COMODO
Creating Trust Online®

Comodo
Client - Security for MAC

Software Version 2.4

User Guide

Guide Version 2.4.071619

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

Table of Contents

1. Introduction to Comodo Client - Security for MAC

Comodo Client - Security (CCS) for MAC offers complete protection against viruses, worms and Trojan horses for MAC OS X based computers. The software is easy to use and features real-time virus monitoring, full event logs, cloud-based analysis of unknown files and more.

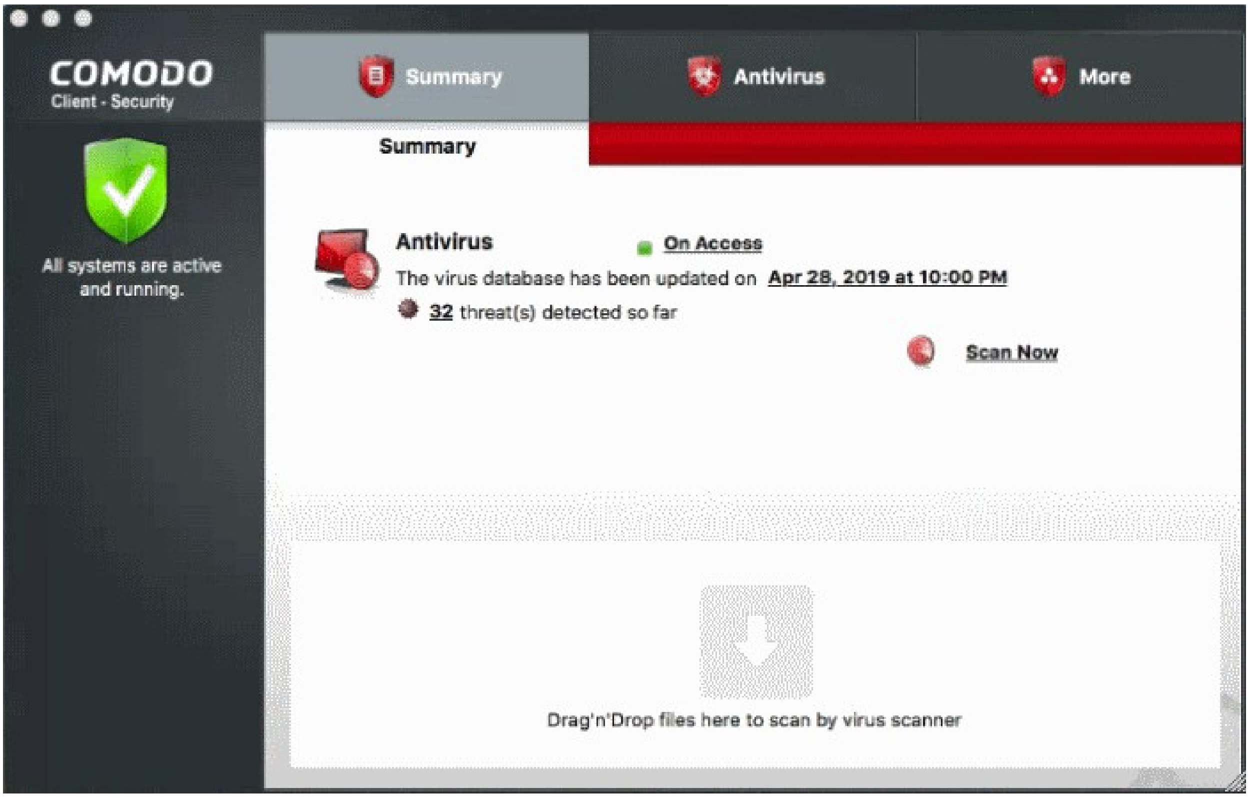
- To run a virus scan, click the 'Scan Now' link on the summary screen.
- To scan individual items:
  - Drag them into the scan box in the 'Summary' area

OR

  - Drag them onto the Comodo dock icon

Features at a glance

- Detects, blocks and eliminates viruses from desktops and networks
- Constantly protects you with real-time and on-access scanning
- Scheduler allows you to run scans at a time that suits you
- Automatically runs unknown files inside a secure container which is isolated from the rest of your computer
- Daily, automatic updates of virus definitions
- Simple to use: install and forget while CSS protects you in the background



Antivirus On Access

The virus database has been updated on Apr 28, 2019 at 10:00 PM

32 threat(s) detected so far

COMODO
Client - Security
Summary
Antivirus
More
Summary
All systems are active and running.
Scan Now
Drag'n'Drop files here to scan by virus scanner

Guide Structure

This guide explains the basic usage of CCS to Endpoint Manager admins and end-users.

  - **Introduction to Comodo Client - Security**

1.1. System Requirements

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

CSS for MAC solution should be compatible with the following hardware platforms:

- Mac Intel x86_64

Operating systems:

- Mac OS X 10.11.x
- Mac OS X 10.12.x
- Mac OS X 10.13.x

1.2. Install Comodo Client - Security for MAC

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

This section covers how to:

- **Subscribe for Endpoint Manager**
- **Enroll users**
- **Add Devices**
- **Deploy CCS on Mac endpoints**

Skip to straight to **Deploy CCS** if you have already completed the first three steps.

Subscribe for Endpoint Manager

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

- Dragon / C1 -
  - Sign up for Dragon at **https://platform.comodo.com/signup**, or C1 at **https://one.comodo.com/signup**
  - After sign-up, login to the portal then click 'Applications > 'Endpoint Manager'.
- Stand-alone Endpoint Manager
  - Visit **https://secure.comodo.com/home/purchase.php?pid=98&license=try** for the trial version or **https://secure.comodo.com/home/purchase.php?pid=98** for the full version.
  - After sign-up, you can access your Endpoint Manager at the URL provided during setup.

Enroll Users

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

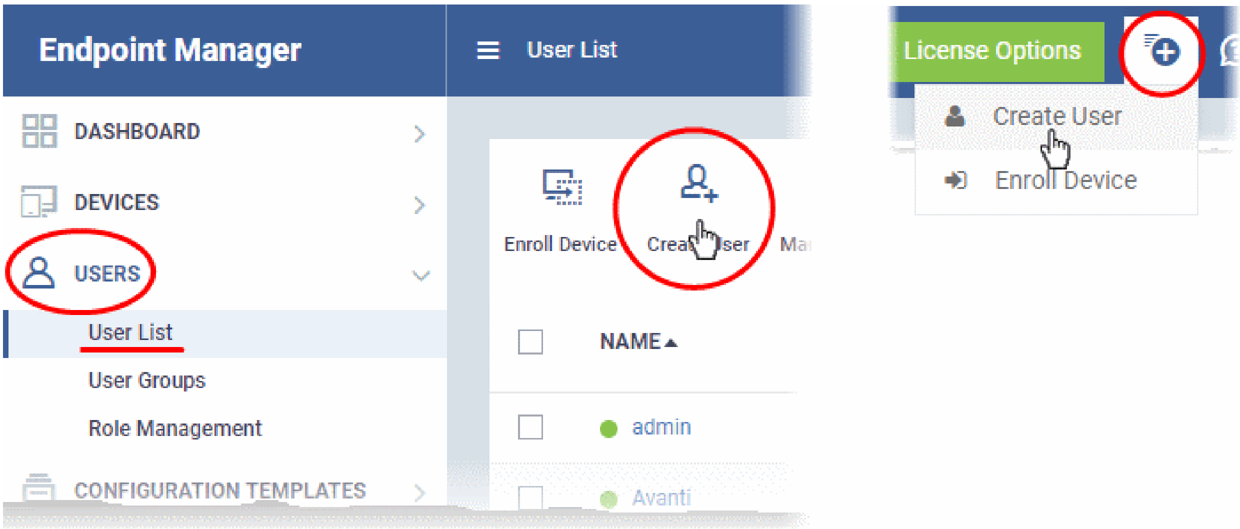
- **Dragon MSP / C1 MSP customers -** You can create multiple companies and can enroll users to any of them.
- **Dragon Enterprise / C1 Enterprise, and stand-alone Endpoint Manager customers -** All users are enrolled to the default company.

Add a user

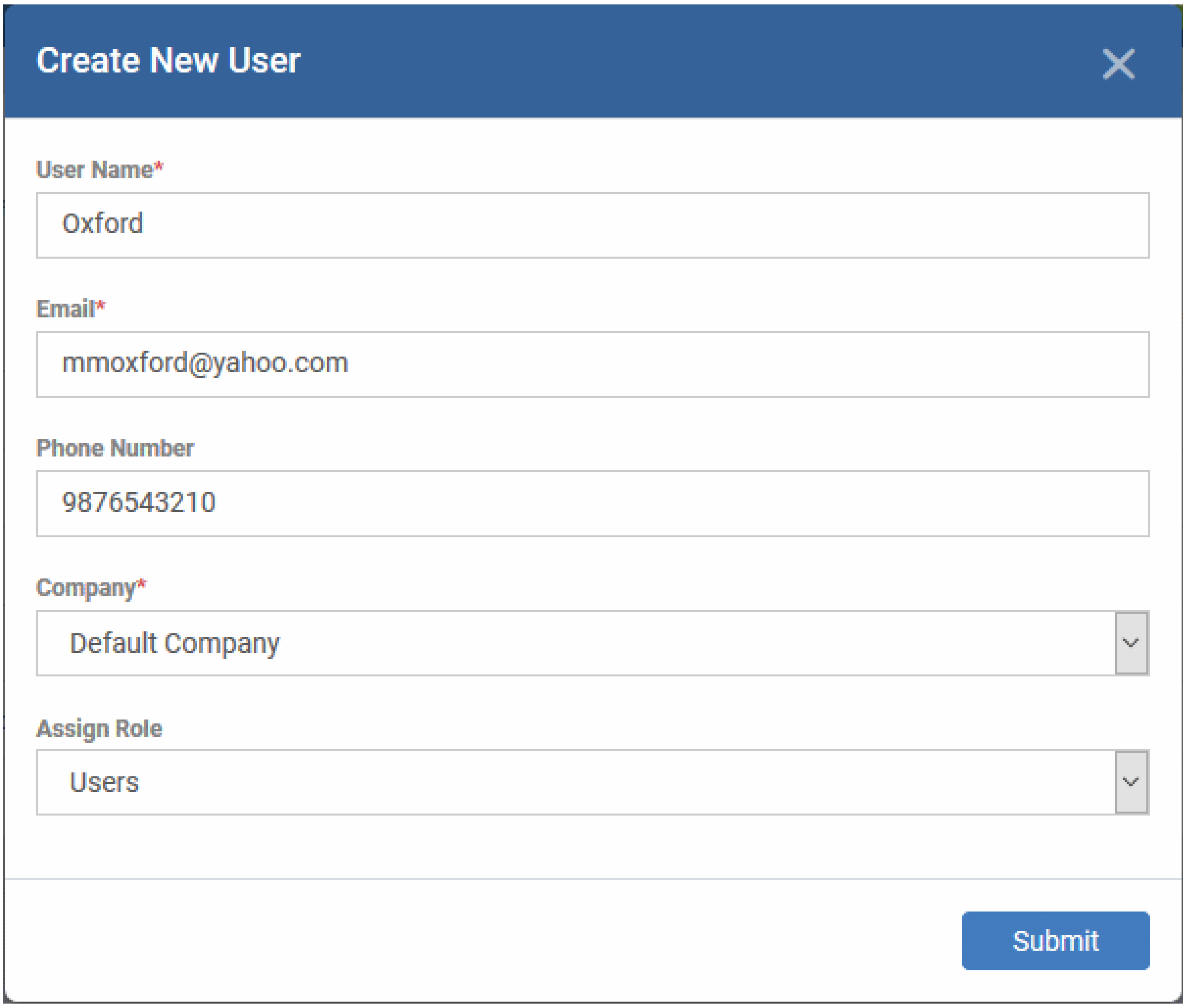
- Open Endpoint Manager
- Click 'Users' > 'User List'
- Click 'Create User'

  or

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



The create user form will open:



Create New User

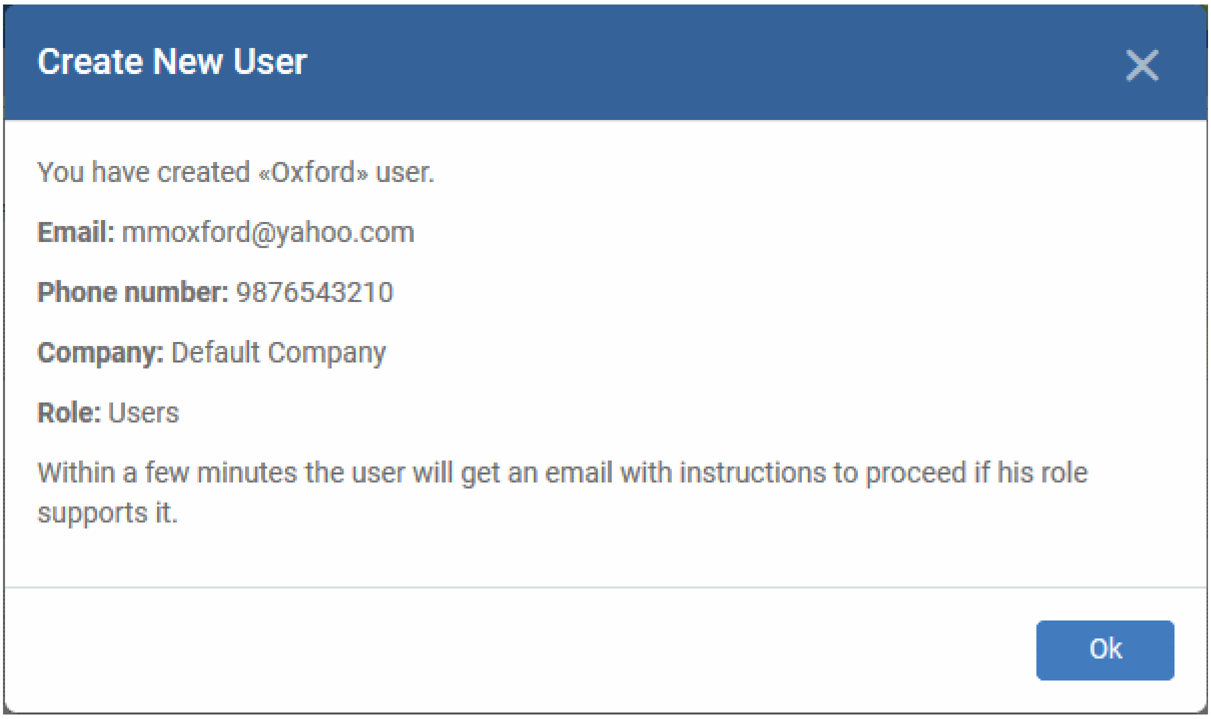
User Name*	Oxford
Email*	mmoxford@yahoo.com
Phone Number	9876543210
Company*	Default Company
Assign Role	Users

Submit

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

- **Company -** The organization to which you want to add the user.
- **Assign Role -** A role determines user permissions within the Endpoint Manager console itself. EM ships with two default roles:
  - **Administrators -** Full privileges in the EM console. The permissions for this role are not editable.
  - **Users -** In most cases, a user will simply be an owner of a managed device and should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

You should see the following confirmation message:



Create New User

You have created «Oxford» user.

Email: mmoxford@yahoo.com

Phone number: 9876543210

Company: Default Company

Role: Users

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

- Repeat the process to add more users.
- New users will be listed in 'Users' > 'User List'

Tip: You can also import a list of users from a .csv file, and bulk enroll users/endpoints from Active Directory (AD). See **https://help.comodo.com/topic-399-1-786-10125-Create-New-User-Accounts.html** if you want to learn more about these options.

Enroll Devices

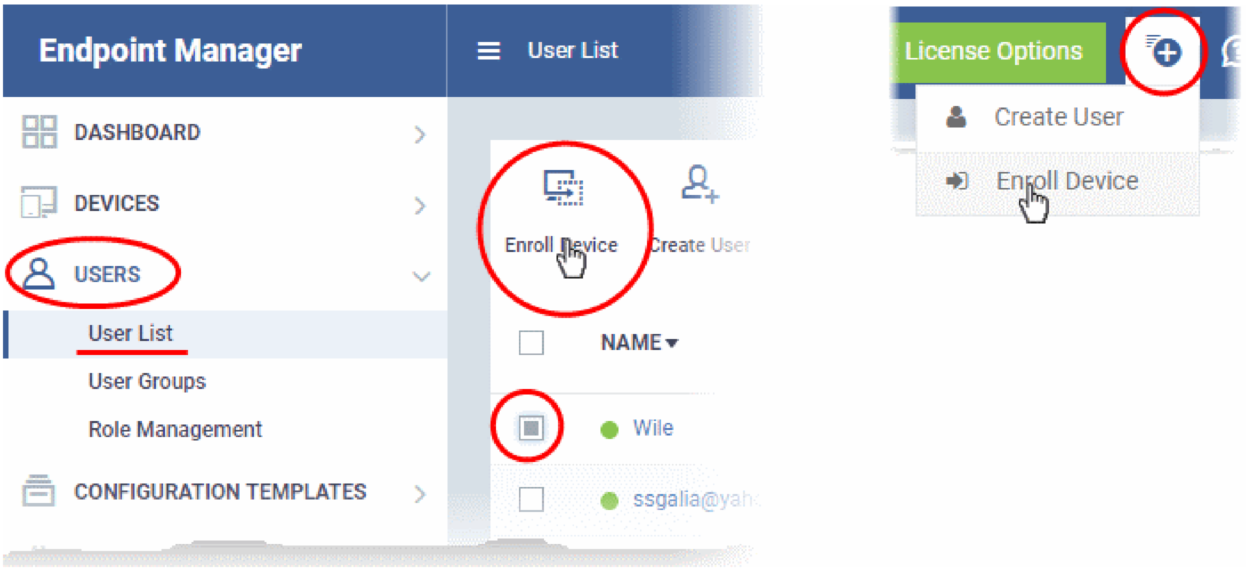
The next step is to add devices which belong to your users. You can then manage the devices using Endpoint Manager.

Enroll devices

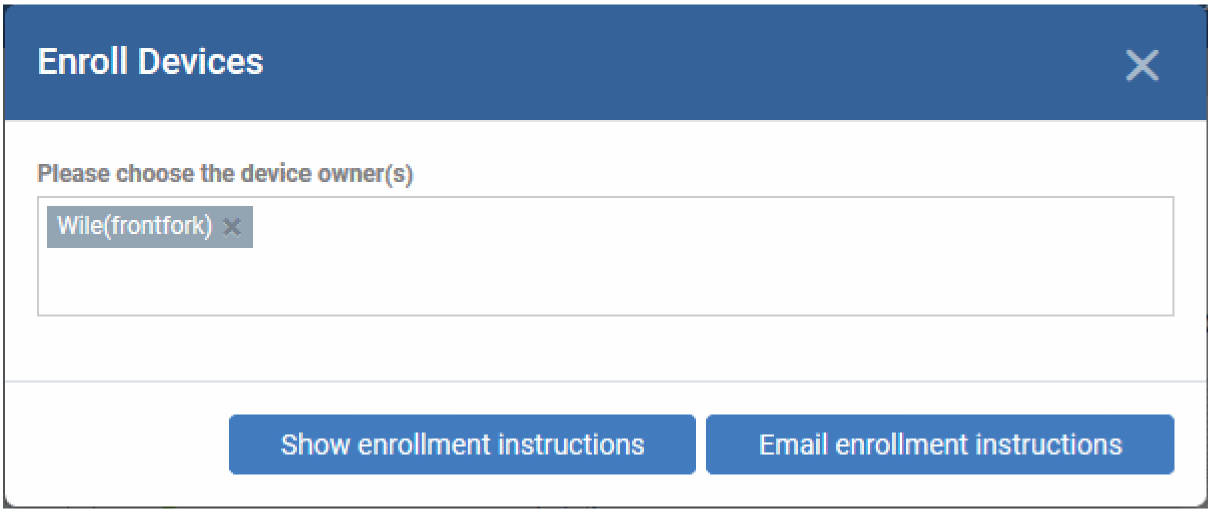
- Click 'Users' > 'User List'
- Select users for whom you want to enroll devices
- Click the 'Enroll Device' button above the table

  Or

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

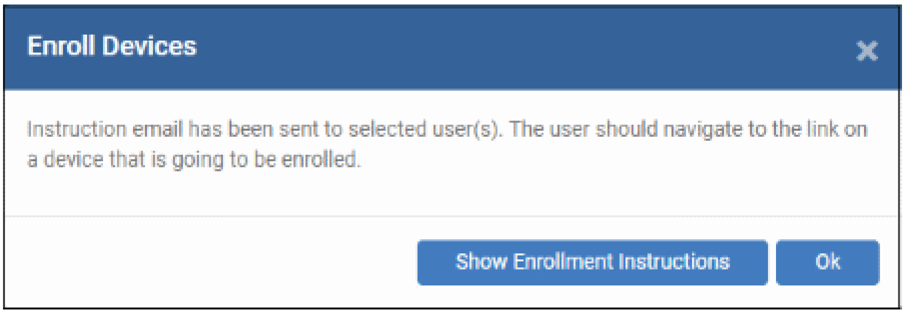


The 'Enroll Devices' dialog will open:


Enroll Devices
Please choose the device owner(s)
Wile(frontfork)
Show enrollment instructions
Email enrollment instructions

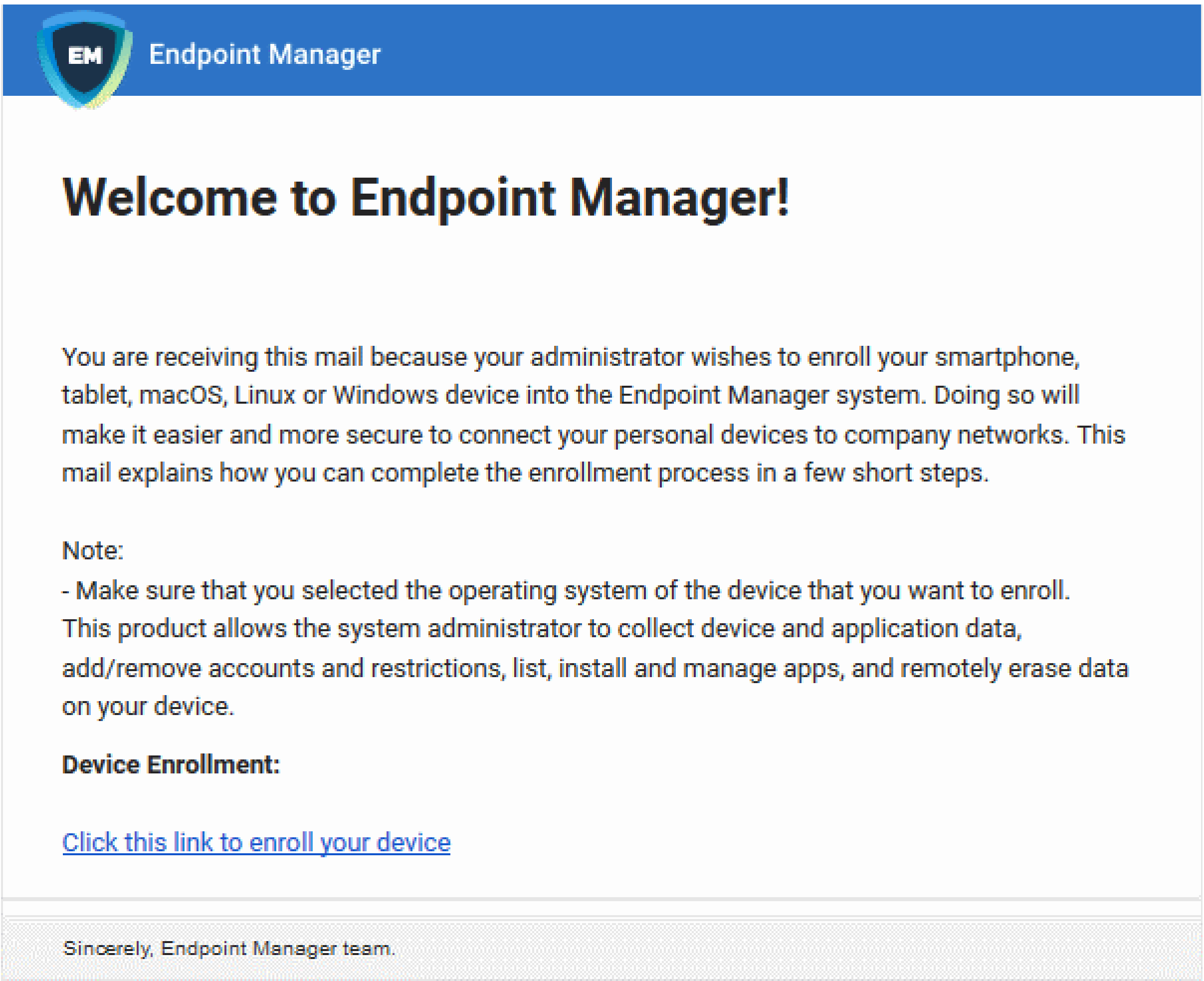
The device owners field is pre-populated with the users you selected in the previous step.

- To add more users, start typing first few letters of their username and choose from the results
- **Show Enrollment Instructions -** Show advice on how to add a device in a pop-up window. Useful for admins who want to enroll their own devices.
- **Email Enrollment Instructions -** Send device enrollment instructions to all selected users. Users must enroll their own devices by following the instructions in the email. The following confirmation is shown after clicking this button:



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

An example mail is shown below:



Endpoint Manager

Welcome to Endpoint Manager!

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

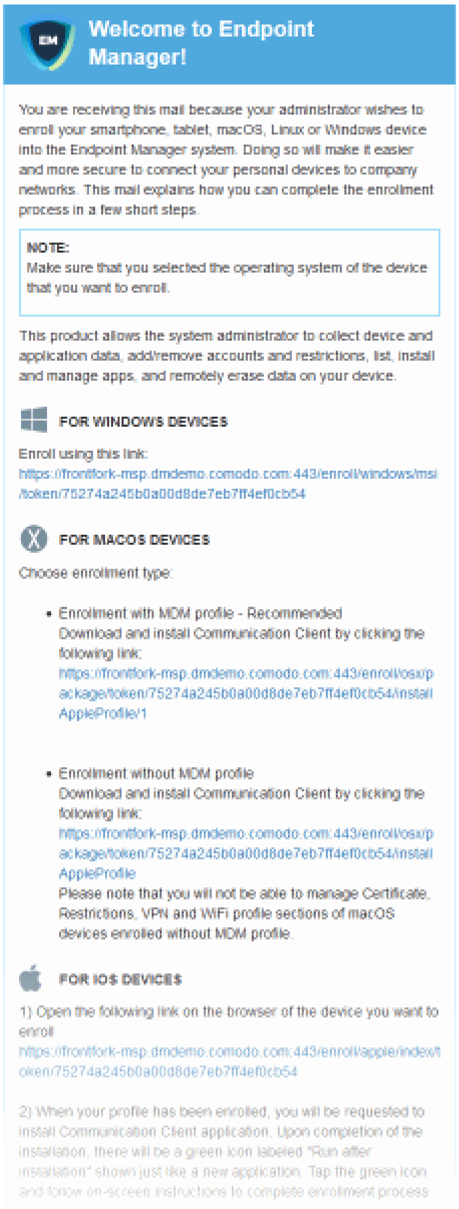
Note:
- Make sure that you selected the operating system of the device that you want to enroll.
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Device Enrollment:

Click this link to enroll your device

Sincerely, Endpoint Manager team.

- The link takes the user to a page which lets them download the communication client and profile:



Welcome to Endpoint Manager!

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

NOTE:
Make sure that you selected the operating system of the device that you want to enroll.

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

FOR WINDOWS DEVICES

Enroll using this link:
https://frontfork-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/75274a245b0a00d8de7eb7ff4ef0cb54

FOR MACOS DEVICES

Choose enrollment type:

- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

FOR IOS DEVICES

1) Open the following link on the browser of the device you want to enroll
https://frontfork-msp.dmdemo.comodo.com:443/enroll/apple/index/token/75274a245b0a00d8de7eb7ff4ef0cb54

2) When your profile has been enrolled, you will be requested to install Communication Client application. Upon completion of the installation, there will be a green icon labeled "Run after installation" shown just like a new application. Tap the green icon and follow on-screen instructions to complete enrollment process.

You can add MAC devices either with or without installing the Endpoint Manager (EM) profile.

- Background - Apple only allow one portal to manage network features on a MAC device. This causes issues with customers who want to use Endpoint Manager in conjunction with another management platform.
- 'Profile-less' enrollment lets you use EM to manage security/remote control while using another platform for general Mac management.
- However, you cannot use EM to manage certain items if you use profile-less enrollment. See the following table for details:

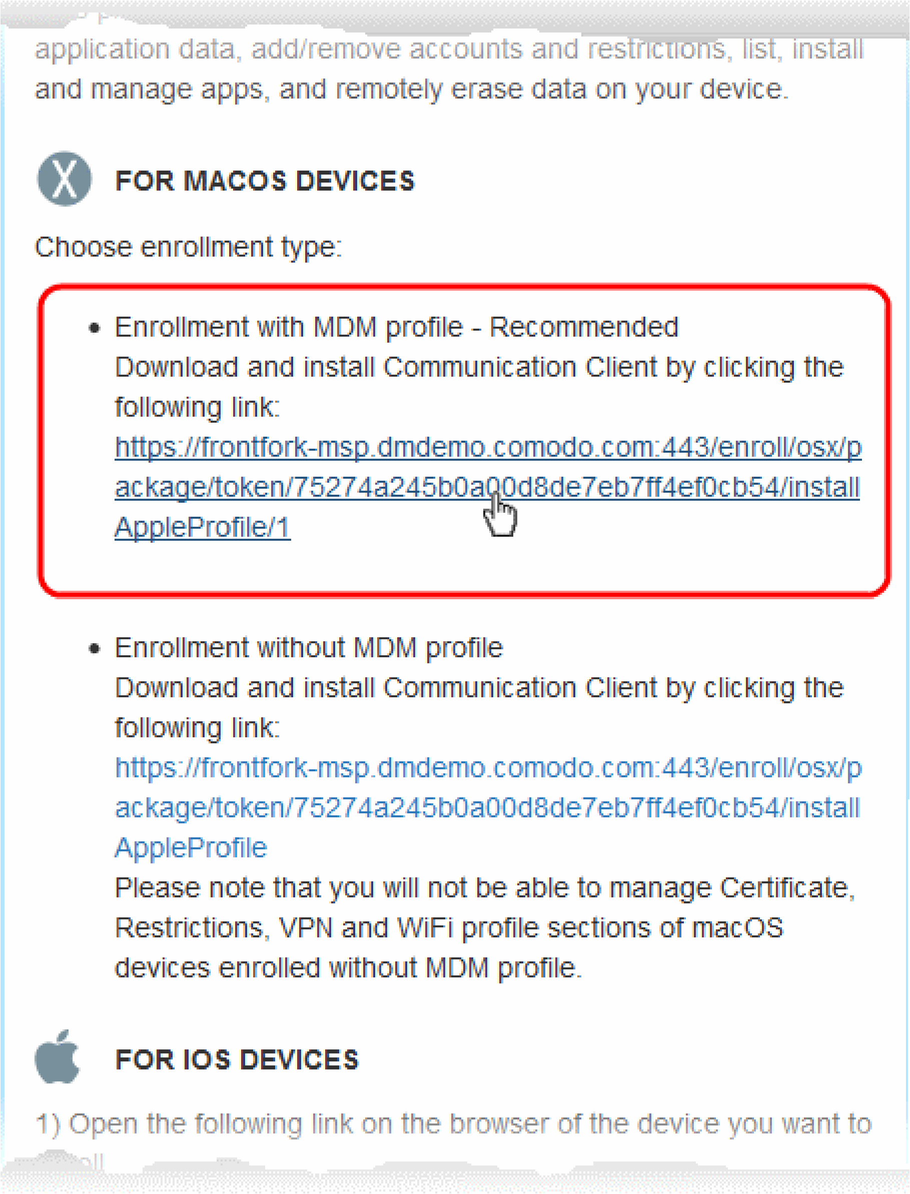
Enroll with MDM Profile	'Profile-less' enrollment
Use Endpoint Manager to manage: • Antivirus Settings • Remote Control Settings • Valkyrie Settings • Certificates	Use Endpoint Manager to manage: • Antivirus Settings • Remote Control Settings • Valkyrie Settings

• Restrictions • VPN • Wi-Fi	

- Click the following links for help with either method:
  - **Enroll with MDM Profile**
  - **Enroll without MDM Profile**

Enroll with MDM Profile

- Users should open the mail on the device you want to enroll
- They should scroll to the 'FOR MAC OS DEVICES' section.
- Click the 'Enrollment with MDM profile' link:



application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR MACOS DEVICES

Choose enrollment type:

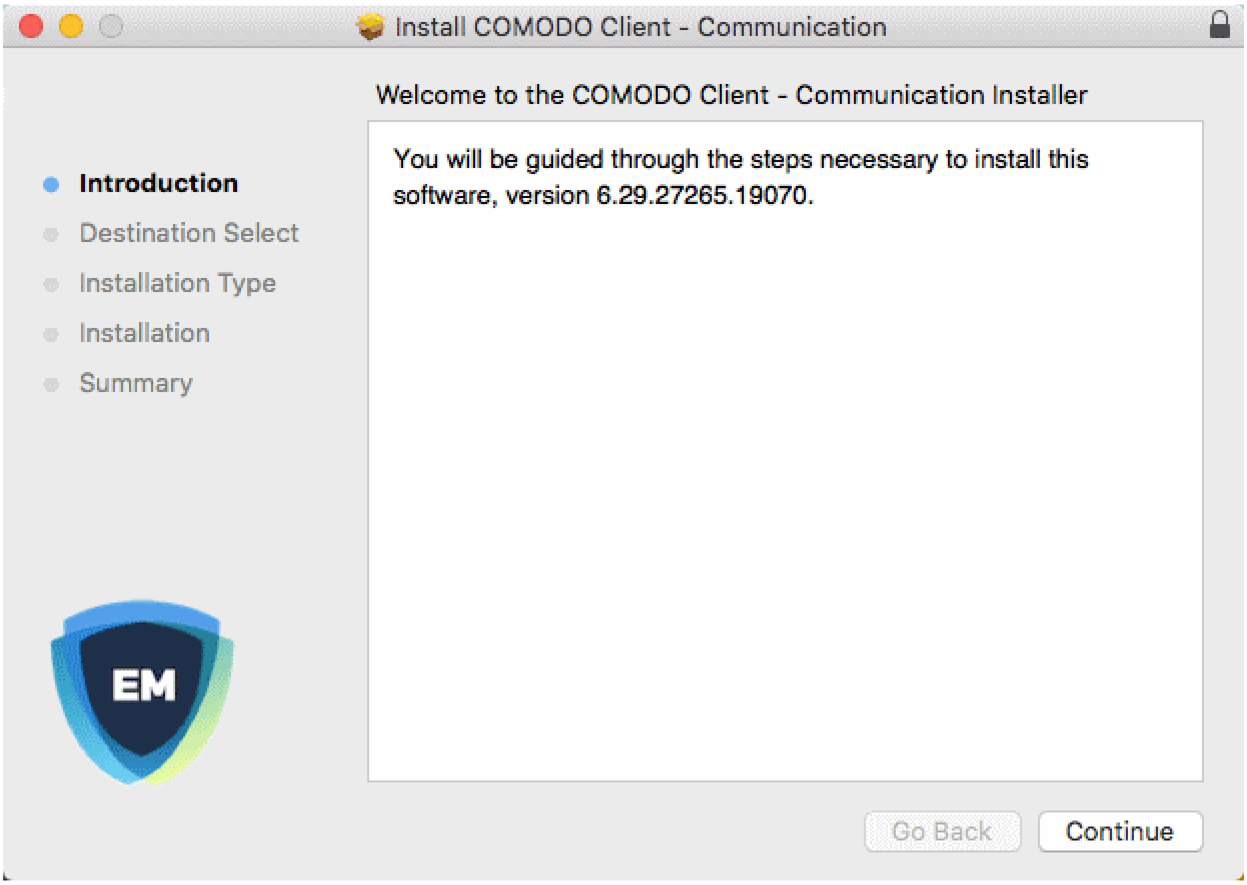
- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

FOR IOS DEVICES

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

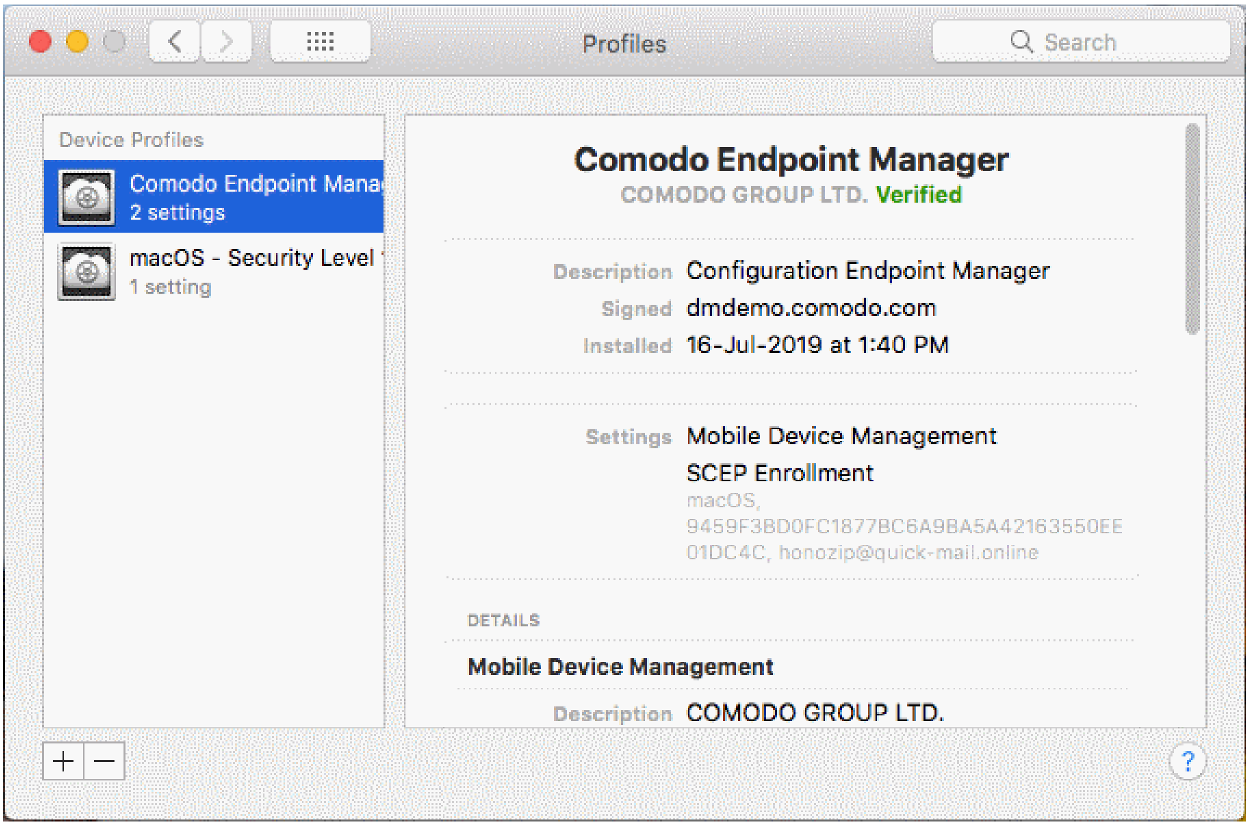
This will start the installation wizard:



Welcome to the COMODO Client - Communication Installer

You will be guided through the steps necessary to install this software, version 6.29.27265.19070.

- The user follows the wizard and completes the installation.
- The device profiles screen appears when installation is complete:



Comodo Endpoint Manager

COMODO GROUP LTD. Verified

Description Configuration Endpoint Manager

Signed dmdemo.comodo.com

Installed 16-Jul-2019 at 1:40 PM

Settings Mobile Device Management

SCEP Enrollment

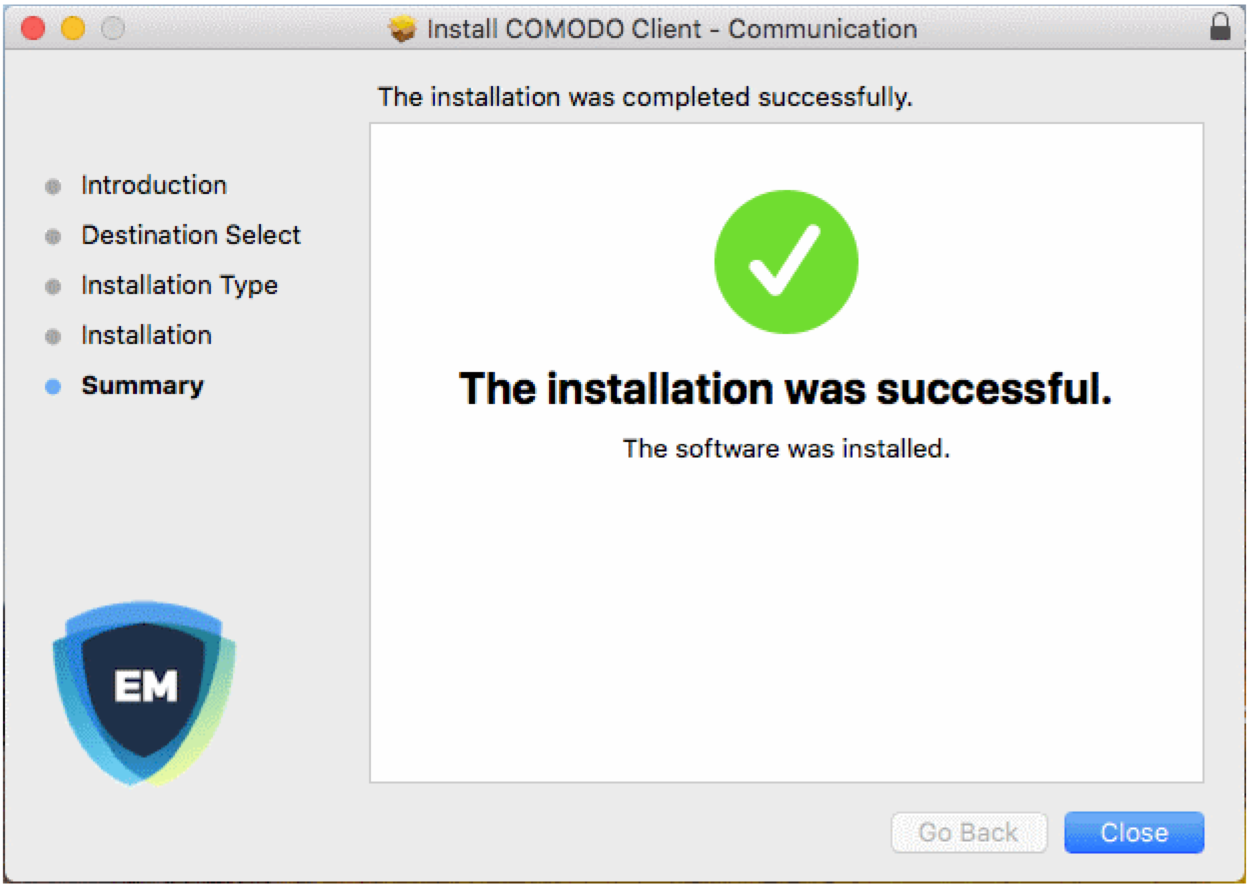
macOS, 9459F3BD0FC1877BC6A9BA5A42163550EE01DC4C, honozip@quick-mail.online

DETAILS

Mobile Device Management

Description COMODO GROUP LTD.

The client connects to the EM server:



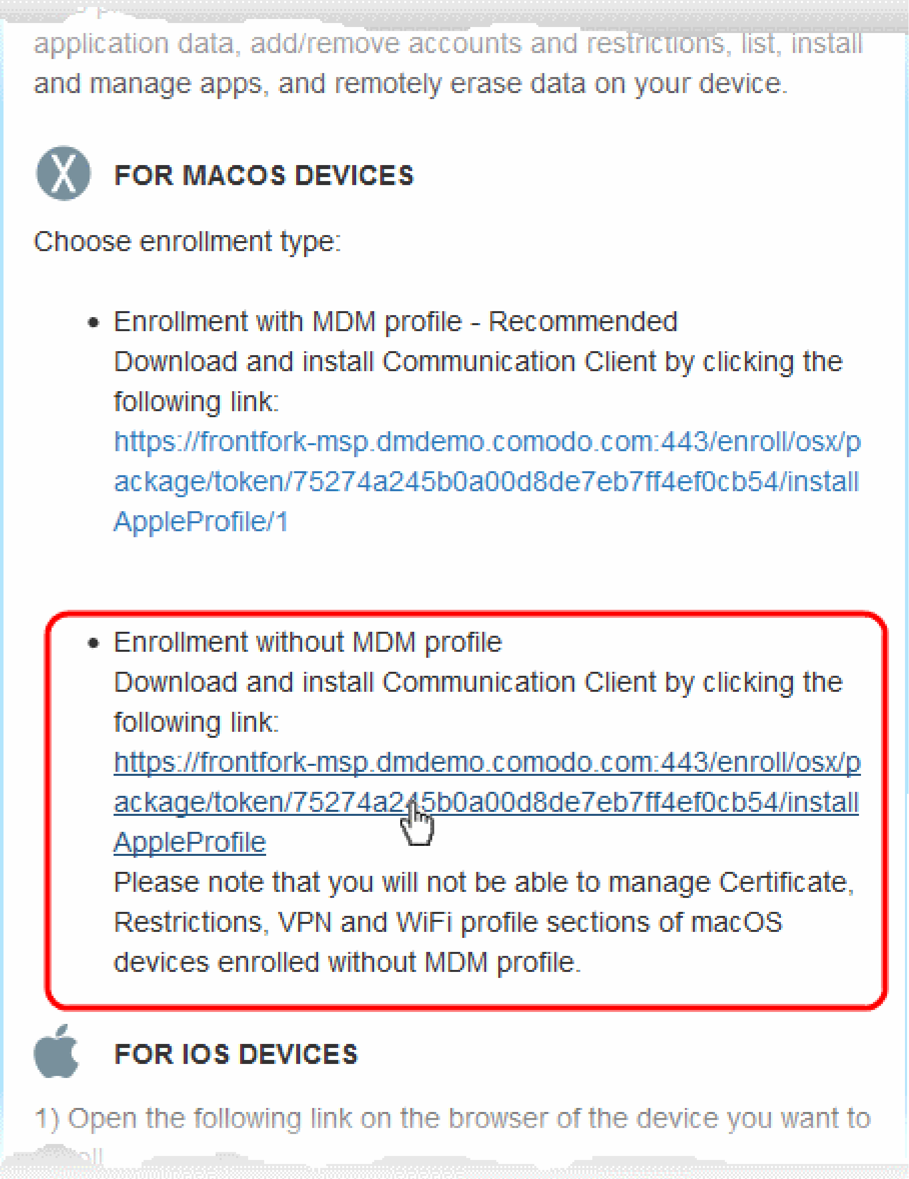
The installation was completed successfully.

The installation was successful.

The software was installed.

Enroll without MDM Profile

- Users should open the mail on the device you want to enroll
- They should scroll to the 'FOR MAC OS DEVICES' section.
- Click the 'Enrollment without MDM link:



application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

FOR MACOS DEVICES

Choose enrollment type:

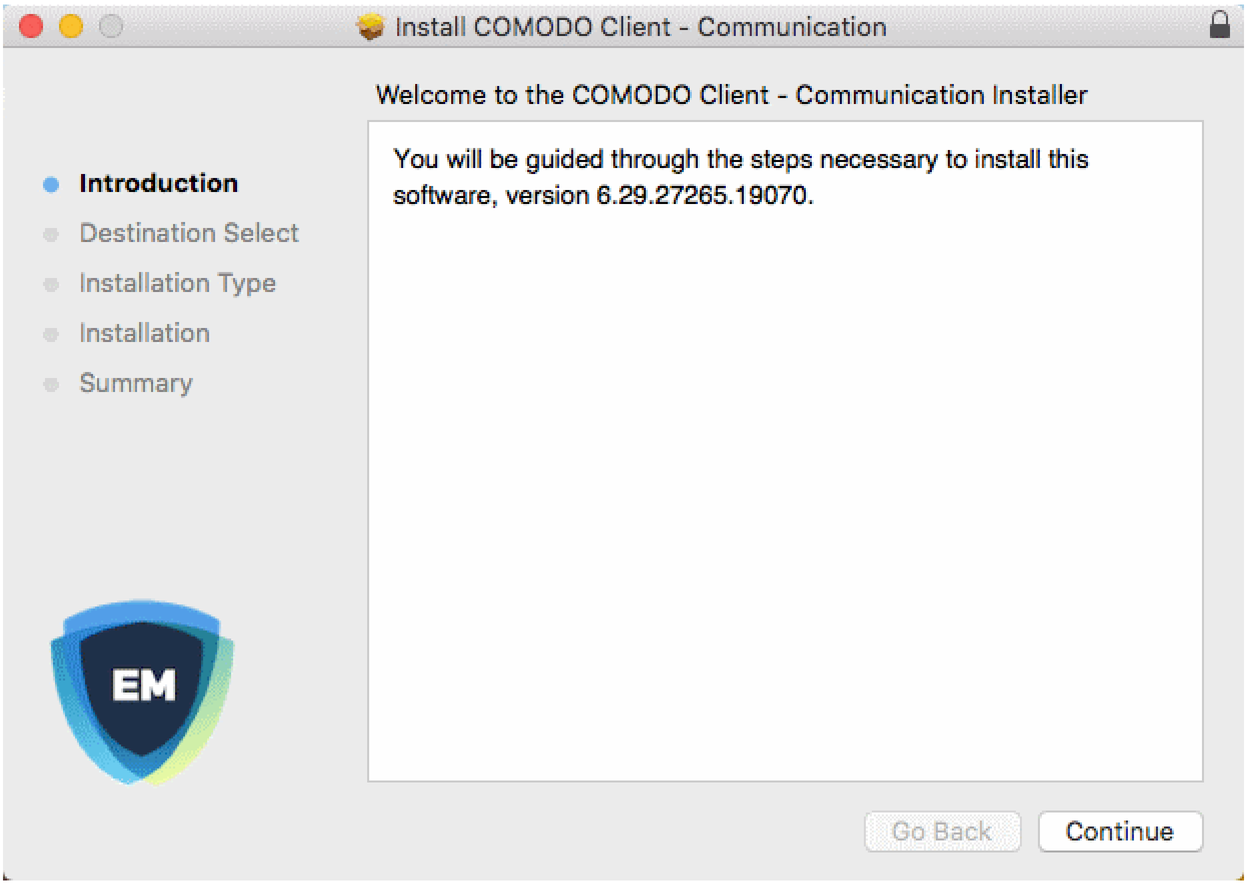
- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.

FOR IOS DEVICES

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

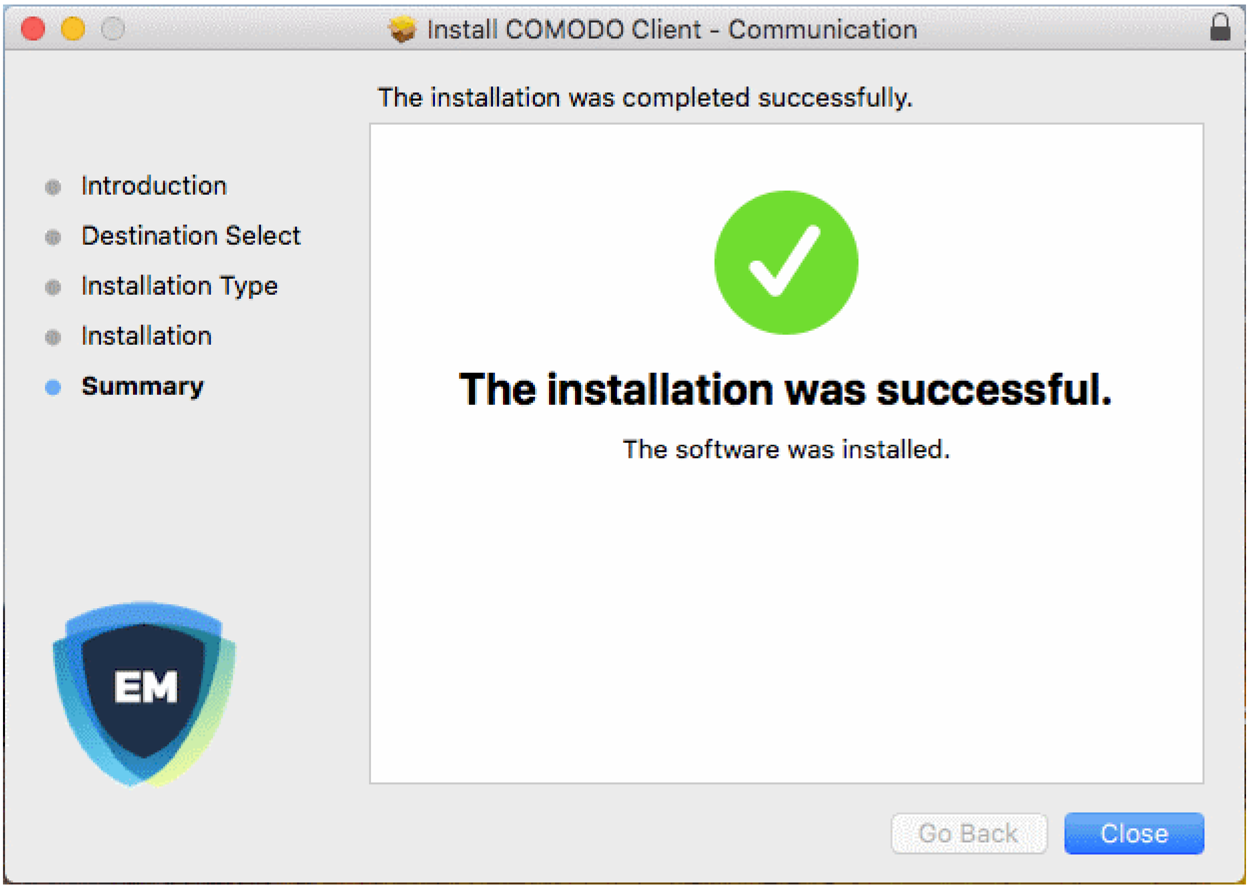
This will start the installation wizard for the communication client:



Welcome to the COMODO Client - Communication Installer

You will be guided through the steps necessary to install this software, version 6.29.27265.19070.

- The user follows the wizard and completes the installation.
- Once installation is complete, the client starts communicating with the EM portal.



The installation was completed successfully.

The installation was successful.

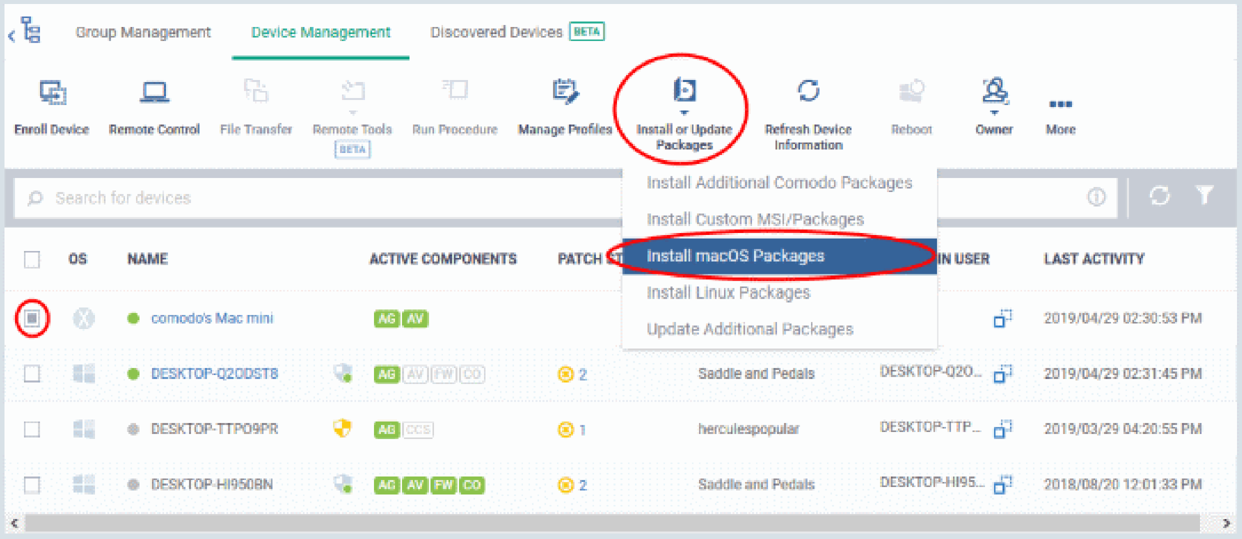
The software was installed.

Deploy Comodo Client Security

Note - Please uninstall any other antivirus products from target endpoints before proceeding. Failure to do so could cause conflicts that mean CCS will not function correctly.

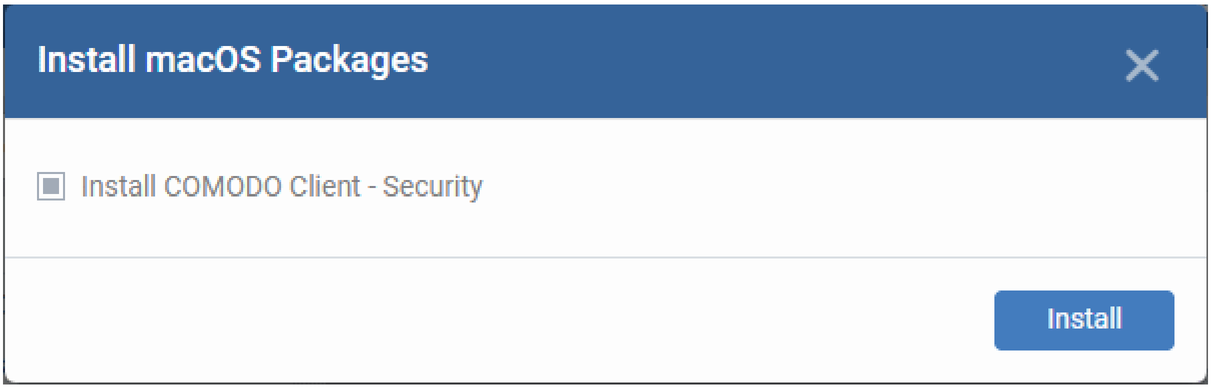
Install CCS

- Log into Dragon / Comodo One
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Click the funnel icon on the right and select 'MacOS', to see only Mac OS endpoints
  - Click 'All Devices' to view every device in Endpoint Manager
- Select your target Mac OS device(s) using the check-box(es) on the left
- Click 'Install or Update Packages':



□	OS	NAME	ACTIVE COMPONENTS	PATCH ST		IN USER	LAST ACTIVITY
☒		comodo's Mac mini	AG AV				2019/04/29 02:30:53 PM
□		DESKTOP-Q2ODST8	AG AV FW CO	2	Saddle and Pedals	DESKTOP-Q2O...	2019/04/29 02:31:45 PM
□		DESKTOP-TTPO9PR	AG CCS	1	herculespopular	DESKTOP-TTP...	2019/03/29 04:20:55 PM
□		DESKTOP-HI950BN	AG AV FW CO	2	Saddle and Pedals	DESKTOP-HI95...	2018/08/20 12:01:33 PM

- Select 'Install macOS Packages' from the drop-down.
- Choose 'Install Comodo Client - Security'
- Click 'Install':


Install macOS Packages

☒ Install COMODO Client - Security

- A command will be sent to target endpoints to install CCS
- The EM agent on the endpoint will download and install CCS

The application will become effective immediately after installation.

- You can configure CCS settings in the EM profile which is applied to the endpoint.

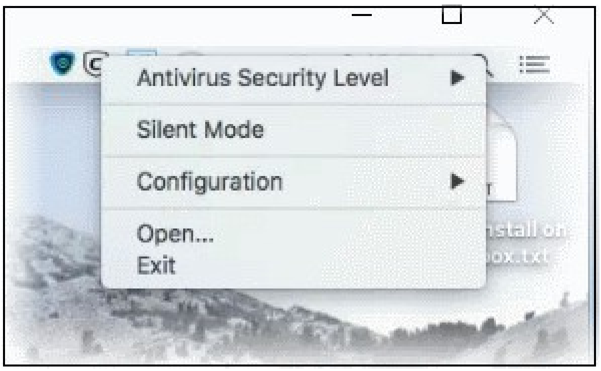
- See **https://help.comodo.com/topic-399-1-786-10854-Profiles-for-Mac-OS-Devices.html** for more details on this.

1.3. Start CCS

- After installation, Comodo Client Security (CCS) will load at computer start-up. Real-time virus monitoring is enabled.
- If you need to access the local interface, you can do so using the following methods:
  - **Taskbar**
  - **Launchpad**
  - **Dock**

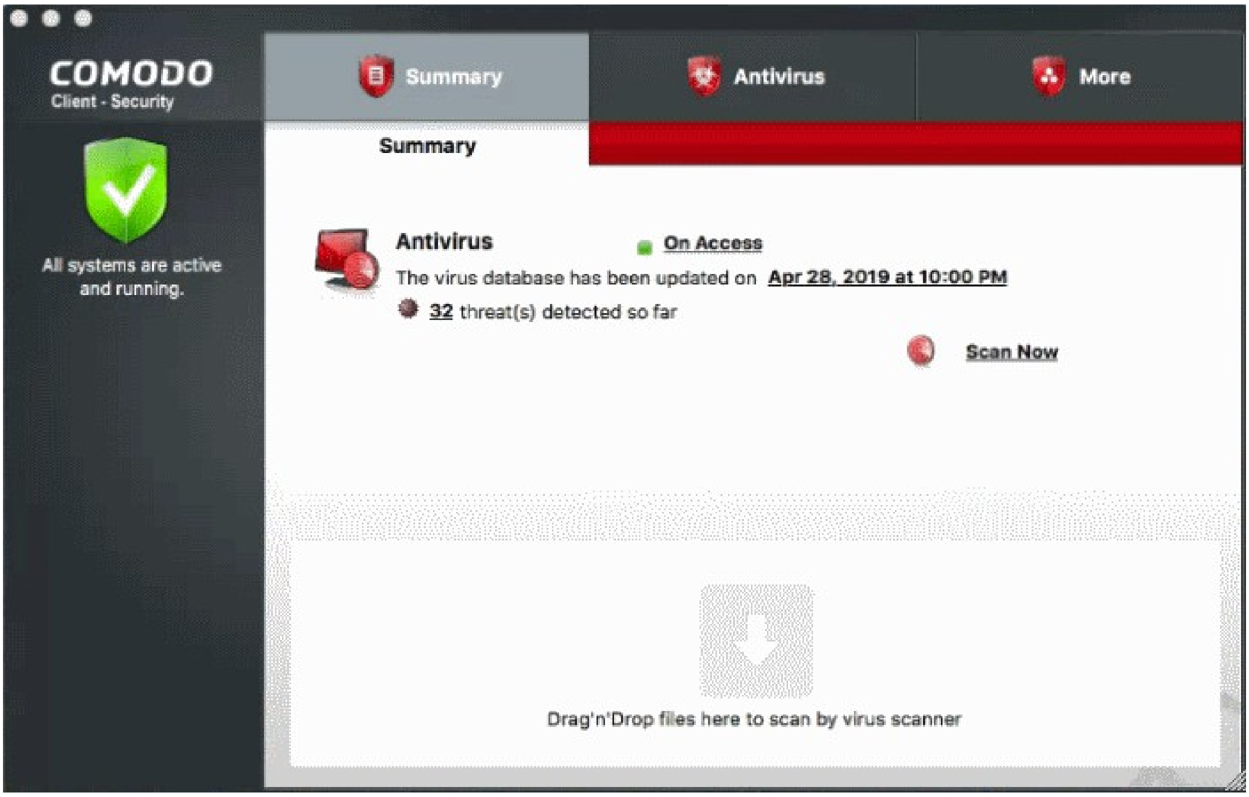
Taskbar icon

The 'Taskbar' (top-right) lets you open the application, enable/disable real-time scanning, switch to silent mode, and manage your CCS configurations.



- **Antivirus Security Level -** Enable or disable the real-time virus monitor:
  - **On Access** - Any file opened is scanned before it is allowed to run.
  - **Disabled** - Switches the real-time scanner off.
- **Silent Mode -** Temporarily disables alerts so they don't interrupt you when running a full screen presentation or playing a game. Protection remains enabled.
- **Configuration -** Create, import and export CCS security configurations. This is useful if you want to implement specific settings on multiple endpoints.
- **Open**... - Open the CCS main interface.
- Click 'Open' to launch the application.

The application will open at the 'Summary' screen:


COMODO
Client - Security
Summary
Antivirus
More
Summary
All systems are active and running.
Antivirus
On Access
Scan Now
Drag'n'Drop files here to scan by virus scanner

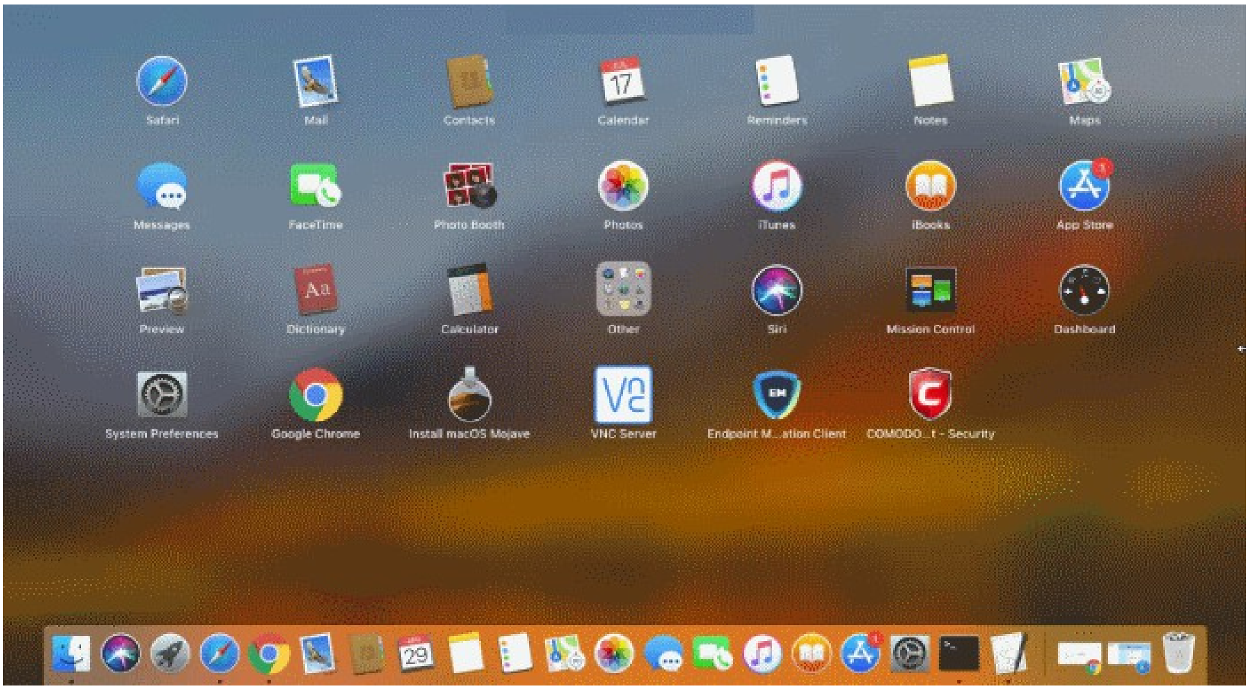
The virus database has been updated on Apr 28, 2019 at 10:00 PM

32 threat(s) detected so far

Note: We recommend your first task should be a full scan of your computer. Click 'Antivirus' > 'Run a Scan' > 'Full Scan' to do this.

Launchpad

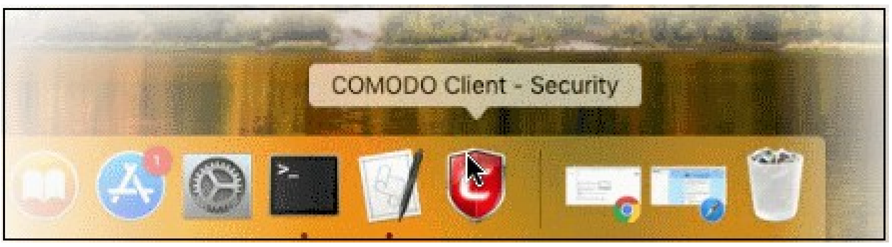
- Open the launchpad on your Mac device



- Click the Comodo Client Security icon to open the application

Dock icon

Use the quick launch icon on the MAC OS dock to open the interface at any time:

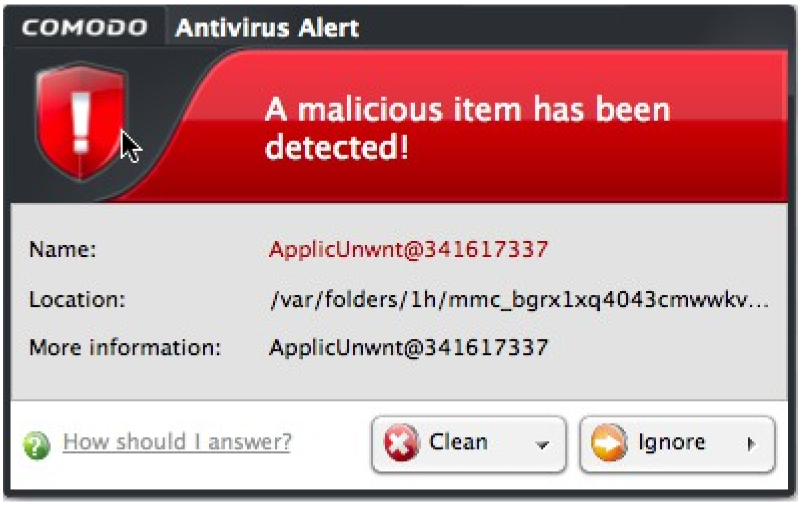


Tip: You can run scans on any file or folder by simply dragging it onto the CCS dock icon. If this icon is not present you can add it as follows:

- Click the 'Finder' icon on the Dock
- Click 'Applications' on the left menu
- Click, hold and drag 'Comodo Client Security' icon onto the dock.

1.4. Understand CCS Alerts

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



A malicious item has been detected!

Name: ApplicUnwnt@341617337

Location: /var/folders/1h/mmc_bgrx1xq4043cmwwkv...

More information: ApplicUnwnt@341617337

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'. Select either of these to view further options.

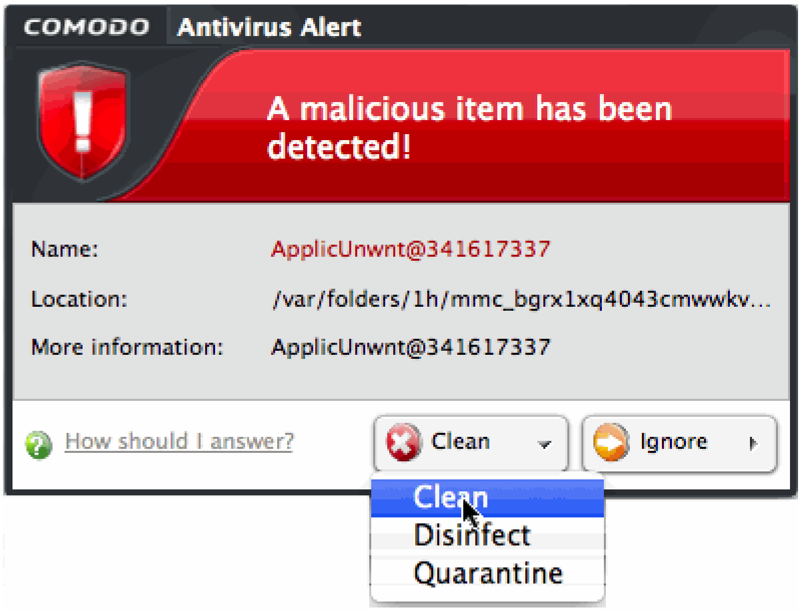
- **'Clean'** presents you with the following options:

  - Clean the file - Will delete the file.
  - Quarantine the file. This will move the file to **Quarantined Items**

    OR
  - Disinfect the file,
    - If CCS has a disinfection routine available it will disinfect the file.
    - If not, then the file will be deleted.
- **'Ignore'** presents you with the following options:
    - Once - Ignore the file this time only. If the same file is detected at another time then another alert will be shown.
    - Add to Exclusions - The virus is added to your local **Exclusions** list. Comodo Client - Security will no longer report this file as malicious or raise an alert the next time the file is detected.

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.



COMODO Antivirus Alert

A malicious item has been detected!

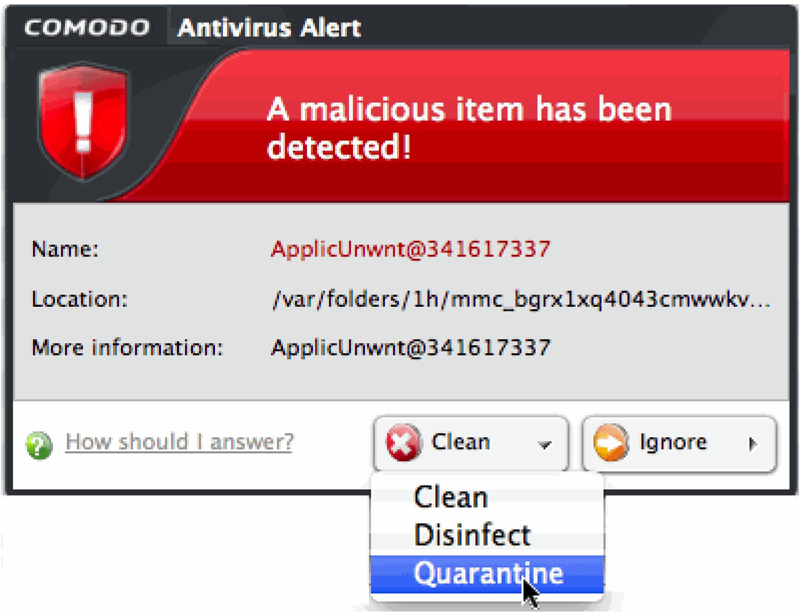
Name: ApplicUnwnt@341617337

Location: /var/folders/1h/mmc_bgrx1xq4043cmwwkv...

More information: ApplicUnwnt@341617337

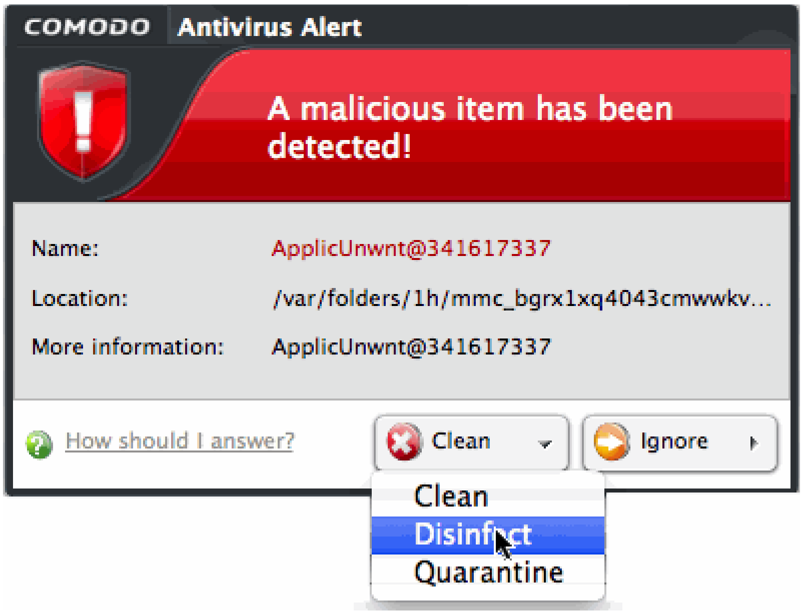
To move a file or an application to Quarantine

- Select 'Quarantine' under the 'Clean' drop-down button.


COMODO Antivirus Alert
A malicious item has been detected!
Name: ApplicUnwnt@341617337
Location: /var/folders/1h/mmc_bgrx1xq4043cmwwkv...
More information: ApplicUnwnt@341617337
How should I answer?
Clean
Ignore
Clean
Disinfect
Quarantine

To disinfect the file or application

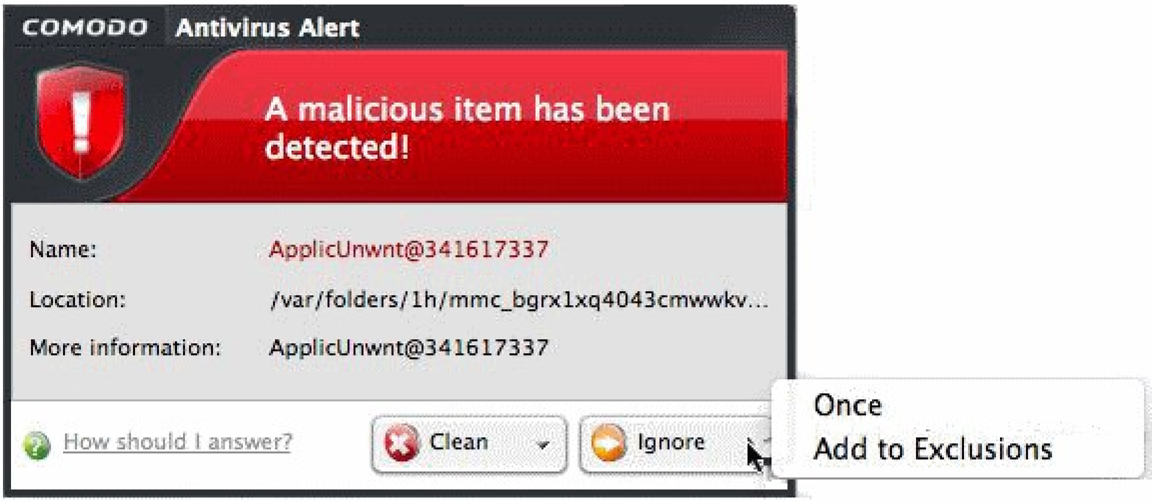
- Select 'Disinfect' under the 'Clean' drop-down button.


COMODO Antivirus Alert
A malicious item has been detected!
Name: ApplicUnwnt@341617337
Location: /var/folders/1h/mmc_bgrx1xq4043cmwwkv...
More information: ApplicUnwnt@341617337
How should I answer?
Clean
Ignore
Clean
Disinfect
Quarantine

CCS will attempt to disinfect the file. If this is not possible then the file will be deleted.

To ignore an alert to trust a file/application

- Click 'Ignore' at an alert.



COMODO Antivirus Alert

A malicious item has been detected!

Name: ApplicUnwnt@341617337

Location: /var/folders/1h/mmc_bgrx1xq4043cmwwkv...

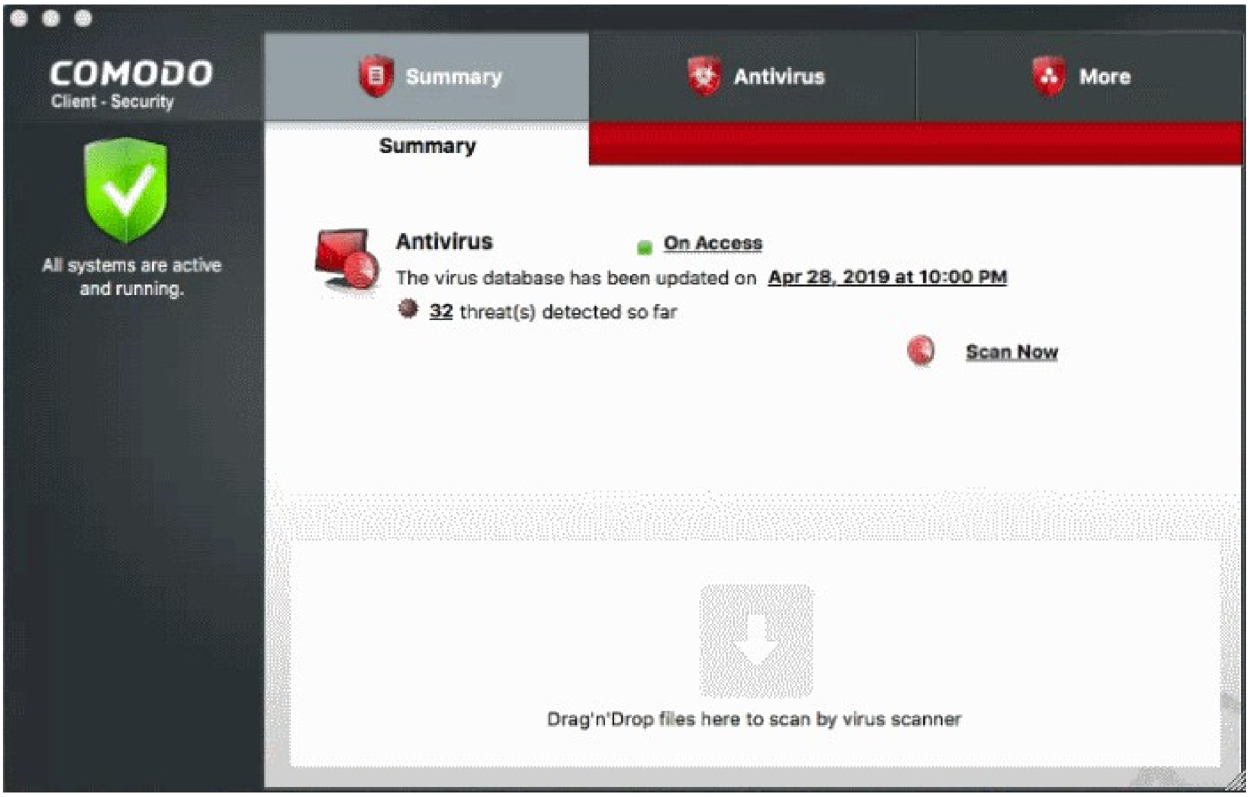
More information: ApplicUnwnt@341617337

- This provides you with three options:
  - **Once -** The file is ignored this time only. If the same file is detected at a later date then another alert will shown
  - **Add to Exclusions -** If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. This means Comodo Client - Security will no longer report this file as malicious or raise an alert the next time the file is detected.

Note - When an alert is shown, the item will be blocked access from other applications. If you choose not to answer the alert or if the alert time runs out, then no action is taken against it. The alert will be shown next time when it is accessed again.

2. The Summary Screen

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


COMODO
Client - Security
Summary
Antivirus
More
Summary
All systems are active and running.
Antivirus
On Access
The virus database has been updated on Apr 28, 2019 at 10:00 PM
32 threat(s) detected so far
Scan Now
Drag'n'Drop files here to scan by virus scanner

To scan individual files for viruses, drag 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. There are four CCS indicators: yellow, green, red and blue

   - **Yellow** - There are actions you need to take. For example, because you need to run a full scan or because the real-time scanner is switched off.
   - **Green -** All systems are active and running.
   - **Red** - Serious security risks. For example, when the EM agent is not running or a CCS setting is corrupted.
   - **Blue -** Silent mode is active. Alerts are temporarily disabled.

2. **Antivirus**

   The 'Antivirus' summary box contains:

   i. **Status of Real Time Virus Scanning**
      - The status of the virus scanning setting is displayed as a link (on Access in the example).
      - Click 'On Access' to open the 'Virus Scanner Settings' panel.
      - To quickly set the 'Real Time Scanning' level, move the status slider. See **Scanner Settings** for more details on Virus Scanner Settings.

   ii. **When the Virus Database was Last Updated**
      - The date when the virus database was last updated is shown as a link.
      - Click the link to start the the database update.

   iii. **Number of Detected Threats**
      - The number of threats detected from the start of the current session of Comodo Client - Security.
      - Click the <number> link to open the 'Antivirus Events' panel. For more details, see **Antivirus Events**.

   iv. **Scan Now**

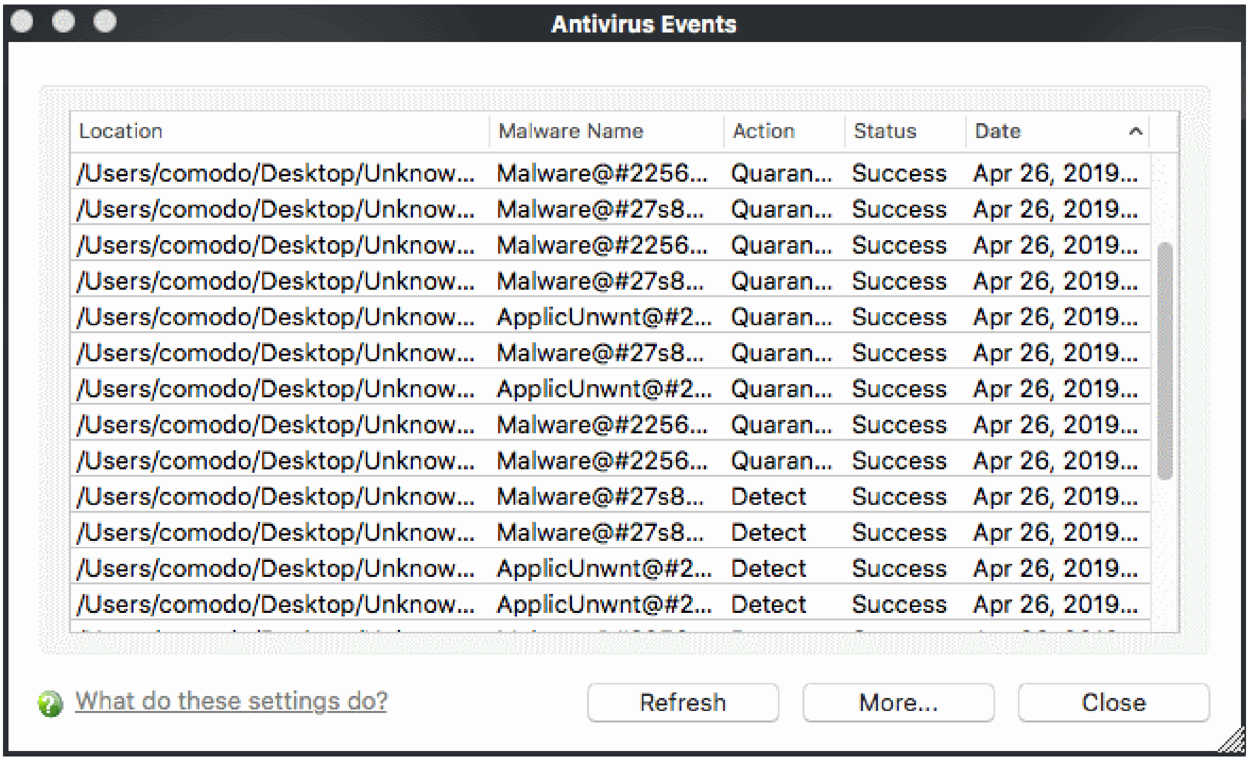
Click the 'Scan Now' link to instantly **run a scan**.

2.1. 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 tells you:

- The date and time a particular virus was detected
- Location and the action that was taken by Comodo Client - Security in response
- Click the number in front of 'Threat(s) detected so far' on the 'Summary' screen to open the event viewer.



Antivirus Events

Location	Malware Name	Action	Status	Date
/Users/comodo/Desktop/Unknow...	Malware@#2256...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#27s8...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#2256...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#27s8...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	ApplicUnwnt@#2...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#27s8...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	ApplicUnwnt@#2...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#2256...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#2256...	Quaran...	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#27s8...	Detect	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	Malware@#27s8...	Detect	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	ApplicUnwnt@#2...	Detect	Success	Apr 26, 2019...
/Users/comodo/Desktop/Unknow...	ApplicUnwnt@#2...	Detect	Success	Apr 26, 2019...

Column Descriptions

- **Location** - The path of the malicious file
- **Malware Name** - The label of the malicious file
- **Action** - Indicates how CCS acted on the malware. Possible actions include 'Detect', 'Quarantine' and 'Ignore'
- **Status** - Whether or not the action was successful
- **Date** - The date and time of the event

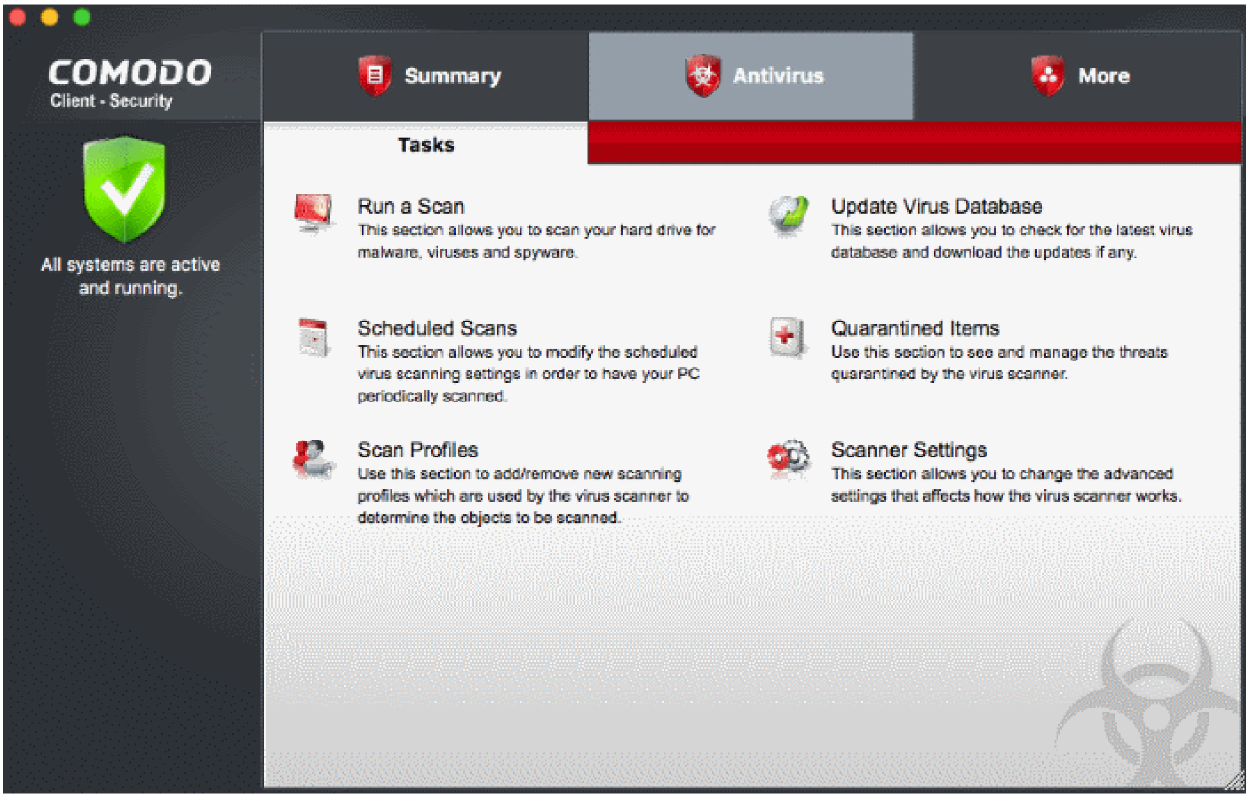
Controls

- **Refresh** - Click to load the very latest events
- **More...** - Opens the 'Log Viewer' screen. See **View Logs** for more details.
- **Close** - Exit the 'Antivirus Events' screen

3. Antivirus Tasks - Introduction

- Click the 'Antivirus' tab on the CCS home-screen to open this interface.

- The tasks area 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 schedules to run scans at regular intervals.
- You can also create custom scan profiles, view event logs, change update settings and review quarantined files



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles
Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

Scanner Settings
This section allows you to change the advanced settings that affects how the virus scanner works.

Background - How antivirus scans work

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

The following sections explain more about each task:

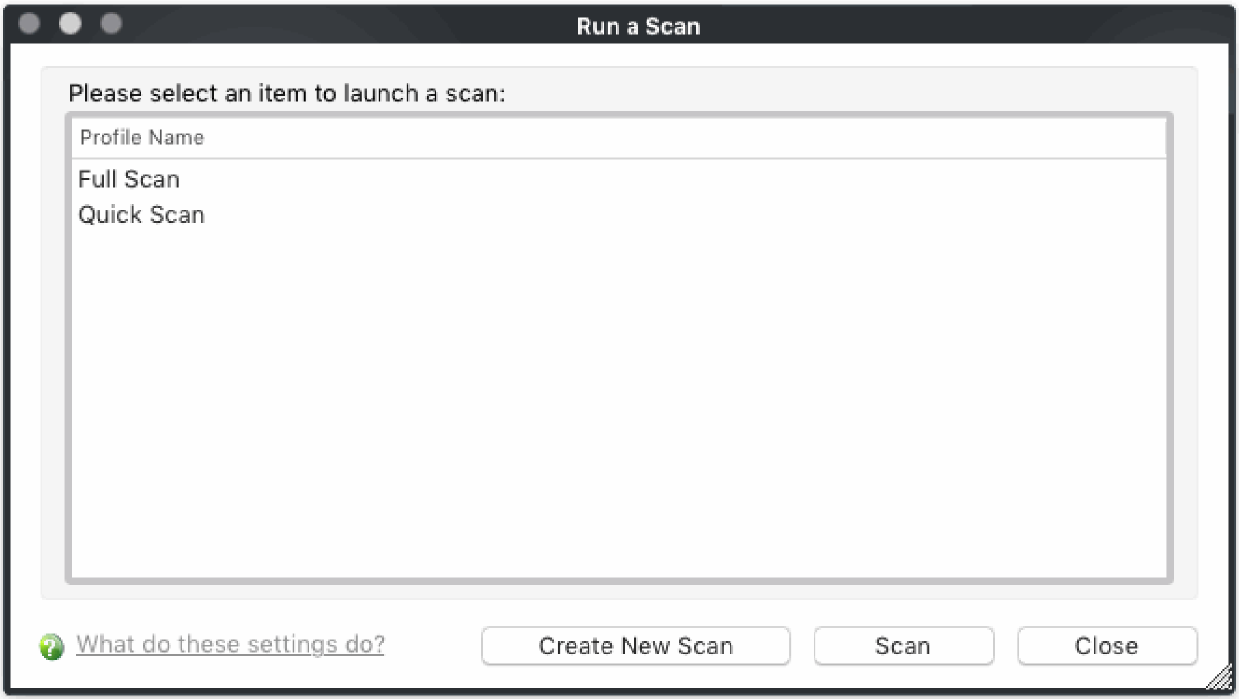
- **Run a Scan**
- **Update Virus Database**
- **Quarantined Items**
- **Scanner Settings**
- **Scheduled Scans**
- **Scan Profiles**

3.1. Run a Scan

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

Run an on-demand virus scan

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click the 'Run a Scan' box


Run a Scan
Please select an item to launch a scan:
Profile Name
Full Scan
Quick Scan
What do these settings do?
Create New Scan
Scan
Close

Choose one of the following options:

- **Full Scan** - Scans every drive, folder and file on your system, including external connected devices
- **Quick Scan** - Scans important operating system files, system memory, auto-run entries, registry keys and hidden services.
- **Create New Scan** - Create your own custom scan of specific files, folders or drives.

Click 'Scan' after making your selection (or just double-click the profile name).

Custom Scan

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

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click the 'Run a Scan' box
- Click 'Create New Scan'
- Type a name for your new profile. For example, 'My External Drives'.
- Click 'Add' to choose files, folders or drives you want to include in the profile
- Repeat the process to add multiple items

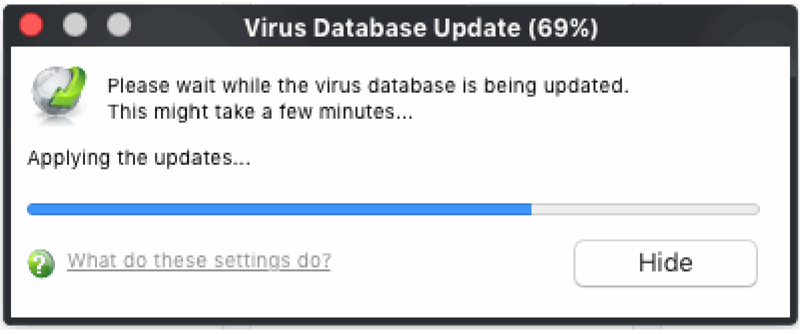
- Click 'Apply'. Your new profile will be listed in the 'Run a Scan' dialog
- Select your new profile in the list and click 'Scan'
- Next, see:
  - **Scan progress and results**
  - **View the results window**
  - **Save results as a text file**
  - **Remove selected items**
  - **Move threats to quarantine**
  - **Disinfect / delete threats**
  - **Ignore a result once / ignore and create an exception**

Tip: Drag an item into the scan box on the 'Summary' screen for a quick scan. You can also drag items onto the CCS dock icon.

Tip: For more details on scan profiles, see **Scan Profiles** for more details.

To scan progress and results

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



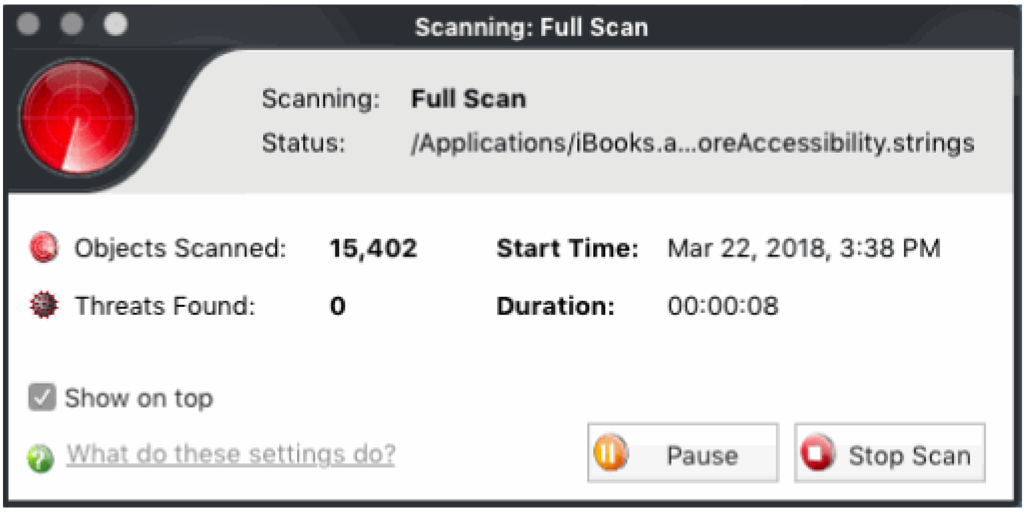
Virus Database Update (69%)

Please wait while the virus database is being updated.
This might take a few minutes...

Applying the updates...

The scan will begin immediately after updates have been installed.

The progress dialog shows you 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.



Scanning: Full Scan

Scanning: **Full Scan**
Status: /Applications/iBooks.a...oreAccessibility.strings

Objects Scanned: **15,402**
Start Time: Mar 22, 2018, 3:38 PM
Threats Found: **0**
Duration: 00:00:08

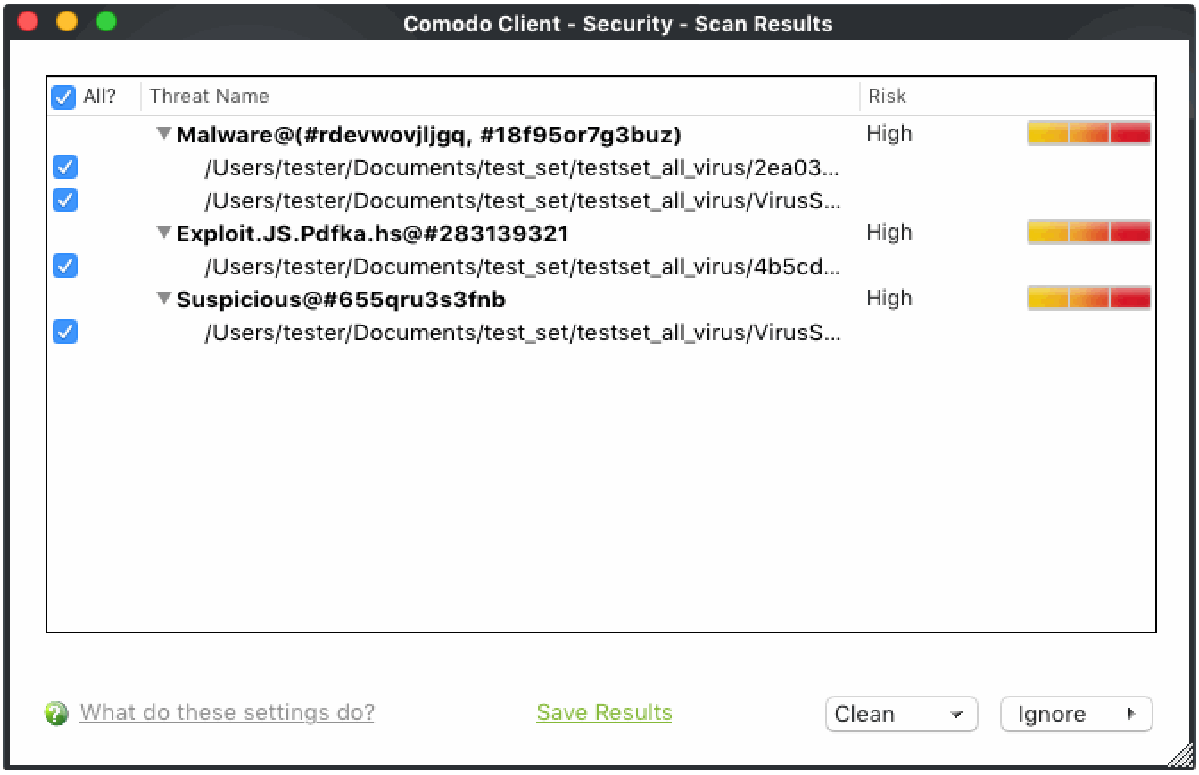
☑ Show on top

- Click the 'Pause' to suspend the task
- Click the 'Resume' to resume a paused task
- Click 'Stop Scan' to abort the scan process altogether.

Once the scan is complete, the results window opens:

View the Scan Results Window

The results screen lists the name and severity of all threats found:



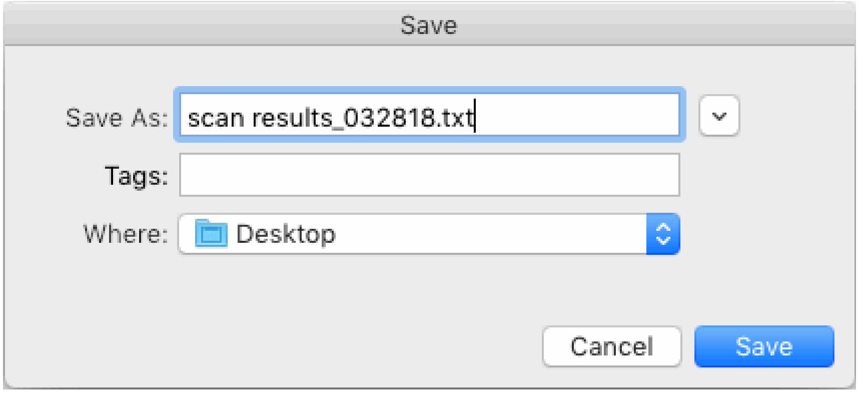
Comodo Client - Security - Scan Results
What do these settings do?
Save Results
Clean
Ignore

☑ All?	Threat Name	Risk
	Malware@(#rdevwovjljgq, #18f95or7g3buz)	High
☑	/Users/tester/Documents/test_set/testset_all_virus/2ea03...	
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	
	Exploit.JS.Pdfka.hs@#283139321	High
☑	/Users/tester/Documents/test_set/testset_all_virus/4b5cd...	
	Suspicious@#655qru3s3fnb	High
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	

- Click the 'Threat Name' column header to sort results in alphabetical order
- Click the 'Risk' column header to sort results by risk level
- Select 'All' if you want to apply 'Clean' or 'Ignore' actions to every threat.

Save the scan results as a text file

- Click the 'Save Results' link on the bottom
- Type a name in the 'Save' dialog, enter the location and click 'Save'.



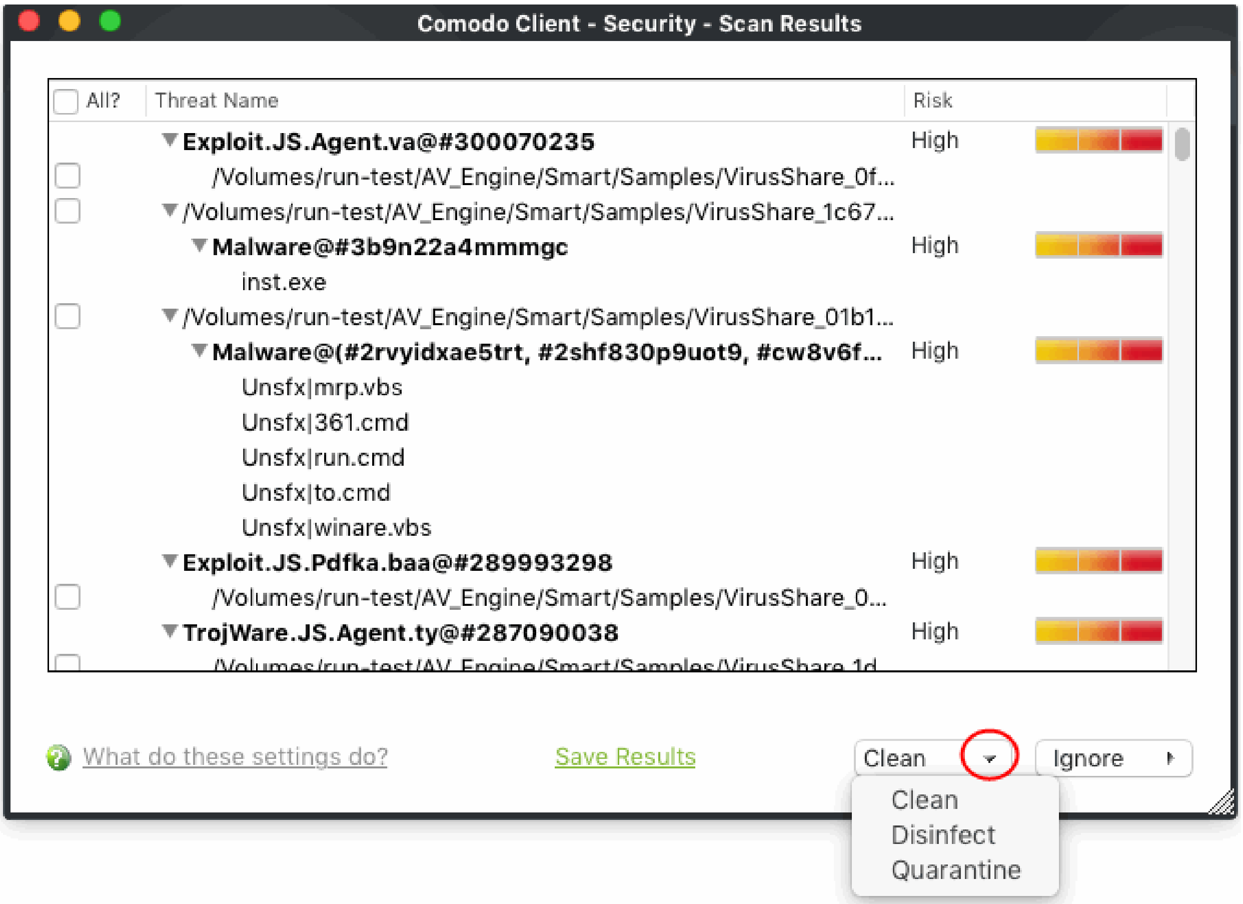
Save As: scan results_032818.txt

Tags:

Where: Desktop

Remove selected items

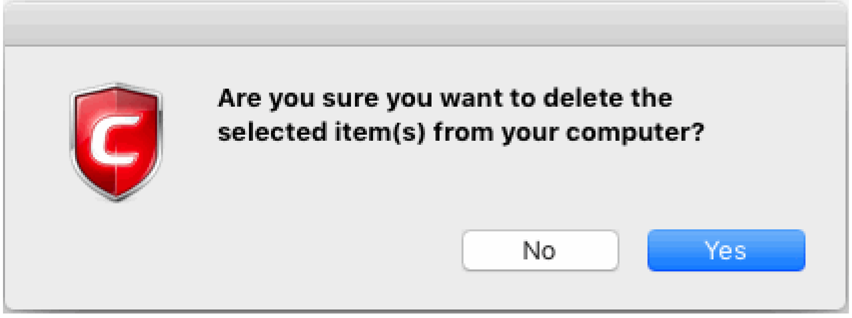
- Select the file from the results
- Click the 'Clean' drop-down and select 'Clean'.



Comodo Client - Security - Scan Results

□ All?	Threat Name	Risk
	▼ **Exploit.JS.Agent.va@#300070235**	High
□	/Volumes/run-test/AV_Engine/Smart/Samples/VirusShare_0f...	
□	▼ /Volumes/run-test/AV_Engine/Smart/Samples/VirusShare_1c67...	
	▼ **Malware@#3b9n22a4mmmgc**	High
	inst.exe	
□	▼ /Volumes/run-test/AV_Engine/Smart/Samples/VirusShare_01b1...	
	▼ **Malware@(#2rvyidxae5trt, #2shf830p9uot9, #cw8v6f...**	High
	Unsfx|mrp.vbs	
	Unsfx|361.cmd	
	Unsfx|run.cmd	
	Unsfx|to.cmd	
	Unsfx|winare.vbs	
	▼ **Exploit.JS.Pdfka.baa@#289993298**	High
□	/Volumes/run-test/AV_Engine/Smart/Samples/VirusShare_0...	
	▼ **TrojWare.JS.Agent.ty@#287090038**	High
□	/Volumes/run-test/AV_Engine/Smart/Samples/VirusShare_1d	

- Click 'Yes' in the confirmation dialog box:

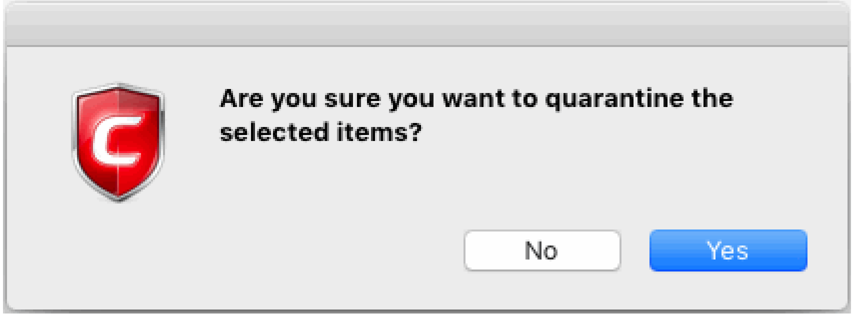


Are you sure you want to delete the selected item(s) from your computer?

The file will be deleted permanently from your system.

Move selected threats to quarantine

- Select the file from the results
- Click the 'Clean' drop-down and select 'Quarantine'.



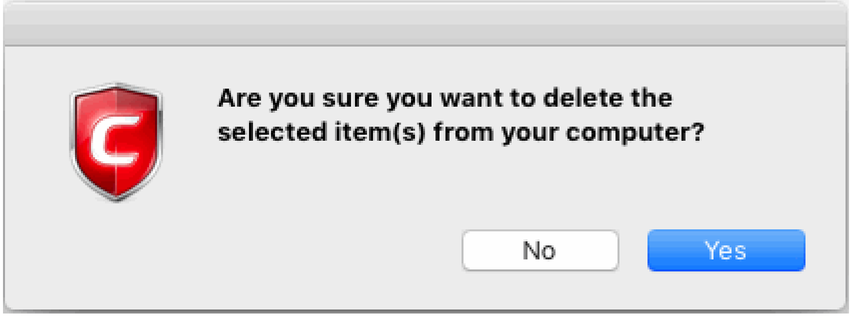
Are you sure you want to quarantine the selected items?

- Click 'Yes' in the confirmation dialog box.

The selected file is moved to the **Quarantined items**.

Disinfect a file

- Select the file from the results
- Click the 'Clean' drop-down and select 'Disinfect'.



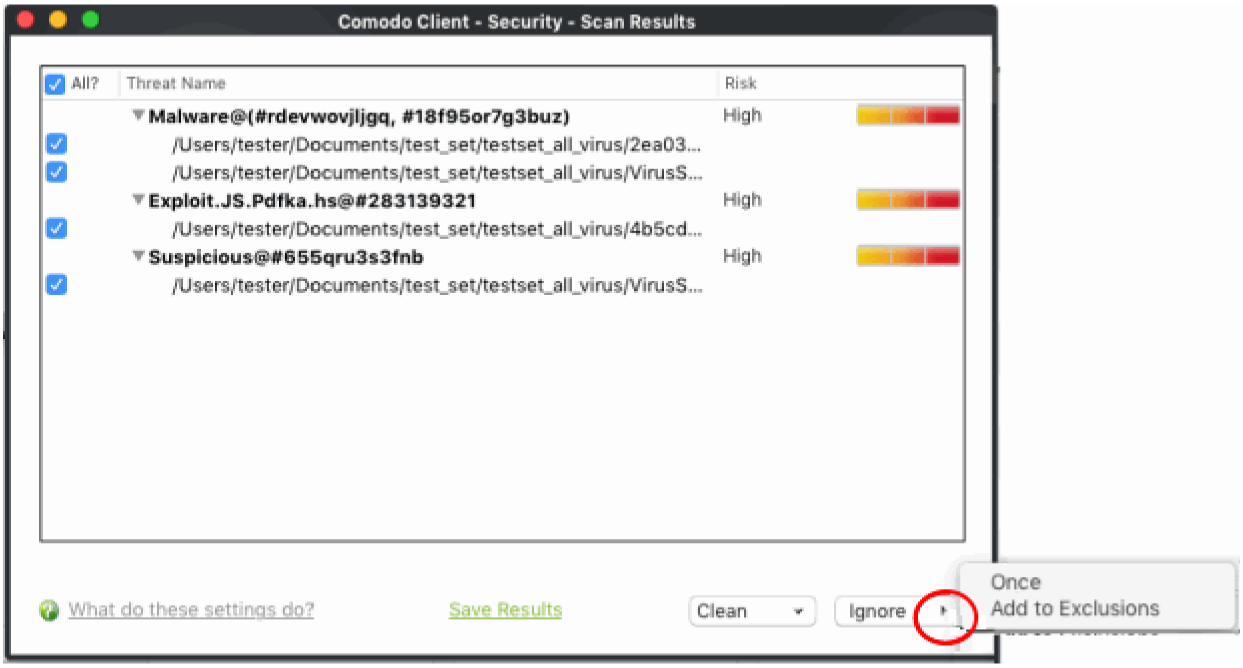
Are you sure you want to delete the selected item(s) from your computer?

- Click 'Yes' at the confirmation dialog box.

CCS will disinfect 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.

Ignore a result if you consider the file safe

- Select the application / file from the results
- Click the 'Ignore' drop-down



Comodo Client - Security - Scan Results

☑ All?	Threat Name	Risk
	▼ **Malware@(#rdevwovjljgq, #18f95or7g3buz)**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/2ea03...	
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	
	▼ **Exploit.JS.Pdfka.hs@#283139321**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/4b5cd...	
	▼ **Suspicious@#655qru3s3fnb**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	

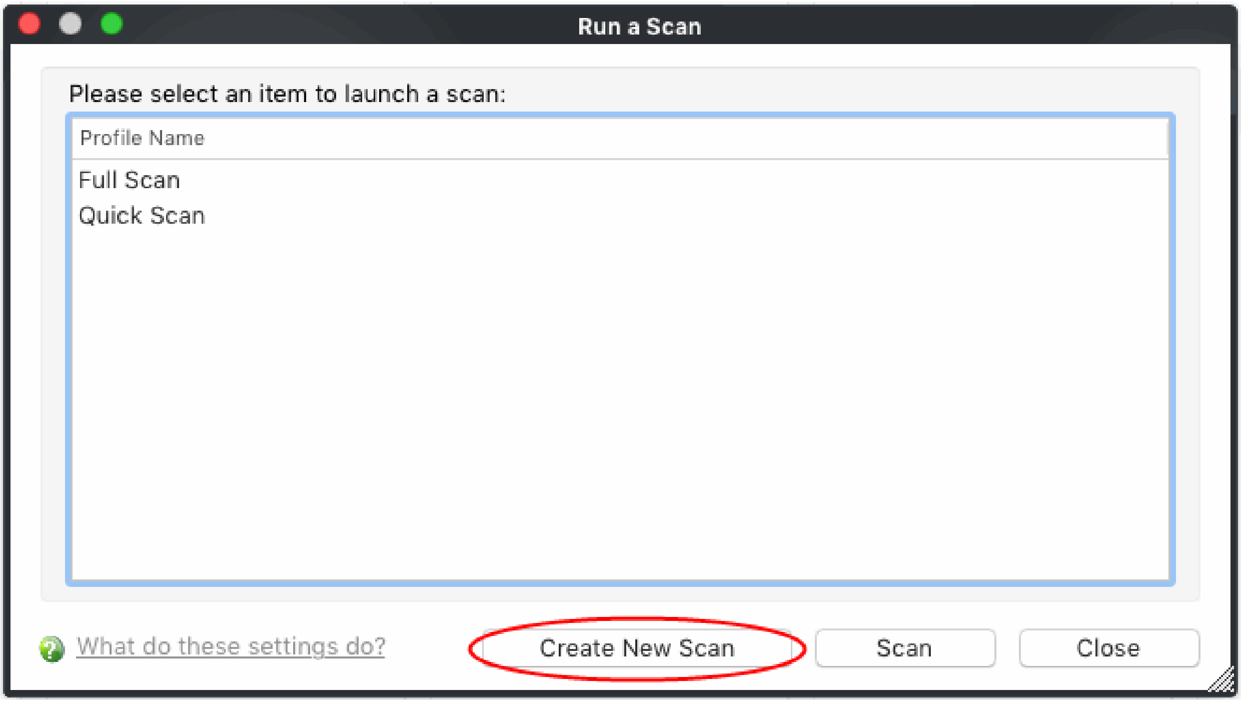
'Ignore' provides you with two options:

- **Once -** The threat is ignored this time only. The virus scanner will detect the file as a threat on the next scan, and show another alert.
- **Add to Exclusions -** Create an exception for the file. The file is placed on the **exclusions** list and the scanner will not flag it as a threat on subsequent scans.

Create a Scan profile

A custom scan profile is a scan of specific files, folders and drives. You choose which items are scanned, You can re-run your custom scan profile at any time.

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

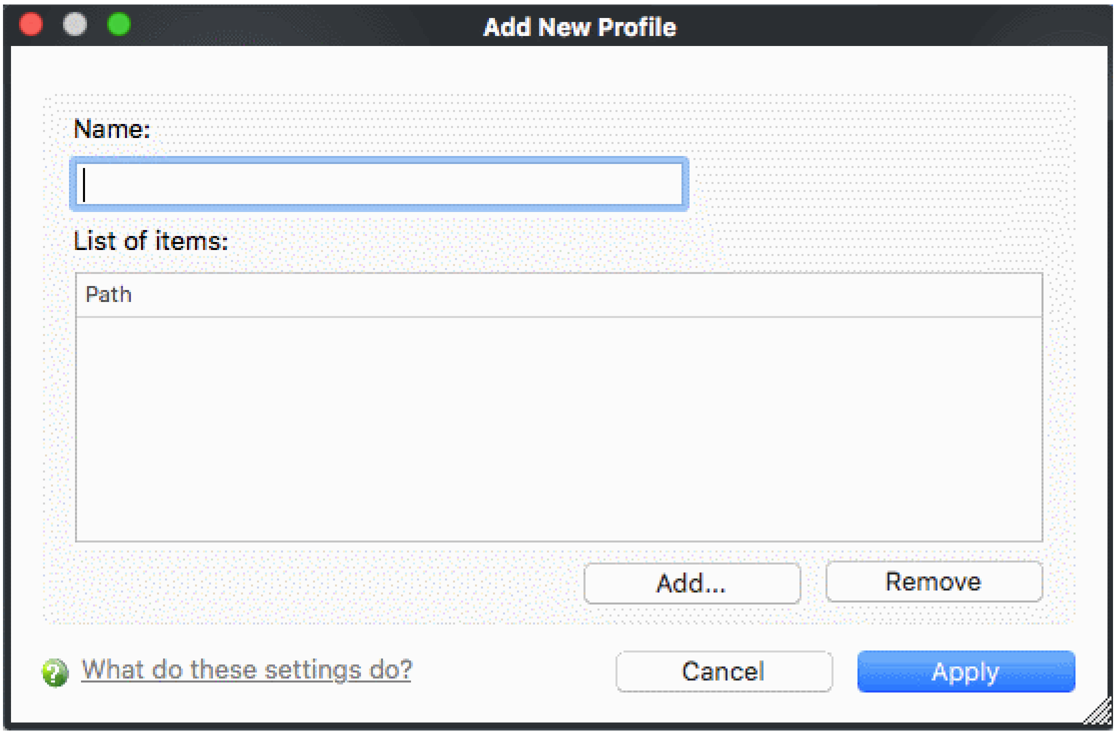


Run a Scan

Please select an item to launch a scan:

Profile Name
Full Scan
Quick Scan

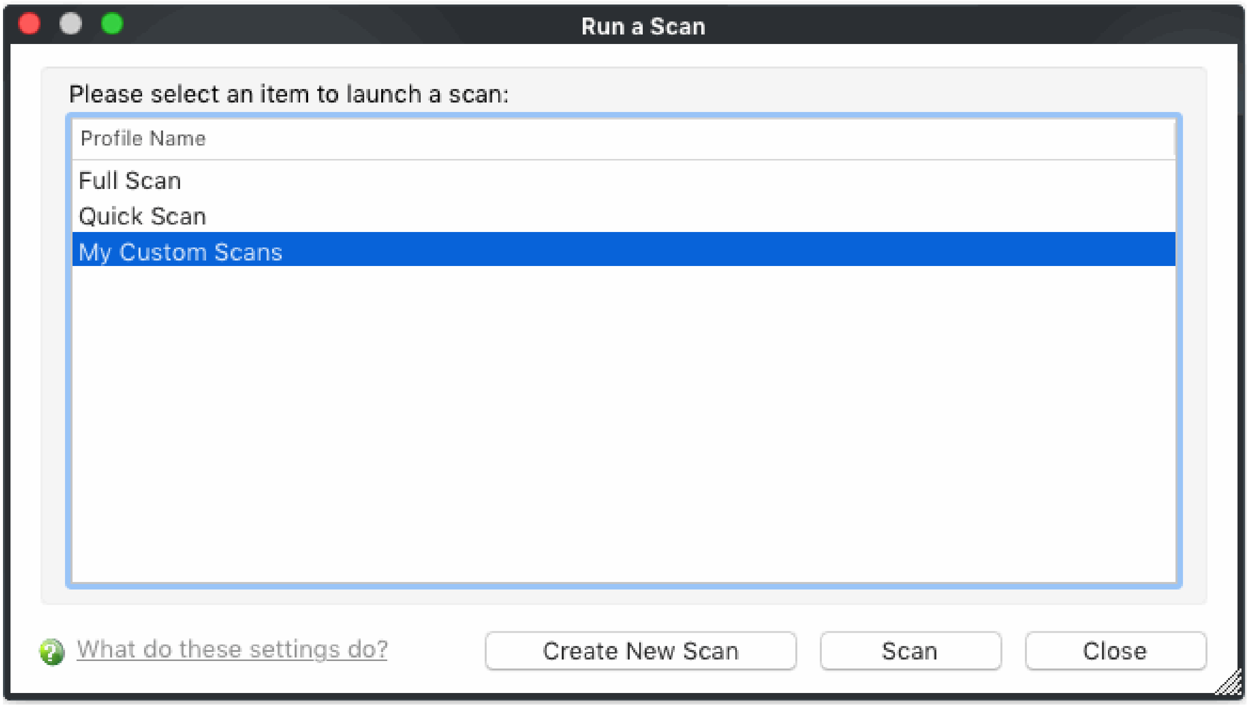
'Add New Profile' dialog opens:


Add New Profile

Name:

List of items:

- Type a name for the scan profile in the 'Name' box
- Click 'Add' to select the items you wish to include in the scan
- Repeat the process to create more scan profiles
- Click 'Apply'.


Run a Scan

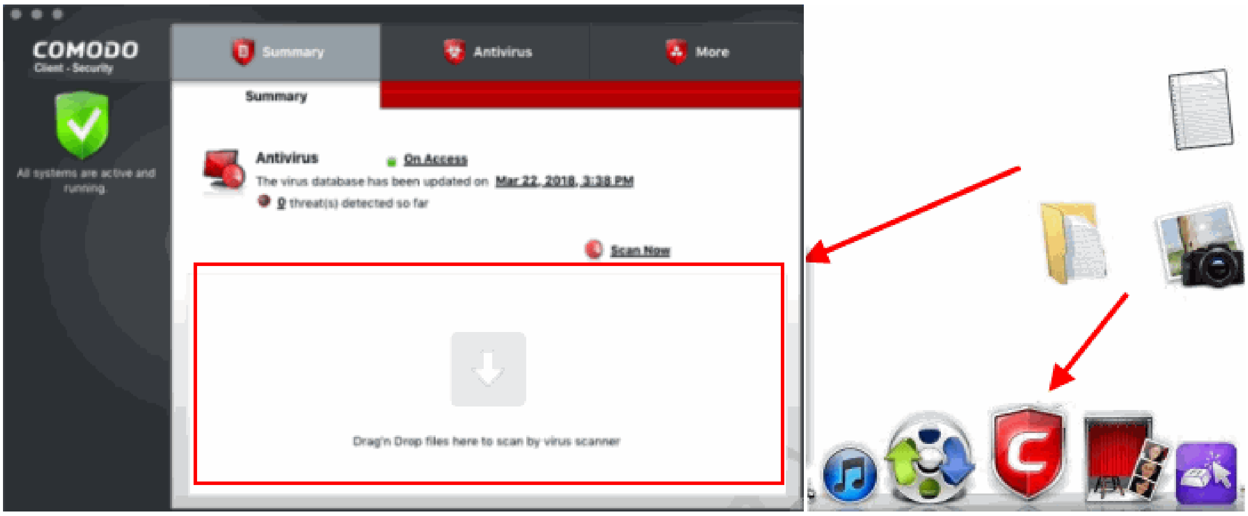
Please select an item to launch a scan:

Profile Name
Full Scan
Quick Scan
My Custom Scans

- Note 1: You can also create new Scan Profiles by accessing **Scan Profiles** in the 'Antivirus' task interface.
- Note 2: Managed endpoints - Scan profiles should be configured in the Endpoint Manager profile.

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.


COMODO
Client - Security
All systems are active and running.
Summary
Antivirus
More
Summary
Antivirus
On Access
The virus database has been updated on Mar 22, 2018, 3:38 PM
0 threat(s) detected so far
Scan Now
Drag'n Drop files here to scan by virus scanner

3.2. Update Virus Database

To ensure your system remains virus-free, it is imperative that the virus database is kept up-to-date.

You can download updates from Comodo's update servers to your system in two ways:

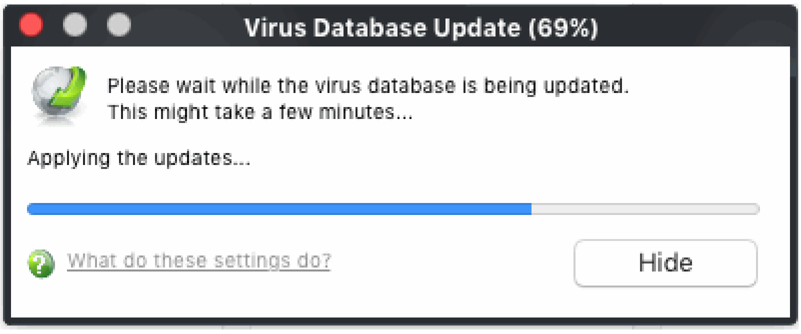
- **Download updates manually**
- **Download updates automatically**

Manually check for the latest virus database and then download the updates

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

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

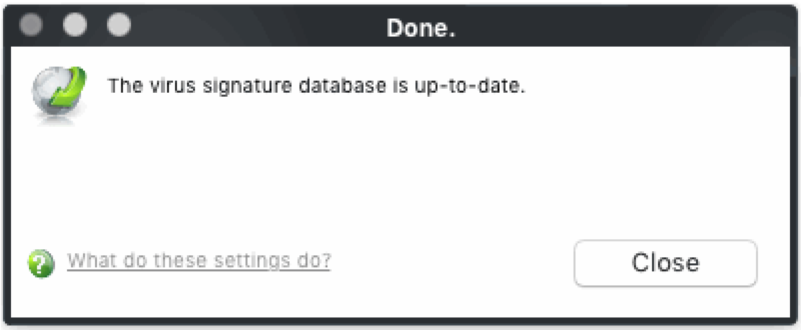
The following notification is shown when the update is complete:


Virus Database Update (69%)

Please wait while the virus database is being updated.
This might take a few minutes...

Applying the updates...

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



The virus signature database is up-to-date.

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

Automatic Updates

- By default, CCS is set to automatically check for and download updates from the Comodo servers before commencing a scan of any type.
- You can configure whether these automatic checks updates take place on a 'per scanner' basis in the '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.

3.3. Quarantined Items

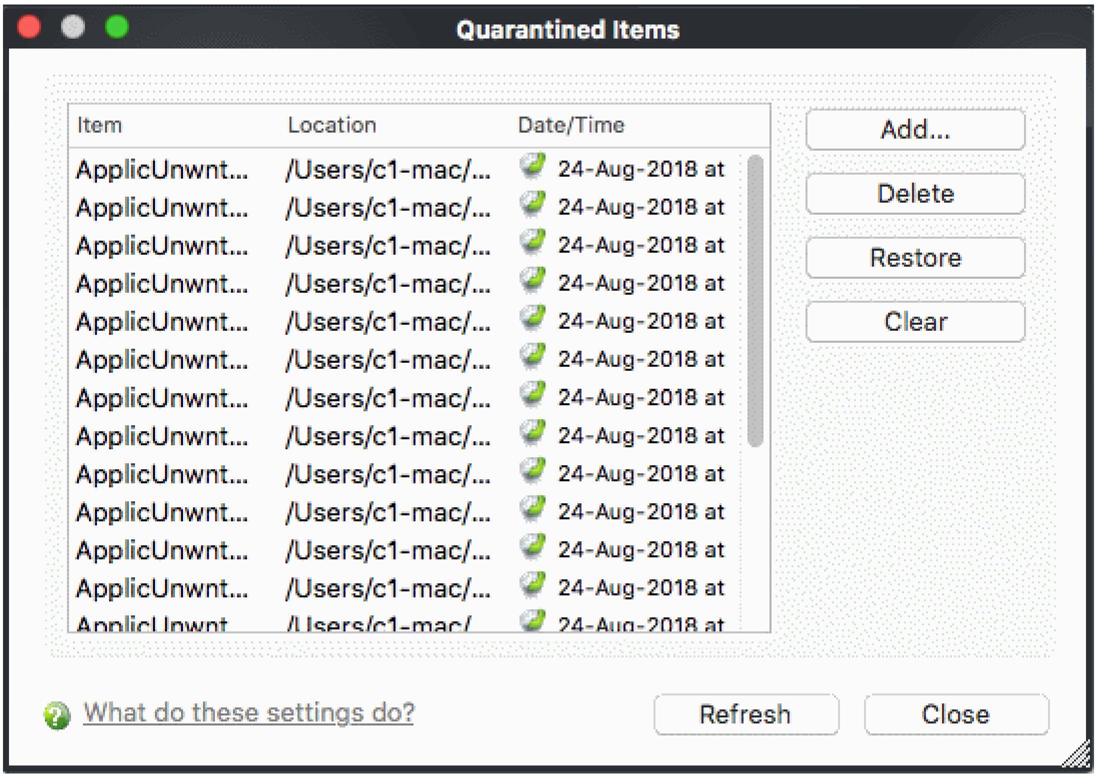
- Quarantine is an encrypted holding area for threats identified by the antivirus scanner.
- Quarantined files cannot be executed, so they present no danger to your computer or data.

The quarantine interface lets you:

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

View Quarantined Items

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



Item	Location	Date/Time
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt	/Users/c1-mac/	24-Aug-2018 at

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

Manually add files to quarantine

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

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

Delete a quarantined item from the system

- Open CCS > Click 'Antivirus' > 'Quarantined Items'
- Select the item and click 'Delete'.

This deletes the file from your computer permanently.

Restore a quarantined item to its original location

- Open CCS > Click 'Antivirus' > 'Quarantined Items'
- Select the item and click 'Restore'.
  - If the restored item does not contain a malware, it operates as usual
  - If it contains a malware, it is detected as a threat immediately

Delete all quarantined items

- Open CCS > Click 'Antivirus' > 'Quarantined Items'
- Click 'Clear'

This deletes all the quarantined items from the system permanently.

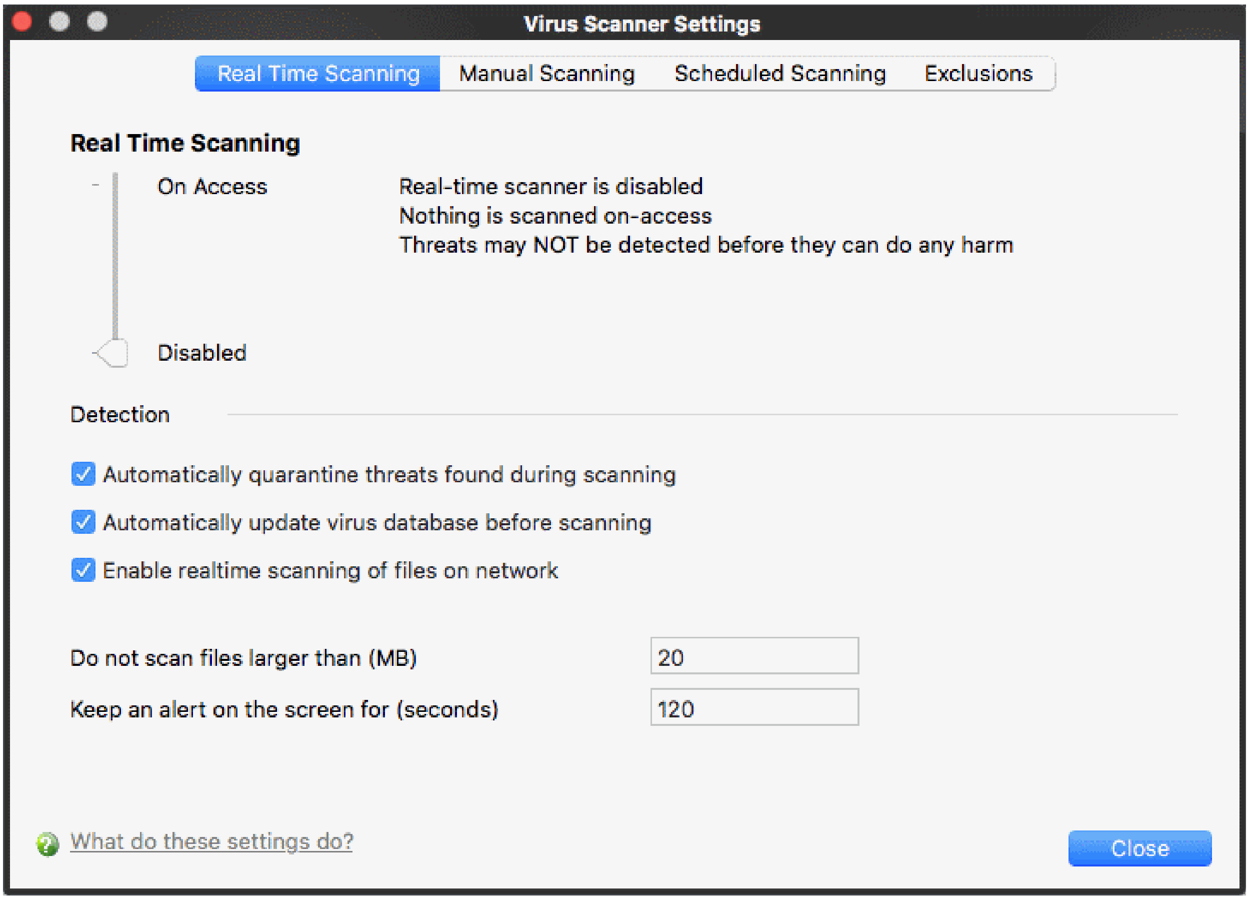
3.4. Scanner Settings

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

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

Open Scanner Settings

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



Real Time Scanning

Real-time scanner is disabled
Nothing is scanned on-access
Threats may NOT be detected before they can do any harm

Detection

☑ Automatically quarantine threats found during scanning

☑ Automatically update virus database before scanning

☑ Enable realtime scanning of files on network

Do not scan files larger than (MB) 20

Keep an alert on the screen for (seconds) 120

Antivirus settings are broken down into the following areas:

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

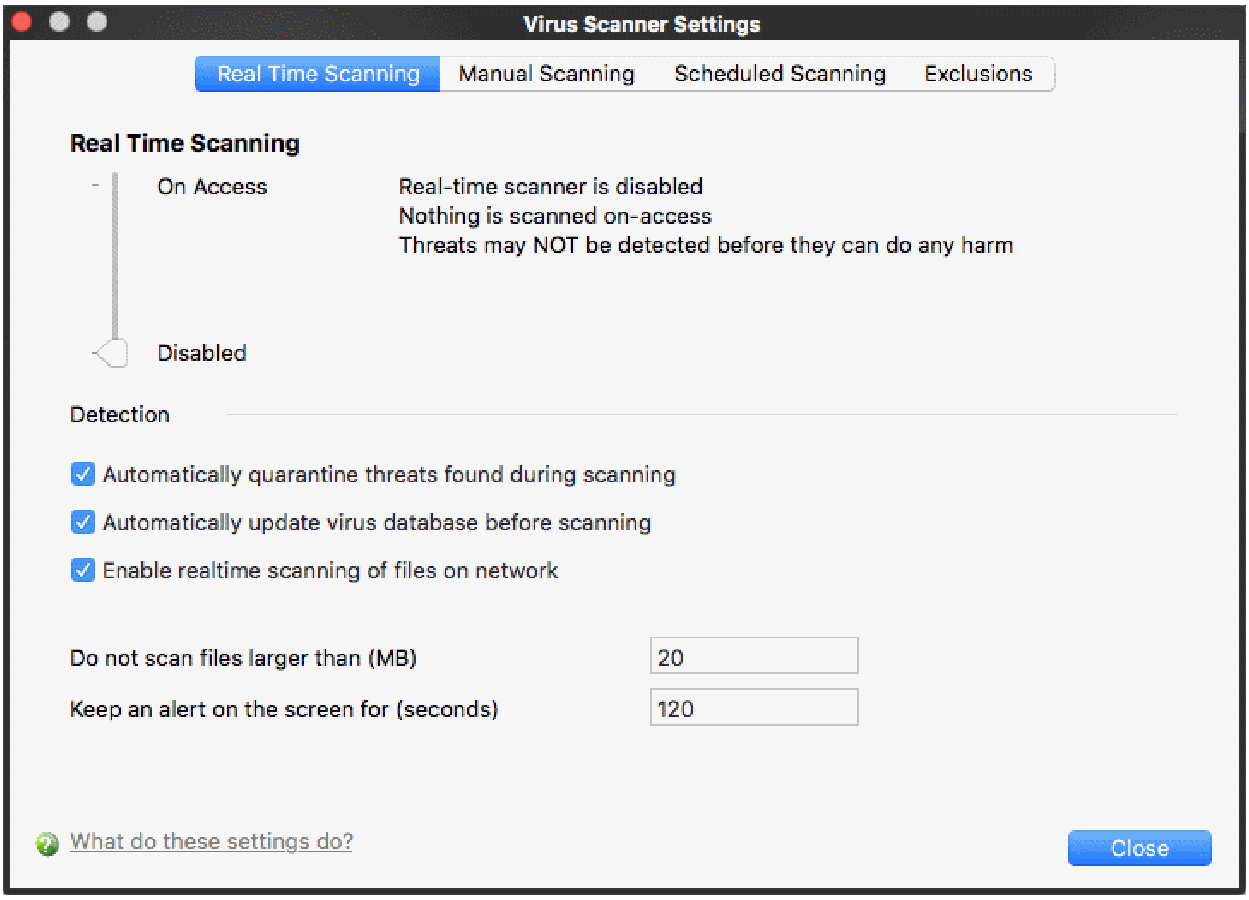
3.4.1. Real Time Scan

- The real-time scanner is the 'always on' virus monitor which runs in the background, checking files when they are opened, copied or downloaded.
- We highly recommended you keep the real-time scanner active at all times.

- The real-time scanning area lets you enable or disable the scanner, and configure scan options.
- Note: Managed endpoints - Scanner settings should be configured in the Endpoint Manager profile.

Set the 'Real Time Scanning' level

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



Virus Scanner Settings

Real Time Scanning

On Access

Disabled

Real-time scanner is disabled
Nothing is scanned on-access
Threats may NOT be detected before they can do any harm

Detection

☑ Automatically quarantine threats found during scanning

☑ Automatically update virus database before scanning

☑ Enable realtime scanning of files on network

Do not scan files larger than (MB) 20

Keep an alert on the screen for (seconds) 120

Use the slider to enable or disable the real-time virus monitor:

- **On Access** - Any file opened is scanned before it is allowed to run.
- **Disabled** - Switches the real-time scanner off.

Detection Settings

- **Automatically quarantine threats found during scanning** - Select the action to be taken when CCS finds malware on your computer.
  - **Enabled** - Detected threats are moved to quarantine, a secure holding area for suspicious files. Quarantined files cannot be executed so pose no threat to your computer. See **Quarantined Items** for more details. ***(Default).***
  - **Disabled** - Detected threats are not quarantined. Instead, an alert is shown with details about the threat. You can block or ignore the threat at the alert. See **Understand CCS Alerts** for more help with this.
- **Automatically update virus database before scanning** - CCS will check for and download the latest virus database prior to running a scan ***(Default = Enabled).***
- **Enable realtime scanning of files on network** - Activate or deactivate automatic scans of files on network drives.
  - **Enabled** - CCS checks all files you interact with on a network drive, even if you do not copy it to your local machine.

- **Disabled -** Network files are not checked unless you copy them to your local machine (***Default***).
- **Do not scan files larger than -** Set the maximum file size that the real-time scanner should scan. Files larger than the size specified here are not scanned ***(Default = 20 MB).***
- **Keep an alert on the screen for -** Set the length of time that the alert message should stay on the screen ***(Default = 120 seconds)***.
- Click 'Close'

3.4.2. Manual Scan

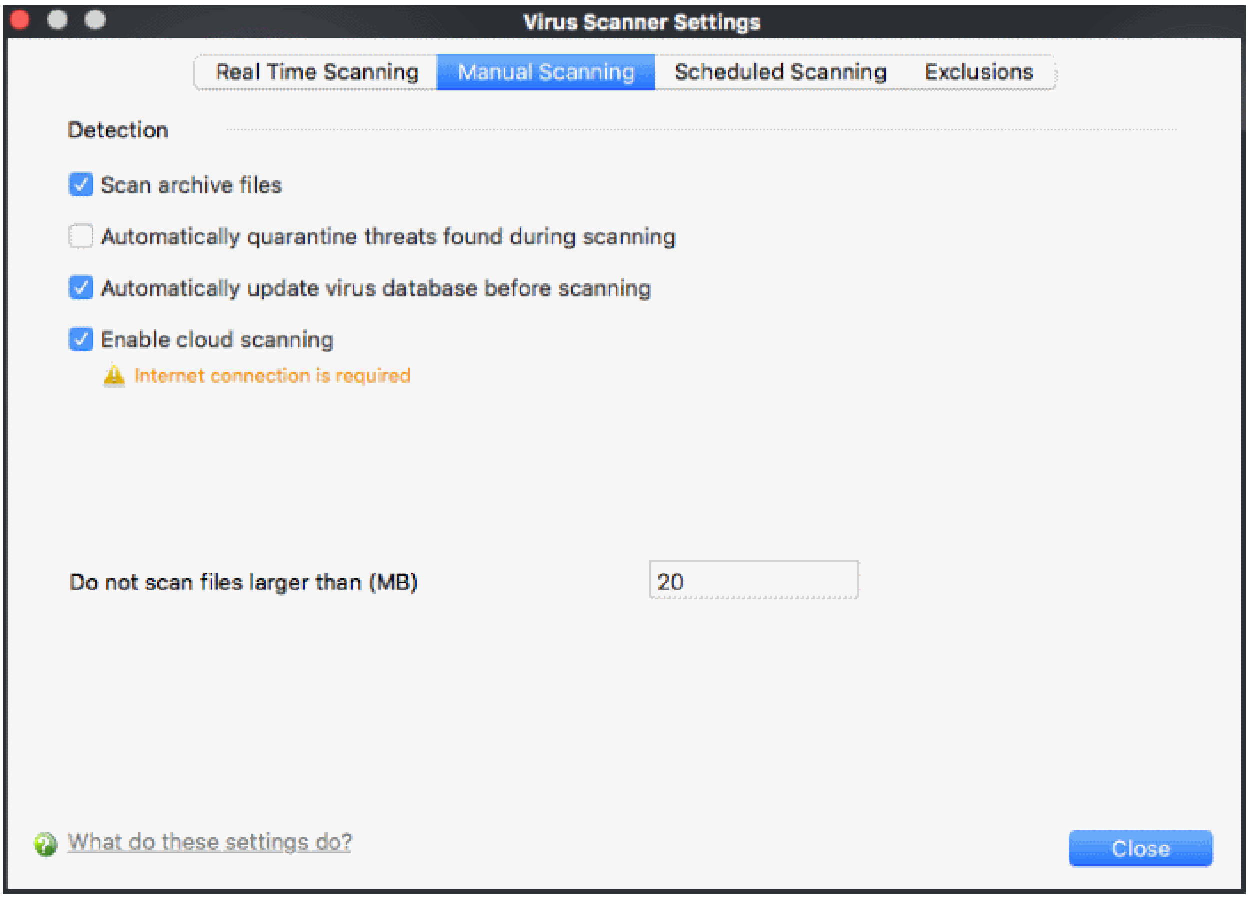
The options in the manual scanning area apply to any on-demand scans you run. For example, these settings are used when:

- You click 'Scan Now' on the home screen then run a full, quick or custom scan
- You drag an item into the scan-box on the home screen
- You right-click on a file and select 'Scan with COMODO Client – Security'.

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

Configure Manual Scans

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



Detection

☑ Scan archive files

□ Automatically quarantine threats found during scanning

☑ Automatically update virus database before scanning

☑ Enable cloud scanning

⚠ Internet connection is required

Do not scan files larger than (MB) 20

- **Scan archive files -** The antivirus will scan archive files such as .ZIP and .RAR files. 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 -** CCS will place any threats it finds in quarantine, a secure holding area for suspicious files. Files can be restored or deleted from quarantine at your will ***(Default = Enabled).***

- **Automatically update virus database before scanning -** Instructs CCS to download the latest virus database before starting an on-demand scan ***(Default = Enabled)***.

There are separate update options for real time, manual and scheduled scans. You can also manually update by clicking 'Antivirus' > 'Update Virus database'. See '**Update Virus Database**' for more details.

- **Enable cloud scanning -** CCS will use the latest online database to check whether a file is malware. The local scan is augmented with a real-time look-up of Comodo's online signature database. This makes it possible to detect zero-day malware even if your local database is outdated. ***(Default = Disabled)***.
  - Note - This setting needs to be enabled to submit unknown files to Valkyrie for analysis. Valkyrie is configured in the Endpoint Manager profile.
- **Do not scan files larger than -** Set the maximum file size that the AV should attempt to scan. Files larger than the size specified here are not scanned ***(Default = 20 MB)***.

- Click 'Close'

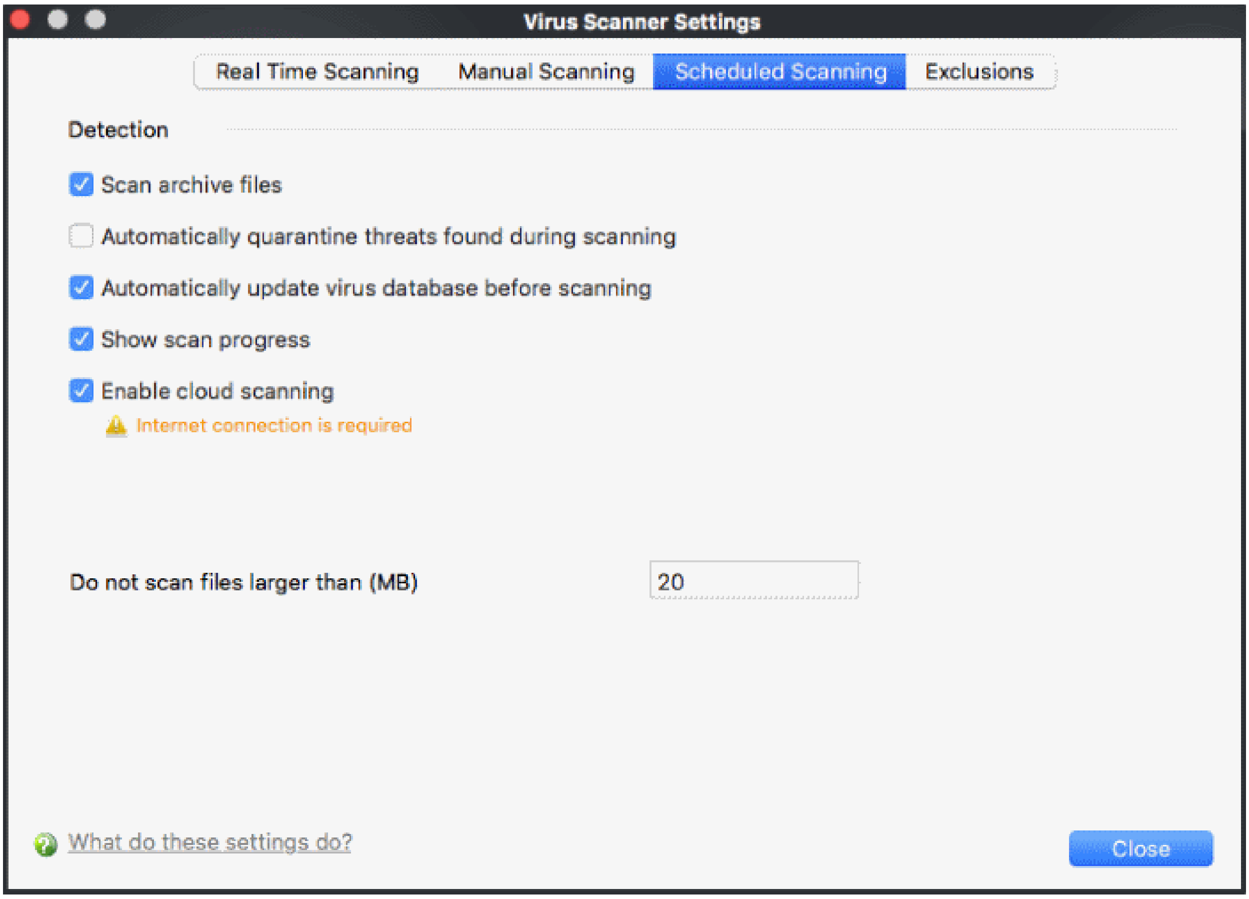
3.4.3. Scheduled Scan

The options you set in the 'Scheduled Scanning' area will apply to every scheduled scan you create.

- Note: Managed endpoints - Scanner settings should be configured in the Endpoint Manager profile.

Configure scheduled scan options

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



Detection

☑ Scan archive files

□ Automatically quarantine threats found during scanning

☑ Automatically update virus database before scanning

☑ Show scan progress

☑ Enable cloud scanning

Internet connection is required

Do not scan files larger than (MB) 20

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.

- **Scan archive files -** The antivirus will scan archive files such as .ZIP and .RAR files. 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 -** CCS will place any threats it finds in quarantine, a secure holding area for suspicious files. Files can be restored or deleted from quarantine at your will ***(Default = Enabled).***
- **Automatically update virus database before scanning** - Instructs CCS to download the latest virus database before starting an on-demand scan ***(Default = Enabled)***.

There are separate update options for real time, manual and scheduled scans. You can also manually update by clicking 'Antivirus' > 'Update Virus database'. See '**Update Virus Database**' for more details.

- **Enable cloud scanning -** CCS will use the latest online database to check whether a file is malware. The local scan is augmented with a real-time look-up of Comodo's online signature database. This makes it possible to detect zero-day malware even if your local database is outdated. ***(Default = Disabled)***.
  - Note - This setting needs to be enabled to submit unknown files to Valkyrie for analysis. Valkyrie is configured in the Endpoint Manager profile.
- **Do not scan files larger than -** Set the maximum file size that the AV should attempt to scan. Files larger than the size specified here are not scanned ***(Default = 20 MB)***.

- Click 'Close

3.4.4. Exclusions

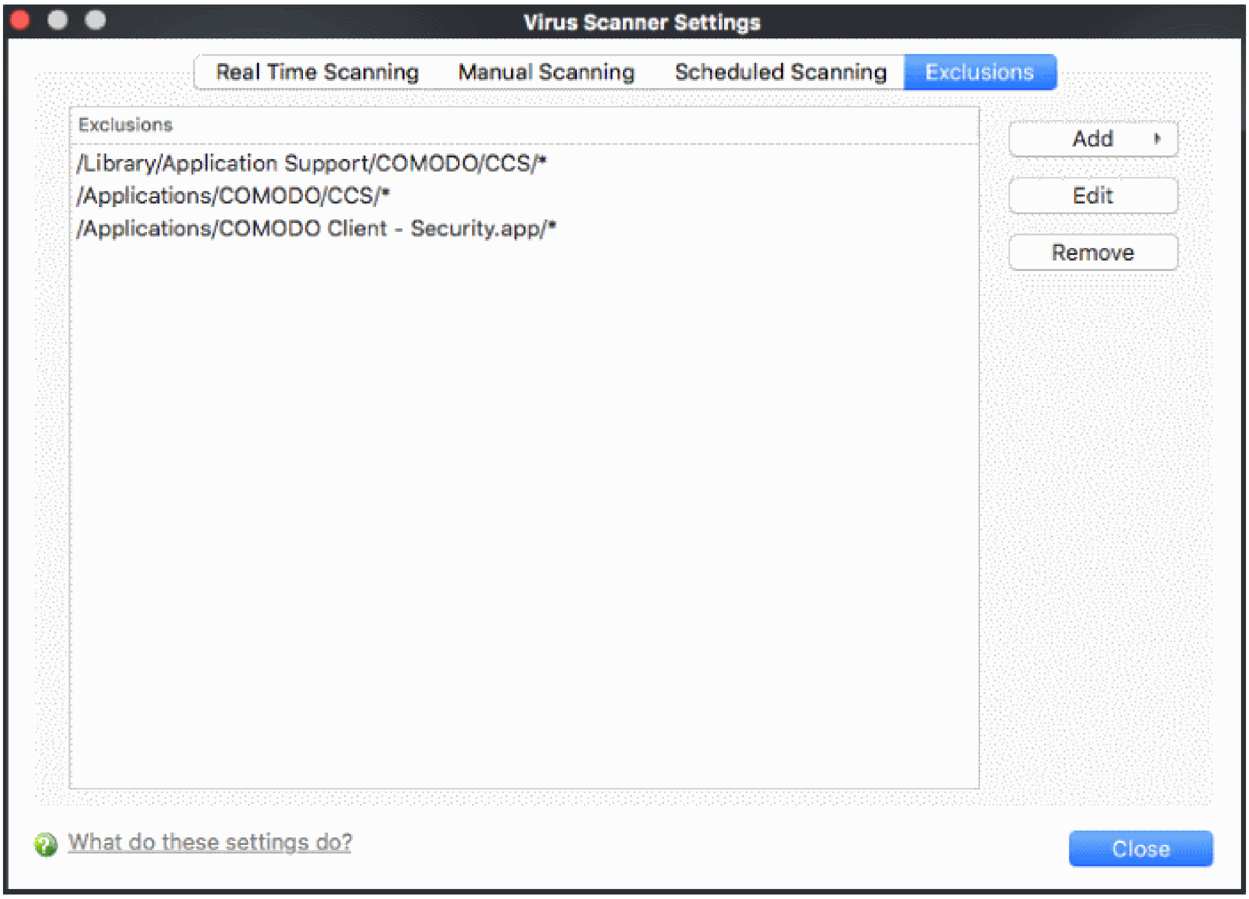
The 'Exclusions' tab shows threats which you ignored and and created an exception for. You can create exceptions at a virus alert, or in the results at the end of a scan.

Use this interface to add more exceptions or remove existing exceptions.

- Note: Managed endpoints - Scanner settings should be configured in the Endpoint Manager profile.

To set the 'Exclusions Scanning' level

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



Exclusions

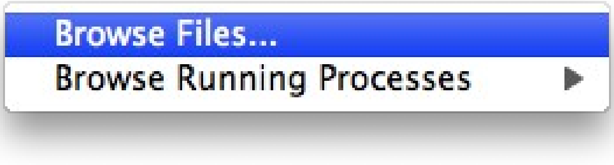
/Library/Application Support/COMODO/CCS/*
/Applications/COMODO/CCS/*
/Applications/COMODO Client - Security.app/*

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

- Click 'Add'. There are two methods available to choose the application that you want to trust: 'Browse Files...' and 'Browse Running Processes':



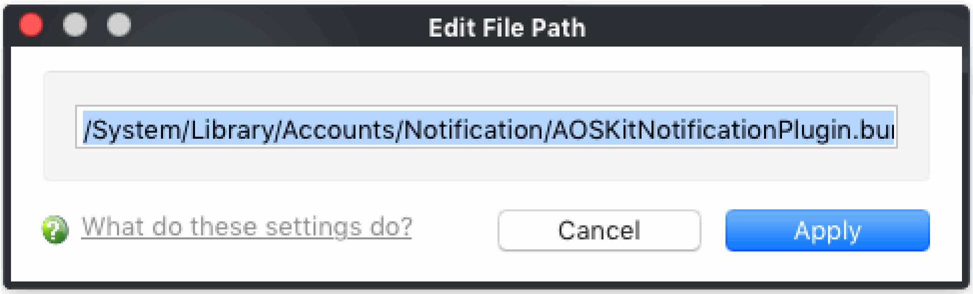
  - **Browse Files...** - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.
  - **Browse Running Processes -** As the name suggests, this option allows you to choose the target application from a list of processes that are currently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

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

- Click 'Close'

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.


Edit File Path
/System/Library/Accounts/Notification/AOSKitNotificationPlugin.bu
What do these settings do?
Cancel
Apply

- Click 'Apply'

3.5. Scheduled Scans

- The highly customizable scheduler lets you timetable virus scans according to your preference.
- You can schedule a scan of your entire computer or specific areas. You can create an unlimited number of schedules.
- You can run scans at daily, weekly, monthly or custom intervals.
- Note: Managed endpoints - Scheduled scans should be configured in the Endpoint Manager profile.

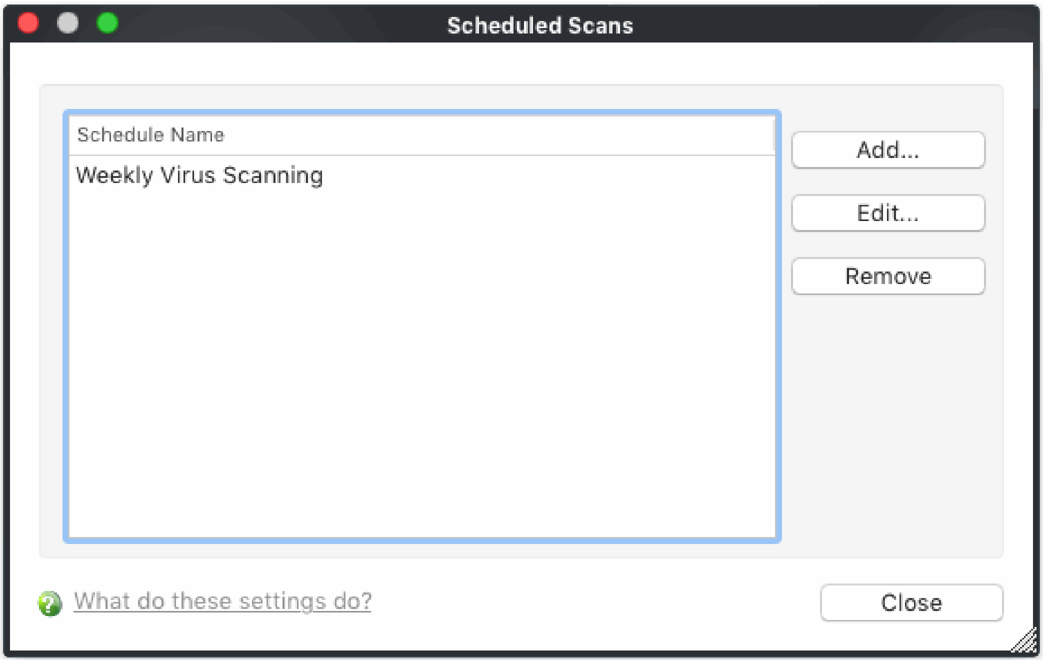
See the following for more help:

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

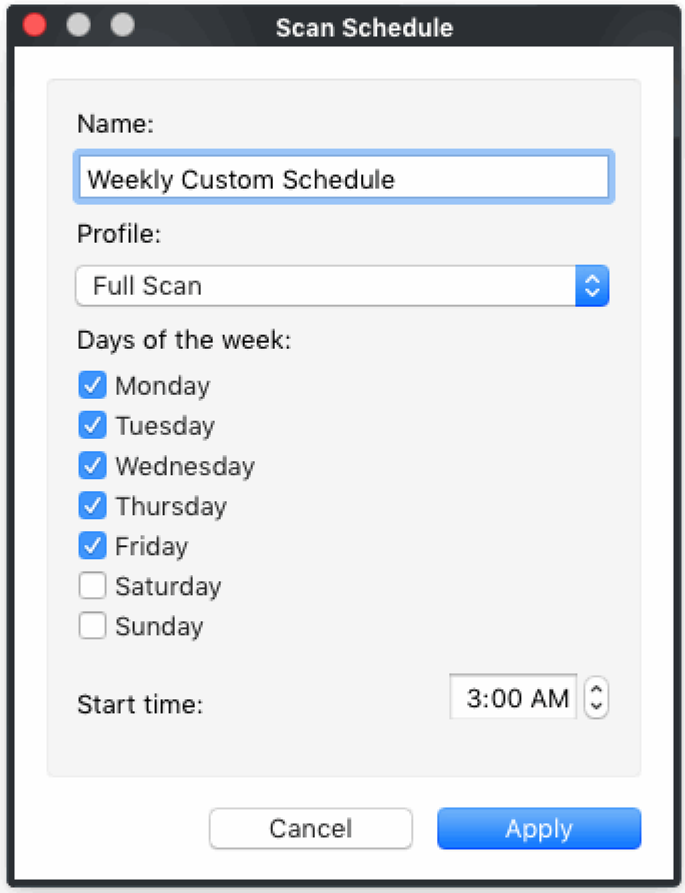
- Note. Click 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning' to configure general settings for all scheduled scans.

Create a scheduled scan

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



- Configure your schedule in the following settings screen:



Scan Schedule

Name:

Weekly Custom Schedule

Profile:

Full Scan

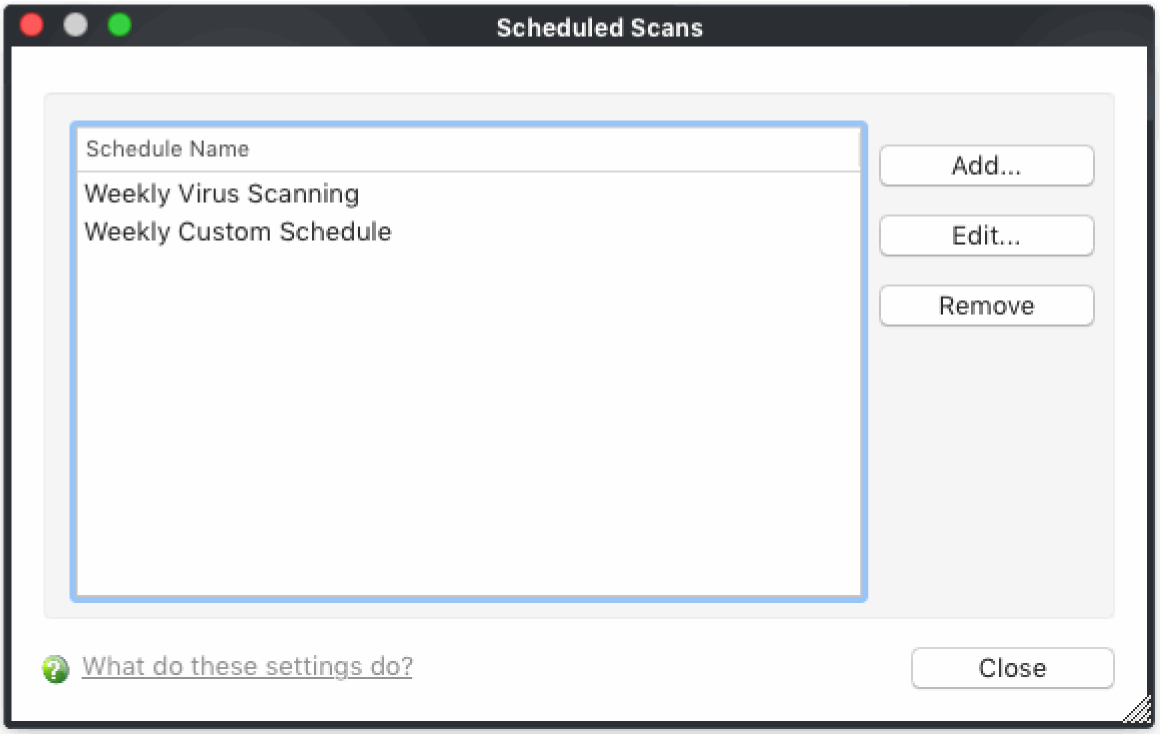
Days of the week:

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday
□ Sunday

Start time: 3:00 AM

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

- Click 'Apply'.



Scheduled Scans

Schedule Name
Weekly Virus Scanning
Weekly Custom Schedule

- Repeat the process to create more scan schedules.

Edit a scheduled scan

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

Remove a scheduled scan

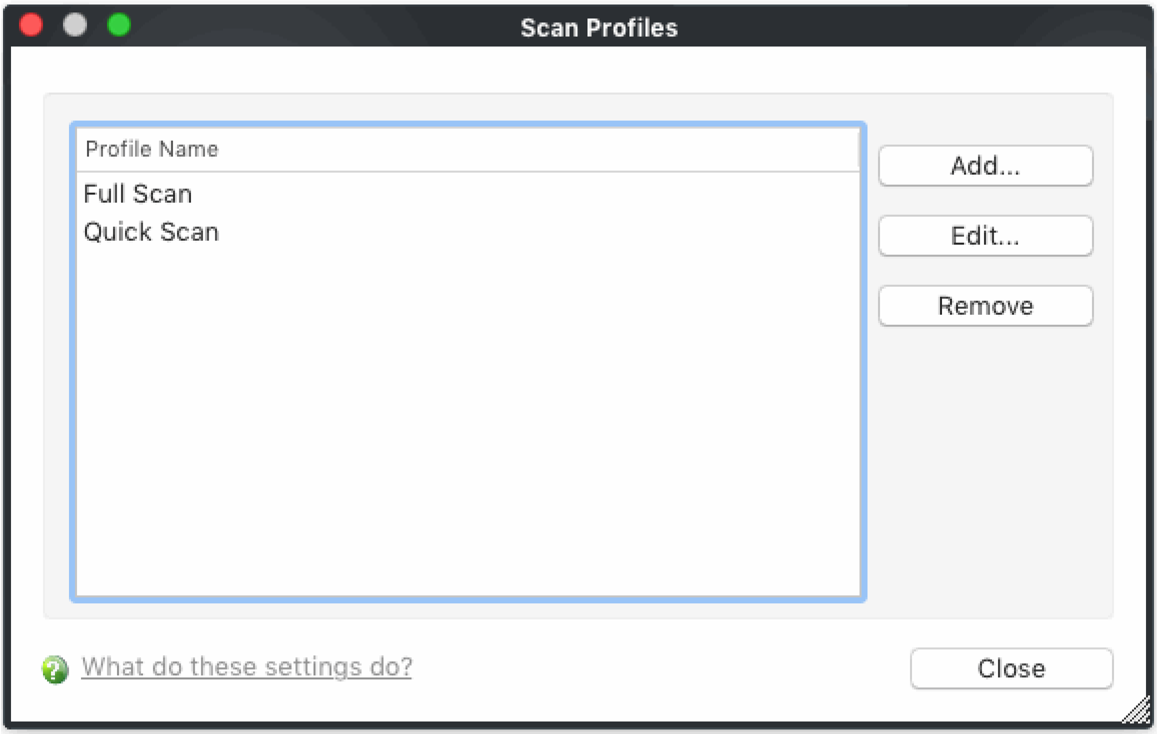
- Select the scan schedule profile you wish to cancel
- Click 'Remove'.

3.6. Scan Profiles

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

Open the Scan Profiles interface

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Scan Profiles' in the antivirus tasks interface.



Comodo Client - Security has two default profiles: 'Full Scan' and 'Quick Scan'. These two profiles are predefined and cannot be edited or removed.

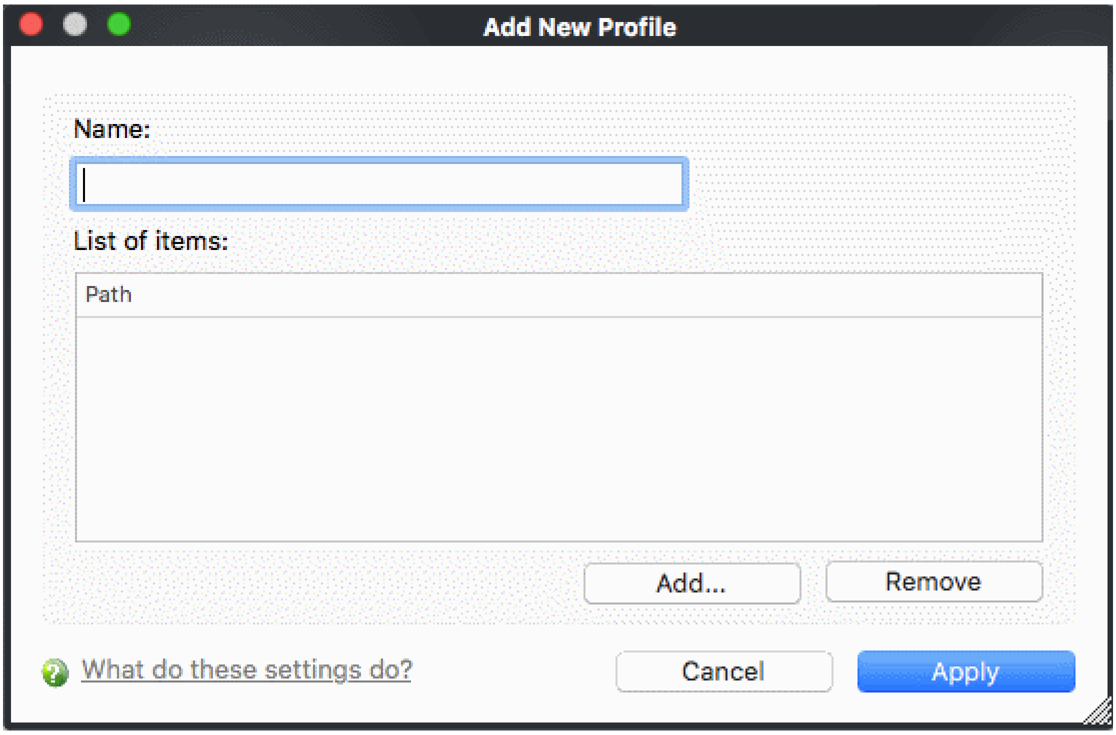
- **Full Scan** - CCS scans every local drive, folder and file on your system.
- **Quick Scan** - CCS runs a targeted scan of important operating system files and folders.

The following sections explain how to:

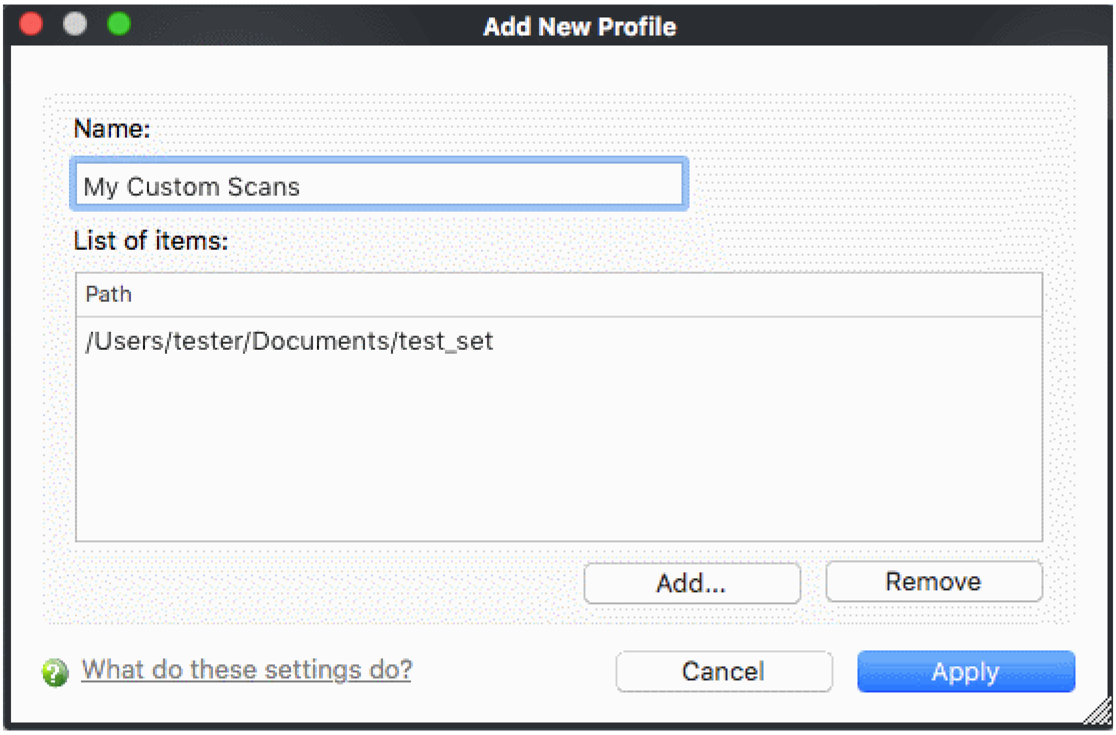
- **Create a scan profile**
- **Remove a custom scan profile**

To create a new scan profile

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



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



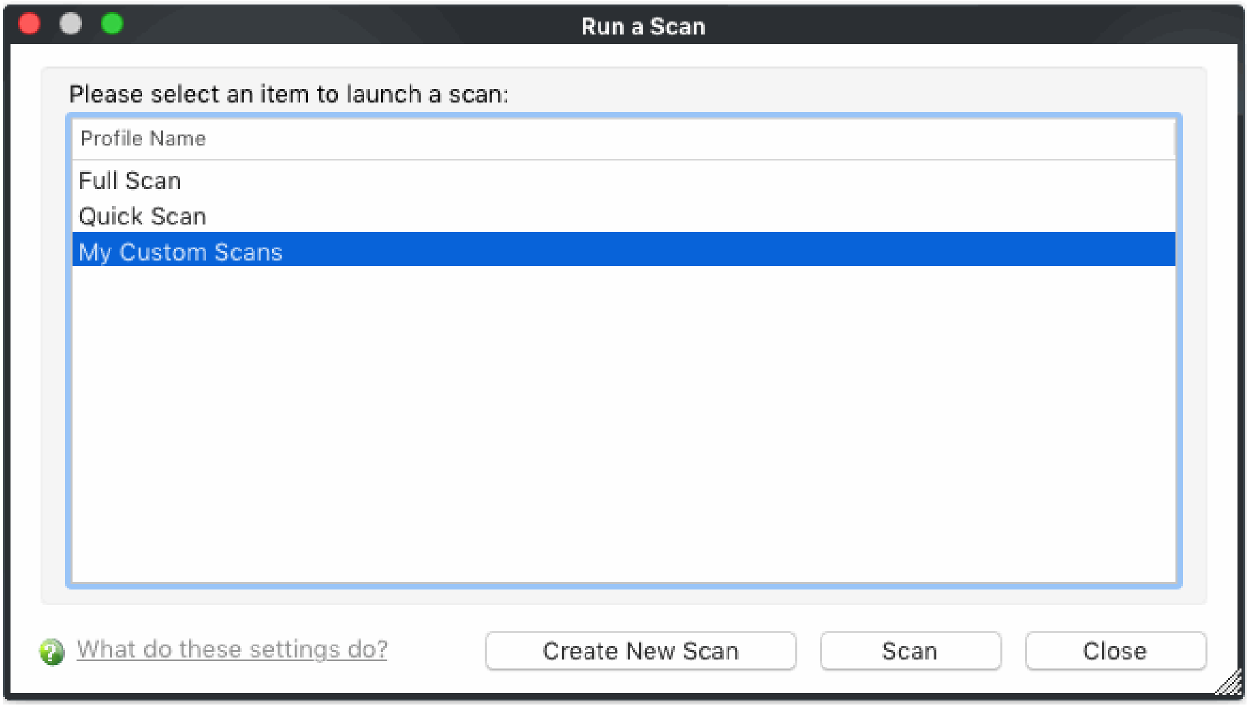
Name: My Custom Scans

List of items:

Path
/Users/tester/Documents/test_set

- To remove an item, select it from the dialog and click 'Remove'.
- Click 'Apply' for the created profiles to take effect.

The new profile will become available for selection in the 'Run a Scan' panel:



Run a Scan

Please select an item to launch a scan:

Profile Name
Full Scan
Quick Scan
My Custom Scans

It is also available for selection during a scheduled scan. See **Scheduled Scans** for more details.

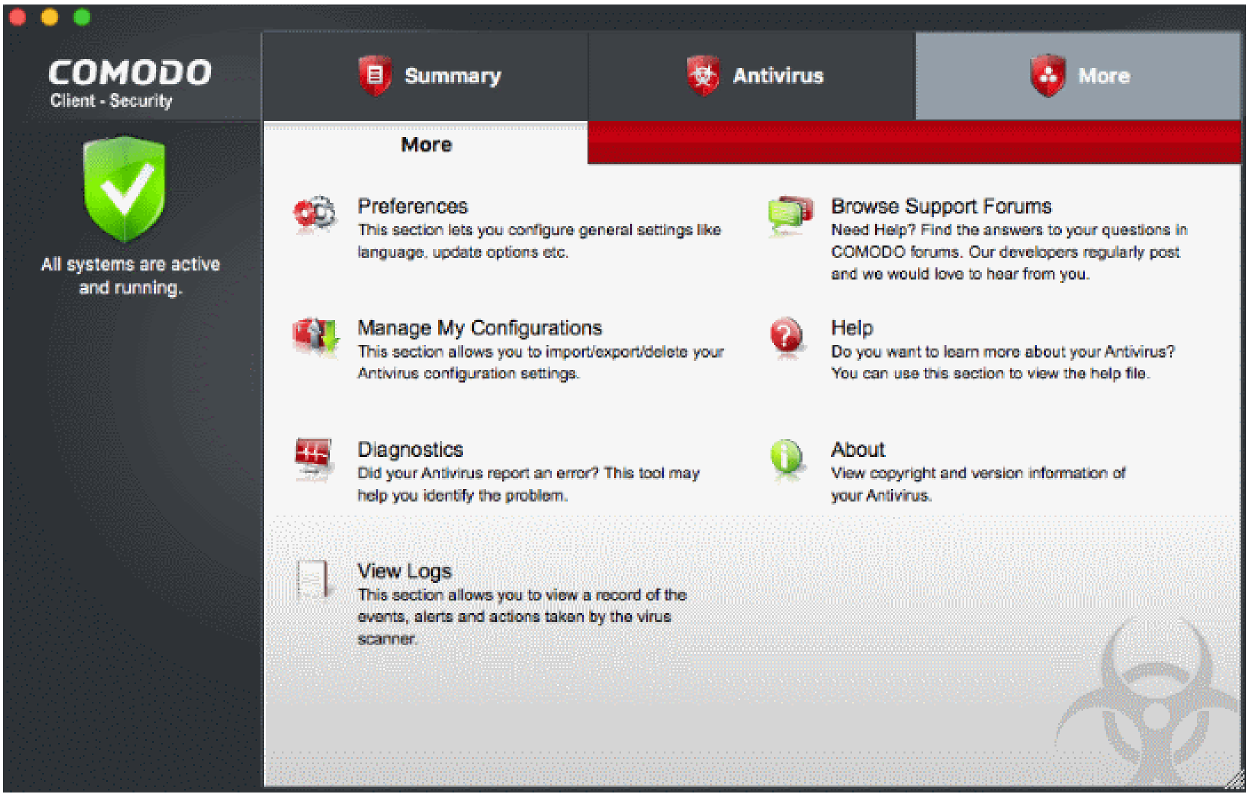
Remove a custom scan profile

- Select the profile you want to remove from the list and click 'Remove'

Note: You cannot delete predefined scan profiles (Full Scan and Quick Scan).

4. More Options - Introduction

The 'More Options' area lets you view and modify various program settings. It also contains utilities and shortcuts to help enhance your experience with Comodo Client Security.



Preferences
This section lets you configure general settings like language, update options etc.

Browse Support Forums
Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.

Manage My Configurations
This section allows you to import/export/delete your Antivirus configuration settings.

Help
Do you want to learn more about your Antivirus? You can use this section to view the help file.

Diagnostics
Did your Antivirus report an error? This tool may help you identify the problem.

About
View copyright and version information of your Antivirus.

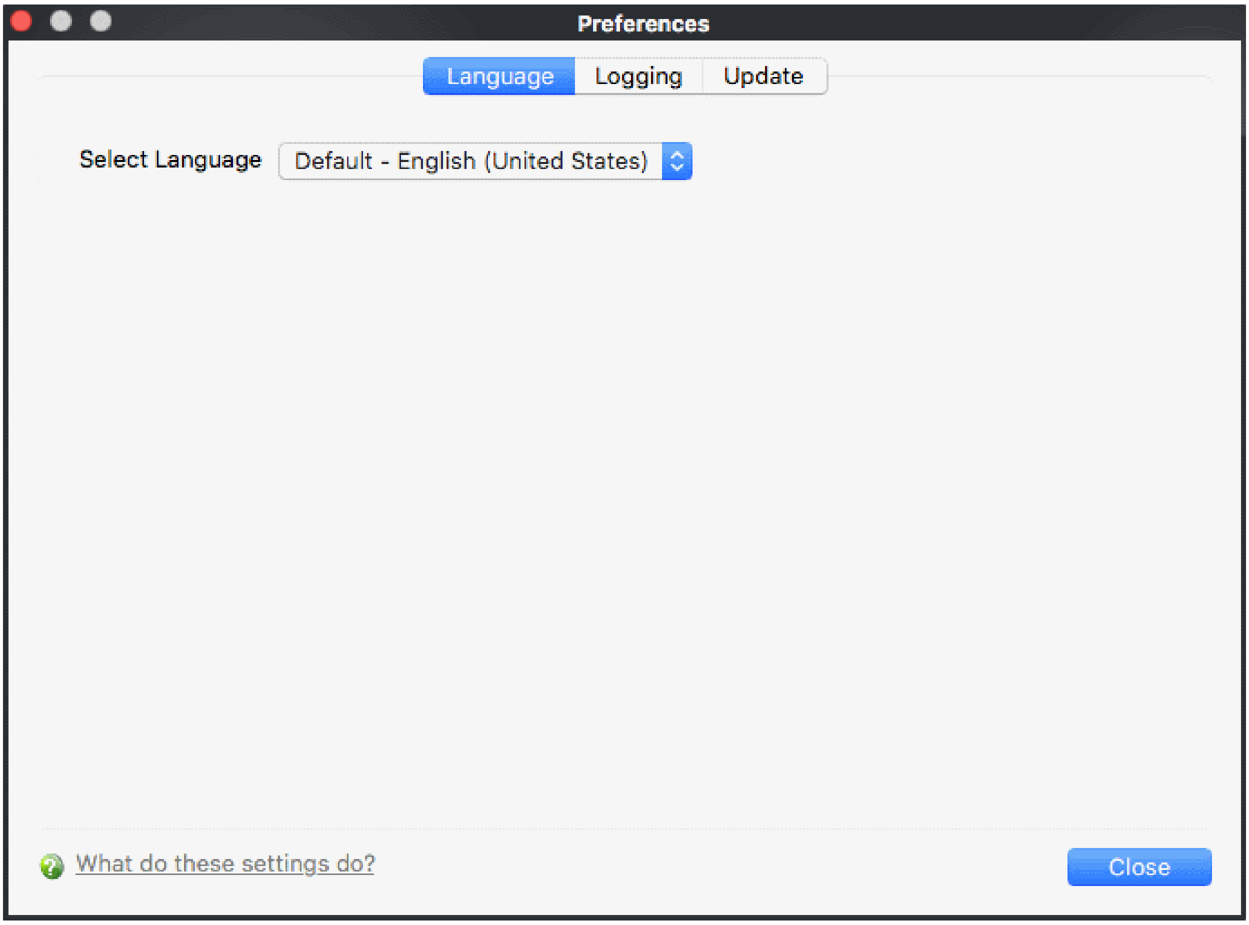
View Logs
This section allows you to view a record of the events, alerts and actions taken by the virus scanner.

The area has shortcuts for the following tasks:

- **Preferences** - Configure interface language, update options and log preferences.
- **Manage My Configurations** - Import/export CCS configuration profiles
- **Diagnostics** - Identify any problems with your installation
- **Browse Support Forums** - Link to Comodo community forums
- **Help** - Open the online help guide
- **About** - View product version and copyright information
- **View Logs** - Manage event logs

4.1. Preferences

- Open Comodo Client Security
- Click 'More' on the home screen then 'Preferences'
- The preferences area lets you specify top-level options regarding language, updates and event logging.



Select Language: Default - English (United States)

Click the following for more information:

- Language
- Logging
- Update

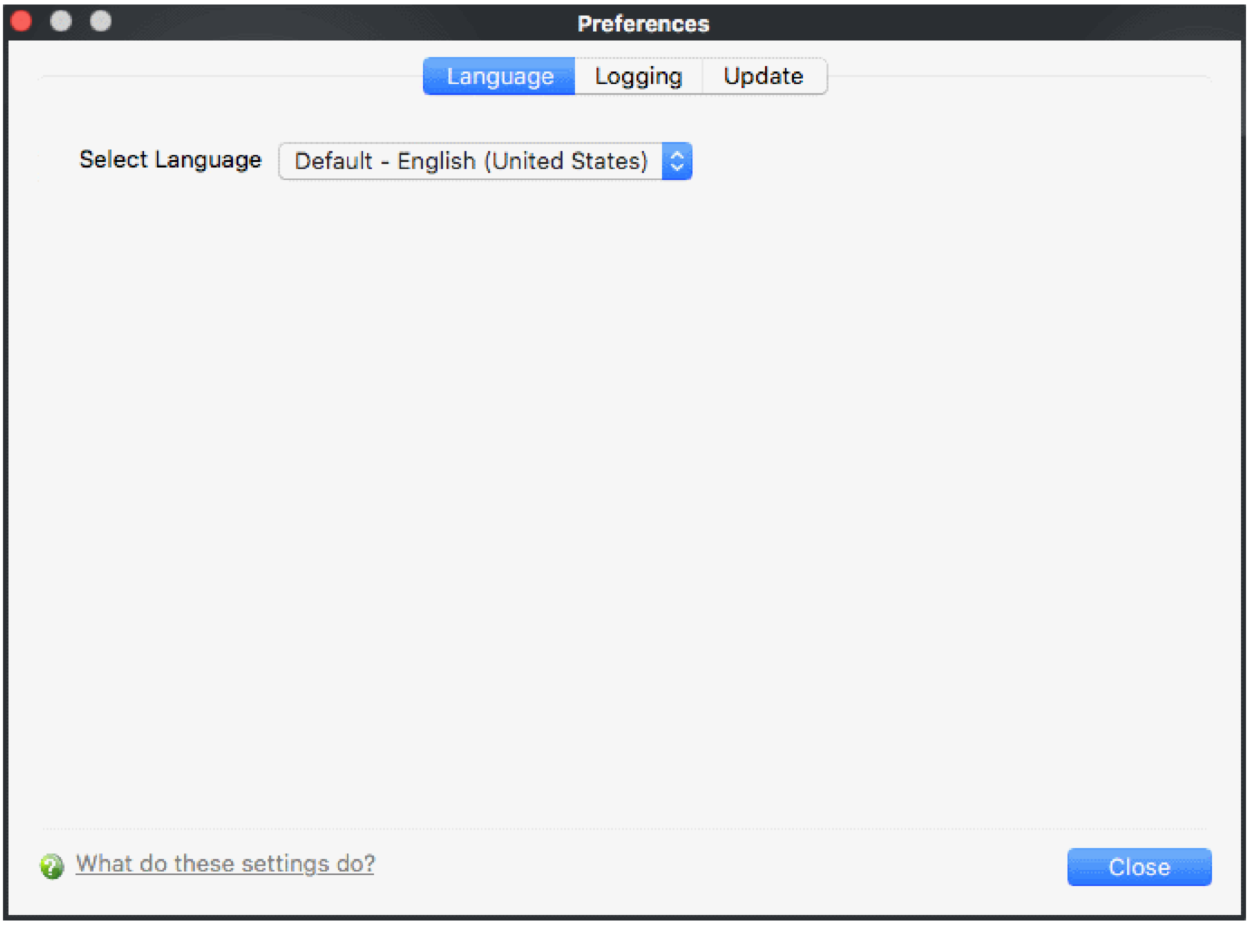
4.1.1. Language Settings

The 'Language' area lets you choose the language which is shown in the CCS interface.

To open the language interface screen

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

The settings screen will open:



Select Language: Default - English (United States)

CCS for Mac is available in multiple languages.

- **Select Language -** Choose your preferred language from the drop-down ***(Default = English (United States)).***
- Click 'Close'

- You must restart the application for your language to take effect.

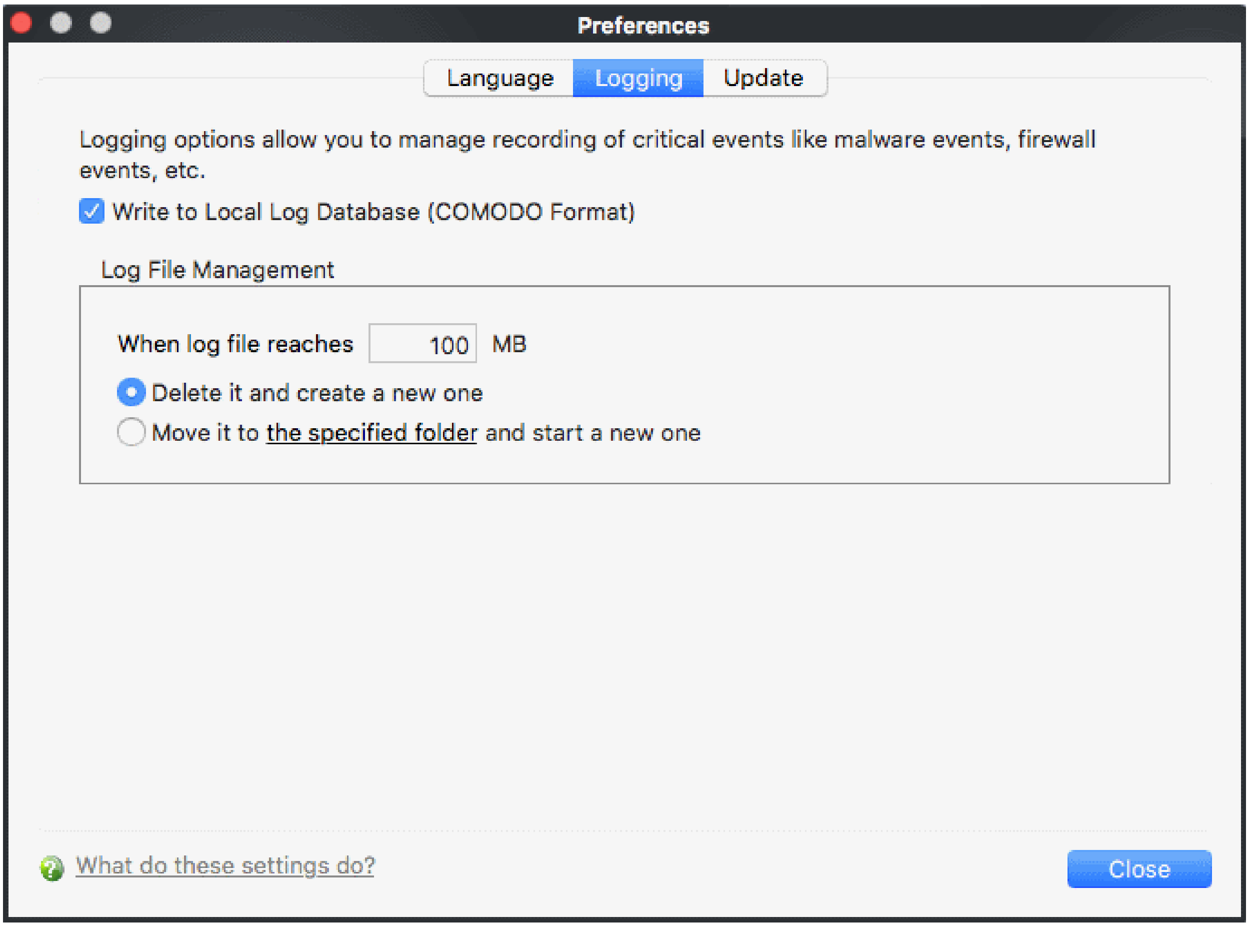
4.1.2. Log Settings

- Click 'More' on the home screen
- Click 'Preferences' > 'Logging'

The log settings area lets you:

- Enable or disable logging. (Note: Managed endpoints **-** Log settings should be configured in the Endpoint Manager profile)
- Configure how CCS should behave once a log file reaches a certain size.
- CCS logs all events by default. Logs can be viewed by clicking 'Antivirus' on the home screen then '**View Antivirus Events**'.

The settings screen opens:



Logging options allow you to manage recording of critical events like malware events, firewall events, etc.

☑ Write to Local Log Database (COMODO Format)

Log File Management

When log file reaches 100 MB

● Delete it and create a new one

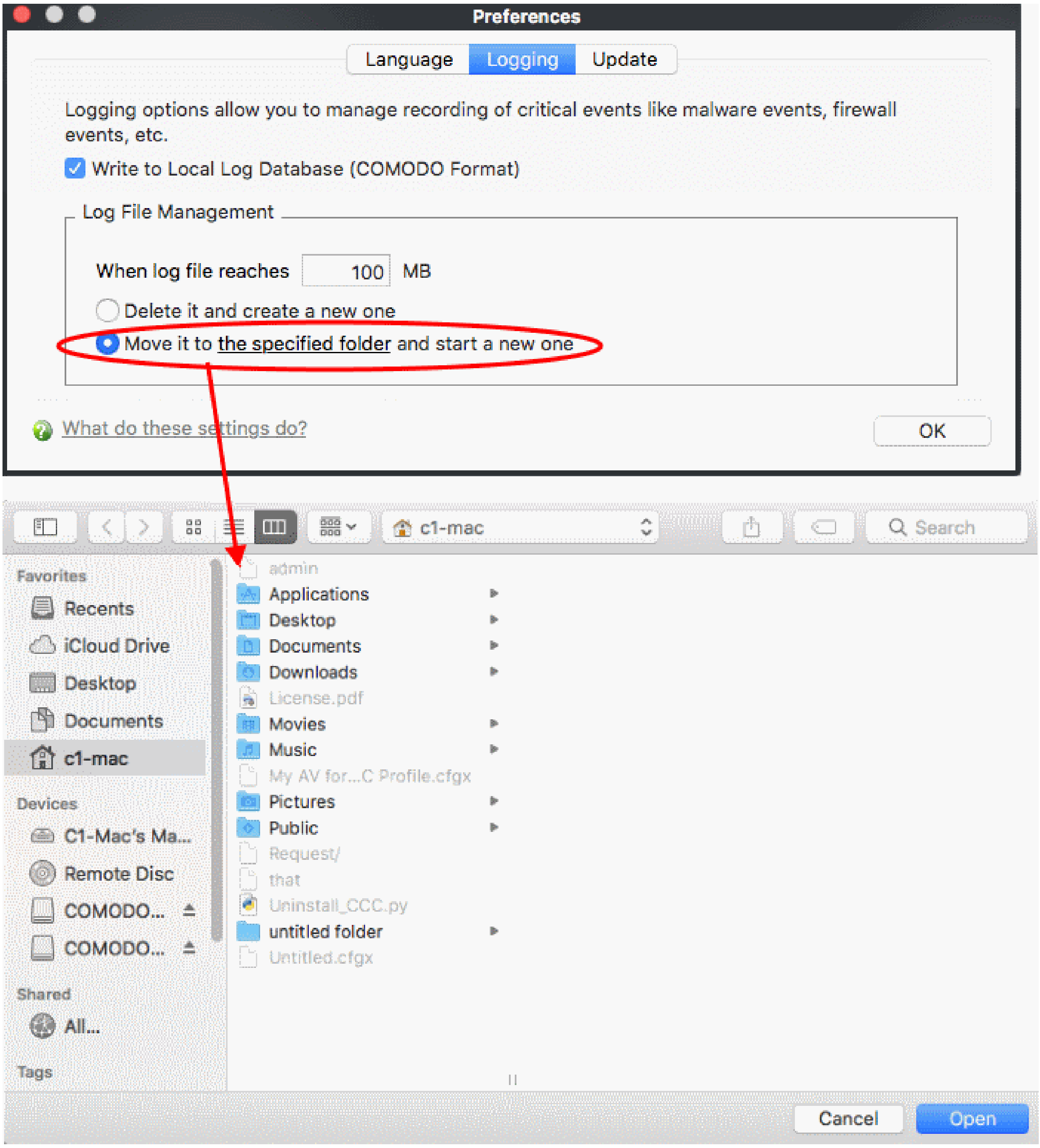
○ Move it to the specified folder and start a new one

General Log File Options

- **Write to local log database (COMODO format)** - CCS logs events in Comodo format and the log storage depends on settings done in Log File Management section below. ***(Default = Enabled)***

Log File Management

- **When log file reaches (MB)** - Configure how to handle a log file when it reaches a spec size.
  - **When the log file reaches...** - Specify the maximum size of a log file ***(Default = 100 MB).***
  - **Delete it and create a new one** - Creates a blank new file when the max. size is reached, and deletes the old one.***(Default = Enabled).***
  - **Move it to...** - Starts a new file once the log reaches the max size. The old log is archived in the location you specify. ***(Default = Disabled).***



Preferences

Language | Logging | Update

Logging options allow you to manage recording of critical events like malware events, firewall events, etc.

☑ Write to Local Log Database (COMODO Format)

Log File Management

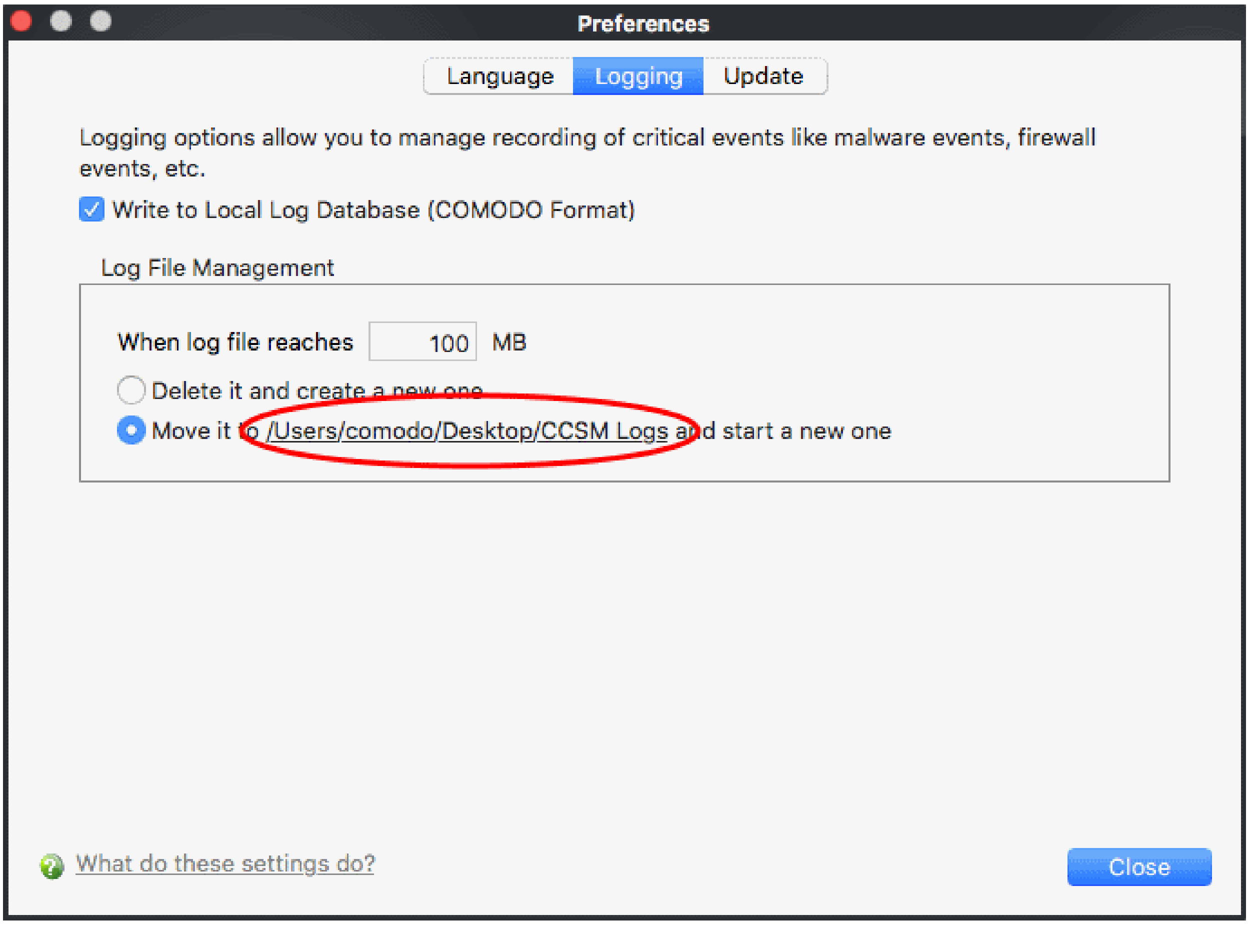
When log file reaches 100 MB

○ Delete it and create a new one

● Move it to the specified folder and start a new one

What do these settings do?

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



Logging options allow you to manage recording of critical events like malware events, firewall events, etc.

☑ Write to Local Log Database (COMODO Format)

Log File Management

When log file reaches 100 MB

○ Delete it and create a new one

● Move it to /Users/comodo/Desktop/CCSM Logs and start a new one

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

4.1.3. Update Settings

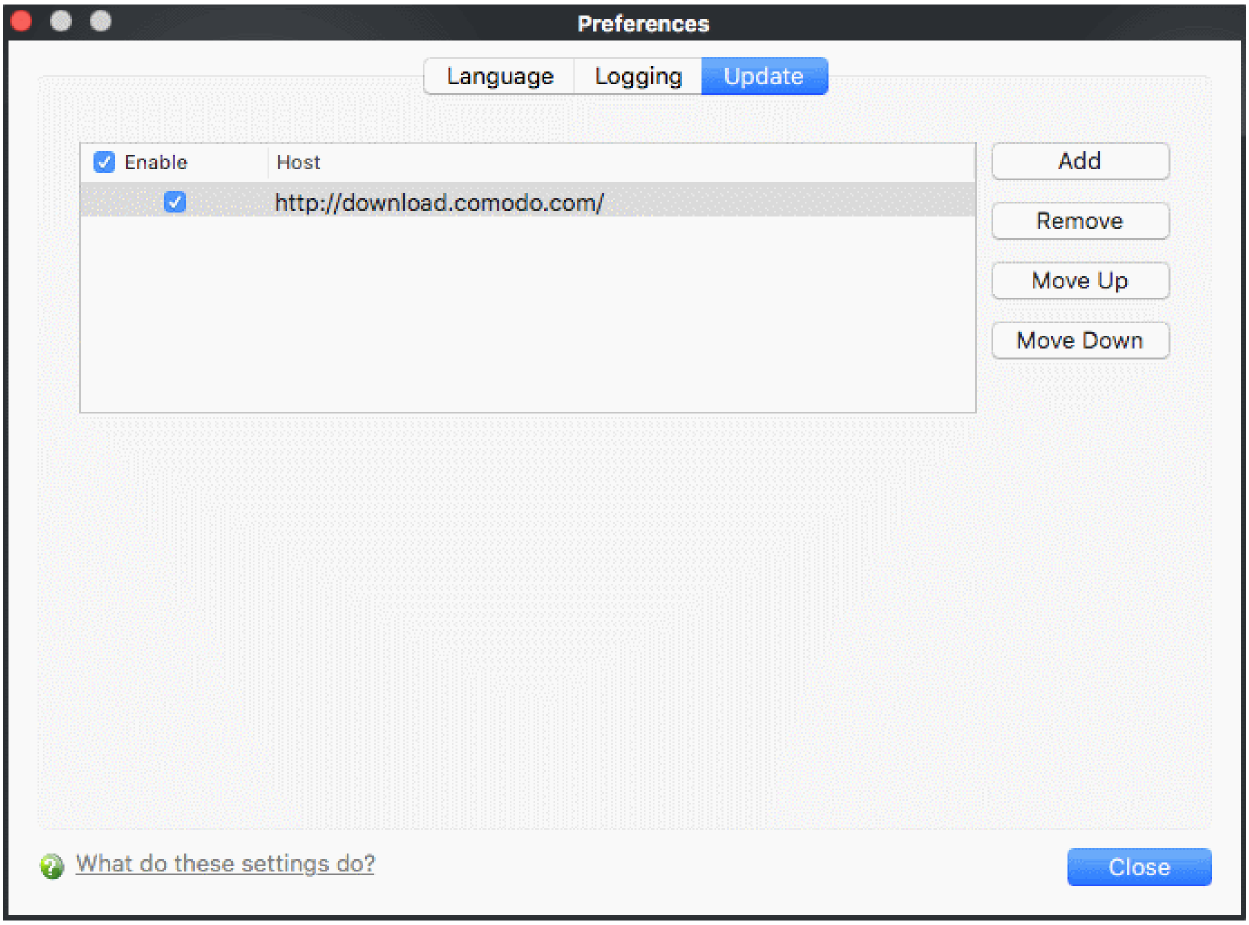
The 'Update' area lets you:

- Enable or disable automatic updates for CCS
- Choose the host from which updates should be downloaded. Default = **http://download.comodo.com**
- Note: Managed endpoints - Update settings should be configured in the Endpoint Manager profile.

To access the 'Updates' settings interface

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

The settings screen opens:



☑ Enable	Host
☑	http://download.comodo.com/

- By default, updates are downloaded from **http://download.comodo.com**
- Leave this setting alone if you always want to download updates from Comodo servers
- You can add the URL of an alternative download host if required. For example, you may want to store updates on a server on your local network prior to distribution to endpoints.

  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 to add multiple hosts.
  - Use 'Move Up' and 'Move Down' buttons to re-order the priority of host.
  - CCS for MAC will automatically check the host specified here and download updates from the host even when you are offline.
- Click 'Close'

4.2. Manage My Configurations

- Comodo Client - Security allows you to maintain, save and export multiple configurations of your security settings.
- Exporting your settings can be a great time-saver if:
  - You need to uninstall and re-install CCS in order to upgrade your system.
  - You are a network admin looking to roll out a standard security configuration to multiple computers.
- **Comodo Preset Configurations**
- **Import /Export and Managy Personal Configurations**

4.2.1. Comodo Preset Configurations

Click 'More' > 'Manage my configurations' to open this area.

- Comodo Antivirus ships with preset security profiles that strike a good balance between security and usability.
- The profile that is currently in use is the 'Active' profile.

The 'Comodo Client - Security' profile has the following default settings:

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

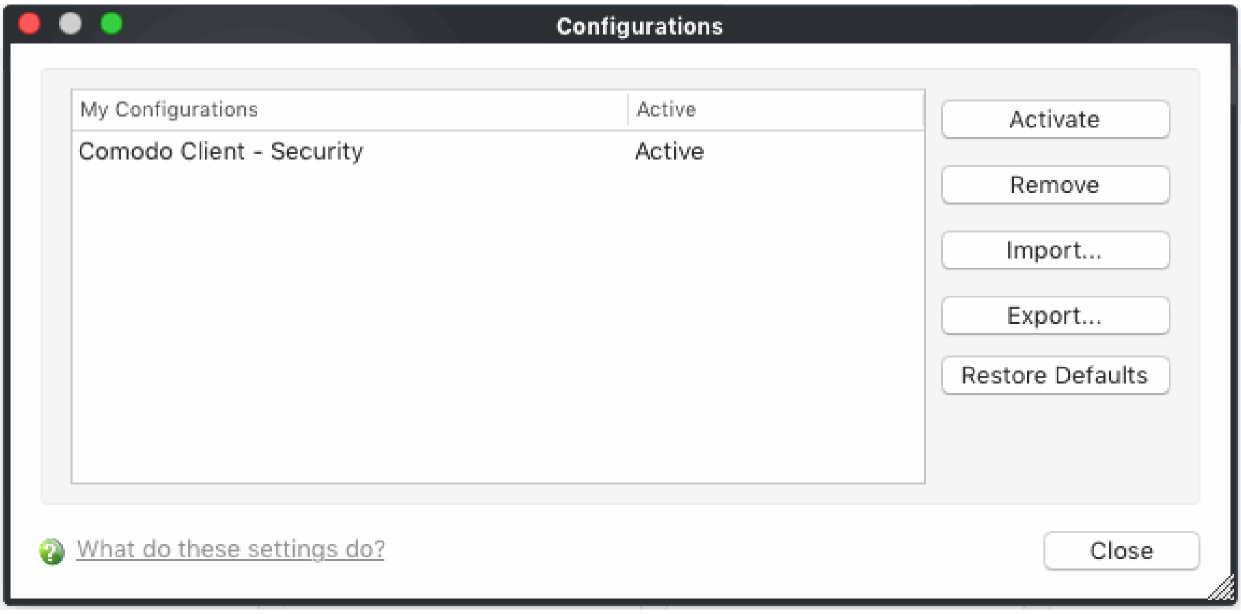
Click 'Restore Defaults' to revert to the the settings above.

- The 'Active' profile is updated over time if you make changes to your configuration.
- Exporting the active profile will, therefore, export your settings as they currently stand.

4.2.2. Import / Export And Manage Personal Configurations

To access the configurations interface

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



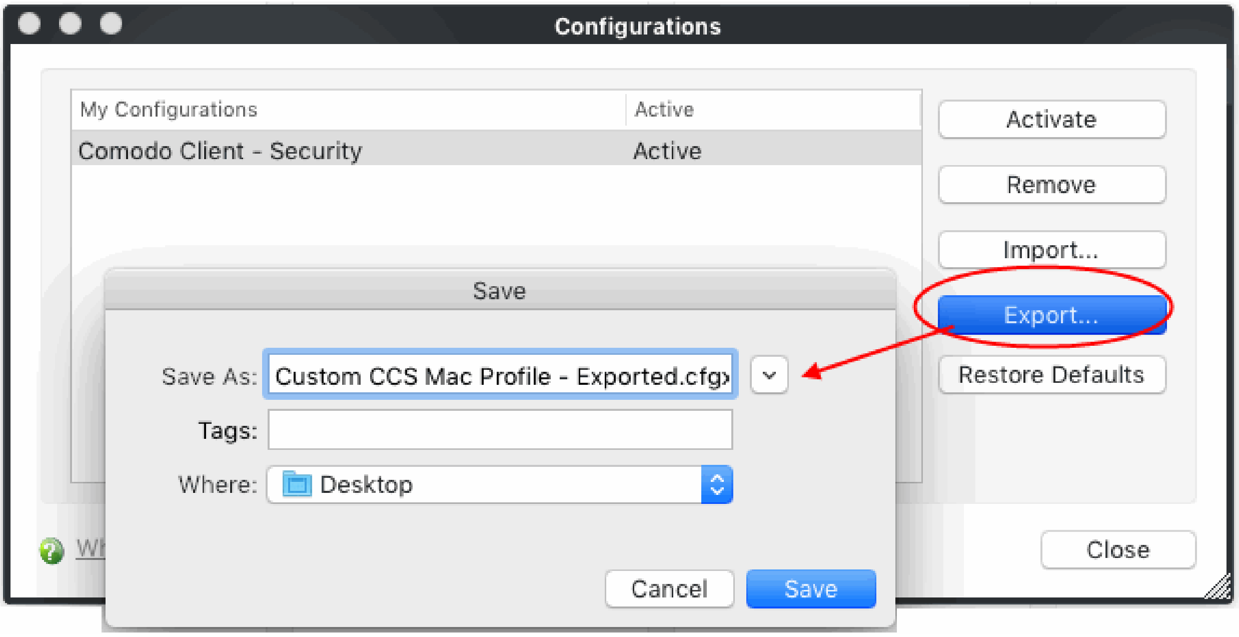
My Configurations	Active
Comodo Client - Security	Active

By default, the interface contains one preset configuration - 'Comodo Client - Security'. The current configuration is labeled as 'Active' in this interface.

- Click the area on which you would like more information:
  - **Export stored configuration to a file**
  - **Import a saved configuration from a file**
  - **Select a different active configuration setting**
  - **Delete a inactive configuration profile**
  - **Reset to a default profile**

Export stored configuration to a file

- Open CCS > select 'More'
- Select 'Configuration' > 'Export'
- Type a file name for the profile (e.g., 'Custom CCS for MAC Profile') and save to the location of your choice.

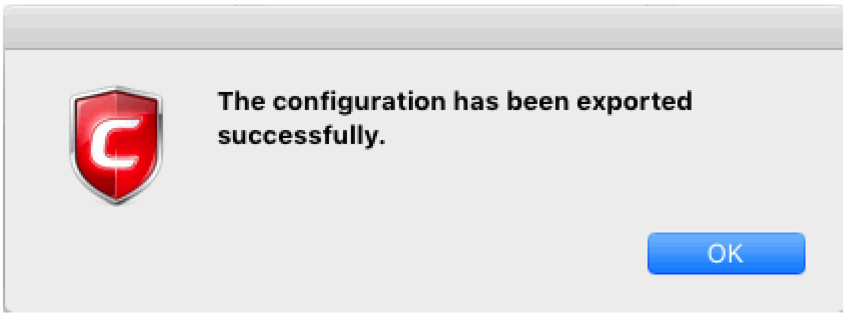


Comodo Client - Security Active

Save As: Custom CCS Mac Profile - Exported.cfgx

Where: Desktop

A confirmation dialog will appear if the export is successful:



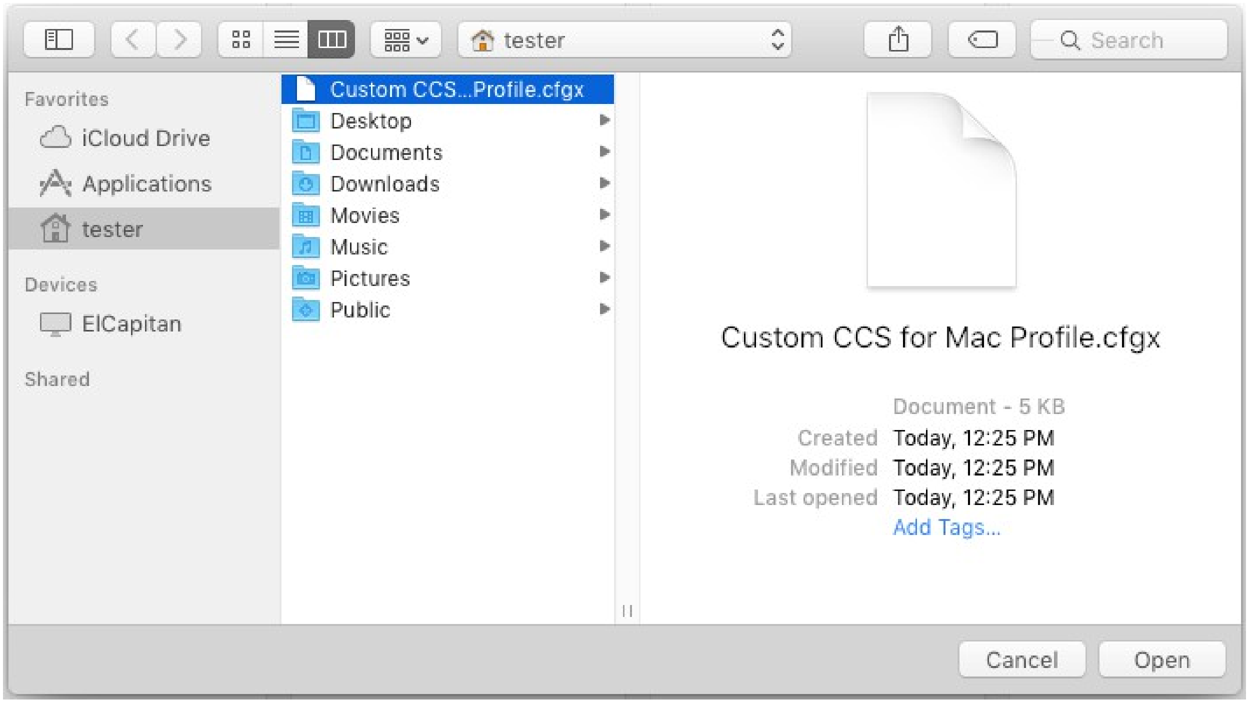
The configuration has been exported successfully.

Import a saved configuration from a file

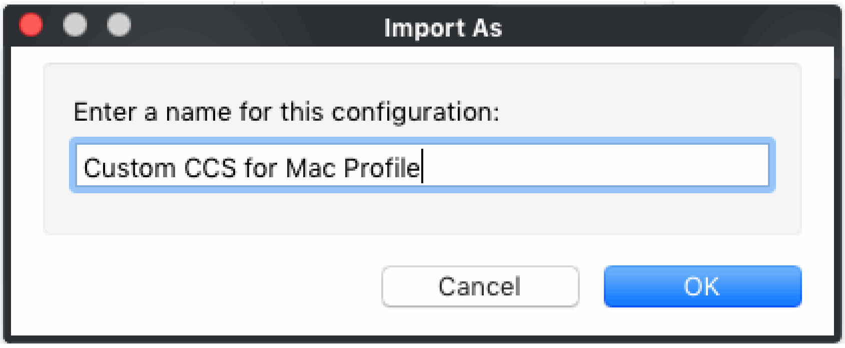
- CCS allows you to import profiles in .cfgx format.
- Any profile you import will not become active until you click the 'Activate' button

To import a configuration file:

- Open CCS > select 'More'
- Select 'Configuration' > 'Import'
- Browse to the location of the saved profile and click 'Open'.



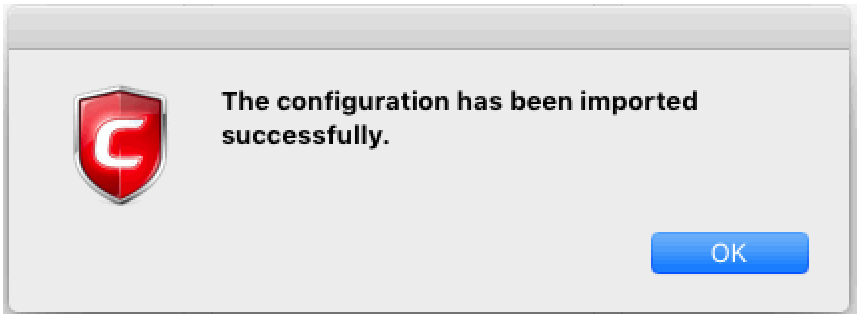
- In the 'Import As' dialog that appears, assign a name for the profile you wish to import and click 'OK'.



Enter a name for this configuration:

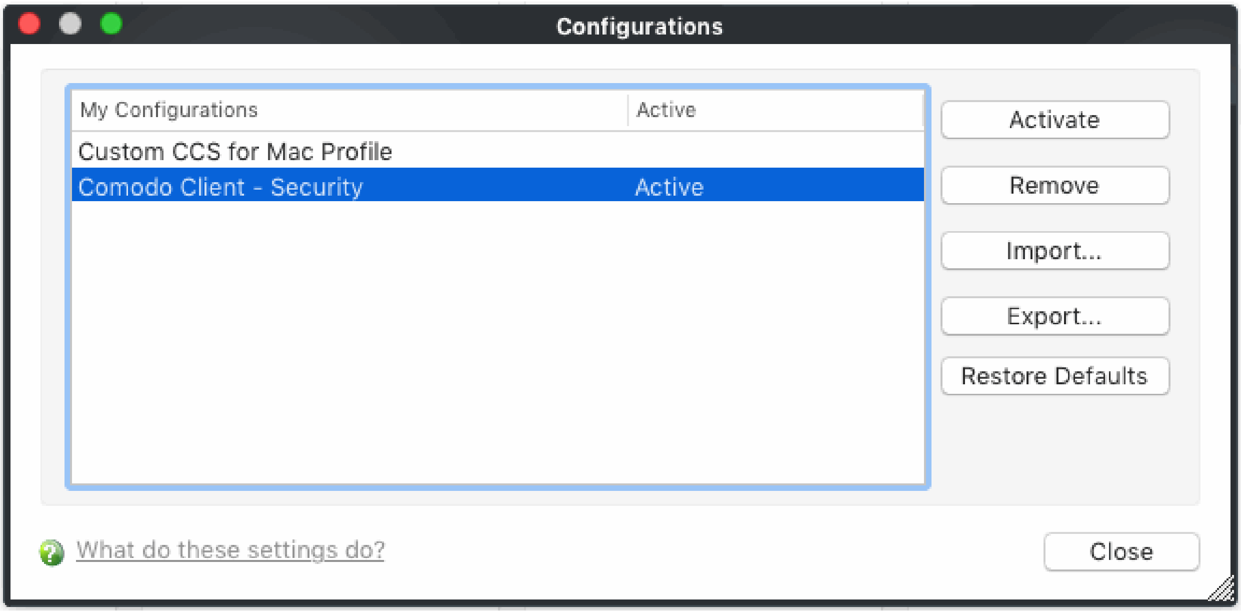
Custom CCS for Mac Profile

A confirmation dialog will appear indicating the successful import of the profile.



The configuration has been imported successfully.

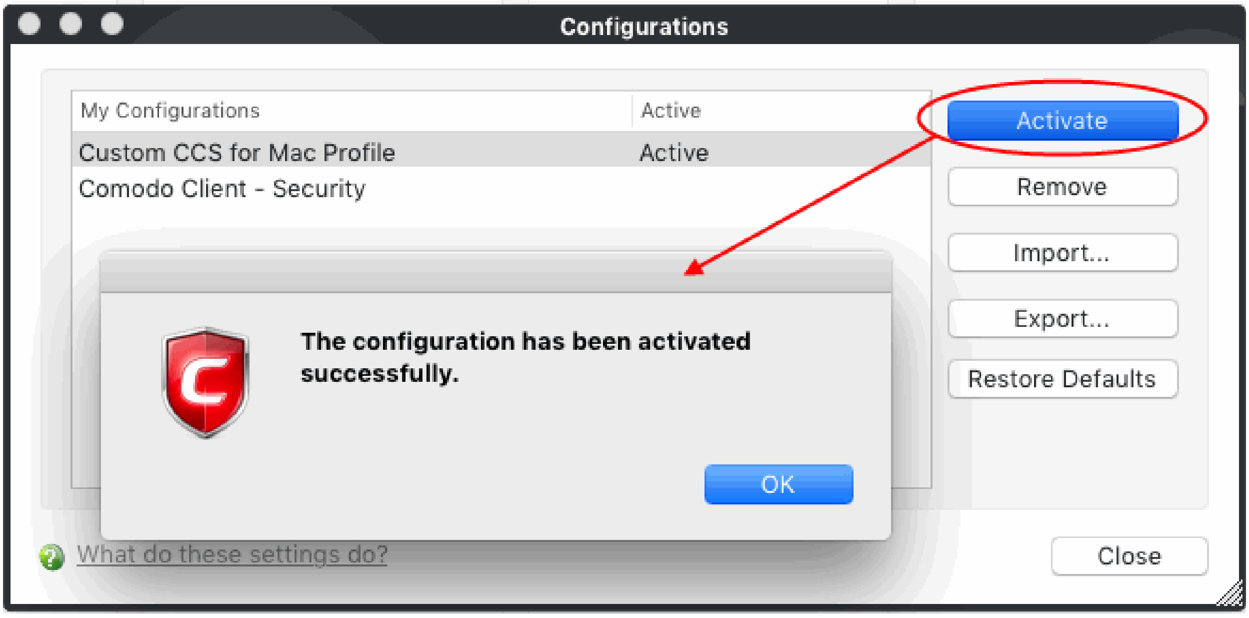
Click the 'Activate' button if you want to implement the profile in this installation of CCS.



Select and Implement a different configuration profile

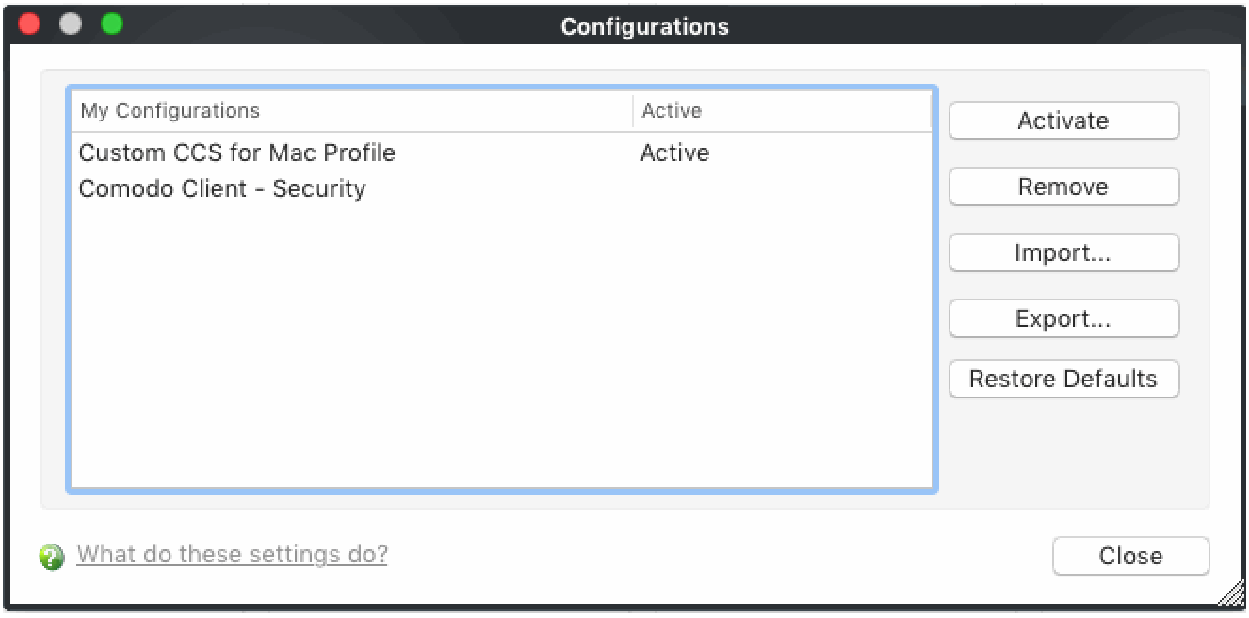
You can change the active configuration profile at any time from the 'Configurations' panel.

- Open CCS > 'More' > 'Manage My Configurations'
- Click on the profile you want to select and activate
- Click the 'Activate' button.
- Click 'OK' at the confirmation dialog:



The configuration has been activated successfully.

The profile will be marked as 'Active' in the profile list:

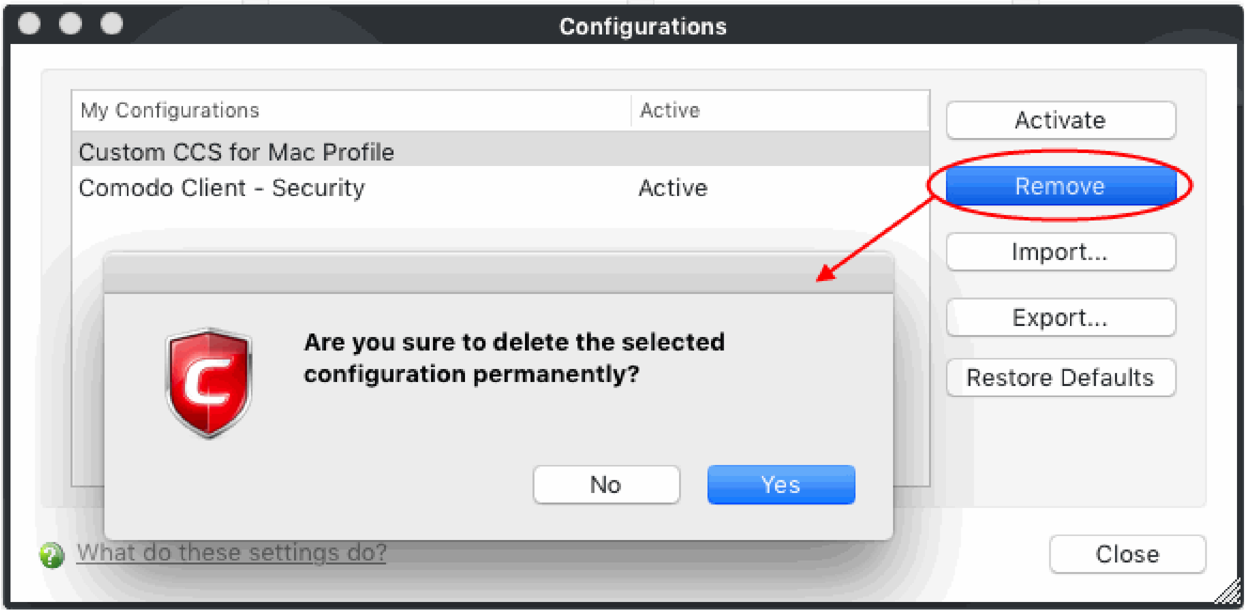


Delete an inactive configuration profile

- You can remove unwanted configuration profiles from the list of stored configuration profiles.
- You cannot delete the 'Active' profile. You can only delete inactive profiles.

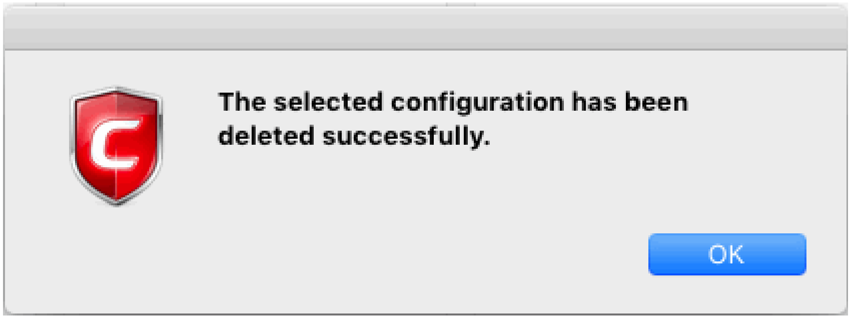
To remove an unwanted profile

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



Are you sure to delete the selected configuration permanently?

- The profile will be removed from your computer:

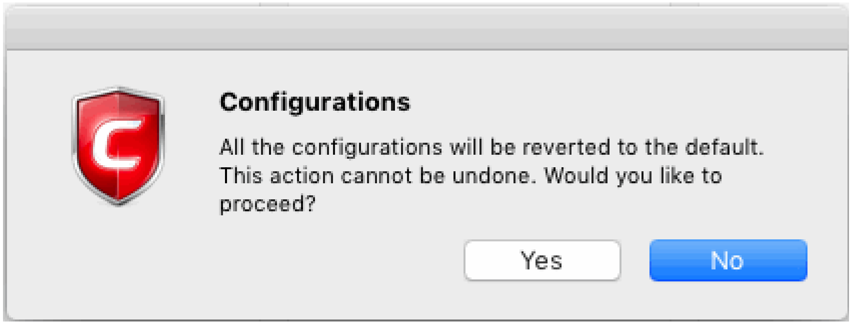


The selected configuration has been deleted successfully.

Reset to a default profile

- Select the profile and click 'Restore to Defaults' button.

A confirmation dialog will appear:



Configurations

All the configurations will be reverted to the default. This action cannot be undone. Would you like to proceed?

- Click 'Yes'.

4.3. Diagnostics

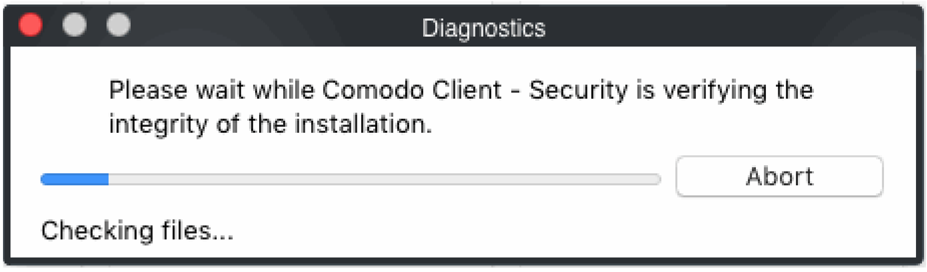
The diagnostics scanner checks your system to make sure that the application is installed correctly.

It checks:

- File System - Check that all of Comodo's system files are present and have been correctly installed.
- Registry - Check that all of Comodo's registry keys are present and in the correctly installed.
- Incompatible software - Checks for software that is known to have compatibility issues with CCS.

To open the diagnostics tool

- Open Comodo Client Security
- Click the 'More' tab > Click 'Diagnostics' in the tasks interface.

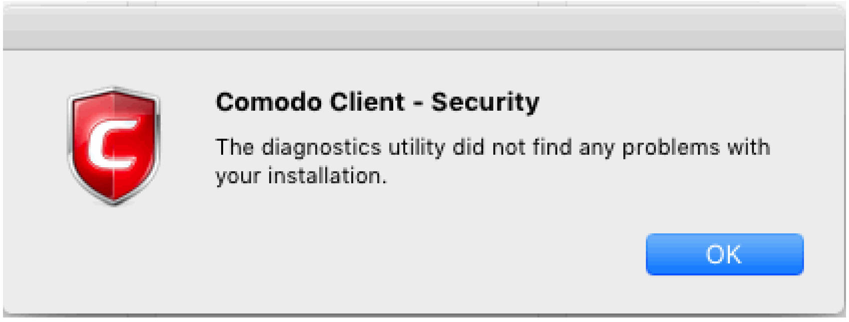


Diagnostics

Please wait while Comodo Client - Security is verifying the integrity of the installation.

Checking files...

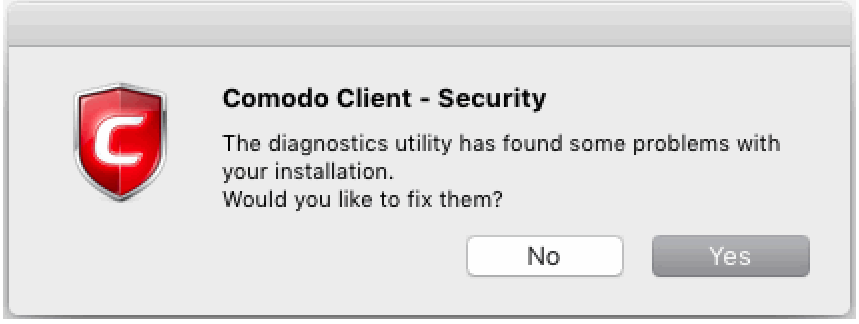
- If your installation does not have any errors, you will see the following dialog:



Comodo Client - Security

The diagnostics utility did not find any problems with your installation.

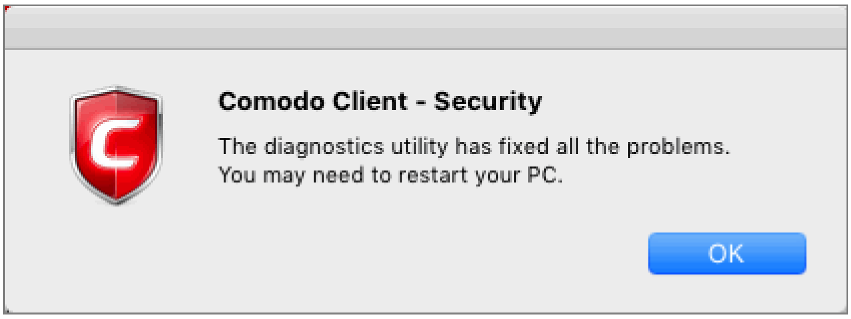
- If the utility finds errors you will be prompted to fix them:



Comodo Client - Security

The diagnostics utility has found some problems with your installation.
Would you like to fix them?

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

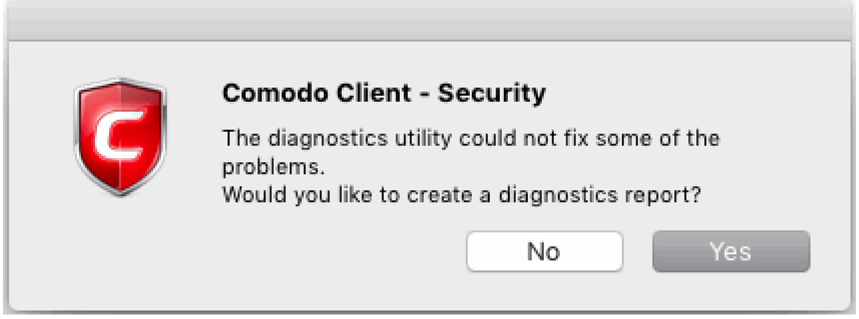


Comodo Client - Security

The diagnostics utility has fixed all the problems.
You may need to restart your PC.

  - Restart your computer for the changes to take effect.

- If the utility could not fix the problems, it will prompt you to create a diagnostics report:



Comodo Client - Security

The diagnostics utility could not fix some of the problems.
Would you like to create a diagnostics report?

4.4. Browse Support Forums

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

Visit the forum

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

Online Knowledge Base

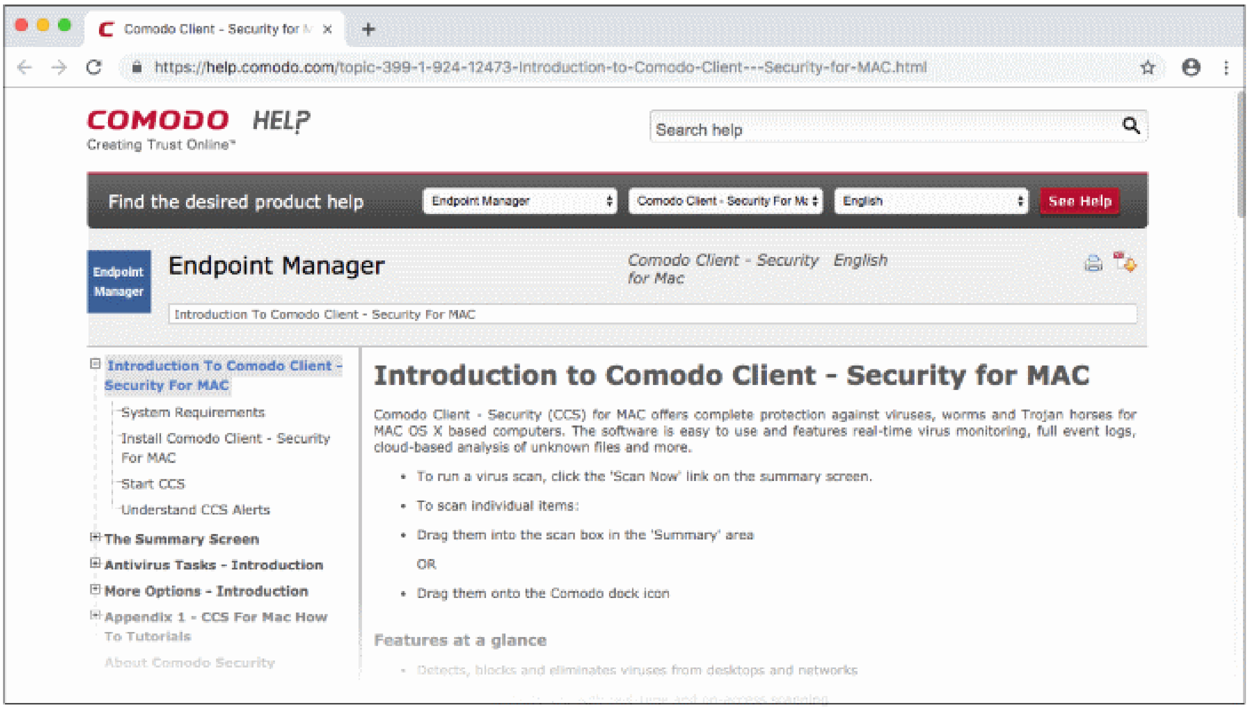
The knowledge base contains a range of articles and FAQs about Comodo products. It also features a support ticketing system. Visit the knowledgebase at **http://support.comodo.com**. Registration is free.

4.5. Help

The 'Help' link lets you view the CCS online help guide at **http://help.comodo.com/**. Each area has its own dedicated page and contains detailed descriptions about the functionality of our applications.

Open the online guide

- Open Comodo Client Security
- Click the 'More' tab
- Click 'Help'


Comodo Client - Security for M
https://help.comodo.com/topic-399-1-924-12473-Introduction-to-Comodo-Client---Security-for-MAC.html
COMODO HELP
Creating Trust Online
Search help
Find the desired product help
Endpoint Manager
Comodo Client - Security For Ma
English
See Help

Endpoint Manager

Comodo Client - Security for Mac *English*

Introduction To Comodo Client - Security For MAC

- Introduction To Comodo Client - Security For MAC
  - System Requirements
  - Install Comodo Client - Security For MAC
  - Start CCS
  - Understand CCS Alerts
- The Summary Screen
- Antivirus Tasks - Introduction
- More Options - Introduction
- Appendix 1 - CCS For Mac How To Tutorials
- About Comodo Security

Introduction to Comodo Client - Security for MAC

Comodo Client - Security (CCS) for MAC offers complete protection against viruses, worms and Trojan horses for MAC OS X based computers. The software is easy to use and features real-time virus monitoring, full event logs, cloud-based analysis of unknown files and more.

- To run a virus scan, click the 'Scan Now' link on the summary screen.
- To scan individual items:
- Drag them into the scan box in the 'Summary' area

  OR
- Drag them onto the Comodo dock icon

Features at a glance

- Detects, blocks and eliminates viruses from desktops and networks

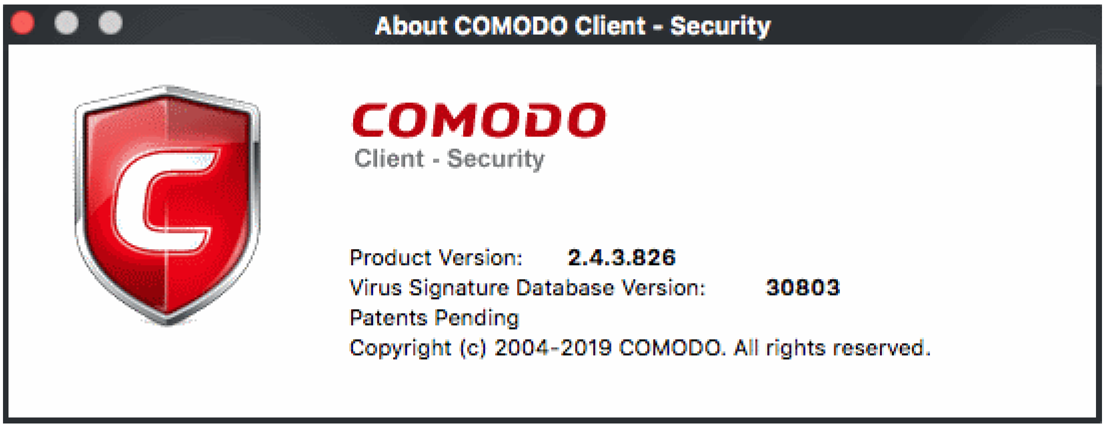
You can also download the .pdf version of the guide from here.

4.6. About

The 'About' dialog shows copyright information and the software version number.

To view the 'About' information

- Open Comodo Client Security
- Click the 'More' tab
- Click the 'About' option



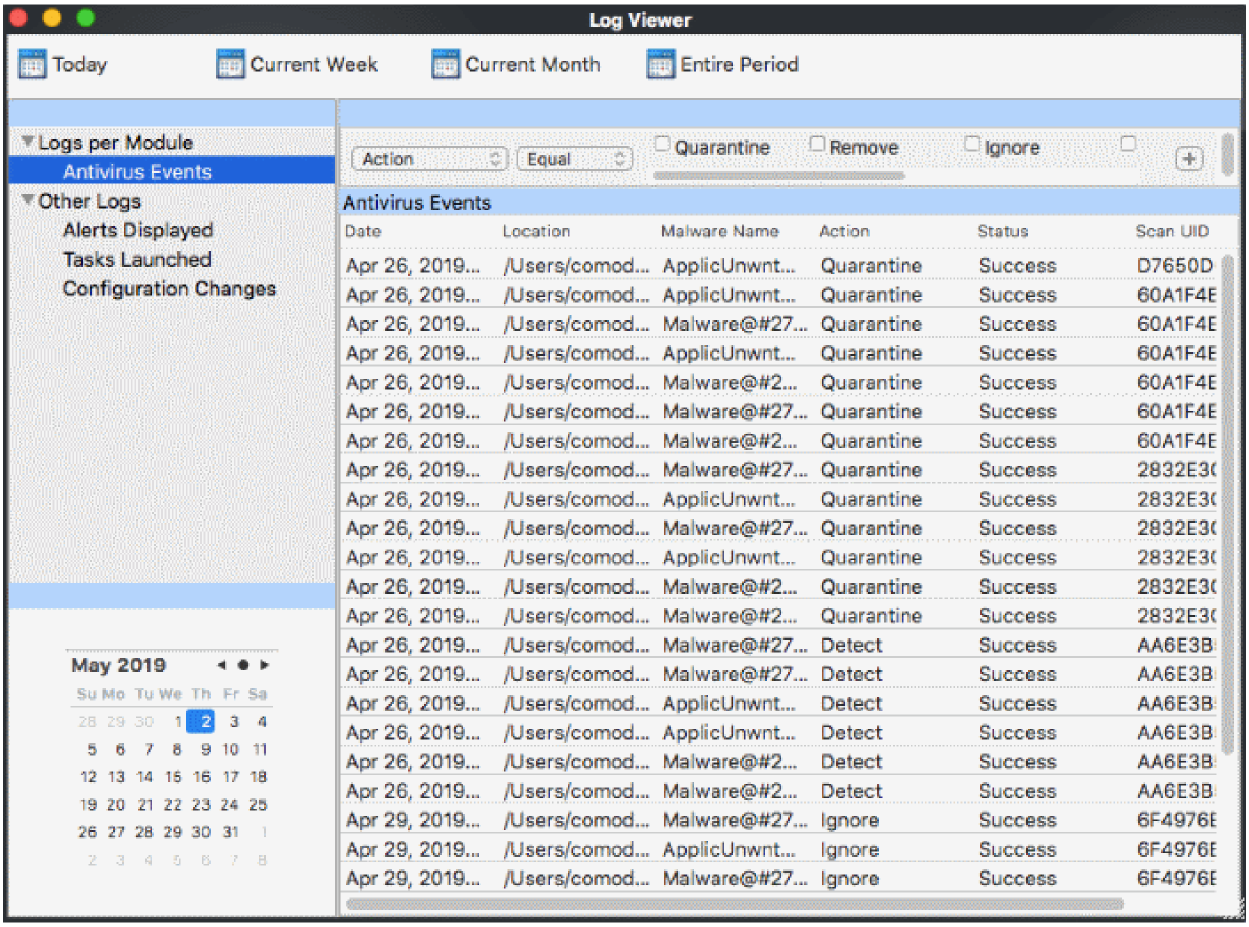
Product Version: **2.4.3.826**
Virus Signature Database Version: **30803**
Patents Pending
Copyright (c) 2004-2019 COMODO. All rights reserved.

4.7. View Logs

- CCS for MAC records all antivirus events in extensive but easy-to-understand logs.

To view logs

- Open Comodo Client Security
- Click the 'More' tab
- Click 'View Logs'



Antivirus Events

Date	Location	Malware Name	Action	Status	Scan UID
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976E
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976E
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976E

- Choose the type of log you want to see from the list on the left:
  - **Antivirus Events -** Shows all events generated by the antivirus module
  - The 'Other Logs' options contains logged events of the following:
    - **Alerts Displayed**: The list of various alerts that were displayed to the user, the response given by the user to those alert, and other related details.
    - **Tasks Launched**: 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**: Log of all configuration changes made by the user in the CCS for MAC application.
- The events themselves are shown in the main panel on the right.
- The links along the top of the interface let you filter the logs by date.
  - **Today -** Shows events logged since 12 AM on today's date.
  - **Current Week -** All logged events during the current week. The current week is calculated from the Sunday to Saturday.
  - **Current Month -** All logged events during the month.
  - **Entire Period -** Every event logged since CCS was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- You can also use the 'Advanced Filter' bar to filter by various other criteria. For example, you can choose to show all events where an item was quarantined.

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

'Logs per Module':

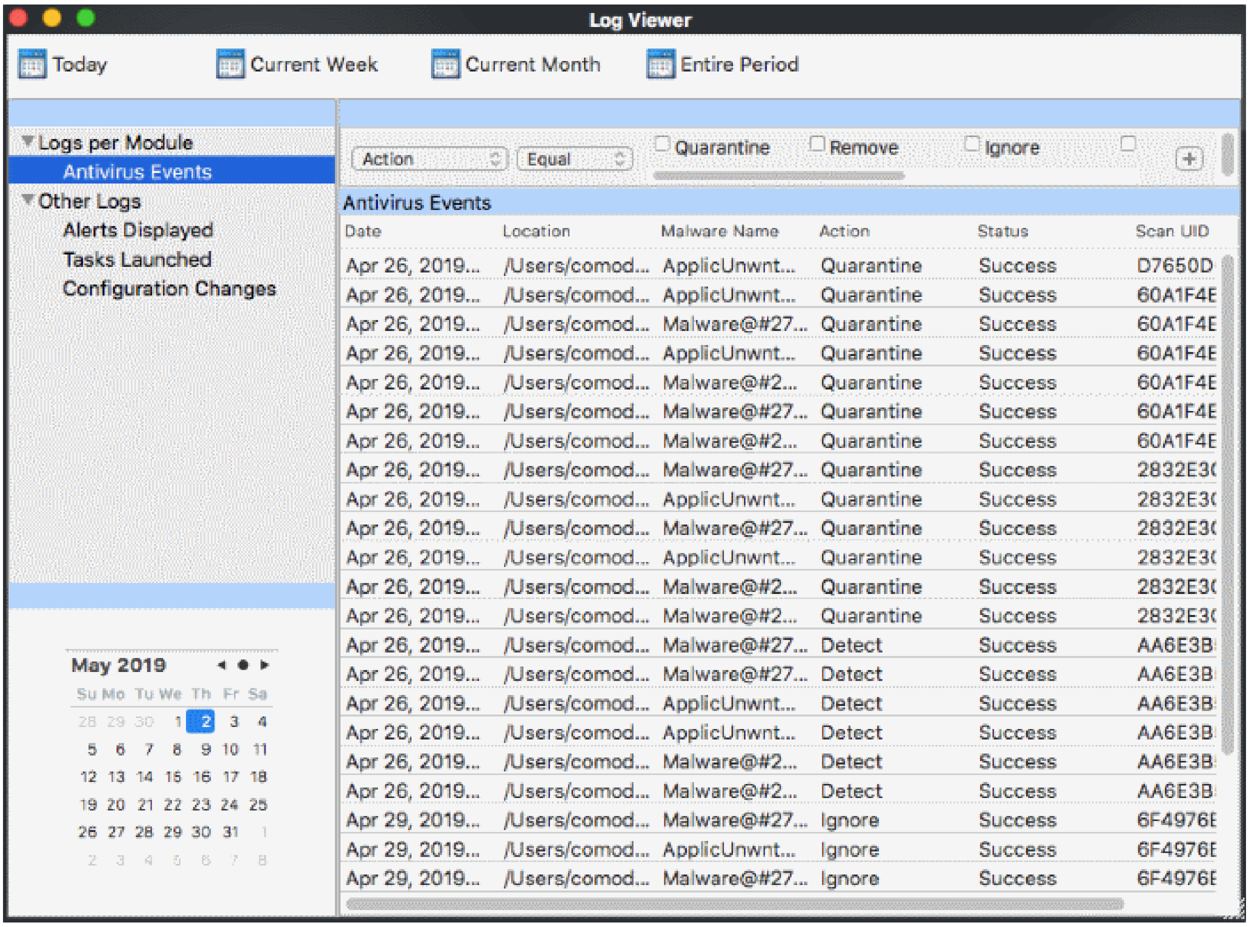
- **Antivirus Events**

'Other Logs':

- **Alerts Displayed Logs**
- **Tasks Launched Logs**
- **Configuration Changes Logs**

4.7.1. Antivirus Logs

Antivirus logs contain statistics on all discovered threats. This includes the time of the event, the malware name, and the action that taken on the threat.

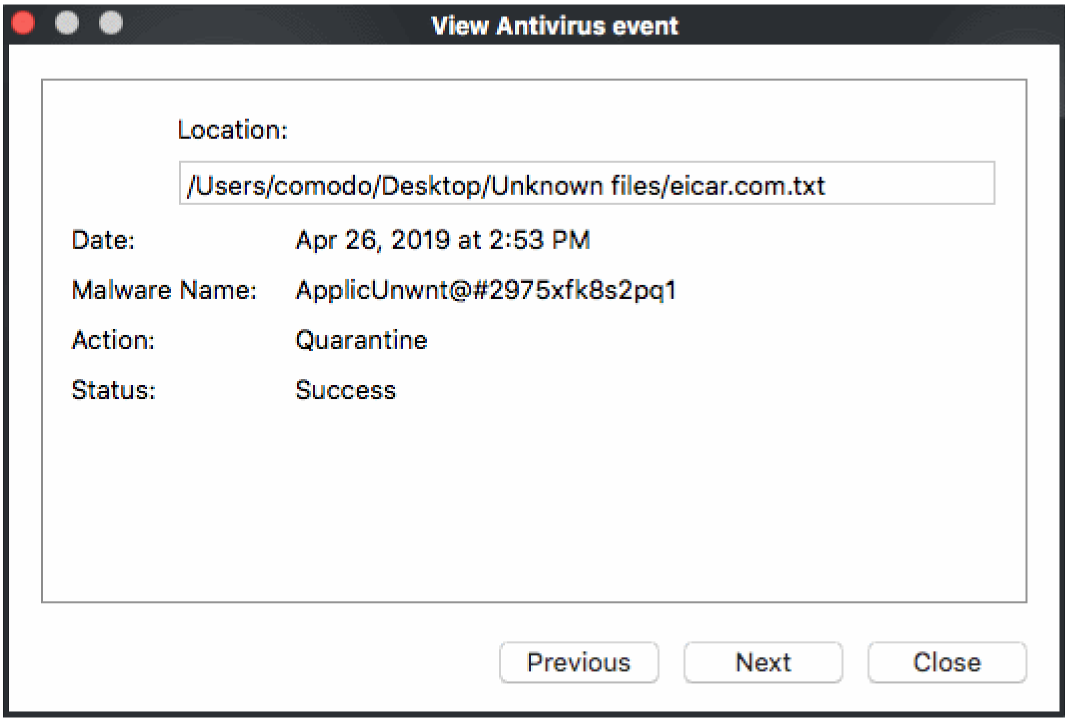


Antivirus Events

Date	Location	Malware Name	Action	Status	Scan UID
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4E
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3(
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976E
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976E
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976E

1. **Date -** The time of the event.
2. **Location -** The path where the threat was found
3. **Malware Name -** Malware label
4. **Action -** Action taken on the malware. This can be 'Quarantine', 'Detect' or Ignore'.
5. **Status -** States whether the attempted action succeeded or failed.
6. **Scan UID -** The unique identification code of the scan profile that caught the malware. Each profile has its own UID. All zeroes = code for a real-time scan.

Double-click on an entry to view a summary of the log:



View Antivirus event

Location:

/Users/comodo/Desktop/Unknown files/eicar.com.txt

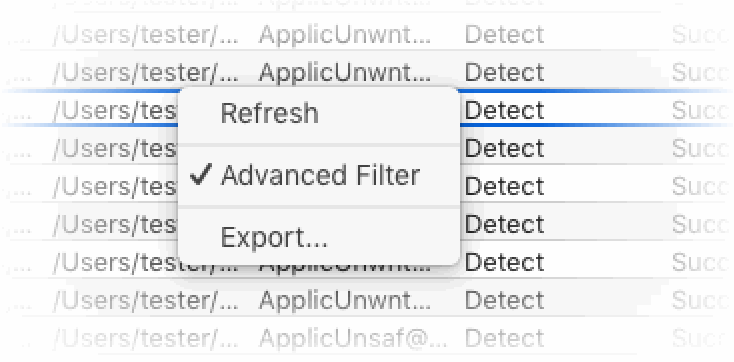
Date: Apr 26, 2019 at 2:53 PM

Malware Name: ApplicUnwnt@#2975xfk8s2pq1

Action: Quarantine

Status: Success

You can right-click on an item to view further options:



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

4.7.1.1. Filter Antivirus Logs

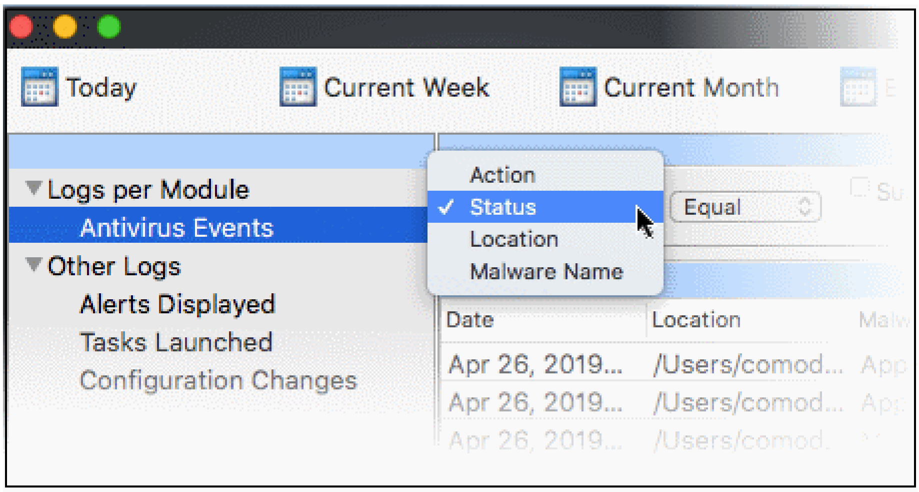
You can create custom views of all logged events according to the following criteria:

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

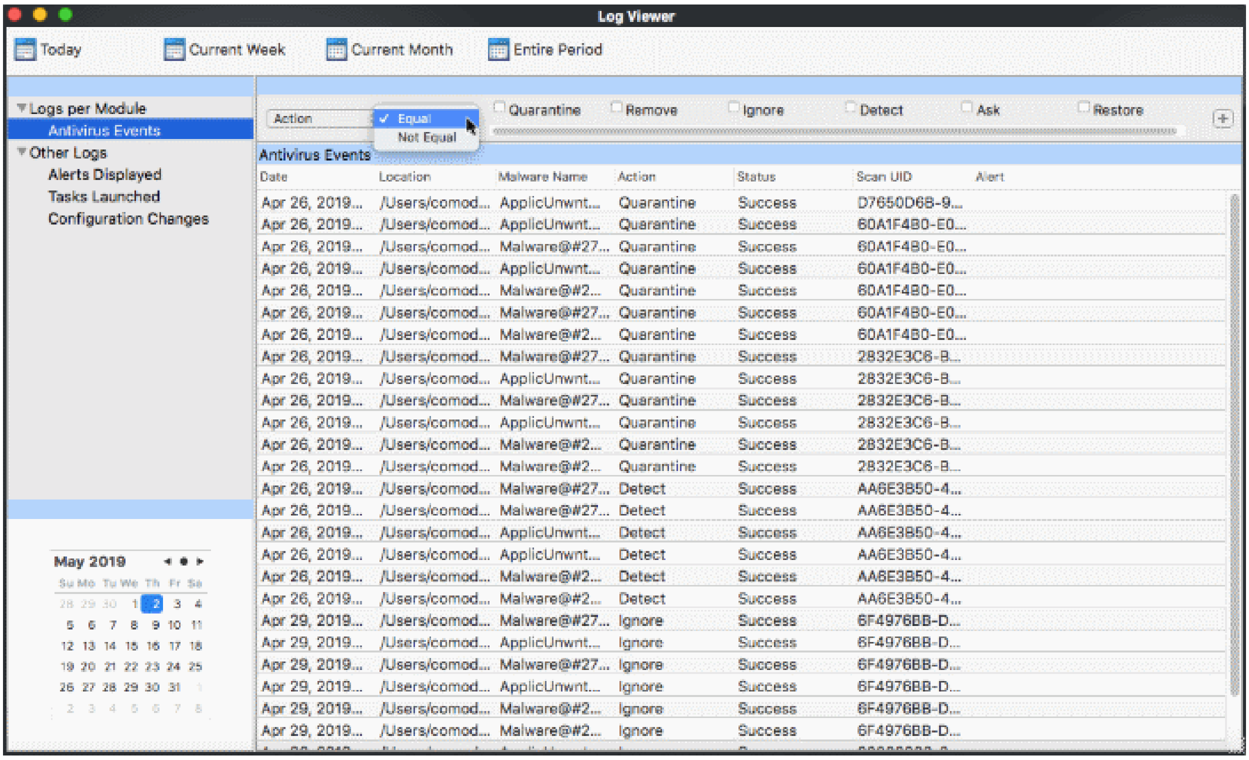
Configure Event Filters

- Open CCS.
- Click 'More' > 'View Logs' > 'Antivirus Events'
- Right-click inside the log viewer module and choose 'Advanced Filter'

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



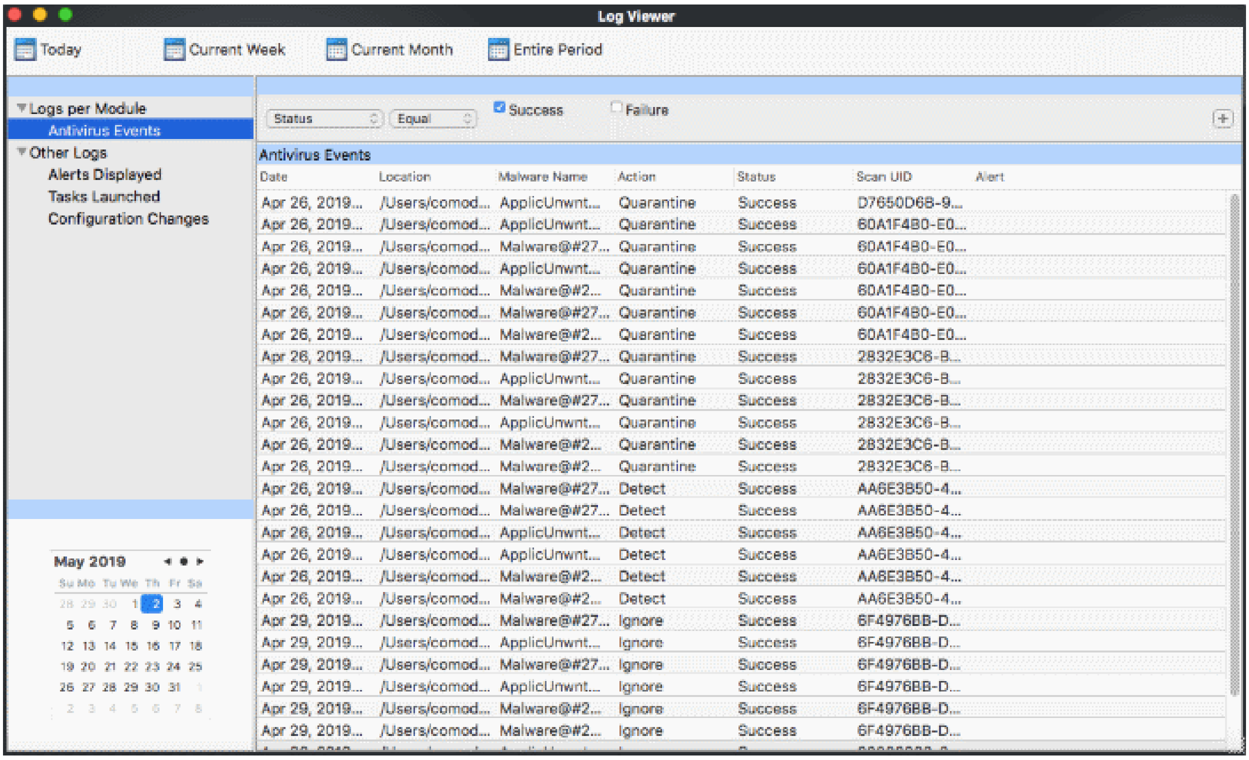
Action: Filter logs by the action taken by CCS on the detected threat. You can then filter by a specific type of action. For example, to only show events where the threat was quarantined.



Date	Location	Malware Name	Action	Status	Scan UID	Alert
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D6B-9...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	

- Select 'Equal' or 'Not Equal' from the drop-down.
  - **Equal -** Show only events which feature the action you select. You can select multiple actions.
  - **Not Equal -** Inverts your choice. For example, select 'Not Equal' + 'Ignore' to view every event except those that were ignored.
- Select the specific actions you want to view from:
  - **Quarantine**: Events where the threat was placed in quarantine
  - **Remove**: Events where the user chose to delete a threat
  - **Ignore**: Events where the user chose to ignore an item
  - **Detect:** Events where the malware was first detected
  - **Ask**: Events where the user was asked to provide a response to a discovered threat. The response from the user might be 'Quarantine', 'Remove', 'Ignore' or 'Restore'. Users are asked for their response at a threat alerts, and at the scan results screen.
  - **Restore**: Events where the user removed the threat from quarantine and restored it to its original location.

Status: Filter logs by whether or not the action taken on the threat was successful. You choose to view only successful actions, or only failed actions.

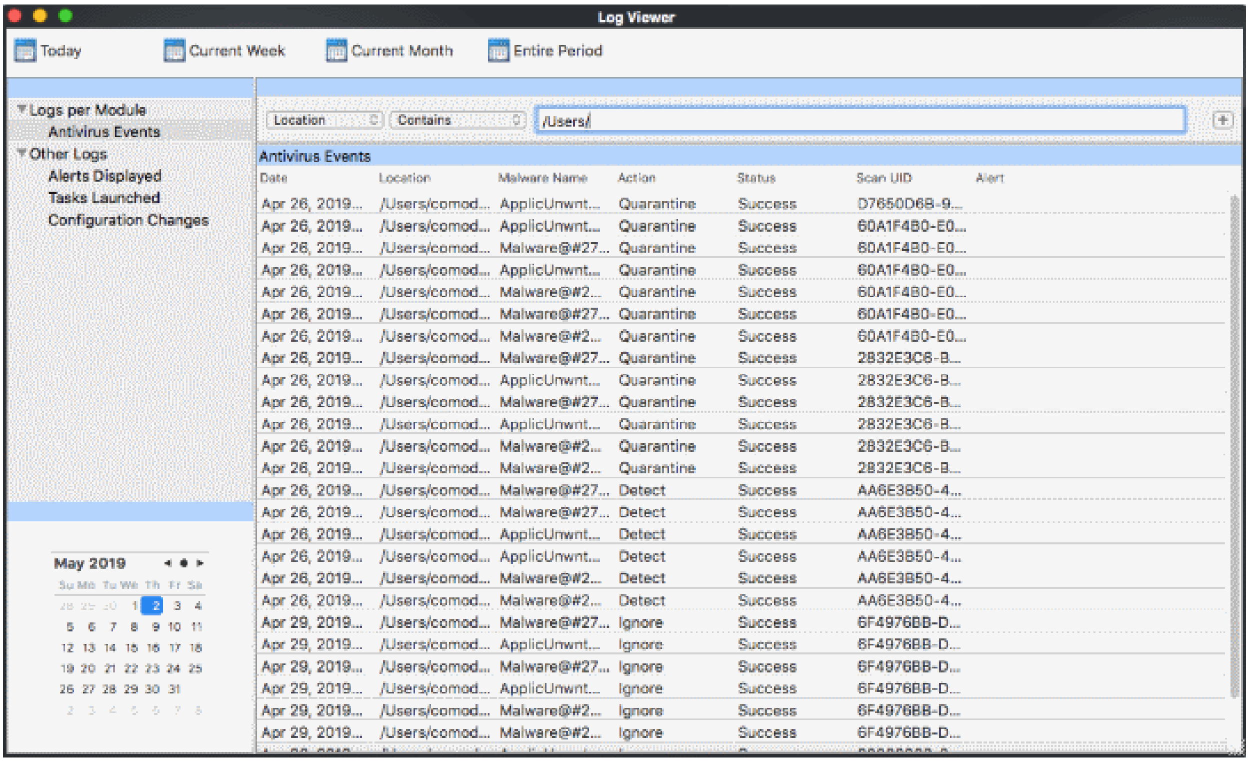


Status | Equal | ☑ Success | □ Failure

Antivirus Events

Date	Location	Malware Name	Action	Status	Scan UID	Alert
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D6B-9...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	

- Select 'Equal' or 'Not Equal' from the drop-down.
  - **Equal -** Show only events which feature the result you select.
  - **Not Equal -** Inverts your choice. For example, select 'Not Equal' + 'Success' to view every event except those that were successful.
- Select the specific results you want to view:
  - **Success:** View events where the task in the 'Action' column was completed.
  - **Failure:** View events where the task in the 'Action' column was not completed.
- **Location**: View logs that concern files at a specific path. You need to enter the path in the field provided:

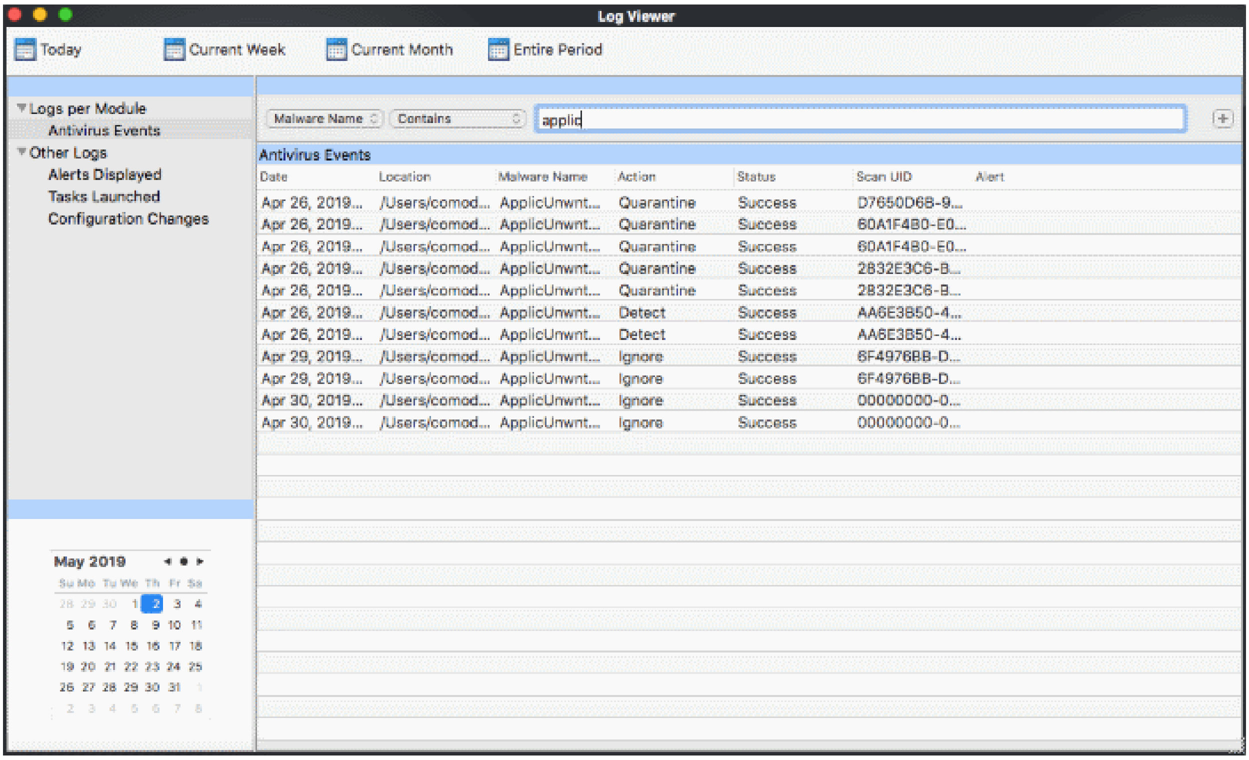


Location | Contains | /Users/

Antivirus Events

Date	Location	Malware Name	Action	Status	Scan UID	Alert
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D6B-9...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Quarantine	Success	2832E3C6-B...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#27...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	Malware@#2...	Detect	Success	AA6E3B50-4...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#27...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	Malware@#2...	Ignore	Success	6F4976BB-D...	

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



Malware Name | Contains | applic

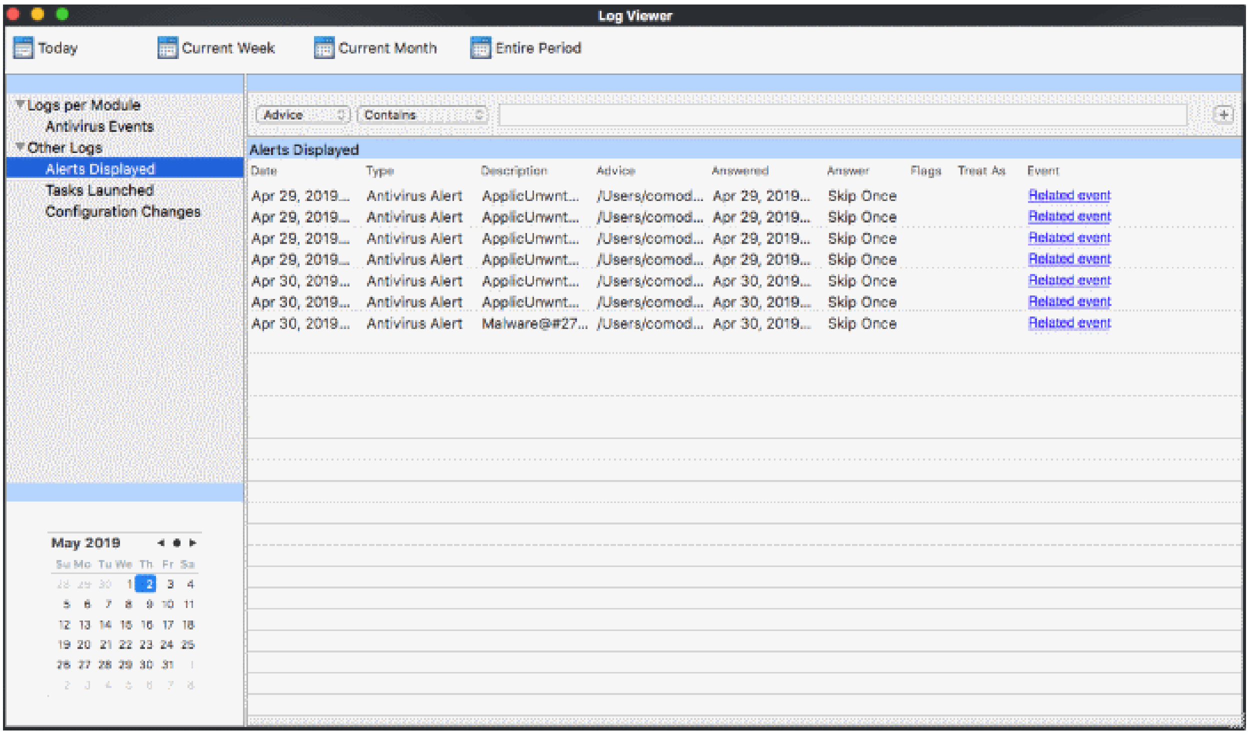
Antivirus Events

Date	Location	Malware Name	Action	Status	Scan UID	Alert
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	D7650D6B-9...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	60A1F4B0-E0...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2B32E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Quarantine	Success	2B32E3C6-B...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 26, 2019...	/Users/comod...	ApplicUnwnt...	Detect	Success	AA6E3B50-4...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 29, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	6F4976BB-D...	
Apr 30, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	00000000-0...	
Apr 30, 2019...	/Users/comod...	ApplicUnwnt...	Ignore	Success	00000000-0...	

- Select 'Contains' or 'Does Not Contain' from the second drop-down:
  - **Contains -** Show only those events which concern the malware named in the text field. You can add multiple malware names.
  - **Does Not Contain -** Show only those events which did not involve the malware named in the text field.

4.7.2. 'Alerts Displayed' Logs

Alert logs are a history of security alerts shown to users when a threat was detected. The action taken depends on how the user responded to the alert.



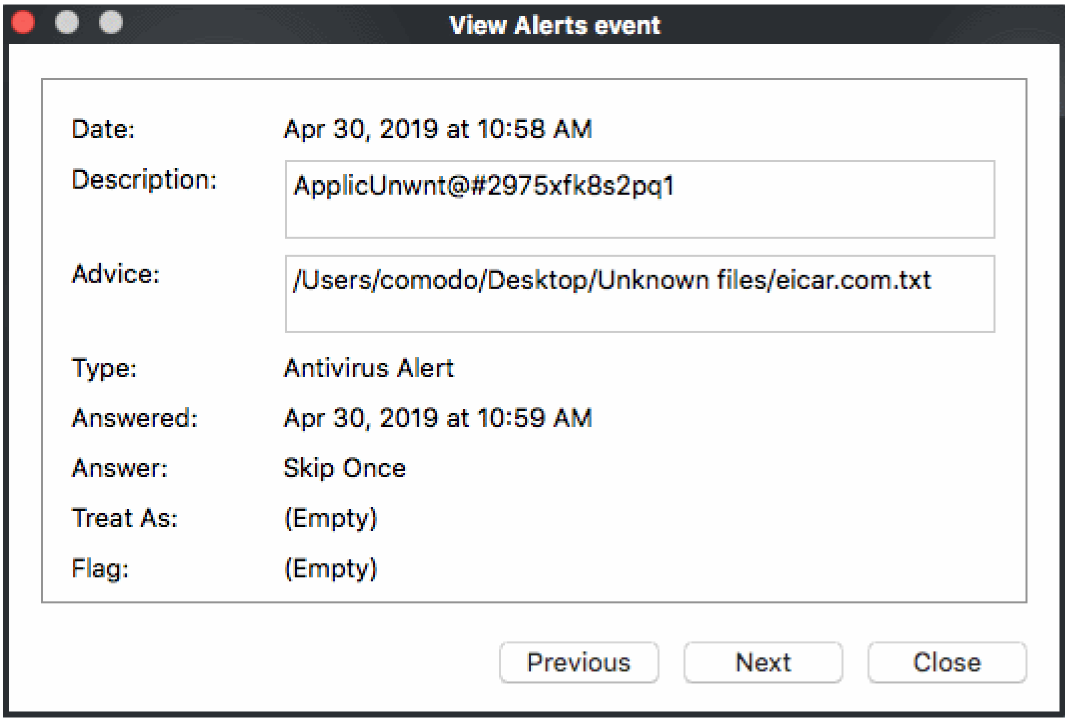
Advice | Contains

Alerts Displayed

Date	Type	Description	Advice	Answered	Answer	Flags	Treat As	Event
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once			Related event
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once			Related event
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once			Related event
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once			Related event
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once			Related event
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once			Related event
Apr 30, 2019...	Antivirus Alert	Malware@#27...	/Users/comod...	Apr 30, 2019...	Skip Once			Related event

1. **Date** - The time the alert was shown.
2. **Type -** The alert category. Categories include antivirus alerts and execution alerts. Note **-** execution alert are coming in later versions of CCS.
3. **Description** - Malware name
4. **Advice** - Location where the malware was detected
5. **Answered -** Whether the user responded to the alert. If yes, you will see the date and time of the response.
6. **Answer -** The response given by the user.
7. **Flags -** Not used.
8. **Treat As -** Not used.
9. **Event** - Click 'Related Event' to view a summary of the incident.

To view full details of a particular alert event, double-click the entry:



View Alerts event

Date: Apr 30, 2019 at 10:58 AM

Description: ApplicUnwnt@#2975xfk8s2pq1

Advice: /Users/comodo/Desktop/Unknown files/eicar.com.txt

Type: Antivirus Alert

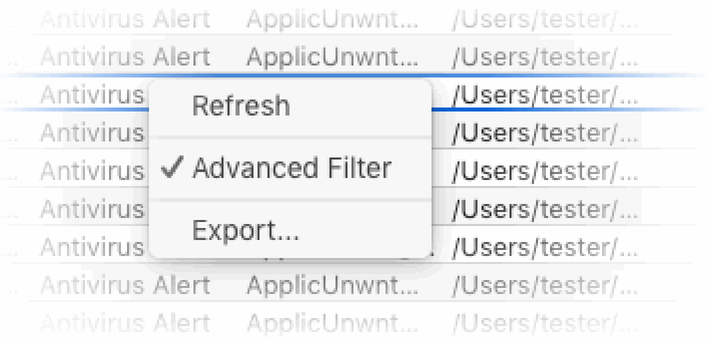
Answered: Apr 30, 2019 at 10:59 AM

Answer: Skip Once

Treat As: (Empty)

Flag: (Empty)

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



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

4.7.2.1. Filter 'Alerts Displayed' Logs

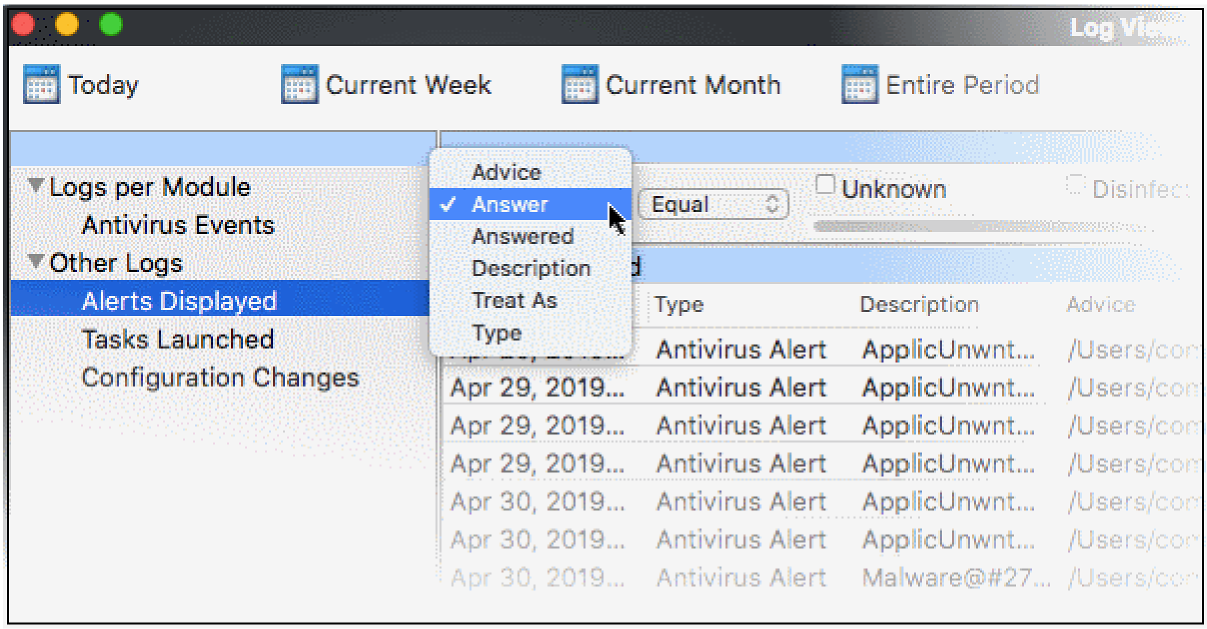
You can create custom views of all logged events according to the following criteria:

- **Advice:** Filter events by the path at which the malware was found
- **Answer:** Filter events according to the user's response. For example,'Skip once'.
- **Answered:** Filter events by specific dates
- **Description:** Filter events by malware name
- **Treat As:** Not used
- **Type:** Filter events by alert category. Possible categories are antivirus alerts and execution alerts. Execution alerts are coming in a future version of CCS.

Configure Event Filters

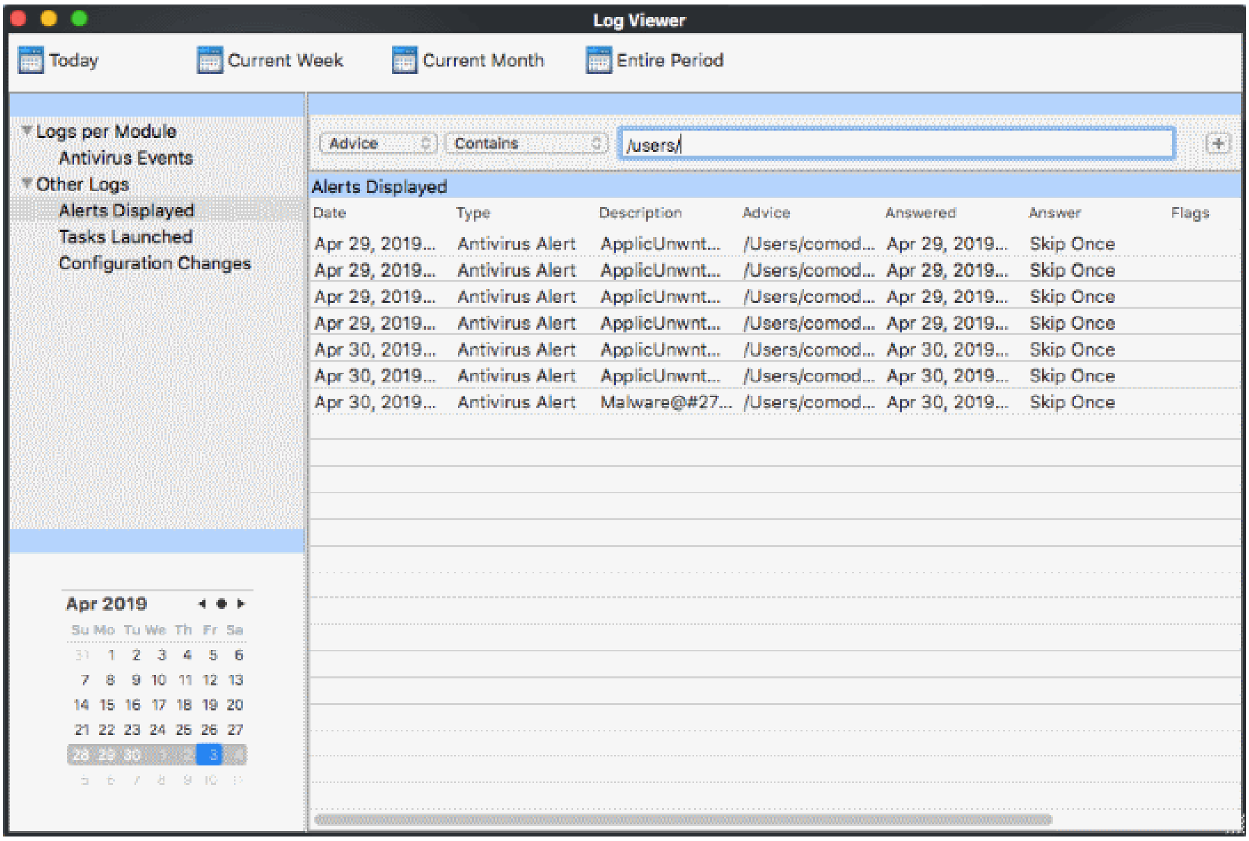
- Open CCS.
- Click 'More' > 'View Logs' > 'Other Logs' > 'Alerts Displayed'
- Right-click inside the log viewer module and choose 'Advanced Filter'

There are 6 types of filter. Each of these can be further refined by selecting or deselecting specific parameters.



	Type	Description	Advice
	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/co...
Apr 30, 2019...	Antivirus Alert	Malware@#27...	/Users/co...

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



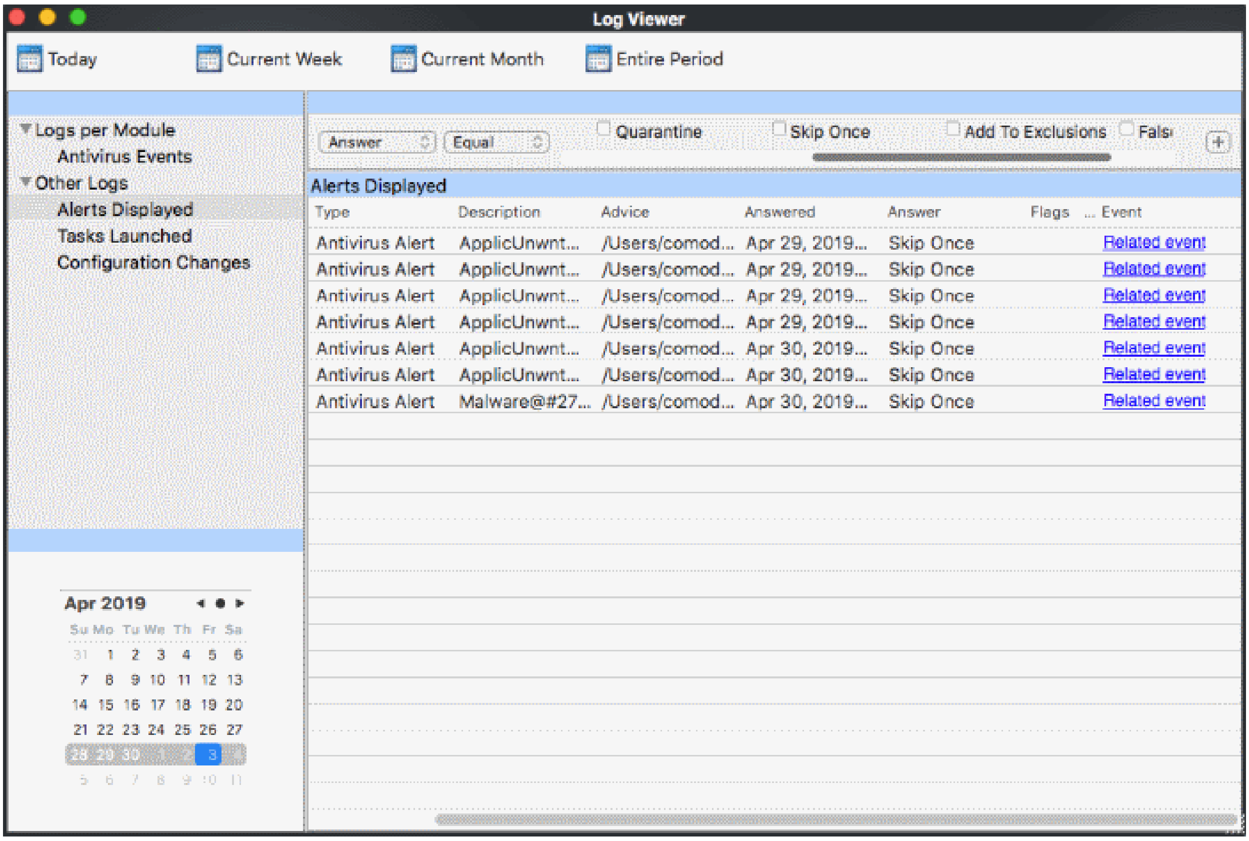
Advice | Contains | /users/

Alerts Displayed

Date	Type	Description	Advice	Answered	Answer	Flags
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once	
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once	
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once	
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once	
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once	
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once	
Apr 30, 2019...	Antivirus Alert	Malware@#27...	/Users/comod...	Apr 30, 2019...	Skip Once	

- Select 'Contains' or 'Does Not Contain' option from the drop-down.
  - **Contains -** Show only those events which concern items at the location you specify. You can add multiple locations.
  - **Does Not Contain -** Show events which did not concern files at the locations you specify.

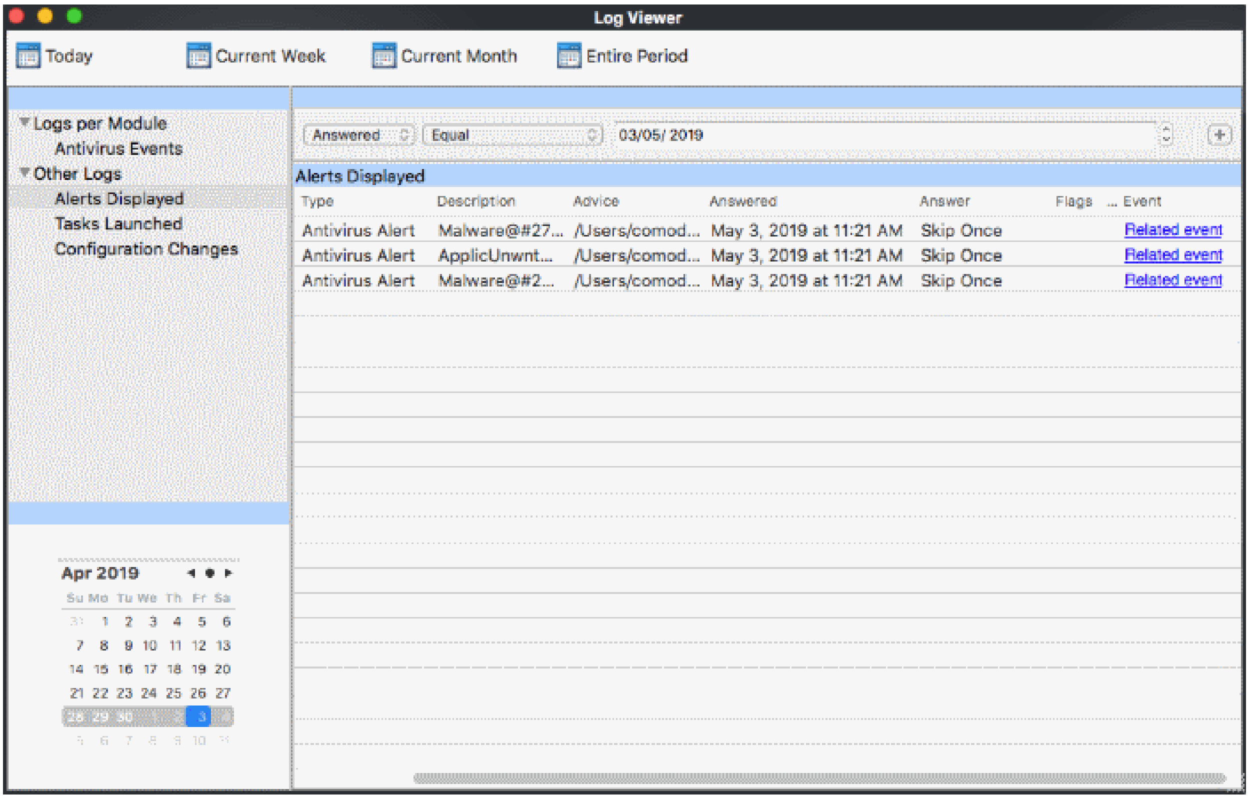
- **Answer**: Filter logs by the action taken by the user on the detected threat. You can then filter by a specific type of action. For example, to only show events where the threat was quarantined.



Alerts Displayed

Type	Description	Advice	Answered	Answer	Flags	... Event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once		Related event
Antivirus Alert	Malware@#27...	/Users/comod...	Apr 30, 2019...	Skip Once		Related event

- Select 'Equal' or 'Not Equal' from the drop-down.
  - **Equal -** Show only events which feature the action you select. You can select multiple actions.
  - **Not Equal -** Inverts your choice. For example, select 'Not Equal' + 'Quarantine' to view every event except those that were quarantined.
- Select the specific actions you want to view from:
  - **Unknown -** Events where the user did not respond to alerts.
  - **Disinfect -** Events where the user chose to run a disinfection routine on the malware
  - **Delete -** Events where the user chose to clean (delete) the file
  - **Quarantine -** Events where the user chose to place the malware files in quarantine
  - **Skip Once** - Events where the user chose to ignore the alert once
  - **Add To Exclusions -** Events where the user chose to include the files to exclusions list
  - **False Positive -** Not used.
- **Answered:** Filter logs by date of the response. You need to enter the date in the field provided. You can then refine your filter with other parameters:

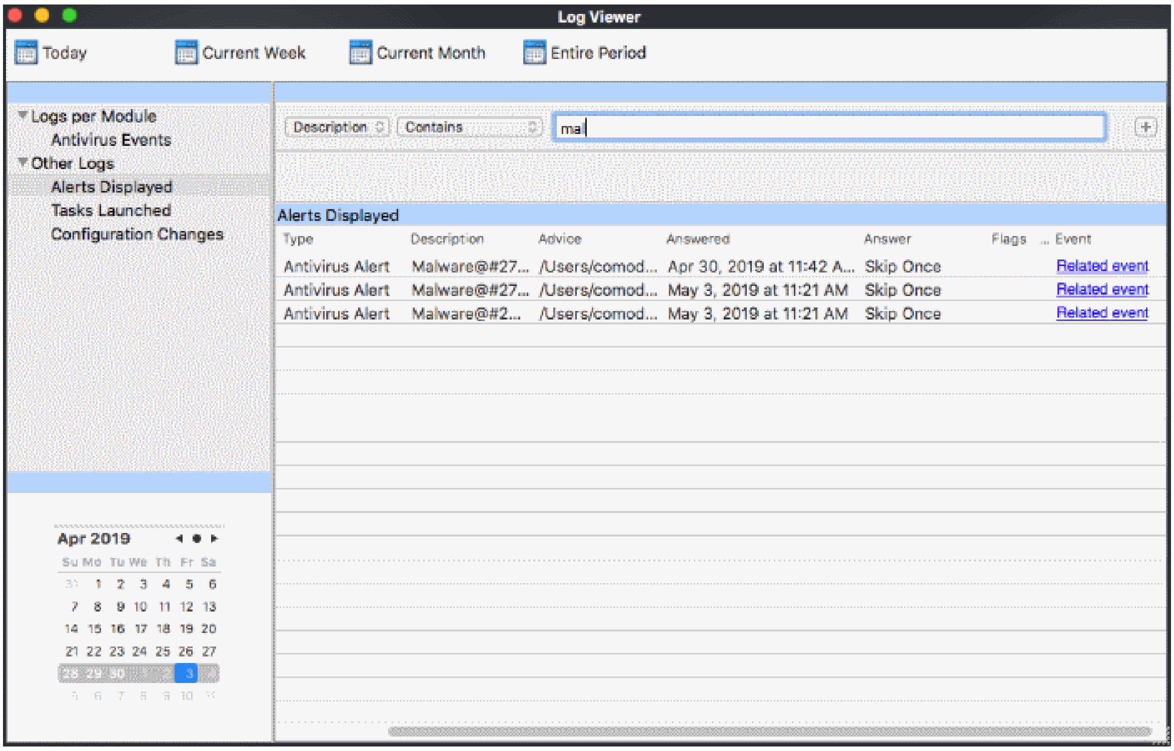


Answered | Equal | 03/05/ 2019

Alerts Displayed

Type	Description	Advice	Answered	Answer	Flags	... Event
Antivirus Alert	Malware@#27...	/Users/comod...	May 3, 2019 at 11:21 AM	Skip Once		Related event
Antivirus Alert	ApplicUnwnt...	/Users/comod...	May 3, 2019 at 11:21 AM	Skip Once		Related event
Antivirus Alert	Malware@#2...	/Users/comod...	May 3, 2019 at 11:21 AM	Skip Once		Related event

- Select any of the following options in the second drop-down:
  - **Equal** - Show only events that occurred on the specified date
  - **Greater than** - Show only events that occurred later than the specified date
  - **Greater than or Equal** - Show only events that occurred later than or on the specified date
  - **Less than** - Show only events that occurred before the specified date
  - **Less than or Equal** - Show only events that occurred before than or on the specified date
  - **Not Equal** - Show events that occurred on all dates except the specified date
- **Description:** Filter logs by the name of the malicious item. You need to enter the name of the malware in the field provided:

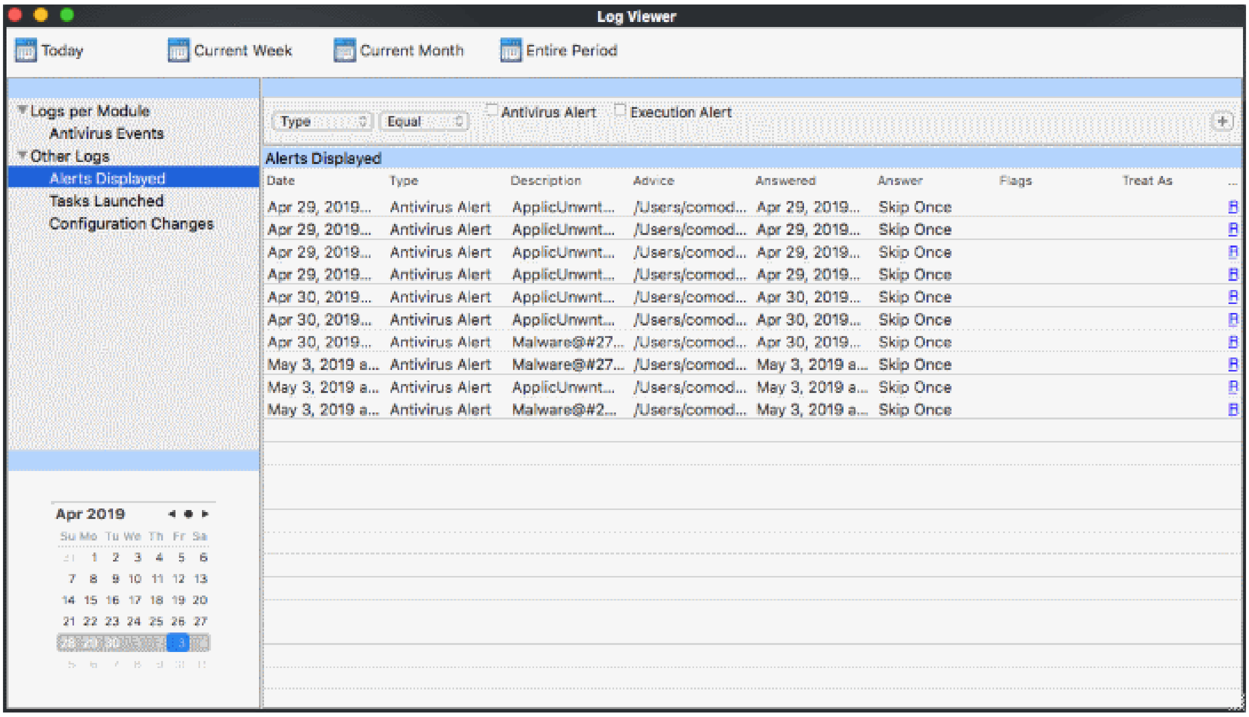


Description | Contains | mal

Alerts Displayed

Type	Description	Advice	Answered	Answer	Flags	Event
Antivirus Alert	Malware@#27...	/Users/comod...	Apr 30, 2019 at 11:42 A...	Skip Once		Related event
Antivirus Alert	Malware@#27...	/Users/comod...	May 3, 2019 at 11:21 AM	Skip Once		Related event
Antivirus Alert	Malware@#2...	/Users/comod...	May 3, 2019 at 11:21 AM	Skip Once		Related event

- Select 'Contains' or 'Does Not Contain' from the second drop-down:
  - **Contains -** Show only those events which concern the malware named in the text field. You can add multiple malware names.
  - **Does Not Contain -** Show only those events which did not involve the malware named in the text field.
- **Type**: Filter events by alert category. Possible categories are antivirus alerts and execution alerts. Execution alerts are coming in a future version of CCS.



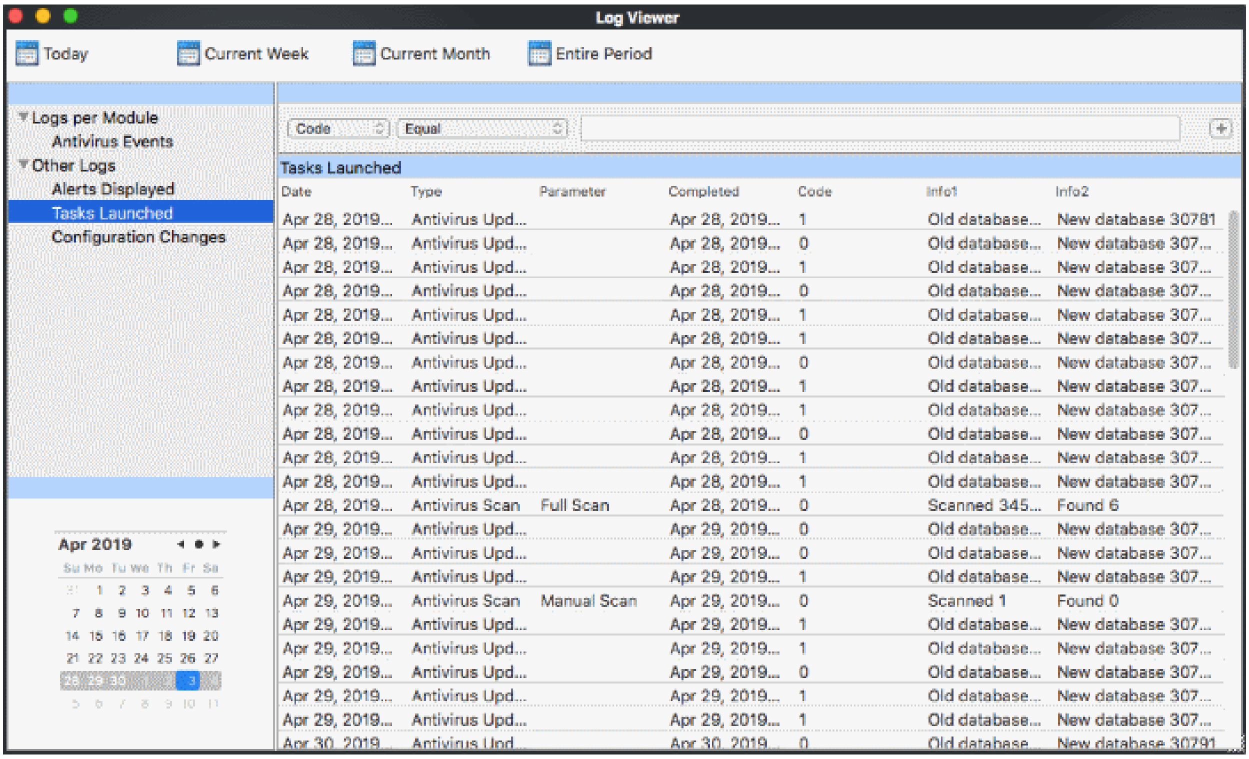
Alerts Displayed

Date	Type	Description	Advice	Answered	Answer	Flags	Treat As
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		
Apr 29, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 29, 2019...	Skip Once		
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once		
Apr 30, 2019...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	Apr 30, 2019...	Skip Once		
Apr 30, 2019...	Antivirus Alert	Malware@#27...	/Users/comod...	Apr 30, 2019...	Skip Once		
May 3, 2019 a...	Antivirus Alert	Malware@#27...	/Users/comod...	May 3, 2019 a...	Skip Once		
May 3, 2019 a...	Antivirus Alert	ApplicUnwnt...	/Users/comod...	May 3, 2019 a...	Skip Once		
May 3, 2019 a...	Antivirus Alert	Malware@#2...	/Users/comod...	May 3, 2019 a...	Skip Once		

- Select 'Equal' or 'Not Equal' from the second drop-down.
  - **Equal** - Show only events which feature the alert type you select.
  - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Execution Alert' to view all antivirus alert events.

4.7.3. Tasks Launched Logs

A record of all tasks launched by CCS and the user. Example tasks are virus database updates and virus scans. Each row shows the type of task and various other details.

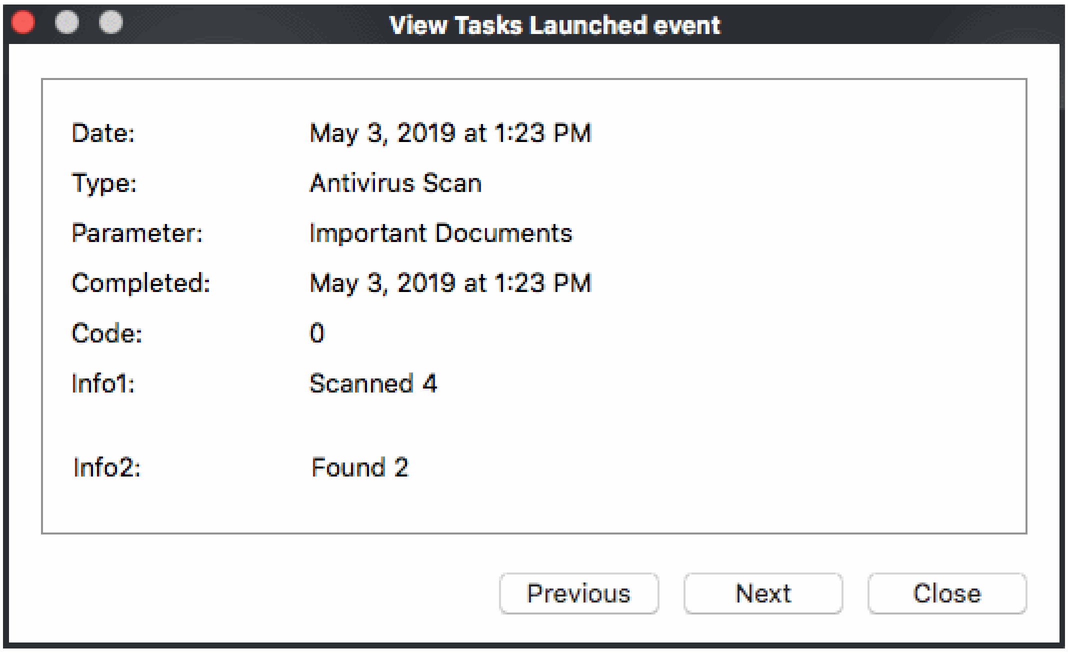


Tasks Launched

Date	Type	Parameter	Completed	Code	Info1	Info2
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 30781
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 307...
Apr 28, 2019...	Antivirus Scan	Full Scan	Apr 28, 2019...	0	Scanned 345...	Found 6
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 307...
Apr 29, 2019...	Antivirus Scan	Manual Scan	Apr 29, 2019...	0	Scanned 1	Found 0
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 307...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 307...
Apr 30, 2019...	Antivirus Upd...		Apr 30, 2019...	0	Old database...	New database 30791

1. **Date** - The time the task was launched.
2. **Type -** The category of task. For example, 'Antivirus Scan'.
3. **Parameter -** Name of the scan profile. For example, full scan, quick scan, custom scan.
4. **Completed -** Date and time the task finished.
5. **Code -** Internal CCS code for the task type.
6. **Info 1 & Info 2 -** Additional information of the task. For example, these columns will shown the number of files scanned and number of infected items if the task type = 'Antivirus Scan'.

To view full details of a particular tasks event, double-click the entry:



View Tasks Launched event

Date: May 3, 2019 at 1:23 PM

Type: Antivirus Scan

Parameter: Important Documents

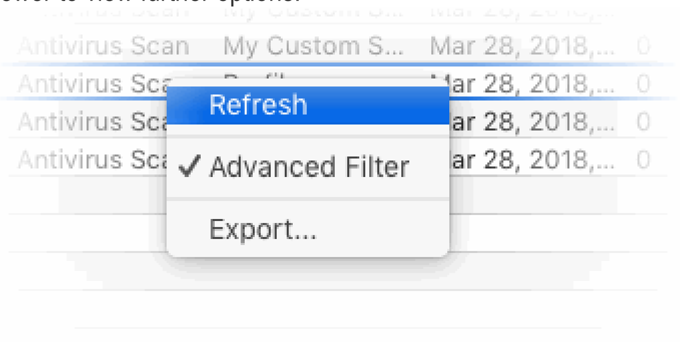
Completed: May 3, 2019 at 1:23 PM

Code: 0

Info1: Scanned 4

Info2: Found 2

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



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

4.7.3.1. Filter 'Tasks Launched' Logs

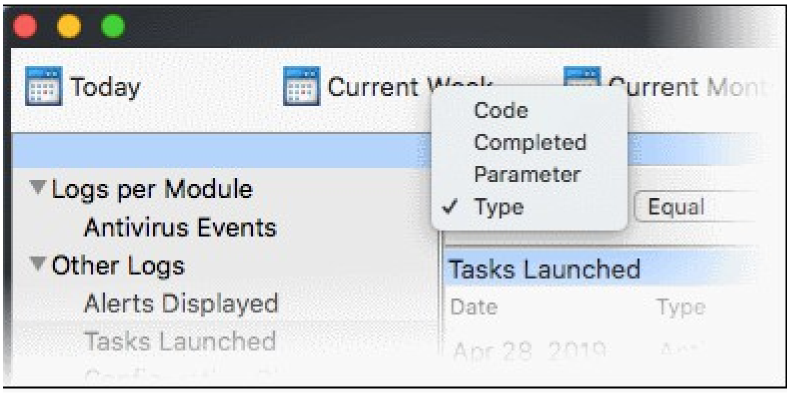
You can create custom views of all logged events according to the following criteria:

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

Configure Event Filters

- Open CCS.
- Click 'More' > 'View Logs' > 'Other Logs' > 'Tasks Launched'
- Right-click inside the log viewer module and choose 'Advanced Filter'

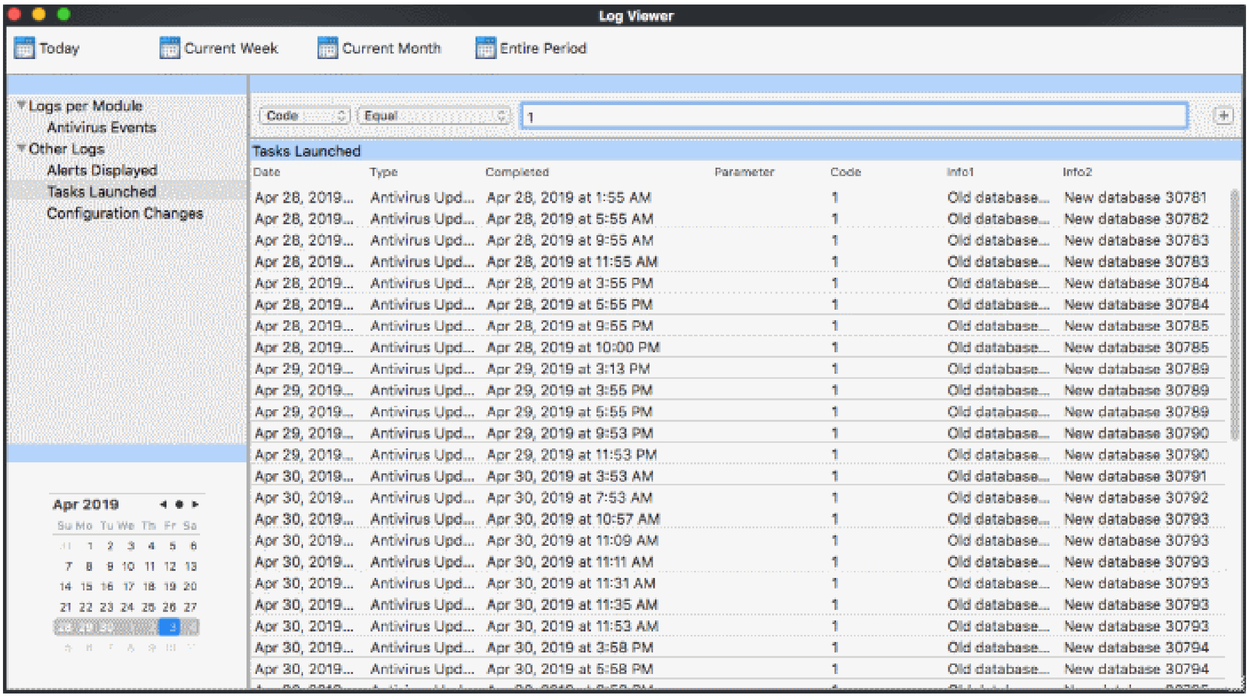
There are 4 types of filter. Each of these can be further refined by various parameters.



- **Code:** Filter logs by CCS internal code. You need to enter the code value in the field provided.

  Code values are as follows:

  - 0 - Success
  - 1 - Failure
  - 2 - Connection Error (internet connection failed)
  - 7 - User Cancel (when AV update dialog is closed midway)



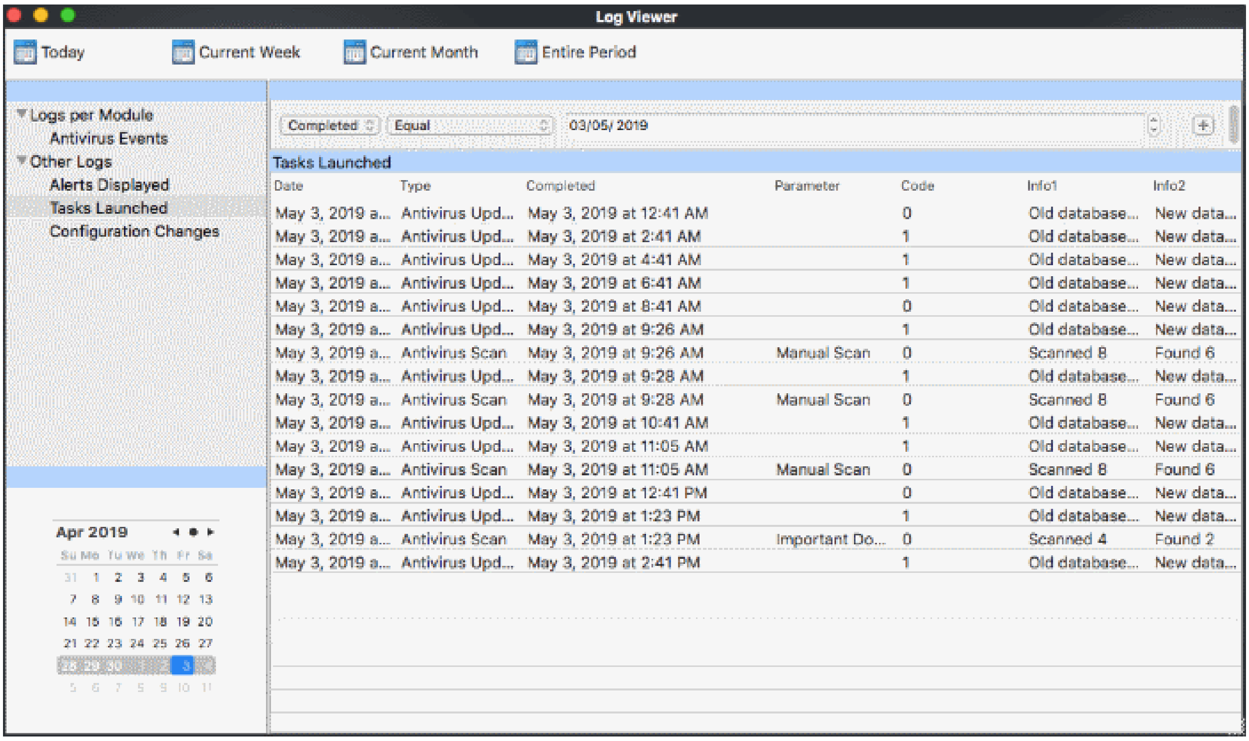
Code | Equal | 1

Tasks Launched

Date	Type	Completed	Parameter	Code	Info1	Info2
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 1:55 AM		1	Old database...	New database 30781
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 5:55 AM		1	Old database...	New database 30782
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 9:55 AM		1	Old database...	New database 30783
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 11:55 AM		1	Old database...	New database 30783
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 3:55 PM		1	Old database...	New database 30784
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 5:55 PM		1	Old database...	New database 30784
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 9:55 PM		1	Old database...	New database 30785
Apr 28, 2019...	Antivirus Upd...	Apr 28, 2019 at 10:00 PM		1	Old database...	New database 30785
Apr 29, 2019...	Antivirus Upd...	Apr 29, 2019 at 3:13 PM		1	Old database...	New database 30789
Apr 29, 2019...	Antivirus Upd...	Apr 29, 2019 at 3:55 PM		1	Old database...	New database 30789
Apr 29, 2019...	Antivirus Upd...	Apr 29, 2019 at 5:55 PM		1	Old database...	New database 30789
Apr 29, 2019...	Antivirus Upd...	Apr 29, 2019 at 9:53 PM		1	Old database...	New database 30790
Apr 29, 2019...	Antivirus Upd...	Apr 29, 2019 at 11:53 PM		1	Old database...	New database 30790
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 3:53 AM		1	Old database...	New database 30791
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 7:53 AM		1	Old database...	New database 30792
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 10:57 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 11:09 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 11:11 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 11:31 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 11:35 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 11:53 AM		1	Old database...	New database 30793
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 3:58 PM		1	Old database...	New database 30794
Apr 30, 2019...	Antivirus Upd...	Apr 30, 2019 at 5:58 PM		1	Old database...	New database 30794

- Select any of the following options from the second drop-down.
  - **Equal** - Show only events matching the CCS Code
  - **Greater than** - Show only events where CCS code is higher than the specified value
  - **Greater than or equal** - Show only events where CCS code is higher or same as the specified value
  - **Less than** - Show only events where CCS code is lower than the specified value
  - **Less than or Equal** - Show only events where CCS code is lower or same as the specified value
  - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + enter '1' to view all events except of CCS code of '1'

- **Completed**: Filter log entries by their end dates. You need to specify the date in the field provided. You can then refine your filter by specifying more parameters such as greater than the specified date and so on.

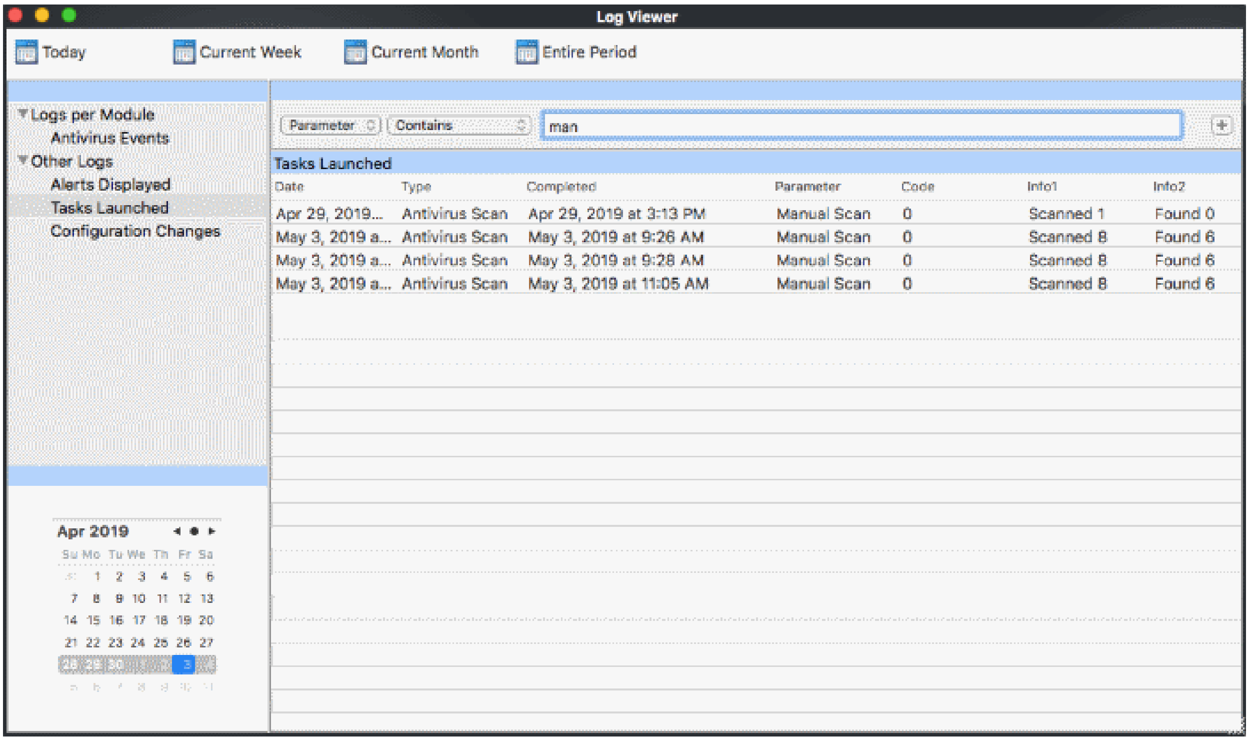


Completed | Equal | 03/05/ 2019

Tasks Launched

Date	Type	Completed	Parameter	Code	Info1	Info2
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 12:41 AM		0	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 2:41 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 4:41 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 6:41 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 8:41 AM		0	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 9:26 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 9:26 AM	Manual Scan	0	Scanned 8	Found 6
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 9:28 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 9:28 AM	Manual Scan	0	Scanned 8	Found 6
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 10:41 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 11:05 AM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 11:05 AM	Manual Scan	0	Scanned 8	Found 6
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 12:41 PM		0	Old database...	New data...
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 1:23 PM		1	Old database...	New data...
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 1:23 PM	Important Do...	0	Scanned 4	Found 2
May 3, 2019 a...	Antivirus Upd...	May 3, 2019 at 2:41 PM		1	Old database...	New data...

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



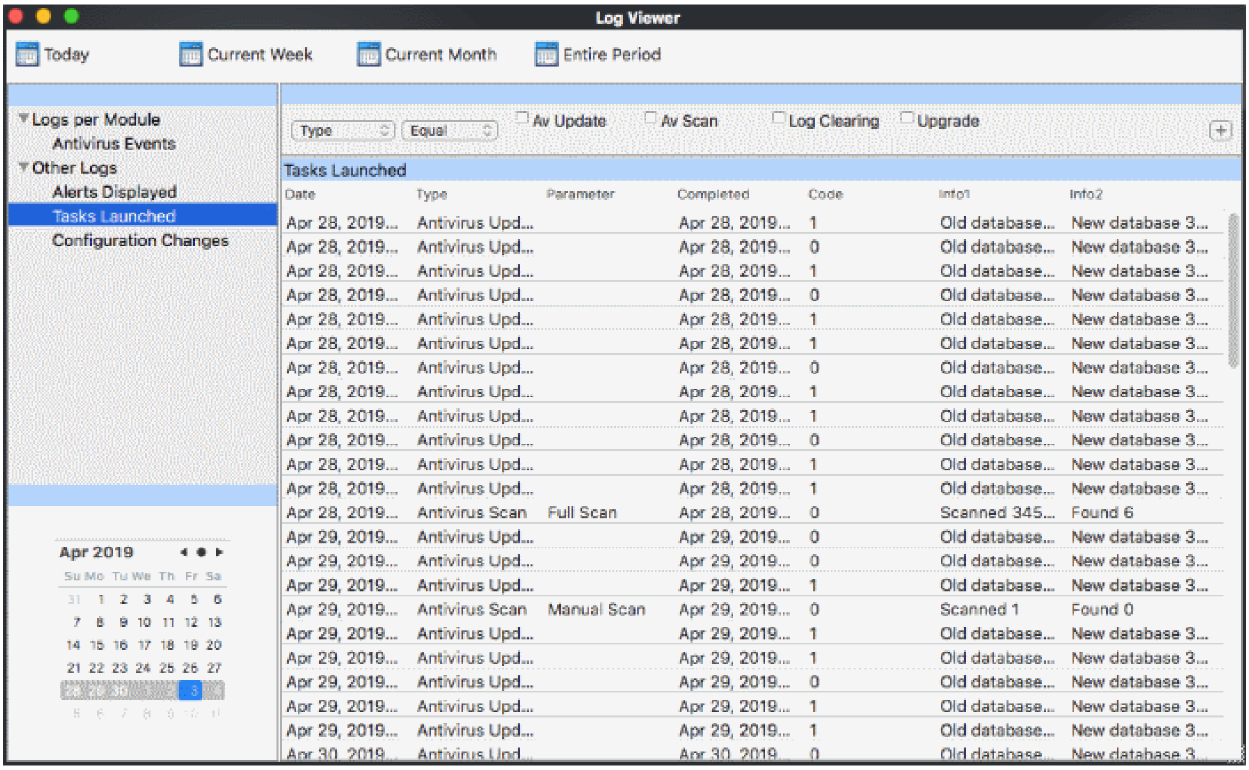
Parameter | Contains | man

Tasks Launched

Date	Type	Completed	Parameter	Code	Info1	Info2
Apr 29, 2019...	Antivirus Scan	Apr 29, 2019 at 3:13 PM	Manual Scan	0	Scanned 1	Found 0
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 9:26 AM	Manual Scan	0	Scanned 8	Found 6
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 9:28 AM	Manual Scan	0	Scanned 8	Found 6
May 3, 2019 a...	Antivirus Scan	May 3, 2019 at 11:05 AM	Manual Scan	0	Scanned 8	Found 6

- Select 'Contains' or 'Does Not Contain' from the second drop-down:
  - **Contains -** Show only events which concern the parameter (scan type) you enter. You can add multiple parameters.
  - **Does Not Contain -** Show events which did not concern parameters you specify.

- **Type:** Filter by tasks category. You can then filter by a specific type of category. For example, to only show AV update events.



Type | Equal | □ Av Update □ Av Scan □ Log Clearing □ Upgrade

Tasks Launched

Date	Type	Parameter	Completed	Code	Info1	Info2
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	0	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Upd...		Apr 28, 2019...	1	Old database...	New database 3...
Apr 28, 2019...	Antivirus Scan	Full Scan	Apr 28, 2019...	0	Scanned 345...	Found 6
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 3...
Apr 29, 2019...	Antivirus Scan	Manual Scan	Apr 29, 2019...	0	Scanned 1	Found 0
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	0	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 3...
Apr 29, 2019...	Antivirus Upd...		Apr 29, 2019...	1	Old database...	New database 3...
Apr 30, 2019...	Antivirus Upd...		Apr 30, 2019...	0	Old database...	New database 3...

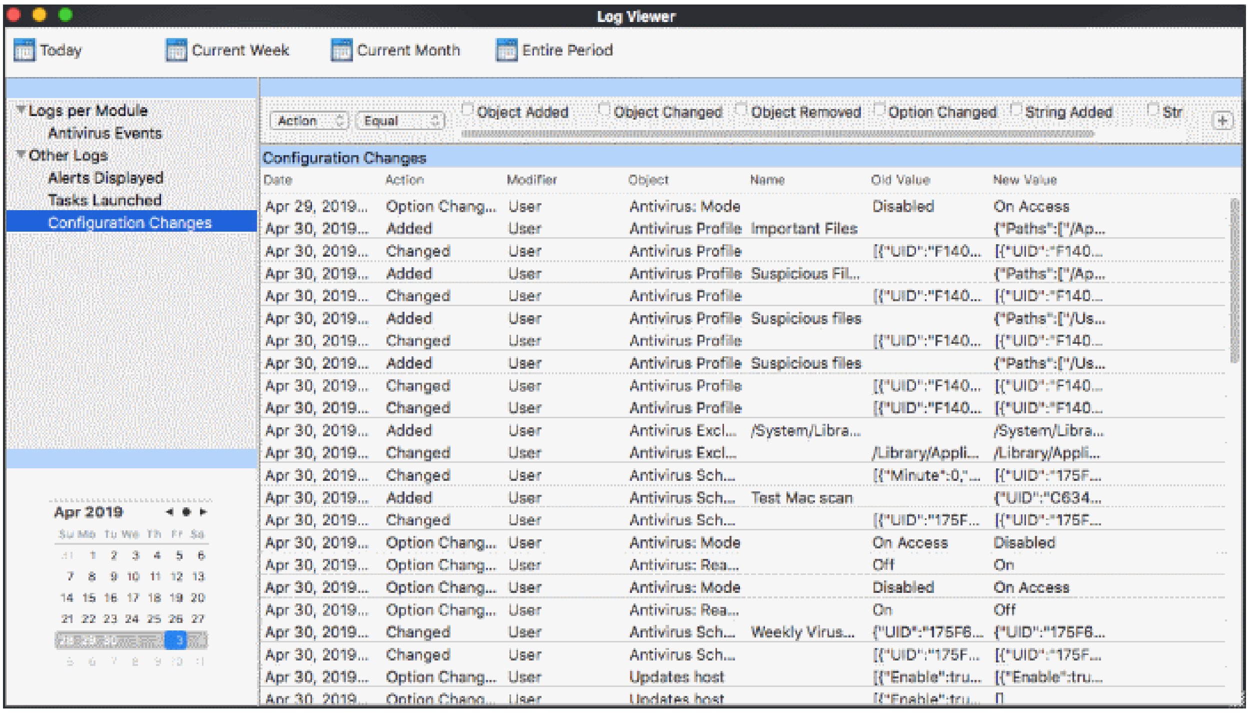
- Select 'Equal' or 'Not Equal' from the second drop-down.

- **Equal -** Show only events which feature the task category you select. You can select multiple categories.
- **Not Equal -** Inverts your choice. For example, select 'Not Equal' + 'AV Update' to view every event except 'AV Update' types.

- Select the specific type you want to view from:
  - **AV Update -** Task events of antivirus database updates
  - **AV Scan -** Events of antivirus scans
  - **Log Clearing -** Events of all logs deleted.
  - **Upgrade -** Not used.

4.7.4. Configuration Change Logs

Configuration change logs record all modifications to CCS settings since installation:

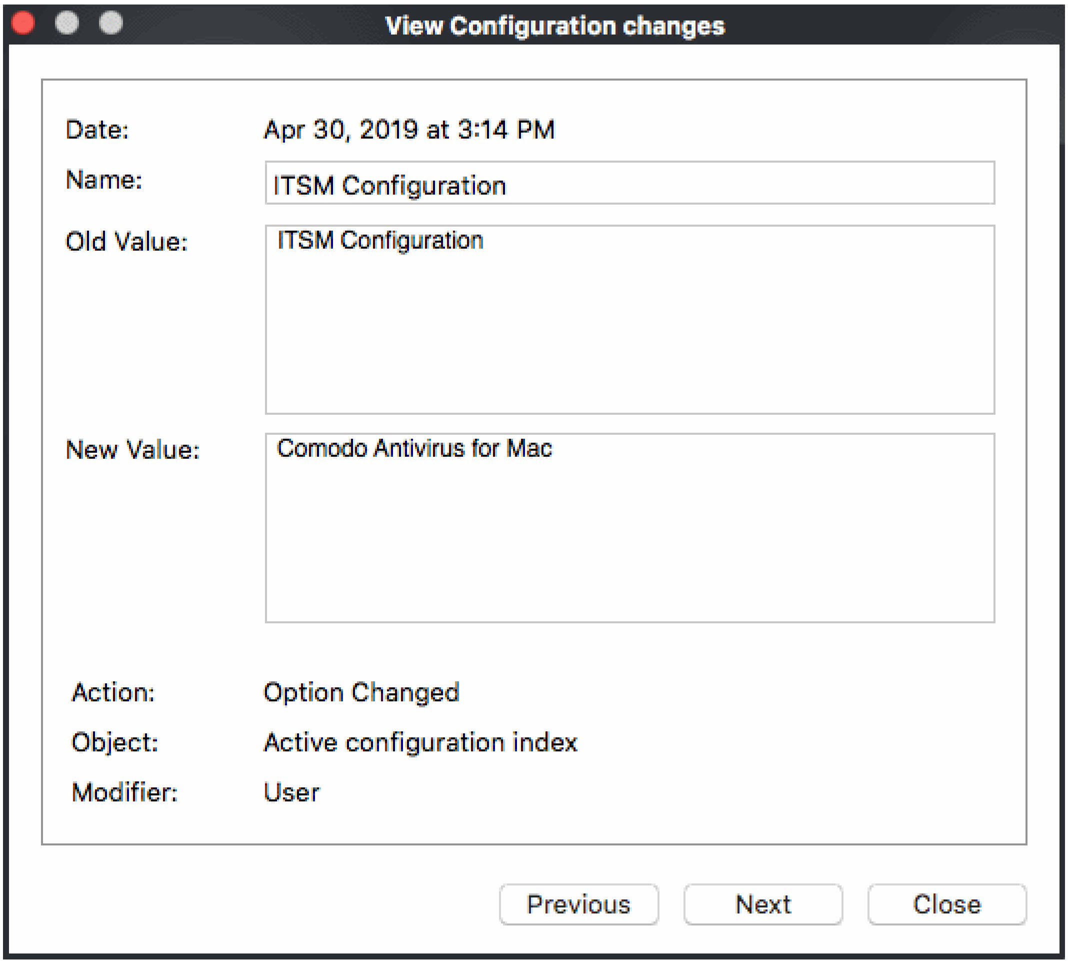


Configuration Changes

Date	Action	Modifier	Object	Name	Old Value	New Value
Apr 29, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Added	User	Antivirus Profile	Important Files		{"Paths":["/Ap...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious Fil...		{"Paths":["/Ap...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious files		{"Paths":["/Us...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious files		{"Paths":["/Us...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Excl...	/System/Libra...		/System/Libra...
Apr 30, 2019...	Changed	User	Antivirus Excl...		/Library/Appli...	/Library/Appli...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"Minute":0,"...	[{"UID":"175F...
Apr 30, 2019...	Added	User	Antivirus Sch...	Test Mac scan		{"UID":"C634...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"UID":"175F...	[{"UID":"175F...
Apr 30, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 30, 2019...	Option Chang...	User	Antivirus: Rea...		Off	On
Apr 30, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Option Chang...	User	Antivirus: Rea...		On	Off
Apr 30, 2019...	Changed	User	Antivirus Sch...	Weekly Virus...	{"UID":"175F6...	{"UID":"175F6...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"UID":"175F...	[{"UID":"175F...
Apr 30, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":tru...
Apr 30, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[]

1. **Date -** The time of the configuration change.
2. **Action -** The nature of the configuration change. For example, AV profile added.
3. **Modifier -** The user that made the configuration change.
4. **Object -** The CCS setting that was affected by the change.
5. **Name -** The rule, program or the file that was changed.
6. **Old Value -** The setting before the configuration change.
7. **New Value -** The setting after the configuration change.

Double-click on an entry to view a summary of the log:



View Configuration changes

Date: Apr 30, 2019 at 3:14 PM

Name: ITSM Configuration

Old Value: ITSM Configuration

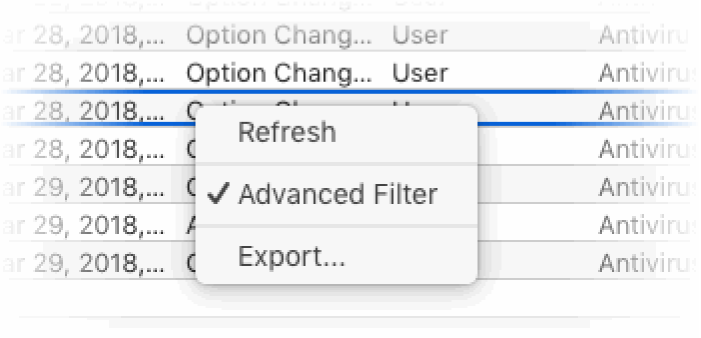
New Value: Comodo Antivirus for Mac

Action: Option Changed

Object: Active configuration index

Modifier: User

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



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

4.7.4.1. Filter 'Configuration Change' Logs

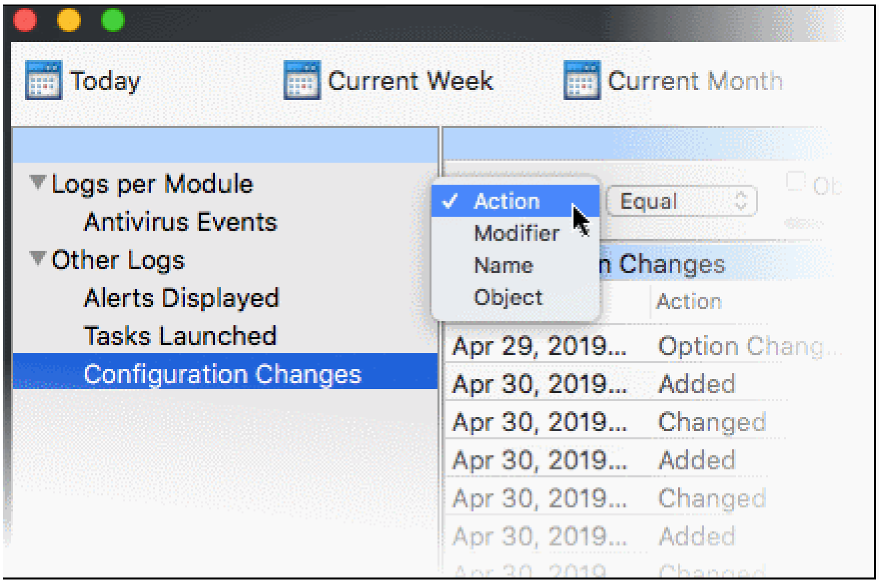
You can create custom views of logged events according to the following criteria:

- **Action:** Filter by the activity performed on the item in the 'Object' column. For example, 'Added', 'Changed'.
- **Modifier:** Filter by who, or what made the change.
- **Name:** Filter by the file/folder/path involved in the configuration change. For example, a particular folder/file was added to a scan profile.
- **Object** : The antivirus feature that was modified in the event. For example, AV profile, AV exclusion and so on.

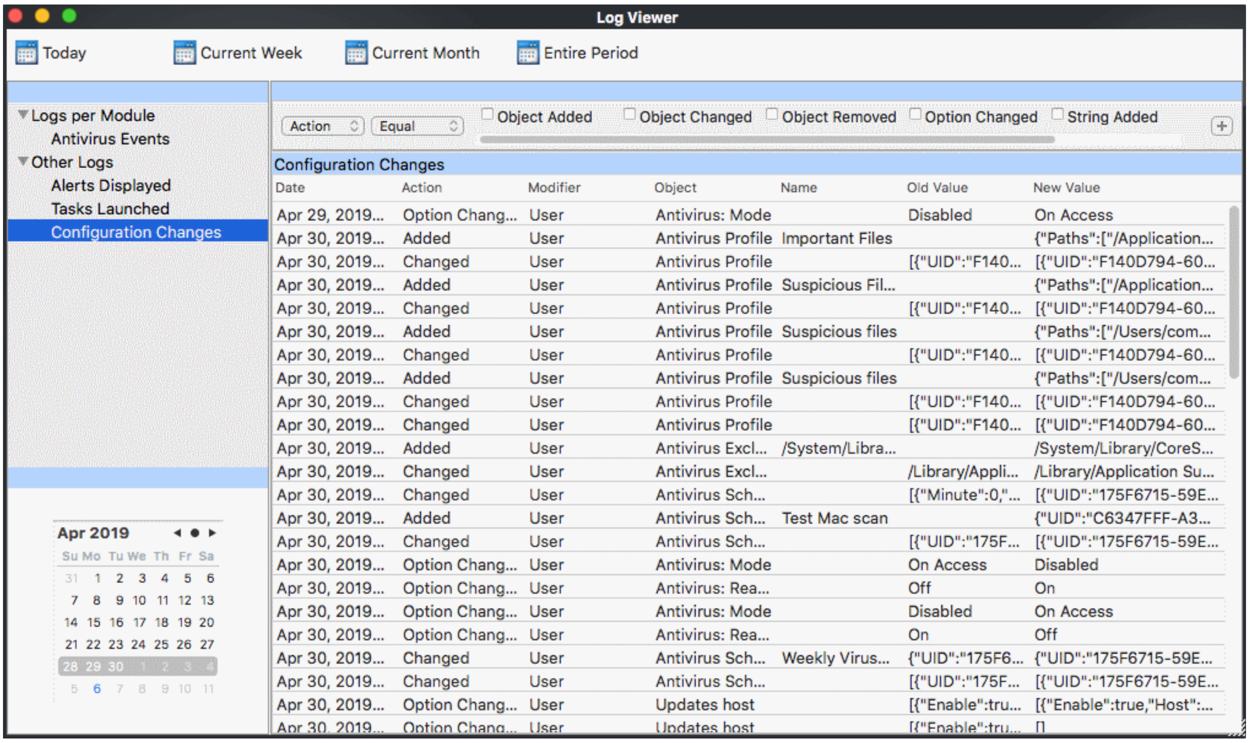
Configure Event Filters

- Open CCS.
- Click 'More' > 'View Logs' > 'Other Logs' > 'Configuration Changes'
- Right-click inside the log viewer module and choose 'Advanced Filter'

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



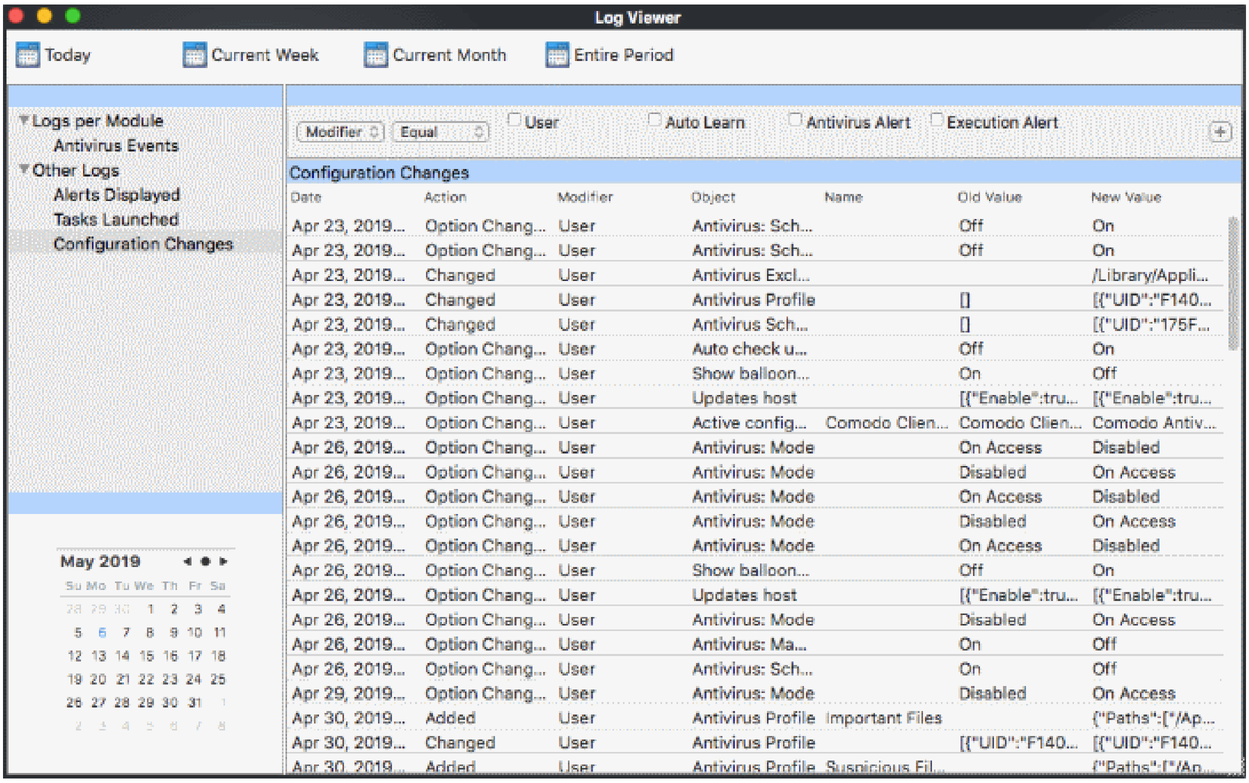
- **Action:** Filter events by updates to the configuration settings such as profile added and so on. You can filter by a specific type of action. For example, to only show events where an object was added.



Configuration Changes

Date	Action	Modifier	Object	Name	Old Value	New Value
Apr 29, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Added	User	Antivirus Profile	Important Files		{"Paths":["/Application...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140D794-60...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious Fil...		{"Paths":["/Application...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140D794-60...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious files		{"Paths":["/Users/com...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140D794-60...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious files		{"Paths":["/Users/com...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140D794-60...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140D794-60...
Apr 30, 2019...	Added	User	Antivirus Excl...	/System/Libra...		/System/Library/CoreS...
Apr 30, 2019...	Changed	User	Antivirus Excl...		/Library/Appli...	/Library/Application Su...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"Minute":0,"...	[{"UID":"175F6715-59E...
Apr 30, 2019...	Added	User	Antivirus Sch...	Test Mac scan		{"UID":"C6347FFF-A3...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"UID":"175F...	[{"UID":"175F6715-59E...
Apr 30, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 30, 2019...	Option Chang...	User	Antivirus: Rea...		Off	On
Apr 30, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Option Chang...	User	Antivirus: Rea...		On	Off
Apr 30, 2019...	Changed	User	Antivirus Sch...	Weekly Virus...	{"UID":"175F6...	{"UID":"175F6715-59E...
Apr 30, 2019...	Changed	User	Antivirus Sch...		[{"UID":"175F...	[{"UID":"175F6715-59E...
Apr 30, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":true,"Host":...
Apr 30, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[]

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

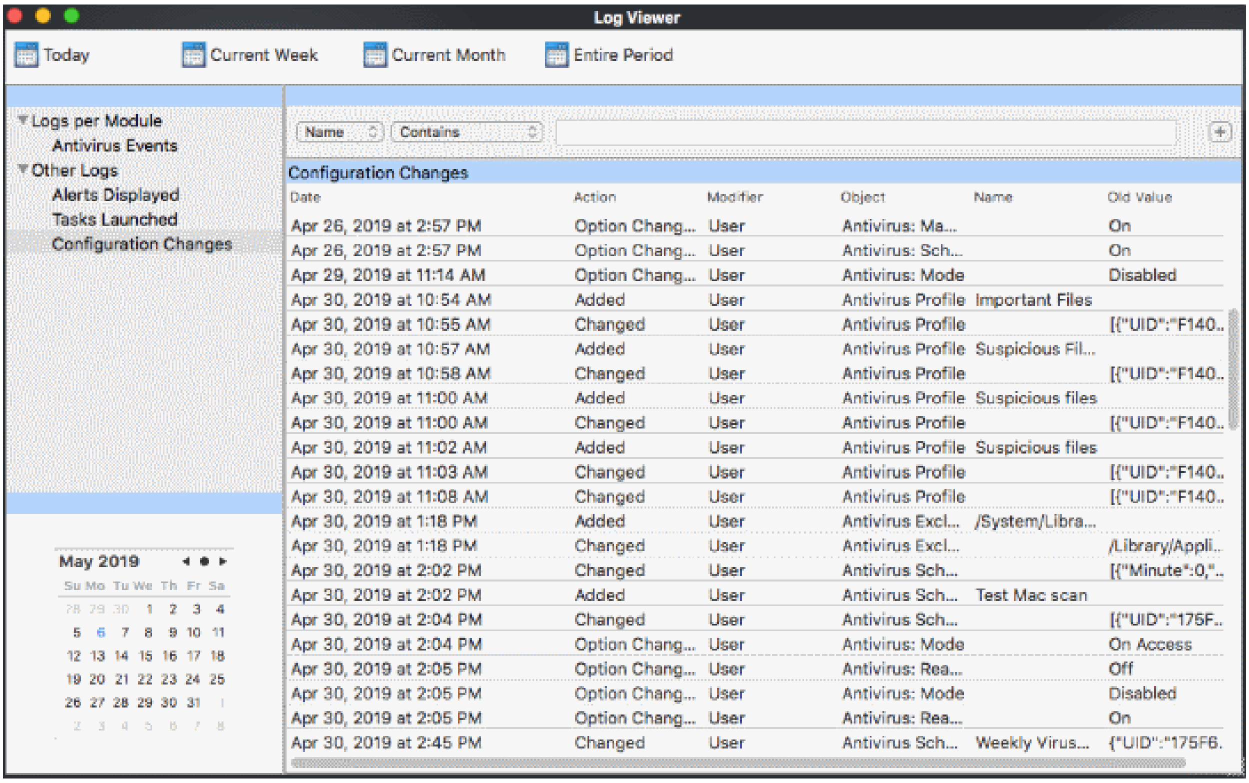


Modifier | Equal | □ User | □ Auto Learn | □ Antivirus Alert | □ Execution Alert

Configuration Changes

Date	Action	Modifier	Object	Name	Old Value	New Value
Apr 23, 2019...	Option Chang...	User	Antivirus: Sch...		Off	On
Apr 23, 2019...	Option Chang...	User	Antivirus: Sch...		Off	On
Apr 23, 2019...	Changed	User	Antivirus Excl...			/Library/Appli...
Apr 23, 2019...	Changed	User	Antivirus Profile		[]	[{"UID":"F140...
Apr 23, 2019...	Changed	User	Antivirus Sch...		[]	[{"UID":"175F...
Apr 23, 2019...	Option Chang...	User	Auto check u...		Off	On
Apr 23, 2019...	Option Chang...	User	Show balloon...		On	Off
Apr 23, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":tru...
Apr 23, 2019...	Option Chang...	User	Active config...	Comodo Clien...	Comodo Clien...	Comodo Antiv...
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Show balloon...		Off	On
Apr 26, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":tru...
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Ma...		On	Off
Apr 26, 2019...	Option Chang...	User	Antivirus: Sch...		On	Off
Apr 29, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Added	User	Antivirus Profile	Important Files		{"Paths":["/Ap...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious Fil...		{"Paths":["/Ap...

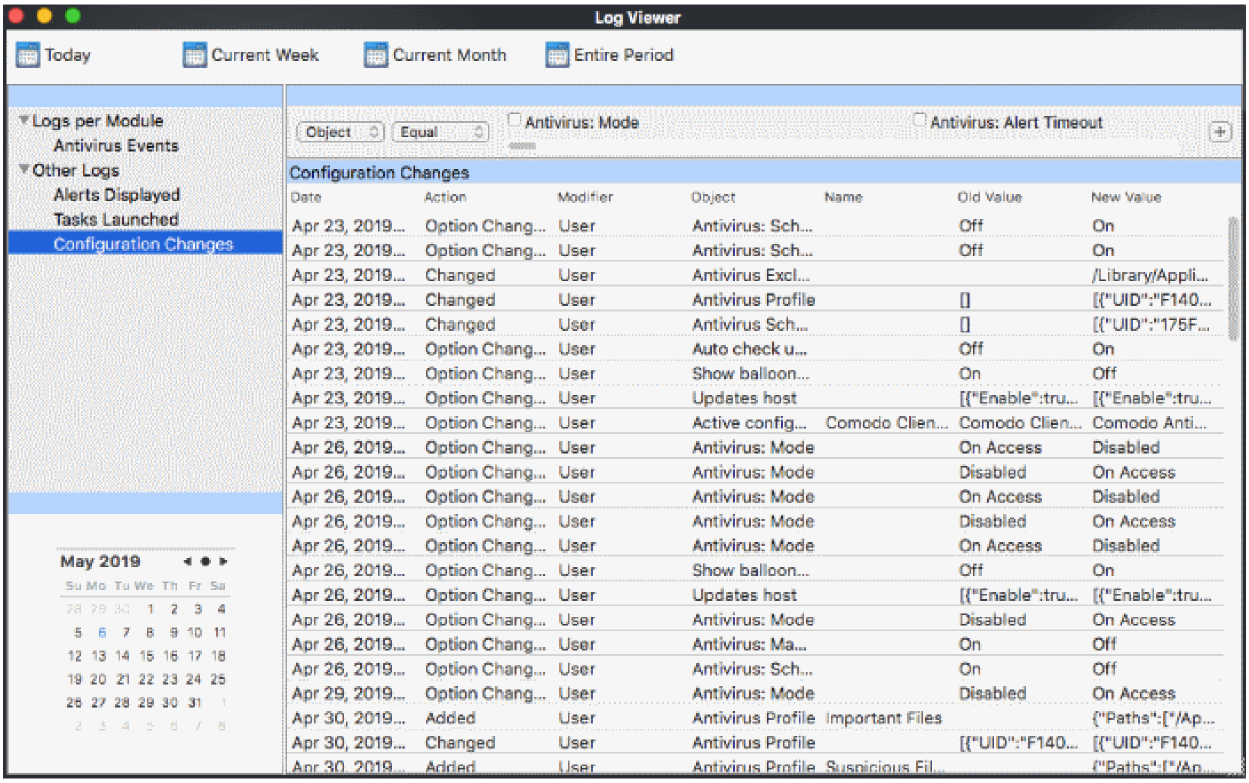
- Select 'Equal' or 'Not Equal' option from the second drop-down.
  - **Equal** - Show only events which feature the action you select. You can select multiple actions.
  - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'User' to view every event except those that were modified by the user.
- Select the specific actions you want to view from:
  - **User** - Events that were modified by the user
  - **Auto Learn** - Not used.
  - **Antivirus Alert** - Not used.
  - **Execution Alert** - Execution alert is reserved for future version of CCSM
- **Name:** Filter events by files/folders/path of files that was involved in the configuration change. For example, a particular folder/file was added to a scan profile. You need to enter the label in the field provided:



Configuration Changes

Date	Action	Modifier	Object	Name	Old Value
Apr 26, 2019 at 2:57 PM	Option Chang...	User	Antivirus: Ma...		On
Apr 26, 2019 at 2:57 PM	Option Chang...	User	Antivirus: Sch...		On
Apr 29, 2019 at 11:14 AM	Option Chang...	User	Antivirus: Mode		Disabled
Apr 30, 2019 at 10:54 AM	Added	User	Antivirus Profile	Important Files	
Apr 30, 2019 at 10:55 AM	Changed	User	Antivirus Profile		[{"UID":"F140..
Apr 30, 2019 at 10:57 AM	Added	User	Antivirus Profile	Suspicious Fil...	
Apr 30, 2019 at 10:58 AM	Changed	User	Antivirus Profile		[{"UID":"F140..
Apr 30, 2019 at 11:00 AM	Added	User	Antivirus Profile	Suspicious files	
Apr 30, 2019 at 11:00 AM	Changed	User	Antivirus Profile		[{"UID":"F140..
Apr 30, 2019 at 11:02 AM	Added	User	Antivirus Profile	Suspicious files	
Apr 30, 2019 at 11:03 AM	Changed	User	Antivirus Profile		[{"UID":"F140..
Apr 30, 2019 at 11:08 AM	Changed	User	Antivirus Profile		[{"UID":"F140..
Apr 30, 2019 at 1:18 PM	Added	User	Antivirus Excl...	/System/Libra...	
Apr 30, 2019 at 1:18 PM	Changed	User	Antivirus Excl...		/Library/Appli..
Apr 30, 2019 at 2:02 PM	Changed	User	Antivirus Sch...		[{"Minute":0,"..
Apr 30, 2019 at 2:02 PM	Added	User	Antivirus Sch...	Test Mac scan	
Apr 30, 2019 at 2:04 PM	Changed	User	Antivirus Sch...		[{"UID":"175F..
Apr 30, 2019 at 2:04 PM	Option Chang...	User	Antivirus: Mode		On Access
Apr 30, 2019 at 2:05 PM	Option Chang...	User	Antivirus: Rea...		Off
Apr 30, 2019 at 2:05 PM	Option Chang...	User	Antivirus: Mode		Disabled
Apr 30, 2019 at 2:05 PM	Option Chang...	User	Antivirus: Rea...		On
Apr 30, 2019 at 2:45 PM	Changed	User	Antivirus Sch...	Weekly Virus...	{"UID":"175F6.

- Select 'Contains' or 'Does Not Contain' from the second drop-down:
    - **Contains -** Show only those events which concern items that you specify. You can add multiple names.
    - **Does Not Contain -** Show events which did not concern names that you specify.
- **Object**: Filter events by the item that was changed. Examples include AV profile, AV schedule, AV alert timeout, and more.



Configuration Changes

Date	Action	Modifier	Object	Name	Old Value	New Value
Apr 23, 2019...	Option Chang...	User	Antivirus: Sch...		Off	On
Apr 23, 2019...	Option Chang...	User	Antivirus: Sch...		Off	On
Apr 23, 2019...	Changed	User	Antivirus Excl...			/Library/Appli...
Apr 23, 2019...	Changed	User	Antivirus Profile		[]	[{"UID":"F140...
Apr 23, 2019...	Changed	User	Antivirus Sch...		[]	[{"UID":"175F...
Apr 23, 2019...	Option Chang...	User	Auto check u...		Off	On
Apr 23, 2019...	Option Chang...	User	Show balloon...		On	Off
Apr 23, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":tru...
Apr 23, 2019...	Option Chang...	User	Active config...	Comodo Clien...	Comodo Clien...	Comodo Anti...
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		On Access	Disabled
Apr 26, 2019...	Option Chang...	User	Show balloon...		Off	On
Apr 26, 2019...	Option Chang...	User	Updates host		[{"Enable":tru...	[{"Enable":tru...
Apr 26, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 26, 2019...	Option Chang...	User	Antivirus: Ma...		On	Off
Apr 26, 2019...	Option Chang...	User	Antivirus: Sch...		On	Off
Apr 29, 2019...	Option Chang...	User	Antivirus: Mode		Disabled	On Access
Apr 30, 2019...	Added	User	Antivirus Profile	Important Files		{"Paths":["/Ap...
Apr 30, 2019...	Changed	User	Antivirus Profile		[{"UID":"F140...	[{"UID":"F140...
Apr 30, 2019...	Added	User	Antivirus Profile	Suspicious Fil...		{"Paths":["/Ap...

- Select 'Equal' or 'Not Equal' from the second drop-down.
  - **Equal** - Show only events which feature the action you select. You can select multiple actions.
  - **Not Equal** - Inverts your choice. For example, select 'Not Equal' + 'Antivirus: Alert Timeout' to view every event except those of changes to AV alert timeout settings.
- Select the specific actions you want to view from:
  - Antivirus: Mode
  - Antivirus: Alert Timeout
  - Antivirus: Real-Time Show Alerts
  - Antivirus: Real-Time Scan Memory
  - Antivirus: Real-Time Auto Update
  - Antivirus: Real-Time Auto Quarantine
  - Antivirus: Real-Time Size Limit
  - Antivirus: Real-Time Time Limit
  - Antivirus: Manual Scan Archives
  - Antivirus: Manual Scan Memory
  - Antivirus: Manual Auto Update
  - Antivirus: Manual Size Limit
  - Antivirus: Scheduled Scan Archives
  - Antivirus: Scheduled Scan Memory
  - Antivirus: Scheduled Scan Auto Update
  - Antivirus: Scheduled Auto Quarantine
  - Antivirus: Scheduled Size Limit
  - Antivirus Profile
  - Antivirus Schedule
  - Antivirus Exclusion
  - Antivirus: Disable Logging

- Active configuration index
- Password protection
- Antivirus: Suppress Alert when password protected
- Show balloon messages
- Auto check updates
- GUI language
- Password
- Updates host
- Log file size limit
- Log overflow handling
- Log backup folder
- Antivirus: Write to syslog server
- Syslog server host
- Syslog server port

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

The 'How To...' section of the guide contains guidance on key tasks of Comodo Client - Security.

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

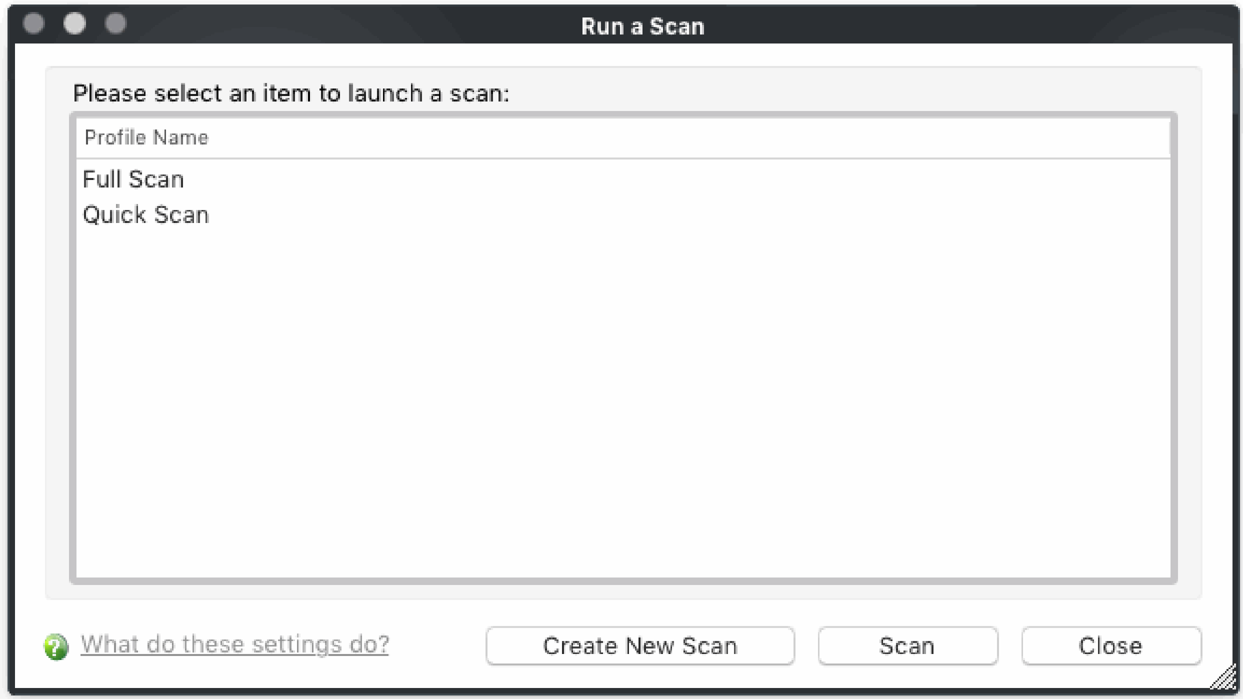
- **Scan your Computer for Viruses** - How to automatically or manually scan your computer
- **View Antivirus Events** - How to view logs made by the virus scanner
- **Configure Database Updates** - Specify how virus signature updates should be handled
- **Quickly Change Security Levels** - How to enable or disable real-time virus scans
- **Change CCS Language Settings** - Change the language used in the CCS interface
- **Run an instant Antivirus scan on Selected Items** - How to run custom scans on specific items or areas
- **Create a Scheduled Scan** - Setup up a virus scan which automatically runs at regular intervals
- **Restore Incorrectly Quarantined Item(s)** - Revert quarantined files to their original location
- **Switch Off Automatic Antivirus Updates** - Disable automatic virus updates
- **Suppress Alerts with Silent mode** - Switch off alerts and notifications to avoid interruption during important tasks.

Scan your Computer for Viruses

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

Run an on-demand virus scan

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click the 'Run a Scan' box



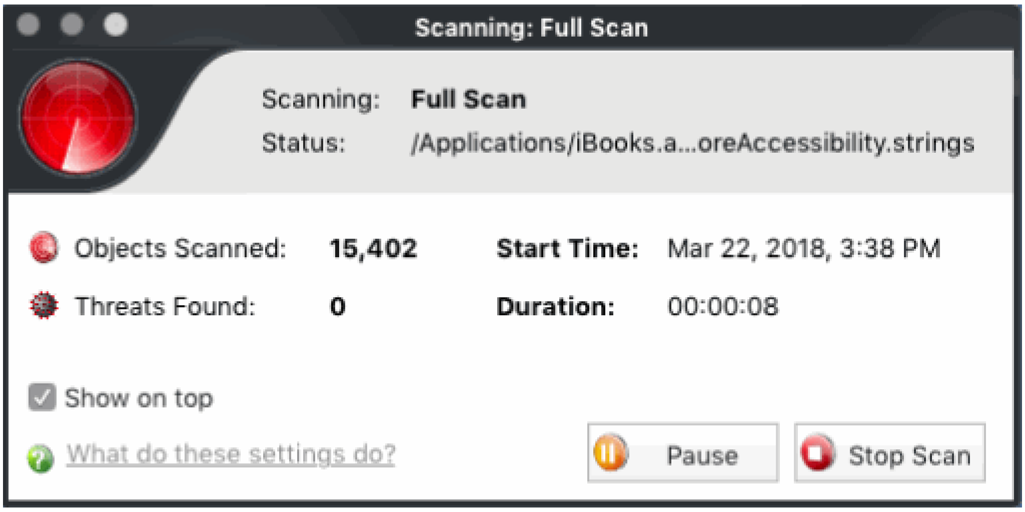
Please select an item to launch a scan:

Profile Name
Full Scan
Quick Scan

Choose one of the following options:

        - **Full Scan** - Scans every drive, folder and file on your system, including external connected devices
        - **Quick scan** - Scans important operating system files, system memory, auto-run entries, registry keys and hidden services.
    - **Create New Scan** - Create your own custom scan of specific files, folders or drives. See **custom scan** to find out more.
- Click 'Scan' after making your selection (or just double-click the profile name).

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

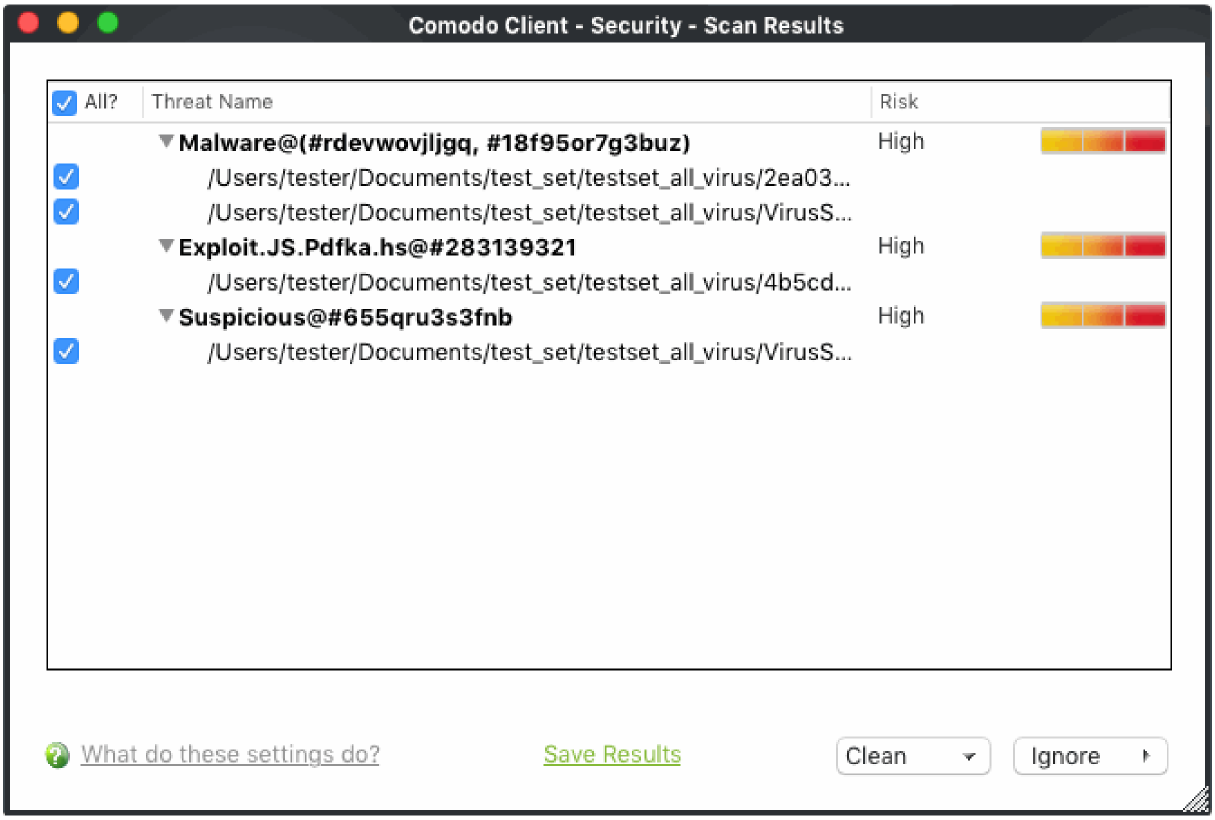


Scanning: **Full Scan**
Status: /Applications/iBooks.a...oreAccessibility.strings

Objects Scanned: **15,402** **Start Time:** Mar 22, 2018, 3:38 PM
Threats Found: **0** **Duration:** 00:00:08

☑ Show on top

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



Comodo Client - Security - Scan Results

☑ All?	Threat Name	Risk
	▼ **Malware@(#rdevwovjljgq, #18f95or7g3buz)**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/2ea03...	
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	
	▼ **Exploit.JS.Pdfka.hs@#283139321**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/4b5cd...	
	▼ **Suspicious@#655qru3s3fnb**	High
☑	/Users/tester/Documents/test_set/testset_all_virus/VirusS...	

Use the check-boxes on the left to select specific files, or select 'All?' to choose every file. Then pick one of the following options:

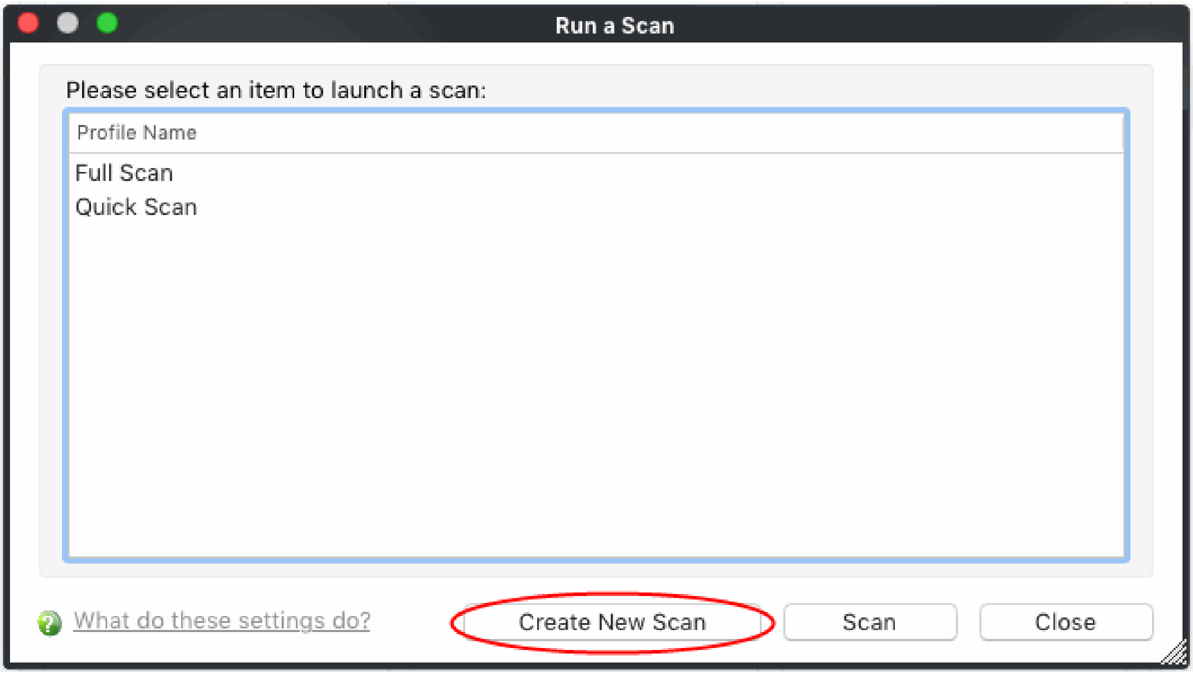
- **Clean** - CCS will deal with the threats. They will either be deleted, disinfected, or moved to **Quarantine**, depending on the type of threat found.
- **Ignore** - Take no action on the threat. You can also create a permanent exclusion for the file.
- You can export the results to a text file by clicking the 'Save Results' link.

See **Quarantined Items** for more details on quarantined applications.

See **Ignore an application/file** for more details on the 'Ignore' options.

Create a Scan profile

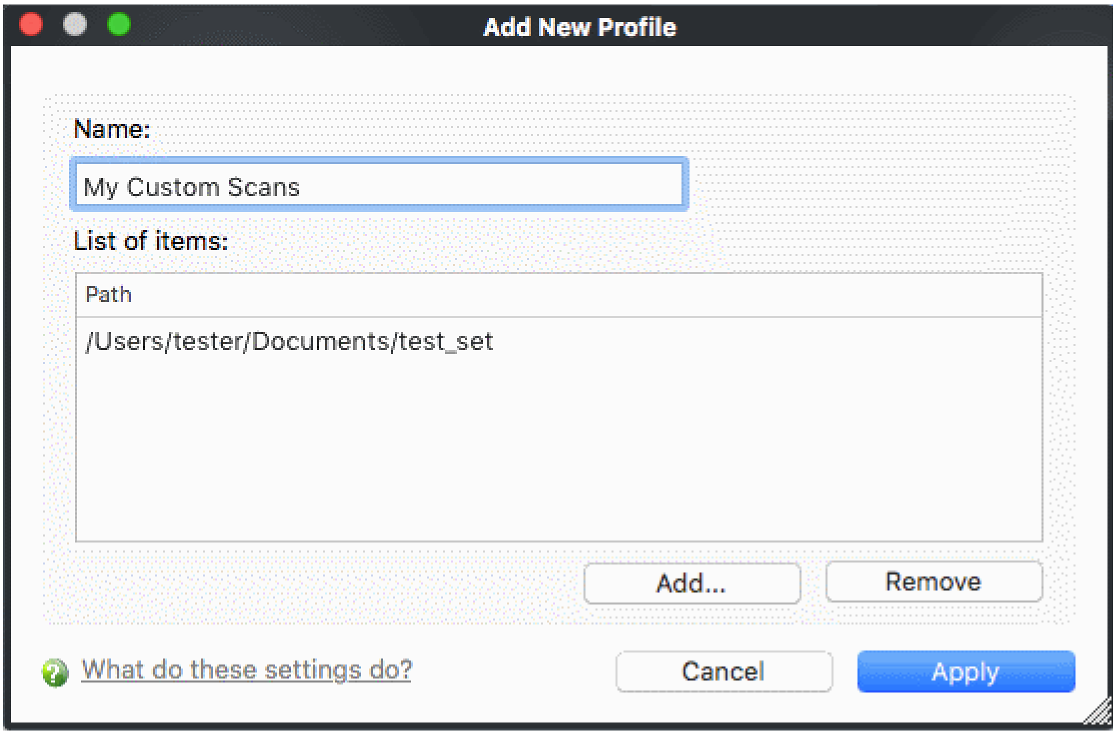
- Click 'Create New Scan' in the 'Run a Scan' interface.


Run a Scan

Please select an item to launch a scan:

Profile Name
Full Scan
Quick Scan

- Type a name for the scan profile. Click 'Add' to select the items you want to include in the scan.


Add New Profile

Name: My Custom Scans

List of items:

Path
/Users/tester/Documents/test_set

- Repeat the process to add more items.
- Click 'Apply' to save your profile.
- You can now select this profile after clicking 'Run a scan' or 'Scan Now'.

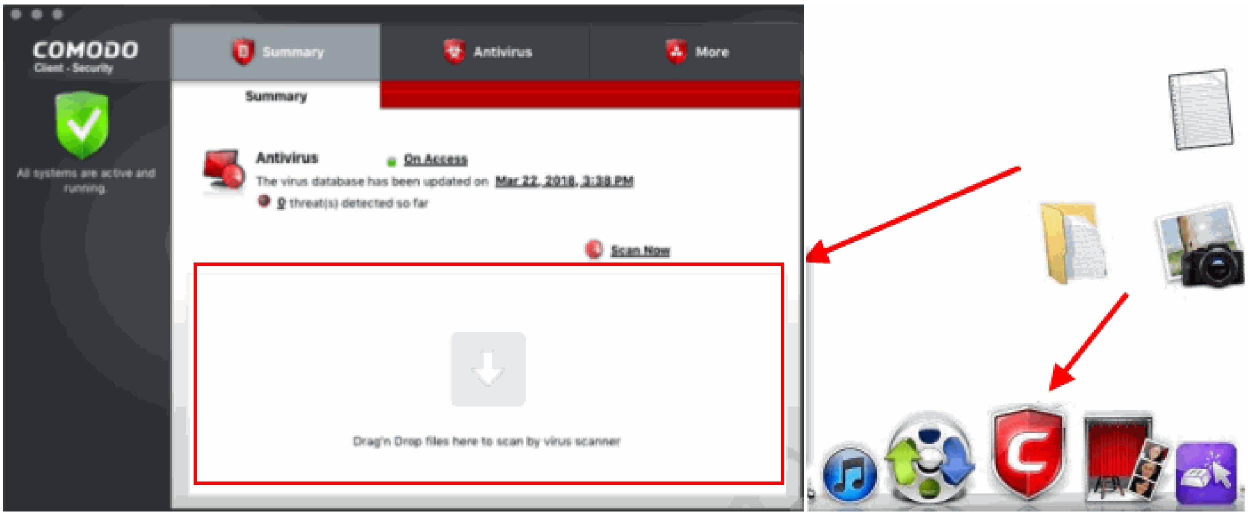
For more details on custom scan creation, see **Creating a Scan profile**.

Instantly Scan Objects

- Drag files/folders into the scan box on the summary screen

OR

- Drag them onto the Comodo dock icon



All systems are active and running.

The virus database has been updated on Mar 22, 2018, 3:38 PM

0 threat(s) detected so far

Drag'n Drop files here to scan by virus scanner

View Antivirus Events

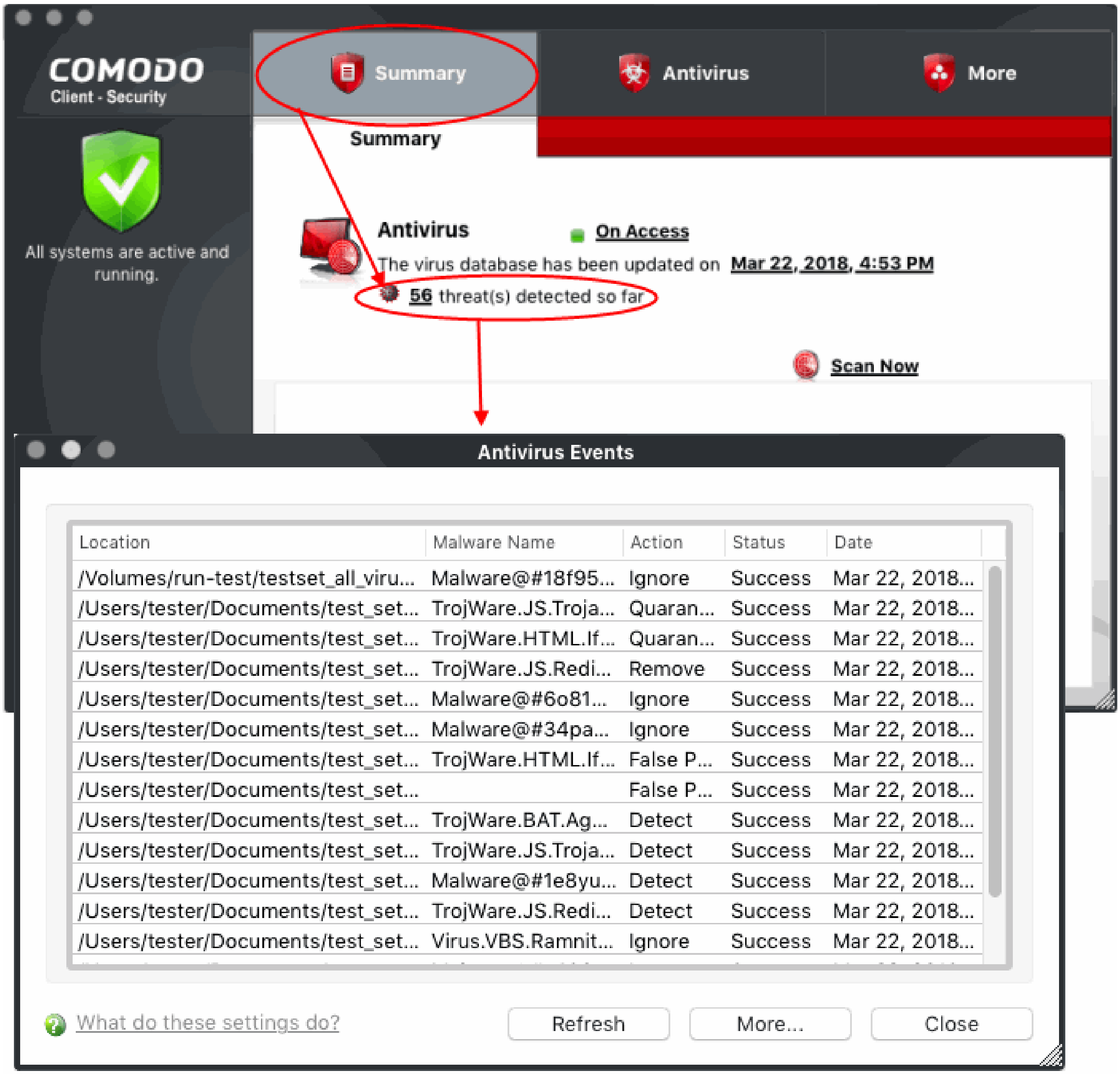
The antivirus events area contains logs of all actions taken by the virus scanner.

The basic event viewer shows:

- The date and time the threat was detected
- The location of the threat
- The action taken against it.

View Antivirus Events

- Open CIS at the summary screen
- Click the number in front of 'Threat(s) detected so far'



All systems are active and running.

Antivirus On Access

The virus database has been updated on Mar 22, 2018, 4:53 PM

56 threat(s) detected so far

Antivirus Events

Location	Malware Name	Action	Status	Date
/Volumes/run-test/testset_all_viru...	Malware@#18f95...	Ignore	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.JS.Troja...	Quaran...	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.HTML.If...	Quaran...	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.JS.Redi...	Remove	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	Malware@#6o81...	Ignore	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	Malware@#34pa...	Ignore	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.HTML.If...	False P...	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...		False P...	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.BAT.Ag...	Detect	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.JS.Troja...	Detect	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	Malware@#1e8yu...	Detect	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	TrojWare.JS.Redi...	Detect	Success	Mar 22, 2018...
/Users/tester/Documents/test_set...	Virus.VBS.Ramnit...	Ignore	Success	Mar 22, 2018...

What do these settings do?

- See **View Antivirus Events** for more help with event logs.

Configure Database Updates

To ensure maximum protection against the latest viruses, it is essential that you have the most recent virus database installed.

The default policy of CCS for MAC:

i. Periodically check for and download database updates

ii. Automatically check and update the virus database before starting any scan.

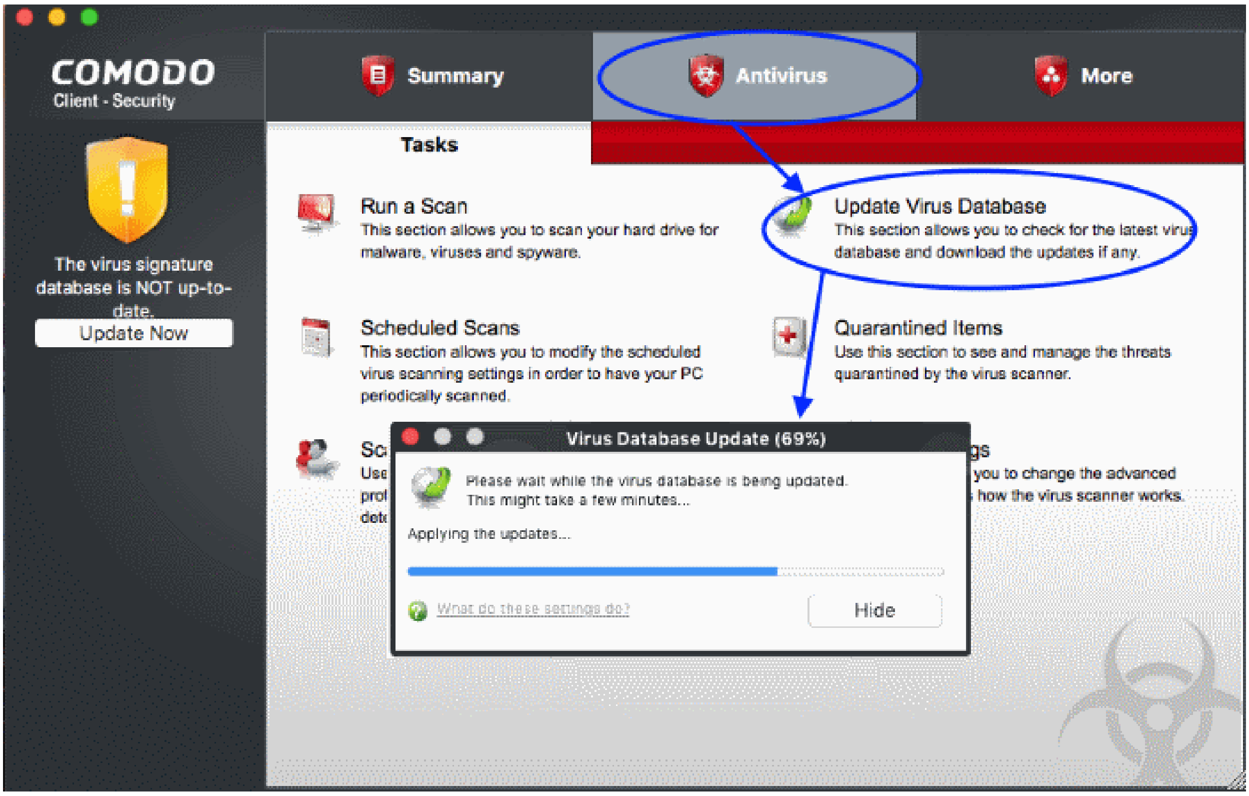
Please see the following links if you would like to manage updates:

- **Manually update the virus database**
- **Configure automatic database updates**

Manually update the virus database

- Open Comodo Client Security
- Click Antivirus' > 'Update Virus Database'

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


COMODO
Client - Security
The virus signature database is NOT up-to-date.
Update Now
Summary
Antivirus
More
Tasks
Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.
Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.
Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.
Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.
Virus Database Update (69%)
Please wait while the virus database is being updated. This might take a few minutes...
Applying the updates...
What do these settings do?
Hide

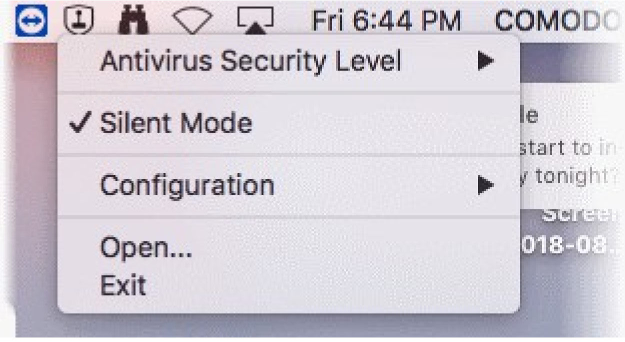
Configure automatic database updates before scanning

- Open Comodo Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Select 'Real Time Scanning', 'Manual Scanning' or 'Scheduled Scanning'
- Enable or disable the 'Automatically update virus database before scanning' check-box
- You can also enable or disable pre-scan updates for each scan type

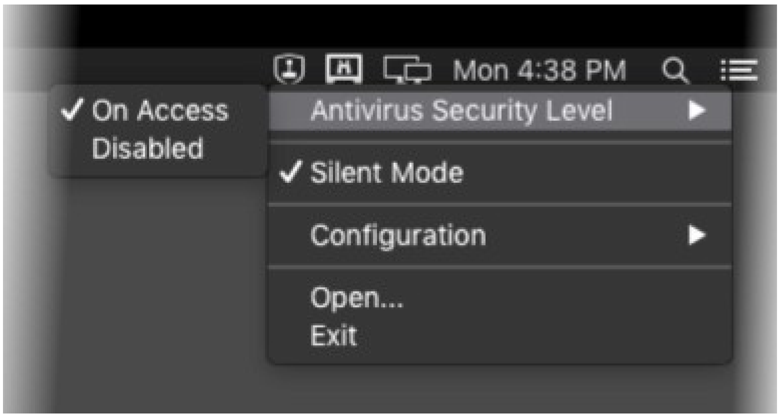
See '**Scanner Settings**' if you need more help with this.

Quickly Set up Security Levels

Right-click on the system tray icon to quickly view or change the current security level:



- Move your mouse cursor over the 'Antivirus Security Level'



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

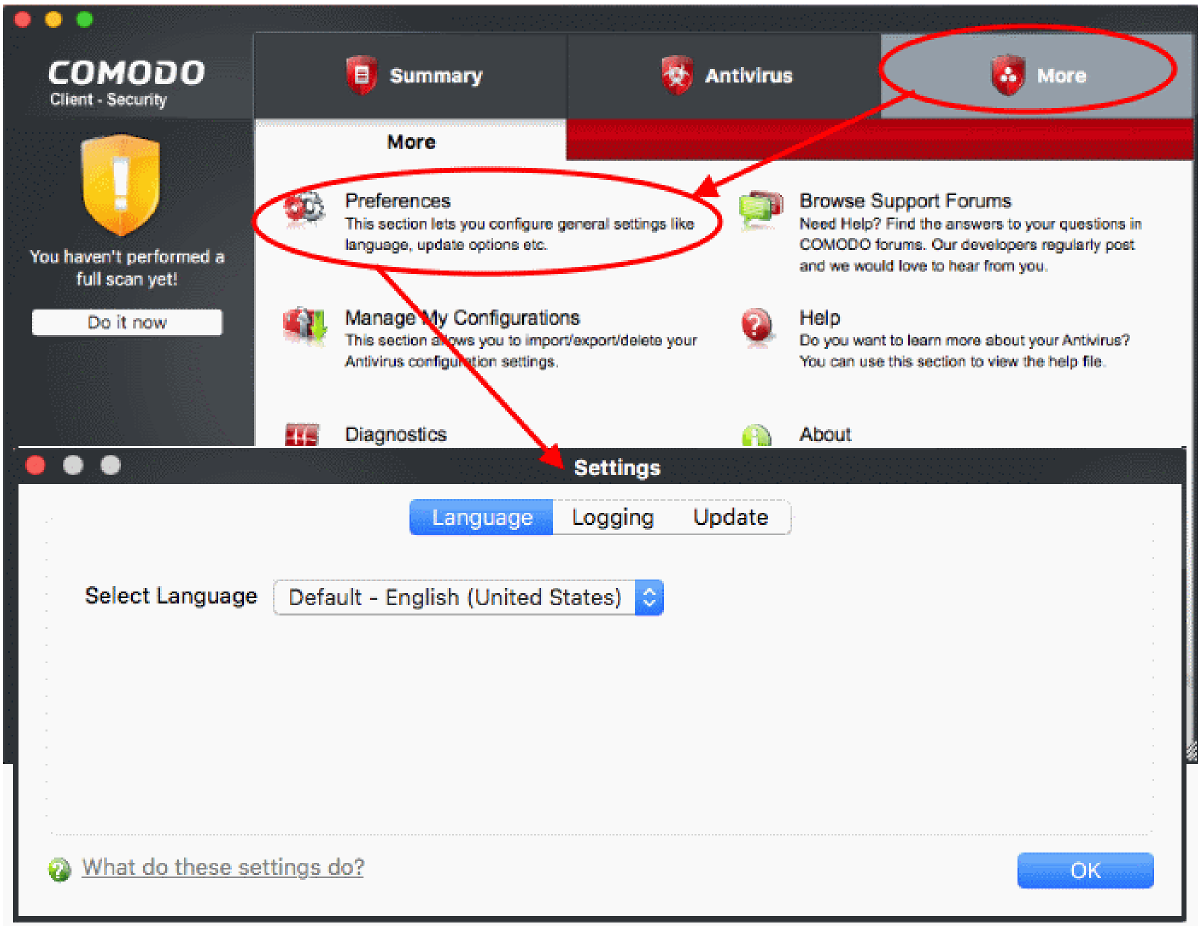
The currently active configuration is shown with a check-mark next to it. See **Real Time Scan** for more details.

You can also access these settings through the the **summary screen**.

Change CCS Language Settings

To view or modify the language

- Open Comodo Client Security
- Click ‘More’ tasks > 'Preferences'
- Click 'Language'
- Choose the language you wish to use from the drop-down menu. The currently active language will have a check-mark next to it:



You haven't performed a full scan yet!

Preferences
This section lets you configure general settings like language, update options etc.

Browse Support Forums
Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.

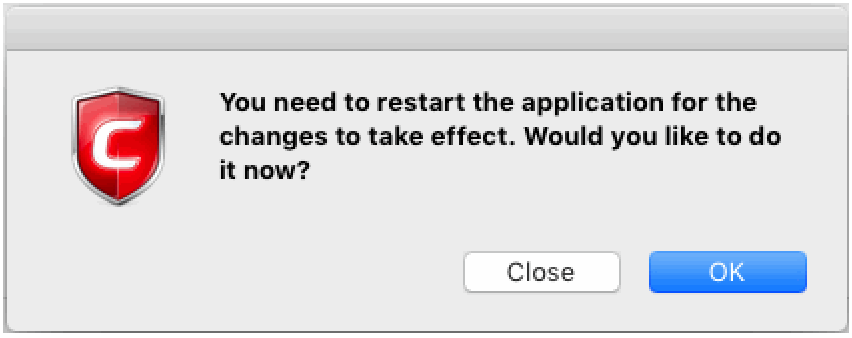
Manage My Configurations
This section allows you to import/export/delete your Antivirus configuration settings.

Help
Do you want to learn more about your Antivirus? You can use this section to view the help file.

Select Language: Default - English (United States)

What do these settings do?

- Click 'OK' then restart the application to apply changes:



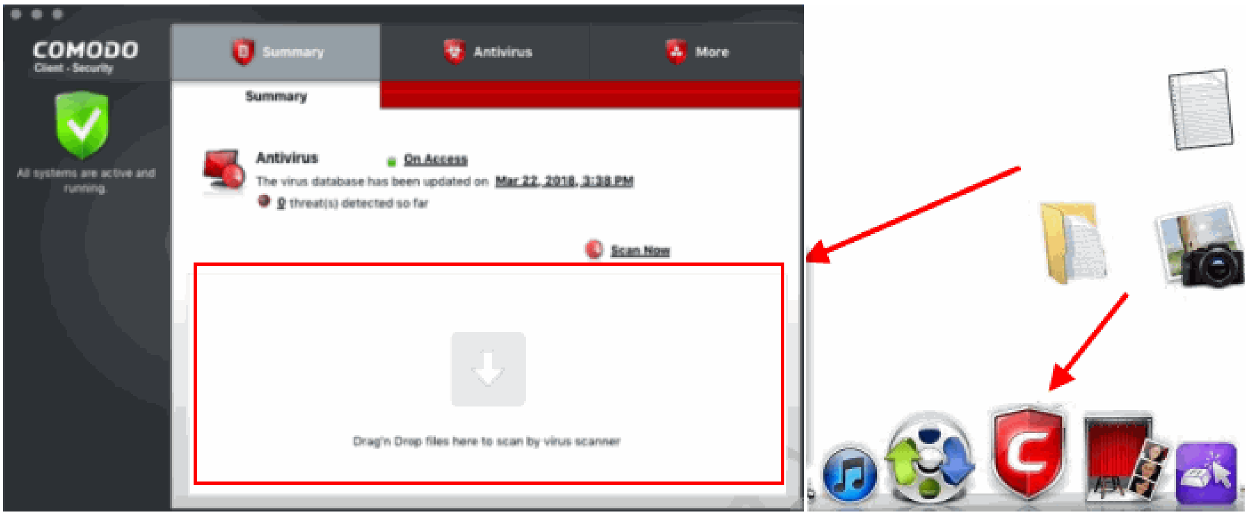
You need to restart the application for the changes to take effect. Would you like to do it now?

Run an Instant Antivirus Scan on Selected Items

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

Scan selected item(s):

- Open Comodo Client Security
- Drag the items into the scan box in the 'Summary' interface
- Alternatively, drag the items onto the Comodo icon on the dock.

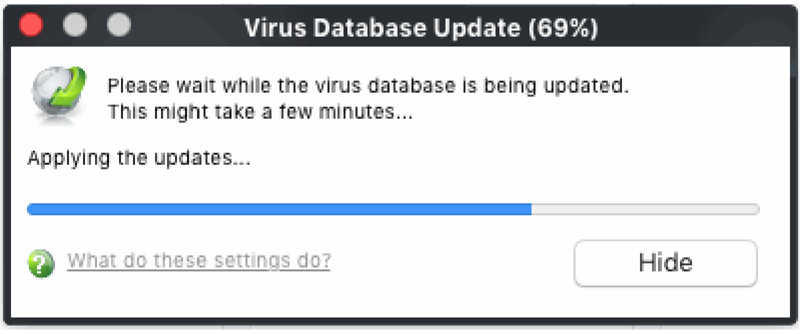


The virus database has been updated on Mar 22, 2018, 3:38 PM

0 threat(s) detected so far

Drag'n Drop files here to scan by virus scanner

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

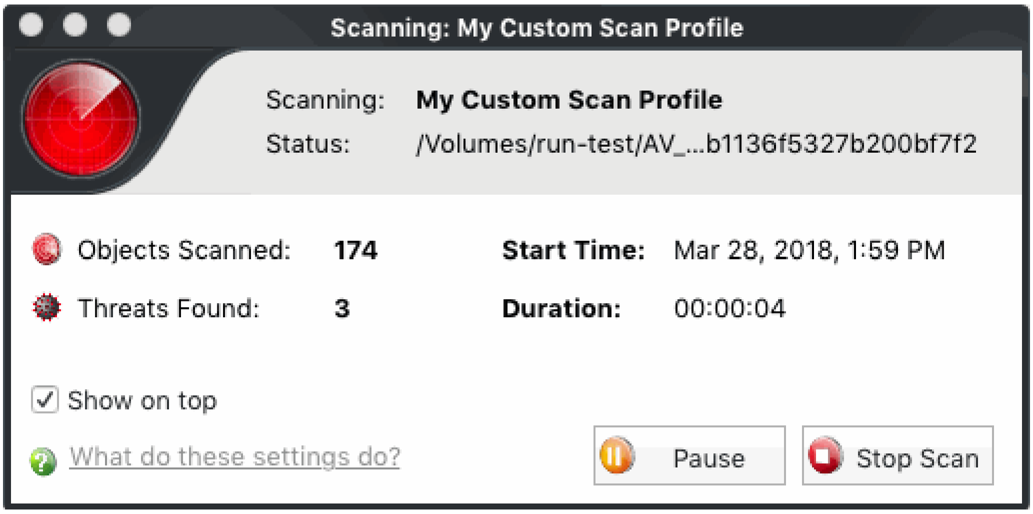


Virus Database Update (69%)

Please wait while the virus database is being updated.
This might take a few minutes...

Applying the updates...

Scanning will commence immediately after the updates are installed.



Scanning: My Custom Scan Profile

Scanning:	**My Custom Scan Profile**		
Status:	/Volumes/run-test/AV_...b1136f5327b200bf7f2		
Objects Scanned:	**174**	**Start Time:**	Mar 28, 2018, 1:59 PM
Threats Found:	**3**	**Duration:**	00:00:04

☑ Show on top

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

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

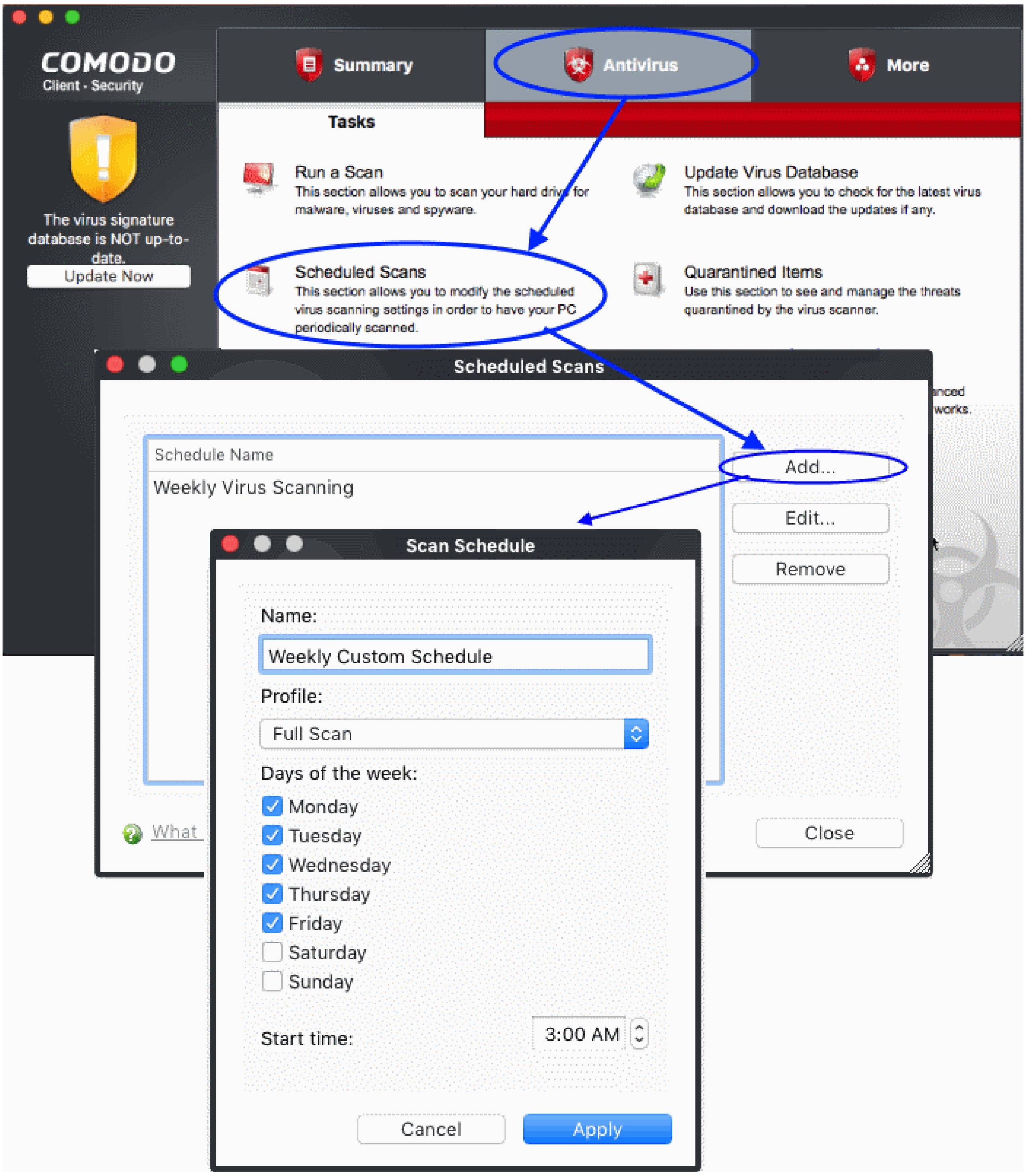
Create a Scheduled Scan

- The highly customizable scheduler lets you timetable virus scans to run when you decide.
- You can schedule a scan of your entire computer or specific areas. You can create an unlimited number of schedules.

- You can run scans at daily, weekly, monthly or custom intervals.
- Note: Managed endpoints - Scheduled scans should be configured in the Endpoint Manager profile.

Create an antivirus scan schedule

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



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scheduled Scans

Schedule Name
Weekly Virus Scanning

Scan Schedule

Name: Weekly Custom Schedule

Profile: Full Scan

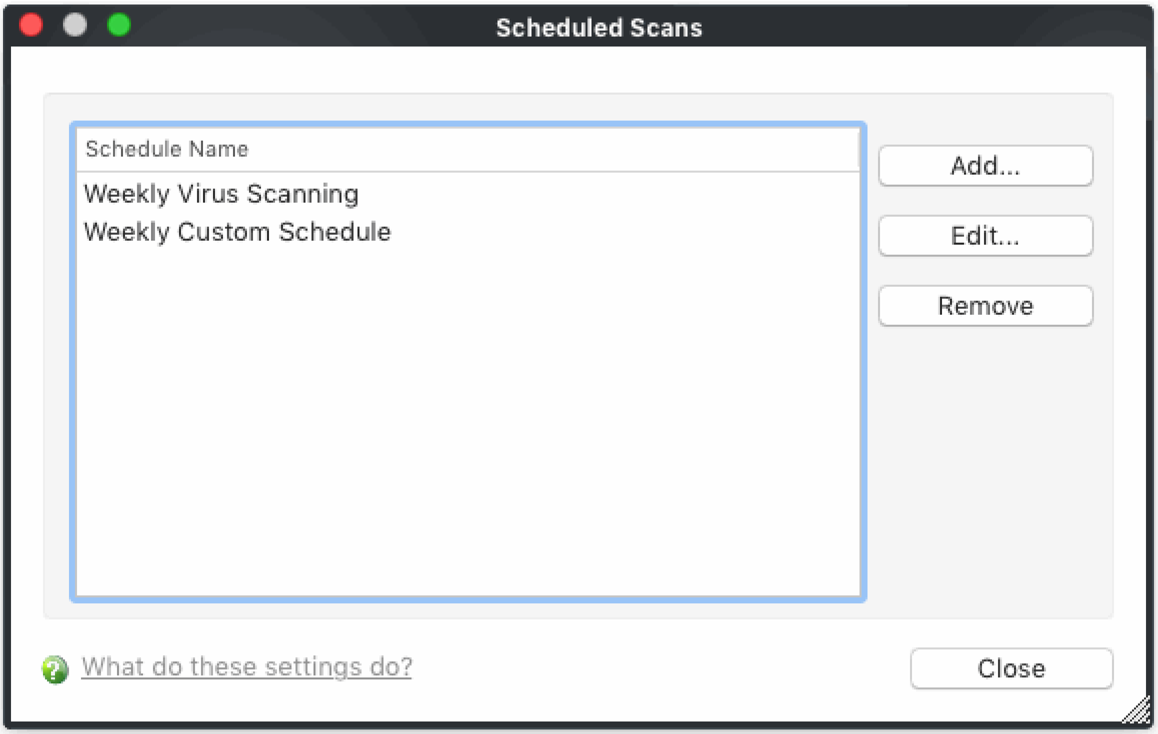
Days of the week:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday
□ Sunday

Start time: 3:00 AM

- **Name -** Enter a label for the new schedule. E.g. 'Daily scan of external devices'
- **Profile -** The profile determines which areas of your computer are scanned. 'Full Scan' and 'Quick Scan' are the default options. You can also create your own profile of specific targets.

  - See **Scan Profiles** for help to create a custom scan profile.
- **Days of the week** - Select the weekdays the scan should run.
- **Start time** - Select the time the scan should start on the specified weekdays
- Click 'Apply'.

The 'Scheduled Scans' interface lists all current schedules:



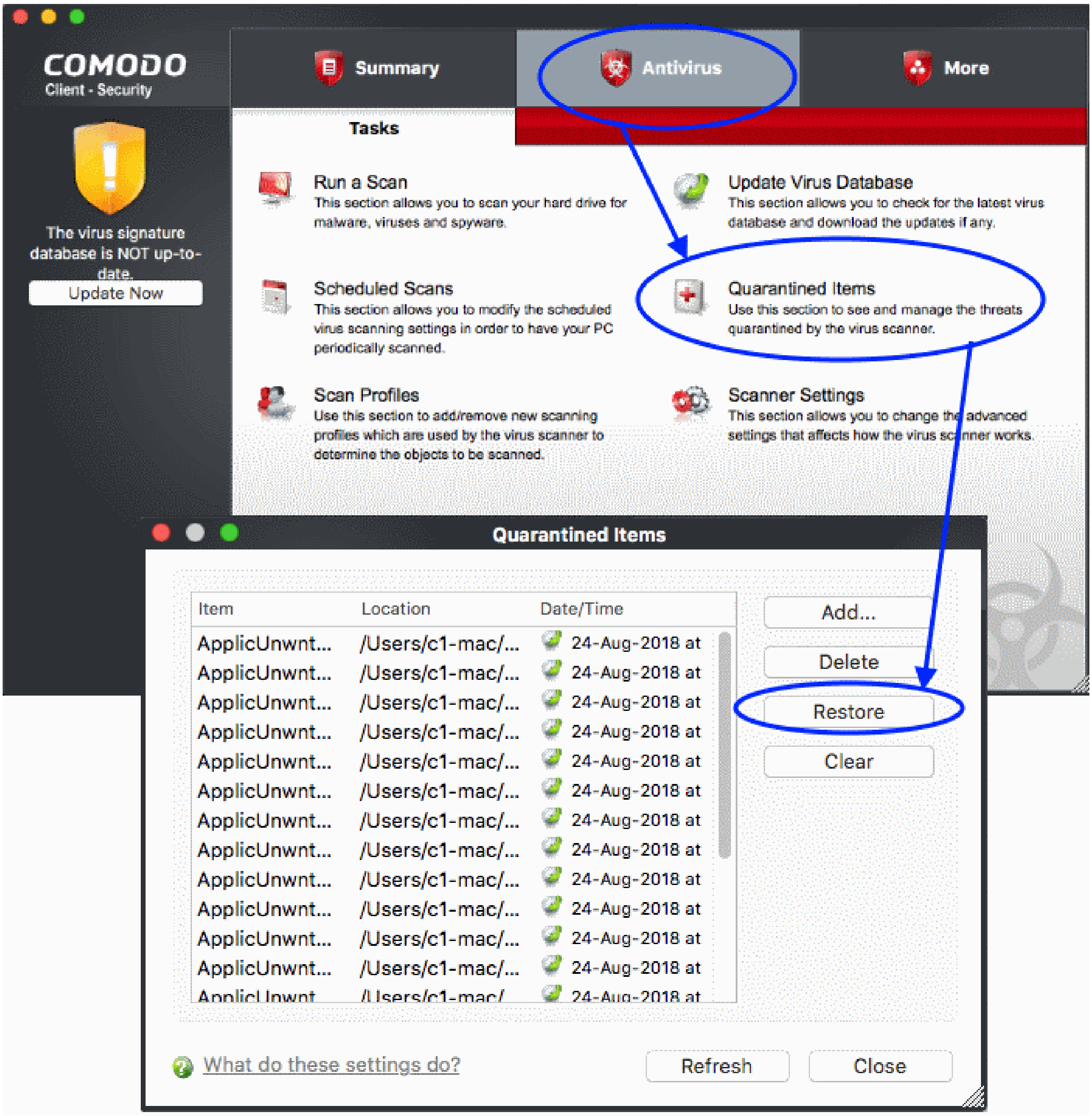
Weekly Virus Scanning
Weekly Custom Schedule

- Click 'Edit' to modify a profile. Click 'Remove' to delete a profile.
- For more details, see **Scheduled Scans**.

Restore Incorrectly Quarantined Items

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

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



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles
Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

Scanner Settings
This section allows you to change the advanced settings that affects how the virus scanner works.

Quarantined Items

Item	Location	Date/Time
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at
ApplicUnwnt...	/Users/c1-mac/...	24-Aug-2018 at

- Click 'Restore'

All selected files will be restored to their original locations immediately.

See **Quarantined Items** for more details.

Switch off Automatic Antivirus Updates

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

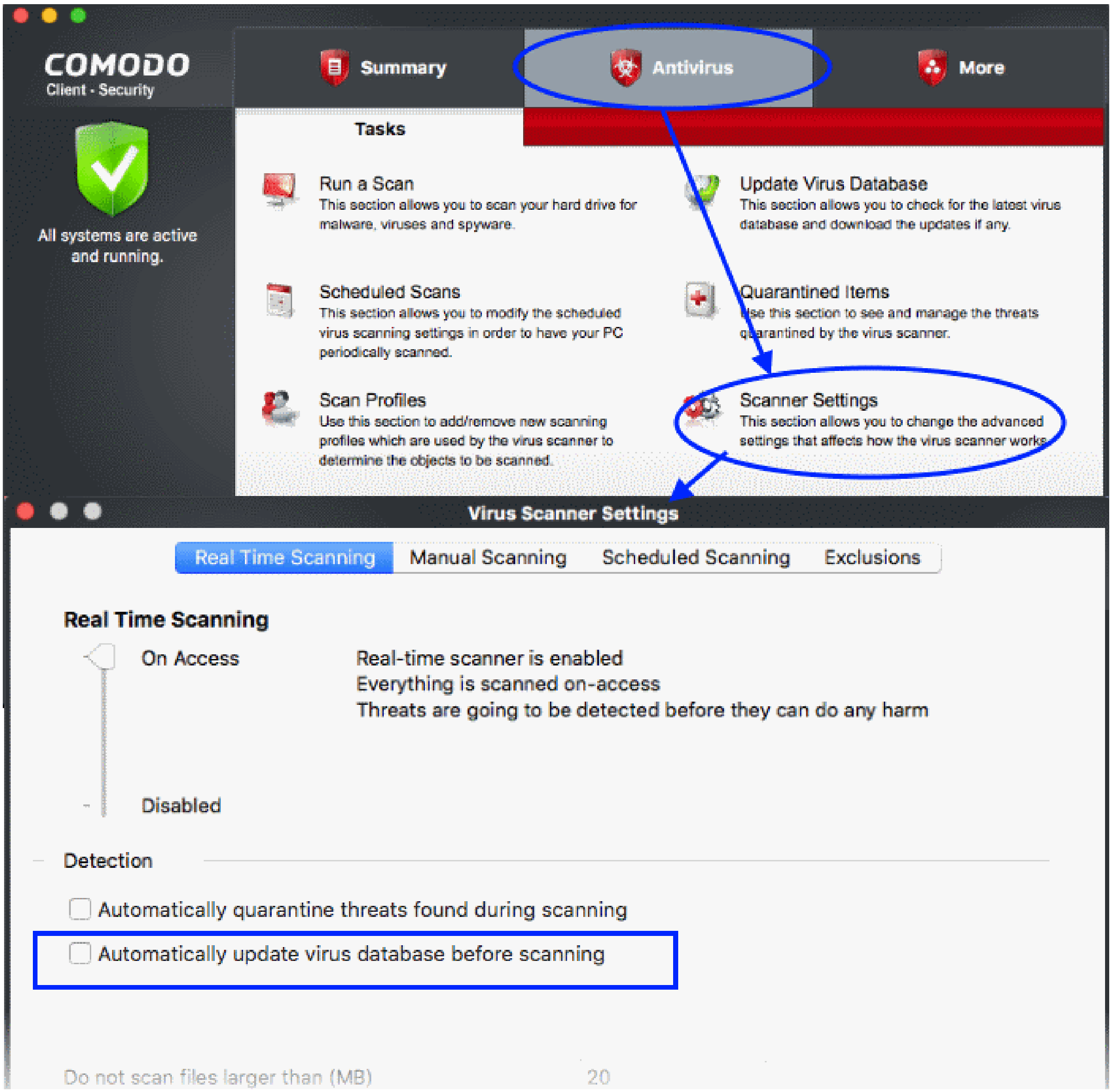
Automatic virus updates can be completely switched off, or can be switched off for individual scans.

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

Switch off automatic virus database updates

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



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles
Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

Scanner Settings
This section allows you to change the advanced settings that affects how the virus scanner works.

Real Time Scanning

On Access — Real-time scanner is enabled
Everything is scanned on-access
Threats are going to be detected before they can do any harm

Disabled

Detection

☐ Automatically quarantine threats found during scanning

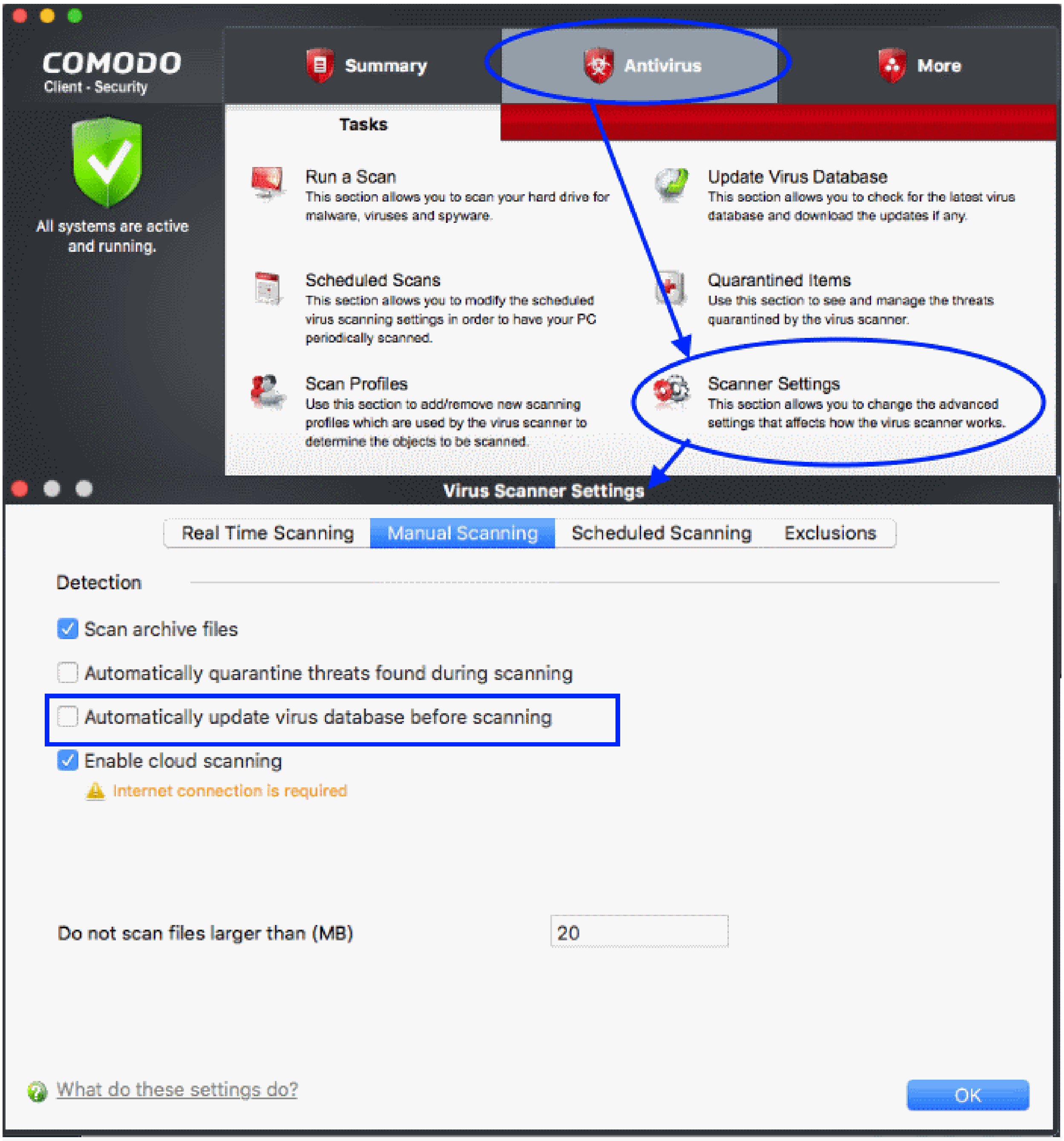
☐ Automatically update virus database before scanning

Do not scan files larger than (MB) 20

- Click 'OK'.

Switch off virus database updates prior to a Manual Scan

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



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles
Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

Scanner Settings
This section allows you to change the advanced settings that affects how the virus scanner works.

Virus Scanner Settings

Real Time Scanning | Manual Scanning | Scheduled Scanning | Exclusions

Detection

☑ Scan archive files

□ Automatically quarantine threats found during scanning

□ Automatically update virus database before scanning

☑ Enable cloud scanning

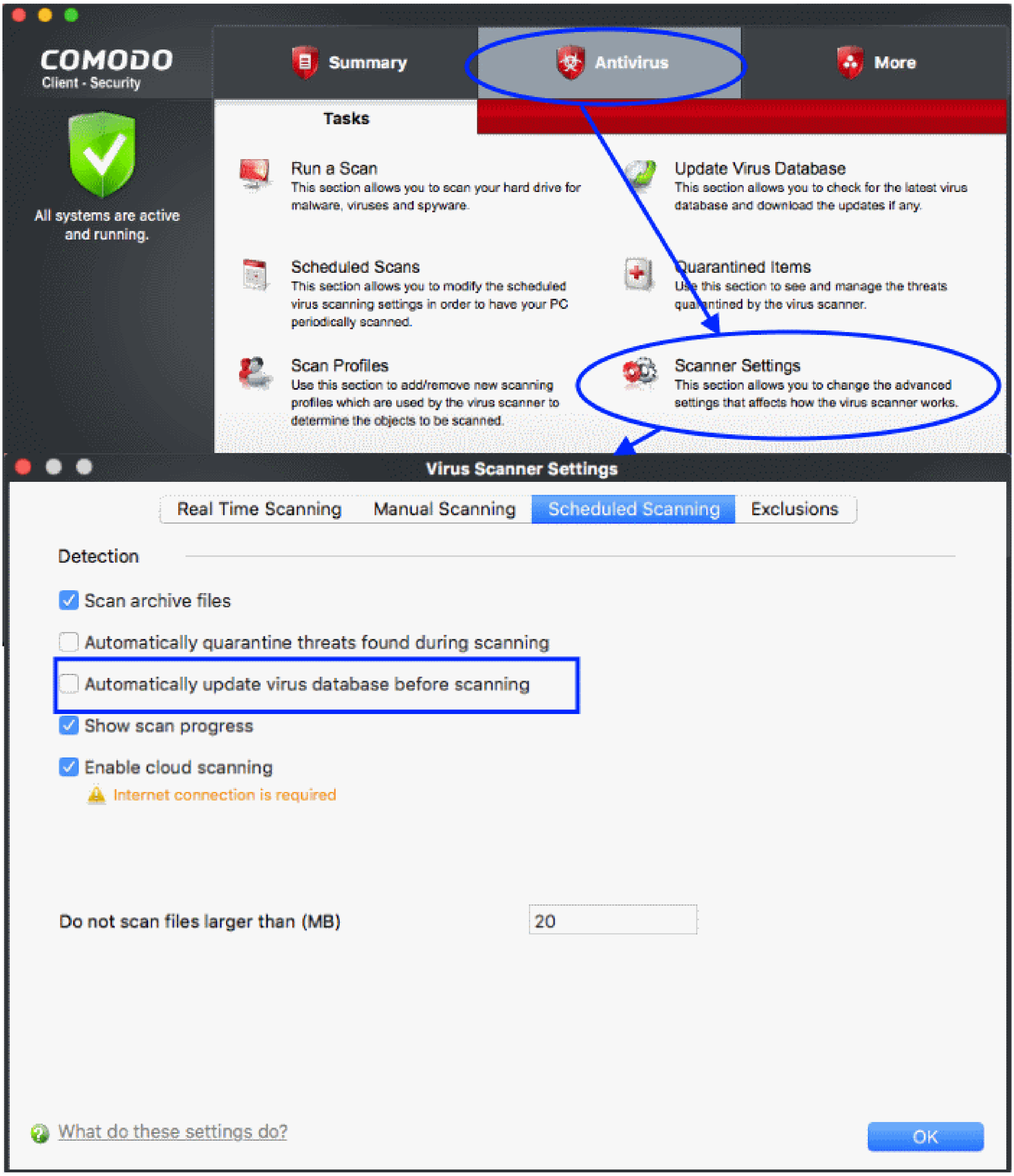
⚠ Internet connection is required

Do not scan files larger than (MB) 20

- Click 'OK'.

Disable updates prior to a scheduled scan

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



Run a Scan
This section allows you to scan your hard drive for malware, viruses and spyware.

Update Virus Database
This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans
This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items
Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles
Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

Scanner Settings
This section allows you to change the advanced settings that affects how the virus scanner works.

Virus Scanner Settings

Real Time Scanning | Manual Scanning | Scheduled Scanning | Exclusions

Detection

☑ Scan archive files

□ Automatically quarantine threats found during scanning

□ Automatically update virus database before scanning

☑ Show scan progress

☑ Enable cloud scanning

Internet connection is required

Do not scan files larger than (MB) 20

- Click 'OK'.

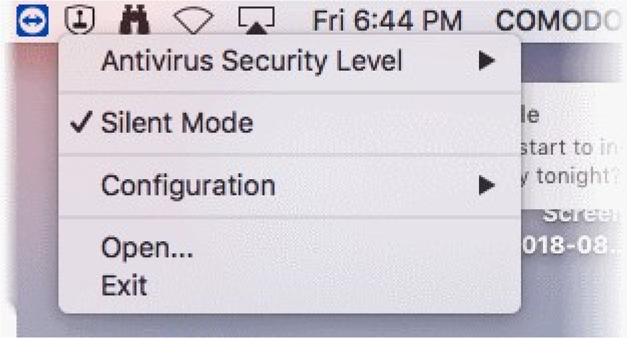
CCS will no longer automatically check for download database updates prior to running a scan.

Suppress Alerts with Silent mode

- Silent mode temporarily disables alerts so they don't interrupt you when playing a game or running a full screen presentation.
- Scheduled virus scans and database updates are also postponed until this mode is disabled.
- All protection components are 100% active in silent mode. Any threats are automatically blocked.

Enable silent mode

- Right-click on the CCS system tray icon.
- Select 'Silent Mode' from the options:



Deactivate 'Silent Mode' to resume alerts, updates and scheduled scans.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**