

Comodo Client - Security for MAC

Software Version 2.4

User Guide Guide Version 2.4.050820



Table of Contents

1. Introduction to Comodo Client - Security for MAC	4
1.1.System Requirements	6
1.2.Install Comodo Client - Security for MAC	6
1.3.Start CCS	15
1.4.Understand CCS Alerts	17
2. The Summary Screen	20
2.1.View Antivirus Events	
3. Antivirus Tasks – Introduction	23
3.1.Run a Scan	24
3.2.Update Virus Database	31
3.3.Quarantined Items	
3.4.Scanner Settings	
3.4.1.Real Time Scan	
3.4.2.Manual Scan	
3.4.3.Scheduled Scan	
3.4.4.Exclusions	
3.5.Scheduled Scans	41
3.6.Scan Profiles	44
4. More Options – Introduction	47
4.1.Preferences	47
4.1.1.Language Settings	
4.1.2.Log Settings	49
4.1.3.Update Settings	
4.2.Manage My Configurations	
4.2.1.Comodo Preset Configurations	54
4.2.2.Import / Export And Manage Personal Configurations	
4.3.Diagnostics	
4.4.Browse Support Forums	61
4.5.Help	61
4.6.About	61
4.7.View Logs	62
4.7.1.Antivirus Logs	63
4.7.1.1.Filter Antivirus Logs	65
4.7.2.'Alerts Displayed' Logs	
4.7.2.1.Filter 'Alerts Displayed' Logs	71
4.7.3.Tasks Launched Logs	76
4.7.3.1.Filter 'Tasks Launched' Logs	
4.7.4.Configuration Change Logs	83
4.7.4.1.Filter 'Configuration Change' Logs	85
Appendix 1 - CCS for Mac How To Tutorials	91
Scan your Computer for Viruses	91



View Antivirus Events	
Configure Database Updates	
Quickly Set up Security Levels	97
Change CCS Language Settings	
Run an Instant Antivirus Scan on Selected Items	
Create a Scheduled Scan	101
Restore Incorrectly Quarantined Items	102
Switch off Automatic Antivirus Updates	
Suppress Alerts with Silent mode	107

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

•••			
COMODO Client - Security	O Summary	🐯 Antivirus	ore 🔯
All systems are active and running.	Summary Antivirus Antivirus The virus database	On Access has been updated on May 6, 2020 ected so far	<u>at 6:13 PM</u> <u>Scan Now</u>
	Drag'r	b'Drop files here to scan by virus scar	nner



Guide Structure

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

- Introduction to Comodo Client Security
 - System Requirements
 - Install Comodo Client Security for Mac
 - Start CCS
 - Understand CCS Alerts
- The Summary Screen
 - View Antivirus Events
 - Antivirus Tasks Introduction
 - Run a Scan
 - Update Virus Database
 - Quarantined Items
 - Scanner Settings
 - Real Time Scan
 - Manual Scan
 - Scheduled Scan
 - Exclusions
 - Scheduled Scans
 - Scan Profiles
- More Options Introduction
 - Preferences
 - Language Settings
 - Log Settings
 - Update Settings
 - Manage My Configuration
 - Diagnostics
 - Browse Support Forums
 - Help
 - About
 - View Logs
- CCS How To... Tutorials
 - Scan your Computer for Viruses
 - View Antivirus Events
 - Configure Database Updates
 - Quickly Set up Security Levels
 - Change CCS Language Settings
 - Run an Instant Antivirus Scan on Selected Items
 - Create a Scheduled Scans
 - Restore Incorrectly Quarantined Item(s)
 - Switch off Automatic Antivirus Updates
 - Suppress Alerts with Silent mode



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.

CCS for MAC solution is compatible with the following hardware platform:

• Mac Intel x86_64

Operating systems:

- Mac OS X 10.11.x
- Mac OS X 10.12.x
- Mac OS X 10.13.x
- Mac OS X 10.14.x
- Mac OS X 10.15.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 ITarian platform.

This section covers how to:

- Subscribe for Endpoint Manager
- Enroll users
- Enroll devices

Subscribe for Endpoint Manager

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

- ITarian Sign up for ITarian at https://www.itarian.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.

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

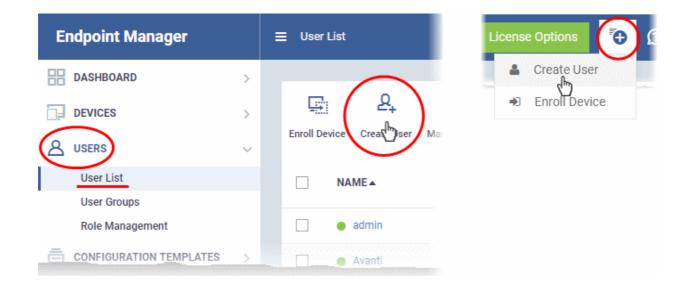
Add a user

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

or

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

Comodo Client - Security for MAC - User Guide



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.



Role

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

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

A confirmation message is shown:

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.	
	Ok

- Repeat the process to add more users.
- New users are added to the 'Users' interface (click '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://community.itarian.com/help/topic-459-1-1005-14819-Create-New-User-Accounts.html if you want to learn more about these options.

Enroll Devices

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

Enroll devices

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

Comodo Client - Security for MAC - User Guide

Endpoint Manager		≡ User List	License Options
DASHBOARD	>		🛓 Create User
DEVICES	>	E 2	Enpoll Device
A USERS	~	Enroll Revice Create User	_
User List		NAME ▼	
User Groups		\sim	
Role Management		Wile	
	>	ssgalia@yaha	

This starts step 1 of the device enrollment wizard:

Step 1 - Device Options

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

Enrollment Wizard		Supported Device Platforms Close
 Device options Enrollment Options Installation Summary Installation Instructions 	Average A	rer device rd to Specify User
	Next	



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

Step 2 - Enrollment Options

Enrollment Type

Applies to Windows, Mac and Linux devices.

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

Background. There are two types of client:

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

Enrollment Wizard			Supported Device Platforms	Enrollment Instruction	S Close
 Device options Enrollment Options 	Select Operating	System of TI	ne Device		
 Installation Summary Installation Instructions 	Windows	Linux	macOS	É 105	
	اللہ ا Android	Not Specified			
	Select Enrollmer		Il doesn't require.		
	Enroll and Protect Recommended	-O- Just Enroll			
	Select Method				

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

Option 1 - Enroll + Protect - Single Operating System

- Choose this if you want to deploy both communication and security clients
 - Click the Mac OS box. Please make sure all your target devices use this operating system.
 - The wizard will send enrollment mails which only contain download links for the Mac clients.
 - You can customize enrollment options as required. You can configure items such as enrollment type,



MDM profile and device name.

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

Option 2 - Enroll Only - Multiple Operating Systems

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

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

OR

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

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

Click 'Next' to proceed to step 3

Step 3 - Installation Summary

Review your choices so far.



Enrollment Wizard		Supported Device Platforms	Enrollment Instruction	Close
 Device options Enrollment Options Installation Summary Installation Instructions 	Device Information Concernent type Enroll and protect Concernent of the protect Concernent of the protect Concernent of the protect of t		Change Configuration	
	Back Ne:	xt		

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

Step 4 - Installation Instructions

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

Enrollment Wizard	Supported Device Platforms Enrollment Instruction Sec.	lose
 Device options Enrollment Options Installation Summary Installation Instructions 	Encliment Link to complete the user device enrollment, copy and send this link to user. Inters://herculespopular-msp.cmdm.comodo.com/enroll/device/by/token/2374247e59121941fc Cend To Email What's next? Enroll Another Device Control Contro	
	Back Finish	

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



3. Email Sent	
	Instruction email has been sent to selected user successful!
	Ok

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

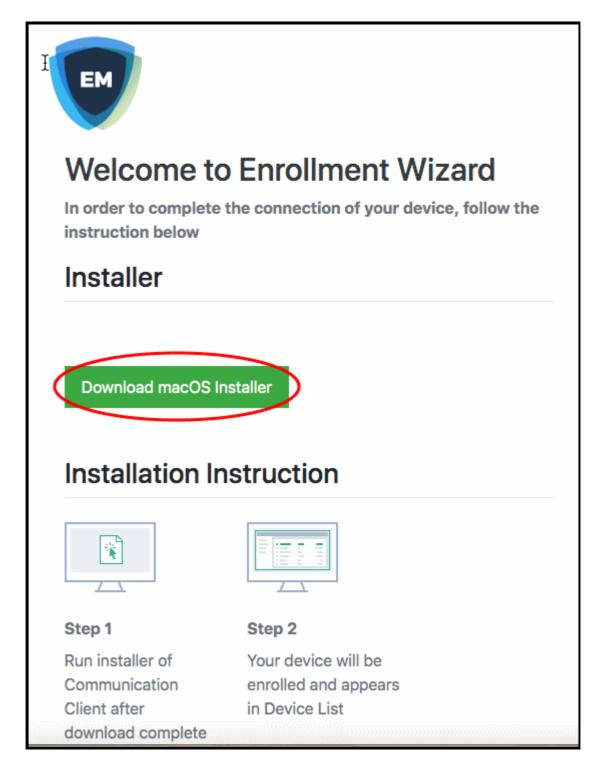
An example mail is shown below:

Dear Grey Pelican,	
Congratulations, your Endpoint Manager account has been successfully created. Please click the following link to activate your account and set up your password:	
<u>https://herculespopular-msp.cmdm.comodo.com/user/site/activate/username /Grey+Pelican/key/499cdc1039e5fd03080347b55a776adc658c5c77</u>	
Sincerely, Endpoint Manager team.	

The user experience is as follows:

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





- The EM client setup file gets downloaded.
- Run the setup file to install the client on the endpoint.
- The device is automatically added to Endpoint Manager once installation is complete. The EM communication client icon 💿 appears at the top-right of the endpoint screen.
- Protection is effective immediately after the computer restarts.

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

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



Manage Default Profiles for more details.

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

1.3. 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
All systems are active and running.	Summary Antivirus The virus database Otherwise	On Access has been updated on May 6, 202 ected so far	20 at 6:13 PM <u>Scan Now</u>
	Drag'r	n'Drop files here to scan by virus s	canner

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

- 17 P A 8 . 0 0 9 **V**² 0 🛂 🐟 🔗 🧭 🍤 📓 📃 🙉 📁 江 🎎 🛞 🍩 🤜 🤜 🤡 🎒 🔛 🐩 📖 🖷 🗑
- 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.



Answer 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.

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 Antivi	rus Alert		
	A malicious item has been detected!		
Name:	ApplicUnwnt@341617337		
Location:	/var/folders/1h/mmc_bgrx1xq4043cmwwkv		
More information:	ApplicUnwnt@341617337		
How should I answ			
	Clean Disiñfect Quarantine		

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: Location: More information:	ApplicUnwnt@341617337 /var/folders/1h/mmc_bgrx1xq4043cmwwkv ApplicUnwnt@341617337		
How should I answer	wer? Clean V S Ignore V Clean Disinfect Quarantine		

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 ans	wer? 🔞 Clean 🗸 😂 Ignore 🔸		
	Clean		
	Disinfact		
	Quarantine		

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

Ignore an alert to trust a file/application

• Click 'Ignore' at an alert.

	A malicious item has been detected!	
Name: Location: More information:	ApplicUnwnt@341617337 /var/folders/1h/mmc_bgrx1xq4043cmwwkv ApplicUnwnt@341617337	
How should I ans	wer? 🔞 Clean 👻 😋 Ignore 🙀	Once Add to Exclusions

- 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	B Summary	🐯 Antivirus	🤯 More
All systems are active and running.	Summary Antivirus The virus database In virus database	On Access has been updated on May 6, 202 ected so far	20 at 6:13 PM <u>Scan Now</u>
	Dragh	n'Drop files here to scan by virus s	canner

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.

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

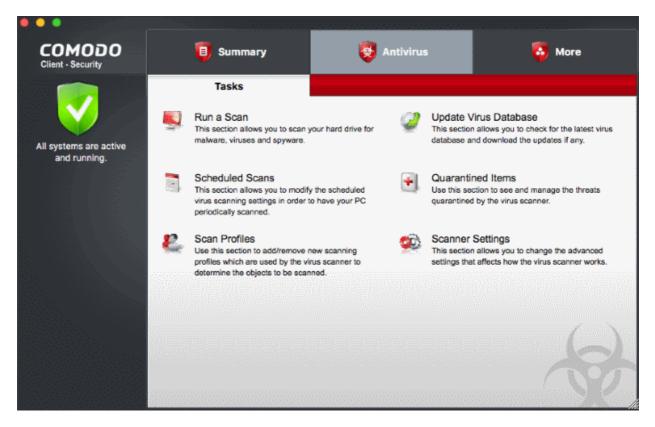
- Location The path of the malicious file
- Malware Name The label of the malicious file
- Action Indicates how CCS acted on the malware. Possible actions include 'Detect', 'Quarantine' and 'Ignore'
- Status Whether or not the action was successful
- Date The date and time of the event

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



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

Click 'Antivirus' > 'Run a Scan'

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

Run an on-demand virus scan

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

•••		Run a Scan		
Please select an ite	m to launch a scan:			
Profile Name				
Full Scan Quick Scan				
What do these sett	tings 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.

Scan progress and results

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



The scan 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.



•••	Scann	ning: Full Scan	
	Scanning: Full Scan Status: /usr/sbin/chat		
Objects ScaThreats Fou	anned: 3,632 und: 0	Start Time: Duration:	May 6, 2020 at 3:57 PM 0:00:18
🗹 Show on top)		
😵 <u>What do the</u>	ese settings do?	0	Pause 🛈 Stop Scan

- 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:

V All?	Threat Name	Risk	
	Malware@(#rdevwovjljgq, #18f95or7g3buz)	High	
\checkmark	/Users/tester/Documents/test_set/testset_all_virus/2ea03		
\checkmark	/Users/tester/Documents/test_set/testset_all_virus/VirusS		
	Exploit.JS.Pdfka.hs@#283139321	High	STATE OF THE OWNER
\checkmark	/Users/tester/Documents/test_set/testset_all_virus/4b5cd		
	Suspicious@#655qru3s3fnb	High	
\checkmark	/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'.

Comodo Client - Security for MAC - User Guide



	Save		
Save As:	scan results_032818.txt		~
Tags:			
Where:	🔲 Desktop	\$	
		Cancel	Save

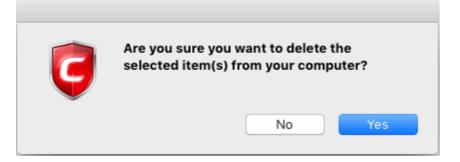
Remove selected items

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

	Threat Name Factor Content of the second state of the second stat	Risk High	
	Exploit.JS.Agent.va@#300070235	High	
		5	
	/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 🛛 👘	100
\square	///olumes/run_test/AV_Engine/Smart/Samples///irusShare.1d		_

• Click 'Yes' in the confirmation dialog box:





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'.

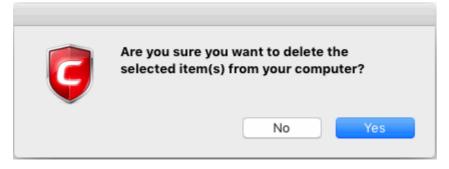
Ç	Are you sure you want to quarantine the selected items?
	No Yes

• 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'.



• 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



🗸 All?	Threat Name	Risk	[
	Malware@(#rdevwovjljgq, #18f95or7g3buz)	High	1
1	/Users/tester/Documents/test_set/testset_all_virus/2ea03		
/	/Users/tester/Documents/test_set/testset_all_virus/VirusS		
	Texploit.JS.Pdfka.hs@#283139321	High	
1	/Users/tester/Documents/test_set/testset_all_virus/4b5cd		
	▼ Suspicious@#655qru3s3fnb	High	
1	/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 rerun 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	
Pl	lease select an item to launch a scan:	
P	Profile Name	
	Full Scan Quick Scan	
L ⊗ ⊻	What do these settings do? Create New Scan Scan Close	

'Add New Profile' dialog opens:

		ist of items:
		Path
Remove	Add	

- 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'.

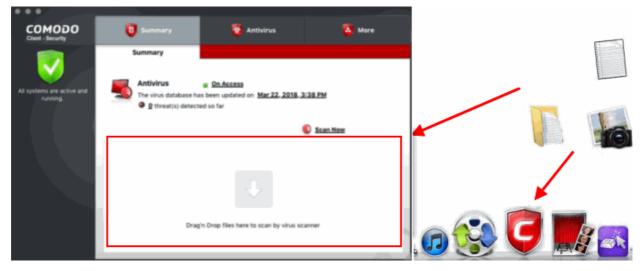


•	🔍 🔍 Run a Scan	
	Please select an item to launch a scan:	
	Profile Name	
	Full Scan	
	Quick Scan	
	My Custom Scans	
0	What do these settings do? Create New Scan Scan Close	

- 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.



3.2. Update Virus Database

Click 'Antivirus' > '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



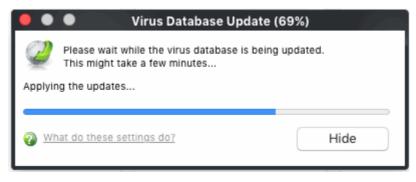
Download updates automatically

Manually check for the latest virus database

- 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:



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

••	Done.	
<i>Q</i>	The virus signature database is up-to-date.	
<u>wi</u>	at do these settings do?	Close

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

Click the 'Antivirus' tab > 'Quarantined Items'



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

The quarantine interface lets you:

- 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'

ltem	Location ^	Date/Time	Add
Contractor and the second second	/Users/comodo/ /Users/comodo/	05-May-2020 at 05-May-2020 at	Delete
-	/Users/comodo/ /Users/comodo/	05-May-2020 at 05-May-2020 at	Restore
	/Users/comodo/	@ 05-May-2020 at	Clear

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

Manually add files to quarantine

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

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

Delete a quarantined item from the system

Open Comodo Client Security



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

This deletes the file from your computer permanently.

Restore a quarantined item to its original location

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

Item	Location ^	Date/Time	Add
	/Users/comodo/ /Users/comodo/	05-May-2020 at 05-May-2020 at	Delete
	/Users/comodo/	@ 05-May-2020 at	Restore
-	/Users/comodo/ /Users/comodo/	© 05-May-2020 at © 05-May-2020 at	Clear
0	Add the file to t is always skipp	he exclusions list, so th	at it

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

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

Delete all quarantined items

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

This deletes all the quarantined items from the system permanently.

3.4. Scanner Settings

Click the 'Antivirus' tab > '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'

••	Vir	us Scanner	r Settings		
Real Time So	canning Manual S	canning	Scheduled Scanning	Exclusions	
Real Time Scanning					
On Access	Real-time scan Everything is so Threats are goi	canned on-		do any harm	
Disabled					
Detection					
Automatically quarantin	e threats found duri	ng scannin	g		
🗹 Automatically update vi	rus database before	scanning			
🗹 Enable realtime scannin	g of files on network	c			
Do not scan files larger tha	an (MB)	4	20		
Keep an alert on the scree	n for (seconds)	1	120		
What do these settings do	?				Close

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

Click 'Antivirus' > 'Scanner Settings'

- 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 S	canner Settings		
Real Time S	canning Manual Scan	ning Scheduled Scanning	g Exclusions	
Real Time Scanning				
On Access	Real-time scanner Everything is scann Threats are going t		an do any harm	
- Disabled				
Detection				
Automatically quarantin	ne threats found during s	canning		
🗹 Automatically update vi	irus database before sca	nning		
Enable realtime scannir	ng of files on network			
Do not scan files larger tha	an (MB)	20		
Keep an alert on the scree	n for (seconds)	120		
What do these settings do	?			Close

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 When enabled, all detected threats will be moved to quarantine. Once quarantined, the detected threat can be restored or deleted at your wish. 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.
 - 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 (Default).
- 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

Click 'Antivirus' > 'Scanner Settings'

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':

•		Virus Scanne	er Settings	
	Real Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions
Detection				
Scan ard	chive files			
🗹 Automa	tically quarantine threats	found during scanni	ng	
🗹 Automat	tically update virus datab	base before scanning	J	
	cloud scanning net connection is required			
Do not scar	n files larger than (MB)		20	
What do th	ese settings do?			Close

- 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

Click 'Antivirus' > 'Scanner Settings'

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':

Real Time Scanning M	anual Scanning	Scheduled Scanning	Exclusions
Detection			
C Scan archive files			
🗹 Automatically quarantine threats for	und during scannin	ng	
🗹 Automatically update virus database	e before scanning		
🗹 Show scan progress			
Enable cloud scanning Internet connection is required			
Do not scan files larger than (MB)	[20	
What do these settings do?			Clos

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

Click 'Antivirus' > 'Scanner Settings'

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.

Set the exclusions scanning level

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

	Real Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions	· · · · · · · · · · · · · · · · · · ·
Exclusions					Add +
/Library/Ap	plication Support/COMC	DO/CCS/*			
	ns/COMODO/CCS/*				Edit
/Applicatio	ns/COMODO Client - Se	curity.app/*		· · · ·	Demonster
					Remove
	ese settings do?				

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.



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	
Browse Running Processes	•

(Real Time Scanning	Manual Coopeing			
		Manual Scanning	Scheduled Scanning	Exclusions	
Exclusions				Add	Browse Files
/Library/Application Support/COMODO/CCS/* /Applications/COMODO Client - Security.app/*		Edit	Browse Running Processes		
				Remove	•

• **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.

🗉 < > 🔡 🗾 🧖 App	lications	Q Search
lame	Date Modified	Size
App Store	14-Nov-2019 at 10:4	6 AM 1.5 MB
Automator	14-Nov-2019 at 10:4	6 AM 8.5 MB
Calculator	07-Oct-2017 at 11:17	7 AM 5.7 MB
D Calendar	14-Nov-2019 at 10:4	6 AM 20.8 MB
Chess	14-Nov-2019 at 10:4	6 AM 7.9 ME
G COMODO Client - Security	04-Jul-2019 at 2:23	AM 76.1 ME
B Contacts	14-Nov-2019 at 10:4	6 AM 19.9 ME
B Dashboard	19-Oct-2017 at 9:00	AM 568 KE
Dictionary	14-Nov-2019 at 10:4	6 AM 2.9 ME
DVD Player	12-Oct-2017 at 7:41	AM 23.9 ME
Endpoint Manager Communication Client	29-Apr-2020 at 5:54	1 PM 86.9 ME
FaceTime	14-Nov-2019 at 10:4	6 AM 8.3 ME
Font Book	05-Feb-2018 at 1:46	AM 12.9 ME
🖻 🌍 Google Chrome	25-Apr-2020 at 6:18	AM 454.4 ME
 iBooks 	14-Nov-2019 at 10:4	6 AM 50.1 ME
Image Capture	13-Dec-2017 at 11:55	9 AM 2.3 ME
*····	85 5 1 8648 1 3 64	
		Cancel Open

• **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.

	and the second second		COMODO Client - Security
Real Time Scanning Manual Scanning Scheduled Scanning Excl	usiona		CVMServer
Exclusions	Add +	Browse Files	CloudKeychainProxy
/Library/Application Support/COMODO/CCS/*	Add +	Browse Running Processes	CommCenter
/Applications/COMODO Client - Security.app/*	Edit		ComodoAgent
Maharana comoso anni - occardappi	Con		ContactsAccountsService
	Remove		CoreLocationAgent
			CrashReporterSupportHelper DiskUnmountWatcher
			Diskunmountwatcher
			Endpoint Manager Communication
			Endpoint Manager Communication Finder
			Google Chrome
			IMAutomaticHistoryDeletionAgent
			IMRemoteURLConnectionAgent
			IMRemoteURLConnectionAgent
			Invite of the contraction of gent
			KernelEventAnent
			KernelEventAgent KeychalnSvocingOverIDSProvy
			KeychainSyncingOverIDSProxy
			KeychainSyncingOverIDSProxy LaterAgent
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NotificationCenter
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NotificationCenter ProtectedCloudKeySyncing
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NotificationCenter ProtectedCloudKeySyncing RHost
			KeychainSyncingOverIDSProxy LaterAgent MTLComplerService NotificationCenter ProtectedCloudKeySyncing RHost SSMenuAgent
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NotificationCenter ProtectedCloudKeySyncing RHost
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NotificationCenter ProtectedCloudKeySyncing RHost SSMenuAgent Script Editor SocialPushAgent
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NatificationCenter ProtectedCloudKeySyncing RHost SSMenuAgent Script Editor
			KeychainSyncingOverIDSProxy LaterAgent MTLCompilerService NatificationCenter ProtectedCloudKeySyncing RHost SSMenuAgent Script Editor SocialPushAgent Spotlight SubmitDiaginfo
			KeychainSynclingOverIDSProxy LaterAgent MTLComplierService NotificationCenter ProtectedCloudKeySyncling RHost SSMenuAgent Soript Editor SocialPushAgent Spotlight

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

Click 'Close'

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	
	/Users/comodo/Downloads/Xco	de_10.3.xip	
0	What do these settings do?	Cancel	Apply

• Click 'Apply'.

3.5. Scheduled Scans

Click 'Antivirus' > 'Scheduled Scans'

- The highly customizable scheduler lets you timetable virus scans according to your preference.
- You can schedule a scan of your entire computer or specific areas. You can create an unlimited number of schedules.
- You can run scans at daily, weekly, monthly or custom intervals.
- 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:

Scheduled Scans	
Schedule Name Weekly Virus Scanning	Add Edit Remove
What do these settings do?	Close

Configure your schedule in the following settings screen:



Scan Sche	dule 🧳
Name:	
Profile:	
Full Scan	0
Days of the week:	
🗹 Monday	
🗹 Tuesday	
🗹 Wednesday	
🗹 Thursday	
🗹 Friday	
Saturday	
🗹 Sunday	
Start time:	12:00 AM 🗘
	0
Cancel	Apply

- 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'.

Schedule Name	Add
Neekly Virus Scanning Daily scan of external devices	Edit
Weekly Custom Schedule	Remove



• 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

Click the 'Antivirus' tab > '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'

•	🛢 😑 Scan Profiles	
	Profile Name Full Scan Quick Scan	Add Edit Remove
0	What do these settings do?	Close

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

Create a new scan profile

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

	Add New Profile
Name:	
List of items:	
Path	
	Add Remove
	Add
	Add

Name - Enter a label for the scan profile.

•

• Click 'Add' to select the items you wish to include in the scan.



My Custom Scans	
list of items:	
Path	
/Users/tester/Documents/test_se	

- 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:

Full Scan		
Quick Scan		
My Custom Scans		

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

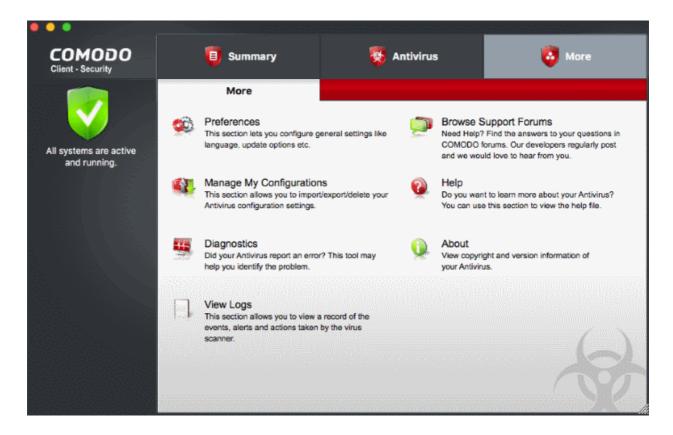
Remove a custom scan profile

• 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

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



The 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.



• • •		Preferences	5	
	Language	Logging	Update	
Select Language	Default - English (United	States) ᅌ		
What do these set	tings do?			 Close

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.

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

The settings screen will open:



•	•		Preferences	
		Language	Logging Update	
	Select Language	Default - English (United	States) ᅌ	
2	What do these set	tings do?		

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:



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	
Keep on updating it removing the oldest records	
Move it to <u>the specified folder</u> and start a new one	
	1
What do these settings do? Close	e

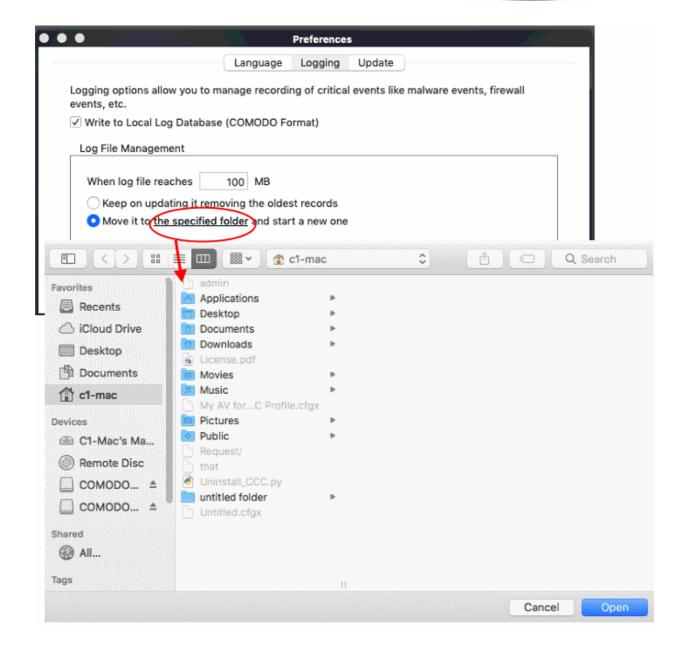
General Log File Options

• 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).
 - Keep on updating it removing the oldest records 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*).





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



Preferences
Language Logging Update
Logging options allow you to manage recording of critical events like malware events, firewall
events, etc. Vrite to Local Log Database (COMODO Format)
Log File Management
When log file reaches 100 MB
Keep on updating it removing the oldest records
Move it to Users/comodo/Documents and start a new one
What do these settings do? Close

• Click 'Close'.

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.

Access the updates settings

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

The settings screen opens:



•	Preferences	
	Language Logging Update	
🗸 Enable	Host	Add
	http://download.comodo.com/	Remove
		Move Up
		Move Down
	e settings do?	

- 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

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

Click 'More' > '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

- 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

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

My Configurations	Active	Activate
Comodo Client - Security	Active	Remove
		Import
		Export
		Restore Defaults
What do these settings do?		Close

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



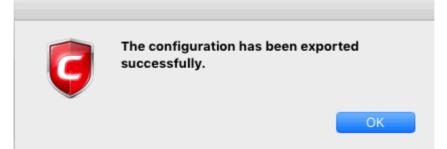
• Reset to a default profile

Export stored configuration to a file

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

$\mathbf{P} \bullet$	Configurations	
My Configurations	Active	Activate
Comodo Client - Security	Active	
		Remove
		Import
	Save	Export
Save As: Custom CCS Mac	Profile - Exported.cfg	Restore Defaults
Tags:		
Where: Desktop	٥	
W		Close
	Cancel Save	

A confirmation dialog will appear if the export is successful:



Import a saved configuration from a file

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

To import a configuration file:

- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Click 'Import'
- Browse to the location of the saved profile and click 'Open'.

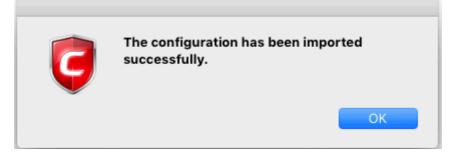


	■ Ⅲ 	ester	\$	▲
Favorites iCloud Drive A Applications tester Devices ElCapitan Shared	Custom CCSProfi Desktop Documents Downloads Movies Music Pictures Public	le.cfgx	Created Modified	S for Mac Profile.cfgx Document - 5 KB Today, 12:25 PM Today, 12:25 PM Today, 12:25 PM Add Tags
				Cancel Open

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

•	Import As	
	Enter a name for this configuration:	
	Custom CCS for Mac Profile	
	Cancel	ок

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



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



My Configurations	Active	Activate
Custom CCS for Mac Profile		
Comodo Client - Security	Active	Remove
		Import
		Export
		Restore Defaults

Select and implement a different configuration profile

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

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

	Configurations	
My Configurations	Active	Activate
Custom CCS for Mac Profile	Active	
Comodo Client - Security		Remove
		Import
The configur	Export	
successfully		Restore Defaults
	ОК	
What do these settings do?		Close

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



	Configurations	
My Configurations	Active	Activate
Custom CCS for Mac Profile Comodo Client - Security	Active	Remove Import Export Restore Defaults
What do these settings do?		Close

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.

Remove an unwanted profile

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

My Configurations	Active	Activate
Custom CCS for Mac Profile		
Comodo Client - Security	Active	Remove
	×	Import
Are you sure to a configuration pe	Export	
	Restore Defaults	
	No Yes	

• The profile will be removed from your computer:





Reset to a default profile

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

A confirmation dialog will appear:

	Configurations
9	All the configurations will be reverted to the default. This action cannot be undone. Would you like to proceed?
	Yes No

Click 'Yes'.

4.3. Diagnostics

Click the 'More' tab > '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.

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 w integrity of the installation.	erifying the
_		Abort
Che	cking files	

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

.

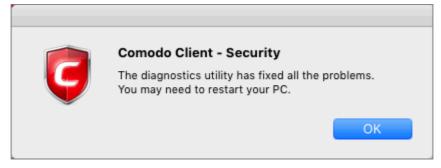




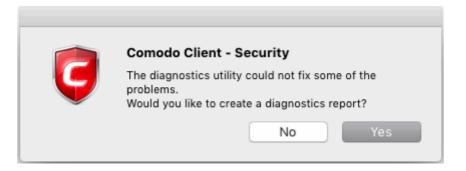
If the utility finds errors you will be prompted to fix them:



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



- Restart your computer for the changes to take effect.
- If the utility could not fix the problems, it will prompt you to create a diagnostics report:





4.4. Browse Support Forums

- Click the 'More' tab > 'Browse Support Forum'
- You can post questions and suggestions about CCS in our community forum
- You also can send 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
- Visit https://forum.itarian.com/ for the ITarian forum
- · 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.

4.5.Help

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

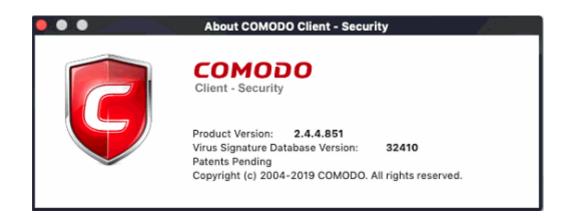
- Open Comodo Client Security
- Click the 'More' tab
- Click 'Help'

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.

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





4.7. View Logs

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

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

		Log Vie	ewer			
Today 📰 Currer	nt Week 🛅 Cu	urrent Month	Entire Period			
Logs per Module Antivirus Events	Action	C) (Equal C)	Quarantine	Remove	C Ignore	•
• Other Logs	Antivirus Events					
Alerts Displayed	Date	Location	Malware Name	Action	Status	Scan UID
Tasks Launched	Apr 26, 2019	/Users/comod	Appliel Inwrit	Quarantine	Success	D76500
Configuration Changes	Apr 26, 2019	/Users/comod		Quarantine	Success	60A1F4
	Apr 26, 2019		Malware@#27	a construction	Success	60A1F4
	Apr 26, 2019	/Users/comod		Quarantine	Success	60A1F4
	Apr 26, 2019	/Users/comod		Quarantine	Success	60A1F4
	Apr 26, 2019		Malware@#27	exercise and the second second second	Success	60A1F4
	Apr 26, 2019	/Users/comod		Quarantine	Success	60A1F4
	Apr 26, 2019		Malware@#27	Quarantine	Success	2832E3
	Apr 26, 2019	/Users/comod		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	AA6E3
May 2019 4 • •	Apr 26, 2019	/Users/comod	Malware@#27	Detect	Success	AA6E3
Su Mo Tu We Th Fr Sa	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3
28 29 30 1 2 3 4	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3
5 6 7 8 9 10 11	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3
12 13 14 15 16 17 18 19 20 21 22 23 24 25	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3
26 27 28 29 30 31	Apr 29, 2019	/Users/comod	Malware@#27	Ignore	Success	6F4976
2 3 4 5 6 7 8	Apr 29, 2019	/Users/comod	ApplicUnwnt	Ignore	Success	6F4976
2 0 . 0 0 1 0	Apr 29, 2019	/Users/comod	Malware@#27	Ignore	Success	6F4976

- 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.

Logs per Module Antivirus Events	Action	C Equal C	Quarantine	Remove	GIgnore	•
Other Logs	Antivirus Event	S				
Alerts Displayed	Date	Location	Malware Name	Action	Status	Scan UID
Tasks Launched	Apr 26, 2019	/Users/comod	ApplicUnwnt	Quarantine	Success	D76500
Configuration Changes	Apr 26, 2019			Quarantine	Success	60A1F4
	Apr 26, 2019		Malware@#27		Success	60A1F4
	Apr 26, 2019	·····		Quarantine	Success	60A1F4
	Apr 26, 2019			Quarantine	Success	60A1F4
	Apr 26, 2019	ana fanana na Mirana a sa sa sa	Malware@#27	Quarantine	Success	60A1F4
	Apr 26, 2019			Quarantine	Success	60A1F4
	Apr 26, 2019		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	AA6E3
May 2019 4 • •	Apr 26, 2019	/Users/comod	Malware@#27	Detect	Success	AA6E3
Su Mo Tu We Th Fr Sa	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3
28 29 30 1 2 3 4	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3
5 6 7 8 9 10 11	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3
12 13 14 15 16 17 18	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3
19 20 21 22 23 24 25 26 27 28 29 30 31	Apr 29, 2019	/Users/comod	Malware@#27	Ignore	Success	6F4976
202/28293031	Apr 29, 2019	/Users/comod	ApplicUnwnt	Ignore	Success	6F4976
2 3 4 3 0 7 0	Apr 29, 2019	/Users/comod	Malware@#27	Ignore	Success	6F4976

- 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:

Location	ו:
/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:

/Users/tester/ ApplicUnwnt	Detect	
/Users/tester/ ApplicUnwnt	Detect	Succ
/Users/tes Refresh	Detect	Succ
/Users/tes	Detect	Succ
/Users/tes ✓ Advanced Filter	Detect	Succ
/Users/tes Export	Detect	Succ
/Users/testory	Detect	Succ
/Users/tester/ ApplicUnwnt	Detect	Succ
/Users/tester/ ApplicUnsaf@	Detect	

- 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 Comodo Client Security
- 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.

Today 📑 Currer	ent Week 📰 Current Month				
 Logs per Module Antivirus Events Other Logs 	Action Action Status Location Malware Name	Equal 0			
Alerts Displayed	Date	Location	Mai		
Tasks Launched Configuration Changes	Apr 26, 2019	/Users/comod	Ap		
configuration changes	Apr 26, 2019	/Users/comod			
	Apr 26, 2019				

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.



" Logs per Module	Action	🗸 Equal 🔥	Quarantine	Remove	lgnore	Detect	Ask	Restore	6
Antivirus Events		Not Equal							1.0000
Vother Logs	Antivirus Events	· moster constrained		1.4					
Alerts Displayed	Date	Location	Malware Name	Action	Status	Scan UID	Alert		
Tasks Launched	Apr 26, 2019	/Users/comod	ApplicUnwnt	Quarantine	Success	D7650D68			
Configuration Changes	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	AA6E3850	-4		
	Apr 26, 2019	/Users/comod	Malware@#27	Detect	Success	AA6E3B50	-4		
	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3850	-4		
May 2019 4 . >	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3850	-4		
SulMo Tu We Th Fr Sa	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3B50	-4		
28 29 30 1 2 3 4	Apr 26, 2019	/Users/comod	Malware@#2	Detect	Success	AA6E3850	-4		
5 6 7 8 9 10 11	Apr 29, 2019	/Users/comod	Malware@#27	Ignore	Success	6F4976BB-	-D		
12 13 14 15 16 17 18	Apr 29, 2019		ApplicUnwnt	Ignore	Success	6F4976BB	-D		
19 20 21 22 23 24 25	Apr 29, 2019		Malware@#27		Success	6F4976BB-	-D		
26 27 28 29 30 31 1	Apr 29, 2019		ApplicUnwnt	Ignore	Success	6F4976BB-			
2345578	Apr 29, 2019		Malware@#2	Ignore	Success	6F4976BB			
	Apr 29, 2019		Malware@#2	Ignore	Success	6F4976BB-			
	1 00 0010	http://www.woonlogin	A Palanti	- And	0	00000000			

- 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 guarantine
 - 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.



Logs per Module	Status	0 Equal 0	Success	Failure			(+
Antivirus Events							
Vother Logs Alerts Displayed	Antivirus Events		A de la compañía de la	i di meta m	and the	in the state	
Tasks Launched	Date	Location	Malware Name	Action	Status	Scan UID Alert	
	Apr 26, 2019		ApplicUnwnt	Quarantine	Success	D7650D68-9	
Configuration Changes	Apr 26, 2019		. ApplicUnwnt	Quarantine	Success	60A1F4B0-E0	
	Apr 26, 2019		. 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	
May 2019 4 • •	Apr 26, 2019	/Users/comod	ApplicUnwnt	Detect	Success	AA6E3B50-4	
SulMo Tu We Th Fr Sa	Apr 26, 2019		Malware@#2	Detect	Success	AA6E3B50-4	
28 29 30 1 2 3 4	Apr 26, 2019		Malware@#2	Detect	Success	AA6E3B50-4	
5 6 7 8 9 10 11	Apr 29, 2019	and the second se	Malware@#27		Success	6F4976BB-D	
12 13 14 15 16 17 18	Apr 29, 2019		ApplicUnwnt	Ignore	Success	6F4976BB-D	
19 20 21 22 23 24 25	Apr 29, 2019		Malware@#27		Success	6F4976BB-D	
26 27 28 29 30 31 1	Apr 29, 2019		ApplicUnwnt	Ignore	Success	6F4976BB-D	
2345678	Apr 29, 2019		Malware@#2	Ignore	Success	6F4976BB-D	
	Apr 29, 2019		Malware@#2	Ignore	Success	6F4976BB-D	
	1 00 0010	hi i i	A 11 11	- Strong	0	00000000	

- 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:



* Logs per Module Antivirus Events	Location C)	Contains	/Users/					
T Other Logs	Antivirus Events	ano ha subar						
Alerts Displayed	1153	cation	Malware Name	Action	Status	Scan UID	Alert	
Tasks Launched	1884		ApplicUnwnt	Quarantine	Success	D7650D68-9		
Configuration Changes	21(1)		ApplicUnwrit	Quarantine	Success	60A1F4B0-E0		
	XXXXI * * * * * * * * * * * * *		Malware@#27		Success	60A1F4B0-E0		
	1919		ApplicUnwnt	Quarantine	Success	60A1F4B0-E0		
	2000		Malware@#2	Quarantine	Success	60A1F4B0-E0		
	\$770		Malware@#27		Success	60A1F4B0-E0		
	2710		Malware@#2	Quarantine	Success	60A1F4B0-E0		
	Stol		Malware@#27		Success	2832E3C6-B		
	2221		ApplicUnwnt	Quarantine	Success	2832E3C6-B		
	0.00		Malware@#27		Success	2832E3C6-B		
	Apr 26, 2019 /U				Success	2832E3C6-B		
	SSS21		Malware@#2	Quarantine	Success	2832E3C6-B		
	1821		Malware@#2	Quarantine	Success	2832E3C6-B		
	820		Malware@#27	Detect	Success	AA6E3850-4		
	1010		Malware@#27		Success	AA6E3B50-4		
		Jsers/comod	ApplicUnwnt	Detect	Success	AA6E3B50-4		
May 2019 4 . >	Apr 26, 2019 /U	Jsers/comod	ApplicUnwnt	Detect	Success	AA6E3B50-4		
Sume to we think to	Apr 26, 2019 /U	Jsers/comod	Malware@#2	Detect	Success	AA6E3B50-4		
28 25 20 1 2 3 4	Apr 26, 2019 /U	Jsers/comod	Malware@#2	Detect	Success	AA6E3B50-4		
5 6 7 8 9 10 11	Apr 29, 2019 /U	Jsers/comod	Malware@#27	Ignore	Success	6F4976BB-D		
12 13 14 15 16 17 18	Apr 29, 2019 /U	Jsers/comod	ApplicUnwnt	Ignore	Success	6F4976BB-D		
19 20 21 22 23 24 25	Apr 29, 2019 /U	Jsers/comod	Malware@#27	Ignore	Success	6F4976BB-D		
26 27 28 29 30 31	Apr 29, 2019 /U	Jsers/comod	ApplicUnwnt	Ignore	Success	6F4976BB-D		
2345578	Apr 29, 2019 /U	Jsers/comod	Malware@#2	Ignore	Success	6F4976BB-D		
	Apr 29, 2019 /U	Jsers/comod	Malware@#2	Ignore	Success	6F4976BB-D		
	a sala a	enter a substant a subs	100100100100000000000000000000000000000	We Ison with the test of t	THE REAL PROPERTY OF THE PROPERTY OF THE REAL PROPE			

- 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:



Logs per Module Antivirus Events	Malware Name	Contains) applid					
Other Logs	Antivirus Events							
Alerts Displayed	Date	Location	Malware Name	Action	Status	Scan UID	Alert	
Tasks Launched	Apr 26, 2019	/Users/comod	ApplicUnwnt	Quarantine	Success	D7650D68-9		
Configuration Changes	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	2832E3C6-B		
	Apr 26, 2019	/Users/comod	ApplicUnwnt	Quarantine	Success	2832E3C6-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	0000000-0		
	Apr 30, 2019	/Users/comod	ApplicUnwnt	Ignore	Success	0000000-0		
	10 million in the second							
	in the second second							
May 2019 4 • •								
Su Mo Tu We Th Fr Sa	Contraction of the local distance of the							
28 29 30 1 2 3 4								
5 6 7 8 9 10 11								
12 13 14 15 16 17 18								
19 20 21 22 23 24 25								
26 27 28 29 30 31 1								

- 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.



Logs per Module									
Antivirus Events	(Advice 0)	Contains	0						
Other Logs	Alerts Displayed								
Alerts Displayed	Date	Туре	Description	Advice	Answered	Answer	Flags Treat As	Event	
Tasks Launched	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod	Apr 29, 2019	Skip Once		Related event	
Configuration Changes	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	
May 2019 4 • •									
Su Mo Tu We Th. Fr. Sa									
28 Z9 30 1 2 3 4									
5 6 7 8 9 10 11									
12 13 14 15 16 17 18									
19 20 21 22 23 24 25 26 27 28 29 30 31									

- 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:



Date:	Apr 30, 2019 at 10:58 AM
Description:	ApplicUnwnt@#2975xfk8s2pq1
Advice:	/Users/comodo/Desktop/Unknown files/eicar.com.txt
Туре:	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:

	Alert	ApplicUnwnt	/Users/tester/
Antivirus	Alert	ApplicUnwnt	/Users/tester/
Antivirus	Re	fresh	/Users/tester/
Antivirus			/Users/tester/
Antivirus	✓ Ad	vanced Filter	/Users/tester/
Antivirus	Ew	- art	/Users/tester/
Antivirus	EX	port	/Users/tester/
Antivirus	Alert	ApplicUnwnt	/Users/tester/
	Alert	ApplicUnwnt	/Users/tester/

- 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 Comodo Client Security



- 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.

📅 Today 🗰 Currer	nt Week 🧮 Cu	rrent Month	📰 Entire Period		
▼Logs per Module Antivirus Events ▼Other Logs	Advice Answer Answered Description	Equal 0	Unknown	Disinfec	
Alerts Displayed	Treat As	Туре	Description	Advice	
Tasks Launched	Туре	Antivirus Alert	ApplicUnwnt	/Users/co	
Configuration Changes	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		

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

Logs per Module Antivirus Events	(Advice 0)	Contains	Jusers/				
Other Logs	Alerts Displayed	I					
Alerts Displayed	Date	Туре	Description	Advice	Answered	Answer	Flags
Tasks Launched	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod	Apr 29, 2019	Skip Once	
Configuration Changes	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod	Apr 29, 2019	Skip Once	
	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod		Skip Once	
	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod	Apr 29, 2019	Skip Once	
	Apr 30, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod		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	
Apr 2019 4 • •							
Su Mo Tu We Th Fr Sa							
3) 1 2 3 4 5 6							
7 8 9 10 11 12 13 14 15 16 17 18 19 20							
21 22 23 24 25 26 27							
2. 22 20 24 20 20 2/	1						



- 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.

Logs per Module Antivirus Events	Answer 0	Equal 0)	Quarantine	Skip Once	Add To Ex	clusions Gralsr
Other Logs	Alerts Displayed					
Alerts Displayed	Туре	Description	Advice	Answered	Answer Fl	ags Event
Tasks Launched Configuration Changes	Antivirus Alert		/Users/comod		Skip Once	Related event
Computation Changes	Antivirus Alert	ApplicUnwnt	/Users/comod		Skip Once	Related event
	Antivirus Alert	ApplicUnwnt	/Users/comod		Skip Once	Related event
	Antivirus Alert	ApplicUnwnt	/Users/comod		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
Apr 2019 🔹 • •						
Su Mo Tu We Th Fr Sa						
31 1 2 3 4 5 6						
7 8 9 10 11 12 13						
14 15 16 17 18 19 20 21 22 23 24 25 26 27						

- 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:



Logs per Module Antivirus Events	Answered C	Equal	03/05/ 2019)		3 (
Other Logs	Alerts Displayed					
Alerts Displayed	Туре	Description	Advice	Answered	Answer	Flags Event
Tasks Launched	Antivirus Alert	Malware@#27	/Users/comod	May 3, 2019 at 11:21 AM	Skip Once	Related eve
Configuration Changes	Antivirus Alert			May 3, 2019 at 11:21 AM		Related eve
	Antivirus Alert			May 3, 2019 at 11:21 AM		Related eve
Apr 2019 4 • •						
Su Mo Tu We Th Fr Sa						
Su Mo Tu We Th Fr Sa 31 1 2 3 4 5 6						
Su Mo Tu We Th Fr Sa 3 1 2 3 4 5 6 7 8 9 10 11 12 13						
Su Mo Tu We Th Fr Sa 31 1 2 3 4 5 6						

- 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:



🔍 🔍 🔍			Log Viewer			
Today 💼 Curren	t Week 🛛 🧮 Curr	ent Month	Entire Period			
 ▼Logs per Module Antivirus Events ▼Other Logs Alerts Displayed 	[Description 0] [(Contains () mal			•
Tasks Launched	Alerts Displayed					
Configuration Changes	COLO INTERNA DE LA COLORIZA DE LA C	Description	Advice	Answered	Answer	Flags Event
	Antivirus Alert	Malware@#27	/Users/comod	Apr 30, 2019 at 11:42 A	Skip Once	Related event
	N.0.1			May 3, 2019 at 11:21 AM		Related event
				May 3, 2019 at 11:21 AM		Related event
Apr 2019 4 • •						
Su Mo Tu We Th Fr Sa						
3 1 2 3 4 5 6						
7 8 9 10 11 12 13						
14 15 16 17 18 19 20						
21 22 23 24 25 26 27						
28 29 30 2 3						
5 6 7 8 9 10 33						
	(883)					

- 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.

Comodo Client - Security for MAC - User Guide



Logs per Module Antivirus Events	Туре	Equal 0	Antivirus Alert	Execution Alert					
Other Logs	Alerts Displayed	1							
Alerts Displayed	Date	Туре	Description	Advice	Answered	Answer	Flags	Treat As	
Tasks Launched	Apr 29, 2019	Antivirus Alert	ApplicUnwnt	/Users/comod	Apr 29, 2019	Skip Once			
Configuration Changes	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			
	2007 · ·	Antivirus Alert		/Users/comod					
	2211 ··· · · · · · · · · · · · · · · · ·	Antivirus Alert		/Users/comod	" "	5			
	0001 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Antivirus Alert		/Users/comod					
	2004 · · · · · · · · · · · · · · · · · ·	Antivirus Alert		/Users/comod					
	1100 E 10 I	Antivirus Alert		/Users/comod					
	May 3, 2019 a	Antivirus Alert	Malware@#2	/Users/comod	May 3, 2019 a	Skip Once			
Apr 2019 4 • •									
Su Mo Tu We Th Fr Sa									
31 1 2 3 4 5 6									
7 8 9 10 11 12 13									
14 15 16 17 18 19 20									
21 22 23 24 25 26 27									

- 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.



Logs per Module Antivirus Events	Code	Equal	\$			•
Other Logs	Tasks Launch	hed				
Alerts Displayed	Date	Туре	Parameter	Completed	Code	Info1
Tasks Launched	May 6, 2020	Antivirus Up	d	May 6, 2020	2	Old dat
Configuration Changes	May 6, 2020			May 6, 2020	0	Old dat
	May 6, 2020			May 6, 2020	1	Old dat
		Antivirus Up		May 6, 2020	1	Old dat.
		Antivirus Sc		May 6, 2020	0	Scanne
May 2020						
Su Mo Tu We Th Fr Sa						
26 27 28 29 30 1 2						
3 4 5 6 7 8 9						
10 11 12 13 14 15 16						
17 18 19 20 21 22 23						
24 25 26 27 28 29 30						

- 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 6, 2020 at 10:13 AM
Type:	Antivirus Update
Parameter:	(Empty)
Completed:	May 6, 2020 at 11:39 AM
Code:	2
Info1:	Old database 1
Info2:	New database 1
	Previous Next Close

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

Antivirus Scan	My Custom S	Mar 28, 2018,	
Antivirus Sca	D ()	1ar 28, 2018,	
Antivirus Sca	Refresh	ar 28, 2018,	
Antivirus Sc: 🗸	Advanced Filter	ar 28, 2018,	0
	Export		

- 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:

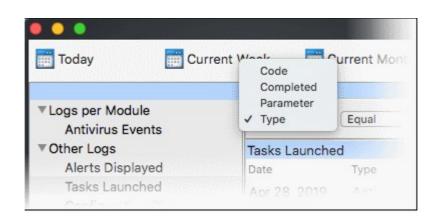
- Code Filter events by CCS internal code for the tasks
- Completed Filter by task end date and time
- **Parameter** Filter by AV scan type. Scan types include full scan, manual scan and quick scan. You can also filter by any custom scan that you have created.
- Type Filter by task category. Example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



Configure Event Filters

- Open Comodo Client Security
- 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)



Logs per Module Antivirus Events	Code	Equal	٥			
Other Logs	Tasks Launch	ed				
Alerts Displayed	Date	Туре	Parameter	Completed	Code	Info1
Tasks Launched	May 6, 2020.	Antivirus Upd		May 6, 2020	2	Old dat
Configuration Changes	May 6, 2020.			May 6, 2020	0	Old dat
	May 6, 2020.			May 6, 2020	1	Old dat
		Antivirus Upd		May 6, 2020	1	Old dat
		Antivirus Sca		May 6, 2020		Scanne
May 2020						
Su Mo Tu We Th Fr Sa						
26 27 28 29 30 1 2						
3 4 5 6 7 8 9						
10 11 12 13 14 15 16						

- 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.

Comodo Client - Security for MAC - User Guide



Logs per Module Antivirus Events	Completed 0 Equal	03/05/ 2019				: +
Other Logs	Tasks Launched					
Alerts Displayed	Date Type	Completed	Parameter	Code	Info1	Info2
Tasks Launched	May 3, 2019 a Antivirus Upd			0		New dat
Configuration Changes	May 3, 2019 a Antivirus Upd	A 0.		•		New dat
	May 3, 2019 a Antivirus Opd May 3, 2019 a Antivirus Upd			1		New dat
	May 3, 2019 a Antivirus Upd			1		New dat
	May 3, 2019 a Antivirus Opd May 3, 2019 a Antivirus Upd			0		New dat
	May 3, 2019 a Antivirus Opd May 3, 2019 a Antivirus Upd	· · · · · · · · · · · · · · · · · · ·		1		New dat
	May 3, 2019 a Antivirus Opu May 3, 2019 a Antivirus Scan		Manual Scan	0	0.00.0000000000	Found 6
	May 3, 2019 a Antivirus Upd		manual ocan	1		New dat
	May 3, 2019 a Antivirus Scan		Manual Scan	0		Found €
	May 3, 2019 a Antivirus Upd	7 1	manual oran	1		New da
	May 3, 2019 a Antivirus Upd			1	Info1 Old database Old database Old database Old database Old database Scanned 8 Old database Old database Old database Old database Old database Old database Old database Old database Old database Old database	New da
	May 3, 2019 a Antivirus Scan		Manual Scan	0		Found 6
	May 3, 2019 a Antivirus Upd			0		New da
	May 3, 2019 a Antivirus Upd			1		New da
Apr 2019 4 • •	May 3, 2019 a Antivirus Scan		Important Do	0		Found 2
Su Mo Yu We Th Fr Sa	May 3, 2019 a Antivirus Upd			1		New da
31 1 2 3 4 5 6	indy of 2010 and 10111100 of an					
7 8 9 10 11 12 13						
14 15 16 17 18 19 20						
21 22 23 24 25 26 27						

- 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.

Comodo Client - Security for MAC - User Guide



Antivirus Events	Statement and a state of the state	Contains	🖄 man				
Other Logs	Tasks Launched						
Alerts Displayed	Date	Туре	Completed	Parameter	Code	Into1	Info2
Tasks Launched	Apr 29, 2019	Antivirus Scan	Apr 29, 2019 at 3:13 PM	Manual Scan	0	Scanned 1	Found
Configuration Changes			May 3, 2019 at 9:26 AM	Manual Scan	0	Scanned 8	Found
	May 3, 2019 a	Antivirus Scan	May 3, 2019 at 9:28 AM	Manual Scan	0	Scanned 8	Found
	May 3, 2019 a	Antivirus Scan	May 3, 2019 at 11:05 AM	Manual Scan	0	Scanned 8	Found
Apr 2019 🖪 🕈 🕨							
Su Mo Tu We Th Fr Sa .: 1 2 3 4 5 6							
2 8 9 10 11 12 13							
14 15 16 17 18 19 20	Contradict and a first a first a first a first a first						

- 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.

Logs per Module Antivirus Events	(Туре С)	Equal 0	Av Update C	Av Scan 🗆 L	og Clearing	Opgrade	
Other Logs	Tasks Launched						
Alerts Displayed	Date	Туре	Parameter	Completed	Code	info1	Info2
Tasks Launched	Apr 28, 2019	Antivirus Upd		Apr 28, 2019	1	Old database	New database 3
Configuration Changes	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 2019 🔹 🕨 🕨	Apr 29, 2019	Antivirus Upd		Apr 29, 2019	0	Old database	New database 3.
Su Mo Tu We Th Fr Sa	Apr 29, 2019	Antivirus Upd		Apr 29, 2019	1	Old database	New database 3.
31 1 2 3 4 5 6 7 8 9 10 11 12 13	Apr 29, 2019	Antivirus Scan	Manual Scan	Apr 29, 2019	0	Scanned 1	Found 0
14 15 16 17 18 19 20	Apr 29, 2019	Antivirus Upd		Apr 29, 2019	1	Old database	New database 3.
21 22 23 24 25 26 27	Apr 29, 2019	Antivirus Upd		Apr 29, 2019	1	Old database	New database 3.
21 22 23 24 25 26 27	Apr 29, 2019	Antivirus Upd		Apr 29, 2019	0	Old database	New database 3.
5 6 7 8 3 10 11	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 Und.		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:

		Log Vie	wer			
🧰 Today 📰 Current	t Week 🛛 🧮 Cu	irrent Month	🧰 Entire P	eriod		
▼Logs per Module Antivirus Events	Action 0 Ec	qual 🔿 🗆 Obj	ect Added	Object Changed	Object Removed	+
▼ Other Logs	Configuration C	hanges				
Alerts Displayed	Date	Action	Modifier	Object	Name	Old Value
Tasks Launched	May 6, 2020	Added	User	Antivirus Excl	/Users/comod	
Configuration Changes	May 6, 2020	Added	User	Antivirus Sch	Daily scan of	
	May 6, 2020	Changed	User	Antivirus Sch	Daily scan of	{"UID":
	May 6, 2020	Added	User	Antivirus Sch	weekly Custo	
	May 6, 2020	Changed	User	Antivirus Sch	weekly Custo	{"UID":
	May 6, 2020	Removed	User	Antivirus Sch	Daily scan of	{"UID":
	May 6, 2020	Added	User	Antivirus Profile	My daily scan	
	May 6, 2020	Option Chang	User	Log overflow		Delete
	May 6, 2020	Option Chang	User	Log backup f		
	May 6, 2020	Option Chang	User	Log backup f		/Users/
	May 6, 2020	Option Chang	User	Log backup f		/Users/
May 2020 🖪 🔍 🕨						
Su Mo Tu We Th Fr Sa						
26 27 28 29 30 1 2						
3 4 5 6 7 8 9						
10 11 12 13 14 15 16						
17 18 19 20 21 22 23						
24 25 26 27 28 29 30						
31 1 2 3 4 5 6						

- 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:

Date:	May 6, 2020 at 4:37 PM
Name:	Daily scan of externel devices
Old Value:	{ "UID" : "E02799A0-667F-46E9-839E-8FBC663F1073", "Minute" : 0, "WeekDays" : 54, "Name" : "Daily scan of externel devices", "Hour" : 0, "Profile! IID" : "E140D794-60B6-4E00-9235-D6457AA25B22"
New Value:	{ "UID" : "E02799A0-667F-46E9-839E-8FBC663F1073", "Minute" : 0, "WeekDays" : 54, "Name" : "Daily scan of external devices", "Hour" : 0, "ProfileLIID" : "E140D794-60B6-4E00-9235-D6457AA25B22"
Action:	Changed
Object:	Antivirus Schedule
Modifier:	User

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

2020	Added	User
20 20	Added	User
2020	Refresh	ser
2020		ser
2020 🗸	Advanced Filter	ser
2020	Evport	ser
2020	Export	ser
2020	Option Chang	User
2020	Option Chang	User
20 20	Option Chang	User

- 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

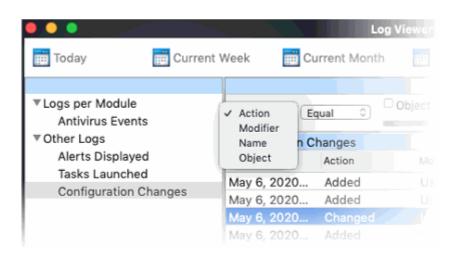
You can create custom views of logged events according to the following criteria:

- 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 Comodo Client Security
- 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.



Today 📰 Curre	ent Week 💼 Cu	urrent Month	📰 Entire Pe	eriod		
Logs per Module Antivirus Events	Action 0 Ec	qual 🔿 🗆 (Dbject Added	Object Changed	Object Removed	+
Other Logs	Configuration C	hanges				
Alerts Displayed	Date	Action	Modifier	Object	Name	Old Val
Tasks Launched	May 6, 2020	Added	User	Antivirus Excl	/Users/comod	
Configuration Changes	May 6, 2020	Added	User	Antivirus Sch	Daily scan of	
	May 6, 2020	Changed	User	Antivirus Sch	Daily scan of	{"UID"
	May 6, 2020	Added	User	Antivirus Sch	weekly Custo	-
	May 6, 2020	Changed	User	Antivirus Sch	weekly Custo	{"UID"
	May 6, 2020	Removed	User	Antivirus Sch	Daily scan of	{"UID'
	May 6, 2020	Added	User	Antivirus Profile	My daily scan	
	May 6, 2020	Option Chang	User	Log overflow		Delete
	May 6, 2020	Option Chang	J User	Log backup f		
	May 6, 2020	Option Chang		Log backup f		/Users
	May 6, 2020	Option Chang	J User	Log backup f		/Users
May 2020 🖪 🖉 🕨						
Su Mo Tu We Th Fr Sa						
26 27 28 29 30 1 2						
3 4 5 6 7 8 9						
10 11 12 13 14 15 16						
17 18 19 20 21 22 23						
24 25 26 27 28 29 30 31 1 2 3 4 5 6						

- 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.



* Logs per Module Antivirus Events	(Modifier 0) E	anal () CRe	91	O Auto Learn O Ant	ivirus Alert 🔅 I	Execution Alert	
▼ Other Logs	Configuration C	hanges					
Alerts Displayed	Date	Action	Modifier	Object N	lame	Old Value	New Value
Tasks Launched	Apr 23, 2019	Option Chang	User	Antivirus: Sch		Off	On
Configuration Changes	Apr 23, 2019	Option Chang		Antivirus: Sch		Off	On
	Apr 23, 2019	Changed	User	Antivirus Excl			/Library/Appli
	Apr 23, 2019	Changed	User	Antivirus Profile		0	[{"UID":"F140
	Apr 23, 2019	Changed	User	Antivirus Sch		0	[{"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 0	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
May 2019 🔹 🔹 🕨	Apr 26, 2019	Option Chang	User	Show balloon		Off	On
Su Mo Tu We Th Fr Sa	Apr 26, 2019	Option Chang	User	Updates host		[{"Enable":tru	[{"Enable":tru.
28 29 30 1 2 3 4 5 6 7 8 9 10 11	Apr 26, 2019	Option Chang	User	Antivirus: Mode		Disabled	On Access
12 13 14 15 16 17 18	Apr 26, 2019	Option Chang	User	Antivirus: Ma		On	Off
19 20 21 22 23 24 25	Apr 26, 2019	Option Chang	User	Antivirus: Sch		On	Off
26 27 28 29 30 31	Apr 29, 2019	Option Chang	User	Antivirus: Mode		Disabled	On Access
2 3 4 5 6 7 8	Apr 30, 2019	Added	User	Antivirus Profile	mportant Files		{"Paths":["/Ap
	Apr 30, 2019	Changed	User	Antivirus Profile		[{"UID":"F140	[{"UID":"F140.
	Apr 30, 2019	Added	User	Antivirus Profile S	Suspicious Fil		{"Paths":["/An

- 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:



Logs per Module Antivirus Events	Name 0) Contains 0	3				
Other Logs	Configuration Changes					
Alerts Displayed	Date	Action	Modifier	Object	Name	Old Value
Tasks Launched	Apr 26, 2019 at 2:57 PM	Option Chang	User	Antivirus: Ma		On
Configuration Changes	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":"F14
	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":"F14
	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":"F14
	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":"F14
	Apr 30, 2019 at 11:08 AM	Changed	User	Antivirus Profile		[{"UID":"F14
	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/App
May 2019 🔹 🕨 🕨	Apr 30, 2019 at 2:02 PM	Changed	User	Antivirus Sch		[{"Minute":0
Su Mo Tu We Th Fr Sa	Apr 30, 2019 at 2:02 PM	Added	User	Antivirus Sch	Test Mac scan	
28 29 30 1 2 3 4 5 6 7 8 9 10 11	Apr 30, 2019 at 2:04 PM	Changed	User	Antivirus Sch		[{"UID":"175
	Apr 30, 2019 at 2:04 PM	Option Chang	User	Antivirus: Mode		On Access
19 20 21 22 23 24 25	Apr 30, 2019 at 2:05 PM	Option Chang	User	Antivirus: Rea		Off
26 27 28 29 30 31	Apr 30, 2019 at 2:05 PM	Option Chang	User	Antivirus: Mode		Disabled
2 3 4 5 6 7 8	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":"175F

- 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.



VLogs per Module	(Object 0) Ed	aual 0) 🗆 Ant	ivirus: Mode		⊂ An	tivirus: Alert Timed	out
Antivirus Events Other Logs	Configuration C	hannes					
Alerts Displayed	Date	Action	Modifier	Object	Name	Old Value	New Value
Tasks Launched	Apr 23, 2019	Option Chang		Antivirus: Sch		Off	On
Configuration Changes	Apr 23, 2019	Option Chang		Antivirus: Sch		Off	On
here in the second states of the second	Apr 23, 2019	Changed	User	Antivirus Excl		011	/Library/Appli.
	Apr 23, 2019	Changed	User	Antivirus Profile		п	[{"UID";"F140.
	Apr 23, 2019	Changed	User	Antivirus Sch		0	[{"UID":"175F.
	Apr 23, 2019	Option Chang	User	Auto check u		Off	On
	Apr 23, 2019	Option Chang		Show balloon		On	Off
	Apr 23, 2019	Option Chang		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
May 2019 4 • •	Apr 26, 2019	Option Chang	User	Show balloon		Off	On
Su Mo Tu We Th Fr Sa	Apr 26, 2019	Option Chang	User	Updates host		[{"Enable":tru	[{"Enable":tru
28 29 33 1 2 3 4 5 6 7 8 9 10 11	Apr 26, 2019	Option Chang	User	Antivirus: Mode		Disabled	On Access
5 6 7 8 9 10 11 12 13 14 15 16 17 18	Apr 26, 2019	Option Chang	User	Antivirus: Ma		On	Off
19 20 21 22 23 24 25	Apr 26, 2019	Option Chang	User	Antivirus: Sch		On	Off
26 27 28 29 30 31	Apr 29, 2019	Option Chang	User	Antivirus: Mode		Disabled	On Access
2 3 4 3 6 7 8	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'



\bullet \bullet	Run a Scan	
Please select an item to laund	h 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. 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:

••	C	DMODO Client - Security - Scar	n Finished
	anning: atus:	Scan Finished /Users/comodo/Desktop/Sus.	f68ecbb0d19e1f29dafdc.exe
Objects Scanne	ed: 10	Start Time:	May 5, 2020 at 9:59 AM
Threats Found:	5	Duration:	0:00:00
✓ Show on top			
What do these :	settings	do?	Results

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



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

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	
What do these settings do? Create New So	an Scan Close

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

List of items: Path /Users/tester/Documents/test_set	My Custom Scans	
/Users/tester/Documents/test_set	Path	

- Repeat the process to add more items.
- Click 'Apply' to save your profile.

•

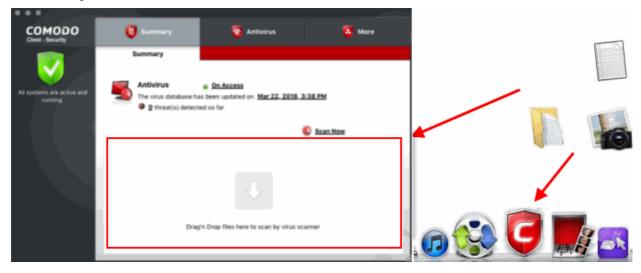
• You can now select this profile after clicking 'Run a scan' or 'Scan Now'.

For more details on custom scan creation, see Create 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



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 Comodo Client Security at the summary screen
- Click the number in front of 'Threat(s) detected so far'



stems are active and running.	ntivirus <u>o</u> e virus database has been <u>56</u> threat(s) detected so		<u>Mar 22, 20</u>	018, <u>4:53 PM</u>
				Scan Now
	Antivirus Ever			
Location	Malware Name	Action	Status	Date
/Volumes/run-test/testset_all_viru	Malware@#18f95	. Ignore	Success	Mar 22, 2018
	TroiWaro IS Troia	Quaran	Success	Mar 22, 2018
/Users/tester/Documents/test_set	nojware.55.noja		0000000	Mar 22, 2010
/Users/tester/Documents/test_set /Users/tester/Documents/test_set				
	t TrojWare.HTML.lf	. Quaran		Mar 22, 2018
/Users/tester/Documents/test_set	t TrojWare.HTML.If t TrojWare.JS.Redi	. Quaran Remove	Success	Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6o81	Quaran Remove Ignore	Success Success	Mar 22, 2018 Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6o81 t Malware@#34pa	Quaran Remove Ignore Ignore	Success Success Success Success	Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6081 t Malware@#34pa t TrojWare.HTML.lf	Quaran Remove Ignore Ignore	Success Success Success Success Success	Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6081 t Malware@#34pa t TrojWare.HTML.lf t	Quaran Remove Ignore Ignore False P False P	Success Success Success Success Success	Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6081 t Malware@#34pa t TrojWare.HTML.lf t t TrojWare.BAT.Ag	Quaran Remove Ignore Ignore False P False P Detect	Success Success Success Success Success Success	Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6081 t Malware@#34pa t TrojWare.HTML.lf t t TrojWare.BAT.Ag t TrojWare.JS.Troja	Quaran Remove Ignore Ignore False P False P Detect Detect	Success Success Success Success Success Success Success	Mar 22, 2018 Mar 22, 2018
/Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set /Users/tester/Documents/test_set	t TrojWare.HTML.lf t TrojWare.JS.Redi t Malware@#6081 t Malware@#34pa t TrojWare.HTML.lf t t TrojWare.BAT.Ag t TrojWare.JS.Troja t Malware@#1e8yu	Quaran Remove Ignore Ignore False P False P Detect Detect Detect	Success Success Success Success Success Success Success Success	Mar 22, 2018 Mar 22, 2018

• 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:

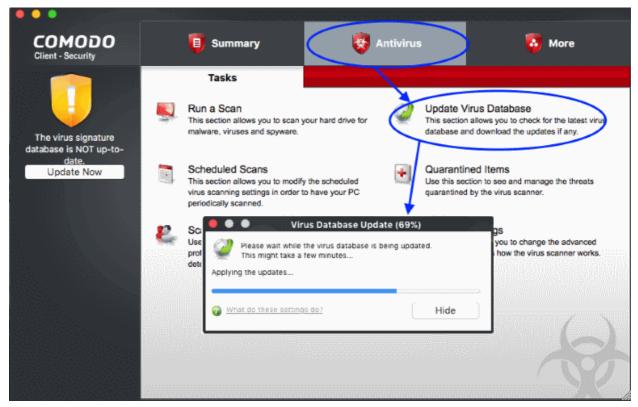
- Manually update the virus database
- Configure automatic database updates

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.



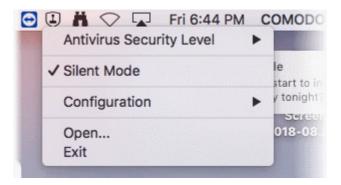
Configure automatic database updates before scanning

- 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

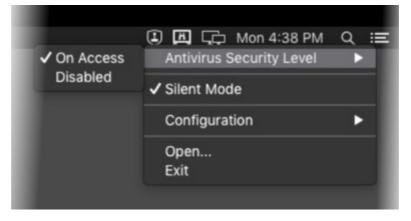
See 'Scanner Settings' if you need more help with this.

Quickly Set up Security Levels

Right-click on the CCS menu bar 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.

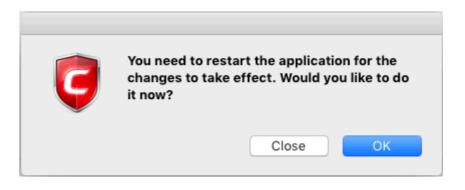
You can also access these settings through the the summary screen.

Change CCS Language Settings

- 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:

•••			
COMODO Client - Security	O Summary	🐯 Antivirus	s 🚱 More
	More		
You haven't performed a full scan yet!	Preferences This section lets you configure language, update options etc.	general settings like	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.
Do it now	Manage My Configuratio This section allows you to impo Antivirus configuration settings.	rt/export/delete your 🛛 💆	Help Do you want to learn more about your Antivirus? You can use this section to view the help file.
	Diagnostics	<u> </u>	About
• • •		Settings	
1.1	Language	Logging Update)
Select Language D	efault - English (United S	States) ᅌ	
What do these setting	<u>gs do?</u>		ОК

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



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.





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			
📀 <u>Wh</u>	at do these settings do?	Hide	

Scanning will commence immediately after the updates are installed.

	Scanning: My Custom Scan Profile			
	Scanning: Status:	My Custom Scan Profile /Volumes/run-test/AVb1136f5327b200bf7f2		
Objects Scanr # Threats Found		Start Time: Duration:	Mar 28, 2018, 1:59 PM 00:00:04	
 Show on top What do these settings do? Pause Stop Scan 				

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:

• • •		
COMODO Client - Security	🔋 Summary 🛛 🤯 Antivir	us 🦉 More
The virus signature database is NOT up-to- date. Update Now	Tasks Image: A constraint of the section allows you to scan your hard drive for maware, viruses and spyware. Scheduled Scans This section allows you to modify the scheduled your PC periodically scanned. Scheduled Scans Scheduled Scans <	Update Virus Database This section allows you to check for the latest virus database and download the updates if any. Quarantined Items Use this section to see and manage the threats quarantined by the virus scanner.
Schedule Na	me	Add
Weekly Vir	Scan Schedule Name:	Edit Remove
	Weekly Custom Schedule Profile:	
2 What	Full Scan Image: Constraint of the week: Image: Days of the week: Image: Constraint of the week: Image: Monday Image	Close
	Start time: 3:00 AM 🗘	
	Cancel Apply	



- 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:

• /		Scheduled Scans	
	Schedule Name Weekly Virus Scanning Weekly Custom Schedule		Add Edit Remove
2	What do these settings do?		Close

- 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
- Click 'Restore'



ltem	Location ^	Date/Time	Add
	/Users/comodo/ /Users/comodo/	05-May-2020 at 05-May-2020 at	Delete
Malware@#18	/Users/comodo/	@ 05-May-2020 at 🤇	Restore
-	/Users/comodo/ /Users/comodo/	2 05-May-2020 at 05-May-2020 at	Clear
	Add the file to t	he exclusions list, so the	at it
	is always skippe	ed	

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

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

Switch off Automatic Antivirus Updates

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

• • •		
COMODO Client - Security	🔋 Summary 🔯 Antivirus 🖏 More	
	Tasks	
All systems are active and running.	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 the 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.	
• • •	Virus Scanner Settings	
Real	Time Scanning Manual Scanning Scheduled Scanning Exclusions	
Real Time Scann	s 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 la	arger 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':

COMODO Client - Security	🯮 Summary (🐯 Antiviru:	s 🔰 🐯 More	
	Tasks			
All systems are active and running.	Run a Scan This section allows you to scar 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 mod virus scanning settings in order periodically scanned.	· · · · · · · · · · · · · · · · · · ·	Quarantined Items Use this section to see and manage the threats guarantined by the virus scanner.	
	Scan Profiles Use this section to add/remove profiles which are used by the determine the objects to be sca	virus scanner to	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 Sca	nning Scheduled Sc	anning Exclusions	
·				
Detection				
🗹 Scan archive file	es			
🗌 Automatically qu	uarantine threats found during	scanning		
Automatically up	odate virus database before sc	anning		
Enable cloud sci		Ū.		
	ction is required			
Do not scan files la	rger than (MB)	20		
What do these sett	ings do?		ОК	

• 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':

COMODO Client - Security	🧻 Summary 🌔	🐯 Antiviru	s 👌 More
	Tasks		
All systems are active and running.	Run a Scan This section allows you to scan matware, viruses and spyware.	your hard drive for	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 modi virus scanning settings in order 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 profiles which are used by the v determine the objects to be sca	rirus scanner to	Scanner Settings This section allows you to change the advanced settings that affects how the virus scanner works.
• • •	Virus	Scanner Settings	
Peal 1	Time Scanning Manual Sca		canning Exclusions
· · · · · · · · · · · · · · · · · · ·	mine ocanning - Mandar oca	ining concource of	Excitations
Detection			
🗹 Scan archive file:	S		
Automatically qu	arantine threats found during	scanning	
	date virus database before sc		
Show scan progr	ess		
Enable cloud sca	inning		
🔔 Internet connec	ction is required		
Do not scan files lar	ger than (MB)	20	
What do these setting	ngs do?		ОК

• Click 'OK'.

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

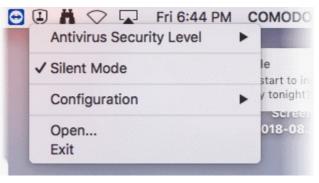


Suppress Alerts with Silent mode

- 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 menu bar icon
- Select 'Silent Mode' from the options:



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