

COMODO
Creating Trust Online®



Comodo Antivirus

Software Version 2.2

User Guide

Guide Version 2.2.120318

Comodo Security Solutions Inc.
1255 Broad Street
Clifton, NJ 07013

Table of Contents

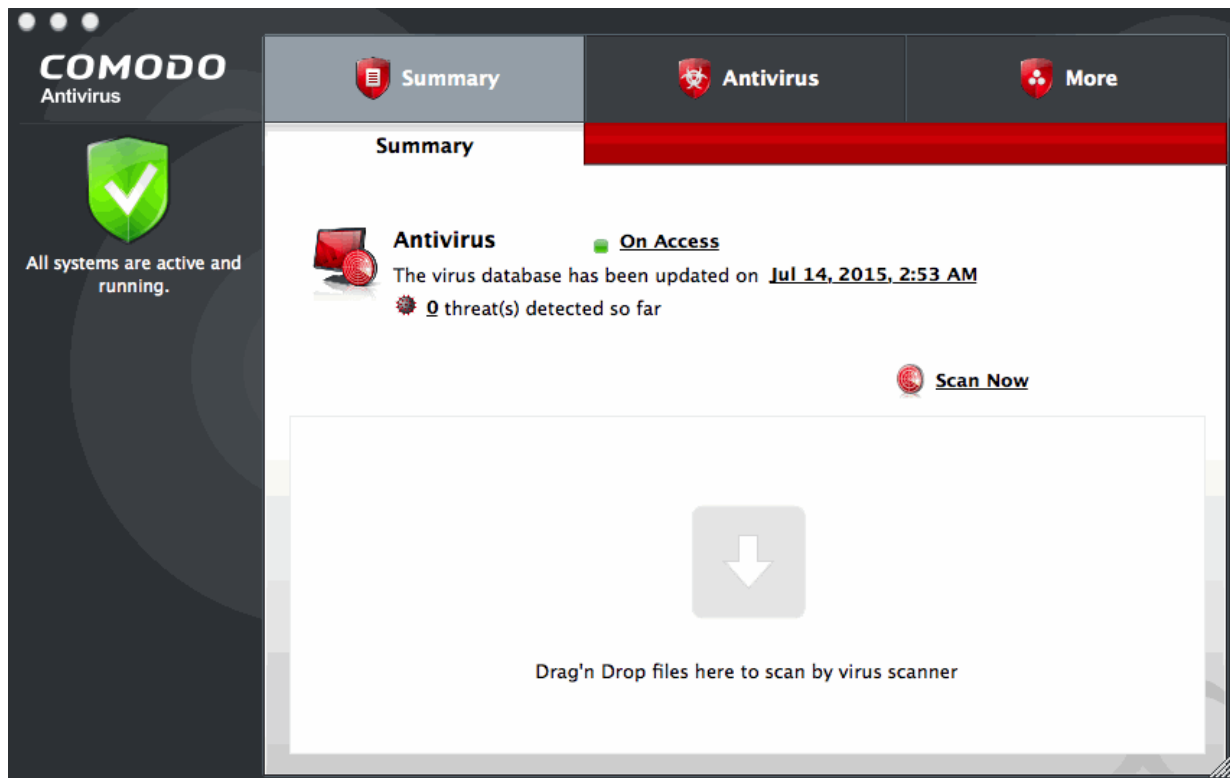
1.Introduction to Comodo Antivirus.....	4
1.1.System Requirements.....	5
1.2.Comodo Antivirus for MAC - Installation.....	6
1.3.Starting Comodo Antivirus.....	10
1.4.Comodo Antivirus - The Summary Screen.....	12
1.5.View Antivirus Events.....	13
1.6.Comodo Antivirus - Navigation	14
1.7.Understanding Alerts.....	14
1.8.Comodo Antivirus - How To... Tutorials.....	17
1.8.1.How to Scan your Computer for Viruses.....	18
1.8.2.How to Configure Database Updates.....	21
1.8.3.How to Quickly Set up Security Levels.....	23
1.8.4.How to Change Language Settings	24
1.8.5.How to Password Protect Your CAV Settings.....	25
1.8.6.How to Run an Instant Antivirus Scan on Selected Items	26
1.8.7.How to Create a Scheduled Scan.....	28
1.8.8.How to Restore Incorrectly Quarantined Items.....	29
1.8.9.How to Submit Quarantined Items to Comodo for Analysis.....	30
1.8.10.How to Switch off Automatic Software and Antivirus Updates.....	32
1.8.11.How to Temporarily Suppress Alerts while Playing a Game.....	37
1.8.12.How to View Antivirus Events.....	38
2. Antivirus Tasks - Introduction.....	38
2.1.Run a Scan.....	39
2.2.Update Virus Database.....	48
2.3.Quarantined Items.....	49
2.4.Scanner Settings.....	51
2.4.1.Real Time Scanning	52
2.4.2.Manual Scanning.....	53
2.4.3.Scheduled Scanning	54
2.4.4.Exclusions.....	55
2.5.Submit Files to Comodo for Analysis.....	56
2.6.Scheduled Scans.....	58
2.7.Scan Profiles.....	61
3.More Options-Introduction.....	65
3.1.Preferences.....	66
3.1.1.General Settings.....	67
3.1.2.Language.....	68
3.1.3.Parental Control Settings.....	68
3.1.4.Log Settings.....	69
3.1.5.Update Settings.....	72
3.2.Manage My Configurations.....	72
3.2.1.Comodo Preset Configurations.....	73
3.2.2.Importing/Exporting And Managing Personal Configurations.....	73
3.3.Diagnostics.....	78

3.4. Check for Updates.....	79
3.5. Browse Support Forums.....	82
3.6. Help	83
3.7. About.....	84
3.8. View Logs.....	85
3.8.1. Antivirus Logs.....	88
3.8.1.1. Filter Antivirus Logs.....	89
3.8.2. 'Alerts Displayed' Logs.....	92
3.8.2.1. Filter 'Alerts Displayed' Logs.....	93
3.8.3. Tasks Launched.....	100
3.8.3.1. Filter 'Tasks Launched' Logs.....	101
3.8.4. Configuration Changes.....	105
3.8.4.1. Filter 'Configuration Changes' Logs.....	106
About Comodo Security Solutions.....	111

1. Introduction to Comodo Antivirus

Comodo Antivirus (CAV) offers complete protection against viruses, worms and Trojan horses for MAC OS X based computers. The software is easy to configure and use and features real-time, on-access and on-demand virus scanning, full event logging, cloud based behavior analysis of unknown files and more. Users can start virus scans immediately by clicking the 'Scan Now' link on the summary screen. Individual files can be checked for viruses at any time by dragging them into the scan box in the 'Summary' area or, if the interface is not open, by dragging them onto the Comodo dock icon.

- Detects, blocks and eliminates viruses from desktops and networks
- Constantly protects with Real-Time and On-Access scanning
- Built in 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
- Simple to use: install and forget while Comodo Antivirus protects you in the background



Guide Structure

This introduction is intended to provide an overview of Comodo Antivirus. Please use the links below to jump to the section that you need help with.

- [Introduction to Comodo Antivirus](#)
 - [System Requirements](#)
 - [Installation](#)
 - [Starting Comodo Antivirus](#)
 - [The summary screen](#)
 - [View Antivirus Events](#)
 - [Navigation](#)
 - [Understanding Alerts](#)

- **How To... Tutorials**
- **Antivirus Tasks - Introduction**
 - **Run a Scan**
 - **Update Virus Database**
 - **Quarantined Items**
 - **Scanner Settings**
 - **Real Time Scanning**
 - **Manual Scanning**
 - **Scheduled Scanning**
 - **Exclusions**
 - **Submit Files to Comodo for Analysis**
 - **Scheduled Scans**
 - **Scan Profiles**
- **More... Options**
 - **Preferences**
 - **General Settings**
 - **Language Settings**
 - **Parental Control Settings**
 - **Log Settings**
 - **Update Settings**
 - **Manage My Configuration**
 - **Diagnostics**
 - **Check For Updates**
 - **Browse Support Forums**
 - **Help**
 - **About**
 - **View Logs**

1.1. System Requirements

To ensure optimal performance of Comodo Antivirus, please ensure that your computer complies with the minimum system requirements as stated below.

COMODO AV solution should be compatible with the following hardware platforms:

- Mac Intel x86_64

Operating systems:

- Mac OS X 10.9 x
- Mac OS X 10.10.x

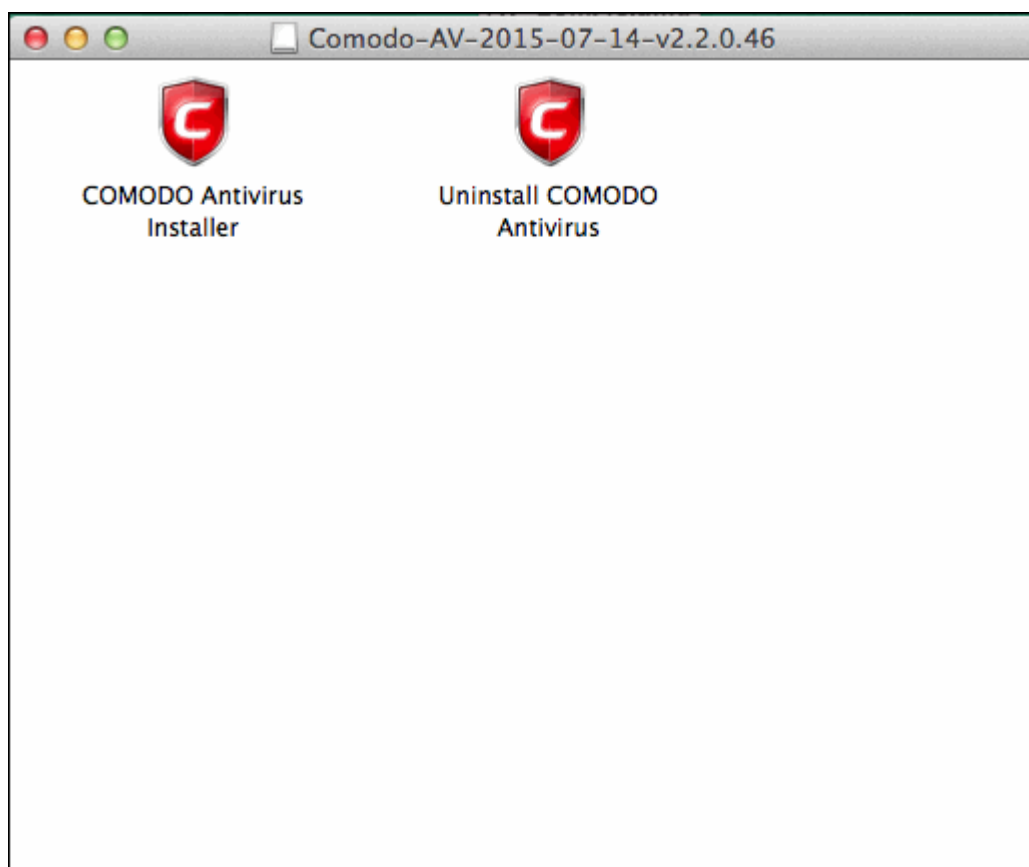
1.2. Comodo Antivirus for MAC - Installation

There are two ways to install Comodo Antivirus:

- **Installation wizard**
- **Console**

Installation wizard

- Download the setup file from <http://download.comodo.com/cis/download/installs/mac/CAVSetup.dmg.zip>.
- After downloading, double-click 'Comodo Antivirus Installer' to start the installation wizard:



STEP 1 - Choose the Interface Language

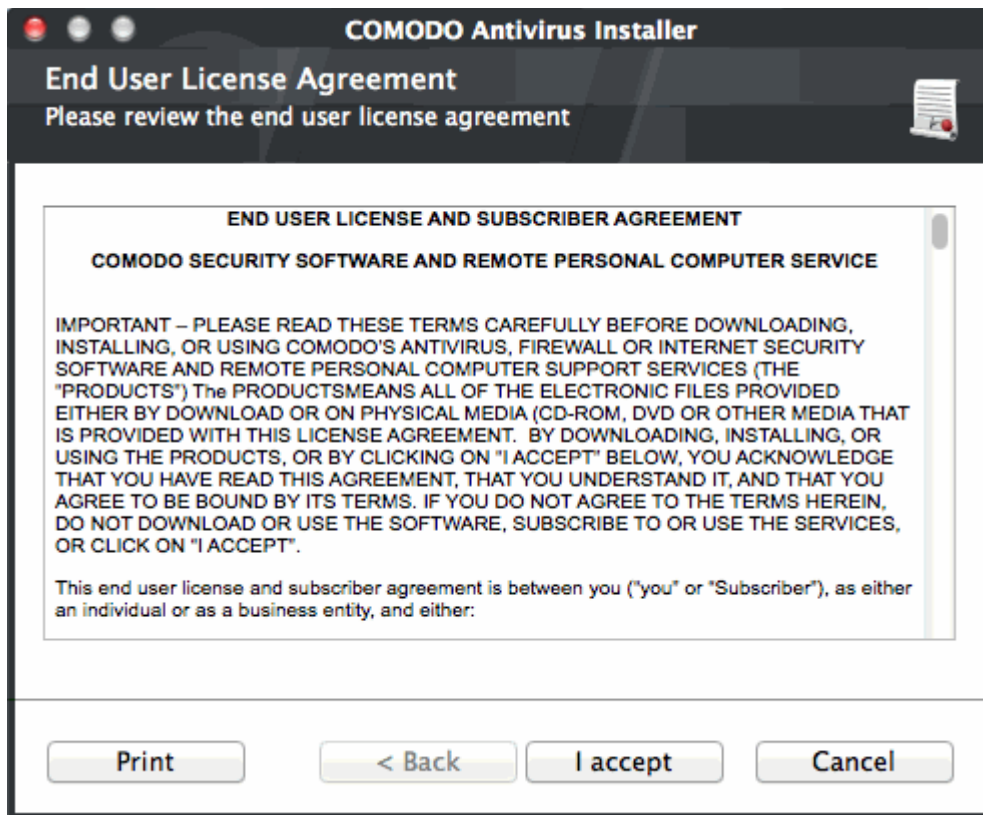
The installation wizard starts automatically.

- Select the language in which you want install Comodo Antivirus and click 'OK':



STEP 2 - End User License Agreement

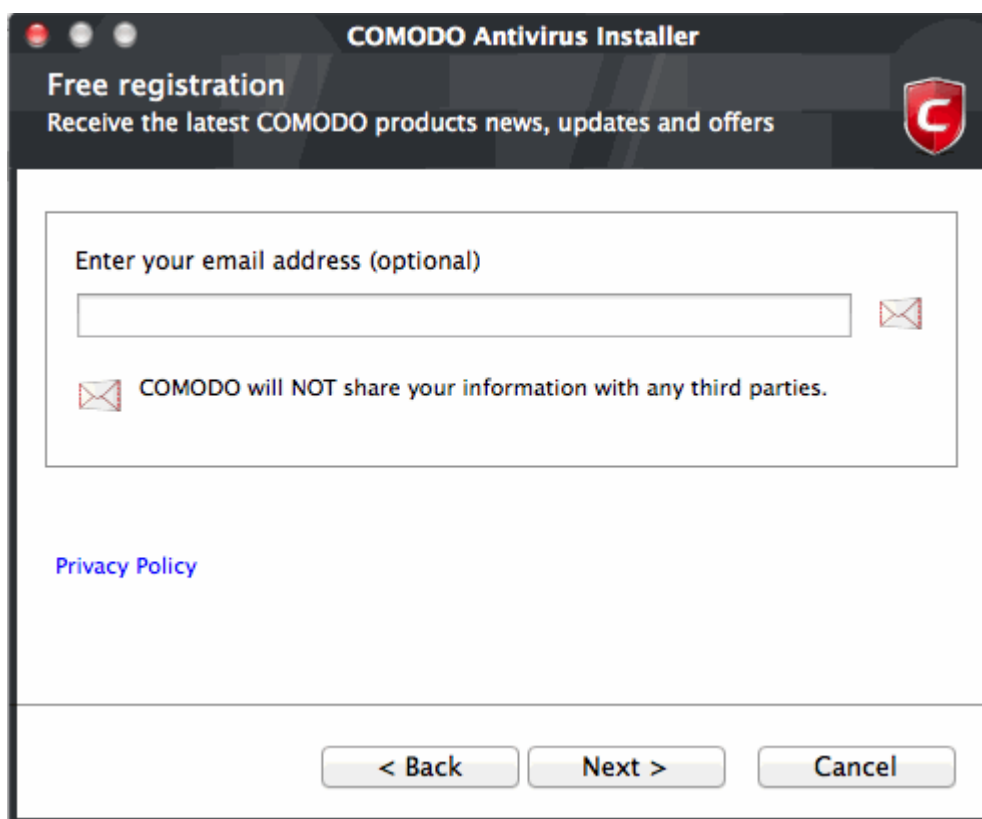
To continue with the installation, you must next read and accept the 'End User License Agreement' (EULA):



Click 'I accept' to continue the installation. If you want to cancel the installation at this stage, click 'Cancel'.

STEP 3 - Free Product Registration

Comodo Antivirus is activated free of charge for life. If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.



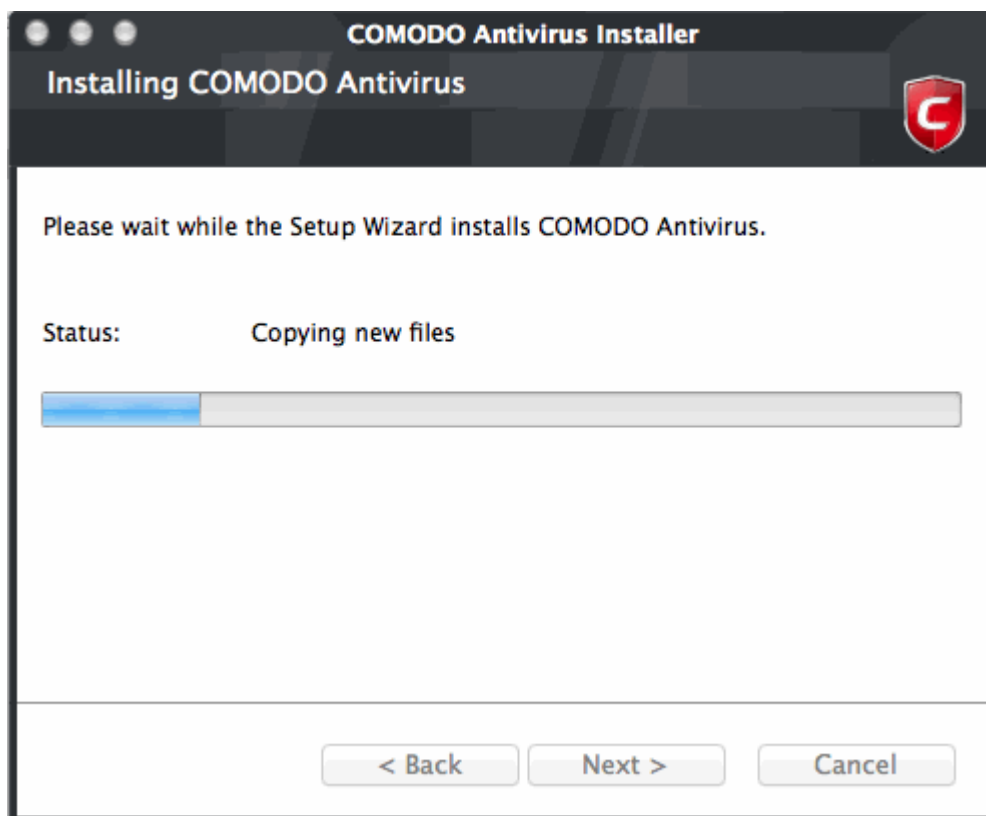
Click 'Next' to continue.

STEP 4 - Confirmation dialog

Please check all your settings are correct then click 'Install'. Click the 'Back' button to review and/or modify any of settings you have previously specified.

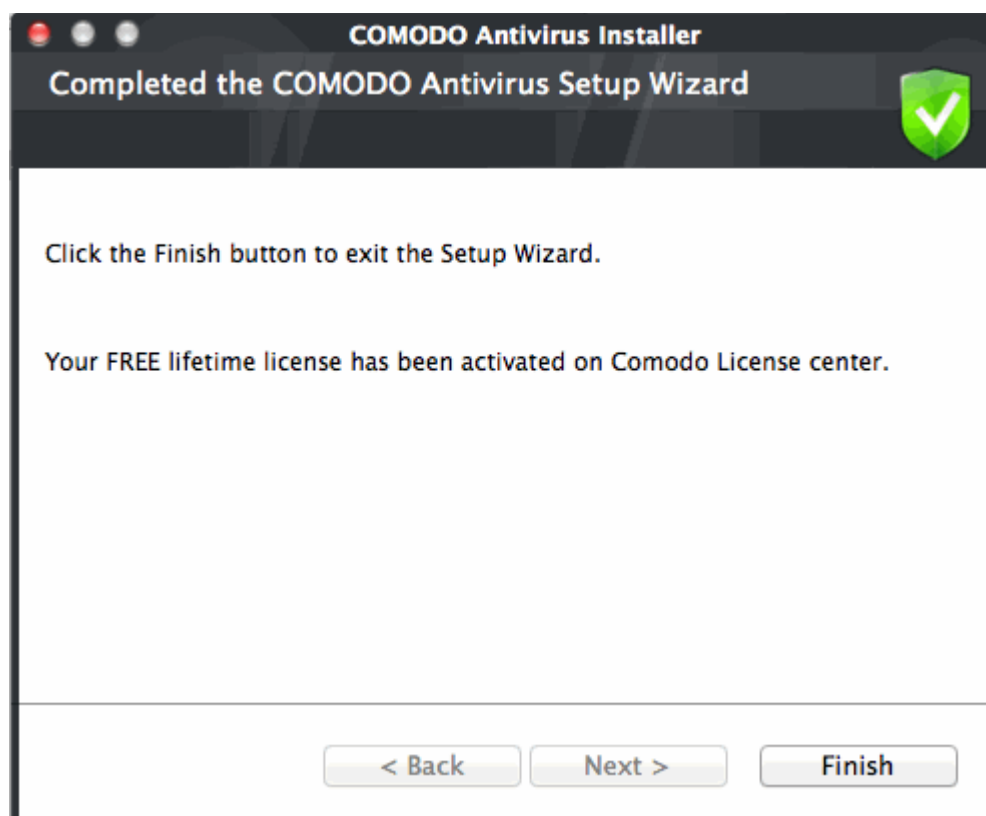


The setup status box will be displayed. You will see a progress bar indicating that files are being installed.

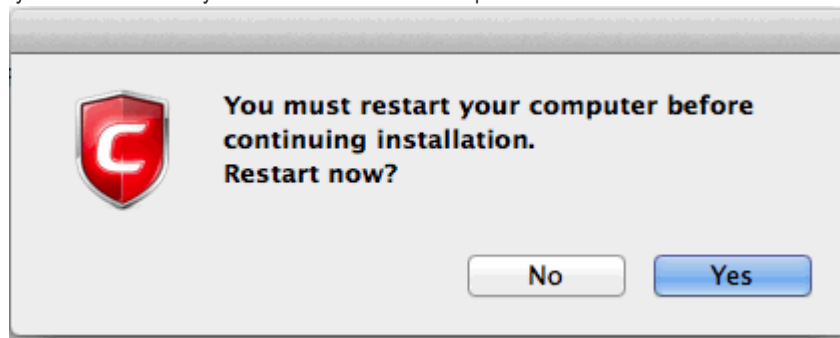


STEP 5 - Installation Complete

Click 'Finish' to finalize the installation:



- You must restart your computer to complete the installation.
- Make sure you have saved all your work then click 'Yes' to proceed:



To install AV for MAC using CESM console

Comodo Antivirus for MAC can be remotely deployed through the Comodo Endpoint Security Manager console. [Click here for more details on Importing Mac OS based Computers](#)

1.3. Starting Comodo Antivirus

After installation, Comodo Antivirus will be automatically loaded whenever you start your computer. Real-time protection and on-access scanning is automatically enabled so you are protected immediately after the restart. To configure the application and view settings, you need to access the management interface.

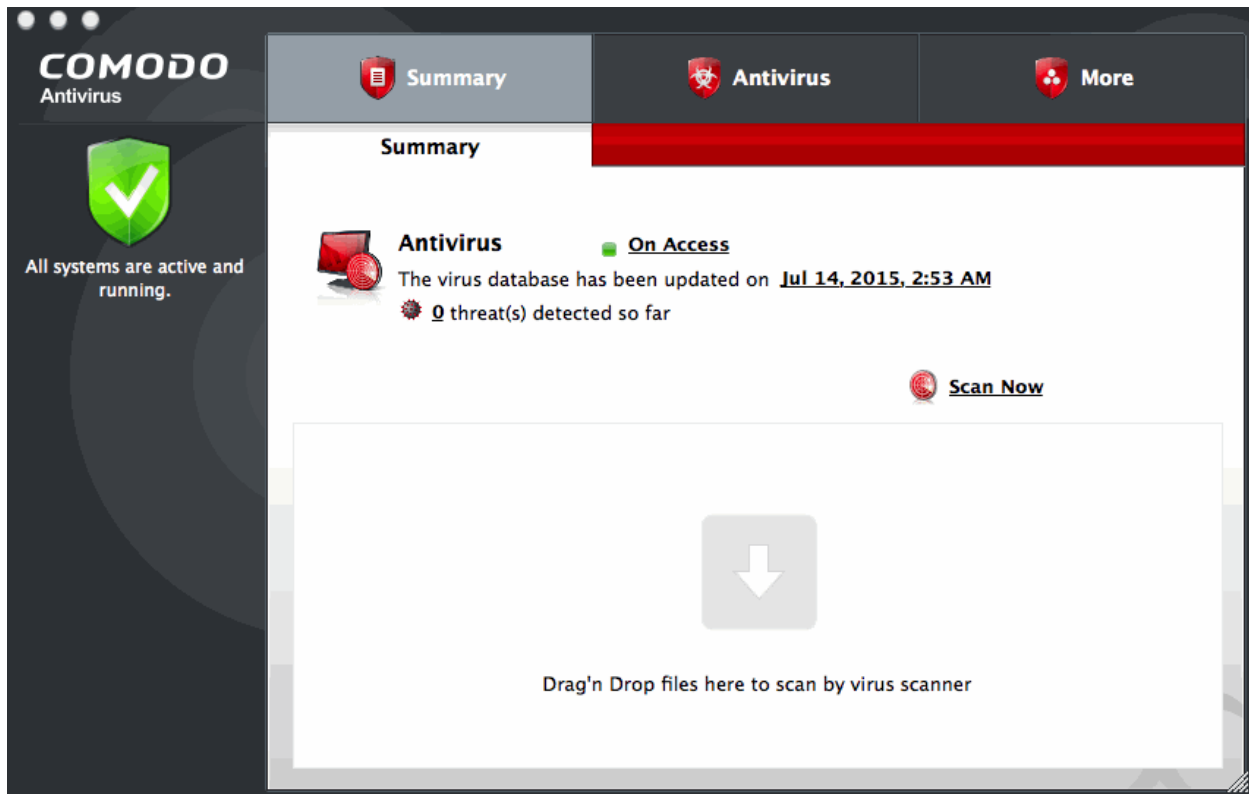
There are two main ways to do this - by [clicking the taskbar icon](#) or by [clicking the dock icon](#).

Open by clicking the taskbar icon

To open the interface, click the CAV taskbar icon as shown:



This will open Comodo Antivirus at the Summary screen. We recommend your first task should be to run a full scan on your computer. Click 'Do it now' under the yellow shield on the left to start a full scan. Alternatively, see ['The Summary Screen'](#) and ['Antivirus Tasks - Introduction'](#) if you wish to learn more about the application.



Open by clicking the dock icon

Comodo Antivirus will automatically add an application quick launch icon to the MAC OS dock. You can open the interface at any time by clicking the icon as shown:



Tip: You can run scans on any file or folder by simply dragging it onto the CAV dock icon. If, for whatever reason, this icon is removed or is not present and you wish to manually add it then please follow these steps:

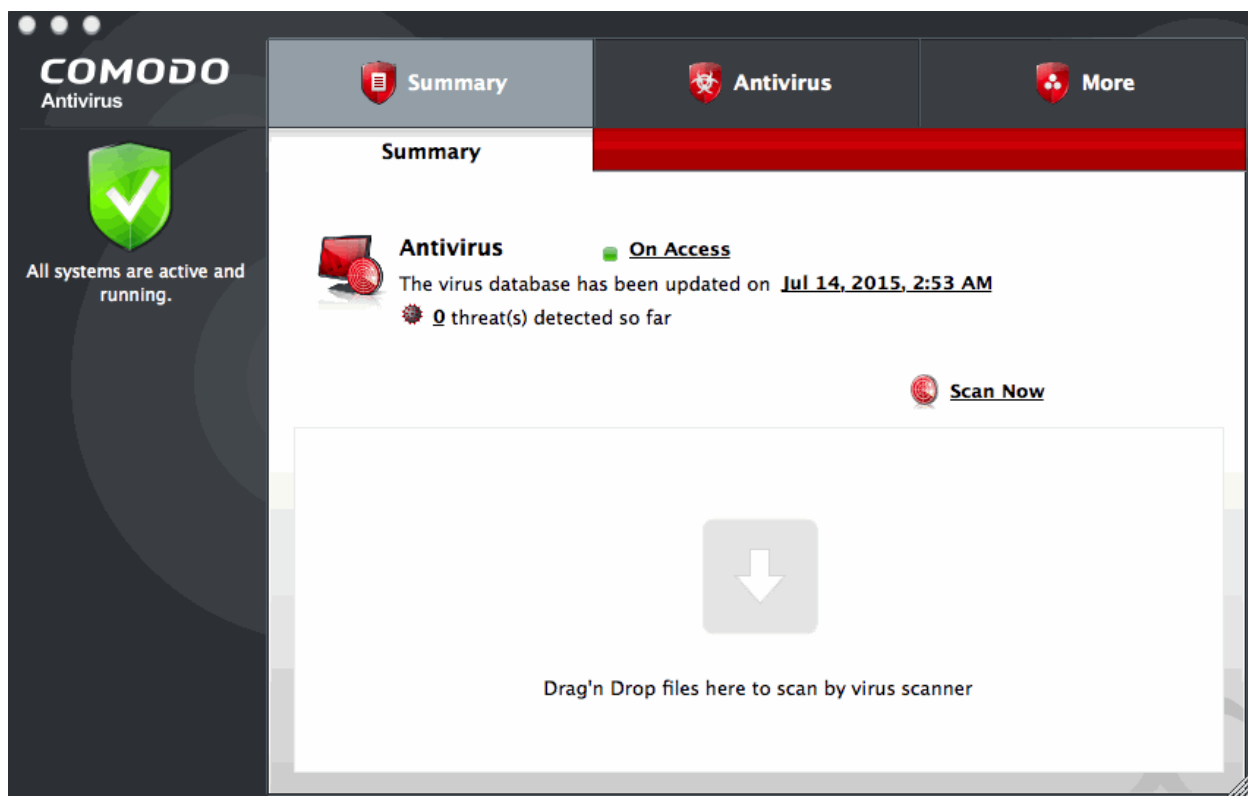
Double click 'Macintosh HD' on your desktop:



- Click 'Applications' then double-click the 'Comodo' folder
- Click and hold the 'Comodo Antivirus' icon and simply drag it down to the dock.
- From now onwards, you will be able to open the application by clicking the dock icon.

1.4. Comodo Antivirus - The Summary Screen

The 'Summary' screen is shown by default when you open the application. It provides an at-a-glance summary of protection and update status as well as allowing you to quickly run a virus scan with a single click. You can access this area at any time by selecting the 'Summary' tab as shown in [General Navigation](#).



Individual files can be scanned for viruses by dragging them into the scan area.

The summary screen contains the following information:

1. System Status

The shield icon on the left of the interface is a high visibility indicator of your current protection level. In the example above, we see a yellow icon indicating that there are actions you need to take. In this case it is yellow because you need to run a full scan. Once you have done this (and providing 'Real Time Scanning is not disabled), the shield icon should turn green and display the message 'All systems are active and running'.

2. Antivirus

The Antivirus summary box contains:

i. The Status of Realtime Virus Scanning

The status of the virus scanning setting is displayed as a link (*on Access* in the example above). On clicking this link, the Virus Scanner Settings panel will open, allowing you to quickly set the level of Real Time Scanning, by moving the status slider. See **Scanner Settings**, for more details on Virus Scanner Settings.

ii. When the Virus Database was Last Updated

The day and time at which the virus database was last updated is displayed as a link. On clicking the link, the update of the virus database is started and the current date and time are displayed on completion of the process.

iii. Number of Detected Threats

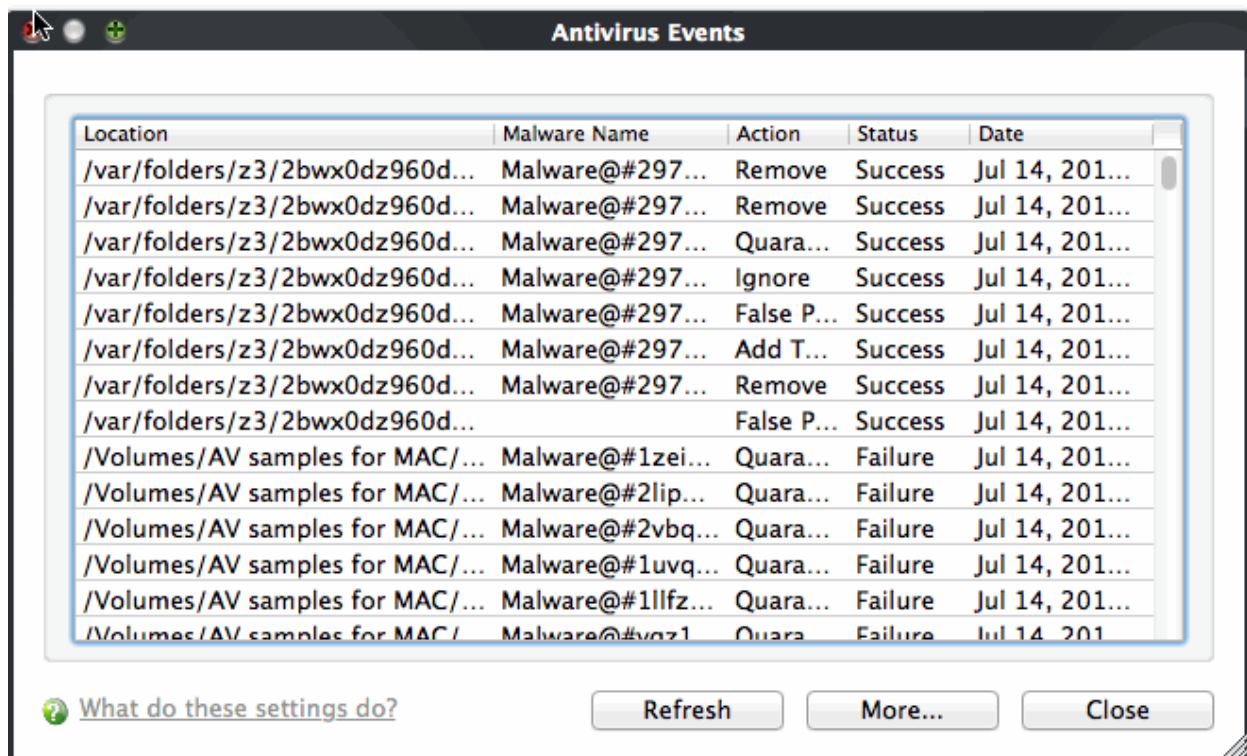
The number of threats detected so far from the start of the current session of Comodo Antivirus is displayed here as a link. On clicking the link, the Antivirus Events panel will open. See **Antivirus Events**, for more details on viewing Antivirus events

iv. Scan Now

The 'Scan Now' link in this box allows you to instantly **Run a Scan**.

1.5. View Antivirus Events

- The 'Antivirus Events' viewer contains a log of actions taken by the virus scanner when it encountered a malicious file.
- The viewer will tell you the date and time a particular virus was detected, where it was located and the action that was taken by Comodo Antivirus in response.
- You can open the event viewer by clicking the number in front of 'Threat(s) detected so far' on the 'Summary' screen.



Column Descriptions

- **Location** - The location where the malicious file was detected
- **Malware Name** – The name of the malware
- **Action** - The action taken against the malware
- **Status** – Indicates whether or not the action was successful
- **Date** - Indicates the date of the event
- To refresh the events, click the 'Refresh' button.
- Click the 'More' button to open the Comodo Log Viewer. See [View Logs](#) for more details.
- To close the events, click the 'Close' button.

1.6. Comodo Antivirus - Navigation

The Comodo Antivirus interface is divided into three main functional areas - 'Summary', 'Antivirus' and 'More'. You can access any of these areas by clicking the icons along the top of the interface.



- **Summary** - Contains at-a-glance details of important settings, activity and other information.
- **Antivirus** - Opens the **Antivirus Tasks** configuration section. This area allows you to run scans, configure settings, schedules, updates, scan profiles and more.
- **More** - Opens the **More** options screen which contains options relating to the overall configuration of Comodo Antivirus.

Each of these areas contains several sub-sections that provide granular control over the configuration of the application.

1.7. Understanding Alerts

Antivirus alerts immediately inform you if a virus has been detected and provide options and information so you can make an informed decision on how to proceed. Alerts can also be used to instruct Comodo Antivirus on how it should behave in future when it encounters activities of the same type.



Answering an Antivirus Alert

Alerts are generated whenever a virus or malware tries to be copied to or run on your system. Alerts appear at the

bottom right hand side of your computer screen. The alert contains the name of the virus detected and the location of the virus on your disk and, if available, more information about the virus.

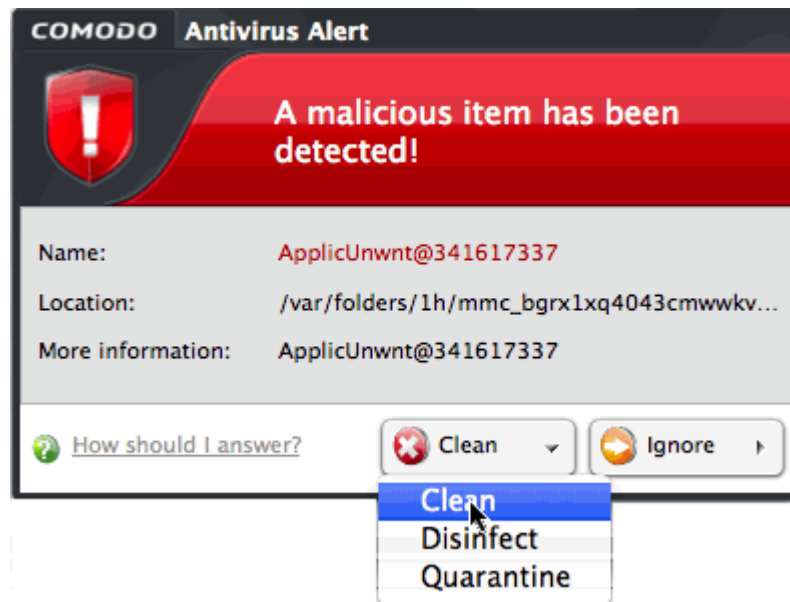
Each alert has two main options - 'Clean' and 'Ignore'. Selecting either of these will present further options.

- Clicking 'Clean' will allow you to:
 - Clean the file
 - Quarantine the file. This will move the file to **Quarantined Items**OR
 - Disinfect the file. If CAV has a disinfection routine available it will disinfect the file. If not, then the file will be deleted.
- Clicking 'Ignore' will present you with the following options:
 - Once - If you click 'Once', the file is ignored this time only. If the same file is detected at another time then another alert will be displayed.
 - Report this to COMODO as a False Alert - If you are sure that the file is safe, select 'Report this to Comodo as a False Alert'. This will submit the file to Comodo for analysis. If the file is found to be trustworthy, it will be added to the Comodo whitelist.
 - Add to Exclusions - If you click 'Add to Exclusions', the virus is added to your local **Exclusions** list. This means Comodo Antivirus will no longer report this file as malicious or raise an alert the next time the file is detected.

Ignore the alert only if you trust the application.

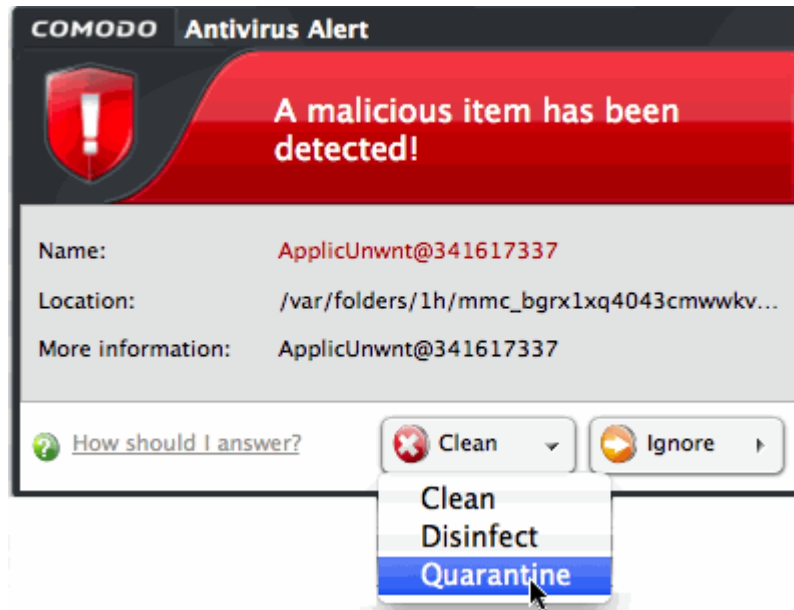
To clean the file or application form your system

- Click the drop-down arrow beside the 'Clean' button and select 'Clean' from the 'Clean' options.



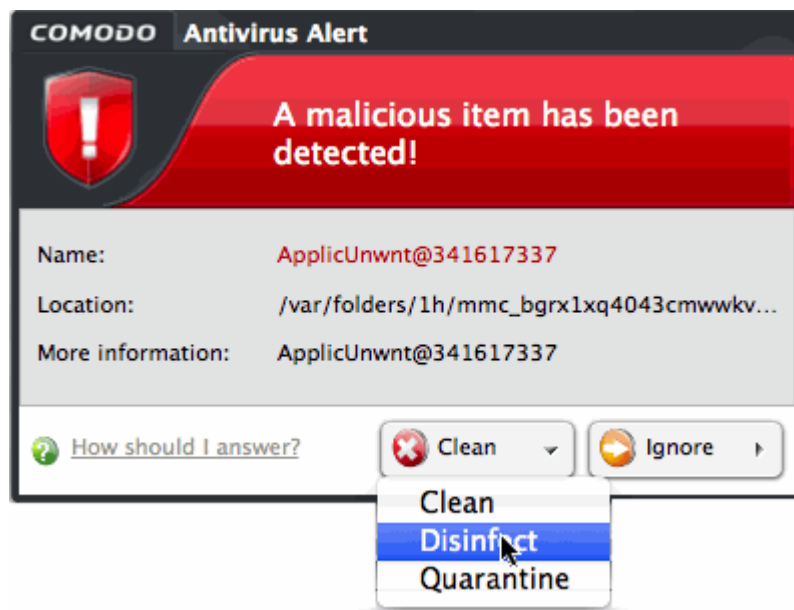
To move the file or application to Quarantine

- Click the drop-down arrow beside the 'Clean' button and select 'Quarantine' from the 'Clean' options.



To disinfect the file or application

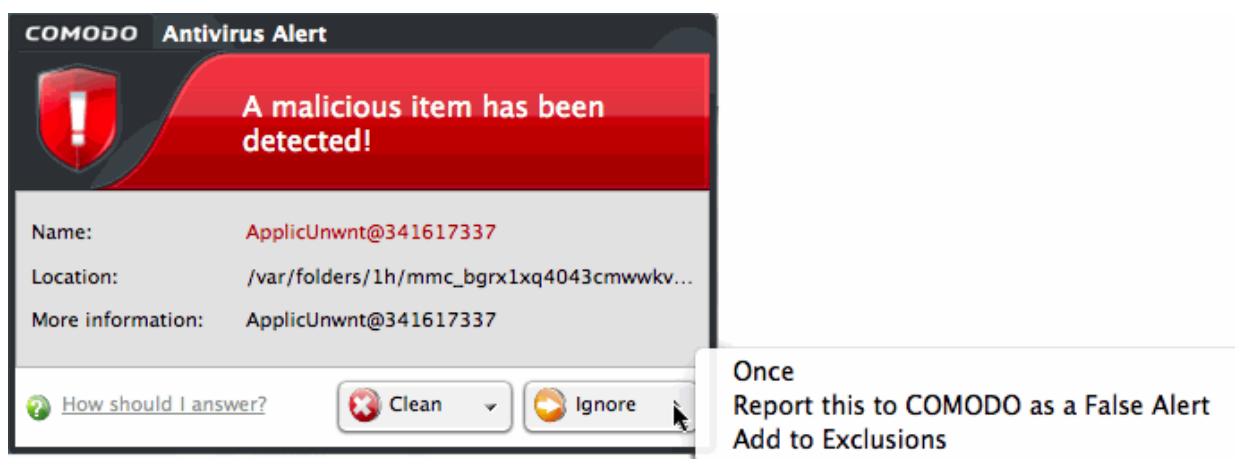
- Click the drop-down arrow beside the 'Clean' button and select 'Disinfect' from the 'Clean' options.



Comodo Antivirus will first attempt to disinfect the file in question. If this is not possible, then the file will be deleted.

To ignore the alert if you trust the file/application

- Click the 'Ignore'. Selecting 'Ignore' provides you with three options:



- **Once.** If you click 'Once', the file is ignored this time only. If the same file is detected at a later date then another alert will be displayed.
- **Report this to COMODO as a False Alert.** If you are sure that the file is safe, select 'Report this to Comodo as a False Alert'. This will submit the file to Comodo for analysis. If the file is found to be trustworthy, it will be added to the Comodo white-list.
- **Add to Exclusions.** If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. This means Comodo Antivirus will no longer report this file as malicious or raise an alert the next time the file is detected.

1.8. Comodo Antivirus - How To... Tutorials

The 'How To...' section of the guide contains guidance on key tasks of Comodo Antivirus. Use the links below to go to each tutorial's page.

- **How to Scan your Computer for Viruses** - Explains how automatically or manually you scan your computer
- **How to Configure Database Updates** – Allows you to specify how virus signature updates should be handled
- **How to Quickly Setup Security Levels** - Guidance on changing the antivirus security level
- **How to Change Comodo Antivirus Language Settings** - Explains how to switch languages
- **How to Password Protect your CAV settings** - Explains how to prevent your antivirus settings from being changed by others
- **How to Run an instant Antivirus scan on Selected Items** - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware
- **How to Create a Scheduled Scan** – Specify a schedule to scan selected items at certain times
- **How to Restore Incorrectly Quarantined Item(s)** - Help to restore files and executables that were moved to quarantine by mistake
- **How to Submit Quarantined Items to Comodo for Analysis** - Advice on how to send suspicious files/executables to Comodo for analysis
- **How to Switch Off Automatic Software and Antivirus Updates** - Explains how to stop automatic software and virus updates
- **How to Temporarily Suppress Alerts when Playing a Game** - Helps you to switch off pop-up alerts to avoid interruptions while playing games
- **How to View Antivirus Reports** – Help to view all scan events

1.8.1. How to Scan your Computer for Viruses

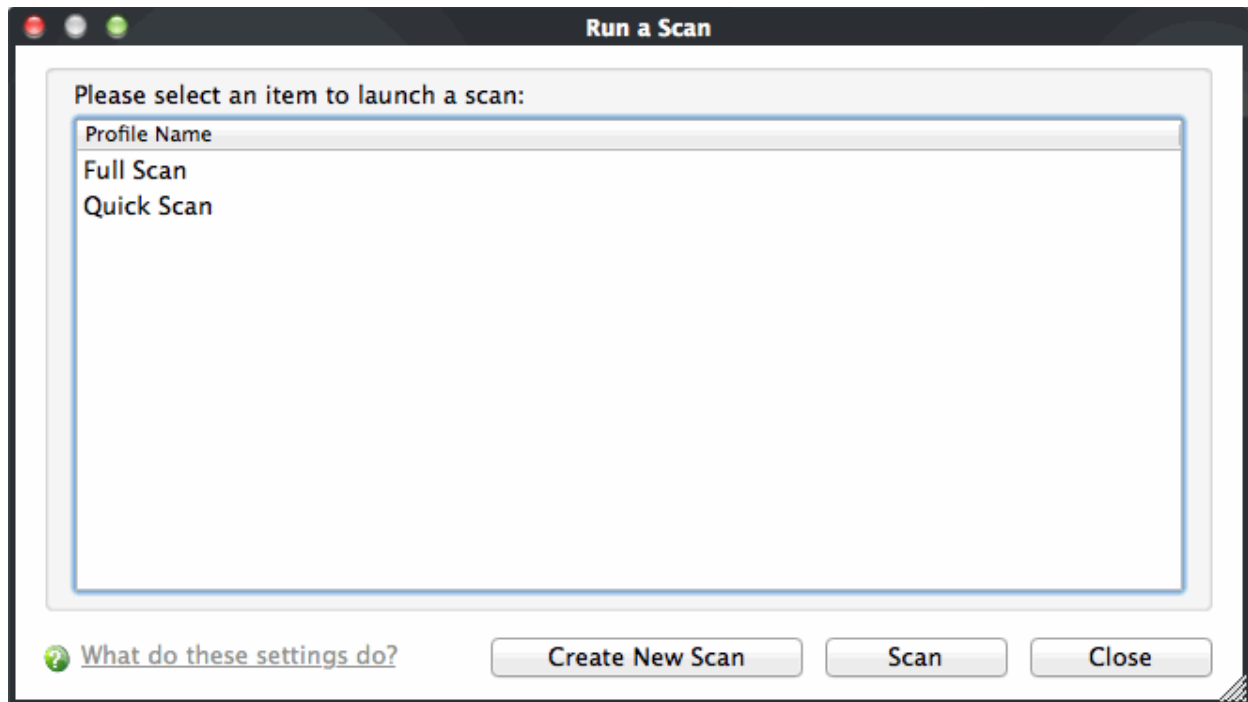
Comodo Antivirus lets you quickly run an on-demand scan on any file or area on your computer.

- **Start a manual scan of your whole computer or specific locations**
- **Run a quick scan on a particular item**

Start a manual scan of your computer or specific location

- Click 'Scan Now' on the CAV home screen
 - Or click the 'Antivirus' tab followed by 'Run a Scan'

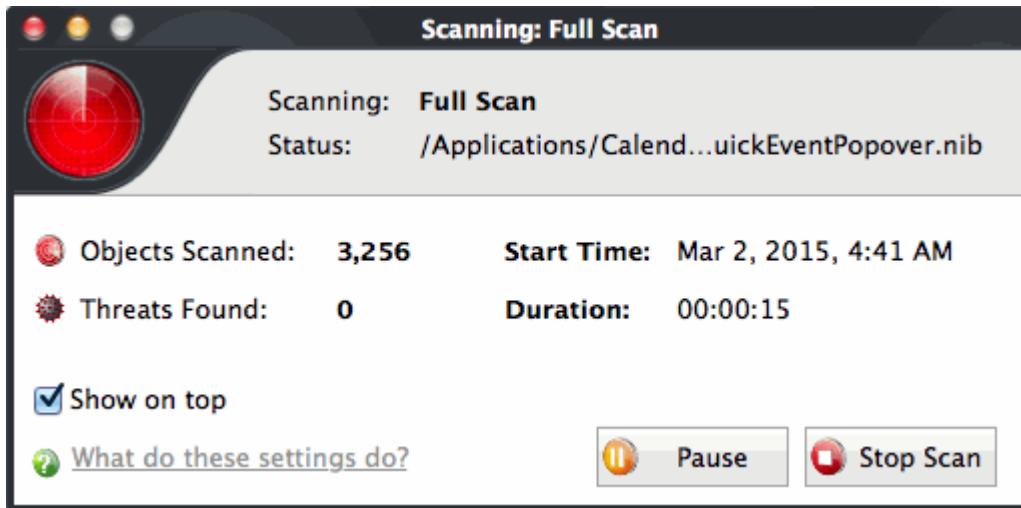
Either method will open the 'Run a Scan' dialog:



- You have two broad options:
 - Run a predefined scan profile:
 - 'Full Scan' - Scans your entire computer
 - 'Quick scan' - A faster, targeted scan of important files and folders.
 - OR
 - Create a custom scan:
 - Choose specific files, folders or drives to scan. See **custom scan** if you need more help with this option.

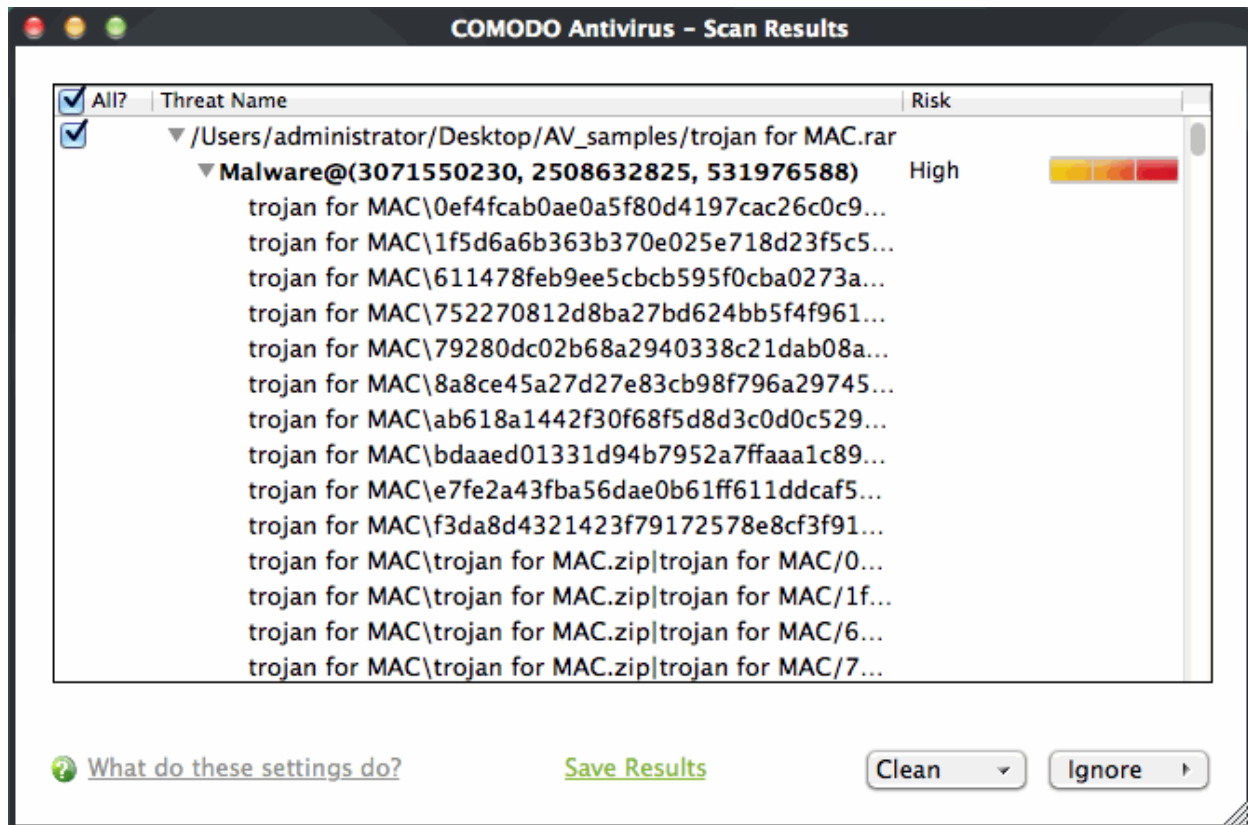
After clicking the scan button, Comodo Antivirus will first check for database updates. If they are available, they will be downloaded and installed before the scan runs.

Scanning will commence immediately after any updates are applied.



The progress dialog shows the following items: profile name, the scanned location, the start time and duration of the scan, the total number of objects scanned and the number of threats found.

The scan results lists all threats found and their corresponding risk levels:



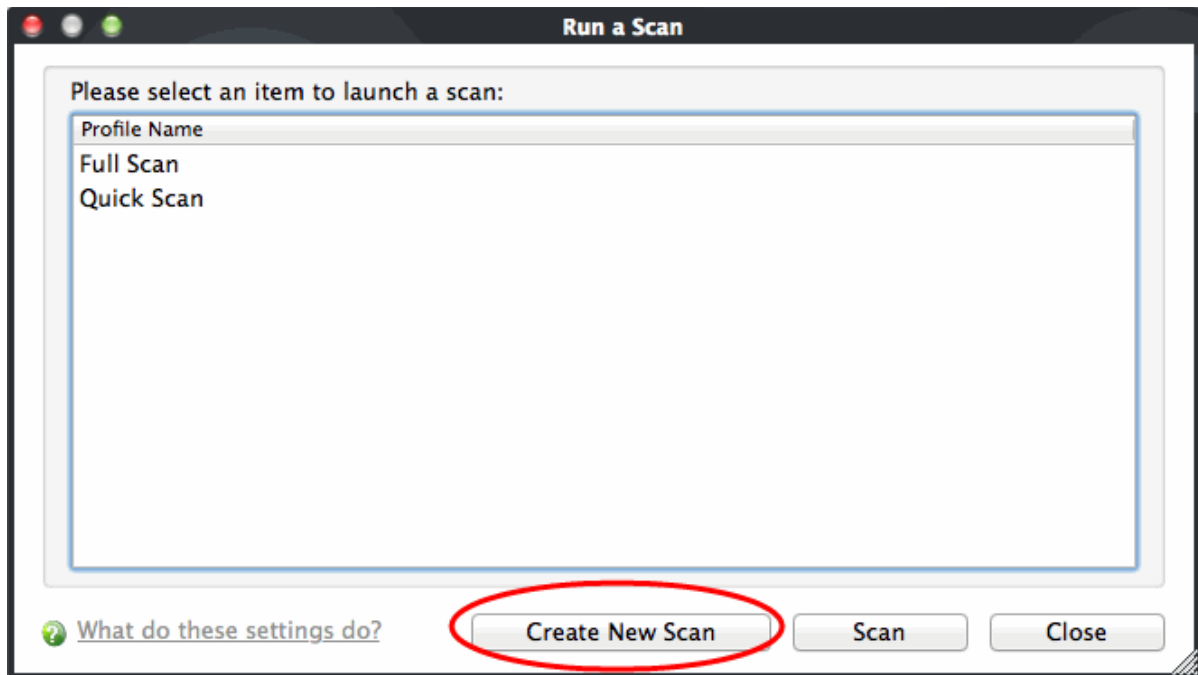
- Clean - Selected items will be deleted, disinfected, or moved to **Quarantine**
- Ignore - You can ignore files once, report the files to Comodo as a false positive, or create an exclusion for the file.
 - Use the check-boxes next to the threat name to select individual files.
 - If the 'All?' check-box is ticked then your choice of 'Clean' or 'Ignore' will apply to every threat found.
- Save Results – Export the results to file.

See **Antivirus Tasks > Quarantined Items**, for more details on quarantined applications.

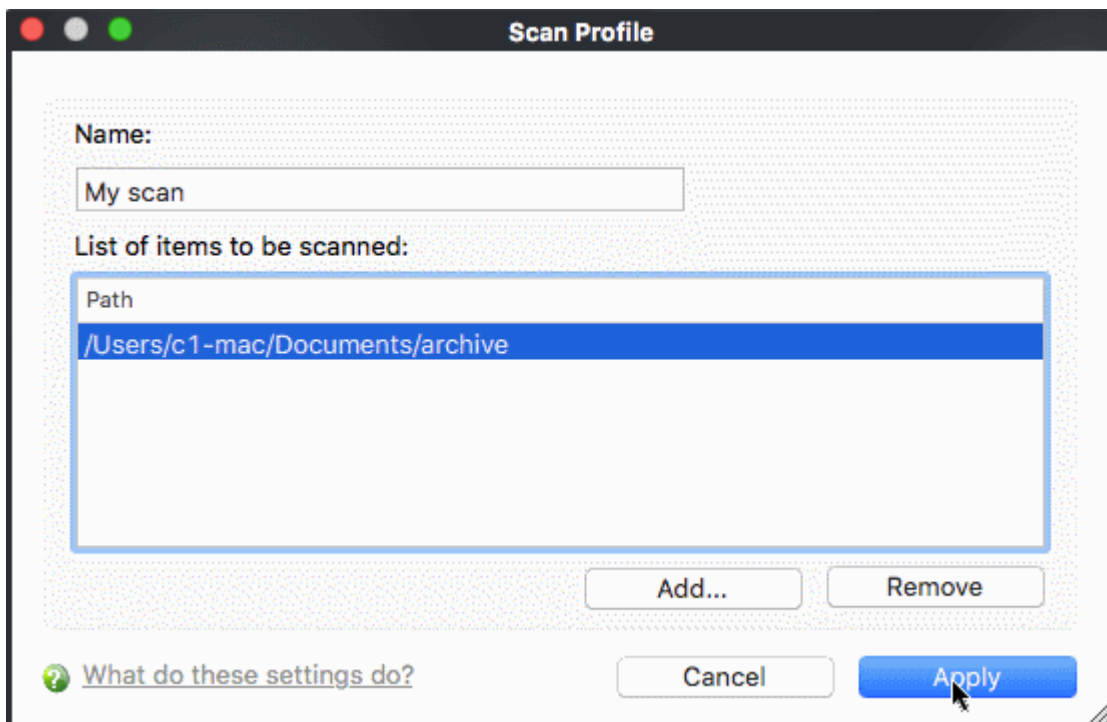
See **Ignore an application/file**, for more details on ignore options.

To create a new scan profile

- Click 'Create New Scan' in the 'Run a Scan' interface.

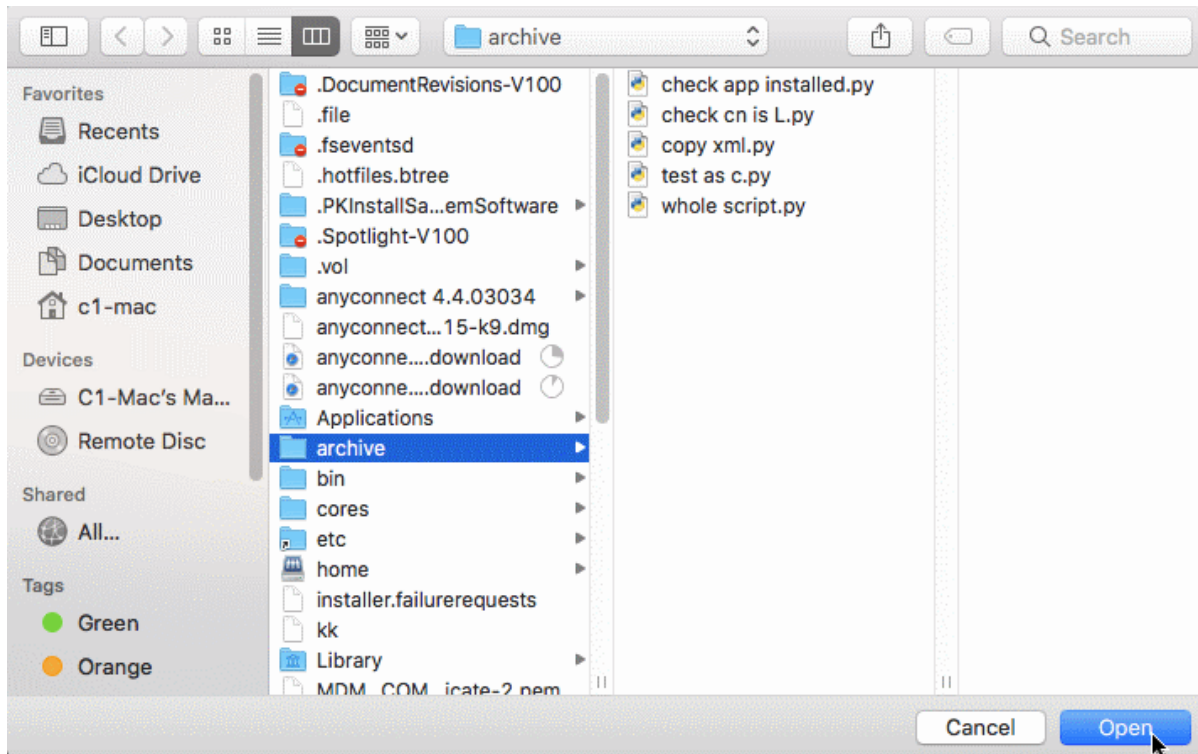


- Type a name for the scan profile to be created in the 'Name' box.
- Click 'Add'.
- Select the locations to be scanned when the newly created scan profile is selected.



Specify the path of the destination file or folder by selecting the locations to be scanned as part of the profile.

- Select the files or folders and click 'Open'.

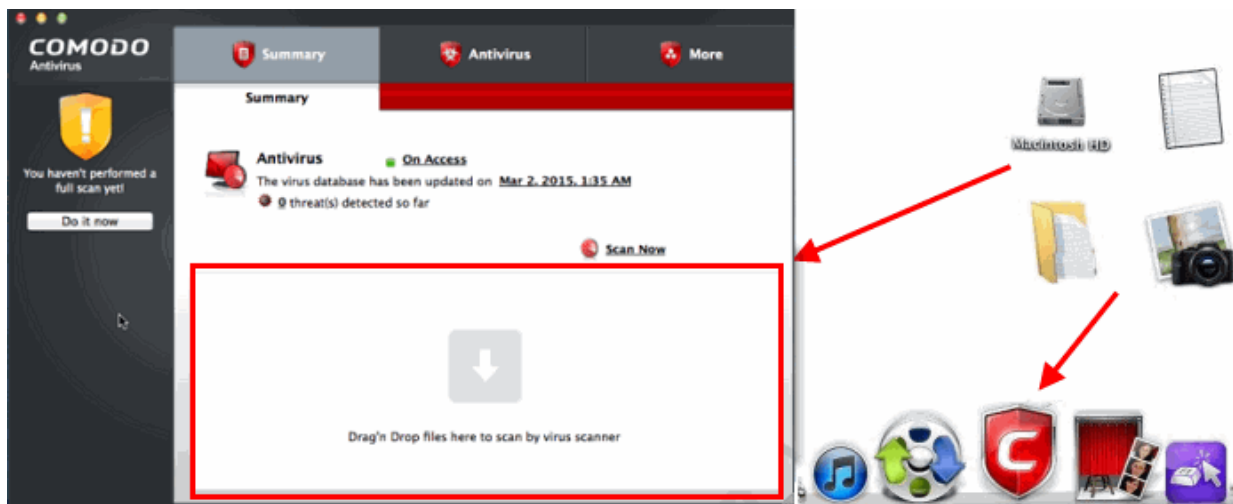


- Repeat the process to create more Scan Profiles.
- Click 'Apply' in the 'Scan Profiles' interface for the created profiles to take effect.

See [Creating a Scan profile](#), for more details on scan create.

To run an instant scan on a particular item

You can instantly virus scan virtually any file, folder, photo, application or hard-drive by simply dragging the item into the scan box on the summary screen or onto the Comodo icon on the dock.



Please see [Starting Comodo Antivirus](#) for more details. See also [how to create a Scan Schedule](#).

1.8.2. How to Configure Database Updates

It is essential that you have the latest virus database installed to guarantee protection against the most recent viruses.

For this reason, it is the default policy of CAV to

- (1) Periodically check for and download database updates
- (2) Check and update the database just before a scan

Updates can also be downloaded manually. Pre-scan updates can be disabled on a per-scanner basis.

- **To manually update the virus database**
- **To configure automatic database updates**
- **To configure pre-scan database updates**

To manually update the virus database

- Click the 'Antivirus' tab
- Click 'Update Virus Database'
- CAV will contact Comodo servers and install any available updates.



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

To configure automatic database updates

To switch automatic updates ON/OFF in absolute sense:

- Click the 'Antivirus' button along the top navigation
- Click 'Scanner Settings'
- Make sure the interface is open at the 'Real Time Scanning' area
- Enable or Disable 'Automatically update virus database'

To configure pre-scan virus database updates

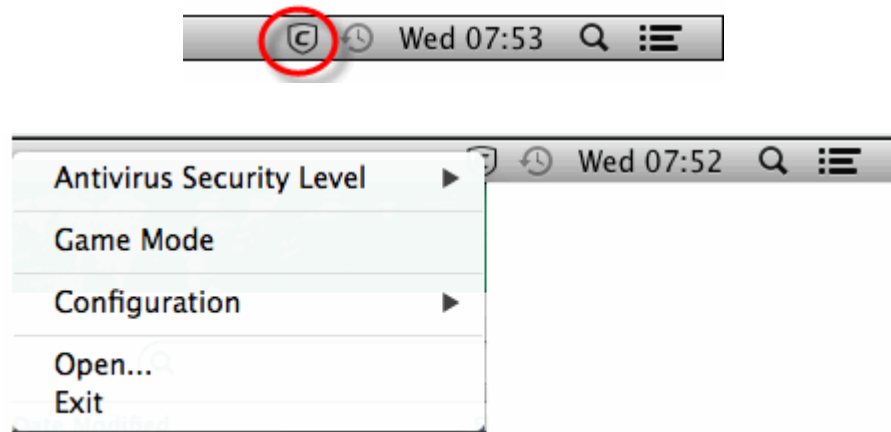
Pre-scan update checks can be switched ON/OFF on a 'per-scanner' basis for 'On Access' and 'Scheduled' scan types. To do this:

- Click the 'Antivirus' tab
- Click 'Scanner Settings'
- Select either the 'On Access Scan' or 'Scheduled Scan' button as required
- Enable or disable 'Automatically update virus database' as required

More details on these settings can be found in the '[Scanner Settings](#)' section of this guide.

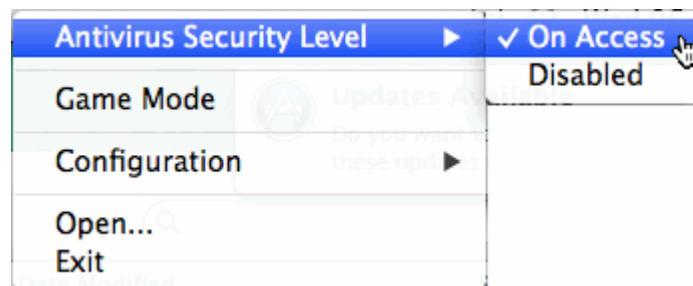
1.8.3. How to Quickly Set up Security Levels

You can change security levels by right-clicking on the system tray icon:



To set the Real time Scanning level

- Right-click on the system tray icon
- Move your mouse over 'Antivirus Security Level':

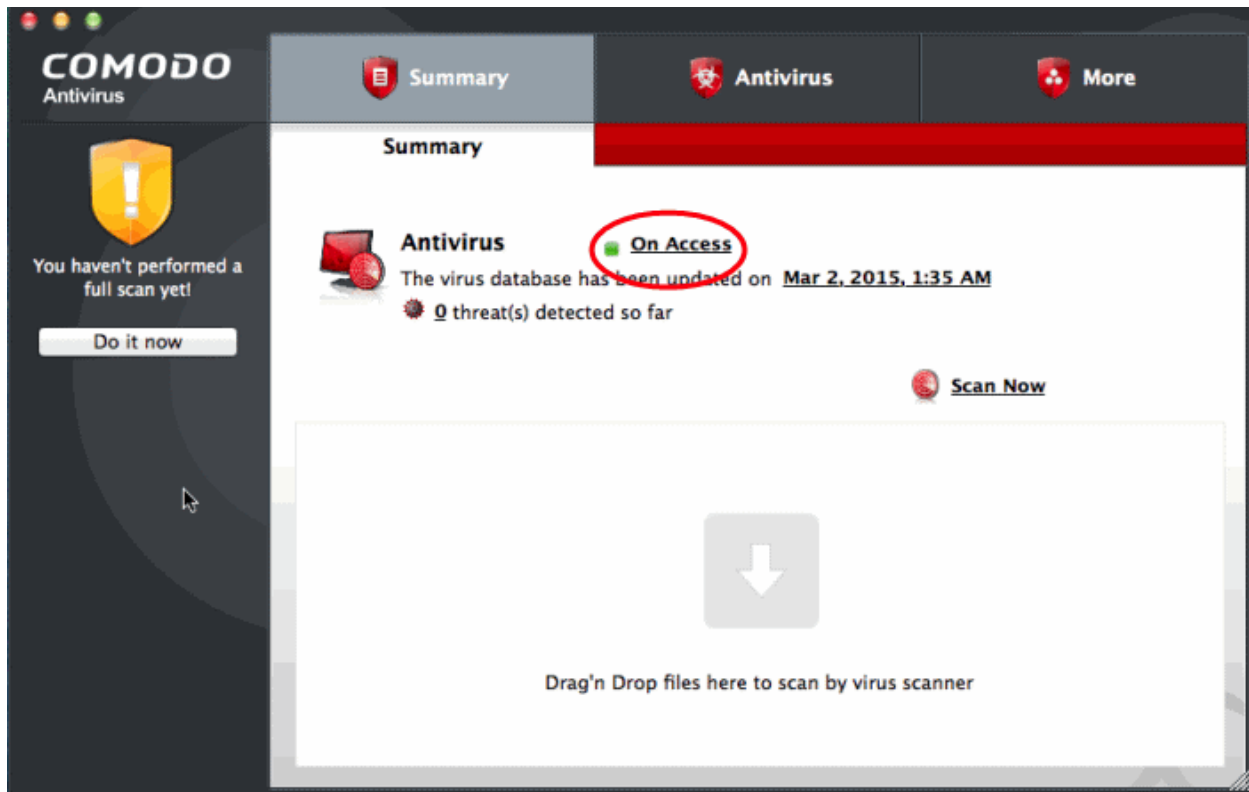


The available security levels are:

- On Access - Files are scanned whenever you, or another program, attempts to open them. Recommended.
- Disabled - Not recommended. Files are not scanned when they are opened. This strongly raises the possibility that your system will get infected.

The currently active configuration has a check-mark next to it. See [Scanner Settings > Real Time Scanning](#) for more details on these settings.

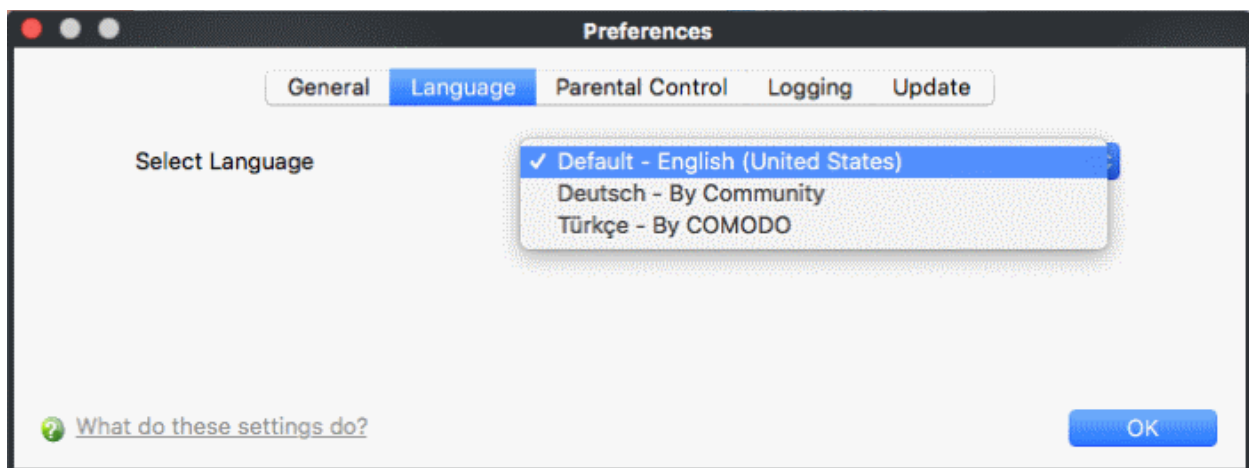
- You can also access these settings through the [CAV summary screen](#).
- In the example below, the security level is 'On Access'.
- Click the word to access the settings described on this page:



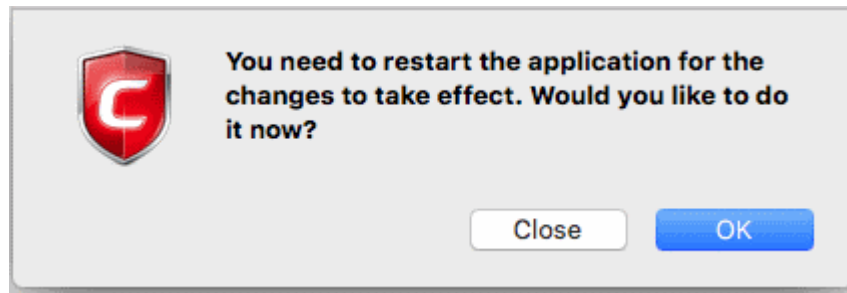
1.8.4. How to Change Language Settings

To view or modify the language used in the Comodo Antivirus interface:

- Click 'More' on the top navigation
- Click 'Preferences' > 'Language'
- Choose your preferred language from those available in the drop-down. The current language has a check-mark next to it:



- If you change the language, click 'OK' to save your preference then restart the application to apply the changes:



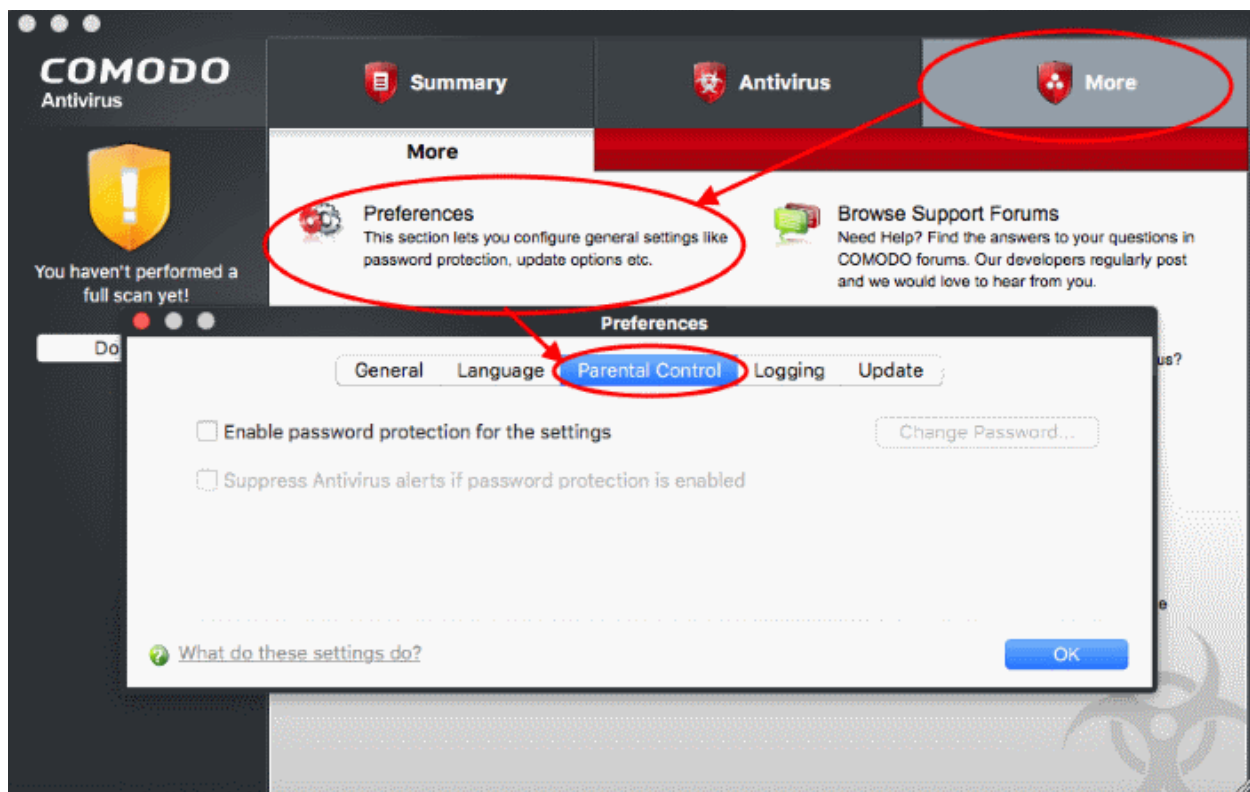
1.8.5. How to Password Protect Your CAV Settings

This page explains how to password protect access to the CAV interface. Implementing the steps explained on this page means another user will not be able to access the CAV interface to modify or over-ride the security settings you have implemented.

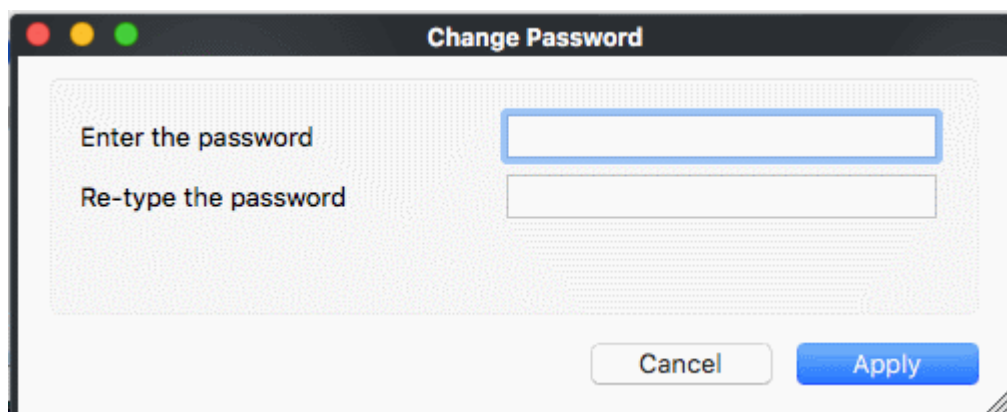
[Click here](#) for more details on parental control settings.

To enable password protection

- Click the 'More' button along the top navigation
- Click 'Preferences' in 'More' menu
- Click on 'Parental Control' tab



- Select 'Enable password protection for the settings' checkbox to activate password protection
- Click 'Change Password'

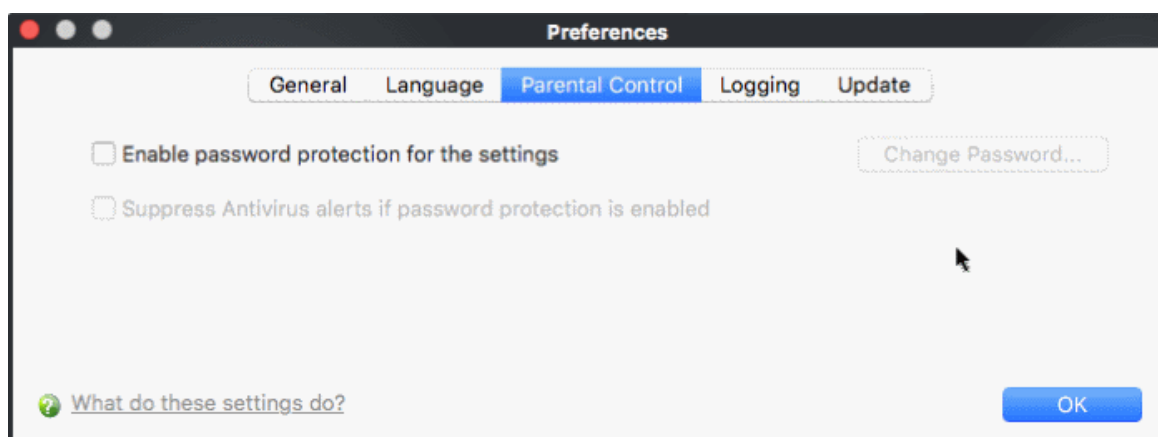


- In the 'Change Password' dialog, type a password and retype the password in the respective text boxes
- Click 'Apply'.

Enabling password protection will secure all of your important CAV settings and configurations. After setting a password, users will be asked for this password every time they try to access important configuration of the Antivirus Tasks areas.

Suppress alerts when password protection is enabled

- If password protection is enabled, you also have the option to suppress alerts. This option means threats are blocked but no alert is shown to the user.
- This avoids the situation where a user could click 'Allow' just to dismiss an alert, and thus expose the computer to infection.



If you choose to suppress alerts, you must remember to un-suppress them next time you log on. If you don't, then CAV will continue to silently block certain actions without notification.

Notes:

- The 'suppress' setting blocks all alerts, so some software updaters may be unable to run.
- One idea is to create a preset configuration called 'Updaters'. Configure it to allow all your updaters to run smoothly.

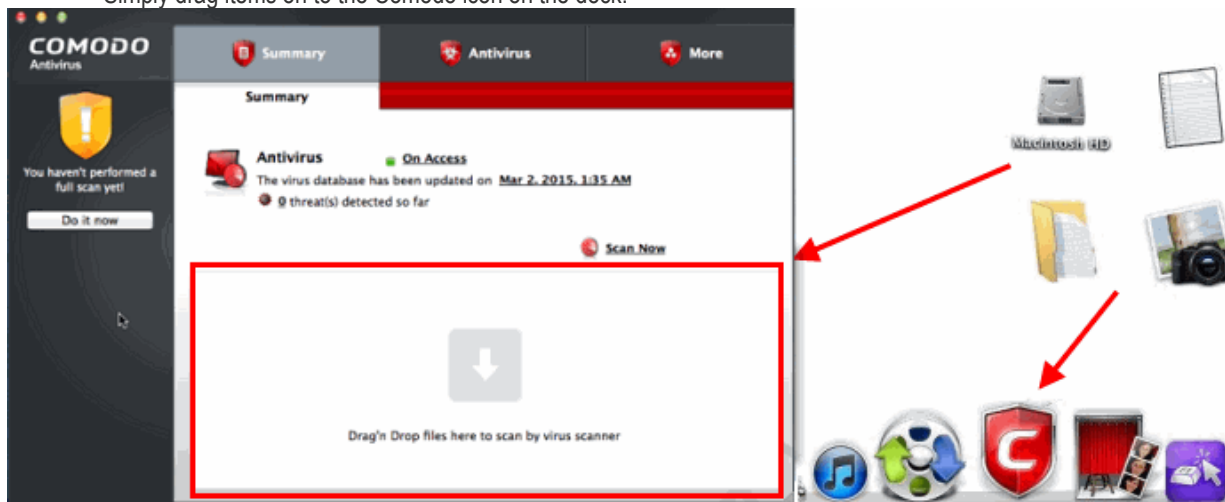
1.8.6. How to Run an Instant Antivirus Scan on Selected Items

You can scan any file, folder or drive by simply dragging the item into the scan box or onto the Comodo dock icon.

- Open Comodo Antivirus for MAC
- Drag items you want to scan into the box on the summary screen

OR

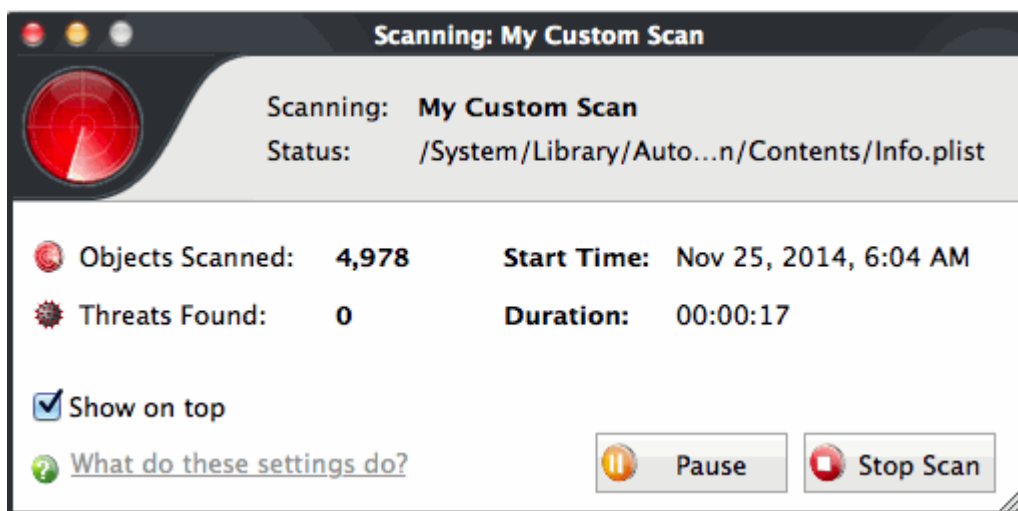
- Simply drag items on to the Comodo icon on the dock.



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



Scanning will commence immediately after the updates are installed.



The scan results list all detected threats along with their risk level.

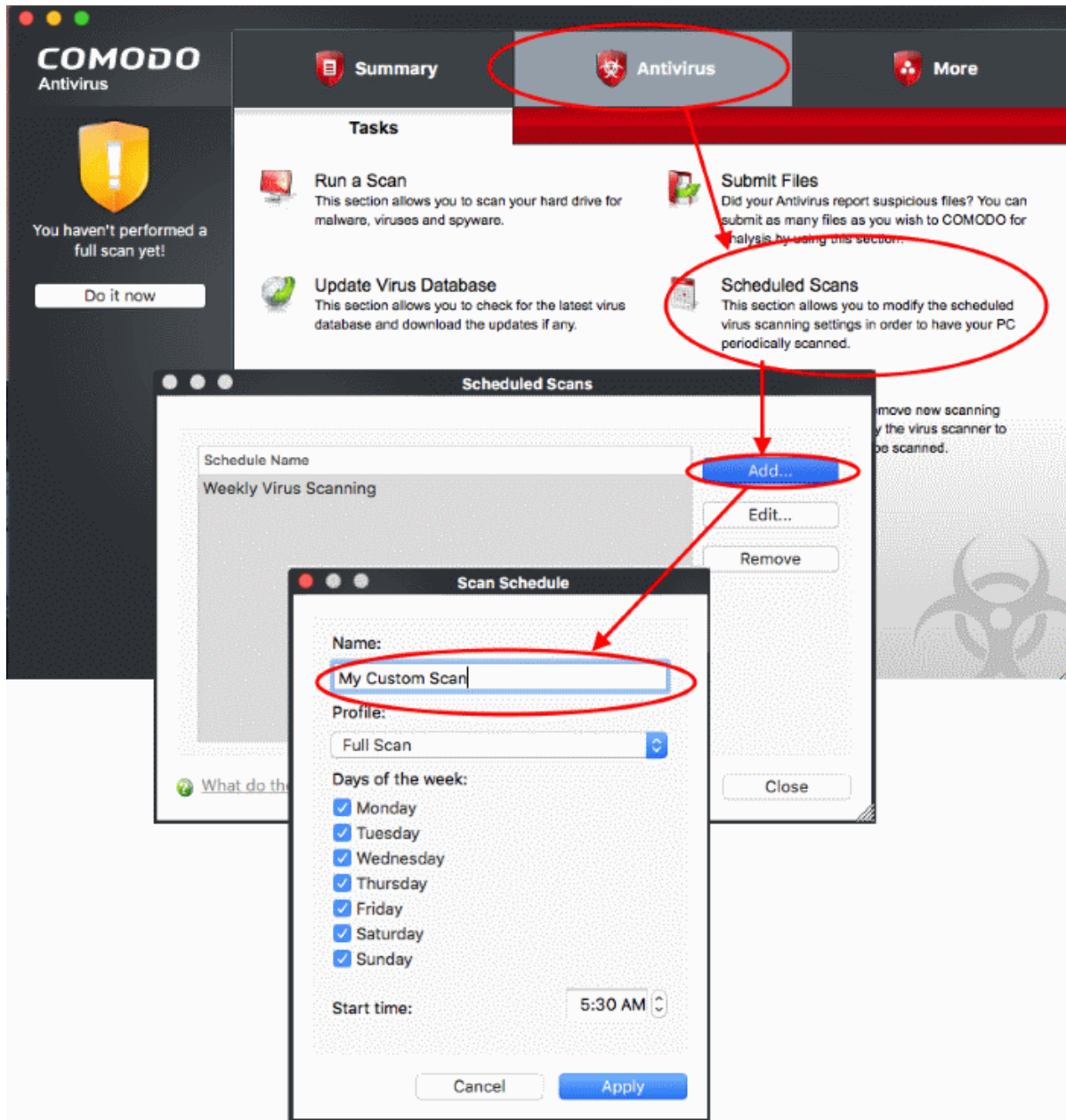
[Click here](#) for help on how to react if infected item(s) are found.

1.8.7. How to Create a Scheduled Scan

Comodo Antivirus lets you schedule virus scans on your entire system or on specific areas.

Create an antivirus scan schedule

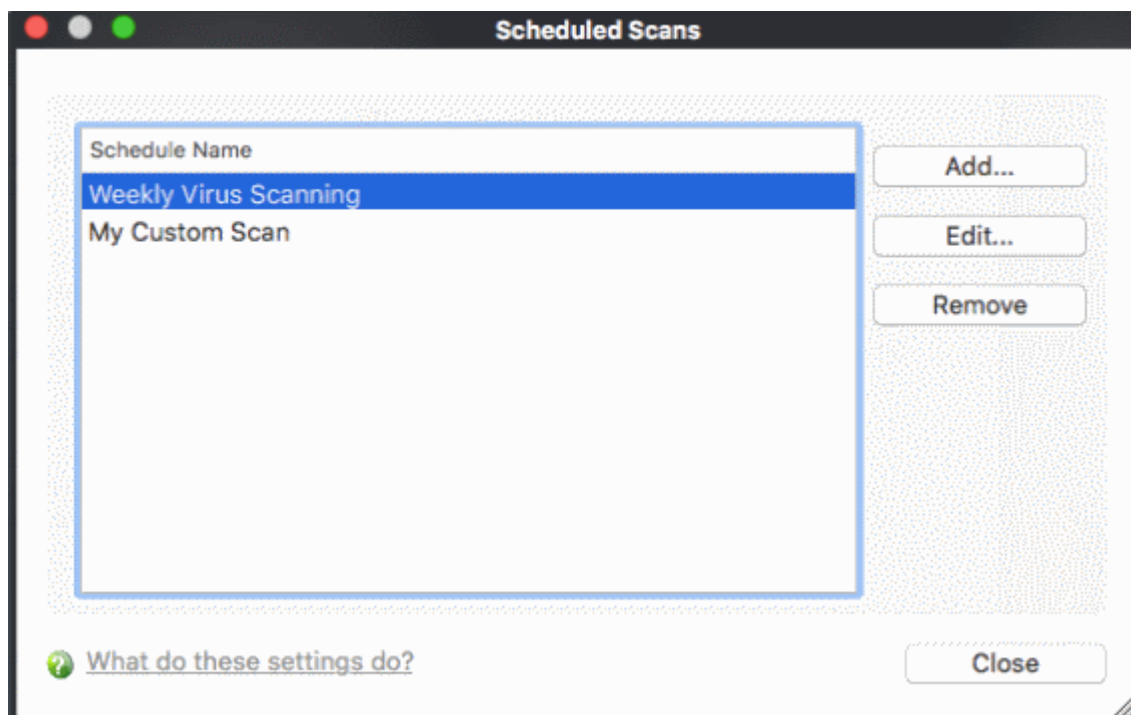
- Click the 'Antivirus' tab on the home screen
- Click 'Scheduled Scans' then 'Add'
- Type a name for your schedule, and pick the days and time of the scans.



- Profile - A profile determines what areas of your computer are scanned. Chose a profile from the drop-down.
 - **Full Scan** – Scans every file, folder and drive on your computer.
 - **Quick Scan** – A faster, targeted scan of very important areas on your computer.
 - You can also create your own custom profiles if required.
 - Click the 'Antivirus' tab > 'Scan Profiles' > click the 'Add...' button
 - See 'Antivirus Tasks' > 'Scan Profiles' if you need help with this.

- Click 'Apply' to save your schedule.

Your new scan schedule will be listed in the 'Scheduled Scans' interface. You can modify or remove it at any time by clicking the 'Edit...' or 'Remove'.



Repeat the process to add new scan schedules.

See '[Antivirus Tasks](#)' > '[Scheduled Scans](#)', for more details on the 'Scheduled Scans'.

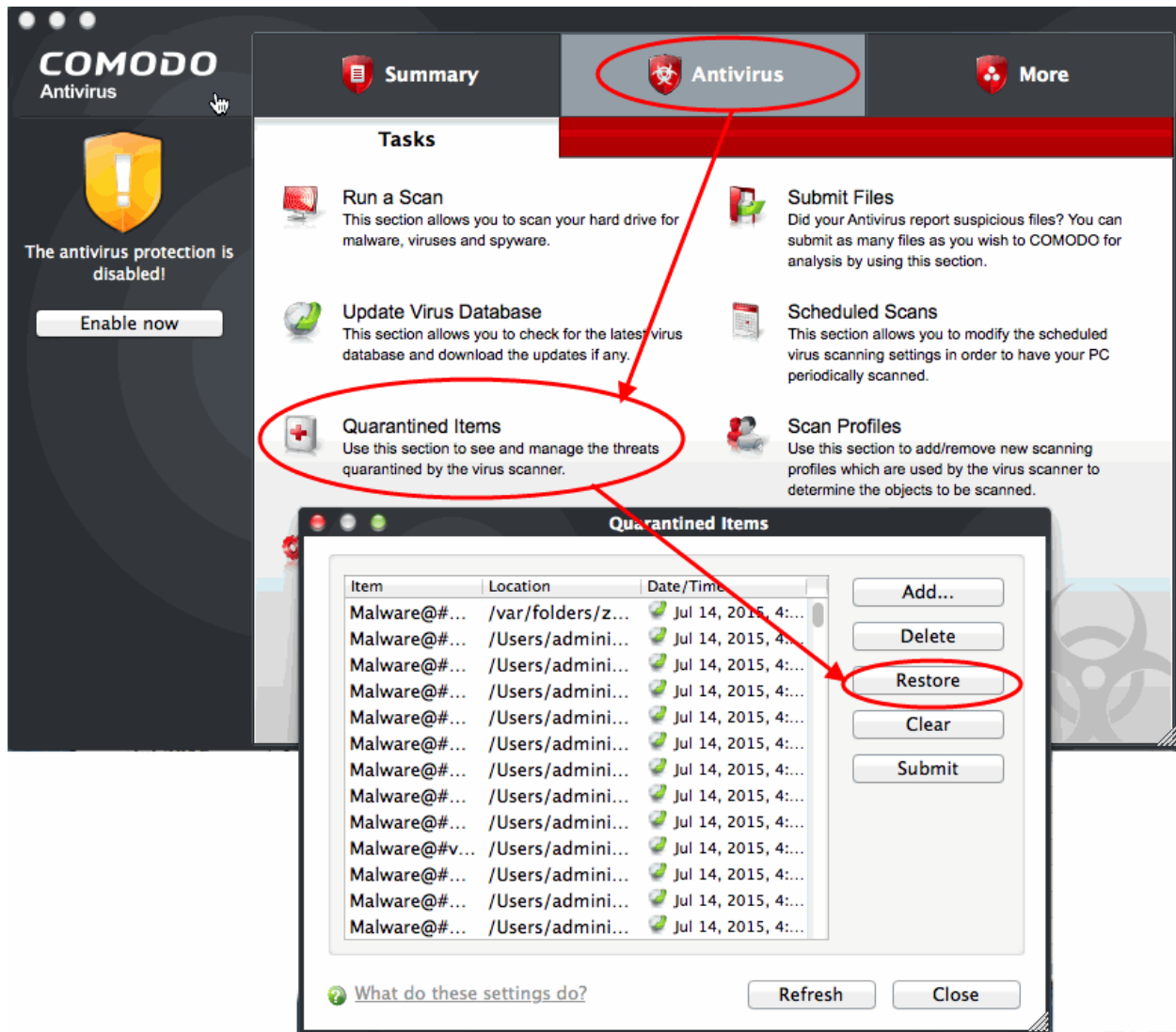
1.8.8. How to Restore Incorrectly Quarantined Items

You may want to remove an item from quarantine if:

- You have incorrectly placed an item in quarantine
- You think CAV has quarantined a safe item (a false positive)

You can restore items as follows:

- Click 'Antivirus' on the CAV home screen
- Click 'Quarantined Items'
- Select the items you wish to remove from quarantine. Hold down the CTRL key to select multiple items.
- Click the 'Restore' button.



All selected items will be restored to their original locations.

- Click 'Close' to exit.

[Click here](#) for more details on quarantined items.

1.8.9. How to Submit Quarantined Items to Comodo for Analysis

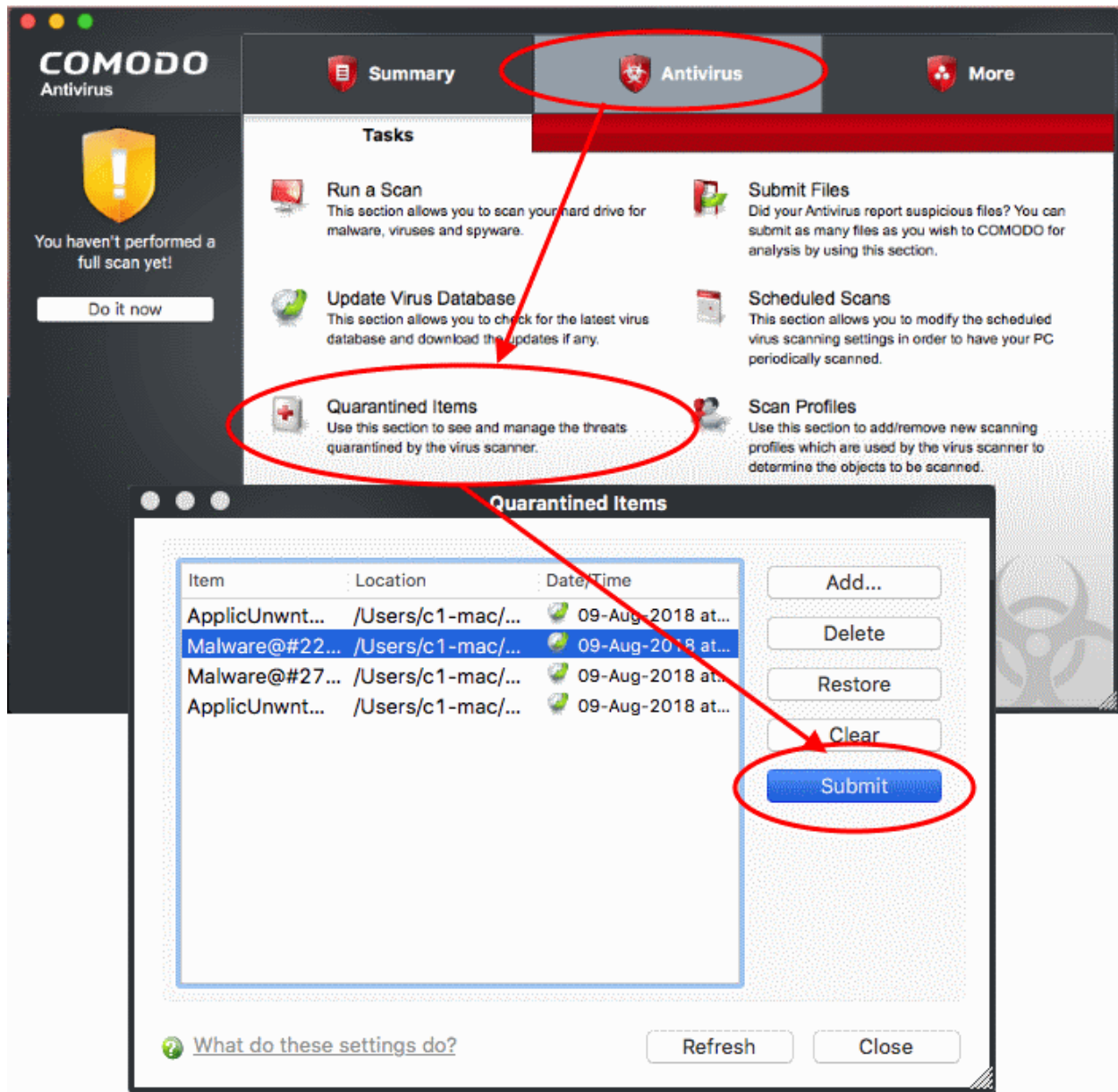
- Items which have been quarantined by the antivirus engine can be sent to Comodo for further analysis. The analysis can have the following outcomes:
 - Confirmed as malware. The item will remain on the global blacklist
 - Confirmed as false-positive. The item will be moved to the global white-list. It will no longer be flagged as malware by antivirus scans.
- This helps Comodo to enhance its virus signature database and helps benefit millions of other CAV users.

[Click here](#) for more details on 'Quarantined Items'.

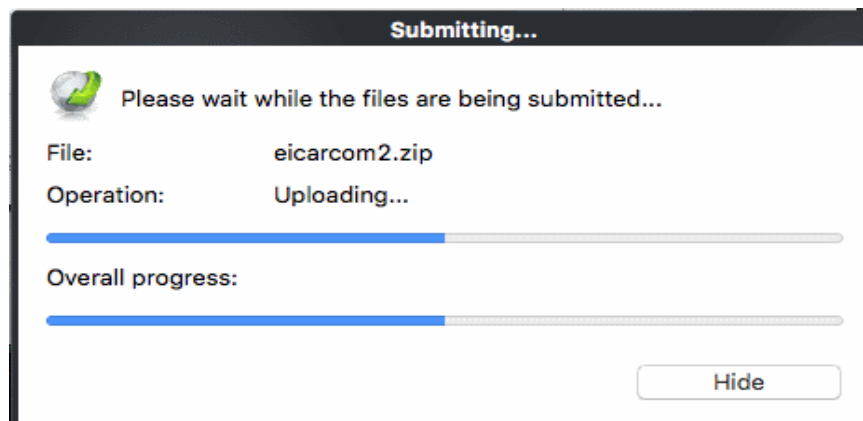
To submit quarantined items

- Click 'Antivirus' on the home screen
- Click 'Quarantined Items'
- Select the items you wish to submit for analysis. To select multiple items, press and hold down the «COMMAND» key.

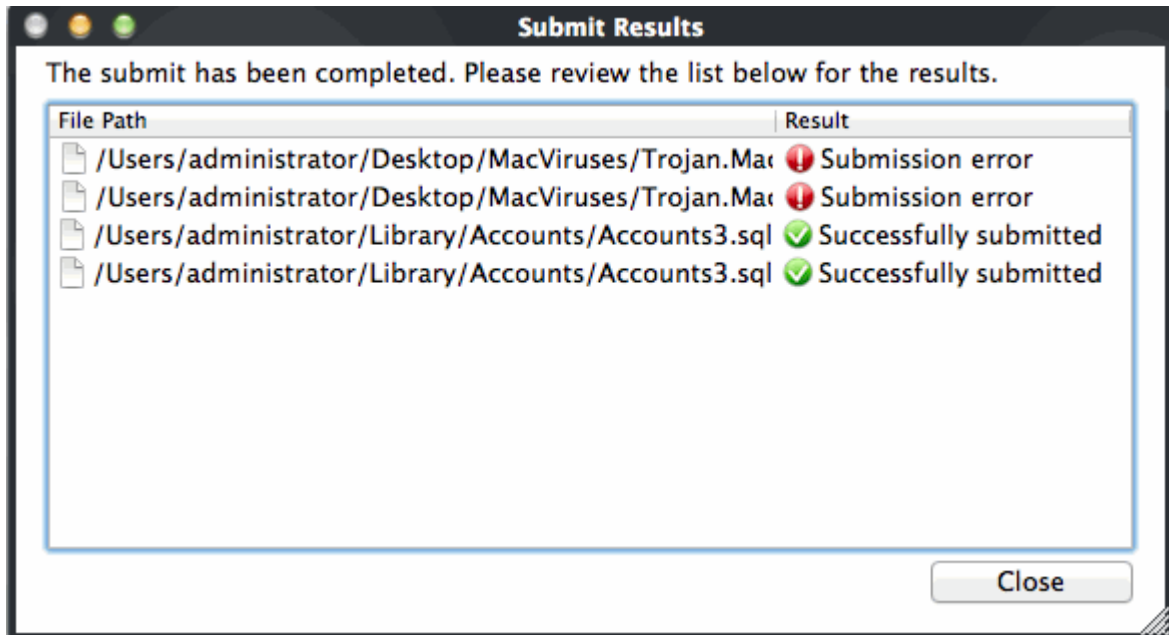
- Click 'Submit'



The file will be submitted to Comodo:



The summary screen tells you whether the submission was successful or not:



1.8.10. How to Switch off Automatic Software and Antivirus Updates

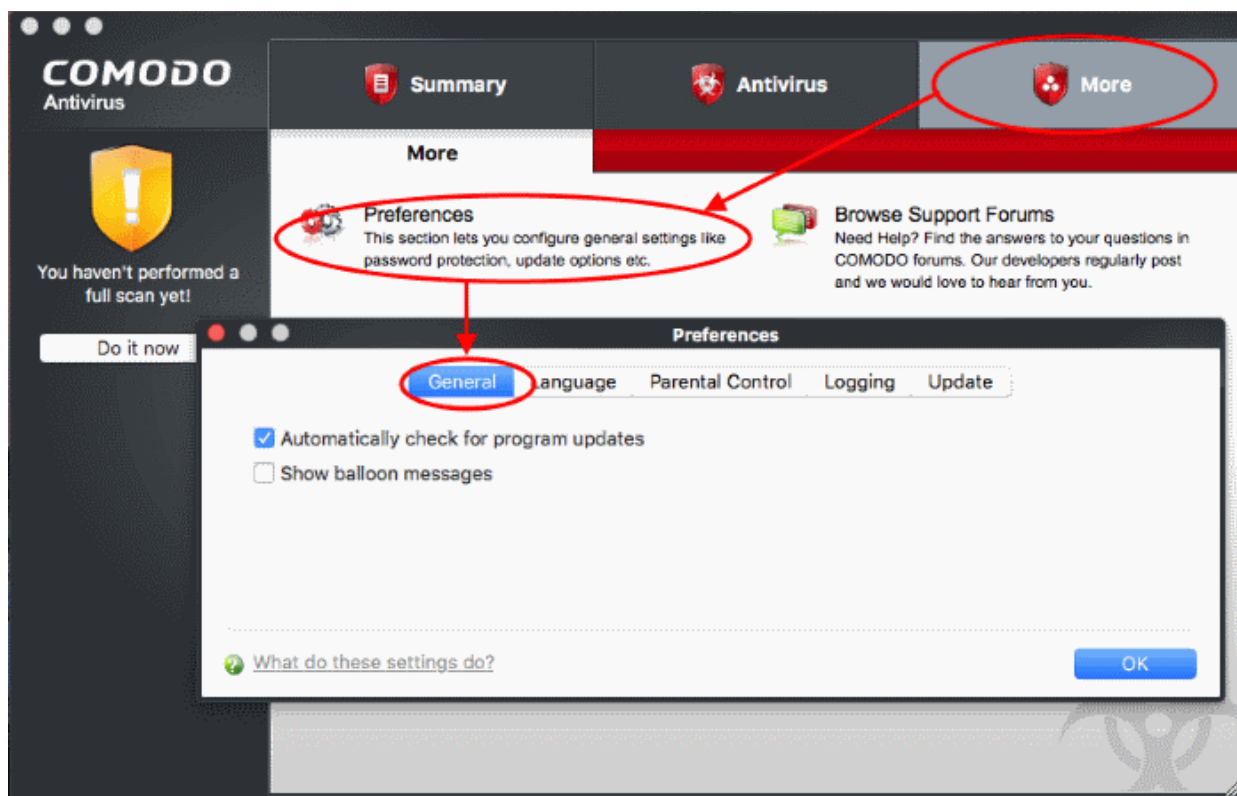
- By default, Comodo Antivirus automatically checks for software and virus database updates.
- However, some users like to have control over what gets downloaded and when it gets downloaded.
 - For example, network administrators may not wish to automatically download because it will take up too much bandwidth during the day.
- Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

CAV provides full control over virus and software updates. Click the appropriate link below to find out more:

- [Switch off automatic software updates](#)
- [Switch off automatic virus updates](#)

To switch off automatic software updates:

- Click 'More' on the CAV home screen.
- Click 'Preferences' > 'General'
- Deselect 'Automatically check for program updates'.



- Click 'OK'.

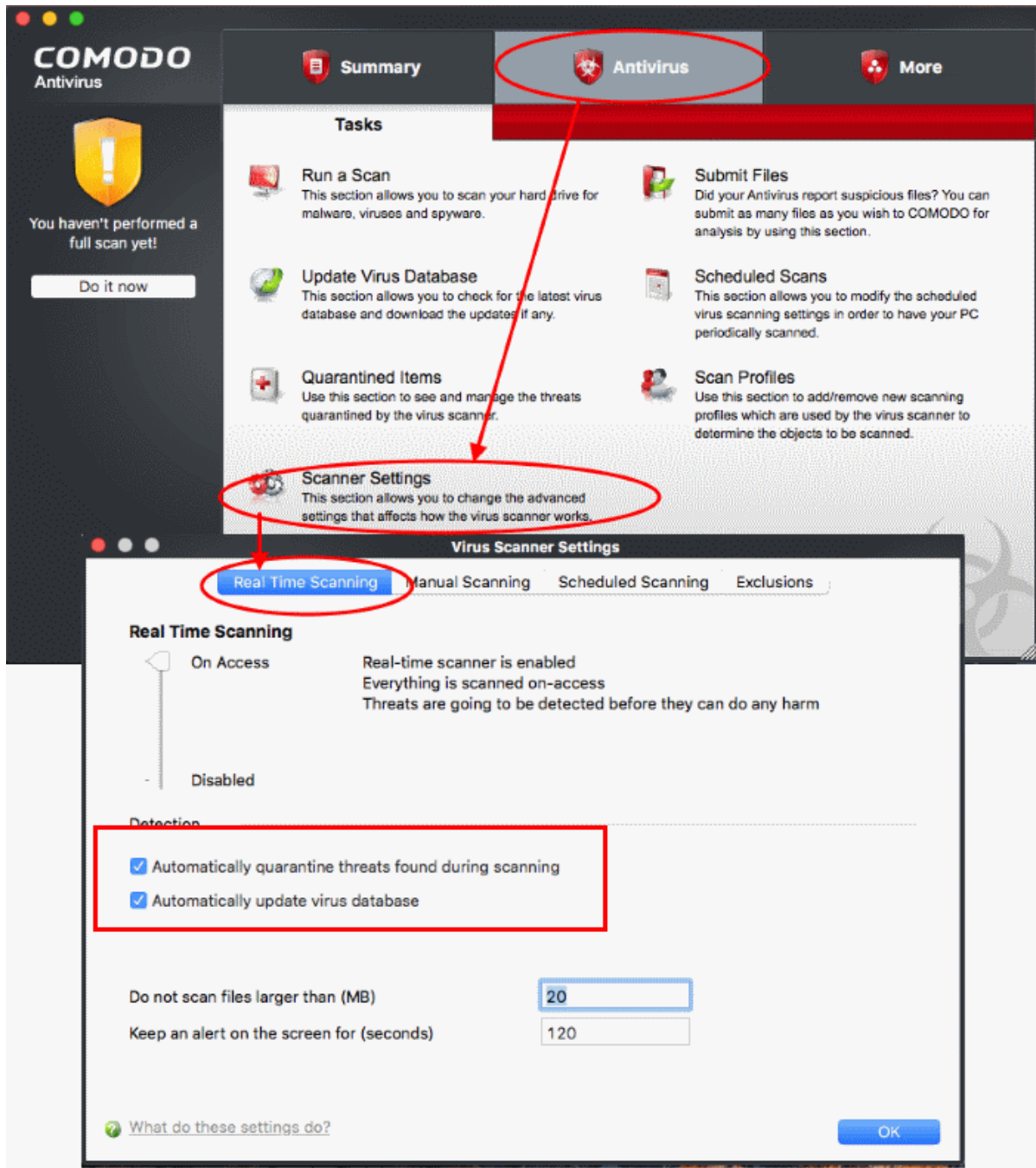
To switch off automatic Antivirus database updates:

Automatic virus updates can be completely switched off, or can be switched off for individual scans. Click the link appropriate to your requirements:

- [Switch off automatic virus updates](#)
- [Switch off updates prior to a Manual Scan](#)
- [Switch off updates prior to a Scheduled scan](#)

To Switch off automatic virus database updates

- Click 'Antivirus' on the CAV home screen.
- Click 'Scanner Settings' > 'Real Time Scanning'
- Deselect 'Automatically update virus database'



- Click 'OK'.

Comodo Antivirus will no longer check for or download database updates.

To switch off virus database updates prior to a Manual Scan

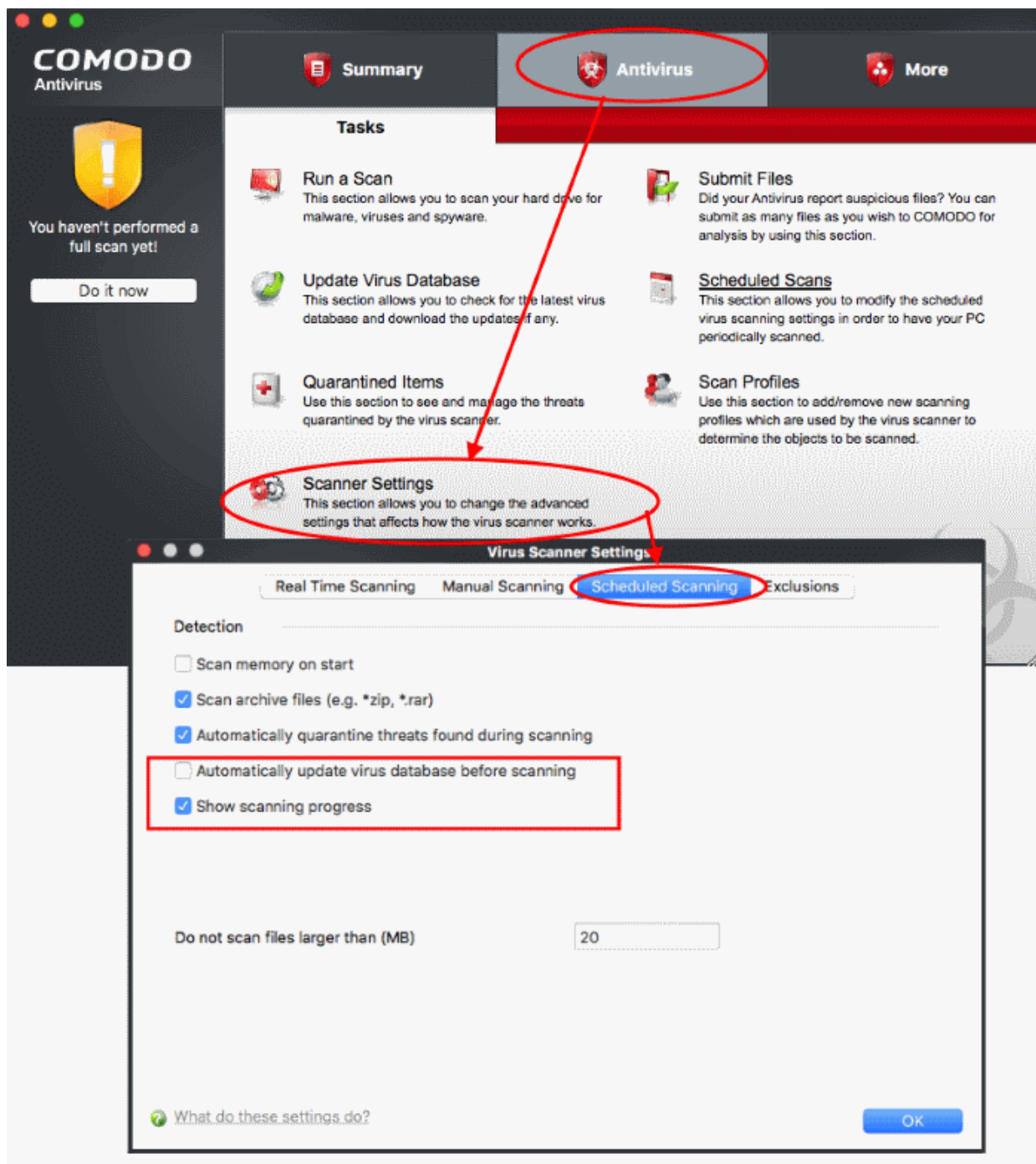
- Click 'Antivirus' on the CAV home screen
- 'Scanner Settings' > 'Manual Scanning'
- Disable 'Automatically update the virus database before scanning'.
- Click 'OK'.

The screenshot displays the Comodo Antivirus for MAC user interface. The main window has a dark sidebar on the left with the Comodo logo and a notification: "You haven't performed a full scan yet!" with a "Do it now" button. The main area has a top navigation bar with "Summary", "Antivirus", and "More" tabs. The "Antivirus" tab is selected and circled in red. Below the navigation bar is a "Tasks" section with several options: "Run a Scan", "Update Virus Database", "Quarantined Items", "Submit Files", "Scheduled Scans", and "Scan Profiles". The "Scanner Settings" option is circled in red, and a red arrow points from the "Antivirus" tab to it. A "Virus Scanner Settings" dialog box is open in the foreground, with the "Manual Scanning" tab selected and circled in red. The dialog box has four tabs: "Real Time Scanning", "Manual Scanning", "Scheduled Scanning", and "Exclusions". Under the "Detection" section, there are four checkboxes: "Scan memory on start" (unchecked), "Scan archive files (e.g. *.zip, *.rar)" (checked), "Automatically quarantine threats found during scanning" (checked), and "Automatically update virus database before scanning" (checked). The last two checked items are enclosed in a red box. Below this is a field "Do not scan files larger than (MB)" with the value "20". At the bottom left is a link "What do these settings do?" and at the bottom right is an "OK" button.

CAV will no longer download updates prior to on demand scans.

To switch off virus database updates prior to a Scheduled Scan

- Click 'Antivirus' on the CAV home screen
- 'Scanner Settings' > 'Scheduled Scanning'
- Disable 'Automatically update the virus database before scanning'.
- Click 'OK'.



CAV will no longer download database updates prior to a scheduled scan.

1.8.11. How to Temporarily Suppress Alerts while Playing a Game

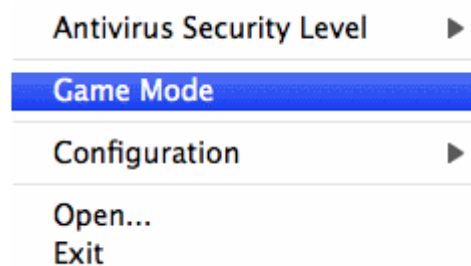
- Placing CAV in 'Game Mode' will temporarily disable alerts from appearing.
- Scheduled virus scans and database updates are postponed until this mode is disabled.
- Real-time protection remains active, your computer remains protected.

To enable game mode

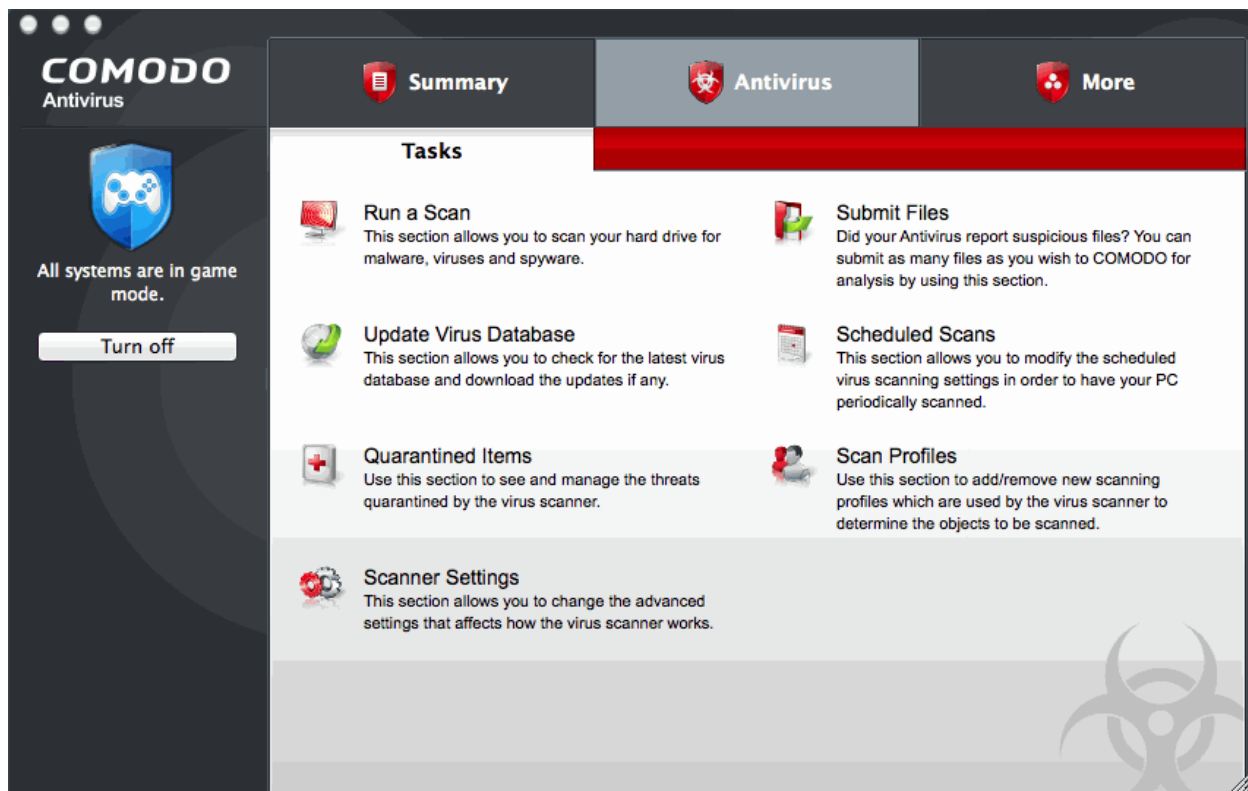
- Right-click on the CAV 'System Tray' icon.



- Select 'Game Mode' from the options.



Alerts are now suppressed. Scheduled scans and virus database updates will not resume until this mode is deactivated.

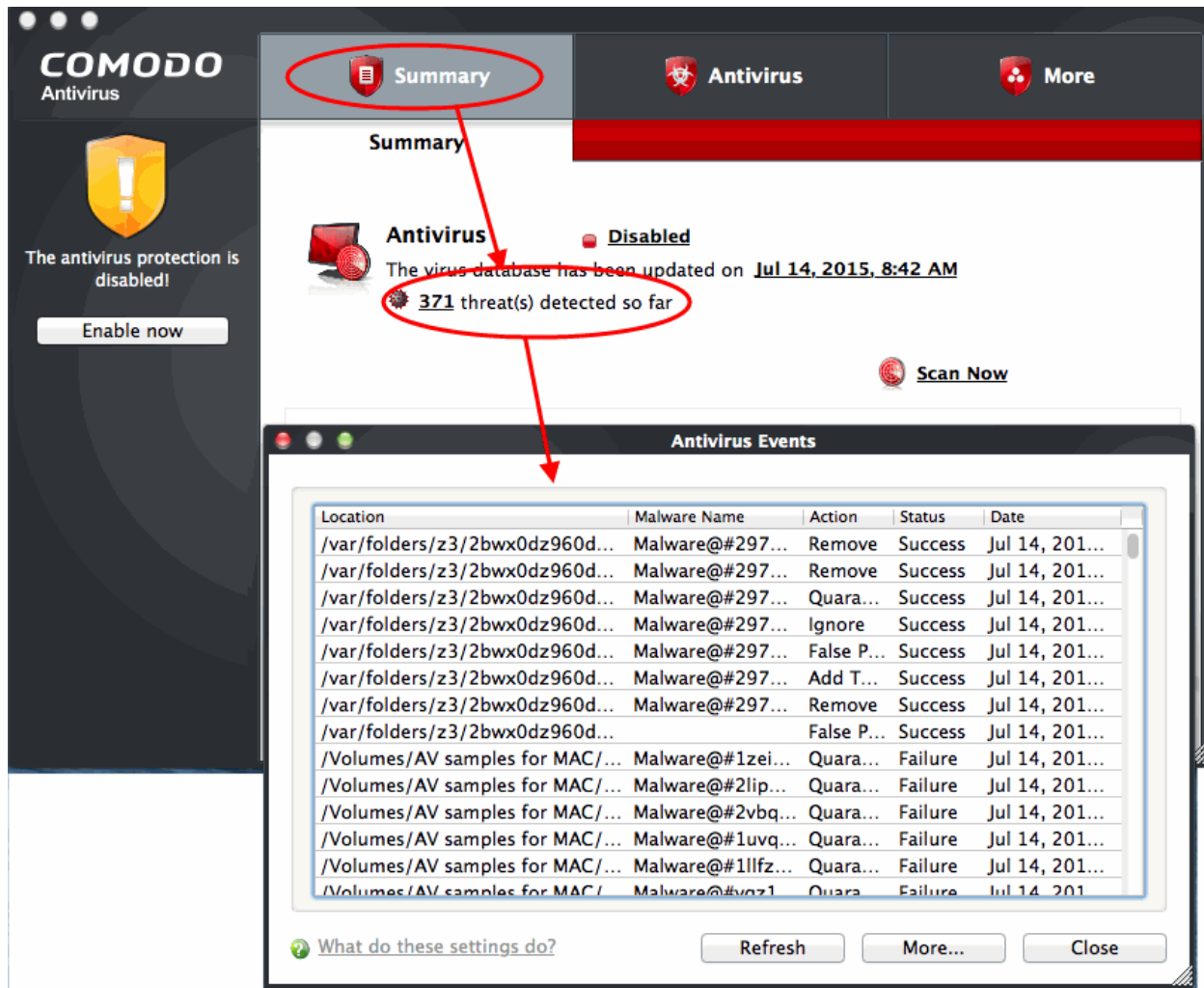


1.8.12. How to View Antivirus Events

- The antivirus events module contains extensive logs of all actions taken by the virus scanner.
- The event viewer tells you the date and time a particular virus was detected, where it was located, and the action that was taken to deal with it.

To view Antivirus Events

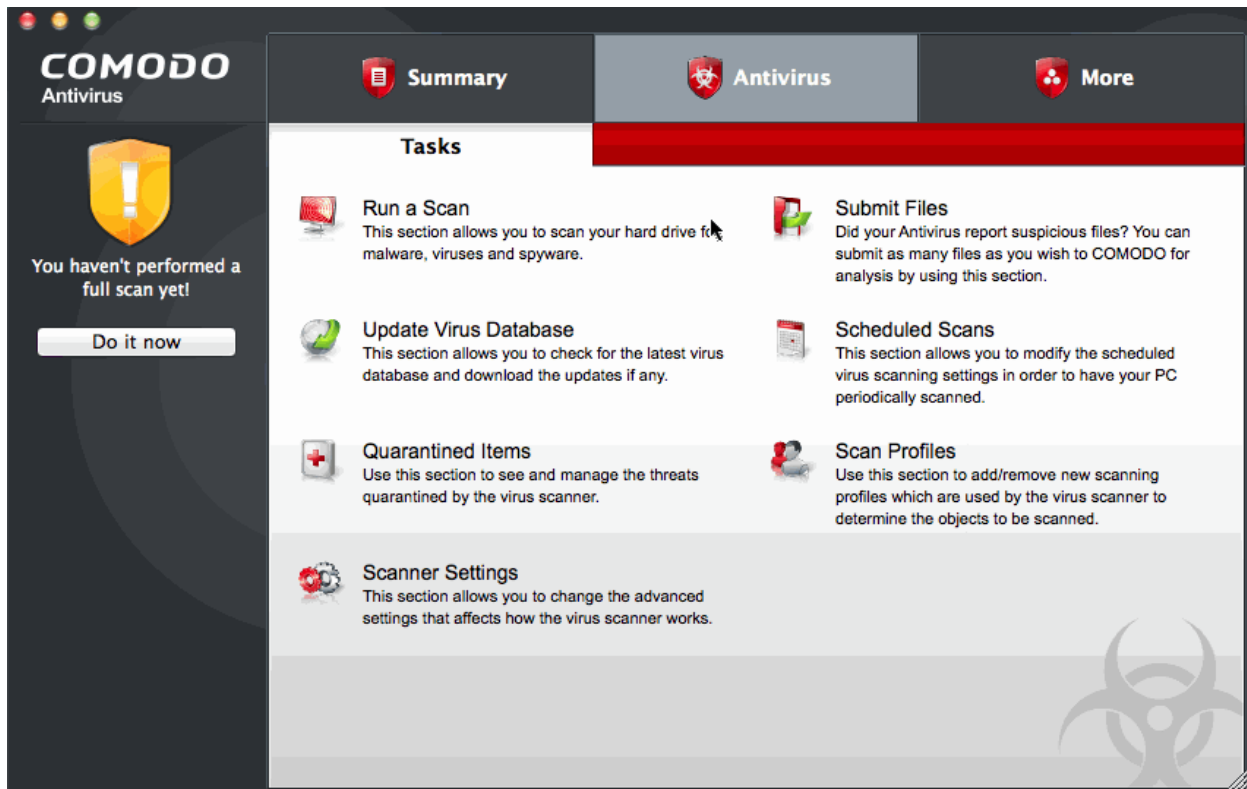
- Click the 'Summary' tab on the CAV home screen
- Click the '<number> of threats detected so far'
- This opens the event log viewer:



See '[View Antivirus Events](#)' section for more detailed information.

2. Antivirus Tasks - Introduction

- Click the 'Antivirus' tab on the home screen to open this interface.
- The antivirus task center lets you run on-demand virus scans and configure how you want the scanner to behave.
- You can alter settings for each scan type and create recurring, scheduled scans.
- You can also create custom scan profiles, manage event logs, change update settings, submit files for analysis and view quarantined files.

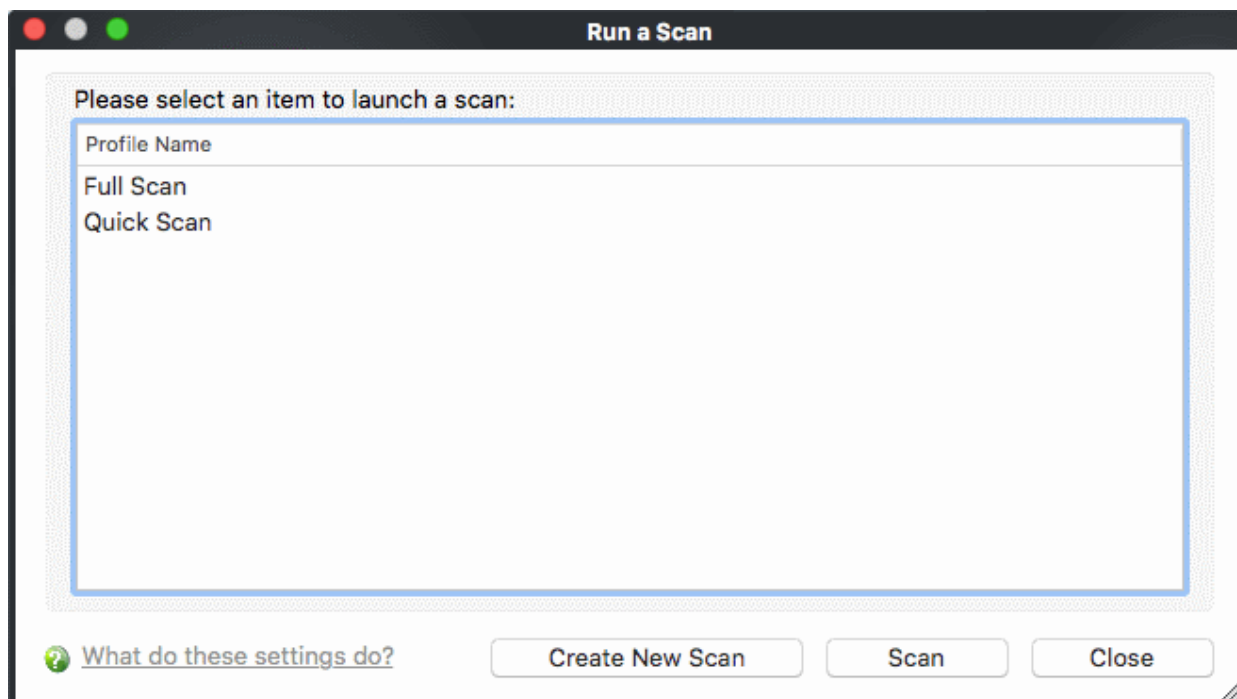


Click the links below to see detailed explanations of each area in this section.

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

2.1. Run a Scan

- The 'Run a Scan' area allows you to launch an **On-Demand Scan** on an item of your choice.
- The item can be anything you choose – your entire computer, a specific drive or partition, or even a single file.
- You can also scan a wide range of removable storage devices such as CD's, DVD's, external hard-drives, USB connected drives, digital cameras and more.



You have two options available when you choose to run an On-Demand Scan:

1. Scan a **preselected area**
2. Define a **custom scan** of the areas you choose.

Scanning Preselected Areas

Comodo Antivirus has two pre-defined scan profiles – 'Full Scan' and 'Quick Scan'. These cannot be edited or removed. They are:

- i. **Full Scan** - When this profile is selected, Comodo Antivirus scans every local drive, folder and file on your system including external devices, storage drives, digital cameras.
- ii. **Quick Scan** - When this profile is selected, Comodo Antivirus runs a scan of important operating system files and folders including system memory, auto-run entries, hidden services.

To run one of these profiles, simply highlight it from the list and click 'Scan' (or just double-click the profile name).

Custom Scan

To run a scan on a particular item of your choosing, you first need to create a scan profile. To do this:

- Click 'Create New Scan'
- Type a name for your new profile in the 'Scan Profile' dialog (for example, 'My External Drives')
- Click 'Add' to choose the files, folders or drives you wish to include in the scan profile. You can select multiple items
- Click 'Apply' to return to the 'Scan Profile' dialog then 'Apply' again. Your new profile will be listed in the 'Run a Scan' dialog (see [Create a Scan Profile](#) if you need more help with this).
- Select your new profile in the list and click 'Scan'
- Your scan will begin. Next, see:
 - [Scan progress and results](#)
 - [The results window](#)
 - [Save results as a text file](#)
 - [Remove selected items](#)

- **Move threats to quarantine**
- **Disinfect/delete threats**
- **Ignore a result once / Ignore and report as false positive / Ignore and create an exception**

Tip: If you just want to run a quick scan on a file or folder, you can just drag it into the scan box in the 'Summary' area or, if the interface is not open, by dragging it onto the Comodo dock icon.

Tip: See **Antivirus Tasks > Scan Profiles**, for more details on scan profiles.

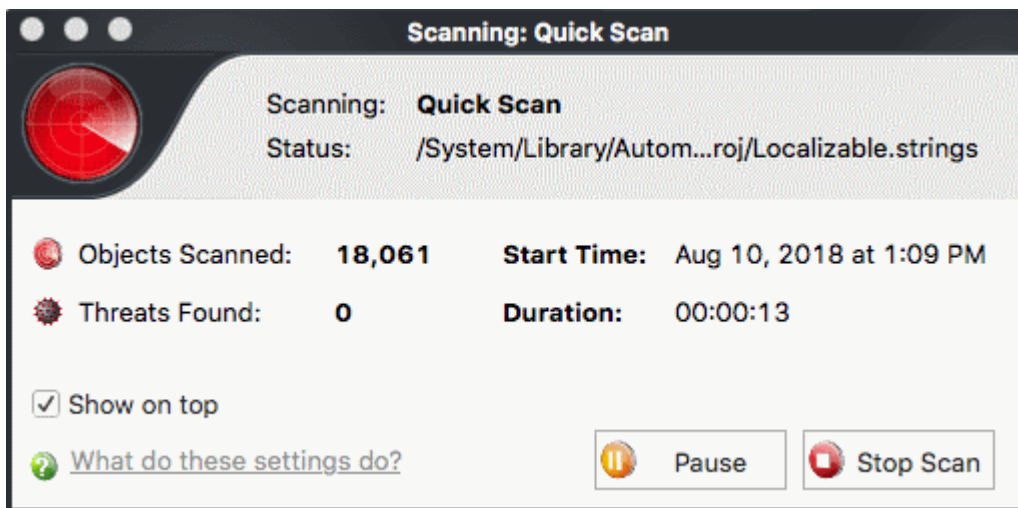
Scan progress and results

Before running the scan, Comodo Antivirus 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 after updates have been installed. The progress dialog displays 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.

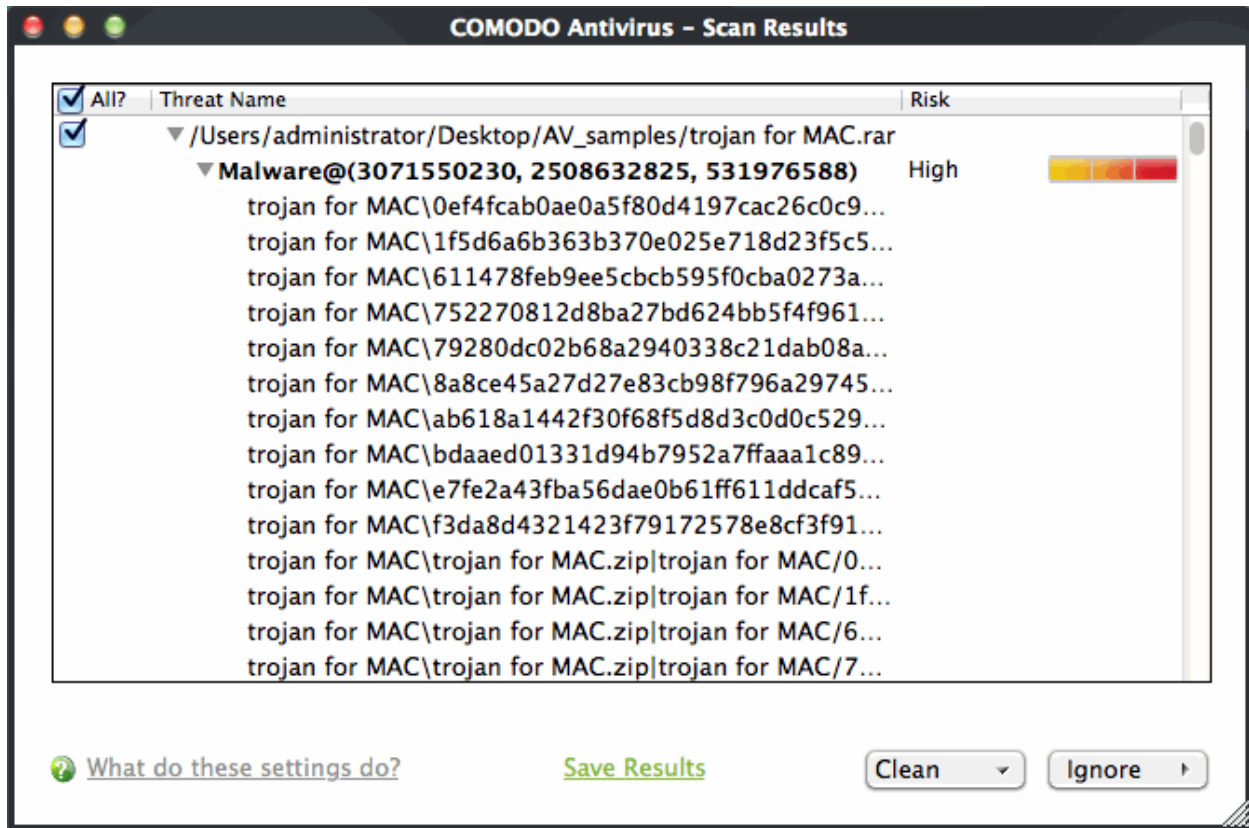
Clicking 'Pause' will suspend the scan until you click 'Resume'. Click 'Stop Scan' to abort the scan process altogether.



Once the scan is complete, the results window will open:

The Results Window

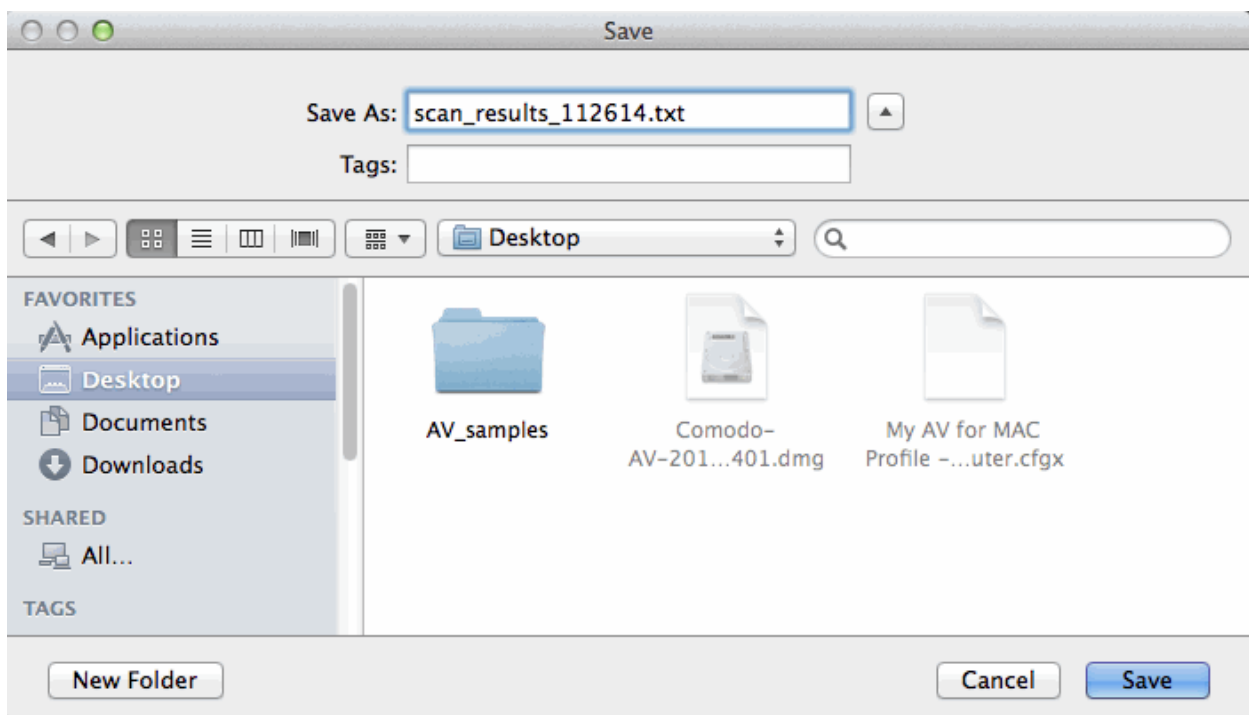
On scan completion, the results screen will list the name and risk level of all threats found:



You can sort the results alphabetically by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header. To select all the entries for actions such as moving them to quarantine or disinfect, select the check box beside the 'Threat name'.

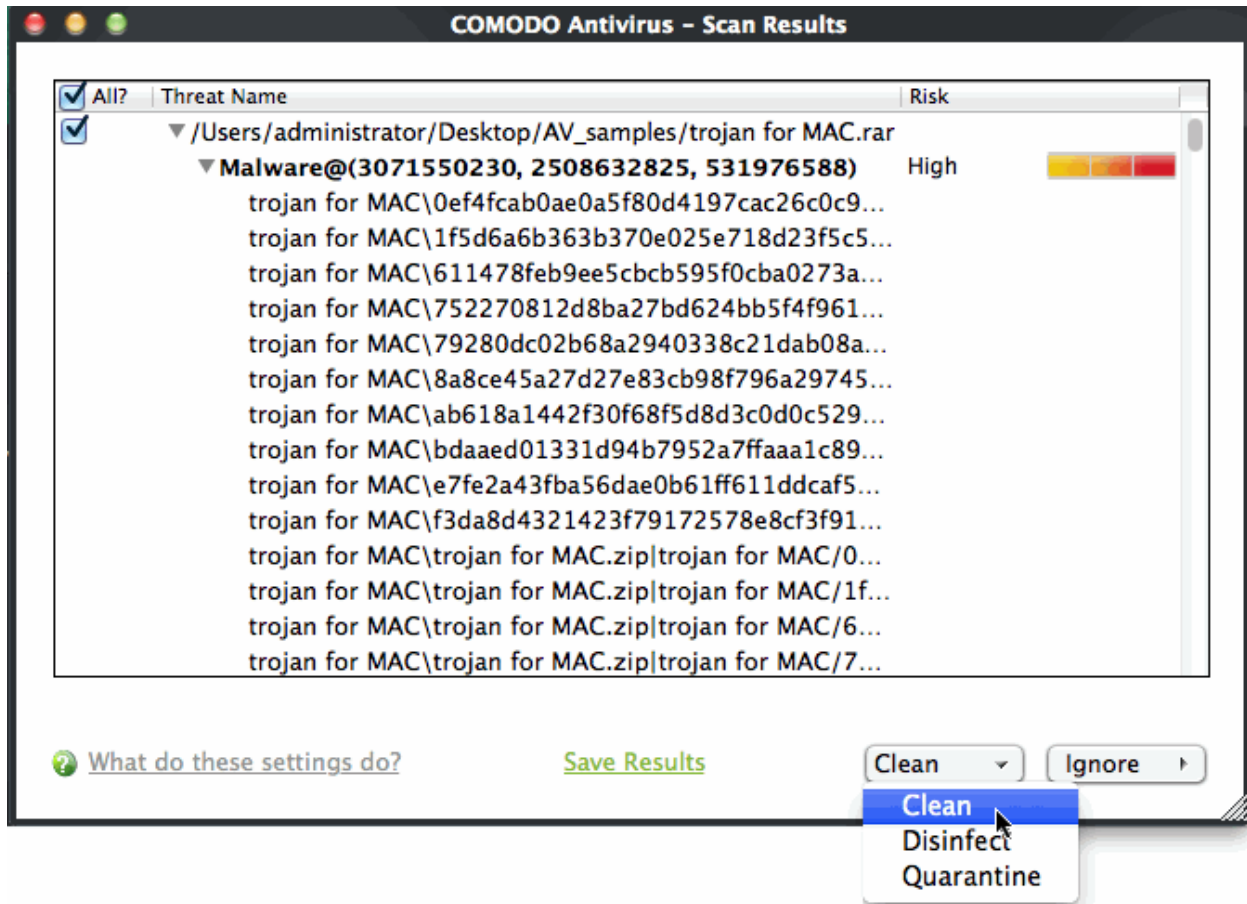
To save the Scan Results as a Text File

1. Click 'Save' and enter the location in the 'Save' dialog box.

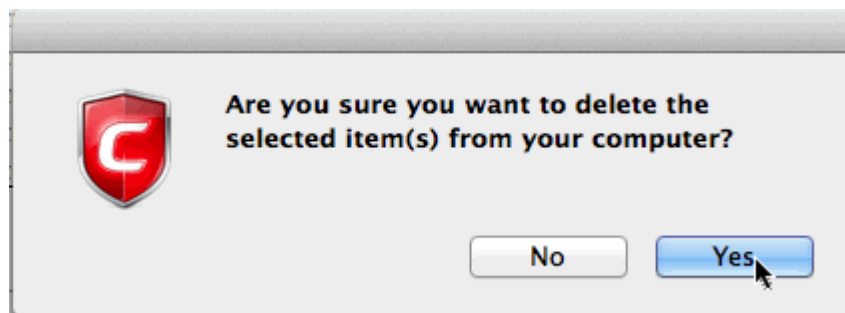


To remove selected items

1. Select the application from the results, click the drop-down button beside 'Clean' and select 'Clean'.



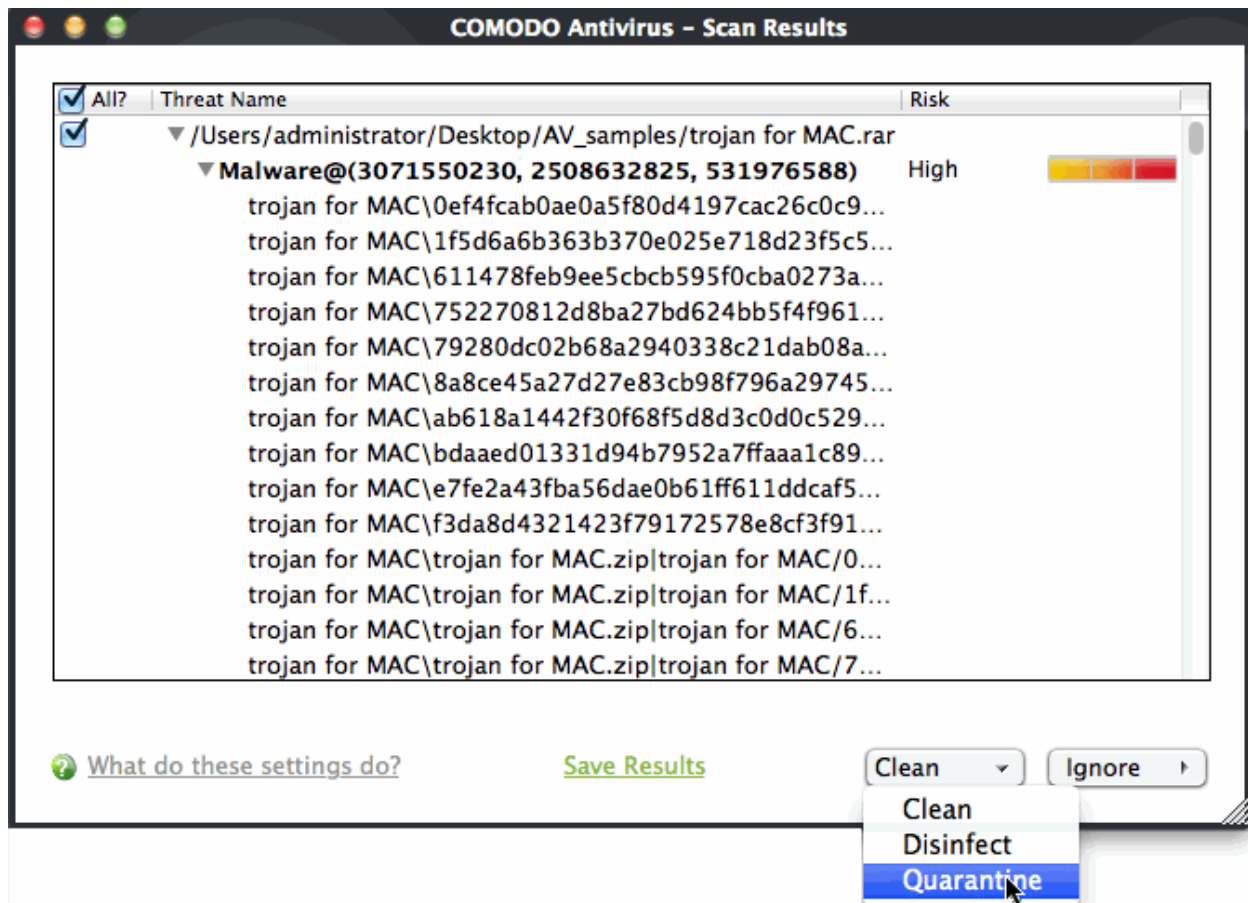
2. Click 'Yes' at the confirmation dialog box.



The file will be deleted permanently from your system.

To move selected threats to Quarantined Items

1. Select the application from the results, click the drop-down button beside 'Clean' and select 'Quarantine'.



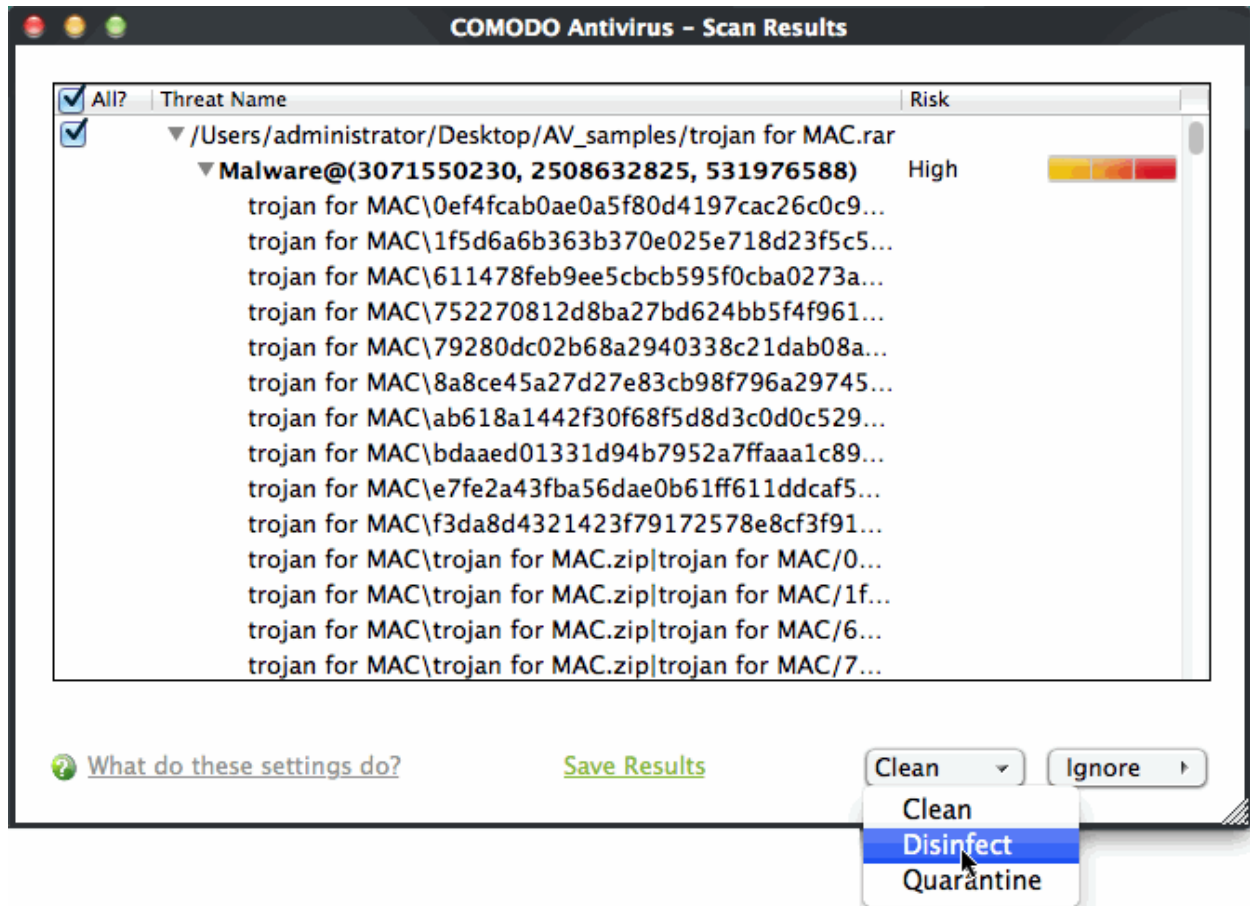
3. Click 'Yes' at the confirmation dialog box.



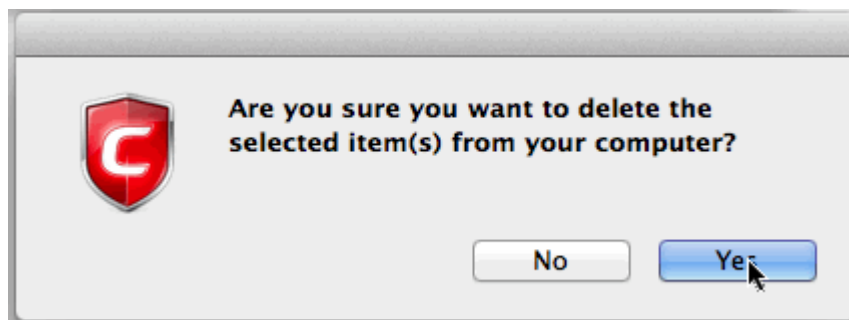
The selected application is moved to the 'Quarantined Items' section. See '[Antivirus Tasks](#)' > '[Quarantined Items](#)', for more details on quarantined applications.

To disinfect a file or application

1. Select the applications from the results, click the drop-down button beside the 'Clean' button and choose 'Disinfect'.



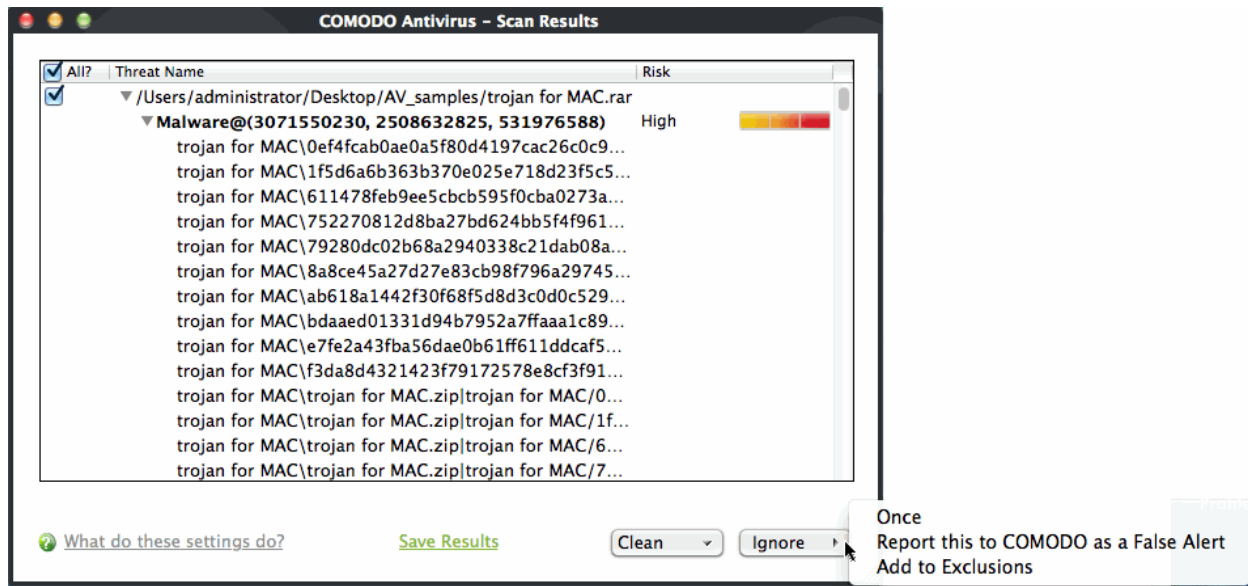
2. Click 'Yes' at the confirmation dialog box.



The Antivirus disinfects the file if a disinfection routine exists. The file will be returned to its pre-viral state. If no disinfection routine is available, the file is deleted permanently from your system.

To ignore an application / file you consider as safe from the threat list

- Click 'Ignore'



Selecting 'Ignore' provides you with three options.

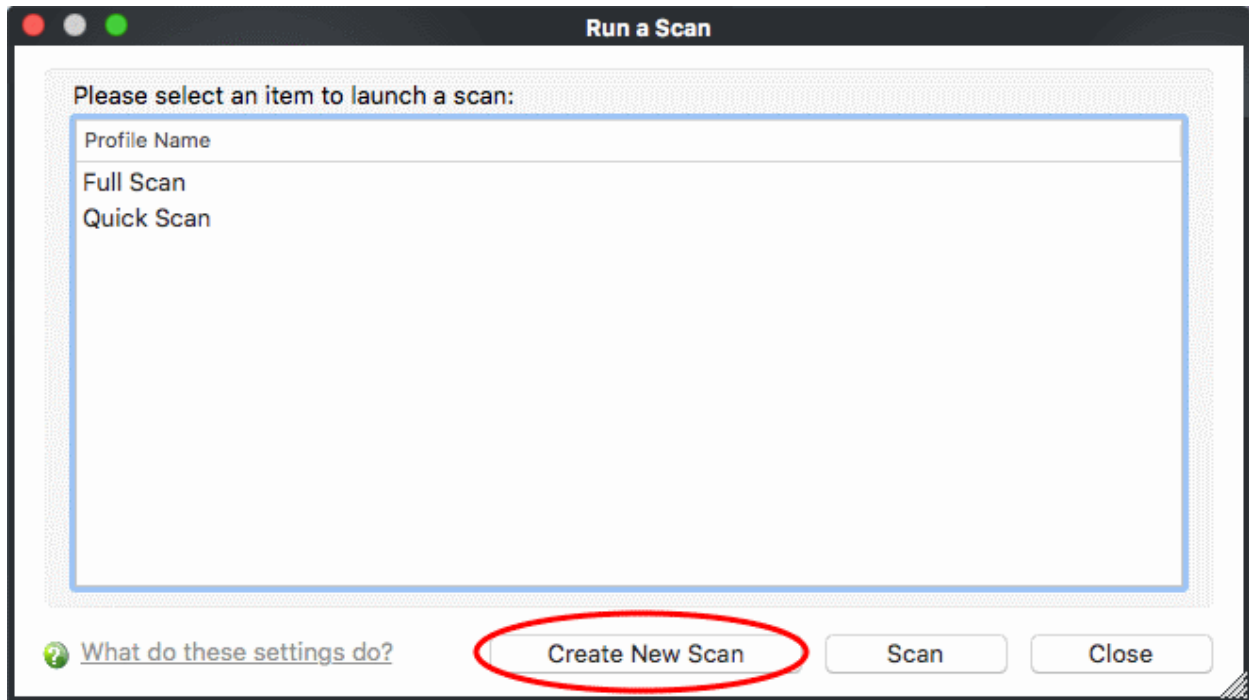
- **Once** - If you click 'Once', the virus is ignored only at that time only. If the same application invokes again, an alert will be displayed.
- **Report this to COMODO as a False Alert** – If you are sure that the file is safe, select 'Report this to Comodo as False Alert'. This will submit the file to Comodo for analysis. If the file is found to be trustworthy, it will be added to the Comodo white-list.
- **Add to Exclusions** - If you click 'Add to Exclusions', the virus is moved to '**Exclusions**' list. The alert is not generated if the same application invokes again.

Creating a Scan profile

'Scan Profiles' are the user-defined profiles containing specific areas on your system that you wish to scan and can be re-used for all future scans.

To create a new scan profile

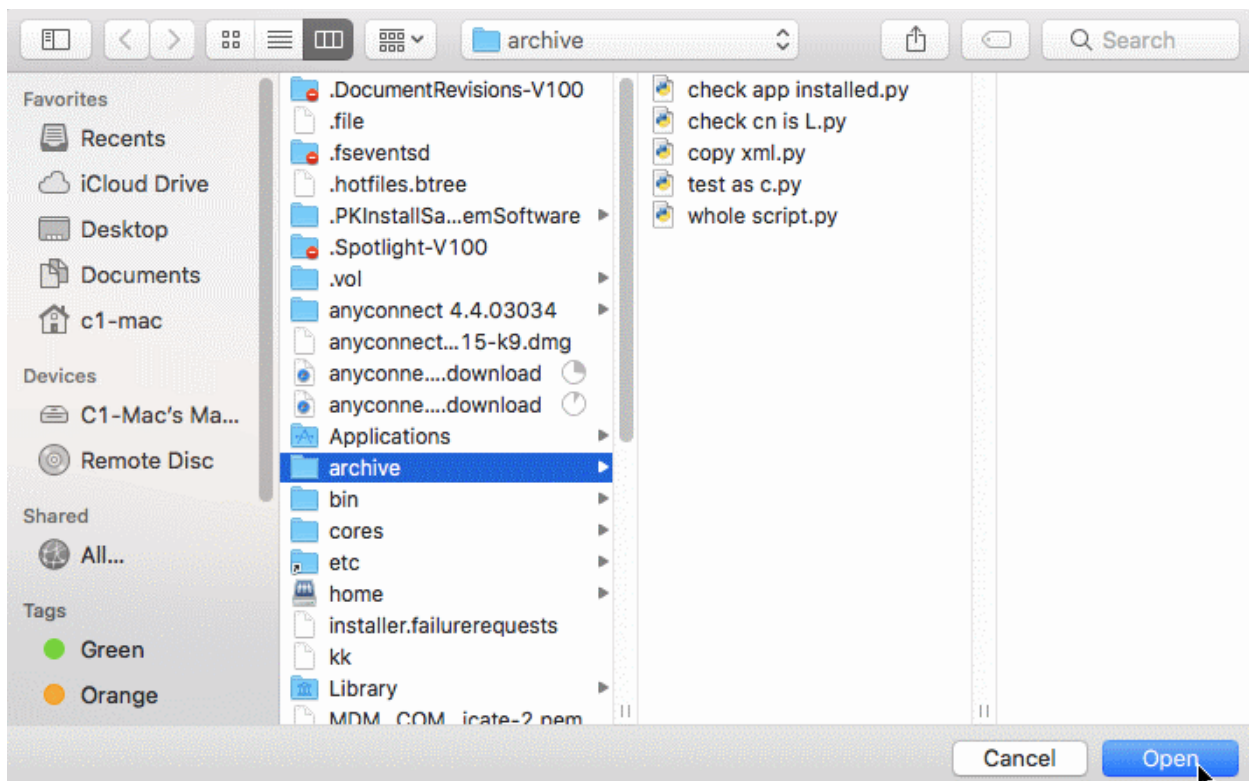
- Click the 'Antivirus' tab on the CAV home screen
- Click 'Run a Scan' > 'Create New Scan'



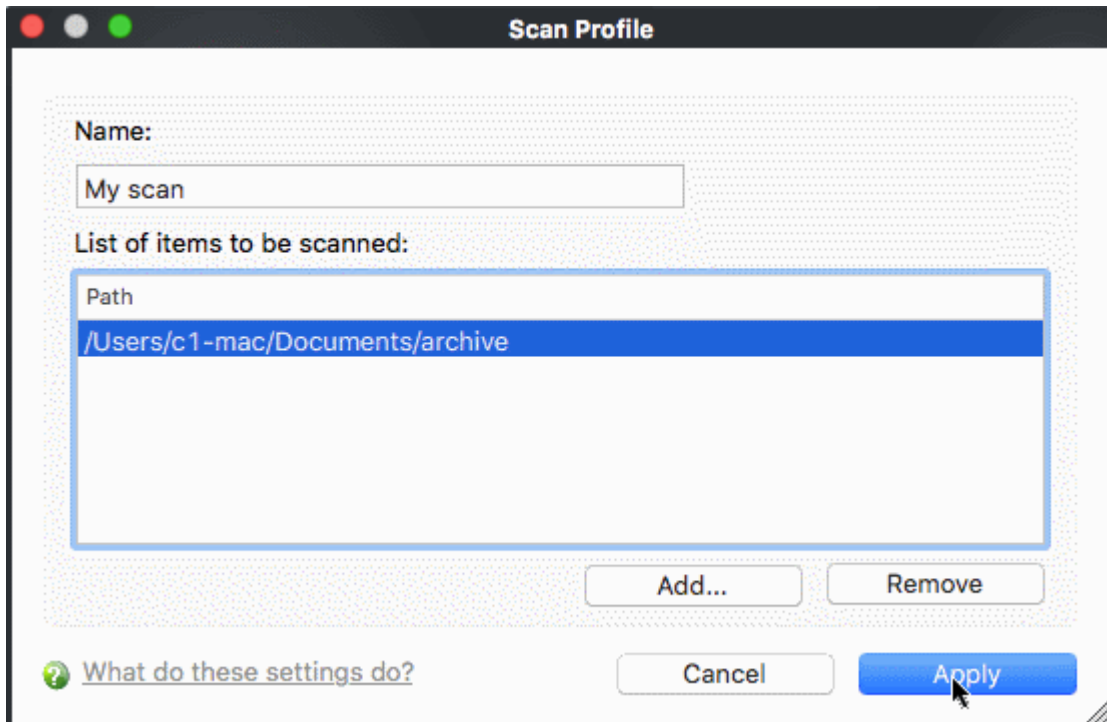
A 'Scan Profile' configuration appears.

- Type a name for the scan profile to be created in the 'Name' box.
- Click 'Add'.

A locator appears, prompting you to select the locations to be scanned when the newly created scan profile is selected.



- Select the folder or file path for scan from the left column
- Click 'Open'
- Click 'Apply'.

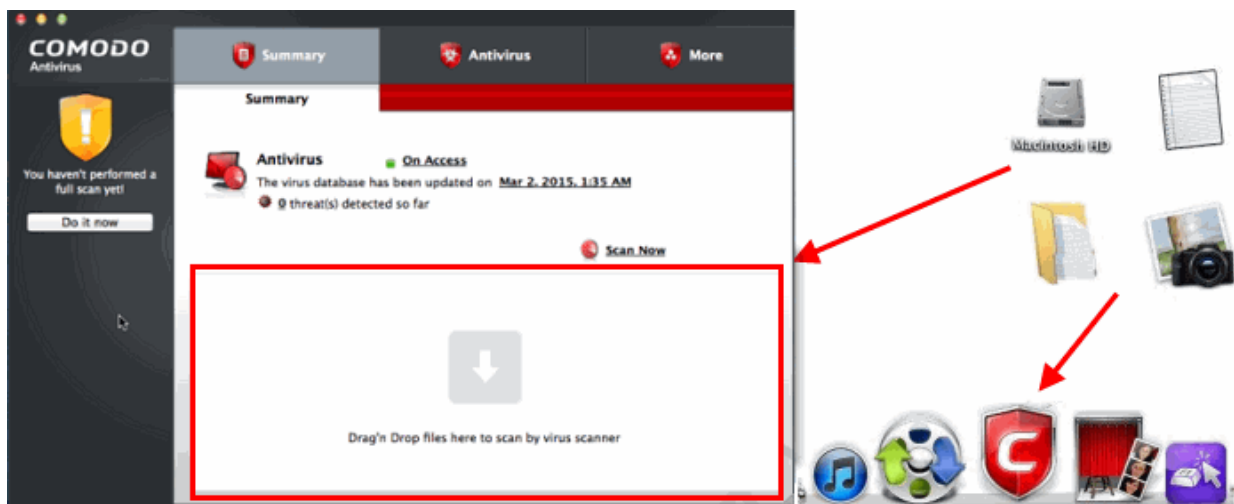


- Repeat the process to create more scan profiles.

Note: You can also create new scan profiles by accessing **Scan Profiles** in the 'Antivirus' screen.

Instantly Scan Objects

You can instantly virus scan virtually any file, folder, photo, application or hard-drive by simply dragging the item into the scan box on the summary screen or onto the Comodo icon on the dock.



2.2. Update Virus Database

- In order to guarantee the continuing effectiveness of your antivirus software, it is imperative that your virus databases are updated as regularly as possible.
- Our antivirus database is maintained and updated around the clock by a team of dedicated technicians, providing you with constant protection against the latest virus outbreaks.

- Updates can be downloaded to your system **manually** or **automatically**.

To manually check for the latest virus Database and then download the updates

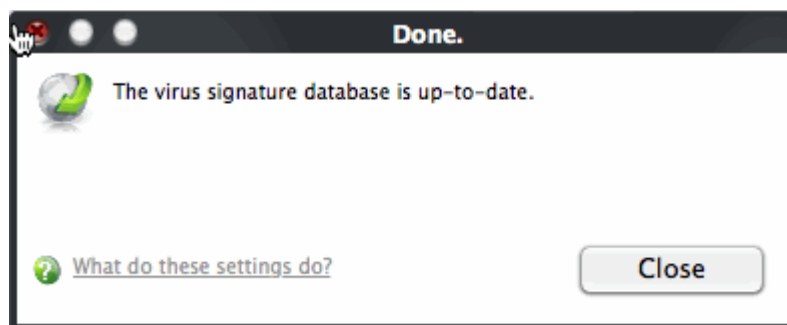
1. Click the 'Antivirus' tab on the CAV home screen
2. Click 'Update Virus Database'

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

A dialog box appears, showing you the progress of update process.



You will see the following notification 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 Antivirus recommends a course of action and gives a supporting explanation.

Automatic Updates

By default, Comodo Antivirus is set to automatically check for and download updates from the Comodo servers before commencing a scan of any type. You can configure whether these automatic checks updates take place on a 'per scanner' basis in 'Scanner Settings'. See **Real Time Scanning Settings** and **Scheduled Scanning Settings** 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.

2.3. Quarantined Items

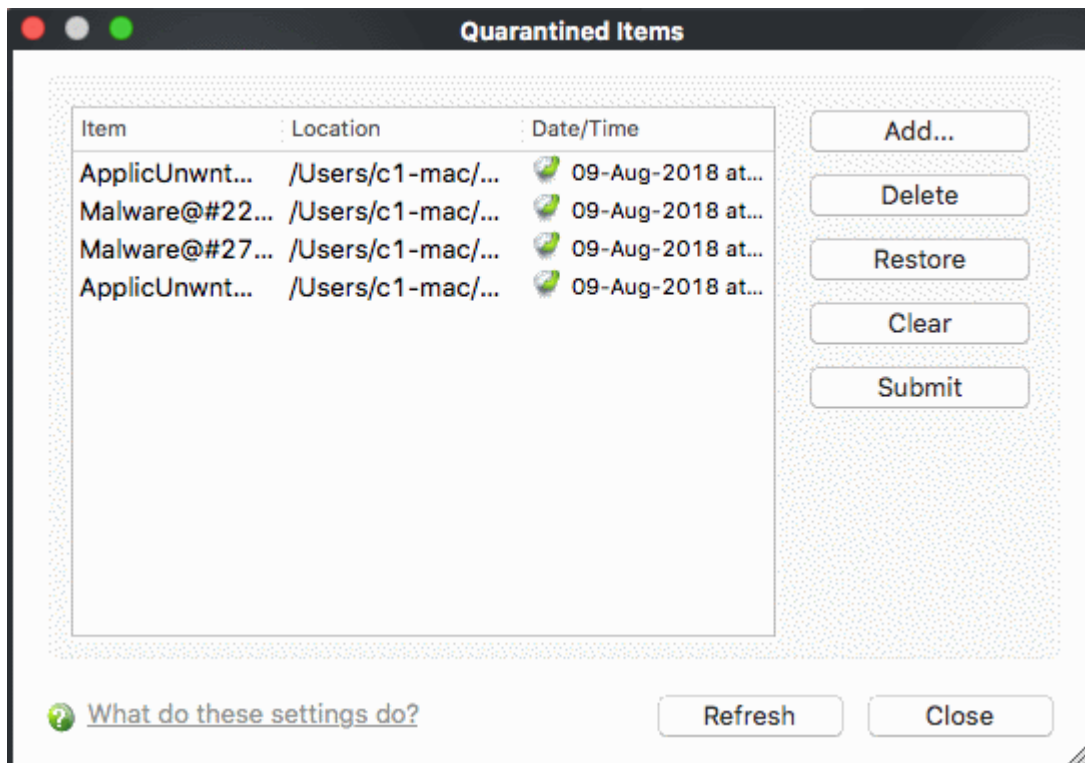
- Click 'Antivirus' > 'Quarantined Items' to open this interface
- Comodo Antivirus virus places threats that it finds on your computer into quarantine.
- Quarantined files are encrypted, so they cannot run or cause damage.
- This isolation prevents infected files from affecting your computer.

The quarantine area lets you:

- **Manually add files to quarantine**
- **Delete quarantined items**
- **Restore quarantined items**
- **Submit quarantined items to Comodo for analysis**

To view Quarantined Items

- Click the 'Antivirus' tab on the CAV home screen.
- Click 'Quarantined Items' in the antivirus tasks screen
- This will open a list of all items in quarantine (if any):



Manually add files to Quarantine

You can move a file to quarantine if you suspect it is malicious, but hasn't been detected by the AV scanner.

- Click 'Antivirus' > 'Quarantined Items'
- Click 'Add' and select the file you want to quarantine

To delete a quarantined item

- Click 'Antivirus' > 'Quarantined Items'
- Select the item you want to remove then click 'Delete'.

This deletes the file from your computer permanently.

To restore a quarantined item to its original location

- Click 'Antivirus' > 'Quarantined Items'
- Select the item and click 'Restore'.

If the restored item is not malicious then it will run as normal. If it contains malware then it will be flagged as a threat and re-quarantined. You should add the file as an exception if you do not want this to happen.

To submit quarantined items to Comodo for analysis

- Click 'Antivirus' > 'Quarantined Items'
- Select the desired item from the list and click 'Submit'.
- The file will undergo behavior analysis from Comodo's automated testing systems, and by our human operatives.
- If it is found to be safe (a false-positive), it will be added to the white-list of safe files.
- If it is confirmed as malicious then it will remain on the black-list of known threats.

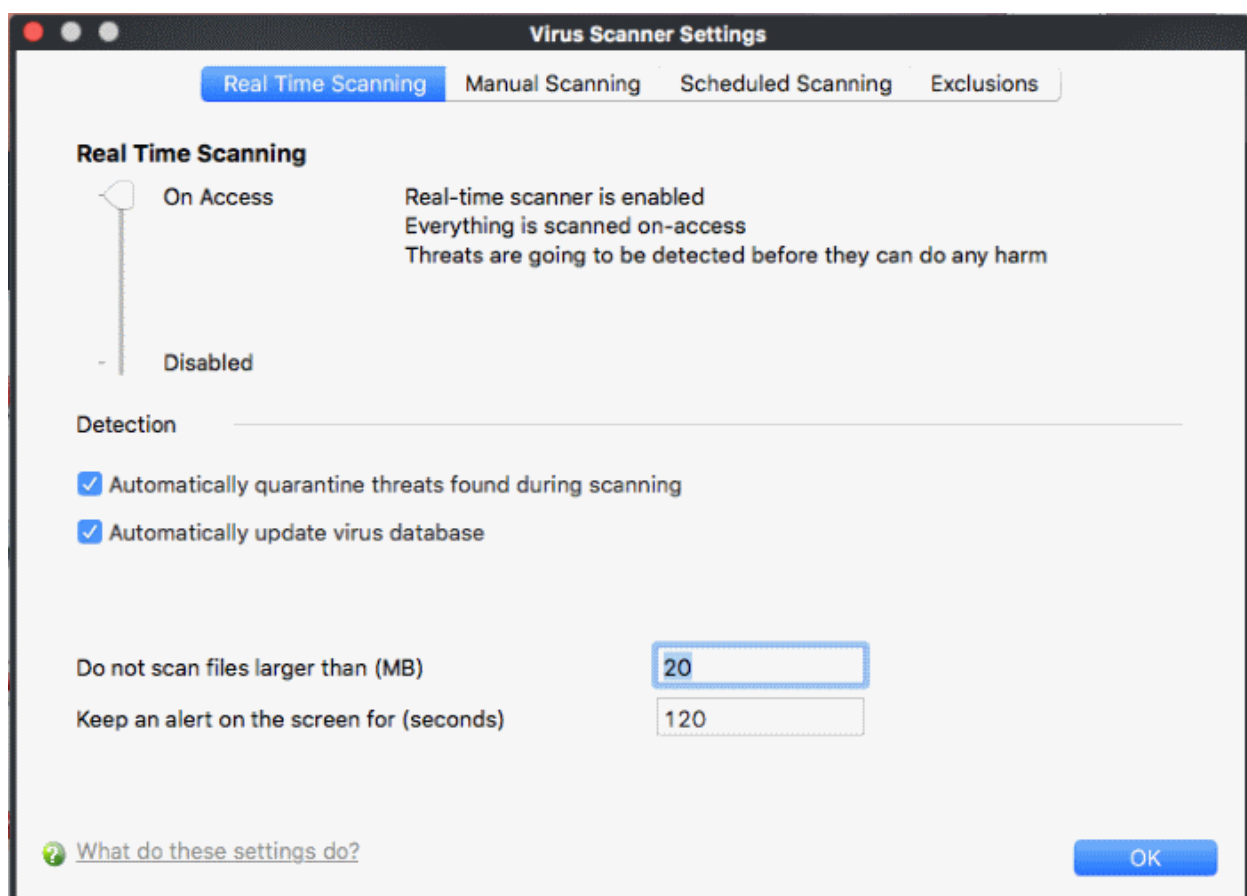
2.4. Scanner Settings

The 'Settings' configuration panel lets you customize various options related to the antivirus scanner.

- Setting changes for each scan type will apply to all future scans of that type.
- Items added to exclusions will be skipped by future scans of all types.

To open Virus Scanner Settings panel

- Click the 'Antivirus' tab on the home screen
- Click 'Scanner Settings' in the AV tasks scan
- You can now configure scanner settings:



The options that can be configured using the settings panel are

- **Real Time Scanning** - To set the parameters for on-access scanning;

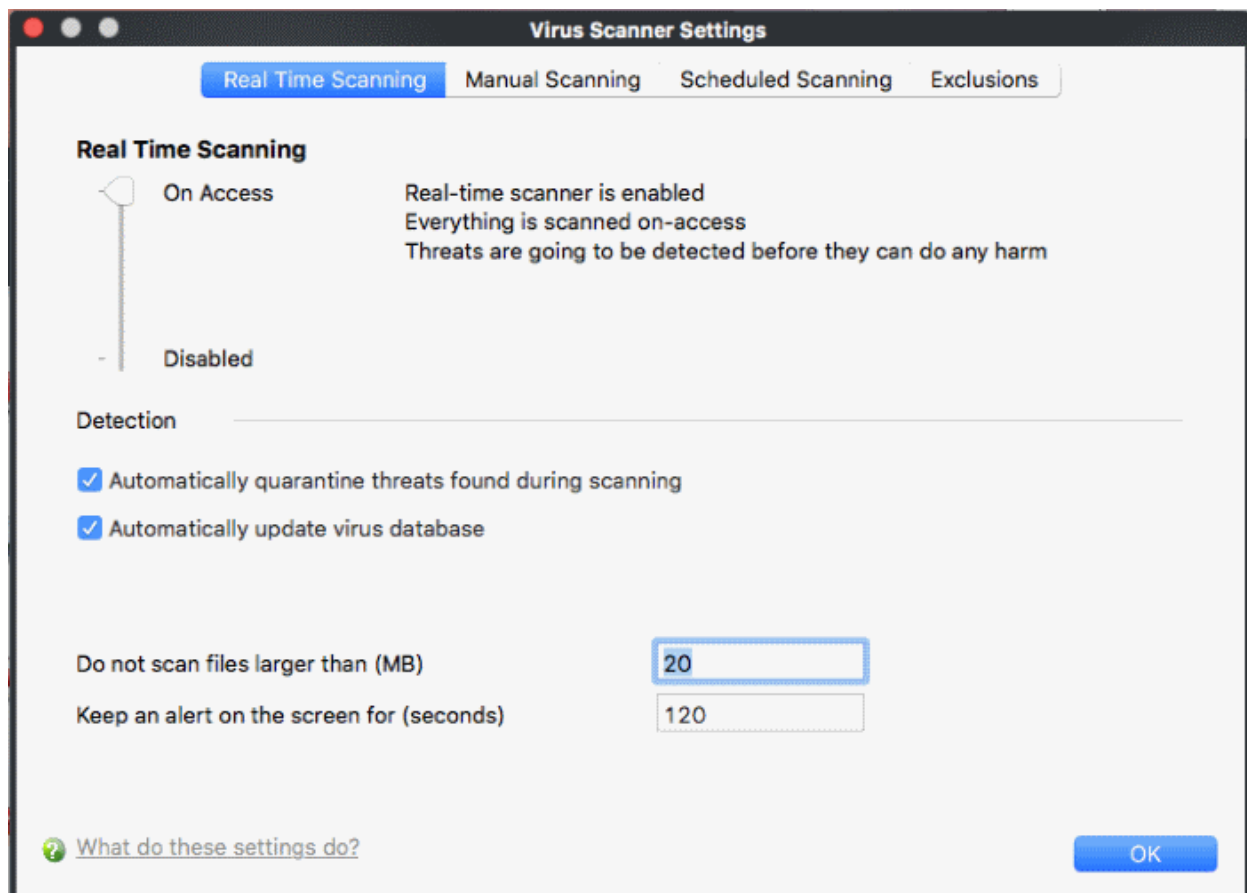
- **Manual Scanning** - To set the parameters for manual Scanning (Run a Scan);
- **Manual Scanning** - To set the parameters for scheduled scanning;
- **Exclusions** - To see the list of ignored threats and to set the parameters for Exclusions.

2.4.1. Real Time Scanning

- Click 'Antivirus' > 'Scanner Settings' to open this interface
- The real-time scanner constantly monitors your system for virus activity. The scanner is always ON and checks files when they are created, opened or copied.
- The settings area lets you:
 - Enable or disable the real-time scanner
 - Enable or disable automatic database updates
 - Enable or disable automatic quarantine of threats
 - Choose maximum file size which is scanned
 - Select how long an alert remains on-screen

Real Time Scanning level

- Drag the slider to the required level.
 - You can choose '**Disabled**' (not recommended) or '**On Access**'.
 - The setting you choose here is also shown on the home screen for easy reference.



- **On Access** – Files are scanned as soon as you, or any process, interacts with them. Virus protection is always running in the background and threats are detected before they get a chance to run.
- **Disabled** – Real-time protection is disabled, leaving your system highly vulnerable to infection.

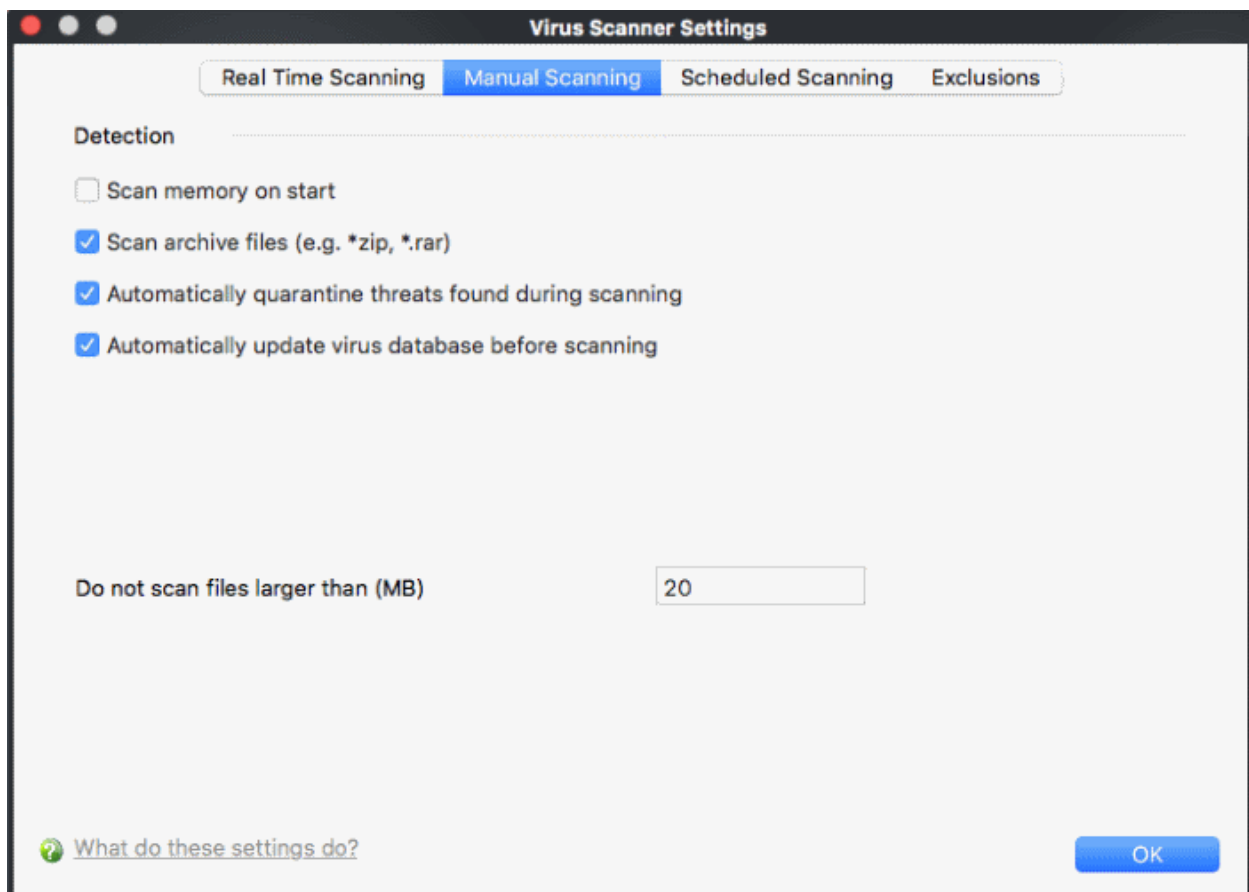
Detection Settings

- **Automatically quarantine threats found during scanning** – CAV will encrypt discovered threats and move them to a safe holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system. You can review quarantined files and permanently delete or restore them as required (**Default = Disabled**).
- **Automatically update virus database** - Comodo Antivirus will check for and download the latest virus database updates on system start-up and at regular intervals (**Default = Enabled**).
- **Do not scan files larger than** - Set the maximum size (in MB) that should be scanned by the on-access scanner. Files larger than the size specified here will not be scanned. (**Default = 20 MB**).
- **Keep an alert on the screen for** - Set the length of time that alerts should remain visible if the user does not manually dismiss them (**Default = 120 seconds**).

Click 'OK' for the settings to take effect.

2.4.2. Manual Scanning

- Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning' to open this interface
- A manual scan is one that you run on-demand on a drive, file/folder, or your entire computer.
- For example, these options will be used when you click 'Scan Now' on the home screen or 'Run A Scan' in the antivirus tasks menu.



- **Scan memory on start** – CAV will scans system memory (RAM) at the start of a manual scan (**Default = Disabled**).
- **Scan archive files** – CAV will scan compressed files such as .ZIP and .RAR files. (**Default = Enabled**)
- **Automatically quarantine threats found during scanning** – CAV will encrypt discovered threats and move them to a safe holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat

to your system. You can review quarantined files and permanently delete or restore them as required **(Default = Disabled)**.

- **Automatically update virus database** - Comodo Antivirus will check for and download the latest virus database updates on system start-up and at regular intervals **(Default = Enabled)**.

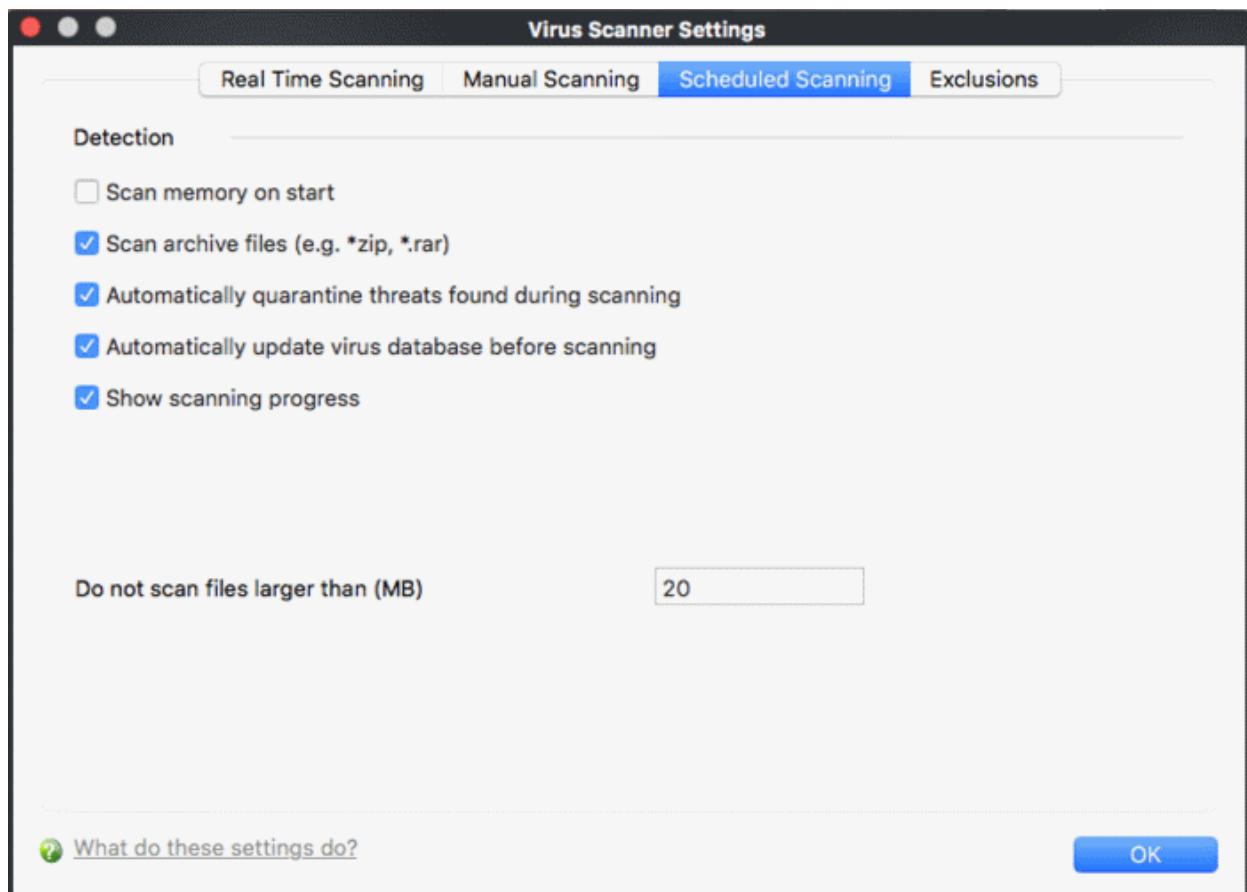
There are separate update options in for real time, manual and scheduled scanning settings. Disabling here will switch off auto - updates for this scan type only. Updates can be downloaded manually by clicking 'Antivirus' > 'Update Virus database'. See **'Update Virus Database'** for more details.

- **Do not scan files larger than** - Set the maximum size (in MB) that should be scanned by the on-access scanner. Files larger than the size specified here will not be scanned. **(Default = 20 MB)**.

Click 'OK' for the settings to take effect.

2.4.3. Scheduled Scanning

- Click 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning' to open this interface
- You can determine the scan parameters that will be implemented when a scheduled scan takes place.



You can choose to run scheduled scans at a certain time on a daily, weekly, monthly or custom interval basis. You can also choose which specific files, folders or drives are included in that scan by choosing the scan profiles.

The detection settings are as follows:

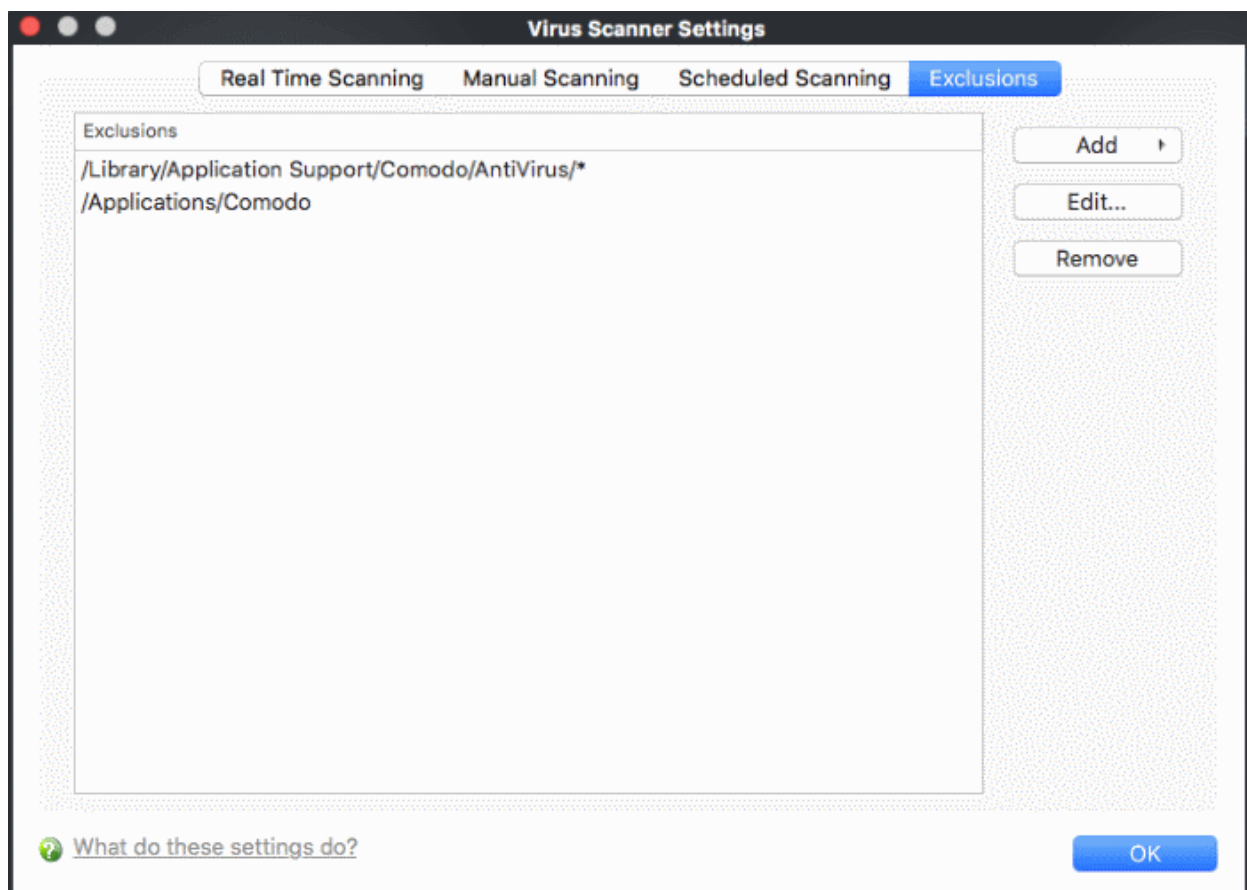
- **Scan memory on start** - When this check box is selected, the Antivirus scans system memory at the start of any scheduled scan **(Default = Disabled)**.
- **Scan archive files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files during any scheduled scan. You are alerted to the presence of viruses in compressed files before you even open them. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives **(Default = Enabled)**.

- **Automatically quarantine threats found during scanning** – CAV will encrypt discovered threats and move them to a safe holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system. You can review quarantined files and permanently delete or restore them as required (**Default = Disabled**).
- **Automatically update virus database** - Comodo Antivirus will check for and download the latest virus database updates on system start-up and at regular intervals (**Default = Enabled**).
- **Show Scanning progress** - When this check box is selected, a progress bar is displayed on start of a scheduled scan. Clear this box if you do not want to see the progress bar (**Default = Enabled**).
- **Do not scan files larger than** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during scheduled scanning. Files larger than the size specified here, are not scanned (**Default = 20 MB**).

Click 'OK' for the settings to take effect.

2.4.4. Exclusions

- Click 'Antivirus' > 'Scanner Settings' > 'Exclusion' to open this interface
- The 'Exclusions' tab in the Scanner Settings panel displays a list of applications/files for which you have selected 'Ignore' in the 'Scan Results' window of 'Run a Scan' option or added to 'Exclusions' from an Antivirus alert.



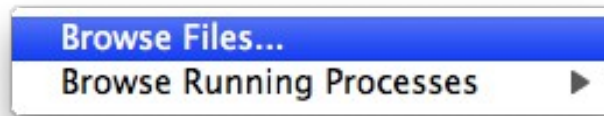
All items listed in the 'Exclusions' area are excluded from future scans of all types.

Also, you can manually define trusted files or applications to be excluded from a scan .

To define a file/application as excluded from scanning

1. Click 'Add'.

You now have 2 methods available to choose the application that you want to trust - '**Browse Files...**' and '**Browse Running Processes**'.



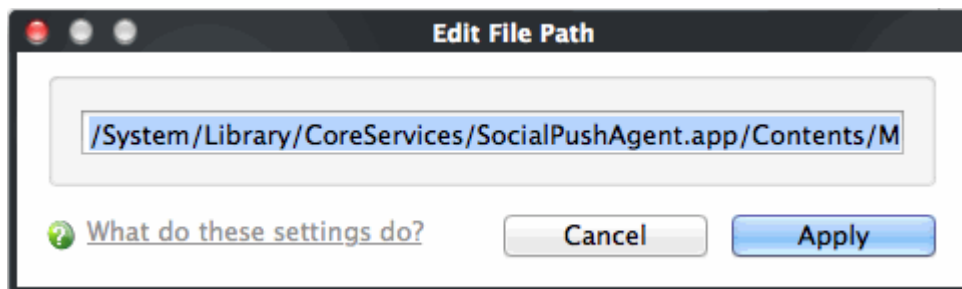
- **Browse Files...** - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.
- **Browse Running Processes** - As the name suggests, this option allows you to choose the target application from a list of processes that are currently running on your computer.

When you have chosen the application using one of the methods above, the application name appears along with its location.

2. Click 'OK' for the settings to take effect.

To edit the path (location) of an Excluded application

- Select the file or application for the list of excluded items
- Click 'Edit'
- Make the required changes for the file path in the 'Edit Property' dialog.

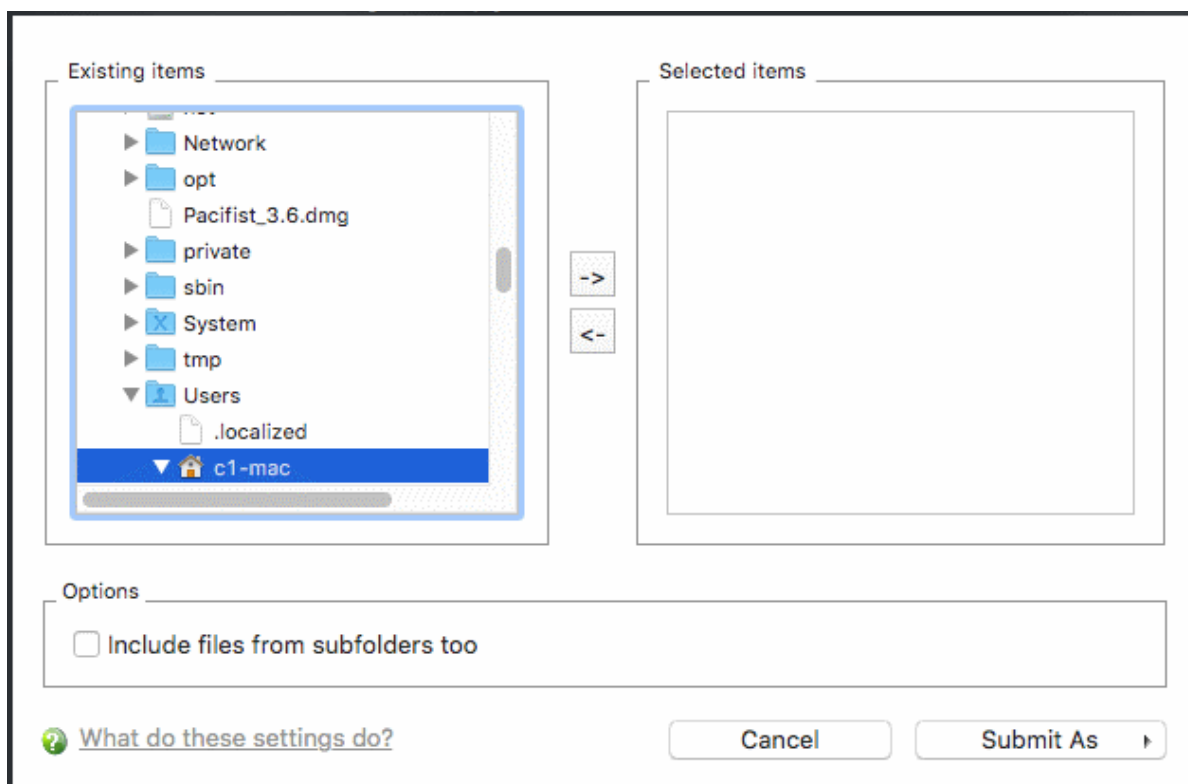


2.5. Submit Files to Comodo for Analysis

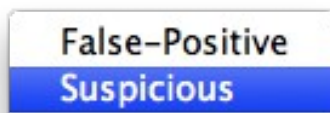
- Click 'Antivirus' > 'Submit Files' to open this interface
- You can submit files that have an 'Unknown' trust rating to Comodo for analysis. 'Unknown' files are those which are neither definitely safe (whitelisted), nor definitely malware (blacklisted).
- You can also submit false positives. These are files which you consider to be safe, but which CAV has quarantined.
- All submitted files are analyzed by Comodo experts and added to the whitelist or blacklist accordingly.

To submit files to Comodo

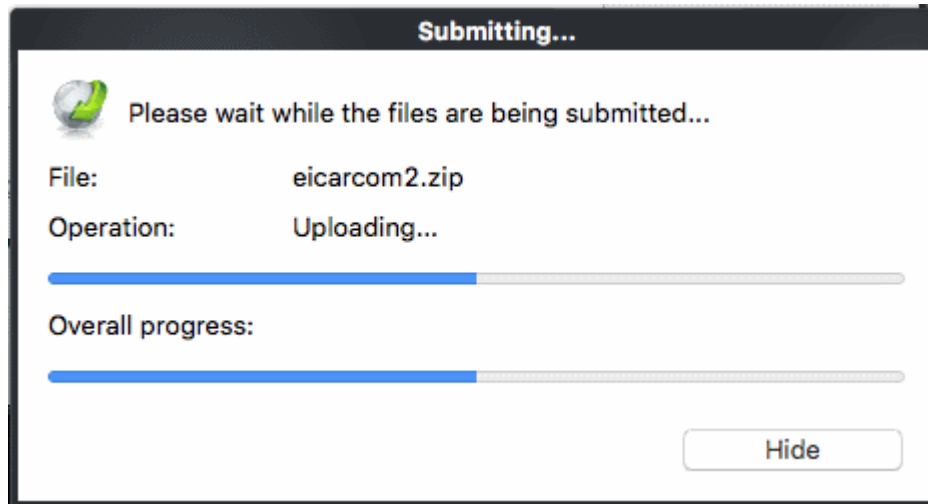
1. Click on the 'Submit Files' link in the main 'Antivirus Task Manager' screen. This will open the file selection screen:



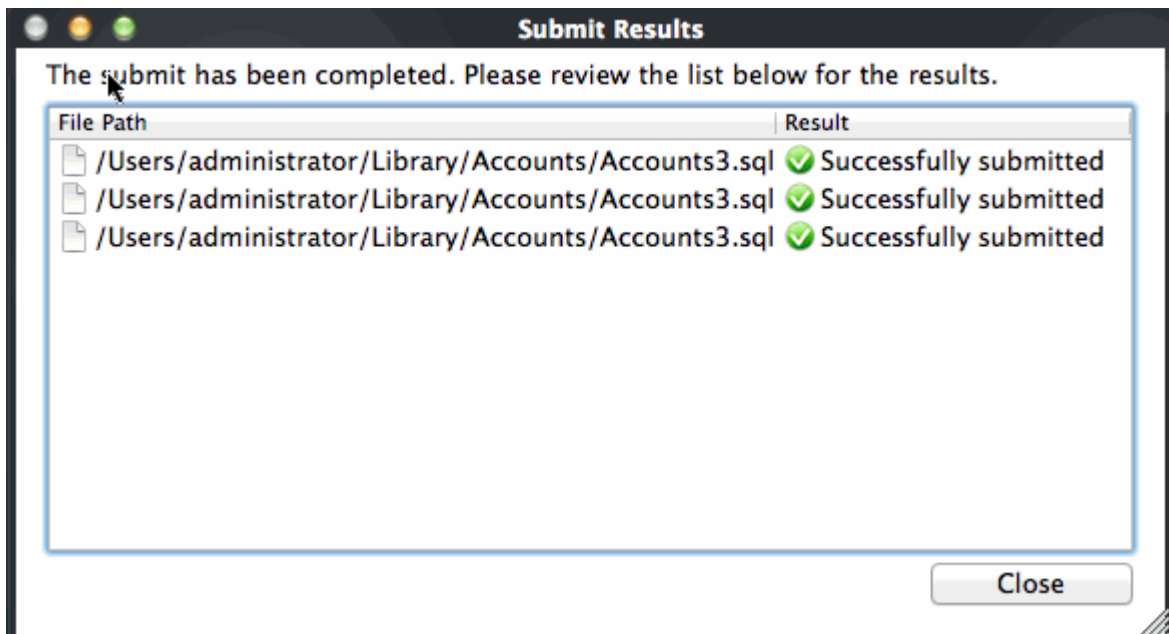
2. Select a file that you want to submit on the right. Click the → arrow to move it to the left pane.
3. Repeat the process to select more items.
4. Click 'Submit As' and select:
 - 'False-Positive' for files you consider to be safe
 - or
 - 'Suspicious' for files you suspect to be malware



Progress bars indicate the progress of the files submission to Comodo.



When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen displays these results:



- 'Successfully submitted' - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- 'Already submitted' - The file has *already* been submitted to our labs by another Antivirus user and was not uploaded from your machine at this time.

Comodo will analyze *all* submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

2.6. Scheduled Scans

- Click 'Antivirus' > 'Scheduled Scans' to open this interface
- Comodo Antivirus features a highly customizable scheduler that lets you timetable scans according to your preferences.
- Comodo Antivirus automatically starts scanning the entire system or the disks or folders contained in the profile selected for that scan.

- You can add an unlimited number of scheduled scans to run at a time that suits your preference. A scheduled scan may contain any profile of your choice.
- You can choose to run scans at a certain time on a daily, weekly, monthly or custom interval basis.
- You can also choose which specific files, folders or drives are included in that scan.
- Comodo Antivirus gives you the power to choose, allowing you to get on with more important matters with complete peace of mind.

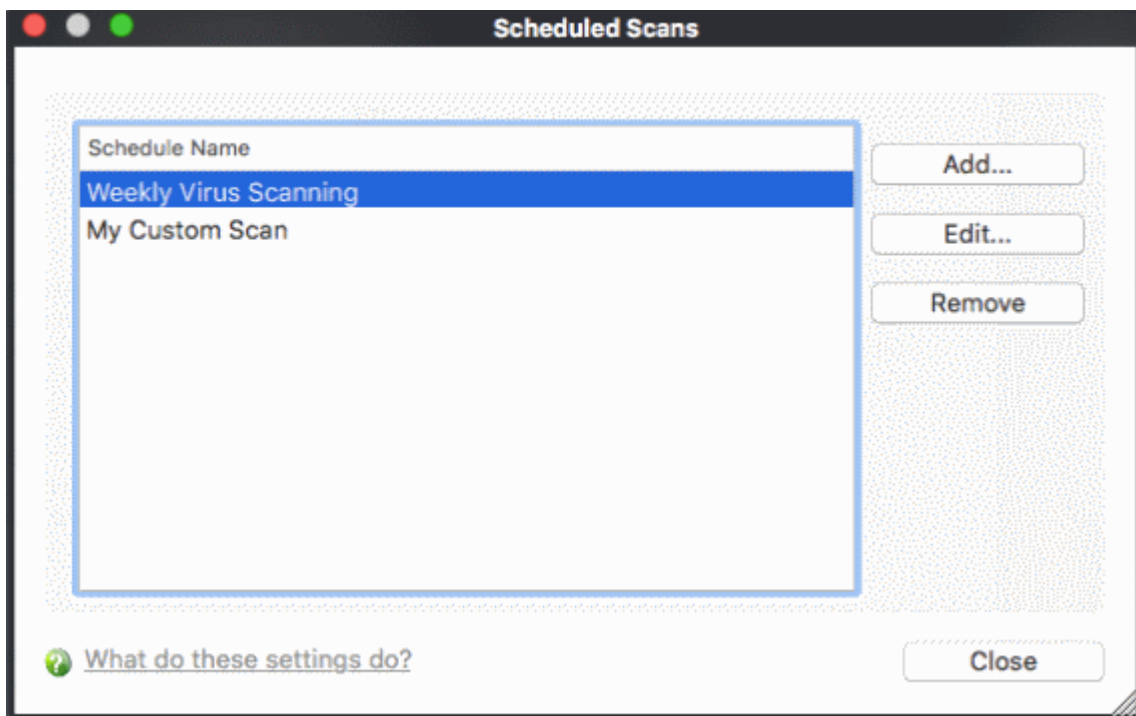
From the 'Scheduled Scans' panel, you can

- **Set a new scheduled scan**
- **Edit a pre-scheduled scan**
- **Cancel a pre-scheduled scan**

The detection settings for the 'Scheduled Scans' can be configured under the '**Scheduled Scanning**' tab of the '**Scanner Settings**' interface.

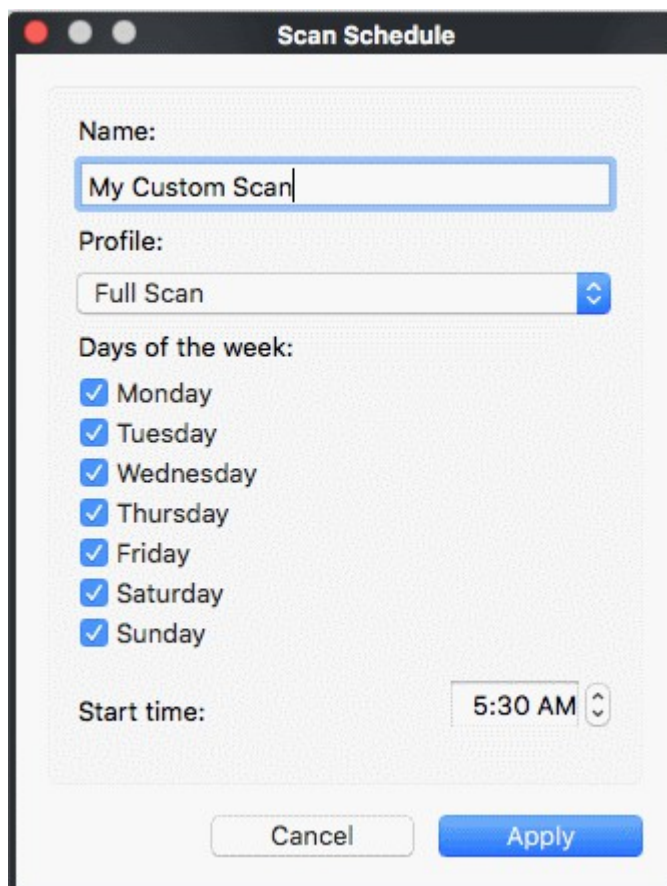
To set a Scheduled Scan

1. Click on the 'Scheduled Scans' link in the main 'Antivirus Task Manager' screen.

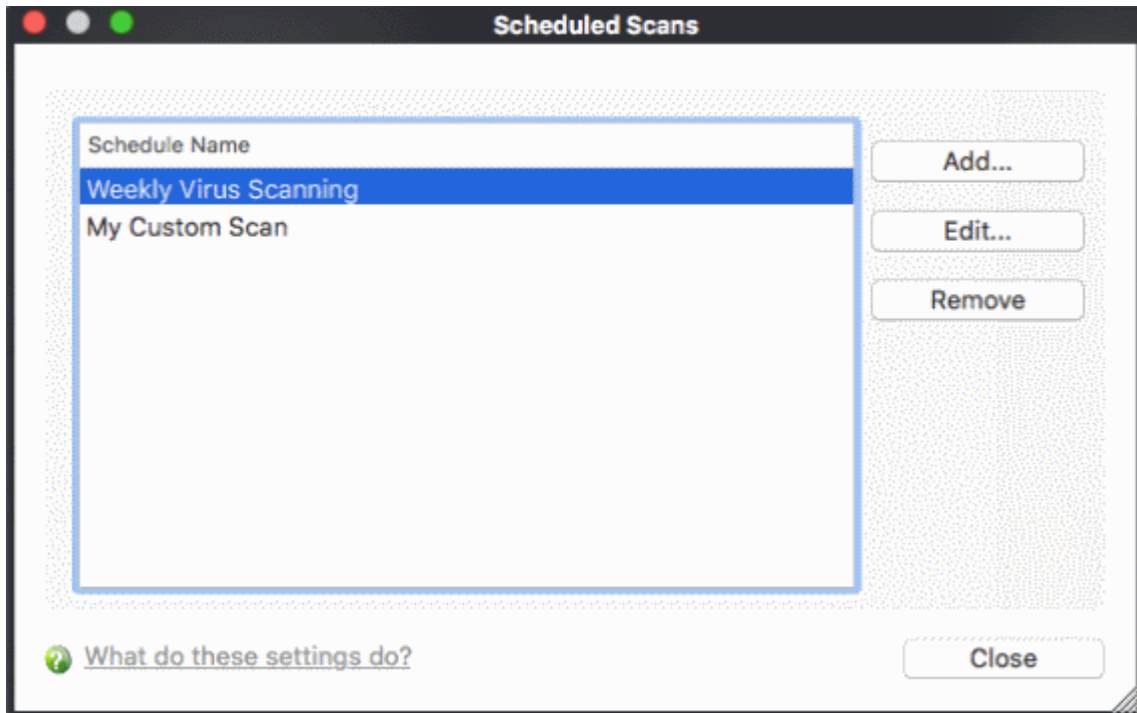


A default schedule 'Weekly Virus Scanning' is displayed. This schedule is set so that your computer is scanned on every day at 16:00pm. You can edit this schedule by selecting it and clicking the 'Edit' button.

2. Click 'Add'. The 'Scan Schedule' panel opens.



3. Type a name for the newly scheduled scan in the 'Name:' box.
4. Select a scanning profile from the list of preset scanning profiles by clicking at the drop-down arrow, in the 'Profile' box. (For more details on creating a custom 'Scan Profile' that can be selected in a scheduled scan, see ['Antivirus Tasks' > 'Scan Profiles'](#)).
5. Select the days of the week you wish to schedule the scanning from 'Days of the Week' check boxes.
6. Set the starting time for the scan in the selected days in the 'Start time' drop-down boxes.
7. Click 'Apply'.



- Repeat the process to schedule other scans with other predefined scan profiles.

To 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'.

To cancel a pre-scheduled scan

- Select the scan schedule you wish to cancel in the 'Scheduled Scans' settings panel.
- Click 'Remove'.

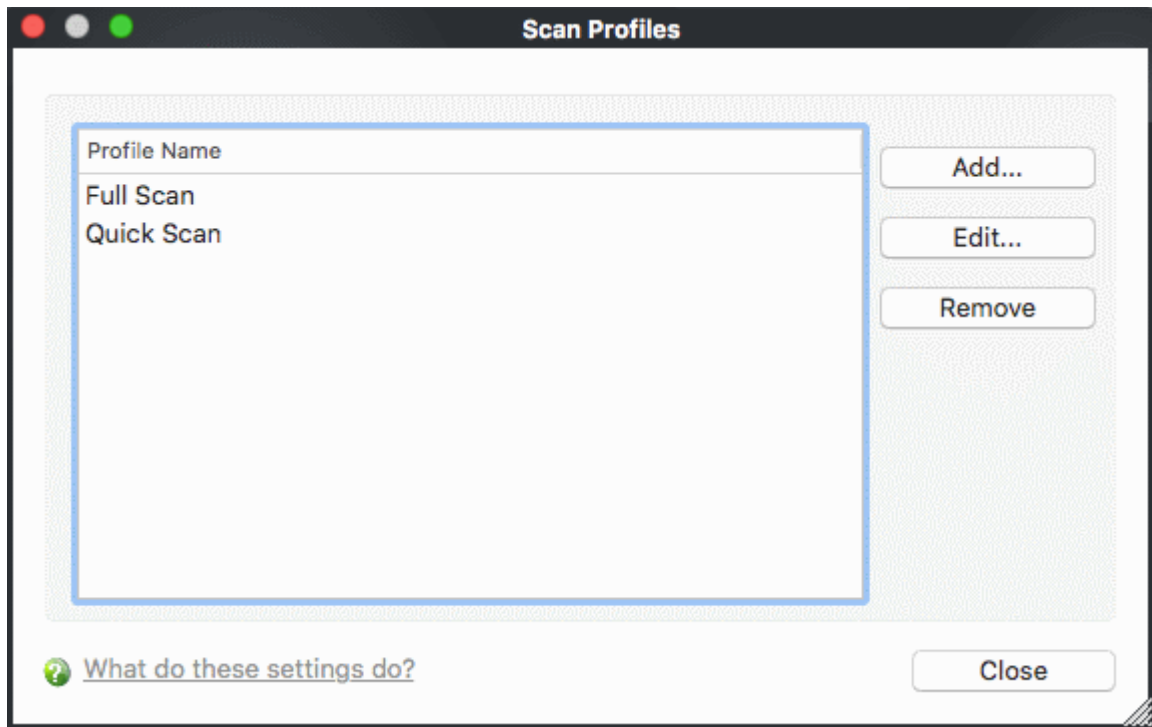
2.7. Scan Profiles

- Click 'Antivirus' > 'Scan Profiles' to open this interface
- A profile instructs Comodo Antivirus to scan specific areas, folders or drives on your system.
- Comodo ships with two profiles by default – 'Full Scan' and 'Quick Scan'.
- You can also create custom profiles which target areas you select.
- You can then select the profile when running an on-demand scan.
- You can also add the profile to a scheduled scan.

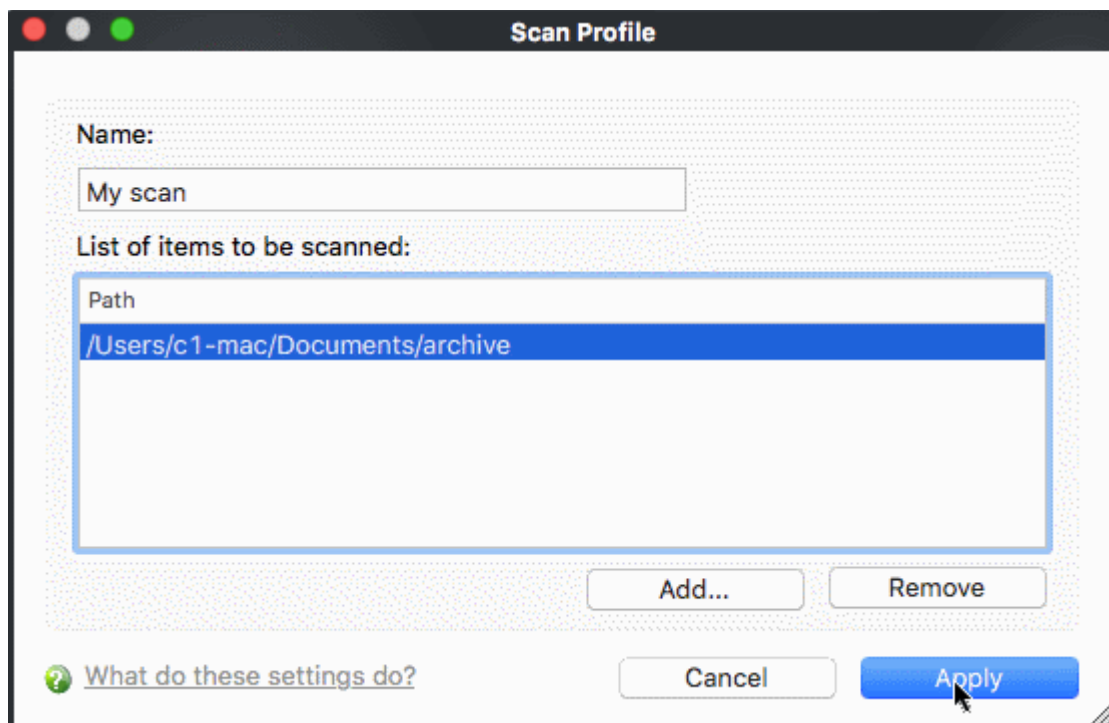
Note - Scan profiles are purely concerned with scan locations, not the parameters of the scan. All scan profiles use the settings in the '**Scanner Settings**' tab of that type of scan.

To create a new scan profile:

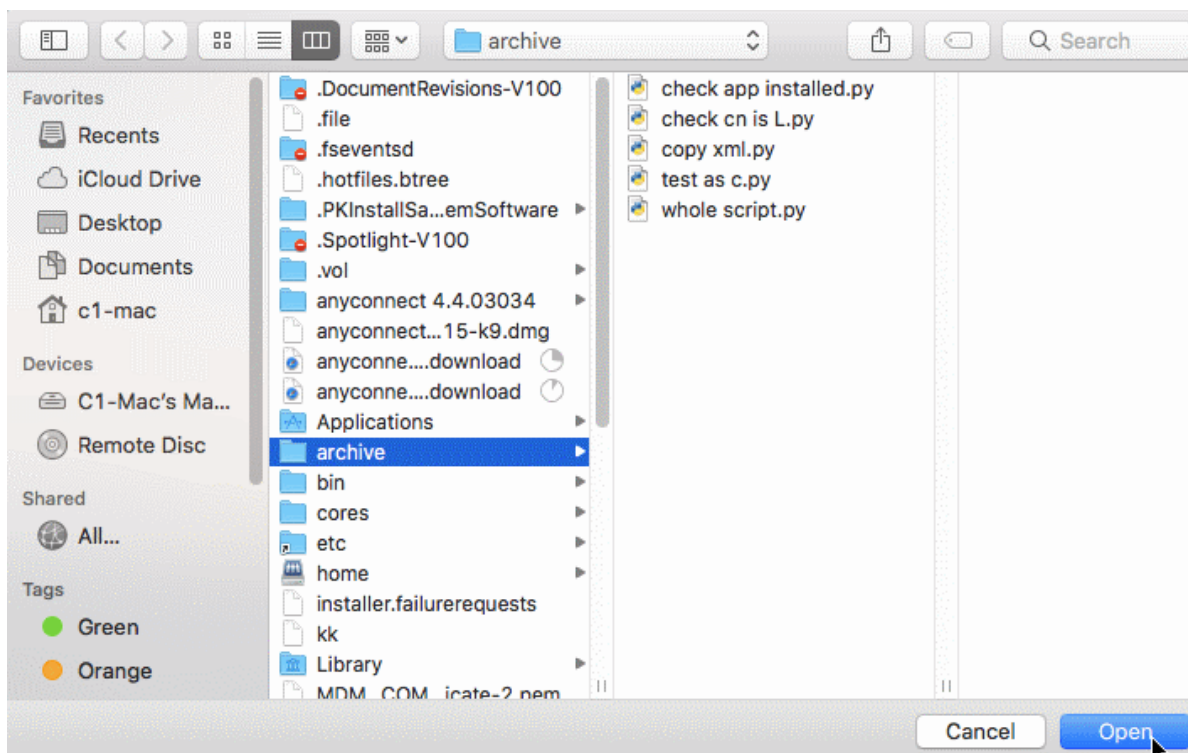
- Open the Comodo Antivirus home screen
- Click 'Antivirus' > 'Scan Profiles'
- Click 'Add...' to open the profile configuration screen



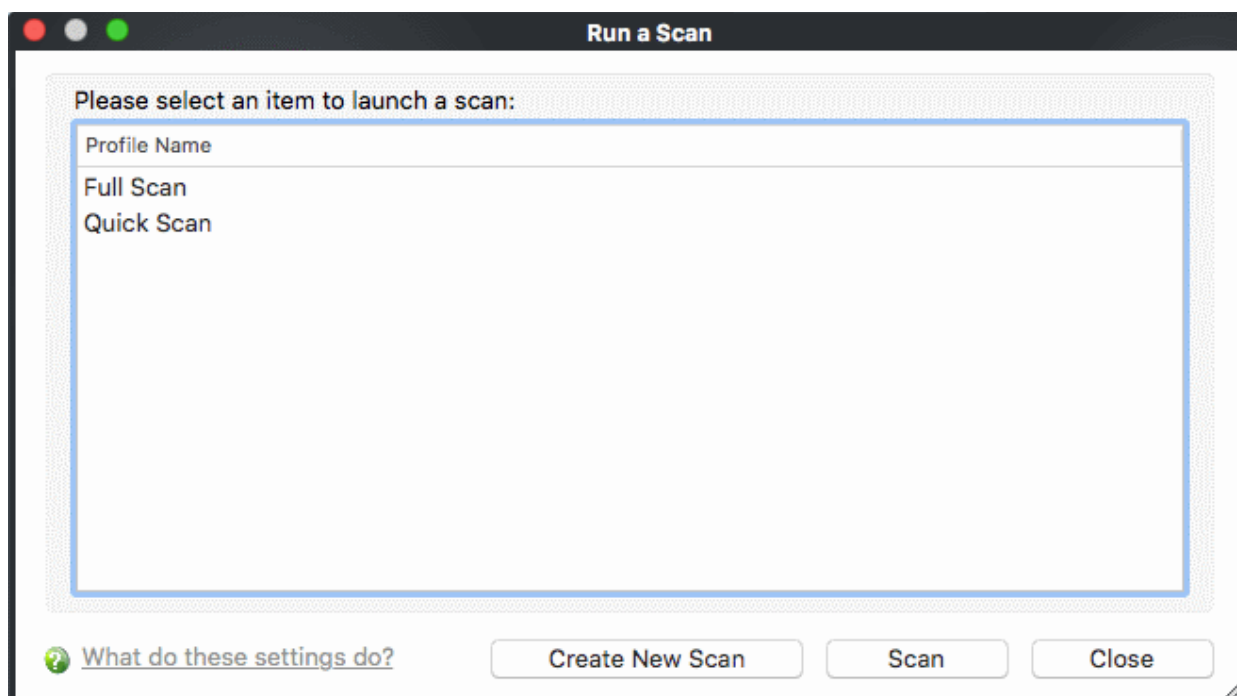
- Type a name for the profile
- Click 'Add' to select the files/ folders/ drives you wish to include in the profile:



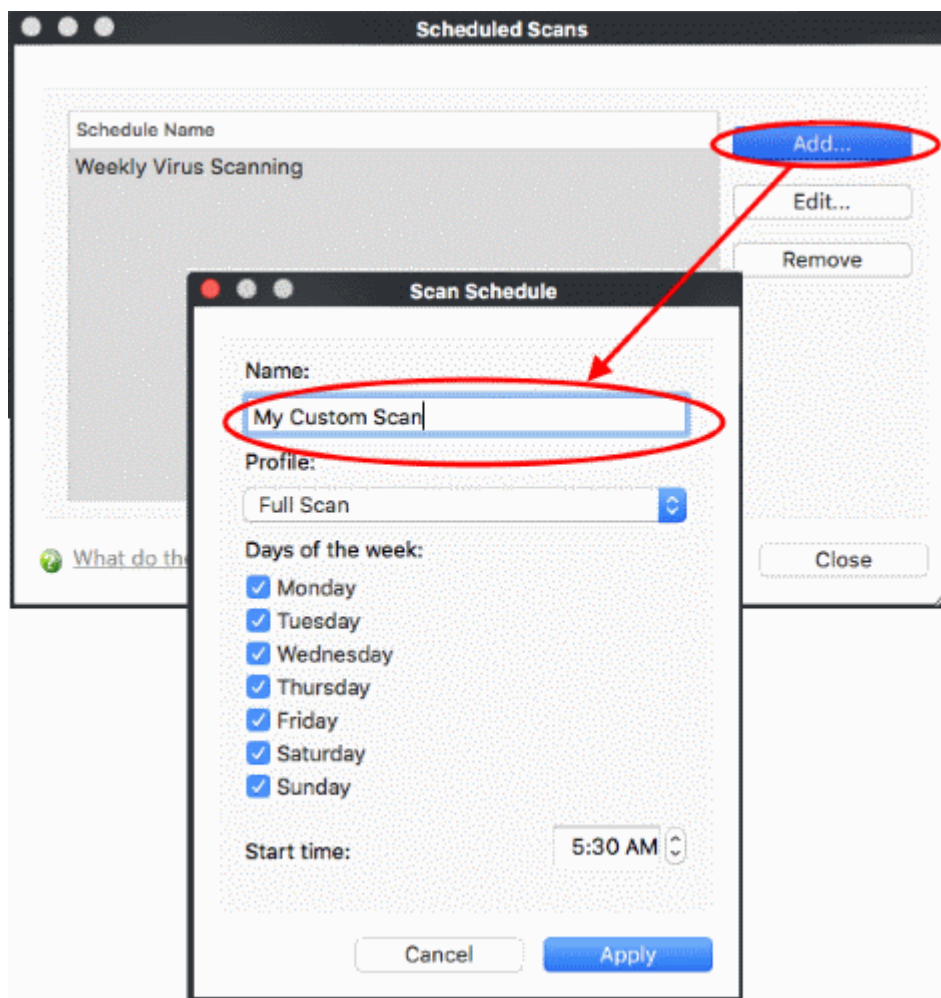
- Drag and drop the items you want from the left pane into the right pane:



- Click 'Apply' to save the profile.
- Repeat the process to create more profiles
- The profile will appear in the 'Run a Scan' panel ...



- ...and the scheduled scan 'Profile' drop-down:

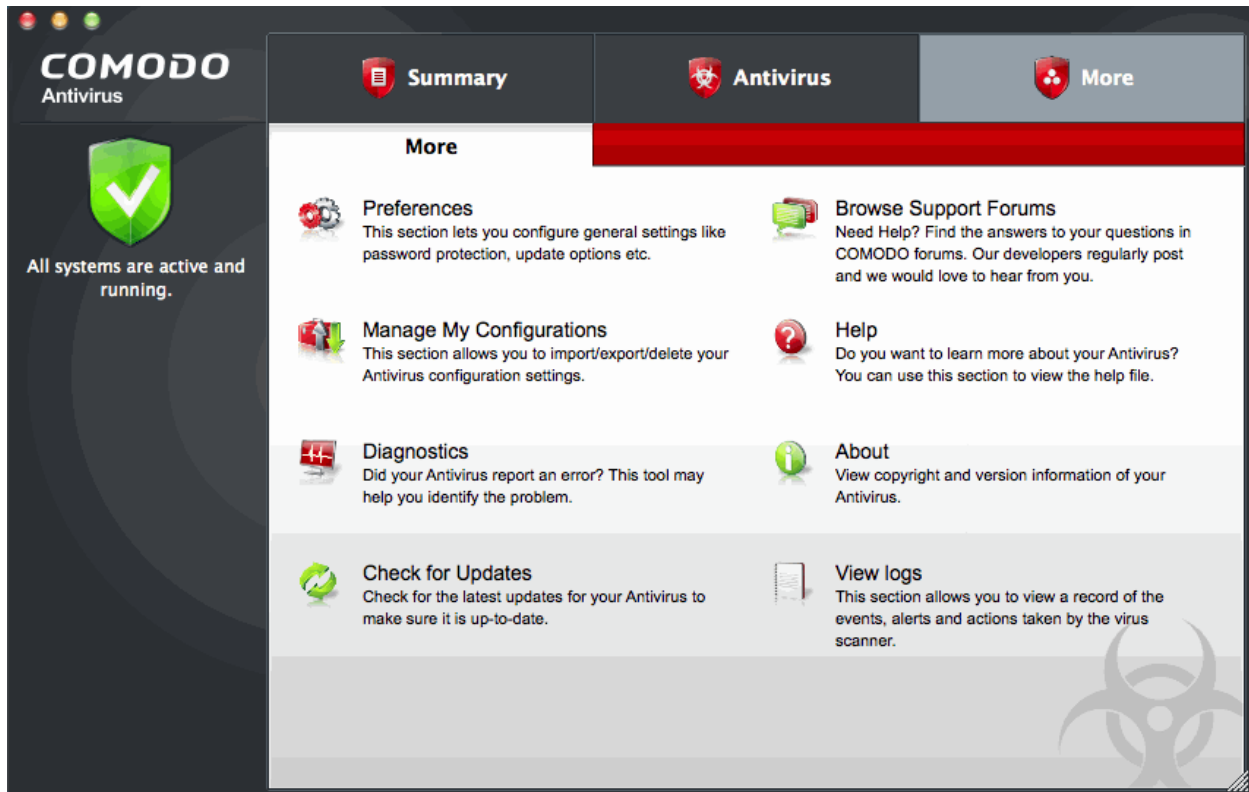


- To edit a 'Scan Profile', select the profile and click 'Edit'.
- To delete a 'Scan Profile', select the profile and click 'Remove'.

3. More Options-Introduction

The 'More Options' area allows you to view and modify various program settings and also contains additional utilities you may enjoy.

- Click 'More' in the navigation panel to access these options:

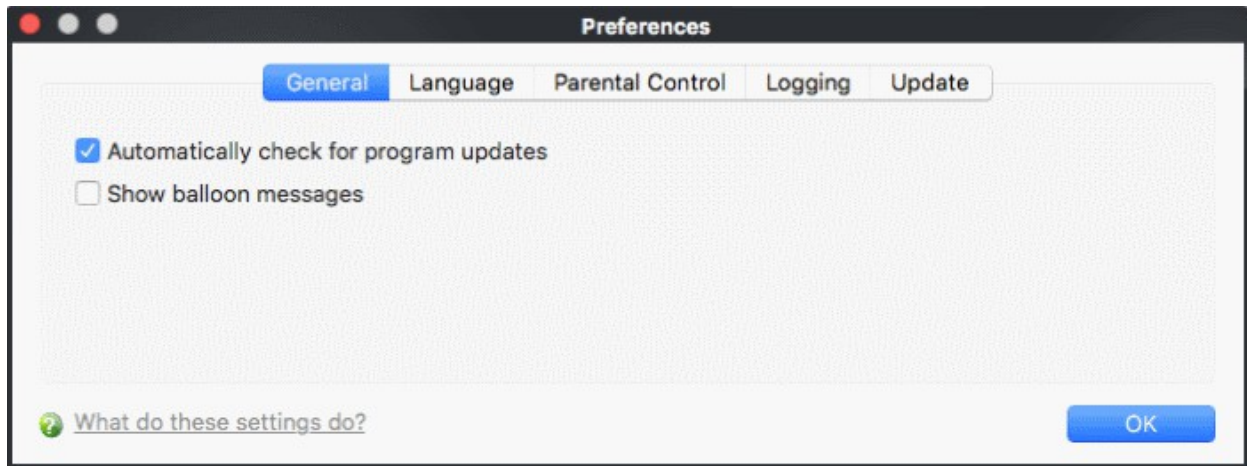


Click the links below to see detailed explanations of each area in this section.

- **Preferences:** Allows the user to configure general Comodo Antivirus settings (password protection, update options, language)
- **Manage My Configurations:** Allows the user to manage, import and export their Comodo Antivirus configuration profile.
- **Diagnostics:** Helps to identify any problems with your installation.
- **Check For Updates:** Launches the Comodo Antivirus updater.
- **Browse Support Forums:** Links to Comodo User Forums.
- **Help:** Launches the online help guide.
- **About:** Displays version and copy-right information about the product.
- **View Logs:** Contains a log of events.

3.1. Preferences

- Click 'More' in the CAV home screen
- Click 'Preferences' in the 'More' interface
- Click 'General' in 'Preferences' interface
- The '**Preferences**' menu lets you configure various options related to the operation of Comodo Antivirus.



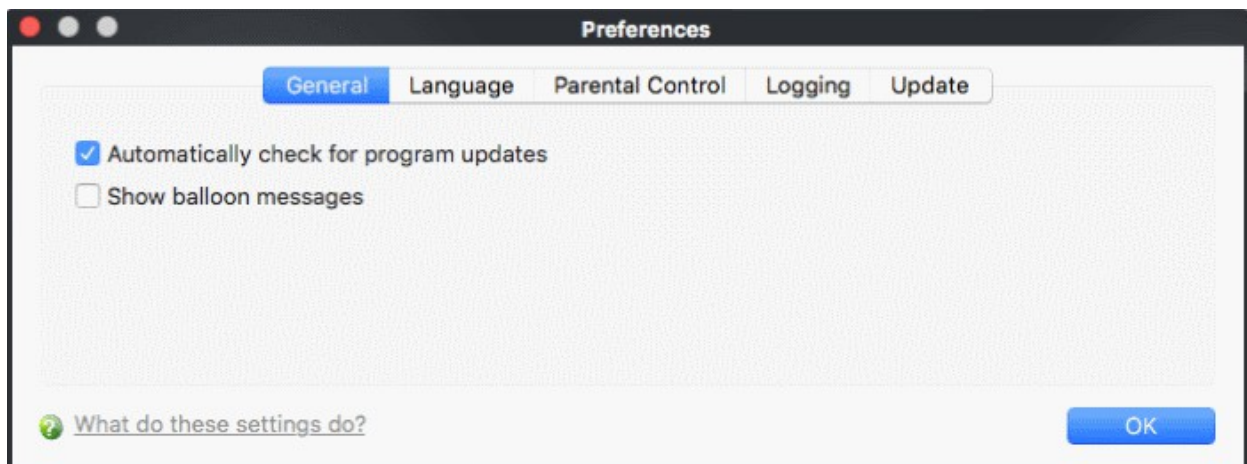
To open Preferences

- Click 'More' then 'Preferences'

The preferences dialog contains the following areas:

- **General**
- **Language**
- **Parental Control**
- **Logging**
- **Update**

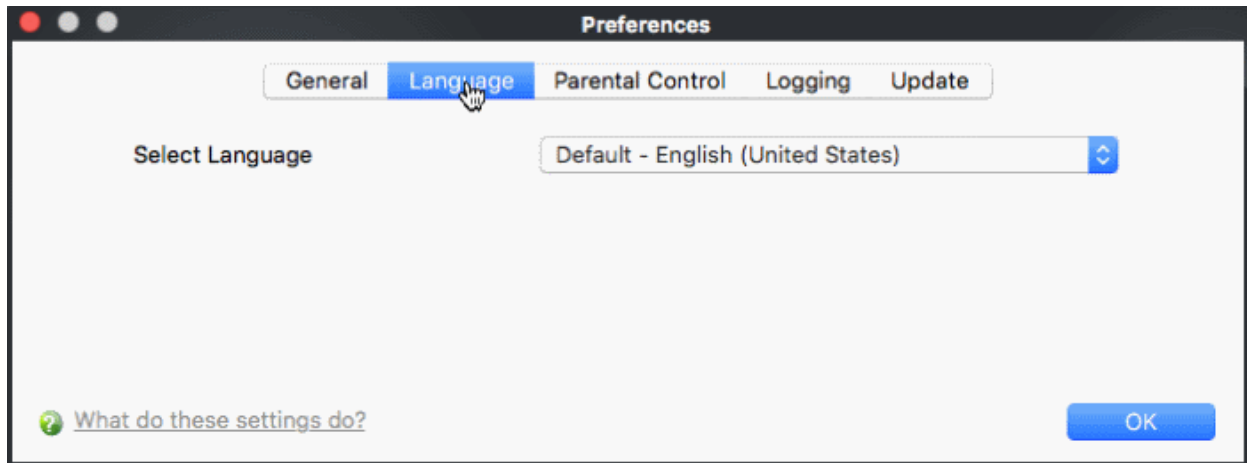
3.1.1. General Settings



- **Automatically check for the program updates** - This option determines whether or not Comodo Antivirus should automatically contact Comodo servers for updates. With this option selected, Comodo Antivirus automatically checks for updates every 24 hours AND every time you start your computer. If updates are found, they are automatically downloaded and installed. We recommend that users leave this setting enabled to maintain the highest levels of protection. Users who choose to disable automatic updates can download them manually by clicking '**Check for Updates**' in the 'More...' section (**Default = Enabled**).
- **Show the balloon messages** - These are the notifications that appear in the bottom right hand corner of your screen - just above the tray icons. Usually these messages like '*Comodo Antivirus is learning*' and are generated when these modules are learning the activity of previously unknown components of trusted applications. Clear this check box if you do not want to see these messages (**Default = Disabled**).

3.1.2. Language

- Click 'More' in the CAV home screen
- Click 'Preferences' in the 'More' interface
- Click 'Language' in 'Preferences' interface
- The '**Language**' tab allows you to choose the interface language of Comodo Antivirus

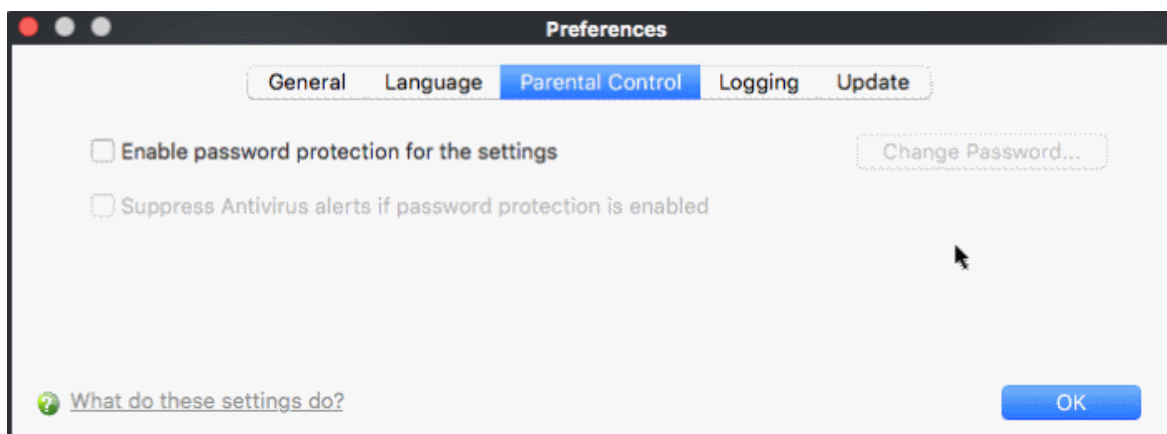


Comodo Antivirus is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (**Default = English (United States)**).

In order for your language to take effect, you must restart the application.

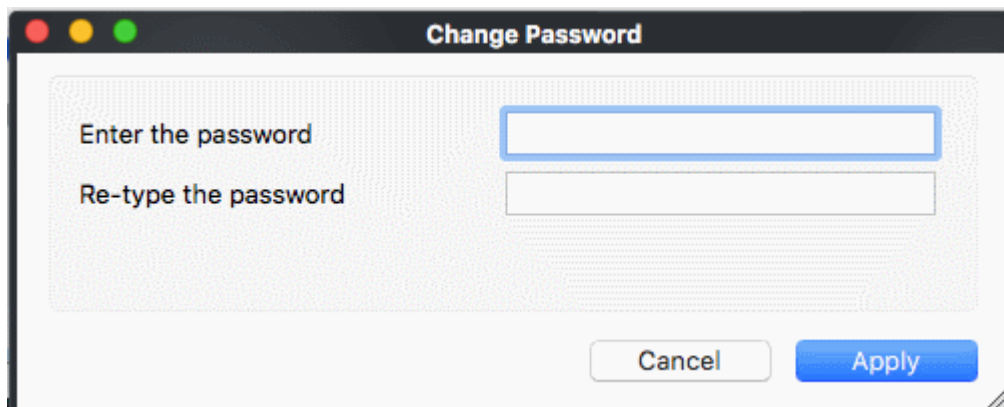
3.1.3. Parental Control Settings

- Click 'More' in the CAV home screen
- Click 'Preferences' in the 'More' interface
- Click 'Parental Control' in 'Preferences' interface
- The '**Parental Control**' tab allows you to configure password protection for Comodo Antivirus.



- **Enable password protection for settings** - Selecting this option activates password protection for all important configuration sections and wizards within the interface.
 - If you choose this option, you must first specify and confirm a password by clicking the 'Change Password...' button.
 - You are asked for this password every time you try to access important configuration areas (**Antivirus**

Tasks areas require this password before allowing you to view or modify their settings).

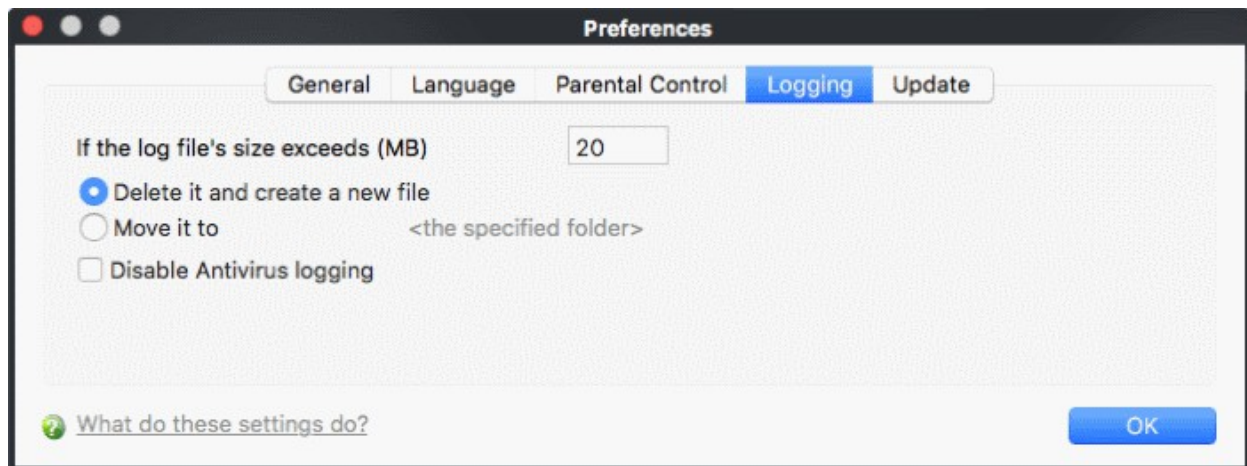


This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and possibly exposing the machine to threats (**Default = Disabled**).

- **Suppress Antivirus alerts when password protection is enabled** - If selected, any detected threats will be automatically blocked but no Antivirus Alerts will be displayed.
 - **Password protection** needs to be enabled for this option to become available.
 - Parents and network administrators may want to enable this setting if they do not want users to be made aware when an Antivirus alert has been triggered.
 - For example, a virus program may be attempting to copy itself and infect user's computer without permission or knowledge of the user.
 - Usually, Comodo Antivirus would generate an alert and ask the user how to proceed.
 - If that user is a child or an inexperienced user then they may unwittingly click 'allow' just to 'get rid' of the alert and/or gain access to the website in question - thus exposing the machine to attack. (**Default = Disabled**).

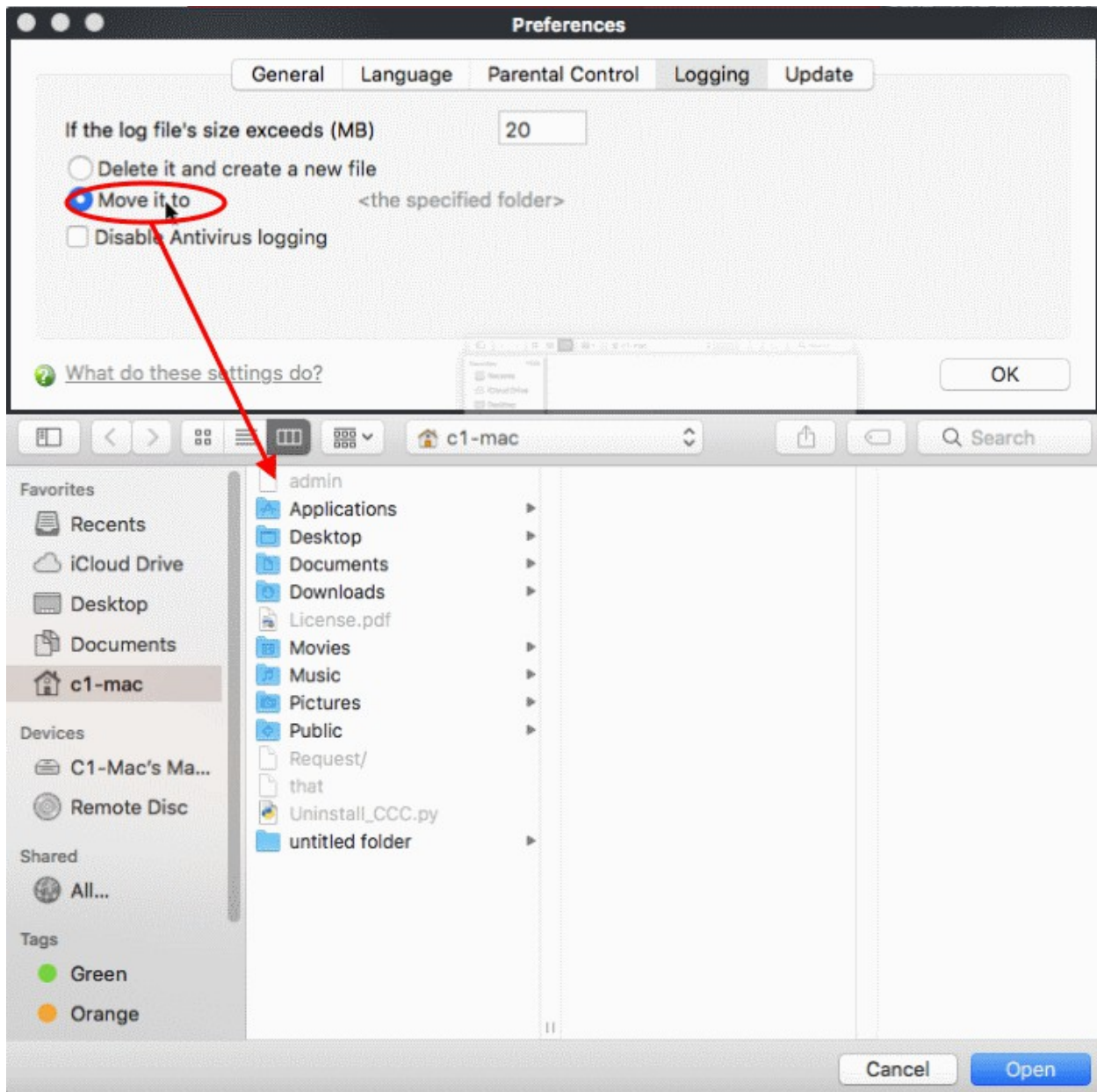
3.1.4. Log Settings

- Click 'More' in the CAV home screen
- Click 'Preferences' in the 'More' interface
- Click 'Parental Control' in 'Preferences' interface
- By default, Comodo Antivirus maintains a log of all events, which can be accessed by clicking **View Antivirus Events** from the 'Antivirus' tasks interface.
- The 'Logging' tab of the 'Preferences' interface allows you to configure how CAV should behave once this log file reaches a certain size and also allows you to disable the logging of specific types of event.
- This 'Logging' interface allows you to specify whether you want to enable logging; the maximum size of the log file and how CAV should react if the maximum file size is exceeded.
- Note: If you wish to actually view, manage logs, then you need to open the **'View Logs'** interface under 'More' in the Antivirus Events interfaces.

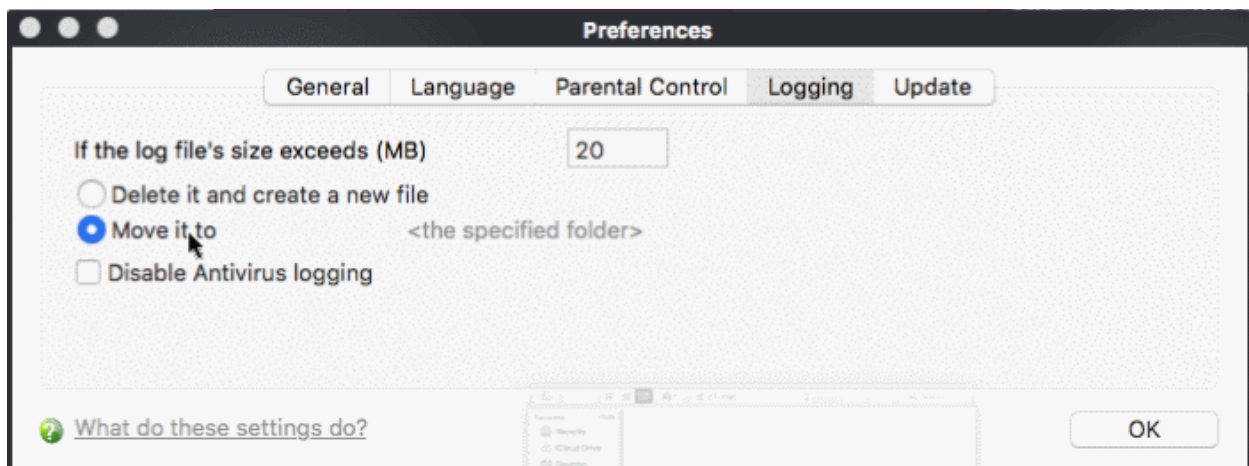


Log File Management

- **If the log file's size exceeds (MB):**
 - Enables you to configure for deleting or moving the log file if it reaches a specified size in MB.
 - You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
 - Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' (**Default = 20MB**).
 - If you want to discard the log file if it reaches the maximum size, select '**Delete it and create a new file**'.
 - Once the log file reaches the maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant (**Default = Enabled**).
- If you want to save the log file even if it reaches the maximum size, select '**Move it to**' and select a destination folder for the log file (**Default = Disabled**).



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



Once the log file reaches the maximum size, it will be automatically moved to the selected folder and a new log file will be created with the log of events occurring from that instant.

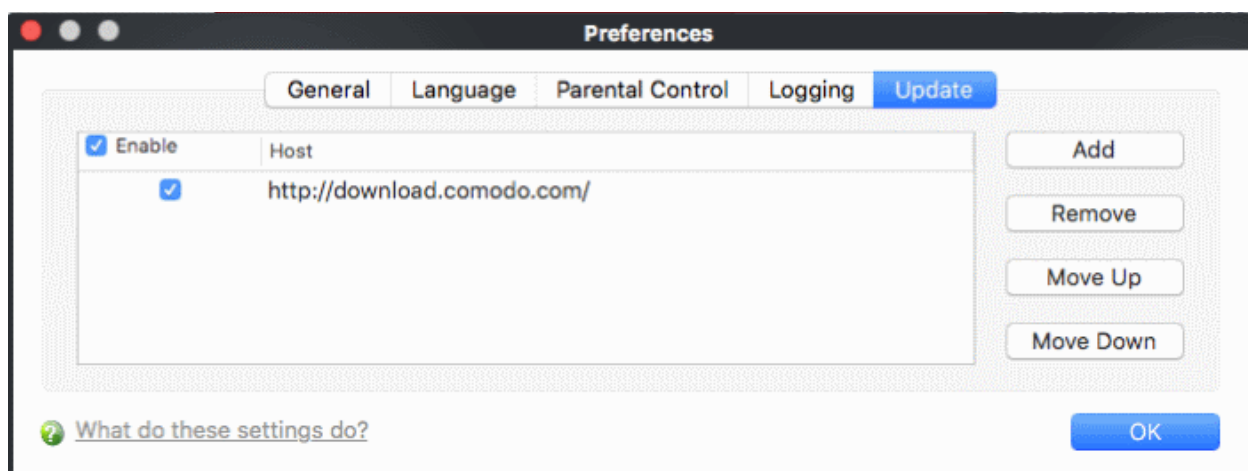
Check Boxes:

The check boxes allow you to disable logging of events according to your preferences.

- **Disable Antivirus logging** – Instructs Comodo Antivirus to not to log Antivirus events (**Default = Disabled**).

3.1.5. Update Settings

- Click 'More' in the CAV home screen
- Click 'Preferences' in the 'More' interface
- Click 'Parental Control' in 'Preferences' interface
- The '**Update**' tab allows you enable/disable CAV program updates and to select the host from which the updates are to be downloaded.
- By default, updates are downloaded from <http://download.comodo.com>



- Leave this setting alone if you always want to download the updates from Comodo servers
- You can add the URL of an alternative download host if required. For example, if CAV updates are available on a server on your local network which is running Comodo Offline Updater.
 - To add a host, click 'Add' and enter the URL or IP address of the host in the next row that appears.
 - Repeat the process for adding multiple hosts.
 - Select the host by using the Move Up and Move Down buttons.
 - CAV will automatically check the host specified here and download the updates from the host even when you are offline.
- Click 'OK' for your settings to take effect.

Note: CAV program updates can also be checked manually. Click 'More Options' > 'Check For Updates' if you wish to update manually. [Click here](#) to view the help page on manual updates.

3.2. Manage My Configurations

- Click 'More' > 'Manage My Configurations' to open this interface.
- Comodo Antivirus allows you to maintain, save and export multiple configurations of your security settings.
- This is especially useful if you are a network administrator looking to roll out a standard security configuration to multiple computers.
- If you are upgrading your system, and have to uninstall Comodo Antivirus, you can export your

configuration settings to a safe place. After re-installing, you can import your old settings.

- This feature is also a great time saver for anyone with more than one computer. You can quickly implement your current security settings on another computer without having to manually configure them.
 - **Comodo Preset Configurations**
 - **Importing/Exporting and Managing Personal Configurations**

3.2.1. Comodo Preset Configurations

- Click 'More' on the CAV home screen
- Click 'Manage My Configurations'

Comodo Antivirus ships with preset configurations that strike a good balance between security and usability.

- The profile that is currently in use is the 'Active' profile.
- Any changes you make to settings over time are saved in the 'active' profile.
- Exporting the active profile will, therefore, export your settings as they currently stand.

Before modification, the '**Comodo Antivirus for MAC**' profile has the following default settings:

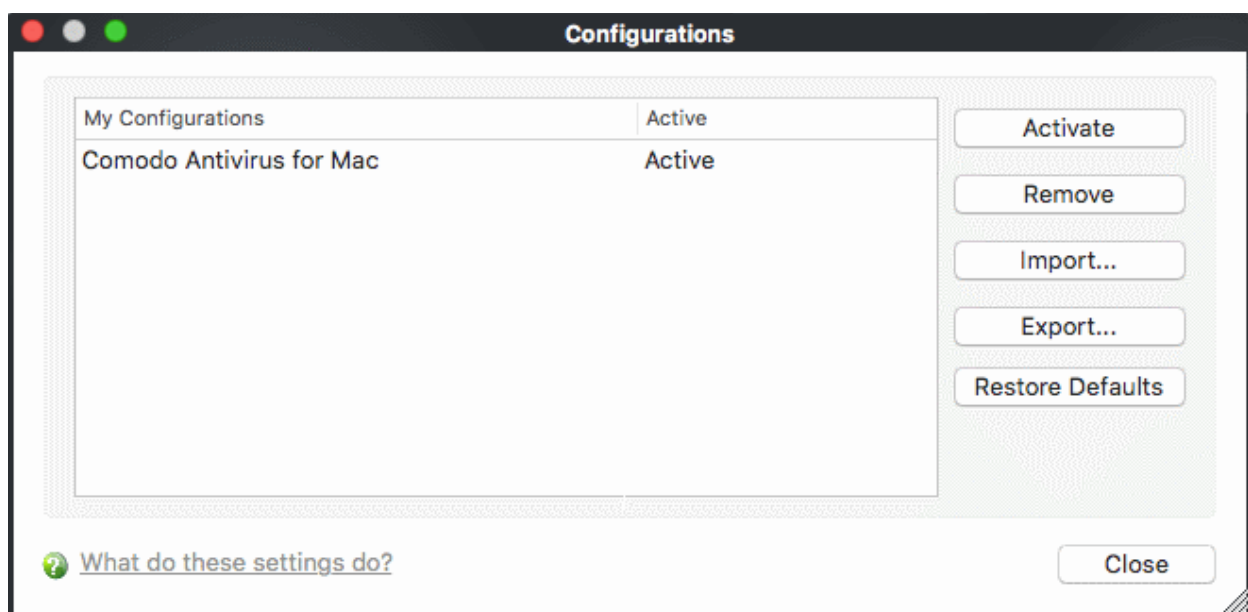
- Automatic Program Updates - ON
- Automatic Virus Updates - ON
- not scan files larger than - 20 MB (all scanner types)
- Real Time Scanning – On Access

Over time, you may have made changes that have altered this profile. If you want to restore the settings above, then click 'Restore Defaults'.

You can switch to a preset configuration in the 'Configurations' interface.

3.2.2. Importing/Exporting And Managing Personal Configurations

- Click 'More' in the CAV home screen
- Click 'Manage My Configurations'



- The interface has one preset configuration by default - 'Comodo Antivirus for MAC'.

- The configuration that CCAV is currently using is marked 'Active'.

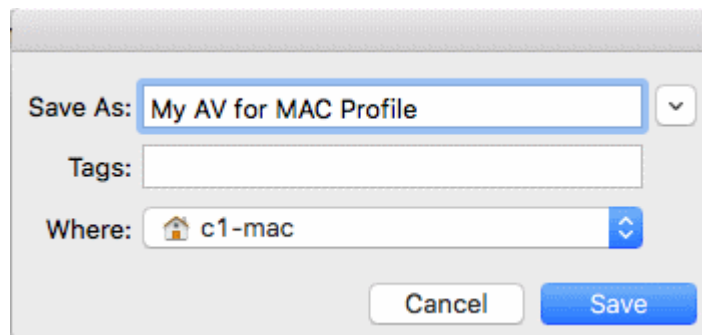
Click the links below for more help:

- [Export my configuration to a file](#)
- [Import a saved configuration from a file](#)
- [Select a different active configuration setting](#)
- [Delete a inactive configuration profile](#)

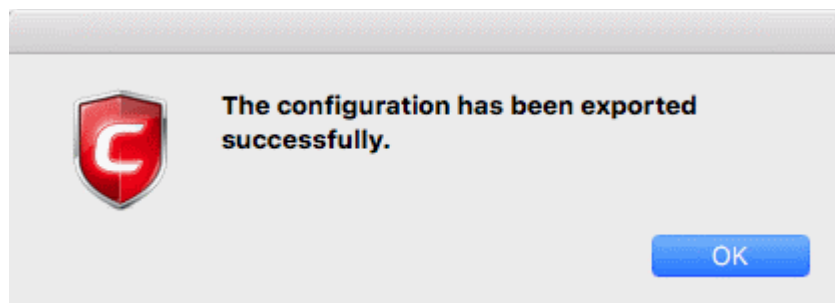
Export my configuration to a file

To export your currently active configuration

- Select the configuration and click the 'Export' button.
- Type a file name for the profile (e.g., 'My AV for MAC Profile') and save to the location of your choice. Or select a path to export the configuration dialog by clicking the arrow button beside the 'Save As' text box.



A confirmation dialog appears for the successful export of the configuration.

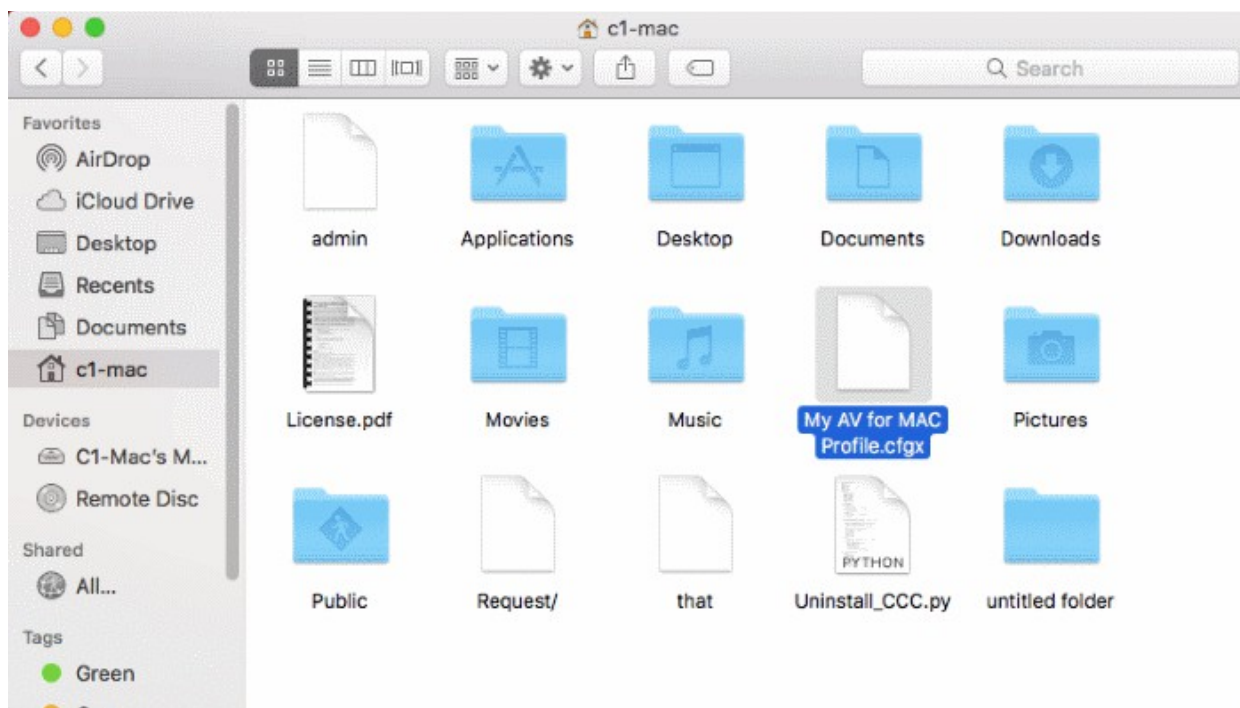


Import a saved configuration from a file

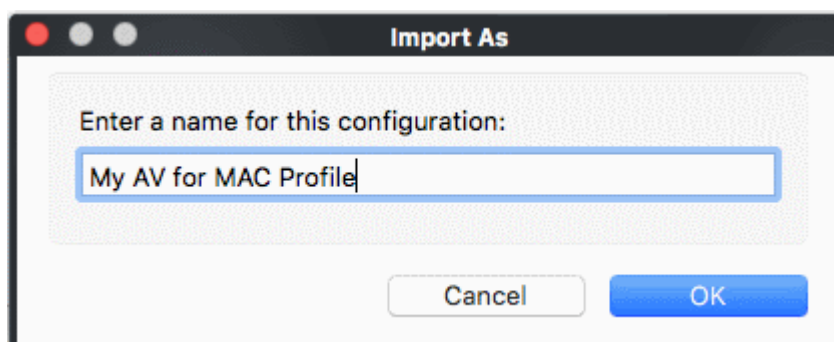
- Importing a profile lets you store it within Comodo Antivirus.
- Profiles you import do not become active until you **select them for use**.

To import a profile

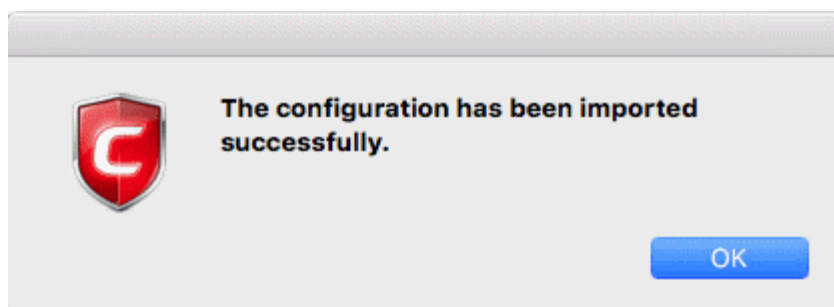
1. Click the 'Import' button.
2. Browse to the location of the saved profile and click 'Open'.



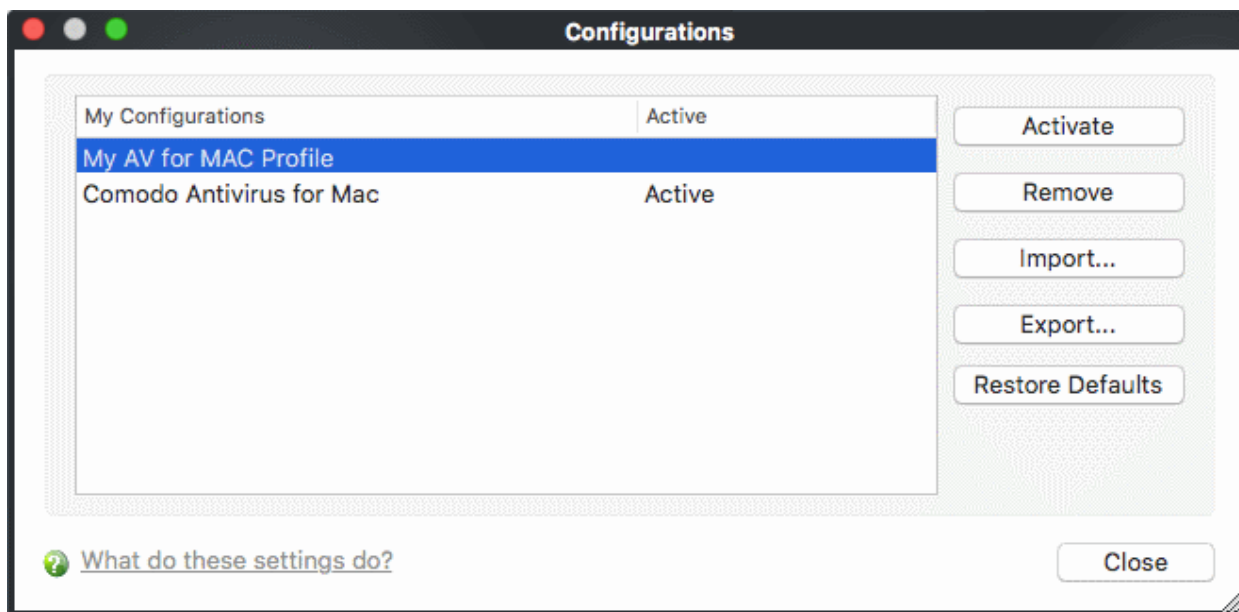
3. In the 'Import As' dialog that appears, assign a name for the profile you wish to import and click 'OK'.



A confirmation dialog appears indicating the successful import of the profile.



Once imported, the configuration profile is available for deployment by **selecting it**.



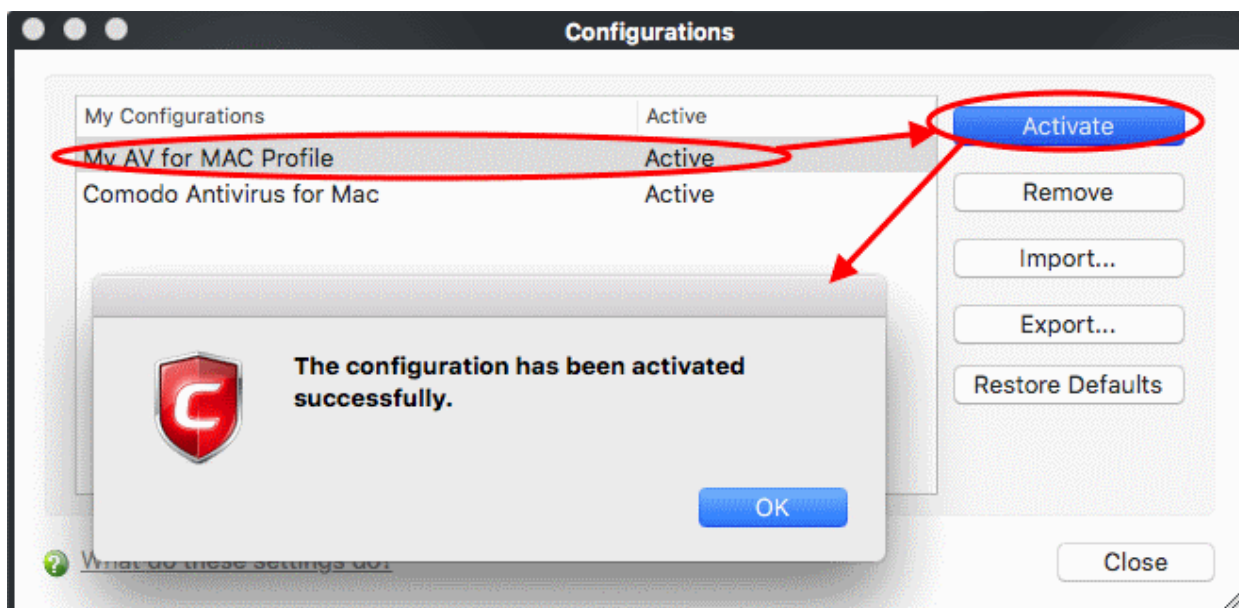
Select and Implement a different configuration profile

The **Activate** option allows you to quickly switch between configuration profiles.

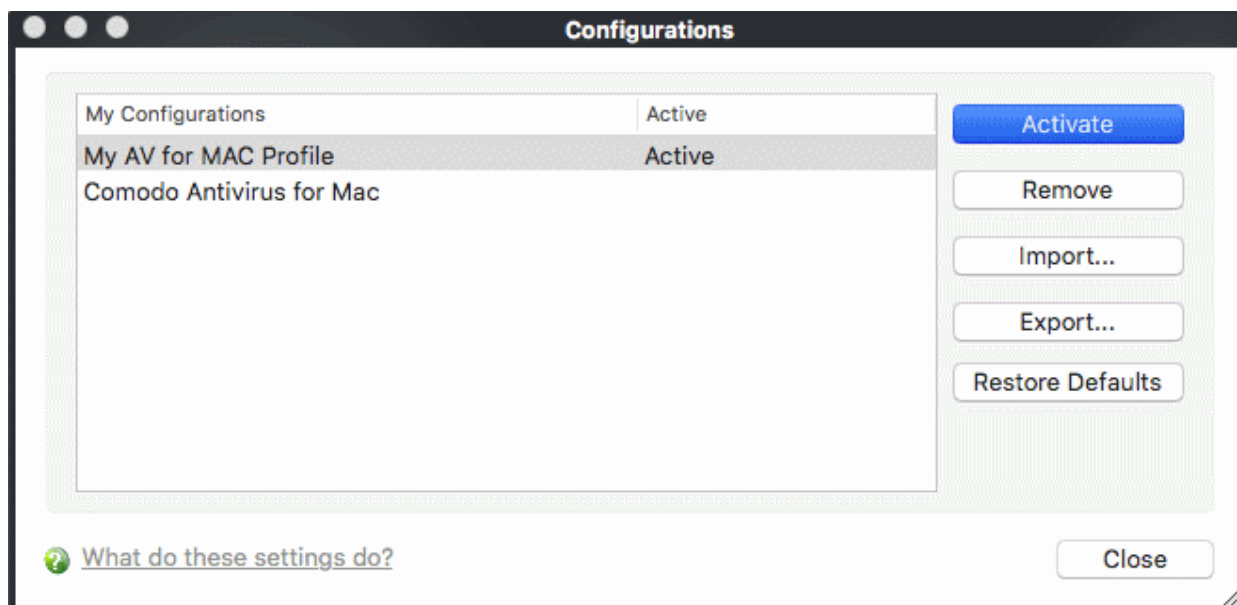
To select a different configuration

1. Click on the profile you want to select and activate.
2. Click the 'Activate' button.

A confirmation dialog appears.



The selected configuration is activated.

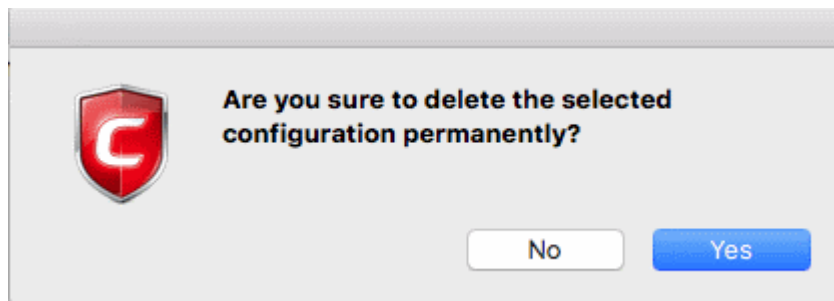


Delete an inactive configuration profile

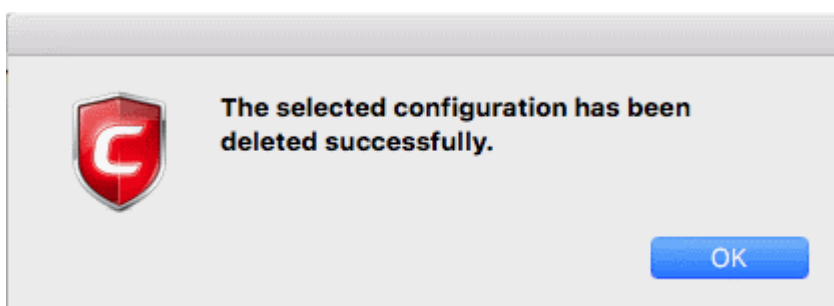
- Select a profile then click the 'Remove' button to delete it
- Only inactive profiles can be deleted. You cannot delete the profile that Comodo Antivirus is currently using.

To remove an unwanted profile

1. Select the profile and click 'Remove' button. A confirmation dialog appears.

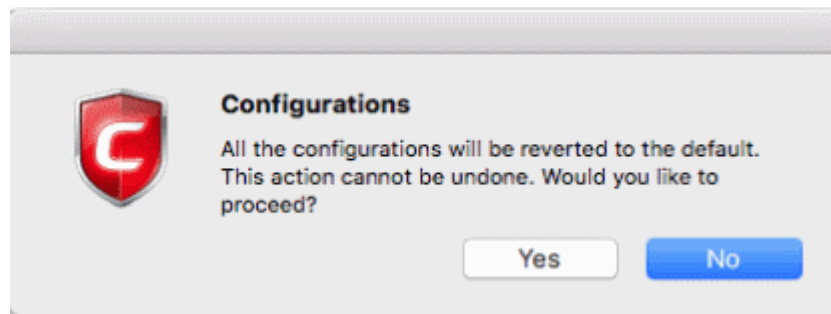


2. Click 'Yes' if you are sure to delete. The selected profile is removed from the list and a confirmation dialog appears.



To reset to a default profile

1. Select the profile and click 'Restore to Defaults' button. A confirmation dialog appears.



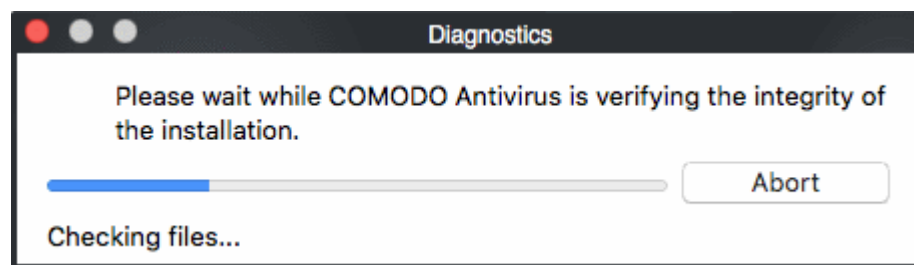
2. Click 'Yes' if you are sure to restore.

3.3. Diagnostics

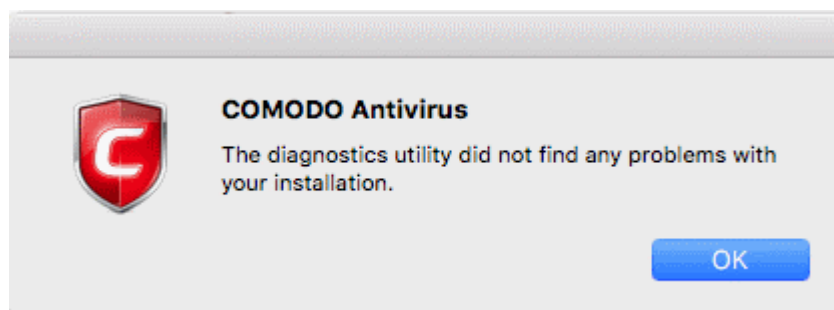
- Click 'More' on the 'CAV' home screen
- Click 'Diagnostics' in the 'More' interface

Comodo Antivirus has its own integrity checker. This checker scans your system to make sure that the application is installed correctly. It checks:

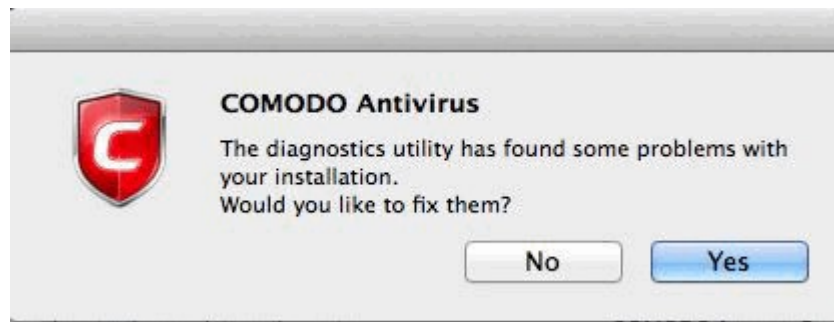
- File System - Checks that all Comodo system files are correctly installed.
- Registry - Checks that all Comodo registry keys are correctly installed.
- Incompatible software. Checks for the presence of software that is known to have compatibility issues with Comodo Antivirus.



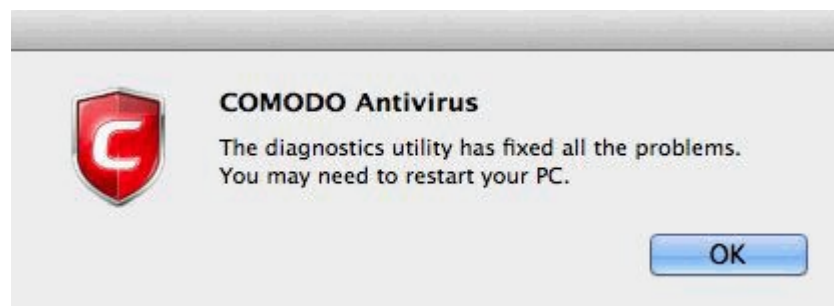
The results of the scan are shown in the following pop-up window. If your installation does not have any errors the following dialog is displayed.



If the diagnostics utility has found some errors in the installation, the following dialog is displayed.



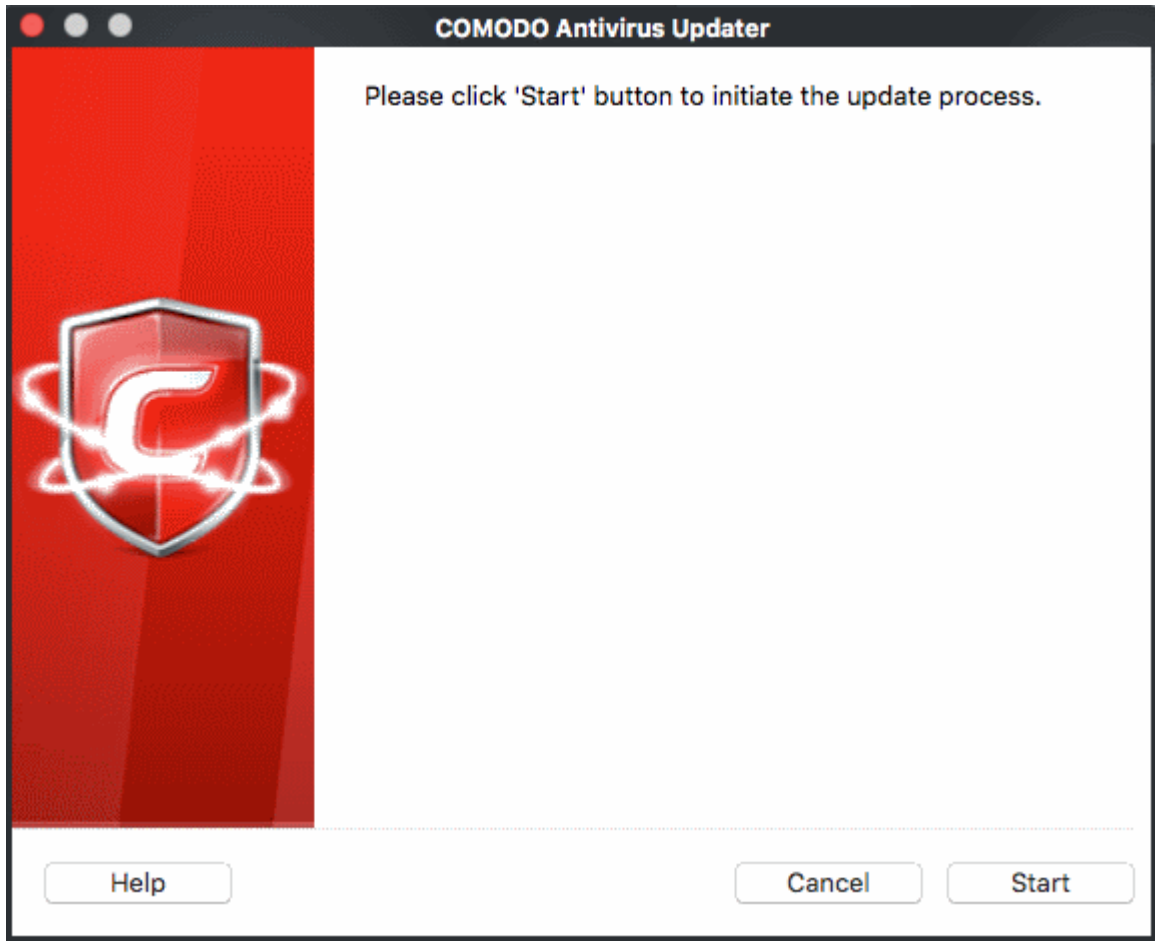
Click 'Yes'. The diagnostics utility automatically fixes the problems and prompts you to restart the computer.



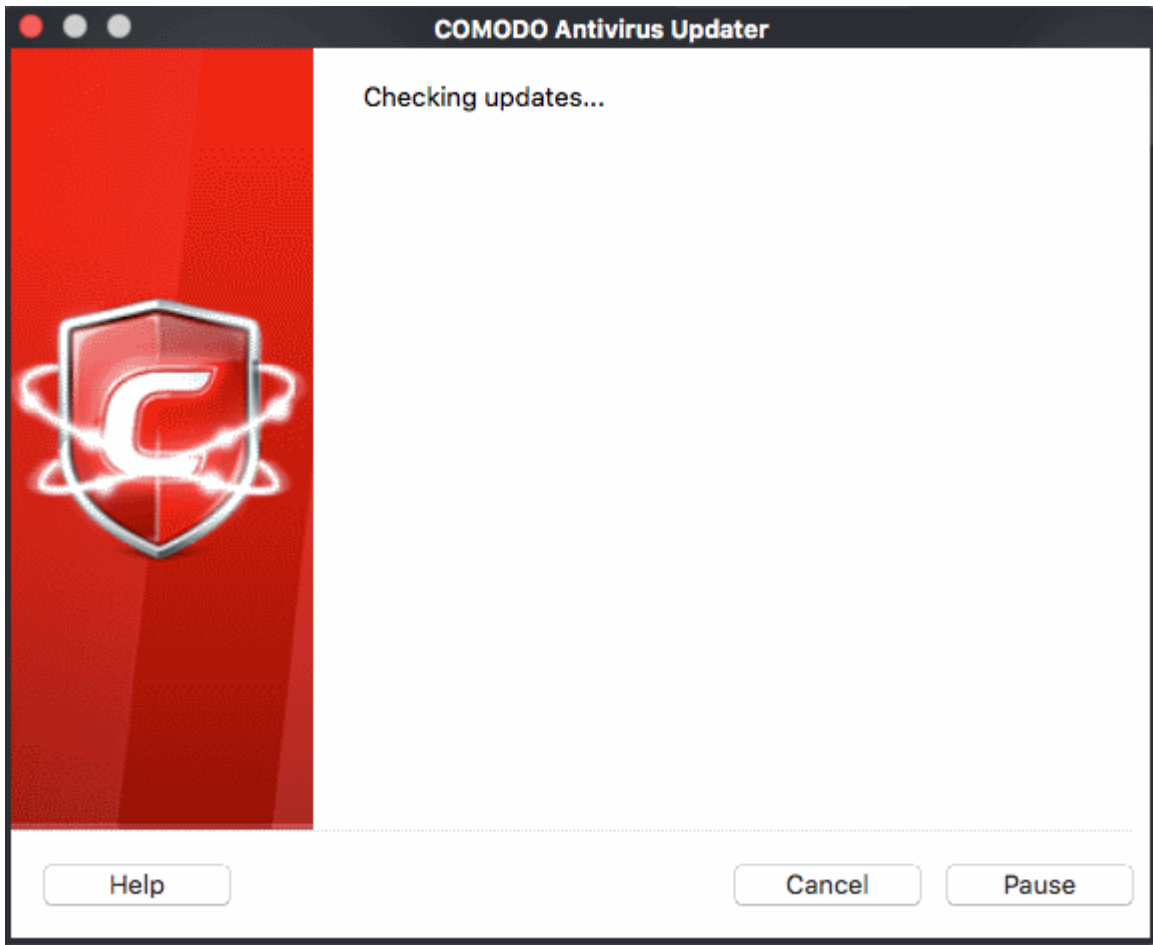
Restart your computer for the changes to take effect.

3.4. Check for Updates

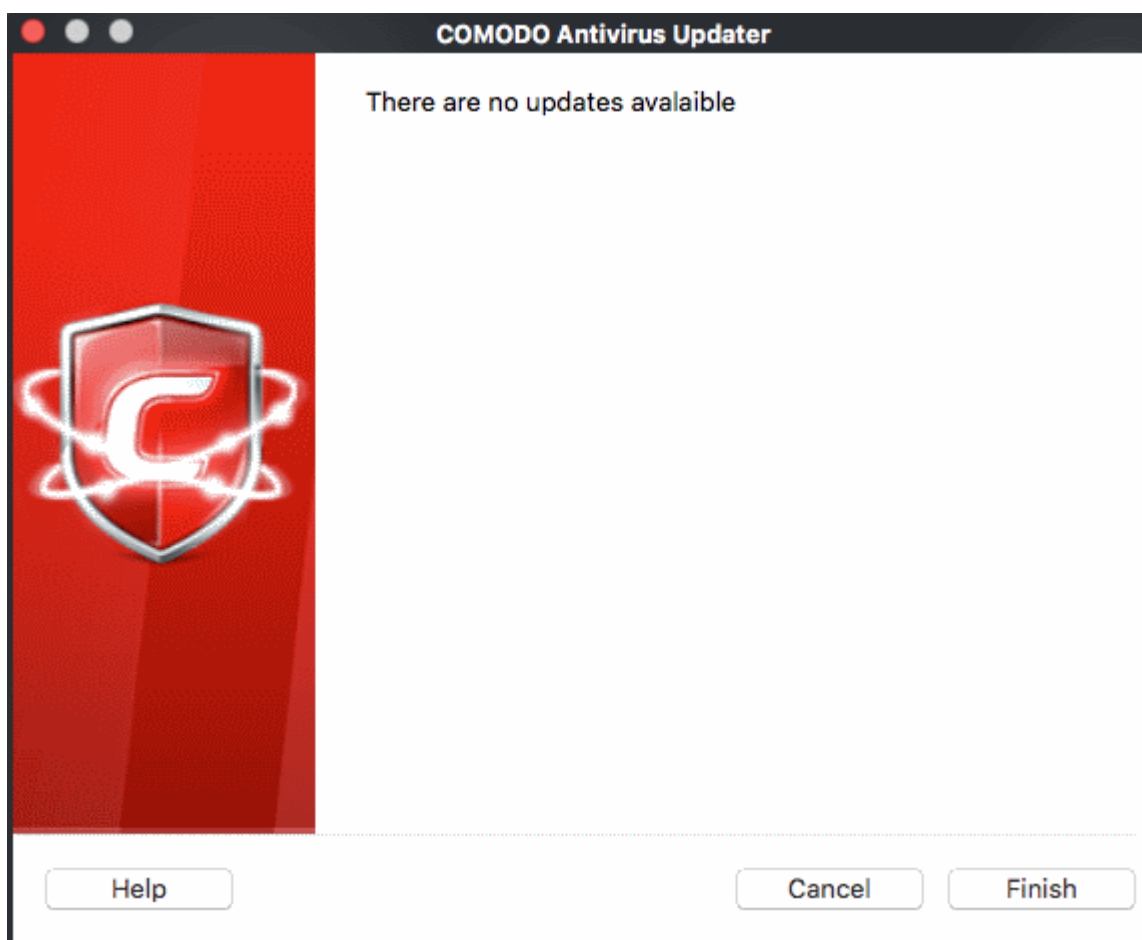
- Click 'More' on the 'CAV' home screen
- Click 'Check for Updates' in the 'More' interface.
 - Click 'Start' to begin the update process:



- Click 'Pause' to temporarily stop the process



- You will see the following screen after a successful update:

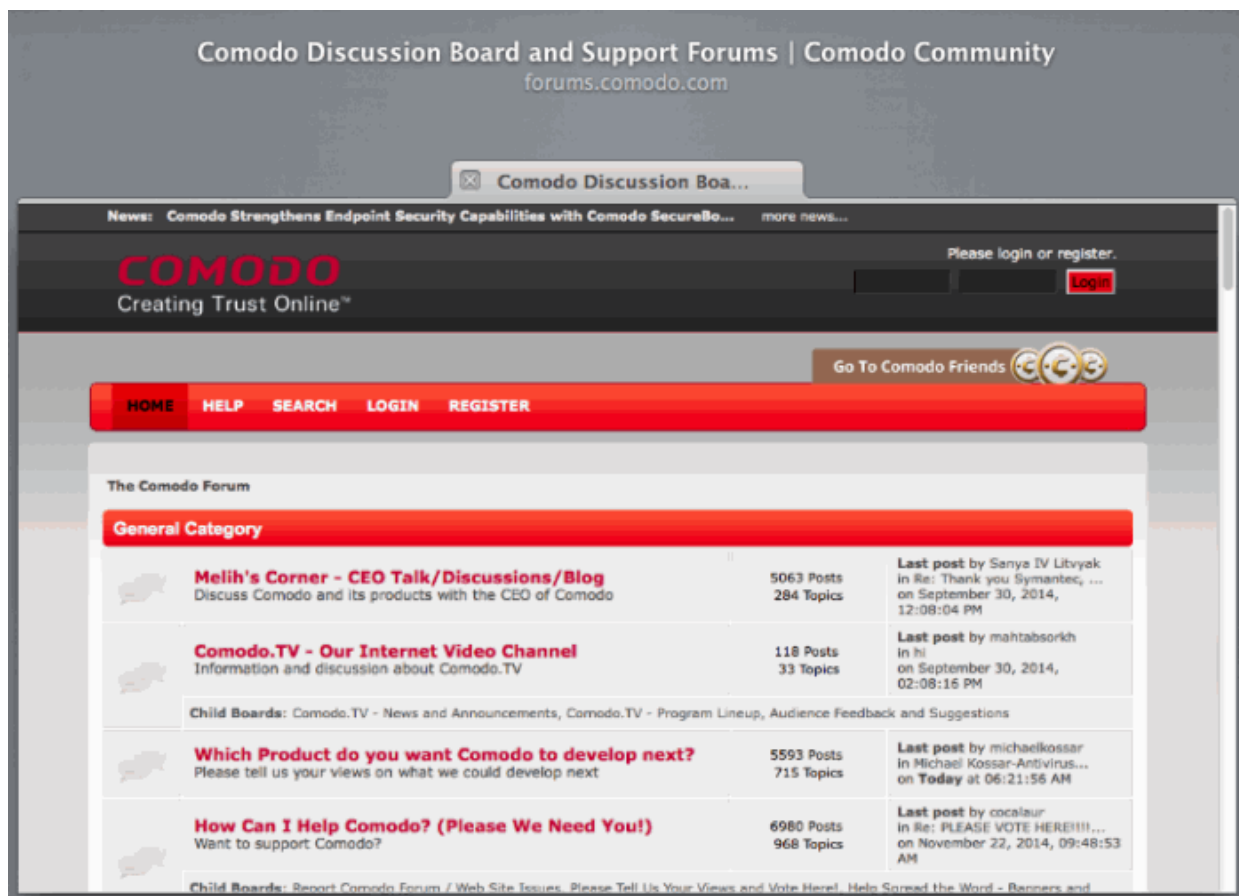


- Click 'Finish' to close the window.

3.5. Browse Support Forums

Comodo forums are the fastest way to get help with Comodo Antivirus.

- Click 'More' on the 'CAV' home screen
- Click 'Browse Support Forums' in the 'More' interface
- This will open Comodo's community forums in your default browser.
 - Alternatively, copy the following URL into your browser address bar: <http://forums.comodo.com>
- Click the 'Register' link if you do not yet have an account. Registration is free.
- Post away!! Submit any questions and suggestions you like about our products. You'll benefit from expert advice from fellow users and Comodo developers alike.

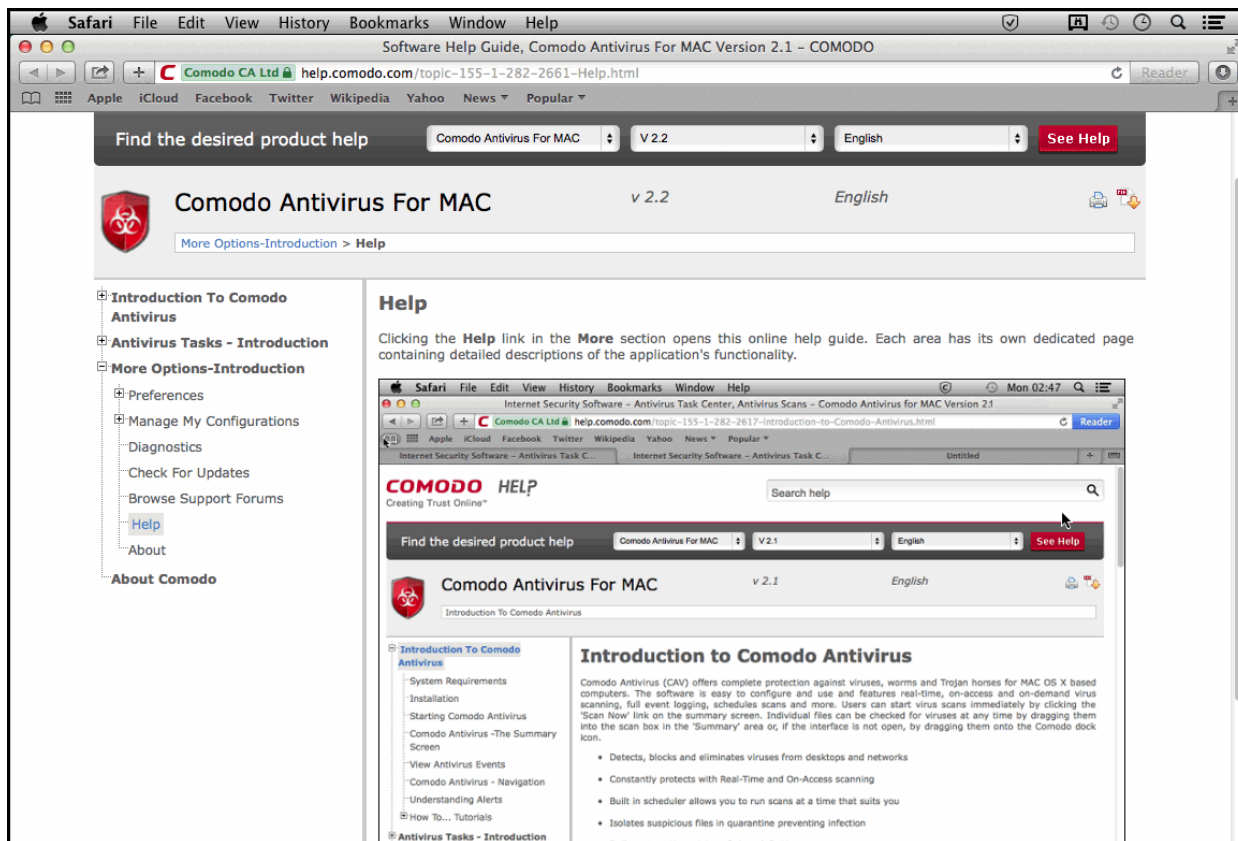


Online Knowledge Base

We also have an online knowledge base and support ticketing system at <http://support.comodo.com>. Registration is free.

3.6. Help

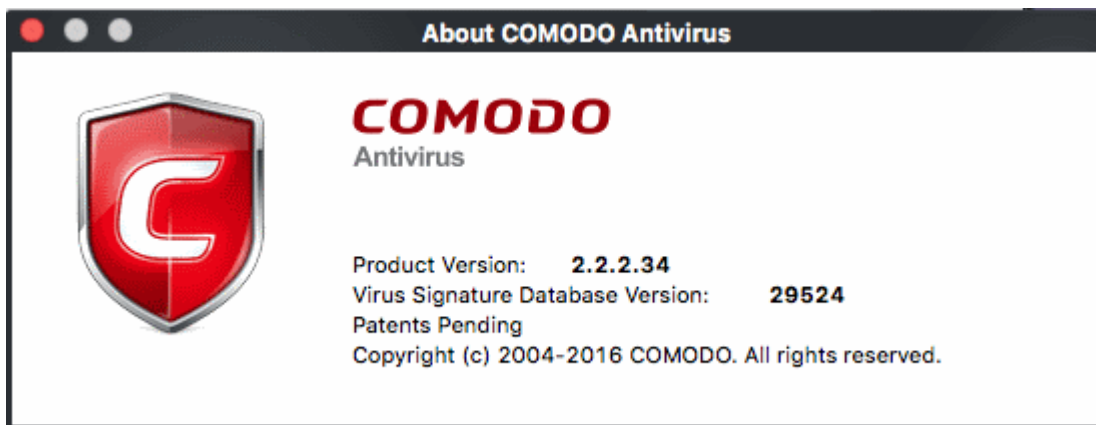
- Click 'More' on the 'CAV' home screen
- Click 'Help' in the 'More' interface
- This will open Comodo Antivirus for Mac help guide at <https://help.comodo.com/>
- Each feature has a dedicated page with detailed explanations of product functionality.



You can also print the guide or download it as a .pdf.

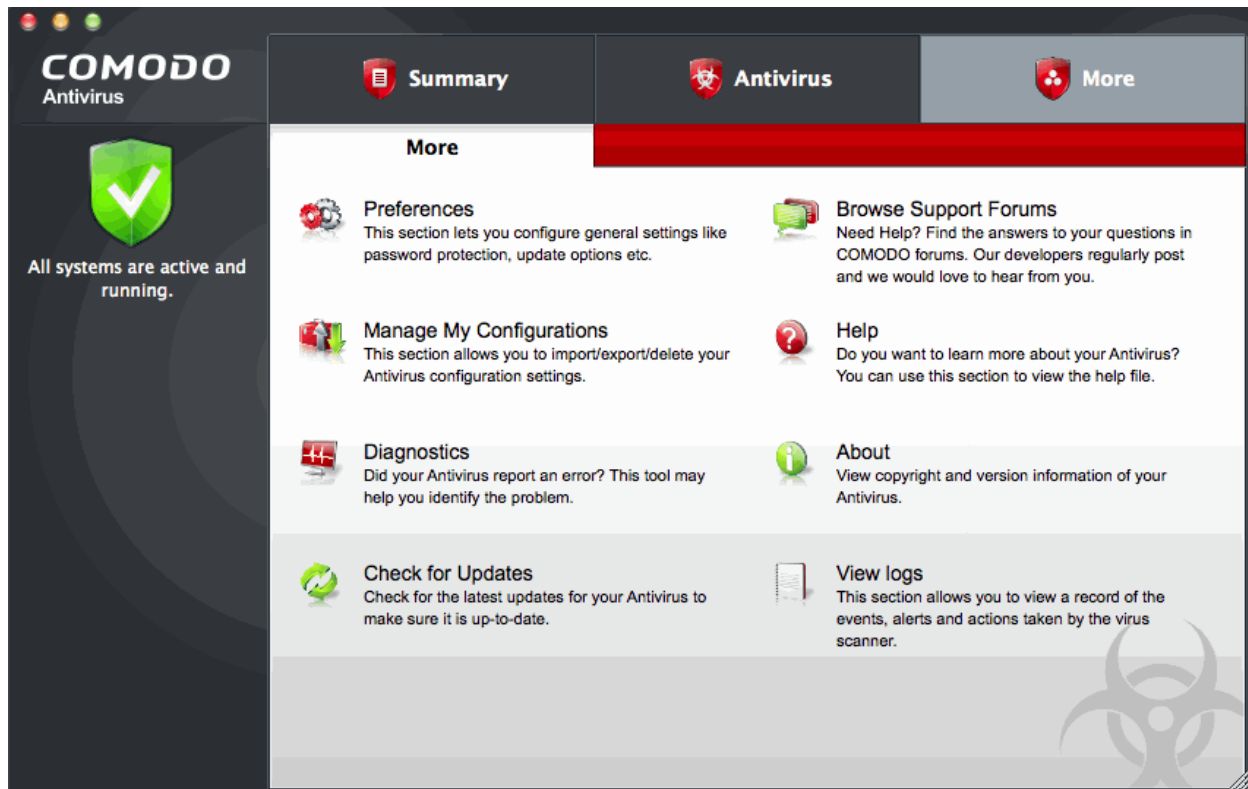
3.7. About

- Click 'More' on the 'CAV' home screen
- Click 'About' in the 'More' interface
- The 'About' dialog shows the software version and database version that you currently have installed.



3.8. View Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Comodo Antivirus for MAC records all actions it takes in extensive but easy to understand reports.
- A detailed scan report contains statistics on all scanned objects, the settings used for each task, and the history of actions performed on each individual file.
- Reports are also generated during real-time protection, and after updating the anti-virus database and application modules.



To view a log of Antivirus Events

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Click 'View Antivirus' from the 'Log Viewer' interface.

Date	Location	Malware Name	Action	Status	Alert	Scan UID
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Quarantine	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Ignore	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	False Positive	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Add To Exclusions	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	False Positive	Success		00000000-00...
Jul 14, 2015,...	/Volumes/A...	Malware@#1zejn0p...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2lip27dn...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2vbq6nvg...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1uvqv9p...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1l1fz4ca0...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#vgz10056...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1hqko49z...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#26k0348...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2h5rxwhk...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3mjs9wg...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#7n54h8r7...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3s46sen3...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3rebzpiy...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#37hshce...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#jw2oyhuq...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1qupwwx...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2e3ln8wp...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#jj24um6rivu...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3h6v2zy0...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1c4qxs6w...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3gdyrqjm...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#p8po2w4...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3g9cl0f6...	Quarantine	Failure		FC2FD708-4C...

The 'Log Viewer' Module is divided into three sections.

- The top panel displays a set of handy, predefined time filters.
- The left panel displays the types of logs.
- The right hand side panel displays the actual events that were logged for the time period you selected in the top panel and the type of log selected in the left panel (or the events that correspond to the filtering criteria you selected).

The 'Logs per Module' option contains the logged events of Antivirus modules and 'Other Logs' options contains logged events of the following:

- **Alerts Displayed:** Displays the list of various alerts that were displayed to the user, the response given by the user to those alerts and other related details of the alert.
- **Tasks Launched:** Displays the various Antivirus tasks such as updates and scans that have taken place. This area will contain a log of all on demand and scheduled AV scans and the result of that scan.
- **Configuration Changes:** Displays a log of all configuration changes made by the user in the CAVM application.

Filtering Log Files

AV for MAC allows you to create custom views of all logged events according to user defined criteria.

Creating custom filters

- You can filter logs using the controls in the 'Advanced Filter' bar above the report list.
- If you wish to view and filter event logs for other modules then simply click the log name in the tree
- This section will deal with advanced event filters related to 'Antivirus Events', but will also cover custom filters for 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes').

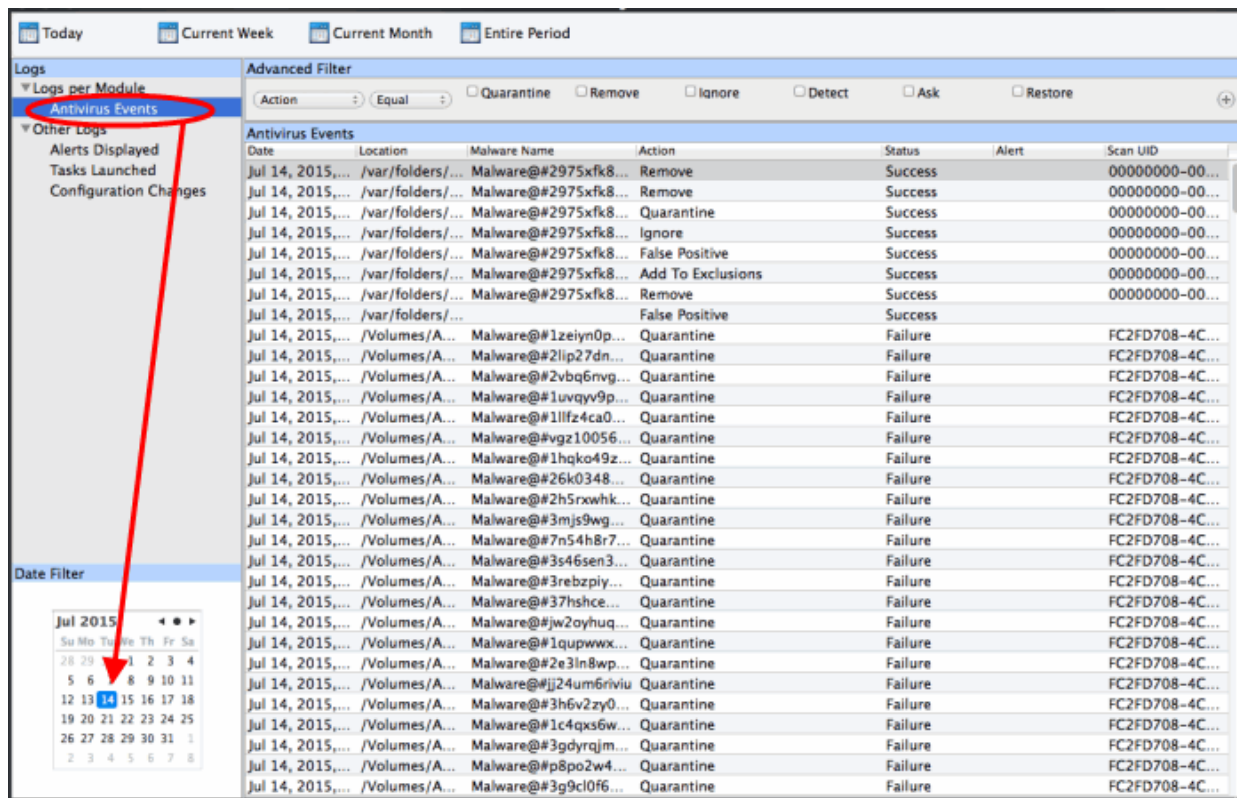
Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **Today** - Displays all logged events for today.

- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Antivirus for MAC was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).

The example below shows an example display when the Antivirus Events for 'Today' are displayed.



Click the following links for more explanations of the options available for each type of filter:

'Logs per Module':

- [Antivirus Logs](#)

'Other Logs':

- ['Alerts Displayed' Logs](#)
- [Tasks Launched](#)
- [Configuration Changes](#)

3.8.1. Antivirus Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Each antivirus log is a record of a malware discovery event. The list view shows the malware name, its location, the action that was taken on the file and whether the action was successful or not.

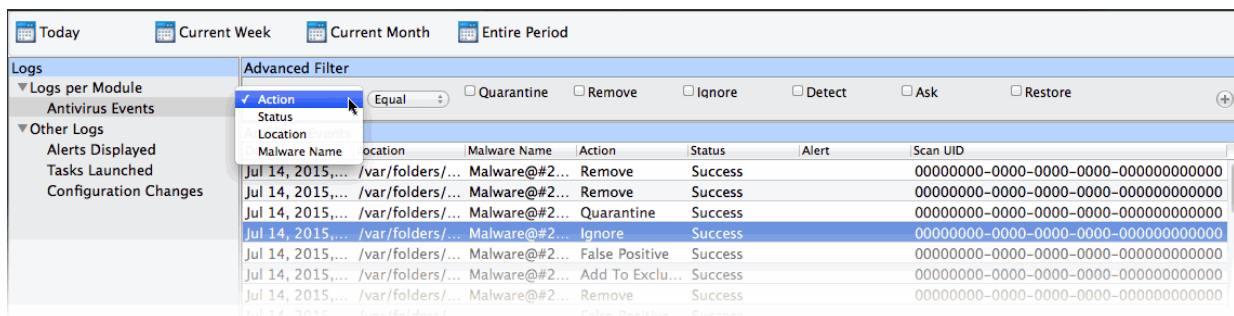
Date	Location	Malware Name	Action	Status	Alert	Scan UID
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Quarantine	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Ignore	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	False Positive	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Add To Exclusions	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...	Malware@#2975xfk8...	Remove	Success		00000000-00...
Jul 14, 2015,...	/var/folders/...		False Positive	Success		
Jul 14, 2015,...	/Volumes/A...	Malware@#1zeiyn0p...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2lip27dn...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2vbq6nvg...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1uvqyv9p...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1lfz4ca0...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#vgz10056...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1hqko49z...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#26k0348...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2h5rxwhk...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3mjs9wg...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#7n54h8r7...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3s46sen3...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3rebzpiy3...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#37hshc...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#jw2oyhuq...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1qpwpx...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#2e3ln8wp...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#jj24um6rivi...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3h6v2zy0...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#1c4qxs6w...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3gdyrqjm...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#p8po2w4...	Quarantine	Failure		FC2FD708-4C...
Jul 14, 2015,...	/Volumes/A...	Malware@#3g9cl0f6...	Quarantine	Failure		FC2FD708-4C...

Column Descriptions

1. **Date** - Indicates the date of the event.
2. **Location** - Indicates the location where the application detected with a threat is stored.
3. **Malware Name** - Name of the malware event that has been detected.
4. **Action** - Indicates action taken against the malware through **Antivirus**.
5. **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.
6. **Alert** - Details of any alert shown for the malware.
7. **Scan UID** - Gives the details of activities executed by the processes that are run by the infected application.

3.8.1.1. Filter Antivirus Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Click 'Antivirus Events' in 'Logs Per Module' option
- The 'Antivirus logs' can be viewed by selecting 'Antivirus Events' from the drop-down of the log viewer interface.
- You have 4 categories of filter that you can add. **Each of these categories can be further refined by selecting or deselecting filter parameters, or by typing a search term in the field provided.**

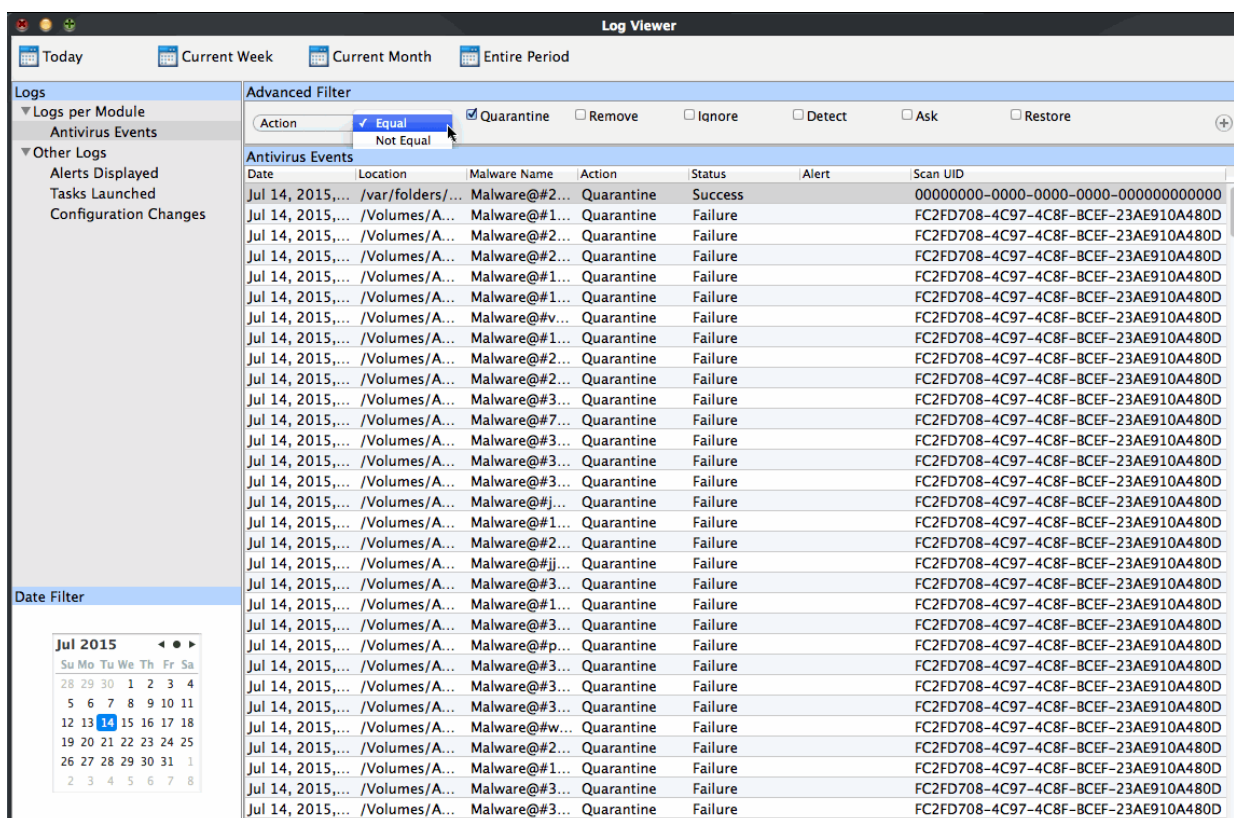


- You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. Action:

- Lets you filter logs by the action taken by CAV on the threat.
- Selecting the 'Action' option displays a drop down field and a set of specific filter parameters that can be selected or deselected.

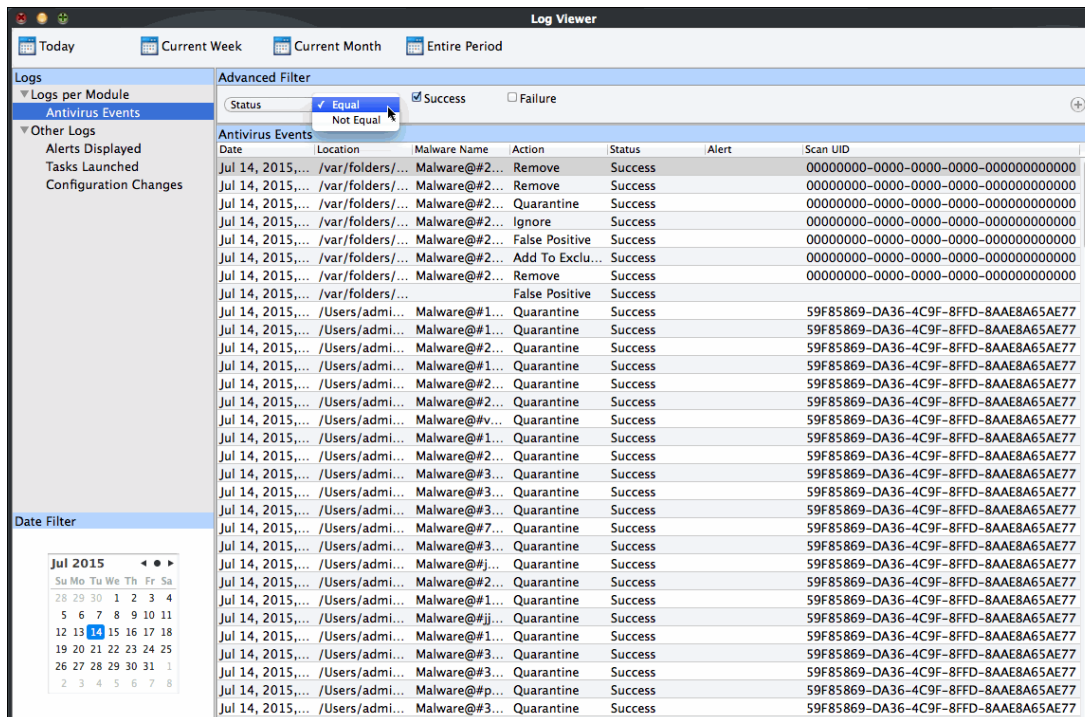


- Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Quarantine: Displays events where the user chose to quarantine a file
 - Remove: Displays events where the user chose to delete an item
 - Ignore: Displays events where the user chose to ignore an item
 - Detect: Displays events for detection of a malware
 - Ask: Displays events when user was asked by alert concerning some Antivirus event
 - Restore: Displays events of the applications that were quarantined and restored

For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

ii. Status:

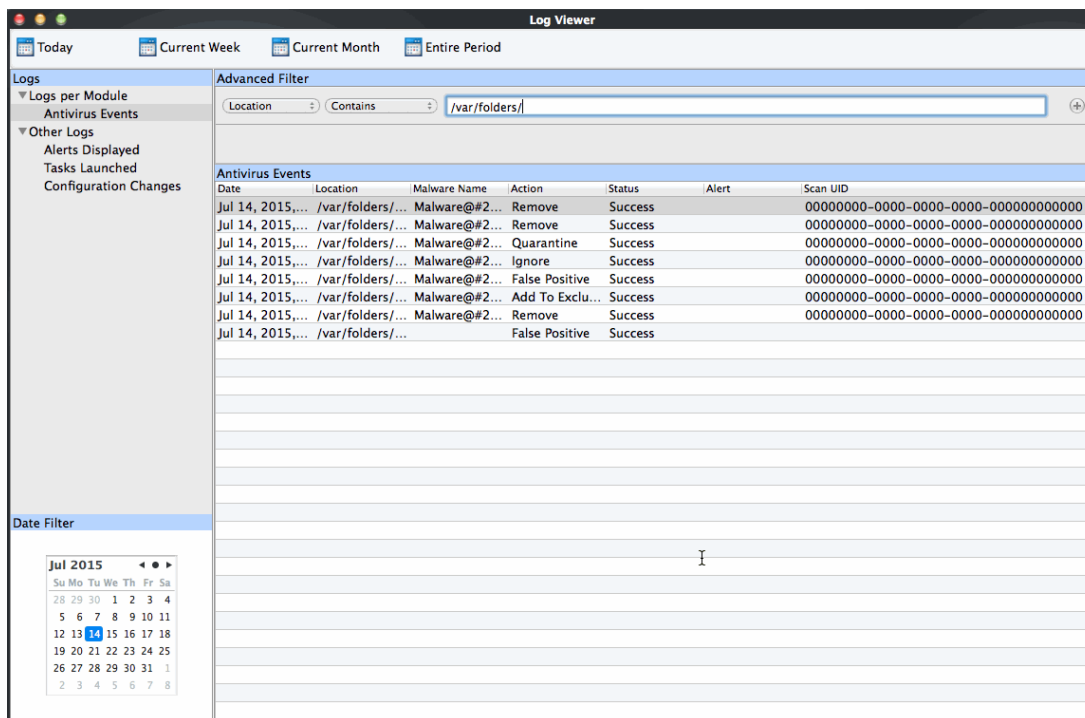
- Lets you filter logs by the success or failure of the action taken by CAV.
- Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Success: Displays Events that successfully executed (for example, the malware was successfully quarantined)
 - Failure: Displays Events that failed to execute (for example, the database malware was not disinfected)

iii. Location:

- Lets you filter logs by location of the threat
- Selecting the 'Location' option displays a drop-down field and text entry field.

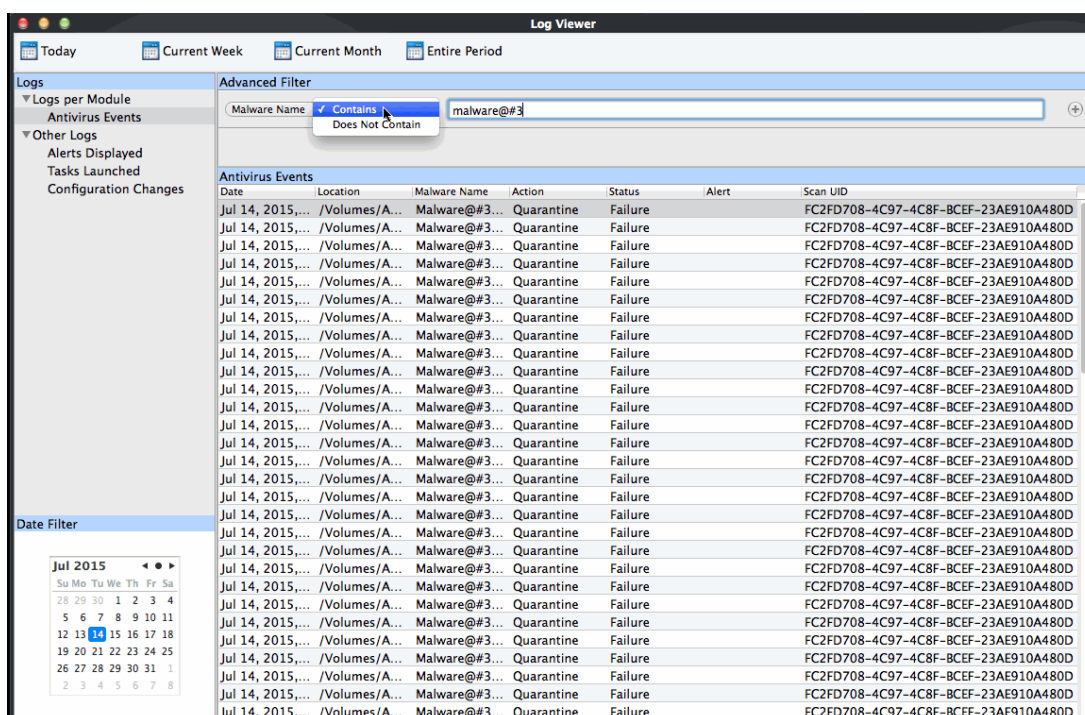


- Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- Enter the text or word that needs to be filtered.

For example, if you select 'Contains' option from the drop-down and enter the phrase '/var/folders/' in the text field, then all events containing the entry '/var/folders/' in the Location field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase '/var/folders/' in the text field, then all events that do not have the entry '/var/folders/' will be displayed.



iv. Malware Name:

- Lets you filter logs by the threat name
- Selecting the 'Malware Name' option displays a drop-down field and text entry field.



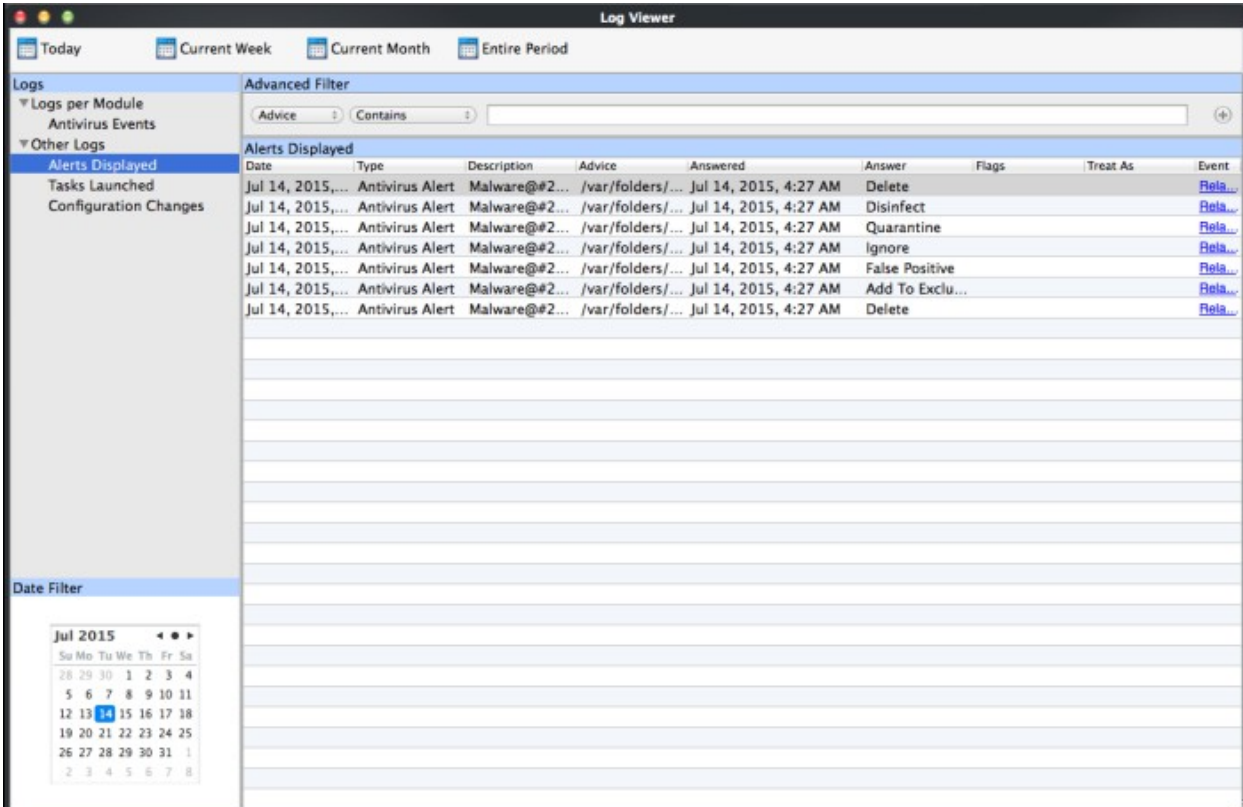
- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'malware@#3' in the text field, then all events containing the entry malware@#3 in the Malware Name field will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'malware@#3' in the text field, then all events that do not have the entry 'malware@#3' in the 'Malware Name' field will be displayed.

- You can add more filter types in the 'Advanced Filter' pane by clicking the  button at the top right of the filter pane.
- You can also remove a filter type by clicking the  button at the top right of the filter pane.
- The filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

3.8.2. 'Alerts Displayed' Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Click Other Logs > 'Alerts Displayed' link in 'Log Viewer' interface
- 'Alerts Displayed' is a record of security alerts generated by CAV. The 'Answer' column shows the action taken on the malware as a result of the user's response to the alert.



The screenshot shows the 'Log Viewer' application window. At the top, there are tabs for 'Today', 'Current Week', 'Current Month', and 'Entire Period'. Below these is a navigation pane on the left with options like 'Logs per Module', 'Antivirus Events', and 'Other Logs', with 'Alerts Displayed' selected. The main area shows an 'Advanced Filter' set to 'Advice: Contains' and a table of logs. A 'Date Filter' at the bottom left shows a calendar for July 2015 with the 14th selected.

Date	Type	Description	Advice	Answered	Answer	Flags	Treat As	Event
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Delete			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Disinfect			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Quarantine			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Ignore			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	False Positive			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Add To Exclu...			Rela...
Jul 14, 2015,...	Antivirus Alert	Malware@#2... /var/folders/...		Jul 14, 2015, 4:27 AM	Delete			Rela...

Column Descriptions

1. **Date** - Contains precise details of the date and time of the alert generation.
2. **Type** - Indicates the type of the alert.
3. **Description** - Brief description of the file or the event that triggered the alert.

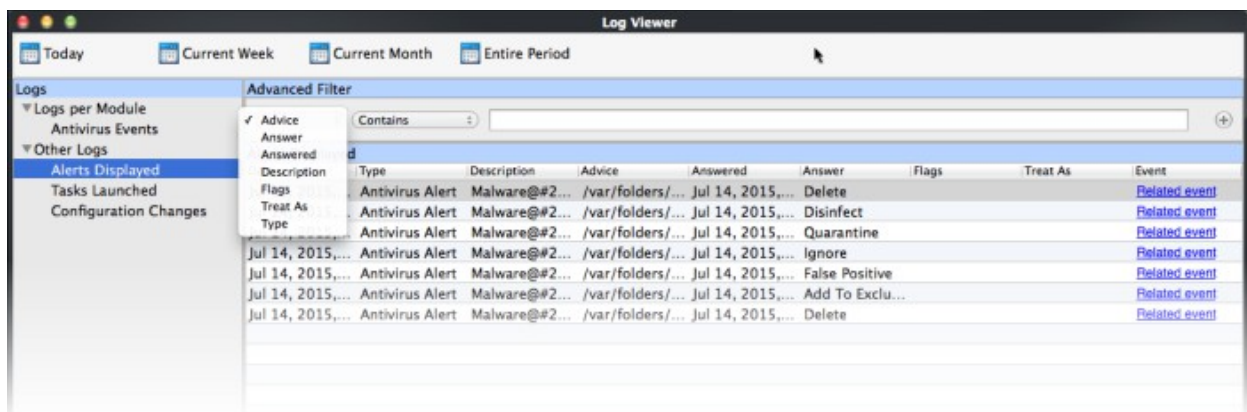
4. **Advice** - Advice offered by CAVM on how to respond for the alert.
5. **Answered** - Indicates whether the alert has been answered by the user and if answered, contains precise details of the date and time of response from the user.
6. **Answer** - Indicates the response given by the user.
7. **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
8. **Treat As** - Based on the response how the file is treated, whether it is treated as a safe application, installer and so on.
9. **Event** - Clicking 'Related Event' opens the details of the event that has triggered the alert.

3.8.2.1. Filter 'Alerts Displayed' Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' > 'Other Logs' > 'Alerts Displayed'
- You can create custom views of all logged events
- Comodo Antivirus for MAC allows you to create custom views of all logged events according to user defined criteria

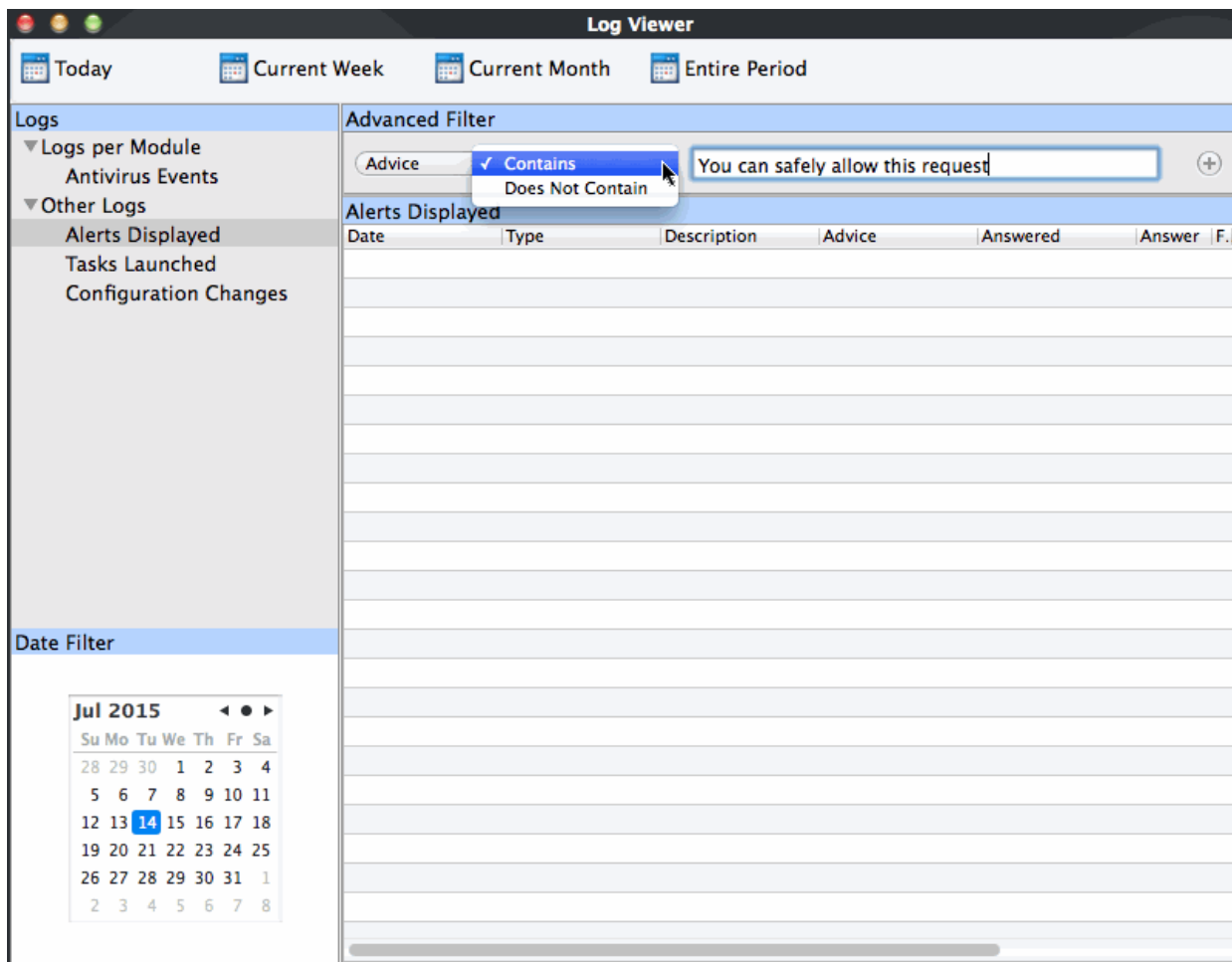
To configure Advanced Filters for Antivirus events

- Select 'View Logs' > under 'Other Logs', select 'Alerts Displayed'.
- You have 7 categories of filter that you can add.
 - Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.
- You can add and configure any number of filters in the 'Advanced Filter' dialog.



Following are the options available in the 'Add' drop down menu:

- i. **Advice:**
 - The 'Advice' option enables you to filter the alerts based on recommendations given by CAV in the alert.
 - Selecting the 'Advice' option displays a drop-down field and text entry field.

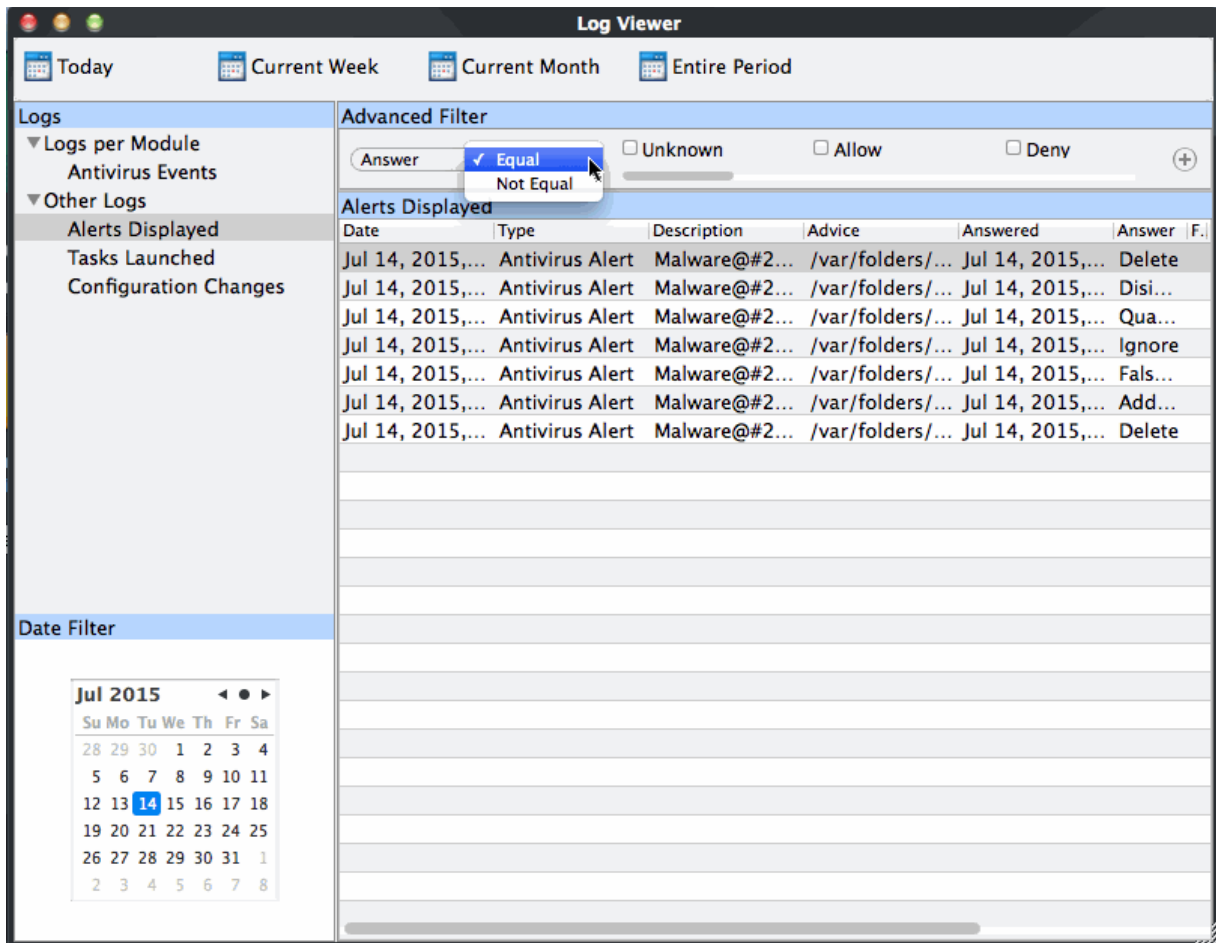


- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'you can safely allow this request' in the text field, then only the entries containing 'you can safely allow this request' in the 'Advice' column will be displayed.

ii. Answer:

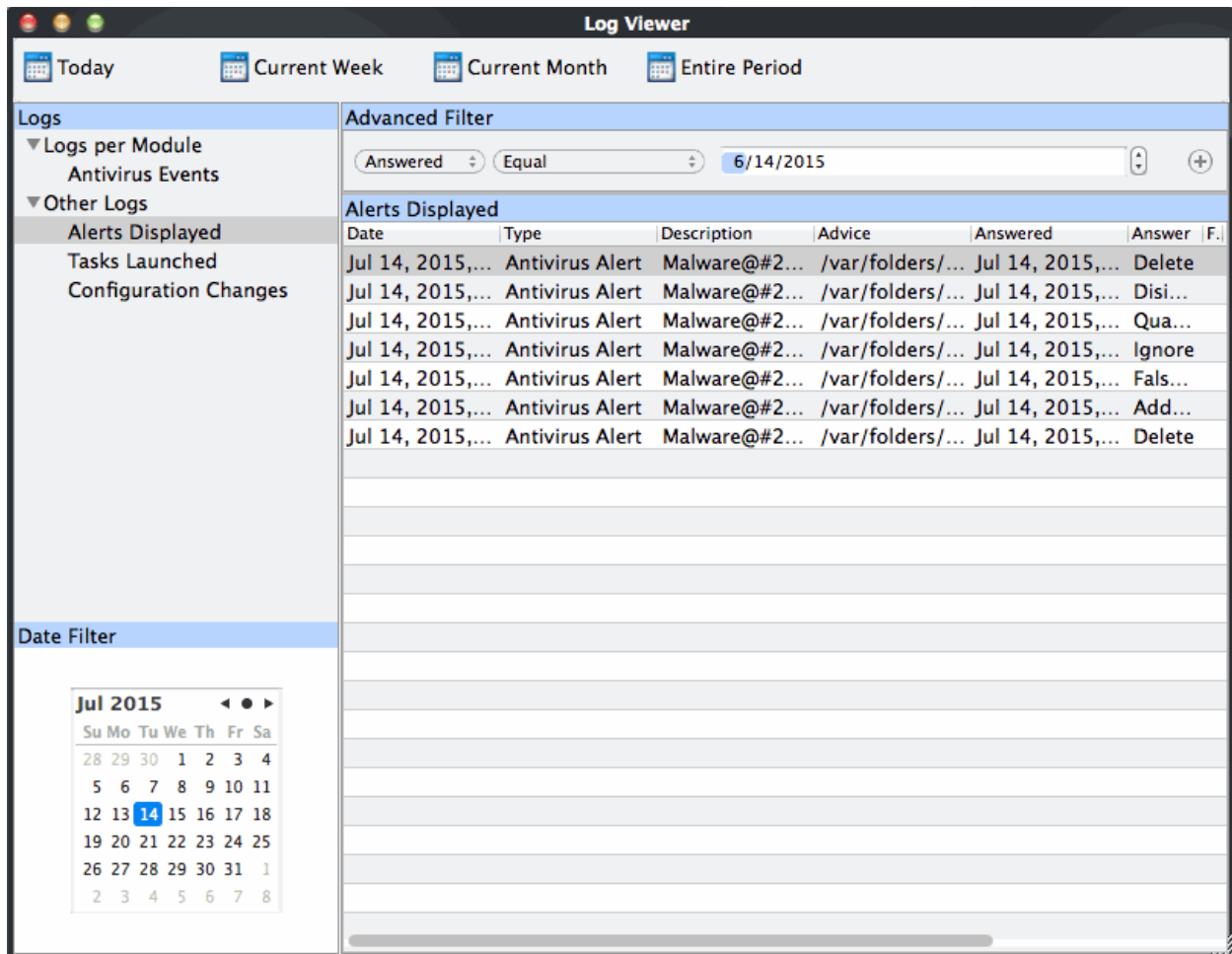
- The 'Answer' option enables you to filter the alerts based on how you answered for the alerts.
- Selecting the 'Answer' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - Unknown
 - Allow
 - Deny
 - Treat As
 - Time-out
 - Disinfect
 - Quarantine
 - Skip Once
 - Add to Exclusions
 - Add to Trusted Files
 - False Positive
 - Skip
 - Terminate

For example, if you choose 'Equal' from the drop-down and select 'Add to Exclusions' checkbox, only the log of Antivirus alerts for which you answered as 'Ignore' > 'Ignore and Add to Exclusions' will be displayed.

iii. Answered: The Answered option enables you to filter the log based on the date you answered the alerts. Selecting the 'Answered' option displays a drop-down box and date entry field.



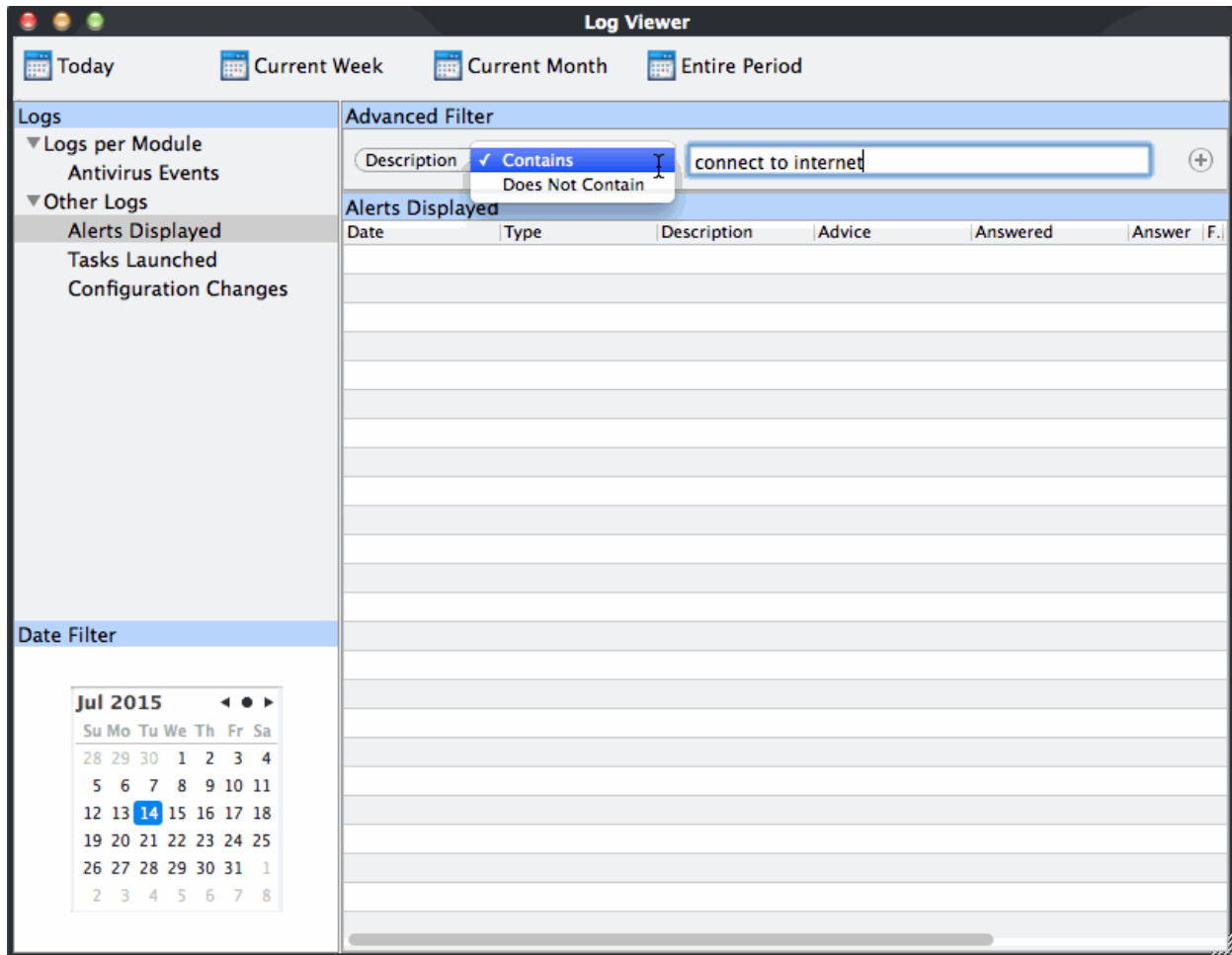
a. Select any one of the following option the drop-down box.

- Equal
- Not Equal

b. Enter the date by selecting it from the calendar displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '06/14/2015', only the log of alerts answered on 06/14/2015 will be displayed.

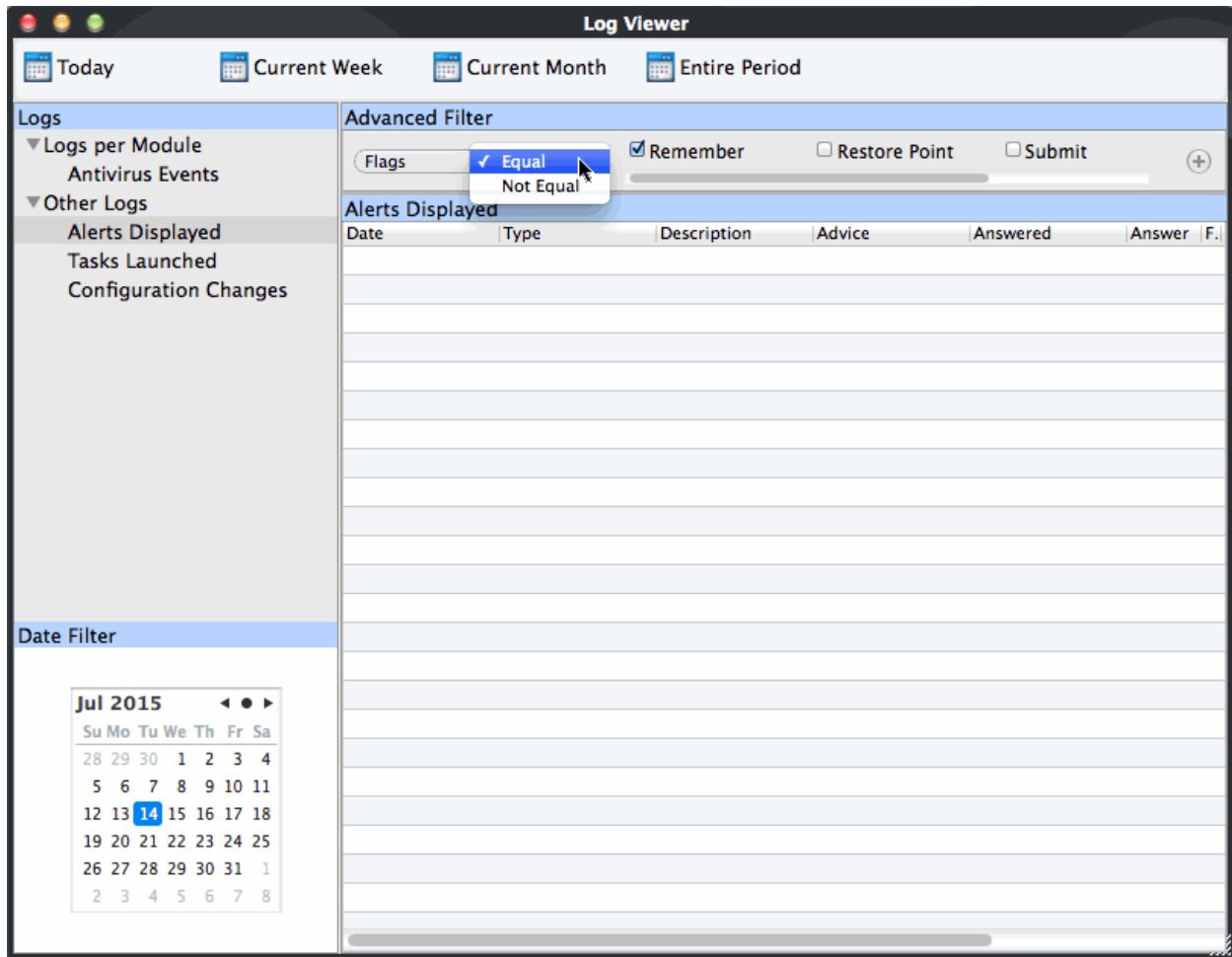
iv. Description: The Description option enables you to filter the log based on the description of the attempt displayed in the alert. Selecting the 'Description' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you select 'Contains' from the drop-down and enter 'connect to the Internet', only the log entries of Firewall alerts that contain the phrase 'connect to the Internet' in the description, will be displayed.

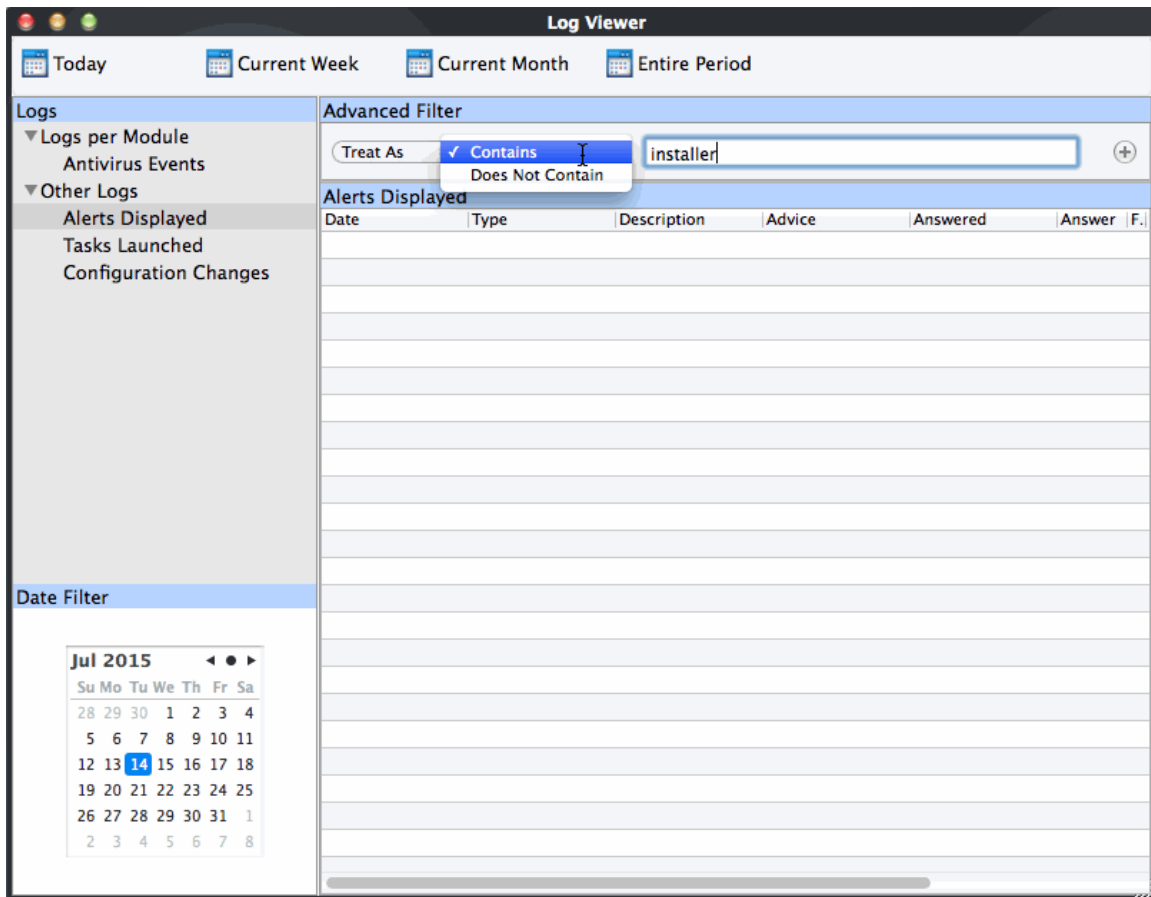
v. Flags: The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - Remember
 - Restore Point
 - Submit
 - Trusted Publisher

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

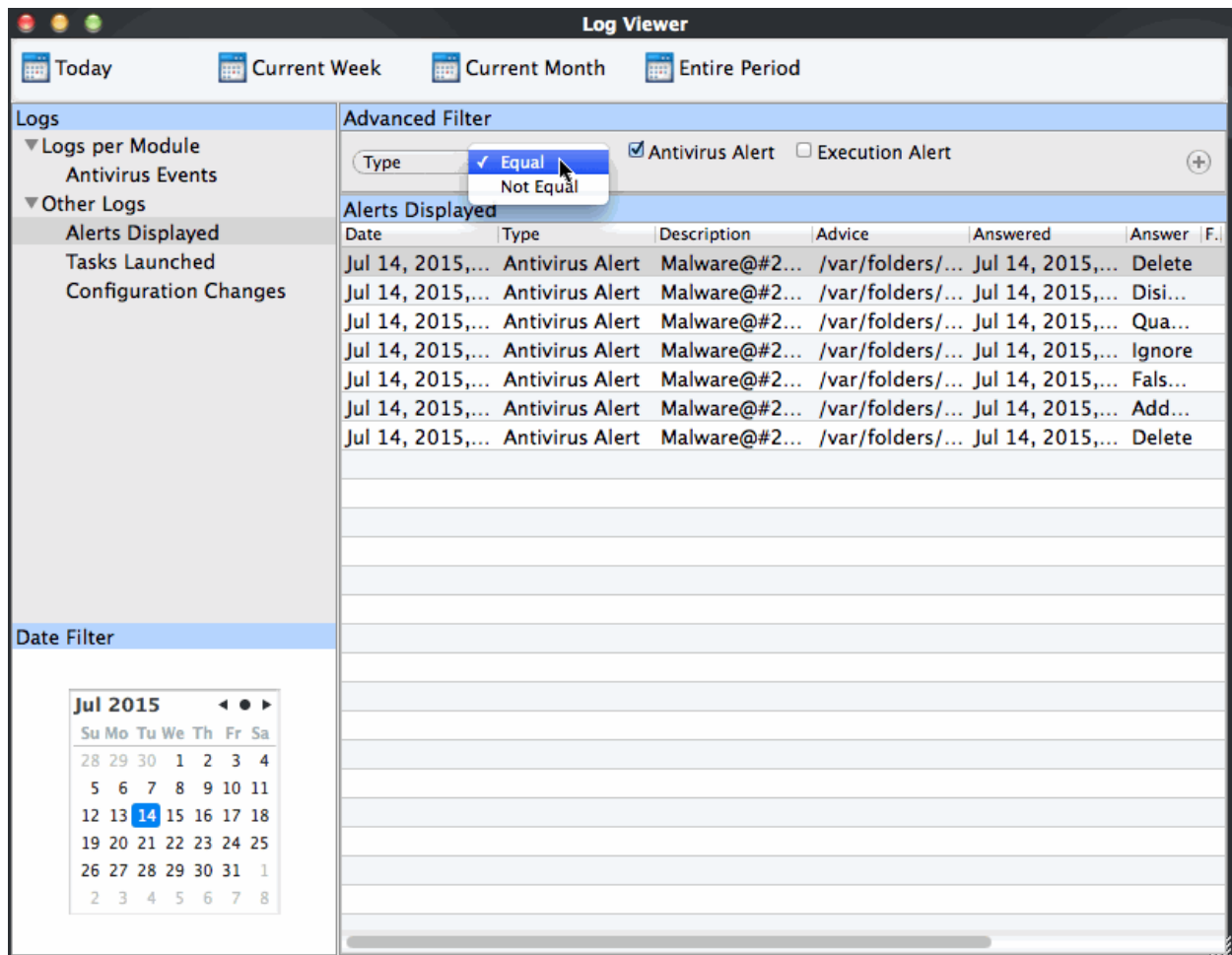
vi. Treat As: The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria



For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

vii. Type: The 'Type' option enables you to filter the entries based on the component of CIS that has triggered the alert. Selecting the 'Type' option displays a drop down menu and a set of specific alert types that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - Antivirus Alert
 - Execution Alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of Antivirus alerts will be displayed.

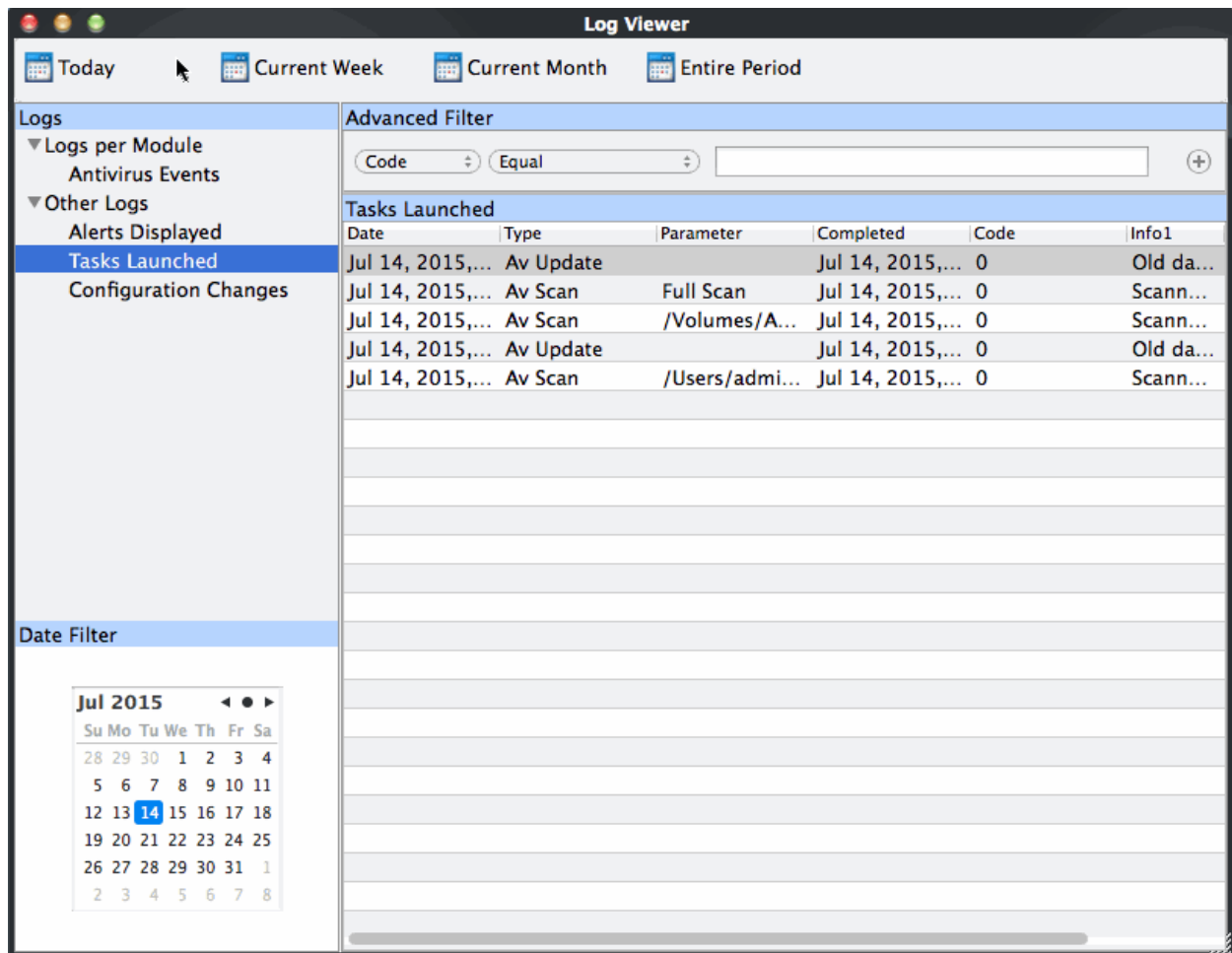
- You can add more filter types in the 'Advanced Filter' pane by clicking  the button at the top right of the filter pane.
- You can also remove a filter type by clicking the  button at the top right of the filter pane.

The filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

3.8.3. Tasks Launched

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' in the 'More' interface
- Click Other Logs > 'Tasks Launched' link in 'Log Viewer' interface
- Comodo Antivirus for MAC records a history of all the CAV tasks like virus signature database updates, scans run and so on.
- The 'Tasks Launched' log window displays a list of tasks launched at various time points with their

completion status and other details.



Column Descriptions

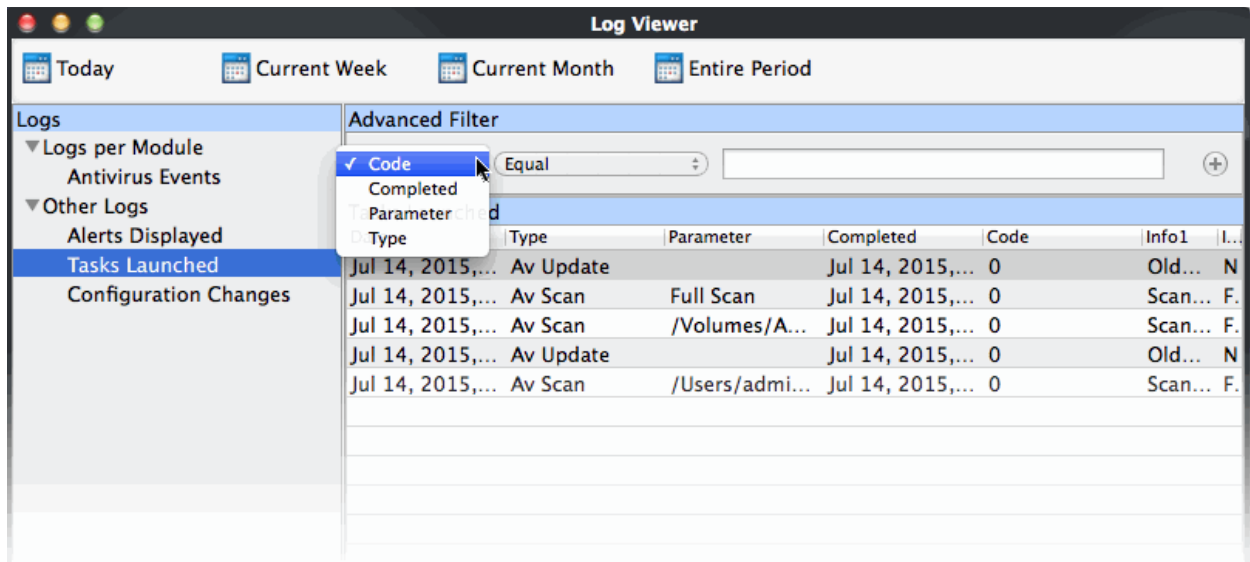
1. **Date** - Contains precise details of the date and time when the task is launched.
2. **Type** - Indicates the type of the task.
3. **Parameter** - Indicates the parameter (like scan type) associated with the task.
4. **Completed** - Contains precise details of the date and time of the completion of the task.
5. **Code** - Indicates the code of the task as assigned by CAV.
6. **Info & Additional Info** - Provides additional information of the task.

3.8.3.1. Filter 'Tasks Launched' Logs

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' > 'Other Logs' > 'Tasks Launched'
- You can create custom views of all logged events
- Comodo Antivirus for MAC allows you to create custom views of all logged events according to user defined criteria.

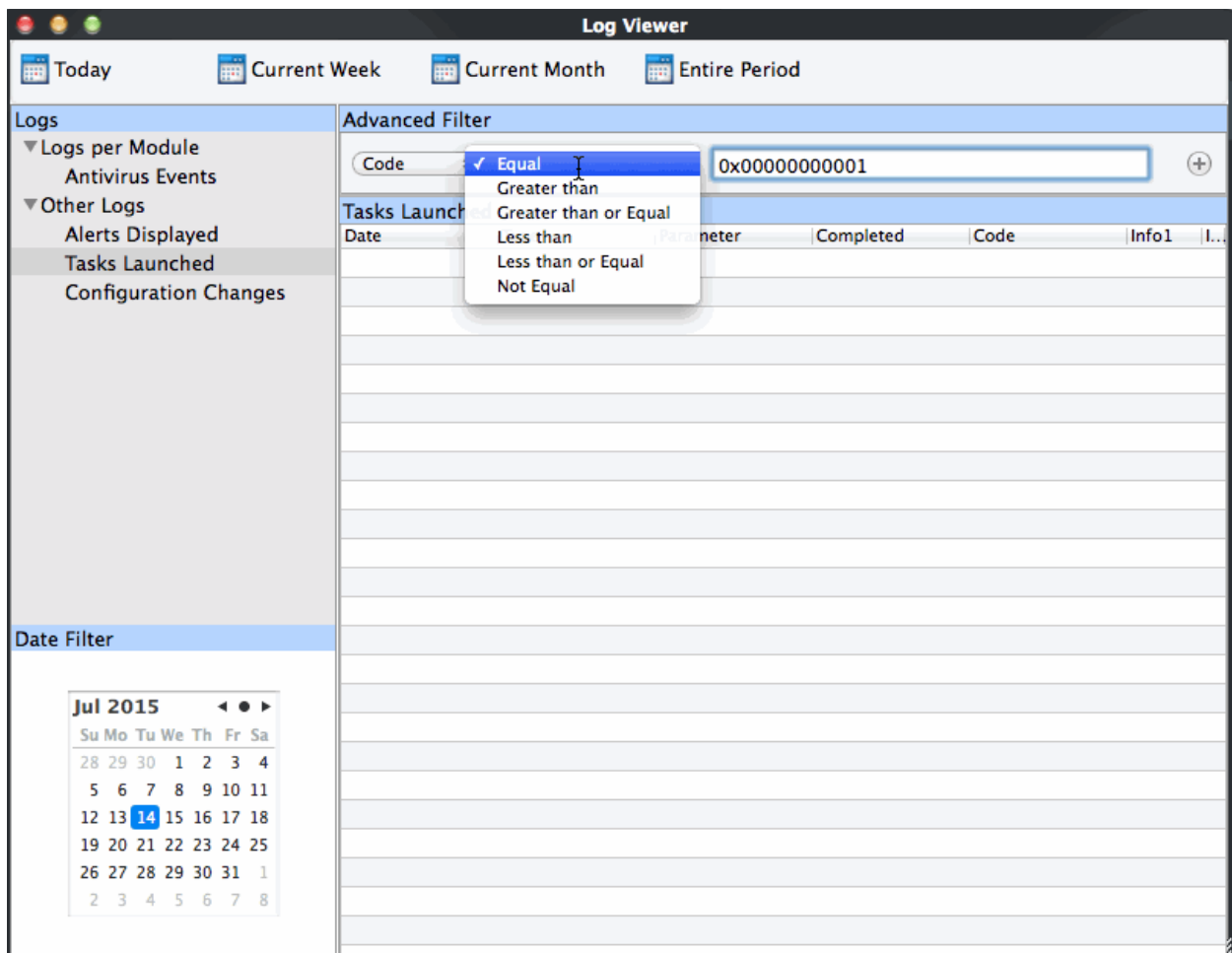
From 'Task Launched' interface, you can chose the category of filter from a drop-down box. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.

1. Click 'Advanced Filter' drop-down when you have chosen the category upon which you wish to filter.



- You have 4 categories of filters that you can add. You can chose the category of filter from a drop down box.
- Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.
- Following are the options available in the 'Advanced Filter' drop down menu:

i. **Code:** The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.

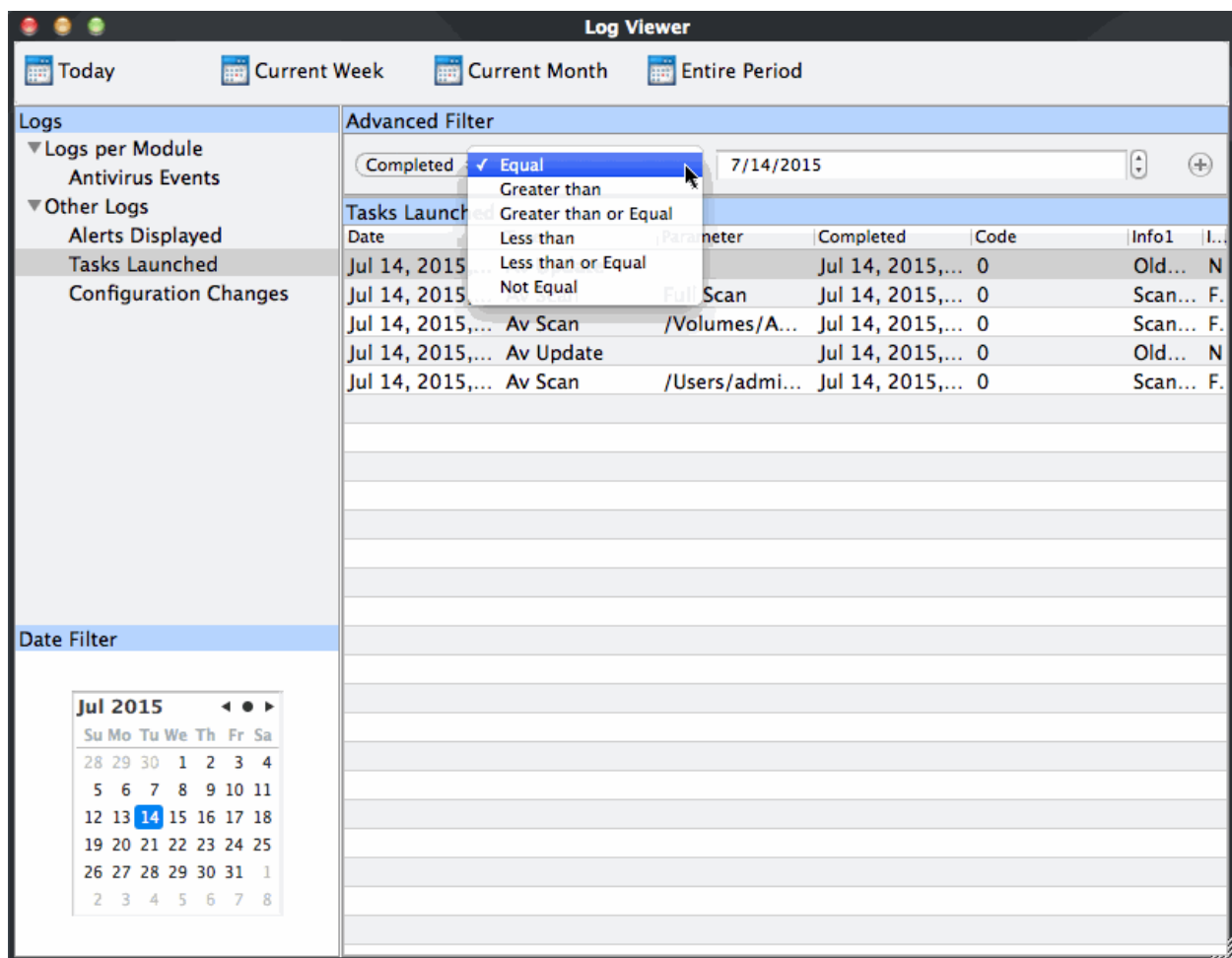


- a. Select the options from the drop-down box. 'Not Equal' will invert your selected choice. The available are:
 - Equal
 - Greater then
 - Greater than or Equal
 - Less then
 - Less than or Equal
 - Not Equal

- b. Enter the code or a part of it as your filter criteria in the text field.

For example if you have chosen 'Equal' from the drop-down and entered '0x00000001' in the text field, then only the log entries with the value 0x00000001 in the code column will be displayed.

ii. Completed: The 'Completed' option enables you to filter the log entries based on the completion dates of the Tasks. Selecting the 'Completed' option displays a drop-down box and date entry field.



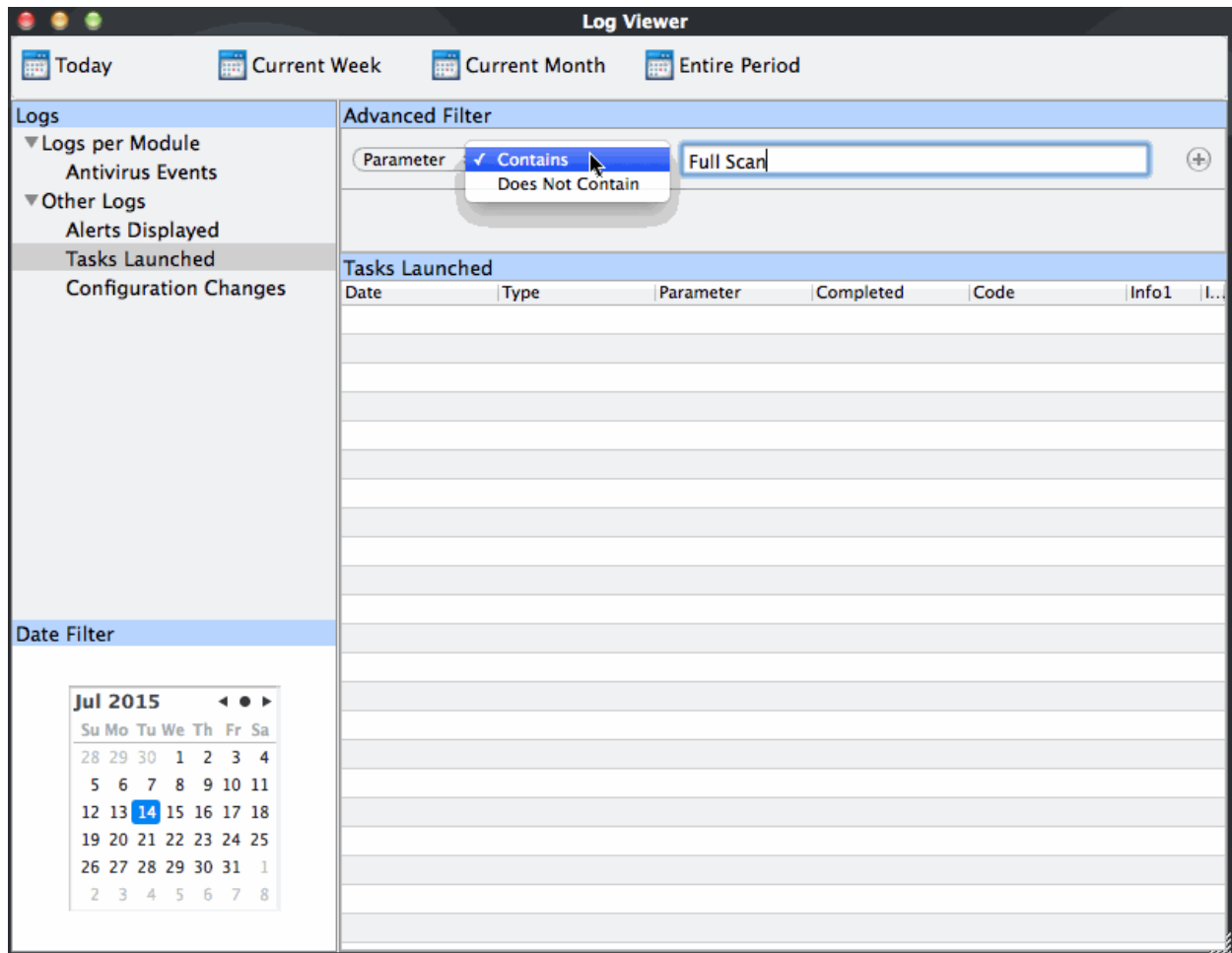
- a. Select any one of the following option the drop-down box.

- Equal
- Greater then
- Greater than or Equal
- Less then
- Less than or Equal
- Not Equal

- b. Enter the date by selecting it from the calender displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '07/14/2015', only the log of Tasks completed on 07/14/2015 will be displayed.

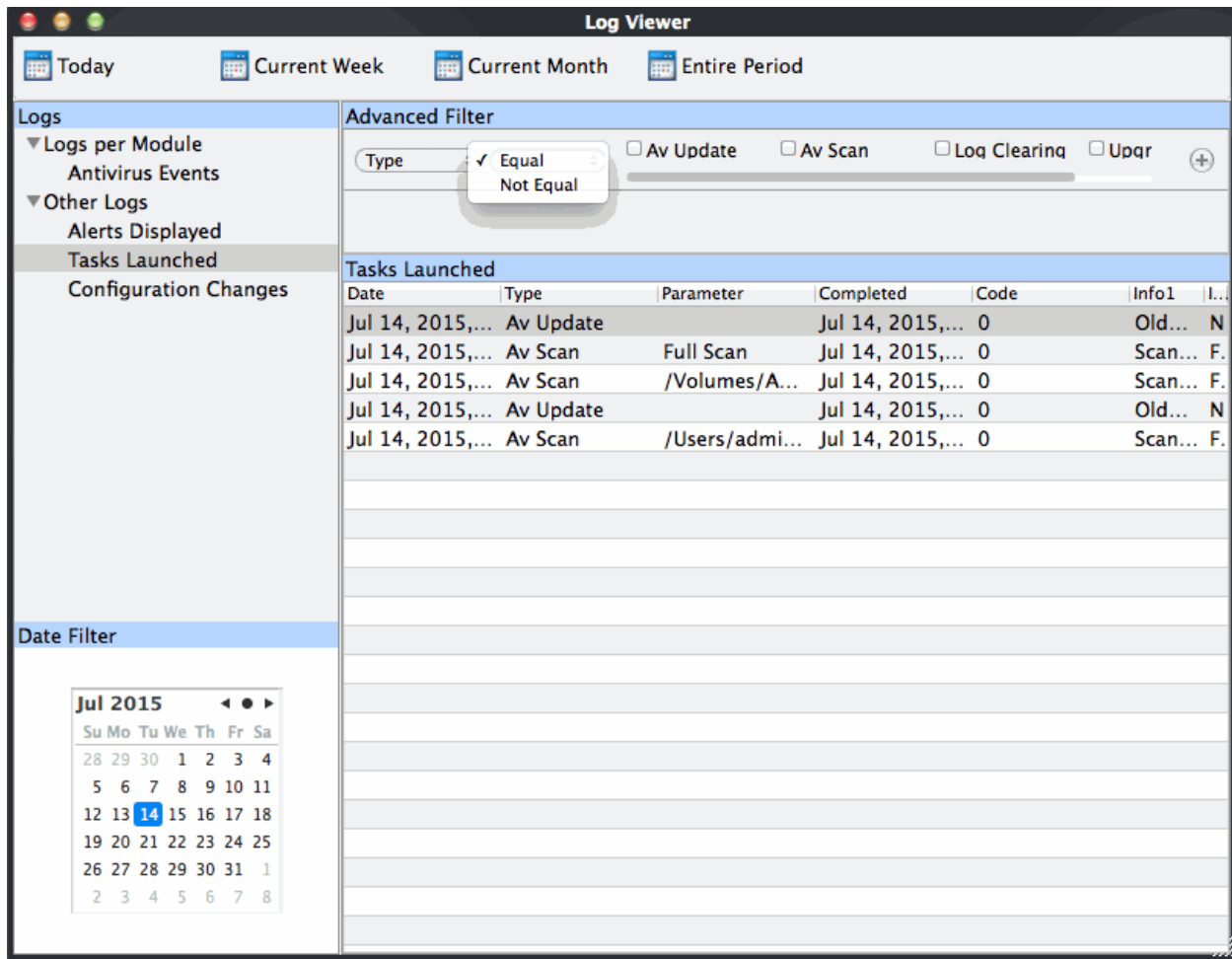
iii. Parameter: The Parameter option enables you to filter the entries based on the parameters like scan locations, associated with the Task.





- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Full Scan' in the text field, then only the entries of Antivirus Scan Tasks with the scan parameter 'Full Scan' will be displayed.

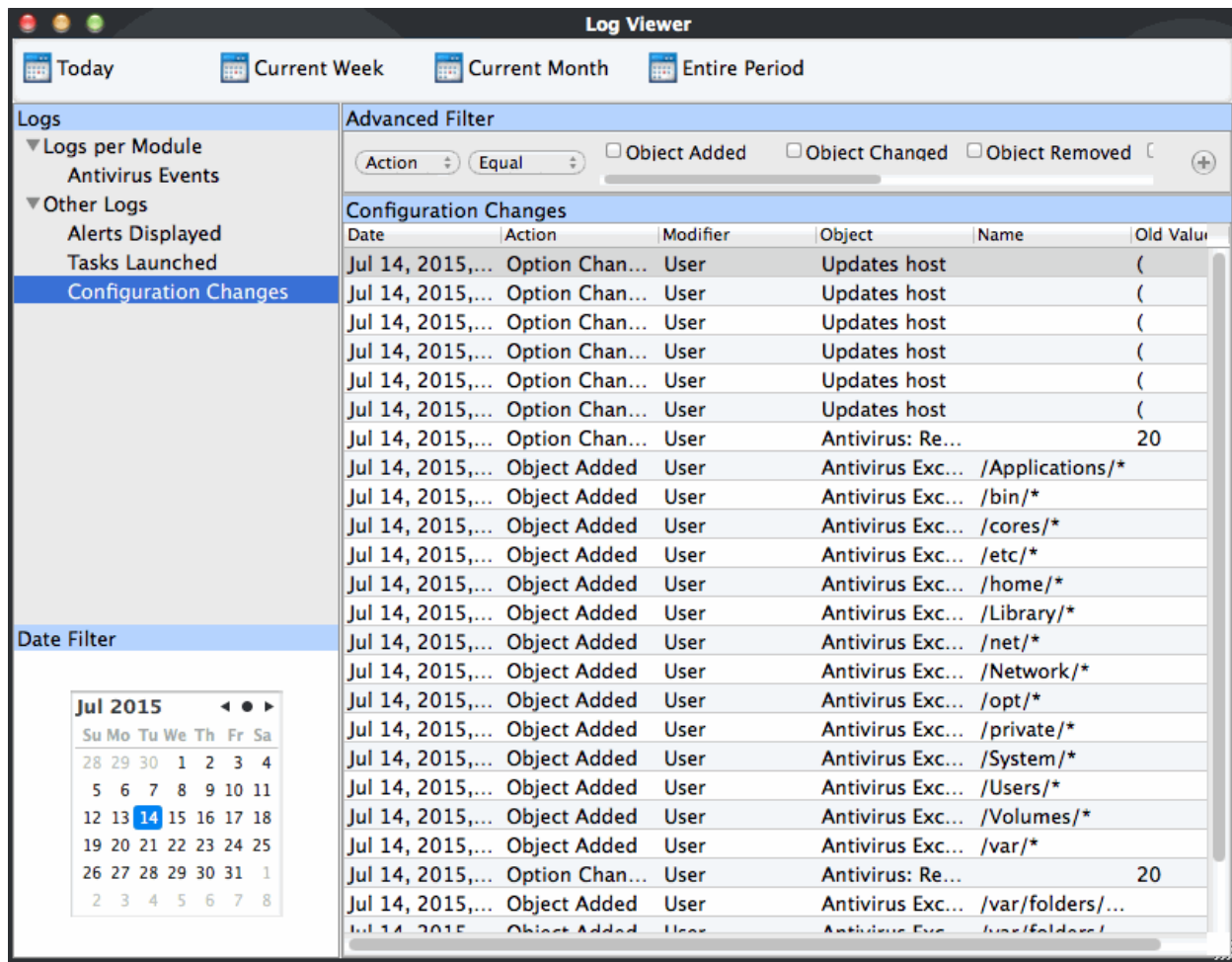
iv. Type: The 'Type' option enables you to filter the entries based on the type of Tasks launched. Selecting the 'Type' option displays a drop down menu and a set of specific task types that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - AV Update
 - AV Scan
 - Log Clearing
 - Upgrade
- You can add more filter types in the 'Advanced Filter' pane by clicking  the button at the top right of the filter pane.
- You can also remove a filter type by clicking the  button at the top right of the filter pane.
- Only those entries selected based on your set filter criteria will be displayed in the log viewer.

3.8.4. Configuration Changes

- Click 'More' on the 'CAV' home screen
- Click 'View Logs' > 'Other Logs' > 'Configuration Changes'
- You can create custom views of all logged events
- CAV keeps track of all the changes made to its configuration since its installation.
- The 'Configuration Changes' log viewer displays a list of changes to various options and other configuration changes made to the application.



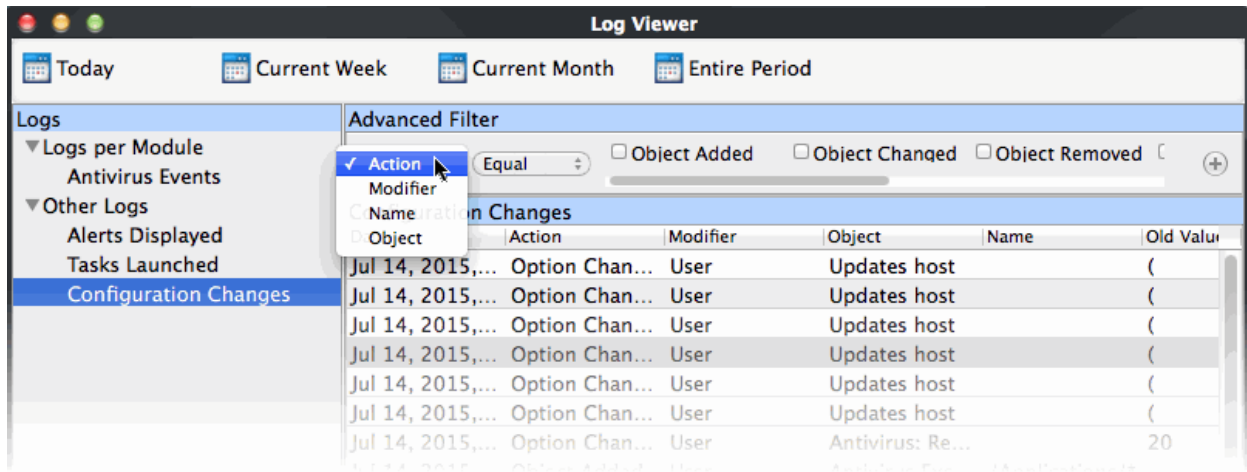
Column Descriptions

1. **Date** - Contains precise details of the date and time of the configuration change.
2. **Action** - Indicates the nature of the configuration change.
3. **Modifier** - Indicates the user that has made the configuration change.
4. **Object** - Indicates the CAV object that was affected by the configuration change.
5. **Name** - Indicates the name of the rule, program or the file that has been changed.
6. **Old value** - Indicates the value of the parameter before the configuration change.
7. **New value** - Indicates the value of the parameter after the configuration change.

3.8.4.1. Filter 'Configuration Changes' Logs

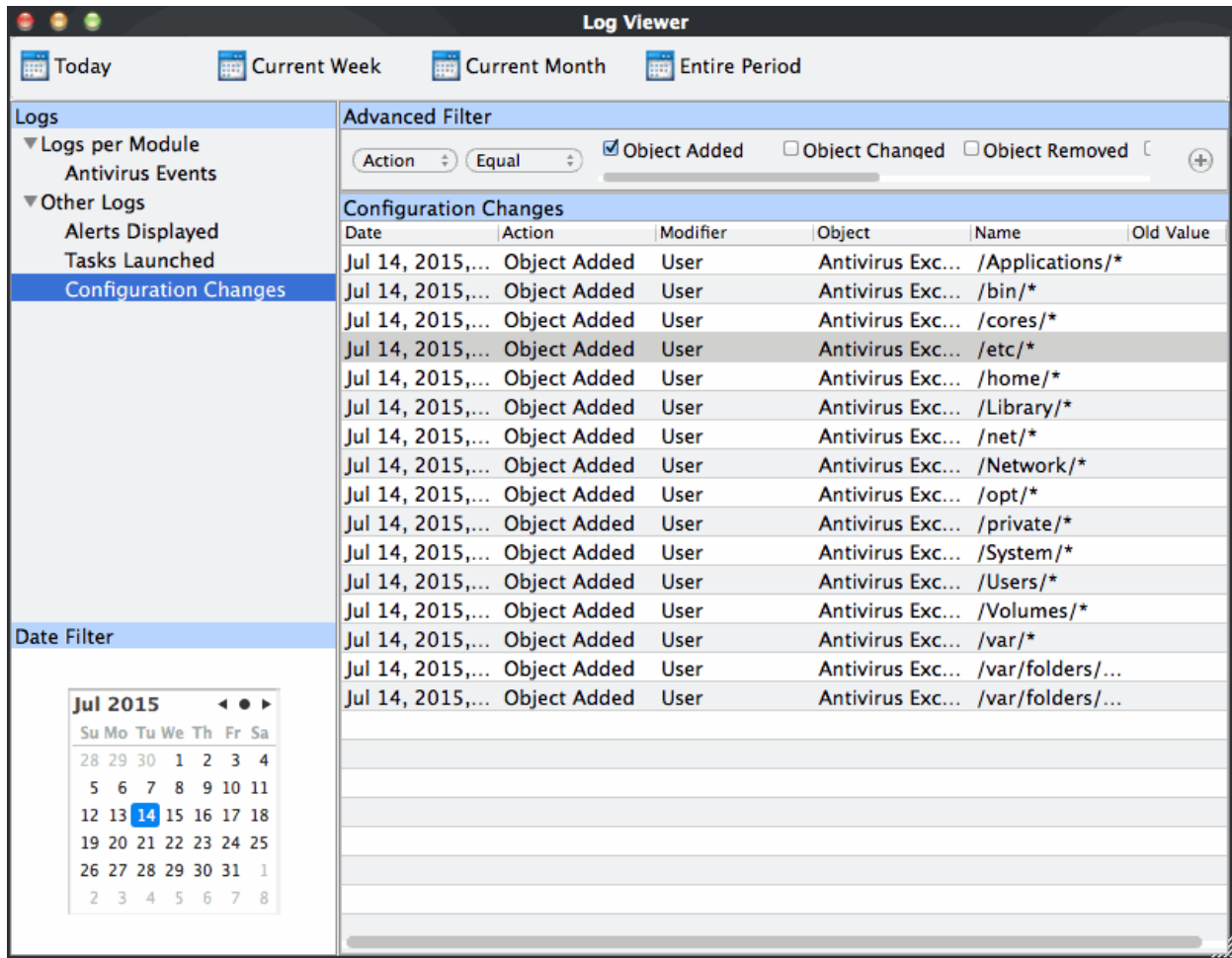
- Click 'More' on the 'CAV' home screen
- Click 'View Logs' > 'Other Logs' > 'Configuration Changes'
- You can create custom views of all logged events
- Comodo Antivirus for MAC allows you to create custom views of all logged events according to user defined criteria.
- From 'Configuration Changes' interface, you can chose the category of filter from a drop down box.

- Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.
1. Click 'Advanced Filter' drop-down when you have chosen the category upon which you wish to filter.



- You have 4 categories of filter that you can add.
- You can chose the category of filter from the 'Advanced Filter' drop-down.
- Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by entering a filter string in the field provided.
- Following are the options available in the drop down menu:

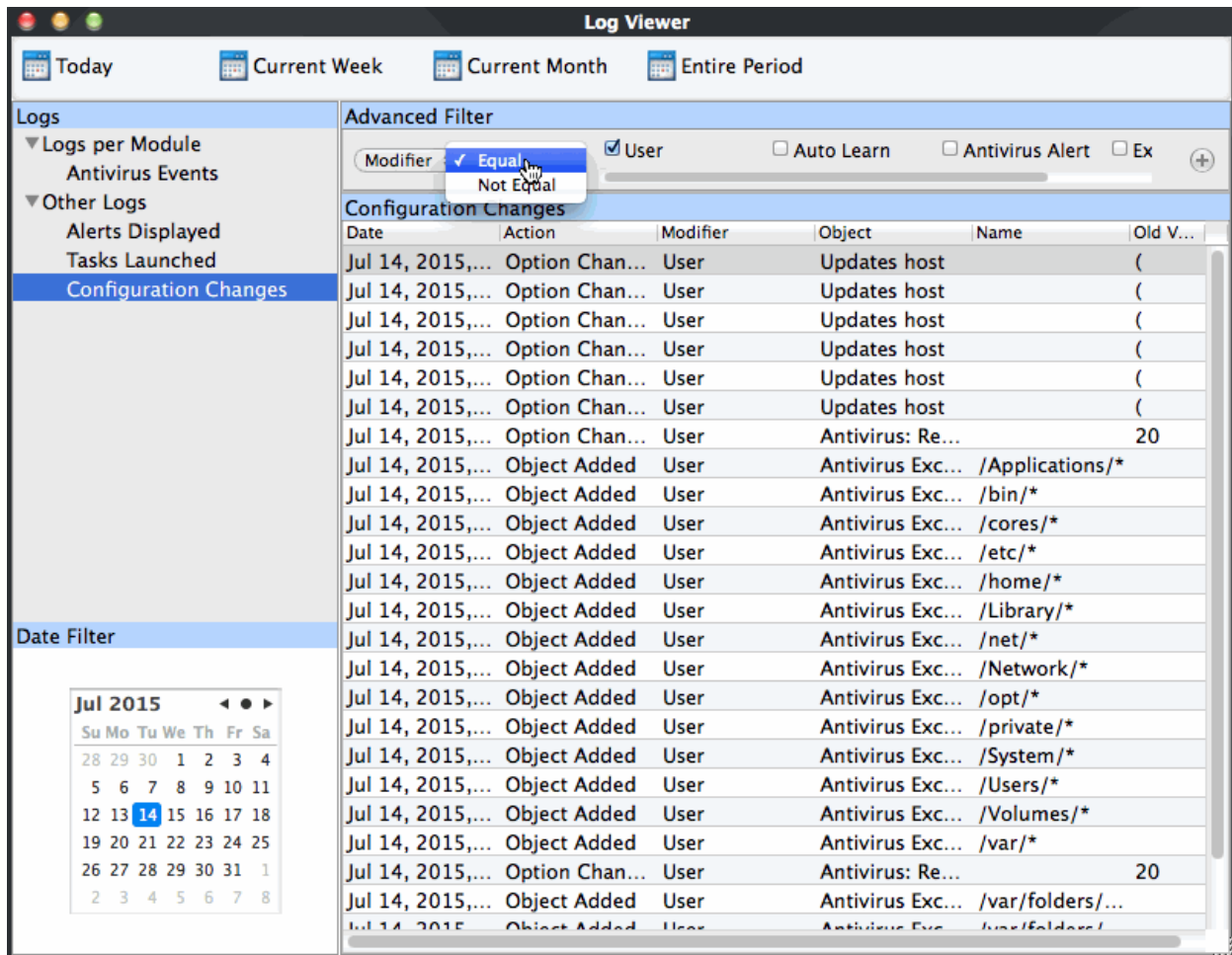
i. Action: The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
 - Object Added
 - Object Changed
 - Object Removed
 - Option Changed
 - String Added
 - String Removed

For example, if you choose Equal in the drop-down and select 'Object Added' checkbox, then, only the log entries with the value 'Object Added' in the 'Action' column will be displayed.

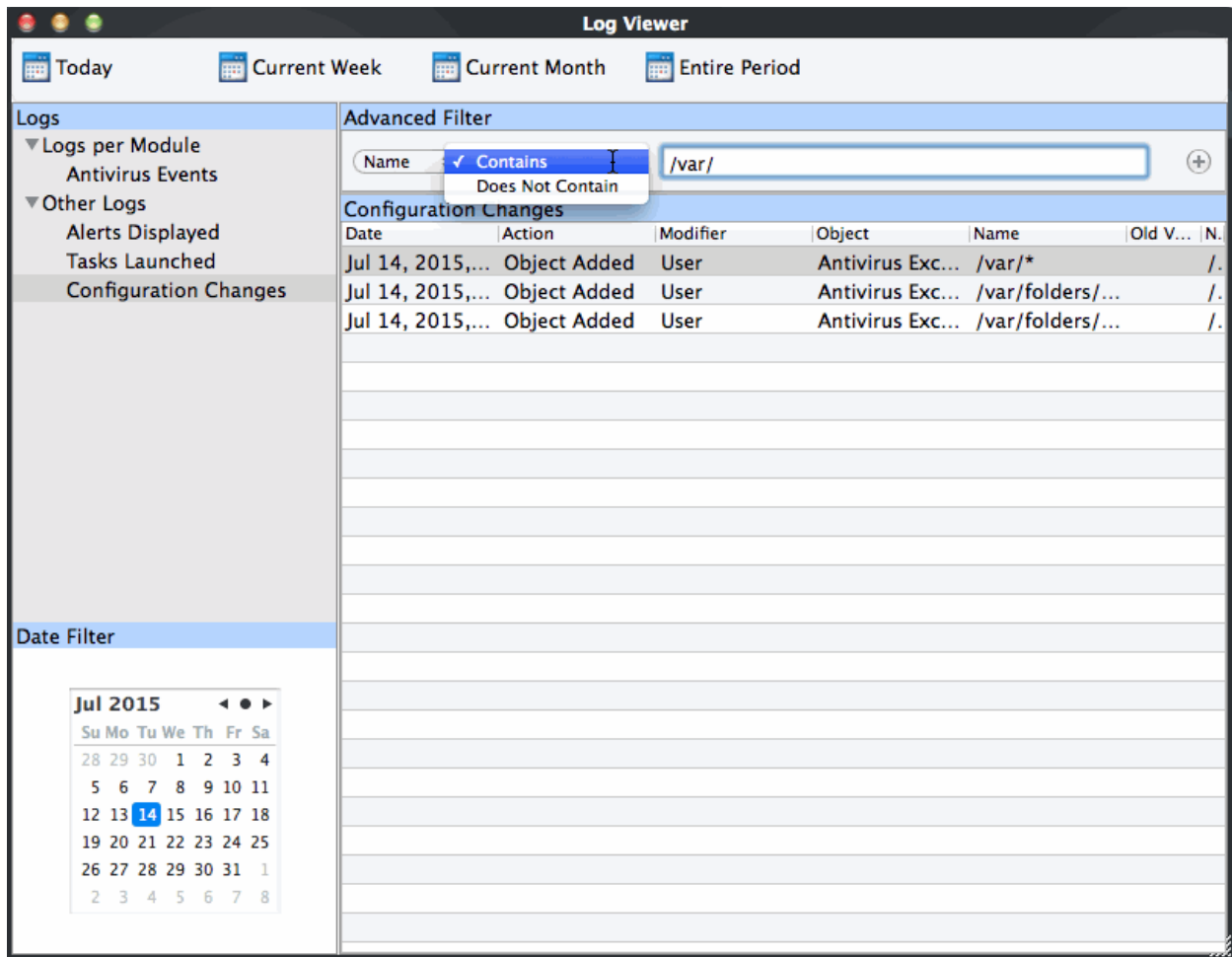
ii. Modifier: The 'Modifier' option allows you to filter the log entries based on the entity that is responsible for the configuration change. It can be the user or the response given to an alert. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:
 - User
 - Auto Learn
 - Antivirus Alert
 - Execution Alert

For example, if you have chosen Equal in the drop-down and selected 'User' checkbox, then, only the log entries related to the configuration changes effected by responses to 'User' will be displayed.

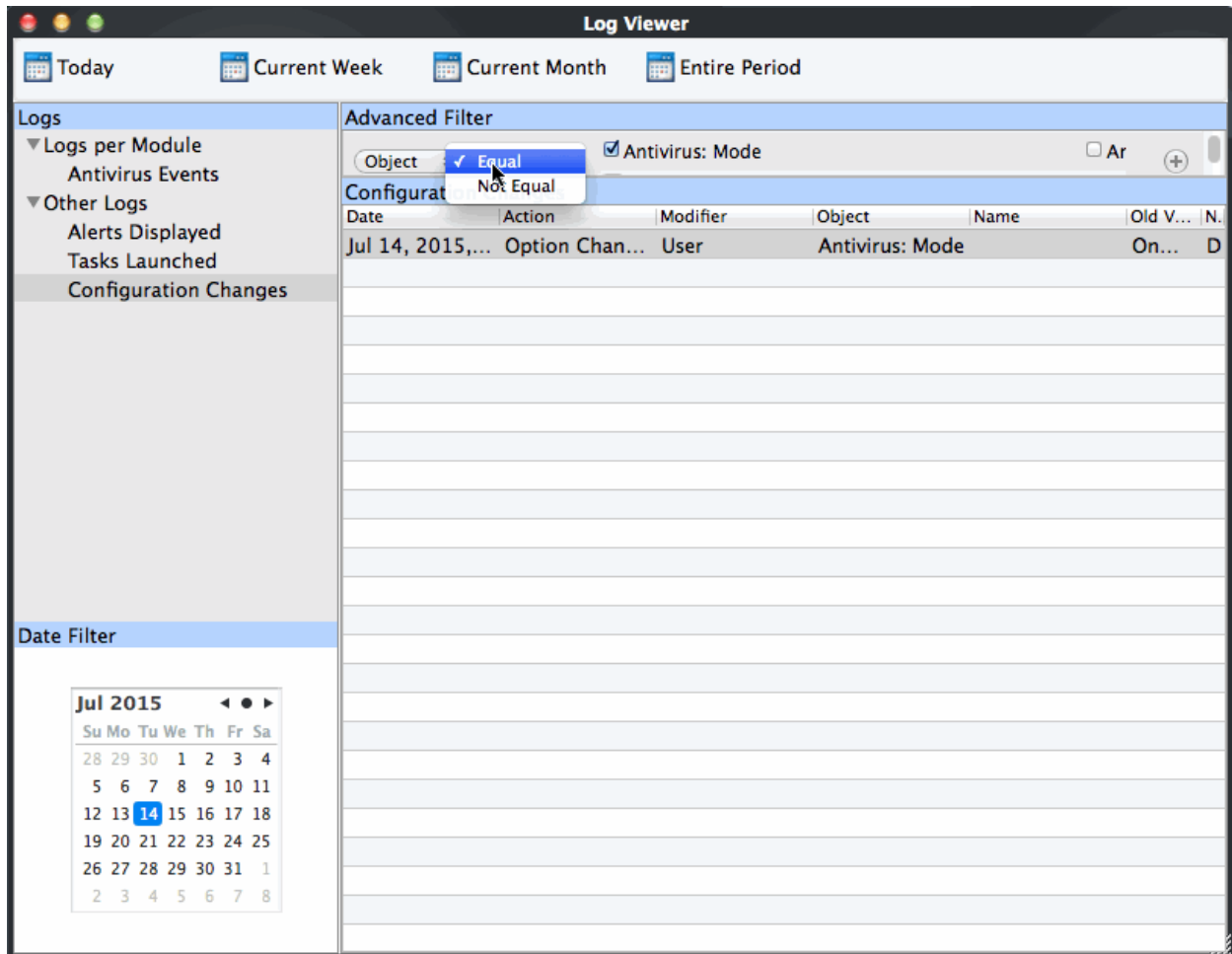
- iii. **Name:** The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the name of the change, partly or fully as filter criteria in the text box.



For example, if you choose 'Contains' option from the drop-down and enter the phrase '/var/' in the text field, then only the log entries containing the /var/ in the name column will be displayed.

iv. Object: The 'Object' option enables you to filter the log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays a drop down menu and the objects of CAV configuration, that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- Now select the check-boxes of the specific objects as filter parameters to refine your search. Use toggle to move forward/backward to to see all the parameters options.

For example, if you have chosen 'Equal' from the drop-down and selected 'Antivirus: Mode' checkbox, only the log entries related to the change of Antivirus mode will be displayed.

- You can add more filter types in the 'Advanced Filter' pane by clicking  the button at the top right of the filter pane.
- You can also remove a filter type by clicking the  button at the top right of the filter pane.
- Only those entries selected based on your set filter criteria will be displayed in the log viewer.

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