

COMODO
Creating Trust Online®



Comodo

Client - Security for Linux

Software Version 2.2

User Guide
Guide Version 2.2.060920

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Client - Security for Linux	4
1.1.Features.....	6
1.2.System Requirements.....	6
1.3.Install Comodo Client - Security for Linux	6
1.4.Start CCS for Linux.....	16
1.5.Understand CCS Alerts.....	18
2. The Summary Screen	19
3. Antivirus Tasks – Introduction	21
3.1.Run a Scan.....	22
3.2.Update Virus Database.....	29
3.3.Scheduled Scans.....	30
3.4.Quarantined Items.....	32
3.5.Scan Profiles.....	34
3.6.Scanner Settings.....	38
3.6.1.Real Time Scan.....	39
3.6.2.Manual Scan.....	41
3.6.3.Scheduled Scan.....	43
3.6.4.Exclusions.....	44
4. More Options – Introduction	47
4.1.Preferences.....	48
4.1.1.Language Settings.....	49
4.1.2.Log Settings.....	50
4.1.3.Connection Settings.....	52
4.1.4.Update Settings.....	53
4.1.5.External Device Control Settings.....	55
4.2.Manage My Configurations.....	58
4.2.1.Comodo Preset Configuration.....	58
4.2.2.Import /Export and Manage Personal Configurations.....	60
4.3.Diagnostics.....	66
4.4.View Antivirus Events.....	67
4.4.1.Log Viewer Module.....	68
4.4.1.1.Antivirus Logs.....	69
4.4.1.1.1.Filter Antivirus Logs.....	71
4.4.1.2.Device Control Logs.....	73
4.4.1.2.1.Filter Device Control Logs.....	75
4.4.1.3.'Alerts Displayed' Logs.....	76
4.4.1.3.1.Filter 'Alerts Displayed' Logs.....	77
4.4.1.4.'Tasks Launched' Logs.....	80
4.4.1.4.1.Filter 'Tasks Launched' Logs.....	82
4.4.1.5.Configuration Change Logs.....	84
4.4.1.5.1.Filter 'Configuration Change' Logs.....	86
4.5.Browse Support Forums.....	89

4.6.Help	90
4.7.About.....	90
Appendix 1 - CCS for Linux How To... Tutorials.....	91
Scan your Computer for Viruses.....	91
View Antivirus Events.....	97
Configure Database Updates.....	98
Quickly Set up Security Levels.....	99
Change CCS Language Settings	100
Run an Instant Antivirus Scan on Selected Items.....	102
Create a Scheduled Scan.....	103
Restore Incorrectly Quarantined Item(s).....	105
Switch off Automatic Antivirus Updates.....	106
Control External Device Accessibility.....	109
About Comodo Security Solutions.....	111

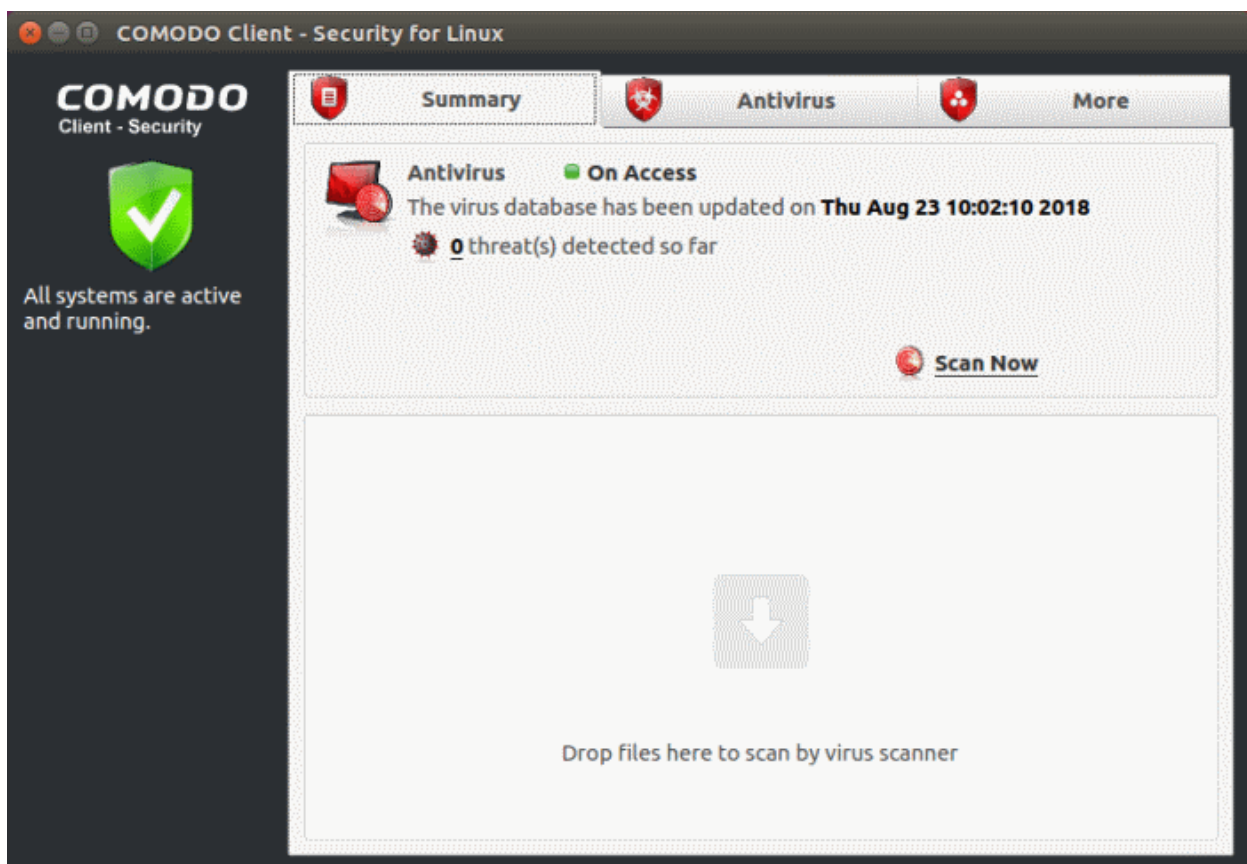
1. Introduction to Comodo Client - Security for Linux

Comodo Client Security for Linux (CCS) offers complete protection against viruses, worms and Trojan horses for Linux based computers. The software is easy to setup and features real-time virus monitoring, full event logging, scheduled scans and more.

- Click 'Scan Now' on the summary screen to run a scan of your system
- Drag files and folders into the scan box to check individual items

Features

- Detects, blocks and eliminates viruses from desktops and networks
- Constantly protects with real-time and on-access scanning
- Scheduler allows you to run scans at a time that suits you
- Isolates suspicious files in quarantine preventing infection
- Daily, automatic updates of virus definitions
- Device control allows you to block access to unknown external storage devices



Guide Structure

Click the links below to jump to the section that you need help with.

Introduction - An overview of Comodo Client - Security for Linux.

- **Features**

- **System Requirements**
- **Install Comodo Client - Security for Linux**
- **Start CCS for Linux**
- **Understand CCS Alerts**

The Summary Screen - At-a-glance details of important settings, activity and other information.

Antivirus Tasks - Introduction - Run scans, configure settings, schedules, updates, scan profiles and more.

- **Run A Scan**
- **Update Virus Database**
- **Scheduled Scans**
- **Quarantined Items**
- **Scan Profiles**
- **Scanner Settings**
 - **Real Time Scan**
 - **Manual Scan**
 - **Scheduled Scan**
 - **Exclusions**

More Options - Introduction - Overall configuration of Comodo Client - Security and view logs.

- **Preferences**
 - **Language Settings**
 - **Log Settings**
 - **Connection Settings**
 - **Update Settings**
 - **External Device Control Settings**
- **Manage My Configurations**
- **Diagnostics**
- **View Antivirus Events**
 - **Log Viewer Module**
 - **Antivirus Logs**
 - **Filter Antivirus Logs**
 - **Device Control Logs**
 - **Filter Device Control Logs**
 - **Alerts Displayed Logs**
 - **Filter Alerts Displayed Logs**
 - **Tasks Launched Logs**
 - **Filter Tasks Launched Logs**
 - **Configuration Changes Logs**
 - **Filter Configuration Changes Logs**
- **Browse Support Forums**
- **Help**
- **About**

Appendix 1 CCS for Linux How to... Tutorials

- **Scan your Computer for Viruses**
- **View Antivirus Events**
- **Configure Database Updates**

- **Quickly Set up Security Levels**
- **Change CCS Language Settings**
- **Run an Instant Antivirus Scan on Selected Items**
- **Create a Scheduled Scans**
- **Restore Incorrectly Quarantined Item(s)**
- **Switch off Automatic Antivirus Updates**
- **Control External Device Accessibility**

1.1. Features

- Detects and eliminates viruses from desktops, laptops and servers
- Cloud based scans mean you get the highest protection even if your database is outdated
- Heuristic techniques identify previously unknown threats
- Rootkit scanner identifies malware deeply hidden on you system
- Daily, automatic updates of virus definitions
- Built-in scheduler allows you to run scans at a time that suits you
- Simple to use - install and forget while CCS protects you in the background
- Control over access to external devices like USB sticks and external drives.

1.2. System Requirements

Supported Operating Systems

- Ubuntu 16.04.2 LTS x64 or higher
- Debian 8.8 x64 or higher
- Red Hat Enterprise Linux Server 7 x64 or higher

Please note: The real-time or on-access antivirus scanning is not supported in Debian.

1.3. Install Comodo Client - Security for Linux

You can use Endpoint Manager (EM) to deploy Comodo Client Security (CCS) to your endpoints. You can purchase EM as stand-alone application or as a part of the Comodo Dragon/C1 platforms.

This section covers how to:

- **Subscribe for Endpoint Manager**
- **Enroll users**
- **Enroll devices**

Subscribe for Endpoint Manager

You can purchase Endpoint Manager as stand-alone application or as part of the Dragon or Comodo One suite:

Dragon / C1

- **Dragon** - Sign up for Dragon at <https://platform.comodo.com/signup>
- **Comodo One** - Customers who already purchased Advanced Endpoint Protection (AEP) licenses from Comodo or its resellers can sign-in to C1 at <https://one.comodo.com/app/login>

- Use your username / password of your Comodo account created during purchase of AEP licenses
- Set-up your C1 MSP / Enterprise account
- After sign-up, login to the portal then click 'Applications > 'Endpoint Manager'.

Stand-alone Endpoint Manager


- Visit <https://secure.comodo.com/home/purchase.php?pid=98&license=try> for the trial version or <https://secure.comodo.com/home/purchase.php?pid=98> for the full version.
- You can access your EM instance at the URL provided during setup.

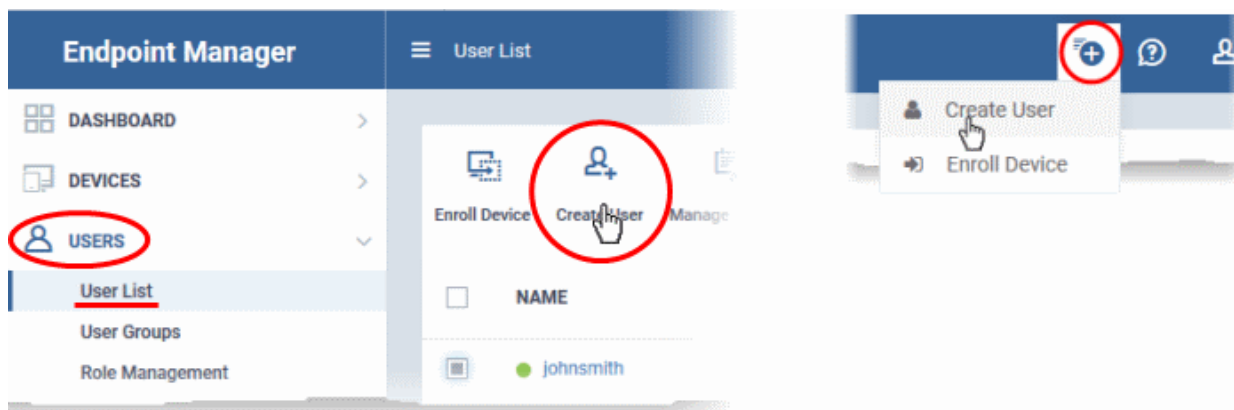
Enroll Users

You must add users to Endpoint Manager before you can install CCS on your endpoints.

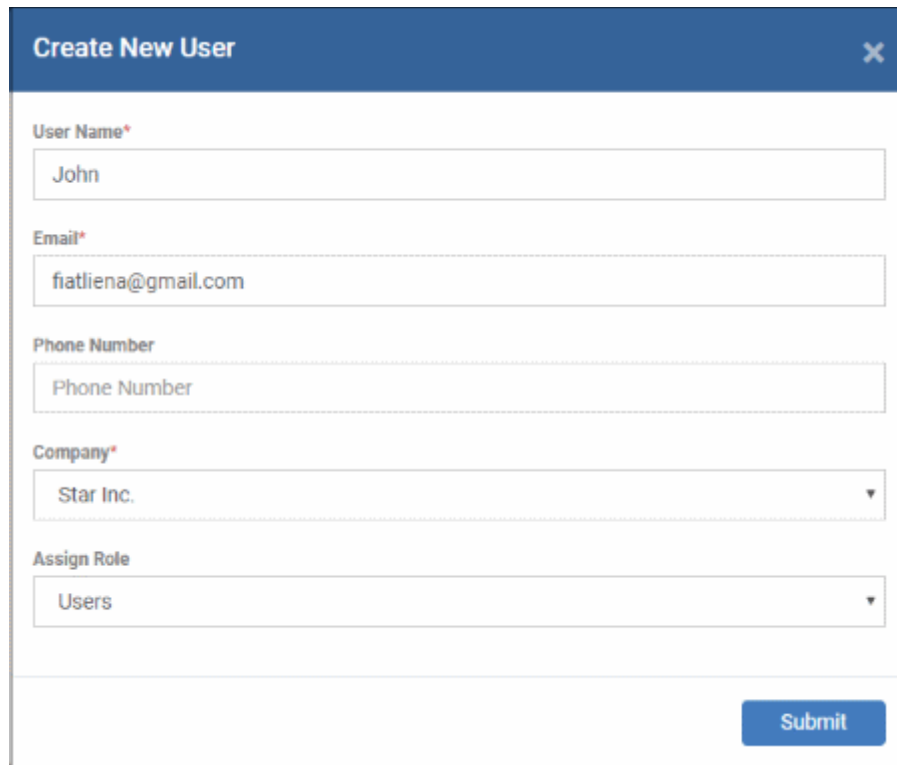
- **Dragon MSP / C1 MSP customers** - You can create multiple companies and enroll users to any of them.
- **Dragon Enterprise / C1 Enterprise, and stand-alone Endpoint Manager customers** - All users are enrolled to the default company.

Add a user

- Open Endpoint Manager
- Click 'Users' > 'User List'
- Click 'Create User'
- or
- Click the 'Add' button  on the menu bar and choose 'Create User'.



The create user form will open:



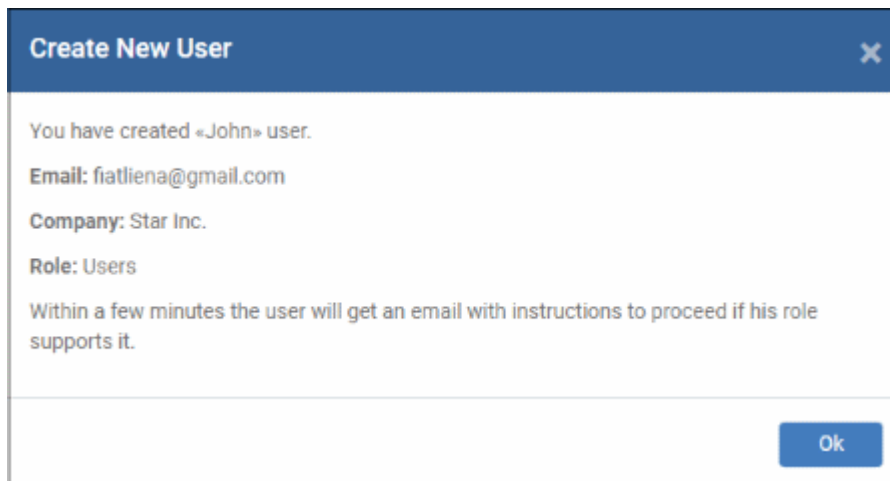
The screenshot shows a 'Create New User' dialog box. It has a blue header bar with the text 'Create New User' and a close button (X). Below the header are five input fields: 'User Name*' (containing 'John'), 'Email*' (containing 'fiatliena@gmail.com'), 'Phone Number' (containing 'Phone Number'), 'Company*' (a dropdown menu with 'Star Inc.' selected), and 'Assign Role' (a dropdown menu with 'Users' selected). At the bottom right of the form is a blue 'Submit' button.

- **User Name** - Enter the login username of the user. They will appear under this name in the EM interface.
- **Email** - Account and device activation mails will be sent to this address.
- **Phone Number** - The contact number of the user.
- **Company** - The organization to which you want to add the user.
- **Role**

A 'role' determines user permissions within the Endpoint Manager console itself. Endpoint Manager ships with two default roles:

- **Administrator** - Full privileges in the Endpoint Manager console. The permissions for this role are not editable.
 - **User** - In most cases, a user is simply an owner of a managed device. They should not require access to the Endpoint Manager console. Under default settings, users cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

A confirmation message is shown:




- Repeat the process to add more users.
- New users are added to the 'Users' interface (click 'Users' > 'User List')

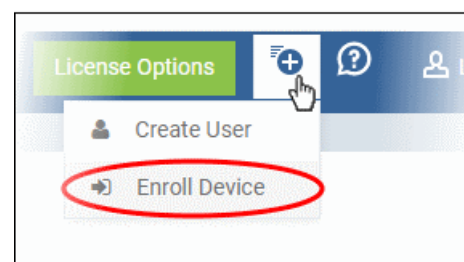
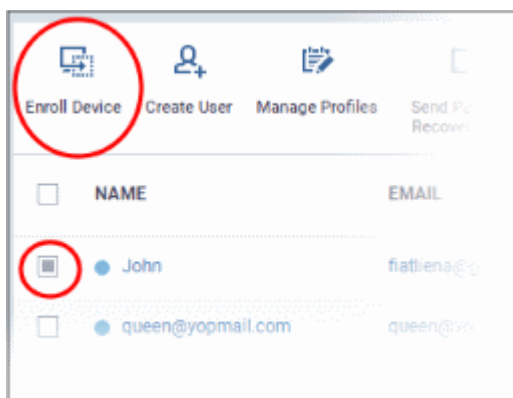
Tip: You can also bulk import users from a .csv file. See <https://help.comodo.com/topic-399-1-786-12973-Import-Users-from-a-CSV-File.html> for more details.

Enroll Devices

The next step is to add user devices so you can manage them with Endpoint Manager.

Enroll devices

- Click 'Users' > 'User List'
- Select users for whom you want to enroll devices
- Click the 'Enroll Device' button above the table
- Or
- Click the 'Add' button  on the menu bar and choose '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:

- 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.
- Click 'Next' to proceed to step 2.

Step 2 - Enrollment Options

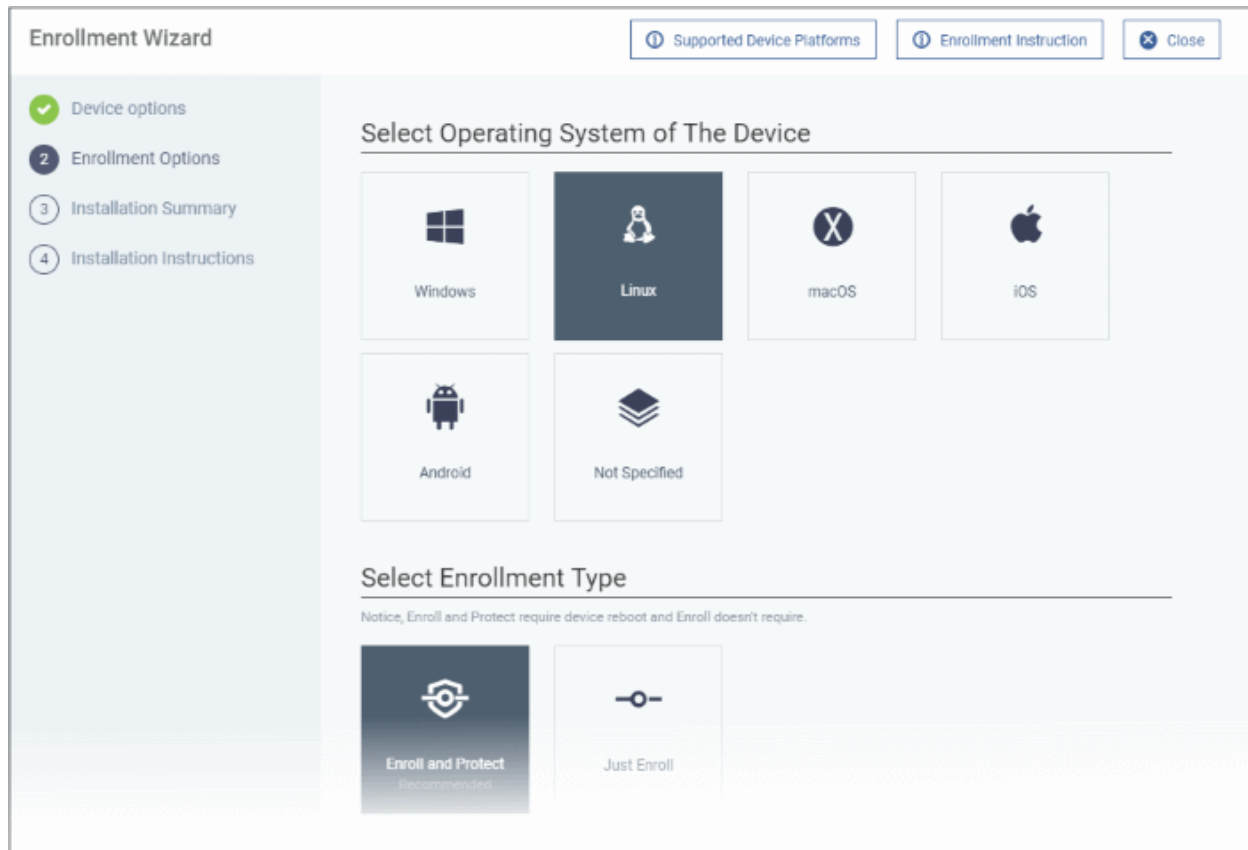
Enrollment Type

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.



TLDR - 'Not specified' only installs the communication client so the device can connect to Endpoint Manager. It does not install the security client. Click one of the operating system tiles if you also want to install the security client.

Option 1 - Enroll + Protect - Single Operating System

- Choose this if you want to deploy both communication and security clients
 - Click the Linux OS box. Please make sure all your target devices use this operating system.
 - The wizard will send enrollment mails which *only* contain download links for the Linux clients.
 - You can customize enrollment options as required. You can configure items such as enrollment type, Linux OS version and device name.
 - Note - Please uninstall any other antivirus products from target endpoints before proceeding. Failure to do so could cause conflicts that mean CCS does not function correctly.

Option 2 - Enroll Only - Multiple Operating Systems

- Choose this if you only want to deploy the communication client. If required, you can install the security client later after enrolling the endpoint.
 - Click 'Devices' > 'Device List'
 - Select the target devices
 - Click the 'Install or Update Package' button > Choose 'Install Comodo Client – Security'.

Click 'Next' to **skip to step 3** if you are happy with your choices thus far

OR

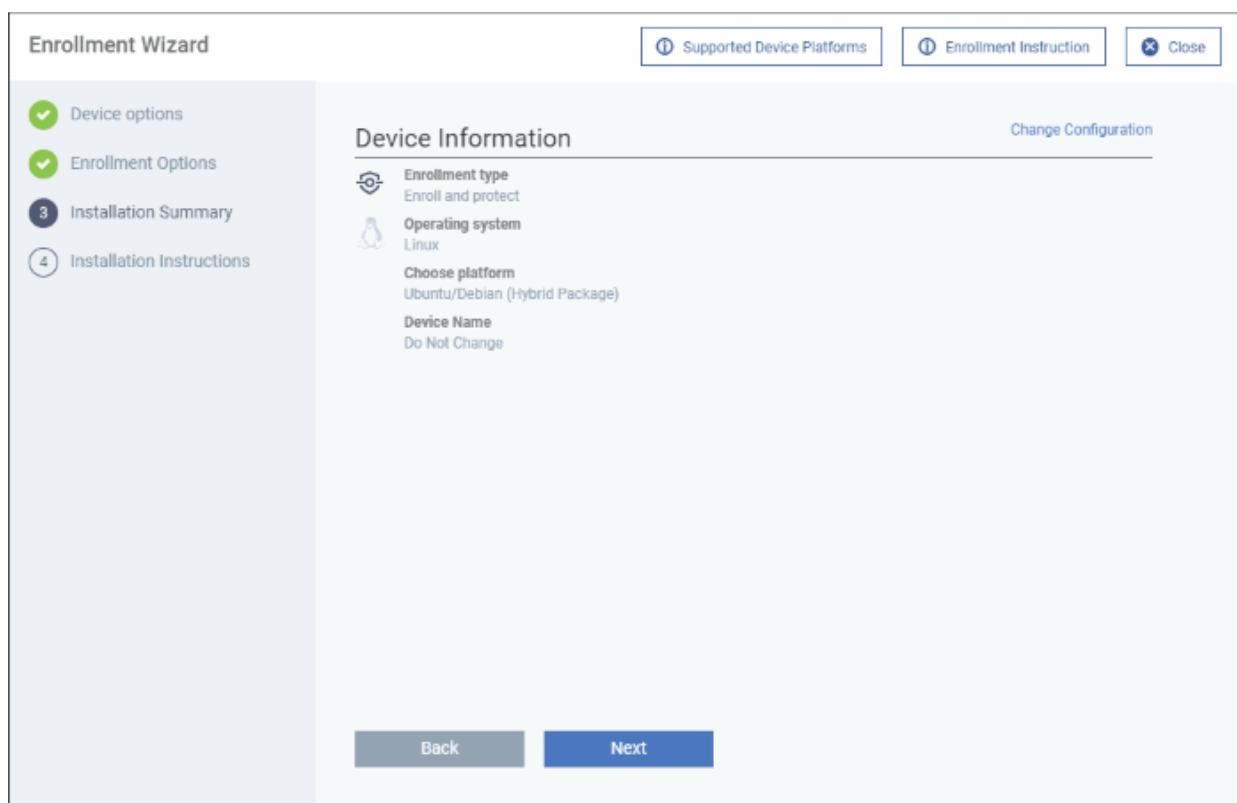
See the table below for more information about the options on this page

Setting	Description
Choose platform	Select Linux OS version <ul style="list-style-type: none"> • Ubuntu / Debian (Hybrid Package) • RHEL / CentOS (Hybrid Package) • 'Hybrid' just means the package is suitable for both types of OS.
Device Name Options	<ul style="list-style-type: none"> • 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

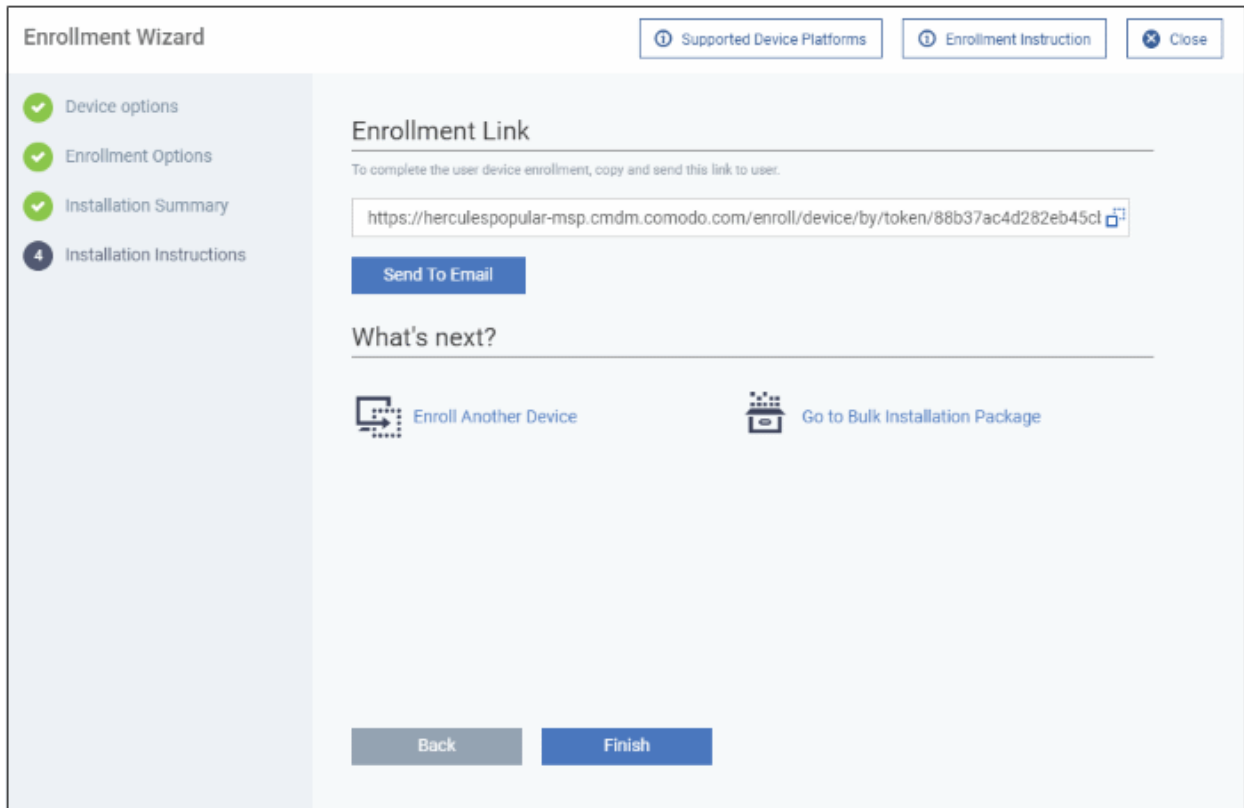
Review your choices so far.



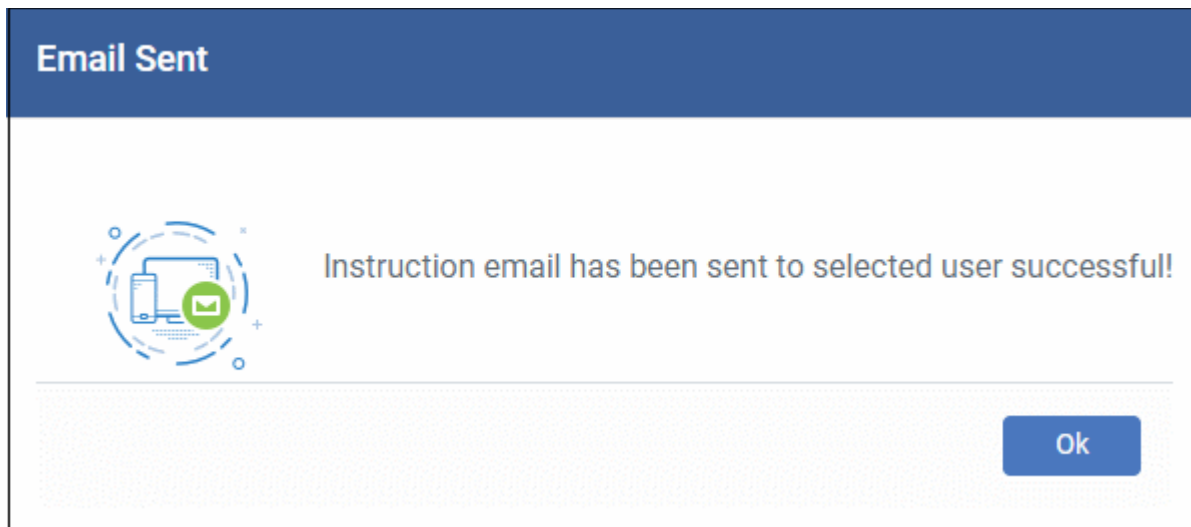
- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4

Step 4 - Installation Instructions

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



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



- **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.

An example mail is shown below:

Dear Grey Pelican,

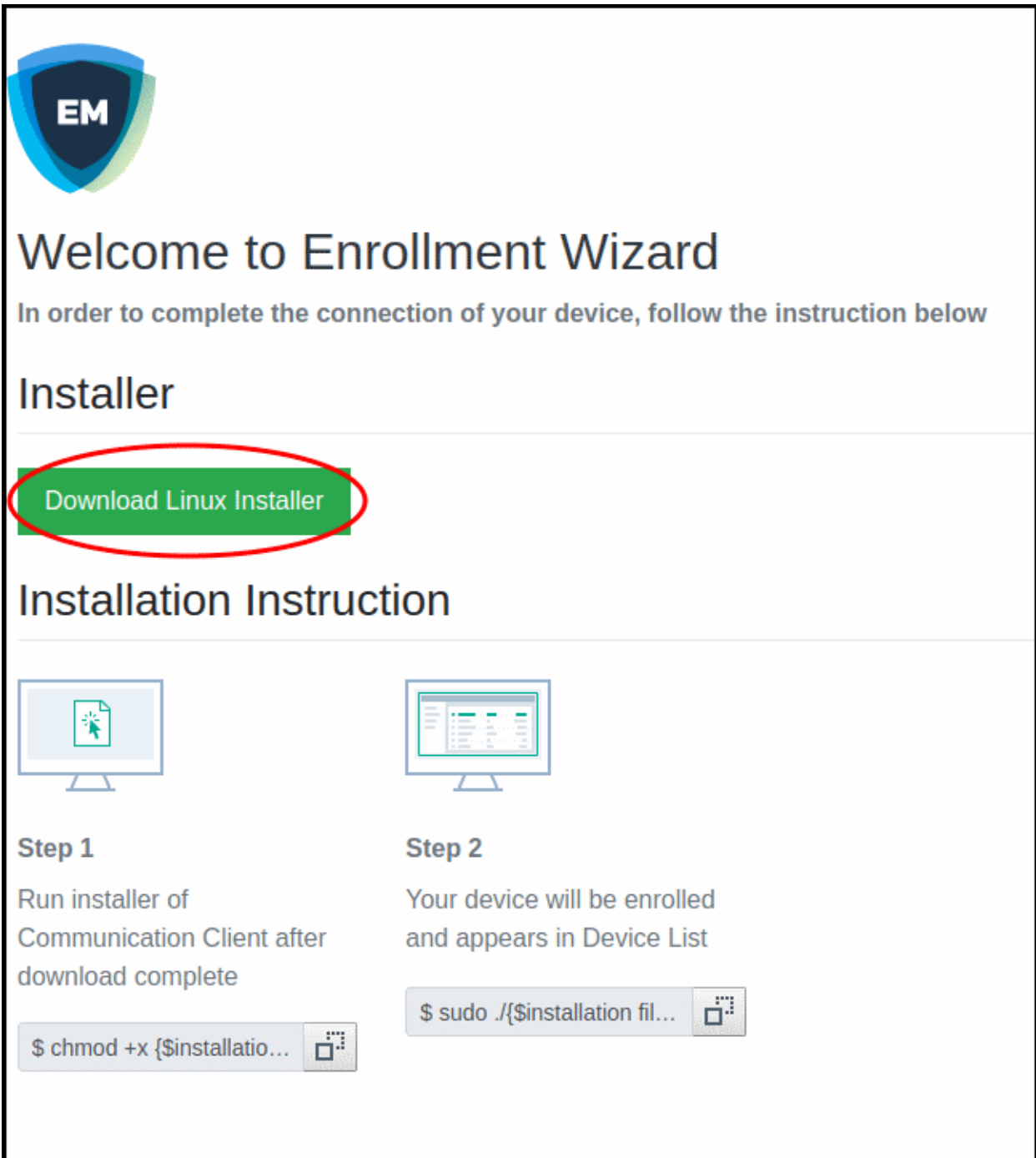
Congratulations, your Endpoint Manager account has been successfully created. Please click the following link to activate your account and set up your password:


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

Sincerely, Endpoint Manager team.

The user experience is as follows:

- User opens the email on the Linux endpoint you want to enroll.
- Click the enrollment link in the email to open the device enrollment page
- Click the 'Download Linux Installer' button:







Welcome to Enrollment Wizard

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

Installer

[Download Linux Installer](#)

Installation Instruction

 <p>Step 1 Run installer of Communication Client after download complete</p> <pre>\$ chmod +x {\$installation file\$}</pre>	 <p>Step 2 Your device will be enrolled and appears in Device List</p> <pre>\$ sudo ./{\$installation fil...}</pre>
--	--

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_cTjIw6gG_installer.run  
sudo./itsm_cTjIw6gG_installer.run
```

```
c1@c1-VirtualBox: ~/Downloads
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. The EM communication client icon  appears at the top-right of the endpoint screen.
- Protection is effective immediately after the computer restarts.

An Endpoint Manager (EM) security profile is applied to the device.

- 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 Linux 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.

1.4. Start CCS for Linux

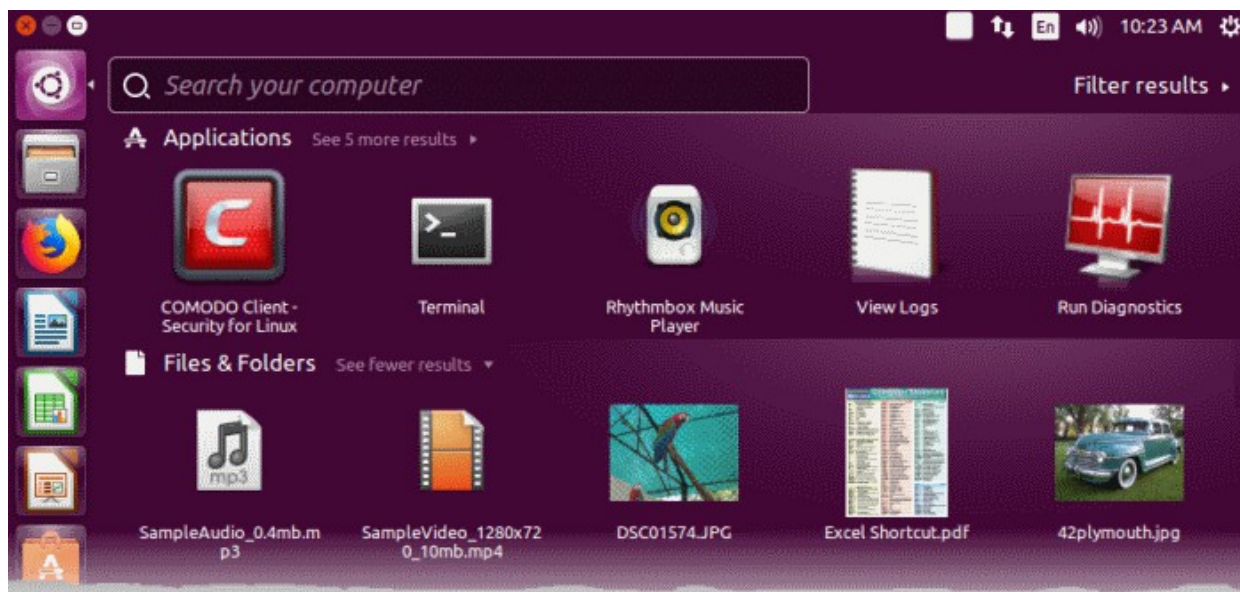
- After installation, Comodo Client Security (CCS) will load at computer start-up.
- Real-time protection and on-access scanning is automatically enabled, so you are protected immediately after the restart.
- You need to open the management interface to configure application settings.

There are three ways you can open the interface:

- **Applications Menu**
- **Desktop Menu**
- **Dock Icon**

Applications Menu

- Click 'Applications' to view CCS product group icons:

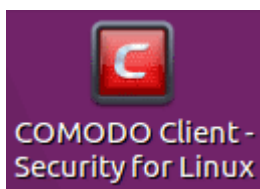


The applications menu provides shortcuts to:

- **Comodo Client Security** – Double-click to start the application.
- **Run Diagnostics**
- **View Logs**

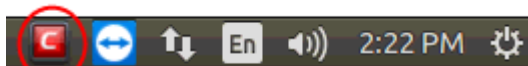
Desktop Menu

- Double-click the CCS icon in the desktop to start Comodo Client – Security.

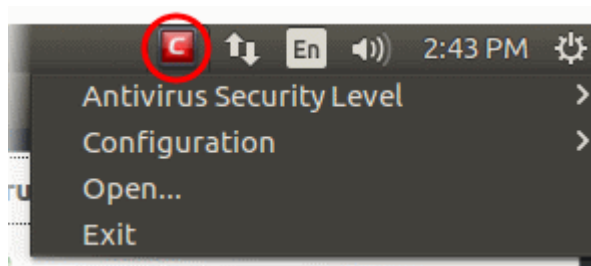


Dock icon

- Double-click the CCS icon in the dock area to start Comodo Client - Security.



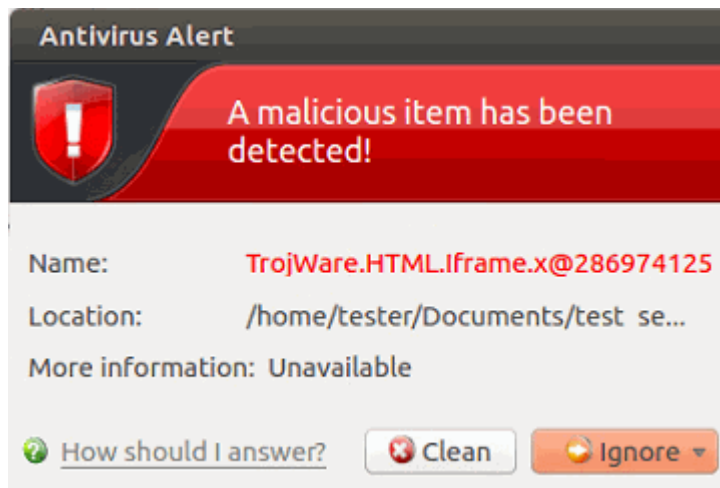
- Right-click on the dock icon to access CCS options:



See **Real Time Scan** and **Manage My Configurations** for more details.

1.5. Understand CCS Alerts

- Antivirus alerts inform you if a virus has been detected and provide options on how to handle the threat.
- Alerts can also be used to instruct CCS on how it should behave in future when it encounters activities of the same type.

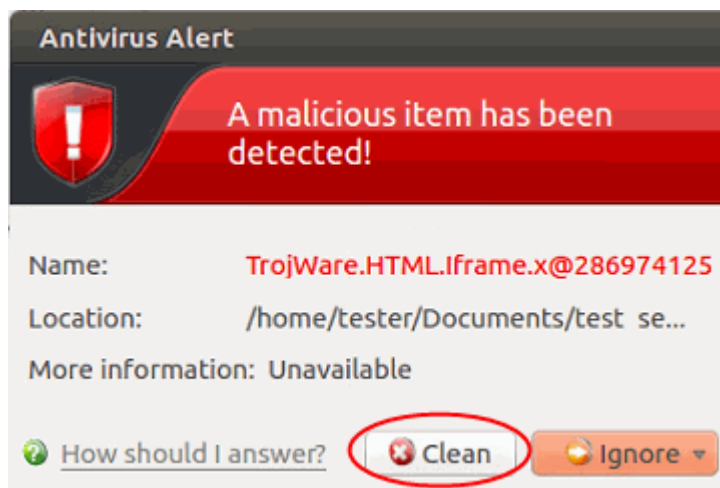


Note: Real-time scans are not supported on Debian. Hence, antivirus alerts are not shown on Debian.

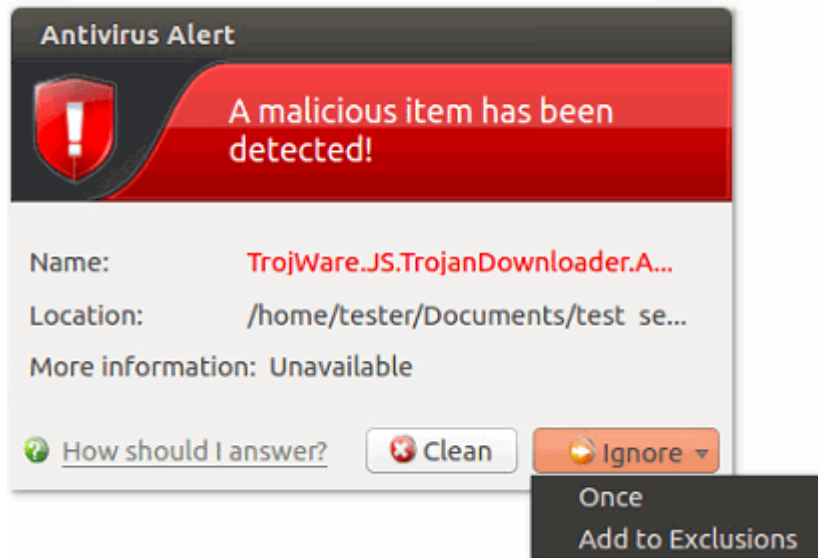
Answer an antivirus alert

- Alerts are generated whenever malware is detected.
- The alert contains the name of the virus, its location on your disk, and other information about the virus.

You can clean the threat or ignore it:



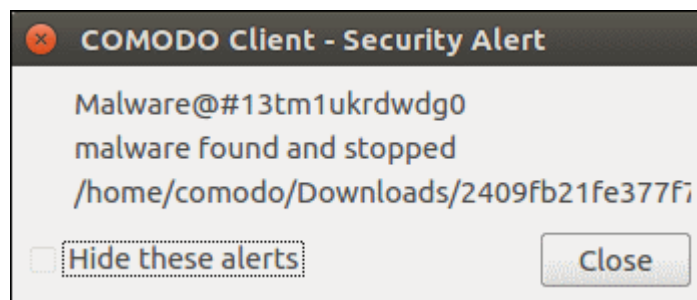
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists then the file is moved to **Quarantined Items**.
- **Ignore** - Dismisses the alert and allows the file to run. Only do this if you are 100% sure the file is safe.



- Two options are available if you select 'Ignore':
 - **Once** -The file is allowed to run this time only. The file will still be detected as a threat by future scans and another alert shown.
 - **Add to Exclusions** – Allow the file to run and create a permanent exception for the file. Future scans will not flag the file as a threat nor raise an alert. The file is also added to the **Exclusions** list.

Antivirus Notification

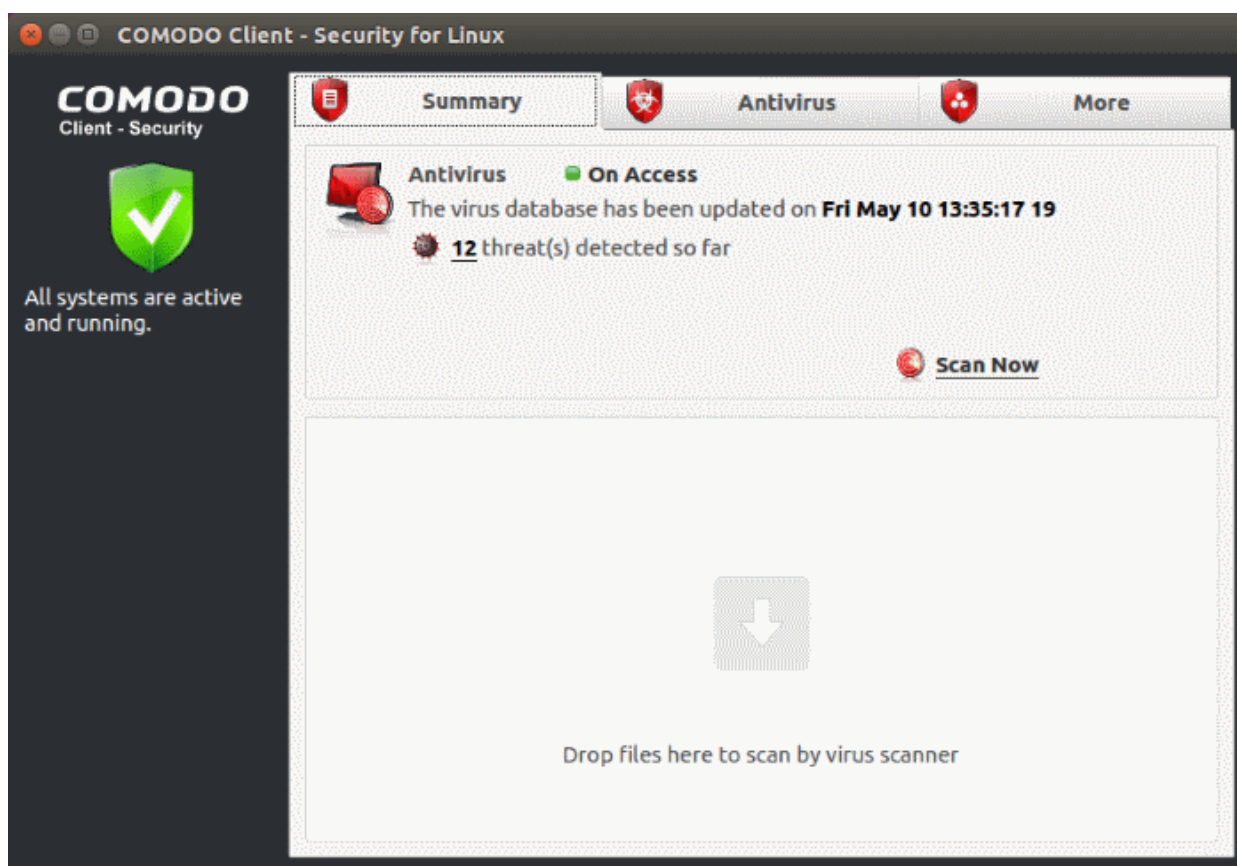
- You can configure the on-access scanner to automatically quarantine any threats it finds.
- If enabled, you will see a notification when CCS quarantines a file:



- Hide these alerts – CCS will still quarantine the threat but will not show the notification.

2. The Summary Screen

- The summary area is shown by default when you open the application
- It provides an at-a-glance summary of protection and update status
- You can also run a virus scan with a single click from here.



- You can scan files and folders by simply dragging them onto the scan box.

The summary screen contains the following information:

1. System Status

The shield icon on the left shows your current protection level. There are three colors - yellow, green and red

- **Yellow** - Your security is at risk. For example, because you need to run a full scan, because the database is outdated, or because the real-time scanner is switched off.
- **Green** - All systems are active and running.
- **Red** - Serious security risks. For example, you have malware on your system.

2. Antivirus

Scanner status - Shows whether the 'always-on' virus monitor is active or not. Possible states are:

- **On Access:** Real-time virus protection is enabled. All files you open or download are scanned before they are allowed to open.
- **Disabled:** Real-time protection is switched off.
Click the status link to configure real-time protection.
See **Scanner Settings** for more help with this area.

Database Updates

- The date when the virus database was last updated is shown as a link.
- Click the link to run a database update.
- See **Update Virus Database** for more details

Number of Detected Threats

- The number of threats found in this session.
- Click the number to view a list of threats detected. See **Antivirus Events** for more info on this

screen.

Scan Now

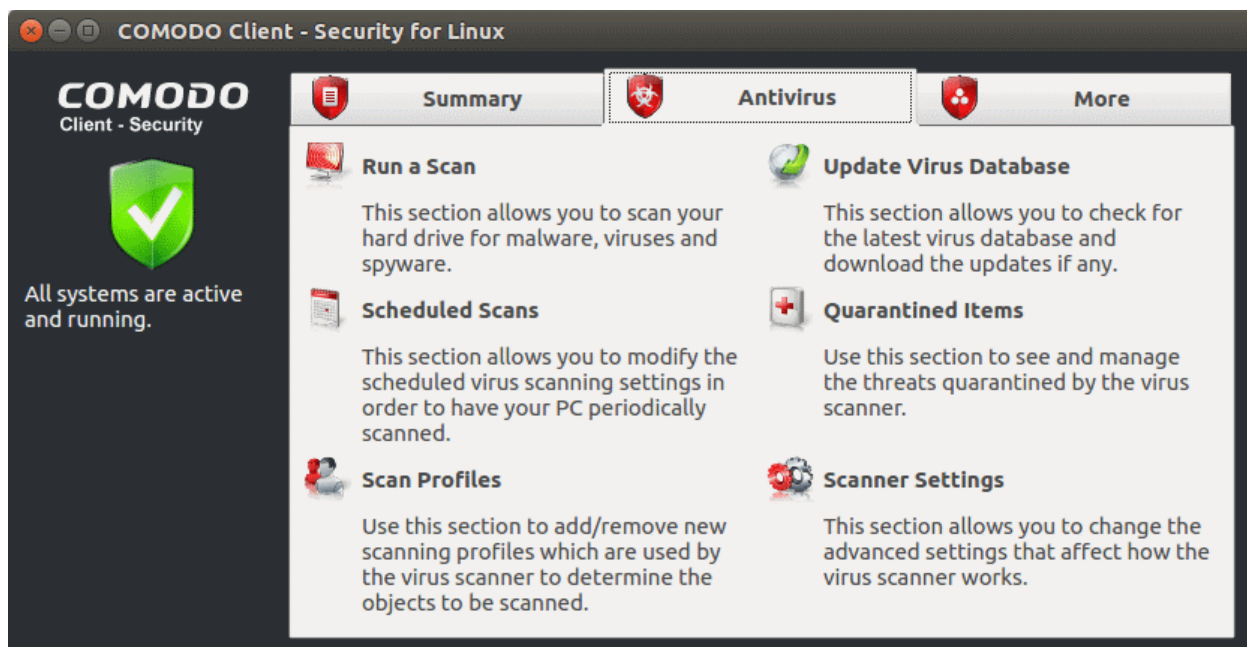
- Click the 'Scan Now' link to start a **virus scan**.

3. Scan Box

- Drag any file, folder or drive into the box to run an instant virus scan on it.
- The results screen has controls that let you deal with any identified threats.

3. Antivirus Tasks – Introduction

- Click the 'Antivirus' tab on the CCS home-screen to open this interface.
- The tasks screen lets you run on-demand virus scans and configure scanner settings.
- You can also set up a scan schedule, manage quarantined items, update the virus database, and create a custom scan profile.



Background – How antivirus scans work

1. Files on the host are checked against the local virus database and Comodo's master, cloud database.
 - Note – Realtime scans only use the local virus database.
2. Discovered malware is handled per the scanner settings. You can automatically quarantine threats, or have an alert shown which lets you choose what to do with each threat.
3. If the file's signature is not available in FLS, then the file is given an 'unknown' trust rating. Unknown files are submitted to Valkyrie for analysis if so configured in the Endpoint Manager profile.
 - Valkyrie is Comodo's online file rating system. It tests the runtime behavior of unknown files in order to identify those that are malicious.
 - Note – You need to enable 'Enable Cloud Scanning' in settings to activate this feature.
4. Unknown files run normally until Valkyrie analysis is complete.
5. If Valkyrie finds that the file is malicious then it is added to the malware blacklist. CCS will flag the file as a virus on the next scan.

Tip: The logs area contains a record of all virus events, tasks, scans and configuration changes. Click 'More' >

'View Antivirus Events' to open it. See [View Antivirus Events](#) if you need help.

The following sections explain more about each task:

- [Run a Scan](#)
- [Update Virus Database](#)
- [Scheduled Scans](#)
- [Quarantined Items](#)
- [Scan Profiles](#)
- [Scanner Settings](#)

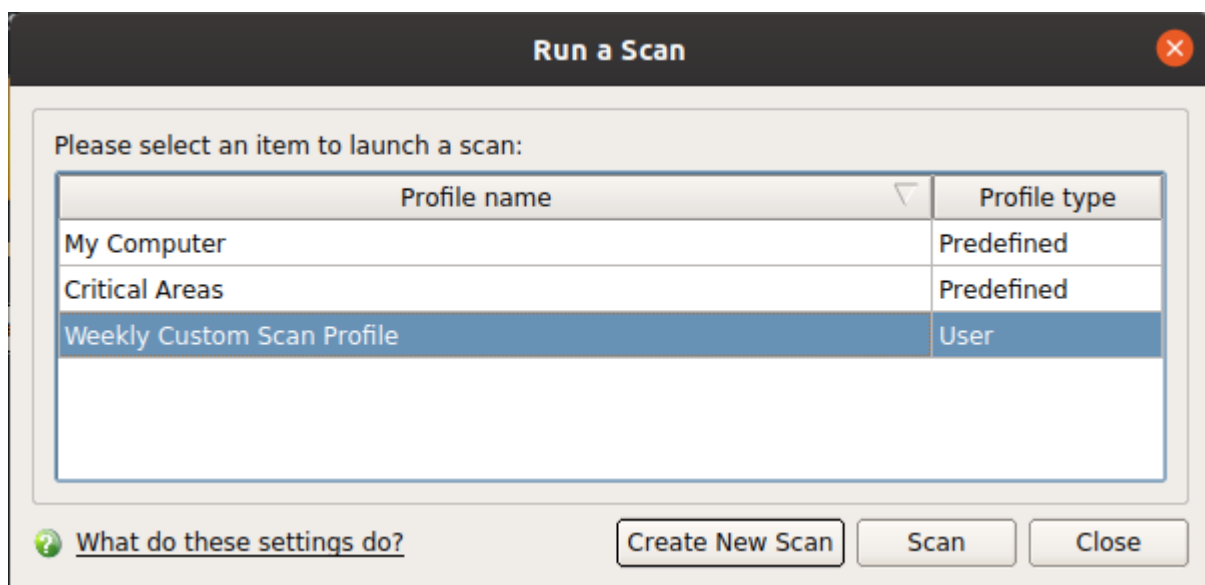
3.1. Run a Scan

Click 'Antivirus' > 'Run a Scan'

- The 'Run a Scan' area lets you launch an on-demand scan on an item of your choice.
- The item scanned can be anything you choose - your entire computer, a specific drive, or even a single file.
- You can also scan a wide range of removable storage devices, including external hard-drives, USB sticks, digital cameras and more.

Run an on-demand virus scan

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Run a Scan' in the antivirus tasks area



Choose one of the following options:

- **Profile name** - A scan profile defines the folders, drives or areas that are covered by the scan.
CCS ships with two pre-defined scan profiles - 'My Computer' and 'Critical Areas'. These cannot be edited or removed:
 - **My Computer** - Scans every drive, folder and file on your system, including external connected devices

- **Critical Areas** - A targeted scan of important operating system files and folders.
- **Profile type** - Shows whether the profile is predefined (created by Comodo) or user-defined.
- **Create New Scan** – Create your own **custom scan** of specific files, folders or drives.

Click 'Scan' after making your selection.

Custom Scan

You need to create a scan profile in order to run a custom scan. Once created, you can re-run the scan in future.

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click the 'Run a Scan' box
- Click 'Create New Scan'
- Type a name for your new profile. For example, 'My External Drives'.
- Click 'Add' to choose files, folders or drives you want to include in the profile
- Click 'Apply'. Your new profile will be listed in the 'Run a Scan' dialog
 - Note - You can also create custom **scan profiles** in the scan profiles area.
- Select your new profile in the list and click 'Scan'
- Next, see:
 - **Scan progress and results**
 - **Create a custom scan profile**
 - **Instantly scan items**

Tip: If you just want to scan on a file or folder, you can just drag it into the scan box in the 'Summary' area.

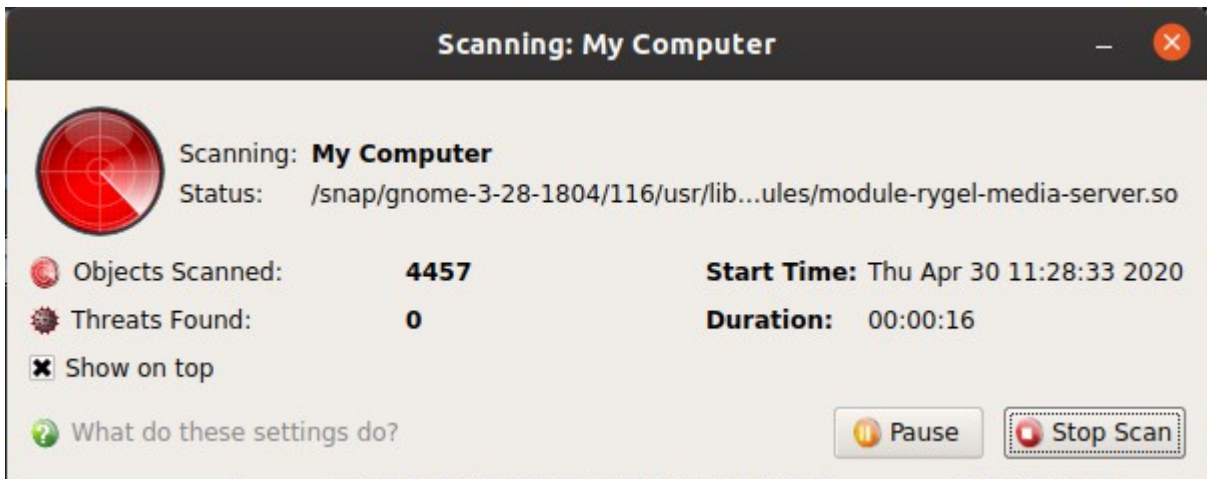
Scan progress and results

Before running the scan, Comodo Client Security will first check for AV database updates. If updates are available they will be downloaded and installed.



The scan, based on the profile you selected, will begin immediately.

The progress dialog shows the profile name, the location that is currently being scanned, the start time and duration of the scan, the total number of objects scanned so far, and the number of threats found:

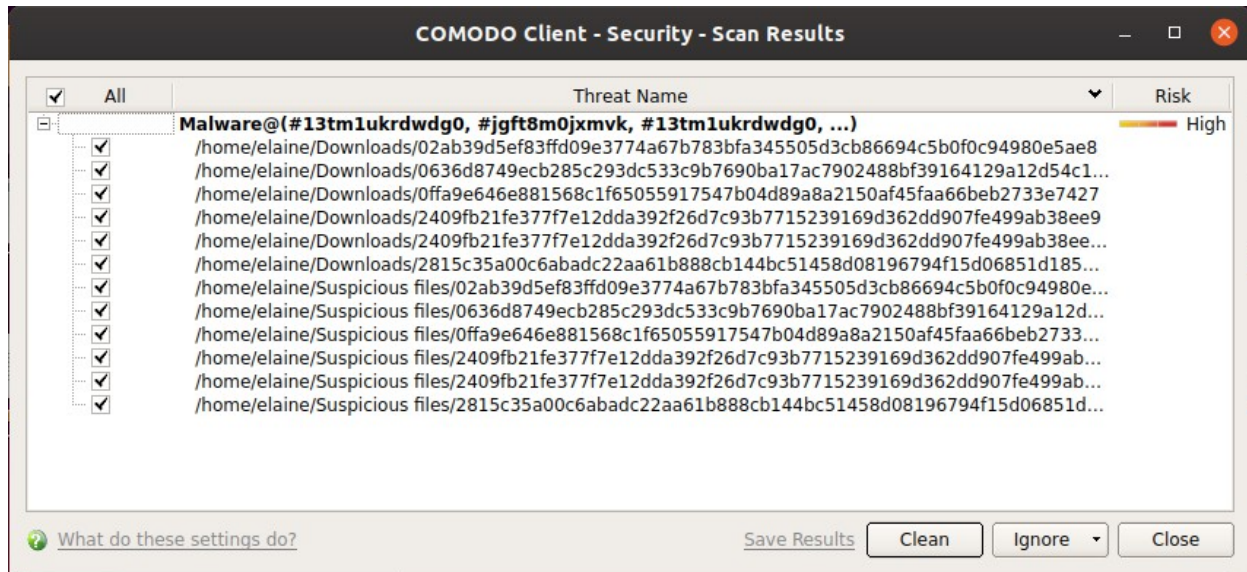


- Click 'Pause' to suspend the scan
- Click 'Resume' to recommence the scan
- Click 'Stop Scan' to abort the scan altogether.

Results are shown at the end of the scan:



- Click the 'Results' button to see detailed file information.
- The results window lists all threats discovered by the scan and provides controls which let you deal with the them:

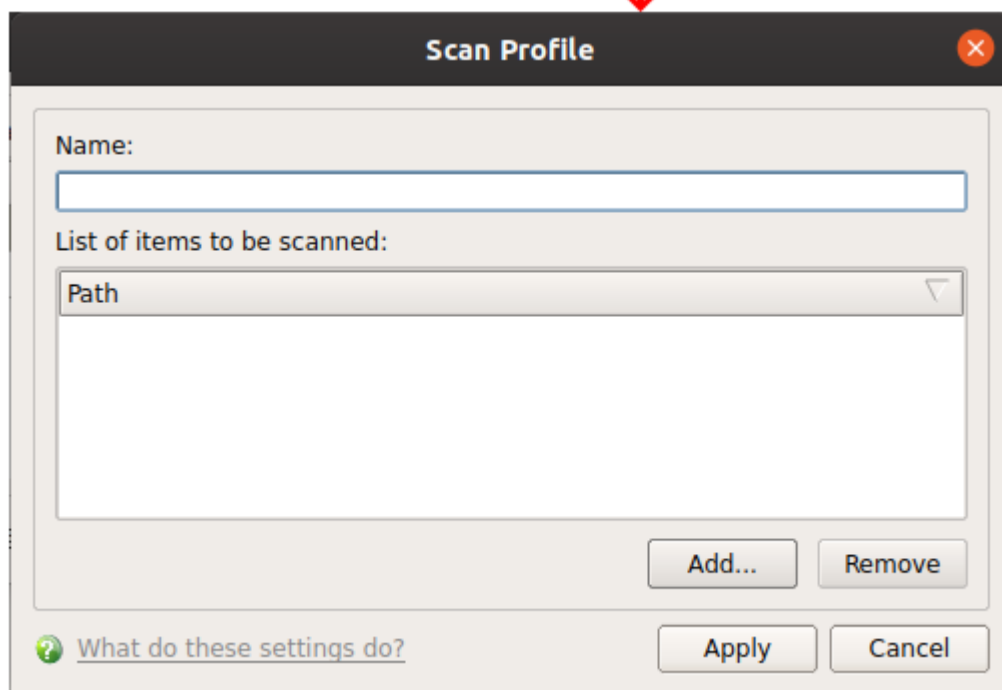
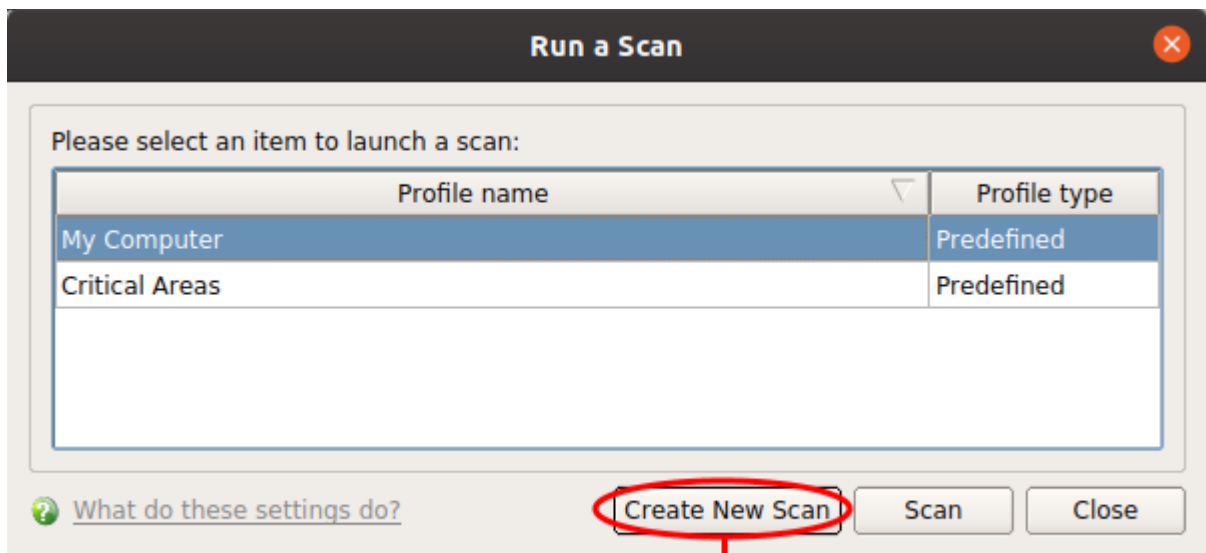


- Click the 'Threat Name' column header to sort results in alphabetical order
- Click the 'Risk' column header to sort results by risk level
- Select 'All' if you want to apply 'Clean' or 'Ignore' actions to every threat.
- **Save Results** – Click the link to store the scan results as a text file.
- **Clean** - If a disinfection routine exists, CCS will remove the infection and retain the original file. If no disinfection routine exists, CCS will move the file to **Quarantine**.
- **Ignore** - Two options:
 - **Once** - The file is removed from the threat results. The file isn't, however, added to the list of exclusions. The file will be detected as a threat again by the next scan.
 - **Add to Exclusions** - The file is moved to the **Exclusions** list. CCS will skip this file in future scans and not consider it to be a threat.

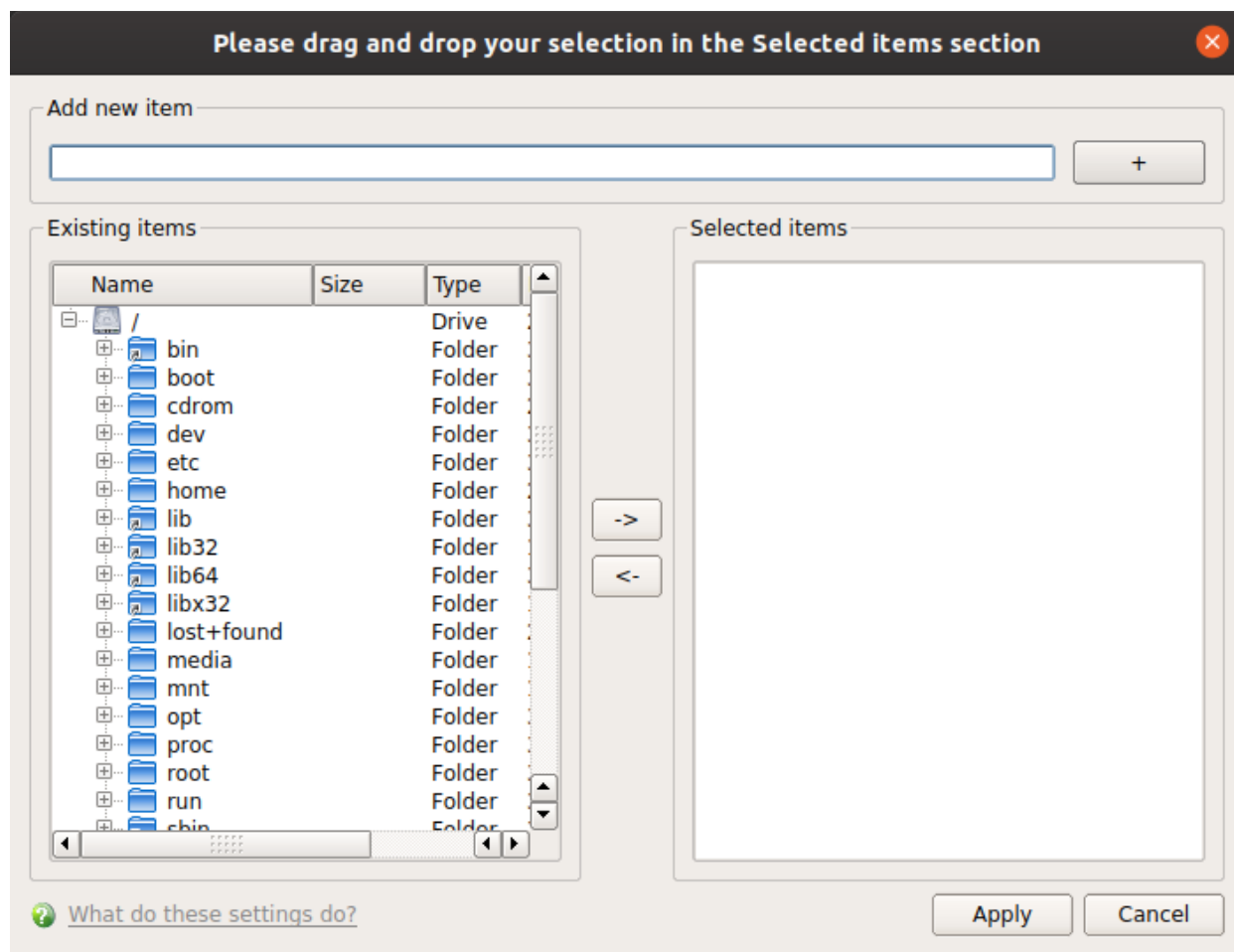
Create a Scan Profile

'Scan Profiles' let you set up custom scans on specific areas on your system. Scan profiles can be run on-demand at any time.

- Open Comodo Client Security
- Click the 'Antivirus' tab > Click 'Run a Scan'
- Click 'Create New Scan'

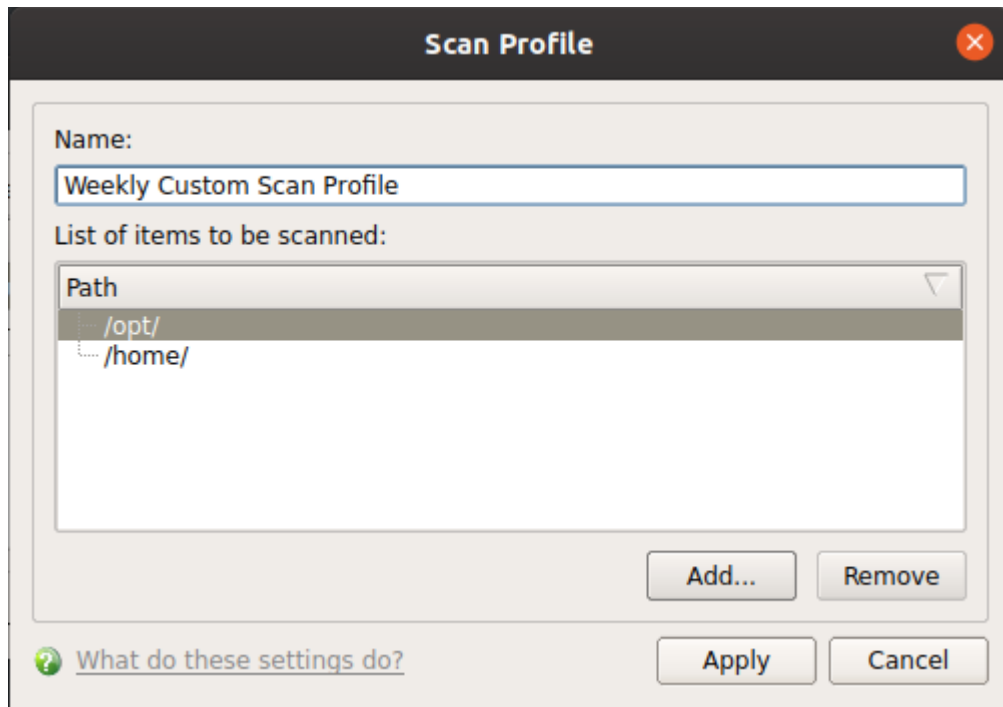


- **Name** - Enter a label for the scan profile.
- Click 'Add' to select the items you wish to include in the scan

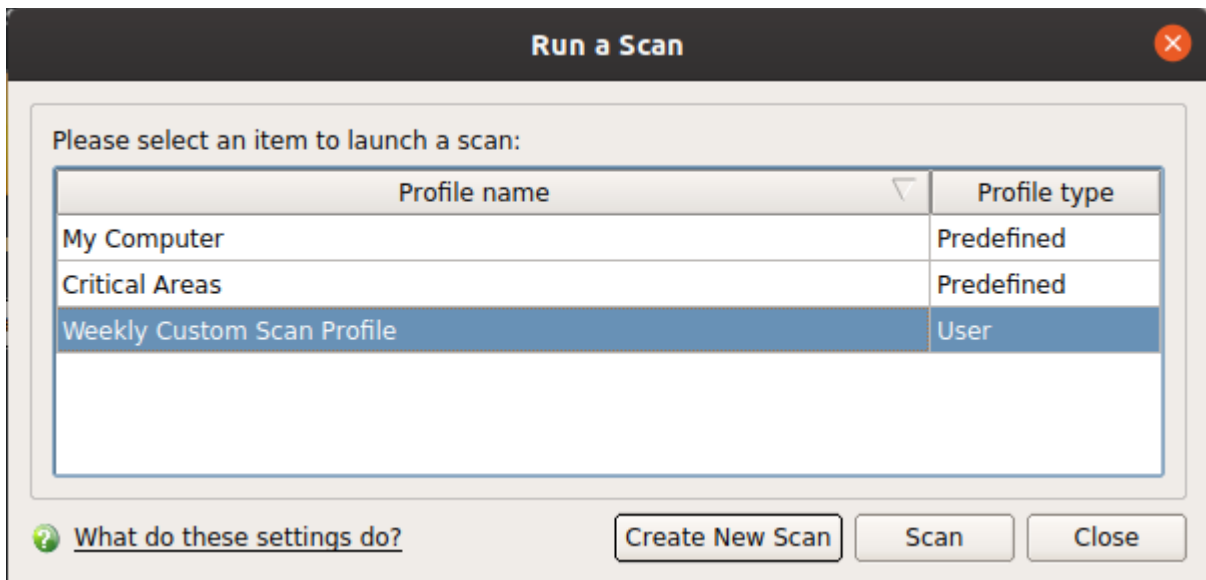


You can add items in two ways:

- Manually enter the path in the 'Add new item' field and click the '+' button
- Drag and drop the files, folders and/or drives you require from the left pane to the right pane.
- Repeat the process to select multiple items
- Click 'Apply'



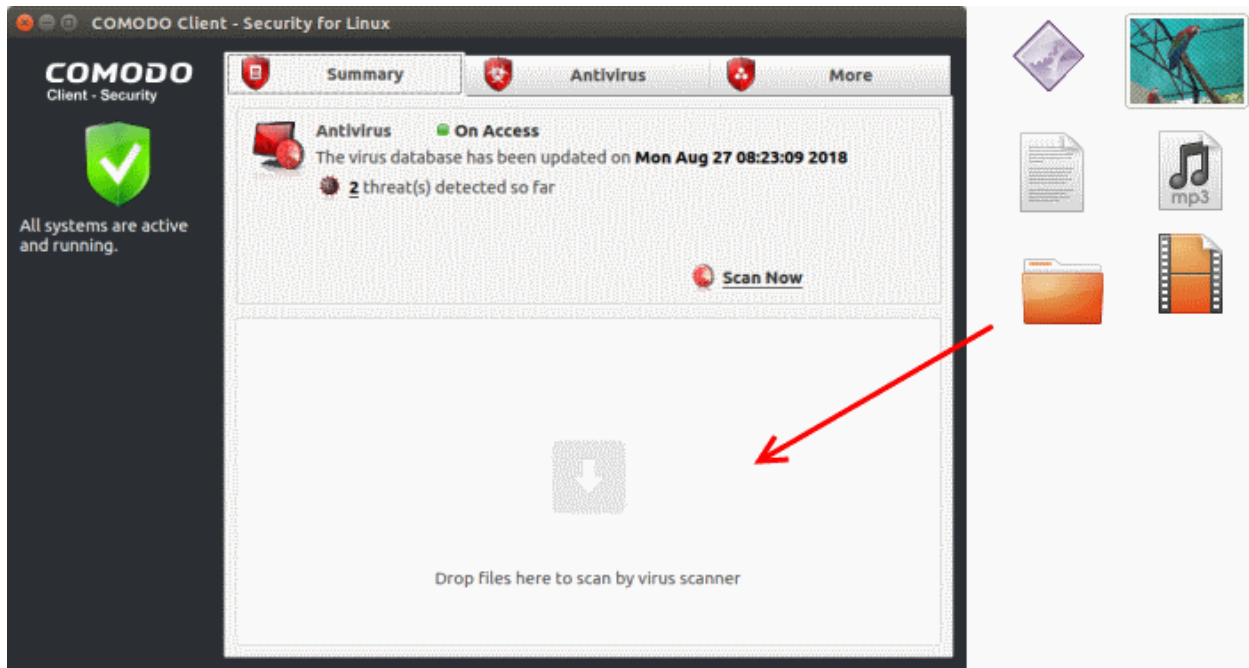
- Click 'Apply' in the scan profile dialog



You can also create profiles in the **Scan Profiles** area (open CCS > 'Antivirus' tab > 'Scan Profiles').

Instantly scan objects

- Drag items into the scan box on the summary screen.
- You can drag virtually any type of item - files, folders, photos, applications or drives.



3.2. Update Virus Database

Click 'Antivirus' > 'Update Virus Database'

The virus database must be kept up-to-date to ensure your system is constantly protected against threats.

There are two ways to download updates from Comodo's servers:

- **Download update manually**
- **Download update automatically**

Manually check for and download the latest updates

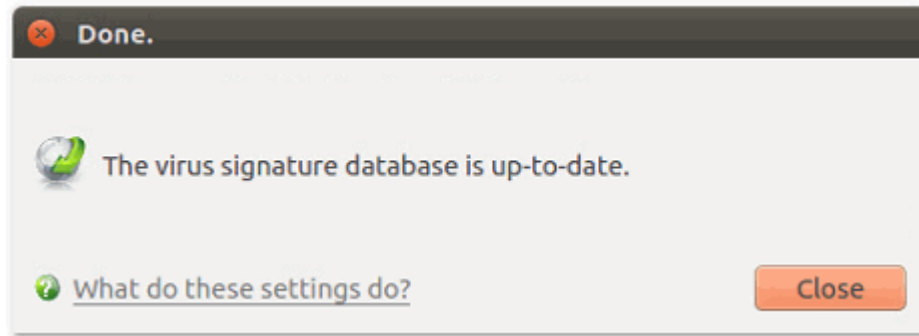
- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Update Virus Database' on the tasks screen

Note: You must be connected to internet to download the updates.

The following notifications are shown during the update process:



The following notification will appear when the update process is complete:



When infected or possibly infected files are found, if the anti-virus database has been not updated for a critically long time, or your computer has not been scanned for a long time, the main window of Comodo Client - Security recommends a course of action and gives a supporting explanation.

Automatic updates

- By default, CCS is set to automatically check for and download updates from the Comodo servers before commencing a scan of any type.
- You can configure CCS to download updates on a per-scanner basis in 'Scanner Settings'. See **Real Time Scan**, **Manual Scan** and **Scheduled Scan** for more details.
- 'Manual Scanning' refers to 'on demand' scans carried out on items when, for instance, they are dragged in the scan box or the Comodo dock icon.

3.3. Scheduled Scans

Click 'Antivirus' > 'Scheduled Scans'

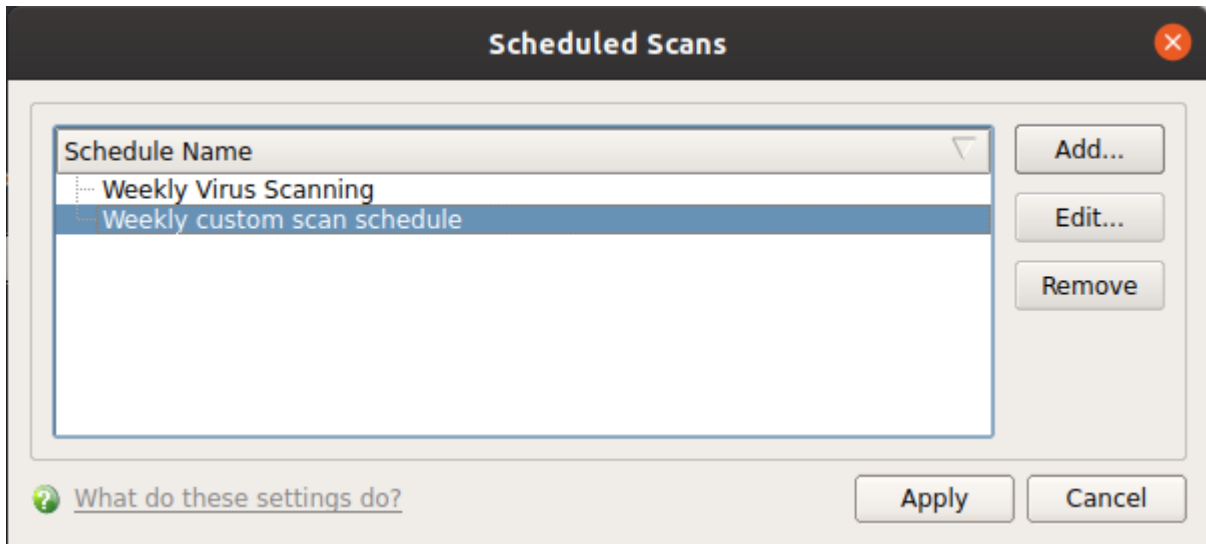
- The highly customizable scheduler lets you timetable virus scans according to your preference.
- You can schedule a scan of your entire computer or specific areas. You can create an unlimited number of schedules.
- You can run scans at daily, weekly, monthly or custom intervals.
 - Managed endpoints – scheduled scans should be configured in an Endpoint Manager profile.
- Click 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning' to configure general settings for scheduled scans.

See the following help to create a schedule in CCS:

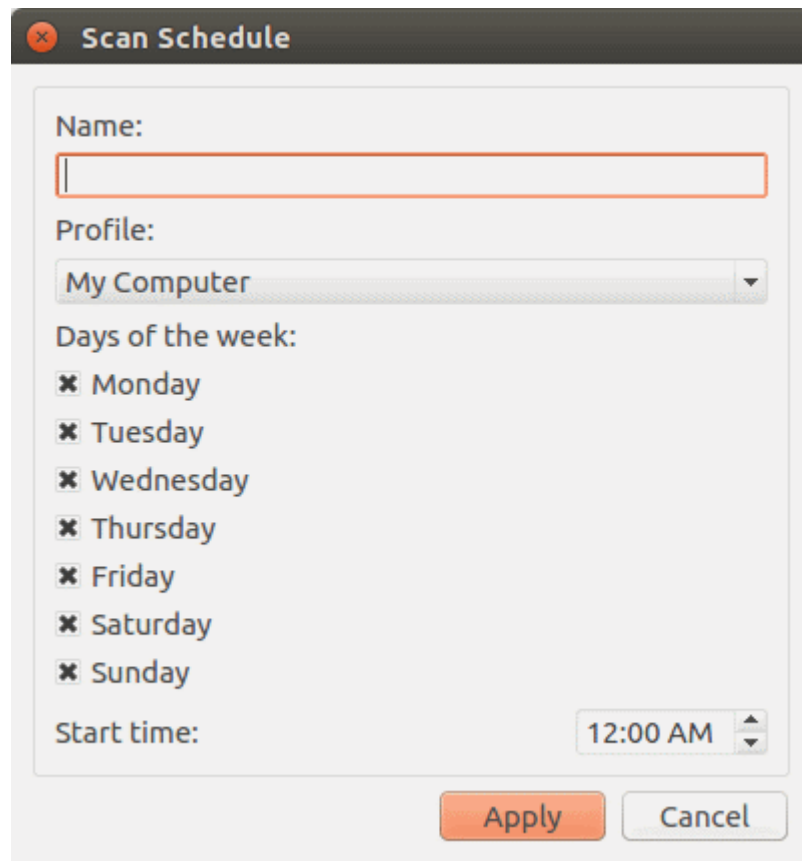
- **Create a scheduled scan**
- **Edit a pre-scheduled scan**
- **Cancel a pre-scheduled scan**

Create a scheduled scan

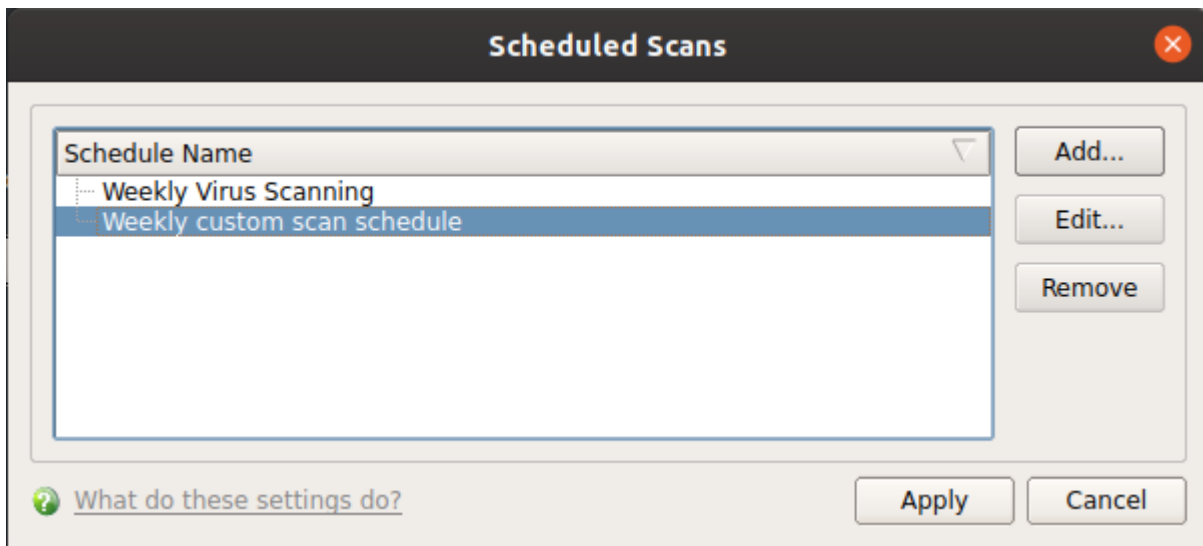
- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scheduled Scans' in antivirus tasks
- Click 'Add' to create a new schedule:



- Configure your schedule in the following settings screen:



- **Name** – Enter a label for the new schedule. E.g. 'Daily scan of external devices'
- **Profile** – The profile determines which areas of your computer are scanned. 'Full Scan' and 'Quick Scan' are the default options. You can also create your own profile of specific targets.
 - See [Scan Profiles](#) for help to create a custom scan profile.
- **Days of the week** – Select the weekdays the scan should run.
- **Start time** – Select the time the scan should start on the specified weekdays
- Click 'Apply'.



- Repeat the process to create more scan schedules.

Edit a scheduled scan

- Select the schedule from the list
- Click 'Edit' in the 'Scheduled Scans' setting panel
- Edit the necessary fields in the 'Scan Schedule' panel
- Click 'Apply'.

Remove a scheduled scan

- Select the scan schedule profile you wish to cancel
- Click 'Remove'.

3.4. Quarantined Items

Click the 'Antivirus' tab > 'Quarantined Items'

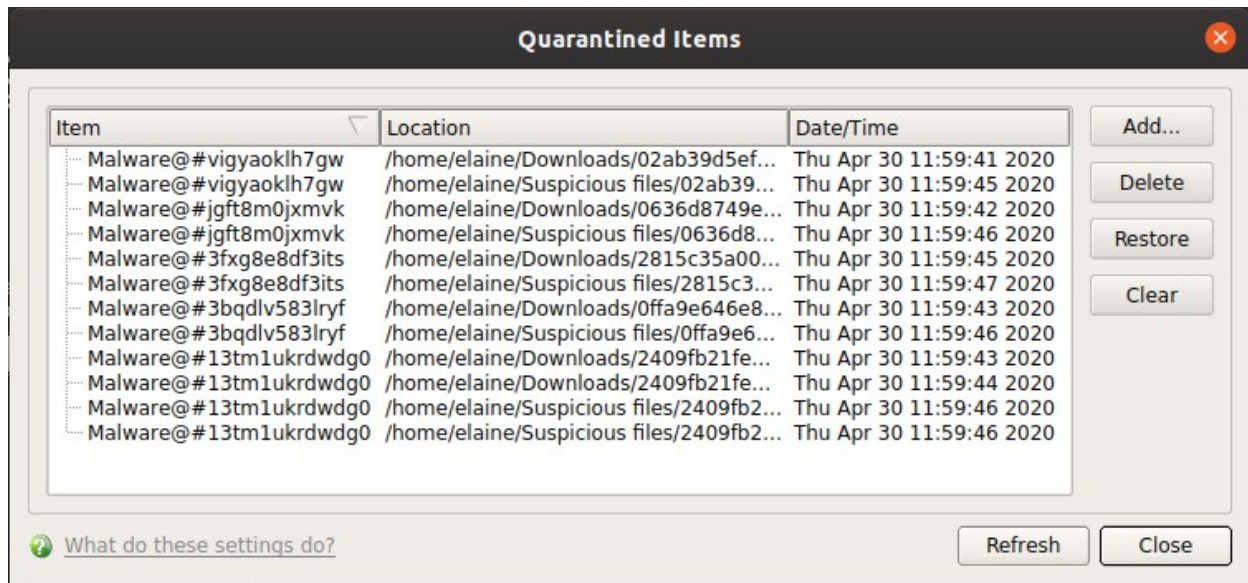
- Quarantine is an encrypted holding area for threats detected by the antivirus scanner
- Quarantined files cannot be executed, so they present no danger to your computer or data
- You can analyze the trustworthiness of these items and take actions like permanently remove them from your computer or restore them to their original location.

The quarantine interface lets you:

- **View quarantined items**
- **Manually quarantine files**
- **Delete quarantined items from your computer**
- **Restore a quarantined item**
- **Delete all quarantined items**

View quarantined items

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Quarantined Items'



- **Item** - The application or process that was quarantined
- **Location** - Path of the malicious item
- **Date/Time** - Date and time when the item was moved to quarantine.

Manually add files to quarantine

You can quarantine items that you suspect are malicious but were not detected by the scanner.

- Open Comodo Client Security
- Click 'Antivirus' > 'Quarantined Items'
- Click 'Add'
- Browse to the file you want to quarantine and click 'Open'

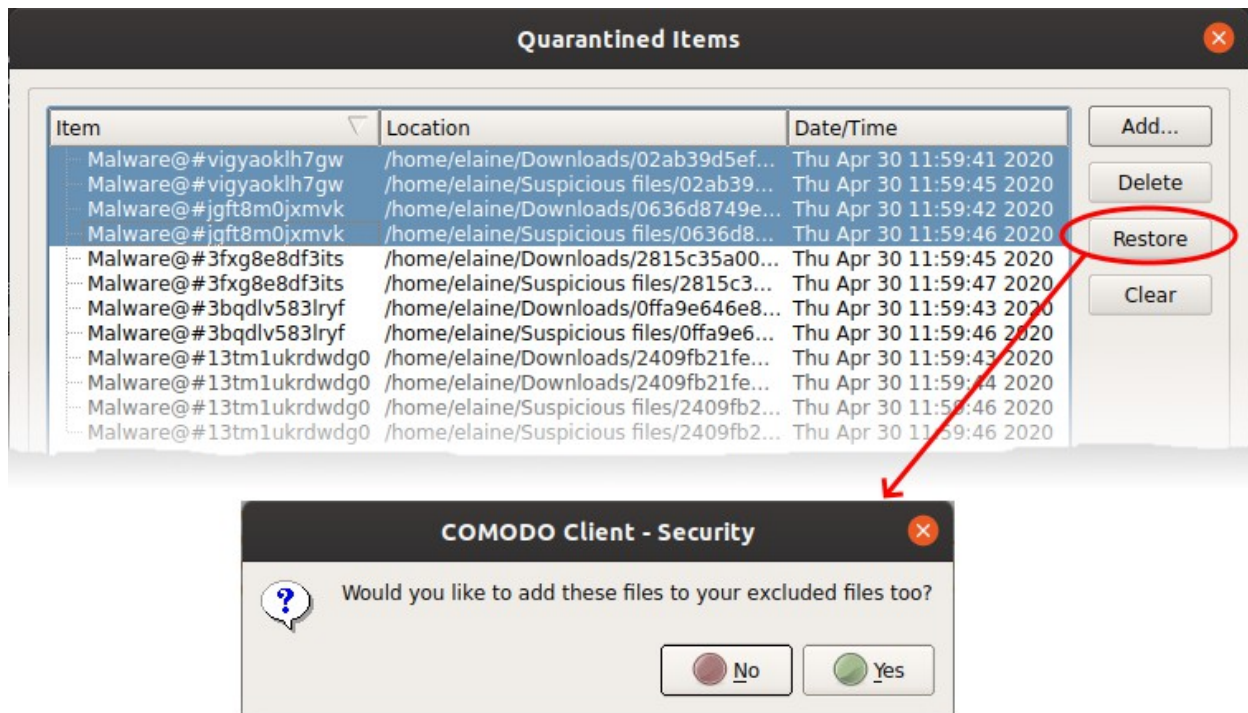
Delete quarantined items from your system

- Open Comodo Client Security
- Click 'Antivirus' > 'Quarantined Items'
- Select the item and click 'Delete'.

This deletes the file from your computer permanently.

Restore a quarantined item to its original location

- Open Comodo Client Security
- Click 'Antivirus' > 'Quarantined Items'
- Select the items to be moved back to their original locations and click the 'Restore'



You will be asked if you want to add the item to the Scan Exclusions list:

- **'Yes'** - The file is restored to its original location. It is not flagged as dangerous nor quarantined by future antivirus scans. You can manage excluded items in the Scanner Settings interface ('Antivirus' > 'Scanner Settings' > 'Exclusions'). See **Exclusions** for more details.
- **'No'** - The file is restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.

Permanently delete all quarantined items

- Open Comodo Client Security
- Click 'Antivirus' > 'Quarantined Items'
- Click 'Clear'.

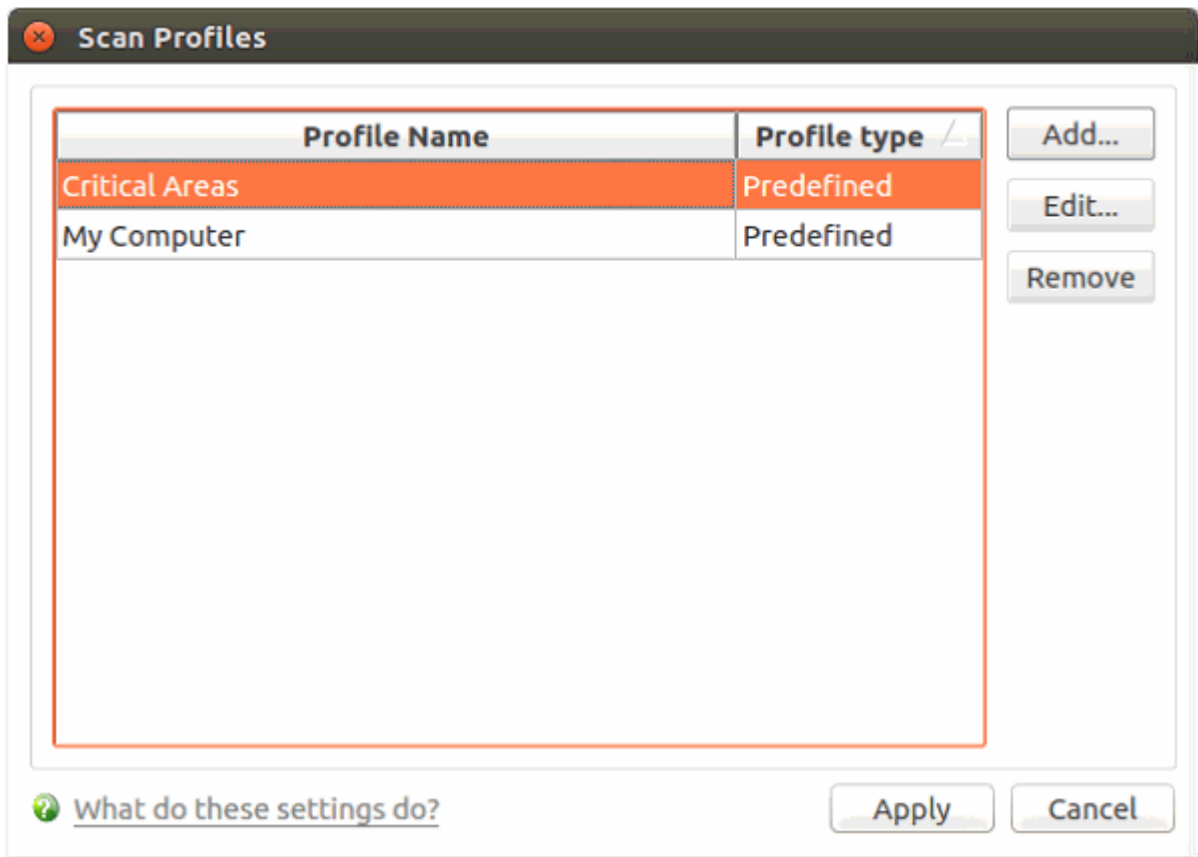
This deletes all quarantined items permanently.

3.5. Scan Profiles

- Scan profiles let you choose specific folders, drives or areas to scan. Once saved, you can apply a scan profile to a scheduled or on-demand scan.
- You can create as many custom scan profiles as you want
- Note: Managed endpoints – scan profiles should be configured in the Endpoint Manager profile.

Open the Scan Profiles interface

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scan Profiles'



CCS has two default profiles: 'Critical Areas' and 'My Computer'. These two profiles are predefined and cannot be edited or removed.

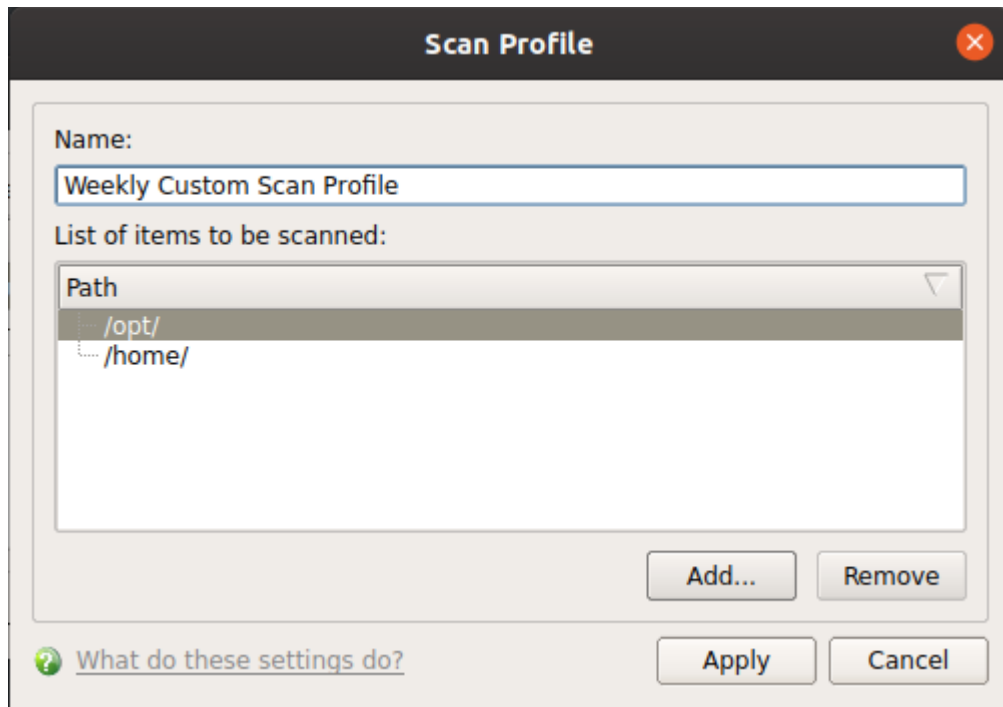
- **My Computer** - Scans every local drive, folder and file on your system.
- **Critical Areas** - A targeted scan of important operating system files and folders.

The following sections explain how to:

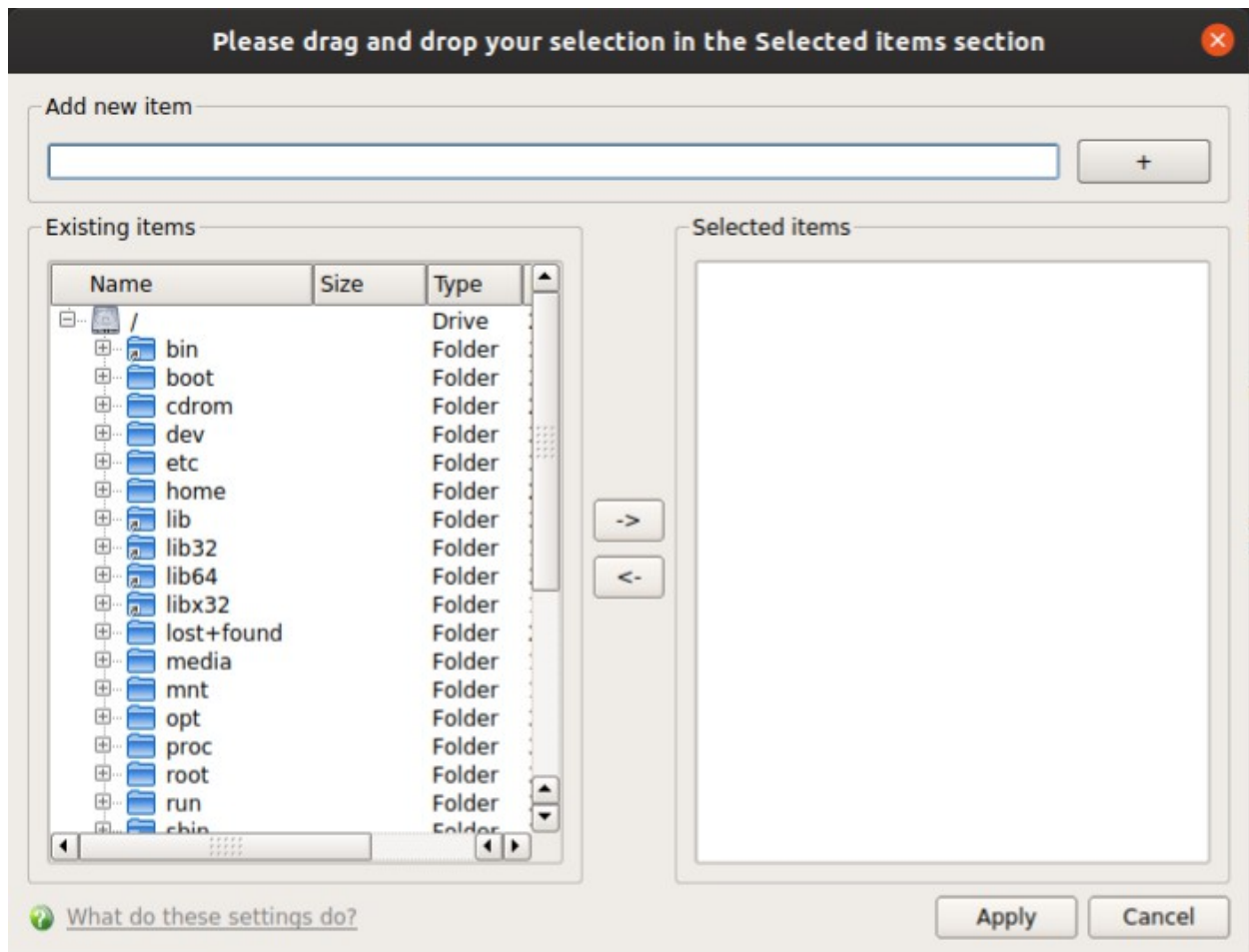
- **Create a scan profile**
- **Edit a scan profile**
- **Remove a custom scan profile**

Create a new scan profile

- Click 'Scan Profiles' in the 'Antivirus' tasks interface.
- Click 'Add'. The 'Scan Profile' dialog appears:



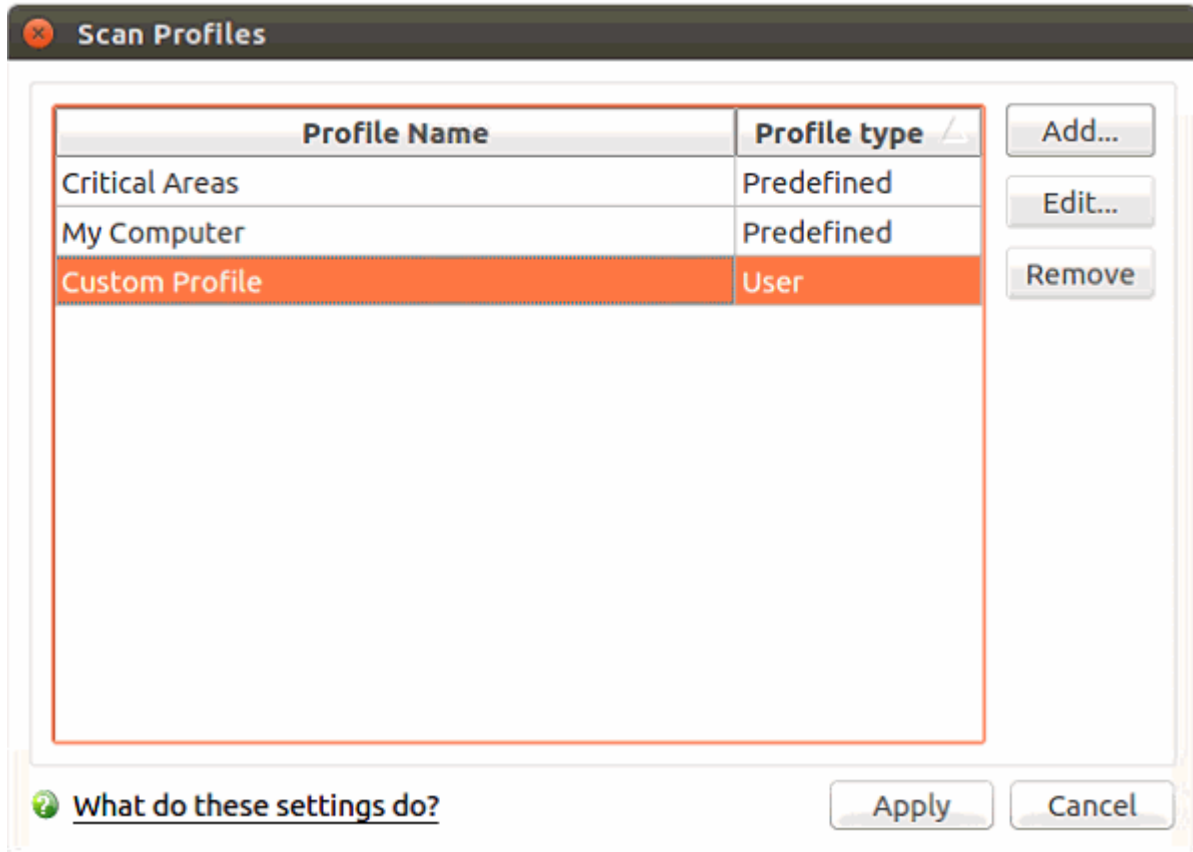
- **Name** – Enter a label for the scan profile.
- Click 'Add' to select the items you want to include in the scan.



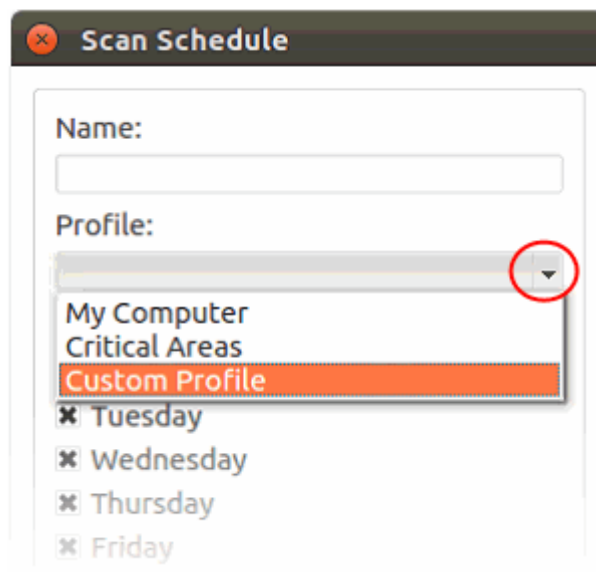
There are two ways to add scan locations:

- Manually enter the path in the 'Add new item' field. Click '+' to add the item.
- Drag and drop items from the left pane to the right pane. You can also use the arrow buttons.
- Click 'Apply'.
- Repeat the process to add more items.
- Click 'Apply' in the scan profile dialog

The new profile will be available in the 'Run a Scan' panel:



It is also available for selection during a scheduled scan. See [Scheduled Scans](#) for more details.



Edit a custom scan profile

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scan Profiles'
- Select the profile you want to update from the list and click 'Edit'. The procedure to update a scan profile is the same as adding a profile (explained above).

Remove custom scan profiles

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scan Profiles'
- Select the profile you want to remove from the list and click 'Remove'

Note: You cannot delete predefined scan profiles ('Critical Areas' and 'My Computer').

3.6. Scanner Settings

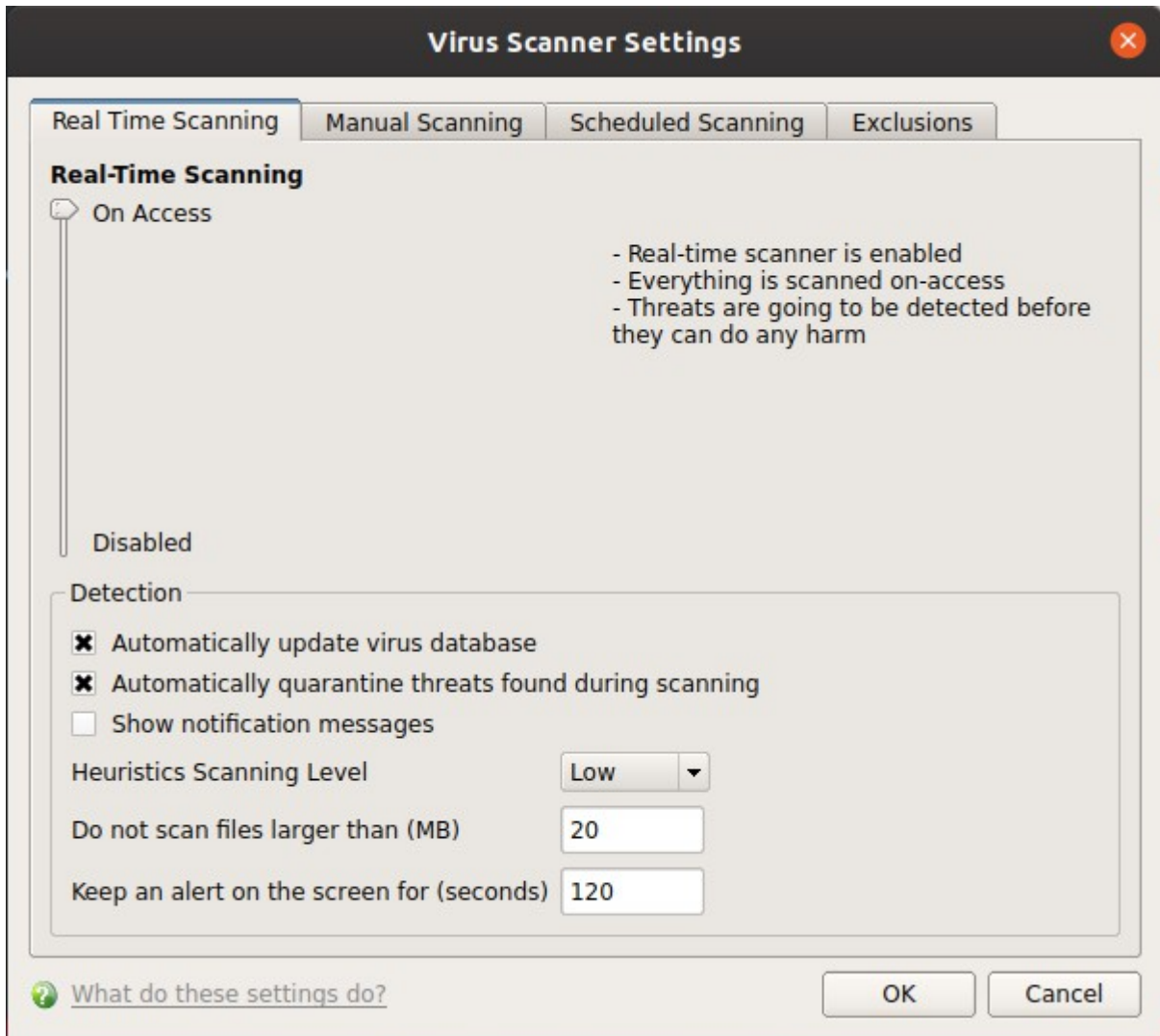
Click 'Antivirus' > 'Scanner Settings'

The settings area lets you configure real-time scans, manual scans, scheduled scans and exclusions.

- The settings you implement here will apply to all future scans of that type.
- Items added to 'Exclusions' are omitted from all types of scan
- Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile.

Open scanner settings

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scanner Settings'



Antivirus settings are broken down into the following areas:

- **Real Time Scan** - Configure the 'always-on' virus monitor
- **Manual Scan** - Configure on-demand scans
- **Scheduled Scan** - Configure a scan schedule
- **Exclusions** - View and manage items which will be skipped by virus scans.

3.6.1. Real Time Scan

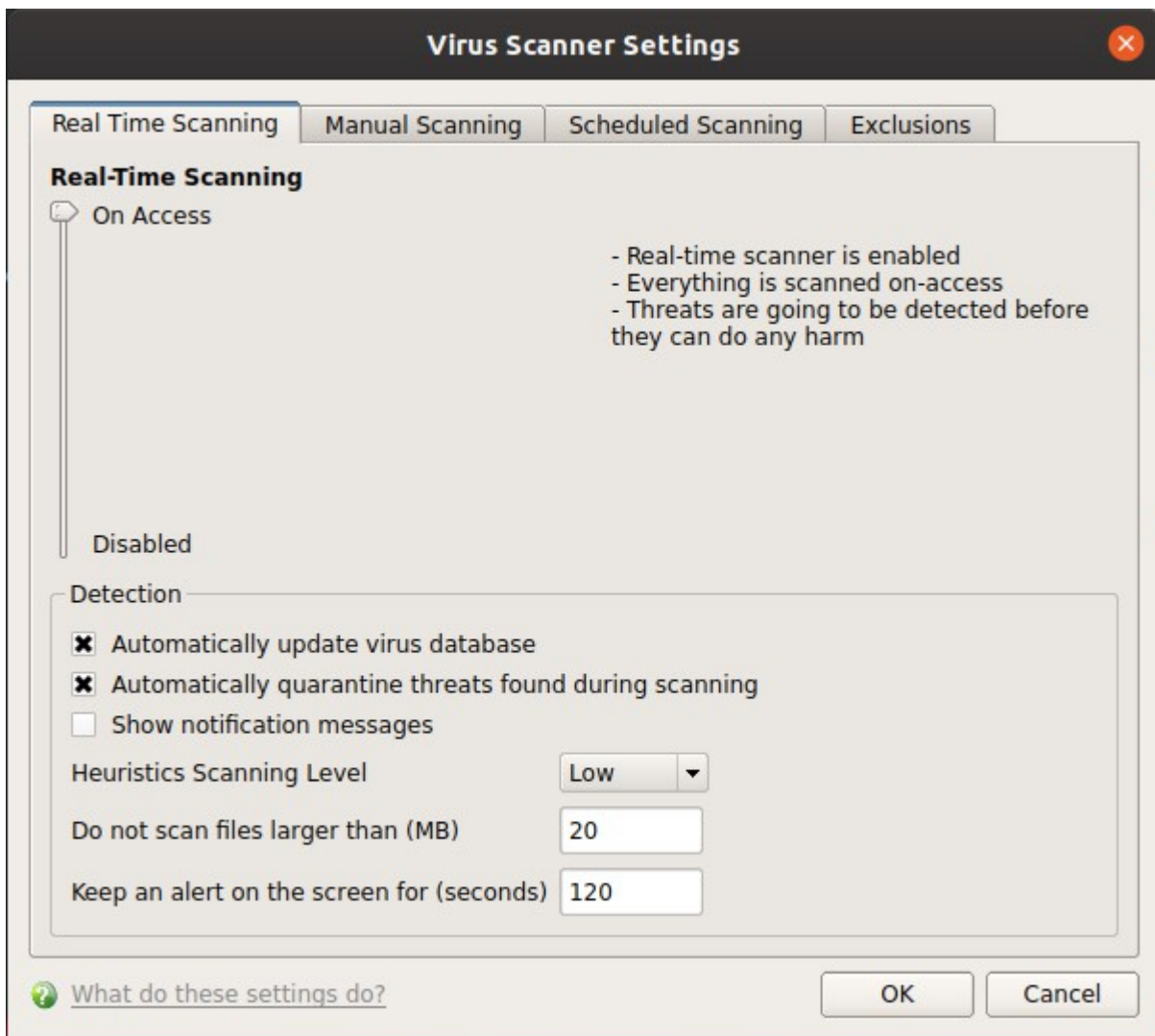
Click 'Antivirus' > 'Scanner Settings' > 'Real Time Scanning'

- The real-time scanner is the 'always on' virus monitor which runs in the background, checking files when they are opened, copied or downloaded.
- The real-time scanning area lets you enable or disable the scanner and configure scan options. We highly recommend you keep the real-time scanner active at all times.
- Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile.

Configure real time scan settings

- Open Comodo Client Security

- Click 'Antivirus'
- Click 'Scanner Settings' > 'Real Time Scanning':



Real-Time Scanning

- Use the slider to activate or deactivate the real-time virus monitor:
 - **On Access** - Any file opened is scanned before it is allowed to run.
 - **Disabled** - Switches the real-time scanner off.

Please note: Real-time scanning is not supported on Debian. This feature is not available on Debian.

Detection Settings

- **Automatically update virus database** - CCS checks for and downloads the latest database at system start-up and regular intervals thereafter (**Default = Enabled**).
However, some people like to have control over what gets downloaded and when it gets downloaded. Automatic updates may be inconvenient if you have a slower connection, or have many downloads going at the same time. Network admins may not want automatic downloads because they take up too much bandwidth during the day.
If you disable this option then you need to periodically select '**Update Virus Database**'.
- **Automatically quarantine threats found during scanning** - Whether or not CCS should automatically

take action against malware found by the scan. (**Default = Enabled**).

- **Enabled** = CCS moves detected malware into an encrypted holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system.
 - Click 'Antivirus' > 'Quarantined Items' to review quarantined files. You can restore items to their original location or permanently delete them.
- **Disabled** = CCS shows an alert when a malware is found, with its details. You can choose to clean the malware or to ignore the alert.
 - See **Understand CCS Alerts** for more details.
- **Show notification messages** – Alerts appear at the bottom-right of the screen whenever malware is found and moved to quarantine. Available only if 'Automatically quarantine threats found during scanning' is enabled. (**Default = Disabled**).
- **Heuristics Scanning Level** - Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the current virus database.

The drop-down menu lets you select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

- **Off** - Disable heuristic scanning. This means that virus scans only use the 'traditional' virus database to determine whether or not a file is malicious.
- **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts. Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (**Default**)
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives.
- **Do not scan files larger than** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here (**Default = 20 MB**).
- **Keep an alert on the screen for** - Specify the length of time that virus alerts should stay on the screen. (**Default = 120 seconds**).
- Click 'OK' to apply your changes.

3.6.2. Manual Scan

Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning'.

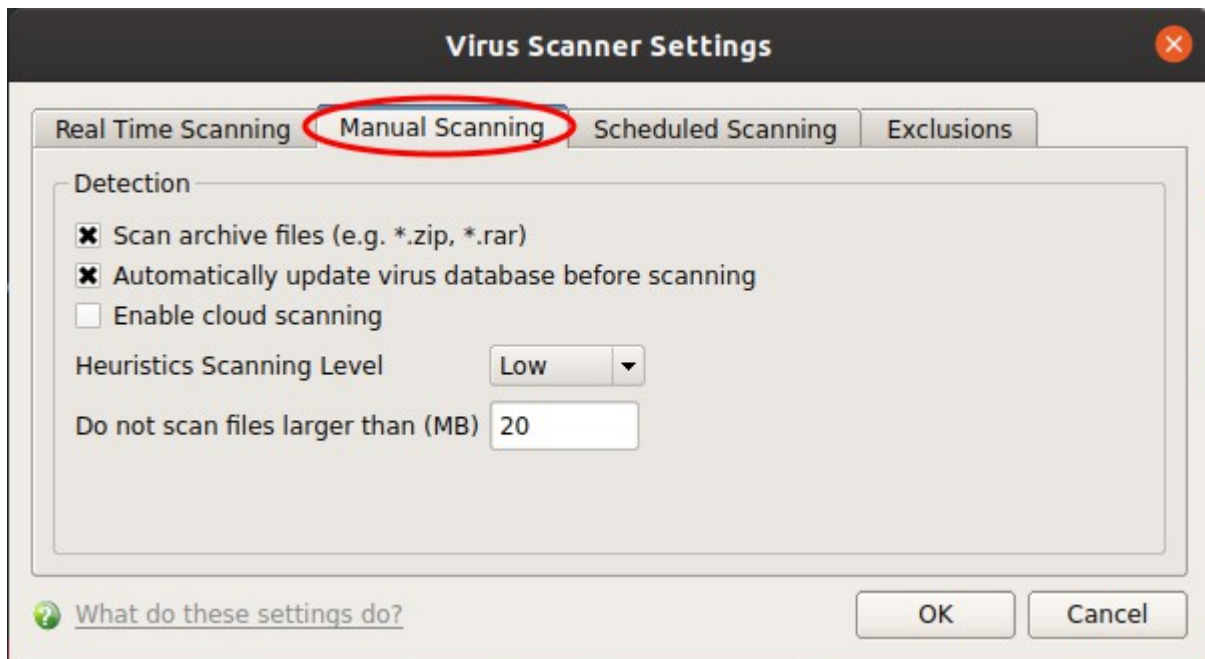
- Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile.

The options you set here will apply to all on-demand scans on your computer. For example, these settings will be used when:

- You click 'Scan Now' on the home screen then run a full or quick scan
- You scan an item by dragging it into the scan-box on the home screen
- You scan a file in the 'Run A Scan' from the 'Antivirus' menu

Configure manual scan settings

- Open Comodo Client Security
- Click 'Antivirus'
- Click 'Scanner Settings' > 'Manual Scanning':



- **Scan archive files** - The scan will include compressed file formats such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (**Default = Enabled**).
- **Automatically update virus database before scanning** - Check for and download the latest virus signature database prior to running a scan (**Default = Enabled**).
- **Enable cloud scanning** - Improves scan accuracy by augmenting the local scan with an online look-up of Comodo's latest virus database. Cloud Scanning means CCS can detect the latest malware even if your database is out-dated (**Default = Disabled**).
 - Note – This setting needs to be enabled if you want to submit unknown files to Valkyrie for analysis. Valkyrie is configured in an Endpoint Manager profile.
- **Heuristics Scanning Level** - Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the virus database.

The drop-down menu lets you select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

- **Off** - Disable heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether or not a file is malicious.
- **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts. Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users (**Default**).
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives.
- **Do not scan files larger than** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here (**Default = 20 MB**).
- Click 'OK' to apply your changes.

3.6.3. Scheduled Scan

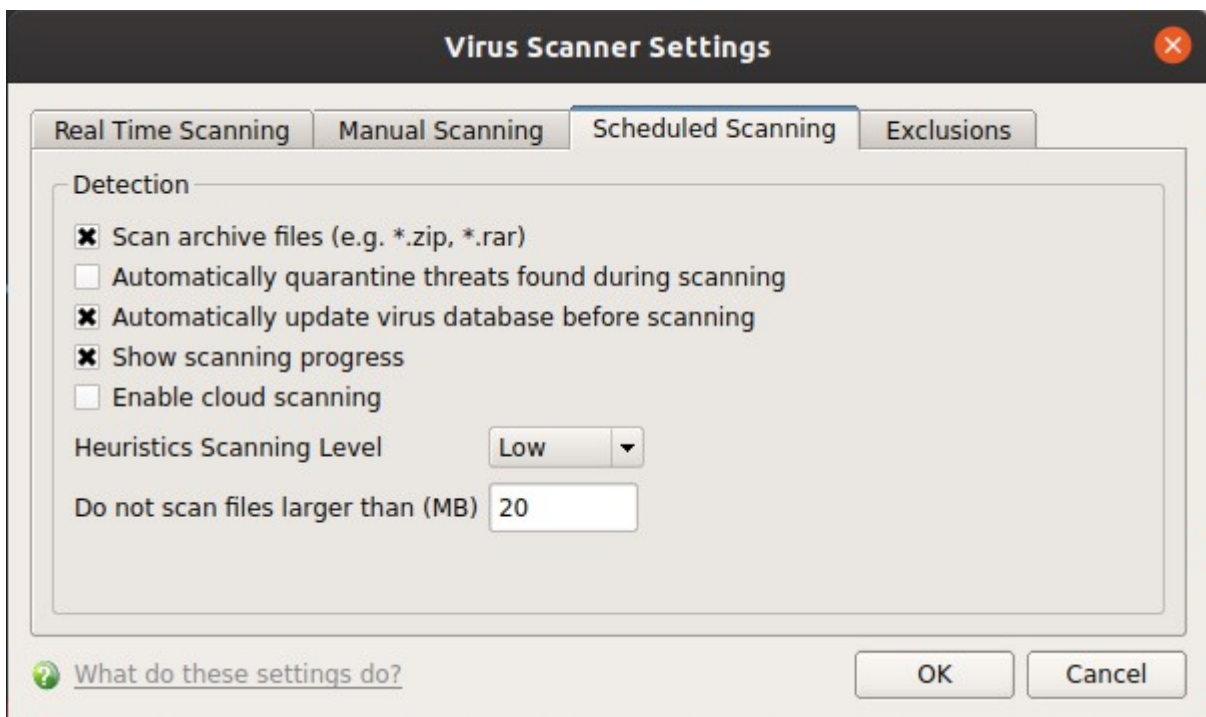
Click 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning'

The options you set in the 'Scheduled Scanning' tab will apply to all your scheduled scans. See [Scheduled Scans](#) for help to actually create a scan schedule.

- Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile.

Configure schedule scan settings

- Open Comodo Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click 'Scheduled Scanning':



The detection settings are as follows:

- **Scan archive files** - The scan will include compressed file formats such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives. (**Default = Enabled**).
- **Automatically quarantine threats found during scanning** - Whether or not CCS should automatically take action against malware found by the scan. (**Default = Disabled**)
 - **Enabled** = CCS moves detected malware into an encrypted holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system.
 - Click 'Antivirus' > 'Quarantined Items' to review quarantined files. You can restore items to their original location or permanently delete them.
 - **Disabled** = CCS shows a results screen at the end of the scan. The results screen lists all threats discovered by the scan and provides controls for you to deal with them. See [Scan Progress and Results](#) screen in [Run a Scan](#) for more details.
- **Automatically update virus database before scanning** - Check for and download the latest virus database prior to running a scan. (**Default = Enabled**).
- **Show scanning progress** – A progress bar is shown on start of a scheduled scan. Clear this box if

you do not want to see the scan progress status. (**Default = Enabled**).

- **Enable cloud scanning** - Improves scan accuracy by augmenting the local scan with an online look-up of Comodo's latest virus database. Cloud Scanning means CCS can detect the latest malware even if your virus database is out-dated. (**Default = Enabled**).
 - Note – This setting needs to be enabled if you want to submit unknown files to Valkyrie for analysis. Valkyrie is configured in an Endpoint Manager profile.
- **Heuristics Scanning Level** - Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the virus database.

The drop-down menu lets you select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

- **Off** - Disable heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether or not a file is malicious.
- **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts. Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (**Default**)
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives.
- **Do not scan files larger than** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (**Default = 20 MB**).
- Click 'OK' to apply your changes.

3.6.4. Exclusions

Click 'Antivirus' > 'Scanner Settings' > 'Exclusions'

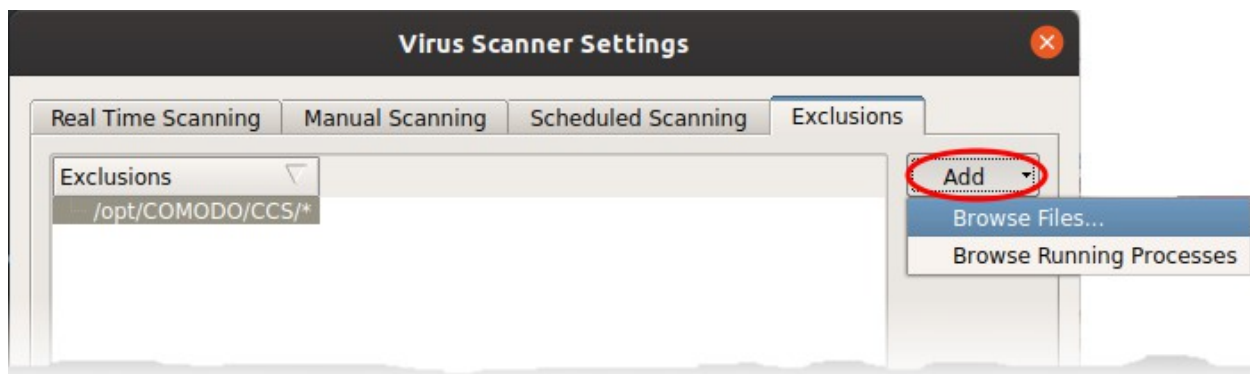
- The exclusions area shows files and paths that you have chosen to skip during virus scans.
- CCS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.
- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.
- Use this interface to add or remove exceptions.
- Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile.

Add scan exclusions

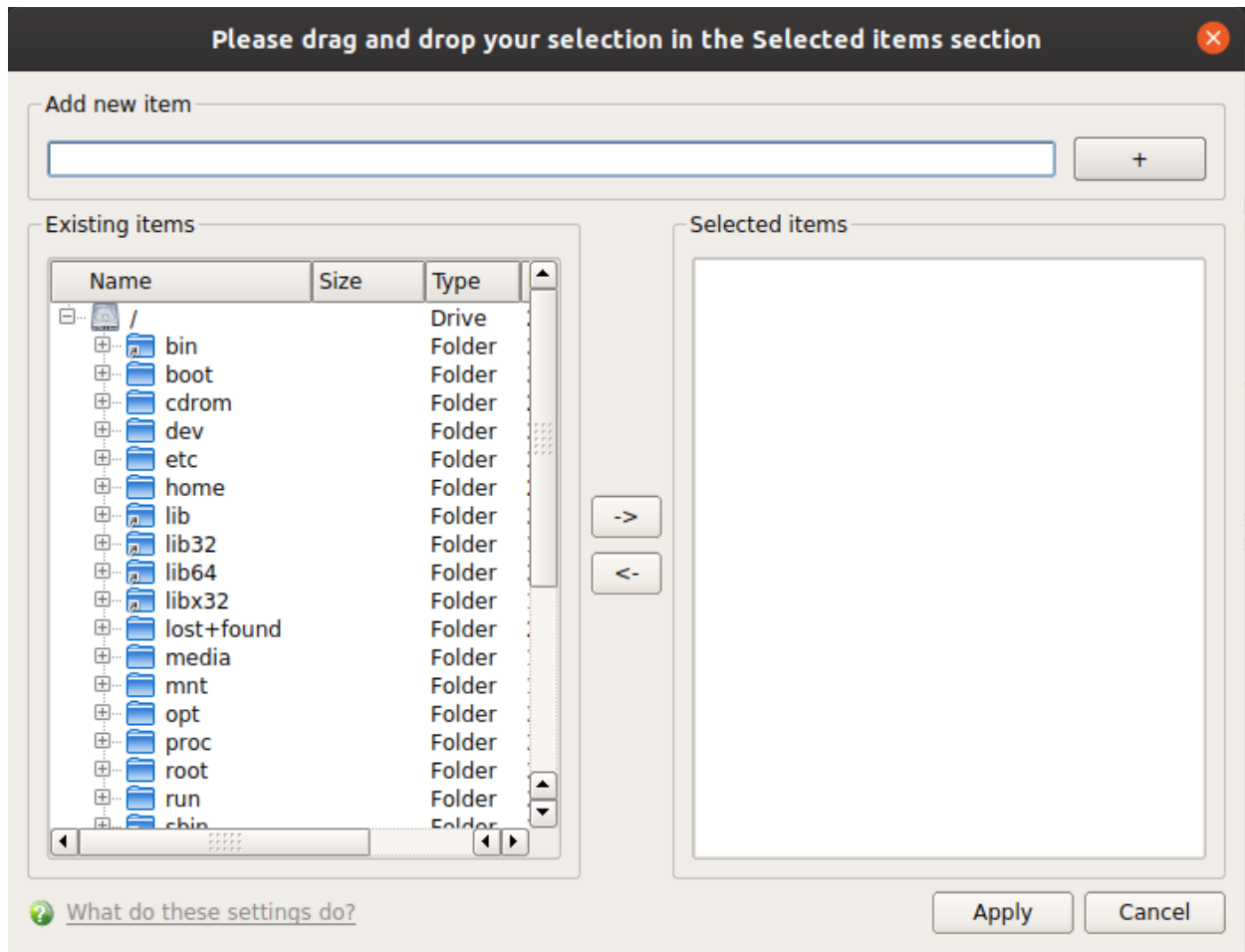
- Open Comodo Client Security
- Click 'Antivirus'
- Click 'Scanner Settings' > 'Exclusions':



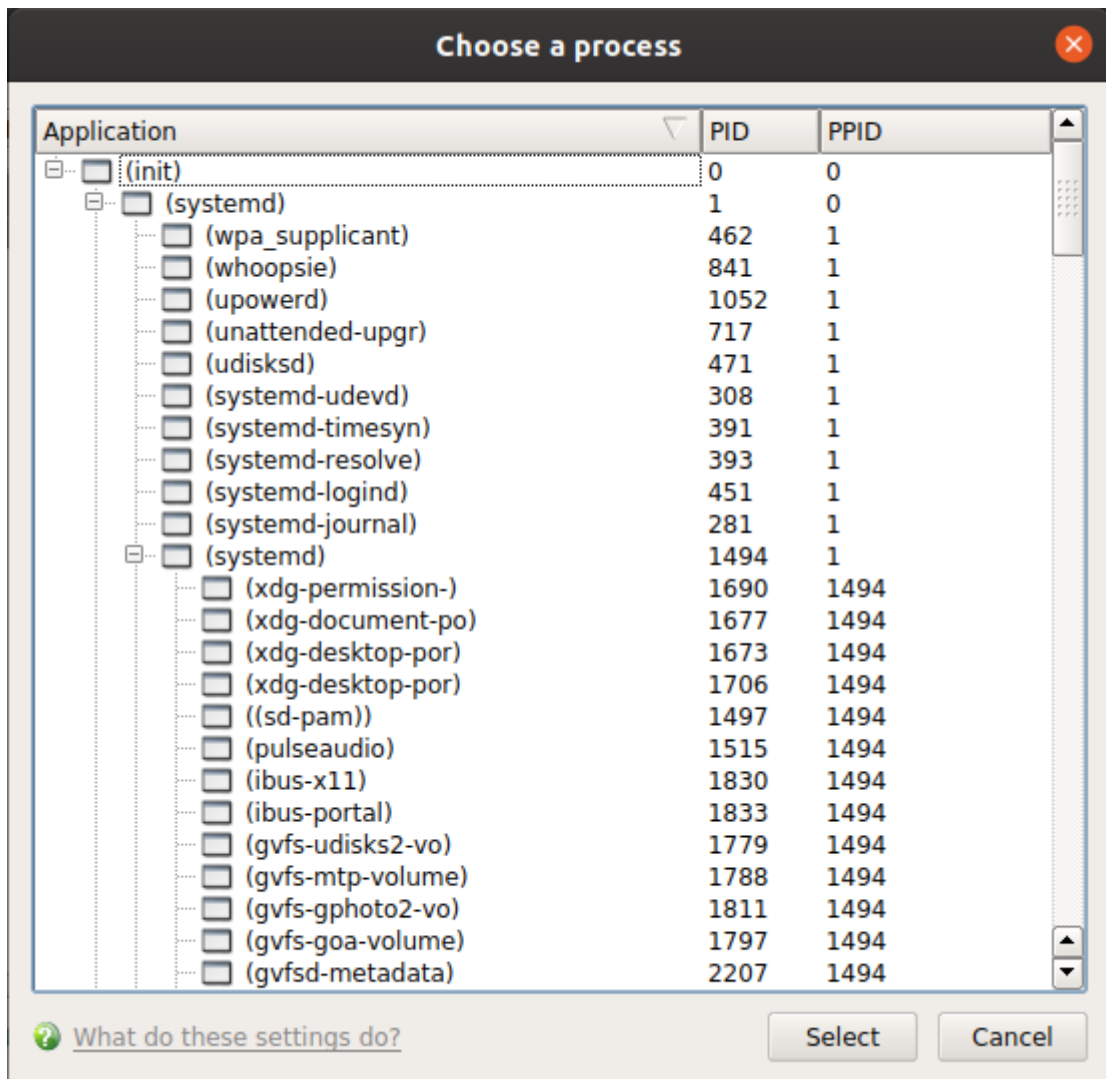
- Click the 'Add' button.
- There are two ways to choose the application that you want to exclude:



- **Browse Files...** - Browse to the file you want to exclude.



- **Browse Running Processes** - Choose the target application from a list of processes running on your PC. The parent file of the process is added to exclusions.



- Click 'OK' to register your exclusions.

4. More Options – Introduction

- Click the 'More' tab on the CCS home-screen to open this interface
- You view and modify various program settings
- You can use utilities and shortcuts to help enhance your experience with Comodo Client Security

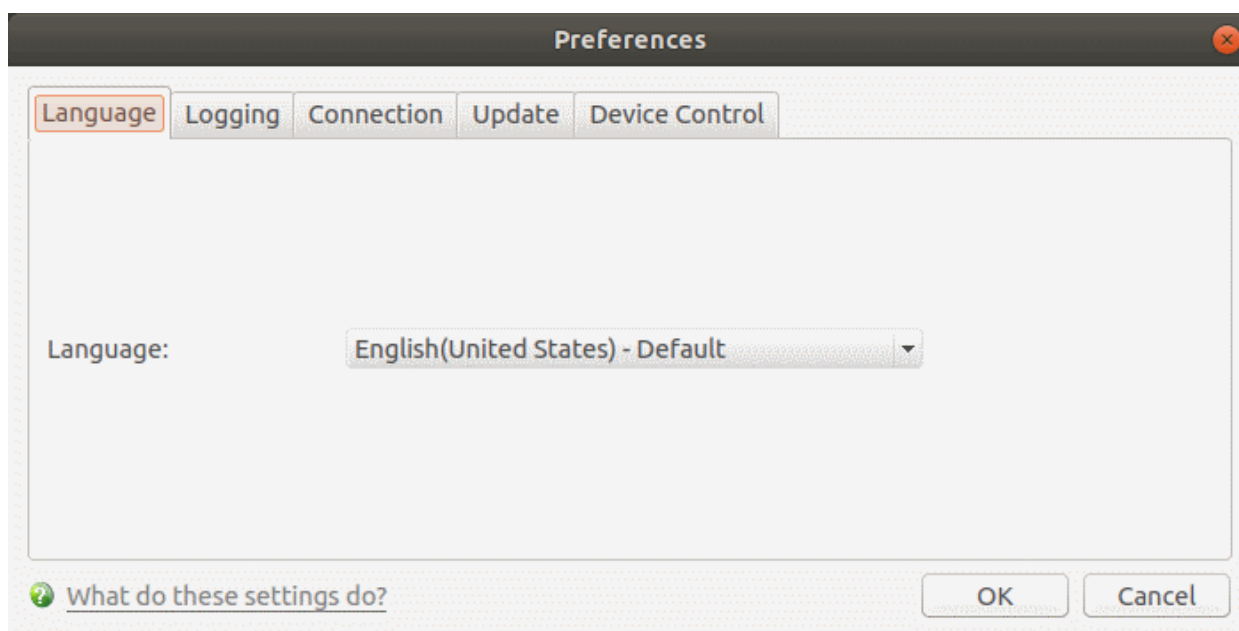


The following sections explain about each option in detail:

- **Preferences** - Configure general CCS settings (interface language, log storage, update options, external device control, and so on).
- **Manage My Configurations** - Manage, import and export CCS security settings as configuration profiles.
- **Diagnostics** - Identify any problems with your installation.
- **Browse Support Forums** - Links to Comodo User Forums.
- **Help** - The online help guide.
- **About** - Version and copy-right information about the product.
- **View Antivirus Events** - Manage logs of all antivirus events including files intercepted by real-time protection, manual scans, virus signature database updates and more.

4.1. Preferences

- Open Comodo Client Security
- Click 'More' > 'Preferences' tab
- The preferences area lets you specify top-level settings regarding the interface.
- This include updates, language, event logs, external devices, and more.



Click the following for more information:

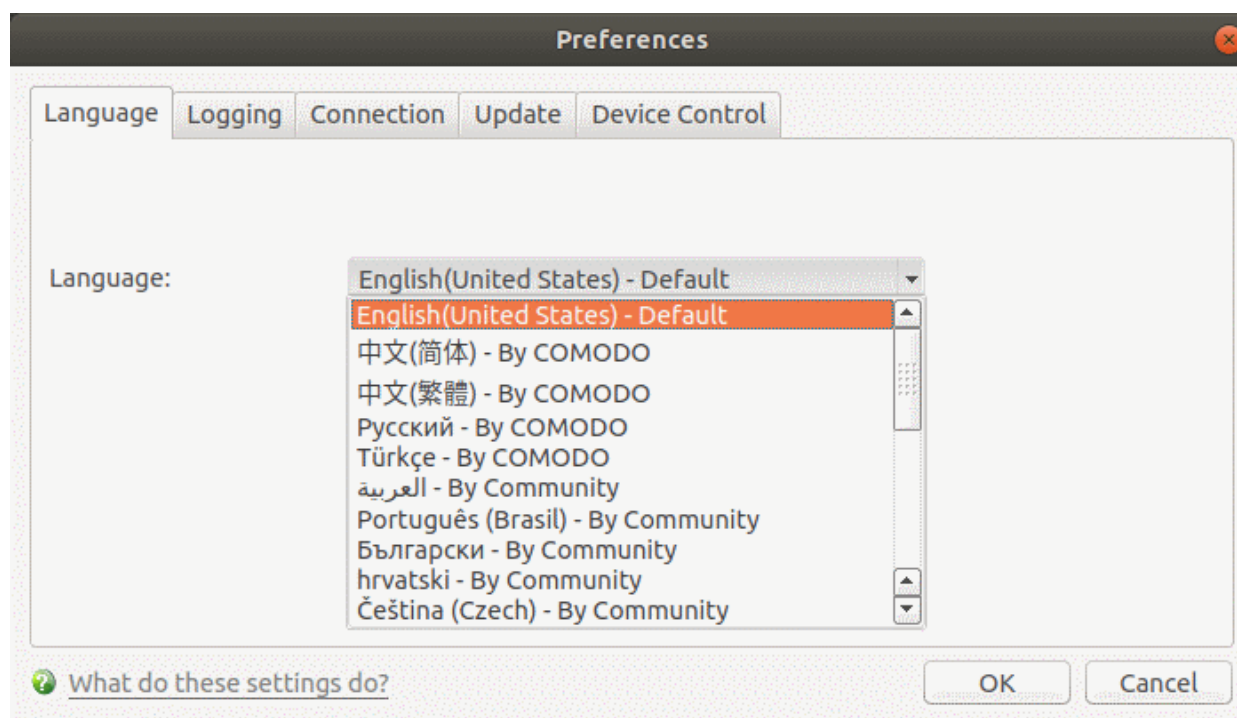
- [Language](#)
- [Logging](#)
- [Connection](#)
- [Update](#)
- [Device Control](#)

4.1.1. Language Settings

Click 'More' > 'Preferences' > 'Language'

The language tab lets you choose the language which is shown in the CCS interface.

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Language':



- **Language** - Choose your preferred language from the drop-down (**Default = English (United States)**).
- Click 'OK'
- You must restart the application for the change to take effect.

4.1.2. Log Settings

Click 'More' > 'Preferences' > 'Logging'

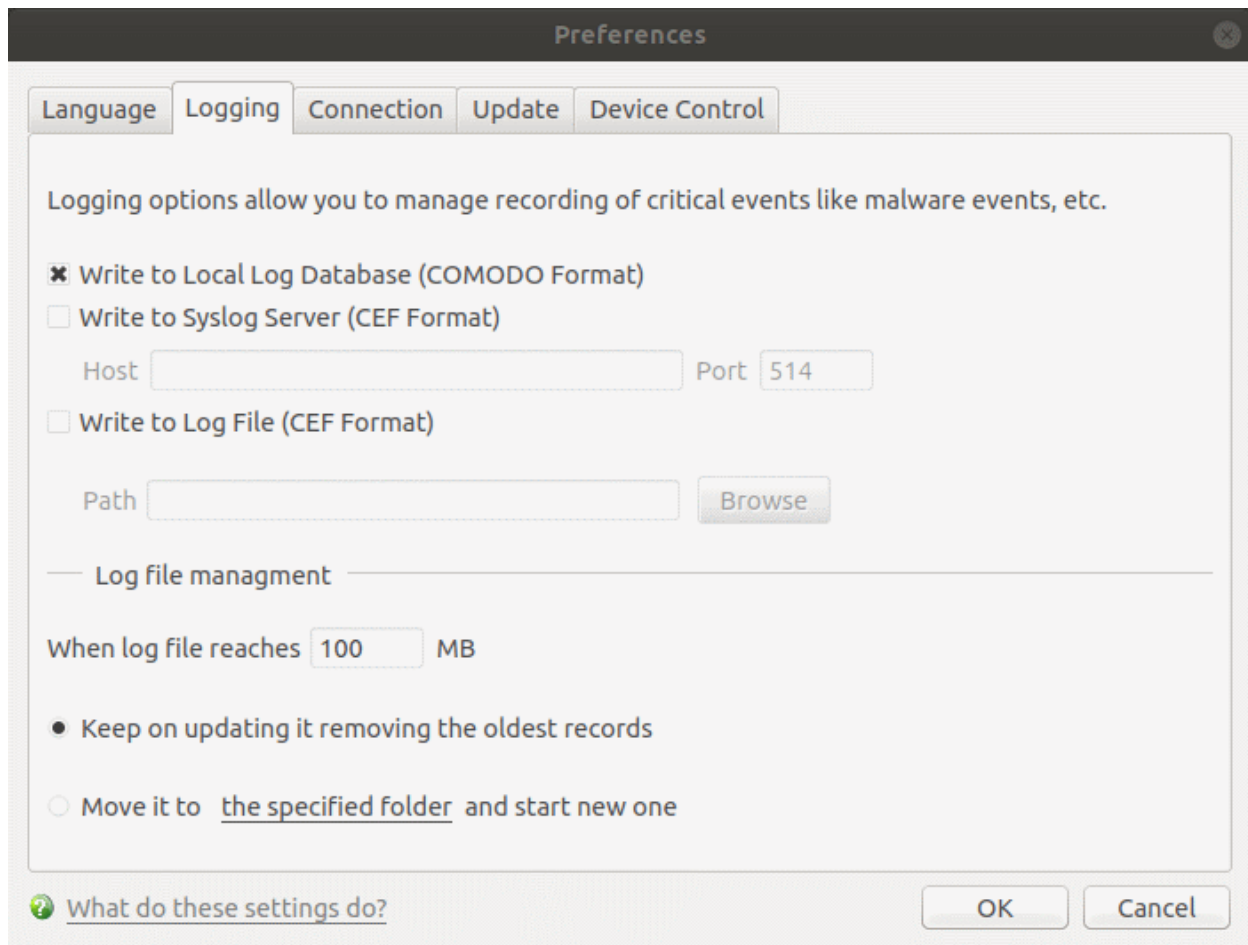
- Logs are a record of antivirus events. For example, a log entry is created when CCS detects a piece of malware.
- CCS logs all events by default. You can view the logs themselves in 'More' > 'View Antivirus Events'.

The log settings area lets you:

- Enable or disable logging.
- Configure how CCS should behave once a log file reaches a certain size.
- Configure how logs should be written (to file and/or to syslog server)

Configure logging settings

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Logging':



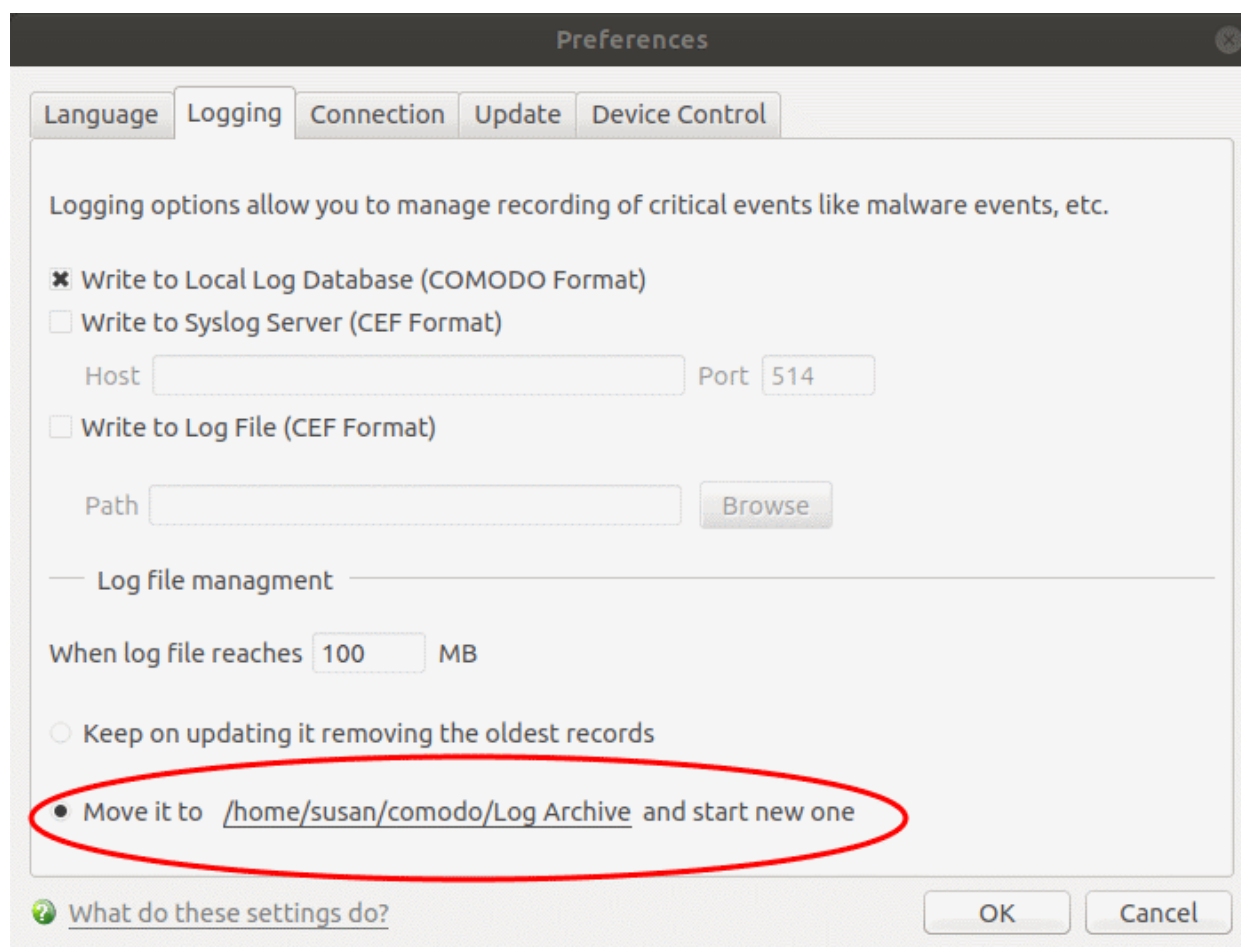
General Log File Options

- **Write to Local Log Database (COMODO format)** - CCS records events in a local database. Log storage depends on the settings in the log file management section below. **(Default = Enabled)**
- **Write to Syslog Server (CEF Format)** - CCS forwards the logs to an external Syslog server integrated with Endpoint Manager (EM). Enter the IP/hostname and port of the Syslog server in fields provided. **(Default = Disabled)**.
 - **Host** – Specify the server details (IP or host name)
 - **Port** – Enter port number at which CCS will connect to the Syslog server
- **Write to Log File (CEF Format)** - CCS stores the logs at a specific location. Click 'Browse' to select the storage location **(Default = Disabled)**.
 - **Path** - Specify the location in the local computer (network path not supported)

Log File Management

- **When log file reaches (MB)** - Configure how to handle a log file when it reaches a certain size.
 - **When the log file reaches** - Specify the maximum size of a log file **(Default = 100 MB)**.
 - **Keep on updating it removing the oldest records** - When a log file reaches the max. size, CCS will delete the earliest log entries to make room for the new entries. **(Default = Enabled)**
 - **Move it to the specified folder** - When a log file reaches the max. size, CCS starts a new log file and moves the old one to a folder of your choice. **(Default = Disabled)**
 - Select the option and click 'the specified folder' to choose the storage folder:

The selected folder path will appear beside 'Move it to':



Once the log file reaches the maximum size, it is automatically moved to the selected folder. A new log file is created with events occurring from that instant.

- Click 'OK' to save your settings.

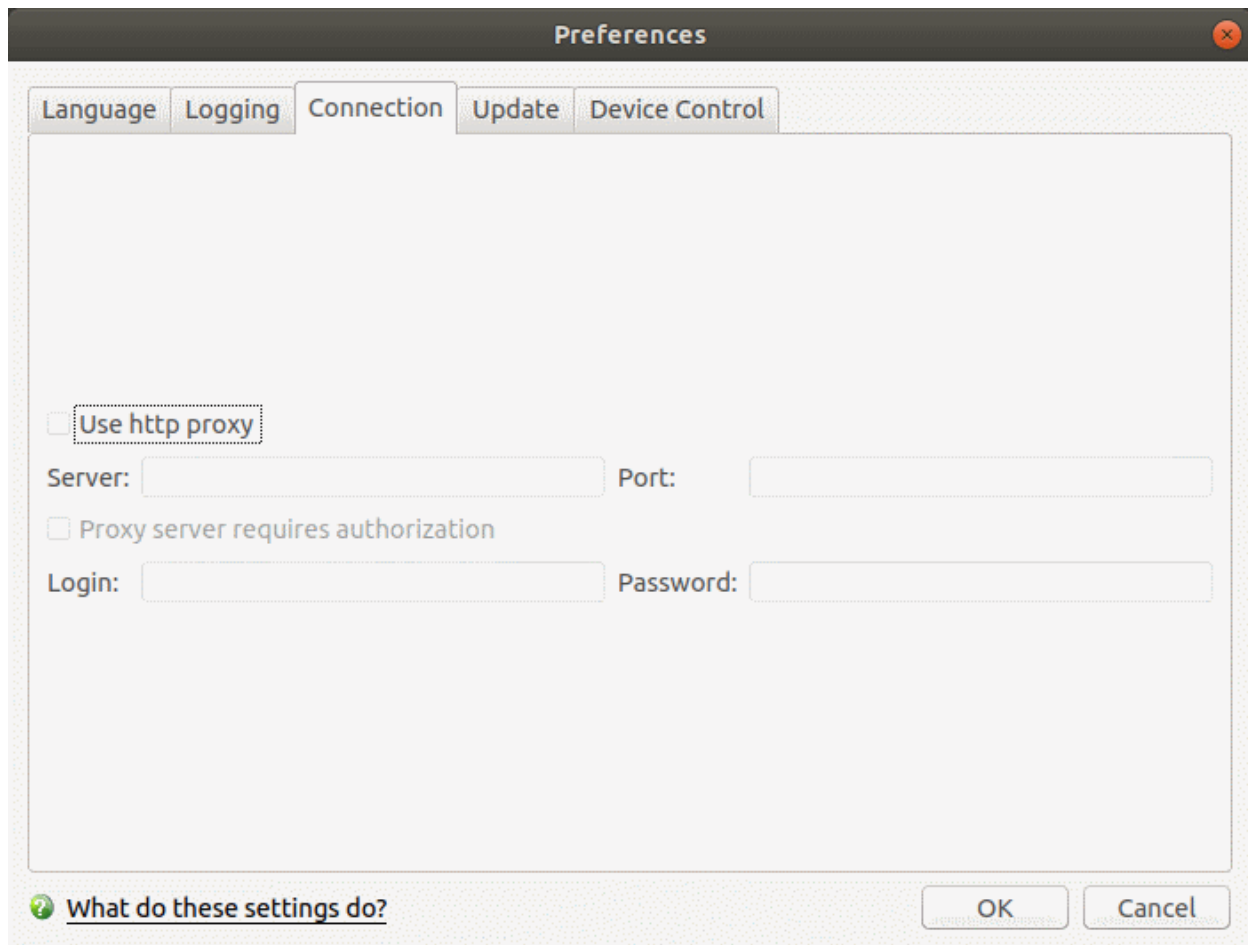
4.1.3. Connection Settings

Click 'More' > 'Preferences' > 'Connection'

- The connection area lets you configure how CCS should connect to Comodo servers in order to receive antivirus database updates.
- This is useful if you want CCS to connect through a proxy server

Configure proxy connection settings to receive virus signature database updates

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Connection':



- **Use http proxy** – CCS connects to a proxy server to download updates (**Default = Disabled**)
 - **Server** – Specify proxy server details (IP address or name)
 - **Port** – Enter the port number via which the proxy server will connect to Comodo servers
- **Proxy server requires authorization** - If required, enter appropriate credentials in the fields provided (**Default = Disabled**).
- Click 'OK' to save your settings.

4.1.4. Update Settings

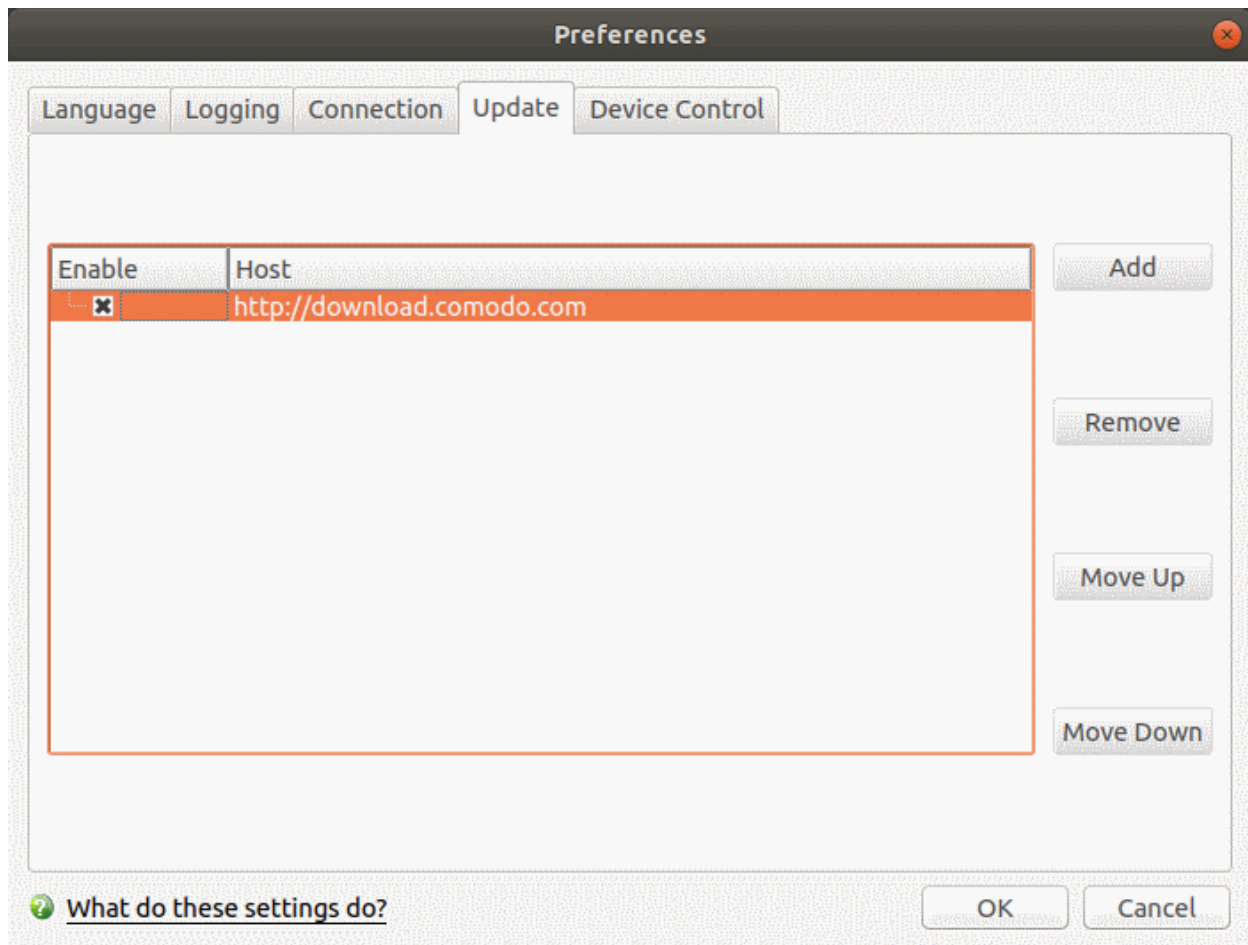
Click 'More' > 'Preferences' > 'Update'

The update area lets you:

- Enable or disable automatic virus database updates
- Choose the host from which updates should be downloaded. Default = <https://download.comodo.com>.

Configure update settings

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Update':



- By default, CCS downloads updates direct from Comodo servers. Alternatively, admins can download updates to a local server first.
- Individual endpoints can then fetch updates from this local server instead of from Comodo servers. This helps save bandwidth and accelerates updates when a large number of endpoints are involved.

Note: You need to install the 'ESM Update Mirror' utility to download updates to the local server.

- 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

Add a host:

- Click 'Add' and enter the URL or IP address of the host in the next row that appears.
- Repeat the process to add multiple hosts.
- Use 'Move Up' and 'Move Down' buttons to re-order the priority of host.
- CCS for Linux will automatically check the host specified here and download updates from the host even when you are offline.
- Click 'OK' for your settings to take effect.

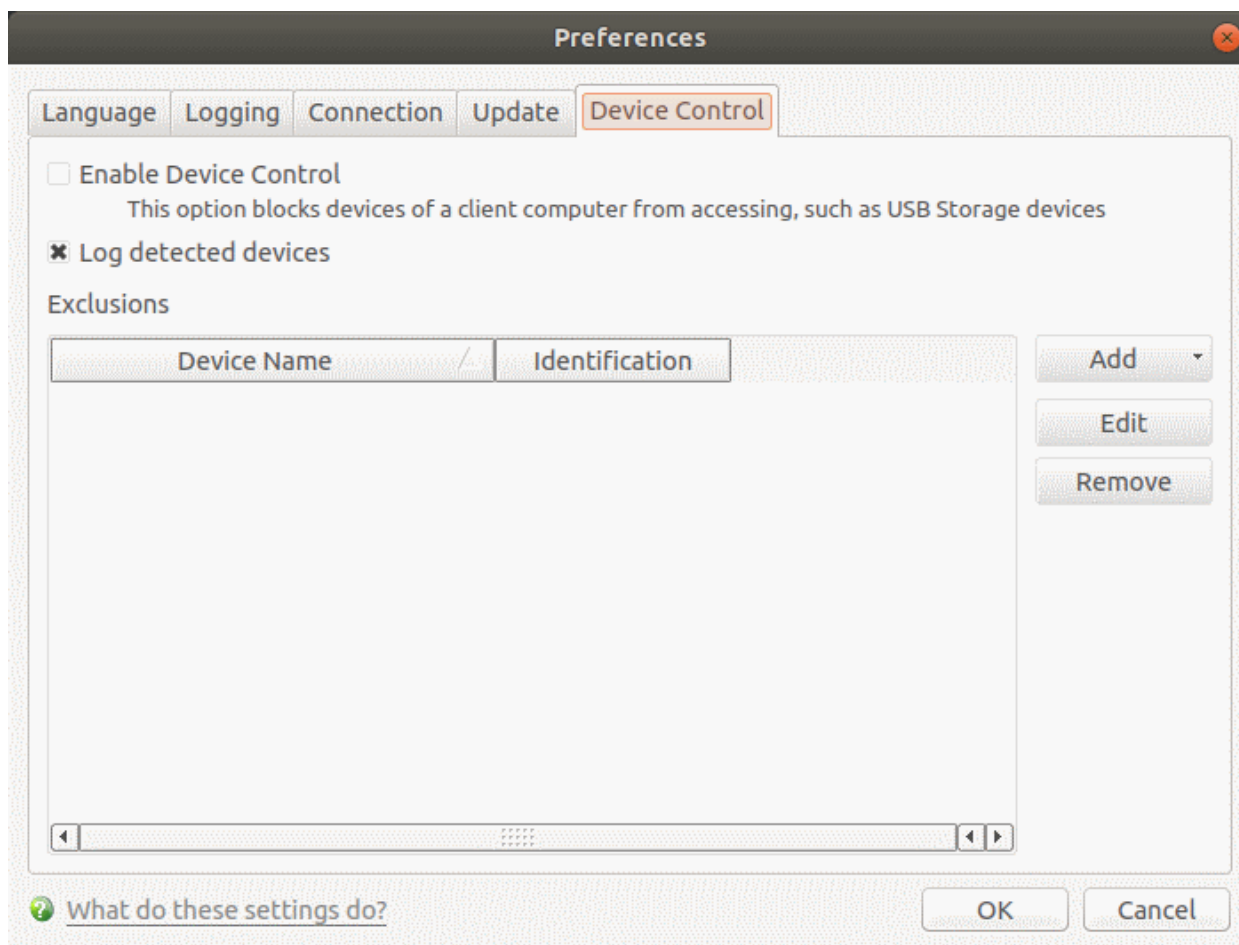
4.1.5. External Device Control Settings

Click 'More' > 'Preferences' > 'Device Control'

- Device control lets you block access to external devices like USB sticks and external drives.
- You can also define exclusions for selected devices. The selected devices will be allowed to connect, but all others will be blocked.

Configure device control

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Device Control':



- **Enable Device Control** - Prohibits access to external storage devices like USB cards and external drives. You can define exclusions to allow selected devices to connect (**Default = Disabled**).
- **Log detected devices** - All device connection / disconnection events, whether allowed or blocked, are added to CCS logs. You can view the logs in the 'Log Viewer' module (**Default = Enabled**).
 - Click 'More' > 'View Antivirus Events' > 'More' > 'Device Control Events'
 - See **Device Control Logs** for more details.
- **Exclusions** - Add exceptions to device control. Devices specified here are allowed access to your computer even if 'Device Control' is active. For example, if your company uses USB tokens to authenticate remote VPN connections, you should create exceptions for those tokens.

Add exclusions

You can specify the exceptions in two ways:

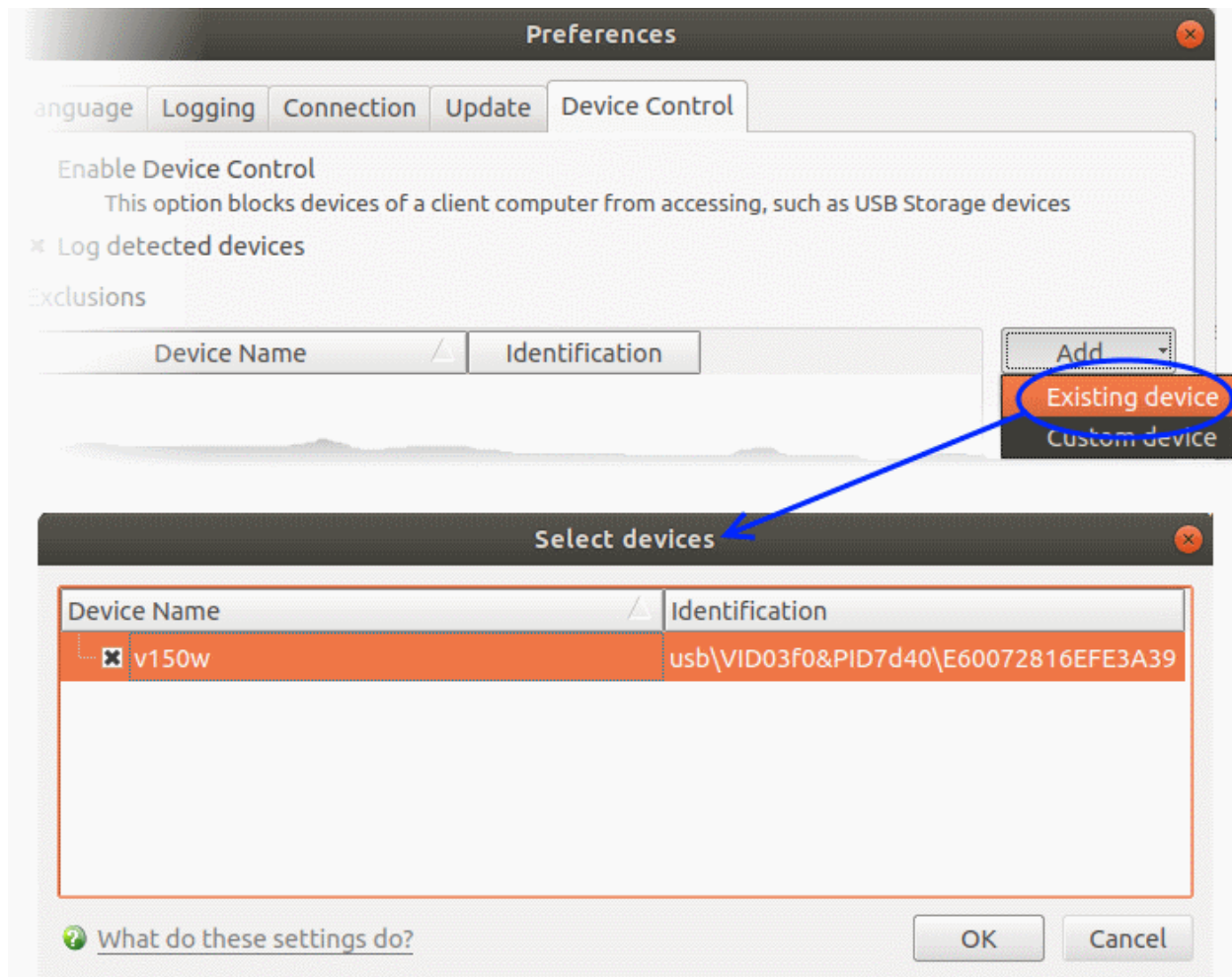
- **Select from currently connected devices**

- **Specify a custom device**

Connect a device then create an exclusion for it

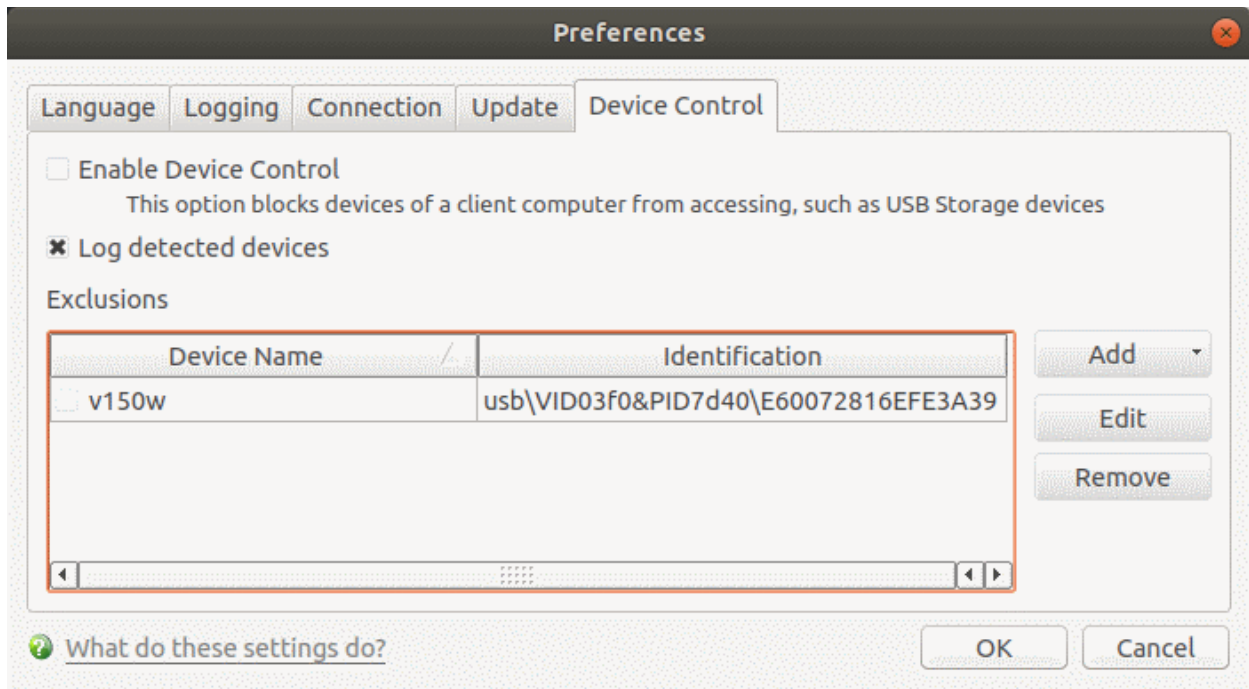
Note - You need to create your exceptions before enabling device control.

- Make sure the external device is connected to the computer
- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Device Control':
- Click the 'Add' button then choose 'Existing Device' from the drop-down



The screen lists all devices that are currently connected to your computer.

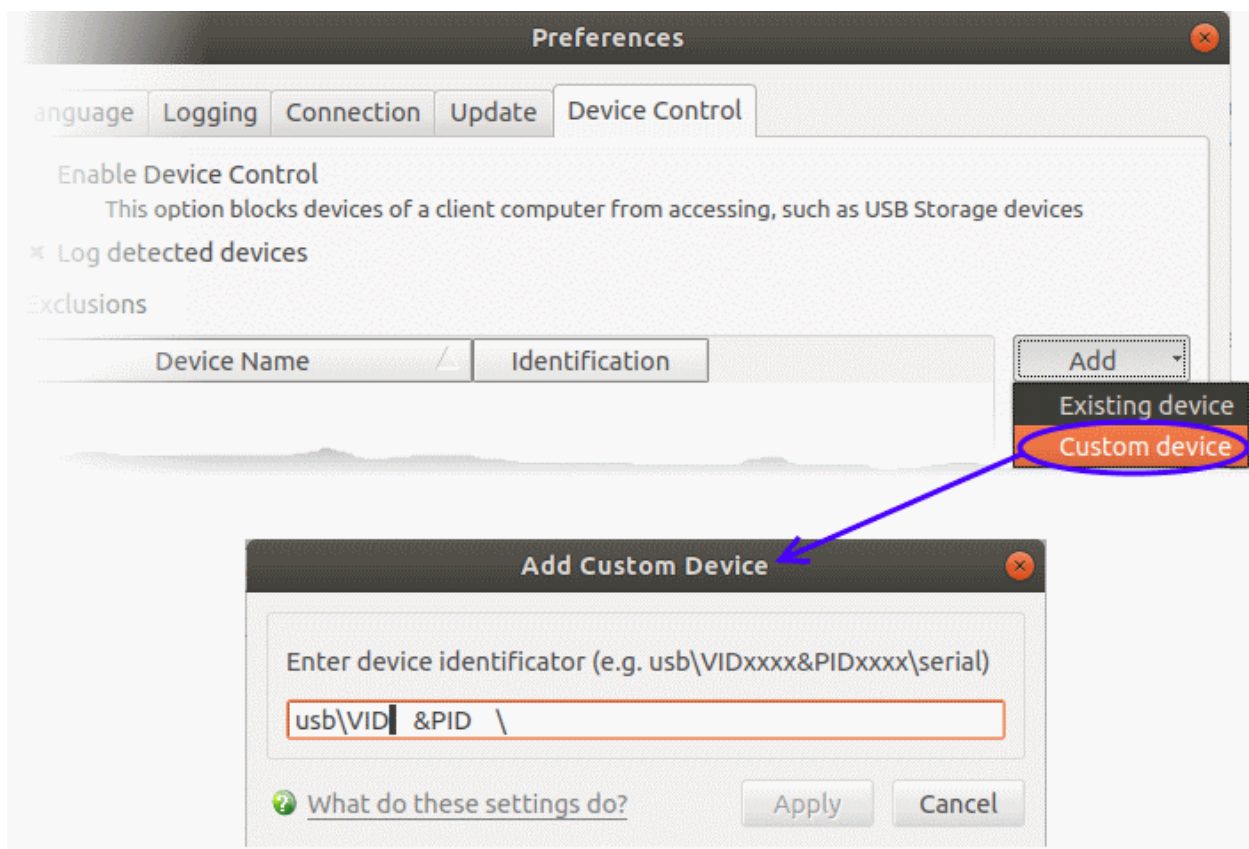
- Select the devices you want to add to exclusions and click 'OK'
- The device is added to the exclusions:



- Repeat the process to exclude more devices
- Click 'OK' in for your settings to take effect

Specify custom devices to be excluded

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Device Control'
- Click the 'Add' button beside 'Exclusions' then choose 'Custom Device' from the drop-down

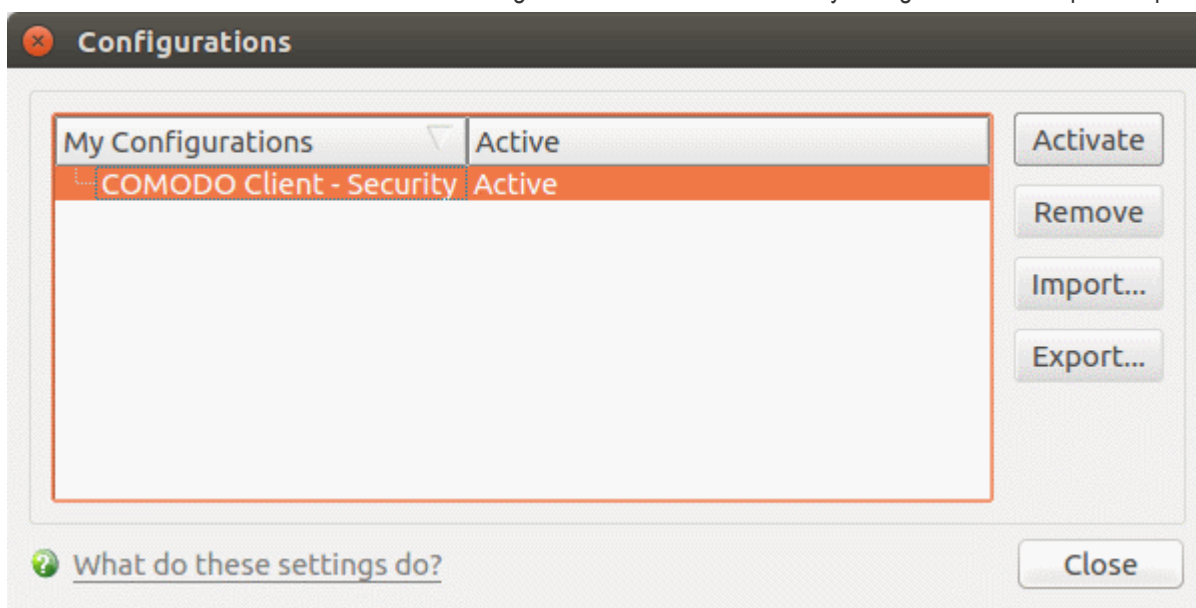


- Enter the vendor identifier and product identifier in the respective areas. Example: VID0951&PID1643. You can use wildcard character to add a series of devices to exclusions. E.g. VID0951&PID16*
- Click 'Apply' in the 'Add Custom Device' dialog
- Click 'OK' in the 'Preferences' dialog for your settings to take effect.

4.2. Manage My Configurations

Click 'More' > 'Manage My Configurations'

- A configuration profile is a template of Comodo Client Security settings. You can import and export configuration profiles as required.
- The 'Active' profile is actually a record of your current configuration. It contains all changes you have made since installation (or since you last changed the active profile).
- Exporting your settings can be a great time-saver if:
 - You need to uninstall and re-install CCS for any reason. For example, if you are upgrading your computer.
 - You are a network admin looking to roll out a standard security configuration to multiple computers.



See the following sections for more details about:

- [Comodo Preset Configurations](#)
- [Import / Export and Manage Personal Configurations](#)

4.2.1. Comodo Preset Configuration

Click 'More' > 'Manage My Configurations'

- The profile that is currently in use is the 'Active' profile. The active profile is a record of your current configuration.
- The default profile installed with CCS is called 'Comodo Client - Security'.
- This profile has the following settings:

Setting	Value
Preferences	
Language	English (US)
Logging Settings:	
• Write to Local Log Database	Enabled
• Write to Syslog Server (CEF Format)	Disabled
• Write to Log File (CEF Format)	Disabled
• Maximum log file size	100 MB
• Log file size action	Keep on updating it removing the oldest records
Connection Settings:	
• Use http proxy	Disabled
Update Settings:	
• Update Server	http://download.comodo.com
Scanner Settings	
Realtime Scanning Settings:	
• Enable Real-time Scan	Enabled
• Automatically quarantine threats found during scanning	Disabled
• Automatically update virus database	Enabled
• Show notification messages	Disabled
• Heuristics Scanning Level	LOW
• Do not scan files larger than	20 MB
• Keep an alert on the screen for	120 Seconds
Manual Scanning Settings:	
• Scan archive files (e.g. *.zip, *.rar)	Enabled
• Automatically update virus database before scanning	Enabled
• Enable cloud scanning	Disabled
• Heuristics Scanning Level	LOW
• Do not scan files larger than	20 MB
Scheduled Scanning Settings:	
• Scan archive files (e.g. *.zip, *.rar)	Enabled

Setting	Value
<ul style="list-style-type: none"> Automatically quarantine threats found during scanning 	Disabled
<ul style="list-style-type: none"> Automatically update virus database before scanning 	Enabled
<ul style="list-style-type: none"> Show scanning progress 	Enabled
<ul style="list-style-type: none"> Enable cloud scanning 	Disabled
<ul style="list-style-type: none"> Heuristics Scanning Level 	LOW
<ul style="list-style-type: none"> Do not scan files larger than 	20 MB
Scan Profiles:	
<ul style="list-style-type: none"> Predefined Scan Profiles 	My Computer, Critical Areas
<ul style="list-style-type: none"> Custom Scan Profiles 	None
Scan Schedules:	
<ul style="list-style-type: none"> Weekly Virus Scanning 	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Scan Profile 	'My Computer' profile
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Schedule 	Weekly, on Sunday at 12:00 AM.

- Note: Managed endpoints – The default CCS profile is configured and deployed by your Endpoint Manager admin. Because of this, the settings in your 'default' profile may differ to those listed above.

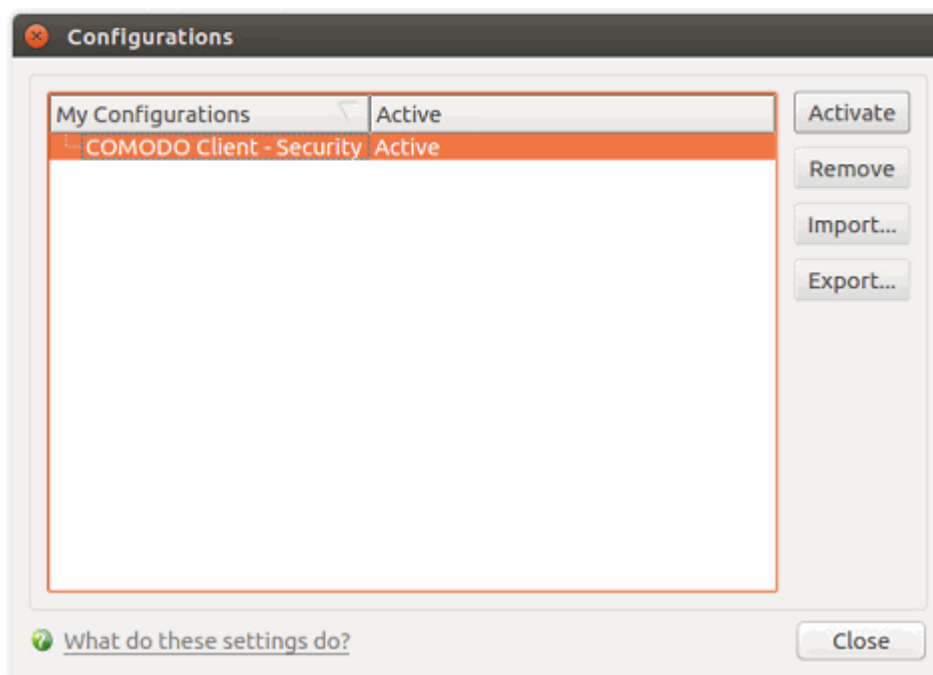
4.2.2. Import /Export and Manage Personal Configurations

Click 'More' > 'Manage My Configurations'

- The configurations interface lets you export your current CCS settings as a profile.
- You can also import and implement a saved profile. This is useful if you wish to roll out a standard configuration to multiple endpoints.
- All settings in the CCS application will be configured as per the imported configuration.
 - Note: Managed endpoints – The default CCS profile is configured and deployed by your Endpoint Manager admin.

Open the configurations interface

- Open Comodo Client Security
- Click 'More > 'Manage My Configurations'



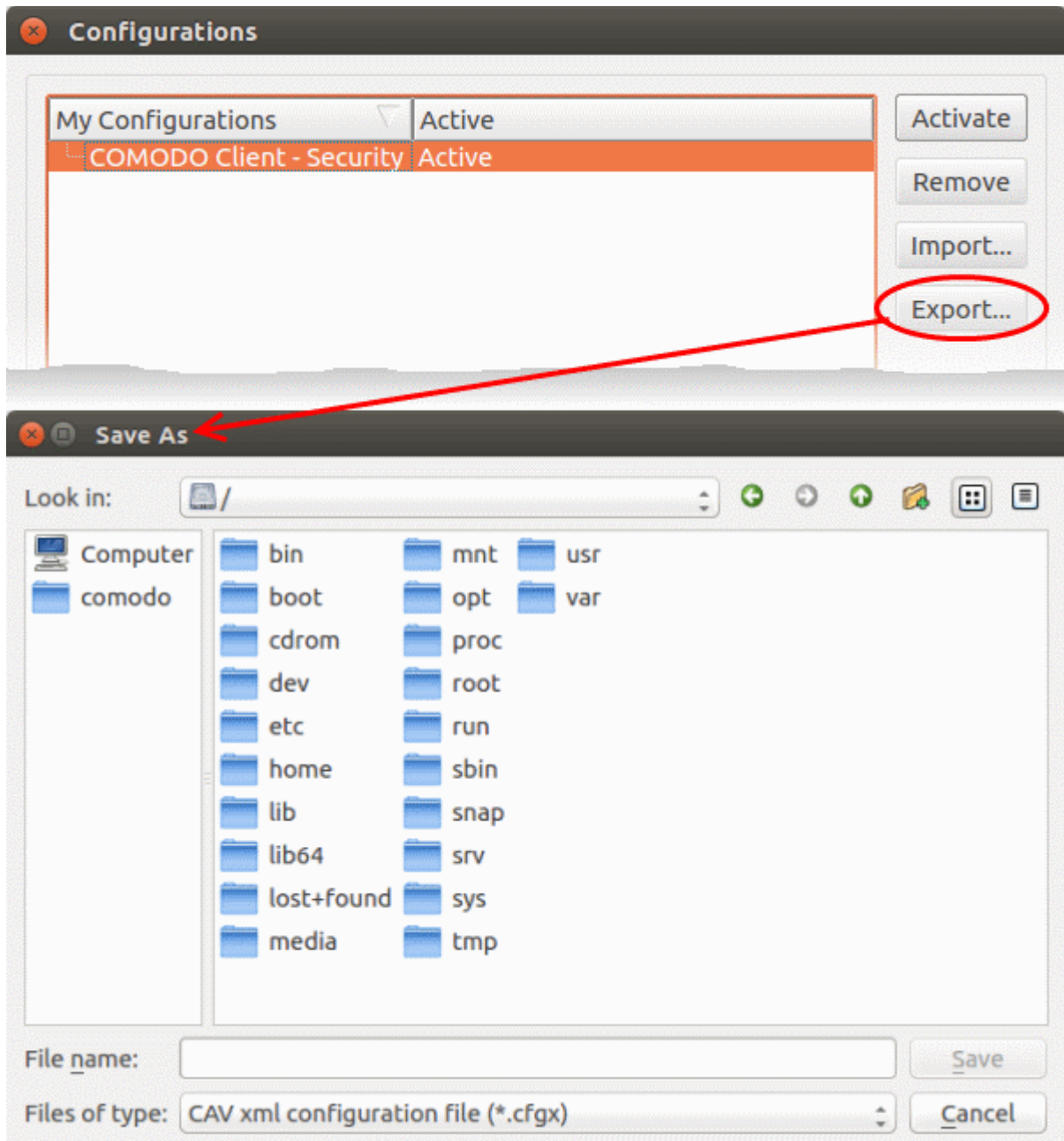
- By default, the interface contains one preset configuration - 'Comodo Client - Security'.
- The current configuration is labeled as 'Active' in this interface.
- The 'Active' configuration is a record of your current configuration. It contains all your settings, changes and preferences.

Click the area on which you would like more information:

- **Export the current configuration**
- **Import a saved configuration**
- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

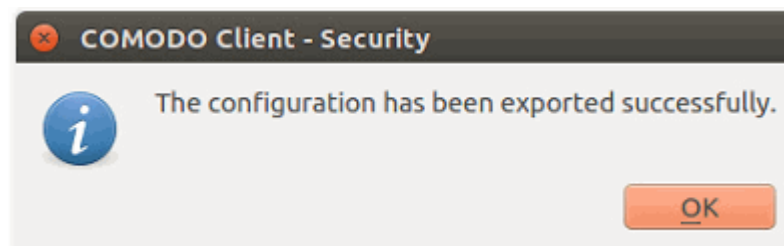
Export your current configuration to a file

- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Select the currently active configuration and click 'Export'
- Type a file name for the configuration (e.g., 'Custom CCS for Linux Profile') and save to the location of your choice.



- Type a file name for the profile (e.g. 'Custom CCS Profile') and save to the location of your choice.

A confirmation dialog will appear if the export is successful:

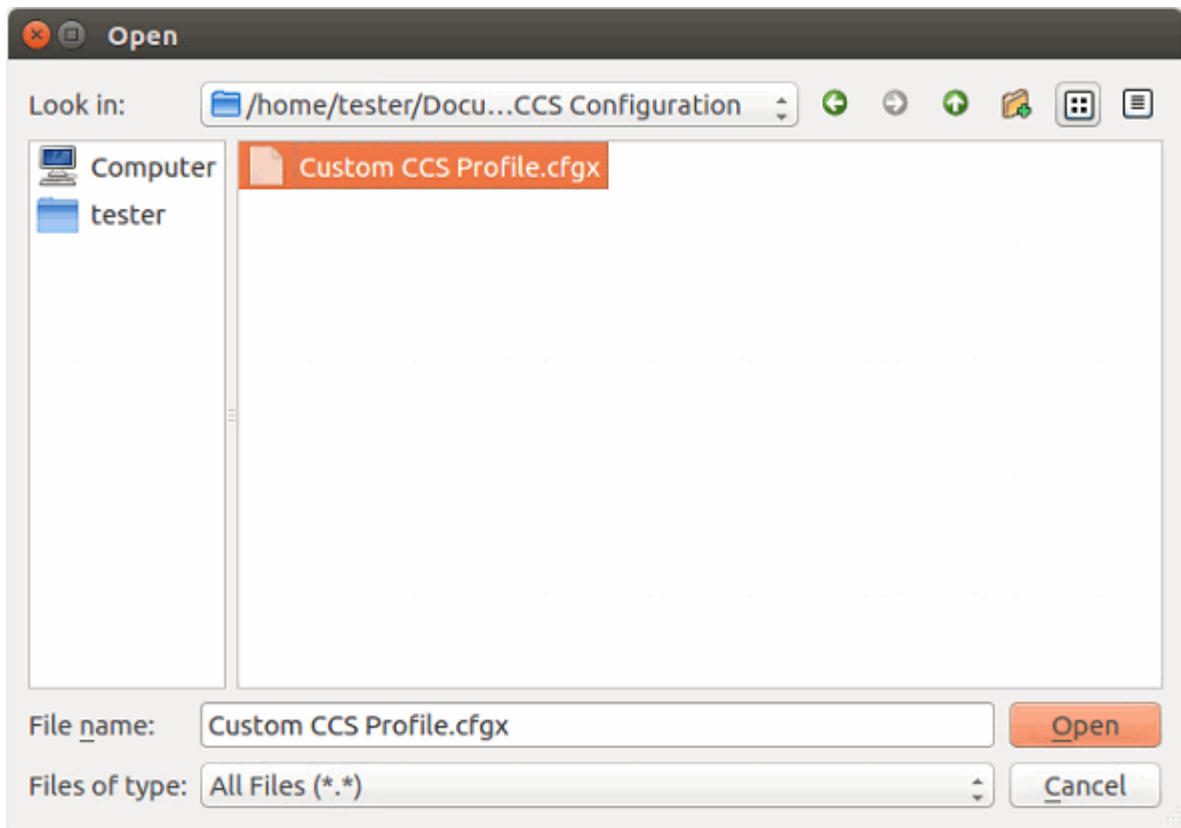


Import a saved configuration from a file

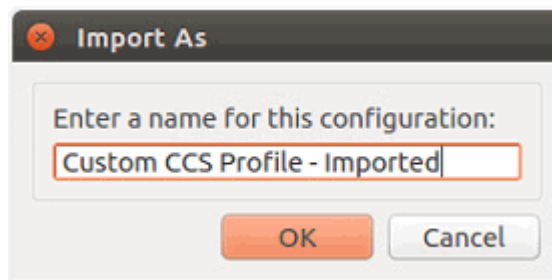
- CCS allows you to import profiles in .cfgx format.
- Any profile you import will not become active until you click the 'Activate' button

Import a configuration file

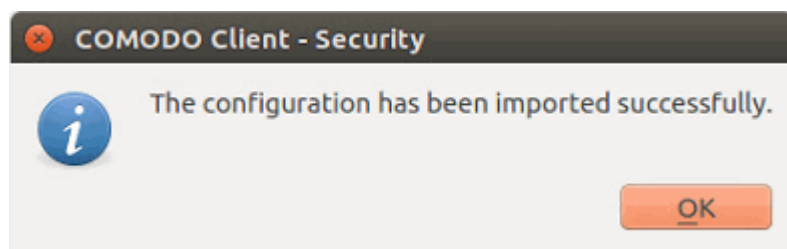
- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Click 'Import' in the 'Configurations' interface



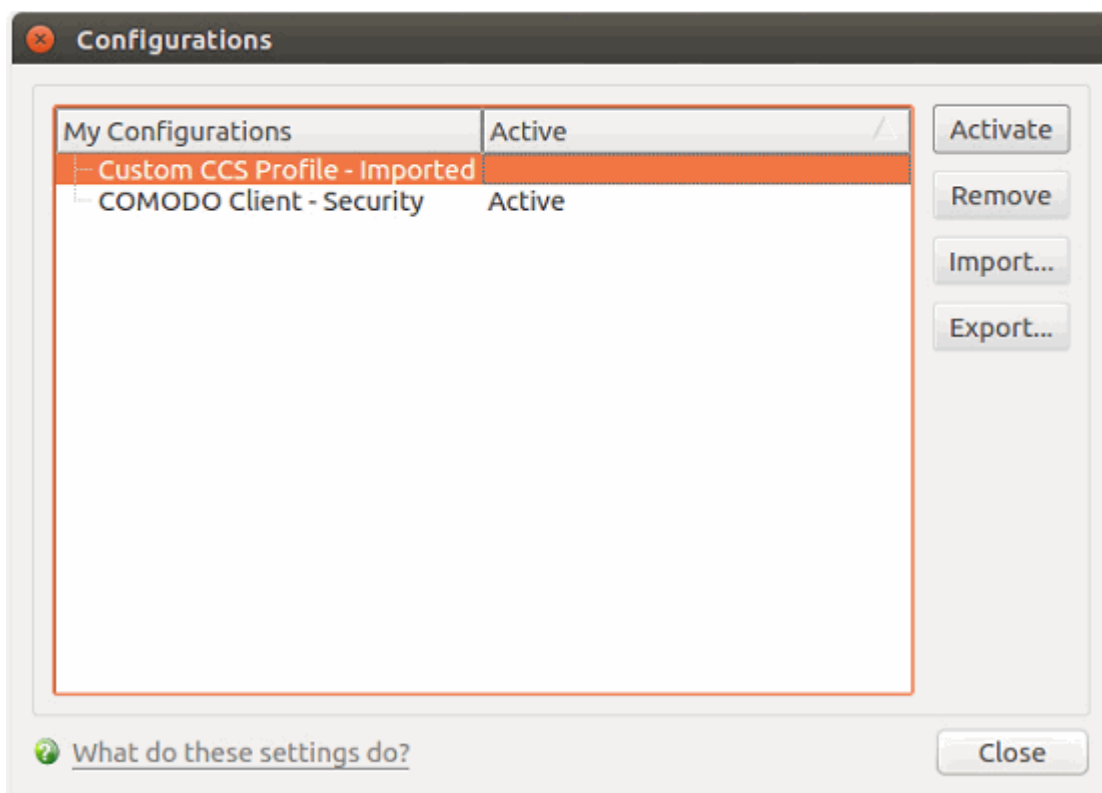
- Navigate to the location of the saved configuration file, select it, and click 'Open'.
- Create a name for the profile you want to import and click 'OK'.
 - This doesn't change the filename. It is just a label for the profile in the CCS interface.



- You will see the following confirmation after import:



- The profile is now available for activation if required:

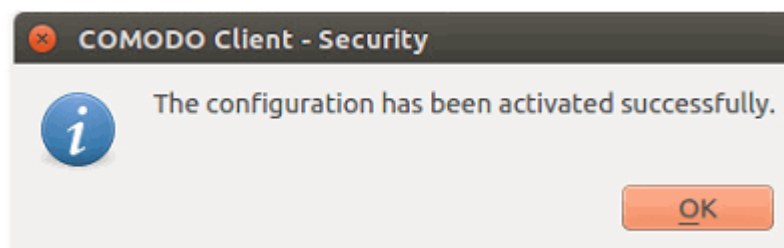


Select and implement a different configuration profile

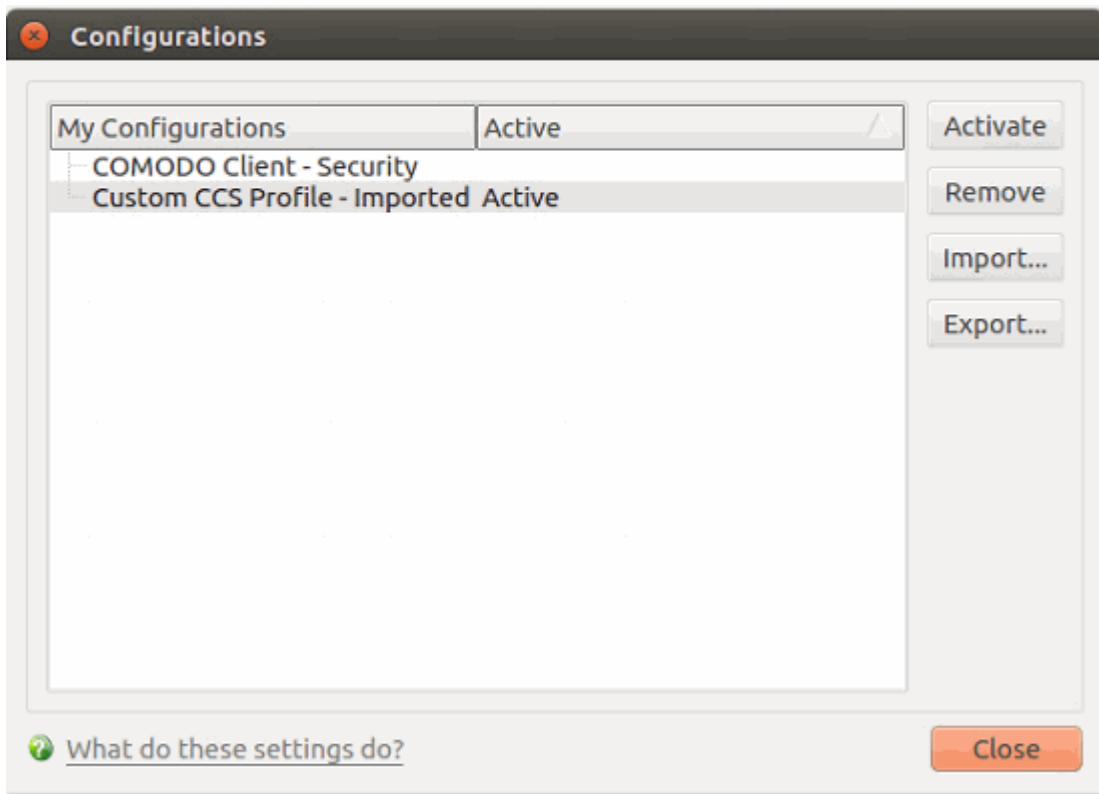
The configurations interface lets you quickly switch between different security profiles.

- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Select the configuration profile you want to use
- Click the 'Activate' button.

You will see the following confirmation dialog:



The profile is marked as 'Active' in the profile list:

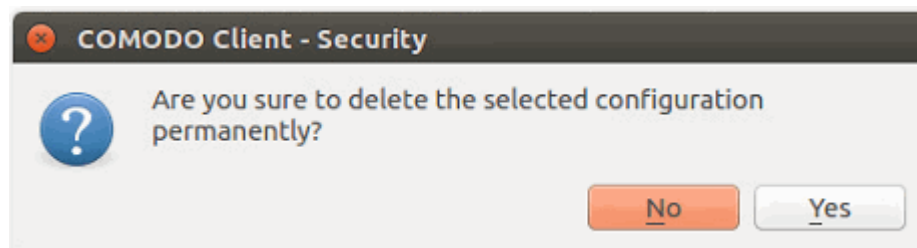


Delete an inactive configuration profile

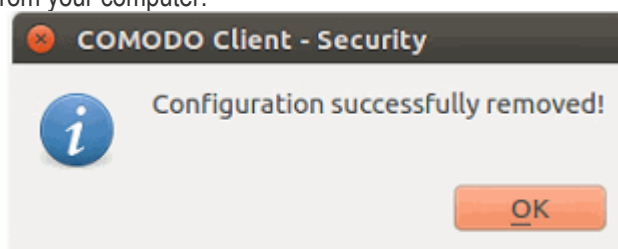
- You can remove inactive profiles that you no longer require
- You cannot delete the active profile.

Remove an unwanted profile

- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Select the profile and click the 'Remove' button.
- Click 'Yes' at the confirmation dialog:



The profile will be removed from your computer:



4.3. Diagnostics

Click 'More' > 'Diagnostics'

The diagnostics scanner checks your system to make sure that the application is installed correctly.

It checks:

- File System - Checks all Comodo system files are present and correctly installed.
- Incompatible software - Checks whether your computer has software that has compatibility issues with CCS.

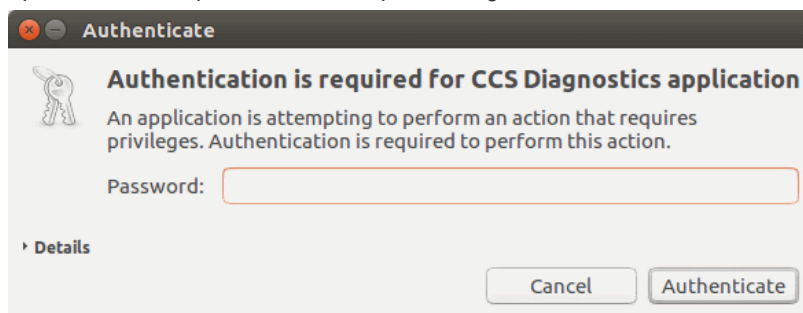
Open the diagnostics tool

- Open Comodo Client Security
- Click 'More' > 'Diagnostics'

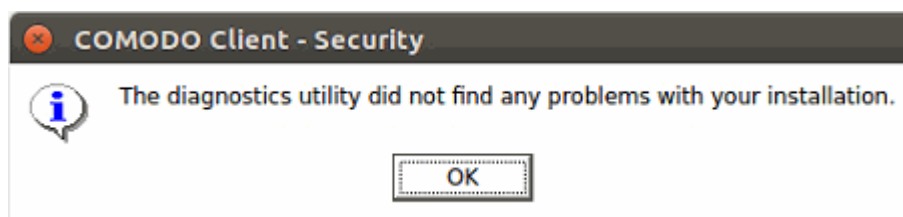
OR

- Click 'Run Diagnostics' 

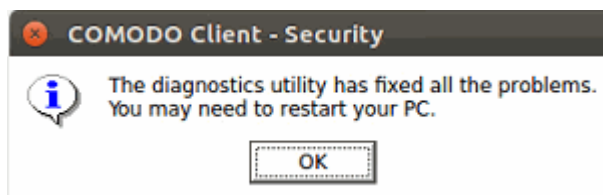
- Note: diagnostics can only be run by root users (admins). If you are not logged in as root, then you will need to provide the root password before proceeding:



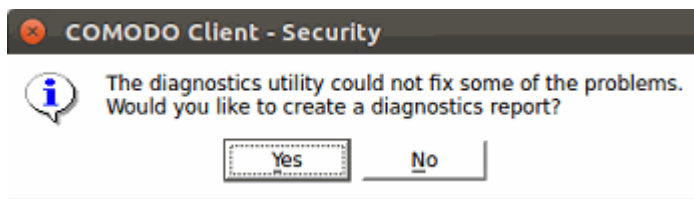
- You will see the following message if your installation does not have any errors:



- If errors are found, then the utility will attempt to fix them. You will see the following message:



- Click 'OK'. The diagnostics utility automatically fixes the problems and prompts you to restart the computer
 - Restart your computer for the changes to take effect.
- If the utility could not fix the problems, it will prompt you to create a diagnostics report:



4.4. View Antivirus Events

- Open the Comodo Client Security home screen
- Click the number in front of 'threat(s) detected so far'
- Or
- Click 'More' > 'View Antivirus Events'

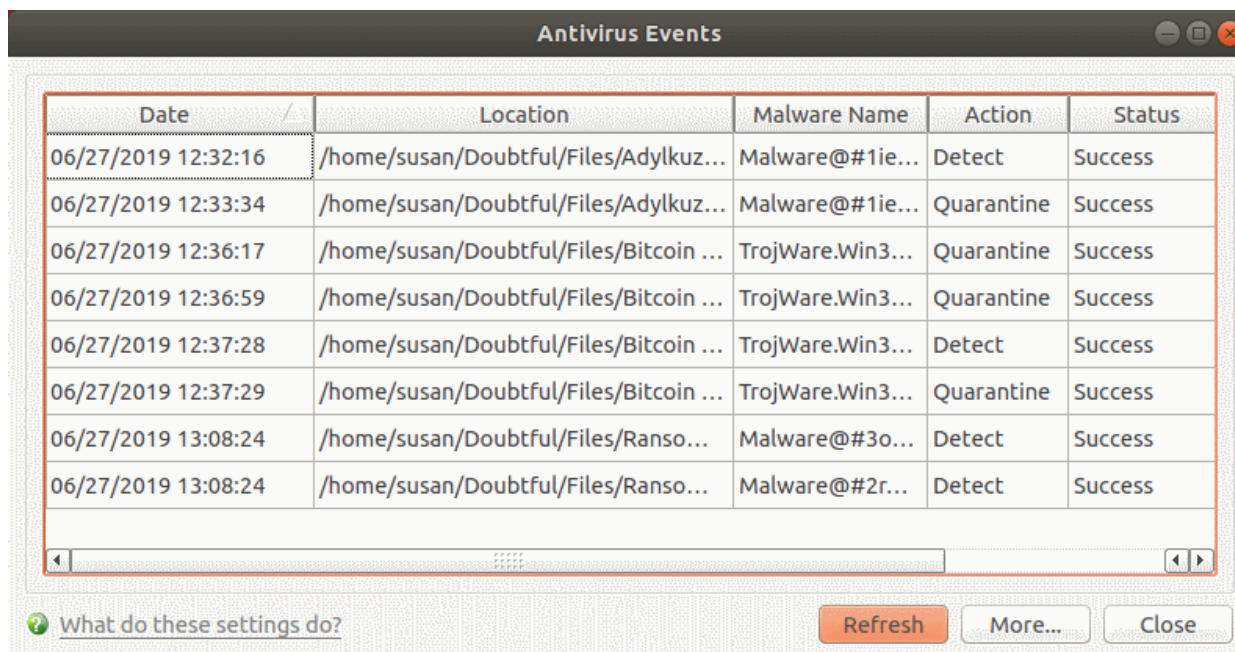
Antivirus events are a record of the actions taken by CCS when it encounters malware.

The log viewer tells you:

- The name of the malware and the location it was detected on your computer
- The date and time it was detected
- The action that was taken on the malware, and whether or not the action was successful.

View antivirus events

- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'



Antivirus Events - Column Descriptions	
Column Header	Descriptions
Date	When the malware was detected and the action taken against it.
Location	The path where the malware was detected.

Malware Name	The malware variant and identifier
Action	How CCS attempted to deal with the malware
Status	Whether or not the action was successful


- Click any column header to sort items in order of the entries in that column.
- Click the 'More' button to open the **'Log Viewer Module'**.

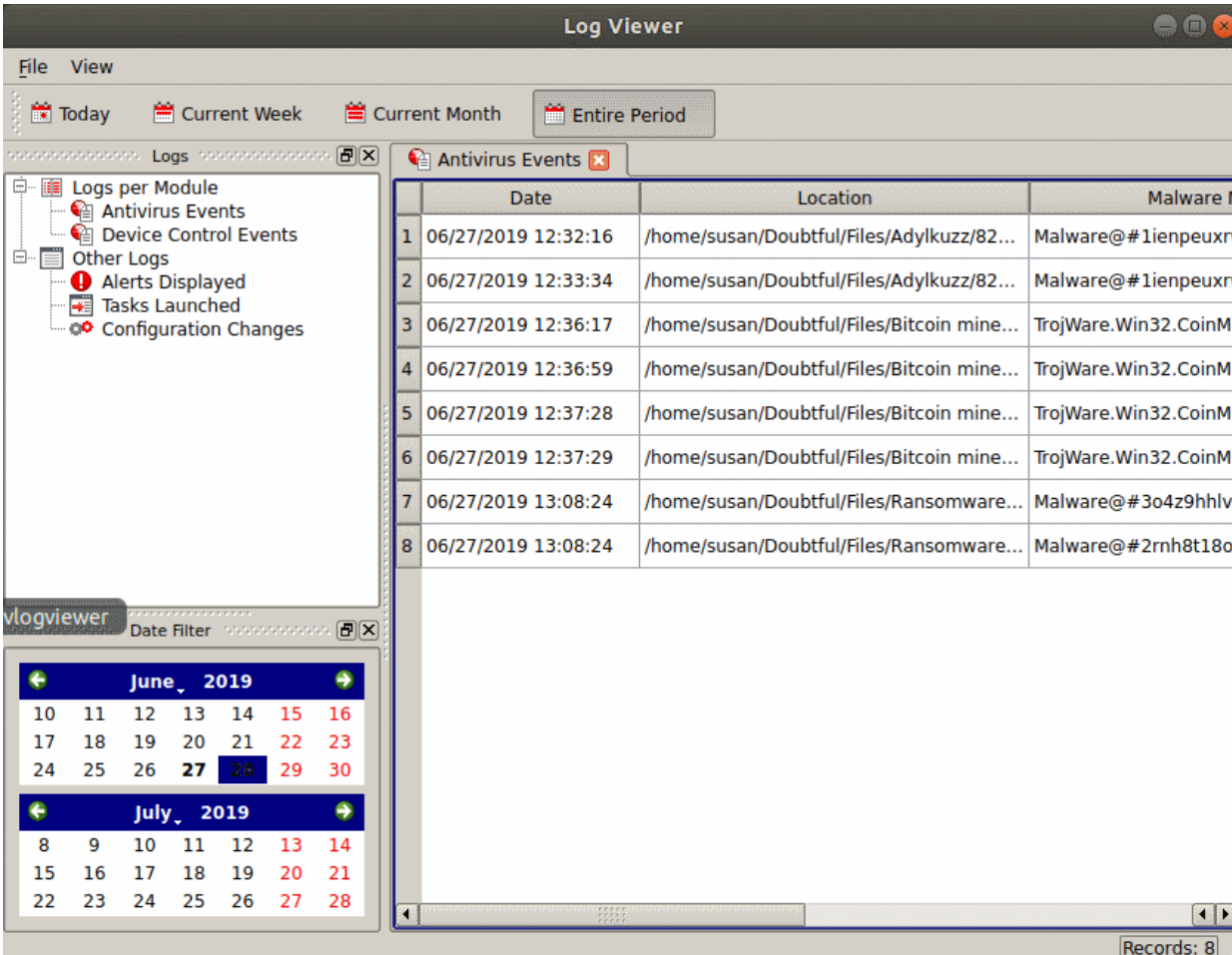
4.4.1. Log Viewer Module

- CCS records all antivirus events in extensive but easy to understand logs.
- Logs are created when malware is found, after running an update, and for various other reasons.

Open log viewer panel

- Open Comodo Client Security
 - Click 'More' > 'View Antivirus Events'
 - Click 'More' in the 'Antivirus Events' interface
- OR

- Click 'View Logs'  in the 'Applications' panel



The screenshot shows the 'Log Viewer' application window. It features a menu bar with 'File' and 'View'. Below the menu bar are navigation buttons for 'Today', 'Current Week', 'Current Month', and 'Entire Period'. A sidebar on the left lists log categories: 'Logs per Module', 'Antivirus Events', 'Device Control Events', 'Other Logs', 'Alerts Displayed', 'Tasks Launched', and 'Configuration Changes'. The main area displays a table of 'Antivirus Events' with columns for 'Date', 'Location', and 'Malware Name'. Below the table is a 'Date Filter' section with two calendar views for June and July 2019. The bottom right corner shows 'Records: 8'.

	Date	Location	Malware Name
1	06/27/2019 12:32:16	/home/susan/Doubtful/Files/Adylkuzz/82...	Malware@#1ienpeuxrv
2	06/27/2019 12:33:34	/home/susan/Doubtful/Files/Adylkuzz/82...	Malware@#1ienpeuxrv
3	06/27/2019 12:36:17	/home/susan/Doubtful/Files/Bitcoin mine...	TrojWare.Win32.CoinMi
4	06/27/2019 12:36:59	/home/susan/Doubtful/Files/Bitcoin mine...	TrojWare.Win32.CoinMi
5	06/27/2019 12:37:28	/home/susan/Doubtful/Files/Bitcoin mine...	TrojWare.Win32.CoinMi
6	06/27/2019 12:37:29	/home/susan/Doubtful/Files/Bitcoin mine...	TrojWare.Win32.CoinMi
7	06/27/2019 13:08:24	/home/susan/Doubtful/Files/Ransomware...	Malware@#3o4z9hhlvr
8	06/27/2019 13:08:24	/home/susan/Doubtful/Files/Ransomware...	Malware@#2rn8t18of

The panel on the left lists the various types of logs available. Choose the type of log you want to see:

- **Antivirus Events** - Shows logs generated by the antivirus module. For example, a log is created when malware is found, when an alert is generated, and when an item is quarantined.
- **Device Control Events** - Events where an external device was connected or disconnected. Example devices are USB sticks and external storage drives.
- **Other Logs:**
 - **Alerts Displayed:** Lists all warnings that were displayed to the user. Includes the response given by the user to those alerts and alert details.
 - **Tasks Launched:** Various antivirus tasks that have taken place, including database updates and scans. This area contains a log of all scans and the result of the scan.
 - **Configuration Changes:** Log of all settings changes made by the user.
- The events themselves are shown in the main panel on the right.
- The links along the top of the interface let you filter the logs by date.
 - **Today** - Shows events logged since 12 AM on today's date.
 - **Current Week** - All logged events during the current week. The current week is calculated from the Sunday to Saturday.
 - **Current Month** - All logged events during the month.
 - **Entire Period** - Every event logged since CCS was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.

You can also use the advanced filter feature to filter by various other criteria. For example, you can choose to show all events where an item was quarantined.

Export Log Files

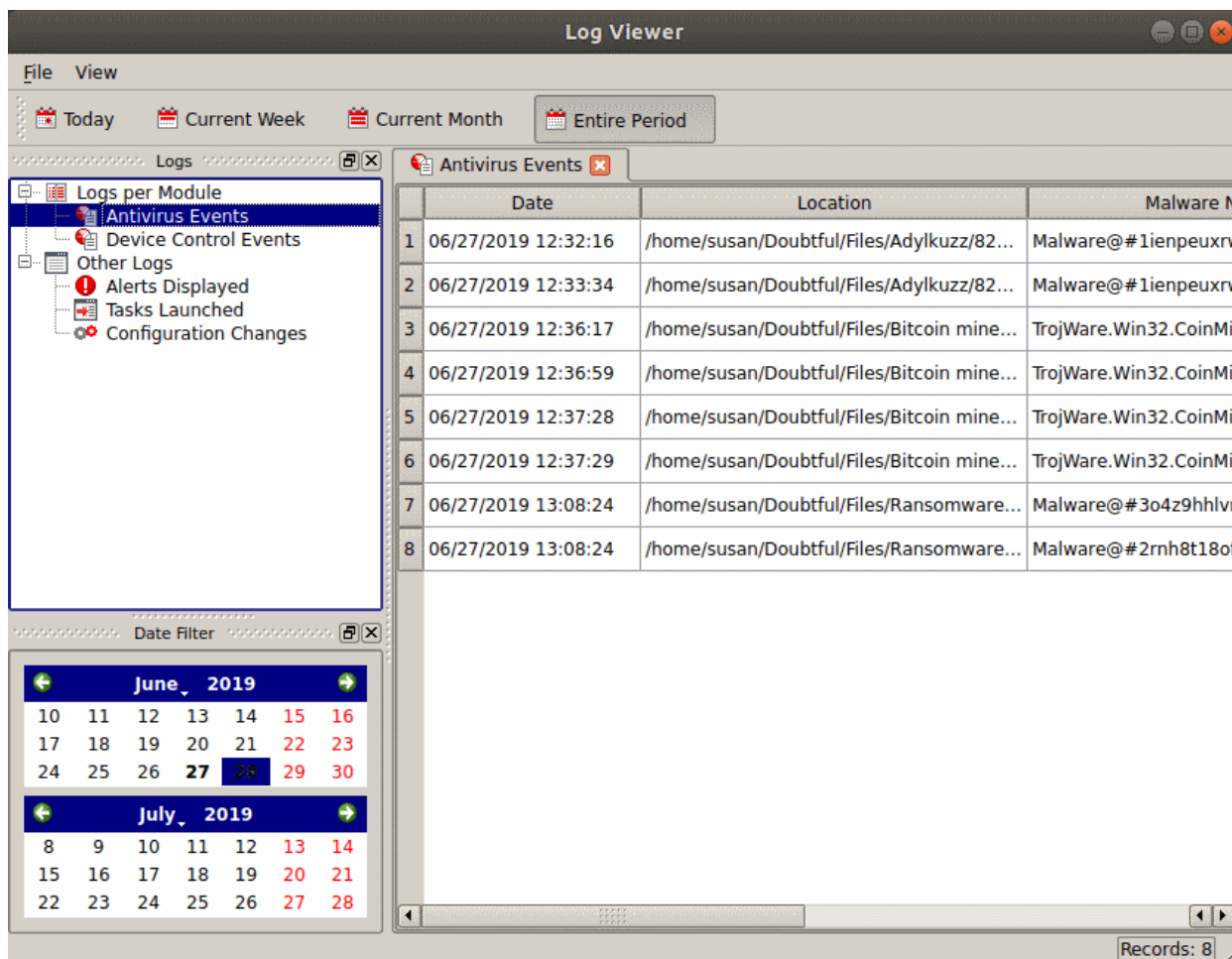
- There are two ways to export log files:
 1. Right-click the log file you want to export > select 'Export'.
 2. File menu:
 - Select the event you want to export.
 - Click 'Export' in the 'File' menu

The following sections contain more details about each type of log:

- **Antivirus Logs**
- **Device Control Logs**
- **'Alerts Displayed' Logs**
- **'Tasks Launched' Logs**
- **Configuration Change Logs**

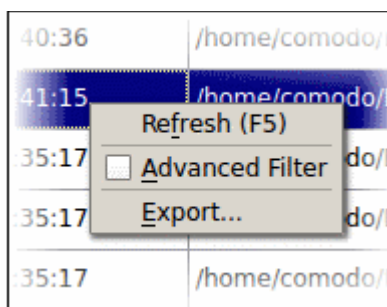
4.4.1.1. Antivirus Logs

- Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Antivirus Events'
- Antivirus logs contain statistics on all discovered threats.
- This includes the time of the event, the malware name, and the action taken on the threat.



Antivirus Events - Column Descriptions	
Column Header	Descriptions
Date	When the malware was detected and the action taken against it.
Location	Path where the file was detected
Malware Name	The type of the malware and its identifier
Action	How CCS attempted to deal with the file
Status	Whether the action was a successful
Alert	Click 'Related Alert' to view details of the alert shown at the time of the event. You'll also see the user's response. See ' Alerts Displayed ' Logs for more details.

- Right-click anywhere inside the log viewer to view further options:



- **Refresh** – Adds recently created logs to the list
- **Advanced Filter** – Filter AV events by various criteria, including action, type and more.
- **Export...**- Save the events list as an HTML file.

4.4.1.1.1. Filter Antivirus Logs

You can create custom views of all logged events according to the following criteria:

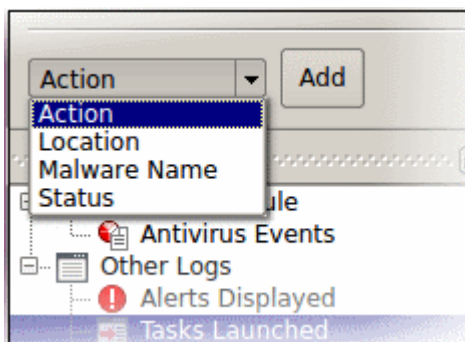
- **Action** - Filter events according to the response (action taken) by the antivirus
- **Location** - Filter events by the path at which the malware was found
- **Malware Name** - Display only those events that reference a specific piece of malware
- **Status** - Filter events according to whether the attempted action was successful or not. Status options are 'Success' or 'Fail'

Configure Event Filters

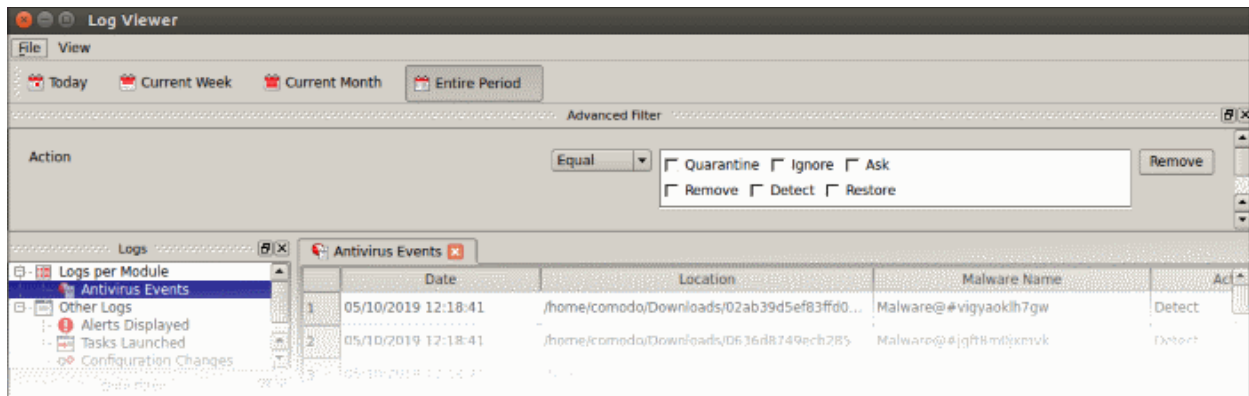
- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Antivirus Events' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'
- OR
- Click 'View' on the menu bar and select 'Advanced Filter'

There are 4 types of filter. Each of these can be further refined by selecting or deselecting specific parameters.

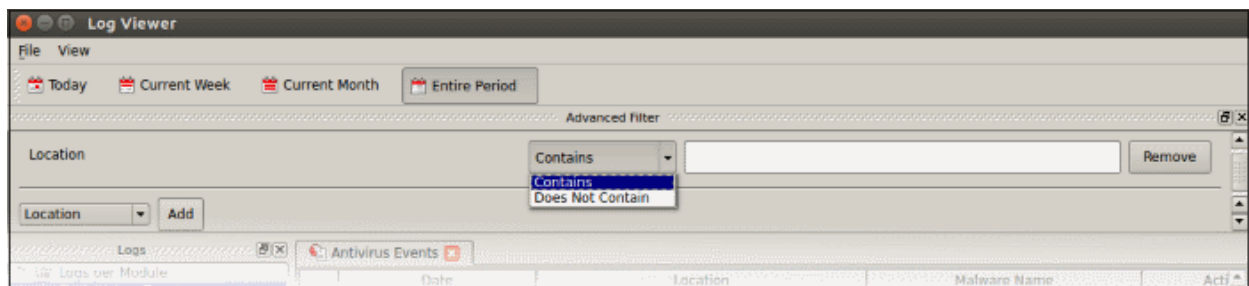
- Select a filter criteria and click 'Add'



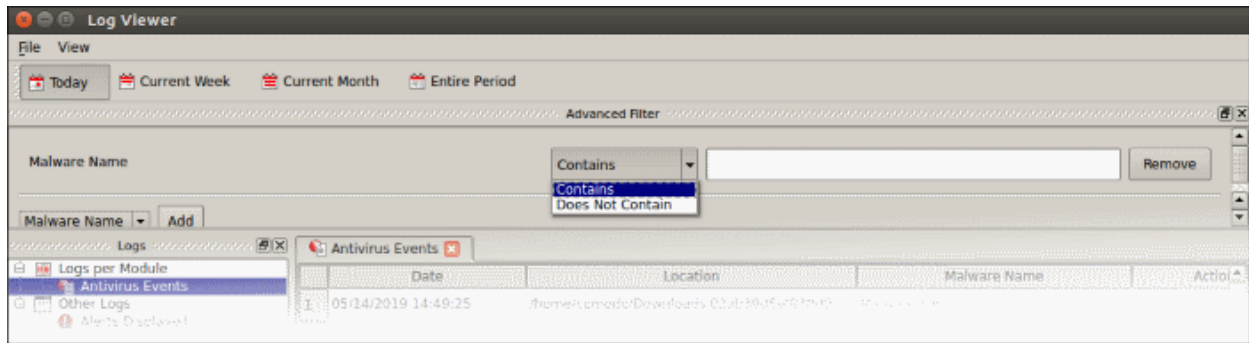
1. **Action:** Filter logs by the response to the threat. You can then select a specific action. For example, only show events where the threat was quarantined.



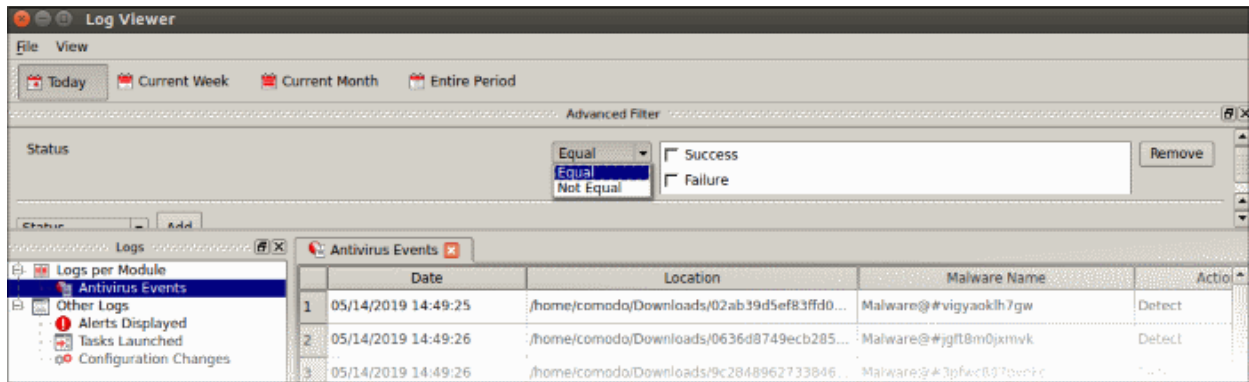
- Select 'Equal' or 'Not Equal' from the drop-down.
 - **Equal** – Show only events which feature the action you select. You can select multiple actions.
 - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Ignore' to view every event except those that were ignored.
- Choose the events you want to view:
 - **Quarantine:** Events where the threat was placed in quarantine
 - **Remove:** Events where the user chose to delete a threat
 - **Ignore:** Events where the user allowed the threat to proceed
 - **Detect:** Events where a piece of malware was first identified
 - **Ask:** Events where the user was asked to provide a response to a discovered threat. Users are asked for their response at an alert, or the results screen at the end of a scan. The response from the user might be 'Quarantine', 'Remove', 'Ignore' or 'Restore'.
 - **Restore:** Events where the user removed the threat from quarantine and moved it back to its original location.
- 2. **Location:** View logs that concern files at a specific path. You need to enter the path in the field provided:



- Select 'Contains' or 'Does Not Contain' from the second drop-down:
 - **Contains** – Show only events which concern items at the location you specify. You can add multiple locations.
 - **Does Not Contain** – Inverts your choice. Show all events except those at the location you specify.
- 3. **Malware Name:** Filter logs by the label of the malicious item. You need to enter the name of the malware in the field provided:



- Select 'Contains' or 'Does Not Contain' from the second drop-down:
 - **Contains** – Show only events which concern the malware named in the text field. You can add multiple malware names.
 - **Does Not Contain** – Inverts your choice. Show all events except those that involve the malware you specify.
- 4. **Status:** Filter logs by whether or not the action taken on the threat was successful. You can view only successful actions, or only failed actions.



- Select 'Equal' or 'Not Equal' from the drop-down.
 - **Equal** - Show only events which feature the result you select.
 - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Success' to view every event except those that were successful.
- Choose the outcomes you want to view:
 - **Success:** View events where the task in the 'Action' column was completed.
 - **Failure:** View events where the task in the 'Action' column was not completed.

4.4.1.2. Device Control Logs

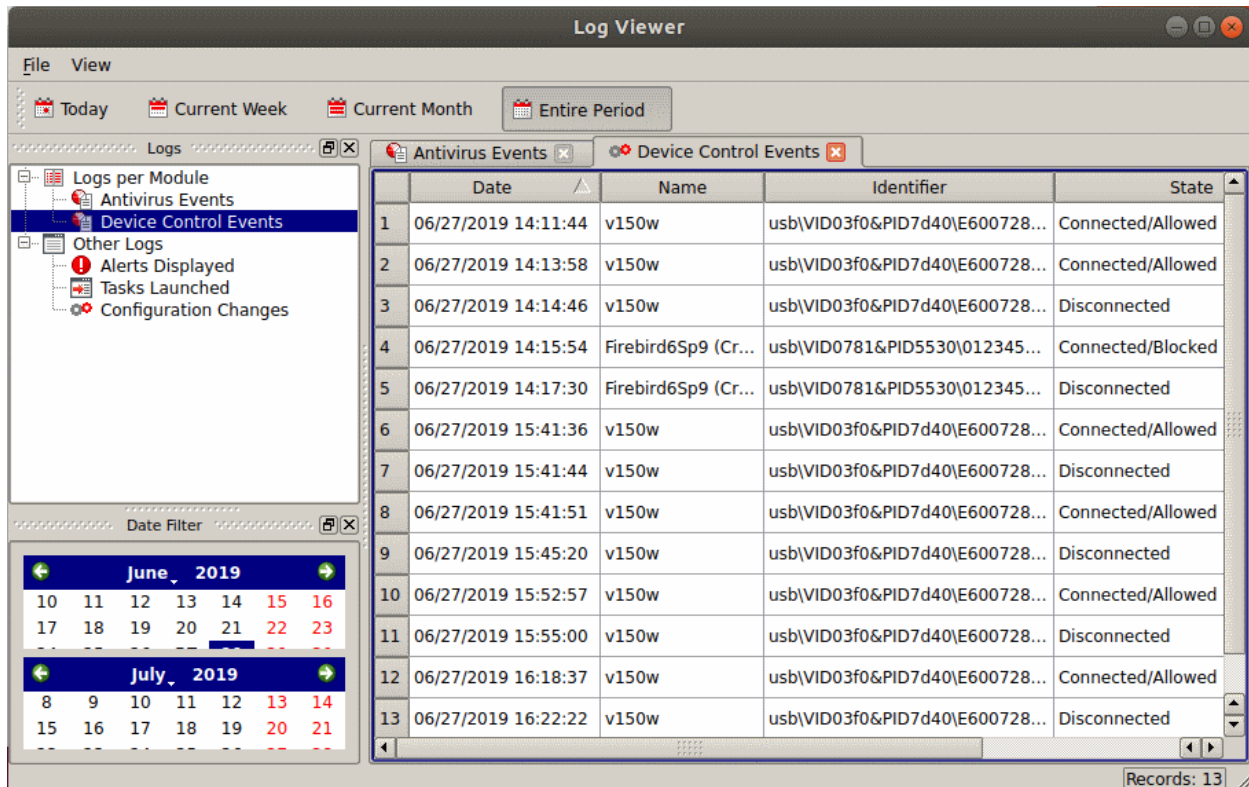
- Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Device Control Events'
- Device control logs show events where an external device was connected, or disconnected, from the endpoint. The log also tells you if the connection was allowed or blocked.
- Each log shows the time of the connection, the device connected and whether the connection was allowed or blocked.

View external device connection logs

- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module

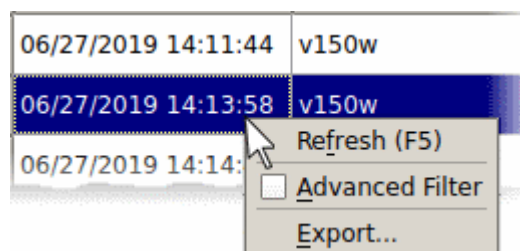
- Select 'Device Control Events' in the left-menu

The device control logs are shown on a new tab in the log viewer module.



Device Control Events - Column Descriptions	
Column Header	Descriptions
Date	Date and time the USB storage device connection event.
Name	The label of the device.
Identifier	The unique identification string of the device. The identifier is a combination of the vendor identification number (VID) and the product identification number (PID).
State	Whether the device was connected or disconnected and whether the connection was allowed or blocked.

- Right-click anywhere inside the log viewer to view further options:



- **Refresh** – Adds recently created logs to the list
- **Advanced Filter** – Filter device control events by various criteria, including name, identifier and state.
- **Export...** - Save the events list as an HTML file.

4.4.1.2.1. Filter Device Control Logs

You can create custom views of all logged events according to the following criteria:

- **Name** - Show events that involve specific devices
- **Identifier** – Show events that involve devices with a specific ID code
- **State** - Filter events by whether the connection attempt was successful or not

Configure event filters

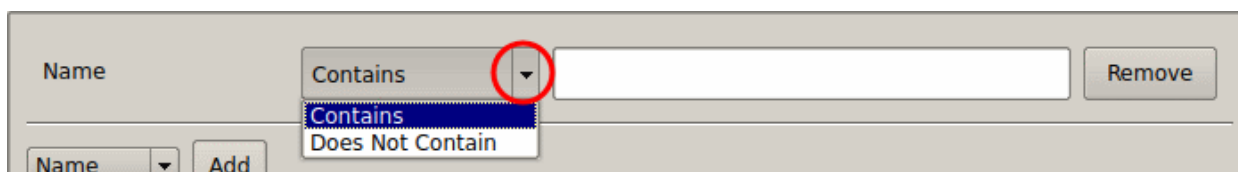
- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Device Control Events' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'
- OR
- Click 'View' on the menu bar and select 'Advanced Filter'

There are 3 types of filter. Each of these can be further refined by selecting or deselecting specific parameters.

- Select a filter criteria and click 'Add'

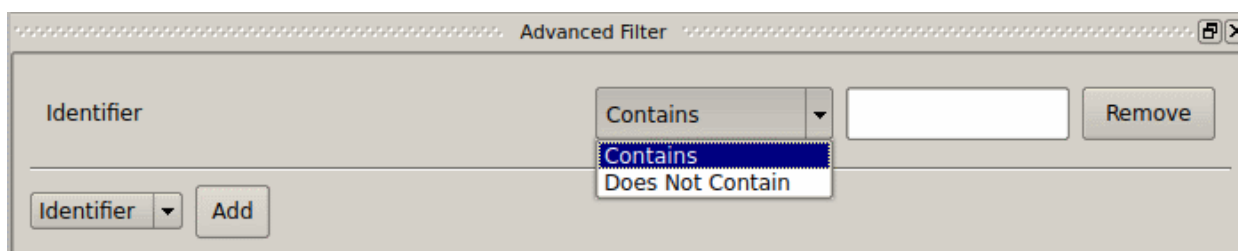


1. **Name:** Filter logs based on the label of the device



- Select 'Contains' or 'Does Not Contain' from the second drop-down:
 - **Contains** - Show only events which concern device name you specify.
 - **Does Not Contain** - Inverts your choice. Show all events except those involving the device name you specify.
- Enter your filter criteria in the text field

2. **Identifier:** Filter entries based on the device ID of the external device.



- Select 'Contains' or 'Does Not Contain' from the second drop-down:

- **Contains** – Show only events which concern device ID you specify.
- **Does Not Contain** – Inverts your choice. Show all events except those involving the device ID you specify.
- Enter the device ID in part or full as your filter criteria in the text field
- 3. **State:** Filter events based on whether the device connection attempt was allowed or blocked.
 - Select 'Equal' or 'Not Equal' from the drop-down.
 - Equal - Show only events that meet the criteria you select.
 - Not Equal - Inverts your choice. For example, select 'Not Equal' + 'Allowed' to view every event except those where devices were allowed.
 - Now select the state from 'Allowed' or 'Blocked'

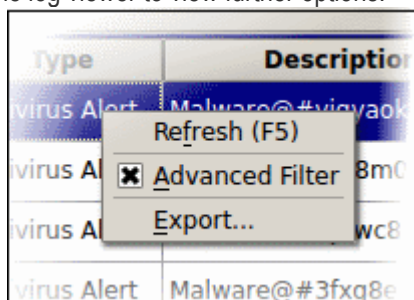
4.4.1.3. 'Alerts Displayed' Logs

- Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Alerts Displayed'
- These logs show a user's response to a threat alert
- The action taken on the threat depends on how the user responded to the alert

	Date	Type	Description
1	06/27/2019 12:32:16	Antivirus Alert	Malware@#1ienpeuxrw2dy
2	06/27/2019 12:33:34	Antivirus Alert	Malware@#1ienpeuxrw2dy

'Alerts Displayed' Logs - Column Descriptions	
Column Header	Descriptions
Date	The time the alert was shown.
Type	The alert category. Currently, 'Antivirus' is the only alert type.
Description	Malware name.
Advice	Location where the malware was detected.
Answered	Whether the user responded to the alert. If yes, you will see the date and time of the response.
Answer	The response provided by the user.
Flags	Not used.
Treat as	Not used.
Event	Click 'Related Event' to view details of the event that triggered the alert. You'll also see the action taken by CCS on the event. See ' Antivirus Logs ' for more details.

- Right-click anywhere inside the log viewer to view further options:



- **Refresh** - Adds recently created logs to the list
- **Advanced Filter** - Filter alert events by various criteria, including answer, date of alert, and more
- **Export...** - Save the events list as an HTML file.

4.4.1.3.1. Filter 'Alerts Displayed' Logs

You can create custom views of all logged events according to the following criteria:

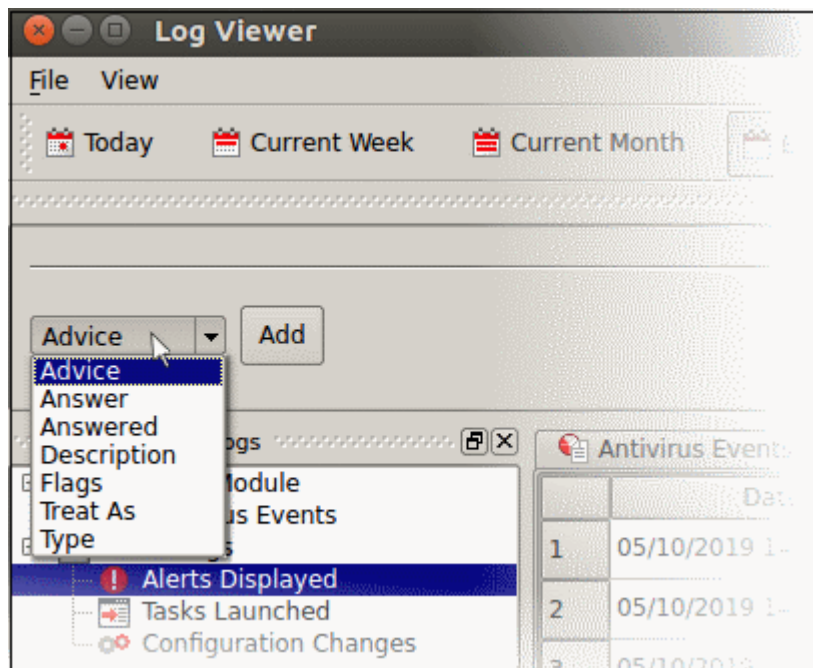
- **Advice**: Filter events by the path at which the malware was found
- **Answer**: Filter events according to the user's response. For example, 'Skip once'.
- **Answered**: Filter events by specific dates
- **Description**: Filter events by malware name
- **Flags**: Not used
- **Treat As**: Not used
- **Alert Type**: Filter events by alert category. Currently, 'Antivirus' is the only category available.

Configure Event Filters

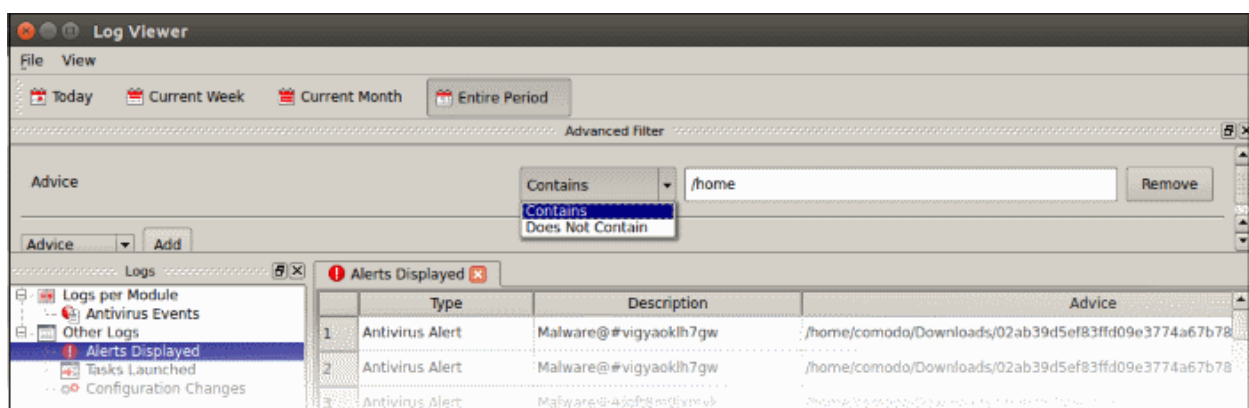
- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Alerts Displayed' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'
- OR
- Click 'View' on the menu bar and select 'Advanced Filter'

There are 5 types of filter. Each of these can be further refined by selecting or deselecting specific parameters.

- Select a filter criteria and click 'Add'

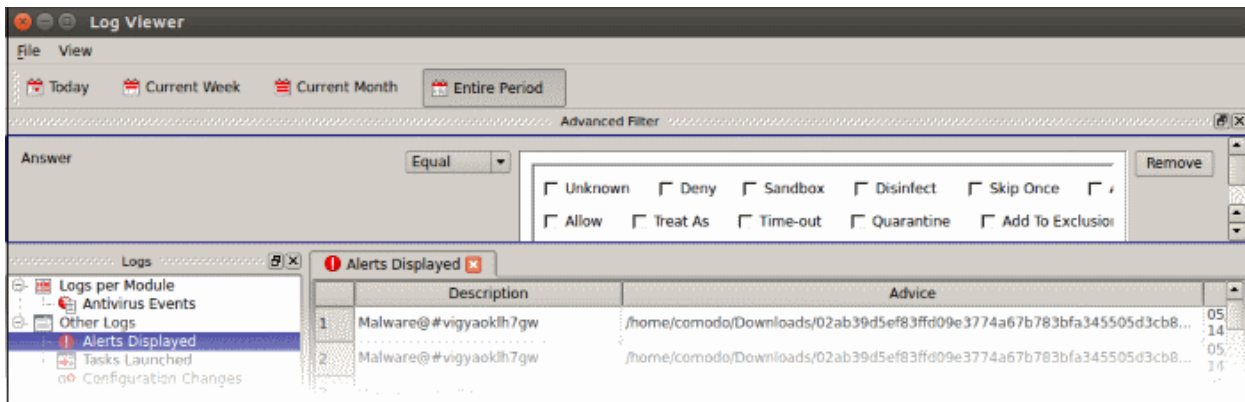


1. **Advice:** View logs that concern files at a specific path. You need to enter the path in the field provided:

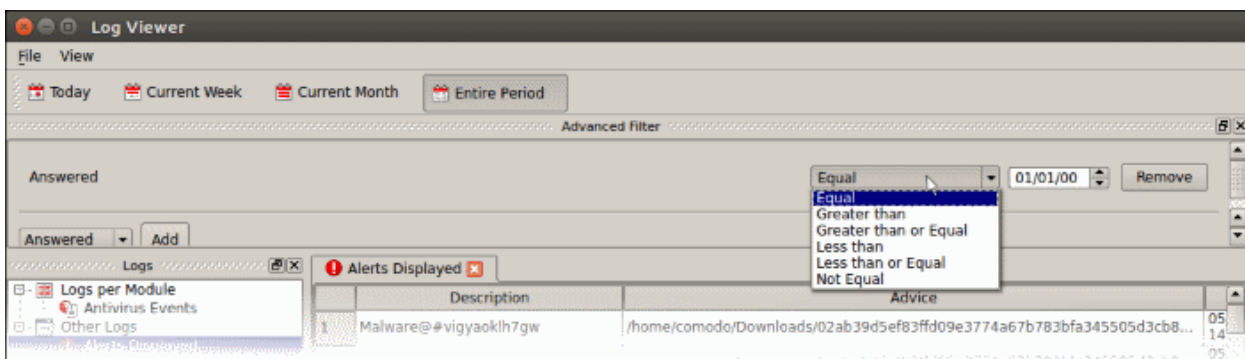


- Select 'Contains' or 'Does Not Contain' option from the drop-down.
 - **Contains** - Show only alerts which concern items at the location you specify. You can add multiple locations.
 - **Does Not Contain** - Inverts your choice. Show all alerts except those about items in the location you specify.

- Answer:** Filter logs by the action taken by the user at the alert. You can then filter by a specific type of action. For example, show events where the threat was quarantined.



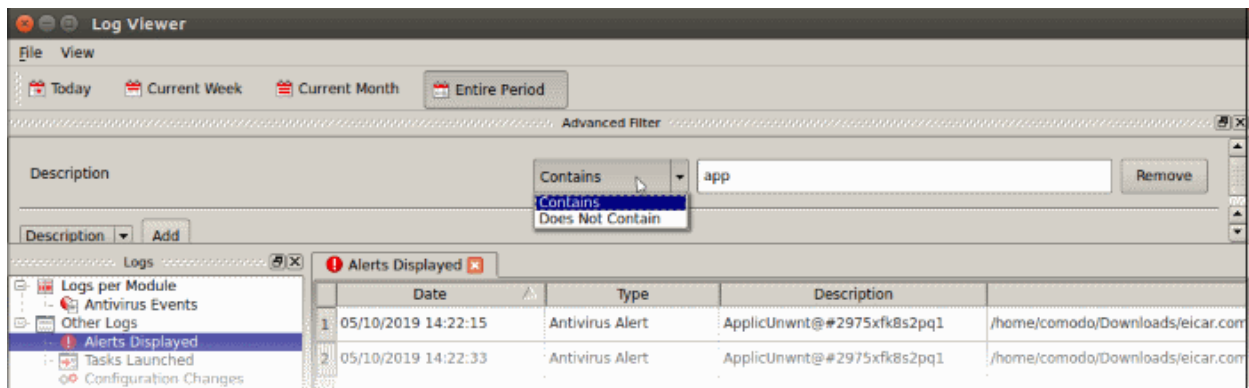
- Select 'Equal' or 'Not Equal' from the drop-down.
 - Equal** - Show only events which feature the action you select. You can select multiple actions.
 - Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Quarantine' to view every alert *except* those that where the threat was quarantined.
 - Select the action you want to view:
 - Unknown** - Events where the user did not respond to the alert.
 - Quarantine** - Events where the user chose to place the threat in quarantine
 - Skip Once** - Events where the user chose to allow the threat.
 - Add to Exclusions** - Events where the user created an exception for the threat at the alert.
 - Note – Other actions shown in the screen are not applicable.
- Answered:** Filter logs by date of the response. You need to enter the date in the field provided. You can then refine your filter with other parameters:



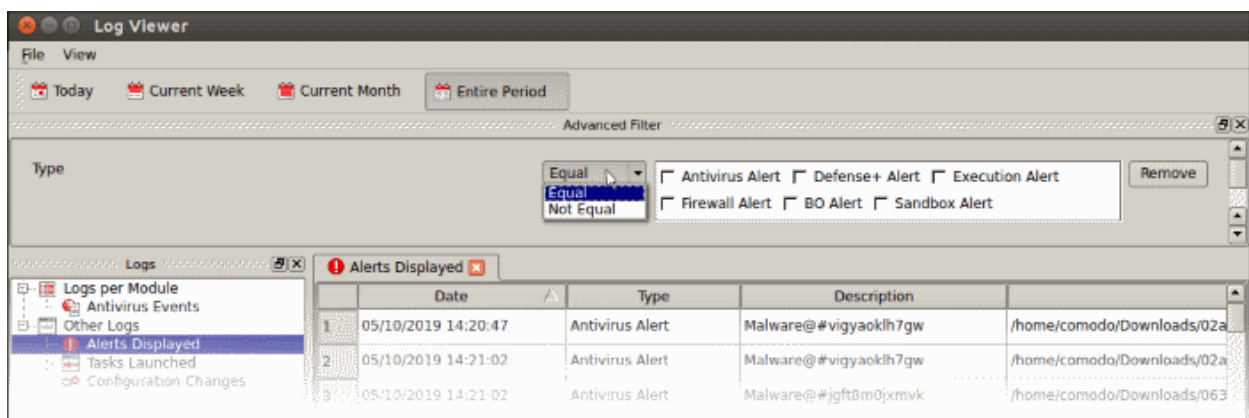
- Select any of the following options in the drop-down:
 - Equal – Show only events that occurred on the specified date
 - Greater than - Show only events that occurred later than the specified date
 - Greater than or Equal – Show only events that occurred on, or after, the specified date
 - Less than - Show only events that occurred before the specified date
 - Less than or Equal – Show only events that occurred on, or before, the specified date
 - Not Equal – Show events that occurred at any time *except* the specified date

- Description:** Filter logs by the name of the malicious item. You need to enter the name of the malware in

the field provided:



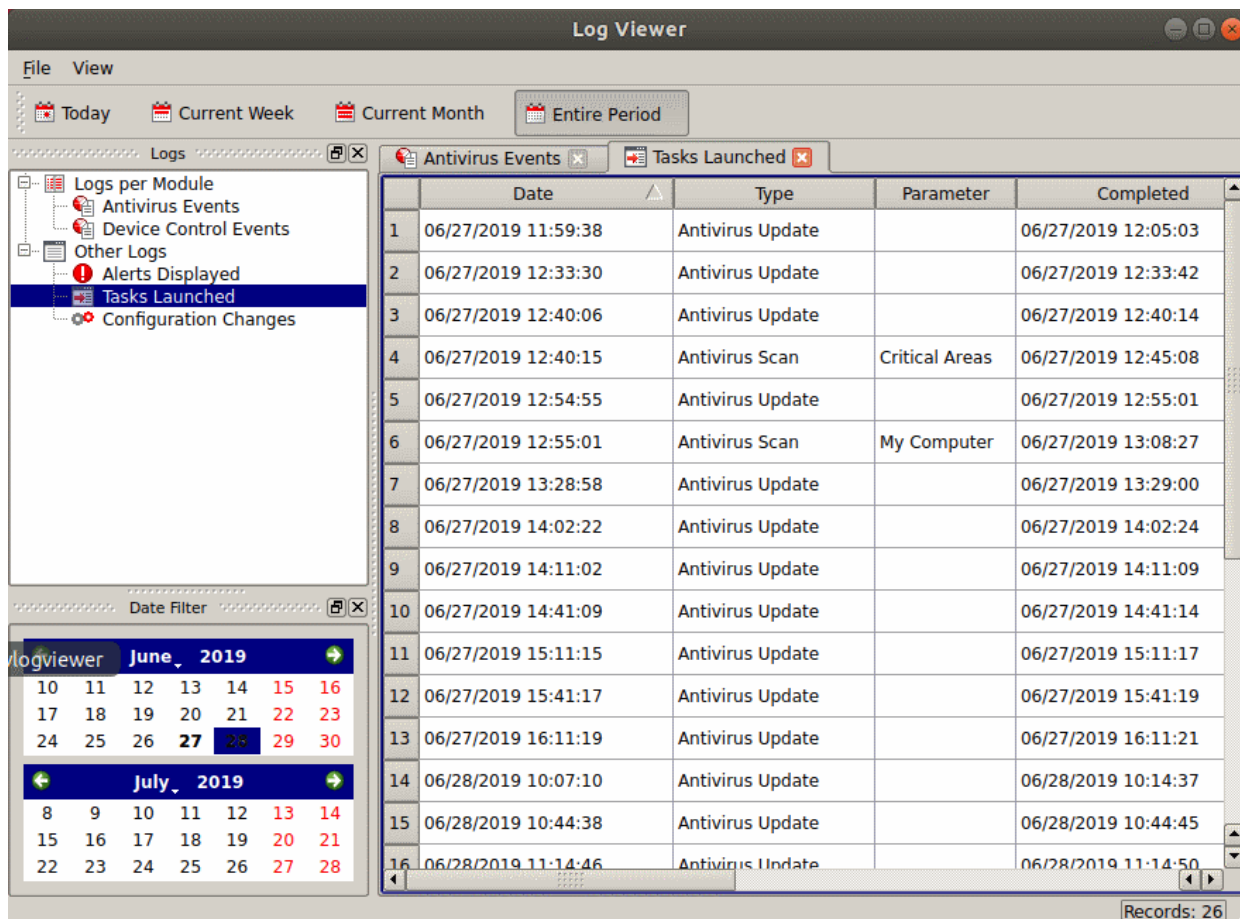
- Select 'Contains' or 'Does Not Contain' from the drop-down:
 - **Contains** – Show only those events which concern the malware named in the text field. You can add multiple malware names.
 - **Does Not Contain** - Show only those events which did not involve the malware named in the text field.
- 5. **Type:** Filter events by alert category. Currently, 'Antivirus' is the only category available.



- Select 'Equal' or 'Not Equal' from the drop-down.
 - **Equal** – Show only events which feature the alert type you select.
 - **Not Equal** - Inverts your choice.

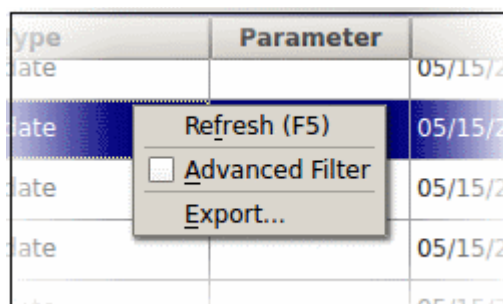
4.4.1.4. 'Tasks Launched' Logs

- Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Tasks Launched'
- Task logs show all activities run by either CCS or the user.
- Example tasks are virus database updates and virus scans. Each row shows the type of task and various other details.



'Tasks Launched' Logs - Column Descriptions	
Column Header	Descriptions
Date	When the task was launched.
Type	The category of the task. For example, 'Antivirus Scan', 'Antivirus Update'.
Parameter	Name of the scan profile. For example, full scan, quick scan, custom scan.
Completed	When the task was finished.
Code	Internal CCS code for the task type.
Info and Additional Info	Details of the task. For example if the task is an antivirus scan, the 'Info' column shows the number of files scanned and the 'Additional Info' column shows the number of identified malware.

- Right-click anywhere inside the log viewer to view further options:



- **Refresh** - Adds recently created logs to the list
- **Advanced Filter** - Filter task events by various criteria, including code, completed and more
- **Export...** - Save the events list as an HTML file.

4.4.1.4.1. Filter 'Tasks Launched' Logs

You can create custom views of all logged events according to the following criteria:

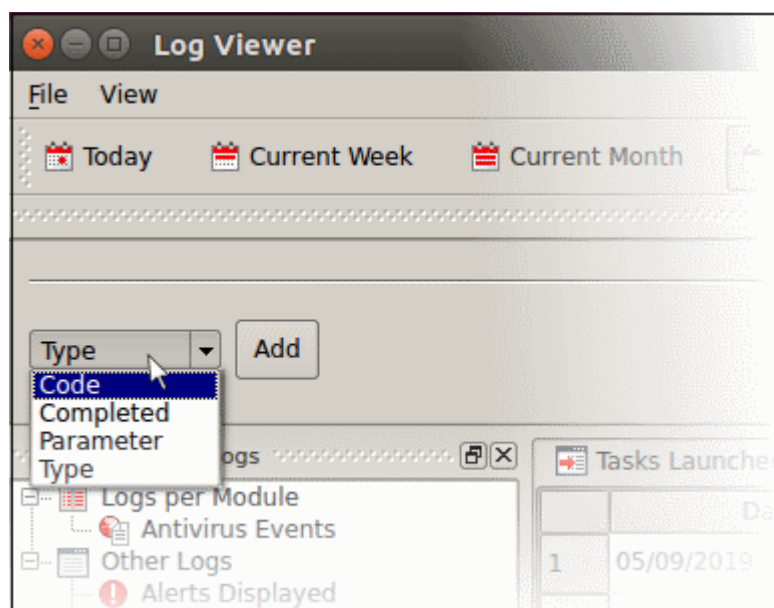
- **Code** - Filter events by the internal CCS code for the task
- **Completed** - Filter by task end date and time
- **Parameter** - Filter by AV scan type. Scan types include full scan, manual scan and quick scan. You can also filter by any custom scan type that you have created.
- **Type** - Filter by task category. Example task categories include antivirus updates, antivirus scans and log clearing.

Configure Event Filters

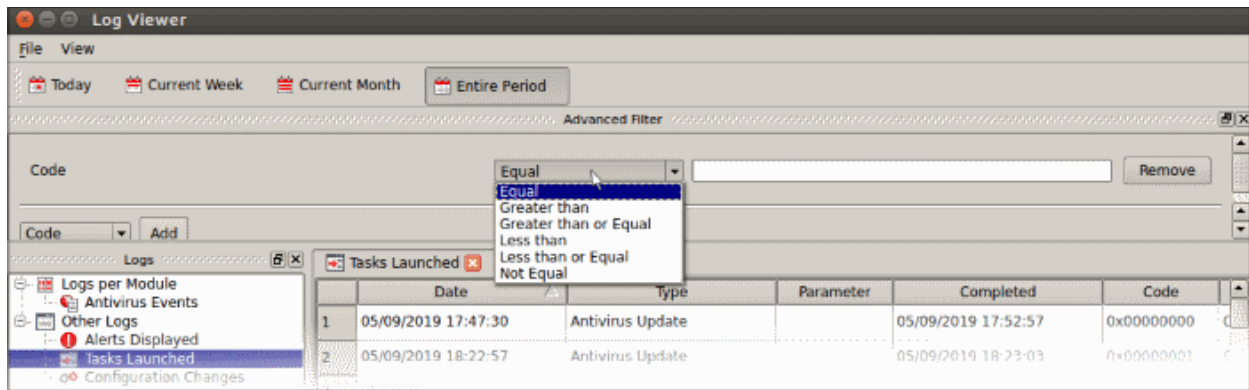
- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Tasks Launched' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'
- OR
- Click 'View' on the menu bar and select 'Advanced Filter'

There are 4 types of filter. Each of these can be further refined by specific parameters.

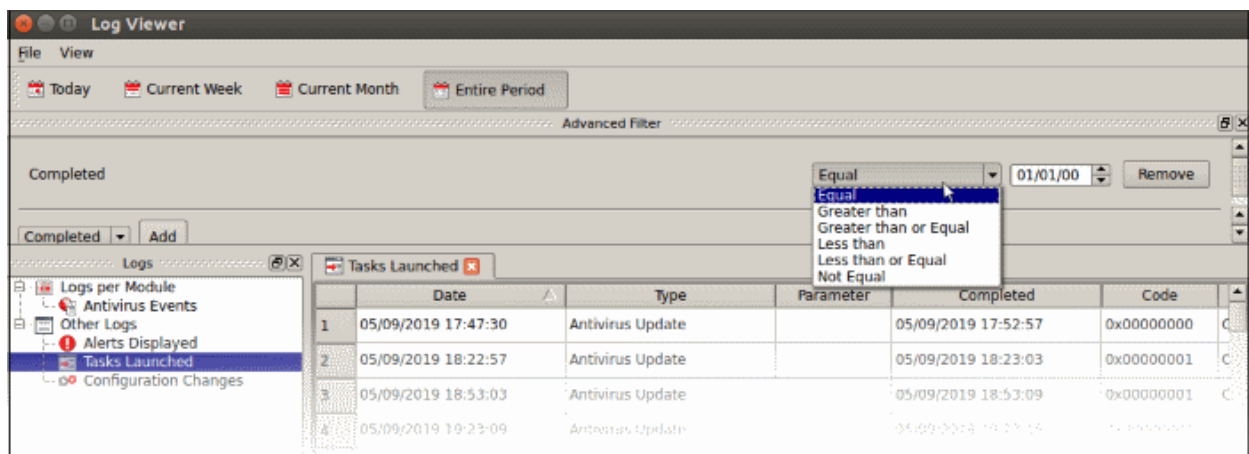
- Select a filter criteria and click 'Add'



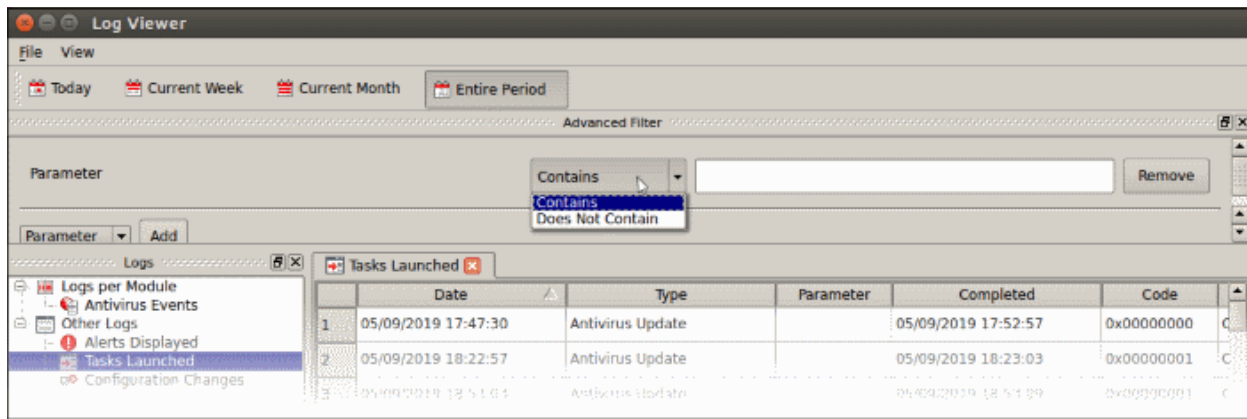
1. **Code**: Filter logs by the CCS code for the task. You need to enter the code value in the field provided.



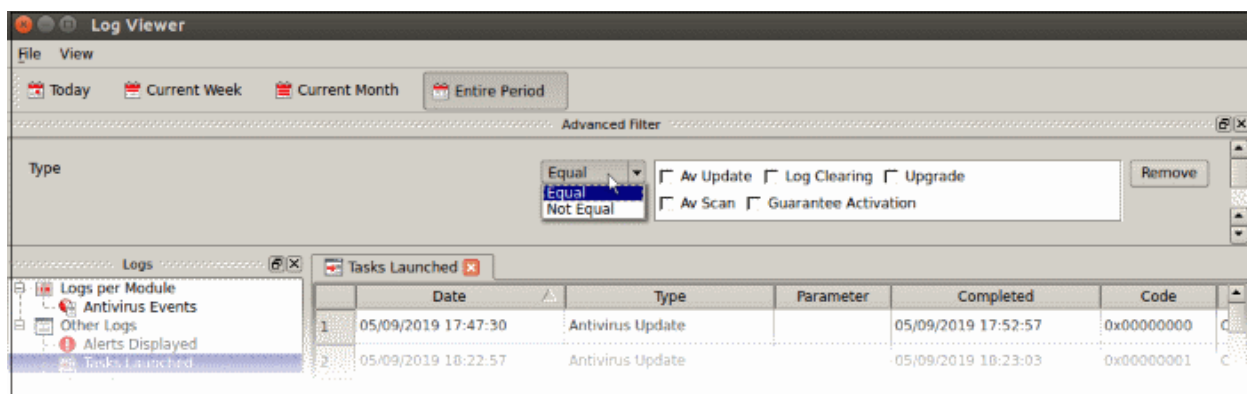
- Select any of the following options from the drop-down.
 - Equal - Show only events matching the CCS Code
 - Greater than - Show only events with a CCS code higher than the specified value
 - Greater than or Equal - Show only events with a CCS code which matches, or is higher, than the specified value
 - Less than - Show only events with a CCS code lower than the specified value
 - Less than or Equal - Show only events with a CCS code which matches, or is lower, than the specified value
 - Not Equal - Inverts your choice. Show all events except those that have the task code you entered
- 2. **Completed:** Filter logs by task end date. You need to specify the date in the field provided. You can then refine your filter by specifying more parameters.



- Select any of the following option from the drop-down.
 - Equal - Show only tasks that occurred on the specified date
 - Greater than - Show only tasks that occurred later than the specified date
 - Greater than or Equal - Show only tasks that occurred on, or later than, the specified date
 - Less than - Show only tasks that occurred before the specified date
 - Less than or Equal - Show only tasks that occurred on, or before, the specified date
 - Not Equal - Show tasks that occurred on any dates *except* the date you specified.
- 3. **Parameter:** Filter logs by antivirus scan type. For example, full scan, manual scan, scan profile. You need to enter the parameter in the text field provided.



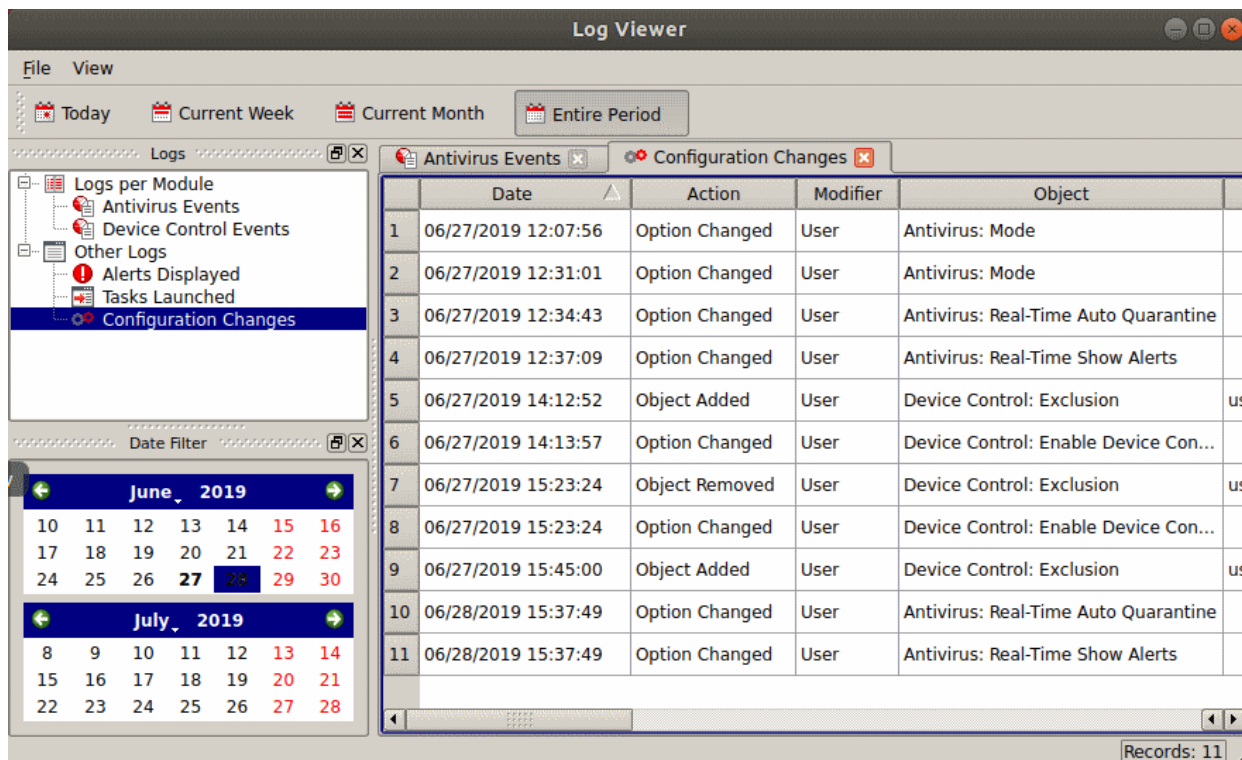
- Select 'Contains' or 'Does Not Contain' from the second drop-down:
 - **Contains** - Show only events which concern the scan type you entered. You can add multiple scan types.
 - **Does Not Contain** - Show all scan types *except* the type you entered.
- 4. **Type:** Filter by task category.



- Select 'Equal' or 'Not Equal' from the drop-down.
 - **Equal** – Show only events which feature the task category you select. You can select multiple categories.
 - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'AV Update' to view every type of task *except* AV updates.
- Select the specific type you want to view from:
 - AV Update – Antivirus database updates
 - AV Scan – Antivirus scan events
 - Log Clearing – Events where logs were deleted
 - Upgrade – Not used.
 - Guarantee Activation – Not used

4.4.1.5. Configuration Change Logs

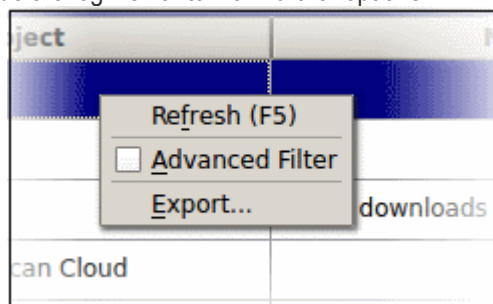
- Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Configuration Changes'
- Configuration change logs record all modifications to CCS settings since installation:



'Configuration Changes' Logs - Column Descriptions

Column Header	Descriptions
Date	When the setting was changed.
Action	The nature of the configuration change. For example, AV profile added.
Modifier	The user that made the configuration change.
Object	The CCS setting that was affected by the change.
Name	The scan profile that was changed.
Old Value	The setting before the configuration change.
New Value	The setting after the configuration change.

- Right-click anywhere inside the log viewer to view further options:



- **Refresh** – Adds recently created logs to the list
- **Advanced Filter** – Filter configuration events by various criteria, including action, type and more.
- **Export...** - Save the events list as an HTML file.

4.4.1.5.1. Filter 'Configuration Change' Logs

You can filter logged events by the following criteria:

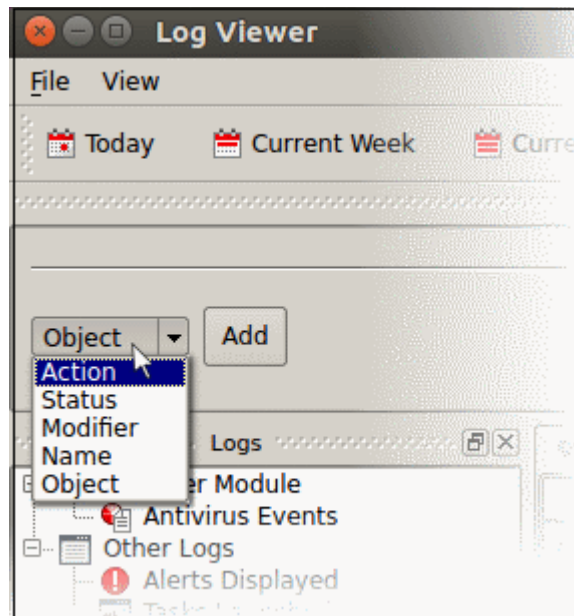
- **Action:** Filter by the activity performed on the item in the 'Object' column. For example, 'Added', 'Changed'.
- **Status:** Not used
- **Modifier:** Filter by who, or what made the change.
- **Name:** Filter by the scan profile affected by the change, if any.
- **Object :** Filter logs based on the setting affected by the change.

Configure Event Filters

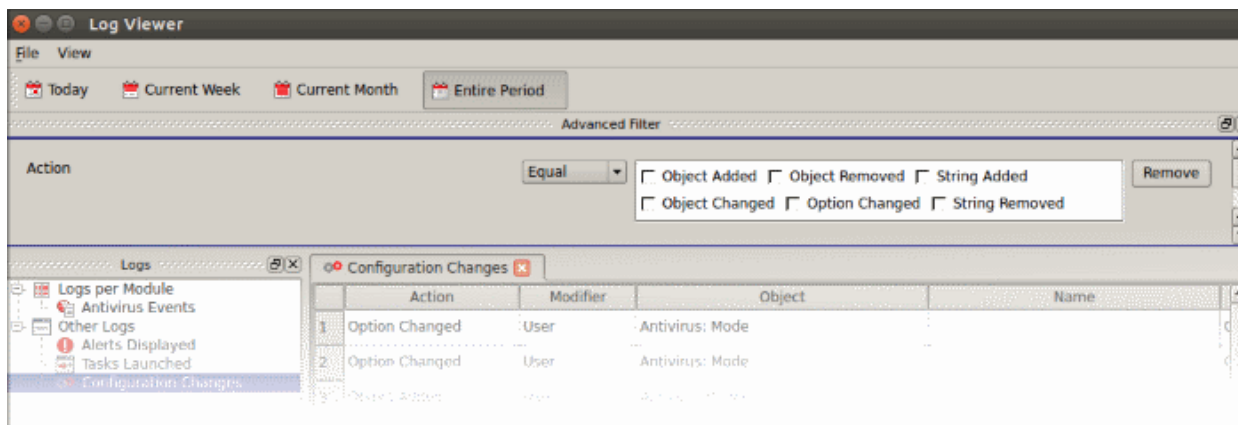
- Open Comodo Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Configuration changes' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'
- OR
- Click 'View' on the menu bar and select 'Advanced Filter'

There are 4 types of filter. Each of these can be further refined by specific parameters.

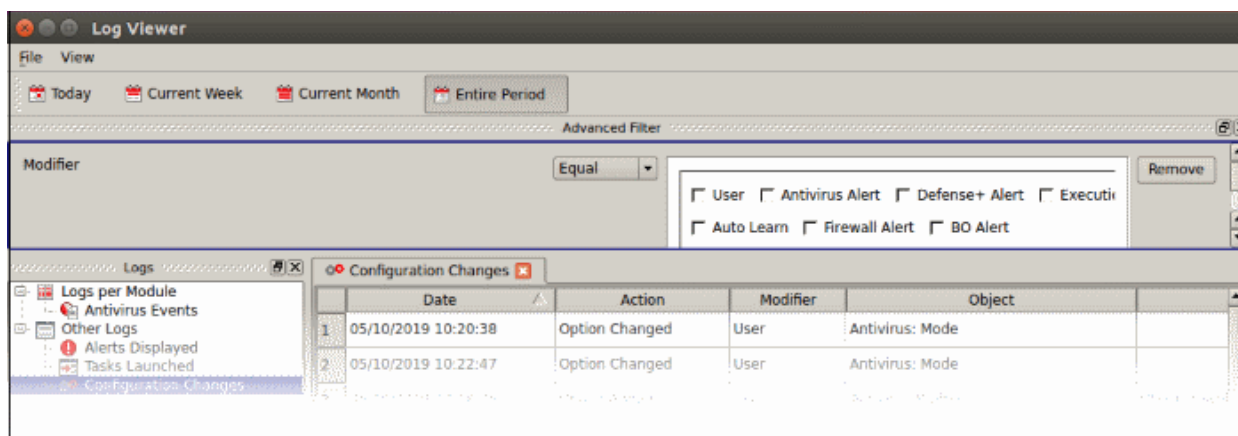
- Select a filter criteria and click 'Add'



1. **Action:** Filter events by the activity which was recorded. For example, 'Object added', 'Object removed', or 'Option changed'.

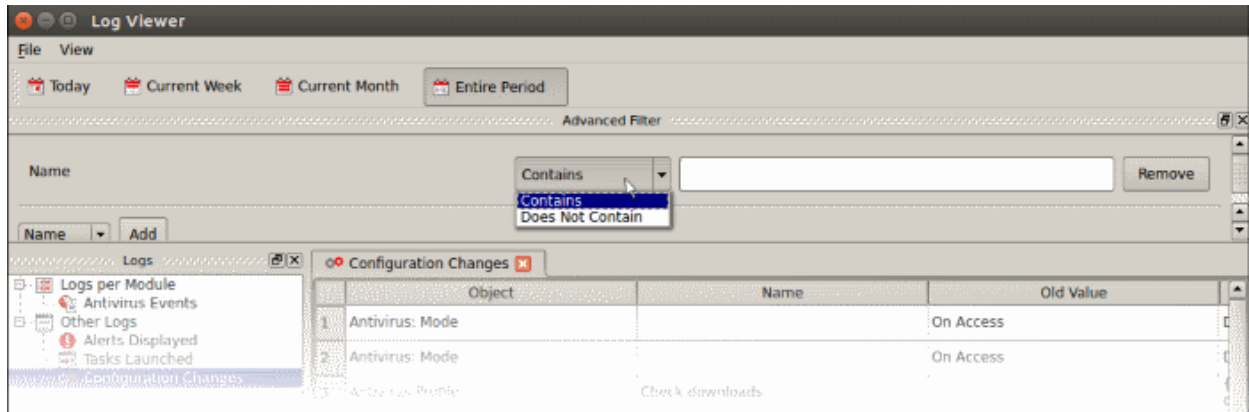


- Select 'Equal' or 'Not Equal' option from the drop-down.
 - **Equal** – Show only events which feature the action you select. You can select multiple actions.
 - **Not Equal** - Inverts your choice. For example, 'Not Equal' + 'Object Added' shows every event except those where objects were added.
- Select the actions you want to view:
 - **Object Added** - Events where an item was created
 - **Object Changed** - Events where an item was modified. For example, an update to a scan profile.
 - **Object Removed** - Events where an item was deleted
 - **Option Changed** - Events where a setting was modified. For example, 'Show scan progress' was changed from enabled to disabled.
 - **String Added** – Not used.
 - **String Removed** – Not used.
- 2. **Modifier:** Filter events by the agent that made the change. 'User' is the only possible option.

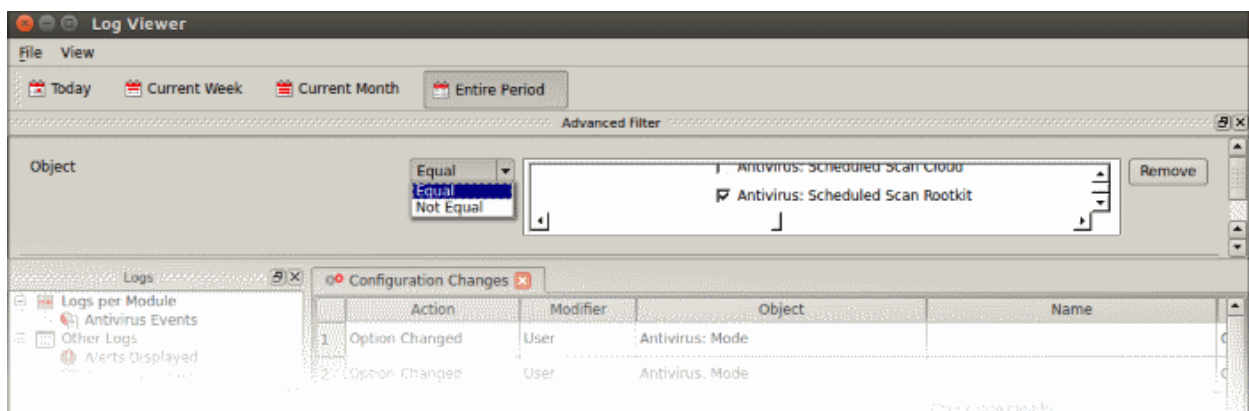


- Select 'Equal' or 'Not Equal' option from the drop-down.
 - **Equal** – Show only events which feature the action you select. You can select multiple actions.
 - **Not Equal** - Inverts your choice. For example, 'Not Equal' + 'User' shows every modification except those by a user.
- Select the configuration changes you want to view:
 - **User** – Show changes which were made by a user
 - **Antivirus Alert** - Not used
 - **Auto Learn** - Not used
 - **Firewall Alert** - Not used

- **Defense+ Alert** - Not used
 - **BO Alert** - Not used
 - **Execution Alert** - Not used
3. **Name:** Filter events by the profile label involved in the configuration change. For example, a folder was added to a particular scan profile. You need to enter the profile name in the field provided:



- Select 'Contains' or 'Does Not Contain' from the drop-down:
 - **Contains** – Show only events which concern the items you specify.
 - **Does Not Contain** – Show all events *except* those that concern the items you specify.
4. **Object:** Filter events by the item that was changed. Examples include AV profile, AV schedule, AV alert timeout, and more.



- The following list shows all available object types:
 - Antivirus Mode
 - Antivirus Timeout
 - Antivirus Realtime AutoUpdate
 - Antivirus Realtime Auto Quarantine
 - Antivirus Realtime Heuristics Level
 - Antivirus Realtime Size Limit
 - Antivirus Realtime Time Limit
 - Antivirus Manual Scan Archives
 - Antivirus Manual Auto Update
 - Antivirus Manual Heuristics Level
 - Antivirus Manual Size Limit
 - Antivirus Manual Scan Cloud

- Antivirus Scheduled Scan Archives
- Antivirus Scheduled AutoUpdate
- Antivirus Scheduled Auto Quarantine,
- Antivirus Scheduled Heuristics Level
- Antivirus Scheduled Size Limit
- Antivirus Scheduled Scan Cloud
- Antivirus Profile
- Antivirus Schedule
- Antivirus Exclusion
- Antivirus Disable Logging
- Active Configuration Index
- Password Protection
- Use Proxy
- Proxy Authentication
- Proxy Server
- Proxy Port
- Proxy Login
- Proxy Password
- GUI Language
- Password
- Updates Host
- Log File Size Limit
- Log overflow handling
- Log Backup Folder

Select 'Equal' or 'Not Equal' option from the drop-down.

- **Equal** – Show only events which feature the action you select. You can select multiple actions.
- **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Antivirus: Alert Timeout' to view every configuration change *except* changes to alert timeouts.

4.5. Browse Support Forums

Click 'More' > 'Browse Support Forums'

You can post questions and suggestions about CCS in our community forum, a message board to discuss anything related to our products.

Visit the forum

- Open Comodo Client Security
- Click the 'More' tab
- Click 'Browse Support Forum' to visit the message board
- New users will need to create an account. Registration is free.
- Post away!! You'll benefit from expert feedback from developers and fellow users alike.

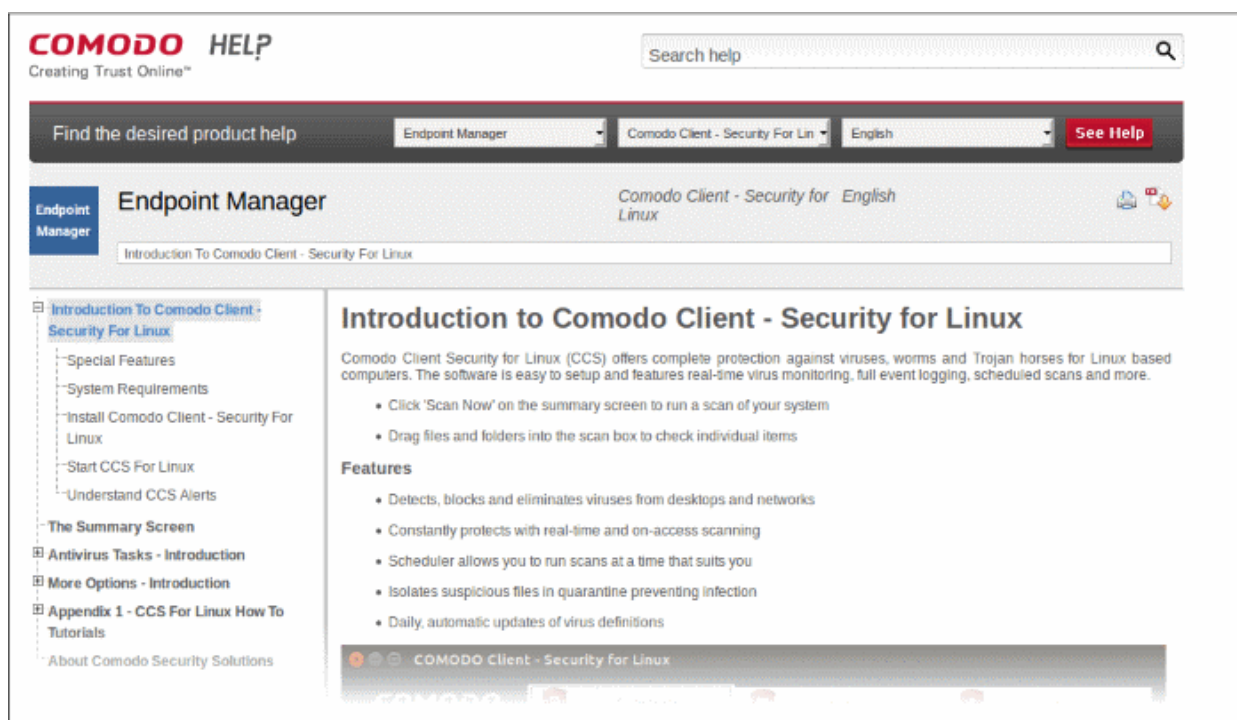
Online Knowledge Base

The knowledge base contains a range of articles and FAQs about Comodo products. It also features a support ticketing system. Visit the knowledgebase at <http://support.comodo.com>. Registration is free.

4.6. Help

Click 'More' > 'Help'

- The help link opens the online user guide at <https://help.comodo.com/>. Each area has its own dedicated page and contains detailed descriptions of the application's functionality.
- Open Comodo Client Security
- Click 'More' > 'Help'

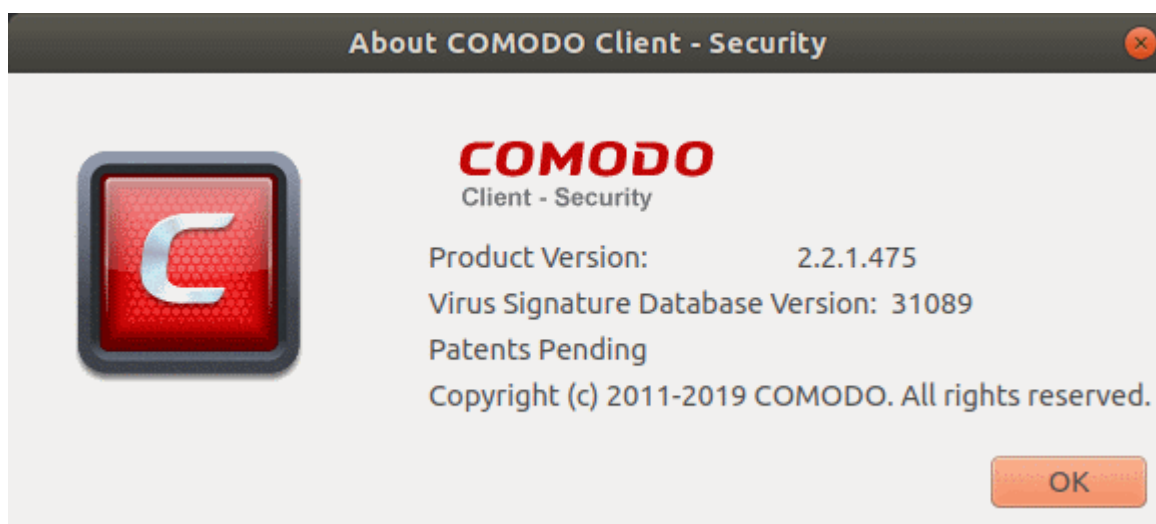


You can also click the pdf icon at top-right to download the guide in PDF format.

4.7. About

The about dialog shows copyright information and the software version number.

- Open Comodo Client Security
- Click 'More' > 'About'



Appendix 1 - CCS for Linux How To... Tutorials

This section contains tutorials on key tasks in Comodo Client Security.

Use the links below to go to each tutorial's page:

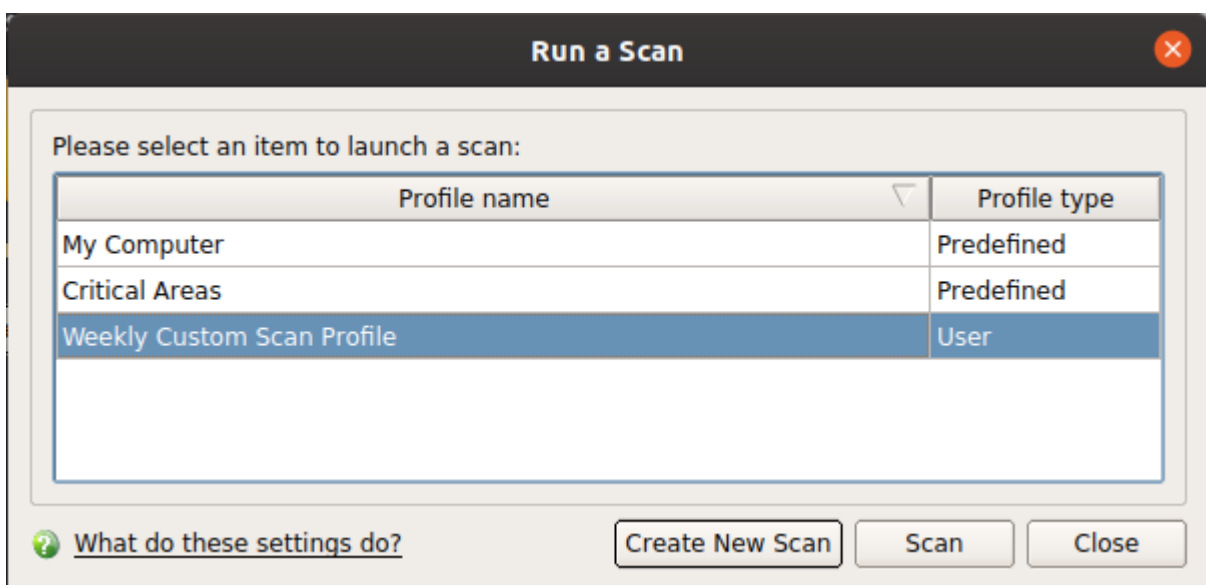
- **Scan your Computer for Viruses** - How to automatically or manually scan your computer
- **View Antivirus Events** - How to view logs made by the virus scanner
- **Configure Database Updates** - Specify how virus signature updates should be handled
- **Quickly Change Security Levels** - How to enable or disable real-time virus scans
- **Change CCS Language Settings** - Change the language used in the CCS interface
- **Run an instant Antivirus scan on Selected Items** - How to run custom scans on specific items or areas
- **Create a Scheduled Scan** - Setup up a virus scan which automatically runs at regular intervals
- **Restore Incorrectly Quarantined Item(s)** - Revert quarantined files to their original location
- **Switch Off Automatic Antivirus Updates** - Disable automatic and virus signature database updates
- **Control External Device Accessibility** - Restrict access to external devices such as USB pen drive

Scan your Computer for Viruses

You can run a full scan, a quick scan, or create a custom scan according to your preferences.

Run an on-demand virus scan

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Run a Scan' in the antivirus tasks area



CCS ships with two pre-defined scan profiles

- **My Computer** - Scans every drive, folder and file on your system, including external devices.
- **Critical Areas** - A targeted scan of important files and folders.
Select the profile you want to use then click 'Scan'.
- **Create New Scan**. Create your own custom scan of specific files, folders or drives. See **custom scan** to find out more.

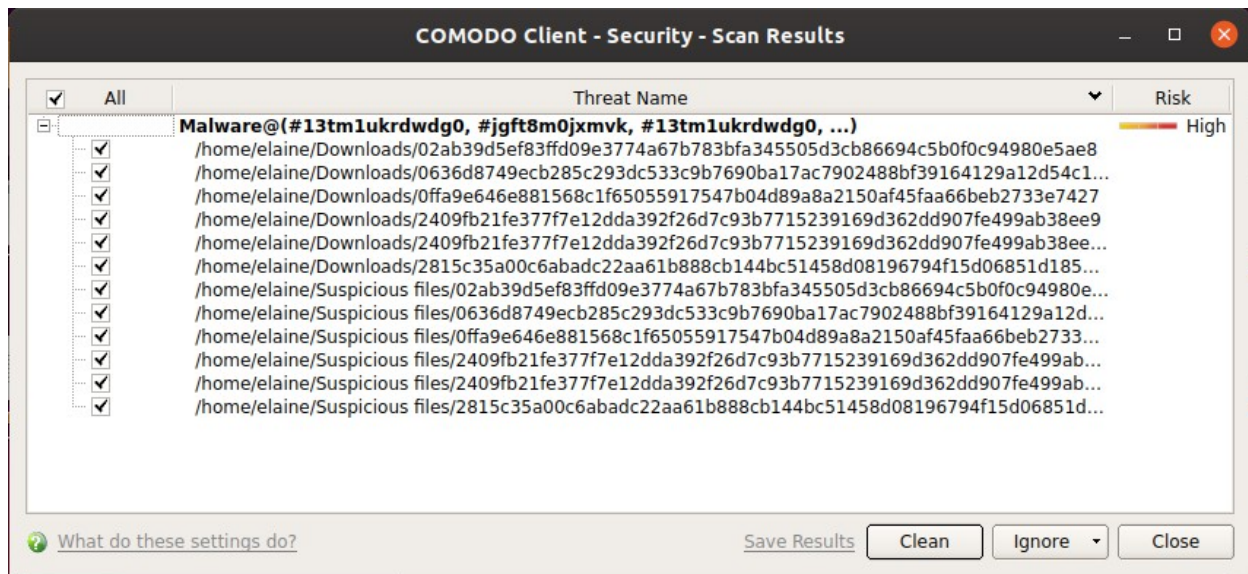
CCS will check for and download any available updates before starting the scan. The scan will commence after updates have been installed:



Results are shown at the end of the scan:



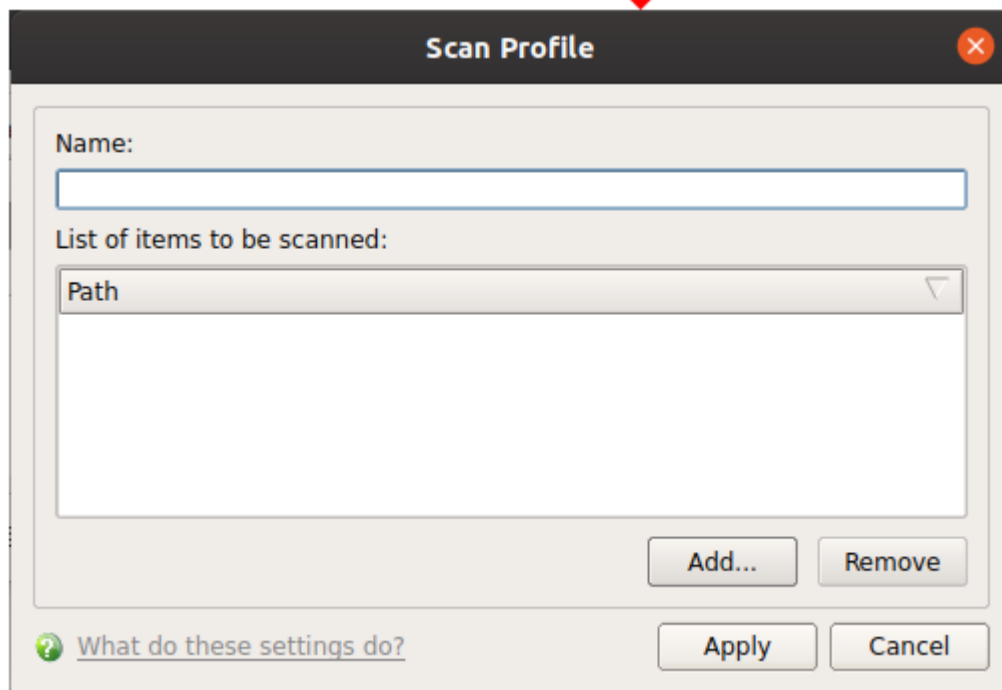
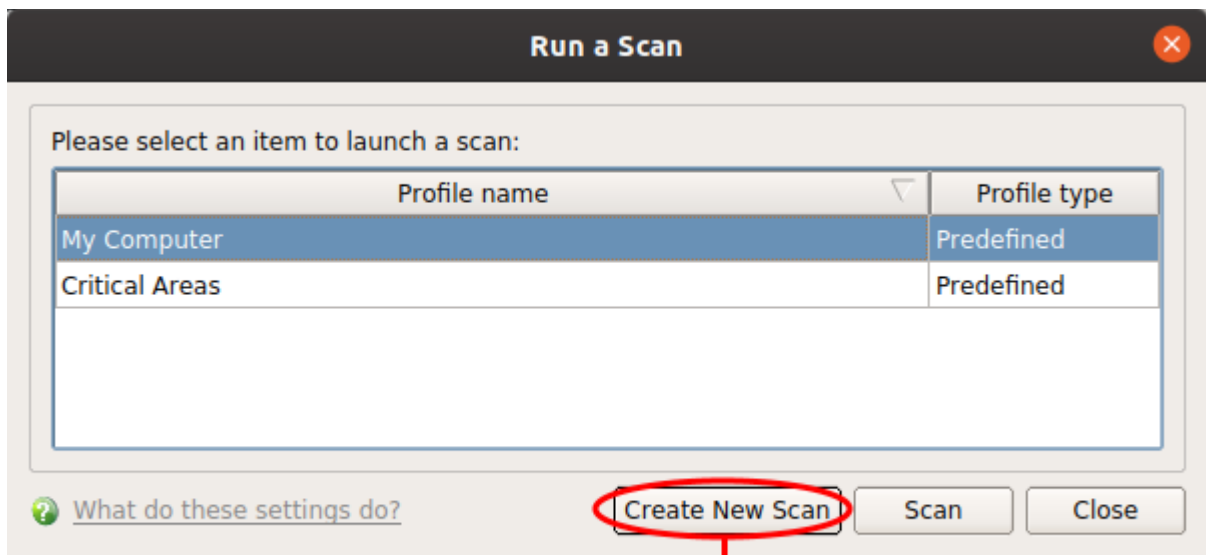
- Click the 'Results' button to see detailed file information.
- The results window shows any threats discovered by the scan and lets you decide how to handle them:



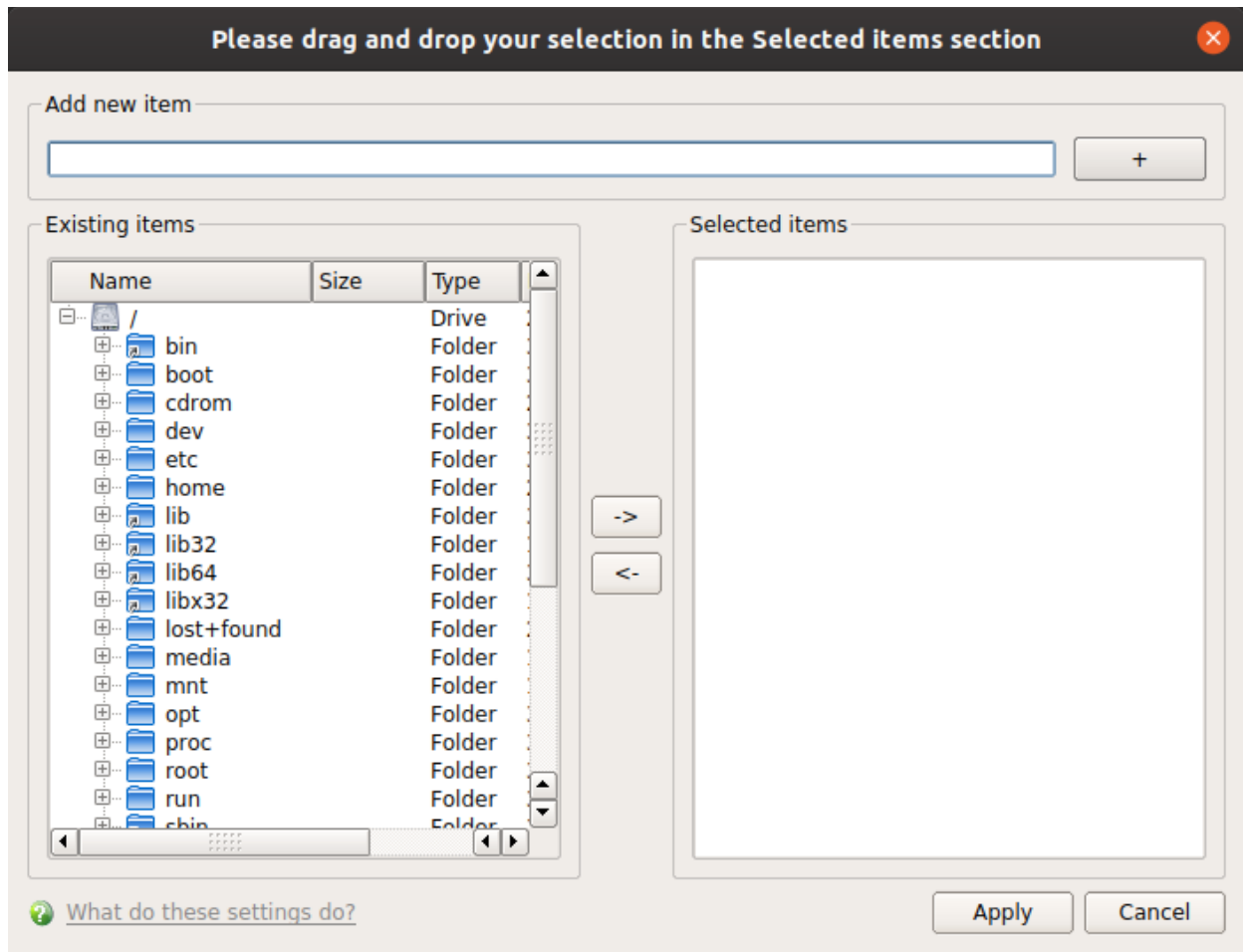
- **Clean** - If a disinfection routine exists, CCS will remove the infection and retain the original file. If no routine exists, CCS will move the file to **Quarantine**.
- **Ignore** - Two options:
 - **Once** - The file is removed from the threat results and remains in its current location. The file will be detected as a threat again by the next scan.
 - **Add to Exclusions** – Creates an exception for the file. The virus scanner will skip the file in future and not consider it to be a threat. The file is added to the **Exclusions** list.
- **Save Results** - Export the scan results to a text file.
- Select 'All' if you want to apply 'Clean' or 'Ignore' actions to every threat.

Create a new scan profile

- Open Comodo Client Security
- Click the 'Antivirus' tab > Click 'Run a Scan'
- Click 'Create New Scan'



- **Name** - Create a label for the scan profile.
- Click 'Add' to select the files/ folders/ drives you want in the scan

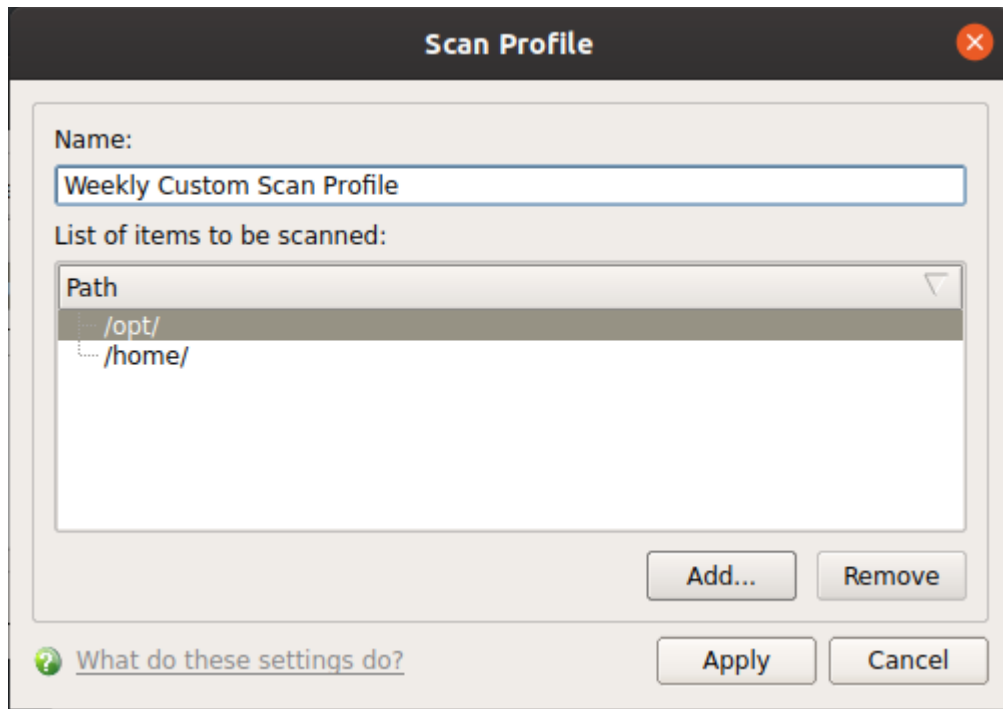


There are two ways to add items:

- Manually enter the path in the 'Add new item' field > Click the '+' button

OR

- Drag and drop items from the left pane to the right pane.
- Repeat the process to add multiple items
- Click 'Apply'.



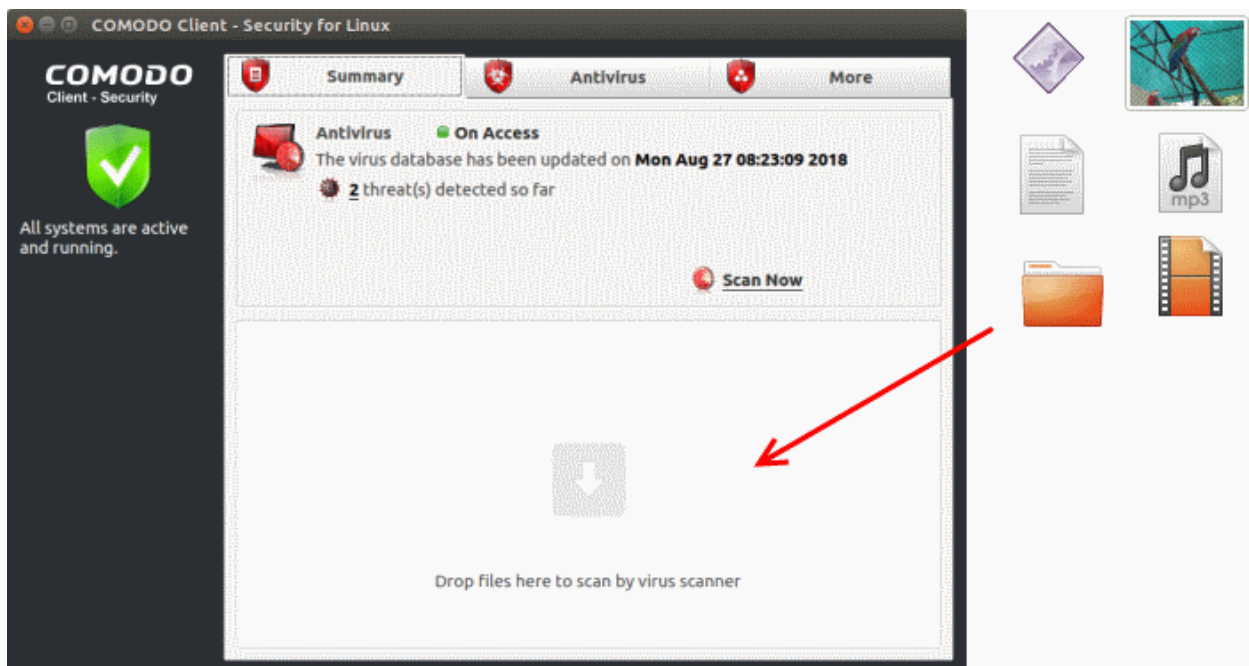
- Click 'Apply' again to save the profile.

You can also create profiles in the **Scan Profiles** area (open CCS > 'Antivirus' tab > 'Scan Profiles')

- Note: Managed endpoints – Scan profiles should be configured in an Endpoint Manager profile.

Instantly Scan Objects

- Drag items into the scan box on the summary screen.
- You can drag virtually any type of item - files, folders, photos, applications or drives.



See [Run an Instant Antivirus Scan on Selected Items](#) for more help with this.

View Antivirus Events

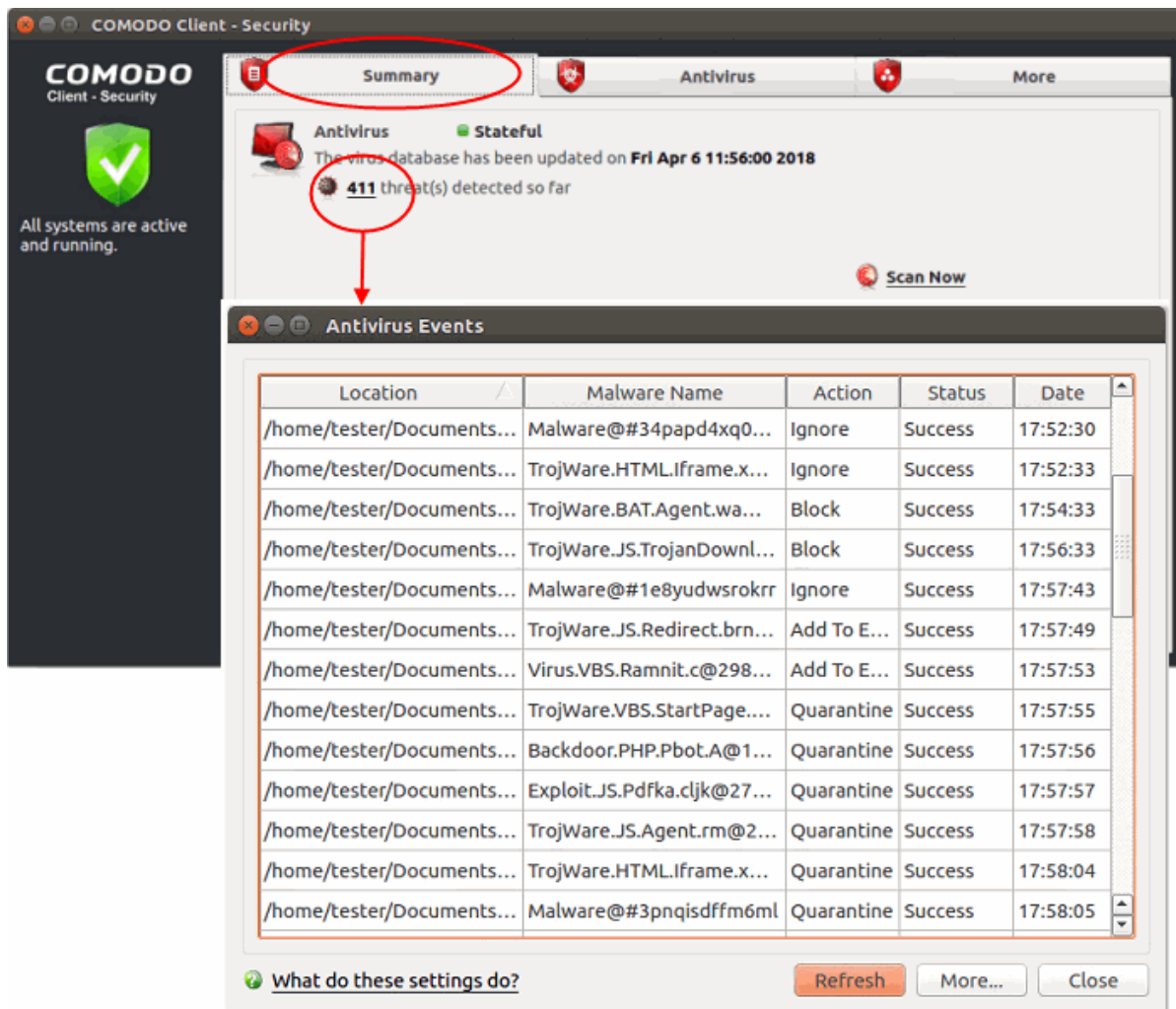
The events area is a log of actions taken by CCS when it encounters a malicious file.

The basic event viewer shows:

- The name of the malware and the location where it was detected on your computer
- The date and time it was detected
- The action that was taken on the malware by CCS, and whether or not the action was successful.

View antivirus events

- Open Comodo Client Security at the summary screen
- Click the number in front of 'threat(s) detected so far' on the home screen
- Or
- Click 'More' > 'View Antivirus Events'



- See [View Antivirus Events](#) for more help with event logs.
- Click the 'More' button to open the '[Log Viewer Module](#)'.

Configure Database Updates

It is essential you have the latest virus database to ensure you are protected against the newest threats.

- Note: Managed endpoints – Database update settings should be configured in an Endpoint Manager profile.

The default policy of CCS for Linux:

- i. Periodically check for and download database updates
- ii. Automatically update the virus database before starting a scan.

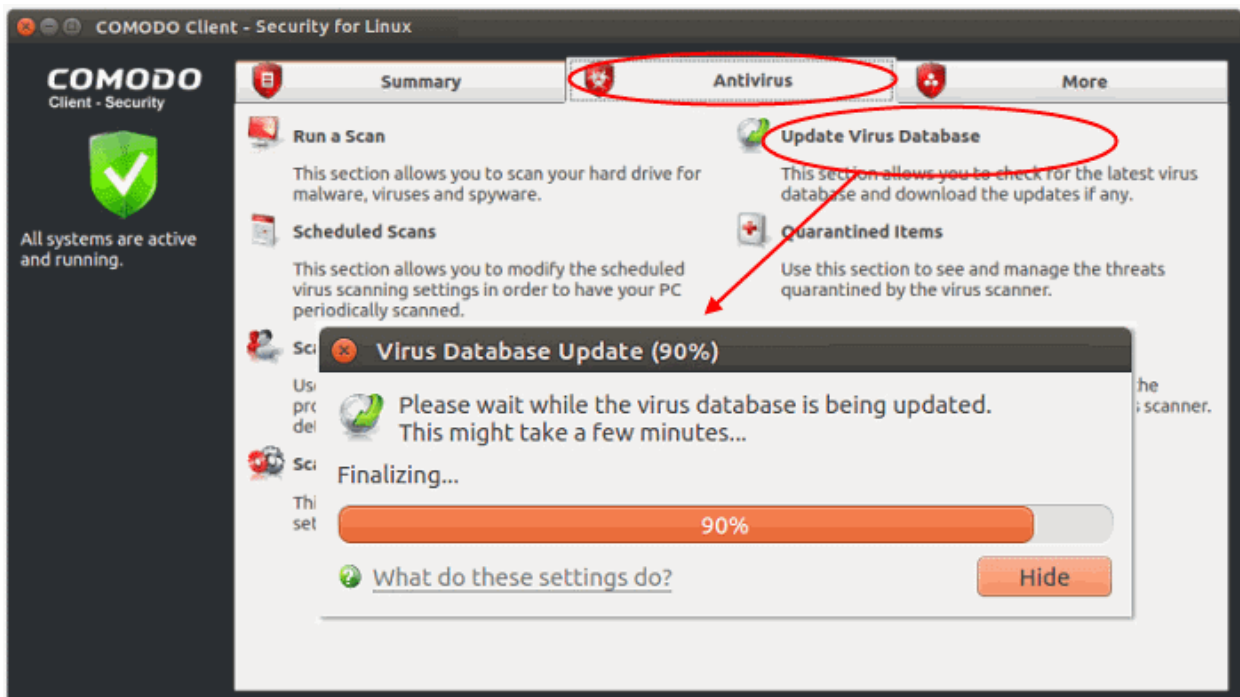
See the following links for more details:

- [Manually update the virus database](#)
- [Configure automatic database updates](#)

Manually update the virus database

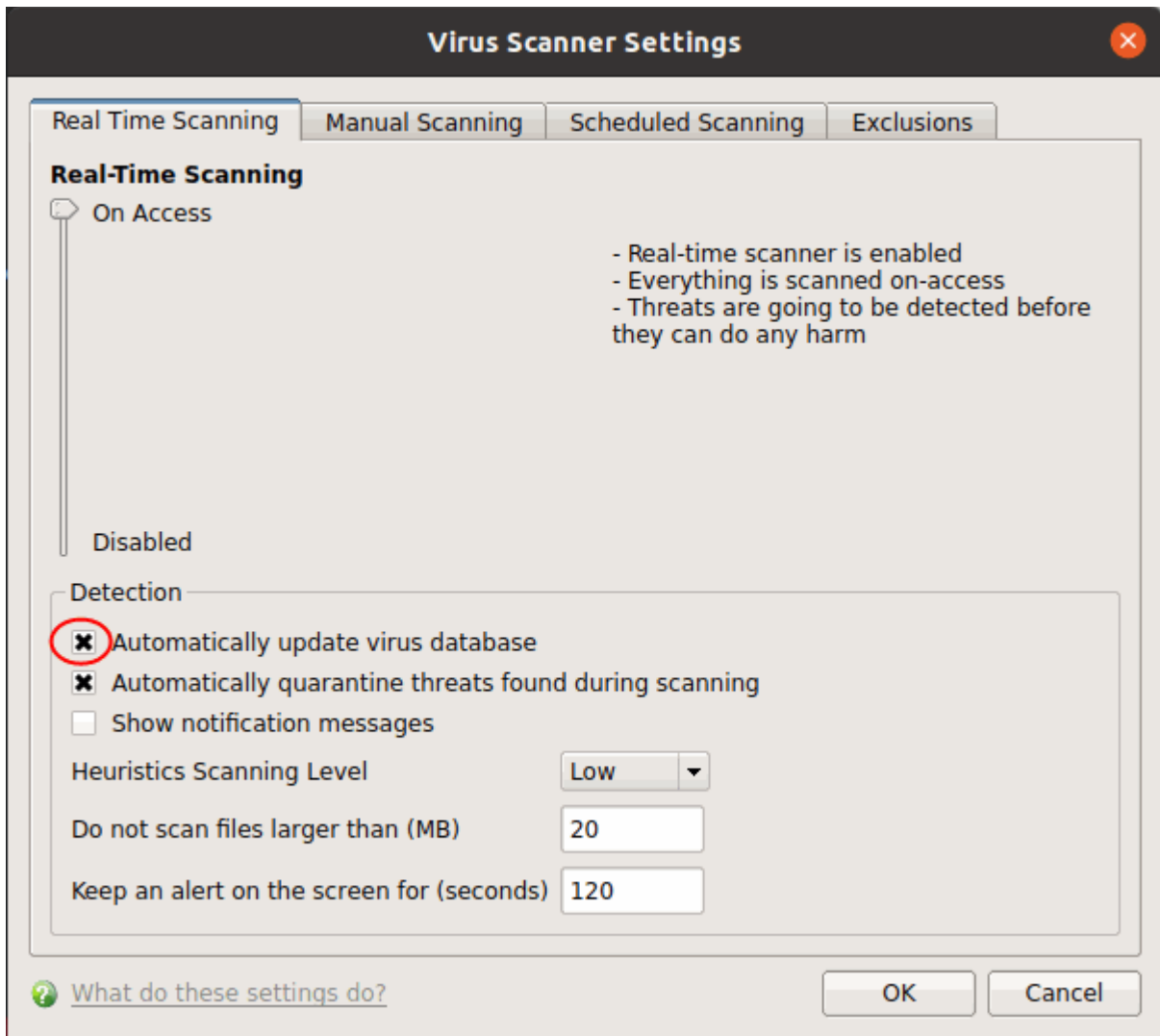
- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Update Virus Database' on the tasks screen

CCS will contact Comodo servers and download any available updates. Please ensure you are connected to the internet.



Configure automatic database updates

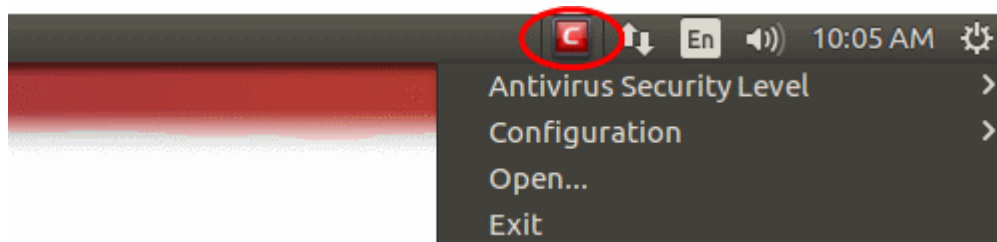
- Open Comodo Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Select 'Real Time Scanning'
- Enable the 'Automatically update virus database' option



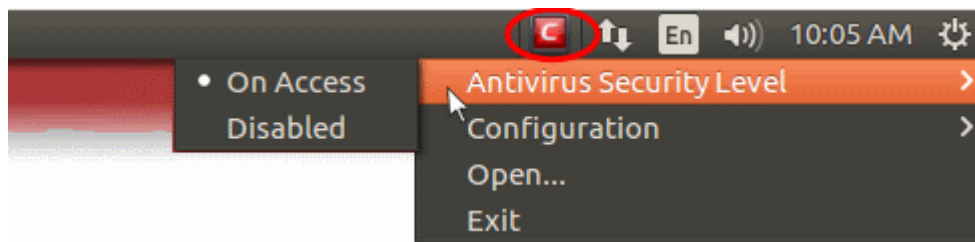
- Note - You can enable or disable pre-scan updates for manual and scheduled antivirus scan types. See '[Scanner Settings](#)' if you need more help with this.

Quickly Set up Security Levels

- Right-click on the CCS menu bar icon to quickly view or change the current security level:



- Move your mouse cursor over 'Antivirus Security Level'



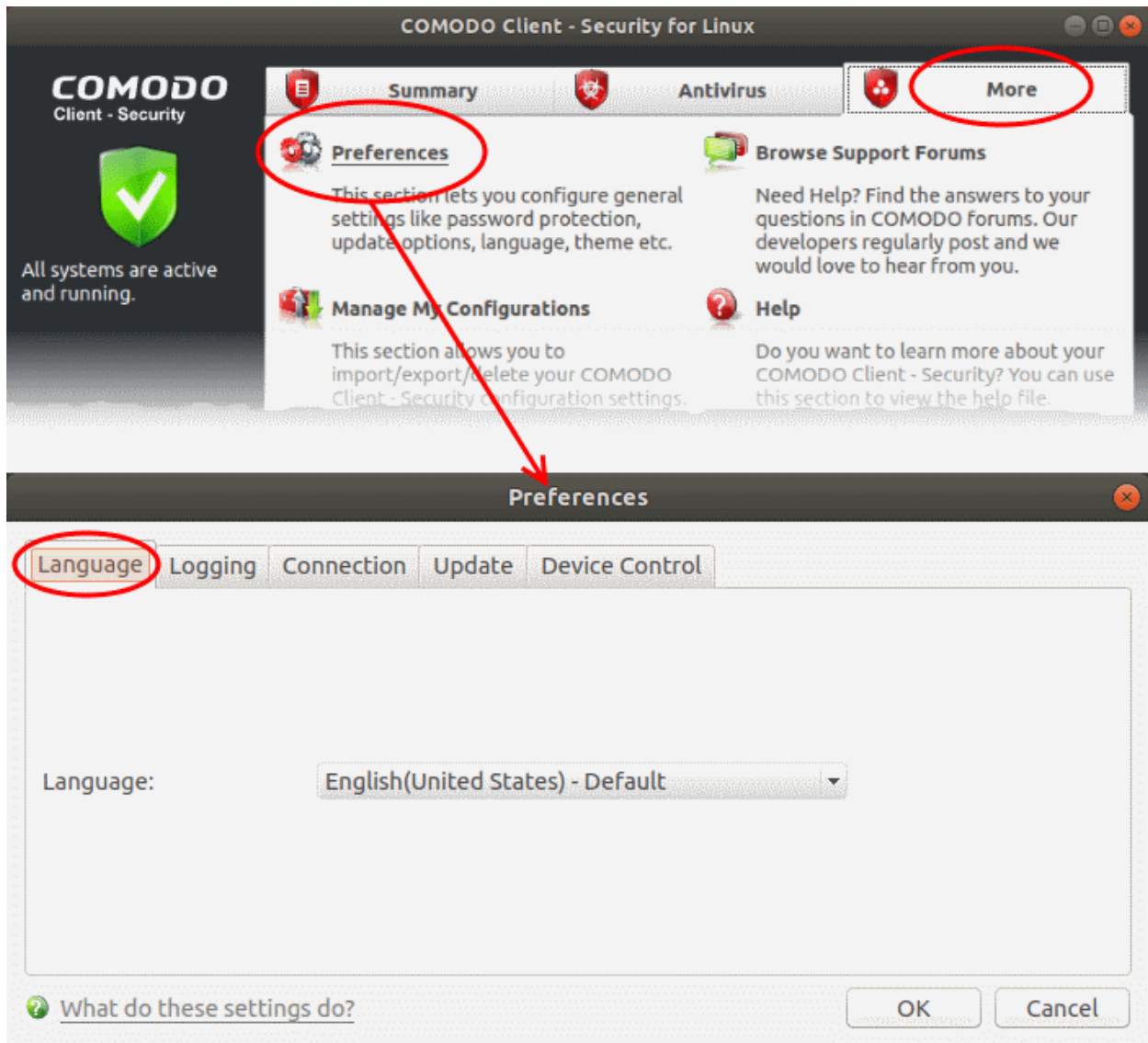
- **On Access** - Files will be scanned as soon as you open them. 'On access' is another name for the 'Real-Time Scanning' feature that is mentioned elsewhere in the interface. We highly recommend you leave this enabled.
- **Disabled** - Not recommended. Files are not scanned when they are opened, increasing the likelihood that your system will get infected.

The currently active configuration is shown with a check-mark next to it. See [Real Time Scan](#) for more details.

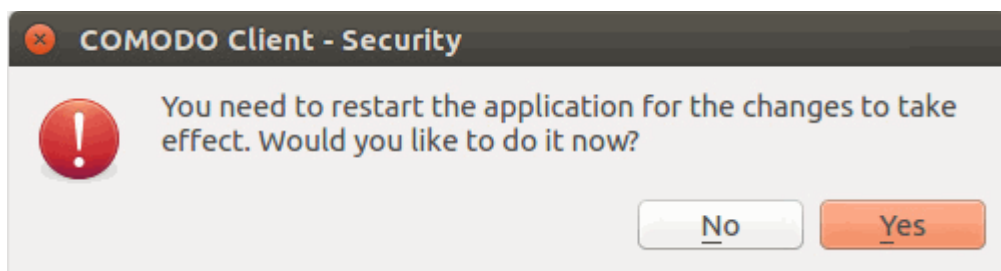
You can also access these settings from the [summary screen](#).

Change CCS Language Settings

- Open Comodo Client Security
- Click 'More' > 'Preferences'
- Click the 'Language' tab



- Choose the language you wish to use from the drop-down menu
- Click 'OK' then restart the application to apply your changes:



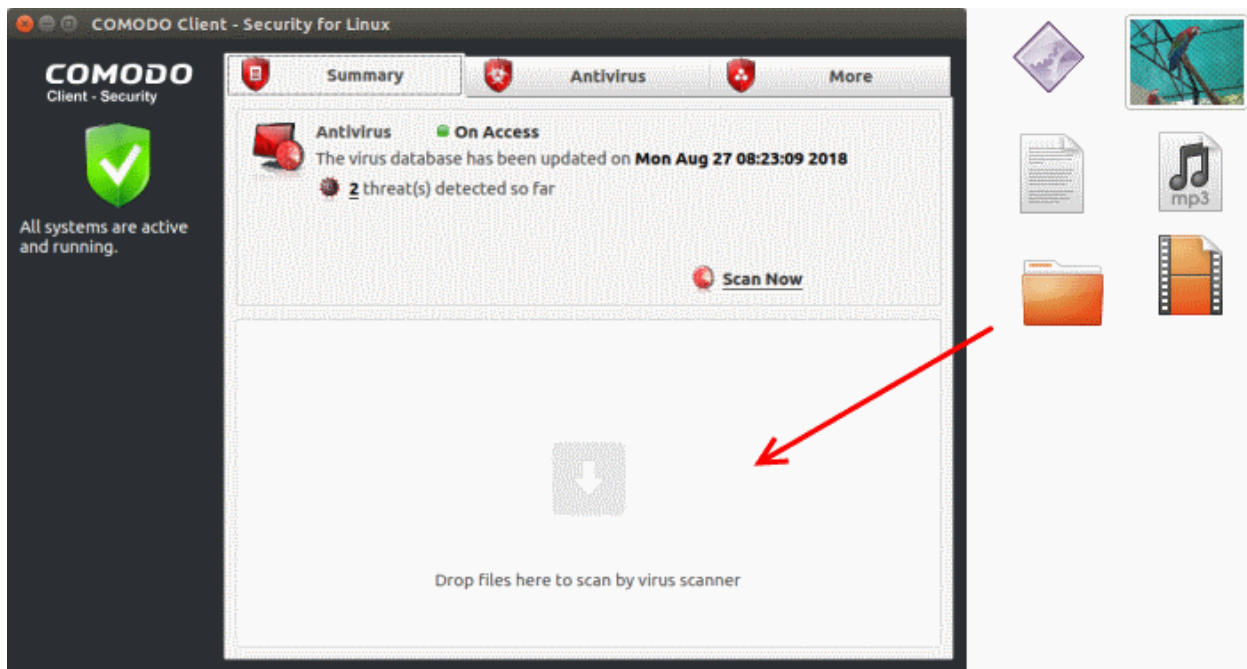
- Note: Managed endpoints – You should configure language preference in an Endpoint Manager profile.

Run an Instant Antivirus Scan on Selected Items

- You can instantly scan a file, folder or drive by dragging them into the scan box on the 'Summary' screen
- You can also drag them onto the Comodo icon on the dock

Instantly scan items

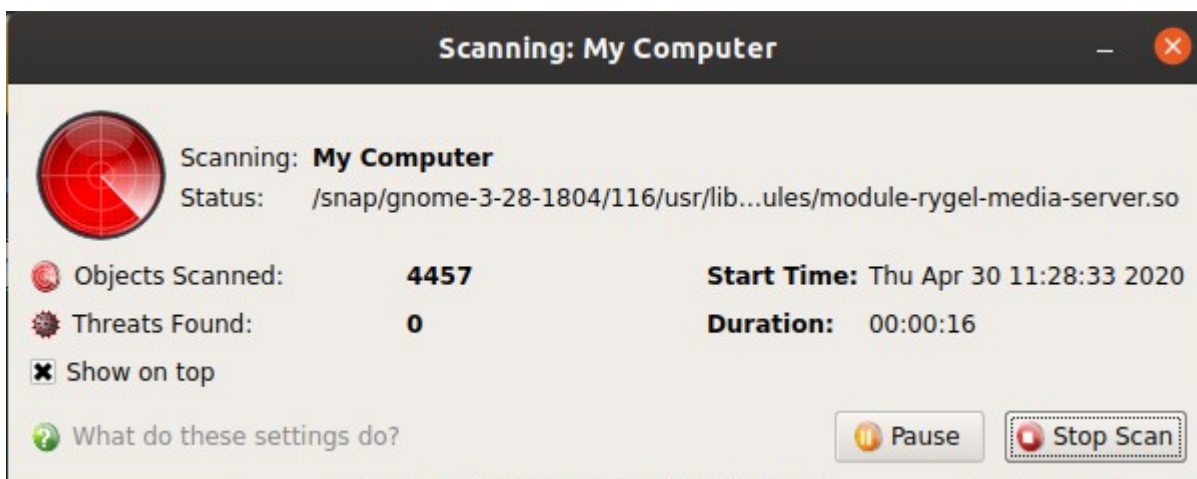
- Open Comodo Client Security
- Drag the items into the scan box in the 'Summary' interface
- You can drag virtually any type of item - files, folders, photos, applications or drives.



CCS will first check for AV database updates. If updates are available they will be downloaded and installed:



The scan will begin immediately after the updates are installed.



The results will be shown at the end of the scan. The results show any threats found along with their location and severity level.

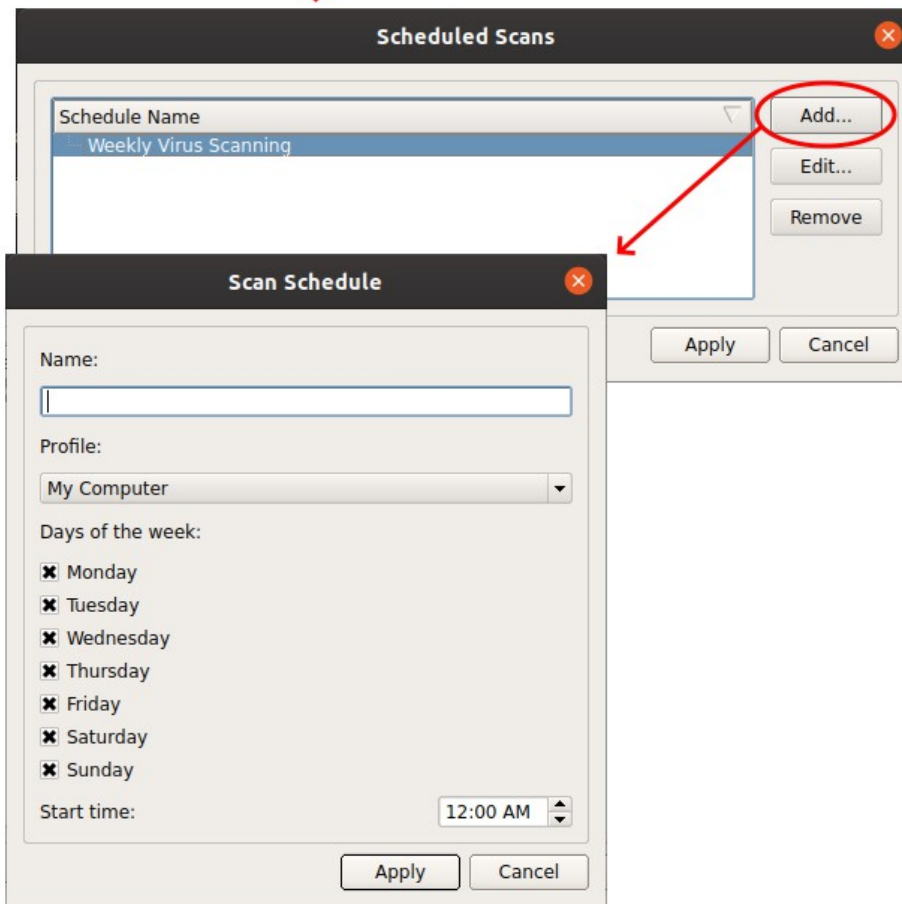
See [Run a Scan](#) for help on how to react if infected item(s) are found.

Create a Scheduled Scan

- The highly customizable scheduler lets you timetable virus scans to run when you decide.
- You can schedule a scan of your entire computer or specific areas. You can create multiple schedules.
- You can run scans at daily, weekly, monthly or custom intervals.
- Note: Managed endpoints – You should configure scan schedules in an Endpoint Manager profile.

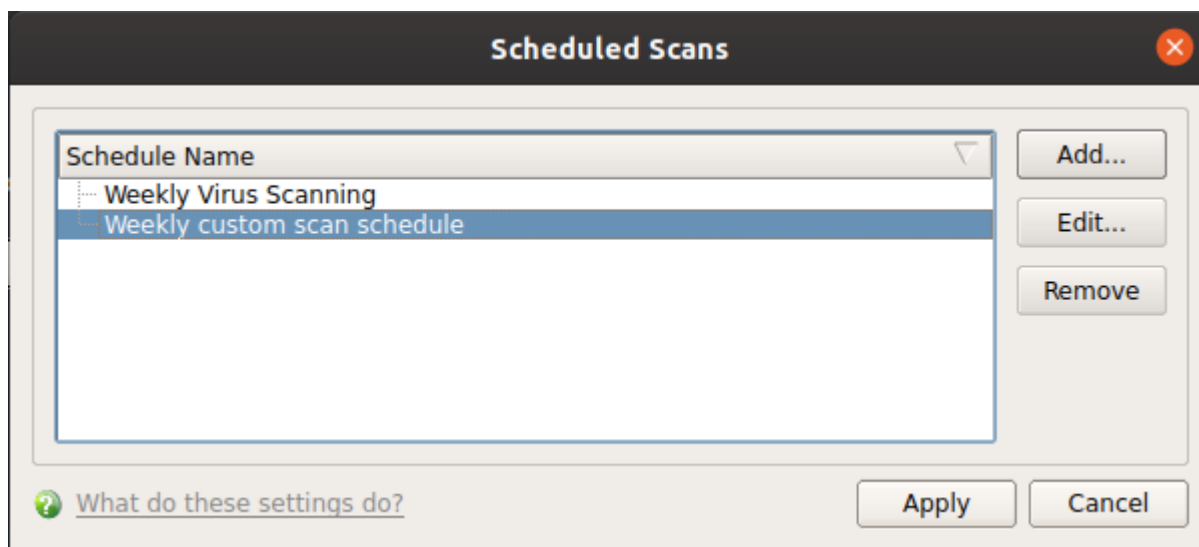
Create an antivirus scan schedule

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scheduled Scans'
- Click 'Add' to create a new schedule:



- **Name** - Create a label for the new schedule. E.g. 'Daily scan of external devices'
- **Profile** - The profile determines which areas of your computer are scanned:
 - Full Scan - Scans every file, folder and drive on your system
 - Quick Scan - A targeted scan of important operating system and user files/folders
 - Custom Scan - A user-created scan of specific items
 - See **Scan Profiles** for more advice on profiles
- **Days of the week** - Select the weekdays the scan should run.
- **Start time** - Select the time the scan should start on the specified weekdays
- Click 'Apply'.

Your new schedule will be listed in the scheduled scans interface:

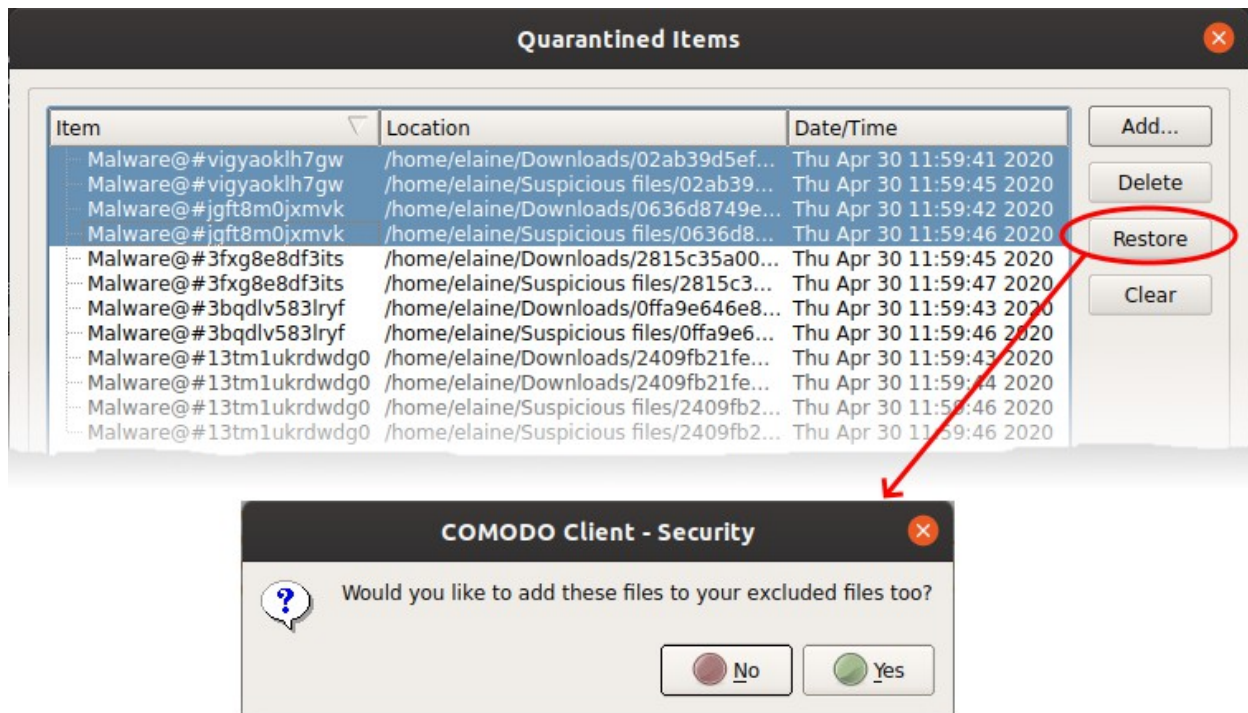


- Click 'Edit' to modify a profile.
- Click 'Remove' to delete a profile.
- For more details, see [Scheduled Scans](#).

Restore Incorrectly Quarantined Item(s)

You can restore items you believe were incorrectly quarantined to their original location:

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Quarantined Items'
- Select the items you want to restore. Hold down the command key to select multiple items
- Click 'Restore'



You will be asked if you want to add the item to the Scan Exclusions list:

- **'Yes'** - The file is restored to its original location. It is not flagged as dangerous nor quarantined by future antivirus scans. You can manage excluded items in the Scanner Settings interface ('Antivirus' > 'Scanner Settings' > 'Exclusions'). See [Exclusions](#) for more details.
- **'No'** - The file is restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.

Switch off Automatic Antivirus Updates

- By default, Comodo Client Security automatically checks for software and virus database updates.
- However, some users like to have control over what gets downloaded and when it gets downloaded.
- For example, network admins might not want automatic downloads because they take up too much bandwidth during the day.
- CCS provides full control over virus and software updates.
- Note: Managed endpoints – Automatic antivirus updates should be configured in an Endpoint Manager profile.

Automatic updates can be disabled on a per-scanner basis. The following links explain how to do this for each type:

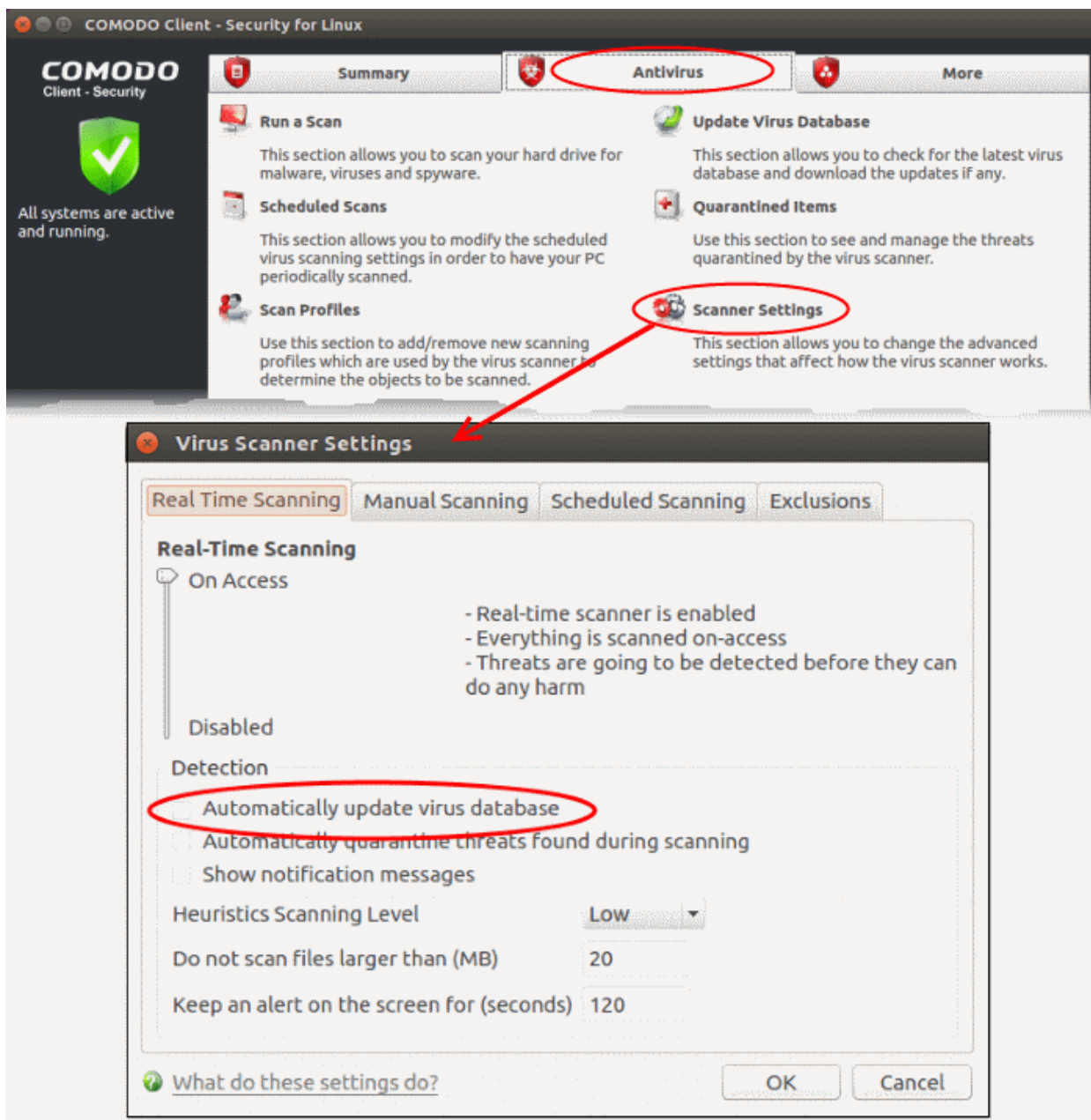
- [Switch off automatic updates in general](#)
- [Switch off updates prior to manual scans](#)
- [Switch off updates prior to scheduled scans](#)

Switch off automatic updates in general

Disabling updates here means CCS will not download updates in the background.

- Open Comodo Client Security

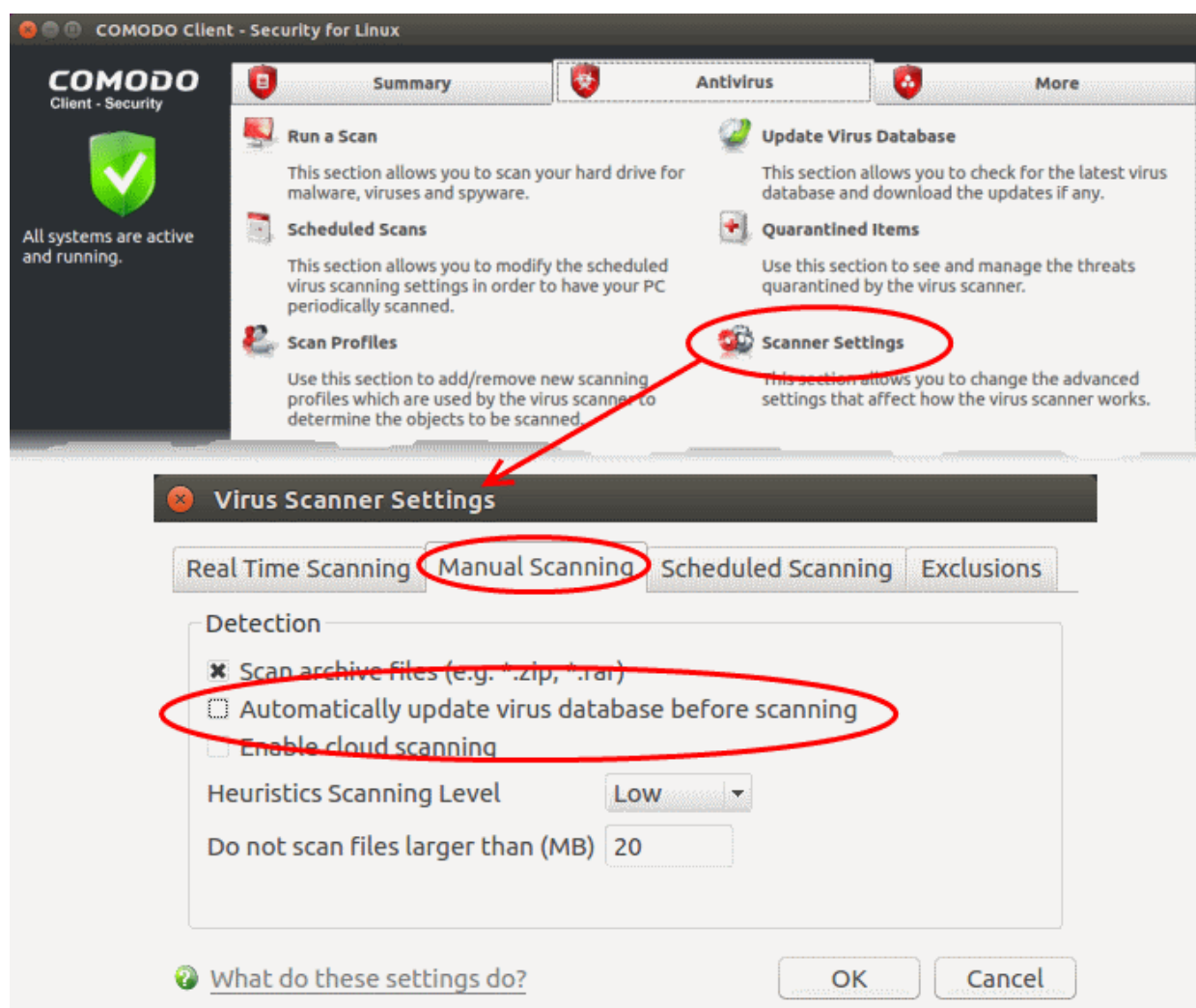
- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Real Time Scanning' tab
- Deselect 'Automatically update virus database':



- Click 'OK'
- You can still update the database manually by clicking the 'Update' tile on the home screen.

Switch off updates prior to manual scans

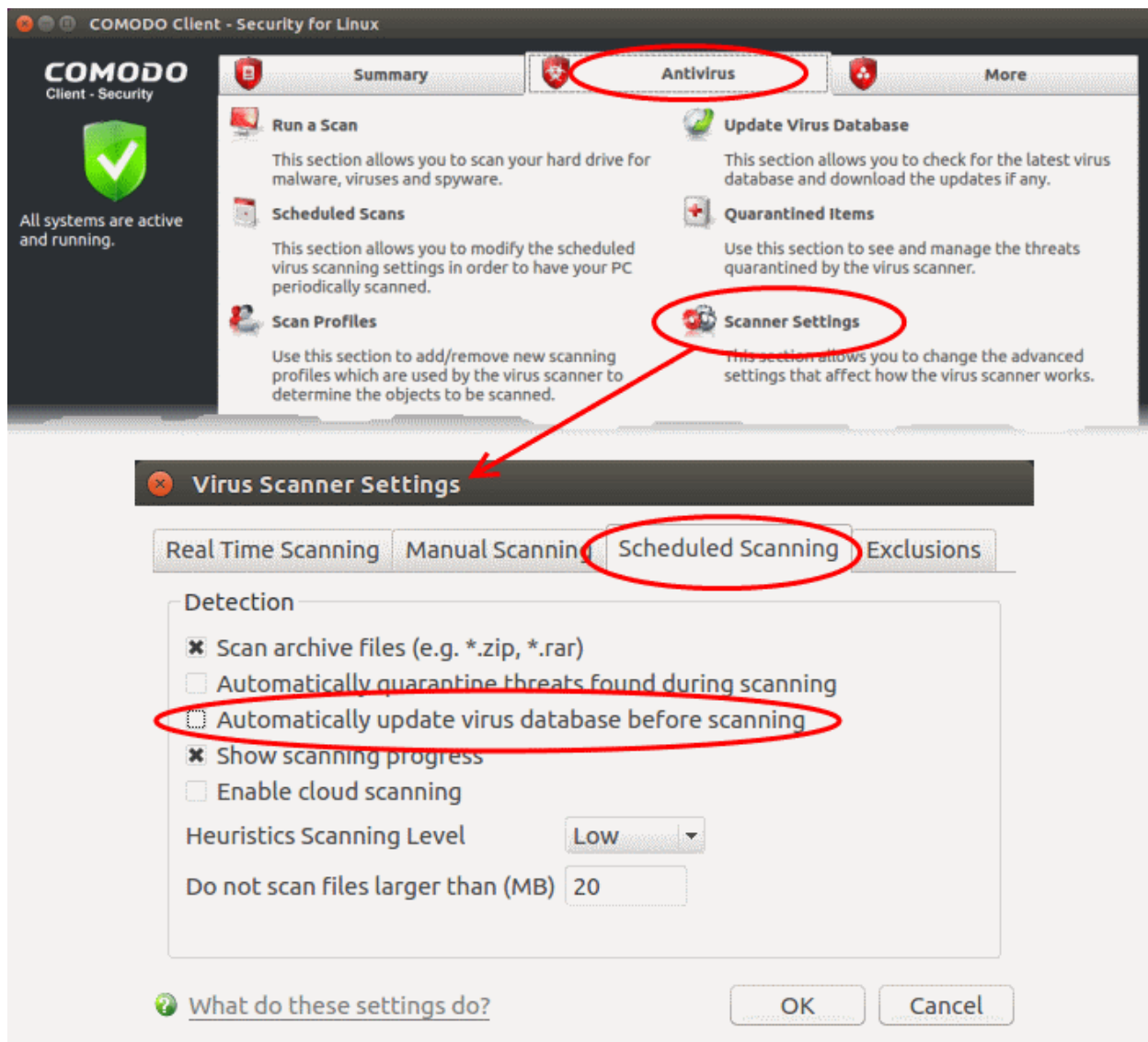
- Open Comodo Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Manual Scanning' tab
- Deselect 'Automatically update the virus database before scanning':



- Click 'OK'
- This action means CCS will not check for updates prior to running a manual scan.

Switch off updates prior to scheduled scans

- Open Comodo Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click 'the Scheduled Scanning' tab
- Deselect 'Automatically update the virus database before scanning':



- Click 'OK'.

CCS will no longer automatically check for download database updates prior to running a scan.

Control External Device Accessibility

- Click 'More' > 'Preferences' > 'Device Control'
- The device control panel lets you block access to external devices such as USB sticks and external drives.
- You can also define exclusions for selected devices. The selected devices will be allowed to connect, but all others will be blocked.

Configure device control

- Open Comodo Client Security
- Click 'More' > 'Preferences' > 'Device Control':



- **Enable Device Control** - Prohibits access to external storage devices like USB sticks and external drives. You can define exclusions to allow certain devices to connect. (**Default = Disabled**)
- **Log detected devices** - All device connection / disconnection events, whether allowed or blocked, are added to CCS logs. You can view the logs in the 'Log Viewer' module. (**Default = Enabled**)
 - Click 'More' > 'View Antivirus Events' > 'More' > 'Device Control Events'
 - See **Device Control Logs** for more details.
- **Exclusions** - Add exceptions to device control. Excluded devices are to connect to your computer even if 'Device Control' is active. For example, if your company uses USB tokens to authenticate remote VPN connections, you should create exceptions for those tokens.
 - **Click here** for more help on adding devices to exclusions list.

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](https://www.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