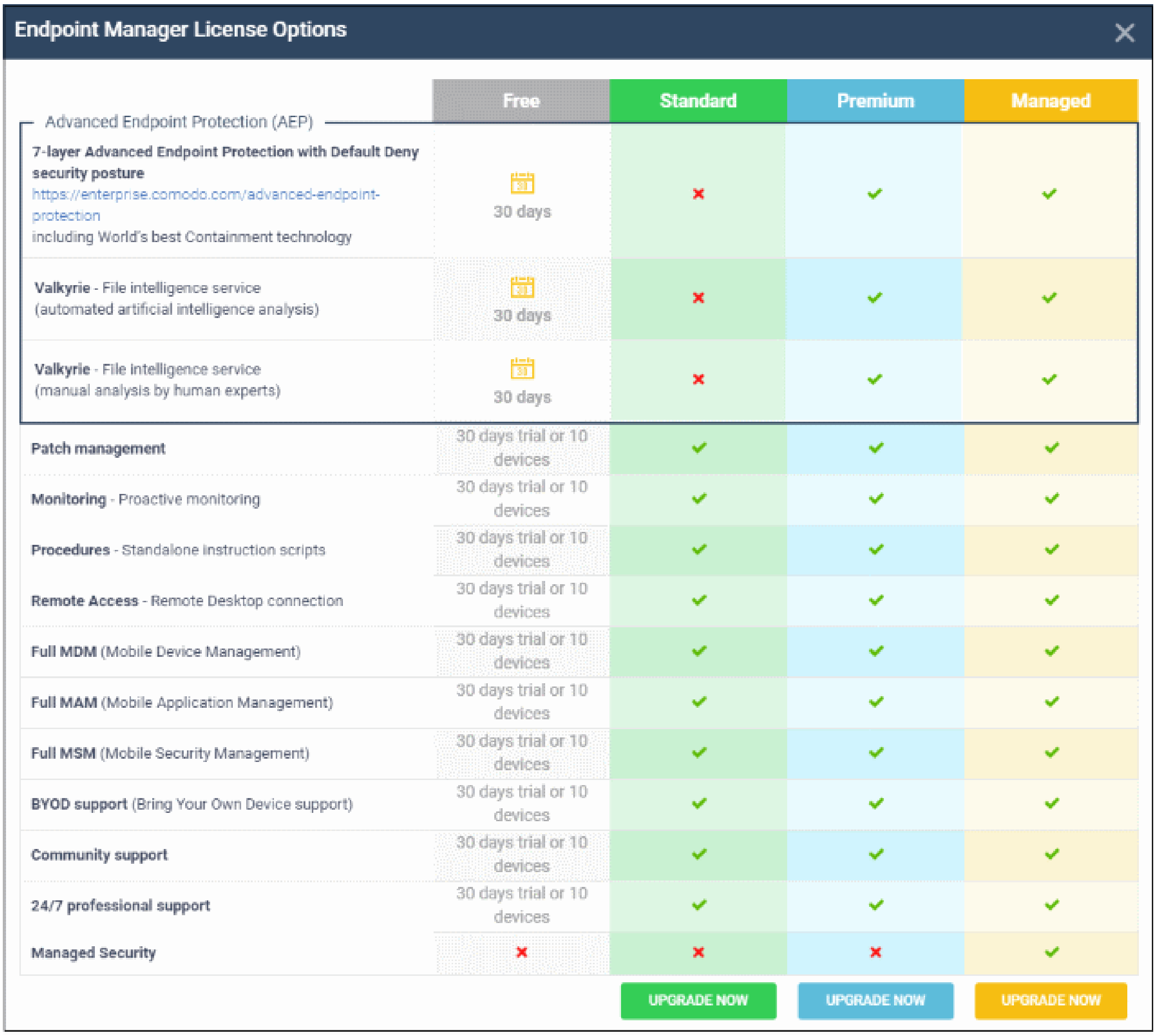
## Renew a License

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Select the license and click 'Renew License' at the top



| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE |
|---|---|---|---|---|---|---|
| ☒ | G | 463f7e7... | Endpoint Manager + Valkyrie | 6 | 6 | |
| □ | G | 576fd2cf... | Endpoint Manager + Valkyrie | ∞ | 5 | ∞ |

The 'License Options' screen shows a comparison of available license types:



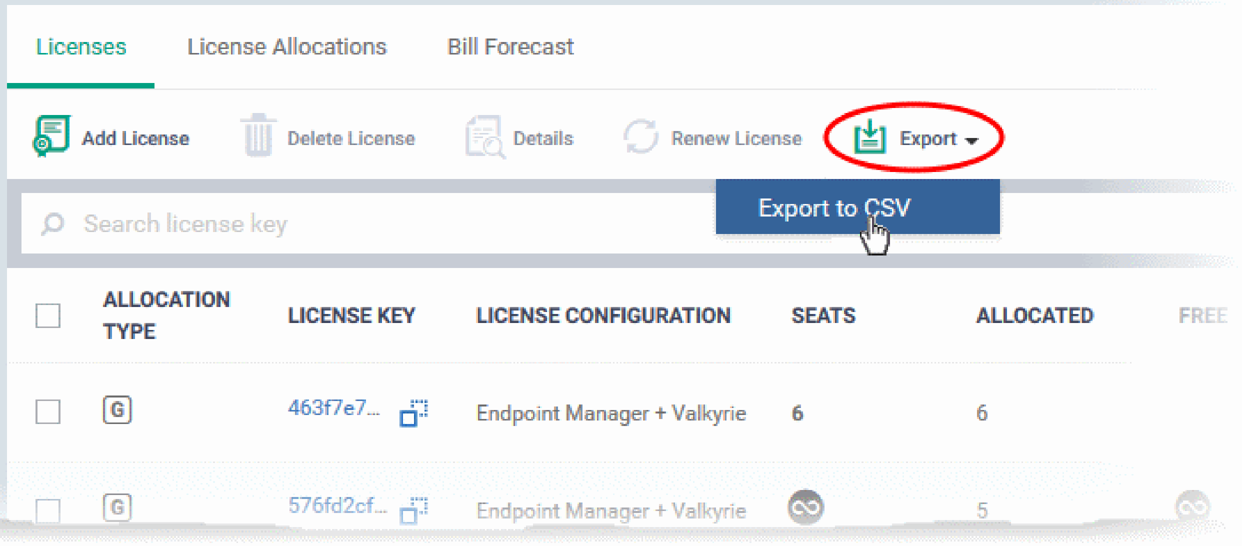
| Advanced Endpoint Protection (AEP) | Free | Standard | Premium | Managed |
|---|---|---|---|---|
| **7-layer Advanced Endpoint Protection with Default Deny security posture** https://enterprise.comodo.com/advanced-endpoint-protection including World's best Containment technology | 30 days | ✗ | ✓ | ✓ |
| **Valkyrie** - File intelligence service (automated artificial intelligence analysis) | 30 days | ✗ | ✓ | ✓ |
| **Valkyrie** - File intelligence service (manual analysis by human experts) | 30 days | ✗ | ✓ | ✓ |
| **Patch management** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Monitoring** - Proactive monitoring | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Procedures** - Standalone instruction scripts | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Remote Access** - Remote Desktop connection | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MDM** (Mobile Device Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MAM** (Mobile Application Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Full MSM** (Mobile Security Management) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **BYOD support** (Bring Your Own Device support) | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Community support** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **24/7 professional support** | 30 days trial or 10 devices | ✓ | ✓ | ✓ |
| **Managed Security** | ✗ | ✗ | ✗ | ✓ |
| | | UPGRADE NOW | UPGRADE NOW | UPGRADE NOW |

- Click 'Upgrade Now' under the license type you want.

You will be taken to the order forms to complete the purchase.

### Export the list of licenses

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button above the table then choose 'Export to CSV':



| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE |
|---|---|---|---|---|---|---|
| □ | G | 463f7e7... | Endpoint Manager + Valkyrie | 6 | 6 | |
| □ | G | 576fd2cf... | Endpoint Manager + Valkyrie | ∞ | 5 | ∞ |

- The CSV file will be available in 'Dashboard' > 'Reports'
- See **Reports** in **The Dashboard** for more details.

## 12.2. Manage License Allocation

- You can use a single license on multiple customers, or use multiple licenses on a single customer
- Make sure the license allocation type is 'Global':
    - Select the license, click 'Details' at the top then 'Edit'
    - Locate the 'Allocation type' drop-down.
    - Change the type to 'Global'

**Allocate licenses to customers**

**View license usage by customers**

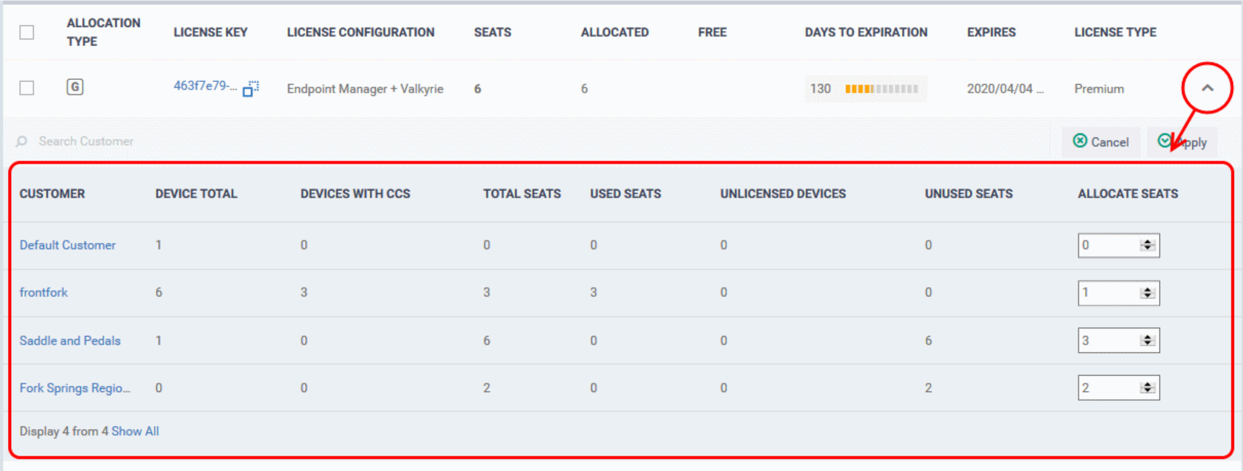
### Allocate licenses to customers

There are two ways to assign licenses to customers:

- **Method 1 - Select a license and assign it to different customers**
- **Method 2 - Select a customer and assign them licenses**

**Select a license and assign it to different customers**

- Click 'License Management' > 'License Management'
- Open the 'Licenses' tab
- Expand a license row to view your customers



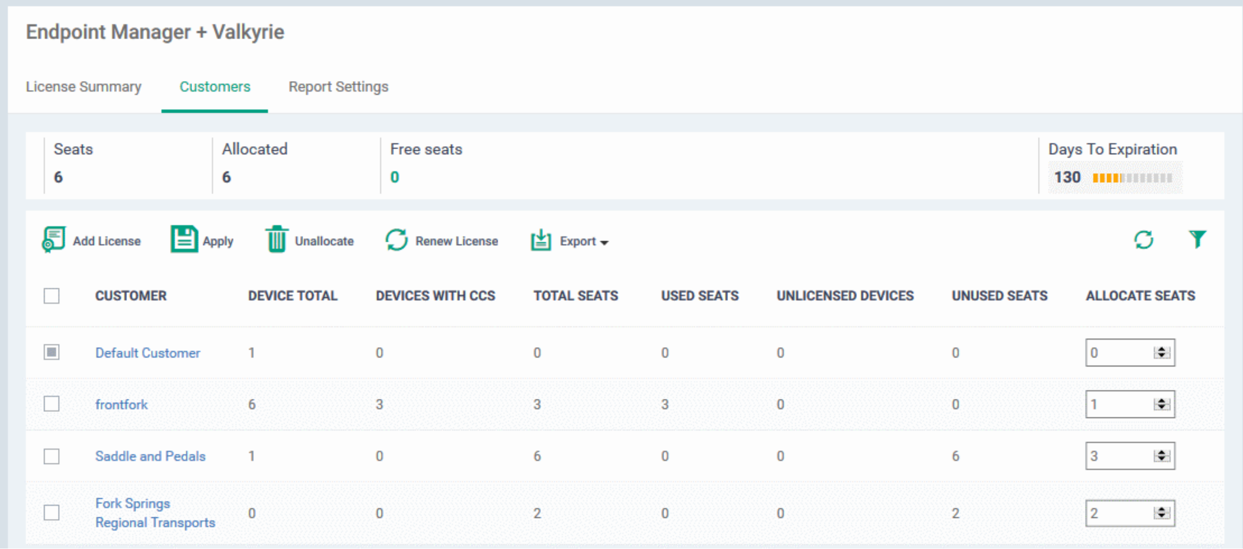
| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE | DAYS TO EXPIRATION | EXPIRES | LICENSE TYPE |
|---|---|---|---|---|---|---|---|---|---|
| □ | G | 463f7e79-... | Endpoint Manager + Valkyrie | 6 | 6 | | 130 | 2020/04/04 ... | Premium |

| CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS | ALLOCATE SEATS |
|---|---|---|---|---|---|---|---|
| Default Customer | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| frontfork | 6 | 3 | 3 | 3 | 0 | 0 | 1 |
| Saddle and Pedals | 1 | 0 | 6 | 0 | 0 | 6 | 3 |
| Fork Springs Regio... | 0 | 0 | 2 | 0 | 0 | 2 | 2 |

Display 4 from 4 Show All

OR

- Select a license then click 'Details' > Click the 'Customers' tab



Endpoint Manager + Valkyrie

Seats 6 | Allocated 6 | Free seats 0 | Days To Expiration 130

| □ | CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS | ALLOCATE SEATS |
|---|---|---|---|---|---|---|---|---|
| ☒ | Default Customer | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | frontfork | 6 | 3 | 3 | 3 | 0 | 0 | 1 |
| □ | Saddle and Pedals | 1 | 0 | 6 | 0 | 0 | 6 | 3 |
| □ | Fork Springs Regional Transports | 0 | 0 | 2 | 0 | 0 | 2 | 2 |

### Allocate seats to a customer

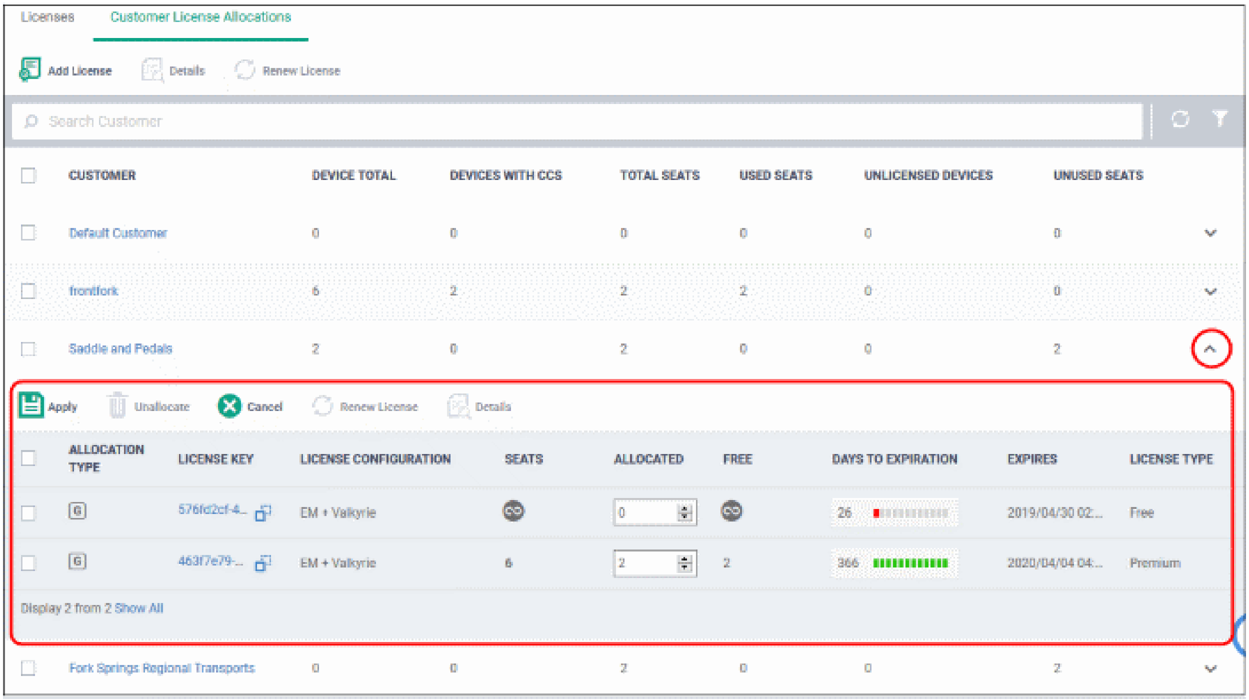
- Type a number in the 'Allocate seats' box next to a customer to assign seats to them.
- Click 'Apply'
- Make sure enough free seats are available on the license.

### Remove seats from customer

- Select a customer and click 'Unallocate'.

## Allocate seats from multiple licenses to a customer

- Click 'License Management' > 'License Management'
- Click the 'License Allocations' tab
- Click the down-arrows on the right to view all licenses assigned to a customer



| □ | CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS |
|---|---|---|---|---|---|---|---|
| □ | Default Customer | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | frontfork | 6 | 2 | 2 | 2 | 0 | 0 |
| □ | Saddle and Pedals | 2 | 0 | 2 | 0 | 0 | 2 |

| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE | DAYS TO EXPIRATION | EXPIRES | LICENSE TYPE |
|---|---|---|---|---|---|---|---|---|---|
| □ | G | 576fd2cf-4... | EM + Valkyrie | ∞ | 0 | ∞ | 26 | 2019/04/30 02:... | Free |
| □ | G | 463f7e79-... | EM + Valkyrie | 6 | 2 | 2 | 366 | 2020/04/04 04:... | Premium |

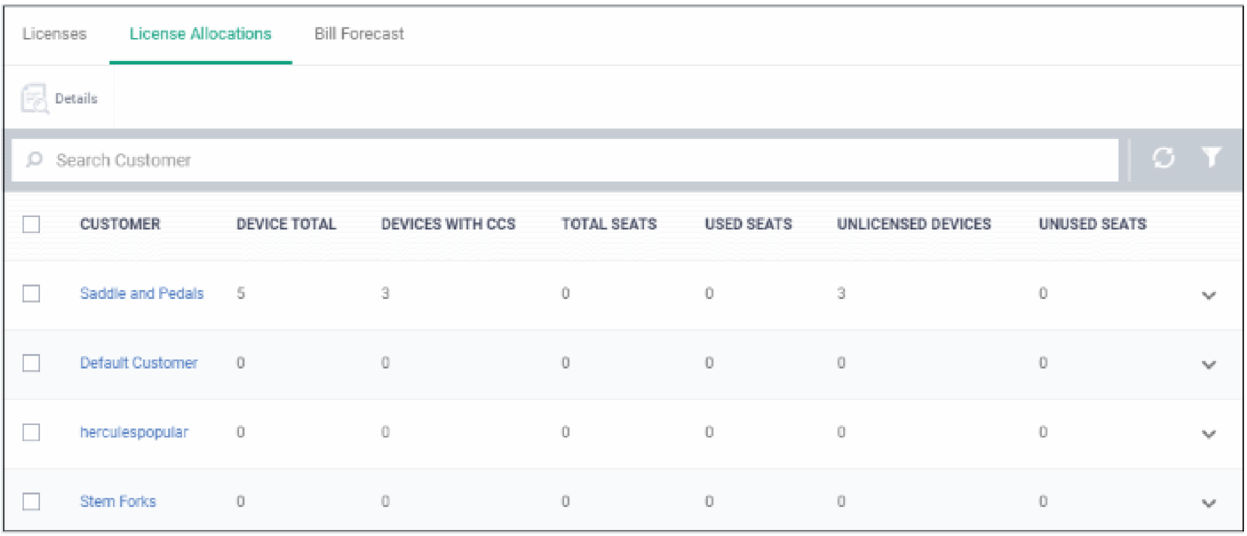
Display 2 from 2 Show All

| □ | CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS |
|---|---|---|---|---|---|---|---|
| □ | Fork Springs Regional Transports | 0 | 0 | 2 | 0 | 0 | 2 |

- Type a number in the 'Allocate seats' box to assign seats from a specific license.
- Click 'Apply'

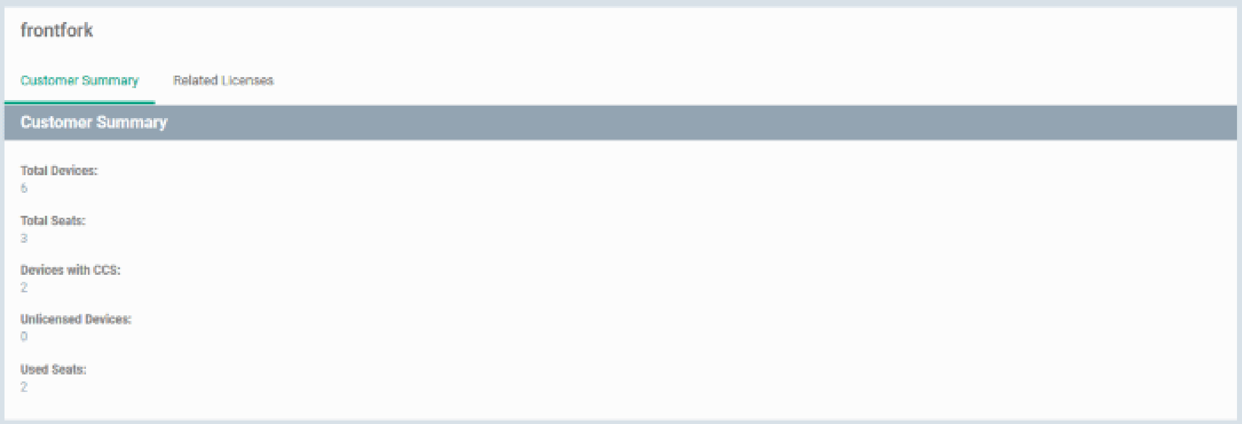
## View license usage

- Click 'License Management' > 'License Management'
- Open the 'License Allocations' tab



| □ | CUSTOMER | DEVICE TOTAL | DEVICES WITH CCS | TOTAL SEATS | USED SEATS | UNLICENSED DEVICES | UNUSED SEATS |
|---|---|---|---|---|---|---|---|
| □ | Saddle and Pedals | 5 | 3 | 0 | 0 | 3 | 0 |
| □ | Default Customer | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | herculespopular | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | Stem Forks | 0 | 0 | 0 | 0 | 0 | 0 |

- Click a customer name to open their details screen:



frontfork

Customer Summary | Related Licenses

**Customer Summary**

Total Devices:
6

Total Seats:
3

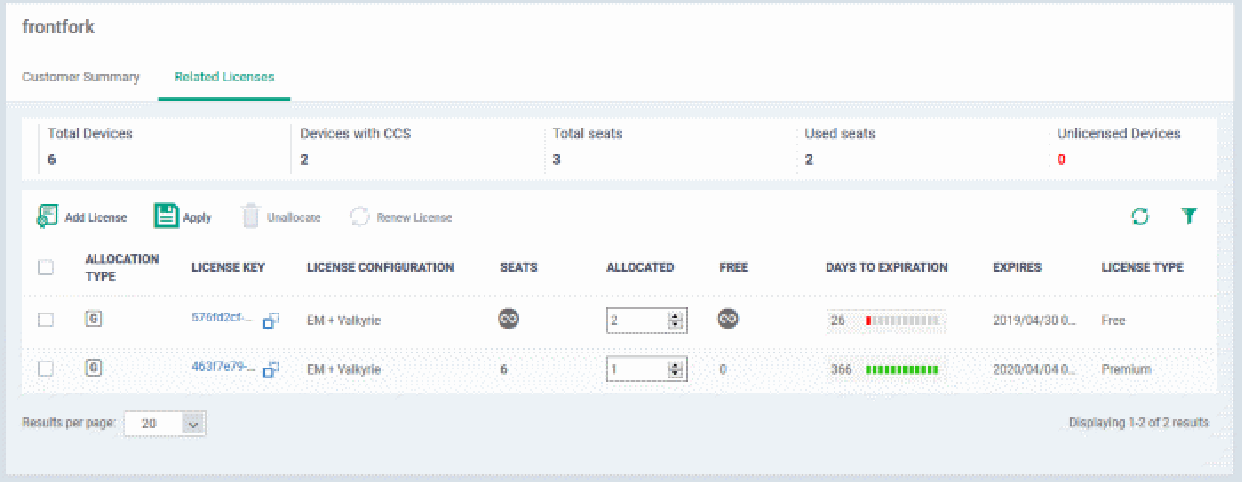
Devices with CCS:
2

Unlicensed Devices:
0

Used Seats:
2

This interface has two tabs:

- **Customer Summary** - Overall licensing information about the company.
- **Related Licenses** - Details of seat allocation from different licenses.



frontfork

Customer Summary | Related Licenses

| Total Devices | Devices with CCS | Total seats | Used seats | Unlicensed Devices |
|---|---|---|---|---|
| 6 | 2 | 3 | 2 | 0 |

| □ | ALLOCATION TYPE | LICENSE KEY | LICENSE CONFIGURATION | SEATS | ALLOCATED | FREE | DAYS TO EXPIRATION | EXPIRES | LICENSE TYPE |
|---|---|---|---|---|---|---|---|---|---|
| □ | G | 576fd2cf-... | EM + Valkyrie | ∞ | 2 | ∞ | 26 | 2019/04/30 0... | Free |
| □ | G | 463f7e79-... | EM + Valkyrie | 6 | 1 | 0 | 366 | 2020/04/04 0... | Premium |

Results per page: 20

Displaying 1-2 of 2 results

- You can allocate / remove seats as explained **above**.

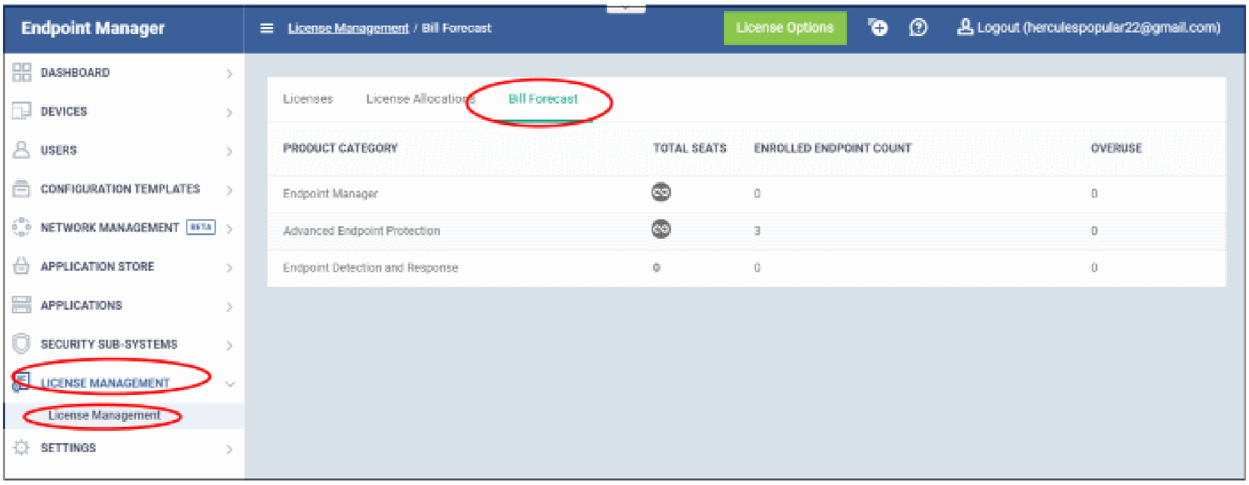
## 12.3. Bill Forecast

- Click 'License Management' > 'License Management' > 'Bill Forecast'

The bill forecast area summarizes license usage on your account.

- **Total seats -** The number of licensed seats you have available per-product, across all licenses.
- **Enrolled Endpoints -** The number of devices you have enrolled in each product category. Here are the conditions under which a device is classed as 'enrolled' for each category:
  - **Endpoint Manager -** Device has the communication client (CCC) installed, but not the security client (CCS) or Endpoint Detection and Response (EDR) client.
  - **Advanced Endpoint Protection -** Device has CCS installed.
  - **Endpoint Detection and Response -** Device has the EDR client installed.

  If a device has both the CCS and EDR clients installed, it will be added to the counts for both products.
- **Overuse -** The number of unlicensed endpoints. You will need to purchase licenses for unlicensed endpoints.



| PRODUCT CATEGORY | TOTAL SEATS | ENROLLED ENDPOINT COUNT | OVERUSE |
|---|---|---|---|
| Endpoint Manager | ∞ | 0 | 0 |
| Advanced Endpoint Protection | ∞ | 3 | 0 |
| Endpoint Detection and Response | 0 | 0 | 0 |

| | |
|---|---|
| Product Category | Product name. |
| Total Seats | The number of licenses you have available for deployment for the product.<br>• An infinity symbol indicates a free license with unlimited seats. |
| Enrolled Endpoint Count | Devices count as enrolled for each category as follows:<br>**Endpoint Manager -** Devices that only have CCC installed. These are 'manage only' devices that do not have the security or EDR clients installed.<br>**Advanced Endpoint Protection (AEP) -** Devices that have Comodo Client Security installed.<br>**Endpoint Detection and Response (EDR) -** Devices that have the EDR client installed.<br>A device that has both the EDR and CCS clients will count as an enrolled device in both the AEP and EDR columns. |
| Overuse | Number of endpoints over your licensed limit. Some scenarios:<br>**Endpoint Manager-** You can add more endpoints than covered by your licenses, but we will charge you for the excess.<br>• We will bill you for the additional devices on the last day of the month.<br>• We will block the additional devices if no payment is received within 14 days.<br>**AEP -** All endpoints must be licensed or CCS is disabled on all devices.<br>• If you deployed CCS in bulk then any excess endpoints are shown here.<br>• You have to purchase licenses for the excess devices or security functionality is disabled for *all* devices.<br>• Alternatively, you can remove CCS from the excess devices.<br>**EDR -** You must purchase licenses beforehand. You cannot deploy EDR on more devices than allowed by your license. There is no bulk installation option for EDR as of now. |

# Appendix 1a: Endpoint Manager Services - IP Nos, Host Names and Port Details - EU Customers

**Note**: This page contains information for customers located in Europe. **Click here** to see USA information instead.

- Endpoint Manager communicates with Comodo servers and your devices to issue commands, run virus scans, deploy updates and more.
- You need to configure your firewall accordingly to allow these connections.
- All client to server communications are encrypted over https connections using the strongest TLS protocols, RSA 2048 bit keys and SHA 256 algorithms.
- The tables on this page show firewall requirements for the following Comodo services:
    - **Communication Client (CC)**
    - **Comodo Client - Security (CCS)**
    - **Endpoint Manager Server (on premise installations)**
    - **Remote Control sessions**
        - ***Remote Control Direct connection***
        - ***Remote Control Peer to Peer connection***
        - ***Remote Control Relay connection***
    - **Diagnostic Tools**
    - **All settings grouped by port**

**Communication Client (CC)**

| Communication Client (CC) | | | | | |
|---|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** | **Criticality and notes** |
| CC | Communication between device and EM server | subdomain.cmdm.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Mandatory |
| Enrollment | To get client certificates | mdmsupport.comodo.com (up to CCC 6.29)<br>mdmsupport.cmdm.comodo.com (CCC 6.30+) | 54.93.214.133 | 443 | Mandatory |
| Monitoring and alerts | Access to Monitoring and alerts server | plugins.cmdm.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Mandatory |

| | | | | | |
|---|---|---|---|---|---|
| File rating management | Access to Local Verdict Server | subdomain.cmdm.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Optional<br>This is for reporting data from CCS |
| Windows push service (XMPP) | Device communication (push messages) | xmpp.cmdm.comodo.com | 18.196.138.4<br>18.197.8.210 | 443 | Mandatory |
| LDAP synchronization | Synchronization with LDAP via device | User's LDAP server host | User's LDAP server IP | 389<br>636 (LDAPS) | Optional<br>For LDAP sync via device only. Related to<br>Device to LDAP server connections only |
| SSO | Single Sign On | one.comodo.com | Dynamic (Amazon load balancing) | 443 | Mandatory |
| Client Security installation | Download and install/upgrade Client Security agent.<br>Requests to download.comodo.com are redirected to<br>cdn.download.comodo.com which is managed by<br>The CDN provider, and those IP addresses can change | download.comodo.com | 178.255.82.5 | 443, 80 | Optional<br>For CCS installation/upgrade only |
| | | cdn.download.comodo.com | Cloudflare's IP range:<br>104.37.182.3 | 443, 80 | |
| OCSP | Client certificate revocation checking | http://ocsp.comodoca.com/ | Dynamic load balancing | 80 | Optional<br>For mobile devices only.<br>The Windows client does not perform OCSP checks. |
| CRL | Client certificate revocation checking | http://crl.comodoca.com/ | Dynamic load balancing | 80 | Optional<br>For mobile devices only.<br>The Windows client does not perform CRL checks. |
| 3rd Party Patch Management | 3rd party applications updates | patchportal.one.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Optional<br>For 3rd party software updates only |
| Telemetry | Sending telemetry data for analysis | cescollector.cwatchapi.com | Dynamic<br>(Amazon load balancing) | 443 | Optional |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Local distribution of packages | Distribute different types of updates via local network | Local hostname | Local IP | 6881, 6882 | Optional. Used for updates distribution locally by torrent principle. Ports are bound by EM Service. 6882 is used if 6881 is in use already. |

**Comodo Client - Security (CCS)**

| Comodo Client - Security (CCS) |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** | **Protocol** | **Criticality and notes** |
| FLS | FLS lookup | fls.security.comodo.com | 199.66.201.16 | 4447 (optional), 53 | UDP | Mandatory - choose *either* UDP or TCP for FLS<br>UDP is the main, preferred FLS lookup channel<br>53 - Default port.<br>4447 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open. |
|  | FLS lookup | fls.security.comodo.com | 199.66.201.16 | 4448 (optional), 80 | TCP | Mandatory - choose *either* UDP or TCP for FLS<br>TCP is the reserve FLS lookup channel.<br>80 - Default port<br>4448 - Reserve port. Can be specified manually in profile. At least one of the two ports must be open |
| Valkyrie | Valkyrie lookup | valkyrie.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Optional<br>Valkyrie lookup is currently disabled on CCS,<br>CCS gets Valkyrie verdicts from LVS. |
|  | Submit to Valkyrie | valkyrie.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Mandatory |
| cdn.download.comodo.com | Update / upgrade mirror | cdn.download.comodo.com | Cloudflare's IP range:<br>104.37.182.3 | 80 | HTTP | Mandatory |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | cdn.download.comodo.com | Cloudflare's IP range:<br>104.37.182.3 | 443 | HTTPS | |
| download.comodo.com | Update/upgrade.<br>Requests to download.comodo.com are redirected to<br>cdn.download.comodo.com which is managed by<br>The CDN provider, and those IP addresses can change | download.comodo.com | 178.255.82.5 | 80 | HTTP | Mandatory |
| | | download.comodo.com | 178.255.82.5 | 443 | HTTPS | |
| LVS | Download the EM verdicts database | s3.eu-central-1.amazonaws.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Mandatory |
| | LVS lookup | subdomain.cmdm.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | |
| OCSP | Client certificate revocation checking | http://ocsp.comodoca.com/ | Dynamic load balancing | 80 | - | Optional<br>CCS does not perform CRL checking yet |
| CRL | Client certificate revocation checking | http://crl.comodoca.com/ | Dynamic load balancing | 80 | - | Optional<br>CCS does not perform CRL checking yet |
| Telementry | Sending telemetry data for analysis | tel.security.comodo.com | 159.203.65.195 | 261 | HTTPS | |
| FLEVEN | Sending telemetry data for analysis | cis.td.security.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | |
| CWATCH | Sending telemetry data for analysis | api.mssp.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | |

**Endpoint Manager Server** (on premise installation)

| Endpoint Manager Server (on premise) | | | | |
|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** |
| E-mail | Connection to the configured SMTP server for e-mail | SMTP server hostname | SMTP server IP | 25 |

| | | | | |
|---|---|---|---|---|
| | sending | | | |
| LDAP synchronization | Direct synchronization with LDAP | User's LDAP server host | User's LDAP server IP | 389<br>636 (LDAPS) |
| Connection to Comodo Accounts Manager | License verification | https://accounts.comodo.com | 178.255.85.140 | 443 |
| Google Cloud Messaging | To push messages | https://android.googleapis.com/gcm/send | Dynamic | 443 |
| Local Verdict Server | File rating management | EM server hostname | EM server IP | 443 |

### Remote Control

| Remote Control | | | | | | |
|---|---|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** | **Protocol** | **Criticality and notes** |
| XMPP | Remote Control Session (with new version of Comodo RC* | xmpp.cmdm.comodo.com | 18.196.138.4<br>18.197.8.210 | 443 | HTTPS | Mandatory for both RC host and target device |
| STUN server | To receive possible network configuration, external ip etc. | stun.l.google.com | Dynamic | 19302 | UDP | Mandatory for both RC host and target device for peer-to-peer and relay connections. |
| Direct connection | Establish direct connection between RC and target device. | - | IP of the RC host AND target host | Local port range specified in profile.<br>Win7+/MacOS. Default port range= 49152 - 65535<br>WinXP/2003. Default port range = 1025-5000 | UDP | Mandatory for both RC host and target device |
| Peer-to-peer connection | Establish peer-to-peer connection RC and target device. | - | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | UDP | Mandatory for both RC host and target device for peer-to-peer connections. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Relay connection | Establish relay connection between RC and target device. | - | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478, 49152 - 65535 | UDP | Mandatory for both RC host and target device for relay connections. |

***Remote Control - Direct connection by traffic direction ****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP 1 | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | Local IP 2 | local port range specified in profile (Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | UDP |

| Incoming Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP 2 | local port range specified in profile (Win7+/MacOS default port range: 49152 - 65535) (WinXP/2003 default port range: 1025-5000) | Local IP 1 | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535) (WinXP/2003 default port range: 1025-5000) | UDP |

* - applies to both sides - RC host and target

***Remote Control - Peer to Peer Connection by traffic direction ****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | UDP |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535)(WinXP/2003 default port range: 1025-5000) | stun.l.google.com | 19302 | |

| Incoming Traffic | | |
|---|---|---|
| Source | Destination | Protocol |

| | | | | |
|---|---|---|---|---|
| IP | Port | IP | Port | |
| 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | UDP |
| stun.l.google.com | 19302 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535)(WinXP/2003 default port range: 1025-5000) | |

* - applies to both sides - RC host and target

***Remote Control - Relay connection by traffic direction****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478,<br>49152 - 65535 | UDP |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535)(WinXP/2003 default port range: 1025-5000) | stun.l.google.com | 19302 | |

| Incoming Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478,<br>49152 - 65535 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | UDP |
| stun.l.google.com | 19302 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | |

- - applies to both sides - RC host and target

**Diagnostic Tools**

| Diagnostic Tools |
|---|

| Service | Purpose | Hostname | IP | Port | Critically and notes |
|---|---|---|---|---|---|
| CCS Report Tool | Collect event logs to help more effectively troubleshoot issues. | c1report.comodo.com | 178.255.85.136 | 22 | Optional. For manual log uploads |

**All settings grouped by port**

This table contains the same information as the other four tables on this page but with services grouped by port number.

| Settings Grouped by Port | | | | | |
|---|---|---|---|---|---|
| **Port** | **Service** | **IP** | **URL / Hostname** | **Protocol** | **Component** |
| 443 | CC | Dynamic (Amazon load balancing) | subdomain.cmdm.comodo.com | HTTPS | Communication Client |
| | Enrollment | 54.93.214.133 | mdmsupport.comodo.com | HTTPS | |
| | Monitoring and alerts | Dynamic (Amazon load balancing) | plugins.cmdm.comodo.com | HTTPS | |
| | File rating management | Dynamic (Amazon load balancing) | subdomain.cmdm.comodo.com | HTTPS | |
| | Windows push service (XMPP) | 18.196.138.4<br>18.197.8.210 | xmpp.cmdm.comodo.com | HTTPS | |
| | SSO | 69.4.89.244 | one.comodo.com | HTTPS | |
| | 3rd party patch management | Dynamic<br>(Amazon load balancing) | patchportal.one.comodo.com | HTTPS | |
| | Client Security installation | 178.255.82.5 | download.comodo.com | HTTPS | |
| | | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |

| | | | | | |
|---|---|---|---|---|---|
| | Telemetry | Dynamic (Amazon load balancing) | cescollector.cwatchapi.com | HTTPS | |
| | Valkyrie | 178.255.87.4 | valkyrie.comodo.com | HTTPS | Comodo Client Security |
| | FLEVEN | Dynamic (Amazon load balancing) | cis.td.security.comodo.com | HTTPS | |
| | CWATCH | Dynamic (Amazon load balancing) | api.mssp.comodo.com | HTTPS | |
| | Update/upgrade.<br>Requests to download.comodo.com are redirected to<br>cdn.download.comodo.com which is managed by<br>The CDN provider, and those IP addresses can change | 178.255.82.5 | download.comodo.com | HTTPS | |
| | Updates/upgrades mirror | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | LVS | Dynamic (Amazon load balancing) | s3.eu-central-1.amazonaws.com | HTTPS | |
| | | Dynamic (Amazon load balancing) | subdomain.cmdm.comodo.com | HTTPS | |
| | License verification | 178.255.85.140 | accounts.comodo.com | HTTPS | EM server (on premise) |
| | Google cloud messaging | Dynamic | android.googleapis.com/gcm/send | HTTPS | |
| | Apple push notifications | Dynamic | gateway.push.apple.com | HTTPS | |
| | Local Verdict Server | EM server IP | EM server | HTTPS | |

| | | | | | |
|---|---|---|---|---|---|
| | | | hostname | | |
| | XMPP | 18.196.138.4<br>18.197.8.210 | xmpp.cmdm.comodo.com | HTTPS | Remote Control |
| 80 | Client Security installation | 178.255.82.5 | download.comodo.com | HTTPS | Communication Client |
| | | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | OCSP | Dynamic load balancing | http://ocsp.comodoca.com/ | HTTPS | |
| | CRL | Dynamic load balancing | http://crl.comodoca.com/ | HTTPS | |
| | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | HTTPS | Comodo Client Security |
| | Update/upgrade.<br>Requests to download.comodo.com are redirected to<br>cdn.download.comodo.com which is managed by<br>The CDN provider, and those IP addresses can change | 178.255.82.5 | download.comodo.com | HTTPS | |
| | Updates/upgrades mirror | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | OCSP | Dynamic load balancing | http://ocsp.comodoca.com/ | HTTPS | |
| | CRL | Dynamic load balancing | http://crl.comodoca.com/ | HTTPS | |
| | Apple push notifications | Dynamic | gateway.push.apple.com | HTTPS | EM server (on premise) |

| | | | | | |
|---|---|---|---|---|---|
| 22 | CCS Report Tool | 178.255.85.136 | c1report.comodo.com | SSH | Comodo Client Security |
| 25 | Email | SMTP server IP | SMTP server hostname | SMTP | EM server (on premise) |
| 53 | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 4447 (Optional) | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 4448 (Optional) | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 389 | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | - | Communication Client |
| | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | - | EM server (on premise) |
| 636 | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | - | Communication Client |
| | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | - | EM server (on premise) |
| 2195 | Apple push notifications | Dynamic | gateway.push.apple.com | - | EM server (on premise) |
| 261 | Telementry | 159.203.65.195 | tel.security.comodo.com | HTTPS | Comodo Client Security |
| 6881, 6882 | Local distribution of packages | Local IP | Local hostname | HTTPS | Communication Client |
| 2196 | Apple push notifications | Dynamic | gateway.push.apple.com | - | EM server (on premise) |
| 19302 | STUN server | Dynamic (Amazon load balancing) | stun.l.google.com | UDP | Remote Control tool |
| Win7+/MacOS. Default port range = 49152 - 65535<br>WinXP/2003. Default port range = 1025-5000 | Direct connection | IP of the RC host AND target host | N/A | UDP | |
| 3478 | Peer-to-peer | 18.196.107.208 | - | UDP | |

| | | | | | |
|---|---|---|---|---|---|
| | connection | 52.29.123.206<br>34.232.133.48<br>18.208.23.45 | | | |
| 3478, 49152 - 65535 | Relay connection | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | - | UDP | |

# Appendix 1b: Endpoint Manager Services - IP Nos, Host Names and Port Details - US Customers

**Note**: This page contains information for customers located in the USA. **Click here** to see Europe information instead.

- Endpoint Manager communicates with Comodo servers and your devices to issue commands, run virus scans, deploy updates and more.
- You need to configure your firewall accordingly to allow these connections.
- All client to server communications are encrypted over https connections using the strongest TLS protocols, RSA 2048 bit keys and SHA 256 algorithms.
- The tables on this page show firewall requirements for the following Comodo services:
    - **Communication Client (CC)**
    - **Comodo Client - Security (CCS)**
    - **Endpoint Manager Server (on premise installations)**
    - **Remote Control sessions**
        - ***Remote Control Direct connection***
        - ***Remote Control Peer to Peer connection***
        - ***Remote Control Relay connection***
    - **Diagnostic Tools**
    - **All settings grouped by port**

**Communication Client (CC)**

| Communication Client (CC) |
|---|

| Service | Purpose | Hostname | IP | Port | Criticality and notes |
|---|---|---|---|---|---|
| CC | Communication between device and EM server | subdomain.itsm-us1.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Mandatory |
| Enrollment | To get client certificates | mdmsupport.comodo.com (up to CCC 6.29)<br>mdmsupport.cmdm.comodo.com<br>(CCC 6.30+)<br>mdmsupport.itsm-us1.comodo.com<br>(CCC 6.30+) | 54.93.214.133 | 443 | Mandatory |
| Monitoring and alerts | Access to Monitoring and alerts server | plugins.itsm-us1.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Mandatory |
| File rating management | Access to Local Verdict Server | subdomain.itsm-us1.comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Optional<br>This is for reporting data from CCS |
| Windows push service (XMPP) | Device communication (push messages) | xmpp.itsm-us1.comodo.com | 34.193.74.83<br>54.163.100.185 | 443 | Mandatory |
| LDAP synchronization | Synchronization with LDAP via device | User's LDAP server host | User's LDAP server IP | 389<br>636 (LDAPS) | Optional<br>For LDAP sync via device only. Related to<br>Device to LDAP server connections only |
| SSO | Single Sign On | one-us.comodo.com | Dynamic (Amazon load balancing) | 443 | Mandatory |
| Client Security installation | Download and install/upgrade Client Security agent. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP | download.comodo.com | 178.255.82.5 | 443, 80 | Optional<br>For CCS installation/upgrade only |
| | | cdn.download.comodo.com | Cloudflare's IP range:<br>104.37.182.3 | | |

| | | | | | |
|---|---|---|---|---|---|
| | addresses can change. | | | | |
| OCSP | Client certificate revocation checking | http://ocsp.comodoca.com/ | Dynamic load balancing | 80 | Optional<br>For mobile devices only.<br>The Windows client does not perform OCSP checks. |
| CRL | Client certificate revocation checking | http://crl.comodoca.com/ | Dynamic load balancing | 80 | Optional<br>For mobile devices only.<br>The Windows client does not perform CRL checks. |
| 3rd Party Patch Management | 3rd party applications updates | patchportal.one-us.<br>comodo.com | Dynamic<br>(Amazon load balancing) | 443 | Optional<br>For 3rd party software updates only |
| Telemetry | Sending telemetry data for analysis | cescollector.cwatchapi.com | Dynamic (Amazon load balancing) | 443 | Optional |
| Local distribution of packages | Distribute different types of updates via local network | Local hostname | Local IP | 6881, 6882 | Optional. Used for updates distribution locally by torrent principle. Ports are bound by EM Service. 6882 is used if 6881 is in use already. |

**Comodo Client - Security (CCS)**

| Comodo Client - Security (CCS) | | | | | | |
|---|---|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** | **Protocol** | **Criticality and notes** |
| FLS | FLS lookup | fls.security.comodo.com | 199.66.201.16 | 4447 (optional), 53 | UDP | Mandatory - choose *either* UDP or TCP for FLS<br>UDP is the main, preferred FLS lookup channel<br>53 - Default port.<br>4447 - Reserve port. Can be specified manually in profile.<br>At least one of the two ports must be open. |
| | FLS lookup | fls.security.comodo.com | 199.66.201.16 | 4448 (optional), | TCP | Mandatory - choose *either* UDP or TCP for |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | 80 | | FLS<br>TCP is the reserve FLS lookup channel.<br>80 - Default port<br>4448 - Reserve port.<br>Can be specified manually in profile.<br>At least one of the two ports must be open |
| Valkyrie | Valkyrie lookup | valkyrie.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Optional<br>Valkyrie lookup is currently disabled on CCS,<br>CCS gets Valkyrie verdicts from LVS. |
| | Submit to Valkyrie | valkyrie.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Mandatory |
| cdn.download.comodo.com | Update / upgrade mirror | cdn.download.comodo.com | Cloudflare's IP range: 104.37.182.3 | 80 | HTTP | Mandatory |
| | | cdn.download.comodo.com | Cloudflare's IP range: 104.37.182.3 | 443 | HTTPS | |
| download.comodo.com | Update/upgrade. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change | download.comodo.com | 178.255.82.5 | 80 | HTTP | Mandatory |
| | | download.comodo.com | 178.255.82.5 | 443 | HTTPS | Mandatory |
| LVS | Download the EM verdicts database | s3.us-east-1.amazonaws.com | Dynamic (Amazon load balancing) | 443 | HTTPS | Mandatory |
| | LVS lookup | subdomain.itsm-us1.comodo.com | Dynamic (Amazon load balancing) | 443 | HTTPS | |
| OCSP | Client certificate revocation checking | *http://ocsp.comodoca.com/* | Dynamic load balancing | 80 | - | Optional<br>CCS does not perform CRL checking yet |
| CRL | Client certificate | http://crl.co | Dynamic load | 80 | - | Optional |

| | | | | | | |
|---|---|---|---|---|---|---|
| | revocation checking | modoca.com/ | balancing | | | CCS does not perform CRL checking yet |
| Telementry | Sending telemetry data for analysis | tel.security.comodo.com | 159.203.65.195 | 261 | - | |
| FLEVEN | Sending telemetry data for analysis | cis.td.security.comodo.com | Dynamic (Amazon load balancing) | 443 | - | |
| CWATCH | Sending telemetry data for analysis | cis.td.security.comodo.com | Dynamic (Amazon load balancing) | 443 | - | |

**Endpoint Manager Server** (on premise installation)

| Endpoint Manager Server (on premise) | | | | |
|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** |
| E-mail | Connection to the configured SMTP server for e-mail sending | SMTP server hostname | SMTP server IP | 25 |
| LDAP synchronization | Direct synchronization with LDAP | User's LDAP server host | User's LDAP server IP | 389<br>636 (LDAPS) |
| Connection to Comodo Accounts Manager | License verification | https://accounts.comodo.com | 178.255.85.140 | 443 |
| Google Cloud Messaging | To push messages | https://android.googleapis.com/gcm/send | Dynamic | 443 |
| Local Verdict Server | File rating management | EM server hostname | EM server IP | 443 |

**Remote Control**

| Remote Control | | | | | | |
|---|---|---|---|---|---|---|
| **Service** | **Purpose** | **Hostname** | **IP** | **Port** | **Protocol** | **Criticality and notes** |
| XMPP | Remote Control Session (with new version of Comodo RC* | xmpp.itsm-us1.comodo.com | 34.193.74.83<br>54.163.100.185 | 443 | HTTPS | Mandatory for both RC host and target device |
| STUN server | To receive possible network configuration, external ip etc. | stun.l.google.com | Dynamic | 19302 | UDP | Mandatory for both RC host and target device for peer-to-peer and relay connections. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Direct connection | To establish direct or relay connection between RC and target device. | - | | 1025 - 65535 | UDP | Mandatory for both RC host and target device |
| Direct connection | Establish direct connection between RC and target device. | - | IP of the RC host AND target host | Local port range specified in profile.<br>Win7+/Mac OS. Default port range= 49152 - 65535<br>WinXP/2003. Default port range = 1025-5000 | UDP | Mandatory for both RC host and target device |
| Peer-to-peer connection | Establish peer-to-peer connection RC and target device. | - | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | UDP | Mandatory for both RC host and target device for peer-to-peer connections. |
| Relay connection | Establish relay connection between RC and target device. | - | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478, 49152 - 65535 | UDP | Mandatory for both RC host and target device for relay connections. |

***Remote Control - Direct connection by traffic direction ****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP 1 | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | Local IP 2 | local port range specified in profile (Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | UDP |

| Incoming Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |

|  |  |  |  |  |
|---|---|---|---|---|
| Local IP 2 | local port range specified in profile (Win7+/MacOS default port range: 49152 - 65535)<br>(WinXP/2003 default port range: 1025-5000) | Local IP 1 | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)<br>(WinXP/2003 default port range: 1025-5000) | UDP |

* - applies to both sides - RC host and target.

***Remote Control - Peer to Peer Connection by traffic direction ****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | UDP |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535)(WinXP/2003 default port range: 1025-5000) | stun.l.google.com | 19302 | |

| Incoming Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 - 65535)(WinXP/2003 default port range: 1025-5000) | UDP |
| stun.l.google.com | 19302 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535)(WinXP/2003 default port range: 1025-5000) | |

* - applies to both sides - RC host and target.

***Remote Control - Relay Connection by traffic direction****

| Outgoing Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478,<br>49152 - 65535 | UDP |

| | | | | |
|---|---|---|---|---|
| | 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | | | |
| Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | stun.l.google.com | 19302 | UDP |

| Incoming Traffic | | | | |
|---|---|---|---|---|
| Source | | Destination | | Protocol |
| IP | Port | IP | Port | |
| 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | 3478,<br>49152 - 65535 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | UDP |
| stun.l.google.com | 19302 | Local IP | local port range specified in profile(Win7+/MacOS default port range: 49152 — 65535) (WinXP/2003 default port range: 1025-5000) | UDP |

* - applies to both sides - RC host and target.

### Diagnostic Tools

| Diagnostic Tools | | | | | |
|---|---|---|---|---|---|
| Service | Purpose | Hostname | IP | Port | Critically and notes |
| CCS Report Tool | Collect event logs to more effectively troubleshoot issues | c1report.comodo.com | 178.255.85.136 | 22 | Optional. For manual log uploads |

### All settings grouped by port

This table contains the same information as the other four tables on this page but with services grouped by port number.

| Settings Grouped by Port | | | | | |
|---|---|---|---|---|---|
| Port | Service | IP | URL / Hostname | Protocol | Component |

| | | | | | |
|---|---|---|---|---|---|
| 443 | CC | Dynamic (Amazon load balancing) | subdomain.itsm-us1.comodo.com | HTTPS | Communication Client |
| | Enrollment | 54.93.214.133 | mdmsupport.comodo.com | HTTPS | |
| | Monitoring and alerts | Dynamic (Amazon load balancing) | plugins.itsm-us1.comodo.com | HTTPS | |
| | File rating management | Dynamic (Amazon load balancing) | subdomain.itsm-us1.comodo.com | HTTPS | |
| | Windows push service (XMPP) | 34.193.74.83<br>54.163.100.185 | xmpp.itsm-us1.comodo.com | HTTPS | |
| | SSO | 69.4.89.244 | one-us.comodo.com | HTTPS | |
| | 3rd party patch management | Dynamic<br>(Amazon load balancing) | patchportal.one-us.<br>comodo.com | HTTPS | |
| | Client Security installation | 178.255.82.5 | download.comodo.com | HTTPS | |
| | | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | Telemetry | Dynamic<br>(Amazon load balancing) | cescollector.cwatchapi.com | HTTPS | |
| | Valkyrie | 178.255.87.4 | valkyrie.comodo.com | HTTPS | Comodo Client Security |
| | Update/upgrade. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change | 178.255.82.5 | download.comodo.com | HTTPS | |
| | Updates/upgrades mirror | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | FLEVEN | Dynamic<br>(Amazon load balancing) | cis.td.security.comodo.com | HTTPS | |
| | CWATCH | Dynamic | api.mssp.comodo.com | HTTPS | |

| | | | | | |
|---|---|---|---|---|---|
| | | (Amazon load balancing) | | | |
| | LVS | Dynamic (Amazon load balancing) | s3.us-east1.amazonaws.com | HTTPS | |
| | | Dynamic (Amazon load balancing) | subdomain.itsm-us1.comodo.com | HTTPS | |
| | License verification | 178.255.85.140 | accounts.comodo.com | HTTPS | EM server (on premise) |
| | Google cloud messaging | Dynamic | android.googleapis.com/gcm/send | HTTPS | |
| | Apple push notifications | Dynamic | gateway.push.apple.com | HTTPS | |
| | Local Verdict Server | EM server IP | EM server hostname | HTTPS | |
| | XMPP | 34.193.74.83<br>54.163.100.185 | xmpp.itsm-us1.comodo.com | HTTPS | Remote Control tool |
| 80 | Client Security installation | 178.255.82.5 | download.comodo.com | HTTPS | Communication Client |
| | | Cloudflare's IP range:<br>104.37.182.3 | cdn.download.comodo.com | HTTPS | |
| | OCSP | Dynamic load balancing | http://ocsp.comodoca.com/ | HTTPS | |
| | CRL | Dynamic load balancing | http://crl.comodoca.com/ | HTTPS | |
| | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | HTTPS | Comodo Client Security |
| | Update/upgrade. Requests to download.comodo.com are redirected to cdn.download.comodo.com which is managed by The CDN provider, and those IP addresses can change | 178.255.82.5 | download.comodo.com | HTTPS | |
| | Updates/upgrades mirror | Cloudflare's IP range:<br>104.16.0.0/12 | cdn.download.comodo.com | HTTPS | |
| | OCSP | Dynamic load balancing | http://ocsp.comodoca.com/ | HTTPS | |

| | | | | | |
|---|---|---|---|---|---|
| | CRL | Dynamic load balancing | http://crl.comodoca.com/ | HTTPS | |
| | Apple push notifications | Dynamic | gateway.push.apple.com | HTTPS | EM server (on premise) |
| 22 | CCS Report Tool | 178.255.85.136 | c1report.comodo.com | SSH | Comodo Client Security |
| 25 | Email | SMTP server IP | SMTP server hostname | SMTP | EM server (on premise) |
| 53 | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 4447<br>(Optional) | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 4448<br>(Optional) | FLS Lookup | 199.66.201.16 | fls.security.comodo.com | UDP | Comodo Client Security |
| 389 | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | | Communication Client |
| | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | | EM server (on premise) |
| 636 | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | | Communication Client |
| | LDAP synchronization | User's LDAP server IP | User's LDAP server IP | | EM server (on premise) |
| 2195 | Apple push notifications | Dynamic | gateway.push.apple.com | | EM server (on premise) |
| 2196 | Apple push notifications | Dynamic | gateway.push.apple.com | | EM server (on premise) |
| 6881, 6882 | Local distribution of packages | Local IP | Local hostname | HTTPS | Communication Client |
| 19302 | STUN server | Dynamic (Amazon load balancing) | stun.l.google.com | UDP | Remote Control tool |
| 261 | Telementry | 159.203.65.195 | tel.security. comodo.com | HTTPS | Comodo Client Security |
| Win7+/MacOS. Default port range = 49152 - 65535<br>WinXP/2003. Default port range = 1025-5000 | Direct connection | IP of the RC host AND target host | N/A | Win7+/MacOS. Default port range = 49152 - 65535<br>WinXP/2003. Default port range = 1025-5000 | Remote Control tool |
| 3478 | Peer-to-peer | 18.196.107.208 | - | 3478 | |

| | | | | | |
|---|---|---|---|---|---|
| | connection | 52.29.123.206<br>34.232.133.48<br>18.208.23.45 | | | |
| 3478, 49152 - 65535 | Relay connection | 18.196.107.208<br>52.29.123.206<br>34.232.133.48<br>18.208.23.45 | - | 3478, 49152 - 65535 | |

# Appendix 2 – Endpoint Manager License Types

Each Endpoint Manager license offers different levels of protection and features.

The four license types are:

- Free
- Standard
- Premium
- Managed

The following table shows the features available with each license type:

| Feature | Free | Standard | Premium | Managed |
|---|---|---|---|---|
| **Advanced Endpoint Protection** | | | | |
| **7-layer Advanced Endpoint Protection (AEP) with Default Deny security posture** (including world's best Containment technology).<br>See **https://www.comodo.com/aep.php** to read more. | 30 days | ✗ | ✓ | ✓ |
| **Valkyrie -** File intelligence service (automated artificial intelligence analysis) | 30 days | ✗ | ✓ | ✓ |
| **Valkyrie -** File intelligence service (manual analysis by human experts) | 30 days | ✗ | ✓ | ✓ |
| **IT Management** | | | | |
| **Patch management** | 50 devices | ✓ | ✓ | ✓ |
| **Monitoring** - Proactive monitoring | 50 devices | ✓ | ✓ | ✓ |
| **Procedures -** Standalone instruction scripts | 50 devices | ✓ | ✓ | ✓ |
| **Remote Access -** Remote Desktop connection | 50 devices | ✓ | ✓ | ✓ |
| **Full MDM** (Mobile Device Management) | 50 devices | ✓ | ✓ | ✓ |
| **Full MAM** (Mobile Application Management) | 50 devices | ✓ | ✓ | ✓ |
| **Full MSM** (Mobile Security Management) | 50 devices | ✓ | ✓ | ✓ |
| **BYOD support** (Bring Your Own Device support) | 50 devices | ✓ | ✓ | ✓ |
| **Community support** | 50 devices | ✓ | ✓ | ✓ |
| **24/7 professional support** | 50 devices | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| **Managed Security**<br>- Dedicated NOC support engineer for your account<br>- Complete management of your EM portal (request custom scripts, profiles, procedures etc)<br>- 24/7 monitoring of your environment | ✗ | ✗ | ✗ | ✓ |

# Appendix 3: Pre-configured Profiles

Endpoint Manager ships with the following built-in profiles:

- Windows - Security Level 1 Profile (default profile)
- Windows - Security Level 1 Profile [Former Standard Profile]
- Windows - Security Level 2 Profile
- Windows - Security Level 3 Profile
- Mac OS - Security Level 1 Profile for EM (default profile)
- iOS - Security Level 1 Profile for EM (default profile)
- Android - Security Level 1 Profile for EM (default profile)
- Linux - Security Level 1 Profile for EM (default profile)

'Default' profiles are automatically applied to devices which match their operating system IF no custom profile exists for the device.

**Windows Profile Settings**

| Section | Security Level 1 | Security Level 1 [Former 'Standard' profile] | Security Level 2 | Security Level 3 |
|---|---|---|---|---|
| **Containment Rule** | All malicious files are blocked and quarantined<br>All files in suspicious and containment folders are blocked<br>Metro apps are not contained<br>All unrecognized files are contained | All malicious files are blocked and quarantined<br>All files in suspicious and containment folders are blocked<br>Metro apps are not contained<br>All unrecognized files are contained. | All malicious files are blocked and quarantined<br>All files in suspicious and containment folders are blocked<br>All unrecognized files are contained.<br>All contained files are logged | All malicious files are blocked and quarantined<br>All files in suspicious and containment folders are blocked<br>All unrecognized files are contained.<br>All contained files are logged |
| **HIPS** | Enabled<br>'Safe Mode' action = 'Allow Requests'<br>'Enhanced Protection Mode' - Disabled, | Enabled<br>'Safe Mode' action = 'Allow Requests'<br>'Enhanced Protection Mode' = Disabled<br>'Enable Embedded Code Detection and Heuristic Command-line Analysis for Certain Applications' = Enabled | Enabled<br>'Safe Mode' action = 'Block Requests'<br>'Enhanced Protection Mode' = Enabled | Enabled<br>Safe Mode action = 'Block Requests'<br>'Enhanced Protection Mode' = Disabled<br>'Enable Embedded Code Detection and Heuristic Command-Line Analysis for Certain Applications' = Enabled with all applications selected |
| **Firewall** | Enabled<br>'Safe Mode' action = 'Allow Requests' | Enabled<br>'Safe Mode' action = 'Allow Requests' | Enabled<br>'Safe Mode' action = 'Block Requests' | Enabled<br>'Safe Mode' action = 'Block Requests' |

| | | | | |
|---|---|---|---|---|
| **VirusScope** | Enabled<br>'Monitor Contained Applications only' = Enabled | Enabled<br>'Monitor Contained Applications only' = Enabled | Enabled<br>'Monitor Contained Applications only' = Disabled | Enabled<br>'Monitor Contained Applications only' = Disabled |
| **File Rating** | Enabled<br>'Detect potentially unwanted applications' = Enabled | Enabled<br>'Detect potentially unwanted applications' = Enabled | Enabled<br>'Detect potentially unwanted applications' = Enabled | Enabled<br>'Detect potentially unwanted applications' = Enabled |
| **Antivirus** | 'Realtime Scan' - Enabled<br>Full Scan - 'Use cloud while scanning' - Disabled | 'Realtime Scan' - Enabled<br>Full Scan - 'Use cloud while scanning' - Disabled | 'Realtime Scan' - Enabled<br>Full Scan - 'Use cloud while scanning' - Disabled | 'Realtime Scan' - Enabled<br>Full Scan - 'Use cloud while scanning' - Enabled |
| **Miscellaneous** | Unrecognized autorun entries related to new/modified registry items are ***ignored***. | Unrecognized autorun entries related to new/modified registry items are ***ignored***. | Unrecognized autorun entries related to new/modified registry items are ***terminated and disabled***. | Unrecognized autorun entries related to new/modified registry items are ***quarantined and disabled***. |

# About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

# About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

**https://www.comodo.com**

Email: **EnterpriseSolutions@Comodo.com**